MobileIron Cloud Derived Credential Guide

Revised: January 6, 2021

For complete product documentation see:
MobileIron Cloud Product Documentation

Revision history

TABLE 1. REVISION HISTORY

Date	Revision
January 6, 2021	• Updated date to reflect the general availability of the PIV-D Manager app. The PIV-D Manager app was previously available as a limited release on December 14.
December 14, 2020	• Limited availability. • MobileIron PIV-D Entrust is renamed to MobileIron PIV-D Manager. • Removed Intercede derived credential support for Android.
May 28, 2019	• Clarified non-AppConnect app use case for Using Entrust for push notification authentication to enterprise servers (iOS only).
April 15, 2019	• Added Intercede derived credential support for Android. • Added Bluetooth-related enhancements for Entrust derived credentials supported by the PIV-D Manager app 2.2 for iOS. ◦ Creating, changing, and resetting the derived credential PIN ◦ Reconnecting Bluetooth connection automatically
March 5, 2019	Added Bluetooth-related enhancements supported by the PIV-D Manager app 1.3 for Android. • Creating, changing, and resetting the derived credential PIN • Reconnecting Bluetooth connection automatically
January 9, 2019	• Added Bluetooth feature. • Added authentication confirmation to web services. (Entrust and iOS)

Contents

About Derived Credentials with MobileIron Cloud

Smart cards contain identity certificates that give your users access to various computing resources without using passwords. The identity certificates make up the user's *primary credential*. A *derived credential*:

- derives from the primary credential.
  The derived credential contains identity certificates derived from the primary credential's identity certificates. Therefore, if the primary credential becomes revoked or expired, the derived credential also becomes revoked or expired.
- is an X.509 public key certificate
- is stored on the user's mobile device.

Apps on the user's iOS or Android mobile device can use these derived identity certificates for these purposes:

TABLE 2. PURPOSES FOR USING DERIVED CREDENTIALS

Purpose	Supported platforms
Authenticating to your backend servers, such as web servers, app servers, or content servers	iOS and Android
Authenticating to your backend email server	iOS and Android
Digital signing	iOS and Android
Encryption	iOS and Android

Typically, a different identity certificate is used for authentication, signing, and encryption. The identity certificates each have the same identity information, but the private and public key pair for each is different.

Mobile device requirements for using derived credentials

To use a derived credential on a mobile device:

- The device must be an iOS or Android device.
- The device must be registered to MobileIron Cloud.
- The device must have the MobileIron Go app installed.
- An Android device must have the Secure Apps Manager app installed.

- The app that uses the derived credential must be an AppConnect app.
- The device must have an app that obtains derived credentials from a derived credential provider. This app is known as a *derived credential app*. The required app depends on the derived credential provider and device platform.

The following table shows the derived credential providers that MobileIron Cloud supports on iOS and Android, and the required derived credential app.

TABLE 3. DERIVED CREDENTIAL APP REQUIRED FOR EACH PROVIDER AND DEVICE PLATFORM

Derived credential provider	Device platform	Derived credential app
Entrust	iOS	PIV-D Manager
	Android	PIV-D Manager • Android AppConnect
DISA Purebred	iOS	PIV-D Manager
Other	iOS	A third-party derived credential app for iOS created specifically for the derived credential provider. This app is built with the AppConnect for iOS SDK using APIs provided by MobileIron.

App use cases for derived credentials

The following table shows what AppConnect apps can use derived credentials and for what purposes.

TABLE 4. APPCONNECT APPS THAT CAN USE DERIVED CREDENTIALS AND THEIR USE CASES

App	Supported Platforms	Use cases
Email+	iOS Android	• S/MIME signing • S/MIME encryption • Identifying and authenticating the email user to the email server NOTE: Email+ *supports* certificate-based authentication using derived credentials with Microsoft Exchange servers only. However, Email+ usage of certificate-based authentication using derived credentials is *compatible* with any ActiveSync server that supports certificate-based authentication.
Web@Work	iOS Android	• Identifying and authenticating the Web@Work user to backend servers
Docs@Work	iOS Android	• Identifying and authenticating the Docs@Work user to content servers
In-house AppConnect apps	iOS Android	• Any use of identity certificates in an app's key-value pairs. • iOS only: Identifying and authenticating the app user to backend services using AppConnect for iOS certificate authentication provided by the AppConnect for iOS library. NOTE: MobileIron Cloud does not support derived credentials with third-party iOS AppConnect apps, which are imported from the Apple App Store.

NOTE: Non-AppConnect apps on iOS devices can use Entrust derived credentials to authenticate to enterprise servers or web services that use SAML-based authentication. See Using Entrust for push notification authentication to enterprise servers (iOS only).

MobileIron products involved with derived credentials

The following table shows the MobileIron products involved with using derived credentials.

TABLE 5. MOBILEIRON PRODUCTS INVOLVED WITH USING DERIVED CREDENTIALS

Product	Role in supporting derived credentials
MobileIron Cloud	You configure MobileIron Cloud so that the appropriate AppConnect apps use derived credentials.
MobileIron Go for iOS	On iOS devices: • Registers the device users with MobileIron Cloud • Stores the derived credential that a derived credential app obtained from a derived credential provider. • Delivers the certificates from the credential to the appropriate AppConnect apps.
MobileIron Go for Android	On Android devices: • Registers the device users with MobileIron Cloud • Passes information between the Secure Apps Manager and MobileIron Cloud.
Secure Apps Manager for Android	On Android devices: • Stores the Entrust derived credential. • Delivers the certificates from the credential to the appropriate AppConnect apps.
PIV-D Manager app for Android AppConnect	On Android devices: • Obtains the Entrust derived credential from Entrust. • Delivers the credential to the Secure Apps Manager.
PIV-D Manager app for iOS	On iOS devices: • Obtains the derived credential from Entrust or DISA Purebred • Delivers the credential to MobileIron Go for iOS.
iOS: AppConnect for iOS SDK or wrapper used in in-house AppConnect apps **Android:** the AppConnect wrapper	Provides AppConnect functionality to apps. Only AppConnect apps can use derived credentials.
Standalone Sentry	Provides email access control and AppTunnel support for iOS AppConnect apps using derived credentials, just as it does for any app.

NOTE: On iOS devices, for derived credential providers other than those supported by the PIV-D Manager app, a third-party derived credential app can be used. The app must be built with MobileIron-provided APIs in the AppConnect for iOS SDK. It obtains a derived credential from the derived credential provider and delivers the credential to Mobile@Work.

Related topics

- App use cases for derived credentials
- For information about supported and compatible versions of MobileIron components, see:
  - *MobileIron Cloud Release Notes*
  - *MobileIron Go for iOS Release Notes*

- *MobileIron Go for Android Release Notes*
- *Android Secure Apps Release Notes and Upgrade Guide*
- *MobileIron PIV-D Manager App for iOS Release Notes*
- *MobileIron PIV-D Manager App for Android Release Notes*

2

Derived Credentials Setup Overview

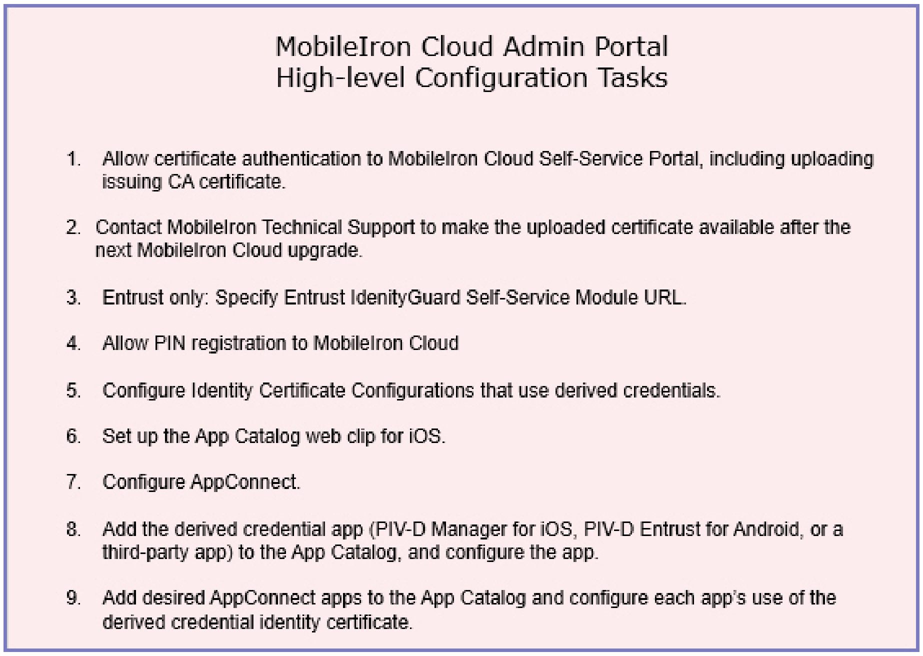
Setting up your device users to use derived credentials in their AppConnect apps requires the following:

- You configure MobileIron Cloud to support derived credentials.
  See What you configure on MobileIron Cloud to use derived credentials.
- Device users set up their devices to use derived credentials.
  See Device user tasks to use derived credentials.

What you configure on MobileIron Cloud to use derived credentials

The following list shows the high-level configuration tasks necessary on MobileIron Cloud to support derived credentials for AppConnect.

FIGURE 1. HIGH-LEVEL CONFIGURATION TASKS ON ADMIN PORTAL



MobileIron Cloud Admin Portal
High-level Configuration Tasks

1. Allow certificate authentication to MobileIron Cloud Self-Service Portal, including uploading issuing CA certificate.
2. Contact MobileIron Technical Support to make the uploaded certificate available after the next MobileIron Cloud upgrade.
3. Entrust only: Specify Entrust IdenityGuard Self-Service Module URL.
4. Allow PIN registration to MobileIron Cloud
5. Configure Identity Certificate Configurations that use derived credentials.
6. Set up the App Catalog web clip for iOS.
7. Configure AppConnect.
8. Add the derived credential app (PIV-D Manager for iOS, PIV-D Entrust for Android, or a third-party app) to the App Catalog, and configure the app.
9. Add desired AppConnect apps to the App Catalog and configure each app's use of the derived credential identity certificate.

The following table provides more details. The table:

- Describes each configuration task related to derived credentials that is necessary on MobileIron Cloud.
- Indicates to which derived credential providers and device platform (iOS, Android AppConnect) the task

applies.

- Provides a cross-reference to the detailed steps for each task.

NOTE: The task list assumes that you want device users to register MobileIron Go using a registration PIN rather than with a user ID and password, since typically, device users who use smart cards do not have passwords. However, using a registration PIN is a requirement only with Entrust derived credentials. For other derived credential providers, it is not a requirement, and therefore the related tasks are optional.

TABLE 6. DERIVED CREDENTIALS CONFIGURATION TASKS ON MOBILEIRON CLOUD

Task	Notes
1. Allow device users to authenticate to the MobileIron Cloud self-service user portal with the identity certificate on their smart cards. **Related topics** Configuring certificate authentication to the MobileIron Cloud Self-Service Portal	Allowing certificate authentication includes uploading to Cloud a valid issuing (CA) certificate or a valid supporting certificate chain. **Entrust** This task is required for Entrust derived credentials, because it is a prerequisite for configuring Cloud to use the Entrust IdentityGuard Self-Service Module (SSM) URL. **All other derived credentials providers** Although not strictly required for other derived credential providers, device users who use smart cards typically do not have passwords. Therefore, if you want them to be able to access the self-service user portal to, for example, generate a registration PIN, this step is required. IMPORTANT: The certificate that you upload to MobileIron Cloud is not immediately available for device users to authenticate against. It is only available for authentication after the next MobileIron Cloud upgrade. Contact MobileIron Technical Support to ask MobileIron to make your certificate available for use after the next upgrade.
2. Provide the Entrust IdentityGuard Self-Service Module (SSM) URL to MobileIron Cloud. **Related topics** Configuring the Entrust IdentityGuard SSM Module URL	**Entrust** MobileIron Cloud uses this URL to get derived credentials from Entrust. The device user will use the PIV-D Manager app for iOS or the PIV-D Manager app for Android to activate the derived credential on a device.
3. Allow device users to register MobileIron Go on their devices to MobileIron Cloud using a one-time registration PIN.	**Entrust** This task is required for Entrust derived credentials because device users need a registration PIN to request an Entrust derived credential.

TABLE 6. DERIVED CREDENTIALS CONFIGURATION TASKS ON MOBILEIRON CLOUD (CONT.)

Task	Notes
Related topics Configuring PIN-based registration	**All other derived credentials providers** Although not strictly required for other derived credential providers, device users who use smart cards typically do not have passwords. Therefore, if you want them to be register MobileIron Go using a one-time registration PIN, this step is required.
4. Configure Identity Certificate Configurations that use derived credentials. **Related topics** Configuring an identity certificate for derived credentials	**All derived credential providers** The activated derived credentials are stored in MobileIron Go for iOS or Secure Apps Manager for Android. Each of these components provides an identity certificate from the derived credential to the AppConnect app. You configure an AppConnect app to use derived credentials by referencing an Identity Certificate Configuration that specifies using derived credentials. The reference to the Identity Certificate Configuration is in the app's AppConnect Certificate Configuration. You configure an Identity Certificate Configuration for one of these purposes, as needed: authentication, signing, or encryption.
5. Set up the App Catalog web clip for device users. **Related topics** Configuring the App Catalog web clip for iOS	**All derived credential providers** **iOS only** You use the App Catalog web clip on devices to distribute apps from the MobileIron Cloud App Catalog.
6. Configure AppConnect. **Related topics** Configuring AppConnect for iOS Configuring AppConnect for Android	**All derived credential providers** Configuring AppConnect allows device users to use AppConnect apps, including the derived credential app.
7. Add the derived credential app to the App Catalog on MobileIron Cloud. **Related topics** Adding the PIV-D Manager app for iOS to the App Catalog Adding a third-party iOS derived credential app to the App Catalog Adding the PIV-D Manager app for Android to the App Catalog	**Entrust on Android** Add the PIV-D Manager app for Android to the App Catalog on MobileIron Cloud. **Entrust and DISA Purebred on iOS** Add the PIV-D Manager app for iOS to the App Catalog on MobileIron Cloud **Other derived credential providers on iOS** Add the appropriate third-party derived credential app to the App Catalog on MobileIron Cloud.

TABLE 6. DERIVED CREDENTIALS CONFIGURATION TASKS ON MOBILEIRON CLOUD (CONT.)

Task	Notes
8. Configure the PIV-D Manager app for iOS. **Related topics** Adding the PIV-D Manager app for iOS to the App Catalog Configuring the PIV-D Manager app for iOS for analytics Configuring the PIV-D Manager app for iOS for feedback	**iOS only** Configure the PIV-D Manager app for iOS as follows: **Entrust** • Configure the Entrust activation URL that MobileIron Cloud sends to the PIV-D Manager app so that the app can activate the device user’s derived credentials. • Configure a unique device identifier that the PIV-D Manager app sends to the Entrust IdentityGuard server. The identifier allows an administrator to determine which device contains a given derived credential, allowing control around auditing and revocation. **DISA Purebred** • Configure the PIV-D Manager app to support DISA Purebred derived credentials. **For both Entrust and DISA Purebred** • Configure the PIV-D Manager app to turn on or off analytics reporting. • Configure the PIV-D Manager app to allow the device user to send feedback to a specified email address.
9. Configure the PIV-D Manager app for Android. **Related topics** Adding the PIV-D Manager app for Android to the App Catalog	**Entrust** **Android only** Configure the PIV-D Manager app for Android to: • receive the Entrust activation URL from MobileIron Cloud so that it can activate the device user’s derived credentials. • send a unique device identifier to the Entrust IdentityGuard server. The identifier allows an administrator to determine which device contains a given derived credential, allowing control around auditing and revocation.
10. Configure a third-party iOS derived credential app. **Related topics** Adding a third-party iOS derived credential app to the App Catalog	**Derived credential providers other than Entrust or DISA Purebred** **Derived credential providers other than Entrust or DISA Purebred** **iOS only** You configure an iOS third-party derived credential app to receive app-specific settings from MobileIron Cloud, as defined by the app vendor or developer.
11. Add the AppConnect apps that will use the derived credential to the App Catalog on MobileIron	**All derived credential providers** When you add each AppConnect app that uses derived credentials

TABLE 6. DERIVED CREDENTIALS CONFIGURATION TASKS ON MOBILEIRON CLOUD (CONT.)

Task	Notes
Cloud. These AppConnect apps can include Web@Work, Docs@Work, Email +, and in-house AppConnect apps. **Related topics** Adding Web@Work for iOS to the App Catalog Adding Web@Work for Android to the App Catalog Adding Docs@Work for iOS to the App Catalog Adding Docs@Work for Android to the App Catalog Setting up Email+ to use derived credentials Adding in-house iOS AppConnect apps to the App Catalog Adding Android AppConnect apps to the App Catalog	to the App Catalog, you specify in its AppConnect Certificate Configuration which derived credential identity certificate to use.

Device user tasks to use derived credentials

After you have configured MobileIron Cloud to support the use of derived credentials, the tasks that a device user does to use derived credentials depends on:

- whether the device is Android or iOS
- whether the derived credential provider is Entrust, DISA Purebred, or another provider

The tasks are listed in:

- Device user tasks to use Entrust derived credentials
- Device user tasks to use DISA Purebred derived credentials
- Device user tasks to use another provider’s derived credentials

NOTE: These task lists assume that you want device users to register to MobileIron Cloud using a registration PIN rather than with a user ID and password, since typically, device users who use smart cards do not have passwords. However, using a registration PIN is a requirement only with Entrust derived credentials. For other derived credential providers, it is not a requirement, and therefore the related tasks are optional.

Device user tasks to use Entrust derived credentials

Device users who have not yet registered with MobileIron Cloud can get Entrust derived credentials by doing the following:

1. Authenticate to the MobileIron Cloud Self-Service Portal with a smart card.
2. Generate a one-time registration PIN.
3. Request a derived credential from Entrust, which generates a one-time Entrust activation password.
4. Install MobileIron Go on the device. For Android, this includes installing the Secure Apps Manager.
5. Register MobileIron Go with MobileIron Cloud using the one-time registration PIN.
6. For Android devices, install the PIV-D Manager app, and any AppConnect apps on the device.
7. For iOS devices, install the Install the PIV-D Manager app and any AppConnect apps on the device.
8. For iOS devices, launch the PIV-D Manager app and select the Entrust option to activate the derived credential with the one-time Entrust activation password.
9. For Android devices, launch the PIV-D Manager app to activate the derived credential with the one-time activation password.
10. Use the AppConnect apps.

Device users who are already registered with MobileIron Cloud can get derived credentials by doing the following:

1. Get a QR code and Entrust activation password from the Entrust self-service portal.
2. Get a derived credential using the PIV-D Manager app for iOS or the PIV-D Manager app for Android.

The following diagrams summarize what happens when:

- A device user requests a registration PIN and Entrust derived Credential
- An iOS user activates an Entrust derived Credential
- An Android AppConnect user activates an Entrust derived Credential

FIGURE 2. A DEVICE USER REQUESTS A REGISTRATION PIN AND ENTRUST DERIVED CREDENTIAL

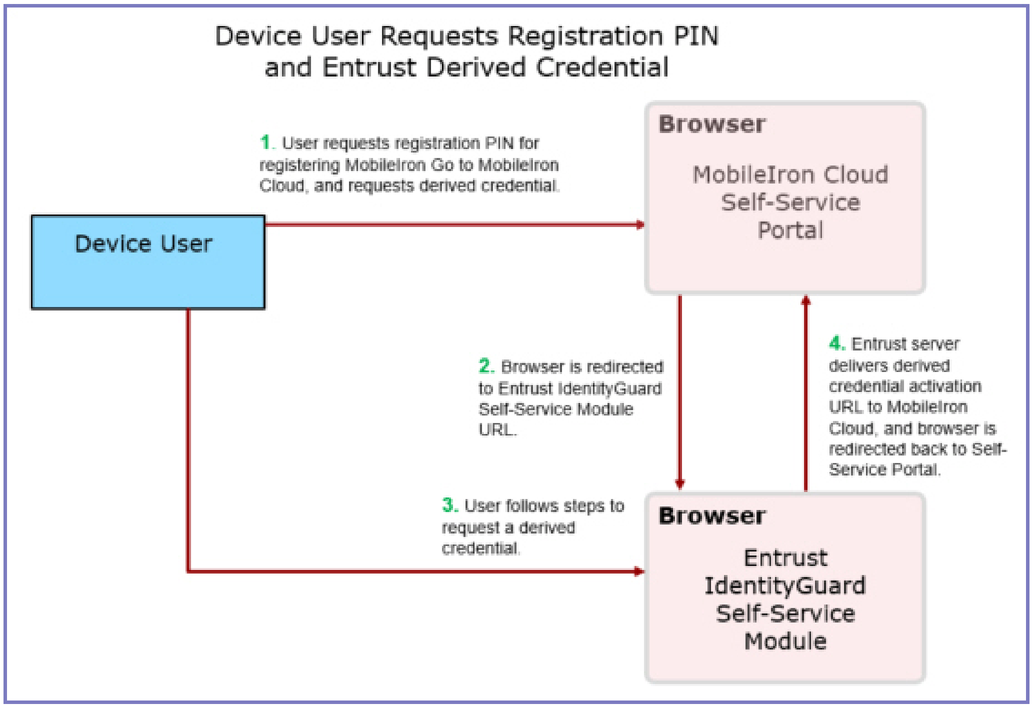

Device User Requests Registration PIN
and Entrust Derived Credential
Browser
MobileIron Cloud Self-Service Portal
1. User requests registration PIN for registering MobileIron Go to MobileIron Cloud, and requests derived credential.
Device User
2. Browser is redirected to Entrust IdentityGuard Self-Service Module URL.
4. Entrust server delivers derived credential activation URL to MobileIron Cloud, and browser is redirected back to Self-Service Portal.
3. User follows steps to request a derived credential.
Browser
Entrust IdentityGuard Self-Service Module

FIGURE 3. AN IOS USER ACTIVATES AN ENTRUST DERIVED CREDENTIAL

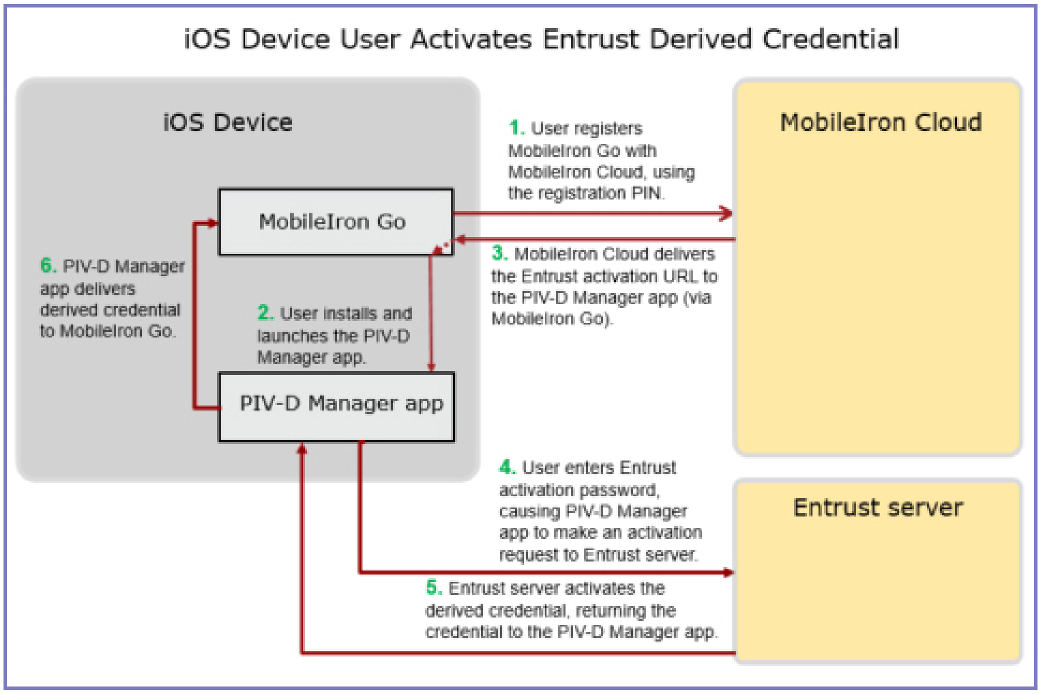
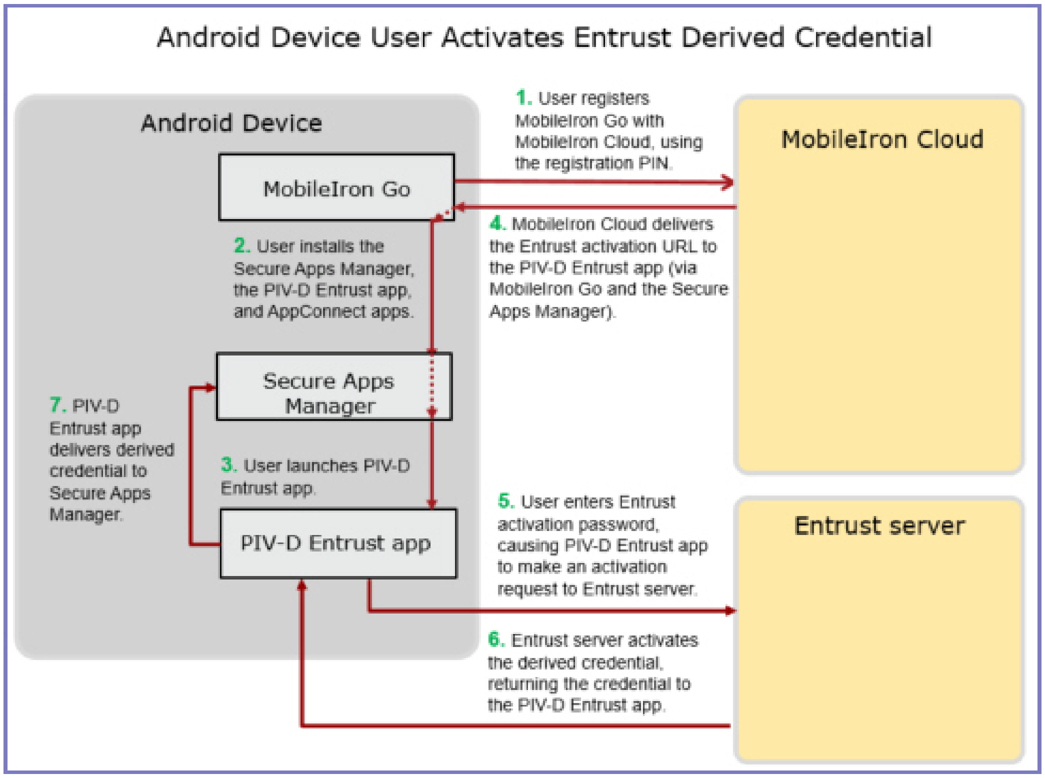

iOS Device User Activates Entrust Derived Credential
iOS Device
MobileIron Go
1. User registers MobileIron Go with MobileIron Cloud, using the registration PIN.
MobileIron Cloud
3. MobileIron Cloud delivers the Entrust activation URL to the PIV-D Manager app (via MobileIron Go).
6. PIV-D Manager app delivers derived credential to MobileIron Go.
2. User installs and launches the PIV-D Manager app.
PIV-D Manager app
4. User enters Entrust activation password, causing PIV-D Manager app to make an activation request to Entrust server.
Entrust server
5. Entrust server activates the derived credential, returning the credential to the PIV-D Manager app.

FIGURE 4. AN ANDROID APPCONNECT USER ACTIVATES AN ENTRUST DERIVED CREDENTIAL


Android Device User Activates Entrust Derived Credential
Android Device
MobileIron Go
Secure Apps Manager
PIV-D Entrust app
MobileIron Cloud
Entrust server
1. User registers MobileIron Go with MobileIron Cloud, using the registration PIN.
2. User installs the Secure Apps Manager, the PIV-D Entrust app, and AppConnect apps.
3. User launches PIV-D Entrust app.
4. MobileIron Cloud delivers the Entrust activation URL to the PIV-D Entrust app (via MobileIron Go and the Secure Apps Manager).
5. User enters Entrust activation password, causing PIV-D Entrust app to make an activation request to Entrust server.
6. Entrust server activates the derived credential, returning the credential to the PIV-D Entrust app.
7. PIV-D Entrust app delivers derived credential to Secure Apps Manager.

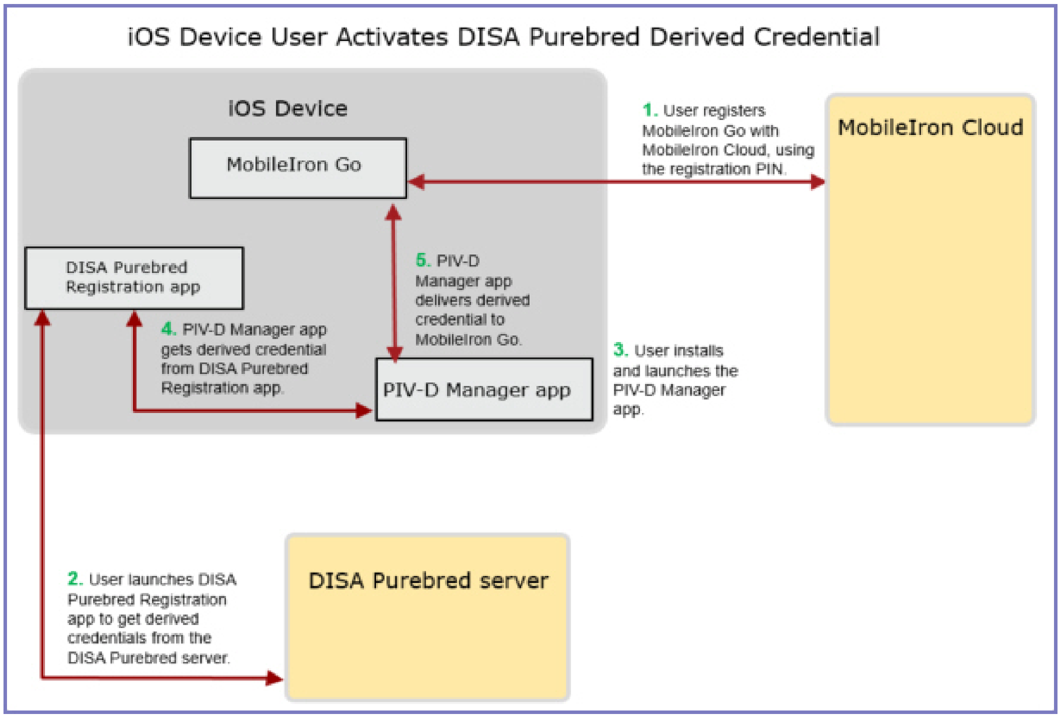
Device user tasks to use DISA Purebred derived credentials

Using DISA Purebred derived credentials is supported only on iOS devices.

1. Authenticate to the MobileIron Cloud self-service user portal with a smart card.
2. Generate a one-time registration PIN.
3. Install MobileIron Go on the device.
4. Register MobileIron Go with MobileIron Go using the one-time registration PIN.
5. Install the DISA Purebred Registration app on the device.
6. Install the PIV-D Manager app for iOS on the device.
7. Launch the DISA Purebred Registration app to get the derived credential
8. Launch the PIV-D Manager app and select the DISA Purebred option to import the derived credential's certificates from the DISA Purebred Registration app. The PIV-D Manager app then sends all the certificates to MobileIron Go.
9. Install the AppConnect apps on the device.
10. Use the AppConnect apps.

The following diagram displays the what happens when the device user gets a DISA Purebred derived credential.

FIGURE 5. AN IOS USER ACTIVATES A DISA PUREBRED DERIVED CREDENTIAL


iOS Device User Activates DISA Purebred Derived Credential
iOS Device
MobileIron Go
DISA Purebred Registration app
PIV-D Manager app
MobileIron Cloud
DISA Purebred server
1. User registers MobileIron Go with MobileIron Cloud, using the registration PIN.
2. User launches DISA Purebred Registration app to get derived credentials from the DISA Purebred server.
3. User installs and launches the PIV-D Manager app.
4. PIV-D Manager app gets derived credential from DISA Purebred Registration app.
5. PIV-D Manager app delivers derived credential to MobileIron Go.

Device user tasks to use another provider's derived credentials

Third-party derived credential apps are supported on iOS devices.

1. Authenticate to the MobileIron Cloud self-service user portal with a smart card.
2. Generate a one-time registration PIN.
3. Install MobileIron Go on the device.
4. Register MobileIron Go with MobileIron Cloud using the one-time registration PIN.
5. For Android devices, install the Secure Apps Manager for Android on the device, followed by any AppConnect apps.
6. For iOS devices, install the third-party derived credential app for iOS and any AppConnect apps on the device.
7. Launch the derived credential app and follow its instructions.
8. Use the AppConnect apps.

Related topics

Mobile device requirements for using derived credentials

Configuring MobileIron Cloud for derived credentials

Tasks before configuring MobileIron Cloud

Before configuring MobileIron Cloud for derived credentials, the following tasks are necessary depending on your derived credential provider, device platform, and use of derived credentials:

TABLE 7. CONFIGURATION TASKS OUTSIDE OF MOBILEIRON CLOUD

Task	Derived credential providers	Device platforms
Setting up your Entrust self-service portal	Entrust	iOS, Android
Setting up Microsoft Exchange for certificate authentication	Any	iOS, Android
Installing the DISA Purebred Registration app on devices	DISA Purebred	iOS

Setting up your Entrust self-service portal

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Entrust
Device platforms	iOS, Android

Set up an Entrust self-service portal for your device users, and provide a URL for each of the following:

- the Entrust IdentityGuard Self-Service Module (SSM) URL
  You configure MobileIron Cloud with this URL. The URL is used when a device user generates the one-time MobileIron registration PIN and requests a derived credential on the MobileIron Cloud Self-Service Portal. The request causes the MobileIron Cloud Self-Service Portal to redirect the browser to this URL.
  Work with Entrust to ensure that the Entrust IdentityGuard SSM is set up to pass the activation link and its expiration time to MobileIron Cloud. Also, make sure the Entrust IdentityGuard SSM has callback enabled so it can redirect the browser back to MobileIron Cloud.
- the Entrust URL for getting a QR (Quick Response) code and Entrust activation password.
  Inform device users of this URL.

Depending on your Entrust setup, these URLs could be the same.

Work with Entrust to ensure that the Entrust IdentityGuard server is set up to pass the activation link and its expiration time to MobileIron Cloud. Also, make sure the server is enabled to callback (redirect back to) MobileIron Cloud after

Setting up Microsoft Exchange for certificate authentication

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any
Device platforms	iOS, Android

If you are setting up Email+ for iOS or Email+ for Android so that device users authenticate to Microsoft Exchange with derived credentials, you must set up Microsoft Exchange to accept certificate authentication.

See Configuring Certificate-Based Authentication for Microsoft Exchange.

Installing the DISA Purebred Registration app on devices

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	DISA Purebred
Device platforms	iOS

If you use DISA Purebred derived credentials, make sure the iOS devices have the DISA Purebred Registration app installed. Device users use the DISA Purebred Registration app to get the Purebred derived credential. The app passes the credential’s certificates to the PIV-D Manager app, which in turn passes them to MobileIron Go for iOS.

Configuration tasks on MobileIron Cloud

The following table shows the tasks for configuring MobileIron Cloud for derived credentials. For each task, the table shows for which derived credential providers and device platforms the task is applicable. For example, if you are configuring MobileIron Cloud to support only DISA Purebred derived credentials, skip the tasks that are only applicable to Entrust derived credentials.

TABLE 8. MOBILEIRON CLOUD CONFIGURATION TASKS BY DERIVED CREDENTIAL PROVIDER AND DEVICE PLATFORM

Task	Derived credential providers	Device platforms
Configuring certificate authentication to the MobileIron Cloud Self-Service Portal	Required for Entrust, typical for all others	iOS, Android
Configuring the Entrust IdentityGuard SSM Module URL	Entrust	iOS, Android
Configuring PIN-based registration	Required for Entrust, typical for all others	iOS, Android
Configuring an identity certificate for derived credentials	Any	iOS, Android
Configuring the App Catalog web clip for iOS	Any	iOS
Configuring AppConnect for iOS	Any	iOS
Configuring AppConnect for Android	Entrust	Android
Adding the PIV-D Manager app for iOS to the App Catalog	Entrust, DISA Purebred	iOS
Configuring the PIV-D Manager app for iOS for analytics	Entrust, DISA Purebred	iOS
Configuring the PIV-D Manager app for iOS for feedback	Entrust, DISA Purebred	iOS
Adding a third-party iOS derived credential app to the App Catalog	Any other than Entrust or DISA Purebred	iOS
Adding the PIV-D Manager app for Android to the App Catalog	Entrust	Android
Adding Web@Work for iOS to the App Catalog	Any	iOS
Adding Web@Work for Android to the App Catalog	Any	Android
Adding Docs@Work for iOS to the App Catalog	Any	iOS
Adding Docs@Work for Android to the App Catalog	Any	Android
Setting up Email+ to use derived credentials	Any	iOS, Android
Adding in-house iOS AppConnect apps to the App Catalog	Any	iOS
AppConnect custom configuration key-value pairs for in-house iOS AppConnect apps	Any	iOS
Adding Android AppConnect apps to the App Catalog	Any	Android

Related topics

- *The MobileIron Cloud Administrator Guide*
- *MobileIron Web@Work for iOS Guide for Administrators*
- *MobileIron Web@Work for Android Guide for Administrators*
- *MobileIron Docs@Work for iOS Guide for Administrators*
- *MobileIron Docs@Work for Android Guide for Administrators*
- *MobileIron Email+ for iOS Guide for Administrators*
- *MobileIron Email+ for Android Guide for Administrators*
- *AppConnect Secure Apps for Android Release Notes and Upgrade Guide*

Configuring certificate authentication to the MobileIron Cloud Self-Service Portal

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Required for Entrust, typical for all others
Device platforms	iOS, Android

Device users use the MobileIron Cloud Self-Service Portal to get a one-time registration PIN (and for Entrust, to request an Entrust derived credential.) The device users authenticate to the MobileIron Cloud Self-Service Portal with the identity certificate on their smart cards.

Before you begin

- To allow device users to authenticate to the MobileIron Cloud Self-Service Portal with the identity certificate on their smart cards, you need a PEM-formatted file that you upload to MobileIron Cloud. The file contains either a valid issuing (CA) certificate or a valid supporting certificate chain. When a user signs in to the MobileIron Cloud Self-Service Portal, they provide an identity certificate from a smart card. The user identity in the identity certificate must contain the User Principal Name (UPN) in the Subject Alternative Name (SAN).The MobileIron Cloud Self-Service Portal validates the identity certificate against the certificate that you upload to MobileIron Cloud.

IMPORTANT: The certificate that you upload to MobileIron Cloud is not immediately available for device users to authenticate against. It is only available for authentication after the next MobileIron Cloud upgrade. Contact MobileIron Technical Support to ask MobileIron to make your certificate available for use after the next upgrade.

- This procedure creates a Self Service Portal Authentication Setting that you apply to the appropriate user groups. Therefore, create the appropriate user groups at **Users > User Groups > +Add**.

If you want to apply the setting to all users, you can edit the default Self Service Portal Authentication Setting.

Procedure

1. In the Admin Portal, select **Users > User Settings**.
2. Under **Self Service Portal Authentication Setting,** select **+Add setting for specific user groups**.
3. Enter a name for the setting.
4. For **Self Service Portal Authentication Type**, select **Certificate.**

5. Click **Choose File.**
6. Select the PEM-formatted file that contains either the issuing CA certificate or the supporting certificate chain.
7. Click **Next.**

if you are editing the default Self Service Portal Authentication Setting, click **Done**.

8. Select the appropriate user groups for the setting.
9. Click **Done**.

Configuring the Entrust IdentityGuard SSM Module URL

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Entrust
Device platforms	iOS, Android

To use Entrust derived credentials, you configure MobileIron Cloud with the Entrust Identity Guard SSM Module URL.

1. In the Admin Portal, select **Users > User Settings**.
2. Under **Self Service Portal Authentication Setting,** click the edit icon next to the setting you created in Configuring certificate authentication to the MobileIron Cloud Self-Service Portal.
3. Turn on the **Derived Mobile Smart Credential** option.
   The field **Entrust IdentityGuard Self Service Module URL** appears.
4. Enter the Entrust IdentityGuard Self Service Module URL.
   The MobileIron Cloud Self-Service Portal directs the user to this URL when the user requests a derived credential.
   Example: https://yourEntrustSSM.yourcorp.com:8448/SelfService
5. Click **Next.**
6. Click **Done**.

Configuring PIN-based registration

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Required for Entrust, typical for all others
Device platforms	iOS, Android

This task is necessary to allow your users to register MobileIron Go to MobileIron Cloud with a PIN.

Before you begin

This procedure creates a Device Registration Setting that you apply to the appropriate user groups that require PIN-based registration. Therefore create the appropriate user groups at **Users > User Groups > +Add**.

NOTE: If you want to apply PIN-based registration to all users, you can edit the default Device Registration Setting.

Procedure

1. In the Admin Portal, select **Users > User Settings**.
2. Under **Device Registration Setting,** select **+Add setting for specific user groups**.
3. Enter a name for the setting.
4. If your enterprise requires a minimum iOS version, turn on **Enable Minimum Version** for iOS devices in the section **OS Minimum Version Blocking**, and select the minimum iOS version.
5. In **Device Registration Authentication Type**, select **PIN Only.**
6. Change the **PIN length** and **PIN lifetime** according to your requirements.
7. Enable **Allow user to request a new PIN.**

An Entrust derived credential is associated with a registration PIN. Because an Entrust derived credential expires after a short time, make sure the device user can request a new registration PIN.

8. Click **Next.**

if you are editing the default Device Registration Setting, click **Done**.

9. Select the appropriate user groups for the setting.
10. Click **Done.**

Configuring an identity certificate for derived credentials

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any
Device platforms	iOS, Android

An identity certificate configuration is necessary for each of the purposes an app uses derived credentials. These purposes are authentication, signing, and encryption. For each app using derived credentials, the app’s AppConnect custom configuration refers to this identity certificate configuration.

Procedure

1. In the Admin Portal, select **Configurations.**
2. Click **+Add**.
3. Click **Identity Certificate**.
4. Enter a name for the identity certificate configuration**.**
5. In the **Configuration Setup** section, in the **Certificate Distribution** field, select **Derived Credential**.

6. In **Derived Credential Usage**, select the purpose for the derived credential from the drop-down choices: **Authentication**, **Encryption**, or **Signing**.
7. Click **Next**.

In the screen displayed, the Identity Certificate Configuration is applied to no devices, and you cannot change that option. The reason is that an AppConnect app's custom configuration will refer to this Identity Certificate Configuration. When the app is applied to a device, this configuration is also applied to the device.

8. Select **Allow this configuration to be available in all spaces** if you want this setting to be available in all spaces rather than only the Default Space.
9. Click **Done**.

Repeat these steps for each of the derived credential purposes your device users require.

Configuring the App Catalog web clip for iOS

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any
Device platforms	iOS

Registered devices receive the App Catalog web clip from MobileIron Cloud. The App Catalog web clip allows the device user to view the iOS apps that are in the App Catalog, and install them. You configure which device users receive the App Catalog web clip in the Apple App Catalog configuration. Make sure all devices that will use derived credentials receive the App Catalog web clip.

Procedure

1. In the Admin Portal, go to **Configurations**.
2. Click **Apple App Catalog**.
3. Click the Edit Distribution icon.
4. Select one of the following distribution options:
   - **All Devices** - all compatible devices will have this configuration sent to them.
   - **Custom** - define specific device groups that will have this configuration sent to them.
5. Click **Save**.

Configuring AppConnect for iOS

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any
Device platforms	iOS

Configuring AppConnect for iOS is required for device users to use:

- any derived credential app for iOS including the PIV-D Manager app
- AppConnect apps that use derived credentials

To use AppConnect apps on an iOS device, the device must have an AppConnect Device Configuration or the default iOS AppConnect Configuration. This procedure assumes you create an AppConnect Device Configuration.

Procedure

1. In the Admin Portal, go to **Configurations > +Add**.
2. Select **AppConnect Device**.
3. For **Name**, enter a name for the new AppConnect Device Configuration.
4. For **OS**, select **iOS**.
5. In the **AppConnect Passcode** section, turn on the **Secure Apps Passcode** option.
6. In the **AppConnect Passcode** section, configure the following passcode settings according to your organization’s requirements. For example, make the passcode requirements NIST SP 800-157 compliant as described in http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf.
   - **4-digit numeric or alphanumeric**
   - **Minimum passcode length** (for alphanumeric passcodes)
   - **Minimum number of complex characters** (for alphanumeric passcodes)
7. Fill in the remaining fields in the AppConnect Device Configuration according to your requirements.
8. Click **Next**.
9. Select the devices or device groups that you want to distribute the AppConnect Device Configuration to.
10. Click **Done**.

Configuring AppConnect for Android

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Entrust
Device platforms	Android

Configuring AppConnect is required for Android device users to use:

- the PIV-D Manager app for Android AppConnect
- AppConnect apps that use derived credentials

To use AppConnect apps on an Android device, the device must have an AppConnect Device Configuration or the default Android AppConnect Configuration. This procedure assumes you create an AppConnect Device Configuration.

NOTE: The AppConnect device configuration includes Data Loss Prevention (DLP) settings which you set according to your organization’s security requirements. One of the Android DLP settings allows or disables camera access for taking pictures or video. The PIV-D Manager app for Android uses the camera **only** for scanning the QR code, **not** for taking pictures or video. Therefore, you can still use the Android camera DLP setting to disable camera use in AppConnect apps.

Procedure

1. In the Admin Portal, go to **Configurations > +Add**.
2. Select **AppConnect Device**.
3. For **Name**, enter a name for the new AppConnect Device Configuration.
4. For **OS**, select **Android**.
5. In the **AppConnect Passcode** section, turn on the **Secure Apps Passcode** option.
6. In the **AppConnect Passcode** section, configure the following passcode settings according to your organization's requirements. For example, make the passcode requirements NIST SP 800-157 compliant as described in http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf.
   - **4-digit numeric or alphanumeric**
   - **Minimum passcode length** (for alphanumeric passcodes)
   - **Minimum number of complex characters** (for alphanumeric passcodes)
7. In the **AppConnect Passcode** section, turn on **Allow user to recover passcode.**
8. Fill in the remaining fields in the AppConnect Device Configuration according to your requirements.
9. Click **Next**.
10. Select the devices or device groups that you want to distribute the AppConnect Device Configuration to.
11. Click **Done**.

Adding the PIV-D Manager app for iOS to the App Catalog

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Entrust, DISA Purebred
Device platforms	iOS

Device users use the PIV-D Manager app for iOS to use derived credentials on iOS devices. You add the app to the App Catalog, configuring it to have a AppConnect custom configuration. The key-value pairs you configure in the AppConnect custom configuration depend on the derived credential provider.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Click **+Add**.
3. Select **iOS Store** to search the Apple App Store.
4. Enter **MobileIron PIV-D Manager** in the search field.
5. Select the MobileIron PIV-D Manager app that displays.
6. **Click Next.**
7. **Click Next.**
8. **Click Next.**
9. Select the users and user groups that you want to distribute the app to.
10. **Click Next.**
11. Scroll down to **AppConnect Custom Configuration**.
12. Select **+** to add a new AppConnect custom configuration.

13. Enter a name for the AppConnect custom configuration.
14. In the **AppConnect Custom Configuration section**, add the **case-sensitive** key-value pairs, depending on the derived credential provider:

TABLE 9. KEY-VALUE PAIRS FOR PIV-D MANAGER WHEN USING ENTRUST

Key	Value	Description
Required key and value MI_CREDENTIAL_ACTIVATION_URL	${pivdActivationLink}	Entrust provides the activation URL to MobileIron Cloud when the user requests a derived credential on the MobileIron Cloud Self-Service Portal. The PIV-D Manager app receives the value when the user launches the app on the device.
Optional key and value MI_CREDENTIAL_DEVICE_ID	A MobileIron Cloud substitution variable that uniquely identifies the device. Examples: ${deviceClientDeviceIdentifier} ${deviceUDID} ${deviceIMSI}	This key-value pair contains a unique device identifier that the PIV-D Manager app sends to the Entrust IdentityGuard server. This identifier allows an administrator to determine which device contains a given derived credential, allowing control around auditing and revocation.

TABLE 10. KEY-VALUE PAIRS FOR PIV-D MANAGER WHEN USING DISA PUREBREAD

Key	Value	Description
MI_CREDENTIAL_ENABLE_PUREBRED	True	Enables the PIV-D Manager app to support DISA Purebred derived credentials

15. Select the users and user groups that you want to distribute the AppConnect custom configuration to.
16. Click **Next**.
17. Click **Done**.

Configuring the PIV-D Manager app for iOS for analytics

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Entrust, DISA Purebred
Device platforms	iOS

By default, the PIV-D Manager app for iOS reports app analytics to MobileIron. The collected data includes information such as the device model, the iOS version, the city, and app events such as succeeded and failed derived credential activations.

IMPORTANT: The collected data does not include any personal information.

You can turn off analytics reporting on the PIV-D Manager app by adding a key-value pair with the key name **disable_analytics**.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Click on the name of the MobileIron PIV-D Manager app for iOS.
3. Click **App Configurations**.
4. Click **AppConnect Custom Configuration**.
5. Click the name of the AppConnect custom configuration that you want to edit.
6. Click **Edit**.
7. In the **AppConnect Custom Configuration** section, add the **case-sensitive** key-value pair:

Key	Value
disable_analytics	True

8. Click **Update**.

Configuring the PIV-D Manager app for iOS for feedback

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Entrust, DISA Purebred
Device platforms	iOS

You can configure the PIV-D Manager app for iOS to provide a feedback button on its About screen. The device user taps this button to send an email with feedback about the app. The email is addressed to an email address that you configure.

By default, the iOS native email app is used to create and send the email. However, you can configure the PIV-D Manager app to launch Email+ for iOS instead.

To configure the feedback button, you add key-value pairs to the app’s AppConnect custom configuration.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.

2. Click on the name of the MobileIron PIV-D Manager app for iOS.
3. Click **App Configurations**.
4. Click **AppConnect Custom Configuration**.
5. Click the name of the AppConnect custom configuration that you want to edit.
6. Click **Edit**.
7. In the **AppConnect Custom Configuration** section, add the **case-sensitive** key-value pair:

Key	Value	Description
`feedback_email_address`	Email address to send feedback to.	A value for this key causes the PIV-D Manager app to display the feedback button on the About screen. The device user taps the button to send an email. The specified email address displays in the **To** field.
`use_emailplus_application_for_feedback`	**Yes** or **No**	Default value: **No** The value **No** means that the iOS Native email app is used for sending feedback. The value **Yes** causes the PIV-D Manager app to prompt the device user to choose an app for sending feedback. The device user must choose Email+. Any other choice results in an error message.

8. Click **Update**.

Adding a third-party iOS derived credential app to the App Catalog

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any other than Entrust or DISA Purebred
Device platforms	iOS

A device user uses a derived credential app to obtain derived credentials on an iOS device after registering a device to MobileIron Cloud. A derived credential app can require an AppConnect custom configuration, which contains key-value pairs for the app. The app vendor or developer describes these key-value pairs, if any, in the app's documentation.

When you configure an AppConnect custom configuration, the derived credential app receives the key-value pairs when the user launches the app on the device.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Click **+Add**.
3. Select **iOS Store** to search the Apple App Store.
4. Enter the name of the derived credential app in the search field.
5. Select the app when it displays.
6. **Click Next.**
7. **Click Next.**
8. **Click Next.**
9. Select the users and user groups that you want to distribute the app to.
10. **Click Next.**
11. Scroll down to **AppConnect Custom Configuration**.
12. Select **+** to add a new AppConnect custom configuration.
13. Enter a name for the AppConnect custom configuration.
14. In the **AppConnect Custom Configuration section**, add the **case-sensitive** key-value pairs as directed by the app's vendor.
15. Select the users and user groups that you want to distribute the AppConnect custom configuration to.
16. Click **Next**.
17. Click **Done**.

Adding the PIV-D Manager app for Android to the App Catalog

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Entrust
Device platforms	Android

Device users use the PIV-D Manager for Android app to activate derived credentials on Android devices.

Procedure

1. Go to http://support.mobileiron.com/mi/android-entrust/current.
   Alternatively, go to https://help.mobileiron.com and select the Software tab.

Accessing these sites requires MobileIron credentials.

2. Download the PIV-D Manager app for Android APK file.
1. In the Admin Portal, go to **Apps > App Catalog**.
2. Click **+Add**.
3. Select **In-House** to upload the app.
4. Drag and drop the PIV-D Manager app for Android APK file to the designated area.
5. Click **Next**.
6. In **Category**, enter a category.
7. Click **Next**.
8. Click **Next**.
9. Click **Next**.

10. Select the users and user groups that you want to distribute the app to.
11. **Click Next.**
12. **Next to AppConnect Custom Configuration, click the + sign.**
13. Enter a name for the configuration.
14. n the **AppConnect Custom Configuration** section, add the **case-sensitive** key-value pairs:

Key	Value	Description
Required key and value MI_CREDENTIAL_ACTIVATION_URL	${pivdActivationLink}	Entrust provides the activation URL to MobileIron Cloud when the user requests a derived credential on the MobileIron Cloud Self-Service Portal. The PIV-D Manager app receives the value when the user launches the app on the device.
Optional key and value MI_CREDENTIAL_DEVICE_ID	A MobileIron Cloud substitution variable that uniquely identifies the device. Examples: ${deviceClientDeviceIdentifier} ${deviceUDID} ${deviceIMSI}	This key-value pair contains a unique device identifier that the PIV-D Manager app sends to the Entrust IdentityGuard server. This identifier allows an administrator to determine which device contains a given derived credential, allowing control around auditing and revocation.

15. Click **Next**.
16. Click **Done**.

Adding Web@Work for iOS to the App Catalog

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any
Device platforms	iOS

Web@Work can use derived credentials to authenticate the device user to internal websites.

The steps for configuring derived credentials use in Web@Work are:

1. Requiring a device password for iOS devices
2. Adding Web@Work for iOS to the App Catalog

Requiring a device password for iOS devices

A device password enables iOS data protection, which is necessary for Web@Work for iOS to encrypt browser data.

Procedure

1. In the Admin Portal, go to **Configurations > +Add**.
2. Select **Passcode**.

Alternatively, edit an existing Passcode Configuration.

3. For **Name**, enter a name for the new Passcode Configuration.
4. Fill in each field according to your security requirements.
5. Click **Next**.
6. Select the devices or device groups that you want to distribute the Passcode Configuration to.
7. Click **Done**.

Adding Web@Work for iOS to the App Catalog

Add Web@Work for iOS to the App Catalog and define its key-value pairs for using derived credentials.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Click **+Add**.
3. In the **Business Apps** section, select **Web@Work for iOS**.
4. Click **Next**.
5. Click **Next**.
6. Select the users and user groups that you want to distribute the app to.
7. Click **Next**.
8. Scroll down to **Web@Work Configuration**.
9. Select **+** to add a new Web@Work configuration.
10. Enter a name for the Web@Work configuration.
11. In the **AppConnect Custom Configuration** section, add the **case-sensitive** key-value pairs:

Key	Value
IdCertificate_1_host	The URL for the website to which the certificate from the derived credential will be presented. Wildcards are permitted. For example: • myhost.mycompany.com • *.mycompany.com/myfolder

Repeat with similar keys with different numbers for other URLs. For example:

Key	Value
IdCertificate_2_host	AnotherHost.mycompany.com
IdCertificate_3_host	YetAnotherHost.mycompany.com

12. In the **AppConnect Certificate Configuration** section, add the **case-sensitive** key-value pairs:

Key	Value
IdCertificate_1	Select an identity certificate configuration for derived credentials from the drop-down list. The identity certificate configuration must have the purpose **Authentication**. Web@Work will use this certificate to identify to the website specified in idCertificate_1_host.

Repeat with similar keys with different numbers for other URLs. For example:

Key	Value
IdCertificate_2	Web@Work will use this certificate to identify to the website specified in idCertificate_2_host.
IdCertificate_3	Web@Work will use this certificate to identify to the website specified in idCertificate_2_host.

13. Add any other key-value pairs that you require for Web@Work.
14. Select the users and user groups that you want to distribute the AppConnect custom configuration to.
15. Click **Next**.
16. Click **Done**.

Related topics

- *MobileIron Web@Work for iOS Guide for Administrators*

Adding Web@Work for Android to the App Catalog

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Entrust
Device platforms	Android AppConnect

Web@Work can use derived credentials to authenticate the device user to internal websites.

Procedure

1. Go to https://help.mobileiron.com and select the Software tab.
2. Download the Web@Work for Android APK file.
1. In the Admin Portal, go to **Apps > App Catalog**.
2. Click **+Add**.
3. Select **In-House** to upload the app.
4. Drag and drop the Web@Work for Android APK file to the designated area.
5. Click **Next**.
6. In **Category**, enter a category.
7. Click **Next**.
8. Click **Next**.
9. Click **Next**.
10. Select the users and user groups that you want to distribute the app to.
11. **Click Next.**
12. **Next to Web@Work Configuration, click the + sign.**
13. Enter a name for the Web@Work configuration.
14. In the **AppConnect Custom Configuration** section, add the **case-sensitive** key-value pairs:

Key	Value
IdCertificate_1_host	The URL for the website to which the certificate from the derived credential will be presented. Wildcards are permitted. For example: • myhost.mycompany.com • *.mycompany.com/myfolder

Repeat with similar keys with different numbers for other URLs. For example:

Key	Value
IdCertificate_2_host	AnotherHost.mycompany.com
IdCertificate_3_host	YetAnotherHost.mycompany.com

15. In the **AppConnect Certificate Configuration** section, add the **case-sensitive** key-value pairs:

Key	Value
IdCertificate_1	Select an identity certificate configuration for derived credentials from the drop-down list. The identity certificate configuration must have the purpose **Authentication**. Web@Work will use this certificate to identify to the website specified in idCertificate_1_host.

Repeat with similar keys with different numbers for other URLs. For example:

Key	Value
IdCertificate_2	Web@Work will use this certificate to identify to the website specified in idCertificate_2_host.
IdCertificate_3	Web@Work will use this certificate to identify to the website specified in idCertificate_2_host.

16. Add any other key-value pairs that you require for Web@Work.
17. Select the users and user groups that you want to distribute the AppConnect custom configuration to.
18. Click **Next**.
19. Click **Done**.

Related topics

- *MobileIron Web@Work for Android Guide for Administrators*

Adding Docs@Work for iOS to the App Catalog

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any
Device platforms	iOS

If you are using Docs@Work for iOS with derived credentials, add Docs@Work to the App Catalog on MobileIron Cloud. Docs@Work for iOS can use derived credentials to authenticate the device user to internal websites such as SharePoint sites.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Click **+Add**.
3. In the **Business Apps** section, select **Docs@Work for iOS**.
4. Click **Next**.
5. Click **Next**.
6. Select the users and user groups that you want to distribute the app to.
7. Click **Next**.
8. Scroll down to **Docs@Work Configuration**.
9. Select **+** to add a new Docs@Work configuration.
10. Enter a name for the Docs@Work configuration.
11. In the **AppConnect Custom Configuration** section, add this **case-sensitive** key-value pair:

Key	Value
IdCertificate_1_host	The URL for the website to which the certificate from the derived credential will be presented. Wildcards are permitted. For example: • myhost.mycompany.com • *.mycompany.com/myfolder

Repeat with similar keys with different numbers for other URLs. For example:

Key	Value
IdCertificate_2_host	AnotherHost.mycompany.com
IdCertificate_3_host	YetAnotherHost.mycompany.com

12. In the **AppConnect Certificate Configuration** section, add this **case-sensitive** key-value pair:

Key	Value
IdCertificate_1	Select an identity certificate configuration for derived credentials from the drop-down list. The identity certificate configuration must have the purpose **Authentication**. Docs@Work will use this certificate to identify to the website specified in idCertificate_1_host.

Repeat with similar keys with different numbers to correspond to other URLs. For example:

Key	Value
IdCertificate_2	Docs@Work will use this certificate to identify to the website specified in idCertificate_2_host.
IdCertificate_3	Docs@Work will use this certificate to identify to the website specified in idCertificate_3_host.

13. Add any other key-value pairs that you require for Docs@Work.
14. Select the users and user groups that you want to distribute the AppConnect custom configuration to.
15. Click **Next**.
16. Click **Done**.

Related topics

- *MobileIron Docs@Work for iOS Guide for Administrators*

Adding Docs@Work for Android to the App Catalog

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Entrust
Device platforms	Android AppConnect

Docs@Work can use derived credentials to authenticate the device user to internal websites.

Procedure

1. Go to https://help.mobileiron.com and select the Software tab.
2. Download the Docs@Work for Android APK file.
3. In the Admin Portal, go to **Apps > App Catalog**.
4. Click **+Add**.
5. Select **In-House** to upload the app.
6. Drag and drop the Docs@Work for Android APK file to the designated area.
7. Click **Next**.
8. In **Category**, enter a category.
9. Click **Next**.
10. Click **Next**.
11. Click **Next**.
12. Select the users and user groups that you want to distribute the app to.
13. **Click Next.**
14. **Next to Docs@Work Configuration, click the + sign.**
15. Enter a name for the Docs@Work configuration.
16. In the **AppConnect Custom Configuration** section, add the **case-sensitive** key-value pairs:

Key	Value
IdCertificate_1_host	The URL for the website to which the certificate from the derived credential will be presented. Wildcards are permitted. For example: • myhost.mycompany.com • *.mycompany.com/myfolder

Repeat with similar keys with different numbers for other URLs. For example:

Key	Value
IdCertificate_2_host	AnotherHost.mycompany.com
IdCertificate_3_host	YetAnotherHost.mycompany.com

17. In the **AppConnect Certificate Configuration** section, add the **case-sensitive** key-value pairs:

Key	Value
IdCertificate_1	Select an identity certificate configuration for derived credentials from the drop-down list. The identity certificate configuration must have the purpose **Authentication**. Docs@Work will use this certificate to identify to the website specified in idCertificate_1_host.

Repeat with similar keys with different numbers for other URLs. For example:

Key	Value
IdCertificate_2	Docs@Work will use this certificate to identify to the website specified in idCertificate_2_host.
IdCertificate_3	Docs@Work will use this certificate to identify to the website specified in idCertificate_2_host.

18. Add any other key-value pairs that you require for Docs@Work.
19. Select the users and user groups that you want to distribute the AppConnect custom configuration to.
20. Click **Next**.
21. Click **Done**.

Related topics

- *MobileIron Docs@Work for Android Guide for Administrators*

Setting up Email+ to use derived credentials

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any for iOS Entrust for Android
Device platforms	iOS, Android AppConnect

Email+ for iOS and Email+ for Android can use derived credentials for:

- S/MIME signing
- S/MIME encryption
- Identifying and authenticating the email user to the email server

The tasks for configuring derived credentials use in Email+ are:

1. Uploading the root and issuer chain certificates

2. Adding Email+ for iOS to the App Catalog
3. Adding Email+ for Android to the App Catalog
4. Setting up MobileIron Tunnel for iOS if the Exchange server is behind your firewall

Before you begin

- Set up the Microsoft Exchange server to accept certificate authentication.
  See Configuring Certificate-Based Authentication for Microsoft Exchange.
- Have available for upload to MobileIron Cloud the certificate authority (CA) root certificate and certificate chain certificates that match your device users' smart card certificates.
  These certificates are necessary if your device users are using derived credentials to sign or encrypt S/MIME emails. They allow Email+ on the devices receiving the signed or encrypted email to trust the issuer chain certificates of the derived credentials.

Related topics

- *MobileIron Email+ for iOS Guide for Administrators*
- *MobileIron Email+ for Android Guide for Administrators*

Uploading the root and issuer chain certificates

If device users are using derived credentials for S/MIME encryption or signing, you provide a certificate configuration for the CA root certificate and each issuer chain certificate.

Procedure

For the CA root certificate and each issuer chain certificate:

1. In the Admin Portal, go to **Configurations**.
2. Click **+Add**.
3. Select **Certificate**.
4. Enter a name for the certificate configuration.
5. Drag and drop the certificate to the screen.
6. Click **Next**.
7. Select the devices to distribute the certificate to.
8. Click **Done**.

Adding Email+ for iOS to the App Catalog

Add Email+ for iOS to the App Catalog on the MobileIron Cloud Admin Portal.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Click **+Add**.
3. In the **Business Apps** section, select **Email+ (iOS**).
4. Click **Next**.
5. Click **Next**.
6. Select the users and user groups that you want to distribute the app to.
7. Click **Next**.
8. Scroll down to **Email+ Configuration**.
9. Select **+** to add a new Email+ configuration.

10. Enter a name for the Email+ configuration.
11. Enter field values according to the following table:

Item	Description
Email address	Enter the email address, typically **${userEmailAddress}.**
Email Password	Do not enter a value.
Exchange Host	Enter the fully qualified domain name of the Exchange server, **not** the Standalone Sentry. You do not configure a Standalone Sentry for ActiveSync.
Exchange Username	Enter the user name appropriate for your Exchange environment. For example, typically this value is **${userUID}**. Another possibility is **${userUIDLocalPart}**.
SSL required	Select this option to secure communication to the Exchange server using HTTPS.
Minimum Characters for GAL search	Enter the minimum number of characters for Email+ for iOS to use for automatic Global Address List (GAL) lookup in Mail and Contacts.
Identity Certificate	Select an identity certificate configuration for derived credentials from the drop-down list. The identity certificate configuration must have the purpose **Authentication**. Email+ will use this certificate to identify the device user to the Exchange server.
Trust All Certificates	Do not select.
Prompt for Password Before Connecting to Server	Do not select.
Lotus Notes Traveler	Do not select.
All remaining selections	Select according to your requirements. For more information, see MobileIron Email+ for iOS Guide for Administrators.

12. In the **AppConnect Certificate Configuration** section, add the **case-sensitive** key-value pairs necessary for Email+ to use derived credentials. Specifically:

Use case	Key	Value
Signing S/MIME emails	`email_signing_certificate`	Select an identity certificate configuration for derived credentials from the drop-down list. The identity certificate configuration must have the purpose **Signing**.
Encrypting S/MIME emails	`email_encryption_certificate`	Select an identity certificate configuration for derived credentials from the drop-down list. The identity certificate configuration must have the purpose **Encryption**.
Signing or encrypting S/MIME emails	`email_certificate_X` where X is 1 through 10	Select the CA root certificate or certificate chain certificate from the drop-down list.

13. Select the users and user groups that you want to distribute the Email+ configuration to.
14. Click **Next**.
15. Click **Done**.

Related topics

- *MobileIron Email+ for iOS Guide for Administrators*

Adding Email+ for Android to the App Catalog

Add Email+ for Android to the App Catalog on the MobileIron Cloud Admin Portal.

Procedure

1. Go to https://help.mobileiron.com and select the Software tab.
2. Download the Email+ for Android APK file.
3. In the Admin Portal, go to **Apps > App Catalog**.
4. Click **+Add**.
5. Select **In-House** to upload the app.
6. Drag and drop the Email+ for Android APK file to the designated area.
7. Click **Next**.
8. In **Category**, enter a category.
9. Click **Next**.
10. Click **Next**.
11. Click **Next**.
12. Select the users and user groups that you want to distribute the app to.
13. **Click Next.**
14. **Next to Email+ Configuration, click the + sign.**
15. Enter a name for the Email+ configuration.
16. In the **AppConnect Custom Configuration** section, add the **case-sensitive** key-value pair:

Key	Value
email_exchange_host	Enter the fully qualified domain name of the Exchange server, **not** the Standalone Sentry. You do not configure a Standalone Sentry for ActiveSync.

17. Confirm or change default values for the other key-value pairs in the **AppConnect Custom Configuration** section.
18. In the **AppConnect Certificate Configuration** section, add the **case-sensitive** key-value pairs necessary for Email+ to use derived credentials. Specifically:

Use case	Key	Value
Login certificate	`email_login_certificate`	Select an identity certificate configuration for derived credentials from the drop-down list. The identity certificate configuration must have the purpose **Authentication**. Email+ will use this certificate to identify the device user to the Exchange server.
Signing S/MIME emails	`email_signing_certificate`	Select an identity certificate configuration for derived credentials from the drop-down list. The identity certificate configuration must have the purpose **Encryption**.
Encrypting S/MIME emails	`email_encryption_certificate`	Select an identity certificate configuration for derived credentials from the drop-down list. The identity certificate configuration must have the purpose **Encryption**.
Signing or encrypting S/MIME emails	`email_certificate_X` where X is 1 through 10	Select the CA root certificate or certificate chain certificate from the drop-down list.

19. Select the users and user groups that you want to distribute the AppConnect custom configuration to.
20. Click **Next**.
21. Click **Done**.

Related topics

- *MobileIron Email+ for Android Guide for Administrators*

Setting up MobileIron Tunnel for iOS if the Exchange server is behind your firewall

Detailed information about setting up MobileIron Tunnel for iOS is available in the *MobileIron Tunnel for iOS Guide for Administrators*.

Adding in-house iOS AppConnect apps to the App Catalog

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any
Device platforms	iOS

Any in-house iOS AppConnect app can use certificates, and therefore certificates from a derived credential, as follows:

- In app-defined key-value pairs: The app processes key-value pairs that it expects in its AppConnect custom configuration. The app developer or vendor provides you the a list of key-value pairs, which you configure in the app’s AppConnect custom configuration and certificate configuration on the MobileIron Cloud Admin Portal.
- The app can authenticate to an enterprise service with a certificate, using the certificate authentication feature that the AppConnect library provides.
  This use case requires no development in the iOS AppConnect app. The AppConnect library that is built into each iOS AppConnect app receives the certificate and handles sending the certificate to the appropriate enterprise service.

NOTE: MobileIron Cloud does not support derived credentials with AppConnect apps it imports from the Apple App Store.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Select **+Add**.
3. Select **In-House** in the drop-down box to upload an in-house AppConnect app.
4. Drag and drop the app (IPA file) to the screen.
5. **Click Next.**
6. Enter a category in the **Category** field.
7. **Click Next.**
8. Optionally add screenshots.
9. **Click Next.**
10. **Click Next.**
11. Select the users and user groups that you want to distribute the app to.
12. **Click Next.**
13. Scroll down to **AppConnect Custom Configuration**.
14. Select **+** to add a new AppConnect custom configuration.
15. Enter a name for the AppConnect custom configuration.
16. In the **AppConnect Custom Configuration** section and the **AppConnect Certificate Configuration** section, add the **case-sensitive** key-value pairs to use derived credentials.
    For details, see AppConnect custom configuration key-value pairs for in-house iOS AppConnect apps.
17. Select the users and user groups that you want to distribute the AppConnect custom configuration to.
18. Click **Next**.
19. Click **Done**.

Related topics

AppConnect custom configuration key-value pairs for in-house iOS AppConnect apps

AppConnect custom configuration key-value pairs for in-house iOS AppConnect apps

Add key-value pairs to the AppConnect custom configuration for an in-house iOS AppConnect app to use derived credentials. The key-value pairs that you add depend on why the app uses derived credentials:

- App-defined key-value pairs
- AppConnect library certificate authentication feature

App-defined key-value pairs

The app can receive custom configuration settings that it defines. You add the keys that have non-certificate values to the AppConnect Custom Configuration for the app. You add keys with certificate values to the AppConnect Certificate Configuration for the app. The app developer or vendor provides you the a list of key-value pairs.

In the **AppConnect Certificate Configuration** section for the app, add the specified **case-sensitive** keys and their values to use a derived credential for this use case:

Key	Value
<app-specific key name> NOTE: The app developer or vendor provides you the app-specific key name.	Select an identity certificate configuration for derived credentials from the drop-down list. The identity certificate configuration must have the purpose (Authentication, Signing, or Encryption) appropriate for this app-specific key. MobileIron Go delivers to the app the certificate from the derived credential that corresponds to the purpose.

AppConnect library certificate authentication feature

The app can authenticate to an enterprise service with a certificate, using the certificate authentication feature that the AppConnect library provides.

1. In the **AppConnect Custom Configuration** section, add this **case-sensitive** key-value pair to use a derived credential for this use case:

Key	Value
MI_AC_CLIENT_CERT_1_RULE	The URL for the website to which the certificate from the derived credential will be presented. Wildcards are permitted in the host name. Examples: • *.mycompany.com/sales • myserver.mycompany.com/hr/benefits

2. Repeat with similar keys with different numbers for other rules. For example
   :

Key	Value
MI_AC_CLIENT_CERT_2_RULE	myOtherServer.mycompany.com
MI_AC_CLIENT_CERT_3_RULE	YetAnotherServer.mycompany.com

3. In the **AppConnect Certificate Configuration** section, add this **case-sensitive** key-value pair:

Key	Value
MI_AC_CLIENT_CERT_1	Select an identity certificate configuration for derived credentials from the drop-down list. The identity certificate configuration must have the purpose **Authentication**. This certificate is presented to URLs defined by the corresponding rule.

4. Repeat with similar keys with different numbers to correspond to the other rules. For example:

Key	Value
MI_AC_CLIENT_CERT_2	Select an identity certificate configuration for derived credentials from the drop-down list. The identity certificate configuration must have the purpose **Authentication**.
MI_AC_CLIENT_CERT_3	Select an identity certificate configuration for derived credentials from the drop-down list. The identity certificate configuration must have the purpose **Authentication**.

Related topics

In the *MobileIron Core AppConnect and AppTunnel Guide,* "Certificate authentication from AppConnect apps to enterprise services", which includes details about what the value of the MI_AC_CLIENT_CERT_#_RULE keys can be

Adding Android AppConnect apps to the App Catalog

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Entrust
Device platforms	Android

If you are using Android AppConnect apps with derived credentials, add the apps to the App Catalog on MobileIron Cloud.

Before you begin

Get the AppConnect app (the APK file) from the in-house or third-party developer.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Click **+Add**.
3. Select **In-House** to upload the app.
4. Drag and drop the AppConnect app's APK file to the designated area.
5. Click **Next**.
6. In **Category**, enter a category.
7. Click **Next**.
8. Click **Next**.
9. Click **Next**.
10. Select the users and user groups that you want to distribute the app to.
11. **Click Next.**
12. **Next to AppConnect Custom Configuration, click the + sign.**
13. Enter a name for the configuration.
14. In the **AppConnect Custom Configuration** section, add the key-value pairs as specified by the app developer or vendor.
15. In the **AppConnect Certificate Configuration** section, add the key-value pairs as specified by the app developer or vendor.
16. Select the users and user groups that you want to distribute the AppConnect custom configuration to.
17. Click **Next**.
18. Click **Done**.

Device User Experience with Entrust

Setting up Entrust derived credentials during registration

When device users register their devices with MobileIron Cloud, they can set up derived credentials for use by AppConnect apps. The device user does the following tasks as part of this registration and derived credential setup process:

- Authenticating to the MobileIron Cloud Self-Service Portal with a smart card
- Generating the one-time registration PIN and requesting a derived credential
- Installing MobileIron Go
- Registering MobileIron Go for iOS
- Registering MobileIron Go for Android and installing Android AppConnect apps
- Setting up Entrust derived credentials during registration
- Activating the Entrust derived credential requested on the Self-Service Portal
- Installing AppConnect apps for iOS
- Running AppConnect apps for iOS
- Running AppConnect apps for Android

Authenticating to the MobileIron Cloud Self-Service Portal with a smart card

A device user authenticates to the MobileIron Cloud Self-Service Portal with a smart card. This procedure is supported only on desktop computers. It is not supported with:

- mobile devices
- Firefox

This procedure assumes you have sent the device user an email invitation to register with MobileIron Cloud. The email provides a link to the Self-Service Portal sign-in page because you have configured both of the following for the device user:

- A Self Service Portal Authentication setting where the **Self Service Portal Authentication Type** is **Certificate**
- A Device Registration Setting where the **Device Registration Authentication Type** is **PIN Only**

Procedure

1. Connect a smart card reader, with a smart card inserted, to a desktop computer.

2. On the desktop computer, point a supported browser to the link specified in the email.
3. Click **Sign in with Certificate**.
4. Select the certificate from the smart card.
5. When prompted, enter the PIN for the smart card.

Generating the one-time registration PIN and requesting a derived credential

After signing in to the MobileIron Cloud Self-Service Portal, a device user requests a one-time registration PIN and a derived credential from Entrust.

NOTE: Do not register the device until after you request a derived credential and receive the Entrust activation password.

Procedure

1. Click **Request PIN and Derived Credential**.
   The MobileIron Cloud Self-Service Portal redirects the browser to the Entrust IdentityGuard Self-Service Module, which requests the user to login with their smart card to access the site.
2. On the Entrust.IdentityGuard Self-Service Module, follow the steps to request a derived credential. These steps are specific to your Entrust setup.
   As part of these steps, be sure to:
   a. Copy the Entrust activation password to enter later in the PIV-D Manager app on the device.
   b. Click **Done** to return to the MobileIron Cloud Self-Service Portal.
   The Entrust Identity Guard Self-Service Module redirects the browser back to the MobileIron Cloud Self-Service Portal.
   A registration PIN displays.
3. Copy the registration PIN to enter later into MobileIron Go on the device.

About a derived credential requested from the MobileIron Cloud Self-Service Portal

A derived credential (and its Entrust activation password) typically expire after a short time, such as 30 minutes (configurable in your Entrust Identity Guard Self-Service Module setup). Therefore, consider these scenarios:

- The derived credential expires before the device user registers a device.
  If the device user registers with the existing registration PIN, the user must request and activate a new derived credential as described in Setting up Entrust derived credentials after registration. Alternatively, the device user can generate a new registration PIN and request another derived credential.
- The derived credential expires after the device user registers a device.
  The device user must request and activate a new derived credential as described in Setting up Entrust derived credentials after registration.

Installing MobileIron Go

Instruct your device users to install the following apps, depending on whether they use iOS or Android:

- **iOS:** MobileIron Go for iOS
  Device users get the app from the Apple App Store.
- **Android:**
  - MobileIron Go for Android
  - the Secure Apps Manager app

Device users get the MobileIron Go from Google Play. The Secure Apps Manager app is bundled in MobileIron Go and installs as a separate app on the device.

Registering MobileIron Go for iOS

The device user registers MobileIron Go for iOS to MobileIron Cloud using the one-time registration PIN that the device user generated on the MobileIron Cloud Self-Service Portal.

Procedure

1. Launch MobileIron Go on the device.
2. Enter the user name.
3. Tap **Next**.
4. Enter the one-time registration PIN generated from the MobileIron Cloud Self-Service Portal.
5. Tap **Sign In**.
6. Follow the MobileIron Go instructions to complete registration.

Registering MobileIron Go for Android and installing Android AppConnect apps

To register to MobileIron Cloud, device users must first generate a one-time registration PIN and request a derived credential using the MobileIron Cloud Self-Service Portal. Then device users launch MobileIron Go on the device and enter:

- their user name
- the one-time registration PIN

For Android AppConnect, device users then follow MobileIron Go instructions to install the Secure Apps Manager. The Secure Apps Manager gives instructions to:

- create the secure apps passcode.
- install the PIV-D Manager app and any other mandatory AppConnect apps that you have assigned to this device.

Installing the PIV-D Manager app for iOS

The device user installs the PIV-D Manager app for iOS, which allows device users to activate the derived credential that they requested when they requested the MobileIron Cloud registration PIN. Device users can also use the app to request new derived credentials after they have already registered the device.

Procedure

1. Launch the App Catalog on the device.
2. Tap the listing for the PIV-D Manager app.
3. Tap **Install**.
4. On the pop-up, tap **Install**.

Activating the Entrust derived credential requested on the Self-Service Portal

The device user activates the derived credential that they requested on the MobileIron Cloud Self-Service Portal.

The different procedures for iOS and Android devices are described in:

- Activating the Entrust derived credential on an iOS device
- Activating the Entrust derived credential on an Android device

Activating the Entrust derived credential on an iOS device

Procedure

1. Launch the PIV-D Manager app for iOS.
   The app switches control to MobileIron Go, which prompts the device user to create a secure apps passcode.
2. Follow the MobileIron Go instructions to create a secure apps passcode.
3. After creating the secure apps passcode, tap **Done**.
   Control switches back to the PIV-D Manager app.
4. Tap on **Entrust IdentityGuard**.
   The app displays a screen that indicates that a new credential is ready for activation, and prompts for the Entrust activation password.
5. Tap **Enter Password**.
   The app displays a screen for entering the Entrust activation password.
   Enter the Entrust activation password.
6. Tap **Activate**.
7. Wait while the app validates the entry with Entrust.
   When the validation is complete, the app displays a screen for setting the derived credential PIN. This PIN is used when the device user authenticates over Bluetooth to a Windows 10 computer with the derived credential.
8. Enter a new derived credential PIN and enter it again to confirm it.
9. Tap **Done**.
   The app displays that the derived credential has been successfully activated.
10. Tap anywhere on the screen.
    The app displays the derived credential, which is now available for AppConnect apps to use.
    If you re-launch the PIV-D Manager app, a screen displays that activation was successful.

NOTE: If the Entrust activation password has expired, the PIV-D Manager app displays that an error occurred during activation. Tap **Try Again** to return to the **Authentication required** screen. Tap **Scan QR code** at the bottom of the screen to create a new derived credential. See Setting up Entrust derived credentials after registration.

Activating the Entrust derived credential on an Android device

Procedure

1. Launch the PIV-D Manager app.
2. If prompted, enter the secure apps passcode
3. Enter the Entrust activation passcode.
4. Tap **Activate**.
5. Wait while the PIV-D Manager app validates the entry with Entrust.
   When the validation is complete, the app displays a screen for setting the derived credential PIN. This PIN is used when the device user authenticates over Bluetooth to a Windows 10 computer with the derived credential.
6. Enter a new derived credential PIN and enter it again to confirm it.

7. Tap **Done**.
   The app displays the derived credential. The derived credential, which includes three certificates, is now available for AppConnect apps to use.

NOTE: If the Entrust activation password has expired, the PIV-D Manager app displays that an error occurred during activation. Tap **Try Again** to return to the screen for entering the activation password. Close the keyboard to reveal the icon for scanning the QR code. Tap the icon to create a new derived credential. See Setting up Entrust derived credentials after registration.

Related topics

"About the derived credential PIN" in Using Bluetooth for Entrust derived credential authentication on Windows

Installing AppConnect apps for iOS

The device user installs each AppConnect app for iOS that uses derived credentials.

Procedure

1. Launch the App Catalog for iOSon the device.
2. Tap the listing for the AppConnect app.
3. Tap **Install**.
4. On the pop-up, tap **Install**.

Running AppConnect apps for iOS

To run an iOS AppConnect app, including Web@Work, Docs@Work, or Email+, the device user launches the app, and then enters the secure apps passcode if prompted by MobileIron Go.The app then receives the derived credential from MobileIron Go.

NOTE: If an AppConnect app expects certificates from a derived credential but the derived credential is not available in MobileIron Go, the app becomes unauthorized. Some apps, such as Web@Work, display the unauthorized message. It says: “Missing required credentials. Please ensure you provisioned the credentials”.

Running AppConnect apps for Android

To run an Android AppConnect app, including Web@Work, Docs@Work, or Email+, the device user launches the app, and then enters the secure apps passcode if prompted by the Secure Apps Manager. The app then receives the derived credential from the Secure Apps Manager.

NOTE: If an AppConnect app expects certificates from a derived credential but the derived credential is not available in the Secure Apps Manager, the app becomes unauthorized.

Setting up Entrust derived credentials after registration

If device users do not set up derived credentials when they register their device, they can set them up later. The procedure is different than the procedure at registration.

A device user does the following tasks:

- Getting a QR code and Entrust activation password
- Depending on whether using iOS or Android:
  - Getting Entrust derived credentials using the PIV-D Manager app for iOS
  - Getting Entrust derived credentials using the PIV-D Manager app for Android

Getting a QR code and Entrust activation password

The user gets a QR code and Entrust activation password from your Entrust self-service portal. This portal is specific to your set up. Therefore, the following steps are *general* steps. They do not include wording and navigation specific to your Entrust self-service portal.

Procedure

1. Connect a smart card reader, with a smart card inserted, to a desktop computer.
2. On the desktop, open a browser and enter the https:// URL for your Entrust self-service portal.
3. Login to the portal with the smart card certificate.
4. When prompted, enter the PIN for the smart card.
5. Select the option to enroll for derived credentials using the PIV-D Manager app.
6. Provide a name for the new derived credential identity.
   On iOS devices, MobileIron Go will use this name when displaying the derived credential. On Android devices, the PIV-D Manager app will display this name.
7. Provide other information, if requested.

The Entrust self-service portal displays:

- a QR code
- an Entrust activation password

Leave the screen displaying on the desktop while continuing to the next task, which is on the device.

Getting Entrust derived credentials using the PIV-D Manager app for iOS

After using the Entrust self-service portal to get a QR (Quick Response) code and Entrust activation password, an iOS device user uses the PIV-D Manager app to get derived credentials on a device

Procedure

1. Install the PIV-D Manager app if it is not already installed:
   a. Launch Apps@Work on the device.
   b. Tap the listing for the PIV-D Manager app.
   c. Tap **Install**.
   d. On the pop-up, tap **Install**.
2. Launch the PIV-D Manager app.

3. If this is the first time you launch an AppConnect app on the device, follow the MobileIron Go instructions to create a secure apps passcode.
   After you create the secure apps passcode, control returns to the PIV-D Manager app
4. Tap on **Entrust IdentityGuard**.
5. Tap **OK** if you are prompted to allow the PIV-D Manager app to access the camera.
   The app displays a screen that uses the camera to scan the QR code, which is displaying on the desktop computer on the Entrust self-service portal.
6. Point the camera at the QR code to scan it.
   When the app has scanned the QR code, it prompts you to enter the Entrust activation password.
7. Enter the Entrust activation password, which is displaying on the desktop computer on the Entrust self-service portal.
8. Tap **Activate**.
9. Wait while the app validates the entry with Entrust.
   When the validation is complete, the app displays a screen for setting the derived credential PIN. This PIN is used when the device user authenticates over Bluetooth to a Windows 10 computer with the derived credential.
10. Enter a new derived credential PIN and enter it again to confirm it.
11. Tap **Done**.
    The app displays that the derived credential has been successfully activated.
12. Tap anywhere on the screen indicating success.
    The app displays the derived credential, which is now available for AppConnect apps to use.
    If you re-launch the PIV-D Manager app, a screen displays that activation was successful.

Getting Entrust derived credentials using the PIV-D Manager app for Android

After using the Entrust self-service portal to get a QR (Quick Response) code and Entrust activation password, an Android device user uses the PIV-D Manager app to get derived credentials on a device.

Procedure

1. Launch the PIV-D Manager app.
2. If prompted, enter the secure apps passcode.

If the app opens to the screen for entering the Entrust activation passcode, close the keyboard and tap the Scan QR code button in the lower right-hand corner.

3. If prompted, allow the PIV-D Manager app to take pictures and record video.
4. Point the camera at the QR code to scan it.
   When the app has scanned the QR code, it prompts you to enter the Entrust activation password.
5. Enter the Entrust activation password, which is displaying on the desktop computer on the Entrust self-service portal.
6. Tap **Activate**.
7. Wait while the app validates the entry with Entrust.
   When the validation is complete, the app displays a screen for setting the derived credential PIN. This PIN is used when the device user authenticates over Bluetooth to a Windows 10 computer with the derived credential.
8. Enter a new derived credential PIN and enter it again to confirm it.
9. Tap **Done**.

The PIV-D Manager app displays the derived credential. The derived credential is now available for AppConnect apps to use.

Related topics

"About the derived credential PIN" in Using Bluetooth for Entrust derived credential authentication on Windows

Managing Entrust derived credentials on iOS devices

In MobileIron Go for iOS, you can:

- View a derived credential.
- Delete a derived credential.

Deleting a derived credential unauthorizes all AppConnect apps that use the credential. An app is unauthorized on its next check-in.

- Get a new derived credential.
  This action replaces the existing derived credential.

Viewing an Entrust derived credential on iOS devices

Procedure

1. In MobileIron Go, tap **Settings**.
2. Tap **Entrust Credential**.
   MobileIron Go displays the credential’s information.

NOTE: After a credential has been activated, the PIV-D Manager app provides a button labeled **Manage Existing Credential**. Tapping this button launches MobileIron Go, which displays the credential’s information.

Deleting an Entrust derived credential on iOS devices

WARNING: Deleting a derived credential unauthorizes all AppConnect apps that use the credential. An app is unauthorized on its next check-in.

Procedure

1. In MobileIron Go for iOS, tap **Settings**.
2. Tap **Entrust Credential**.
   MobileIron Go displays the credential’s information.
3. Click the trash icon in the upper right hand corner.
4. Click **Delete**.

Getting a new Entrust derived credential on iOS devices

Getting a new Entrust derived credential replaces the existing derived credential.

Procedure

1. Follow the instructions in Getting a QR code and Entrust activation password.
2. In MobileIron Go for iOS, tap **Settings**.
3. Tap **Entrust Credential**.
4. Tap **Activate New Credential**.

   The PIV-D Manager app launches. The app displays a screen that uses the camera to scan the QR code, which is displaying on the desktop computer on the Entrust self-service portal.
5. Point the camera at the QR code to scan it.

   When the app has scanned the QR code, it prompts you to enter the Entrust activation password.
6. Enter the Entrust activation password, which is displaying on the desktop computer on the Entrust self-service portal.
7. Tap **Activate**.
8. Wait while the app validates the entry with Entrust.

   When the validation is complete, a screen displays that indicates success. The derived credential, which includes three certificates, is now available in MobileIron Go for AppConnect apps to use.

NOTE: When a derived credential has been activated, the PIV-D Manager app also provides a button labeled **Activate New Credential**. Clicking this button leads to step Point the camera at the QR code to scan it. above.

Managing Entrust derived credentials on Android devices

In the PIV-D Manager app for Android AppConnect , you can:

- View a derived credential.
- Delete a derived credential.

  NOTE: Deleting a derived credential unauthorizes all AppConnect apps that use the credential. An app is unauthorized on its next check-in.
- Get a new derived credential.

  This action replaces the existing derived credential.

Viewing an Entrust derived credential on Android devices

Procedure

1. Launch the PIV-D Manager app.

   If prompted, enter the secure apps passcode. (Only for PIV-D Manager for Android AppConnect.)

   When a credential is activated, the app displays the credential’s name and expiration date.
2. Tap the credential to display its detailed information, including each certificate.
3. Tap on each certificate to see details about the certificate.

Deleting an Entrust derived credential on Android devices

WARNING: Deleting a derived credential unauthorizes all AppConnect apps that use the credential. An app is unauthorized on its next check-in.

Procedure

1. Launch the PIV-D Manager app.
   If prompted, enter the secure apps passcode. (Only for PIV-D Manager for Android AppConnect.)
   When a credential is activated, the app displays the credential's name and expiration date.
2. Tap the credential to display its detailed information.
3. Click the trash icon in the upper right hand corner.
4. Click **Delete**.

Getting a new Entrust derived credential on Android devices

Getting a new Entrust derived credential replaces the existing derived credential.

Procedure

1. Follow the instructions in Getting a QR code and Entrust activation password.
1. Launch the PIV-D Manager app.
2. If prompted, enter the secure apps passcode. (Only for PIV-D Manager for Android AppConnect.)
3. If prompted, allow the PIV-D Manager app to take pictures and record video.
4. Point the camera at the QR code to scan it.
   When the app has scanned the QR code, it prompts you to enter the Entrust activation password.
5. Enter the Entrust activation password, which is displaying on the desktop computer on the Entrust self-service portal.
6. Tap **Activate**.
7. Wait while the app validates the entry with Entrust.
   When the validation is complete, the PIV-D Manager app displays the derived credential.The derived credential, which includes three certificates, is now available for AppConnect apps to use.

Using Bluetooth for Entrust derived credential authentication on Windows

The PIV-D Manager app for iOS and for Android support using an Entrust derived credential from an iOS or Android device to authenticate to a Windows 10 computer. This procedure is a convenient substitute to authenticating to a Windows computer by placing a smart card in a smart card reader attached to the workstation.

To use this authentication procedure, the Windows 10 computer must:

- install an Entrust Smart Credential Dongle (necessary only when using iOS devices)
- install the Entrust IdentityGuard Bluetooth Smart Credential Reader application
- have smart card login enabled

Using the PIV-D Manager app, the user activates an Entrust derived credential on the device. After a derived credential is activated:

- The iOS user uses the PIV-D Manager app to pair the iOS device with the Windows 10 computer using Bluetooth.
- The Android user pairs the Android device with the Windows 10 computer using Bluetooth

Once paired with the device, the Windows 10 computer has access to the derived credential on the device. The user can now:

- Log into the Windows 10 computer by entering the derived credential PIN.
- Authenticate to protected websites from the Windows 10 computer by entering the smart card PIN. A protected website in this scenario is a website which the user normally authenticates to with a smart card.

Related topics

- About the derived credential PIN
- Tasks for Windows authentication from an iOS device
- Tasks for Windows authentication from an Android device

About the derived credential PIN

When a device user activates an Entrust derived credential on a device, a PIN is associated with the derived credential. The device user enters this derived credential PIN when authenticating over Bluetooth with the derived credential to:

- a Windows 10 computer
- a protected website

The derived credential PIN on iOS devices

On iOS devices running the PIV-D Manager app 2.2 through the most recently released version as supported by MobileIron, the device user sets the derived credential PIN when the derived credential is activated. Using options in the **Settings > Entrust** screen of the PIV-D Manager app for iOS, device users can later change the derived credential PIN, or reset it if they forgot it. Some device users find it convenient to set the derived credential PIN the same as the secure apps passcode.

The derived credential PIN has a minimum length of 4 digits and a maximum length of 8 digits. Only digits (0 - 9) are allowed.

NOTE: If the device user has already activated a derived credential before upgrading to PIV-D Manager app 2.2, the user can find out what the derived credential PIN is by going to the Entrust IdentityGuard Self-Service Module. Alternatively, the device user can reset the derived credential PIN.

Related topics

- Changing the derived credential PIN on iOS devices
- Resetting the derived credential PIN on iOS devices
- Activating the Entrust derived credential on an iOS device
- Getting Entrust derived credentials using the PIV-D Manager app for iOS

The derived credential PIN on Android devices

On Android devices running the PIV-D Manager app 1.3 through the most recently released version as supported by MobileIron, the device user sets the derived credential PIN when the derived credential is activated. Using options in the **General Settings** screen of the PIV-D Manager app for Android, device users can later change the derived credential PIN, or reset it if they forgot it. Some device users find it convenient to set the derived credential PIN the same as the secure apps passcode.

The derived credential PIN has a minimum length of 4 digits and a maximum length of 8 digits. Only digits (0 - 9) are allowed.

NOTE: If the device user has already activated a derived credential before upgrading from PIV-D Manager app 1.2, the derived credential PIN is automatically set to the same PIN as the smart card PIN. The device user can then use the PIV-D Manager app to change the derived credential PIN if desired.

Related topics

- Changing the derived credential PIN on an Android device
- Resetting the derived credential PIN on an Android device
- Activating the Entrust derived credential on an Android device
- Getting Entrust derived credentials using the PIV-D Manager app for Android

Tasks for Windows authentication from an iOS device

To use an Entrust derived credential from an iOS device to authenticate to a Windows 10 computer using Bluetooth:

- Providing the Entrust derived credential from an iOS device to a Windows computer over Bluetooth
- Authenticating to a Windows computer with an Entrust derived credential from an iOS device using Bluetooth
- Authenticating to protected websites with an Entrust derived credential from an iOS device using Bluetooth
- Tearing down the Bluetooth connection with an iOS device
- Changing the derived credential PIN on iOS devices
- Resetting the derived credential PIN on iOS devices
- Reconnecting Bluetooth connection automatically on iOS devices

Providing the Entrust derived credential from an iOS device to a Windows computer over Bluetooth

Before you begin

1. Activate an Entrust derived credential on your iOS device.
   See Setting up Entrust derived credentials during registration or Setting up Entrust derived credentials after registration.
2. Enable smart card login on your Windows 10 computer.
3. Install the Entrust IdentityGuard Bluetooth Smart Credential Reader application on the Windows 10 computer.
4. Connect the Entrust Smart Credential Dongle to the Windows 10 computer.

Procedure

1. In **Settings** on the iOS device, enable Bluetooth.
2. Launch the PIV-D Manager app.
   If prompted, enter the AppConnect passcode or AppConnect biometric authentication.

3. Tap **Entrust IdentityGuard**.
   The **Entrust IdentityGuard** screen displays.
4. Tap **Add Bluetooth device**.
   All available, unconnected Bluetooth devices are displayed.
5. Tap on the entry for the Windows 10 computer.
   The Bluetooth pairing code displays.
6. Enter the Bluetooth pairing code on the display that appears on the Windows 10 computer. You have limited time to enter the pairing code.
   When the iOS device has accepted the pairing, the Windows dialog indicates success.
7. Click **Close** on the Windows dialog.
   You can now use the Entrust derived credential on the iOS device for authenticating to the Windows 10 computer. You can also use it to authenticate to protected websites from the Windows 10 computer. For these authentications to succeed, the Bluetooth pairing must remain connected.

Authenticating to a Windows computer with an Entrust derived credential from an iOS device using Bluetooth

After you have completed the steps in Providing the Entrust derived credential from an iOS device to a Windows computer over Bluetooth, you can use the derived credential to authenticate to the Windows 10 computer, instead of authenticating with a smart card.

Procedure

1. On the Windows 10 computer, select the option to login with a smart card.
2. When prompted by the Windows 10 computer, enter your derived credential PIN.
   You can view the derived credential PIN on the iOS device in the PIV-D Manager in the Entrust IdentityGuard screen by tapping **ShowPIN**. The derived credential PIN is not necessarily the same as the smart card PIN.
   After entering the derived credential PIN, you are logged into the Windows 10 computer.

Authenticating to protected websites with an Entrust derived credential from an iOS device using Bluetooth

After you have completed the steps in Providing the Entrust derived credential from an iOS device to a Windows computer over Bluetooth, you can use the derived credential to authenticate to protected websites, instead of authenticating with a smart card. A protected website in this scenario is one that you can authenticate to with a smart card.

Before you begin

Complete the steps in Providing the Entrust derived credential from an iOS device to a Windows computer over Bluetooth. Note that the Bluetooth connection must still be active for you to authenticate to protected websites with the Entrust derived credential.

Procedure

1. On the Windows computer, navigate to a protected website in a browser and follow the instructions to login to the website.
   Windows displays a dialog for you to choose the appropriate certificate.

2. Select the certificate for which the serial number corresponds to the derived credential from the iOS device.
   To know which certificate to select, view the serial number on the iOS device in the PIV-D Manager in the Entrust IdentityGuard screen. The identity is displayed under **Current Identity**.
3. Click **OK** on the Windows display after you have selected the correct certificate.
4. When prompted by the Windows computer, enter your derived credential PIN.
   You can view the derived credential PIN on the iOS device in the PIV-D Manager in the Entrust IdentityGuard screen by tapping **ShowPIN**.
   After entering the derived credential PIN, you are logged into the protected website.

Tearing down the Bluetooth connection with an iOS device

Only one iOS device can be paired with a Windows 10 computer for the purpose of giving the Windows computer access to the Entrust derived credential.

The following procedure describes how to tear down a Bluetooth connection.

Procedure

1. On the iOS device, launch the PIV-D Manager app.
   If prompted, enter the AppConnect passcode or AppConnect biometric authentication.
2. In the Entrust IdentityGuard screen, tap on the information icon next to the name of the connected Windows computer.
3. Tap **Forget this device**.
4. Go to iOS Settings.
5. Tap **Bluetooth**.
6. Tap the name of the Windows computer.
7. Tap **Forget This Device**.
8. On the Windows computer, open the Manage Bluetooth Smart Credential Dongle app.
9. Select the iOS device.
10. Click **Remove Device**.

Changing the derived credential PIN on iOS devices

When you use a derived credential to authenticate from an iOS device over Bluetooth to a Windows 10 computer or protected website, the Windows 10 computer prompts you for your derived credential PIN. You can change your derived credential PIN.

Procedure

1. On the iOS device, launch the PIV-D Manager app.
   If prompted, enter the secure apps passcode or biometric authentication.
2. Select the settings icon in the upper right corner of the screen.
   The **Settings** screen displays.
3. Select **Entrust**.
4. Select **Change PIN**.
5. Enter your current derived credential PIN, your new derived credential PIN, and reenter your derived credential PIN.
6. Tap **Change**.
   The derived credential PIN has changed. The app returns to the **Settings** screen.

7. Tap **Done** to exit **Settings**.

Related topics

About the derived credential PIN

Resetting the derived credential PIN on iOS devices

When you use a derived credential to authenticate from an iOS device over Bluetooth to a Windows 10 computer or protected website, the Windows 10 computer prompts you for your derived credential PIN. You can reset your derived credential PIN if you forget it.

Procedure

1. On the iOS device, launch the PIV-D Manager app.
   If prompted, enter the secure apps passcode or biometric authentication.
2. Select the settings icon in the upper right corner of the screen.
   The **Settings** screen displays.
3. Select **Entrust**.
4. Select **Reset PIN**.
   The resulting screen displays the **Unblock Challenge** which you will use in a later step. It also displays the steps you will take.
5. Connect a smart card reader, with a smart card inserted, to a desktop computer.
6. On the desktop computer, open a browser and enter the https:// URL for your Entrust self-service portal.
7. Log in to the portal with the smart card certificate.
8. When prompted, enter the PIN for the smart card.
9. Click **I'd like to unlock my smart credential**.
10. Select the device that you want to unlock and click **Yes**.
11. Select **Windows 7 PIN Unblock**, regardless of your Windows operating system, and click **Next**.
    Do not select **Card Unblocking Key**.
12. In the **Challenge** field, enter the **Unblock Challenge** displayed in the PIV-D Manager app.
13. Click **OK**.
    The Entrust IdentityGuard SSM Module displays an unblock response code.
14. In the PIV-D Manager app on the device, tap **Next**.
15. Enter the unblock response code in the **Unblock Response** field.

The unblock response code you enter in the PIV-D Manager app is not case sensitive and can have spaces in it.

16. Enter a new derived credential PIN and reenter it to confirm it.
17. Tap **Reset**.
    The derived credential PIN has been reset. The app returns to the **Settings** screen.
18. Tap **Done** to exit **Settings**.

Related topics

About the derived credential PIN

Reconnecting Bluetooth connection automatically on iOS devices

When a device user has authenticated to a Windows 10 computer with a derived credential using Bluetooth, the Bluetooth connection drops when the user leaves the room with only her iOS device. The user can configure the PIV-D Manager app to automatically re-establish the connection when the device and Windows 10 computer are again within Bluetooth range. This setting is enabled by default.

Some other scenarios that cause the PIV-D Manager to automatically re-establish the connection are:

- The device user turns the laptop off and on.
- The device user puts the iOS device in and then out of airplane mode.

Note The Following:

- Automatically re-establishing the connection occurs only for the most recent Windows 10 computer that the device user authenticated to using Bluetooth.
- Automatically re-establishing the connection does not occur if the device user manually tears down the Bluetooth connection.

Procedure

1. On the iOS device, launch the PIV-D Manager app.
   If prompted, enter the secure apps passcode or biometric authentication.
2. Select the settings icon in the upper right corner of the screen.
3. Select **Entrust**.
4. Select **Entrust > Bluetooth - Auto Re-Connect** to enable automatic reconnection. Unselect the option to disable automatic reconnection.

Tasks for Windows authentication from an Android device

To use an Entrust derived credential from an iOS device to authenticate to a Windows 10 computer using Bluetooth:

- Setting up Bluetooth for Entrust derived credential authentication from an Android device to a Windows computer
- Authenticating to a Windows computer with an Entrust derived credential from an Android device using Bluetooth
- Authenticating to protected websites with an Entrust derived credential from an Android device using Bluetooth
- Stop sharing the derived credential from an Android device using Bluetooth
- Changing the derived credential PIN on an Android device
- Resetting the derived credential PIN on an Android device
- Reconnecting Bluetooth connection automatically on an Android device

Setting up Bluetooth for Entrust derived credential authentication from an Android device to a Windows computer

Before you begin

1. Activate an Entrust derived credential on your Android device.
   See Setting up Entrust derived credentials during registration or Setting up Entrust derived credentials after registration.

2. Make sure you know your derived credential PIN, which you set when you activated the derived credential. The derived credential PIN is not necessarily the same as the smart card PIN.
3. Enable smart card login on your Windows 10 computer.
4. Install the Entrust IdentityGuard Bluetooth Smart Credential Reader application on the Windows 10 computer.
5. Enable smart card login on your Windows 10 computer.
6. Enable Bluetooth on the Windows 10 computer.

NOTE: No physical dongle is used on the Windows 10 computer.

Procedure

1. Launch the PIV-D Manager app on the Android device.
   If prompted, enter the secure apps passcode or biometric authentication.
   The app displays the active derived credential.
2. Tap the Bluetooth icon.
   A pop-up displays instructing you to enable Bluetooth in device settings.
3. Tap **Settings** in the pop-up.
   The settings screen for Bluetooth displays.
4. Enable Bluetooth.
   Available devices for Bluetooth pairing display.
5. Tap the Windows 10 computer to pair with.
6. Tap **OK** in the pop-up to confirm the pairing request.
7. Confirm the pairing request on the Windows 10 computer
8. Click **Close** on the Windows dialog.
   The PIV-D Manager app displays the pairing.
   Once paired, you are ready to use the Entrust derived credential on the Android device for authenticating to the Windows 10 computer. You can also use it to authenticate to protected websites from the Windows computer. For these authentications to succeed, the Bluetooth pairing must remain active.

Authenticating to a Windows computer with an Entrust derived credential from an Android device using Bluetooth

After you have completed the steps in Setting up Bluetooth for Entrust derived credential authentication from an Android device to a Windows computer, you can use the derived credential to authenticate to the Windows 10 computer, instead of authenticating with a smart card.

Procedure

1. On the Windows 10 computer, select the option to login with a smart card.
2. Launch the PIV-D Manager app on your Android device.
   If prompted, enter the secure apps passcode or biometric authentication.
   The app displays the **Active Credentials** screen.
3. Tap the Bluetooth icon.
4. Tap the paired device corresponding to the Windows 10 computer.
   A pop-up displays asking if you want to connect with the Windows 10 computer to share the current derived credential.
5. Tap **Connect**.

If you were already connected to another Windows 10 computer, that computer is disconnected and its entry changes back to paired.

6. When prompted by the Windows 10 computer, enter your derived credential PIN.
   You are now logged into the Windows computer.
   The entry for the Windows 10 computer now indicates the computer is *connected* instead of *paired*. If you logout of the Windows 10 computer, you can login again by re-entering your derived credential PIN.
   When connected, the Windows computer can access the derived credential, so you can now also use the derived credential to authenticate to protected websites from the Windows computer.

Authenticating to protected websites with an Entrust derived credential from an Android device using Bluetooth

After you have completed the steps in Authenticating to a Windows computer with an Entrust derived credential from an Android device using Bluetooth, you can use the derived credential to authenticate to protected websites, instead of authenticating with a smart card. A protected website in this scenario is one that you can authenticate to with a smart card.

Before you begin

Complete the steps in Authenticating to a Windows computer with an Entrust derived credential from an Android device using Bluetooth. Note that the Bluetooth entry for the Windows 10 computer in the PIV-D Manager app must display **Connected**. When connected (not simply **Paired**), the Android device can share the derived credential with the Windows 10 computer.

Procedure

1. On the Windows 10 computer, navigate to a protected website in a browser and follow the instructions to login to the website.
   Windows displays a dialog for you to choose the appropriate certificate.
2. Select the certificate for which the serial number corresponds to the derived credential from the Android device.
3. Click **OK** on the Windows display after you have selected the correct certificate.
4. When prompted by the Windows 10 computer, enter your derived credential PIN.
   You are now logged into the protected website.

Stop sharing the derived credential from an Android device using Bluetooth

The following procedure describes how to stop sharing the derived credential using a Bluetooth connection.

Procedure

1. On the Android device, launch the PIV-D Manager app.
   If prompted, enter the secure apps passcode or biometric authentication.
2. Navigate to the screen that displays the Bluetooth pairings.
3. Tap the entry for a Windows 10 computer that is connected.
   A pop-up displays asking if you want to disconnect the Windows computer to stop sharing the derived credential.
4. Tap **Disconnect**.

The entry for the Windows 10 computer now indicates the computer is paired instead of connected. You can no longer use the derived credential on the Windows computer.

Changing the derived credential PIN on an Android device

When you use a derived credential to authenticate from an Android device over Bluetooth to a Windows 10 computer or protected website, the Windows 10 computer prompts you for your derived credential PIN. You can change your derived credential PIN.

Procedure

1. On the Android device, launch the PIV-D Manager app.
   If prompted, enter the secure apps passcode or biometric authentication.
2. Select the settings icon in the upper right corner of the screen.
3. Select **General Settings > Change Derived Credential PIN**.
4. Enter your current derived credential PIN, your new derived credential PIN, and reenter you derived credential PIN.
5. Tap **Done**.

Related topics

About the derived credential PIN

Resetting the derived credential PIN on an Android device

When you use a derived credential to authenticate from an Android device over Bluetooth to a Windows 10 computer or protected website, the Windows 10 computer prompts you for your derived credential PIN. You can reset your derived credential PIN if you forget it.

Procedure

1. On the Android device, launch the PIV-D Manager app.
   If prompted, enter the secure apps passcode or biometric authentication.
2. Select the settings icon in the upper right corner of the screen.
3. Select **General Settings > Reset Derived Credential PIN**.
   This screen displays the **Unblock Challenge** which you will use in a later step. It also displays the steps you will take.
4. Connect a smart card reader, with a smart card inserted, to a desktop computer.
5. On the desktop computer, open a browser and enter the https:// URL for your Entrust self-service portal.
6. Log in to the portal with the smart card certificate.
7. When prompted, enter the PIN for the smart card.
8. Click **I'd like to unlock my smart credential**.
9. Select the device that you want to unlock and click **Yes**.
10. Select the type of unlock key based on your Windows operating system and click **Next**.
    Do not select **Card Unblocking Key**.
11. In the **Challenge** field, enter the **Unblock Challenge** displayed in the PIV-D Manager app.
12. Click **OK**.
    The Entrust IdentityGuard SSM Module displays an unblock response code.
13. In the PIV-D Manager app on the device, tap **Next**.
14. Enter the unblock response code in the **Unblock Response** field.

15. Enter a new derived credential PIN and reenter it to confirm it.
16. Tap **Done**.

Related topics

About the derived credential PIN

Reconnecting Bluetooth connection automatically on an Android device

When a device user has authenticated to a Windows 10 computer with a derived credential using Bluetooth, the Bluetooth connection drops when the user leaves the room with only her Android device. The user can configure the PIV-D Manager app to automatically re-establish the connection when the device and Windows 10 computer are again within Bluetooth range. This setting is enabled by default.

Procedure

1. On the Android device, launch the PIV-D Manager app.
   If prompted, enter the secure apps passcode or biometric authentication.
2. Select the settings icon in the upper right corner of the screen.
3. Select **General Settings > Bluetooth - Auto reconnect to avoid manually connection to Bluetooth** to enable automatic reconnection. Unselect the option to disable automatic reconnection.

Using Entrust for push notification authentication to enterprise servers (iOS only)

The PIV-D Manager app for iOS supports handling push notifications to authenticate a non-AppConnect app to the app's enterpise server or web service with an Entrust derived credential. The enterprise server or web service (from here on called simply an enterprise server) must use SAML-based authentication.

In this scenario, the following steps occur:

1. A non-AppConnect app makes an authentication request to its SAML-based enterprise server.
2. The enterprise server responds to the app with a redirection request to the appropriate identity provider (IdP).
3. The IdP makes a request to an Entrust server.
4. The Entrust server sends an iOS push notification to the PIV-D Manager app.
5. The device user taps the notification to open the PIV-D Manager app. If necessary, control switches to MobileIron Go to prompt the device user for the secure apps passcode, and then control switches back to the PIV-D Manager app.
6. The PIV-D Manager app prompts the user to confirm the authentication request.
7. The user taps to confirm the authentication request.
8. The PIV-D Manager app signs the authentication request with the derived credential's authentication certificate's private key, and sends the request to the Entrust server.
9. The Entrust server validates the authentication request's signature, and tells the IdP to issue the SAML token to the app and to the app's enterprise server.

To set up this scenario:

1. Work with Entrust so that your IdP can interact with Entrust authentication services.
2. Configure derived credentials on MobileIron Cloud.

3. Activate an Entrust derived credential on your iOS device.

   See Setting up Entrust derived credentials during registration or Setting up Entrust derived credentials after registration.

What the device user experiences:

1. The device user opens a non-AppConnect app.
2. The user’s iOS device receives a push notification to the PIV-D Manager to confirm the authentication to the app's enterprise server.
3. The user taps the notification to open the PIV-D Manager, and enters the secure apps passcode if prompted.

   The PIV-D Manager displays a dialog box to confirm the authentication.

If the PIV-D Manager is in the foreground when the notification is received, it displays the dialog box.

4. The user taps one of the following:
   - **Confirm** to confirm the authentication.
   - **Cancel** to cancel the authentication.
   - **It Wasn’t Me** to indicate that the authentication is fraudulent.

Device User Experience with DISA Purebred on iOS devices

Setting up Purebred derived credentials on iOS devices

After device users register their devices with MobileIron Cloud, they can set up DISA Purebred derived credentials for use by AppConnect apps. The device user does the following tasks:

- Authenticating to the MobileIron Cloud Self-Service Portal with a smart card
- Generating the one-time registration PIN
- Installing MobileIron Go for iOS
- Registering MobileIron Go for iOS
- Installing the DISA Purebred Registration app
- Installing the PIV-D Manager app for iOS
- Getting a DISA Purebred derived credential
- Installing AppConnect apps for iOS
- Running AppConnect apps for iOS

Authenticating to the MobileIron Cloud Self-Service Portal with a smart card

A device user authenticates to the MobileIron Cloud Self-Service Portal with a smart card. This procedure is supported only on desktop computers. It is not supported with:

- mobile devices
- Firefox

This procedure assumes you have sent the device user an email invitation to register with MobileIron Cloud. The email provides a link to the Self-Service Portal sign-in page because you have configured both of the following for the device user:

- A Self Service Portal Authentication setting where the **Self Service Portal Authentication Type** is **Certificate**
- A Device Registration Setting where the **Device Registration Authentication Type** is **PIN Only**

Procedure

1. Connect a smart card reader, with a smart card inserted, to a desktop computer.
2. On the desktop computer, point a supported browser to the link specified in the email.
3. Click **Sign in with Certificate**.
4. Select the certificate from the smart card.
5. When prompted, enter the PIN for the smart card.

Generating the one-time registration PIN

After signing in to the MobileIron Cloud Self-Service Portal, a device user requests a one-time registration PIN on the Portal.

1. Click **Request a PIN**.
   A one-time registration PIN displays.
2. Copy the registration PIN and user name to enter later into MobileIron Go on the device.

Installing MobileIron Go for iOS

Instruct your device users to install MobileIron Go for iOS on their devices. Device users get the app from the Apple App Store.

Registering MobileIron Go for iOS

The device user registers MobileIron Go for iOS to MobileIron Cloud using the one-time registration PIN that the device user generated on the MobileIron Cloud Self-Service Portal.

Procedure

1. Launch MobileIron Go on the device.
2. Enter the user name.
3. Tap **Next**.
4. Enter the one-time registration PIN generated from the MobileIron Cloud Self-Service Portal.
5. Tap **Sign In**.
6. Follow the MobileIron Go instructions to complete registration.

Installing the DISA Purebred Registration app

The DISA Purebred Registration app gets the Purebred derived credential and passes the credential’s certificates to the PIV-D Manager app, which in turn passes them to MobileIron Go for iOS. Make sure the app is installed on applicable devices. Instruct the device users appropriately.

Installing the PIV-D Manager app for iOS

The device user installs the PIV-D Manager app for iOS. This app gets the DISA Purebred derived credential from the DISA Purebred Registration app, and passes the derived credential’s certificates to MobileIron Go for iOS.

Procedure

1. Launch the App Catalog on the device.
2. Tap the listing for the PIV-D Manager app.
3. Tap **Install**.
4. On the pop-up, tap **Install**.

Getting a DISA Purebred derived credential

The device user gets the DISA Purebred derived credential by using the DISA Purebred Registration app. Then the device user uses the PIV-D Manager app for iOS to import the derived credential's certificates from the DISA Purebred Registration app. The PIV-D Manager app imports the authentication, signing, and encryption certificates, and then sends all the certificates to MobileIron Go for iOS. These certificates overwrite any existing DISA Purebred derived credential certificates that the PIV-D Manager had previously sent to MobileIron Go.

Procedure

1. Launch the DISA Purebred Registration app.
2. Follow the app's instructions to get a DISA Purebred derived credential.
3. Launch the PIV-D Manager app for iOS.
   The app switches control to MobileIron Go, which prompts the device user to create a secure apps passcode.
4. Follow the MobileIron Go instructions to create a secure apps passcode.
5. After creating the secure apps passcode, tap **Done**.
   Control switches back to the PIV-D Manager app.
6. Tap **DISA Purebred**.
7. Tap **Import All**.
8. Tap **Browse**.
9. Tap **Locations**.
10. Tap the Purebred option.
11. Tap the first entry.
12. Follow the instructions to import the derived credential to the PIV-D Manager app and send it to MobileIron Go.

Installing AppConnect apps for iOS

The device user installs each AppConnect app for iOS that uses derived credentials.

Procedure

1. Launch the App Catalog for iOS on the device.
2. Tap the listing for the AppConnect app.
3. Tap **Install**.
4. On the pop-up, tap **Install**.

Running AppConnect apps for iOS

To run an iOS AppConnect app, including Web@Work, Docs@Work, or Email+, the device user launches the app, and then enters the secure apps passcode if prompted by MobileIron Go.The app then receives the derived credential from MobileIron Go.

NOTE: If an AppConnect app expects certificates from a derived credential but the derived credential is not available in MobileIron Go, the app becomes unauthorized. Some apps, such as Web@Work, display the unauthorized message. It says: "Missing required credentials. Please ensure you provisioned the credentials".

Managing DISA Purebred derived credentials on iOS devices

Using MobileIron Go for iOS and the PIV-D Manager app, you can do the following tasks:

- Viewing a DISA Purebred derived credential on iOS devices
- Deleting a DISA Purebred derived credential on iOS devices
- Getting a new DISA Purebred derived credential on iOS devices
- Importing selected certificates from a DISA Purebred derived credential on iOS devices

Viewing a DISA Purebred derived credential on iOS devices

Procedure

1. In MobileIron Go, tap **Settings**.
2. Tap **Purebred Credential**.
   MobileIron Go displays the credential's information.

NOTE: After a credential has been activated, the PIV-D Manager app provides a **Current Identity** section. Tapping it launches MobileIron Go, which displays the credential's information.

Deleting a DISA Purebred derived credential on iOS devices

WARNING: Deleting a derived credential unauthorizes all AppConnect apps that use the credential. An app is unauthorized on its next check-in.

Procedure

1. In MobileIron Go, tap **Settings**.
2. Tap **Purebred Credential**.
   MobileIron Go displays the credential's information.
3. Click the trash icon in the upper right hand corner.
4. Click **Delete**.

Getting a new DISA Purebred derived credential on iOS devices

Getting a new derived credential and importing it into MobileIron Go replaces the existing derived credential in MobileIron Go.

Procedure

1. Launch the DISA Purebred Registration app.
2. Follow the app's instructions to get a DISA Purebred derived credential.
3. Launch the PIV-D Manager app for iOS.
   The app switches control to MobileIron Go, which prompts the device user for the secure apps passcode.
4. Enter the secure apps passcode.
   Control switches back to the PIV-D Manager app.
5. Tap **DISA Purebred**.
6. Tap **Import All**.
7. Tap **Browse**.
8. Tap **Locations**.

9. Tap the Purebred option.
10. Tap the first entry.
11. Follow the instructions to import the derived credential to the PIV-D Manager app and send it to MobileIron Go..

Importing selected certificates from a DISA Purebred derived credential on iOS devices

After you have used the DISA Purebred Registration app to get DISA Purebred derived credentials, you use the PIV-D Manager app to import either all the derived credential’s certificates or only some of them.

When importing only some of the certificates, the PIV-D Manager app imports the selected certificates (selected from among authentication, signing, and encryption certificates) from the DISA Purebred Registration app. Then the PIV-D Manager app sends all the selected certificates to MobileIron Go for iOS.

IMPORTANT: The selected certificates overwrite **all** existing DISA Purebred derived credential certificates that the PIV-D Manager had previously sent to MobileIron Go.

Procedure

1. In the PIV-D Manager app, tap **DISA Purebred**.
2. Tap **Import Selected**.
3. Tap a certificate that you want to import.
4. Tap **Import**.
5. Tap **Import Other Certificate** if you want to import another certificate.
6. Repeat steps 3 and 4 if you want to import another certificate.
7. Tap **Send to MobileIron App**.

Device User Experience with other derived credential providers on iOS devices

- Setting up derived credentials on iOS devices
- Managing derived credentials on iOS devices

Setting up derived credentials on iOS devices

When using derived credentials on an iOS device from a provider other than Entrust or DISA Purebred, the device user does the following tasks:

- Authenticating to the MobileIron Cloud Self-Service Portal with a smart card
- Generating the one-time registration PIN
- Installing MobileIron Go
- Registering MobileIron Go
- Installing the derived credential app
- Installing AppConnect apps
- Running AppConnect apps

Authenticating to the MobileIron Cloud Self-Service Portal with a smart card

A device user authenticates to the MobileIron Cloud Self-Service Portal with a smart card. This procedure is supported only on desktop computers. It is not supported with:

- mobile devices
- Firefox

This procedure assumes you have sent the device user an email invitation to register with MobileIron Cloud. The email provides a link to the Self-Service Portal sign-in page because you have configured both of the following for the device user:

- A Self Service Portal Authentication setting where the **Self Service Portal Authentication Type** is **Certificate**
- A Device Registration Setting where the **Device Registration Authentication Type** is **PIN Only**

Procedure

1. Connect a smart card reader, with a smart card inserted, to a desktop computer.
2. On the desktop computer, point a supported browser to the link specified in the email.
3. Click **Sign in with Certificate**.
4. Select the certificate from the smart card.
5. When prompted, enter the PIN for the smart card.

Generating the one-time registration PIN

After signing in to the MobileIron Cloud Self-Service Portal, a device user requests a one-time registration PIN on the Portal.

1. Click **Request a PIN**.
   A one-time registration PIN displays.
2. Copy the registration PIN and user name to enter later into MobileIron Go on the device.

Installing MobileIron Go

Instruct your device users to install the MobileIron Go for iOS app on their devices, if it is not already there. Device users get the app from the Apple App Store.

Registering MobileIron Go

The device user registers MobileIron Go for iOS to MobileIron Cloud using the one-time registration PIN that the device user generated on the MobileIron Cloud Self-Service Portal.

Procedure

1. Launch MobileIron Go on the device.
2. Enter the user name.
3. Tap **Next**.
4. Enter the one-time registration PIN generated from the MobileIron Cloud Self-Service Portal.
5. Tap **Sign In**.
6. Follow the MobileIron Go instructions to complete registration.

Installing the derived credential app

The device user installs the derived credential app obtained from a derived credential provider. Provide the device user instructions on using the app based on documentation from the app vendor or developer.

Procedure

1. Launch the App Catalog on the device.
2. Tap the listing for the derived credential app.
3. Tap **Install**.
4. On the pop-up, tap **Install**.

Installing AppConnect apps

The device user installs each AppConnect app that uses derived credentials.

Procedure

1. Launch the App Catalog on the device.
2. Tap the listing for the AppConnect app.
3. Tap **Install**.
4. On the pop-up, tap **Install**.

Running AppConnect apps

To run an iOS AppConnect app, including Web@Work, Docs@Work, or Email+, the device user launches the app, and then enters the secure apps passcode if prompted by MobileIron Go.The app then receives the derived credential from MobileIron Go.

NOTE: If an AppConnect app expects certificates from a derived credential but the derived credential is not available in MobileIron Go, the app becomes unauthorized. Some apps, such as Web@Work, display the unauthorized message. It says: “Missing required credentials. Please ensure you provisioned the credentials”.

Managing derived credentials on iOS devices

In MobileIron Go, you can:

- View a derived credential.
- Delete a derived credential.

Deleting a derived credential unauthorizes all AppConnect apps that use the credential. An app is unauthorized on its next check-in.

- Get a new derived credential.
  This action replaces the existing derived credential.

Viewing a derived credential

Procedure

1. In MobileIron Go, tap **Settings**.
2. Tap the credential setting.
   MobileIron Go displays the credential’s information.

Deleting a derived credential

WARNING: Deleting a derived credential unauthorizes all AppConnect apps that use the credential. An app is unauthorized on its next check-in.

Procedure

1. In MobileIron Go, tap **Settings**.
2. Tap the credential setting.
   MobileIron Go displays the credential’s information.
3. Click the trash icon in the upper right hand corner.
4. Click **Delete**.

Getting a new derived credential

Getting a new derived credential replaces the existing derived credential.

Procedure

1. In MobileIron Go, tap **Settings**.
2. Tap the credential setting.
3. Tap **Activate New Credential**.
   The derived credential app launches. Follow instructions provided in the app or its documentation to obtain a new derived credential.