

NetAttest EPS 設定例

連携機器：

Cisco ASA 5510

Case：AnyConnect を利用した、
証明書とパスワードによるハイブリッド認証

Version 1.0

株式会社ソリトンシステムズ

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。

Copyright © 2013, Soliton Systems K.K. , All rights reserved.

はじめに

本書について

本書は、NetAttest EPS と Cisco Systems 社製 Cisco ASA 5510 との証明書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
ABCDabcd1234 (normal)	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例を示します。
ABCDabcd1234 (bold)	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して示します。
<i>ABCDabcd1234</i> (italic)	変数を示します。実際に使用する特定の名前または値で置き換えます。

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 ASA 5510 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。

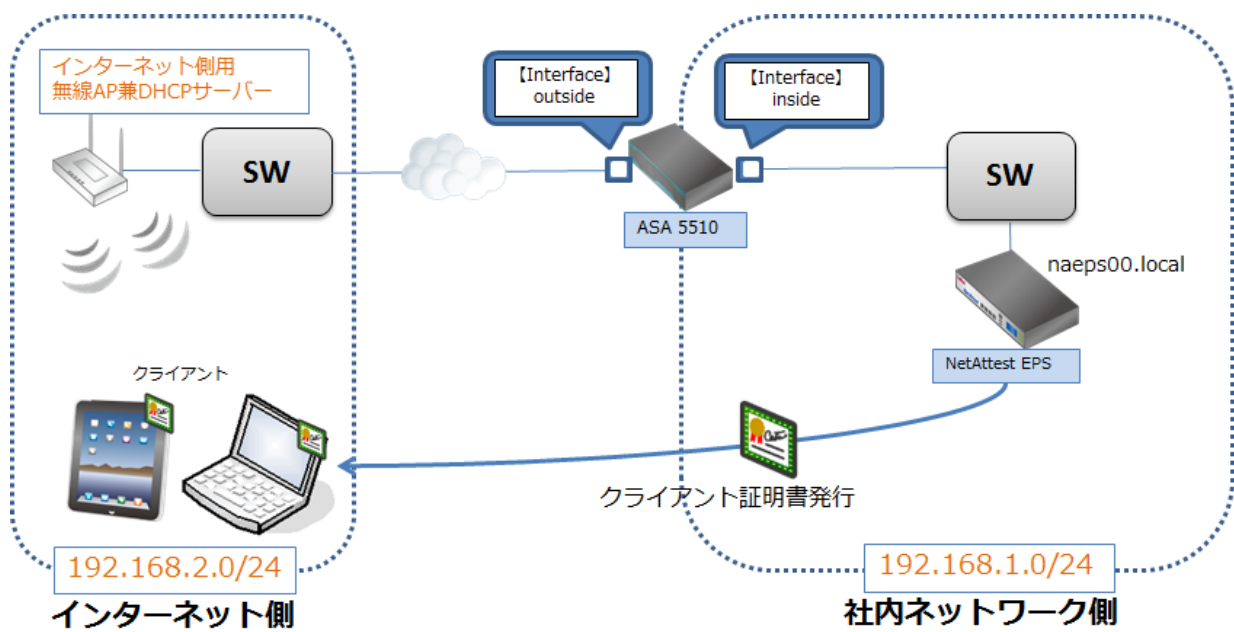
目次

1	構成	7
1-1	構成図	7
1-2	環境	8
2	NetAttest EPS の設定	9
2-1	システム初期設定ウィザードの実行	10
2-2	サービス初期設定ウィザードの実行	11
2-3	認証ユーザーの追加登録	12
2-4	クライアント証明書の発行	13
3	ASA 5510 の設定準備	14
3-1	インターフェイスの設定	15
3-2	システム時刻の設定	17
4	ASA 5510 の PKI 関連の設定	18
4-1	CSR の生成 (ASA 5510)	19
4-2	サーバー証明書署名要求 (NetAttest EPS)	22
4-3	サーバー証明書の発行 (NetAttest EPS)	23
4-4	サーバー証明書のダウンロード (NetAttest EPS)	24
4-5	CA 証明書の取得 (NetAttest EPS)	25
4-6	CA 証明書のインポート (ASA 5510)	26
4-7	サーバー証明書のインポート (ASA 5510)	28
5	ASA 5510 の接続設定	29
5-1	IP アドレスプールの設定	30
5-2	AAA サーバー(RADIUS サーバー)の設定	31
5-3	AnyConnect VPN Connection Setup Wizard	33
6	Windows 版 AnyConnect の設定	38
6-1	PC へのデジタル証明書のインストール	39
6-2	Windows 版 AnyConnect の設定	41
7	iOS 版 AnyConnect の設定	42
7-1	iPad へのデジタル証明書のインストール	43
7-2	iOS 版 AnyConnect の設定	44

8 接続の確認.....	45
8-1 PC における AnyConnect を利用した SSL-VPN 接続	45
8-2 iPad における AnyConnect を利用した SSL-VPN 接続	46

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	SWバージョン
Authentication Server (認証サーバー)	Soliton Systems	NetAttest EPS-ST03	Ver. 4.4.0
RADIUS クライアント (SSL VPN 機器)	Cisco Systems	ASA 5510	Ver.8.4(1)
Client PC	Lenovo	ThinkPad X200	Windows XP SP3
Client Tablet	Apple	iPad	iOS 5
無線 AP	BUFFALO	WAPM-APG300N	-

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-ST03	ASA 5510	Client PC	Client Tablet	無線 AP
IP アドレス	192.168.1.2/24	192.168.1.1/24	DHCP (無線 AP から)	DHCP (無線 AP から)	192.168.2.110/24
RADIUS port (Authentication)	TCP 1812		-	-	-
RADIUS port (Accounting)	TCP 1813		-	-	-
RADIUS Secret (Key)	secret		-	-	-

2 NetAttest EPS の設定

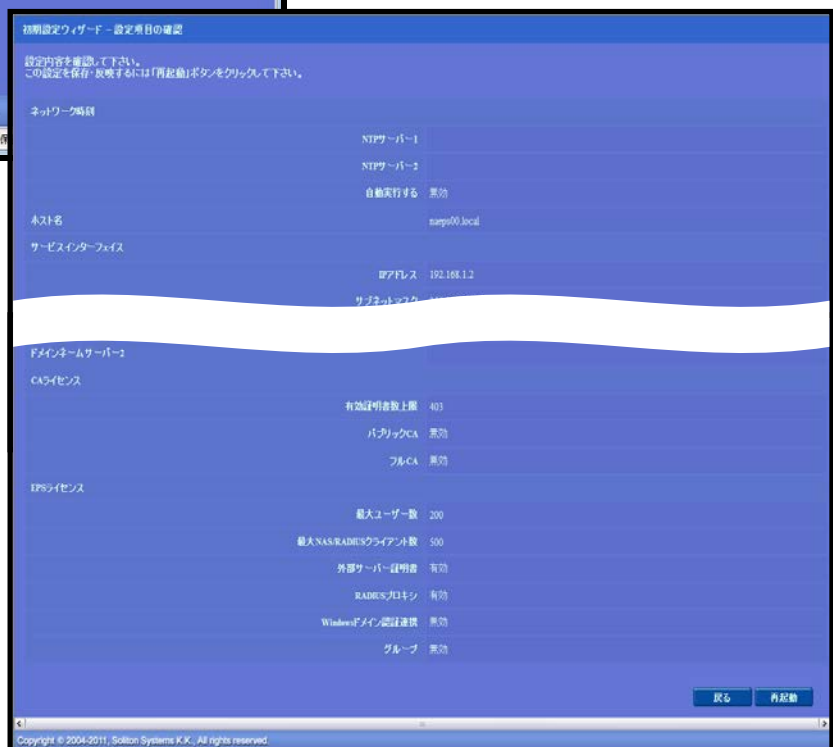
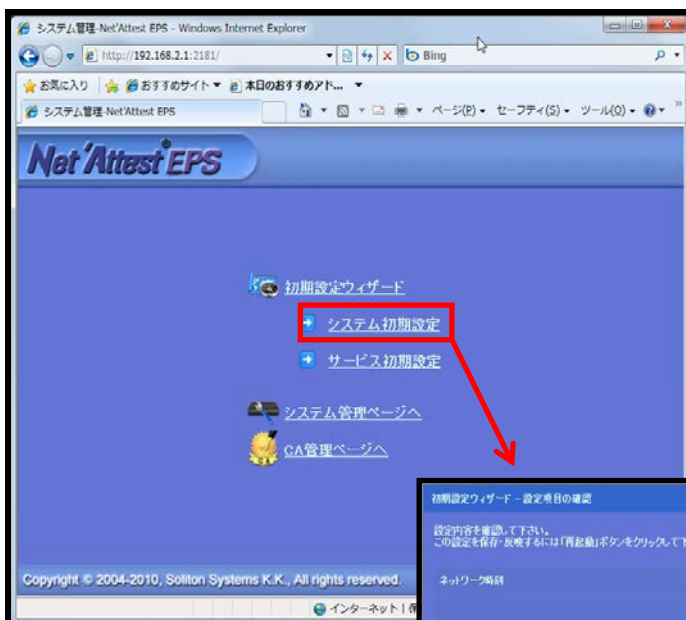
NetAttest EPS 設定の手順

1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. 認証ユーザーの追加登録
4. クライアント証明書の発行

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】

- ・ naeps00.local

【IP アドレス】

- ・ デフォルト

【ライセンス】

- ・ なし

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

【CA 種別選択】

・ ルート CA

【公開鍵方式】

・ R S A

【鍵長】

・ 2048

【CA 名】

・ naca00

【NAS/RADIUS クライアント名】

・ CiscoASA

【IP アドレス(Authenticator)】

・ 192.168.1.1

【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、ユーザー登録を行います。

「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】

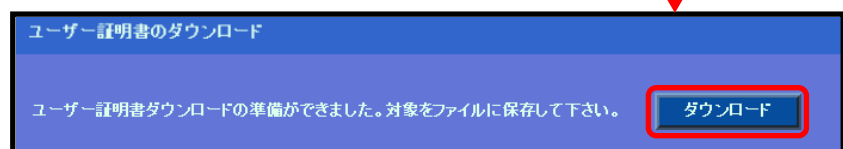
- ・ 365

【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 ASA 5510 の設定準備

ASDM のセットアップと ASA 5510 の基本設定

1. インターフェイスの設定
2. システム時刻の設定

3-1 インターフェイスの設定

ASA 5510 の設定は ASDM(Adaptive Security Device Manager)で行います。

本環境では、ASDM ver.6.4(1)を使用しています。

ASA 5510 のインターフェイスの設定は、下記の通りです。

Name	Switch Ports	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Restrict Traffic flow	VLAN	Management Only
inside	Ethernet0/0, Ethernet0/2, Et.	Yes	100	192.168.1.1	255.255.255.0	No	vlan1	No
outside	Ethernet0/1	Yes	100	192.168.2.2	255.255.255.0	No	vlan2	No

【Ethernet0/0】 inside

IP:192.168.1.1 255.255.255.0 . . . 社内 LAN に接続。管理 interface としても使用。

【Ethernet0/1】 outside

IP:192.168.2.2 255.255.255.0 . . . AnyConnect による接続を受け付ける interface。



ASA 5510 のセットアップ方法は、

ASA 5500 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。

また、 [Enable traffic between two or more interfaces which are configured with same security levels]を有効にします。

The screenshot shows the Soliton configuration interface. The main window displays the 'Configuration > Device Setup > Interfaces' page. A table lists the configured interfaces:

Name	Switch Ports	Enabled	Security Level	IP Address	Subnet Mask Prefix Length
inside	Ethernet0/0, Ethernet0/2, Et...	Yes	100	192.168.1.1	255.255.255.0
outside	Ethernet0/1	Yes	100	192.168.2.2	255.255.255.0

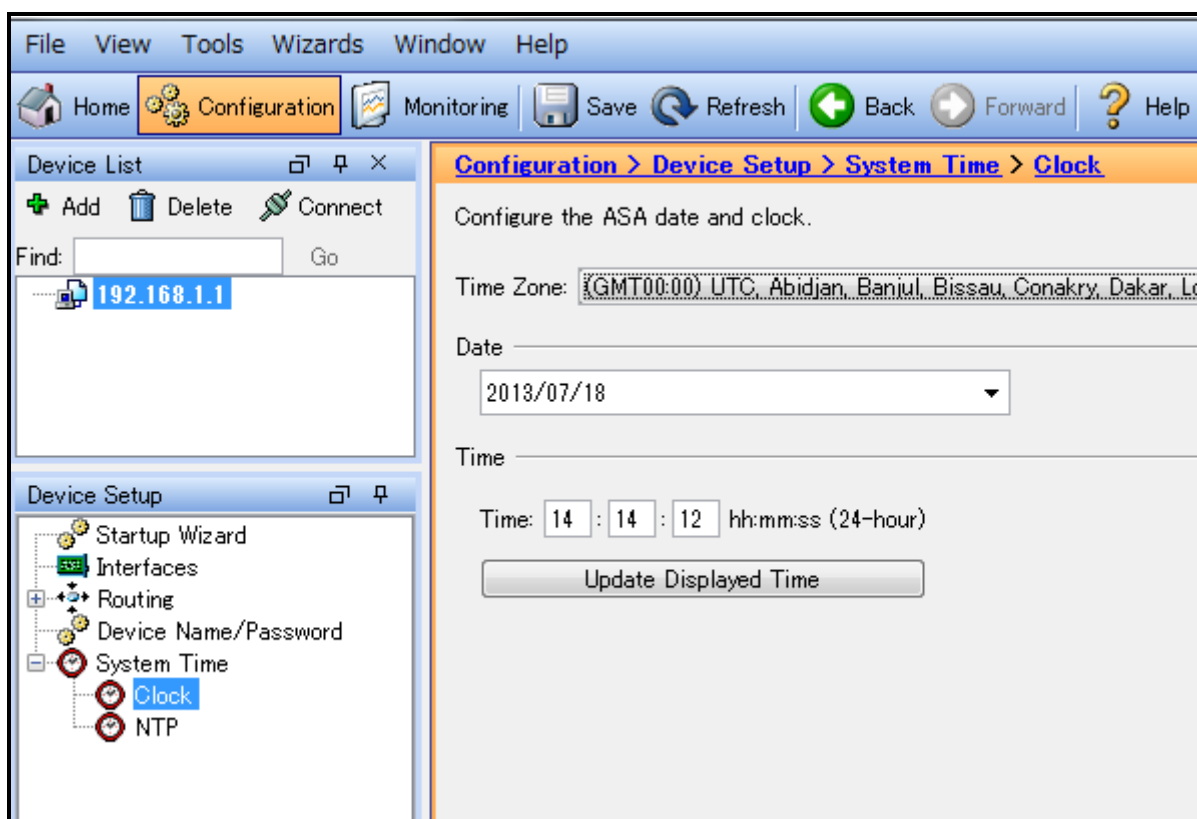
At the bottom of the interface, there are two checkboxes for enabling traffic:

- Enable traffic between two or more interfaces which are configured with same security levels
- Enable traffic between two or more hosts connected to the same interface

3-2 システム時刻の設定

NetAttest EPS と同じ時刻を設定します。

「Configuration」 - 「Device Setup」 - 「System Time」 - 「Clock」 から設定します。



【Time Zone】

- Tokyo

4 ASA 5510 の PKI 関連の設定

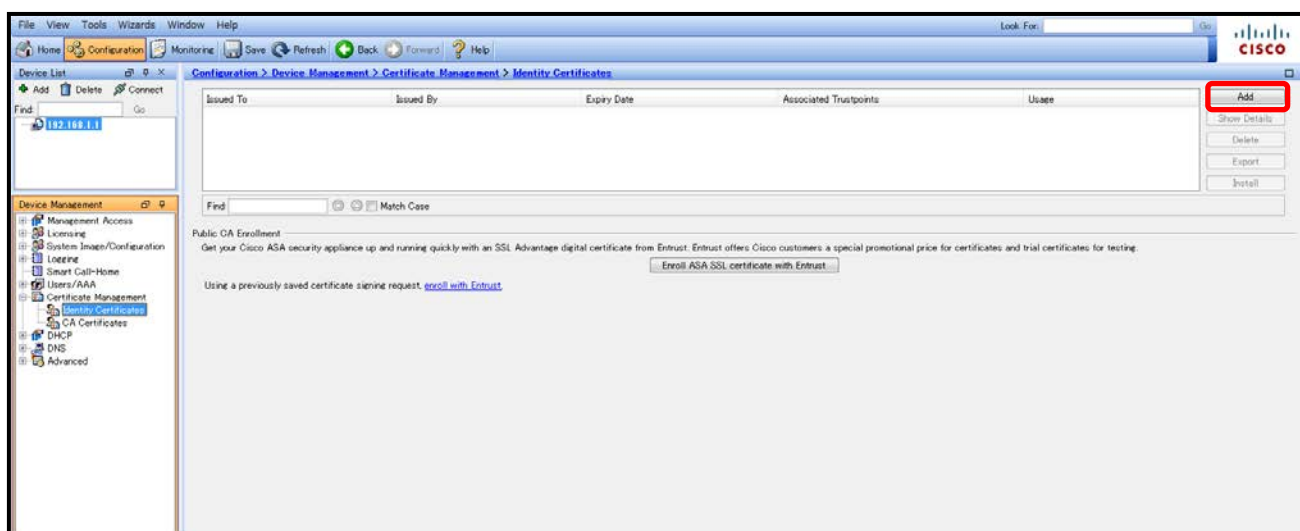
証明書の取得とインポートの手順

1. CSR の生成 (ASA 5510)
2. サーバー証明書署名要求 (NetAttest EPS)
3. サーバー証明書の発行 (NetAttest EPS)
4. サーバー証明書のダウンロード (NetAttest EPS)
5. CA 証明書の取得 (NetAttest EPS)
6. CA 証明書のインポート (ASA 5510)
7. サーバー証明書のインポート (ASA 5510)

4-1 CSR の生成 (ASA 5510)

ASA 5510 で CSR(Certificate Signing Request)を生成します。

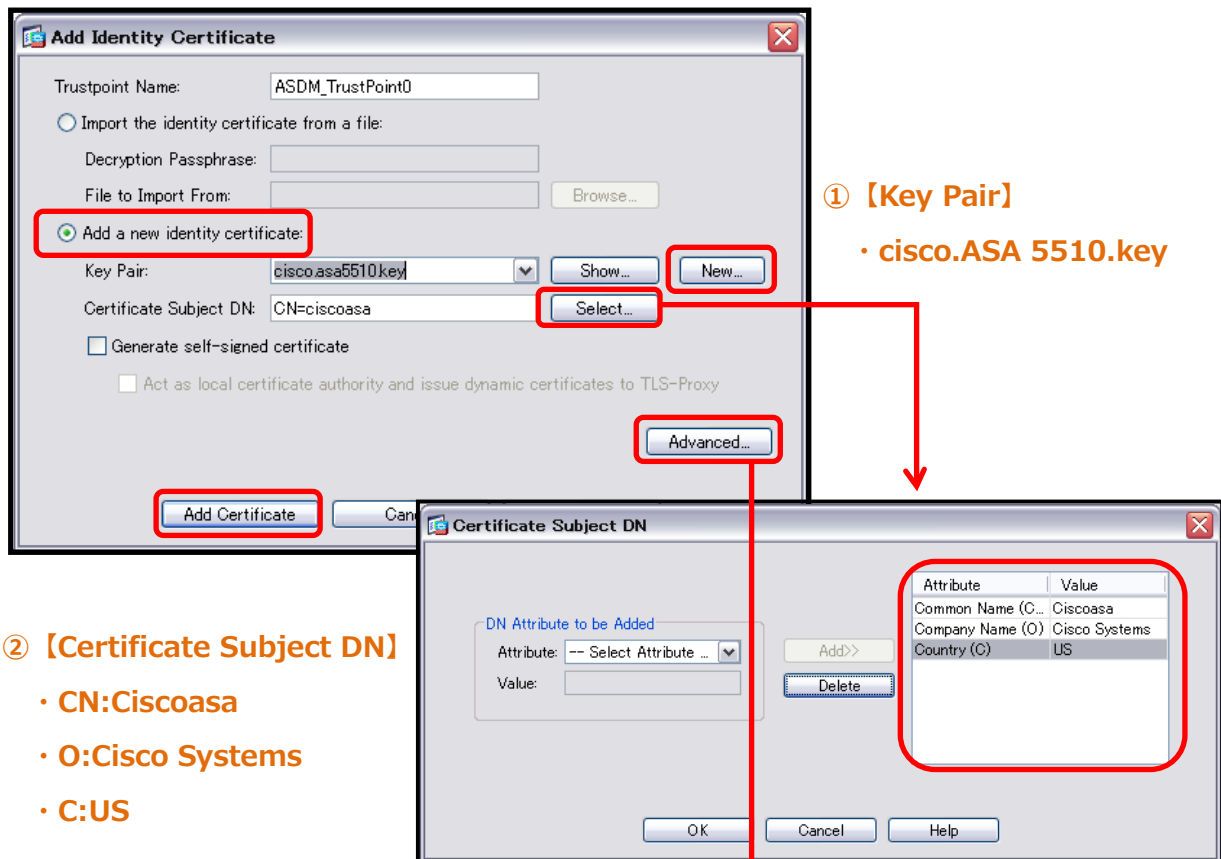
「Configuration」 - 「Device Management」 - 「Certificate Management」 - 「Identity Certificates」 の画面で『Add』 ボタンを選択します。



↓ 次ページへ

[Add Identity Certificate]画面で「Add a new identity certificate」を選択します。

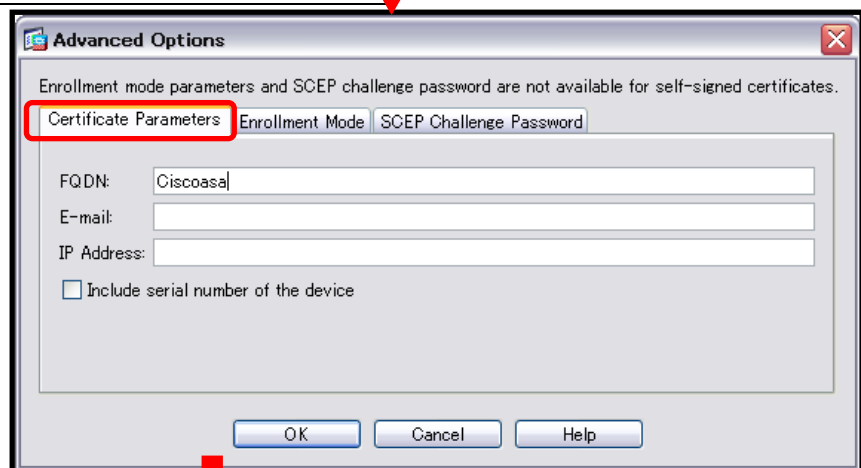
- ① [Key Pair]の『New』ボタンをクリックし新しいKey Pair名を作成した後、
- ② [Certificate Subject DN]を設定します。
- ③ 『Advanced』ボタンをクリックし、証明書のパラメータを設定します。



証明書サブジェクトは必ず指定して下さい。

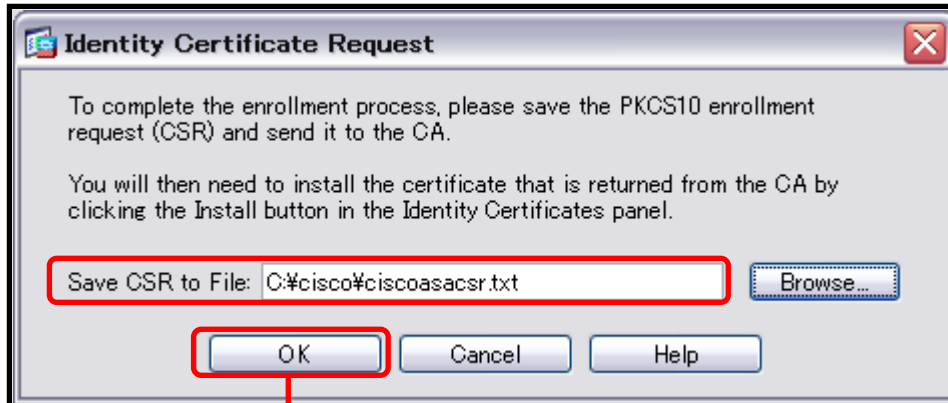
NetAttest EPS では、デフォルトでは CN が必須です。

- ③ **【FQDN】**
 ・ Ciscoasa



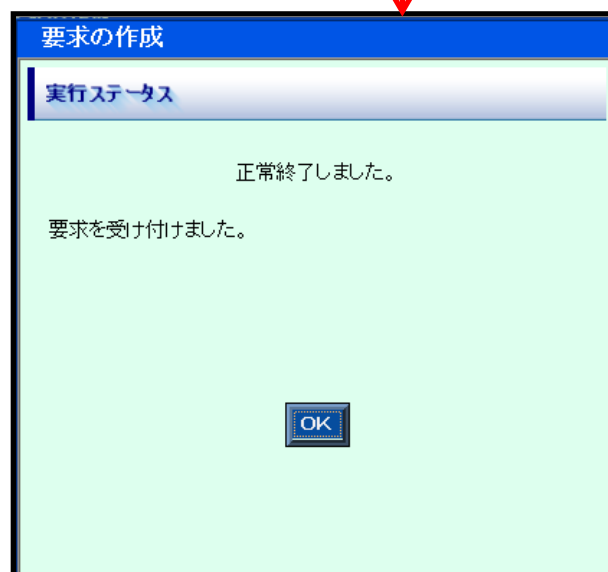
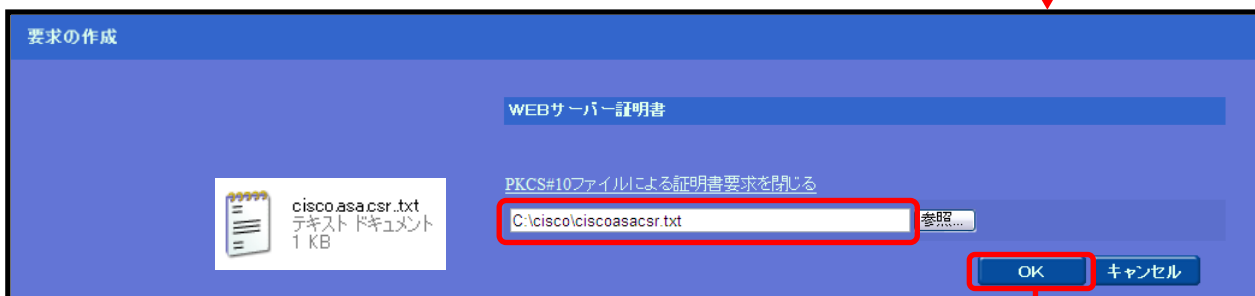
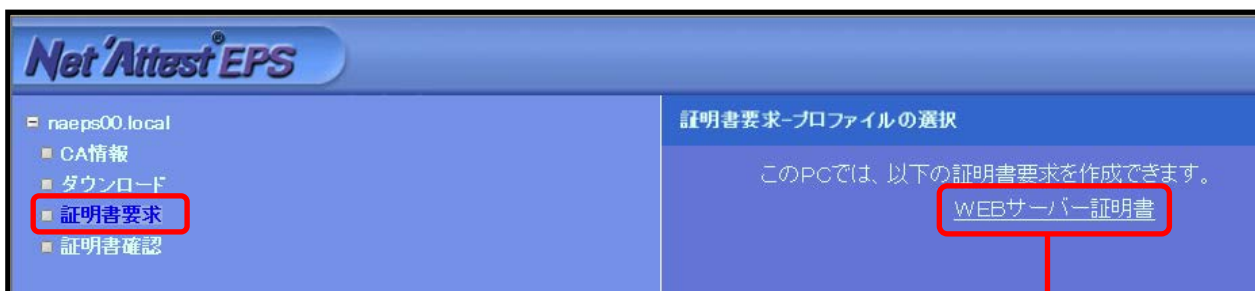
次ページへ

上記設定終了後、『Add Certificate』ボタンをクリックし次の画面に進み、CSR を保存します。保存場所へのパスはすべて英語表記にする必要があります。



4-2 サーバー証明書署名要求 (NetAttest EPS)

ASA 5510 で生成した CSR を基に NetAttest EPS で ASA 5510 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(<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。



4-3 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。



要求リスト

状態 **保留のみ表示**

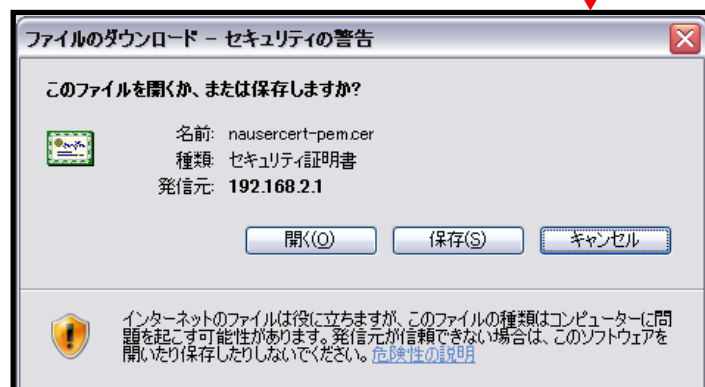
[詳細オプションの設定](#)

	状態	受付日時	送信元	プロフィール
<input checked="" type="checkbox"/>	保留	2012/02/29 22:07:19	CAadm: 192.168.2.212:Mozilla/4.0 (compatible; MSIE 8.0; Windows	WEBサーバー証明書

発行: 有効日数

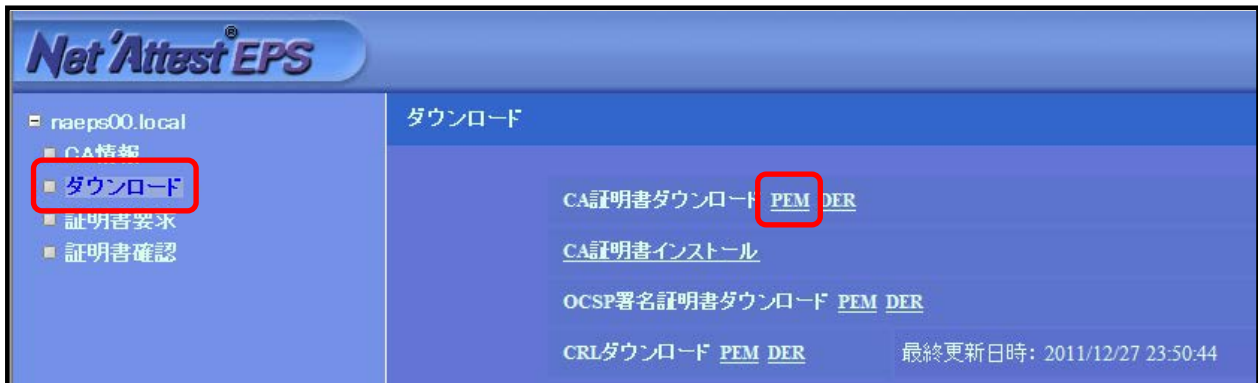
4-4 サーバー証明書のダウンロード (NetAttest EPS)

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。



4-5 CA 証明書の取得 (NetAttest EPS)

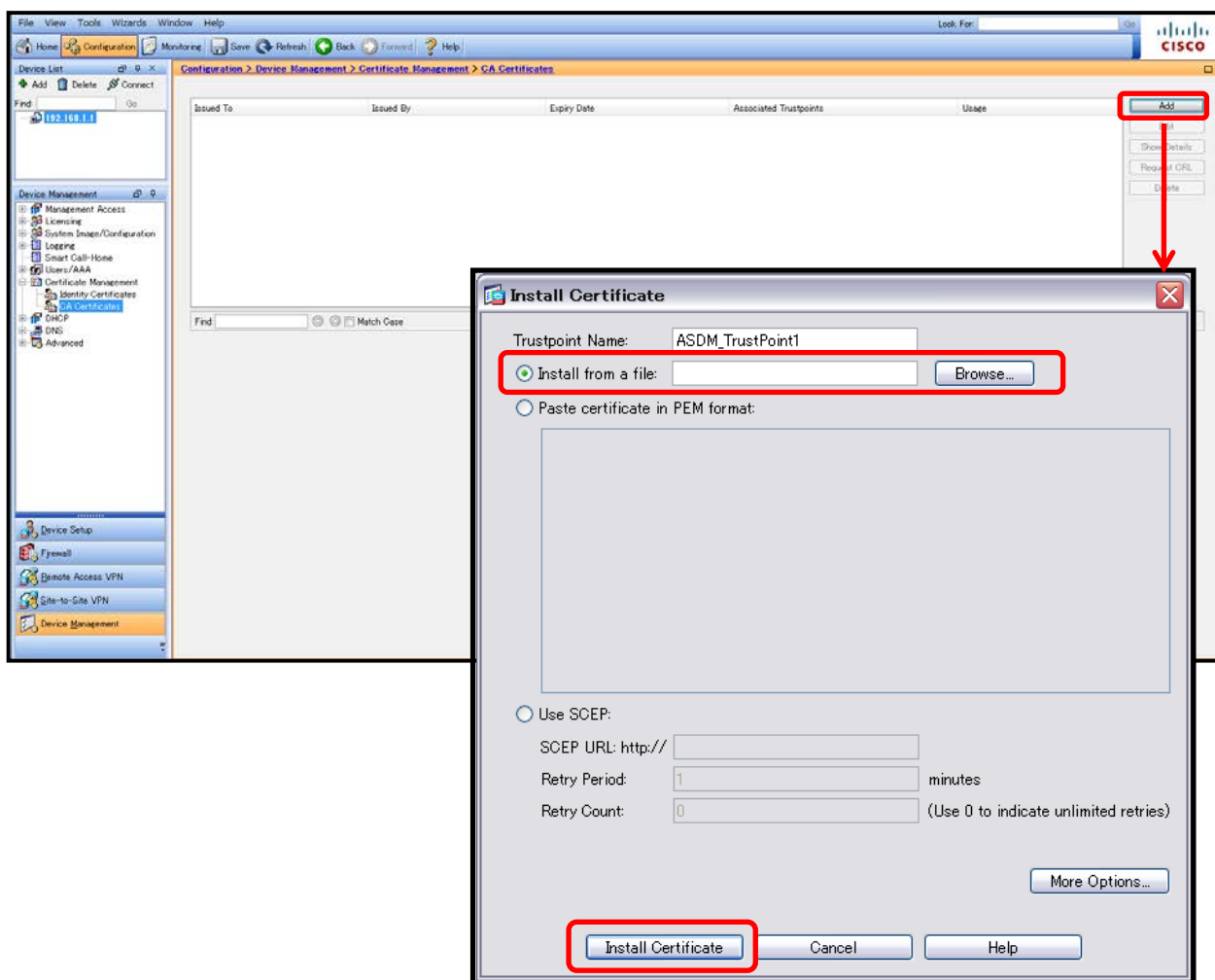
管理者向け証明書サービスページから、NetAttest EPS の CA 証明書をダウンロードします。CA 証明書は、PEM 形式(nacacert-pem.cer)を選択します。



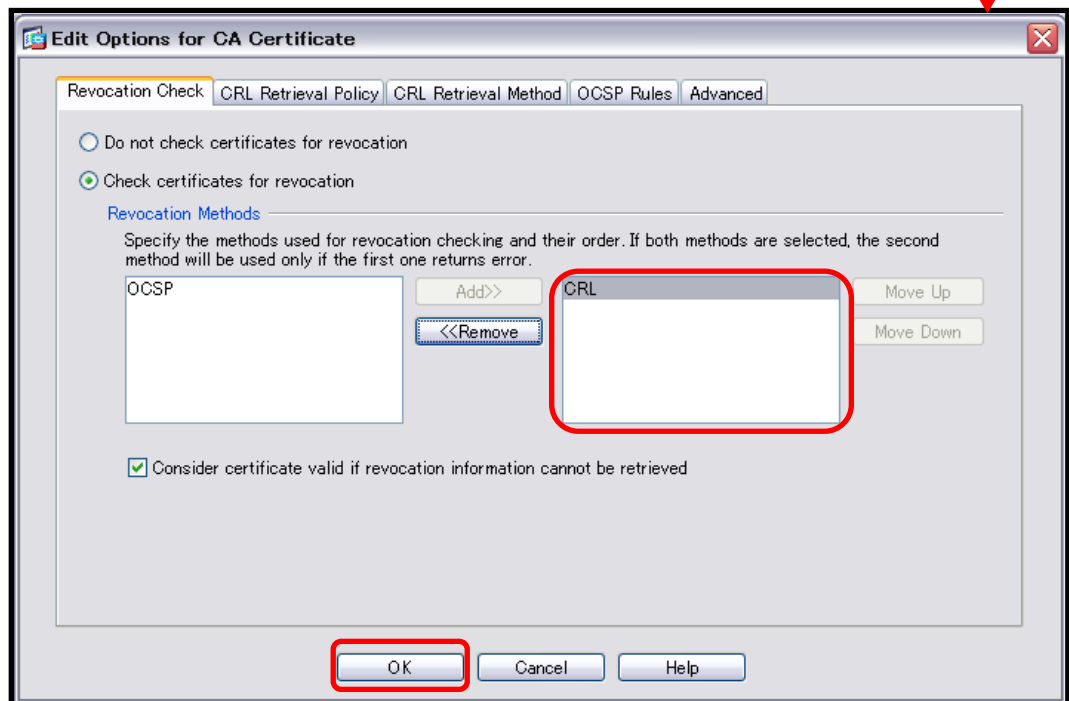
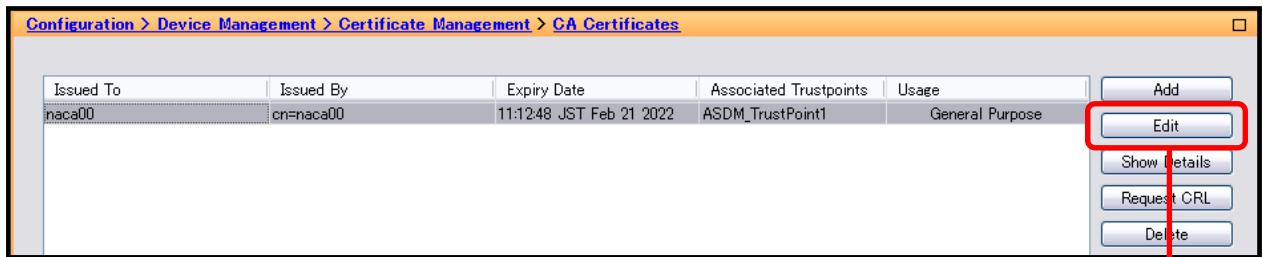
4-6 CA 証明書のインポート (ASA 5510)

NetAttest EPS からダウンロードした CA 証明書(nacacert-pem.cer)を ASA 5510 にインポートします。

「Configuration」 - 「Device Management」 - 「Certificate Management」 - 「CA Certificates」の画面からインポートを行います。



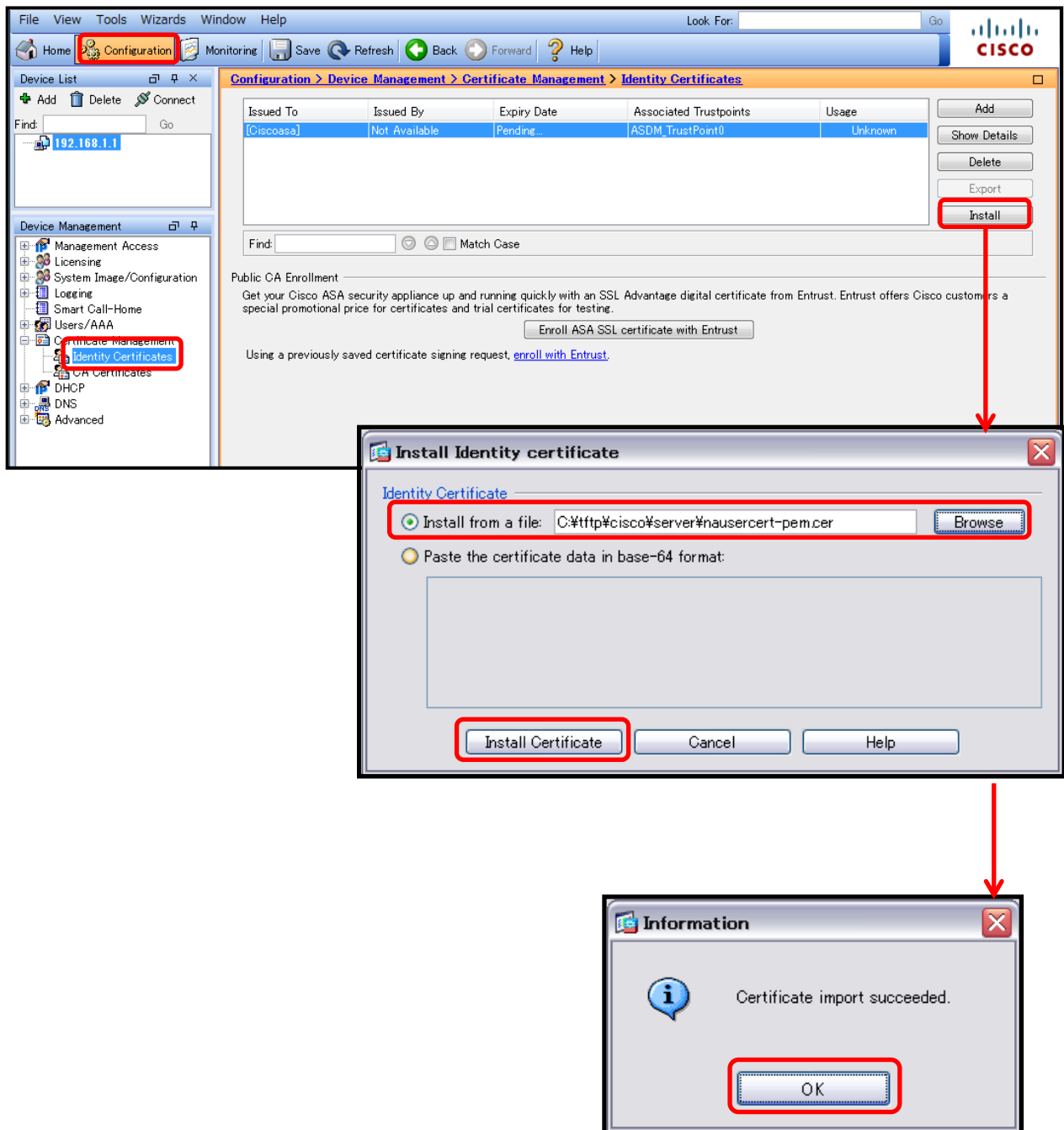
次に、インポートした CA 証明書を選択し、CRL の設定をします。



4-7 サーバー証明書のインポート (ASA 5510)

NetAttest EPS で発行したサーバー証明書をインポートします。

「Configuration」 - 「Device Management」 - 「Certificate Management」 - 「Identity Certificates」の画面からインポートします。



5 ASA 5510 の接続設定

ASA 5510 の接続に関する設定の流れ

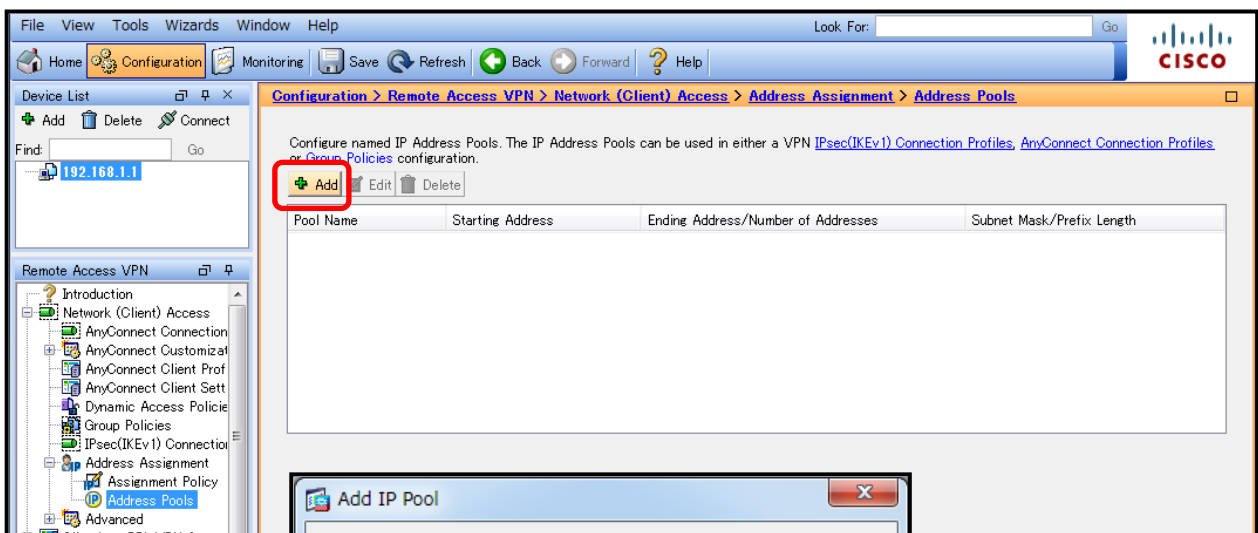
1. IP アドレスプールの設定
2. AAA サーバー(RADIUS サーバー)の設定
3. AnyConnect VPN Connection Setup Wizard

5-1 IP アドレスプールの設定

AnyConnect を用いて SSL-VPN 接続に成功した VPN クライアントに対して、割り当てる IP アドレスプールを設定します。

「Configuration」 - 「Remote Access VPN」 - 「Network (Client) Access」 - 「Address Assignment」 の「Address Pools」で『Add』をクリックします。

[Add IP Pool]で割り当てる範囲の IP アドレスを指定します。



Add IP Pool

Name:

Starting IP Address:

Ending IP Address:

Subnet Mask:

[Name]

• pool-sample

[Starting IP Address]

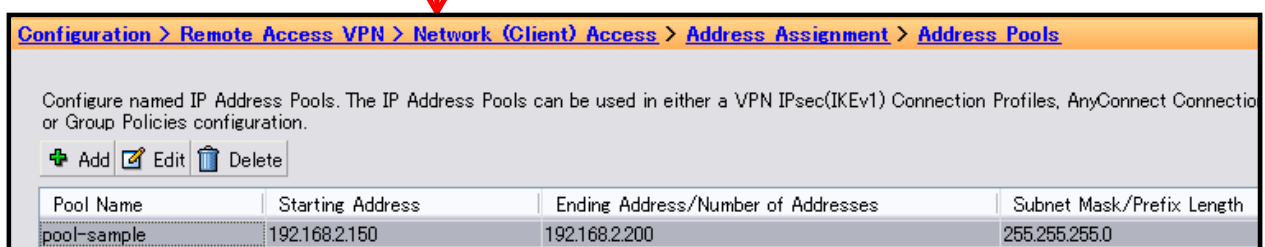
• 192.168.1.150

[Ending IP Address]

• 192.168.1.200

[Subnet Mask]

• 255.255.255.0



5-2 AAA サーバー(RADIUS サーバー)の設定

NetAttest EPS に問合わせの際のプロトコル等を指定します。

「Configuration」 - 「Remote Access VPN」 - 「AAA/Local Users」 - 「AAA Server Groups」 の[AAA Server Groups]から設定します。

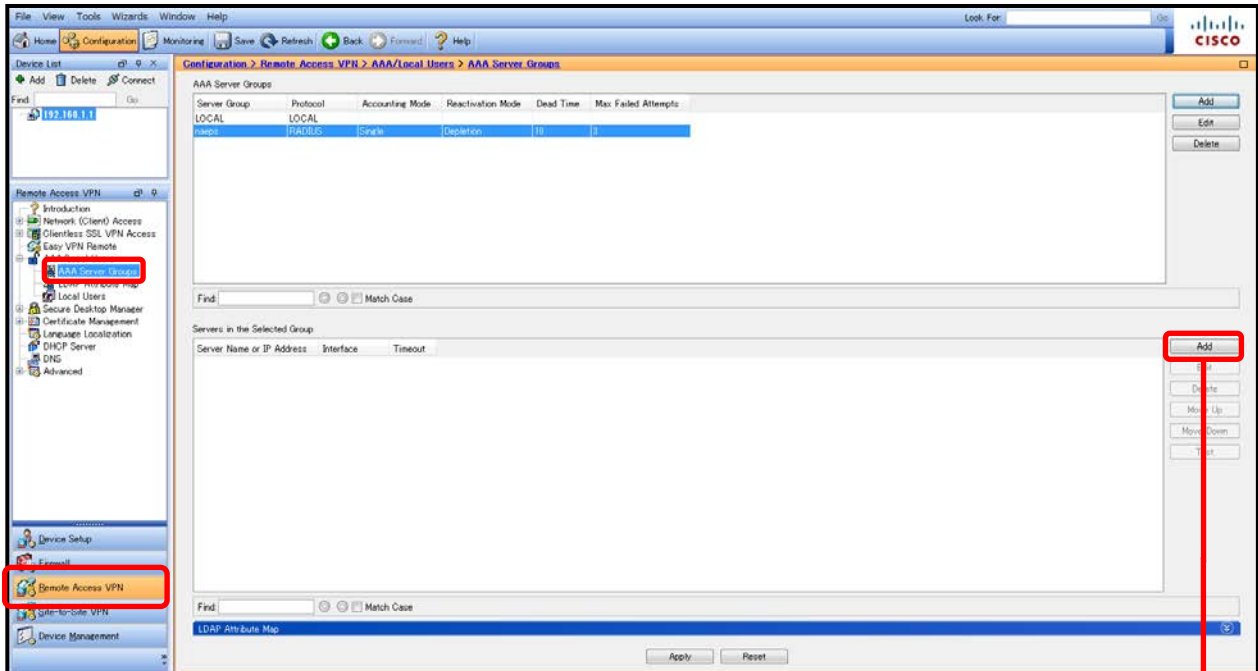
The screenshot shows the Cisco configuration interface for AAA Server Groups. The main window displays a table with columns for Server Group, Protocol, Accounting Mode, Reactivation Mode, Dead Time, and Max Failed Attempts. The 'Add' button is highlighted with a red box, and a red arrow points to the 'Add AAA Server Group' dialog box.

The 'Add AAA Server Group' dialog box contains the following configuration:

- Server Group: naeps
- Protocol: RADIUS
- Accounting Mode: Simultaneous Single
- Reactivation Mode: Depletion Timed
- Dead Time: 10 minutes
- Max Failed Attempts: 3
- Enable interim accounting update
- VPN3K Compatibility Option: [Dropdown]
- Buttons: OK (highlighted with a red box), Cancel, Help

↓ 次ページへ

次に、[Servers in the Selected Group]で RADIUS サーバーとして NetAttest EPS を指定します。



[Interface Name]

- outside

[Server name or IP Address]

- 192.168.1.2

[Server Authentication Port]

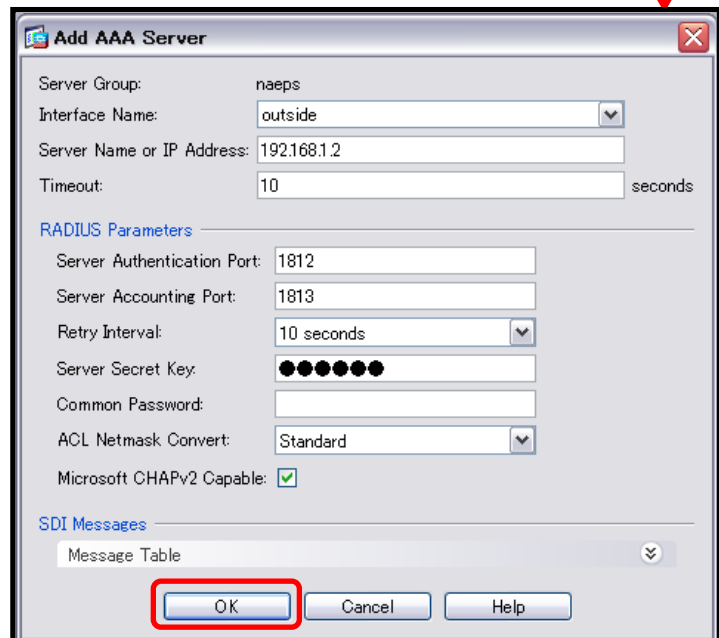
- 1812

[Server Accounting Port]

- 1813

[Server Secret Key]

- secret

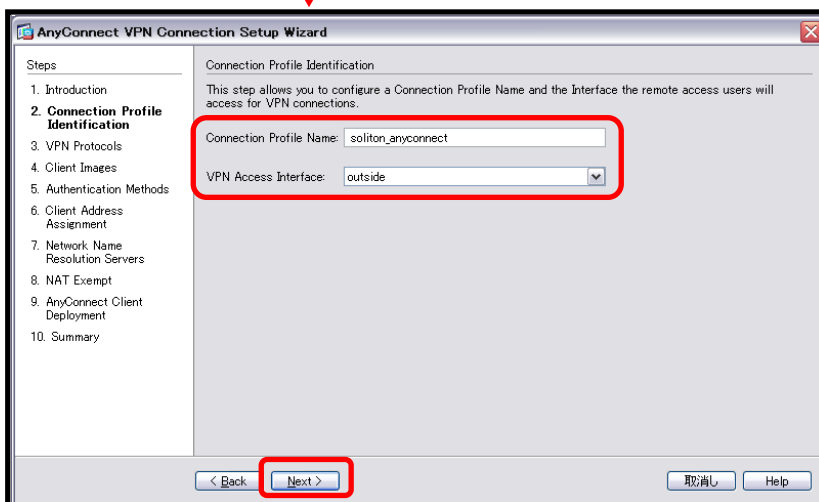
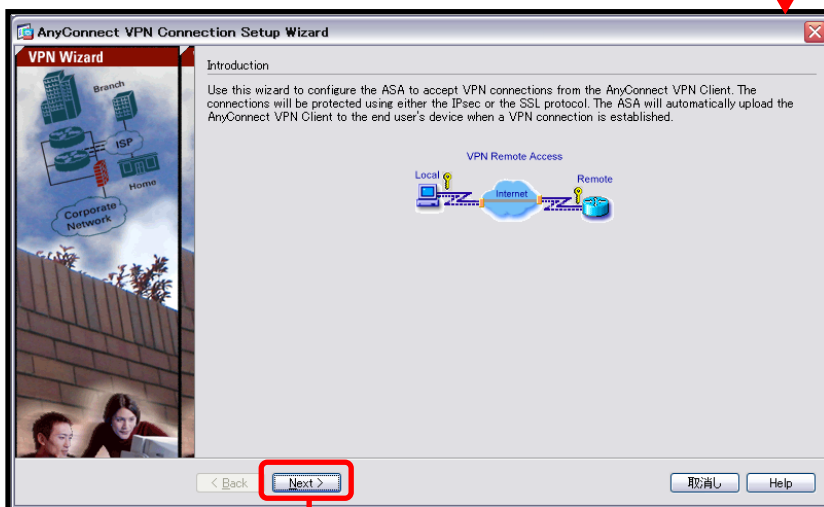
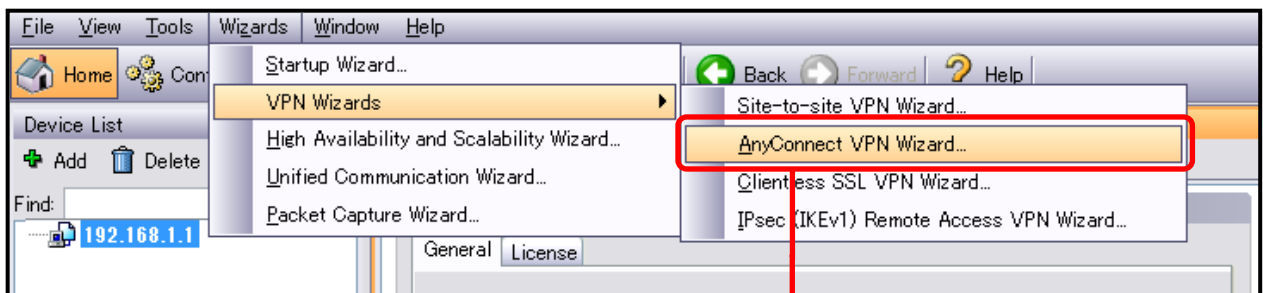


↓ 次ページへ

5-3 AnyConnect VPN Connection Setup Wizard

AnyConnect(SSL-VPN)の接続プロファイルを作成します。

「AnyConnect VPN Wizard」を利用し、プロファイルを作成します。

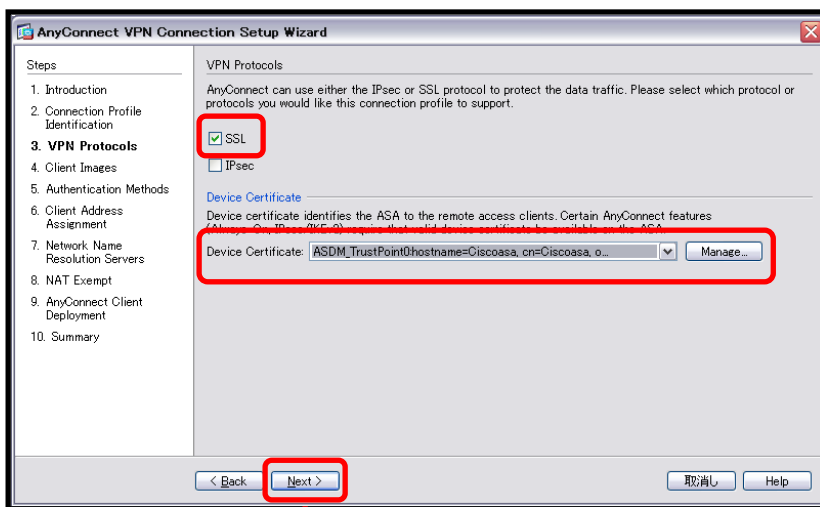


[Connection Profile Name]

• soliton_anyconnect

[VPN Access Interface]

• outside

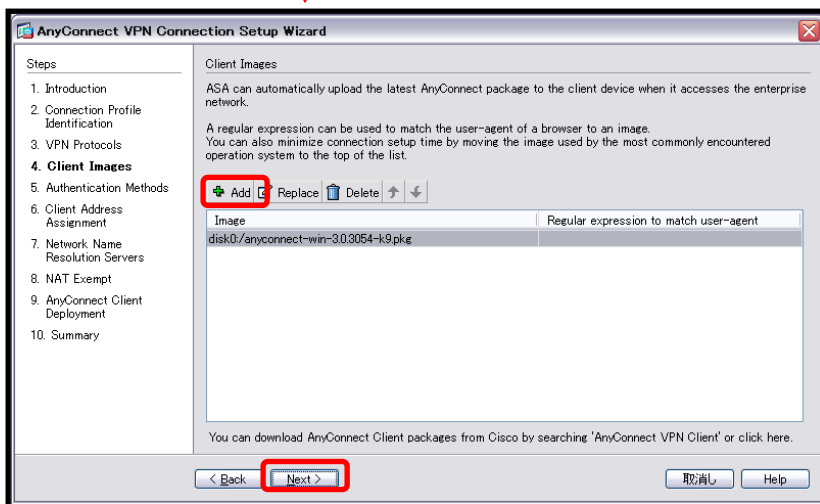


[VPN Protocols]

- ・ SSL

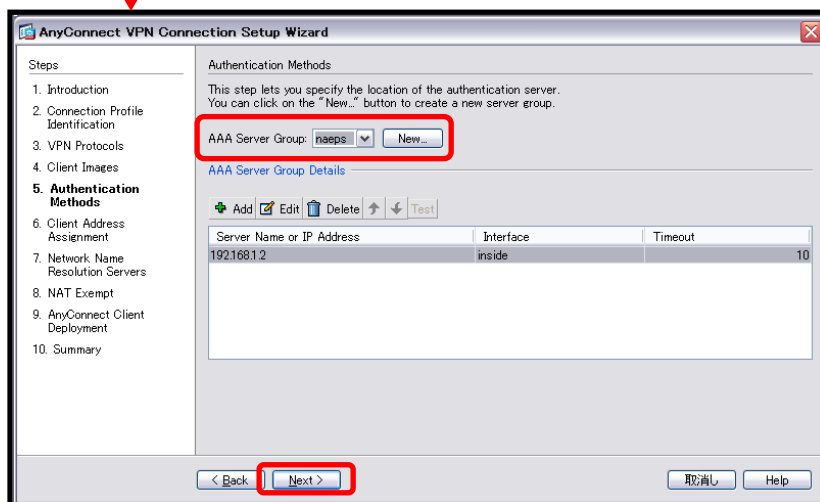
[Device Certificate]

- ・ インポートしたサーバ証明書を選



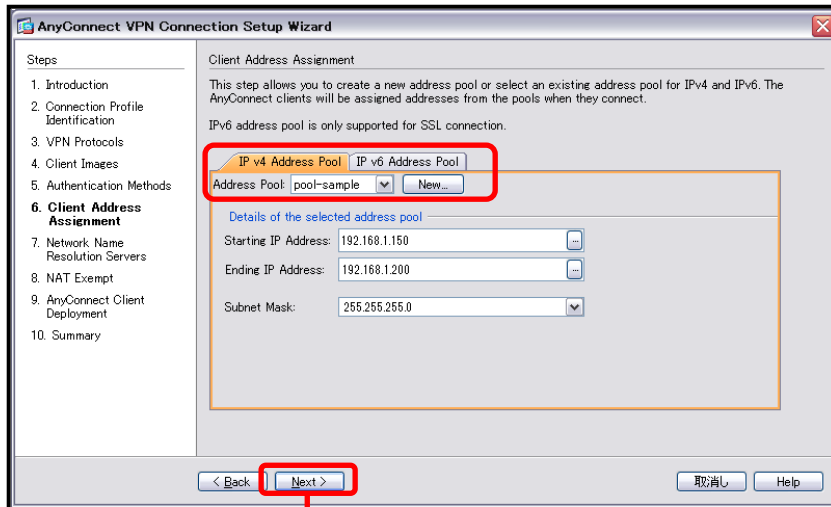
- ・ Add ボタンから、クライアントイメージ [Any Connect pkg ファイル] を選択

pkg ファイル(クライアント用 AnyConnect ソフトウェアイメージ)をインポートしなければ、AnyConnect を受付ける Interface が有効になりません。最新バージョンを取得するには cisco.com でダウンロードして下さい。

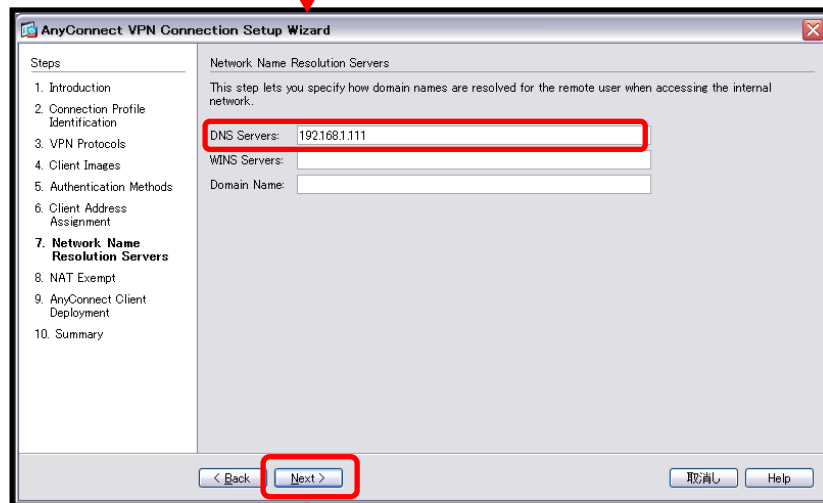


[AAA Server Group]

- ・ 作成済みの [naeps] を指定

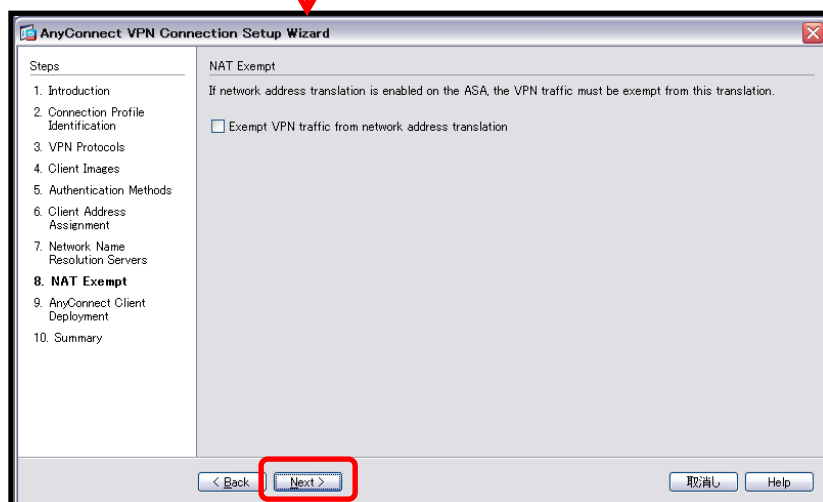


【IPv4 Address Pool】
作成済みの IP アドレスプ
ールを指定

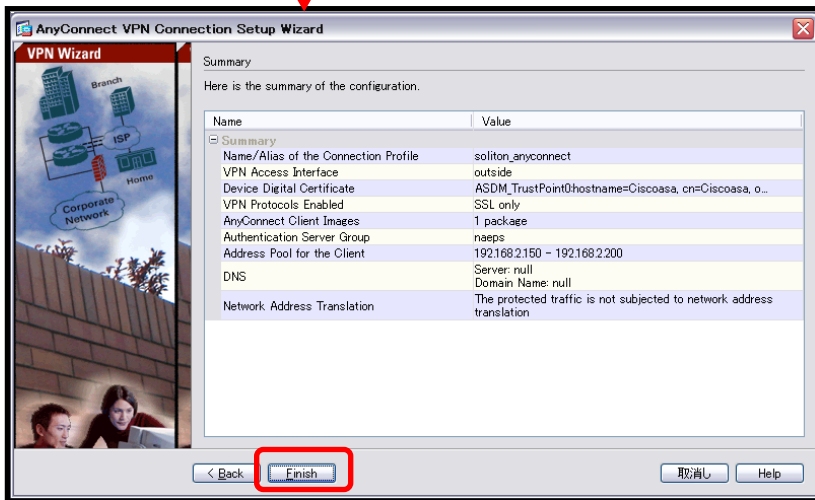
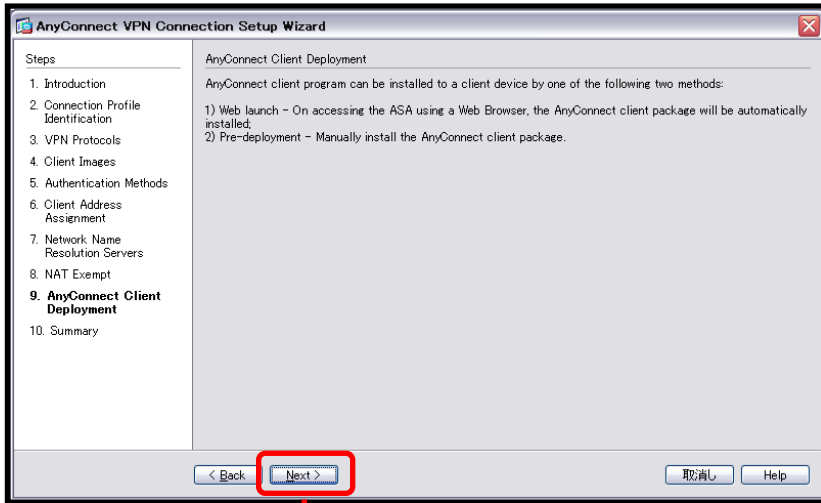


【DNS Servers】
・DNS のアドレスを指定

 **本項目は必須のため、DNSが無い場合でも適当な値を指定してください。**



【NAT Exempt】
・チェックなし



作成された[Connection Profiles]を『edit』から編集します。

[AAA Server Group]には、先程作成した[AAA Server Group]を選択します。

The screenshot shows the Cisco AnyConnect configuration interface. The main window displays the 'AnyConnect Connection Profiles' configuration page. A red box highlights the 'Add' button in the 'Connection Profiles' section. A red arrow points from this button to the 'Edit AnyConnect Connection Profile' dialog box.

The 'Edit AnyConnect Connection Profile' dialog box shows the following configuration:

- Name:** soliton_anyconnect
- Aliases:** soliton_anyconnect
- Authentication Method:** Both (selected)
- AAA Server Group:** naeps (selected)
- Client Address Assignment:** None (selected)
- Client Address Pools:** pool-sample
- Client IPv6 Address Pools:** (empty)
- Default Group Policy:** GroupPolicy_soliton_anyconnect
- Enable SSL VPN client protocol:** checked
- Enable IPsec(IKEv2) client protocol:** unchecked
- DNS Servers:** 192.168.1.111
- WINS Servers:** (empty)
- Domain Name:** (empty)

The 'OK' button is highlighted with a red box.

[Method]

- Both

[AAA Server Group]

- naeps

6 Windows 版 AnyConnect の設定

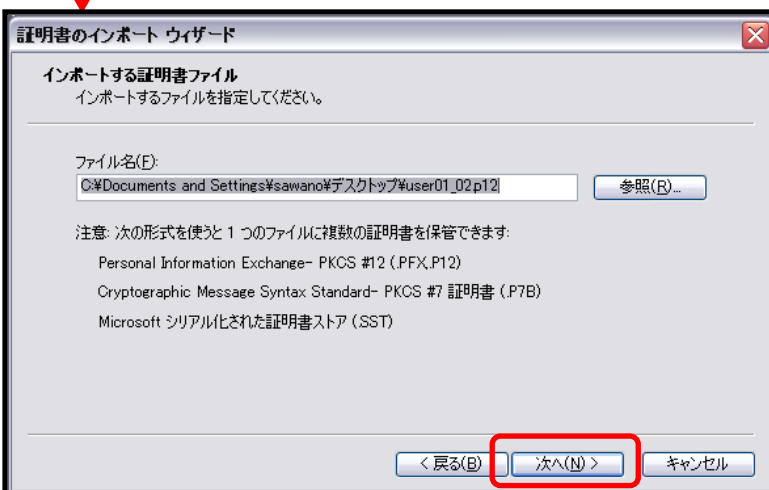
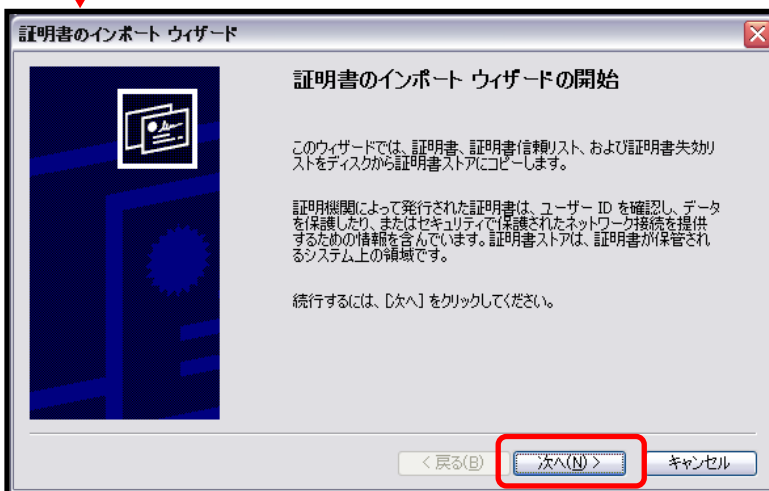
AnyConnect VPN クライアントの設定

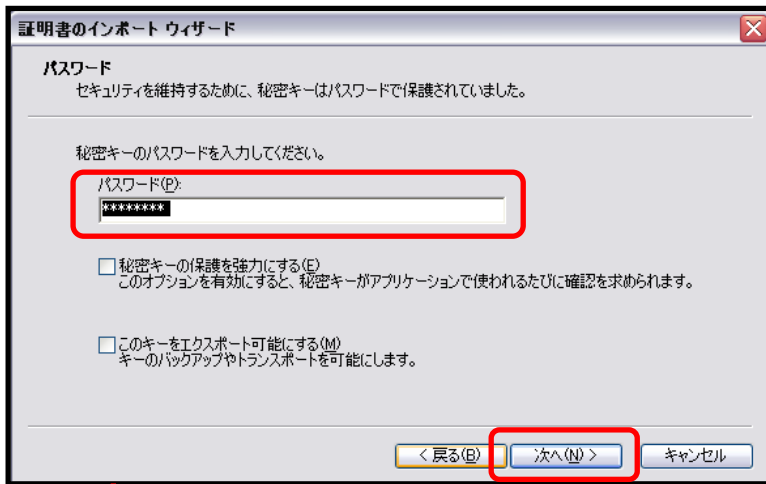
1. PC へのデジタル証明書のインストール
2. Windows 版 AnyConnect の設定

6-1 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。

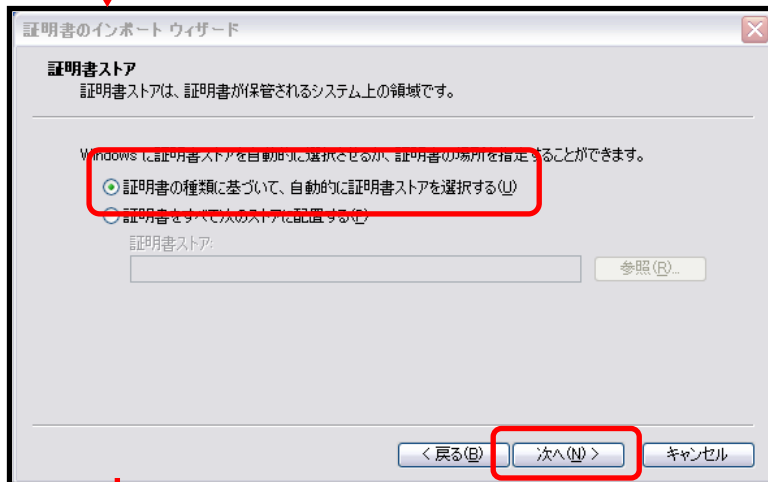
ダウンロードしておいたクライアント証明書(user01_02.p12)をダブルクリックすると、証明書インポートウィザードが実行されます。



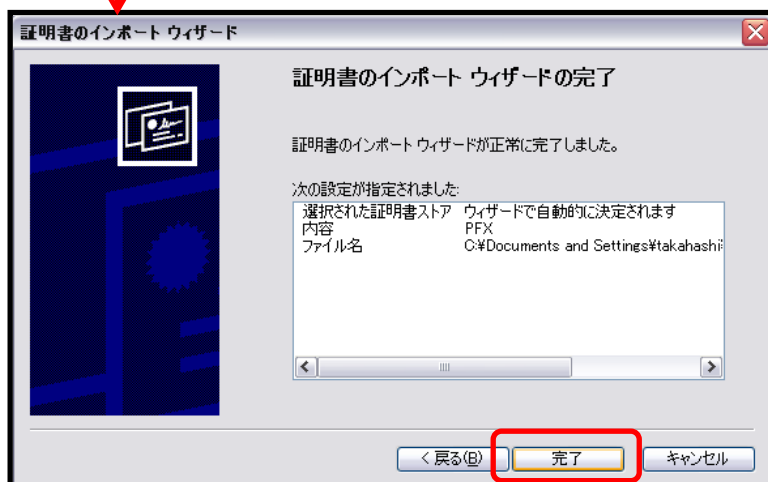


【パスワード】
NetAttest EPS で証明書を
発行した際に設定したパスワードを入力

 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



6-2 Windows 版 AnyConnect の設定

Cisco AnyConnect VPN クライアントを Cisco.com もしくは ASA ユーザーサービスページからダウンロードし、インストールします。ASA ユーザーサービスからダウンロードする場合は、本環境では <http://192.168.2.2/> にアクセスして下さい。

AnyConnect をインストールすると[タスクトレイ]に  アイコンが表示されます。クリックすると以下の画面が表示されますので、接続先の ASA を指定します。



7 iOS 版 AnyConnect の設定

AnyConnect VPN クライアントの設定

1. iPad へのデジタル証明書のインストール
2. iOS 版 AnyConnect の設定

7-1 iPad へのデジタル証明書のインストール

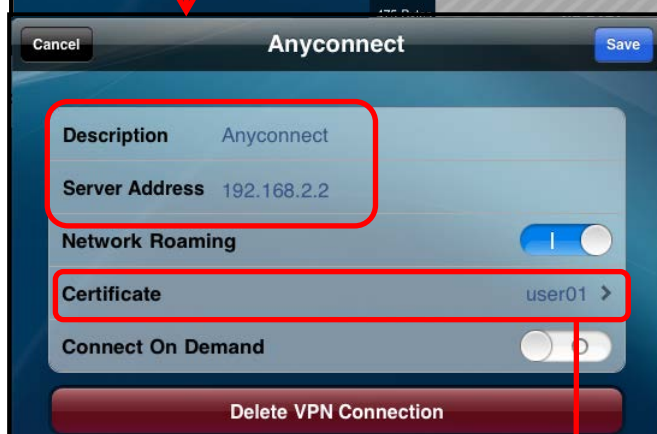
NetAttest EPS から発行したデジタル証明書を iOS デバイスにインストールする方法として、下記 3 つの方法などがあります。

- 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) NetAttest EPS-ap を使い、SCEP で取得する方法

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。

7-2 iOS 版 AnyConnect の設定

Cisco AnyConnect VPN クライアントを Apple App Store からインストールします。
インストール後アプリを起動し、AnyConnect の設定を行います。
下記のように接続先と認証に使うデジタル証明書を選択します。

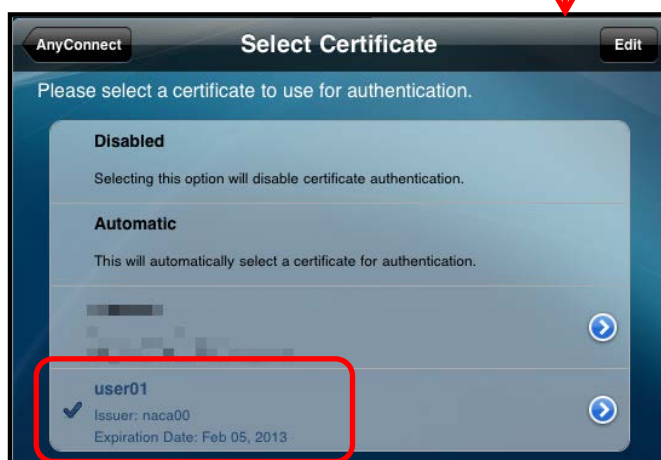


【Description】

・任意

【Server Address】

・ASA のアドレス(192.168.2.2)

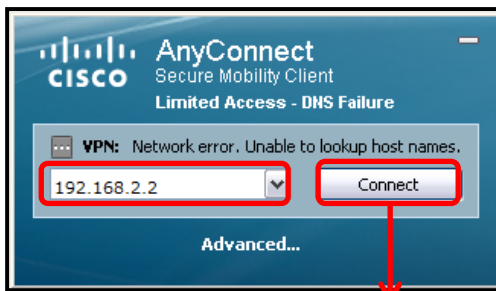


インストールした証明書を選択

8 接続の確認

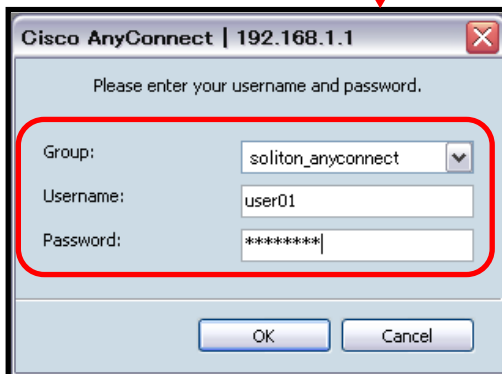
8-1 PC における AnyConnect を利用した SSL-VPN 接続

Cisco AnyConnect VPN クライアントを利用し、VPN 接続を行います。



[VPN]

・ 192.168.2.2



[Group]

・ Soliton_anyconnect

[username]


・ user01

[password]

・ password



[Group] には Connection Profile Name を指定。

AnyConnect 接続が完了すると、タスクトレイのアイコン  が表示され、IP アドレスプールから IP アドレスが払い出されます。

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\>ipconfig

Windows IP Configuration

Ethernet adapter ワイヤレス ネットワーク接続:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.232
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter ローカル エリア接続:

    Media State . . . . . : Media disconnected

Ethernet adapter Cisco AnyConnect Secure Mobility Client Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.151
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254

C:\Documents and Settings\>
  
```

8-2 iPad における AnyConnect を利用した SSL-VPN 接続

Cisco AnyConnect VPN クライアントを利用し、VPN 接続を行います。

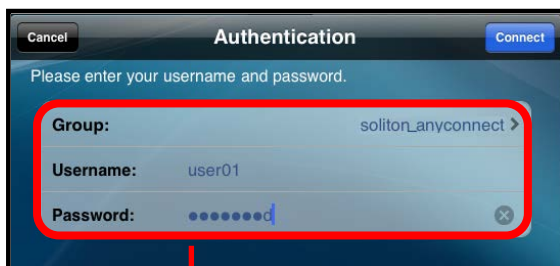
AnyConnect アプリを起動し、「Choose a connection」で作成済みの接続プロファイルを選択し、「AnyConnect VPN」を ON にします。



【Choose a connection】

- Anyconnect

表示される認証ウィンドウで必要事項を入力します。



【Group】

- Soliton_anyconnect

【username】

- user01

【password】

- password

接続が完了すると、IP アドレスプールから IP アドレスが払い込まれます。



改訂履歴

日付	版	改訂内容
2012/03/30	1.0	初版作成
2013/08/13	1.1	誤表記修正