AirWatch®MDM ソリューション向け

DigiCert® 統合ガイド

2015 年 9 月 15 日版

digicert®

AirWatch® MDM ソリューション向け DigiCert® 統合ガイド

本書で説明するソフトウェアはライセンス契約のもとで提供され、ご使用の際には契約条項に従っていただく必要があります。

文書作成日 : 2015 年 9 月 15 日

法的通知

デジサート・ジャパン合同会社

〒 104-0061
東京都中央区銀座 6 丁目 10 番地 1 号
GINZA SIX 8 階
03-4560-3900
https://www.digicert.co.jp
JPN-DIV-MPKI@digicert.com

目次

第 1 章

DigiCert PKI 証明書と AirWatch MDM ソリューションの統合

企業の職場環境は、それぞれの組織の壁を越えてグローバルなモバイル環境へと移行しました。エンドユーザーの生産性を維持するためには、モバイルプラットフォームから企業リソースへのアクセスが必要です。一方で企業は、社内システムにアクセスするエンドユーザーと、ユーザーが使用するモバイルデバイス（会社支給か個人所有かは問いません）を信頼できなければなりません。

DigiCert PKI Platform の電子証明書は、ユーザー名とパスワードの入力やハードウェアトークンの追加導入を必要とせずに、この信頼を実現できます。DigiCert PKI Platform はスケーラブルに、数台から数千台ものデバイスに対応します。また、クラウドソリューションなので、短期間で導入し、容易に管理することができます。その上、先進のセキュリティがついているため、内製の PKI ソリューションとは比較になりません。

本書は、MDM ベンダーとして AirWatch を選択されたお客様を対象としています。本書では、Web サービスまたは Simple Certificate Enrollment Protocol（SCEP）を使用して、Client Authentication、セキュアメール（S/MIME）、MDM をサポートするエンドエンティティ証明書をモバイルデバイスに発行するための DigiCert PKI Platform の設定方法について説明します。これらの証明書をユーザーに提供するための AirWatch MDM ソリューションの設定手順については、『AirWatch Integration with DigiCert PKI Guide』を参照してください。このガイドは AirWatch または https://knowledge.digicert.com/generalinformation/INFO3433.html から入手可能です。

パートナー情報

この統合のサポート対象は、DigiCert PKI Platform 8.x と次のパートナープラットフォームです。

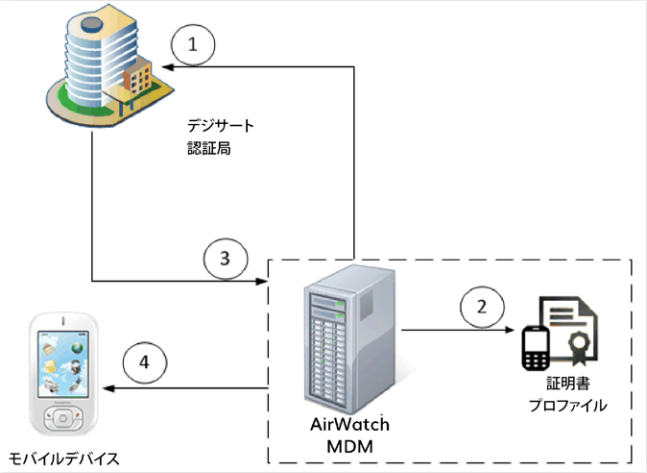
表 1-1 パートナー情報

パートナー名	AirWatch®
製品名	AirWatch® MDM ソリューション 6.0 以降
デバイス（証明書の申請およびインストール対象）	iOS、Android

統合アーキテクチャ

次の図をもとに、AirWatch MDM ソリューションと DigiCert PKI Platform の統合の仕組みについて説明します。

図 1-1 AirWatch MDM と DigiCert PKI Platform の通信



1. AirWatch MDM は、デジサート認証局と通信して RA 証明書を生成します。

2. DigiCert PKI Platform 8.x で作成されたプロファイルに対応する証明書テンプレートを作成します。
3. ActiveSync、VPN、または Wi-Fi のペイロードを設定するために、PKI または SCEP を使用してデジサートの認証局から証明書を取得します。
4. AirWatch MDM は、モバイルデバイスに証明書プロファイルを配布します。

前提条件

- AirWatch MDM ソリューションから接続する前に、DigiCert PKI Platform で証明書プロファイルを少なくとも 1 つ設定する必要があります。
- 本書に記載する手順は、DigiCert PKI Platform 8.x アカウントおよび AirWatch MDM ソリューション 6.0 にアクセスできることを前提としています。

統合のワークフロー

次の図をもとに、DigiCert PKI アカウントをセットアップし、DigiCert PKI 証明書と AirWatch MDM を統合するために必要な一般手順を説明します。

図 1-2 DigiCert PKI Platform と AirWatch の統合ワークフロー

作業 1. DigiCert PKI Platform 8.x アカウントをセットアップする

デジサートの営業担当者に連絡して、DigiCert PKI アカウントをセットアップします。担当者から、お客様のアカウントおよび証明書プロファイルの定義に必要な情報が提供されます。

以下の文書に必要な情報をすべて入力し、返送してください。必要に応じて、デジサートの担当者がフォームの取得と入力をお手伝いします。

- 基本契約書
- CA ネーミングドキュメント
- カスタマープロビジョニングフォーム (CPF)
- 注文書、クレジットカード、またはリファレンス番号

最初の DigiCert PKI 管理者 ID を取得する必要があります。これが、組織の DigiCert PKI アカウントにアクセスするためのクレデンシャルとなります。DigiCert PKI 管理者 ID の取得は、デジサートの担当者がお手伝いします。お客様が DigiCert PKI 管理者 ID を使用して DigiCert PKI Manager にログインし、DigiCert PKI アカウントを設定し、RA 証明書を取得します。DigiCert PKI Platform の設定の詳細については、DigiCert PKI Manager とそのオンラインヘルプを参照してください。

作業 2. DigiCert PKI Platform を使用して RA 証明書を生成する

AirWatch MDM が DigiCert PKI Platform と通信するには、RA 証明書を生成する必要があります。

1. 任意のローカルマシン上で、証明書署名リクエスト (CSR) を生成します。CSR を生成する手順は、オペレーティングシステムによって異なります。
   - Windows で CSR を生成する方法については、http://support.microsoft.com/kb/295281 を参照してください。
   - Linux で CSR を生成する方法については、http://www.trustis.com/pki/fpsia/guide/ssl-server/csr/apache_redhat.htm を参照してください。
   - Mac で CSR を生成する方法については、http://support.apple.com/kb/HT3976 を参照してください。

2. CSR が生成されたら、CSR をローカルマシンに保存します。

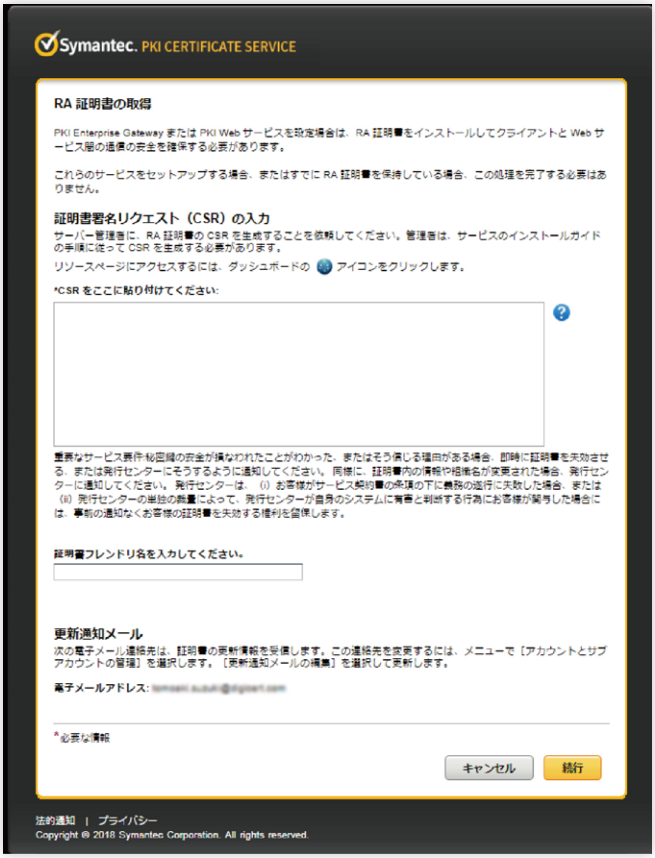
3. 管理者証明書を使用して、DigiCert PKI Platform の DigiCert PKI Manager にログインします。DigiCert PKI Client の PIN を入力するように要求されます。

4. DigiCert PKI Manager の最下部にあるナビゲーションバーで[タスク]メニューをクリックし、展開されたメニューから**[RA 証明書の取得]**を選択します。

図 1-3 RA 証明書の取得

5. 手順 1 で生成した CSR を**[証明書署名リクエスト(CSR)の入力]**テキストボックスに貼り付けます。

図 1-4 CSR の貼り付け



6. **[続行]**をクリックし、.cer ファイルを生成します。

7. 指示に従って RA 証明書を生成し、その証明書を .pfx ファイルとしてエクスポートします。

8. この .pfx ファイルが、AirWatch MDM が DigiCert PKI Platform 8.x との通信に使用する RA 証明書です。RA のインストールの詳細については、『AirWatch Integration with DigiCert PKI Guide』を参照してください。このガイドは AirWatch から入手可能です。

DigiCert PKI 証明書プロファイルを作成する

証明書プロファイルは、DigiCert PKI Platform の DigiCert PKI Manager で作成します。証明書プロファイルは、エンドユーザーに発行される証明書のタイプを定義するものです。発行された証明書は、任意のサポート対象モバイルデバイスで使用できます。DigiCert PKI Platform 8.x は、次の証明書タイプでテスト済みです。

- Client Authentication - VPN や Web サイトなどの企業リソースに対してユーザーを認証し、通信のセキュリティ保護に使用できる証明書を発行します。
- セキュアメール（S/MIME） - S/MIME によるメールのデジタル署名や認証に使用できる証明書を発行します。セキュアメールプロファイルでは、デフォルトで［鍵預託］オプションがサポートされています。このオプションを選択すると、証明書の生成および発行時に証明書の秘密鍵が自動でバックアップされます。AirWatch MDM ソリューションはキーリカバリ鍵管理要求もサポートしています。
- MDM - VPN や Web サイトなどの企業リソースに対してユーザーを認証し、通信のセキュリティ保護に使用できる証明書をモバイルデバイスに発行します。

公開される証明書の数を減らすため、複数のペイロードで 1 つの証明書プロファイルを使用することをお勧めします。

DigiCert PKI Platform の証明書プロファイルを作成するには、次の手順に従ってください。

9. 管理者証明書を使用して、DigiCert PKI Manager にログインします。DigiCert PKI Client の PIN を入力するように要求されます。
10. DigiCert PKI Manager の最下部にあるナビゲーションバーで、**[証明書プロファイルの管理]**をクリックするか、［タスク］メニューから**[証明書プロファイルの管理]**を選択します。

図 1-5 証明書プロファイルの管理

11. 表示される［証明書プロファイルの管理］ページの最上部にある**[証明書プロファイルの追加]**をクリックします。
12. これらの証明書をテストモードと本番モードのどちらで発行するかを選択し、**[続行]**をクリックします。
13. プロファイルのタイプと証明書のニーズに基づいて、残りの証明書プロファイルを設定します。**表 1-2** に、いくつかのガイドラインを示します。

表 1-2 証明書プロファイルのオプション

証明書プロファイルテンプレートの種類	オプション	値
Client Authentication	証明書テンプレート	Client Authentication
	申請方法	• PKI Certificate Service に代わり、ユーザー向けに独自の証明書管理アプリケーションを開発する場合は、**[PKI Web サービス]** を選択します。 • ユーザーが SCEP を使用して証明書の申請を行う場合は、**[SCEP]** を選択します。
	認証方法	• 申請方法が [PKI Web サービス] の場合、認証方法は **[サードパーティのアプリケーション]** になります。 • 申請方法が [SCEP] の場合、認証方法は **[申請コード]** になります。
Secure Email (S/MIME)	証明書テンプレート	Secure Email
	申請方法	• ユーザーがブラウザを使用して証明書の申請を行う場合は、**[OS/ ブラウザ]** を選択します。 • ユーザーが DigiCert PKI Client を使用して証明書申請を行う場合は、**[PKI Client]** を選択します。 • ユーザーがサードパーティのアプリケーションを使用して証明書の申請を行う場合は、**[PKI Web サービス]** を選択します。
	認証方法	• 申請方法が [PKI Web サービス] の場合、認証方法は **[サードパーティのアプリケーション]** になります。 • 申請方法が [PKI Client] または [OS/browser (OS/ブラウザ)] の場合、認証方法は **[Active Directory]** になります。
MDM	証明書テンプレート	MDM
	申請方法	SCEP
	認証方法	申請コード

14. **[詳細オプション]** をクリックして証明書のオプションを表示し、必要に応じて追加の属性を定義します。
Secure Email プロファイルの [鍵預託] オプションは、[追加の証明書オプション] で選択できます。

図 1-6 Secure Email プロファイルの鍵預託

15. **[保存]**をクリックします。

確認ページで、シート ID に使用される属性を確認できます。これは AirWatch の設定で必須の属性です。また、カスタムスクリプトの追加、言語やメール通知のカスタマイズなど、このページでプロファイルをさらにカスタマイズすることもできます。

iOS デバイスのデバイス ID 証明書

iOS デバイスの設定をプロビジョニングする方法はいくつかあります。これらの設定をセキュアに暗号化するにはクライアント認証証明書が必要であり、これらの設定を復号化するにはデバイス証明書が必要です。MDM 製品はデバイス ID 証明書を使用して、これらの設定の暗号化と復号化を行います。

実際のプロファイル（Client Authentication や Secure Email (S/MIME) など）をユーザーの意図したデバイスに配布するため、MDM プロファイルによって、特定のデバイス用にカスタマイズされたプロファイルが送信されます。環境によっては、企業の設定やポリシーがセキュアに保護されていることを確認することが重要です。iOS ではこの保護を実現するため、プロファイルを暗号化し、意図した 1 つのデバイスでしか読み取れないようにすることができます。暗号化されたプロファイルは、設定プロファイルのペイロードがデバイスの X.509 ID に関連付けられた公開鍵で暗号化されている点を除けば、通常の、設定プロファイルと酷似しています。

デバイス証明書の申請を行う前に、必ず MDM タイプのプロファイルを作成してください。MDM 証明書の詳細については、8 ページの**表 1-2「証明書プロファイルのオプション」**を参照してください。

第 2 章

AirWatch MDM を DigiCert PKI Platform 8.x 用に設定する

AirWatch MDM ソリューションを DigiCert PKI Platform 8.x と統合するには、次の手順に従ってください。

- AirWatch を DigiCert PKI 認証局と統合します。
- AirWatch から配布される証明書テンプレートを設定します。
- AirWatch からユーザーのデバイスに証明書プロファイルを配布します。

これらの手順の実行方法の詳細については、『AirWatch Integration with DigiCert PKI Guide』を参照してください。このガイドは AirWatch または https://knowledge.digicert.com/generalinformation/INFO3433.html から入手可能です。