使用FlexVPN配置ISE狀態

目錄

簡介

本文檔提供了如何使用AnyConnect IKEv2和EAP-Message Digest 5(EAP-MD5)身份驗證方法為具有安全狀態的遠端訪問配置IOS XE頭端的示例。

必要條件

需求

思科建議您瞭解以下主題：

- IOS XE上的FlexVPN遠端訪問(RA)VPN配置
- AnyConnect(AC)客戶端配置
- 身份服務引擎(ISE)2.2及更高版本上的狀態流
- 在ISE上配置終端安全評估元件
- 在Windows Server 2008 R2上配置DNS伺服器

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行IOS XE 16.8的Cisco CSR1000V [Fuji]
- 在Windows 7上運行的AnyConnect客戶030404.5.1版
- Cisco ISE 2.3
- Windows 2008 R2伺服器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

為確保強制實施的網路安全措施保持相關性和有效性，Cisco ISE使您能夠在訪問受保護網路的任何客戶端電腦上驗證和維護安全功能。通過採用旨在確保客戶端電腦上可用的最新安全設定或應用的安全狀態策略，思科ISE管理員可以確保任何訪問網路的客戶端電腦滿足並繼續滿足企業網路訪問定義的安全標準。狀態合規性報告可在使用者登入時以及定期重新評估發生的任何時間為思科ISE提供客戶端電腦合規性級別的快照。

狀態可以用三個主要元素表示：

1. ISE作為策略配置分發和決策點。從ISE的管理員角度可以配置終端安全評估策略（將裝置標籤為符合公司要求的確切條件）、客戶端調配策略（應在何種型別的裝置上安裝何種代理軟體）和授權策略（應分配何種型別的許可權，取決於其終端安全評估狀態）。

2. 作為策略實施點的網路接入裝置(NAD)。在NAD端在使用者身份驗證時應用實際授許可權制。作為策略點的ISE提供授權引數，如訪問控制清單(ACL)。傳統上，為了實施安全狀態，需要需要NAD支援授權更改(CoA)，以便在終端的狀態確定後重新驗證使用者。從ISE 2.2開始，不需要支援NAD支援重定向。
   附註：運行IOS XE的路由器不支援重定向。**附註**：IOS XE軟體必須具備針對以下缺陷的修復程式，才能使CoA with ISE完全運行：
   CSCve16269 IKEv2 CoA與ISE不相容
   CSCvi90729 IKEv2 CoA不能與ISE一起使用（coa-push=TRUE而不是true）
3. 代理軟體，作為資料收集點並與終端使用者進行互動。代理從ISE接收有關終端安全評估要求的資訊，並向該ISE提供有關要求狀態的報告。本文檔基於Anyconnect ISE終端安全評估模組，該模組是唯一一個完全支援終端安全評估而不重定向的模組。

無重定向的終端安全評估流在「ISE終端安全評估樣式比較前後2.2」一節「ISE終端安全評估流2.2中的終端安全評估流」一節中有很好的記錄。

使用FlexVPN的Anyconnect ISE終端安全評估模組調配可通過兩種不同方式完成：

- 手動 — 通過思科軟體下載門戶上的Anyconnect軟體包，在客戶端工作站上手動安裝模組：https://software.cisco.com/download/home/283000185。
  對於使用手動ISE終端安全評估模組調配的終端安全評估工作，必須滿足以下條件：

  1.域名伺服器(DNS)必須將完全限定域名(FQDN)**enroll.cisco.com**解析為策略服務節點(PSN)IP。在第一次連線嘗試期間，狀態模組不包含有關可用PSN的任何資訊。它正在傳送發現探測以查詢可用的PSN。FQDN enroll.cisco.com用於其中一個探測中。

2. PSN IP必須允許**TCP埠8905**。在此案例中，安全狀態通過TCP埠8905進行。

3. PSN節點上的**Admin certificate**必須在**SAN欄位中具有enroll.cisco.com**。VPN使用者與PSN節點之間通過TCP 8905的連線通過管理員證書受到保護，如果PSN節點的Admin證書中沒有這樣的名稱「enroll.cisco.com」，使用者將獲得證書警告。

附註：根據RFC6125 ，如果指定了SAN值，則應該忽略證書CN。這意味著我們還需要在SAN欄位中新增管理員證書的CN。

- 通過客戶端調配門戶(CPP)自動調配 — 通過直接通過門戶FQDN訪問CPP，從ISE下載並安裝模組。
  必須為使用自動ISE終端安全評估模組調配的終端安全評估工作滿足以下條件：

  1. DNS必須將**CPP的FQDN**解析為策略服務節點(PSN)IP。

  2. PSN **IP必須允許TCP埠80、443和CPP埠**（預設情況下為8443）。客戶端需要直接通過HTTP（將重定向到HTTPS）或HTTPS開啟CPP FQDN，此請求將重定向到CPP埠（預設情況下為8443），然後終端安全評估通過該埠。

  3. PSN節**點上的管**理和CPP證書必須在**SAN字**段中**具有CPP FQDN**。通過TCP 443在VPN使用者和PSN節點之間的連線受Admin證書保護，並且CPP埠上的連線受CPP證書保護。

附註：根據RFC6125 ，如果指定了SAN值，則應該忽略證書CN。這意味著我們還需要在相應證書的SAN欄位中新增管理員證書和CPP證書的CN。

附註：如果ISE軟體不包含CSCvj76466的修復程式，則僅當安全或客戶端調配在客戶端通過身份驗證的相同PSN上完成時，安全或客戶端調配才能生效。

在使用FlexVPN的安全狀況時，流程包括以下步驟：

1.使用者使用Anyconnect客戶端連線到FlexVPN中心。

2. ISE向FlexVPN中心傳送訪問接受，需要應用ACL名稱來限制訪問。

3a。使用手動調配的第一個連線 — ISE狀態模組開始發現策略伺服器，通過TCP埠8905將探測傳送到enroll.cisco.com。作為成功的結果，終端安全評估模組下載已配置的終端安全評估配置檔案並更新客戶端上的合規性模組。

在下一次連線嘗試期間，ISE終端安全評估模組還將使用終端安全評估配置檔案的Call Home清單中指定的名稱和IP進行策略伺服器檢測。

3b。與自動預配的第一個連線 — 客戶端通過FQDN開啟CPP。成功的結果是在客戶端的工作站上下載網路設定助手，然後下載並安裝ISE終端安全評估模組、ISE合規性模組和終端安全評估配置檔案。

在下一次連線嘗試期間，ISE終端安全評估模組將使用終端安全評估配置檔案的Call Home清單中指定的名稱和IP進行策略伺服器檢測。

4.安全評估模組啟動合規性檢查並將檢查結果傳送到ISE。

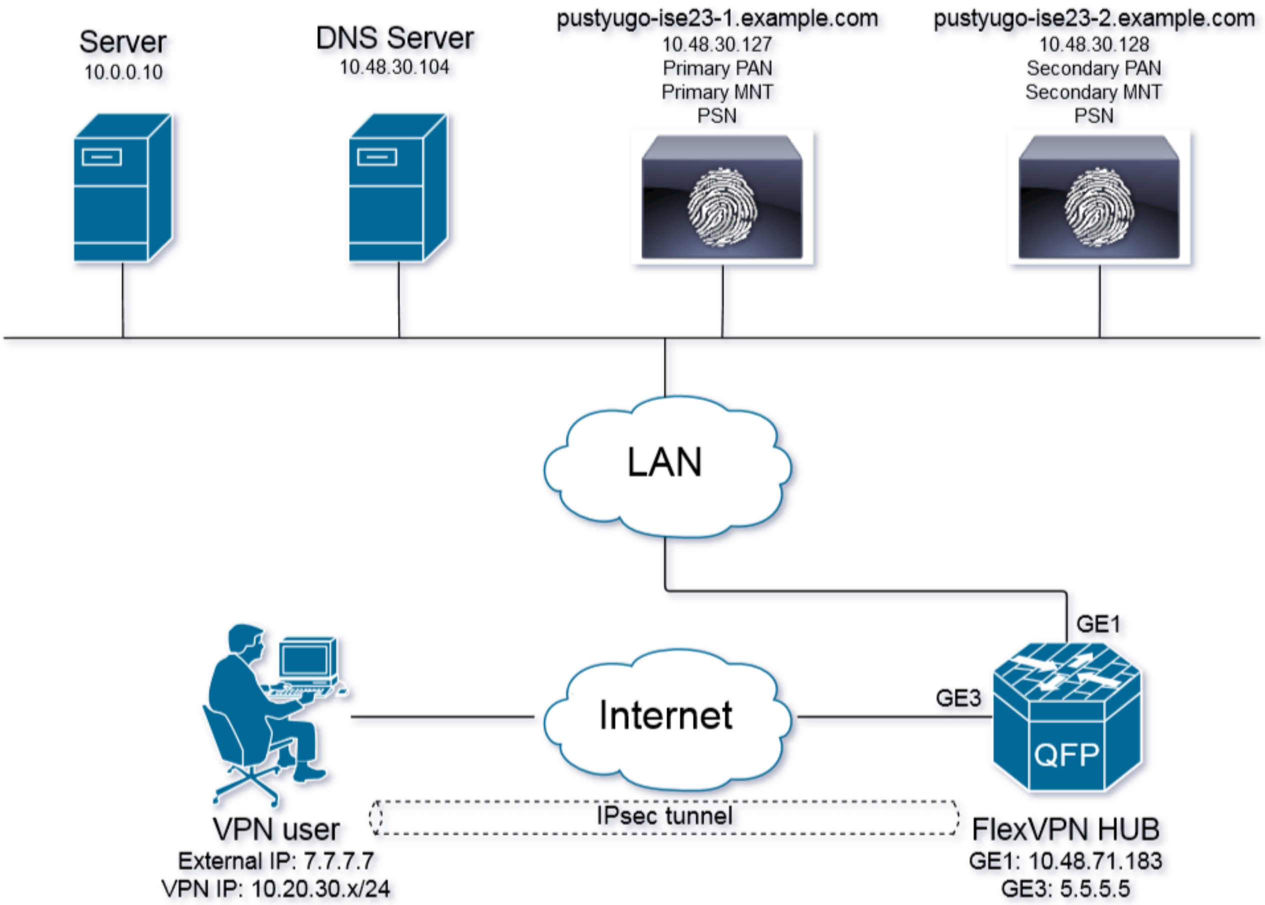
5.如果客戶端的狀態為「相容」，則ISE會向FlexVPN中心傳送訪問接受，且需要將ACL名稱應用於相容客戶端。

6，客戶端訪問網路。

有關終端安全評估流程的更多詳細資訊，請參閱文檔「ISE終端安全評估樣式比較前後2.2」。

設定

網路圖表

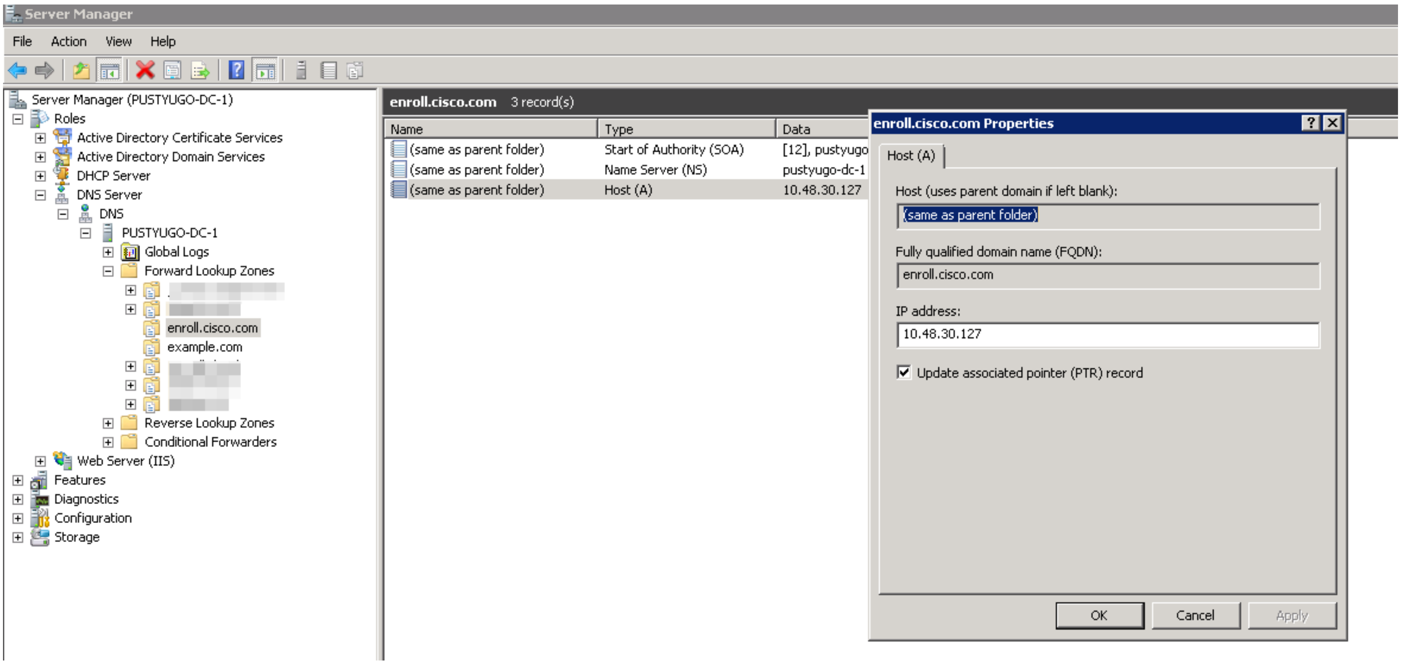


VPN使用者只有在符合狀態時才可訪問伺服器(10.0.0.10)。

DNS伺服器配置

在本文檔中，Windows Server 2008 R2用作DNS伺服器。

步驟1.為**enroll.cisco.com新增**指向PSN的IP的**主機(A)記錄**:



Server Manager (PUSTYUGO-DC-1)
- Roles
  - Active Directory Certificate Services
  - Active Directory Domain Services
  - DHCP Server
  - DNS Server
    - DNS
      - PUSTYUGO-DC-1
        - Global Logs
        - Forward Lookup Zones
          - [redacted]
          - [redacted]
          - enroll.cisco.com
          - example.com
          - [redacted]
        - Reverse Lookup Zones
        - Conditional Forwarders
  - Web Server (IIS)
- Features
- Diagnostics
- Configuration
- Storage

enroll.cisco.com 3 record(s)

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[12], pustyugo
(same as parent folder)	Name Server (NS)	pustyugo-dc-1
(same as parent folder)	Host (A)	10.48.30.127

enroll.cisco.com Properties

Host (A)

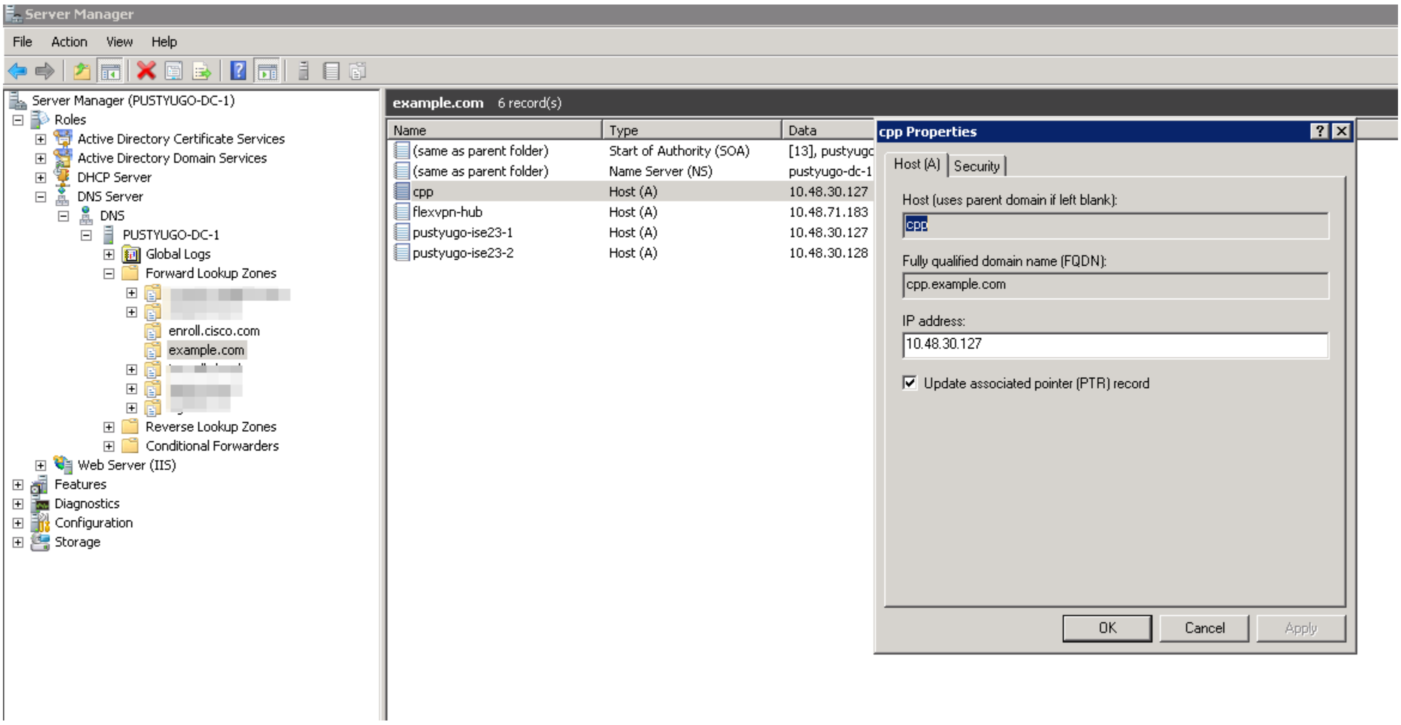
Host (uses parent domain if left blank): (same as parent folder)

Fully qualified domain name (FQDN): enroll.cisco.com

IP address: 10.48.30.127

☑ Update associated pointer (PTR) record

步驟2.為CPP FQDN(本示例中使用的**cpp.example.com)新增主機**(A)記錄，指向**PSN的IP**:



Server Manager (PUSTYUGO-DC-1)
- Roles
  - Active Directory Certificate Services
  - Active Directory Domain Services
  - DHCP Server
  - DNS Server
    - DNS
      - PUSTYUGO-DC-1
        - Global Logs
        - Forward Lookup Zones
          - [redacted]
          - enroll.cisco.com
          - example.com
          - [redacted]
        - Reverse Lookup Zones
        - Conditional Forwarders
  - Web Server (IIS)
- Features
- Diagnostics
- Configuration
- Storage

example.com 6 record(s)

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[13], pustyugc
(same as parent folder)	Name Server (NS)	pustyugo-dc-1
cpp	Host (A)	10.48.30.127
flexvpn-hub	Host (A)	10.48.71.183
pustyugo-ise23-1	Host (A)	10.48.30.127
pustyugo-ise23-2	Host (A)	10.48.30.128

cpp Properties

Host (A) Security

Host (uses parent domain if left blank): cpp

Fully qualified domain name (FQDN): cpp.example.com

IP address: 10.48.30.127

☑ Update associated pointer (PTR) record

IOS XE初始配置

配置身份證書

路由器將使用證書來向Anyconnect客戶端進行身份驗證。路由器證書應由使用者的作業系統信任，以避免連線建立階段出現證書警告。

可以通過以下方式之一提供身份證書：

> **附註**：IKEv2 FlexVPN不支援使用自簽名證書。

選項1 — 在路由器上配置證書頒發機構(CA)伺服器

附註：可以在同一IOS路由器或其他路由器上建立CA伺服器。在本文中，CA是在同一路由器上建立的。

附註：您需要先將時間與NTP伺服器同步，然後才能啟用CA伺服器。

附註：請注意，使用者將無法驗證此證書的真實性，因此除非在建立連線之前手動驗證CA證書並將其匯入使用者電腦，否則使用者資料不會受到中間人攻擊。

步驟1.為CA伺服器生成RSA金鑰：

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

步驟2.生成身份證書的RSA金鑰：

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

驗證：

```
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
------
```

步驟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
```

驗證：

```
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
```

步驟4.配置信任點：

```
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
```

步驟5.驗證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.
```

步驟6.將路由器註冊到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' commandwill 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
```

檢查CA上掛起的證書請求並驗證指紋是否匹配：

```
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
```

步驟7.使用正確的ReqID授予證書：

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

等到路由器再次請求證書（根據此配置，它每分鐘檢查一次10次）。 查詢系統日誌消息：

```
May 21 16:18:56.375: %PKI-6-CERTRET: Certificate received from Certificate Authority
```

驗證是否已安裝憑證：

```
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
```

選項2 — 匯入外部簽名的證書

```
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

步驟1.配置RADIUS伺服器和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
```

步驟2.配置身份驗證和授權清單：

```
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
```

步驟3.建立ikev2授權策略：

```
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
```

步驟4.建立IKEv2配置檔案：

```
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
```

步驟5.建立轉換集和ipsec配置檔案：

```
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
```

步驟6.建立虛擬模板介面：

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

步驟7.建立本地池：

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

步驟8.建立ACL以限制不合規客戶端的訪問。在未知狀態期間，至少應提供這些許可權：

- DNS流量
- 通過埠80、443和8905到ISE PSN的流量
- CPP門戶FQDN指向的ISE PSN流量
- 必要時流向補救伺服器的流量

以下是沒有修正伺服器的ACL範例，為便於檢視而新增10.0.0.0/24網路的顯式deny，ACL結尾有隱含的「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
```

步驟9.建立ACL以允許相容客戶端訪問：

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

步驟10.拆分隧道配置（可選）

預設情況下，所有流量都將通過VPN進行定向。為了僅將流量通道化到指定的網路，您可以在ikev2授權策略部分指定這些流量。可以新增多個語句或使用標準訪問清單。

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

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

步驟11.遠端客戶端的網際網路訪問（可選）

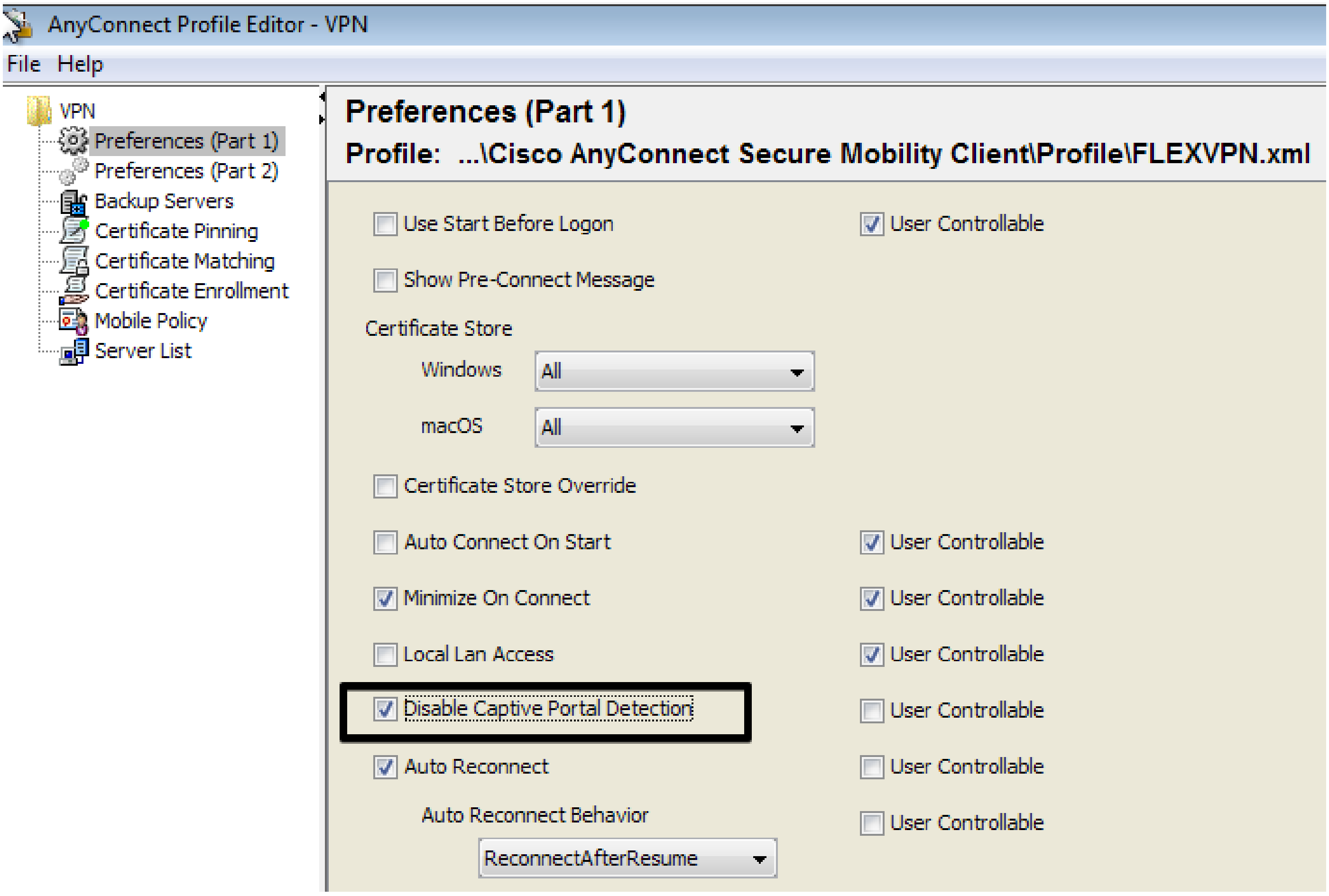
要使從遠端訪問客戶端到網際網路中主機的出站連線通過NAT連線到路由器的全域性IP地址，請配置NAT轉換：

```
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客戶端配置檔案配置

使用AnyConnect配置檔案編輯器配置客戶端配置檔案。Windows 7和10上的Anyconnect安全移動客戶端的配置檔案儲存在**%ProgramData%\Cisco\Cisco AnyConnect安全移動客戶端\Profile**中。

步驟1.禁用強制網路門戶檢測功能。如果未在FlexVPN中心上禁用http伺服器，則AnyConnect強制網路門戶檢測功能將導致連線失敗。請注意，沒有HTTP伺服器，CA伺服器將無法工作。



Preferences (Part 1)

Profile: ...\Cisco AnyConnect Secure Mobility Client\Profile\FLEXVPN.xml

☐ Use Start Before Logon ☑ User Controllable

☐ Show Pre-Connect Message

Certificate Store

Windows: All

macOS: All

☐ Certificate Store Override

☐ Auto Connect On Start ☑ User Controllable

☑ Minimize On Connect ☑ User Controllable

☐ Local Lan Access ☑ User Controllable

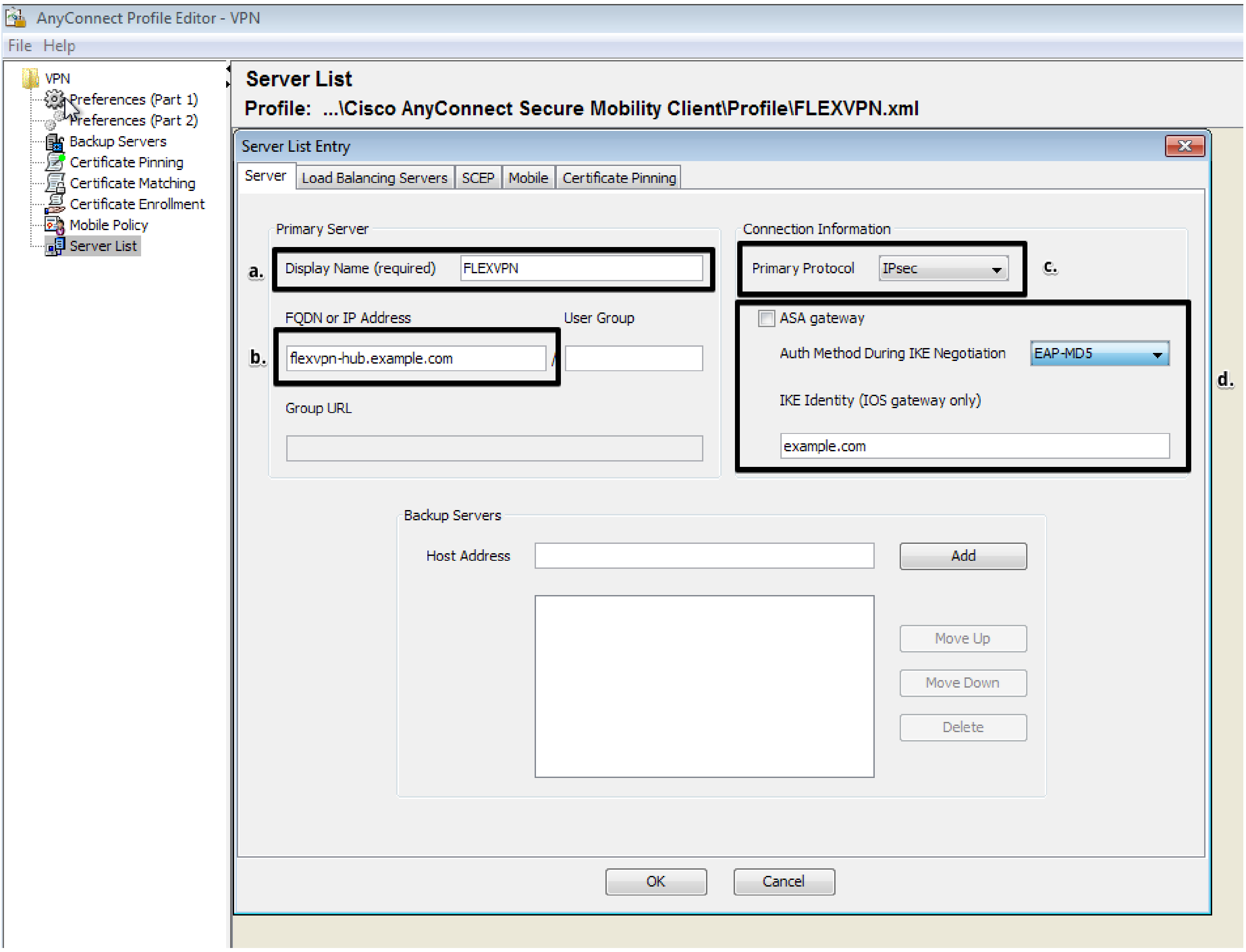
☑ Disable Captive Portal Detection ☐ User Controllable

☑ Auto Reconnect ☐ User Controllable

Auto Reconnect Behavior ☐ User Controllable

ReconnectAfterResume

步驟2.配置伺服器清單：



Server List

Profile: ...\Cisco AnyConnect Secure Mobility Client\Profile\FLEXVPN.xml

Display Name (required) FLEXVPN

FQDN or IP Address flexvpn-hub.example.com

Primary Protocol IPsec

☐ ASA gateway

Auth Method During IKE Negotiation EAP-MD5

IKE Identity (IOS gateway only) example.com

- 輸入顯示名稱。
- 輸入FlexVPN中心的**FQDN或IP**地址。
- 選擇**IPsec**作為主協定。
- 取消選中「ASA網關」覈取方塊，並指定**EAP-MD5作為**身份驗證方法。輸入IKE身份與FlexVPN中心上的IKEv2配置檔案配置完全相同(在本示例中，IKEv2配置檔案是使用「match identity remote key-id example.com」命令配置的，因此我們需要將**example.com**用作IKE身份)。

步驟3.將配置檔案儲存到**%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile**，然後重新啟動AC。

配置檔案的XML等效項：

```
<?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>
```

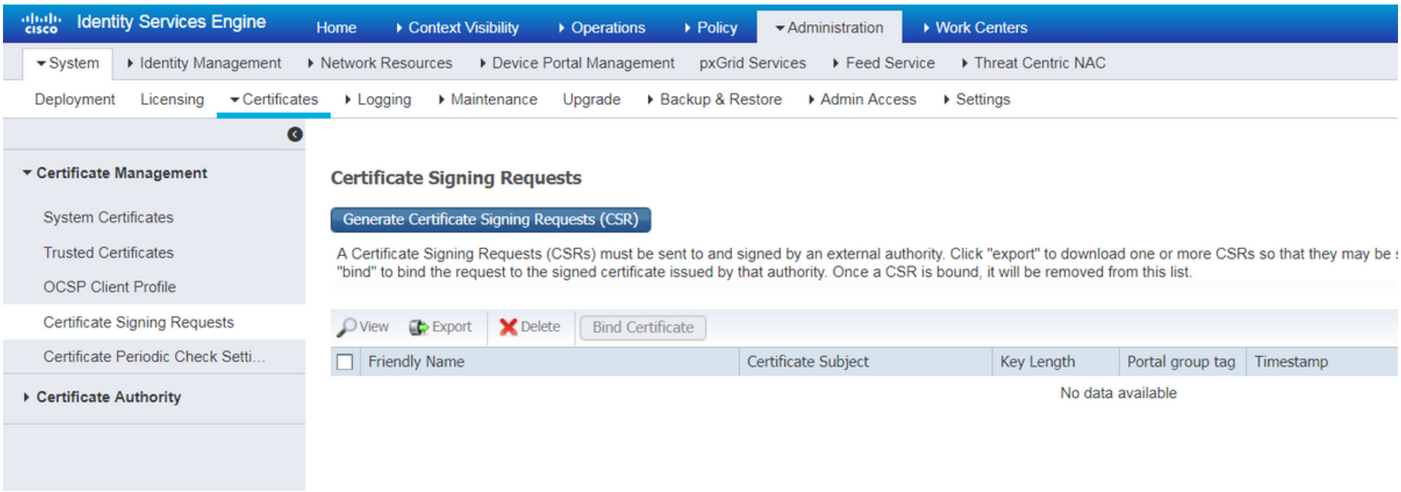
```
        <CertificateStoreOverride>false</CertificateStoreOverride>
        <ProxySettings>Native</ProxySettings>
        <AllowLocalProxyConnections>false</AllowLocalProxyConnections>
        <AuthenticationTimeout>12</AuthenticationTimeout>
        <AutoConnectOnStart UserControllable="true">false</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>
        <PPPExclusion UserControllable="false">Automatic
            <PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
        </PPPExclusion>
        <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 組態

管理員和CPP證書配置

附註：更改管理員證書將重新啟動已更改證書的節點。

步驟1。前往**管理 — >系統 — >憑證 — >憑證簽署請求**，按一下**Generate Certificate Signing Requests(CSR):**



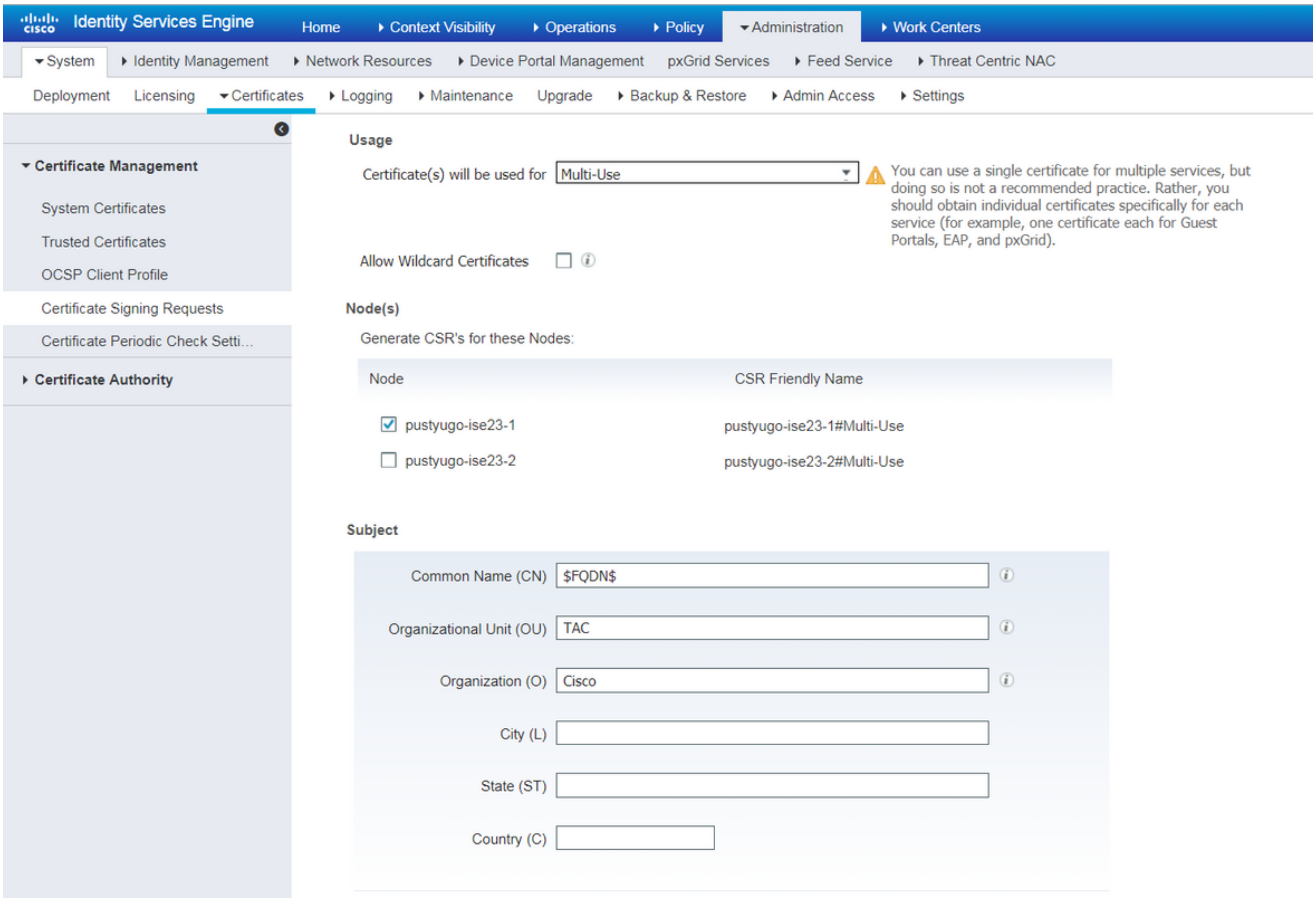
Certificate Signing Requests

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 s "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.

□ Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp
No data available				

步驟2.在開啟的頁面上，選擇必要的PSN節點，填寫必要的欄位，並在SAN欄位中新增節點的FQDN、enroll.cisco.com、cpp.example.com和IP地址，然後按一下**Generate**:



Usage

Certificate(s) will be used for: Multi-Use

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 □

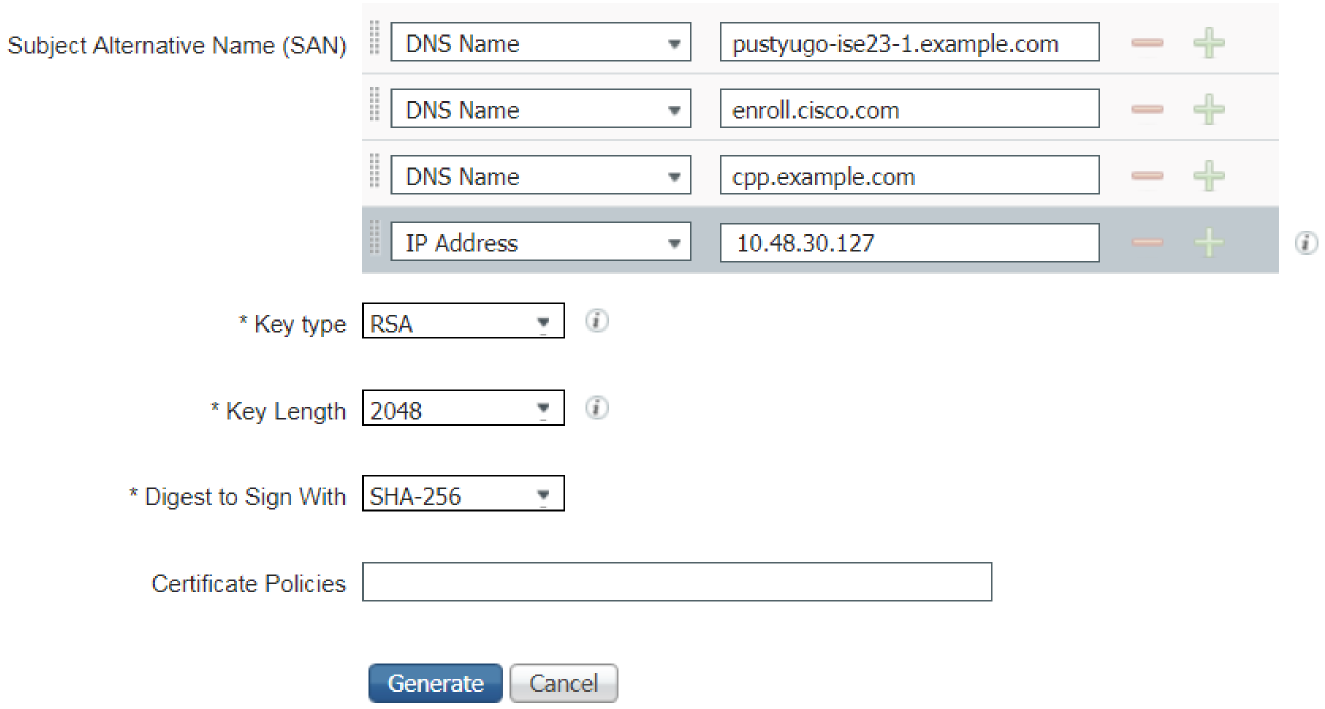
Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ pustyugo-ise23-1	pustyugo-ise23-1#Multi-Use
□ pustyugo-ise23-2	pustyugo-ise23-2#Multi-Use

Subject

Common Name (CN)	$FQDN$
Organizational Unit (OU)	TAC
Organization (O)	Cisco
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: RSA

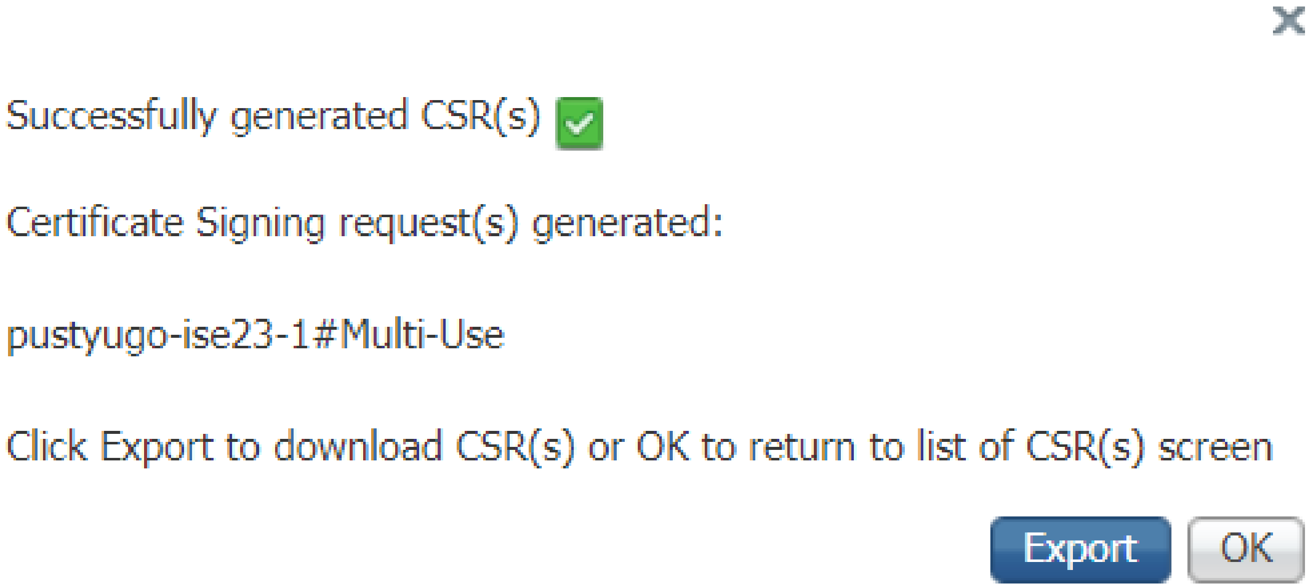
* Key Length: 2048

* Digest to Sign With: SHA-256

Certificate Policies:

附註：如果在此步驟中選擇**Multi-Use**，則您也可以將同一證書用於Portal。

在出現的視窗中，按一下**Export**，將CSR以pem格式儲存到本地工作站：



Successfully generated CSR(s) ✓

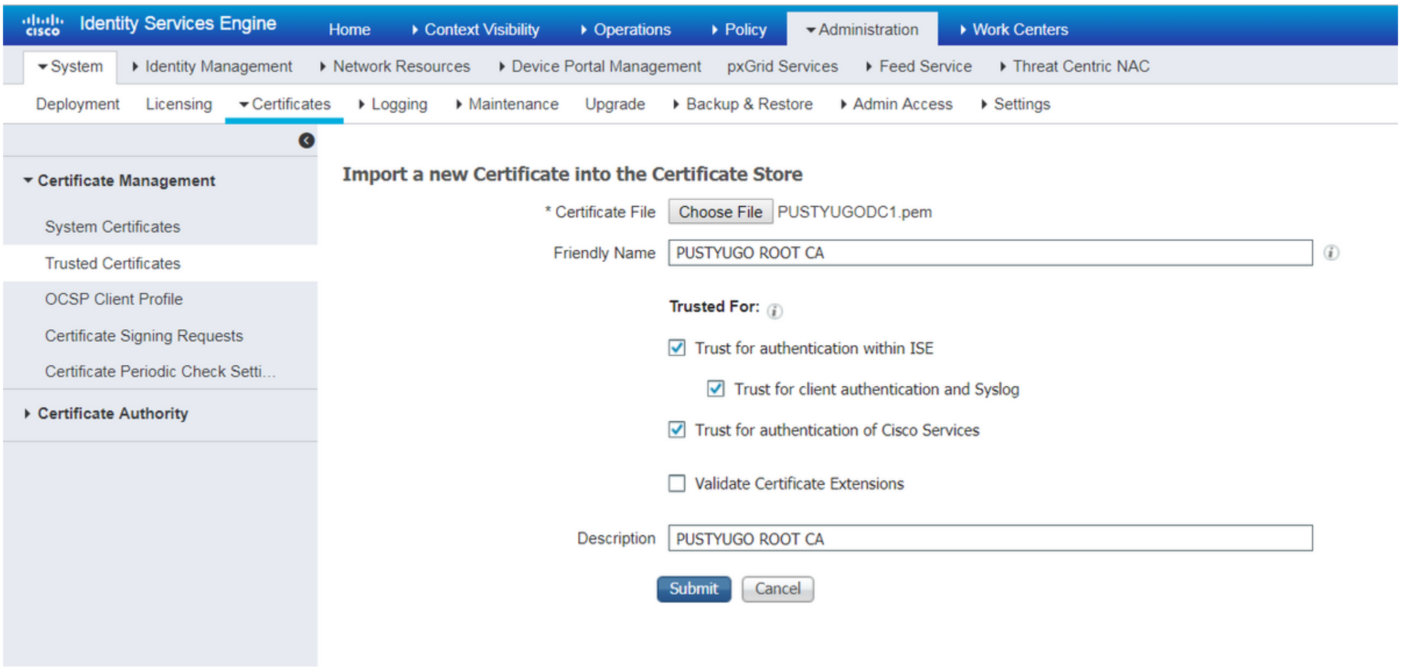
Certificate Signing request(s) generated:

pustyugo-ise23-1#Multi-Use

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

步驟3.使用具有受信任CA的CSR，並從CA以及完整CA憑證鏈結（根和中間）取得憑證檔案。

步驟4.轉至**Administration -> System -> Certificates -> Trusted Certificates**，然後點選**Import。在下一個螢幕上，按一下Choose file**，然後選擇**Root CA** certificate file，根據需要填寫Friendly name和Description，選擇必要的**Trusted For**選項，然後按一下**Submit:**



Import a new Certificate into the Certificate Store

* Certificate File: PUSTYUGODC1.pem

Friendly Name: PUSTYUGO ROOT CA

Trusted For:

☑ Trust for authentication within ISE

☑ Trust for client authentication and Syslog

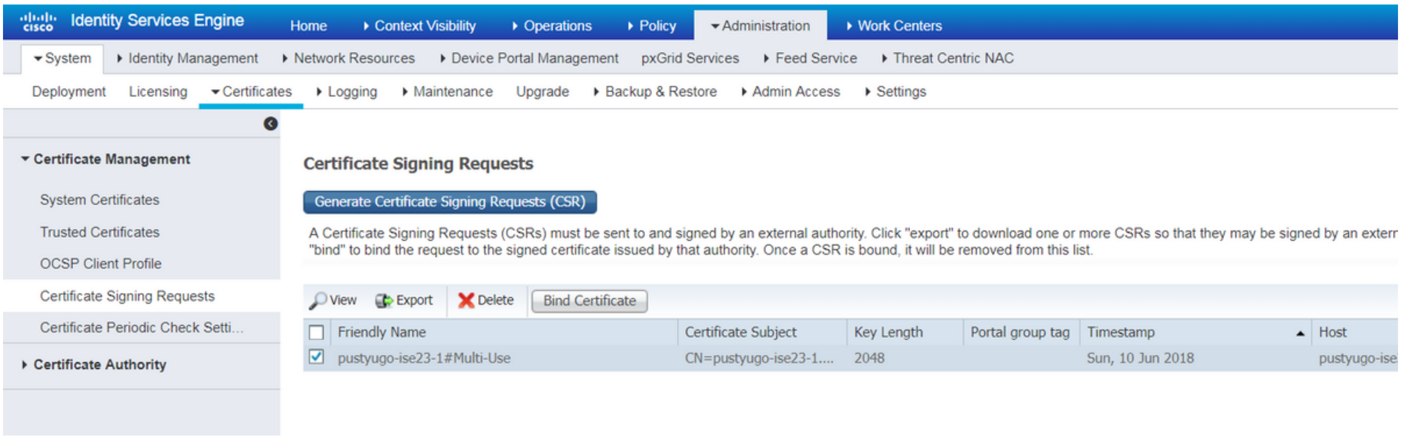
☑ Trust for authentication of Cisco Services

□ Validate Certificate Extensions

Description: PUSTYUGO ROOT CA

對鏈中的所有中間憑證（如果有）重複此步驟。

步驟5.返回**Administration -> System -> Certificates -> Certificate Signing Requests，選擇必要的CSR**，然後點選**Bind Certificate:**

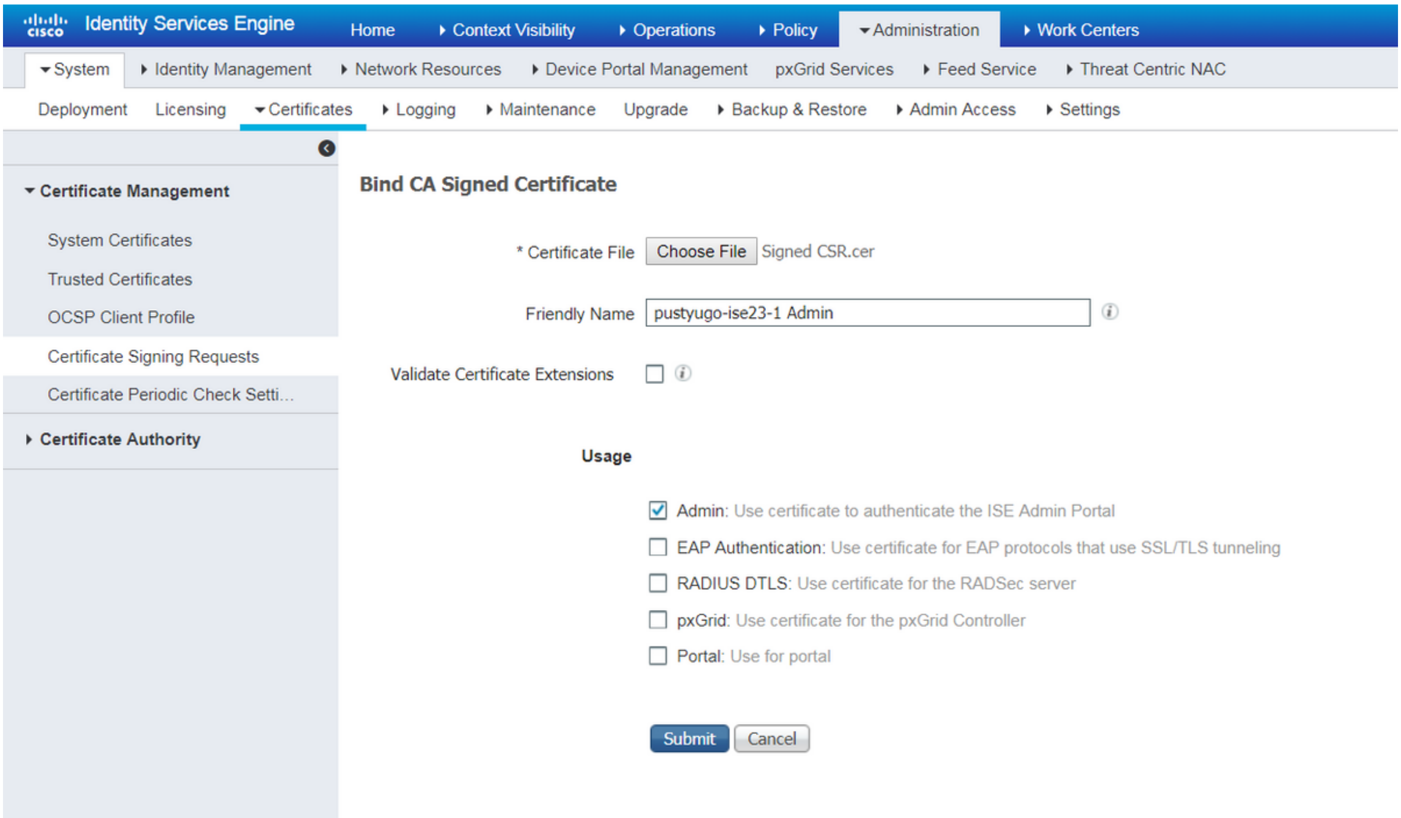


Certificate Signing Requests

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 signed by an exterr "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.

□	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

步驟6.在開啟的頁面上，按一下**選擇檔案**，選擇從CA接收的證書檔案，然後根據需要輸入友好名稱，然後選擇**用法：Admin (用法：如果**CSR是使用「**Multi-Use**（多用途）」建立的，則也**可以在此處選**擇入口網站，然**後點選Submit**:



Bind CA Signed Certificate

* Certificate File Choose File Signed CSR.cer

Friendly Name pustyugo-ise23-1 Admin

Validate Certificate Extensions □

Usage

☑ Admin: Use certificate to authenticate the ISE Admin Portal

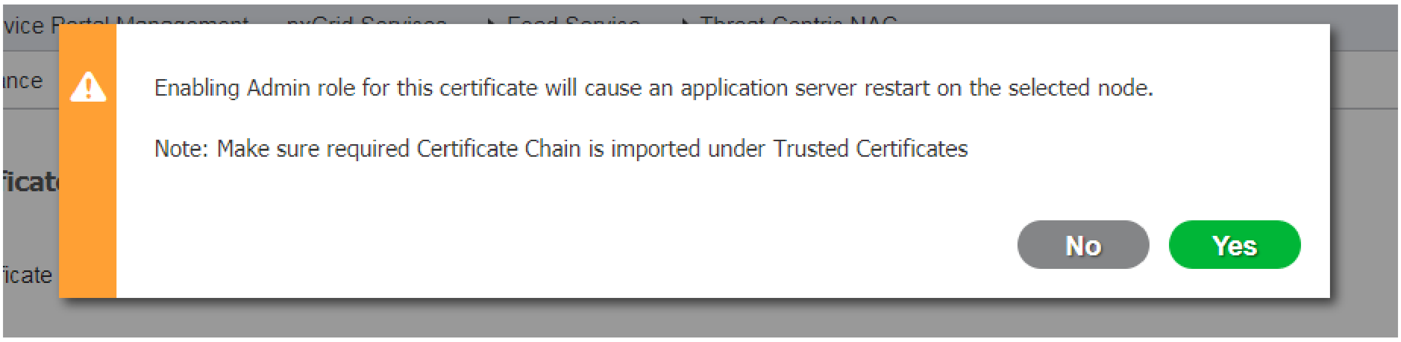
□ EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling

□ RADIUS DTLS: Use certificate for the RADSec server

□ pxGrid: Use certificate for the pxGrid Controller

□ Portal: Use for portal

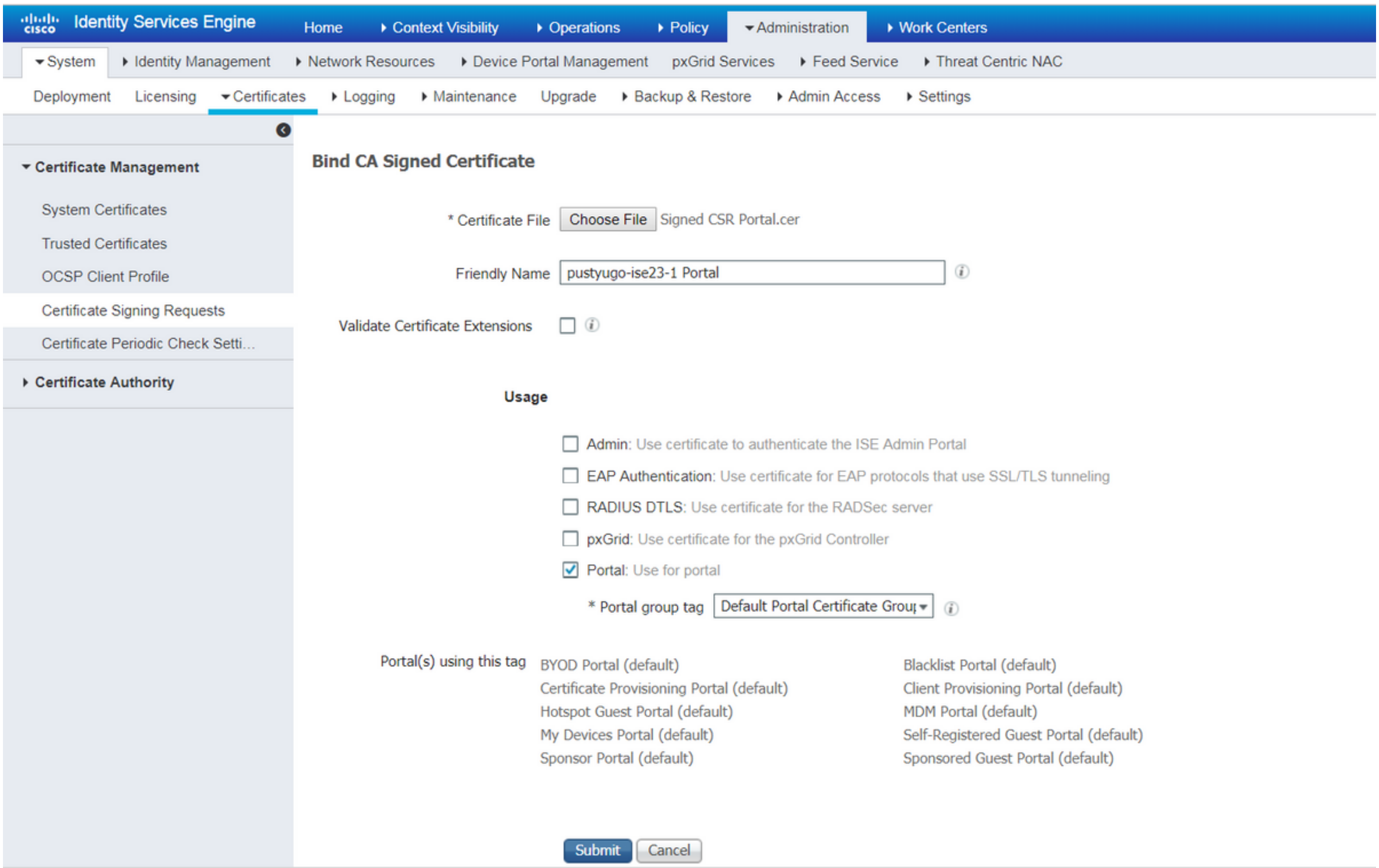
步驟7.在警告彈出視窗中，按一下**Yes**完成匯入。將重新啟動受管理員證書更改影響的節點：


vice Portal Management pxGrid Services Feed Service Threat Centric NAC
nce
ficat
ficate
No
Yes

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

如果您決定對門戶使用單獨的證書，請重複更改CPP證書的步驟。在第6步中選擇**Usage:輸入門**戶並點選**提交**：



Bind CA Signed Certificate

* Certificate File: Choose File Signed CSR Portal.cer

Friendly Name: pustyugo-ise23-1 Portal

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: Default Portal Certificate Grou

Portal(s) using this tag:
BYOD Portal (default)
Certificate Provisioning Portal (default)
Hotspot Guest Portal (default)
My Devices Portal (default)
Sponsor Portal (default)
Blacklist Portal (default)
Client Provisioning Portal (default)
MDM Portal (default)
Self-Registered Guest Portal (default)
Sponsored Guest Portal (default)

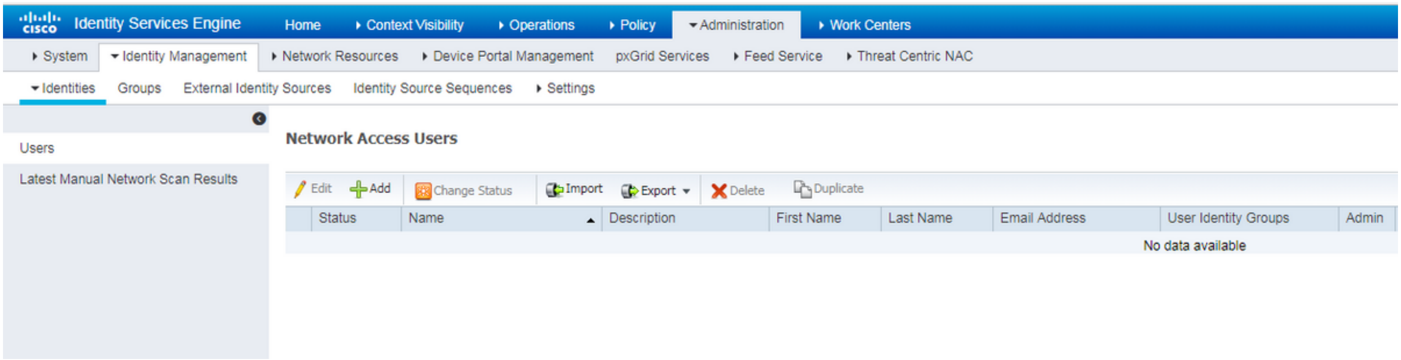
Submit Cancel

對ISE部署中的所有PSN重複這些步驟。

在ISE上建立本地使用者

附註：通過EAP-MD5方法，ISE僅支援本地使用者。

步驟1.轉至**Administration -> Identity Management -> Identities -> Users**，點選**Add**。

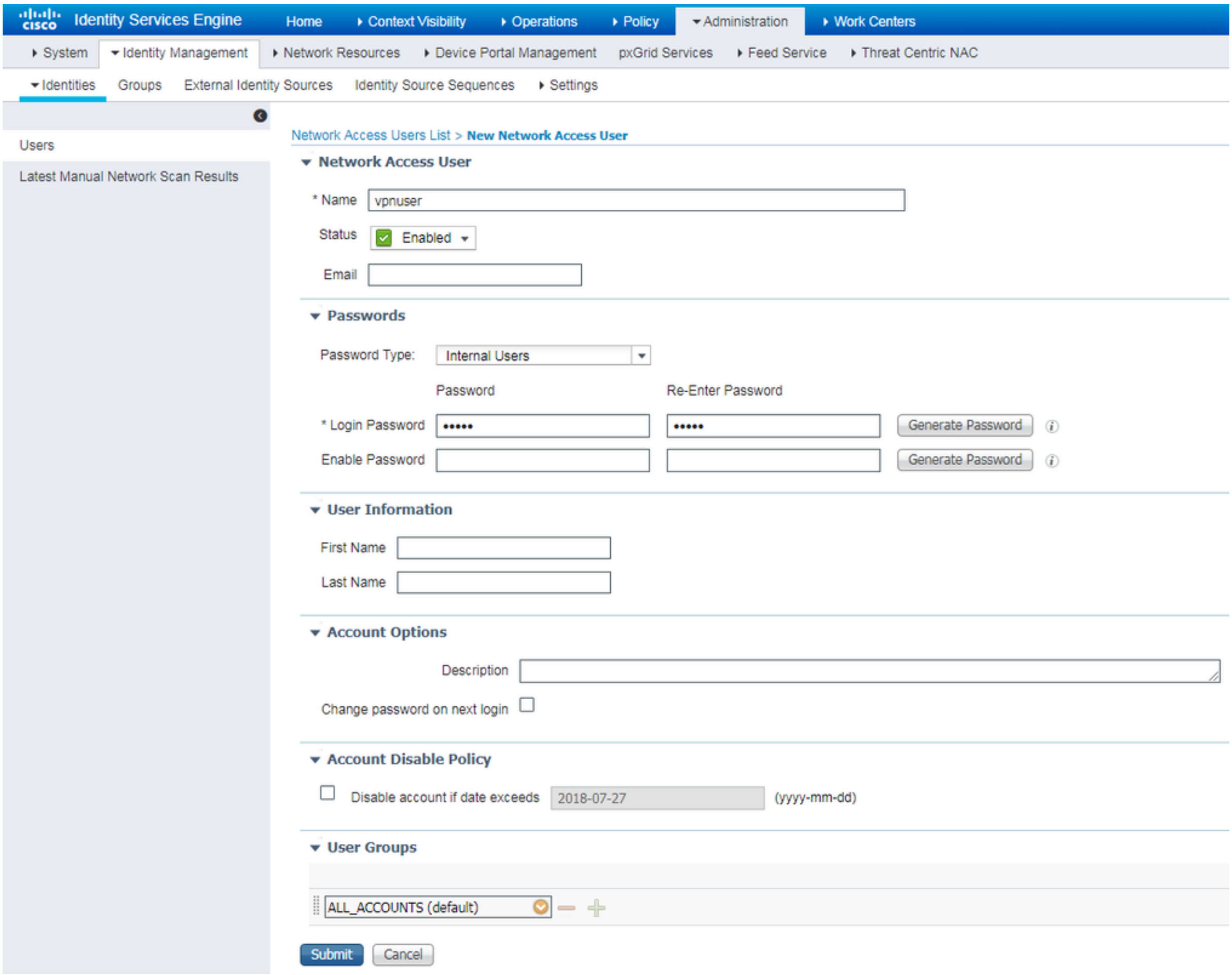


Network Access Users

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin

No data available

步驟2.在開啟的頁面上輸入使用者名稱、密碼和其他必要資訊，然後按一下**Submit**。



Network Access Users List > New Network Access User

Network Access User

* Name: vpnuser

Status: ☑ Enabled

Email:

Passwords

Password Type: Internal Users

	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

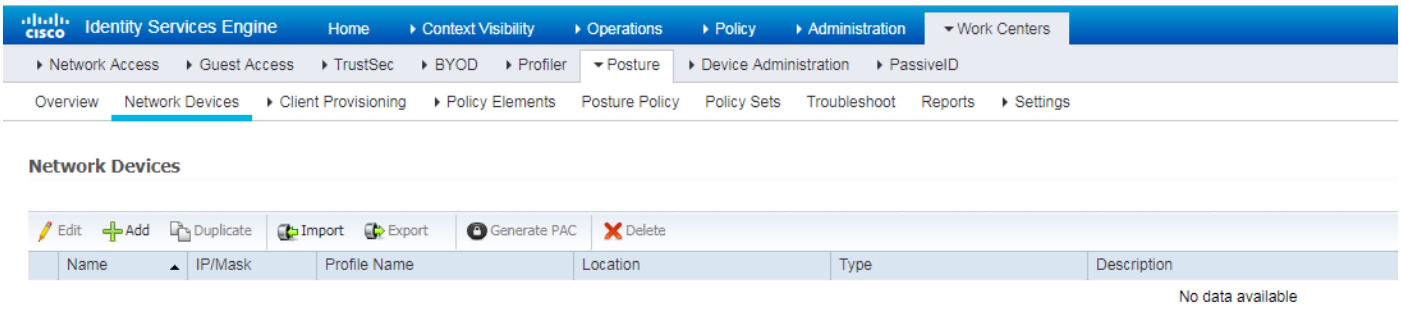
□ Disable account if date exceeds 2018-07-27 (yyyy-mm-dd)

User Groups

ALL_ACCOUNTS (default)

將FlexVPN中心新增為Radius客戶端

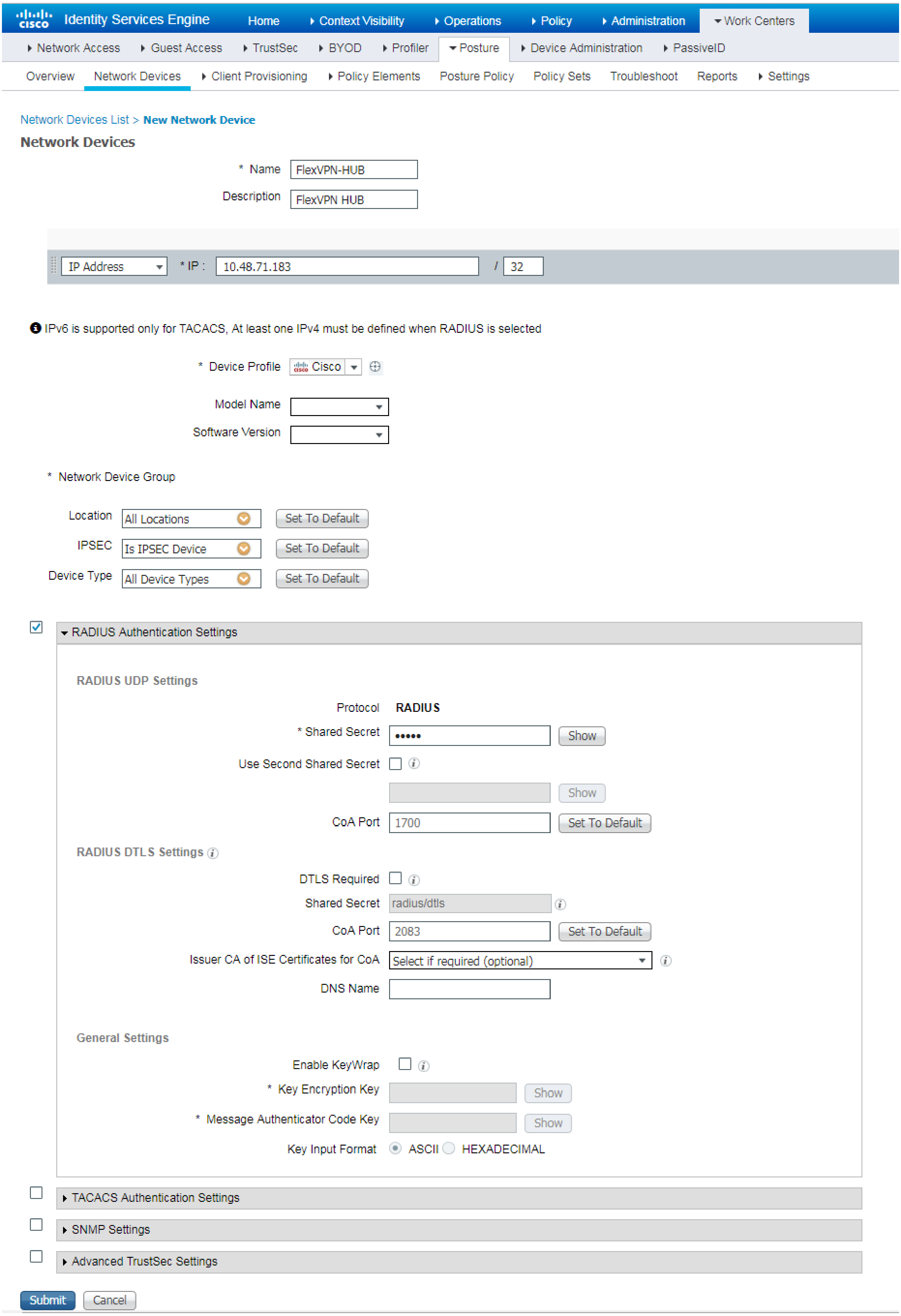
步驟1.轉至**Work Centers -> Posture -> Network Devices**，點選**Add**。



Network Devices

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

步驟2.在開啟的頁面上輸入裝置名稱、IP地址和其他必要資訊，選中覈取方塊「RADIUS身份驗證設定」，輸入共用金鑰，然後按一下頁面底部的**Submit**。



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
IPSEC	Is IPSEC Device
Device Type	All Device Types

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol	**RADIUS**
* Shared Secret	•••••
Use Second Shared Secret	□
CoA Port	1700

RADIUS DTLS Settings

DTLS Required	□
Shared Secret	radius/dtls
CoA Port	2083
Issuer CA of ISE Certificates for CoA	Select if required (optional)
DNS Name	

General Settings

Enable KeyWrap	□
* Key Encryption Key	
* Message Authenticator Code Key	
Key Input Format	● ASCII ○ HEXADECIMAL

□ TACACS Authentication Settings

□ SNMP Settings

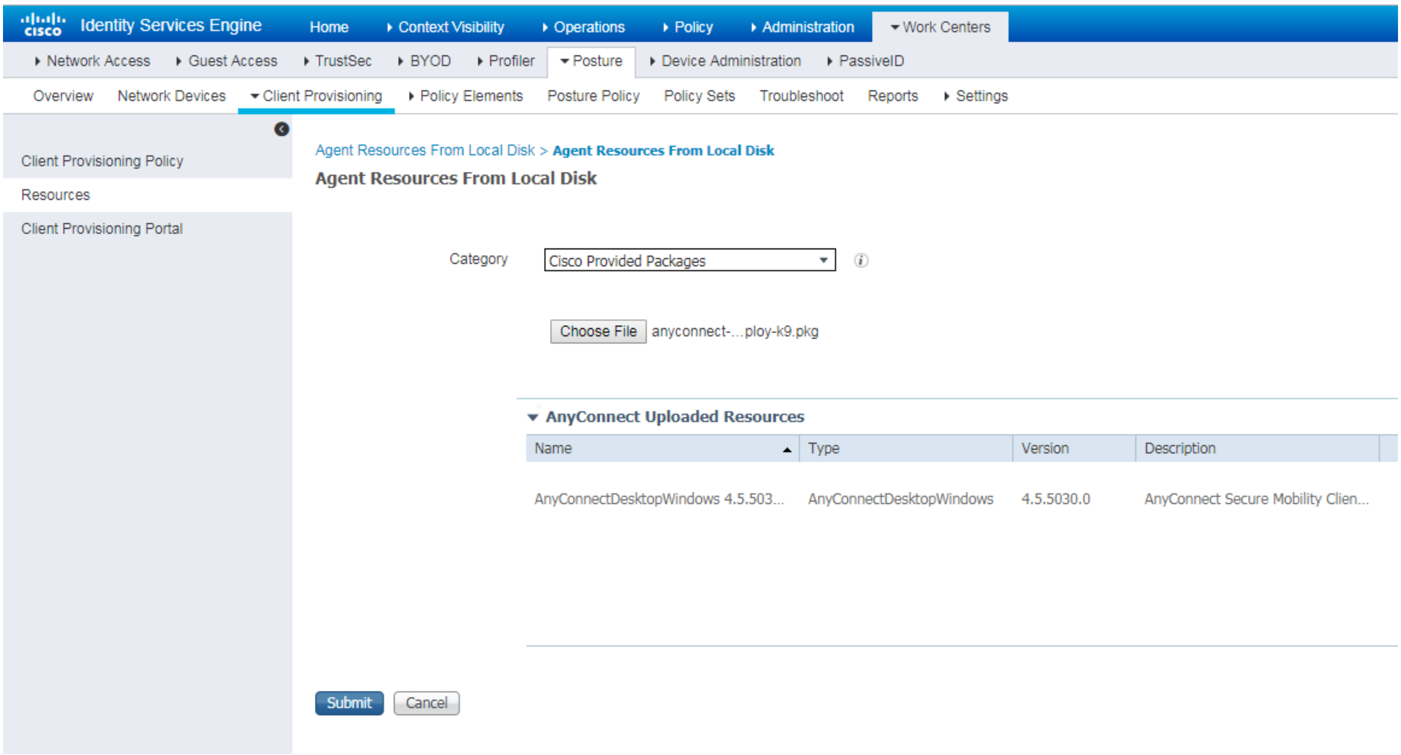
□ Advanced TrustSec Settings

客戶端調配配置

以下是準備Anyconnect配置的步驟。

步驟1. Anyconnect軟體包下載。Anyconnect軟體包本身無法從ISE直接下載，因此開始之前，請確保您的PC上有AC。此連結可用於交流下載 — http://cisco.com/go/anyconnect。本文檔中使用anyconnect-win-4.5.05030-webdeploy-k9.pkg包。

步驟2.若要將AC包上傳到ISE，請導航到**Work Centers -> Posture -> Client Provisioning ->** Resources並點選**Add**。選擇**Agent resources from local disk**。在新視窗中選擇**Cisco Provided Packages**，按一下**Choose File**，然後在PC上選擇AC軟體包。



Agent Resources From Local Disk

Category: Cisco Provided Packages

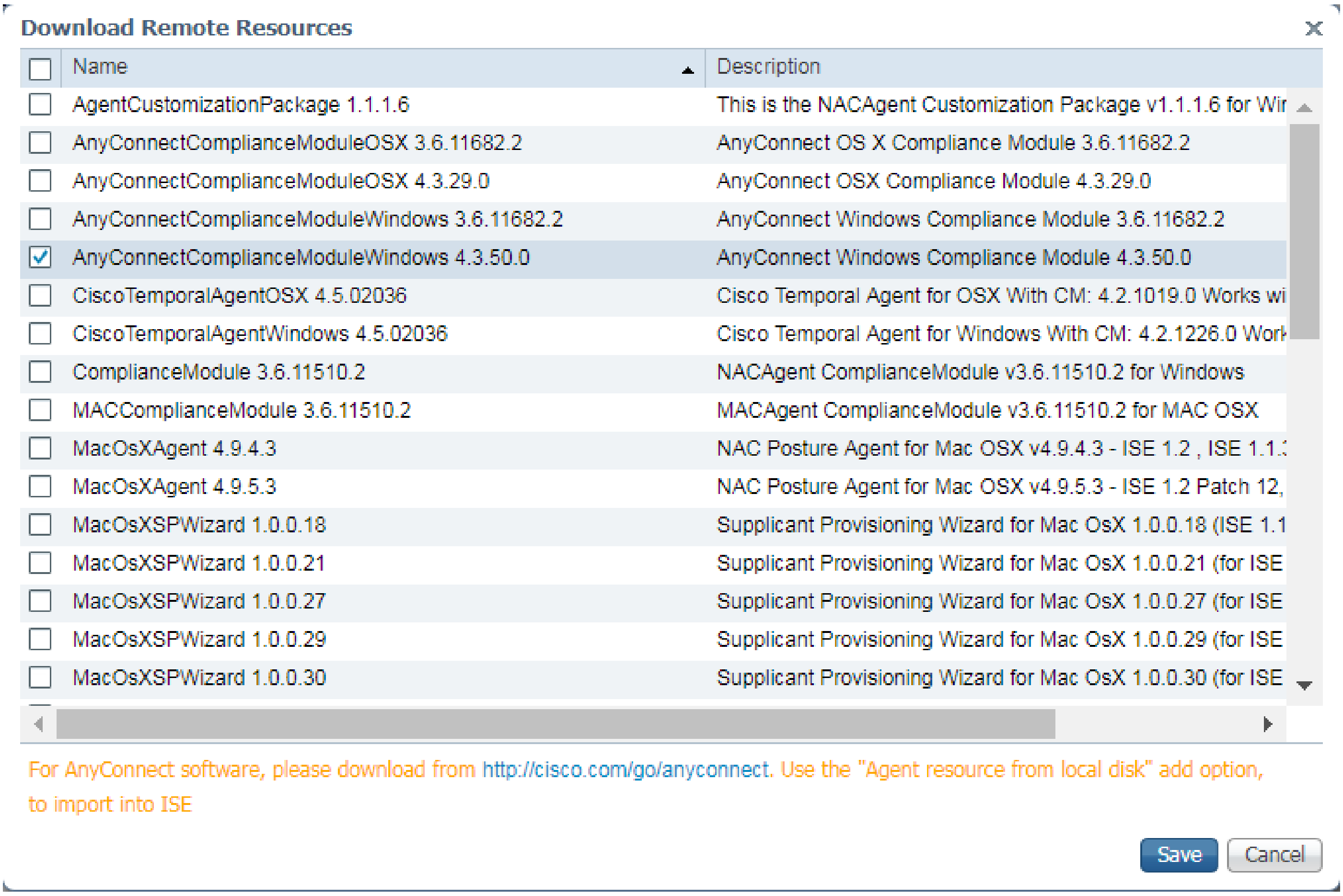
Choose File anyconnect-...ploy-k9.pkg

AnyConnect Uploaded Resources

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

按一下**Submit**完成匯入。驗證資料包的雜湊並按確認。

步驟3.合規性模組必須上傳到ISE。在同一頁(**工作中心 — >狀態 — >客戶端調配 — >資源**)上，按一下**新增**，然後從思科站點選擇**代理資源**。在資源清單中，您應檢查合規性模組並按一下**儲存**。（此檔案）AnyConnectComplianceModuleWindows 4.3.50.0合規性模組。

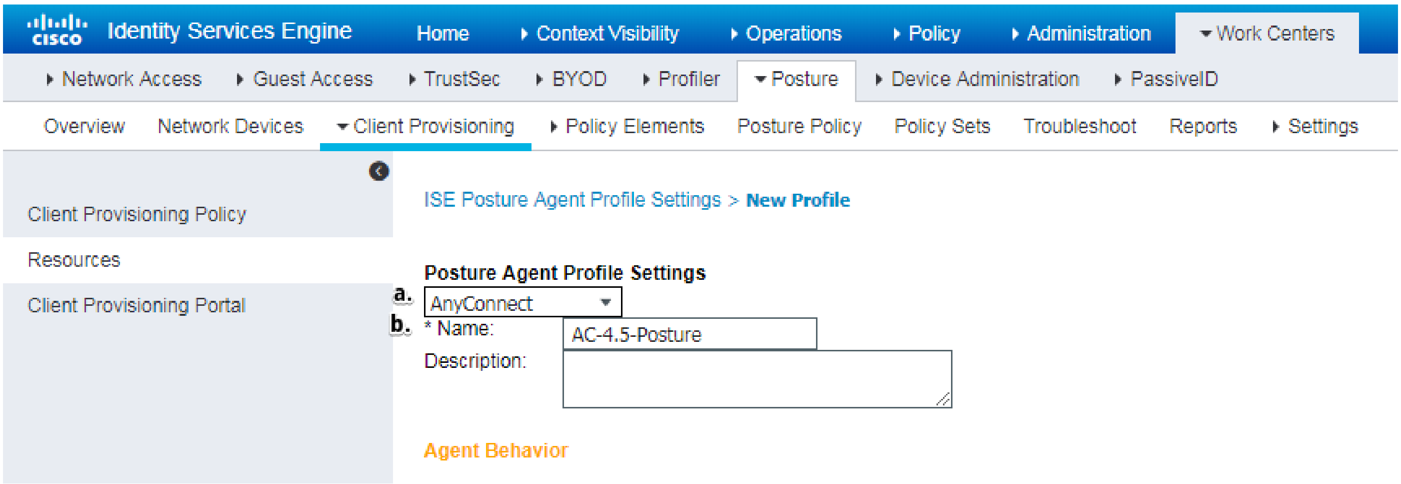


Download Remote Resources

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

步驟4.現在必須建立交流狀態配置檔案。按一下「**Add**」，然後選擇「**NAC agent**」或「**Anyconnect posture profile**」。



ISE Posture Agent Profile Settings > **New Profile**

Posture Agent Profile Settings

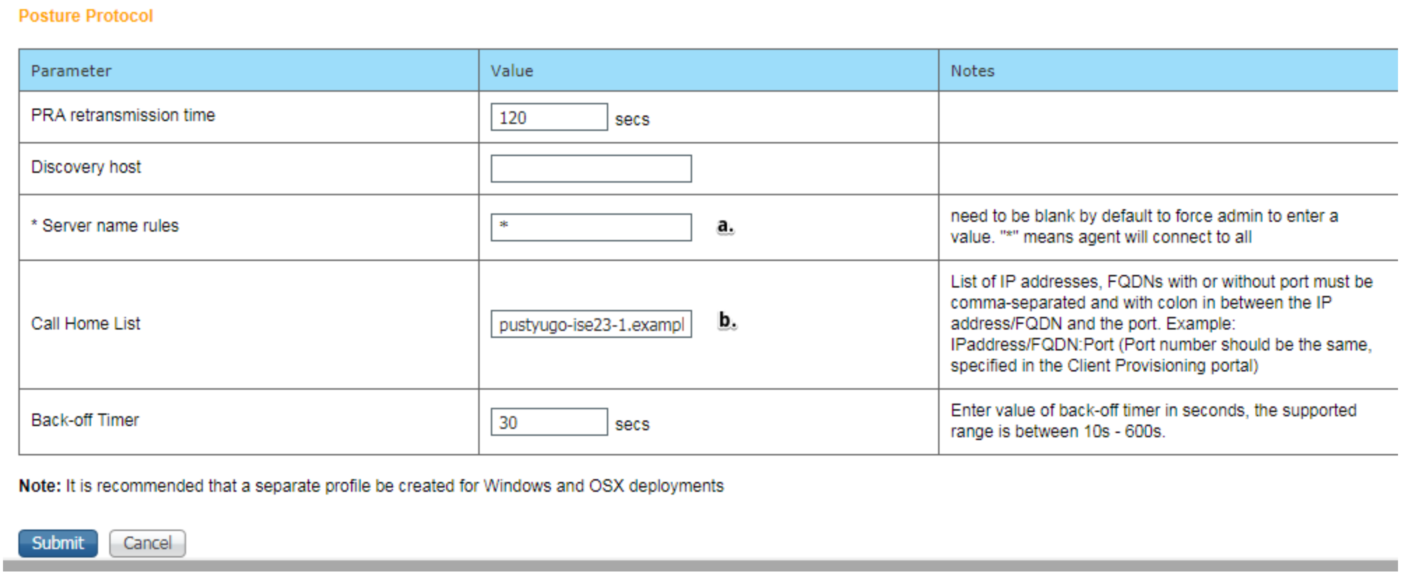
a. AnyConnect

b. * Name: AC-4.5-Posture

Description:

Agent Behavior

- 選擇配置檔案的型別。此案例應使用AnyConnect。
- 指定配置檔名稱。導航到配置檔案的**Posture Protocol**部分



Posture Protocol

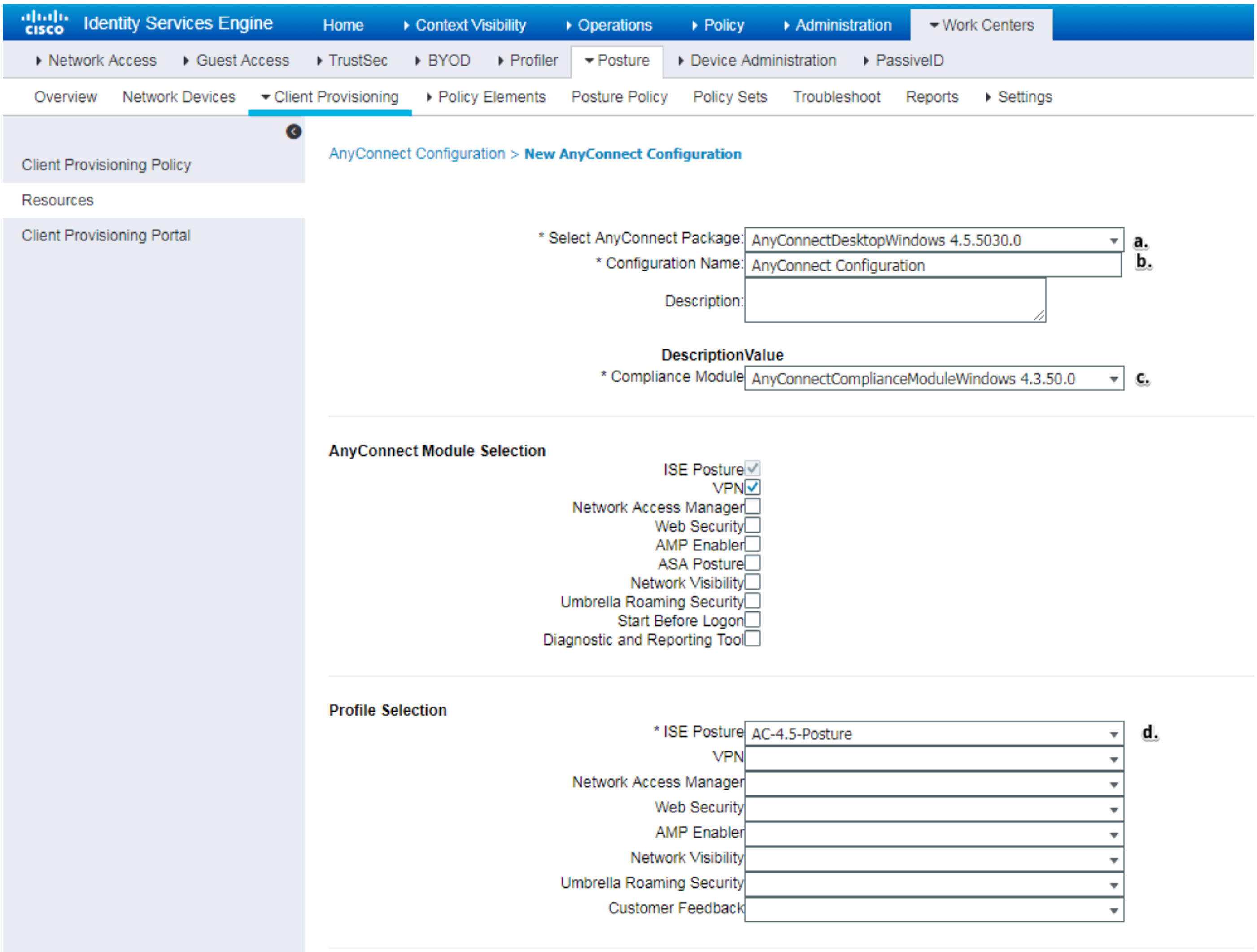
Parameter	Value	Notes
PRA retransmission time	120 secs	
Discovery host		
* Server name rules	* a.	need to be blank by default to force admin to enter a value. "*" means agent will connect to all
Call Home List	pustyugo-ise23-1.exampl b.	List of IP addresses, FQDNs with or without port must be comma-separated 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

- 指定**伺服器名稱規則**，此欄位不能為空。欄位可以包含帶有萬用字元的FQDN，此萬用字元限制來自相應名稱空間的AC狀態模組與PSN的連線。如果允許任何FQDN，則放置星號。

- 此處指定的名稱和IP在終端安全評估發現的第2階段使用(請參閱「ISE 2.2中的終端安全評估流」部分的步驟14)。 您可以按逗號分隔名稱，並且可以使用冒號在FQDN/IP之後新增埠號。

步驟5.建立AC配置。導航到**工作中心 — >狀態 — >客戶端調配 — >資源**，然後按一下**新增**，然後選擇**AnyConnect配置**。



AnyConnect Configuration > **New AnyConnect Configuration**

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

DescriptionValue
* 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:

- 選擇AC包。

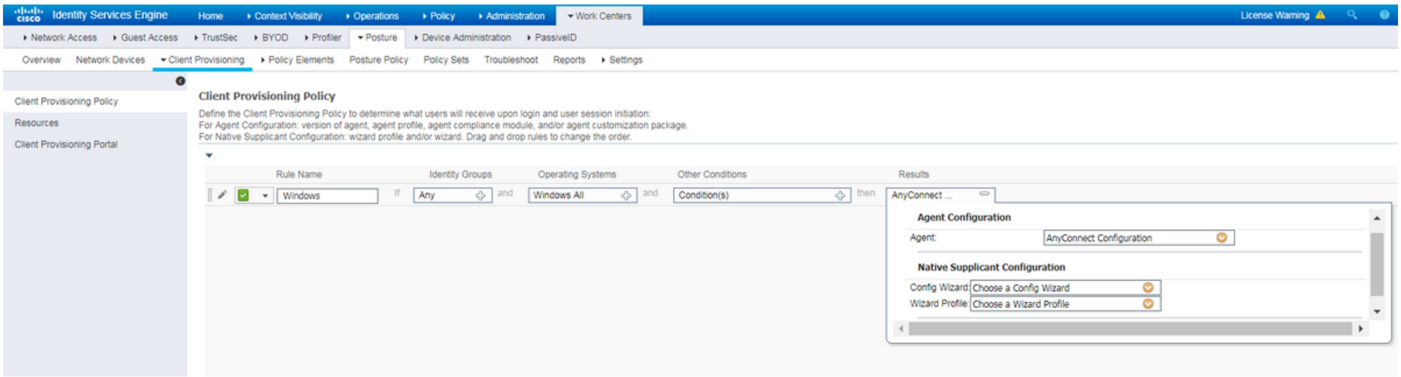
- 提供AC配置名稱。

- 選擇合規性模組版本。

- 從下拉選單中選擇AC狀態配置檔案。

步驟6.配置客戶端調配策略。導航到**工作中心 — >狀態 — >客戶端調配**。如果是初始配置，可以在預設策略中填充空值。如果需要將策略新增到現有狀態配置，請導航到可重用的策略，然後選擇**Duplicate Above**或**Duplicate Below。**還可以建立新的策略。

這是文檔中使用的策略的示例。



Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
☑ Windows	If	Any	and	Windows All	and	Condition(s)	then	AnyConnect ...

Agent Configuration

Agent: AnyConnect Configuration

Native Supplicant Configuration

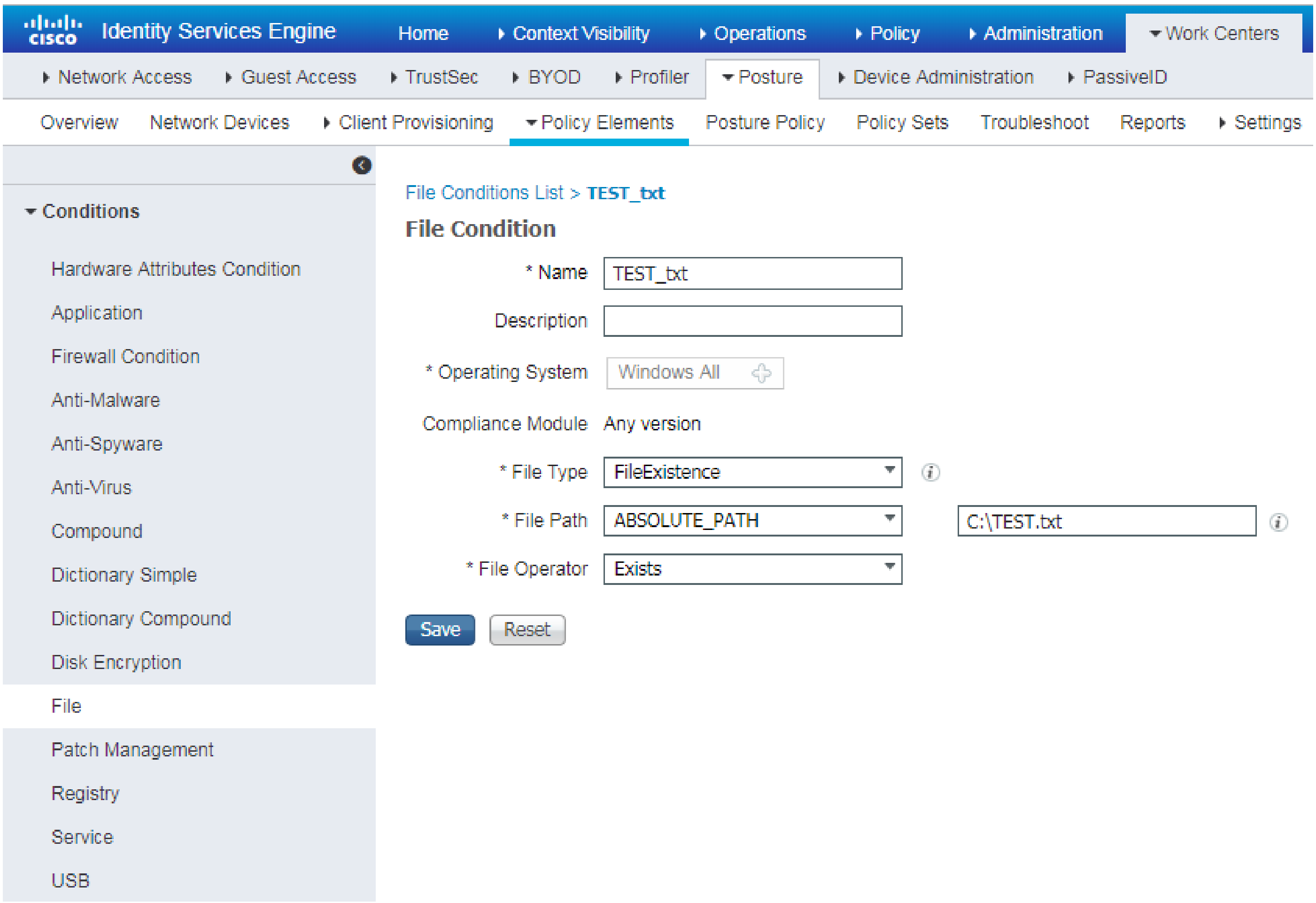
Config Wizard: Choose a Config Wizard
Wizard Profile: Choose a Wizard Profile

在結果部分選擇您的AC配置。

終端安全評估策略和條件

使用簡單的狀態檢查。ISE配置為檢查終端裝置端存在檔案C:\TEST.txt。實際場景可能更為複雜，但一般配置步驟是相同的。

步驟1.建立狀態條件。狀態條件位於**工作中心 — >狀態 — >策略元素 — >條件**。*選擇狀態條件的型別，然後按一下***Add**。指定必要資訊，然後按一下「**Save**」。下面是一個服務條件示例，它應檢查檔案C:\TEST.txt是否存在。



File Conditions List > **TEST_txt**

File Condition

* Name: TEST_txt

Description:

* Operating System: Windows All

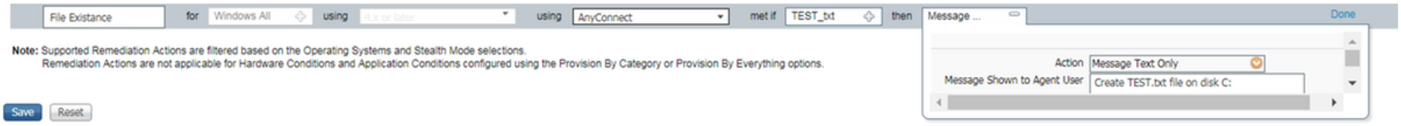
Compliance Module: Any version

* File Type: FileExistence

* File Path: ABSOLUTE_PATH C:\TEST.txt

* File Operator: Exists

步驟2.狀態要求配置。導航至**工作中心 — >狀態 — >策略元素 — >要求**。以下是一個檔案TEST.txt存在的示例：



File Existance for Windows All using 4.x or later using AnyConnect met if TEST_txt then Message ...

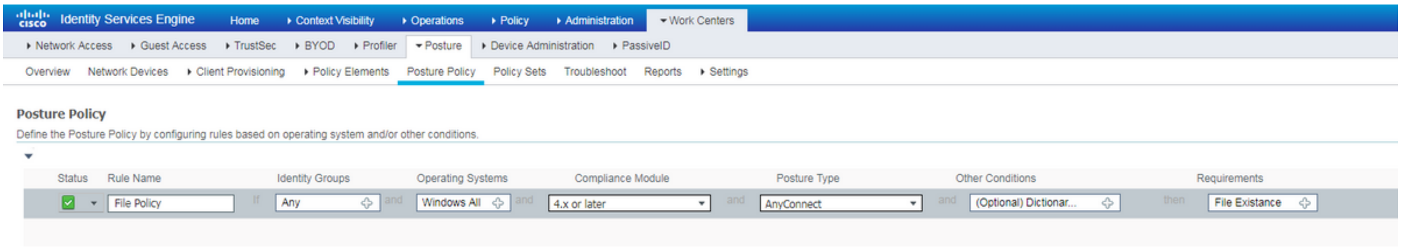
Action: Message Text Only

Message Shown to Agent User: Create TEST.txt file on disk C:

Note: Supported Remediation Actions are filtered based on the Operating Systems and Stealth Mode selections.
Remediation Actions are not applicable for Hardware Conditions and Application Conditions configured using the Provision By Category or Provision By Everything options.

在新的要求中選擇您的狀態條件並指定補救操作。

步驟3.狀態策略配置。導航至**工作中心 — >狀態 — >狀態策略**。您可以在下面找到用於本文檔的策略示例。策略將「檔案存在」要求指定為強制要求，並且未分配任何其他條件。



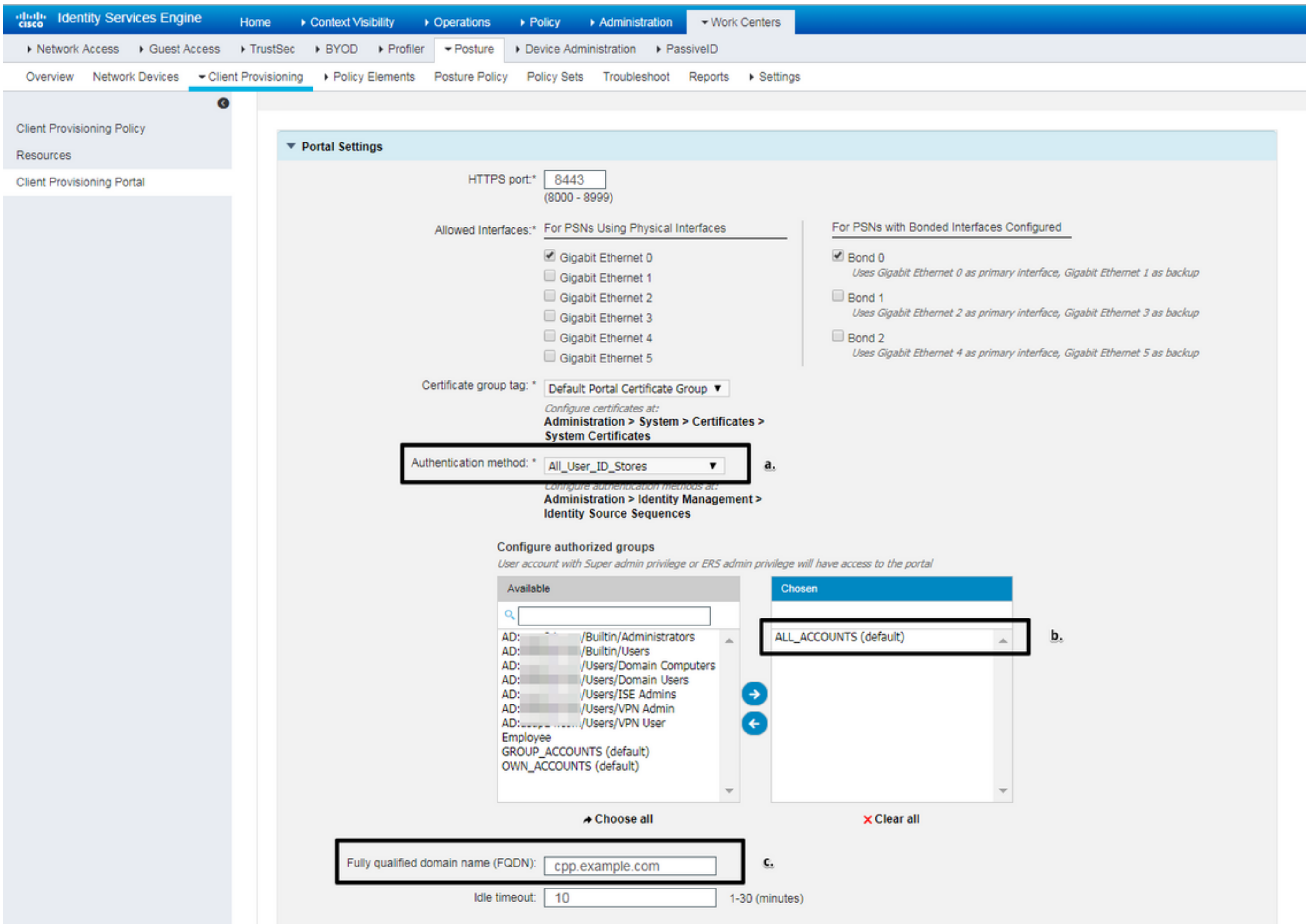
Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Rule Name		Identity Groups		Operating Systems		Compliance Module		Posture Type		Other Conditions		Requirements
☑	File Policy	If	Any	and	Windows All	and	4.x or later	and	AnyConnect	and	(Optional) Dictionar...	then	File Existance

配置客戶端調配門戶

對於無重定向的安全狀態，必須編輯客戶端調配門戶的配置。導航到**工作中心 — >狀態 — >客戶端調配-> 客戶端調配門戶**您可以使用預設門戶或建立您自己的門戶。



Portal Settings

HTTPS port:* 8443
(8000 - 8999)

Allowed Interfaces:*

For PSNs Using Physical Interfaces
- ☑ Gigabit Ethernet 0
- □ Gigabit Ethernet 1
- □ Gigabit Ethernet 2
- □ Gigabit Ethernet 3
- □ Gigabit Ethernet 4
- □ Gigabit Ethernet 5

For PSNs with Bonded Interfaces Configured
- ☑ Bond 0
  Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup
- □ Bond 1
  Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup
- □ Bond 2
  Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup

Certificate group tag: * Default Portal Certificate Group ▼
Configure certificates at:
Administration > System > Certificates > System Certificates

Authentication method: * All_User_ID_Stores ▼
Configure authentication methods at:
Administration > Identity Management > Identity Source Sequences

Configure authorized groups
User account with Super admin privilege or ERS admin privilege will have access to the portal

Available:
AD:[redacted]/Builtin/Administrators
AD:[redacted]/Builtin/Users
AD:[redacted]/Users/Domain Computers
AD:[redacted]/Users/Domain Users
AD:[redacted]/Users/ISE Admins
AD:[redacted]/Users/VPN Admin
AD:[redacted]/Users/VPN User
Employee
GROUP_ACCOUNTS (default)
OWN_ACCOUNTS (default)

Chosen:
ALL_ACCOUNTS (default)

Fully qualified domain name (FQDN): cpp.example.com

Idle timeout: 10 1-30 (minutes)

對於非重定向方案，應在門戶配置中編輯這些設定：

- 在身份驗證中，指定SSO找不到使用者會話時應使用的身份源序列。
- 根據選定的身份源序列，填充可用組的清單。此時，您需要選擇授權進行門戶登入的組。
- 必須指定客戶端調配門戶的FQDN。此FQDN應可解析為ISE PSN IP。應指示使用者在第一次連線嘗試期間在Web瀏覽器中指定FQDN。

配置授權配置檔案和策略

當終端安全評估狀態不可用時，需要限制客戶端的初始訪問。這可以通過多種方式實現：

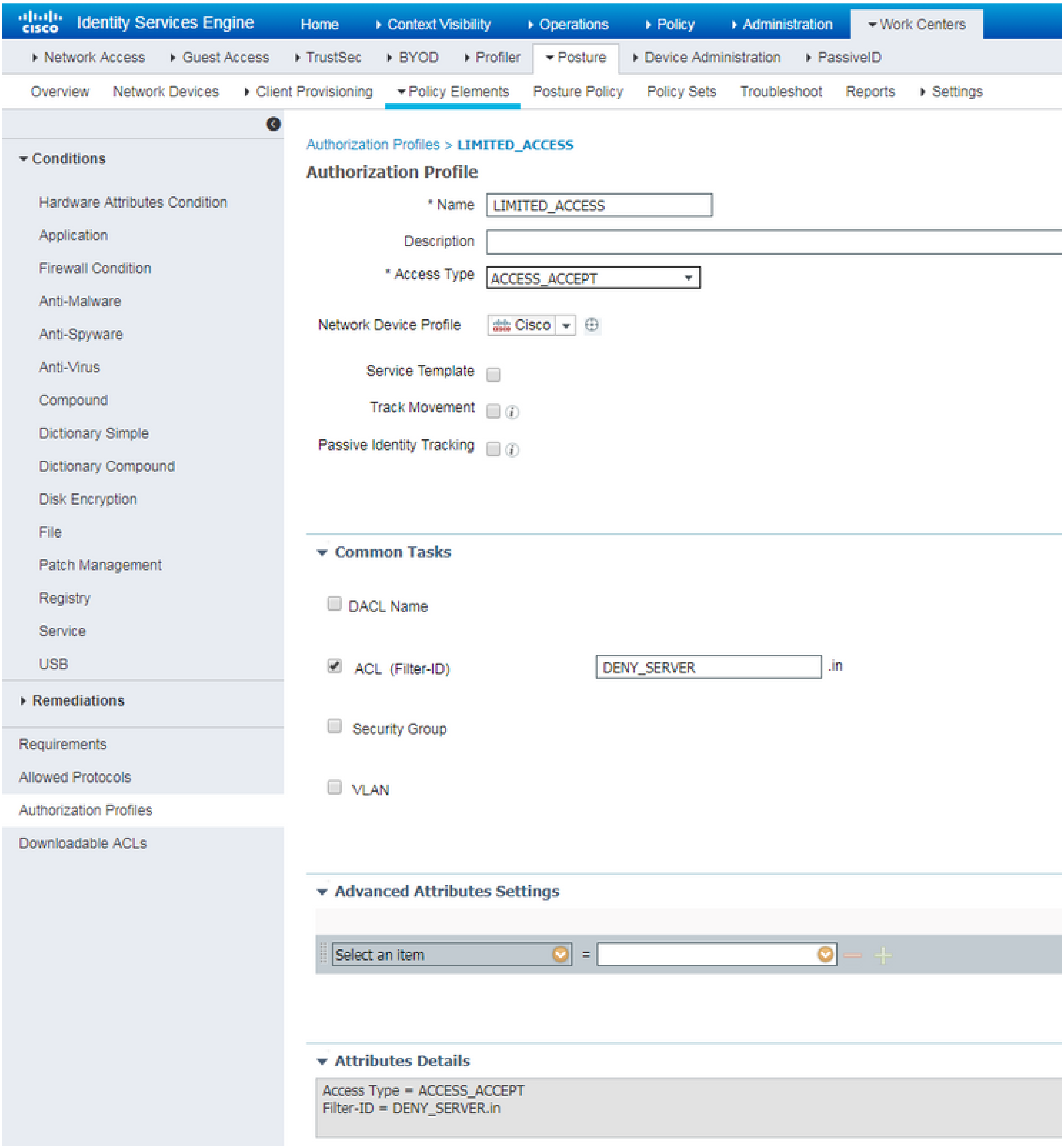
- Radius Filter-Id — 使用此屬性，可以將NAD上本地定義的ACL分配給狀態未知的使用者。由於這是標準RFC屬性，因此此方法應適合所有NAD供應商。
- Cisco:cisco-av-pair = ip:interface-config — 與Radius Filter-Id非常相似，可在本地定義的ACL分配給狀態未知的使用者。配置示例：
  cisco-av-pair = ip:interface-config=ip access-group DENY_SERVER in

步驟1.配置授權配置檔案。

安全狀態通常需要兩個授權配置檔案。第一個應包含任何型別的網路訪問限制。此配置檔案可應用於狀態不等於合規性的身份驗證。第二個授權配置檔案可能只包含允許訪問，並且可以應用於狀態為合規的會話。

要建立授權配置檔案，請導航至**工作中心 — >狀態 — >策略元素 — >授權配置檔案。**

具有Radius Filter-Id的受限訪問配置檔案示例：



Authorization Profiles > LIMITED_ACCESS

Authorization Profile

* Name: LIMITED_ACCESS

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

□ DACL Name

☑ ACL (Filter-ID) DENY_SERVER .in

□ Security Group

□ VLAN

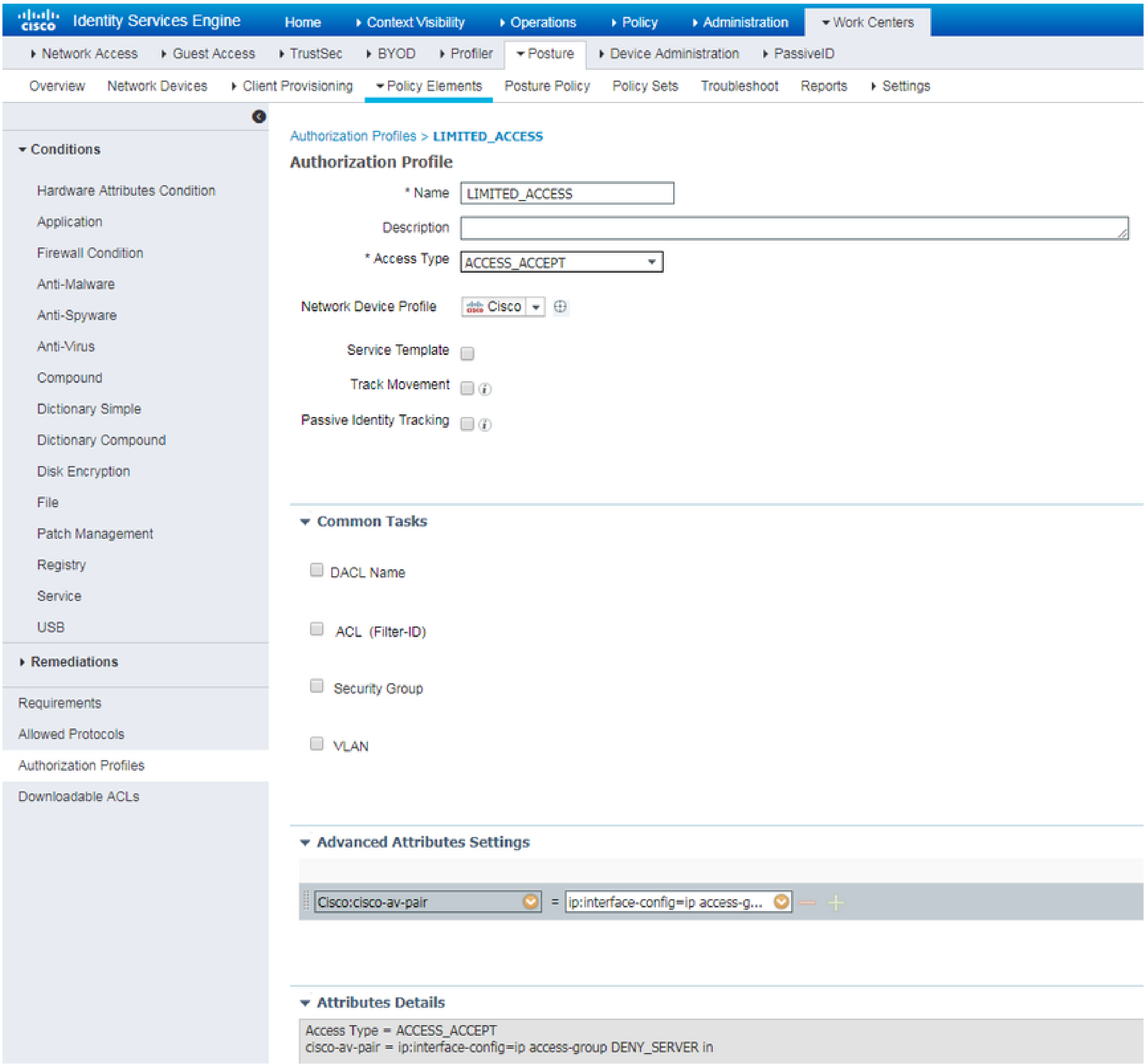
Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
Filter-ID = DENY_SERVER.in

使用cisco-av-pair的受限訪問配置檔案示例：



Authorization Profiles > LIMITED_ACCESS

Authorization Profile

* Name	LIMITED_ACCESS
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	Cisco
Service Template	□
Track Movement	□
Passive Identity Tracking	□

Common Tasks

□ DACL Name

□ ACL (Filter-ID)

□ Security Group

□ VLAN

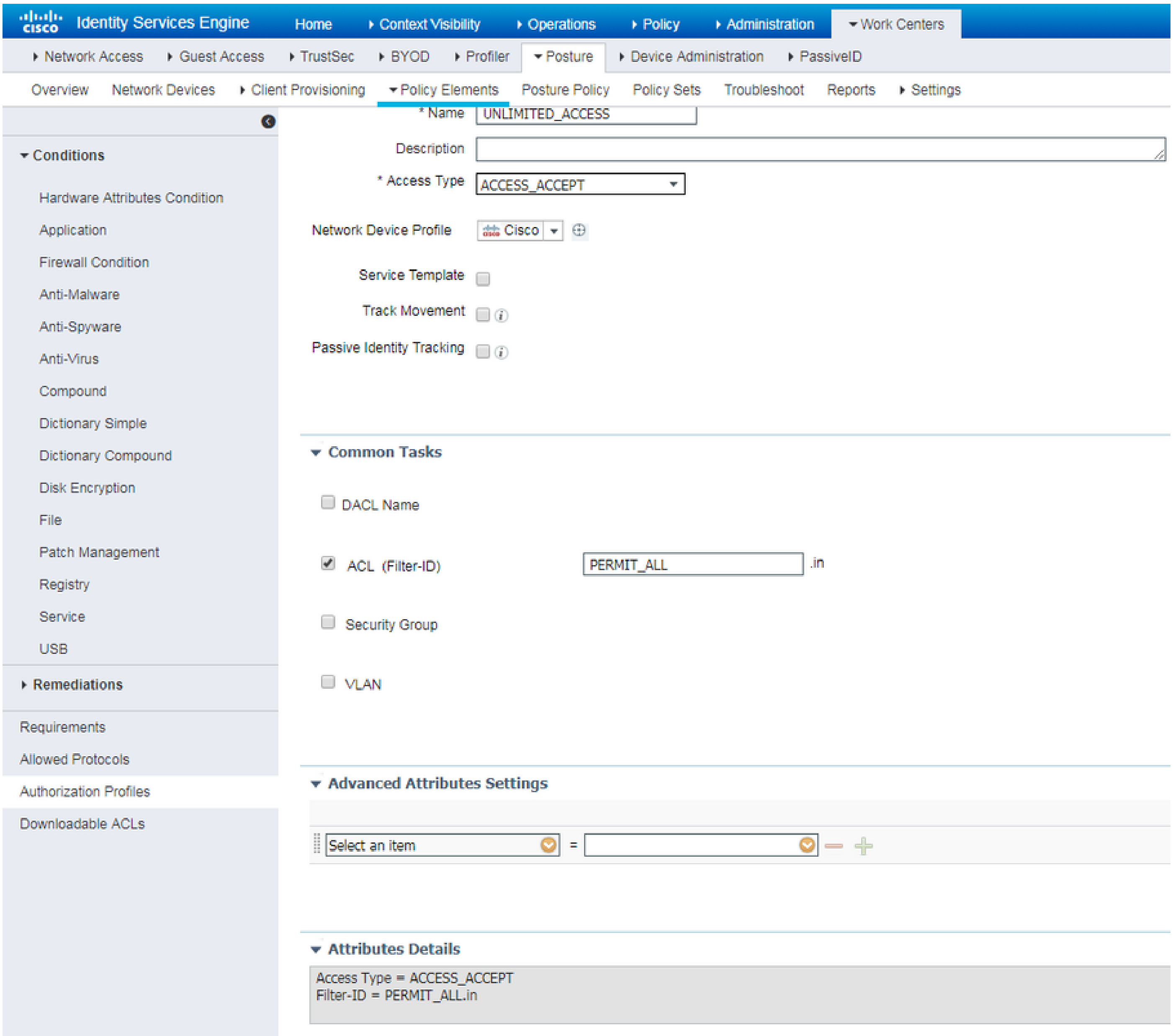
Advanced Attributes Settings

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

具有Radius Filter-Id的無限制訪問配置檔案的示例：



* Name 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

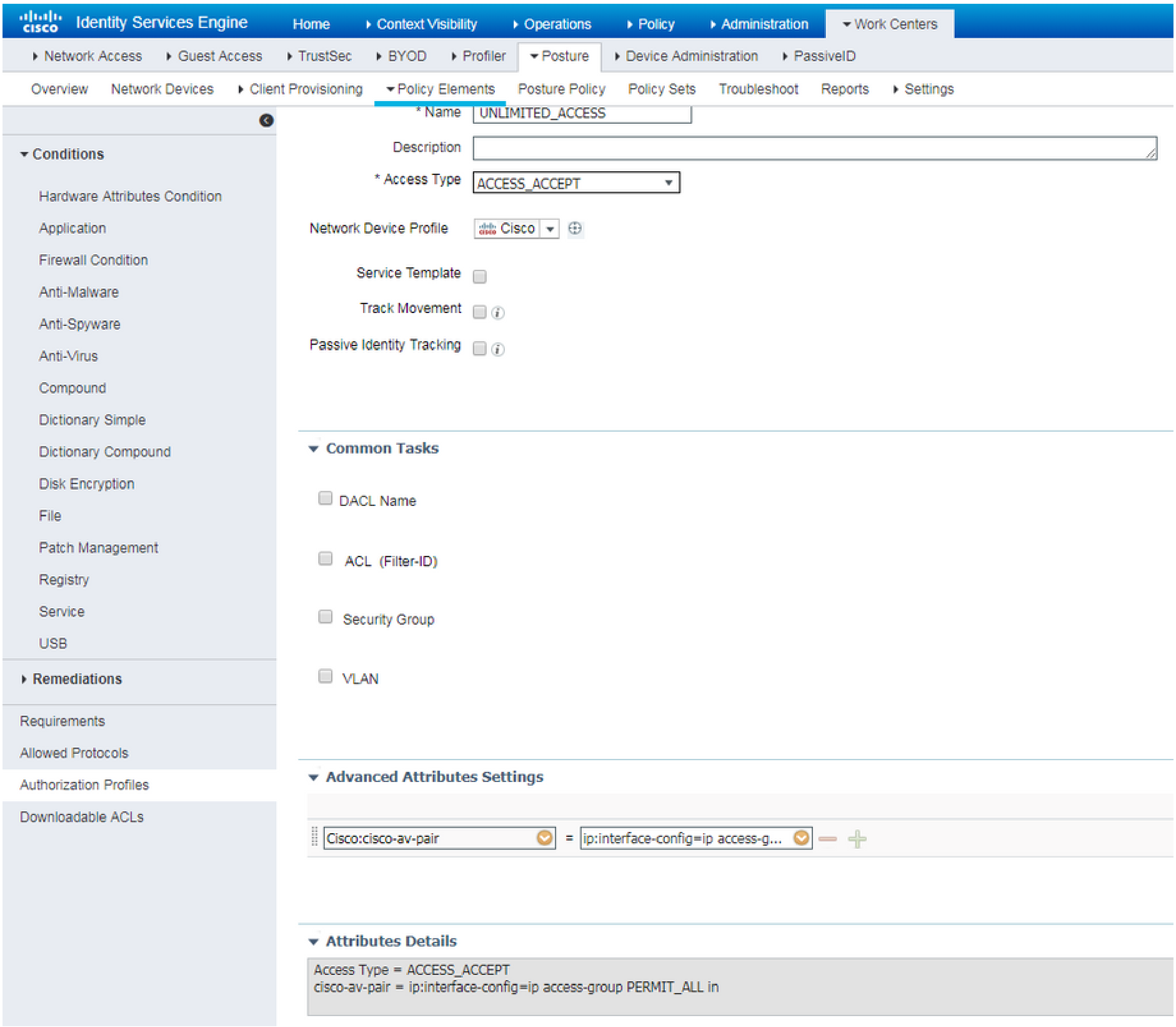
Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
Filter-ID = PERMIT_ALL.in

使用cisco-av-pair的無限制訪問配置檔案的示例：



* Name: 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)

□ Security Group

□ VLAN

Advanced Attributes Settings

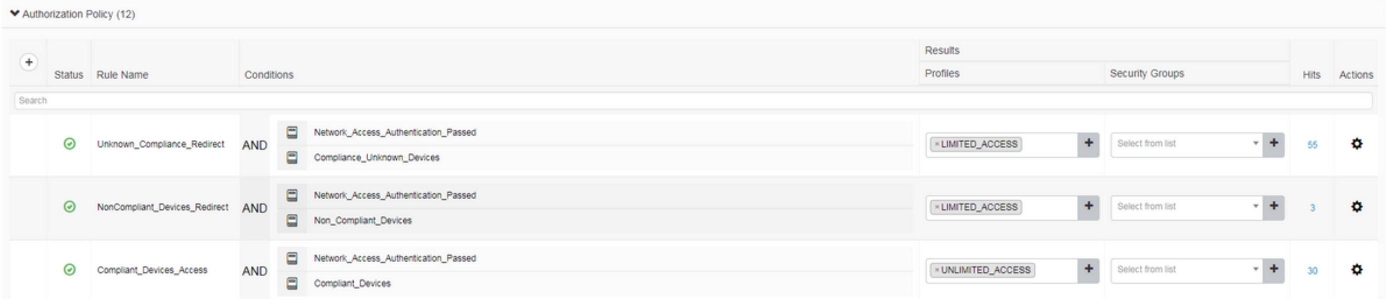
Cisco:cisco-av-pair = ip:interface-config=ip access-g...

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = ip:interface-config=ip access-group PERMIT_ALL in
```

步驟2.配置授權策略。在此步驟中，應建立兩個授權策略。一個用於匹配初始身份驗證請求與未知的安全評估狀態，另一個用於在成功的安全評估過程後分配完全訪問許可權。

以下是此案例的簡單授權策略的示例：


Authorization Policy (12)

Status	Rule Name		Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	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	⚙

身份驗證策略的配置不是本文檔的一部分，但您應該記住，身份驗證需要成功才能開始授權策略處理。

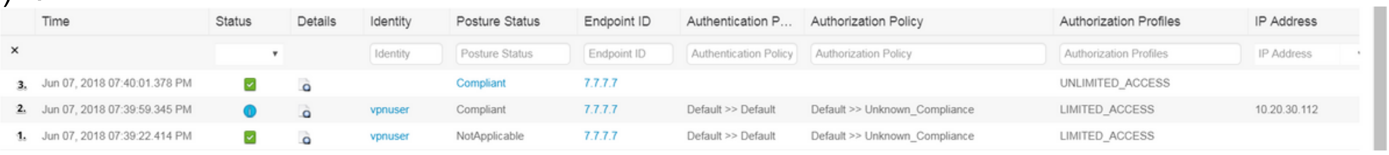
驗證

流的基本驗證可能包括三個主要步驟：

步驟1. FlexVPN中心上的RA VPN會話驗證：

```
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
```

步驟2.驗證流量驗證（Radius即時日誌）：



	Time	Status	Details	Identity	Posture Status	Endpoint ID	Authentication P...	Authorization Policy	Authorization Profiles	IP Address
×		▾		Identity	Posture Status	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
3.	Jun 07, 2018 07:40:01.378 PM	✓	🔍		Compliant	7.7.7.7			UNLIMITED_ACCESS	
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	NotApplicable	7.7.7.7	Default >> Default	Default >> Unknown_Compliance	LIMITED_ACCESS	

1. 初始身份驗證。對於此步驟，您可能想要驗證已應用了哪個授權配置檔案。如果已應用意外授

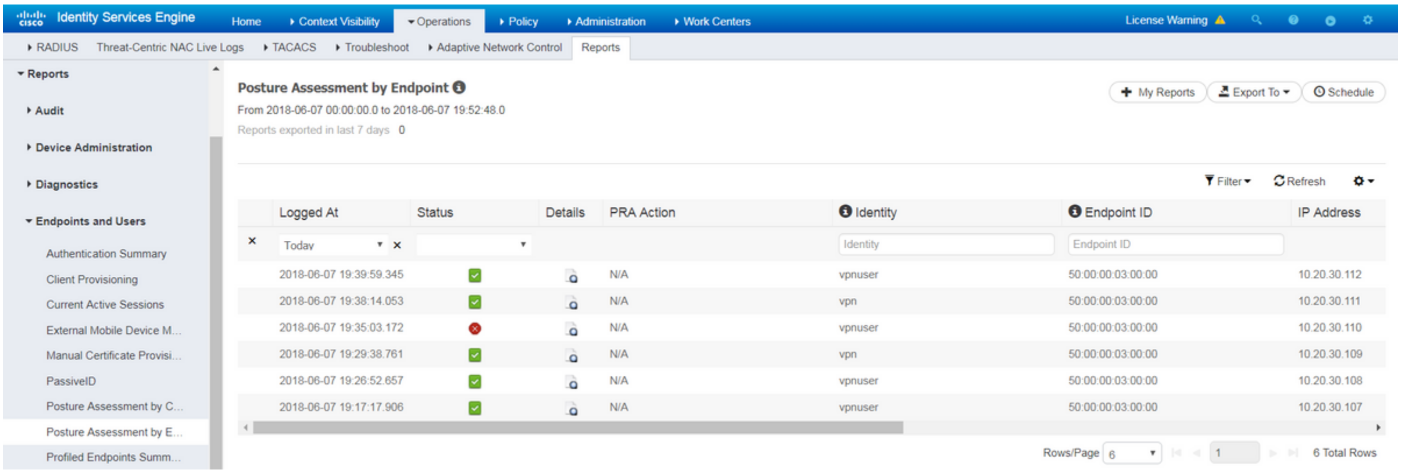
權配置檔案，請調查詳細的身份驗證報告。您可以通過按一下「詳細資訊」列中的放大鏡來開啟此報告。您可以將詳細身份驗證報告中的屬性與授權策略中預期匹配的條件進行比較。

2. 會話資料更改，在此特定示例中，會話狀態已從「不適用」更改為「相容」。

3. COA連線到網路接入裝置。此COA應成功從NAD端推送新身份驗證，並在ISE端推送新授權策略分配。如果COA失敗，您可以開啟詳細報告以調查原因。COA的最常見問題包括： COA超時 — 在這種情況下，已傳送請求的PSN未配置為NAD端的COA客戶端，或者已在途中的某個位置丟棄COA請求。COA負ACK — 表示NAD已接收COA，但由於某種原因無法確認COA操作。對於此方案，詳細報告應包含更詳細的說明。

由於基於IOS XE的路由器已用作本示例的需要地址，因此您看不到該使用者的後續身份驗證請求。發生這種情況的原因是ISE使用COA推送來進行IOS XE，從而避免VPN服務中斷。在這種情況下，COA本身包含新的授權引數，因此不需要重新身份驗證。

第3步：狀態報告驗證 — 導航到**操作 — >報告 — >報告 — >終端和使用者 — >終端安全評估。**



Posture Assessment by Endpoint

From 2018-06-07 00:00:00.0 to 2018-06-07 19:52:48.0

Reports exported in last 7 days 0

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

Rows/Page 6 1 6 Total Rows

您可以從這裡開啟每個特定事件的詳細報告，以檢查此報告屬於哪個會話ID、ISE為終端選擇了哪種確切的安全狀態要求以及每個要求的狀態。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

1. 要從頭端收集的IKEv2調試：

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

2. AAA調試以檢視本地和/或遠端屬性的分配：

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

3. 來自AnyConnect客戶端的DART。
4. 對於狀態進程故障排除，必須在可能發生狀態進程的ISE節點上啟用這些ISE元件進行調試：**client-webapp -**負責代理程式設定的元件。目標日誌檔案**guest.log**和**ise-psc.log**。**訪客** — 負責客戶端調配門戶元件和會話所有者查詢的元件（當請求遇到錯誤的PSN時）。 目標日誌檔案 — **guest.log**。**provisioning — 負責客戶端調配策略處理的元件。目標日誌檔案- guest.log。posture** — 所有與終端安全評估相關的事件。目標日誌檔案**- ise-psc.log**
5. 對於客戶端故障排除，您可以使用：**AnyConnect.txt** — 此檔案可在DART捆綁包中找到，用於VPN故障排除。**acisensa.log** — 如果客戶端上的客戶端調配失敗，則會在下載NSA的同一資料夾中建立此檔案（通常為Windows的「下載」目錄），**AnyConnect_ISEPosture.txt** — 此檔案可在**Cisco AnyConnect ISE Posture Module目錄中的DART套件組合中找到**。所有有關ISE PSN發現和狀態流程常規步驟的資訊均記錄在此檔案中。