

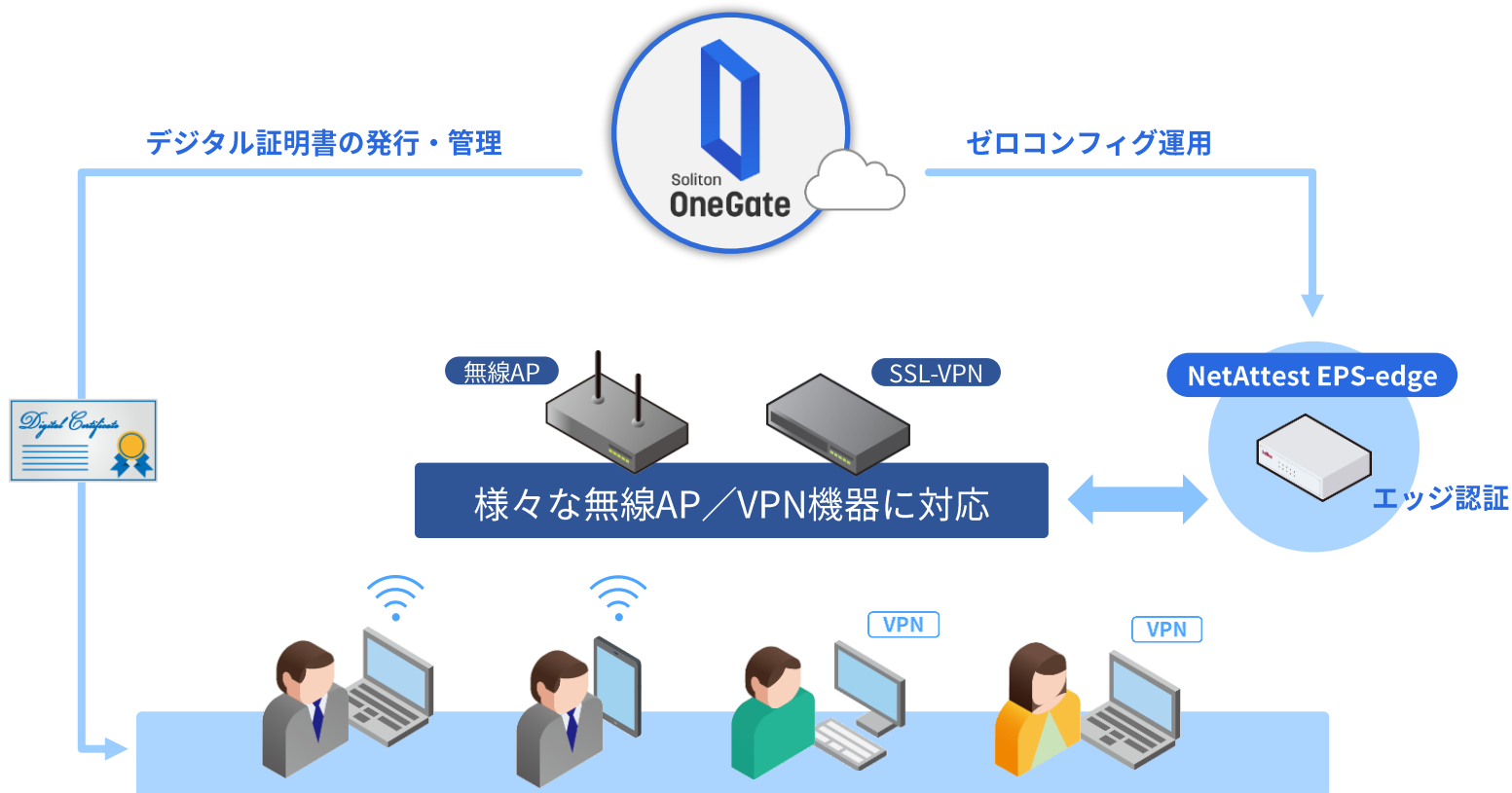
Wi-Fi/VPN認証サービスをご検討の方へ

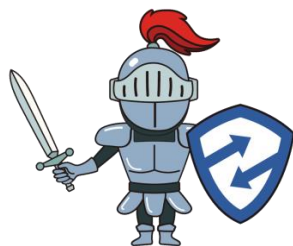
各機器の連携設定について



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

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 Hide key	+ × Test

[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 認証を執行

MAC 認証フェイルスルー

アカウントING

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ING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INGポート

1813

共有キー

キーの再入力

タイムアウト

5 秒

単位は秒数

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

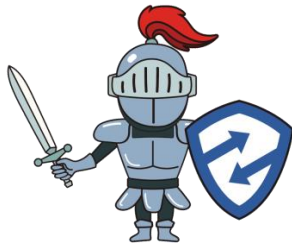
リクエストタイムアウト: 秒間

再試行の最大数: 回

OK キャンセル

- 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

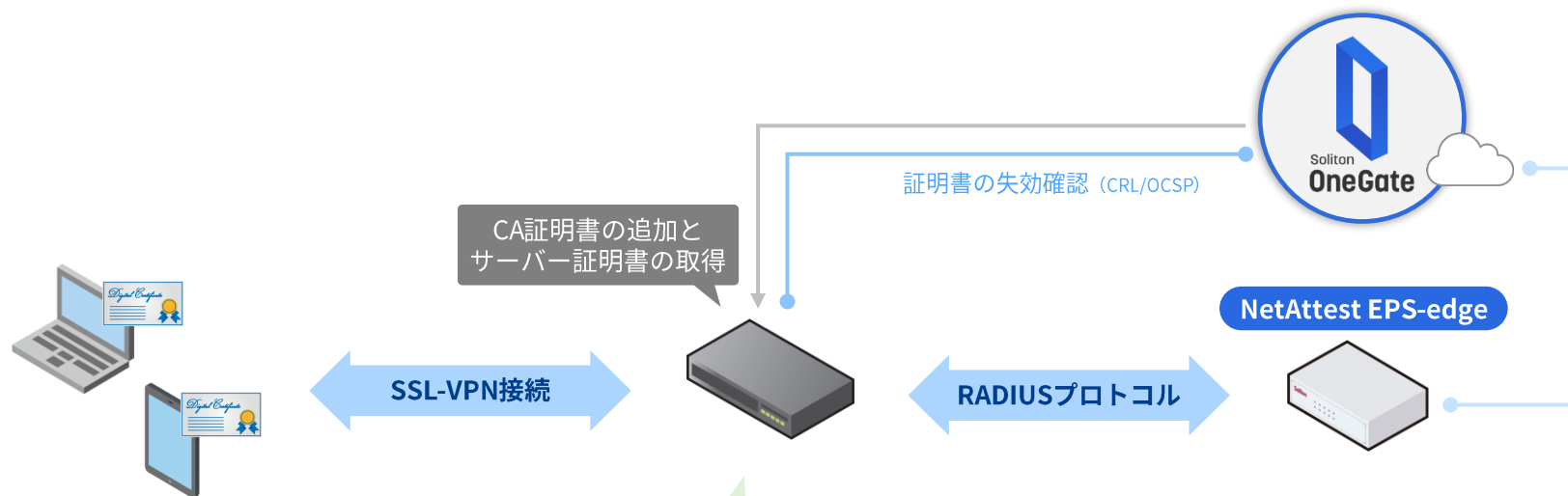
- 名前 : 任意の登録名
- タイプ : RADIUS
- 暗号化 : オフ
- 認証方法 : PAP
- IPアドレス : EPS-edgeのアドレス
- ポート : 1812
- 共有シークレット : EPS-edgeのSecret



VPN機器の設定例

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。





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

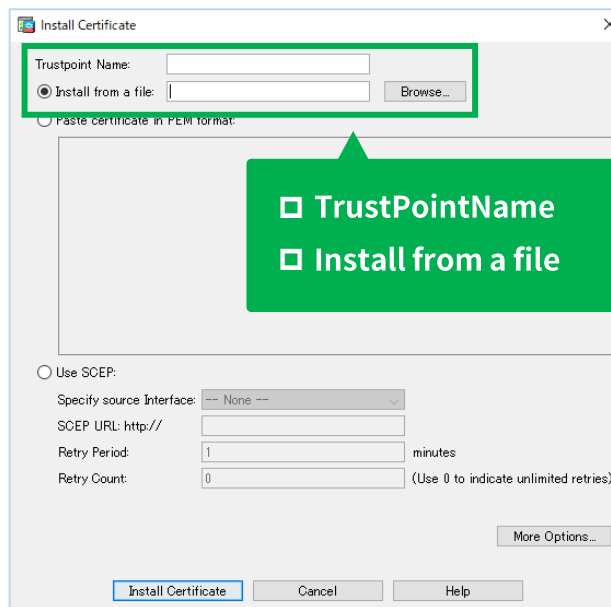
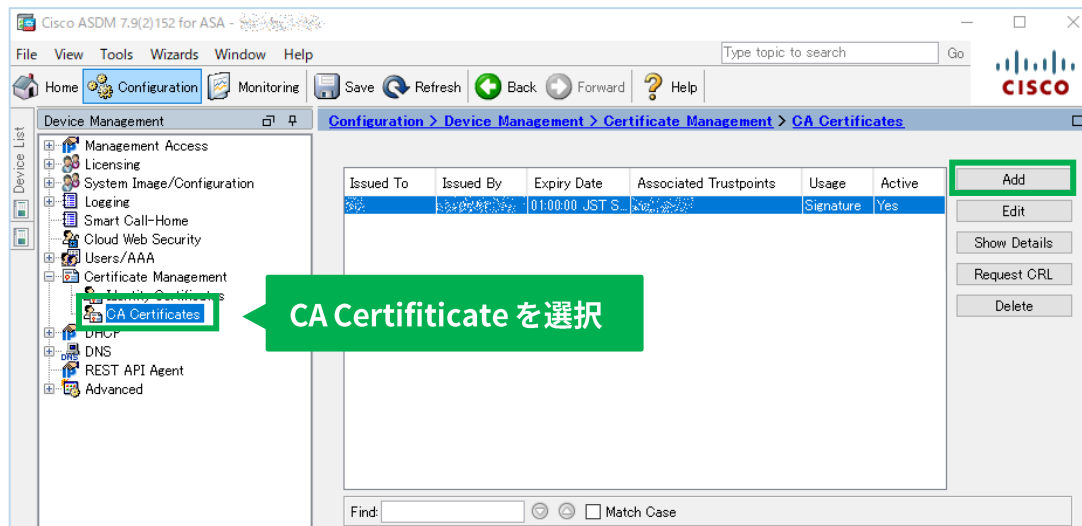
[証明書管理] - [CA情報]

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 type="radio"/> PEM形式 <input checked="" type="radio"/>

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





- 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

Consider certificate valid if revocation information cannot be retrieved

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:

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:

Enable HTTP

Enable Simple Certificate Enrollment Protocol (SCEP)

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 shows the 'AAA Server Groups' configuration table:

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

Green boxes highlight the 'Add' button in the top right and the 'Add' button in the bottom right of the 'Servers in the Selected Group' table.

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 and labeled '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), and Max Failed Attempts (3).

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 (実際は使用しません)
- ServerSecretKey : EPS-edgeのSecret
- MS Chapv2 : オフ

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		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow 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](#).

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)

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。

FortiGate VMX FortiGate-VMX

root

ダッシュボード

セキュリティファブリック

FortiView

ネットワーク

システム

ポリシー & オブジェクト

セキュリティプロファイル

VPN

オーバーレイコントロールVPN

IPsecトンネル

IPsecウィザード

IPsecトンネルテンプレート

SSL-VPNポータル

SSL-VPN設定

SSL-VPN設定

接続設定

リッスンするインターフェース

リッスンするポート

Webモードアクセスをリッスンするポート:
[https://\[ip\]:10443](https://[ip]: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 特定ホストへアクセス制限

アイドルログアウト

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

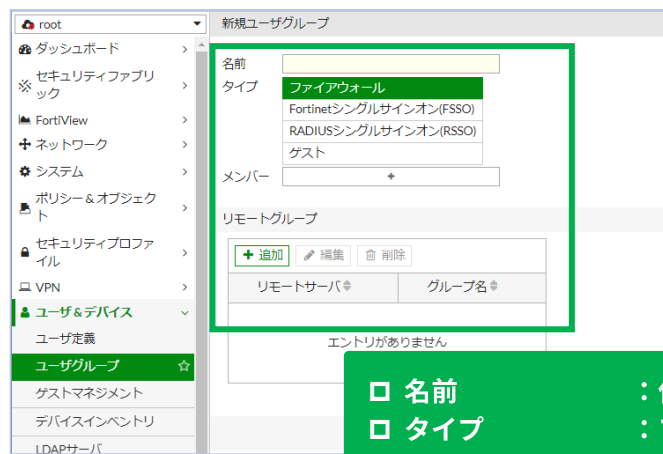
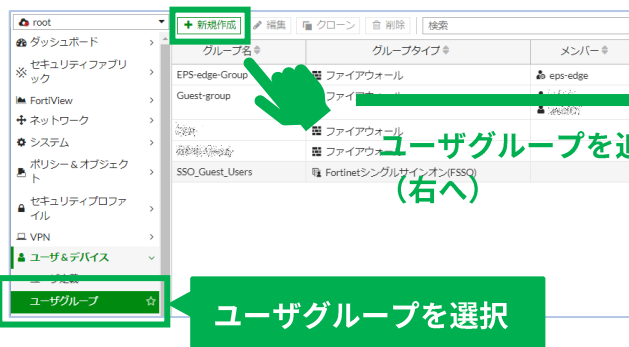
トンネルモードクライアント設定

アドレス範囲

自動的にアドレス割り当て カスタムIP範囲を指定

トンネルユーザは、以下の範囲内のIPを受け取ります: [ip]-[ip]

☑ クライアント証明書を要求 : オン



root

ダッシュボード

セキュリティファブリック

FortiView

ネットワーク

システム

ポリシー & オブジェクト

IPv4ポリシー ☆

認証ルール

アドレス

インターネットサービスデータベース

Edit Policy

名前

着信インターフェース SSL-VPNトンネルインターフェース

発信インターフェース mgmt

送信元 SSLVPN_TUNNEL_ADDR1
EPS-edge-Group

宛先 LAN

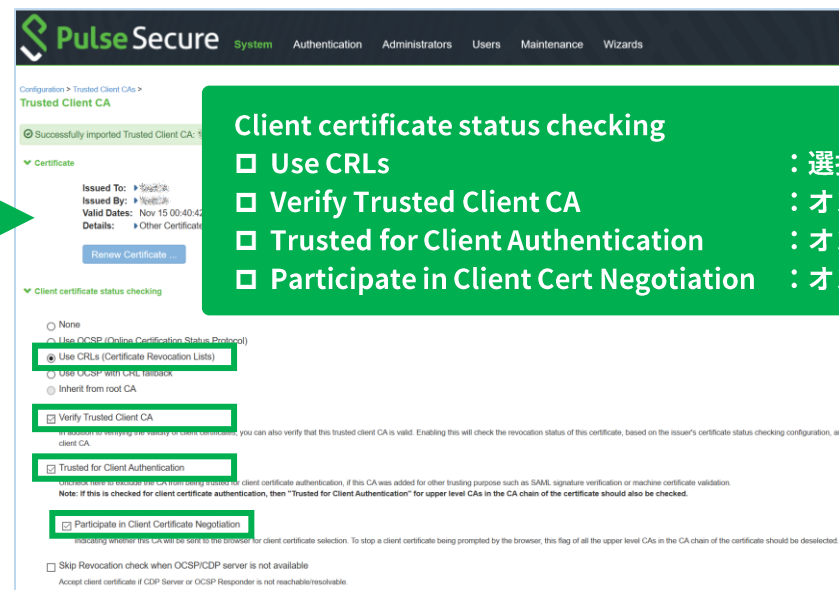
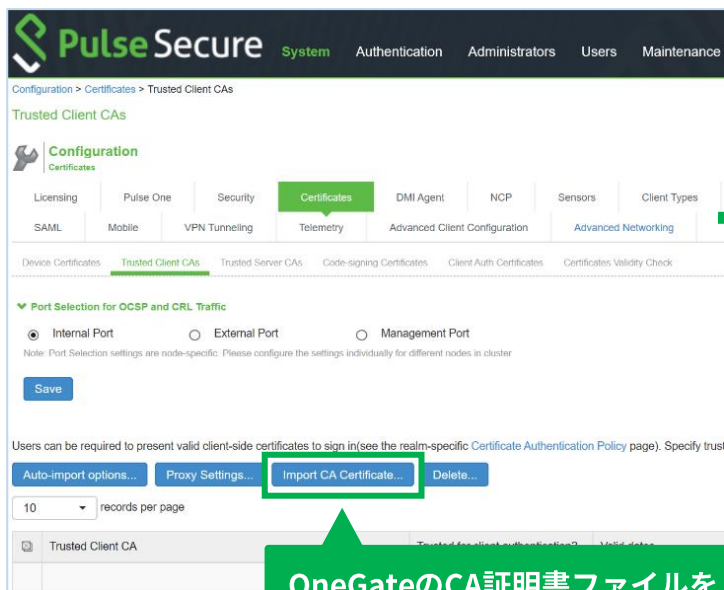
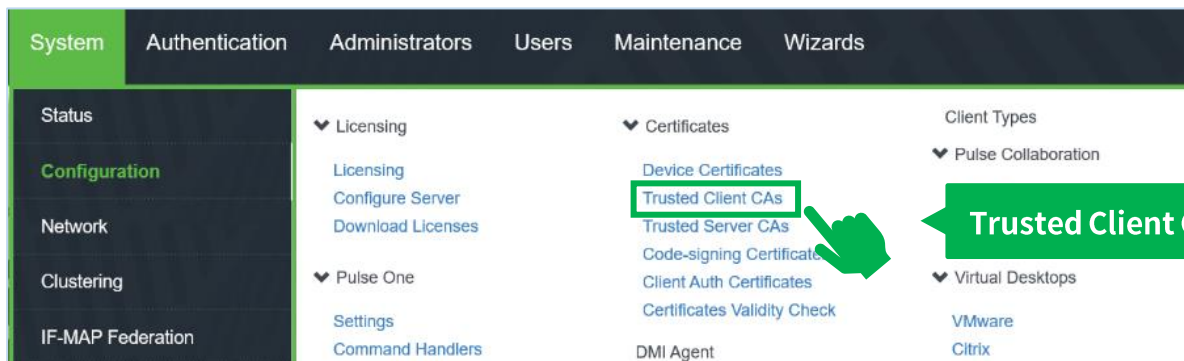
スケジュール always

サービス ALL

アクション ACCEPT DENY

インスペクションモード フローベース プロキシベース

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



CRL Checking Options

CRL Settings
Certificate revocation lists (CRL) are used to verify the ongoing validity of user certificates, and are obtained from a CRL distribution point (CDP).

	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
<input type="checkbox"/>	RADIUS Server
<input type="checkbox"/> System Local	Local Authentication

Certificate Serverを選択

Pulse Secure System Authentication Administrators

Auth Servers > naeps.example.com > Settings

Settings

Settings Users

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

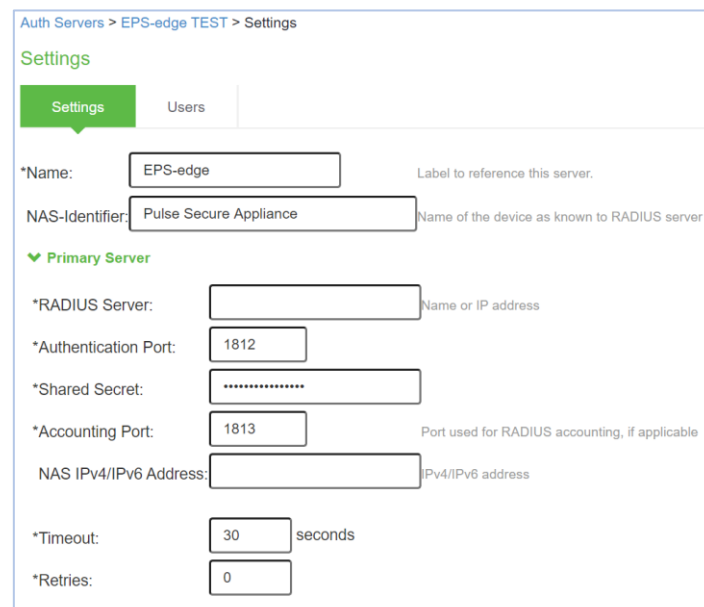
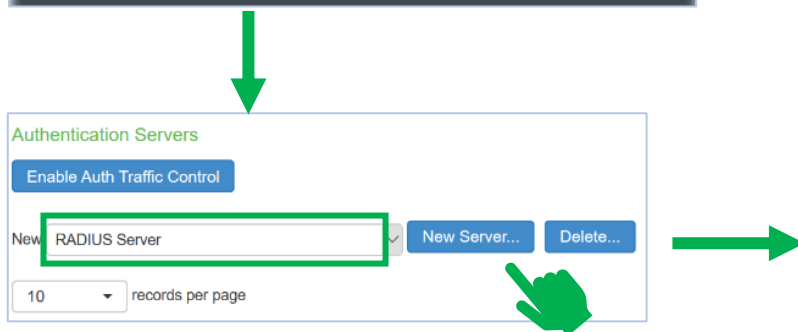
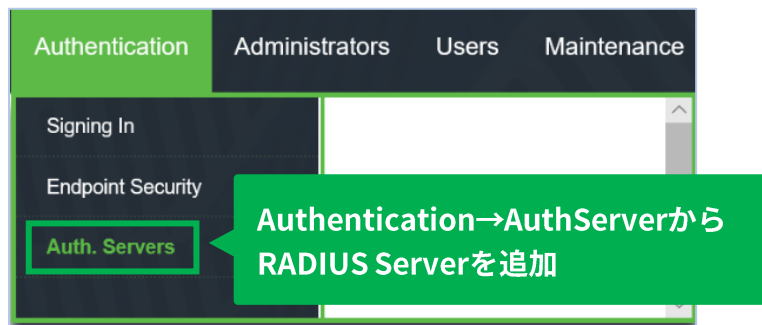
▼ User Record Synchronization

Enable User Record Synchronization

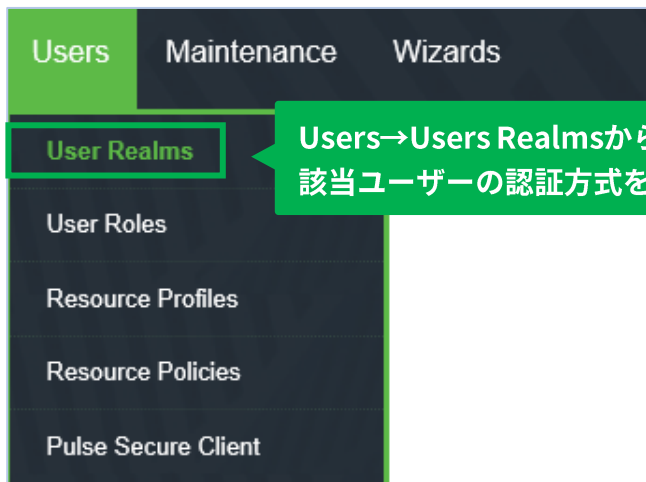
Logical Auth Server Name:

- Name : 任意のCertificate Server登録名





- 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



User Realms > VPNRealms > General

General

Authentication Policy

Role Mapping

* 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:

User Directory/Attribute: None

Accounting: None

Device Attributes: None

▼ Additional Authentication Server

Enable additional authentication server

You can specify an additional authentication server for s... they can be pre-defined below, in which case the user v...

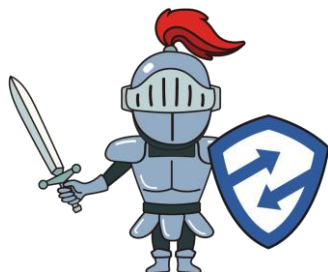
Enable adaptive authentication

Note: Adaptive authentication is supported by leveraging... 'Anonymous' type authentication server selected as au...

Authentication #2:

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



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

