

NetAttest EPS

認証連携設定例

【連携機器】 F5 Networks BIG-IP Access Policy Manager

【Case】 証明書と ID・Password によるハイブリッド認証

Rev1.0

株式会社ソリトンシステムズ

はじめに

本書について

本書は、NetAttest EPS と F5 Networks 社製 VPN ゲートウェイ BIG-IP Access Policy Manager(BIG-IP APM)との証明書+ID・Password 認証連携について記載した設定例です。各機器の管理 IP アドレス設定など、基本設定は既に完了しているものとします。設定は管理者アカウントでログインし、設定可能な状態になっていることを前提に記述します。



表記方法

表記方法	説明
『 』	参照するドキュメントを示します。
「 」	参照する章、節、ボタンやメニュー名、強調する単語を示します。
[キー]	キーボード上のキーを表します。
[キー1]+[キー2]	[キー1]を押しながら[キー2]を押すことを表します。

表記方法(コマンドライン)

表記方法	説明
%, \$, >	一般ユーザーのプロンプトを表します。
#	特権ユーザーのプロンプトを表します。
[filename]	[] は省略可能な項目を示します。この例では、filename は省略してもよいことを示しています。

アイコンについて

アイコン	説明
	利用の参考となる補足的な情報をまとめています。
	注意事項を説明しています。場合によっては、データの消失、機器の破損の可能性があります。

画面表示例について

このマニュアルで使用している画面(画面キャプチャ)やコマンド実行結果は、実機での表示と若干の違いがある場合があります。

ご注意

本書は、当社での検証に基づき、NetAttest EPS 及び BIG-IP APM の操作方法を記載したものです。すべての環境での動作を保証するものではありません。

NetAttest®は、株式会社ソリトンシステムズの登録商標です。

その他、本書に掲載されている会社名、製品名は、それぞれ各社の商標または登録商標です。

本文中に ™、®、©は明記していません。

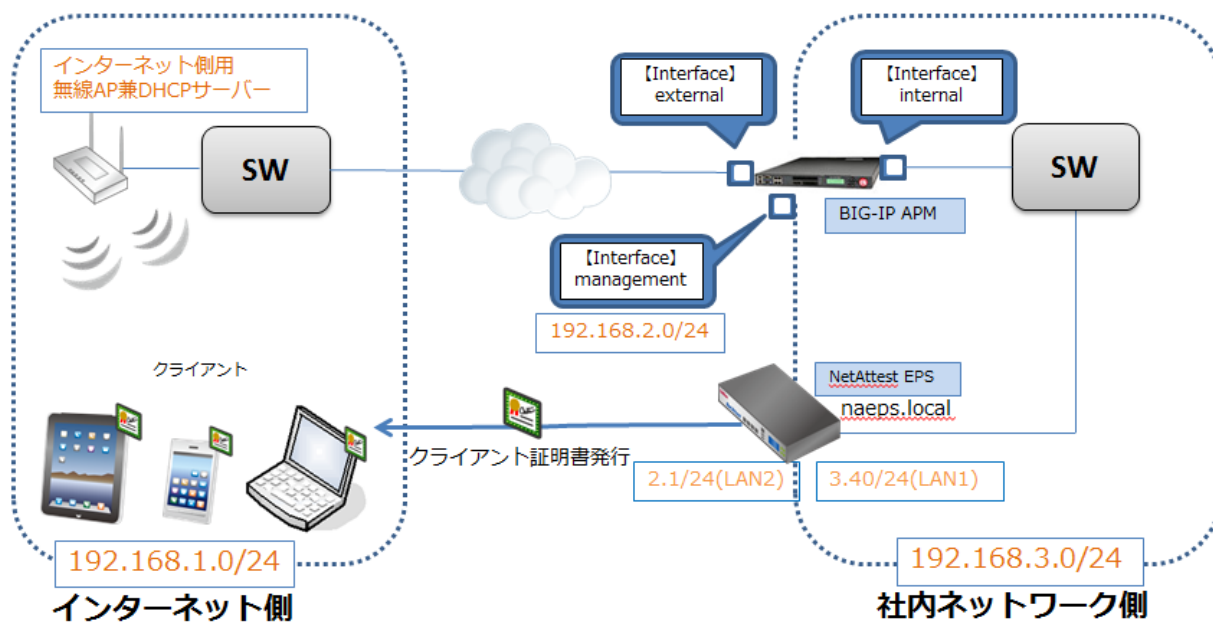
目次

1. 構成.....	6
1-1 構成図.....	6
1-2 環境.....	7
1-2-1 機器.....	7
1-2-2 認証方式.....	7
1-2-3 ネットワーク設定.....	7
2. NetAttest EPS の設定.....	8
2-1 システム初期設定ウィザードの実行.....	8
2-2 サービス初期設定ウィザードの実行.....	9
2-3 認証ユーザーの追加登録.....	10
2-4 クライアント証明書の発行.....	11
3. BIG-IP APM の設定.....	12
3-1 管理インターフェイスの設定.....	12
3-2 デバイスウィザードの実行.....	13
3-3 AAA サーバーの登録.....	18
3-4 Access Policy の設定.....	19
3-4-1 RADIUS 認証の設定.....	20
3-4-2 証明書認証の設定.....	21
3-5 サーバー証明書の発行とインポート手順.....	22
3-5-1 CSR の作成(BIG-IP APM).....	23
3-5-2 サーバー証明書の発行 (NetAttest EPS).....	25
3-5-4 CA 証明書と CRL の取得 (NetAttest EPS).....	26
3-5-5 サーバー証明書のインポート (BIG-IP APM).....	27
3-5-6 CA 証明書のインポート (BIG-IP APM).....	28
3-6 SSL 接続関連の設定(BIG-IP APM).....	29
3-6-1 CRL のインポート (アップロード).....	29
3-6-2 SSL プロファイル設定.....	29
4. 各種 VPN クライアントの設定.....	33
4-1 Windows 版 BIG-IP Edge Client.....	33
4-1-1 PC へのデジタル証明書のインストール.....	33

4-1-2 BIG-IP Edge Client の接続設定	35
4-1-3 接続テスト	36
4-2 iOS 版 BIG-IP Edge Client	37
4-2-1 iOS へのデジタル証明書のインストール.....	37
4-2-2 BIG-IP Edge Client の接続設定	38
4-2-3 iOS 版 BIG-IP Edge Client を利用した VPN 接続.....	39
4-3 Android 版 BIG-IP Edge Client.....	40
4-3-1 Android へのデジタル証明書のインストール.....	40
4-3-2 VPN クライアント(BIG-IP Edge Client)の接続設定	41
4-3-3 接続テスト	42

1. 構成

1-1 構成図



1-2環境

1-2-1機器

製品名	メーカー	役割	バージョン
NetAttest EPS-ST04	Soliton Systems	認証サーバー (RADIUS サーバー、CA)	Ver. 4.4.3
BIG-IP Access Policy Manager	F5 Networks Japan	RADIUS クライアント (SSL VPN 機器)	Ver. 10.2.4.577.0
WAPM-APG300N	BUFFALO	無線 AP (インターネット側用)	Ver. 2.5.1
Let's note CF-SX2	Panasonic	Client PC	Windows 7 SP1
iPhone	Apple	Client smart Device1	iOS 6.1.2
Nexus7	google	Client smart Device2	4.2.2

1-2-2認証方式

デジタル証明書認証+ID・Password 認証

1-2-3ネットワーク設定

	EPS-ST04	BIG-IP APM	Client PC	Client Tablet	無線 AP
IP アドレス	192.168.3.40/24 (LAN1) 192.168.2.1/24 (LAN2)	192.168.1.200/24(external) 192.168.2.200/24(manage) 192.168.3.200/24(internal) 192.168.1.10/24(仮想 sv)	DHCP (無線 AP から)	DHCP (無線 AP から)	192.168.1.110 /24
RADIUS port (Authentication)	UDP 1812		-	-	-
RADIUS port (Accounting)	UDP 1813		-	-	-
RADIUS Secret (Key)	secret		-	-	-

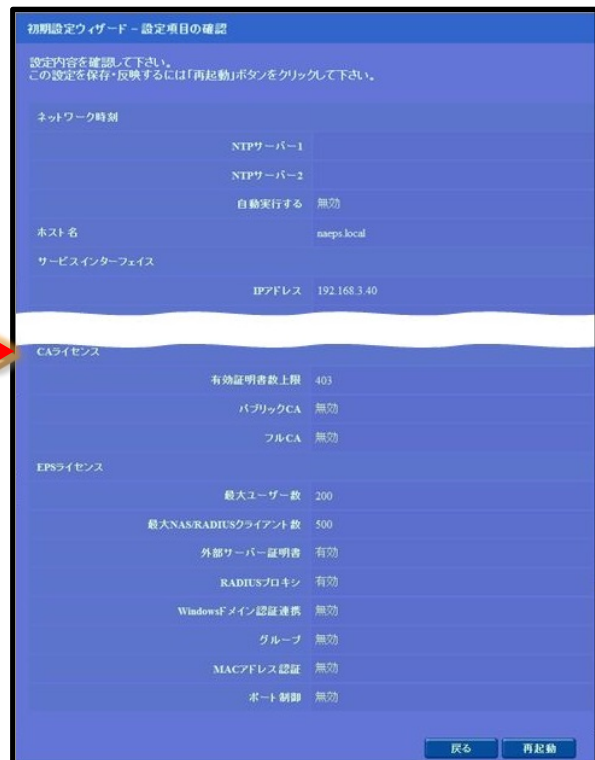
2. NetAttest EPS の設定

2-1システム初期設定ウィザードの実行

http://192.168.2.1:2181(LAN2 デフォルト)にアクセスしシステム初期設定ウィザードを使用し、以下の項目を設定します。

- タイムゾーンと日付・時刻の設定
- ホスト名の設定
- サービスインターフェイスの設定
- 管理インターフェイスの設定

メインネームサーバーの設定



2-2サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

本手順書では値を記載しているもの以外はすべてデフォルト設定で行いました。

- CA 構築
- LDAP データベースの設定
- RADIUS サーバーの基本設定 (全般)
- RADIUS サーバーの基本設定 (証明書検証)
- NAS/RADIUS クライアント設定

項目	値
CA 種別選択	ルート CA
公開鍵方式	RSA
鍵長	2048
CA 名	TestCA

項目	値
NAS/RADIUS クライアント名	BIGip_APM
IP アドレス (Authenticator)	192.168.3.200
シークレット	secret

2-3 認証ユーザーの追加登録

NetAttest EPS の管理画面より、認証ユーザーの登録を行います。

「ユーザー」→「ユーザー一覧」から、「追加」ボタンでユーザー登録を行います。

項目	値
姓	user01
ユーザーID	user01
パスワード	password

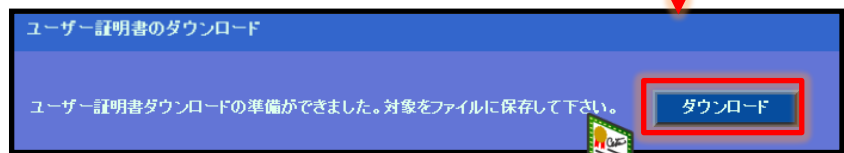
2-4クライアント証明書発行

NetAttest EPS の管理画面より、クライアント証明書の発行を行います。

「ユーザー」→「ユーザー一覧」から、該当するユーザーのクライアント証明書を発行します。(クライアント証明書は、user01_02.p12 という名前で保存)



項目	値
証明書有効期限	365
PKCS#12 ファイルに証明機関の...	チェック有



3. BIG-IP APM の設定

3-1 管理インターフェイスの設定

BIG-IP APM の管理インターフェイスの IP アドレスと Default Gateway 設定は CLI で行います。

```
BIG-IP 10.2.4 Build 577.0
Kernel 2.6.18-164.11.1.el5.1.0.f5app on an i686
epstestAPM login: root
Password:
Last login: Fri Jul 19 20:29:31 on tty1
[root@epstestAPM:Active] config # tms
root@epstestAPM(Active)(tmos)# create sys management-ip 192.168.2.200/255.255.25
5.0
root@epstestAPM(Active)(tmos)# save sys base-config
/config/bigip_base.conf was renamed to /config/bigip_base.conf.bak (64 lines).
/config/bigip_sys.conf was renamed to /config/bigip_sys.conf.bak (69 lines).
root@epstestAPM(Active)(tmos)# _
```

```
# tms
```

```
# create sys management-ip 192.168.2.200/255.255.255.0
```

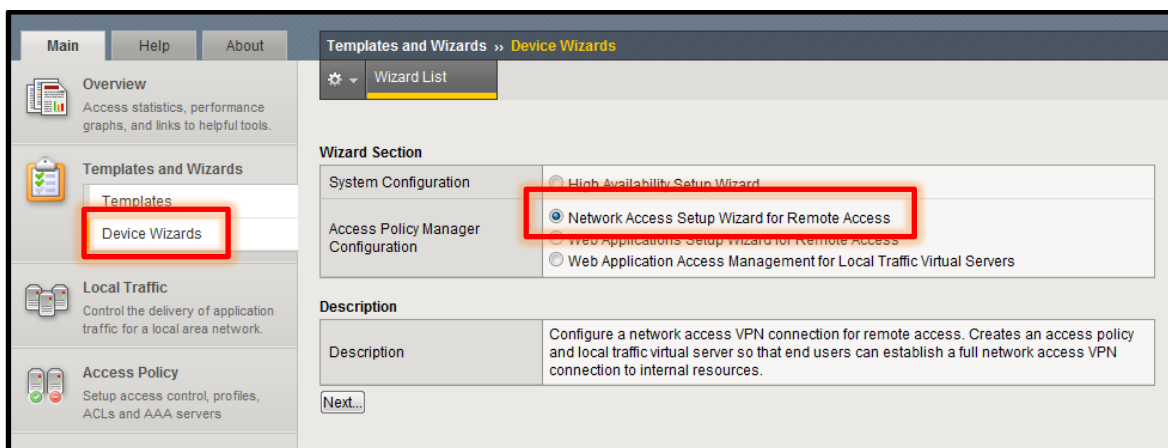
```
# save sys base-config
```

3-2デバイスウィザードの実行

管理 PC にて[3-1 管理インターフェイスの設定]で付与した IP アドレスに対し Web ブラウザにてアクセス(<https://192.168.2.200>)します。admin アカウント(ライセンス適用時に設定したパスワード)でログインし、デバイスウィザードから以下の項目を設定します。

- Basic Properties
- SystemDNS/NTP Configuration
- Select Authentication
- Lease Pool
- Network Access
- DNS Hosts
- Virtual Server

デバイスウィザードは、[Templates and Wizard]-[Device Wizards]から実行します。



【Basic Properties の設定】

アクセスポリシーなどを設定する際に使用する、ポリシー名などを設定します。

The **Default Language** specifies the language to be displayed to end users by default. Choices are English (en), Japanese (jp), Simplified Chinese (zh-cn), and Traditional Chinese (zh-tw).

The **Client Side Checks** checkbox allows you to add a simple antivirus client-side check to the access policy, to ensure end users connecting have antivirus software enabled. You can later configure this antivirus check for specific antivirus vendor products, versions, and virus definition dates.

Policy Name	test_policy
Default Language	ja
Client Side Checks	<input type="checkbox"/> Enable Antivirus Check in Access Policy

Buttons:

項目	値
Policy Name	test_policy
Default Language	jp
Client Side Checks	チェックなし

【SystemDNS/NTP の設定】

DNS、NTP を設定します。必須項目のため、仮の値でも良いので設定を行なってください。

Please configure system DNS and NTP server settings. These system settings are critical for correct operation of created access policies.

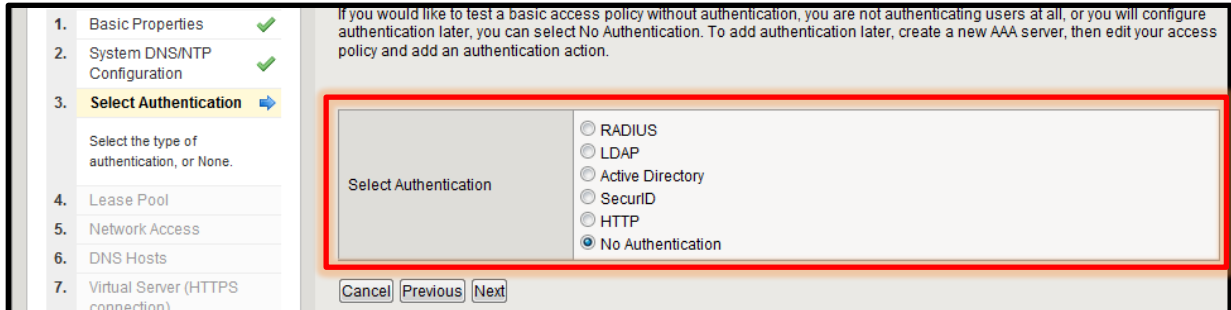
Properties	Address
DNS Lookup Server List	192.168.2.10
DNS Search Domain List	
DNS Cache	<input type="checkbox"/>
Time Server List	192.168.2.10

Buttons:

項目	値
DNS Lookup Server List	192.168.2.10
Time Server List	192.168.2.10

【Select Authentication の設定】

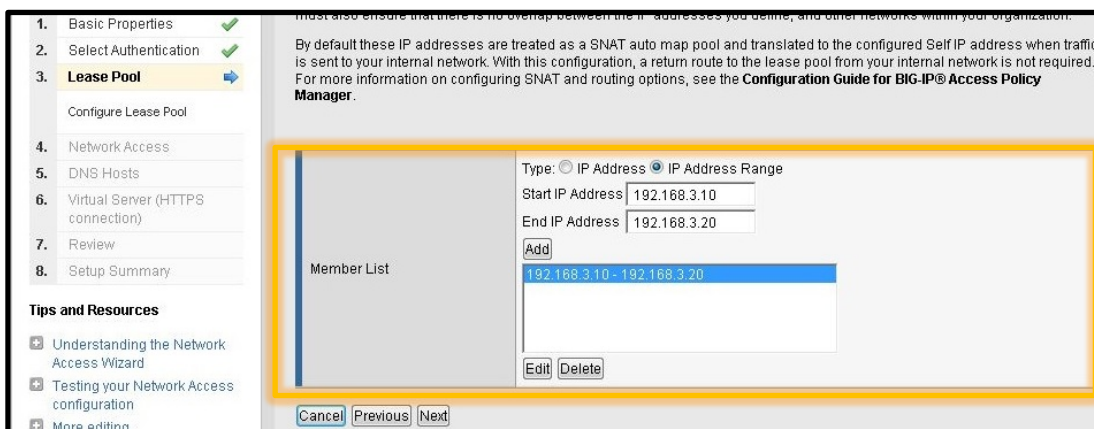
認証タイプを指定します。認証サーバー設定は後で行いますので、ここでは「No Authentication」を指定します。



項目	値
Selected Authentication	No Authentication

【Lease Pool】

VPN 装置がクライアントに動的に割り当てるアドレスプールを設定します。



項目	値
Member List	IP Address Range
Start IP Address	192.168.3.10
End IP Address	192.168.3.20

【Network Access】

クライアントの通信設定を行います。本書では、デフォルト設定のままとします。

1. Basic Properties ✓
 2. System DNS/NTP Configuration ✓
 3. Select Authentication ✓
 4. Lease Pool ✓
 5. **Network Access** →
 Configure Network Access
 6. DNS Hosts
 7. Virtual Server (HTTPS connection)

Compression: No Compression

Client Settings

Traffic Options: Force all traffic through tunnel
 Use split tunneling for traffic

Allow Local Subnet: Enable

Client Side Security: Prohibit routing table changes during Network Access connection

DTLS:

【DNS Hosts】

クライアント端末に配布する DNS サーバー情報の設定を行います。

1. Basic Properties ✓
 2. System DNS/NTP Configuration ✓
 3. Select Authentication ✓
 4. Lease Pool ✓
 5. Network Access ✓
 6. **DNS Hosts** →
 Configure DNS Hosts
 7. Virtual Server (HTTPS connection)
 8. Review
 9. Setup Summary

Tips and Resources
 Understanding the Network Access Wizard
 Testing your Network Access configuration
 More editing...

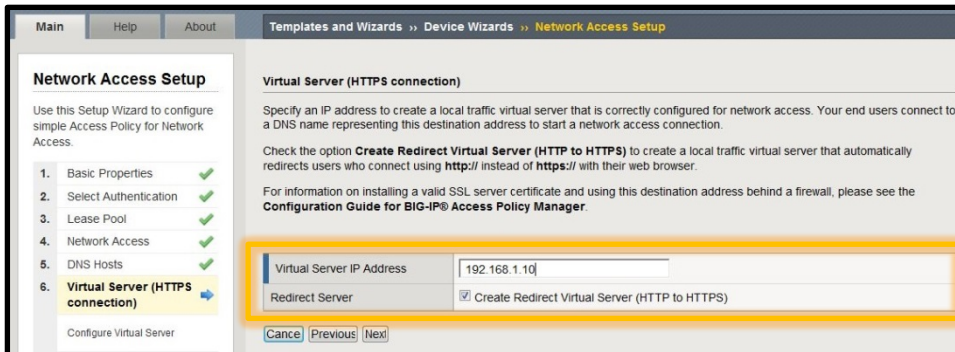
These settings may be different than the DNS System Settings configured under System > Configuration > Device > DNS. For more information on these configuration options, click the Help tab on the navigation pane.

Primary Name Server: 192.168.2.10
 Secondary Name Server:
 Primary WINS Server:
 Secondary WINS Server:
 DNS Default Domain Suffix:
 Host Name:
 IP Address:
 Add
 Static Hosts
 Edit Delete

項目	値
Primary Name Server	192.168.2.10

【Virtual Server (HTTPS Connection)】

仮想サーバーの IP アドレスの設定を行います。クライアントが VPN リモートアクセスの際にこの IP アドレスを指定します。本設定完了後、デバイスウィザードで設定した内容の確認画面が出ますので、設定が間違っていないか確認します。



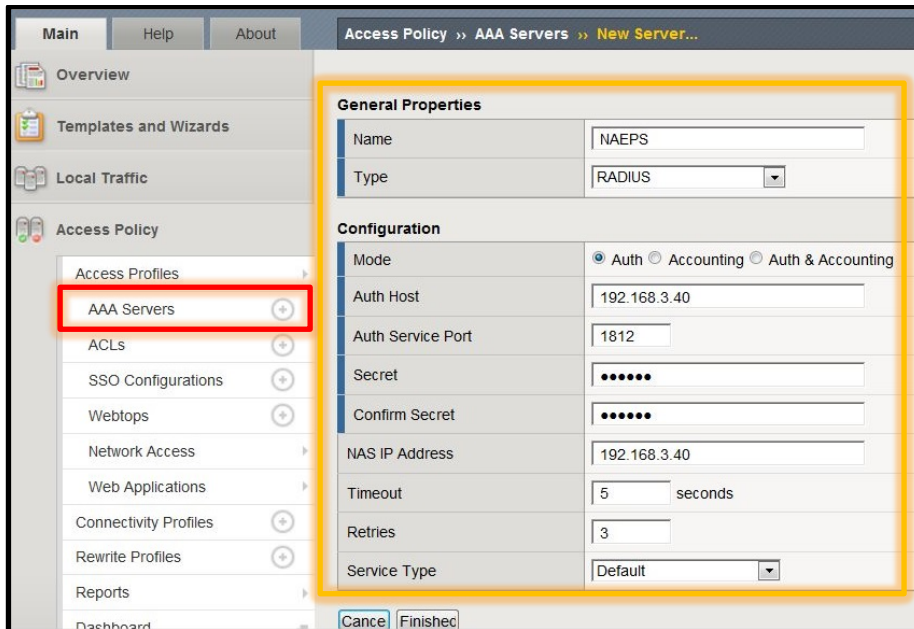
The screenshot shows the 'Network Access Setup' wizard. On the left, a list of steps includes 'Virtual Server (HTTPS connection)' as the current step. The main area is titled 'Virtual Server (HTTPS connection)' and contains instructions. A yellow box highlights the 'Virtual Server IP Address' field with the value '192.168.1.10' and the 'Create Redirect Virtual Server (HTTP to HTTPS)' checkbox, which is checked.

項目	値
Virtual Server IP Address	192.168.1.10

3-3AAA サーバーの登録

NetAttest EPS を RADIUS サーバーとして登録します。

[Access Policy]-[AAA Servers]と進み登録してください。

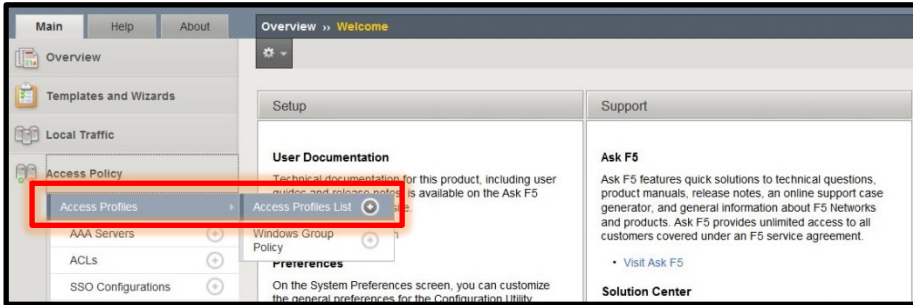


項目	値
Name	NAEPS
Type	RADIUS
Mode	Auth
Auth Host	192.168.3.40
Auth Service Port	1812
Secret	secret
Nas IP Address	192.168.3.40

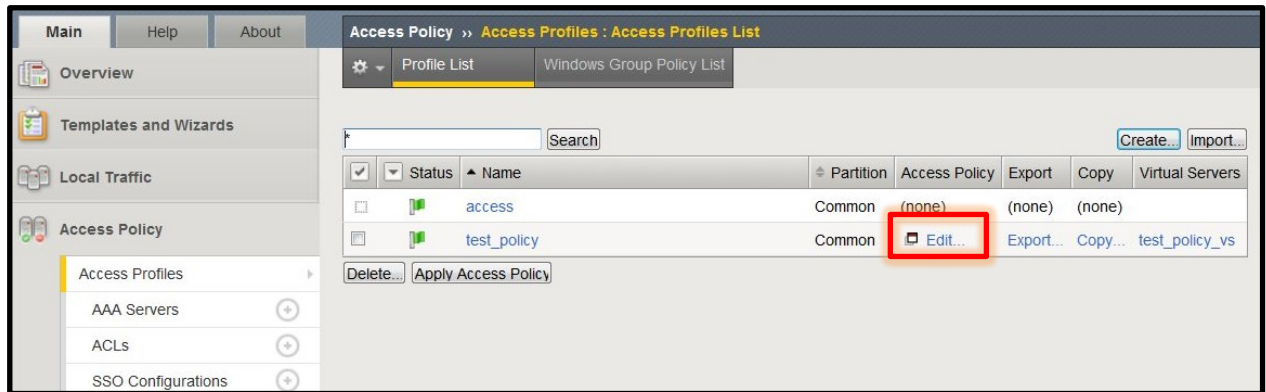
3-4 Access Policy の設定

証明書 + ID・Password での認証が行えるよう、Access Policy の設定を行います。

[Access Policy]-[Access Profiles]-[Access Profiles List]と進みます。

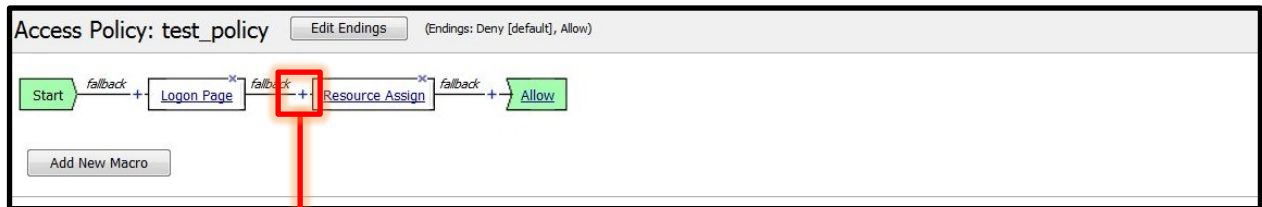


「3-2.デバイスウィザードの設定」で作成した Policy 「test_policy」を編集し、RADIUS 認証の設定と証明書認証の設定を行います。



3-4-1 RADIUS 認証の設定

[Resource Assign]の左側の[+]をクリックし RADIUS 認証設定を行います。

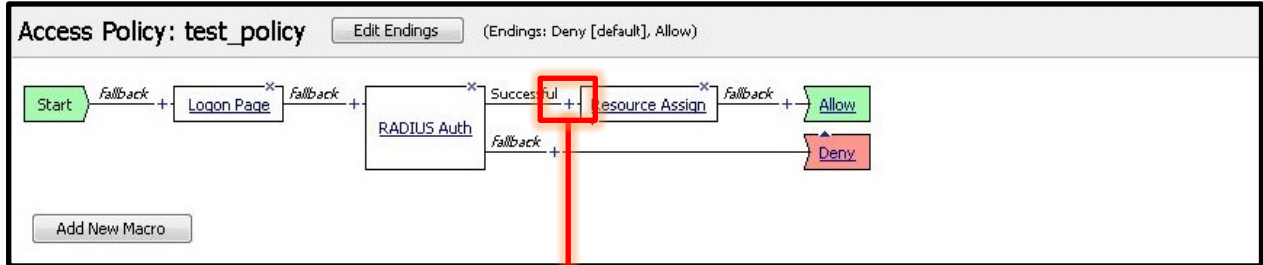


項目	値
Authentication	RADIUS Auth

項目	値
AAA Server	NAEPS

3-4-2 証明書認証の設定

[Resource Assign]左側の[+]をクリックし証明書認証の設定をします。



- Logging Agent
- Message Box
- Decision box agent with two options
- Raises ACCESS_POLICY_AGENT_EVENT in iRule
- Empty Action
- Authentication**
 - Active Directory Authentication
 - Active Directory Query / Group Mapping
 - Check the result of client cert authenticated by the clientSSL profile
 - HTTP Authentication
 - LDAP Authentication
 - LDAP Query / Group Mapping
 - On-Demand Cert Auth** - Initiate SSL rehandshake and validate the received certificate
 - RADIUS Authentication
 - RADIUS Accounting
 - RSA SecurID Authentication
- Client Side Checks**
 - Antivirus Check for Windows, Mac and Linux
 - Firewall Check for Windows, Mac and Linux
 - Windows File Check
 - Windows Machine Cert Auth

Buttons: Cancel, Add Item, Help

項目	値
Auth Mode	Require

Properties* Branch Rules

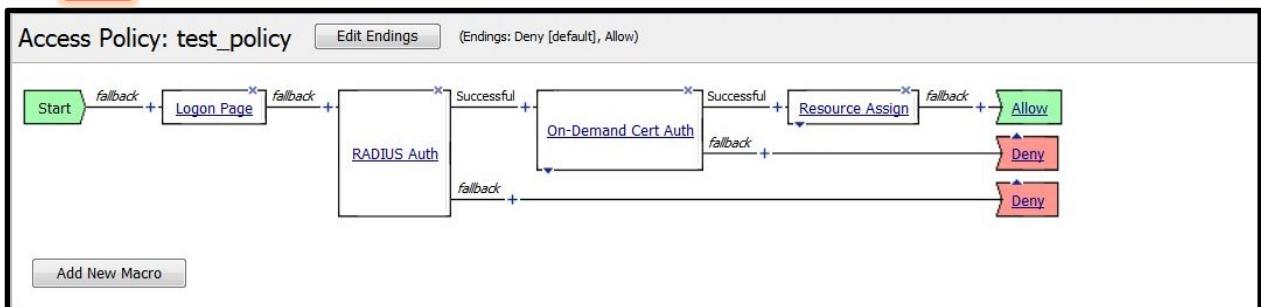
Name: On-Demand Cert Auth

On-Demand Cert Auth

Auth Mode: Require

Buttons: Cancel, Save (Data in tab has been changed, please don't forget to save), Help

項目	値
Authentication	On-Demand Cert Auth



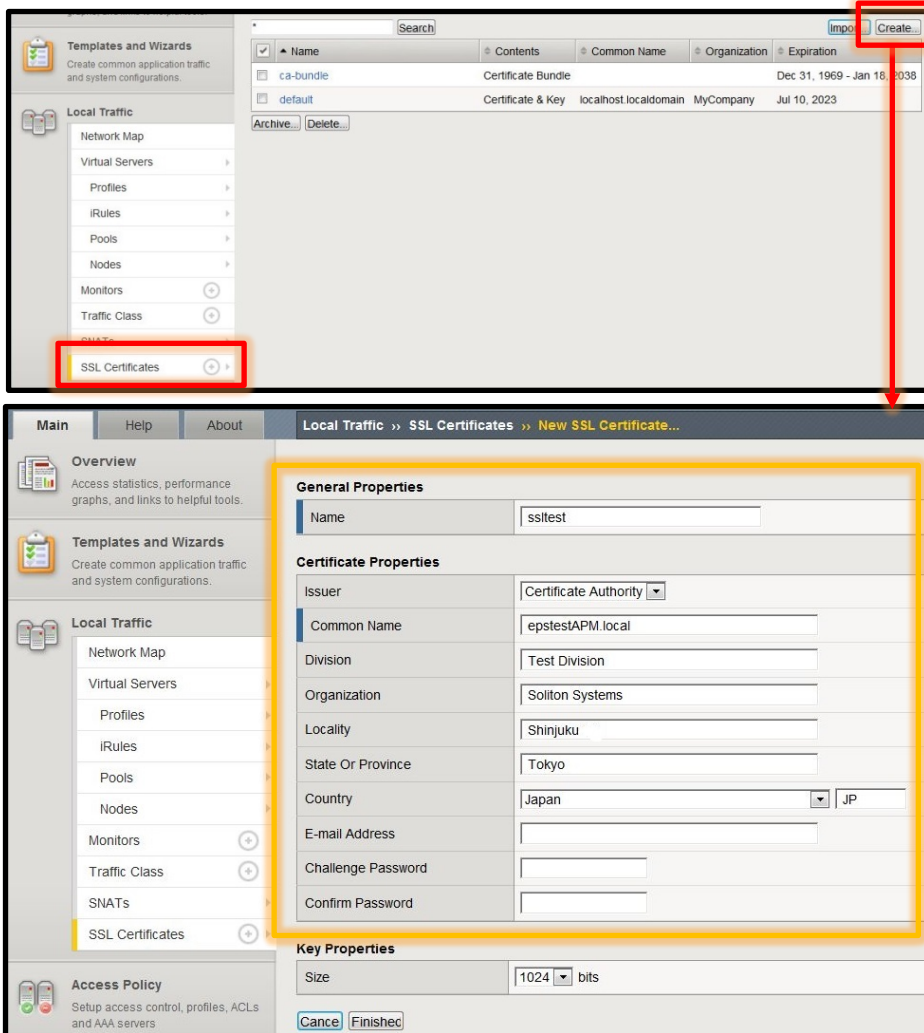
3-5サーバー証明書の発行とインポート手順

以下の手順でサーバー証明書と CA 証明書を BIG-IP APM にインポートします。

- CSR の作成
- サーバー証明書署名要求
- サーバー証明書の発行
- サーバー証明書ダウンロード
- CA 証明書の取得
- CA 証明書のインポート
- サーバー証明書のインポート

3-5-1 CSR の作成(BIG-IP APM)

[Local Traffic]-[SSL Certificates]-[create]と進み、CSR を作成します。



項目	値
Name	ssltest
Issuer	Certificate Authority
Common Name	epstestAPM.local
Division	Test Division
Organization	Soliton Systems
Locality	Shinjuku
State Or Province	Tokyo
Country	Japan/JP

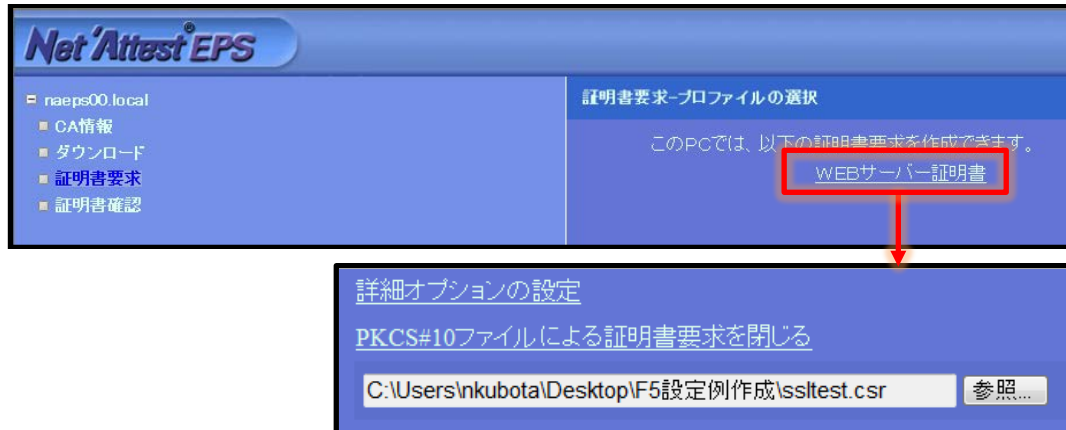
以下の画面が表示されたら[Request File]の[Download ssltest.csr]をクリックし、CSR をダウンロードします。

Certificate Signing Request	
Request Text	<pre>-----BEGIN CERTIFICATE REQUEST----- MIIBwTCCASoCAQAwgYAx CzA JBgNVBAYTAkp A1UEBxMLU2hpbmp1a3Uta3UxGDAWBgNVBAc A1UECzMNVGVzdCBEaXZpc21vbjEzMBCGAlU nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYE PnOSWgh715GnSueVaAjzGZMbmbpr3K9q1Zy RydyGJi/1ghJfpICSLou6hT1z30+/j fLqWK</pre>
Request File	Download ssltest.csr
Certificate Authorities	Digital Signature Trust Company Entrust GlobalSign VeriSign

Finishec

3-5-2サーバー証明書の発行 (NetAttest EPS)

BIG-IP APM で生成した CSR をもとに NetAttest EPS で BIG-IP APM 用サーバー証明書を発行します。NetAttest EPS の管理者向け証明書サービスページ(<http://192.168.2.1/certsrv/>)にアクセスし、下記の手順で CSR をインポートします。



次に、CA 管理ページ(<http://192.168.2.1:2181/caadmin/>)にアクセスし、【保留】状態のサーバー証明書を承認します。

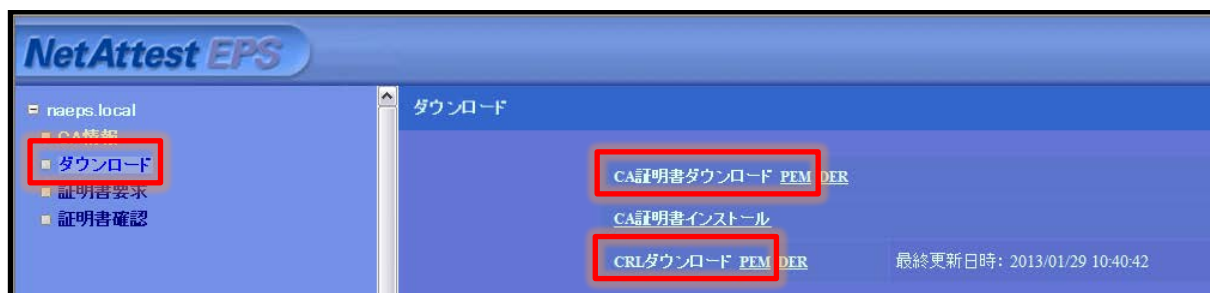


管理者向け証明書サービスページにアクセスします。「証明書の確認」を選択すると状態が【発行】になっていますので、サーバー証明書(nausercert-pem.cer)をダウンロードします。



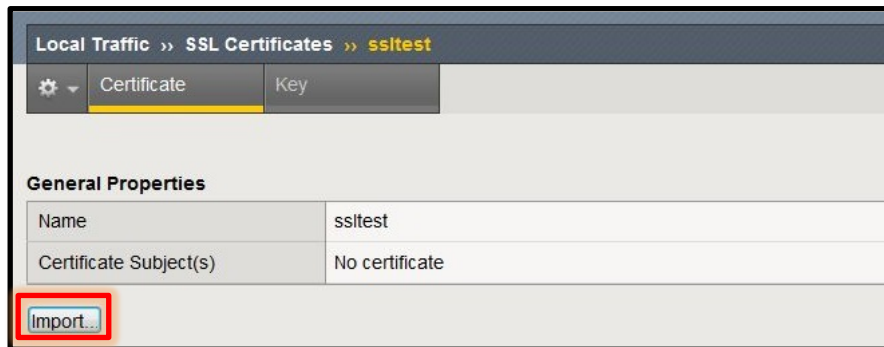
3-5-4CA 証明書と CRL の取得 (NetAttest EPS)

管理者向け証明書サービスページから、NetAttest EPS の CA 証明書をダウンロードします。CA 証明書は、PEM 形式(nacacert-pem.cer)を選択します。

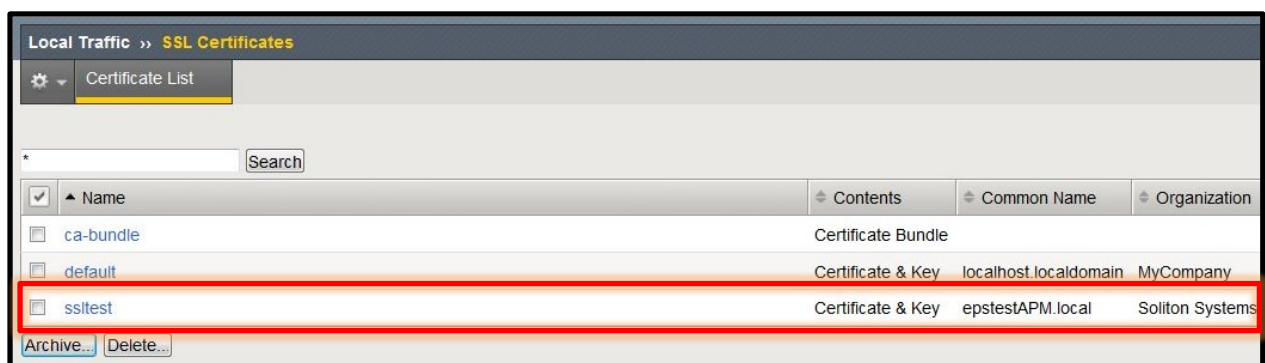
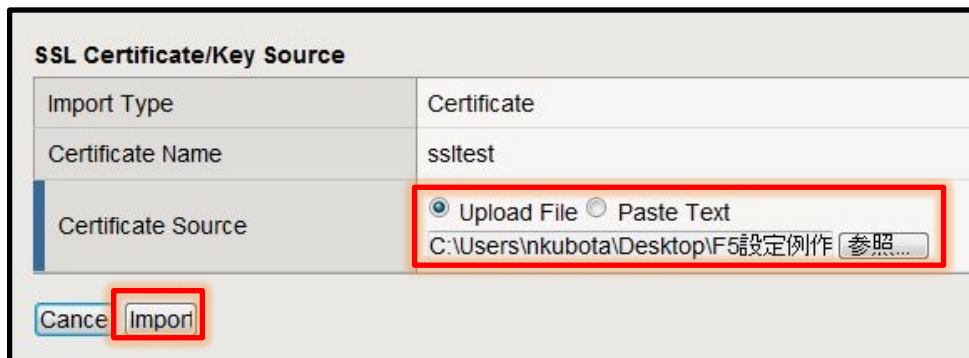


3-5-5サーバー証明書のインポート (BIG-IP APM)

NetAttest EPS から発行したサーバー証明書をインポートします。3-5-1 で CSR のダウンロードを行った後[finished]をクリックすると以下の画面に進みますので[import]をクリックし、NetAttest EPS から作成したサーバー証明書をインポートしてください。



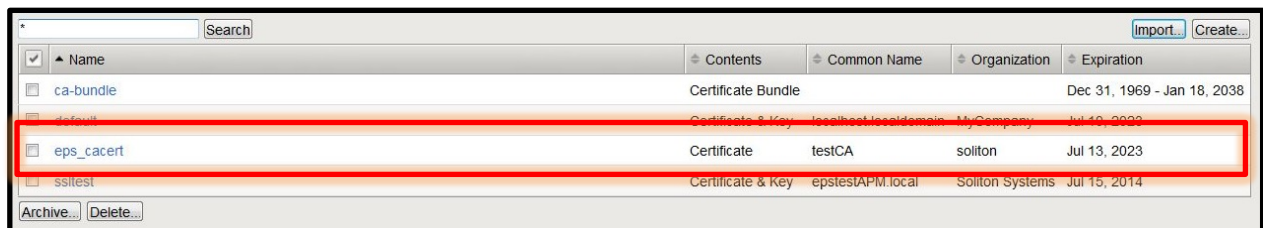
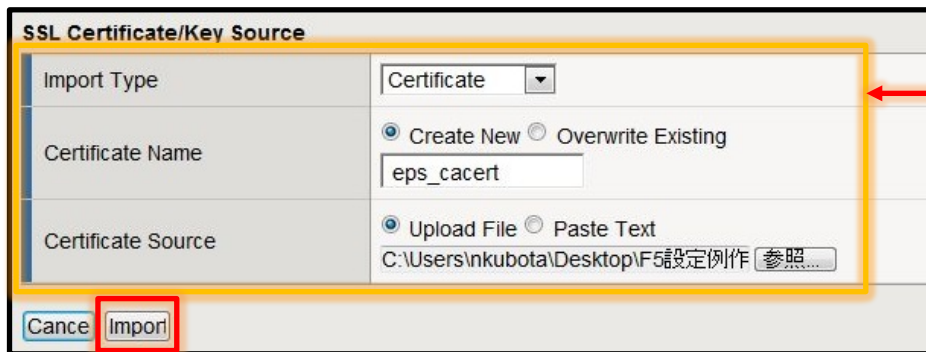
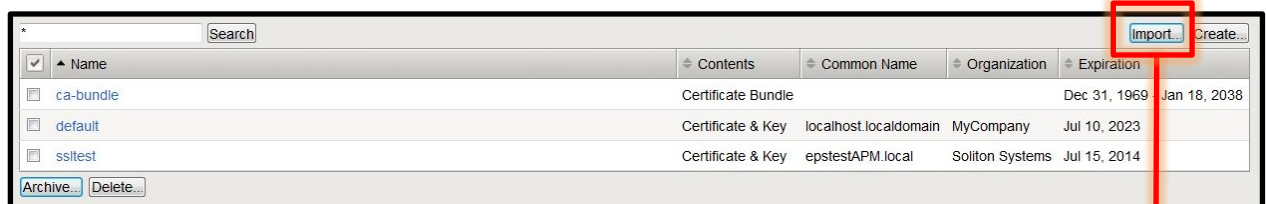
[Upload File]を選択し、NetAttest EPS で発行したサーバー証明書を指定してください。



3-5-6CA 証明書のインポート (BIG-IP APM)

NetAttest EPS からダウンロードした CA 証明書を BIG-IP APM にインポートします。

「Configuration」 - 「Certificates」 - 「Trusted Client CAs」の「Import CA Certificate」から、CA 証明書(nacacert-pem.cer)をインポートします。



3-6 SSL 接続関連の設定(BIG-IP APM)

インポートした証明書を SSL で利用できるようにします。まず、CRL のインポートを行った後に CA 証明書、サーバー証明書、CRL の指定を行います。

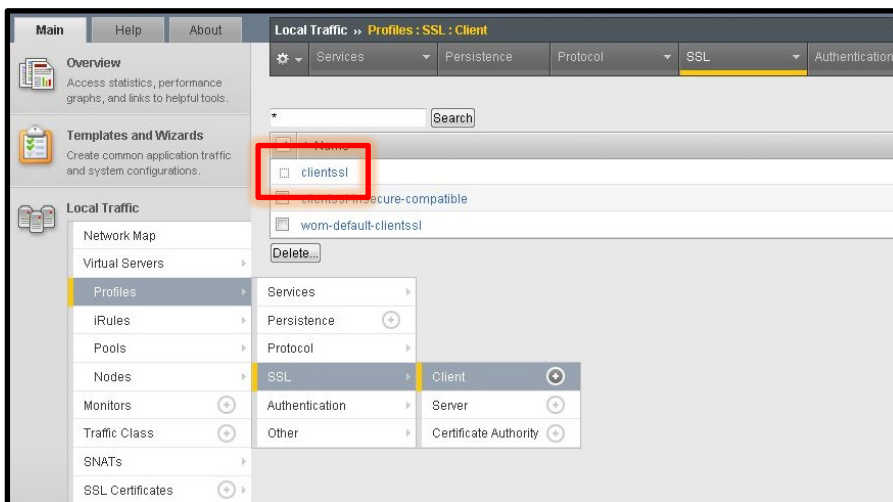
3-6-1 CRL のインポート(アップロード)

CRL を BIG-IP APM にインポートします。今回は CRL のインポートに WinSCP というツールを用いて行いました。WinSCP をコマンド時から実行しました。手順は以下の通りです。

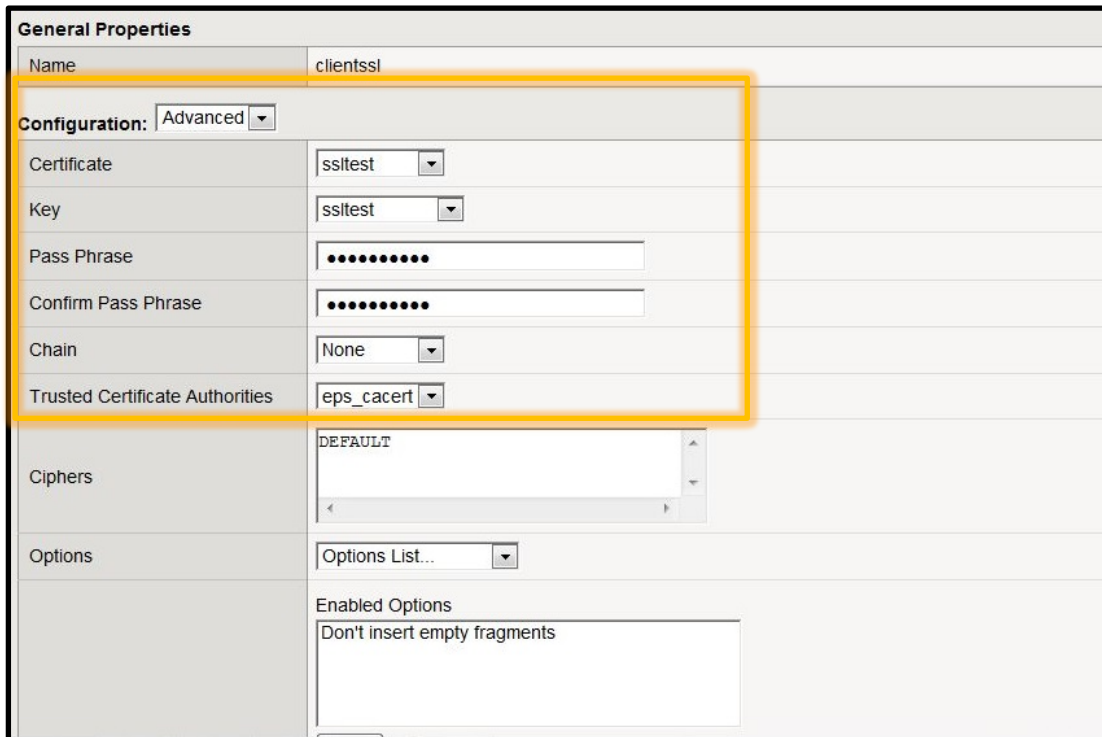
```
> open root:root@192.168.2.200  
> put c:\¥nacacrl.crl /config/ssl/ssl.crl/  
> ls /config/ssl/ssl.crl/  
> close
```

3-6-2 SSL プロファイル設定

次に[Local traffic]-[Profiles]-[SSL]-[Client]と進み、デフォルトで登録されているプロファイル [Client SSL]をクリックします。



Configuration を Basic から Advanced に変更し、CA 証明書とサーバー証明書を指定します。



General Properties

Name: clientssl

Configuration: **Advanced**

Certificate: ssltest

Key: ssltest

Pass Phrase:

Confirm Pass Phrase:

Chain: None

Trusted Certificate Authorities: eps_cacert

Ciphers: DEFAULT

Options: Options List...

Enabled Options: Don't insert empty fragments

項目	値
certificate	ssltest
key	ssltest
trusted Certificate Authorities	eps_cacert

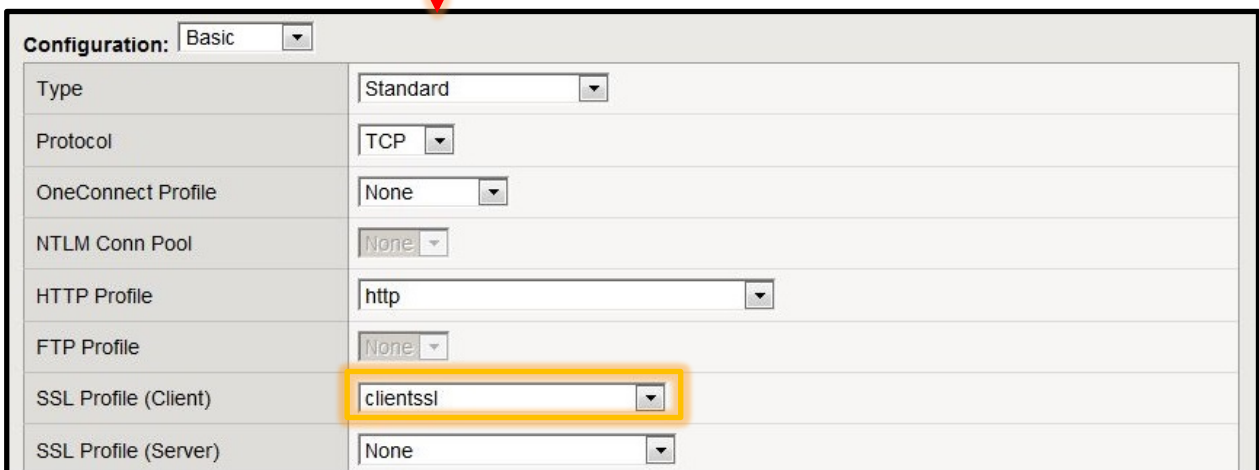
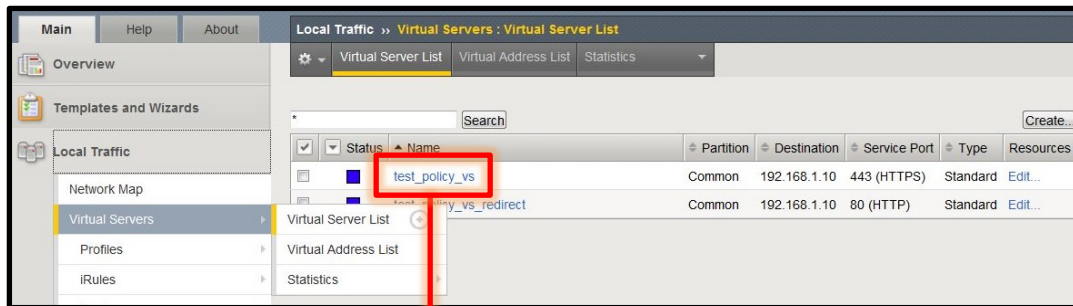
次に、Client Authentication を設定します。

この際、先ほどインポートした CRL を[Certificate Revocation List(CRL)]で指定します。

Options List	<input type="button" value="Disable"/> Available Options Netscape® reuse cipher change bug workaroun... Microsoft® big SSLv3 buffer Microsoft® IE SSLv2 RSA padding SSLeay 080 client DH bug workaround TLS D5 bug workaround <input type="button" value="Enable"/>
ModSSL Methods	<input type="checkbox"/>
Cache Size	262144 sessions
Cache Timeout	Specify... 3600 seconds
Alert Timeout	Specify... 60 seconds
Handshake Timeout	Specify... 60 seconds
Renegotiation	<input checked="" type="checkbox"/> Enabled
Renegotiate Period	Indefinite
Renegotiate Size	Indefinite
Renegotiate Max Record Delay	Specify... 10 records
Secure Renegotiation	Require
Unclean Shutdown	<input checked="" type="checkbox"/> Enabled
Strict Resume	<input type="checkbox"/>
Non-SSL Connections	<input type="checkbox"/>
Client Authentication	
Client Certificate	require
Frequency	always
Certificate Chain Traversal Depth	9
Advertised Certificate Authorities	eps_cacert
Certificate Revocation List (CRL)	certs.crl
<input type="button" value="Update"/>	

項目	値
client certificate	require
frequency	always
Advertised Certificate Authorities	eps_cacert
Certificate Revocation List(CRL)	cert.crl

設定した「client ssl」を[Local traffic]-[Virtual Server]-[Virtual Server list]から[test_policy_vs]のプロファイルとして指定します。



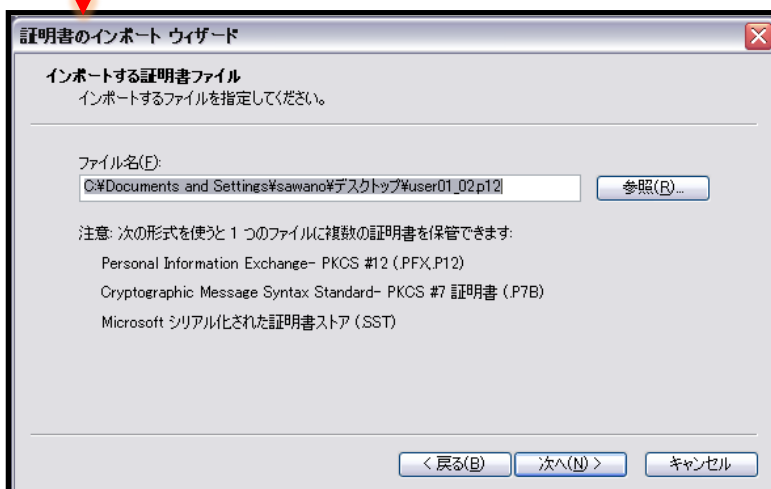
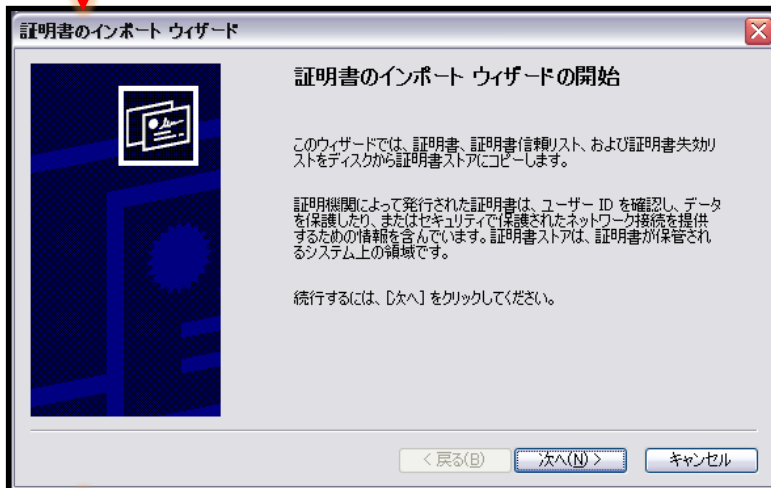
項目	値
SSL Profile (client)	clientssl

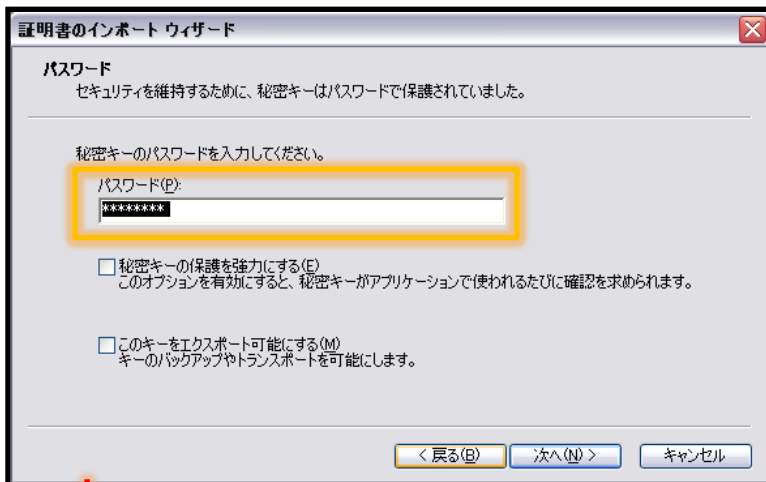
4. 各種 VPN クライアントの設定

4-1 Windows 版 BIG-IP Edge Client


4-1-1 PC へのデジタル証明書のインストール

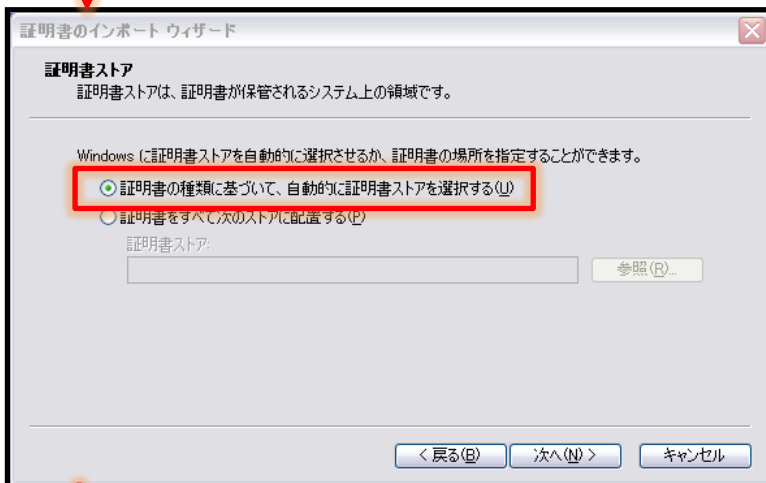
PC にクライアント証明書をインポートします。ダウンロードしておいたクライアント証明書 (user01_02.p12) をダブルクリックすると、証明書インポートウィザードが実行されます。





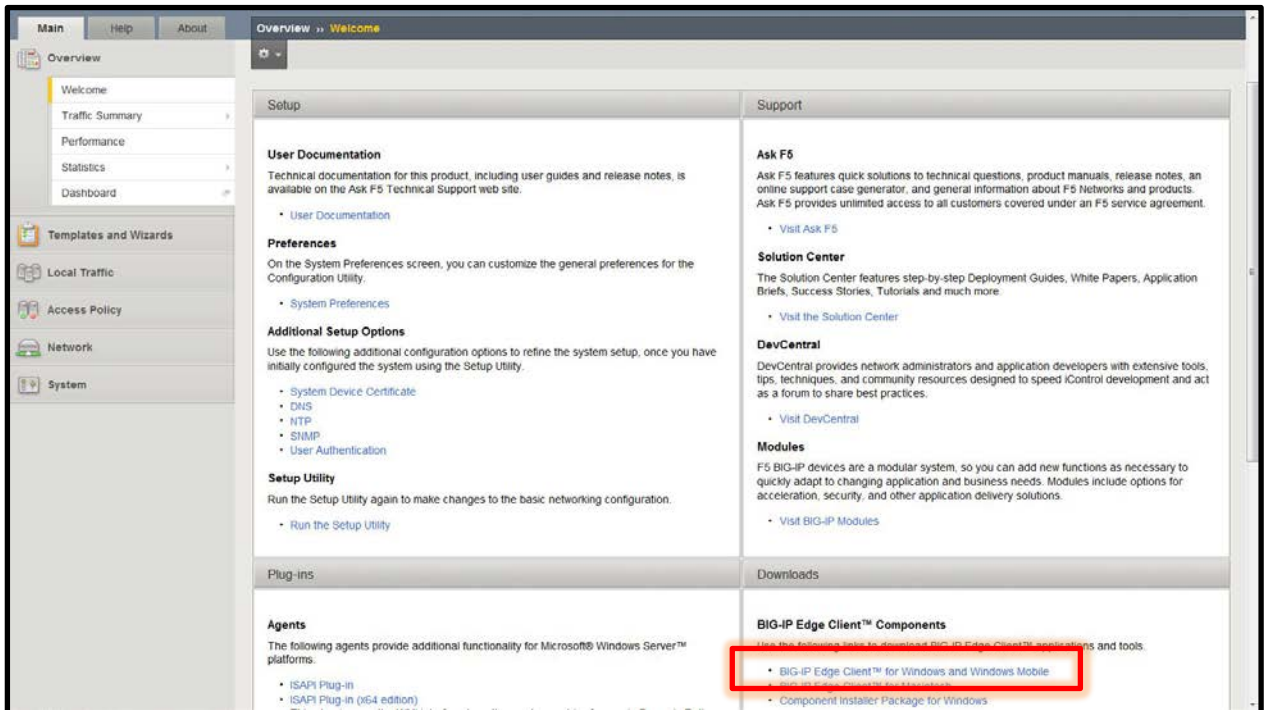
【パスワード】
NetAttest EPS で証明書を
発行した際に設定したパスワードを入力

 iPhone 構成ユーティリティを利用し iOS デバイスにデジタル証明書をインストールする場合は、【このキーをエクスポート可能にする】チェックを入れる必要があります。



4-1-2BIG-IP Edge Client の接続設定

Edge Client を BIG-IP APM からダウンロードし、インストールします。BIG-IP 管理画面 TOP の [BIG-IP Edge Client for Windows and Windows Mobile]からダウンロードします。



インストール後、[サーバーの変更]からサーバーを指定します。この際、3-2 デバイスウィザードで設定した仮想サーバーの IP アドレス(名前解決できるようにであれば名前)を指定します。



4-1-3接続テスト

BIG-IP Edge Client を利用し、VPN 接続を行います。なお、ブラウザを利用して、接続することも可能です。



項目	値
ユーザー名	user01
パスワード	password



4-2iOS 版 BIG-IP Edge Client

4-2-1iOS へのデジタル証明書のインストール

NetAttest EPS から発行したデジタル証明書を iOS デバイスにインストールする方法として、下記の方法などがあります。

- 1) iPhone 構成ユーティリティ（構成プロファイル）を使う方法
- 2) デジタル証明書をメールに添付し iOS デバイスに送り、インストールする方法
- 3) SCEP で取得する方法 (NetAttest EPS-ap を利用できます)

いずれかの方法で CA 証明書とクライアント証明書をインストールします。

※本書では割愛します。

4-2-2 BIG-IP Edge Client の接続設定

BIG-IP Edge Client を Apple App Store からインストールします。

インストール後 BIG-IP Edge Client を起動し、下記のように設定を保存します。

項目	値
接続先名	192.168.1.10
サーバ	192.168.1.10
証明書の使用	オン
証明書	user01
ユーザー名	user01
パスワード	password

4-2-3iOS 版 BIG-IP Edge Client を利用した VPN 接続

BIG-IP Edge Client を利用し、VPN 接続を行います。



4-3Android 版 BIG-IP Edge Client

4-3-1 Android へのデジタル証明書のインストール

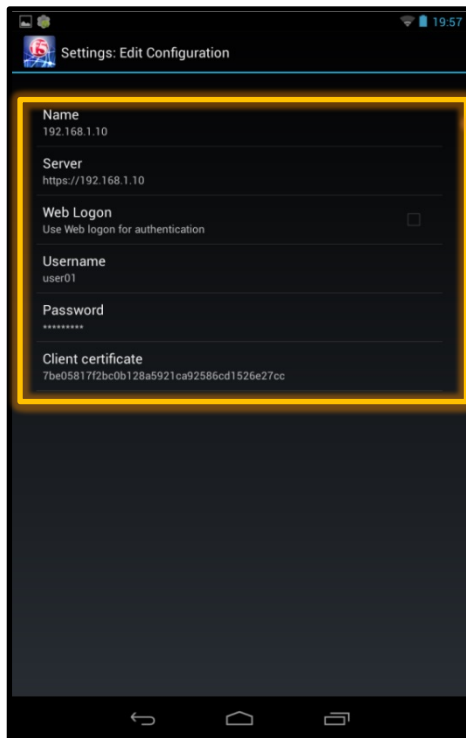
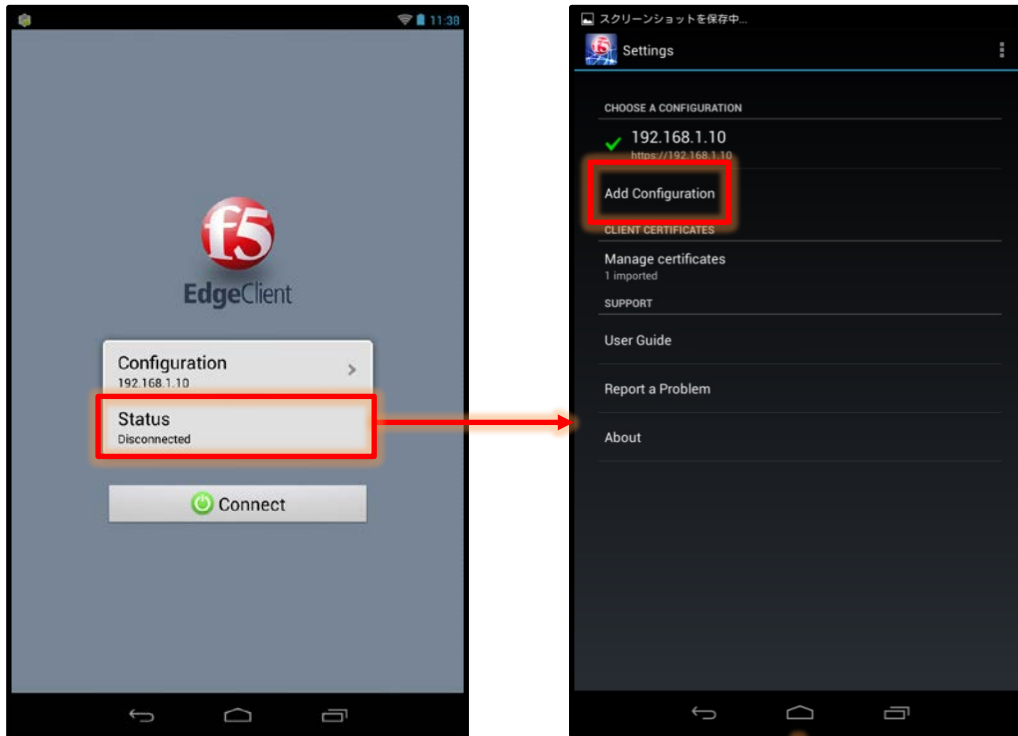
NetAttest EPS から発行したデジタル証明書を Android デバイスにインストールする方法として、下記の方法などがあります。

- 1)USB 接続し証明書を Android 内部に保存した後、インポートする方法
- 2) デジタル証明書をメールに添付し Android に送り、インストールする方法

いずれかの方法で CA 証明書とクライアント証明書をインストールしますが、実際のインポート方法、手順などは各 Android 端末に依存するため本書では割愛します。

4-3-2VPN クライアント(BIG-IP Edge Client)の接続設定

BIG-IP Edge Client を google play Store からインストールします。インストール後 BIG-IP Edge Client を起動し、下記のように設定を保存してください。



項目	値
Name	192.168.1.10
Server	https://192.168.1.10
Username	user01
Password	password
Client certificate	インポートした証明書を選択
Name	192.168.1.10

4-3-3

4-3-4接続テスト

BIG-IP Edge Client を利用し、VPN 接続を行います。

