MobileIron Core 11.0.0.0 Derived Credentials Guide

January 7, 2021

For complete product documentation see:
MobileIron PIV-D Manager for Android Product Documentation

Contents

New features and enhancements

This guide documents the following new features and enhancements:

- **Product name change**: MobileIron PIV-D Entrust is now MobileIron PIV-D Manager.
  See the *MobileIron PIV-D Manager 1.5 for Android Release Notes* for information about the new features provided with MobileIron PIV-D Manager 1.5.
  The release notes are available at PIV-D Manager for Android Product Documentation.
- **Documentation update**: Removed Intercede related content.

About Derived Credentials with MobileIron

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 1. 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
Decryption of older emails when the certificate that had been used for encryption has expired	iOS
Authenticating the user to Standalone Sentry when using AppTunnel with Kerberos authentication to the backend server	iOS

Typically, a different identity certificate is used for authentication, signing, encryption, and the expired certificates used for decryption. 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 Core.
- The device must have the Mobile@Work 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 Core supports on iOS and Android, and the required derived credential app.

TABLE 2. DERIVED CREDENTIAL APP REQUIRED FOR EACH PROVIDER AND DEVICE PLATFORM

Derived credential provider	Device platform	Derived credential app
Entrust	iOS	PIV-D Manager app for iOS
Entrust	Android	PIV-D Manager app for Android
DISA Purebred	iOS	PIV-D Manager app for iOS
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 MobileIron-provided APIs.

App use cases for derived credentials

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

TABLE 3. 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. **iOS only:** • S/MIME decryption of older emails for which the original encryption certificate has expired. This feature requires: - Mobile@Work 10.2 for iOS through the most recently released version as supported by MobileIron - PIV-D Manager 2.1 for iOS through the most recently released version as supported by MobileIron - Email+ 3.8 for iOS through the most recently released version as supported by MobileIron - A derived credential provider that provides a set of decryption certificates
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.
Third-party AppConnect apps	iOS	• Any use of identity certificates in an app's key-value pairs. • Identifying and authenticating the app user to backend services using AppConnect for iOS certificate authentication provided by the AppConnect for iOS library.

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.

Related topics

- Tunneling use cases for derived credentials on iOS
- Using Entrust for push notification authentication to enterprise servers (iOS only)

Tunneling use cases for derived credentials on iOS

AppTunnel with HTTP/S tunneling and Kerberos authentication to the backend resource

NOTE: This use of derived credentials is supported only on iOS devices.

Consider the case where:

- You want to use AppTunnel to tunnel data between an AppConnect app on an iOS device to a backend resource, and
- You want to authenticate the device user to the backend resource using Kerberos authentication.

This scenario requires:

- AppTunnel with HTTP/S tunneling, because only it, not AppTunnel with TCP tunneling (also known as Advanced AppTunnel), supports Kerberos authentication to the backend resource
- Authenticating the device to the Sentry using a certificate that identifies the user, not just the device. This identity certificate can be a derived credential. You specify the derived credential when setting up the AppTunnel configuration for an AppConnect app.

MobileIron Tunnel app and certificate authentication to the backend or web resource

NOTE: This use of derived credentials is supported only on iOS devices.

Consider the case where:

- You want to tunnel data between an AppConnect app on an iOS device and a backend or web resource, and
- You want to authenticate the device user to the resource using a derived credential.

This scenario requires AppTunnel with TCP tunneling (also known as Advanced AppTunnel), which uses the MobileIron Tunnel app. This set up allows the app to pass an identity certificate to a backend or web resource. This identity certificate can be a derived credential.

To configure this scenario:

- You configure AppTunnel with TCP tunneling as you normally would. This configuration involves using the MobileIron Tunnel app to set up a per-app VPN for the app.
- You configure the AppConnect app in MobileIron Core so that the app will receive the derived credential in its app-specific configuration key-value pairs.

Related topics

App use cases for derived credentials

Multiple derived credential providers on an iOS device

Derived credentials with MobileIron Core supports multiple derived credential providers on a single iOS device. This feature is not supported on Android devices.

When you configure an AppConnect app in MobileIron Core to use derived credentials, you specify which derived credential provider it will use for each purpose (authentication, signing, encryption, decryption). Each app can use only one derived credential provider for each purpose.

This feature requires Mobile@Work 9.8 for iOS through the most recently released version as supported by MobileIron. Older versions of Mobile@Work use one of the available derived credentials, but cannot guarantee which one.

Related topics

- Adding a derived credential provider
- Configuring the default derived credential provider
- Configuring client-provided certificate enrollment settings

MobileIron products involved with derived credentials

The following table shows the MobileIron products necessary for an AppConnect app to use derived credentials.

TABLE 4. MOBILEIRON PRODUCTS INVOLVED WITH USING DERIVED CREDENTIALS

Product	Role in supporting derived credentials
MobileIron Core	You configure Core so that the appropriate AppConnect apps use derived credentials. NOTE: MobileIron Connected Cloud does not support derived credentials.
Mobile@Work for iOS	On iOS devices: • Registers the device users with MobileIron Core • 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.
Mobile@Work for Android	On Android devices: • Registers the device users with MobileIron Core

TABLE 4. MOBILEIRON PRODUCTS INVOLVED WITH USING DERIVED CREDENTIALS (CONT.)

Product	Role in supporting derived credentials
	• Passes information between the Secure Apps Manager and MobileIron Core.
Secure Apps Manager for Android	On Android devices: • Stores the derived credential. • Delivers the certificates from the credential to the appropriate AppConnect apps.
PIV-D Manager app for Android	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 Mobile@Work for iOS.
iOS: AppConnect for iOS SDK or wrapper used in third-party or 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 APIs provided by MobileIron 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 Core and Connector Release Notes and Upgrade Guide*
  - *Mobile@Work for iOS Release Notes*
  - *Mobile@Work 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*

Derived Credentials Setup Overview

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

- You configure MobileIron Core to support derived credentials.
  See What you configure on Core 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 Core to use derived credentials

The following diagram summarizes the MobileIron Core configuration for using derived credentials, and shows whether you do the configuration on the System Manager or the Admin Portal.

The table following the diagram:

- Describes each configuration task.
- Indicates to which derived credential providers and device platform (iOS or Android) the task applies.

Note The Following:

- The task list assumes you use Apps@Work to distribute apps to iOS devices. However, using Apps@Work is not required. Various methods are available for device users to get the app on their iOS devices. Therefore, tasks related to using Apps@Work are optional.
- The task list assumes that you want device users to register Mobile@Work 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.

FIGURE 1. DERIVED CREDENTIAL CONFIGURATION SUMMARY ON MOBILEIRON CORE

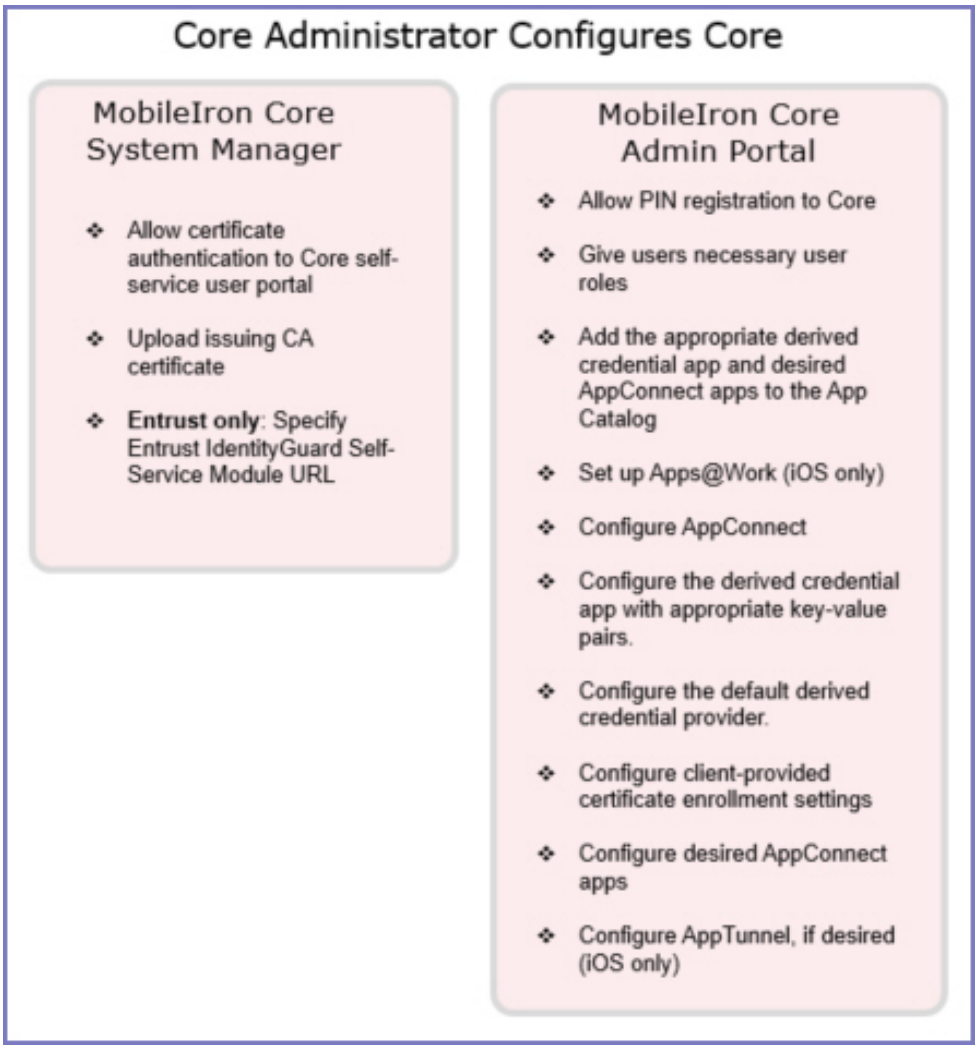


TABLE 5. DERIVED CREDENTIALS CONFIGURATION TASKS ON MOBILEIRON CORE

Task	Notes
1. Allow device users to authenticate to the MobileIron Core self-service user portal with the identity certificate on their smart cards.	Allowing certificate authentication includes uploading to Core 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 Core 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.
2. Provide the Entrust IdentityGuard Self-Service Module (SSM) URL to Core.	**Entrust** Core uses this URL to get derived credentials from Entrust. The device user will use the PIV-D Manager app to activate the derived credential on a device.
3. Allow device users to register Mobile@Work on their devices to Core 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. **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 Mobile@Work using a one-time registration PIN, this step is required.
4. Give device users the necessary user roles to use the MobileIron Core self-service user portal.	**All derived credentials providers** From the user portal, the device users can: • generate the one-time registration PIN. • reset their AppConnect passcode, if they forget it. An AppConnect passcode is necessary for a device user to access AppConnect apps. **Additionally, when using Entrust** From the user portal, device users get an Entrust derived credential, which includes getting the Entrust activation password to enter later on the device to activate the derived credential. This capability has no corresponding user portal role.
5. Add the derived credential app to	**Entrust on Android**

TABLE 5. DERIVED CREDENTIALS CONFIGURATION TASKS ON MOBILEIRON CORE (CONT.)

Task	Notes
the App Catalog on Core.	Add the PIV-D Manager app for Android to the App Catalog on Core. **Entrust and DISA Purebred on iOS** Add the PIV-D Manager app for iOS to the App Catalog on Core **Other derived credential providers on iOS** Add the appropriate third-party derived credential app to the App Catalog on Core. NOTE FOR iOS DEVICES: • For iOS devices, although the app is required on the device, this task is optional because it assumes you use Apps@Work, which is not required. Various methods are available for device users to get the app on their iOS devices.
6. Add the AppConnect apps that will use the derived credential to the App Catalog on Core.	**All derived credentials providers** NOTE FOR iOS DEVICES: • For iOS devices, although the app is required on the device, this task is optional because it assumes you use Apps@Work, which is not required. Various methods are available for device users to get the app on their iOS devices.
7. Set up Apps@Work for device users.	**All derived credentials providers** **iOS only** This task assumes you use Apps@Work for iOS. However, various methods are available for device users to get apps on their devices.
8. Configure AppConnect.	**All derived credentials providers** Configuring AppConnect allows device users to use AppConnect apps, including the derived credential app.
9. Configure the PIV-D Manager app for iOS.	**Configure the PIV-D Manager app for iOS as follows:** **Entrust** • Configure the Entrust activation URL that Core 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**

TABLE 5. DERIVED CREDENTIALS CONFIGURATION TASKS ON MOBILEIRON CORE (CONT.)

Task	Notes
	• 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.
10. Configure the PIV-D Manager app for Android.	**Entrust on Android** Configure the PIV-D Manager app for Android to: • receive the Entrust activation URL from Core 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.
11. Configure a third-party iOS derived credential app.	**On iOS, derived credential providers other than Entrust or DISA Purebred** You configure a third-party derived credential app to receive app-specific settings from Core, as defined by the app vendor or developer.
12. Configure the default derived credential provider.	**All derived credentials providers** **iOS only** Select which derived credential provider is the default choice. If necessary, add a derived credential provider to the list.
13. Configure client-provided certificate enrollment settings.	**All derived credentials providers** The activated derived credentials are stored in Mobile@Work for iOS or Secure Apps Manager for Android. You configure an AppConnect app to use derived credentials by referencing a client-provided certificate enrollment setting from the app's AppConnect app configuration (or Web@Work setting or Docs@Work setting). You configure a client-provided certificate enrollment setting for one of these purposes, as needed: authentication, signing, encryption, or decryption. NOTE: The certificate enrollment setting is called *client-provided* because Mobile@Work for iOS or Secure Apps Manager for Android, known as *client* apps, provide the identity certificate to the AppConnect app.

TABLE 5. DERIVED CREDENTIALS CONFIGURATION TASKS ON MOBILEIRON CORE (CONT.)

Task	Notes
14. Configure Web@Work.	**All derived credentials providers** This task is necessary only if your device users use Web@Work
15. Configure Docs@Work.	**All derived credentials providers** This task is necessary only if your device users use Docs@Work.
16. Configure Email+.	**All derived credentials providers** This task is necessary only if your device users use Email+.
17. Configure third-party and in-house AppConnect apps.	**All derived credentials providers** This task is necessary only if your device users use other AppConnect apps that use derived credentials.
18. Configure AppTunnel with HTTP/S tunneling to use derived credentials.	**All derived credentials providers** **iOS only** This task is necessary only if you want to use: • Kerberos authentication to the backend resource, and • AppTunnel to the backend resource Using AppTunnel with HTTP/S tunneling, you authenticate the user to the Standalone Sentry using a derived credential.
19. Configure AppTunnel with TCP tunneling to use derived credentials.	**All derived credentials providers** **iOS only** This task is necessary only if you want to use: • certificate authentication to the backend or web resource, and • AppTunnel to the backend or web resource Using per-app VPN with MobileIron Tunnel for iOS (AppTunnel with TCP tunneling), AppConnect apps can authenticate to the backend resource with a derived credential.

Device user tasks to use derived credentials

After you have configured MobileIron Core 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 The Following:

- These task lists assume you use Apps@Work to distribute apps to iOS devices. However, using Apps@Work is not required. Various methods are available for device users to get the app on their iOS devices. Therefore, tasks related to using Apps@Work are optional.
- These task lists assume that you want device users to register Mobile@Work 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

1. Authenticate to the MobileIron Core self-service user 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 Mobile@Work on the device.
5. Register Mobile@Work with MobileIron Core using the one-time registration PIN.
6. For Android devices, install the Secure Apps Manager for Android on the device, followed by the PIV-D Manager app, and any AppConnect apps.
7. For iOS devices, install the AppConnect apps on the device.
8. For iOS devices:
   a. Install the PIV-D Manager app for iOS on the device.
   b. 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:
   a. Install the PIV-D Manager app for Android on the device.
   b. 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 Core 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 user activates an Entrust derived Credential

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

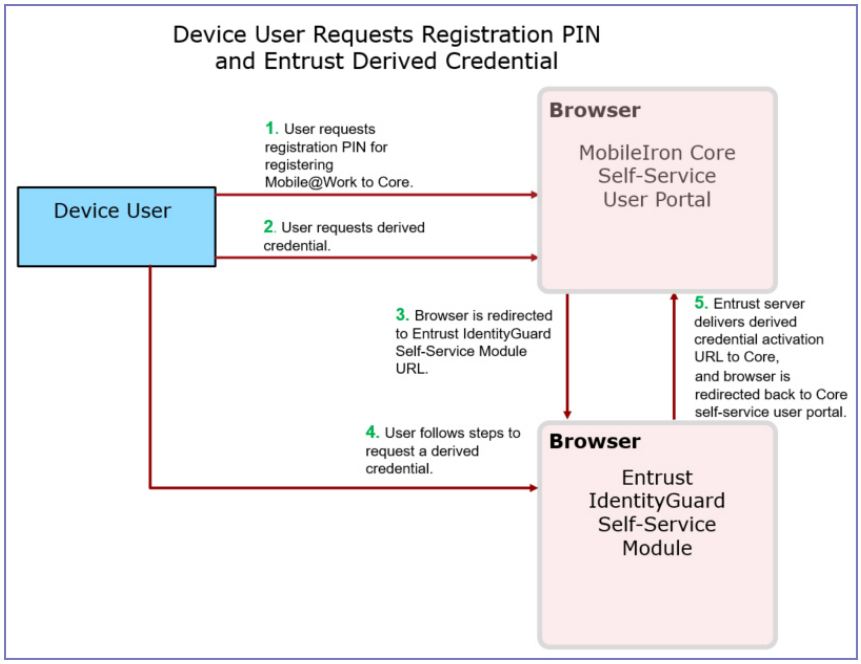


FIGURE 3. AN IOS USER ACTIVATES AN ENTRUST DERIVED CREDENTIAL

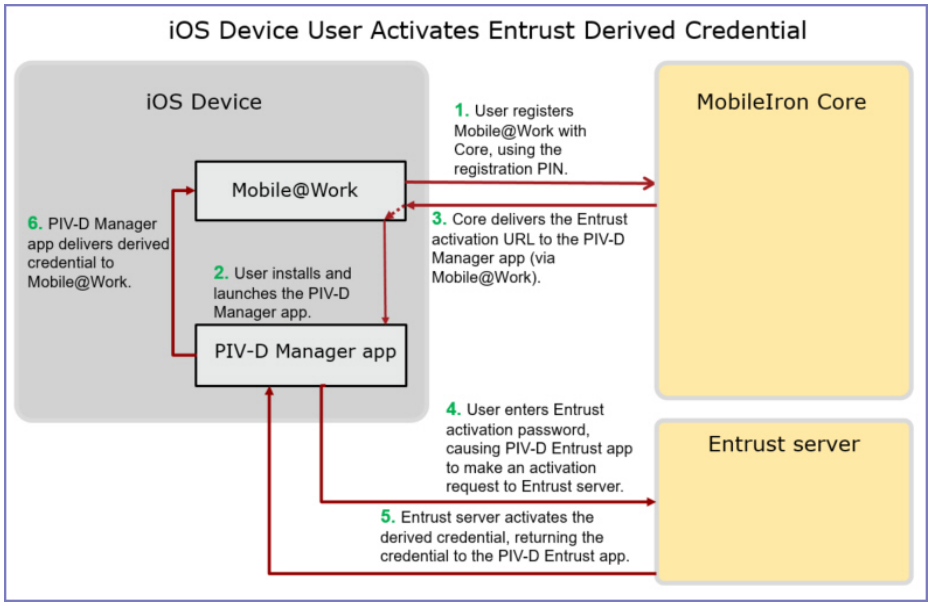
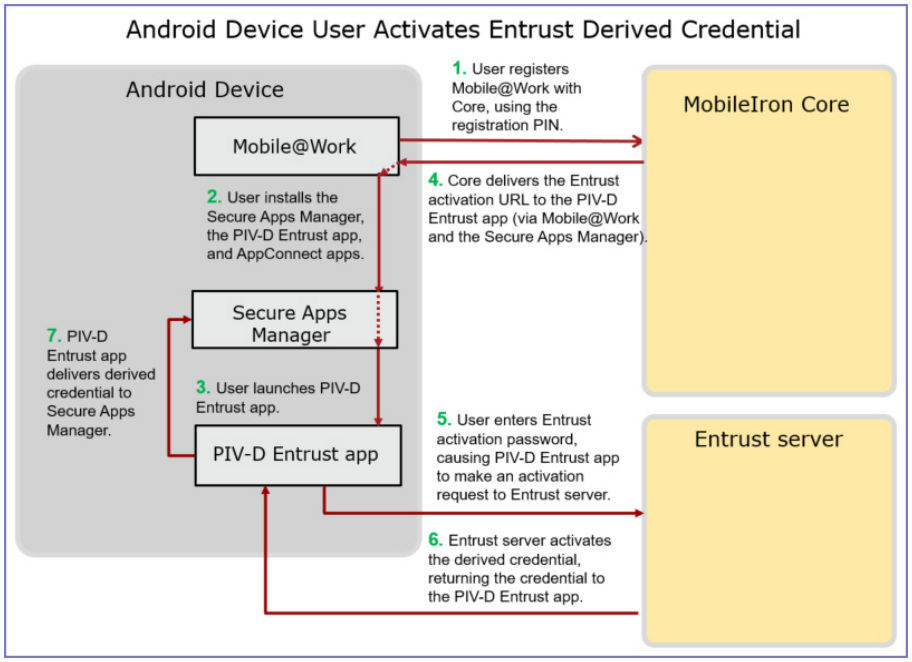


FIGURE 4. AN ANDROID USER ACTIVATES AN ENTRUST DERIVED CREDENTIAL



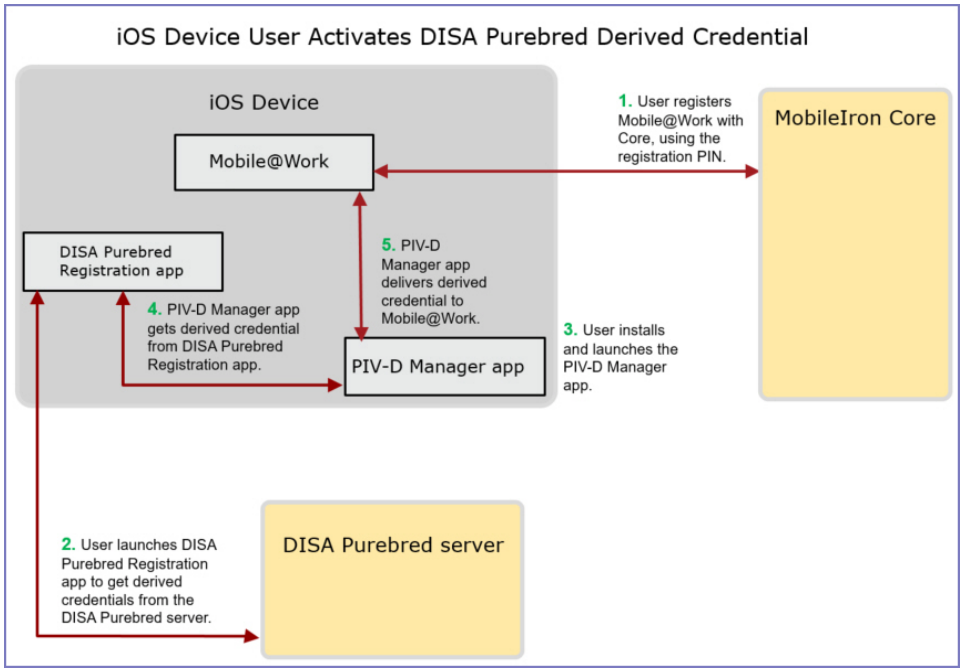
Device user tasks to use DISA Purebred derived credentials

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

1. Install the DISA Purebred Registration app on the device.
2. Authenticate to the MobileIron Core self-service user portal with a smart card.
3. Generate a one-time registration PIN.
4. Install Mobile@Work for iOS on the device.
5. Register Mobile@Work with MobileIron Core using the one-time registration PIN.
6. Install the AppConnect apps on the device.
7. Install the PIV-D Manager app for iOS on the device.
8. Launch the DISA Purebred Registration app to get the derived credential
9. 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 Mobile@Work.
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



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 Core self-service user portal with a smart card.
2. Generate a one-time registration PIN.
3. Install Mobile@Work on the device.
4. Register Mobile@Work with MobileIron Core using the one-time registration PIN.
5. For iOS devices, install the third-party derived credential app for iOS and any AppConnect apps on the device.
6. Launch the derived credential app and follow its instructions.
7. Use the AppConnect apps.

Related topics

Mobile device requirements for using derived credentials

Configuring MobileIron Core for derived credentials

Tasks before configuring MobileIron Core

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

TABLE 6. CONFIGURATION TASKS OUTSIDE OF MOBILEIRON CORE

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 the Core System Manager with this URL. After a device user generates the one-time MobileIron registration PIN on the Core self-service user portal, the user requests a derived credential. The request causes the user 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.

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 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 Mobile@Work for iOS.

Configuration tasks on MobileIron Core

The following table shows the tasks for configuring MobileIron Core 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 Core to support only DISA Purebred derived credentials, skip the tasks that are only applicable to Entrust derived credentials.

TABLE 7. CORE CONFIGURATION TASKS BY DERIVED CREDENTIAL PROVIDER AND DEVICE PLATFORM

Task	Derived credential providers	Device platforms
Configuring certificate authentication to the user 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 user portal roles	Required for Entrust, typical for all others	iOS, Android
Adding the Secure Apps Manager for Android to the App Catalog	Entrust	Android
Adding the PIV-D Manager app for iOS to the App Catalog	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 AppConnect apps to the App Catalog	Any	iOS, Android
Configuring Apps@Work for iOS	Any	iOS
Configuring AppConnect	Any	iOS, Android
Configuring the PIV-D Manager app for iOS for Entrust	Entrust	iOS
Configuring the PIV-D Manager app for iOS for DISA Purebred	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
Configuring a third-party iOS derived credential app	Any other than Entrust or DISA Purebred	iOS
Configuring the PIV-D Manager app for Android	Entrust	Android
Adding a derived credential provider	Any	iOS
Configuring the default derived credential provider	Any	iOS

TABLE 7. CORE CONFIGURATION TASKS BY DERIVED CREDENTIAL PROVIDER AND DEVICE PLATFORM (CONT.)

Task	Derived credential providers	Device platforms
Configuring client-provided certificate enrollment settings	Any	iOS, Android
Configuring Web@Work to use derived credentials	Any	iOS, Android
Configuring Docs@Work to use derived credentials	Any	iOS, Android
Configuring Email+ to use derived credentials	Any	iOS, Android
Configuring AppConnect apps to use derived credentials	Any	iOS, Android
Configuring AppTunnel with HTTP/S tunneling to use derived credentials	Any	iOS
Configuring the MobileIron Tunnel app to use derived credentials	Any	iOS

Configuring certificate authentication to the user 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 self-service user portal to get a one-time registration PIN (and, for Entrust, to request a derived credential). The device users authenticate to the user portal with the identity certificate on their smart cards.

Before you begin

To allow device users to authenticate to the MobileIron Core self-service user portal with the identity certificate on their smart cards, you need a PEM-formatted file. The file contains either a valid issuing (CA) certificate or a valid supporting certificate chain. When a user signs in to the user portal, they provide an identity certificate from a smart card. The user portal validates the identity certificate against the certificate that you upload to Core.

NOTE: The user identity in the identity certificate must contain the User Principal Name (UPN) in the Subject Alternative Name (SAN).

Procedure

1. In the System Manager, select **Security > Advanced > Admin/Self-Service User Portal Authentication**.

2. Under **Password Authentication**, clear the checkmark for **Self-Service User Portal.**
3. Select **Certificate Authentication.**
4. Under **Certificate Authentication**, select **Self-Service User Portal.**
5. Click **Upload Issuing CA Certificate**.
   A dialog appears for uploading the certificate.
6. Click **Choose File**, and select the PEM-formatted file that contains either the issuing CA certificate or the supporting certificate chain.
7. Click **Upload Certificate**.
8. Click **OK**.
9. Click **Apply > OK**.

Related topics

"Self-service user portal authentication" in the *MobileIron Core System Manager Guide*

Configuring the Entrust IdentityGuard SSM Module URL

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Entrust
Device platforms	iOS, Android

When you have configured certificate authentication for the user portal, the System Manager presents you with the option to configure the Entrust Identity Guard SSM Module URL.

Procedure

1. In the System Manager, select **Security > Advanced > Self-Service User Portal Authentication**.
2. Select **Derived Mobile Smart Credential**.
   The field **Entrust IdentityGuard SSM Module URL** appears.
3. Enter the Entrust IdentityGuard SSM Module URL.
   The self-service user portal directs the user to this URL when the user requests a derived credential.
   Example: https://yourEntrustSSM.yourcorp.com:8448/SelfService
4. Click **Apply > OK**.

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 Mobile@Work to MobileIron Core with a PIN.

Procedure

1. In the Admin Portal, go to **Settings > Users & Devices > Device Registration**.
2. For **In-App Registration Requirement**, select **Registration PIN**.
3. Click **Save**.

Configuring user portal roles

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 self-service user portal to get a one-time registration PIN (and, for Entrust, to request a derived credential). They can also use the user portal to reset the secure apps passcode. These capabilities require you to give the user the associated user roles.

Procedure

1. In the Admin Portal, go to **Devices & Users > Users**.
2. Select the devices users whose user roles you want to change.
3. Select **Actions > Assign Roles**.
4. Select **User Portal**.
5. Select **Register Device**.
6. Select **Reset Secure Apps Passcode**.
7. Click **Save**.

Adding the Secure Apps Manager for Android to the App Catalog

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Entrust
Device platforms	Android

Android device users require the Secure Apps Manager app because AppConnect apps are the apps that use derived credentials.

Procedure

1. Go to https://support.mobileiron.com/mi/android-sam/current. Alternatively, go to https://help.mobileiron.com and select the Software tab. Accessing these sites requires MobileIron credentials.
2. Download the Secure Apps Manager APK file.
3. In the Admin Portal, go to **Apps > App Catalog**.
4. Select **Android** from the **Platform** list.
5. Click **Add+** to open the app wizard.
6. Click **In-house**.
7. Click **Browse** to navigate to the Secure Apps Manager APK file.
8. Click **Next**.
9. Optionally add a description and select a category.
10. Click **Next**.
11. Optionally change Apps@Work catalog options, and the icon and screenshots.
12. Click **Next**.
13. Make sure the **Mandatory** setting is selected. It is the default selection.
14. Click **Finish**.

Apply the appropriate labels to the Secure Apps Manager as follows:

1. Select the Secure Apps Manager in the App Catalog.
2. Select **Actions > Apply to Labels**.
3. Select the labels associated with devices to which you want to send the Secure Apps Manager.
4. Click **Apply**.

Related topics

"Adding secure apps for Android" in the *MobileIron Core Apps@Work Guide*

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.

Various methods are available for device users to get the app on their iOS devices. This task assumes you use Apps@Work for iOS.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Select **iOS** from the **Platform** list.
3. Click **Add+.**
   The **iOS Add App Wizard** opens.
4. Click **iTunes** to import the PIV-D Manager app from the Apple App Store.

5. In **Application Name,** enter **MobileIron PIV-D Manager**.
6. Click **Search**.
7. Select the row naming the **MobileIron PIV-D Manager**.
8. Click **Next**.
9. Click **Next**.
10. Select **Feature this App in the Apps@Work catalog**.
11. Click **Next**.
12. Click **Finish**.

Apply the appropriate labels to the PIV-D Manager app as follows:

1. Select the PIV-D Manager app in the App Catalog.
2. Select **Actions > Apply to Labels**.
3. Select the labels associated with devices to which you want to send the PIV-D Manager app.
4. Click **Apply**.

Related topics

"Using the wizard to import iOS apps from the Apple App Store" in the *MobileIron Core Apps@Work Guide*

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

For derived credential providers other than Entrust and DISA Purebred, iOS device users use a third-party derived credential app to obtain derived credentials.

Various methods are available for device users to get the app on their iOS devices. This task assumes you use Apps@Work for iOS.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Select **iOS** from the **Platform** list.
3. Click **Add+.**
   The **iOS Add App Wizard** opens.
4. Click **iTunes** to import the derived credential app from the Apple App Store.
5. In **Application Name,** enter the name of the derived credential app.
6. Click **Search**.
7. Select the row naming the derived credential app.
8. Click **Next**.
9. Click **Next**.

10. Select **Feature this App in the Apps@Work catalog**.
11. Click **Next**.
12. Click **Finish**.

Apply the appropriate labels to the derived credential app as follows:

1. Select the derived credential app in the App Catalog.
2. Select **Actions > Apply to Labels**.
3. Select the labels associated with devices to which you want to send the derived credential app.
4. Click **Apply**.

Related topics

"Using the wizard to import iOS apps from the Apple App Store" in the *MobileIron Core Apps@Work Guide*

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.
3. In the Admin Portal, go to **Apps > App Catalog**.
4. Select **Android** from the **Platform** list.
5. Click **Add+** to open the app wizard.
6. Click **In-house**.
7. Click **Browse** to navigate to the PIV-D Manager app APK file.
8. Click **Next**.
9. Optionally add a description and select a category.
10. Click **Next**.
11. Optionally change Apps@Work catalog options, and the icon and screenshots.
12. Click **Next**.
13. Make sure the **Mandatory** setting is selected. It is the default selection.
14. Click **Finish**.

Apply the appropriate labels to the PIV-D Manager app for Android as follows:

1. Select the PIV-D Manager app for Android in the App Catalog.
2. Select **Actions > Apply to Labels**.
3. Select the labels associated with devices to which you want to send the PIV-D Manager app for Android.

4. Click **Apply**.

Related topics

"Adding secure apps for Android" in the *MobileIron Core Apps@Work Guide*

Adding AppConnect apps to the App Catalog

For the iOS apps, these tasks assume you use Apps@Work for iOS. However, various methods are available for device users to get apps on their iOS devices.

Adding Web@Work for iOS

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any
Device platforms	iOS

If you are using Web@Work for iOS with derived credentials, add Web@Work to the App Catalog on Core.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Select **iOS** from the **Platform** list.
3. Click **Add+.**
   The **iOS Add App Wizard** opens.
4. Click **iTunes** to import Web@Work from the Apple App Store.
5. In **Application Name,** enter **Web@Work.**
6. Click **Search**.
7. Select the row showing **MobileIron Web@Work**.
8. Click **Next**.
9. Click **Next**.
10. Select **Feature this App in the Apps@Work catalog**.
11. Click **Next**.

12. Click **Finish**.

Apply the appropriate labels to the Web@Work for iOS app as follows:

1. Select the MobileIron Web@Work for iOS app in the App Catalog.
2. Select **Actions > Apply to Labels**.
3. Select the labels associated with devices to which you want to send the Web@Work for iOS app.
4. Click **Apply**.

Related topics

"Using the wizard to import iOS apps from the Apple App Store" in the *MobileIron Core Apps@Work Guide*

Adding Web@Work for Android

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Entrust
Device platforms	Android

If you are using Web@Work for Android with derived credentials, add Web@Work to the App Catalog on Core.

Procedure

1. Go to https://support.mobileiron.com/mi/android-browser/current/. Alternatively, go to https://help.mobileiron.com and select the Software tab. Accessing these sites requires MobileIron credentials.
2. Download the Web@Work for Android APK file.
3. In the Admin Portal, go to **Apps > App Catalog**.
4. Select **Android** from the **Platform** list.
5. Click **Add+** to open the app wizard.
6. Click **In-house**.
7. Click **Browse** to navigate to the Web@Work APK file.
8. Click **Next**.
9. Optionally add a description and select a category.
10. Click **Next**.
11. Optionally change Apps@Work catalog options, and the icon and screenshots.
12. Click **Next**.
13. Click **Finish**.

Apply the appropriate labels to Web@Work for Android as follows:

1. Select Web@Work for Android in the App Catalog.
2. Select **Actions > Apply to Labels**.
3. Select the labels associated with devices to which you want to send the Web@Work for Android app.
4. Click **Apply**.

Related topics

"Adding secure apps for Android" in the MobileIron Core Apps@Work Guide

Adding Docs@Work for iOS

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 Core.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Select **iOS** from the **Platform** list.
3. Click **Add+.**
   The **iOS Add App Wizard** opens.
4. Click **iTunes** to import Docs@Work from the Apple App Store.
5. In **Application Name,** enter **Docs@Work.**
6. Click **Search**.
7. Select the row showing **MobileIron Docs@Work**.
8. Click **Next**.
9. Click **Next**.
10. Select **Feature this App in the Apps@Work catalog**.
11. Click **Next**.
12. Click **Finish**.

Apply the appropriate labels to the Docs@Work for iOS app as follows:

1. Select the MobileIron Docs@Work for iOS app in the App Catalog.
2. Select **Actions > Apply to Labels**.
3. Select the labels associated with devices to which you want to send the Docs@Work for iOS app.
4. Click **Apply**.

Related topics

"Using the wizard to import iOS apps from the Apple App Store" in the MobileIron Core Apps@Work Guide

Adding Docs@Work for Android

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Entrust
Device platforms	Android

If you are using Docs@Work for Android with derived credentials, add Docs@Work to the App Catalog on Core.

Procedure

1. Go to https://support.mobileiron.com/mi/android-browser/current/. Alternatively, go to https://help.mobileiron.com and select the Software tab. Accessing these sites requires MobileIron credentials.
2. Download the Docs@Work for Android APK file.
3. In the Admin Portal, go to **Apps > App Catalog**.
4. Select **Android** from the **Platform** list.
5. Click **Add+** to open the app wizard.
6. Click **In-house**.
7. Click **Browse** to navigate to the Web@Work APK file.
8. Click **Next**.
9. Optionally add a description and select a category.
10. Click **Next**.
11. Optionally change Apps@Work catalog options, and the icon and screenshots.
12. Click **Next**.
13. Click **Finish**.

Apply the appropriate labels to Docs@Work for Android as follows:

1. Select Docs@Work for Android in the App Catalog.
2. Select **Actions > Apply to Labels**.
3. Select the labels associated with devices to which you want to send the Docs@Work for Android app.
4. Click **Apply**.

Related topics

"Adding secure apps for Android" in the MobileIron Core Apps@Work Guide

Adding Email+ for iOS

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any
Device platforms	iOS

If you are using Email+ for iOS with derived credentials, add Email+ for iOS to the App Catalog on Core.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Select **iOS** from the **Platform** list.
3. Click **Add+.**
   The **iOS Add App Wizard** opens.
4. Click **iTunes** to import Email+ for iOS from the Apple App Store.
5. In **Application Name,** enter **MobileIron Email+.**
6. Click **Search**.
7. Select the row showing **MobileIron Email+**.
8. Click **Next**.
9. Click **Next**.
10. Select **Feature this App in the Apps@Work catalog**.
11. Click **Next**.
12. Click **Finish**.

Apply the appropriate labels to the Email+ app as follows:

1. Select the Email+ for iOS app in the App Catalog.
2. Select **Actions > Apply to Labels**.
3. Select the labels associated with devices to which you want to send the Email+ for iOS app.
4. Click **Apply**.

Related topics

"Using the wizard to import iOS apps from the Apple App Store" in the MobileIron Core Apps@Work Guide

Adding Email+ for Android

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Entrust
Device platforms	Android

If you are using Email+ for Android with derived credentials, add Email+ to the App Catalog on Core.

Procedure

1. Go to https://support.mobileiron.com/mi/android-browser/current/. Alternatively, go to https://help.mobileiron.com and select the Software tab. Accessing these sites requires MobileIron credentials.
2. Download the Email+ for Android APK file.
3. In the Admin Portal, go to **Apps > App Catalog**.
4. Select **Android** from the **Platform** list.
5. Click **Add+** to open the app wizard.
6. Click **In-house**.
7. Click **Browse** to navigate to the Email+ APK file.

8. Click **Next**.
9. Optionally add a description and select a category.
10. Click **Next**.
11. Optionally change Apps@Work catalog options, and the icon and screenshots.
12. Click **Next**.
13. Click **Finish**.

Apply the appropriate labels to Email+ for Android as follows:

1. Select Email+ for Android in the App Catalog.
2. Select **Actions > Apply to Labels**.
3. Select the labels associated with devices to which you want to send the Web@Work for Android app.
4. Click **Apply**.

Related topics

"Adding secure apps for Android" in the MobileIron Core Apps@Work Guide

Adding third-party iOS AppConnect apps from the Apple App Store

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any
Device platforms	iOS

If you are using third-party iOS AppConnect apps from the Apple App Store with derived credentials, add the apps to the App Catalog on Core.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Select **iOS** from the **Platform** list.
3. Click **Add+.**
   The **iOS Add App Wizard** opens.
4. Click **iTunes** to import Email+ for iOS from the Apple App Store.
5. In **Application Name,** enter the name of the app**.**
6. Click **Search**.
7. Select the row showing the app.
8. Click **Next**.
9. Click **Next**.
10. Select **Feature this App in the Apps@Work catalog**.
11. Click **Next**.
12. Click **Finish**.

Apply the appropriate labels to the app as follows:

1. Select the app in the App Catalog.

2. Select **Actions > Apply to Labels**.
3. Select the labels associated with devices to which you want to send the app.
4. Click **Apply**.

Related topics

"Using the wizard to import iOS apps from the Apple App Store" in the MobileIron Core Apps@Work Guide

Adding in-house iOS AppConnect apps

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any
Device platforms	iOS

If you are using in-house AppConnect apps with derived credentials, add the apps to the App Catalog on Core.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Select **iOS** from the **Platform** list.
3. Click **Add+.**
   The **iOS Add App Wizard** opens.
4. Click **In-House**.
5. Next to **Upload In-House App,** click **Browse** and navigate to the in-house iOS AppConnect app (.ipa) that you want to upload.
6. Click **Next**.
7. Click **Next**.
8. Click **Next**.
9. Click **Finish**.

Apply the appropriate labels to the app as follows:

1. Select the app in the App Catalog.
2. Select **Actions > Apply to Labels**.
3. Select the labels associated with devices to which you want to send the app.
4. Click **Apply**.

Related topics

"Using the wizard to add an in-house app for iOS to the App Catalog" in the MobileIron Core Apps@Work Guide

Adding Android AppConnect apps

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 Core.

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. Select **Android** from the **Platform** list.
3. Click **Add+** to open the app wizard.
4. Click **In-house**.
5. Click **Browse** to navigate to the AppConnect app's APK file.
6. Click **Next**.
7. Optionally add a description and select a category.
8. Click **Next**.
9. Optionally change Apps@Work catalog options, and the icon and screenshots.
10. Click **Next**.
11. Click **Finish**.

Apply the appropriate labels to the Android AppConnect app as follows:

1. Select the Android AppConnect app in the App Catalog.
2. Select **Actions > Apply to Labels**.
3. Select the labels associated with devices to which you want to send the Android AppConnect app.
4. Click **Apply**.

Related topics

"Adding secure apps for Android" in the MobileIron Core Apps@Work Guide

Configuring Apps@Work for iOS

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any
Device platforms	iOS

- Setting authentication options

- Sending the Apps@Work web clip to devices

This task assumes you use Apps@Work for iOS. However, various methods are available for device users to get apps on their devices.

Related topics

"Setting up Apps@Work for iOS" in the *MobileIron Core Apps@Work Guide*

Setting authentication options

Set the Apps@Work authentication option to use certificate authentication. By default, both certificate-based app authentication and HTTP basic authentication are enabled.

Procedure

1. In the Admin Portal, go to **Apps > Apps@Work Settings**.
2. Under **iOS App Storefront Authentication**
   a. Select **Certificate Authentication (iOS 5 and later)**.
   b. Clear **HTTP Basic Authentication**.
3. Click **Save**.

Sending the Apps@Work web clip to devices

MobileIron Core does not send the Apps@Work web clip to devices until you assign labels to the web clip.

Procedure

1. In the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select the **WEBCLIP** type setting called **System - iOS Enterprise AppStore**.
3. Select **More Actions > Apply to Label**.
4. Select the labels associated with devices to which you want to send the Apps@Work web clip.
5. Click **Apply**.
6. Click **OK**.

Configuring AppConnect

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any
Device platforms	iOS, Android

- Configuring AppConnect licenses
- Configuring the AppConnect global policy

Configuring AppConnect is required for device users to use derived credentials.

Related topics

"How to configure AppConnect and AppTunnel" in the *MobileIron Core AppConnect and AppTunnel Guide*

Configuring AppConnect licenses

Configure the necessary licensing in the MobileIron Core Admin Portal.

Procedure

1. Go to **Settings > System Settings > Additional Products > Licensed Products.**
2. If you are using Web@Work, select **Web@Work**.
3. If you are using Docs@Work, select **Docs@Work**.
4. For all other AppConnect apps, including Email+ for iOS, select **AppConnect for third-party and in-house apps**.
5. If you are using AppTunnel with third-party or in-house AppConnect apps, select **AppTunnel for Third-party and In-house Apps.**

Tunneling use cases with derived credentials are supported only on iOS devices.

6. Click **Save**.

Configuring the AppConnect global policy

To use AppConnect apps on a device, the device must have an AppConnect global policy. Typically, you configure a separate AppConnect global policy for iOS and Android devices.

ANDROID NOTE: The AppConnect global policy 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 when using Entrust derived credentials.

Procedure

1. In the Admin Portal, select **Policies & Configs > Policies**.
2. Select **Add New > AppConnect**.

Alternatively, use an existing AppConnect global policy.

3. For **Name**, enter a name for the new AppConnect global policy.
4. For **AppConnect**, select **Enabled**.
   The display now shows all the AppConnect global policy fields.
5. 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.
   - **Passcode Type**
   - **Minimum Passcode Length**.
   - **Minimum Number of Complex Characters**.
6. If the AppConnect global policy will be applied to iOS devices, in the **AppConnect Passcode** section:

   a. Select **Passcode is required for IOS devices**.
   b. Select **Allow iOS users to recover their passcode**.
7. If the AppConnect global policy will be applied to Android devices, in the **AppConnect Passcode** section:
   a. Select **Passcode is required for Android devices**.
   b. Select **Allow Android users to recover their passcode**.
8. In the **Security Policies** section, select **Authorize for Apps without an AppConnect container policy**.

If you do not select this option, provide an AppConnect container policy for each AppConnect app, including Web@Work, Docs@Work, and Email+, third-party and in-house AppConnect apps, and the derived credential app that you use, Note that Core automatically creates an AppConnect container policy for each Android AppConnect app, except for Web@Work and Docs@Work, when you upload the app to the App Catalog.

9. Click **Save > OK**.
10. Select the AppConnect global policy that you just created.
11. Select **More Actions > Apply to Label**.
12. Select the labels associated with devices to which you want to send the AppConnect global policy.
13. Click **Apply > OK**.

Configuring the PIV-D Manager app for iOS for Entrust

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Entrust
Device platforms	iOS

A device user uses the MobileIron PIV-D Manager app for iOS to activate Entrust derived credentials on a device after registering a device to MobileIron Core. This capability requires you to configure a key-value pair for the PIV-D Manager app in its AppConnect app configuration. The value is a Core variable that contains the activation URL. Entrust provides the activation URL to Core when the user requests a derived credential on the self-service user portal. The PIV-D Manager app receives the value when the user launches the app on the device.

You can also configure a key-value pair containing a unique device identifier that the 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.

Procedure

1. On the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select **Add New > AppConnect > App Configuration.**
3. Enter a name for the AppConnect app configuration, such as **PIV-D Manager app for iOS**.
4. Enter a description for the AppConnect app configuration.
5. In the **Application** field for the iOS app, enter **com.mobileiron.credentialmanager**.
6. In the **App-specific Configurations** section, add the **case-sensitive** key-value pairs:

Key	Value
MI_CREDENTIAL_ACTIVATION_URL	$DEVICE_PIVD_ACTIVATION_LINK$
Optional key and value MI_CREDENTIAL_DEVICE_ID	A MobileIron Core substitution variable that uniquely identifies the device. Examples: $DEVICE_ID$ $DEVICE_UUID$ $DEVICE_IMSI$

7. Click **Save**.
8. Select the AppConnect app configuration that you just created.
9. Click **More Actions > Apply to Label**.
10. Select the labels to which you want to apply this policy.
11. Click **Apply**.

Configuring the PIV-D Manager app for iOS for DISA Purebred

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	DISA Purebred
Device platforms	iOS

A device user uses the MobileIron PIV-D Manager app for iOS to use DISA Purebred derived credentials on a device after registering a device to MobileIron Core. This capability requires you to configure a key-value pair for the PIV-D Manager app that enables the app to support DISA Purebred derived credentials. You configure the key-value pair in the app's AppConnect app configuration.

Procedure

1. On the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select **Add New > AppConnect > App Configuration.**
3. Enter a name for the AppConnect app configuration, such as **PIV-D Manager app for iOS**.
4. Enter a description for the AppConnect app configuration.
5. In the **Application** field for the iOS app, enter **com.mobileiron.credentialmanager**.
6. In the **App-specific Configurations** section, add the **case-sensitive** key-value pair:

Key	Value
MI_CREDENTIAL_ENABLE_PUREBRED	True

7. Click **Save**.

8. Select the AppConnect app configuration that you just created.
9. Click **More Actions > Apply to Label**.
10. Select the labels to which you want to apply this policy.
11. Click **Apply**.

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. On the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select the AppConnect app configuration that you configured for the PIV-D Manager app for iOS.
3. Click **Edit**.
4. In the **App-specific Configurations** section, add the **case-sensitive** key-value pair:

Key	Value
disable_analytics	True

5. Click **Save**.

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 app configuration.

Procedure

1. On the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select the AppConnect app configuration that you configured for the PIV-D Manager app for iOS.
3. Click **Edit**.
4. In the **App-specific Configurations** section, add these **case-sensitive** key-value pairs:

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 c**auses 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.

5. Click **Save**.

Configuring a third-party iOS derived credential app

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 third-party iOS derived credential app to obtain derived credentials on a device after registering a device to MobileIron Core. A derived credential app can have app-specific configuration settings that require you to configure key-value pairs for the app in its AppConnect app configuration. The app vendor or developer describes these settings, if any, in the app's documentation.

When you configure these settings on Core, the derived credential app receives the values when the user launches the app on the device.

Procedure

1. On the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select **Add New > AppConnect > App Configuration.**
3. Enter a name for the AppConnect app configuration, such as **Derived credential app**.
4. Enter a description for the AppConnect app configuration.
5. In the **Application** field, enter the bundle ID of the app.
6. In the **App-specific Configurations** section, add the **case-sensitive** key-value pairs as specified by the app vendor.
7. Click **Save**.
8. Select the AppConnect app configuration that you just created.
9. Click **More Actions > Apply to Label**.
10. Select the labels to which you want to apply this policy.
11. Click **Apply**.

Configuring the PIV-D Manager app for Android

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Entrust
Device platforms	Android

A device user uses the MobileIron PIV-D Manager app to activate Entrust derived credentials on a device after registering a device to MobileIron Core. This capability requires you to configure a key-value pair for the PIV-D Manager app in its AppConnect app configuration. The value is a Core variable that contains the activation URL. Entrust provides the activation URL to Core when the user requests a derived credential on the self-service user portal. The PIV-D Manager app receives the value when the user launches the app on the device.

You can also configure a key-value pair containing a unique device identifier that the 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.

Note that Core automatically creates an AppConnect app configuration for the PIV-D Manager app for Android when you upload the app to the App Catalog. This procedure assumes you use that AppConnect app configuration.

Procedure

1. On the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select the AppConnect app configuration that Core automatically created for the PIV-D Manager app for Android. It has the name **PIV-D Manager app**, the configuration type is **APPCONFIG**, and the package name **forgepond.com.mobileiron.android.pivd.**
3. Click **Edit**.
4. In the **App-specific Configurations** section, add the **case-sensitive** key-value pairs:

Key	Value
Required key and value MI_CREDENTIAL_ACTIVATION_URL	$DEVICE_PIVD_ACTIVATION_LINK$
Optional key and value MI_CREDENTIAL_DEVICE_ID	A MobileIron Core substitution variable that uniquely identifies the device. Examples: $DEVICE_ID$ $DEVICE_UUID$ $DEVICE_IMSI$

5. Click **Save**.
6. Select the AppConnect app configuration that you just created.
7. Click **More Actions > Apply to Label**.
8. Select the labels to which you want to apply this policy.

Core already labeled it with the same labels you applied to the PIV-D Manager app for Android.

9. Click **Apply**.

Adding a derived credential provider

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any
Device platforms	iOS

On the Admin Portal, the screen at **Settings > System Settings > Security > Derived Credential Providers** provides a list of derived credential providers. You specify one of these providers in each client-provided certificate enrollment setting. The AppConnect app configuration for an AppConnect app points to a client-provided certificate enrollment setting in one of its key-value pairs. When Mobile@Work for iOS sends the derived credential certificates to the AppConnect app, it uses the certificates from the specified provider.

If you are using a derived credential provider that is not already listed at **Settings > Security > Derived Credential Providers**, add the provider.

Procedure

1. On the Admin Portal, go to **Settings > System Settings > Security > Derived Credential Providers**.
2. Click **Add+**.
3. Enter the name of the derived credential provider.
4. Click **Save**.

Note The Following:

To change the name of a derived credential provider that you added, do the following:

1. Delete the derived credential provider.
2. Add the derived credential provider with the new name.
3. Modify any client-provided certificate enrollment settings that used the old name to now use the new name.

Related topics

- Configuring the default derived credential provider
- Configuring client-provided certificate enrollment settings
- Multiple derived credential providers on an iOS device

Configuring the default derived credential provider

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any
Device platforms	iOS

You can specify your default derived credential provider. The provider you specify is automatically selected on each client-provided certificate enrollment setting that you create. However, you can select a provider other than the default on a setting.

Procedure

1. On the Admin Portal, go to **Settings > System Settings > Security > Derived Credential Providers**.
2. Click **Select as Default** next to the derived credential provider that you want to be the default selection on client-provided certificate enrollment settings.
3. Click **Confirm**.

Related topics

- Adding a derived credential provider
- Configuring client-provided certificate enrollment settings
- Multiple derived credential providers on an iOS device

Configuring client-provided certificate enrollment settings

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any
Device platforms	iOS, Android

A client-provided certificate enrollment setting is necessary for each of the purposes an app uses derived credentials. These purposes are authentication, signing, encryption, and, for iOS only, decryption. For each app using derived credentials, the app's AppConnect app configuration (or Web@Work setting or Docs@Work setting) refers to this certificate enrollment setting.

Procedure

1. On the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select **Add New > Certificate Enrollment > Client-Provided.**
3. Enter a name for the setting, such as **Derived Credential Authentication.**
4. Enter a description for the setting.
5. Select the purpose for the setting from the drop-down choices: **Authentication**, **Decryption**, **Encryption**, or **Signing**.

Decryption is only supported for iOS devices.

6. Select the appropriate derived credential provider from the drop-down choices.

   - This field is applicable only for iOS devices. It has no impact on Android devices.
   - If the selected derived credential provider is not available in Mobile@Work for iOS, the app becomes unauthorized.
   - Each app can use only one derived credential provider for each purpose.
7. Click **Save**.

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

Related topics

- Adding a derived credential provider
- Configuring the default derived credential provider
- Multiple derived credential providers on an iOS device

Configuring Web@Work to use derived credentials

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

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

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. Require a device password for iOS devices
2. Configure a Web@Work setting

Related topics

- *MobileIron Web@Work for iOS Guide for Administrators for MobileIron Core and MobileIron Cloud*
- *MobileIron Web@Work for Android Guide for Administrators for MobileIron Core and MobileIron Cloud*

Require 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. On the Admin Portal, go to **Policies & Configs > Policies**.
2. Select the security policy that applies to the devices that you want to run Web@Work for iOS.
3. Click **Edit**.
4. For the **Password** option, select **Mandatory**.
5. Fill in the remaining options relating to device passwords.
6. Click **Save**.
7. Click **OK**.
8. Repeat steps 2 through 6 for all security policies that apply to devices on which you want to run Web@Work for iOS.

Related topics

"Security Policies" in *Getting Started with MobileIron Core*.

Configure a Web@Work setting

Configure a Web@Work setting so that Web@Work uses derived credentials to authenticate to your websites.

Procedure

1. On the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select **Add New > Web@Work.**

Alternatively, edit an existing Web@Work setting if you have one already.

3. Enter a name for the Web@Work setting.
4. In the **Custom Configurations** section, add the following **case-sensitive** key-value pairs:

Key	Value
IdCertificate_1	Select a client-provided certificate enrollment setting from the drop-down list. The setting must have the purpose **Authentication**.
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	Select a client-provided certificate enrollment setting from the drop-down list. The setting must have the purpose **Authentication**.
IdCertificate_2_host	AnotherHost.mycompany.com
IdCertificate_3	Select a client-provided certificate enrollment setting from the drop-down list. The setting must have the purpose **Authentication**.
IdCertificate_3_host	YetAnotherHost.mycompany.com

5. Click **Save**.
6. Select the Web@Work setting that you just created.
7. Click **More Actions > Apply to Label**.
8. Select the labels to which you want to apply this policy.
9. Click **Apply**.

Related topics

- "Web@Work configuration" in the *MobileIron Web@Work for iOS Guide for Administrators for MobileIron Core and MobileIron Cloud*
- "Configuring a Web@Work configuration" in *MobileIron Web@Work for Android Guide for Administrators for MobileIron Core and MobileIron Cloud*

Configuring 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

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

- S/MIME signing
- S/MIME encryption
- S/MIME decryption of older emails (supported in Email+ 3.8 for iOS through the most recently released version as supported by MobileIron).
- Identifying and authenticating the email user to the email server

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

1. Providing special key-value pairs in the AppConnect app configuration
2. Uploading the root and issuer chain certificates
3. Referring to the root and issuer chain certificates in the AppConnect app configuration
4. Setting up MobileIron Tunnel if the Exchange server is behind your firewall (iOS only)

Related topics

- *MobileIron Email+ for iOS Guide for Administrators for MobileIron Core and MobileIron Cloud*
- *MobileIron Email+ for Android Guide for Administrators for Android AppConnect and Android enterprise for MobileIron Core and MobileIron Cloud*

Before you begin

- Set up the Microsoft Exchange server to accept certificate authentication.
- Have available for upload to MobileIron Core 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, or decrypt S/MIME emails. They allow Email+ on the devices handling the signed or encrypted email to trust the issuer chain certificates of the derived credentials.

Providing special key-value pairs in the AppConnect app configuration

Special key-value pairs are necessary in the AppConnect app configuration for Email+ if it is using derived credentials. Specifically:

- If device users will authenticate to the Exchange server with a derived credential's certificate:
  - Set the value of the key `email_exchange_host` to the Exchange server, **not** the Standalone Sentry, Therefore, you do not configure a Standalone Sentry for ActiveSync.
  - Set the value of the key `email_login_certificate` to a client-provided certificate enrollment setting from the drop-down list. The setting must have the purpose **Authentication**.
- If device users will sign S/MIME emails with a derived credential's certificate:
  - Set the value of the key `email_signing_certificate` to a client-provided certificate enrollment setting from the drop-down list. The setting must have the purpose **Signing**.
- If device users will encrypt S/MIME emails with a derived credential's certificate:

  - Set the value of the key `email_encryption_certificate` to a client-provided certificate enrollment setting from the drop-down list. The setting must have the purpose **Encryption**.
- If iOS device users will decrypt older S/MIME emails, for which the original certificate has expired, with a derived credential's certificate:
  - Set the value of the key `email_decryption_certificates` to a client-provided certificate enrollment setting from the drop-down list. The setting must have the purpose **Decryption**.

NOTE: The names of keys are case-sensitive.

Procedure

1. On the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select **Add New > AppConnect > App Configuration.**

Alternatively, edit the existing AppConnect app configuration for Email+ for iOS or Email+ for Android if you have one already.

3. Enter a name for the AppConnect app configuration, such as **Email+ for iOS** or **Email+ for Android**.
4. Enter a description for the AppConnect app configuration.
5. In the **Application** field:
   - For Email+ for iOS, enter **com.mobileiron.ios.emailplus**.
   - For Email+ for Android, select Email+ from the dropdown. It is listed because you added Email+ for Android to the MobileIron Core App Catalog.
6. In the **App-specific Configurations** section, add the key-value pairs listed above, plus other Email+ key-value pairs you require.
7. Click **Save**.
8. Select the AppConnect app configuration that you just created.
9. Click **More Actions > Apply to Label**.
10. Select the labels to which you want to apply this policy.
11. Click **Apply**.

Related topics

Adding AppConnect apps to the App Catalog

Uploading the root and issuer chain certificates

Provide a Certificates setting for the CA root certificate and each issue chain certificate if device users are using derived credentials for any of the following:

- S/MIME encryption
- S/MIME decryption of older emails for which the original encryption certificate has expired
- S/MIME signing

Procedure

1. In the Admin Portal, go to **Policies & Configs > Configuration > Add New > Certificates**.
2. Enter a **Name** and **Description** for the certificate.
3. Click **Browse** to select the certificate.
4. Click **Save**.

Referring to the root and issuer chain certificates in the AppConnect app configuration

Procedure

1. On the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select the AppConnect app configuration you created for Email+.
3. **Click Edit.**
4. In the **App-specific Configurations** section, add a key-value pair for the root certificate and each issuer chain certificate as follows:
   - Key: email_certificate_X, where X is 1 through 10
   - Value: Select the Certificates setting name from the drop-down list
5. Click **Save**.

Setting up MobileIron Tunnel if the Exchange server is behind your firewall (iOS only)

If the Exchange server is behind your firewall, use MobileIron Tunnel to tunnel to the Exchange server from mobile devices running Email+. Detailed information about setting up MobileIron Tunnel is available in the MobileIron Tunnel for iOS Guide for Administrators for MobileIron Core and MobileIron Cloud.

Configuring Docs@Work to use derived credentials

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

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

Docs@Work for iOS and Docs@Work for Android can use derived credentials to authenticate the device user to internal websites such as SharePoint sites.

Procedure

1. On the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select **Add New > Docs@Work.**

Alternatively, edit an existing Docs@Work setting if you have one already.

3. Enter a name for the Docs@Work setting.
4. In the **Custom Configurations** section, add the following **case-sensitive** key-value pairs:

Key	Value
IdCertificate_1	Select a client-provided certificate enrollment setting from the drop-down list. The setting must have the purpose **Authentication**.
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	Select a client-provided certificate enrollment setting from the drop-down list. The setting must have the purpose **Authentication**.
IdCertificate_2_host	AnotherHost.mycompany.com
IdCertificate_3	Select a client-provided certificate enrollment setting from the drop-down list. The setting must have the purpose **Authentication**.
IdCertificate_3_host	YetAnotherHost.mycompany.com

5. Click **Save**.
6. Select the Docs@Work setting that you just created.
7. Click **More Actions > Apply to Label**.
8. Select the labels to which you want to apply this Docs@Work setting.
9. Click **Apply**.

Related topics

- The *MobileIron Docs@Work for iOS Guide*
- The *MobileIron Docs@Work for Android Guide*

Configuring AppConnect apps to use derived credentials

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

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

Use cases for derived certificates in AppConnect apps

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

- The app can receive certificates that it expects in its app-specific app configuration. The app developer or vendor provides you the a list of key-value pairs, which you configure in the app's AppConnect app configuration on the MobileIron Core Admin Portal.
- **iOS only:** 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.

Configuring an AppConnect app configuration for the AppConnect app

Configure an AppConnect app configuration so that the AppConnect app uses derived credentials. Follow the procedure for iOS AppConnect apps or Android AppConnect apps.

Procedure for iOS AppConnect apps

1. On the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select **Add New > AppConnect > App Configuration.**

Alternatively, edit an existing AppConnect app configuration for the AppConnect app if you have one already.

3. Enter a name for the AppConnect app configuration.
4. Enter a description for the AppConnect app configuration.
5. In the **Application** field:
   enter the case-sensitive bundle ID for the AppConnect app.
   - For iOS AppConnect apps, enter the case-sensitive bundle ID for the AppConnect app.
   - For Android AppConnect apps, select the app from the dropdown. It is listed because you added it to the MobileIron Core App Catalog.
6. In the **App-specific Configurations** section:
   a. If the app expects key-value pairs for which the value is a certificate from a derived credential, add the following **case-sensitive** keys and their values:

Key	Value
<app-specific key name> NOTE: The app developer or vendor provides you the app-specific key name.	Select a client-provided certificate enrollment setting from the drop-down list. The setting must have the purpose (Authentication, Signing, Encryption, or Decryption) appropriate for this app-specific key. Depending on the selected setting, Mobile@Work delivers the corresponding certificate from the derived credential to the app. For the Decryption purpose, Mobile@Work delivers a list of certificates.

b. If you are using the AppConnect feature that causes the AppConnect library within the app to handle certificate authentication to an enterprise service, add the following **case-sensitive** key-value pairs:

Key	Value
MI_AC_CLIENT_CERT_1	Select a client-provided certificate enrollment setting from the drop-down list. The setting must have the purpose **Authentication**.
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

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

Key	Value
MI_AC_CLIENT_CERT_2	Select a client-provided certificate enrollment setting from the drop-down list. The setting must have the purpose **Authentication**.
MI_AC_CLIENT_CERT_2_RULE	myOtherServer.mycompany.com
MI_AC_CLIENT_CERT_3	Select a client-provided certificate enrollment setting from the drop-down list. The setting must have the purpose **Authentication**.
MI_AC_CLIENT_CERT_3_RULE	YetAnotherServer.mycompany.com

7. Click **Save**.

8. Select the AppConnect app configuration that you just created.
9. Click **More Actions > Apply to Label**.
10. Select the labels to which you want to apply this policy.
11. Click **Apply**.

Procedure for Android AppConnect apps

Note that Core automatically creates an AppConnect app configuration for an AppConnect app for Android when you upload the app to the App Catalog. This procedure assumes you use that AppConnect app configuration.

1. On the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select the AppConnect app configuration that Core automatically created for the app. It has the configuration type is **APPCONFIG.**
3. Click **Edit**.
4. In the **App-specific Configurations** section, add the following **case-sensitive** keys and their values to support the use of derived credentials:

Key	Value
<app-specific key name> NOTE: The app developer or vendor provides you the app-specific key name.	Select a client-provided certificate enrollment setting from the drop-down list. The setting must have the purpose (Authentication, Signing, or Encryption) appropriate for this app-specific key. Depending on the selected setting, the Secure Apps manager delivers the corresponding certificate from the derived credential to the app.

5. Click **Save**.
6. Select the AppConnect app configuration that you just created.
7. Click **More Actions > Apply to Label**.
8. Select the labels to which you want to apply this policy.

Core already labeled it with the same labels you applied to the app.

9. Click **Apply**.

Related topics

In the *MobileIron Core AppConnect and AppTunnel Guide:*

- “Configuring an AppConnect app configuration”
- “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

Configuring AppTunnel to use derived credentials on iOS devices

APPLICABLE DERIVED CREDENTIAL PROVIDERS AND DEVICE PLATFORMS

Derived credential providers	Any
Device platforms	iOS

You can configure these AppTunnel scenarios to use derived credentials on iOS devices:

- Configuring AppTunnel with HTTP/S tunneling to use derived credentials
- Configuring the MobileIron Tunnel app to use derived credentials

Configuring AppTunnel with HTTP/S tunneling to use derived credentials

NOTE: This use of derived credentials is supported only on iOS devices.

When using AppTunnel with HTTP/S tunneling, you can use Kerberos authentication to the backend resource. In this scenario, you authenticate the iOS device to the Standalone Sentry using a certificate that identifies the user, not just the device. This identity certificate can be a derived credential.

Procedure

1. Follow the instructions in the *MobileIron Sentry Guide* to set up Standalone Sentry for AppTunnel with HTTP/S tunneling and Kerberos authentication.
2. Follow the instructions in the *MobileIron Core AppConnect and AppTunnel Guide* to set up the AppConnect app to use AppTunnel.
3. In the **AppTunnel Rules** section in the app's AppConnect app configuration (or Web@Work setting or Docs@Work setting), for the **Identity Certificate** field, select a client-provided certificate enrollment setting from the drop-down list. The setting must have the purpose **Authentication**.

Configuring the MobileIron Tunnel app to use derived credentials

NOTE: This use of derived credentials is supported only on iOS devices.

When using the MobileIron Tunnel app (AppTunnel with TCP tunneling) with iOS devices, you can authenticate the device user to a backend or web resource using a derived credential. This identity certificate can be a derived credential.

Procedure

1. Follow the instructions in the MobileIron Tunnel for iOS Guide for Administrators for MobileIron Core and MobileIron Cloud to set up TCP tunneling for the AppConnect app.
2. For Web@Work, in the Web@Work setting, set up the key-value pairs for certificate authentication.
   See Configuring Web@Work to use derived credentials.
3. For Docs@Work, in the Docs@Work setting, set up the key-value pairs for certificate authentication.
   See Configuring Docs@Work to use derived credentials.
4. For a third-party or in-house AppConnect app, in the AppConnect app configuration, set up the key-value pairs for certificate authentication.
   See Configuring AppConnect apps to use derived credentials.

Device User Experience with Entrust

When using derived credentials from Entrust, the device user does the following tasks:

- Setting up Entrust derived credentials during registration
- Setting up Entrust derived credentials after registration
- Managing Entrust derived credentials on iOS devices
- Managing derived credentials on Android devices
- Using Bluetooth for Entrust derived credential authentication on Windows
- Using Entrust for push notification authentication to enterprise servers (iOS only)

Setting up Entrust derived credentials during registration

When device users register their devices with MobileIron Core, they can set up Entrust 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 user portal with a smart card
- Generating the one-time registration PIN
- Requesting an Entrust derived credential
- Installing Mobile@Work
- Registering Mobile@Work for iOS
- Registering Mobile@Work for Android and installing Android AppConnect apps
- Installing the PIV-D Manager app for iOS
- Activating the Entrust derived credential requested on the user portal
- Installing AppConnect apps for iOS
- Running AppConnect apps for iOS
- Running AppConnect apps for Android

Authenticating to the user portal with a smart card

A device user authenticates to the user portal with a smart card. This procedure is supported only on desktop computers. It is not supported with:

- mobile devices
- Firefox

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 https://<*Your MobileIron Core domain*>.
   For example: https://core.mycompany.com
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 user portal, a device user generates a one-time registration PIN on the user portal.

Procedure

1. Click **Request Registration PIN**.
   A form called **Request Registration PIN** displays.
2. For **Platform**, select **iOS** or **Android**, depending on the device.
3. Fill in the remaining required fields.
4. Click **Request PIN**.
   A registration PIN displays along with the user name.
5. Copy the registration PIN and user name to enter later into Mobile@Work on the device.

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

Requesting an Entrust derived credential

After the device user has generating the one-time registration PIN, the device user must request an Entrust derived credential *before* registering the device.

To request an Entrust derived credential, the device user continues on the self-service user portal on the screen that confirms that the registration PIN was successfully generated.

Procedure

1. Click **Request Derived Credential**.
   The user portal redirects the browser to the Entrust.IdentityGuard Self-Service Module, which requests the user to enter their smart card's PIN 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.
   Important:
   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 Core self-service user portal.
   The Entrust Identity Guard Self-Service Module redirects the browser back to the MobileIron Core self-service user portal.

About an Entrust derived credential requested from the user portal

An Entrust 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). Furthermore, the derived credential that is requested from the self-service user portal is associated with the registration PIN just generated. Therefore, consider these scenarios:

- The Entrust 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 Entrust 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 Mobile@Work

Instruct your device users to install the Mobile@Work for iOS app or Mobile@Work for Android app on their devices. Typically, device users download the iOS app from the Apple App Store, and the Android app from Google Play. However, if your environment provides Mobile@Work for iOS through the MobileIron Core App Catalog, instruct the device users appropriately.

Registering Mobile@Work for iOS

The device user registers Mobile@Work for iOS to MobileIron Core using the one-time registration PIN that the device user generated on the user portal. The device user must also have requested an Entrust derived credential on the user portal.

Procedure

1. Launch Mobile@Work on the device.
2. Enter the user name.
3. Enter the MobileIron Core address
   For example: core.mycompany.com
4. Enter the one-time registration PIN generated from the user portal.
5. Tap **Register**.
6. Follow the Mobile@Work instructions to complete registration.

Registering Mobile@Work for Android and installing Android AppConnect apps

The device user registers Mobile@Work for Android to MobileIron Core using the one-time registration PIN that the device user generated on the user portal. The device user must also have requested an Entrust derived credential on the user portal.

The registration process concludes with:

- Installing the Secure Apps Manager, the PIV-D Manager app, and any other mandatory AppConnect apps that you have assigned to this device.
  Because these apps are specified as mandatory apps in the MobileIron Core App Catalog, they are all installed.
- Creating the secure apps passcode.

Procedure

1. Launch Mobile@Work on the device.
2. Enter your email address or tap **Or register with server URL** to enter the MobileIron Core address, such as core.mycompany.com.
3. Tap **Next**.
4. If prompted, accept the certificate.
5. Tap **Continue** on the screen about privacy.
6. Enter the one-time registration PIN generated from the user portal.
7. Tap **Sign In**.

8. Follow the Mobile@Work instructions to complete its setup, leading you to the screen for setting up the Secure Apps Manager.
9. Tap **Continue**.
10. Tap **Begin** to install the Secure Apps Manager, the PIV-D Manager app, and any other mandatory AppConnect apps that you have assigned to this device.
11. Follow the instructions to install the apps.
    After the installations complete, the **Passcode Setup** screen displays.
12. Enter a new secure apps passcode.
13. Enter the secure apps passcode again.
14. Tap the checkmark.

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 Entrust derived credential that they requested when they requested the MobileIron Core registration PIN. Device users can also use the app to request new Entrust derived credentials after they have already registered the device.

Procedure

1. Launch Apps@Work 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 user portal

The device user activates the Entrust derived credential that they requested on the MobileIron Core self-service user portal.

- Activating the Entrust derived credential on iOS devices
- Activating the Entrust derived credential on Android devices

Activating the Entrust derived credential on iOS devices

Procedure

1. Launch the PIV-D Manager app for iOS.
   The app switches control to Mobile@Work, which prompts the device user to create a secure apps passcode.
2. Follow the Mobile@Work 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 Android devices

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 Apps@Work for iOS on the device.
2. Tap the listing for the AppConnect app.
3. Tap **Request**.
4. 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 Mobile@Work.The app then receives the Entrust derived credential from Mobile@Work.

NOTE: If an AppConnect app expects certificates from a derived credential but the derived credential is not available in Mobile@Work, 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, 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 Entrust 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 Entrust 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
- Getting Entrust derived credentials on the device

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 on Android or the PIV-D Manager app on iOS.
6. Provide a name for the new derived credential identity.
   On iOS devices, Mobile@Work 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 on the device

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

- Getting Entrust derived credentials on an iOS device
- Getting Entrust derived credentials on an Android device

Getting Entrust derived credentials on an iOS 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.
2. If this is the first time you launch an AppConnect app on the device, follow the Mobile@Work instructions to create a secure apps passcode.
   After you create the secure apps passcode, control returns to the PIV-D Manager app.
3. Tap on **Entrust IdentityGuard**.
   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.
4. Tap **OK** if you are prompted to allow the PIV-D Manager app to access the camera.
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, 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.
9. Enter a new derived credential PIN and enter it again to confirm it.
10. Tap **Done**.
    The app displays that the derived credential has been successfully activated.
11. 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 on an Android 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 Mobile@Work for iOS, you can:

- View an Entrust derived credential.
- Delete an Entrust 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 Entrust derived credential.
  This action replaces the existing derived credential.

Viewing an Entrust derived credential on iOS devices

Procedure

1. In Mobile@Work, tap **Settings**.
2. Tap **Entrust Credential**.
   Mobile@Work 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 Mobile@Work, 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 Mobile@Work, tap **Settings**.
2. Tap **Entrust Credential**.
   Mobile@Work 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 derived credential replaces the existing derived credential.

Procedure

1. Follow the instructions in Getting a QR code and Entrust activation password.
2. In Mobile@Work, 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, Mobile@Work launches and displays the derived credential.

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

Managing derived credentials on Android devices

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

- View an Entrust derived credential.
- Delete an Entrust 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 Entrust 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.
   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.
   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 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.
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 the PIV-D Manager app 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 for iOS or PIV-D Manager app for Android, 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: Uf 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.

The derived credential PIN on Android devices

On Android devices running the PIV-D Manager app, 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 Entrust 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 Android devices
- Resetting the derived credential PIN on Android devices
- "Activating the Entrust derived credential on Android devices" in Setting up Entrust derived credentials during registration
- "Getting Entrust derived credentials on an Android device" in Setting up Entrust derived credentials after registration

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.
   After entering the derived credential PIN, you are logged into the Windows 10 computer.

Related topics

About the derived credential PIN

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.
   After entering the derived credential PIN, you are logged into the protected website.

Related topics

About the derived credential PIN

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 Android 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

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.

Related topics

About the derived credential PIN

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 Android devices

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 your derived credential PIN.
5. Tap **Done**.

Related topics

About the derived credential PIN

Resetting the derived credential PIN on Android devices

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.

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

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 Android 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 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 connecting 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 Mobile@Work 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 Core.
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

When using derived credentials from DISA Purebred on an iOS device, the device user does the following tasks:

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

NOTE: MobileIron does not support DISA Purebred credentials on Android devices.

Setting up Purebred derived credentials on iOS devices

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

- Authenticating to the user portal with a smart card
- Generating the one-time registration PIN
- Installing Mobile@Work for iOS
- Registering Mobile@Work 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 user portal with a smart card

A device user authenticates to the user portal with a smart card. This procedure is supported only on desktop computers. It is not supported with:

- mobile devices
- Firefox

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 https://<*Your MobileIron Core domain*>.
   For example: https://core.mycompany.com
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 user portal, a device user generates a one-time registration PIN on the user portal.

Procedure

1. Click **Request Registration PIN**.
   A form called **Request Registration PIN** displays.
2. For **Platform**, select **iOS**.
3. Fill in the remaining required fields.
4. Click **Request PIN**.
   A registration PIN displays along with the user name.
5. Copy the registration PIN and user name to enter later into Mobile@Work on the device.

Installing Mobile@Work for iOS

Instruct your device users to install the Mobile@Work for iOS app on their devices. Typically, device users download the app from the Apple App Store. However, if your environment provides Mobile@Work for iOS through the MobileIron Core App Catalog, instruct the device users appropriately.

Registering Mobile@Work for iOS

The device user registers Mobile@Work for iOS to MobileIron Core using the one-time registration PIN that the device user generated on the user portal.

Procedure

1. Launch Mobile@Work on the device.
2. Enter the user name.
3. Enter the MobileIron Core address
   For example: core.mycompany.com
4. Enter the one-time registration PIN generated from the user portal.
5. Tap **Register**.
6. Follow the Mobile@Work 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 Mobile@Work 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 Mobile@Work for iOS.

Procedure

1. Launch Apps@Work 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, encryption, and decryption certificates, and then sends all the certificates to Mobile@Work for iOS. These certificates overwrite any existing DISA Purebred derived credential certificates that the PIV-D Manager had previously sent to Mobile@Work.

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 Mobile@Work, which prompts the device user to create a secure apps passcode.
4. Follow the Mobile@Work 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 Mobile@Work.

Installing AppConnect apps for iOS

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

Procedure

1. Launch Apps@Work for iOS on the device.
2. Tap the listing for the AppConnect app.
3. Tap **Request**.
4. 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 Mobile@Work.The app then receives the derived credential from Mobile@Work.

NOTE: If an AppConnect app expects certificates from a derived credential but the derived credential is not available in Mobile@Work, 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 Mobile@Work 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 Mobile@Work, tap **Settings**.
2. Tap **Purebred Credential**.
   Mobile@Work 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 Mobile@Work, 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 Mobile@Work, tap **Settings**.
2. Tap **Purebred Credential**.
   Mobile@Work 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 Mobile@Work replaces the existing derived credential in Mobile@Work.

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 Mobile@Work, 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 Mobile@Work..

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, encryption. and decryption certificates) from the DISA Purebred Registration app. Then the PIV-D Manager app sends all the selected certificates to Mobile@Work for iOS.

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

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

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

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

Setting up derived credentials on iOS devices

The device user does the following tasks as part of the derived credential setup process:

- Authenticating to the user portal with a smart card
- Generating the one-time registration PIN
- Installing Mobile@Work for iOS
- Registering Mobile@Work for iOS
- Installing the derived credential app
- Installing AppConnect apps for iOS
- Running AppConnect apps for iOS

Authenticating to the user portal with a smart card

A device user authenticates to the user portal with a smart card. This procedure is supported only on desktop computers. It is not supported with:

- mobile devices
- Firefox

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 https://<*Your MobileIron Core domain*>.
   For example: https://core.mycompany.com
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 user portal, a device user generates a one-time registration PIN on the user portal.

Procedure

1. Click **Request Registration PIN**.
   A form called **Request Registration PIN** displays.
2. For **Platform**, select **iOS**.
3. Fill in the remaining required fields.
4. Click **Request PIN**.
   A registration PIN displays along with the user name.
5. Copy the registration PIN and user name to enter later into Mobile@Work on the device.

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

Installing Mobile@Work for iOS

Instruct your device users to install the Mobile@Work for iOS app on their devices. Typically, device users download the app from the Apple App Store. However, if your environment provides Mobile@Work for iOS through the MobileIron Core App Catalog, instruct the device users appropriately.

Registering Mobile@Work for iOS

The device user registers Mobile@Work for iOS to MobileIron Core using the one-time registration PIN that the device user generated on the user portal.

Procedure

1. Launch Mobile@Work for iOS on the device.
2. Enter the user name.
3. Enter the MobileIron Core address
   For example: core.mycompany.com
4. Enter the one-time registration PIN generated from the user portal.
5. Tap **Register**.
6. Follow the Mobile@Work instructions to complete registration.

Installing the derived credential app

The device user installs the derived credential app that obtains derived credentials 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 Apps@Work 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 for iOS

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

Procedure

1. Launch Apps@Work for iOS on the device.
2. Tap the listing for the AppConnect app.
3. Tap **Request**.
4. 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 Mobile@Work.The app then receives the derived credential from Mobile@Work.

NOTE: If an AppConnect app expects certificates from a derived credential but the derived credential is not available in Mobile@Work, 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 Mobile@Work 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 a derived credential on iOS devices

Procedure

1. In Mobile@Work, tap **Settings**.
2. Tap the credential setting.
   Mobile@Work displays the credential's information.

Deleting a 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 Mobile@Work, tap **Settings**.
2. Tap the credential setting
   Mobile@Work displays the credential's information.
3. Click the trash icon in the upper right hand corner.
4. Click **Delete**.

Getting a new derived credential on iOS devices

Getting a new derived credential replaces the existing derived credential.

Procedure

1. In Mobile@Work, 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.