

NetAttest EPS 設定例

連携機器：

SonicWALL Aventail 10.5.3

Case：証明書とパスワードによるハイブリッド認証

Version 1.0

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 © 2011, Soliton Systems K.K. , All rights reserved.

はじめに

本書について

本書は CA 内蔵 RADIUS サーバプライアンス NetAttest EPS と SonicWALL 社製 SSL VPN 製品 Aventail 10.5.3 との証明書認証連携について、設定例を示したものです。

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。設定例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として記述します。

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 Aventail 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。

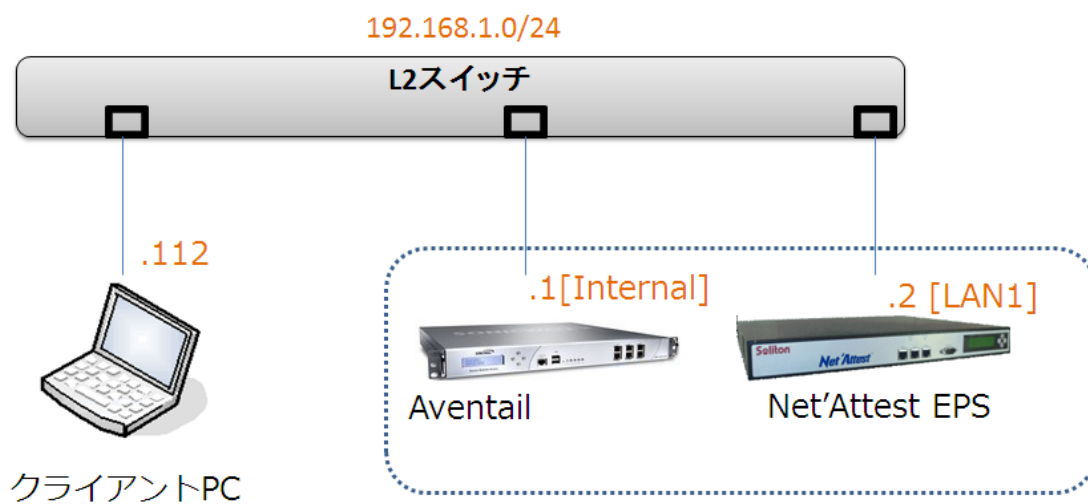
目次

1	構成	7
1-1	構成図	7
1-2	環境	8
2	NetAttest EPS	9
2-1	NetAttest EPS 設定の流れ	9
2-2	システム初期設定ウィザードの実行	10
2-3	サービス初期設定ウィザードの実行	11
2-4	RADIUS クライアントの登録	12
2-5	認証ユーザーの追加登録	13
2-6	ユーザー証明書の発行	14
3	証明書の取得とインポート	15
3-1	操作の流れ	15
3-2	CA 証明書のインポート (Aventail)	16
3-3	CSR の生成 (Aventail)	18
3-4	仮クライアント証明書のインストール (NetAttest EPS)	20
3-5	サーバー証明書署名要求の受付 (NetAttest EPS)	21
3-6	サーバー証明書の発行 (NetAttest EPS)	23
3-7	サーバー証明書のダウンロード (NetAttest EPS)	24
3-8	サーバー証明書のインポート (Aventail)	25
3-9	証明書の選択 (Aventail)	27
4	Aventail の認証設定	29
4-1	Aventail の認証設定の流れ	29
4-2	認証サーバーの設定(RADIUS)	30
4-3	認証サーバーの設定(PKI)	31
4-4	Realm の追加	33
5	クライアント PC の設定	35
5-1	クライアント PC 設定の流れ	35
5-2	証明書のインポート	36
5-3	認証の確認	39

1 構成

1-1 構成図

- ・有線LANで接続する機器はすべて、L2スイッチに収容



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 ST-03	Ver. 4.2.0
RADIUS クライアント (SSL VPN 機器)	SonicWALL	Aventail	Ver.10.5.3
Client PC	Lenovo	ThinkPad X200	Windows XP SP3

1-2-2 認証方式

PKI 認証+ID/Password

1-2-3 ネットワーク設定

	EPS-ST03	Aventail	Client PC
IP アドレス	192.168.1.2/24	192.168.1.1/24	192.168.1.112/24 (DHCP)
RADIUS port (Authentication)	TCP 1645※		—
RADIUS port (Accounting)	TCP 1813		—
RADIUS Secret (Key)	Password		—

※Aventail の RADIUS port(Authentication)はデフォルトで TCP 1645 を利用

2 NetAttest EPS

2-1 NetAttest EPS設定の流れ

設定の流れ

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. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. ユーザー証明書の発行

2-2 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

The screenshot shows the initial setup wizard interface. The main window displays the following options:

- 初期設定ウィザード
 - システム初期設定
 - サービス初期設定
- システム管理ページへ
- CA管理ページへ
- V3.x 設定 / データのリ

The confirmation dialog box, titled '初期設定ウィザード - 設定項目の確認', displays the following settings:

ホスト名	naeps.snwl.jp
サービスインターフェイス	
IPアドレス	192.168.1.2
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	
管理インターフェイス	
IPアドレス	192.168.2.1
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	
同期通信インターフェイス	
IPアドレス	192.168.3.1
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	
ドメインネームサーバー1	
ドメインネームサーバー2	

設定内容を確認して下さい。
この設定を保存・反映するには「再起動」ボタンをクリックして下さい。

Copyright © 2004-2010, Soliton Systems K.K., All rights reserved.

2-3 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。

本書では、黒文字の項目のみ、設定しました。

- ◆ 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

The image displays three overlapping screenshots of the Soliton service initial setup wizard. The background window is titled "初期設定ウィザード - CA構築" (Initial Setup Wizard - CA Construction). The top-right window is titled "初期設定ウィザード - LDAPデータベースの設定" (Initial Setup Wizard - LDAP Database Settings). The bottom-right window is titled "初期設定ウィザード - RADIUSサーバーの基本設定" (Initial Setup Wizard - RADIUS Server Basic Settings).

初期設定ウィザード - CA構築

CA種別選択	ルートCA
CA秘密鍵生成	
公開鍵方式	RSA
鍵長	2048
CA情報	
CA名(必須)	na-labo CA01
国名	日本
都道府県名	Tokyo
市区町村名	Shinjuku
会社名(組織名)	Soliton Systems K.K.
部署名	Mktg
E-mailアドレス	na-admin@na-labo.soliton
CA署名設定	
ダイジェストアルゴリズム	SHA1
有効日数	3650

Copyright © 2004-2010, Soliton Systems K.K., All rights reserved.

初期設定ウィザード - LDAPデータベースの設定

編集対象:	新規
名前*	LocalLdap01
サフィックス*	dc=na-labo,dc=soliton,dc=jp
説明	

戻る 次へ

初期設定ウィザード - RADIUSサーバーの基本設定

全般

認証ポート*	1645
アカウントングポート*	1813
<input type="checkbox"/> ログにパスワードを表示する(PAP認証のみ)	
<input type="checkbox"/> セッション管理を使用する	
<input checked="" type="checkbox"/> 冗長構成時、アカウントングパケットをパートナーに転送する	

2-4 RADIUSクライアントの登録

WebGUI より、RADIUS クライアントの登録を行います。

「RADIUS サーバー設定」 → 「NAS/RADIUS クライアント追加」 から、RADIUS クライアントの追加を行います。

The screenshot shows the Net Attest EPS WebGUI interface. The main window displays a table for NAS/RADIUS clients. An inset window shows the configuration form for a new client named 'TEST' with IP address 192.168.1.1 and password 'password'.

【NAS/RADIUS クライアント名】

- ・ TEST

【IP アドレス(Authenticator)】

- ・ 192.168.1.1

【シークレット】

- ・ password

2-5 認証ユーザーの追加登録

WebGUI 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始めます。

The screenshots illustrate the steps to add a new user:

- Access the 'ユーザー一覧' (User List) page and click the '追加' (Add) button.
- Fill out the 'ユーザー設定' (User Settings) form with the following details:
 - 姓 (Surname): ソリトン (Soliton)
 - 名 (Name): 一郎 (Ichiro)
 - E-Mail: [Empty]
 - 詳細情報 (Detailed Information): [Empty]
 - 認証情報 (Authentication Information):
 - ユーザーID (User ID): soliton_user
 - パスワード (Password): [Masked]
 - パスワード(確認) (Password Confirmation): [Masked]
 - 一時利用停止 (Temporary Suspension): [Unchecked]
 - グループ情報 (Group Information): [Empty]
- Click the 'OK' button to save the user.
- The user is added to the 'ユーザー一覧' table:

名前	ユーザーID	証明書	タスク
ソリトン 一郎	soliton_user	発行	変更 削除

2-6 ユーザー証明書の発行

WebGUI より、ユーザー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「証明書」の欄の『発行』ボタンでユーザー証明書の発行を始めます。



【証明書有効期限】

- ・ 365

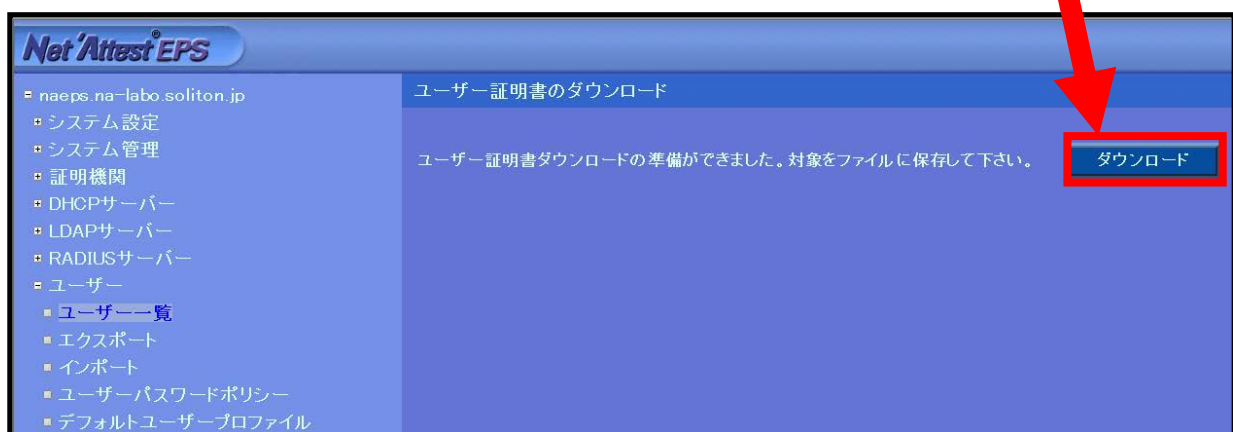
【証明書ファイルオプションパスワード】

- ・ password

【PKCS#12 ファイルに証明機関の・・・】

- ・ チェック有

The screenshot shows the '基本情報' (Basic Information) form for issuing a certificate. The '有効期限' (Validity Period) is set to 365 days. The '証明書ファイルオプション' (Certificate File Options) section is highlighted with an orange box, showing the password field and the checked option for PKCS#12 files. The '発行' (Issue) button is highlighted with a red box and a red arrow.



3 証明書の取得とインポート

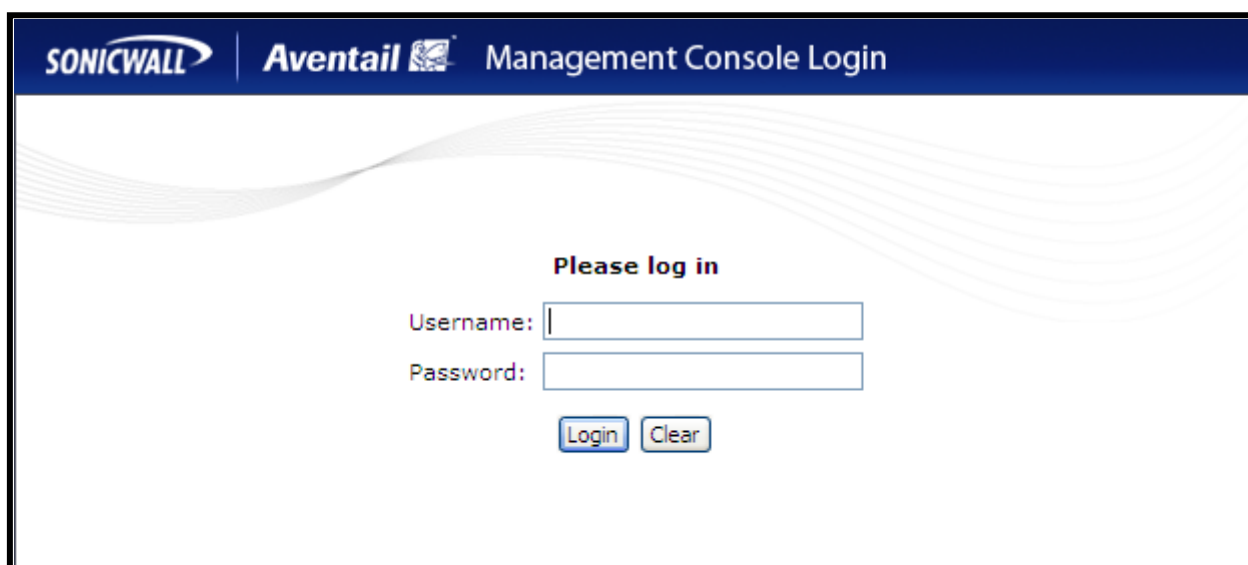
3-1 操作の流れ

操作の流れ

1. CA 証明書のインポート (Aventail)
2. CSR の生成 (Aventail)
3. 仮クライアント証明書のインストール (NetAttest EPS)
4. サーバー証明書署名要求の受付 (NetAttest EPS)
5. サーバー証明書の発行 (NetAttest EPS)
6. サーバー証明書のダウンロード (NetAttest EPS)
7. サーバー証明書のインポート (Aventail)
8. 証明書の選択 (Aventail)

3-2 CA証明書のインポート (Aventail)

SonicWALL 社製 SSL VPN Aventail を設定するためには、管理 WebGUI を利用する方法があります。本書では、管理 WebGUI から各種設定を実施する方法を紹介します。NetAttest EPS でダウンロードした CA 証明書 `nacacert-pem.cer` のインポートを行います。Aventail Management Console にログインします。



SONICWALL | **Aventail** Management Console

Security Administration
 Access Control
 Resources
 Users & Groups

User Access
 Realms
 Aventail WorkPlace
 Agent Configuration
 End Point Control

System Configuration
 General Settings
 Network Settings
 SSL Settings
 Authentication Servers
 Services
 Virtual Assist
 Maintenance

Monitoring
 User Sessions
 System Status
 Logging
 Troubleshooting

AMC Home
 Use the Aventail Management Console (AMC) to manage your Aventail SSL VPN appliance. Click the links at the left to manage your security policy, configure the system, monitor the appliance, and deploy secure access to your users.

System Status Auto-refresh:

50 Users
 2% of 19.35 GB
 0 %
 Disk space CPU usage

Active users
 1.00 Mbps
 Network bandwidth (internal/external)
 Details | View logs

Appliance name
 avtl
Last reboot
 3 days 22 hrs 16 mins 18 secs
System time
 Fri Jul 15 2011 14:23:00 JST

Services Status
 Network tunnel
 Web proxy
 Aventail WorkPlace

Log in to Aventail WorkPlace
 Click the following link(s) to log in to WorkPlace and test user access.
[Default WorkPlace site](#)
[WorkPlace for SBB](#)

Technical Resources
[Online Help](#)
[mySonicWALL.com](#)

S/N: 00401023ECD3
 Version: 10.5.3-052
 © 2010 SonicWALL, Inc.

SSL Settings から CA certificates の Edit を選択します。

New を選択し、Certificate file の参照で NetAttest EPS でダウンロードした CA 証明書 nacacert-pem.cer を選択し、Import ボタンを押すと追加されます。

The screenshot displays the SonicWall Management Console interface. On the left, the 'SSL Settings' menu item is highlighted with a red box. The main content area shows the 'SSL Settings' page with a list of certificates. The 'CA Certificates' section is expanded, and the 'New' button is circled in red. A red arrow points from the 'New' button to the 'Import CA Certificate' dialog box. In this dialog, the 'Certificate file' option is selected, and the file path 'C:\Documents and Settings\... \nacacert-pem.cer' is entered. A file icon next to the path is circled in orange. At the bottom of the dialog, the 'Import' button is circled in orange. The 'Usage' section shows three checked options: 'Authentication server connections (LDAPS)', 'Web server connections (HTTPS)', and 'Device profiling (End Point Control)'.

3-3 CSRの生成 (Aventail)

次に CSR(Certificate Signing Request)の生成を行います。

SSL Settings から SSL certificates の Edit を選択します。

Certificate Signing Requests の New をクリック後、必須項目を埋めて Save を選択します。

SSL Settings

SSL certificates

- Main appliance certificate** (WorkPlace and other access methods) [Edit](#)
- 192.168.10.41 (self-signed)
- Valid through: 13 7 2016
- Management console certificate (AMC)**
- 192.168.0.10 (self-signed)
- Valid through: 13 7 2016
- Virtual hosting certificate** (WorkPlace sites and URL resources)
- N/A

SSL Certificates

General | **Certificate signing requests**

Manage SSL server certificates used to access resources

Certificate signing requests

[New](#) [Delete](#)

Issued to

Create Certificate Signing Request

Create a CSR for use in obtaining an SSL certificate from a commercial CA.

Certificate information

The information below will be stored in the CSR and used in your SSL certificate.

Fully qualified domain name: *
snwl.jp

Organization: *
SonicWALL.inc

State: *
Tokyo

Country: *
JP

Key length:
2048 bits

[Save](#) [Cancel](#)

[Fully qualified domain name]

• snwl.jp

[Organization]

• SonicWALL.inc

[State]

• Tokyo

[Country]

• JP

CSR が生成されるのですべての文字列をコピーし OK を選択します。
コピーした CSR をテキストに貼りつけ、テキストファイルにします。

Certificate Signing Request [SSL Certificates > Certificate Signing Request](#)

Your CSR was successfully created. The information contained in the CSR is:

Host name:	snwl.jp
Created:	Fri Jul 15 15:55:34 JST 2011
Organization unit:	Unknown
Organization:	SonicWALL.inc
Locale:	Unknown
State:	Tokyo
Country:	JP
Key length:	2048

Send the following CSR to your commercial CA. This is usually done by copying it and pasting it into a form on the CA's web site. See the Help for other options.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICjDCCAXQCAQAwRzELMAkGA1UEBhMC51AxDAjAMBgNVBAGTBVRva31vMRwYFAyDVQKKEw1Tb25p
Y1dBTEwuaW5jMRAwDgYDVQQGEwdzbnN5LmpwMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKc
AQEApQpxkULoEps+J4xzV2CSqJ9+Fh0rbk+hVAO11CmHqMKp44T00cTBdECvkPENIMP/2S6smFzD
XmHkPOY1KJjkF1z9GSRkBVowZSMz077j4az7Pgs96504ipsC4Zi20ueXYeZpNjRabLx3vxz+4wJM
YFR1thpp5p7LcH6UM1fPh/c6S8FmOars8/9xG4JPT7uzxy60bBI2jmc/SPr6pBarhok15m1VBanL
TzhiDnL061Hzmf+hX0uo335F620rUK6pb0p7xerUZc4Ti5K/nSL6LwnvdxftbXubf8sQ7OxdU7XE
PJUqFVCHI9POJxJ1y4Qw6UyRAX2+NvPXH0dkCsF+NQIDAQAB0AAwDQYJKoZIhvcNAQEEBQADggEB
AAVxmBMCbusiahI3iAFmjYtncGg6QXY6qzwmKU5A1t+t95+Q2qs0oC22FMkwIjhiVj2Wr9ww601+
wZ4dNAkQNJfbUweu27oXCF4Ob45tzIqOLwo30P42z7DpGQ5P+KFIEvcDG12go4/aHpxAZHF6i8N9
VgoFkwCPGma7012Ymvxf1BACV++6I7RPs0q0IL2p6fDVHZWN1gaBrceEnHDPp38Ts0KK3RLNmtmm
```

3-4 仮クライアント証明書のインストール (NetAttest EPS)

NetAttest EPS の管理者向け証明書サービスページにアクセスします。

管理者向け証明書サービスページの URL は「http://192.168.2.1/certsrva/」です。

証明書要求を選択し、要求の作成画面で OK を押します。

その後、証明書が発行されるのでインストールを選択します。

The image displays three sequential screenshots of the NetAttest EPS web interface, illustrating the process of installing a temporary client certificate. Red arrows and boxes highlight key elements in each step.

- Top Screenshot:** The left sidebar menu has '証明書要求' (Certificate Request) highlighted with a red box. The main content area is titled '要求の作成' (Request Creation) and shows a form for '仮クライアント証明書' (Temporary Client Certificate). Fields include '名前(必須)' (Name, required) with 'NacaCertRequester', '国名' (Country) with '指定しない' (None), and others. An 'インストール' (Install) button is visible at the bottom.
- Middle Screenshot:** The '証明書インストール' (Certificate Install) screen is shown. A message states '証明書が発行されました。' (Certificate issued). The 'インストール' (Install) button is highlighted with a red circle. A red arrow points from this button to the 'インストール' button in the next screenshot.
- Bottom Screenshot:** The '証明書インストール' (Certificate Install) screen is shown again. A 'VBScript' dialog box is displayed, indicating '正常にインストールされました。' (Installed successfully). The dialog box has an 'OK' button, which is highlighted with a red box. A red arrow points from the 'インストール' button in the previous screenshot to this dialog box.

3-5 サーバー証明書署名要求の受付 (NetAttest EPS)

有効なデジタル証明書を選択します。

Aventail で発行したデジタル証明書を選択し、OK を押します。

証明書要求—プロファイルの選択画面で WEB サーバー証明書を選択します。

The screenshot displays the '証明書インストール' (Certificate Install) window for 'naeps.snwl.jp'. The left sidebar contains a menu with '証明書要求' (Certificate Request) selected. The main area contains the instruction: 'こちらをクリックして再度アクセスし、有効なデジタル証明書を選択してください。' (Click here to re-access and select a valid digital certificate). A red arrow points from this instruction to the 'デジタル証明書の選択' (Select Digital Certificate) dialog box. This dialog box shows a table with one entry: 'NacaCertRequester' (Name) and 'SonicWALL, Inc.' (Issuer). The 'OK' button is circled in red. A second red arrow points from the 'OK' button to the '証明書要求—プロファイルの選択' (Select Certificate Request Profile) dialog box. This dialog box lists various certificate request profiles that can be created on the PC, with 'WEBサーバー証明書' (Web Server Certificate) circled in red. At the bottom of this dialog box, there is a link for '既存証明書の更新を要求する' (Request update of existing certificates).

証明書インストール

こちらをクリックして再度アクセスし、有効なデジタル証明書を選択してください。

デジタル証明書の選択

名前	発行者
NacaCertRequester	SonicWALL, Inc.

OK

証明書要求—プロファイルの選択

このPCでは、以下の証明書要求を作成できます。

- CA証明書
- クライアント証明書
- 電子メール保護証明書
- IPsec証明書
- スマートカードログオン証明書
- コード署名証明書
- WEBサーバー証明書
- ドメインコントローラ証明書
- カスタム証明書
- SCEPカスタム証明書

既存証明書の更新を要求する

要求の作成画面の PKCS#10 ファイルによる証明書要求を選択します。

次に参照から Aventail から生成された CSR を貼りつけたテキストファイルを選択します。

要求の作成

WEBサーバー証明書

名前(必須)

国名 指定しない

都道府県名

市区町村名

会社名(組織名)

部署名

E-mailアドレス

プリンシパル名

詳細オプションの設定

PKCS#10ファイルによる証明書要求

要求の作成

WEBサーバー証明書

名前(必須)

国名 指定しない

都道府県名

市区町村名

会社名(組織名)

部署名

E-mailアドレス

プリンシパル名

参照

C:\Documents and Settings\sawano\Desktop\SonicWA

OK キャンセル

要求の作成

実行ステータス

正常終了しました。

要求を受け付けました。

OK

3-6 サーバー証明書の発行 (NetAttest EPS)

CA 管理ページにアクセスします。

CA 管理ページの URL は「http://192.168.2.1:2181/caadmin/」です。

要求管理を選択すると、先程ユーザー向け証明書サービスページから要求された WEB サーバー証明書が表示されているので、選択にチェックを入れ発行を選択します。

NetAttest EPS

要求リスト

表示: 状態 **保留のみ表示** 詳細オプションの設定 **更新**

選択	状態	受付日時	送信元	プロファイル	証明書目的	申請者
<input checked="" type="checkbox"/>	保留	2011/07/15 16:08:16	CAadm.admin Serial:06 Cn:NacaCertRequester	WEBサーバー証明 (unknown)		CN=snwl.jp,O=SonicWALL,inc,ST 確認

拒否 削除 発行: 有効日数 **デフォルト** **発行**

Copyright © 2004-2010, Soliton Systems K.K., All rights reserved.

要求リスト

実行ステータス

正常終了しました。

1件の要求の発行を開始しました。
しばらく待ってからOKボタンをクリックして下さい。

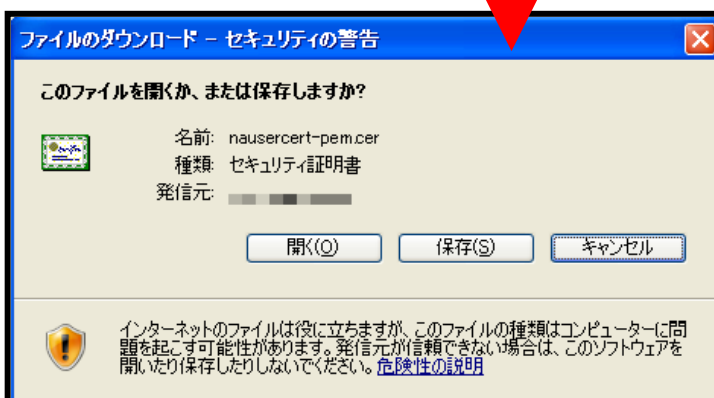
OK

3-7 サーバー証明書のダウンロード (NetAttest EPS)

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。

管理者向け証明書サービスページの URL は「http://192.168.2.1/certsrva/」です。

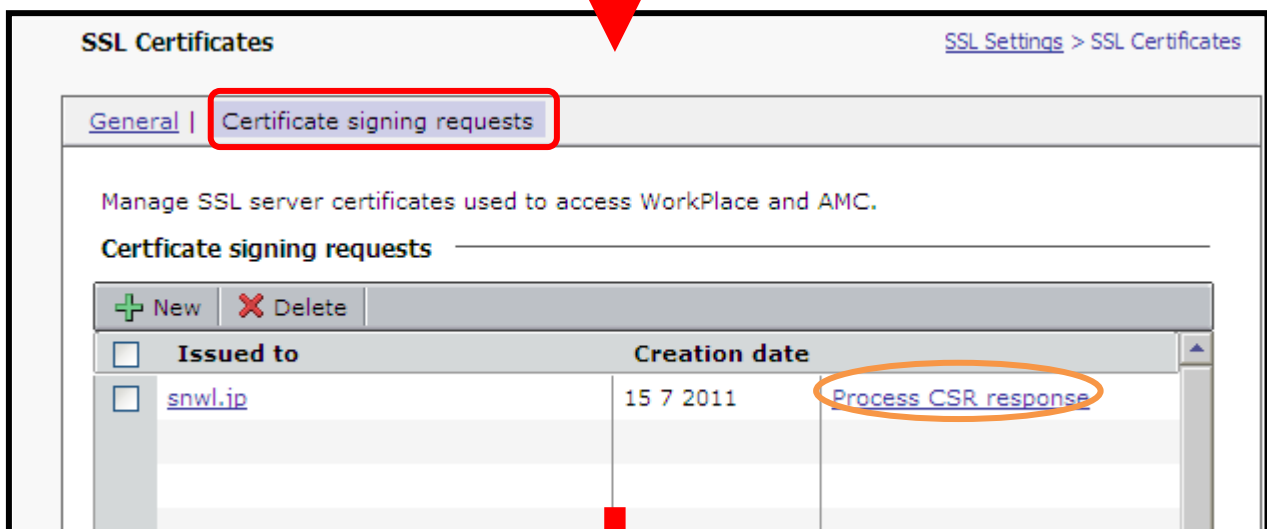
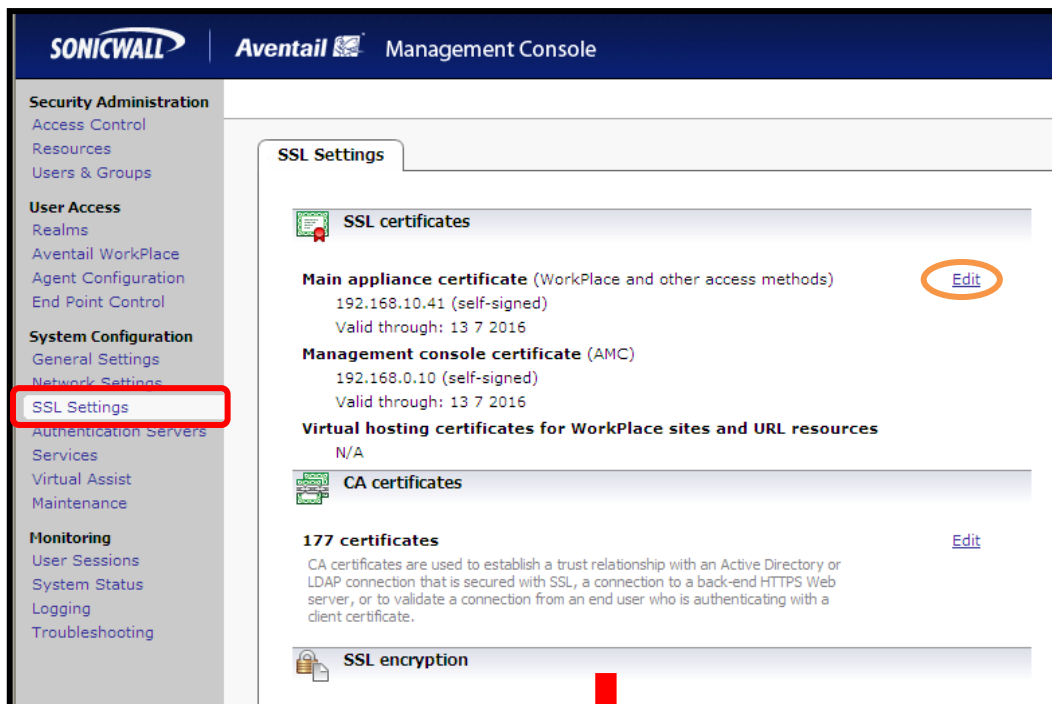
証明書の確認を選択すると状態が発行になっていますので、インストールを選択します。



3-8 サーバー証明書のインポート (Aventail)

Aventail Management Console にログインします。

SSL Settings から Edit→Certificate Signing Requests を選択し、その中の「snwl.jp」の Process CSR response を選択します。



次ページへ

参照ボタンから NetAttest EPS からダウンロードしたサーバー証明書を選択し、Save を選択します。これでサーバー証明書のインポートは完了です。

Import CSR Certificate

[SSL Certificates](#) > Import CSR Certificate

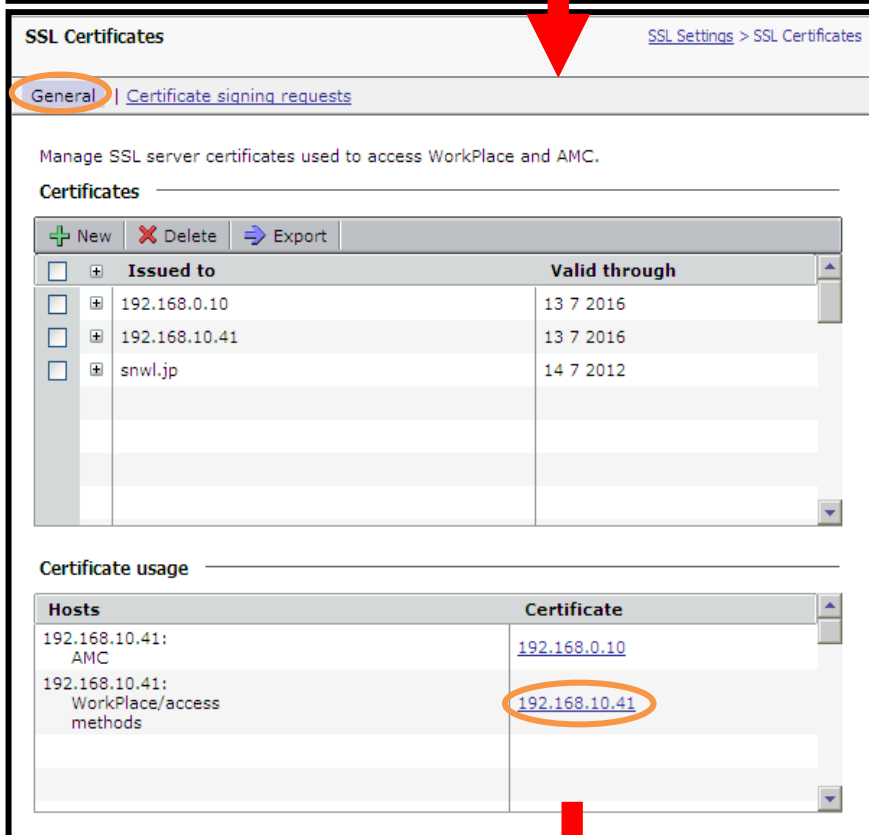
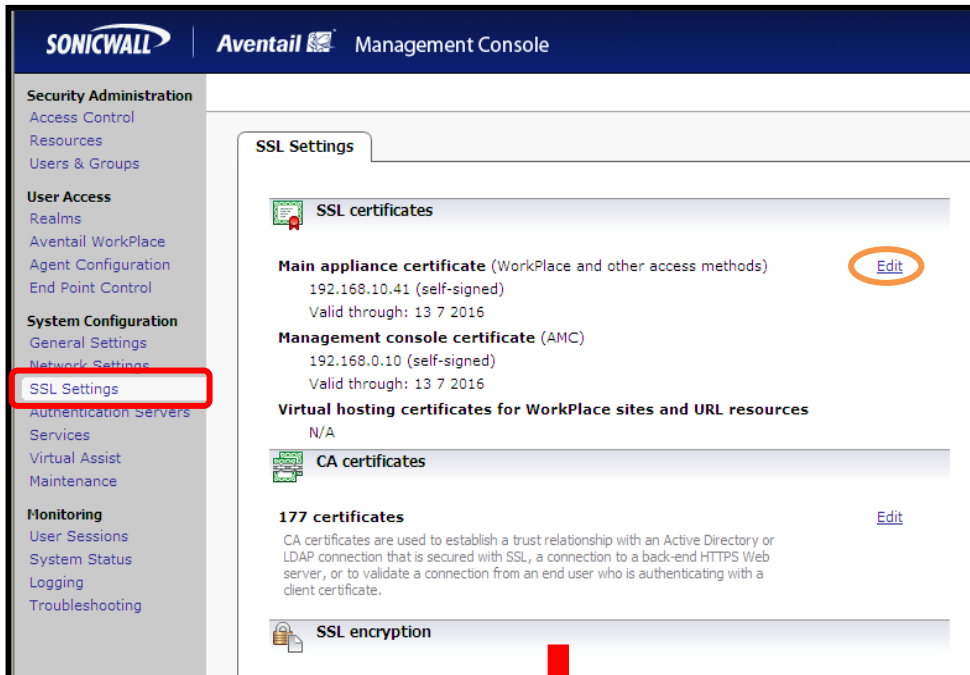
Import a certificate from a commercial certificate authority (CA). To import a certificate, either click **Browse** to import a certificate file (in PKCS#7 or X509 format), or copy the certificate text and paste it in the area provided. Include the --BEGIN CERTIFICATE-- and --END CERTIFICATE-- banners.

Certificate file:

Certificate text:

3-9 証明書を選択 (Aventail)

SSL Settings から Edit→General を選択し、Certificate usage の WorkPlace/access methods の Certificate を選択します。



次ページへ

プルダウンメニューからインポートした証明書を選択し、OK を押します。

以上で証明書の選択は完了です。

SSL Certificates [SSL Settings > SSL Certificates](#)

General | [Certificate signing requests](#)

Manage SSL server certificates used to access WorkPlace and AMC.

Certificates

<input type="checkbox"/>	<input type="checkbox"/> + Issued to	Valid through
<input type="checkbox"/>	<input type="checkbox"/> + 192.168.0.10	13 7 2016
<input type="checkbox"/>	<input type="checkbox"/> + 192.168.10.41	13 7 2016
<input type="checkbox"/>	<input type="checkbox"/> + snwl.jp	14 7 2012

Certificate usage

Hosts	Certificate
192.168.10.41: AMC	192.168.0.10
192.168.10.41: WorkPlace/access methods	snwl.jp

OK Cancel

4 Aventail の認証設定

4-1 Aventailの認証設定の流れ

設定の流れ

1. 認証サーバーの設定(RADIUS)
2. 認証サーバーの設定(PKI)
3. Realm の追加

4-2 認証サーバーの設定(RADIUS)

認証サーバー(RADIUS)の設定を行います。

Authentication Servers から New を選択します。

次に New Authentication Server 画面で下記設定後、Continue を選択します。

次に Configure Authentication Server 画面で下記設定後、Save を選択します。

The screenshot shows the SonicWall Management Console interface. The left sidebar has 'Authentication Servers' highlighted in red. The main content area shows 'Authentication Servers' with a 'New...' button circled in orange. Below it, 'Other servers' and 'RADIUS Accounting' are visible. A red arrow points from the 'New...' button to the 'New Authentication Server' screen. In this screen, 'Authentication directory' is set to 'RADIUS' and 'Credential type' is set to 'Username/Password', both circled in red. A red arrow points from the 'Continue...' button to the 'Configure Authentication Server' screen. In this screen, 'Name' is 'NetAttest EPS', 'Primary RADIUS server' is '192.168.10.80', and the 'Save' button is circled in orange.

■ New Authentication Server

【Authentication directory】

• RADIUS

【Credential Type】

• Username/Password

■ Configure Authentication Server

【Name】

• NetAttest EPS

【Primary RADIUS Server】

• 192.168.1.2

4-3 認証サーバーの設定(PKI)

認証サーバー(PKI)の設定を行います。

Authentication Servers から New を選択します。

次に New Authentication Server 画面で下記設定後、Continue を選択します。

次に Configure Authentication Server 画面で下記設定後、Save を選択します。

The screenshot shows the SonicWall Management Console interface. The left sidebar has 'Authentication Servers' highlighted in red. The main content area shows the 'Authentication Servers' configuration page. A red arrow points from the 'New...' button to the 'New Authentication Server' dialog. In this dialog, 'Authentication directory' is set to 'Public Key Infrastructure (PKI)' and 'Credential type' is set to 'Digital certificate'. A red arrow points from the 'Continue...' button to the 'Configure Authentication Server' dialog. In this dialog, 'Credential type' is set to 'Certificate', 'Name' is 'NetAttest EPS CA', and the 'All CA certificates' and 'Trusted CA certificates' lists are highlighted in red.

■ New Authentication Server

【Authentication directory】

・Public Key Infrastructure(PKI)

【Credential Type】

・Digital certificate

■ Configure Authentication Server

【Name】

・NetAttest EPS CA

【All CA certificates】

・SonicWALL.Inc

以上で認証サーバー(RADIUS、PKI)の設定は完了です。

The screenshot displays the 'Authentication Servers' configuration page in the Soliton web interface. The left sidebar contains a navigation menu with categories like Resources, User Access, System Configuration, Services, and Monitoring. The main content area is titled 'Authentication Servers' and includes a sub-section 'Authentication servers' with a 'New...' link. Below this, two entries are listed: 'NetAttest EPS' and 'NetAttest EPS CA', both of which are enclosed in a red rounded rectangle. The 'NetAttest EPS' entry shows Type: RADIUS, Credentials: Username/Password, Uses SSL: N/A, and Used by realms: None. The 'NetAttest EPS CA' entry shows Type: Certificate, Credentials: Digital Certificate, Uses SSL: N/A, and Used by realms: None. Below these are 'Other servers' sections for 'RADIUS Accounting' and 'One-Time Passwords', each with an 'Edit' link. The 'RADIUS Accounting' section shows Enabled: No, Primary: N/A, and Secondary: N/A. The 'One-Time Passwords' section shows SMTP enabled: No, SMTP server: N/A, and SMTP authentication: Disabled. At the bottom left, there is a footer with S/N: 00401023ECD3, Version: 10.5.3-052, and © 2010 SonicWALL, Inc.

Server Name	Type	Credentials	Uses SSL	Used by realms
NetAttest EPS	RADIUS	Username/Password	N/A	None
NetAttest EPS CA	Certificate	Digital Certificate	N/A	None

RADIUS Accounting
Sends accounting information to a RADIUS server for billing purposes.
Enabled: No
Primary: N/A
Secondary: N/A

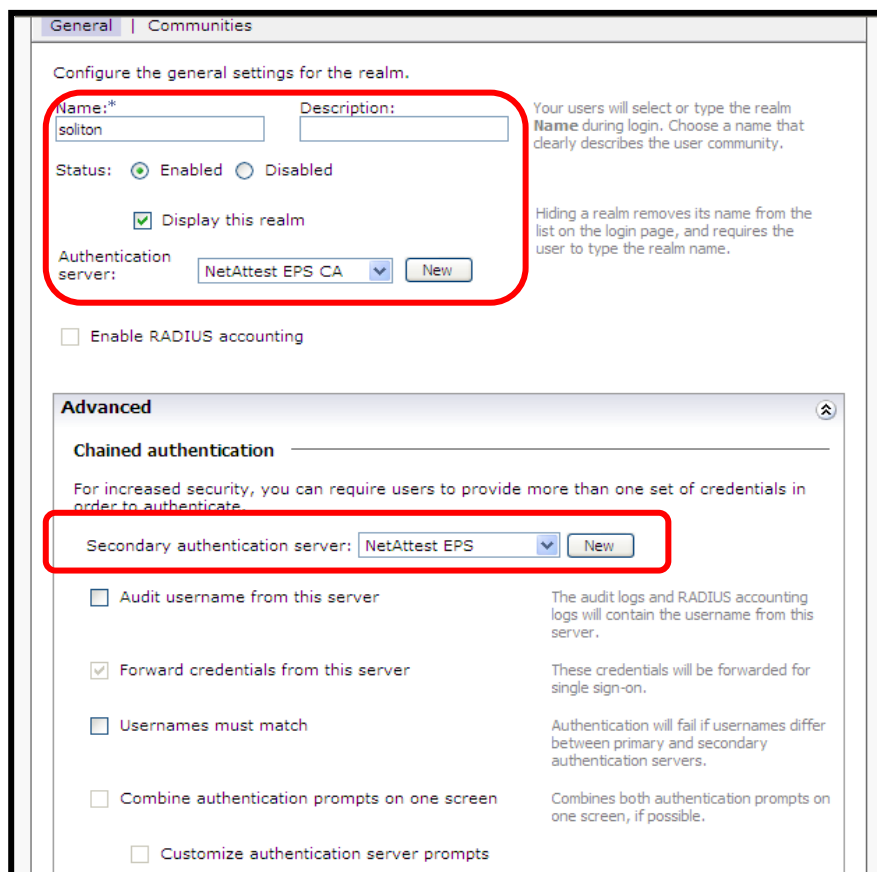
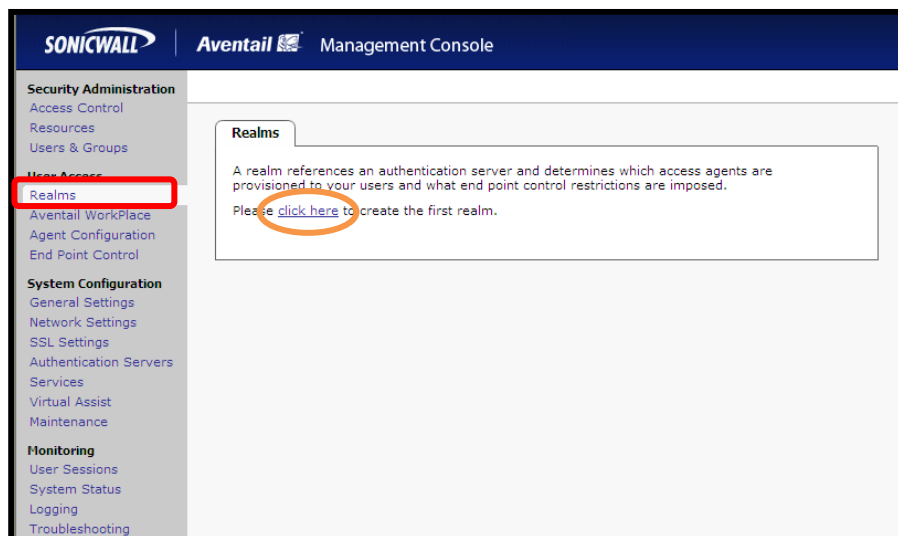
One-Time Passwords
Sends randomly generated single-use passwords via email to provide two-factor authentication.
SMTP enabled: No
SMTP server: N/A
SMTP authentication: Disabled

4-4 Realmの追加

続いて Realm の追加を行います。

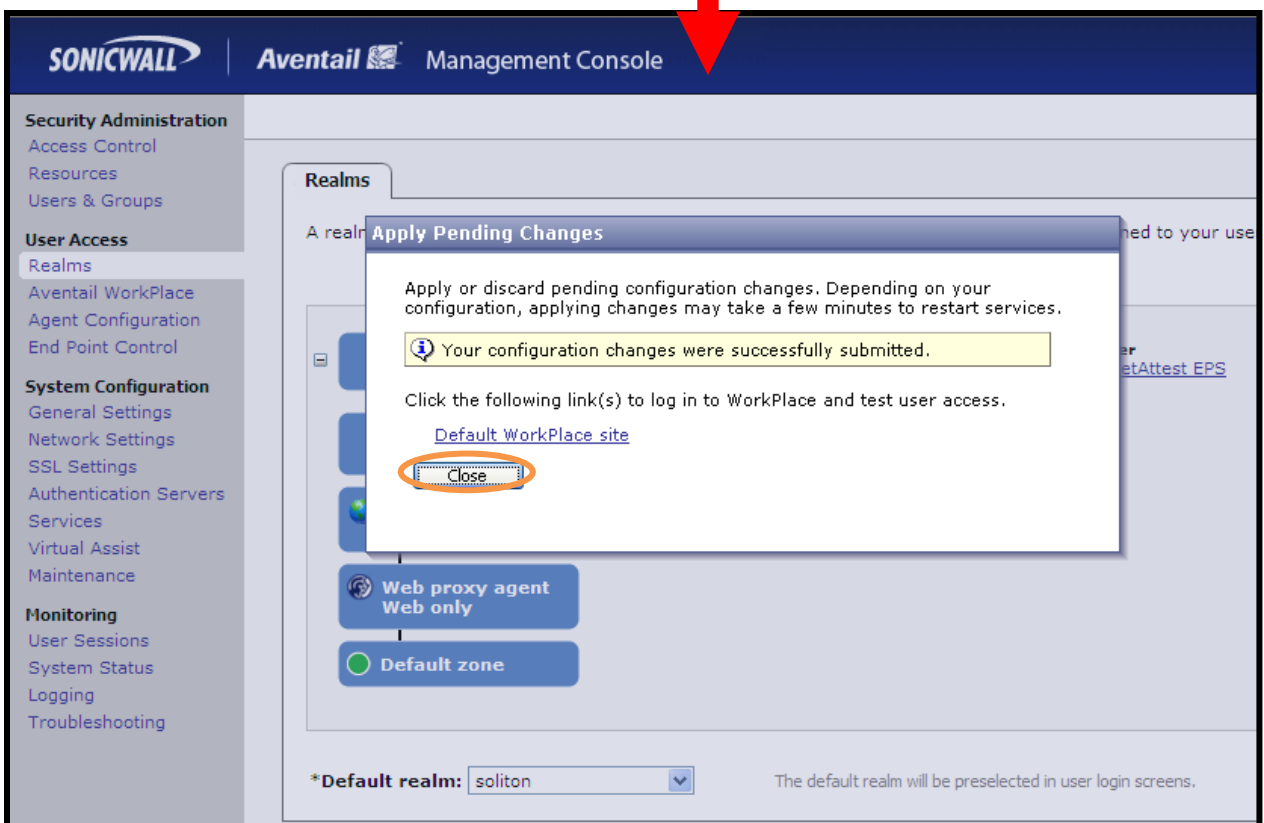
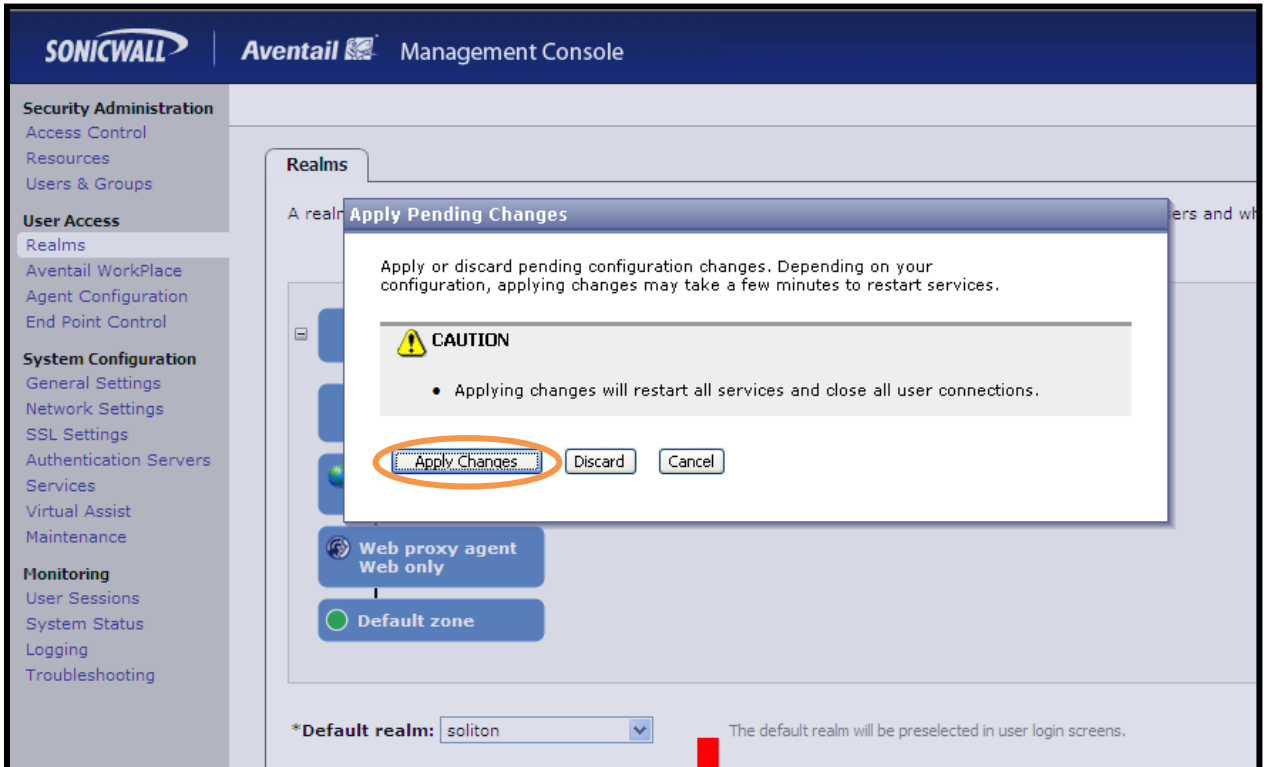
Realms から [click here](#) を選択し、下記の様に設定します。

次に進んで下さい。



設定変更を許可します。

以上で Realm の追加は完了です。



5 クライアントPCの設定

5-1 クライアントPC設定の流れ

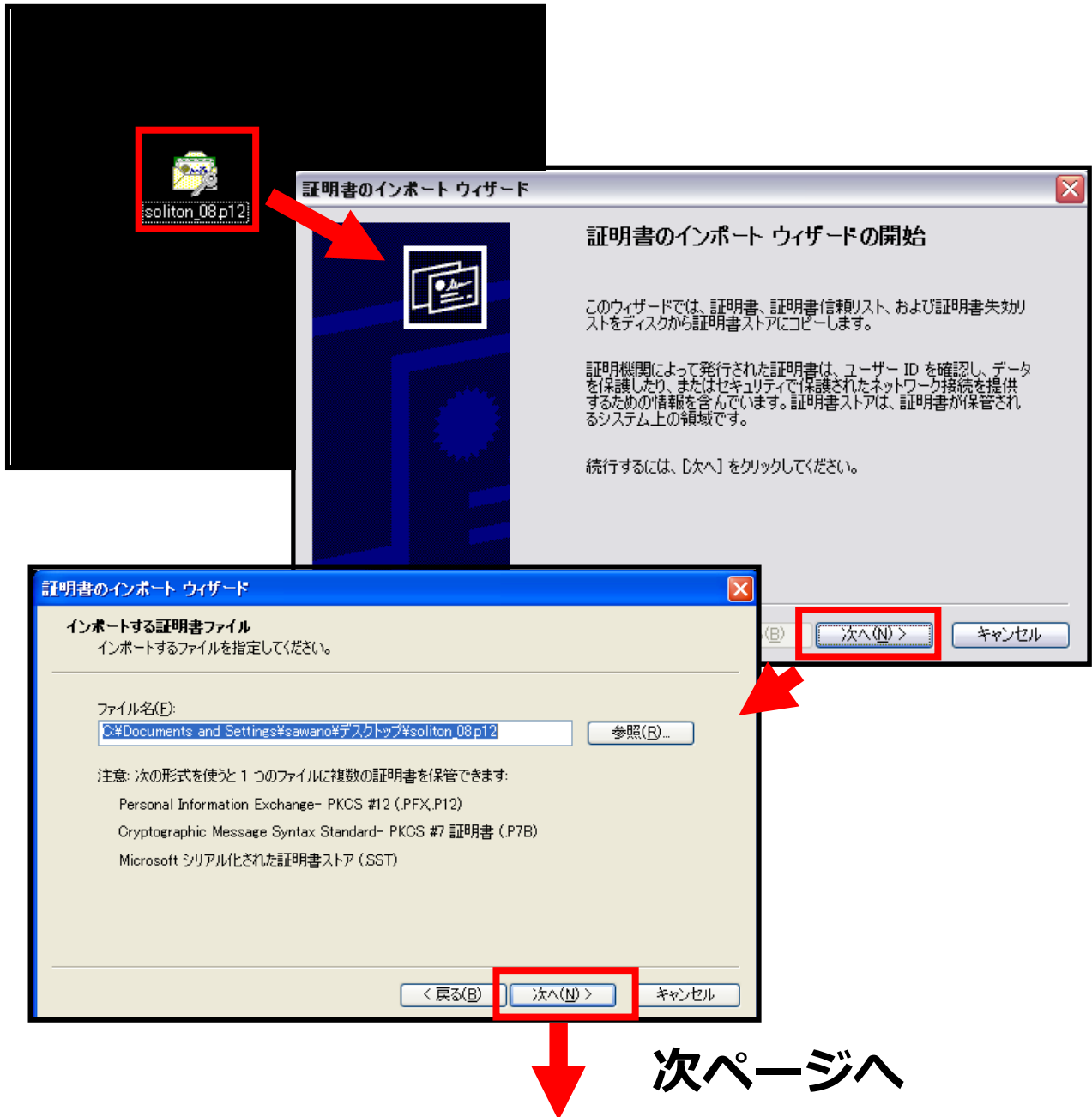
設定の流れ

1. 証明書のインポート
2. 認証の確認

5-2 証明書のインポート

NetAttest EPS からダウンロードした証明書をインポートします。

本書では、デスクトップ上に保存されている「soliton_08p12」アイコンをダブルクリックします。

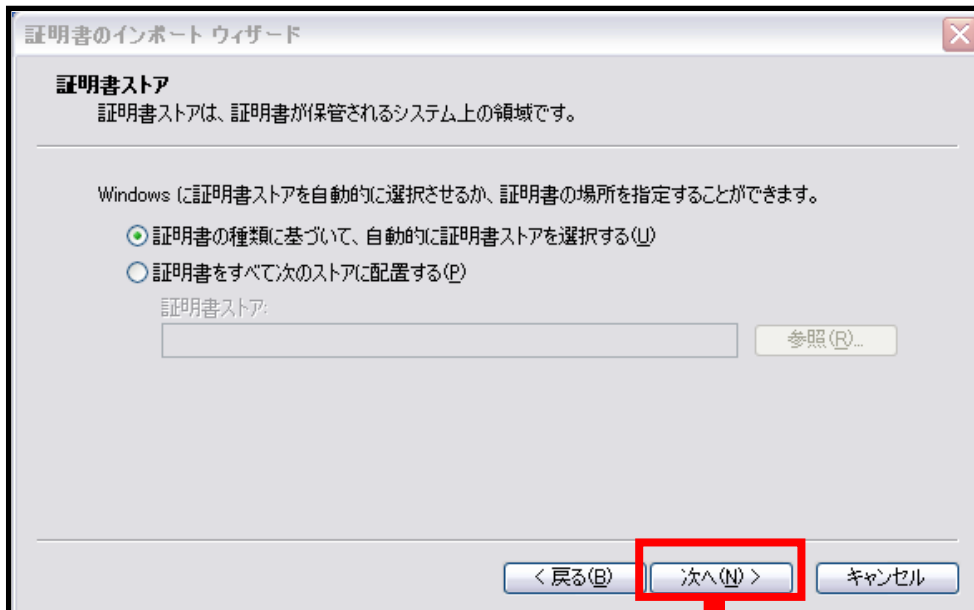


NetAttest EPS にてユーザー証明書を発行した
際に設定したパスワードを入力します。

【パスワード】

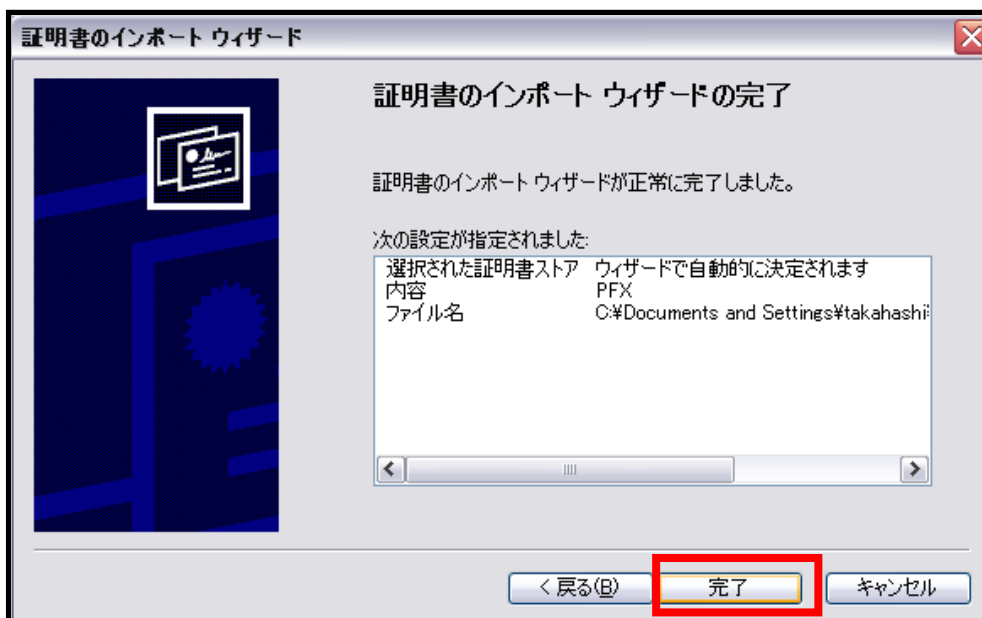
- ・ password

次ページへ



【証明書の種類に基づいて・・・】

・チェック有



5-3 認証の確認

SSL VPN 認証画面にログイン出来たら確認完了です。

【ユーザー名】

・ soliton

【パスワード】

・ password

