Configurazione della postura di ISE con FlexVPN

Sommario

Introduzione

In questo documento viene illustrato un esempio di come configurare un headend IOS XE per l'accesso remoto con postura utilizzando il metodo di autenticazione AnyConnect IKEv2 e EAP-Message Digest 5 (EAP-MD5).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione VPN ad accesso remoto FlexVPN (RA) su IOS XE
- Configurazione client AnyConnect (AC)
- Flusso di postura su Identity Service Engine (ISE) 2.2 e versioni successive
- Configurazione dei componenti di postura su ISE
- Configurazione del server DNS in Windows Server 2008 R2

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco CSR1000V con IOS XE 16.8 [Fuji]
- Client AnyConnect versione 4.5.03040 in esecuzione su Windows 7
- Cisco ISE 2.3
- Server Windows 2008 R2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Per garantire che le misure di sicurezza della rete imposte rimangano pertinenti ed efficaci, Cisco ISE consente di convalidare e mantenere le funzionalità di sicurezza su qualsiasi computer client che accede alla rete protetta. Utilizzando policy di postura progettate per garantire la disponibilità delle impostazioni o delle applicazioni di sicurezza più aggiornate sui computer client, l'amministratore Cisco ISE può garantire che tutti i computer client che accedono alla rete soddisfino e continuino a soddisfare gli standard di sicurezza definiti per l'accesso alla rete aziendale. I report di conformità della postura forniscono a Cisco ISE un'istantanea del livello di conformità del client al momento dell'accesso dell'utente, nonché ogni volta che si verifica una rivalutazione periodica.

La postura può essere rappresentata da tre elementi principali:

1. ISE è un punto di distribuzione e decisione per la configurazione dei criteri. Dal punto di vista dell'amministratore di ISE, è possibile configurare i criteri di postura (quali condizioni esatte devono essere soddisfatte per contrassegnare il dispositivo come conforme a livello aziendale), i criteri di provisioning client (quale software agente deve essere installato sui tipi di dispositivi) e i criteri di autorizzazione (a quale tipo di autorizzazioni assegnare, in base allo stato della postura).

2. Il dispositivo di accesso alla rete (NAD) funge da punto di applicazione dei criteri. Sul lato AND vengono applicate restrizioni effettive alle autorizzazioni al momento dell'autenticazione dell'utente. ISE come punto dei criteri fornisce parametri di autorizzazione quali l'Access Control List (ACL). In genere, per consentire la postura, i servizi NAD devono supportare la funzione di modifica dell'autorizzazione (CoA) per riautenticare l'utente dopo la determinazione dello stato di postura dell'endpoint. A partire da ISE 2.2, i servizi NAD non devono supportare il reindirizzamento.
   Nota: I router che eseguono IOS XE non supportano il reindirizzamento.**Nota:** Affinché CoA con ISE sia completamente operativo, il software IOS XE deve avere le correzioni per i seguenti difetti:
   CSCve16269 IKEv2 CoA non funziona con ISE
   CSCvi90729 IKEv2 CoA non funziona con ISE (coa-push=TRUE anziché TRUE)
3. Software agente come punto di raccolta dei dati e interazione con l'utente finale. L'agente riceve informazioni sui requisiti di postura dall'ISE e fornisce all'ISE un report relativo allo

stato dei requisiti. Questo documento è basato sul modulo Anyconnect ISE Posture, l'unico che supporta completamente la postura senza reindirizzamento.

Il flusso di postura senza reindirizzamento è ben documentato nell'articolo "ISE Posture Style Comparison for Pre and Post 2.2", sezione "Posture flow in ISE 2.2".

Il provisioning del modulo Anyconnect ISE Posture con FlexVPN può essere eseguito in due modi:

- Manuale - il modulo viene installato manualmente sulla postazione di lavoro del client dal pacchetto Anyconnect disponibile sul portale di download del software Cisco: https://software.cisco.com/download/home/283000185.
  Le seguenti condizioni devono essere soddisfatte per il lavoro di postura con il provisioning manuale del modulo di postura ISE:

  1. Il DNS (Domain Name Server) deve risolvere l'FQDN (Fully Qualified Domain Name) **enroll.cisco.com** in IP di PSN (Policy Service Nodes). Durante il primo tentativo di connessione, il modulo della postura non dispone di informazioni sui PSN disponibili. È in corso l'invio di richieste di individuazione per trovare PSN disponibili. L'FQDN enroll.cisco.com viene utilizzato in una di queste richieste.

  2. La porta **TCP 8905** deve essere consentita per gli IP dei PSN. in questo scenario, la postura passa attraverso la porta TCP 8905.

  3. Il **certificato di amministrazione** sui nodi PSN deve avere **enroll.cisco.com** nel **campo SAN**. La connessione tra l'utente VPN e il nodo PSN tramite TCP 8905 è protetta tramite certificato amministratore e l'utente riceverà un avviso di certificato se non è presente il nome "enroll.cisco.com" nel certificato amministratore del nodo PSN.

  Nota: In base a RFC6125, i CN dei certificati devono essere ignorati se sono stati specificati valori SAN. Significa anche che dobbiamo aggiungere CN di amministrazione certificato in campo SAN.

- Provisioning automatico tramite il CPP (Client Provisioning Portal): il modulo viene scaricato e installato dall'ISE accedendo direttamente al CPP tramite il FQDN del portale.
  Le seguenti condizioni devono essere soddisfatte per il lavoro di postura con il provisioning automatico del modulo ISE Posture:

  1. Il DNS deve risolvere il **nome di dominio completo (FQDN) del PCP** negli IP dei nodi di servizio dei criteri (PSN).

  2. **Le porte TCP 80, 443 e la porta CPP (8443 per impostazione predefinita)** devono essere consentite per i PSN e IP. Il client deve aprire l'FQDN di CPP direttamente tramite HTTP (verrà reindirizzato a HTTPS) o HTTPS. La richiesta verrà reindirizzata alla porta di CPP (per impostazione predefinita 8443) e quindi la postura passerà attraverso tale porta.

  3. **I certificati di amministrazione e CPP** sui nodi PSN devono avere un **FQDN CPP** nel **campo SAN**. La connessione tra l'utente VPN e il nodo PSN tramite TCP 443 è protetta dal certificato di amministrazione e la connessione sulla porta CPP è protetta dal certificato CPP.

  Nota: In base a RFC6125, i CN dei certificati devono essere ignorati se sono stati specificati

valori SAN. Significa anche che dobbiamo aggiungere CN di amministrazione e certificati CPP nel campo SAN dei certificati corrispondenti.

Nota: Se il software ISE non contiene una correzione per CSCvj76466, la postura o il provisioning del client funzioneranno solo se l'esposizione o il provisioning del client vengono eseguiti sullo stesso PSN su cui il client è stato autenticato.

In caso di postura con FlexVPN, il flusso include i seguenti passaggi:

1. L'utente si connette all'hub FlexVPN utilizzando il client Anyconnect.

2. ISE invia un messaggio di accesso/accettazione all'hub FlexVPN con il nome ACL che deve essere applicato per limitare l'accesso.

3 bis. Prima connessione con il provisioning manuale: il modulo di postura ISE inizia a rilevare il policy server che invia la sonda a enroll.cisco.com tramite la porta TCP 8905. Di conseguenza, il modulo di postura scarica il profilo di postura configurato e aggiorna il modulo di conformità sul lato client.

Durante i successivi tentativi di connessione, il modulo di postura ISE utilizzerà anche i nomi e gli IP specificati nell'elenco Call Home del profilo di postura per il rilevamento del policy server.

3 ter. Prima connessione con Provisioning automatico - Il client apre CPP tramite FQDN. Come risultato positivo Network Setup Assistant viene scaricato sulla workstation del client, quindi scarica e installa il modulo ISE Posture, il modulo ISE Compliance e il profilo postura.

Durante i successivi tentativi di connessione, il modulo di postura ISE utilizzerà i nomi e gli IP specificati nell'elenco Call Home del profilo di postura per il rilevamento del policy server.

4. Il modulo Posture avvia i controlli di conformità e invia i risultati dei controlli all'ISE.

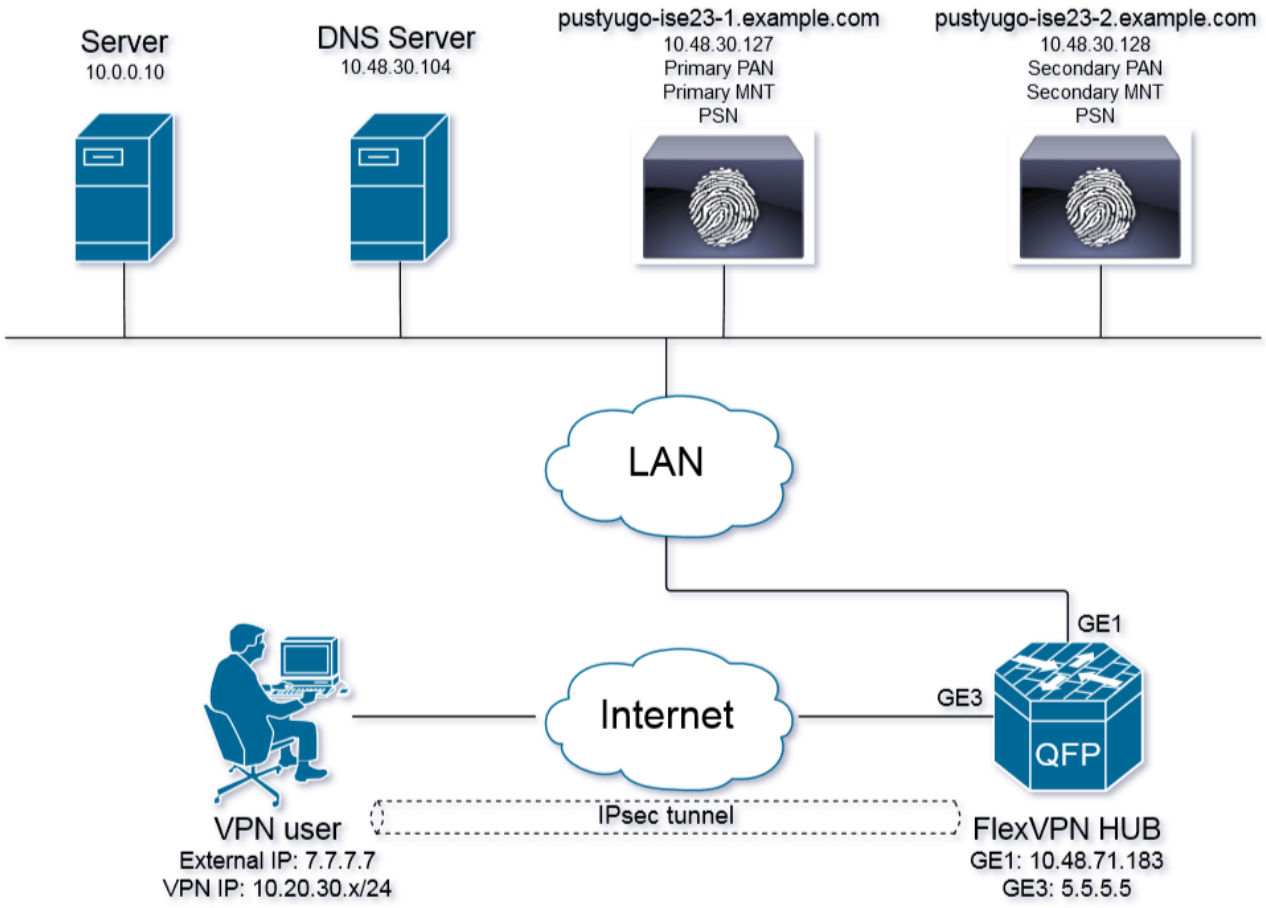
5. Se lo stato del client è Conforme, ISE invia Access-Accept all'hub FlexVPN con il nome ACL che deve essere applicato al client conforme.

6, il client ottiene l'accesso alla rete.

Per ulteriori informazioni sul processo di postura, consultare il documento "ISE Posture Style Comparison for Pre and Post 2.2".

Configurazione

Esempio di rete

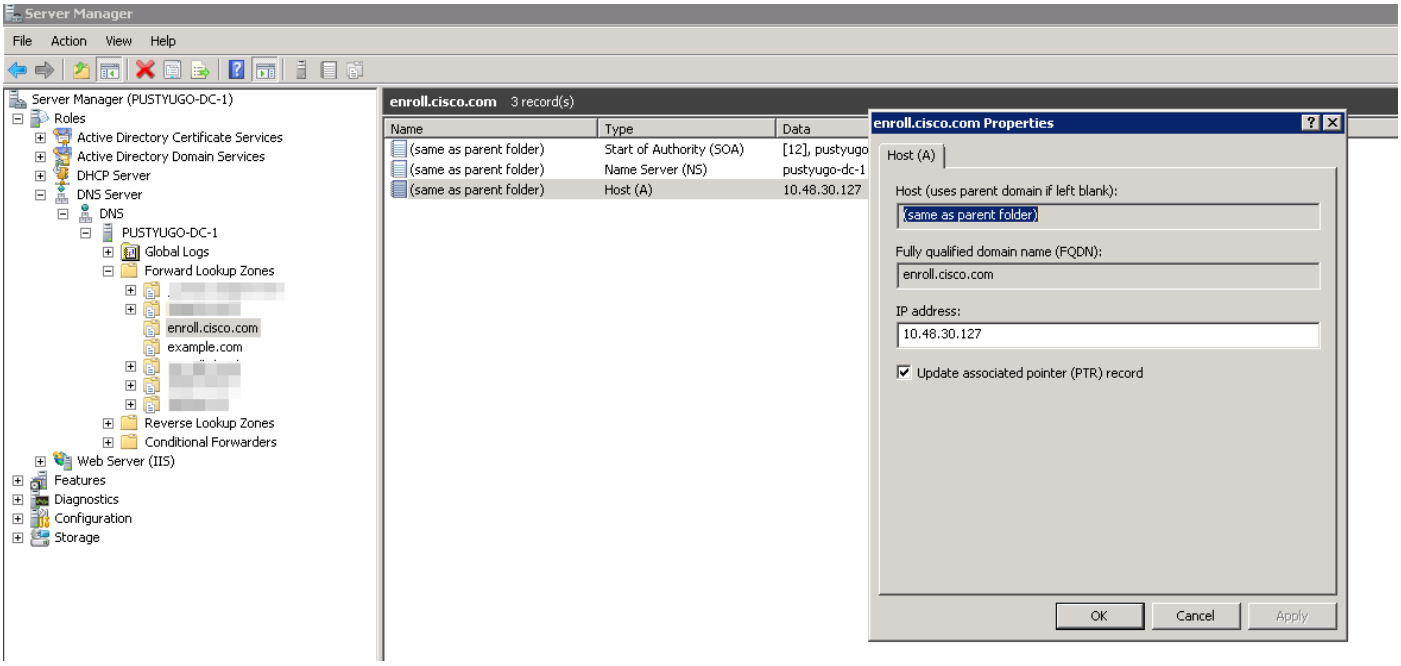


L'utente VPN avrà accesso al server (10.0.0.10) solo se è conforme allo stato.

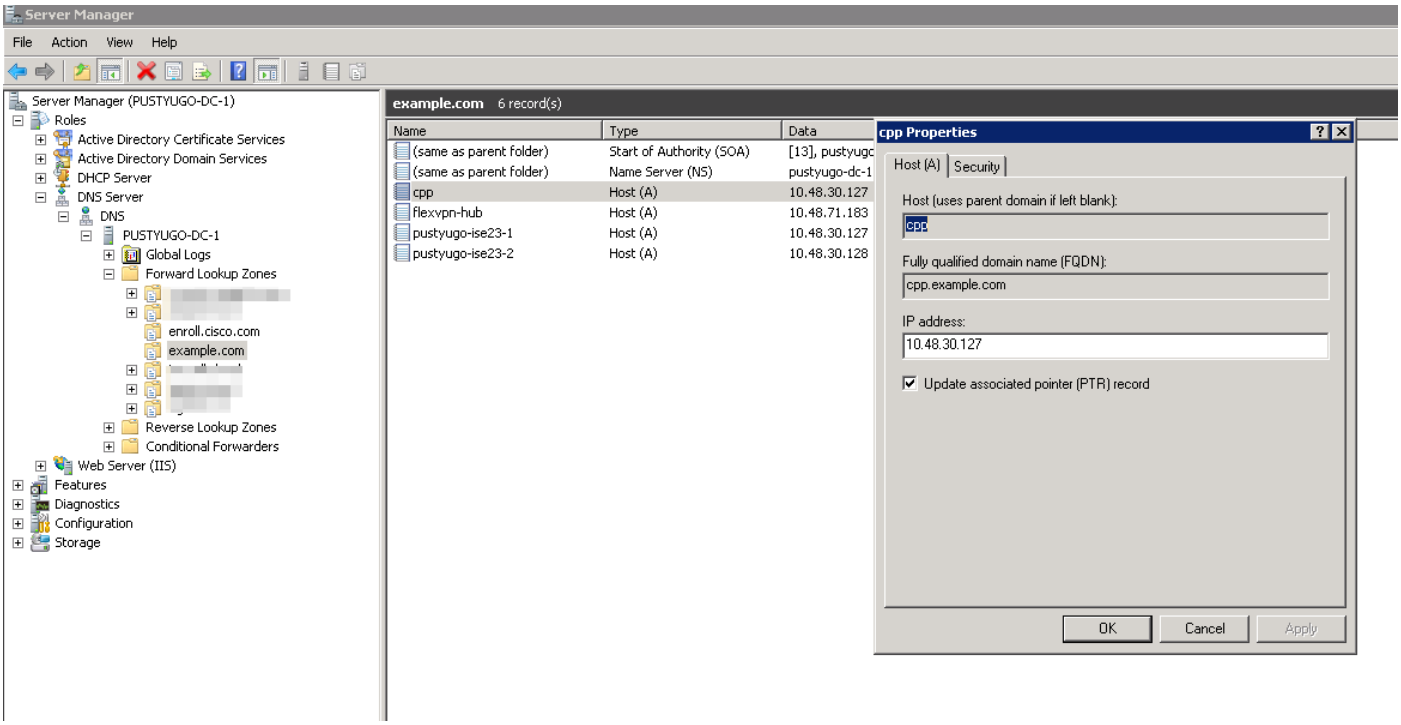
Configurazione server DNS

In questo documento Windows Server 2008 R2 viene utilizzato come server DNS.

Passaggio 1. Aggiungere il record **dell'host (A)** per **enroll.cisco.com** che punta all'**IP del PSN**:



Passaggio 2. Aggiungere il record **host (A)** per l'FQDN del PCP (**cpp.example.com** utilizzato in questo esempio) che punta all'**IP del PSN**:



Configurazione iniziale di IOS XE

Configura certificato di identità

Il router utilizzerà un certificato per autenticarsi al client Anyconnect. Il certificato del router deve essere considerato attendibile dal sistema operativo dell'utente in modo da evitare avvisi relativi al certificato durante la fase di connessione.

Il certificato di identità può essere fornito in uno dei modi seguenti:

> **Nota:** L'utilizzo di certificati autofirmati non è supportato con IKEv2 FlexVPN.

Opzione 1 - Configurare il server Autorità di certificazione (CA) sul router

> **Nota:** È possibile creare un server CA sullo stesso router IOS o su un altro router. In questo articolo la CA viene creata sullo stesso router.

> **Nota:** È necessario sincronizzare l'ora con il server NTP prima di abilitare il server CA.

> **Nota:** Si noti che l'utente non sarà in grado di verificare l'autenticità di questo certificato, pertanto i dati utente non saranno protetti da attacchi man-in-the-middle a meno che il certificato CA non venga verificato manualmente e importato nel computer dell'utente prima di stabilire la connessione.

Passaggio 1. Generare le chiavi RSA per il server CA:

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

Passaggio 2. Generare le chiavi RSA per il certificato di identità:

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

Verifica:

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

Passaggio 3. Configurare la 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
```

Verifica:

```
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
```

Passaggio 4. Configurare il trust point:

```
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
```

Passaggio 5. Autenticare la 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.
```

Passaggio 6. Registrazione del router nella 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
```

Controllare le richieste di certificati in sospeso nella CA e verificare che l'impronta digitale corrisponda a:

```
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
```

Passaggio 7. Concedere il certificato utilizzando il ReqID appropriato:

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

Attendere finché il router non richiede nuovamente il certificato (in base a questa configurazione verrà controllato 10 volte al minuto). Cerca messaggio syslog:

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

Verificare che il certificato sia installato:

```
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
```

Opzione 2 - Importare un certificato firmato esternamente

```
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)#
```

Configurare IKEv2

Passaggio 1. Configurare il server RADIUS e il 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
```

Passaggio 2. Configurare gli elenchi di autenticazione e autorizzazione:

```
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
```

Passaggio 3. Creare i criteri di autorizzazione ikev2:

```
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
```

Passaggio 4. Creare il profilo IKEv2:

```
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
```

Passaggio 5. Creare il set di trasformazioni e il profilo IPSec:

```
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
```

Passaggio 6. Creazione dell'interfaccia del modello virtuale:

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

Passaggio 7. Creare il pool locale:

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

Passaggio 8. Creare un ACL per limitare l'accesso dei client non conformi. Durante lo stato di postura sconosciuto devono essere fornite almeno le autorizzazioni seguenti:

- traffico DNS
- Traffico per ISE PSN tramite le porte 80, 443 e 8905
- Traffico verso i PSN ISE a cui punta l'FQDN del portale CPP
- Traffico verso i server di monitoraggio e aggiornamento, se necessario

Questo è un esempio di ACL senza server di monitoraggio e aggiornamento, con l'aggiunta dell'opzione di negazione esplicita per la rete 10.0.0.0/24 per ottenere visibilità, l'opzione implicita di "negazione ip any any" esiste alla fine dell'ACL:

```
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
```

Passaggio 9. Creare un ACL per consentire l'accesso ai client conformi:

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

Passaggio 10. Configurazione del tunnel suddiviso (facoltativo)

Per impostazione predefinita, tutto il traffico verrà indirizzato su VPN. Per eseguire il tunnel del traffico solo sulle reti specificate, è possibile specificarle nella sezione dei criteri di autorizzazione ikev2. È possibile aggiungere più istruzioni o utilizzare l'elenco degli accessi standard.

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

Passaggio 11. Accesso a Internet per client remoti (facoltativo)

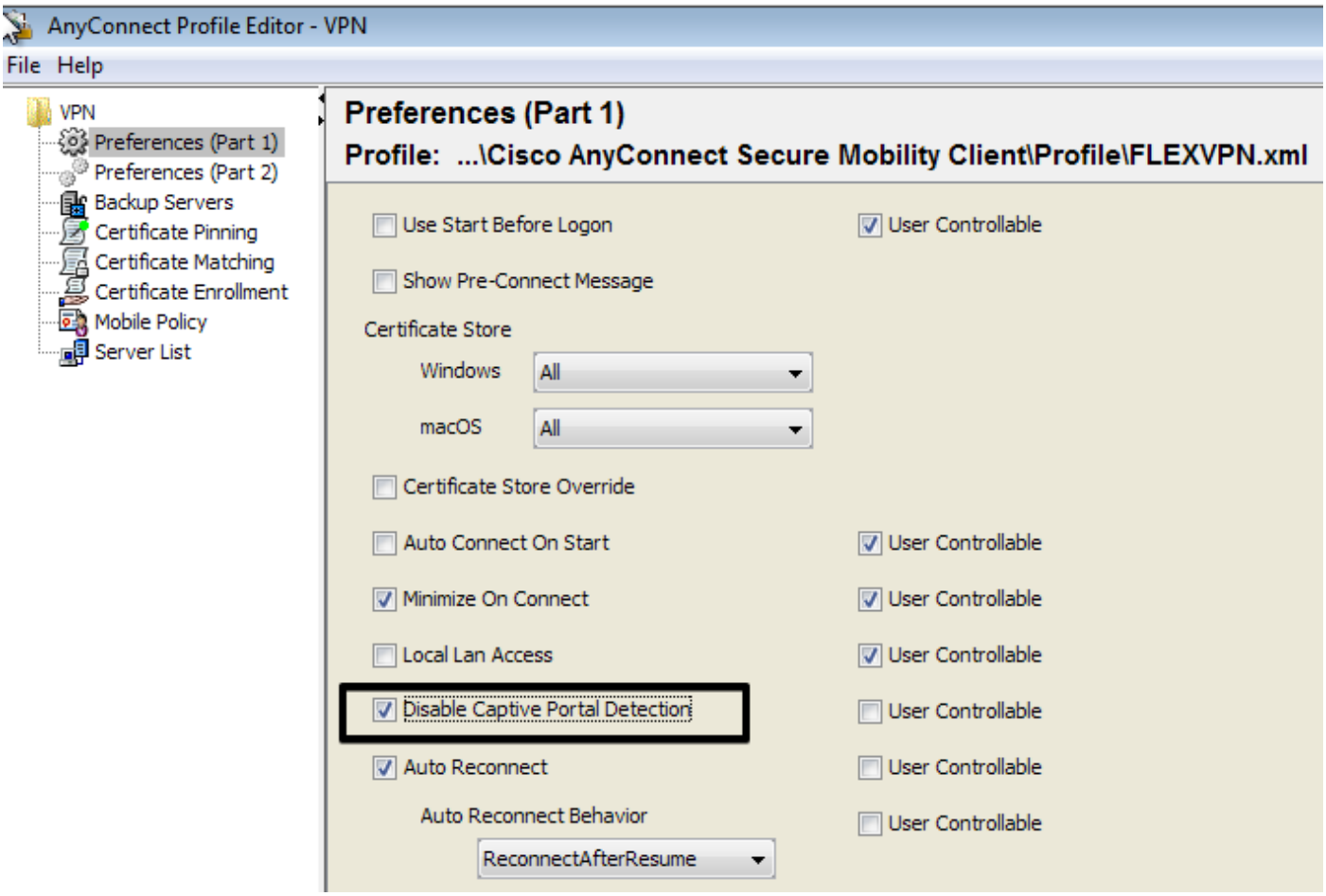
Affinché le connessioni in uscita dai client di accesso remoto agli host in Internet siano collegate tramite NAT all'indirizzo IP globale del router, configurare la conversione NAT:

```
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
```

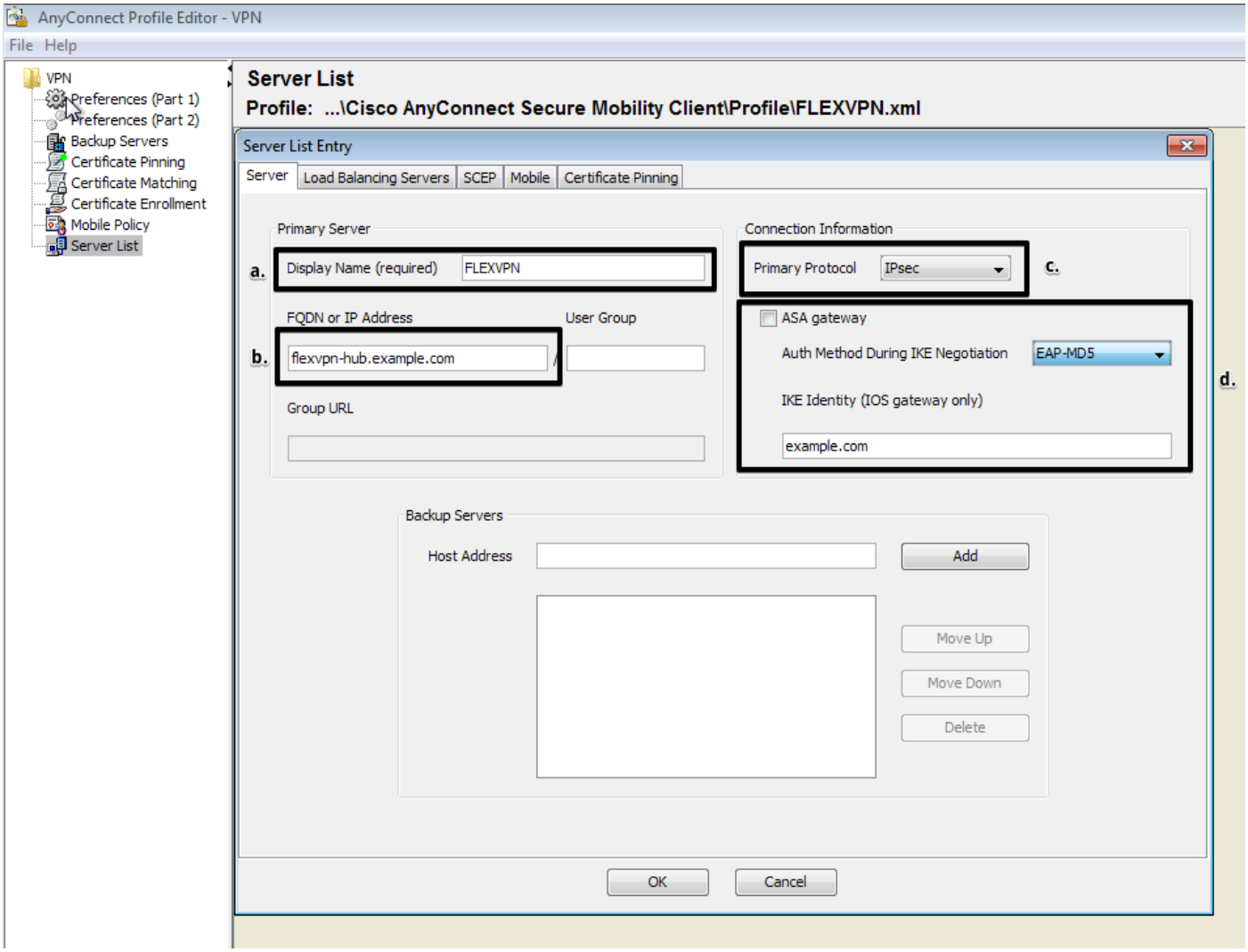
Configurazione profilo client Anyconnect

Configurare il profilo client utilizzando l'Editor profili AnyConnect. I profili di Anyconnect Security Mobile Client su Windows 7 e 10 sono salvati in **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile**.

Passaggio 1. Disabilitare la funzionalità di rilevamento dei portali vincolati. Se il server http non è disabilitato sull'hub FlexVPN, la funzione di rilevamento del portale captive di AnyConnect impedirà il completamento della connessione. Il server CA non funzionerà senza il server HTTP.



Passaggio 2. Configurare l'elenco dei server:



- Immettere il nome visualizzato.
- Immettere **FQDN** o **indirizzo IP** dell'hub FlexVPN.
- Selezionare **IPsec** come protocollo primario.
- Deselezionare la casella di controllo "ASA gateway" e specificare **EAP-MD5** come metodo di autenticazione. Immettere l'identità IKE esattamente uguale a quella della configurazione del profilo IKEv2 sull'hub FlexVPN (in questo esempio il profilo IKEv2 è configurato con il comando "match identity remote key-id example.com", quindi è necessario utilizzare **example.com** come identità IKE).

Passaggio 3. Salvare il profilo in **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile** e riavviare l'applicazione CA.

L'equivalente XML del profilo:

```
<?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>
```

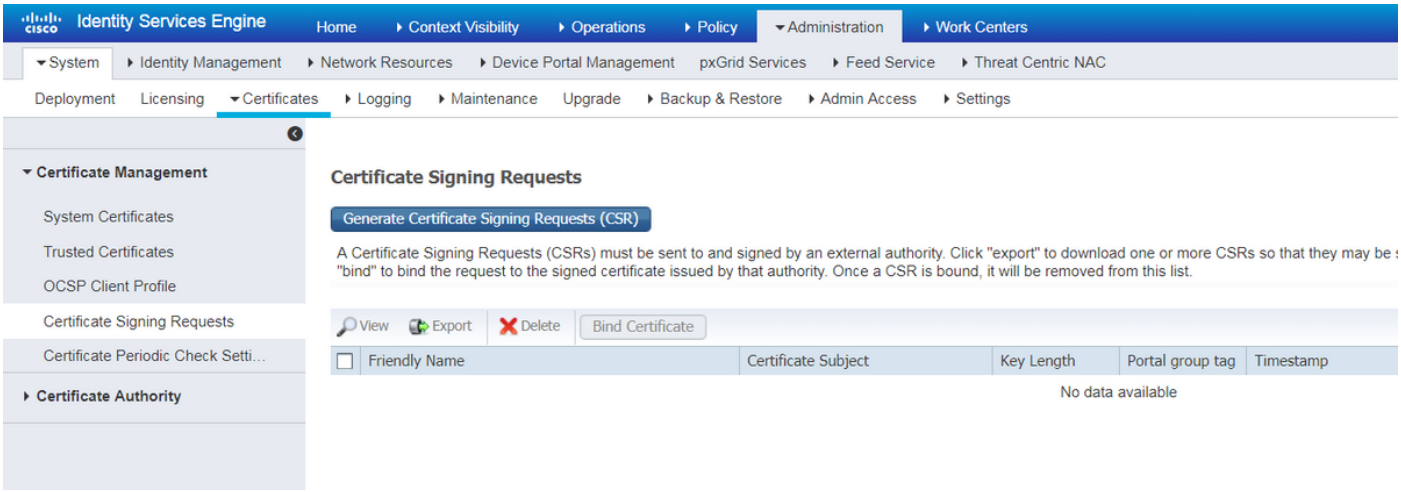
```
        <CertificateStore>All</CertificateStore>
        <CertificateStoreMac>All</CertificateStoreMac>
        <CertificateStoreOverride>false</CertificateStoreOverride>
        <ProxySettings>Native</ProxySettings>
        <AllowLocalProxyConnections>false</AllowLocalProxyConnections>
        <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>
```

Configurazione di ISE

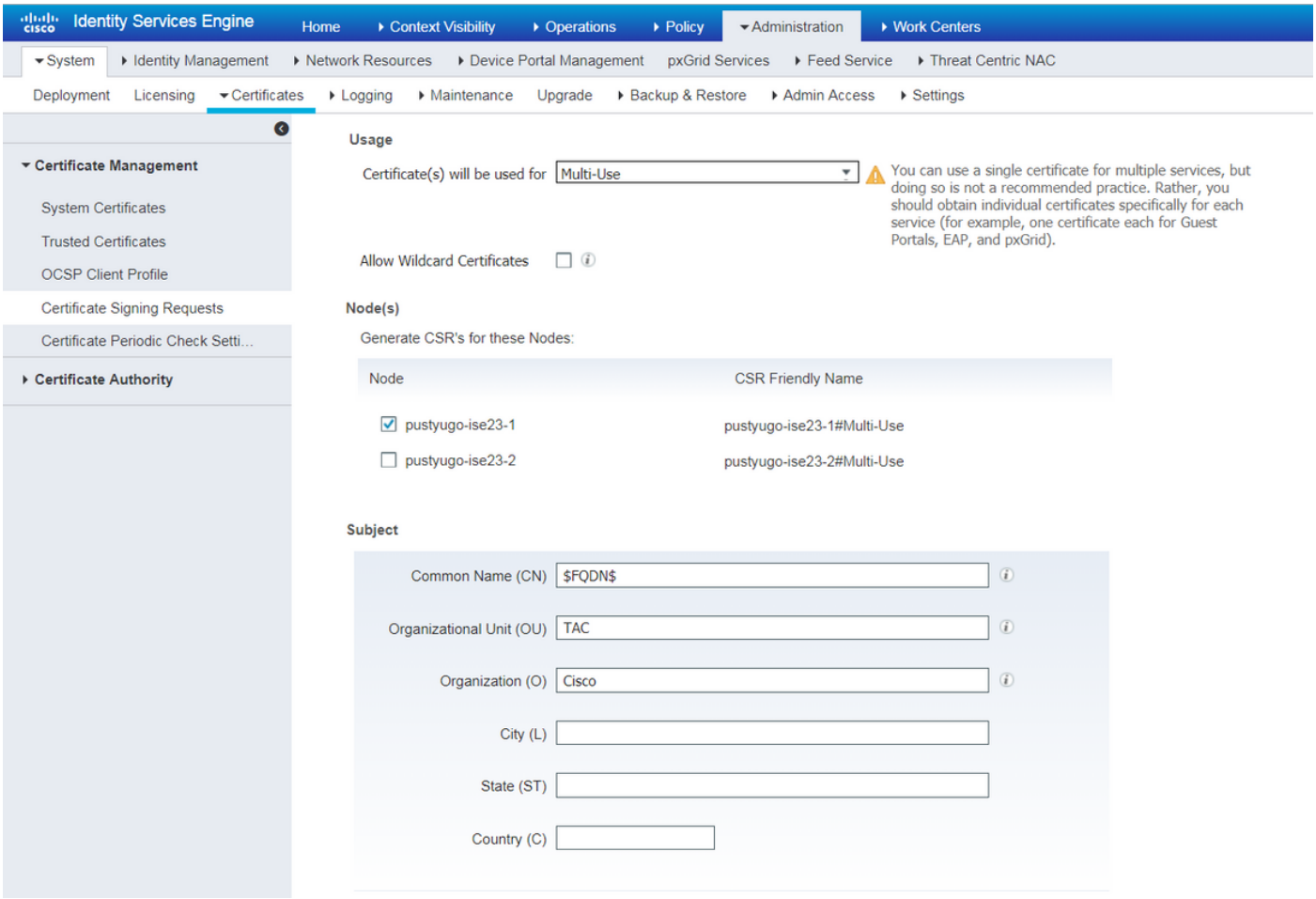
Configurazione dei certificati Amministratore e CPP

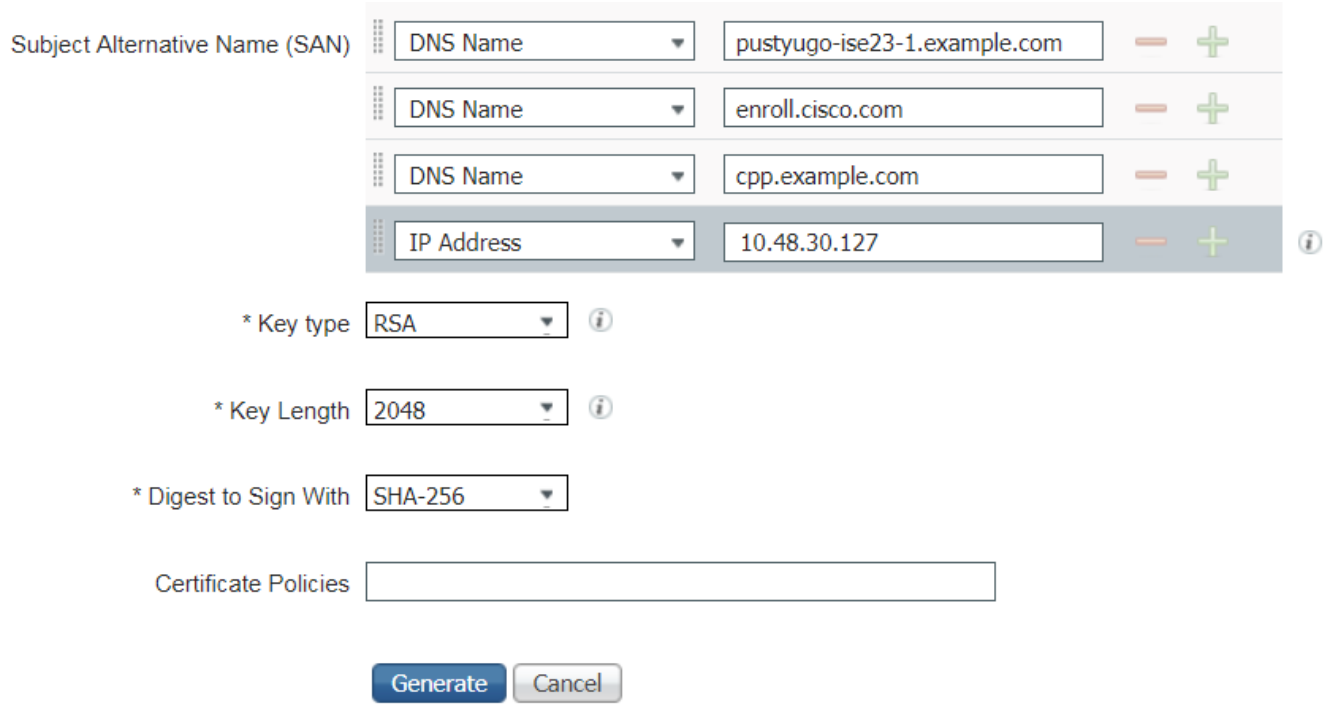
> **Nota:** La modifica del certificato di amministrazione comporta il riavvio del nodo in cui il certificato è stato modificato.

Passaggio 1. Accedere ad **Amministrazione -> Sistema -> Certificati -> Richieste di firma del certificato,** quindi fare clic su **Genera richieste di firma del certificato (CSR):**



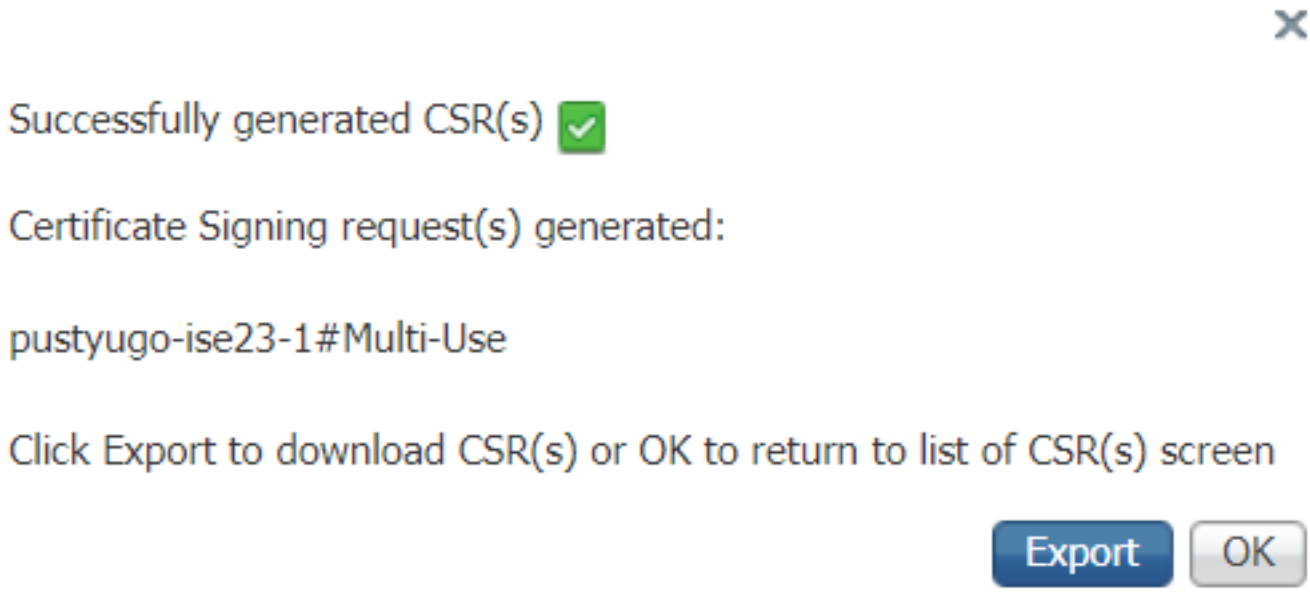
Passaggio 2. Nella pagina aperta selezionare il nodo PSN necessario, compilare i campi necessari e aggiungere il nome di dominio completo del nodo, enroll.cisco.com, cpp.example.com e l'indirizzo IP del nodo nei campi SAN e fare clic su **Genera**:





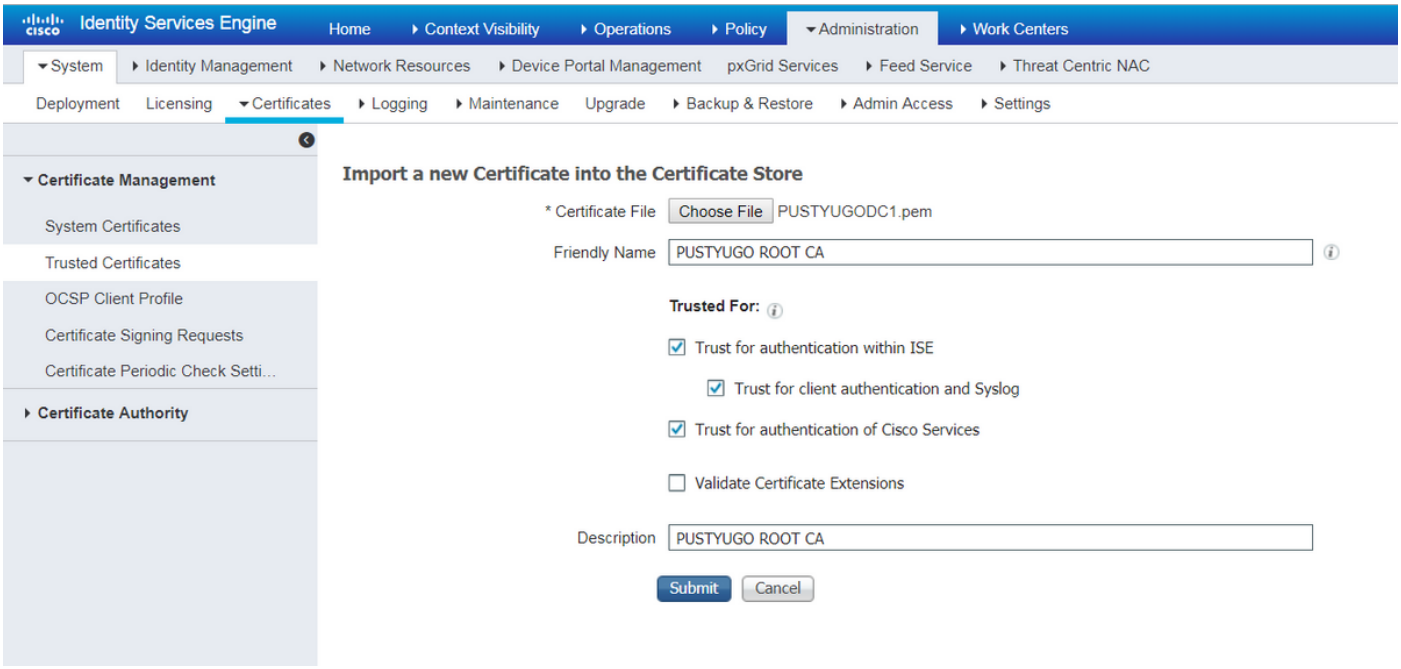
Nota: Se si seleziona **Multiuso** in questo passaggio, è possibile utilizzare lo stesso certificato anche per Portal.

Nella finestra visualizzata, fare clic su **Esporta** per salvare il CSR in formato pem nella workstation locale:



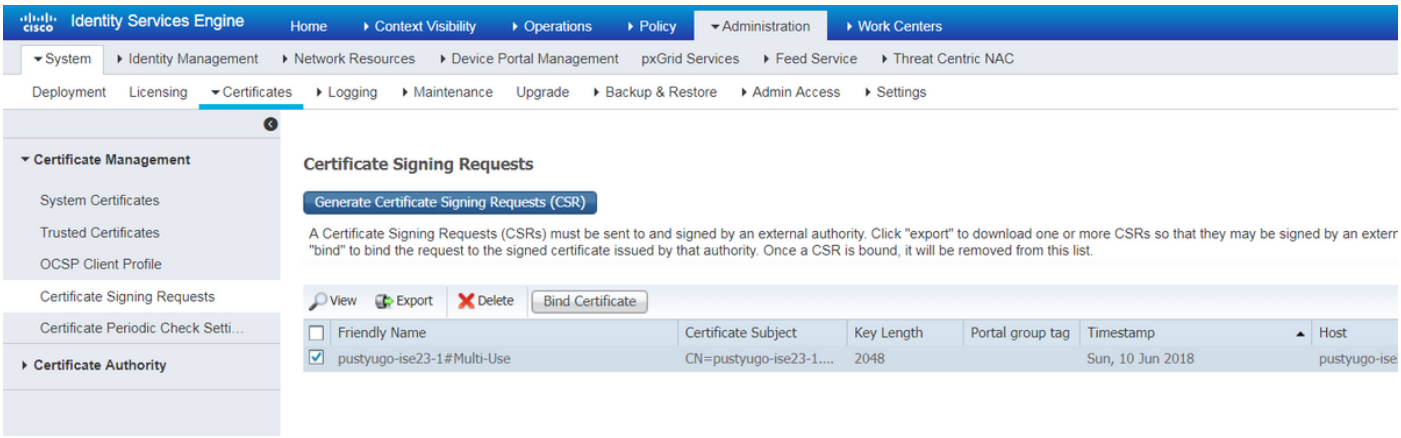
Passaggio 3. Firmare il CSR con un'autorità di certificazione attendibile e ottenere il file di certificato dall'autorità di certificazione, nonché la catena completa di certificati dell'autorità di certificazione (radice e intermedia).

Passaggio 4. Accedere ad **Amministrazione -> Sistema -> Certificati -> Certificati attendibili**, quindi fare clic su **Importa. Nella schermata successiva fare clic su Choose file** (Scegli file) e selezionare **Root CA** certificate file (File certificato CA radice), inserire Nome descrittivo e Descrizione se necessario, selezionare le opzioni **Trusted For** necessarie e fare clic su **Submit (Invia):**

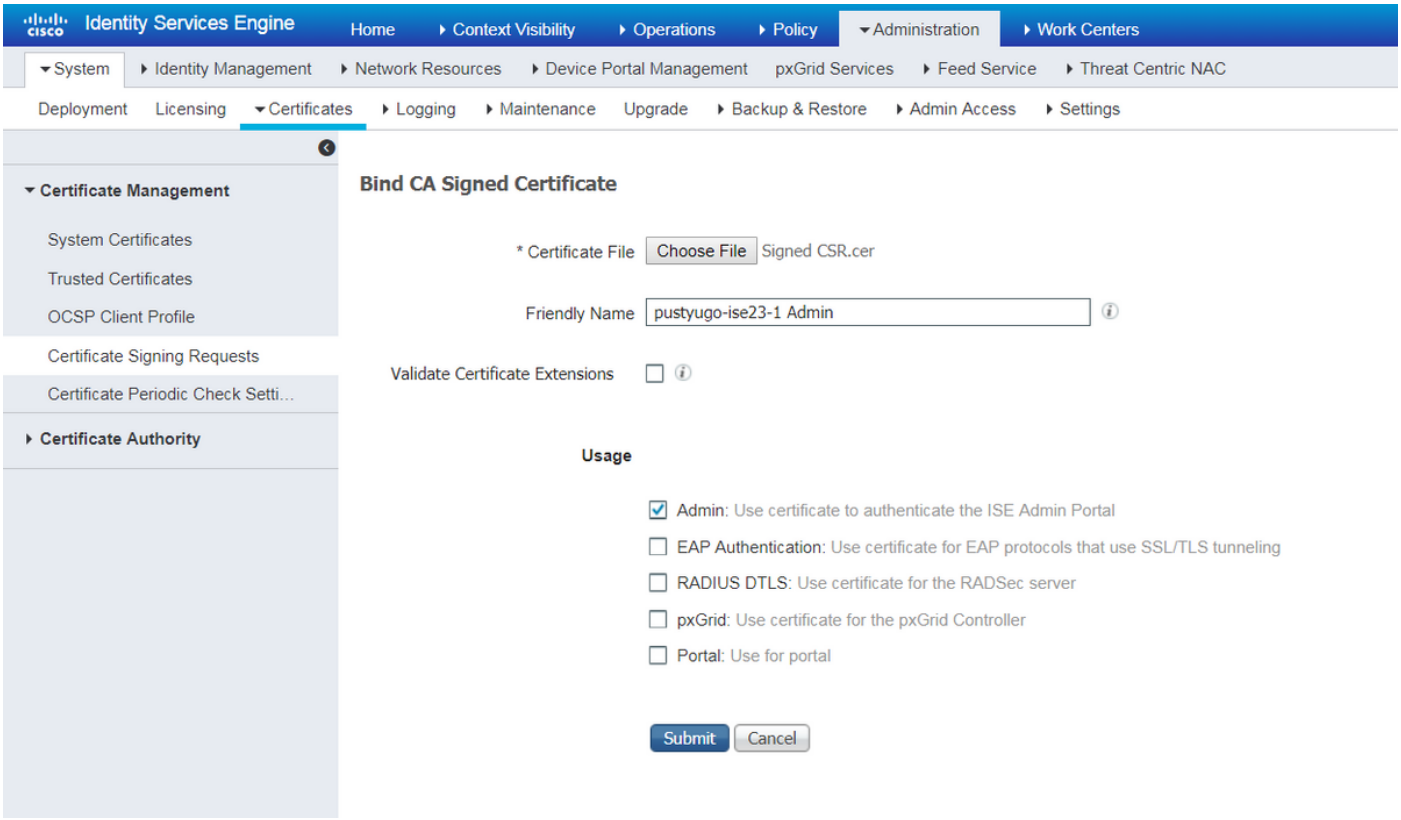


Ripetere questo passaggio per tutti i certificati intermedi nella catena, se presenti.

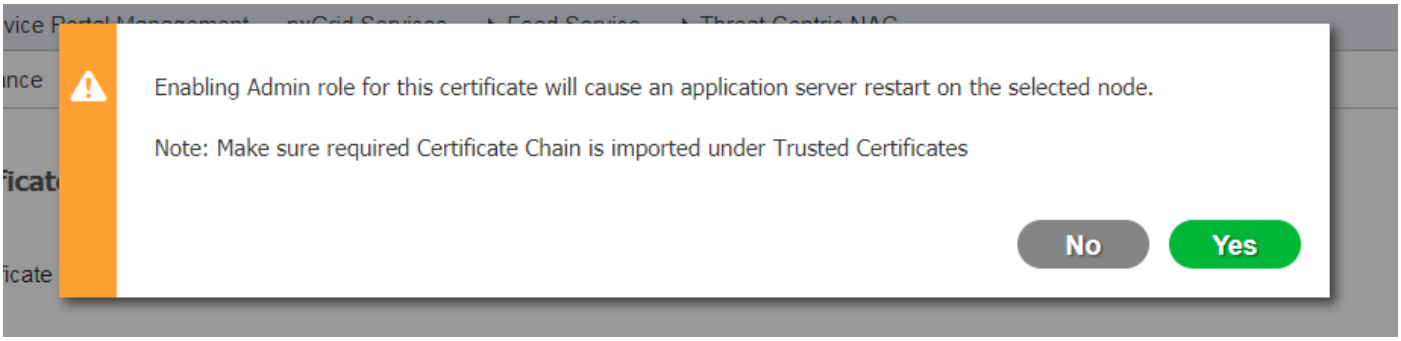
Passaggio 5. Tornare ad **Amministrazione -> Sistema -> Certificati -> Richieste di firma del certificato,** selezionare CSR necessario e fare clic su **Associa certificato:**



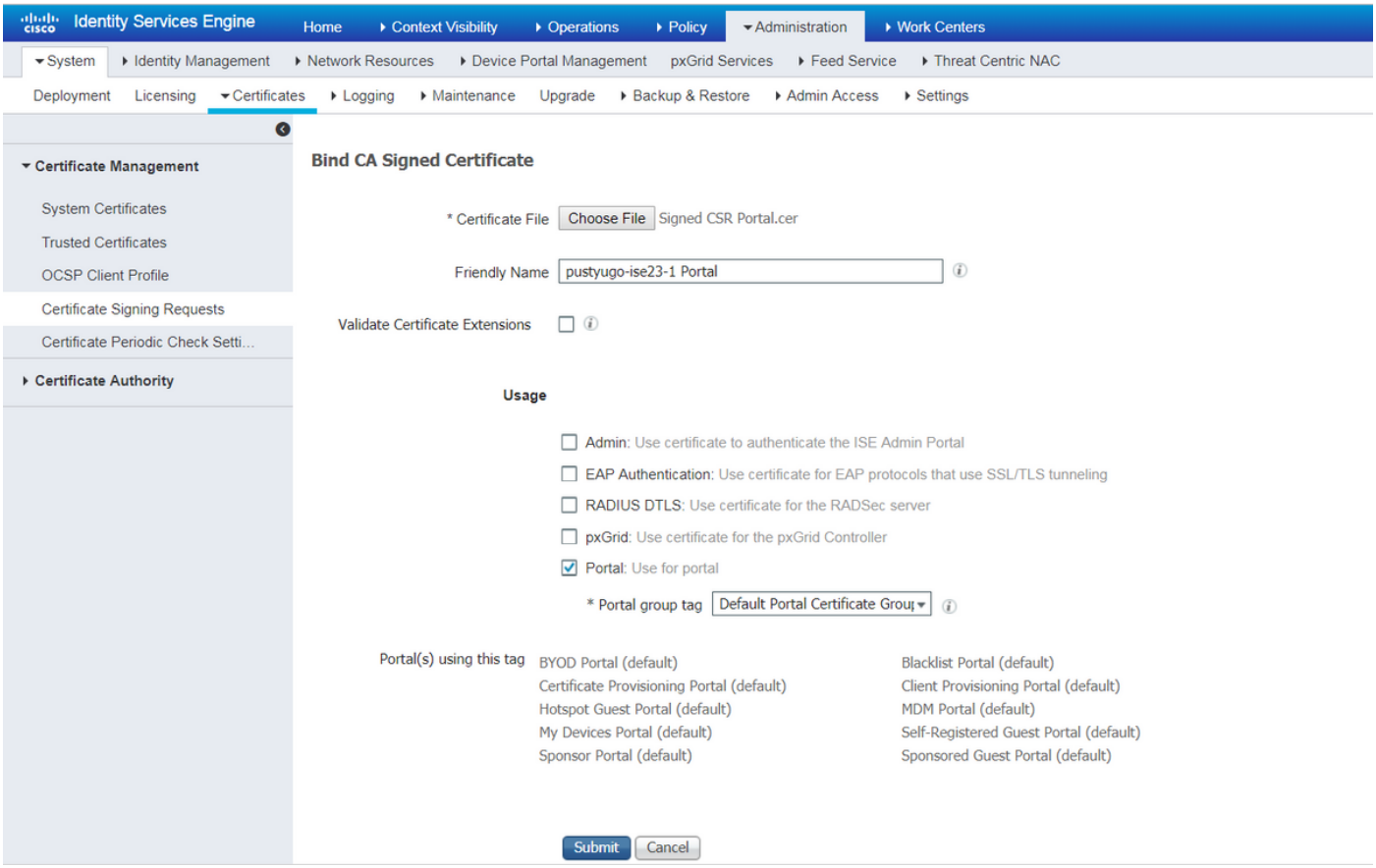
Passaggio 6. Nella pagina aperta fare clic su **Scegli file**, selezionare il file del certificato ricevuto dall'autorità di certificazione, immettere Nome descrittivo, se necessario, quindi selezionare **Uso: Admin** (**Sintassi: Il portale** può essere selezionato anche qui se il CSR è stato creato con **multiuso**) e fare clic su **Invia**:



Passaggio 7. Nel popup di avviso fare clic su **Sì** per completare l'importazione. Il nodo interessato dalla modifica del certificato di amministrazione verrà riavviato:



Ripetere i passaggi per la modifica del certificato CPP se si decide di utilizzare un certificato separato per il portale. Nel passo 6, selezionare **Uso: Portal** e fare clic su **Submit:**

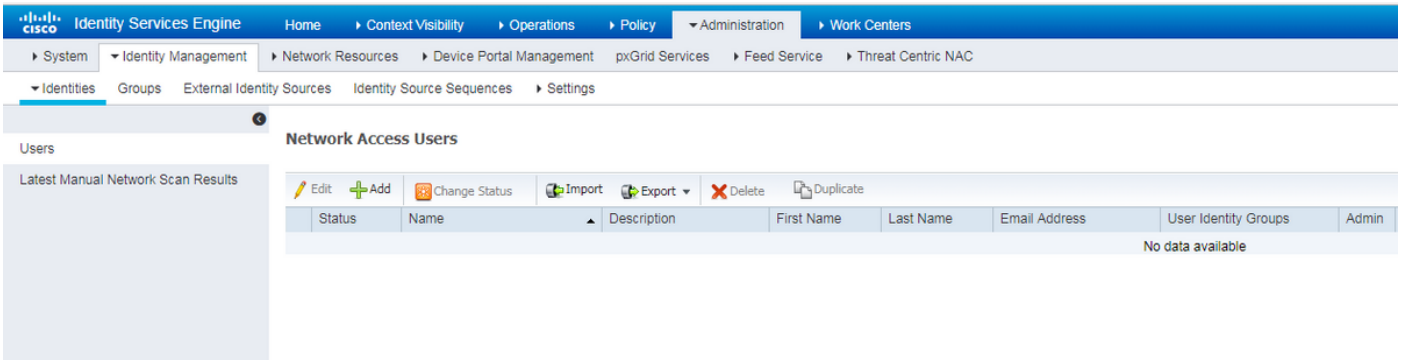


Ripetere i passaggi per tutti i nomi PSN nella distribuzione ISE.

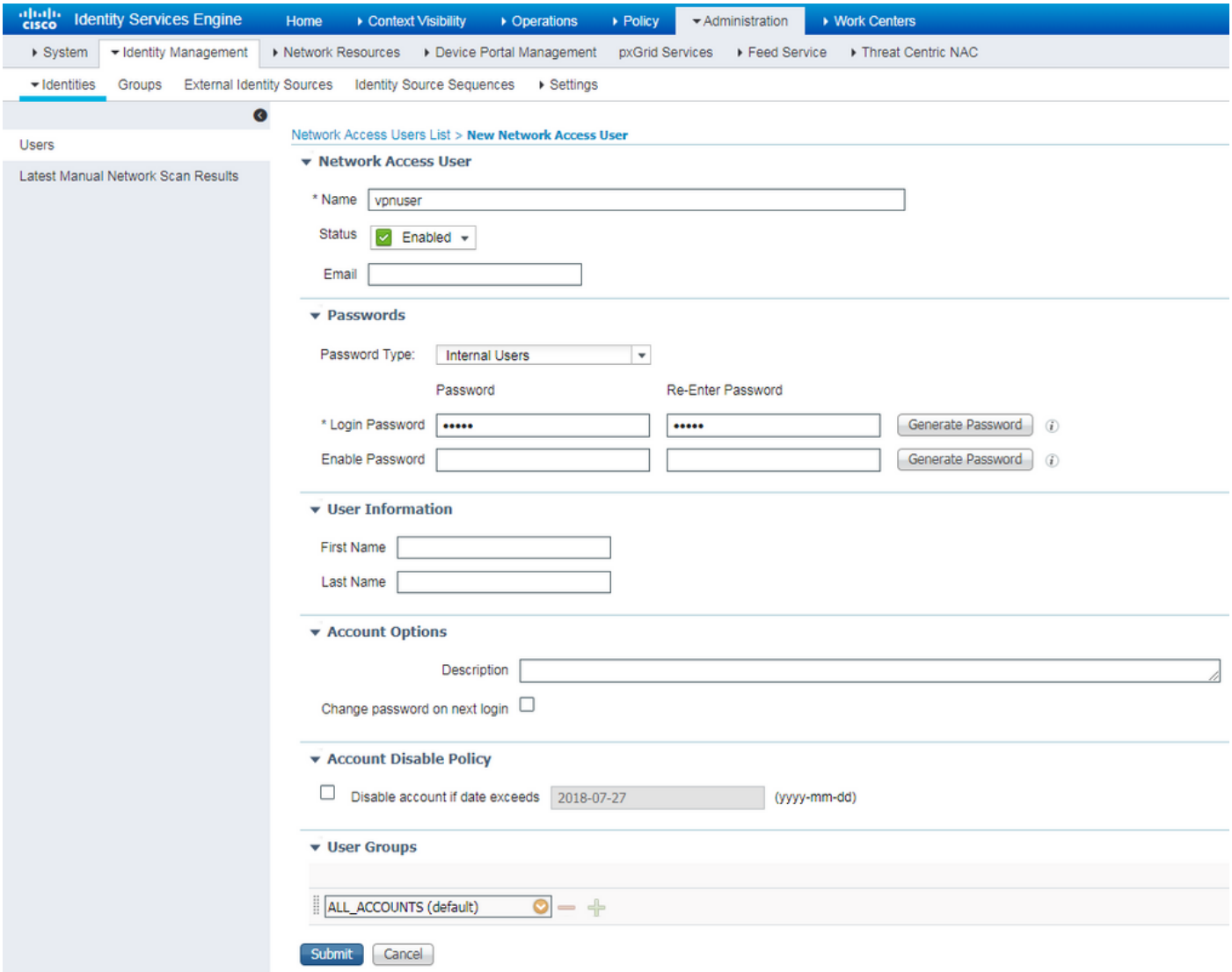
Creare un utente locale su ISE

> **Nota:** Con il metodo EAP-MD5, ISE supporta solo gli utenti locali.

Passaggio 1. Accedere ad **Amministrazione -> Gestione delle identità -> Identità -> Utenti**, quindi fare clic su **Aggiungi**.

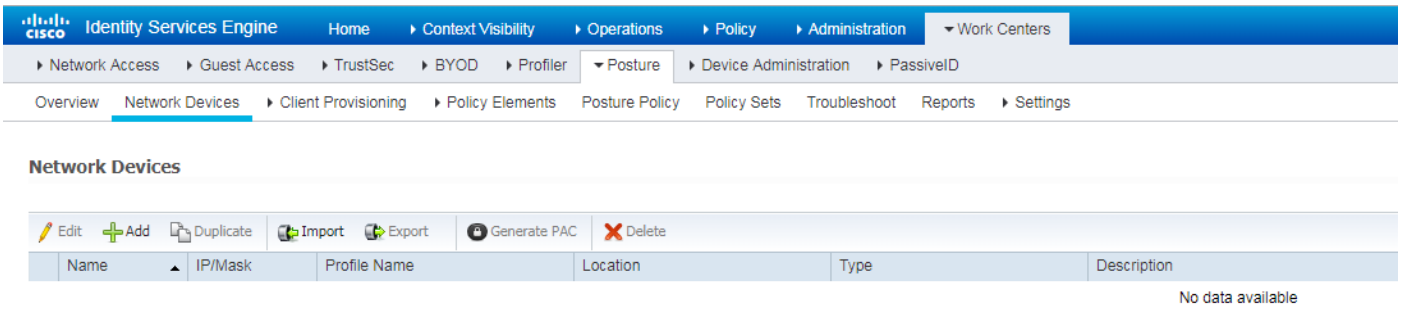


Passaggio 2. Nella pagina aperta immettere nome utente, password e altre informazioni necessarie e fare clic su **Invia**.

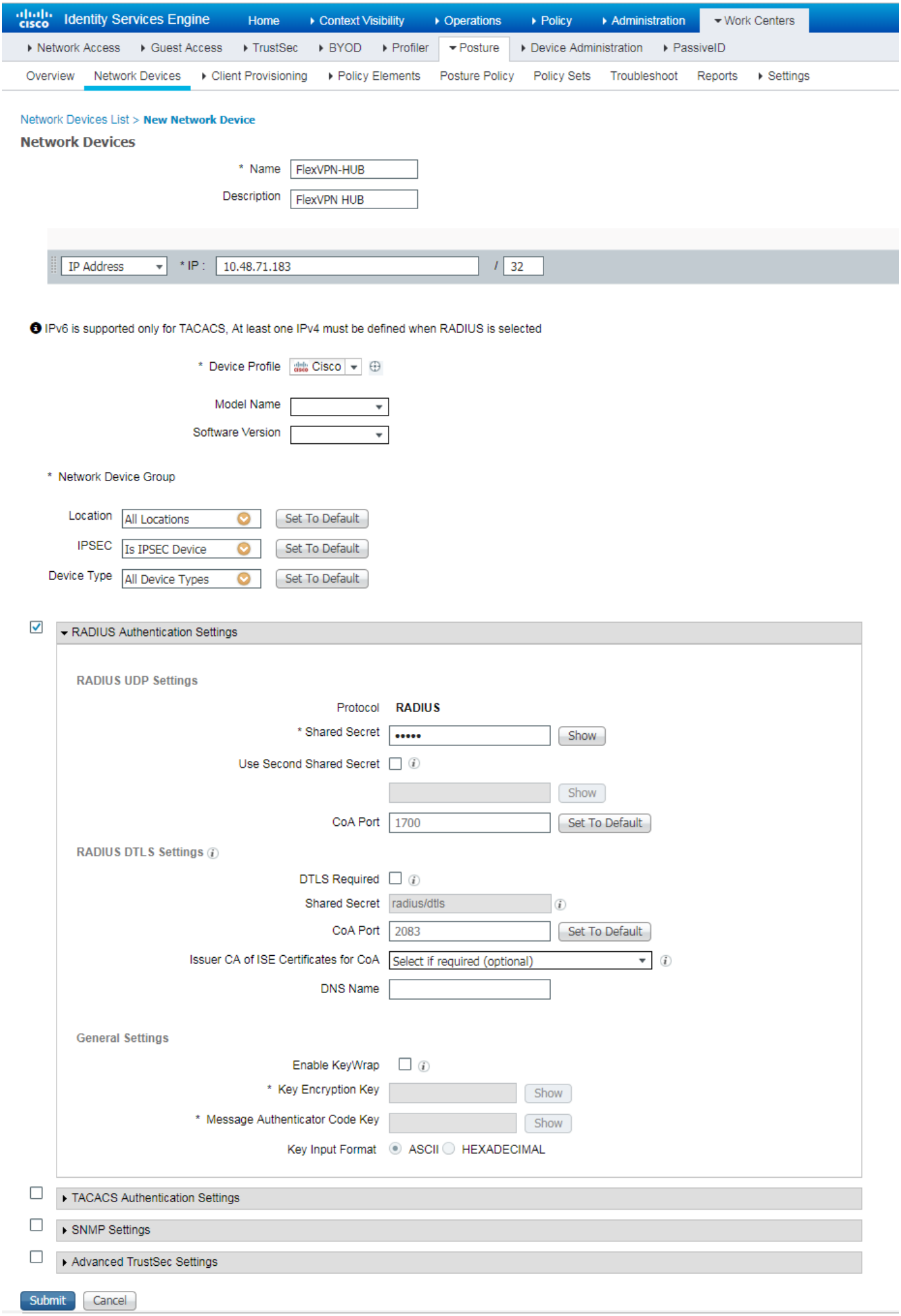


Aggiungere l'HUB FlexVPN come client Radius

Passaggio 1. Accedere a **Centri di lavoro -> Postura -> Dispositivi di rete**, quindi fare clic su **Aggiungi**.



Passaggio 2. Nella pagina aperta immettere Nome dispositivo, indirizzo IP e altre informazioni necessarie, selezionare la casella di controllo "Impostazioni autenticazione RADIUS", immettere il segreto condiviso e fare clic su **Invia** nella parte inferiore della pagina.

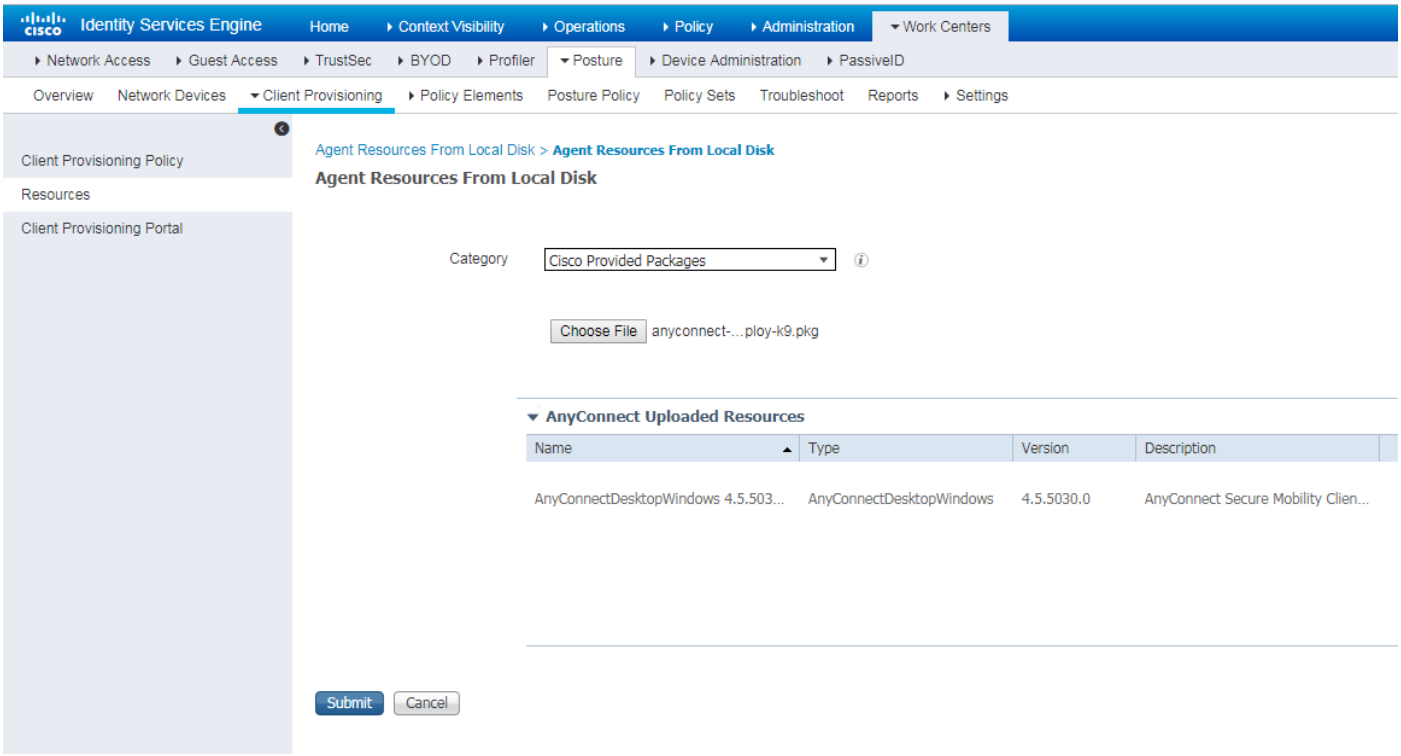

Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Network Access
Guest Access
TrustSec
BYOD
Profiler
Posture
Device Administration
PassiveID
Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Policy Sets
Troubleshoot
Reports
Settings
Network Devices 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

Configurazione provisioning client

Di seguito viene riportata la procedura per preparare la configurazione di Anyconnect.

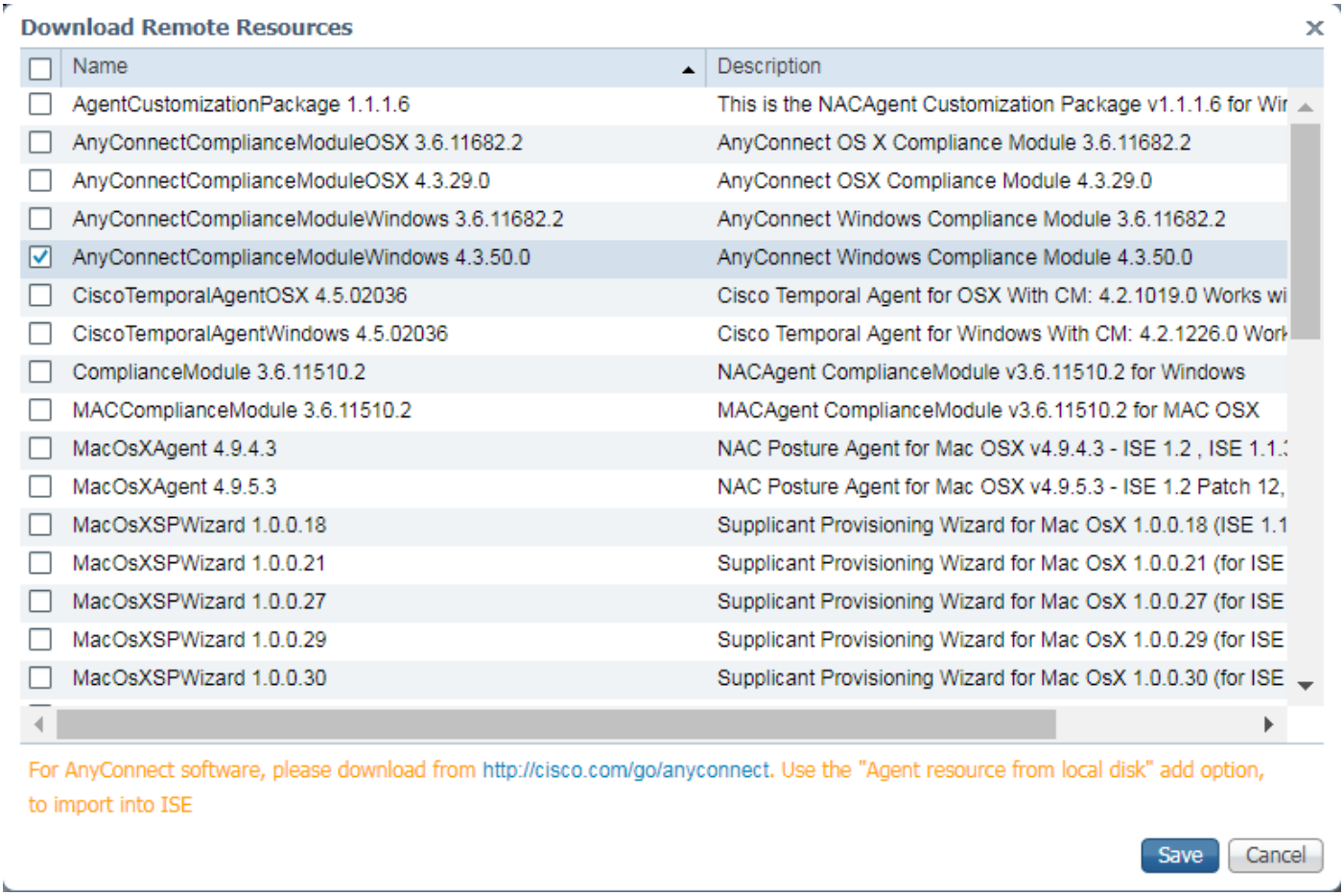
Passaggio 1. Download del pacchetto Anyconnect. Il pacchetto Anyconnect non è disponibile per il download diretto da ISE, quindi prima di iniziare, verificare che l'alimentazione sia disponibile sul PC. Questo collegamento può essere utilizzato per il download di CA - http://cisco.com/go/anyconnect. In questo documento viene usato il pacchetto anyconnect-win-4.5.05030-webdeploy-k9.pkg.

Passaggio 2. Per caricare il pacchetto di corrente alternata in ISE, passare a **Work Center -> Posture -> Client Provisioning ->** Resources e fare clic su **Add**. Scegliere **Risorse agente dal disco locale**. Nella nuova finestra selezionare **Cisco Provided Packages** (Pacchetti forniti da Cisco), fare clic su **Choose File** (Scegli file), quindi selezionare AC Package (Pacchetto CA) sul PC.

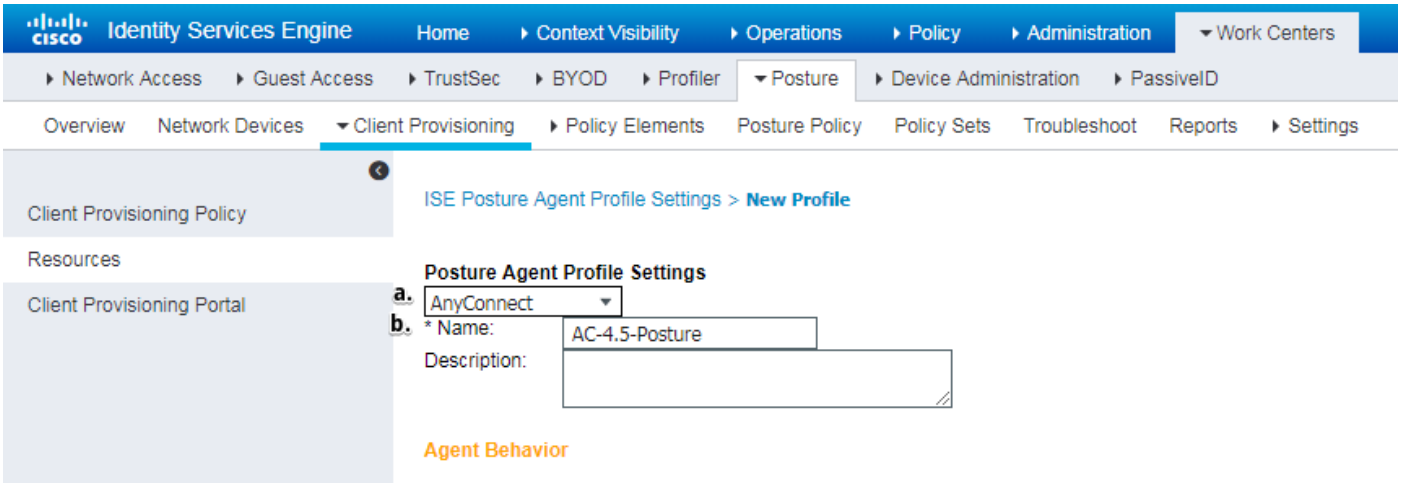


Fare clic su **Invia** per completare l'importazione. Verificare l'hash del pacchetto e premere **Confirm**.

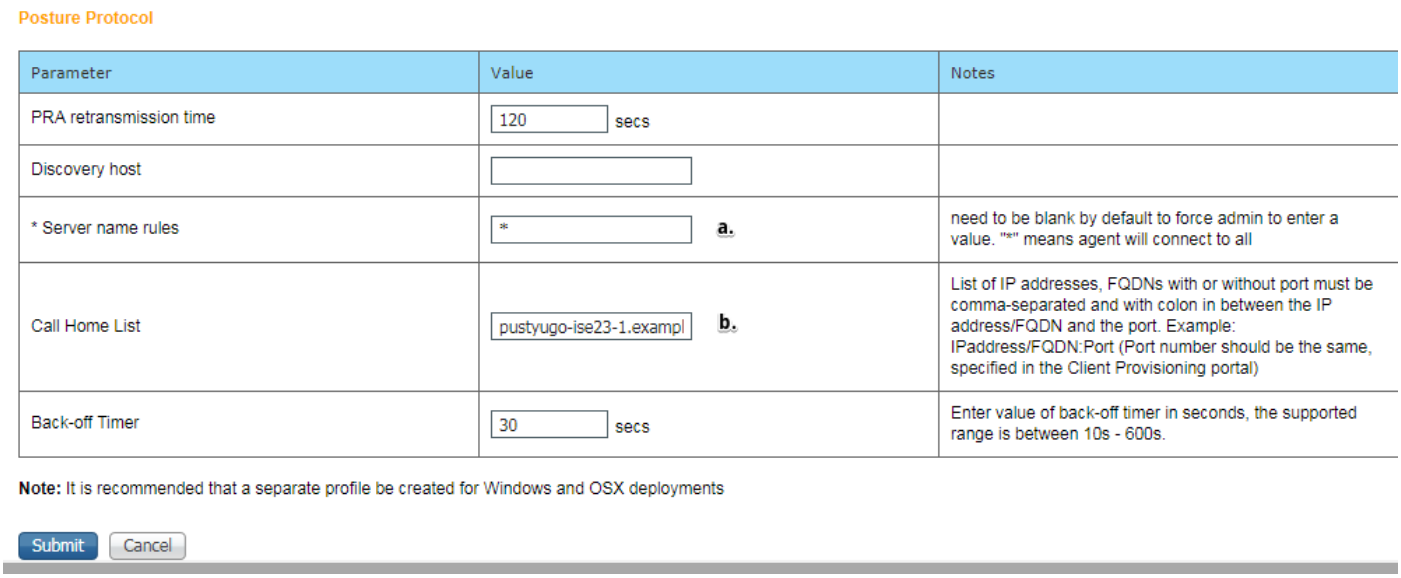
Passaggio 3. Il modulo sulla conformità deve essere caricato su ISE. Nella stessa pagina (**Centri di lavoro -> Postura -> Provisioning client -> Risorse**) fare clic su **Aggiungi** e scegliere **Risorse agente dal sito Cisco**. Nell'elenco delle risorse è necessario controllare un modulo di conformità e fare clic su **Salva**. Per questo documento AnyConnectComplianceModule Viene utilizzato il modulo di conformità di Windows 4.3.50.0.



Passaggio 4. A questo punto è necessario creare il profilo della postura CA. Fare clic su **Add** (Aggiungi), quindi selezionare **NAC agent** o **Anyconnect posture profile** (Profilo di postura Anyconnect).



- Scegliere il tipo di profilo. Per questo scenario, usare AnyConnect.
- Specificare il nome del profilo. Passare alla sezione **Protocollo postura** del profilo



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.

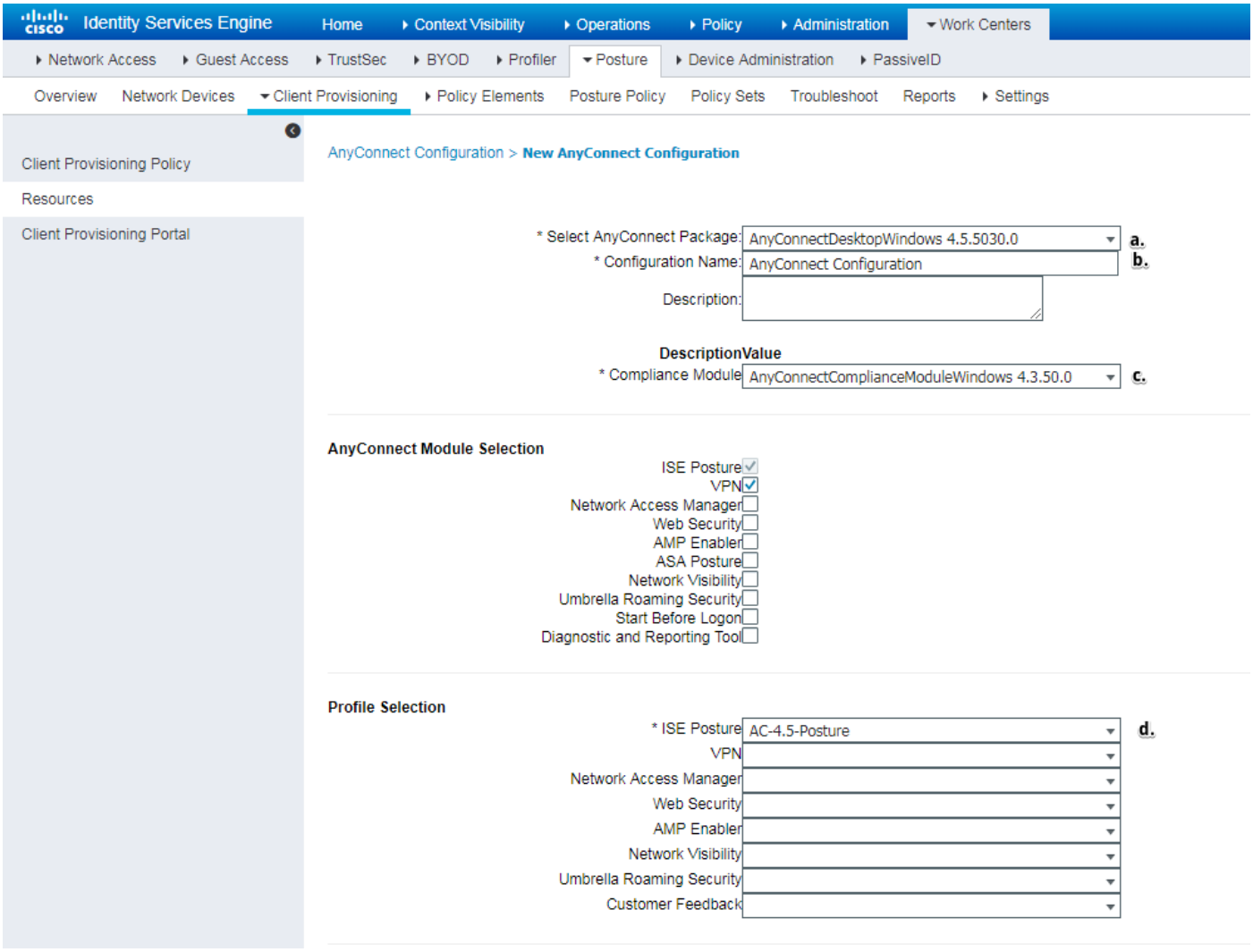
Note: It is recommended that a separate profile be created for Windows and OSX deployments

Submit Cancel

- Specificare **Regole nome server**. Questo campo non può essere vuoto. Il campo può contenere FQDN con caratteri jolly che limita la connessione del modulo di postura CA ai PSN dello spazio dei nomi appropriato. Inserire asterisco se è consentito un FQDN.

- I nomi e gli IP specificati qui sono in uso durante la fase 2 del rilevamento della postura (vedere il passo 14 della sezione "Flusso di postura in ISE 2.2"). È possibile separare i nomi tramite virgola e aggiungere un numero di porta dopo FQDN/IP utilizzando i due punti.

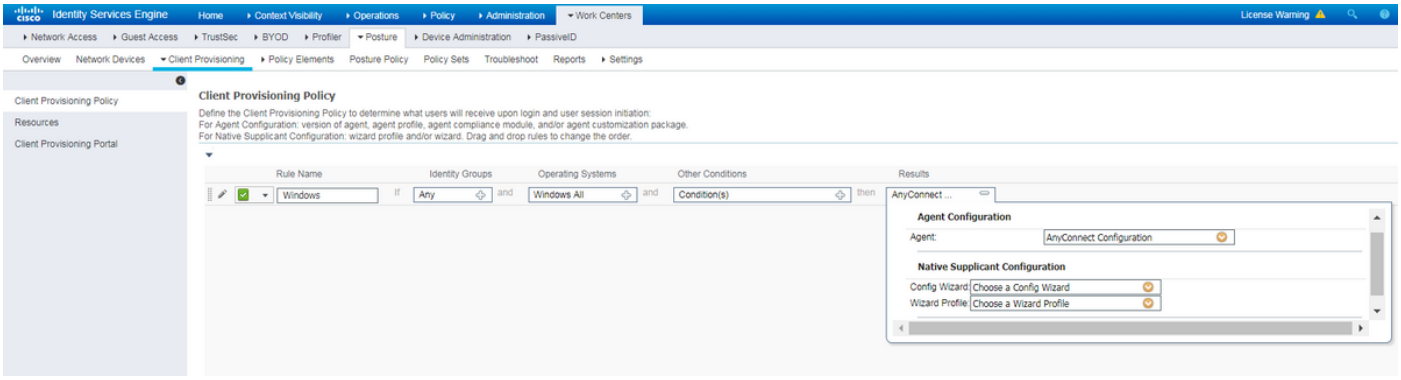
Passaggio 5. Creare la configurazione CA. Passare a **Centri di lavoro -> Postura -> Provisioning client -> Risorse** e fare clic su **Aggiungi**, quindi selezionare **Configurazione AnyConnect**.



- Selezionare la confezione CA.
- Specificare il nome della configurazione CA.
- Scegliere la versione del modulo di conformità.
- Selezionare il profilo di configurazione della postura CA dall'elenco a discesa.

Passaggio 6. Configurare i criteri di provisioning client. Passare a **Centri di lavoro -> Postura -> Provisioning client**. In caso di configurazione iniziale è possibile inserire valori vuoti nei criteri presentati con i valori predefiniti. Per aggiungere i criteri alla configurazione di postura esistente, passare ai criteri che possono essere riutilizzati e scegliere **Duplica sopra** o **Duplica sotto.** Si possono anche creare nuove regole.

Questo è l'esempio del criterio utilizzato nel documento.

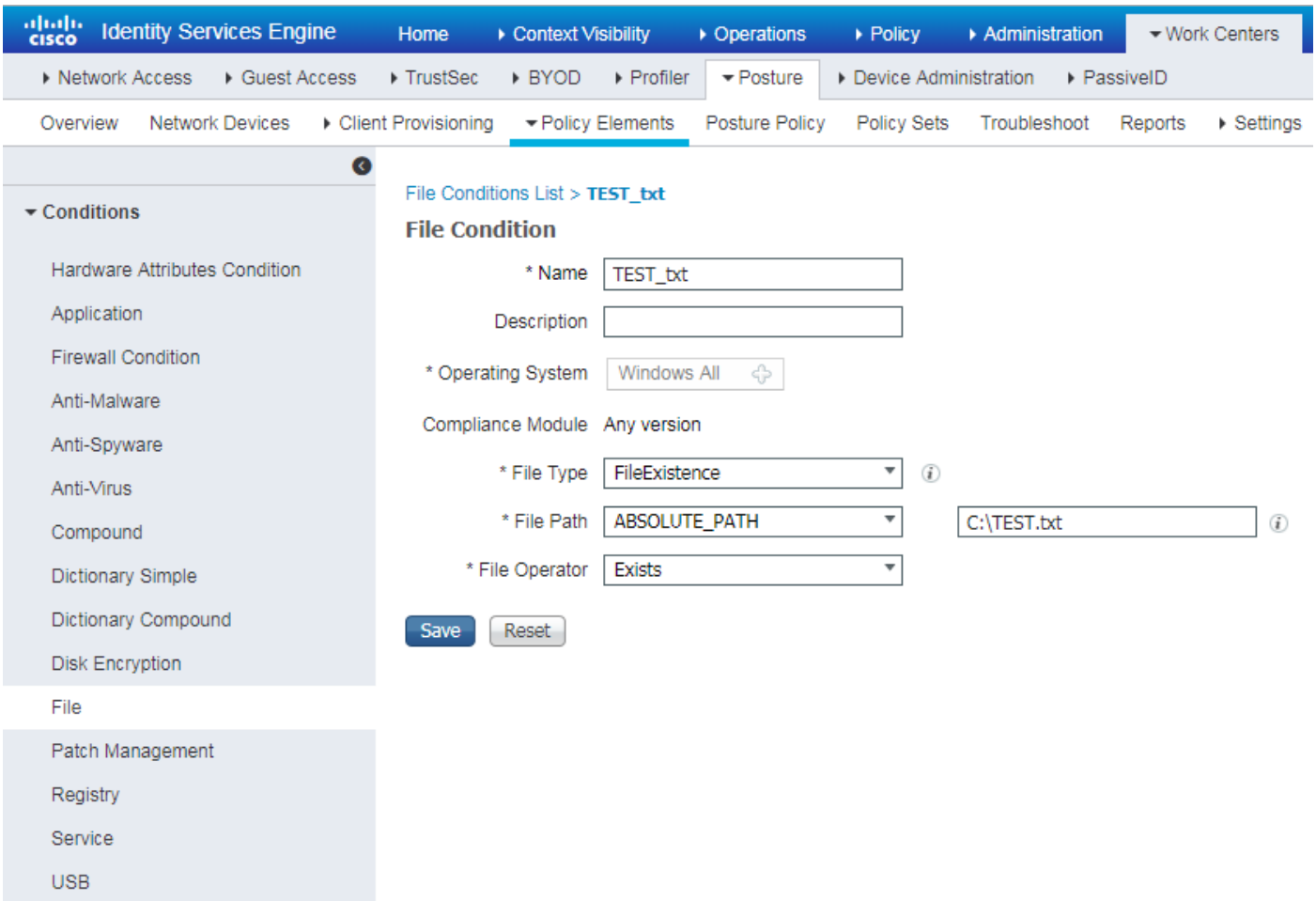


Scegliere la configurazione CA nella sezione dei risultati.

Criteri e condizioni di postura

Viene utilizzato un semplice controllo della postura. ISE è configurato per verificare l'esistenza del file C:\TEST.txt sul lato del dispositivo terminale. Gli scenari reali possono essere molto più complicati, ma i passaggi di configurazione generali sono gli stessi.

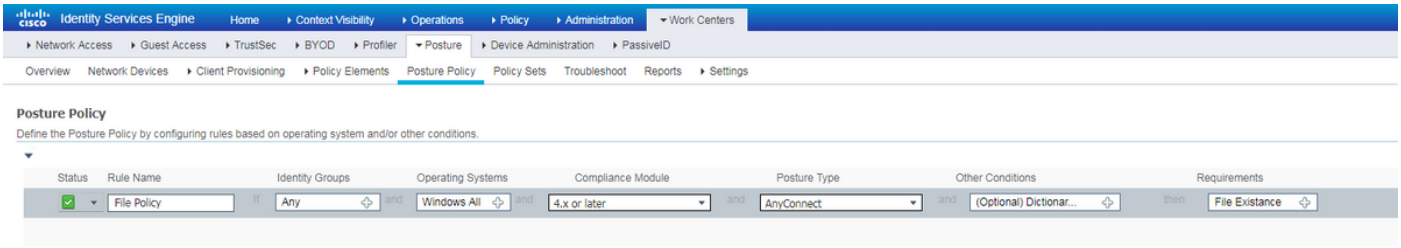
Passaggio 1. Creare una condizione di postura. Le condizioni di postura si trovano in **Centri di lavoro -> Postura -> Elementi della politica -> Condizioni**. *Selezionate il tipo di condizione di postura e fate clic su* **Aggiungi (Add)**. Specificare le informazioni necessarie e fare clic su **Salva**. Di seguito è riportato un esempio di condizione del servizio che verifica se il file C:\TEST.txt esiste.



Passaggio 2. Configurazione dei requisiti di postura. Passare a **Centri di lavoro -> Postura -> Elementi criteri -> Requisiti**. Questo è un esempio di esistenza del file TEST.txt:

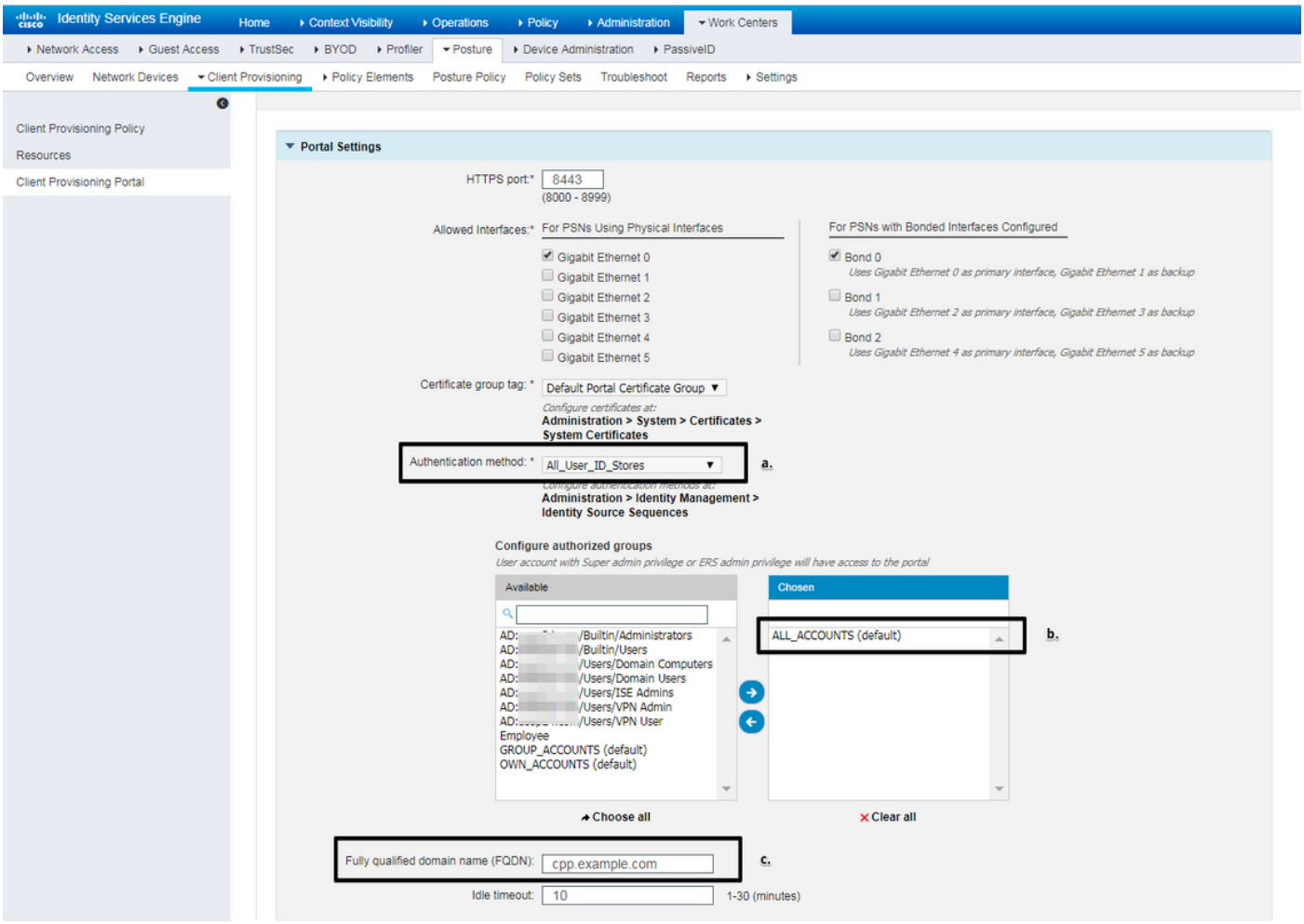
Scegliere la condizione di postura in un nuovo requisito e specificare un'azione di correzione.

Passaggio 3. Configurazione dei criteri di postura. Passare a **Centri di lavoro -> Postura -> Criteri di postura**. Di seguito sono riportati alcuni esempi di criteri utilizzati per questo documento. Ai criteri è assegnato il requisito di "esistenza file" come obbligatorio e non sono assegnate altre condizioni.



Configura portale di provisioning client

Per la postura senza reindirizzamento, è necessario modificare la configurazione del portale di provisioning client. Passare a **Centri di lavoro -> Postura -> Provisioning client -> Portale di provisioning client** È possibile utilizzare il portale predefinito o crearne uno personalizzato.



Tali impostazioni devono essere modificate nella configurazione del portale per lo scenario di non reindirizzamento:

- In Autenticazione specificare la sequenza di origine dell'identità da utilizzare se SSO non è in grado di individuare la sessione per l'utente.

- In base all'elenco di gruppi disponibili della sequenza di origine identità selezionata, viene compilato. A questo punto è necessario selezionare i gruppi autorizzati per l'accesso al portale.

- Ènecessario specificare il nome di dominio completo del portale di provisioning client. Questo FQDN deve essere risolvibile in IP di ISE PSN. Durante il primo tentativo di connessione, gli utenti devono essere informati di specificare il FQDN nel Web browser.

Configura profili e criteri di autorizzazione

Ènecessario limitare l'accesso iniziale del client quando lo stato di postura non è disponibile. Questo obiettivo può essere raggiunto in diversi modi:

- ID filtro raggio: con questo attributo, è possibile assegnare all'utente con stato di postura sconosciuto un ACL definito localmente su NAD. Poiché si tratta di un attributo RFC standard, questo approccio dovrebbe funzionare correttamente per tutti i fornitori di servizi di supporto all'installazione e alla distribuzione.

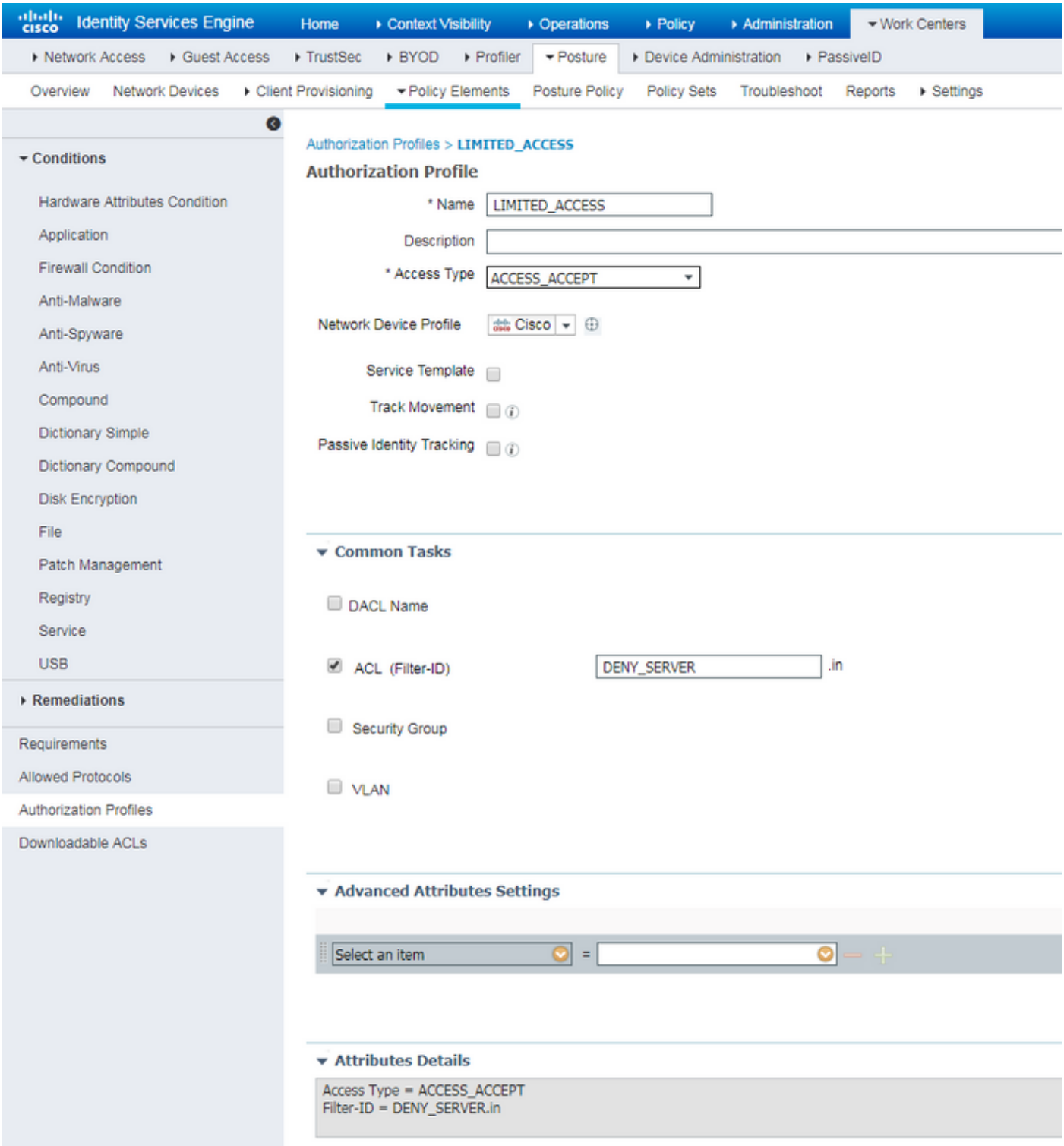
- Cisco:cisco-av-pair = ip:interface-config - molto simile a Radius Filter-Id, è possibile assegnare all'utente un ACL definito localmente su NAD con stato di postura sconosciuto. Esempio di configurazione:
  cisco-av-pair = ip:interface-config=ip access-group DENY_SERVER in

Passaggio 1. Configurare il profilo di autorizzazione.

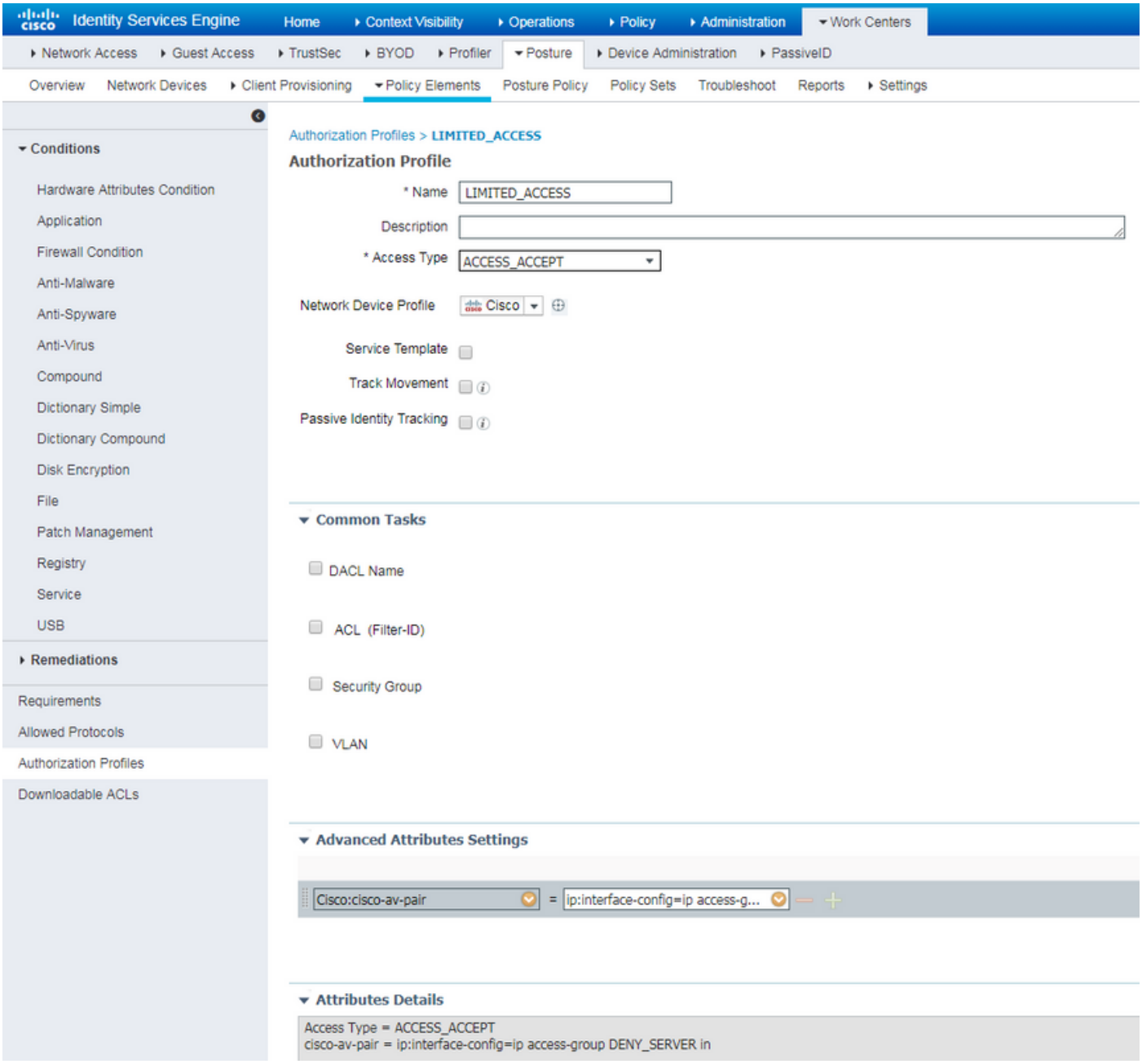
Come al solito per la postura sono richiesti due profili di autorizzazione. Il primo deve contenere qualsiasi tipo di restrizione di accesso alla rete. Questo profilo può essere applicato alle autenticazioni il cui stato di postura è diverso da conforme. Il secondo profilo di autorizzazione può contenere solo l'accesso consentito e può essere applicato per una sessione con stato di postura uguale a conforme.

Per creare un profilo di autorizzazione, passare a **Centri di lavoro -> Postura -> Elementi criteri -> Profili di autorizzazione**.

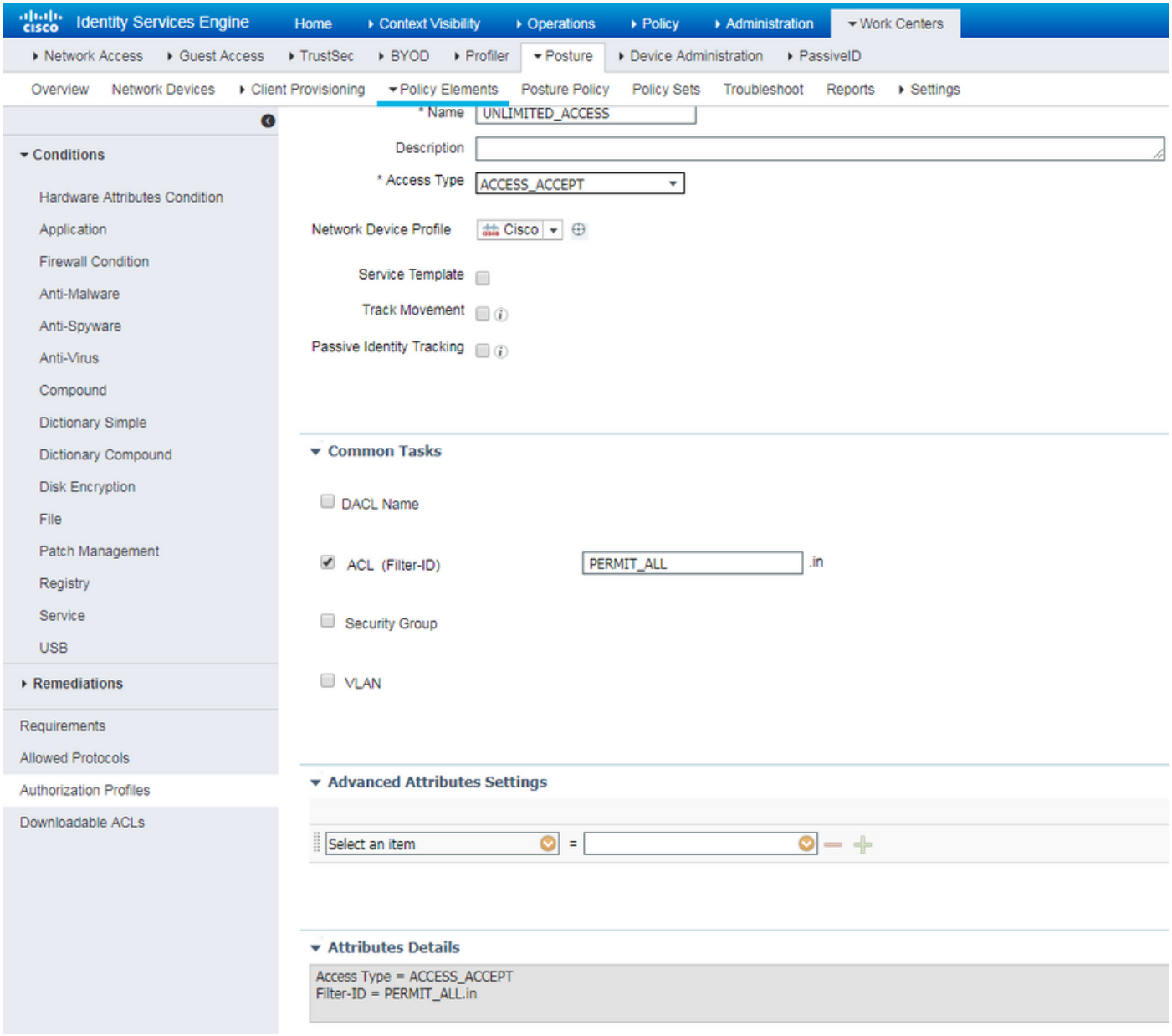
Esempio di profilo ad accesso limitato con ID filtro raggio:



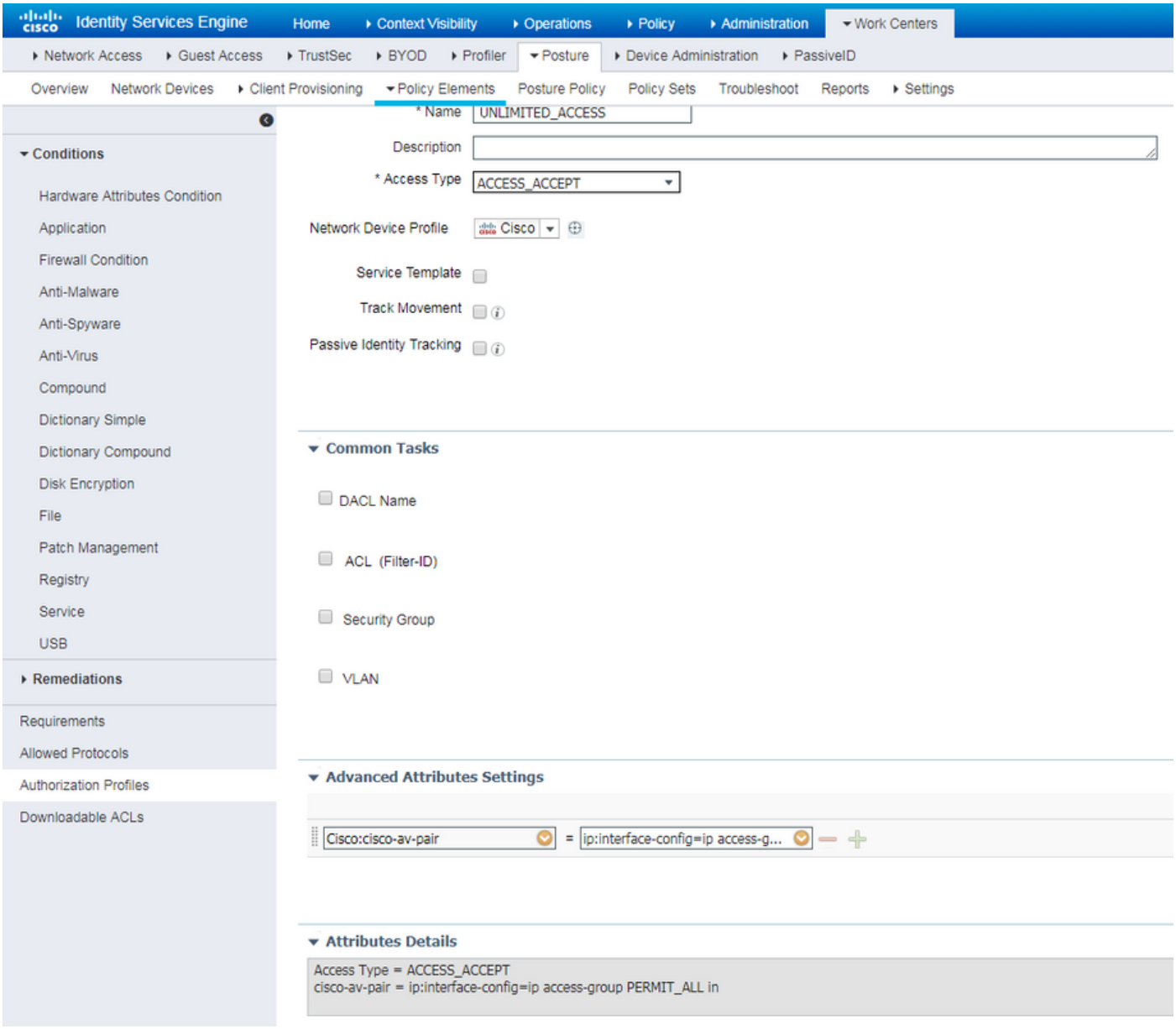
Esempio di profilo ad accesso limitato con cisco-av-pair:



Esempio di profilo di accesso illimitato con ID filtro raggio:



Esempio di profilo di accesso illimitato con cisco-av-pair:



Passaggio 2. Configurare i criteri di autorizzazione. In questa fase è necessario creare due criteri di autorizzazione. Uno per soddisfare la richiesta di autenticazione iniziale con stato di postura sconosciuto e l'altro per assegnare l'accesso completo dopo il processo di postura riuscito.

Si tratta di un esempio di criteri di autorizzazione semplici per questo caso:

La configurazione dei criteri di autenticazione non fa parte di questo documento, ma è necessario tenere presente che l'autenticazione deve avere esito positivo prima che l'elaborazione dei criteri di autorizzazione abbia inizio.

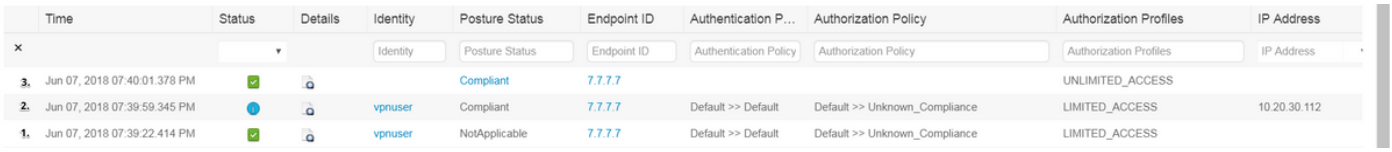
Verifica

La verifica di base del flusso può consistere in tre fasi principali:

Passaggio 1. Verifica della sessione VPN di Assistenza remota sull'HUB FlexVPN:

```
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
```

Passaggio 2. Verifica del flusso di autenticazione (Radius Live Logs):



	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	

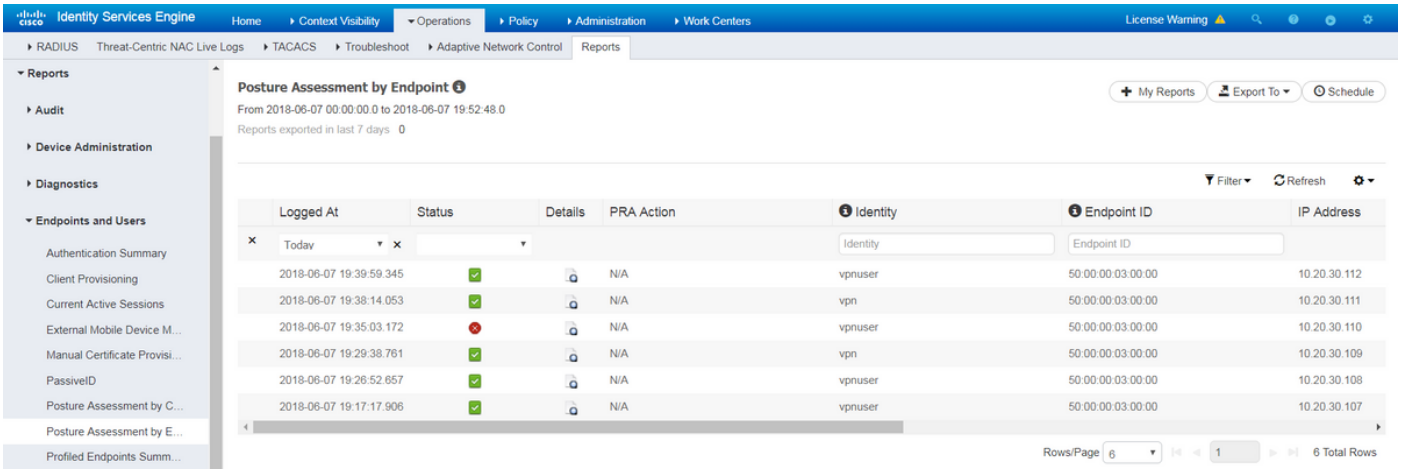
1. Autenticazione iniziale. Per questo passaggio può essere utile verificare il profilo di autorizzazione applicato. Se è stato applicato un profilo di autorizzazione imprevisto, esaminare il rapporto di autenticazione dettagliato. È possibile aprire questo report facendo clic sulla lente di ingrandimento nella colonna Dettagli. È possibile confrontare gli attributi nel report di autenticazione dettagliato con la condizione nel criterio di autorizzazione che si prevede corrisponda.

2. Modifica dei dati della sessione. In questo esempio, lo stato della sessione è stato modificato da NonApplicabile a Conforme.

3. Certificato di autenticità (COA) per il dispositivo di accesso alla rete. Il certificato di autenticità deve essere in grado di eseguire il push della nuova autenticazione dal lato AND e della nuova assegnazione dei criteri di autorizzazione dal lato ISE. Se il certificato di autenticità non riesce, è possibile aprire un report dettagliato per verificarne il motivo. I problemi più comuni relativi al certificato di autenticità possono essere: Timeout COA: in questo caso, il PSN che ha inviato la richiesta non è configurato come client COA sul lato NAD oppure la richiesta COA è stata eliminata da qualche parte.ACK negativi COA: indicare che il COA è stato ricevuto da NAD ma per qualche motivo non è possibile confermare l'operazione. Per questo scenario la relazione dettagliata dovrebbe contenere spiegazioni più dettagliate.

Poiché per questo esempio è stato utilizzato un router basato su IOS XE come NAD, non viene visualizzata alcuna richiesta di autenticazione successiva per l'utente. Ciò è dovuto al fatto che ISE utilizza il push COA per IOS XE, che evita l'interruzione del servizio VPN. In questo scenario, il certificato di autenticità contiene nuovi parametri di autorizzazione, pertanto non è necessaria la riautenticazione.

Passo 3.Verifica report postura - Passare a **Operazioni -> Report -> Report -> Endpoint e utenti -> Valutazione postura per endpoint**.



Da qui è possibile aprire un report dettagliato per ogni evento specifico per controllare ad esempio a quale ID sessione appartiene questo report, quali requisiti di postura esatti sono stati selezionati da ISE per l'endpoint e lo stato per ogni requisito.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

1. Debug IKEv2 da raccogliere dall'headend:

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

2. Debug AAA per visualizzare l'assegnazione degli attributi locali e/o remoti:

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

3. DART dal client AnyConnect.
4. Per la risoluzione dei problemi del processo di postura, i componenti ISE devono essere abilitati nel debug sui nodi ISE in cui può avvenire il processo di postura:**client-webapp** - componente responsabile del provisioning dell'agente. File di log di destinazione **guest.log** e **ise-psc.log**.**guestaccess**: componente responsabile della ricerca del componente del portale di provisioning client e del proprietario della sessione (quando la richiesta arriva al PSN errato). File di log di destinazione - **guest.log.provisioning - componente responsabile dell'elaborazione dei criteri di provisioning client. File di log di destinazione - guest.log.postura**: tutti gli eventi correlati alla postura. File di registro di destinazione: **ise-psc.log**
5. Per la risoluzione dei problemi lato client è possibile utilizzare:**AnyConnect.txt** - Questo file è disponibile nel bundle DART e viene usato per la risoluzione dei problemi della VPN.**acisensa.log**-In caso di errore di provisioning del client sul lato client, questo file viene creato nella stessa cartella in cui è stato scaricato NSA (directory di download per Windows normalmente),**AnyConnect_ISEPosture.txt** - Questo file è disponibile nella directory **Cisco AnyConnect ISE Posture Module** del bundle DART. Tutte le informazioni su ISE PSN discovery e le fasi generali del flusso di postura sono registrate in questo file.