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

クライアント証明書による認証設定

Ver.2.1
2019 年 1 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」で発行したクライアント証明書を利用して、Pulse Secure社のSSL-VPN装置「Pulse Connect Secure」を利用してのトンネリング接続を行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
- 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：Windows 10 Pro / Internet Explorer 11
  ※以後、「PC」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
  ※本書記載の内容は他のiPadシリーズやiPhone・iPod touchにも適用できます

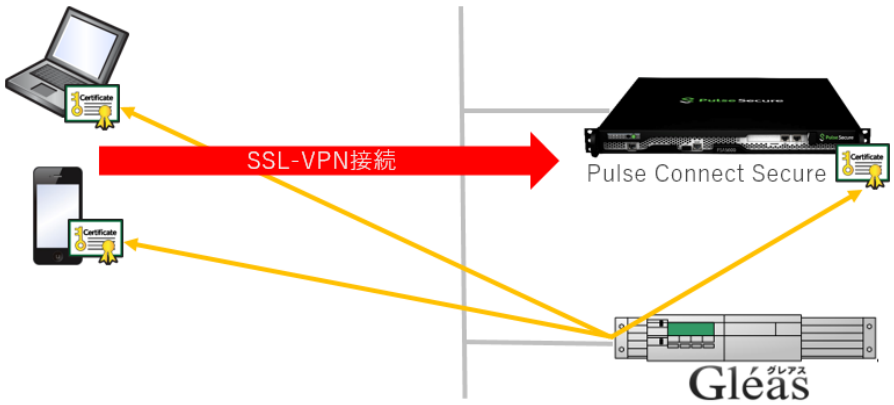
以下については、本書では説明を割愛します。

- Connect Secureでのサーバ証明書設定やネットワーク設定、アクセス権限等の設定
- Gléasでのユーザ登録やクライアント証明書発行等の基本設定
- PC・iPadでのネットワーク設定等の基本設定
- Pulse Secureクライアント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. Gléasは、Connect Secureにサーバ証明書を、PCとiPadにクライアント証明書を発行する
2. Connect Secureに発行されたサーバ証明書を設定する
3. PCとiPadは、Gléas(UA)よりクライアント証明書をインポートする
4. Pulse Secureに、クライアント証明書を使ってVPNアクセスをする

2.7項では、Connect SecureのLocation Awareness機能を利用したPCでのVPN自動接続について記載します。

※5.1項の[Pulse Secure SSL-VPNの設定]で、[オンデマンド接続先]を設定することによりiPadでもVPN自動接続を行うことが可能です

7項では、Connect Secureのデバイスオンボーディング機能を利用した証明書配布について記載します。

1.4. 証明書発行時における留意事項

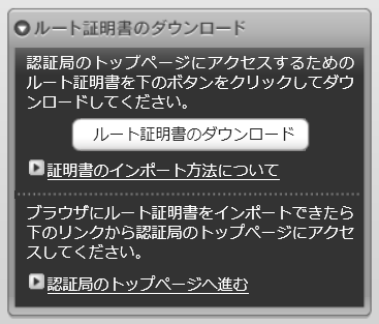
Gléasで電子証明書を発行する際に以下の点に留意する必要があります。

- 本書2.2の方法でサーバ証明書を発行する場合は、事前にサーバアカウントを作成しておく必要があります。

2. Connect Secureの設定

2.1. 信頼するルート認証局の設定

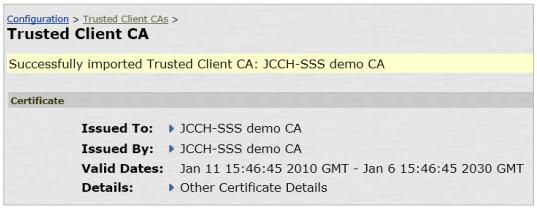
今回利用するクライアント証明書のトラストアンカとなるルート認証局を設定します。
あらかじめ Gléas よりルート証明書をダウンロードしておきます。
Gléas に http://hostname/ （http であることに注意）でアクセスすると、ダウンロードが可能です。



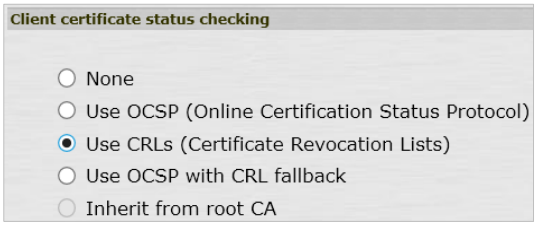
管理者画面左側のメニューより[Configuration] > [Certificates] > [Trusted Client CAs]と進み、右側に出現する[Import CA Certificate…]ボタンをクリックします。

[Import From:]のところで[参照]ボタンを押し、ローカルに保存してあるルート証明書を選択し、[Import Certificate]ボタンをクリックします。

成功すると以下のような画面が現れます。



失効リスト（CRL）を利用したクライアント証明書の失効確認をおこなう場合は、Client certificate status checking 項目で、[Use CRLs (Certificate Revocation Lists)]を選択します

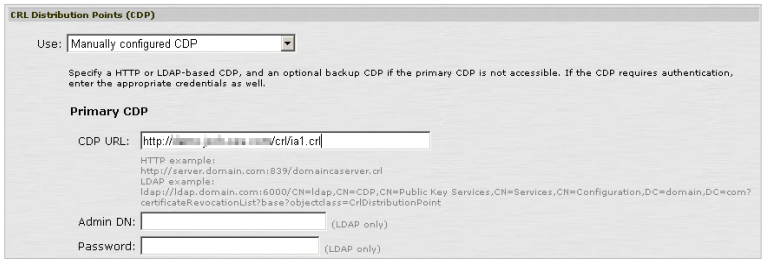


ここで一度[Save Setting]をクリックして、設定を保存します。

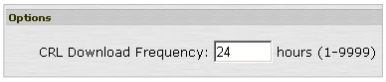
その後、画面最下部にある CRL Setting の項目で、[CRL Checking Options…]をクリックします。
CRL Checking Option の設定画面に移動しますので、以下の設定をおこないます。

- [Use:]のドロップボックスより[Manually Configured CDP]を選択
- Primary CDP の[CDP URL]に CRL 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

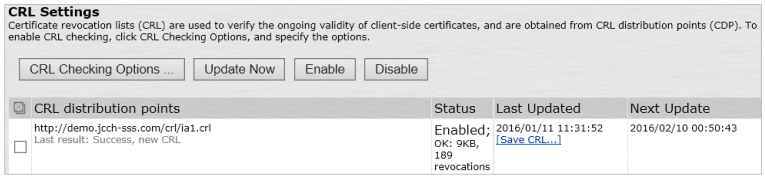
以下は Gléas が http で公開している CRL を取得する場合の設定例となります。



また CRL の取得間隔を指定したい場合は、Options 項目で[CRL Download Frequency]を指定することにより可能です。
以下は CRL の有効期限に関係なく、24 時間毎に CRL を取得する場合の設定例です。

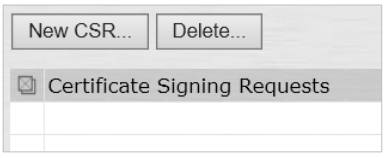


設定終了後、[Save Setting]をクリックして設定を保存してします。
遷移した画面の CRL Setting の Status 欄に Enabled と表示されます。



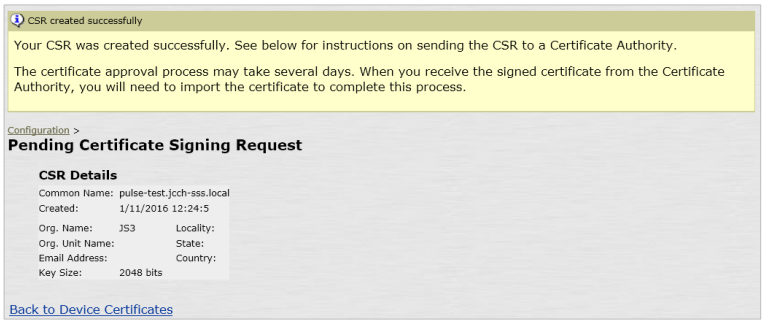
2.2. サーバ証明書の設定

管理者画面左側のメニューより[Configuration] > [Certificates] > [Device Certificates]と進みます。その後、[New CSR...]をクリックし証明書署名要求(CSR)を発行します。

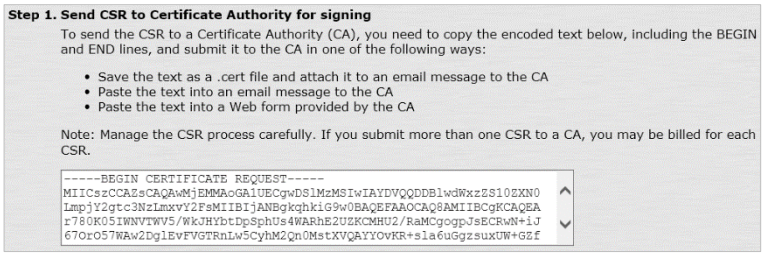


ホスト名など、必要事項を入力し[Create CSR]をクリックします。
以下はRSA2048ビットの鍵長でCSRを作成する例です。
※1024ビットは現在推奨されない鍵長となるので、それ以上の鍵長にすることを推奨します
※Gléasでは、3072ビットの鍵長はサポートされないため2048を選択します

CSRの生成がおこなわれます。



画面下部のテキストエリアにCSRが表示されます。
この内容をテキストファイルに保存します。



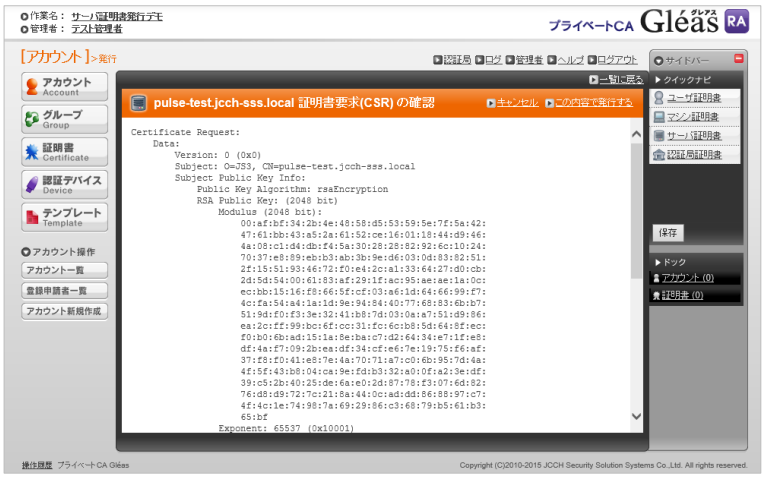
Gléas（RA）にログインし、該当のサーバアカウントのページへ移動します。
小メニューの[証明書発行]をクリックします。

上級者向け設定を展開し、以下の操作をおこないます。

- 証明書要求（CSR）ファイルをアップロードする：の[参照…]ボタンよりダウンロードした CSR ファイルを選択
- [CSR ファイルの内容を確認する]にチェック

その後、[発行]ボタンをクリックします。

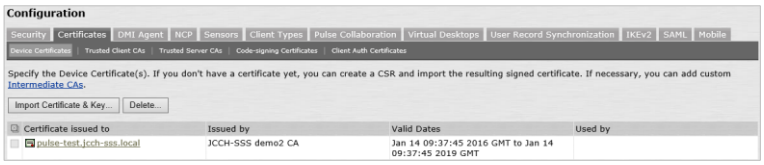
証明書の要求内容が表示されるので確認し、[▶この内容で発行する]をクリックし、証明書の発行をおこないます。



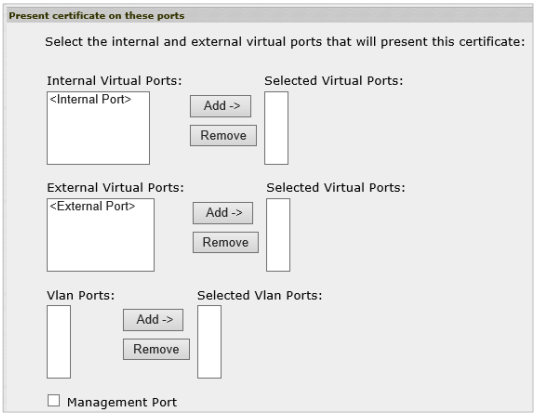
証明書発行完了後、証明書詳細画面の証明書ファイル欄の「証明書：あり」をクリックし、発行された証明書をダウンロードします。

Connect Secure に戻り、ダウンロードした証明書を指定し、[Import]をクリックしアップロードします。

以上でサーバ証明書の登録が完了です。
Device Certificates にアップロードした証明書が表示されます。



※複数のサーバ証明書が格納されている場合は、クライアントからのアクセスを受け付けるポートを指定する必要があります。上の画面の証明書名のリンクをクリックすることでその設定がおこなえます



2.3. 認証サーバの設定

左側のメニューから[Auth. Server]をクリックし、右側の画面の[New:]のドロップダウンより[Certificate Server]を選択し、[New Server…]をクリックします。
認証サーバの設定画面に移動するので、以下の設定を行います。

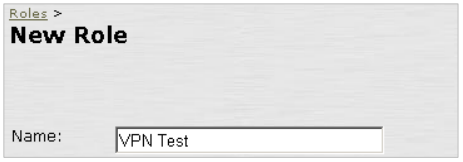
- [Name:]には、一意の認証サーバ名称を入力
- [User Name Template:]にはConnect SecureでユーザIDとして扱う属性を指定
  ※クライアント証明書のサブジェクトCN（Common Name）を利用するケースでは、デフォルトで入っている <certDN.CN> のままにしておきます

設定終了後、[Save Change]をクリックして設定を保存してください。

2.4. ロール（ユーザ権限）の作成

左側のメニューより[User Roles] > [New User Role]をクリックします。
ロールの作成画面に移動しますので、以下の設定を行います。

- [Name:]に一意のロール名称を入力
- [Options]の欄で、[Pulse Secure Client]にチェック
- [Access features]の欄で、[VPN Tunneling]にチェック
- 必要に応じその他の項目を設定



設定終了後、[Save Change]をクリックして設定を保存してください。

画面上部の[VPN Tunneling]タブを選択し、トンネリングに関する設定を行います。
※ここではクライアントへのIPアドレス割当設定のみを記載します。その他各種設定（アクセスコントロール、接続プロファイル、スプリットトンネル、帯域幅の管理等）については説明を割愛します。ネットワーク環境やポリシーに応じて設定を行ってください

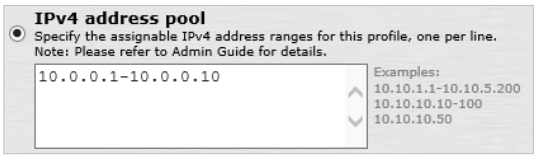
画面最下部の[Connection Profiles]リンクをクリックします。

Network Connect Connection Profiles画面に移動します。[New Profiles]ボタンをクリックし、プロファイルの作成画面に移動しますので以下の設定を行います。

- [Name:]には、一意のルール名称を入力
- IP address assignmentの項目に、クライアントに対するIPアドレスの配布方法を選択（既存のDHCPサーバを利用か、管理者が割り当てるIPアドレスレンジを設定）
- 必要に応じその他の項目を設定

以下はクライアントに対し、10.0.0.1から10.0.0.10までのアドレスを割り当てる設

定例となります。



設定終了後、[Save Change]をクリックして設定を保存してください。

2.5. レルム（ユーザ認証）の作成

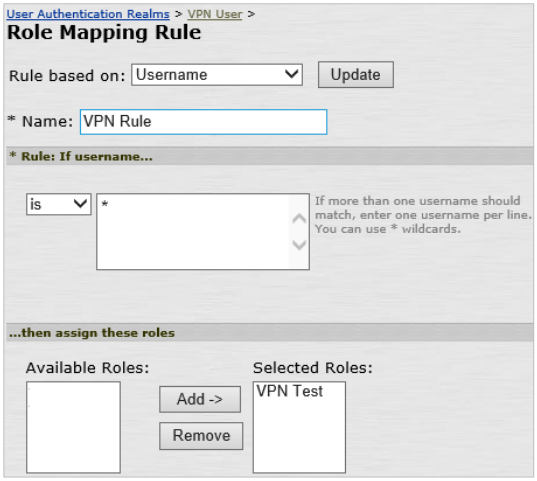
左側のメニューより[User Realms] > [New User Realm]をクリックします。
Realm の作成画面に移動しますので、以下の設定を行います。

- [Name:]には、一意のレルム名称を入力
- [Authentication:]には、2.3項で設定した認証サーバを選択
- 必要に応じその他の項目を設定

設定終了後、[Save Change]をクリックして設定を保存してください。その後、Role Mapping設定画面に移動しますので、[New Rule…]をクリックします。
Role Mapping Rule画面に移動しますので、以下の設定を行います。

- [Rule based on:]には、ドロップダウンメニューより[Username]を選択し、
  ※[Certificate]を選択した場合、証明書サブジェクトOU等による制御が可能
- [Name:]には、一意のルール名称を入力
- [Rule: If username...]項目にはこのロールを適用するユーザ名を入力
  ※ワイルドカード "*" の利用も可能
- [...then assign these roles]項目には、2.4項で作成したロールを選択
- 必要に応じその他の項目を設定

以下は、有効なクライアント証明書が提示された場合、証明書のサブジェクトCN（2.3項でユーザIDとして設定済み）が何であろうと「VPN Test」というロールにマッピングする例です。



設定終了後、[Save Change]をクリックして設定を保存してください。

2.6. サインインポリシの設定

左側のメニューから[Signing-in] > [Sign-in Policies]をクリックし、右側の画面のUser URLsの[*/]（ユーザ用のデフォルトページ）をクリックします。
その後、当該ログインページの設定画面に移動するので、[Authentication realm]の項目で以下を設定します。

- [User picks from a list of authentication realms]を選択
- [Available Realm]ボックスにある2.5で作成したレルムを、[Selected Realm]ボックスに移動

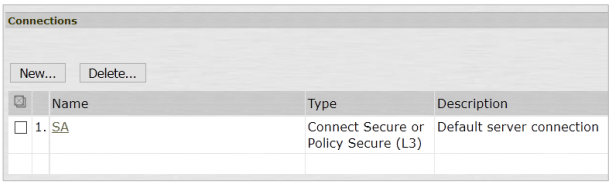
設定終了後、[Save Change]をクリックして設定を保存してください。

2.7. Location Awareness の設定

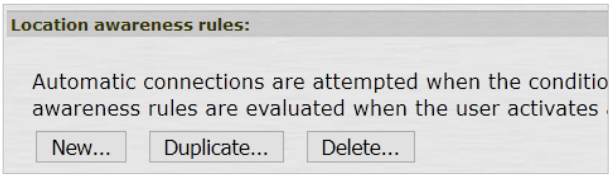
※本項は、1.3項で言及したLocation Awareness機能を利用したPCでのVPN自動接続をおこなう

場合にのみ必要な設定なります

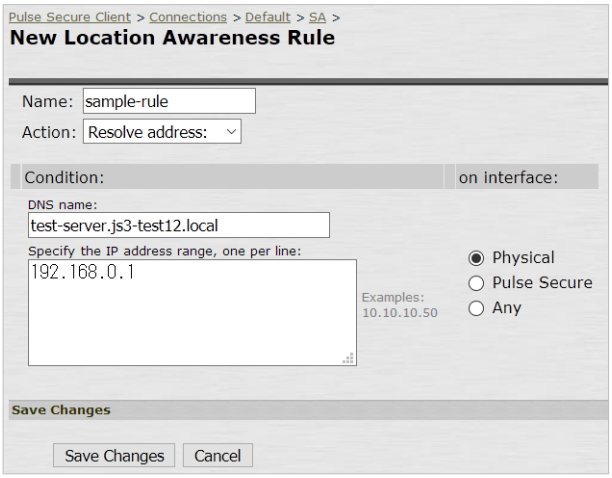
左側のメニューから[Users] > [Pulse Secure Client] > [Connections]を選択し、右側の画面で Default をクリックします。
その次の画面の Connections にて SA をクリックします。



Location awareness rules: より自動接続させるルールを設定するため。[New...]をクリックします。



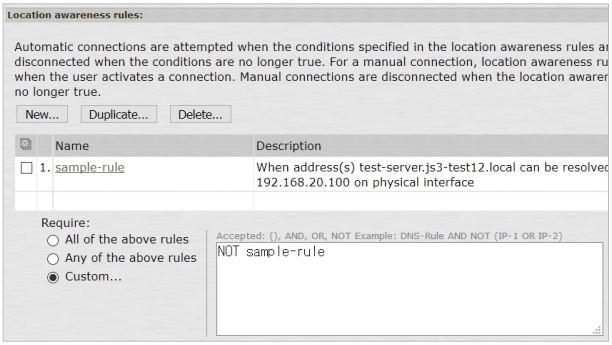
自動接続の条件を設定します。
以下は、「物理ネットワークインターフェースで、test-server.js3-test12.localが192.168.0.1に解決される」ことを設定した例です。



設定後、[Save Changes]をクリックして保存します。

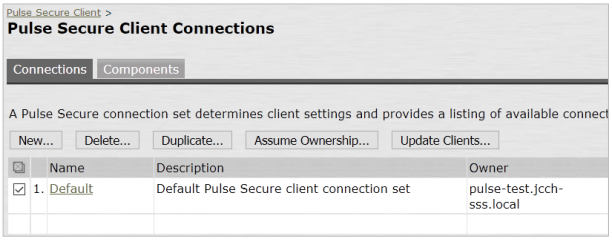
Location awareness rules:で以下の通り設定します。

- Require:の部分に、[Custom...]を選択
- Accepted:の部分に、[NOT sample-rule]とします。



これにより「物理ネットワークインターフェースで、test-server.js3-test12.localが192.168.0.1に解決されない場合にVPN自動接続」となります。

また、PC側のクライアントソフトウェア（Pulse Secure Client）へこの設定を反映させるため以下をおこないます。
[Users] > [Pulse Secure Client] > [Connections]を選択し、対象の設定をチェックして[Update Clients]をクリックして、その後確認画面が表示されるので[Update]をクリックします。



※Location AwarenessルールがPCに反映されるのは、次回のPulse Secure ClientでのVPN接続後となります

3. Gléas の管理者設定（PC）

GléasのUA（申込局）より発行済み証明書をPCにインポートできるよう設定します。
※下記設定は、Gléasの納品時に弊社で設定をおこなっている場合があります

GléasのRA（登録局）にログインし、画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、設定を行うUAをクリックします。

[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

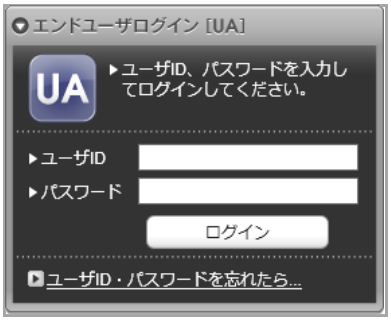
- [証明書ストアへのインポート]をチェック
- [証明書ストアの選択]で[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]にチェック

設定終了後、[保存]をクリックし設定を保存します。

4. PC での接続操作

4.1. クライアント証明書のインポート

Internet Explorer で Gléas の UA にアクセスします。
ログイン画面が表示されるので、ユーザ ID とパスワードを入力しログインします。



ログインすると、ユーザ専用ページが表示されます。
[証明書のインポート]ボタンをクリックすると、クライアント証明書が証明書ストアにインポートされます。
※初回ログインの際は、ActiveX コントロールのインストールを求められるので、画面の指示に従いインストールを完了してください。

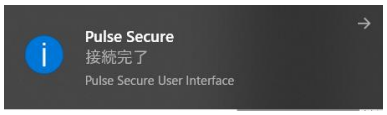
「インポートワンス」を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度のインポートを行うことはできません。

4.2. クライアントからのVPN接続（PC）

2.6項で設定したConnect Secureのサインインページに、Pulse Secure クライアントから接続すると、証明書認証がおこなわれたのちに接続します。
（証明書が一枚しかない場合は、それがバックグラウンドで自動的に選択されます）

失効された証明書でアクセスすると以下のエラーが表示されます。

Location Awarenessが設定されている場合は、事前設定した条件が満たされる場合に自動的にVPN接続がおこなわれます。
VPN接続がバックグラウンドでおこなわれると、タスクバーに以下のメッセージが表示されます。



5. Gléasの管理者設定（iPad）

Gléas で、発行済みのクライアント証明書を含む Pulse Secure 接続設定（構成プロファイル）を iPad にインポートするための設定を本章では記載します。

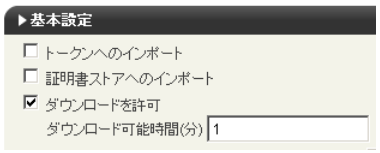
※下記設定は、Gléas 納品時等に弊社で設定を既に行っている場合があります
※Pulse Secure 用の構成プロファイル生成機能は Gléas ではオプションとなります。詳細は最終項の問合せ先までお問い合わせください

5.1. UA（ユーザ申込局）設定

GléasのRA（登録局）にログインし、画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、設定を行うUAをクリックします。

[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [ダウンロードを許可]をチェック
- [ダウンロード可能時間(分)]の設定
  この設定を行うと、GléasのUAからダウンロードしてから、指定した時間（分）を経過した後に、構成プロファイルのダウンロードが不可能になります（「インポートロック」機能）。このインポートロックにより複数台のiPadへの構成プロファイルのインストールを制限することができます。



[認証デバイス情報]の[iPhone/iPadの設定]までスクロールし、[iPhone/iPad用UAを利用する]をチェックします。

構成プロファイル生成に必要となる情報を入力する画面が展開されるので、各項目を入力します。

- [名前]、[識別子]、[プロファイルの組織名]、[説明]は必須
- [削除パスワード]を設定すると、利用者が設定プロファイルを削除する際に管理者が定めたパスワードが必要となり、利用者の誤操作等による構成プロファイルの削除を防止できます。
  ※ここでパスワードを設定した場合でも、Pulse Secureアプリから接続設定を削除することはできてしまうため注意が必要

さらに[Pulse Secure SSL-VPNの設定]項目に以下を設定します。

- [SSL-VPN 接続名]に、任意の接続名を入力（必須）
- [SSL-VPN ホスト名]に、接続先のConnect Secureのホスト名（或いはIPアドレス）を入力（必須）
- [オンデマンド接続先]に、自動VPN接続のトリガとなる文字列（ドメイン名など）を入力（オプション）

  ※ここで指定された接続先（後方一致）が、名前解決できない場合に自動的にVPN接続を開始します（アプリケーションがオンデマンドVPNに対応している必要があります）

  例：ここに“.js3-test12.local”を指定すると、safariで“http://www.js3-test12.local/”にアクセスすると後方一致の条件を満たすので自動的にVPN接続がおこなわれます

各項目の入力が終わったら、 [保存]をクリックします。
以上でGléasの設定は終了です。

6. iPad での接続操作

6.1. Pulse Secureのインストール

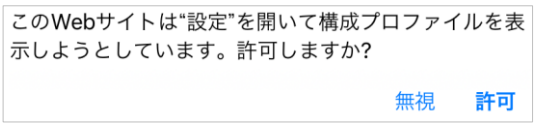
iPadでPulse Secureを利用する場合は、クライアントソフトウェアのダウンロードが必要です。App Store より事前にインストールを行ってください。
本書ではPulse Secureのインストール方法については割愛します。

6.2. クライアント証明書のインポート

iPadのブラウザ（Safari）でGléasのUAサイトにアクセスします。
ログイン画面が表示されるので、ユーザIDとパスワードを入力しログインします。

ログインすると、そのユーザ専用ページが表示されるので、[ダウンロード]をタップし、構成プロファイルのダウンロードを開始します。
※インポートロックを有効にしている場合は、この時点からカウントが開始されます

自動的にプロファイル画面に遷移するので、構成プロファイルの表示を[許可]し、その後に[インストール]をタップします。



※[詳細]をタップすると、インストールされる証明書情報を見ることが可能ですので、ルート証明書のフィンガープリントなどを必要に応じ確認します

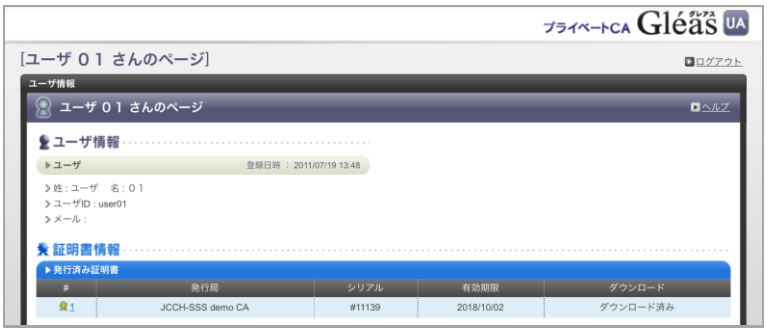
以下のプライベート認証局のルート証明書のインストール確認画面が現れますので、[インストール]をクリックして続行します。

インストール完了画面になりますので、[完了]をタップします。

元のUA画面に戻りますので、[ログアウト]をタップしてUAからログアウトします。

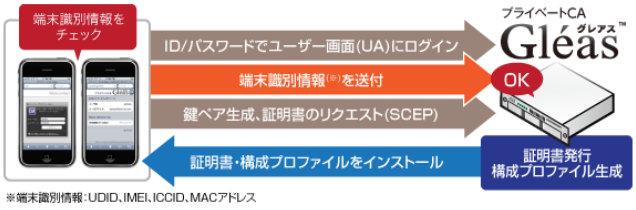
以上で、iPadでの構成プロファイルのインストールは終了です。
なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り

「ダウンロード済み」という表記に変わり、以後のダウンロードは一切不可となります。



6.3. OTAエンロールメントを利用した証明書発行について

Gléasでは、iOSデバイスに対するOver The Air（OTA）エンロールメントを利用した証明書の発行・構成プロファイルの配布も可能です。
OTAを利用すると事前に指定した端末識別番号を持つ端末だけに証明書の発行を限定することも可能になります。

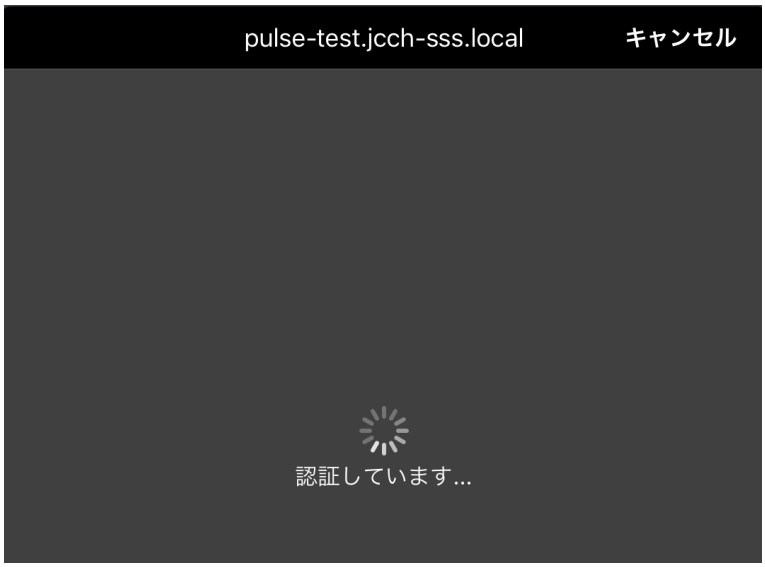


詳細は最終項のお問い合わせ先までお問い合わせください。

6.4. Pulse Secureから接続

インポートが完了すると、Connect Secureへの接続に利用するクライアント証明書やVPN接続先が設定されています。
Pulse Secure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

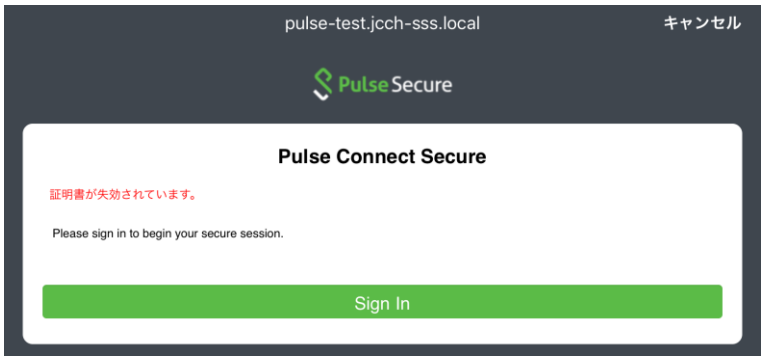
以下はPulse Secureから接続した画面です。



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。

証明書を持っていない場合、失効された証明書を提示した場合（※）は接続失敗の表示になります。以下は失効された証明書でアクセスした場合の表示となります。

※該当する証明書の失効情報を含むCRLがConnect Secureに伝搬されている必要があります



7. オンボーディングを利用した証明書配布

7.1. Gléasでの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。

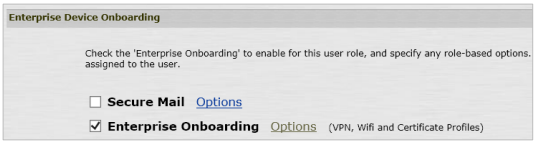
登録局詳細の「▶SCEP の設定」で、以下設定をおこないます。

- 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 Connect Secure 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”の形式で接続許可する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。

7.2. Connect Secureでの設定

管理者画面左側のメニューの[User Roles]より、Onboarding を利用するロールの設定画面で[Enterprise Onboarding]をチェックします。

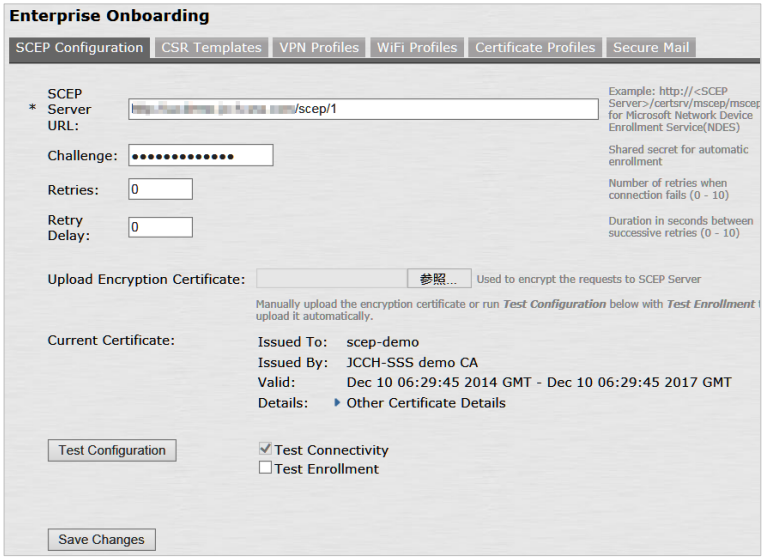


その後、[Save Changes]をクリックし、設定を保存します。

また、必要に応じオプションも設定します。

管理者画面左側のメニューの[Enterprise Onboarding] > [SCEP Configuration]と進み、[SCEP Configuration]タブで以下設定をおこないます。

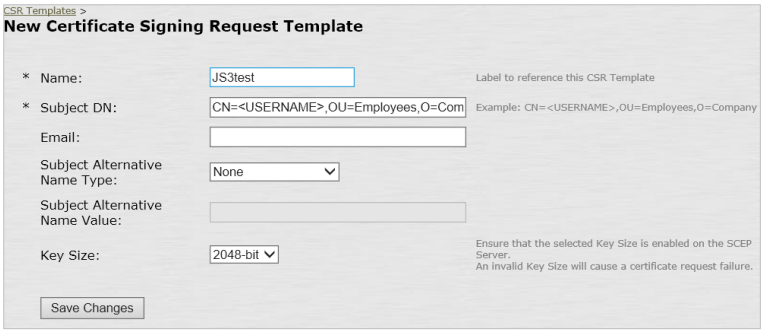
- [SCEP Server URL]には、Gléas の SCEP 用 URL を入力します
  ※URL は以下の形式で入力します。
  http(s)://[Gléas UA ホスト名]/scep/[認証局番号]
  例：デフォルトの認証局で発行する場合： http://ua.example.com/scep/1
- [Challenge]には、Gléas で設定したチャレンジ値を入力します
- [Upload Encryption Certificate:]には、Gléas にアップロードした SCEP 用の証明書を設定します
  ※PKCS#12 ファイル（*.p12）ではなく、証明書ファイル（*.crt）を Gléas よりダウンロードしてここの設定をおこないます



設定後に、[Save Changes]をクリックし保存します。

[CSR Template]タブで[New CSR Template]をクリックし、CSR テンプレートの設定をおこないます。

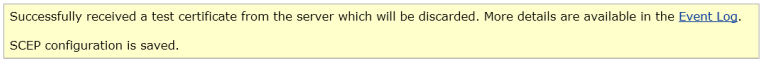
- [Name]には、任意の設定名を入力
- [Subject DN]には、証明書のサブジェクトになるものを入力
  CN=<USERNAME>とすることで、Connect Secure のユーザ ID を証明書サブジェクト CN とすることができます。
  また、Gléas には Connect Secure のユーザ ID と同一のアカウントが作成されている必要があります（Gléas は未登録ユーザ ID への証明書発行を拒否します）。



設定後に、[Save Changes]をクリックし保存します。

[SCEP Configuration]タブに戻り、接続及び証明書発行のテストをおこないます。
※Connect Secure の管理ユーザ ID と同一のアカウントを Gléas にあらかじめ作成しておく必要があります

成功すると、以下のメッセージが表示されます。



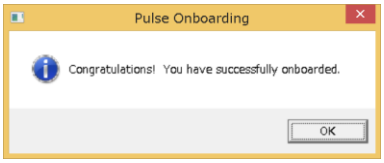
[Certificate Profile]タブで、証明書の配布設定をおこないます。

- [Import and Use CA Certificate]にチェックを入れ、クライアントに送信するルート証明書をアップロード
- [Generate per User Certificate]にチェックを入れ、設定したCSRテンプレートを選択

設定後、[Save Changes]をクリックして設定を保存します。

Onboarding機能がオンになった状態でWindowsからWebアクセスをおこなうと、[オンボード]タブが表示されます。

画面表示にしたがい、オンボーディングを実行します。成功すると以下のダイアログが表示されます。



8. 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

■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