



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

AirWatchとPulse Connect Secure

デバイスコンプライアンス設定

Ver.1.0

2018年5月

- ・ JCCH・セキュリティ・ソリューション・システムズ、JS3 およびそれらを含むロゴは日本および他の国における株式会社 JCCH・セキュリティ・ソリューション・システムズの商標または登録商標です。Gléas は株式会社 JCCH・セキュリティ・ソリューション・システムズの商標です。
- ・ その他本文中に記載されている製品名および社名は、それぞれ各社の商標または登録商標です。
- ・ Microsoft Corporation のガイドラインに従って画面写真を掲載しています。

プライベート認証局 Gléas ホワイトペーパー
AirWatch と Pulse Connect Secure
証明書によるデバイスコンプライアンス設定

目次

1. はじめに.....	4
1.1. 本書について.....	4
1.2. 本書における環境.....	4
1.3. 本書における構成.....	5
1.4. 証明書発行時における留意事項.....	6
2. Connect Secure の設定.....	6
2.1. 認証サーバの設定.....	6
2.2. レルム（認証）の設定.....	8
3. iPad での接続操作.....	9
3.1. Pulse Secure クライアントのインストール.....	9
3.2. デバイス証明書の配信.....	10
3.3. Pulse Secure から接続.....	10
4. 問い合わせ.....	12

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、VMware Workspace ONEの機能、「VMware AirWatch」(MDM機能部分)とを連携させモバイルデバイスにプッシュ配布したデバイス証明書を利用して、Pulse Secure社のSSL-VPN装置「Pulse Connect Secure」へのログイン時にデバイス属性を参照した認証をおこなう環境を構築するため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活用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。

- Pulse Connect Secure (バージョン8.3R3 (build 59199))
※以後、「Connect Secure」と記載します
- モバイルデバイス管理：VMware AirWatch 9.3.0.7
※以後、「AirWatch」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)
※以後、「Gléas」と記載します
- クライアント:iPad Air2 (iOS 11.2.6) / Pulse Secure (バージョン6.5.2.74525)
※以後、「iPad」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。

- Connect Secureの基本設定および電子証明書認証の設定
※Connect Secureでのクライアント証明書認証に関する設定について、弊社では以下のURLでドキュメントを公開しております
参考URL：<https://www.gleas.jp/news/whitepaper/pulse-connect-secure>
- AirWatchでの基本設定や、順守ポリシーの設定方法
- AirWatchと、Gléasとのクライアント証明書発行の連携設定

プライベート認証局 Gléas ホワイトペーパー
AirWatch と Pulse Connect Secure
証明書によるデバイスコンプライアンス設定

※AirWatchとGléasの証明書発行およびプッシュ配信に関する連携設定について、弊社では以下のURLでドキュメントを公開しています

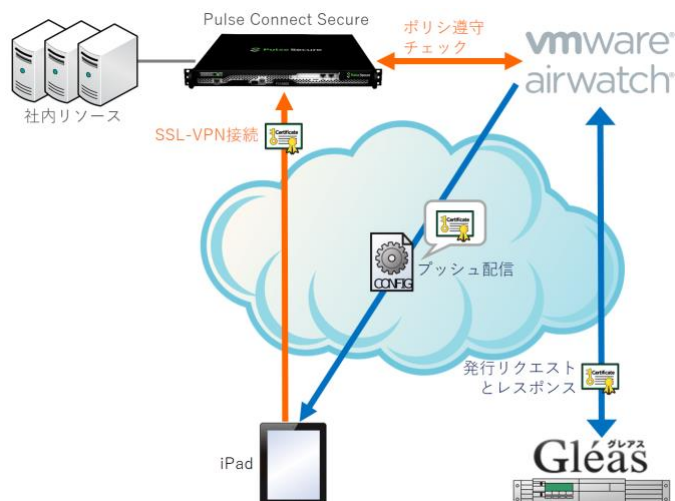
<https://www.gleas.jp/news/whitepaper/airwatch>

- Gléasでのユーザ登録やクライアント証明書発行などの基本設定
- iPadでのネットワーク設定などの基本設定、クライアントソフト Pulse Secureのインストール方法

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. AirWatch管理下のiPadに対し、Gléasから発行されたUDID情報を含むデバイス証明書がプッシュ配信される。
2. デバイスはConnect Secureにアクセスする
3. Connect Secureは、デバイス証明書による認証をおこなう。
4. Connect Secureは、証明書からUDIDを取得し、AirWatchに対しそのUDIDを持つデバイスの属性情報をリクエストし、AirWatchはその情報を返す。
5. Connect Secureは、AirWatchでのデバイス順守ポリシーを満たしている場合は接続を許可し、そうでない場合は接続を拒否する
(本ドキュメントでは、これを「デバイスコンプライアンスチェック」と呼びます)

1.4. 証明書発行時における留意事項

AirWatchでの証明書テンプレート設定（要求テンプレート）で、サブジェクト名を”CN={DeviceUid}”としておきます。

証明書テンプレートの追加/編集	
名前*	sample
説明	
認証局*	Test CA
プロファイルID*	0
プロダクトコード*	0
有効期間(年)*	1
サブジェクト名	CN={DeviceUid}
証明書の自動更新	<input type="checkbox"/>
証明書の取り消しを有効化	<input checked="" type="checkbox"/>

2. Connect Secureの設定

2.1. 認証サーバの設定

AirWatch を認証サーバとして設定します。

管理者画面左側のメニューより [Authentication] > [Auth. Server] と進み、右側の「New:」のドロップダウンより [MDM Server] を選択し、 [New Server...] ボタンをクリックします。



MDM サーバの設定ページに遷移するので、以下を設定します。

- Name:には、任意の認証サーバの名称を入力
- Type:には、 [Air Watch] を選択
- Server URL: には、 AirWatch のホスト名を入力(https://.....)
- Username:には、 AirWatch の管理ユーザ名を入力

プライベート認証局 Gléas ホワイトペーパー
AirWatch と Pulse Connect Secure
証明書によるデバイスコンプライアンス設定

- Password: には、上記ユーザのパスワードを入力
- Tenant Code: には、AirWatchAPI サービスの API キーを入力
※API キーは AirWatch の管理コンソールから[グループと設定] > [すべての設定] > [高度な設定] > [API] > [REST API]と進むと表示されます



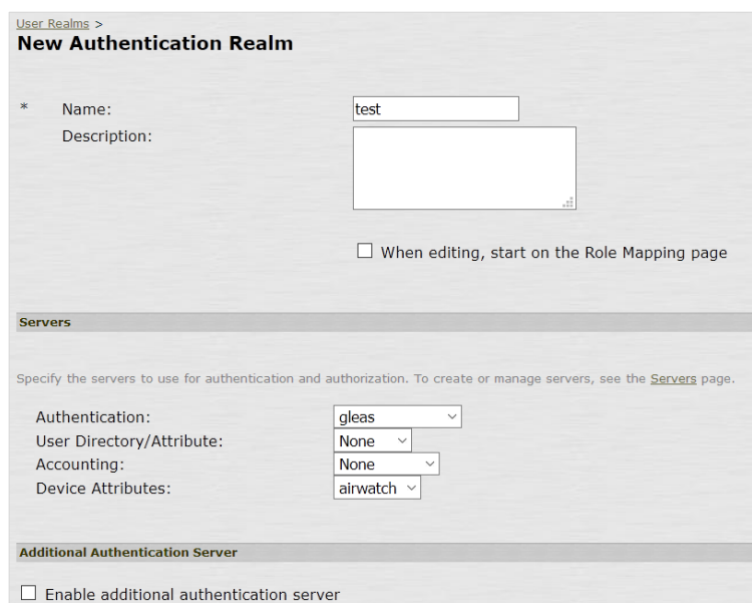
- ID Template:に "<certDN.CN>" (デフォルト値)を指定、ID Type:に、[UDID]を選択し、証明書サブジェクトの CN がデバイスの UDID として扱われるよう設定

上記の設定後、[Save Changes]をクリックして保存します。

2.2. レルム（認証）の設定

左側のメニューより [User Realms] > [New User Realm] をクリックします。
レルムの作成画面に移動しますので、General タブで以下の設定を行います。

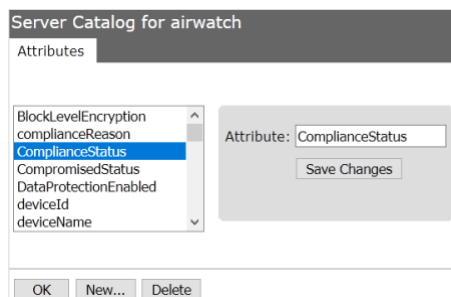
- Name:には、一意のレルム名称を入力
- Authentication:には、Auth. ServerでCertificate Serverとして設定したものを
選択
- Device Attributes:には、2.1項で設定したMDMサーバを選択



※ユーザ認証を追加したい場合など、[Enable additional authentication server]にチェックをすることにより、追加の認証方式を設定することが可能です

Role Mapping の設定画面に遷移するので、[New Rule...]をクリックし、以下の設定をおこないます。

- Rule based on:には、[Device Attribute]を選択し、[Update]をクリック
- Name:には、任意の識別名称を入力
- [Attribute]ボタンをクリックし、“ComplianceStatus”を追加



プライベート認証局 Gléas ホワイトペーパー
AirWatch と Pulse Connect Secure
証明書によるデバイスコンプライアンス設定

- Attribute:には、[ComplianceStatus]を選択し、[Update]をクリック
- 条件として、[is:]を選択し、テキストボックスに”Compliant”を入力
- Then assign these roles に、割り当てるロールを指定

User Realms > test > Role Mapping >
Role Mapping Rule

Rule based on: Device attribute Update

* Name: deviceComplianceCheck

Rule: If device has any of the following attribute values...

Attribute: ComplianceStatus Attributes...
is Compliant If more than one value for this attribute

then assign these roles

Available Roles: Selected Roles:
Add -> Users
Remove

Stop processing rules when this rule matches

To manage roles, see the [Roles](#) configuration page.

Save Changes

Save Changes Save + New

上記の設定後、[Save Changes]をクリックして保存します。

3. iPad での接続操作

3.1. Pulse Secureクライアントのインストール

iPadでPulse Secureを利用する場合は、クライアントソフトウェアのダウンロードが必要です。App Store より事前にインストールをおこないます。本書ではPulse Secureのインストール方法については割愛します。

3.2. デバイス証明書の配信

AirWatchの管理下になり適切なプロファイルが適用されたiPadには、AirWatchより自動的にデバイス証明書、および(VPNプロファイルの設定もなされていれば)Pulse Secureクライアントの設定がプッシュ配信されます。

3.3. Pulse Secureから接続

Airwatchでは、iPadはポリシー順守状態にしておきます。



Pulse Secureクライアントを起動し[接続]ボタンをタップすると、バックグラウンドでクライアント証明書を利用した認証を行いVPNの接続がおこなわれます。

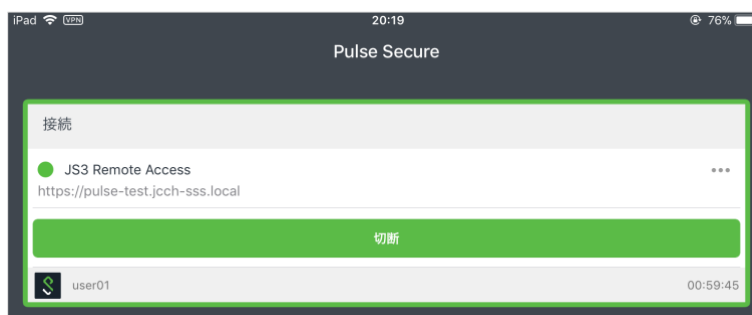
※提示可能な証明書が複数ある場合は、選択ダイアログが表示されます

以下はPulse Secureクライアントから接続した画面です。



接続成功すると、通知エリアに VPN アイコンが表示されます。

プライベート認証局 Gléas ホワイトペーパー
AirWatch と Pulse Connect Secure
証明書によるデバイスコンプライアンス設定



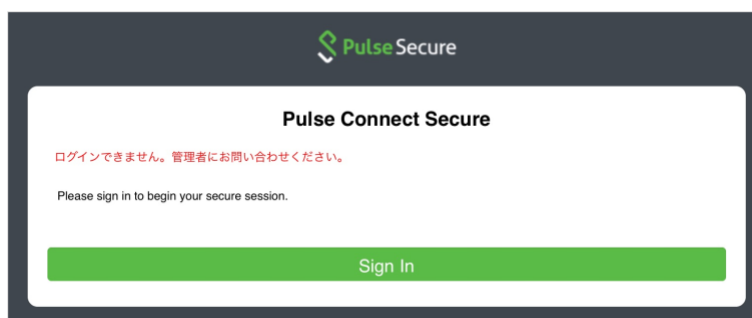
Connect Secureのイベントログに、AirwatchのAPIから取得したデバイス属性情報が表示されます。そこを見ると、ロールマッピングルールで設定した通り ComplianceStatusという属性が含まれていることがわかります。

```
ive - [127.0.0.1] System()[] - airwatch Response 1234567890: Status: 200: {...,"ComplianceStatus":"Compliant",...}
```

次に、AirWatchでiPadを順守違反の状態にします。



この状態でVPN接続をおこなうと、接続に失敗します。



Connect Secure の イベント ログ を 見 る と 、 AirWatch から 取 得 し た ComplianceStatus属性が“NonCompliant”となっていることがわかります。

```
ive - [127.0.0.1] System()[] - airwatch Response 1234567891: Status: 200: {...,"ComplianceStatus":"NonCompliant",...}
```

ロールマッピングルールに該当するものがないため、ログイン失敗となります。このときConnect Secureのユーザアクセスログには、“Login failed. Reason: No Roles”と表示されます。

4. 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。

■Connect Secureに関するお問い合わせ先

パルスセキュアジャパン株式会社

Tel: 03-6809-6836

Mail: info_jp@pulsesecure.net

■Workspace ONE (Airwatch) に関するお問い合わせ先

ヴェイムウェア株式会社

URL : <https://www.vmware.com/jp/company/contact.html>

■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