NetAttest EPS 設定例

連携機器：

Cisco ASA 5505

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 1.3

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 Cisco Systems 社製 Cisco ASA 5505 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。
ABCDabcd1234 (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。

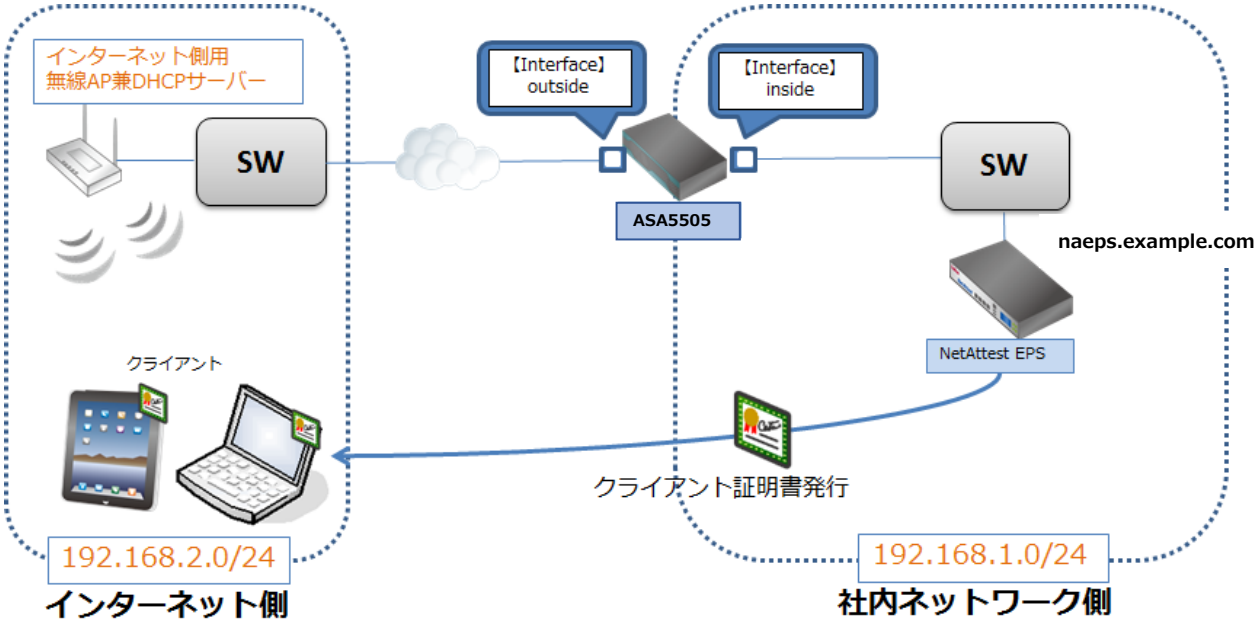
ご注意

本書は、当社での検証に基づき、NetAttest EPS 及び ASA 5505 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

1-1　構成図



※NetAttest EPS の設定は、設定用の Windows 管理端末 と NetAttest EPS の管理ポート（LAN2）を直結して行います。

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)	ソリトンシステムズ	NetAttest EPS (EPS-ST05-A)	Ver. 4.10.0
RADIUS クライアント (SSL VPN 機器)	Cisco Systems	ASA 5505	Ver.8.4(1)
Client PC	Microsoft	Surface3 Pro	Windows 8.1
Client Smart Phone	Apple	iPhone X	iOS 11.1.2
Client Smart Phone	Huawei	Nexus 6P	Android 7.1.2
無線 AP	Allied	AT-TQ3400	-

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-ST05-A	ASA 5505	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

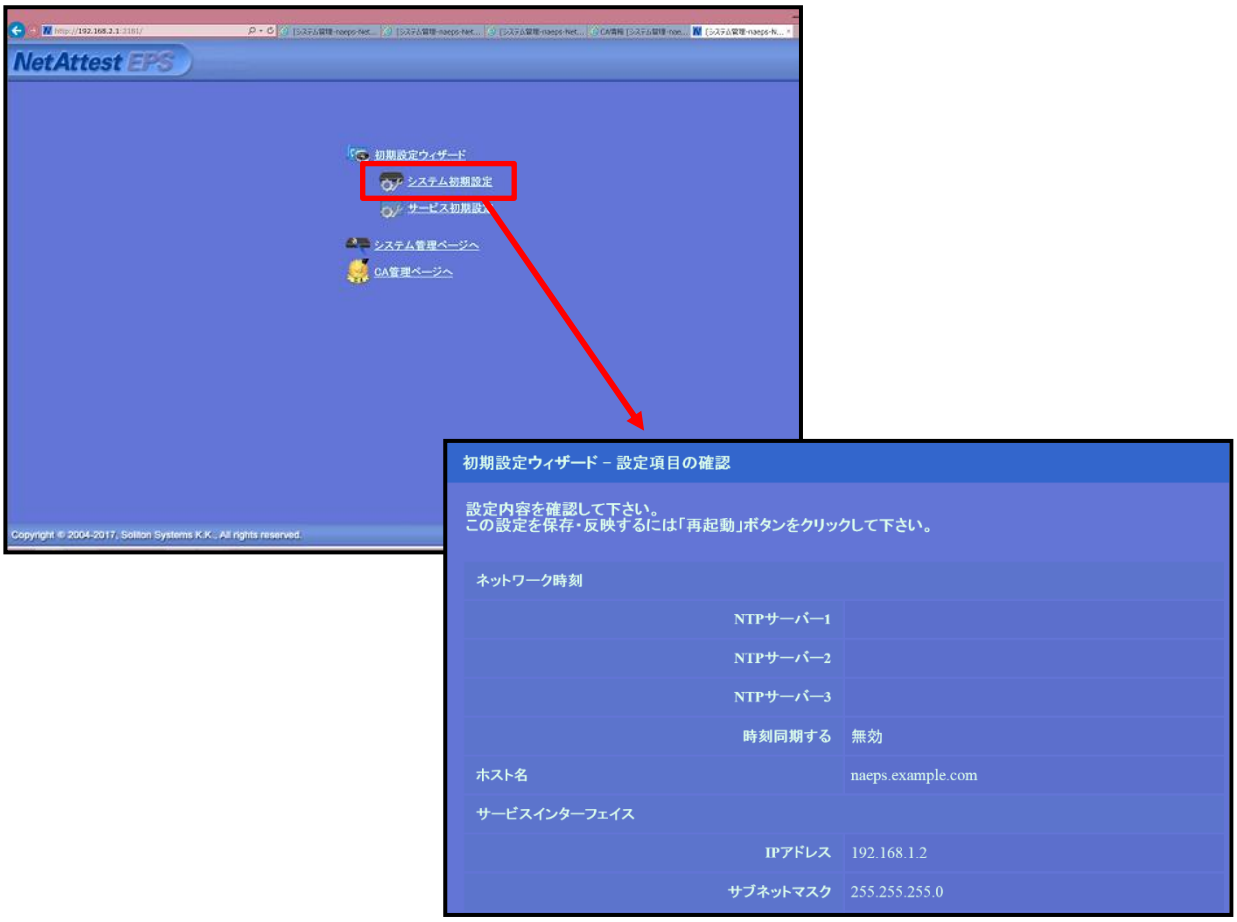
NetAttest EPS 設定の手順

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に従って、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.example.com

【IP アドレス】：デフォルト（LAN1:192.168.1.2,LAN2:192.168.2.1）

【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）

【CA 種別選択】

・ルート CA

【公開鍵方式】

・ＲＳＡ

【鍵長】

・2048

【CA 名】

・EPS ROOT CA

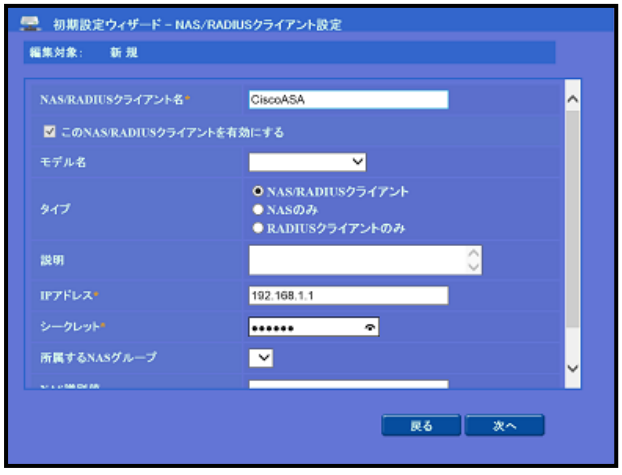
【国名】

・日本

【著名アルゴリズム】

・SHA256

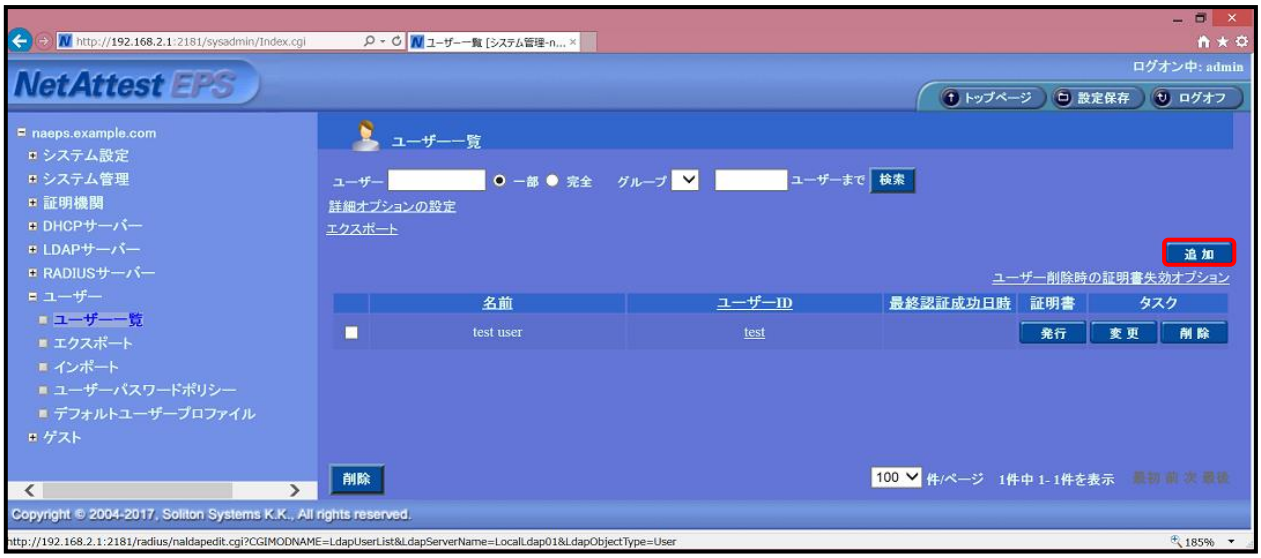
- ◆ RADIUS サーバーの基本設定（証明書検証）
- ◆ NAS/RADIUS クライアント設定



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

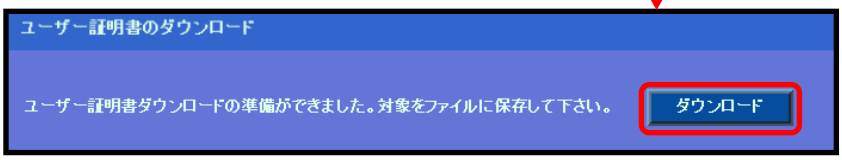
【パスワード】

・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_01.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 5505 の設定準備

ASDM のセットアップと ASA 5505 の基本設定

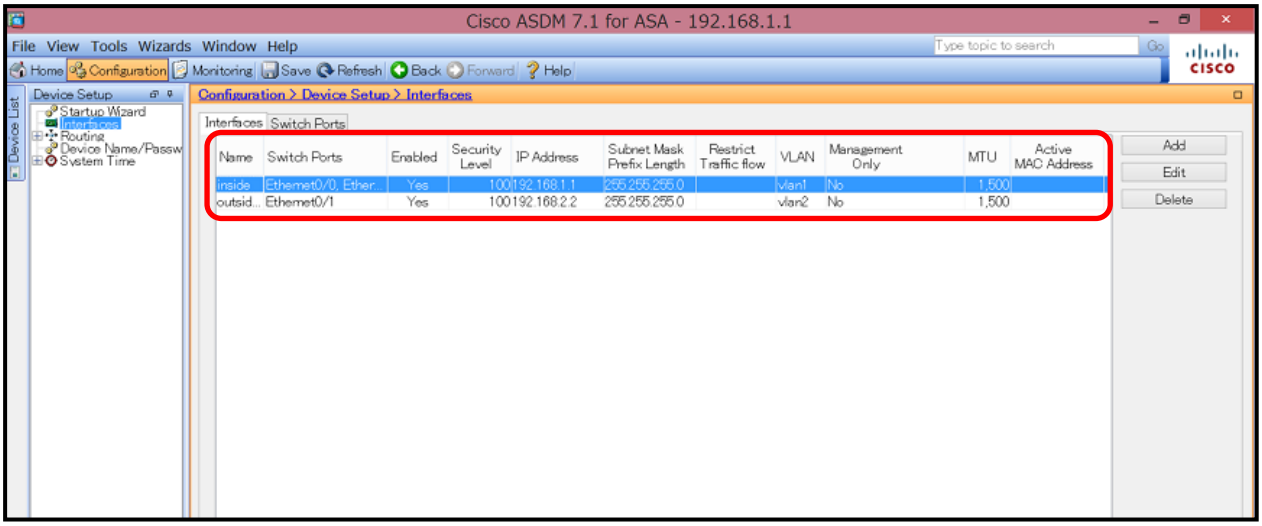
1. インターフェイスの設定
2. システム時刻の設定

3-1　インターフェイスの設定

ASA 5505 の設定は ASDM(Adaptive Security Device Manager)で行います。

本環境では、ASDM ver.7.1(7)を使用しています。

ASA 5505 のインターフェイスの設定は、下記の通りです。



【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。

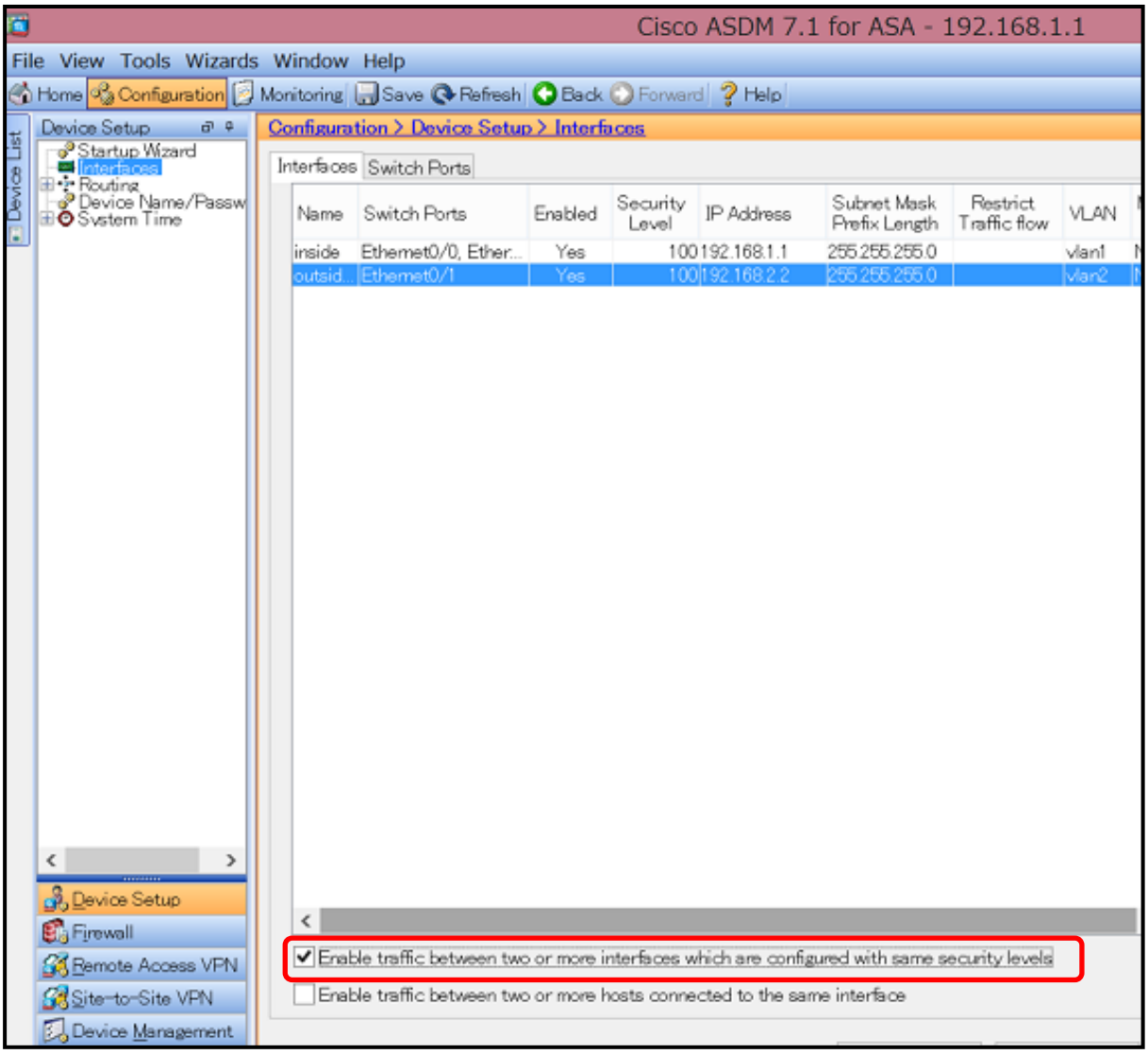
【Ethernet0/1】outside

IP:192.168.2.2 255.255.255.0 ・・・AnyConnect による接続を受付ける interface。

ASA 5505 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。

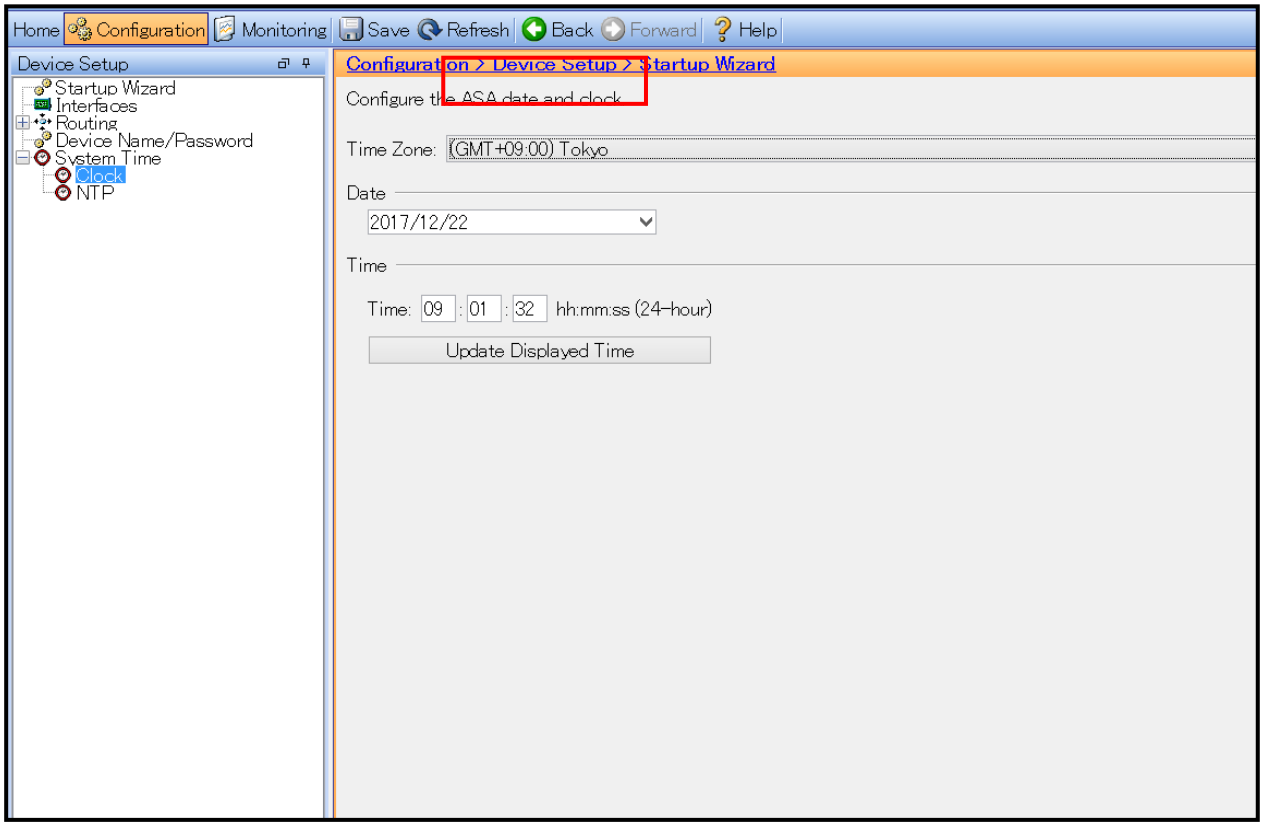
また、 [Enable traffic between two or more interfaces which are configured with same security levels]を有効にします。



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 5505 の PKI 関連の設定

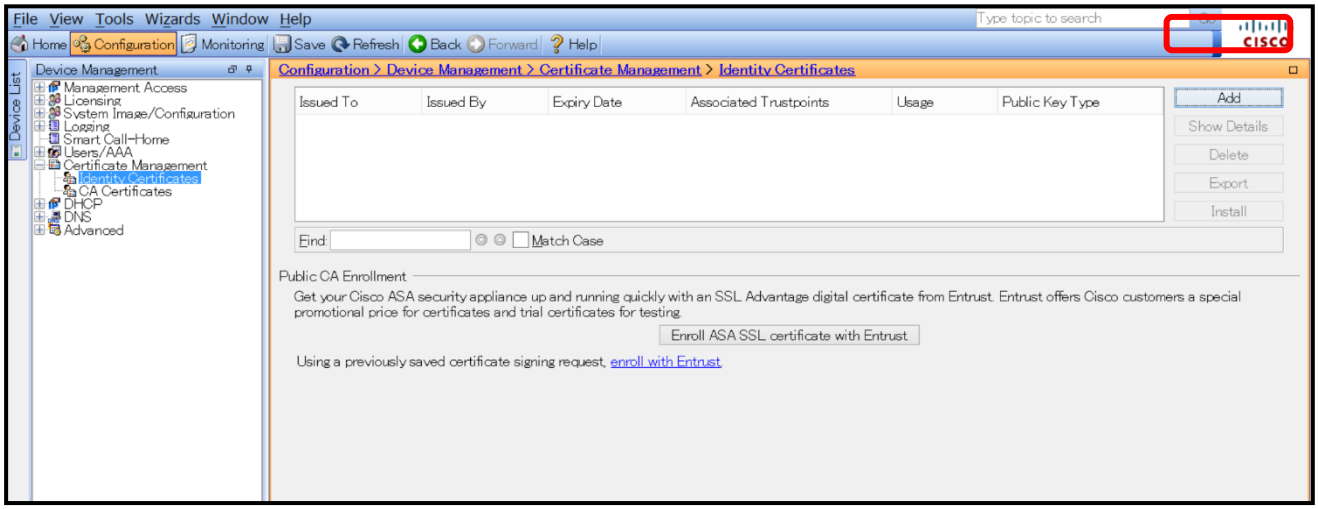
証明書の取得とインポートの手順

1. CSR の生成（ASA 5505）
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 5505）
7. サーバー証明書のインポート（ASA 5505）

4-1　CSR の生成（ASA 5505）

ASA 5505 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。



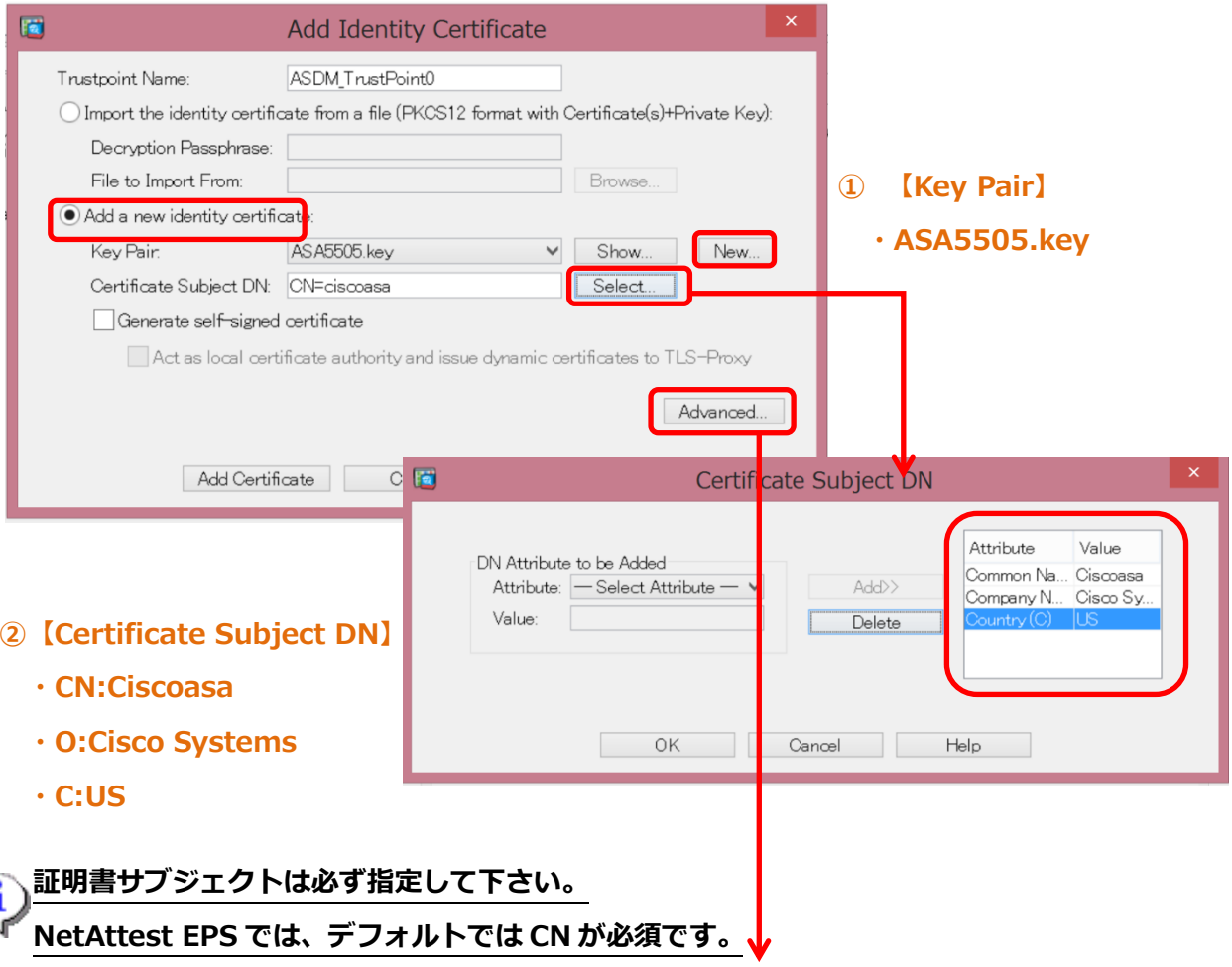
次ページへ

[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。



① 【Key Pair】

・ASA5505.key

② 【Certificate Subject DN】

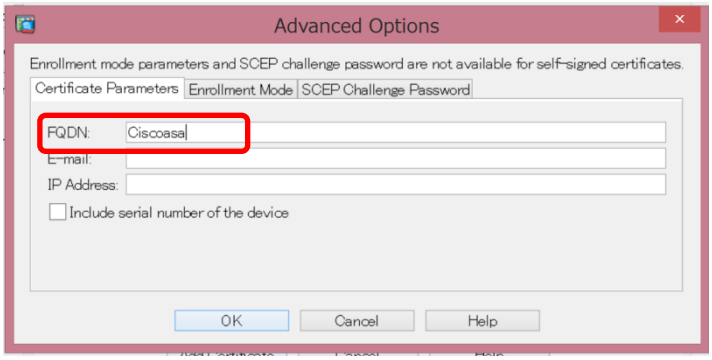
・CN:Ciscoasa

・O:Cisco Systems

・C:US

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。

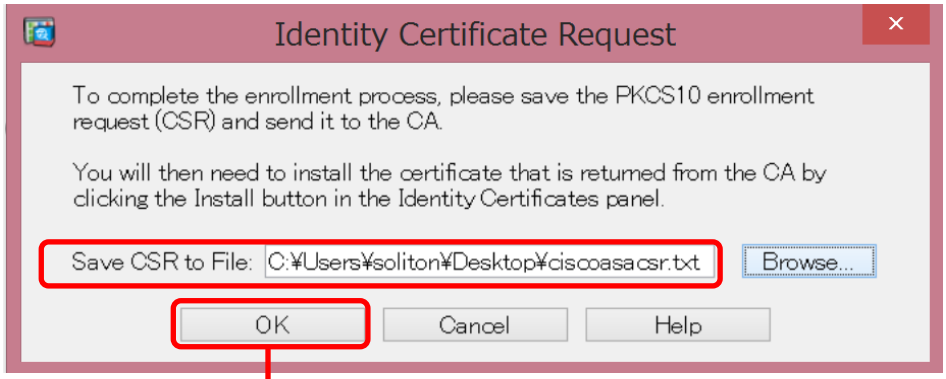


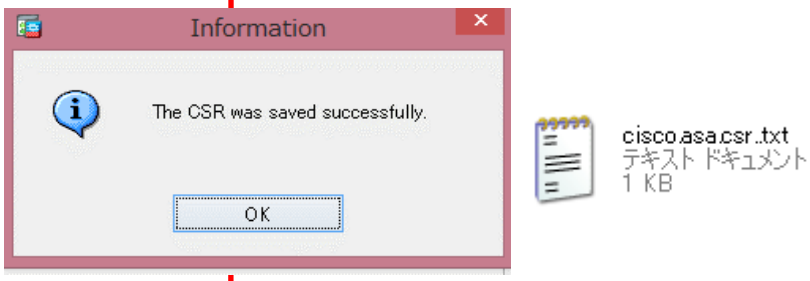
③ 【FQDN】

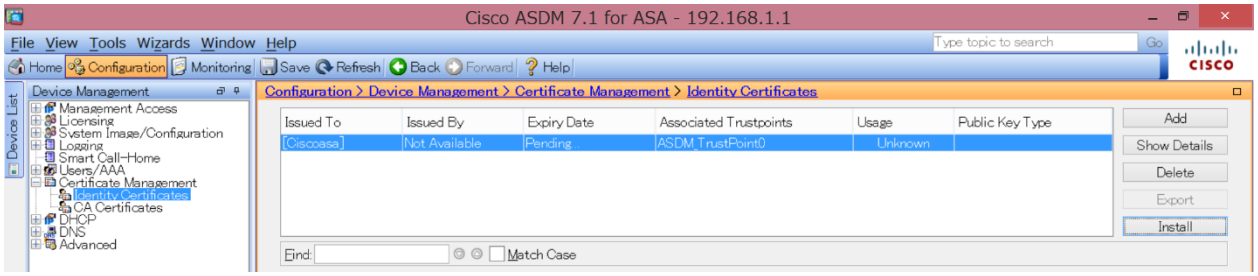
・Ciscoasa

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。

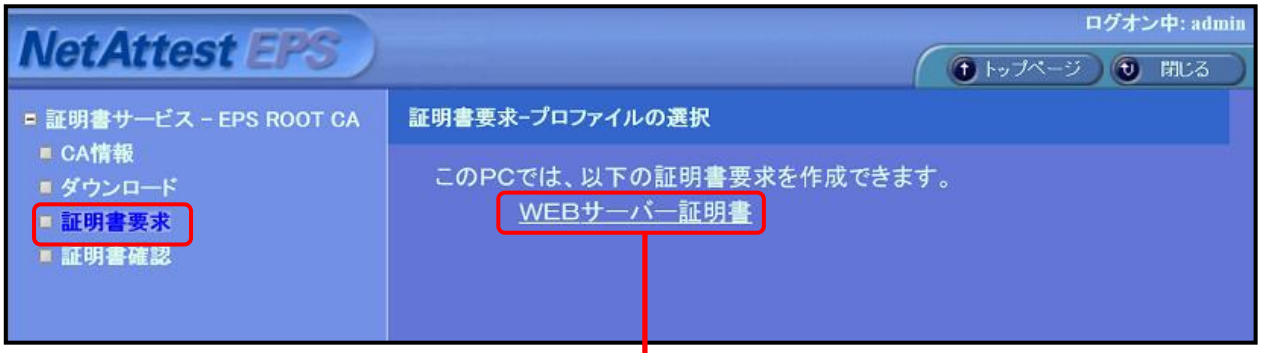


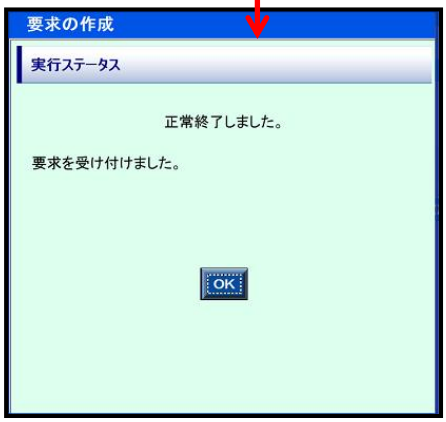




4-2 サーバー証明書署名要求（NetAttest EPS）

ASA 5505 で生成した CSR を基に NetAttest EPS で ASA 5505 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/certsrva/)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。

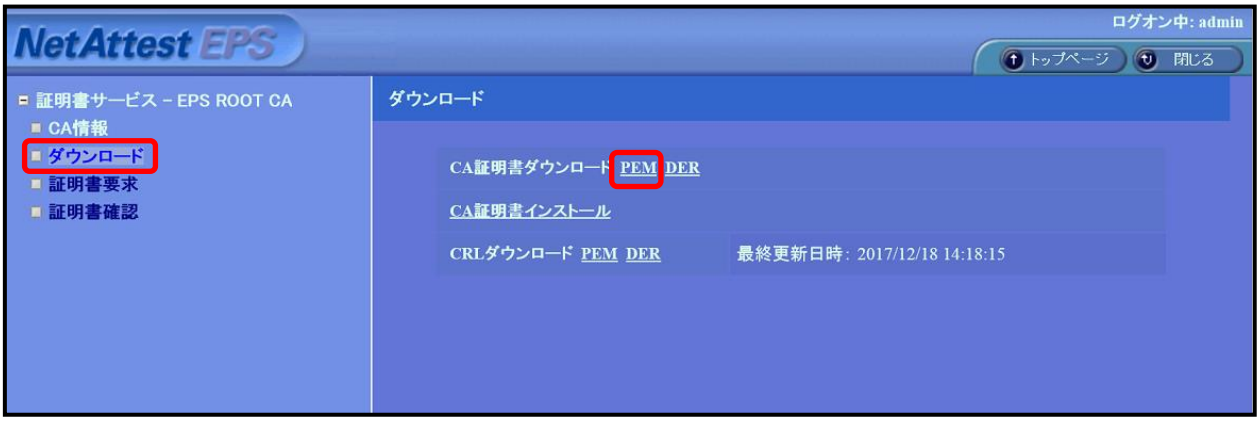
VPN 接続を IP アドレスで行う際は、ASA のサブジェクト別名に使用する IP を追加する必要があります。サブジェクト別名に IP アドレスが記載されてない場合、SSL 通信が正常に行われません。

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)

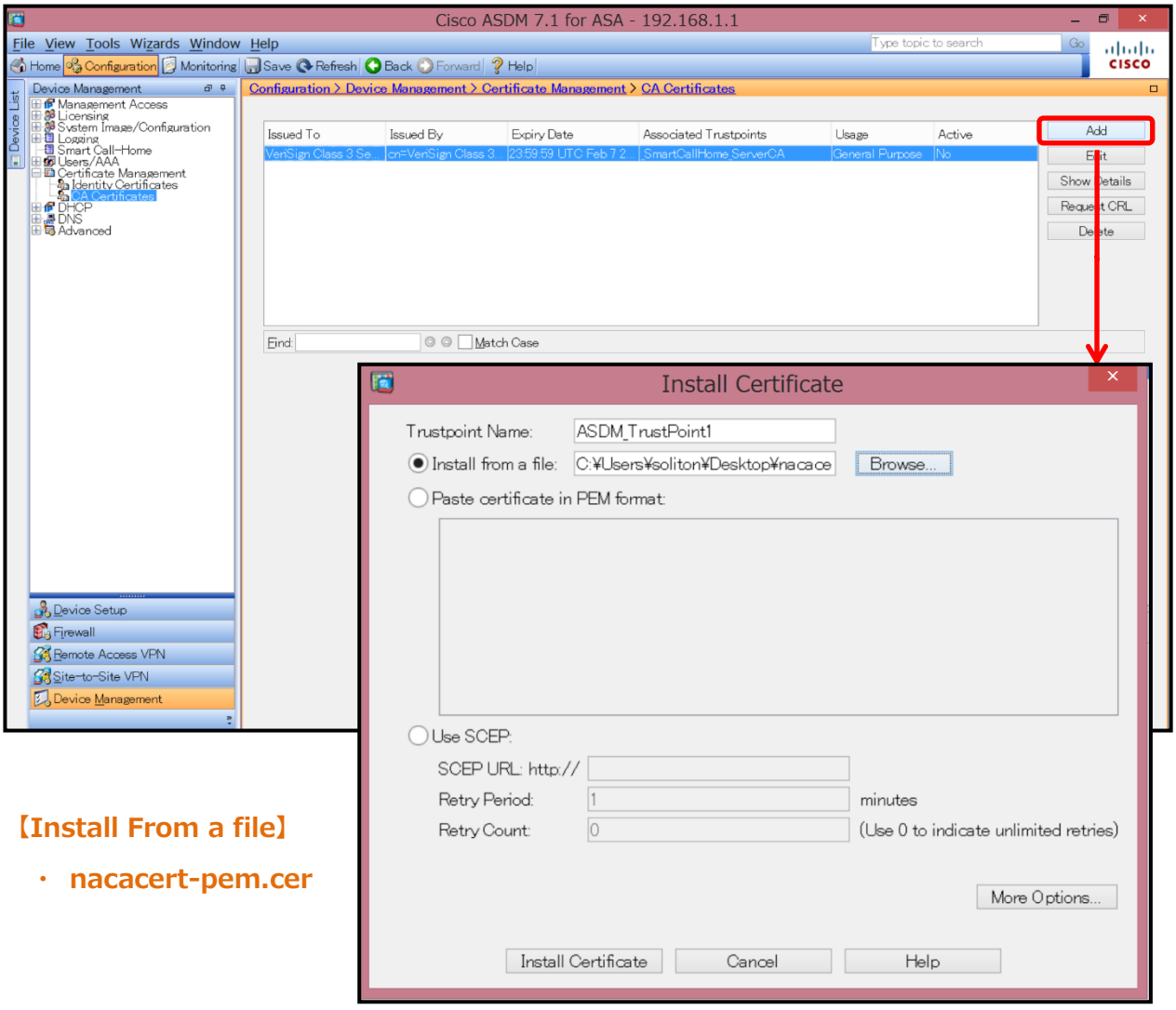
管理者向け証明書サービスページから、NetAttest EPS の CA 証明書をダウンロードします。CA 証明書は、PEM 形式(nacacert-pem.cer)を選択します。



4-6 CA 証明書のインポート (ASA 5505)

NetAttest EPS からダウンロードした CA 証明書(nacacert-pem.cer)を ASA 5505 にインポートします。

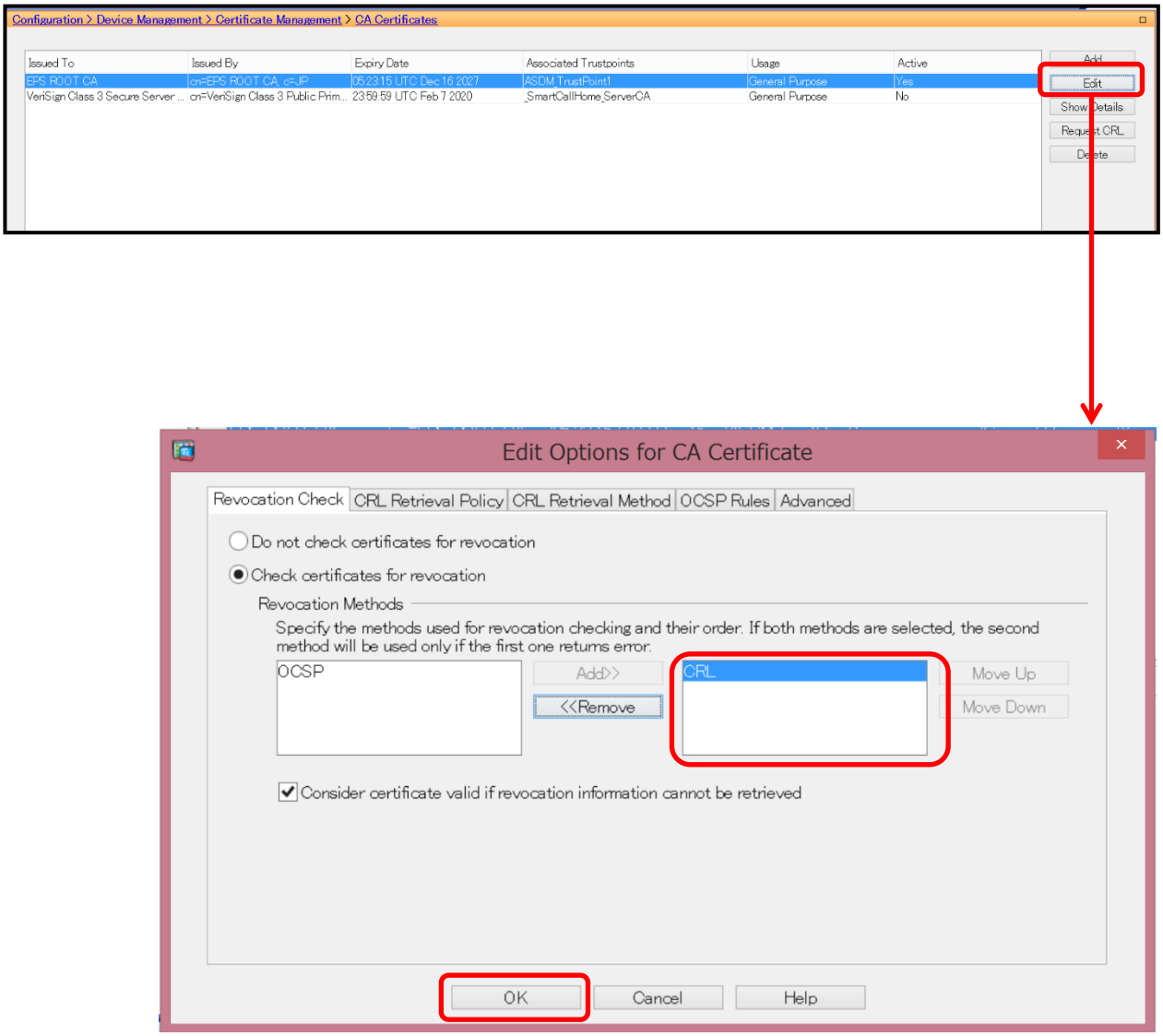
「Configuration」-「Device Management」-「Certificate Management」-「CA Certificates」の画面からインポートを行います。



【Install From a file】

- **nacacert-pem.cer**

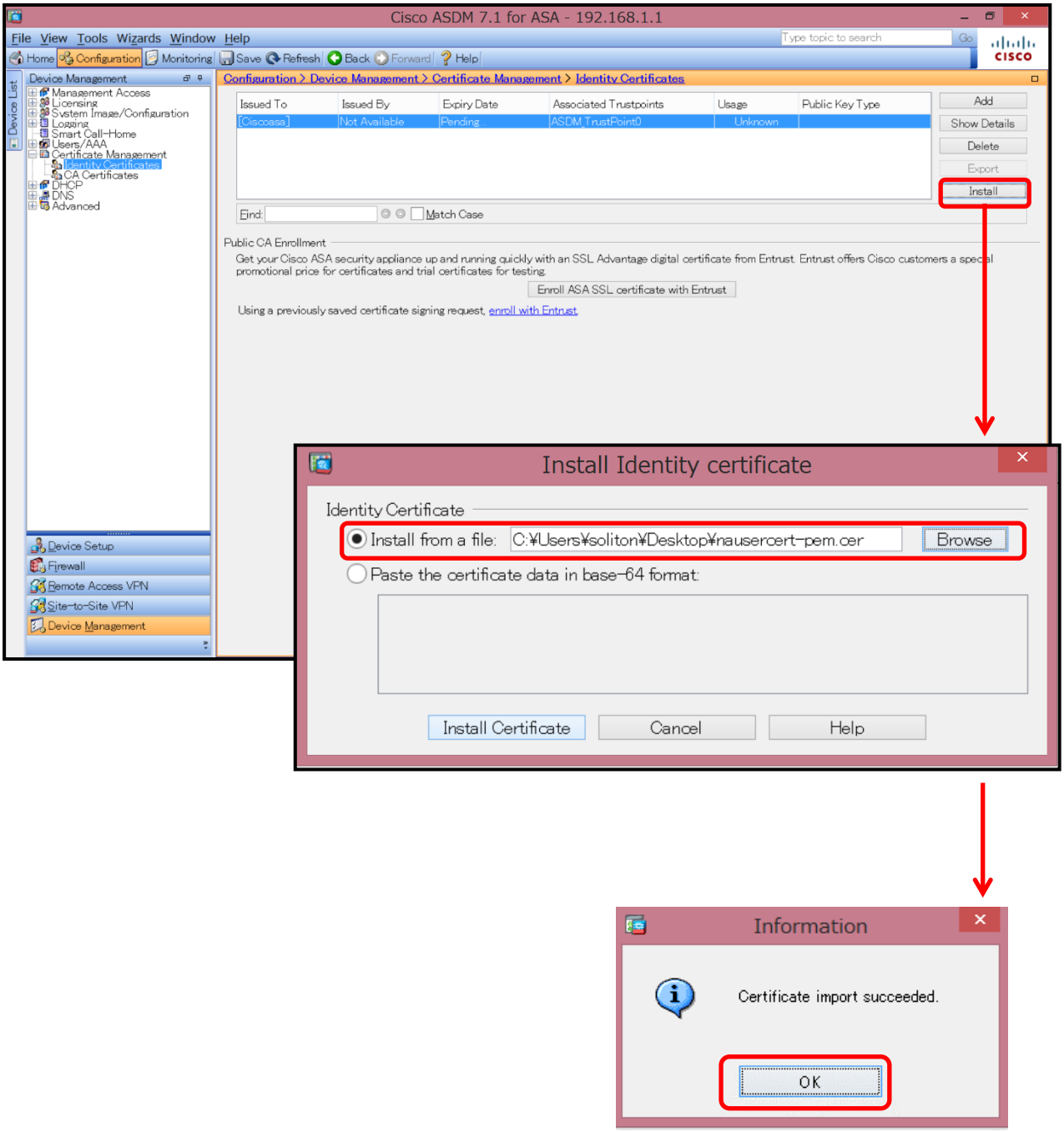
次に、インポートした CA 証明書を選択し、CRL の設定をします。



4-7 サーバー証明書のインポート (ASA 5505)

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 5505 の接続設定

ASA 5505 の接続に関する設定の流れ

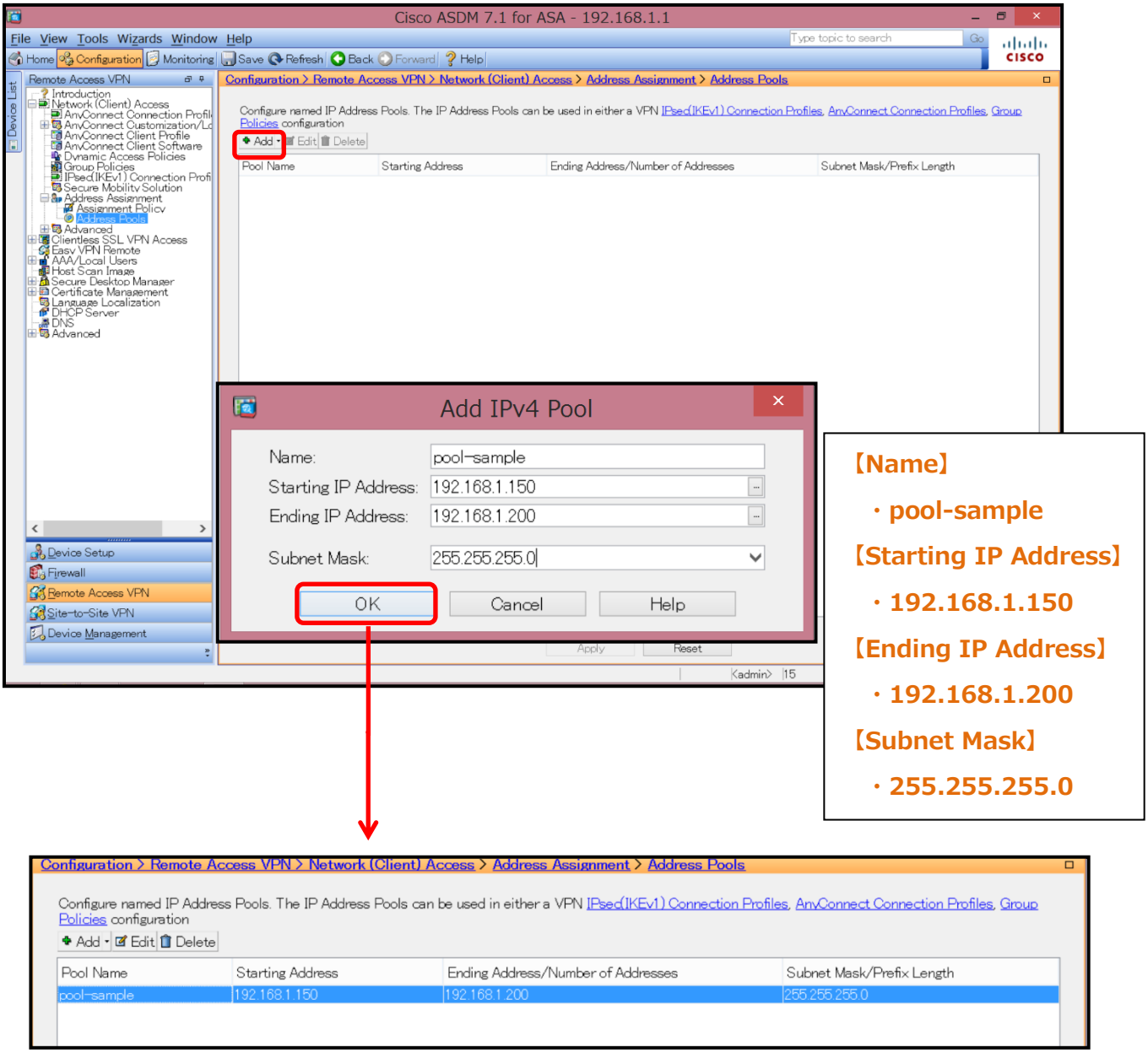
1. IP アドレスプールの設定
2. AAA サーバー(RADIUS サーバー)の設定
3. AnyConnect VPN Connection Setup Wizard

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。

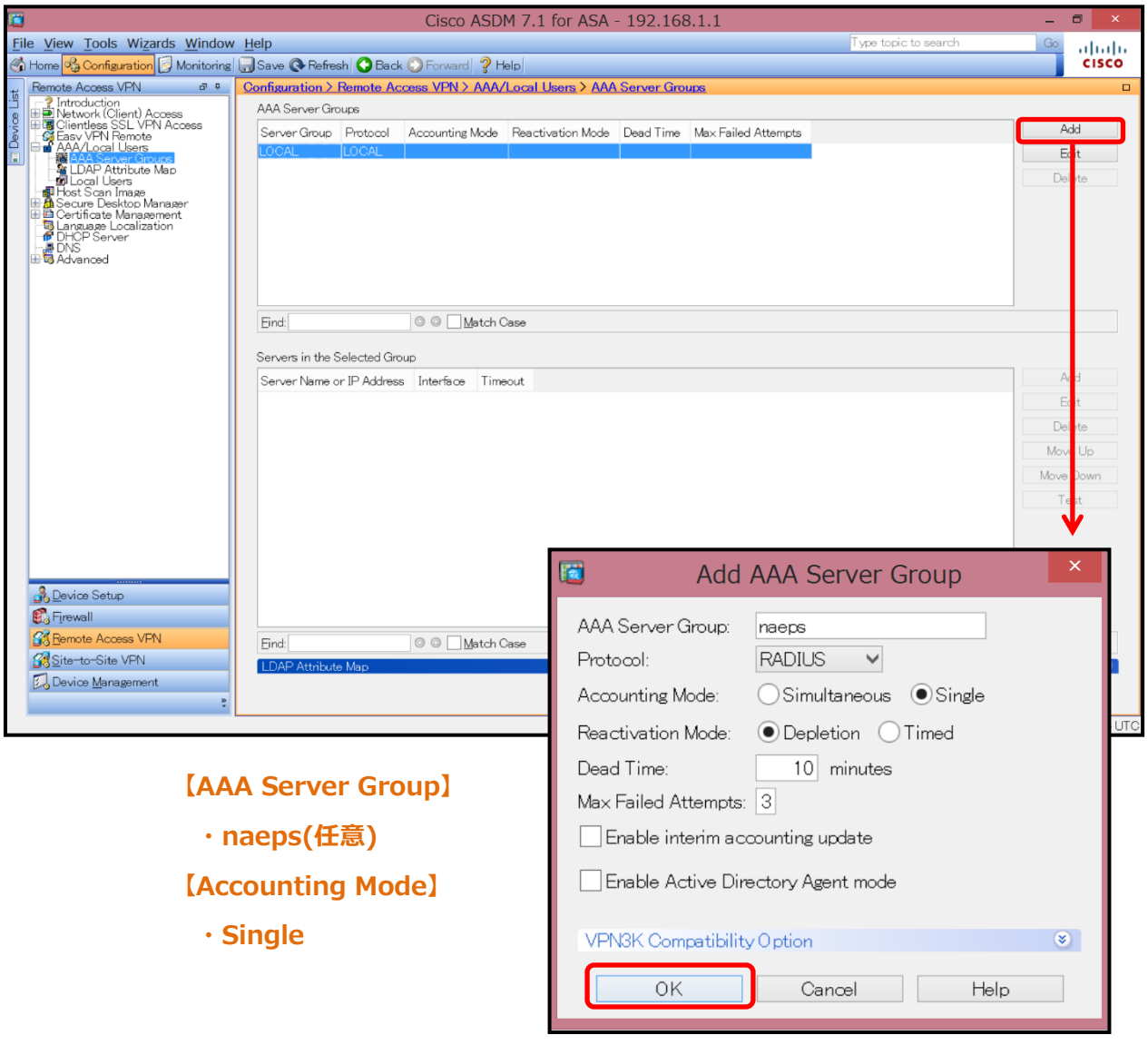
[Add IP Pool]で割り当てる範囲の IP アドレスを指定します。



5-2　AAA サーバー(RADIUS サーバー)の設定

NetAttest EPS に問合わせる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。



【AAA Server Group】

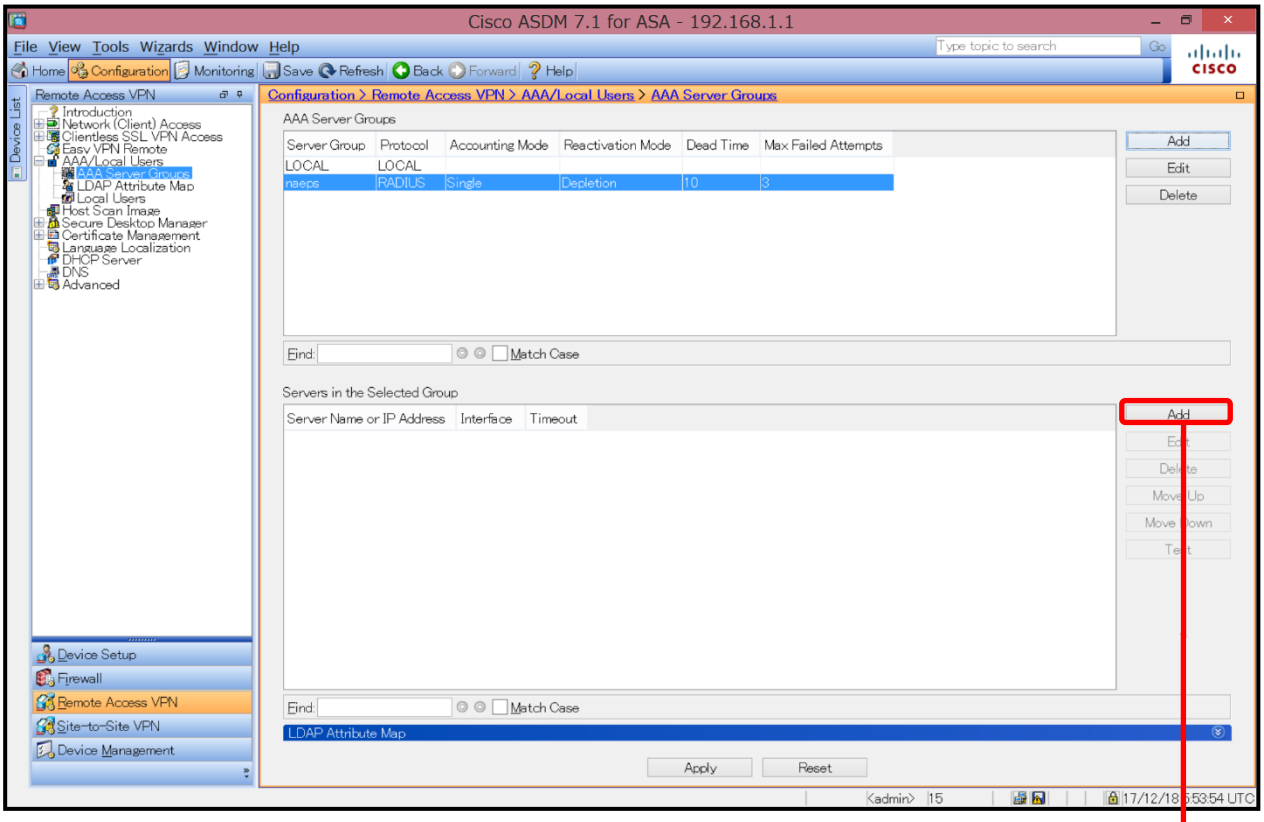
・naeps(任意)

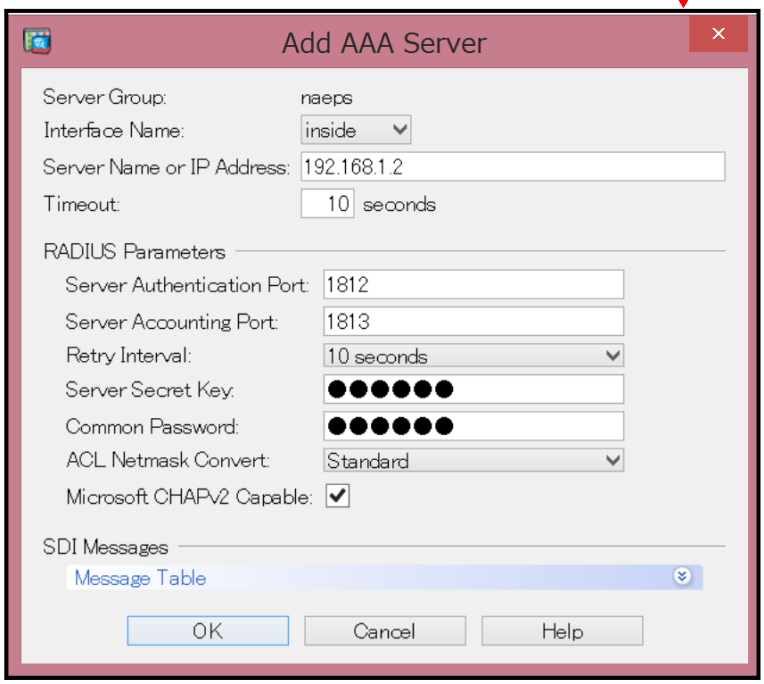
【Accounting Mode】

・Single

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】

・inside

【Server name or IP Address】

・192.168.1.2

【Server Authentication Port】

・1812

【Server Accounting Port】

・1813

【Server Secret Key】

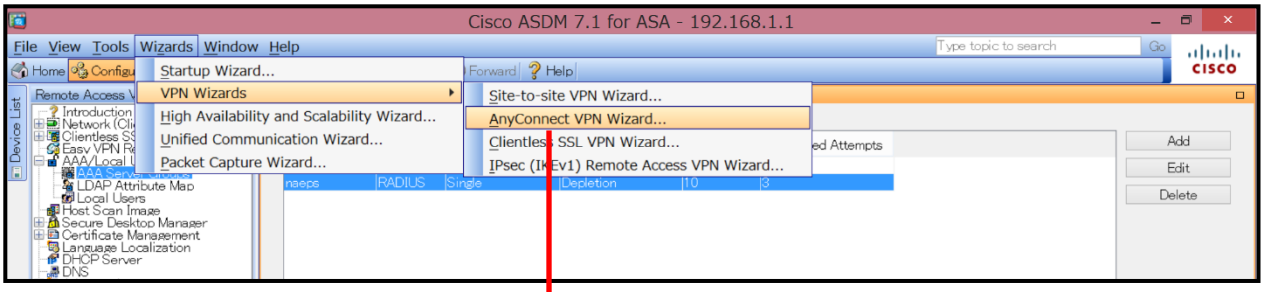
・secret

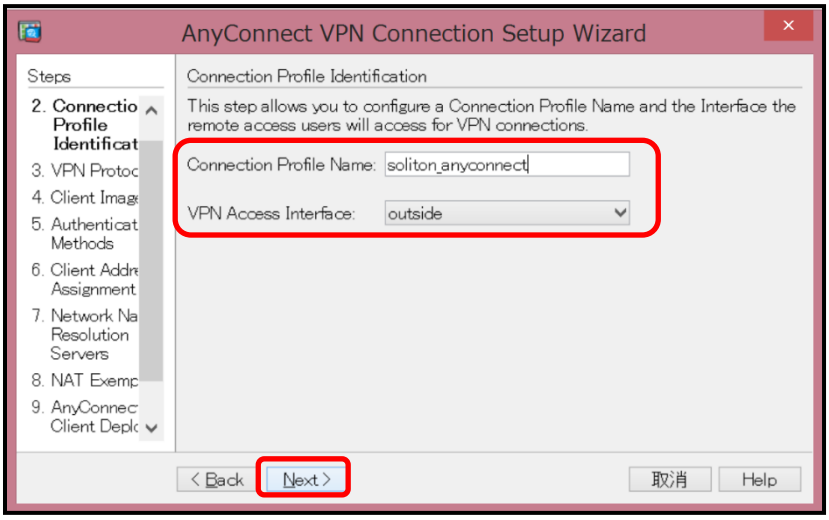
次ページへ

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。



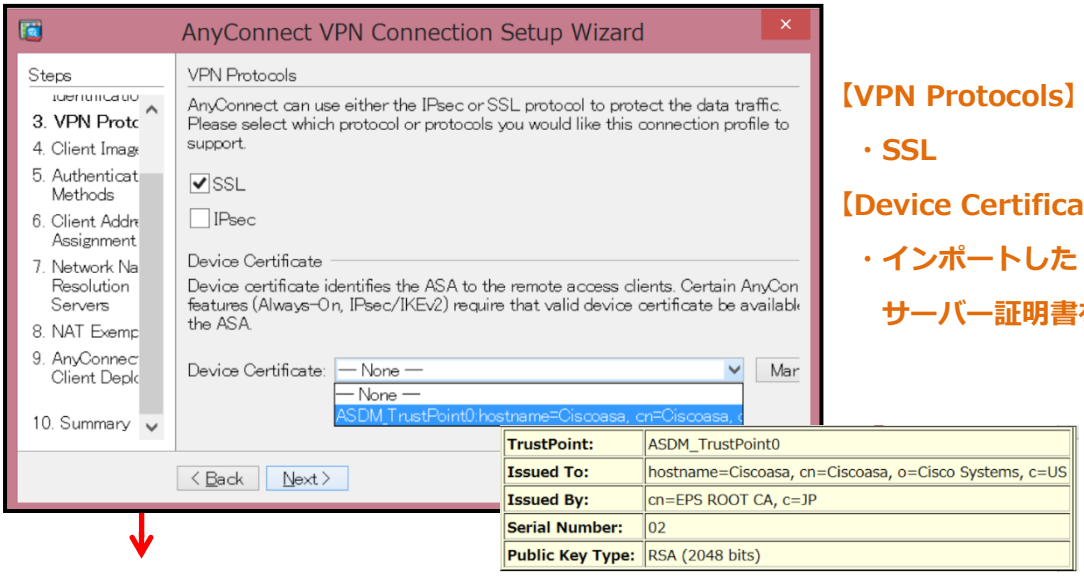


【Connection Profile Name】

・soliton_anyconnect

【VPN Access Interface】

・outside



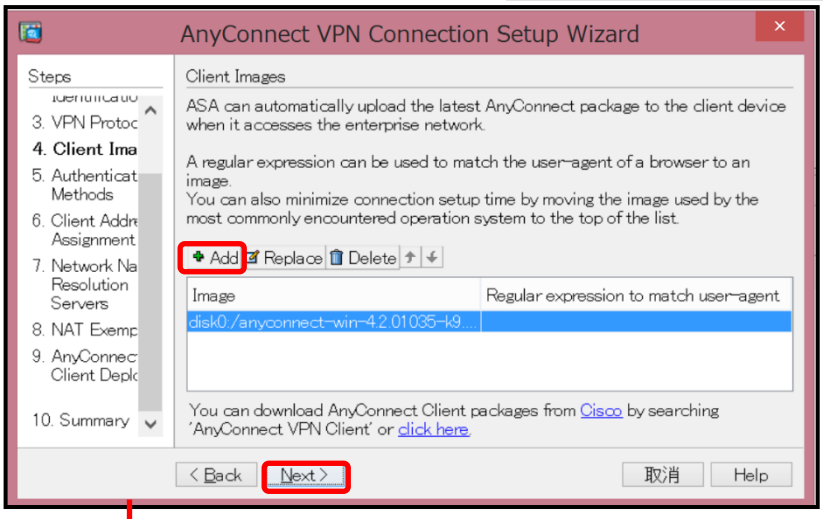
【VPN Protocols】

・SSL

【Device Certificate】

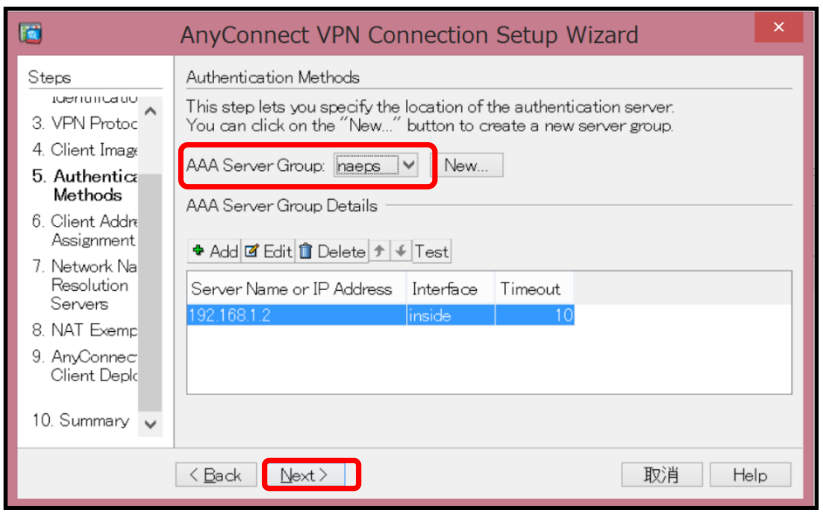
・インポートした

サーバー証明書を選択



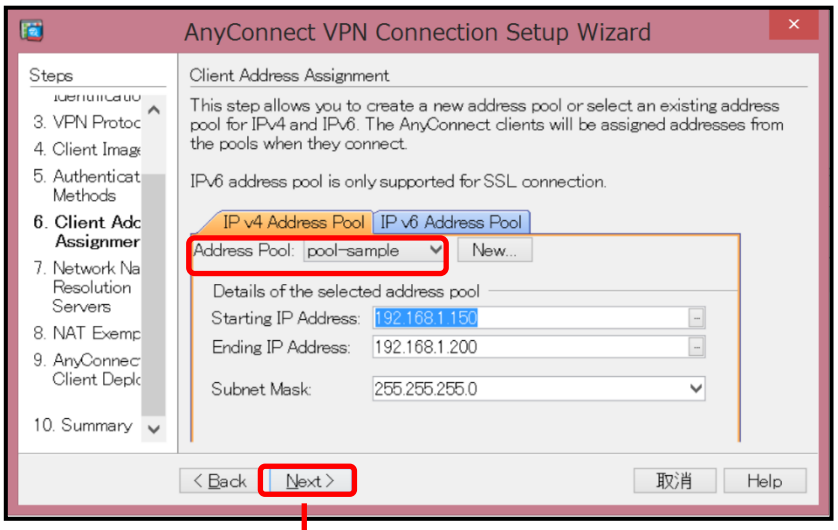
【Add】ボタンから、クライアントイメージ[Any Connect pkg ファイル]を選択

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。



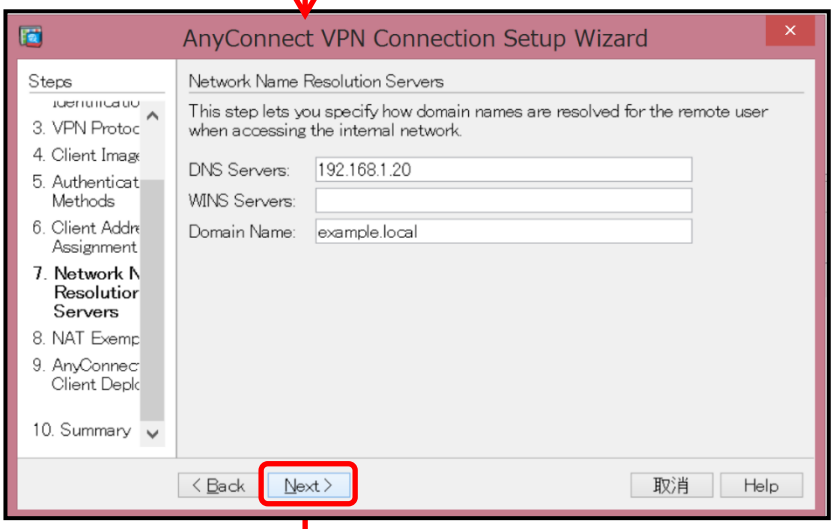
【AAA Server Group】

・作成済みの[naeps]を指定



【IPv4 Address Pool】

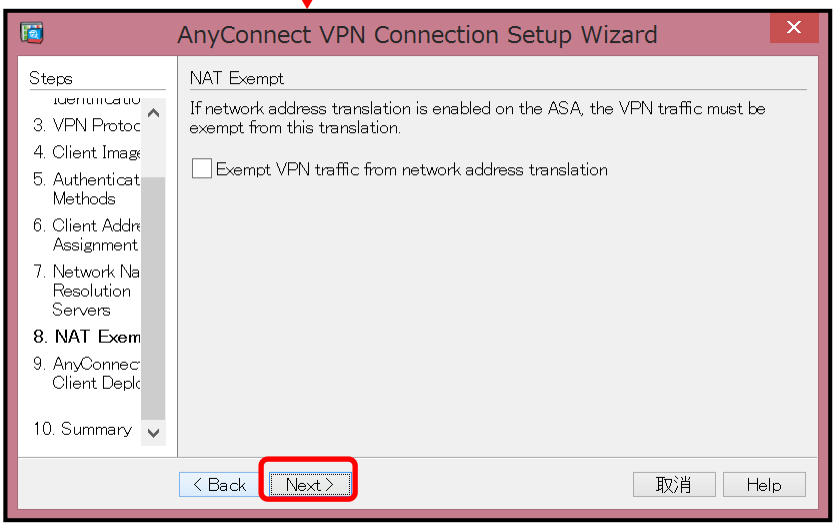
作成済みの IP アドレスプールを指定



【DNS Servers】

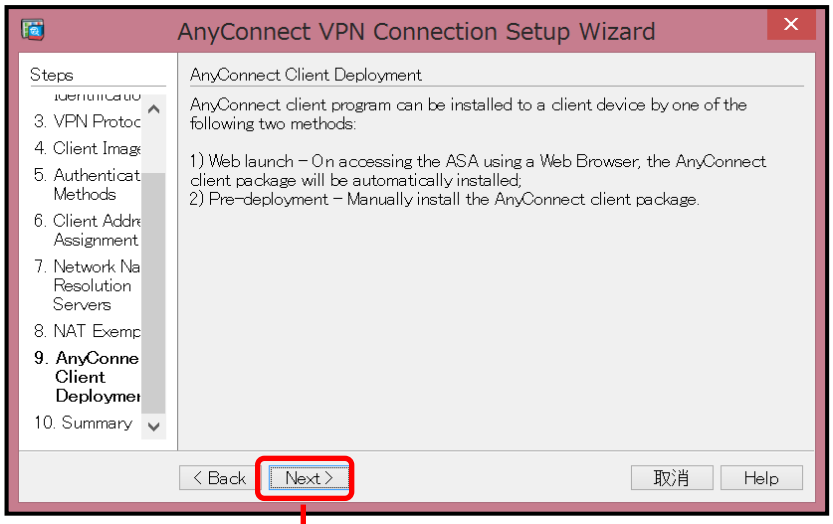
・DNS のアドレスを指定

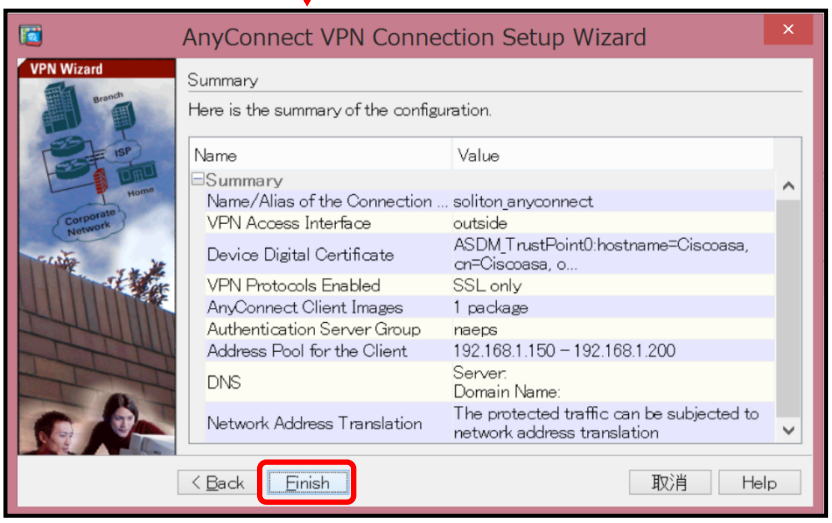
本項目は必須のため、DNSが無い場合でも適当な値を指定してください。



【NAT Exempt】

・チェックなし

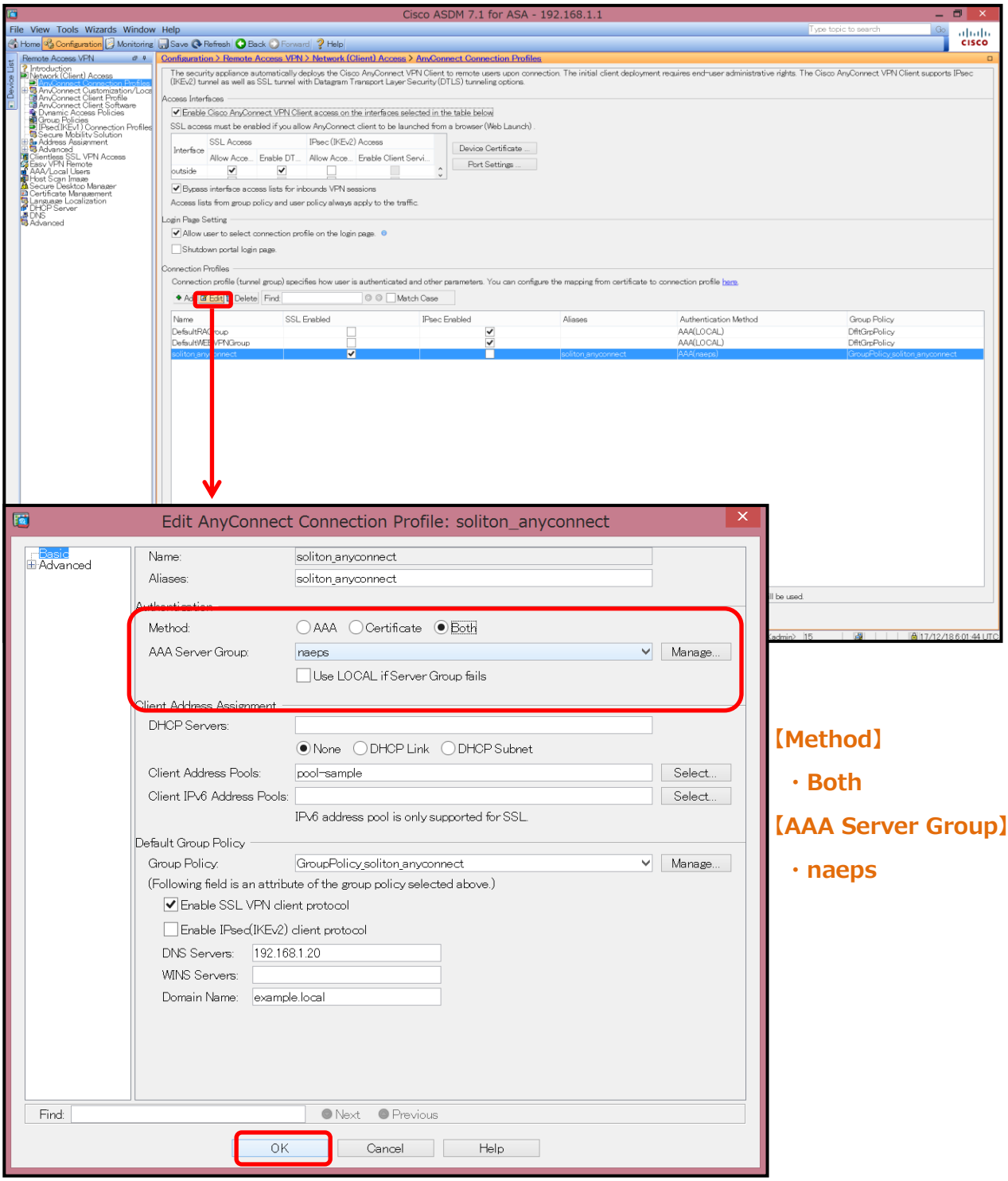

AnyConnect VPN Connection Setup Wizard
Steps
3. VPN Protoc
4. Client Imag
5. Authenticat Methods
6. Client Addr Assignment
7. Network Na Resolution Servers
8. NAT Exemp
9. AnyConne Client Deploymer
10. Summary
AnyConnect Client Deployment
AnyConnect client program can be installed to a client device by one of the following two methods:
1) Web launch – On accessing the ASA using a Web Browser, the AnyConnect client package will be automatically installed;
2) Pre-deployment – Manually install the AnyConnect client package.
< Back
Next >
取消
Help


AnyConnect VPN Connection Setup Wizard
VPN Wizard
Summary
Here is the summary of the configuration.
Name
Value
Summary
Name/Alias of the Connection ...
soliton_anyconnect
VPN Access Interface
outside
Device Digital Certificate
ASDM_TrustPoint0:hostname=Ciscoasa, cn=Ciscoasa, o...
VPN Protocols Enabled
SSL only
AnyConnect Client Images
1 package
Authentication Server Group
naeps
Address Pool for the Client
192.168.1.150 – 192.168.1.200
DNS
Server:
Domain Name:
Network Address Translation
The protected traffic can be subjected to network address translation
< Back
Finish
取消
Help

次ページへ

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。



【Method】

・Both

【AAA Server Group】

・naeps

6　Windows 版 AnyConnect の設定

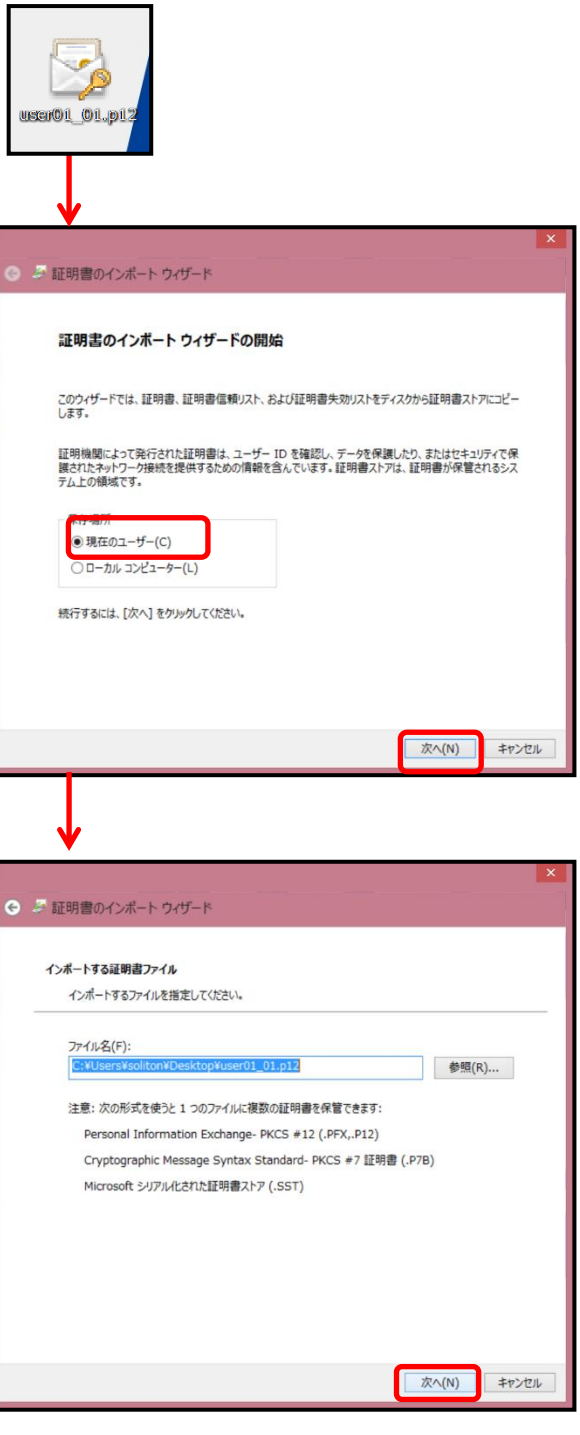
AnyConnect VPN クライアントの設定

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_01.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。



【現在のユーザー】を選択

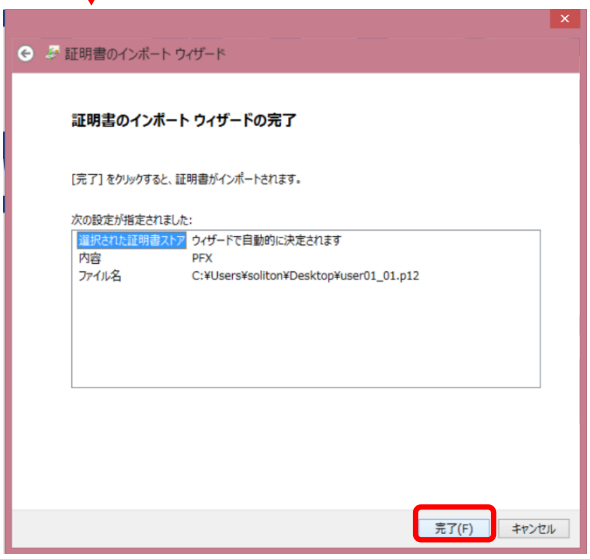
【パスワード】

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

【証明書の種類に基づいて・・・】

・チェック有

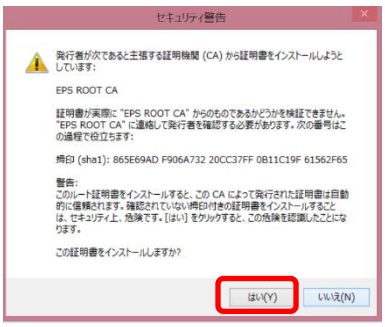


インポートウィザードが完了すると

ユーザー証明書/CA 証明書がユーザーの

PC にインポートされます。

セキュリティ警告画面は【はい】を押下します。

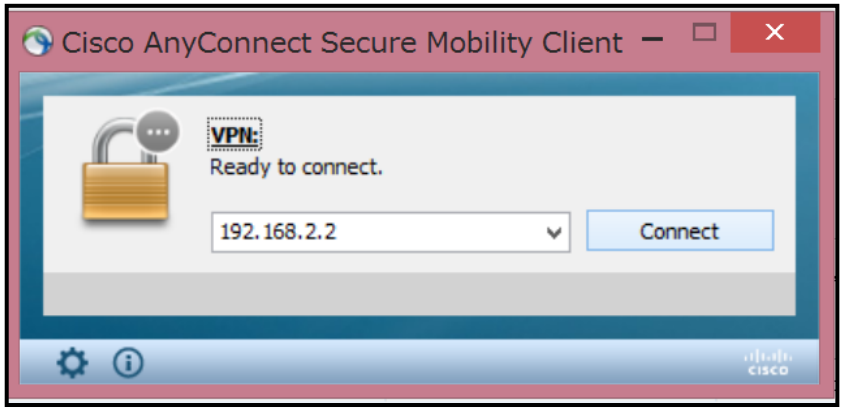


6-2　Windows 版 AnyConnect の設定

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。

AnyConnect のバージョンによって表示される画面構成は異なる場合があります。



7　iOS 版 AnyConnect の設定

AnyConnect VPN クライアントの設定

1. iPhone 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　iPhone への VPN 用デジタル証明書のインストール

NetAttest EPS から発行した VPN 用デジタル証明書を iOS デバイスにインストールする方法として、下記 4 つの方法などがあります。

1)NetAttest EPS-ap を使い、SCEP で取得する方法
2)Apple Configurator2（構成プロファイル）を使う方法
3)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
4)HTTP アクセス可能なサーバーに証明書をアップロードして、インストールする方法

上記いずれかの方法で CA 証明書とユーザー証明書をインストールします。
本手順では証明書のインポート方法については割愛いたします。

iOS 10 以降の OS 仕様上 ROOT 証明書をインポートする場合、
手動でインポートした証明書を信頼させる必要があります。

証明書をメール添付して iOS デバイスに送りインストールする方法は、
Legacy AnyConnect にのみ適用されます。(Legacy AnyConnect は iOS12 以降では利用できません。)
新しい AnyConnect の場合は以下の様な方法があります。

- **Web サーバーに証明書をアップロードし、ダウンロード URL を用いてインポートを行う方法**
- **メール添付等で iOS デバイスに送った証明書を iOS の「システム共有機能」を利用しインポートを行う方法**
- **EPS-ap で証明書配布時に、VPN プロファイルも配布する方法**

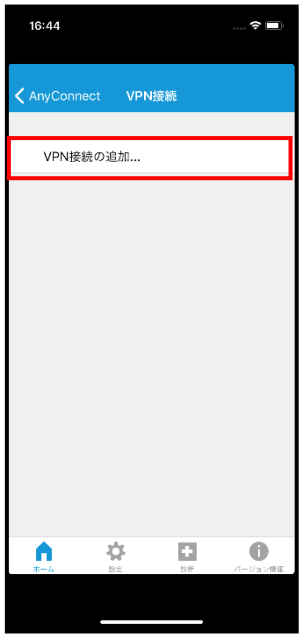
EPS-ap プロファイル管理ページの[プロファイル]-[VPN]-[接続タイプ]

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インポートし、
VPN の設定を行います。
(本手順書は CiscoAnyConnect for iOS V4.0.0 を基準で作成されています。)

7-2-1.AnyConnect VPN の基本設定

1. AnyConnect 起動
【接続】タップ。



2.【VPN 接続の追加】を
タップ。

3.VPN 接続の追加
[説明]
・任意(CiscoASA)
【サーバー】
・ASA のアドレス(192.168.2.2)
【保存】ボタンで設定保存。

8　Android OS 版 AnyConnect の設定

AnyConnect　VPN　クライアントの設定

1. Android 端末への VPN 用デジタル証明書のインストール
2. Android 版 AnyConnect の設定(基本設定、ユーザー証明書インポート)

8-1　Android 端末への VPN 用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 VPN 用ユーザー証明書を Android デバイスにインストールする方法として、下記 3 つの方法などがあります。

1)NetAttest EPS-ap を使い、SCEP で取得する方法
2)デジタル証明書をメールに添付し Android デバイスに送り、インストールする方法
3)HTTP アクセス可能なサーバーに証明書をアップロードして、インストールする方法

上記いずれかの方法で Android OS の「VPN とアプリ」に CA 証明書とユーザー証明書をインストールします。
本手順では証明書のインポート方法については割愛いたします。

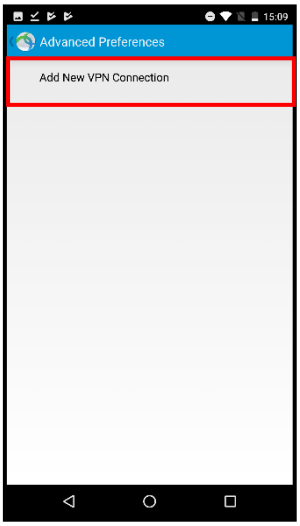
Android 用の AnyConnect アプリの仕様で、ユーザー証明書を Android OS の「VPN とアプリ」にインストール後、AnyConnect 上で別途インポートする必要があります。

8-2　Android OS 版 AnyConnect 設定

Cisco AnyConnect VPN クライアントを Google Play 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インポートし、
VPN 設定を行います。
(本手順書は CiscoAnyConnect for Android V4.0.09039 を基準で作成されています。)

8-2-1. AnyConnect VPN の基本設定

1.AnyConnect を起動。



2.【Add New VPN Connection】をタップ。

3.接続エディタ
[説明]
・CISCO(任意)
[サーバー]
・ASA の IP を入力
【保存】ボタンで設定保存 。

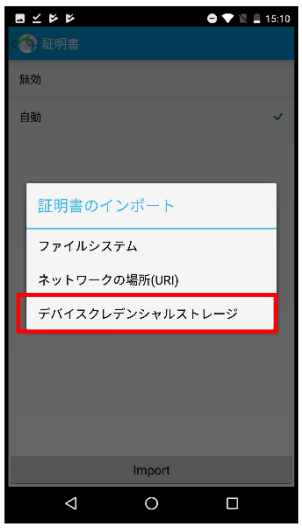
8-2-2 AnyConnect にユーザー証明書のインポート

1. AnyConnect を起動
【接続】をタップ。

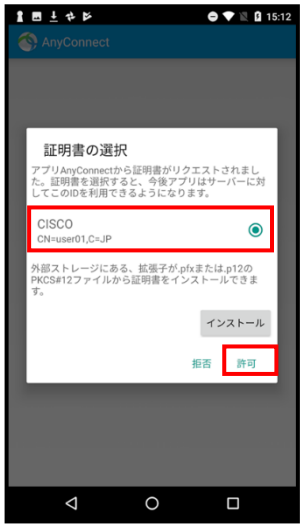
2. 8-2-1 で作成した
【CISCO】を長押しし、
【接続を編集】ボタンを
タップ。

3.【証明書】をタップ。

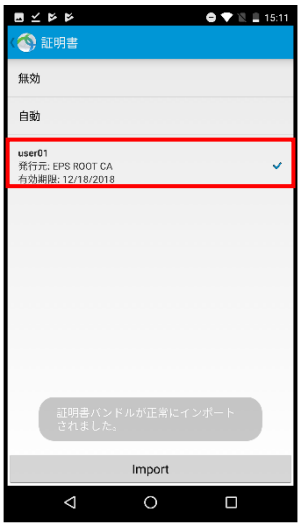
4.下段の【Import】を
タップ。



5.【デバイスクレデンシャル
ストレージ】 をタップ。



6.【証明書の選択】で
8-1 でインストールした
証明書を選択し、
【許可】ボタンをタップ。



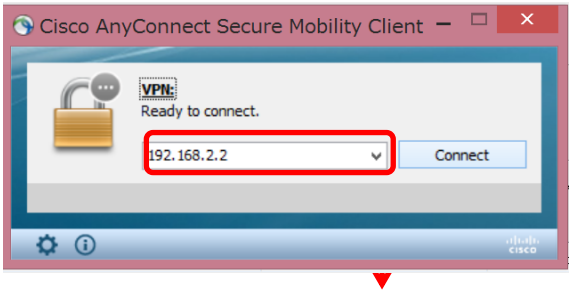
7. AnyConnect にインポートされたユーザー証明書をタップ。

8. 下段の【完了】ボタンをタップし、インポート完了。

9　接続の確認

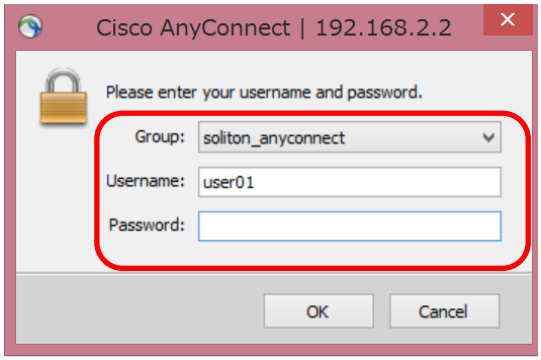
9-1　PC における AnyConnect を利用した SSL-VPN 接続

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

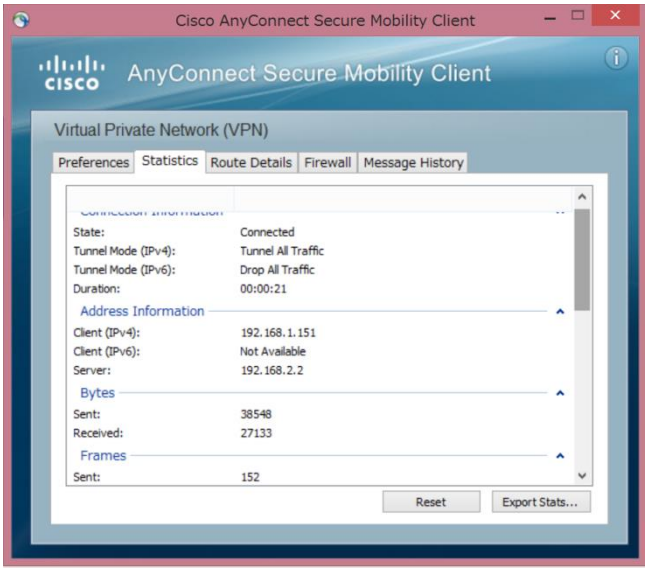
【password】

・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。



9-2　iPhone 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、「接続」で作成済みの接続プロファイルを選択し、「Any Connect VPN」を ON にします。

1. 【接続】
   ・CiscoASA

2. 【Group】
   ・soliton_anyconnect
   【username】
   ・user01
   【password】
   ・password

3. 【詳細】で
   IP 払い出し情報
   確認可能。

9-3　Android 端末で 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、「接続」で作成済みの接続プロファイルを選択し、「Any Connect VPN」を ON にします。

1.【接続】
・Cisco

2.【Group】
・soliton_anyconnect
【username】
・user01
【password】
・password

3.【詳細】で
IP 払い出し情報
確認可能。

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
2018/1/22	1.2	設定内容を ASA 5505 にあわせて更新
2018/10/31	1.3	誤表記修正