RADIUS를 통해 MSCHAPv2를 사용하여 FTD 원격 액세스 VPN 구성

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[배경 정보](#)
[구성](#)
[네트워크 다이어그램](#)
[FMC를 통해 AAA/RADIUS 인증을 사용하여 RA VPN 구성](#)
[MS-CHAPv2를 인증 프로토콜로 지원하도록 ISE 구성](#)
[다음을 확인합니다.](#)
[문제 해결](#)

소개

이 문서에서는 RADIUS(Remote Authentication Dial-In User Service) 인증을 사용하는 원격 액세스 VPN 클라이언트에 대해 FMC(Firepower Management Center)를 통한 인증 방법으로 MS-CHAPv2(Microsoft Challenge Handshake Authentication Protocol version 2)를 활성화하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FTD(Firepower Threat Defense)
- FMC(Firepower Management Center)
- Identity Services Engine(ISE)
- Cisco AnyConnect Secure Mobility Client
- RADIUS 프로토콜

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- FMCv - 7.0.0(빌드 94)
- FTDv - 7.0.0(빌드 94)
- ISE - 2.7.0.356

- AnyConnect - 4.10.02086
- Windows 10 Pro

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

기본적으로 FTD는 AnyConnect VPN 연결을 위해 RADIUS 서버를 사용하는 인증 방법으로 PAP(Password Authentication Protocol)를 사용합니다.

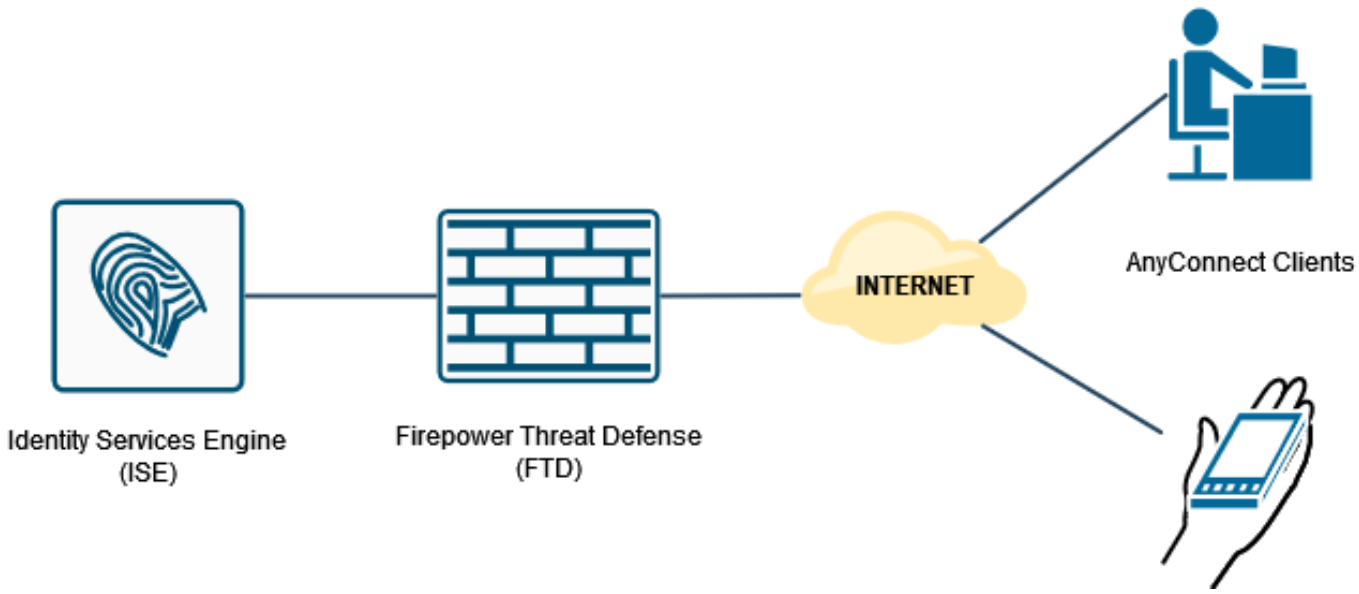
PAP는 사용자가 양방향 핸드셰이크로 ID를 설정할 수 있는 간단한 방법을 제공합니다. PAP 비밀번호는 공유 암호로 암호화되며 가장 정교한 인증 프로토콜입니다. PAP는 반복적인 시도 및 오류 공격으로부터 거의 보호를 제공하지 않으므로 강력한 인증 방법이 아닙니다.

MS-CHAPv2 인증에서는 피어 및 암호 변경 기능 간의 상호 인증을 도입합니다.

VPN 연결을 위해 ASA와 RADIUS 서버 간에 사용되는 프로토콜로 MS-CHAPv2를 활성화하려면 연결 프로파일에서 비밀번호 관리를 활성화해야 합니다. 비밀번호 관리를 활성화하면 FTD에서 RADIUS 서버로 MS-CHAPv2 인증 요청이 생성됩니다.

구성

네트워크 다이어그램



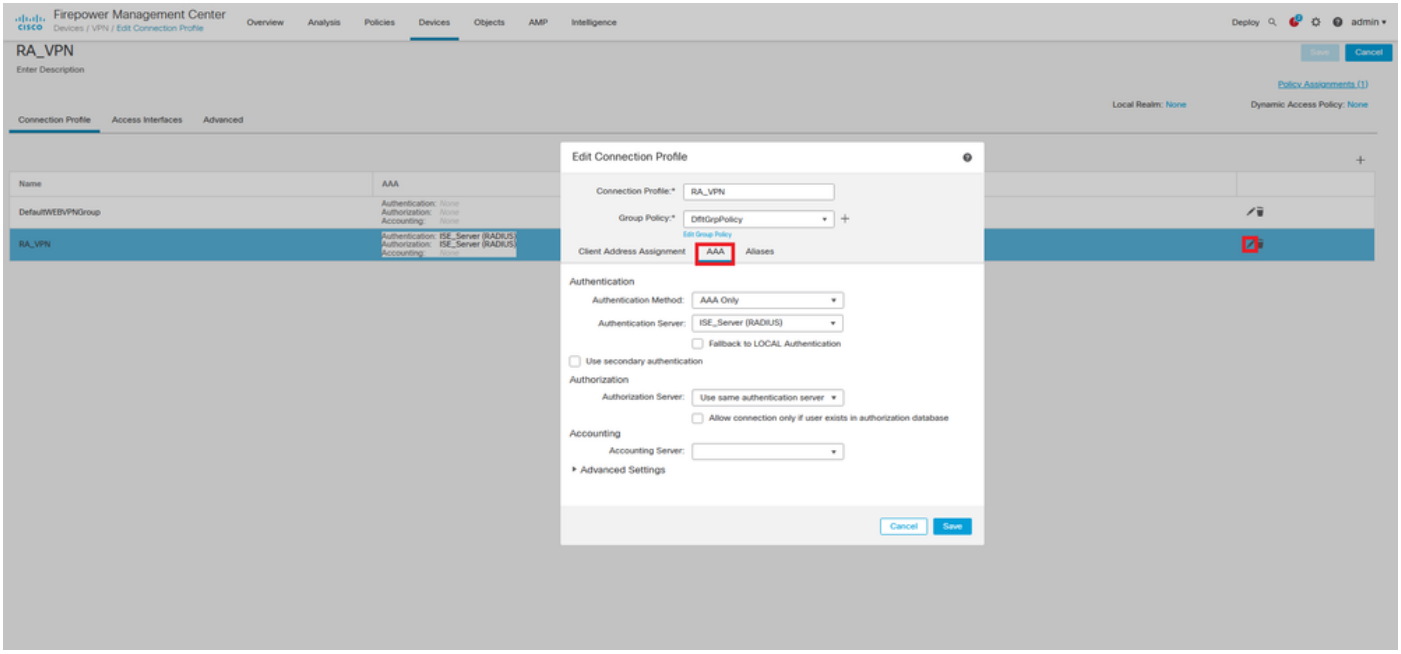
FMC를 통해 AAA/RADIUS 인증을 사용하여 RA VPN 구성

단계별 절차는 이 문서와 다음 비디오를 참조하십시오.

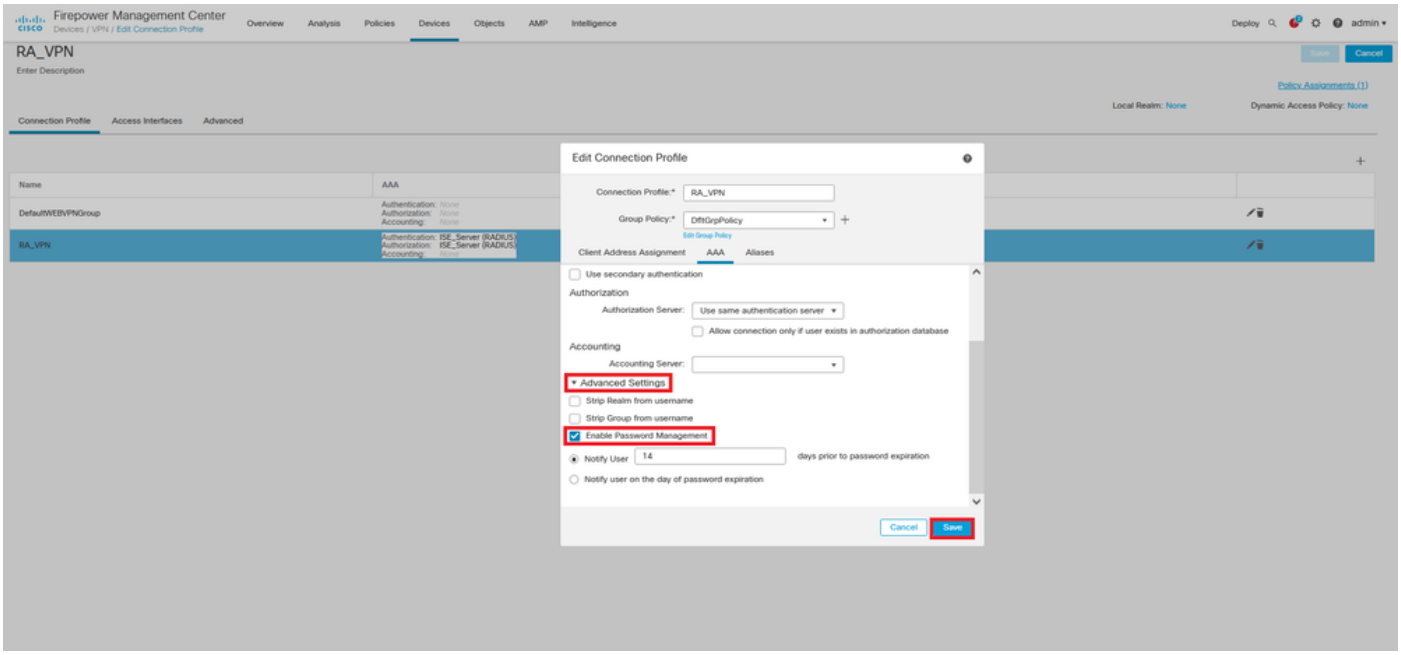
- FTD의 AnyConnect 원격 액세스 VPN 컨피그레이션
- FMC에서 관리하는 FTD의 초기 AnyConnect 컨피그레이션

1단계. Remote Access VPN이 구성되면 **Devices(디바이스) > Remote Access(원격 액세스)**로 이동

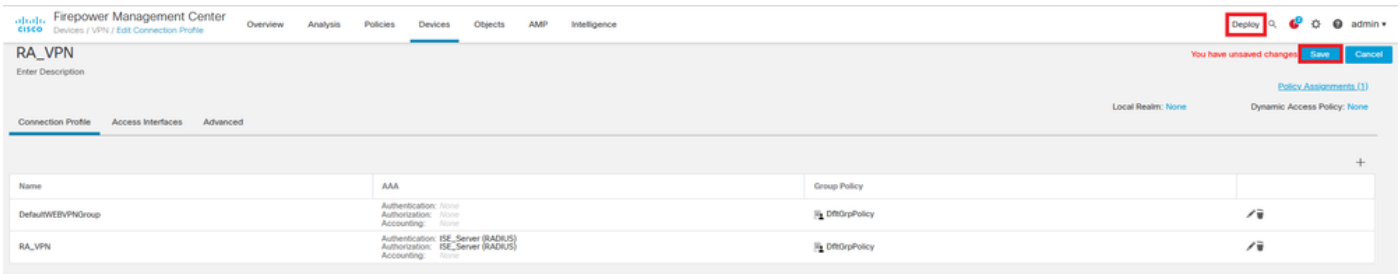
하고 새로 생성된 Connection Profile(연결 프로파일)을 수정한 다음 **AAA** 탭으로 이동합니다.



Advanced Settings(**고급 설정**) 섹션을 확장하고 Enable Password **Management(비밀번호 관리 활성화**) 확인란을 클릭합니다. 저장을 **클릭합니다**.



저장 및 **구축**.



FTD CLI의 원격 액세스 VPN 컨피그레이션은 다음과 같습니다.

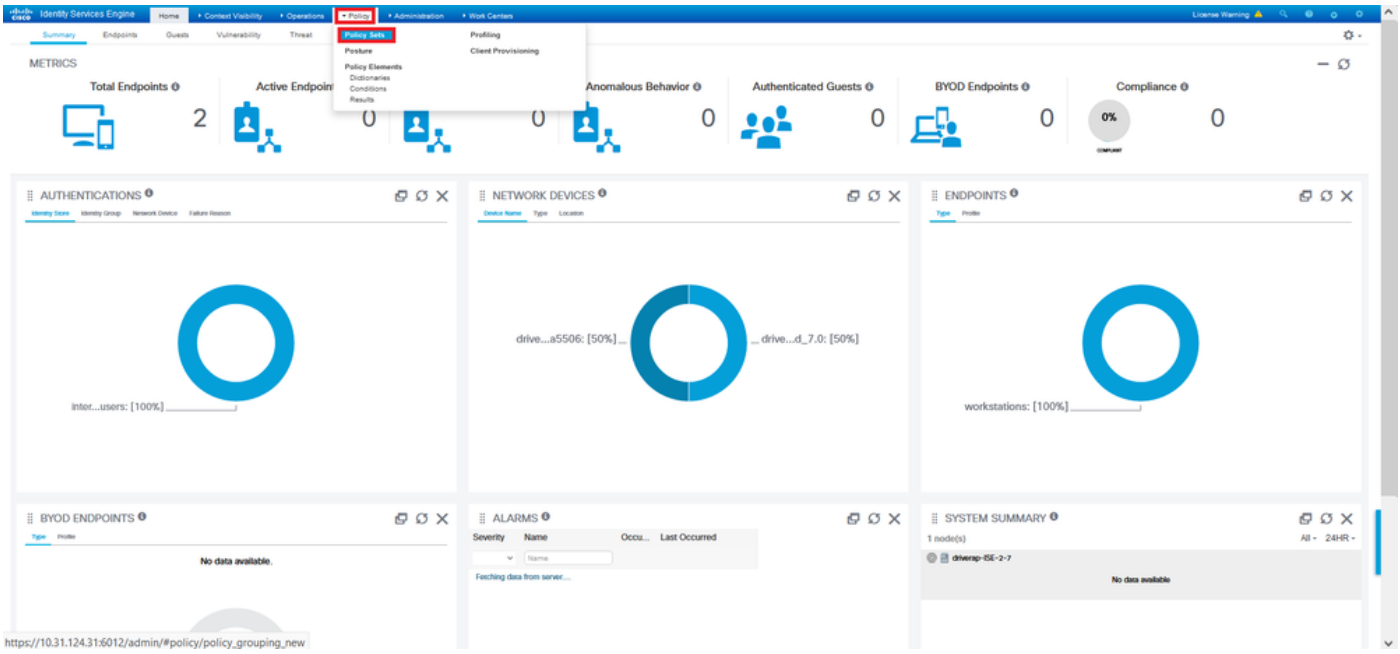
```
ip local pool AC_Pool 10.0.50.1-10.0.50.100 mask 255.255.255.0

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
```

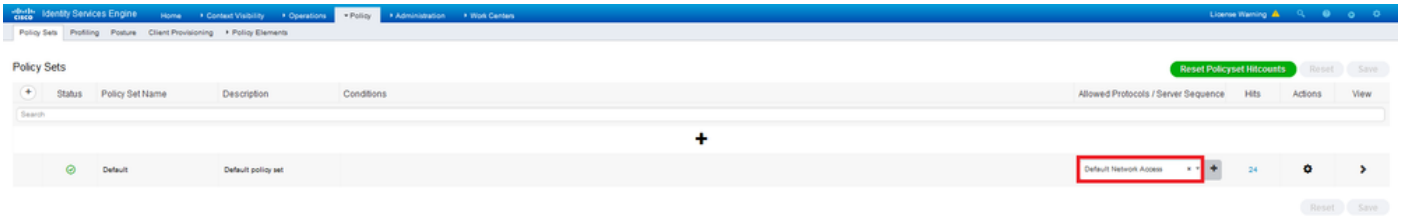
MS-CHAPv2를 인증 프로토콜로 지원하도록 ISE 구성

다음과 같은 것으로 가정합니다.

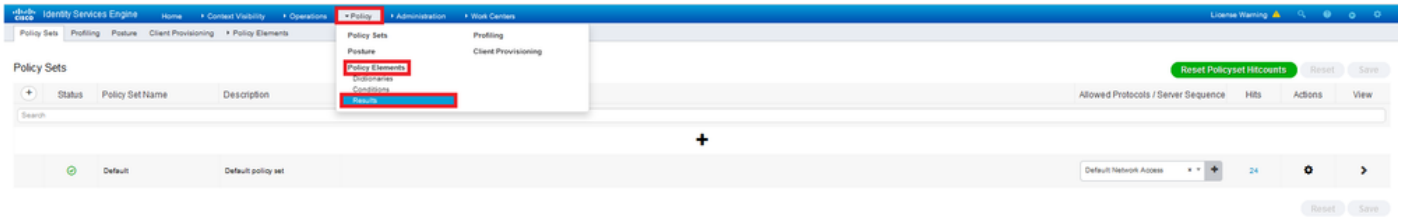
1. FTD는 이미 ISE의 네트워크 디바이스로 추가되어 FTD에서 RADIUS 액세스 요청을 처리할 수 있습니다.
2. ISE에서 AnyConnect 클라이언트를 인증할 수 있는 사용자가 하나 이상 있습니다.

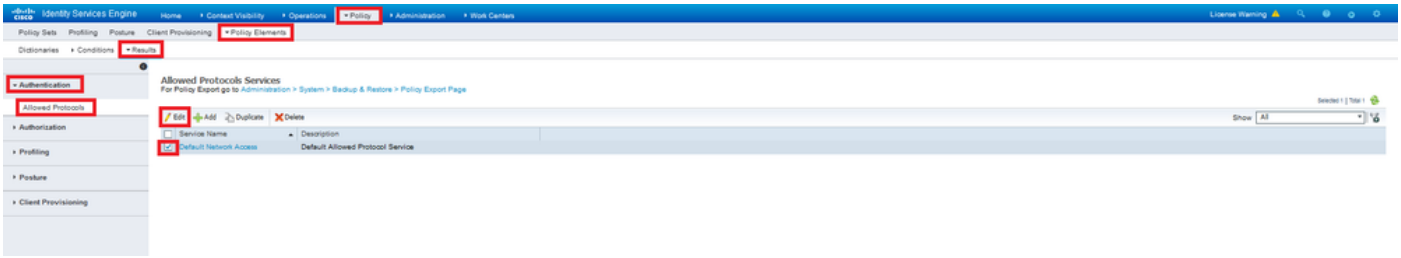
2단계. Policy(**정책) > Policy Sets(정책 세트)**로 이동하고 AnyConnect 사용자가 인증되는 정책 세트에 연결된 **Allowed Protocols**(허용된 프로토콜) 정책을 찾습니다. 이 예에서는 하나의 정책 집합만 있으므로 해당 정책이 *Default Network Access*입니다.



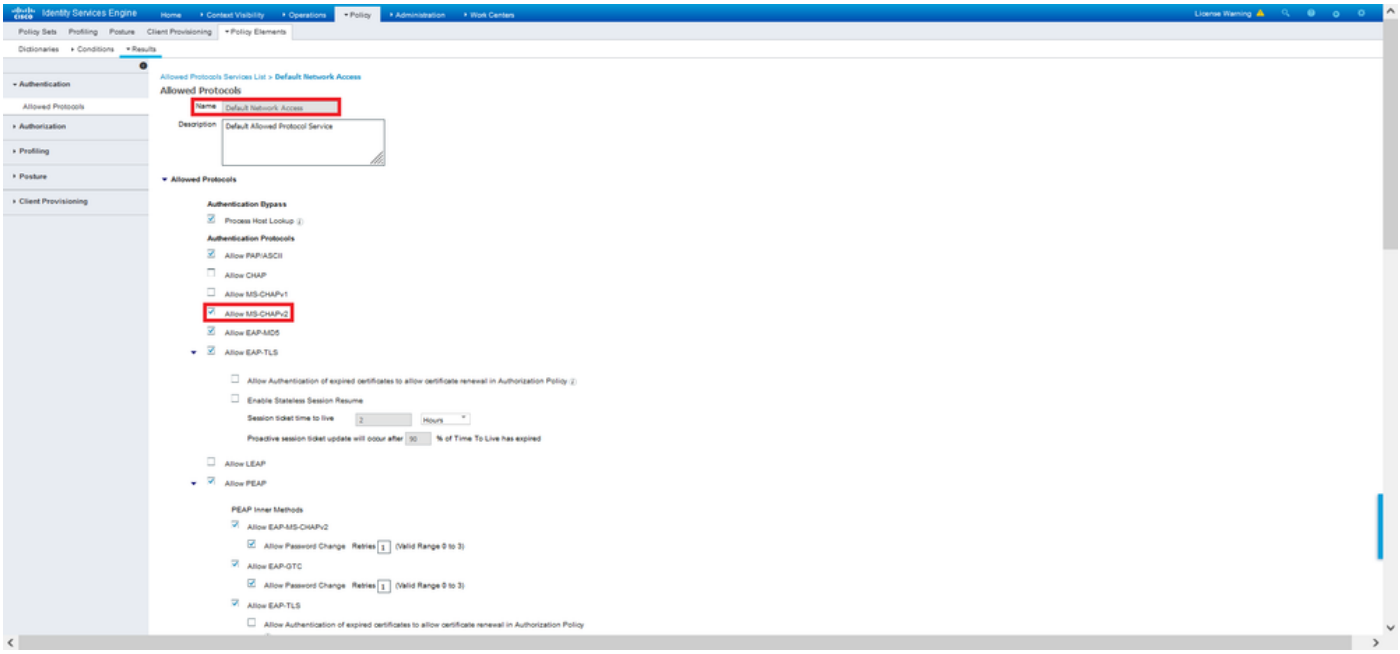


3단계. Policy(정책) **> Policy Elements(정책 요소) > Results(결과)로 이동합니다.** Authentication(**인증) > Allowed Protocols(허용된 프로토콜)** 아래에서 Default Network Access(**기본 네트워크 액세스**)**를** 선택하고 **편집합니다**.



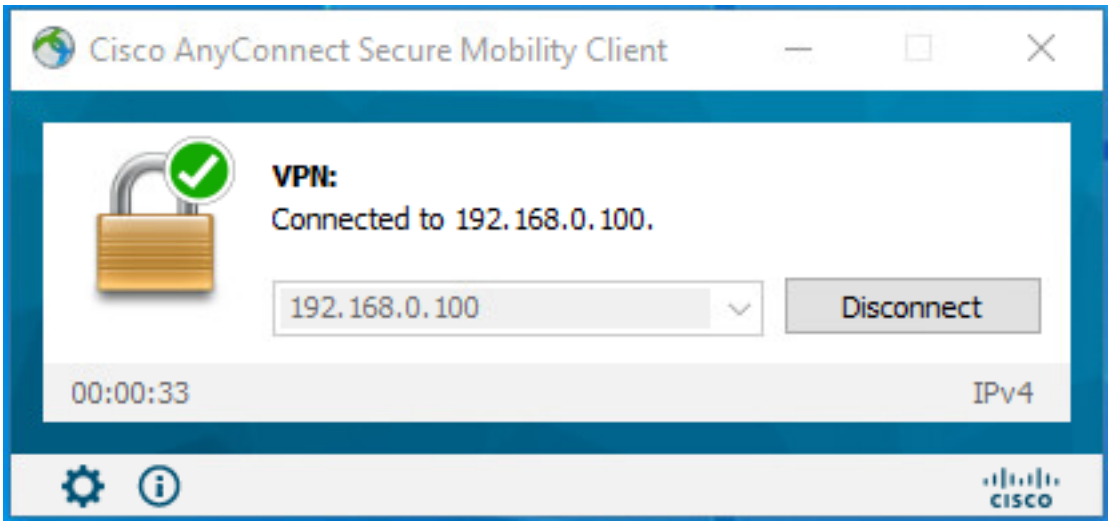


Allow **MS-CHAPv2(ms-CHAPv2 허용)** 확인란이 선택되었는지 확인합니다. 아래로 스크롤해서 **저장**.

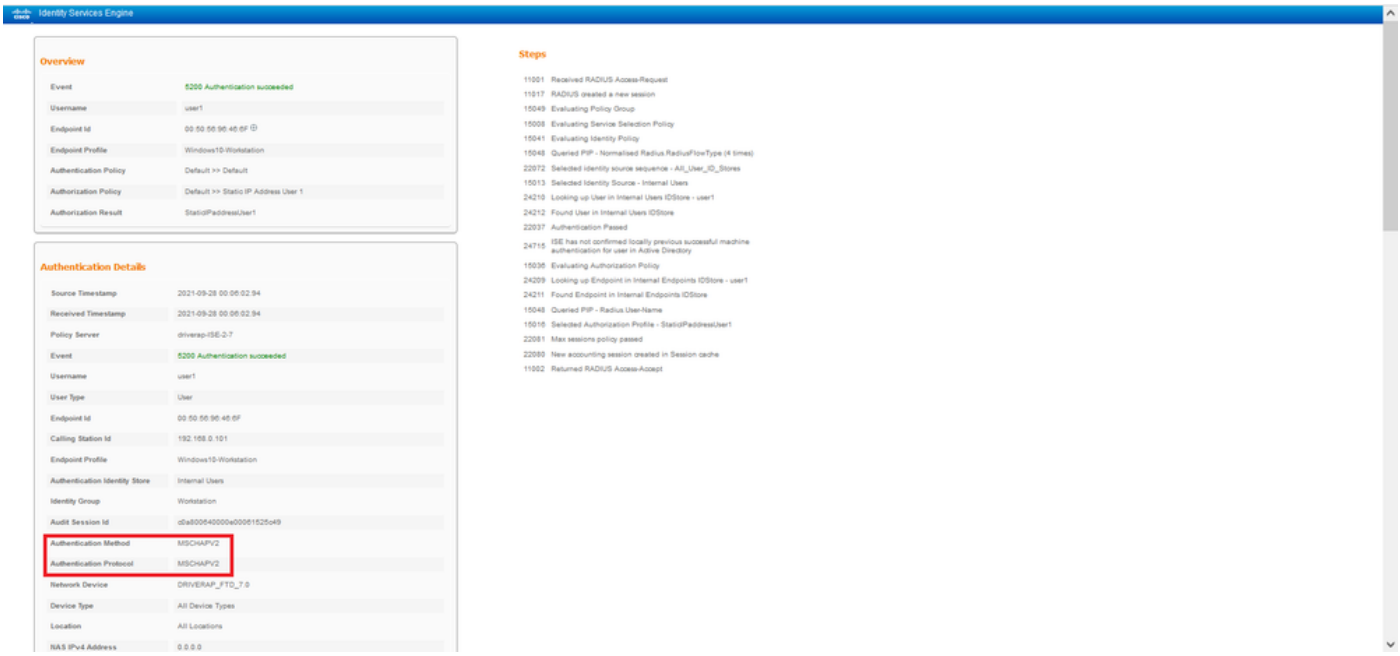


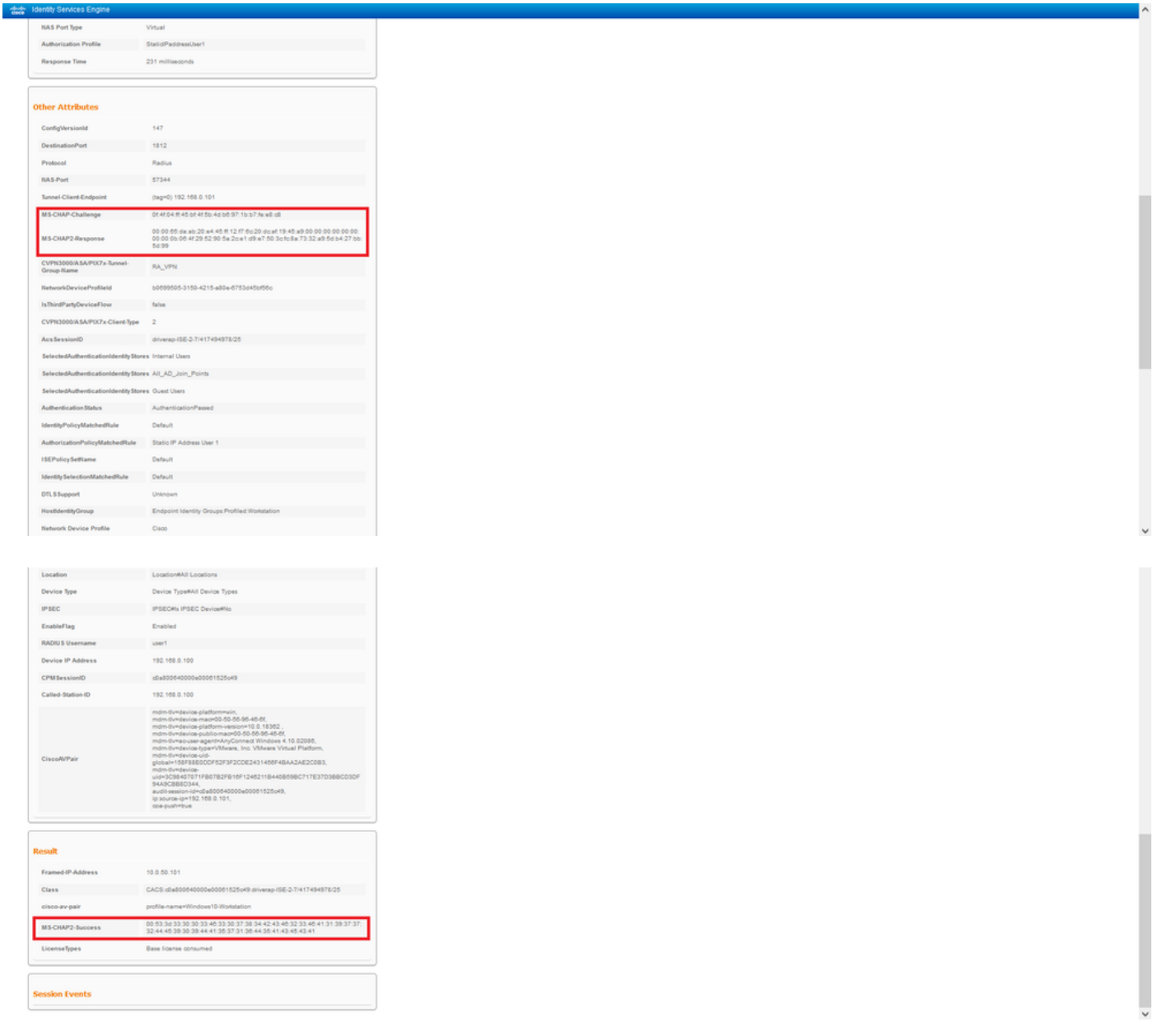
다음을 확인합니다.

Cisco AnyConnect Secure Mobility 클라이언트가 설치된 클라이언트 시스템으로 이동합니다. FTD 헤드엔드(이 예에서는 Windows 시스템이 사용됨)에 연결하고 사용자 자격 증명을 입력합니다.



ISE의 RADIUS Live Logs에는 다음이 표시됩니다.





참고: **test aaa-server authentication** 명령은 항상 PAP를 사용하여 인증 요청을 RADIUS 서버

로 전송하므로 방화벽에서 MS-CHAPv2를 이 명령과 함께 사용하도록 강제할 방법이 없습니다.

firepower# **테스트 aaa-server 인증 ISE_Server 호스트 172.16.0.8 사용자 이름 user1 비밀번호 XXXXXX**
정보: IP 주소에 대한 인증 테스트 시도(172.16.0.8)(시간 제한: 12초)
정보: 인증 성공

참고: AnyConnect VPN(SSL 및 IPSec) 연결에 대해 RADIUS를 통해 협상된 인증 프로토콜에는 영향을 주지 않으므로 Flex-config를 통해 **터널 그룹 ppp** 특성을 수정하지 마십시오.

tunnel-group RA_VPN ppp 특성
인증 pap 없음
인증 chap
인증 ms chap-v1
인증 ms chap-v2 없음
인증 eap-proxy 없음

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

FTD:

- **디버그 radius 모두**

ISE에서:

- RADIUS 라이브 로그