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

Pulse Connect Secure / Workspace ONE UEMでの Per-App VPN

Ver. 1.0
2019 年 2 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

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、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 UEM」(AirWatchの後継サービス）を連携させ、デバイスにプッシュ配信した電子証明書を利用して、Pulse Secure社の「Pulse Connect Secure」 をゲートウェイとしたPer-App VPN（アプリケーション単位でのVPN）接続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。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な場合は、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

本書は、以下の環境で検証をおこなっております。

- Pulse Secure Pulse Connect Secure（バージョン 9.0R2 Build 63965）
  ※以後、「PCS」と記載します
- VMware Workspace ONE UEM（バージョン 18.11.0.4）
  ※以後、「WS1 UEM」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
- Webサーバ：CentOS 7.6.1810 / Apache 2.4.6
  ※以後、「Webサーバ」と記載します。ApacheはOSのパッケージを利用
- Apple iPad (iOS 12.1.1)
  Pulse Secure (バージョン 7.1.1 78493) / Workspace ONE Web (バージョン 7.2.1)
  ※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。

- PCSのVPN設定およびクライアント証明書認証の設定
  ※PCSでの証明書認証設定について、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/pulse-connect-secure
  Per-App VPN接続時にはパスワードなどのユーザ入力待ちが発生してはならないので、本書で

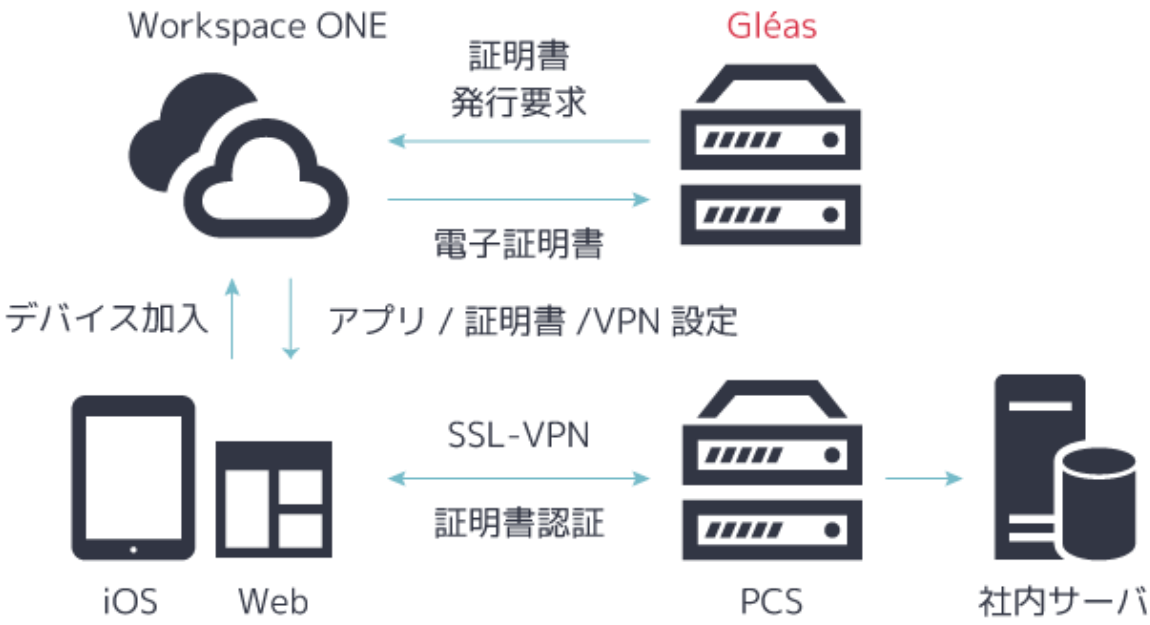
はクライアント証明書認証のみを前提とします

- WS1 UEMの基本操作およびGléasとの証明書発行連携の設定
  ※WS1 UEM（AirWatch）とGléasの証明書発行連携の設定について、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
  事前にWS1 UEMで認証局と証明書発行テンプレートの設定をしておきます
- iPadのネットワーク設定
- Gléasの基本操作

以上については、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。

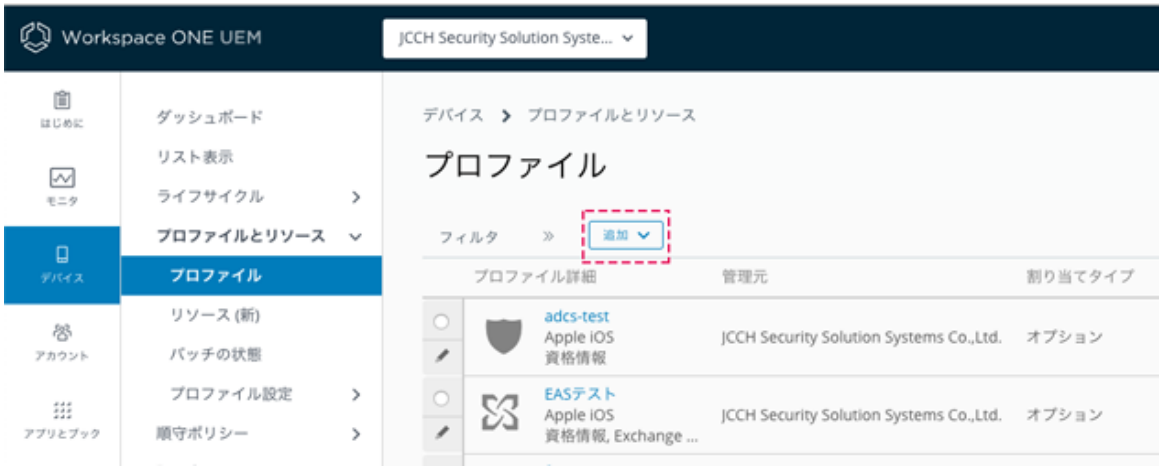


1. iPadで、WS1 UEMへの加入操作をおこなう
2. WS1 UEMはGléasと連携して発行した証明書と、Per-App VPN設定を含むプロファイルをiPadに配布する
3. iPadで、Workspace ONE Webを起動すると自動的にPCSへのVPN接続がおこなわれ、社内サーバにアクセス可能となる。

2. WS1 UEM での Per-App VPN 設定

2.1. プロファイル設定

WS1 UEM の管理画面で、[デバイス]→[プロファイルとリソース]→[プロファイル]と進み、[追加]のドロップダウンリストから[プロファイルを追加]をクリックします。

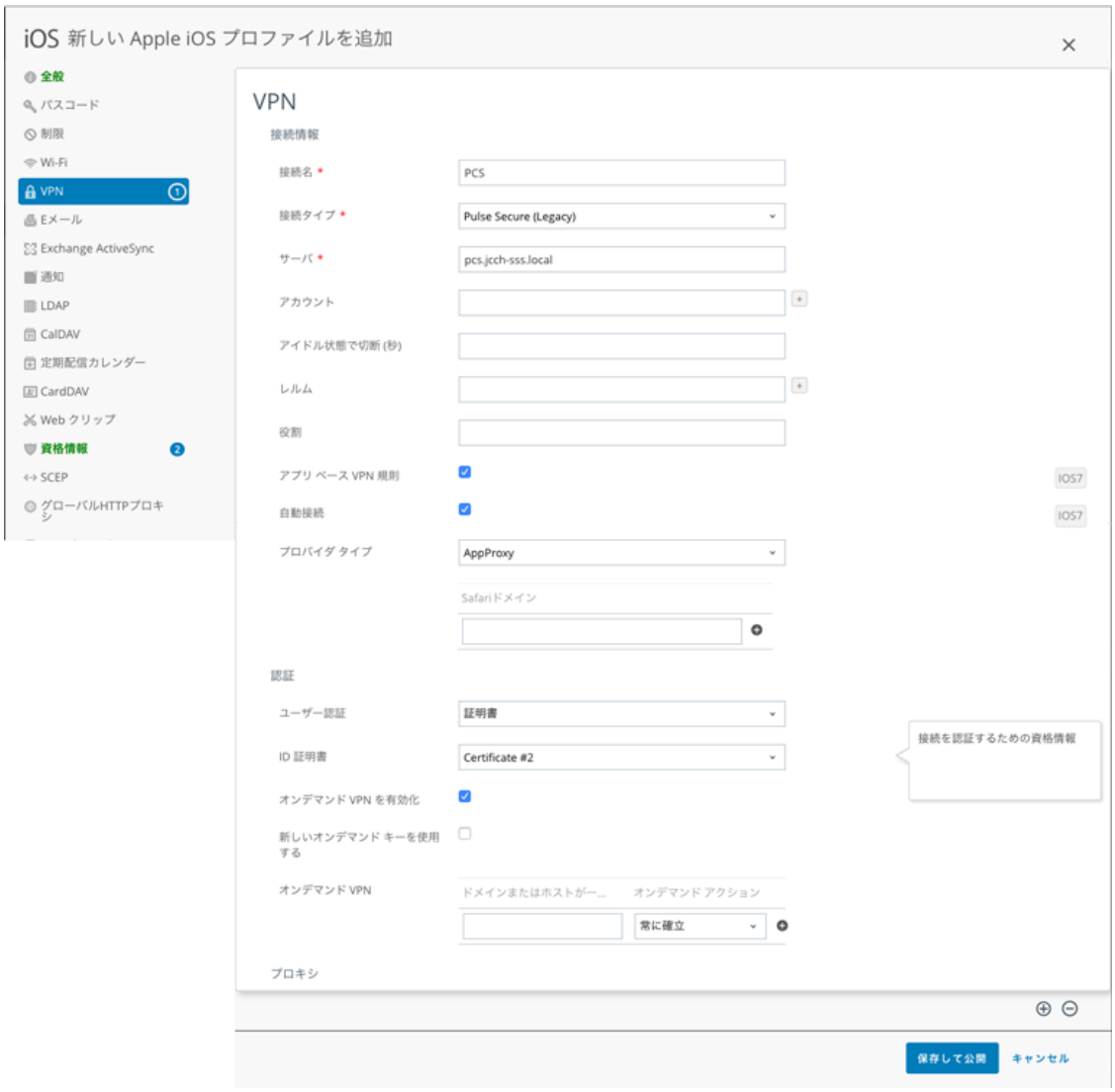


資格情報の項目で、クライアント証明書の発行・配布設定と、ルート証明書の配布設定をおこないます。

※設定内容の詳細は 1.2 項に記載の弊社ホワイトペーパーを参照

VPN の項目で、以下を設定します。

- [接続名]に任意の接続名称を入力
- [接続タイプ]は[Pulse Secure(Legacy)]を選択
- [サーバ]に VPN の接続先ホスト名を入力
- [アプリベース VPN 規則]をチェック
- [プロバイダタイプ]は[AppProxy]を選択
- [ユーザー認証]は[証明書]を選択
- [ID 証明書]には、資格情報プロファイルで設定したクライアント証明書を選択
  ※以下のスクリーンショットは、資格情報の 2 番目にクライアント証明書を設定した場合の例です
- [オンデマンド VPN を有効化]をチェック



設定完了後、[保存して公開]をクリックし対象デバイスへの割り当てをおこないます。

2.2. アプリケーション配布設定

WS1 の管理画面で[アプリとブック]→[ネイティブ]→[パブリック]と進み、[アプリケーションの追加]をクリックし、[Workspace ONE Web]を検索、追加します。

追加したのちに、[編集]タブをクリックし以下の設定をおこないます。

- SDK タブの[SDK プロファイル]で、作成した SDK プロファイルを選択して[保存して割り当て]をクリックします。
  ※SDK プロファイルは、[グループと設定]＞[すべての設定]＞[アプリ]＞[設定とポリシー]＞[プロファイル]で作成できます。Workspace ONE Web の機能制限など各種設定をおこなうことが可能ですが、本書の主旨から外れるので説明は省きます

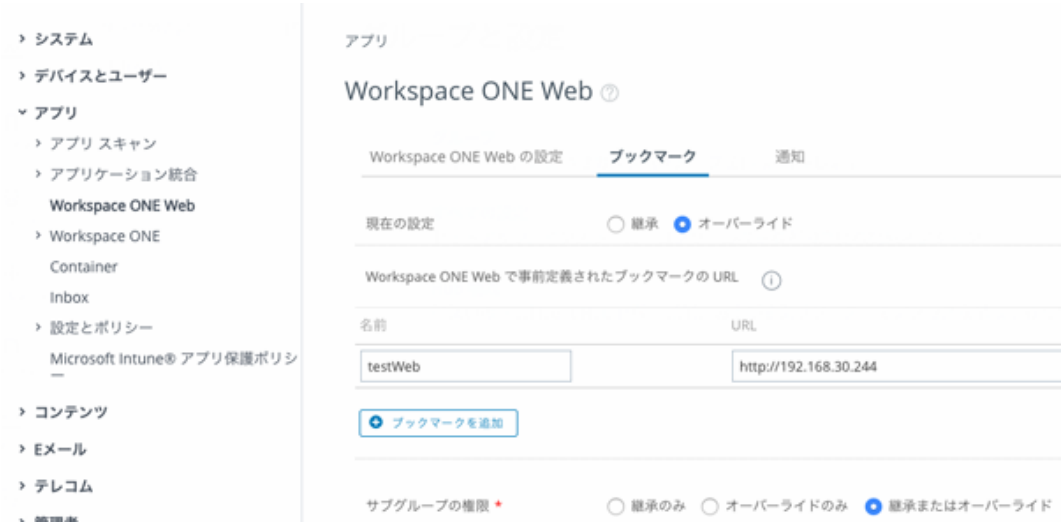
また[割り当て]をクリックして、[割り当ての追加]、或いは既に割り当ててあるグループを選択し、以下の設定をおこないます。

- [管理アクセス]で[有効]を選択
- [アプリトンネル]で[有効]を選択
- [アプリベース VPN プロファイル]で、2.1 項で設定した VPN 項目を含むプロファイルを選択

設定完了後、[保存して公開]をクリックし対象デバイスへの割り当てをおこないます。

2.3. Workspace ONE Webの設定

WS1 の管理画面で[グループと設定]→[すべての設定]→[アプリ]→[Workspace ONE Web]と進みます。
本書の主旨から外れるので詳細設定は省きますが、テスト用 Web サイトの URL をブックマークに追加しておきます。

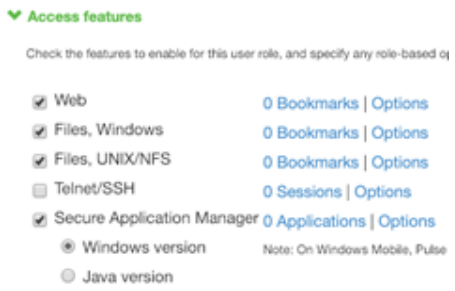


※上のスクリーンショットのようにサーバ URL に IP アドレスを使う場合は、[ブラウザ設定]タブの[IP 閲覧を許可する]を有効にし、[許可された IP アドレス]に Web サーバの IP アドレスを指定する必要があります
設定完了後、[保存]をクリックして設定を保存します。

3. PCS での設定

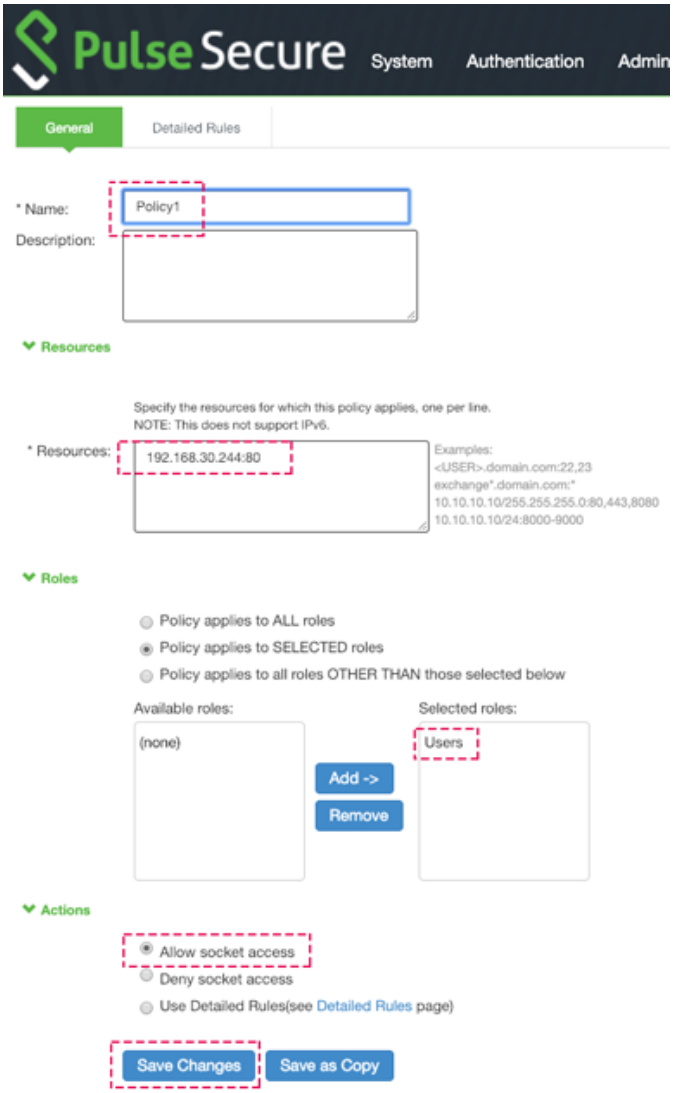
3.1. User Rollの設定

[Users] → [User Roles] で今回使用する User Role をクリックして設定を開きます。
[Access features] → [Secure Applycation Manager] で[Windows version]を選択して[Save Changes]をクリックします。



3.2. SAM Access Controlの設定

[Users] → [Resource Policies] → [SAM] → [Access Control]と進み、[New Policy]をクリックします。[Name]に任意の名前を、[Resources]にイントラサーバのドメイン名あるいは IP アドレスと使用ポートを、[Roles]では[Policy apply to SELECTED roles]を選択し、適用させる Role を[Selected roles]に加え、[Actions]で[Allow ～]を選択し、[Save Changes]をクリックします。



4. iPad での Per-App VPN の実行

4.1. WS1 UEMへの加入とWorkspace ONE Webのインストール

iPad で WS1 UEM に加入すると、WS1 UEM と Gléas との間で証明書発行がおこなわれ、少しの時間が経つと SSL-VPN 接続設定やクライアント証明書を含むプロファイルが自動インストールされます。

また WS1 UEM 加入後に、2.2 項で設定した通り Workspace ONE Web をインストールする旨のメッセージが表示されるのでそれに従いインストールをおこないます。

プロファイルは iPad の[設定]アプリで[一般] > [プロファイルとデバイス管理]と進み、[デバイスマネージャ]という名前でインストールされ、タップすることで内容を確認できます。

またその状態で Pulse Secure アプリを起動すると、[アプリごとの]欄で Per-App VPN が追加されていることがわかります。・

4.2. Per-App VPNの動作確認

iPad で Workspace ONE Web を起動すると、自動的に VPN 接続がおこなわれます。接続時には iPad 画面の右上に VPN マークが表示されます。

ブックマーク設定してあるイントラ Web サーバへアクセスできるようになっています。

Workspace ONE Web を閉じると VPN マークの表示は消えます。同じ URL に対して Safari などの他のブラウザでアクセスしても、VPN に接続できないため、エラーとなります。

5. 問い合わせ

■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

■Pulse 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

■Gléasに関するお問い合わせ先

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