

FlexVPN和Anyconnect IKEv2客戶端配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[設定](#)

[網路圖表](#)

[組態](#)

[集線器配置](#)

[Microsoft Active Directory伺服器配置](#)

[客戶端配置](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹如何配置Cisco AnyConnect安全移動客戶端以使用遠端身份驗證撥入使用者服務 (RADIUS)和本地授權屬性來針對Microsoft Active Directory進行身份驗證。

附註：目前，在Cisco IOS[®]裝置上使用本地使用者資料庫進行身份驗證不起作用。這是因為Cisco IOS不作為EAP身份驗證器運行。新增支援的[增強請求CSCui07025](#)。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS版本15.2(T)或更高版本

- Cisco AnyConnect Security Mobility Solution 3.0或更高版本
- Microsoft Active Directory

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱[思科技術提示慣例](#)以瞭解更多有關文件慣例的資訊。

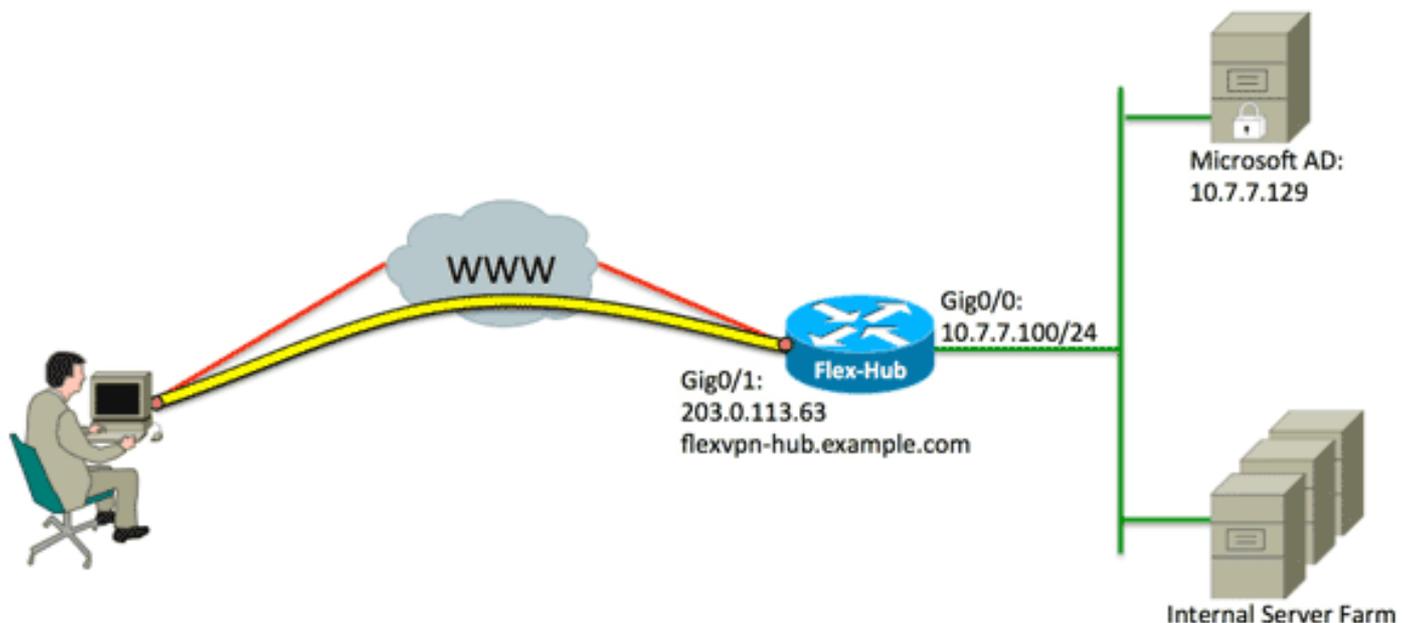
設定

本節提供用於設定本檔案中所述功能的資訊。

使用[命令查詢工具](#)（僅供已註冊客戶使用）可獲取本節中使用的命令的更多資訊。

網路圖表

本檔案會使用以下網路設定：



組態

本檔案會使用以下設定：

- [集線器配置](#)
- [Microsoft Active Directory伺服器配置](#)
- [客戶端配置](#)

集線器配置

1. 配置RADIUS僅用於身份驗證，並定義本地授權。

```
aaa new-model
aaa group server radius FlexVPN-AuthC-Server-Group-1
server-private 10.7.7.129 key Cisco123
aaa authentication login FlexVPN-AuthC-List-1 group
FlexVPN-AuthC-Server-Group-1
aaa authorization network FlexVPN-AuthZ-List-1 local
```

aaa authentication login list命令是指身份驗證、授權和記帳(AAA)組 (用於定義RADIUS伺服器)。 **aaa authorization network list**命令指明將使用本地定義的使用者/組。必須更改RADIUS伺服器上的配置，以允許來自此裝置的身份驗證請求。

2. 配置本地授權策略。

```
ip local pool FlexVPN-Pool-1 10.8.8.100 10.8.8.200
crypto ikev2 authorization policy FlexVPN-Local-Policy-1
pool FlexVPN-Pool-1
dns 10.7.7.129
netmask 255.255.255.0
def-domain example.com
```

ip local pool命令用於定義分配給客戶端的IP地址。使用*FlexVPN-Local-Policy-1*使用者名稱定義授權策略，並且在此處配置客戶端的屬性 (DNS伺服器、網路掩碼、拆分清單、域名等)。

3. 確保伺服器使用證書(rsa-sig)進行身份驗證。

Cisco AnyConnect安全移動客戶端要求伺服器使用證書(rsa-sig)進行身份驗證。路由器必須擁有來自受信任憑證授權單位(CA)的*Web伺服器憑證* (即，在擴充金鑰使用擴充體中具有「伺服器驗證」的憑證)。

請參閱[ASA 8.x手動安裝第三方供應商證書以用於WebVPN配置示例](#)中的步驟1至4，並將所有加密ca例項更改為*crypto pki*。

```
crypto pki trustpoint FlexVPN-TP-1
enrollment url
serial-number none
fqdn flex-hub.example.com
ip-address none
subject-name cn=flex-hub.example.com
revocation-check crl
rsakeypair FlexVPN-TP-1-Key 2048
```

4. 配置此連線的設定。

```
crypto ikev2 profile FlexVPN-IKEv2-Profile-1
match identity remote key-id example.com
identity local dn
authentication remote eap query-identity
authentication local rsa-sig
pki trustpoint FlexVPN-TP-1
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
virtual-template 10
```

crypto ikev2 配置檔案包含此連線的大部分相關設定：**match identity remote key-id** — 指客戶端使用的IKE標識。此字串值在AnyConnect XML配置檔案中配置。**identity local dn** — 定義FlexVPN中心使用的IKE標識。此值使用來自所用證書的值。**authentication remote** — 說明EAP應用於客戶端身份驗證。**authentication local** — 表示證書應用於本地身份驗證。**aaa authentication eap** — 使用EAP進行身份驗證時，使用aaa authentication login list FlexVPN-AuthC-List-1的狀態。**aaa authorization group eap list** — 使用aaa authorization network list FlexVPN-AuthZ-List-1和使用者名稱*FlexVPN-Local-Policy-1*作為授權屬性的狀態。**virtual-template 10** -定義克隆虛擬訪問介面時要使用的模板。

5. 配置回連結到步驟4中定義的IKEv2配置檔案的IPsec配置檔案。

```
crypto ipsec profile FlexVPN-IPsec-Profile-1
set ikev2-profile FlexVPN-IKEv2-Profile-1
```

附註：Cisco IOS使用智慧預設值。因此，不需要顯式定義轉換集。

6. 配置從中克隆虛擬訪問介面的虛擬模板：

ip unnumbered - 從*Inside* interface取消對接口的編號，以便在該介面上啟用IPv4路由。**通道模式ipsec ipv4** - 將介面定義為VTI型別通道。

```
interface Virtual-Template10 type tunnel
ip unnumbered GigabitEthernet0/0
tunnel mode ipsec ipv4
tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
```

7. 將交涉限制為SHA-1。（可選）

由於[CSCud96246](#)（僅限註冊客戶）缺陷，AnyConnect客戶端可能無法正確驗證FlexVPN中心證書。此問題是由於IKEv2為偽隨機函式(PRF)協商SHA-2功能，而已使用SHA-1對FlexVPN-Hub證書進行簽名。以下配置將協商限制為SHA-1:

```
crypto ikev2 proposal SHA1-only
encryption aes-cbc-256
integrity sha1
group 5
crypto ikev2 policy SHA1-only
match fvrfl any
proposal SHA1-only
```

Microsoft Active Directory伺服器配置

1. 在Windows Server Manager中，展開Roles > Network Policy and Access Server > NMPs(Local)> RADIUS Clients and Servers，然後按一下RADIUS Clients。

將出現「新建RADIUS客戶端」對話方塊。

New RADIUS Client

Settings | **Advanced**

Enable this RADIUS client

Select an existing template:

[Empty dropdown menu]

Name and Address

Friendly name:
FlexVPN-Hub

Address (IP or DNS):
10.7.7.100 [Verify...]

Shared Secret

Select an existing Shared Secrets template:
None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

Manual Generate

Shared secret:
[Masked text]

Confirm shared secret:
[Masked text]

[OK] [Cancel]

2. 在「新建RADIUS客戶端」對話方塊中，將Cisco IOS路由器新增為RADIUS客戶端：
按一下**Enable this RADIUS client**覆取方塊。在「友好名稱」欄位中輸入名稱。此範例使用 *FlexVPN-Hub*。在Address欄位中輸入路由器的IP地址。在Shared Secret區域中，按一下 **Manual**單選按鈕，然後在Shared secret和Confirm shared secret欄位中輸入共用金鑰。**注意**：共用金鑰必須與路由器上配置的共用金鑰匹配。按一下「OK」（確定）。
3. 在伺服器管理器介面中，展開**Policies**，然後選擇**Network Policies**。

系統將顯示New Network Policy對話方塊。

New Network Policy

Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:
FlexVPN

Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

Type of network access server:
Unspecified

Vendor specific:
10

Previous Next Finish Cancel

4. 在新網路策略對話方塊中，新增新的網路策略：

在Policy name欄位中輸入名稱。此範例使用*FlexVPN*。按一下**Type of network access server**單選按鈕，然後從下拉選單中選擇**Unspecified**。按「Next」（下一步）。在新網路策略對話方塊中，按一下**Add**以新增新條件。在選擇條件對話方塊中，選擇**NAS IPv4地址條件**，然後按一下**新增**。

系統將顯示NAS IPv4地址對話方塊。

NAS IPv4 Address

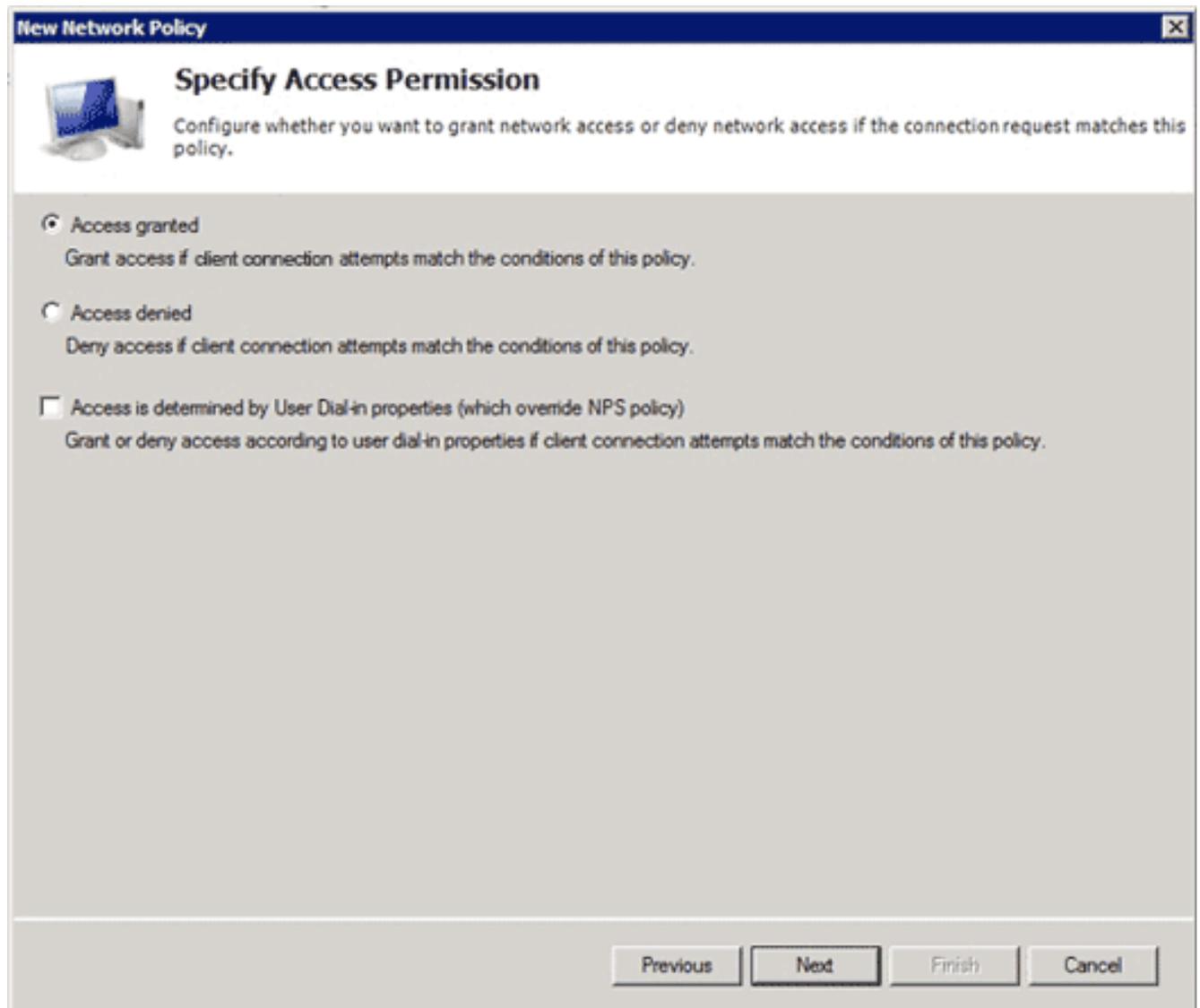
Specify the IPv4 address of the network access server sending the access request message. You can use pattern matching syntax.

10.7.7.100

OK Cancel

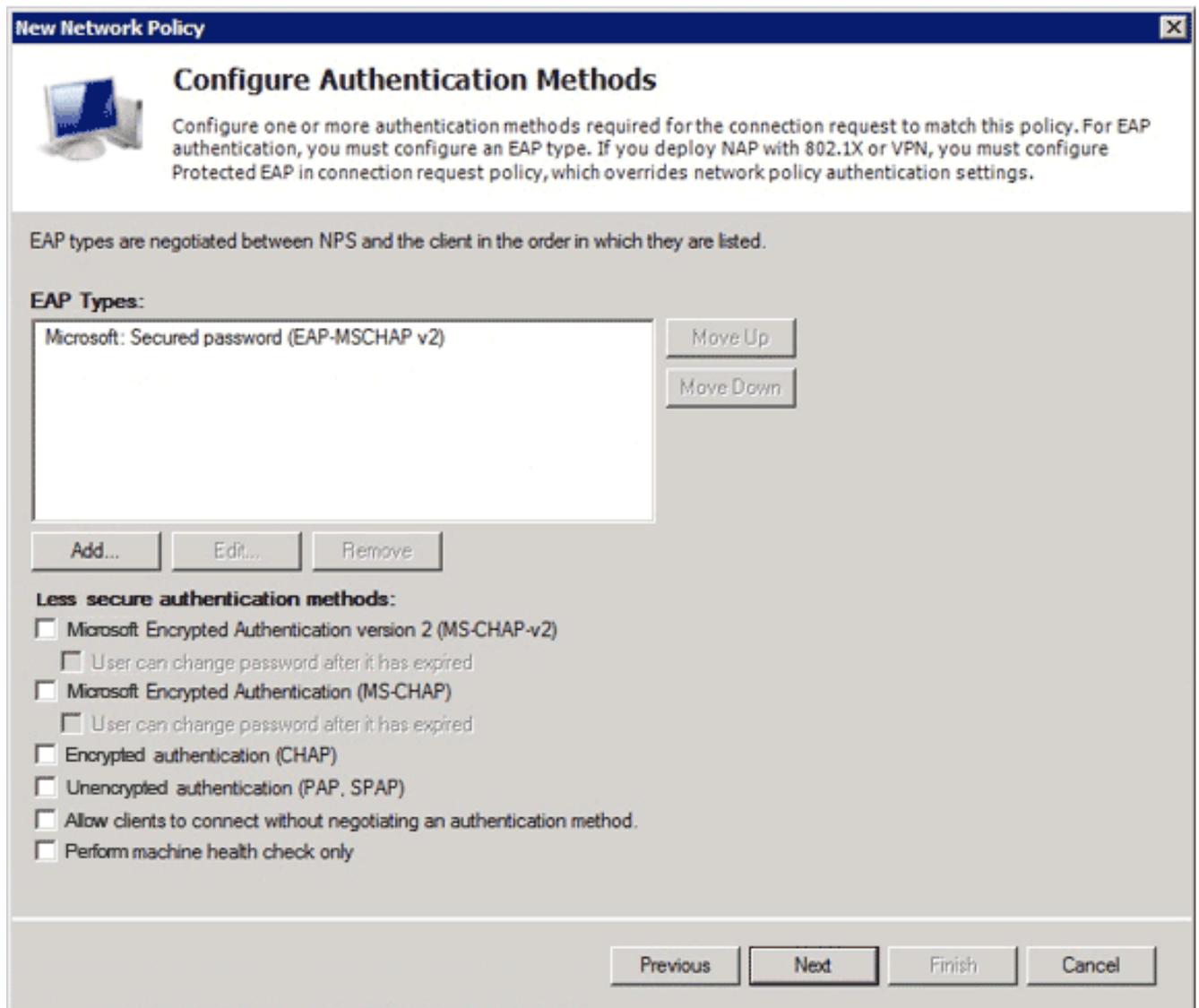
在「NAS IPv4地址」對話方塊中，輸入網路接入伺服器的IPv4地址，以便將網路策略限制為僅來自此Cisco IOS路由器的請求。

按一下「OK」（確定）。



The screenshot shows a Windows-style dialog box titled "New Network Policy" with a close button (X) in the top right corner. Below the title bar is a header area with a computer icon and the text "Specify Access Permission" and "Configure whether you want to grant network access or deny network access if the connection request matches this policy." The main area contains three radio button options: "Access granted" (selected), "Access denied", and "Access is determined by User Dial-in properties (which override NPS policy)". At the bottom right, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

在新網路策略對話方塊中，按一下**Access granted**單選按鈕以允許客戶端訪問網路（如果使用者提供的憑據有效），然後按一下**Next**。



僅確保Microsoft:安全密碼(EAP-MSCHAP v2)出現在「EAP型別」區域中，以允許將EAP-MSCHAPv2用作Cisco IOS裝置與Active Directory之間的通訊方法，然後按一下下一步。

附註：取消選中所有「不安全的身份驗證方法」選項。

繼續通過嚮導並應用您的組織安全策略定義的任何其他約束或設定。此外，請確保先按處理順序列出策略，如下圖所示：

Network Policies



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
FlexVPN	Enabled	1	Grant Acce...	Unspecified
Connections to Microsoft Routing and Remote Access server	Enabled	2	Deny Access	Unspecified
Connections to other access servers	Enabled	3	Deny Access	Unspecified

FlexVPN

Conditions - If the following conditions are met:

Condition	Value
NAS IPv4 Address	10.7.7.100

Settings - Then the following settings are applied:

Setting	Value
Authentication Method	EAP
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed
Ignore User Dial-In Properties	False
Extensible Authentication Protocol Method	Microsoft: Secured password (EAP-MSCHAP v2)

客戶端配置

1. 在文本編輯器中建立XML配置檔案，並將其命名為 *flexvpn.xml*。

此示例使用此XML配置檔案：

```
<?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>
<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>
<ClearSmartcardPin UserControllable="true">>false
</ClearSmartcardPin>
<AutoReconnect UserControllable="false">>true
<AutoReconnectBehavior UserControllable="false">
DisconnectOnSuspend
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="true">>false</AutoUpdate>
<RSA SecurIDIntegration UserControllable="false">
Automatic
</RSA SecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon
</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly
</WindowsVPNEstablishment>
<AutomaticVPNPolicy>>false</AutomaticVPNPolicy>
<PPPEExclusion UserControllable="false">Disable
<PPPEExclusionServerIP UserControllable="false">
</PPPEExclusionServerIP>
</PPPEExclusion>
<EnableScripting UserControllable="true">>true
<TerminateScriptOnNextEvent>true
</TerminateScriptOnNextEvent>
<EnablePostSBLOnConnectScript>true
</EnablePostSBLOnConnectScript>
</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">>false
<AutoServerSelectionImprovement>20
</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4
</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>>false
</RetainVpnOnLogoff>
</ClientInitialization>
<ServerList>
<HostEntry>
```

```
<HostName>FlexVPN Hub</HostName>
<HostAddress>flexvpn-hub.example.com</HostAddress>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>EAP-MSCHAPv2</AuthMethodDuringIKENegotiation>
<IKEIdentity>example.com</IKEIdentity>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

<HostName>是在客戶端中顯示的文本字串。<HostAddress>是FlexVPN中心的完全限定域名 (FQDN)。<PrimaryProtocol>將連線配置為使用IKEv2/IPsec而不是SSL (AnyConnect中的預設值) 。<AuthMethodDuringIKENegotiation>將連線配置為在EAP中使用MSCHAPv2。對Microsoft Active Directory進行身份驗證需要此值。<IKEIdentity>定義將客戶端與集線器上的特定IKEv2配置檔案匹配的字串值 (請參閱上述步驟4) 。

附註：客戶端配置檔案是僅由客戶端使用的檔案。建議管理員使用Anyconnect配置檔案編輯器建立客戶端配置檔案。

2. 將flexvpn.xml檔案儲存到下表中列出的相應目錄中：

3. 關閉並重新啟動AnyConnect客戶端。



4. 在Cisco AnyConnect Secure Mobility Client對話方塊中，選擇**FlexVPN Hub**，然後按一下**Connect**。

Cisco AnyConnect | FlexVPN中心對話方塊。



5. 輸入使用者名稱和密碼，然後按一下OK。

驗證

若要驗證連線，請使用 `show crypto session detail remote client-ipaddress` 命令。有關此命令的詳細資訊，請參閱 [show crypto session](#)。

附註：[輸出直譯器工具](#) (僅供 [已註冊](#) 客戶使用) (OIT) 支援某些 `show` 命令。使用 OIT 檢視 `show` 命令輸出的分析。

疑難排解

為了對連線進行故障排除，請收集和分析來自客戶端的 DART 日誌，並在路由器上使用以下調試命令：`debug crypto ikev2 packet` 和 `debug crypto ikev2 internal`。

附註：使用 `debug` 指令之前，請先參閱有關 `Debug` 指令的重要資訊。

相關資訊

- [技術支援與文件 - Cisco Systems](#)