

使用MSCHAPv2 over RADIUS設定FTD遠端存取VPN

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[通過FMC配置具有AAA/RADIUS身份驗證的RA VPN](#)

[配置ISE以支援MS-CHAPv2作為身份驗證協定](#)

[驗證](#)

[疑難排解](#)

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。

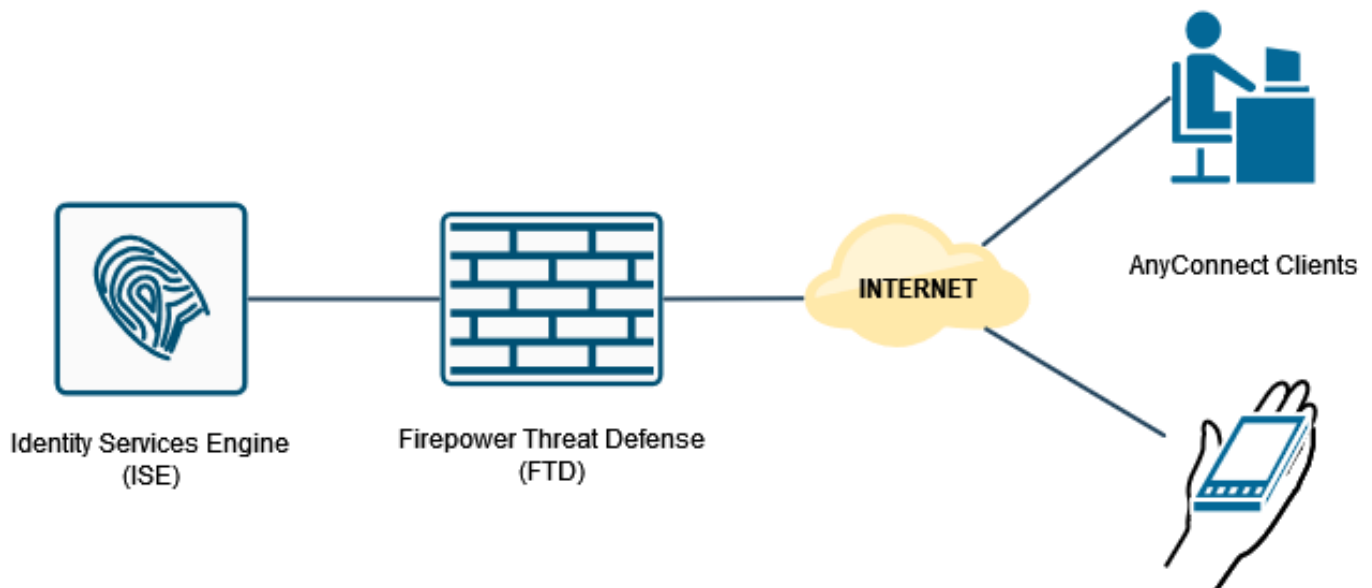
PAP為使用者提供了一種通過雙向握手建立其身份的簡單方法。PAP密碼使用共用金鑰加密，並且是最簡單的身份驗證協定。PAP不是一種強大的身份驗證方法，因為它幾乎無法防止反復的試錯攻擊。

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

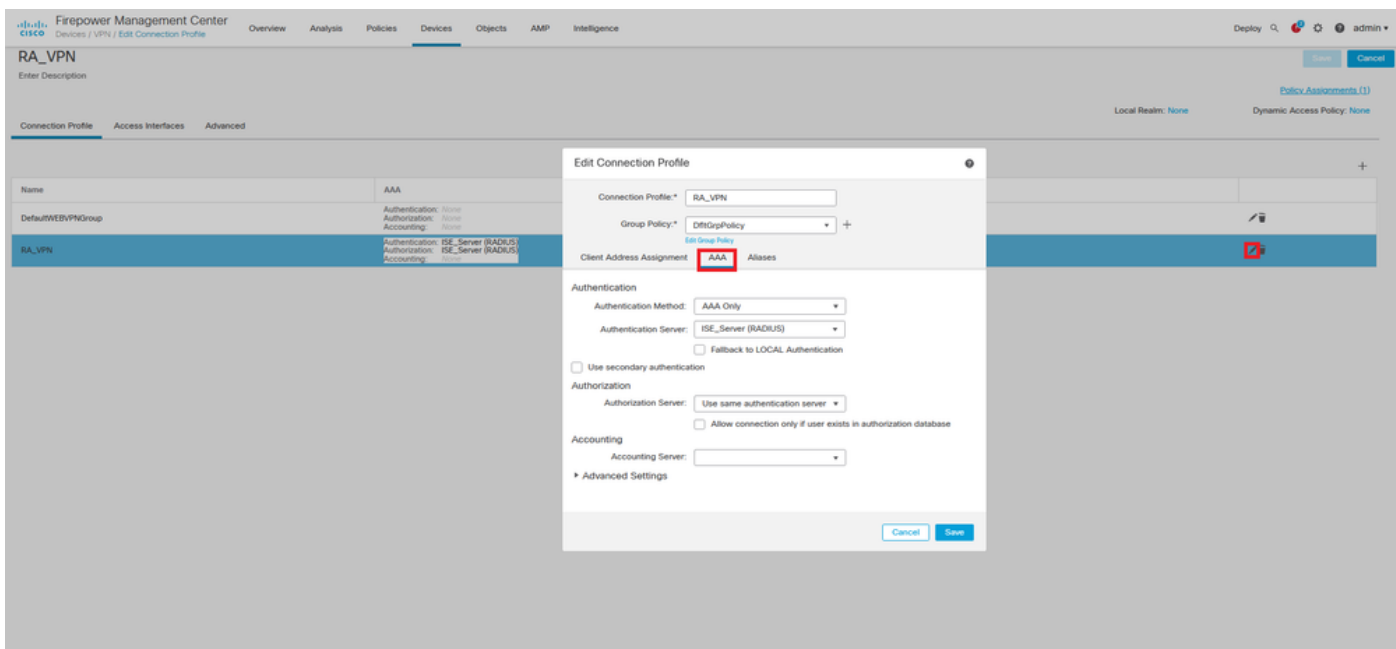


通過FMC配置具有AAA/RADIUS身份驗證的RA VPN

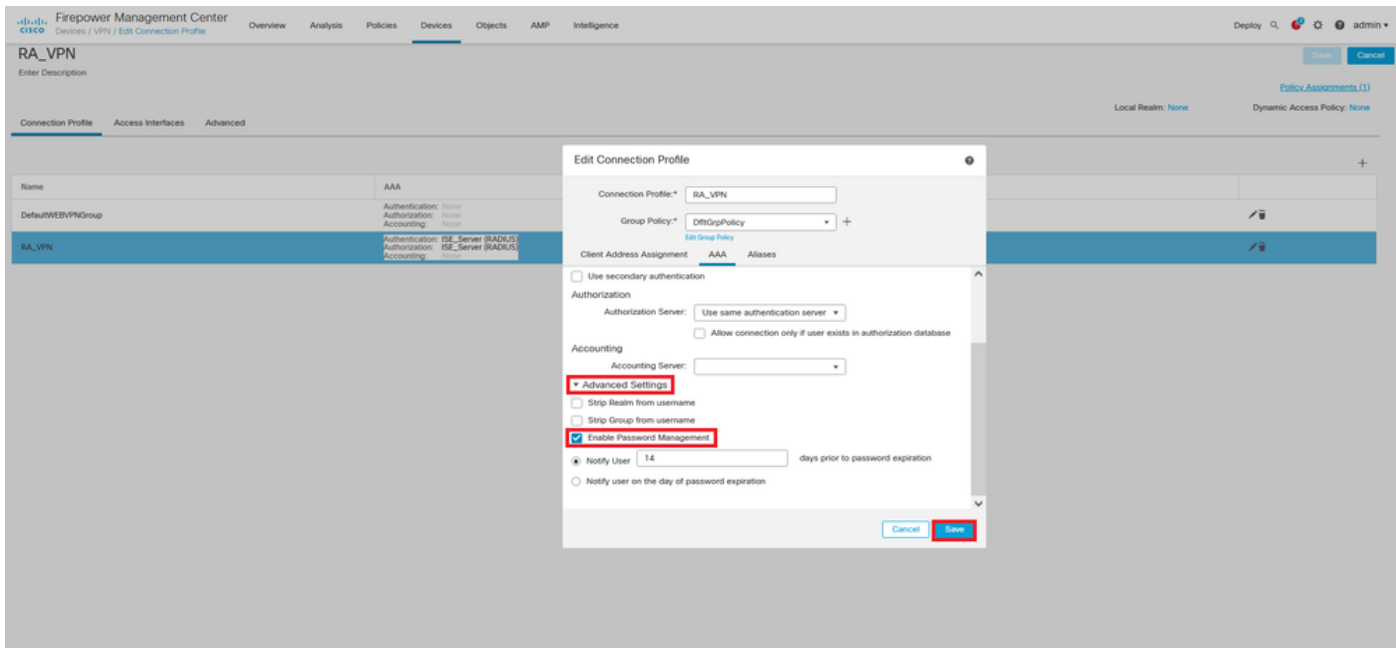
如需逐步程式，請參閱本檔案及以下影片：

- [FTD上的AnyConnect遠端存取VPN組態](#)
- [FMC管理的FTD的初始AnyConnect配置](#)

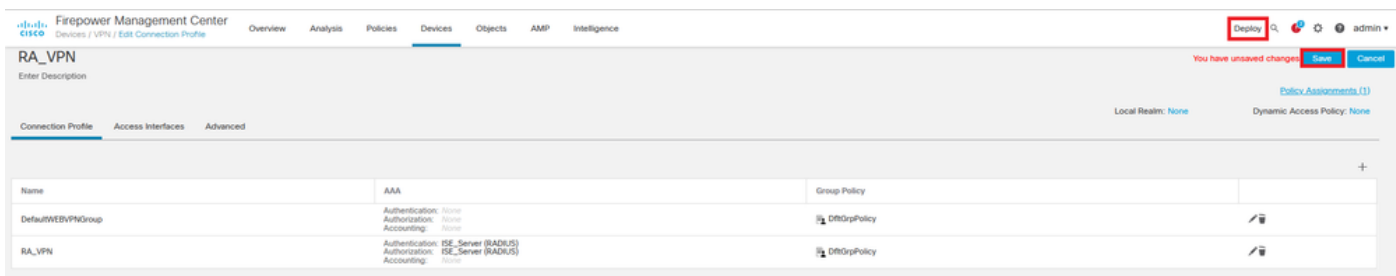
步驟1.配置遠端訪問VPN後，導航到**Devices > Remote Access**，編輯新建立的連線配置檔案，然後導航到**AAA**頁籤。



展開Advanced Settings部分，然後按一下Enable Password Management竅取方塊。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

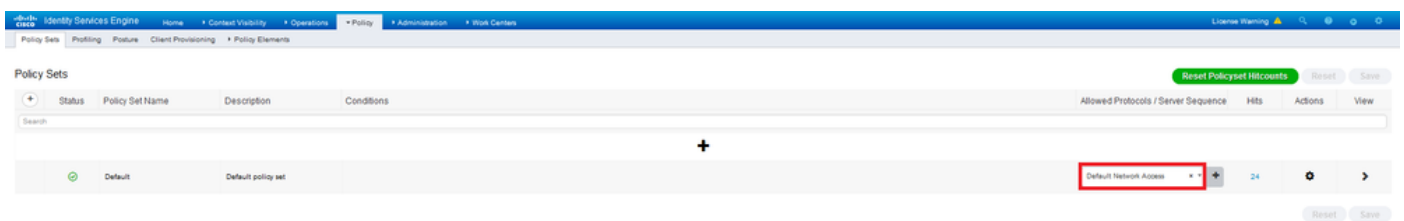
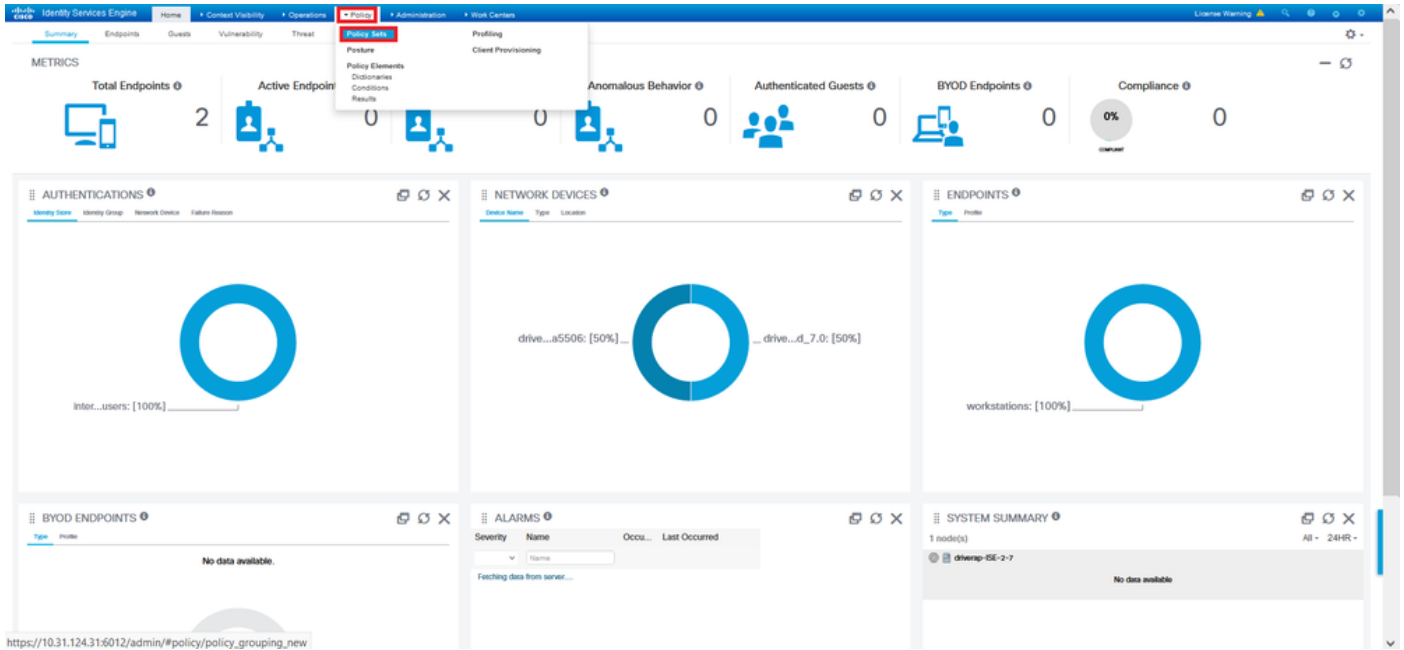
```

配置ISE以支援MS-CHAPv2作為身份驗證協定

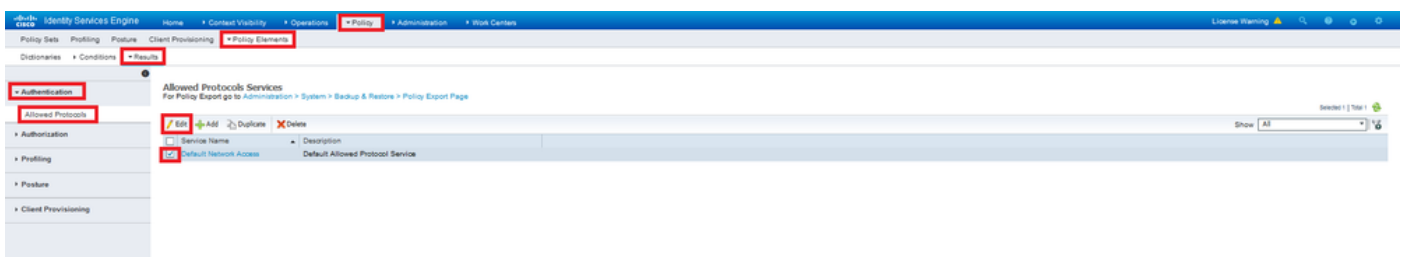
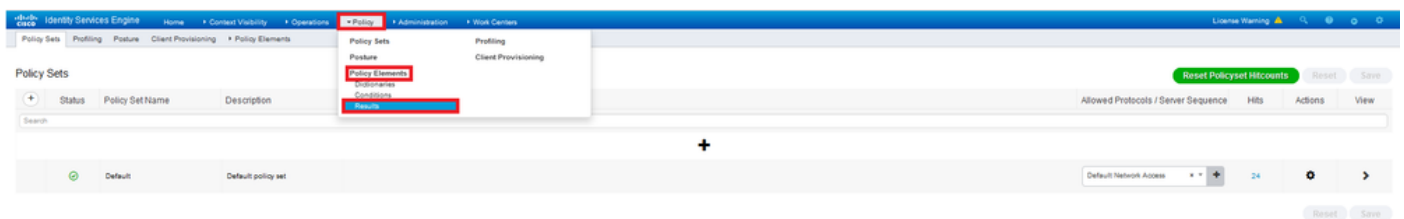
假設：

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。

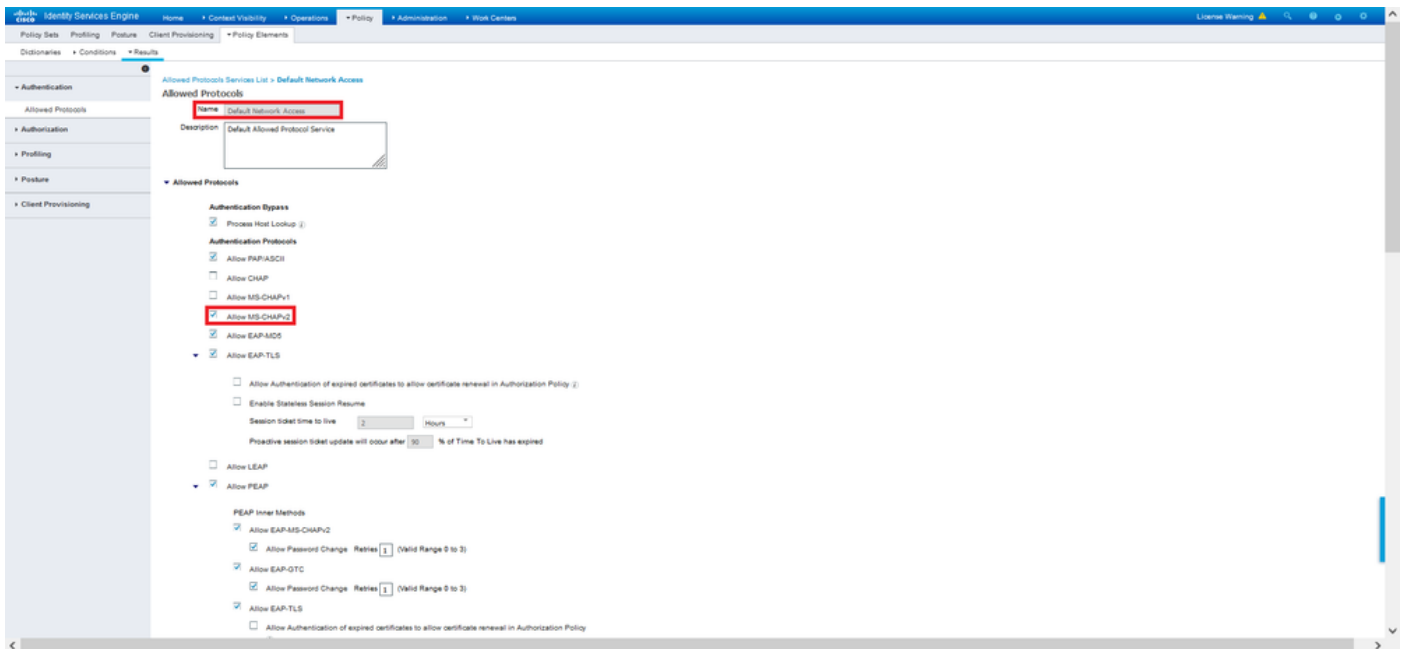
步驟2. 導覽至Policy > Policy Sets，並找到Allowed Protocols策略附加到您的AnyConnect使用者進行身份驗證的策略集。在本示例中，僅存在一個策略集，因此所討論的策略是預設網路訪問。



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

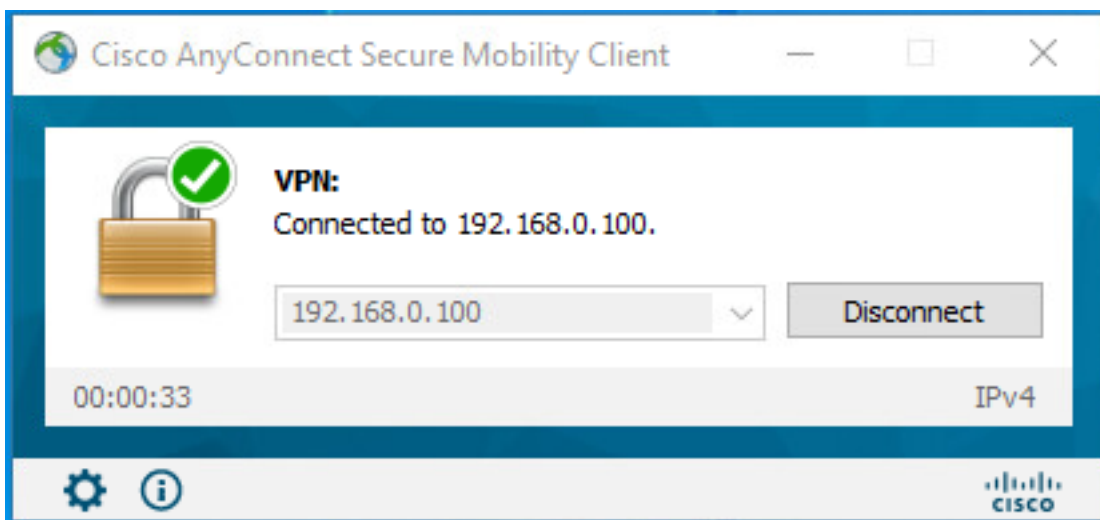


確保選中Allow MS-CHAPv2覈取方塊。一直向下滾動，然後儲存它。



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：

Identity Services Engine

Overview

Event	5200 Authentication succeeded
Username	user1
Endpoint Id	00 50 50 90 40 0F 0
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Static IP Address User 1
Authorization Result	StaticIPAddressUser1

Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 15049 Evaluating Policy Group
- 15058 Evaluating Service Selection Policy
- 15041 Evaluating Identity Policy
- 15043 Queried PIP - Normalised RADIUS Radius/ForType (4 times)
- 22072 Selected Identity source sequence - All_User_ID_Stores
- 15019 Selected Identity Source - Internal Users
- 24210 Looking up User in Internal Users IDStore - user1
- 24212 Found User in Internal Users IDStore
- 22037 Authentication Passed
- 24719 ISE has not confirmed locally previous successful machine authentication for user in Active Directory
- 15036 Evaluating Authorization Policy
- 24209 Looking up Endpoint in Internal Endpoints IDStore - user1
- 24211 Found Endpoint in Internal Endpoints IDStore
- 15045 Queried PIP - Radius User Name
- 15018 Selected Authorization Profile - StaticIPAddressUser1
- 22081 Max session policy passed
- 22080 New accounting session created in Session cache
- 11002 Returned RADIUS Access-Accept

Authentication Details

Source Timestamp	2021-09-28 00:00:02.94
Received Timestamp	2021-09-28 00:00:02.94
Policy Server	drvrapp-ISE-0-7
Event	5200 Authentication succeeded
Username	user1
User Type	User
Endpoint Id	00 50 50 90 40 0F 0
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	d8a30054000a000e1025c49
Authentication Method	MSCHAPV2
Authentication Protocol	MSCHAPV2
Network Device	DRIVERAP_JTD_7-0
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	0.0.0.0

Identity Services Engine

NAS Port Type	Virtual
Authorization Profile	StaticIPAddressUser1
Response Time	231 milliseconds

Other Attributes

ConfigVersionId	147
DestinationPort	1812
Protocol	Radius
NAS-Port	57344
Tunnel-Client-Endpoint	(tag=0) 192.168.0.101
MS-CHAP-Challenge	0F 4F54 9F 45 0F 4F 50 42 50 97 19 57 5E A8 08
MS-CHAP2-Response	00 00 00 00 00 20 04 45 8 12 07 8a 20 0c a1 19 45 a0 00 00 00 00 00 00 00 00 05 4f 29 52 90 5a 2ca1 d9 a7 50 3c f0 8a 73 32 a9 50 54 27 0a 5d 99
CVPR3000ASAPROK7x Tunnel-Group-Name	RA_VPN
NetworkDeviceProfileId	b0099005-3150-4215-a80a-d753a45b850a
IsThirdPartyDeviceFlow	false
CVPR3000ASAPROK7x Client-Type	2
AcxSessionId	drvrapp-ISE-0-7-1417494978-25
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	All_AD_Icon_Points
SelectedAuthenticationIdentityStores	Guest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Static IP Address User 1
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default
DTLS Support	Unknown
HostIdentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco

Location	LocationAll Locations
Device Type	Device TypeAll Device Types
IPSEC	IPSECOnly IPSEC DeviceOnly
EnableFlag	Enabled
RADIUS Username	user1
Device IP Address	192.168.0.100
CPM Session ID	d8a30054000a000e1025c49
Called-Station-ID	192.168.0.100
CiscoAPPar	mdm-dm-device-platform=main,mdm-dm-device-manage=00-50-50-90-40-0f,mdm-dm-device-platform-version=10.0.18.352,mdm-dm-device-publication-id=00-50-50-90-40-0f,mdm-dm-user-agent=AnyConnect,Windows 4.10.22080,mdm-dm-device-type=VMware, Inc. VMware Virtual Platform,mdm-dm-device-uid,global=158788020F52F32C0E2431405F4BA2AE2C0B3,mdm-dm-device-user=3C38427071F90782F816F124621184408698C71E37D388CC03DF94AC8880344,audit-session-id=d8a30054000a000e1025c49,@source-ip=192.168.0.101,00a-push=true

Result

Framed IP Address	10.0.50.101
Class	CACS-d8a30054000a000e1025c49 drvrapp-ISE-0-7-1417494978-25
class-av-pair	profile-name=Windows10-Workstation
MS-CHAP2-Success	00 03 3e 33 30 33 40 33 30 37 38 34 42 43 45 32 33 45 41 31 39 37 37 32 44 48 39 30 39 44 41 39 37 31 39 44 38 41 43 49 43 41
LicenseTypes	Base license consumed

Session Events

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