

# 使用FlexVPN配置ISE终端安全评估

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[DNS服务器配置](#)

[IOS XE初始配置](#)

[配置身份证书](#)

[配置IKEv2](#)

[AnyConnect客户端配置文件配置](#)

[ISE配置](#)

[管理员和CPP证书配置](#)

[在ISE上创建本地用户](#)

[将FlexVPN HUB添加为Radius客户端](#)

[客户端调配配置](#)

[状态策略和条件](#)

[配置客户端调配门户](#)

[配置授权配置文件和策略](#)

[验证](#)

[故障排除](#)

## 简介

本文档提供了如何使用AnyConnect IKEv2和EAP-Message Digest 5(EAP-MD5)身份验证方法配置IOS XE头端以进行远程访问的示例。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- IOS XE上的FlexVPN远程访问(RA)VPN配置
- AnyConnect(AC)客户端配置
- 身份服务引擎(ISE)2.2及更高版本的安全评估流程
- 在ISE上配置状态组件
- 在Windows Server 2008 R2上配置DNS服务器

## 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行IOS XE 16.8 [Fujii]的思科CSR1000V
- 在Windows 7上运行的AnyConnect客户端版本4.5.03040
- 思科ISE 2.3
- Windows 2008 R2服务器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 背景信息

为确保实施的网络安全措施保持相关和有效，思科ISE使您能够验证和维护访问受保护网络的任何客户端计算机的安全功能。通过采用旨在确保客户端计算机上提供最新安全设置或应用的安全评估策略，Cisco ISE管理员可以确保任何访问网络的客户端计算机满足并继续满足企业网络访问定义的安全标准。状态合规性报告为思科ISE提供用户登录时以及定期重新评估时客户端的合规性级别快照。

状态可以用三个主要元素表示：

1. ISE作为策略配置分发和决策点。从ISE的管理员角度，您配置终端安全评估策略（应满足哪些确切条件才能将设备标记为符合公司标准）、客户端调配策略（应在哪种设备上安装什么代理软件）和授权策略（应分配什么权限，取决于其终端安全评估状态）。
2. 网络访问设备(NAD)作为策略实施点。在NAD端，实际授权限制在用户身份验证时应用。ISE作为策略点提供授权参数，如访问控制列表(ACL)。传统上，为了进行状态，需要NAD支持授权更改(CoA)，以在终端的状态确定后对用户重新进行身份验证。从ISE 2.2开始，不需要NAD支持重定向。  
**注意：**运行IOS XE的路由器不支持重定向。**注意：**IOS XE软件必须对以下缺陷进行修复，使CoA与ISE完全可操作：  
[CSCve16269](#) IKEv2 CoA不适用于ISE  
[CSCvi90729](#) IKEv2 CoA与ISE不配合（coa-push=TRUE而非true）
3. 代理软件作为数据收集和与最终用户交互的点。代理从ISE接收有关状态要求的信息，并向ISE提供有关要求状态的报告。本文档基于Anyconnect ISE终端安全评估模块，该模块是唯一一个完全支持终端安全评估且无重定向的模块。

无重定向的终端安全评估流在[“ISE 2.2版和2.2版之前和2.2版的ISE终端安全评估样式比较”](#)部分“ISE 2.2版中的终端安全评估流”中有详细记录。

使用FlexVPN的Anyconnect ISE终端安全评估模块调配可通过两种不同方式完成：

- 手动 — 从思科软件下载门户上提供的Anyconnect软件包在客户端工作站上手动安装模块：  
<https://software.cisco.com/download/home/283000185>。

以下条件必须满足，才能使用手动ISE终端安全评估模块调配进行终端安全评估：

1. 域名服务器(DNS)必须将完全限定域名(FQDN)enroll.cisco.com解析为策略服务节点(PSN)IP。在首次连接尝试期间，状态模块没有任何有关可用PSN的信息。它正在发送发现探测功能以查找可用的PSN。FQDN enroll.cisco.com用于其中一个探测。

2. 必须允许PSN IP使用TCP端口8905。在此场景中，状态通过TCP端口8905进行。

3. PSN节点上的管理证书必须在SAN字段中具有enroll.cisco.com。通过TCP 8905保护VPN用户和PSN节点之间的连接通过管理证书进行保护，如果PSN节点的管理证书中没有此名称“enroll.cisco.com”，用户将收到证书警告。

**注意：**根据RFC6125证书，如果指定了SAN值，应忽略CN。这意味着我们还需要在SAN字段中添加管理员证书的CN。

- 通过客户端调配门户(CPP)自动调配 — 通过直接通过门户FQDN访问CPP，从ISE下载并安装模块。

以下条件必须满足，才能使用自动ISE终端安全评估模块调配进行终端安全评估：

1. DNS必须将CPP的FQDN解析为策略服务节点(PSN)IP。

2. 必须允许PSN IP的TCP端口80、443和CPP端口(默认情况下为8443)。客户端需要通过HTTP直接打开CPP FQDN (将重定向到HTTPS) 或HTTPS，此请求将重定向到CPP端口 (默认情况下为8443)，然后状态将通过该端口进行。

3. PSN节点上的管理员和CPP证书在SAN字段中必须有CPP FQDN。通过TCP 443在VPN用户和PSN节点之间的连接受管理员证书保护，CPP端口上的连接受CPP证书保护。

**注意：**根据RFC6125证书，如果指定了SAN值，应忽略CN。这意味着我们还需要在相应证书的SAN字段中添加管理员证书的CN和CPP证书。

**注意：**如果ISE软件不包含CSCvj76466的修复，则只有在对客户端进行身份验证的同一PSN上执行安全或客户端调配时，安全评估或客户端调配才会起作用。

在使用FlexVPN时，流程包括以下步骤：

1. 用户使用Anyconnect客户端连接到FlexVPN集线器。

2. ISE将Access-Accept发送到FlexVPN中心，需要应用ACL名称来限制访问。

3a 首次连接手动调配 — ISE终端安全评估模块开始发现策略服务器通过TCP端口8905将探测发送到enroll.cisco.com。因此，终端安全评估模块会下载已配置的终端安全评估配置文件并更新客户端上的合规性模块。

在下次连接尝试期间，ISE终端安全评估模块还将使用终端安全评估配置文件的Call Home列表中指定的名称和IP进行策略服务器检测。

3b 首次连接自动调配 — 客户端通过FQDN打开CPP。结果，网络设置助理下载到客户端工作站，然后下载并安装ISE终端安全评估模块、ISE合规性模块和终端安全评估配置文件。

在下次连接尝试期间，ISE终端安全评估模块将使用终端安全评估配置文件的Call Home列表中指定的名称和IP进行策略服务器检测。

4. 安全评估模块开始合规性检查并将检查结果发送到ISE。

5. 如果客户端状态为Compliant，则ISE将Access-Accept发送到FlexVPN中心，需要为符合的客

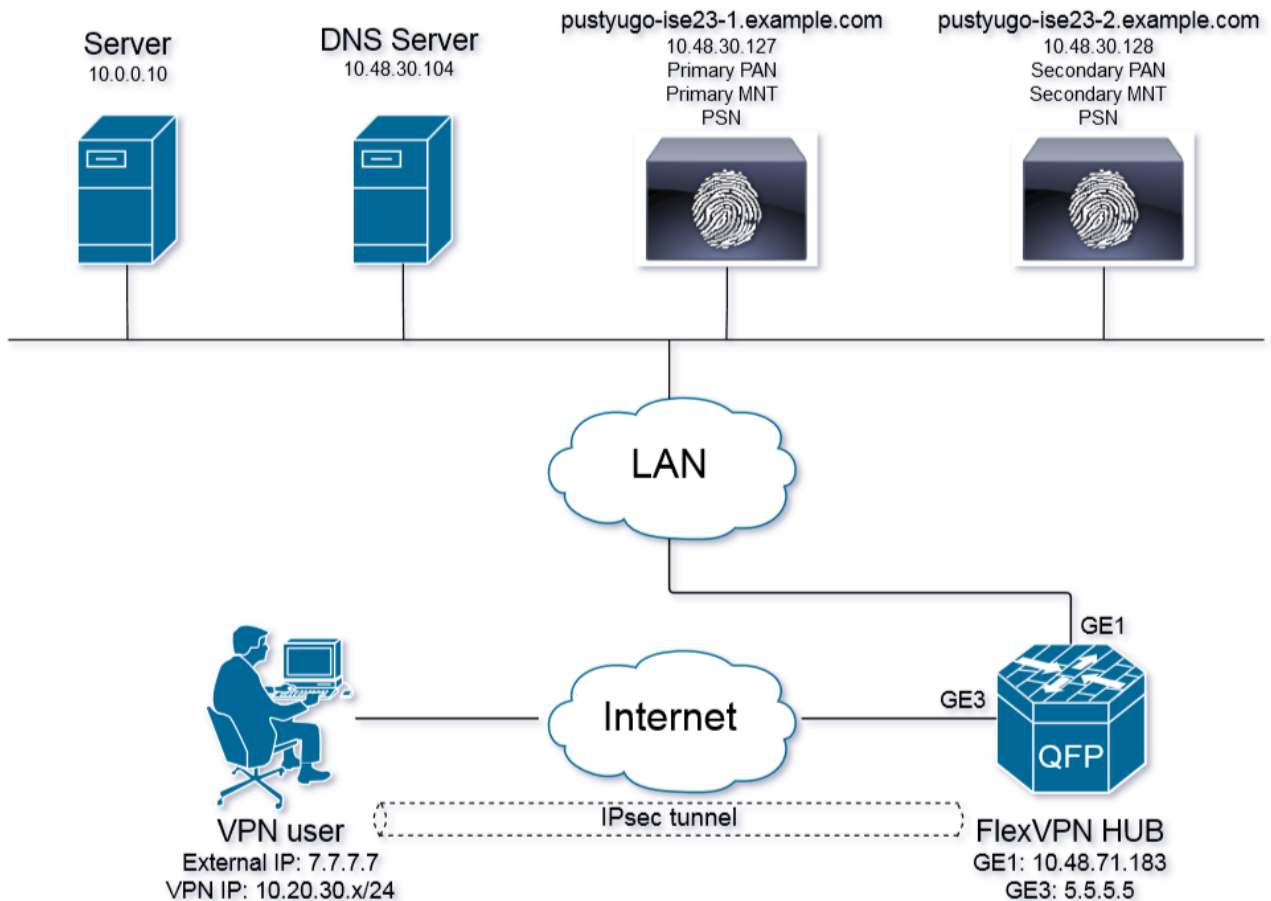
户端应用ACL名称。

6, 客户端可以访问网络。

有关终端安全评估流程的更多详细信息, 请[参阅文档“ISE 2.2版和2.2版的终端安全评估样式比较”](#)。

## 配置

### 网络图

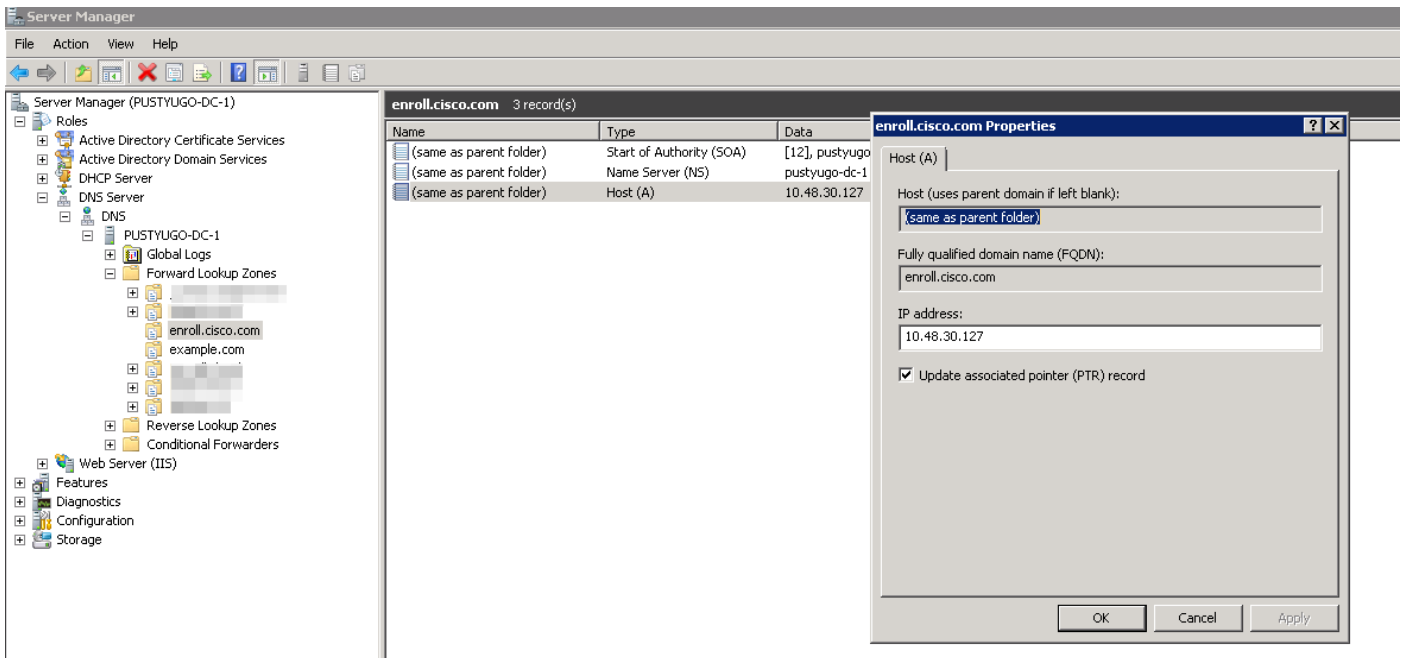


VPN用户只有在具有合规状态时才能访问服务器(10.0.0.10)。

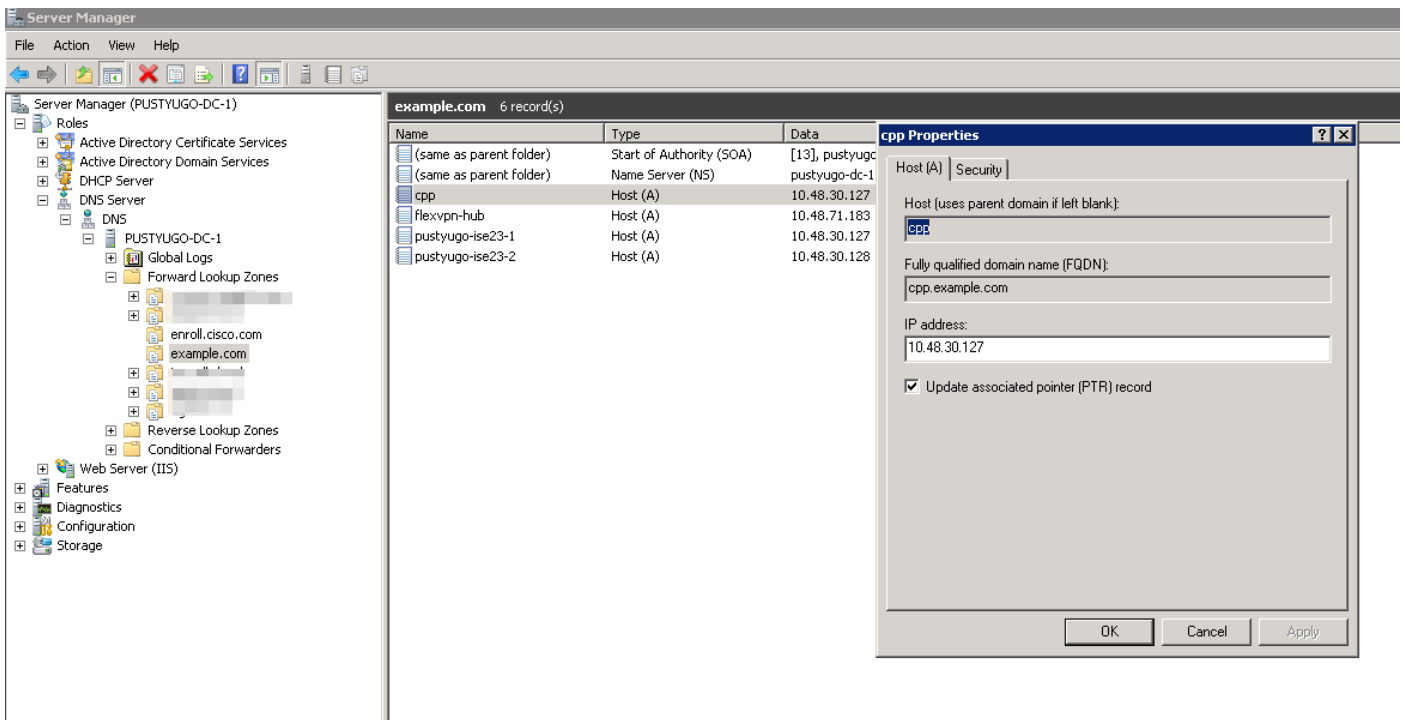
### DNS服务器配置

在本文档中, Windows Server 2008 R2用作DNS服务器。

步骤1. 为enroll.cisco.com添加指向PSN的IP的主机(A)记录:



步骤2.为指向PSN的IP的CPP FQDN(本例中使用的cpp.example.com)添加主机(A)记录:



## IOS XE初始配置

### 配置身份证书

路由器将使用证书向Anyconnect客户端验证自身。路由器证书应由用户的操作系统信任，以避免在连接建立阶段出现证书警告。

身份证书可通过以下方式之一提供：

**注意：** IKEv2 FlexVPN不支持使用自签名证书。

#### 选项1 — 在路由器上配置证书颁发机构(CA)服务器

**注意：**CA服务器可以在同一台IOS路由器或另一台路由器上创建。在本文中，CA是在同一台路由器上创建的。

**注意：**在启用CA服务器之前，您需要将时间同步到NTP服务器。

**注意：**请注意，用户将无法验证此证书的真实性，因此，除非在建立连接之前手动验证CA证书并将其导入用户计算机，否则用户数据将不会受到中间人攻击的保护。

**步骤1.为CA服务器生成RSA密钥：**

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

**步骤2.为身份证生成RSA密钥：**

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

**验证：**

```
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
```

**步骤3.配置CA:**

```
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
```

**验证：**

```
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
```

#### 步骤4.配置信任点：

```
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
```

#### 步骤5.验证CA:

```
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.
```

#### 步骤6.将路由器注册到CA:

```
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
```

检查CA上的待处理证书请求，并验证指纹是否匹配：

```
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
```

## 步骤7.使用正确的ReqID授予证书：

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

等到路由器再次请求证书（根据此配置，它将每分钟检查10次）。查找系统日志消息：

```
May 21 16:18:56.375: %PKI-6-CERTRET: Certificate received from Certificate Authority
验证证书是否已安装：
```

```
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
```

## 选项2 — 导入外部签名证书



```
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)#
```

## 配置IKEv2

### 步骤1.配置RADIUS服务器和CoA:

```
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
```

### 步骤2.配置身份验证和授权列表 :

```
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
```

### 步骤3.创建ikev2授权策略 :

```
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
```

### 步骤4.创建IKEv2配置文件 :

```
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
```

#### 步骤5.创建转换集和ipsec配置文件：

```
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
```

#### 步骤6.创建虚拟模板接口：

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

#### 步骤7.创建本地池：

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

#### 步骤8.创建ACL以限制不合规客户端的访问。在未知状态期间，至少应提供这些权限：

- DNS流量
- 通过端口80、443和8905到ISE PSN的流量
- CPP门户FQDN指向的ISE PSN的流量
- 流量到补救服务器（如果需要）

这是没有补救服务器的ACL的示例，为了获得可视性，添加了10.0.0.0/24网络的显式deny，ACL末尾存在隐式“deny ip any any”：

```
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
```

#### 步骤9.创建ACL以允许合规客户端访问：

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

#### 步骤10.拆分隧道配置（可选）

默认情况下，所有流量都将通过VPN进行定向。要仅将流量隧道化到指定网络，可以在ikev2授权策略略部分中指定这些流量。可以添加多条语句或使用标准访问列表。

```
crypto ikev2 authorization policy FlexVPN-Local-Policy-1
```

```
route set remote ipv4 10.0.0.0 255.0.0.0
```

### 步骤11.远程客户端的Internet访问 ( 可选 )

要将从远程访问客户端到互联网中主机的出站连接通过NAT连接到路由器的全局IP地址，请配置NAT转换：

```
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
```

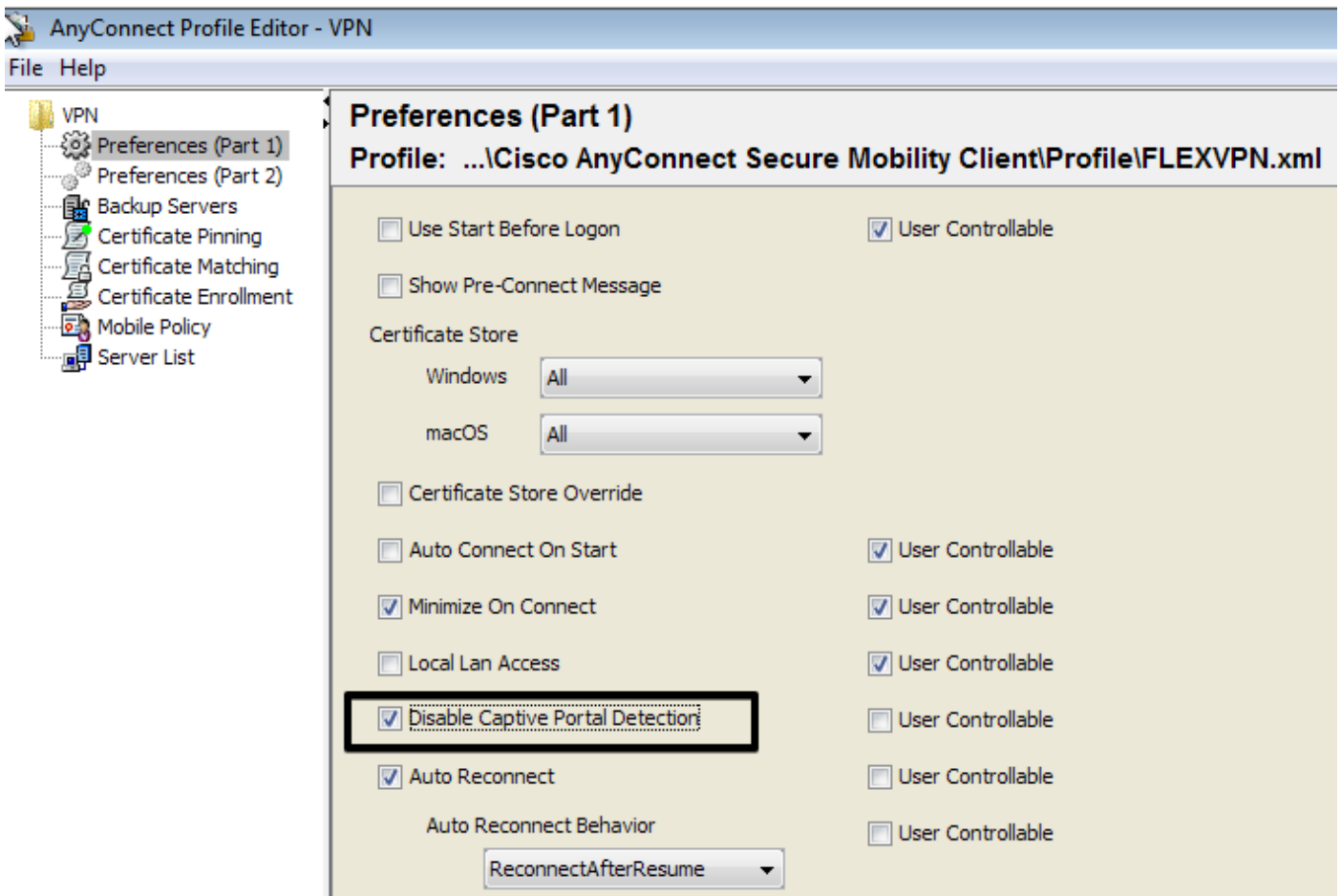
```
interface GigabitEthernet1
 ip nat outside
```

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

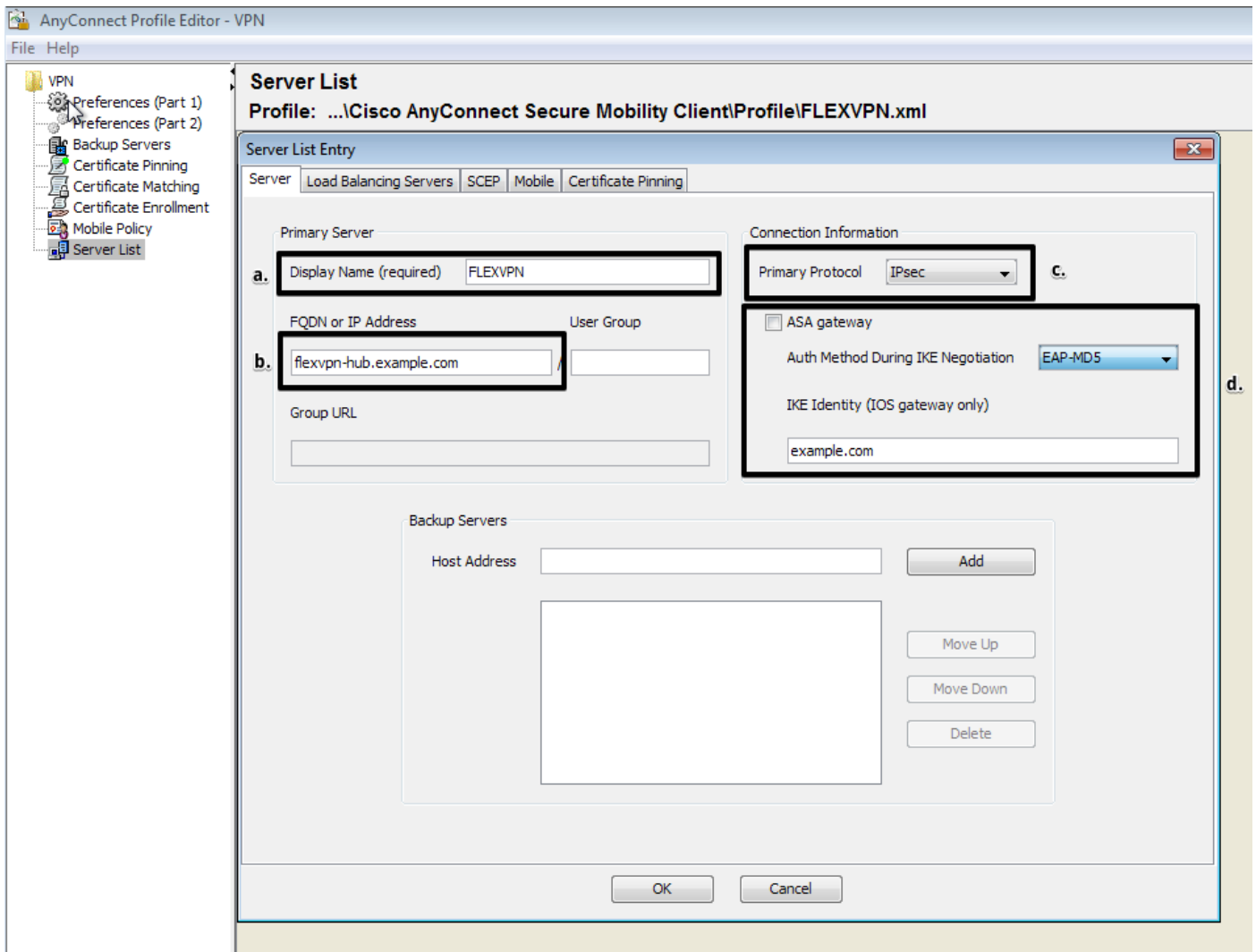
## AnyConnect客户端配置文件配置

使用AnyConnect配置文件编辑器配置客户端配置文件。Windows 7和10上AnyConnect安全移动客户端的配置文件保存在%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile中。

步骤1.禁用强制网络门户检测功能。如果FlexVPN集线器上未禁用http服务器，AnyConnect强制网络门户检测功能将导致连接失败。请注意，没有HTTP服务器，CA服务器将无法工作。



步骤2.配置服务器列表：



- 输入显示名称。
- 输入FlexVPN中心的FQDN或IP地址。
- 选择IPsec 作为主协议。
- 取消选中“ASA网关”复选框并指定EAP-MD5作为身份验证方法。输入与FlexVPN集线器上的IKEv2配置文件配置完全相同的IKE身份(在本示例中，IKEv2配置文件配置了“match identity remote key-id example.com”命令，因此我们需要将example.com用作IKE身份)。

步骤3.将配置文件保存到%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile,然后重新启动AC。

配置文件的XML等效项：

```
<?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>
    <CertificateStoreOverride>>false</CertificateStoreOverride>
  </ClientInitialization>
</AnyConnectProfile>
```

```

<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>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<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配置

### 管理员和CPP证书配置

**注意：**更改管理员证书将重新启动证书已更改的节点。

步骤1.转到Administration -> System -> Certificates -> Certificate Signing Requests , 单击 Generate Certificate Signing Requests(CSR):

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					

步骤2.在打开的页面上，选择必要的PSN节点，填写必要的字段，并在SAN字段中添加节点的FQDN、enroll.cisco.com、cpp.example.com和节点的IP地址，然后单击生成:

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

**注意：**如果在此步骤中选择“多用”，则也可以对门户使用同一证书。

在出现的窗口中，单击**Export**以pem格式将CSR保存到本地工作站：



Successfully generated CSR(s)

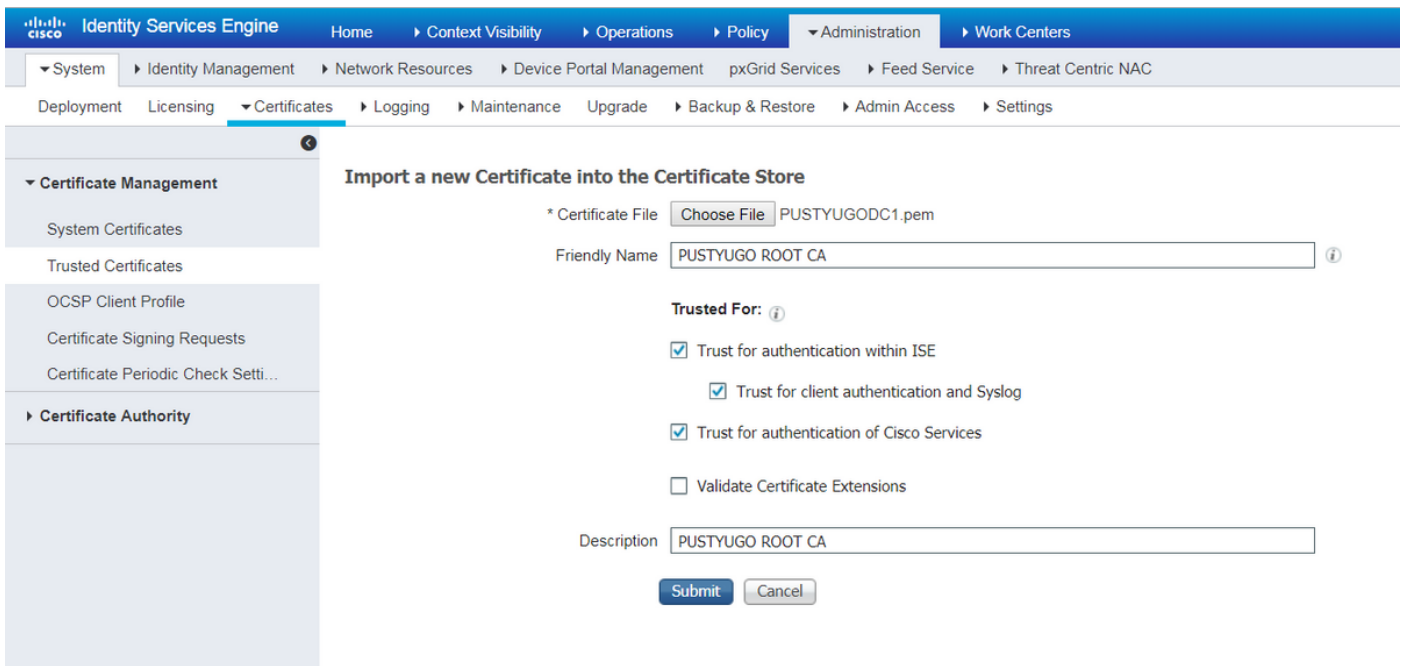
Certificate Signing request(s) generated:

pustyugo-ise23-1#Multi-Use

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

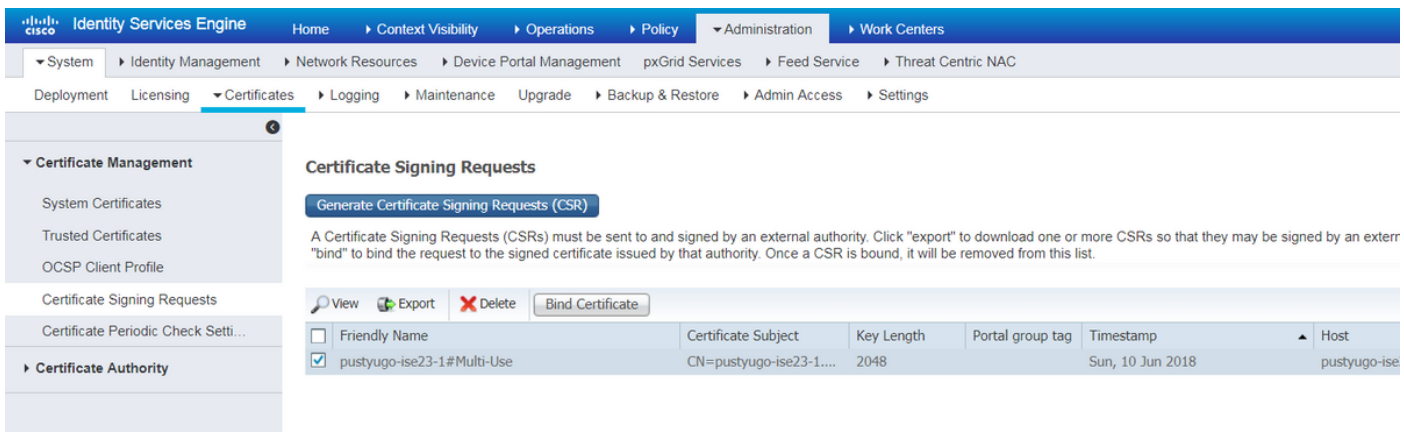
步骤3.使用带有受信任CA的CSR，从CA以及CA证书的完整链（根和中间）获取证书文件。

步骤4.转到“管理” —>“系统” —>“证书” —>“受信任证书”，单击“导入”。在下一个屏幕中，单击“选择文件”，然后选择“根CA证书文件”，填写“友好名称”和“说明”（如果需要），选择必要的“受信任对象”选项，然后单击“提交”：



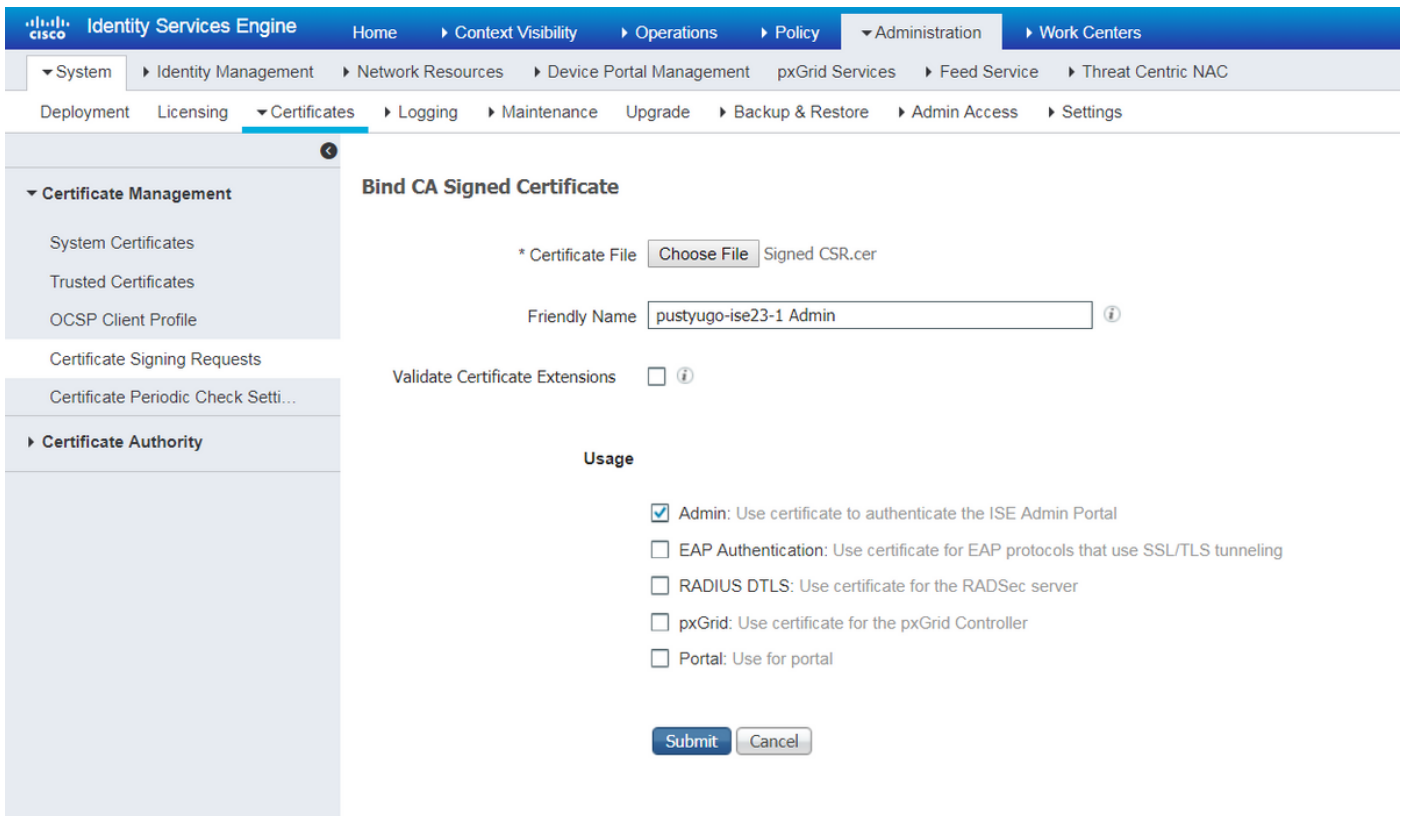
对链中的所有中间证书（如果有）重复此步骤。

步骤5.返回Administration -> System -> Certificates -> Certificate Signing Requests，选择必要的CSR，然后单击Bind Certificate:

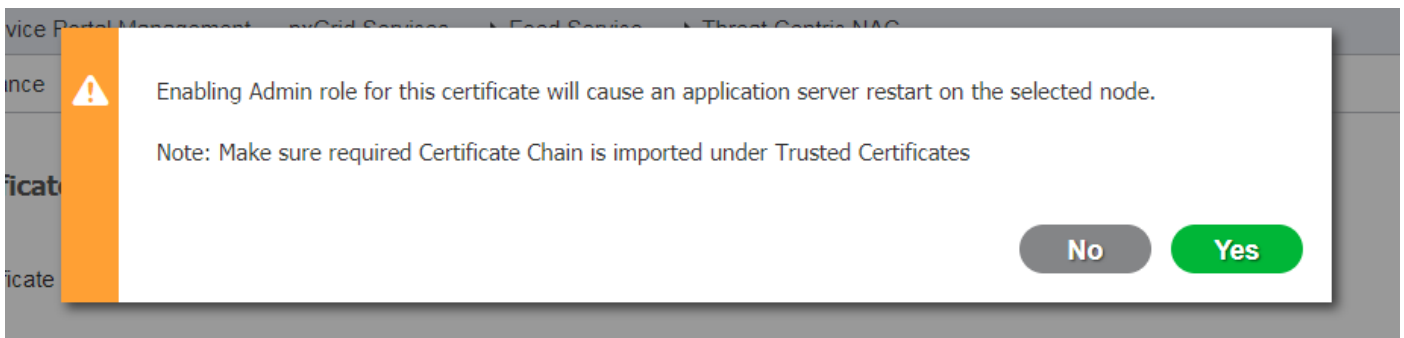


步骤6.在打开的页面上，单击Choose File，选择从CA收到的证书文件，然后输入Friendly Name（如果需要），然后选择Usage:管理(用法：如果CSR是使用“多用途”(Multi-Use)创建的，并单击“提交”(Submit)，也可以在此处选择门户：

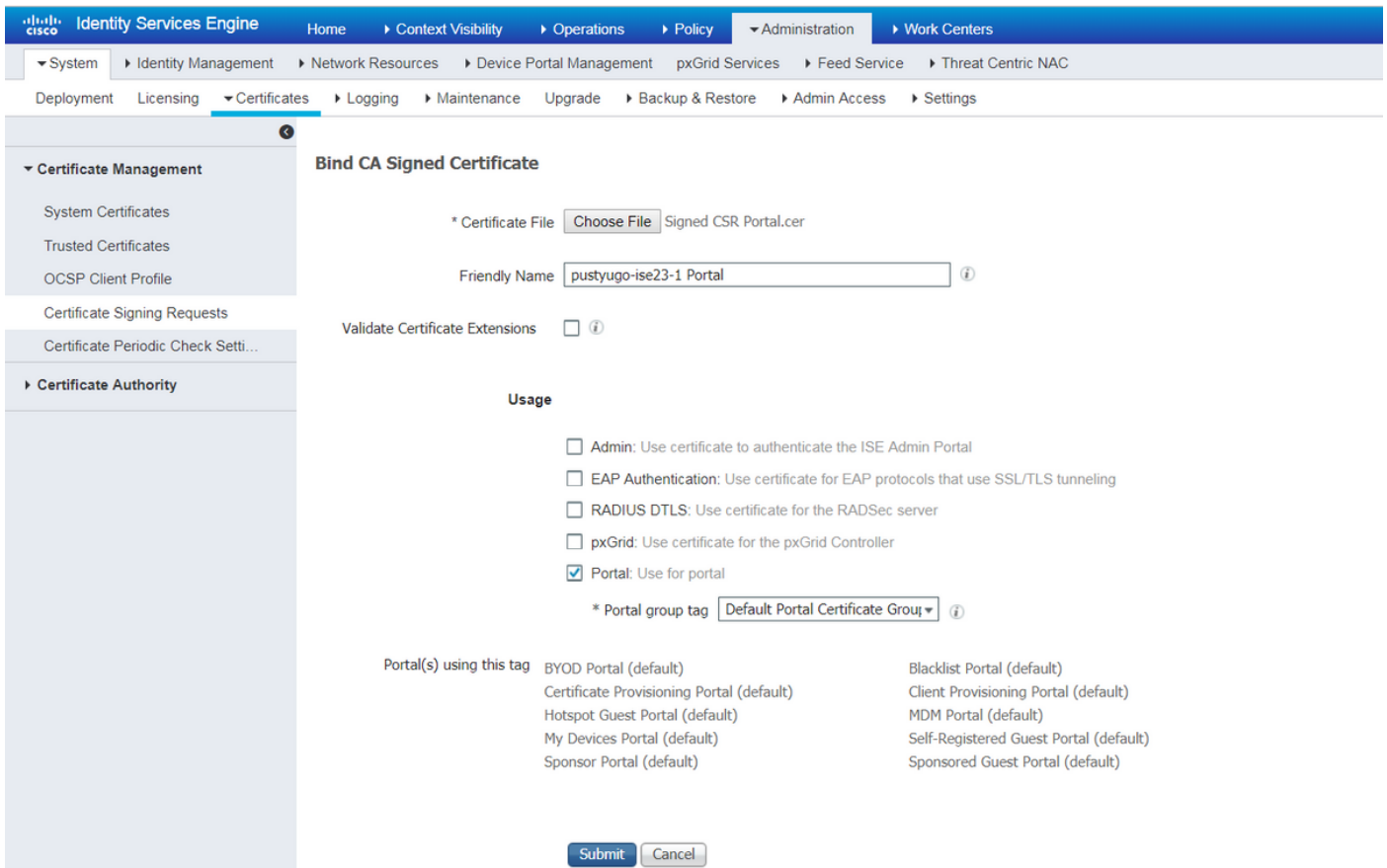




步骤7.在警告弹出窗口中单击“是”完成导入。受管理员证书更改影响的节点将重新启动：



如果决定对门户使用单独的证书，请重复更改CPP证书的步骤。在第6步中，选择使用：门户，然后点击提交：

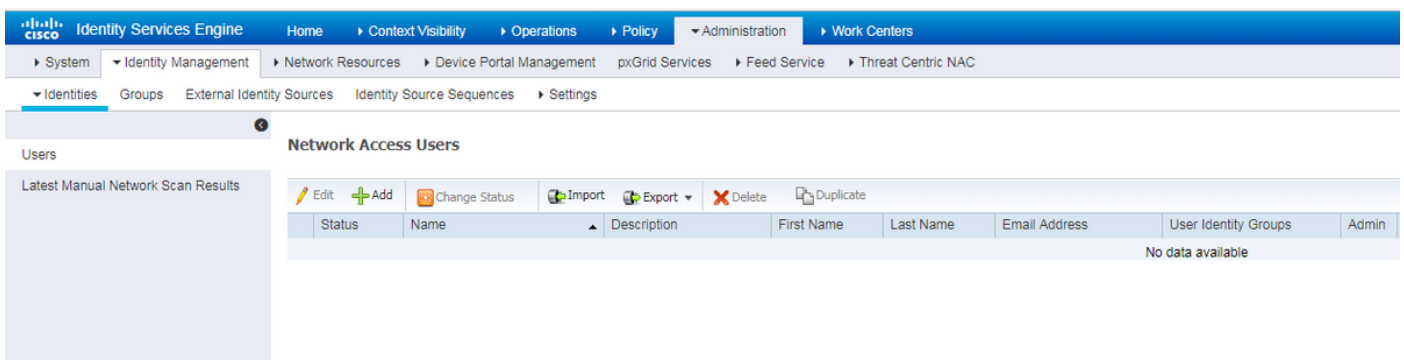


对ISE部署中的所有PSN重复上述步骤。

## 在ISE上创建本地用户

**注意：**使用EAP-MD5方法时，ISE仅支持本地用户。

步骤1.转到“管理” —>“身份管理” —>“身份” —>“用户”，单击“添加”。



步骤2.在打开的页面上输入用户名、密码和其他必要信息，然后单击“提交”。

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**

## 将FlexVPN HUB添加为Radius客户端

步骤1.转到“工作中心” —>“状态” —>“网络设备”，单击“添加”。

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					

Step 2.在打开的页面上，输入设备名称、IP地址和其他必要信息，选中复选框“RADIUS身份验证设置”，输入共享密钥，然后单击页面底部的提交。



Network Devices List > New Network Device

### Network Devices

\* Name

Description

IP Address \* IP:  /

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

\* Device Profile

Model Name

Software Version

\* Network Device Group

Location

IPSEC

Device Type

**RADIUS Authentication Settings**

#### RADIUS UDP Settings

Protocol **RADIUS**

\* Shared Secret

Use Second Shared Secret  **i**

CoA Port

#### RADIUS DTLS Settings **i**

DTLS Required  **i**

Shared Secret  **i**

CoA Port

Issuer CA of ISE Certificates for CoA  **i**

DNS Name

#### General Settings

Enable KeyWrap  **i**

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

TACACS Authentication Settings

SNMP Settings

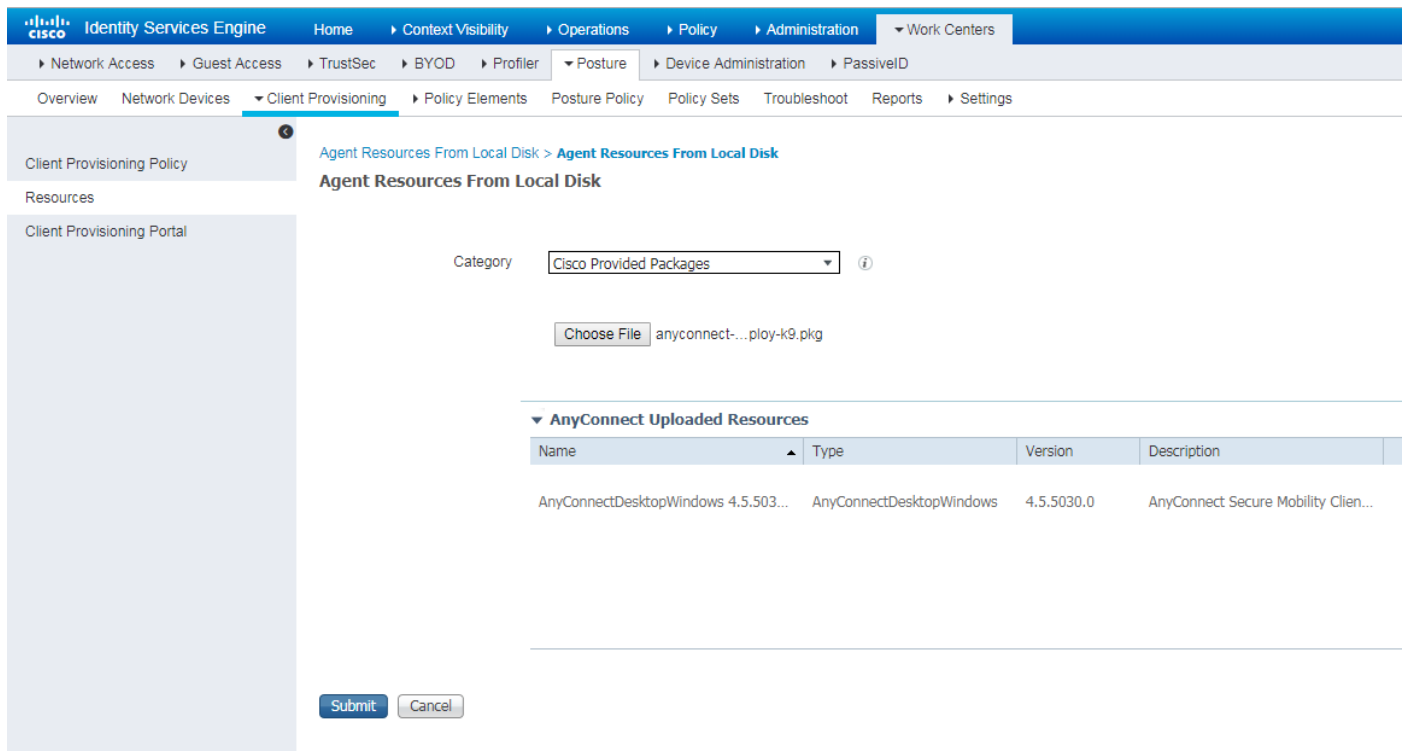
Advanced TrustSec Settings

## 客户端调配配置

以下是准备AnyConnect配置的步骤。

步骤1. 下载AnyConnect软件包。Anyconnect软件包本身不可从ISE直接下载，因此，在开始之前，请确保AC在您的PC上可用。此链接可用于AC下载 — <http://cisco.com/go/anyconnect>。在本文中，使用anyconnect-win-4.5.05030-webdeploy-k9.pkg软件包。

步骤2. 要将AC包上传到ISE，请导航至**工作中心** —>**状态** —>**客户端调配** —>**资源**，然后单击**Add**。从本地磁盘选择代理资源。在新窗口中，选择思科提供的包，单击**选择文件**并选择PC上的AC包。



The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Client Provisioning > Agent Resources From Local Disk > Agent Resources From Local Disk. The page title is "Agent Resources From Local Disk". There is a "Category" dropdown menu set to "Cisco Provided Packages". Below it is a "Choose File" button with the filename "anyconnect-...ploy-k9.pkg" displayed. A table titled "AnyConnect Uploaded Resources" is visible, with the following data:

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

At the bottom of the form, there are "Submit" and "Cancel" buttons.

单击**Submit**完成导入。验证数据包的哈希，然后按**确认**。

步骤3. 合规性模块必须上传到ISE。在同一页(工作中心->状态 —>客户端调配 —>资源)中单击**添加**，然后从**Cisco**站点中选择代理资源。在资源列表中，您应检查合规性模块并单击**保存**。对于本文档AnyConnectComplianceModuleWindows 4.3.50.0合规性模块。

**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

步骤4.现在必须创建AC状态配置文件。单击Add,然后选择NAC代理或Anyconnect终端安全评估配置文件。

Client Provisioning Policy

Resources

Client Provisioning Portal

ISE Posture Agent Profile Settings > New Profile

Posture Agent Profile Settings

a. AnyConnect

b. \* Name: AC-4.5-Posture

Description:

Agent Behavior

- 选择配置文件的类型。AnyConnect应用于此场景。
- 指定配置文件名称。导航至配置文件的**状态协议**部分

## Posture Protocol

Parameter	Value	Notes
PRA retransmission time	120 secs	
Discovery host		
* 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	pustyugo-ise23-1.exempl <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	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

• 指定**服务器名规则**，此字段不能为空。字段可以包含带通配符的FQDN，该通配符将AC状态模块从适当的命名空间限制到PSN的连接。如果应允许任何FQDN，请输入星号。

• 此处指定的名称和IP在状态发现的第2阶段(请参阅“ISE 2.2中的**状态流**”部分的**第14步**)中。您可以通过昏迷来分隔名称，也可以在FQDN/IP后添加端口号，使用冒号。

步骤5.创建交流配置。导航至**工作中心 —>状态 —>客户端调配 —>资源**，然后单击**添加**，然后选择**AnyConnect配置**。

The screenshot shows the 'New AnyConnect Configuration' page in the ISE GUI. 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.

Configuration fields include:

- \* Select AnyConnect Package: AnyConnectDesktopWindows 4.5.5030.0 **a.**
- \* Configuration Name: AnyConnect Configuration **b.**
- Description:
- Description Value
- \* 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

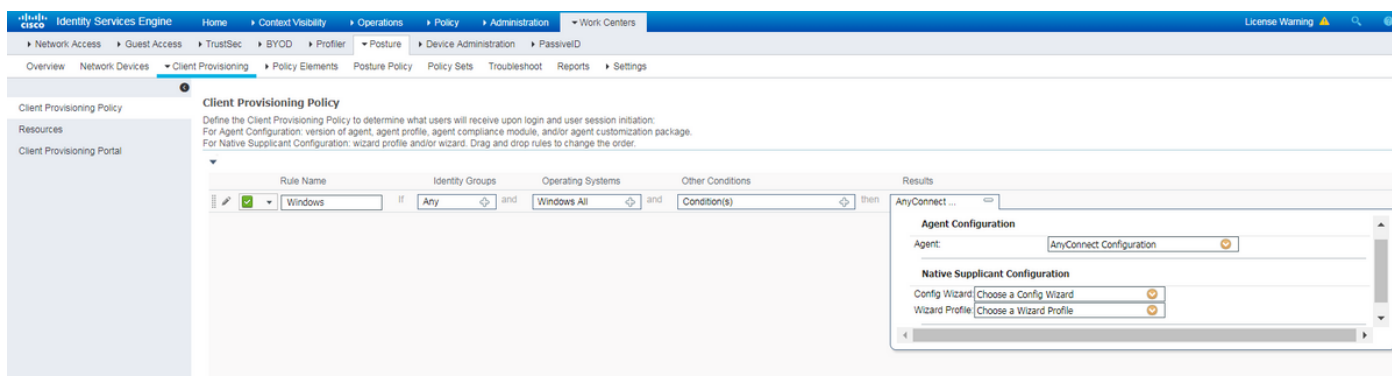
**Profile Selection**

- \* ISE Posture: AC-4,5-Posture **d.**
- VPN:
- Network Access Manager:
- Web Security:
- AMP Enabler:
- Network Visibility:
- Umbrella Roaming Security:
- Customer Feedback:

- 选择AC包。
- 提供交流配置名称。
- 选择合规性模块版本。
- 从下拉列表中选择AC状态配置配置文件。

步骤6.配置客户端调配策略。定位至**工作中心 —>状态 —>客户端设置**。在初始配置中，您可以在默认设置的策略中填充空值。如果需要将策略添加到现有状态配置中，请导航至可重复使用的策略，然后选择**上复制或下复制**。还可以创建全新策略。

这是文档中使用的策略示例。



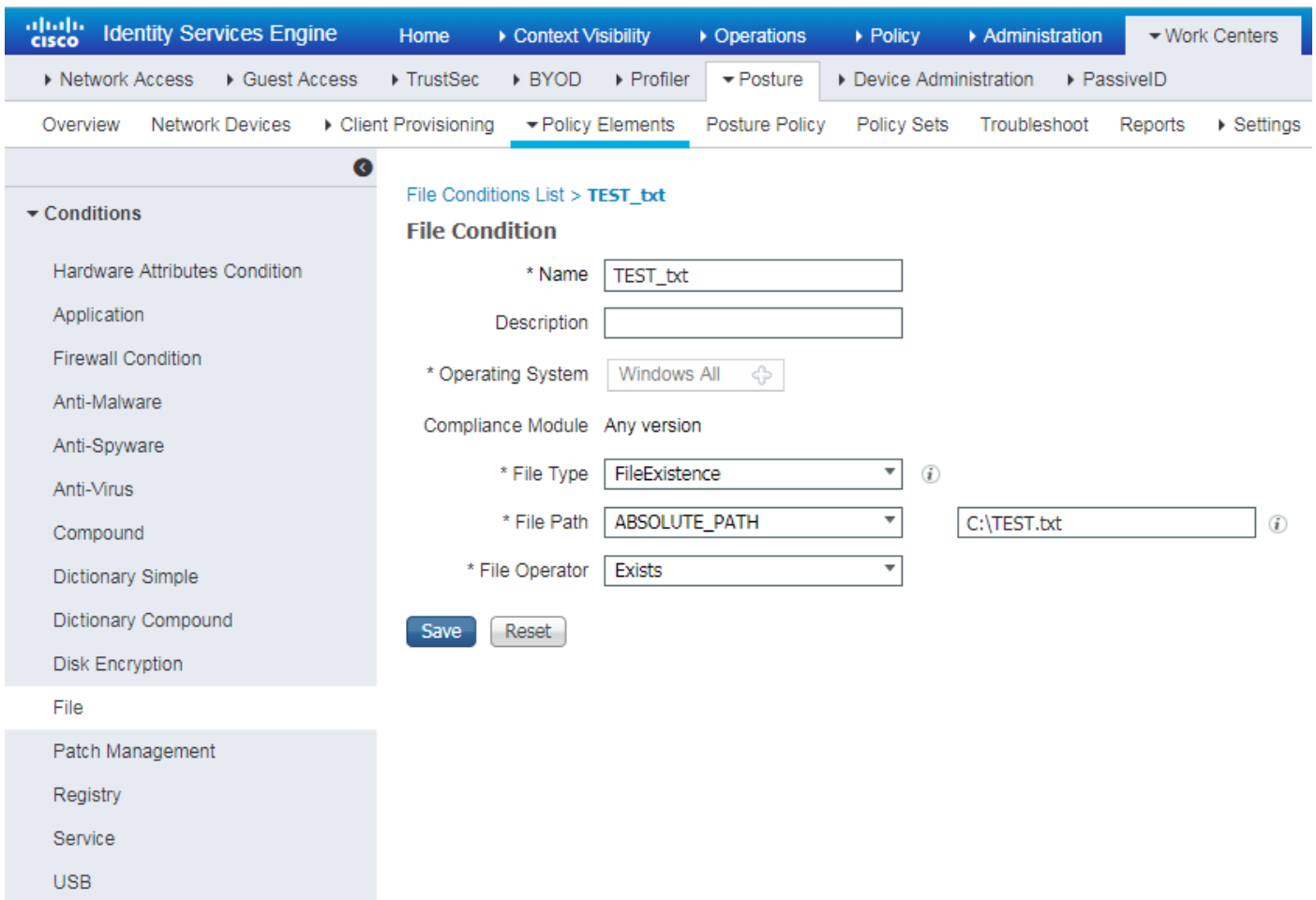
在结果部分选择交流电配置。

## 状态策略和条件

使用简单的状态检查。ISE配置为检查终端设备端是否有文件C:\TEST.txt。现实场景可能更加复杂，但一般配置步骤相同。

步骤1.创建状态条件。状态条件位于**工作中心 —>状态 —>策略元素 —>条件**。选择状态条件的类型，然后单击**Add**。指定必要信息，然后单击**保存**。在下面，您可以找到服务条件示例，该示例应检查文件C:\TEST.txt是否存在。



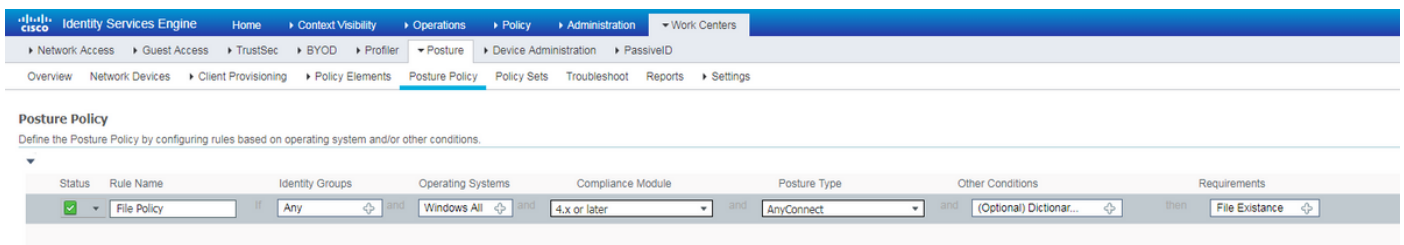


步骤2.状态要求配置。导航至工作中心 —>状态 —>策略元素 —>要求。以下是文件TEST.txt的示例：



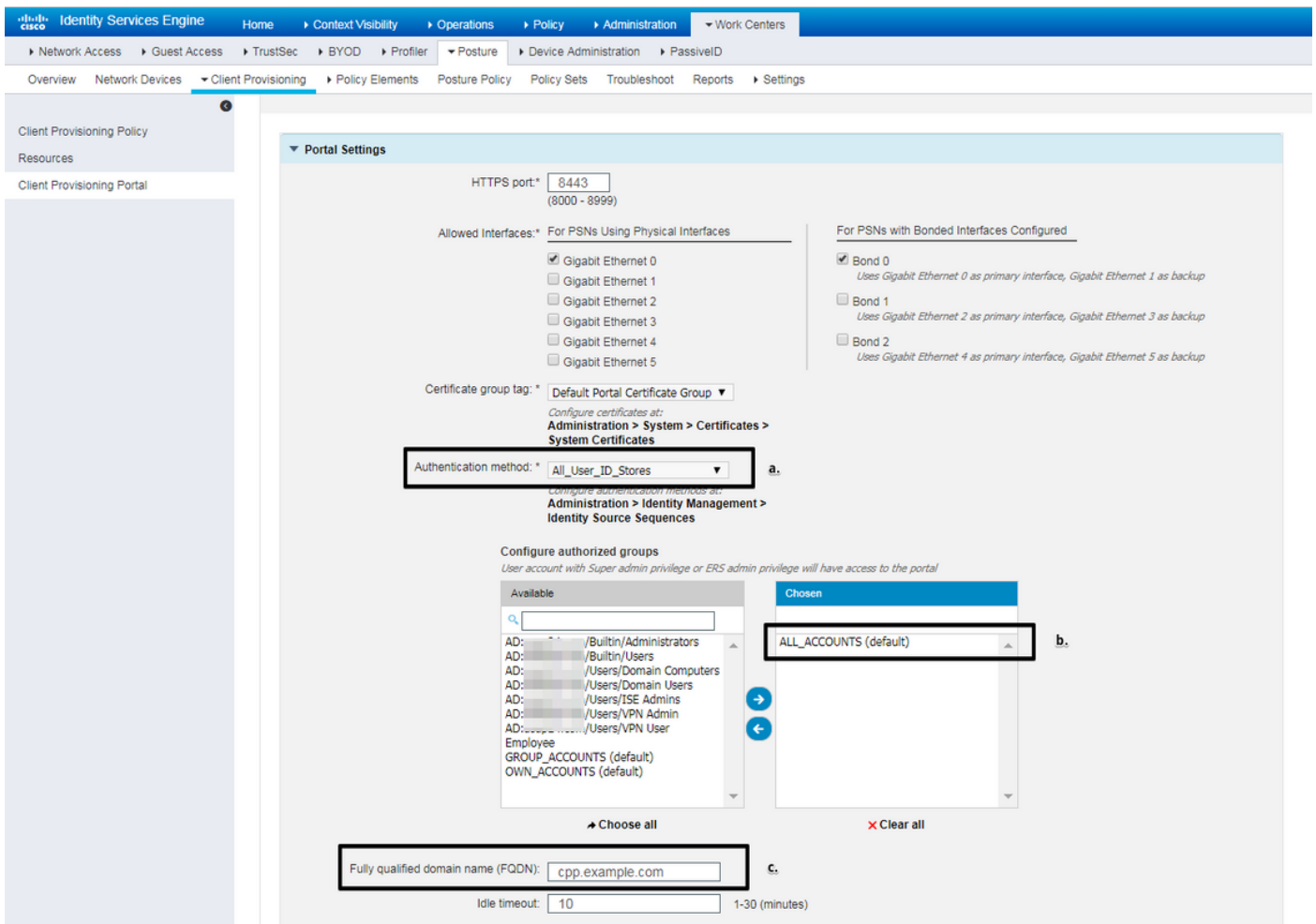
在新要求中选择您的状态条件并指定补救操作。

步骤3.状态策略配置。导航至工作中心 —>状态 —>状态策略。在下面，您可以找到用于本文档的策略示例。策略将“文件存在”要求指定为必填项，且未分配任何其他条件。



## 配置客户端调配门户

对于无重定向的状态，必须编辑客户端调配门户的配置。导航到工作中心 —>状态 —>客户端调配 ->客户端调配门户。您可以使用默认门户或创建自己的门户。



这些设置应在非重定向场景的门户配置中编辑：

- 在身份验证中，指定SSO找不到用户会话时应使用的身份源序列。
- 根据所选的可用组身份源序列列表填充。此时，您需要选择有权登录门户的组。
- 必须指定客户端调配门户的FQDN。此FQDN应可解析为ISE PSN IP。应指示用户在首次尝试连接时在Web浏览器中指定FQDN。

## 配置授权配置文件和策略

当状态不可用时，需要限制客户端的初始访问。这可以通过多种方式实现：

- Radius Filter-Id — 使用此属性，可以将将在NAD上本地定义的ACL分配给状态未知的用户。由于这是标准RFC属性，因此此方法应适用于所有NAD供应商。
- 思科：cisco-av-pair = ip:interface-config — 非常类似于RADIUS过滤器ID，可以将将在NAD上本地定义的ACL分配给状态未知的用户。配置示例：  
cisco-av-pair = ip:interface-config=ip access-group DENY\_SERVER in

步骤1.配置授权配置文件。

与往常一样，安全评估需要两个授权配置文件。首先应包含任何类型的网络访问限制。此配置文件可应用于状态不等于合规的身份验证。第二个授权配置文件可能仅包含允许访问，并且可应用于状态等于兼容的会话。

要创建授权配置文件，请导航至“工作中心”(Work Centers)->“状态”(Posture)->“策略元素”(Policy Elements)->“授权配置文件”(Authorization Profiles)。

使用Radius Filter-Id的受限访问配置文件示例：

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Posture > Policy Elements > Authorization Profiles > LIMITED\_ACCESS. The main configuration area is titled "Authorization Profile" and includes the following fields:

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

Below the main configuration, there are three sections:

- Common Tasks:** Includes checkboxes for DACL Name, ACL (Filter-ID) (checked), Security Group, and VLAN. The ACL (Filter-ID) field is set to DENY\_SERVER.in.
- Advanced Attributes Settings:** A rule editor showing "Select an item" followed by an equals sign and another "Select an item" dropdown, with a plus sign to the right.
- Attributes Details:** A summary box showing "Access Type = ACCESS\_ACCEPT" and "Filter-ID = DENY\_SERVER.in".

使用cisco-av-pair的受限访问配置文件示例：

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: [Text Field]

\* 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

使用Radius Filter-Id的无限访问配置文件示例：

**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

**UNLIMITED\_ACCESS**

Description

\* 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

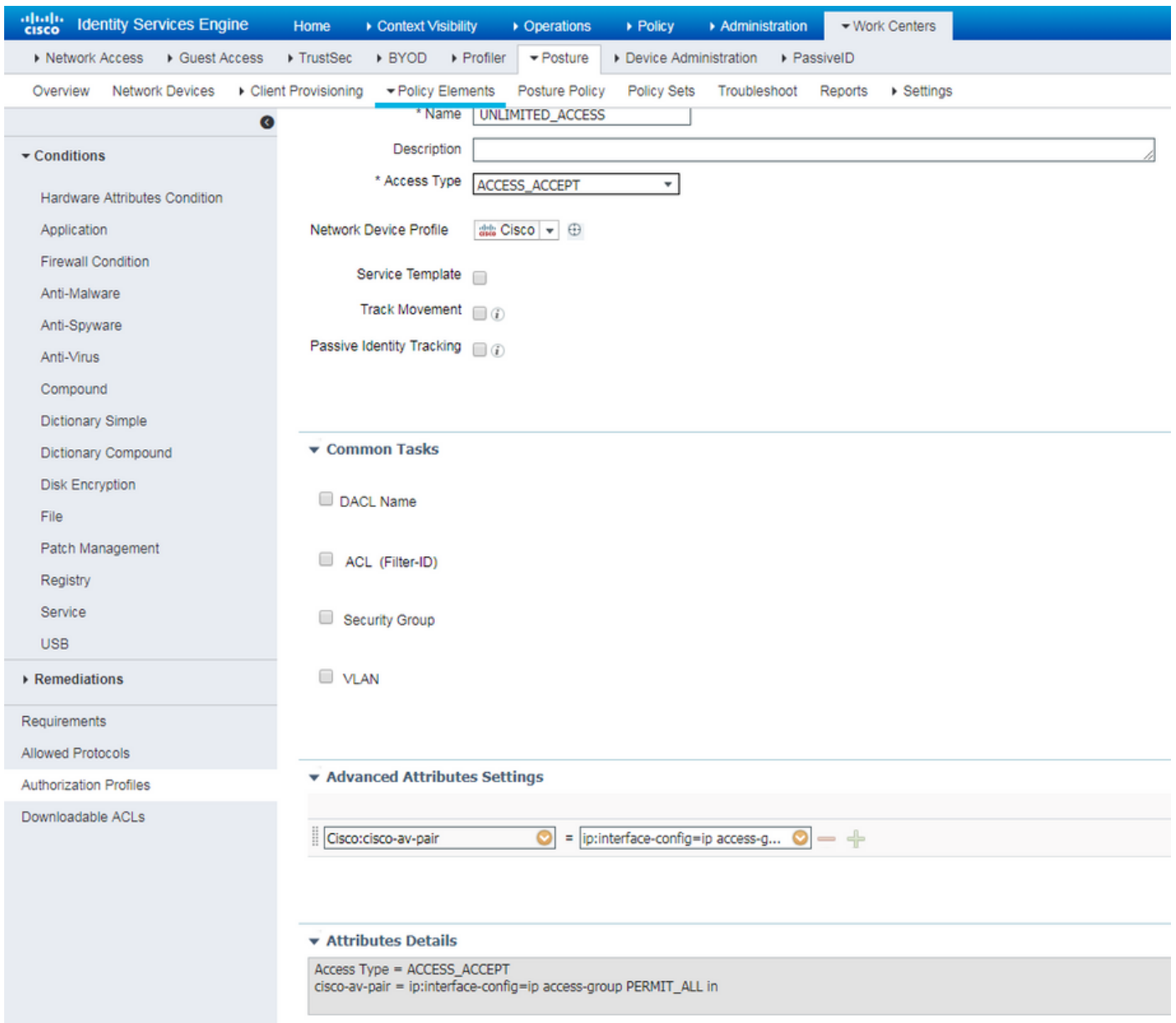
**Advanced Attributes Settings**

Select an item =

**Attributes Details**

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

使用cisco-av-pair的无限访问配置文件示例：



步骤2.配置授权策略。在此步骤中，应创建两个授权策略。一个用于将初始身份验证请求与未知状态进行匹配，另一个用于在安全评估进程成功后分配完全访问权限。

本例中提供了简单授权策略的示例：

Authorization Policy (12)				Results		Hits	Actions
Status	Rule Name	Conditions	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	⚙️	

身份验证策略的配置不是本文档的一部分，但您应记住，身份验证需要在授权策略处理开始之前成功。

## 验证

流的基本验证可能包括三个主要步骤：

## 步骤1.在FlexVPN集线器上验证RA VPN会话：

### 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

## 步骤2.身份验证流验证 ( Radius实时日志 )：

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	Posture Status	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
2. Jun 07, 2018 07:39:59.345 PM	●		vpnuser	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	✓		vpnuser	NoApplicable	7.7.7.7	Default >> Default	Default >> Unknown_Compliance	LIMITED_ACCESS	

1. 初始身份验证。对于此步骤，您可能希望验证已应用的授权配置文件。如果应用了意外的授权



配置文件，请调查详细的身份验证报告。单击“详细信息”列中的放大镜可打开此报告。您可以将详细身份验证报告中的属性与授权策略中希望匹配的条件进行比较。

2. 会话数据更改，在此特定示例中，会话状态已从NotAppliable更改为Compliant。

3. COA到网络访问设备。此COA应能成功推送来自NAD端的新身份验证和ISE端的新授权策略分配。如果COA失败，您可以打开详细报告以调查原因。COA的最常见问题可能是：COA超时—在这种情况下，已发送请求的PSN未配置为NAD端的COA客户端，或者COA请求在途中的某处被丢弃。COA否定确认—表示NAD已收到COA，但由于某些原因，无法确认COA操作。对于此场景，详细报告应包含更详细的说明。

由于基于IOS XE的路由器已用作本例的NAD，因此您看不到用户的后续身份验证请求。这是由于ISE对IOS XE使用COA推送（避免VPN服务中断）。在这种情况下，COA本身包含新的授权参数，因此不需要重新身份验证。

步骤3.状态报告验证 — 导航至操作 —>报告 —>报告 —>终端和用户 —>终端安全评估（按终端）。

Logged At	Status	Details	PRA Action	Identity	Endpoint ID	IP Address
Today				Identity	Endpoint ID	
2018-06-07 19:39:59.345	✓		N/A	vpnuser	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	vpnuser	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	vpnuser	50.00.00.03.00.00	10.20.30.108
2018-06-07 19:17:17.906	✓		N/A	vpnuser	50.00.00.03.00.00	10.20.30.107

您可以从此处打开每个特定事件的详细报告，以检查此报告所属的会话ID、ISE为终端选择的确切状态要求以及每个要求的状态。

## 故障排除

本部分提供了可用于对配置进行故障排除的信息。

1. 要从头端收集的IKEv2调试：

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

2. AAA调试，查看本地和/或远程属性的分配：

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



debug radius accounting

### 3. DART。

4. 对于状态进程故障排除，这些ISE组件必须在可能发生状态进程的ISE节点的调试中启用：  
**client-webapp** — 负责代理调配的组件。目标日志文件**guest.log**和**ise-psc.log**。**guestaccess** — 负责客户端调配门户组件和会话所有者查找的组件（当请求到错误的PSN时）。目标日志文件- **guest.log**。**预配** — 负责客户端预配策略处理的组件。目标日志文件- **guest.log**。**posture** — 所有与状态相关的事件。目标日志文件- **ise-psc.log**
5. 对于客户端故障排除，您可以使用：  
**AnyConnect.txt** — 此文件可在DART套件中找到，用于VPN故障排除。**acisensa.log** -如果客户端上的客户端调配失败，则此文件在NSA下载到的同一文件夹中创建（Windows的下载目录正常），**AnyConnect\_ISEPosture.txt** — 此文件可在Cisco AnyConnect ISE终端安全评估模块目录的**DART套件中找到**。有关ISE PSN发现和安全评估流程的一般步骤的所有信息都记录到此文件中。