



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 Policy Secureでの802.1x EAP-TLS認証設定

Ver. 1.0

2018 年 2 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  
Pulse Policy Secure での 802.1x EAP-TLS 認証設定

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
2. Policy Secure の設定 .....	5
2.1. 信頼するルート認証局の設定 .....	5
2.2. サーバ証明書の設定 .....	8
2.3. User Realm 設定 .....	12
2.4. Authentication Protocol Set 設定 .....	14
2.5. Sign-in Policy の設定 .....	15
2.6. Location Group および RADIUS Attributes 設定 .....	15
3. Gléas の管理者設定 (Windows PC) .....	17
3.1. UA (ユーザ申込局) 設定 .....	17
4. Windows PC での証明書インポート・無線 LAN 設定 .....	18
4.1. Gléas の UA からのインストール .....	18
5. Gléas の管理者設定 (iPad) .....	19
5.1. UA (ユーザ申込局) 設定 .....	19
6. iPad での構成プロファイル・証明書のインストール .....	21
6.1. Gléas の UA からのインストール .....	21
6.2. OTA エンロールメントを利用した証明書発行について .....	24
7. クライアントからの接続 .....	24
8. 問い合わせ .....	25

## 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社製ネットワークアクセス制御機器「Pulse Policy Secure」を利用した802.1x EAP-TLS接続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 Secure Policy Secure (バージョン5.4R1 (build 42499))  
※以後、「Policy Secure」と記載します
  - プライベート認証局Gléas (バージョン1.14.6)  
※以後、「Gléas」と記載します
  - 無線LANアクセスポイント：AirMac Extreme (バージョン7.6.9)
  - クライアント (PC)：Windows 10 Pro  
※以後、「Windows PC」と記載します
  - クライアント (タブレット)：iPad Air 2 (iOS10.3.2)  
※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

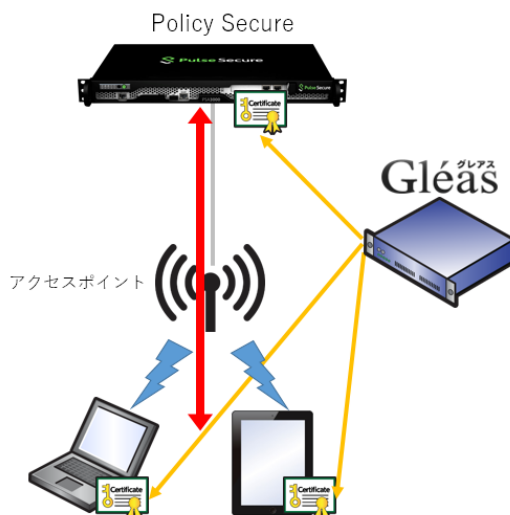
以下については、本書では説明を割愛します。

- Policy Secureでの基本的なネットワーク設定、RADIUSクライアント（無線LANアクセスポイント）の追加方法
- Gléasでのユーザ登録やクライアント証明書発行等の基本操作・設定
- PC・iPadの操作方法

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、Policy Secureにサーバ証明書、Windows PCとiPadにクライアント証明書を発行する。
2. 管理者はPolicy Secureにサーバ証明書を設定する。
3. ユーザは、Gléasの利用者Web画面（UA）より証明書をWindows PCとiPadにインポートする。同時に、無線LANの接続プロファイルもインポートする。
4. Windows PCとiPadからEAP-TLS認証による無線LANアクセスをおこなう。

## 2. Policy Secureの設定

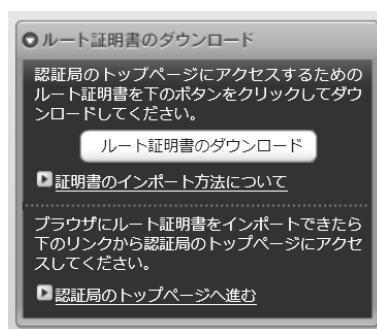
### 2.1. 信頼するルート認証局の設定

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。

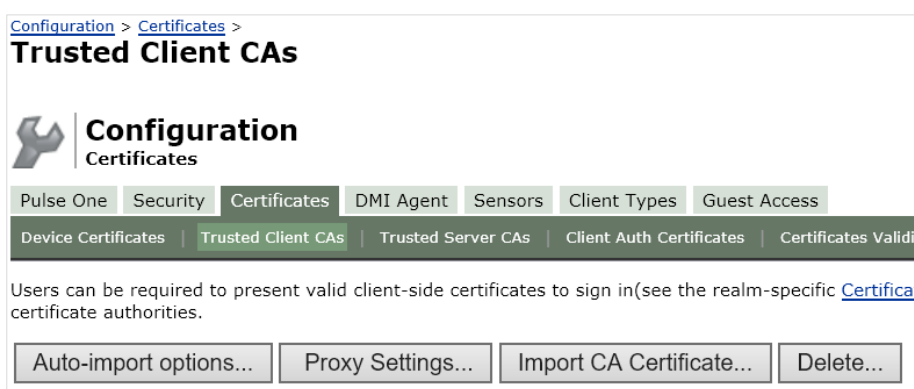
あらかじめ Gléas よりルート証明書をダウンロードしておきます。

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。

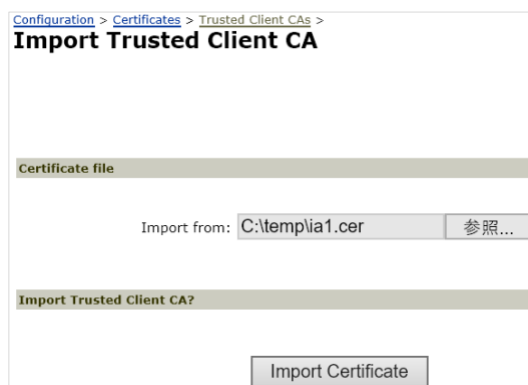
プライベート認証局 Gléas ホワイトペーパー  
Pulse Policy Secure での 802.1x EAP-TLS 認証設定



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。

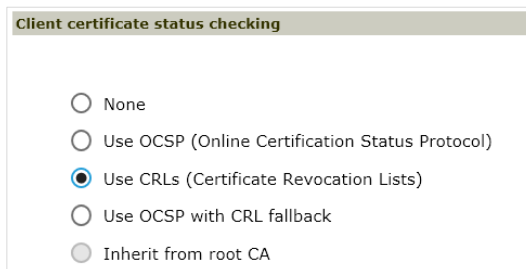


成功すると以下のような画面が現れます。

プライベート認証局 Gléas ホワイトペーパー  
Pulse Policy Secure での 802.1x EAP-TLS 認証設定



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



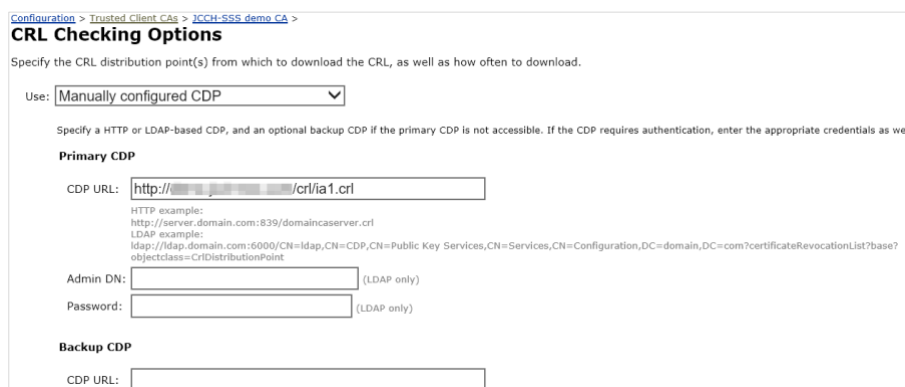
ここで一度[Save Setting]をクリックして、設定を保存します。

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。

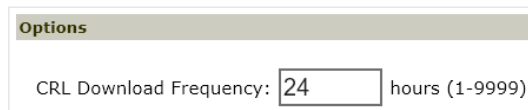
- [Use:]のドロップボックスより[Manually Configured CDP]を選択
- Primary CDP の[CDP URL]に CRL 配布ポイントとなる URL を入力  
※CRL 配布点が複数ある場合は、Backup CDP を設定します

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となります。

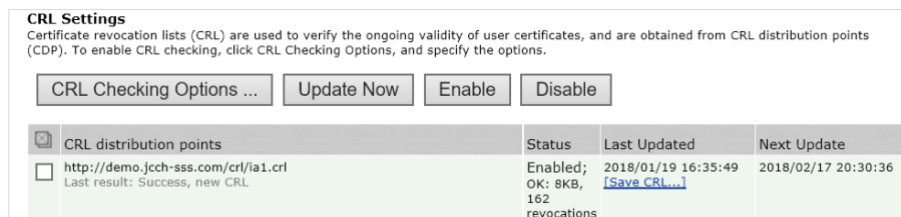


Options

CRL Download Frequency:  hours (1-9999)

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。

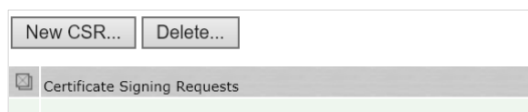


**CRL Settings**  
Certificate revocation lists (CRL) are used to verify the ongoing validity of user certificates, and are obtained from CRL distribution points (CDP). To enable CRL checking, click CRL Checking Options, and specify the options.

CRL distribution points	Status	Last Updated	Next Update
<input type="checkbox"/> <a href="http://demo.jcch-sss.com/crl/ia1.crl">http://demo.jcch-sss.com/crl/ia1.crl</a> Last result: Success, new CRL	Enabled; OK: 8KB, 162 revocations	2018/01/19 16:35:49 <a href="#">[Save CRL...]</a>	2018/02/17 20:30:36

## 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。



☐ Certificate Signing Requests

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。



プライベート認証局 Gléas ホワイトペーパー  
Pulse Policy Secure での 802.1x EAP-TLS 認証設定

[Configuration](#) > [Certificates](#) >  
**New Certificate Signing Request**

Use this page to create a new Certificate Signing Request (CSR) to send to your Certificate Authority of choice.

Common Name:  
(e.g., secure.company.com)

Organization Name:  
(e.g., Company Inc.)

Org. Unit Name:  
(e.g., IT Group)

Locality:  
(e.g., SomeCity)

State (fully spelled out):  
(e.g., California)

Country (2 letter code):  
(i.e., US)

Email Address:


Key Type: ☒ RSA ☐ ECC

Key Length:  bits

Please enter some random characters to augment the system's random key generator.  
We recommend that you enter approximately twenty characters.

Random Data:  
(used for key generation)

CSRの生成がおこなわれます。

 **CSR created successfully**

Your CSR was created successfully. See below for instructions on sending the CSR to a Certificate Authority.

The certificate approval process may take several days. When you receive the signed certificate from the Certificate Authority, you will need to import the certificate to complete this process.

[Configuration](#) >  
**Pending Certificate Signing Request**

**CSR Details**

Common Name:	pulse-test.js3-test12.local		
Created:	1/19/2018 17:18:55		
Org. Name:	JS3	Locality:	
Org. Unit Name:		State:	
Email Address:		Country:	
Key Size:	2048 bits		

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。

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

To send the CSR to a Certificate Authority (CA), you need to copy the encoded text below, including the BEGIN and END lines, and submit it to the CA in one of the following ways:

- 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 a CA, you may be billed for each CSR.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICuzCCAaMCAQAwOjELMAkGA1UEBhMCSlAxDDAKBgNVBAoMA0pTMzEdMBsGA1UE
AwwUcHBzImpzMy10ZXN0MTIubG9jYWwwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQC5hJNlYecIt8KiSpTbjrYsNxPzg+AxvyI3grAnUwnaRkdnE0tXdGQL
InAMKz1S2zHcfNKvadBcoq5U4bFMqXX/OnMdY1O+6RYFPTck63p+rV3eZv/N/wY9
```

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。

## プライベート認証局 Gléas ホワイトペーパー Pulse Policy Secure での 802.1x EAP-TLS 認証設定

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。

## プライベート認証局 Gléas ホワイトペーパー Pulse Policy Secure での 802.1x EAP-TLS 認証設定



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。



Policy 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。

Step 2.

Import signed certificate

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

Signed certificate:

C:\temp\download.crt

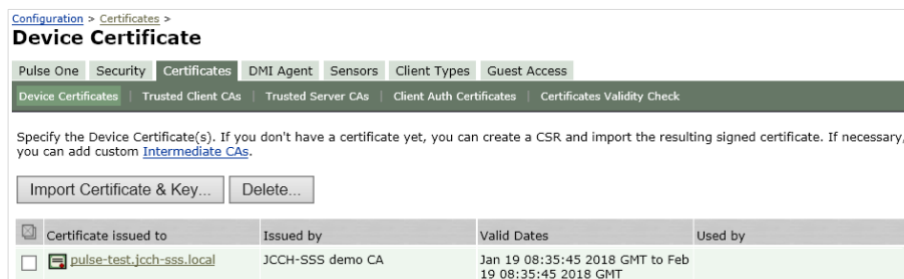
参照...

Import

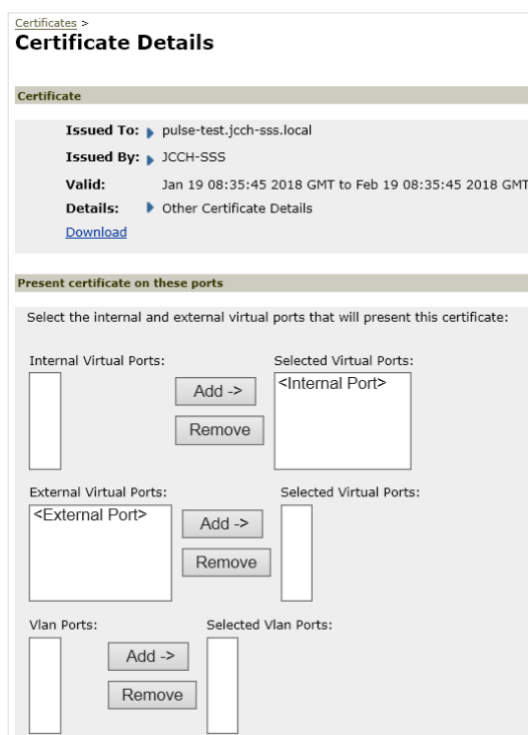
## プライベート認証局 Gléas ホワイトペーパー Pulse Policy Secure での 802.1x EAP-TLS 認証設定

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。以下は内部ポートに割り当てる例となります。



### 2.3. User Realm 設定

管理者画面左側のメニューより [User Realms] > [User Realms] と進みます。

レルム一覧が表示されるので、デフォルトで作られている [Cert Auth] をクリックします。

Authentication に、[Certificate Authentication] が選択されていることを確認します。

プライベート認証局 Gléas ホワイトペーパー  
Pulse Policy Secure での 802.1x EAP-TLS 認証設定

※或いは、新たにUser Realmを作成します

User Realms > Cert Auth >  
**General**

General Authentication Policy Role Mapping

\* Name: Cert Auth Label to reference this realm

Description: System created authentication realm for

☐ When editing, start on the Role Mapping page

**Servers**

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication: Certificate Authentication Specify the server to use for authenticating users.

User Directory/Attribute: None Specify the server to use for authorization.

Accounting: None Specify the server to use for Radius accounting.

Device Attributes: None Specify the server to use for device authorization.

**Dynamic policy evaluation**

☐ Enable dynamic policy evaluation

**Session Migration**

**Other Settings**

Authentication Policy: Certificate restrictions  
Role Mapping: Password restrictions  
1 Rule

Authenticationの選択肢にCertificate Authenticationがない場合は、右側のメニューの[Auth. Servers]で、Server TypeにCertificate Serverを指定した認証サーバ設定をおこなう必要があります。

以下にその場合の手順を記します。

**Authentication Servers**

New: (Select server type) New Server... Delete...

Authentication/Authorization Servers	Type
<a href="#">Administrators</a>	Local Authentication
<input type="checkbox"/> <a href="#">Certificate Authentication</a>	Certificate Server
<input type="checkbox"/> <a href="#">Guest Authentication</a>	Local Authentication
<input type="checkbox"/> <a href="#">MacAuth</a>	MAC Address Authentication
<input type="checkbox"/> <a href="#">System Local</a>	Local Authentication

[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

## プライベート認証局 Gléas ホワイトペーパー Pulse Policy Secure での 802.1x EAP-TLS 認証設定

- [User Name Template:]には、ユーザIDとする証明書内の属性を入力  
※証明書サブジェクト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

設定したレルムには、認証成功後にマッピングされるロールを設定しておきます。  
以下は、証明書サブジェクトのCNにどのような値があろうとUsersロールを割り当てる場合の例となります（以下記載の[Auth. Servers]設定の[User Name Template]で <certDN.CN> を指定していること）。

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. Authentication Protocol Set 設定

Signing-in > Authentication Protocol Sets と進み、認証プロトコルセットに EAP-TLS が含まれるものを作成しておきます。

※Factory Default の状態で、Cert Auth というプロトコルセットが作成されています

## プライベート認証局 Gléas ホワイトペーパー Pulse Policy Secure での 802.1x EAP-TLS 認証設定

Name	Authentication Protocol	PEAP	TTLS
1 <a href="#">802.1X</a> System created default authentication protocol required for UAC agents	EAP-TTLS EAP-PEAP	EAP-JUAC EAP-MS-CHAP-V2	EAP-JUAC PAP MS-CHAP-V2 EAP-MS-CHAP-V2 EAP-GenericTokenCard
2 <a href="#">802.1X-Phones</a> System created default authentication protocol for phones	EAP-MD5-Challenge EAP-TLS		
3 <a href="#">Guest</a> System created authentication protocol for guest users	PAP CHAP		
4 <a href="#">Cert Auth</a> System created authentication protocol for Certificate Authentication	EAP-TLS	EAP-JUAC EAP-TLS	EAP-JUAC EAP-GenericTokenCard

### 2.5. Sign-in Policy の設定

管理者画面左側のメニューより[Signing-in] > [Sign-in Policies]と進みます。その後、[New URL...]をクリックし以下の設定をおこないます。

- Sign-in URLには、サインイン用のURL（以下の例では \*/radius）を設定
- Authentication Realmには、2.3項で設定したレルムと2.4項で設定した認証プロトコルセットを設定

User type: ☒ Users ☐ Administrators

Sign-in URL:  Format: <host>/<path>/; Use \* as wildcard in the beginning of the host name.

Description:

Sign-in page:

**Authentication realm**

Specify what realms will be available when signing in.

Available realms	Authentication protocol set
<input type="checkbox"/> Cert Auth	<input type="text" value="- Not applicable -"/>
<input type="checkbox"/> Cert Auth	<input type="text" value="Cert Auth"/>

### 2.6. Location Group および RADIUS Attributes 設定

管理者画面左側のメニューより[Network Access] > [Location Group]と進みます。その後、[New Location Group...]をクリックします。任意のロケーショングループ名と、2.5項で設定したサインイン用のURLを設定します。

プライベート認証局 Gléas ホワイトペーパー  
Pulse Policy Secure での 802.1x EAP-TLS 認証設定

Network Access > Location Group >  
**New Location Group**

---

**Location Group**

\* Name:  Label to reference this Location Group.  
Description:

\* Sign-In Policy:  To manage policies, see the [Sign-In Policies](#)  
MAC Authentication Realm:  To manage realm, see the [MAC Address Realms](#)

---

**Save changes**

\* indicates required field

保存後、[RADIUS Attributes]タブを選択し、[New Policy...]をクリックします。  
任意のポリシー名称と、本項上部で設定したロケーショングループを設定します。  
またクライアントに適用するRADIUS属性を設定します。  
今回は何の属性の割り当てもしないので、[Open port]を選択しています。

Network Access > [RADIUS Return Attributes Policies](#) >  
**New Policy**

---

\* Name:   
Description:

---

**Location Group**

Specify the Location Group for which this policy applies.

Available Location Groups:   
Guest  
Cert Auth

Add -> Remove

Selected Location Groups:

---

**RADIUS Attributes**

☒ Open port  
☐ VLAN:  (1 - 4094)  
☐ Return Attribute:



### 3. Gléasの管理者設定（Windows PC）

GléasのUA（申込局）より発行済み証明書と無線LAN設定をWindows PCにインポートできるように設定します。

※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

#### 3.1. 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、Windows PC用となるUA（申込局）をクリックします。



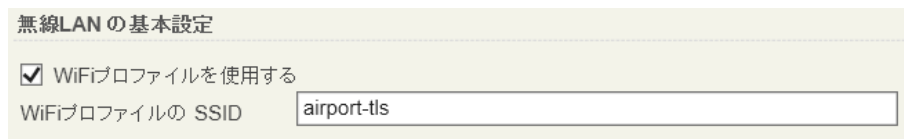
[申込局詳細]画面が開くので、[▶基本設定]の右側にある[▶上級者設定]をクリックし、設定項目を展開し以下の設定をおこないます。

- [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



[無線LANの基本設定]で以下の設定をおこないます。

- [WiFiプロファイルを使用する]をチェック
- [WiFiプロファイルの SSID]に、対象のSSIDを入力



設定終了後、[保存]をクリックし設定を保存します。

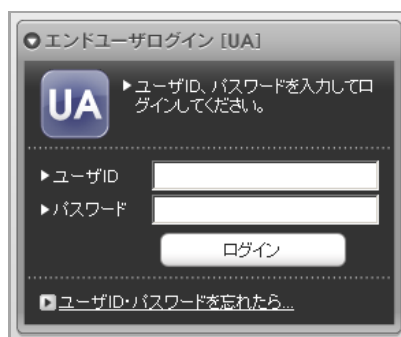
以上でGléasの設定は終了です。

## 4. Windows PC での証明書インポート・無線 LAN 設定

### 4.1. Gléas の UA からのインストール

Internet Explorer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、GléasでのユーザIDとパスワードを入力しログインします。



End User Login [UA]

UA ユーザID、パスワードを入力してログインしてください。

ユーザID

パスワード

ログイン

☐ ユーザID・パスワードを忘れたら...

ログインすると、ユーザ専用ページが表示されます。

※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ます

その後、[証明書のインポート]ボタンをクリックすると、無線LANのプロファイルのインポートと、クライアント証明書のインポートが順次自動でおこなわれます。



[テスト ユーザ01 さんのページ] ログアウト

ユーザ情報

テスト ユーザ01 さんのページ ヘルプ

ユーザ情報

ユーザ 登録日時: 2011/02/28 09:13

姓: テスト 名: ユーザ01

ユーザID: testuser01

メールアドレス:

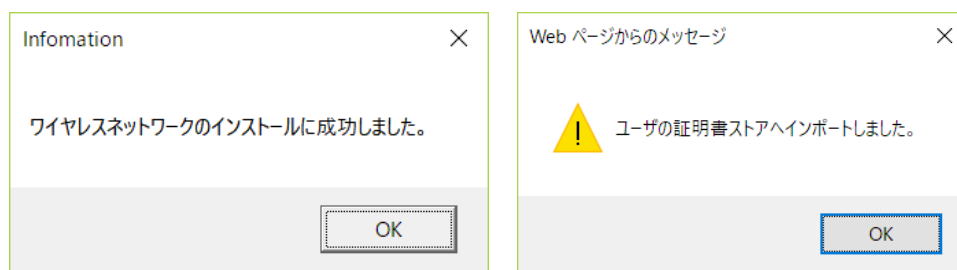
パスワード: \*\*\*\*\*

証明書情報

発行済み証明書

#	発行局	シリアル	有効期限	証明書ストアへインポート
1	JCCH-SSS demo CA	#11256	2019/10/18	証明書のインポート

プライベート認証局 Gléas ホワイトペーパー  
Pulse Policy Secure での 802.1x EAP-TLS 認証設定



「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。



無線LANプロファイルとクライアント証明書がインポートされたWindows PCでは、SSIDを選択するだけで自動的に無線LAN接続をすることが可能です。

## 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無線 LAN 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

### 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、設定をおこなうUA（申込局）をクリックします。

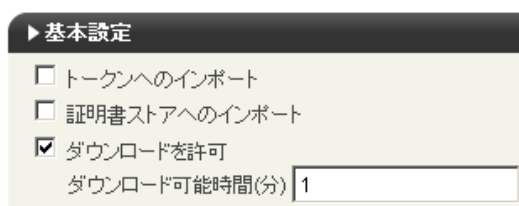
プライベート認証局 Gléas ホワイトペーパー  
Pulse Policy Secure での 802.1x EAP-TLS 認証設定



[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な情報を入力する画面が展開されるので、以下設定を行います。

- [iPhone用レイアウトを利用する]にチェック
- [ログインパスワードで証明書を保護]をチェック
- [iPhone構成プロファイル基本設定]の各項目を入力

※[名前]、[識別子]は必須項目となります

※[削除パスワード]を設定すると、ユーザ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ます（ユーザ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）

プライベート認証局 Gléas ホワイトペーパー  
Pulse Policy Secure での 802.1x EAP-TLS 認証設定

▶ iPhone / iPad の設定

☒ iPhone/iPad 用 UA を利用する

画面レイアウト

☒ iPhone 用レイアウトを使用する ☒ ログインパスワードで証明書を保護

☐ Mac OS X 10.7以降の接続を許可

OTA(Over-the-air)

☐ OTAエンロールメントを利用する ☒ 接続する iOS デバイスを認証する

OTA用SCEP URL

OTA用認証局

デフォルトを利用

iPhone 構成プロファイル基本設定

名前(デバイス上に表示)

プライベート CA Gleas

識別子(例: com.jcch-sss.profile)

com.jcch-sss.demo-mdm

プロファイルの組織名

JCCH セキュリティ・ソリューション・システムズ

説明

テスト用の構成プロファイル

削除パスワード

入力が終わったら、[無線LAN(802.1x)の設定]項目まで移動し以下を設定します。

- [SSID]に、WiFiアクセスポイントのSSIDを入力
- (SSIDをブロードキャストしていない場合) [非公開ネットワーク]をチェック

無線LAN(802.1x)の設定

SSID

airport-tls

☒ 非公開ネットワーク

設定終了後、[保存]をクリックして設定を保存します。

以上でGléasの設定は終了です。

## 6. iPad での構成プロファイル・証明書のインストール

GléasのUAに接続し、発行済みのクライアント証明書・構成プロファイルのインポートを行います。

※本ケースではUAに接続するためのネットワーク接続が必要となります(3G回線や、証明書認証を必要としない無線LAN接続等)

### 6.1. Gléas の UA からのインストール

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。

プライベート認証局 Gléas ホワイトペーパー  
Pulse Policy Secure での 802.1x EAP-TLS 認証設定



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、[構成プロファイルのダウンロード]をタップし、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、[インストール]をタップします。  
なお、[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、必要に応じ確認してください。

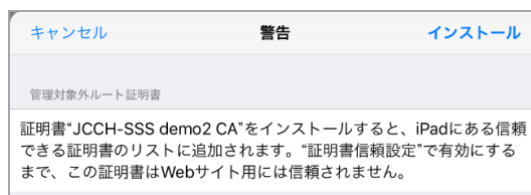


パスコードロックを有効にしている場合（或いは構成プロファイルでパスコードロ  
ックを強制する場合）はパスコードを入力します。

その後、以下のようなルート証明書追加の警告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てください。

※ここでインストールされるルート証明書は、通常のケースではGléasのルート認証局証明書に  
なります

プライベート認証局 Gléas ホワイトペーパー  
Pulse Policy Secure での 802.1x EAP-TLS 認証設定



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からログアウトしてください。

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。

無線LANプロファイルとクライアント証明書がインポートされた端末では、SSIDを選択するだけで自動的にWiFi接続をすることが可能です。

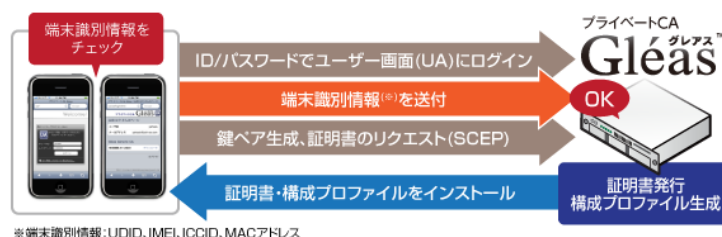
なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロード済み」という表記に変わり、以後のダウンロードは一切不可能となります。



## 6.2. 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。



詳細は最終章のお問い合わせ先までお問い合わせください。

## 7. クライアントからの接続

クライアントデバイスでは無線LANの接続設定はすでにおこなわれているので、対象のSSIDを選択すれば自動的にEAP-TLS認証をおこなって接続されます。

認証の成功時には、Policy SecureのUser Accessログに以下のログエントリが表示されます。

```
Agent login succeeded for USER_NAME/USER_REALM from MAC_ADDRESS.  
Primary authentication successful for USER_NAME/Certificate Authentication from MAC_ADDRESS  
The X.509 certificate for 'CERT_SUBJECT' issued by CERT_ISSUER, successfully passed CRL  
checking  
CRL checking started for certificate 'CERT_SUBJECT' issued by CERT_ISSUER
```

失効済みの証明書でアクセスすると接続に失敗し、Policy SecureのUser Accessログには以下のログエントリが表示されます。

```
Login failed using auth server Certificate Authentication (Certificate Server). Reason:  
Revoked Certificate  
Primary authentication failed for USER_NAME/Certificate Authentication from MAC_ADDRESS  
The X.509 certificate for 'CERT_SUBJECT' issued by CERT_ISSUER failed in CRL checking;  
Status '23'; Detail: 'certificate revoked'  
CRL checking started for certificate 'CERT_SUBJECT' issued by CERT_ISSUER
```



## 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。

### ■Policy Secureに関するお問い合わせ先

マクニカネットワークス株式会社

Pulse Secure 製品担当

TEL: 045-476-1980

Mail: [pulsesecure-sales@cs.macnica.net](mailto:pulsesecure-sales@cs.macnica.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  
営業本部

Tel: 050-3821-2195

Mail: [sales@jcch-sss.com](mailto:sales@jcch-sss.com)