

Configurar a postura do ISE com FlexVPN

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[configuração de servidor DNS](#)

[Configuração inicial do IOS XE](#)

[Configurar certificado de identidade](#)

[Configurar IKEv2](#)

[Configuração do perfil do cliente Anyconnect](#)

[configuração de ISE](#)

[Configuração de certificados de administração e CPP](#)

[Criar um usuário local no ISE](#)

[Adicione o HUB FlexVPN como um cliente Radius](#)

[Configuração de provisionamento do cliente](#)

[Políticas e condições de postura](#)

[Configurar o Portal de Provisionamento do Cliente](#)

[Configurar perfis e políticas de autorização](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento fornece um exemplo de como configurar um headend IOS XE para acesso remoto com postura usando o método de autenticação AnyConnect IKEv2 e EAP-Message Digest 5 (EAP-MD5).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração VPN de acesso remoto FlexVPN (RA) no IOS XE
- Configuração de cliente AnyConnect (AC)
- Fluxo de postura no Identity Service Engine (ISE) 2.2 e posterior
- Configuração de componentes de postura no ISE
- Configuração do Servidor DNS no Windows Server 2008 R2

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco CSR1000V executando IOS XE 16.8 [Fuji]
- Cliente AnyConnect versão 4.5.03040 em execução no 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.

Informações de Apoio

Para garantir que as medidas de segurança de rede impostas permaneçam relevantes e eficazes, o Cisco ISE permite validar e manter os recursos de segurança em qualquer máquina cliente que acesse a rede protegida. Ao empregar políticas de postura projetadas para garantir que as configurações ou aplicativos de segurança mais atualizados estejam disponíveis em máquinas cliente, o administrador do Cisco ISE pode garantir que qualquer máquina cliente que acesse a rede atenda e continue a atender aos padrões de segurança definidos para acesso à rede corporativa. Os relatórios de conformidade de postura fornecem ao Cisco ISE um instantâneo do nível de conformidade da máquina cliente no momento do login do usuário, bem como a qualquer momento em que ocorre uma reavaliação periódica.

A postura pode ser representada por três elementos principais:

1. ISE como ponto de decisão e distribuição da configuração de política. Do ponto de vista do administrador do ISE, você configura políticas de postura (quais condições exatas devem ser atendidas para marcar o dispositivo como um compatível corporativo), políticas de provisionamento do cliente (que software do agente deve ser instalado em que tipo de dispositivos) e políticas de autorização (a que tipo de permissões deve ser atribuído, depende do status da postura).
2. NAD (Network Access Device, dispositivo de acesso à rede) como um ponto de aplicação de política. No lado do NAD, as restrições reais de autorização são aplicadas no momento da autenticação do usuário. O ISE como um ponto de política fornece parâmetros de autorização, como a ACL (Access Control List, lista de controle de acesso). Tradicionalmente, para que a postura ocorra, os NADs são necessários para suportar a CoA (Change of Authorization, alteração de autorização) para reautenticar o usuário depois que o status da postura do ponto de extremidade é determinado. A partir do ISE 2.2, os NADs não são necessários para suportar o redirecionamento.
Note: Os roteadores que executam o IOS XE não suportam redirecionamento. **Note:** O software IOS XE deve ter correções para os seguintes defeitos para ter CoA com ISE totalmente operacional:
[CSCve16269](#) IKEv2 CoA não funciona com ISE
[CSCvi90729](#) IKEv2 CoA não funciona com ISE (coa-push=TRUE em vez de true)
3. Software do agente como ponto de coleta de dados e interação com o usuário final. O agente recebe informações sobre os requisitos de postura do ISE e fornece relatórios ao ISE

sobre o status dos requisitos. Este documento é baseado no Módulo de Postura do ISE do Anyconnect, o único que suporta a postura completamente sem redirecionamento.

O fluxo de postura sem redirecionamento está bem documentado no artigo "[ISE Posture Style Comparison for Pre and Post 2.2](#)" (Comparação do estilo de postura do ISE para Pre e Post 2.2), seção "Posture flow in ISE 2.2" (Fluxo de postura no ISE 2.2).

O provisionamento do módulo de postura do AnyConnect ISE com FlexVPN pode ser feito de duas maneiras diferentes:

- Manual - o módulo é instalado manualmente na operação do cliente a partir do pacote Anyconnect disponível no portal de Download de Software da Cisco:

<https://software.cisco.com/download/home/283000185>.

As seguintes condições devem ser atendidas para o trabalho de postura com o provisionamento manual do ISE Posture Module:

1. O Domain Name Server (DNS) deve resolver o nome de domínio totalmente qualificado (FQDN) **enroll.cisco.com** para IPs de nós de serviço de política (PSNs). Durante a primeira tentativa de conexão, o módulo de postura não tem nenhuma informação sobre PSNs disponíveis. Ele está enviando sondas de descoberta para encontrar PSNs disponíveis. O FQDN enroll.cisco.com é usado em uma dessas sondas.
2. A porta **TCP 8905** deve ser permitida para PSNs IPs. A postura está passando pela porta TCP 8905 neste cenário.
3. O **certificado administrativo** nos nós PSN deve ter **enroll.cisco.com** no campo **SAN**. A conexão entre o usuário VPN e o nó PSN via TCP 8905 é protegida por certificado Admin e o usuário receberá um aviso de certificado se não houver esse nome "enroll.cisco.com" no certificado Admin do nó PSN.

Note: De acordo com o [RFC6125](#), os CNs do certificado devem ser ignorados se houver valores de SAN especificados. Isso significa que também precisamos adicionar CNs de certificado de administração no campo SAN.

- Provisionamento automático através do Client Provisioning Portal (CPP) - o módulo é baixado e instalado do ISE acessando o CPP diretamente através do FQDN do portal.

As seguintes condições devem ser atendidas para o trabalho de postura com o provisionamento automático do ISE Posture Module:

1. O DNS deve resolver o **FQDN do CPP** para IPs de nós de serviço de política (PSNs).
2. **As portas TCP 80, 443 e a porta de CPP (8443 por padrão)** devem ser permitidas para os IPs PSNs. O cliente precisa abrir o FQDN do CPP diretamente via HTTP (será redirecionado para HTTPS) ou HTTPS, essa solicitação será redirecionada para a porta do CPP (8443 por padrão) e a postura passará por essa porta.
3. **Certificados de Admin e CPP** nos nós PSN devem ter **FQDN de CPP** no campo **SAN**. A conexão entre o usuário VPN e o nó PSN via TCP 443 é protegida pelo certificado Admin e a conexão na porta CPP é protegida pelo certificado CPP.

Note: De acordo com o [RFC6125](#), os CNs do certificado devem ser ignorados se houver

valores de SAN especificados. Isso significa que também precisamos adicionar CNs de certificados de Admin e CPP no campo SAN de certificados correspondentes.

Note: Se o software ISE não contiver uma correção para [CSCvj76466](#), a postura ou o provisionamento do cliente funcionará somente se a exposição ou o provisionamento do cliente forem feitos no mesmo PSN no qual o cliente foi autenticado.

Em caso de postura com FlexVPN, o fluxo inclui estes passos:

1. O usuário se conecta ao hub FlexVPN usando o cliente Anyconnect.
2. O ISE envia Access-Accept ao FlexVPN Hub com o nome da ACL deve ser aplicado para restringir o acesso.
- 3 bis. Primeira conexão com o provisionamento manual - O módulo de postura do ISE começa a descobrir o servidor de política enviando a sonda para se inscrever.cisco.com através da porta TCP 8905. Como resultado bem-sucedido, o módulo de postura baixa o perfil de postura configurado e atualiza o módulo de conformidade no lado do cliente.

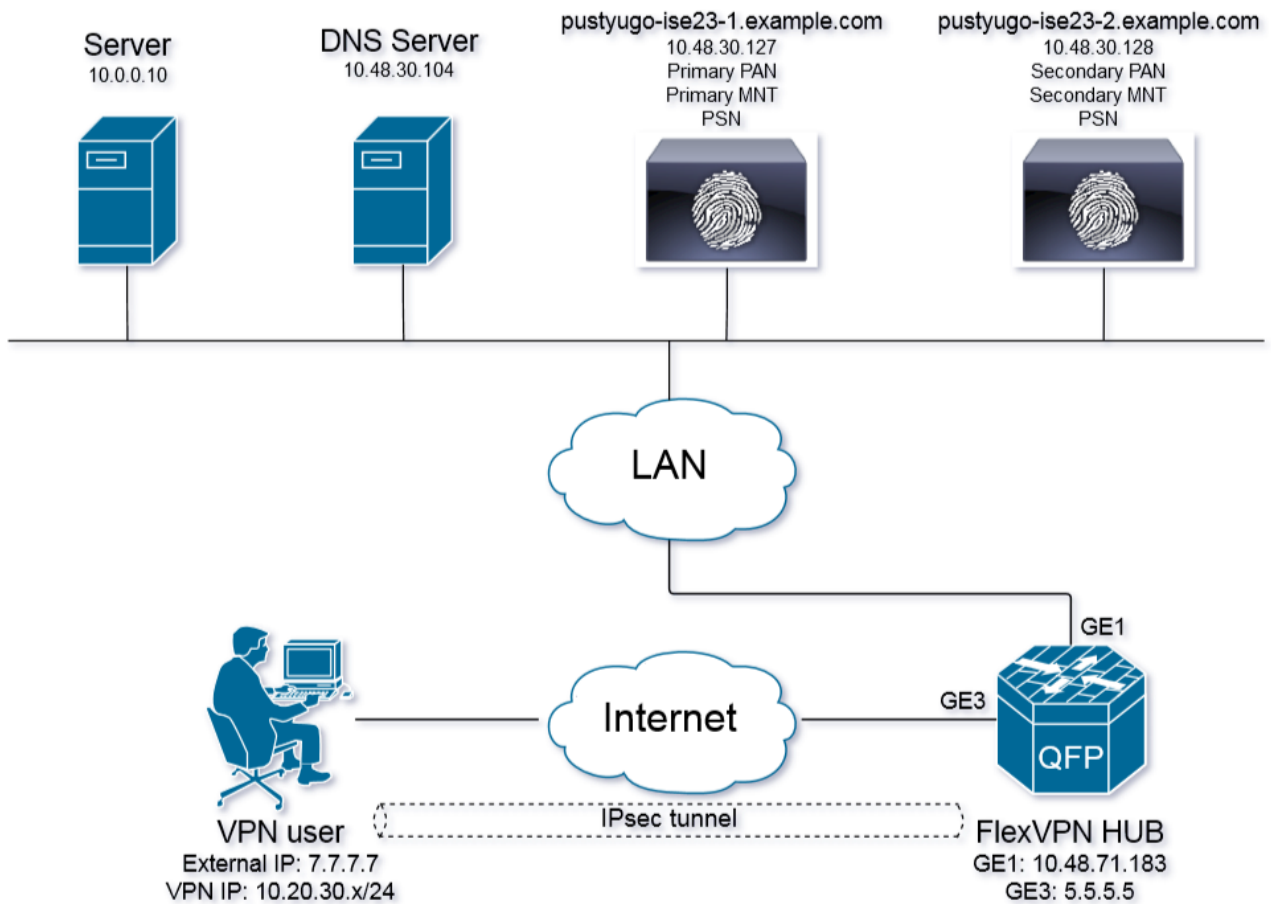
Durante as próximas tentativas de conexão, o módulo de postura do ISE também usará Nomes e IPs especificados na Lista do Call Home do perfil de postura para a detecção do servidor de política.
- 3 ter. Primeira conexão com o provisionamento automático - O cliente abre o CPP via FQDN. Como resultado bem-sucedido, o Network Setup Assistant é baixado na estação de trabalho do cliente e, em seguida, ele faz o download e instala o módulo de postura ISE, o módulo de conformidade ISE e o perfil de postura.

Durante as próximas tentativas de conexão, o módulo de postura do ISE usará Nomes e IPs especificados na Lista do Call Home do perfil de postura para a detecção do servidor de política.
4. O módulo de postura inicia verificações de conformidade e envia os resultados da verificação ao ISE.
5. Se o status do cliente for Compatível, o ISE enviará Access-Accept ao FlexVPN Hub com o nome da ACL deve ser aplicado ao cliente compatível.
- 6, o cliente tem acesso à rede.

Mais detalhes sobre o processo de postura podem ser encontrados no documento "[Comparação de estilo de postura do ISE para Pré e Post 2.2](#)".

Configurar

Diagrama de Rede

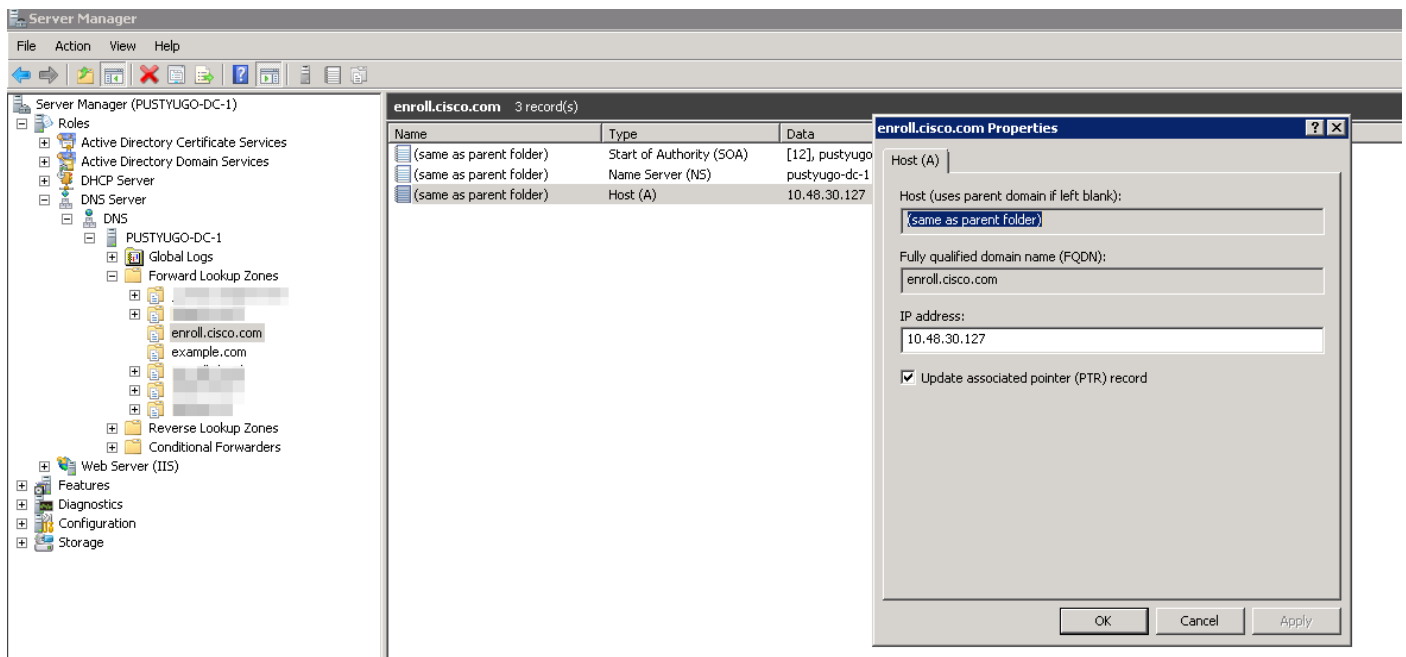


O usuário de VPN terá acesso ao Servidor (10.0.0.10) somente se tiver o status de conformidade.

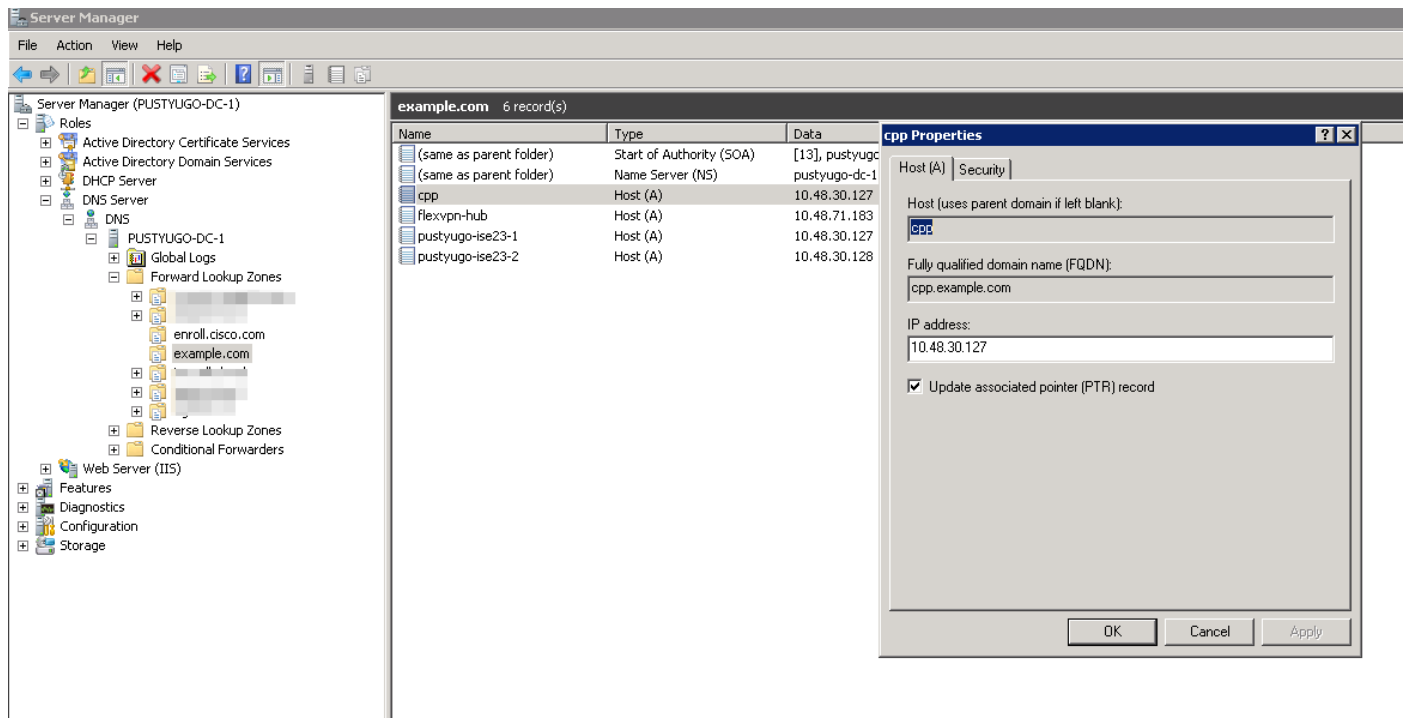
configuração de servidor DNS

Neste documento, o Windows Server 2008 R2 é usado como Servidor DNS.

Etapa 1. Adicione o registro **Host (A)** para **enroll.cisco.com** apontando para o IP da PSN:



Etapa 2. Adicione o registro **Host (A)** para CPP FQDN (**cpp.example.com** usado neste exemplo) apontando para o IP da PSN:



Configuração inicial do IOS XE

Configurar certificado de identidade

O roteador usará o certificado para se autenticar no cliente Anyconnect. O certificado do roteador deve ser confiável pelo sistema operacional do usuário para evitar o aviso de certificado durante a fase de estabelecimento da conexão.

O certificado de identidade pode ser fornecido de uma das seguintes formas:

Note: O uso de certificados autoassinados não é suportado com o IKEv2 FlexVPN.

Opção 1 - Configurar o servidor da autoridade de certificação (CA) no roteador

Note: O servidor CA pode ser criado no mesmo roteador IOS ou em outro roteador. Neste artigo, a CA é criada no mesmo roteador.

Note: Você precisa sincronizar o tempo com o servidor NTP antes que o servidor de CA possa ser ativado.

Note: Observe que o usuário não poderá verificar a autenticidade deste certificado, portanto, os dados do usuário não estarão protegidos contra ataques de intermediários, a menos que o certificado CA seja verificado manualmente e importado na máquina do usuário antes de estabelecer a conexão.

Etapa 1. Gerar chaves RSA para o servidor CA:

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

Etapa 2. Gerar chaves RSA para certificado de identidade:

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

Verificação:

```
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
```

Etapa 3. Configurar a AC:

```
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
```

Verificação:

```
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
```

Etapa 4. Configure o ponto confiável:

```
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
```

Etapa 5. Autenticar a AC:

```
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.
```

Etapa 6. Registre o roteador na CA:

```
FlexVPN-HUB(config)#crypto pki enroll FLEX-TP-1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: cn=flexvpn-hub.example.com
% The fully-qualified domain name will not be included in the certificate
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose FLEX-TP-1' command will show the fingerprint.

May 21 16:16:55.922: CRYPTO_PKI: Certificate Request Fingerprint MD5: 80B1FAFD 35346D0F
D23F6648 F83F039B
May 21 16:16:55.924: CRYPTO_PKI: Certificate Request Fingerprint SHA1: A8401EDE 35EE4AF8
46C4D619 8D653BFD 079C44F7
```

Verifique as solicitações de certificado pendentes na CA e verifique se a impressão digital corresponde a:

```
FlexVPN-HUB#show crypto pki server ROOT-CA requests
Enrollment Request Database:

Subordinate CA certificate requests:
ReqID  State      Fingerprint                               SubjectName
-----
RA certificate requests:
ReqID  State      Fingerprint                               SubjectName
-----
```



```
Router certificates requests:
ReqID State      Fingerprint                               SubjectName
-----
1      pending      80B1FAFD35346D0FD23F6648F83F039B  cn=flexvpn-hub.example.com
```

Passo 7. Conceda o certificado usando a ID de solicitação adequada:

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

Aguarde até que o roteador solicite o certificado novamente (de acordo com essa configuração, ele verificará 10 vezes uma vez por minuto). Procure a mensagem do syslog:

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

Verifique se o certificado está 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
```

Opção 2 - Importar certificado assinado externamente

```
FlexVPN-HUB(config)# crypto pki import FLEX-TP-2 pkcs12 ftp://cisco:cisco@10.48.30.130/ password
ciscol23
% 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)#
```

Configurar IKEv2

Etapa 1. Configurar o servidor RADIUS e 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
```

Etapa 2. Configurar listas de autenticação e autorização:

```
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
```

Etapa 3. Criar política de autorização 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
```

Etapa 4. Criar 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
```

Etapa 5. Criar conjunto de transformações e perfil de 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
```

Etapa 6. Criar interface de modelo virtual:

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

Passo 7. Criar pool local:

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

Etapa 8. Crie uma ACL para restringir o acesso de clientes não compatíveis. Durante o estado de postura desconhecido, pelo menos essas permissões devem ser fornecidas:

- tráfego DNS
- Tráfego para PSNs ISE através das portas 80, 443 e 8905
- Tráfego para PSNs ISE para os quais o portal CPP FQDN aponta
- Tráfego para servidores de correção, se necessário

Este é um exemplo de ACL sem servidores de remediação, a negação explícita para a rede 10.0.0.0/24 é adicionada para visibilidade, existe implícito "deny ip any any" no final da 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
```

Etapa 9. Criar ACL para permitir acesso para clientes compatíveis:

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

Etapa 10. Configuração de túnel dividido (opcional)

Por padrão, todo o tráfego será direcionado sobre VPN. Para fazer o túnel do tráfego apenas para as redes especificadas, você pode especificá-las na seção política de autorização ikev2. É possível adicionar várias instruções ou usar a lista de acesso padrão.

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

Etapa 11. Acesso à Internet para clientes remotos (opcional)

Para que as conexões de saída dos clientes de acesso remoto para os hosts na Internet sejam NAT-ed para o endereço IP global do roteador, configure a conversão 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
```

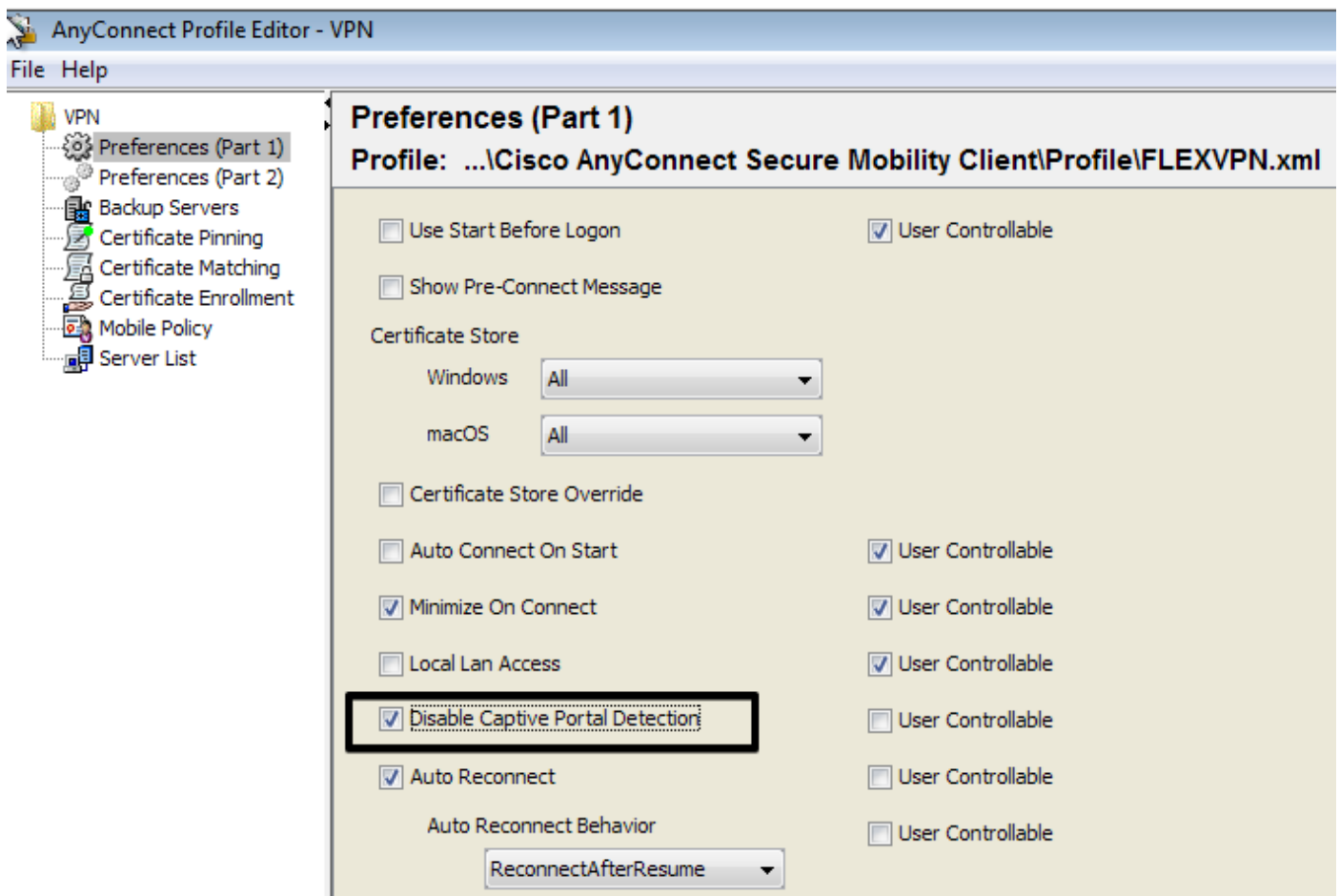
```
interface GigabitEthernet1  
ip nat outside
```

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

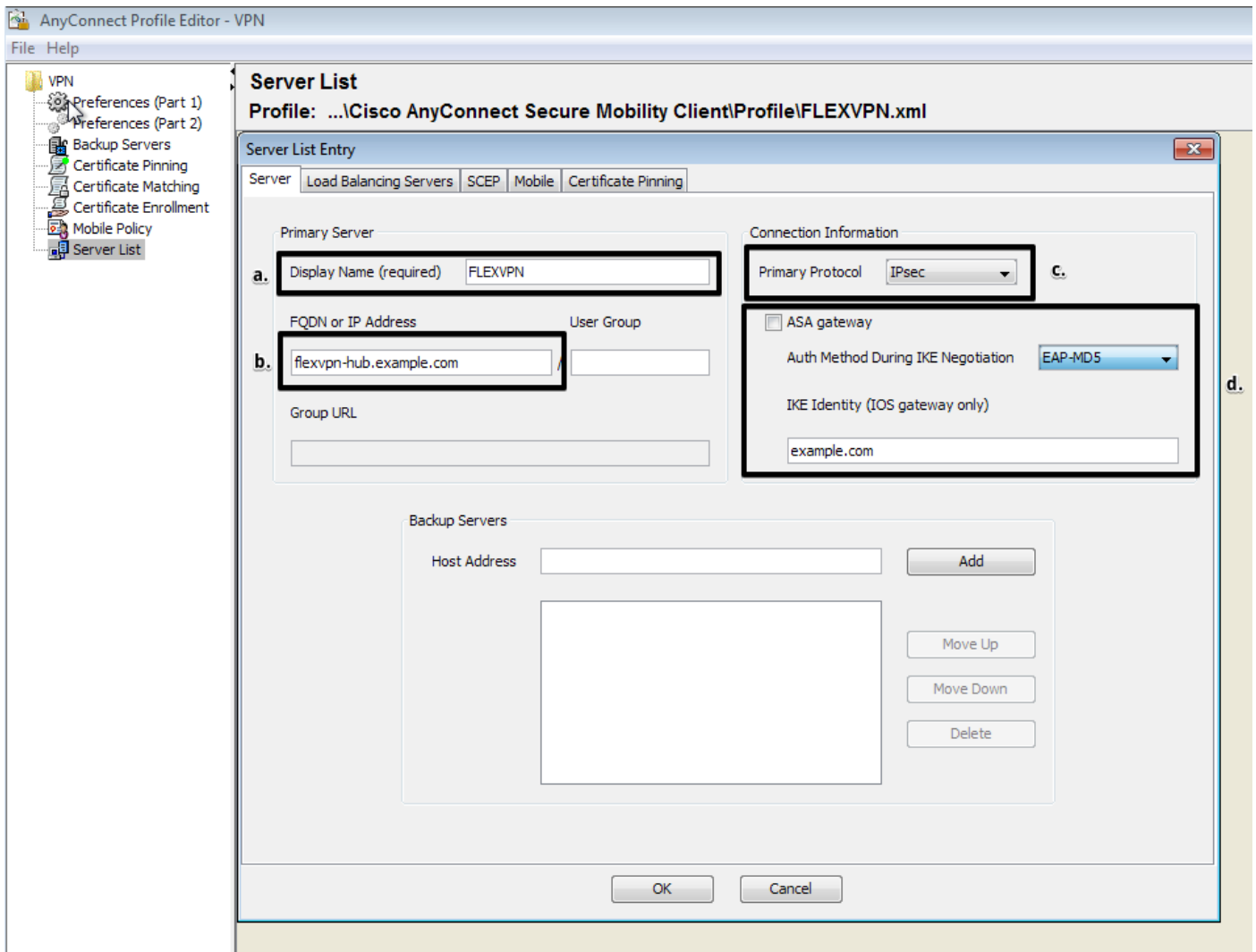
Configuração do perfil do cliente Anyconnect

Configure o perfil do cliente usando o Editor de perfis do AnyConnect. Os perfis do Anyconnect Security Mobile Client no Windows 7 e 10 são guardados em **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile**.

Etapa 1. Desative o recurso Captive Portal Detection (Detecção do portal cativo). Se o servidor http não estiver desabilitado no FlexVPN Hub, o recurso de detecção de portal cativo do AnyConnect fará com que a conexão falhe. Observe que o servidor CA não funcionará sem o servidor HTTP.



Etapa 2. Configurar lista de servidores:



- Insira Display Name (Nome de exibição).
- Insira o endereço FQDN ou IP do FlexVPN Hub.
- Selecione IPsec como Protocolo Primário.
- Desmarque a caixa de seleção "ASA gateway" e especifique **EAP-MD5** como Método de Autenticação. Insira a Identidade IKE exatamente igual à configuração do perfil IKEv2 no Hub FlexVPN (neste exemplo, o perfil IKEv2 é configurado com o comando "match identity remote key-id example.com", portanto precisamos usar **example.com** como Identidade IKE).

Etapa 3. Salve o perfil em %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile e reinicie o AC.

O equivalente XML do 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>
  </ClientInitialization>
</AnyConnectProfile>
```

```

<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>
<RSA SecurIDIntegration UserControllable="false">Automatic</RSA SecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>>false</AutomaticVPNPolicy>
<PPPEExclusion UserControllable="false">Automatic
  <PPPEExclusionServerIP UserControllable="false"></PPPEExclusionServerIP>
</PPPEExclusion>
<EnableScripting UserControllable="false">>false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="true">>false
  <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
  <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>>false
</RetainVpnOnLogoff>
<AllowManualHostInput>>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
  <HostEntry>
    <HostName>FLEXVPN</HostName>
    <HostAddress>flexvpn-hub.example.com</HostAddress>
    <PrimaryProtocol>IPsec
      <StandardAuthenticationOnly>>true
        <AuthMethodDuringIKENegotiation>EAP-MD5</AuthMethodDuringIKENegotiation>
        <IKEIdentity>example.com</IKEIdentity>
      </StandardAuthenticationOnly>
    </PrimaryProtocol>
  </HostEntry>
</ServerList>
</AnyConnectProfile>

```

configuração de ISE

Configuração de certificados de administração e CPP

Note: A alteração do certificado Admin reiniciará o nó no qual o certificado foi alterado.

Etapa 1. Vá para **Administração -> Sistema -> Certificados -> Solicitações de Assinatura de Certificado**, clique em **Gerar Solicitações de Assinatura de Certificado (CSR)**:

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Setti...

Certificate Authority

Certificate Signing Requests

[Generate Certificate Signing Requests \(CSR\)](#)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

View Export Delete Bind Certificate

<input type="checkbox"/>	Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp
No data available					

Etapa 2. Na página aberta, selecione o nó PSN necessário, preencha os campos necessários e adicione o FQDN do nó, enroll.cisco.com, cpp.example.com e o endereço IP do nó nos campos de SAN e clique em **Gerar**:

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Setti...

Certificate Authority

Usage

Certificate(s) will be used for ⚠ You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).

Allow Wildcard Certificates ⓘ

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> pustyugo-ise23-1	pustyugo-ise23-1#Multi-Use
<input type="checkbox"/> pustyugo-ise23-2	pustyugo-ise23-2#Multi-Use

Subject

Common Name (CN) ⓘ

Organizational Unit (OU) ⓘ

Organization (O) ⓘ

City (L)

State (ST)

Country (C)

Subject Alternative Name (SAN)

DNS Name	pustyugo-ise23-1.example.com	-	+
DNS Name	enroll.cisco.com	-	+
DNS Name	cpp.example.com	-	+
IP Address	10.48.30.127	-	+

* Key type ⓘ

* Key Length ⓘ

* Digest to Sign With

Certificate Policies

Note: Se você selecionar **multiuso** nesta etapa, poderá usar o mesmo certificado para o Portal também.

Na janela exibida, clique em **Exportar** para salvar o CSR em formato pem na estação de trabalho local:



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

Etapa 3. Cante o CSR com CA confiável e obtenha o arquivo de certificado da CA, bem como a cadeia completa de certificados CA (raiz e intermediário).

Etapa 4. Vá para **Administração -> Sistema -> Certificados -> Certificados confiáveis**, clique em **Importar**. Na tela seguinte, clique em **Escolher arquivo** e selecione Arquivo certificado **CA raiz**, preencha o nome amigável e a descrição, se necessário, selecione **Opções confiáveis para** e clique em **Enviar**:

Import a new Certificate into the Certificate Store

* Certificate File PUSTYUGODC1.pem

Friendly Name

Trusted For:

Trust for authentication within ISE

Trust for client authentication and Syslog

Trust for authentication of Cisco Services

Validate Certificate Extensions

Description

Repita essa etapa para todos os certificados intermediários na cadeia, se houver algum.

Etapa 5. Retorne a **Administration -> System -> Certificados -> Certificate Signing Requests**, selecione o CSR necessário e clique em **Bind Certificate**:

Certificate Signing Requests

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

<input type="checkbox"/>	Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
<input checked="" type="checkbox"/>	pustyugo-ise23-1#Multi-Use	CN=pustyugo-ise23-1....	2048		Sun, 10 Jun 2018	pustyugo-ise

Etapa 6. Na página aberta, clique em **Escolher arquivo**, selecione o arquivo de certificado recebido da CA, digite o nome amigável, se necessário, e selecione **Uso: Admin (Uso: O portal também pode ser selecionado aqui se o CSR foi criado com multiuso)** e clique em **Enviar**:

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and Threat Centric NAC. The main menu is expanded to Certificates, with sub-menus for Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Settings. The left sidebar shows Certificate Management options: System Certificates, Trusted Certificates, OSCP Client Profile, Certificate Signing Requests, and Certificate Periodic Check Setti... The main content area is titled 'Bind CA Signed Certificate' and contains the following fields and options:

- * Certificate File: Signed CSR.cer
- Friendly Name: ⓘ
- Validate Certificate Extensions: ⓘ
- Usage section with the following options:
 - Admin: Use certificate to authenticate the ISE Admin Portal
 - EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
 - RADIUS DTLS: Use certificate for the RADSec server
 - pxGrid: Use certificate for the pxGrid Controller
 - Portal: Use for portal

At the bottom of the form are and .

Passo 7. Na janela pop-up de aviso, clique em **Sim** para concluir a importação. O nó afetado pela alteração do certificado do administrador será reiniciado:

The screenshot shows a warning pop-up dialog box with a yellow warning icon. The text inside the dialog reads:

Enabling Admin role for this certificate will cause an application server restart on the selected node.

Note: Make sure required Certificate Chain is imported under Trusted Certificates

At the bottom right of the dialog are two buttons: and .

Repita as etapas para alterar o certificado CPP se decidir usar certificado separado para o portal. Na etapa 6, selecione **Uso: Portal** e clique em **Enviar**:

Bind CA Signed Certificate

* Certificate File Signed CSR Portal.cer

Friendly Name ⓘ

Validate Certificate Extensions ⓘ

Usage

- Admin: Use certificate to authenticate the ISE Admin Portal
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- RADIUS DTLS: Use certificate for the RADSec server
- pxGrid: Use certificate for the pxGrid Controller
- Portal: Use for portal

* Portal group tag ⓘ

Portal(s) using this tag

BYOD Portal (default)	Blacklist Portal (default)
Certificate Provisioning Portal (default)	Client Provisioning Portal (default)
Hotspot Guest Portal (default)	MDM Portal (default)
My Devices Portal (default)	Self-Registered Guest Portal (default)
Sponsor Portal (default)	Sponsored Guest Portal (default)

Repita as etapas para todos os PSNs na implantação do ISE.

Criar um usuário local no ISE

Note: Com o método EAP-MD5, somente usuários locais são suportados no ISE.

Etapa 1. Vá para **Administração -> Gerenciamento de identidades -> Identidades -> Usuários**, clique em **Adicionar**.

Network Access Users

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
No data available							

Etapa 2. Na página aberta, digite o nome de usuário, a senha e outras informações necessárias e clique em **Enviar**.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > **New Network Access User**

Network Access User

* Name

Status Enabled

Email

Passwords

Password Type:

Password Re-Enter Password

* Login Password ⓘ

Enable Password ⓘ

User Information

First Name

Last Name

Account Options

Description

Change password on next login

Account Disable Policy

Disable account if date exceeds (yyyy-mm-dd)

User Groups

Adicione o HUB FlexVPN como um cliente Radius

Etapa 1. Vá para **Centros de trabalho -> Postura -> Dispositivos de rede**, clique em **Adicionar**.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassivelD

Overview **Network Devices** Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Network Devices

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

Ster 2. Na página aberta, digite Device Name (Nome do dispositivo), IP address (Endereço IP), outras informações necessárias, marque a caixa de seleção "RADIUS Authentication settings" (Configurações de autenticação RADIUS), digite Shared Secret (Segredo compartilhado) e clique em **Submit (Enviar)** na parte inferior da página.



Network Devices List > New Network Device

Network Devices

* Name

Description

IP Address * IP: /

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

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Use Second Shared Secret ⓘ

CoA Port

RADIUS DTLS Settings ⓘ

DTLS Required ⓘ

Shared Secret ⓘ

CoA Port

Issuer CA of ISE Certificates for CoA ⓘ

DNS Name

General Settings

Enable KeyWrap ⓘ

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

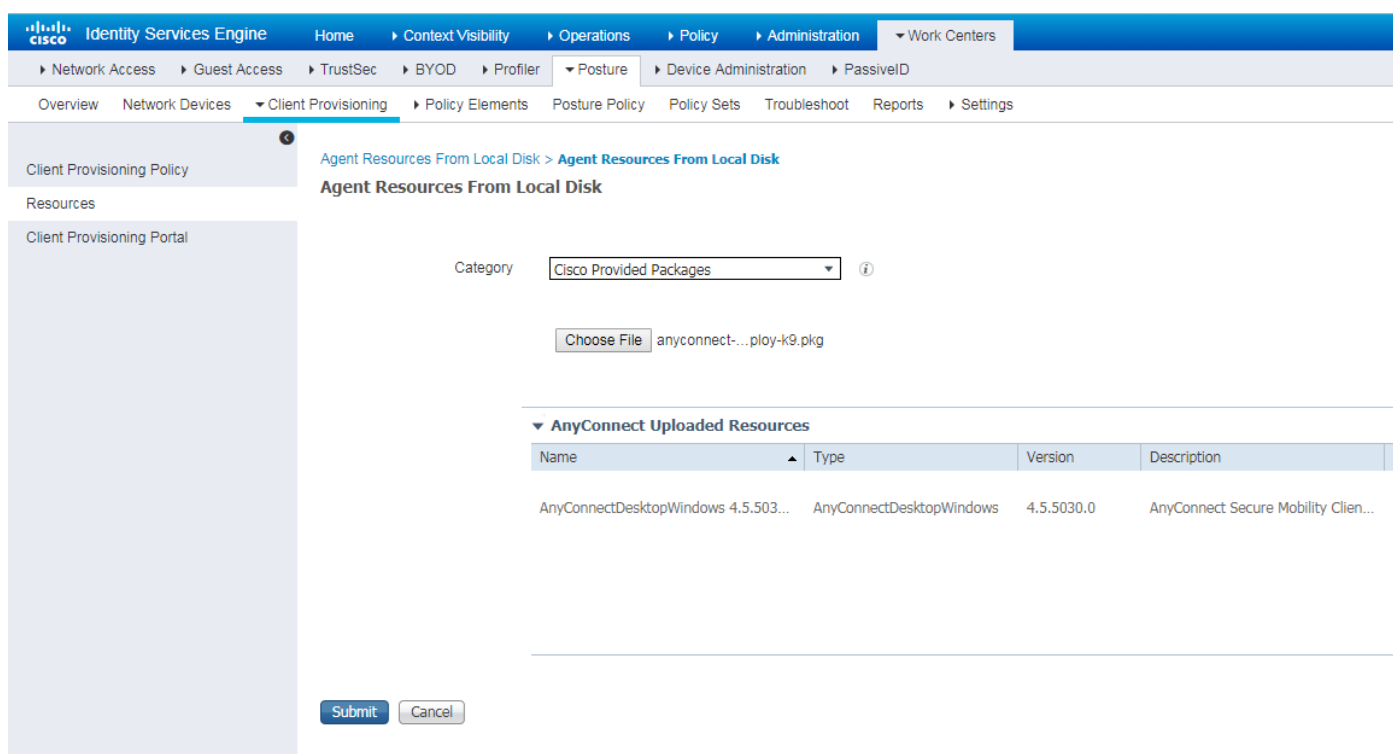
Configuração de provisionamento do cliente

Estas são as etapas para preparar a configuração do Anyconnect.

Etapa 1. Download do pacote do Anyconnect. O pacote do Anyconnect em si não está disponível para download direto do ISE, portanto, antes de começar, certifique-se de que o AC esteja disponível em seu PC. Este link pode ser usado para download em CA -

<http://cisco.com/go/anyconnect>. Neste documento, o pacote anyconnect-win-4.5.05030-webDeployment-k9.pkg é usado.

Etapa 2. Para carregar o pacote AC no ISE, navegue até **Work Centers -> Posture -> Client Provisioning -> Resources** clique em **Add**. Escolha **Recursos do agente no disco local**. Na nova janela, escolha **Cisco Provided Packages**, clique em **Choose File** (Escolher arquivo) e selecione AC package (Pacote CA) em seu PC.



Client Provisioning Policy

Agent Resources From Local Disk > Agent Resources From Local Disk

Agent Resources From Local Disk

Category: Cisco Provided Packages

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

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

Submit Cancel

Clique em **Enviar** para concluir a importação. Verifique o hash da embalagem e pressione **Confirmar**.

Etapa 3. O módulo de conformidade deve ser carregado no ISE. Na mesma página (**Centros de trabalho -> Postura -> Provisionamento de cliente -> Recursos**), clique em **Adicionar** e escolha **Recursos de agente no site da Cisco**. Na lista de recursos, você deve verificar um módulo de conformidade e clicar em **Salvar**. Para este documento É usado o módulo de conformidade AnyConnectComplianceModuleWindows 4.3.50.0.

Download Remote Resources

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization Package v1.1.1.6 for Wir
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 3.6.11682.2	AnyConnect OS X Compliance Module 3.6.11682.2
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.29.0	AnyConnect OSX Compliance Module 4.3.29.0
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 3.6.11682.2	AnyConnect Windows Compliance Module 3.6.11682.2
<input checked="" type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.50.0	AnyConnect Windows Compliance Module 4.3.50.0
<input type="checkbox"/>	CiscoTemporalAgentOSX 4.5.02036	Cisco Temporal Agent for OSX With CM: 4.2.1019.0 Works wi
<input type="checkbox"/>	CiscoTemporalAgentWindows 4.5.02036	Cisco Temporal Agent for Windows With CM: 4.2.1226.0 Work
<input type="checkbox"/>	ComplianceModule 3.6.11510.2	NACAgent ComplianceModule v3.6.11510.2 for Windows
<input type="checkbox"/>	MACComplianceModule 3.6.11510.2	MACAgent ComplianceModule v3.6.11510.2 for MAC OSX
<input type="checkbox"/>	MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9.4.3 - ISE 1.2 , ISE 1.1.:
<input type="checkbox"/>	MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9.5.3 - ISE 1.2 Patch 12,
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.18	Supplicant Provisioning Wizard for Mac OsX 1.0.0.18 (ISE 1.1
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for Mac OsX 1.0.0.21 (for ISE
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for Mac OsX 1.0.0.27 (for ISE
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for Mac OsX 1.0.0.29 (for ISE
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for Mac OsX 1.0.0.30 (for ISE

For AnyConnect software, please download from <http://cisco.com/go/anyconnect>. Use the "Agent resource from local disk" add option, to import into ISE

Save Cancel

Etapa 4. Agora, o perfil de postura AC precisa ser criado. Clique em **Adicionar** e escolha agente NAC ou perfil de postura do Anyconnect.

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

Client Provisioning Policy ISE Posture Agent Profile Settings > **New Profile**

Resources

Client Provisioning Portal

Posture Agent Profile Settings

a. AnyConnect

b. * Name: AC-4.5-Posture

Description:

Agent Behavior

- Escolha o tipo do perfil. O AnyConnect deve ser usado nesse cenário.
- Especifique o nome do perfil. Navegue até a seção **Protocolo de Postura** do perfil

Posture Protocol

Parameter	Value	Notes
PRA retransmission time	<input type="text" value="120"/> secs	
Discovery host	<input type="text"/>	
* Server name rules	<input type="text" value="*"/> a.	need to be blank by default to force admin to enter a value. "*" means agent will connect to all
Call Home List	<input type="text" value="pustyugo-ise23-1.examp"/> 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	<input type="text" value="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

- Especificar **Regras de Nome do Servidor**, este campo não pode estar vazio. O campo pode conter FQDN com curinga que restringe a conexão do módulo de postura AC a PSNs a partir do espaço de nomes apropriado. Coloque a estrela se algum FQDN for permitido.
 - Nomes e IPs especificados aqui estão em uso durante o estágio 2 da descoberta de postura (consulte o passo 14 da seção "[Fluxo de postura no ISE 2.2](#)"). Você pode separar nomes por coma, bem como o número da porta pode ser adicionado após FQDN/IP usando dois-pontos.
- Etapa 5. Criar configuração AC. Navegue até **Centros de trabalho -> Postura -> Provisionamento de cliente -> Recursos** e clique em **Adicionar** e selecione **Configuração do AnyConnect**.

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 ▶ Client Provisioning ▶ Policy Elements Posture Policy Policy Sets Troubleshoot Reports ▶ Settings

Client Provisioning Policy

AnyConnect Configuration > **New AnyConnect Configuration**

Resources

Client Provisioning Portal

* Select AnyConnect Package: AnyConnectDesktopWindows 4.5.5030.0 **a.**

* Configuration Name: AnyConnect Configuration **b.**

Description:

DescriptionValue

* Compliance Module: AnyConnectComplianceModuleWindows 4.3.50.0 **c.**

AnyConnect Module Selection

ISE Posture

VPN

Network Access Manager

Web Security

AMP Enabler

ASA Posture

Network Visibility

Umbrella Roaming Security

Start Before Logon

Diagnostic and Reporting Tool

Profile Selection

* ISE Posture: AC-4.5-Posture **d.**

VPN

Network Access Manager

Web Security

AMP Enabler

Network Visibility

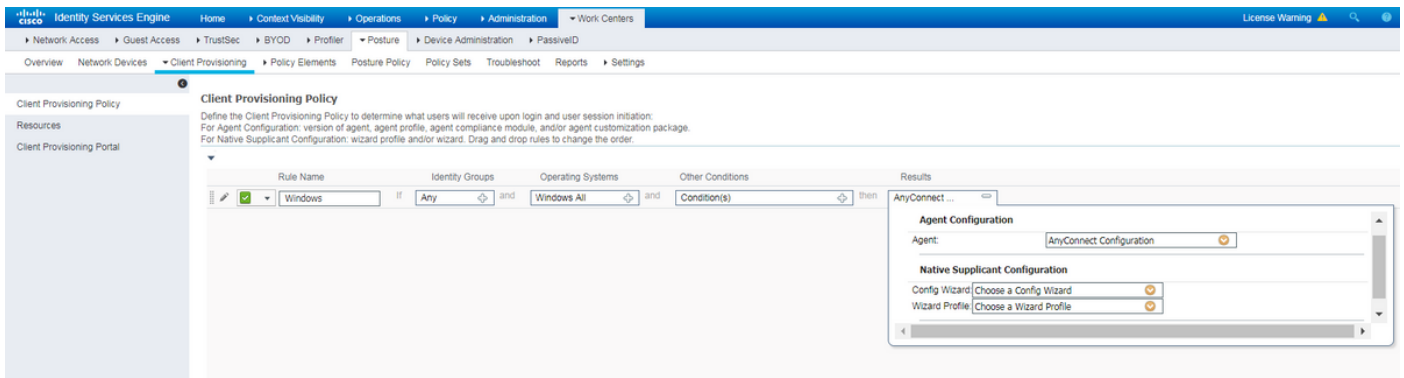
Umbrella Roaming Security

Customer Feedback

- Selecione o pacote AC.
- Forneça o nome da configuração AC.
- Escolha a versão do módulo de conformidade.
- Selecione perfil de configuração de postura AC na lista suspensa.

Etapa 6. Configure a política de provisionamento do cliente. Navegue até **Centros de trabalho -> Postura -> Provisionamento de cliente**. Em caso de configuração inicial, você pode preencher valores vazios na política apresentada com padrões. Em caso de necessidade de adicionar política à configuração de postura existente, navegue até a política que pode ser reutilizada e escolha **Duplicar acima** ou **Duplicar abaixo**. Também pode ser criada uma nova política de marcas.

Este é o exemplo da política usada no documento.

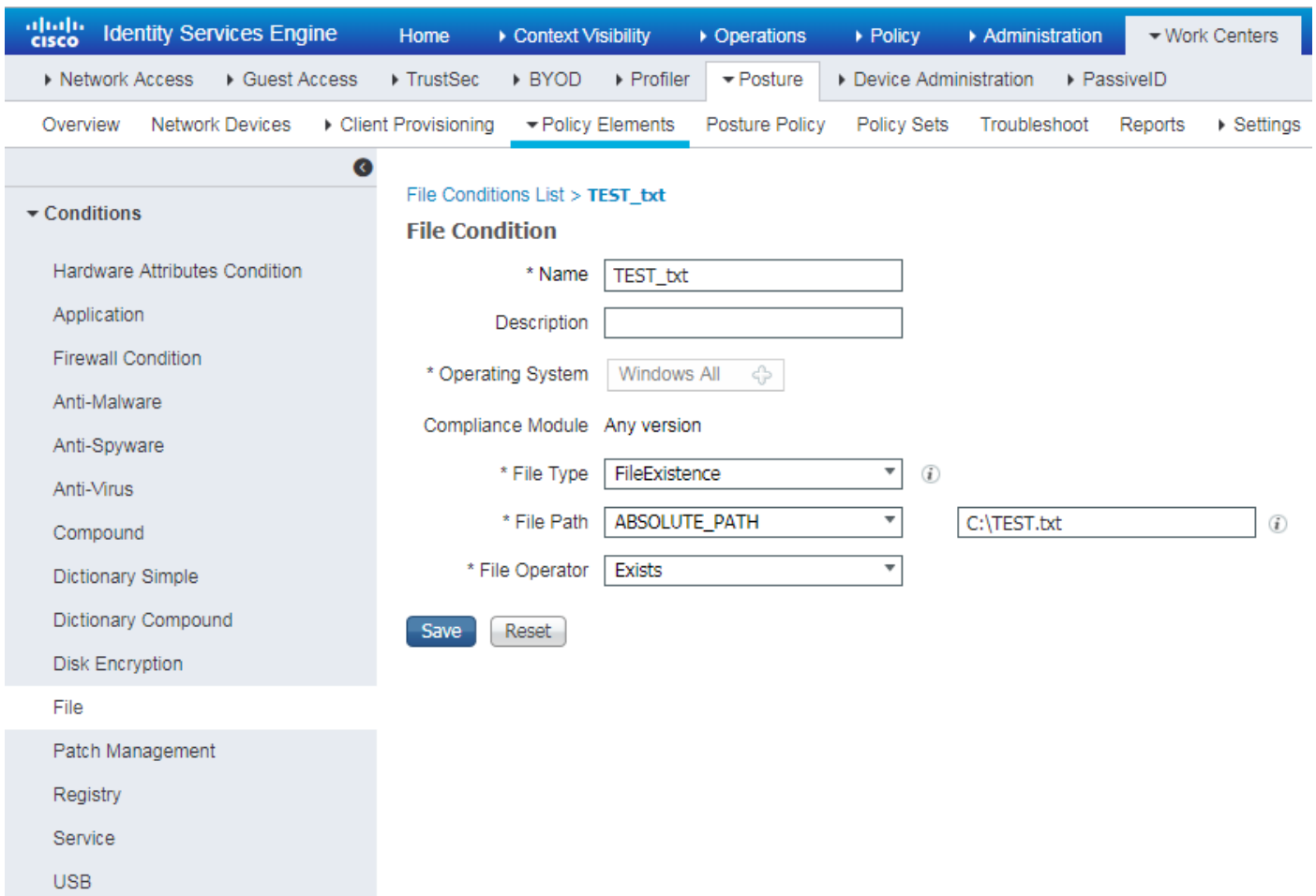


Escolha sua configuração AC na seção de resultados.

Políticas e condições de postura

É usada uma verificação de postura simples. O ISE está configurado para verificar a existência do arquivo C:\TEST.txt no lado do dispositivo final. Os cenários reais podem ser muito mais complicados, mas as etapas gerais de configuração são as mesmas.

Etapa 1. Criar condição de postura. As condições de postura estão localizadas em **Centros de Trabalho -> Postura -> Elementos de Política -> Condições**. Escolha o tipo de condição de postura e clique em **Adicionar**. Especifique as informações necessárias e clique em **Salvar**. Abaixo, você pode encontrar um exemplo de condição de serviço que deve verificar se o arquivo C:\TEST.txt existe.

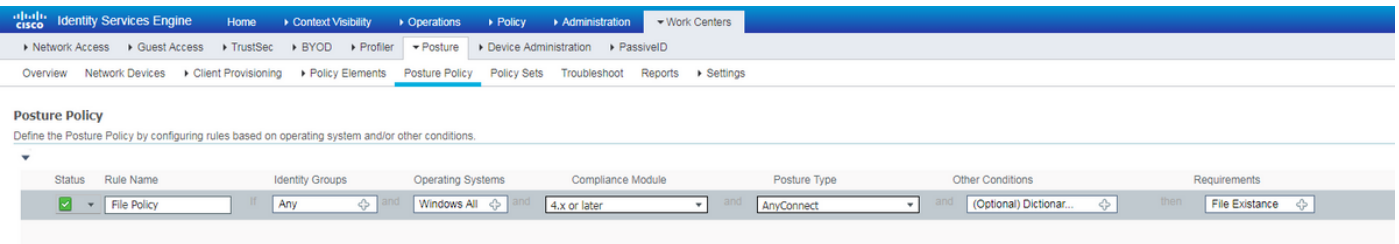


Etapa 2. Postar a configuração dos requisitos. Navegue até **Centros de trabalho -> Postura -> Elementos de política -> Requisitos**. Este é um exemplo da existência do arquivo TEST.txt:



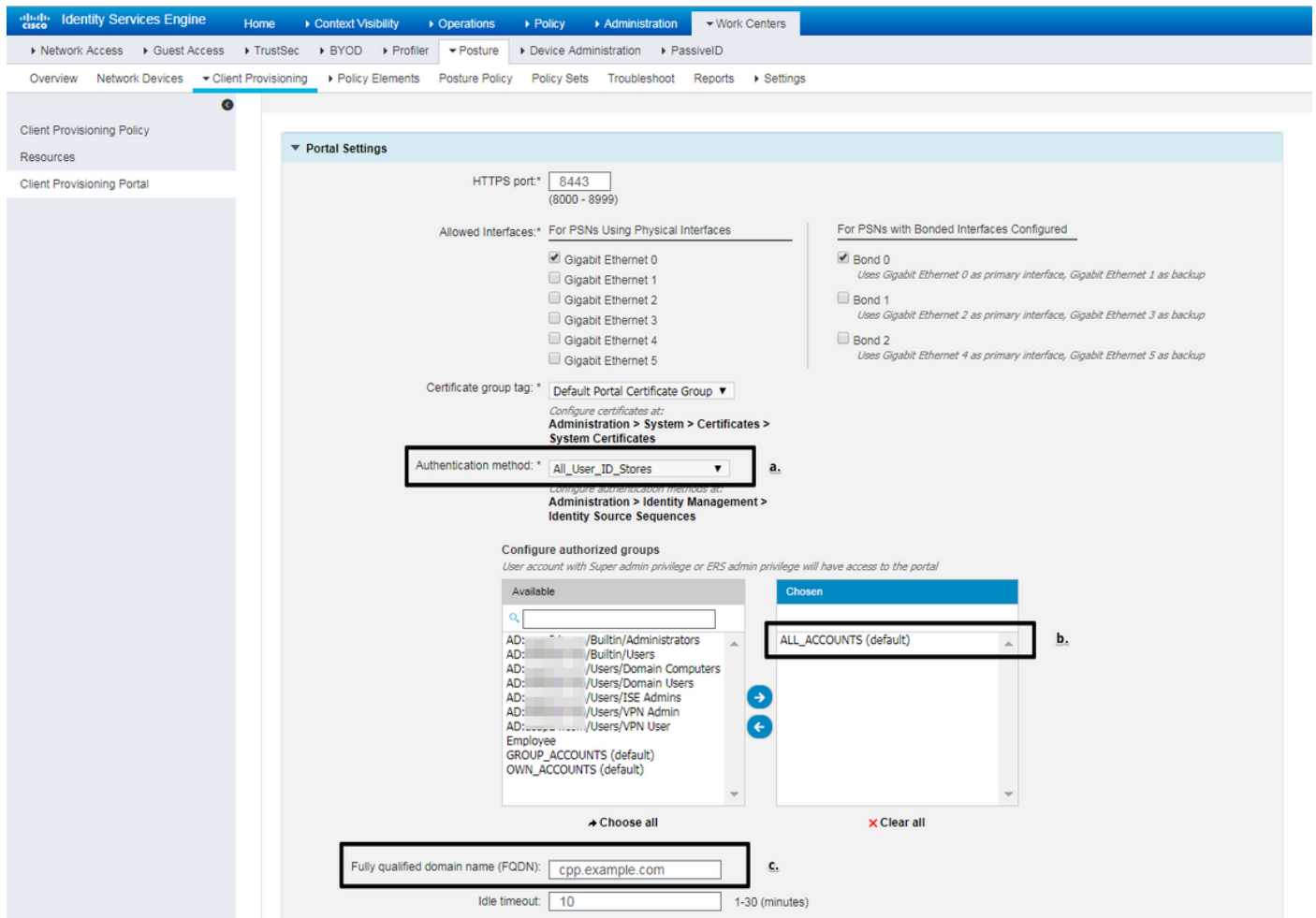
Escolha sua condição de postura em um novo requisito e especifique uma ação de correção.

Etapa 3. Configuração da política de postura. Navegue até **Centros de trabalho -> Postura -> Política de postura**. Abaixo, você pode encontrar um exemplo de política usada para este documento. A política tem o requisito "Existência de arquivo" atribuído como obrigatório e não tem nenhuma outra condição atribuída.



Configurar o Portal de Provisionamento do Cliente

Para postura sem redirecionamento, a configuração do portal de provisionamento do cliente deve ser editada. Navegue até **Centros de trabalho -> Postura -> Provisionamento de cliente -> Portal de provisionamento de cliente**. Você pode usar o portal padrão ou criar o seu próprio.



Essas configurações devem ser editadas na configuração do portal para o cenário de não redirecionamento:

- Na Autenticação, especifique a Sequência de Origem da Identidade que deve ser usada se o SSO não puder localizar a sessão para o usuário.
- De acordo com a sequência de origem de identidade selecionada, a lista de grupos disponíveis é preenchida. Neste ponto, você precisa selecionar grupos autorizados para login no portal.
- O FQDN do portal de provisionamento do cliente deve ser especificado. Esse FQDN deve ser resolvido para IPs de PSNs do ISE. Os usuários devem ser instruídos a especificar o FQDN no navegador da Web durante a primeira tentativa de conexão.

Configurar perfis e políticas de autorização

O acesso inicial para o cliente quando o status da postura não está disponível precisa ser restrito. Isso pode ser feito de várias maneiras:

- ID de filtro de RADIUS - com esse atributo, a ACL definida localmente no NAD pode ser atribuída ao usuário com status de postura desconhecido. Como esse é um atributo de RFC padrão, essa abordagem deve funcionar bem para todos os fornecedores de NAD.
- Cisco:cisco-av-pair = ip:interface-config - muito semelhante a Radius Filter-Id, a ACL definida localmente na NAD pode ser atribuída ao usuário com status de postura desconhecido.

Exemplo de configuração:

```
cisco-av-pair = ip:interface-config=ip access-group DENY_SERVER in
```

Etapa 1. Configure o perfil de autorização.

Como de costume para a postura, são necessários dois perfis de autorização. A primeira deve conter qualquer tipo de restrição de acesso à rede. Esse perfil pode ser aplicado às autenticações para as quais o status da postura não é igual à compatível. O segundo perfil de autorização pode conter apenas acesso de permissão e pode ser aplicado para uma sessão com status de postura igual à conformidade.

Para criar um perfil de autorização, navegue para **Centros de trabalho -> Postura -> Elementos de política -> Perfis de autorização**.

Exemplo de perfil de acesso restrito com ID de filtro de RADIUS:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Network Devices Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Authorization Profiles > LIMITED_ACCESS

Authorization Profile

* Name: LIMITED_ACCESS

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement: *i*

Passive Identity Tracking: *i*

Common Tasks

DACL Name

ACL (Filter-ID): DENY_SERVER.in

Security Group

VLAN

Advanced Attributes Settings

Select an item = +

Attributes Details

Access Type = ACCESS_ACCEPT
Filter-ID = DENY_SERVER.in

Exemplo de perfil de acesso restrito com par cisco-av:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Network Devices Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Authorization Profiles > LIMITED_ACCESS

Authorization Profile

* Name: LIMITED_ACCESS

Description: [Empty text box]

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement: (i)

Passive Identity Tracking: (i)

Common Tasks

DACL Name

ACL (Filter-ID)

Security Group

VLAN

Advanced Attributes Settings

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

Attributes Details

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

Exemplo de perfil de acesso ilimitado com ID de filtro RADIUS:

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

* Name:

Description:

* Access Type:

Network Device Profile:

Service Template:

Track Movement:

Passive Identity Tracking:

Common Tasks

DACL Name

ACL (Filter-ID) .in

Security Group

VLAN

Advanced Attributes Settings

= - +

Attributes Details

Access Type = ACCESS_ACCEPT
Filter-ID = PERMIT_ALL.in

Exemplo de perfil de acesso ilimitado com par cisco-av:

The screenshot shows the configuration page for a policy element in Cisco ISE. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID. The left sidebar contains a tree view with categories: Conditions (Hardware Attributes Condition, Application, Firewall Condition, Anti-Malware, Anti-Spyware, Anti-Virus, Compound, Dictionary Simple, Dictionary Compound, Disk Encryption, File, Patch Management, Registry, Service, USB), Remediations, Requirements, Allowed Protocols, Authorization Profiles, and Downloadable ACLs. The main configuration area includes:

- Name: UNLIMITED_ACCESS
- Description: (empty text area)
- Access Type: ACCESS_ACCEPT
- Network Device Profile: Cisco
- Service Template: (checkbox)
- Track Movement: (checkbox)
- Passive Identity Tracking: (checkbox)
- Common Tasks: (checkboxes for) DACL Name, ACL (Filter-ID), Security Group, VLAN
- Advanced Attributes Settings: Cisco:cisco-av-pair = ip:interface-config=ip access-g...
- Attributes Details: Access Type = ACCESS_ACCEPT; cisco-av-pair = ip:interface-config=ip access-group PERMIT_ALL in

Etapa 2. Configure a política de autorização. Durante esta etapa, devem ser criadas duas políticas de autorização. Um para corresponder a solicitação de autenticação inicial com status de postura desconhecido e outro para atribuir acesso total após o processo de postura bem-sucedido.

É um exemplo de políticas de autorização simples para este caso:

▼ Authorization Policy (12)

Status	Rule Name	Conditions	Results		
			Profiles	Security Groups	Hits
🟢	Unknown_Compliance_Redirect	AND Network_Access_Authentication_Passed Compliance_Unknown_Devices	= LIMITED_ACCESS	Select from list	55
🟢	NonCompliant_Devices_Redirect	AND Network_Access_Authentication_Passed Non_Compliant_Devices	= LIMITED_ACCESS	Select from list	3
🟢	Compliant_Devices_Access	AND Network_Access_Authentication_Passed Compliant_Devices	= UNLIMITED_ACCESS	Select from list	30

A configuração da política de autenticação não faz parte deste documento, mas você deve ter em mente que a autenticação precisa ser bem-sucedida antes do início do processamento da política de autorização.

Verificar

A verificação de base do fluxo pode consistir em três etapas principais:

Etapa 1. Verificação de sessão de VPN RA no 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

Etapa 2. Verificação de fluxo de autenticação (registros ao vivo do Radius):

Time	Status	Details	Identity	Posture Status	Endpoint ID	Authentication P...	Authorization Policy	Authorization Profiles	IP Address
3. Jun 07, 2018 07:40:01.378 PM			Identity	Compliant	7.7.7.7			UNLIMITED_ACCESS	
2. Jun 07, 2018 07:39:59.345 PM			vpuser	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			vpuser	NotApplicable	7.7.7.7	Default >> Default	Default >> Unknown_Compliance	LIMITED_ACCESS	

1. Autenticação inicial. Para esta etapa, você pode estar interessado na validação do perfil de autorização que foi aplicado. Se um perfil de autorização inesperado tiver sido aplicado, investigue o relatório de autenticação detalhado. Você pode abrir este relatório clicando na lente de aumento na coluna Detalhes. Você pode comparar atributos no relatório de autenticação detalhado com a condição na política de autorização que espera corresponder.
2. Alteração de dados de sessão, neste exemplo específico, o estado de sessão mudou de Não Aplicável para Compatível.
3. COA para o dispositivo de acesso à rede. Este COA deve ser bem-sucedido ao enviar nova autenticação do lado do NAD e nova atribuição de política de autorização no lado do ISE. Se o COA falhou, você pode abrir um relatório detalhado para investigar o motivo. Os problemas mais comuns com o COA podem ser: Limite de tempo do COA - nesse caso, o PSN que enviou a solicitação não está configurado como um cliente COA no lado do NAD ou a solicitação do COA foi removida em algum lugar no caminho. COA negativo ACK - indica que o COA foi recebido pelo NAD, mas devido a algum motivo a operação do COA não pode ser confirmada. Para esse cenário, o relatório detalhado deve conter uma explicação mais detalhada.

Como o roteador baseado em IOS XE foi usado como NAD para este exemplo, você não pode ver nenhuma solicitação de autenticação subsequente para o usuário. Isso acontece porque o ISE usa o envio de COA para o IOS XE, o que evita a interrupção do serviço VPN. Nesse cenário, o próprio COA contém novos parâmetros de autorização, portanto, a reautenticação não é necessária.

Etapa 3. Verificação do relatório de postura - Navegue para **Operações -> Relatórios -> Relatórios -> Endpoint e Usuários -> Avaliação de postura por endpoint.**

The screenshot shows the Cisco ISE interface with the 'Posture Assessment by Endpoint' report. The report is filtered for 'Today' and shows a list of posture assessment events. The table below represents the data visible in the screenshot.

Logged At	Status	Details	PRA Action	Identity	Endpoint ID	IP Address
2018-06-07 19:39:59.345			N/A	vpuser	50.00.00.03.00.00	10.20.30.112
2018-06-07 19:38:14.053			N/A	vpn	50.00.00.03.00.00	10.20.30.111
2018-06-07 19:35:03.172			N/A	vpuser	50.00.00.03.00.00	10.20.30.110
2018-06-07 19:29:38.761			N/A	vpn	50.00.00.03.00.00	10.20.30.109
2018-06-07 19:26:52.657			N/A	vpuser	50.00.00.03.00.00	10.20.30.108
2018-06-07 19:17:17.906			N/A	vpuser	50.00.00.03.00.00	10.20.30.107

Você pode abrir um relatório detalhado aqui para cada evento específico para verificar, por exemplo, a ID da sessão a qual esse relatório pertence, quais requisitos de postura exatos foram selecionados pelo ISE para o endpoint e o status de cada requisito.

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

1. Depurações IKEv2 a serem coletadas do headend:

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

2. As depurações AAA para ver a atribuição de atributos locais e/ou remotos:

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

3. DART do cliente AnyConnect.

4. Para a solução de problemas de processos de postura, esses componentes do ISE devem ser ativados na depuração nos nós do ISE onde o processo de postura pode ocorrer: **client-webapp** - componente responsável pelo provisionamento do agente. Arquivos de log de destino **guest.log** e **ise-psc.log.convidado** - componente responsável pela pesquisa do componente do portal de provisionamento do cliente e do proprietário da sessão (quando a solicitação chega ao PSN errado). Arquivo de log de destino - **guest.log.provisionamento** - **componente responsável pelo processamento da política de provisionamento do cliente.** Arquivo de log de destino - **guest.log.postura** - todos os eventos relacionados à postura. Arquivo de log de destino - **ise-psc.log**
5. Para a solução de problemas do lado do cliente, você pode usar: **AnyConnect.txt** - Esse arquivo pode ser encontrado no pacote DART e usado para a solução de problemas de VPN. **acisensa.log** - Em caso de falha no provisionamento do cliente no lado do cliente, esse arquivo é criado na mesma pasta para a qual o NSA foi baixado (o diretório Downloads para Windows normalmente), **AnyConnect_ISEPosture.txt** - Este arquivo pode ser encontrado no pacote DART no diretório **Cisco AnyConnect ISE Posture Module**. Todas as informações sobre a descoberta de PSN do ISE e as etapas gerais do fluxo de postura são registradas neste arquivo.