

# **NetAttest EPS**

## 認証連携設定例

【連携機器】 Juniper NetWorks MAG 2600

【Case】 Junos pluse を利用した、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 Juniper Networks 社製 VPN ゲートウェイ MAG 2600 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 MAG 2600 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

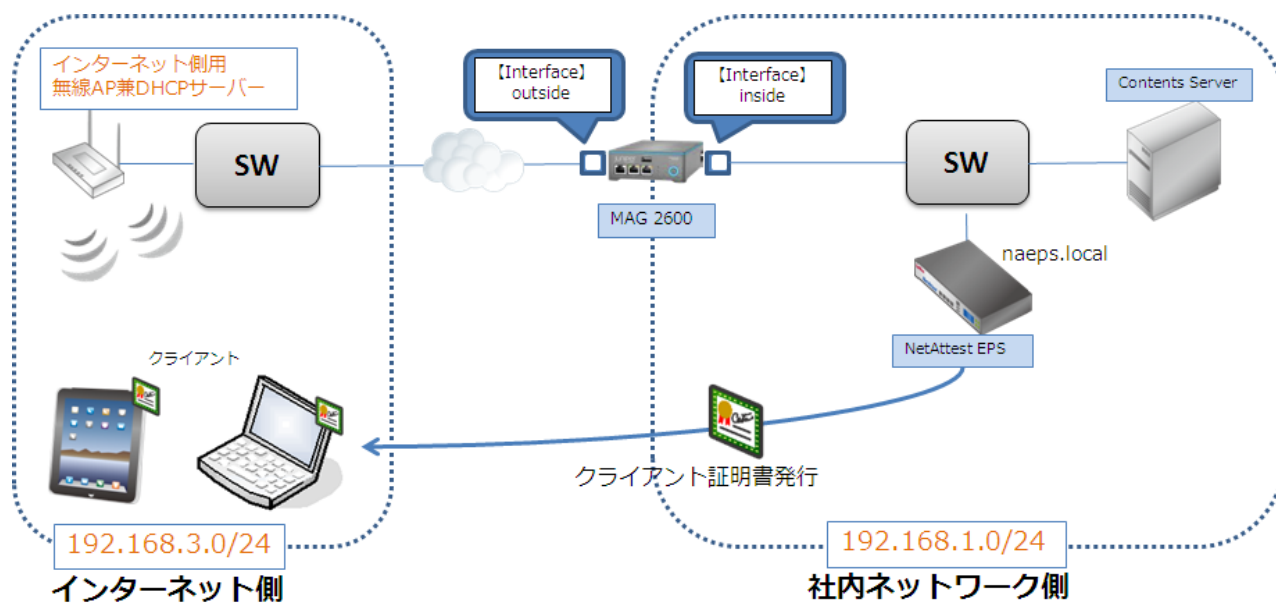
1. 構成.....	6
1-1 構成図.....	6
1-2 環境 .....	7
1-2-1 機器 .....	7
1-2-2 認証方式.....	7
1-2-3 ネットワーク設定.....	7
2. NetAttest EPS の設定 .....	8
2-1 システム初期設定ウィザードの実行.....	8
2-2 サービス初期設定ウィザードの実行.....	8
2-3 認証ユーザーの追加登録 .....	9
2-4 クライアント証明書の発行.....	11
3. MAG 2600 の設定 .....	12
3-1 基本設定.....	12
3-1-1 インターフェイスの設定.....	12
3-1-2 システム時刻設定.....	13
3-1-3 Hosts 設定(任意).....	13
3-2 MAG 2600 の証明書に関する設定 .....	14
3-2-1 SSL に関する設定(参考) (MAG 2600).....	14
3-2-2 CSR の生成 (MAG 2600) .....	15
3-2-3 サーバー証明書署名要求 (NetAttest EPS).....	17
3-2-4 サーバー証明書の発行 (NetAttest EPS).....	17
3-2-5 サーバー証明書のダウンロード (NetAttest EPS) .....	18
3-2-6 CA 証明書の取得 (NetAttest EPS).....	18
3-2-7 サーバー証明書のインポート (MAG 2600) .....	19
3-2-8 CA 証明書のインポート (MAG 2600).....	20
3-3 MAG 2600 の VPN 接続に関する設定 .....	23
3-3-1 RADIUS/Certificate Server の設定.....	23
3-3-2 VPN Roles の設定.....	24
3-3-3 VPN Access Policy の設定.....	26
3-3-4 Authentication Realms の設定 .....	27

---

3-3-5 Sign-In Policy の設定.....	29
3-3-6 IP プールの設定 .....	30
<b>4. 各種 VPN クライアントの設定 .....</b>	<b>31</b>
4-1 Windows 版 Junos Pulse .....	31
4-1-1 PC へのデジタル証明書のインストール .....	31
4-1-2 VPN クライアント(Junos Pulse)の接続設定.....	33
4-2 iOS 版 Junos Pulse .....	34
4-2-1 iOS へのデジタル証明書のインストール .....	34
4-2-2 VPN クライアント(Junos Pulse)の接続設定.....	35
4-3 接続テスト.....	36
4-3-1 Windows 版 Junos Pulse を利用した VPN 接続(トンネリングモード)	36
4-3-2 iOS 版 Junos Pulse を利用した VPN 接続 .....	37

# 1. 構成

## 1-1 構成図



## 1-2環境

### 1-2-1機器

役割	メーカー	製品名	バージョン
Authentication Server (認証サーバー)	Soliton Systems	NetAttest EPS-ST04	Ver. 4.4.3
RADIUS クライアント (SSL VPN 機器)	Juniper Networks	MAG 2600	Ver. 7.1R1 (build 17675)
無線 AP (インターネット側用)	BUFFALO	WAPM-APG300N	Ver. 2.5.1
Client PC	Panasonic	Let's note CF-S9	Windows 7 SP1
Client Tablet	Apple	iPad	iOS 6.0.2

### 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

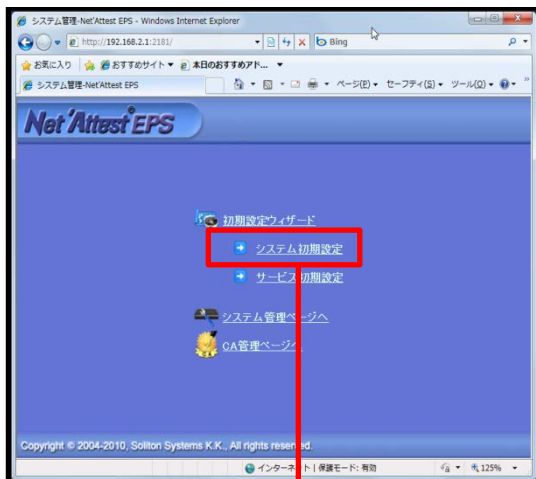
	EPS-ST04	MAG 2600	Client PC	Client Tablet	無線 AP
IP アドレス	192.168.1.2/24	192.168.1.110/24(in) 192.168.3.110/24(out)	DHCP (無線 AP から)	DHCP (無線 AP から)	192.168.3.100/24
RADIUS port (Authentication)	UDP 1812		-	-	-
RADIUS port (Accounting)	UDP 1813		-	-	-
RADIUS Secret (Key)	secret		-	-	-

## 2. NetAttest EPS の設定

### 2-1システム初期設定ウィザードの実行

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



【ホスト名】

・ naeps.local

【IP アドレス】

・ 192.168.1.2(デフォルト)

【ライセンス】

・ なし

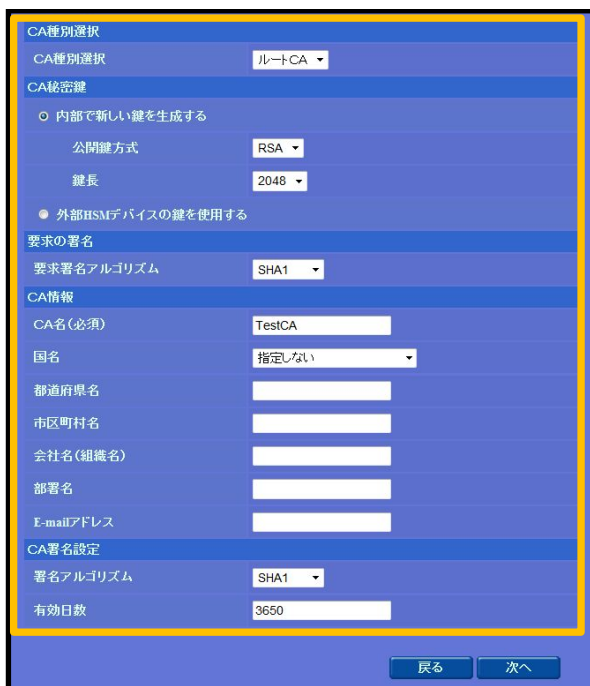


## サービス初期設定ウィザードの実行

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



### 【CA 種別選択】

- ・ ルート CA

### 【公開鍵方式】

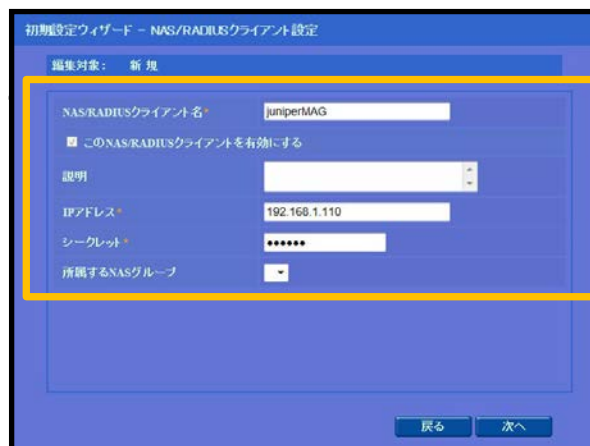
- ・ R S A

### 【鍵長】

- ・ 2048

### 【CA 名】

- ・ TestCA



### 【NAS/RADIUS クライアント名】

- ・ juniperMAG

### 【IP アドレス(Authenticator)】

- ・ 192.168.1.110

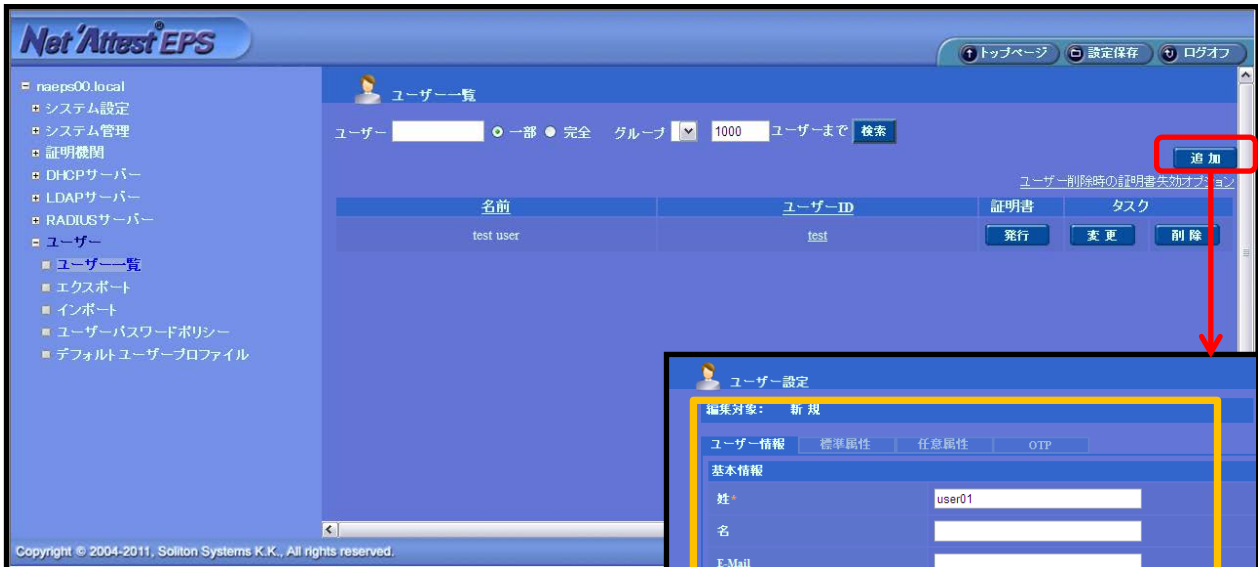
### 【シークレット】

- ・ secret

## 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。



【姓】

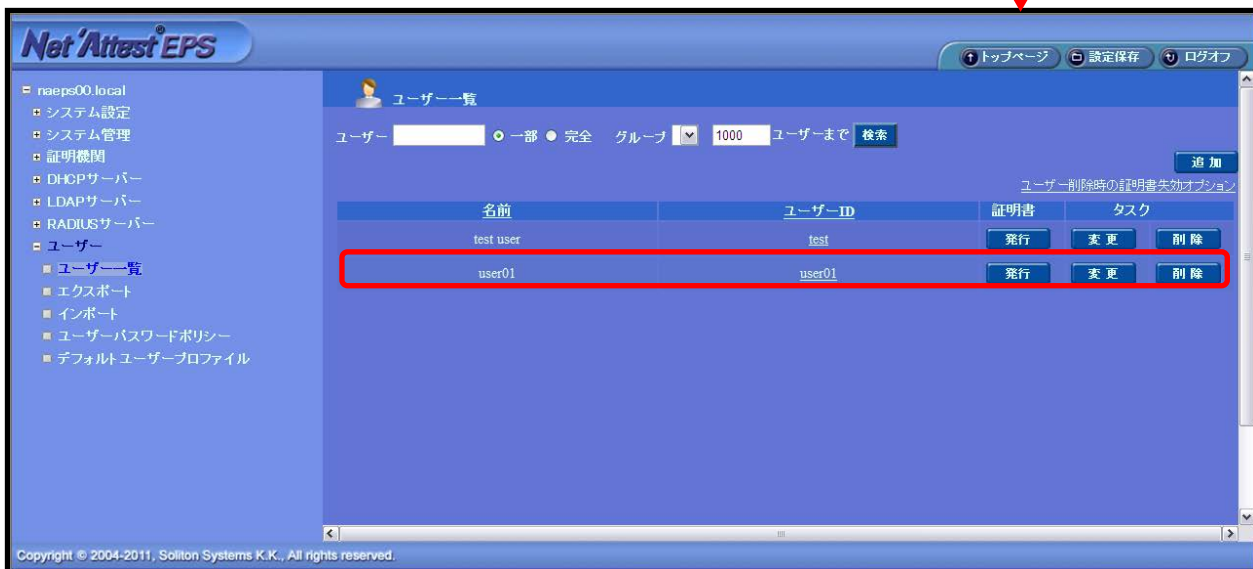
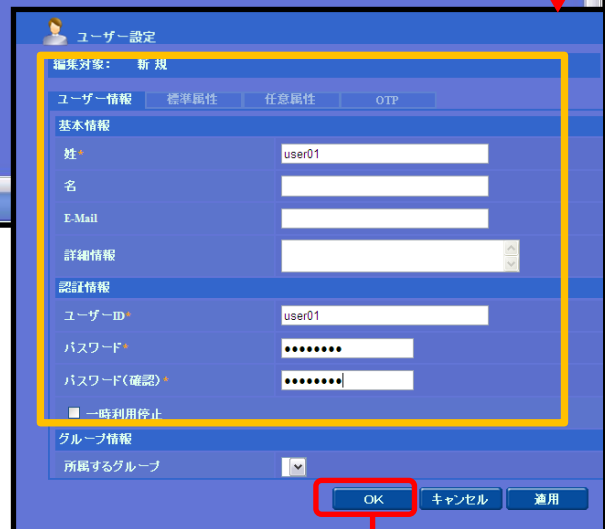
・ user01

【ユーザーID】

・ user01

【パスワード】

・ password



## 2-4クライアント証明書の発行

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)



### 【証明書有効期限】

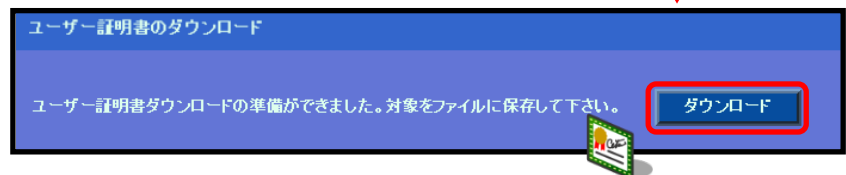
- ・ 365

### 【証明書ファイルオプションパスワード】

- ・ password

### 【PKCS#12 ファイルに証明機関の・・・】

- ・ チェック有



## 3. MAG 2600 の設定

### 3-1 基本設定

#### 3-1-1 インターフェイスの設定

MAG 2600 の設定は WebUI で行います。(サブネットの設定は CLI から)

MAG 2600 のインターフェイスの設定は、下記の通りです。

**Network Settings**  
Internal Port - Settings

Overview | Internal Port | External Port | VLANs | Routes | Hosts | Network Connect

Settings | Virtual Ports | ARP Cache

Enter the network settings and click the Save Changes button at the bottom of the page.

**Port Information**

- \* IP Address: 192.168.1.110
- \* Netmask: 255.255.255.0
- \* Default Gateway: 192.168.1.254

Note: If you need to specify static routes, you can do so on the [Static Routes](#) page.

**Advanced Settings**

- MAC Address: 00:18:7D:23:71:A1
- Link Speed: Auto
- \* ARP Ping Timeout: 5 seconds
- \* MTU: 1500 bytes

#### 【Ethernet0】 Internal Port

IP:192.168.1.110 255.255.255.0

社内 LAN に接続。管理 interface としても使用。

**Network Settings**  
External Port - Settings

Overview | Internal Port | External Port | VLANs | Routes | Hosts | Network Connect

Settings | Virtual Ports | ARP Cache

Enter the network settings and click the Save Changes button at the bottom of the page.

**Use Port?**

Enabled  Disabled

**Port Information**

- \* IP Address: 192.168.3.110
- \* Netmask: 255.255.255.0
- \* Default Gateway: 192.168.3.254

Note: If you need to specify static routes, you can do so on the [Static Routes](#) page.

**Advanced Settings**

- MAC Address: 00:18:7D:23:71:A2
- Link Speed: Auto
- \* ARP Ping Timeout: 5 seconds
- \* MTU: 1500 bytes

#### 【Ethernet1】 External Port

IP:192.168.3.110 255.255.255.0

Junos Pulse による接続を受付ける interface。

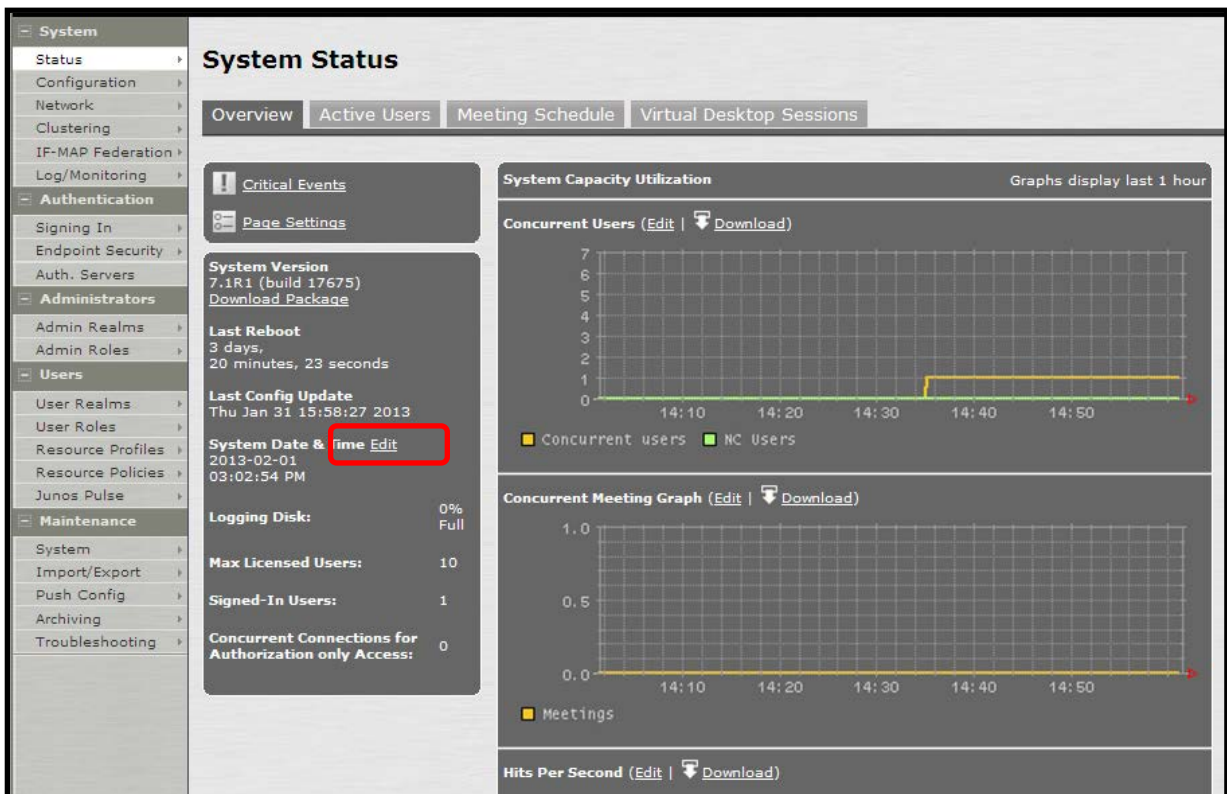


MAG 2600 のセットアップ方法は、  
MAG シリーズのクイックセットアップガイドをご参照下さい。

### 3-1-2システム時刻設定

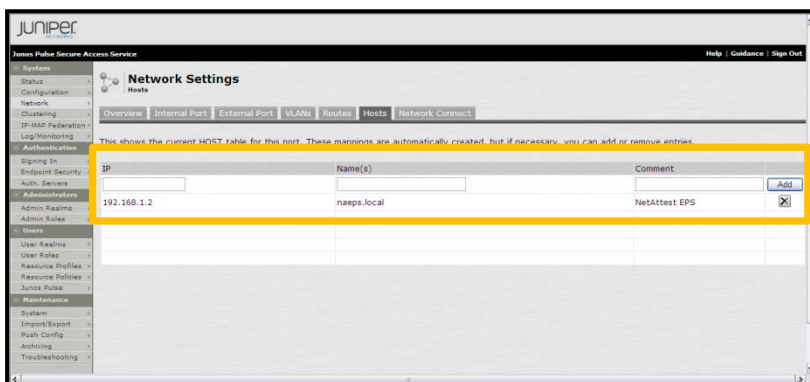
NetAttest EPS と同じ時刻を設定します。

「Status」 - 「System Date & Time」 - 「Edit」 から設定します。



### 3-1-3Hosts 設定(任意)

本検証環境には、DNS サーバーを設置していないため、NetAttest EPS の IP アドレスを Hosts に登録します。「Network」 - 「Hosts」 から設定します。



【IP】

・ 192.168.1.2

【Name】

・ naeps.local

## 3-2MAG 2600 の証明書に関する設定

### 3-2-1SSL に関する設定(参考) (MAG 2600)

SSL に関するセキュリティ設定を行います。

「Configuration」 - 「Security」 から設定します。

The screenshot shows the Juniper Pulse Secure Access Service Configuration page. The left sidebar contains a navigation menu with categories like System, Authentication, Administrators, Users, and Maintenance. The main content area is titled 'Configuration Security' and has tabs for Licensing, Security, Certificates, DMI Agent, NCP, Sensors, and Client T. The 'Security' tab is active, and the 'SSL Options' sub-tab is selected. The page contains several sections for SSL configuration:

- Allowed SSL and TLS Version:** The older SSL V2 protocol has known security issues addressed by SSL V3 and TLS V1. Three radio button options are available:
  - Accept only TLS V1 (maximize security with reduced compatibility)
  - Accept only SSL V3 and TLS V1 (maximize security) - This option is selected.
  - Accept SSL V2 and V3 and TLS V1 (maximize browser compatibility)
- Allowed Encryption Strength:** Strong ciphers (rated by the number of bits in the cipher) improve the security. More than one acceptable cipher, the Junos Pulse Secure Access Service will accept the strongest encryption strength. Changing the encryption strength will cause the web service to restart. Three radio button options are available:
  - Accept only 168-bit and greater (maximize security)
  - Accept only 128-bit and greater (security and browser compatibility) - This option is selected.
  - Accept 40-bit and greater (maximize browser compatibility)
  - Custom SSL Cipher Selection.
- SSL Handshake Timeout option:** By default, the SSL handshake has a timeout of 60 seconds. Use the text box to change the timeout. The current value is 60 seconds.
- SSL Legacy Renegotiation Support option:** When this option is enabled, renegotiation with clients and servers, which do not support renegotiation, will be allowed. When disabled, renegotiation with such clients and servers will not be allowed. The checkbox 'Enable support for SSL legacy renegotiation' is checked.
- Require client certificate on these ports:** Enforce client certificate requirement on ports used for access. Client certificates are required on the selected ports. There are two sections: 'External Virtual Ports' and 'Internal Virtual Ports', each with an 'Add ->' and 'Remove' button.

At the bottom of the page, there is a note: 'Note that changing any of the above settings might restart some services in the Junos Pulse Secure Access Service.' and a 'Save Changes' button.

#### 【Allowed SSL and TLS Version】

- Accept Only SSL V3 and TLS V1

#### 【Allowed Encryption Strength】

- Accept Only 128-bit and greater

#### 【SSL Legacy Renegotiation Support option】

- Enable support for SSL legacy renegotiation



### 3-2-2CSR の生成 (MAG 2600)

MAG 2600 で CSR(Certificate Signing Request)を生成します。

「Configuration」 - 「Certificates」 - 「Device Certificates」 の「New CSR」 より CSR を作成します。「Create CSR」 をクリックすると、以下の画面に遷移します。

**【Common Name】**

- soliton.co.jp

**【Organization Name】**

- Soliton Systems K.K.

**【Locality】**

- Tokyo-to

**【State】**

- Shinjyuku-ku

**【Country】**

- JP

**【Random Data】**

- password

証明書サブジェクトは必ず指定して下さい。  
NetAttest EPS では、デフォルトでは CN が必須です。

**次ページへ**

[Step1. Send CSR to Certificate Authority for signing]の  
文字列すべてをコピーし、テキストデータで保存します。

**JUNIPER**  
Junos Pulse Secure Access Service Help | Guidance

**System**

- Status
- Configuration
- Network
- Clustering
- IF-MAP Federation
- Log/Monitoring

**Authentication**

- Signing In
- Endpoint Security
- Auth. Servers

**Administrators**

- Admin Realms

**Users**

- User Realms
- User Roles
- Resource Profiles
- Resource Policies
- Junos Pulse

**Maintenance**

- System
- Import/Export
- Push Config
- Archiving
- Troubleshooting

**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.

**Pending Certificate Signing Request**

**CSR Details**

Common Name: soliton.co.jp

Org. Name: Soliton Systems K.K. Locality: Tokyo-to  
Org. Unit Name: State: Shinjyuku-ku  
Email Address: Country:JP  
Key Size: 1024 bits

[Back to Device Certificates](#)

**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 one of the following ways:

- Save the text as a .csr 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-----
MIIBrjCCARoCAQAwbjELMAkGA1UEBhMCS1AxFTATBgNVBAgTDFNoaW50eXVrdS1r
dTERMA8GA1UEBxMlVGV9reW8tdG8xHTAbBgNVBAoTFFFNbG10b24gU31zdGV0cyBL
LksuMRywFAVDVQQDEw1zb2xpdG9uLmNvLmNvLmNvLmNvLmNvLmNvLmNvLmNvLmNv
ADCBIQKBgQDRnU9ThqaLH4S2ZxvDufeLqEIwHAC1VnRgt4I0EMD8n1St0DgxEyxR
```

**mag2600csr.txt**  
テキストドキュメント  
1 KB

**Step 2. Import signed certificate**

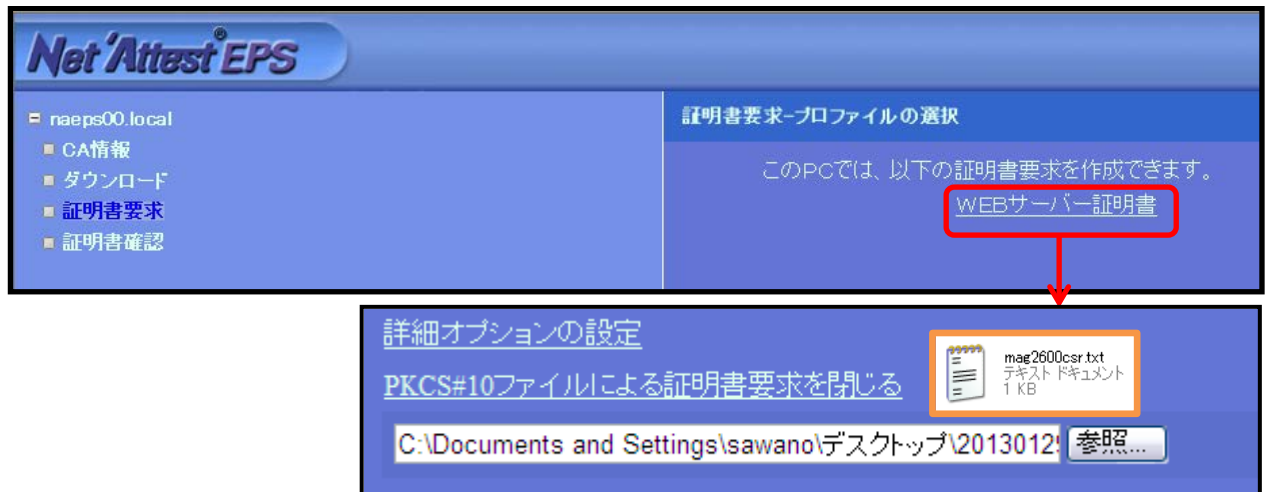
When you receive the signed certificate file from the CA, select it below and click Import. This will add the signed certificate and remove this pending C

Signed certificate:  [参照...](#)



### 3-2-3サーバー証明書署名要求 (NetAttest EPS)

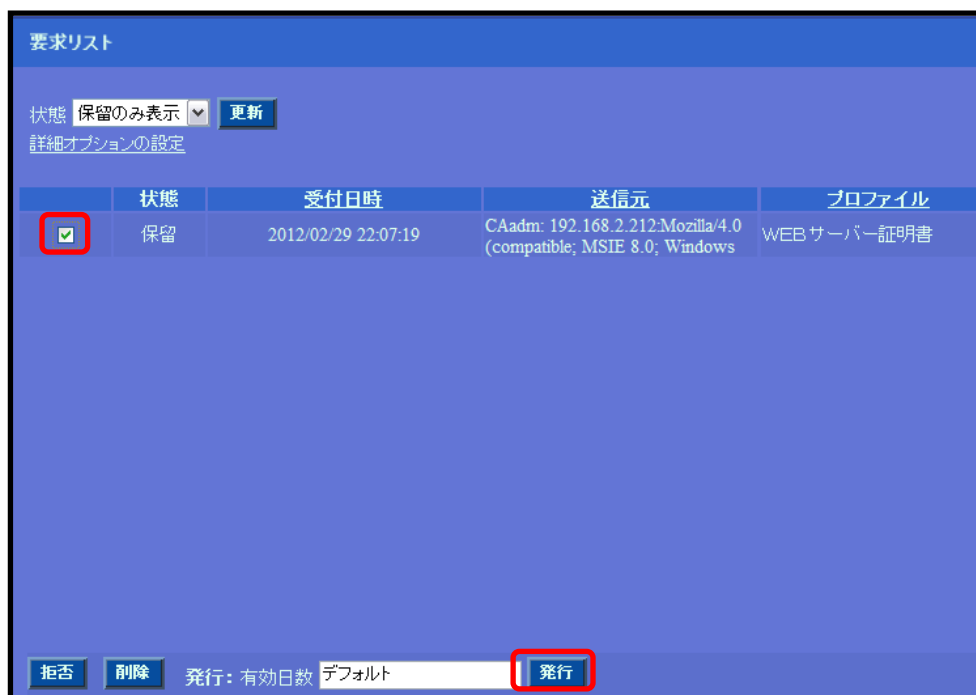
MAG 2600 で生成した CSR を基に NetAttest EPS で MAG 2600 のサーバー証明書を発行します。  
 NetAttest EPS の管理者向け証明書サービスページ( (デフォルト) <http://192.168.2.1/certsrv/>)  
 にアクセスし、証明書要求を行います。下記の手順で CSR をインポートします。



### 3-2-4サーバー証明書の発行 (NetAttest EPS)

サーバー証明書要求の承認・発行を行います。

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(発行)します。



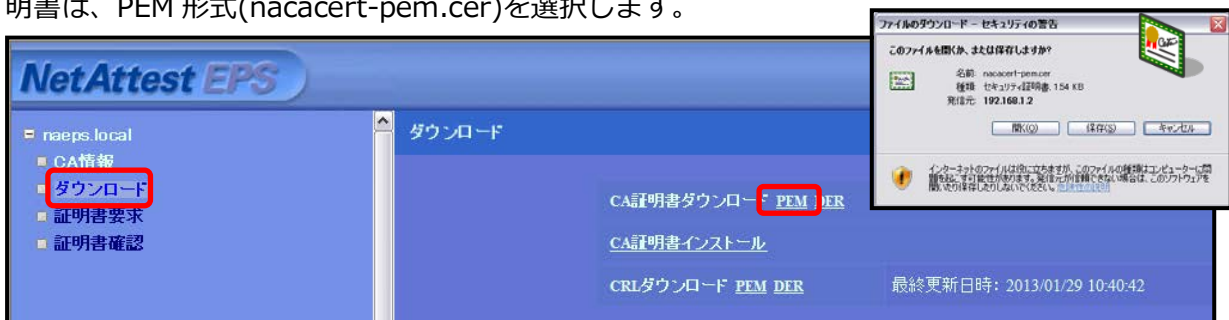
### 3-2-5サーバー証明書のダウンロード (NetAttest EPS)

サーバー証明書をダウンロードするために再度、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。



### 3-2-6CA 証明書の取得 (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。



### 3-2-7サーバー証明書のインポート (MAG 2600)

NetAttest EPS で発行したサーバー証明書をインポートします。

CSR を作成したページの [Step2. Import signed certificate] で、サーバー証明書 (nausercert-pem.cer)をインポートします。

The screenshot shows the Juniper Pulse Secure Access Service configuration interface. A notification at the top states "CSR created successfully". Below this, the "Pending Certificate Signing Request" section is visible, containing "CSR Details" and two steps for handling the CSR.

**CSR Details**

- Common Name: soliton.co.jp
- Org. Name: Soliton Systems K.K. Locality: Tokyo-to
- Org. Unit Name: State: Shinjyuku-ku
- Email Address: Country:JP
- Key Size: 1024 bits

**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 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-----
MIIBrjCCARoCAQAwbjELMAkGA1UEBhMCSlAxFTATBgNVBAgTDGFNoaW5qeXVrdS1r
dTERMA8GA1UEBxMIIVG9reW8tdG8xHTAbBgNVBAoTFFNvbG10b24gU31zdG9vcyBL
LksuMRYwFAYDVQQDEw1zb2xpdG9uLmNvLmNvbWlma0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQDRnU9ThqaLH4S2ZxvDufeLqEiWHACiVnRgt4IOEMD8n1St0DgxEyxA
```

**Step 2. Import signed certificate**

When you receive the signed certificate from the CA, select it below and click Import. This will add the signed certificate and remove this pending C

Signed certificate:

<input type="checkbox"/>	soliton.co.jp	TestCA	Jan 29 07:36:38 2013 GMT to Jan 29 07:41:38 2014 GMT

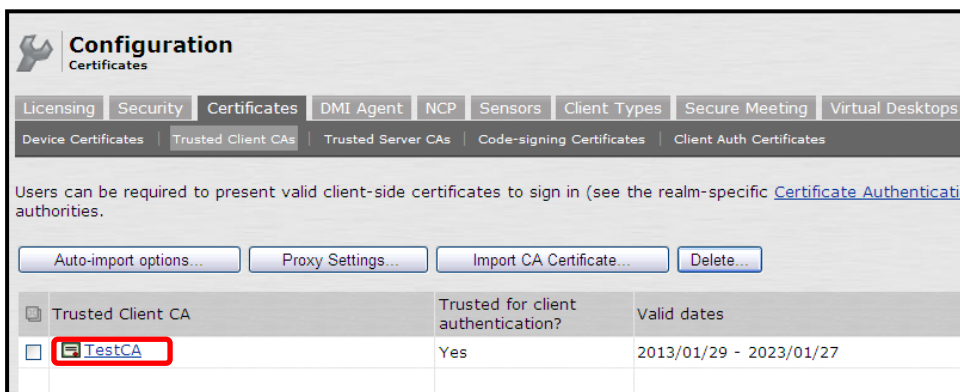
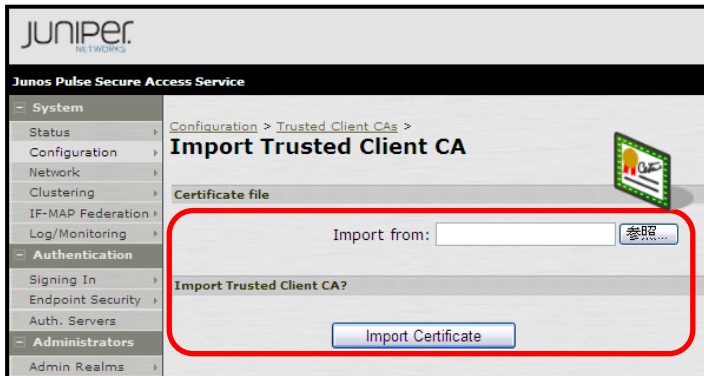
インポート結果

### 3-2-8CA 証明書のインポート (MAG 2600)

NetAttest EPS からダウンロードした CA 証明書を MAG 2600 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。

続いて、インポートされた CA 証明書をクリックし、CRL の設定を行います。



次ページへ

「Client certificate status checking」のいくつかの項目にチェックを入れ、次に、「CRL Checking Options」をクリックします。

**Trusted Client CA**

**Certificate**

Issued To: ▶ TestCA  
 Issued By: ▶ TestCA  
 Valid Dates: Jan 29 01:40:41 2013 GMT - Jan 27 01:45:41 2023 GMT  
 Details: ▶ Other Certificate Details

[Renew Certificate ...](#)

**Client certificate status checking**

- None
- Use OCSP (Online Certification Status Protocol)
- Use CRLs (Certificate Revocation Lists)
- Use OCSP with CRL fallback
- Inherit from root CA

Trusted for Client Authentication  
 Uncheck here to exclude the CA from being trusted for client certificate authentication, if this CA was added for other trusting purpose such as SAML signature verification or machine certificate validation.

Participate in Client Certificate Negotiation  
 Indicating whether this CA will be sent to the browser for client certificate selection. To stop a client certificate being prompted by the browser, this flag of all the upper level CA chain of the certificate should be deselected.

**Advanced Certificate Processing Settings**

**Note: Enabling the certificate policy settings below will cause path validation to comply strictly with RFC 5280. This may cause some previously accepted certificate paths to be rejected.**

Initial Inhibit Policy Mapping  
Policy mapping for certificate paths to inhibit

Initial Require Explicit Policy  
Path must be valid for at least one of the certificate policies in the Initial Policy Set below

Initial Policy Set:  A set of certificate policy identifiers naming the policies that are acceptable to the certificate user.  
 One policy per line, e.g.  
 1.3.6.1.4.1  
 2.16.840.1.101.3.2.1  
 Empty value indicates any policy

[Save Changes](#)

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

[CRL Checking Options ...](#) [Update Now](#) [Enable](#) [Disable](#)

CRL distribution points	Status	Last Updated	Next Update
<input type="checkbox"/> <a href="http://naeps.local/certs/certs.crl">http://naeps.local/certs/certs.crl</a> <small>Last result: Success, new CRL</small>	Enabled; OK: 1KB, 0 revocations	2013/01/29 15:58:27 <a href="#">[Save CRL...]</a>	2013/02/28 10:45:42

↓ 次ページへ

「CRL Distribution Points(CDP)」で「Manually configured CDP」を選択し、「CDP URL」にCRLの保存場所 URL を記載します。

CDP URL は EPS からダウンロードした CA 証明書でも確認できます。

3-1-3 で設定した Hosts により名前解決しているため今回は FQDN で指定しております。名前解決出来ない環境では IP アドレスで指定して下さい。



## 3-3MAG 2600 の VPN 接続に関する設定

### 3-3-1RADIUS/Certificate Server の設定

「Auth. Servers」の「New Server」より「RADIUS」を追加します。

**Settings** Users

\* Name: EPSTEST

NAS-Identifier: JuniperMAG

**Primary Server**

\* Radius Server: 192.168.1.2

\* Authentication Port: 1812

\* Shared Secret: \*\*\*\*\*

\* Accounting Port: 1813

NAS-IP-Address: 192.168.1.110

\* Timeout: 30 seconds

\* Retries: 0

Users authenticate using tokens or one-time passwords

**Backup Server (required only if Backup server exists)**

Radius Server: [ ] Name or IP address

Authentication Port: [ ]

Shared Secret: [ ]

Accounting Port: [ ] Port used for Radius accounting, if applicable

**Radius accounting**

User-Name: <USER>[<REALM>][<ROLE SEP=

- 【Name】**
- EPSTEST**
- 【NAS-Identifier】**
- Juniper MAG**
- 【Radius Server】**
- 192.168.1.2**
- 【Authentication Port】**
- 1812**
- 【Shared Secret】**
- secret**
- 【Accounting Port】**
- 1813**
- 【NAS-IP-Address】**
- 192.168.1.110**

次に「Auth. Servers」の「New Server」より「Certificate Server」を追加します。

**Settings** Users

\* Name: naeps.local

User Name Template: <certDN CN>

Examples:

- <certDN.CN> First CN from the subject DN
- <certAttr.serialNumber> Certificate serial number
- <certAttr.altName.xxx> Where xxx can be:
  - Email The Email alternate name
  - UPN The Principal Name alternate name
  - ... etc
- <certDNText> The complete subject DN
- cert-<certDN.CN> The text "cert-" followed by the first CN from the subject

Enable User Record Synchronization

Logical Auth Server Name: [ ]

Save Changes?

- 【Name】**
- naeps.local**

### 3-3-2VPN Roles の設定

「User Roles」 - 「New User Role」よりユーザーに割り当てるロールの設定を行います。ここでは、許可する VPN 接続方法等を指定します。

The screenshot shows the configuration page for a user role named 'VPNRoles'. The 'Access features' section is highlighted with a yellow border. The following table summarizes the checked and unchecked features:

Feature	Status
Web	Checked
Files, Windows	Unchecked
Files, UNIX/NFS	Unchecked
Secure Application Manager	Unchecked
Telnet/SSH	Unchecked
Terminal Services	Unchecked
Virtual Desktops	Unchecked
Meetings	Unchecked
Network Connect	Checked
IKEv2	Unchecked

**【Name】**

- VPNRoles

**【Options】**

- Session Options

- UI Options

**【Access features】**

- Web

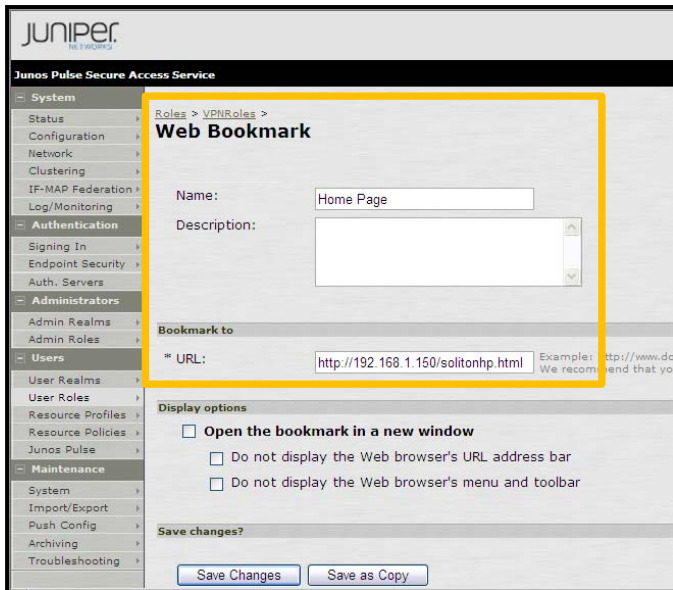
- Network Connect (Junos Pulse)

次ページへ



次に、画面上タブの「Web」より「New Bookmark」を選択し、以下を設定します。

※本設定は任意です。本設定をすることで、ログイン後、登録した BookMark が表示されます。



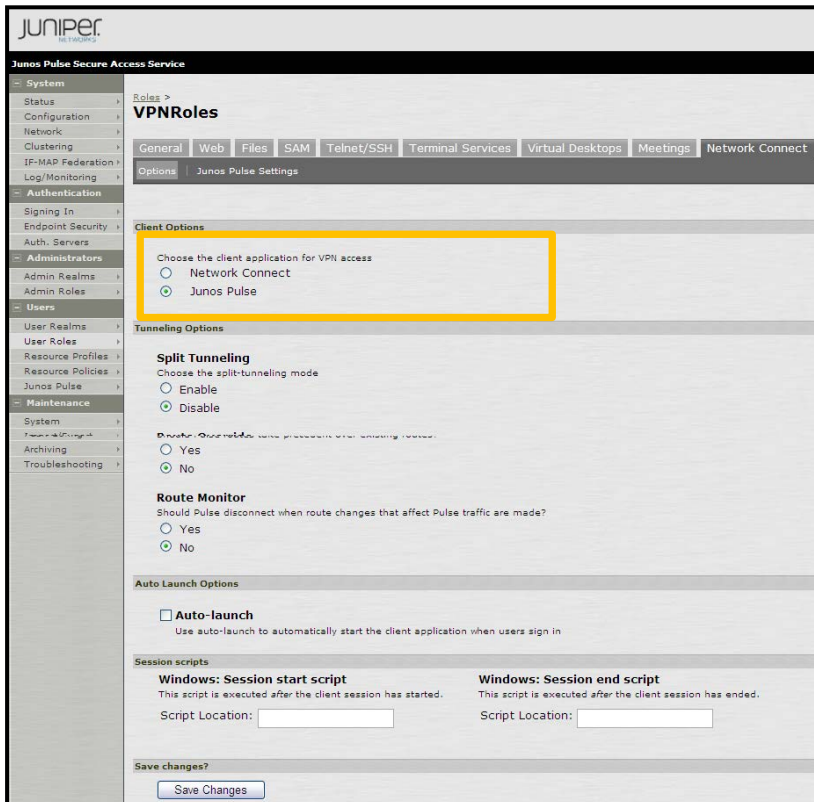
**【Name】**

• Home Page

**【URL】**

• <http://192.168.1.150/solitonhp.html>

続いて、画面上タブの「Network Connect」 - 「Options」より以下を設定します。

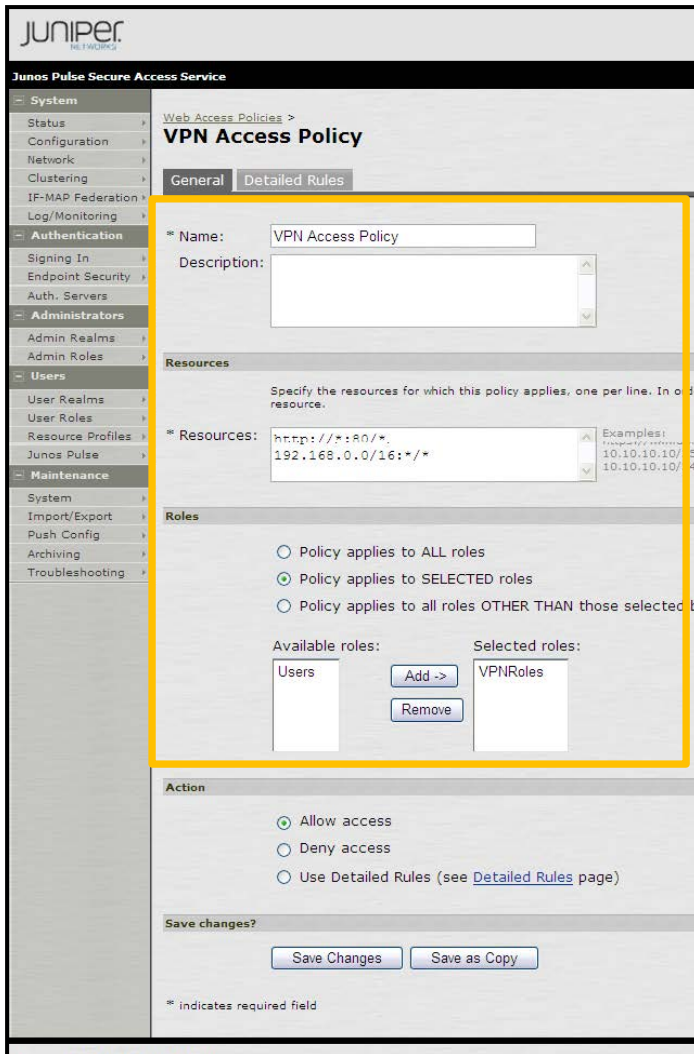


**【Client Options】**

• Junos Pulse

### 3-3-3VPN Access Policy の設定

「Resource Policies」 - 「Web」の「New Policy」でアクセスポリシーの設定を行います。「Roles」で作成した Role(VPNRoles)を選択し、選択したロールとポリシーの紐付けを行います。「Resources」で定義した接続に対して、VPNRoles が適用されます。



#### 【Name】

- VPN Access Policy

#### 【Resources】

- http://\*:80/\*
- 192.168.0.0/16:\*/\*

#### 【Roles】

- Policy applies to SELECTED roles

#### 【Selected roles】

- VPNRoles

### 3-3-4 Authentication Realms の設定

「User Realms」 - 「New User Realms」 でレルムの設定を行います。

「Authentication」に Certificate Server(naeps.local)を指定、「Additional authentication server」には RADIUS(EPSTEST)を指定します。

本設定をすることで、証明書認証 + ID/Password 認証が可能になります。

**【Name】**

• VPNRealms

**【Authentication】**

• naeps.local

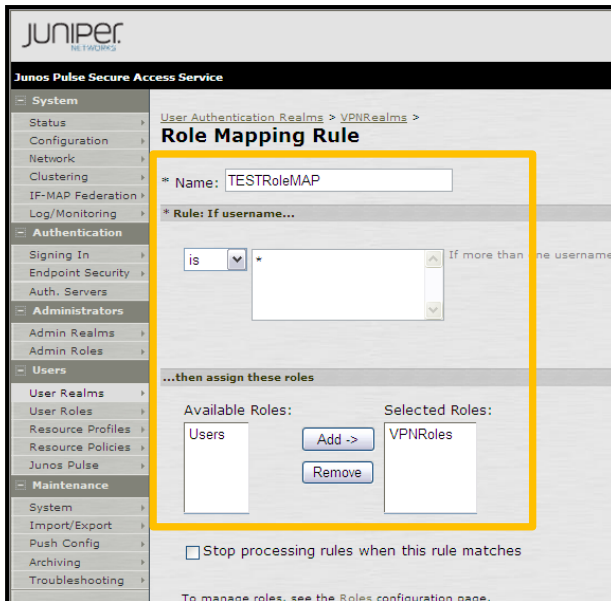
**【Additional authentication server】**

• EPSTEST

**次ページへ**

次に、画面上タブの「Role Mapping」よりユーザーとロールの紐付け設定を行います。

「...then assign roles」では VPNRoles を指定します。



**[Name]**

• TESTRoleMAP

**[Role if username...]**

• is:\*

**[...then assign these roles]**

• VPNRoles

### 3-3-5 Sign-In Policy の設定

「Sign In」 - 「Sign-in Policies」の「New URL」からサインインポリシーの設定を行います。ここでの設定がVPNクライアント(Junos Pulse クライアント)で接続する際の接続先 URL になります。「Authentication realm」では、VPNRealms を指定します。

**[User Type]**

• Users

**[Sign-in URL]**

• \* /vpntest/

**[Authentication realm]**

• User picks a list authentication realms

**[Selected realms]**

• VPNRealms

### 3-3-6IP プールの設定

「Resource Policies」 - 「Network Connect Connection Profiles」 で、VPN クライアントに払い出す IP アドレス(IP プール)等のネットワーク設定を行います。

The screenshot shows the configuration page for a Network Connect Connection Profile named 'VPN-TEST'. The page is divided into several sections:

- Name:** VPN-TEST
- Description:** (Empty field)
- IP address assignment:**
  - DHCP servers:** (Empty field)
  - DHCP options:** (Empty table)
  - IP address pool:** 192.168.1.200-192.168.1.210
- Connection Settings:**
  - Transport:** ESP (maximize performance)
  - UDP port:** 4500
  - ESP to SSL fallback timeout:** 15 seconds
  - Key lifetime (time based):** 20 minutes
  - Key lifetime (bytes transferred):** 3 bytes (0 implies no limits)
  - Replay Protection:** (Checked)
  - Compression:** (Unchecked)
  - Encryption:** AES128/SHA1 (Selected), AES256/MDS, AES256/SHA1 (maximize security)
- DNS Settings:**
  - Manual DNS Settings:**
    - Primary DNS:** 192.168.1.102 (IP address)
    - Secondary DNS:** (Empty field)
    - DNS Domain(s):** (Empty field)
    - WINS:** (Empty field)
  - DHCP DNS Settings:** (Only applicable if DHCP Server is chosen)
- Auto-allow IP's in DNS/WINS settings:** (Unchecked)
- DNS search order:** Search client DNS first, then the device (Selected)
- Proxy Server Settings:**
  - No proxy server:** (Selected)
  - Automatic:** (URL for PAC file on another server)
  - Manual configuration:** (Server: , Port: 0)
  - Preserve client-side proxy settings:** (Selected)
- Roles:**
  - Policy applies to:** ALL roles (Selected)
  - Available roles:** Users, VPNRoles

- [Name]
- VPN-TEST
- [IP address Pool]
- 192.168.1.200-192.168.1.210
- [DNS Settings]
- Manual DNS Settings 192.168.1.102
- [Selected Roles]
- VPNRoles

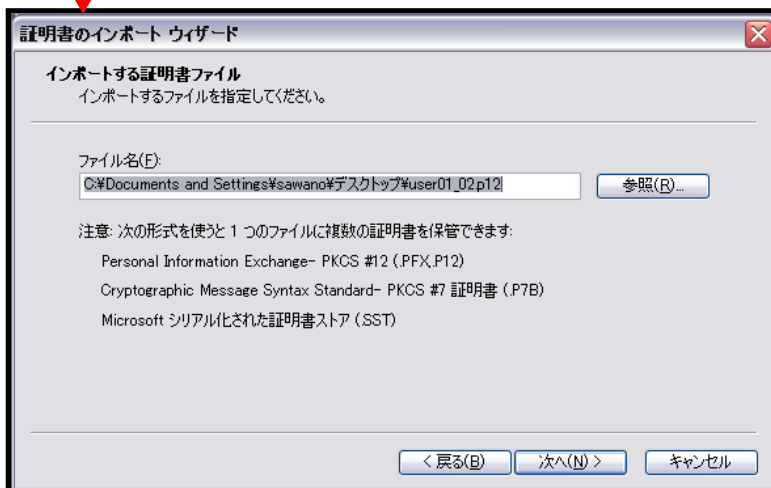
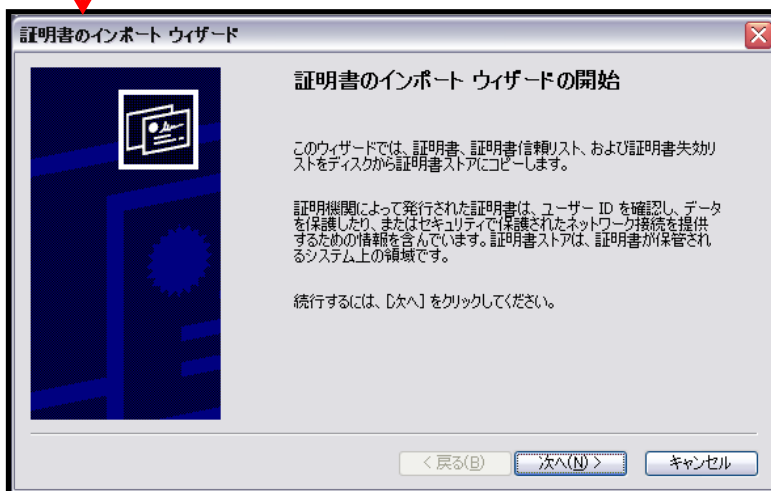
## 4. 各種 VPN クライアントの設定

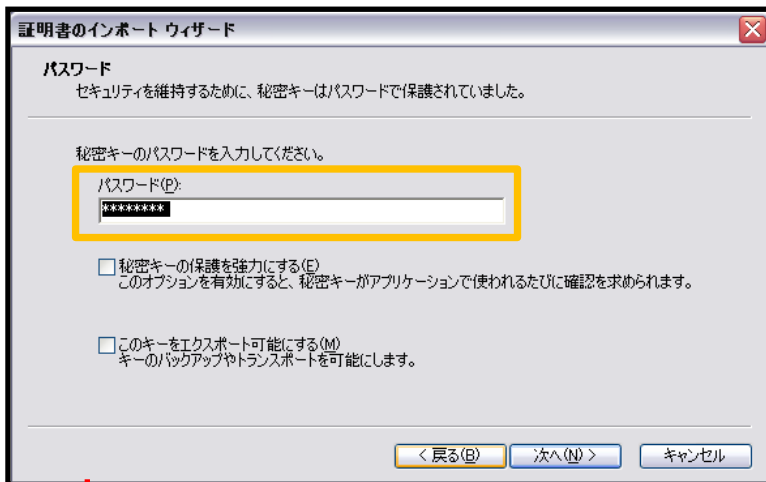
### 4-1 Windows 版 Junos Pulse

#### 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。

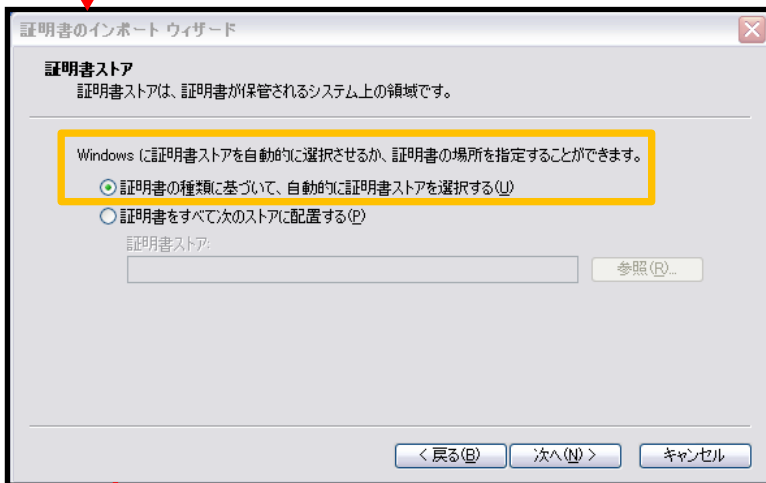




【パスワード】

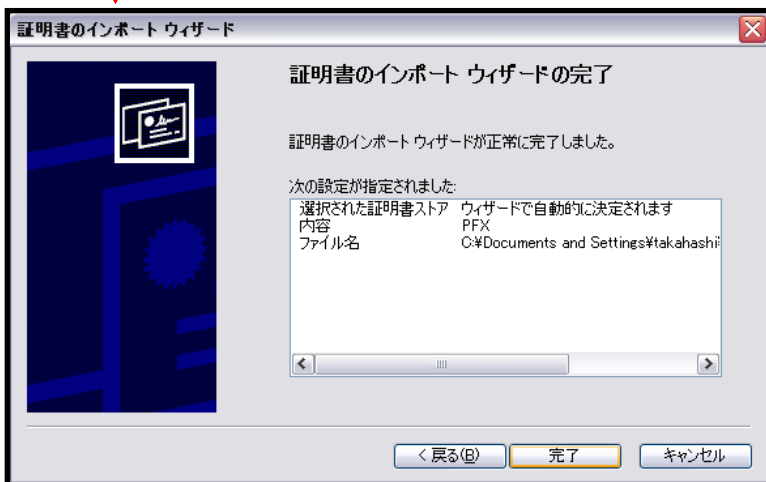
NetAttest EPS で証明書を  
発行した際に設定したパスワードを入力

 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。



【証明書の種類に基づいて・・・】

・チェック有





## 4-1-2VPN クライアント(Junos Pulse)の接続設定

Junos PulseクライアントをJuniper Network社のサイトもしくはMAG 2600からダウンロードし、インストールします。MAG 2600 からダウンロードする場合は、本環境では <https://192.168.3.110/> にアクセスします。Junos Pulseクライアントの設定は下記のとおりです。



【名前】

・ Junos Pulse

【サーバーURL】

・ <https://192.168.3.110/vptest/>

## 4-2iOS 版 Junos Pulse

---

### 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 3つ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)

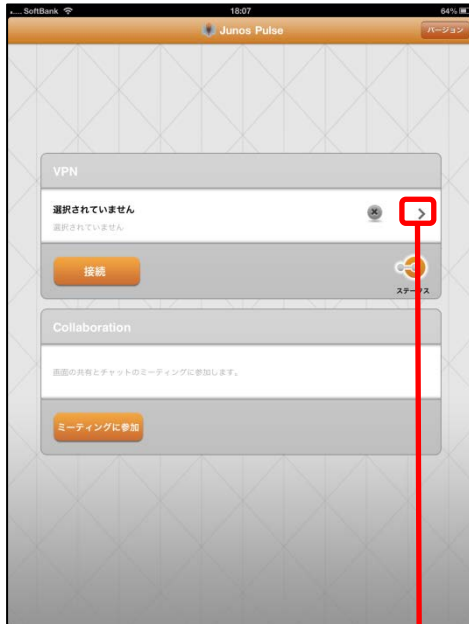
上記いずれかの方法で CA 証明書とクライアント証明書をインストールします。

※本書では割愛させていただきます。

## 4-2-2VPN クライアント(Junos Pulse)の接続設定

Junos Pulse クライアントを Apple App Store からインストールします。

インストール後 Junos Pulse を起動し、下記のように設定します。



### 【名前】

- JuniperMAG

### 【URL】

- <https://192.168.3.110/vpntest/>

### 【証明書】

- インストールした証明書を選択

## 4-3接続テスト

### 4-3-1 Windows 版 Junos Pulse を利用した VPN 接続(トンネリングモード)

Junos Pulse クライアントを利用し、VPN 接続を行います。

なお、ブラウザを利用し、接続することも可能です。



【ユーザー名】

・ user01

【パスワード】

・ password



### 4-3-2iOS 版 Junos Pulse を利用した VPN 接続

Junos Pulse クライアントを利用し、VPN 接続を行います。



- 【ユーザー名】
- ・ user01
- 【パスワード】
- ・ password



