

# Konfigurieren des ISE-Status mit FlexVPN

## Inhalt

- [Einführung](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Hintergrundinformationen](#)
- [Konfigurieren](#)
- [Netzwerkdigramm](#)
- [DNS-Serverkonfiguration](#)
- [Erstkonfiguration von IOS XE](#)
- [Identitätszertifikat konfigurieren](#)
- [Konfigurieren von IKEv2](#)
- [Konfiguration des AnyConnect-Clientprofils](#)
- [ISE-Konfiguration](#)
- [Konfiguration von Admin- und CPP-Zertifikaten](#)
- [Lokalen Benutzer auf der ISE erstellen](#)
- [Fügen Sie den FlexVPN-HUB als Radius-Client hinzu.](#)
- [Konfiguration der Client-Bereitstellung](#)
- [Statusrichtlinien und -bedingungen](#)
- [Konfigurieren des Client Provisioning Portals](#)
- [Konfigurieren von Autorisierungsprofilen und -richtlinien](#)
- [Überprüfen](#)
- [Fehlerbehebung](#)

## Einführung

Dieses Dokument enthält ein Beispiel für die Konfiguration eines IOS XE-Headends für den Remote-Zugriff mit Status mithilfe der Authentifizierungsmethode AnyConnect IKEv2 und EAP-Message Digest 5 (EAP-MD5).

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- FlexVPN Remote Access (RA)-VPN-Konfiguration auf IOS XE
- Client-Konfiguration für AnyConnect (AC)
- Statusfluss auf Identity Service Engine (ISE) 2.2 und höher
- Konfiguration von Statuskomponenten auf der ISE
- Konfiguration des DNS-Servers auf Windows Server 2008 R2

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco CSR1000V mit IOS XE 16.8 [Fujii]
- AnyConnect Client Version 4.5.03040 unter Windows 7
- Cisco ISE 2.3
- Windows 2008 R2 Server

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

Um sicherzustellen, dass die festgelegten Netzwerksicherheitsmaßnahmen relevant und effektiv bleiben, können Sie mit der Cisco ISE Sicherheitsfunktionen auf allen Client-Systemen validieren und aufrechterhalten, die auf das geschützte Netzwerk zugreifen. Durch die Verwendung von Statusrichtlinien, die sicherstellen sollen, dass die aktuellsten Sicherheitseinstellungen oder -anwendungen auf Client-Systemen verfügbar sind, kann der Cisco ISE-Administrator sicherstellen, dass alle Clientsysteme, die auf das Netzwerk zugreifen, die definierten Sicherheitsstandards für den Netzwerkzugriff der Enterprise-Klasse erfüllen und auch weiterhin erfüllen. Statusberichte liefern der Cisco ISE eine Momentaufnahme der Compliance-Stufe des Client-Systems bei der Benutzeranmeldung sowie jedes Mal, wenn eine regelmäßige Neubewertung erfolgt.

Status kann durch drei Hauptelemente dargestellt werden:

1. ISE als Distribution und Entscheidungspunkt für die Richtlinienkonfiguration In Bezug auf die ISE konfigurieren Sie Statusrichtlinien (welche genauen Bedingungen müssen erfüllt sein, um das Gerät als ein unternehmenstaugliches Gerät zu kennzeichnen), Client-Bereitstellungsrichtlinien (welche Agent-Software sollte auf welchen Geräten installiert werden) und Autorisierungsrichtlinien (welche Berechtigungen zugewiesen werden sollten, hängt von deren Status ab).
2. Network Access Device (NAD) als Richtliniendurchsetzungspunkt Auf der NAD-Seite werden zum Zeitpunkt der Benutzerauthentifizierung tatsächliche Autorisierungsbeschränkungen angewendet. Die ISE als Richtlinienpunkt stellt Autorisierungsparameter wie Zugriffskontrolllisten (ACLs) bereit. In der Regel müssen NADs, um Statusüberprüfungen zu ermöglichen, die den Change of Authorization (CoA) unterstützen, um den Benutzer nach Festlegung des Status des Endpunkts erneut zu authentifizieren. Ab ISE 2.2 müssen keine NADs mehr die Umleitung unterstützen.  
**Hinweis:** Router mit IOS XE unterstützen keine Umleitung.**Hinweis:** Die IOS XE-Software muss Fehlerbehebungen für folgende Fehler enthalten, damit CoA mit ISE voll funktionsfähig ist:  
[CSCve16269](#) IKEv2 CoA funktioniert nicht mit ISE  
[CSCvi90729](#) IKEv2 CoA funktioniert nicht mit ISE (Co-Push=TRUE statt true)
3. Agent-Software als Punkt der Datenerfassung und Interaktion mit Endbenutzern. Der Agent

erhält Informationen über Statusanforderungen von der ISE und übermittelt der ISE einen Bericht über den Anforderungsstatus. Dieses Dokument basiert auf dem AnyConnect ISE-Posture-Modul. Es ist das einzige Modul, das die Statusüberprüfung ohne Umleitung vollständig unterstützt.

Statusfluss ohne Umleitung ist im Artikel "[ISE Posture Style Comparison for Pre and Post 2.2](#)", Abschnitt "Posture Flow in ISE 2.2", sehr gut dokumentiert.

AnyConnect ISE Posture Module-Bereitstellung mit FlexVPN kann auf zwei verschiedene Arten erfolgen:

- Manual (Manuell) - Das Modul wird manuell auf der Workstation des Clients über das im Cisco Software Download Portal verfügbare AnyConnect-Paket installiert:  
<https://software.cisco.com/download/home/283000185>.

Für Statusaufgaben müssen die folgenden Bedingungen bei der manuellen ISE Posture Module-Bereitstellung erfüllt werden:

1. Domain Name Server (DNS) muss die IPs der Policy Service Nodes (PSNs) **enroll.cisco.com** auflösen. Beim ersten Verbindungsversuch verfügt das Statusmodul über keine Informationen zu verfügbaren PSNs. Es sendet Discovery-Tests, um verfügbare PSNs zu ermitteln. In einer dieser Probes wird FQDN enroll.cisco.com verwendet.
2. **Der TCP-Port 8905** muss für PSNs-IPs zulässig sein. Der Status wird in diesem Szenario über den TCP-Port 8905 übertragen.
3. **Das Admin-Zertifikat** auf den PSN-Knoten muss im **SAN-Feld enroll.cisco.com aufweisen**. Die Verbindung zwischen dem VPN-Benutzer und dem PSN-Knoten über TCP 8905 ist über das Admin-Zertifikat geschützt, und der Benutzer erhält eine Zertifikatwarnung, wenn der Name "enroll.cisco.com" im Admin-Zertifikat des PSN-Knotens nicht vorhanden ist.

**Hinweis:** Gemäß [RFC6125](#)-Zertifikat sollten CNs ignoriert werden, wenn SAN-Werte angegeben werden. Das bedeutet, dass auch im SAN-Feld CNs des Admin-Zertifikats hinzugefügt werden müssen.

- Automatische Bereitstellung über das Client Provisioning Portal (CPP) - das Modul wird heruntergeladen und von der ISE installiert, indem es direkt über das Portal FQDN auf CPP zugreift.

Die folgenden Bedingungen müssen bei Statusarbeit mit der automatischen ISE-Statusmodul-Bereitstellung erfüllt sein:

1. DNS muss **FQDN von CPP-zu-Policy Service Nodes (PSNs)-IPs** auflösen.
2. **Die TCP-Ports 80, 443 und der CPP-Port (standardmäßig 8443)** müssen für PSNs IPs zulässig sein. Der Client muss CPP FQDN direkt über HTTP (wird an HTTPS umgeleitet) oder HTTPS öffnen. Diese Anforderung wird an den CPP-Port (standardmäßig 8443) umgeleitet, und der Status wird über diesen Port übertragen.
3. **Admin- und CPP-Zertifikate** auf den PSN-Knoten müssen **CPP FQDN im SAN-Feld** aufweisen. Die Verbindung zwischen dem VPN-Benutzer und dem PSN-Knoten über TCP 443 ist durch das Admin-Zertifikat geschützt, und die Verbindung am CPP-Port ist durch das CPP-Zertifikat geschützt.

**Hinweis:** Gemäß [RFC6125](#)-Zertifikat sollten CNs ignoriert werden, wenn SAN-Werte angegeben werden. Im SAN-Feld der entsprechenden Zertifikate müssen außerdem CNs von Admin- und CPP-Zertifikaten hinzugefügt werden.

**Hinweis:** Wenn die ISE-Software keine Reparatur für [CSCvj76466](#) enthält, funktioniert die Statusbereitstellung oder Client-Bereitstellung nur, wenn die Bereitstellung auf demselben PSN erfolgt ist, auf dem der Client authentifiziert wurde.

Bei einer Statusüberprüfung mit FlexVPN umfasst der Datenfluss folgende Schritte:

1. Benutzer stellt über den AnyConnect-Client eine Verbindung zum FlexVPN-Hub her.
2. Die ISE sendet Access-Accept an den FlexVPN-Hub, wobei der Name der ACL zur Einschränkung des Zugriffs verwendet werden muss.
- 3a) Erste Verbindung mit manueller Bereitstellung - ISE-Statusmodul erkennt Richtlinienserver, der die Anfrage an [enroll.cisco.com](#) über TCP-Port 8905 sendet. Als Ergebnis lädt das Statusmodul konfigurierte Statusprofile herunter und aktualisiert Compliance-Modul auf Client-Seite.

Bei den nächsten Verbindungsversuchen verwendet das ISE-Statusmodul außerdem die in der Call Home List des Statusprofils angegebenen Namen und IPs für die Richtlinienservererkennung.

3b) Erste Verbindung mit automatischer Bereitstellung - Der Client öffnet CPP über FQDN. Als erfolgreiches Ergebnis wird der Network Setup Assistant auf die Workstation des Clients heruntergeladen und anschließend das ISE Posture-Modul, das ISE Compliance-Modul und das Statusprofil heruntergeladen und installiert.

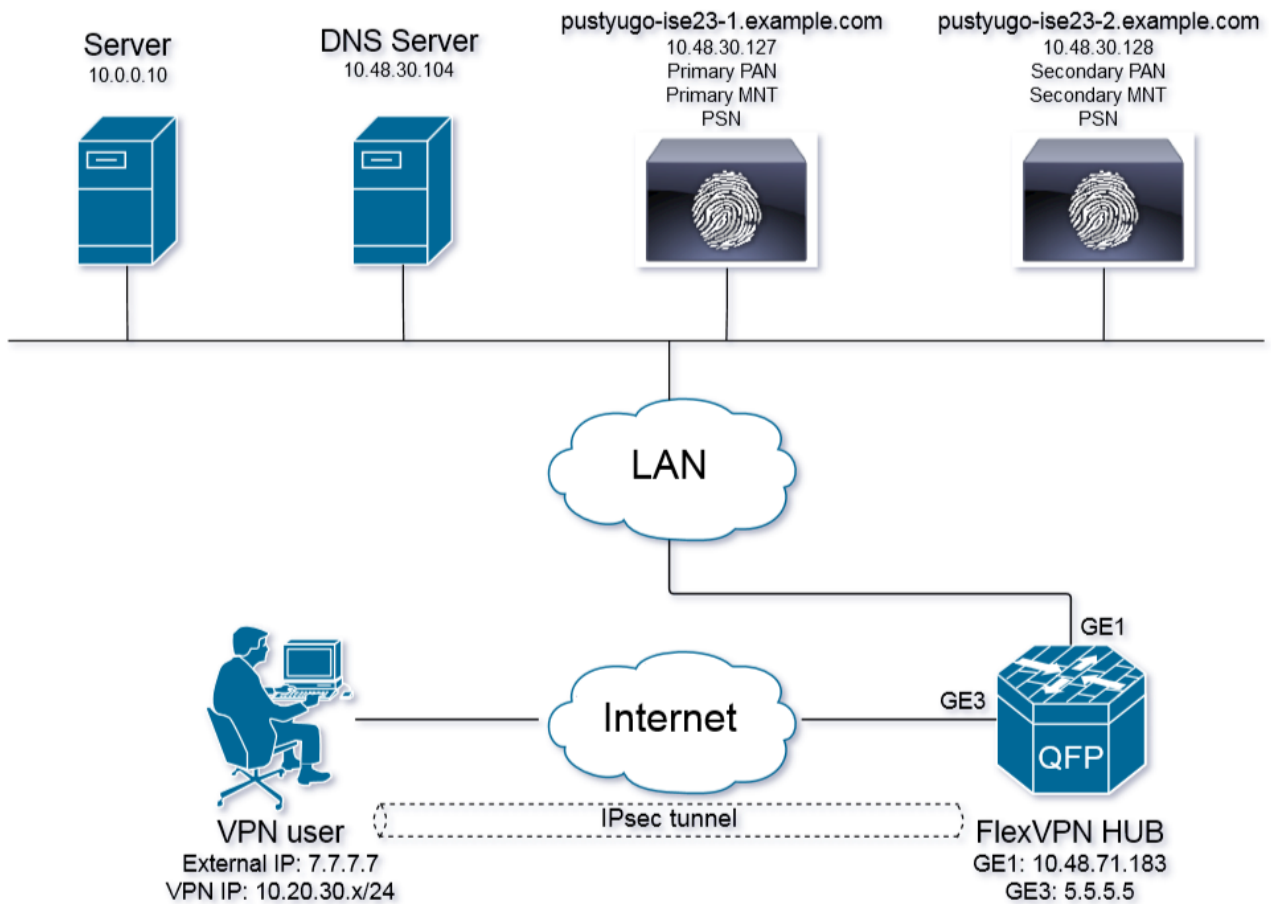
Bei den nächsten Verbindungsversuchen verwendet das ISE-Statusmodul die in der Call Home List des Statusprofils angegebenen Namen und IPs für die Richtlinienservererkennung.

4. Statusmodul startet Compliance-Prüfungen und sendet die Prüfergebnisse an die ISE.
5. Wenn der Client-Status konform ist, sendet die ISE Access-Accept an den FlexVPN-Hub, wobei der Name der ACL für den kompatiblen Client angewendet werden muss.
6. Der Client erhält Zugriff auf das Netzwerk.

Weitere Details zum Status-Prozess finden Sie im Dokument "[ISE Posture Style Comparison for Pre and Post 2.2](#)".

## Konfigurieren

### Netzwerkdiagramm

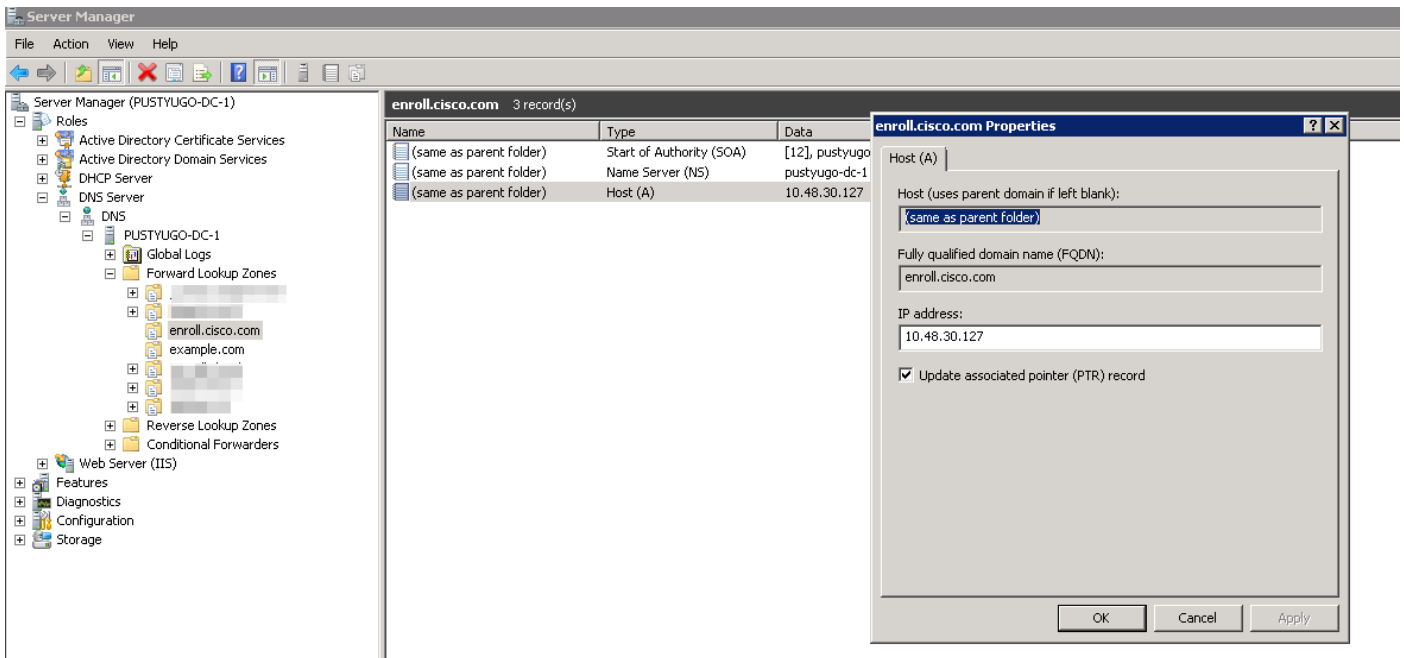


VPN-Benutzer erhalten nur dann Zugriff auf den Server (10.0.0.10), wenn er über einen konformen Status verfügt.

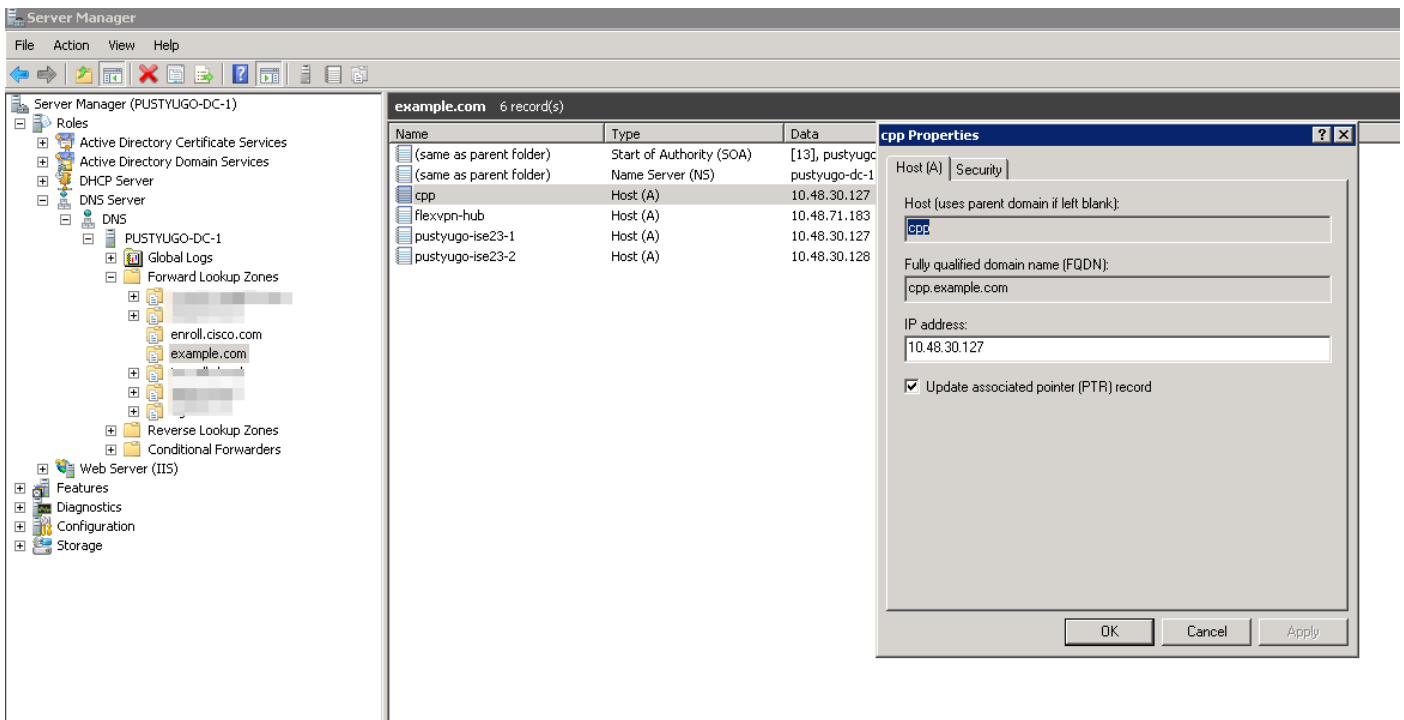
## DNS-Serverkonfiguration

In diesem Dokument wird Windows Server 2008 R2 als DNS-Server verwendet.

Schritt 1: Fügen Sie einen **Host (A)**-Datensatz für **enroll.cisco.com** hinzu, der auf die IP-Adresse des **PSN** verweist:



Schritt 2: Hinzufügen eines **Host (A)**-Datensatzes für CPP FQDN (in diesem Beispiel verwendet **cpp.example.com**), der auf die **IP-Adresse** von PSN verweist:



## Erstkonfiguration von IOS XE

### Identitätszertifikat konfigurieren

Der Router verwendet das Zertifikat, um sich beim AnyConnect-Client zu authentifizieren. Das Router-Zertifikat sollte vom Betriebssystem des Benutzers als vertrauenswürdig eingestuft werden, um während der Verbindungsphase eine Zertifikatwarnung zu vermeiden.

Das Identitätszertifikat kann auf eine der folgenden Arten bereitgestellt werden:

**Hinweis:** Die Verwendung selbstsignierter Zertifikate wird von IKEv2 FlexVPN nicht

unterstützt.

## Option 1: Konfigurieren des Zertifizierungsstellen-Servers (CA) auf dem Router

**Hinweis:** CA-Server können auf demselben IOS-Router oder einem anderen Router erstellt werden. In diesem Artikel wird CA auf demselben Router erstellt.

**Hinweis:** Sie müssen die Zeit mit dem NTP-Server synchronisieren, bevor der CA-Server aktiviert werden kann.

**Hinweis:** Bitte beachten Sie, dass der Benutzer die Authentizität dieses Zertifikats nicht überprüfen kann. Daher werden die Benutzerdaten nicht vor Man-in-the-Middle-Angriffen geschützt, es sei denn, das Zertifizierungsstellen-Zertifikat wird manuell überprüft und vor dem Herstellen der Verbindung in den Computer des Benutzers importiert.

### Schritt 1: Generieren Sie RSA-Schlüssel für den CA-Server:

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

### Schritt 2: RSA-Schlüssel für Identitätszertifikat erstellen:

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

### Überprüfung:

```
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
```

### Schritt 3: Konfigurieren der CA:

```
ip http server
```

```
crypto pki server ROOT-CA
```

```
issuer-name cn=ROOT-CA.example.com
```

```
hash sha256
```

```
lifetime certificate 1095
lifetime ca-certificate 3650
eku server-auth
no shutdown
```

## Überprüfung:

```
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
```

## Schritt 4: Konfigurieren Sie den Trustpoint:

```
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
```

## Schritt 5: Authentifizierung der CA:

```
FlexVPN-HUB(config)#crypto pki authenticate FLEX-TP-1
Certificate has the following attributes:
  Fingerprint MD5: A5522AAB 1410E645 667F0D70 49AADA45
  Fingerprint SHA1: F52EAB1A D39642E7 D8EAB804 0EB30973 7647A860
```

```
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

## Schritt 6: Registrieren Sie den Router für die 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
```

**Überprüfen Sie ausstehende Zertifikatsanfragen der CA, und überprüfen Sie, ob der Fingerabdruck übereinstimmt:**

```
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
```

**Schritt 7: Gewähren Sie das Zertifikat mithilfe der richtigen ReqID:**

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

**Warten Sie, bis der Router das Zertifikat erneut anfordert (entsprechend dieser Konfiguration wird es 10 Mal pro Minute überprüft). Syslog-Meldung suchen:**

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

**Überprüfen Sie, ob das Zertifikat installiert ist:**

```
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 - Extern signiertes Zertifikat importieren

```
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)#
```

## Konfigurieren von IKEv2

### Schritt 1: Konfigurieren des RADIUS-Servers und des 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
```

### Schritt 2: Authentifizierungs- und Autorisierungslisten konfigurieren:

```
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
```

### Schritt 3: Erstellen einer IKV2-Autorisierungsrichtlinie:

```
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
```

#### Schritt 4: IKEv2-Profil erstellen:

```
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
```

#### Schritt 5: Transformationssatz und IPSec-Profil erstellen:

```
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
```

#### Schritt 6: Virtuelle Vorlagenschnittstelle erstellen:

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

#### Schritt 7: Lokalen Pool erstellen:

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

#### Schritt 8: Erstellen Sie eine ACL, um den Zugriff für nicht konforme Clients zu beschränken.

Während unbekannter Statuszustände sollten mindestens folgende Berechtigungen erteilt werden:

- DNS-Datenverkehr
- Datenverkehr zu ISE-PSNs über die Ports 80, 443 und 8905
- Datenverkehr zu ISE-PSNs, auf die das CPP-Portal FQDN hinweist
- Datenverkehr zu Sanierungsservern bei Bedarf

Dies ist ein Beispiel für eine Zugriffskontrollliste ohne Wiederherstellungsserver. Das explizite Ablehnen für das Netzwerk 10.0.0.0/24 wird hinzugefügt, um die Transparenz zu gewährleisten. Das Ende der Zugriffskontrollliste beinhaltet implizit "deny ip any any any":

```
ip access-list extended DENY_SERVER
permit udp any any eq domain
permit tcp any host 10.48.30.127 eq 80
permit tcp any host 10.48.30.127 eq 443
permit tcp any host 10.48.30.127 eq 8443
permit tcp any host 10.48.30.127 eq 8905
permit tcp any host 10.48.30.128 eq 80
permit tcp any host 10.48.30.128 eq 443
```

```
permit tcp any host 10.48.30.128 eq 8443
permit tcp any host 10.48.30.128 eq 8905
deny ip any 10.0.0.0 0.0.0.255
```

Schritt 9: Erstellen Sie eine ACL, um den Zugriff für kompatible Clients zuzulassen:

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

Schritt 10: Split Tunnel Configuration (optional)

Standardmäßig wird der gesamte Datenverkehr über VPN weitergeleitet. Um Datenverkehr nur an die angegebenen Netzwerke weiterzuleiten, können Sie diese im Abschnitt "ikev2-Autorisierungsrichtlinie" angeben. Es ist möglich, mehrere Anweisungen hinzuzufügen oder Standardzugriffslisten zu verwenden.

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

Schritt 11: Internetzugang für Remote-Clients (optional)

Damit die ausgehenden Verbindungen von den Clients für den Remote-Zugriff zu den Hosts im Internet NAT-ed an die globale IP-Adresse des Routers gesendet werden, konfigurieren Sie die NAT-Übersetzung:

```
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

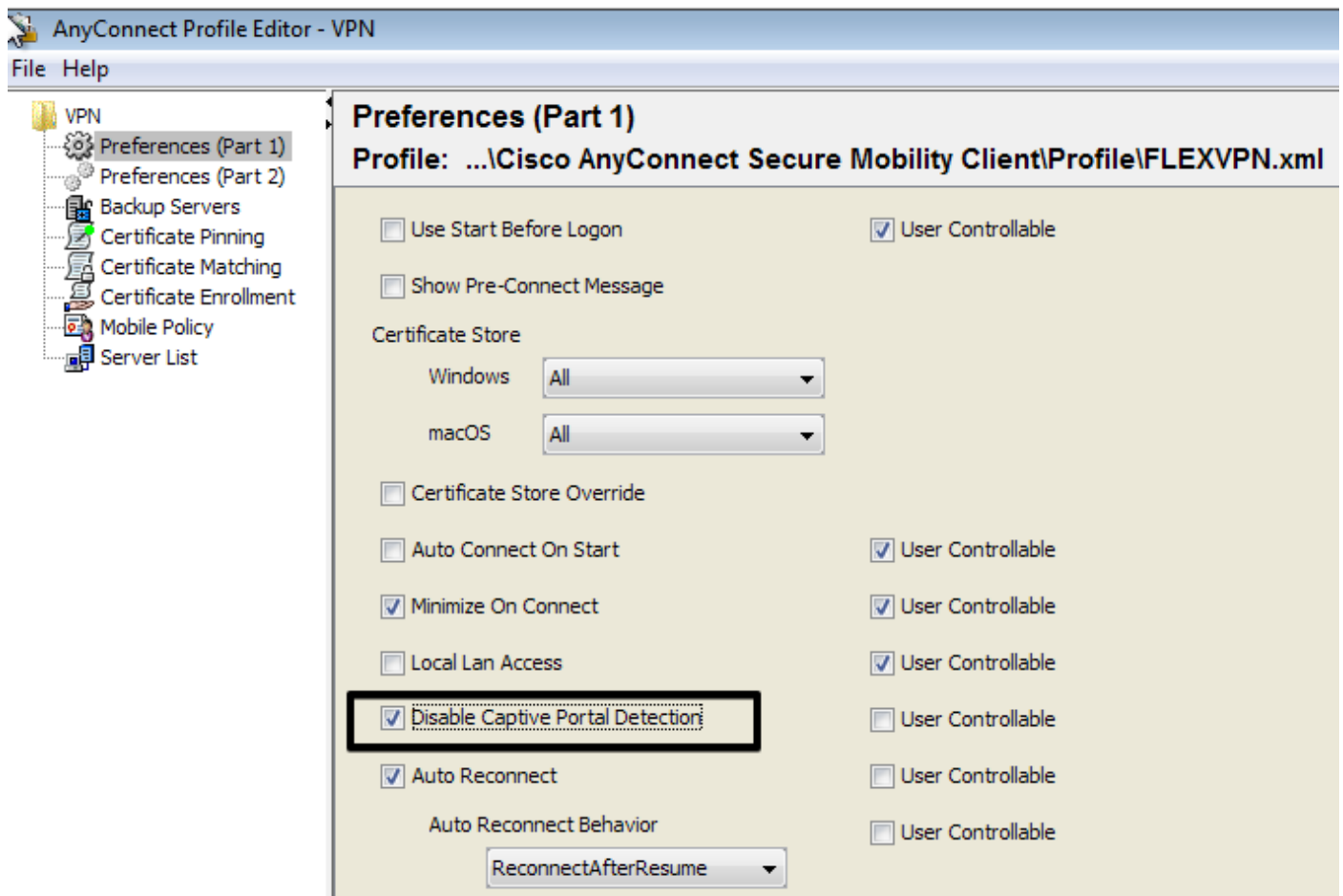
interface GigabitEthernet1
 ip nat outside

interface Virtual-Template 10
 ip nat inside
```

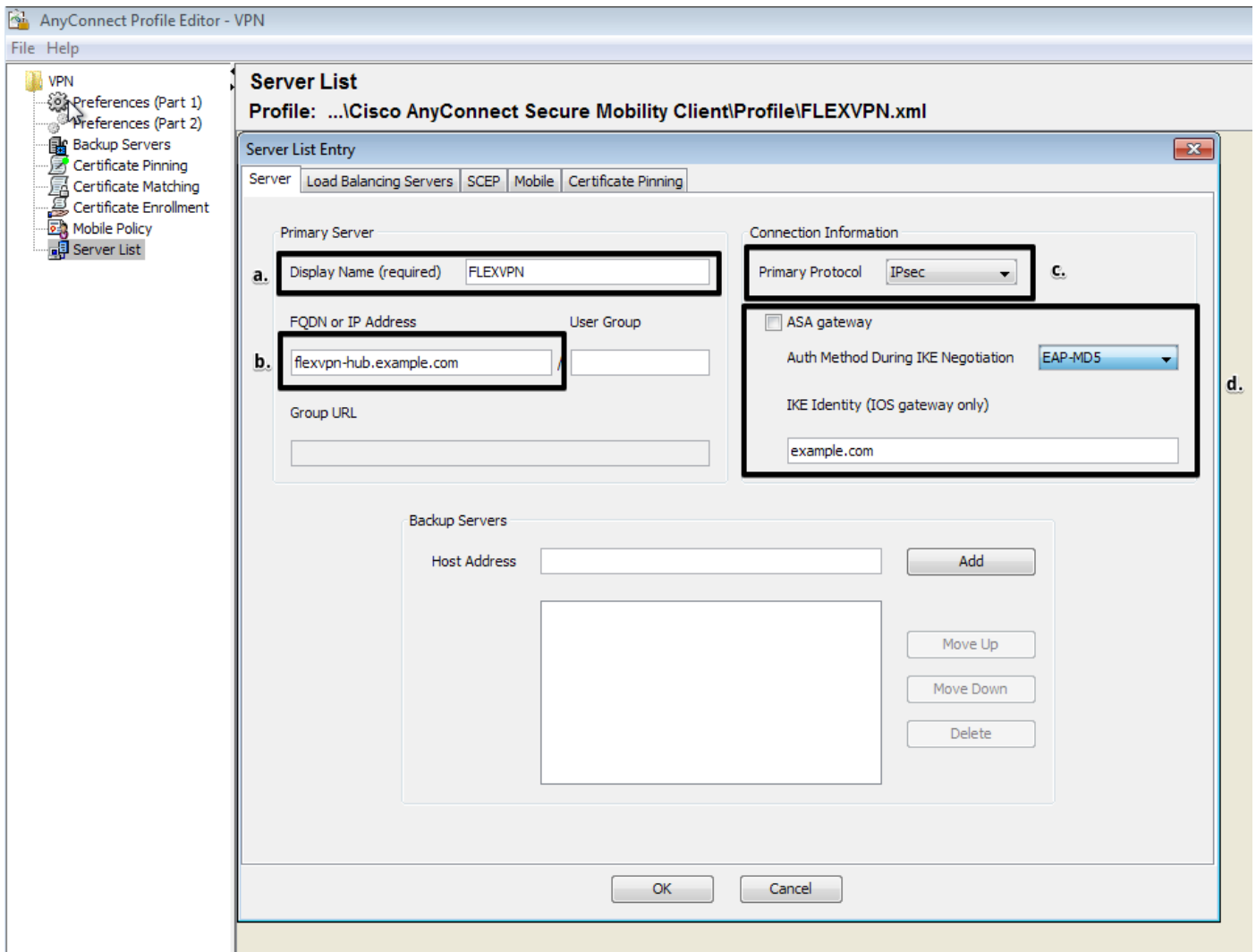
## Konfiguration des AnyConnect-Clientprofils

Konfigurieren Sie das Clientprofil mit dem AnyConnect Profile Editor. Profile von AnyConnect Security Mobile Client unter Windows 7 und 10 werden in **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile** gespeichert.

Schritt 1: Deaktivieren der Funktion zur Erkennung von Captive Portals. Wenn der HTTP-Server auf dem FlexVPN Hub nicht deaktiviert ist, führt die Funktion zur Erkennung des Captive Portals bei AnyConnect zum Ausfall der Verbindung. Beachten Sie, dass der CA-Server ohne HTTP-Server nicht funktioniert.



Schritt 2: Serverliste konfigurieren:



- Geben Sie den Anzeigenamen ein.
- Geben Sie **FQDN** oder **IP-Adresse** des FlexVPN-Hub ein.
- Wählen Sie **IPsec** als Primärprotokoll aus.
- Deaktivieren Sie das Kontrollkästchen "ASA Gateway", und geben Sie **EAP-MD5** als Authentifizierungsmethode an. Geben Sie die IKE-Identität genau wie in der Konfiguration des IKEv2-Profiles auf dem FlexVPN Hub ein (in diesem Beispiel wird das IKEv2-Profil mit dem Befehl "match identity remote key-id example.com" konfiguriert. Daher müssen wir **example.com** als IKE Identity verwenden.)

Schritt 3: Speichern Sie das Profil auf **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile**, und starten Sie das Netzkabel neu.

Die XML-Entsprechung des Profils:

```
<?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>
  </ClientInitialization>
</AnyConnectProfile>
```

```

<CertificateStore>All</CertificateStore>
<CertificateStoreMac>All</CertificateStoreMac>
<CertificateStoreOverride>>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>>false</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">>false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">>true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">>false</LocalLanAccess>
<DisableCaptivePortalDetection
UserControllable="false">>true</DisableCaptivePortalDetection>
<ClearSmartcardPin UserControllable="true">>false</ClearSmartcardPin>
<IPProtocolSupport>IPv4, IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">>true
  <AutoReconnectBehavior
UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
  </AutoReconnect>
<AutoUpdate UserControllable="false">>true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>>false</AutomaticVPNPolicy>
<PPPEXclusion UserControllable="false">Automatic
  <PPPEXclusionServerIP UserControllable="false"></PPPEXclusionServerIP>
</PPPEXclusion>
<EnableScripting UserControllable="false">>false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="true">>false
  <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
  <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>>false
</RetainVpnOnLogoff>
<AllowManualHostInput>>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
  <HostEntry>
    <HostName>FLEXVPN</HostName>
    <HostAddress>flexvpn-hub.example.com</HostAddress>
    <PrimaryProtocol>IPsec
      <StandardAuthenticationOnly>>true
        <AuthMethodDuringIKENegotiation>EAP-MD5</AuthMethodDuringIKENegotiation>
        <IKEIdentity>example.com</IKEIdentity>
      </StandardAuthenticationOnly>
    </PrimaryProtocol>
  </HostEntry>
</ServerList>
</AnyConnectProfile>

```

## ISE-Konfiguration

### Konfiguration von Admin- und CPP-Zertifikaten

**Hinweis:** Beim Ändern des Admin-Zertifikats wird der Knoten neu gestartet, auf dem das Zertifikat geändert wurde.

Schritt 1: Gehen Sie zu **Administration -> System -> Certificates -> Certificate Signing Requests**, und klicken Sie auf **Generate Certificate Signing Requests (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					

Schritt 2: Wählen Sie auf der geöffneten Seite den erforderlichen PSN-Knoten aus, füllen Sie die erforderlichen Felder aus, und fügen Sie FQDN des Knotens, enroll.cisco.com, cpp.example.com und die IP-Adresse des Knotens in SAN-Feldern hinzu, und klicken Sie auf **Generieren**:

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

**Hinweis:** Wenn Sie in diesem Schritt **Multi-Use** auswählen, können Sie auch dasselbe Zertifikat für Portal verwenden.

Klicken Sie im erschienenen Fenster auf **Exportieren**, um die CSR im Paketformat auf der lokalen Workstation zu speichern:



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



Schritt 3: Senden Sie den CSR mit einer vertrauenswürdigen CA, und erhalten Sie die Zertifikatsdatei von der Zertifizierungsstelle sowie die vollständige Kette von Zertifizierungsstellenzertifikaten (Root und Intermediate).

Schritt 4: Gehen Sie zu **Administration** ->System -> Certificates -> Trusted Certificates, und klicken Sie auf **Import**. Klicken Sie auf dem nächsten Bildschirm auf **Datei auswählen** und wählen Sie **Stammzertifizierungsdatei** aus, füllen Sie ggf. Freundlichen Namen und Beschreibung aus, wählen Sie die erforderlichen **Trusted For**-Optionen aus, und klicken Sie auf **Senden**:

Wiederholen Sie diesen Schritt für alle Zwischenzertifikate in der Kette, sofern vorhanden.

Schritt 5: Zurück zu **Administration -> System -> Certificates -> Certificate Signing Requests**, wählen Sie die erforderliche CSR aus und klicken Sie auf **Bind Certificate**:

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

Schritt 6: Klicken Sie auf der geöffneten Seite auf **Choose File (Datei auswählen)**, wählen Sie die Zertifikatsdatei aus, die Sie von der CA erhalten haben, und geben Sie ggf. Friendly Name (Angezeigter Name) ein. Wählen Sie dann **Usage (Nutzung): Administrator (Verwendung: Das Portal kann auch hier ausgewählt werden, wenn der CSR mit Multi-Use erstellt wurde)**, und klicken Sie auf **Senden**:

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**

### Bind CA Signed Certificate

\* Certificate File  Signed CSR.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

Schritt 7: Klicken Sie im Popup-Warnmeldung auf **Ja**, um den Import abzuschließen. Der von der Änderung des Admin-Zertifikats betroffene Knoten wird neu gestartet:

Warning: 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

Wiederholen Sie die Schritte zum Ändern des CPP-Zertifikats, wenn Sie sich für die Verwendung eines separaten Zertifikats für das Portal entschieden haben. Wählen Sie in Schritt 6 **Verwendung aus: Portal** und klicken Sie auf **Senden**:

**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)

Wiederholen Sie die Schritte für alle PSNs in der ISE-Bereitstellung.

## Lokalen Benutzer auf der ISE erstellen

**Hinweis:** Bei der EAP-MD5-Methode werden nur lokale Benutzer von der ISE unterstützt.

Schritt 1: Gehen Sie zu **Administration -> Identity Management -> Identities -> Users**, und klicken Sie auf **Add**.

**Network Access Users**

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

Schritt 2: Geben Sie auf der geöffneten Seite Benutzernamen, Kennwort und andere erforderliche Informationen ein, und klicken Sie auf **Senden**.

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**

Fügen Sie den FlexVPN-HUB als Radius-Client hinzu.

Schritt 1: Gehen Sie zu **Work Centers -> Posture -> Network Devices**, und klicken Sie auf **Add**.

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					

Schritt 2: Geben Sie auf der geöffneten Seite Geräte name, IP-Adresse und andere erforderliche Informationen ein, aktivieren Sie das Kontrollkästchen "RADIUS Authentication settings" (RADIUS-Authentifizierungseinstellungen), geben Sie Shared Secret ein, und klicken Sie unten auf der Seite auf **Submit (Senden)**.



Network Devices List > **New Network Device**

### Network Devices

\* Name

Description

IP Address \* IP :  /

**i** 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  **i**

CoA Port

#### RADIUS DTLS Settings **i**

DTLS Required  **i**

Shared Secret  **i**

CoA Port

Issuer CA of ISE Certificates for CoA  **i**

DNS Name

#### General Settings

Enable KeyWrap  **i**

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

TACACS Authentication Settings

SNMP Settings

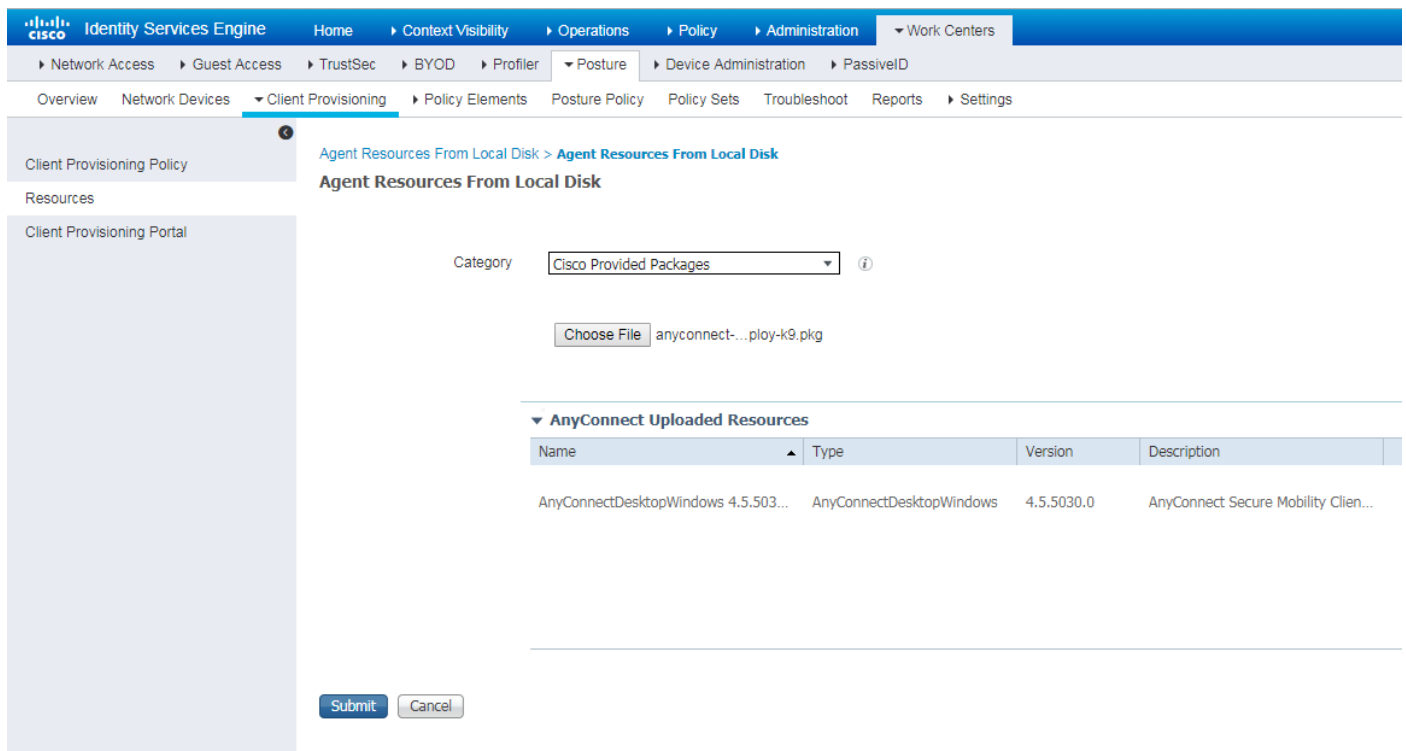
Advanced TrustSec Settings

## Konfiguration der Client-Bereitstellung

Dies sind die Schritte zur Vorbereitung der AnyConnect-Konfiguration.

Schritt 1: Download des AnyConnect-Pakets. AnyConnect-Paket selbst ist nicht zum direkten Download von der ISE verfügbar. Stellen Sie daher vor dem Start sicher, dass Wechselstrom auf Ihrem PC verfügbar ist. Dieser Link kann für den AC-Download verwendet werden - <http://cisco.com/go/anyconnect>. In diesem Dokument wird das Paket anyconnect-win-4.5.05030-webdeploy-k9.pkg verwendet.

Schritt 2: Um AC-Pakete in die ISE hochzuladen, navigieren Sie zu **Work Centers -> Posture -> Client Provisioning -> Resources**, und klicken Sie auf **Add**. Wählen Sie **Agent-Ressourcen von der lokalen Festplatte aus**. Wählen Sie im neuen Fenster **Cisco Provided Packages (Von Cisco bereitgestellte Pakete) aus**, klicken Sie auf **Choose File (Datei auswählen)** und wählen Sie AC Package (AC-Paket) auf Ihrem PC aus.



The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Posture > Device Administration > PassiveID > Client Provisioning > Policy Elements > Agent Resources From Local Disk. The main content area is titled "Agent Resources From Local Disk" and shows a form for adding a new resource. The "Category" dropdown is set to "Cisco Provided Packages". The "Choose File" button is active, and the file "anyconnect-...ploy-k9.pkg" is selected. Below the form, there is a table titled "AnyConnect Uploaded Resources" with the following data:

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

At the bottom of the form, there are "Submit" and "Cancel" buttons.

Klicken Sie auf **Senden**, um den Import abzuschließen. Überprüfen Sie den Hash des Pakets, und drücken Sie **Bestätigen**.

Schritt 3: Compliance-Modul muss in die ISE hochgeladen werden. Klicken Sie auf derselben Seite (**Work Center -> Posture -> Client Provisioning -> Resources**) auf **Add** (Hinzufügen), und wählen Sie **Agent-Ressourcen von der Cisco Website aus**. In der Ressourcenliste sollten Sie ein Compliance-Modul überprüfen und auf **Speichern** klicken. Für dieses Dokument AnyConnectComplianceModule verwendet das Compliance-Modul Windows 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

Schritt 4: Nun muss ein AC-Statusprofil erstellt werden. Klicken Sie auf **Hinzufügen**, und wählen Sie **NAC Agent** oder **AnyConnect-Statusprofil** aus.

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

- Wählen Sie den Profiltyp aus. In diesem Szenario sollte AnyConnect verwendet werden.
- Geben Sie den Profilnamen an. Navigieren Sie zum Profilbereich **Status Protocol** (Statusprotokoll).



## 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"/> <b>a.</b>	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.exempl"/> <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	<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

- Regeln für **Servernamen** angeben, darf dieses Feld nicht leer sein. Feld kann FQDN mit Platzhalter enthalten, wodurch die Verbindung des AC-Statusmoduls aus dem entsprechenden Namespace auf PSNs beschränkt wird. Stern Sie, wenn FQDN zulässig sein soll.
- Die hier angegebenen Namen und IP-Adressen werden in Phase 2 der Statuserkennung verwendet (siehe Schritt 14 im Abschnitt "[Posture Flow in ISE 2.2](#)"). Sie können Namen nach Koma aufteilen, und nach FQDN/IP können mit Doppelpunkt auch Portnummern hinzugefügt werden.

Schritt 5. Erstellen Sie eine AC-Konfiguration. Navigieren Sie zu **Work Centers -> Posture -> Client Provisioning -> Resources (Arbeitscenter)**, und klicken Sie auf **Add (Hinzufügen)**, und wählen Sie **AnyConnect Configuration (AnyConnect-Konfiguration)**.

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

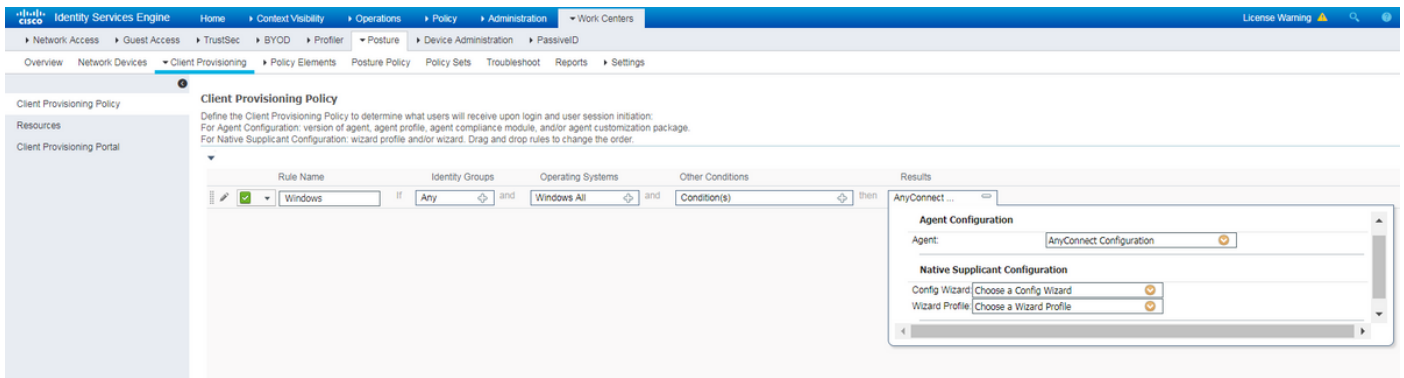
Umbrella Roaming Security

Customer Feedback

- Wählen Sie AC-Paket aus.
- Geben Sie den Namen der AC-Konfiguration an.
- Wählen Sie Compliance Module Version aus.
- Wählen Sie aus der Dropdown-Liste das AC-Status-Konfigurationsprofil aus.

Schritt 6: Konfigurieren der Client-Bereitstellungsrichtlinie Navigieren Sie zu **Work Centers -> Posture -> Client Provisioning (Arbeitscenter)**. Bei der Erstkonfiguration können Sie leere Werte in der Richtlinie ausfüllen, die mit Standardwerten versehen ist. Wenn Sie der vorhandenen Statuskonfiguration Richtlinien hinzufügen möchten, navigieren Sie zu der Richtlinie, die wiederverwendet werden kann, und wählen Sie **Oben Duplikat** oder **Unten Duplizieren** aus. Außerdem können neue Richtlinien erstellt werden.

Dies ist das Beispiel für die im Dokument verwendete Richtlinie.

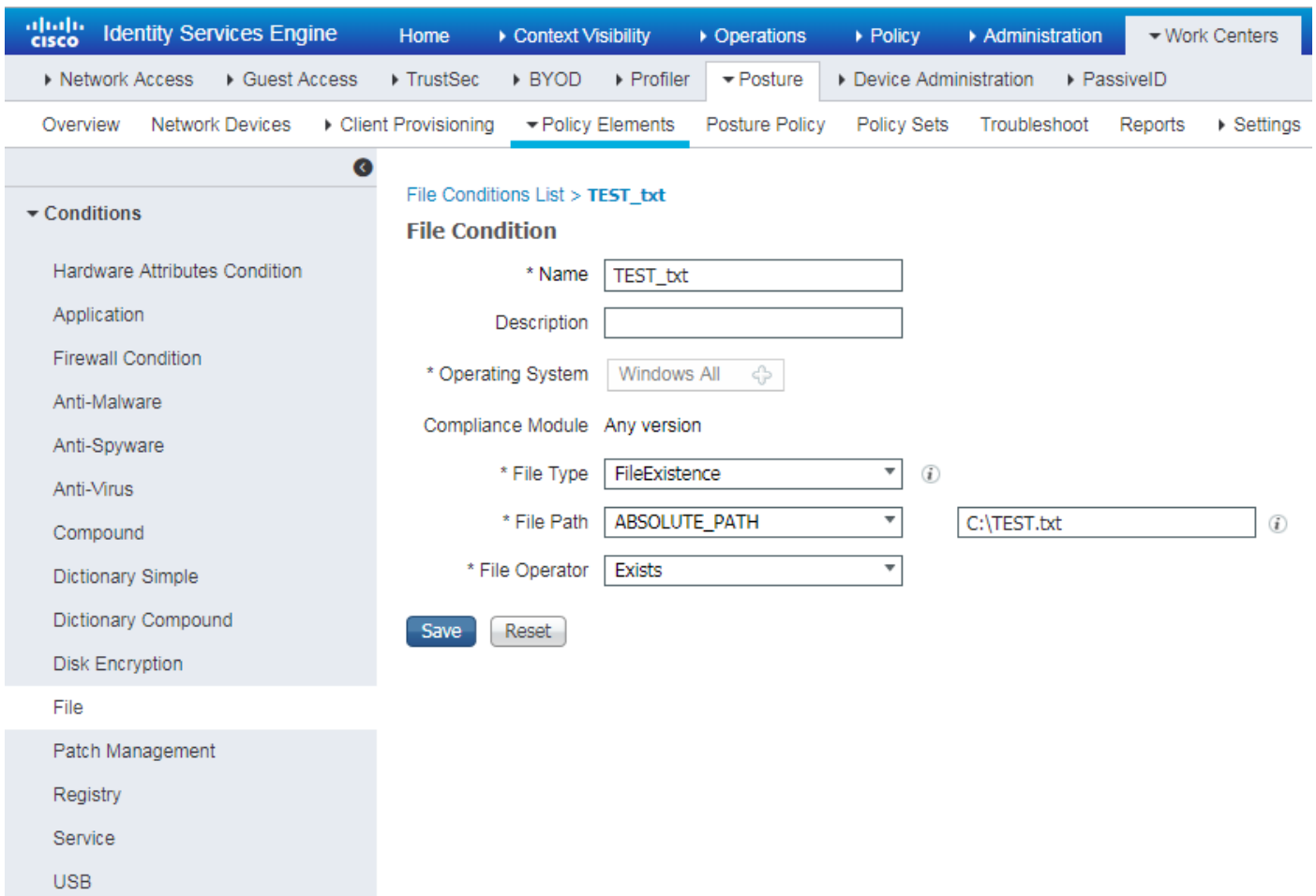


Wählen Sie Ihre AC-Konfiguration im Ergebnisbereich aus.

## Statusrichtlinien und -bedingungen

Es wird eine einfache Statusprüfung verwendet. Die ISE ist so konfiguriert, dass auf der Endgeräteseite geprüft wird, ob die Datei C:\TEST.txt vorhanden ist. Echte Szenarien können viel komplizierter sein, aber die allgemeinen Konfigurationsschritte sind dieselben.

Schritt 1: Erstellen Sie eine Statusbedingung. Die Statusbedingungen finden Sie in **Work Centers > Posture -> Policy Elements -> Conditions**. Wählen Sie den Status-Typ aus, und klicken Sie auf **Hinzufügen**. Geben Sie die erforderlichen Informationen an, und klicken Sie auf **Speichern**. Im Folgenden finden Sie ein Beispiel für eine Dienstbedingung, die überprüfen sollte, ob die Datei C:\TEST.txt vorhanden ist.

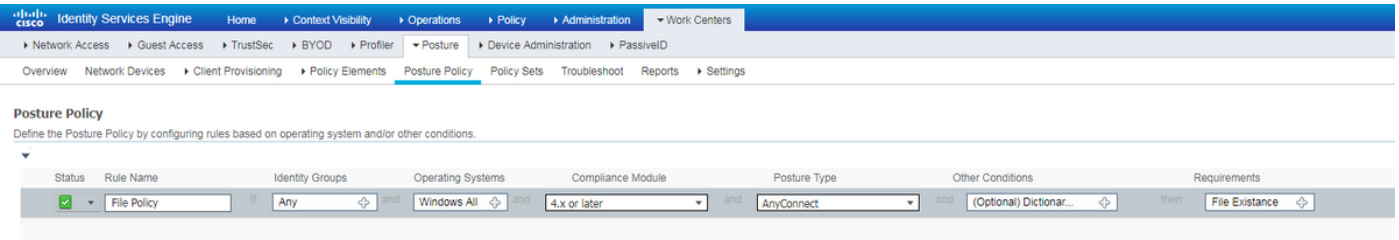


Schritt 2: Konfiguration der Statusanforderungen Navigieren Sie zu **Work Centers -> Posture -> Policy Elements -> Requirements**. Dies ist ein Beispiel für die TEST.txt-Datei:



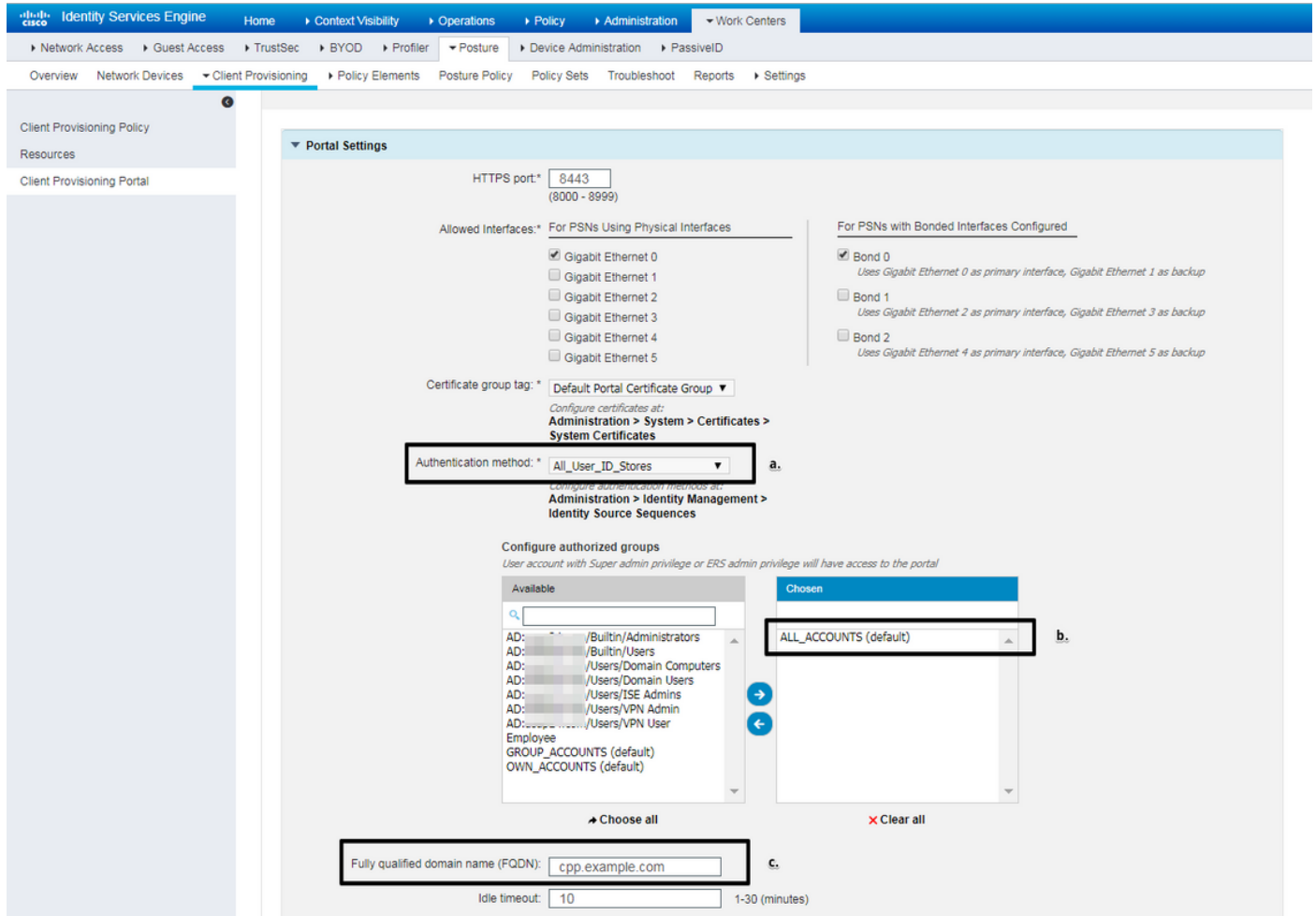
Wählen Sie in einer neuen Anforderung den Status aus, und geben Sie eine Behebungsmaßnahme an.

Schritt 3: Statusrichtlinienkonfiguration. Navigieren Sie zu **Work Centers -> Posture -> Posture Policy**. Unten sehen Sie ein Beispiel für eine Richtlinie, die für dieses Dokument verwendet wird. Für Richtlinien ist "File Existence"-Anforderung als obligatorisch zugewiesen, und es sind keine weiteren Bedingungen zugewiesen.



## Konfigurieren des Client Provisioning Portals

Für Statusüberprüfung ohne Umleitung muss die Konfiguration des Client-Bereitstellungsportals bearbeitet werden. Navigieren Sie zu **Work Centers -> Posture -> Client Provisioning -> Client Provisioning Portal**. Sie können entweder das Standardportal verwenden oder ein eigenes erstellen.



Diese Einstellungen sollten in der Portalkonfiguration für Szenarien ohne Umleitung bearbeitet werden:

- Geben Sie unter Authentication (Authentifizierung) die Identitätsquellensequenz an, die verwendet werden sollte, wenn SSO keine Sitzung für den Benutzer finden kann.
- Entsprechend der ausgewählten Identitätsquellensequenz wird die Liste der verfügbaren Gruppen ausgefüllt. An dieser Stelle müssen Sie Gruppen auswählen, die für die Portalanmeldung autorisiert sind.
- FQDN des Client Provisioning Portals muss angegeben werden. Dieser FQDN sollte auf ISE-PSNs IPs auflösbar sein. Benutzer sollten angewiesen werden, den FQDN im Webbrowser während des ersten Verbindungsversuchs anzugeben.

### Konfigurieren von Autorisierungsprofilen und -richtlinien

Der erstmalige Zugriff für den Client muss eingeschränkt werden, wenn kein Status verfügbar ist. Dies kann auf verschiedene Weise erfolgen:

- Radius-Filter-ID: Mit diesem Attribut kann die lokal in NAD definierte ACL dem Benutzer mit unbekanntem Status zugewiesen werden. Da es sich um ein Standard-RFC-Attribut handelt, sollte dieser Ansatz für alle NAD-Anbieter gut funktionieren.
- Cisco:cisco-av-pair = ip:interface-config - Ähnlich wie Radius Filter-Id kann die lokal auf NAD definierte ACL dem Benutzer mit unbekanntem Status zugewiesen werden.

Konfigurationsbeispiel:

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

Schritt 1: Konfigurieren Sie das Autorisierungsprofil.

Wie bei Status sind zwei Autorisierungsprofile erforderlich. Der erste sollte jegliche Art von Netzwerkzugriffsbeschränkungen enthalten. Dieses Profil kann auf Authentifizierungen angewendet werden, bei denen der Status nicht dem Compliance-Status entspricht. Das zweite Autorisierungsprofil kann nur Berechtigungen für den Zugriff enthalten und für Sitzungen mit Status-Status angewendet werden, die den Vorgaben entsprechen.

Um ein Autorisierungsprofil zu erstellen, navigieren Sie zu **Work Center -> Posture -> Policy Elements -> Authorization Profiles (Work Center -> Status -> Richtlinien-Elemente -> Autorisierungsprofile)**.

Beispiel für ein beschränktes Zugriffsprofil mit Radius-Filter-ID:

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

Beispiel für ein eingeschränktes Zugriffsprofil mit cisco-av-pair:

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

Beispiel für ein unbeschränktes Zugriffsprofil mit Radius-Filter-ID:

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: UNLIMITED\_ACCESS

Description: [Empty text box]

\* Access Type: ACCESS\_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:  ⓘ

Passive Identity Tracking:  ⓘ

---

▼ Common Tasks

DACL Name

ACL (Filter-ID) PERMIT\_ALL.in

Security Group

VLAN

---

▼ Advanced Attributes Settings

Select an item = [Empty dropdown] - +

---

▼ Attributes Details

Access Type = ACCESS\_ACCEPT  
Filter-ID = PERMIT\_ALL.in

Beispiel für ein unbegrenztes Zugriffsprofil mit cisco-av-pair:



The screenshot shows the Cisco ISE configuration interface for a policy element. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID. The main navigation bar includes: Overview, Network Devices, Client Provisioning, Policy Elements (selected), Posture Policy, Policy Sets, Troubleshoot, Reports, and Settings.

**Policy Element Configuration:**

- Name:** UNLIMITED\_ACCESS
- Description:** (empty text area)
- Access Type:** ACCESS\_ACCEPT
- Network Device Profile:** Cisco
- Service Template:** (checkbox, unchecked)
- Track Movement:** (checkbox, unchecked)
- Passive Identity Tracking:** (checkbox, unchecked)

**Common Tasks:**

- DACL Name
- ACL (Filter-ID)
- Security Group
- VLAN

**Advanced Attributes Settings:**

- Configuration: Cisco:cisco-av-pair = ip:interface-config=ip access-g... (with minus and plus icons)

**Attributes Details:**

- Access Type = ACCESS\_ACCEPT
- cisco-av-pair = ip:interface-config=ip access-group PERMIT\_ALL in

**Left Sidebar (Conditions and Remediations):**

- 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:** (empty)
- Requirements:** Allowed Protocols, Authorization Profiles, Downloadable ACLs.

Schritt 2: Konfigurieren Sie die Autorisierungsrichtlinie. In diesem Schritt sollten zwei Autorisierungsrichtlinien erstellt werden. Eine muss der ursprünglichen Authentifizierungsanfrage mit dem Status "Unknown" (Unbekannter Status) entsprechen, und die andere muss nach erfolgreichem Statusprozess vollen Zugriff zuweisen.

Dies ist ein Beispiel für einfache Autorisierungsrichtlinien in diesem Fall:

▼ 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

Die Konfiguration der Authentifizierungsrichtlinie ist nicht Bestandteil dieses Dokuments, Sie sollten jedoch bedenken, dass die Authentifizierung erfolgreich sein muss, bevor die Verarbeitung der Autorisierungsrichtlinien beginnt.

# Überprüfen

Die grundlegende Überprüfung des Datenflusses kann aus drei Hauptschritten bestehen:

Schritt 1: RA VPN-Sitzungsüberprüfung auf dem FlexVPN-HUB:

```
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
```

Schritt 2: Überprüfung des Authentifizierungsflusses (Radius-Live-Protokolle):

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. Erstauthentifizierung. In diesem Schritt können Sie überprüfen, welches Autorisierungsprofil angewendet wurde. Wenn ein unerwartetes Autorisierungsprofil angewendet wurde, überprüfen Sie bitte den detaillierten Authentifizierungsbericht. Sie können diesen Bericht öffnen, indem Sie in der Spalte Details auf die Lupe klicken. Sie können Attribute im detaillierten Authentifizierungsbericht mit der Bedingung in der Autorisierungsrichtlinie vergleichen, die Sie voraussichtlich abgleichen.
2. Änderung der Sitzungsdaten, in diesem speziellen Beispiel, hat sich von NotApplication zu Compliant geändert.
3. COA für Netzwerkzugriffsgerät. Dieses COA sollte die neue Authentifizierung von NAD-Seite und die Zuweisung neuer Autorisierungsrichtlinien auf ISE-Seite erfolgreich durchsetzen. Wenn der COA fehlschlägt, können Sie einen detaillierten Bericht öffnen, um den Grund zu untersuchen. Die häufigsten Probleme im Zusammenhang mit COA sind: COA-Timeout - in diesem Fall wird entweder das PSN, das die Anfrage gesendet hat, auf NAD-Seite nicht als COA-Client konfiguriert oder die COA-Anfrage an einer anderen Stelle auf dem Weg verworfen. COA-negative ACK - gibt an, dass COA bei der NAD eingegangen ist, aber aus irgendeinem Grund nicht bestätigt werden kann, dass COA-Operation nicht bestätigt werden kann. Für dieses Szenario sollte der detaillierte Bericht eine ausführlichere Erläuterung enthalten.

Da für dieses Beispiel ein IOS XE-basierter Router als NAD verwendet wurde, können Sie keine nachfolgende Authentifizierungsanforderung für den Benutzer sehen. Dies liegt daran, dass die ISE COA-Push für IOS XE verwendet, wodurch eine Unterbrechung des VPN-Service vermieden wird. In einem solchen Szenario enthält COA selbst neue Autorisierungsparameter, sodass keine erneute Authentifizierung erforderlich ist.

Schritt 3: Statusberichtsüberprüfung - Navigieren Sie zu **Operations -> Reports -> Reports -> Endpoint and Users -> Posture Assessment by 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 events with columns for Logged At, Status, Details, PRA Action, Identity, Endpoint ID, and IP Address.

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

Sie können von hier aus einen detaillierten Bericht für jedes einzelne Ereignis öffnen, um z. B. zu prüfen, zu welcher Sitzungs-ID dieser Bericht gehört, welche genauen Statusanforderungen von der ISE für den Endpunkt und wie der Status für jede Anforderung festgelegt wurden.

# Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

1. IKEv2-Debug, der vom Headend erfasst werden soll:

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

2. AAA-Debugger zum Anzeigen der Zuweisung von lokalen und/oder Remote-Attributen:

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

3. DART vom AnyConnect-Client.
4. Für die Fehlerbehebung bei Statusprozessen müssen diese ISE-Komponenten beim Debuggen auf den ISE-Knoten aktiviert werden, auf denen Statusprozesse stattfinden können:**client-webapp** - Komponente, die für die Bereitstellung durch Agenten verantwortlich ist. Zielprotokolldateien **guest.log** und **ise-psc.log**.**Gastzugriff** - Komponente, die für die Client-Bereitstellung der Portalkomponente und die Suche nach Sitzungseigentümern verantwortlich ist (wenn die Anfrage zu einem falschen PSN kommt). Zielprotokolldatei - **guest.log**.**Bereitstellung** - Komponente, die für die Verarbeitung von Client-Bereitstellungsrichtlinien verantwortlich ist. Zielprotokolldatei - **guest.log**.**Status** - alle zustandsbezogenen Ereignisse. Zielprotokolldatei - **ise-psc.log**
5. Für die Client-seitige Fehlerbehebung können Sie Folgendes verwenden:**AnyConnect.txt** - Diese Datei befindet sich im DART-Paket und wird zur VPN-Fehlerbehebung verwendet.**cisensa.log**-Bei einem Clientausfall wird diese Datei im gleichen Ordner erstellt, in den NSA heruntergeladen wurde (Downloads-Verzeichnis für Windows normal),**AnyConnect\_ISEPosture.txt** - Diese Datei finden Sie im DART-Paket im Verzeichnis **Cisco AnyConnect ISE Posture Module**. Alle Informationen über die ISE PSN-Erkennung und die allgemeinen Schritte des Statusflusses werden in dieser Datei protokolliert.