JCCH・セキュリティ・ソリューション・システムズ

プライベート認証局Gléas ホワイトペーパー

MobileIron Cloudと連携したクライアント証明書配布

Ver.1.2
2019 年 6 月

目次

1. はじめに

1.1. 本書について

本書では弊社製品「プライベート認証局Gléas」と、MobileIron社のMDM/EMM「MobileIron Cloud」を連携させ、MobileIron Cloudに加入したデバイスに、自動的にGléasのクライアント証明書を配布する環境の設定例を記載します。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あらゆる環境での動作を保証するものではありません。弊社製品を用いたシステム構築の一例として、ご参照いただけますようお願いいたします。

弊社では試験用証明書の提供も行っております。検証などで必要な場合は、最終項のお問い合わせ先までお気軽にご連絡ください。

1.2. 本書における環境

本書における手順は、以下の環境で動作確認を行っています。

- MobileIron Cloud（Platinum バージョンR54）
  ※以下「MobileIron」と記載します
- 中継用サーバ MobileIron Cloud Connector（バージョン54.0.0.69）
  ※以下「Connector」と記載します
- JS3 プライベート認証局Gléas （バージョン1.16.9）
  ※以下「Gléas」と記載します
- クライアント：Dell XPS 12 (Windows 10 Pro)
  ：iPhone 6S+（iOS 11.4）
  ：mac mini Late 2012（macOS High Sierra）
  ：Nexus 9（Android 7.1.1）
  ※それぞれ以下「Windows」「iOS」「macOS」「Android」と記載します

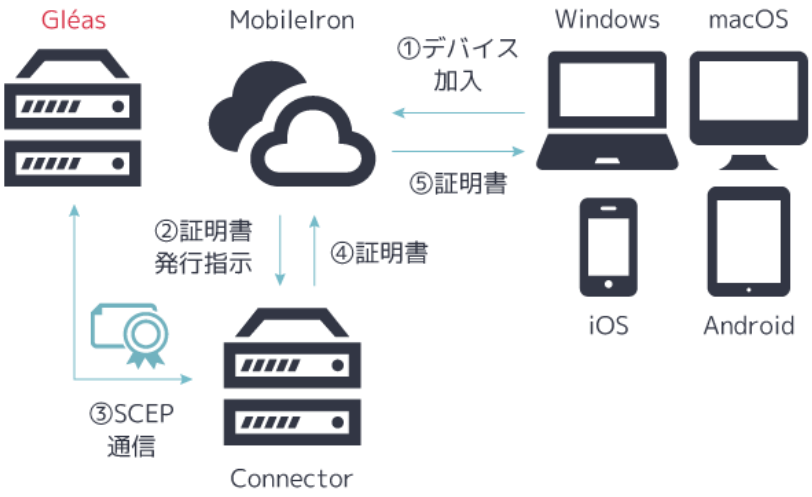
以下については、本書では説明を割愛します。

- MobileIronの基本設定
- Connectorの基本設定
- Gléasの基本設定
- クライアントの基本設定

これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている販売店にお問い合わせください。

1.3. 本書における構成

本書では、以下の構成で検証を行っています。



1. クライアントがMobileIronへデバイス加入をすると、MobileIronはConnectorを経由して連携設定をされたGléasへSCEPによる証明書発行要求をする。
2. GléasはMobileIron（Connector）からのSCEP要求に対し、クライアント証明書を発行し、証明書はMobileIronからクライアントへプッシュ配信される。

2. Gléasの設定

2.1. SCEP サーバの利用開始設定

SCEP 通信には専用の電子署名用証明書が必要になるので、事前に Gléas より SCEP サーバに利用する証明書を発行し、ファイルダウンロードしておきます。
RA で上部の[認証局] > [デフォルト登録局]をクリックします。

登録局詳細の「▶SCEP の設定」で、以下設定をおこないます。

- SCEP 用の証明書をアップロードする
- [静的チャレンジを利用する]にチェックを入れ、チャレンジ値を入力する
  ※チャレンジ値は MobileIron にも設定します
- [接続を許可するネットワーク]に、”ネットワークアドレス/ネットマスク”の形式で、Connector のネットワーク情報を入力します

※未入力の場合は、全てのアドレスからのアクセスを許可します

設定が完了したら[保存]をクリックすることで SCEP サーバ機能が利用可能になります。

3. MobileIronの設定

3.1. 認証機関の追加

管理画面上部のメニューより[管理]をクリックし、左側メニューの[インフラ]にある[認証機関]をクリックします。

画面中央にある[+追加]をクリックし、[外部認証機関を追加]にある[続行]をクリックします。[認証機関]のプルダウンメニューで、[汎用 SCEP サーバー]を選択し、[名前]に任意の名称を入力、[SCEP URL]に Gléas の SCEP 用 URL を入力します

※https://[Gléas UA ホスト名]/scep/[認証局番号]

例：デフォルトの認証局で発行する場合： https://ua.example.com/scep/1

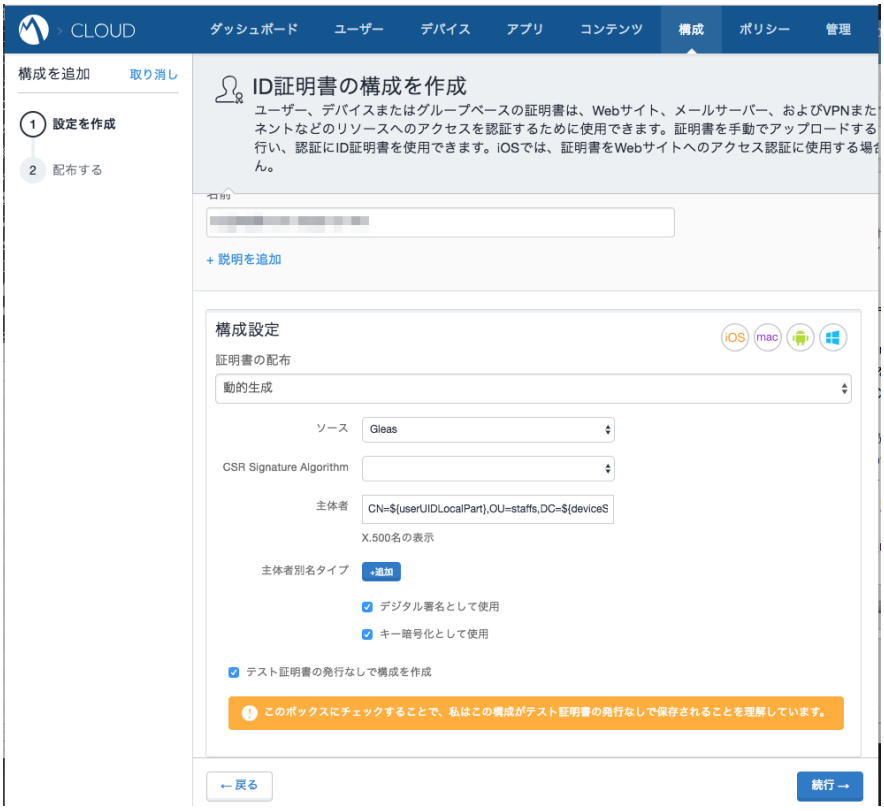
2.1 項で設定したチャレンジ値を[チャレンジパスワード]に入力し、[完了]をクリックします。

3.2. ID 証明書の構成を作成

管理画面上部のメニューより[構成]をクリックし、画面左上の[+追加]をクリックします。

[ID 証明書]をクリックし、[構成設定] > [証明書の配布]のプルダウンメニューから[動的生成]を選択し、[ソース]は 3.1 項で設定した Gléas を選択します。
[主体者]には MobileIron が用意するシステム属性の他に、固定値を入力もできます。

Gléas が SCEP 要求によって証明書を発行するためには、CN として指定されたアカウントが Gléas 内に存在する必要があります。
[テスト証明書の発行なしで構成を作成]にチェックを入れ、[続行]をクリックします。
※MobileIron からテスト証明書の発行をする場合は、事前に Gléas に test_user_id のアカウントを作成しておく必要があります。

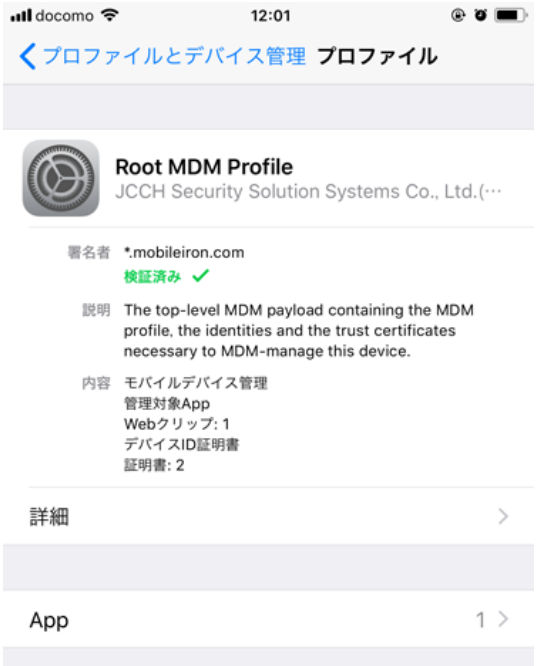


構成を当てはめるデバイスグループを選択し、[完了]をクリックします。

4. MobileIron へのデバイス加入

クライアントからMobileIronへデバイス加入すると、MDMプロファイルがインストールされます。続いてGléasが発行したクライアント証明書が自動でクライアントに配布されます。

iOSでのMDMプロファイルインストール完了時画面



iOSでのMobileIronからクライアント証明書のインストール完了後画面

5. 問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■Gléasや検証用の証明書に関するお問い合わせ

株式会社JCCH・セキュリティ・ソリューション・システムズ
Tel: 050-3821-2195
Mail: sales@jcch-sss.com