

# FlexVPNによるISEポスチャの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[DNSサーバの設定](#)

[IOS XEの初期設定](#)

[ID証明書の設定](#)

[IKEv2 の設定](#)

[AnyConnect クライアント プロファイルの設定](#)

[ISE の設定](#)

[AdminおよびCPP証明書の設定](#)

[ISEでのローカルユーザの作成](#)

[FlexVPN HUBをRADIUSクライアントとして追加する](#)

[クライアント プロビジョニングの設定](#)

[ポスチャ ポリシーおよび条件](#)

[クライアント プロビジョニング ポータルの設定](#)

[認可プロファイルおよびポリシーの設定](#)

[確認](#)

[トラブルシューティング](#)

## 概要

このドキュメントでは、AnyConnect IKEv2およびEAP-Message Digest 5(EAP-MD5)認証方式を使用して、ポスチャを使用したリモートアクセス用のIOS XEヘッドエンドを設定する方法の例を示します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- IOS XEでのFlexVPNリモートアクセス(RA)VPNの設定
- AnyConnect(AC)クライアント設定
- Identity Service Engine(ISE)2.2以降のポスチャフロー
- ISE でのポスチャ コンポーネントの設定
- Windows Server 2008 R2でのDNSサーバの設定

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- IOS XE 16.8が稼働するCisco CSR1000V [Fuji]
- Windows 7 で動作する AnyConnect クライアント バージョン 4.5.03040
- Cisco ISE 2.3
- Windows 2008 R2サーバ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 背景説明

Cisco ISEを使用すると、課せられたネットワークセキュリティ対策が適切かつ効果的に維持されるように、保護されたネットワークにアクセスするクライアントマシンのセキュリティ機能を検証し、維持できます。Cisco ISE管理者は、最新のセキュリティ設定またはアプリケーションをクライアントマシンで使用できるように設計されたポスチャポリシーを使用することで、ネットワークにアクセスするすべてのクライアントマシンが、定義されたエンタープライズネットワークアクセスのセキュリティ標準を満たすことができます。ポスチャコンプライアンスレポートは、Cisco ISEに、ユーザログイン時のクライアントマシンのコンプライアンスレベルのスナップショットと、定期的な再評価が行われるたびに提供します。

ポスチャは、次の3つの主要な要素で表すことができます。

1. ポリシー構成の配布および決定ポイントとしてのISE。管理者の観点から、ポスチャポリシー（デバイスを企業に準拠させるために満たす正確な条件）、クライアントプロビジョニングポリシー（どの種類のデバイスにインストールする必要があるか）、許可ポリシー（権限の種類はポスチャの状態によって異なります）。
2. ポリシー適用ポイントとしてのネットワークアクセスデバイス(NAD)。NAD側では、実際の認証制限は、ユーザ認証時に適用されます。ポリシーポイントとしてのISEは、アクセスコントロールリスト(ACL)などの認証パラメータを提供します。従来、ポスチャを発生させるには、エンドポイントのポスチャステータスが決定された後でユーザを再認証する認可変更 (CoA)をサポートする必要があります。  
注：IOS XEを実行しているルータは、リダイレクションをサポートしていません。注：IOS XEソフトウェアには、ISEが完全に動作するCoAを次の不具合に対する修正が必要です。  
[CSCve16269](#) IKEv2 CoAがISEで動作しない  
[CSCvi90729](#) IKEv2 CoAがISEで動作しない ( trueではなくcoa-push=TRUE )
3. データ収集およびエンド ユーザとのインタラクションのポイントとしてのエージェント ソフトウェア。エージェントは ISE からポスチャ要件に関する情報を受け取り、要件のステータスに関するレポートを ISE に提供します。このドキュメントは、リダイレクトなしで完全にポスチャをサポートする唯一のAnyconnect ISEポスチャモジュールに基づいています。

リダイレクションのないポスチャフローは、記事「[ISE Posture Style Comparison for Pre and Post 2.2](#)」、「Posture flow in ISE 2.2」で詳しく説明されています。

FlexVPNによるAnyconnect ISEポスチャモジュールのプロビジョニングは、次の2つの方法で行えます。

- 手動：モジュールは、Ciscoソフトウェアダウンロードポータルで入手できるAnyconnectパッケージから、クライアントのワークステーションに手動でインストールされます。

<https://software.cisco.com/download/home/283000185> にアクセスしてください。

ISEポスチャモジュールの手動プロビジョニングを使用したポスチャ作業では、次の条件を満たす必要があります。

1. ドメインネームサーバ(DNS)は、完全修飾ドメイン名(FQDN) **enroll.cisco.com**をポリシーサービスノード(PSN)IPに解決する必要があります。最初の接続試行時に、ポスチャモジュールには使用可能なPSNに関する情報がありません。使用可能なPSNを見つけるためにディスカバリプローブを送信しています。FQDN enroll.cisco.comは、次のいずれかのプローブで使用されます。

2. PSN IPに対してTCPポート**8905**を許可する必要があります。このシナリオでは、ポスチャはTCPポート8905を経由しています。

3. PSNノードの**管理証明書**は、[SAN]フィールドに**enroll.cisco.com**が必要です。VPNユーザとPSNノード間のTCP 8905経由の接続は管理証明書によって保護され、PSNノードの管理証明書にそのような名前「enroll.cisco.com」がない場合、ユーザには証明書の警告が表示されます。

注：[RFC6125](#)に従って、[SAN値が指定](#)されている場合は、CNを無視する必要があります。つまり、SANフィールドに管理証明書のCNを追加する必要があります。

- Automatic provisioning via Client Provisioning Portal(CPP)：このモジュールは、ポータルのFQDNを介して直接CPPにアクセスすることにより、ISEからダウンロードおよびインストールされます。

ISEポスチャモジュールの自動プロビジョニングを使用したポスチャ作業では、次の条件を満たす必要があります。

1. DNSはCPPのFQDNをポリシーサービスノード(PSN)のIPに解決する必要があります。

2. PSN IPには、TCPポート**80**、**443**および**CPPポート**（デフォルトでは**8443**）を許可する必要があります。クライアントはHTTP（HTTPSにリダイレクトされる）またはHTTPSを介してCPP FQDNを直接開く必要があります。この要求はCPPのポート（デフォルトでは8443）にリダイレクトされ、ポスチャはそのポートを経由します。

3. PSNノードの**Admin証明書**と**CPP証明書**は、SANフィールドに**CPP FQDN**を持つ必要があります。TCP 443を介したVPNユーザとPSNノード間の接続は管理証明書によって保護され、CPPポートでの接続はCPP証明書によって保護されます。

注：[RFC6125](#)に従って、[SAN値が指定](#)されている場合は、CNを無視する必要があります。つまり、対応する証明書のSANフィールドにAdmin証明書とCPP証明書のCNを追加する必要があります。

注：ISEソフトウェアに[CSCvj76466の修正が含まれていない場合](#)、ポスチャまたはクライアントプロビジョニングは、クライアントが認証された同じPSNでポスチャまたはクライアントプロビジョニングが実行された場合にのみ機能します。

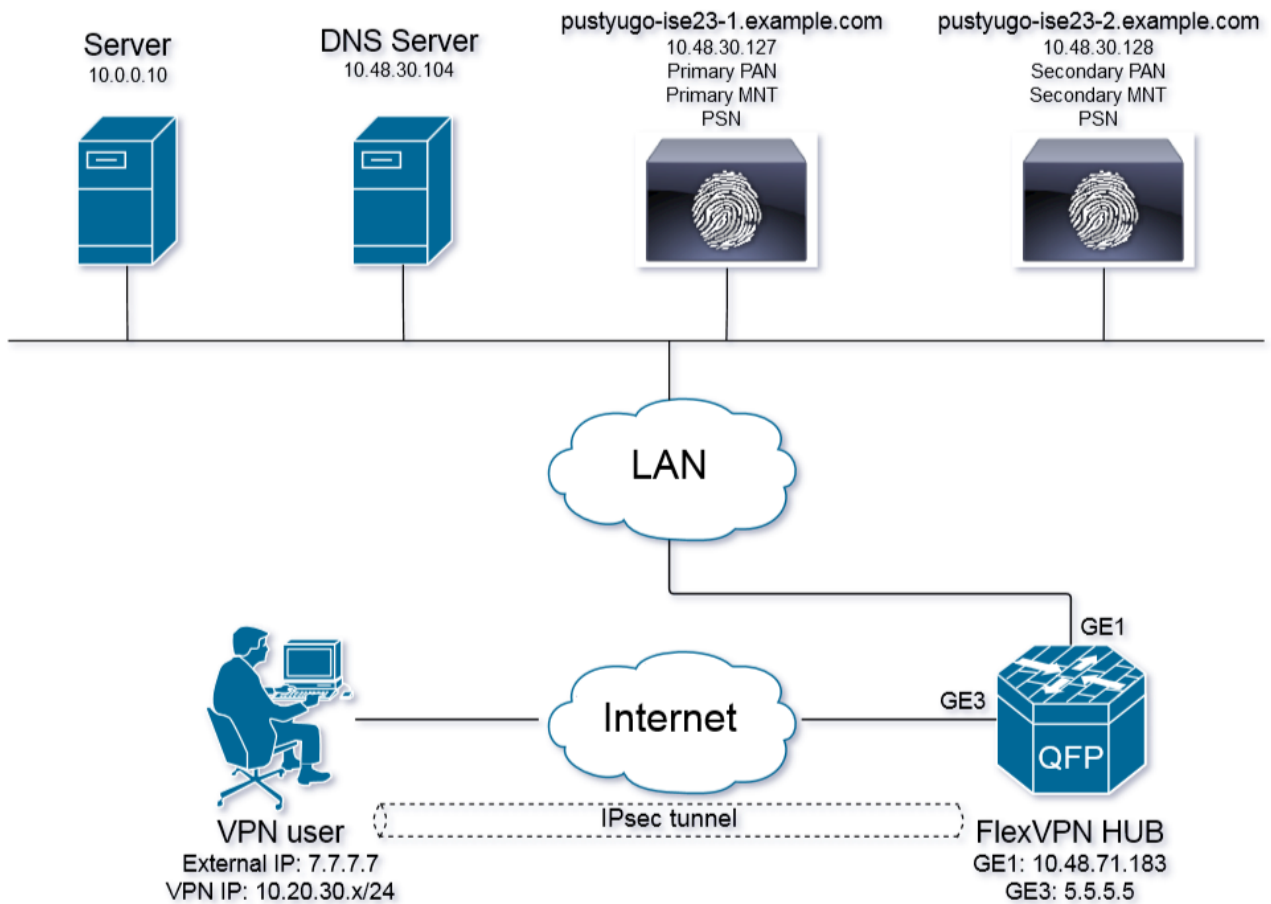
FlexVPNを使用したポスチャの場合、フローには次の手順が含まれます。

1. ユーザはAnyconnectクライアントを使用してFlexVPNハブに接続します。
2. ISEは、アクセスを制限するためにACL名を使用してAccess-AcceptをFlexVPNハブに適用する必要があります。
- 3a. 手動プロビジョニングによる最初の接続：ISEポスチャモジュールは、TCPポート8905を介してenroll.cisco.comにプローブを送信するポリシーサーバの検出を開始します。正常に完了すると、ポスチャモジュールは設定済みのポスチャプロファイルをダウンロードし、クライアント側のコンプライアンスモジュールを更新します。  
  
次の接続試行時に、ISEポスチャモジュールは、ポリシーサーバの検出にポスチャプロファイルのCall Homeリストで指定された名前とIPも使用します。
- 3b. 自動プロビジョニングによる最初の接続：クライアントはFQDNを介してCPPを開きます。その結果、Network Setup Assistantがクライアントのワークステーションにダウンロードされ、ISEポスチャモジュール、ISEコンプライアンスモジュール、およびポスチャプロファイルがダウンロードされてインストールされます。  
  
次の接続試行時に、ISEポスチャモジュールは、ポリシーサーバの検出にポスチャプロファイルのCall Homeリストで指定された名前とIPを使用します。
4. ポスチャモジュールはコンプライアンスのチェックを開始し、チェックの結果をISEに送信します。
5. クライアントのステータスがCompliantの場合、ISEはAccess-AcceptをFlexVPNハブに送信します。ACLの名前は、準拠クライアントに適用する必要があります。
6. クライアントはネットワークにアクセスします。

ポスチャプロセスの詳細については、ドキュメント『[ISE Posture Style Comparison for Pre and Post 2.2](#)』を参照してください。

## 設定

### ネットワーク図



VPNユーザは、準拠ステータスの場合にのみサーバ(10.0.0.10)にアクセスできます。

## DNSサーバの設定

このドキュメントでは、Windows Server 2008 R2がDNSサーバとして使用されます。

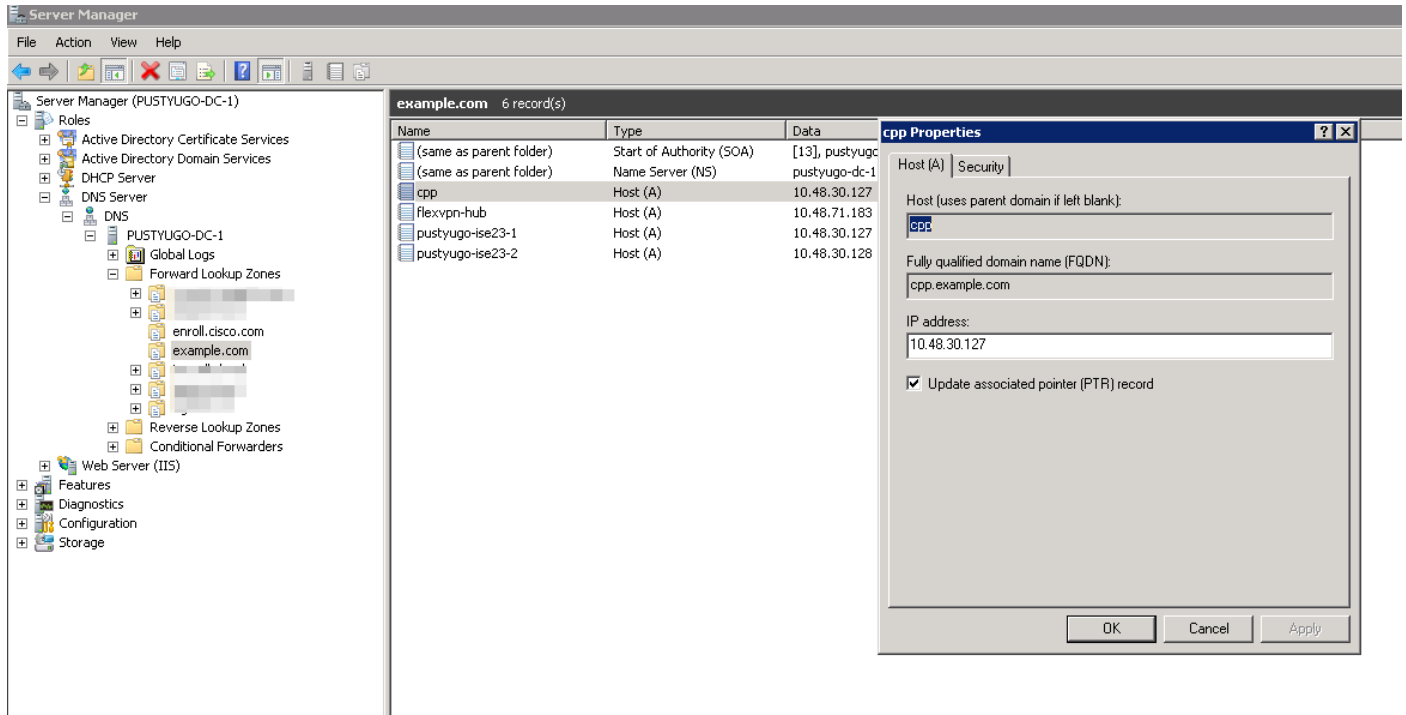
ステップ1:PSNのIPを指定するenroll.cisco.comのホスト(A)レコードを追加します。

The screenshot shows the Windows Server Manager interface. The left pane displays the server configuration tree, including the DNS Server role and the Forward Lookup Zones for PUSTYUGO-DC-1. The right pane shows the DNS records for enroll.cisco.com. The 'enroll.cisco.com Properties' dialog box is open, showing the Host (A) record configuration. The dialog box has the following fields:

- Host (A): [same as parent folder]
- Fully qualified domain name (FQDN): enroll.cisco.com
- IP address: 10.48.30.127
- Update associated pointer (PTR) record

The dialog box has OK, Cancel, and Apply buttons at the bottom.

ステップ2:PSNのIPを指定するCPP FQDN(この例で使用するcpp.example.com)のホスト(A)レコードを追加します。



## IOS XEの初期設定

### ID証明書の設定

ルータは、Anyconnectクライアントに対して自身を認証するために証明書を使用します。接続の確立フェーズで証明書の警告を回避するには、ルータ証明書をユーザのオペレーティングシステムで信頼する必要があります。

ID証明書は、次のいずれかの方法で提供できます。

注：自己署名証明書の使用は、IKEv2 FlexVPNではサポートされません。

#### オプション1：ルータで証明機関(CA)サーバを設定する

注：CAサーバは、同じIOSルータまたは別のルータに作成できます。この記事では、CAは同じルータで作成されます。

注：CAサーバを有効にするには、NTPサーバと時刻を同期する必要があります。

注：ユーザはこの証明書の信頼性を確認できないため、接続を確立する前にCA証明書を手動で確認してユーザのマシンにインポートしない限り、ユーザデータは中間者攻撃から保護されません。

ステップ1:CAサーバのRSAキーを生成します。

```
FlexVPN-HUB(config)# crypto key generate rsa label ROOT-CA modulus 2048
```

ステップ2:ID証明書のRSAキーを生成します。

```
FlexVPN-HUB(config)# crypto key generate rsa label FLEX-1 modulus 2048
```

検証:

```
FlexVPN-HUB# show crypto key mypubkey rsa
```

```
---- output truncated ----
```

```
Key name: ROOT-CA
```

```
Key type: RSA KEYS
```

```
Storage Device: private-config
```

```
Usage: General Purpose Key
```

```
Key is not exportable. Redundancy enabled.
```

```
Key Data:
```

```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
```

```
00C01F04 E0AF3AB8 97CED516 3B31152A 5C3678A0 829A0D0D 2F46D86C 2CBC9175
```

```
----- output truncated ----- ----- output truncated ----- Key name: FLEX-1
```

```
Key type: RSA KEYS
```

```
Storage Device: private-config
```

```
Usage: General Purpose Key
```

```
Key is not exportable. Redundancy enabled.
```

```
Key Data:
```

```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
```

```
009091AE 4185DC96 4F561F7E 506D56E8 240606D0 CC16CC5E E4E24EEB 1664E42C ----- output truncated
```

ステップ3:CAを設定します。

```
ip http server
```

```
crypto pki server ROOT-CA
```

```
issuer-name cn=ROOT-CA.example.com
```

```
hash sha256
```

```
lifetime certificate 1095
```

```
lifetime ca-certificate 3650
```

```
eku server-auth
```

```
no shutdown
```

検証:

```
FlexVPN-HUB# show crypto pki server
```

```
Certificate Server ROOT-CA:
```

```
Status: enabled
```

```
State: enabled
```

```
Server's configuration is locked (enter "shut" to unlock it)
```

```
Issuer name: cn=ROOT-CA.example.com
```

```
CA cert fingerprint: A5522AAB 1410E645 667F0D70 49AADA45
```

```
Granting mode is: auto
```

```
Last certificate issued serial number (hex): 3
```

```
CA certificate expiration timer: 18:12:07 UTC Mar 26 2021
```

```
CRL NextUpdate timer: 21:52:55 UTC May 21 2018
```

```
Current primary storage dir: nvram:
```

```
Database Level: Minimum - no cert data written to storage
```

ステップ4:トラストポイントを設定します。

```
interface loopback 0
ip address 10.10.10.10 255.255.255.255
crypto pki trustpoint FLEX-TP-1
  enrollment url http://10.10.10.10:80
  fqdn none
  subject-name cn=flexvpn-hub.example.com
  revocation-check none
  rsakeypair FLEX-1
```

## ステップ5:CAを認証します。

```
FlexVPN-HUB(config)#crypto pki authenticate FLEX-TP-1
Certificate has the following attributes:
  Fingerprint MD5: A5522AAB 1410E645 667F0D70 49AADA45
  Fingerprint SHA1: F52EAB1A D39642E7 D8EAB804 0EB30973 7647A860
```

```
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

## ステップ6 : ルータをCAに登録します。

```
FlexVPN-HUB(config)#crypto pki enroll FLEX-TP-1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: cn=flexvpn-hub.example.com
% The fully-qualified domain name will not be included in the certificate
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose FLEX-TP-1' command will show the fingerprint.

May 21 16:16:55.922: CRYPTO_PKI: Certificate Request Fingerprint MD5: 80B1FAFD 35346D0F
D23F6648 F83F039B
May 21 16:16:55.924: CRYPTO_PKI: Certificate Request Fingerprint SHA1: A8401EDE 35EE4AF8
46C4D619 8D653BFD 079C44F7
```

## CAで保留中の証明書要求を確認し、フィンガープリントが一致することを確認します。

```
FlexVPN-HUB#show crypto pki server ROOT-CA requests
Enrollment Request Database:

Subordinate CA certificate requests:
ReqID State Fingerprint SubjectName
-----
RA certificate requests:
ReqID State Fingerprint SubjectName
-----

Router certificates requests:
ReqID State Fingerprint SubjectName
```



```
-----  
1      pending      80B1FAFD35346D0FD23F6648F83F039B cn=flexvpn-hub.example.com
```

ステップ7：適切なReqIDを使用して証明書を許可します。

```
FlexVPN-HUB#crypto pki server ROOT-CA grant 1
```

ルータが証明書を再度要求するまで待ちます（この設定によると、1分間に10回チェックされま  
す）。syslogメッセージを探します。

```
May 21 16:18:56.375: %PKI-6-CERTRET: Certificate received from Certificate Authority  
証明書がインストールされていることを確認します。
```

```
FlexVPN-HUB#show crypto pki certificates FLEX-TP-1
```

```
Certificate  
Status: Available  
Certificate Serial Number (hex): 04  
Certificate Usage: General Purpose  
Issuer:  
  cn=ROOT-CA.example.com  
Subject:  
  Name: flexvpn-hub.example.com  
  cn=flexvpn-hub.example.com  
Validity Date:  
  start date: 16:18:16 UTC May 21 2018  
  end   date: 18:12:07 UTC Mar 26 2021  
Associated Trustpoints: FLEX-TP-1
```

```
CA Certificate
```

```
Status: Available  
Certificate Serial Number (hex): 01  
Certificate Usage: Signature  
Issuer:  
  cn=ROOT-CA.example.com  
Subject:  
  cn=ROOT-CA.example.com  
Validity Date:  
  start date: 18:12:07 UTC Mar 27 2018  
  end   date: 18:12:07 UTC Mar 26 2021  
Associated Trustpoints: FLEX-TP-1 ROOT-CA  
Storage: nvram:ROOT-CAexamp#1CA.cer
```

## オプション2 – 外部署名証明書のインポート

```
FlexVPN-HUB(config)# crypto pki import FLEX-TP-2 pkcs12 ftp://cisco:cisco@10.48.30.130/ password  
cisco123  
% Importing pkcs12...  
Address or name of remote host [10.48.30.130]?  
Source filename [FLEX-TP-2]? flexvpn-hub.example.com.p12  
Reading file from ftp://cisco@10.48.30.130/flexvpn-hub.example.com.p12!  
[OK - 4416/4096 bytes]  
% The CA cert is not self-signed.  
% Do you also want to create trustpoints for CAs higher in  
% the hierarchy? [yes/no]:  
May 21 16:55:26.344: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named FLEX-TP-2 has been generated or  
imported  
yes
```

```
CRYPTO_PKI: Imported PKCS12 file successfully.
FlexVPN-HUB(config)#
May 21 16:55:34.396: %PKI-6-PKCS12IMPORT_SUCCESS: PKCS #12 Successfully Imported.
FlexVPN-HUB(config)#
```

## IKEv2 の設定

ステップ1:RADIUSサーバとCoAを設定します。

```
aaa group server radius FlexVPN-AuthC-Server-Group-1
  server-private 10.48.30.127 key Cisco123
server-private 10.48.30.128 key Cisco123
```

```
aaa server radius dynamic-author
  client 10.48.30.127 server-key Cisco123
client 10.48.30.128 server-key Cisco123
  server-key Cisco123
  auth-type any
```

ステップ2 : 認証および許可リストを設定します。

```
aaa new-model
aaa authentication login FlexVPN-AuthC-List-1 group FlexVPN-AuthC-Server-Group-1
aaa authorization network FlexVPN-AuthZ-List-1 local
aaa accounting update newinfo
aaa accounting network FlexVPN-Accounting-List-1 start-stop group FlexVPN-AuthC-Server-Group-1
```

ステップ3:ikev2認可ポリシーを作成します。

```
crypto ikev2 authorization policy FlexVPN-Local-Policy-1
  pool FlexVPN-Pool-1
  dns 10.48.30.104
  netmask 255.255.255.0
  def-domain example.com
```

ステップ4:IKEv2プロファイルを作成します。

```
crypto ikev2 profile FlexVPN-IKEv2-Profile-1
  match identity remote key-id example.com
  identity local dn
  authentication local rsa-sig
  authentication remote eap query-identity
  pki trustpoint FLEX-TP-2
  dpd 60 2 on-demand
  aaa authentication eap FlexVPN-AuthC-List-1
  aaa authorization group eap list FlexVPN-AuthZ-List-1 FlexVPN-Local-Policy-1
  aaa authorization user eap cached
  aaa accounting eap FlexVPN-Accounting-List-1
  virtual-template 10
```

ステップ5 : トランスフォームセットとipsecプロファイルを作成します。

```
crypto ipsec transform-set FlexVPN-TS-1 esp-aes esp-sha-hmac
  mode tunnel
crypto ipsec profile FlexVPN-IPsec-Profile-1
  set transform-set FlexVPN-TS-1
  set ikev2-profile FlexVPN-IKEv2-Profile-1
```

ステップ6：仮想テンプレートインターフェイスを作成します。

```
interface Virtual-Template10 type tunnel
 ip unnumbered GigabitEthernet3
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
```

ステップ7：ローカルプールの作成：

```
ip local pool FlexVPN-Pool-1 10.20.30.100 10.20.30.200
```

ステップ8：非準拠クライアントのアクセスを制限するACLを作成します。未知のポスチャの状態のときには、少なくとも次の権限を指定する必要があります。

- DNS トラフィック
- ポート80、443、および8905を介したISE PSNへのトラフィック
- CPP ポータルの FQDN が指す ISE PSN へのトラフィック
- 必要な場合、修復サーバへのトラフィック

次に、修復サーバのないACLの例を示します。10.0.0.0/24ネットワークの明示的な拒否が可視性のために追加され、暗黙の「deny ip any any」がACLの最後に存在します。

```
ip access-list extended DENY_SERVER
 permit udp any any eq domain
 permit tcp any host 10.48.30.127 eq 80
 permit tcp any host 10.48.30.127 eq 443
 permit tcp any host 10.48.30.127 eq 8443
 permit tcp any host 10.48.30.127 eq 8905
 permit tcp any host 10.48.30.128 eq 80
 permit tcp any host 10.48.30.128 eq 443
 permit tcp any host 10.48.30.128 eq 8443
 permit tcp any host 10.48.30.128 eq 8905
 deny ip any 10.0.0.0 0.0.0.255
```

ステップ9：準拠クライアントへのアクセスを許可するACLを作成します。

```
ip access-list extended PERMIT_ALL
 permit ip any any
```

ステップ10：スプリットトンネルの設定 ( オプション )

デフォルトでは、すべてのトラフィックはVPN経由で転送されます。トラフィックを指定されたネットワークだけにトンネリングするには、「ikev2 authorization policy」セクションでトラフィックを指定できます。複数のステートメントを追加したり、標準アクセスリストを使用したりできます。

```
crypto ikev2 authorization policy FlexVPN-Local-Policy-1
 route set remote ipv4 10.0.0.0 255.0.0.0
```

ステップ11：リモートクライアントのインターネットアクセス ( オプション )

リモートアクセスクライアントからインターネット内のホストへのアウトバウンド接続を、ルータのグローバルIPアドレスにNAT変換するには、NAT変換を設定します。

```
ip access-list extended NAT
```

```
permit ip 10.20.30.0 0.0.0.255 any
```

```
ip nat inside source list NAT interface GigabitEthernet1 overload extended
```

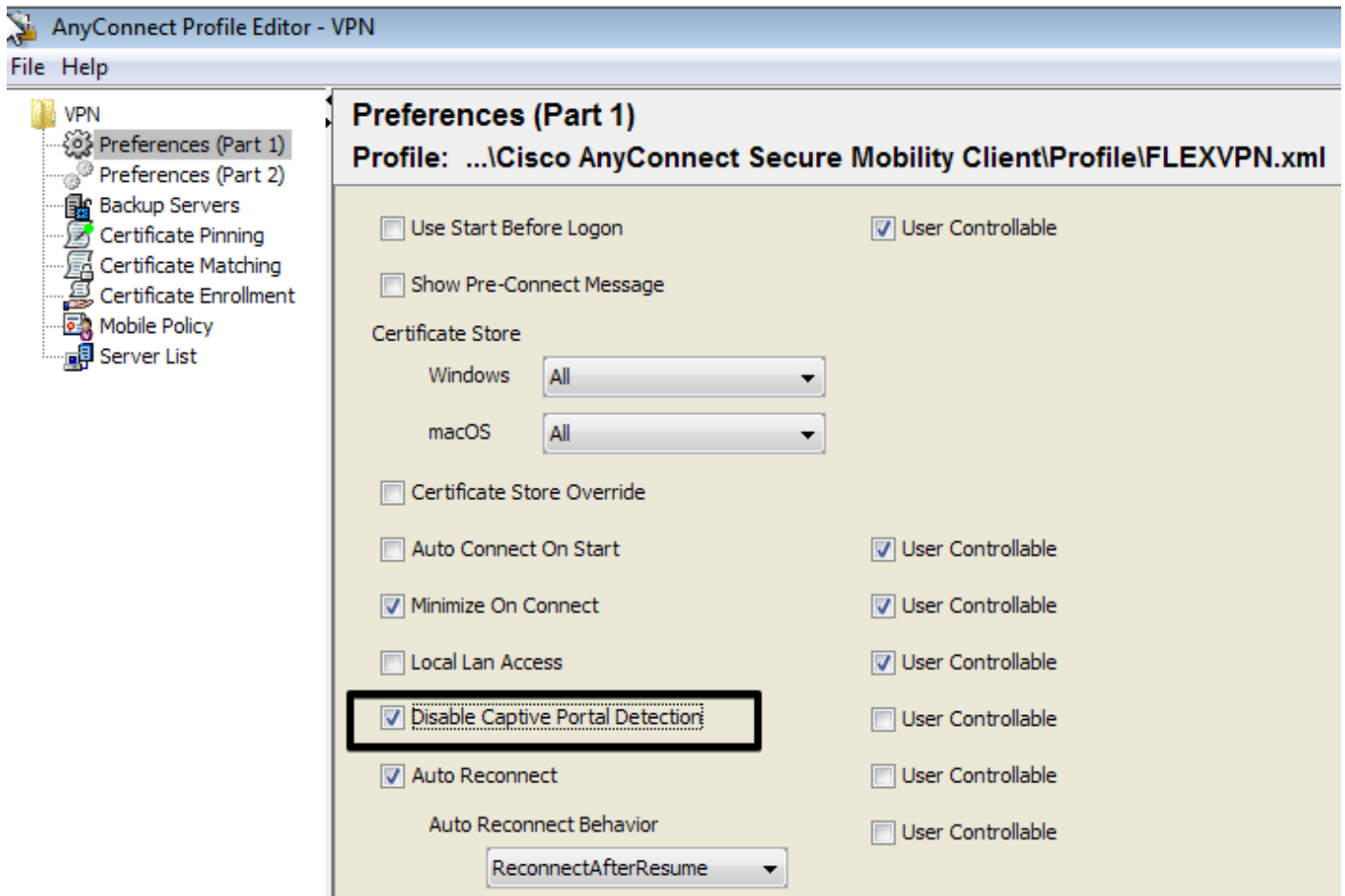
```
interface GigabitEthernet1  
ip nat outside
```

```
interface Virtual-Template 10  
ip nat inside
```

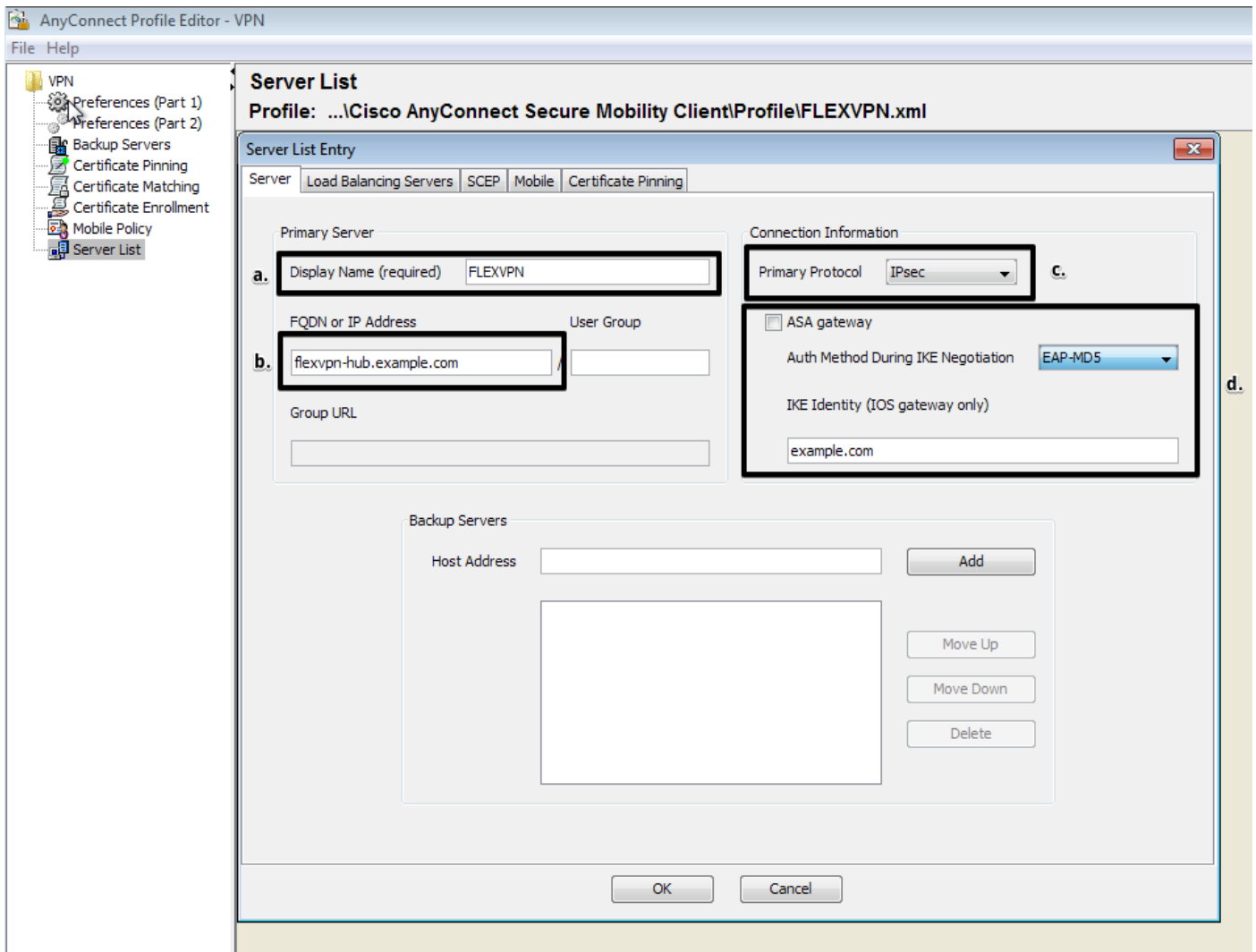
## AnyConnect クライアント プロファイルの設定

AnyConnectプロファイルエディタを使用してクライアントプロファイルを設定します。Windows 7および10上のAnyconnect Security Mobile Clientのプロファイルは、  
%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profileに保存されています。

ステップ1：キャプティブポータル検出機能を無効にします。FlexVPNハブでhttpサーバが無効になっていない場合、AnyConnectキャプティブポータル検出機能によって接続が失敗します。CAサーバはHTTPサーバがないと動作しないことに注意してください。



ステップ2：サーバリストの設定：



- 表示名を入力します。
- FlexVPNハブのFQDNまたはIPアドレスを入力してください。
- [プライマリプロトコル]として[IPsec]を選択します。
- [ASA gateway]チェックボックスをオフにし、[Auth Method]に[EAP-MD5]を指定します。  
FlexVPNハブのIKEv2プロファイル設定とまったく同じIKE Identityを入力します(この例では、IKEv2プロファイルは「match identity remote key-id example.com」コマンドで設定されているため、example.comをIKE Identityとして使用する必要があります)。

ステップ3 : プロファイルを%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profileに保存し、ACを再起動します。

このプロファイルに相当する XML :

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
  <ClientInitialization>
    <UseStartBeforeLogon UserControllable="true">>false</UseStartBeforeLogon>
    <AutomaticCertSelection UserControllable="true">>true</AutomaticCertSelection>
    <ShowPreConnectMessage>>false</ShowPreConnectMessage>
    <CertificateStore>All</CertificateStore>
    <CertificateStoreMac>All</CertificateStoreMac>
  </ClientInitialization>
</AnyConnectProfile>
```

```

<CertificateStoreOverride>>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>>false</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">>false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">>true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">>false</LocalLanAccess>
<DisableCaptivePortalDetection
UserControllable="false">>true</DisableCaptivePortalDetection>
<ClearSmartcardPin UserControllable="true">>false</ClearSmartcardPin>
<IPProtocolSupport>IPv4, IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">>true
  <AutoReconnectBehavior
UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">>true</AutoUpdate>
<RSA SecurID Integration UserControllable="false">Automatic</RSA SecurID Integration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVpNEstablishment>LocalUsersOnly</WindowsVpNEstablishment>
<AutomaticVPNPolicy>>false</AutomaticVPNPolicy>
<PPPEExclusion UserControllable="false">Automatic
  <PPPEExclusionServerIP UserControllable="false"></PPPEExclusionServerIP>
</PPPEExclusion>
<EnableScripting UserControllable="false">>false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="true">>false
  <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
  <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>>false
</RetainVpnOnLogoff>
<AllowManualHostInput>>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
  <HostEntry>
    <HostName>FLEXVPN</HostName>
    <HostAddress>flexvpn-hub.example.com</HostAddress>
    <PrimaryProtocol>IPsec
      <StandardAuthenticationOnly>>true
        <AuthMethodDuringIKENegotiation>EAP-MD5</AuthMethodDuringIKENegotiation>
        <IKEIdentity>example.com</IKEIdentity>
      </StandardAuthenticationOnly>
    </PrimaryProtocol>
  </HostEntry>
</ServerList>
</AnyConnectProfile>

```

## ISE の設定

### AdminおよびCPP証明書の設定

注：管理証明書を変更すると、証明書が変更されたノードが再起動します。

ステップ1:[Administration] -> [System] -> [Certificates] -> [Certificate Signing Requests]に移動し、[Generate Certificate Signing Requests (CSR)]をクリックします。

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

**Certificate Management**

- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Setti...

**Certificate Authority**

### Certificate Signing Requests

[Generate Certificate Signing Requests \(CSR\)](#)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

View Export Delete Bind Certificate

<input type="checkbox"/>	Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp
No data available					

ステップ2：開いたページで必要なPSNノードを選択し、必要なフィールドに入力し、ノードのFQDN、enroll.cisco.com、cpp.example.com、およびSANフィールドにノードのIPアドレスを追加し、[Generate]をクリックします。

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

**Certificate Management**

- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Setti...

**Certificate Authority**

### Usage

Certificate(s) will be used for  ⚠ You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).

Allow Wildcard Certificates  ⓘ

### Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> pustyugo-ise23-1	pustyugo-ise23-1#Multi-Use
<input type="checkbox"/> pustyugo-ise23-2	pustyugo-ise23-2#Multi-Use

### Subject

Common Name (CN)  ⓘ

Organizational Unit (OU)  ⓘ

Organization (O)  ⓘ

City (L)

State (ST)

Country (C)

Subject Alternative Name (SAN)

DNS Name	pustyugo-ise23-1.example.com	-	+
DNS Name	enroll.cisco.com	-	+
DNS Name	cpp.example.com	-	+
IP Address	10.48.30.127	-	+

\* Key type  ⓘ

\* Key Length  ⓘ

\* Digest to Sign With

Certificate Policies

注：このステップで[Multi-Use]を選択すると、ポータルにも同じ証明書を使用できます。

表示されたウィンドウでExportをクリックし、CSRをpem形式でローカルワークステーションに保存します。



Successfully generated CSR(s)

Certificate Signing request(s) generated:

pustyugo-ise23-1#Multi-Use

Click Export to download CSR(s) or OK to return to list of CSR(s) screen

ステップ3：信頼できるCAを使用してCSRを実行し、CAから証明書ファイルとCA証明書の完全なチェーン（ルートおよび中間）を取得します。

ステップ4:[Administration] -> [System] -> [Certificates] -> [Trusted Certificates]に移動し、[Import]をクリックします。次の画面で、[Choose file]をクリックして[Root CA certificate file]を選択して、必要に応じて[Friendly name]と[Description]に入力し、必要な[Trusted For options]を選択して[Submit]:



チェーン内のすべての中間証明書がある場合は、この手順を繰り返します。

ステップ5:[Administration] -> [System] -> [Certificates] -> [Certificate Signing Requests]に戻り、必要なCSRを選択し、[Bind Certificate]をクリックします。

Friendly Name
 Certificate Subject | Key Length | Portal group tag | Timestamp | Host | pustyugo-ise23-1#Multi-Use | CN=pustyugo-ise23-1.... | 2048 | Sun, 10 Jun 2018 | pustyugo-ise |

 The 'Friendly Name' column has a checkbox in the first row and a checked checkbox in the second row."/>

ステップ6：開いたページで、[Choose File]をクリックし、CAから受け取った証明書ファイルを選択し、必要に応じて[Friendly Name]を入力して、[Usage:管理(使用：CSRがMulti-Useで作成されている場合は、ここでポータルを選択し、[Submit]をクリックできます。

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

**Certificate Management**

- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Setti...

**Certificate Authority**

### Bind CA Signed Certificate

\* Certificate File  Signed CSR.cer

Friendly Name  ⓘ

Validate Certificate Extensions  ⓘ

**Usage**

- Admin: Use certificate to authenticate the ISE Admin Portal
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- RADIUS DTLS: Use certificate for the RADSec server
- pxGrid: Use certificate for the pxGrid Controller
- Portal: Use for portal

ステップ7：警告ポップアップで、[はい]をクリックしてインポートを終了します。管理証明書の変更の影響を受けるノードが再起動します。

Enabling Admin role for this certificate will cause an application server restart on the selected node.

Note: Make sure required Certificate Chain is imported under Trusted Certificates

ポータルに別の証明書を使用する場合は、CPP証明書を変更する手順を繰り返します。ステップ6で、[Usage]を選択します。ポータルで[Submit]をクリックします。

**Bind CA Signed Certificate**

\* Certificate File  Signed CSR Portal.cer

Friendly Name  ⓘ

Validate Certificate Extensions  ⓘ

**Usage**

- Admin: Use certificate to authenticate the ISE Admin Portal
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- RADIUS DTLS: Use certificate for the RADSec server
- pxGrid: Use certificate for the pxGrid Controller
- Portal: Use for portal

\* Portal group tag  ⓘ

Portal(s) using this tag

BYOD Portal (default)	Blacklist Portal (default)
Certificate Provisioning Portal (default)	Client Provisioning Portal (default)
Hotspot Guest Portal (default)	MDM Portal (default)
My Devices Portal (default)	Self-Registered Guest Portal (default)
Sponsor Portal (default)	Sponsored Guest Portal (default)

ISE展開のすべてのPSNに対して手順を繰り返します。

## ISEでのローカルユーザの作成

注：EAP-MD5方式では、ローカルユーザだけがISEでサポートされます。

ステップ1:[Administration] -> [Identity Management] -> [Identities] -> [Users]に移動し、[Add]をクリックします。

**Network Access Users**

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
No data available							

ステップ2：開いたページで、ユーザ名、パスワード、およびその他の必要な情報を入力し、[送信]をクリックします。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

**Network Access User**

\* Name

Status  Enabled

Email

**Passwords**

Password Type:

Password Re-Enter Password

\* Login Password    ⓘ

Enable Password    ⓘ

**User Information**

First Name

Last Name

**Account Options**

Description

Change password on next login

**Account Disable Policy**

Disable account if date exceeds  (yyyy-mm-dd)

**User Groups**

## FlexVPN HUBをRADIUSクライアントとして追加する

ステップ1:[Work Centers] -> [Posture] -> [Network Devices]に移動し、[Add]をクリックします。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Network Devices Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

**Network Devices**

Name	IP/Mask	Profile Name	Location	Type	Description
No data available					

スター2：開いたページで、[Device Name]、[IP address]、その他の必要な情報を入力し、[RADIUS Authentication settings]チェックボックスをオンにして、[Shared Secret]を入力し、ページの下部にある[Submit]をクリックします。



Network Devices List > New Network Device

Network Devices

\* Name FlexVPN-HUB

Description FlexVPN HUB

IP Address \* IP : 10.48.71.183 / 32

IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected

\* Device Profile Cisco

Model Name

Software Version

\* Network Device Group

Location All Locations Set To Default

IPSEC Is IPSEC Device Set To Default

Device Type All Device Types Set To Default

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

\* Shared Secret Show

Use Second Shared Secret

Show

CoA Port 1700 Set To Default

RADIUS DTLS Settings

DTLS Required

Shared Secret radius/dtls

CoA Port 2083 Set To Default

Issuer CA of ISE Certificates for CoA Select if required (optional)

DNS Name

General Settings

Enable KeyWrap

\* Key Encryption Key Show

\* Message Authenticator Code Key Show

Key Input Format ASCII HEXADECIMAL

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

Submit Cancel

## クライアント プロビジョニングの設定

これらは AnyConnect 設定を準備するためのステップです。

ステップ 1 : Anyconnect パッケージのダウンロード。Anyconnect パッケージ自体は ISE からの直接ダウンロードには使用できないので、開始する前に AC が PC 上で使用可能であることを確認してください。このリンクはACダウンロードに使用できます。

<http://cisco.com/go/anyconnect> にアクセスしてください。このドキュメントでは、anyconnect-win-4.5.05030-webdeploy-k9.pkgパッケージを使用します。

ステップ2:ACパッケージをISEにアップロードするには、[Work Centers] -> [Posture] -> [Client Provisioning] -> [Resources]に移動し、[Add]をクリックします。[Agent resources from local disk]を選択します。新しいウィンドウで、[Cisco Provided Packages]を選択し、[Choose File]をクリックして、PCで[AC package]を選択します。

Client Provisioning Policy

Resources

Client Provisioning Portal

Agent Resources From Local Disk > Agent Resources From Local Disk

Agent Resources From Local Disk

Category: Cisco Provided Packages

Choose File: anyconnect-...ploy-k9.pkg

AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.5.503...	AnyConnectDesktopWindows	4.5.5030.0	AnyConnect Secure Mobility Clie...

Submit Cancel

[Submit] をクリックしてインポートを終了します。パッケージのハッシュを確認し、[確認]を押します。

ステップ 3 : コンプライアンス モジュールは ISE にアップロードする必要があります。同じページ([Work Centers] -> [Posture] -> [Client Provisioning] -> [Resources] )で[Add] をクリックし、[Agent resources from Cisco site] を選択します。リソースリストで、コンプライアンスモジュールを確認し、[Save] をクリックします。このドキュメントの場合 AnyConnectComplianceModuleWindows 4.3.50.0ジュールが使用されます。

**Download Remote Resources**

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization Package v1.1.1.6 for Wir
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 3.6.11682.2	AnyConnect OS X Compliance Module 3.6.11682.2
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.29.0	AnyConnect OSX Compliance Module 4.3.29.0
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 3.6.11682.2	AnyConnect Windows Compliance Module 3.6.11682.2
<input checked="" type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.50.0	AnyConnect Windows Compliance Module 4.3.50.0
<input type="checkbox"/>	CiscoTemporalAgentOSX 4.5.02036	Cisco Temporal Agent for OSX With CM: 4.2.1019.0 Works wi
<input type="checkbox"/>	CiscoTemporalAgentWindows 4.5.02036	Cisco Temporal Agent for Windows With CM: 4.2.1226.0 Work
<input type="checkbox"/>	ComplianceModule 3.6.11510.2	NACAgent ComplianceModule v3.6.11510.2 for Windows
<input type="checkbox"/>	MACComplianceModule 3.6.11510.2	MACAgent ComplianceModule v3.6.11510.2 for MAC OSX
<input type="checkbox"/>	MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9.4.3 - ISE 1.2 , ISE 1.1.:
<input type="checkbox"/>	MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9.5.3 - ISE 1.2 Patch 12,
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.18	Supplicant Provisioning Wizard for Mac OsX 1.0.0.18 (ISE 1.1
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for Mac OsX 1.0.0.21 (for ISE
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for Mac OsX 1.0.0.27 (for ISE
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for Mac OsX 1.0.0.29 (for ISE
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for Mac OsX 1.0.0.30 (for ISE

For AnyConnect software, please download from <http://cisco.com/go/anyconnect>. Use the "Agent resource from local disk" add option, to import into ISE

Save Cancel

ステップ4:ACポスチャプロファイルを作成する必要があります。[Add] をクリックし、NAC エージェントまたは AnyConnect ポスチャ プロファイルを選択します。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The 'Posture' section is selected under 'Policy'. The 'Client Provisioning Policy' page is displayed, showing the 'Posture Agent Profile Settings' configuration. The 'AnyConnect' option is selected in the dropdown menu, and the '\* Name' field is filled with 'AC-4.5-Posture'. The 'Description' field is empty. The 'Agent Behavior' section is visible below.

- プロファイルのタイプを選択します。このシナリオでは AnyConnect を使用する必要があります。
- プロファイル名を指定します。プロファイルの [Posture Protocol] セクションに移動します。



## Posture Protocol

Parameter	Value	Notes
PRA retransmission time	<input type="text" value="120"/> secs	
Discovery host	<input type="text"/>	
* Server name rules	* <input type="text"/> <b>a.</b>	need to be blank by default to force admin to enter a value. "*" means agent will connect to all
Call Home List	<input type="text" value="pustyugo-ise23-1.examp"/> <b>b.</b>	List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)
Back-off Timer	<input type="text" value="30"/> secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.

**Note:** It is recommended that a separate profile be created for Windows and OSX deployments

Submit

Cancel

- [Server Name Rules] を指定します。このフィールドは空にすることはできません。フィールドには、適切な名前空間から PSN への AC ポスチャ モジュール接続を制限する FQDN を、ワイルドカードを使用して含めることができます。いずれかの FQDN を許可する必要がある場合は、星を付けます。
- ここで指定した名前とIPは、ポスチャ検出のステージ2で使用されています(「[ISE 2.2のポスチャフロー](#)」セクションのステップ14を参照)。名前はカンマで区切ることができます。ポート番号は、FQDN/IP の後にコロンを使用して追加できます。

ステップ5:AC設定を作成します。[Work Centers] -> [Posture] -> [Client Provisioning] -> [Resources]に移動し、[Add]をクリックし、[AnyConnect Configuration]を選択します。



The screenshot shows the 'New AnyConnect Configuration' page in the Cisco ISE interface. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Posture > Device Administration > PassiveID > Client Provisioning > Policy Elements > Posture Policy > Policy Sets > Troubleshoot > Reports > Settings.

On the left, there is a navigation pane with 'Client Provisioning Policy' and 'Client Provisioning Portal'.

The main configuration area includes:

- \* Select AnyConnect Package: AnyConnectDesktopWindows 4.5.5030.0 (a.)
- \* Configuration Name: AnyConnect Configuration (b.)
- Description: [Empty text box]
- DescriptionValue: [Empty text box]
- \* Compliance Module: AnyConnectComplianceModuleWindows 4.3.50.0 (c.)

**AnyConnect Module Selection**

- ISE Posture
- VPN
- Network Access Manager
- Web Security
- AMP Enabler
- ASA Posture
- Network Visibility
- Umbrella Roaming Security
- Start Before Logon
- Diagnostic and Reporting Tool

**Profile Selection**

- \* ISE Posture: AC-4.5-Posture (d.)
- VPN: [Empty dropdown]
- Network Access Manager: [Empty dropdown]
- Web Security: [Empty dropdown]
- AMP Enabler: [Empty dropdown]
- Network Visibility: [Empty dropdown]
- Umbrella Roaming Security: [Empty dropdown]
- Customer Feedback: [Empty dropdown]

- AC パッケージを選択します。
- AC 設定名を入力します。
- コンプライアンス モジュールのバージョンを選択します。
- ドロップダウン リストから、AC ポスチャ設定プロファイルを選択します。

ステップ 6: クライアント プロビジョニング ポリシーを設定します。[Work Centers] -> [Posture] -> [Client Provisioning] に移動します。初期設定の場合、デフォルトで表示されるポリシーに空の値を入力できます。既存のポスチャ設定にポリシーを追加する必要がある場合は、再利用できるポリシーに移動し **Duplicate Above** まったく新しいポリシーを作成することもできます。

これはこのドキュメントで使用するポリシーの例です。

The screenshot shows the 'Client Provisioning Policy' configuration page. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Posture > Device Administration > PassiveID > Client Provisioning > Policy Elements > Posture Policy > Policy Sets > Troubleshoot > Reports > Settings.

The main configuration area includes:

- Rule Name: [Empty text box]
- Identity Groups: Any
- Operating Systems: Windows All
- Other Conditions: Condition(s)
- Results: AnyConnect Configuration

**Agent Configuration**

- Agent: AnyConnect Configuration

**Native Supplicant Configuration**

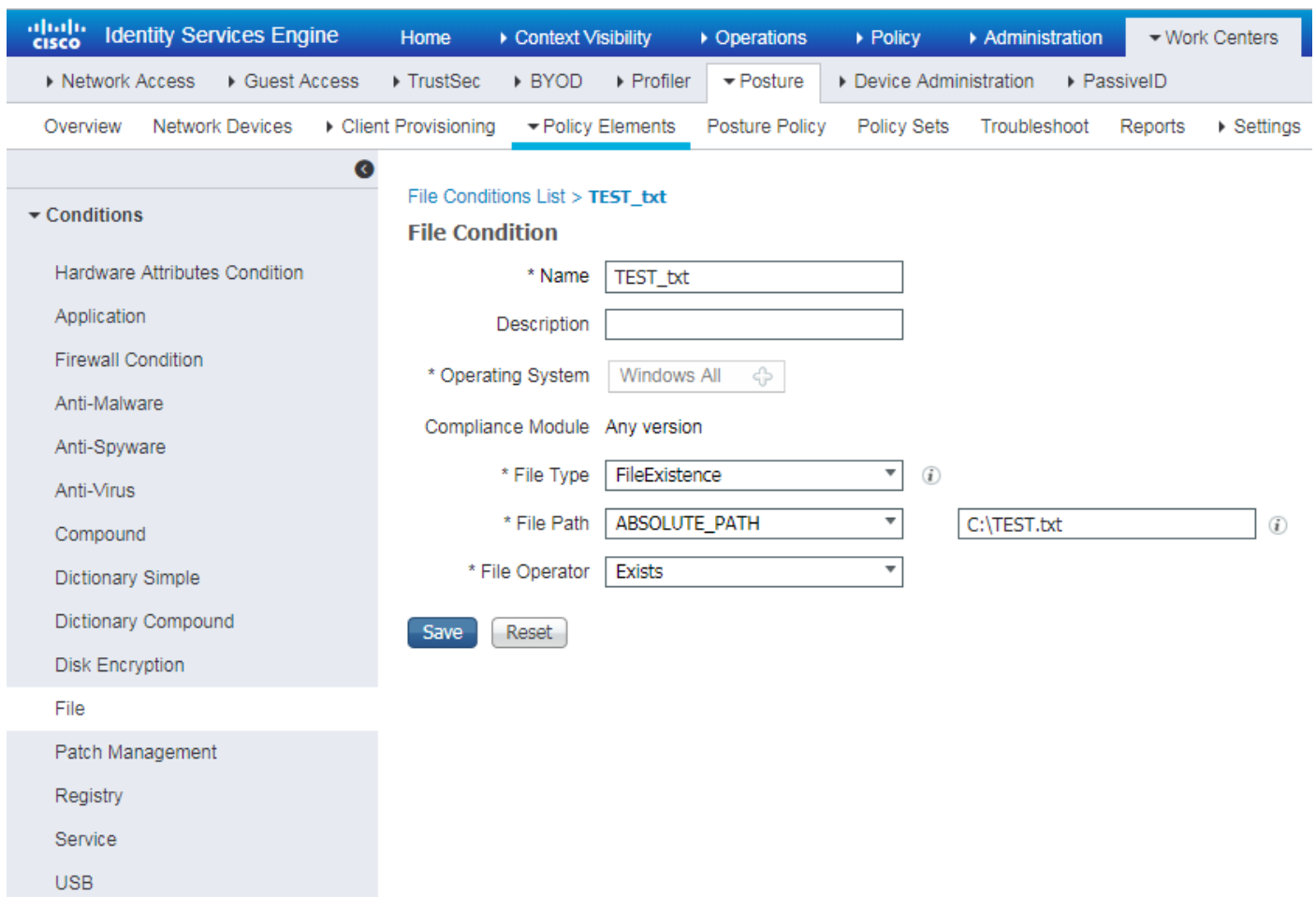
- Config Wizard: Choose a Config Wizard
- Wizard Profile: Choose a Wizard Profile

結果のセクションで AC 設定を選択します。

## ポストチャ ポリシーおよび条件

簡易なポストチャ チェックが使用されます。ISEは、エンドデバイス側のファイルC:\TEST.txtの存在をチェックするように設定されています。実際のシナリオははるかに複雑な場合がありますが、一般的な設定手順は同じです。

ステップ 1： ポストチャ ステータスの作成。ポストチャの条件は、[ワークセンター] -> [ポストチャ] -> [ポリシー要素] -> [条件]にあります。ポストチャ条件のタイプを選択し、[Add]をクリックします。必要な情報を指定し、[保存]をクリックします。次に、C:\TEST.txtファイルが存在するかどうかを確認するサービス条件の例を示します。

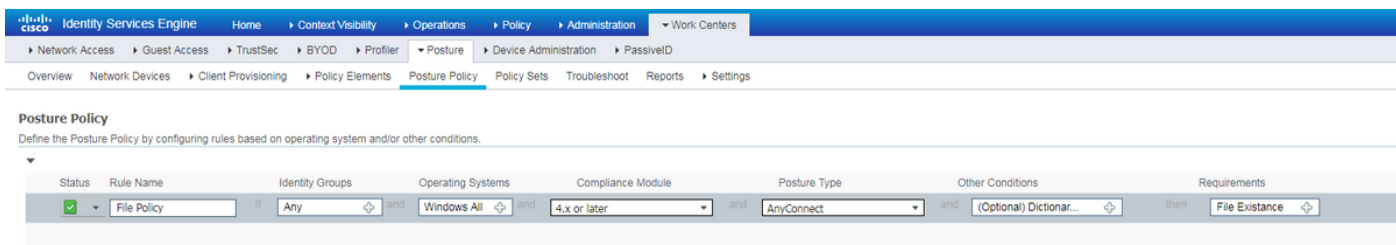


ステップ 2： ポストチャ要件の設定。[Work Centers] -> [Posture] -> [Policy Elements] -> [Requirements]に移動します。TEST.txtファイルの例を次に示します。



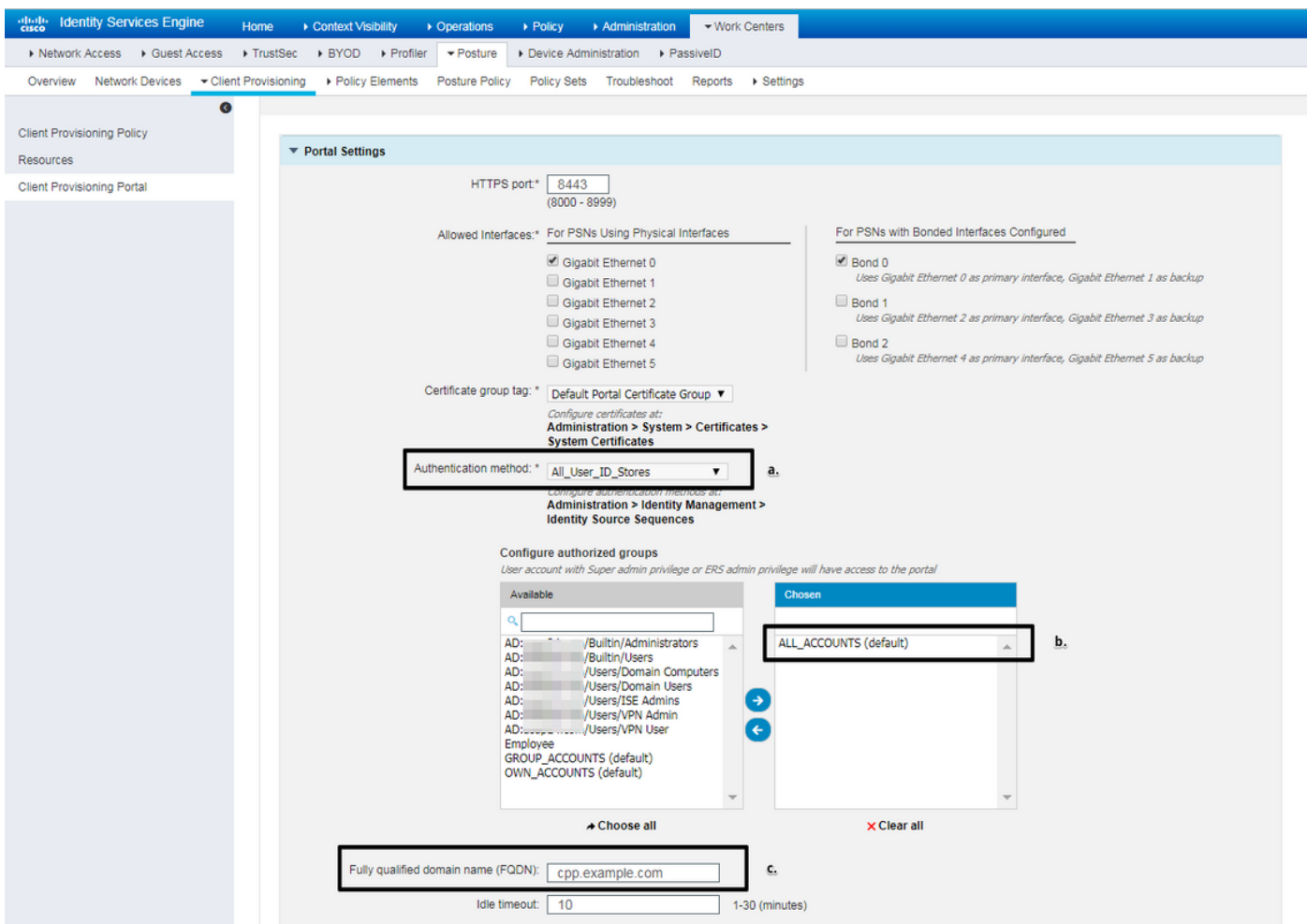
新しい要件でポストチャ条件を選択し、修復アクションを指定します。

ステップ 3： Posture policy configuration.[Work Centers] -> [Posture] -> [Posture Policy]に移動します。このドキュメントで使用されているポリシーの例を以下に示します。ポリシーには「ファイルの存在」要件が必須として割り当てられており、他の条件は割り当てられていません。



## クライアント プロビジョニング ポータルの設定

リダイレクションなしポスチャの場合には、クライアント プロビジョニング ポータルの設定を編集する必要があります。[ワークセンター] -> [ポスチャ] -> [クライアントプロビジョニング] -> [クライアントプロビジョニングポータル]に移動します。デフォルトポータルを使用するか、独自のポータルを作成できます。



これらの設定は、リダイレクトがないシナリオではポータル設定で編集する必要があります。

- [Authentication] では、SSO でユーザのセッションを見つけられない場合に使用する ID ソースシーケンスを指定します。
- 選択された ID ソースシーケンスに従って、使用可能なグループのリストが入力されます。この時点で、ポータルログインが許可されたグループを選択する必要があります。
- クライアント プロビジョニング ポータルの FQDN を指定する必要があります。この FQDN は ISE PSNs IP に解決できる必要があります。最初の接続の試行中に、Web ブラウザで FQDN を指定するようにユーザに指示する必要があります。

## 認可プロファイルおよびポリシーの設定

ポスチャ ステータスが取得できない場合には、クライアントの初期アクセスを制限する必要があります。これは次のいくつかの方法で実現できます。

- Radius フィルタ ID : この属性により、NAD でローカルに定義した ACL を、ポスチャ ステータスが不明なユーザに割り当てることができます。これは標準の RFC 属性であるため、このアプローチはすべての NAD ベンダーに有効です。
- Cisco:cisco-av-pair = ip:interface-config:Radius Filter-Idに非常によく似ており、NADでローカルに定義されたACLは、不明なポスチャステータスのユーザに割り当てることができます。  
設定例 :

```
cisco-av-pair = ip:interface-config=ip access-group DENY_SERVER in
```

ステップ 1 : 認可プロファイルを設定します。

通常どおり、ポスチャには 2 つの認可プロファイルが必要です。最初に、どのようなネットワークアクセス制限も含める必要があります。このプロファイルは、ポスチャ ステータスが準拠に等しくない認証に適用できます。2 番目の認可プロファイルは、許可アクセスのみが含まれる場合があり、準拠に等しいポスチャ ステータスのセッションに適用できます。

認可プロファイルを作成するには、[Work Centers] -> [Posture] -> [Policy Elements] -> [Authorization Profiles]に移動します。

Radius Filter-Idを使用した制限付きアクセスプロファイルの例 :

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Network Devices Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Authorization Profiles > LIMITED\_ACCESS

### Authorization Profile

\* Name: LIMITED\_ACCESS

Description:

\* Access Type: ACCESS\_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:  *i*

Passive Identity Tracking:  *i*

---

### Common Tasks

DACL Name

ACL (Filter-ID): DENY\_SERVER.in

Security Group

VLAN

---

### Advanced Attributes Settings

Select an item = [ ] +

---

### Attributes Details

Access Type = ACCESS\_ACCEPT  
Filter-ID = DENY\_SERVER.in

cisco-av-pairを使用した制限付きアクセスプロファイルの例：

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Network Devices Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Authorization Profiles > LIMITED\_ACCESS

### Authorization Profile

\* Name: LIMITED\_ACCESS

Description: [Empty text box]

\* Access Type: ACCESS\_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:  (i)

Passive Identity Tracking:  (i)

---

#### Common Tasks

DACL Name

ACL (Filter-ID)

Security Group

VLAN

---

#### Advanced Attributes Settings

Cisco:cisco-av-pair = ip:interface-config=ip access-g... +

---

#### Attributes Details

Access Type = ACCESS\_ACCEPT  
 cisco-av-pair = ip:interface-config=ip access-group DENY\_SERVER in

Radius Filter-Idを使用した無制限アクセスプロファイルの例 :

**Identity Services Engine** Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Network Devices Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

\* Name: UNLIMITED\_ACCESS

Description: [Text Field]

\* Access Type: ACCESS\_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:  ⓘ

Passive Identity Tracking:  ⓘ

---

**Common Tasks**

DACL Name

ACL (Filter-ID) PERMIT\_ALL.in

Security Group

VLAN

---

**Advanced Attributes Settings**

Select an item = [Dropdown] - +

---

**Attributes Details**

Access Type = ACCESS\_ACCEPT  
Filter-ID = PERMIT\_ALL.in

cisco-av-pairを使用した無制限アクセスプロファイルの例：

The screenshot shows the configuration page for a policy named "UNLIMITED\_ACCESS" in the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation includes: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID. The left sidebar lists various conditions and remediations. The main configuration area includes:

- Name:** UNLIMITED\_ACCESS
- Description:** (empty field)
- Access Type:** ACCESS\_ACCEPT
- Network Device Profile:** Cisco
- Service Template:** (checkbox, unchecked)
- Track Movement:** (checkbox, unchecked)
- Passive Identity Tracking:** (checkbox, unchecked)

Below the main configuration, there are sections for:

- Common Tasks:** Includes checkboxes for DACL Name, ACL (Filter-ID), Security Group, and VLAN.
- Advanced Attributes Settings:** Shows a configuration rule: Cisco:cisco-av-pair = ip:interface-config=ip access-g...
- Attributes Details:** Shows the resulting configuration: Access Type = ACCESS\_ACCEPT, cisco-av-pair = ip:interface-config=ip access-group PERMIT\_ALL in

手順 2：許可ポリシーの設定このステップの間に、2つの認可ポリシーが作成されます。1つは初期認証要求を不明なポスチャステータスと照合するためのもので、もう1つは正常なポスチャプロセスの後にフルアクセスを割り当ててするためのものです。

これは、この場合の単純な認可ポリシーの例です。

▼ Authorization Policy (12)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
●	Unknown_Compliance_Redirect	AND Network_Access_Authentication_Passed Compliance_Unknown_Devices	LIMITED_ACCESS	Select from list	55	⚙️
●	NonCompliant_Devices_Redirect	AND Network_Access_Authentication_Passed Non_Compliant_Devices	LIMITED_ACCESS	Select from list	3	⚙️
●	Compliant_Devices_Access	AND Network_Access_Authentication_Passed Compliant_Devices	UNLIMITED_ACCESS	Select from list	30	⚙️

認証ポリシーの設定はこのドキュメントの一部ではありませんが、認証ポリシーの処理を開始する前に認証を成功させる必要があることに注意してください。

## 確認



フローの基本検証は、次の3つの主要ステップで構成できます。

ステップ1: FlexVPN HubでのRA VPNセッションの確認:

```
show crypto session username vpnuser detail
```

```
Crypto session current status
```

```
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
```

```
Interface: Virtual-Access1
```

```
Profile: FlexVPN-IKEv2-Profile-1
```

```
Uptime: 00:04:40
```

```
Session status: UP-ACTIVE
```

```
Peer: 7.7.7.7 port 60644 fvrf: (none) ivrf: (none)
```

```
Phase1_id: example.com
```

```
Desc: (none)
```

```
Session ID: 20
```

```
IKEv2 SA: local 5.5.5.5/4500 remote 7.7.7.7/60644 Active
```

```
Capabilities: DNX connid: 1 lifetime: 23:55:20
```

```
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 10.20.30.107
```

```
Active SAs: 2, origin: crypto map
```

```
Inbound: #pkts dec'ed 499 drop 0 life (KB/Sec) 4607933/3320
```

```
Outbound: #pkts enc'ed 185 drop 0 life (KB/Sec) 4607945/3320
```

```
show crypto ikev2 sa detail
```

```
IPv4 Crypto IKEv2 SA
```

Tunnel-id	Local	Remote	fvrf/ivrf	Status
1	5.5.5.5/4500	7.7.7.7/60644	none/none	READY

Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp: 5, Auth sign: RSA, Auth verify: EAP

Life/Active Time: 86400/393 sec  
CE id: 1010, Session-id: 8  
Status Description: Negotiation done  
Local spi: 54EC006180B502D8 Remote spi: C3B92D79A86B0DF8  
Local id: cn=flexvpn-hub.example.com  
Remote id: example.com  
Remote EAP id: vpnuser  
Local req msg id: 0 Remote req msg id: 19  
Local next msg id: 0 Remote next msg id: 19  
Local req queued: 0 Remote req queued: 19  
Local window: 5 Remote window: 1  
DPD configured for 60 seconds, retry 2  
Fragmentation not configured.  
Dynamic Route Update: disabled  
Extended Authentication configured.  
NAT-T is detected outside  
Cisco Trust Security SGT is disabled  
Assigned host addr: 10.20.30.107  
Initiator of SA : No

```
IPv6 Crypto IKEv2 SA
```

ステップ2: 認証フローの検証 ( Radiusライブログ ):

Time	Status	Details	Identity	Posture Status	Endpoint ID	Authentication P...	Authorization Policy	Authorization Profiles	IP Address
3. Jun 07, 2018 07:40:01.378 PM			Identity	Compliant	7.7.7.7			UNLIMITED_ACCESS	
2. Jun 07, 2018 07:39:59.345 PM			vpnruser	Compliant	7.7.7.7	Default >> Default	Default >> Unknown_Compliance	LIMITED_ACCESS	10.20.30.112
1. Jun 07, 2018 07:39:22.414 PM			vpnruser	NotApplicable	7.7.7.7	Default >> Default	Default >> Unknown_Compliance	LIMITED_ACCESS	

1. 初期認証。このステップに対しては、認可プロファイルが適用されている検証に注目できます。予想外の認可プロファイルが適用されている場合は、詳細な認証レポートを調査してください。[Details] 列で拡大表示をクリックすると、このレポートを開くことができます。詳細認証レポート内の属性は、照合する予定の認可ポリシー内の条件と比較できます。
2. この例では、セッションデータの変更は、NotApplicableからCompliantに変更されています。
3. ネットワーク アクセス デバイスへの COA。このCOAは、NAD側から新しい認証をプッシュし、ISE側で新しい認可ポリシー割り当てをプッシュする必要があります。COAが失敗した場合は、詳細レポートを開いて理由を調査できます。COA で生じる可能性がある一般的な問題には次のものがあります。COA タイムアウト：この場合、要求を送信した PSN が NAD 側で COA クライアントとして設定されていないか、または COA 要求がどこか途中でドロップされたかのいずれかです。COA 否定 ACK：COA は NAD に受け取られましたが、何らかの理由で COA 操作を確認できなかったことを示します。このシナリオの場合、詳細レポートにさらに詳細な説明が記載されています。

この例では、IOS XEベースのルータがNADとして使用されているため、ユーザに対する後続の認証要求を確認できません。これは、ISEがIOS XEのCOAプッシュを使用し、VPNサービスの中断を回避するためです。このようなシナリオでは、COA 自体に新しい認可パラメータが含まれているため、再認証は不要です。

ステップ3：ポスチャレポートの検証 – [Operations] -> [Reports] -> [Reports] -> [Endpoint and Users] -> [Posture Assessment by Endpoint]に移動します。

The screenshot shows the Cisco ISE interface with the 'Posture Assessment by Endpoint' report selected. The report is for the period from 2018-06-07 00:00:00.0 to 2018-06-07 19:52:48.0. The table below represents the data shown in the report.

Logged At	Status	Details	PRA Action	Identity	Endpoint ID	IP Address
2018-06-07 19:39:59.345			N/A	vpnruser	50.00.00.03.00.00	10.20.30.112
2018-06-07 19:38:14.053			N/A	vpn	50.00.00.03.00.00	10.20.30.111
2018-06-07 19:35:03.172			N/A	vpnruser	50.00.00.03.00.00	10.20.30.110
2018-06-07 19:29:38.761			N/A	vpn	50.00.00.03.00.00	10.20.30.109
2018-06-07 19:26:52.657			N/A	vpnruser	50.00.00.03.00.00	10.20.30.108
2018-06-07 19:17:17.906			N/A	vpnruser	50.00.00.03.00.00	10.20.30.107

個別の各イベントについての詳細レポートをここから開いて、たとえばそのレポートが属するセッション ID、エンドポイントに対して ISE で選択された厳密なポスチャ要件、および各要件のステータスを確認できます。

## トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

## 1. ヘッドエンドから収集される IKEv2 デバッグ :

```
debug crypto ikev2
debug crypto ikev2 packet
debug crypto ikev2 internal
debug crypto ikev2 error
```

## 2. ローカル属性とリモート属性の割り当てを表示するための AAA デバッグ :

```
debug aaa authorization
debug aaa authentication
debug aaa accounting
debug aaa coa
debug radius authentication
debug radius accounting
```

## 3. AnyConnect クライアントからの DART。

4. ポスチャ プロセストラブルシューティングの場合、これらの ISE コンポーネントは、ポスチャのプロセスが実行されることがある ISE ノード上でデバッグが有効になっている必要があります。**client-webapp** : エージェント プロビジョニングを担うコンポーネント。ターゲット ログ ファイル **guest.log** および **ise-psc.log**。**guestaccess** : クライアント プロビジョニング ポータル コンポーネントとセッション オーナーのルックアップを担うコンポーネント ( 要求が誤った PSN に送信される場合 )。ターゲット ログ ファイル : **guest.log**。**provisioning** – クライアントのプロビジョニングポリシー処理を担当するコンポーネント。ターゲットログファイル – **guest.log**。**posture** – すべてのポスチャ関連イベント。ターゲットログファイル – **ise-psc.log**
5. クライアント側のトラブルシューティングでは、以下を使用できます。**AnyConnect.txt** : このファイルは DART バンドル内にあり、VPN のトラブルシューティングに使用できます。**acisensa.log** : クライアント側でのクライアント プロビジョニング障害の場合、このファイルは NSA がダウンロードされているのと同じフォルダ内に作成されます ( Windows の場合は通常は Downloads ディレクトリです )。**AnyConnect\_ISEPosture.txt** : このファイルは Cisco AnyConnect ISE Posture Module ディレクトリの DART バンドル内にあります。ISE PSN ディスカバリに関するすべての情報とポスチャ フローの一般的な手順は、このファイルに記録されます。