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CA Gléas ホワイトペーパー

BIG-IP Access Policy Manager （APM）による SSL-VPNトンネリング接続

Ver.1.0
2015 年 11 月

目次

1. はじめに 5
1.1. 本書について 5
1.2. 本書における環境 5
1.3. 本書における構成 6
1.4. 証明書発行時における留意事項 6
2. BIG-IP の設定 7
2.1. トンネリング VPN の設定 7
2.2. サーバ証明書の登録 10
2.3. ルート証明書の登録 15
2.4. 失効リスト（CRL）の登録 16
2.5. SSL プロファイルの作成 17
2.6. SSL プロファイルの適用 18
2.7. Active Directory（ドメインコントローラ）の登録 19
2.8. アクセスポリシーの設定 19
3. Gléas の管理者設定（PC） 22
4. PC からの接続操作 22
4.1. クライアント証明書のインポート 22
4.2. クライアントからの VPN 接続（PC） 24
5. Gléas の管理者設定（iPad） 25
5.1. UA（ユーザ申込局）設定 26
6. クライアントからの VPN 接続（iPad） 27
6.1. Edge Client のインストール 27
6.2. Gléas の UA から配布 28
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 30
6.4. Edge Client から接続 30
7. Gléas の管理者設定（Android） 32
7.1. UA（ユーザ申込局）設定 32
8. クライアントからの VPN 接続（Android） 33
8.1. Edge Client のインストール 33
8.2. Gléas の UA から配布 33

8.3. Edge Client から接続 37
9. 問い合わせ 38

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CA Gléas で発行したクライアント証明書を利用して、F5ネットワークス株式会社の BIG-IP Access Policy Manager （APM）とVPNクライアントソフトウェアである BIG-IP Edge Client を利用してのトンネリング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

本書は、以下の環境で検証をおこなっております。

- BIG-IP Access Policy Manager （BIG-IP 12.0.0 Build 0.0.606）
  以後、「APM」と記載します
- JS3 プライベートCA Gléas（バージョン1.12.96）
  以後、「Gléas」と記載します
- Windows Server 2012 R2 Standard
  以後、「ドメインコントローラ」と記載します
- Windows10 Pro / BIG-IP Ede Client Components （71.2015.0804.0314）
  以後、「Windows」と記載します
- iPad 第３世代（iOS 9.0.1）/ BIG-IP Edge Client （バージョン2.0.5 7060.2015.0508.1）
  以後、「iPad」と記載します
- Nexus7 2012 （Android 5.1）/ BIG-IP Edge Client （バージョン2.0.7 7000.2015.0403.1247）
  以後、「Android」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。

- APMの基本設定（ネットワーク設定や基本的なVPN設定）
  F5ネットワークスでは、以下URLでAPMの操作ガイドを公開しています。

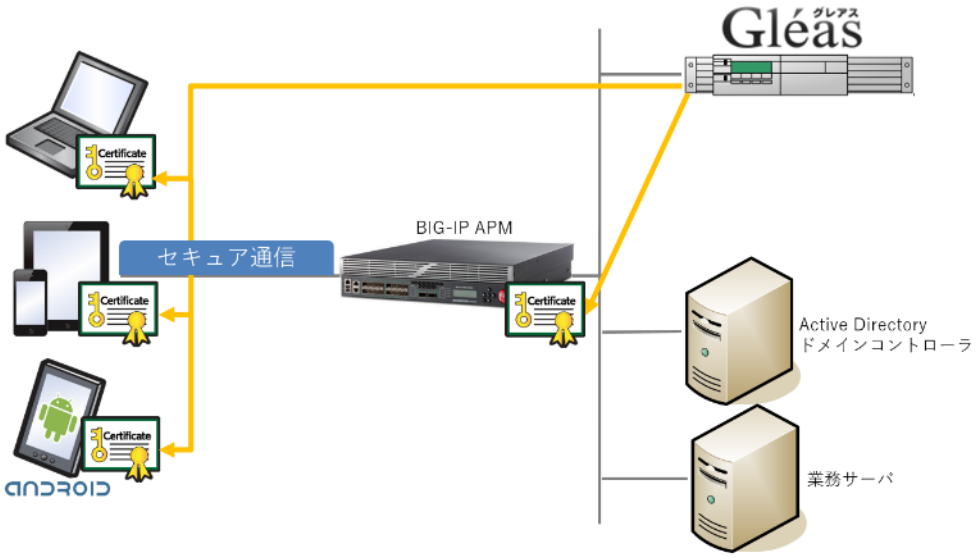
http://www.f5networks.co.jp/depot/
「BIG-IP APM ネットワークアクセス かんたんセットアップガイド 初級編&中級編」

- Gléasでのユーザ登録やクライアント証明書発行などの基本操作
- 各種サーバ・クライアント端末におけるネットワーク設定など

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では、APMにサーバ証明書を、PC・iPad・Androidにクライアント証明書を発行する。
2. 各端末はGléasより証明書をインポートする。
   iPadやAndroidに関しては、VPNの接続設定も同時にインポートする。
3. 各端末はAPMにVPNアクセスし、APMはクライアント証明書認証をおこなう。
   証明書認証後にActive DirectoryでのユーザID・パスワード認証をおこなうが、ユーザIDはクライアント証明書のサブジェクトCNから抽出する。
   （ユーザIDの詐称がおこなえないようにする）

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。

- 本書の構成では、Gléasのアカウント名（＝クライアント証明書のサブジェクトCN）は、Active Directoryのユーザ名（sAMAccountName）と一致さ

せる必要があります。
（Gléasでは、Active Directoryよりアカウント情報をインポートさせることも可能です）

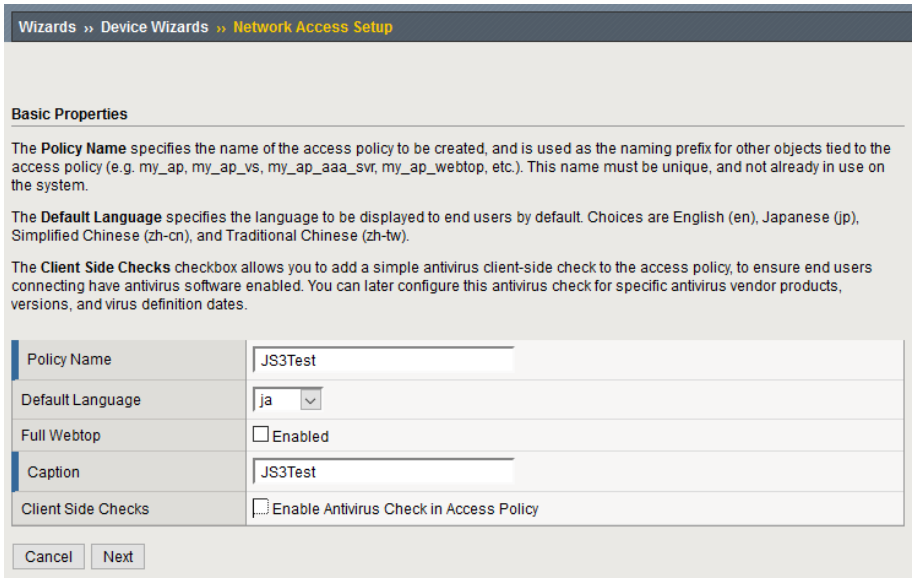
- 本書2.2の方法でサーバ証明書を発行する場合は、事前にサーバアカウントを作成しておく必要があります。

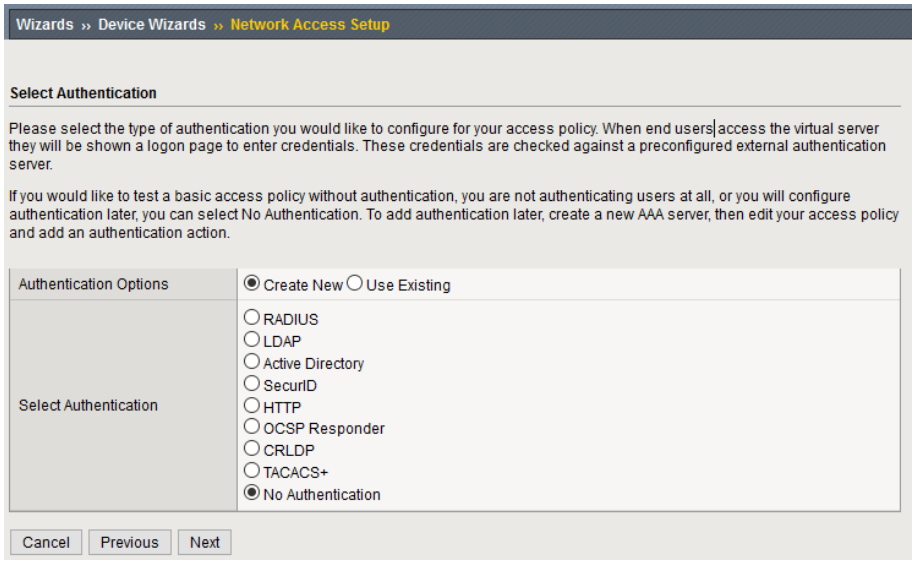
2. BIG-IP の設定

2.1. トンネリングVPNの設定

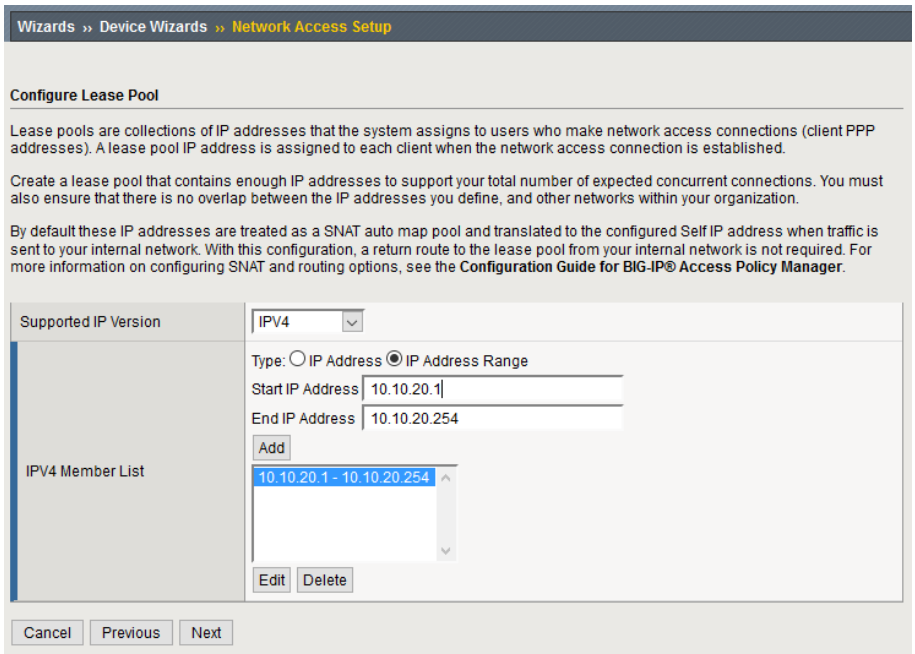
本書ではウィザードを使用して Virtual Server や Network Access をセットアップします。
（すでに作成していれば、本項は実施する必要はありません。2.2 に進んでください）

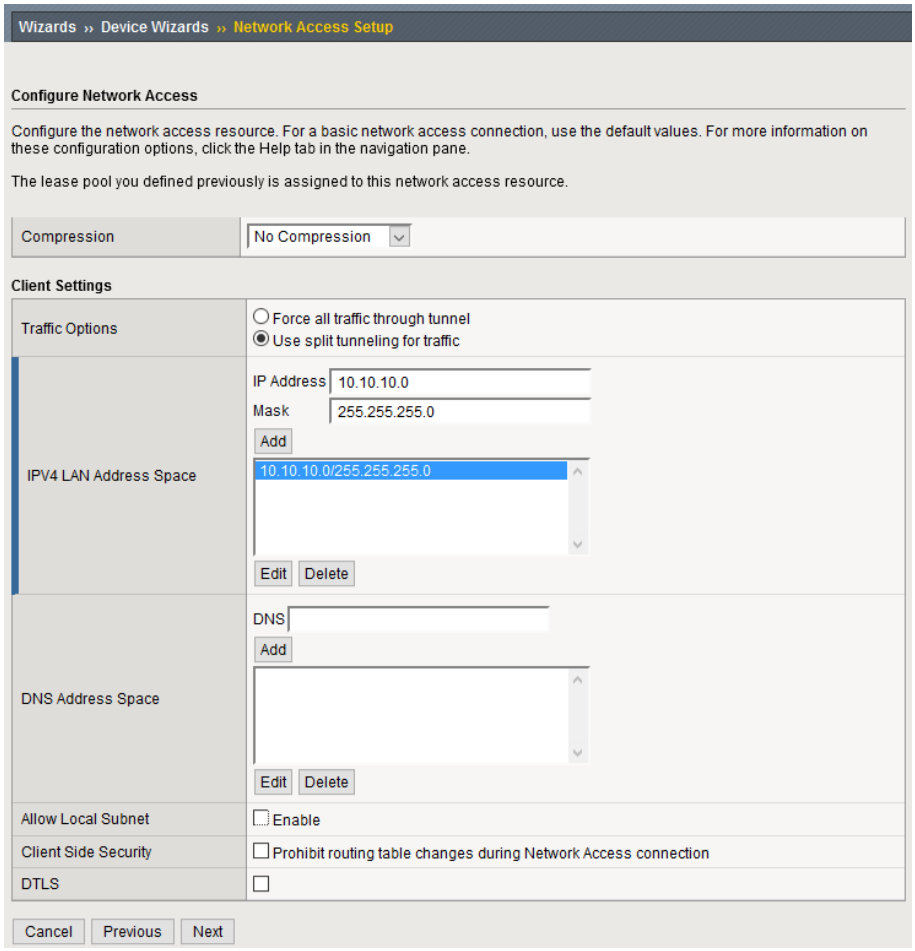
管理画面にログインし、左側メニューから Wizards > Device Wizards と進み、ウィザードの一覧を表示します。Network Access Setup Wizard for Remote Access を利用して、環境に合わせて Network Access をセットアップします。
以下は設定例となります。

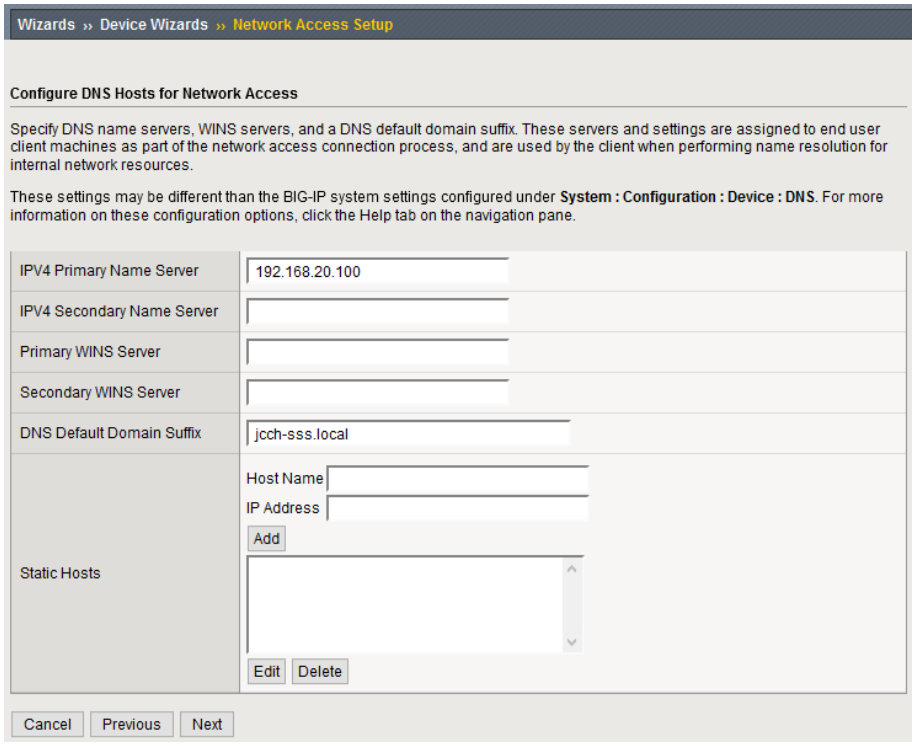


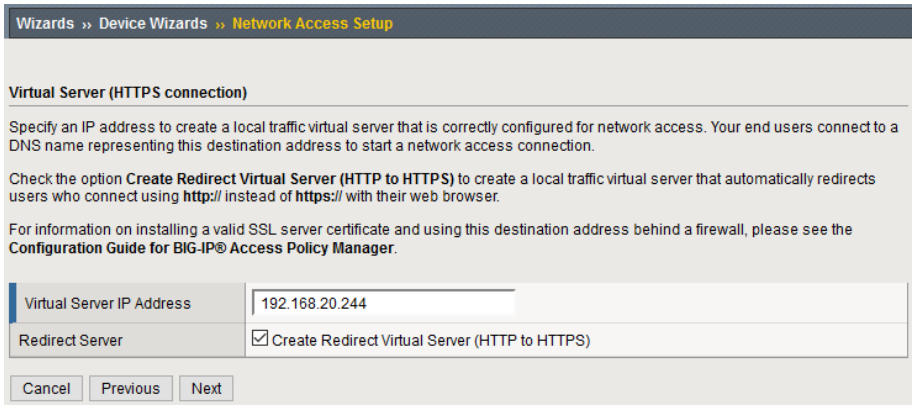


※ここでは No Authentication を選択していますが、Active Directory による認証設定は別途おこないます




Wizards ›› Device Wizards ›› Network Access Setup
Configure Network Access
Configure the network access resource. For a basic network access connection, use the default values. For more information on these configuration options, click the Help tab in the navigation pane.
The lease pool you defined previously is assigned to this network access resource.
Compression
No Compression
Client Settings
Traffic Options
Force all traffic through tunnel
Use split tunneling for traffic
IPV4 LAN Address Space
IP Address 10.10.10.0
Mask 255.255.255.0
Add
10.10.10.0/255.255.255.0
Edit Delete
DNS Address Space
DNS
Add
Edit Delete
Allow Local Subnet
Enable
Client Side Security
Prohibit routing table changes during Network Access connection
DTLS
Cancel Previous Next


Wizards ›› Device Wizards ›› Network Access Setup
Configure DNS Hosts for Network Access
Specify DNS name servers, WINS servers, and a DNS default domain suffix. These servers and settings are assigned to end user client machines as part of the network access connection process, and are used by the client when performing name resolution for internal network resources.
These settings may be different than the BIG-IP system settings configured under System : Configuration : Device : DNS. For more information on these configuration options, click the Help tab on the navigation pane.
IPV4 Primary Name Server
192.168.20.100
IPV4 Secondary Name Server
Primary WINS Server
Secondary WINS Server
DNS Default Domain Suffix
jcch-sss.local
Static Hosts
Host Name
IP Address
Add
Edit Delete
Cancel Previous Next

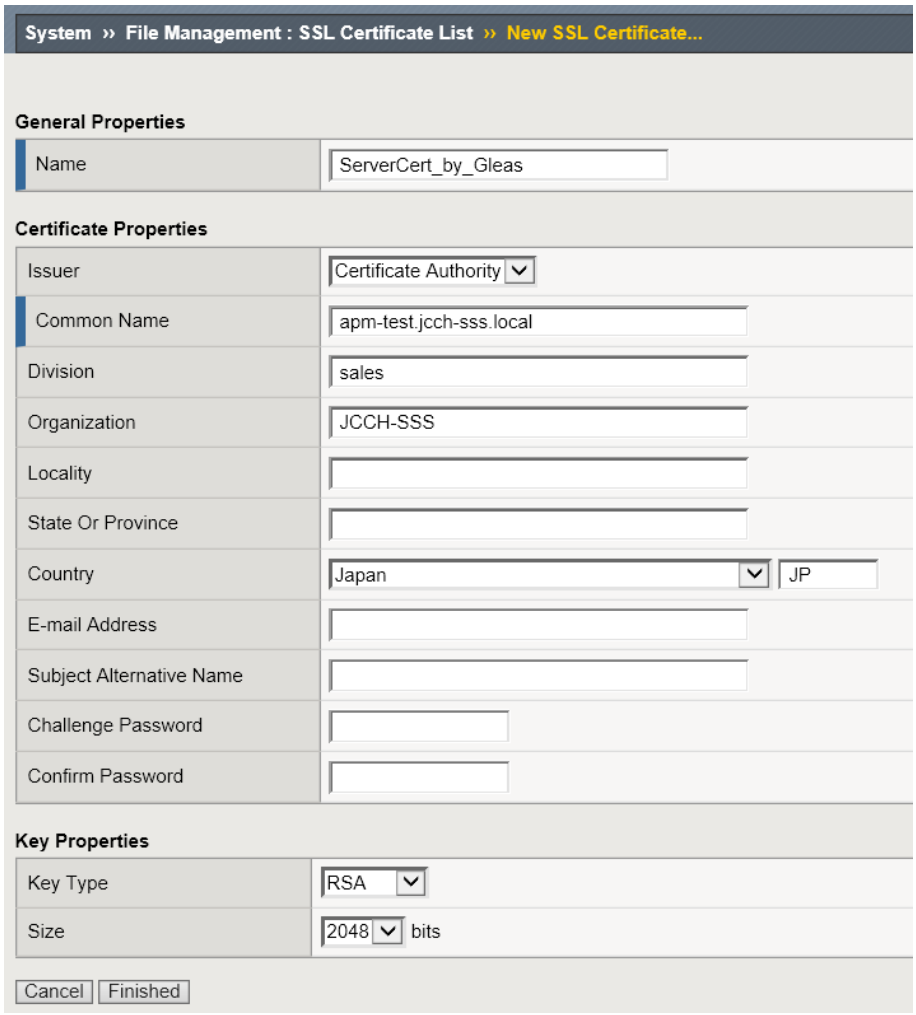


2.2. サーバ証明書の登録

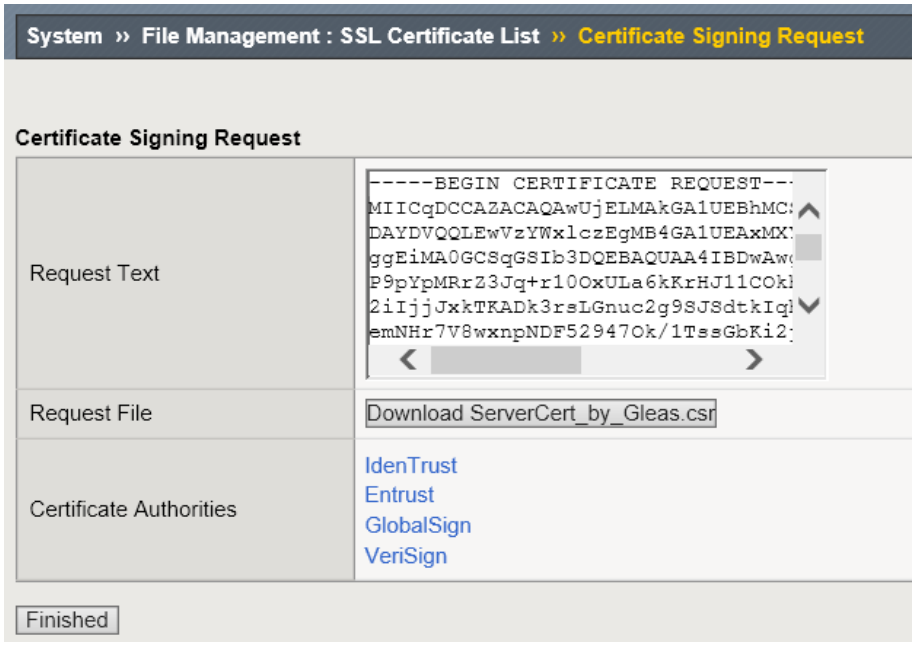
APMのバーチャルサーバに適用するサーバ証明書を発行します。
※本手順では、Gléasで事前にサーバアカウントを作成してあることが前提です
※本手順では、APMで証明書発行リクエスト（CSR）を発行していますが、Gléas側でこれらを一括しておこなうことも可能です

左側メニューから System ›› File Management : SSL Certificate List と進み、右上にある[Create…]ボタンをクリックします。
Name や Common Name などの証明書情報や Key Properties に必要事項を入力し、[Finished]ボタンをクリックします。

以下は Key Properties に RSA 2048bit 鍵長を選択した例です。
※Subject Alternative Name は設定しても、Gléas が証明書を発行するときにテンプレートに基づき上書きします



CSR が発行されるので、Request File 欄にある[Download…]ボタンより CSR ファイルをダウンロードします。



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。

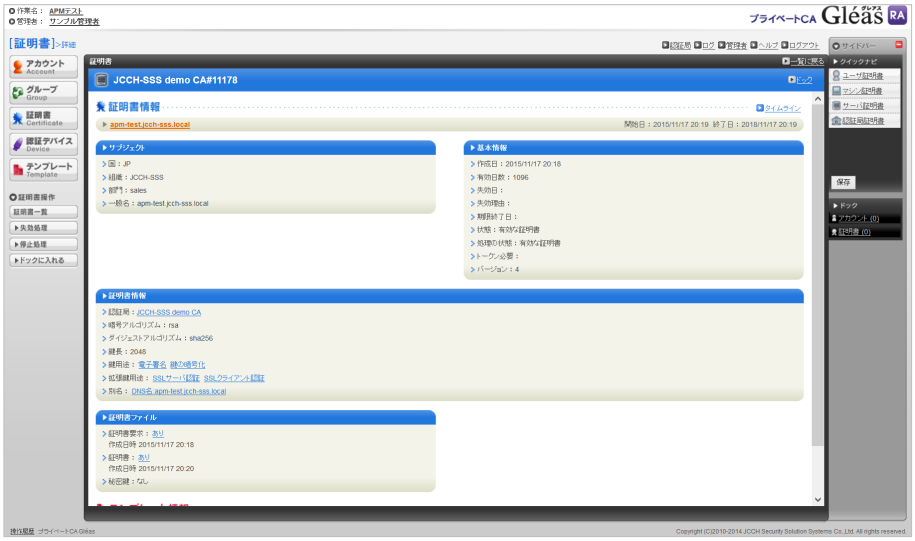
上級者向け設定を展開し、以下の操作をおこないます。

- 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

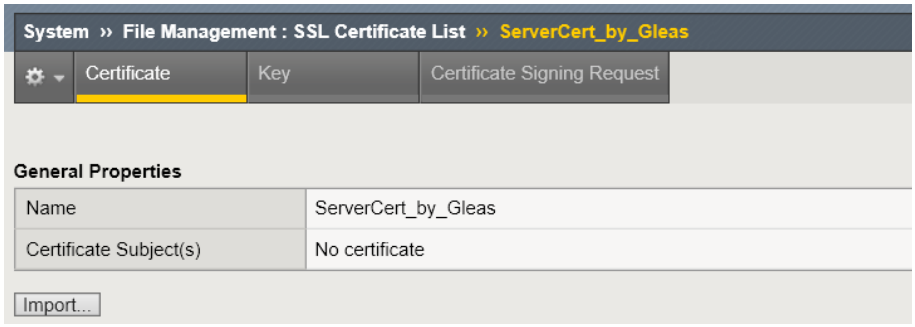
その後、[発行]ボタンをクリックします。

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。

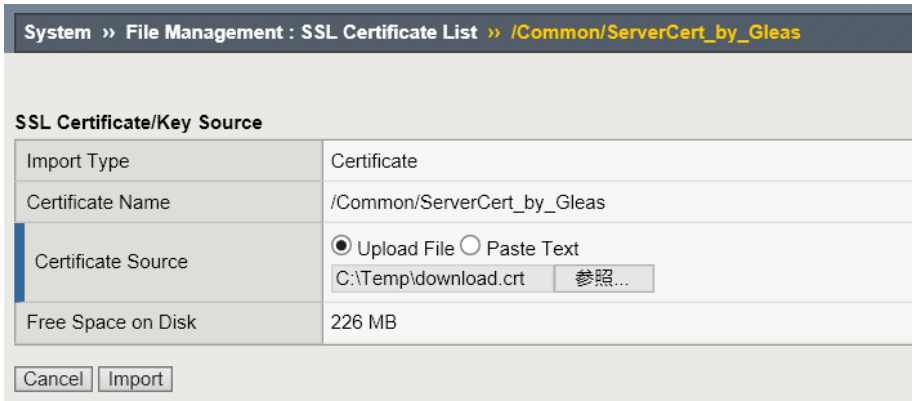
証明書発行完了後、証明書詳細画面の証明書ファイル欄の「証明書：あり」をクリックし、発行された証明書をダウンロードします。



APM の管理画面で、System ›› File Management : SSL Certificate List にて先ほど作成した CSR の詳細画面で、[Import…]ボタンをクリックします。

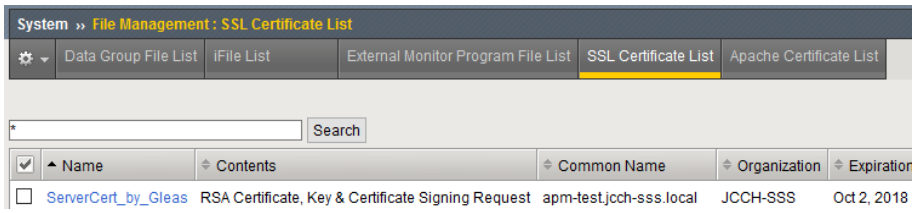


Gléas からダウンロードした証明書ファイルを選択し、[Import…]ボタンをクリックします。



以上でサーバ証明書の登録が完了です。

Contents 欄に、RSA Certificate, Key and Certificate Signing Request と表示されます。



2.3. ルート証明書の登録

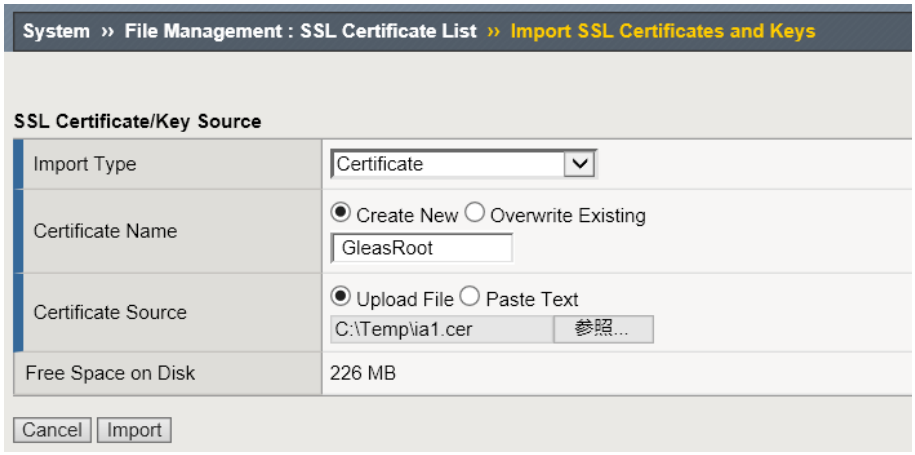
クライアント証明書によるSSL認証を利用するためには、ルート証明書の登録が必要です。これは、クライアントPCから提示されるクライアント証明書が正しいことを検証する際に利用するためです。

本手順の前にGléasよりルート証明書をダウンロードします。
※GléasのデフォルトCAのダウンロードURLは以下となります。
http://hostname/crl/ia1.der

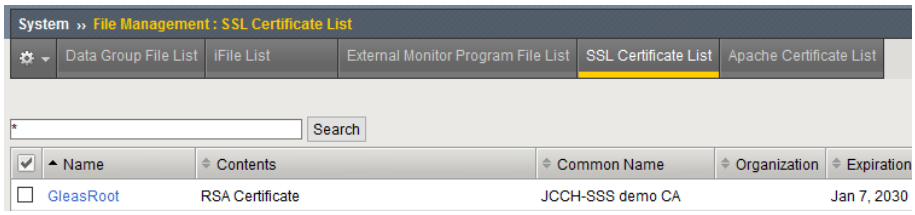
左側メニューから System ›› File Management : SSL Certificate List と進み、右上にある[Import…]ボタンをクリックします。
以下の操作をおこないます。

- Import Type は、[Certificate]を選択
- Certificate Name は、[Create New]を選択し任意の名称を入力
- Certificate Source は、[Upload File]を選択し[参照…]よりダウンロードしたファイルを選択

その後、[Import]をクリックします。



以上でルート証明書の登録が完了です。
Contents 欄に、RSA Certificate と表示されます。



2.4. 失効リスト（CRL）の登録

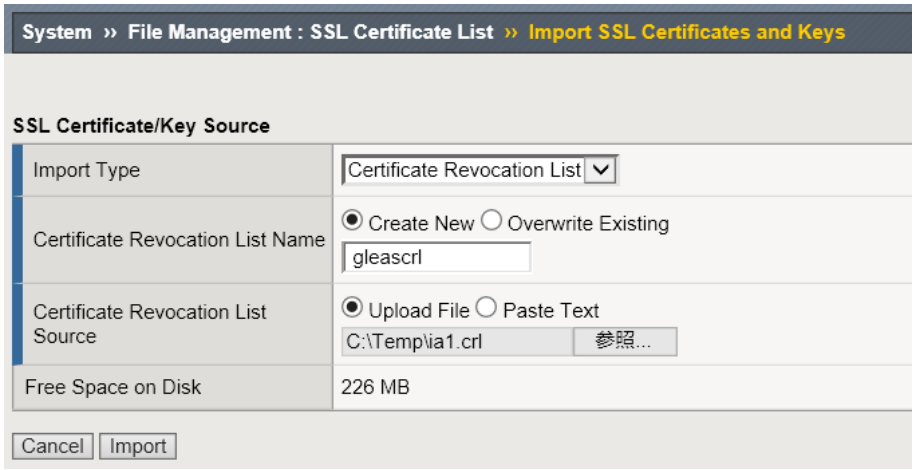
失効済みのクライアント証明書でのアクセスを防ぐために、CRLの登録をします。
あらかじめGléasよりCRLをダウンロードしておき、以下の操作をおこないます。

※ Gléas の初期設定での CRL ファイルの公開場所は以下のとおりです
http://hostname/crl/ia1.crl

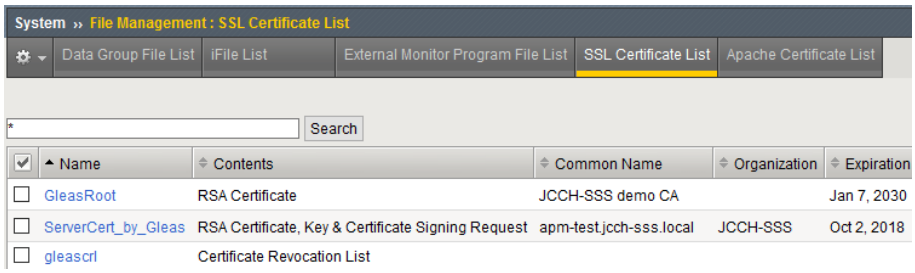
左側メニューから System ›› File Management : SSL Certificate List と進み、右上にある[Import…]ボタンをクリックします。
以下の操作をおこないます。

- Import Type は、[Certificate Revocation List]を選択
- Certificate Name は、[Create New]を選択し任意の名称を入力
- Certificate Source は、[Upload File]を選択し[参照…]よりダウンロードしたファイルを選択

その後、[Import]をクリックします。



以上で CRL の登録が完了です。
Contents 欄に、Certificate Revocation List と表示されます。



CRLを更新する場合は、Certificate Revocation List Name で Overwrite Existing を選択し、更新されたCRLファイルをアップロードします。

また、CRL更新はBIG-IPの管理用シェル（tmsh）からおこなうことも可能です。
以下はコマンド例です。
tmsh modify /sys file ssl-crl *gleascrl.crl* source-path *http://hostname/crl/ia1.crl*
※crontabで上記を実行することで、CRLの定期取得をおこなう設定をすることも可能です
※利用中のCRLは、以下コマンドで確認することが可能です
tmsh list /sys file ssl-crl *gleascrl.crl*

また失効確認には、LDAP（Lightweight Directory Access Protocol）やOCSP（Online Certificate Status Protocol）を利用する方法もあります。

2.5. SSLプロファイルの作成

クライアント証明書による認証を実施するプロファイルを作成します。

左側メニューから Local Traffic > Virtual Servers > Profiles > SSL > Client と進み、右上にある[Create…]ボタンをクリックします（或いは既存のプロファイルの設定変更をおこないます）。

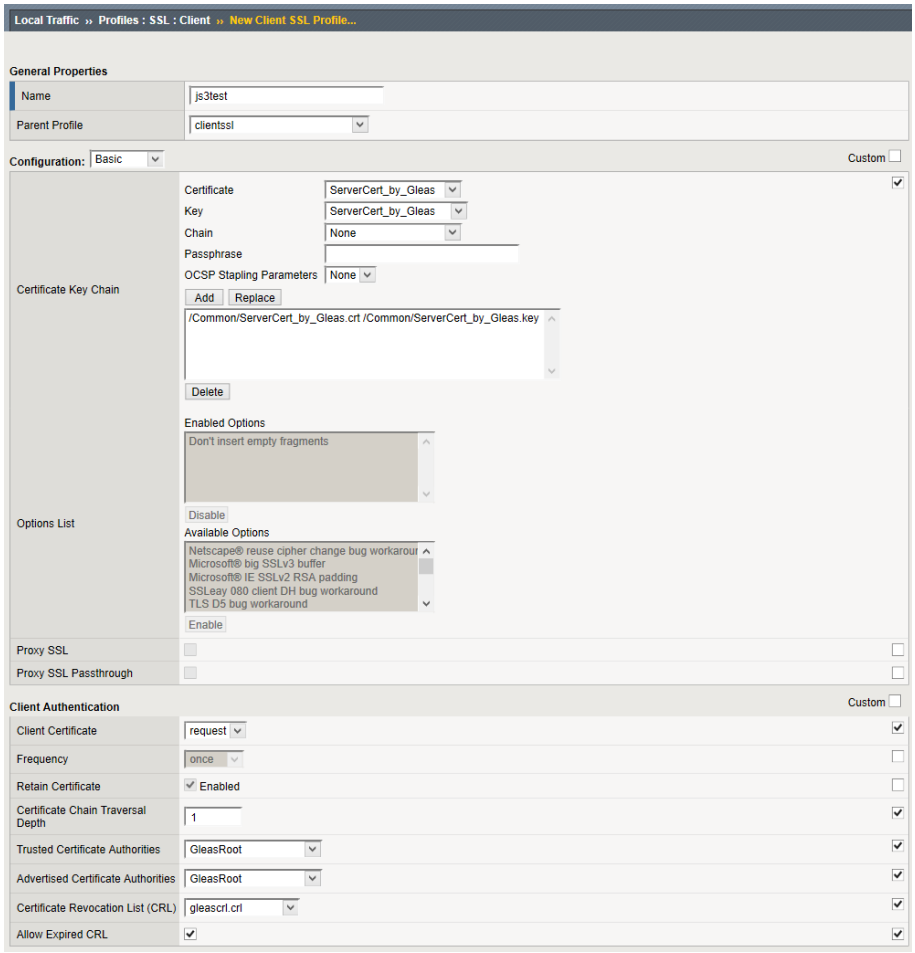
以下の設定変更をおこないます。
（変更する箇所の右側にある Custom チェックボックスをチェックして変更します）

【Configuration】
- Certificate Key Chain：Certificate と Key に 2.2 で設定したサーバ証明書を選択し、[Add]で追加

【Client Authentication】
- Client Certificate： Request を選択

- Trusted Certificate Authorities：2.3 で設定したルート証明書を選択
- Advertised Certificate Authorities：2.3 で設定したルート証明書を選択
- Certificate Revocation List（CRL）：2.4 で設定した CRL を選択
- Allow Expired CRL：必要に応じチェック（弊社未検証）

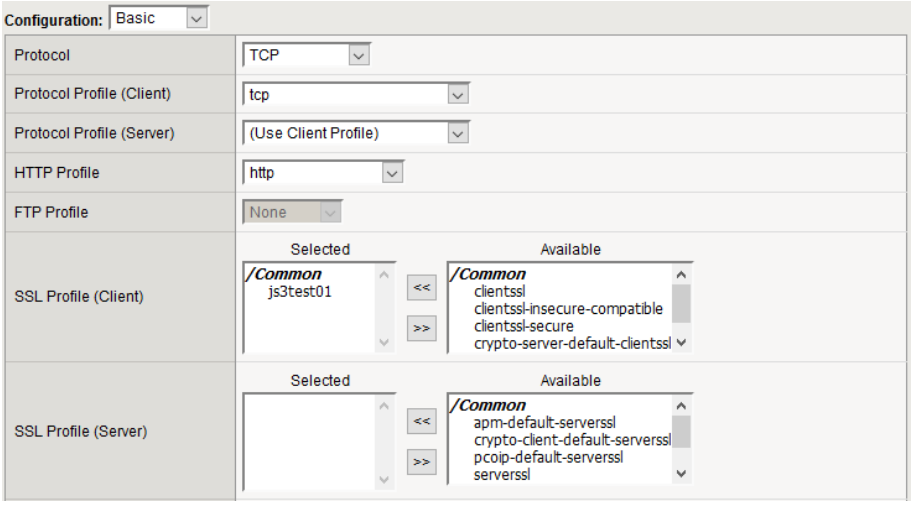
設定後に[Finished]（或いは、[Update]）をクリックし、保存します。



2.6. SSLプロファイルの適用

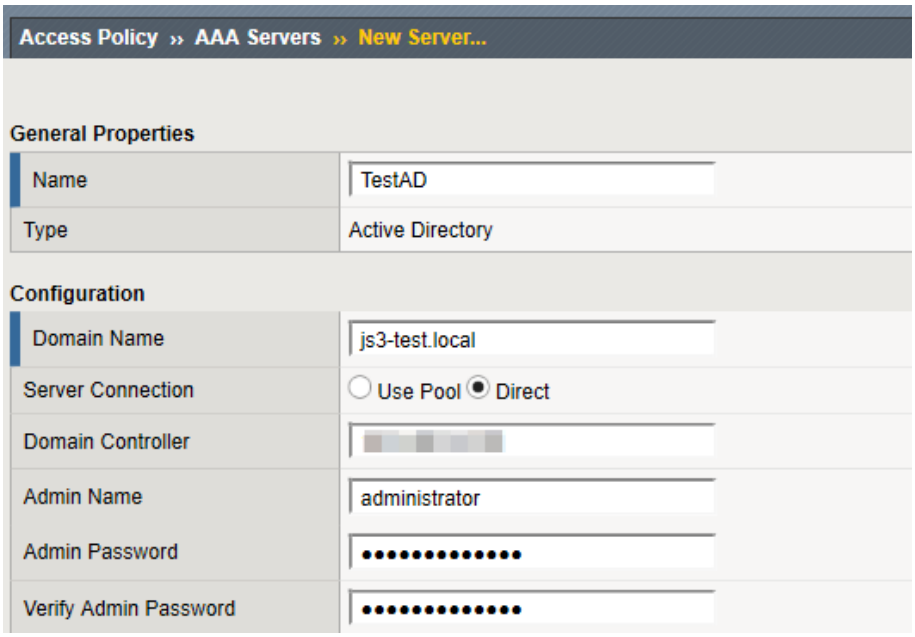
2.5 で作成したプロファイルを対象のバーチャルサーバに適用します。

左側メニューから Local Traffic > Virtual Servers > Virtual Server List と進み、2.1 で設定したバーチャルサーバ（HTTPS のもの）をクリックします。
そのバーチャルサーバの SSL Profile (Client)を 2.4 で作成した SSL プロファイルに変更し、[Update]をクリックし保存します。



2.7. Active Directory（ドメインコントローラ）の登録

左側メニューから Access Policy > AAA Servers > Active Directory と進み、右上の[Create…]をクリックし、認証をおこなうドメインコントローラの情報を登録します。

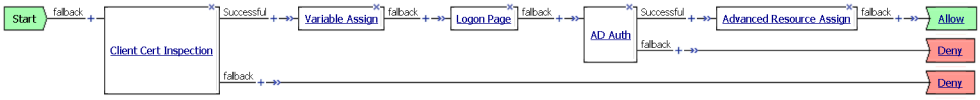


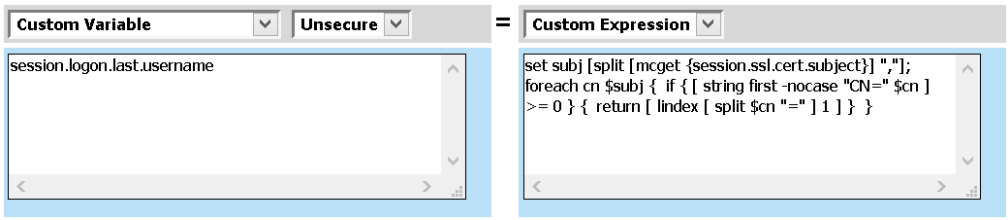
2.8. アクセスポリシーの設定

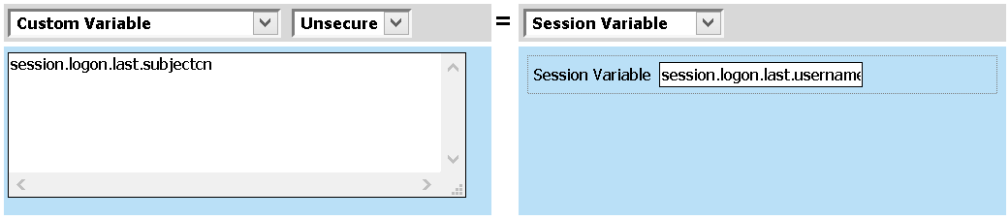
左側メニューから Access Policy > Access Profiles > Access Profiles List と進み、2.1 で設定した Access Profile を編集するため、Access Policy の Edit をクリックしビジュアルポリシーエディタ（VPE）を開きます。

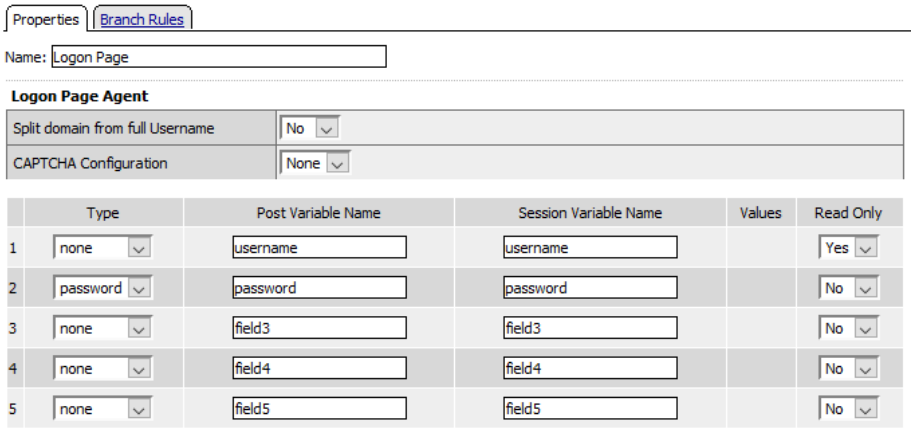
VPE でアクセスポリシーを設定します。以下は今回の設定例となります。

※VPE の操作方法については、本書では省略します

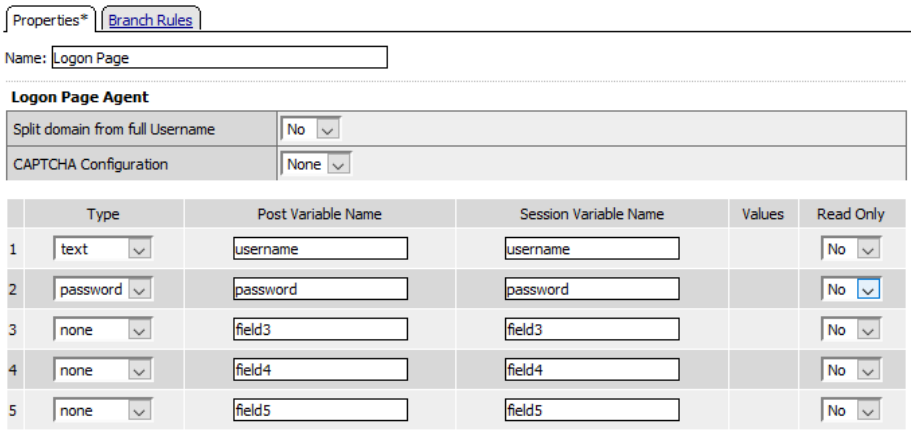


<table>
<tr><td>Client Cert Inspection</td><td>クライアント SSL プロファイルで設定されたクライアント証明書認証の結果をチェックします（デフォルトのまま）。</td></tr>
<tr><td>Variable Assign</td><td>[1 行目]
カスタム変数 session.logon.last.username に証明書サブジェクト cn 値（ユーザ ID）を代入するように設定します。
 

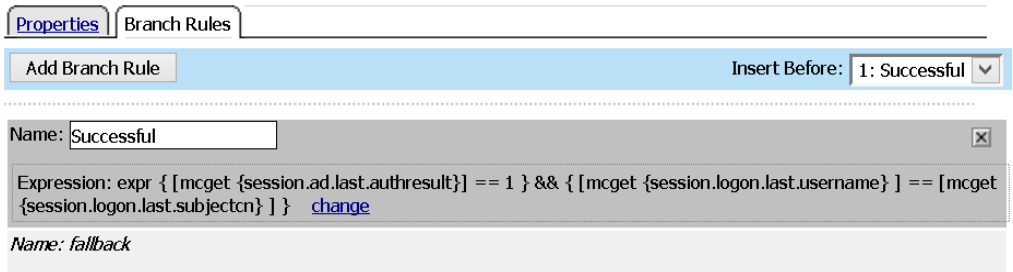
<pre>set subj [split [mcget {session.ssl.cert.subject}] ","];
foreach cn $subj { if { [string first -nocase "CN=" $cn] >= 0 } { return
[lindex [split $cn "="] 1] } }</pre>
[2 行目]
変数 session.logon.last.username を別のカスタム変数にも代入しておきます。(session.logon.last.username はユーザによるログイン操作時に置換されてしまうため)
 
</td></tr>
<tr><td>Logon Page</td><td>Type を [none] に変更することで、ログオン ID に変数 session.logon.last.username に代入された文字列を自動的に適用することができます。（ユーザの画面には表示されません）</td></tr>
</table>



あるいは、Read Only を[Yes]に設定することで、グレーアウトした（変更不可能な）ユーザ ID を表示させることも可能です。



AD Auth	ログインページで入力されたパスワードの認証をおこなうドメインコントローラとして、[Server]に 2.7 で設定した Active Directory を設定します。 さらに、Branch Rule にユーザ ID と、証明書サブジェクト CN を比較する条件を加えます。




```
expr { [mcget {session.ad.last.authresult}] == 1 } && { [mcget
{session.logon.last.username} ] == [mcget {session.logon.last.subjectcn} ] }
```

Resource Assign	設定済みのネットワークアクセスリソースを設定します。

設定完了後、[Apply Access Policy]をクリックしてバーチャルサーバに適用します。

以上でBIG-IPの設定は終了です。

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。

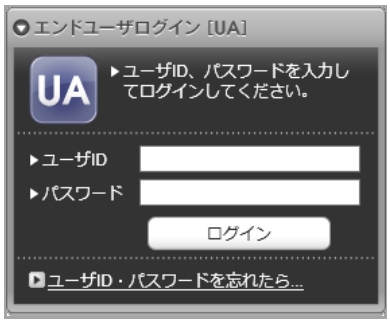
- [証明書ストアへのインポート]をチェック
- [証明書ストアの選択]で[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]にチェック

設定終了後、[保存]をクリックし設定を保存します。

4. PC からの接続操作

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。

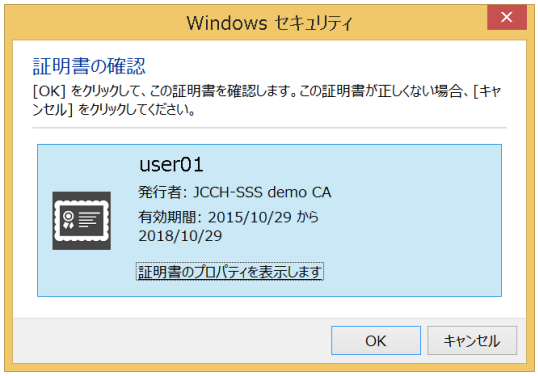


ログインすると、ユーザ専用ページが表示されます。
[証明書のインポート]ボタンをクリックすると、クライアント証明書が証明書ストアにインポートされます。
※初回ログインの際は、ActiveX コントロールのインストールを求められるので、画面の指示に従いインストールを完了してください。

「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。

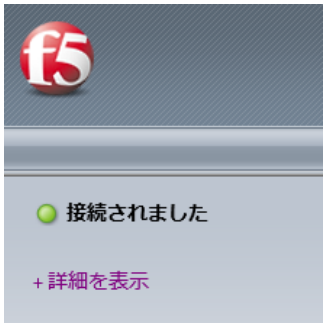
4.2. クライアントからのVPN接続（PC）

APMのバーチャルサーバにWebブラウザで接続します。
クライアント証明書の提示を求められるので提示をするとWebページが表示されます。

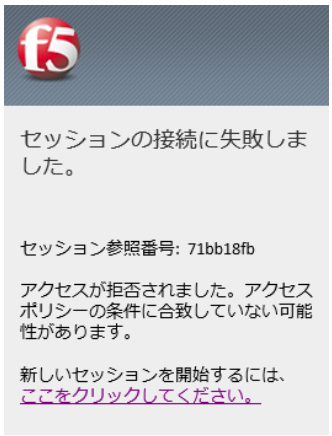


証明書認証がおこなわれるとログイン画面に遷移しますが、パスワード入力欄のみが表示されます。

パスワード認証に成功するとVPN接続がおこなわれます。



証明書を持っていない場合や、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。



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 Edge Client 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書では記載します。

※　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

※　Edge Client 用の構成プロファイル作成機能はオプションとなります。詳細は弊社営業までお

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（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]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・[インポートワンスを利用する]にチェック
  この設定を行うと、GléasのUAからインポートから指定した時間（分）を経過した後は、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）。これにより複数台のデバイス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。

設定終了後、[保存]をクリックし設定を保存します。

[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、以下設定を行います。

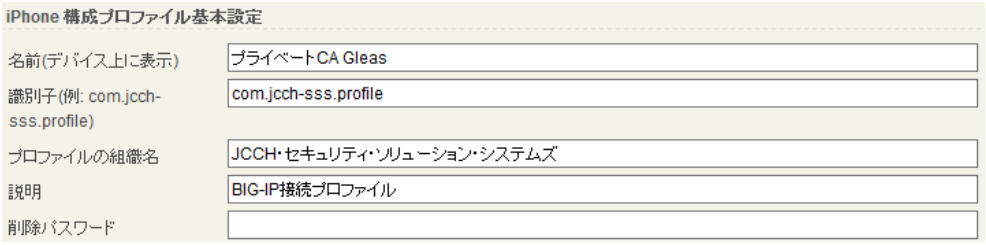
画面レイアウト

- [iPhone用レイアウトを利用する]をチェック
- [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

- [名前]、[識別子]に任意の文字を入力（必須項目）
- [削除パスワード]を設定すると、iPhone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（iPhone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）



F5 SSL-VPNの設定

- [SSL-VPN接続名]に任意の名前を入力（Edge Client上ではDescriptionに対応）
- [F5 SSL-VPN ホスト名]にBIG-IPのホスト名を入力（Edge Client上ではServerに対応）
- [オンデマンド接続先]にオンデマンド接続に利用するドメイン名を入力（Edge Client上ではドメインリストの[必要に応じて接続]に対応）
- [接続設定にユーザID/パスワードの情報を入れる]にチェック

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. クライアントからの VPN 接続（iPad）

6.1. Edge Clientのインストール

iPhoneでEdge Client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Edge Clientのインストール方法については割愛します。

6.2. GléasのUAから配布

iPhone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、[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。

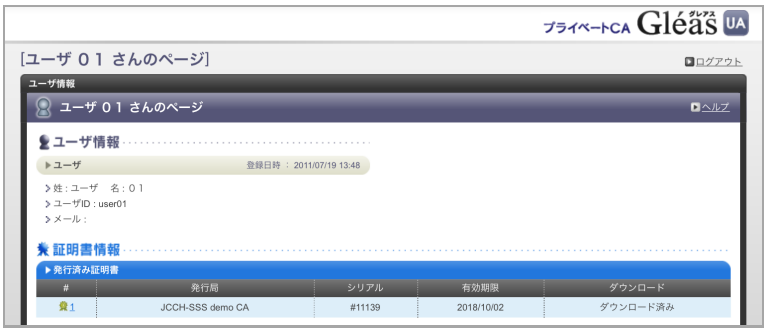
以下のようなルート証明書のインストール確認画面が現れますので、[インストール]をクリックして続行してください。
※ここでインストールされるルート証明書は、通常のケースではGléasのルート認証局証明書になります。

インストール完了画面になりますので、[完了]をタップしてください。

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。

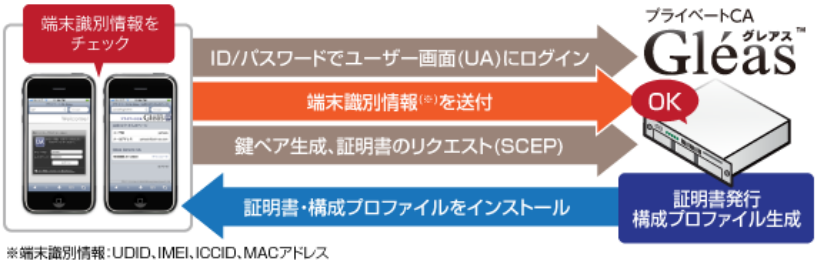
以上で、iPhoneでの構成プロファイルのインストールは終了です。
なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロード済み」という表記に変わり、以後のダウンロードは一切不可となり

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. Edge Clientから接続

インストールが完了すると、APMへの接続に利用するクライアント証明書やユーザID、VPN接続先が設定されています。
Edge Clientを起動し[接続]ボタンをタップすると、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。

以下はEdge Clientから接続した画面です。
接続すると、iPhoneの通知エリアに 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（※）、ログイン時にユーザ名を変更した場合は接続失敗の表示になります。

※失効情報を含むCRLがBIG-IPに伝搬されている必要があります

7. Gléas の管理者設定（Android）

Gléas で、発行済みのクライアント証明書を含む Edge Client 設定を Android にインポートするための設定を本書では記載します。

※　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

7.1. 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（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]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・[インポートワンスを利用する]にチェック
  この設定を行うと、GléasのUAからインポートから指定した時間（分）を経過した後は、クライアント証明書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）。これにより複数台のAndroidへのクライアント証明書のインストールを制限することができます。

設定終了後、[保存]をクリックし設定を保存します。

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

Androidからの接続に必要となる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。

- ログインパスワードで証明書を保護：チェック
- 証明書ダウンロードの種類：[BIG-IP EdgeClientへインポート]を選択
- SSL-VPN接続名：任意の名称を入力
- F5 SSL-VPN名：クライアントからみた接続先ホスト名を入力

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。

8. クライアントからの VPN 接続（Android）

8.1. Edge Clientのインストール

AndroidでEdge Client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。Google Playより事前にインストールを行ってください。
本書ではEdge Clientのインストール方法については割愛します。

8.2. GléasのUAから配布

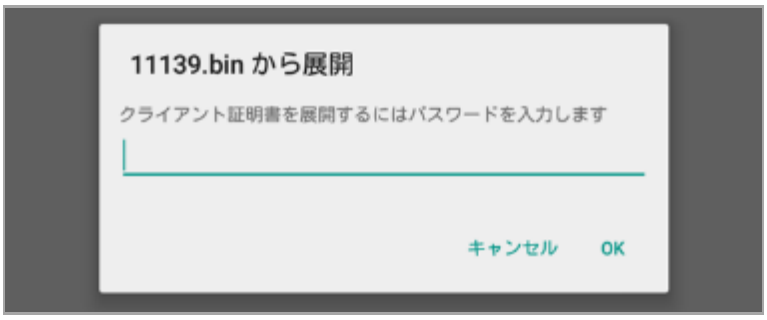
Androidのブラウザ（Chrome）でGléasのUAサイトにアクセスします。
ログイン画面が表示されるので、ユーザIDとパスワードを入力しログインします。

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]をタップしインポートを開始します。

※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

Edge Clientに遷移し警告表示されるので、内容を確認し[許可]をタップします。

クライアント証明書のインストール画面が表示されるので、ログインパスワードを入力します。



識別名を入力しますが、あらかじめ入力されているのでそのまま[OK]をタップします。

インポートが完了します。

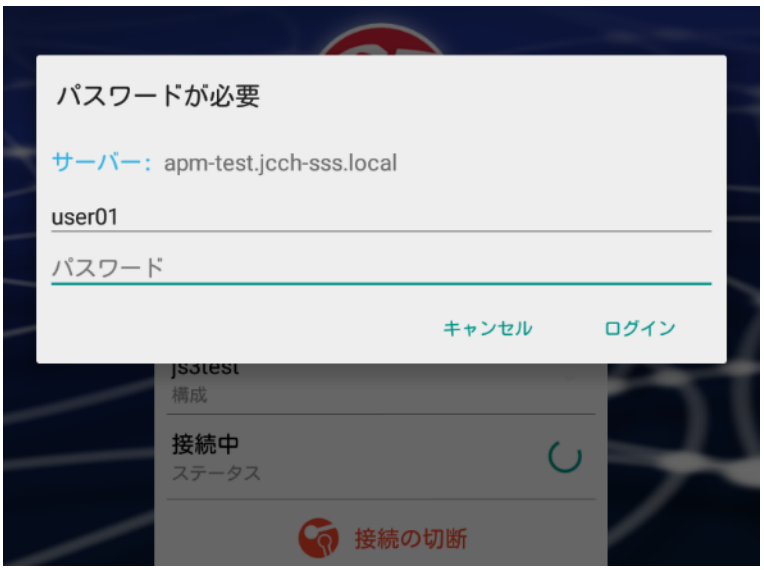
以上で、Androidでのクライアント証明書とVPN接続設定のインストールは終了です。

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。

8.3. Edge Clientから接続

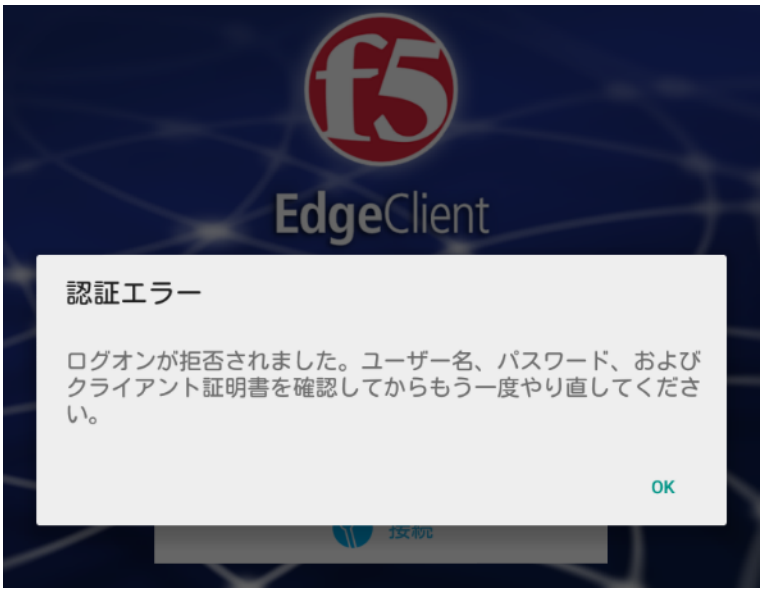
インストールが完了すると、APMへの接続に利用するクライアント証明書やVPN接続先が設定されています。
Edge Clientを起動し[接続]ボタンをタップすると、クライアント証明書を利用した認証を行いVPNの接続がおこなわれます。

以下はEdge Clientから接続した画面です。
（接続すると、通知エリアに  アイコンが表示されます）。



なお、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（※）、ログイン時にユーザ名を変更した場合は接続失敗の表示になります。

※失効情報を含むCRLがBIG-IPに伝搬されている必要があります



9. 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。

■BIG-IP APMに関するお問い合わせ先

F5ネットワークスジャパン株式会社
Tel: 03-5114-3210
URL: https://f5.com/jp/fc/
（上記URLのお問い合わせフォームよりご連絡ください）

■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