



# プライベート認証局Gléas ホワイトペーパー

Workspace ONEとPulse Policy Secureでの  
端末ポリシーチェック

Ver.1.1

2018年7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  
Workspace ONE と Pulse Policy Secure での  
端末ポリシーチェック

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
2. Workspace ONE の設定.....	5
2.1 証明書要求テンプレートの設定.....	5
2.2 プロファイルの設定 (Windows).....	6
2.3 プロファイルの設定 (iOS).....	7
2.4 プロファイルの設定 (macOS).....	9
2.5 順守ポリシーの設定.....	11
3. Pulse Policy Secure の設定.....	12
3.1. 信頼するルート認証局の設定.....	12
3.2. サーバ証明書の設定.....	13
3.3. Authentication Servers の設定.....	15
3.4. User Realms の設定.....	16
4. クライアントでの接続操作.....	17
4.1. Workspace ONE へのデバイス加入.....	17
4.2. Wi-Fi ネットワークへの接続.....	17
5. 問い合わせ.....	17

## 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、VIEWMウェア社のデジタルワークスペース・プラットフォーム VMware Workspace ONEを連携させ、デバイスにプッシュ配布した電子証明書を利用して、Pulse Secure社のネットワークアクセスコントローラ「Pulse Policy Secure」へのLAN接続時に、端末のセキュリティポリシーを参照した認証をおこなう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。

- ▶ Pulse Policy Secure (バージョン9.0R1 build 49495)  
※以下「PPS」と記載します
- ▶ モバイルデバイス管理：Workspace ONE UEM 9.5.0.2  
※以下「Workspace ONE」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 Inspiron 13 7000 (Windows 10 Pro)  
：iPhone 6S+ (iOS 11.4)  
：mac mini Late 2012 (macOS High Sierra)  
※それぞれ以下「Windows」「iOS」「macOS」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。

- PPSの基本設定および802.1X EAP-TLS認証設定  
※PPSの802.1X EAP-TLS認証設定は、下記URLでドキュメントを公開しています。  
<https://www.gleas.jp/news/whitepaper/pulsepolicysecure>
- Workspace ONEの基本設定およびGléasとの連携設定  
※Workspace ONEとGléasの連携設定は、下記URLでドキュメントを公開しています。  
<https://www.gleas.jp/news/whitepaper/airwatch>

プライベート認証局 Gléas ホワイトペーパー  
Workspace ONE と Pulse Policy Secure での  
端末ポリシーチェック

- Gléasの基本設定
- Windows、iOS、macOS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Workspace ONEへデバイス加入をすると、連携設定をされたGléasへWorkspace ONEは証明書発行要求する。
2. Gléasはクライアントの端末識別情報を含むデバイス証明書を発行し、Workspace ONEを経由してクライアントへプッシュ配信される。
3. クライアントがPPSにアクセスする。
4. PPSとクライアントで802.1X EAP-TLS認証が行われる。
5. PPSはWorkspace ONEへクライアントのポリシー順守状況を問い合わせ、クライアントがポリシーを順守していれば接続を許可される。

## 2. Workspace ONEの設定

### 2.1. 証明書要求テンプレートの設定

Workspace ONE の管理画面左側のメニューより[デバイス]>[証明書]>[認証局] と進み、画面中央の「要求テンプレート」のタブを表示させ、「+ 追加」をクリックします。

「サブジェクト名」にCN={DeviceUid} と入力します。この設定により、Gléas で発行される証明書のCN (Common Name) にデバイスのUDID が記載されます。「認証局」で、

プライベート認証局 Gléas ホワイトペーパー  
Workspace ONE と Pulse Policy Secure での  
端末ポリシーチェック

あらかじめ連携させた Gléas を選択し、「名前」「プロファイル ID」「プロダクトコード」を任意に設定して、「保存」をクリックします。

※プロファイル ID は Gléas のグループ ID と紐付けることができます。

## 証明書テンプレートの追加/編集

名前 *	Template-pps
説明	
認証局 *	
プロファイル ID *	34
プロダクトコード *	34
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"/> ⓘ

## 2.2. プロファイルの設定 (Windows)

管理画面左側のメニューより[デバイス]>[プロファイル] と進み、画面中央の「追加」のドロップダウンから「プロファイルを追加」をクリックします。

「プラットフォームを選択」で [Windows]をクリックし、「デバイスタイプを選択」で [Windows デスクトップ] をクリックし、「コンテキストを選択」で「ユーザープロファイル」をクリックすると「全般」のタブが開かれます。

「名前」と「割り当てるグループ」を設定して、左のメニューから「資格情報」をクリックして画面中央の「構成」をクリックします。

「資格情報ソース」で「アップロード」が選択されています。あらかじめ Gléas のルート証明書を <http://hostname/> (http であることに注意) から取得し、アップロードします

プライベート認証局 Gléas ホワイトペーパー  
Workspace ONE と Pulse Policy Secure での  
端末ポリシーチェック

### 資格情報

資格情報ソース	アップロード
証明書 *	アップロード
キーの位置	ソフトウェア
証明書ストア	個人

「キーの位置」は「ソフトウェア」、「証明書ストア」は「個人」を選択します。

続いて右下の「+」ボタンをクリックし、「資格情報ソース」で「定義済み認証局」を選択し、「認証局」で連携済みの Gléas を選択し、「証明書テンプレート」では 2.1 項で作成したものを選択します。

### 資格情報 #2

資格情報ソース	定義済み認証局
認証局 *	
証明書テンプレート *	
キーの位置	ソフトウェア
証明書ストア	個人

## 2.3. プロファイルの設定 (iOS)

管理画面左側のメニューより[デバイス]>[プロファイル] と進み、画面中央の「追加」のドロップダウンから「プロファイルを追加」をクリックします。

「プラットフォームを選択」で [Apple iOS] をクリックすると「全般」のタブが開かれます。「名前」と「割り当てるグループ」を設定して、左のメニューから「資格情報」をクリックして画面中央の「構成」をクリックします。

「資格情報ソース」で「アップロード」が選択されています。あらかじめ Gléas のルート証明書を <http://hostname/> (http であることに注意) から取得し、アップロードします。

プライベート認証局 Gléas ホワイトペーパー  
Workspace ONE と Pulse Policy Secure での  
端末ポリシーチェック



続いて右下の「+」ボタンをクリックし、「資格情報ソース」で「定義済み認証局」を選択し、「認証局」で連携済みの Gléas を選択し、「証明書テンプレート」では 2.1 項で作成したものを選択します。

## 資格情報 #2

資格情報ソース	定義済み認証局
認証局 *	
証明書テンプレート *	

続いて左のメニューから「Wi-Fi」へ移動し、「SSID」に端末ポリシーチェックを実施する SSID 名を入力し、「セキュリティタイプ」を「WPA2 エンタープライズ」にし、「プロトコル」は「EAP-TLS」を選択します。

プライベート認証局 Gléas ホワイトペーパー  
Workspace ONE と Pulse Policy Secure での  
端末ポリシーチェック

## Wi-Fi

SSID (サービスセット ID) *	<input type="text" value="XXXXXXXXXX"/>	+
非公開のネットワーク	<input type="checkbox"/>	
自動参加	<input checked="" type="checkbox"/>	
セキュリティタイプ	WPA2 エンタープライズ	
プロトコル *	<input checked="" type="checkbox"/> EAP-TLS <input type="checkbox"/> TTLS <input type="checkbox"/> LEAP <input type="checkbox"/> PEAP <input type="checkbox"/> EAP-FAST <input type="checkbox"/> EAP-SIM	

「ID 証明書」は「証明書#2」を選択します。この設定により本項で設定した「資格情報 #2」の証明書が EAP-TLS で使用されることとなります。

### 認証

ユーザー名	<input type="text"/>	+
接続時に毎回入力するユーザー パスワード	<input type="checkbox"/>	
パスワード	<input type="password" value="....."/>	変更
ID 証明書	証明書 #2	

「信頼された証明書」は「証明書#1」を選択します。この設定により本項で設定した「資格情報#1」の Gléas のルート証明書がデバイスにインポートされます。

### 信頼

#### 信頼された証明書

- 証明書 #1  
 証明書 #2

「信頼されたサーバ証明書名」に PPS のサーバ名を入力し、画面下部の「保存して公開」をクリックします。

信頼されたサーバ証明書名	<input type="text" value="XXXXXXXXXX"/>	×
	<input type="button" value="+ 追加"/>	

## 2.4. プロファイルの設定 (macOS)

管理画面左側のメニューより[デバイス]>[プロファイル] と進み、画面中央の「追加」の

プライベート認証局 Gléas ホワイトペーパー  
Workspace ONE と Pulse Policy Secure での  
端末ポリシーチェック

ドロップダウンから「プロファイルを追加」をクリックします。「プラットフォームを選択」で [Apple macOS] をクリックし、「コンテキストを選択」で「ユーザープロファイル」をクリックすると「全般」のタブが開かれます。「名前」と「割り当てるグループ」を設定して、左のメニューから「資格情報」をクリックして画面中央の「構成」をクリックします。

「資格情報ソース」で「アップロード」が選択されています。あらかじめ Gléas のルート証明書を <http://hostname/> ([http](http://hostname/) であることに注意) から取得し、アップロードします。



続いて右下の「+」ボタンをクリックし、「資格情報ソース」で「定義済み認証局」を選択し、「認証局」で連携済みの Gléas を選択し、「証明書テンプレート」では 2.1 項で作成したものを選択します。

## 資格情報 #2

資格情報ソース	定義済み認証局
認証局 *	[Redacted]
証明書テンプレート *	[Redacted]

続いて左のメニューから「ネットワーク」へ移動し、「ネットワークインターフェイス」で Wi-Fi を選択し、「SSID」に端末ポリシーチェックを実施する SSID 名を入力し、「セキュリティタイプ」を「WPA2 Enterprise」にし、「プロトコル」は「EAP-TLS」を選択します。

プライベート認証局 Gléas ホワイトペーパー  
Workspace ONE と Pulse Policy Secure での  
端末ポリシーチェック



「ID 証明書」は「証明書#2」を選択します。この設定により本項で設定した「資格情報 #2」の証明書が EAP-TLS で使用されることとなります。

「信頼された証明書」は「証明書#1」を選択します。この設定により本項で設定した「資格情報#1」の Gléas のルート証明書がデバイスにインポートされます。

「信頼されたサーバ証明書名」に PPS のサーバ名を入力し、画面下部の「保存して公開」をクリックします。

認証

ユーザー名

ID 証明書

信頼

信頼された証明書

証明書 #1

証明書 #2

---

信頼されたサーバ証明書名

## 2.5. 順守ポリシーの設定

管理画面左側のメニューより[デバイス] > [順守ポリシー] > [リスト表示]と進み、画面中央の「+ 追加」をクリックします。

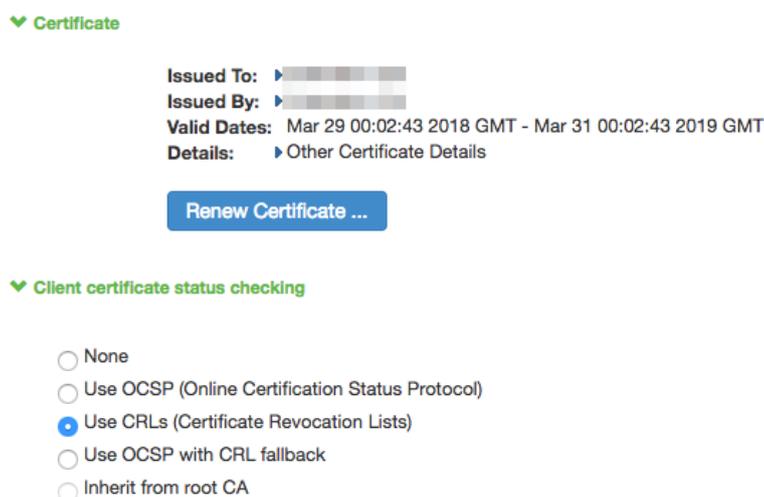
Windows、iOS、macOS で任意のルールを設定し、グループに割り当てます。

## 3. Pulse Policy Secureの設定

### 3.1. 信頼するルート認証局の設定

PPS 管理画面で上部メニュー [System] > [Configuration] > [Certificates] > [Trusted Client CAs]と進み、画面中央の「Import CA Certificate…」をクリックして、2.2~2.4 項で使用した Gléas のルート証明書を PPS にインポートします。

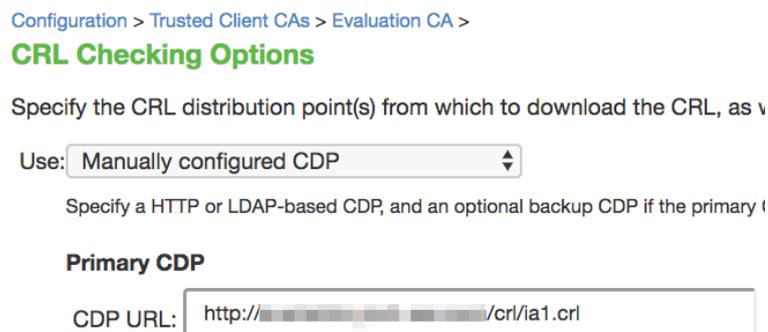
Client certificate status checking 項目で、「Use CRLs (Certificate Revocation Lists)」を選択して「Save Changes」をクリックします。



続いて画面下部の「CRL Checking Options…」をクリックし

- 「Use」ドロップダウンメニューから「Manually configured CDP」を選択
- 「Primary CDP」の「CDP URL」に配布ポイントとなる URL を入力  
※CRL 配布点が複数ある場合は、Backup CDP を設定します。

下記は Gléas が http で公開している CRL を取得する場合の設定例です。



CRL の取得間隔を指定したい場合は、Options 項目で[CRL Download Frequency]を指定

プライベート認証局 Gléas ホワイトペーパー  
Workspace ONE と Pulse Policy Secure での  
端末ポリシーチェック

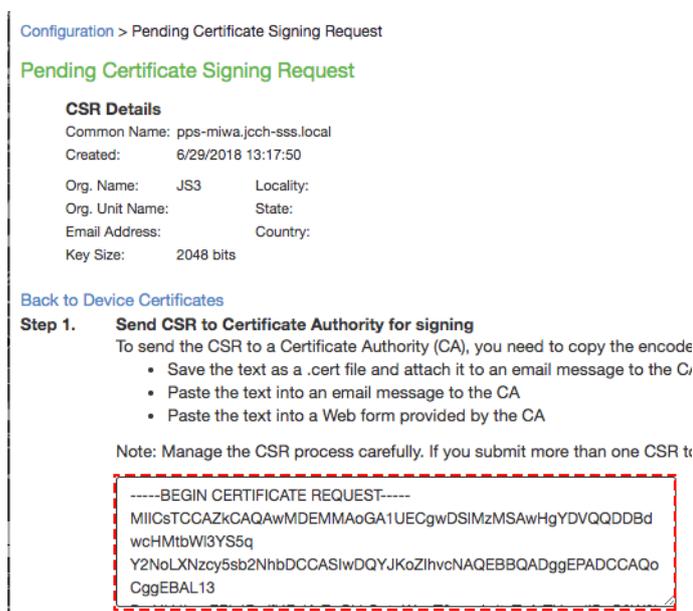
することにより可能です。

設定後、「Save Changes」をクリックします。

### 3.2. サーバ証明書の設定

管理者画面上部メニューより[System] > [Configuration] > [Certificates] > [Device Certificates]と進みます。[New CSR...]をクリックし、「Common Name」など、必要事項を入力し[Create CSR]をクリックします。

画面下部のテキストエリアの内容をテキストファイルに保存します。



Configuration > Pending Certificate Signing Request

#### Pending Certificate Signing Request

**CSR Details**

Common Name: pps-miwa.jcch-sss.local  
Created: 6/29/2018 13:17:50

Org. Name: JS3      Locality:  
Org. Unit Name:      State:  
Email Address:      Country:  
Key Size: 2048 bits

[Back to Device Certificates](#)

**Step 1. Send CSR to Certificate Authority for signing**

To send the CSR to a Certificate Authority (CA), you need to copy the encode

- Save the text as a .cert file and attach it to an email message to the CA
- Paste the text into an email message to the CA
- Paste the text into a Web form provided by the CA

Note: Manage the CSR process carefully. If you submit more than one CSR to

```
-----BEGIN CERTIFICATE REQUEST-----  
MIICsTCCAzkCAQAwMDEMMAoGA1UECgwDSIMzMSAwHgYDVQQDBDd  
wCHMtbWl3YS5q  
Y2NoLXNzcy5sb2NhbDCCASlwDQYJKoZIhvcNAQEBBQADggEPADCCAQo  
CggEBAL13
```

Gléas (RA) にログインし、該当のサーバアカウントのページへ移動し、左側メニューの「証明書発行」をクリックします。



[アカウント] > 詳細

アカウント  
Account

グループ  
Group

証明書  
Certificate

認証デバイス  
Device

テンプレート  
Template

アカウント操作

- アカウント一覧
- 登録申請者一覧
- アカウント新規作成
- 証明書発行
- アカウント削除
- ドックに入れる

アカウント

アカウント情報 ..... 改訂履歴

- サーバ ..... 登録日時: 2018/06/29 13:45
- ステータス: 有効
- サーバ属性 ..... 最終更新: 2018/06/29 13:45 編集
- ホスト名: [REDACTED]

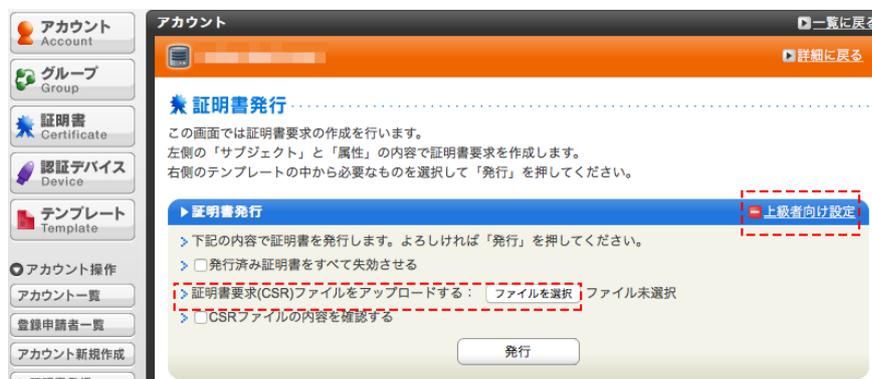
証明書発行の履歴

#	シリアル	開始	有効期限
証明書は発行			

テンプレート情報

プライベート認証局 Gléas ホワイトペーパー  
Workspace ONE と Pulse Policy Secure での  
端末ポリシーチェック

画面右にある「上級者向け設定」をクリックし、CSRのテキストファイルをアップロードして「発行」をクリックします。



証明書発行完了後、証明書詳細画面の証明書ファイル欄の「証明書：あり」をクリックし、発行された証明書をダウンロードします。



PPSのCSR生成画面に戻り、Gléasからダウンロードしたサーバ証明書をインポートします。

Step 2.

**Import signed certificate**

When you receive the signed certificate file from the CA, select it below and

Signed certificate:  No file chosen

### 3.3. Authentication Servers の設定

上部メニューから [Authentication] > [Auth. Servers] へ移動し、「(Select server type)」で「MDM Server」をセットし、「New Server」をクリックします。

「Name」に任意の名前を、「Type」で「Air Watch」を選択、「Server Url」に Workspace ONE のホスト名を、「Username」に Workspace ONE の管理者アカウントを、「Password」に入力した Workspace ONE 管理者のパスワードを、「Tenant Code」に Workspace ONEAPI サービスの API キーを入力します。

※API キーは Workspace ONE の管理コンソールから[グループと設定] > [すべての設定] > [システム] > [高度な設定] > [API] > [REST API]と進むと表示されます

Auth Servers > AirWatch > Settings

Settings

Settings

\*Name:  Label to reference this server.

Type: Air Watch

▼ Server

- Server Url:
- Viewer Url:   
For example: https://cn11.airwatchportals.com/AirWatch/Devices/DeviceDetails/<deviceAttr>
- Request Timeout:

▼ Administrator

- Username:
- Password:
- Tenant Code:

Test Connection

「ID Template」に「<certDN.CN>」（デフォルト値）を指定し、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して、「Save Changes」をクリックします。

プライベート認証局 Gléas ホワイトペーパー  
Workspace ONE と Pulse Policy Secure での  
端末ポリシーチェック

▼ Device Identifier

Please check the options on the Users > Authentication > [Realm] > Authen

Device Identity:  **Require certificate** maximize security  
 Use certificate if present if certificate is not pr  
 Always use MAC address in case certificate dc

ID Template:

The template can contain textual characters as well as \

Examples:

<certDN.CN> First CN from the subject DN  
<certAttr.serialNumber> Certificate serial number  
<certAttr.altName.xxx> Where xxx can be:  
Email The Email alternate name  
UPN The Principal Name alternate r  
... etc

<certDNText> The complete subject DN  
cert-<certDN.CN> The text "cert-" followed by the first C

ID Type:  UUID Universal Unique Identifier  
 Serial Number  
 UDID Unique Device Identifier  
 IMEI International Mobile Equipment Identity

Save Changes

Reset

### 3.4. User Realms の設定

上部メニューから [Users] > [User Realms] へ移動し、デフォルトで作成されている「Cert Auth」をクリックします。

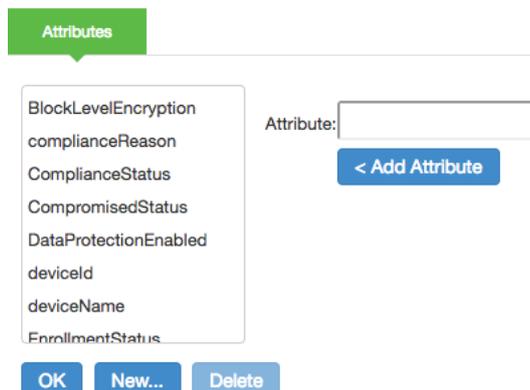
「General」タブの「Servers」で「Authentication」に「Certificate Authentication」が設定されていることを確認し、「Device Attributes」に 3.3 項で設定した Workspace ONE 名をセットして画面下部の「Save Changes」をクリックします。

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 [Device Attribute]を選択し、[Update]をクリック
- 「Name」に任意の名前を入力
- 「Attribute」ボタンをクリックし、「Attribute」に「ComplianceStatus」を入力して「< Add Attribute」をクリックし、「OK」をクリックします。

プライベート認証局 Gléas ホワイトペーパー  
Workspace ONE と Pulse Policy Secure での  
端末ポリシーチェック

Server Catalog for AirWatch



「Attribute」に「ComplianceStatus」を選択し、続いて「is」とし、テキストボックスに「Compliant」と入力します。

「Then assign these roles」に、割り当てるロールを指定して「Save Changes」をクリックします。

## 4. クライアントでの接続操作

### 4.1. Workspace ONEへのデバイス加入

クライアントからWorkspace ONE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Workspace ONEで設定したWi-Fi設定と証明書が自動で配布されます。  
※WindowsはAirWatch Protection Agentのインストールが必要です。

### 4.2. Wi-Fiネットワークへの接続

Workspace ONE管理画面で、クライアントがポリシー順守違反がないことを確認します。



2.2～2.4項で設定したSSIDにクライアントで接続すると、Workspace ONEから配布されたプロファイルに従い、自動で802.1X EAP-TLS認証が行われ、ポリシー順守違反がないため、LAN接続が許可されます。

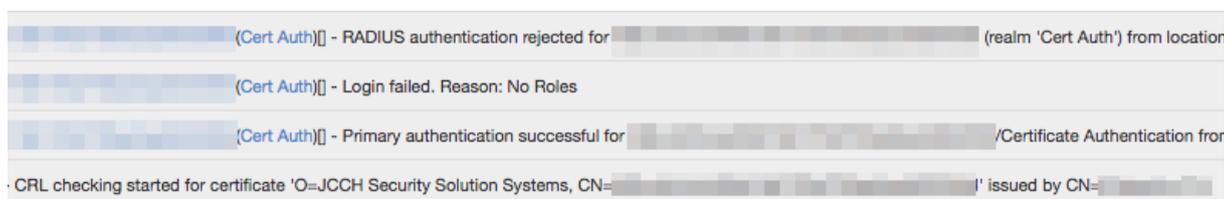
プライベート認証局 Gléas ホワイトペーパー  
Workspace ONE と Pulse Policy Secure での  
端末ポリシーチェック

続いて、Workspace ONEでクライアントを順守違反の状態にします。



同じSSIDへ接続しようとしても、3.4項でWorkspace ONEで「ComplianceStatus」が「Compliant」となっていればUser Rolesを割り当て、そうでない場合はUser Rolesを設定していないため、PPSは接続を拒否します。

PPSのUser Access Logsを見ると、「No Roles」として拒否されているのがわかります。



## 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。

### ■Pulse Policy 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に関するお問い合わせ先

ヴァイエムウェア株式会社

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