

NetAttest EPS

認証連携設定例

【連携機器】 Citrix NetScaler

【Case】 証明書と ID・Password によるハイブリッド認証

Rev1.0

株式会社ソリトンシステムズ

はじめに

本書について

本書は、NetAttest EPS と Citrix 社製 VPN ゲートウェイ NetScaler 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 NetScalar の操作方法を記載したものです。すべての環境での動作を保証するものではありません。

NetAttest®は、株式会社ソリトンシステムズの登録商標です。

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

本文中に ™、®、©は明記していません。

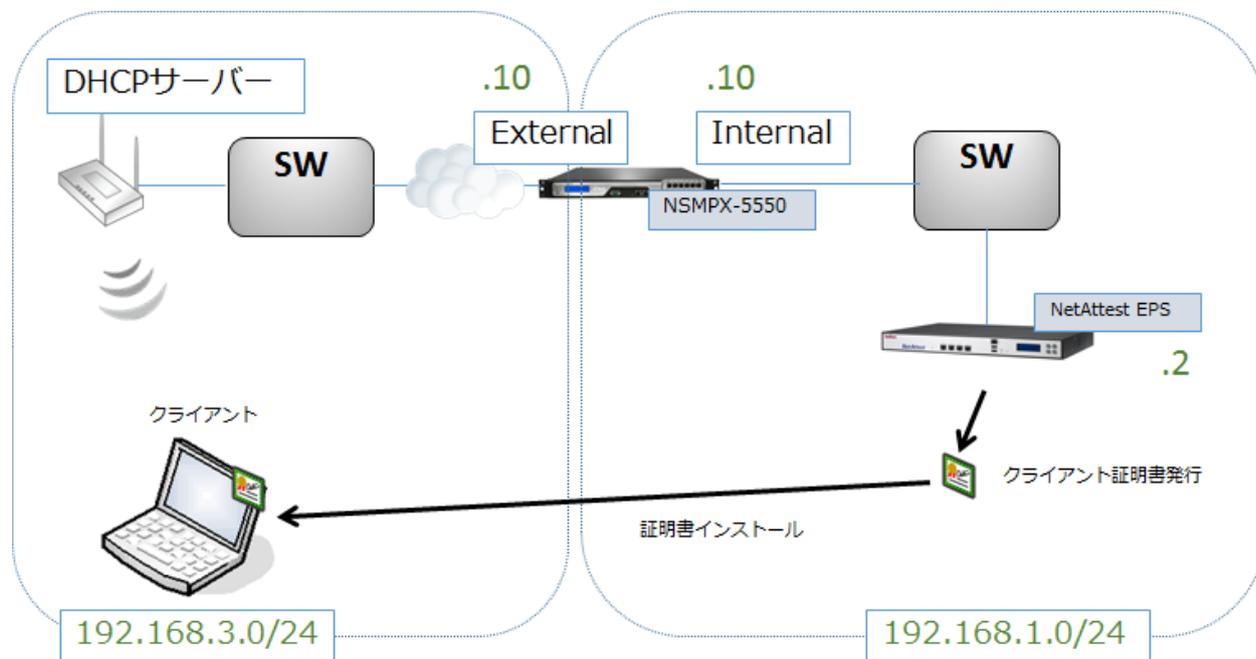
目次

1. 構成.....	6
1-1 構成図.....	6
1-2 環境.....	7
1-2-1 機器.....	7
1-2-2 認証方式.....	7
1-2-3 ネットワーク設定.....	7
2. NetAttest EPS の設定.....	8
2-1 システム初期設定ウィザードの実行.....	8
2-2 サービス初期設定ウィザードの実行.....	9
2-3 認証ユーザーの追加登録.....	10
2-4 クライアント証明書の発行.....	11
3. NetScaler の設定.....	12
3-1 各インターフェイスの設定.....	12
3-2 機能の有効化.....	14
3-3 サーバー証明書、CA 証明書のダウンロードとインポート手順.....	15
3-3-1 CSR の作成(NetScaler).....	16
3-3-2 サーバー証明書のダウンロード (NetAttest EPS).....	20
3-3-3 CA 証明書のダウンロード (NetAttest EPS).....	21
3-3-4 サーバー証明書のインポート (NetScaler).....	22
3-3-5 CA 証明書のインポート (NetScaler).....	24
3-4 OCSP の設定.....	25
3-4-1 OCSP 署名証明書の発行(NetAttest EPS).....	25
3-4-2 OCSP に関する設定(NetScaler).....	26
3-5 RADIUS ポリシーの設定.....	30
3-6 セッションポリシーの設定.....	32
3-7 Virtual Server の設定.....	34
4. VPN クライアントの設定.....	38
4-1 PC へのデジタル証明書のインストール.....	38
4-2 NetScaler Gateway Plug-in のインストール.....	40

5. 接続テスト.....41

1. 構成

1-1構成図



1-2環境

1-2-1機器

製品名	メーカー	役割	バージョン
NetAttest EPS-ST04	Soliton Systems	認証サーバー (RADIUS サーバー、CA)	Ver. 4.6.8
NetScaler MPX-5550	Citrix	RADIUS クライアント (SSL VPN 機器)	Ver. 10.5
GW-MF54G2	PCi	無線 AP (インターネット側用)	-
Let's note CF-SX2	Panasonic	Client PC	Windows 7 SP1

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

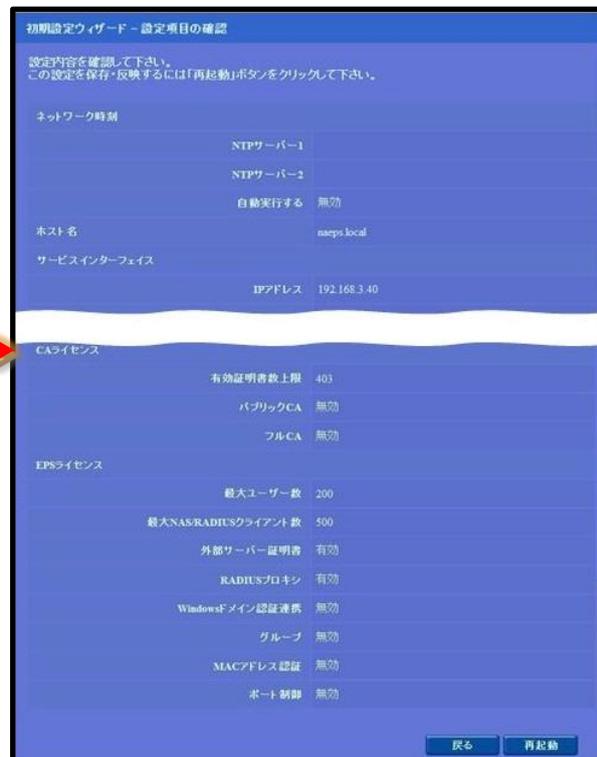
	EPS-ST04	NetScaler MPX-5550	Client PC	無線 AP
IP アドレス	192.168.1.2/24 (LAN1) 192.168.2.1/24 (LAN2)	192.168.3.11/24(external) 192.168.3.10/24(external) 192.168.1.11/24(manage) 192.168.1.10/24(internal)	DHCP (無線 AP から)	192.168.1.100/24
RADIUS port (Authentication)	UDP 1812		-	-
RADIUS Secret (Key)	secret		-	-

2. NetAttest EPS の設定

2-1システム初期設定ウィザードの実行

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

- タイムゾーンと日付・時刻の設定
- ホスト名の設定
- サービスインターフェイスの設定
- 管理インターフェイスの設定
- ドメインネームサーバーの設定



2-2サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

本手順書では値を記載しているもの以外はすべてデフォルト設定で行いました。

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

CA種別選択
CA種別選択: ルートCA

CA秘密鍵
 内部で新しい鍵を生成する
 公開鍵方式: RSA
 鍵長: 2048
 外部HSMデバイスの鍵を使用する

要求の署名
要求署名アルゴリズム: SHA1

CA情報
CA名(必須): TestCA
 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:

CA署名設定
署名アルゴリズム: SHA1
有効日数: 3650

戻る 次へ

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

初期設定ウィザード - NAS/RADIUSクライアント設定
編集対象: 新規

NAS/RADIUSクライアント名:

このNAS/RADIUSクライアントを有効にする

タイプ:

- NAS/RADIUSクライアント
- NASのみ
- RADIUSクライアントのみ

説明:

IPアドレス:

シークレット:

NAS識別値:

戻る 次へ

項目	値
NAS/RADIUS クライアント名	NetScalar
IP アドレス (Authenticator)	192.168.1.10
シークレット	secret

2-3認証ユーザーの追加登録

NetAttest EPS の管理画面より、認証ユーザーの登録を行います。

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

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

2-4クライアント証明書の発行

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)



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



3. NetScaler の設定

3-1 各インターフェイスの設定

NetScaler の各インターフェイスの設定を行います。

管理インターフェイスの IP アドレスはデフォルトで「192.168.100.1」ですので、ブラウザより「http://192.168.100.1/」でアクセスします。

「User Name」「Password」はどちらも「nsroot」ですので、入力後「ログイン」をクリックします。



項目	値
User Name	nsroot
Password	nsroot

ログイン後、[Network]-[IPs]より[IPv4s]タブの「Add」をクリックし、各インターフェイスの設定を行います。

各インターフェイスの「Type」は以下です。

NetScaler IP:管理用

Subnet IP:Internal 用

Virtual IP:external 用

項目	値
NetScaler IP	192.168.1.11
Subnet IP	192.168.1.10
Subnet IP	192.168.3.11
Virtual IP	192.168.3.10

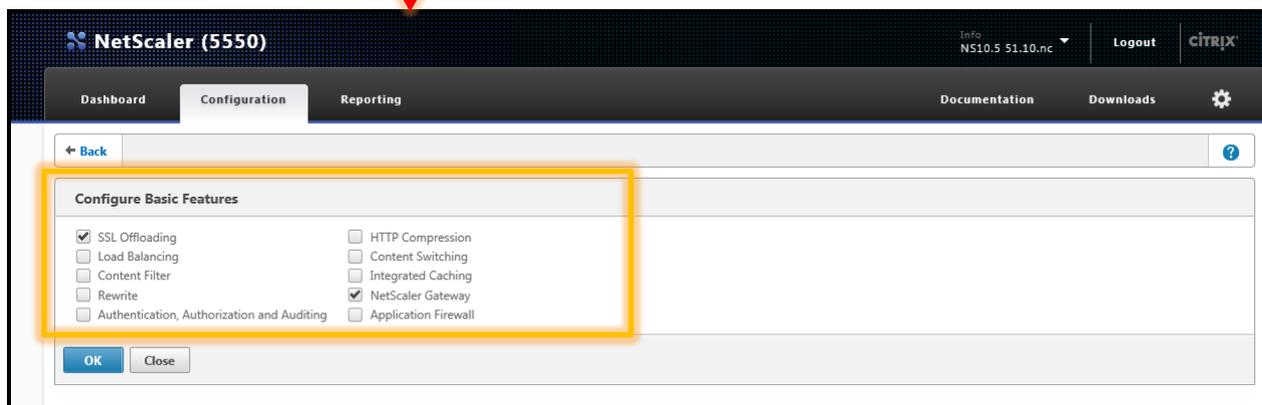
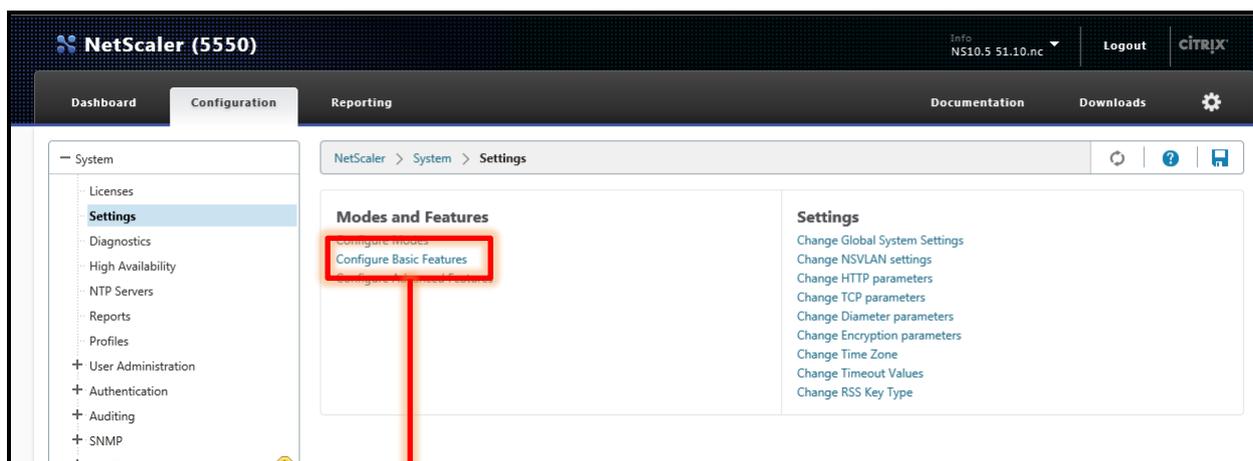
IP Address	State	Type	Mode	ARP	ICMP	Virtual Server	Traffic Domain
▶ 192.168.1.11	Enabled	NetScaler IP	Active	ENABLED	ENABLED	-N/A-	0
▶ 192.168.1.10	Enabled	Subnet IP	Active	ENABLED	ENABLED	-N/A-	0
▶ 192.168.3.10	Enabled	Virtual IP	Active	ENABLED	ENABLED	ENABLED	0
▶ 192.168.3.11	Enabled	Subnet IP	Active	ENABLED	ENABLED	-N/A-	0

3-2機能の有効化

機能を有効にします。

[System]-[Settings]より「Configure Basic Features」をクリックします。

「SSL Offloading」、「NetScaler Gateway」をチェックし、「OK」をクリックします。



3-3サーバー証明書、CA 証明書のダウンロードとインポート手順

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

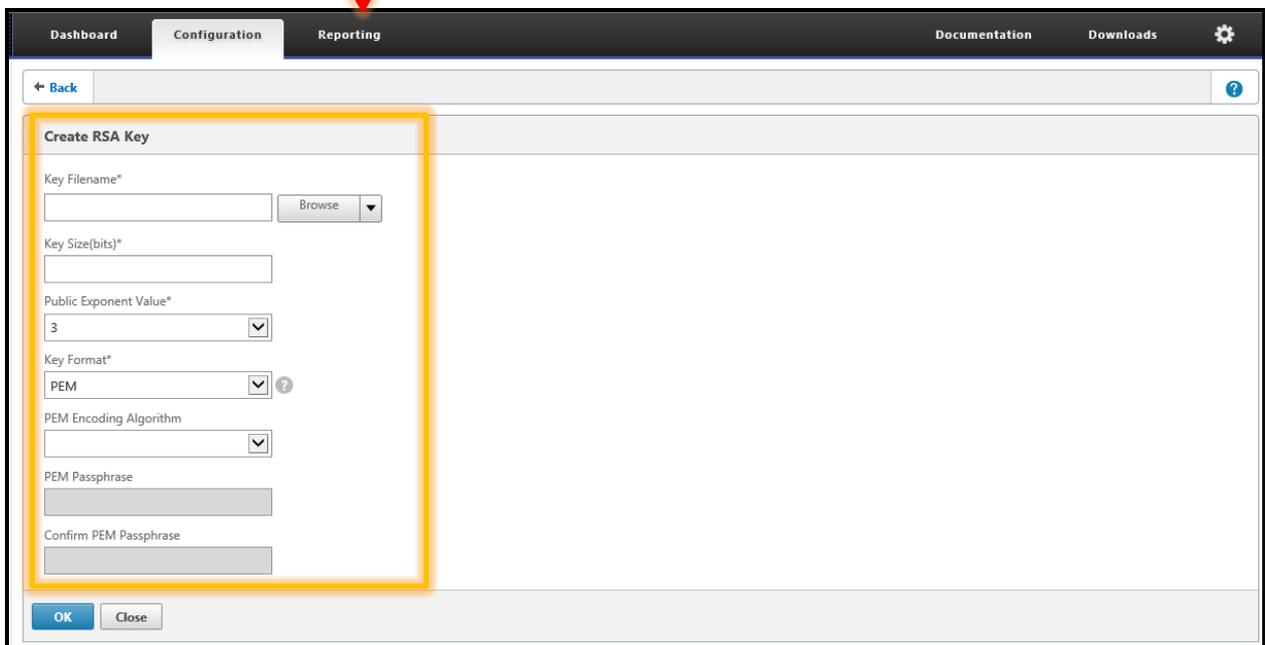
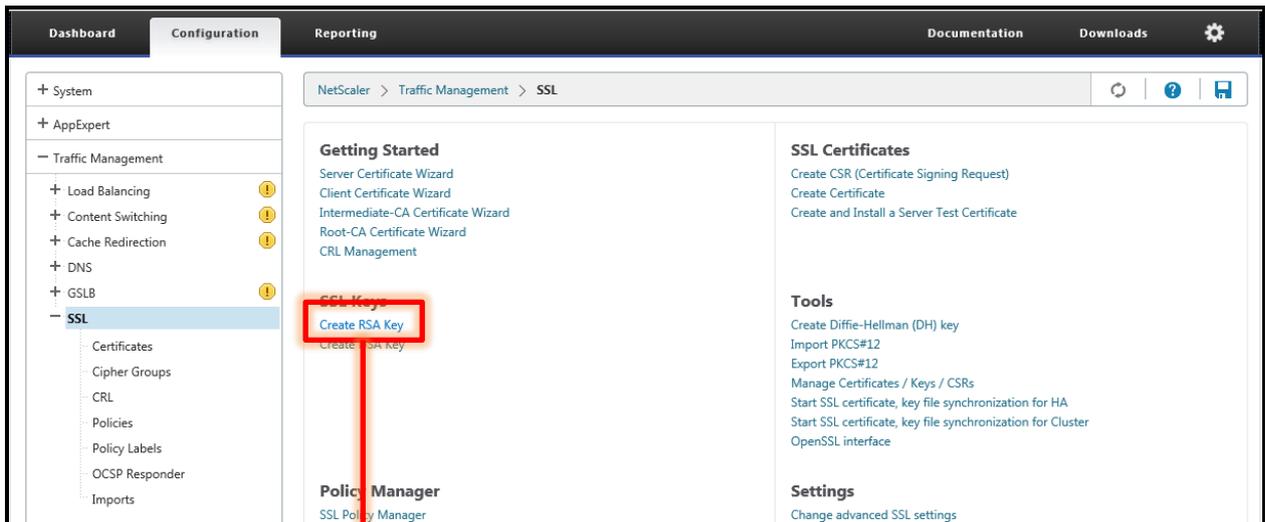
- CSR の作成(NetScaler)
- サーバー証明書ダウンロード(NetAttest EPS)
- CA 証明書のダウンロード(NetAttest EPS)
- サーバー証明書のインポート(NetScaler)
- CA 証明書のインポート(NetScaler)

3-3-1 CSR の作成(NetScaler)

Key の作成を行います。

[Traffic Management]-[SSL]より「Create RSA Key」をクリックします。

「Key Filename」、「Key Size」を入力し、「OK」をクリックします。



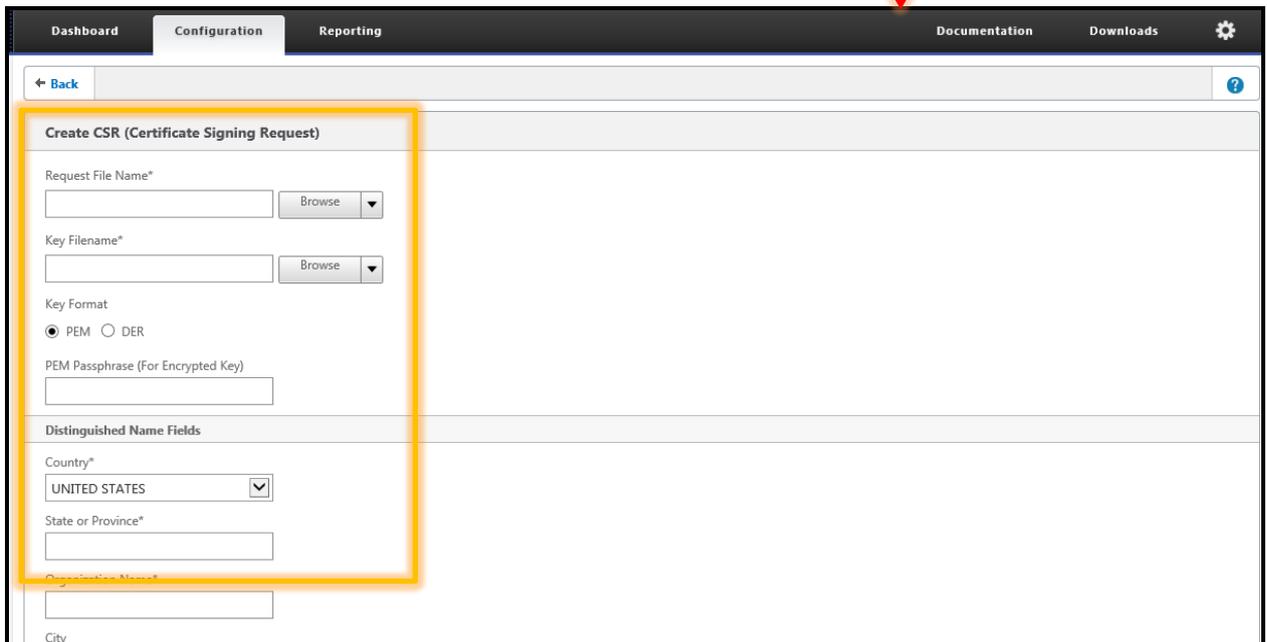
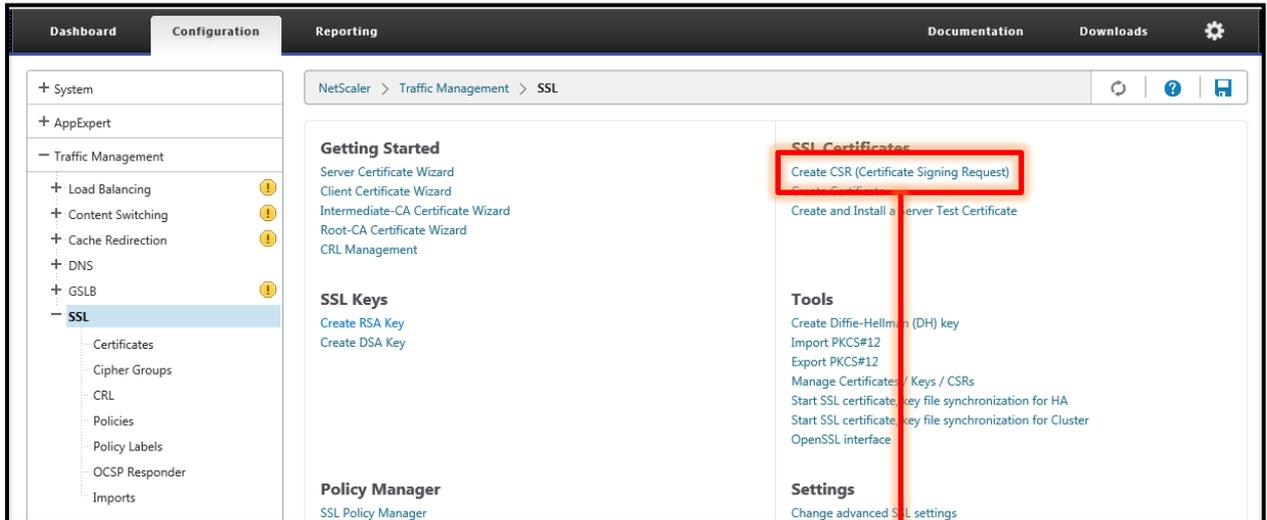
項目	値
Key Filename	Soliton.key
Key Size	2048

CSR の作成を行います。

[Traffic Management]-[SSL]より「Create CSR」をクリックします。

「Request File Name」を入力し、「Key Filename」にて、先ほど作成した Key を選択します。

「Distinguished Name Fields」にてサブジェクトを入力します。



項目	値
Request File Name	Soliton.csr
Key Filename	Soliton.key

Key Format
 PEM DER

PEM Passphrase (For Encrypted Key)

Distinguished Name Fields

Country*

State or Province*

Organization Name*

City

Email Address

Organization Unit

Common Name

Attribute Fields

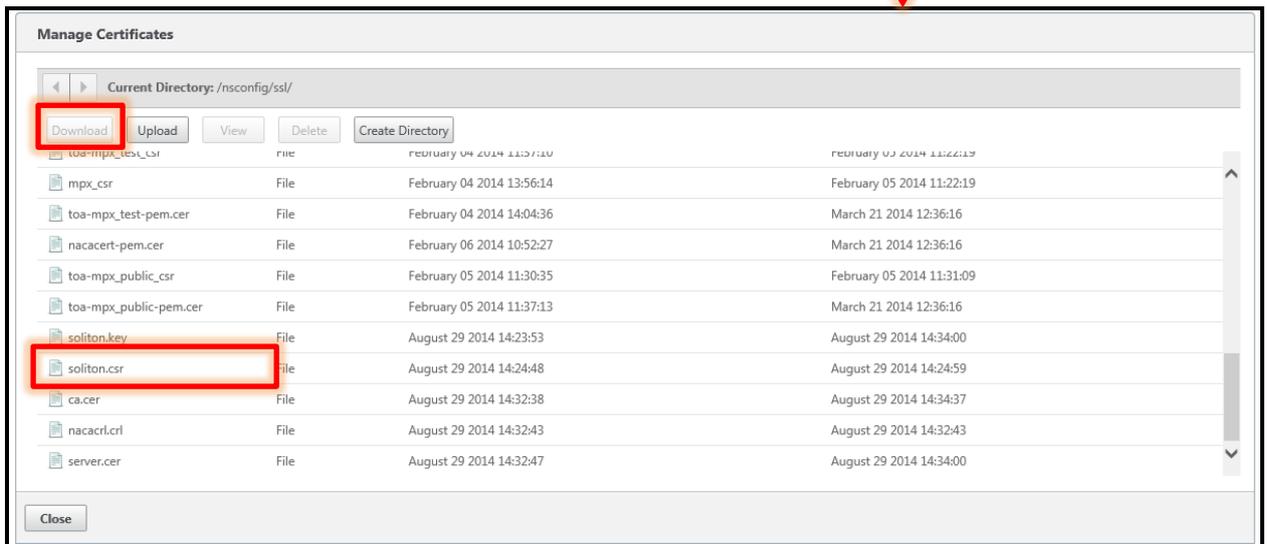
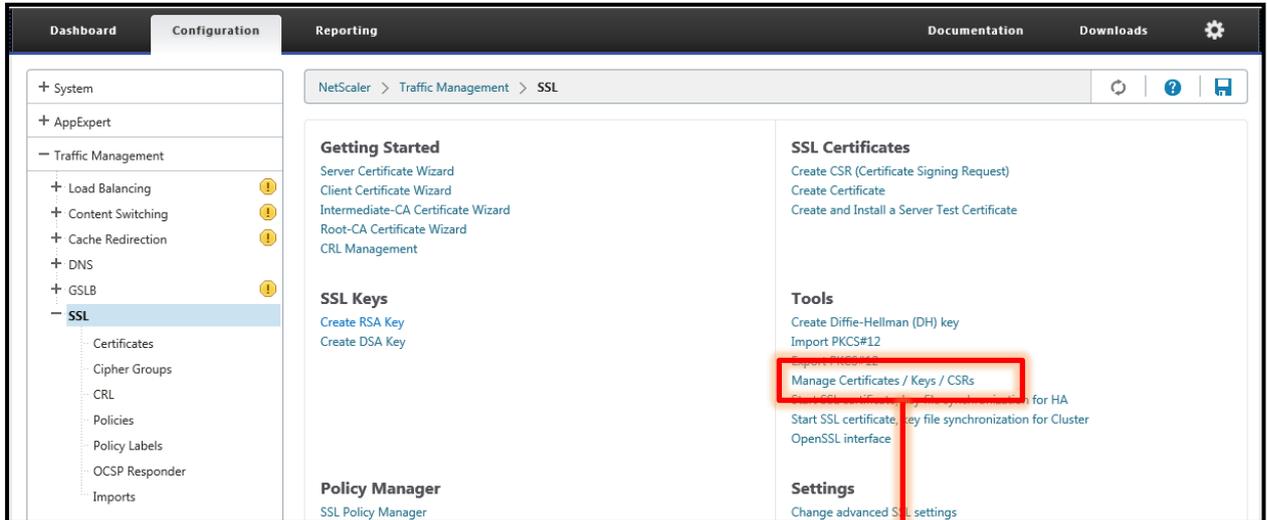
Challenge Password

項目	値
Country	Japan
Organization Name	Soliton
Common Name	192.168.3.10

CSR のダウンロードを行います。

[Traffic Management]-[SSL]より「Manage Certofocates/Keys/CRLs」 をクリックします。

作成した CRL を選択し、「Download」 をクリックします。



3-3-2サーバー証明書のダウンロード（NetAttest EPS）

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



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

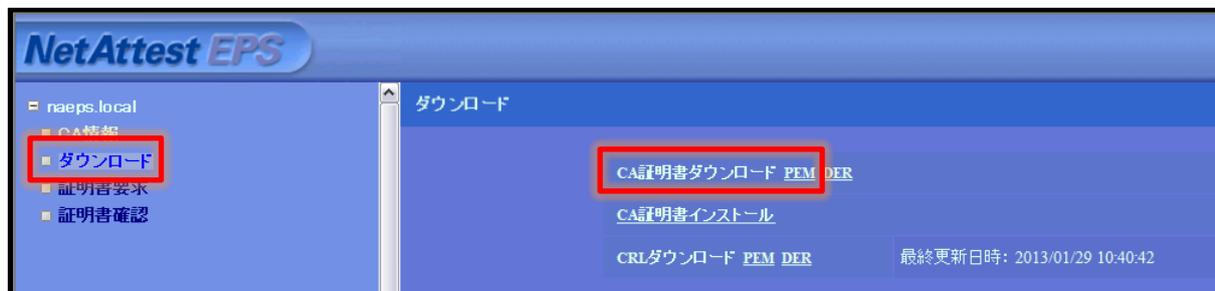


管理者向け証明書サービスページにアクセスします。「証明書の確認」を選択すると状態が【発行】になっていますので、サーバー証明書(nausercert-pem.cer)をダウンロードします。



3-3-3CA 証明書のダウンロード (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。

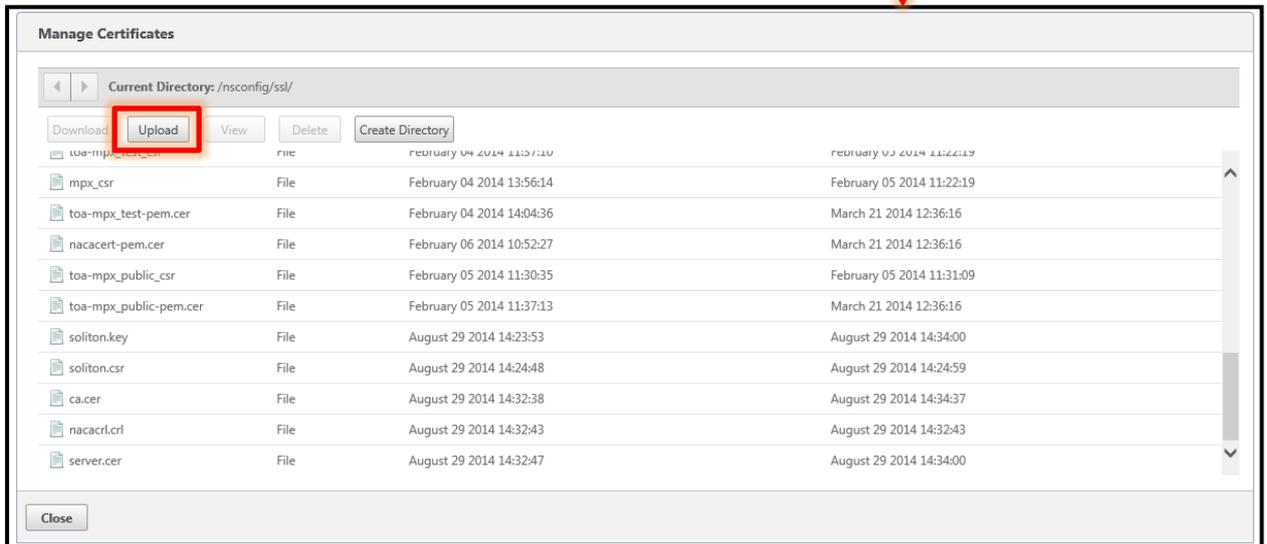
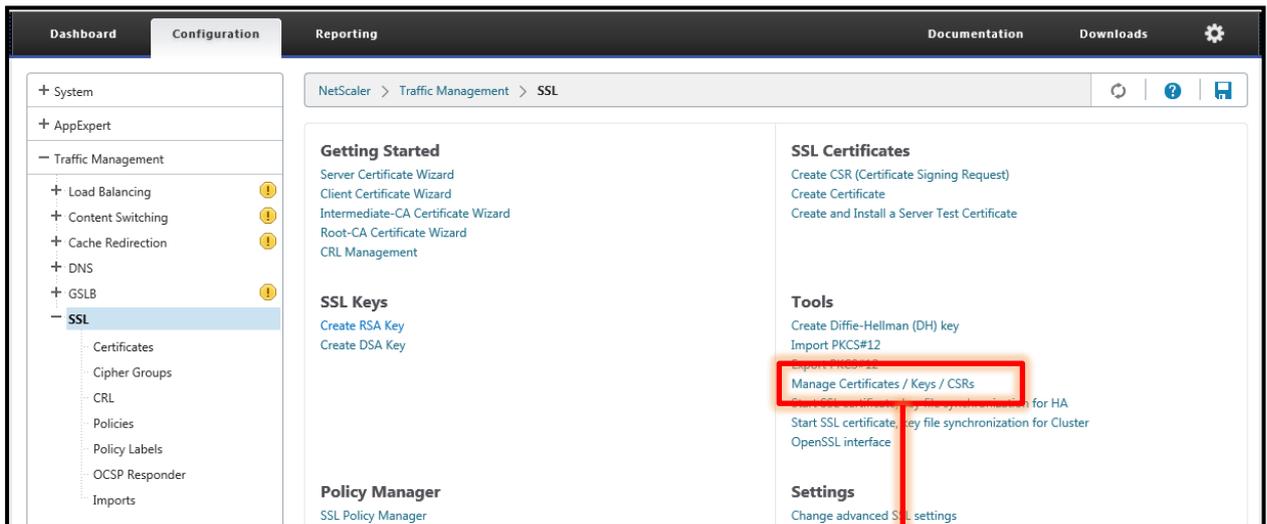


3-3-4サーバー証明書のインポート (NetScaler)

サーバー証明書のインポートを行います。

[Traffic Management]-[SSL]より「Manage Certificates/Keys/CRLs」をクリックします。
 を選択し、「Upload」をクリックします。

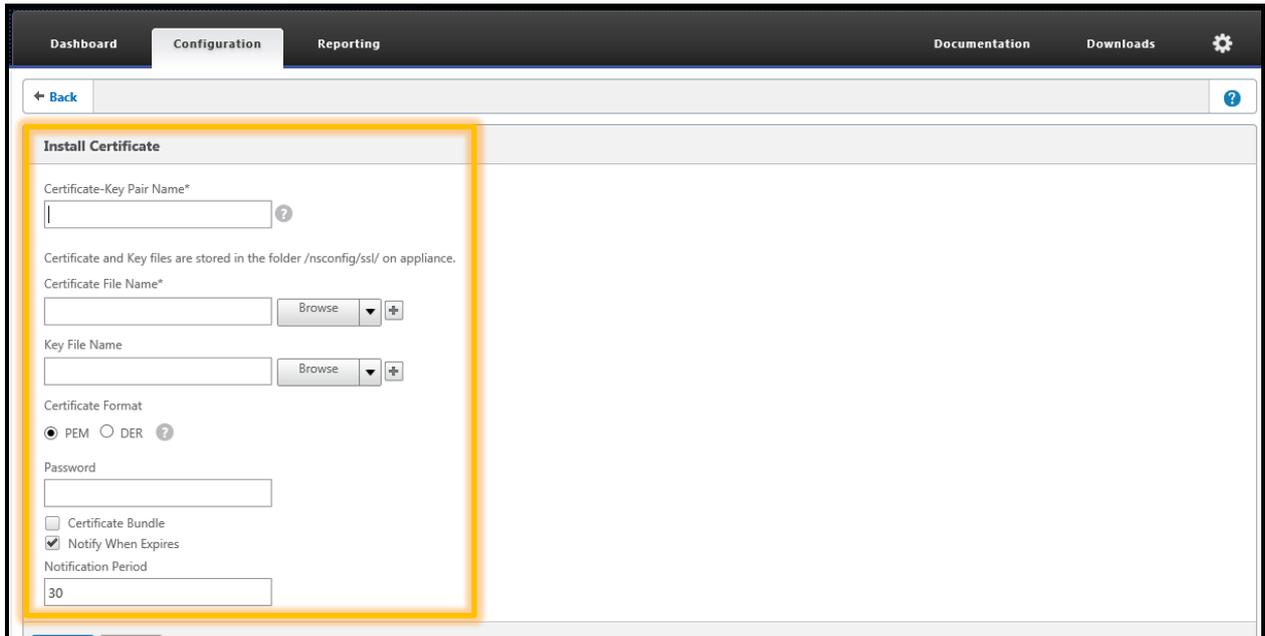
[3-3-2]でダウンロードしたサーバー証明書をアップロードします。また[3-3-3]でダウンロードした CA 証明書もアップロードします。



[SSL]-[Certificates]より「Install」をクリックし、NetAttest EPS からダウンロードしたサーバー証明書と CA 証明書を NetScaler にインストールします。

まずは、サーバー証明書をインストールします。

「Certificate-Key Pair Name」を入力し、「Certificate File Name」に[3-3-4]でアップロードしたサーバー証明書を選択し、「Key file Name」には[3-3-1]で作成した「RSA Key」を選択します。



項目	値
Certificate-Key Pair Name	soliton-server-certificate
Certificate File Name	[3-3-4]でアップロードしたサーバー証明書を選択
Key File Name	[3-3-1]で作成した RSA Key を選択(Soliton.key)

3-3-5CA 証明書のインポート (NetScaler)

次に CA 証明書をインストールします。

同じく「Install Certificate」より、「Certificate-Key Pair Name」を入力し、「Certificate File Name」に[3-3-4]でアップロードした CA 証明書を選択します。

※ 「Key File Name」の選択は必要ありません。

項目	値
Certificate-Key Pair Name	soliton-root-certificate
Certificate File Name	[3-3-4]でアップロードした CA 証明書を選択

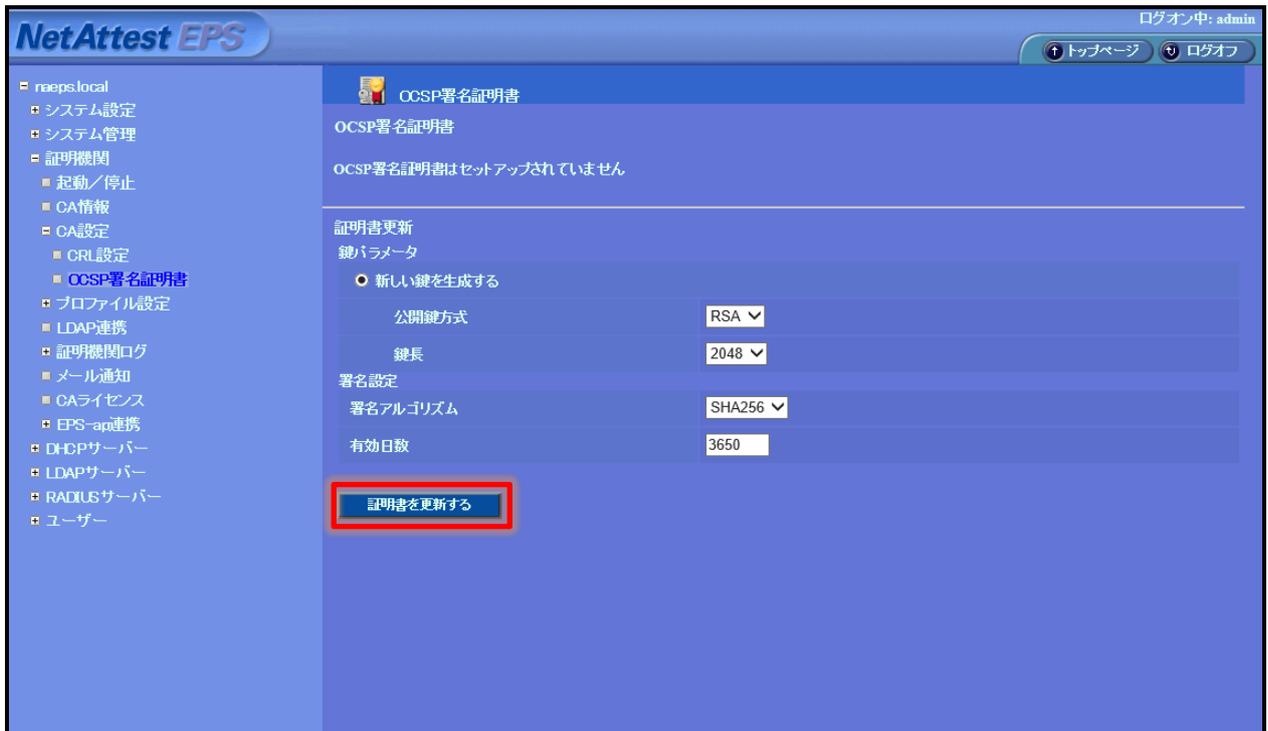
Name	Days to Expire	Status
ns-server-certificate	5528	Valid
soliton-server-certificate	364	Valid
soliton-root-certificate	3648	Valid

3-4OCSP の設定

NetScaler が OCSP を使用して、認証毎に NetAttest EPS に証明書の失効確認を行う設定をします。

3-4-1OCSP 署名証明書の発行(NetAttest EPS)

NetAttest EPS 管理ページより、[証明機関]-[CA 設定]-[OCSP 署名証明書]の「証明書を更新する」をクリックします。



The screenshot shows the NetAttest EPS management console. The left sidebar contains a navigation menu with the following items: neps.local, システム設定, システム管理, 証明機関 (expanded), 起動/停止, CA情報, CA設定 (expanded), CRL設定, **OCSP署名証明書** (selected), プロファイル設定, LDAP連携, 証明機関ログ, メール通知, CAライセンス, EPS-ap連携, DHCPサーバー, LDAPサーバー, RADIUSサーバー, ユーザー. The main content area is titled 'OCSP署名証明書' and displays the following information:

- OCSP署名証明書
- OCSP署名証明書はセットアップされていません
- 証明書更新
- 鍵パラメータ
 - 新しい鍵を生成する
- 公開鍵方式: RSA
- 鍵長: 2048
- 署名設定
- 署名アルゴリズム: SHA256
- 有効日数: 3650

At the bottom of the settings area, there is a button labeled '証明書を更新する' which is highlighted with a red rectangular box.

※NetAttest EPS が OCSP レスポンダとして動作するには、拡張 CA ライセンスが必要です。

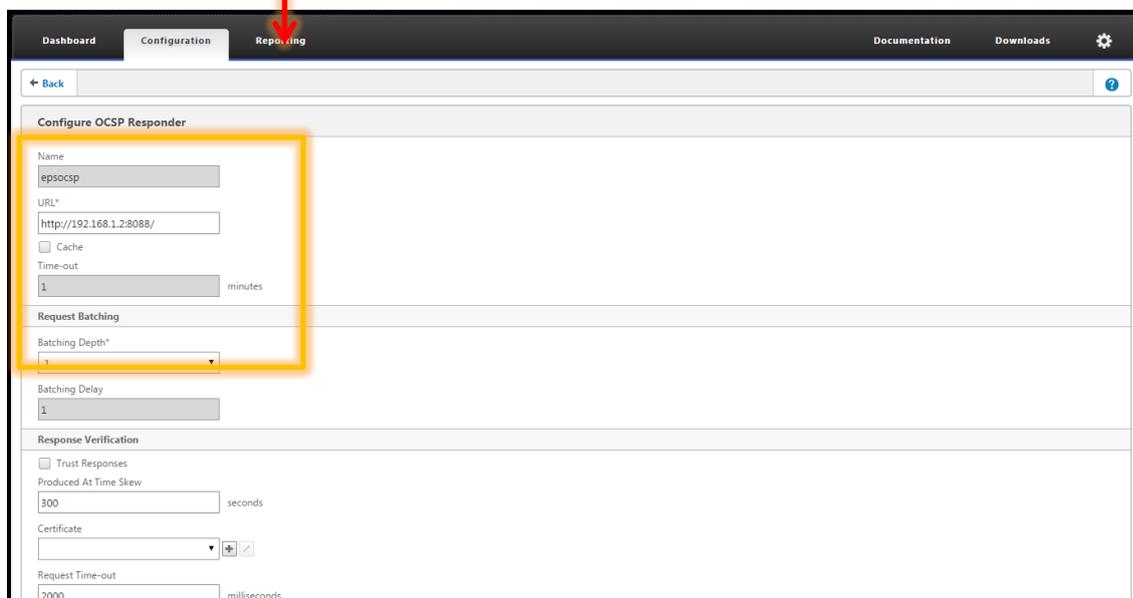
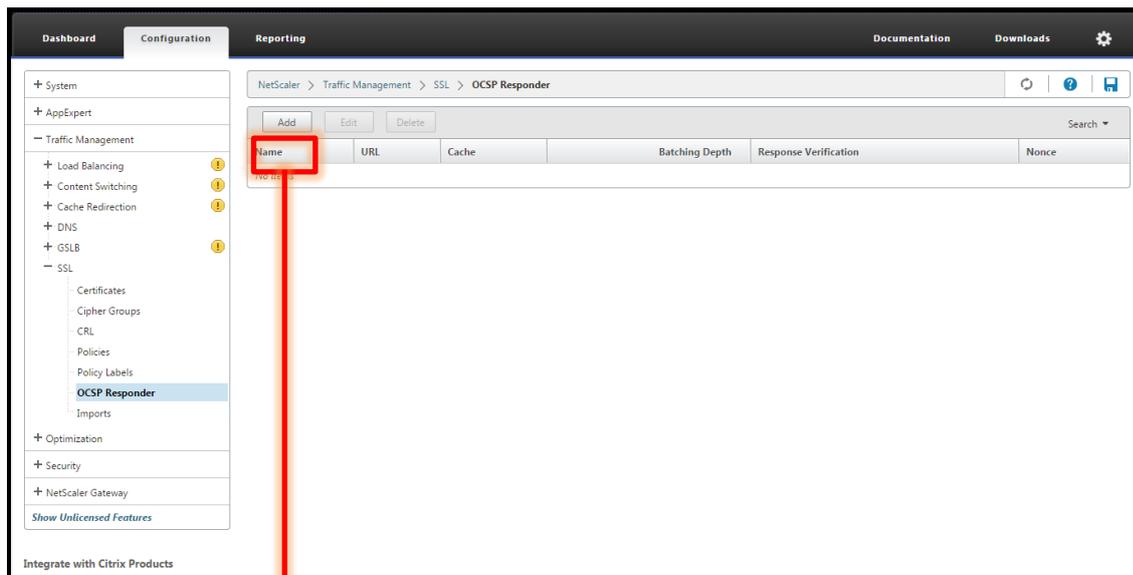
3-4-2OCSP に関する設定(NetScaler)

NetScaler 側で OCSP に関する設定を行います。

[Traffic Management]-[SSL]-[OCSP Responder]より「Add」をクリックします。

「Name」と「URL」を入力します。

NetAttest EPS の OCSP Responder の URL は「http://<EPS の IP(FQDN)>:8088/」です



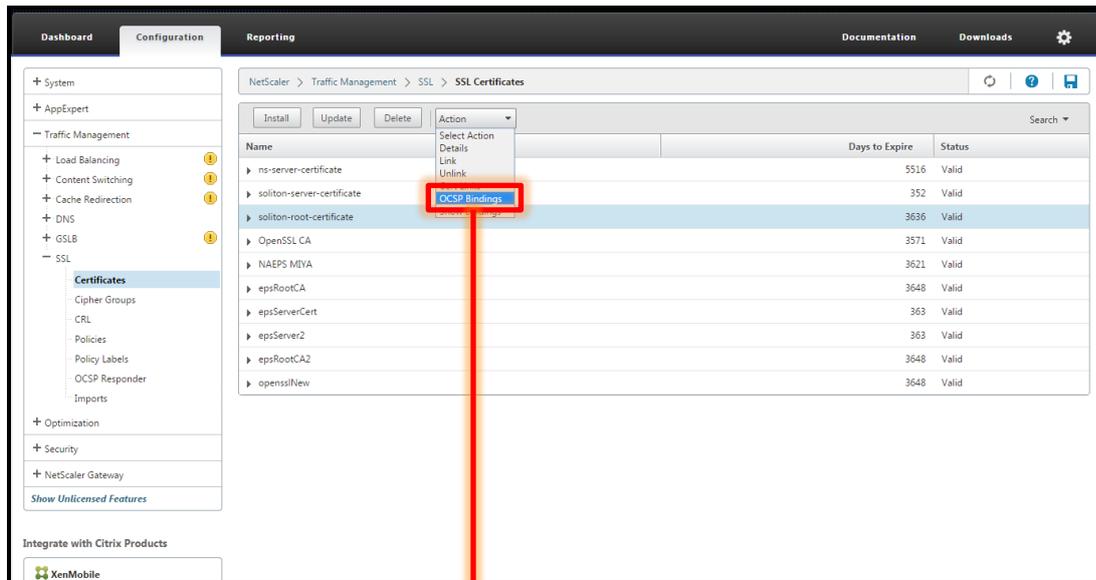
項目	値
Name	epsocsp
URL	http://192.168.1.2:8088/

続いて NetScaler にインストールした CA 証明書に OCSP 設定を紐付けます。

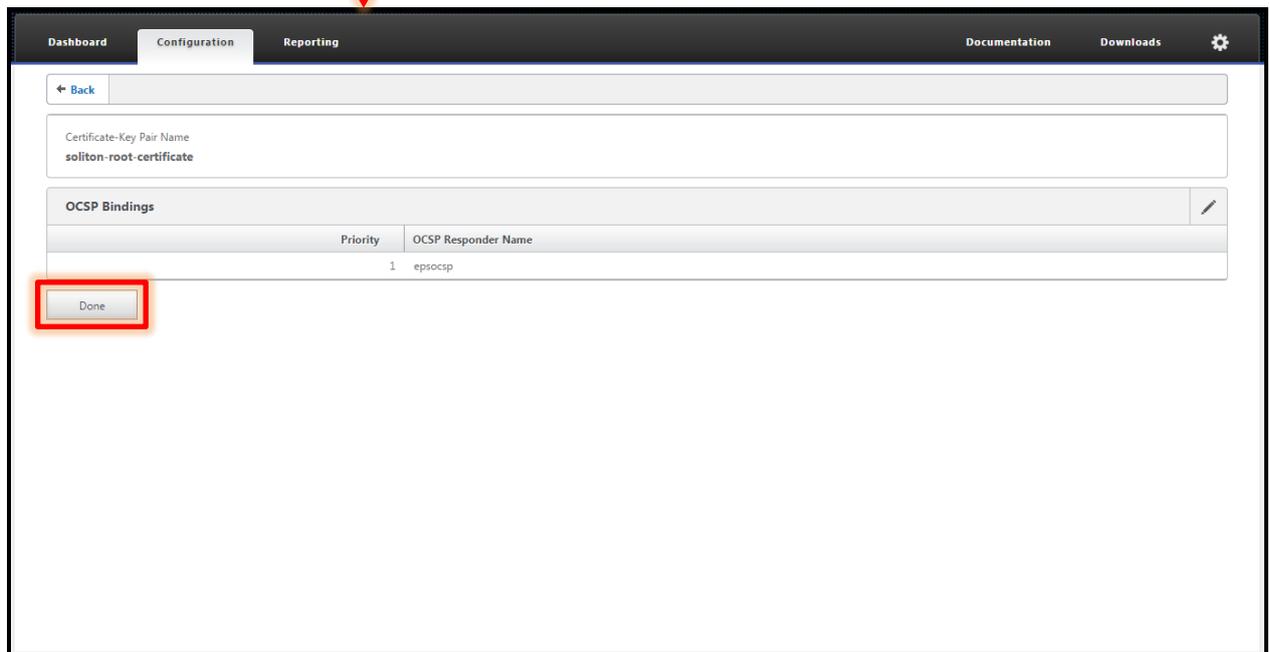
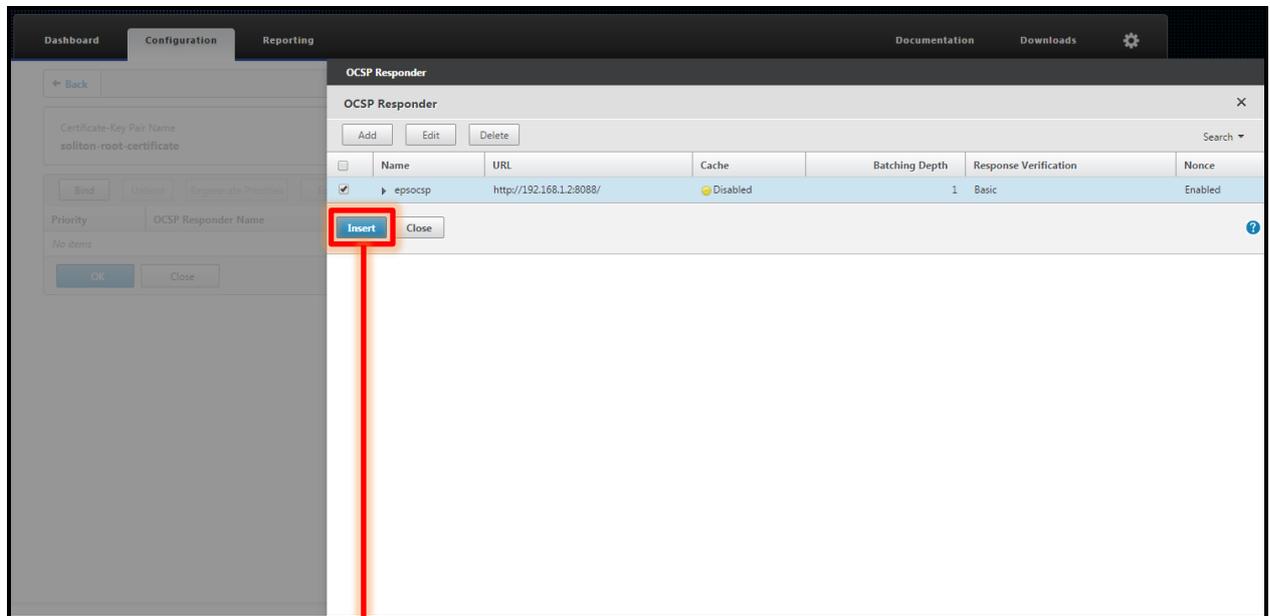
[Traffic Management]-[SSL]-[Certificates]よりインストールした CA 証明書

(soliton-root-certificate)を選択し、「Action」のプルダウンメニューより「OCSP Bindings」をクリックします。

「OCSP Bindings」の右上のペンアイコンをクリックし、その後「Bind」をクリックします。



先ほど作成した「OCSP Responder」設定をチェックし、「Insert」をクリックします。その後「Done」をクリックします。



3-5RADIUS ポリシーの設定

NetScaler で RADIUS ポリシーの設定を行います。

[NetScaler Gateway]-[Policies]-[Authentication]-[RADIUS]より「Servers」タブの「Add」をクリックします。

「Name」、「IP Address」、「Port」、「Secret Key」を入力し、「Create」をクリックします。



← Back

Create Authentication RADIUS Server

Name*

Server Name Server IP

IP Address IPv6

Port

Time-out (seconds) ?

Secret Key*

Confirm Secret Key*

Send Calling Station ID

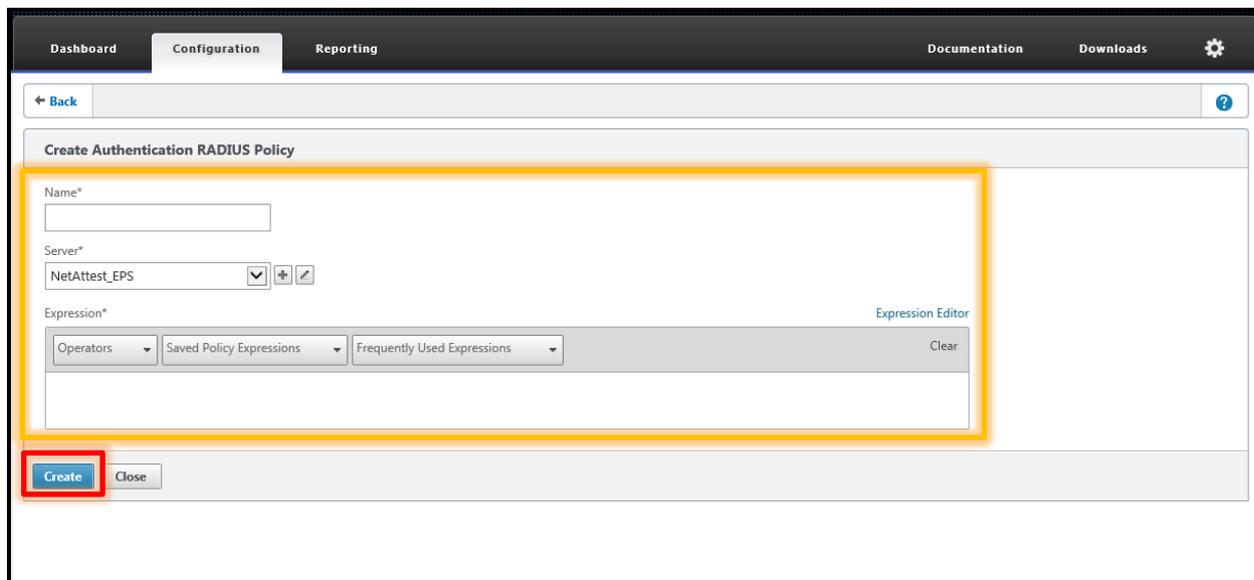
► Details

Create Close

項目	値
Name	NetAttest_EPS
IP Address	192.168.1.2
Port	1812
Secret Key	secret

[NetScaler Gateway]-[Policies]-[Authentication]-[RADIUS]より「Policies」タブの「Add」をクリックします。

「Name」を入力し、「Server」で先ほど作成した RADIUS サーバーを選択します。「Expression」において「ns true」を入力し、「Create」をクリックします。



項目	値
Name	NetAttest_EPS_Policy
Server	NetAttest_EPS を選択
Expression	ns_true

3-6セッションポリシーの設定

NetScaler でセッションの設定を行います。

[NetScaler Gateway]-[Policies]-[Session]より「Profiles」タブの「Add」をクリックします。

「Name」を入力し、「Security」タブの「Default Authorization Action」にチェックを入れ、「ALLOW」を選択します。

Dashboard Configuration Reporting Documentation Downloads

← Back ?

Create NetScaler Gateway Session Profile

Name*

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience **Security** Published Applications

Override Global

Default Authorization Action*

ALLOW

Secure Browse ?

Advanced Settings

Create Close

項目	値
Name	NetAttestEPS_SessionProfile
Default Authorization Action	ALLOW

続いて「Published Applications」タブの「ICA Proxy」をチェックし、「OFF」を選択します。

「Create」をクリックします。

Network Configuration Client Experience Security **Published Applications**

Override Global

ICA Proxy*

OFF

Web Interface Address

Web Interface Address Type*

IPv4

Web Interface Portal Mode*

[NetScaler Gateway]-[Policies]-[Session]より「Policies」タブの「Add」をクリックします。
「Name」を入力し、「Action」で先ほど作成した「Session Profile」を選択します。「Expression」
において「ns_true」を入力し、「Create」をクリックします。

Virtual Server の設定

[NetScaler Gateway]-[Virtual Servers]より「Add」をクリックします。

「Name」、「IPAddress」、「Port」を入力し、「Continue」をクリックします。

VPN Virtual Server

Basic Settings

Name*

IPAddress*
 IPv6

Port*

More

Continue Cancel

項目	値
Name	NetAttest_EPS_Vserver
IPAddress	192.168.3.10
Port	443

続いて、「Certificates」において NetScaler にインポートされたサーバー証明書と CA 証明書を紐付けます。

VPN Virtual Server

Basic Settings

Name	test	Max Users		Double Hop	false
IPAddress	192.168.3.12	Max Login Attempts		Down State Flush	false
Port	443	Failed Login Timeout		AppFlow Logging	false
		State	true	ICA Proxy Session Migration	false
		ICA Only	false	Enable Device Certificate	false
		Enable Authentication	true		

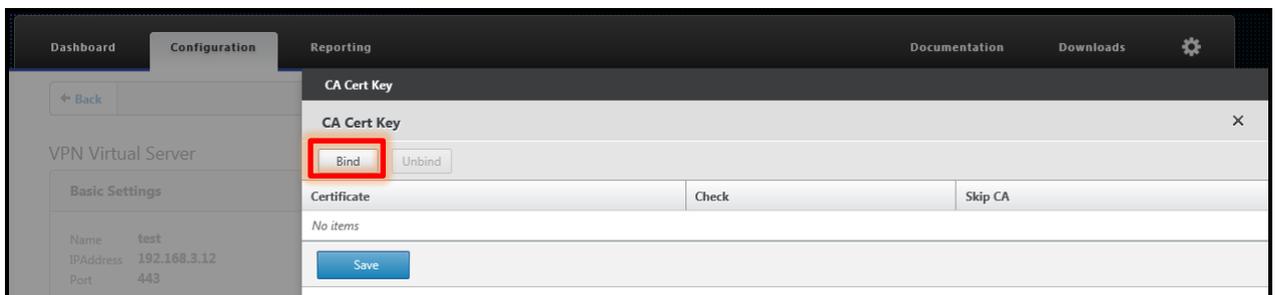
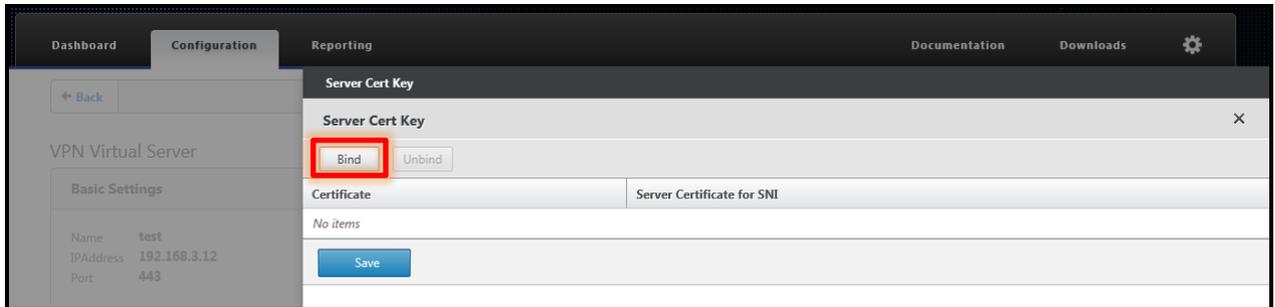
Certificates

No Server Certificate >

No CA Certificate >

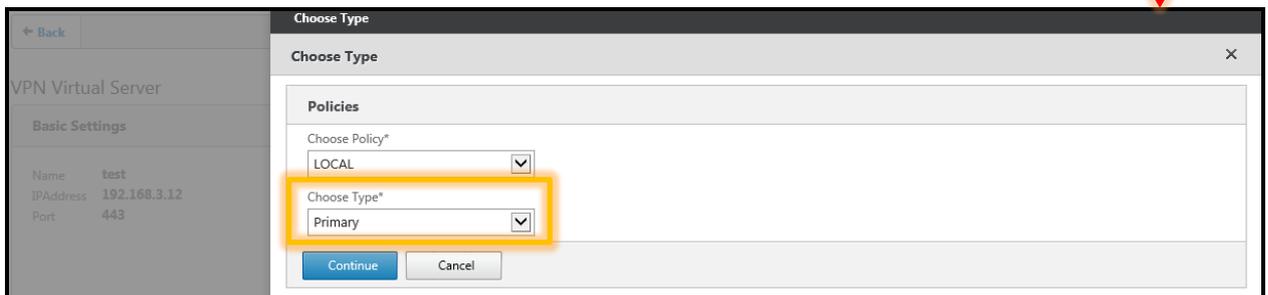
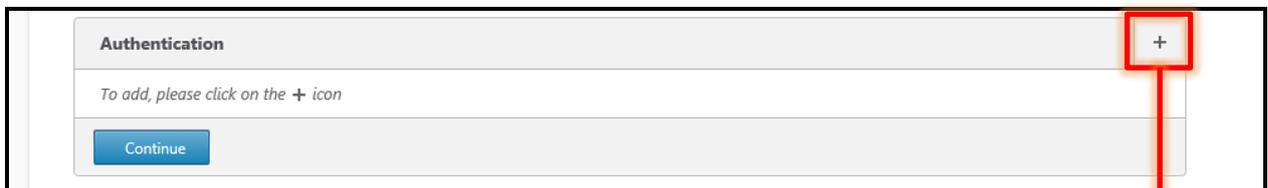
Continue

サーバー証明書、CA 証明書ともに「Bind」をクリックし NetScaler にインポートされた証明書を選択し、「Save」をクリックします。その後「Continue」をクリックします。



続いて「Authentication」の右上の「+」をクリックします。

「Choose Type」で「RADIUS」を選択します。その後「Continue」をクリックします。



項目	値
Choose Type	RADIUS

続いて「SSL Parameters」の右上のペンアイコンをクリックします。

「Client Authentication」にチェックし、「Save」をクリックします。

SSL Parameters	
Enable DH Param	DISABLED
Enable Ephemeral RSA	ENABLED
Refresh Count	0
Enable Session Reuse	ENABLED
Time-out	120
SSL Redirect	DISABLED
Clear Text Port	0
Enable Cipher Redirect	DISABLED
Client Authentication	DISABLED
Send Close-Notify	YES
PUSH Encryption Trigger	Always
SNI Enable	DISABLED
SSLv2 Redirect	DISABLED
SSLv2	DISABLED
SSLv3	ENABLED
TLSv1	ENABLED
TLSv11	ENABLED
TLSv12	ENABLED

SSL Parameters

Enable DH Param
 Enable Ephemeral RSA
Refresh Count:
 Enable Session Reuse
Time-out:
 Enable Cipher Redirect
 SSLv2 Redirect
 Client Authentication

SSL Redirect
 SNI Enable
 Send Close-Notify
Clear Text Port:
PUSH Encryption Trigger:

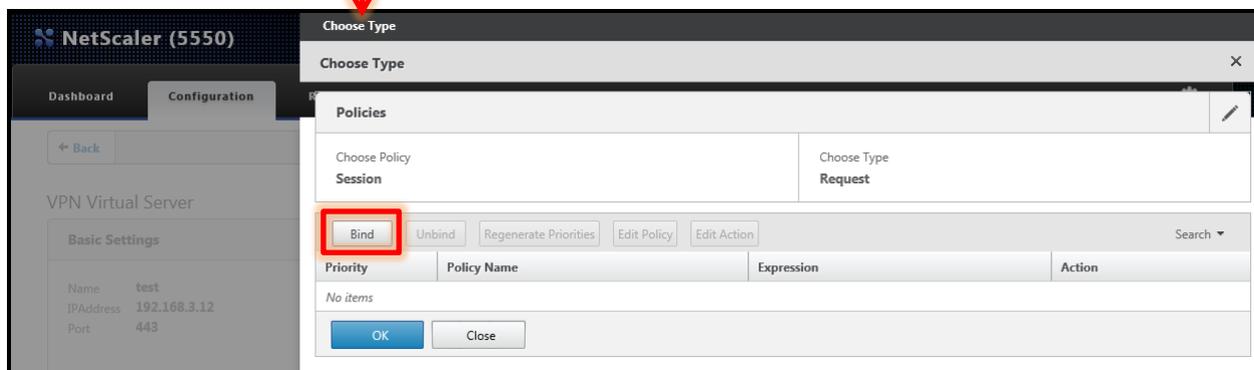
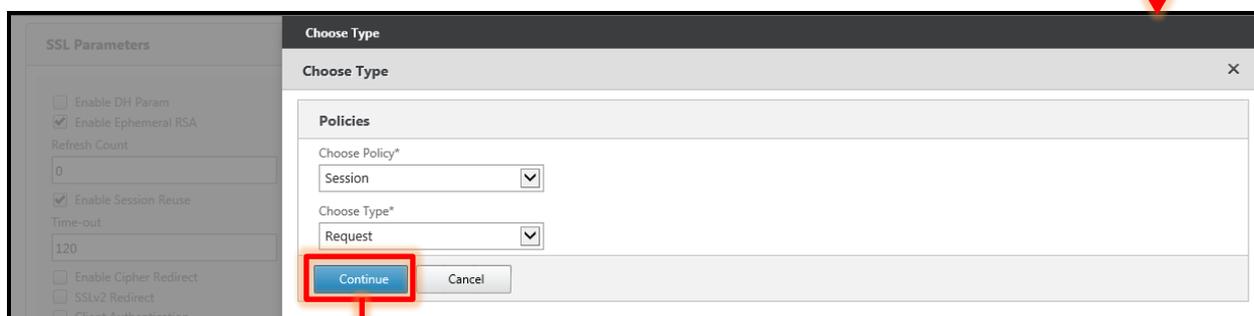
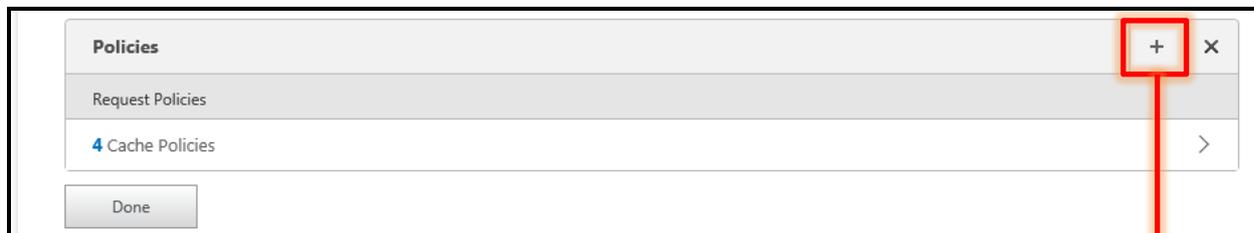
Protocol

SSLv2 SSLv3 TLSv1 TLSv11 TLSv12

続いて「Policies」の右上の「+」をクリックします。

何も変更せずにそのまま「Continue」をクリックします。

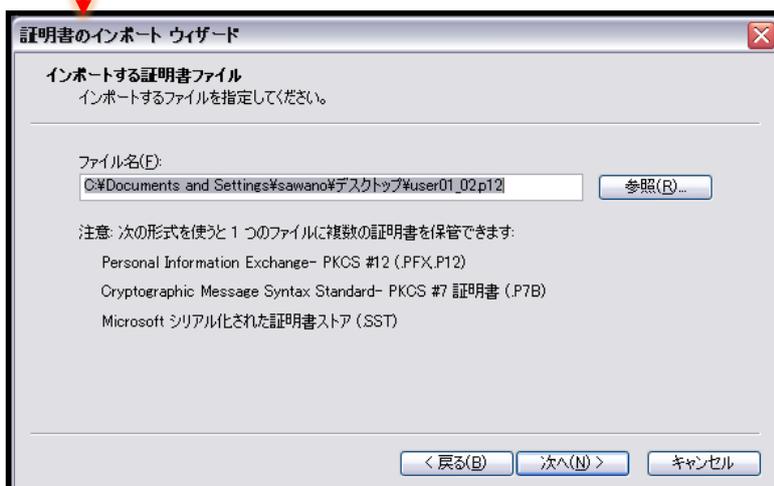
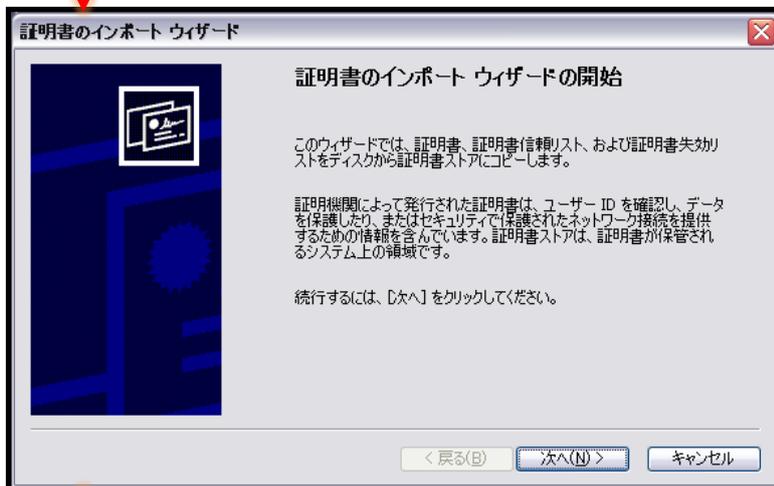
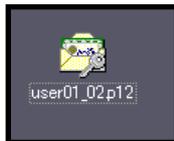
その後、「Bind」をクリックし、[3-6 セッションポリシーの設定]にて作成したポリシーを選択します。「OK」をクリック後、「Done」をクリックします。

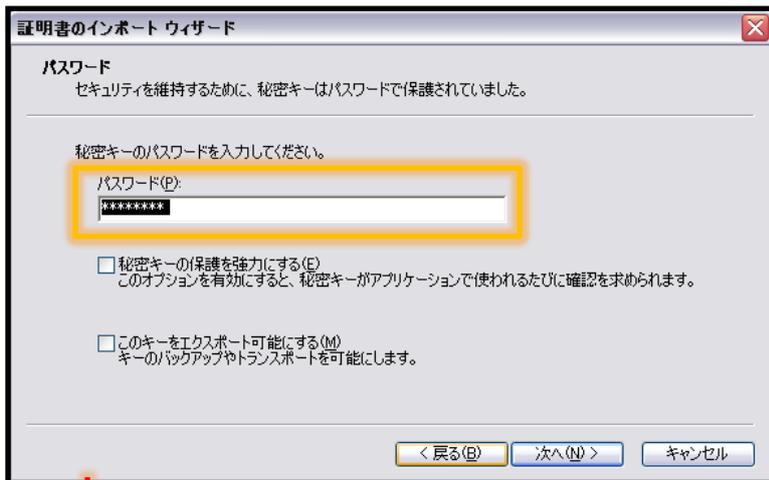


4. VPN クライアントの設定

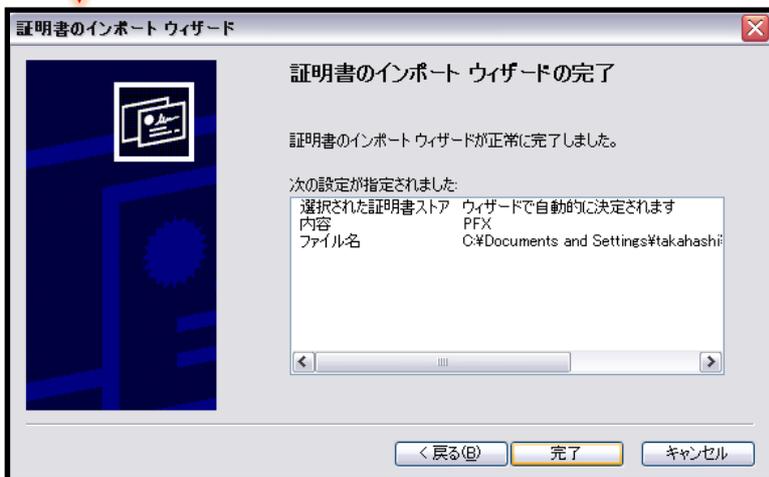
4-1PC へのデジタル証明書のインストール

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



4-2NetScaler Gateway Plug-in のインストール

NetScaler Gateway にアクセスします。External 側のアクセス URL は「https://192.168.3.10/」です。

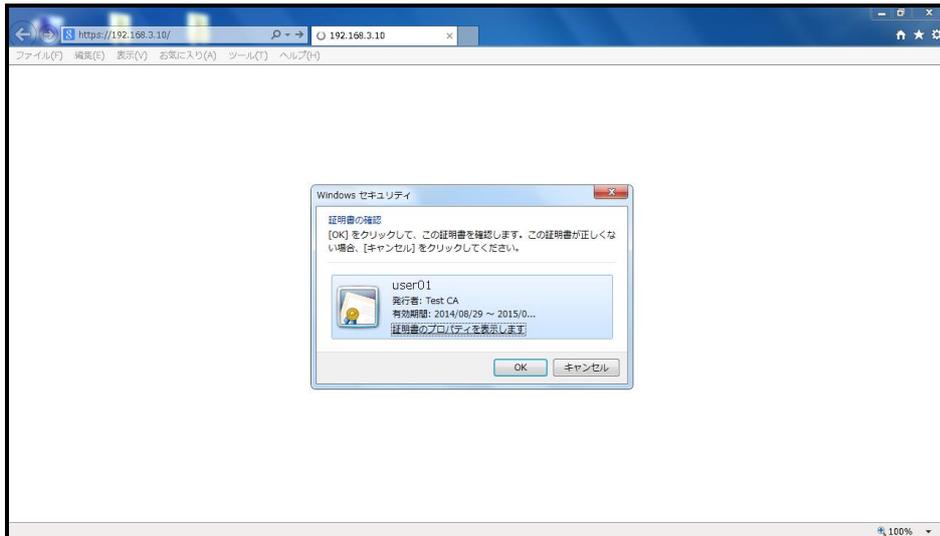
Windows 端末で NetScaler Gateway に初回アクセス行くと、NetScaler Gateway Plug-in のダウンロード画面が表示されます。NetScaler Gateway Plug-in をダウンロードし、インストールを行います。



5. 接続テスト

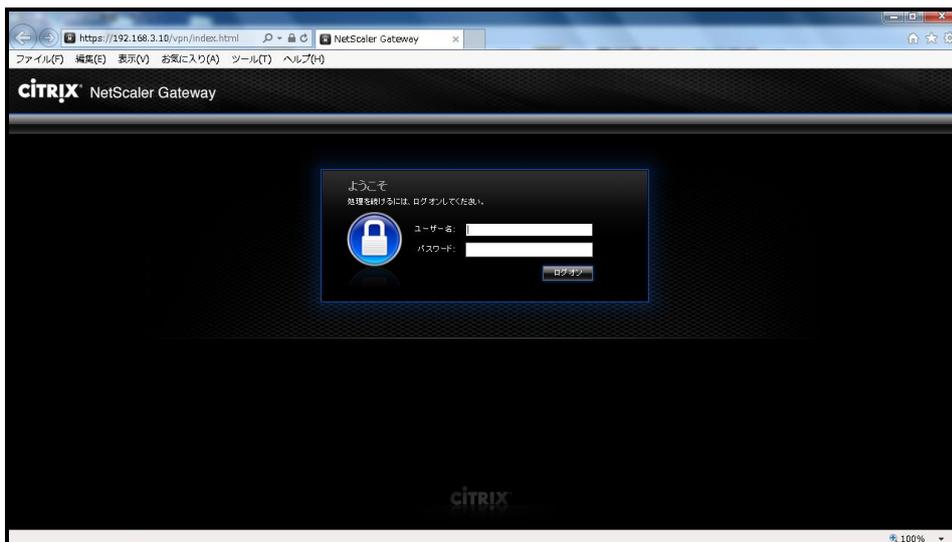
NetScaler Gateway Plug-in がインストールされている端末で、ブラウザを利用して VPN 接続を行います。ブラウザより「https://192.168.3.10/」にアクセスします。

すると、クライアント証明書の提示を求められますので、[4-1 PC へのデジタル証明書のインストール]でインストールしたクライアント証明書を選択し、「OK」をクリックします。。



証明書認証に成功すると、以下の画面が表示されます。

[2-3 認証ユーザーの追加登録]にて NetAttest EPS に登録したユーザーID、パスワードを入力し、「ログオン」をクリックします。



項目	値
ユーザー名	user01
パスワード	password

ログインに成功し、以下の画面が表示されますと、アクセス完了です。

