Wi-Fi／VPN認証サービスをご検討の方へ

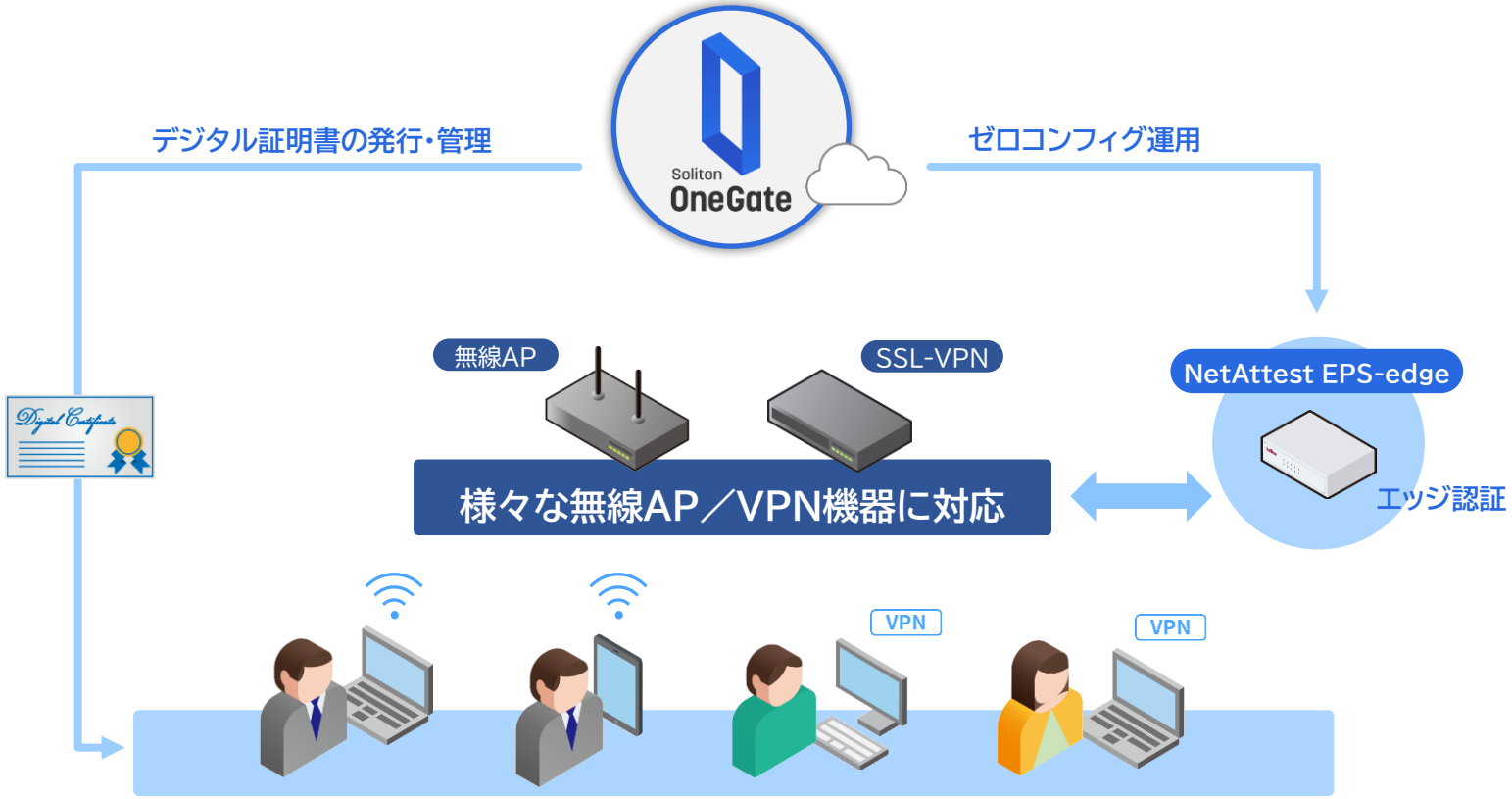
各機器の連携設定について

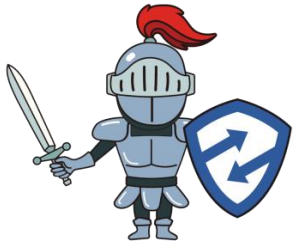
Soliton OneGate

OneGate の Wi-Fi／VPN認証サービス

許可したデバイスだけをLANに繋げる、そんな当たり前をサービスで提供

ゼロコンフィグ運用のNetAttest EPS-edgeを設置するだけで、ネットワークセキュリティを手早く強化。
安全性と運用性の両面で優れるデジタル証明書を用いた認証で、悪意あるユーザー・不適切な端末の進入を防ぎます。





無線LAN機器の設定例

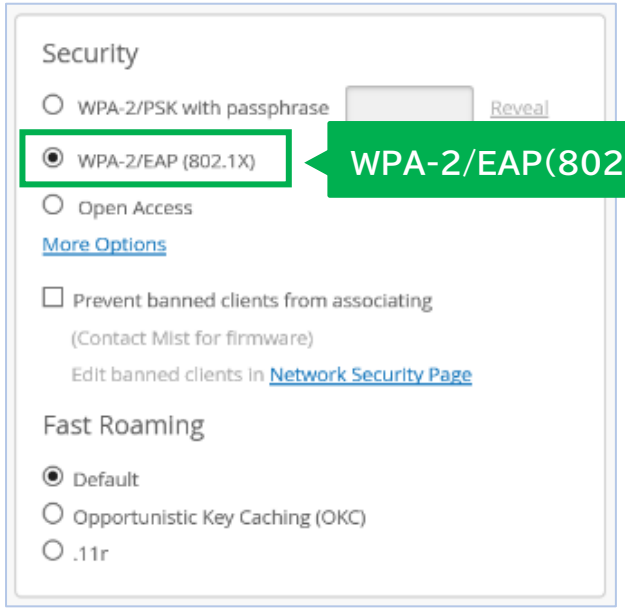
各機器の設定画面は、当社で連携検証を実施した時点のキャプチャです。
本資料に掲載されていない機器、並びに各機器の最新設定画面はFAQもあわせて参照下さい。
https://faq1.soliton.co.jp/

無線LANの802.1X認証設定

無線アクセスポイント／無線コントローラで、802.1Xを使った無線LAN認証を設定しましょう。
メーカーや機器によって表現が変わる場合がありますが、基本的な設定は共通です。

設定項目	設定値	備考
認証方式	WPA2-Enterprise	機器により、WPA2-EAP、WPA2等の表現もあります
暗号化方式	AES	機器により、CCMP-AES等の表現もあります
RADIUSサーバー	EPS-edgeのIPアドレス	802.1X認証を外部RADIUSサーバーへ問合せます
ポート	1812	
シークレット	EPS-edgeのSecret値	アプライアンス管理のRADIUS設定で設定した値です
アカウンティング	OFF	EPS-edgeはアカウンティング非対応です

Juniper MIST の場合

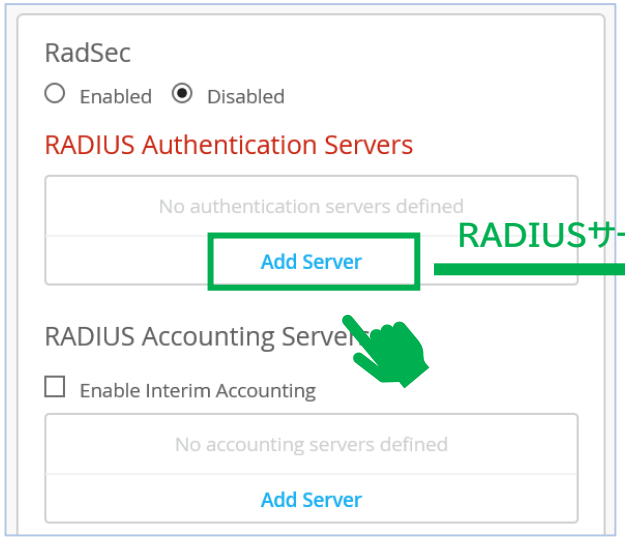


WPA-2/EAP(802.1X)を選択します

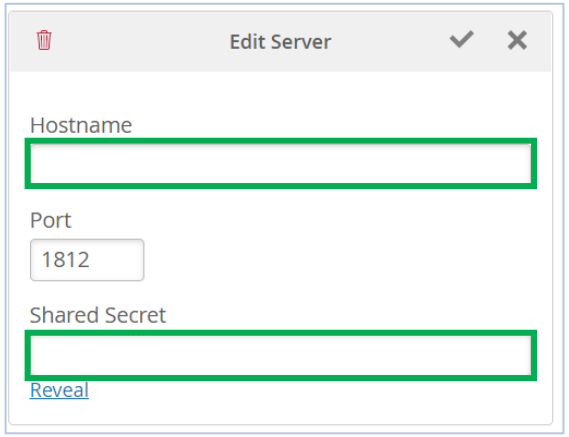
Mist
A Juniper Company

RADIUSサーバーの登録

- Hostname :EPS-edgeのIPアドレス
- Port :1812
- Share Secret :EPS-edgeのSecret



RADIUSサーバーを追加



Cisco Meraki MR の場合

Wi-Fi 認証 Aruba の場合

エンタープライズ
WPA2-エンタープライズを選択

RADIUSサーバーを追加します（下へ）

アカウンティングを無効にします

RADIUSサーバーの登録

- タイプ　　:RADIUS
- 名前　　:任意の登録名
- IPアドレス　:EPS-edgeのIPアドレス
- 共有キー　　:EPS-edgeのSecret

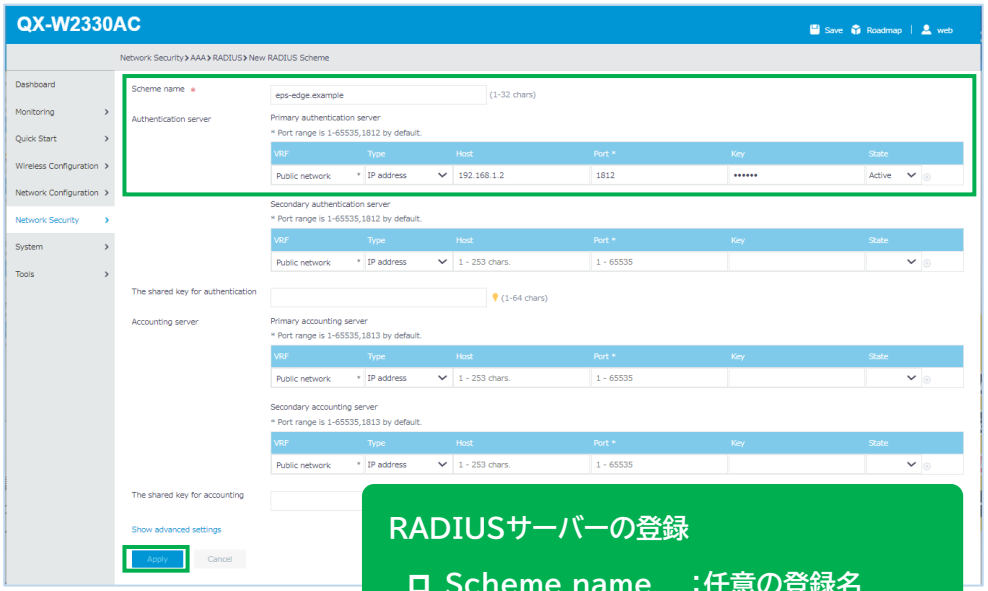
Ruckus の場合

RADIUSサーバーを追加

- 方式　　:802.1x EAP
- 認証サーバー　:追加
- 方式　　:WPA2
- アルゴリズム　:AES
- アカウントサーバー　:無効

- 名前　　:任意の登録名
- タイプ　　:RADIUS
- 暗号化　　:オフ
- 認証方法　:PAP
- IPアドレス　:EPS-edgeのアドレス
- ポート　　:1812
- 共有シークレット:EPS-edgeのSecret

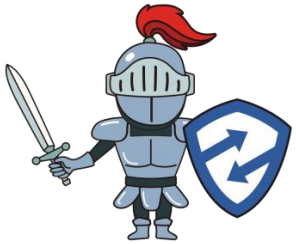
Wi-Fi 認証　NEC（アクセスコントローラー/QX-W2330AC）の場合



RADIUSサーバーの登録

- Scheme name　:任意の登録名
- VRF　:Public network
- Type　:IP address
- Host　:EPS-edgeのアドレス
- Port　:1812
- Key　:EPS-edgeのSecret
- State　:Active

アクセスポイント（QX-W1240）単体での認証連携などの詳細は、FAQに掲載の設定例をご参照ください。
https://faq1.soliton.co.jp/

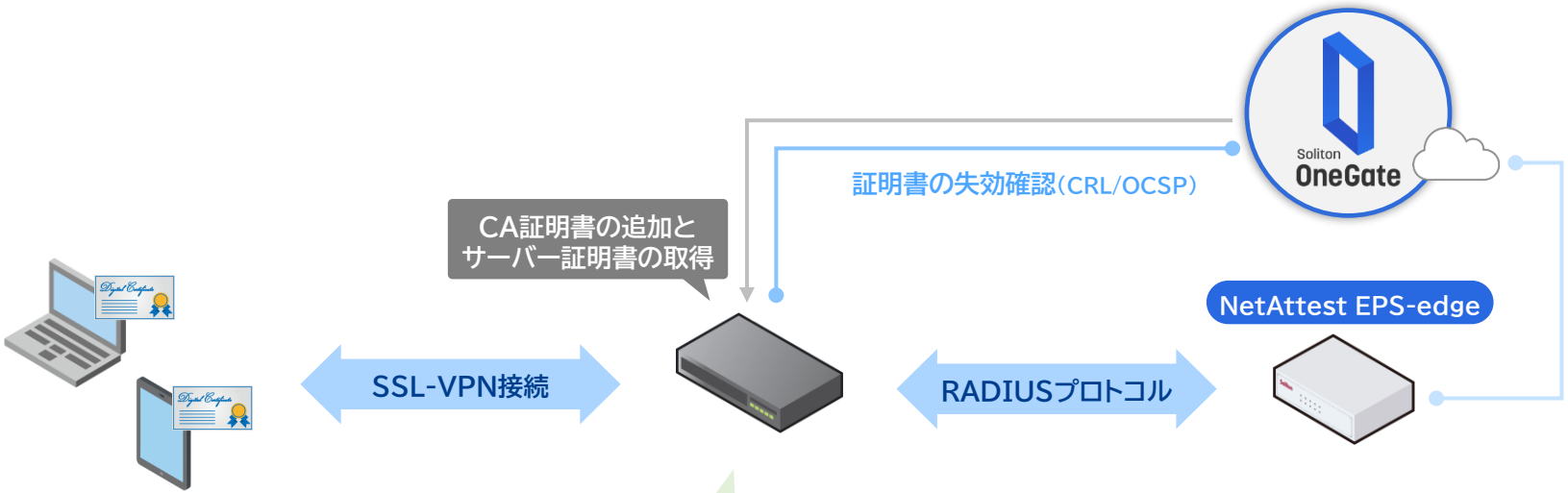


VPN機器の設定例

各機器の設定画面は、当社で連携検証を実施した時点のキャプチャです。
本資料に掲載されていない機器、並びに各機器の最新設定画面はFAQもあわせて参照下さい。
https://faq1.soliton.co.jp/

VPNへ二要素認証の設定

VPN機器で、クライアント証明書とユーザーID・パスワードによる二要素認証の設定をしましょう。
メーカーや機器によって表現が変わる場合がありますが、基本的な設定は共通です。



① クライアント証明書認証のための設定

設定項目	設定値
CA証明書	OneGateのCA証明書をインポート
サーバー証明書	OneGateでサーバー証明書発行も可能（本書では省略）
CRL	CRL配布ポイントURL（CRLのDLによる失効確認）
OCSP	OCSP URL（OCSP URLにアクセスして失効確認）

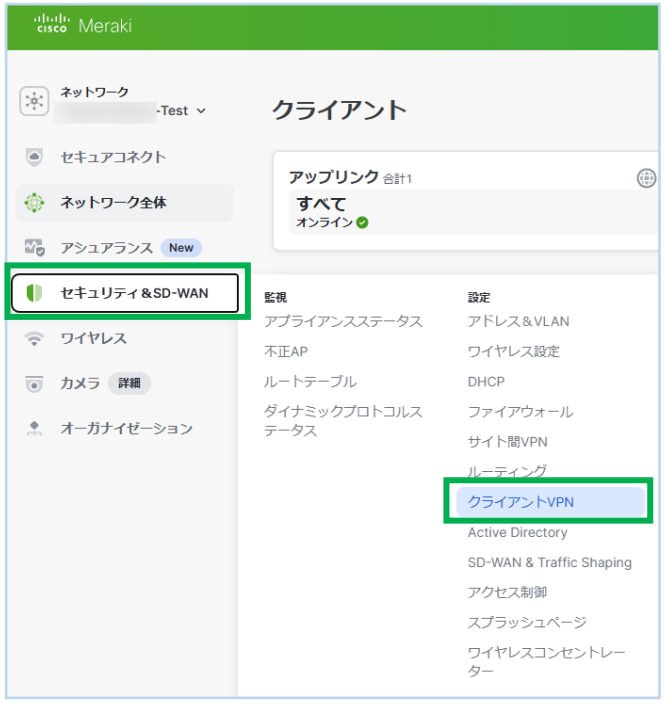
② RADIUS認証のための設定

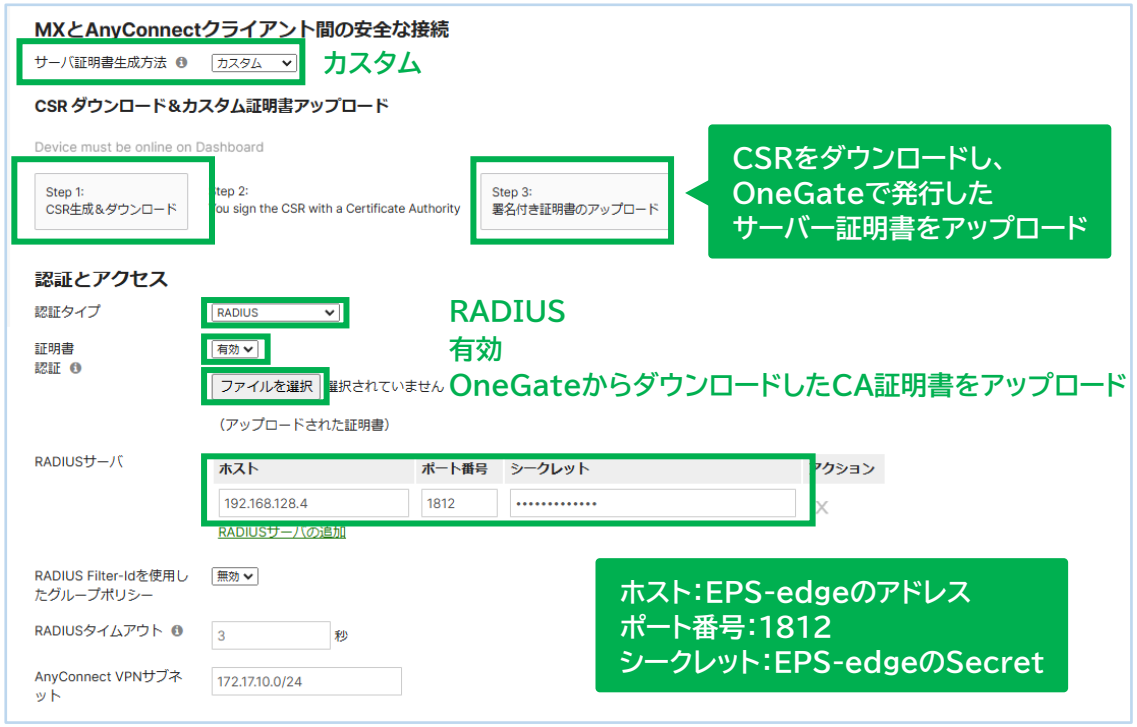
設定項目	設定値
認証プロトコル	PAP
RADIUSサーバー	EPS-edgeのIPアドレス
ポート	1812
シークレット	EPS-edgeのSecret値

※本書ではSSL-VPN方式の設定例を記載しています。

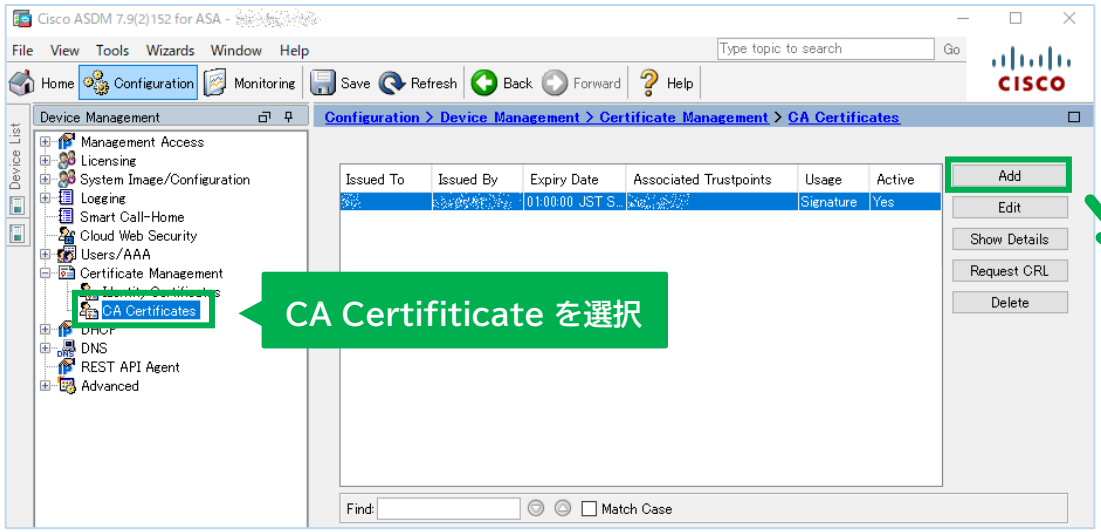
共通）CA証明書のダウンロード

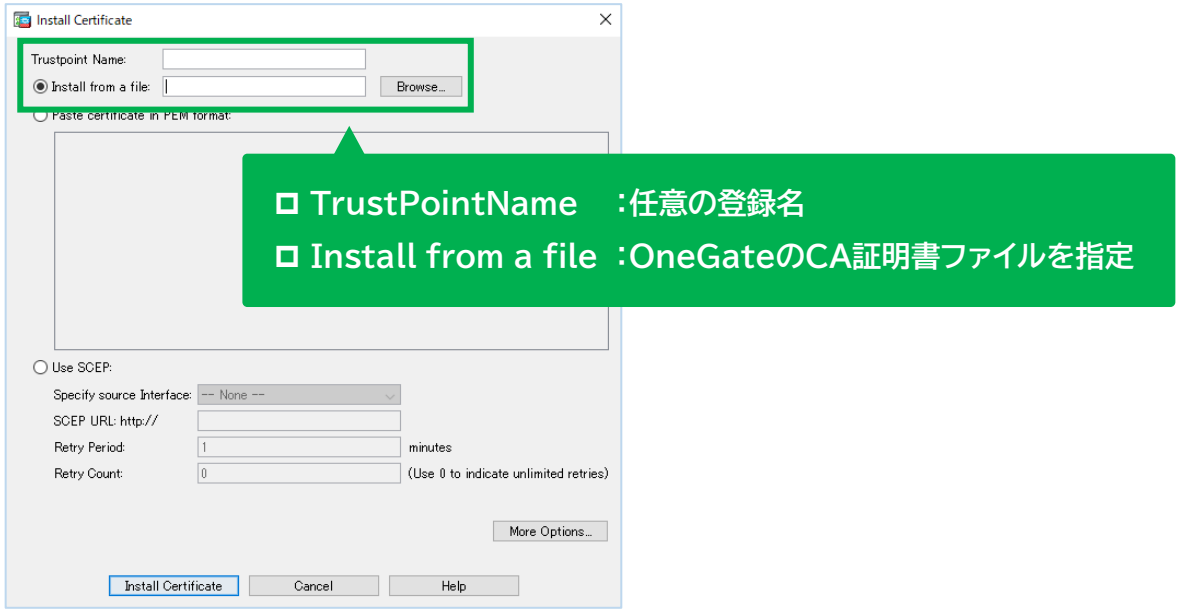
Cisco Meraki MX ～ RADIUS認証設定



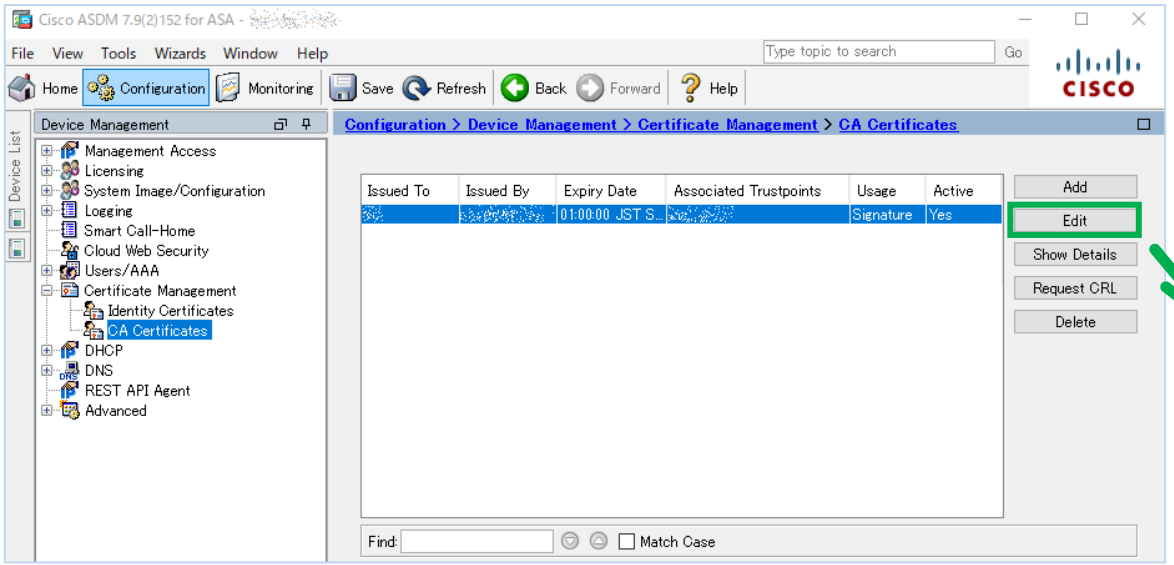


Cisco ASA ～ クライアント証明書認証の設定(1)

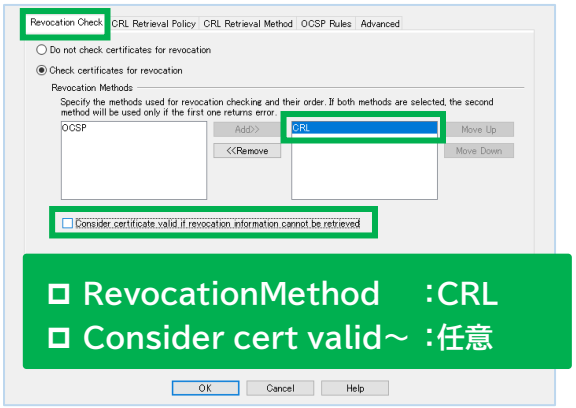




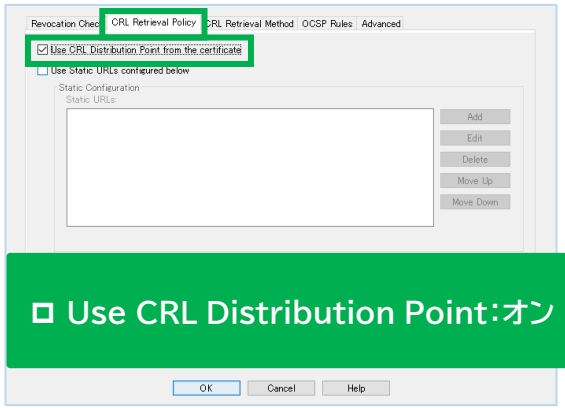
Cisco ASA ～ クライアント証明書認証の設定(2)



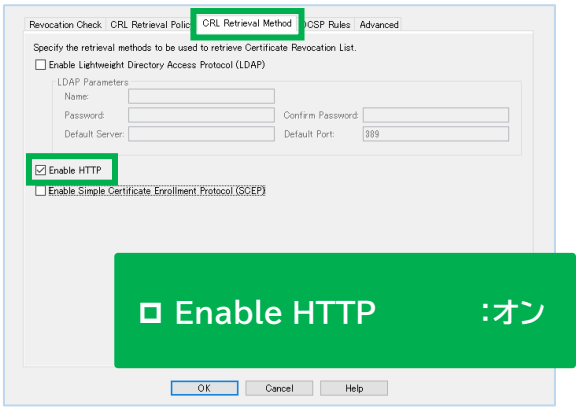
追加したCAをEdit



- RevocationMethod :CRL
- Consider cert valid～ :任意



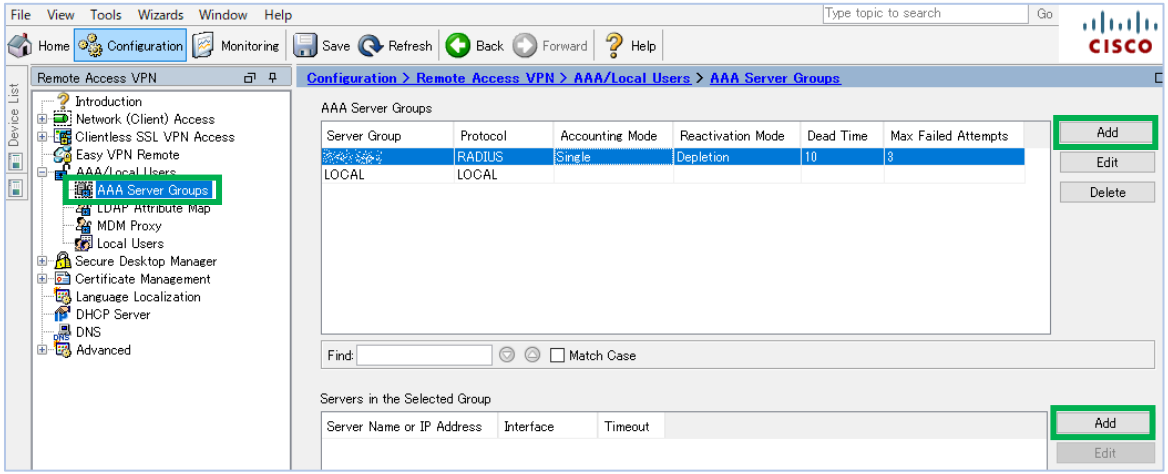
- Use CRL Distribution Point:オン



- Enable HTTP :オン

※CRL方式での動作を確認しています。

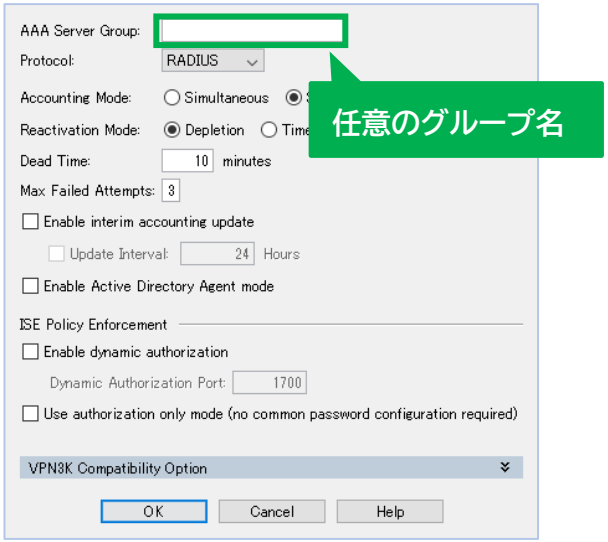
Cisco ASA ～ RADIUS認証の設定(1)



AAA Server Groupsの作成
（左下へ）

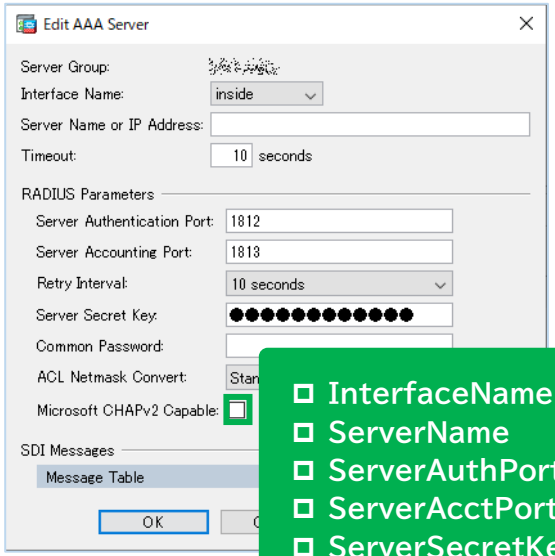
RADIUSサーバーの作成
（右下へ）

AAA Server Groupsを追加



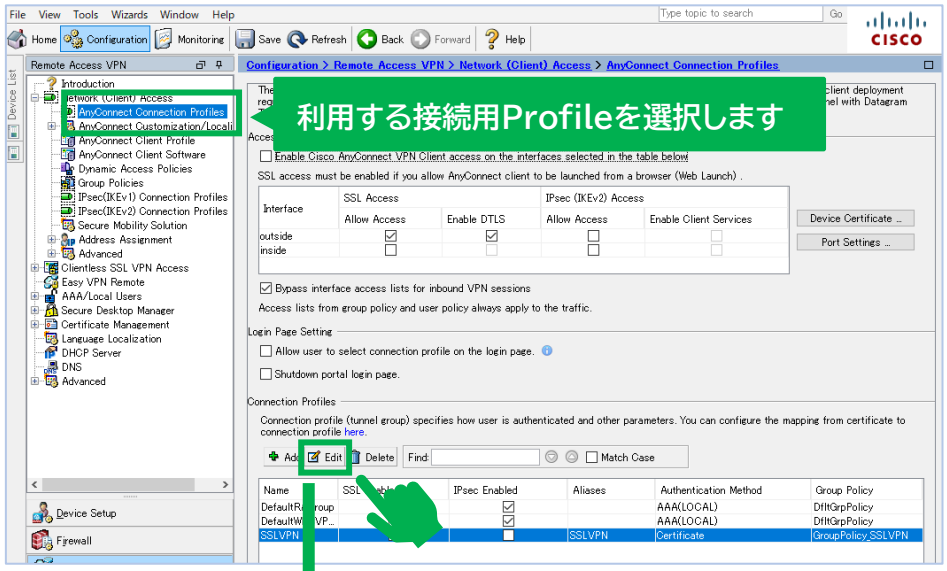
任意のグループ名

RADIUSサーバーを追加

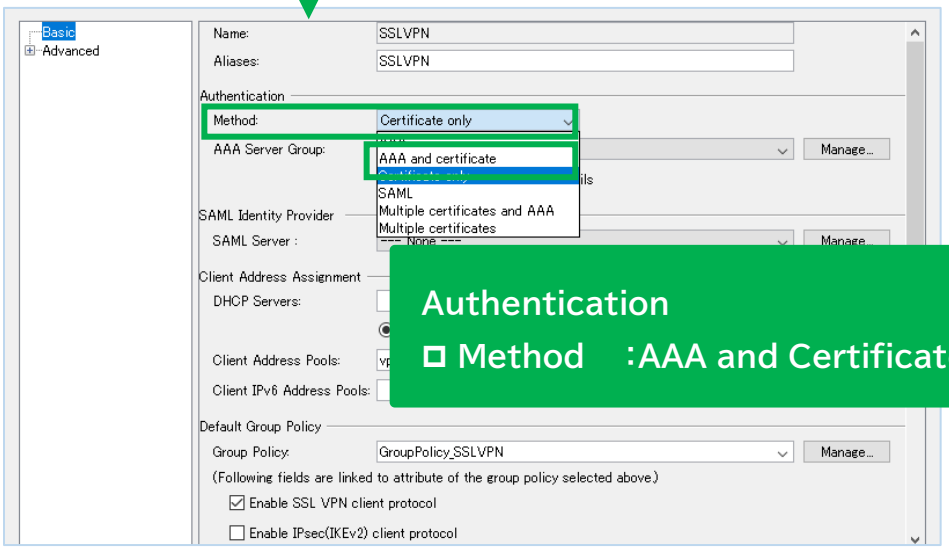


- InterfaceName :EPS-edgeに接続可能なIF
- ServerName :EPS-edgeのアドレス
- ServerAuthPort :1812
- ServerAcctPort :1813（実際は使用しません）
- ServerSecretKey :EPS-edgeのSecret
- MS Chapv2 :オフ

Cisco ASA ～ RADIUS認証の設定(2)



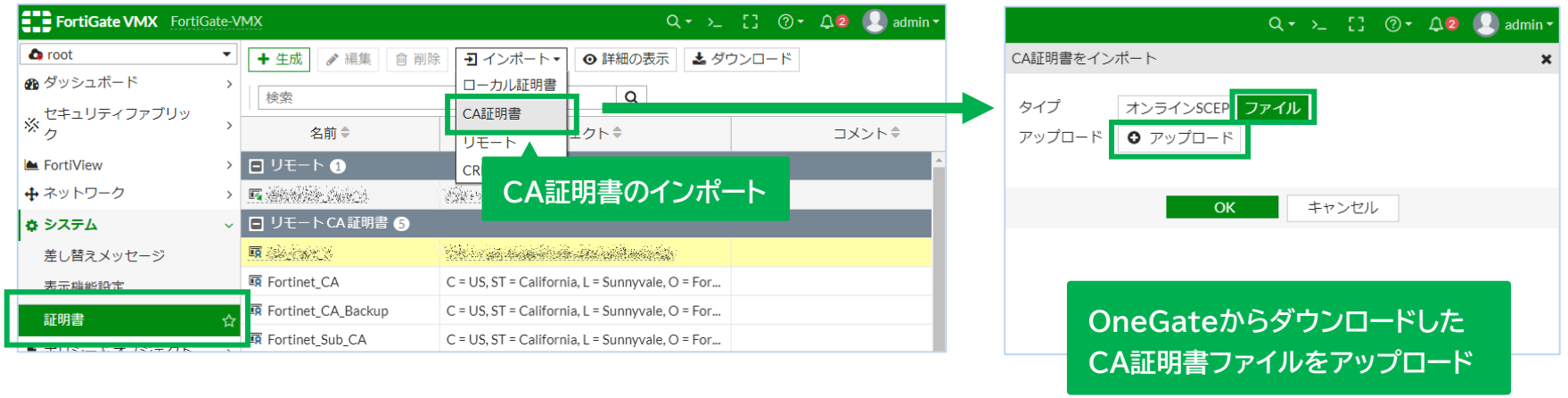
ConnectionProfileを編集(下へ)



Authentication

□ Method　:AAA and Certificate (ID/PW認証＋証明書認証)

FortiGate ～ クライアント証明書認証の設定(1)



□ CLIからOCSPを有効化します。

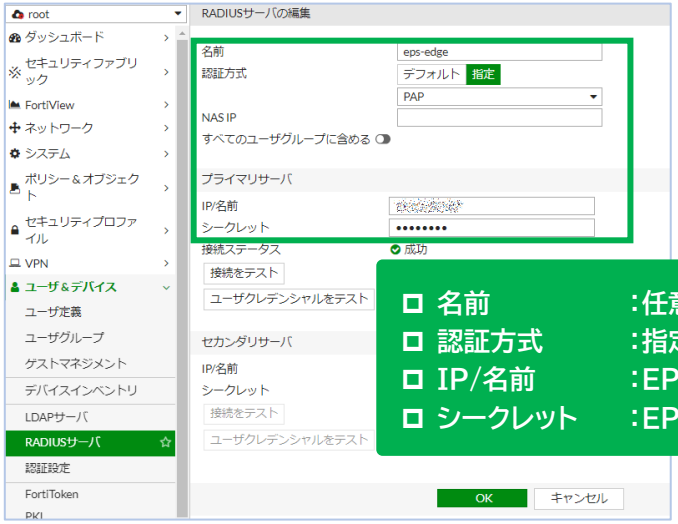
```
FortiGate-VMX (root) # config vpn certificate  setting

FortiGate-VMX (setting) # set ocsp-status enable

FortiGate-VMX (setting) # set ocsp-option server

FortiGate-VMX (setting) # end
```

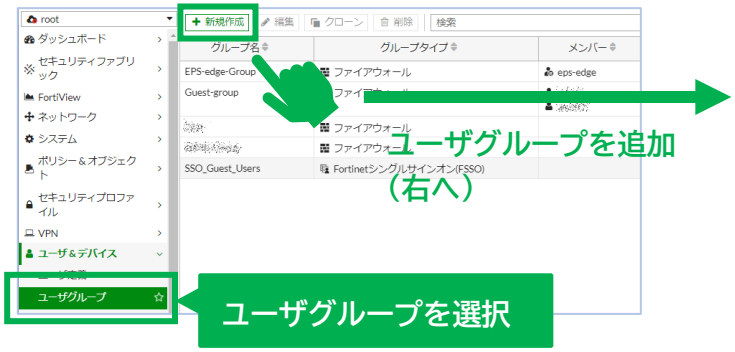
※OCSP方式の場合です。CRL取得方式の場合は、FortiOS6.4.0以上を利用して下さい。

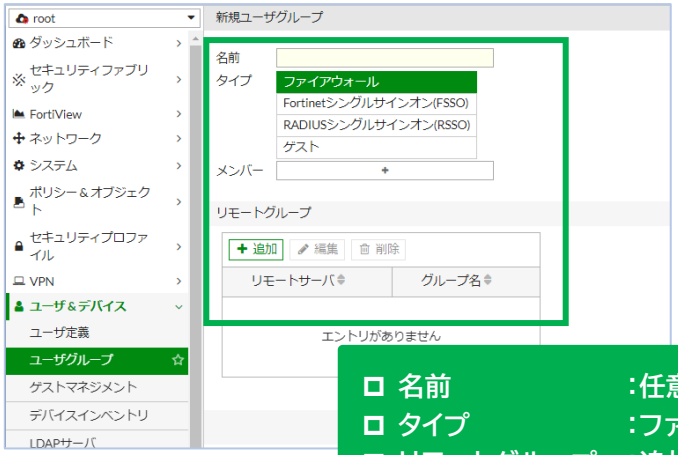
FortiGate ～ クライアント証明書認証の設定(2)

□ クライアント証明書を要求　:オン

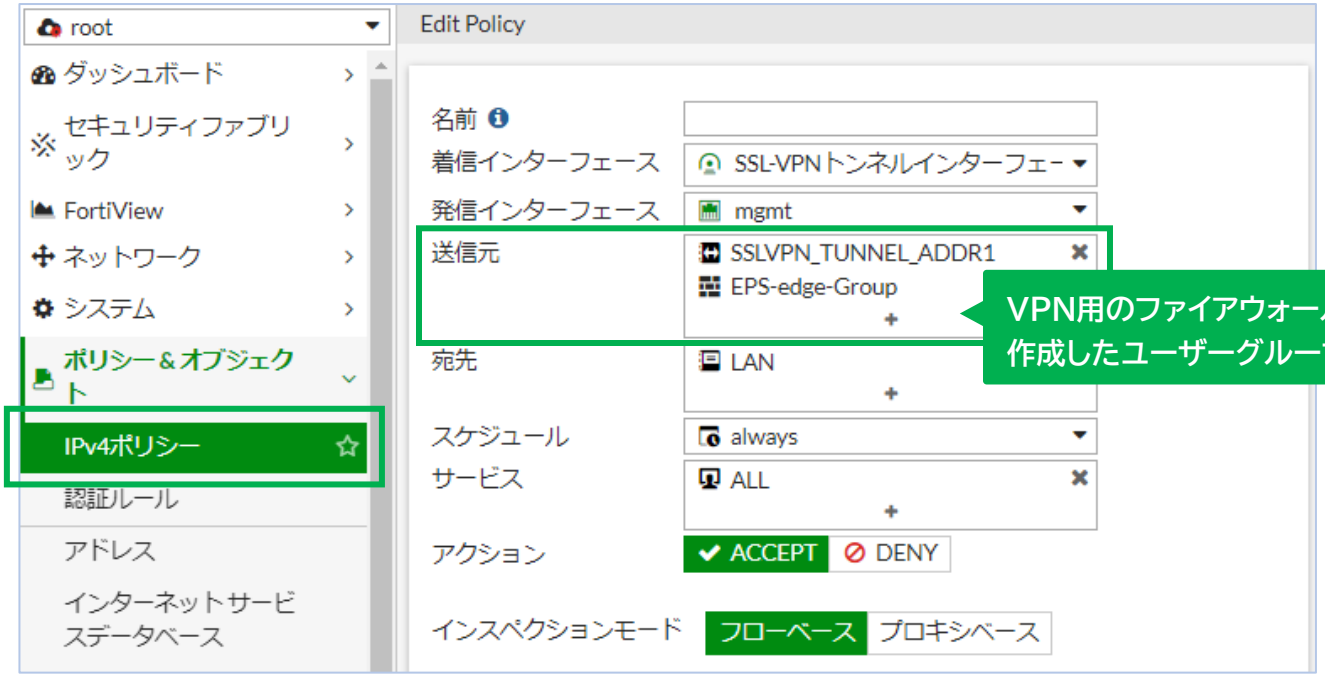
FortiGate ～ RADIUS認証の設定(1)



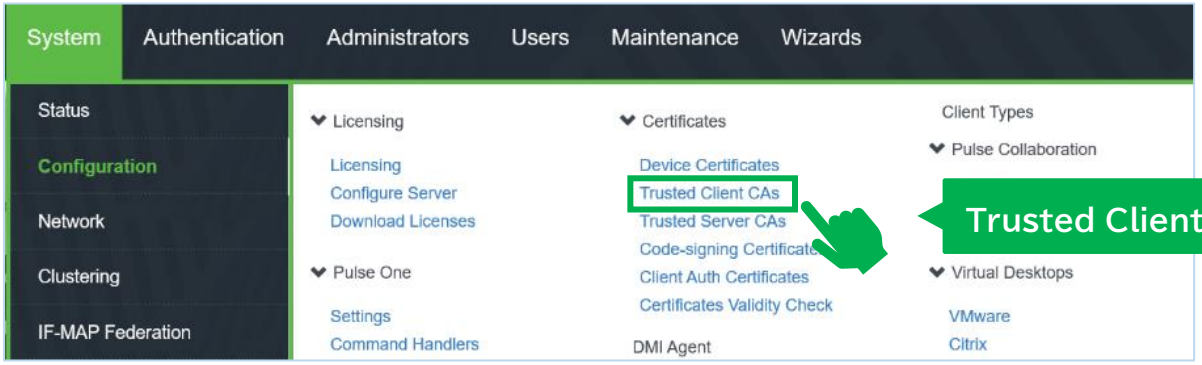


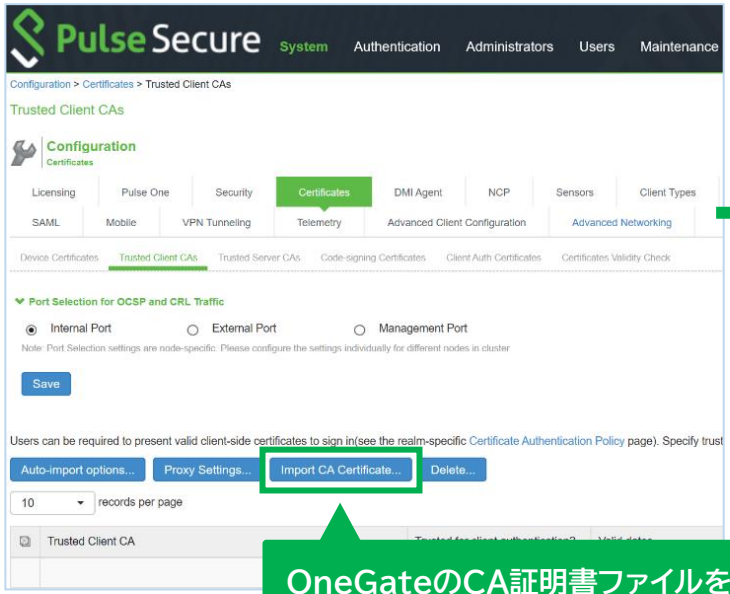


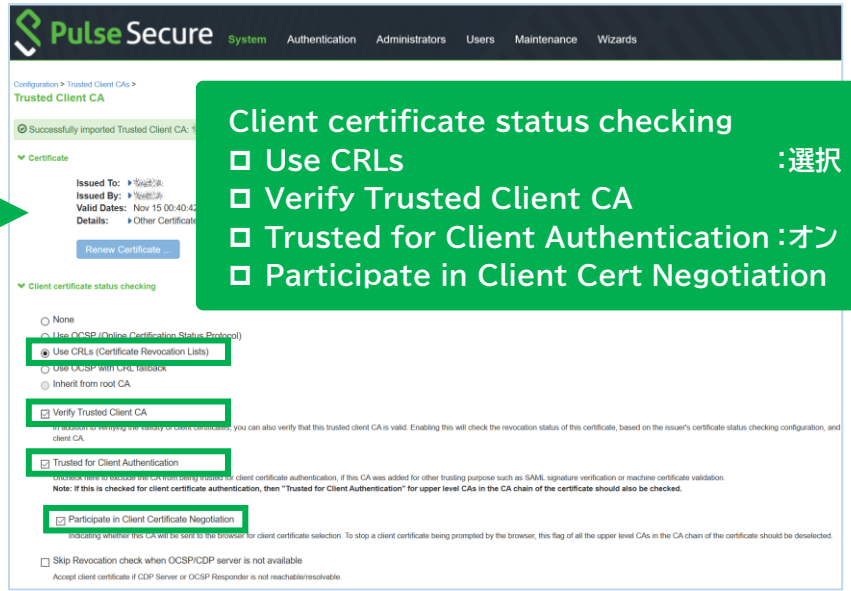
FortiGate ～ RADIUS認証の設定(2)



Pulse Secure ～ クライアント証明書認証の設定(1)

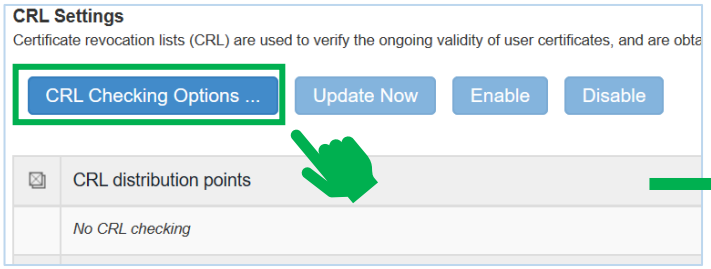


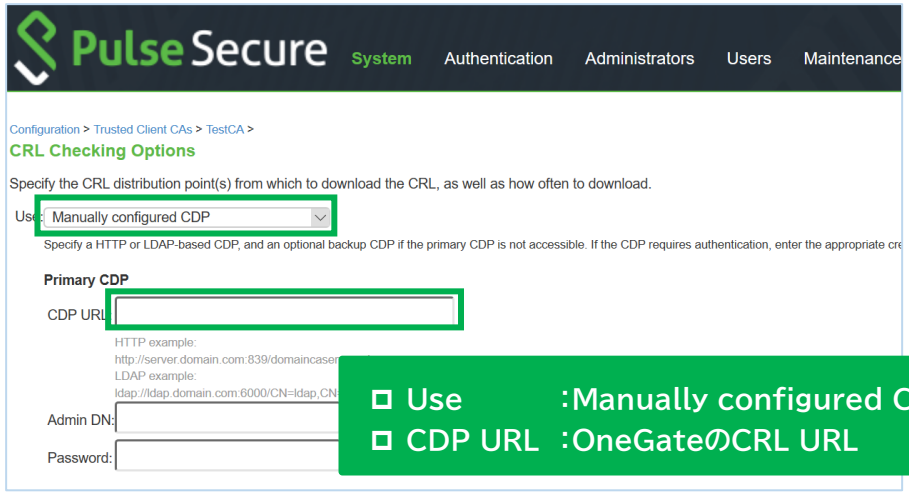




Pulse Secure ～ クライアント証明書認証の設定(2)

CRL Checking Option

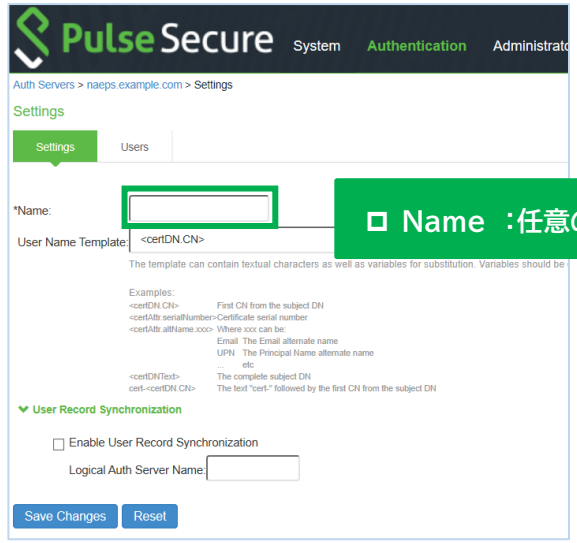




- Use :Manually configured CDP
- CDP URL :OneGateのCRL URL

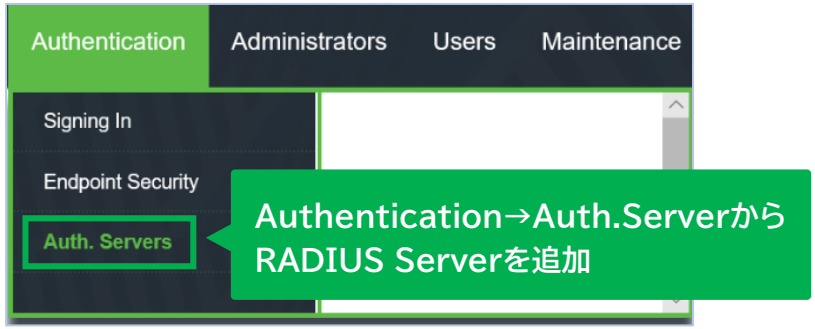
Authentication – Aut.Servers

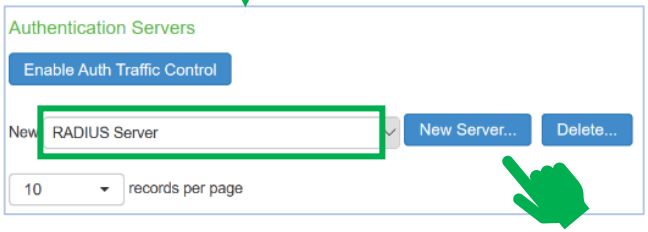
Certificate Serverを選択



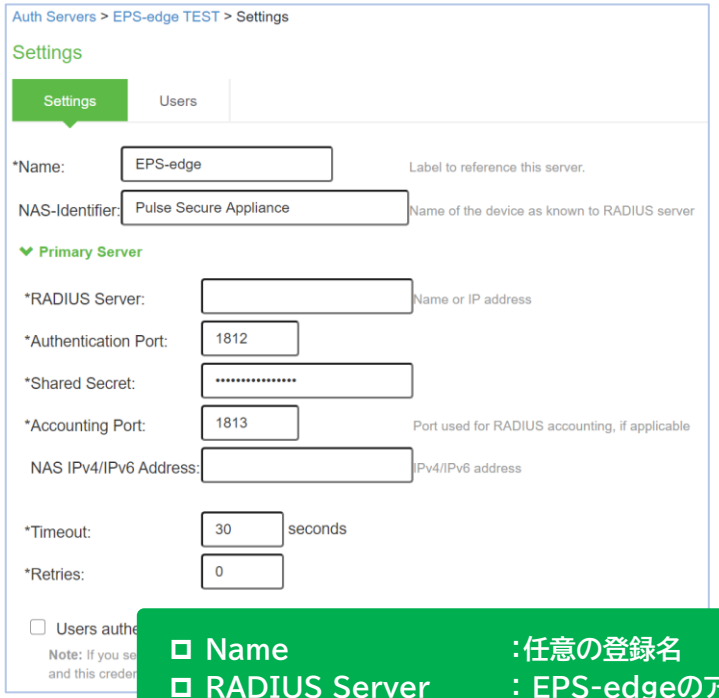
- Name :任意のCertificate Server登録名

Pulse Secure ～ RADIUS認証の設定(1)



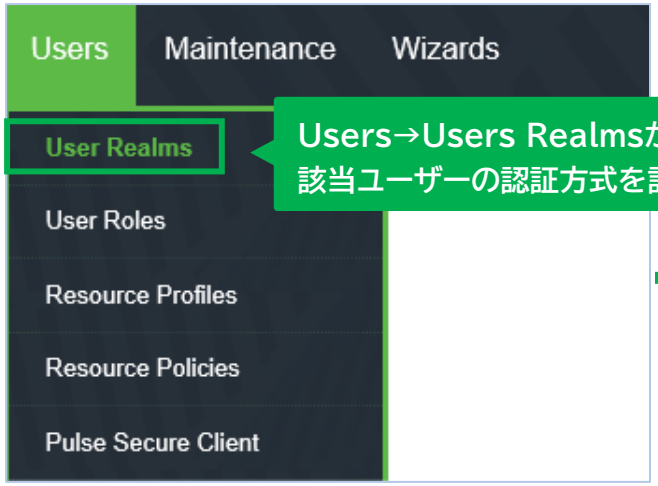


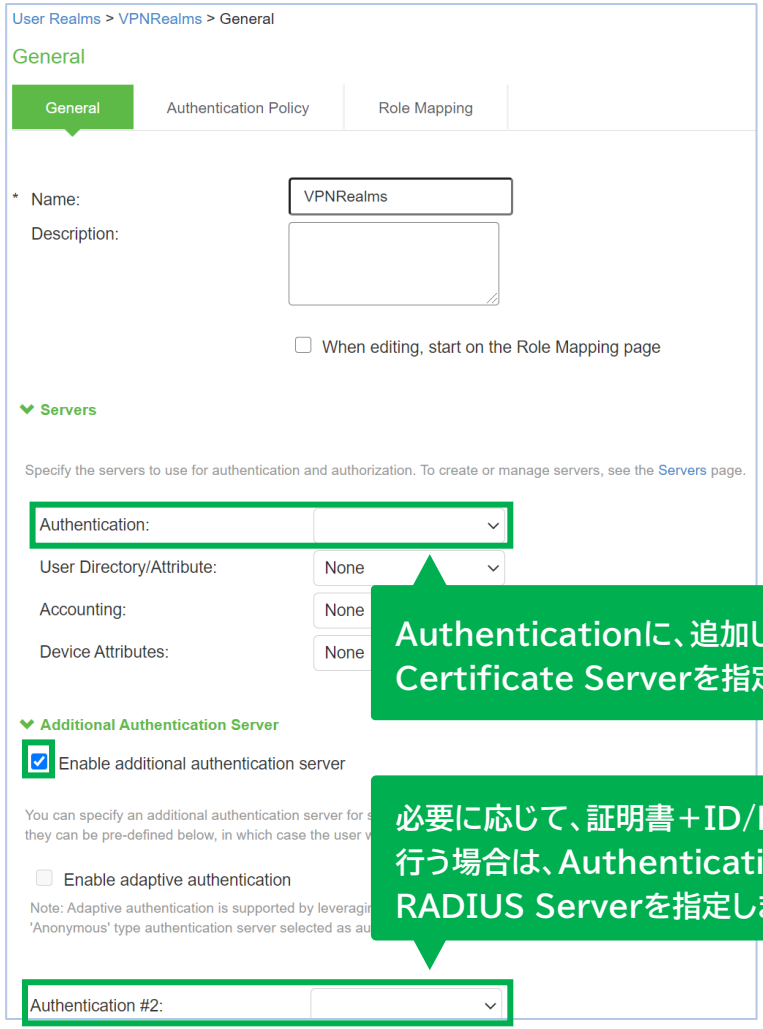
Radiusサーバーを追加
（右へ）

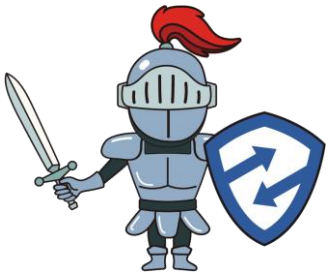


- Name :任意の登録名
- RADIUS Server : EPS-edgeのアドレス
- AuthenticationPort :1812
- AccountingPort :1813
- SharedSecret :EPS-edgeのSecret2

Pulse Secure ～ RADIUS認証の設定(2)







資料のダウンロード、トライアル申込は

ソリトンワンゲート　検索

各機器の設定画面は、当社で連携検証を実施した時点のキャプチャです。
本資料に掲載されていない機器、並びに各機器の最新設定画面はFAQもあわせて参照下さい。
https://faq1.soliton.co.jp/