NetAttest EPS

認証連携設定例

【連携機器】Pulse Secure PSA300

【Case】証明書とユーザーID/パスワード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

本書はオールインワン認証アプライアンス NetAttest EPS と、Pulse Secure 社製 SSL-VPN アプライアンス PSA300 の証明書とパスワードによるハイブリッド認証について設定例を示したものです。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。

アイコンについて

アイコン	説明
ℹ	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 PSA300 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。

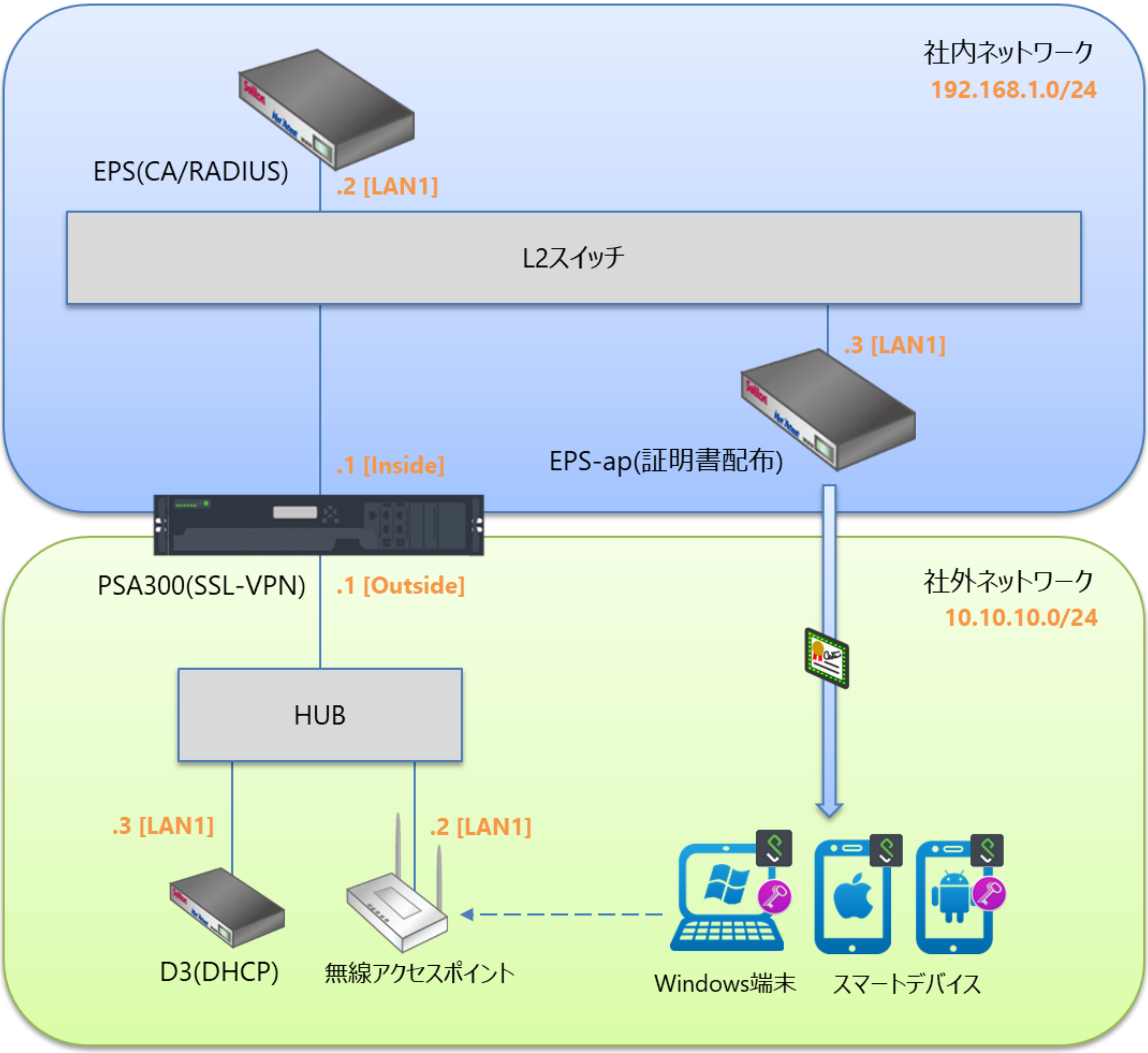
目次

1. 構成

1-1 構成図

以下の環境を構成します。

- 証明書の配布には NetAttest EPS-ap を使用
- 接続するクライアント端末の IP アドレスは、NetAttest D3 の DHCP サーバーから払い出す



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-ST05	ソリトンシステムズ	CA/RADIUS サーバー	4.10.4
PSA300	Pulse Secure	SSL-VPN サーバー	9.0R3.1
VAIO Pro PB	VAIO	クライアント PC	Windows 10 64bit
iPad Air 2	Apple	クライアントタブレット	iOS 12.1.4
Xperia XZ	ソニーモバイルコミュニケーションズ	クライアントスマートフォン	Android 7.0.0
NetAttest EPS-ap-ST05	ソリトンシステムズ	証明書配布サーバー	2.2.5
NetAttest D3-SX15	ソリトンシステムズ	DHCP サーバー	4.2.17

1-2-2 認証方式

デジタル証明書とユーザーID/パスワードによるハイブリッド認証

1-2-3 ネットワーク設定

機器	IP アドレス	RADIUS port (Authentication)	RADIUS Secret (Key)
NetAttest EPS-ST05	192.168.1.2/24	UDP 1812	secret
PSA300	Inside: 192.168.10.1/24 Outside: 10.10.10.1/24		
NetAttest EPS-ap	192.168.1.3/24		
NetAttest D3	10.10.10.3/24		
無線アクセスポイント	10.10.10.2/24	-	-
Client 端末	DHCP	-	-

2. NetAttest EPS の設定

2-1 初期設定ウィザードの実行

NetAttest EPS の初期設定は LAN2(管理インターフェイス)から行います。初期の IP アドレスは「192.168.2.1/24」です。管理端末に適切な IP アドレスを設定し、Internet Explorer から「http://192.168.2.1:2181/」にアクセスしてください。

下記のような流れでセットアップを行います。

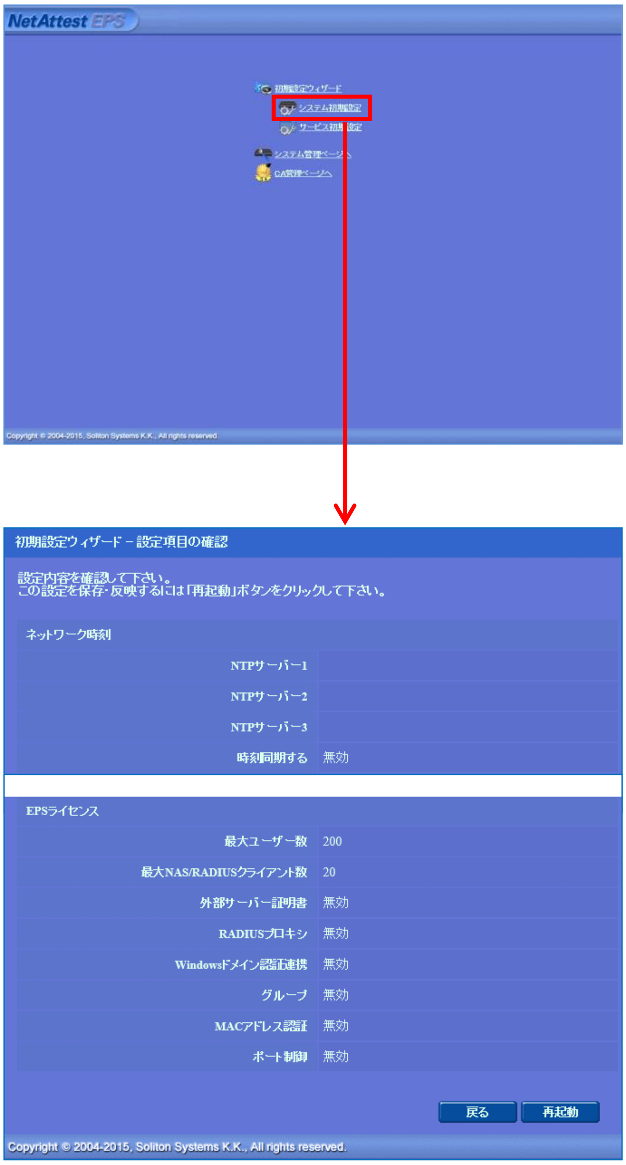
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

2-2 システム初期設定ウィザードの実行

NetAttest EPS の初期設定は LAN2(管理インターフェイス)から行います。初期の IP アドレスは「192.168.2.1/24」です。管理端末に適切な IP アドレスを設定し、Internet Explorer から「http://192.168.2.1:2181/」にアクセスしてください。

その後、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


NetAttest EPS
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
Copyright © 2004-2015, Soliton Systems K.K., All rights reserved.

初期設定ウィザード－設定項目の確認

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。

ネットワーク時刻

NTPサーバー1	
NTPサーバー2	
NTPサーバー3	
時刻同期する	無効

EPSライセンス

最大ユーザー数	200
最大NAS/RADIUSクライアント数	20
外部サーバー証明書	無効
RADIUSプロキシ	無効
Windowsドメイン認証連携	無効
グループ	無効
MACアドレス認証	無効
ポート制御	無効

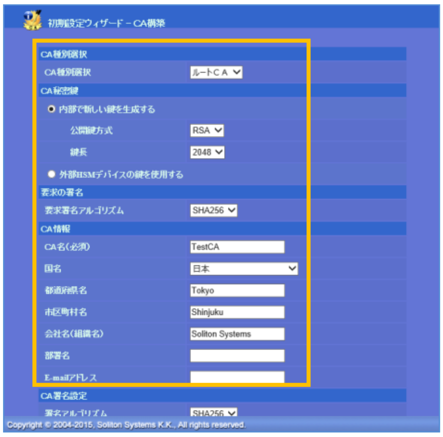
戻る
再起動
Copyright © 2004-2015, Soliton Systems K.K., All rights reserved.

項目	値
ホスト名	naeps.example.com
IP アドレス	デフォルト
ライセンス	なし

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。

- 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（EAP）
- 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

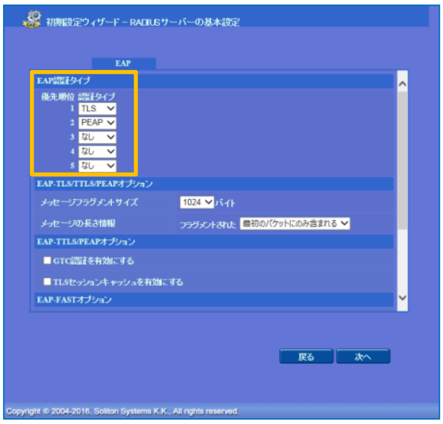


初期設定ウィザード－CA構築

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: SHA256
CA情報
CA名(必須): TestCA
国名: 日本
都道府県名: Tokyo
市区町村名: Shinjuku
会社名(組織名): Soliton Systems
部署名:
E-mailアドレス:
CA署名設定
署名アルゴリズム: SHA256

Copyright © 2004-2015, Soliton Systems K.K., All rights reserved.

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

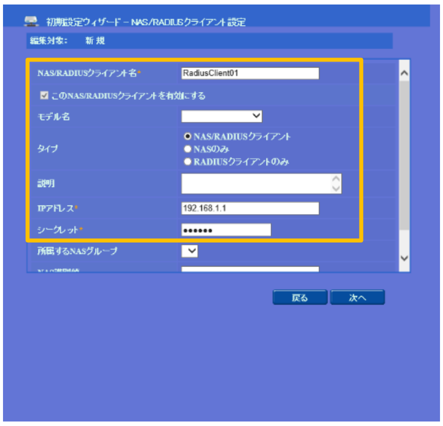


初期設定ウィザード－RADIUSサーバーの基本設定

EAP認証タイプ
優先順位 認証タイプ
1 TLS
2 PEAP
3 なし
4 なし
5 なし
EAP-TLS/TTLS/PEAPオプション
メッセージフラグメントサイズ: 1024 バイト
メッセージの長さ情報: フラグメントされた 最初のパケットにのみ含まれる
EAP-TTLS/PEAPオプション
□ GTC認証を有効にする
□ TLSセッションキャッシュを有効にする
EAP-FASTオプション

Copyright © 2004-2016, Soliton Systems K.K., All rights reserved.

項目	値
優先順位	EAP 認証タイプ
1	TLS
2	PEAP



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

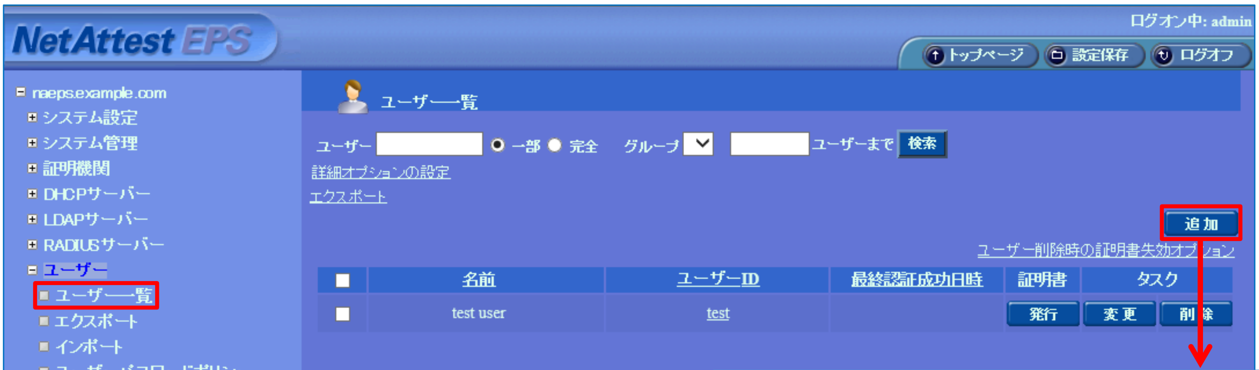
NAS/RADIUSクライアント名*: RadiusClient01
☑ このNAS/RADIUSクライアントを有効にする
モデル名:
タイプ: ● NAS/RADIUSクライアント ○ NASのみ ○ RADIUSクライアントのみ
説明:
IPアドレス*: 192.168.1.1
シークレット*: ••••••
所属するNASグループ:

項目	値
NAS/RADIUS クライアント名	RadiusClient01
IP アドレス	192.168.1.1
シークレット	secret

2-4 ユーザーの登録

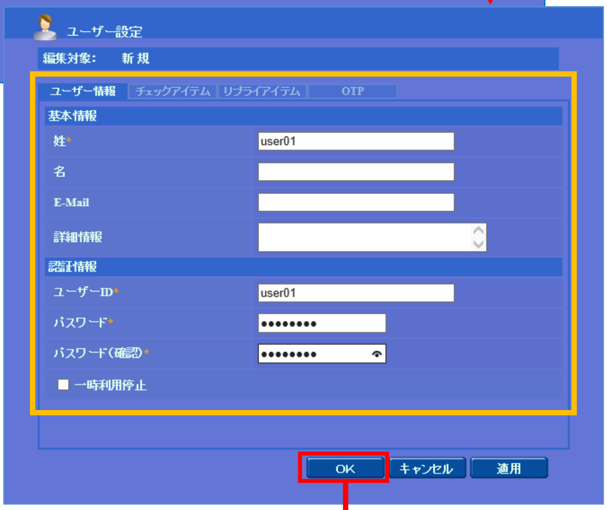
NetAttest EPS の管理画面より、認証ユーザーの登録を行います。

[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。



ユーザー ［　　　　］ ● 一部 ○ 完全　グループ ［　］ ［　　　］ ユーザーまで

□	名前	ユーザーID	最終認証成功日時	証明書	タスク
□	test user	test		発行	変更 削除



編集対象: 新規

基本情報

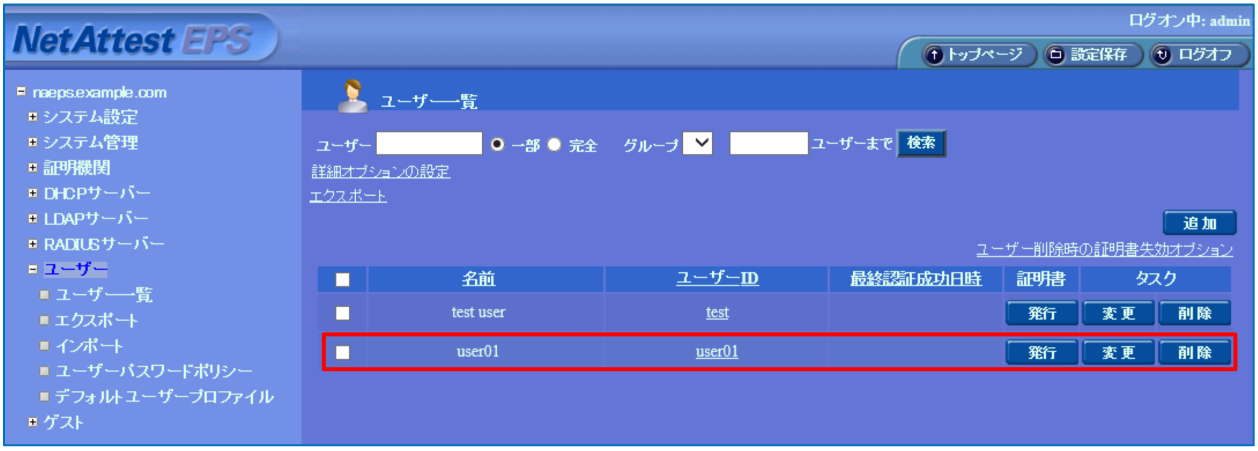
姓*	user01
名	
E-Mail	
詳細情報	

認証情報

ユーザーID*	user01
パスワード*	••••••••
パスワード(確認)*	••••••••

□ 一時利用停止

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



ユーザー ［　　　　］ ● 一部 ○ 完全　グループ ［　］ ［　　　］ ユーザーまで

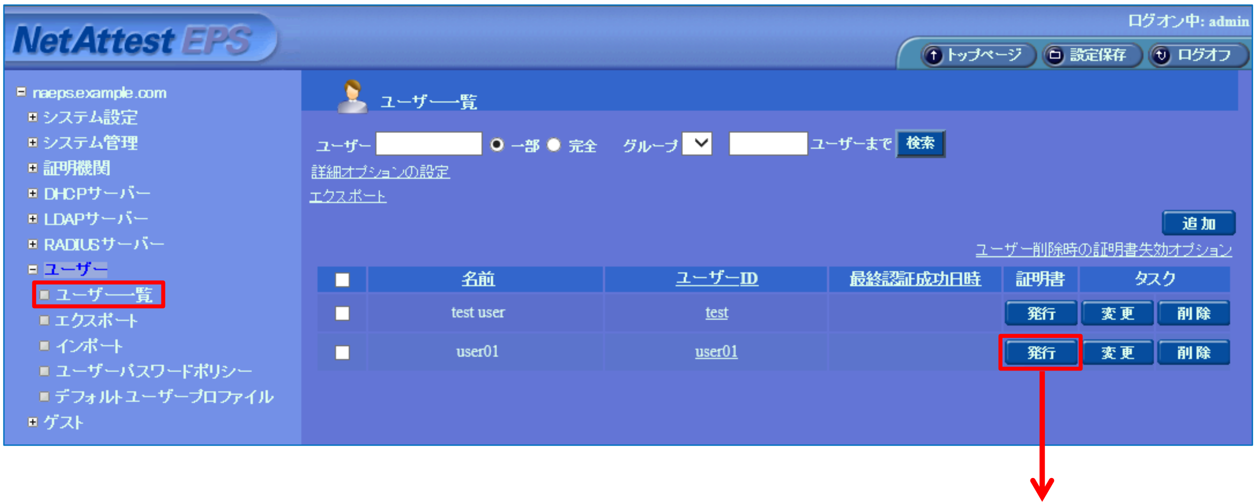
□	名前	ユーザーID	最終認証成功日時	証明書	タスク
□	test user	test		発行	変更 削除
□	user01	user01		発行	変更 削除

2-5 クライアント証明書の発行

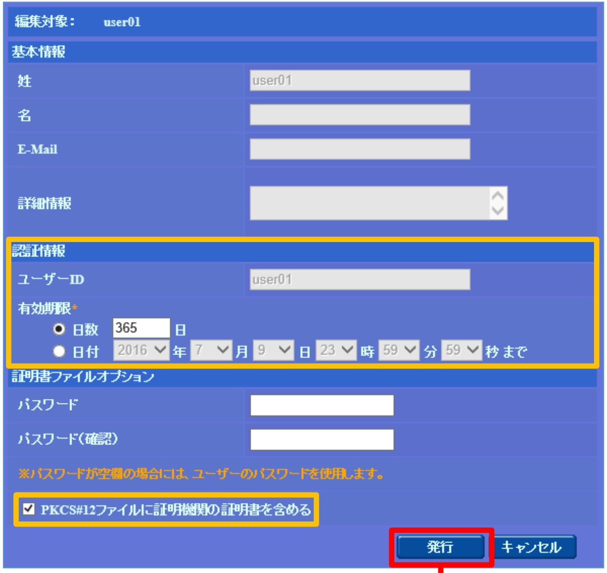
NetAttest EPS の管理画面より、クライアント証明書の発行を行います。

[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.p12 という名前で保存)



□	名前	ユーザーID	最終認証成功日時	証明書	タスク	
□	test user	test		発行	変 更	削 除
□	user01	user01		発行	変 更	削 除



編集対象： user01

基本情報

姓	user01
名	
E-Mail	
詳細情報	

認証情報

ユーザーID	user01

有効期限*
- ● 日数 365 日
- ○ 日付 2016 年 7 月 9 日 23 時 59 分 59 秒 まで

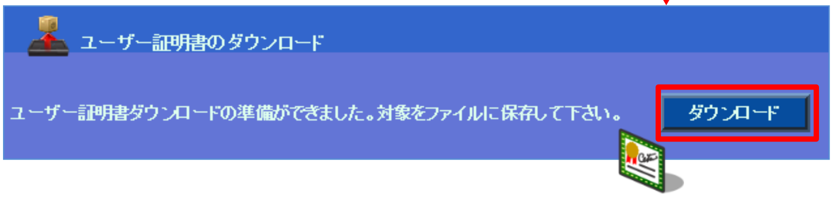
証明書ファイルオプション

パスワード	
パスワード(確認)	

※パスワードが空欄の場合には、ユーザーのパスワードを使用します。

☑ PKCS#12ファイルに証明機関の証明書を含める

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



ユーザー証明書ダウンロードの準備ができました。対象をファイルに保存して下さい。

3. PSA300 の設定

3-1 基本設定

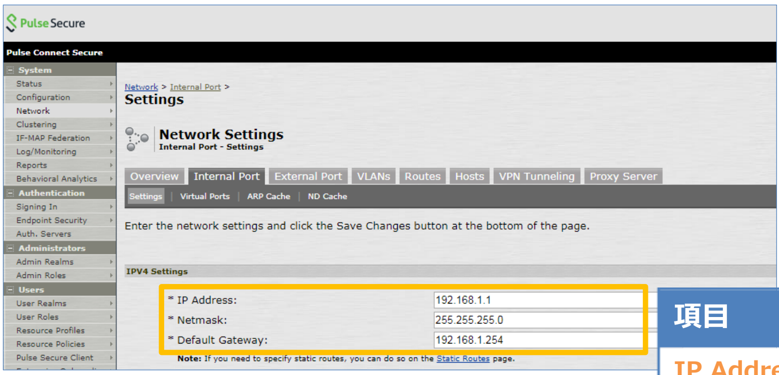
3-1-1 インターフェイスの設定

PSA300 の設定は WebUI で行います。(サブネットの設定は CLI から)

PSA300 のインターフェイスの設定は、下記の通りです。

【Ethernet0】Internal Port

社内 LAN に接続。管理 interface としても使用



Network > Internal Port >
Settings

Network Settings
Internal Port - Settings

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

IPV4 Settings

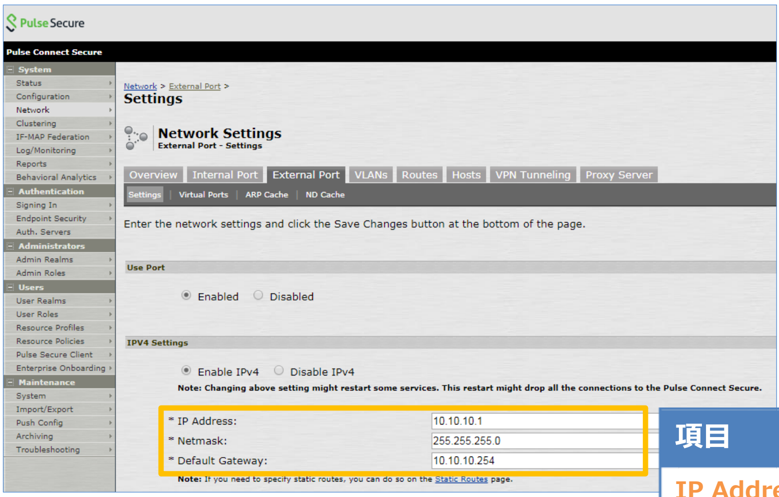
* IP Address:	192.168.1.1
* Netmask:	255.255.255.0
* Default Gateway:	192.168.1.254

Note: If you need to specify static routes, you can do so on the Static Routes page.

項目	値
IP Address	192.168.1.1
Netmask	255.255.255.0
Default Gateway	192.168.1.254

【Ethernet1】External Port

Pulse Secure クライアントによる接続を受付ける interface



Network > External Port >
Settings

Network Settings
External Port - Settings

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

Use Port

● Enabled ○ Disabled

IPV4 Settings

● Enable IPv4 ○ Disable IPv4

Note: Changing above setting might restart some services. This restart might drop all the connections to the Pulse Connect Secure.

* IP Address:	10.10.10.1
* Netmask:	255.255.255.0
* Default Gateway:	10.10.10.254

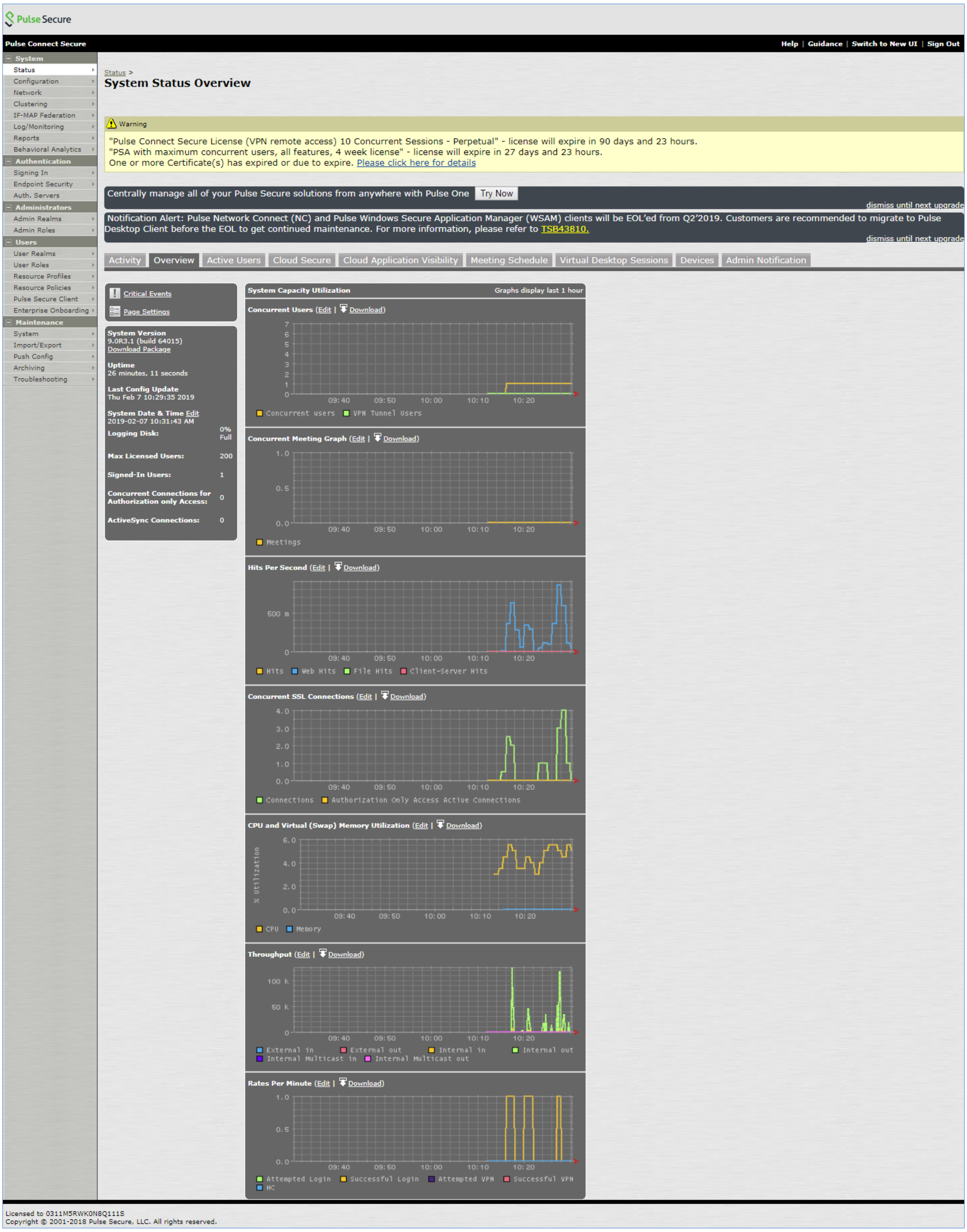
Note: If you need to specify static routes, you can do so on the Static Routes page.

項目	値
IP Address	10.10.10.1
Netmask	255.255.255.0
Default Gateway	10.10.10.254

3-1-2 システム時刻設定

NetAttest EPS と同じ時刻を設定します。

[Status]-[System Date & Time]-[Edit]から設定します。



System Status Overview

Warning

"Pulse Connect Secure License (VPN remote access) 10 Concurrent Sessions - Perpetual" - license will expire in 90 days and 23 hours.
"PSA with maximum concurrent users, all features, 4 week license" - license will expire in 27 days and 23 hours.
One or more Certificate(s) has expired or due to expire. Please click here for details

Centrally manage all of your Pulse Secure solutions from anywhere with Pulse One

Notification Alert: Pulse Network Connect (NC) and Pulse Windows Secure Application Manager (WSAM) clients will be EOL'ed from Q2'2019. Customers are recommended to migrate to Pulse Desktop Client before the EOL to get continued maintenance. For more information, please refer to TSB43810.

System Version
9.0R3.1 (build 64015)
Download Package

Uptime
26 minutes, 11 seconds

Last Config Update
Thu Feb 7 10:29:35 2019

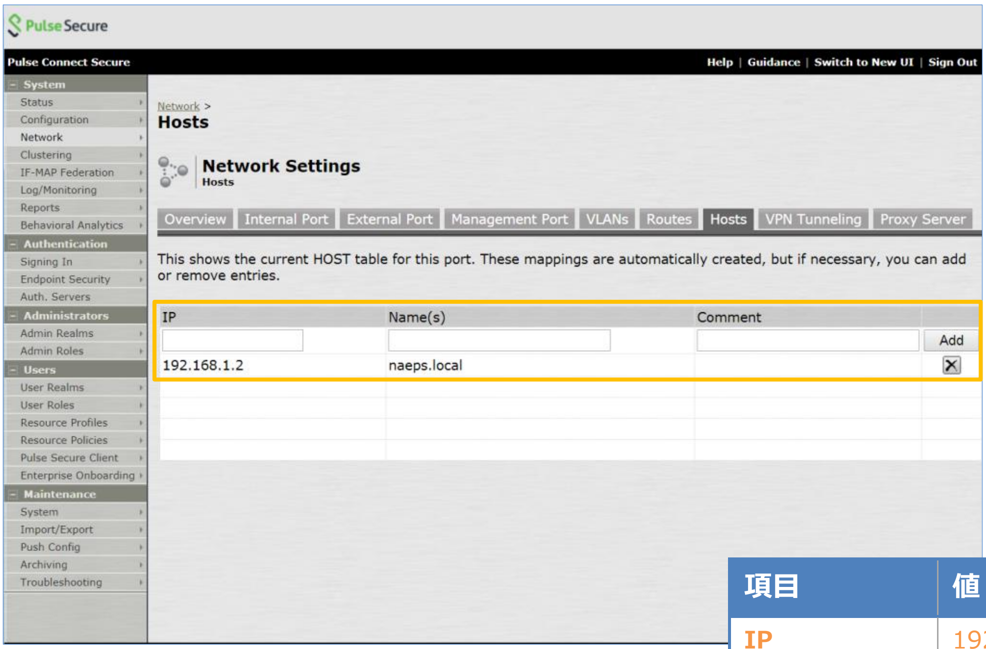
System Date & Time Edit
2019-02-07 10:31:43 AM

Logging Disk:	0% Full
Max Licensed Users:	200
Signed-In Users:	1
Concurrent Connections for Authorization only Access:	0
ActiveSync Connections:	0

Licensed to 0311M5RWK0N8Q111S
Copyright © 2001-2018 Pulse Secure, LLC. All rights reserved.

3-1-3 Hosts 設定(任意)

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



This shows the current HOST table for this port. These mappings are automatically created, but if necessary, you can add or remove entries.

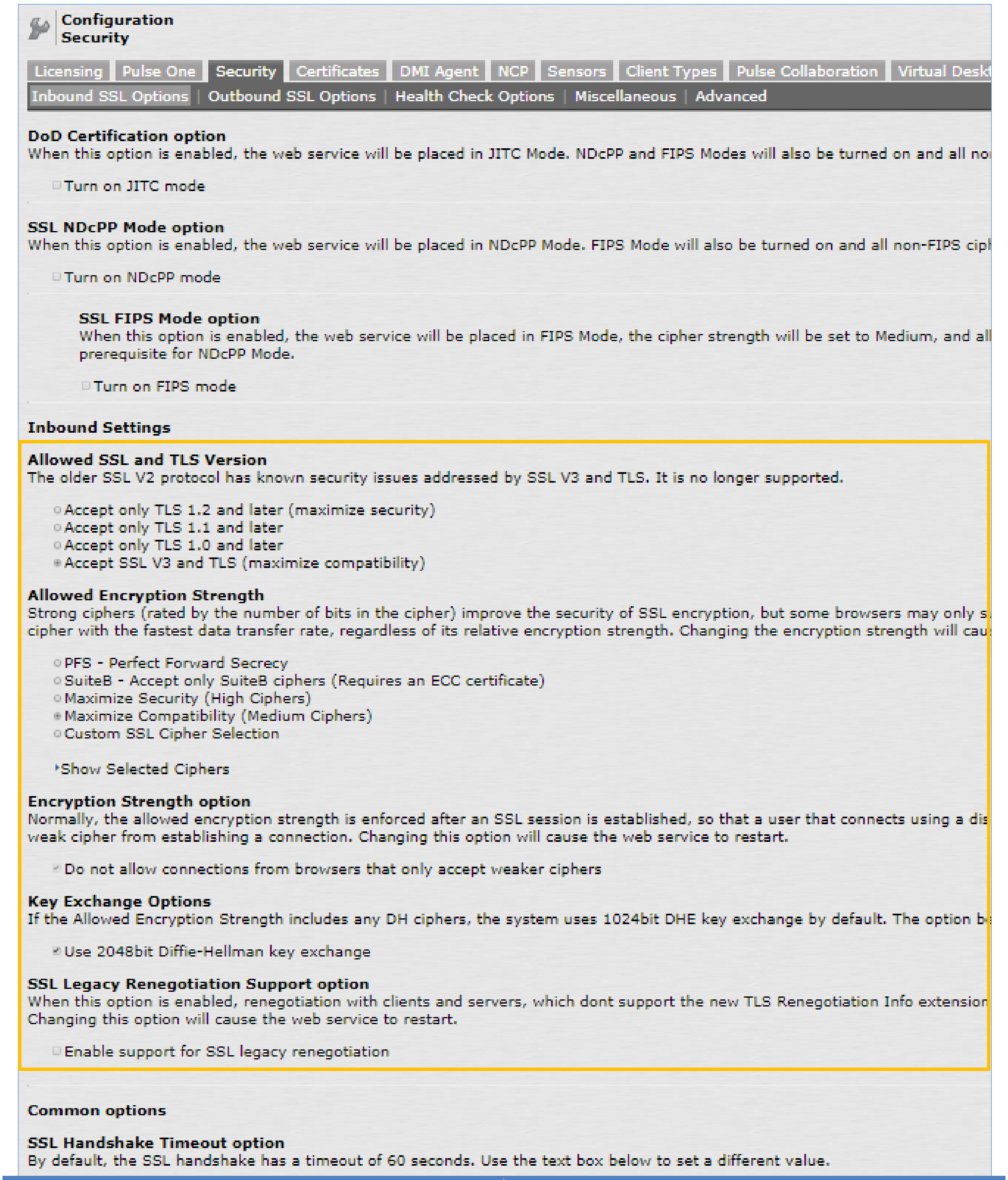
IP	Name(s)	Comment
192.168.1.2	naeps.local	

項目	値
IP	192.168.1.2
Name	naeps.local

3-2 PSA300 の証明書に関する設定

3-2-1 SSL に関する設定(参考) (PSA300)

SSL に関するセキュリティ設定を行います。[Configuration]-[Security]から設定します。



Configuration
Security
Licensing | Pulse One | Security | Certificates | DMI Agent | NCP | Sensors | Client Types | Pulse Collaboration | Virtual Deskt
Inbound SSL Options | Outbound SSL Options | Health Check Options | Miscellaneous | Advanced

DoD Certification option
When this option is enabled, the web service will be placed in JITC Mode. NDcPP and FIPS Modes will also be turned on and all no

□ Turn on JITC mode

SSL NDcPP Mode option
When this option is enabled, the web service will be placed in NDcPP Mode. FIPS Mode will also be turned on and all non-FIPS ciph

□ Turn on NDcPP mode

SSL FIPS Mode option
When this option is enabled, the web service will be placed in FIPS Mode, the cipher strength will be set to Medium, and all prerequisite for NDcPP Mode.

□ Turn on FIPS mode

Inbound Settings

Allowed SSL and TLS Version
The older SSL V2 protocol has known security issues addressed by SSL V3 and TLS. It is no longer supported.

○ Accept only TLS 1.2 and later (maximize security)
○ Accept only TLS 1.1 and later
○ Accept only TLS 1.0 and later
● Accept SSL V3 and TLS (maximize compatibility)

Allowed Encryption Strength
Strong ciphers (rated by the number of bits in the cipher) improve the security of SSL encryption, but some browsers may only s cipher with the fastest data transfer rate, regardless of its relative encryption strength. Changing the encryption strength will cau

○ PFS - Perfect Forward Secrecy
○ SuiteB - Accept only SuiteB ciphers (Requires an ECC certificate)
○ Maximize Security (High Ciphers)
● Maximize Compatibility (Medium Ciphers)
○ Custom SSL Cipher Selection

▸Show Selected Ciphers

Encryption Strength option
Normally, the allowed encryption strength is enforced after an SSL session is established, so that a user that connects using a dis weak cipher from establishing a connection. Changing this option will cause the web service to restart.

☑ Do not allow connections from browsers that only accept weaker ciphers

Key Exchange Options
If the Allowed Encryption Strength includes any DH ciphers, the system uses 1024bit DHE key exchange by default. The option be

☑ Use 2048bit Diffie-Hellman key exchange

SSL Legacy Renegotiation Support option
When this option is enabled, renegotiation with clients and servers, which dont support the new TLS Renegotiation Info extension Changing this option will cause the web service to restart.

□ Enable support for SSL legacy renegotiation

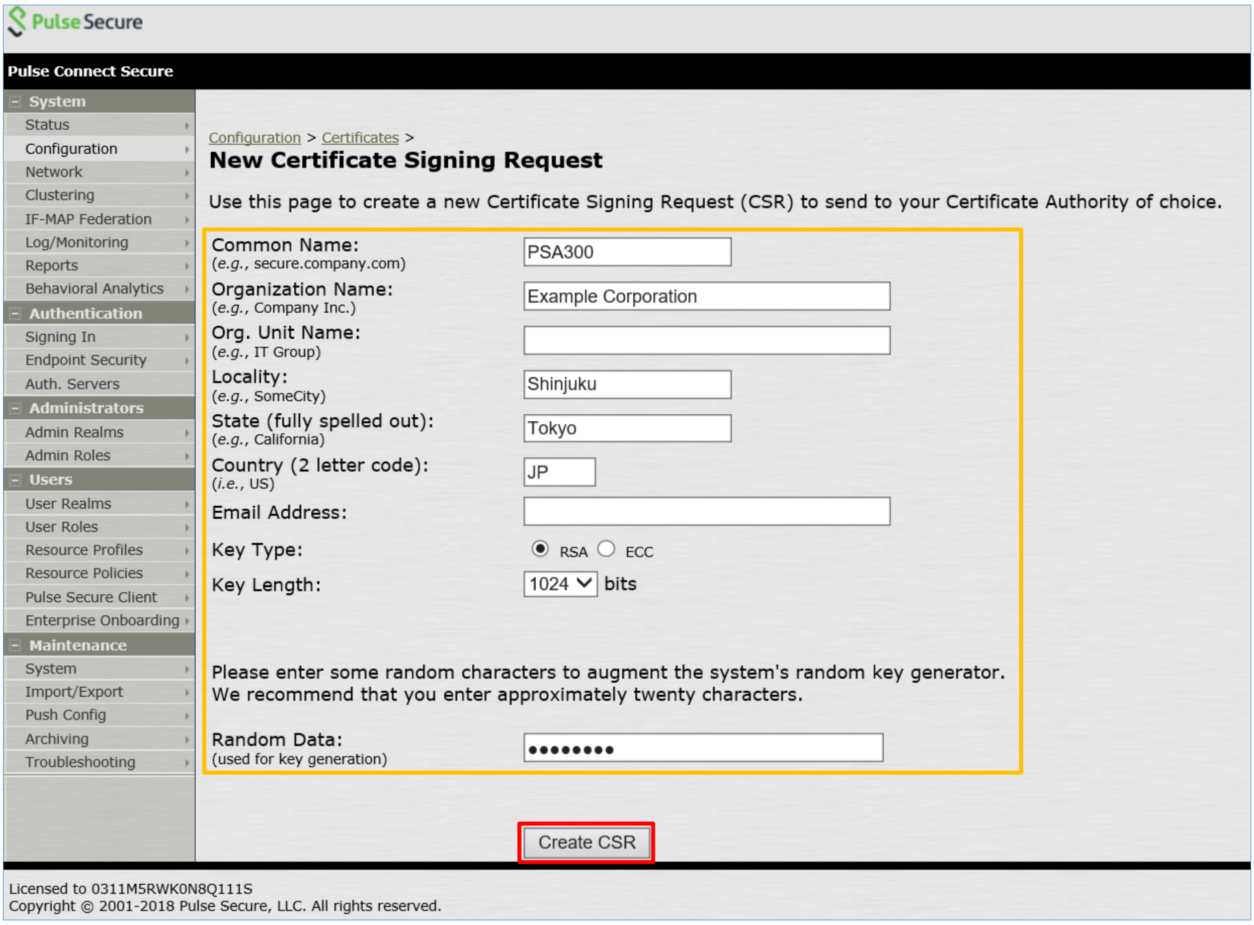
Common options

SSL Handshake Timeout option
By default, the SSL handshake has a timeout of 60 seconds. Use the text box below to set a different value.

項目	値
Allowed SSL and TLS Version	Accept Only SSL V3 and TLS V1
Allowed Encryption Strength	Accept Only 128-bit and greater
SSL Legacy Renegotiation Support option	Enable support for SSL legacy renegotiation

3-2-2 CSR の生成(PSA300)

PSA300 で CSR(Certificate Signing Request)を生成します。
[Configuration]-[Certificates]-[Device Certificates]の「New CSR」より
CSR を作成します。「Create CSR」をクリックすると、以下の画面に遷移します。



Configuration > Certificates >

New Certificate Signing Request

Use this page to create a new Certificate Signing Request (CSR) to send to your Certificate Authority of choice.

Common Name: (*e.g.*, secure.company.com)	PSA300
Organization Name: (*e.g.*, Company Inc.)	Example Corporation
Org. Unit Name: (*e.g.*, IT Group)	
Locality: (*e.g.*, SomeCity)	Shinjuku
State (fully spelled out): (*e.g.*, California)	Tokyo
Country (2 letter code): (*i.e.*, US)	JP
Email Address:	
Key Type:	● RSA ○ ECC
Key Length:	1024 bits

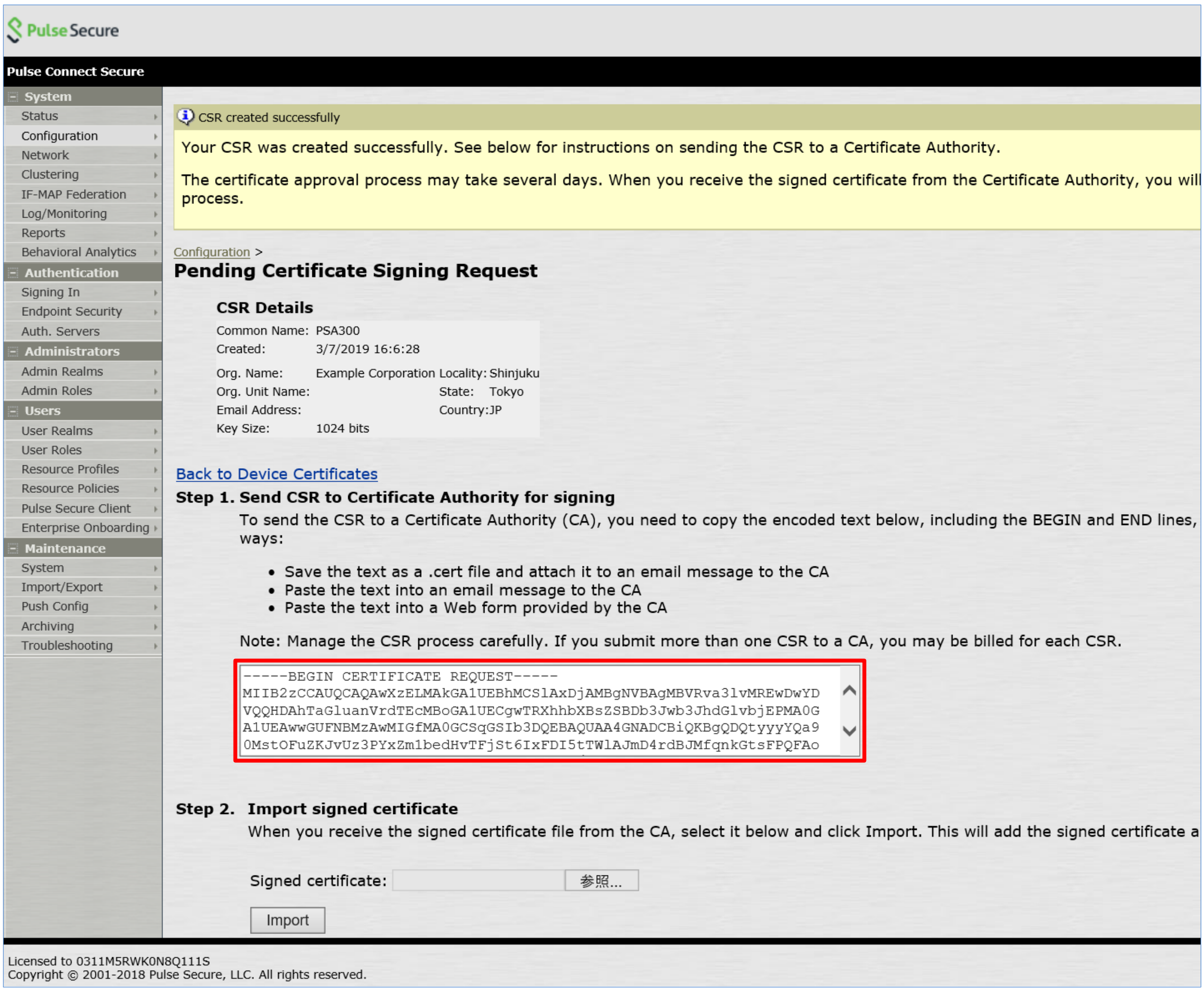
Please enter some random characters to augment the system's random key generator.
We recommend that you enter approximately twenty characters.

Random Data: ••••••••
(used for key generation)

Licensed to 0311M5RWK0N8Q111S
Copyright © 2001-2018 Pulse Secure, LLC. All rights reserved.

項目	値
Common Name	PSA300
Organization Name	Example Corporation
Locality	Shinjuku
State	Tokyo
Country	JP
Random Data	password

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



CSR created successfully

Your CSR was created successfully. See below for instructions on sending the CSR to a Certificate Authority.

The certificate approval process may take several days. When you receive the signed certificate from the Certificate Authority, you will process.

Configuration >

Pending Certificate Signing Request

CSR Details

Common Name: PSA300
Created: 3/7/2019 16:6:28
Org. Name: Example Corporation Locality: Shinjuku
Org. Unit Name: State: Tokyo
Email Address: Country:JP
Key Size: 1024 bits

Back to Device Certificates

Step 1. Send CSR to Certificate Authority for signing

To send the CSR to a Certificate Authority (CA), you need to copy the encoded text below, including the BEGIN and END lines, ways:

- Save the text as a .cert file and attach it to an email message to the CA
- Paste the text into an email message to the CA
- Paste the text into a Web form provided by the CA

Note: Manage the CSR process carefully. If you submit more than one CSR to a CA, you may be billed for each CSR.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB2zCCAUQCAQAwXzELMAkGA1UEBhMCSlAxDjAMBgNVBAgMBVRva3lvMREwDwYD
VQQHDAhTaGluanVrdTEcMBoGA1UECgwTRXhhbXBsZSBDb3Jwb3JhdGlvbjEPMA0G
A1UEAwwGUFNBMzAwMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDQtyyyYQa9
0MstOFuZKJvUz3PYxZm1bedHvTFjSt6IxFDI5tTWlAJmD4rdBJMfqnkGtsFPQFAo
```

Step 2. Import signed certificate

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

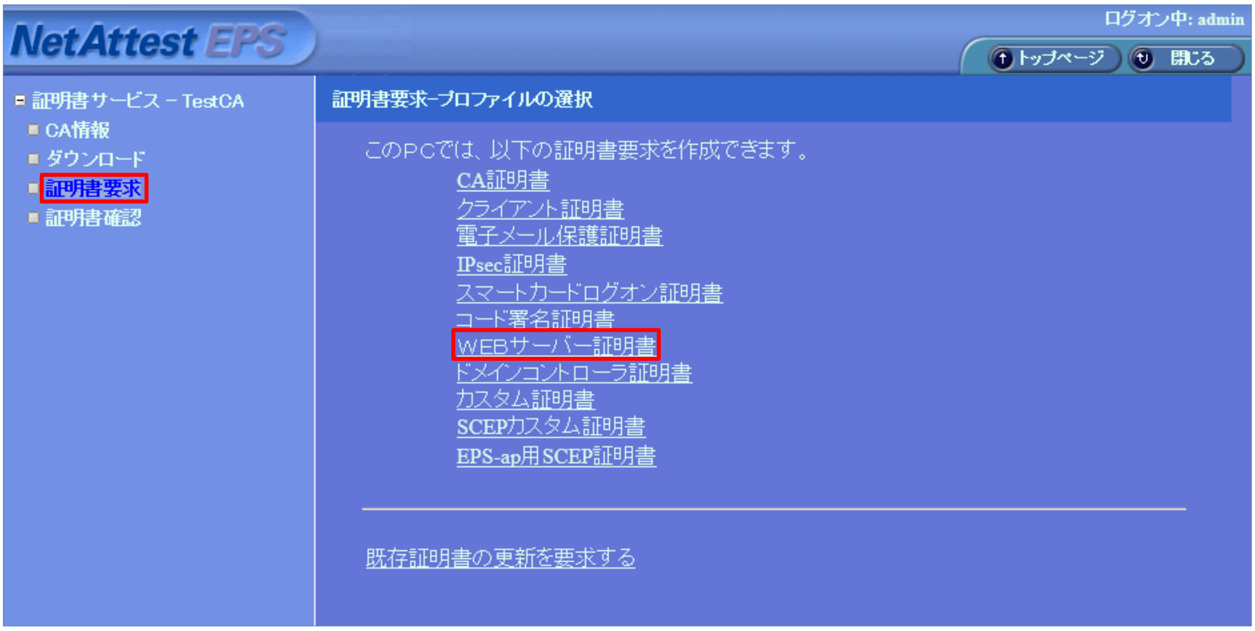
Signed certificate: 参照...

Import

Licensed to 0311M5RWK0N8Q111S
Copyright © 2001-2018 Pulse Secure, LLC. All rights reserved.

3-2-3 サーバー証明書署名要求（NetAttest EPS）

PSA300 で生成した CSR を基に NetAttest EPS で PSA300 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(https://192.168.1.2/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。

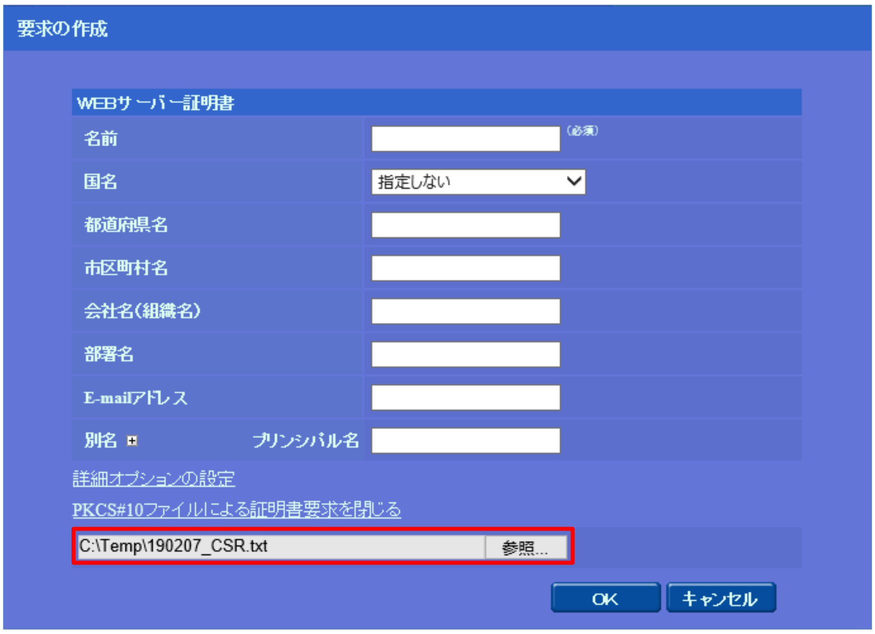


証明書要求－プロファイルの選択

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
- EPS-ap用SCEP証明書

既存証明書の更新を要求する


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	
別名 ⊞ プリンシパル名	

詳細オプションの設定

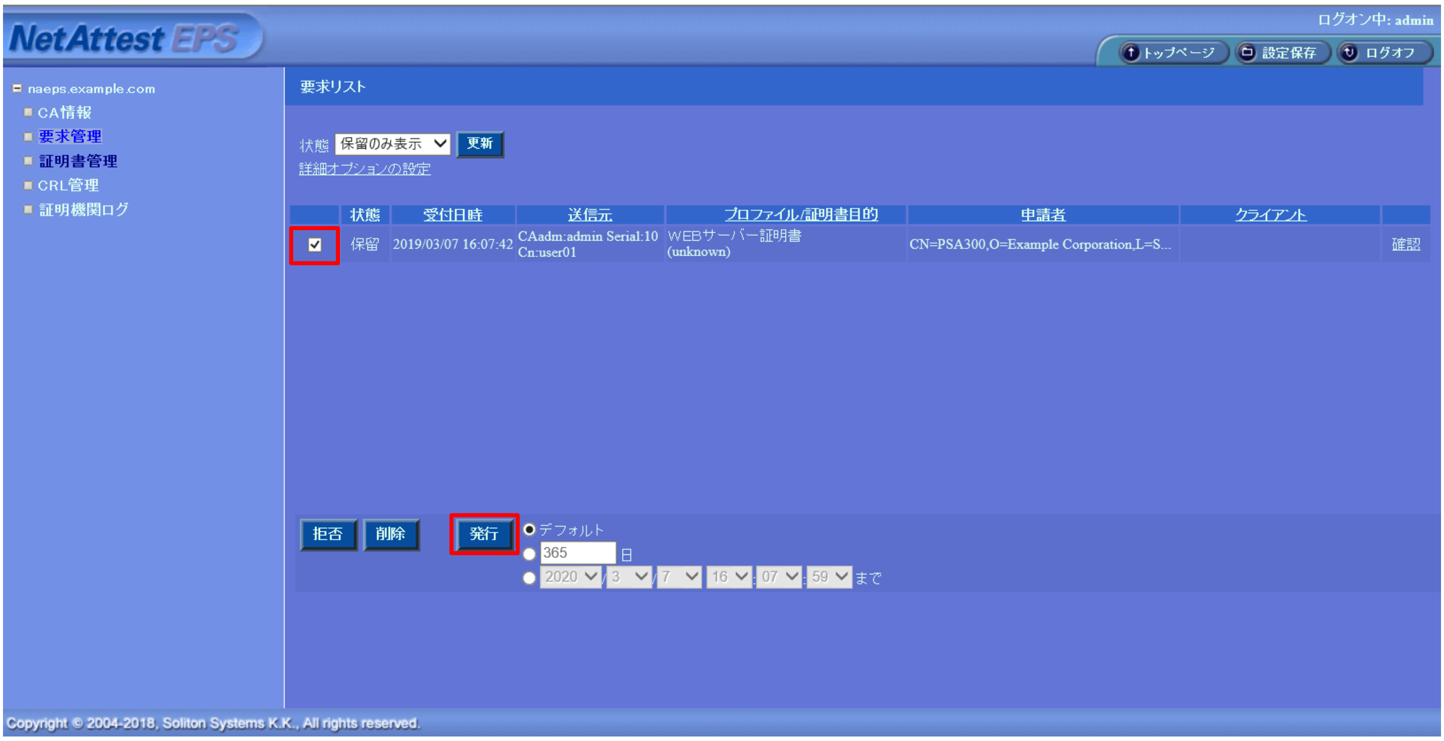
PKCS#10ファイルによる証明書要求を閉じる

C:\Temp\190207_CSR.txt

3-2-4 サーバー証明書の発行（NetAttest EPS）

サーバー証明書要求の承認・発行を行います。

CA 管理ページ(http://192.168.2.1:2181/caadmin/)にアクセスし、「保留」状態のサーバー証明書を発行します。



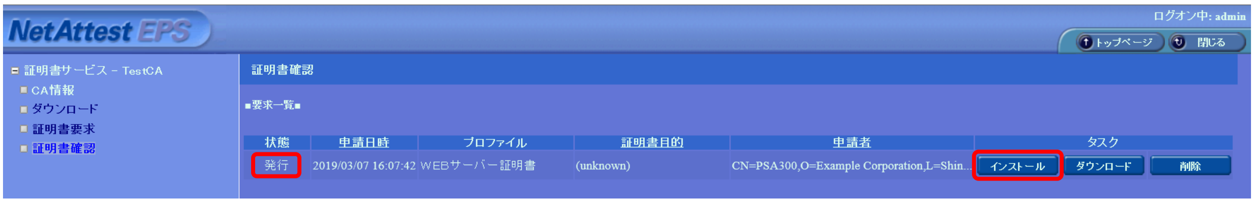
状態 保留のみ表示

	状態	受付日時	送信元	プロファイル/証明書目的	申請者	クライアント	
☑	保留	2019/03/07 16:07:42	CAadm:admin Serial:10 Cn:user01	WEBサーバー証明書 (unknown)	CN=PSA300,O=Example Corporation,L=S...		確認

● デフォルト
○ 365 日
○ 2020 / 3 / 7 16 : 07 : 59 まで

3-2-5 サーバー証明書のダウンロード（NetAttest EPS）

サーバー証明書をダウンロードするために再度、管理者向け証明書サービスページにアクセスします。「証明書の確認」を選択すると状態が「発行」になっていますので、サーバー証明書をダウンロードします。



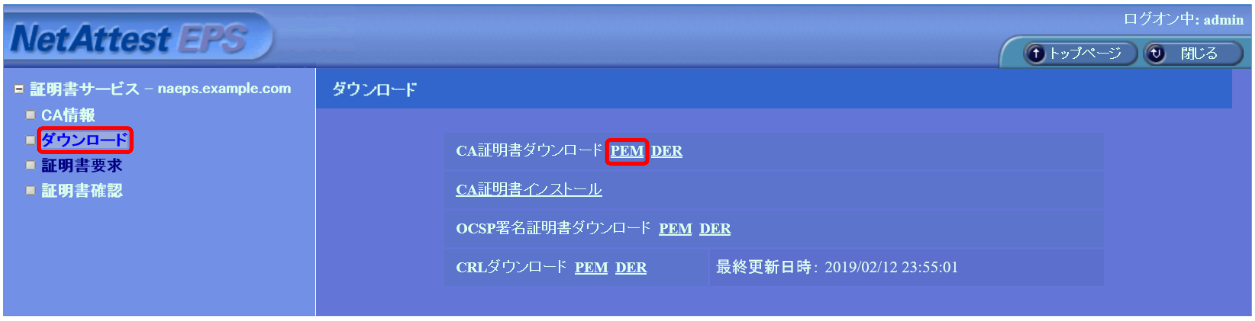
証明書確認

■要求一覧■

状態	申請日時	プロファイル	証明書目的	申請者	タスク
発行	2019/03/07 16:07:42	WEBサーバー証明書	(unknown)	CN=PSA300,O=Example Corporation,L=Shin...	インストール ダウンロード 削除

3-2-6 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 形式を選択します。



ダウンロード

CA証明書ダウンロード PEM DER

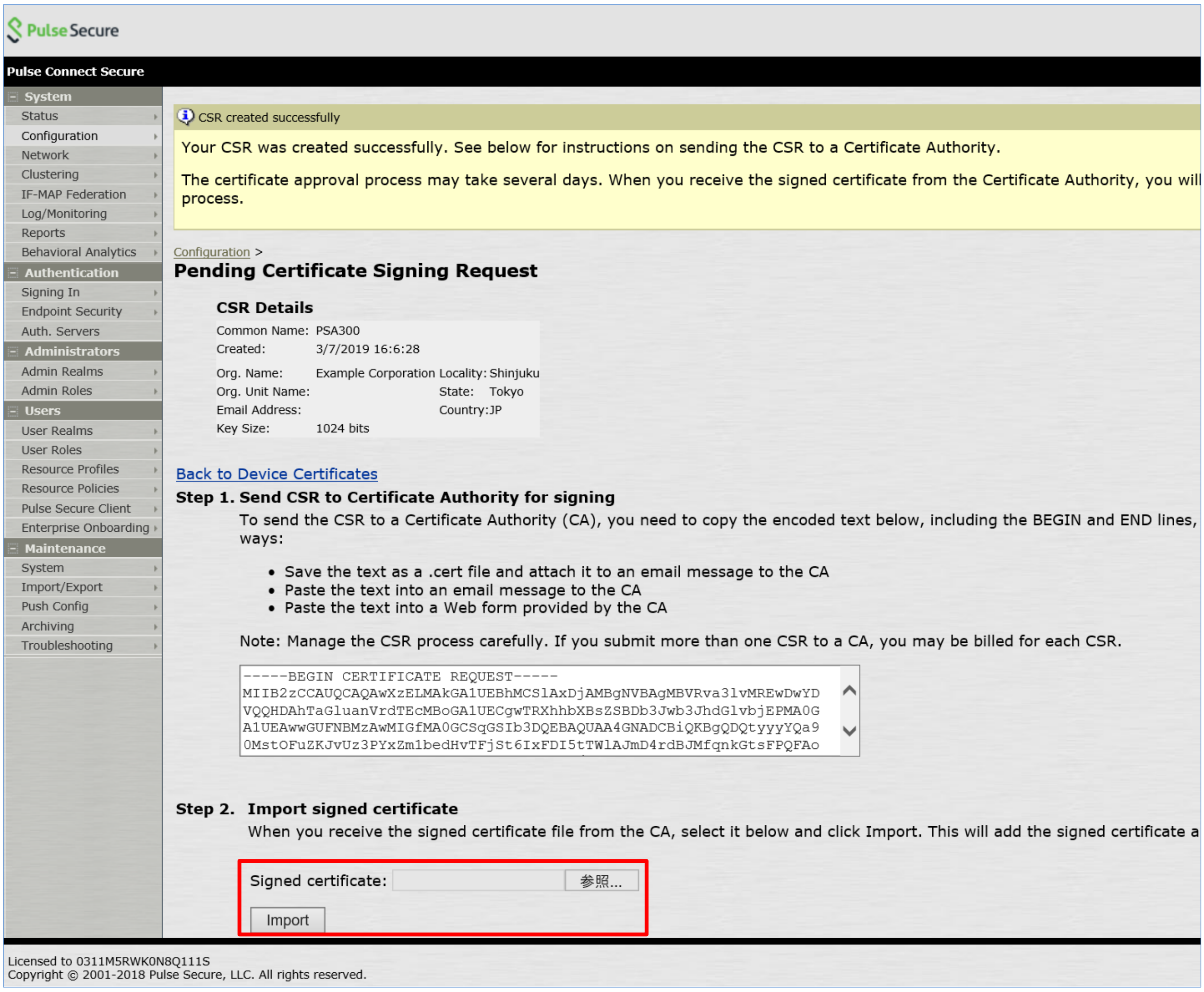
CA証明書インストール

OCSP署名証明書ダウンロード PEM DER

CRLダウンロード PEM DER　最終更新日時: 2019/02/12 23:55:01

3-2-7 サーバー証明書のインポート（PSA300）

NetAttest EPS で発行したサーバー証明書をインポートします。CSR を作成したページの[Step 2. Import signed certificate]で、サーバー証明書(nausercert-pem.cer)をインポートします。



CSR created successfully

Your CSR was created successfully. See below for instructions on sending the CSR to a Certificate Authority.

The certificate approval process may take several days. When you receive the signed certificate from the Certificate Authority, you will process.

Configuration >

Pending Certificate Signing Request

CSR Details

Common Name: PSA300
Created: 3/7/2019 16:6:28
Org. Name: Example Corporation Locality: Shinjuku
Org. Unit Name: State: Tokyo
Email Address: Country:JP
Key Size: 1024 bits

Back to Device Certificates

Step 1. Send CSR to Certificate Authority for signing

To send the CSR to a Certificate Authority (CA), you need to copy the encoded text below, including the BEGIN and END lines, ways:

- Save the text as a .cert file and attach it to an email message to the CA
- Paste the text into an email message to the CA
- Paste the text into a Web form provided by the CA

Note: Manage the CSR process carefully. If you submit more than one CSR to a CA, you may be billed for each CSR.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB2zCCAUQCAQAwXzELMAkGA1UEBhMCSlAxDjAMBgNVBAgMBVRva3lvMREwDwYD
VQQHDAhTaGluanVrdTEcMBoGA1UECgwTRXhhbXBsZSBDb3Jwb3JhdGlvbjEPMA0G
A1UEAwwGUFNBMzAwMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDQtyyyYQa9
0MstOFuZKJvUz3PYxZm1bedHvTFjSt6IxFDI5tTWlAJmD4rdBJMfqnkGtsFPQFAo
```

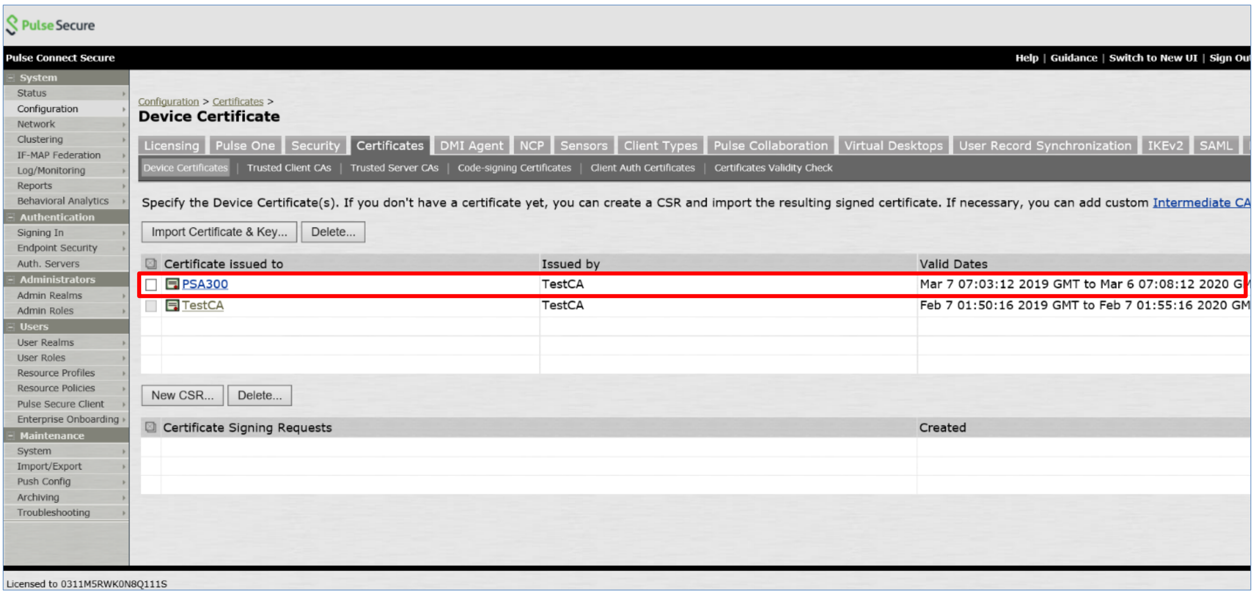
Step 2. Import signed certificate

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

Signed certificate: 参照...

Import

Licensed to 0311M5RWK0N8Q111S
Copyright © 2001-2018 Pulse Secure, LLC. All rights reserved.



Configuration > Certificates >

Device Certificate

Specify the Device Certificate(s). If you don't have a certificate yet, you can create a CSR and import the resulting signed certificate. If necessary, you can add custom Intermediate CA

Import Certificate & Key... Delete...

Certificate issued to	Issued by	Valid Dates
□ PSA300	TestCA	Mar 7 07:03:12 2019 GMT to Mar 6 07:08:12 2020 G
□ TestCA	TestCA	Feb 7 01:50:16 2019 GMT to Feb 7 01:55:16 2020 GM

New CSR... Delete...

Certificate Signing Requests	Created

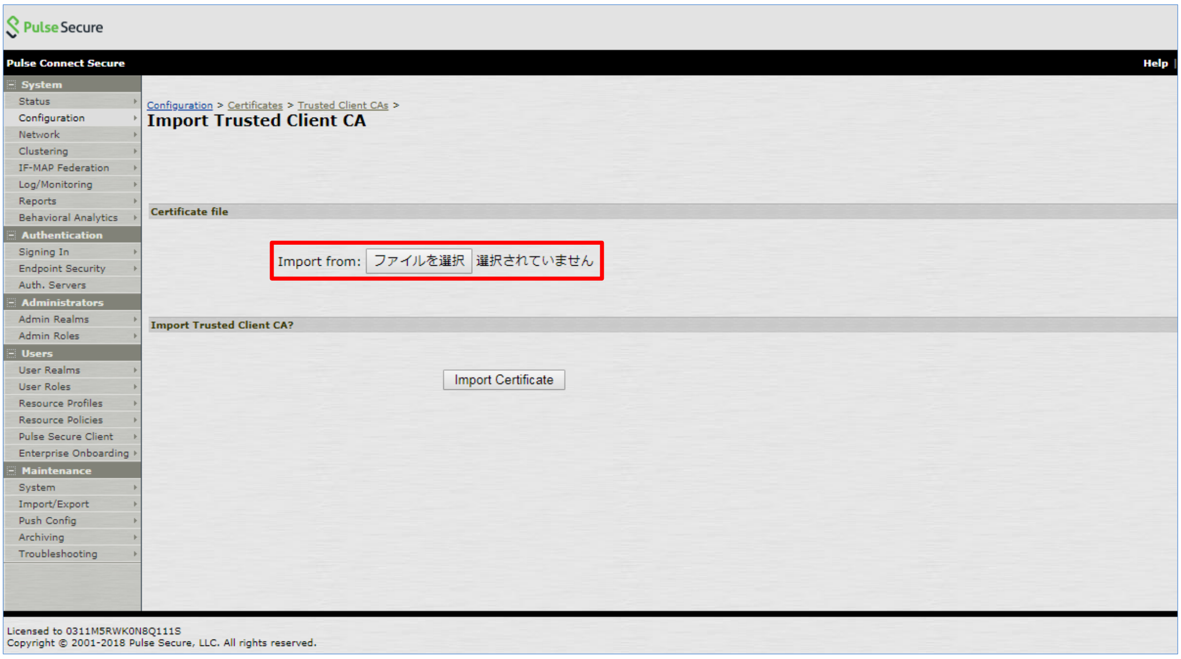
Licensed to 0311M5RWK0N8Q111S

3-2-8 CA 証明書のインポート（PSA300）

NetAttest EPS からダウンロードした CA 証明書を PSA300 にインポートします。

[Configuration]-[Certificates]-[Trusted Client CAs]の「Import CA Certificate」から、CA 証明書(nacacert-pem.cer)をインポートします。

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



Configuration > Certificates > Trusted Client CAs >

Import Trusted Client CA

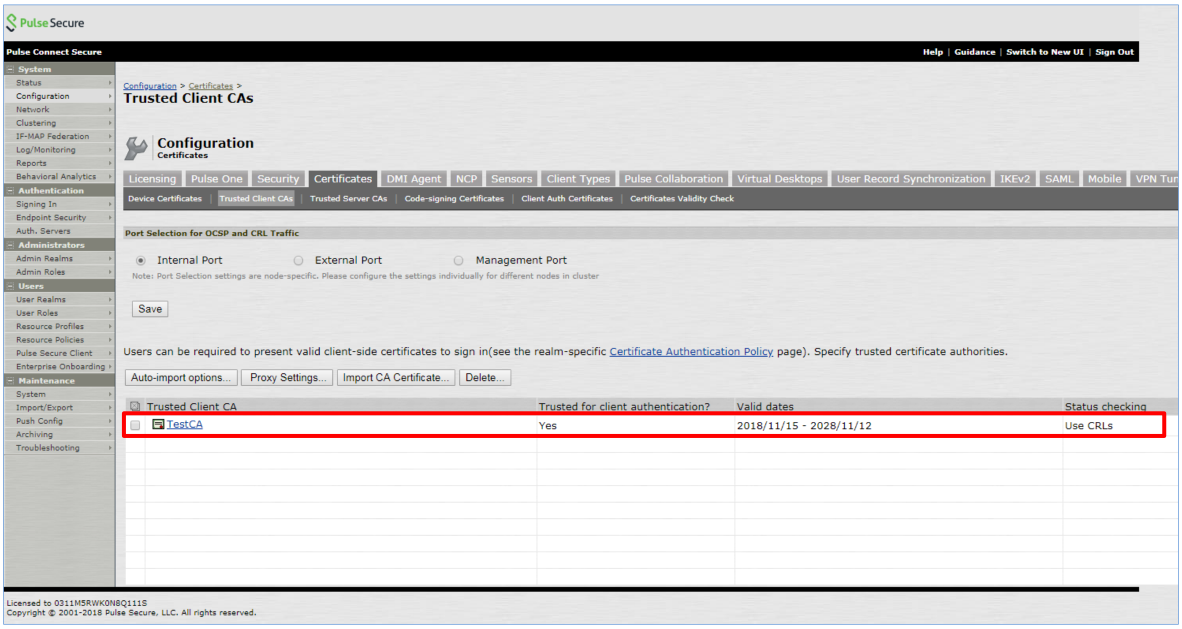
Certificate file

Import from: ファイルを選択 選択されていません

Import Trusted Client CA?

Import Certificate

Licensed to 0311M5RWK0N8Q111S
Copyright © 2001-2018 Pulse Secure, LLC. All rights reserved.



Configuration > Certificates >

Trusted Client CAs

Port Selection for OCSP and CRL Traffic

● Internal Port ○ External Port ○ Management Port

Note: Port Selection settings are node-specific. Please configure the settings individually for different nodes in cluster

Save

Users can be required to present valid client-side certificates to sign in(see the realm-specific Certificate Authentication Policy page). Specify trusted certificate authorities.

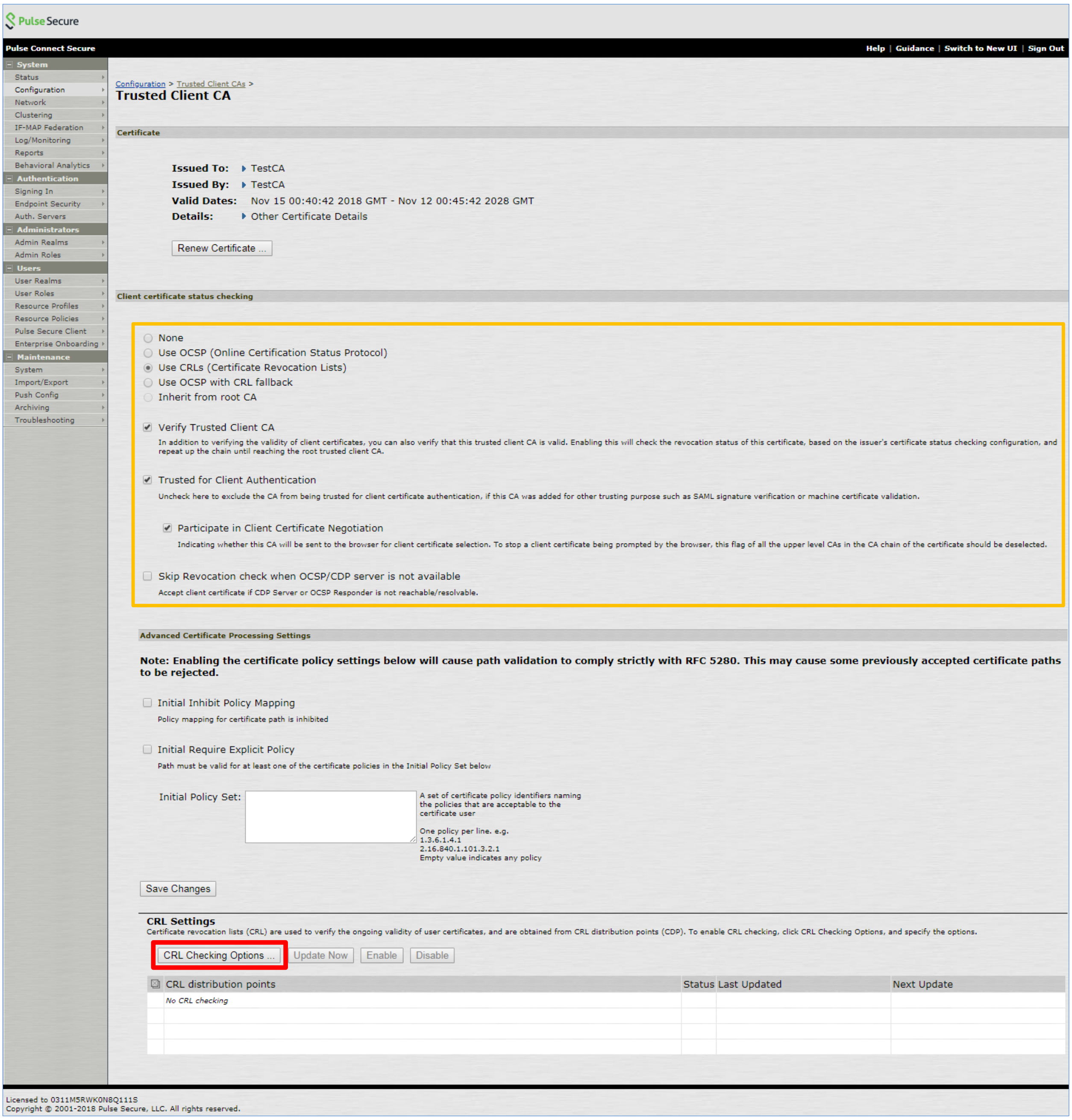
Auto-import options... | Proxy Settings... | Import CA Certificate... | Delete...

☒	Trusted Client CA	Trusted for client authentication?	Valid dates	Status checking
□	TestCA	Yes	2018/11/15 - 2028/11/12	Use CRLs

Licensed to 0311M5RWK0N8Q111S
Copyright © 2001-2018 Pulse Secure, LLC. All rights reserved.

「Client certificate status checking」のいくつかの項目にチェックを入れ、

次に、「CRL Checking Options」をクリックします。



Configuration > Trusted Client CAs >

Trusted Client CA

Certificate

Issued To: TestCA
Issued By: TestCA
Valid Dates: Nov 15 00:40:42 2018 GMT - Nov 12 00:45:42 2028 GMT
Details: Other Certificate Details

Renew Certificate ...

Client certificate status checking

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

☑ Verify Trusted Client CA
In addition to verifying the validity of client certificates, you can also verify that this trusted client CA is valid. Enabling this will check the revocation status of this certificate, based on the issuer's certificate status checking configuration, and repeat up the chain until reaching the root trusted client CA.

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

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

□ Skip Revocation check when OCSP/CDP server is not available
Accept client certificate if CDP Server or OCSP Responder is not reachable/resolvable.

Advanced Certificate Processing Settings

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

□ Initial Inhibit Policy Mapping
Policy mapping for certificate path is inhibited

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

Initial Policy Set:
A set of certificate policy identifiers naming the policies that are acceptable to the certificate user

One policy per line. e.g.
1.3.6.1.4.1
2.16.840.1.101.3.2.1
Empty value indicates any policy

Save Changes

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

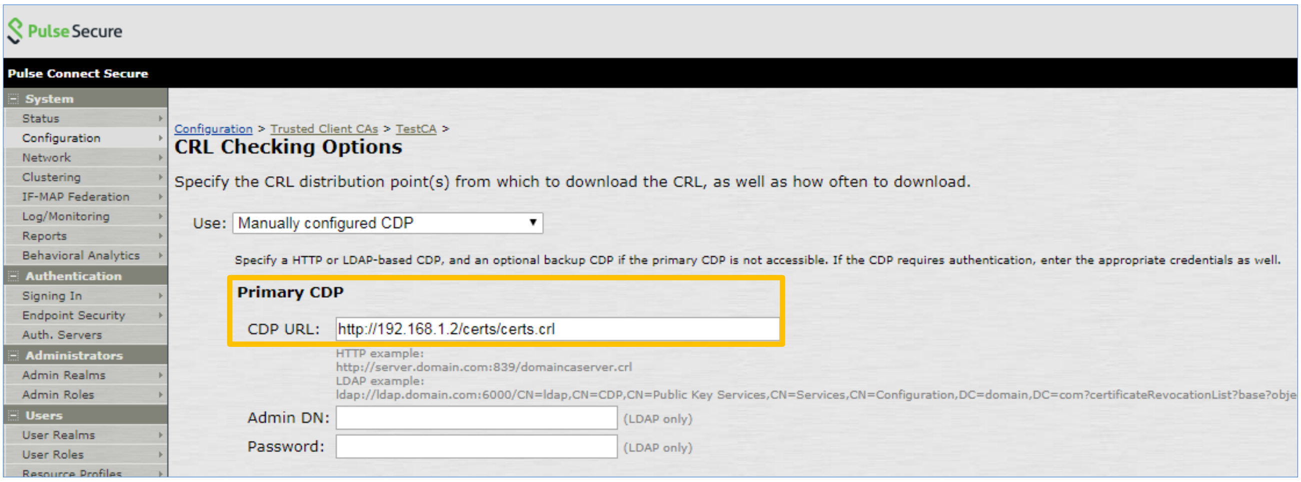
CRL Checking Options ... | Update Now | Enable | Disable

□	CRL distribution points	Status	Last Updated	Next Update
	No CRL checking			

Licensed to 0311M5RWK0N8Q111S
Copyright © 2001-2018 Pulse Secure, LLC. All rights reserved.

項目	値
Client certificate status checking	
- Use CRLs	選択
- Verify Trusted Client CA	有効
- Trusted for Client Authentication	有効
- Participate in Certificate Negotiation	有効

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



Configuration > Trusted Client CAs > TestCA >

CRL Checking Options

Specify the CRL distribution point(s) from which to download the CRL, as well as how often to download.

Use: Manually configured CDP

Specify a HTTP or LDAP-based CDP, and an optional backup CDP if the primary CDP is not accessible. If the CDP requires authentication, enter the appropriate credentials as well.

Primary CDP

CDP URL: http://192.168.1.2/certs/certs.crl

HTTP example:
http://server.domain.com:839/domaincaserver.crl
LDAP example:
ldap://ldap.domain.com:6000/CN=ldap,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=domain,DC=com?certificateRevocationList?base?obje

Admin DN: (LDAP only)

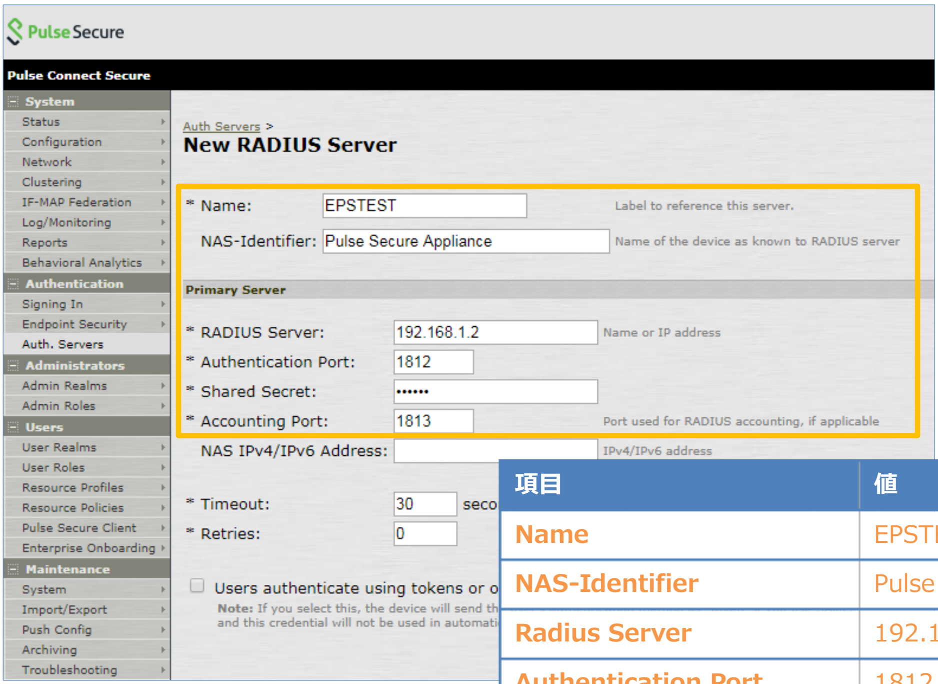
Password: (LDAP only)

項目	値
CDP URL	http://192.168.1.2/certs/certs.crl

3-3 PSA300 の VPN 接続に関する設定

3-3-1 RADIUS/Certificate Server の設定

「Auth. Servers」の「New RADIUS Server」にて RADIUS サーバーを追加します。



Pulse Secure

Pulse Connect Secure

Auth Servers >

New RADIUS Server

* Name: EPSTEST Label to reference this server.

NAS-Identifier: Pulse Secure Appliance Name of the device as known to RADIUS server

Primary Server

* RADIUS Server: 192.168.1.2 Name or IP address

* Authentication Port: 1812

* Shared Secret: ••••••

* Accounting Port: 1813 Port used for RADIUS accounting, if applicable

NAS IPv4/IPv6 Address: IPv4/IPv6 address

* Timeout: 30 seco

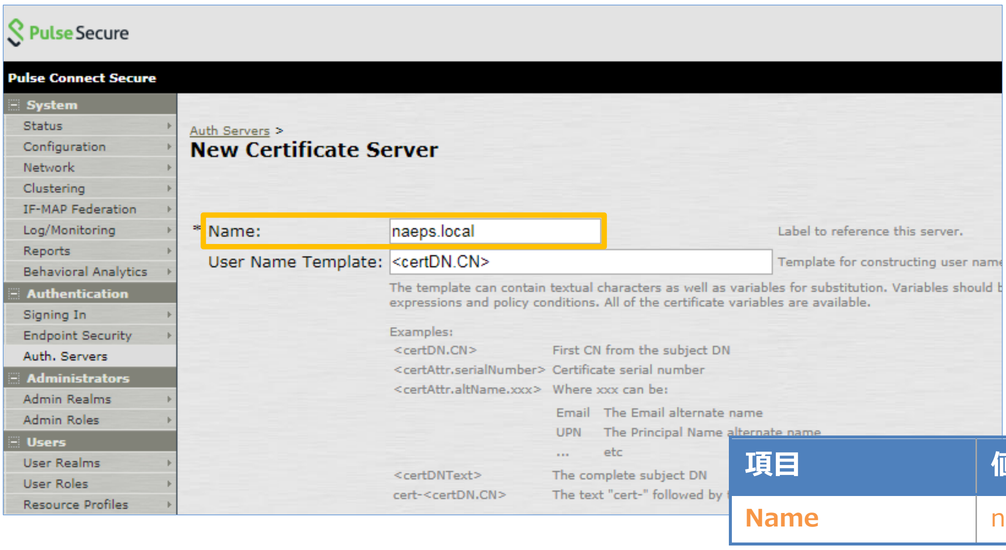
* Retries: 0

□ Users authenticate using tokens or o

Note: If you select this, the device will send th
and this credential will not be used in automati

項目	値
Name	EPSTEST
NAS-Identifier	Pulse Secure Appliance
Radius Server	192.168.1.2
Authentication Port	1812
Shared Secret	secret
Accounting Port	1813

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



Pulse Secure

Pulse Connect Secure

Auth Servers >

New Certificate Server

* Name: naeps.local Label to reference this server.

User Name Template: <certDN.CN> Template for constructing user name

The template can contain textual characters as well as variables for substitution. Variables should b
expressions and policy conditions. All of the certificate variables are available.

Examples:

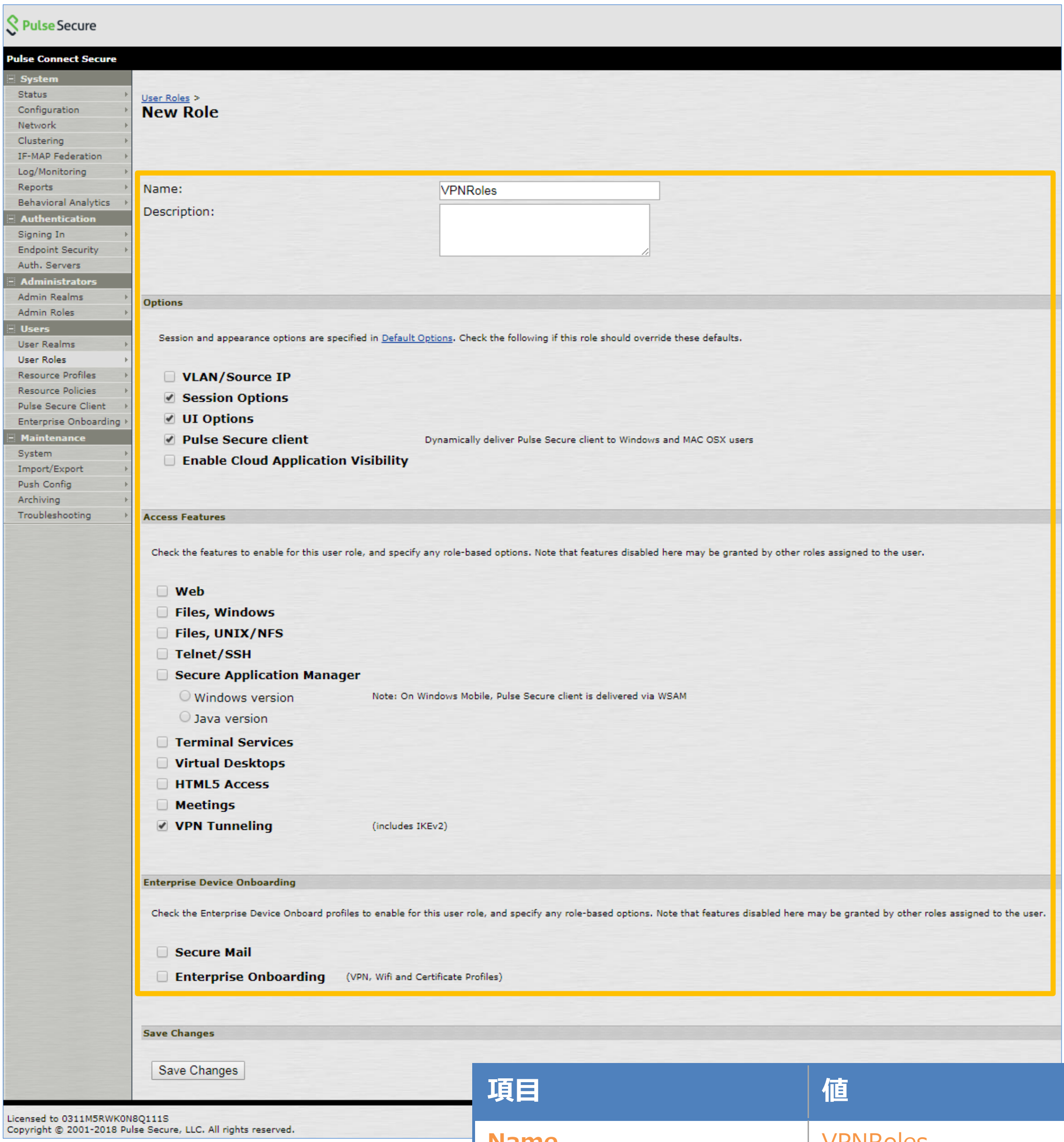
<certDN.CN> First CN from the subject DN
<certAttr.serialNumber> Certificate serial number
<certAttr.altName.xxx> Where xxx can be:
Email The Email alternate name
UPN The Principal Name alternate name
... etc
<certDNText> The complete subject DN
cert-<certDN.CN> The text "cert-" followed by

項目	値
Name	naeps.local

3-3-2 VPN Roles の設定

[User Roles]-[New User Role]よりユーザーに割り当てるロールの設定を行います。

ここでは、許可する VPN 接続方法等を指定します。Pulse Secure client にチェックを入れます。



User Roles >
New Role

Name: VPNRoles
Description:

Options

Session and appearance options are specified in Default Options. Check the following if this role should override these defaults.

- □ VLAN/Source IP
- ☑ Session Options
- ☑ UI Options
- ☑ Pulse Secure client — Dynamically deliver Pulse Secure client to Windows and MAC OSX users
- □ Enable Cloud Application Visibility

Access Features

Check the features to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.

- □ Web
- □ Files, Windows
- □ Files, UNIX/NFS
- □ Telnet/SSH
- □ Secure Application Manager
  - ○ Windows version — Note: On Windows Mobile, Pulse Secure client is delivered via WSAM
  - ○ Java version
- □ Terminal Services
- □ Virtual Desktops
- □ HTML5 Access
- □ Meetings
- ☑ VPN Tunneling (includes IKEv2)

Enterprise Device Onboarding

Check the Enterprise Device Onboard profiles to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.

- □ Secure Mail
- □ Enterprise Onboarding (VPN, Wifi and Certificate Profiles)

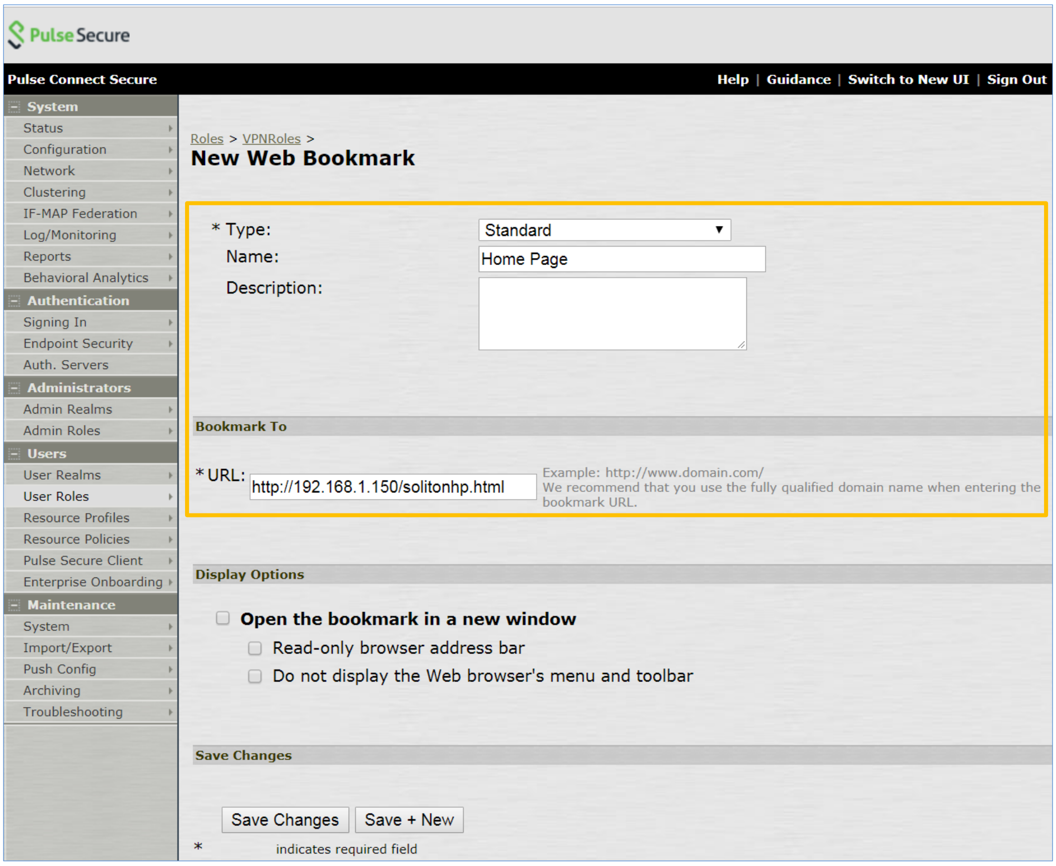
Save Changes

Licensed to 0311M5RWK0N8Q111S
Copyright © 2001-2018 Pulse Secure, LLC. All rights reserved.

項目	値
Name	VPNRoles
Options	Session Options
	UI Options
	Pulse Secure client
Access features	VPN Tunneling

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

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



New Web Bookmark

* Type: Standard

Name: Home Page

Description:

Bookmark To

* URL: http://192.168.1.150/solitonhp.html

Example: http://www.domain.com/
We recommend that you use the fully qualified domain name when entering the bookmark URL.

Display Options

□ Open the bookmark in a new window

□ Read-only browser address bar

□ Do not display the Web browser's menu and toolbar

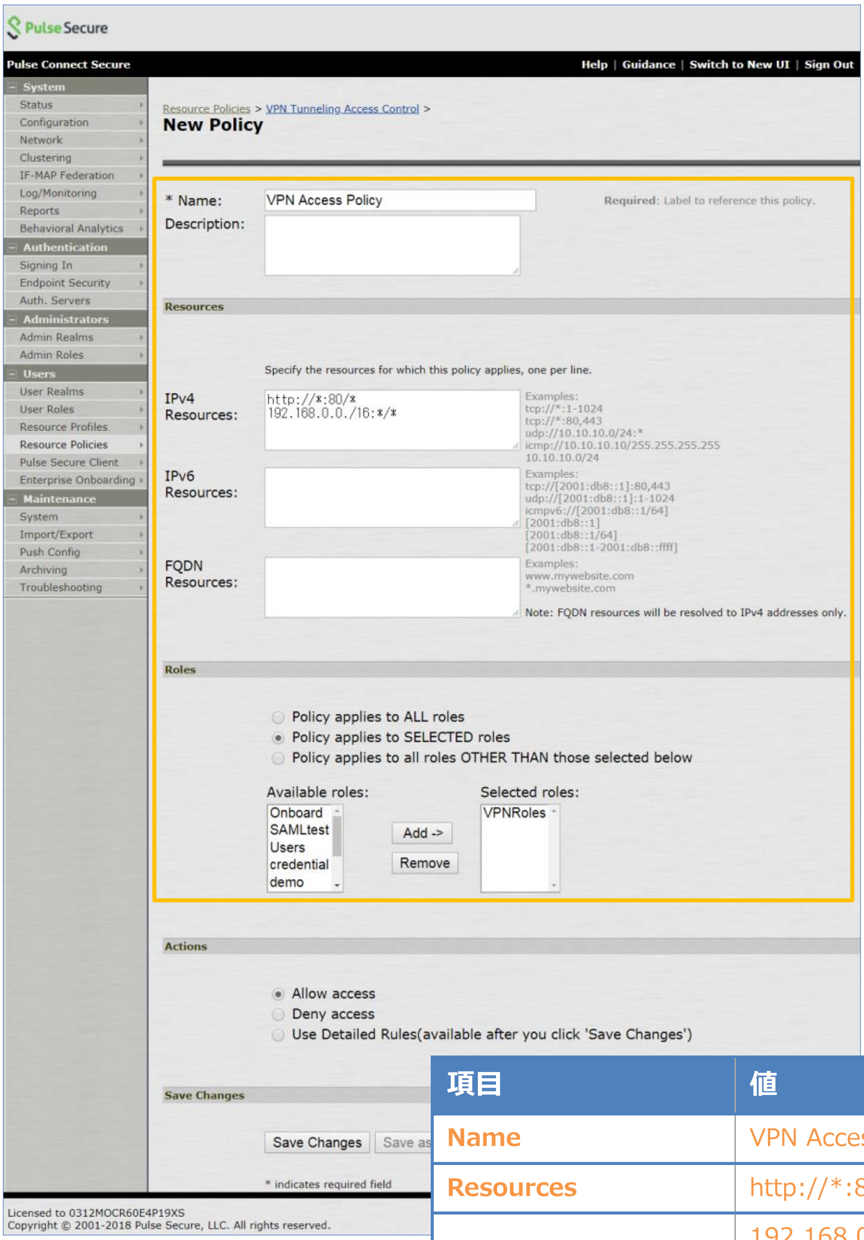
Save Changes

* indicates required field

項目	値
Name	Home Page
URL	http://192.168.1.150/solitonhp.html

3-3-3 VPN Access Policy の設定

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



Resource Policies > VPN Tunneling Access Control >

New Policy

* Name: VPN Access Policy — Required: Label to reference this policy.

Description:

Resources

Specify the resources for which this policy applies, one per line.

IPv4 Resources:

```
http://*:80/*
192.168.0.0./16:*/*
```

Examples:
tcp://*:1-1024
tcp://*:80,443
udp://10.10.10.0/24:*
icmp://10.10.10.10/255.255.255.255
10.10.10.0/24

IPv6 Resources:

Examples:
tcp://[2001:db8::1]:80,443
udp://[2001:db8::1]:1-1024
icmpv6://[2001:db8::1/64]
[2001:db8::1]
[2001:db8::1/64]
[2001:db8::1-2001:db8::ffff]

FQDN Resources:

Examples:
www.mywebsite.com
*.mywebsite.com

Note: FQDN resources will be resolved to IPv4 addresses only.

Roles

○ Policy applies to ALL roles
● Policy applies to SELECTED roles
○ Policy applies to all roles OTHER THAN those selected below

Available roles: Onboard, SAMLtest, Users, credential, demo

Add -> / Remove

Selected roles: VPNRoles

Actions

● Allow access
○ Deny access
○ Use Detailed Rules(available after you click 'Save Changes')

Save Changes

Save Changes | Save as

* indicates required field

Licensed to 0312MOCR60E4P19XS
Copyright © 2001-2018 Pulse Secure, LLC. All rights reserved.

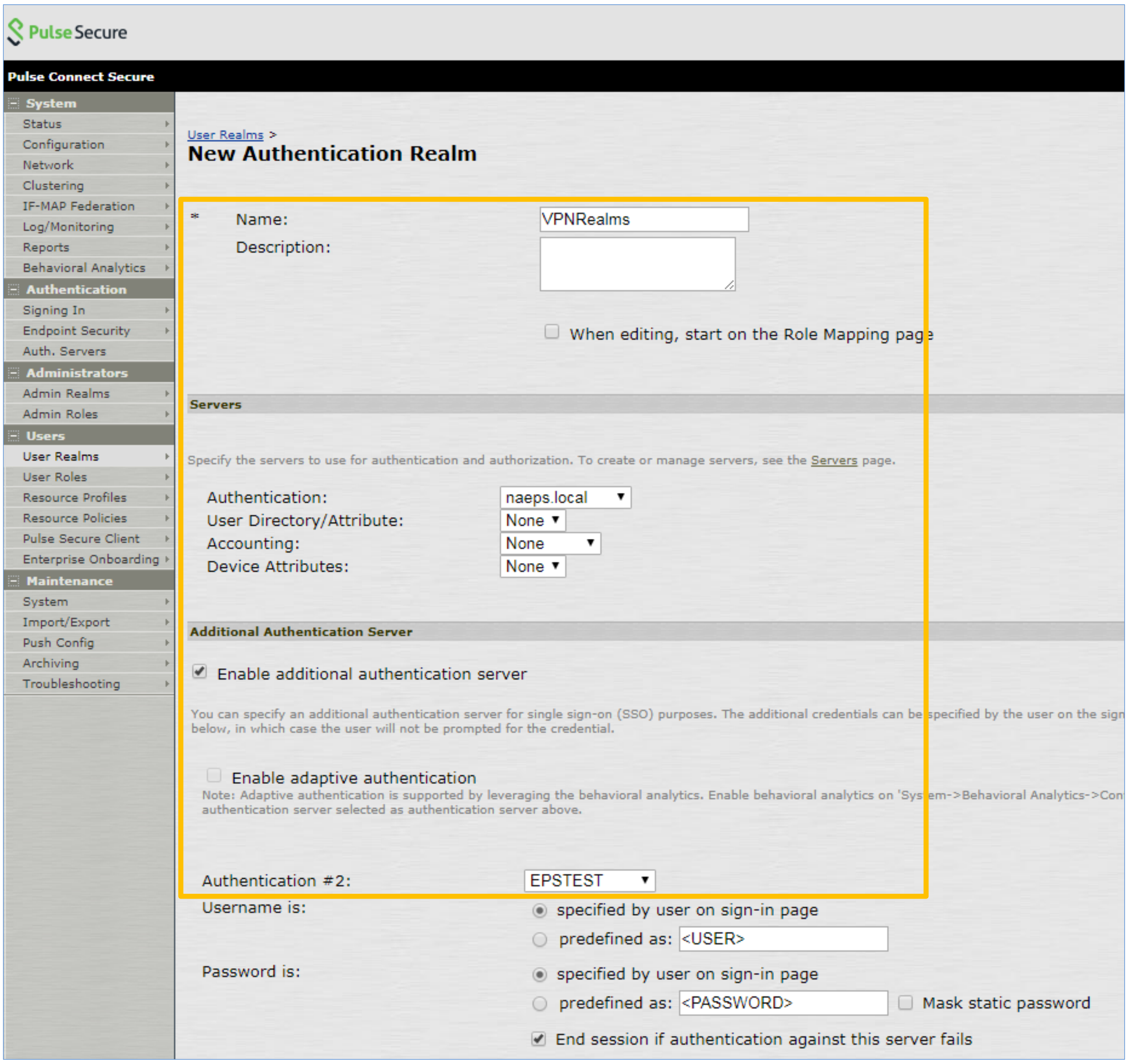
項目	値
Name	VPN Access Policy
Resources	http://*:80/*
	192.168.0.0./16:*/*
Roles	Policy applies to SELECTED roles
Selected roles	VPNRoles

3-3-4 Authentication Realms の設定

[User Realms]-[New User Realms]レルムの設定を行います。

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

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



User Realms >

New Authentication Realm

* Name: VPNRealms

Description:

□ When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the Servers page.

Authentication: naeps.local

User Directory/Attribute: None

Accounting: None

Device Attributes: None

Additional Authentication Server

☑ Enable additional authentication server

You can specify an additional authentication server for single sign-on (SSO) purposes. The additional credentials can be specified by the user on the sign below, in which case the user will not be prompted for the credential.

□ Enable adaptive authentication

Note: Adaptive authentication is supported by leveraging the behavioral analytics. Enable behavioral analytics on 'System->Behavioral Analytics->Con authentication server selected as authentication server above.

Authentication #2: EPSTEST

Username is: ● specified by user on sign-in page
○ predefined as: <USER>

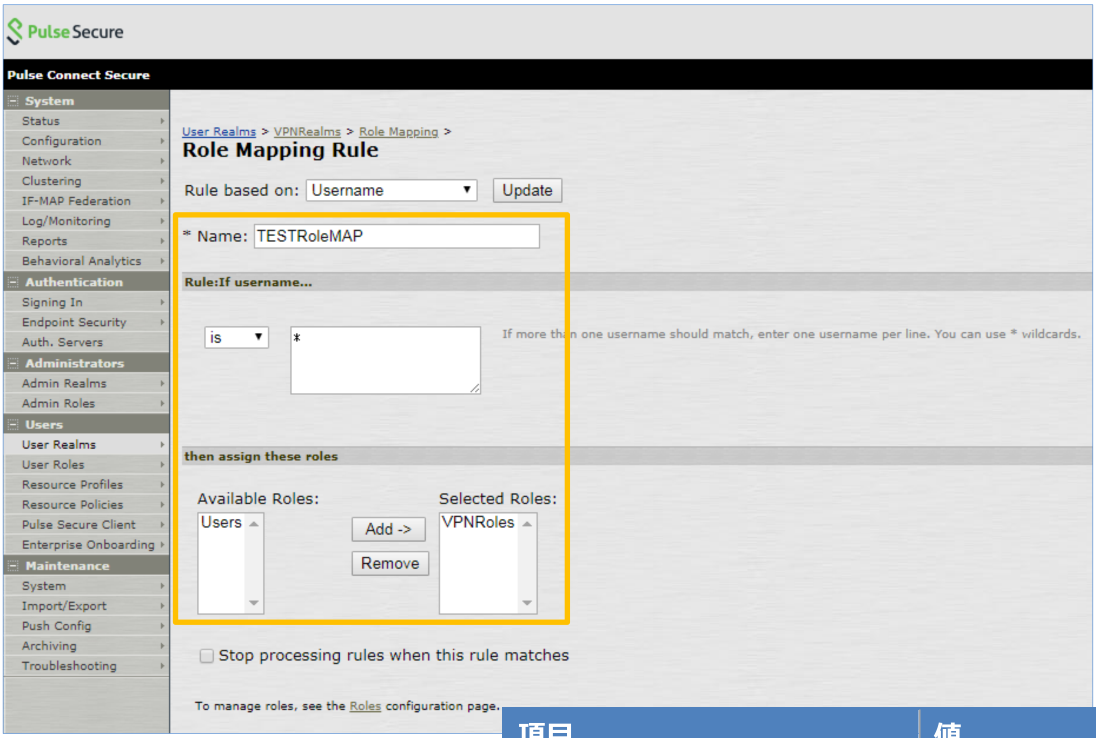
Password is: ● specified by user on sign-in page
○ predefined as: <PASSWORD> □ Mask static password

☑ End session if authentication against this server fails

項目	値
Name	VPNRealms
Authentication	naeps.local
Additional authentication server	EPSTEST

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

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



User Realms > VPNRealms > Role Mapping >

Role Mapping Rule

Rule based on: Username

* Name: TESTRoleMAP

Rule:If username...

is | *

If more than one username should match, enter one username per line. You can use * wildcards.

then assign these roles

Available Roles: Users

Selected Roles: VPNRoles

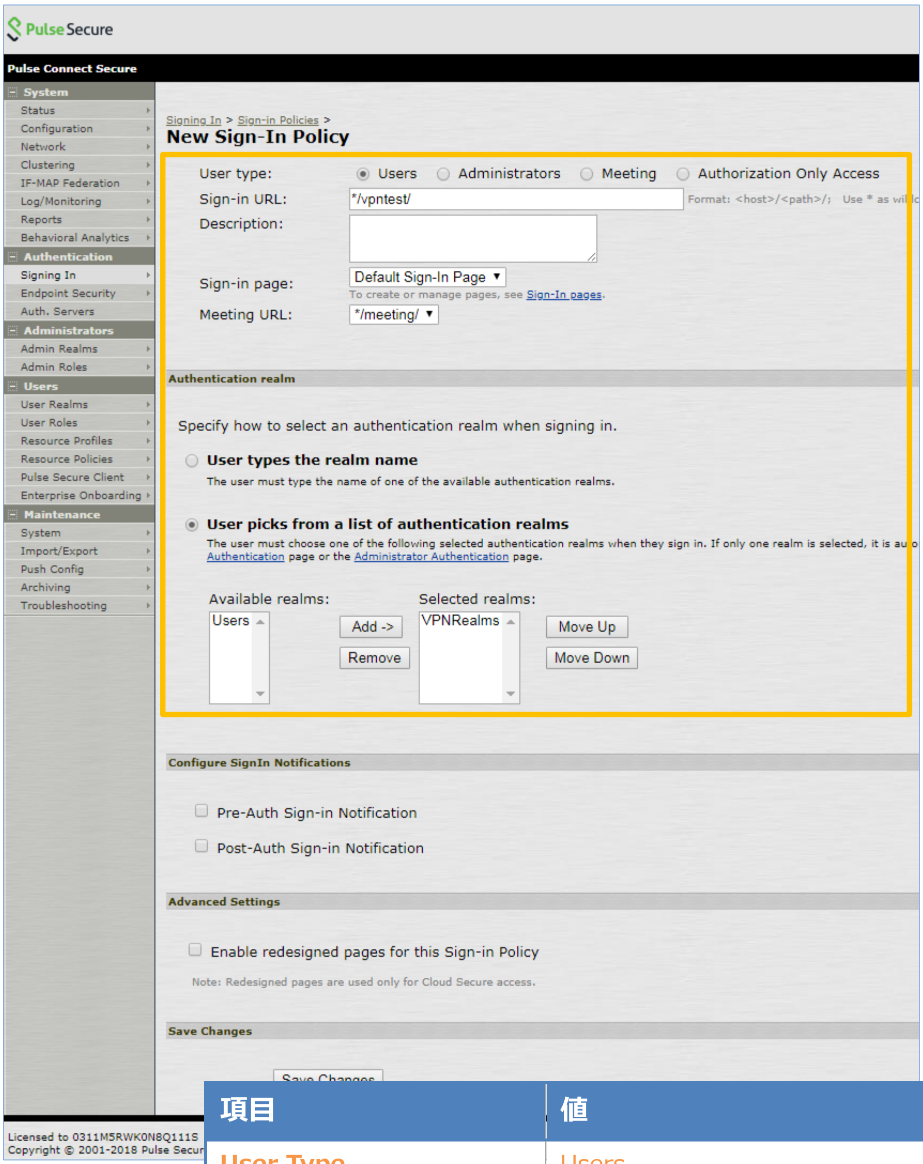
□ Stop processing rules when this rule matches

To manage roles, see the Roles configuration page.

項目	値
Name	TESTRoleMAP
Role if username…	is:*
…then assign these roles	VPNRoles

3-3-5 Sign-In Policy の設定

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



New Sign-In Policy

User type: ● Users ○ Administrators ○ Meeting ○ Authorization Only Access

Sign-in URL: */vpntest/ Format: <host>/<path>/; Use * as wil

Description:

Sign-in page: Default Sign-In Page ▼

To create or manage pages, see Sign-In pages.

Meeting URL: */meeting/ ▼

Authentication realm

Specify how to select an authentication realm when signing in.

○ **User types the realm name**

The user must type the name of one of the available authentication realms.

● **User picks from a list of authentication realms**

The user must choose one of the following selected authentication realms when they sign in. If only one realm is selected, it is au o Authentication page or the Administrator Authentication page.

Available realms: Users

Selected realms: VPNRealms

Configure SignIn Notifications

□ Pre-Auth Sign-in Notification

□ Post-Auth Sign-in Notification

Advanced Settings

□ Enable redesigned pages for this Sign-in Policy

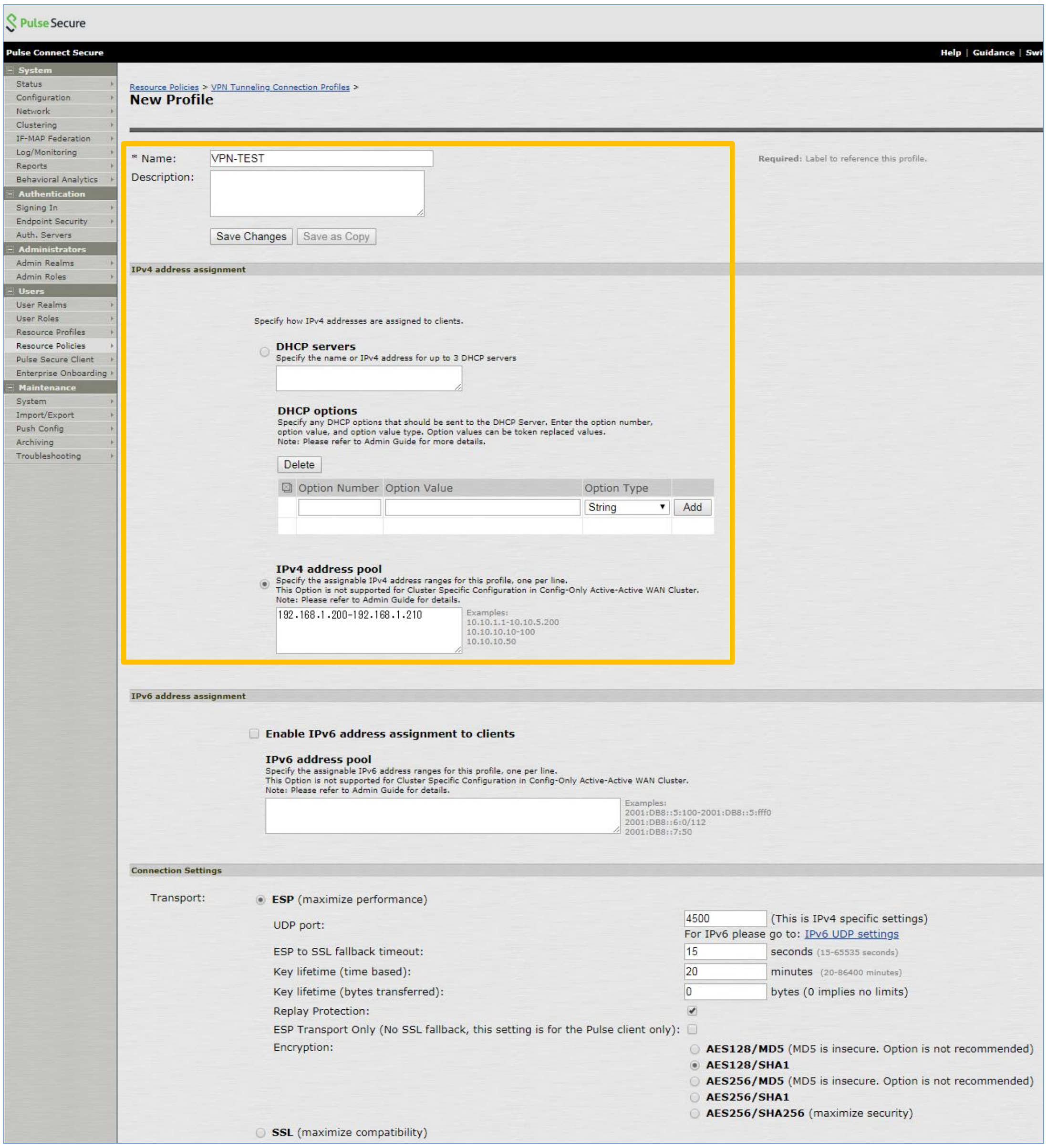
Note: Redesigned pages are used only for Cloud Secure access.

Save Changes

項目	値
User Type	Users
Sign-in URL	*/vpntest/
Authentication realm	User picks from a list authentication realms
Selected realms	VPNRealms

3-3-6 IP プールの設定

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



Resource Policies > VPN Tunneling Connection Profiles >

New Profile

* Name: VPN-TEST

Description:

Required: Label to reference this profile.

Save Changes | Save as Copy

IPv4 address assignment

Specify how IPv4 addresses are assigned to clients.

○ **DHCP servers**
Specify the name or IPv4 address for up to 3 DHCP servers

DHCP options
Specify any DHCP options that should be sent to the DHCP Server. Enter the option number, option value, and option value type. Option values can be token replaced values.
Note: Please refer to Admin Guide for more details.

Delete

□	Option Number	Option Value	Option Type	
			String ▾	Add

● **IPv4 address pool**
Specify the assignable IPv4 address ranges for this profile, one per line.
This Option is not supported for Cluster Specific Configuration in Config-Only Active-Active WAN Cluster.
Note: Please refer to Admin Guide for details.

192.168.1.200-192.168.1.210

Examples:
10.10.1.1-10.10.5.200
10.10.10.10-100
10.10.10.50

IPv6 address assignment

□ **Enable IPv6 address assignment to clients**

IPv6 address pool
Specify the assignable IPv6 address ranges for this profile, one per line.
This Option is not supported for Cluster Specific Configuration in Config-Only Active-Active WAN Cluster.
Note: Please refer to Admin Guide for details.

Examples:
2001:DB8::5:100-2001:DB8::5:fff0
2001:DB8::6:0/112
2001:DB8::7:50

Connection Settings

Transport: ● **ESP** (maximize performance)

UDP port: 4500 (This is IPv4 specific settings)
For IPv6 please go to: IPv6 UDP settings

ESP to SSL fallback timeout: 15 seconds (15-65535 seconds)

Key lifetime (time based): 20 minutes (20-86400 minutes)

Key lifetime (bytes transferred): 0 bytes (0 implies no limits)

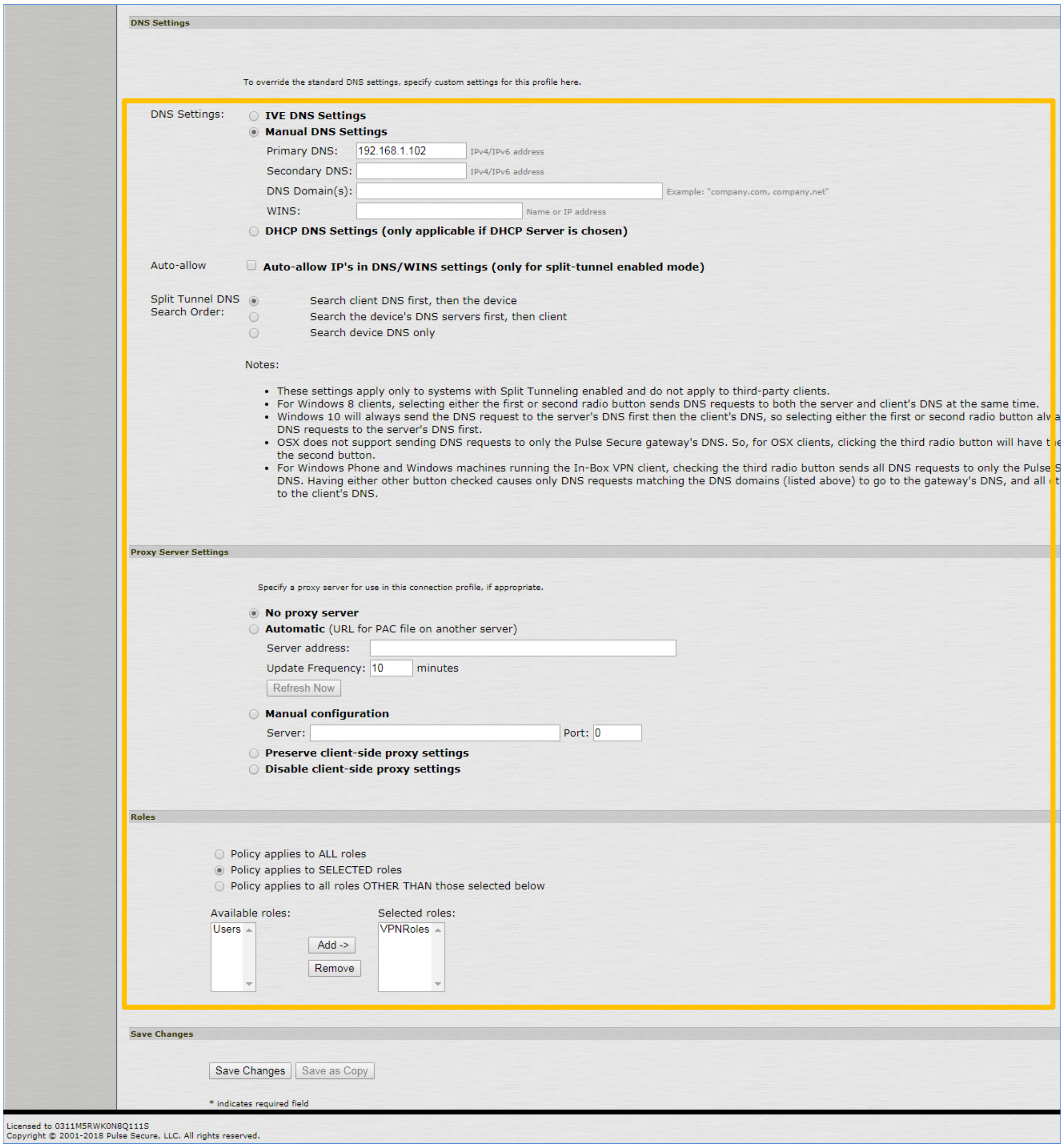
Replay Protection: ☑

ESP Transport Only (No SSL fallback, this setting is for the Pulse client only): □

Encryption:
○ **AES128/MD5** (MD5 is insecure. Option is not recommended)
● **AES128/SHA1**
○ **AES256/MD5** (MD5 is insecure. Option is not recommended)
○ **AES256/SHA1**
○ **AES256/SHA256** (maximize security)

○ **SSL** (maximize compatibility)

項目	値
Name	VPN-TEST
IP Address Pool	192.168.1.200 - 192.168.1.210



DNS Settings

To override the standard DNS settings, specify custom settings for this profile here.

DNS Settings:
○ **IVE DNS Settings**
● **Manual DNS Settings**
Primary DNS: 192.168.1.102 IPv4/IPv6 address
Secondary DNS: IPv4/IPv6 address
DNS Domain(s): Example: "company.com, company.net"
WINS: Name or IP address
○ **DHCP DNS Settings (only applicable if DHCP Server is chosen)**

Auto-allow □ **Auto-allow IP's in DNS/WINS settings (only for split-tunnel enabled mode)**

Split Tunnel DNS Search Order:
● Search client DNS first, then the device
○ Search the device's DNS servers first, then client
○ Search device DNS only

Notes:

- These settings apply only to systems with Split Tunneling enabled and do not apply to third-party clients.
- For Windows 8 clients, selecting either the first or second radio button sends DNS requests to both the server and client's DNS at the same time.
- Windows 10 will always send the DNS request to the server's DNS first then the client's DNS, so selecting either the first or second radio button alwa DNS requests to the server's DNS first.
- OSX does not support sending DNS requests to only the Pulse Secure gateway's DNS. So, for OSX clients, clicking the third radio button will have the the second button.
- For Windows Phone and Windows machines running the In-Box VPN client, checking the third radio button sends all DNS requests to only the Pulse S DNS. Having either other button checked causes only DNS requests matching the DNS domains (listed above) to go to the gateway's DNS, and all t to the client's DNS.

Proxy Server Settings

Specify a proxy server for use in this connection profile, if appropriate.

● **No proxy server**
○ **Automatic** (URL for PAC file on another server)
Server address:
Update Frequency: 10 minutes
Refresh Now

○ **Manual configuration**
Server: Port: 0
○ **Preserve client-side proxy settings**
○ **Disable client-side proxy settings**

Roles

○ Policy applies to ALL roles
● Policy applies to SELECTED roles
○ Policy applies to all roles OTHER THAN those selected below

Available roles: Users
Selected roles: VPNRoles

Save Changes

* indicates required field

Licensed to 0311M5RWK0N8Q111S

項目	値
DNS Settings	Manual DNS Settigns
	192.168.1.102
Selected Roles	VPNRoles

4. Windows 版 Pulse Secure クライアントの設定

4-1 PC への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 PC にインポートする方法として、下記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

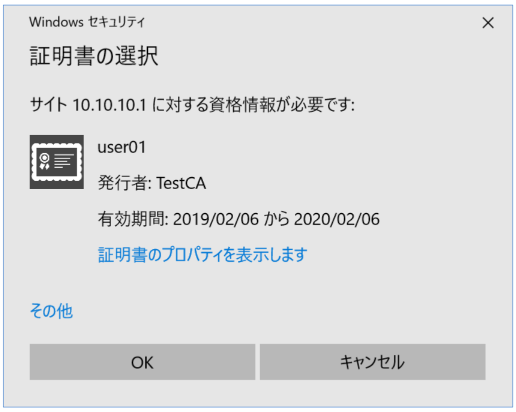
2) PC に証明書ファイル(PKCS#12 形式)と CA 証明書を配置し、証明書インポートウィザードを使ってインポートする方法

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ポートします。
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。

4-2Pulse Secure クライアントの取得と接続

Pulse Secure クライアントをダウンロードし、接続を行います。

「https://10.10.10.1/vpntest」にアクセスし、ユーザー証明書の選択とユーザーID/パスワードの入力を行います。



Windows セキュリティ

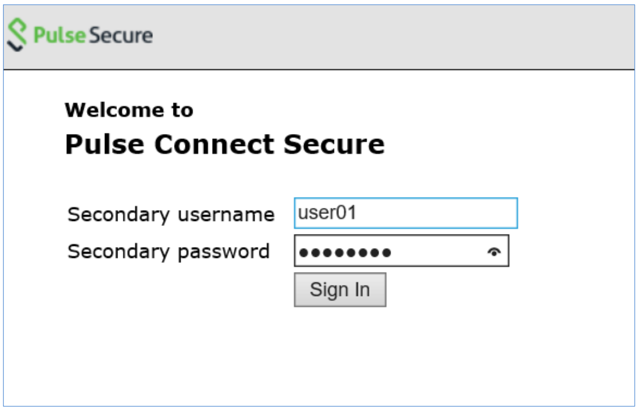
証明書の選択

サイト 10.10.10.1 に対する資格情報が必要です:

user01

発行者: TestCA

有効期間: 2019/02/06 から 2020/02/06



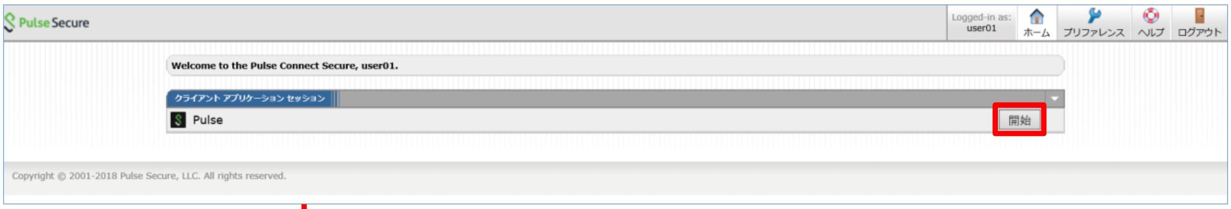
Welcome to

Pulse Connect Secure

Secondary username: user01

Secondary password: ••••••••

表示されるページの「開始」ボタンをクリックし、クライアントソフトウェアのダウンロードを行うと自動的に Pulse Secure に接続されます。

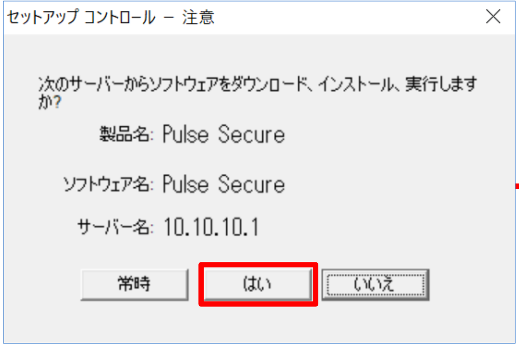


Welcome to the Pulse Connect Secure, user01.

クライアント アプリケーション セッション

Pulse

Copyright © 2001-2018 Pulse Secure, LLC. All rights reserved.



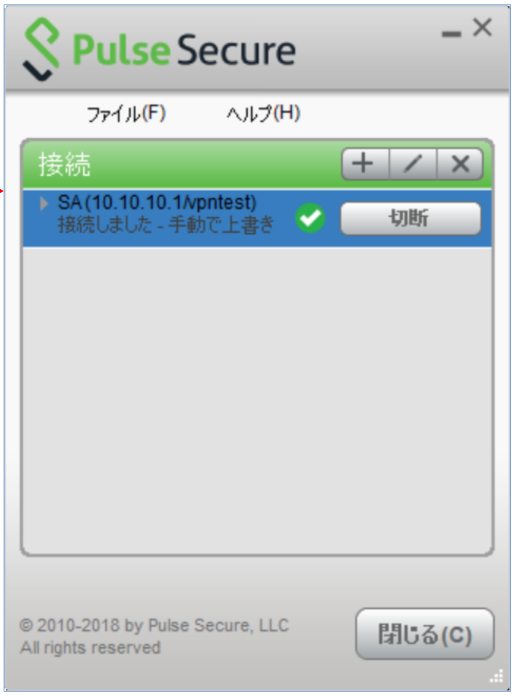
セットアップ コントロール － 注意

次のサーバーからソフトウェアをダウンロード、インストール、実行しますか?

製品名: Pulse Secure

ソフトウェア名: Pulse Secure

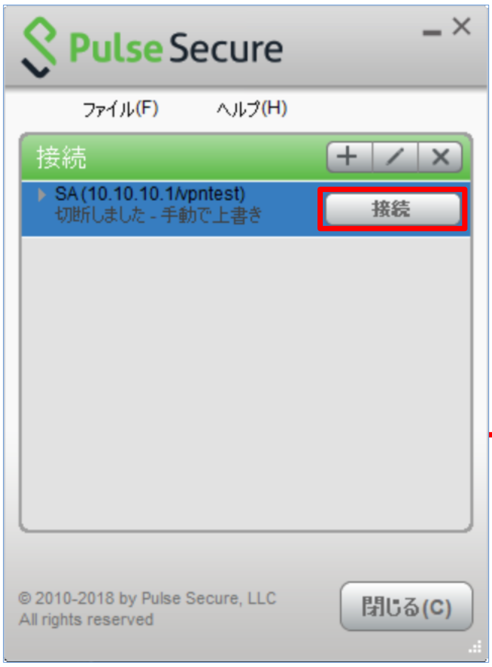
サーバー名: 10.10.10.1



SA(10.10.10.1/vpntest)
接続しました - 手動で上書き

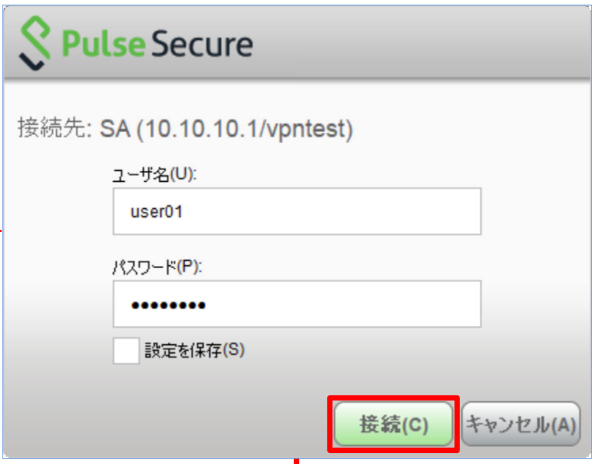
© 2010-2018 by Pulse Secure, LLC
All rights reserved

２回目以降は、Pulse Secure Client を起動し、ユーザー名/パスワードを入力して接続してください。



SA (10.10.10.1/vpntest)
切断しました - 手動で上書き

© 2010-2018 by Pulse Secure, LLC
All rights reserved

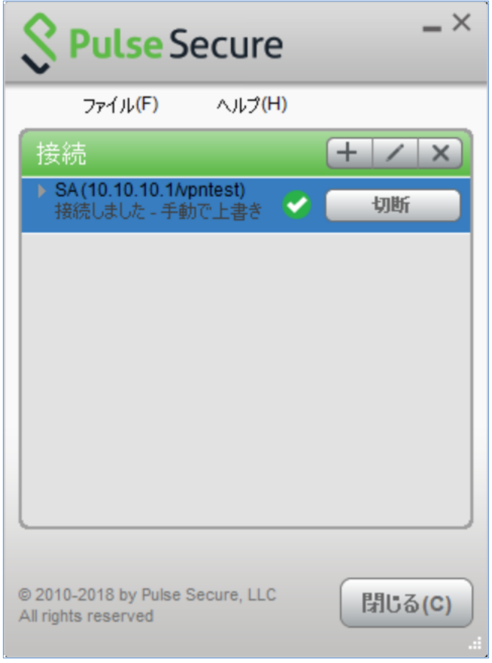


接続先: SA (10.10.10.1/vpntest)

ユーザ名(U): user01

パスワード(P): ●●●●●●●●●

□ 設定を保存(S)



SA (10.10.10.1/vpntest)
接続しました - 手動で上書き ✓

© 2010-2018 by Pulse Secure, LLC
All rights reserved

5. iOS 版 Pulse Secure クライアントの設定

5-1 iOS へのデジタル証明書のインポート

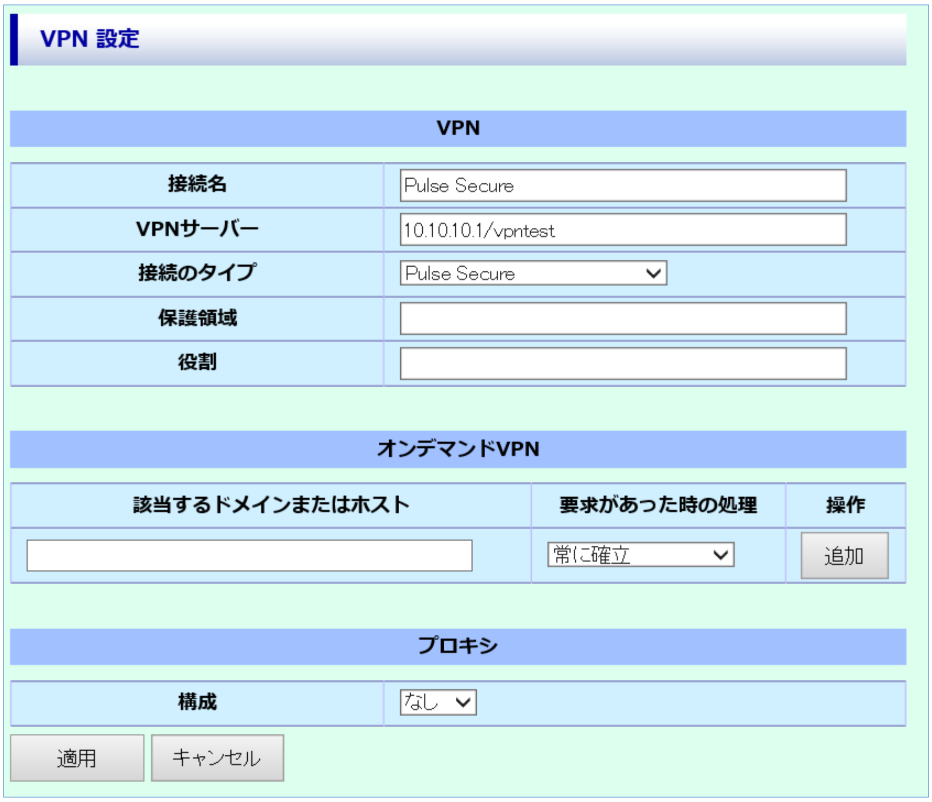
iOS 12 以降では、OS のストアにインポートしたクライアント証明書は、VPN 接続で利用できなくなりました。

EPS-ap を使用して証明書を配布する場合には、同時に VPN プロファイルも配布することで、VPN 接続時の認証に証明書を使用可能になります。

本資料では、EPS-ap を使用して証明書の配布を行っています。

iOS 12 以降を使用する場合は、Pulse Secure Client v7.0.0 以降をご利用ください。

iOS 10.3 以降は、OS の仕様によりプライベート認証局の CA 証明書をインポートする場合、インポートした証明書を手動で信頼させる必要があります。



VPN 設定

VPN	
接続名	Pulse Secure
VPNサーバー	10.10.10.1/vpntest
接続のタイプ	Pulse Secure
保護領域	
役割	

オンデマンドVPN

該当するドメインまたはホスト	要求があった時の処理	操作
	常に確立	追加

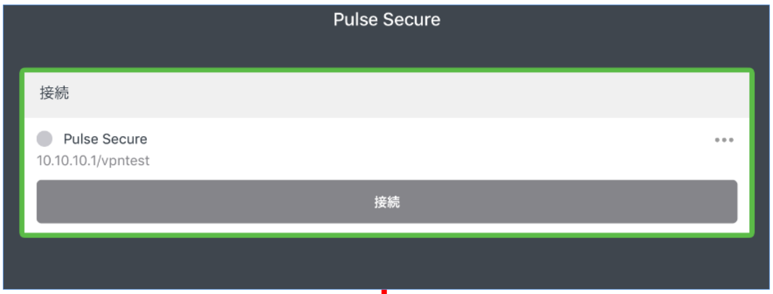
プロキシ	
構成	なし

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]

5-2 Pulse Secure への接続

App Store からインストールした Pulse Secure クライアントを起動します。

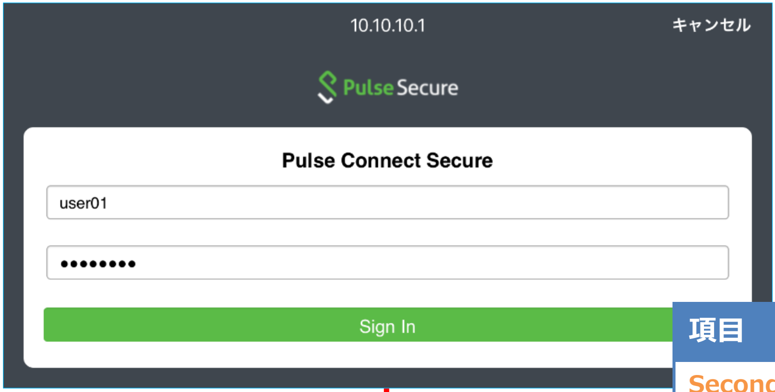
EPS-ap を使用して証明書と VPN プロファイルを配布した場合、アプリ側で設定を行う必要はありません。Pulse Secure クライアントを起動し、VPN 接続を行います。



Pulse Secure

接続

○ Pulse Secure
10.10.10.1/vpntest



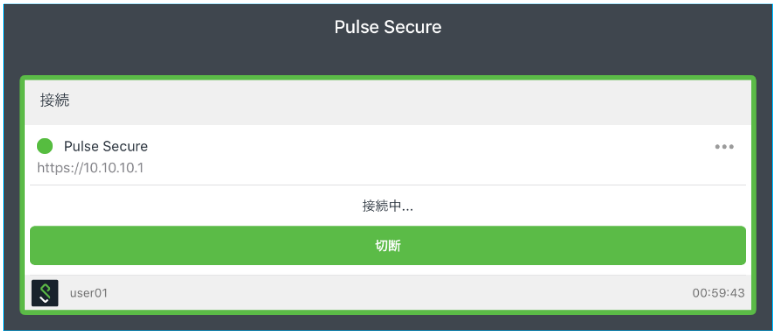
10.10.10.1

Pulse Connect Secure

user01

••••••••

項目	値
Secondary username	User01
Secondary password	password



Pulse Secure

接続

● Pulse Secure
https://10.10.10.1

接続中...

user01 00:59:43

6. Android 版の Pulse Secure クライアント設定

6-1 Android へのデジタル証明書のインポート

NetAttest EPS から発行したデジタル証明書を Android デバイスにインポートする方法として、下記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

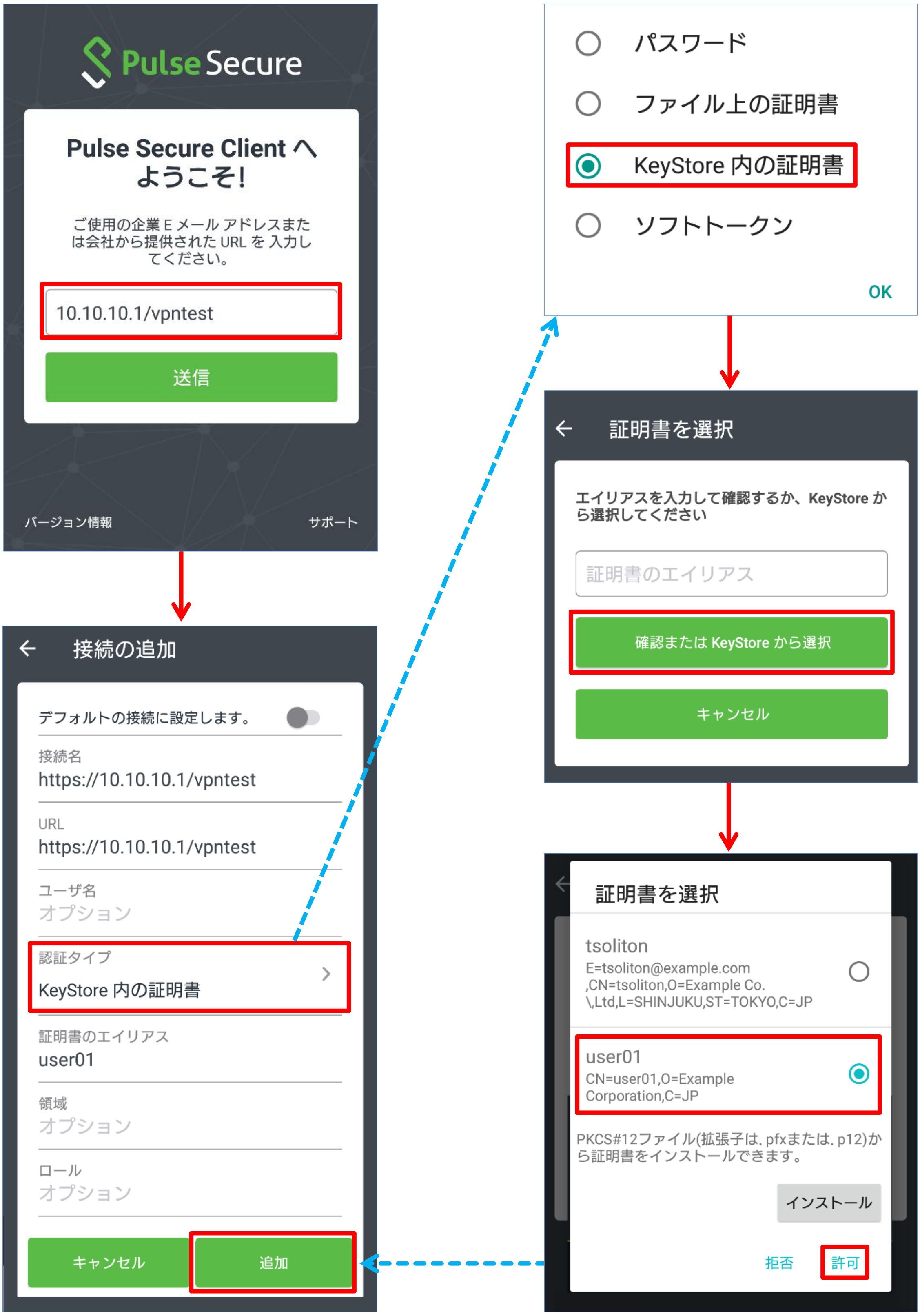
2） デジタル証明書をメールに添付して Android デバイスに送り、インポートする方法

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、インポートする方法

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ポートします。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。

6-2 Pulse Secure クライアントの接続設定

Google Play からインストールした Pulse Secure クライアントを起動し、下記設定を行います。



Pulse Secure

Pulse Secure Client へ ようこそ!

ご使用の企業 E メール アドレスまたは会社から提供された URL を 入力してください。

10.10.10.1/vpntest

送信

バージョン情報　サポート

接続の追加

デフォルトの接続に設定します。

接続名
https://10.10.10.1/vpntest

URL
https://10.10.10.1/vpntest

ユーザ名
オプション

認証タイプ
KeyStore 内の証明書

証明書のエイリアス
user01

領域
オプション

ロール
オプション

キャンセル　追加

○ パスワード
○ ファイル上の証明書
● KeyStore 内の証明書
○ ソフトトークン

OK

証明書を選択

エイリアスを入力して確認するか、KeyStore から選択してください

証明書のエイリアス

確認または KeyStore から選択

キャンセル

証明書を選択

tsoliton
E=tsoliton@example.com
,CN=tsoliton,O=Example Co.
\,Ltd,L=SHINJUKU,ST=TOKYO,C=JP ○

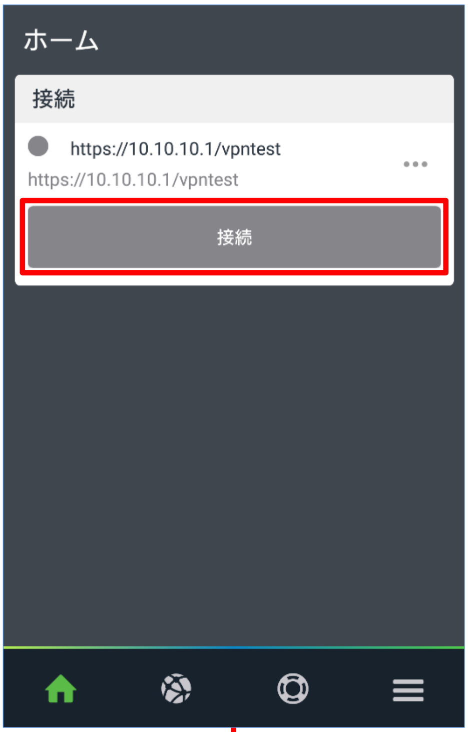
user01
CN=user01,O=Example
Corporation,C=JP ●

PKCS#12ファイル(拡張子は. pfxまたは. p12)から証明書をインストールできます。

インストール

拒否　許可

作成した接続情報を選択し、ユーザーID/パスワードを入力してください。

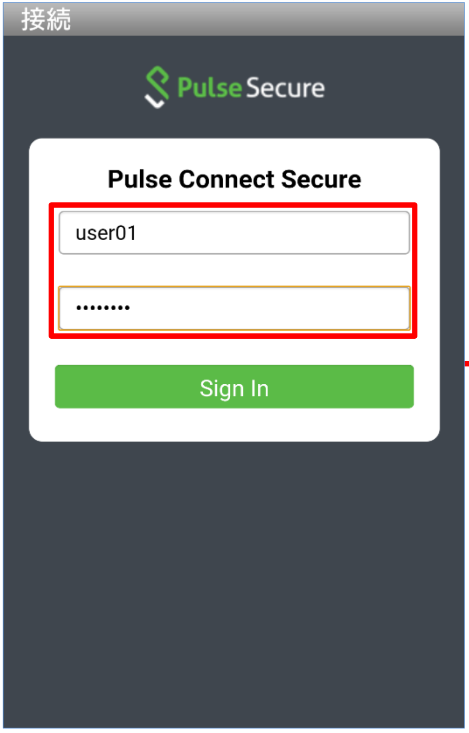


ホーム

接続

https://10.10.10.1/vpntest

https://10.10.10.1/vpntest



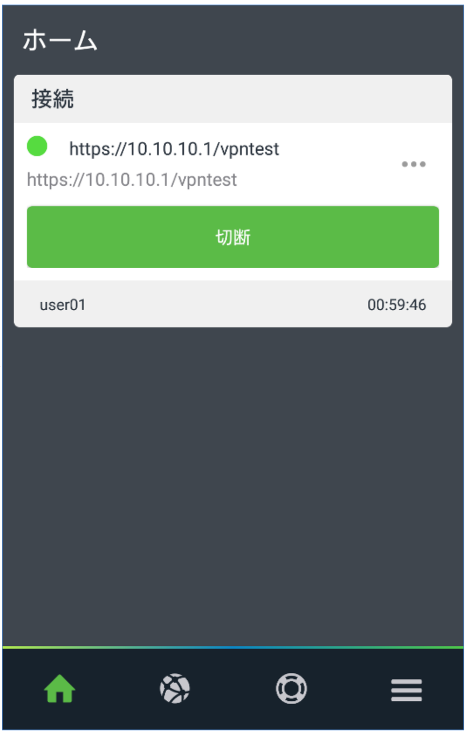
接続

Pulse Secure

Pulse Connect Secure

user01

••••••••



ホーム

接続

https://10.10.10.1/vpntest

https://10.10.10.1/vpntest

user01 00:59:46

改訂履歴

日付	版	改訂内容
2019/03/29	1.0	初版作成