Configuración del estado de ISE con FlexVPN

Contenido

Introducción

Este documento proporciona un ejemplo de cómo configurar una cabecera IOS XE para el acceso remoto con estado usando el método de autenticación AnyConnect IKEv2 y EAP-Message Digest 5 (EAP-MD5).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de VPN de acceso remoto (RA) FlexVPN en IOS XE
- Configuración del cliente AnyConnect (AC)
- Flujo de estado en Identity Service Engine (ISE) 2.2 y versiones posteriores
- Configuración de los componentes de estado en ISE
- Configuración del servidor DNS en Windows Server 2008 R2

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco CSR1000V con IOS XE 16.8 [Fuji]
- Cliente AnyConnect versión 4.5.03040 que se ejecuta en Windows 7
- Cisco ISE 2.3
- Servidor Windows 2008 R2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Para garantizar que las medidas de seguridad de red impuestas sigan siendo relevantes y eficaces, Cisco ISE le permite validar y mantener las capacidades de seguridad en cualquier equipo cliente que acceda a la red protegida. Al emplear políticas de estado diseñadas para garantizar que las aplicaciones o los parámetros de seguridad más actualizados estén disponibles en los equipos cliente, el administrador de Cisco ISE puede garantizar que cualquier equipo cliente que acceda a la red cumpla y siga cumpliendo los estándares de seguridad definidos para el acceso a la red empresarial. Los informes de cumplimiento de estado proporcionan a Cisco ISE una instantánea del nivel de cumplimiento de la máquina cliente en el momento del inicio de sesión del usuario, así como en cualquier momento en que se realice una reevaluación periódica.

La posición puede estar representada por tres elementos principales:

1. ISE como punto de decisión y distribución de la configuración de políticas. Desde la perspectiva del administrador de ISE, puede configurar políticas de estado (qué condiciones exactas se deben cumplir para marcar el dispositivo como conforme con la empresa), políticas de aprovisionamiento de clientes (qué software de agente se debe instalar en qué tipo de dispositivos) y políticas de autorización (a qué tipo de permisos se debe asignar, según su estado).

2. Dispositivo de acceso a la red (NAD) como punto de aplicación de políticas. En el lado NAD, las restricciones reales de autorización se aplican en el momento de la autenticación de usuario. ISE como punto de política proporciona parámetros de autorización, como la lista de control de acceso (ACL). Tradicionalmente, para que se produzca el estado, se requiere que los NAD admitan el cambio de autorización (CoA) para volver a autenticar al usuario después de determinar el estado del terminal. A partir de ISE 2.2, los NAD no son necesarios para admitir la redirección.
   Nota: Los routers que ejecutan IOS XE no admiten redirección.**Nota:** El software IOS XE debe tener correcciones para que los siguientes defectos tengan CoA con ISE totalmente operativo:
   CSCve16269 IKEv2 CoA no funciona con ISE
   CSCvi90729 IKEv2 CoA no funciona con ISE (coa-push=TRUE en lugar de true)
3. Software de agente como punto de recopilación de datos e interacción con el usuario final. El agente recibe información sobre los requisitos de estado de ISE y proporciona un informe a ISE sobre el estado de los requisitos. Este documento se basa en Anyconnect ISE Posture

Module que es el único que soporta el estado completamente sin redirección.
El flujo de estado sin redirección está muy bien documentado en el artículo "Comparación de estilo de postura ISE para pre y post 2.2", sección "Flujo de estado en ISE 2.2".

El aprovisionamiento del módulo de estado de ISE de Anyconnect con FlexVPN se puede realizar de dos maneras diferentes:

- Manual: el módulo se instala manualmente en la estación de trabajo del cliente desde el paquete Anyconnect disponible en el portal de descarga de software de Cisco: https://software.cisco.com/download/home/283000185.
  Se deben cumplir las siguientes condiciones para el trabajo de estado con el aprovisionamiento manual del módulo de estado de ISE:

  1. El servidor de nombres de dominio (DNS) debe resolver el nombre de dominio completo (FQDN) **enroll.cisco.com** a las IP de los nodos de servicio de políticas (PSN). Durante el primer intento de conexión, el módulo de estado no tiene ninguna información sobre los PSN disponibles. Está enviando sondas de detección para encontrar PSN disponibles. FQDN enroll.cisco.com se utiliza en una de estas sondas.

  2. El puerto **TCP 8905** debe estar permitido para las IPs PSN. El estado va a través del puerto TCP 8905 en este escenario.

  3. **El certificado de administrador** en los nodos PSN debe tener **enroll.cisco.com** en el **campo SAN**. La conexión entre el usuario VPN y el nodo PSN a través de TCP 8905 está protegida mediante el certificado de administrador y el usuario recibirá una advertencia de certificado si no existe tal nombre "enroll.cisco.com" en el certificado de administrador del nodo PSN.

  Nota: Según el certificado RFC6125, los CNs deben ignorarse si se especifican valores SAN. Esto significa que también necesitamos agregar CNs de certificado de administrador en el campo SAN.

- Aprovisionamiento automático mediante el portal de aprovisionamiento de clientes (CPP): el módulo se descarga e instala desde el ISE accediendo a CPP directamente a través del FQDN del portal.
  Se deben cumplir las siguientes condiciones para el trabajo de estado con el aprovisionamiento automático del módulo de estado de ISE:

  1. DNS debe resolver **FQDN de CPP** a IP de nodos de servicio de políticas (PSN).

  2. **Los puertos TCP 80, 443 y el puerto CPP (8443 de forma predeterminada)** deben estar permitidos para las IPs PSN. El cliente necesita abrir el FQDN CPP directamente a través de HTTP (se redirigirá a HTTPS) o HTTPS; esta solicitud se redirigirá al puerto CPP (8443 de forma predeterminada) y, a continuación, el estado se realizará a través de ese puerto.

  3. Los **certificados de administrador y CPP** en los nodos PSN deben tener **FQDN CPP** en el **campo SAN**. La conexión entre el usuario VPN y el nodo PSN a través de TCP 443 está protegida por el certificado de administrador y la conexión en el puerto CPP está protegida por el certificado CPP.

  Nota: Según el certificado RFC6125, los CNs deben ignorarse si se especifican valores

SAN. Esto significa que también necesitamos agregar CN de certificados de administración y CPP en el campo SAN de los certificados correspondientes.

Nota: Si el software ISE no contiene una corrección para CSCvj76466, entonces el estado o el aprovisionamiento de clientes sólo funcionarán si se realiza el aprovisionamiento de clientes o de seguros en el mismo PSN en el que se autenticó el cliente.

En caso de estado con FlexVPN, el flujo incluye estos pasos:

1. El usuario se conecta al hub FlexVPN mediante el cliente Anyconnect.

2. ISE envía Access-Accept al FlexVPN Hub con el nombre de ACL que se debe aplicar para restringir el acceso.

3 bis. Primera conexión con aprovisionamiento manual: el módulo de estado de ISE comienza a detectar el servidor de políticas que envía la sonda a enroll.cisco.com a través del puerto TCP 8905. Como resultado exitoso, el módulo de estado descarga el perfil de estado configurado y actualiza el módulo de cumplimiento en el lado del cliente.

Durante los siguientes intentos de conexión, el módulo de estado de ISE también utilizará los nombres e IP especificados en la Lista de inicio de llamadas del perfil de estado para la detección del servidor de políticas.

3 ter. Primera conexión con aprovisionamiento automático: el cliente abre CPP a través de FQDN. Como resultado exitoso, Network Setup Assistant se descarga en la estación de trabajo del cliente y, a continuación, descarga e instala el módulo de estado de ISE, el módulo de cumplimiento de ISE y el perfil de estado.

Durante los siguientes intentos de conexión, el módulo de estado de ISE utilizará los nombres e IP especificados en la Lista de inicio de llamadas del perfil de estado para la detección del servidor de políticas.

4. El módulo de estado inicia las comprobaciones del cumplimiento y envía los resultados de la comprobación al ISE.

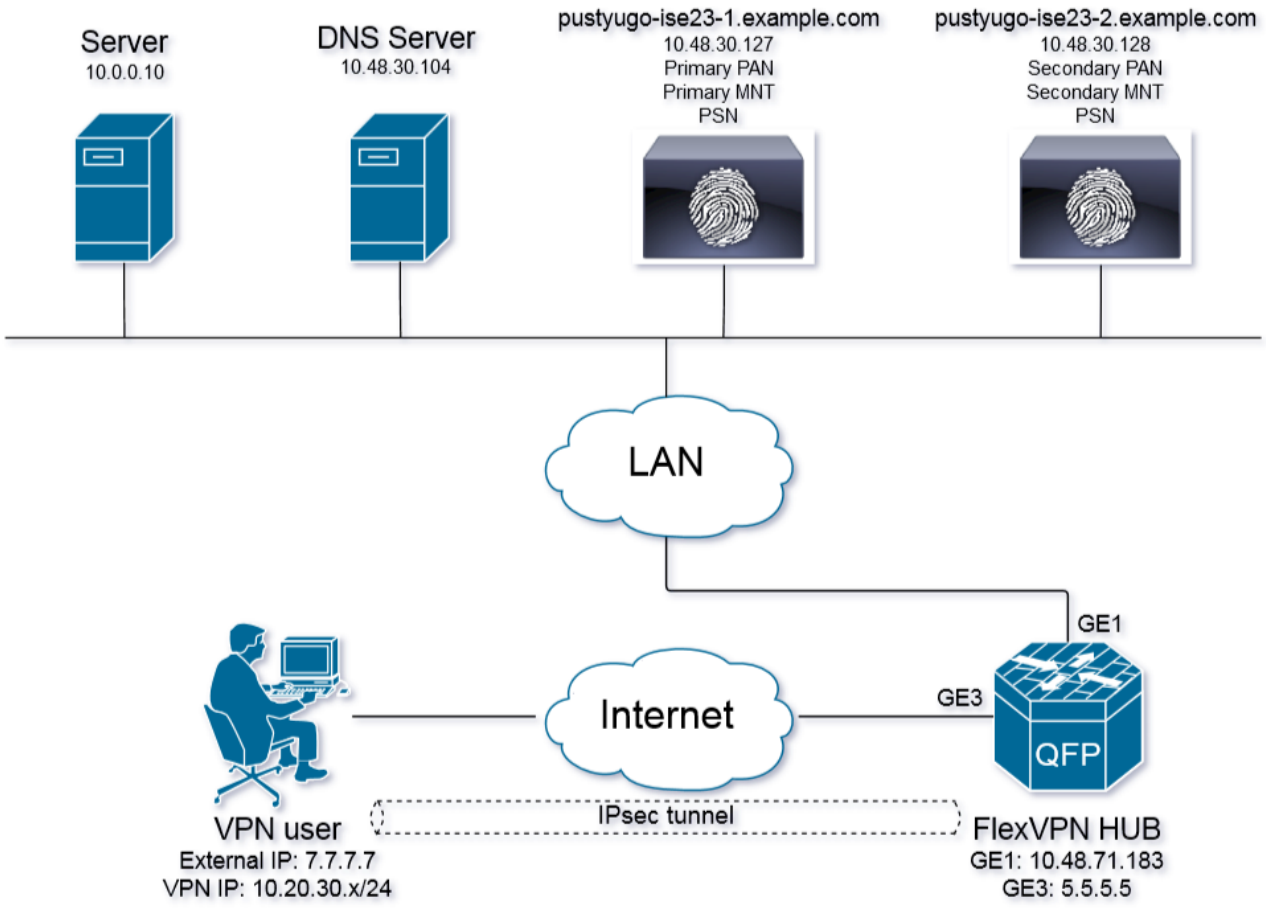
5. Si el estado del cliente es Conforme, ISE envía Access-Accept al FlexVPN Hub con el nombre de ACL debe aplicarse para el cliente conforme.

6, El cliente obtiene acceso a la red.

Puede encontrar más detalles sobre el proceso de estado en el documento "Comparación de estilo de estado ISE para Pre y Post 2.2".

Configurar

Diagrama de la red

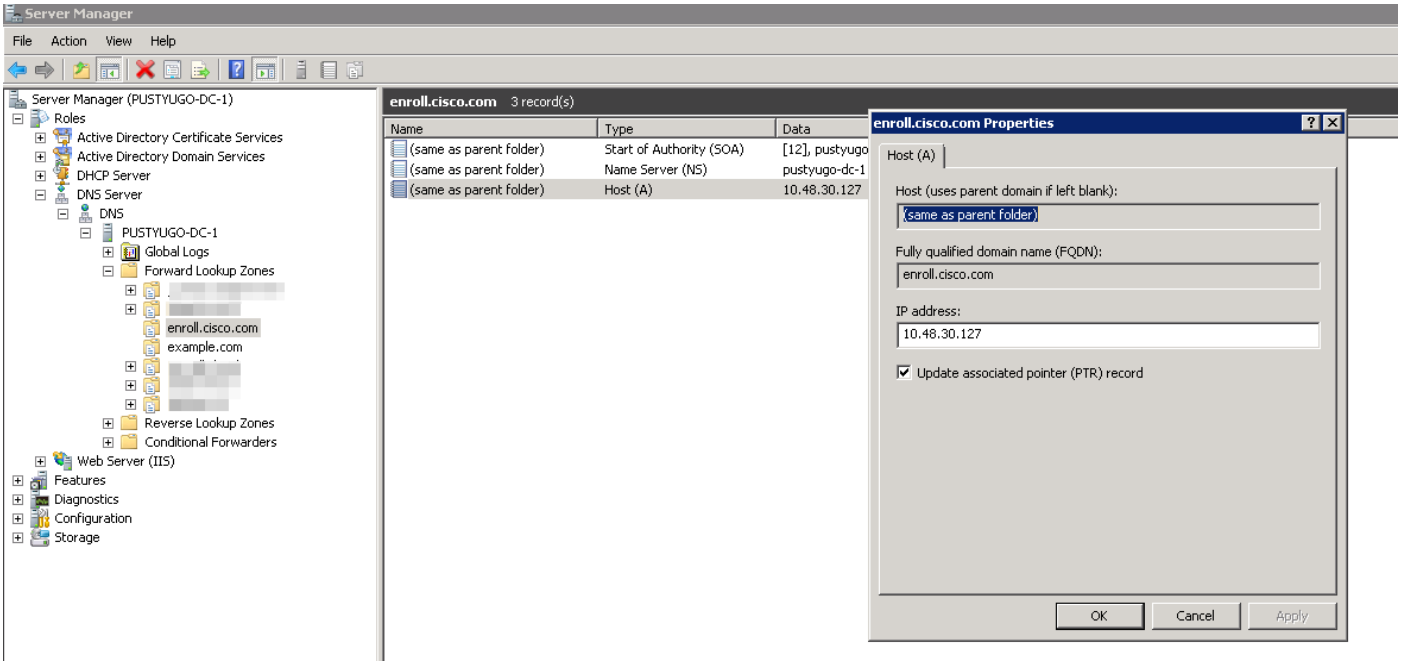


El usuario de VPN obtendrá acceso al servidor (10.0.0.10) sólo si tiene el estado conforme.

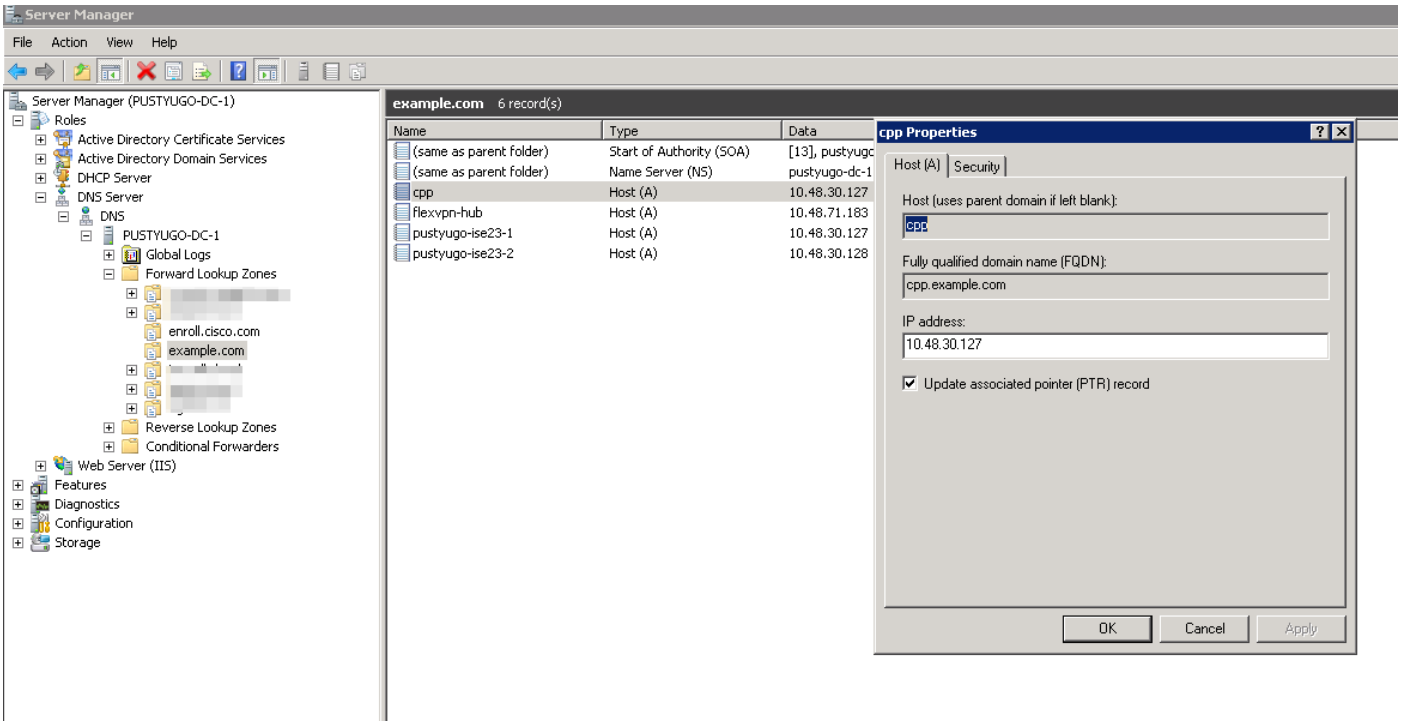
configuración del servidor DNS

En este documento, Windows Server 2008 R2 se utiliza como servidor DNS.

Paso 1. Agregue el registro **Host (A)** para **enroll.cisco.com** señalando a la **IP de PSN**:



Paso 2. Agregue el registro **Host (A)** para el FQDN de CPP (**cpp.example.com** utilizado en este ejemplo) señalando a la **IP de PSN**:



Configuración inicial de IOS XE

Configurar certificado de identidad

El router utilizará el certificado para autenticarse en el cliente Anyconnect. El sistema operativo del usuario debe confiar en el certificado del router para evitar la advertencia del certificado durante la fase de establecimiento de la conexión.

El certificado de identidad se puede proporcionar de una de las siguientes maneras:

> **Nota:** El uso de certificados autofirmados no es compatible con IKEv2 FlexVPN.

Opción 1: Configuración del servidor de la entidad de certificación (CA) en el router

> **Nota:** El servidor de la CA se puede crear en el mismo router del IOS o en otro router. En este artículo, la CA se crea en el mismo router.

> **Nota:** Debe sincronizar la hora con el servidor NTP antes de poder habilitar el servidor de la CA.

> **Nota:** Tenga en cuenta que el usuario no podrá verificar la autenticidad de este certificado, por lo que los datos del usuario no estarán protegidos frente a ataques de intrusos a menos que el certificado de CA se verifique e importe manualmente en el equipo del usuario antes de establecer la conexión.

Paso 1. Genere claves RSA para el servidor CA:

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

Paso 2. Genere claves RSA para el certificado de identidad:

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

Verificación:

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

Paso 3. Configure 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
```

Verificación:

```
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
```

Paso 4. Configure el punto de confianza:

```
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
```

Paso 5. Autentique 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.
```

Paso 6. Inscriba el router en la 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
```

Verifique las solicitudes de certificados pendientes en la CA y verifique que la huella digital coincida con:

```
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
```

Paso 7. Conceda el certificado con el ReqID adecuado:

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

Espere hasta que el router vuelva a solicitar el certificado (según esta configuración, lo comprobará 10 veces una vez por minuto). Busque el mensaje syslog:

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

Verifique que el certificado esté instalado:

```
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
```

Opción 2: importar certificado firmado externamente

```
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)#
```

Configuración de IKEv2

Paso 1. Configuración del servidor RADIUS y 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
```

Paso 2. Configuración de listas de autenticación y autorización:

```
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
```

Paso 3. Cree una política de autorización de 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
```

Paso 4. Crear perfil 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
```

Paso 5. Crear conjunto de transformación y perfil 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
```

Paso 6. Crear interfaz de plantilla virtual:

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

Paso 7. Crear conjunto local:

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

Paso 8. Cree ACL para restringir el acceso para clientes que no cumplen con las normas. Durante el estado desconocido, deben proporcionarse al menos esos permisos:

- tráfico DNS
- Tráfico a PSN ISE a través de los puertos 80, 443 y 8905
- Tráfico a PSN ISE a los que el FQDN del portal CPP señala
- Tráfico a servidores de remediación si es necesario

Este es un ejemplo de ACL sin servidores de remediación, se agrega una negación explícita para la red 10.0.0.0/24 para la visibilidad, existe implícita "deny ip any any" al final de la 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
```

Paso 9. Cree una ACL para permitir el acceso a los clientes conformes:

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

Paso 10. Configuración de túnel dividido (opcional)

De forma predeterminada, todo el tráfico se dirigirá a través de VPN. Para tunelizar el tráfico solamente a las redes especificadas, puede especificarlas en la sección de política de autorización de ikev2. Es posible agregar varias instrucciones o utilizar una lista de acceso estándar.

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

Paso 11. Acceso a Internet para clientes remotos (opcional)

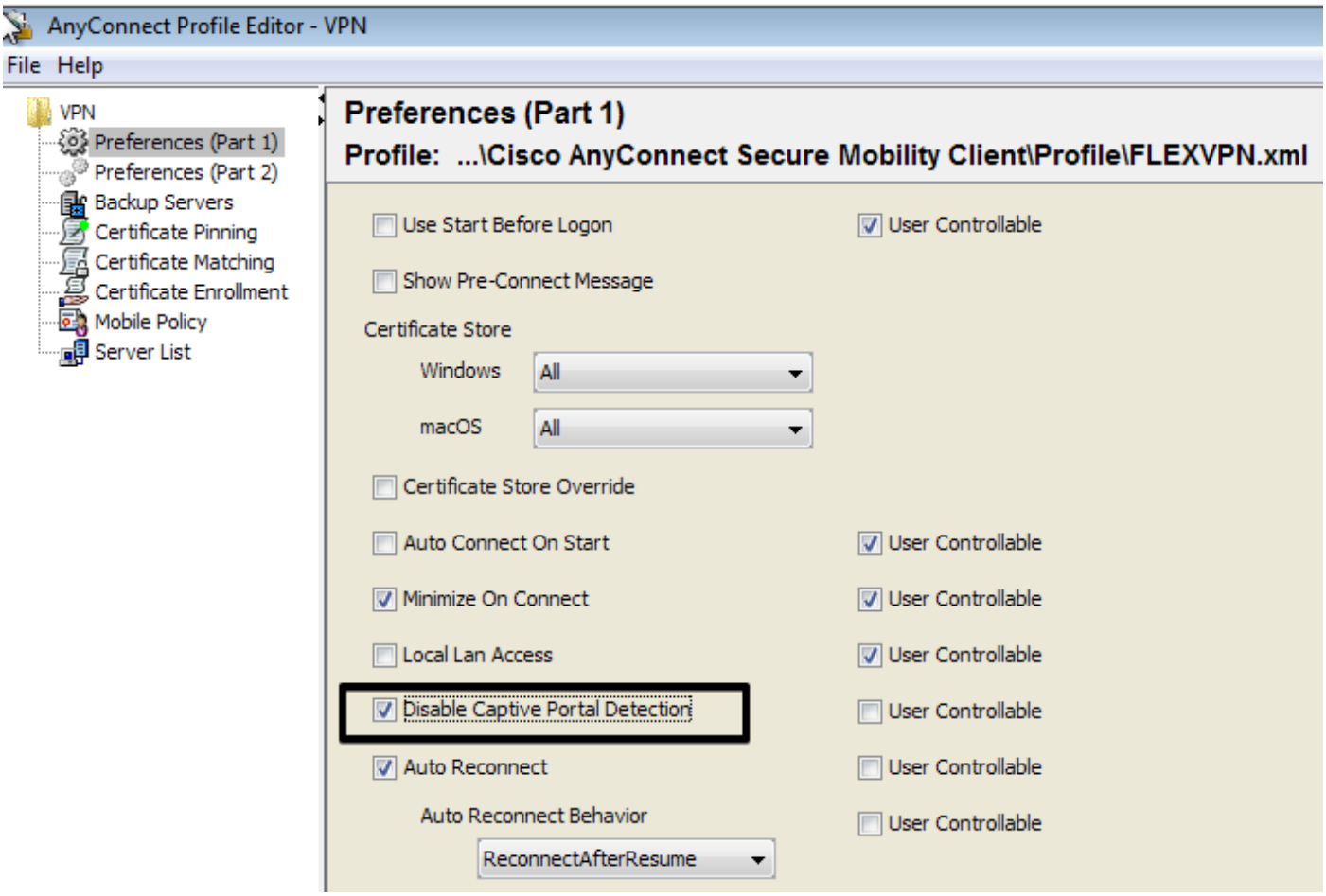
Para que las conexiones salientes de los clientes de acceso remoto a los hosts en Internet sean NAT-ed a la dirección IP global del router, configure la traducción NAT:

```
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
```

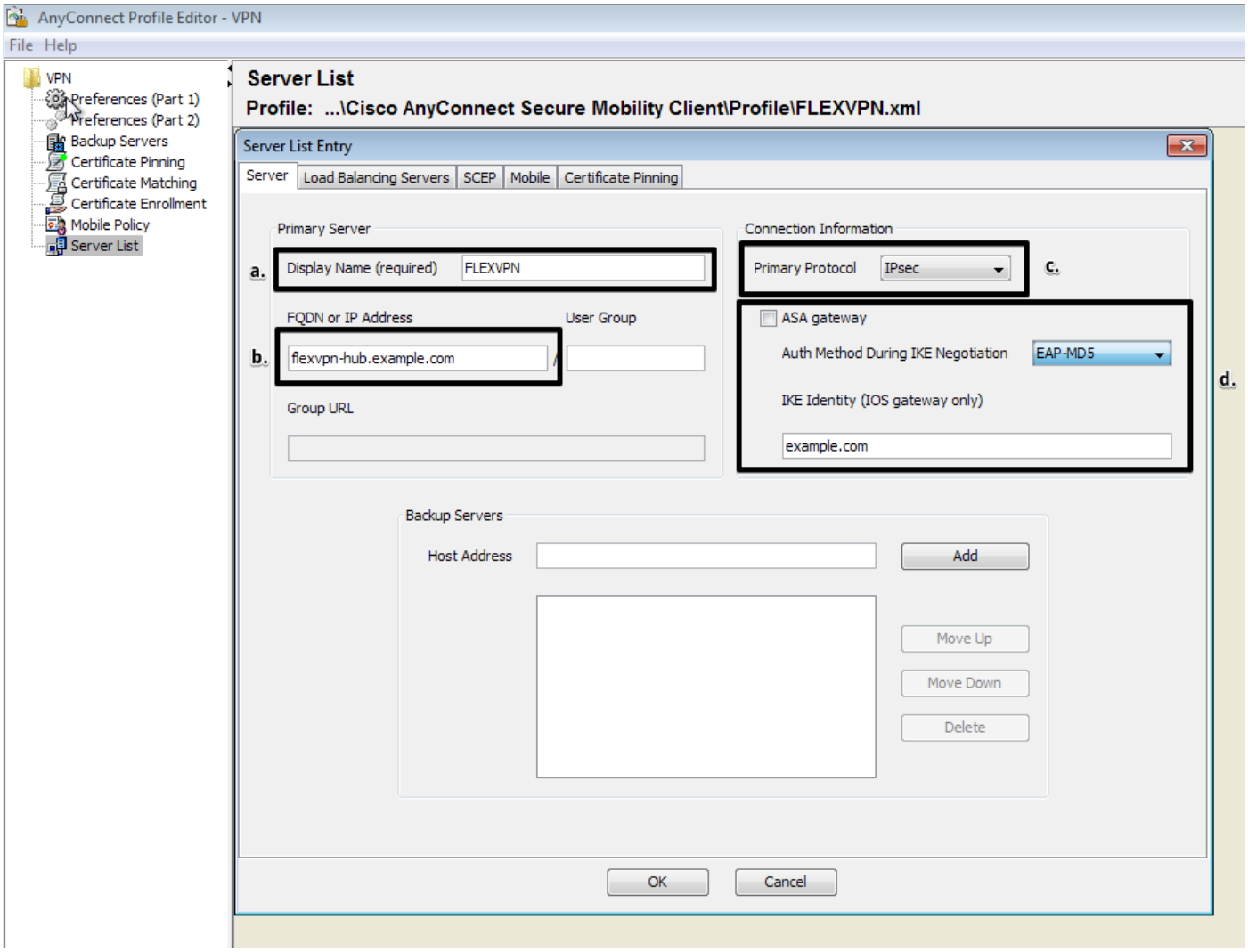
Configuración del perfil del cliente de Anyconnect

Configure el perfil del cliente mediante el Editor de perfiles de AnyConnect. Los perfiles de Anyconnect Security Mobile Client en Windows 7 y 10 se guardan en **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile**.

Paso 1. Desactive la función Captive Portal Detection. Si el servidor http no está desactivado en FlexVPN Hub, la función de detección del portal cautivo AnyConnect provocará un error en la conexión. Tenga en cuenta que el servidor CA no funcionará sin el servidor HTTP.



Paso 2. Configurar lista de servidores:



- Introduzca Nombre para mostrar.
- Ingrese **FQDN** o **dirección IP del FlexVPN Hub.**
- Seleccione **IPsec** como protocolo principal.
- Desmarque la casilla de verificación "gateway ASA" y especifique **EAP-MD5** como método de autenticación. Introduzca la identidad IKE exactamente igual que en la configuración del perfil IKEv2 en el FlexVPN Hub (en este ejemplo, el perfil IKEv2 se configura con el comando "match identity remote key-id example.com", por lo que necesitamos utilizar **example.com** como identidad IKE).

Paso 3. Guarde el perfil en **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile** y reinicie el AC.

El equivalente XML del perfil:

```
<?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>
```

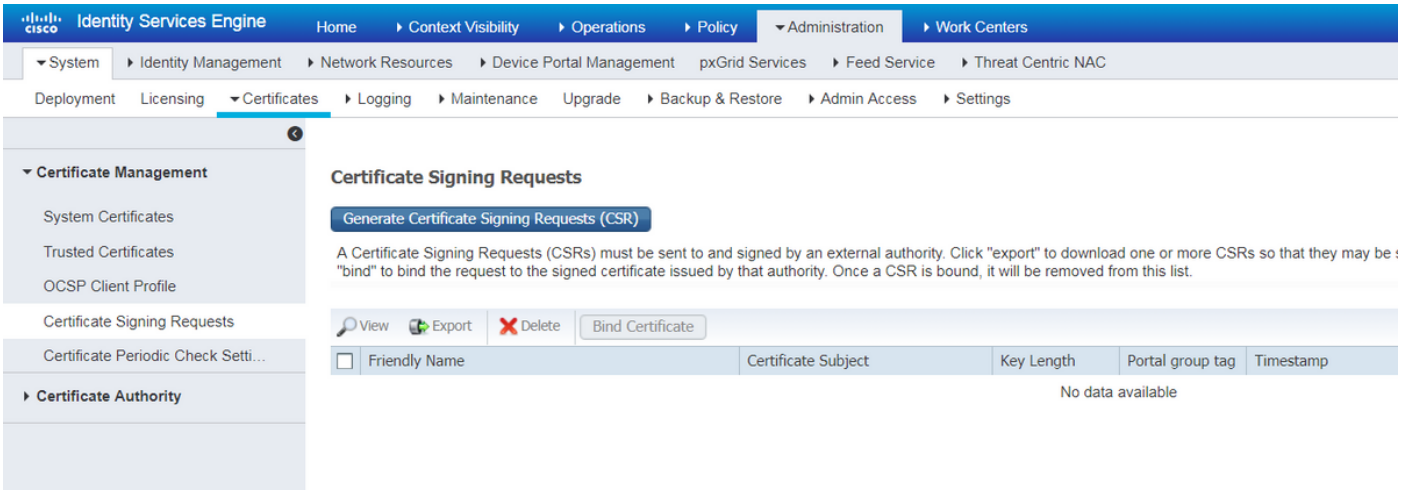
```
        <CertificateStore>All</CertificateStore>
        <CertificateStoreMac>All</CertificateStoreMac>
        <CertificateStoreOverride>false</CertificateStoreOverride>
        <ProxySettings>Native</ProxySettings>
        <AllowLocalProxyConnections>false</AllowLocalProxyConnections>
        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

configuración de ISE

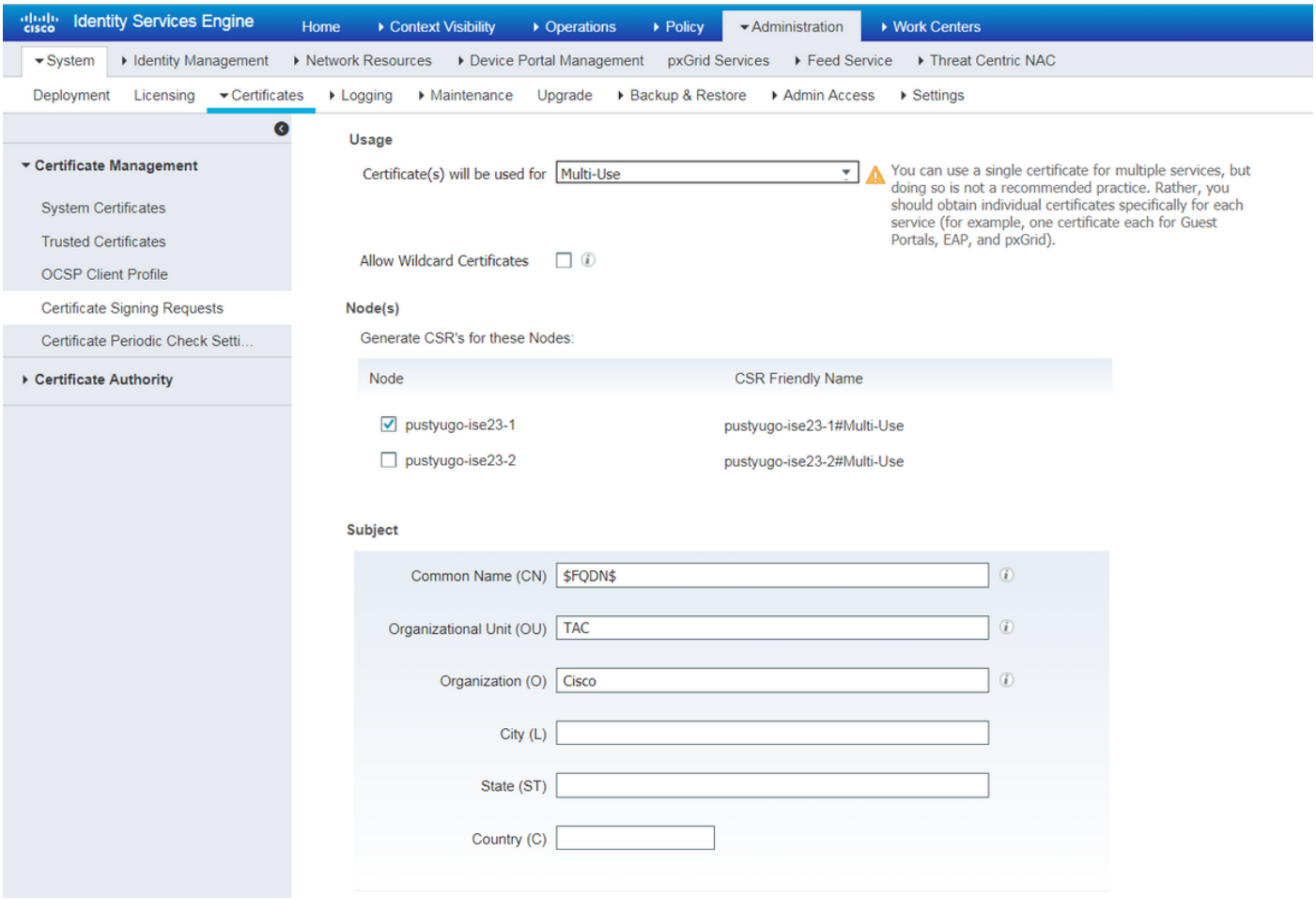
Configuración de certificados de administrador y CPP

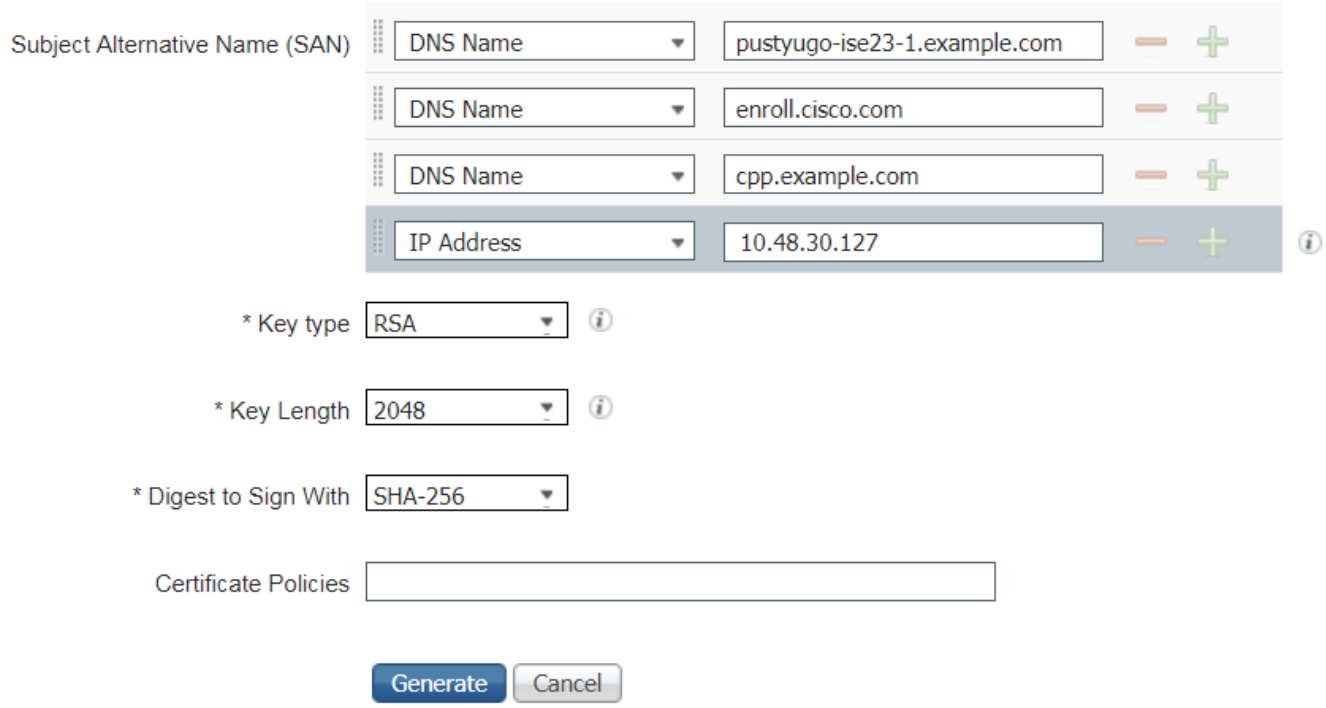
> **Nota:** Al cambiar el certificado de administrador, se reiniciará el nodo en el que se ha cambiado el certificado.

Paso 1. Vaya a **Administración -> Sistema -> Certificados -> Solicitudes de firma de certificados,** haga clic en **Generar solicitudes de firma de certificados (CSR):**



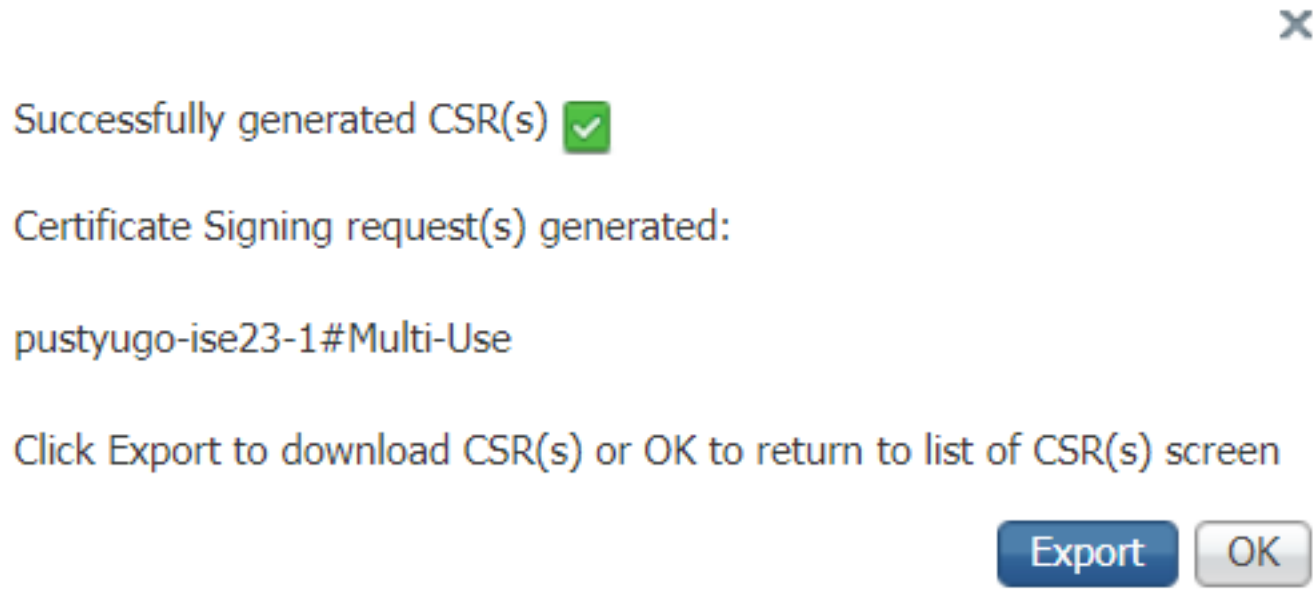
Paso 2. En la página abierta, seleccione el nodo PSN necesario, rellene los campos necesarios y agregue FQDN del nodo, enroll.cisco.com, cpp.example.com y dirección IP del nodo en los campos SAN y haga clic en **Generar**:





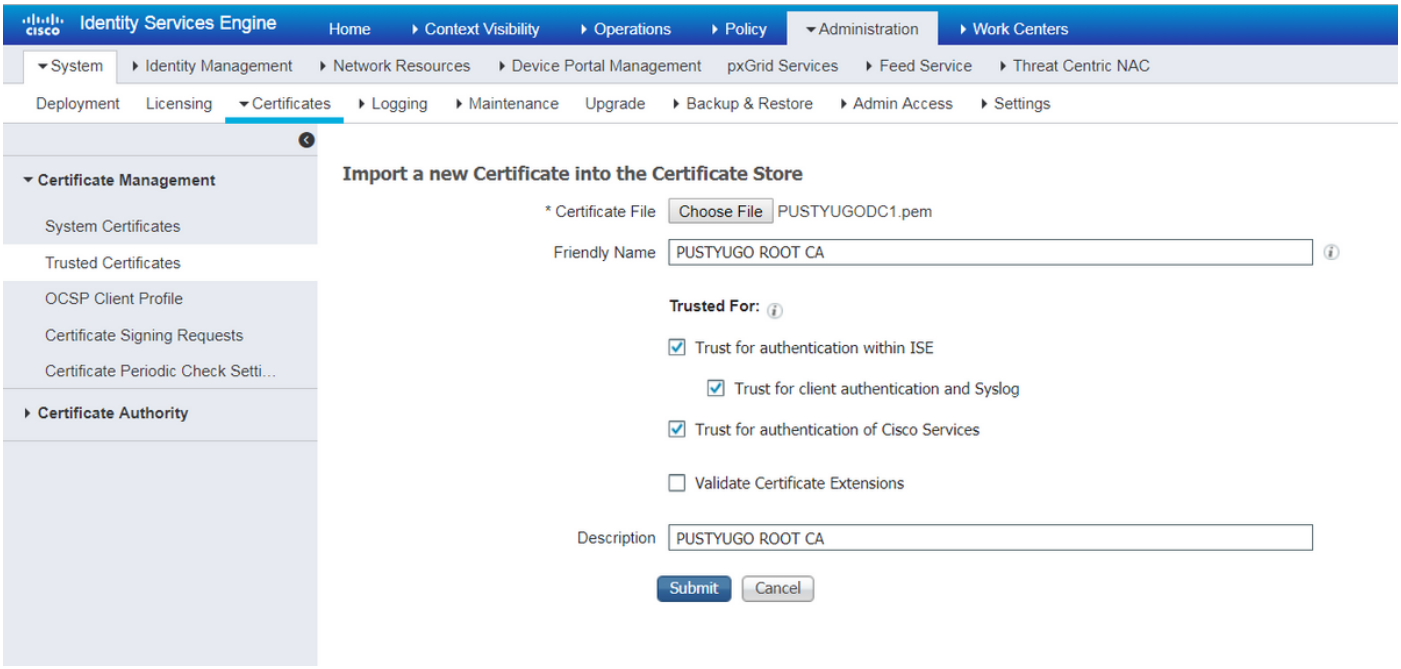
Nota: Si selecciona **Multi-Use** en este paso, también puede utilizar el mismo certificado para Portal.

En la ventana que aparece, haga clic en **Exportar** para guardar el CSR en formato pem en la estación de trabajo local:



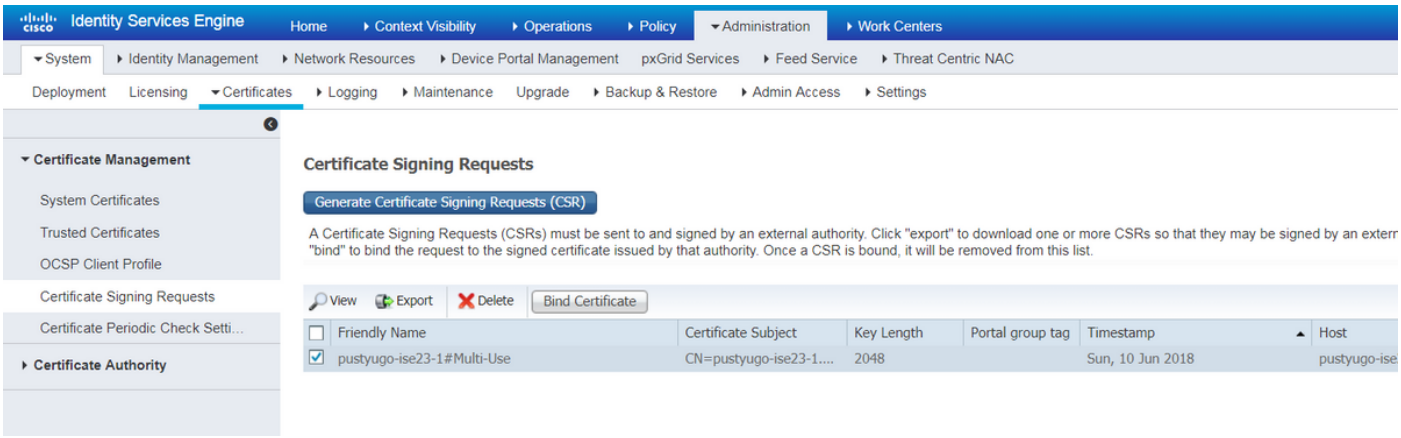
Paso 3. Utilice CSR con CA de confianza y obtenga el archivo de certificado de la CA, así como la cadena completa de certificados de CA (raíz e intermedio).

Paso 4. Vaya a **Administration -> System -> Certificates -> Trusted Certificates**, haga clic en **Import. En la siguiente pantalla, haga clic en Elegir archivo** y seleccione el archivo de **certificado de CA raíz**, rellene el nombre descriptivo y la descripción si es necesario, seleccione las opciones **Confiable** necesarias y haga clic en **Enviar:**

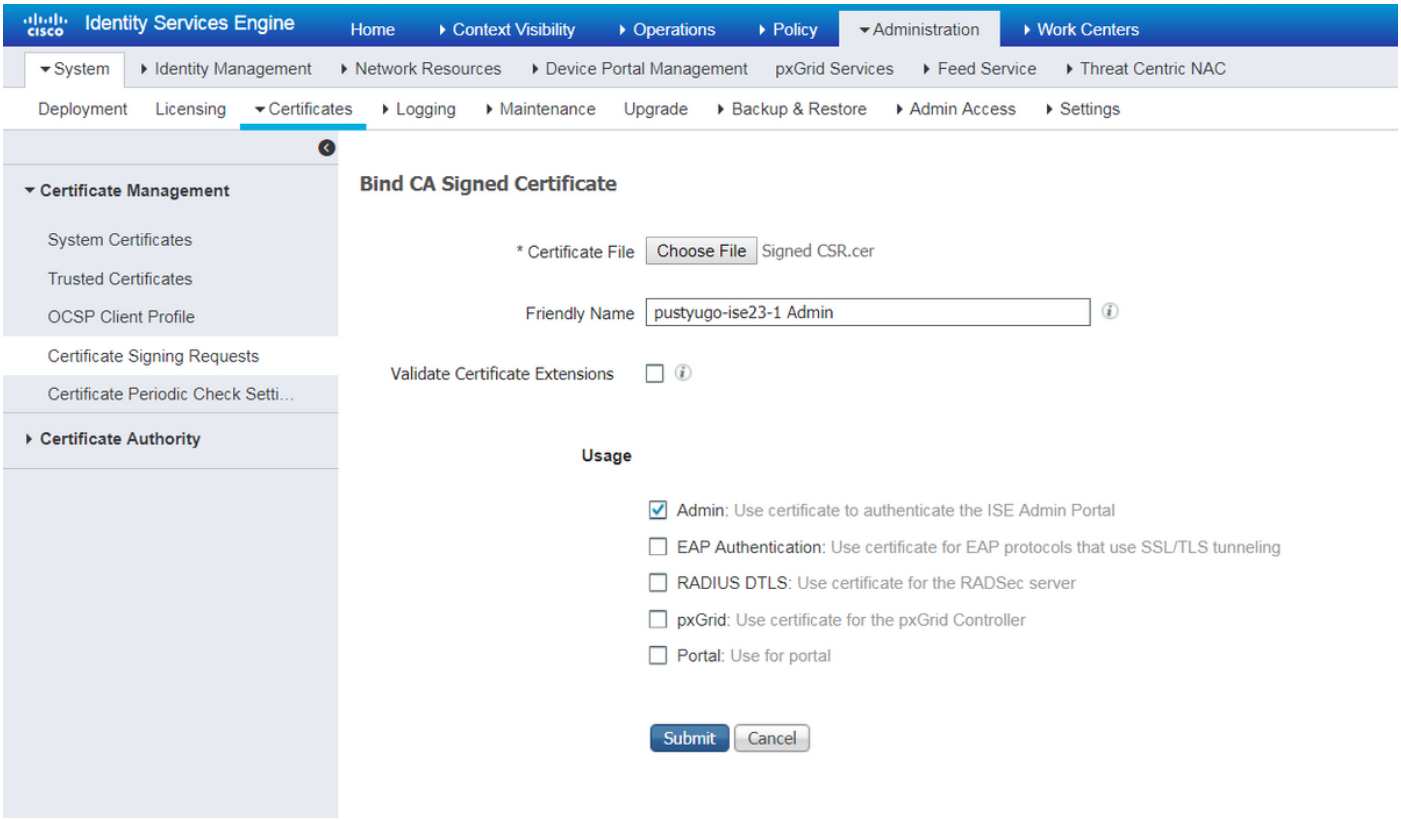


Repita este paso para todos los certificados intermedios de la cadena si los hay.

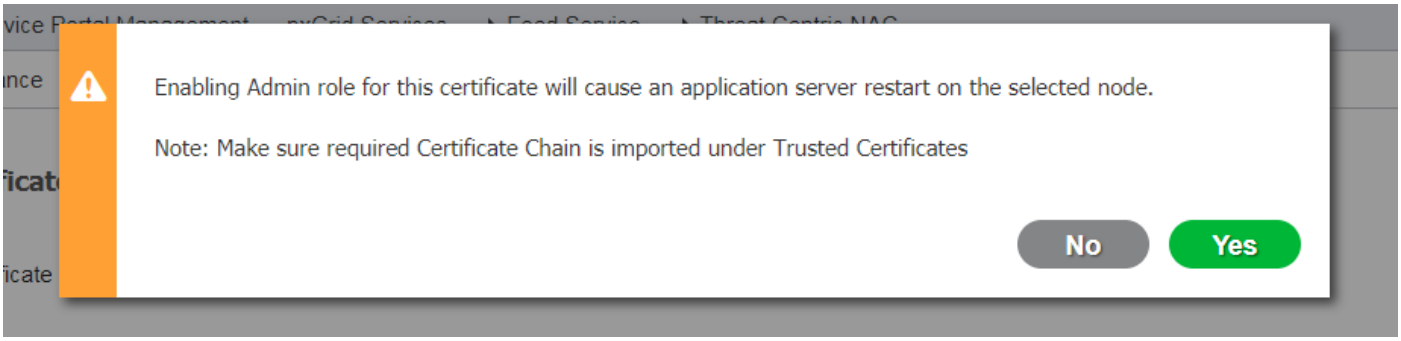
Paso 5. Volver a **Administración -> Sistema -> Certificados -> Solicitudes de firma de certificado,** seleccionar CSR necesario y hacer clic en **Enlazar certificado:**



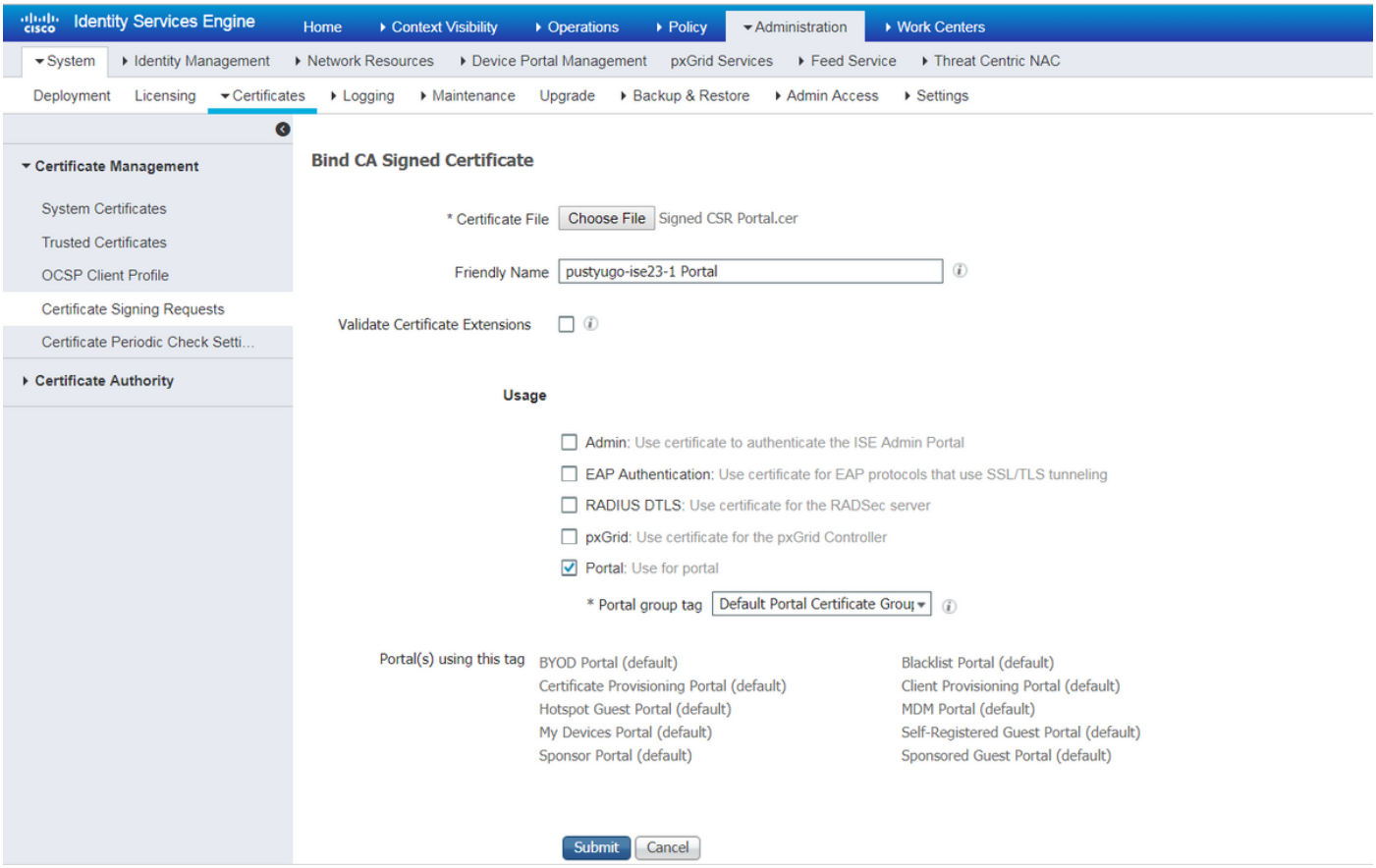
Paso 6. En la página abierta, haga clic en **Elegir archivo**, seleccione el archivo de certificado recibido de la CA y, a continuación, introduzca el nombre descriptivo si es necesario y, a continuación, seleccione **Uso: Admin** (**Uso: El portal** también se puede seleccionar aquí si la CSR se creó con **varios usos**) y haga clic en **Enviar**:



Paso 7. En la ventana emergente de advertencia, haga clic en **Sí** para finalizar la importación. Se reiniciará el nodo afectado por el cambio del certificado de administrador:



Repita los pasos para cambiar el certificado CPP si decidió utilizar un certificado separado para el portal. En el Paso 6 seleccione **Uso: Portal** y haga clic en **Enviar:**

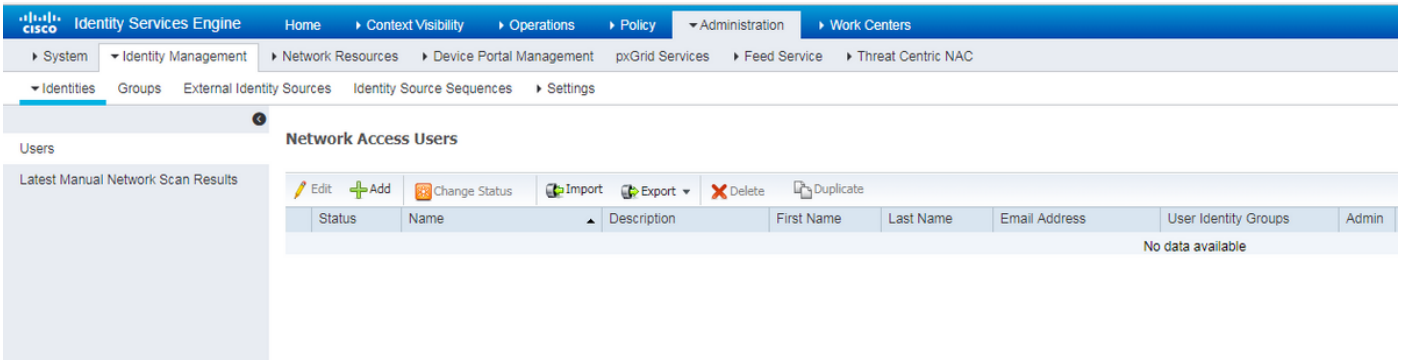


Repita los pasos para todos los PSN en la implementación de ISE.

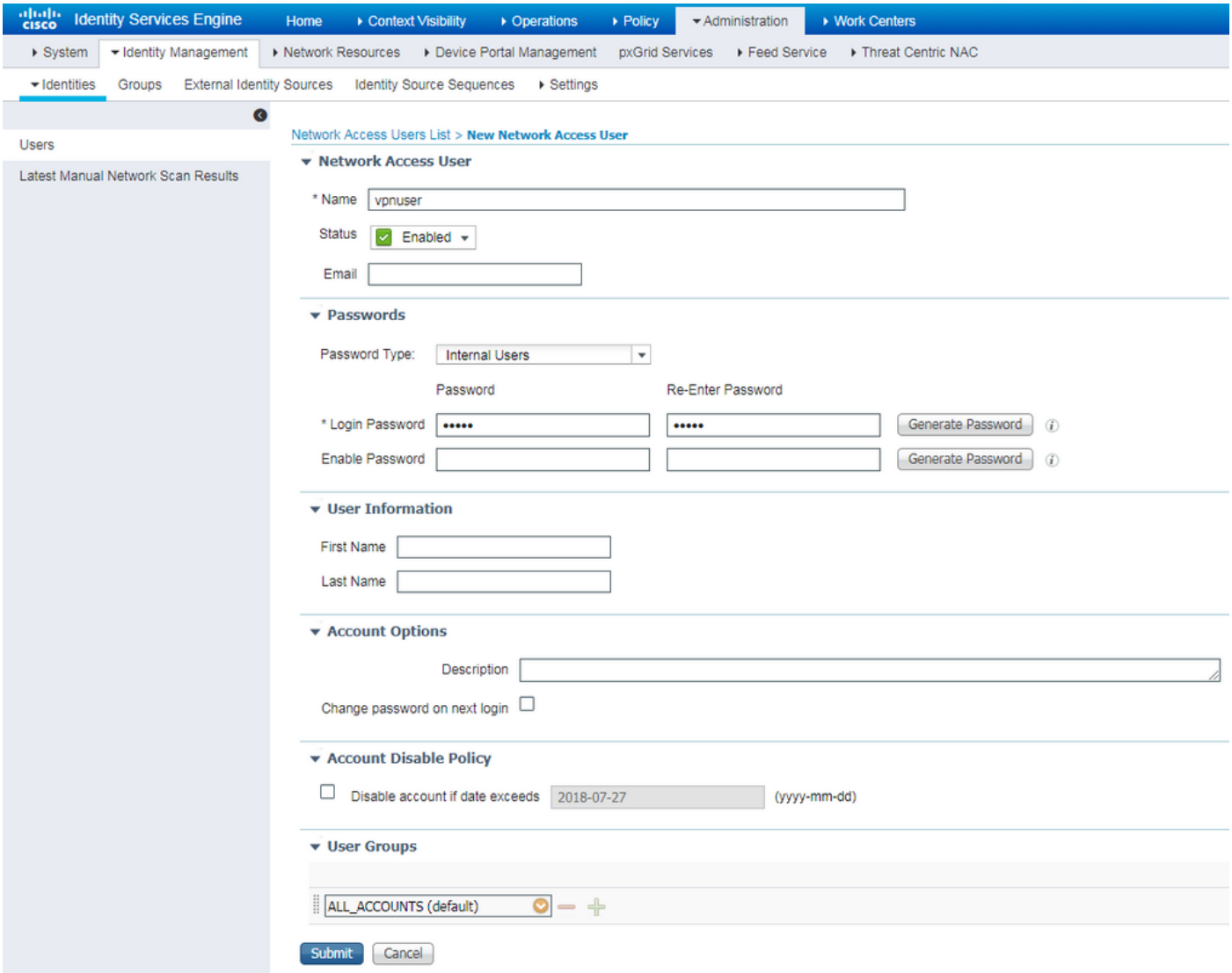
Crear un usuario local en ISE

> **Nota:** Con el método EAP-MD5, ISE sólo admite usuarios locales.

Paso 1. Vaya a **Administration -> Indentity Management -> Identities -> Users**, haga clic en **Add**.

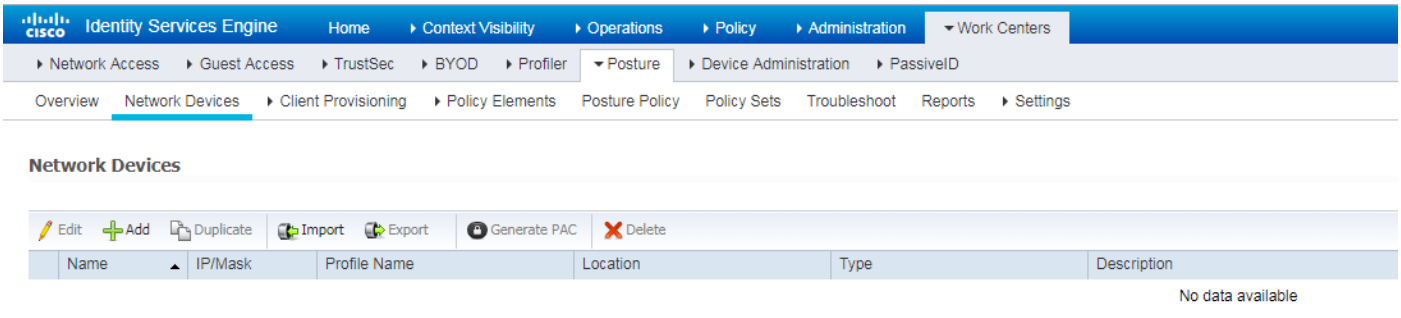


Paso 2. En la página abierta ingrese el nombre de usuario, la contraseña y otra información necesaria y haga clic en **Enviar**.

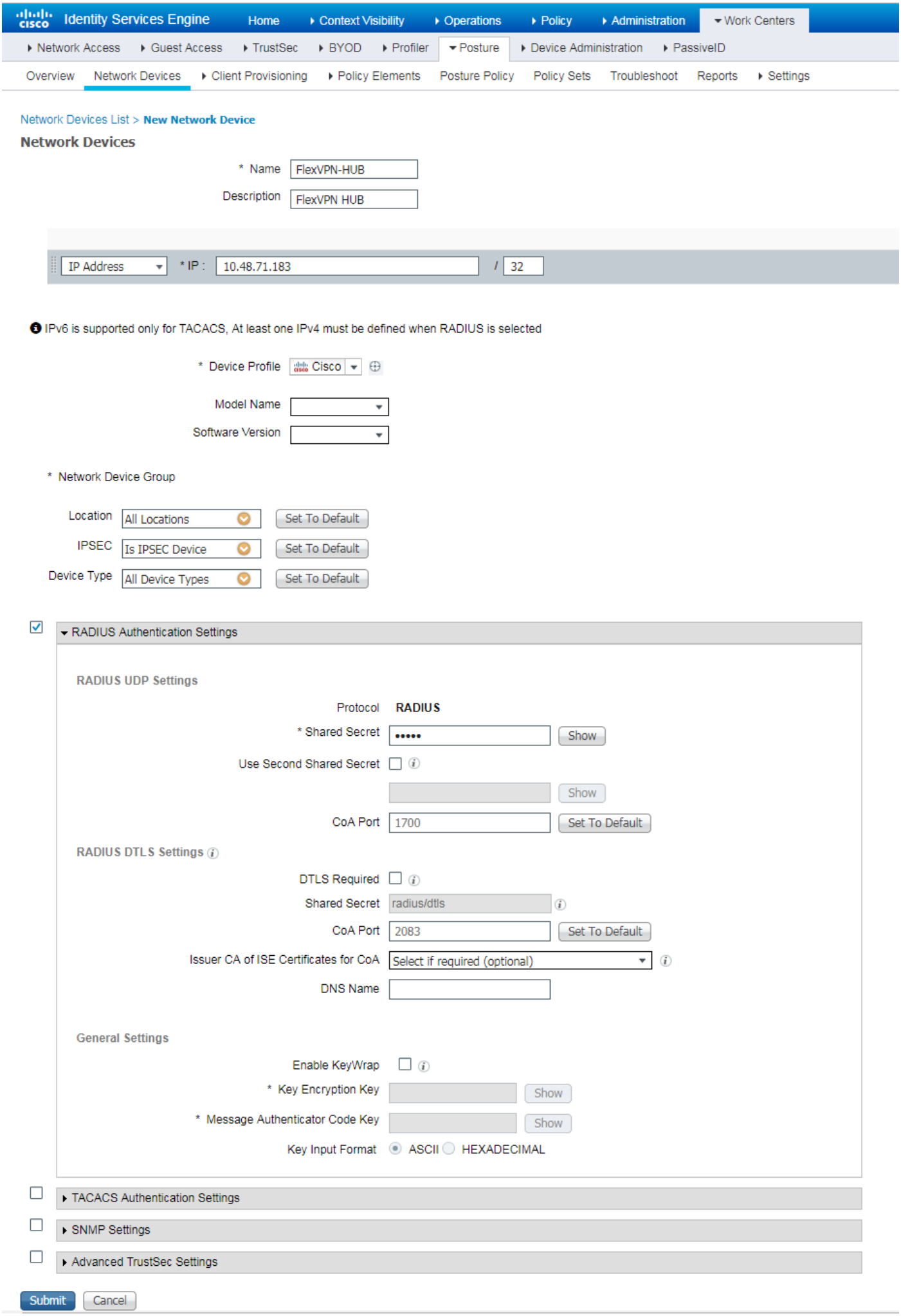


Agregue el HUB FlexVPN como cliente Radius

Paso 1. Vaya a **Centros de trabajo -> Estado -> Dispositivos de red**, haga clic en **Agregar**.



Paso 2. En la página abierta, introduzca el nombre del dispositivo, la dirección IP, otra información necesaria, active la casilla de verificación "Configuración de autenticación RADIUS", introduzca Shared Secret y haga clic en **Enviar** en la parte inferior de la página.

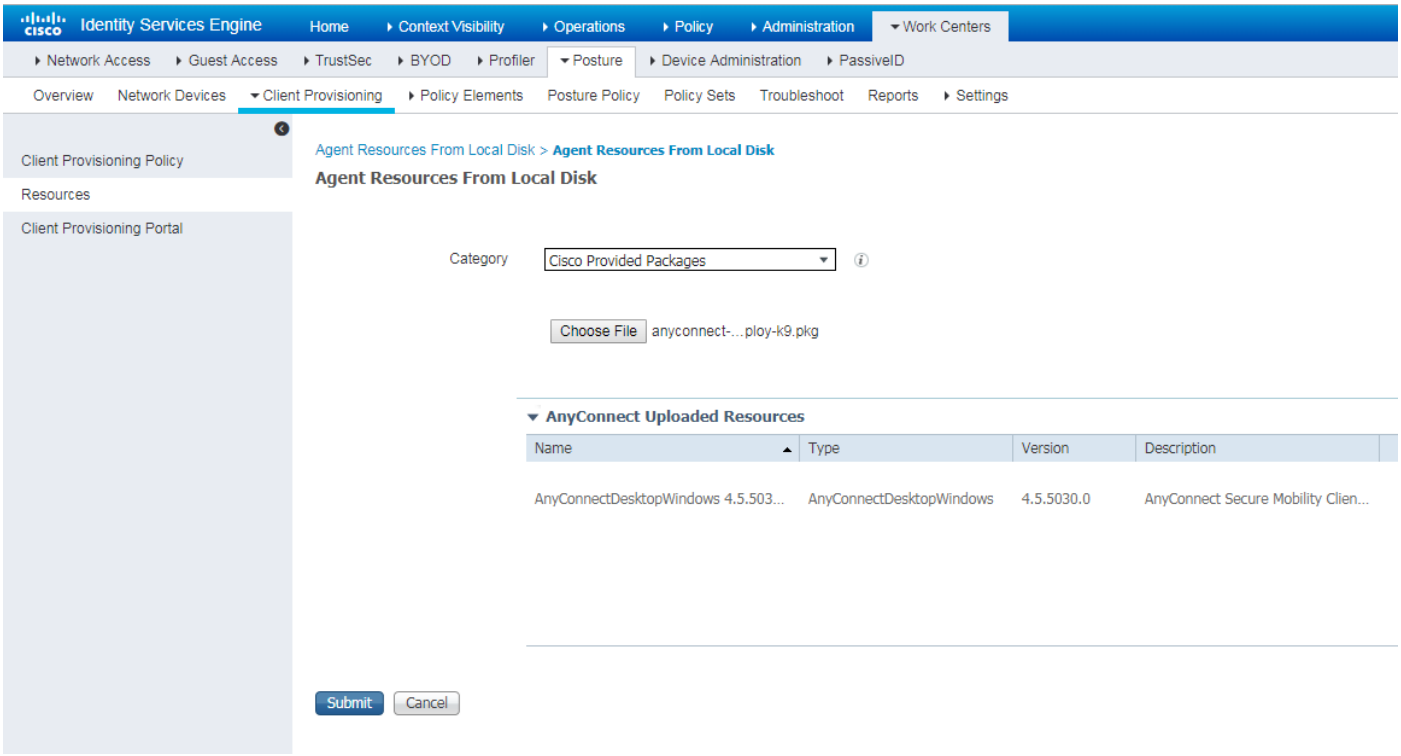

Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Network Access
Guest Access
TrustSec
BYOD
Profiler
Posture
Device Administration
PassiveID
Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Policy Sets
Troubleshoot
Reports
Settings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

Configuración de aprovisionamiento de clientes

Estos son los pasos para preparar la configuración de Anyconnect.

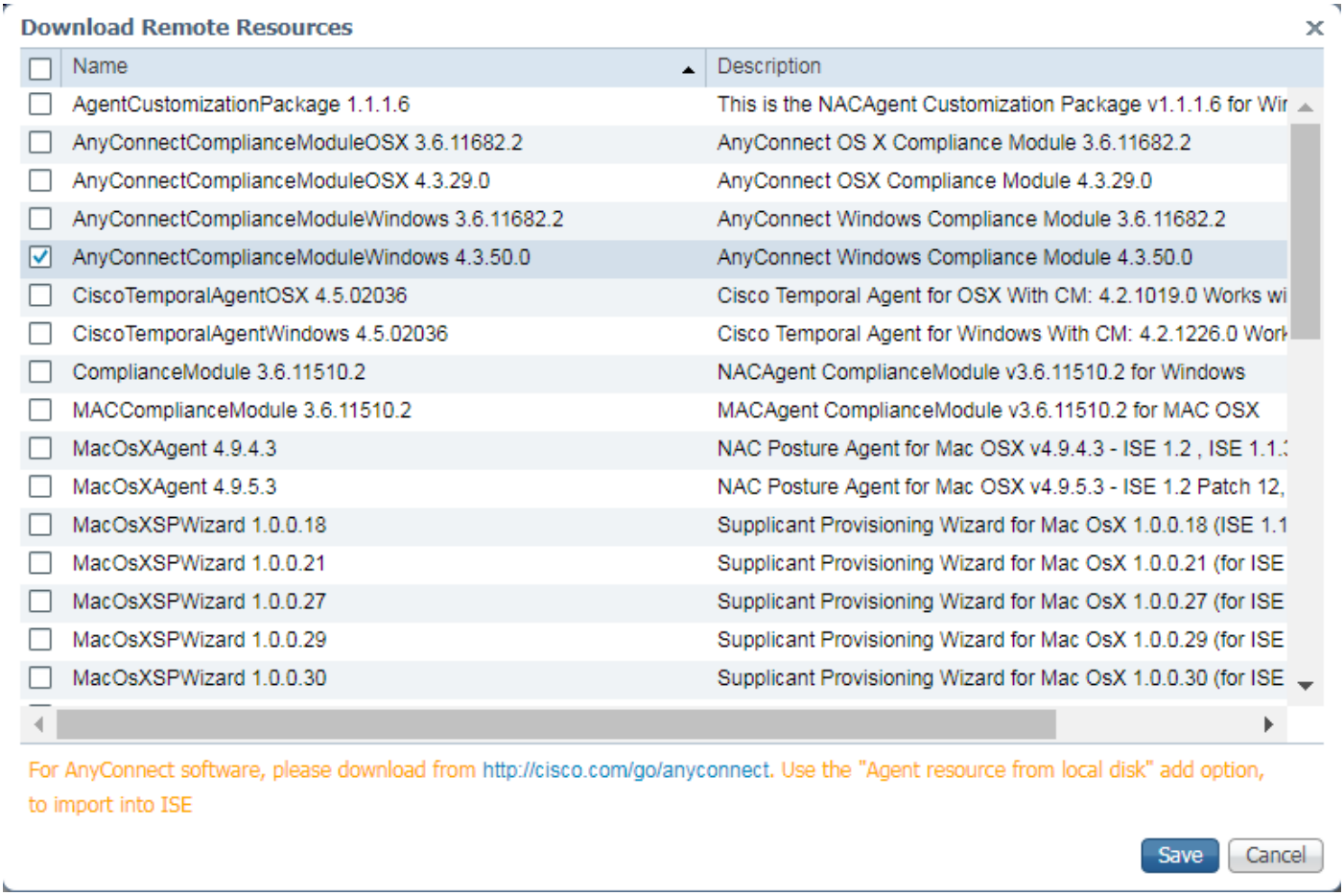
Paso 1. Descarga del paquete Anyconnect. El paquete Anyconnect no está disponible para su descarga directa desde ISE, por lo que antes de empezar, asegúrese de que AC esté disponible en su PC. Este enlace se puede utilizar para la descarga de CA - http://cisco.com/go/anyconnect. En este documento se utiliza el paquete anyconnect-win-4.5.05030-webDeploy-k9.pkg.

Paso 2. Para cargar el paquete de CA en ISE, navegue hasta **Centros de trabajo -> Estado -> Aprovisionamiento de cliente ->** Recursos y haga clic en **Agregar**. Elija **los recursos del agente del disco local**. En la nueva ventana elija **Cisco Provided Packages,** haga clic en **Choose File** y seleccione el paquete AC en su PC.

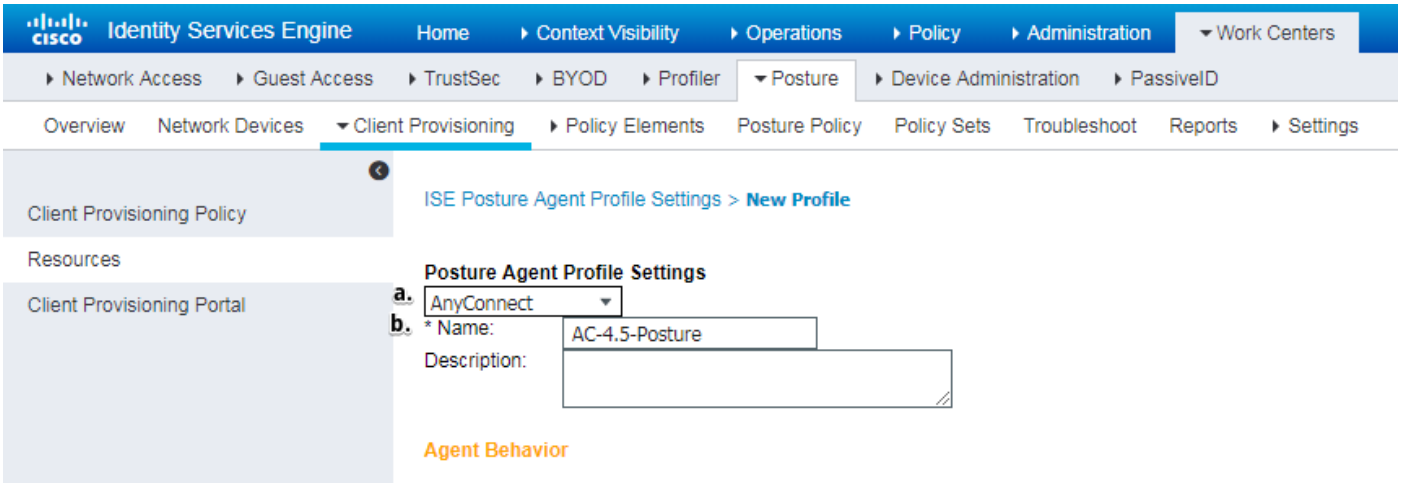


Haga clic en **Enviar** para finalizar la importación. Verifique el hash del paquete y presione **Confirmar**.

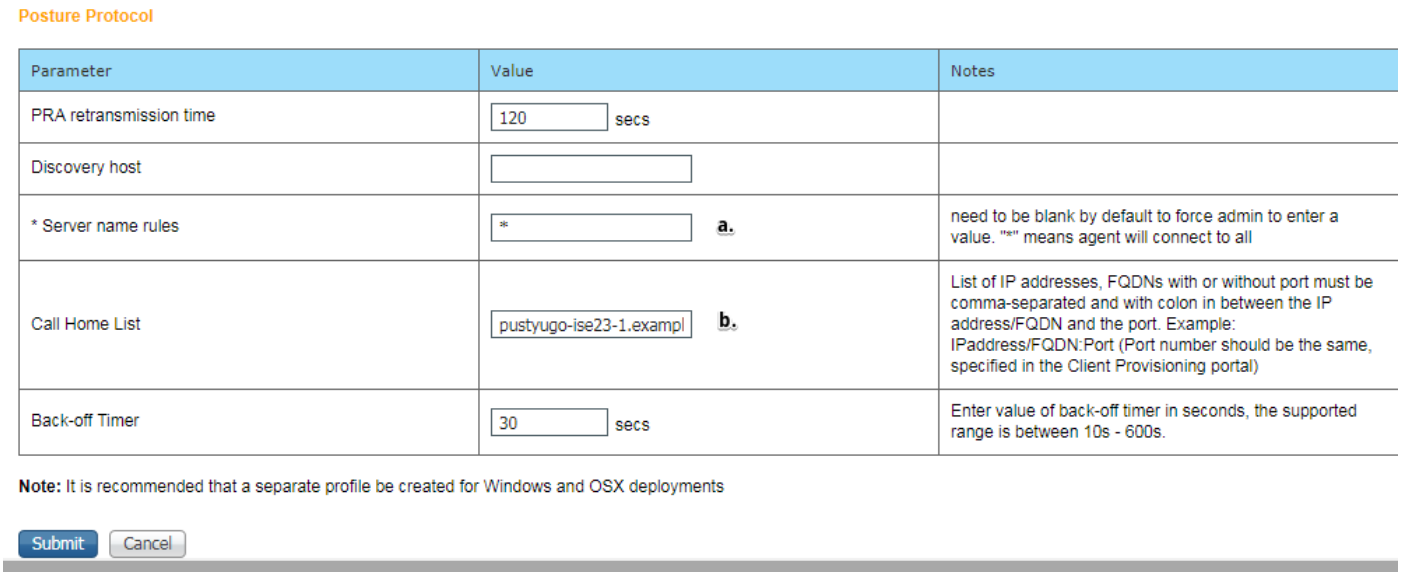
Paso 3. El módulo de cumplimiento debe cargarse en ISE. En la misma página (**Centros de trabajo -> Estado -> Aprovisionamiento de cliente -> Recursos**), haga clic en **Agregar** y seleccione **Recursos de agente del sitio de Cisco**. En la lista de recursos debe verificar un módulo de cumplimiento y hacer clic en **Guardar**. Para este documento AnyConnectComplianceModule se utiliza el módulo de cumplimiento de Windows 4.3.50.0.



Paso 4. Ahora se debe crear el perfil de estado de CA. Haga clic en **Agregar** y elija **agente NAC** o **perfil de estado de Anyconnect**.



- Elija el tipo del perfil. AnyConnect debe utilizarse para este escenario.
- Especifique el nombre del perfil. Vaya a la sección **Protocolo de estado** del perfil



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.

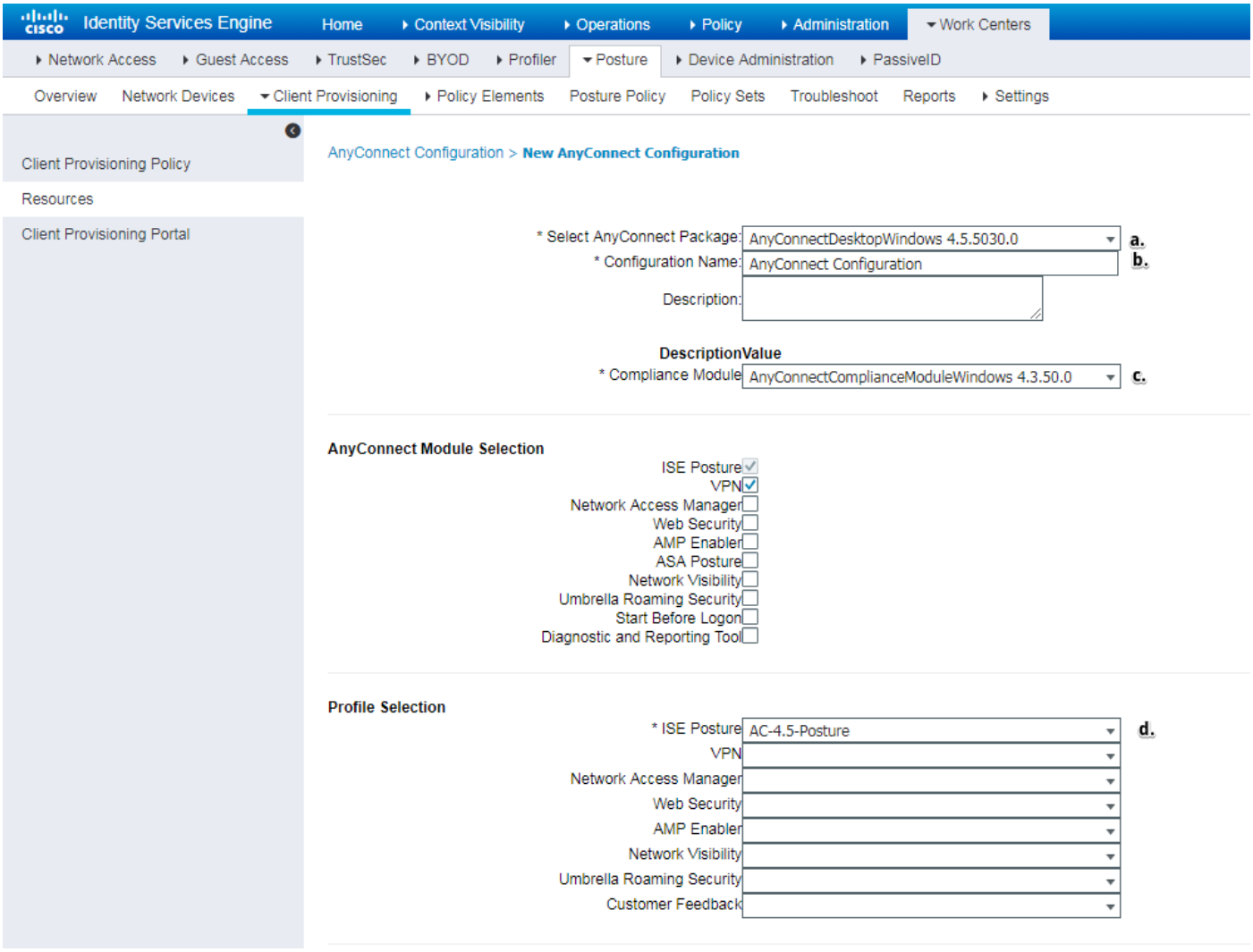
Note: It is recommended that a separate profile be created for Windows and OSX deployments

Submit Cancel

- Especifique **Reglas de nombre de servidor**, este campo no puede estar vacío. El campo puede contener FQDN con comodín que restringe la conexión del módulo de estado de CA a los PSN del espacio de nombres adecuado. Coloque star si se debe permitir cualquier FQDN.

- Los nombres e IP especificados aquí están en uso durante la etapa 2 de la detección de estado (consulte el Paso 14 de la sección "Flujo de estado en ISE 2.2"). Puede separar los nombres por coma, así como agregar el número de puerto después de FQDN/IP utilizando dos puntos.

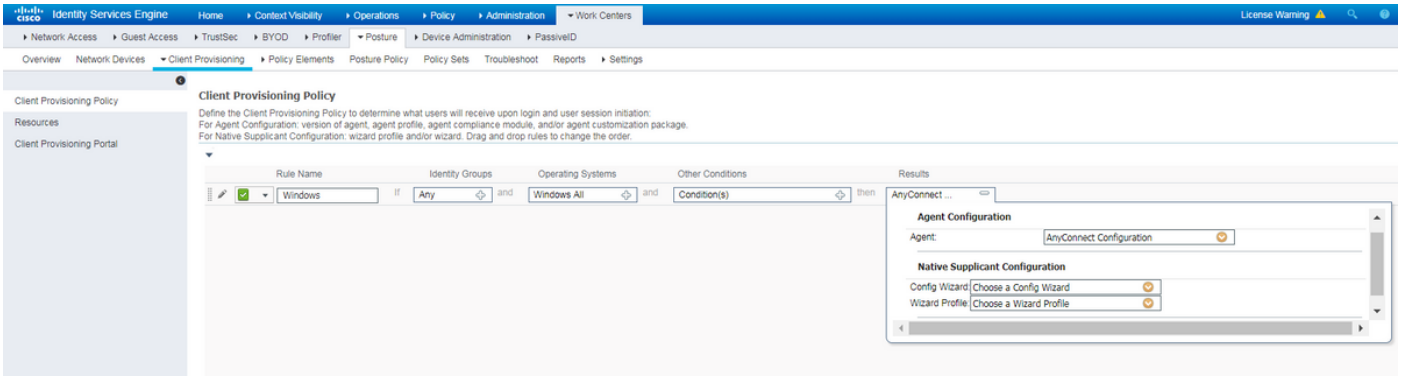
Paso 5.Crear configuración de CA. Navegue hasta **Centros de trabajo -> Estado -> Aprovisionamiento de cliente -> Recursos** y haga clic en **Agregar**, luego seleccione Configuración de AnyConnect.



- Seleccione un paquete AC.
- Proporcione el nombre de la configuración de AC.
- Elija la versión del módulo de cumplimiento.
- Seleccione el perfil de configuración de estado de CA en la lista desplegable.

Paso 6. Configuración de la política de aprovisionamiento del cliente. Vaya a **Centros de trabajo -> Estado -> Aprovisionamiento de cliente**. En caso de configuración inicial, puede rellenar valores vacíos en la política presentada con valores predeterminados. En necesita agregar una política a la configuración de estado existente, desplácese a la política que se puede reutilizar y elija **Duplicar arriba** o **Duplicar abajo.** También se puede crear una nueva política.

Este es el ejemplo de la política utilizada en el documento.

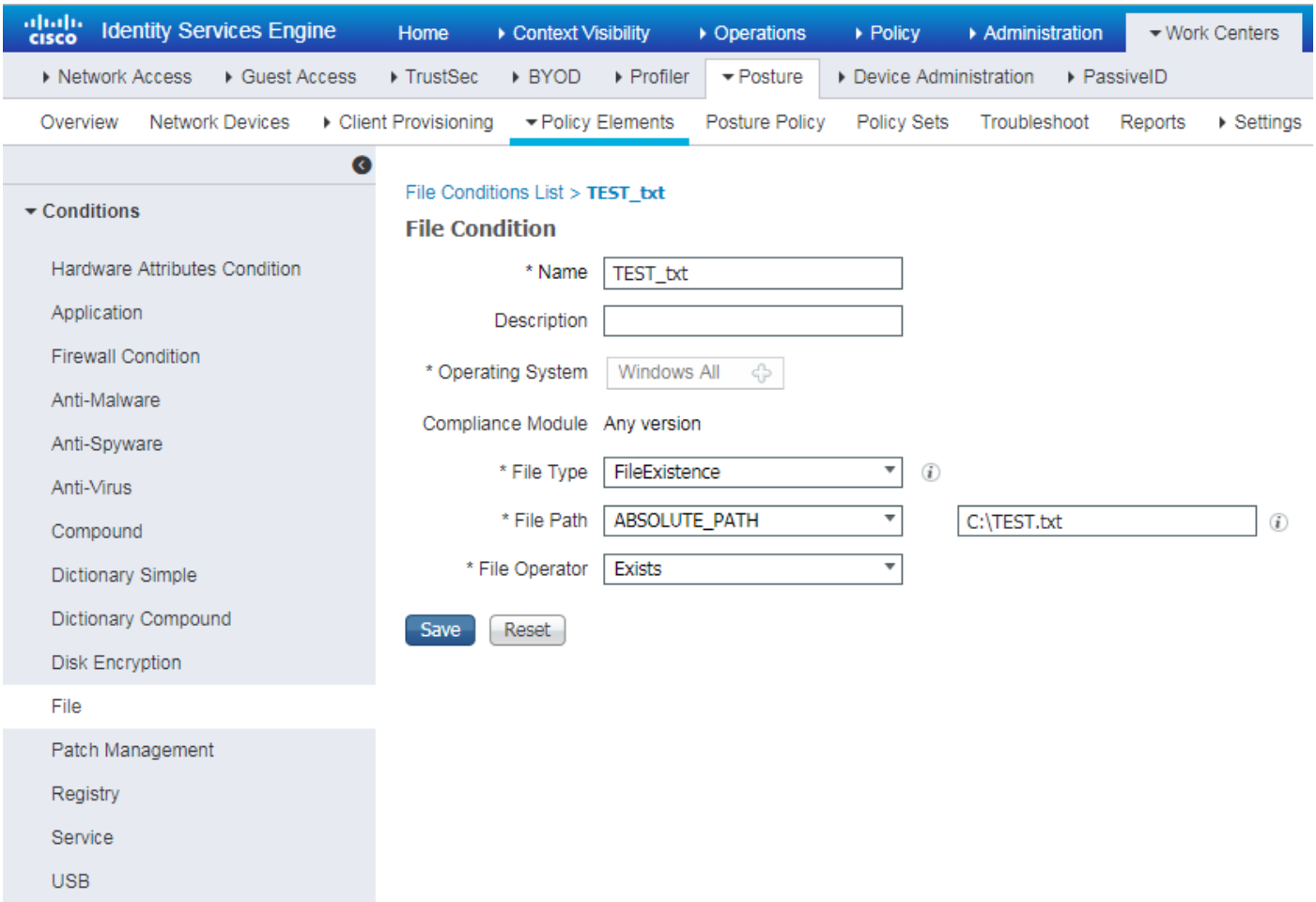


Elija la configuración de AC en la sección de resultados.

Políticas y condiciones de estado

Se usa una simple verificación de estado. ISE está configurado para comprobar la existencia del archivo C:\TEST.txt en el lado del dispositivo final. Los escenarios reales pueden ser mucho más complicados, pero los pasos de configuración generales son los mismos.

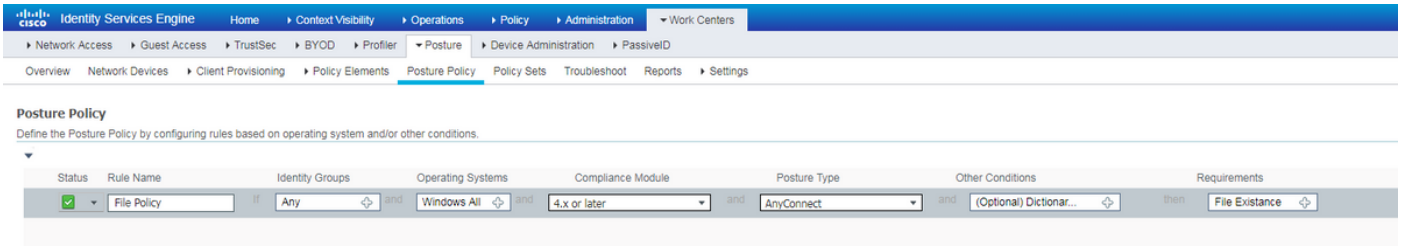
Paso 1. Crear condición de estado. Las condiciones de estado se encuentran en **Centros de trabajo -> Estado -> Elementos de política -> Condiciones**. Elija el tipo de condición de estado y haga clic en **Agregar**. Especifique la información necesaria y haga clic en **Guardar**. A continuación puede encontrar un ejemplo de la condición de servicio que debe comprobar si existe el archivo C:\TEST.txt.



Paso 2.Configuración de los requisitos de estado. Vaya a **Centros de trabajo -> Estado -> Elementos de política -> Requisitos**. Este es un ejemplo de la existencia de archivo TEST.txt:

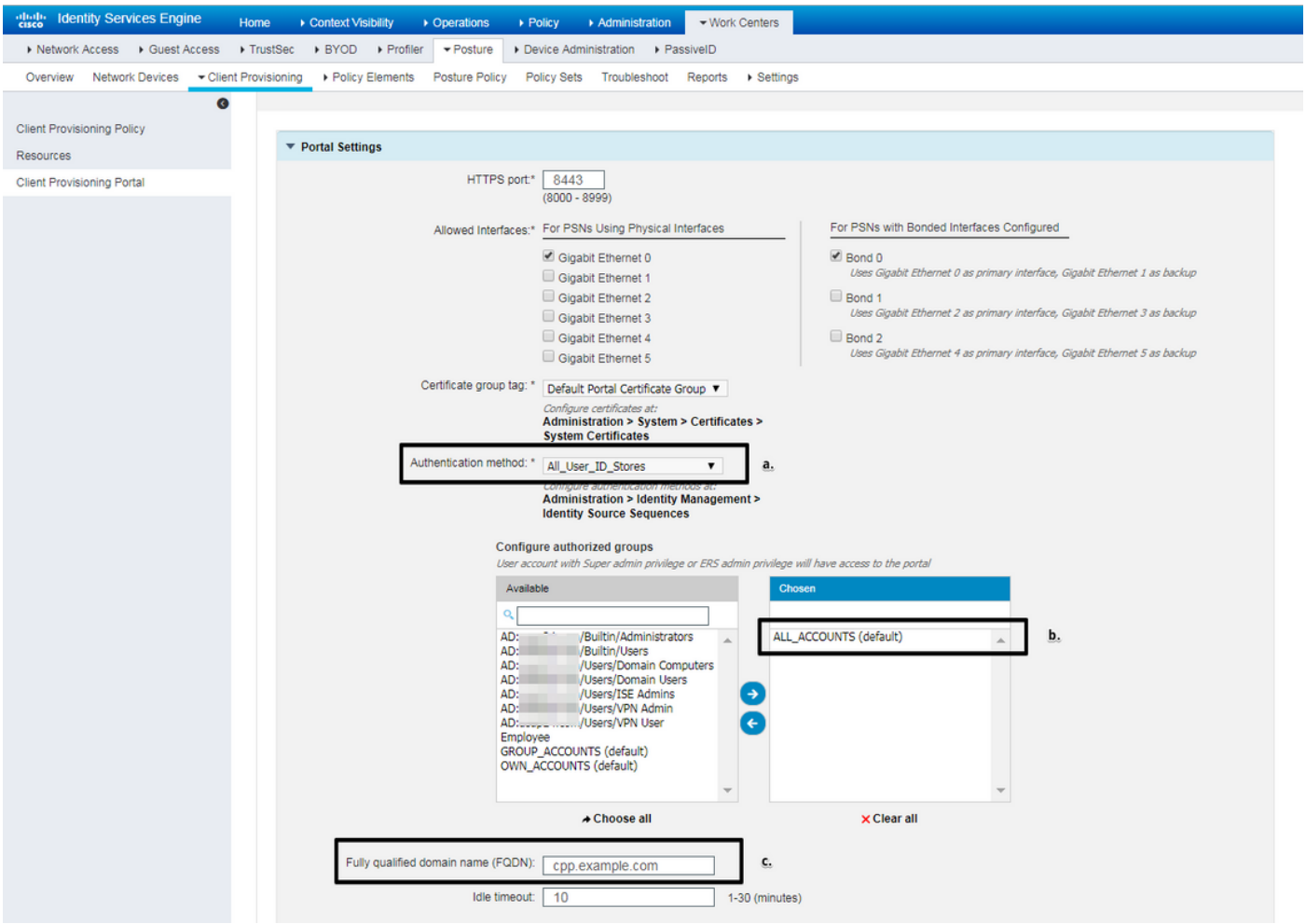
Elija su condición de estado en un nuevo requisito y especifique una acción de remediación.

Paso 3. Configuración de la política de estado. Vaya a **Centros de trabajo -> Estado -> Política de estado**. A continuación puede encontrar un ejemplo de la política utilizada para este documento. La política tiene el requisito de "existencia de archivo" asignado como obligatorio y no tiene asignada ninguna otra condición.



Configurar el portal de aprovisionamiento de clientes

Para el estado sin redirección, la configuración del portal de aprovisionamiento del cliente debe ser editada. Vaya a **Centros de trabajo -> Estado -> Aprovisionamiento de cliente -> Portal de aprovisionamiento de cliente** Puede utilizar el portal predeterminado o crear el suyo propio.



Estos ajustes deben editarse en la configuración del portal para el escenario de no redirección:

- En Authentication (Autenticación), especifique la secuencia de origen de identidad que se debe utilizar si SSO no encuentra la sesión para el usuario.

- De acuerdo con la lista Secuencia de origen de identidad seleccionada, se rellena la lista de grupos disponibles. En este punto, debe seleccionar los grupos autorizados para iniciar sesión en el portal.

- Se debe especificar el FQDN del portal de aprovisionamiento de clientes. Este FQDN debe resolverse para las IPs PSNs de ISE. Se debe indicar a los usuarios que especifiquen el FQDN en el explorador web durante el primer intento de conexión.

Configurar perfiles y políticas de autorización

El acceso inicial para el cliente cuando el estado no está disponible debe estar restringido. Esto podría lograrse de varias maneras:

- ID de filtro de RADIUS: con este atributo, la ACL definida localmente en NAD se puede asignar al usuario con estado desconocido. Como este es un atributo RFC estándar, este enfoque debería funcionar bien para todos los proveedores de NAD.

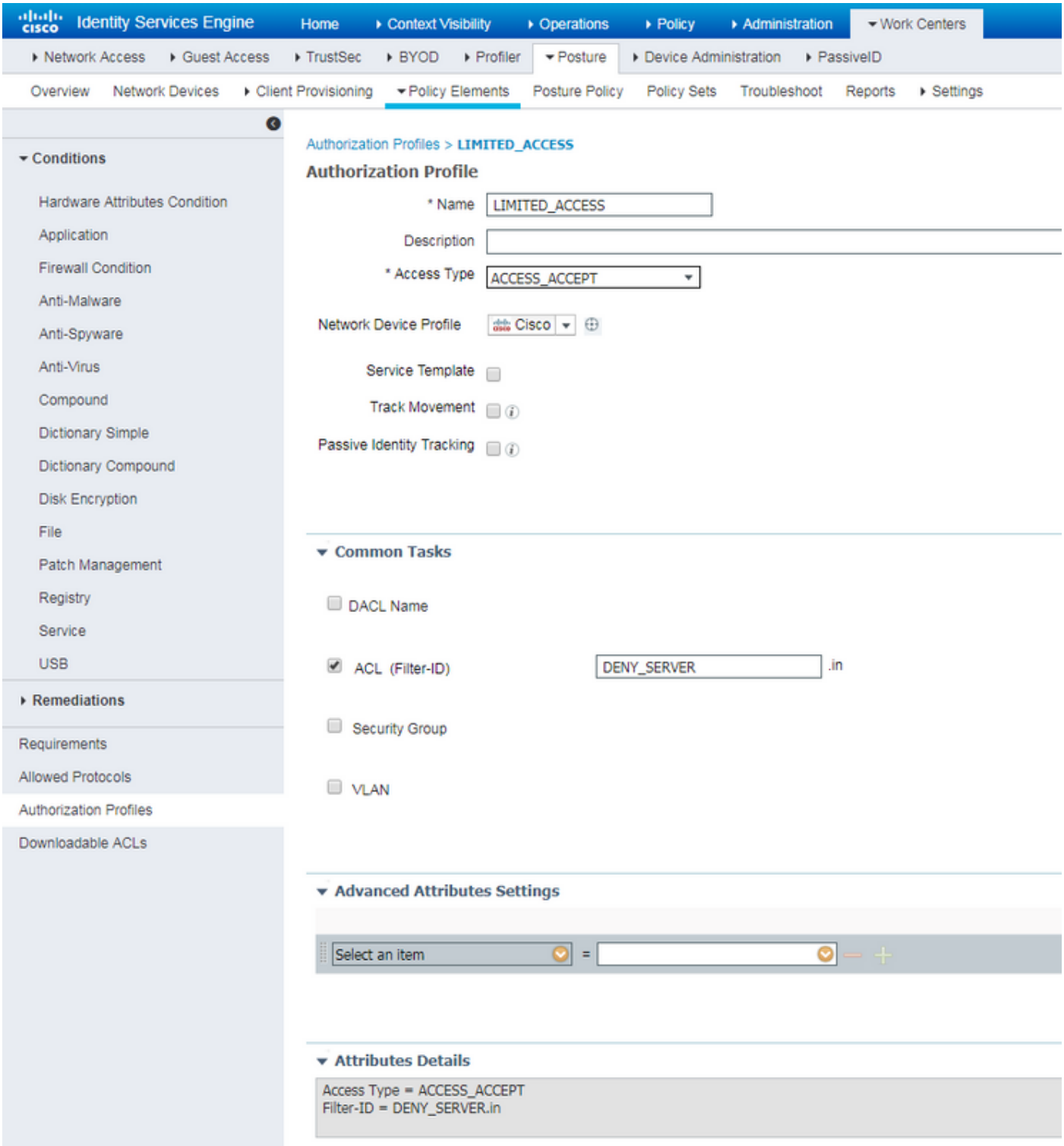
- Cisco:cisco-av-pair = ip:interface-config - muy similar a Radius Filter-Id, ACL definida localmente en NAD se puede asignar al usuario con estado desconocido. Ejemplo de configuración:
  cisco-av-pair = ip:interface-config=ip access-group DENY_SERVER in

Paso 1. Configure el perfil de autorización.

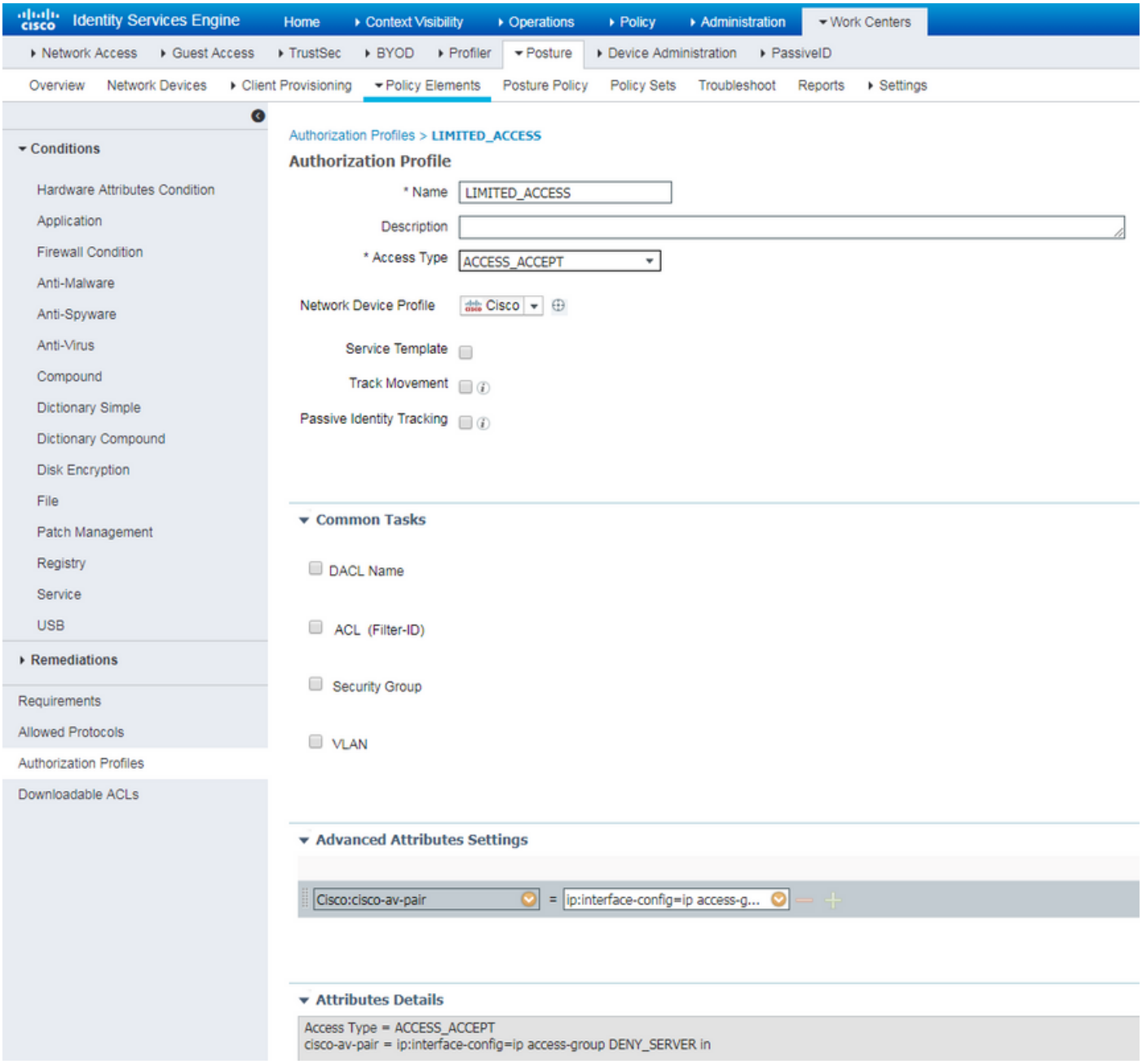
Como de costumbre, se requieren dos perfiles de autorización. La primera debe contener cualquier tipo de restricción de acceso a la red. Este perfil se puede aplicar a las autenticaciones para las que el estado no es igual a conforme. El segundo perfil de autorización puede contener sólo acceso de permiso y se puede aplicar para una sesión con el estado igual a conforme.

Para crear el perfil de autorización, vaya a **Centros de trabajo -> Estado -> Elementos de política -> Perfiles de autorización**.

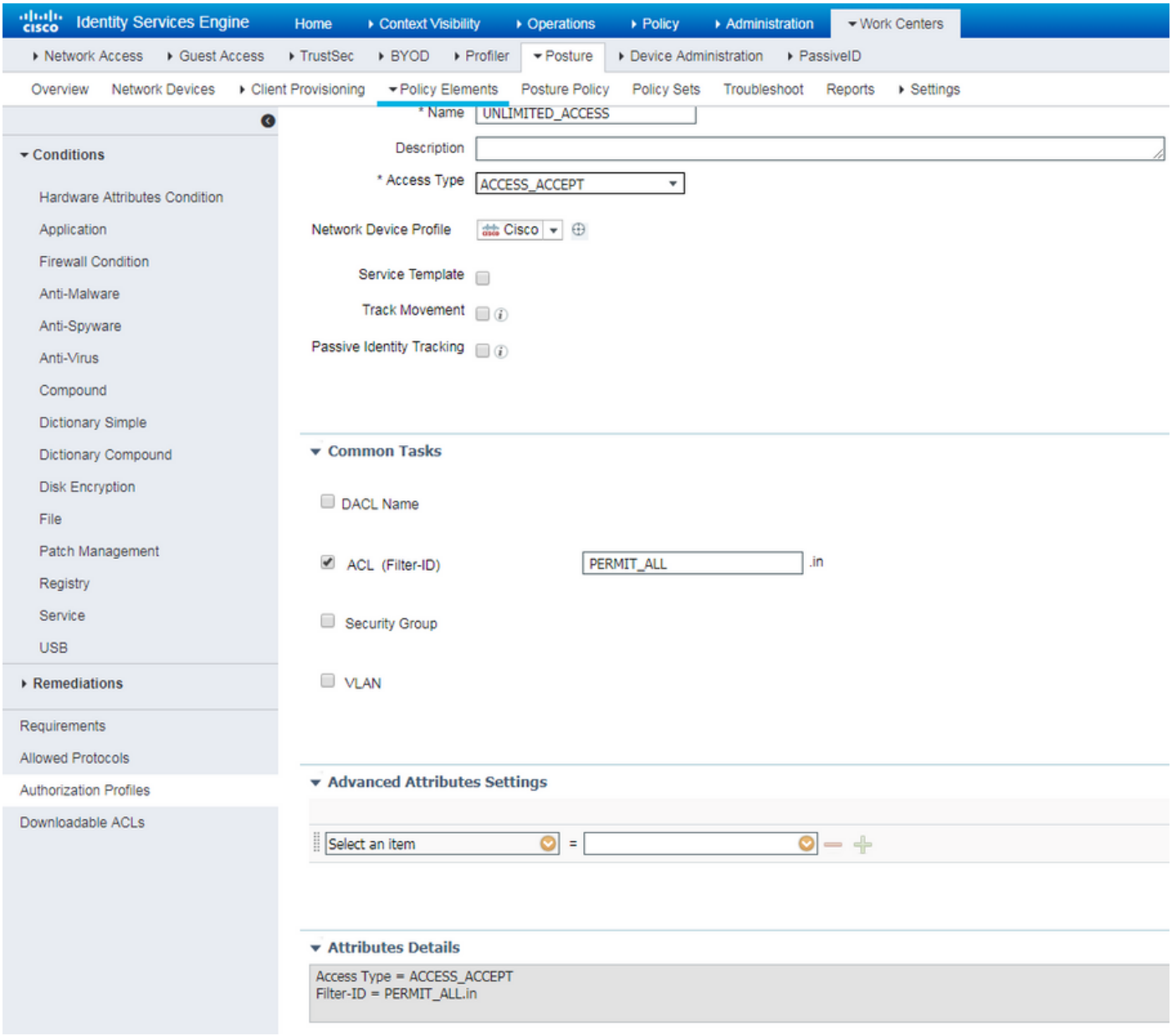
Ejemplo de perfil de acceso restringido con ID de filtro de RADIUS:



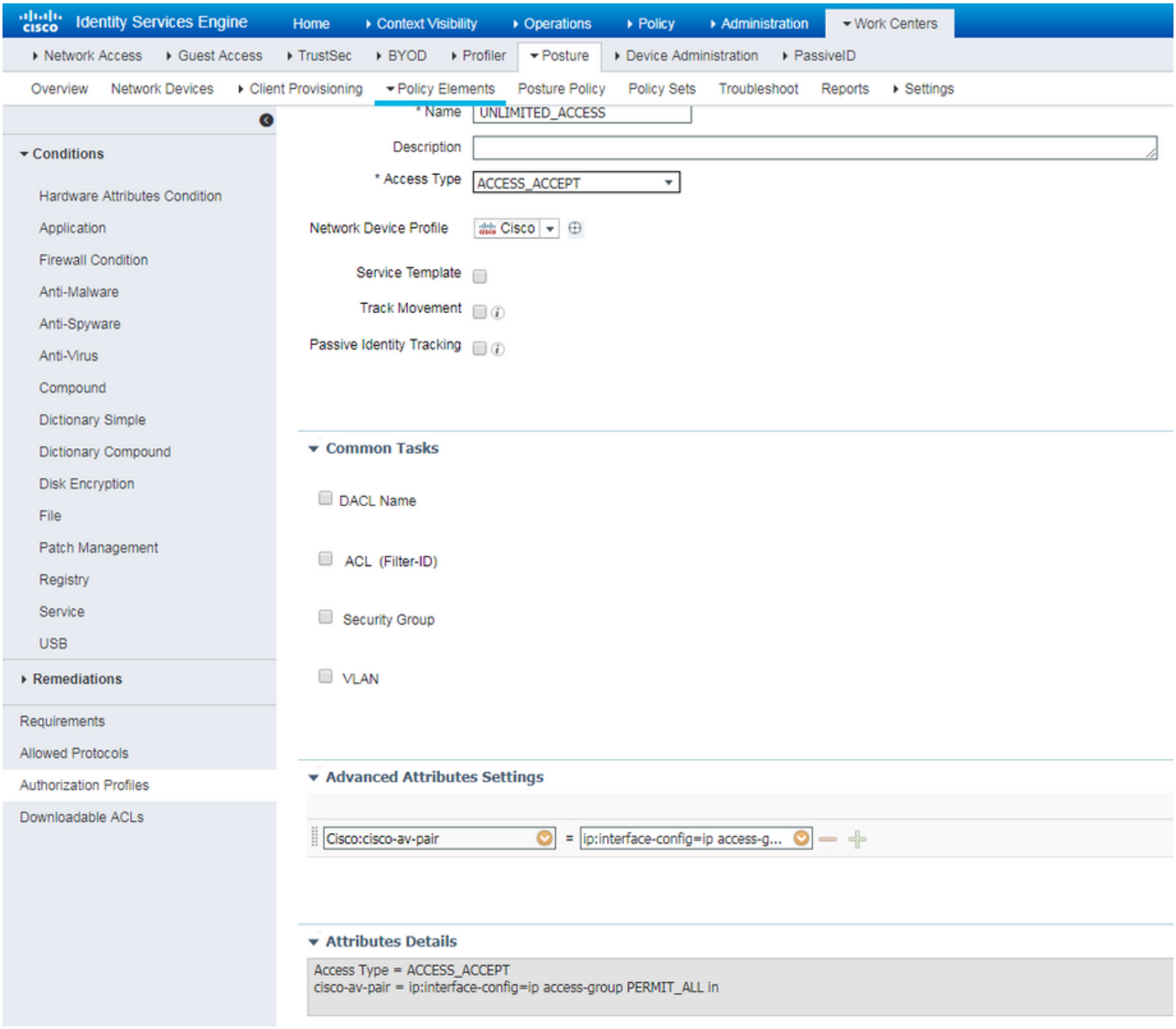
Ejemplo de perfil de acceso restringido con cisco-av-pair:



Ejemplo de perfil de acceso ilimitado con ID de filtro de RADIUS:



Ejemplo de perfil de acceso ilimitado con cisco-av-pair:



Paso 2. Configure la política de autorización. Durante este paso, se deben crear dos políticas de autorización. Uno para hacer coincidir la solicitud de autenticación inicial con el estado desconocido y el segundo para asignar el acceso completo después de un proceso de estado exitoso.

Se trata de un ejemplo de políticas de autorización sencillas para este caso:

La configuración de la política de autenticación no forma parte de este documento, pero debe tener en cuenta que la autenticación debe ser exitosa antes de que comience el procesamiento de la política de autorización.

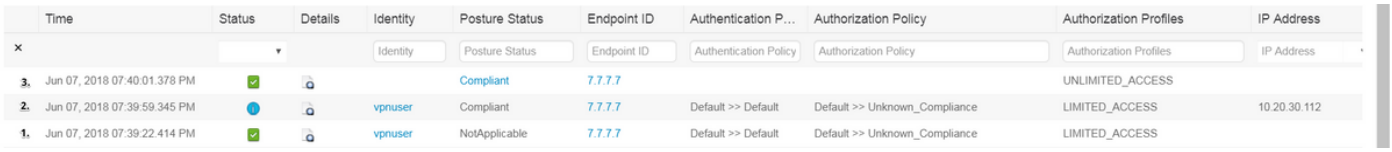
Verificación

La verificación básica del flujo puede constar de tres pasos principales:

Paso 1. Verificación de la sesión VPN RA en el 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
```

Paso 2. Verificación del flujo de autenticación (registros activos de RADIUS):



	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	

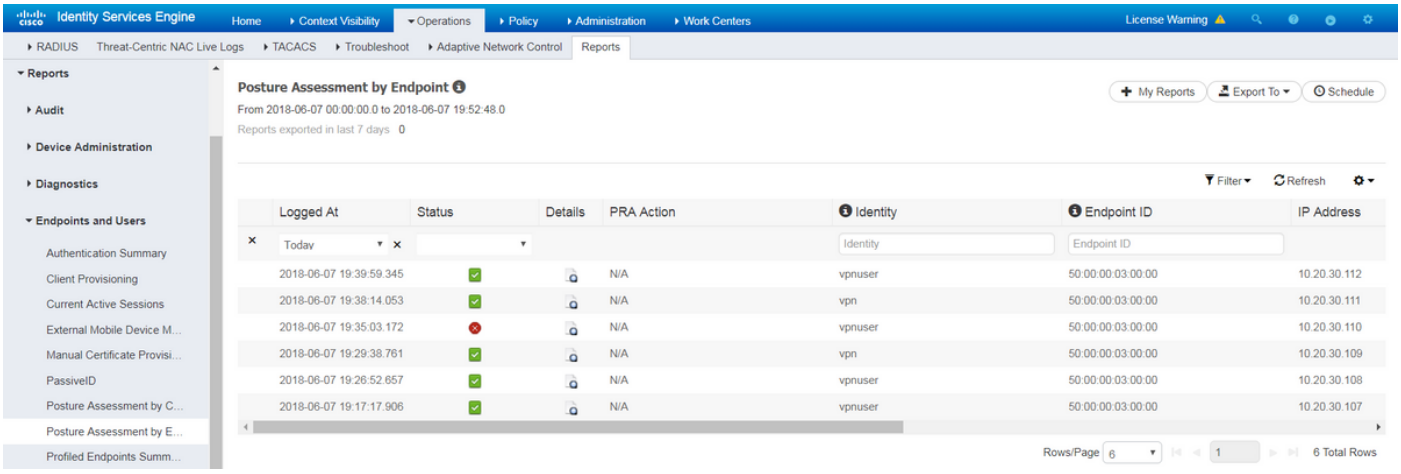
1. Autenticación inicial. Para este paso, puede que le interese validar qué perfil de autorización se ha aplicado. Si se ha aplicado un perfil de autorización inesperado, investigue el informe de autenticación detallado. Para abrir este informe, haga clic en la lupa de la columna Detalles. Puede comparar atributos en un informe de autenticación detallado con una condición en la política de autorización que espera que coincida.

2. Cambio de datos de sesión; en este ejemplo concreto, el estado de sesión ha cambiado de No aplicable a Conforme.

3. COA para el dispositivo de acceso a la red. Este COA debe tener éxito para introducir la nueva autenticación del lado de NAD y la nueva asignación de políticas de autorización en el lado de ISE. Si el COA ha fallado, puede abrir un informe detallado para investigar el motivo. Los problemas más comunes con COA pueden ser: Tiempo de espera de COA: en este caso, PSN que ha enviado la solicitud no se configura como cliente COA en el lado de NAD, o la solicitud de COA se ha descartado en algún lugar del camino.COA negativo ACK - indicar que el COA ha sido recibido por NAD pero debido a alguna razón no se puede confirmar el funcionamiento del COA. Para este escenario, el informe detallado debe contener una explicación más detallada.

Como el router basado en IOS XE se ha utilizado como NAD para este ejemplo, no puede ver ninguna solicitud de autenticación subsiguiente para el usuario. Esto sucede debido al hecho de que ISE utiliza la inserción COA para IOS XE, lo que evita la interoperabilidad del servicio VPN. En este escenario, el COA mismo contiene nuevos parámetros de autorización, por lo que no se necesita la reautenticación.

Paso 3.Verificación del informe de estado - Vaya a **Operaciones -> Informes -> Informes -> Terminales y usuarios -> Evaluación del estado por terminal**.



Puede abrir un informe detallado desde aquí para cada evento concreto a fin de comprobar, por ejemplo, a qué ID de sesión pertenece este informe, a qué requisitos exactos de estado seleccionó ISE para el terminal y el estado para cada requisito.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

1. Depuraciones IKEv2 para recolectar en la cabecera:

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

2. La AAA debuta para ver la asignación de atributos locales y/o remotos:

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

3. DART del cliente AnyConnect.
4. Para la resolución de problemas de procesos de estado, estos componentes de ISE deben habilitarse en la depuración en los nodos de ISE donde puede ocurrir el proceso de estado:**client-webapp**: componente responsable del aprovisionamiento de agentes. Archivos de registro de destino **guest.log** y **ise-psc.log**.**invitados** - componente responsable de la búsqueda del componente del portal de aprovisionamiento del cliente y del propietario de la sesión (cuando la solicitud llega a un PSN incorrecto). Archivo de registro de destino - **guest.log.aprovisionamiento: componente responsable del procesamiento de la política de aprovisionamiento del cliente. Archivo de registro de destino - guest.log.postura** - todos los eventos relacionados con la postura. Archivo de registro de destino - **ise-psc.log**
5. Para la resolución de problemas del lado del cliente puede utilizar:**AnyConnect.txt** - Este archivo se puede encontrar en el paquete DART y se utiliza para la resolución de problemas de VPN.**acisensa.log**: en caso de fallo en el aprovisionamiento del cliente, este archivo se crea en la misma carpeta a la que se ha descargado la NSA (directorio de descargas para Windows normalmente),**AnyConnect_ISEPosture.txt** - Este archivo se puede encontrar en el paquete DART en el directorio **Cisco AnyConnect ISE Posture Module**. Toda la información sobre la detección de ISE PSN y los pasos generales del flujo de estado se registran en este archivo.