

配置FlexVPN：使用本地使用者資料庫的AnyConnect IKEv2遠端訪問

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[網路圖表](#)

[設定](#)

[使用本地資料庫對使用者進行身份驗證和授權](#)

[禁用AnyConnect下載程式功能（可選）。](#)

[AnyConnect XML配置檔案交付](#)

[通訊流](#)

[IKEv2和EAP交換](#)

[驗證](#)

[疑難排解](#)

簡介

本文檔介紹如何配置思科IOS®/XE頭端，以便通過本地使用者資料庫的AnyConnect IKEv2/EAP身份驗證進行訪問。

必要條件

需求

思科建議您瞭解以下主題：

- [IKEv2通訊協定](#)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行Cisco IOS® XE 16.9.2的Cisco雲端服務路由器
- 在Windows 10上運行的AnyConnect客戶030494.6.1版

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

AnyConnect-EAP (也稱為聚合身份驗證) 允許 Flex Server 通過 Cisco 專有 AnyConnect-EAP 方法對 AnyConnect 客戶端進行身份驗證。

與基於標準的可擴展身份驗證協定(EAP)方法(例如 EAP — 通用令牌卡(EAP-GTC)、EAP — 消息摘要5(EAP-MD5)等不同，Flex 伺服器不以 EAP 直通模式運行。

與客戶端的所有 EAP 通訊在 Flex Server 上終止，用於構建 AUTH 負載的所需會話金鑰由 Flex Server 本地計算。

Flex 伺服器必須使用 IKEv2 RFC 要求的證書向客戶端驗證其自身。

Flex Server 現在支援本地使用者身份驗證，並且遠端身份驗證是可選的。

這非常適合於遠端訪問使用者數量較少的小型部署，以及無法訪問外部身份驗證、授權和記帳 (AAA) 伺服器的環境。

但是，對於大規模部署以及需要每個使用者屬性的情況下，仍建議使用外部 AAA 伺服器進行身份驗證和授權。


AnyConnect-EAP 實施允許使用 Radius 進行遠端身份驗證、授權和記帳。

網路圖表



設定

使用本地資料庫對使用者進行身份驗證和授權

 註：要根據路由器上的本地資料庫對使用者進行身份驗證，需要使用 EAP。但是，要使用 EAP，本地身份驗證方法必須是 rsa-sig，因此路由器需要安裝適當的證書，並且不能是自簽名證書。

使用本地使用者身份驗證、遠端使用者和組授權以及遠端記帳的示例配置。

步驟 1. 啟用AAA，配置身份驗證、授權和記帳清單並將使用者名稱新增到本地資料庫：

```
aaa new-model
!
aaa authentication login a-eap-authen-local local
aaa authorization network a-eap-author-grp local
!
username test password cisco123
```

步驟 2. 配置用於儲存路由器證書的信任點。本示例中使用PKCS12檔案匯入。有關其他選項，請參閱PKI(Public Key Infrastructure)配置指南：

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xs-3s/sec-pki-xe-3s-book/sec-cert-enroll-pki.html

```
Router(config)# crypto pki import IKEv2-TP pkcs12 bootflash:IKEv2-TP.p12 password cisco123
```

步驟 3. 定義IP本地池以向AnyConnect VPN客戶端分配地址：

```
ip local pool ACP00L 192.168.10.5 192.168.10.10
```


步驟 4. 建立IKEv2本地授權策略：

```
crypto ikev2 authorization policy ikev2-auth-policy
 pool ACP00L
 dns 10.0.1.1
```

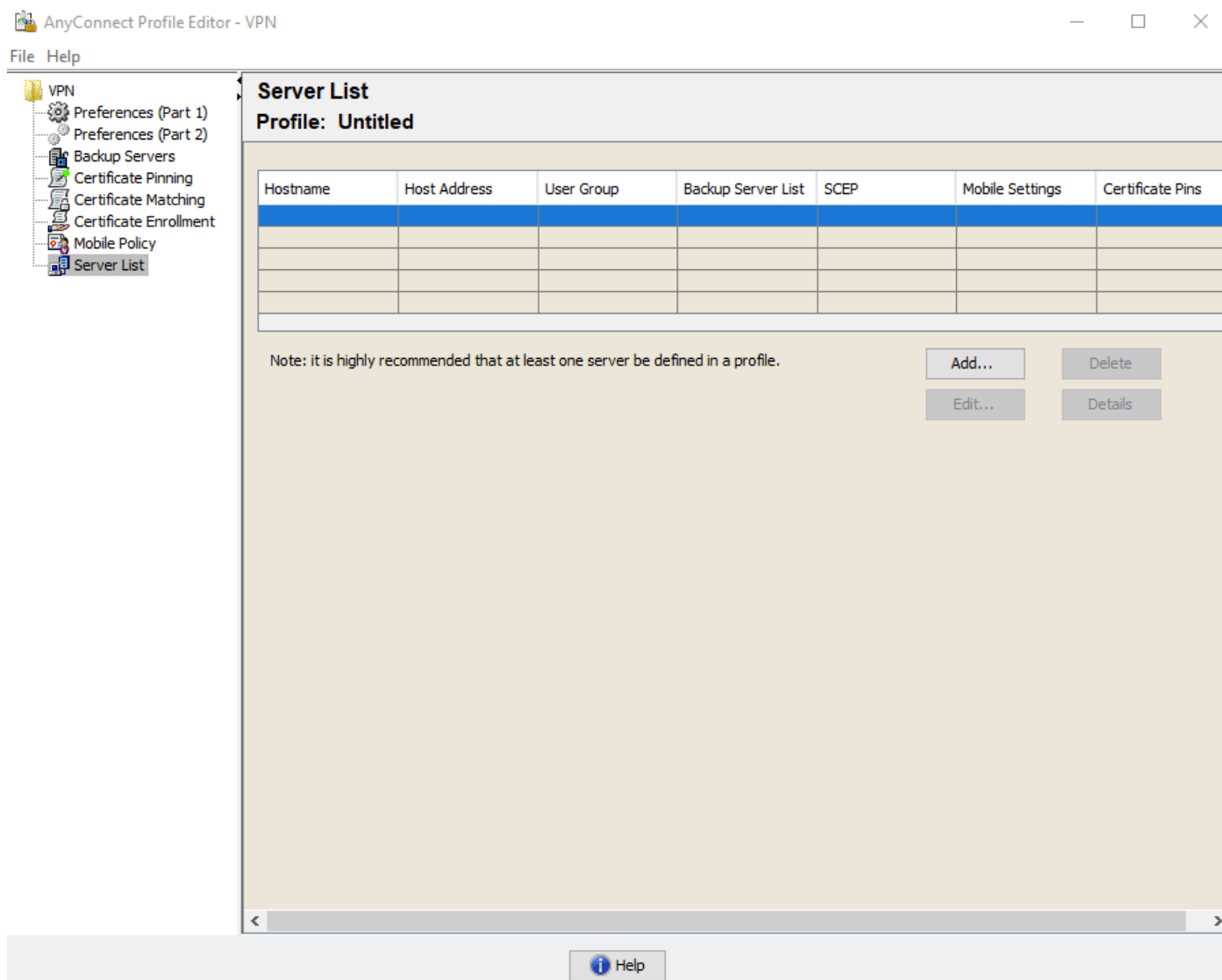
第5步 (可選)。建立所需的IKEv2建議和策略。如果未配置，則使用智慧預設值：

```
crypto ikev2 proposal IKEv2-prop1
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy IKEv2-pol
 proposal IKEv2-prop1
```

步驟 6. 建立AnyConnect配置檔案

 註：需要將AnyConnect配置檔案傳送到客戶端電腦。有關詳細資訊，請參閱下一節。

使用AnyConnect配置檔案編輯器配置客戶端配置檔案，如下圖所示：



按一下「新增」為VPN網關建立條目。確保選擇「IPsec」作為「主協定」。取消選中「ASA網關」選項。

Server **Load Balancing Servers** SCEP Mobile Certificate Pinning

Primary Server

Display Name (required)

FQDN or IP Address /

User Group

Group URL

Connection Information

Primary Protocol

ASA gateway

Auth Method During IKE Negotiation

IKE Identity (IOS gateway only)

Backup Servers

Host Address	
	<input type="button" value="Add"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Delete"/>

儲存配置檔案：檔案 —>另存為。配置檔案的XML等效項：


```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema"
  <ClientInitialization>
    <UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
    <AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
    <ShowPreConnectMessage>false</ShowPreConnectMessage>
    <CertificateStore>All</CertificateStore>
    <CertificateStoreMac>All</CertificateStoreMac>
    <CertificateStoreOverride>false</CertificateStoreOverride>
    <ProxySettings>Native</ProxySettings>
    <AllowLocalProxyConnections>true</AllowLocalProxyConnections>
    <AuthenticationTimeout>12</AuthenticationTimeout>
    <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
    <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
    <LocalLanAccess UserControllable="true">false</LocalLanAccess>
    <DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
    <ClearSmartcardPin UserControllable="true">true</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">Disable
  <PPPEXclusionServerIP UserControllable="false"></PPPEXclusionServerIP>
</PPPEXclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
  <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
  <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
  <HostEntry>
    <HostName>VPN IOS-XE</HostName>
    <HostAddress>vpn.example.com</HostAddress>
    <PrimaryProtocol>IPsec
      <StandardAuthenticationOnly>true
        <AuthMethodDuringIKENegotiation>EAP-AnyConnect</AuthMethodDuringIKENegotiation>
      </StandardAuthenticationOnly>
    </PrimaryProtocol>
  </HostEntry>
</ServerList>
</AnyConnectProfile>

```

 **注意:** AnyConnect使用「*\$AnyConnectClient\$*」作為其型別為key-id的預設IKE標識。但是，可以在AnyConnect配置檔案中手動更改此標識以滿足部署需求。

 **註:** 若要將XML配置檔案上傳到路由器，需要Cisco IOS® XE 16.9.1版或更高版本。如果使用舊版Cisco IOS® XE軟體，則需要在客戶端上禁用配置檔案下載功能。有關詳細資訊，請參閱「禁用AnyConnect下載程式功能」部分。

將建立的XML配置檔案上傳到路由器的快閃記憶體並定義配置檔案：

```
crypto vpn anyconnect profile acvpn bootflash:/acvpn.xml
```

 **註:** 用於AnyConnect XML配置檔案的檔名是acvpn.xml。


步驟 7. 為客戶端身份驗證的AnyConnect-EAP方法建立IKEv2配置檔案。


```

crypto ikev2 profile AnyConnect-EAP
match identity remote key-id *$AnyConnectClient$*
authentication local rsa-sig

```

```
authentication remote anyconnect-eap aggregate
pki trustpoint IKEv2-TP
aaa authentication anyconnect-eap a-eap-authen-local
aaa authorization group anyconnect-eap list a-eap-author-grp ikev2-auth-policy
aaa authorization user anyconnect-eap cached
virtual-template 100
anyconnect profile acvpn
```

 註:CLI接受本地身份驗證方法之前的遠端身份驗證方法配置。但是，如果遠端身份驗證方法是 eap，則對於沒有增強請求修復程式的版本Cisco錯誤ID [CSCvb29701](#)不會生效。對於這些版本，當將eap配置為遠端身份驗證方法時，請確保先將本地身份驗證方法配置為rsa-sig。任何其他形式的遠端身份驗證方法都看不到此問題。

 註：在受Cisco錯誤ID [CSCvb24236](#)影響的代碼版本上，一旦在本地身份驗證之前配置了遠端身份驗證，就不能再在該裝置上配置遠端身份驗證方法。請升級到具有此代碼修復程式的版本。

步驟 8.在路由器上禁用基於HTTP-URL的證書查詢和HTTP伺服器：

```
no crypto ikev2 http-url cert
no ip http server
no ip http secure-server
```

 註：請參閱[本文檔](#)，確認您的路由器硬體是否支援NGE加密演算法（先前的示例中包含NGE演算法），否則，在硬體上安裝IPSec SA會在協商的最後階段失敗。

步驟 9.定義用於保護資料的加密和雜湊演算法

```
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
mode tunnel
```

步驟 10.建立IPSec配置檔案：

```
crypto ipsec profile AnyConnect-EAP
set transform-set TS
set ikev2-profile AnyConnect-EAP
```

步驟 11.使用某個虛擬IP地址配置環回介面。虛擬訪問介面從它借用IP地址。

```
interface loopback100
 ip address 10.0.0.1 255.255.255.255
```

步驟 12. 配置虛擬模板 (在IKEv2配置檔案中關聯模板)

```
interface Virtual-Template100 type tunnel
 ip unnumbered Loopback100
 ip mtu 1400
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile AnyConnect-EAP
```

步驟13 (可選)。預設情況下，來自使用者端的所有流量都會透過通道傳送。您可以配置拆分隧道，僅允許所選流量通過該隧道。

```
ip access-list standard split_tunnel
 permit 10.0.0.0 0.255.255.255
!
crypto ikev2 authorization policy ikev2-auth-policy
 route set access-list split_tunnel
```

第14步 (可選)。如果所有流量都需要通過隧道，請配置NAT以允許遠端客戶端的Internet連線。

```
ip access-list extended NAT
 permit ip 192.168.10.0 0.0.0.255 any
!
ip nat inside source list NAT interface GigabitEthernet1 overload
!
interface GigabitEthernet1
 ip nat outside
!
interface Virtual-Template 100
 ip nat inside
```

禁用AnyConnect下載程式功能 (可選)。

只有在使用Cisco IOS® XE軟體版本低於16.9.1時，才需要執行此步驟。在Cisco IOS® XE 16.9.1之前，無法將XML配置檔案上傳到路由器。預設情況下，成功登入後，AnyConnect客戶端會嘗試下載XML配置檔案。如果配置檔案不可用，連線將失敗。作為解決方法，可以在客戶端本身上禁用AnyConnect配置檔案下載功能。為此，可以修改此檔案：

For Windows:

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\AnyConnectLocalPolicy.xml

For MAC OS:

/opt/cisco/anyconnect/AnyConnectLocalPolicy.xml

「BypassDownloader」選項設定為「true」，例如：

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy xmlns="http://schemas.xmlsoap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema" xsi:schemaLocation="http://schemas.xmlsoap/encoding/ http://www.w3.org/2001/XMLSchema" >
  <BypassDownloader>true</BypassDownloader>
  <EnableCRLCheck>false</EnableCRLCheck>
  <ExcludeFirefoxNSSCertStore>false</ExcludeFirefoxNSSCertStore>
  <ExcludeMacNativeCertStore>false</ExcludeMacNativeCertStore>
  <ExcludePemFileCertStore>false</ExcludePemFileCertStore>
  <ExcludeWinNativeCertStore>false</ExcludeWinNativeCertStore>
  <FipsMode>false</FipsMode>
  <RestrictPreferenceCaching>false</RestrictPreferenceCaching>
  <RestrictTunnelProtocols>false</RestrictTunnelProtocols>
  <RestrictWebLaunch>false</RestrictWebLaunch>
  <StrictCertificateTrust>false</StrictCertificateTrust>
  <UpdatePolicy>
    <AllowComplianceModuleUpdatesFromAnyServer>true</AllowComplianceModuleUpdatesFromAnyServer>
    <AllowISEProfileUpdatesFromAnyServer>true</AllowISEProfileUpdatesFromAnyServer>
    <AllowServiceProfileUpdatesFromAnyServer>true</AllowServiceProfileUpdatesFromAnyServer>
    <AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
    <AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer></UpdatePolicy>
</AnyConnectLocalPolicy>
```

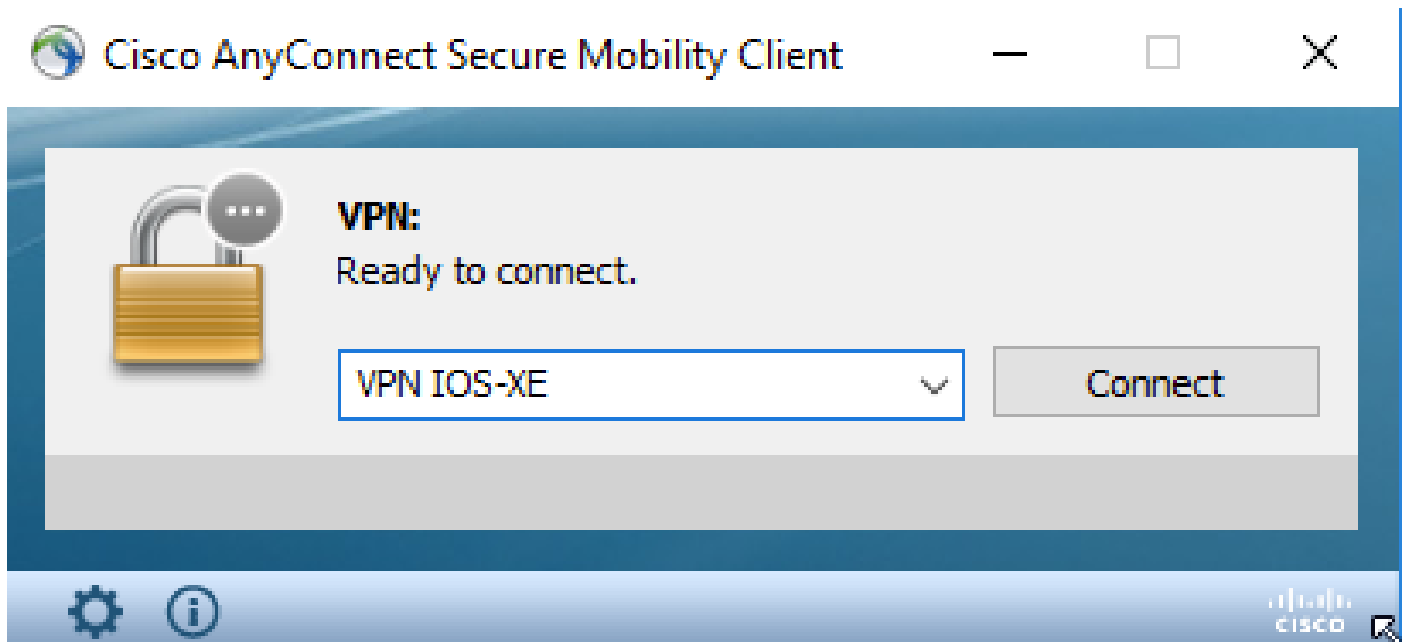
修改完成後，需要重新啟動AnyConnect客戶端。

AnyConnect XML配置檔案交付

通過全新安裝AnyConnect（未新增XML配置檔案），使用者可以在AnyConnect客戶端的位址列中手動輸入VPN網關的FQDN。這會導致到網關的SSL連線。預設情況下，AnyConnect客戶端不會嘗試使用IKEv2/IPsec協定建立VPN隧道。這就是客戶端上必須安裝XML配置檔案才能建立具有Cisco IOS® XE VPN網關的IKEv2/IPsec隧道的原因。

從AnyConnect位址列的下拉選單中選擇配置檔案時，將使用該配置檔案。

顯示的名稱與AnyConnect配置檔案編輯器中的「顯示名稱」中指定的名稱相同。



可以將XML配置檔案手動放入此目錄中：

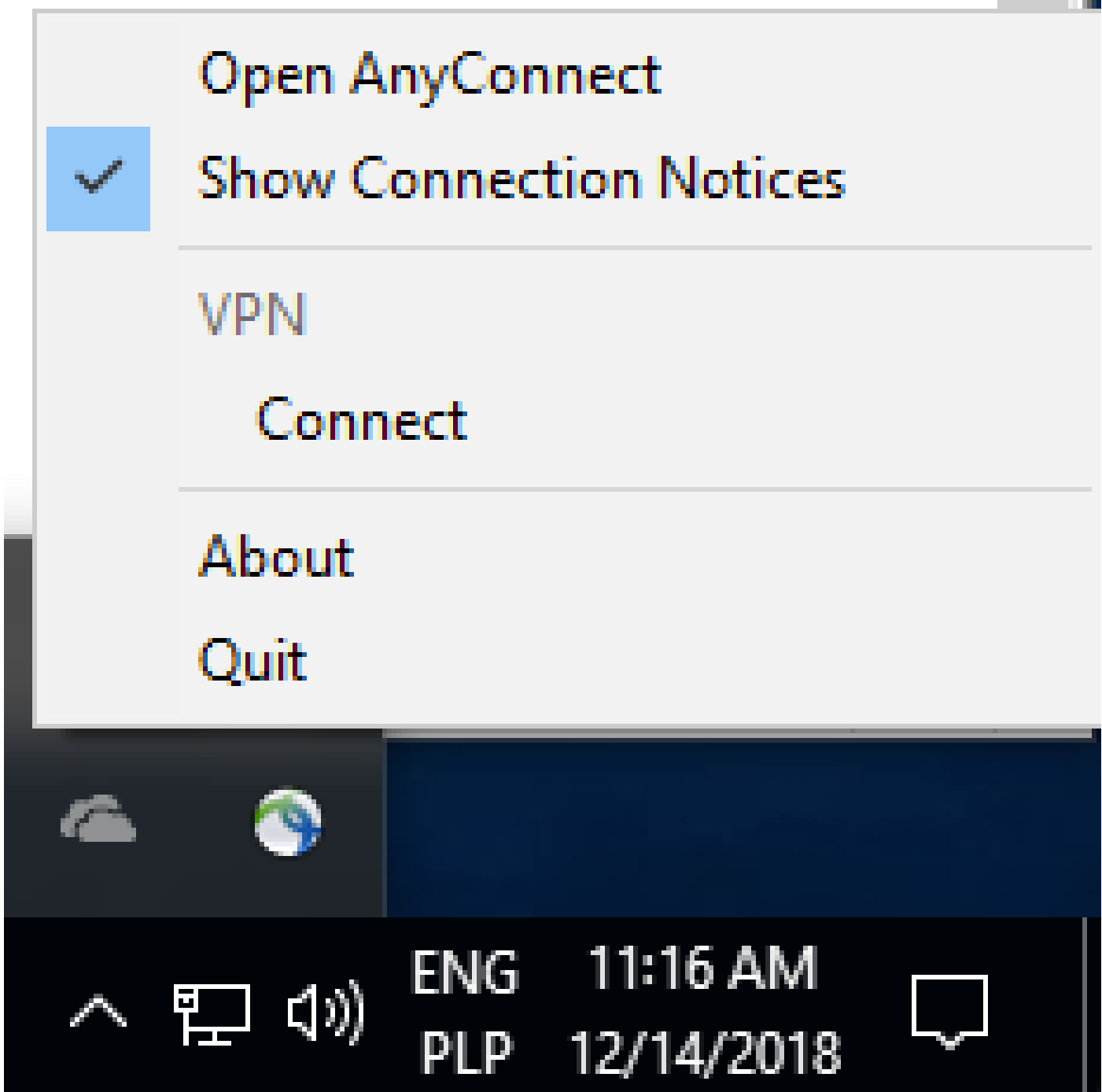
For Windows:

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile

For MAC OS:

/opt/cisco/anyconnect/profile

AnyConnect客戶端需要重新啟動，才能在GUI中看到配置檔案。關閉AnyConnect視窗是不夠的。可通過按一下右鍵Windows工作列中的AnyConnect圖示並選擇「退出」選項來重新啟動該進程：



通訊流

IKEv2和EAP交換

IKE_SA_INIT: HDR, SAi1, KEi, Ni,
V(Fragmentation), V(AnyConnect-EAP),
V(Cisco-Copyright)

IKEv2-INTERNAL (1): Received custom vendor id : CISCO(COPYRIGHT)
IKEv2-INTERNAL (1): Received custom vendor id : CISCO-ANYCONNECT-EAP

IKE_SA_INIT: HDR, SAr1, KEr, Nr,
V(Fragmentation), V(AnyConnect-EAP), V(Cisco-
Copyright), V(Cisco-GRE-MODE)

IKEv2-INTERNAL (1): Sending custom vendor id : CISCO(COPYRIGHT)
IKEv2-INTERNAL (1): Sending custom vendor id : CISCO-GRE-MODE
IKEv2-INTERNAL (1): Sending custom vendor id : CISCO-ANYCONNECT-EAP

IKE_AUTH: HDR, SK (IDi, CERTREQ,
CP(CFG_REQUEST(INTERNAL_IP4_ADDRESS,
INTERNAL_IP4_NETMASK, ...)), SAi2, TSi, TSr)

Searching policy based on peer's identity "\$AnyConnectClient\$" of type 'key ID'

IKE_AUTH: HDR, SK (IDr, CERT, AUTH,
EAP(request{ACDT0{<config-auth
type="hello">}}))

-Sending AnyConnect EAP 'hello' request

IKE_AUTH: HDR, SK (EAP(ESP{ACDT0{
<config-auth type="init">}}))

IKEv2: (SESSION ID = 38, SA ID = 1): Processing AnyConnect EAP response

IKE_AUTH: HDR, SK (IDr, CERT, AUTH,
EAP(request{ACDT0{<config-auth type="auth-
request">}}))

IKEv2: (SESSION ID = 38, SA ID = 1): Sending AnyConnect EAP 'auth-request'

IKE_AUTH: HDR, SK (EAP(ESP{ACDT0{
<config-auth type="auth-reply">}}))

IKEv2: (SESSION ID = 30, SA ID = 1): Processing AnyConnect EAP response

IKE_AUTH: HDR, SK (IDr, CERT, AUTH,
EAP(request{ACDT0{<config-auth
type="complete">}}))

IKEv2: (SESSION ID = 30, SA ID = 1): Sending AnyConnect EAP 'VERIFY' request

Router# show crypto ikev2 sa detailed

IPv4 Crypto IKEv2 SA

Tunnel-id	Local	Remote	fvr/ivrf	Status
1	192.0.2.1/4500			

192.0.2.100/50899

none/none READY

Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: RSA, Auth verify: A

Life/Active Time: 86400/758 sec

CE id: 1004, Session-id: 4

Status Description: Negotiation done

Local spi: 413112E83D493428 Remote spi: 696FA78292A21EA5

Local id: 192.0.2.1

Remote id: *\$AnyConnectClient\$*

Remote EAP id: test

<----- username

Local req msg id: 0 Remote req msg id: 31

Local next msg id: 0 Remote next msg id: 31

Local req queued: 0 Remote req queued: 31

Local window: 5 Remote window: 1

DPD configured for 0 seconds, retry 0

Fragmentation not configured.

Dynamic Route Update: disabled

Extended Authentication not configured.

NAT-T is detected outside

Cisco Trust Security SGT is disabled

Assigned host addr: 192.168.10.8. <---- Assigned IP

Initiator of SA : No

! Check the crypto session information

Router# show crypto session 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

S - SIP VPN

Interface: Virtual-Access1. <----- Virtual interface associated with the client

Profile: AnyConnect-EAP
Uptime: 00:14:54
Session status: UP-ACTIVE

Peer: 192.0.2.100

port 50899 fvrf: (none) ivrf: (none).

<----- Public IP of the remote client

Phase1_id: *\$AnyConnectClient\$*

Desc: (none)

Session ID: 8

IKEv2 SA: local 192.0.2.1/4500 remote 192.0.2.100/50899 Active

Capabilities:N connid:1 lifetime:23:45:06

IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 192.168.10.8

Active SAs: 2, origin: crypto map

Inbound: #pkts dec'ed 89

drop 0 life (KB/Sec) 4607990/2705.

<----- Packets received from the client

Outbound: #pkts enc'ed 2

drop 0 life (KB/Sec) 4607999/2705.

<----- Packets sent to the client

! Check the actual configuration applied for the Virtual-Access interface associated with client

Router# show derived-config interface virtual-access 1.

Building configuration...

Derived configuration : 258 bytes

```
!  
interface Virtual-Access1  
 ip unnumbered Loopback100  
 ip mtu 1400  
 ip nat inside  
 tunnel source 192.0.2.1  
 tunnel mode ipsec ipv4  
 tunnel destination 192.0.2.100  
 tunnel protection ipsec profile AnyConnect-EAP  
 no tunnel protection ipsec initiate  
end
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

1. 要從頭端收集的IKEv2調試：

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

2. AAA調試以檢視本地和/或遠端屬性的分配：

```
debug aaa authorization  
debug aaa authentication
```

3. AnyConnect客戶端的DART。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。