使用MSCHAPv2 over RADIUS設定FTD遠端存取VPN

目錄

簡介

本文檔介紹如何通過Firepower管理中心(FMC)，為具有遠端身份驗證撥入使用者服務(RADIUS)身份驗證的遠端訪問VPN客戶端啟用Microsoft質詢握手身份驗證協定版本2(MS-CHAPv2)作為身份驗證方法。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- 身分識別服務引擎 (ISE)
- Cisco AnyConnect Security Mobility Solution — 遠端存取
- RADIUS通訊協定

採用元件

本檔案中的資訊是根據以下軟體版本：

- FMCv - 7.0.0（內部版本94）
- FTDv - 7.0.0（內部版本94）
- ISE - 2.7.0.356
- AnyConnect - 4.10.02086

- Windows 10 Pro

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

預設情況下，FTD使用密碼驗證通訊協定(PAP)作為AnyConnect VPN連線的RADIUS伺服器的驗證方法。

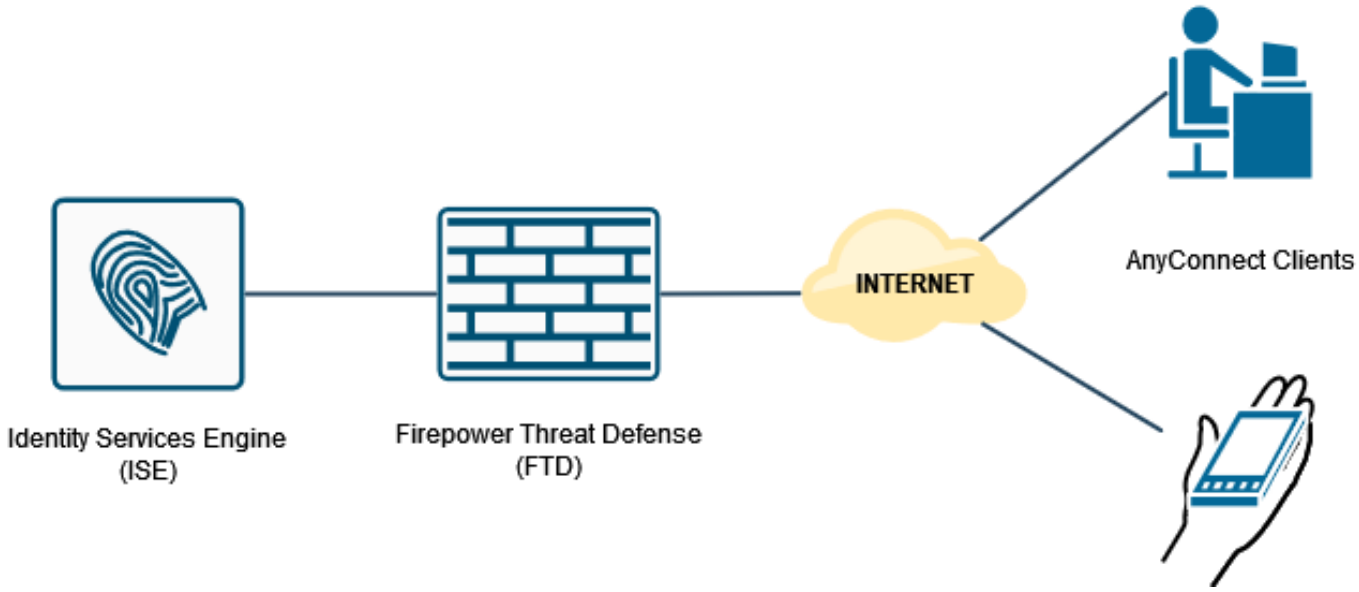
PAP為使用者提供了一種通過雙向握手建立其身份的簡單方法。PAP密碼使用共用金鑰加密，並且是最簡單的身份驗證協定。PAP不是一種強大的身份驗證方法，因為它幾乎無法防止反複的試錯攻擊。

MS-CHAPv2身份驗證引入了對等體之間的相互身份驗證和更改密碼功能。

要啟用MS-CHAPv2作為ASA和RADIUS伺服器之間用於VPN連線的協定，必須在連線配置檔案中啟用密碼管理。啟用密碼管理會生成從FTD到RADIUS伺服器的MS-CHAPv2身份驗證請求。

設定

網路圖表

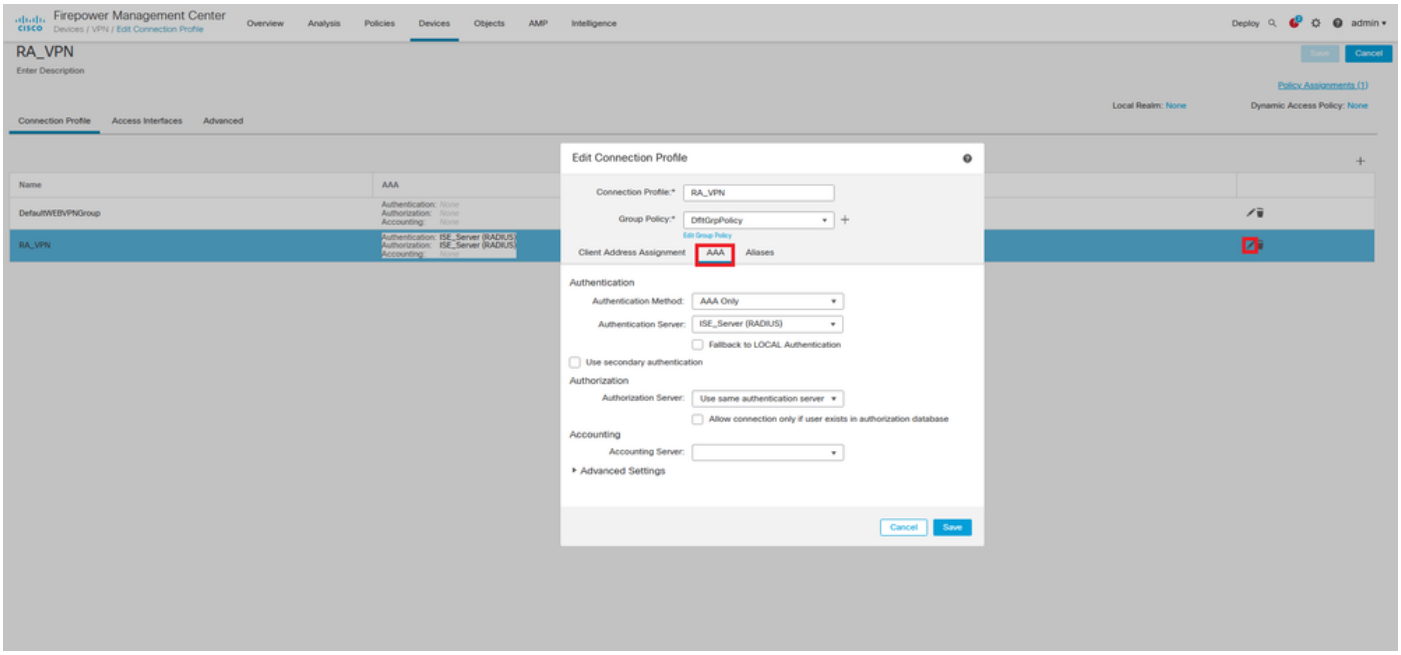


通過FMC配置具有AAA/RADIUS身份驗證的RA VPN

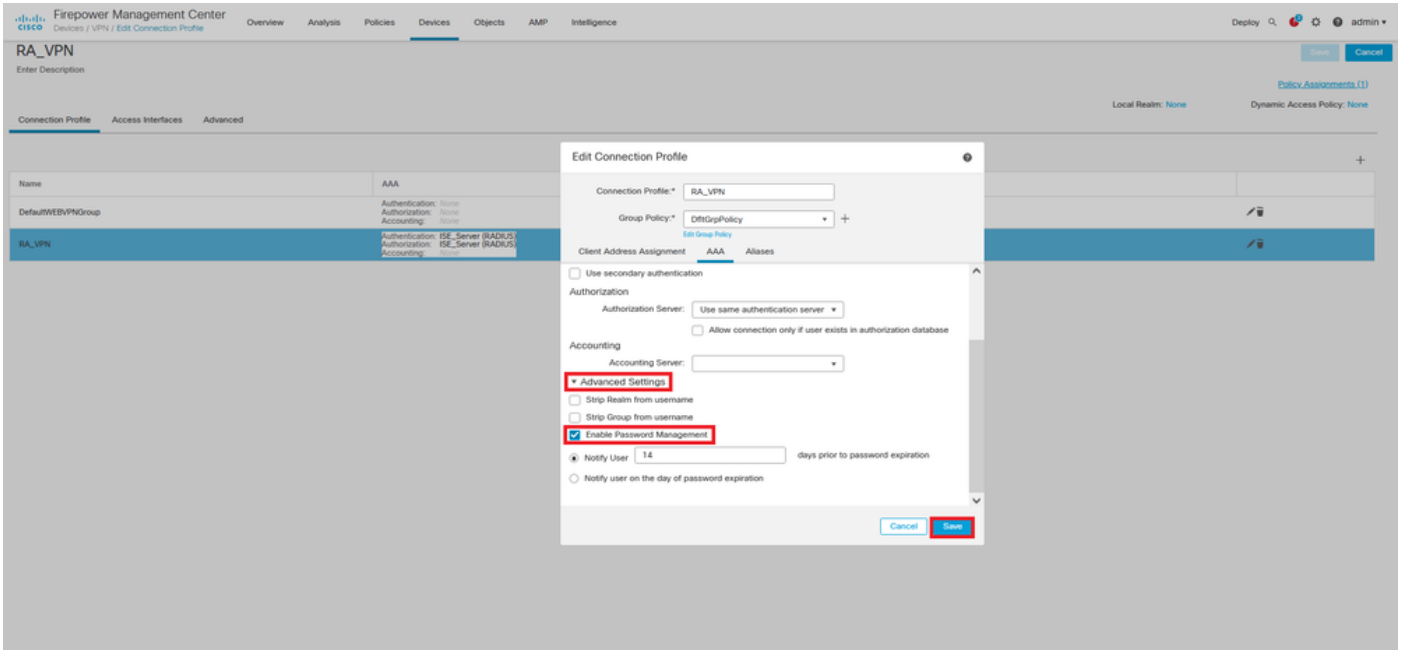
如需逐步程式，請參閱本檔案及以下影片：

- FTD上的AnyConnect遠端存取VPN組態
- FMC管理的FTD的初始AnyConnect配置

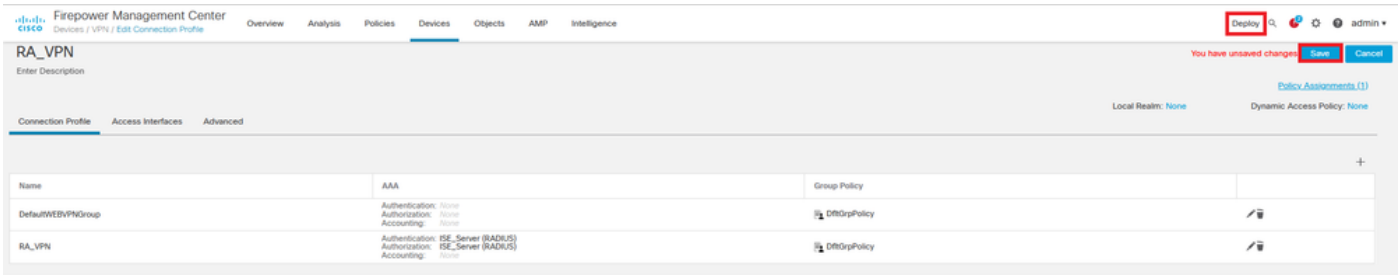
步驟1.配置遠端訪問VPN後，導航到**Devices > Remote Access**，編輯新建立的連線配置檔案，然後導航到**AAA**頁籤。



展開**Advanced Settings**部分，然後按一下**Enable Password Management**覈取方塊。按一下「**Save**」。



儲存和**部署**。



FTD CLI上的遠端存取VPN組態如下：

```
ip local pool AC_Pool 10.0.50.1-10.0.50.100 mask 255.255.255.0
```

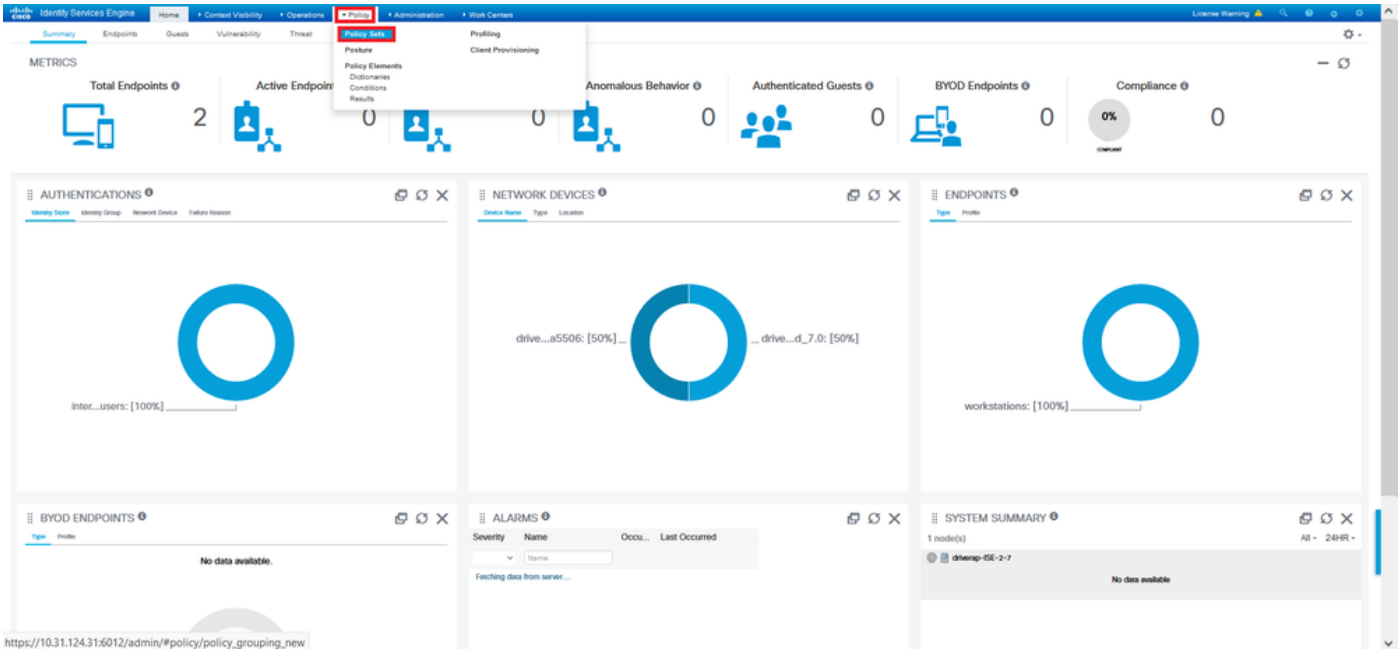
```
interface GigabitEthernet0/0
nameif Outside_Int
security-level 0
ip address 192.168.0.100 255.255.255.0

aaa-server ISE_Server protocol radius
aaa-server ISE_Server host 172.16.0.8
key *****
authentication-port 1812
accounting-port 1813

crypto ca trustpoint RAVPN_Self-Signed_Cert
enrollment self
fqdn none
subject-name CN=192.168.0.100
keypair <Default-RSA-Key>
crl configure

ssl trust-point RAVPN_Self-Signed_Cert

webvpn
enable Outside_Int
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.10.02086-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
no disable
error-recovery disable

group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol ikev2 ssl-client
user-authentication-idle-timeout none
webvpn
anyconnect keep-installer none
anyconnect modules value none
anyconnect ask none default anyconnect
http-comp none
activex-relay disable
file-entry disable
file-browsing disable
url-entry disable
deny-message none

tunnel-group RA_VPN type remote-access
tunnel-group RA_VPN general-attributes
address-pool AC_Pool
authentication-server-group ISE_Server
password-management
tunnel-group RA_VPN webvpn-attributes
group-alias RA_VPN enable
```

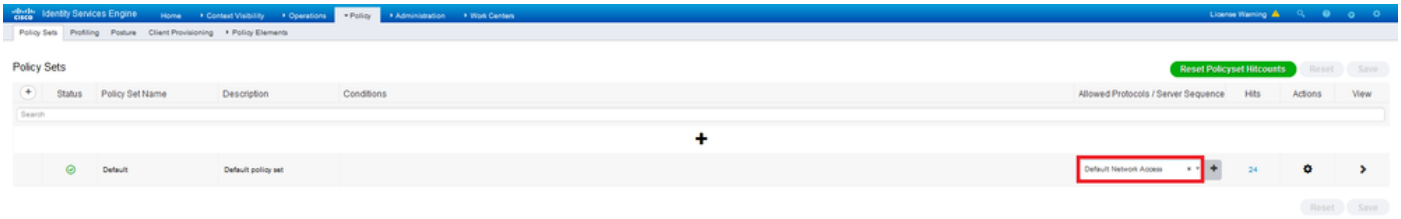
配置ISE以支援MS-CHAPv2作為身份驗證協定

假設：

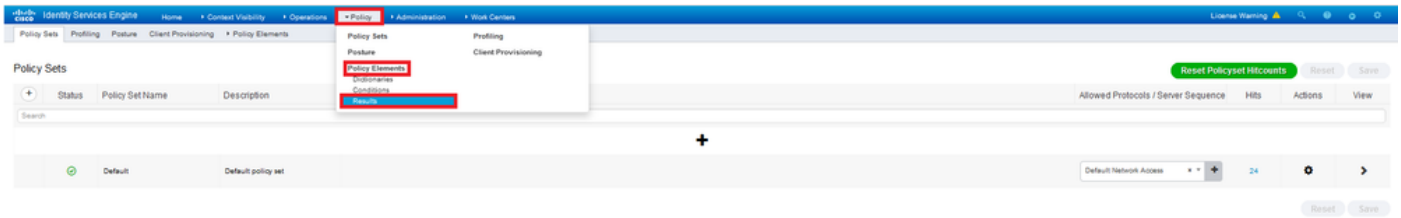
1. FTD已作為ISE上的網路裝置新增，因此它可以處理來自FTD的RADIUS存取要求。
2. 至少有一個使用者可用於ISE對AnyConnect客戶端進行身份驗證。

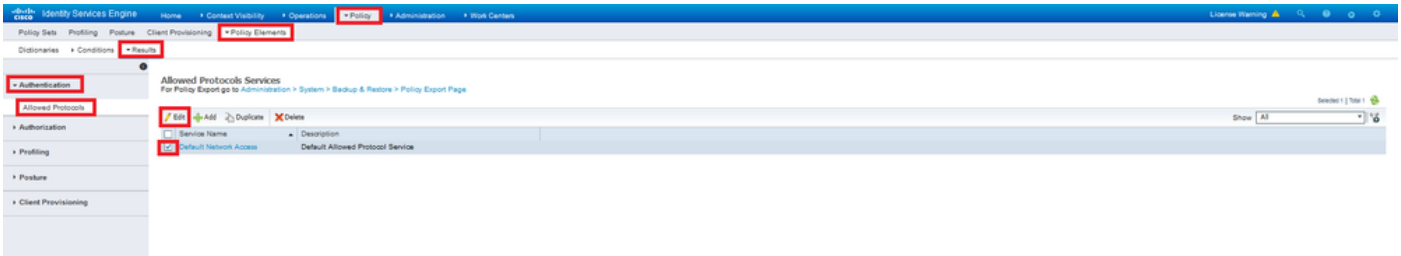
步驟2.導覽至**Policy > Policy Sets**，並找到**Allowed Protocols**策略附加到您的AnyConnect使用者進行身份驗證的策略集。在本示例中，僅存在一個策略集，因此所討論的策略是*預設網路訪問*。



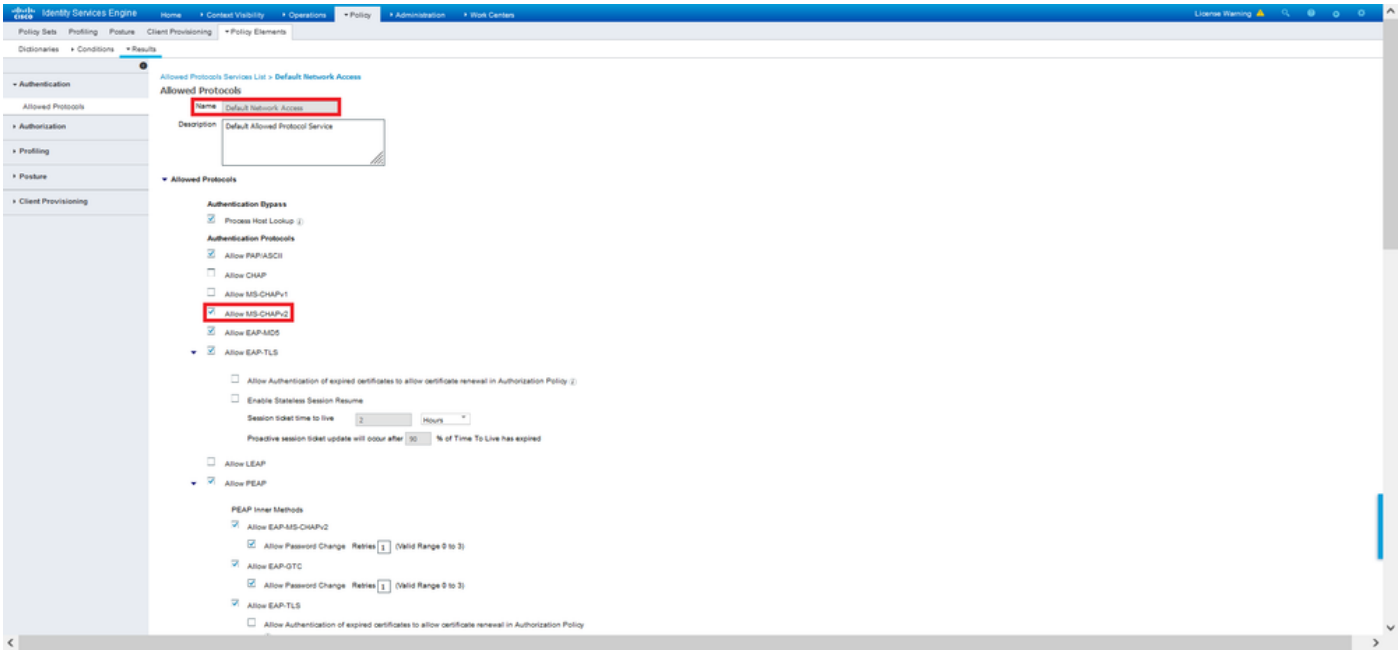


步驟3.導覽至**Policy > Policy Elements > Results**。在**Authentication > Allowed Protocols**下，選擇並編輯**Default Network Access**。



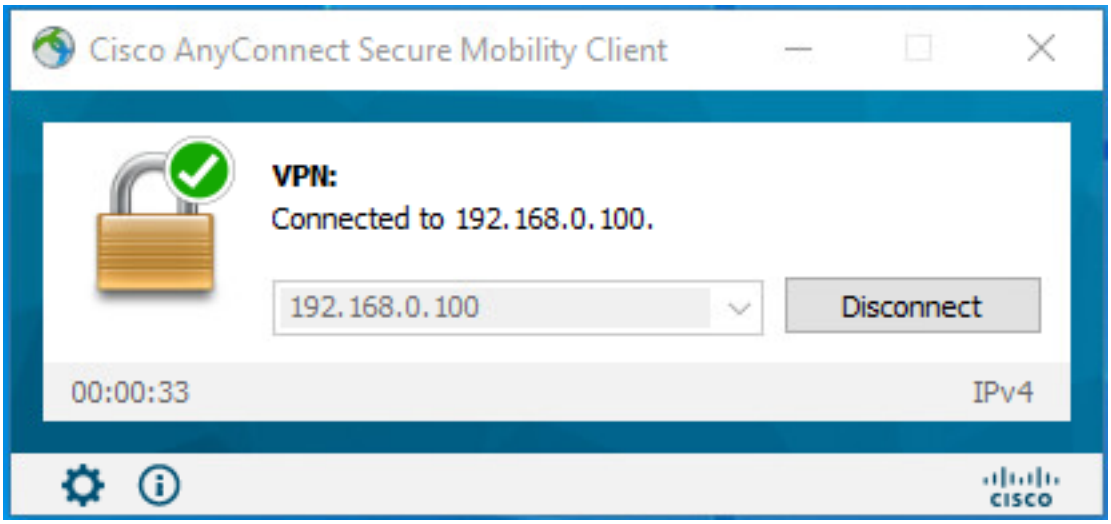


確保選中**Allow MS-CHAPv2**覈取方塊。一直向下滾動，然後**儲存**它。

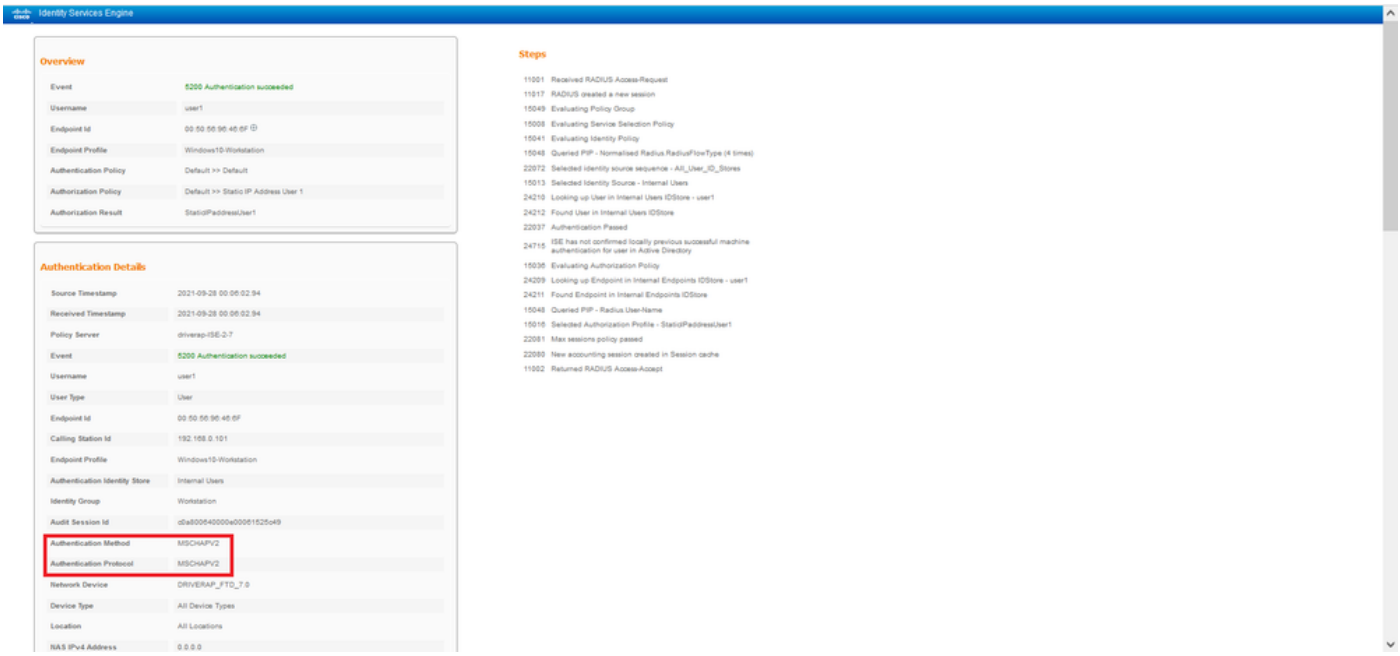


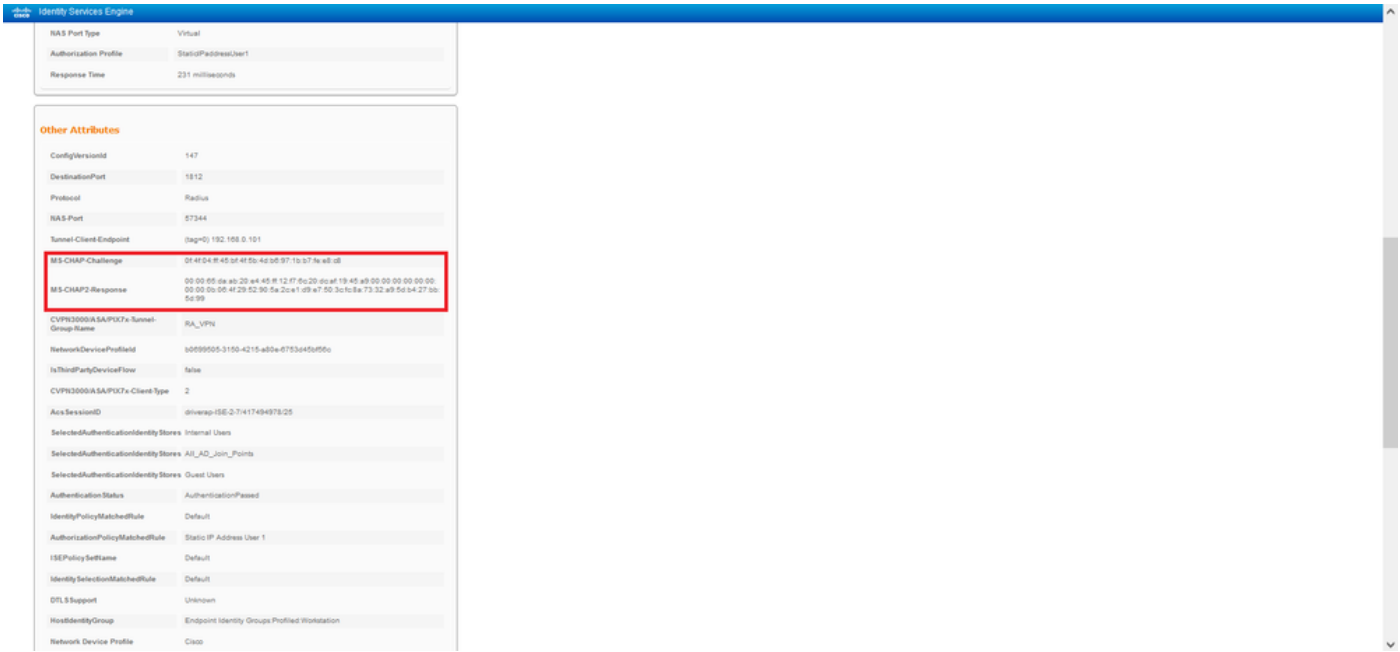
驗證

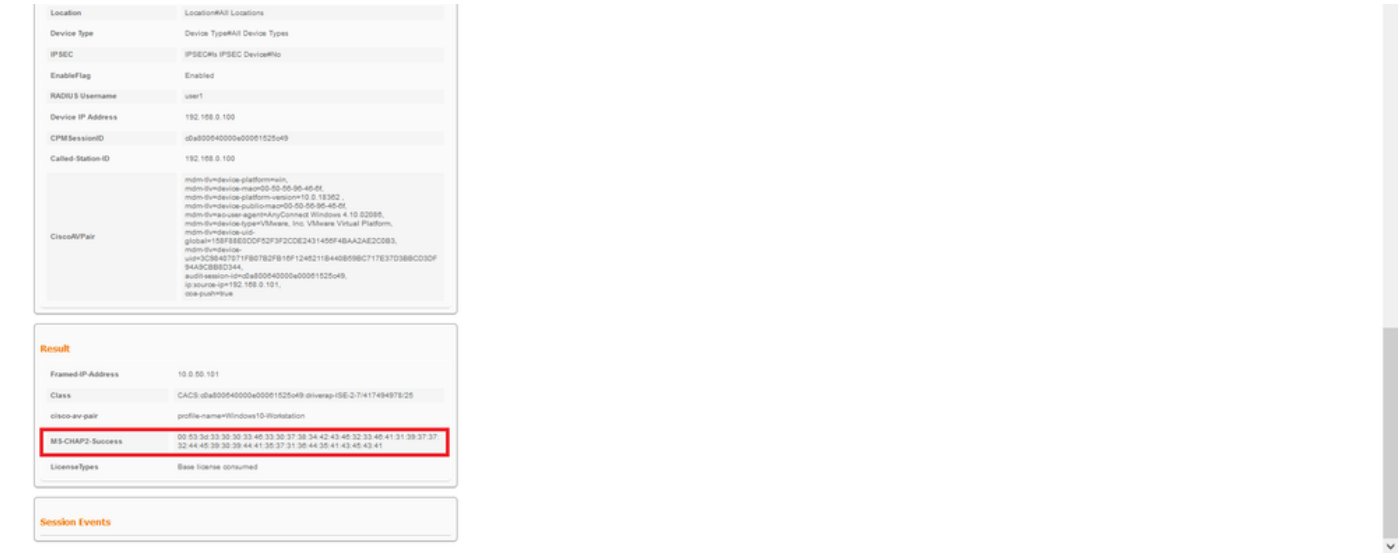
導航到安裝Cisco AnyConnect安全移動客戶端的客戶端電腦。連線到FTD頭端（此範例中使用的是Windows電腦），並鍵入使用者憑證。



ISE上的RADIUS即時日誌顯示：







註:**test aaa-server authentication**命令始終使用PAP向RADIUS伺服器傳送身份驗證請求，無

法通過此命令強制防火牆使用MS-CHAPv2。

firepower# **test aaa-server authentication ISE_Server host 172.16.0.8 username user1 password XXXXXX**
資訊：正在嘗試對IP地址(172.16.0.8)進行身份驗證測試(超時：12秒)
資訊：身份驗證成功

附註：請勿透過Flex-config修改**tunnel-group ppp-attributes**，因為這對透過RADIUS為AnyConnect VPN（SSL和IPSec）連線交涉的驗證通訊協定沒有影響。

tunnel-group RA_VPN ppp-attributes
no authentication pap
驗證chap
驗證ms-chap-v1
no authentication ms-chap-v2
no authentication eap-proxy

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

在FTD:

- **debug radius all**

在ISE上：

- RADIUS即時日誌