# Configurer la position ISE avec FlexVPN

## Contenu

Introduction Conditions préalables **Conditions requises Components Used** Informations générales Configuration Diagramme du réseau Configuration du serveur DNS Configuration initiale IOS XE Configurer le certificat d'identité **Configurer IKEv2** Configuration du profil client Anyconnect **Configuration ISE** Configuration des certificats Admin et CPP Créer un utilisateur local sur ISE Ajouter le concentrateur FlexVPN en tant que client Radius Configuration de l'approvisionnement client Politiques et conditions de posture Configurer le portail d'approvisionnement du client Configurer les profils et les stratégies d'autorisation Vérification Dépannage

## Introduction

Ce document fournit un exemple de configuration d'une tête de réseau IOS XE pour l'accès à distance avec posture à l'aide de la méthode d'authentification AnyConnect IKEv2 et EAP-Message Digest 5 (EAP-MD5).

## Conditions préalables

## **Conditions requises**

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration VPN d'accès à distance (RA) FlexVPN sur IOS XE
- Configuration du client AnyConnect (AC)
- Flux de position sur Identity Service Engine (ISE) 2.2 et versions ultérieures
- Configuration des composants de position sur ISE
- Configuration du serveur DNS sur Windows Server 2008 R2

### **Components Used**

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco CSR1000V exécutant IOS XE 16.8 [Fuji]
- Client AnyConnect version 4.5.03040 sous Windows 7
- Cisco ISE 2.3
- Serveur 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.

## Informations générales

Pour vous assurer que les mesures de sécurité réseau imposées restent pertinentes et efficaces, Cisco ISE vous permet de valider et de maintenir des fonctionnalités de sécurité sur tout ordinateur client qui accède au réseau protégé. En utilisant des politiques de posture conçues pour s'assurer que les paramètres de sécurité ou les applications les plus récents sont disponibles sur les machines clientes, l'administrateur Cisco ISE peut s'assurer que toute machine cliente qui accède au réseau respecte et continue de respecter les normes de sécurité définies pour l'accès au réseau de l'entreprise. Les rapports de conformité de la position fournissent à Cisco ISE un instantané du niveau de conformité de la machine cliente au moment de la connexion de l'utilisateur, ainsi que chaque fois qu'une réévaluation périodique se produit.

La posture peut être représentée par trois éléments principaux :

- ISE en tant que point de distribution et de décision de la configuration des politiques. Du point de vue de l'administrateur sur ISE, vous configurez les stratégies de posture (quelles conditions précises doivent être remplies pour marquer le périphérique comme conforme à l'entreprise), les stratégies de provisionnement du client (quel logiciel d'agent doit être installé sur quel type de périphérique) et les stratégies d'autorisation (quel type d'autorisations doit être attribué, dépend de leur statut).
- 2. Le périphérique d'accès au réseau (NAD) en tant que point d'application des politiques. Du côté NAD, les restrictions d'autorisation réelles sont appliquées au moment de l'authentification de l'utilisateur. ISE en tant que point de stratégie fournit des paramètres d'autorisation tels que la liste de contrôle d'accès (ACL).Traditionnellement, pour que la posture se produise, les NAD doivent prendre en charge le changement d'autorisation (CoA) pour authentifier à nouveau l'utilisateur après avoir déterminé l'état de posture du point de terminaison. Les NAD ISE 2.2 de départ ne sont pas nécessaires pour prendre en charge la redirection.

**Note**: Les routeurs exécutant IOS XE ne prennent pas en charge la redirection.**Note**: Le logiciel IOS XE doit avoir des correctifs pour que CoA avec ISE soit pleinement opérationnel .

### CSCve16269 IKEv2 CoA ne fonctionne pas avec ISE

 <u>CSCvi90729</u> IKEv2 CoA ne fonctionne pas avec ISE (coa-push=TRUE au lieu de true)
 Logiciel d'agent comme point de collecte de données et d'interaction avec l'utilisateur final. L'agent reçoit des informations sur les exigences de position de l'ISE et fournit un rapport à l'ISE concernant l'état des exigences. Ce document est basé sur Anyconnect ISE Posture Module qui est le seul à prendre en charge complètement la posture sans redirection.

Le flux de posture sans redirection est très bien documenté dans l'article "<u>Comparaison des styles</u> <u>de posture ISE pour Pre et Post 2.2</u>« , section « Flux de posture dans ISE 2.2 ».

Le provisionnement du module de posture ISE Anyconnect avec FlexVPN peut être effectué de 2 manières différentes :

• Manuel : le module est installé manuellement sur la station de travail du client à partir du package Anyconnect disponible sur le portail de téléchargement de logiciels Cisco : <u>https://software.cisco.com/download/home/283000185</u>.

Les conditions suivantes doivent être remplies pour le travail de posture avec le provisionnement manuel du module ISE de posture :

1. Le serveur de noms de domaine (DNS) doit résoudre les adresses IP FQDN (Fully Qualified Domain Name) **enroll.cisco.com** en noeud PSN (Policy Service Nodes). Lors de la première tentative de connexion, le module de posture ne dispose d'aucune information sur les PSN disponibles. Il envoie des sondes de détection pour rechercher les PSN disponibles. FQDN enroll.cisco.com est utilisé dans l'une de ces sondes.

2. Le port TCP 8905 doit être autorisé pour les adresses IP de PSN. La position passe par le port TCP 8905 dans ce scénario.

3. Le certificat d'administrateur sur les noeuds PSN doit avoir enroll.cisco.com dans le champ SAN. La connexion entre l'utilisateur VPN et le noeud PSN via TCP 8905 est protégée via le certificat Admin et l'utilisateur reçoit un avertissement de certificat s'il n'existe aucun nom « enroll.cisco.com » dans le certificat Admin du noeud PSN.

**Note**: Selon le certificat <u>RFC6125</u>, les CN doivent être ignorés si des valeurs SAN sont spécifiées. Cela signifie que nous devons également ajouter des CN de certificat Admin dans le champ SAN.

 Provisioning automatique via Client Provisioning Portal (CPP) : le module est téléchargé et installé à partir de l'ISE en accédant directement au CPP via le FQDN du portail.
 Les conditions suivantes doivent être remplies pour le travail de posture avec l'approvisionnement automatique du module ISE de posture :

1. DNS doit résoudre **le nom de domaine complet des** adresses IP **CPP** en noeud de service de stratégie (PSN).

2. Les ports TCP 80, 443 et le port de CPP (8443 par défaut) doivent être autorisés pour les adresses IP de PSN. Le client doit ouvrir le FQDN CPP directement via HTTP (sera redirigé vers HTTPS) ou HTTPS, cette demande sera redirigée vers le port de CPP (8443 par défaut) et la posture passe par ce port.

3. Les certificats Admin et CPP sur les noeuds PSN doivent avoir un nom de domaine complet CPP dans le champ SAN. La connexion entre l'utilisateur VPN et le noeud PSN via TCP 443 est protégée par le certificat Admin et la connexion sur le port CPP est protégée par le certificat CPP.

**Note**: Selon le certificat <u>RFC6125</u>, les CN doivent être ignorés si des valeurs SAN sont spécifiées. Cela signifie que nous devons également ajouter des CN de certificats Admin et CPP dans le champ SAN des certificats correspondants.

**Note**: Si le logiciel ISE ne contient pas de correctif pour <u>CSCvj76466</u>, le provisionnement de la position ou du client ne fonctionnera que si le provisionnement de la position ou du client est effectué sur le même PSN sur lequel le client a été authentifié.

En cas de position avec FlexVPN, le flux inclut les étapes suivantes :

1. L'utilisateur se connecte au concentrateur FlexVPN à l'aide du client Anyconnect.

2. ISE envoie Access-Accepcept au concentrateur FlexVPN avec le nom de la liste de contrôle d'accès doit être appliqué pour restreindre l'accès.

3 bis. Première connexion avec le provisionnement manuel : le module de posture ISE commence à détecter le serveur de stratégies qui envoie l'analyseur à enroll.cisco.com via le port TCP 8905. En conséquence, le module de posture télécharge le profil de posture configuré et met à jour le module de conformité côté client.

Au cours des prochaines tentatives de connexion, le module de posture ISE utilisera également les noms et les adresses IP spécifiés dans la liste Call Home List du profil de posture pour la détection du serveur de stratégies.

3 ter. Première connexion avec l'approvisionnement automatique - le client ouvre CPP via FQDN. L'assistant de configuration réseau est téléchargé sur la station de travail du client, puis télécharge et installe le module ISE Posture, le module de conformité ISE et le profil de position.

Au cours des prochaines tentatives de connexion, le module de posture ISE utilisera les noms et les adresses IP spécifiés dans la liste Call Home List du profil de posture pour la détection du serveur de stratégies.

4. Le module Posture lance des contrôles de conformité et envoie les résultats de la vérification à l'ISE.

5. Si l'état du client est Conforme, ISE envoie Access-Accepcept au concentrateur FlexVPN avec le nom de la liste de contrôle d'accès qui doit être appliquée au client conforme.

6, le client accède au réseau.

Plus de détails sur le processus de posture vous pouvez trouver dans le document "<u>Comparaison</u> <u>des styles de posture ISE pour pré et post 2.2</u>« .

## Configuration

Diagramme du réseau



L'utilisateur VPN n'aura accès au serveur (10.0.0.10) que s'il a un état conforme.

### Configuration du serveur DNS

Dans ce document, Windows Server 2008 R2 est utilisé comme serveur DNS.

Étape 1. Ajouter un enregistrement d'hôte (A) pour enroll.cisco.com pointant vers l'adresse IP de PSN :

File Action Wew Help     Image: PUSTVUGO-DC-1   Image: Roles   Active Directory Certificate Services   Image: Active Directory Certificate Services   Image: DVS Server   Image: DVS
Image:
Server Manager (PUSTYUGO-DC-1) Roles Active Directory Certificate Services Active Directory Domain Services OHCP Server DNS Server DNS Server DNS Server DNS VUGO-DC-1 DNS VUGO-DC-1 Disconse as parent folder) Host (A) Host (B) <
Image: Conditional Forwarders   Image: Web Server (IIS)   Image: Features   Image: Diagnostics   Image: Configuration   Image: Configuration   Image: Storage

Étape 2. Ajouter un enregistrement **hôte (A)** pour le nom de domaine complet du RPC (**cpp.example.com** utilisé dans cet exemple) pointant vers **l'adresse IP de PSN** :

🚆 Server Manager				
File Action View Help				
🗢 🔿 🖄 📷 🗙 🖼 🗟 🔽 📷 🗄 🗊				
Server Manager (PUSTYUGO-DC-1)	example.com 6 record(s)			
Roles  Active Directory Certificate Services  Active Directory Domain Services  DHCP Server  DNS DNS DNS DNS DNS DNS DNS DNS DNS DN	Name     (same as parent folder)       (same as parent folder)     (same as parent folder)       (flex/pn-hub)     (pp       pustyugo-ise23-1     pustyugo-ise23-2	Type Start of Authority (SOA) Name Server (NS) Host (A) Host (A) Host (A) Host (A)	Data [13], pustyugo- pustyugo-dc-1 10.48.30.127 10.48.71.183 10.48.30.127 10.48.30.128	Cpp Properties       ? ×         Host (A)       Security         Host (uses parent domain if left blank):
<ul> <li> <b>∂</b> Features          </li> <li> <b>∂</b> Diagnostics      </li> <li> <b>∂</b> Diagnostics         </li> <li> <b>∂</b> Storage      </li> </ul>				OK Cancel Apply

### Configuration initiale IOS XE

#### Configurer le certificat d'identité

Le routeur utilise le certificat afin de s'authentifier auprès du client Anyconnect. Le certificat du routeur doit être approuvé par le système d'exploitation de l'utilisateur afin d'éviter les avertissements de certificat pendant la phase d'établissement de la connexion.

Le certificat d'identité peut être fourni de l'une des manières suivantes :

Note: L'utilisation de certificats auto-signés n'est pas prise en charge avec IKEv2 FlexVPN.

#### Option 1 : configuration du serveur d'autorité de certification sur le routeur

**Note**: Il est possible de créer un serveur AC sur le même routeur IOS ou un autre routeur. Dans cet article, l'autorité de certification est créée sur le même routeur.

Note: Vous devez synchroniser l'heure sur le serveur NTP avant d'activer le serveur AC.

**Note**: Veuillez noter que l'utilisateur ne pourra pas vérifier l'authenticité de ce certificat, de sorte que les données utilisateur ne seront pas protégées contre les attaques man-in-the-Middle, à moins que le certificat CA ne soit vérifié manuellement et importé dans la machine de l'utilisateur avant d'établir la connexion.

Étape 1. Générer des clés RSA pour le serveur AC :

FlexVPN-HUB(config)# crypto key generate rsa label ROOT-CA modulus 2048 Étape 2. Générer des clés RSA pour le certificat d'identité :

<code>FlexVPN-HUB(config)# crypto key generate rsa label FLEX-1 modulus 2048 Vérification :</code>

---- 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

#### Étape 3. Configurez l'autorité de certification :

FlexVPN-HUB# show crypto key mypubkey rsa

```
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
Vérification :
```

```
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
Étape 4. Configurez le point de confiance :
```

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

#### Étape 5. Authentifier l'autorité de certification :

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.

#### Étape 6. Inscrivez le routeur à 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 Vérifiez les demandes de certificat en attente sur l'autorité de certification et vérifiez que l'empreinte correspond : FlexVPN-HUB#show crypto pki server ROOT-CA requests Enrollment Request Database: Subordinate CA certificate requests: RegID State Fingerprint SubjectName \_\_\_\_\_

RA certificate requests: ReqID State Fingerprint SubjectName

Router	certificate	es requests:	
ReqID	State	Fingerprint	SubjectName
1			l.
1	penaing	80B1FAFD35346D0FD23F6648F83F039B	cn=iiexvpn-nub.exampie.com

Étape 7. Accorder le certificat à l'aide de l'ID de demande approprié :

FlexVPN-HUB#crypto pki server ROOT-CA grant 1 Attendez que le routeur demande à nouveau le certificat (selon cette configuration, il vérifie 10 fois par minute). Rechercher le message syslog :

May 21 16:18:56.375: %PKI-6-CERTRET: Certificate received from Certificate Authority Vérifiez que le certificat est installé :

```
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
```

#### Option 2 - Importer un certificat signé en externe

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)#

#### **Configurer IKEv2**

Étape 1. Configurer le serveur RADIUS et la 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

Étape 2. Configurez les listes d'authentification et d'autorisation :

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 Étape 3. Créer une stratégie d'autorisation 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
Étape 4. Créer un profil 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
```

#### Étape 5. Créer un jeu de transformation et un profil 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 Étano 6. Créar una interface de modèle virtuel

#### Étape 6. Créer une interface de modèle virtuel :

```
interface Virtual-Template10 type tunnel
ip unnumbered GigabitEthernet3
tunnel mode ipsec ipv4
tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
Étape 7. Créer un pool local:
```

ip local pool FlexVPN-Pool-1 10.20.30.100 10.20.30.200

Étape 8. Créer une liste de contrôle d'accès pour restreindre l'accès aux clients non conformes. Pendant l'état de position inconnu, au moins ces autorisations doivent être fournies :

- Trafic DNS
- Trafic vers les PSN ISE via les ports 80, 443 et 8905
- Trafic vers les PSN ISE vers lesquels le FQDN du portail CPP pointe
- Trafic vers les serveurs de correction si nécessaire

Ceci est un exemple de liste de contrôle d'accès sans serveurs de correction, deny explicite pour le réseau 10.0.0.0/24 est ajouté pour la visibilité, deny ip any any implicite existe à la fin de la liste de contrôle d'accès :

```
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 10.48.30.128 eq 800
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 8443
permit tcp any host 10.48.30.128 eq 8905
deny ip any 10.0.0.0 0.0.255
```

Étape 9. Créer une liste de contrôle d'accès pour autoriser l'accès aux clients conformes :

ip access-list extended PERMIT\_ALL
 permit ip any any
Étape 10. Configuration du tunnel partagé (facultatif)

Par défaut, tout le trafic sera dirigé sur VPN. Afin de tunnaliser le trafic uniquement vers les réseaux spécifiés, vous pouvez les spécifier dans la section Stratégie d'autorisation ikev2. Il est possible d'ajouter plusieurs instructions ou d'utiliser une liste de contrôle d'accès standard.

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

Étape 11. Accès Internet pour les clients distants (facultatif)

Afin que les connexions sortantes des clients d'accès distant aux hôtes d'Internet soient définies par NAT à l'adresse IP globale du routeur, configurez la traduction 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

### Configuration du profil client Anyconnect

Configurez le profil client à l'aide de l'éditeur de profil AnyConnect. Les profils d'Anyconnect Security Mobile Client sous Windows 7 et Windows 10 sont enregistrés dans **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile**.

Étape 1. Désactivez la fonction Captive Portal Detection. Si le serveur http n'est pas désactivé sur le concentrateur FlexVPN, la fonctionnalité de détection de portail captif AnyConnect entraînera l'échec de la connexion. Veuillez noter que le serveur AC ne fonctionnera pas sans serveur HTTP.

🔈 AnyConnect Profile Editor -	VPN								
File Help									
VPN VPN Preferences (Part 1) Preferences (Part 2)	Preferences (Part 1) Profile:\Cisco AnyConnect Secure Mobility Client\Profile\FLEXVPN.xml								
Backup Servers Certificate Pinning Certificate Matching Certificate Enrollment Mobile Policy Server List	<ul> <li>Use Start Before Logon</li> <li>Show Pre-Connect Message</li> <li>Certificate Store</li> <li>Windows</li> <li>All</li> <li>macOS</li> <li>All</li> <li>Certificate Store Override</li> <li>Auto Connect On Start</li> <li>Minimize On Connect</li> <li>Local Lan Access</li> </ul>	<ul> <li>✓ User Controllable</li> </ul>							
	<ul> <li>Disable Captive Portal Detection</li> <li>Auto Reconnect</li> </ul>	User Controllable							
	Auto Reconnect Behavior ReconnectAfterResume	User Controllable							

Étape 2. Configurer la liste des serveurs :

AnyConnect Profile Editor File Help	r - VPN	
VPN	, Server List Profile:\Cisco AnyConnect Secure Mobility Client\Profile\FLEXVPN.xml	
Vereficences (Part 2) Preferences (Part 2) Backup Servers Certificate Pinning Certificate Enrollment Mobile Policy Server List	Profile:\Cisco AnyConnect Secure Mobility Client\Profile\FLEXVPN.xml  Server List Entry Server Load Balancing Servers SCEP Mobile Certificate Pinning  Primary Server  a. Display Name (required) FLEXVPN  FQDN or IP Address User Group b. FQDN or IP Address User Group  KE Identity (IOS gateway only) EAP-MDS  KE Identity (IOS gateway only) EXample.com  Backup Servers Host Address Add Move Up Move Down Delete	<b>d</b> .
	OK Cancel	

- Saisissez Display Name.
- Entrez FQDN ou adresse IP du concentrateur FlexVPN.
- Sélectionnez IPsec comme protocole principal.
- Décochez la case « passerelle ASA » et spécifiez EAP-MD5 comme méthode d'authentification. Entrez l'identité IKE exactement comme dans la configuration du profil IKEv2 sur le concentrateur FlexVPN (dans cet exemple, le profil IKEv2 est configuré avec la commande « match identity remote key-id example.com », nous devons donc utiliser example.com comme identité IKE).

Étape 3. Enregistrez le profil dans **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile** et redémarrez l'AC.

Équivalent XML du profil :

```
<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">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>
```

### **Configuration ISE**

Configuration des certificats Admin et CPP

**Note**: La modification du certificat Admin redémarre le noeud sur lequel le certificat a été modifié.

Étape 1. Accédez à Administration -> Système -> Certificats -> Demandes de signature de certificat, cliquez sur Générer des demandes de signature de certificat (CSR) :

dentity Services Engine	Home   Context Visibility	Operations     Policy	✓Administration	Work Centers							
▼System → Identity Management → Network Resources → Device Portal Management pxGrid Services → Feed Service → Threat Centric NAC											
Deployment Licensing -Certificates + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings											
G											
▼ Certificate Management	Certificate Signing Requ	uests									
System Certificates	S Generate Certificate Signing Requests (CSR)										
Trusted Certificates	A Certificate Signing Requests	s (CSRs) must be sent to and s	signed by an external authority	y. Click "export" to downloa	ad one or more CSR	s so that they may be					
OCSP Client Profile	bind to bind the request to th	le signed certificate issued by t	nat autionty. Once a CSR is i	bound, it will be removed in	rom this list.						
Certificate Signing Requests	🔎 View 🚯 Export 🗙 De	lete Bind Certificate									
Certificate Periodic Check Setti	Friendly Name		Certificate Subject	Key Length	Portal group tag	Timestamp					
Certificate Authority				No data	available						

Étape 2. Sur la page ouverte, sélectionnez le noeud PSN nécessaire, renseignez les champs nécessaires et ajoutez le nom de domaine complet du noeud, enroll.cisco.com, cpp.example.com et l'adresse IP du noeud dans les champs SAN, puis cliquez sur **Generate** :

dentity Services Engine	Home → Context Visibility → Operations → Policy
▼System ► Identity Management	Network Resources
Deployment Licensing	s + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings
0	Usage
▼ Certificate Management	Certificate(s) will be used for Multi-Use
System Certificates	doing so is not a recommended practice. Kather, you should obtain individual certificates specifically for each
Trusted Certificates	Service (for example, one certificate each for Guest Portals, EAP, and pxGrid).
OCSP Client Profile	Allow Wildcard Certificates
Certificate Signing Requests	Node(s)
Certificate Periodic Check Setti	Generate CSR's for these Nodes:
Certificate Authority	Node CSR Friendly Name
	✓ pustyugo-ise23-1 pustyugo-ise23-1#Multi-Use
	pustyugo-ise23-2 pustyugo-ise23-2#Multi-Use
	Subject
	Organizational Unit (OU) TAC
	City (L)
	State (ST)
	Country (C)

Subject Alternative Name (SAN)	DNS Name	pustyugo-ise23-1.example.co	m —	÷	
	DNS Name	enroll.cisco.com	_	+	
	DNS Name	cpp.example.com		+	
	IP Address 🔹	10.48.30.127			i
* Key type	RSA 💌 🛈				
* Key Length	2048				
* Digest to Sign With	SHA-256				
Certificate Policies					
	Generate Cancel				

**Note**: Si vous sélectionnez **Multi-Use** à cette étape, vous pouvez également utiliser le même certificat pour Portal.

Dans la fenêtre apparue, cliquez sur **Exporter** pour enregistrer le CSR au format pem sur la station de travail locale :

Successfully generated CSR(s)

Certificate Signing request(s) generated:

pustyugo-ise23-1#Multi-Use

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



х

Étape 3. Envoyez une requête au CSR avec une autorité de certification de confiance et obtenez le fichier de certificat de l'autorité de certification ainsi que la chaîne complète des certificats de l'autorité de certification (racine et intermédiaire).

Étape 4. Accédez à Administration -> Système -> Certificats -> Certificats approuvés, cliquez sur Importer. Dans l'écran suivant, cliquez sur Choisir un fichier et sélectionnez le fichier de certificat d'autorité de certification racine, indiquez le nom convivial et la description si nécessaire, sélectionnez les options Fiable pour nécessaire et cliquez sur Envoyer :



Répétez cette étape pour tous les certificats intermédiaires de la chaîne s'il y en a.

Étape 5. Revenir à Administration -> Système -> Certificats -> Demandes de signature de certificat, sélectionnez le CSR nécessaire et cliquez sur Lier le certificat :



Étape 6. Sur la page ouverte, cliquez sur **Choisir un fichier**, sélectionnez le fichier de certificat reçu de l'Autorité de certification, puis entrez Nom convivial si nécessaire, puis sélectionnez **Utilisation : Admin (Utilisation : Portal** peut également être sélectionné ici si le CSR a été créé avec **Multi-Use**) et cliquez sur **Submit** :

dentity Services Engine	Home	ons  ▶ Policy						
▼System ► Identity Management	Network Resources     Device Portal Mar	agement pxGrid Services + Feed Service + Threat Cent	tric NAC					
Deployment Licensing - Certificate	es ►Logging ►Maintenance Upgrad	Backup & Restore     Admin Access     Settings						
✓ Certificate Management	Bind CA Signed Certificate							
System Certificates	* Certificate File Ch	ose File Signed CSR.cer						
Trusted Certificates OCSP Client Profile	Friendly Name pus	yugo-ise23-1 Admin						
Certificate Signing Requests	Validate Certificate Extensions							
Certificate Authority	Usage							
	$\checkmark$	dmin: Use certificate to authenticate the ISE Admin Portal						
		AP Authentication: Use certificate for EAP protocols that use SSI	L/TLS tunneling					
		ADIUS DTLS: Use certificate for the RADSec server						
		xGrid: Use certificate for the pxGrid Controller						
		ortal: Use for portal						
	S	mit Cancel						

Étape 7. Dans la fenêtre contextuelle d'avertissement, cliquez sur **Oui** pour terminer l'importation. Le noeud affecté par la modification du certificat Admin va être redémarré :

vice P	ortol Ma	anagement puCrid Convises + Food Convises + Threat Contria NAC	
ince		Enabling Admin role for this certificate will cause an application server restart on the selected node.	
icat		Note: Make sure required Certificate Chain is imported under Trusted Certificates	
icate	_	No Yes	

Répétez les étapes de modification du certificat CPP si vous avez décidé d'utiliser un certificat distinct pour le portail. À l'étape 6, sélectionnez **Utilisation : Portail** et cliquez sur **Envoyer :** 



Répétez les étapes pour tous les PSN dans le déploiement ISE.

#### Créer un utilisateur local sur ISE

Note: Avec la méthode EAP-MD5, seuls les utilisateurs locaux sont pris en charge par ISE.

Étape 1. Accédez à Administration -> Gestion des identités -> Identités -> Utilisateurs, cliquez sur Ajouter.

cisco Identity Services Engine	Home + Cont	ext Visibility 🔹 🕨 Op	perations	► Policy -	Administrati	on 🔹 Work C	enters			
► System - Identity Management	Network Resources	Device Portal N	lanagement	pxGrid Service	es 🔸 Feed	Service + Thi	eat Centric NAC			
	y Sources Identity	Source Sequences	<ul> <li>Settings</li> </ul>							
0										
Users	Network Acces	ss Users								
Latest Manual Network Scan Results	/ Edit 🕂 Add	🔀 Change Status	De Import	t 🚯 Export 👻	XDelete	Duplicate				
	Status	Name		Description		First Name	Last Name	Email Address	User Identity Groups	Admin
									No data available	

Étape 2. Sur la page ouverte, saisissez le nom d'utilisateur, le mot de passe et d'autres informations nécessaires, puis cliquez sur **Soumettre**.

cisco	Identi	y Servi	ces E	ngine	Н	ome	<ul> <li>Conte</li> </ul>	ext Visibi	ility	<ul> <li>Operations</li> </ul>	Policy	<b>→</b> Ad	ministration	→ W	Vork Centers
<ul> <li>Syst</li> </ul>	em 🗖	- Identity	Mana	gement	► Ne	twork Re	esources	► De	evice Por	tal Managemen	t pxGrid	Services	Feed Ser	vice	Threat Centric NAC
✓Iden	tities	Groups	Ex	ernal Ide	ntity So	urces	Identity	Source	Sequenc	es • Setting	s				
					9										
Users					N	Jetwork A	work Ac	sers List	t > New	Network Acces	s User				
Latest M	lanual N	letwork S	can F	esults		· neu			/361						
						* Nam	e vpnu	iser							
						Statu	s 🔽	Enabled	d 👻						
						Ema	il 📃								
						▼ Pas	swords	;							
						Pass	word Typ	e:	Internal U	Jsers	-				
								Pa	assword			Re-Enter	Password		
						* Log	in Passv	vord 💽	••••			•••••			Generate Password (i)
						Enab	le Passv	vord							Generate Password (i)
						▼ Use	er Infor	matior	n						
						First	Name								
						Last	Name [								
						▼ Acc	ount O	ptions							
								C	Descriptio	in					1
						Char	nde passi	word on	next loai	in 🗆					
						▼ Acc	ount D	isable	Policy						
							Disable a	account	if date ex	ceeds 2018-	07-27		(уууу	/-mm-d	id)
						▼ Use	er Grou	ps							
						ALL	_ACCOU	NTS (de	fault)	<b>o</b> —	÷				
						Submit	Car	ncel							

#### Ajouter le concentrateur FlexVPN en tant que client Radius

Étape 1. Accédez à Centres de travail -> Posture -> Périphériques réseau, cliquez sur Ajouter.

cisco Identity S	Services Engine	Home	Context Visibility	<ul> <li>Operations</li> </ul>	▶ Policy	► Administration	✓ Work Centers	
Network Access	s 🔸 Guest Access	TrustSec	BYOD     Profile	✓ Posture	Device Admin	nistration + Pas	ssiveID	
Overview Netv	vork Devices + Clie	ent Provisioning	<ul> <li>Policy Elements</li> </ul>	Posture Policy	Policy Sets	Troubleshoot	Reports + Settings	
Network Devi	ces							
🥖 Edit 🛛 🕂 Add	Duplicate 👔	import 🛛 🔂 Exp	ort 🕑 Generate PA	AC 🗙 Delete				
Name	▲ IP/Mask	Profile Name	9	Location		Туре		Description
								No data available

Ster 2. Sur la page ouverte, entrez Device Name (Nom du périphérique), IP address (Adresse IP) et autres informations nécessaires, cochez la case RADIUS Authentication settings (Paramètres d'authentification RADIUS), saisissez Shared Secret (Secret partagé) et cliquez sur **Submit** en bas de la page.

uluilu cisco	Identity Services Engine	Home ► Context Vis	ibility 🕨 K	Operations	▶ Policy	Administration	✓ Work Centers	
Net	work Access	TrustSec     BYOD	Profiler	▼ Posture	Device Admi	nistration Pa	ssiveID	
Overv	iew Network Devices + Clie	ent Provisioning	lements Po	osture Policy	Policy Sets	Troubleshoot	Reports Setting	s
Networ	k Devices List > New Network D ork Devices	* Name FlexVPN-HUB Description FlexVPN HUB						
11								
	IP Address ▼ * IP : 1	0.48.71.183		/ 32				
<b>O</b> IP	v6 is supported only for TACACS, * Dev	At least one IPv4 must be de ice Profile 🗰 Cisco 💌 🕀	fined when R	ADIUS is selec	ted			
	Ма	odel Name	-					
	Softwa	re Version	•					
*	Network Device Group							
	Location All Locations	Set To Default						
	IPSEC Is IPSEC Device	Set To Default						
D	evice Type All Device Types	Set To Default						
•	→ RADIUS Authentication Setting	JS						
	RADIUS UDP Settings							
		Protocol	RADIUS					
		- Snared Secret	•••••		Show			
		ose second snared secret			Show			
		CoA Port	1700		Set T	o Default		
	RADIUS DTLS Settings (i)							
		DTLS Required	(i)					
		Shared Secret	radius/dtls		(j)			
		CoA Port	2083		Set T	o Default		
	Issuer C	JA OF ISE Certificates for CoA	Select if rec	quired (optiona	al)	• (i)		
		Dino iname						
	General Settings							
		Enable KeyWrap	<b>i</b>					
	* ****	* Key Encryption Key			Show			
	^ Mes	Key Input Format			Show			
_		ivey input i onliat						
	TACACS Authentication Setting	gs						
	<ul> <li>SNMP Settings</li> </ul>							
	<ul> <li>Advanced TrustSec Settings</li> </ul>							
Cubr	vit Cancol							

#### Configuration de l'approvisionnement client

Voici les étapes à suivre pour préparer la configuration d'Anyconnect.

Étape 1. Téléchargement du package Anyconnect. Le package Anyconnect lui-même n'est pas disponible en téléchargement direct depuis ISE. Avant de commencer, assurez-vous qu'AC est disponible sur votre ordinateur. Ce lien peut être utilisé pour le téléchargement AC - <u>http://cisco.com/go/anyconnect</u>. Dans ce document, le package anyconnect-win-4.5.05030-webdéploiement-k9.pkg est utilisé.

Étape 2. Afin de télécharger le package AC vers ISE, accédez à Work Centers -> Posture -> Client Provisioning -> Resourceset cliquez sur Add. Choisissez les ressources de l'agent sur le disque local. Dans la nouvelle fenêtre, choisissez Cisco Provided Packages, cliquez sur Choose File et sélectionnez AC package sur votre ordinateur.

dentity Services Engine	Home		nistration - Work Centers		
Network Access     Guest Access	TrustSec     BYOD     Profiler	r  Posture  Device Administration	n   PassiveID		
Overview Network Devices - Clie	nt Provisioning	Posture Policy Policy Sets Troub	leshoot Reports + Settings	3	
Client Provisioning Policy Resources Client Provisioning Portal	Agent Resources From Local Disk Agent Resources From Loc Category	Cisco Provided Packages           Choose File         anyconnect ploy-k9.	v (j) pkg		
	_	AnyConnect Uploaded Resource	5		
		Name 🔺	Туре	Version	Description
		AnyConnectDesktopWindows 4.5.503	AnyConnectDesktopWindows	4.5.5030.0	AnyConnect Secure Mobility Clien
	Submit Cancel				

Cliquez sur **Soumettre** pour terminer l'importation. Vérifiez le hachage du package et appuyez sur **Confirmer**.

Étape 3. Le module de conformité doit être téléchargé vers ISE. Sur la même page (**Centres de travail -> Posture -> Approvisionnement du client -> Ressources**), cliquez sur **Ajouter** et choisissez **des ressources d'agent sur le site Cisco**. Dans la liste des ressources, vérifiez un module de conformité et cliquez sur **Enregistrer**. Pour ce document Module de conformité AnyConnectComplianceWindows 4.3.50.0 est utilisé.

Dov	vnload Remote Resources	:	×
	Name 🔺	Description	
	AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization Package v1.1.1.6 for Wir	h.
	AnyConnectComplianceModuleOSX 3.6.11682.2	AnyConnect OS X Compliance Module 3.6.11682.2	
	AnyConnectComplianceModuleOSX 4.3.29.0	AnyConnect OSX Compliance Module 4.3.29.0	
	AnyConnectComplianceModuleWindows 3.6.11682.2	AnyConnect Windows Compliance Module 3.6.11682.2	
✓	AnyConnectComplianceModuleWindows 4.3.50.0	AnyConnect Windows Compliance Module 4.3.50.0	
	CiscoTemporalAgentOSX 4.5.02036	Cisco Temporal Agent for OSX With CM: 4.2.1019.0 Works wi	
	CiscoTemporalAgentWindows 4.5.02036	Cisco Temporal Agent for Windows With CM: 4.2.1226.0 Work	
	ComplianceModule 3.6.11510.2	NACAgent ComplianceModule v3.6.11510.2 for Windows	
	MACComplianceModule 3.6.11510.2	MACAgent ComplianceModule v3.6.11510.2 for MAC OSX	
	MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9.4.3 - ISE 1.2 , ISE 1.1.	
	MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9.5.3 - ISE 1.2 Patch 12,	
	MacOsXSPWizard 1.0.0.18	Supplicant Provisioning Wizard for Mac OsX 1.0.0.18 (ISE 1.1	
	MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for Mac OsX 1.0.0.21 (for ISE	
	MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for Mac OsX 1.0.0.27 (for ISE	
	MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for Mac OsX 1.0.0.29 (for ISE	
	MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for Mac OsX 1.0.0.30 (for ISE	
		▶	
For	AnyConnect software, please download from http://cisco.com/go/anyc	onnect. Use the "Agent resource from local disk" add option,	

to import into ISE

٢

Save Cancel

Étape 4. Il faut maintenant créer un profil de position CA. Cliquez sur **Ajouter** et choisissez **Agent NAC ou Profil de posture Anyconnect**.

dentity Services Engine	Home	Operations     Policy	Administration	✓ Work Centers
Network Access     Guest Access	TrustSec     BYOD     Profiler	▼ Posture	nistration   Passi	iveID
Overview Network Devices - Clier	t Provisioning  Policy Elements	Posture Policy Policy Sets	Troubleshoot F	Reports > Settings
Client Provisioning Policy	ISE Posture Agent Profile Settings	> New Profile		
Resources	Posture Agent Profile Settings			
Client Provisioning Portal	a. AnyConnect   AnyConnect  AC-4.5-Posture  Description:			
	Agent Behavior			

- Sélectionnez le type du profil. AnyConnect doit être utilisé pour ce scénario.
- Spécifiez le nom du profil. Accédez à la section Protocole de posture du profil

**Posture Protocol** 

н

Parameter	Value	Notes
PRA retransmission time	120 secs	
Discovery host		
* Server name rules	* <u>a.</u>	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>b</b> .	List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.

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

Submit	Cancel				

- Spécifiez les règles de nom de serveur, ce champ ne peut pas être vide. Le champ peut contenir un nom de domaine complet avec un caractère générique qui limite la connexion du module de posture CA aux PSN à partir de l'espace de noms approprié. Mettez en étoile si un nom de domaine complet doit être autorisé.
- Les noms et les adresses IP spécifiés ici sont utilisés au cours de l'étape 2 de la détection de position (voir l'étape 14 de la section "<u>Flux de position dans ISE 2.2</u>"). Vous pouvez séparer les noms par coma, ainsi que le numéro de port peut être ajouté après FQDN/IP à l'aide de deux points.

Étape 5.Créez une configuration CA. Accédez à Work Centers -> Posture -> Client Provisioning -> Resources et cliquez sur Add, puis sélectionnez AnyConnect Configuration.



- Sélectionnez un package CA.
- Indiquez le nom de configuration CA.
- Sélectionnez la version du module de conformité.
- Sélectionnez Profil de configuration de position CA dans la liste déroulante.

Étape 6. Configurez la stratégie d'approvisionnement du client. Accédez à **Centres de travail -> Posture -> Provisionnement client**. En cas de configuration initiale, vous pouvez remplir des valeurs vides dans la stratégie présentée avec les valeurs par défaut. Pour ajouter une stratégie à la configuration de position existante, accédez à la stratégie qui peut être réutilisée et choisissez **Dupliquer au-dessus** ou **Dupliquer au-dessous**. Il est également possible de créer de nouvelles politiques.

Voici l'exemple de la stratégie utilisée dans le document.

cisco Identity Services Engine	Home + Context Visibility + Operations + Policy + Administration + Wiork Centers	License Warning 🔺	Q,	0
Network Access     Guest Access	TrustSec + BYOD + Profiler + Posture + Device Administration + PassiveID			
Overview Network Devices - Clie	t Provisioning + Policy Elements Posture Policy Policy Sets Troubleshoot Reports + Settings			
0				
Client Provisioning Policy	Client Provisioning Policy			
Resources	Define the Citent Provisioning Prolicy to determine what users will receive upon login and user ession initiation: For Apert Configuration, version of apent, apent profile, apent compliance module, and/or spent cutomization package.			
Client Provisioning Portal	For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.			
	Rufe Name Identify Groups Operating Systems Other Conditions Results			
	🖉 🖌 Windows 🕺 🖞 Any 🔷 and Windows All 🔶 and Condition(s) 🔷 then AnyConnect 🗢			_
	Agent Configuration		4	•
	Agent: Any.Connect Configuration 📀			11
	Native Supplicant Configuration		_	
	Conference Compared Conference			
	Vitaad Profile (Choose a Vitaad Profile O		- 1	11
			- N	1

Choisissez votre configuration CA dans la section des résultats.

#### Politiques et conditions de posture

Un simple contrôle de posture est utilisé. ISE est configuré pour vérifier l'existence du fichier C:\TEST.txt côté périphérique final. Les scénarios réels peuvent être beaucoup plus compliqués, mais les étapes générales de configuration sont les mêmes.

Étape 1. Créer une condition de posture. Les conditions de posture se trouvent dans **Centres de travail -> Posture -> Éléments de politique -> Conditions**. Choisissez le type de condition de posture et cliquez sur **Ajouter**. Spécifiez les informations nécessaires et cliquez sur **Enregistrer**. Vous trouverez ci-dessous un exemple de condition de service qui doit vérifier si le fichier C:\TEST.txt existe.

cisco Identity Services Engine	Home → Context V	isibility	Policy ► Admi	nistration	- Worł	Centers
Network Access     Guest Acces	ss + TrustSec + BYOD	► Profiler ▼Posture	Device Administration	n 🕨 Pas	siveID	
Overview Network Devices	Client Provisioning - Policy	Elements Posture Policy	Policy Sets Troub	leshoot	Reports	Settings
<ul> <li>Conditions</li> <li>Hardware Attributes Condition</li> <li>Application</li> <li>Firewall Condition</li> <li>Anti-Malware</li> <li>Anti-Spyware</li> <li>Anti-Virus</li> <li>Compound</li> <li>Dictionary Simple</li> <li>Dictionary Compound</li> </ul>	File Conditions List > T File Condition * Name Description * Operating System Compliance Module * File Type * File Path * File Operator Save Reset	TEST_txt TEST_txt Windows All Any version FileExistence ABSOLUTE_PATH Exists	▼ (i) ▼ C:\TES <sup>*</sup>	T.txt		(j
Disk Encryption						
File						
Patch Management						
Registry						
Service						
USB						

Étape 2.Configuration des exigences Accédez à **Centres de travail -> Posture -> Eléments de politique -> Exigences**. Voici un exemple pour le fichier TEST.txt Existance :

File Existance for Windows All $\diamondsuit$ using Lix or inter vusing AnyConnect v met if TEST_bt $\diamondsuit$ then	Message Done
Note: Supported Remediation Actions are filtered based on the Operating Systems and Stealth Mode selections. Remediation Actions are not applicable for Hardware Conditions and Application Conditions configured using the Provision By Category or Provision By Everything options.	Action Message Text Only O Message Shown to Agent User Create TEST.btt file on disk C:
Save	٠

Choisissez votre condition de posture dans une nouvelle exigence et spécifiez une action de correction.

Étape 3. Configuration de la stratégie de positionnement. Accédez à **Centres de travail -> Posture** -> **Posture Policy**. Vous trouverez ci-dessous un exemple de stratégie utilisée pour ce document. L'exigence relative à l'« Existance des fichiers » est assignée comme obligatoire et aucune autre condition n'est assignée.

titudentity Services Engine Home   Context Visibility	Policy      Administration     ✓We	rk Centers	
► Network Access ► Guest Access ► TrustSec ► BYOD ► P	ofiler   Posture   Device Administration   PassiveID		
Overview Network Devices	Posture Policy Policy Sets Troubleshoot Reports	<ul> <li>Settings</li> </ul>	
Desture Dellar			
Posture Policy			
Define the Posture Policy by configuring rules based on operating system a	nd/or other conditions.		
<b>*</b>			
Status Rule Name Identity Groups	Operating Systems Compliance Module	Posture Type Other Conditions	Requirements
File Policy If Any	and Windows All 💠 and 4.x or later	▼ and AnyConnect ▼ and (Optional) Dictionar ♦	then File Existance 💠

#### Configurer le portail d'approvisionnement du client

Pour une posture sans redirection, la configuration du portail d'approvisionnement client doit être modifiée. Accédez à **Work Centers -> Posture -> Client Provisioning -> Client Provisioning Portal** Vous pouvez utiliser le portail par défaut ou créer le vôtre.



Ces paramètres doivent être modifiés dans la configuration du portail pour le scénario de non-

redirection :

- Dans Authentication, spécifiez Identity Source Sequence qui doit être utilisé si SSO ne parvient pas à localiser la session pour l'utilisateur.
- En fonction de la séquence de source d'identité sélectionnée, la liste des groupes disponibles est renseignée. À ce stade, vous devez sélectionner les groupes autorisés pour la connexion au portail.
- Le nom de domaine complet du portail d'approvisionnement du client doit être spécifié. Ce nom de domaine complet doit pouvoir être résolu sur les adresses IP PSN ISE. Les utilisateurs doivent être invités à spécifier le nom de domaine complet dans le navigateur Web lors de la première tentative de connexion.

#### Configurer les profils et les stratégies d'autorisation

L'accès initial du client lorsque l'état de la position n'est pas disponible doit être restreint. Cela pourrait se faire de plusieurs façons :

- Radius Filter-Id avec cet attribut, la liste de contrôle d'accès définie localement sur NAD peut être attribuée à l'utilisateur avec un état de posture inconnu. Comme il s'agit d'un attribut RFC standard, cette approche devrait fonctionner correctement pour tous les fournisseurs NAD.
- Cisco:cisco-av-pair = ip:interface-config très similaire à Radius Filter-Id, la liste de contrôle d'accès définie localement sur NAD peut être attribuée à l'utilisateur avec un état de position inconnu. Exemple de configuration :

cisco-av-pair = ip:interface-config=ip access-group DENY\_SERVER in

Étape 1. Configurez le profil d'autorisation.

Comme d'habitude pour la posture, deux profils d'autorisation sont requis. La première doit contenir toutes sortes de restrictions d'accès au réseau. Ce profil peut être appliqué aux authentifications pour lesquelles l'état de la posture n'est pas égal à conforme. Le second profil d'autorisation peut contenir uniquement des accès autorisés et peut être appliqué pour une session avec un état de posture égal à conforme.

Pour créer un profil d'autorisation, accédez à Centres de travail -> Posture -> Éléments de stratégie -> Profils d'autorisation.

Exemple de profil d'accès restreint avec l'ID de filtre Radius :

cisco Identity Services Engine	Home	Operations     Policy     Adr	ninistration Vork Centers
Network Access     Guest Access	TrustSec     BYOD     Profile	r Posture Device Administrati	on   PassiveID
Overview Network Devices + Clier	nt Provisioning   Policy Elements	Posture Policy Policy Sets Trou	ubleshoot Reports + Settings
0			
	Authorization Profiles > LIMITED	_ACCESS	
Hardware Attributes Condition	* Name LIM	ITED ACCESS	
Application	Description		
Firewall Condition	* Access Type	ESS ACCEDT	
Anti-Malware	ACC	ESS_ACCEPT	
Anti-Spyware	Network Device Profile	Cisco 👻 🕀	
Anti-Virus	Service Template		
Compound	Track Movement	)	
Dictionary Simple	Passive Identity Tracking		
Dictionary Compound			
Disk Encryption			
File	- Common Tasks		
Patch Management			
Registry	DACL Name		
Service			
USB	ACL (Filter-ID)	DENY_SERVER	.in
Remediations	_		
Requirements	Security Group		
Allowed Protocols			
Authorization Profiles	U VEAN		
Downloadable ACLs			
	- Advanced Attributes Se	ttings	
	Auvaliceu Attributes Se	tungs	
	Select an item	○ =	○ - +
	▼ Attributes Details		
	Access Type = ACCESS_ACCEP	т	
	Filter-ID = DENY_SERVER.in		

Exemple de profil d'accès restreint avec cisco-av-pair :

alialia cisco	Identi	ity Ser	vices Eng	jine	Home	Context Visibili	ty i	<ul> <li>Operations</li> </ul>	Policy	Administration	<b>-</b> Wor	k Centers		
Net	work Ac	cess	Guest A	Access	TrustSec	+ BYOD + F	Profiler	✓ Posture	Device Admi	nistration + Pa	ssiveID			
Overv	view N	Network	Devices	Clie	nt Provisioning	- Policy Elem	nents	Posture Policy	Policy Sets	Troubleshoot	Reports	<ul> <li>Settings</li> </ul>	3	
				G										
- Cond	litions				Authorizati	on Profiles > LIM	ITED_A	CCESS						
Hard	lware At	tributes	Condition		Autionz	* Name	LIMIT	ED ACCESS						
Appl	ication					Description	[	LD_ACCE35						_
Firev	wall Con	dition				* Access Tupe								_//
Anti-	Malware	е				Access Type	ACCES	S_ACCEPT	Ŧ					
Anti-	Spywar	е			Network	Device Profile	ditte Cit	sco 💌 🕀						
Anti-	Virus				s	ervice Template								
Com	pound				1	Frack Movement								
Dicti	onary Si	imple			Passive I	dentity Tracking								
Dicti	onary C	ompour	nd		1 0001101	dentry meeting								
Disk	Encrypt	tion												
File						and the state								
Patc	h Manaş	gement			▼ Comr	non Tasks								
Regi	istry					L Name								
Serv	ice													
USB	1				AC	L (Filter-ID)								
Reme	diation	\$												
Require	ments				Sec	urity Group								
Allowed	Protoco	ols			_									
Authoriz	zation Pr	rofiles			U VLA	AN								
Downlo	adable /	ACLs												
					▼ Adva	nced Attribute	es Setti	ings						
						-1					1			
					II Cisco:	cisco-av-pair		= lip:in	iterrace-config=	ip access-g 🥹	]- +			
					▼ Attrib	outes Details								
					Access T	ype = ACCESS_4	ACCEPT							
					cisco-av-	-pair = ip:interfac	ce-config	g=ip access-gro	up DENY_SERVE	ER in				

Exemple de profil d'accès illimité avec l'ID de filtre Radius :

cisco 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 + Clier	nt Provisioning  Policy Elements Posture Policy Policy Sets Troubleshoot Reports  Settings								
0	* Name UNLIMITED_ACCESS								
- Conditions	Description								
Hardware Attributes Condition	* Access Type ACCESS_ACCEPT								
Application	Network Device Profile data Cisco 👻 🕀								
Firewall Condition									
Anti-Malware	Service Template								
Anti-Spyware	Track Movement 🔲 🥡								
Anti-Virus	Passive Identity Tracking 🔲 👔								
Compound									
Dictionary Simple									
Dictionary Compound	▼ Common Tasks								
Disk Encryption									
File	DACL Name								
Patch Management									
Registry	C ACL (Filter-ID)								
Service	Security Group								
USB									
Remediations	VLAN								
Paquiramente									
Allowed Protocols									
Authorization Profiles	✓ Advanced Attributes Settings								
Downloadable ACLs									
	Select an item 📀 = 💽 🗢 🕂								
	▼ Attributes Details								
	Access Type = ACCESS_ACCEPT								
	Filter-1D = PERMIT_ALL.IN								

Exemple de profil d'accès illimité avec cisco-av-pair :

cisco lo	dentity Services Eng	jine	Home	Context Visibility	Operations	▶ Policy	Administration	<b>→</b> Wor	k Centers		
Network	rk Access 🔹 🕨 Guest A	Access	TrustSec	BYOD     Profile	r <b>v</b> Posture	Device Adm	inistration + Pa	ssiveID			
Overview	V Network Devices	Clier	nt Provisioning		Posture Policy	Policy Sets	Troubleshoot	Reports	<ul> <li>Settings</li> </ul>		
		0		* Name UNI	IMITED_ACCESS	5					
- Conditio	ons			Description						/	
Hardwa	are Attributes Condition			* Access Type ACC	ESS_ACCEPT	*					
Applicat	tion		Network	Device Profile	Cisco 👻 🕀						
Firewall	I Condition										
Anti-Ma	alware		s	ervice Template							
Anti-Sp	yware		т	Frack Movement 🔲 🧃	)						
Anti-Vin	us		Passive I	dentity Tracking 🔲 🧃	)						
Compou	und										
Dictiona	ary Simple										
Dictiona	ary Compound		▼ Comr	non Tasks							
Disk En	ncryption		_								
File				CL Name							
Patch M	lanagement			(Filter ID)							
Registry	у		- AC	L (Filler-ID)							
Service			Sec	urity Group							
USB											
Remedia	ations			AN							
Requireme	ants										
Allowed Pr	rotocols										
Authorizatio	on Profiles		▼ Adva	nced Attributes Se	ttings						
Downloada	able ACLs										
			Cisco:	cisco-av-pair	💟 = ip:i	nterface-config=	ip access-g 📀	- +			
			▼ Attrib	outes Details							
			Access T	ype = ACCESS_ACCEP	T fig=ip_access-or		in				
			cisco-av-	pair - ipinterrace-cor	ing-ip accessign	Jup Perunt 1_ALL					

Étape 2. Configurez la stratégie d'autorisation. Au cours de cette étape, deux stratégies d'autorisation doivent être créées. L'une correspond à la demande d'authentification initiale avec l'état de posture inconnu et l'autre à l'attribution d'un accès complet après le processus de posture réussi.

Il s'agit d'un exemple de politiques d'autorisation simples pour ce cas :

✓ Auth	Authorization Policy (12)										
						Results					
٠	Status	Rule Name	Condit	ions		Profiles		Security Groups		Actions	
Search											
	Ø	Unknown_Compliance_Redirect	AND		Network_Access_Authentication_Passed	LIMITED ACCESS	+	Select from list		8	
					Compliance_Unknown_Devices					Ť	
	Ø	NonCompliant_Devices_Redirect	AND		Network_Access_Authentication_Passed	LIMITED ACCESS	*LIMITED ACCESS	Select from list	2		
					Non_Compliant_Devices	(			1	~	
	0	Compliant Davinas Arrass			Network_Access_Authentication_Passed	VUNUMITED ACCESS	+	Select from list	20		
		Completing Devices_Access	AND		Compliant_Devices	(Monchain reb_) (Goodoo)				~	

La configuration de la stratégie d'authentification ne fait pas partie de ce document, mais vous devez garder à l'esprit que l'authentification doit réussir avant le début du traitement de la stratégie d'autorisation.

## Vérification

La vérification de base du débit peut se faire en trois étapes principales :

Étape 1. Vérification de session VPN RA sur le concentrateur 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 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
       5.5.5.5/4500
                               7.7.7.7/60644
1
                                                    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 Étape 2. Vérification du flux d'authentification (journaux Radius Live)

1

	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		ò		Compliant	7.7.7.7			UNLIMITED_ACCESS	
2.	Jun 07, 2018 07:39:59.345 PM	0	ò	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	<b>~</b>	0	vpnuser	NotApplicable	7.7.7.7	Default >> Default	Default >> Unknown_Compliance	LIMITED_ACCESS	

- Authentification initiale. Pour cette étape, vous pouvez être intéressé par la validation du profil d'autorisation qui a été appliqué. Si un profil d'autorisation inattendu a été appliqué, examinez le rapport d'authentification détaillé. Vous pouvez ouvrir ce rapport en cliquant sur loupe dans la colonne Détails. Vous pouvez comparer des attributs dans un rapport d'authentification détaillé avec une condition dans la stratégie d'autorisation que vous prévoyez de mettre en correspondance.
- 2. La modification des données de session, dans cet exemple particulier, l'état de la session est passé de NotApplicable à Compliant.
- 3. Certificat d'authenticité du périphérique d'accès au réseau. Ce certificat d'authenticité doit réussir à pousser une nouvelle authentification du côté NAD et une nouvelle affectation de stratégie d'autorisation du côté ISE. Si le certificat d'authenticité a échoué, vous pouvez ouvrir un rapport détaillé pour en déterminer la raison. Les problèmes les plus courants peuvent être les suivants : Délai d'attente du certificat d'authenticité : dans ce cas, PSN qui a envoyé la demande n'est pas configuré comme client du certificat d'authenticité côté NAD, ou la demande du certificat d'authenticité a été abandonnée quelque part en cours de route.ACK négatif du certificat d'authenticité : indique que le certificat d'authenticité a été reçu par NAD mais que, pour une raison quelconque, le fonctionnement du certificat d'authenticité ne peut pas être confirmé. Pour ce scénario, le rapport détaillé doit contenir des explications plus détaillées.

Comme le routeur basé sur IOS XE a été utilisé comme NAD pour cet exemple, vous ne voyez aucune demande d'authentification ultérieure pour l'utilisateur. Cela se produit en raison du fait que l'ISE utilise la commande COA pour IOS XE, ce qui évite l'interruption de service VPN. Dans un tel scénario, le mode d'action lui-même contient de nouveaux paramètres d'autorisation, de sorte que la réauthentification n'est pas nécessaire.

Étape 3.Vérification du rapport de position - Accédez à **Opérations -> Rapports -> Rapports -> Terminaux et utilisateurs -> Évaluation de la position par terminal**.

dentity Services Engine	Home	► Conte	ext Visibility	✓ Operations	▶ Policy	Administration	Work Centers		License Warning 🔺 🔍	000	
RADIUS Threat-Centric NAC Live	Logs	+ TACACS	Troubleshoe	ot Adaptive	Network Control	Reports					
▼ Reports	Post	ture Asses	sment by Er	ndpoint 🕄					+ My Reports A Export	To • O Schedule	
▶ Audit	From 2018-06-07 00:00:00 to 2018-06-07 19:52:48:0										
Device Administration	Repo	rts exported i	in last 7 days (	0							
Diagnostics									<b>▼</b> Filter <b>▼</b>	CRefresh O-	
▼ Endpoints and Users		Logged	At	Status	Deta	ails PRA Act	lion	Identity	C Endpoint ID	IP Address	
Authentication Summary	×	Today	* ×					Identity	Endpoint ID		
Client Provisioning		2018-06-0	07 19:39:59.345	5 🔽	1	O N/A		vpnuser	50:00:00:03:00:00	10.20.30.112	
Current Active Sessions		2018-06-0	07 19:38:14.053	3 🔽	1	o N/A		vpn	50:00:00:03:00:00	10.20.30.111	
External Mobile Device M		2018-06-0	07 19:35:03.172	. 0	1	O N/A		vpnuser	50:00:00:03:00:00	10.20.30.110	
Manual Certificate Provisi		2018-06-0	07 19:29:38.761	2		N/A		vpn	50:00:00:03:00:00	10.20.30.109	
PassiveID		2018-06-0	07 19:26:52.657	· 🖉		N/A		vpnuser	50:00:00:03:00:00	10.20.30.108	
Posture Assessment by C		2018-06-0	07 19:17:17.906	3 🔽		o N/A		vpnuser	50:00:00:03:00:00	10.20.30.107	
Posture Assessment by E	4									+	
Profiled Endpoints Summ									Rows/Page 6 🔻 💷 1	6 Total Rows	

Vous pouvez ouvrir un rapport détaillé à partir d'ici pour chaque événement particulier pour vérifier par exemple à quel ID de session ce rapport appartient, quelles exigences de posture exactes ont été sélectionnées par ISE pour le point de terminaison et quel état pour chaque exigence.

## Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

1. Débogues IKEv2 à collecter à partir de la tête de réseau :

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

2. Débogues AAA pour voir l'affectation des attributs locaux et/ou distants :

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

- 3. DART du client AnyConnect.
- 4. Pour le dépannage du processus de posture, ces composants ISE doivent être activés dans le débogage sur les noeuds ISE où le processus de posture peut se produire :client-webapp composant responsable du provisionnement des agents. Fichiers journaux cibles guest.log et ise-psc.log.invité composant responsable de la recherche du composant du portail d'approvisionnement du client et du propriétaire de session (lorsque la demande provient d'un PSN incorrect). Fichier journal cible guest.log.approvisionnement composant responsable du traitement des stratégies d'approvisionnement client. Fichier journal cible guest.log.posture tous les événements liés à la posture. Fichier journal cible ise-psc.log
- 5. Pour le dépannage côté client, vous pouvez utiliser :AnyConnect.txt Ce fichier se trouve dans le bundle DART et est utilisé pour le dépannage VPN.acisensa.log -En cas d'échec du provisionnement du client côté client, ce fichier est créé dans le même dossier que celui dans lequel NSA a été téléchargé (répertoire de téléchargements pour Windows normalement),AnyConnect\_ISEPosture.txt Ce fichier se trouve dans le bundle DART du répertoire Cisco AnyConnect ISE Posture Module. Toutes les informations sur la découverte de ISE PSN et les étapes générales du flux de posture sont enregistrées dans ce fichier.