

Wi-Fi/VPN認証サービスをご検討の方へ

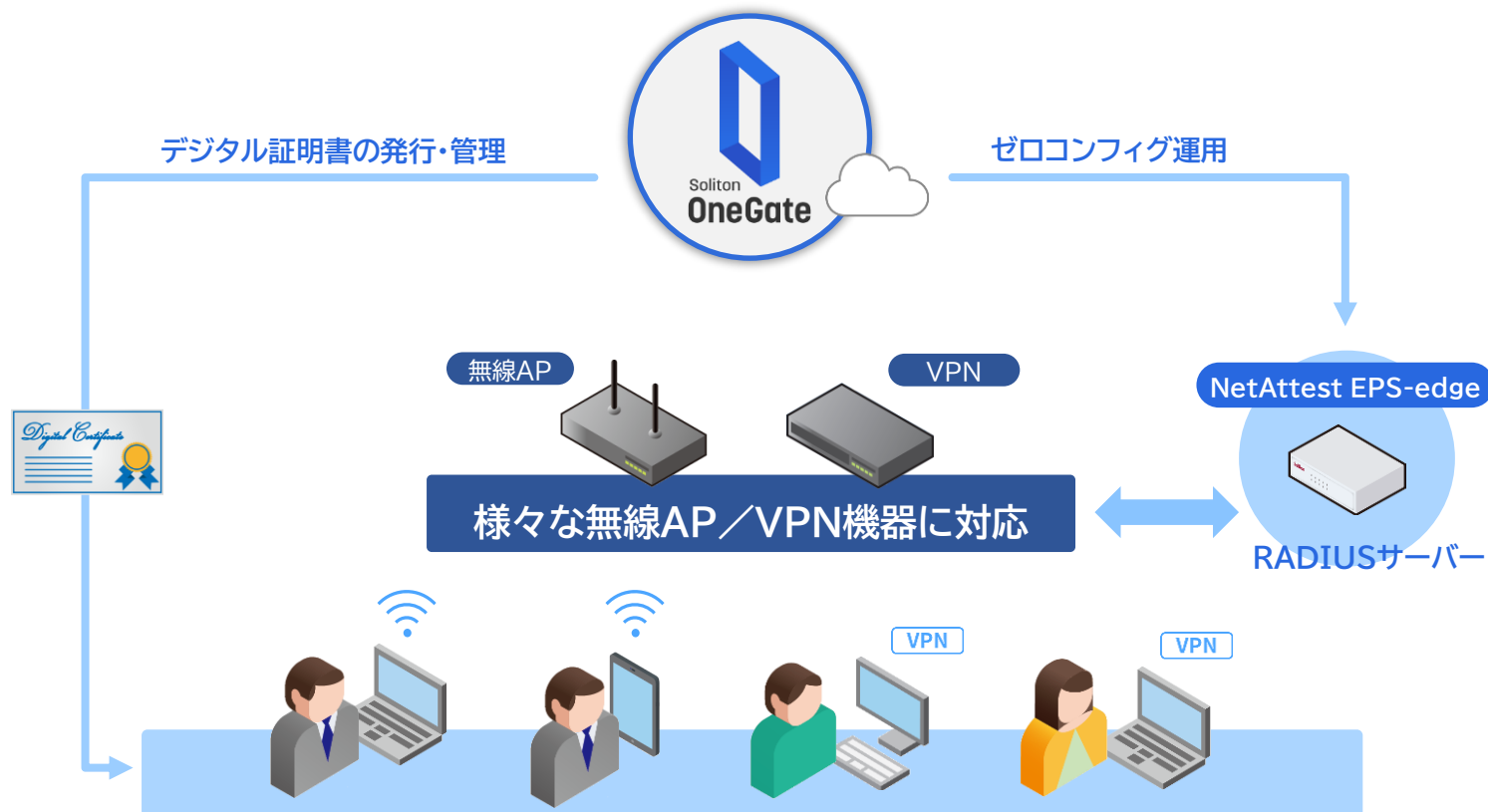
---

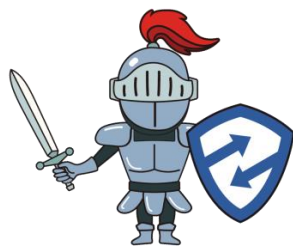
# 各機器の連携設定について



## 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/?site\\_domain=sog](https://faq1.soliton.co.jp/?site_domain=sog)



# 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
アカウントिंग	OFF	EPS-edgeはアカウントिंग非対応です





Security

WPA-2/PSK with passphrase [Reveal](#)

WPA-2/EAP (802.1X)

Open Access

[More Options](#)

Prevent banned clients from associating  
(Contact Mist for firmware)  
Edit banned clients in [Network Security Page](#)

Fast Roaming

Default

Opportunistic Key Caching (OKC)

.11r

WPA-2/EAP(802.1X)を選択します

RadSec

Enabled  Disabled

**RADIUS Authentication Servers**

No authentication servers defined

[Add Server](#)

**RADIUS Accounting Servers**

Enable Interim Accounting

No accounting servers defined

[Add Server](#)

RADIUSサーバーを追加

### 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

Edit Server

Hostname

Port

1812

Shared Secret

[Reveal](#)



## ネットワークアクセス

## 接続条件

- オープン（暗号化なし）  
すべてのユーザが接続可能
- 事前共有キー（PSK）  
接続するにはパスフレーズを入力する必要があります
- MACアドレスベースのアクセス制御（暗号化なし）  
接続時にRADIUSサーバーに問い合わせます。
- エンタープライズ認証 マイRADIUSサーバ  
ユーザ情報は接続時に802.1Xで認証されます
- RADIUSを使用したIdentity PSK  
アソシエーション時にRADIUSサーバーに照会し、クライアントのMACアドレスに基づいてデバイス毎のパスフレーズを取得します。

マイRADIUSサーバーを選択して、  
画面下部でEPS-edgeを登録します

WPA暗号化  
モード

WPA2のみ（ほとんどの展開に推奨）

## RADIUSサーバ

#	ホスト	ポート番号	シークレット	アクション
1	172.17.1.1	1812	secretsecret <span>Hide key</span>	<span>+</span> <span>×</span> <span>Test</span>

[サーバを追加](#)

EPS-edgeのアドレスと  
シークレット値を登録します

## RADIUSテスト ⓘ

RADIUSテストが無効です

## RADIUS CoAサポート ⓘ

RADIUS CoAが無効です

グループポリシーの名前  
を指定するRADIUS属性

Filter-Id ⓘ

## RADIUSアカウントिंग

RADIUSアカウントिंगが無効です

アカウントिंगを無効にします



aruba | VIRTUAL CONTROLLER

新しいネットワーク

1 基本 2 VLAN 3 セキュリティ 4 アクセス

ダッシュボード

概要

ネットワーク

アクセスポイント

クライアント

メッシュデバイス

設定

ネットワーク

アクセスポイント

システム

RF

セキュリティ

セキュリティレベル

セキュリティレベル

エンタープライズ

キー管理

WPA2-エンタープライズ

認証サーバー 1

認証サーバー 2

EAP オフロード

負荷分散

再認証の間隔

0 min.

認証の生存性

MAC 認証

802.1X の前に MAC 認証を実行

MAC 認証フェイルスルー

アカウントング

無効

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)

アカウントングを無効にします

新規認証サーバー

タイプ

RADIUS

LDAP

TACACS

RADIUS タイプ

動的認証のみ

名前

RadSec

IPアドレス

認証ポート

1812

アカウントングポート

1813

共有キー

キーの再入力

タイムアウト

5 秒

キャンセル OK

## 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



### WLAN の作成

認証

方式:  オープン  802.1x EAP  MAC アドレス  802.1x EAP + MAC アドレス

高速 BSS トランジション:  802.11r FT ローミングを有効にする (サポートのために、802.11k 近隣リストレポートを有効にすることを推奨します。)

認証サーバー:

Zero-IT Activation TM:  Zero-IT Activation を有効にする  
(WLAN のユーザーには、ログイン時に構成インストーラーが表示されます。)

暗号化

方式:  WPA2  WPA3  WPA-Mixed  WEP-64 (40 ビット)  WEP-128 (104 ビット)  なし

アルゴリズム:  AES  自動 (TKIP+AES)

802.11w MFP:  無効  オプション  必須

アカウントサーバー:   仮更新を次の間隔で送信:  分

RADIUSサーバーを追加

### 新規作成

名前:

タイプ:  Web ポータル用の AD  LDAP  RADIUS  RADIUS 会計  TACACS+  AD for 802.1x

暗号化:  TLS

認証方法:  PAP  CHAP

バックアップ RADIUS:  バックアップ RADIUS のサポートを有効にする

IP アドレス:

ポート:

共有シークレット:

シークレットの確認:

再試行ポリシー

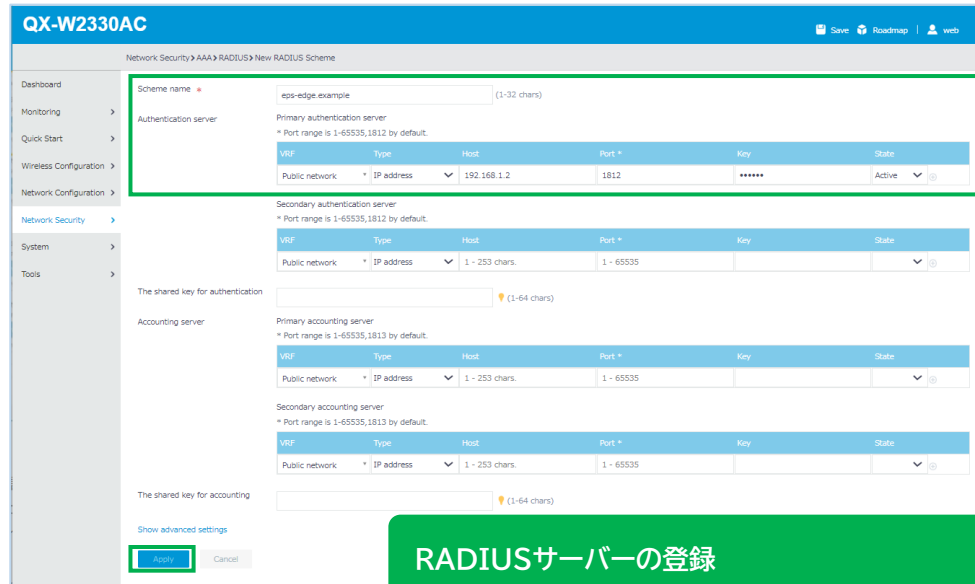
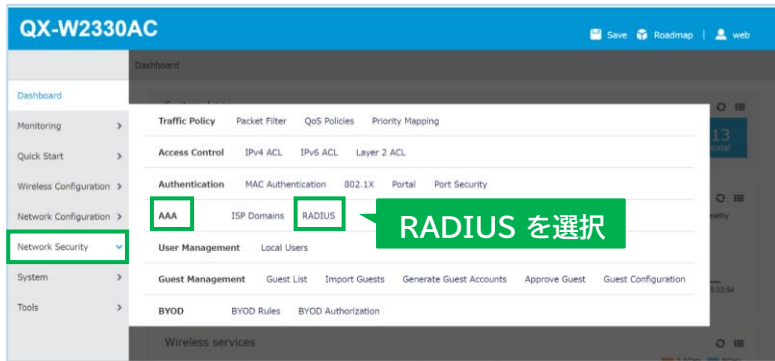
リクエストタイムアウト:  秒間

再試行の最大数:  回

- 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





### RADIUSサーバーの登録

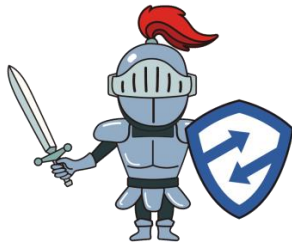
- Scheme name : 任意の登録名
- VRF : Public network
- Type : IP address
- Host : EPS-edgeのアドレス
- Port : 1812
- Key : EPS-edgeのSecret
- State : Active



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。

- [NEC QX-W1240/QX-W2330ACの無線認証連携設定例を教えてください](#)





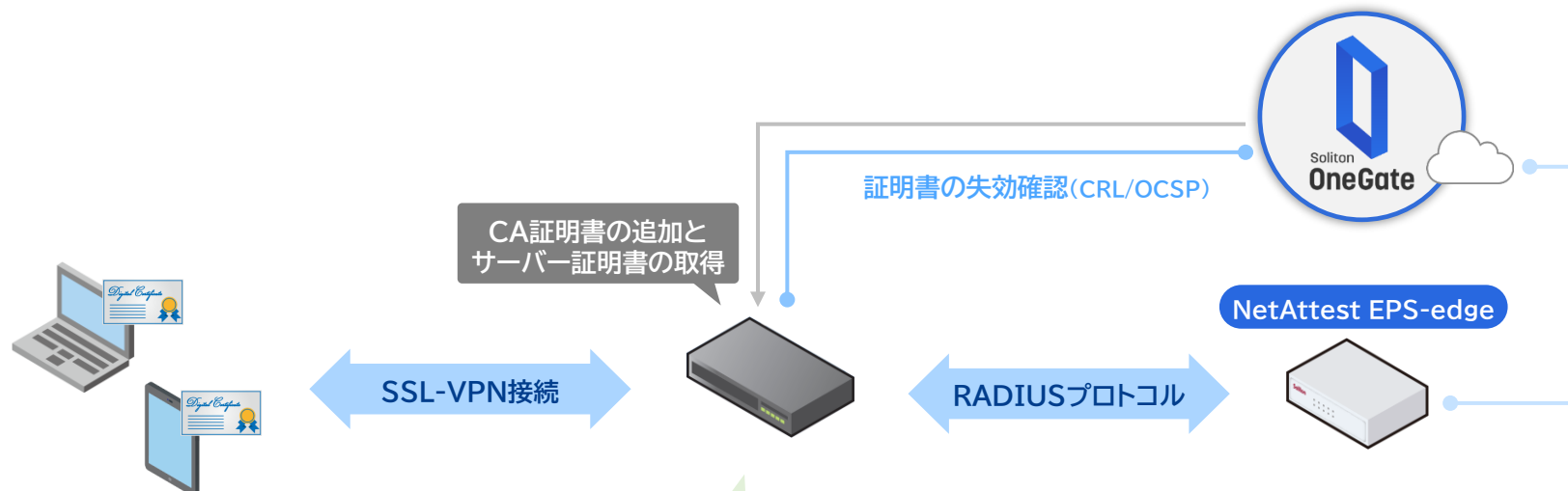
## VPN機器の設定例

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/?site\\_domain=sog](https://faq1.soliton.co.jp/?site_domain=sog)



# VPNでの二要素認証の設定

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方式で、NetAttest EPS-edgeを利用した場合を中心に、主な設定例を抜粋でご紹介しています。詳細な設定方法や、EPS-edgeを利用せず、OneGateをIdPとするSAML認証連携での設定例などは、[FAQ](#)に設定例を掲載していますのでそちらをご参照ください。





利用者管理 ▾ クラウド設定 ▾ AD設定 ▾ **証明書管理 ▾** アプライアンス管理 ▾ 同期スケジュール設定 ▾ システム設定 ▾ ログ管理 ▾

**証明書管理 > CA情報**

以前のCA情報は [こちら](#)

- CA情報
- 招待コード管理
- 証明書一覧
- 証明書ログ

[ 証明書管理 ] - [ CA情報 ]

表示名	?	ids.soliton-ods.jp
公開鍵方式	?	RSA
鍵長	?	2048
名前(CN)	?	ids.soliton-ods.jp
国名(C)	?	
都道府県名(S)	?	
市区町村名(L)	?	
組織名(O)	?	
部署名(OU)	?	
Emailアドレス	?	
署名アルゴリズム	?	SHA256
開始日時	?	2020/07/23 18:57:20
終了日時	?	2030/07/23 18:57:20
OCSP URL	?	http://ids.soliton-ods.jp/certs/1/ocsp
CRL配布ポイント URL	?	http://ids.soliton-ods.jp/certs/1/certs.crl
CA証明書ファイルのダウンロード	?	DER形式 <input checked="" type="radio"/> PEM形式

OCSPとCRLのURLが確認できます

CA証明書がダウンロードできます



Meraki

ネットワーク -Test

クライアント

アップリンク 合計1  
すべて  
オンライン

セキュリティ&SD-WAN

ワイヤレス

カメラ 詳細

オーガナイゼーション

監視

アプライアンスステータス

不正AP

ルータテーブル

ダイナミックプロトコルステータス

設定

アドレス&VLAN

ワイヤレス設定

DHCP

ファイアウォール

サイト間VPN

ルーティング

クライアントVPN

Active Directory

SD-WAN & Traffic Shaping

アクセス制御

スプラッシュページ

ワイヤレスコンセントレーター

## クライアントVPN

[IPsec設定](#) | [AnyConnect設定](#) | [FAQs](#)

AnyConnect Client VPN  有効 **有効**

無効

## MXとAnyConnectクライアント間の安全な接続

サーバ証明書生成方法  **カスタム**

## CSRダウンロード&amp;カスタム証明書アップロード

Device must be online on Dashboard

Step 1:  
CSR生成&ダウンロードStep 2:  
You sign the CSR with a Certificate AuthorityStep 3:  
署名付き証明書のアップロード

CSRをダウンロードし、  
OneGateで発行した  
サーバ証明書をアップロード

## 認証とアクセス

認証タイプ

RADIUS

RADIUS

証明書  
認証

有効

有効

ファイルを選択

OneGateからダウンロードしたCA証明書をアップロード

(アップロードされた証明書)

RADIUSサーバ

ホスト	ポート番号	シークレット	アクション
192.168.128.4	1812	.....	X

RADIUSサーバの追加

RADIUS Filter-Idを使用し  
たグループポリシー

無効

RADIUSタイムアウト

3 秒

AnyConnect VPNサブネ  
ット

172.17.10.0/24

ホスト:EPS-edgeのアドレス  
ポート番号:1812  
シークレット:EPS-edgeのSecret



Cisco ASDM 7.9(2)152 for ASA - Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
		01:00:00 JST S		Signature	Yes

Find:   Match Case

Buttons: Add, Edit, Show Details, Request CRL, Delete

Install Certificate

Trustpoint Name:

Install from a file:

Paste certificate in PEM format

Use SCEP:

Specify source Interface:

SCEP URL: http://

Retry Period:  minutes

Retry Count:  (Use 0 to indicate unlimited retries)

- TrustPointName : 任意の登録名
- Install from a file : OneGateのCA証明書ファイルを指定

Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
		01:00:00 JST S...		Signature	Yes

Buttons: Add, Edit, Show Details, Request CRL, Delete

Find:  Match Case

追加したCAをEdit

Revocation Check | CRL Retrieval Policy | CRL Retrieval Method | OCSP Rules | Advanced

Do not check certificates for revocation

Check certificates for revocation

Revocation Methods:  
Specify the methods used for revocation checking and their order. If both methods are selected, the second method will be used only if the first one returns error.

OCSP:  Add>> CRL Move Up <<Remove

Consider certificate valid if revocation information cannot be retrieved

OK Cancel Help

□ RevocationMethod :CRL  
□ Consider cert valid~ :任意

Revocation Check | CRL Retrieval Policy | CRL Retrieval Method | OCSP Rules | Advanced

Use CRL Distribution Point from the certificate

Use static URLs configured below

Static Configuration  
Static URLs:

Add Edit Delete Move Up Move Down

OK Cancel Help

□ Use CRL Distribution Point:オン

Revocation Check | CRL Retrieval Policy | CRL Retrieval Method | OCSP Rules | Advanced

Specify the retrieval methods to be used to retrieve Certificate Revocation List.

Enable Lightweight Directory Access Protocol (LDAP)

LDAP Parameters:  
Name:   
Password:  Confirm Password:   
Default Server:  Default Port: 389

Enable HTTP

Enable Simple Certificate Enrollment Protocol (SCEP)

OK Cancel Help

□ Enable HTTP :オン

※CRL方式での動作を確認しています。



The screenshot shows the Cisco ASA configuration interface. The left pane shows the configuration tree with 'AAA Server Groups' selected. The main pane displays the 'AAA Server Groups' table:

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	RADIUS	Single	Depletion	10	3

Green boxes highlight the 'Add' buttons in the top right and bottom right of the configuration pane. A green hand icon points to the top 'Add' button.

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

The 'Add AAA Server Group' dialog box is shown. The 'AAA Server Group' field is highlighted with a green box. A green callout box points to this field with the text '任意のグループ名' (Arbitrary group name).

Other fields include: Protocol (RADIUS), Accounting Mode (Simultaneous/Single), Reactivation Mode (Depletion/Time), Dead Time (10 minutes), Max Failed Attempts (3), and various checkboxes for accounting and authorization options.

任意のグループ名

### RADIUSサーバーを追加

The 'Edit AAA Server' dialog box is shown. Fields include: Server Group, Interface Name (inside), Server Name or IP Address, Timeout (10 seconds), RADIUS Parameters (Server Authentication Port: 1812, Server Accounting Port: 1813, Retry Interval: 10 seconds, Server Secret Key, Common Password, ACL Netmask Convert, Microsoft CHAPv2 Capable), and SDI Messages.

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



File View Tools Wizards Window Help

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

利用する接続用Profileを選択します

Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch).

Interface	SSL Access	Enable DTLS	IPsec (IKEv2) Access	Enable Client Services
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

Allow user to select connection profile on the login page.

Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Add Edit Delete Find: Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultR group	<input type="checkbox"/>	<input type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
DefaultW VPN	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
SSLVPN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	SSLVPN	Certificate	GroupPolicy_SSLVPN

ConnectionProfileを編集(下へ)

Basic Advanced

Name: SSLVPN

Aliases: SSLVPN

Authentication

Method: Certificate only

AAA Server Group: AAA and certificate

SAML Identity Provider: Multiple certificates and AAA

SAML Server: NONE

Client Address Assignment

DHCP Servers:

Client Address Pools:

Client IPv6 Address Pools:

Default Group Policy

Group Policy: GroupPolicy\_SSLVPN

(Following fields are linked to attribute of the group policy selected above.)

Enable SSL VPN client protocol

Enable IPsec(IKEv2) client protocol

Authentication

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



CA証明書のインポート

OneGateからダウンロードしたCA証明書ファイルをアップロード

□ 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。

ここでは、NetAttest EPS-edgeを利用したRADIUS認証の設定例を抜粋してご紹介しています。詳細な設定方法や、EPS-edgeを利用せず、OneGateをIdPとするSAML認証連携での設定例は、FAQに設定例を掲載していますのでそちらをご参照ください。

- [フォーティネット FortiGateとのVPN認証連携設定例を教えてください\(RADIUS認証\)](#)
- [FortiGateのシングルサインオン設定例を教えてください\(SAML認証\)](#)

The screenshot shows the FortiGate VMX web interface for configuring SSL-VPN settings. The left sidebar shows the navigation menu with 'VPN' expanded and 'SSL-VPN設定' selected. The main content area is titled 'SSL-VPN設定' and includes the following settings:

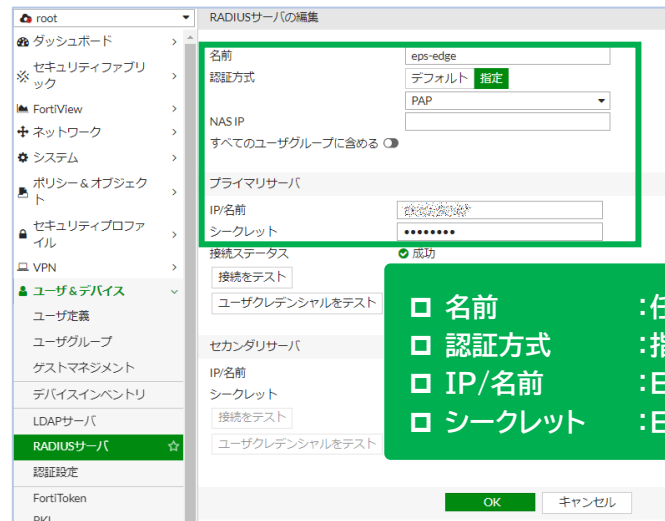
- 接続設定**
  - リッスンするインターフェース: [選択済み]
  - リッスンするポート: 10443
  - Webモードアクセスをリッスンするポート: [https://\[選択済み\]:10443](https://[選択済み]:10443)
- HTTPをSSL-VPNにリダイレクトする:
- アクセスを制限: **任意のホストからアクセス許可** (highlighted in green)
- アイドルログアウト:  (highlighted in green)
- 非アクティブ: 300 秒
- サーバ証明書: fgt.example.jp
- クライアント証明書を要求**:  (highlighted in green with a hand icon)

The 'トンネルモードクライアント設定' section is partially visible at the bottom, showing 'アドレス範囲' set to '自動的にアドレス割り当て'.

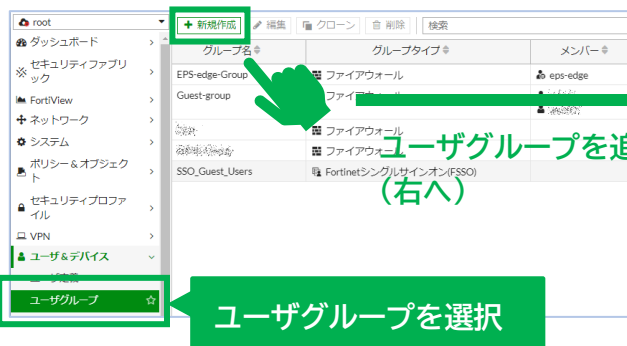
クライアント証明書を要求 :オン



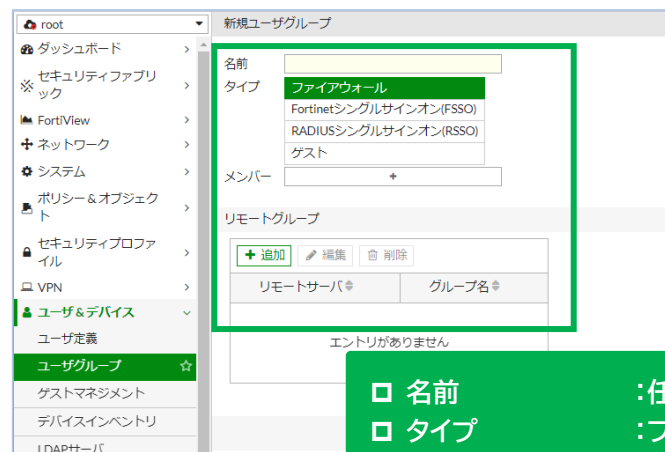
RADIUSサーバを追加  
(右へ)



- 名前 : 任意の登録名
- 認証方式 : 指定/PAP
- IP/名前 : EPS-edgeのアドレス
- シークレット : EPS-edgeのSecret



ユーザグループを追加  
(右へ)



- 名前 : 任意のユーザグループ名
- タイプ : ファイアウォール
- リモートグループ : 追加したRADIUSを選択



The screenshot displays the FortiGate WebUI configuration page for an IPv4 Policy. The left sidebar shows the navigation menu with 'IPv4ポリシー' selected. The main area shows the 'Edit Policy' configuration page with the following settings:

- 名前: [Empty field]
- 着信インターフェース: SSL-VPNトンネルインターフェー
- 発信インターフェース: mgmt
- 送信元: SSLVPN\_TUNNEL\_ADDR1, EPS-edge-Group
- 宛先: LAN
- スケジュール: always
- サービス: ALL
- アクション: ACCEPT (checked), DENY
- インスペクションモード: フローベース (checked), プロキシベース

A green callout box points to the '送信元' field, containing the text: "VPN用のファイアウォールポリシーの送信元に作成したユーザーグループを追加します".

System Administration Interface Navigation:

- System
- Authentication
- Administrators
- Users
- Maintenance
- Wizards

Configuration Menu:

- Licensing
  - Licensing
  - Configure Server
  - Download Licenses
- Pulse One
  - Settings
  - Command Handlers
- Certificates
  - Device Certificates
  - Trusted Client CAs**
  - Trusted Server CAs
  - Code-signing Certificates
  - Client Auth Certificates
  - Certificates Validity Check
  - DMI Agent
- Client Types
  - Pulse Collaboration
  - Virtual Desktops
    - VMware
    - Citrix

Trusted Client CAを選択

Configuration > Certificates > Trusted Client CAs

Trusted Client CAs

Configuration

Device Certificates | **Trusted Client CAs** | Trusted Server CAs | Code-signing Certificates | Client Auth Certificates | Certificates Validity Check

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 trust

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

10 records per page

Trusted Client CA

OneGateのCA証明書ファイルを  
インポート

Configuration > Trusted Client CAs > Trusted Client CA

Successfully imported Trusted Client CA: [Certificate Name]

Renew Certificate...

Client certificate status checking

- None
- Use OCSP (Online Certificate Status Protocol)
- Use CRLs (Certificate Revocation Lists)
- Use OCSP with CRL fallback
- Inherit from root CA
- Verify Trusted Client CA
- Trusted for Client Authentication
- Participate in Client Certificate Negotiation
- Skip Revocation check when OCSP/CDP server is not available

Accept client certificate if CDP Server or OCSP Responder is not reachable/resolvable.

Client certificate status checking

- Use CRLs : 選択
- Verify Trusted Client CA : オン
- Trusted for Client Authentication : オン
- Participate in Client Cert Negotiation : オン

## CRL Checking Option

**CRL Settings**  
Certificate revocation lists (CRL) are used to verify the ongoing validity of user certificates, and are obtained from the following distribution points.

	CRL distribution points
	No CRL checking

**Pulse Secure** System Authentication Administrators Users Maintenance

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:

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.

**Primary CDP**

CDP URL:

HTTP example:  
http://server.domain.com:839/domain.com

LDAP example:  
ldap://ldap.domain.com:6000/CN=ldap.CN

Admin DN:

Password:

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

## Authentication - Aut.Servers

**Pulse Secure** System Authentication Administrators Users Maintenance

Authentication Servers

New:

records per page

Name	Type
Administrators	Local Authentication
	RADIUS Server
System Local	Local Authentication

**Certificate Serverを選択**

**Pulse Secure** System Authentication Administrators

Auth Servers > naeps.example.com > Settings

Settings

Name:

User Name Template: <certDN.CN>

The template can contain textual characters as well as variables for substitution. Variables should be enclosed in <tags>.

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-ccertDN.CN> The text "cert-" followed by the first CN from the subject DN

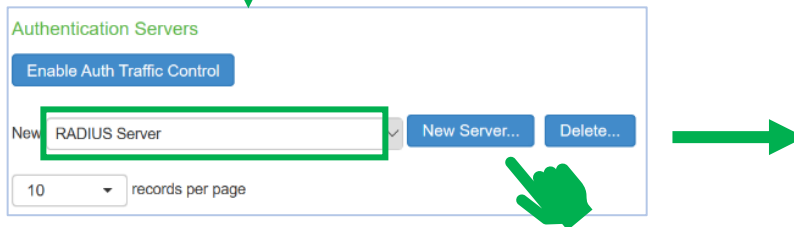
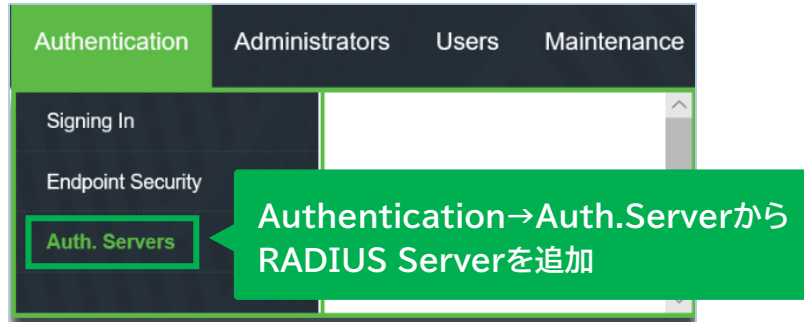
**User Record Synchronization**

Enable User Record Synchronization

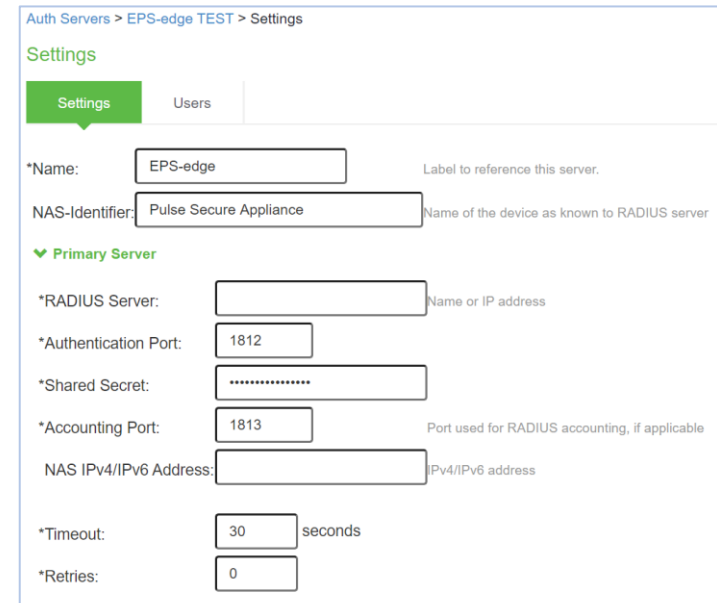
Logical Auth Server Name:

- Name : 任意のCertificate Server登録名





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Secret





Users→Users Realmsから  
該当ユーザーの認証方式を設定

The screenshot shows the configuration page for a User Realm named 'VPNRealms'. The 'General' tab is active. The 'Name' field is set to 'VPNRealms'. The 'Description' field is empty. There is a checkbox for 'When editing, start on the Role Mapping page' which is unchecked. Under the 'Servers' section, the 'Authentication' dropdown is highlighted with a green box. Below it, 'User Directory/Attribute', 'Accounting', and 'Device Attributes' are all set to 'None'. Under the 'Additional Authentication Server' section, the 'Enable additional authentication server' checkbox is checked. Below this, there is a note about adaptive authentication and another dropdown for 'Authentication #2' which is also highlighted with a green box.

Authenticationに、追加した  
Certificate Serverを指定します

必要に応じて、証明書+ID/PW認証を  
行う場合は、Authentication #2に  
RADIUS Serverを指定します



The screenshot shows the Palo Alto Networks management console interface. The top navigation bar includes 'PA-440', 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE' (highlighted with a green box). Below the navigation bar, there is a search bar and a table of certificates. The table has columns for '名前', 'サブジェクト', '発行者', 'CA', 'キー', '有効期限', '状態', 'アルゴリズム', and '用途'. A green callout box points to the 'インポート' (Import) button in the bottom toolbar.

OneGateのCA証明書と  
OneGateで発行したサーバー証明書をインポート

The '証明書のインポート' (Certificate Import) dialog box is shown. It has the following fields and options:

- 証明書タイプ:  ローカル  SCEP
- 証明書名: OneGate\_CA
- 証明書ファイル: C:\fakepath\OneGateCAPem.cer (with a '参照...' button)
- ファイルフォーマット: Base64 エンコード済み証明書 (PEM)
- 秘密鍵はハードウェアセキュリティ モジュール上にあります
- 秘密鍵をインポート
- 秘密鍵のエクスポートをブロック
- キー ファイル: (with a '参照...' button)
- パスフレーズ: (with a '参照...' button)
- パスフレーズの確認: (with a '参照...' button)

Buttons at the bottom: OK, キャンセル

- 証明書名 : 任意の登録名(例: OneGate CA)
- 証明書ファイル: 参照をクリックしOneGateのCA証明書ファイルを指定

ここでは、NetAttest EPS-edgeを利用したRADIUS認証の設定例を抜粋してご紹介しています。EPS-edgeを利用せずOneGateをIdPとするSAML認証連携、Prisma AccessとのSAML認証連携は、FAQに設定例を掲載していますのでそちらをご参照ください。

- [Palo Alto Networks PAシリーズのシングルサインオン設定例を教えてください\(SAML認証\)](#)
- [Prisma Accessのシングルサインオン設定例を教えてください\(SAML認証\)](#)

PA-440 DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE** Commit

0 個の項目

名前	場所	ユーザー名フィールド	ユーザードメイン	名前	デフォルト OCSP URL	OCSP 検証証明書	CRL の使用	OCSP の使用	CRL 受信の有効期限	OCSP 受信の有効期限	証明書の有効期限	不明な証明書のプロック	タイムアウト証明書のプロック	未認証の証明書のプロック	証明書が失効しているセッションをプロック

証明書プロファイル

追加 削除 コピー PDF/CSV

証明書プロファイルを追加

証明書プロファイル

名前 CertProfile\_OneGate

ユーザー名フィールド None

ユーザードメイン

CA 証明書

CA 証明書 OneGate\_CA

デフォルト OCSP URL http://10.10.10.10:8080/ocsp

OCSP 検証証明書 None

テンプレート名/OID

デフォルト OCSP URL (http:// または https:// で開始する必要があります)

CRL の使用

OCSP の使用

CRL より OCSP を優先

CRL 受信の有効期限 (sec) 5

OCSP 受信の有効期限 (sec) 5

証明書の有効期限 (sec) 5

証明書状態が不明な場合にセッションをブロック

タイムアウト時間内に証明書状態を取得できない場合にセッションをブロック

証明書が認証側デバイスに発行されなかった場合セッションをブロック

期限切れ証明書のセッションをブロック

OK キャンセル

証明書プロファイル

名前 CertProfile\_OneGate

ユーザー名フィールド None

ユーザードメイン

CA 証明書

名前	デフォルト OCSP URL	OCSP 検証証明書	テンプレート名/OID
OneGate_CA			

デフォルト OCSP URL (http:// または https:// で開始する必要があります)

CRL の使用

OCSP の使用

CRL より OCSP を優先

CRL 受信の有効期限 (sec) 5

OCSP 受信の有効期限 (sec) 5

証明書の有効期限 (sec) 5

証明書状態が不明な場合にセッションをブロック

タイムアウト時間内に証明書状態を取得できない場合にセッションをブロック

証明書が認証側デバイスに発行されなかった場合セッションをブロック

期限切れ証明書のセッションをブロック

OK キャンセル

□ CA証明書: 先ほど登録したCA証明書(例: OneGate\_CA)

□ デフォルトOCSP URL: OneGateのOCSP URL

□ 名前 :任意の名前(例: CertProfile\_OneGate)

□ CRLの使用 :チェック(任意)

□ OCSPの使用 :チェック(任意)



PA-440 DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE** Commit

応答ページ  
ログ設定  
サーバー プロファイル  
SNMP トラップ  
Syslog  
電子メール  
HTTP  
Netflow  
**RADIUS**  
SCP  
TACACS+

名前	場所	サーバー	その他
1 個の項目			

追加 削除 コピー PDF/CSV

RADIUSサーバープロファイルを追加

RADIUS サーバー プロファイル

プロファイル名

管理者使用のみ

サーバー設定

タイムアウト(sec)

再試行

認証プロトコル

サーバー

名前	RADIUS SERVER	シークレット	ポート
eps-edge.example	172.16.7.89	*****	1812

追加 削除

RADIUS サーバーの IP アドレスまたは FQDN を入力してください

OK キャンセル

- プロファイル名 : 任意の登録名
- サーバーの名前 : EPS-edgeのホスト名
- RADIUS SERVER : EPS-edgeのアドレス
- シークレット : EPS-edgeのSecret
- ポート : 1812

高可用性  
設定監査  
パスワードプロファイル  
管理者  
管理者ロール  
**認証プロファイル**  
認証シーケンス  
ユーザー ID  
データ再配信  
デバイス検疫  
VM 情報ソース

名前	場所	ロックアウト		許可リスト	認証	サーバープロファイル	認証ファクター	その他	ロックされたユーザー
		許容ログイン回数	ロックアウト時間 (分)						
AuthProfile_...			0	all	ローカル				none
AuthProfile_...			0	all	SAMLメタデータ	SAMLProfile...			none
AuthProfile_L...			0	all	SAMLメタデータ	SAMLProfile...			none

3 個の項目s → X

+ 追加 - 削除 コピー PDF/CSV

認証プロファイルを追加

認証プロファイル

名前 AuthProfile\_RADIUS

認証 | 度 | **詳細**

タイプ RADIUS

サーバープロファイル RADIUSProfile\_EPS-edge

RADIUS からユーザー グループを取得

ユーザードメイン

ユーザー名修飾子 %USERINPUT%

シングルサインオン

Kerberos レベルム

Kerberos キータブ [インポート] をクリックして、このフィールドを設定し [X] インポート

OK キャンセル

詳細タブをクリック

AuthProfile\_RADIUS

認証 | 度 | 詳細

許可リスト

許可リスト ^

all

+ 追加 - 削除

アカウントのロックアウト

許容ログイン回数 [0 - 10]

ロックアウト時間 (分) 0

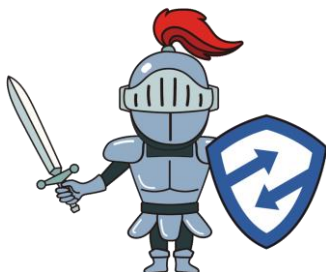
OK キャンセル

- プロファイル名 : 任意の登録名
- サーバプロファイル : 先ほど設定したEPS-edgeのプロファイル

許可リストの追加をクリックし、対象リストを設定してOKをクリック  
(この認証方式を利用するリストとなります。環境に合わせて設定します。)

※ここで作成したRADIUS認証プロファイルをGlobal Protectポータルにて設定します。





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/?site\\_domain=sog](https://faq1.soliton.co.jp/?site_domain=sog)

