

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

Copyright by JCCH Security Solution Systems Co., Ltd. All Rights reserved

- 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。

Copyright by JCCH Security Solution Systems Co., Ltd. All Rights reserved

Workspace ONE と Pulse Policy Secure での

端末ポリシーチェック

目	次
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. Work	space 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. Puls	e 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
34		
5.4.	User Realms の設定	16
4. クラ	User Realms の設定 イアントでの接続操作	16 17
3.4. 4. クラ 4.1.	User Realms の設定 イアントでの接続操作 Workspace ONE へのデバイス加入	16 17 17
 4. クラ 4.1. 4.2. 	User Realms の設定 イアントでの接続操作 Workspace ONE へのデバイス加入 Wi-Fi ネットワークへの接続	16 17 17 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、ヴイエム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

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ヘ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、

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 *	
	24
747747010 ···	34
プロダクトコード*	34
有効期間 (年) <mark>*</mark>	1
	I I POOL I A
サブジェクト名	CN={DeviceUid}
証明書の自動更新	\Box (1)
証明書の取り消しを有効化	V

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

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	v
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。

Workspace ONE と Pulse Policy Secure での

端末ポリシーチェック

iOS		
① 全般		
ペスコード	資格情報	
◎ 制限	資格情報ソース	アップロード
🔅 Wi-Fi		
A VPN	資格情報名 *	証明書がアップロードされると、証明書のファイル名が自動入力
≜ Eメール	証明書 *	アップロード
🔀 Exchange ActiveSync		
1 通知		
LDAP		
31 CalDAV		
🛱 定期配信カレンダー		
ぎ CardDAV		
≫ Web クリップ		
♥ 資格情報		

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 *	1

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) *		+
非公開のネットワーク		
自動参加		
セキュリティ タイプ	WPA2 エンタープライズ	~
プロトコル*	Z EAP-TLS	
	ΠTLS	
	LEAP	
	PEAP	
	EAP-FAST	
	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 で使用されることになります。

認証			
ユーザー名			+
接続時に毎回入力するユーザー パ スワード			
パスワード			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		×
	Dt. 题 ()	

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 であることに注意) から取得し、アップロードします。

macOS 新しい Apple macOS プロファイルを追加				
① 全般				
ペスコード	資格情報			
奈 ネットワーク	資格情報ソース	アップロード		
A VPN				
≜ Eメール	資格情報名 *	証明書がアップロードされると、証		
🔀 Exchange Web Service	証明書 *	アップロード		
LDAP	1000 2 2 101			
🛱 CalDAV	すべてのアプリケーションへのア クセスを許可			
CardDAV				
℅ Web クリップ	キーチェーンからのプライベート キーのエクスポートを許可			
● 資格情報 ①				

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 *	1

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。

Workspace ONE と Pulse Policy Secure での

端末ポリシーチェック

macOS Profile-mac	OS	
() 全般 へ パスコード	ネットワーク	
奈 ネットワーク ① ▲ VPN	ネットワーク インターフェイス	Wi-Fi
≝ Eメール	SSID (サービスセット ID) *	
🔀 Exchange Web Service	接続	□ 非公開のネットワーク 🛛 自動参加
LDAP		
31 CalDAV	セキュリティ タイプ	WPA2 Enterprise
	ログイン ウィンドウ構成として使	
E CardDAV	ログイン ウィンドウ構成として使	 ユーザーはネットワークへの認証のためE
圕 CardDAV ※ Web クリップ	ログイン ウィンドウ構成として使 用する	 ユーザーはネットワークへの認証のためE
国 CardDAV み Web クリップ 資格情報 2	ログイン ウィンドウ構成として使 用する プロトコル	○ ユーザーはネットワークへの認証のためC ✔ EAP-TLS
国 CardDAV み Web クリップ ♥ 資格情報	ログイン ウィンドウ構成として使 用する プロトコル	□ ユーザーはネットワークへの認証のためE ✔ EAP-TLS
国 CardDAV ※ Web クリップ ♥ 資格情報 2 ↔ SCEP I==I Dock	ログイン ウィンドウ構成として使 用する プロトコル	 □ ユーザーはネットワークへの認証のためE ✓ EAP-TLS □ TTLS
国 CardDAV み Web クリップ ● 資格情報 2 ↔ SCEP I==I Dock ◎ 制限	ログイン ウィンドウ構成として使 用する プロトコル	 □ ユーザーはネットワークへの認証のためE ✓ EAP-TLS □ TTLS □ LEAP

「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 で使用されることになります。

「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	証明書 #2 、	,
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。

Certificate	
	Issued To: Issued By: Valid Dates: Mar 29 00:02:43 2018 GMT - Mar 31 00:02:43 2019 GMT Details: Other Certificate Details
	Renew Certificate
♥ Client certifica	ate status checking
○ None	
Use OC	SP (Online Certification Status Protocol)
Use CR	Ls (Certificate Revocation Lists)
Use OC	SP with CRL fallback
Inherit f	rom root CA

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。

Configuration > Trusted Client CAs > Evaluation CA > CRL Checking Options

Specify the CRL distribution point(s) from which to download the CRL, as v

Use: Manually o	onfigured CDP	:	•
Specify a HTT	P or LDAP-based CDP,	and an optior	nal backup CDP if the primary (
Primary CD	P		
CDP URL:	http://	/c	rl/ia1.crl

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

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: Created:	CSR Details Common Name: pps-miwa.jcch-sss.local Created: 6/29/2018 13:17:50			
Org. Name: Org. Unit Name: Email Address: Key Size:	JS3 2048 bits	Locality: State: Country:		
Back to Device Cert	ificates			
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 C/ 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 MIICsTCCAZkCAQAwMDEMMAoGA1UECgwDSIMzMSAwHgYDVQQDDBd wcHMtbWI3YS5q Y2NoLXNzcy5sb2NhbDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQo 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	アカウント					
Group	アカウント	、情報				国改訂履歴
★ 証明書 Certificate	▶サーバ	1.5 1.6			登録日時:	2018/06/29 13:45
認証デバイス Device	> ステータス :	有効				
テンプレート	▶サーパ属性				最終更新:2018/0	06/29 13:45 <u>編集</u>
Template	> ホスト名 :					
●アカウント操作						
アカウントー覧	🏃 証明書発	行の履歴・・・・				
登録申請者一覧	▶1					
アカウント新規作成	#	シリアル	開	冶	有効期限	7
▶証明書発行						証明書は発行
▶アカウント削除		したた				
ドックに入れる						

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。

アカウント	アカウント	□ <u>一覧に戻る</u>
Account		▶詳細に戻る
Group 兼証明書 Certificate	業証明書発行 この画面では証明書要求の作成を行います。	
認証デバイス Device	左側の「サブジェクト」と「属性」の内容で証明書要求を作成します。 右側のテンプレートの中から必要なものを選択して「発行」を押してください。	
Template	▶ 注明書発行 > 下記の内容で証明書を発行します。よろしければ「発行」を押してください。 > □ 発伝法A 550mmまたまなごためさせる。	
●アカウント操作		
アカウント一覧	▶ 証明書要求(CSR)ファイルをアップロードする: ファイルを選択 ■ CSRファイルの内容を確認する	
 登録申請者一覧 アカウント新規作成 ▶ 証旧書登行 	第行	

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:<u>あり</u>」をクリック し、発行された証明書をダウンロードします。

[証明書]>詳細		■認証局 ■ログ ■管理者 ■ヘルプ ■ログアウト
アカウント Account		▶ <u>一覧に戻る</u> ▶ <u>ドック</u>
Corrup Group ※ 証明書 Certificate の認証デバイス Device トランプレート Template	>一般名:	 > 矢効日: > 矢効理由: > 期限終了日: > 状態: 有効な証明書 > 処理の状態: 有効な証明書 > トークン必要: > パージョン: 4
 ○ 証明書操作 証明書一覧 ▶失効処理 ▶ 停止処理 ▶ ドックに入れる 	 ▶ 証明書情報 > 認証局: > 暗号アルゴリズム: rsa > ダイジェストアルゴリズム: sha256 > 鍵長: 2048 > 鍵用流: <u>電子署名 鍵の暗号化</u> > 拡張鍵用流: <u>SSLサーバ際証</u> <u>SSLクライアント認証</u> > 別名: 	
	▶ E明書ファイル > 証明書要求: <u>あり</u> 作成日時 2018/06/26 14:15 > 証明書: <u>あり</u> 作成日時 2018/06/26 14:17 > 秘密鍵: なし	

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 c	ertificate file from the CA, select it below and
	Signed certificate: Browse	No file chosen
	Import	

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.
✓ Server	
* Server Url:	
Viewer Url:	L
* Request Timeout:	For example: https://cn11.airwatchportals.com/AirWatch/Devices/DeviceDetails/ <deviceattr.< th=""></deviceattr.<>
✓ Administrator	
* Username:	an anarother a m
* 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 Identifi	ler			
Please check the	options on the Users	> Authentication > [Realm] > Auther		
Device Identity	: 💿 Require cert	ificate maximize security		
	 Use certifica 	ite if present if certifcate is not pro		
	Always use	MAC addressin case certificate do		
ID Template:	<certdn.cn></certdn.cn>			
	The template can c	ontain textual characters as well as v		
	<pre>Examples: <certdn.cn></certdn.cn></pre>	First CN from the subject DN		
	<certattr.serialnumbe< th=""><th>r>Certificate serial number</th></certattr.serialnumbe<>	r>Certificate serial number		
	<certminarinarine.xxx< th=""><th>Email The Email alternate name</th></certminarinarine.xxx<>	Email The Email alternate name		
		UPN The Principal Name alternate r		
	<certdntext></certdntext>	The complete subject DN		
ID Type:	O UUID	The text "cert-" followed by the first C		
	Serial Number	er		
		Linique Device Identifier		
		International Mobile Equipment		
	0	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 Atribute」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						
Attributes						
Plack avaluation						
complianceBeason						
ComplianceStatus < Add A	ttribute					
CompromisedStatus						
DataProtectionEnabled						
deviceId						
deviceName						
EprollmentStatus						
OK New Delete						

「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ヘ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。

続いて、Works	pace	プライ Wc ONEで	ベート認 prkspace Ol 端末 クライア	証局 Gléas NE と Pulse F ポリシーチ ?ントを順 ⁵	; ホワイト Policy Secure - ェック 守違反の社	ペーパ eでの 犬態に	゚゚゚゚ <u>ー</u> します。	
User-pps1 iPhone iOS 11.4.0 GRWV IPhone 6s Plus 11.4.0 所有形態: 企業 - 専用								
	概要	順守	プロファイル	アプリ	コンテンツ	場所	ユーザー	その他 🗸
	侯害状態不明 1 順守違反 1		し 加入済み 2018/06/28		● 最終接続時間 1時間前			

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。

(Cert Auth)[] - RADIUS authentication rejected for	(realm 'Cert Auth') from location
(Cert Auth)[] - Login failed. Reason: No Roles	
[Cert Auth)[] - Primary authentication successful for	/Certificate Authentication from
CRL checking started for certificate 'O=JCCH Security Solution Systems, CN=	l' issued by CN=

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