FTD Remote Access VPN met MSCHAPv2 via RADIUS configureren

Inhoud

Inleiding

Dit document beschrijft hoe Microsoft Challenge Handshake Authentication Protocol, versie 2 (MS-CHAPv2), kan worden ingeschakeld als de verificatiemethode via Firepower Management Center (FMC) voor Remote Access VPN-clients met RADIUS-verificatie (Dial-In User Service (RADIUS).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Threat Defense (FTD)
- FireSIGHT Management Center (FMC)
- Identity Services Engine (ISE)
- Cisco AnyConnect beveiligde mobiliteit-client
- RADIUS-protocol

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- FMCv - 7.0.0 (bouw 94)
- FTDv - 7.0.0 (gebouwd 94)
- ISE - 2.7.0.356

- AnyConnect - 4.10.2086
- Windows 10 Pro

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

In de standaardinstelling gebruikt FTD Password Authentication Protocol (PAP) als de authenticatiemethode met RADIUS-servers voor AnyConnect VPN-verbindingen.

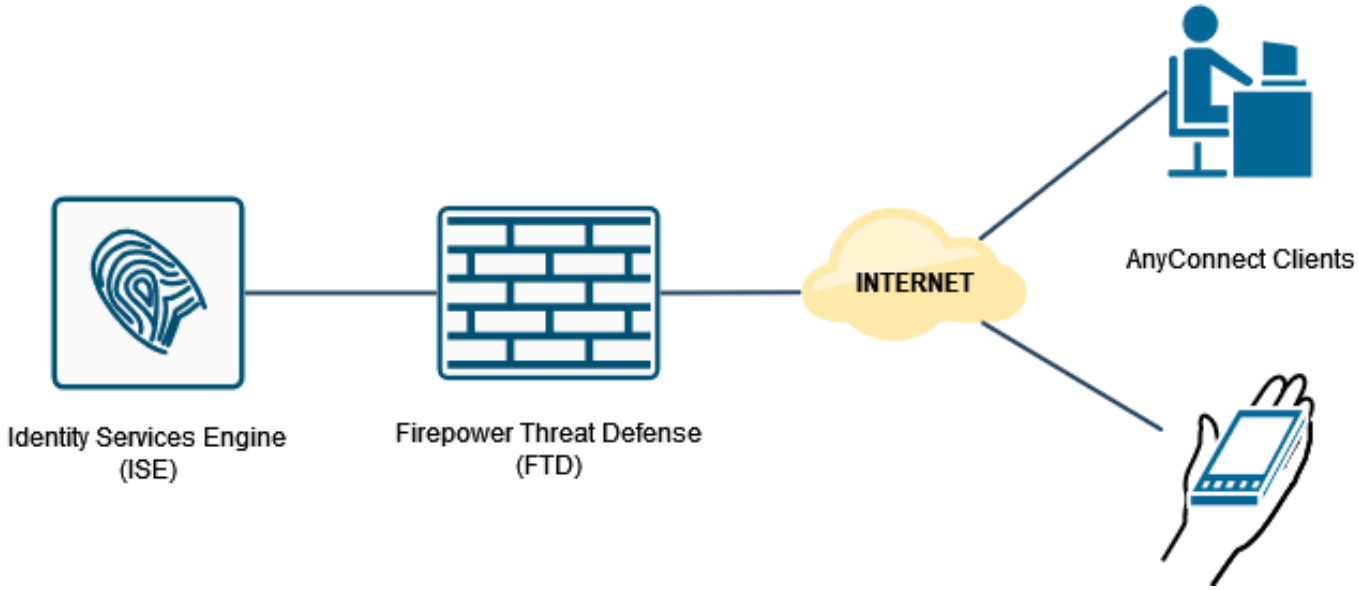
PAP biedt een eenvoudige methode voor gebruikers om hun identiteit vast te stellen met een tweevoudige handdruk. Het PAP-wachtwoord wordt versleuteld met een gedeeld geheim en is het minst gesofisticeerde verificatieprotocol. PAP is geen sterke authenticatiemethode omdat het weinig bescherming biedt tegen herhaalde trial-and-error aanvallen.

MS-CHAPv2 verificatie introduceert wederzijdse authenticatie tussen peers en een wachtwoordfunctie.

Om MS-CHAPv2 als protocol in te schakelen dat tussen de ASA en de RADIUS-server wordt gebruikt voor een VPN-verbinding, moet het wachtwoordbeheer in het verbindingsprofiel worden ingeschakeld. Bij het inschakelen van het wachtwoordbeheer wordt een aanvraag voor MS-CHAPv2-verificatie van de FTD naar de RADIUS-server gegenereerd.

Configureren

Netwerkdiagram

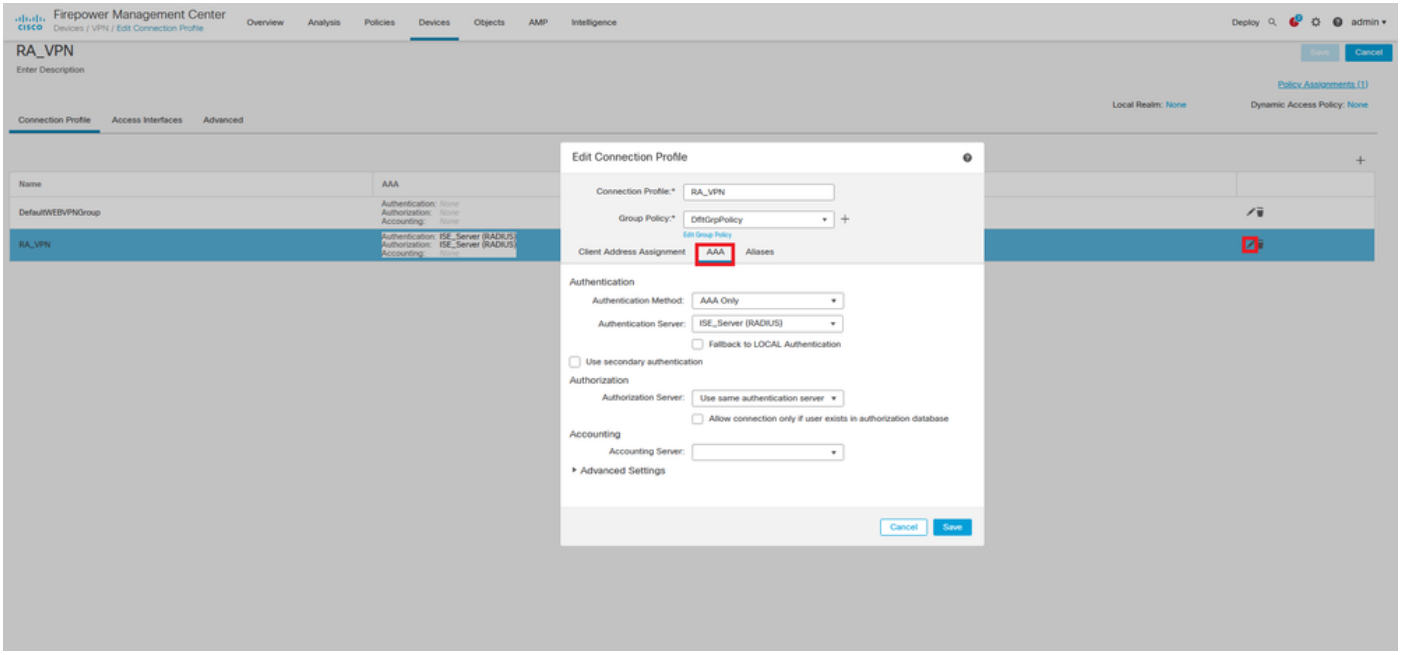


RA VPN-verificatie met AAA/RADIUS-verificatie via FMC configureren

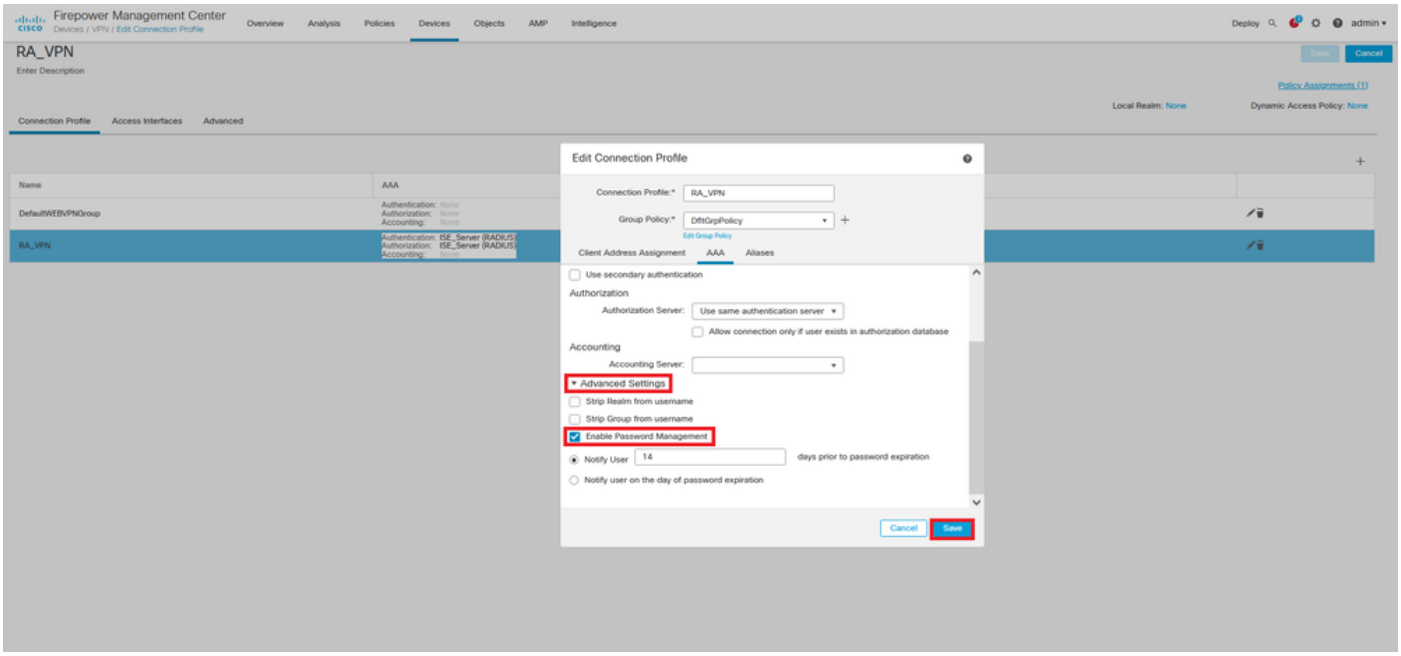
Verwijs voor een stap voor stap naar dit document en deze video:

- AnyConnect Remote Access VPN-configuratie op FTD
- Initiële AnyConnect-configuratie voor FTD beheerde door FMC

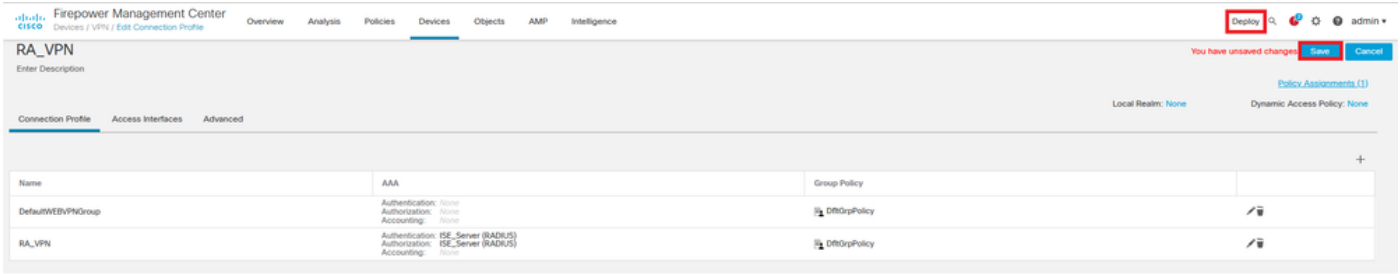
Stap 1. Nadat Remote Access VPN is geconfigureerd, navigeer naar **Apparaten > Externe toegang**, bewerkt het nieuwe verbindingsprofiel en navigeer vervolgens naar het **AAA**-tabblad.



Vul het gedeelte **Geavanceerde instellingen** uit en klik op het vakje **Wachtwoordbeheer inschakelen**. Klik op **Opslaan**.



Opslaan en **implementeren**.



Remote Access VPN-configuratie op FTD CLI is:

```
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
```

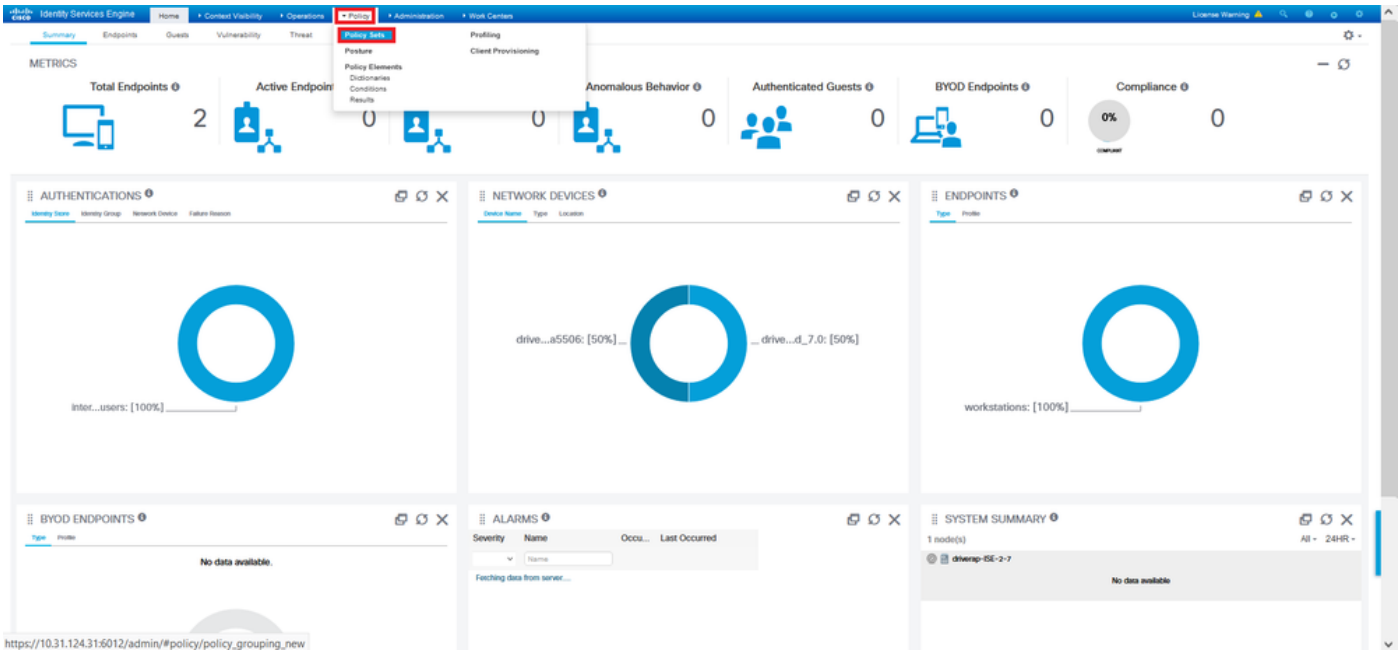
```
file-entry disable
file-browsing disable
url-entry disable
deny-message none

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
```

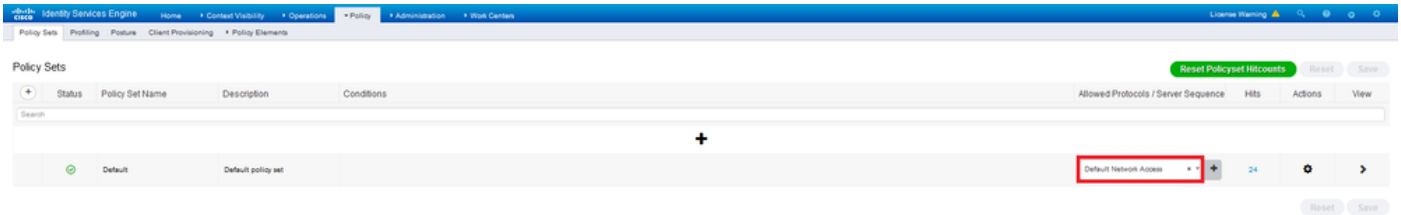
ISE configureren ter ondersteuning van MS-CHAPv2 als verificatieprotocol

Aangenomen wordt dat:

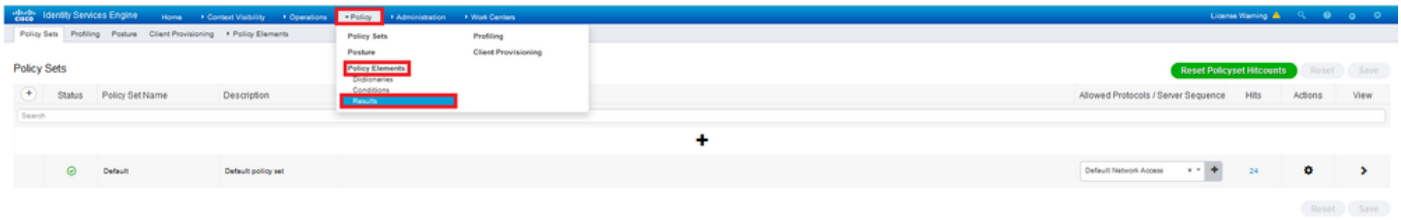
1. De FTD is al toegevoegd als netwerkapparaat op ISE zodat het RADIUS-toegangsaanvragen van de FTD kan verwerken.
2. Er is ten minste één gebruiker beschikbaar voor ISE om de AnyConnect-client te authentiseren.

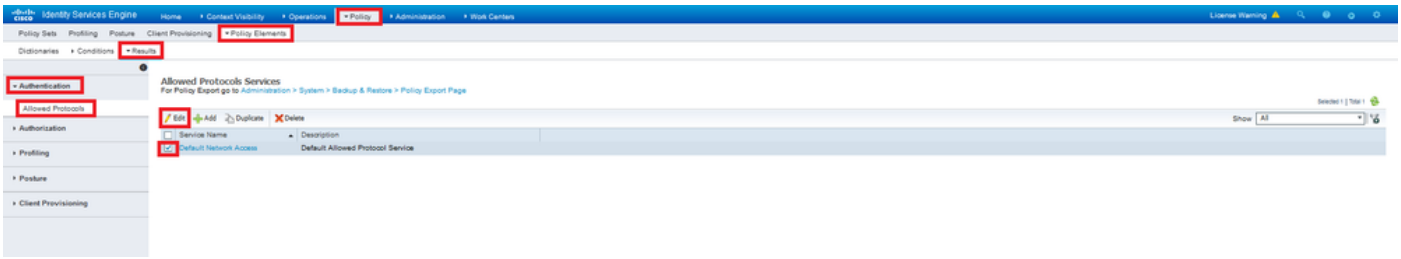
Stap 2. Navigeer naar **beleid > Beleidsformaten** en vind het **toegestane** beleid van **Protocollen** dat aan de beleidsset is toegevoegd en waar uw AnyConnect-gebruikers echt zijn bevonden. In dit voorbeeld is slechts één beleidsset aanwezig, zodat het beleid in kwestie *standaard netwerktoegang* is.



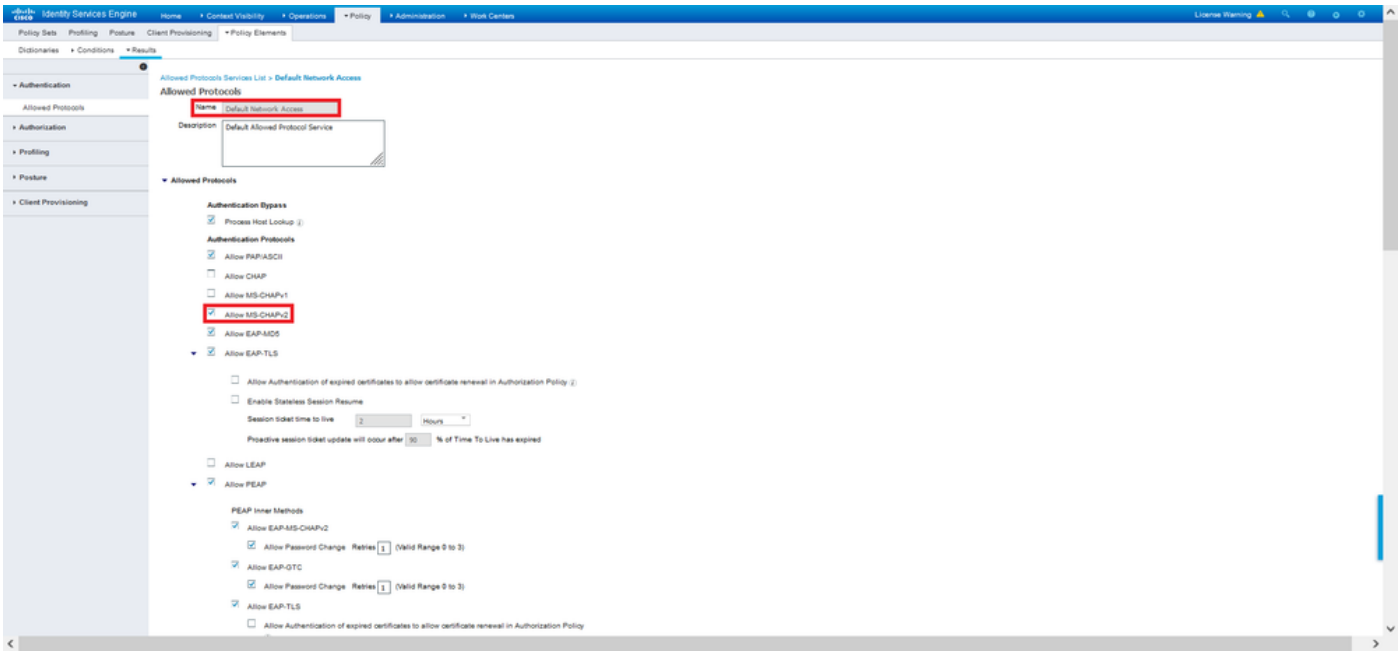


Stap 3. Navigeer in op **beleid > Beleidselementen > Resultaten.** Onder **Verificatie > Geboden protocollen** kiezen en bewerken **standaard netwerktoegang**.



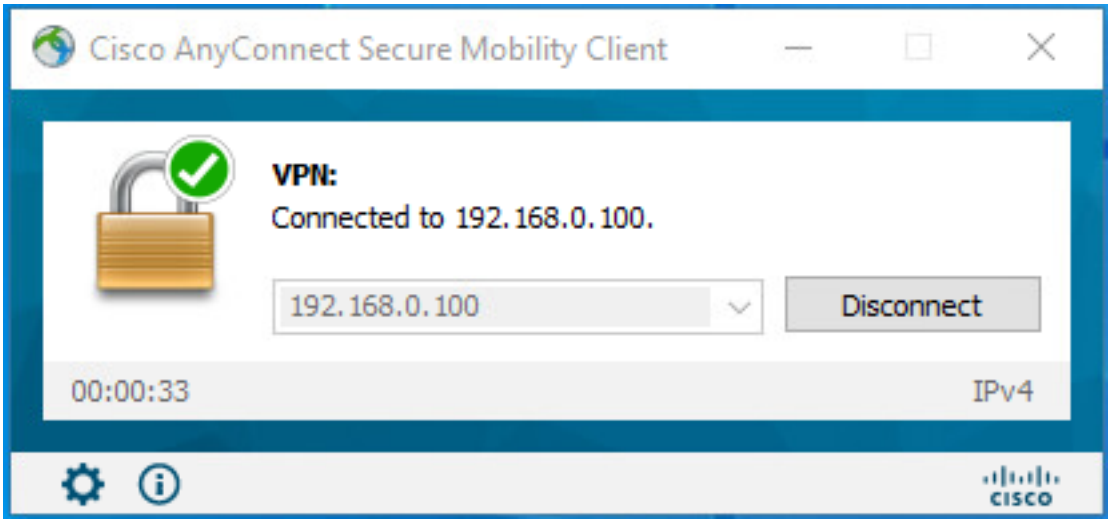


Controleer of het aanvinkvakje **Toestaan MS-CHAPv2** is ingeschakeld. Scrolt helemaal naar beneden en **bewaar** het.

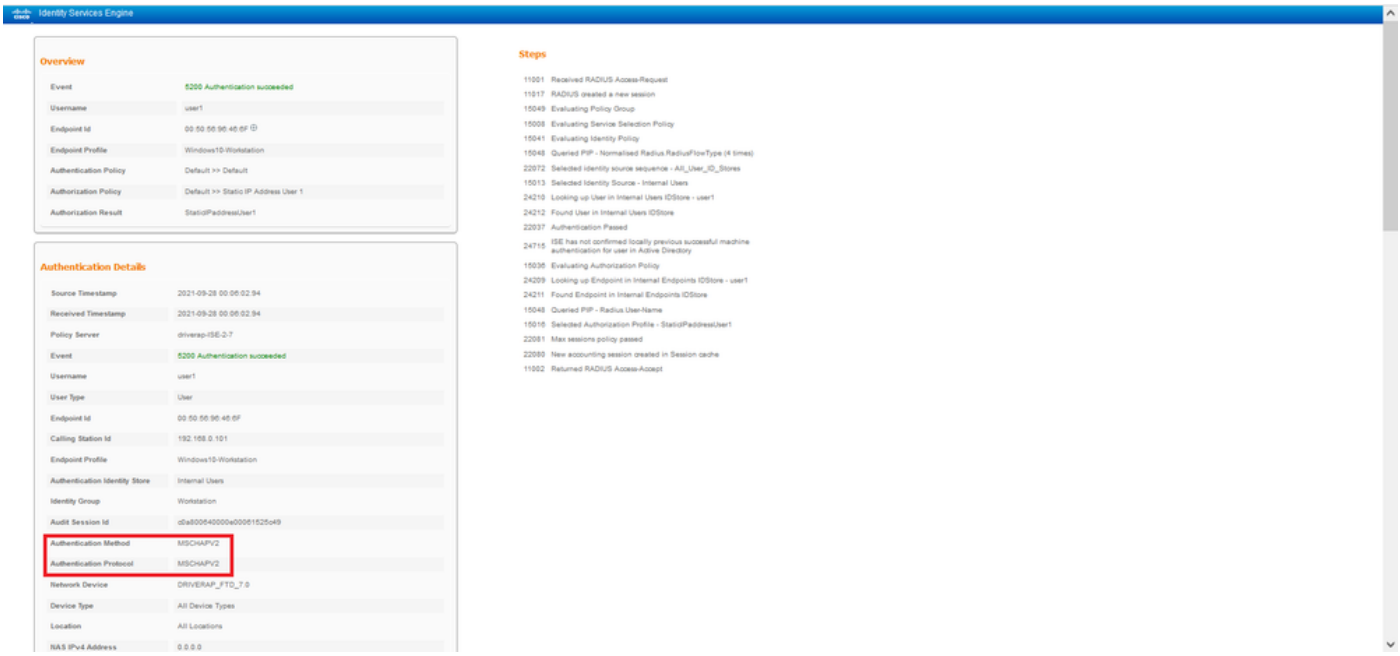


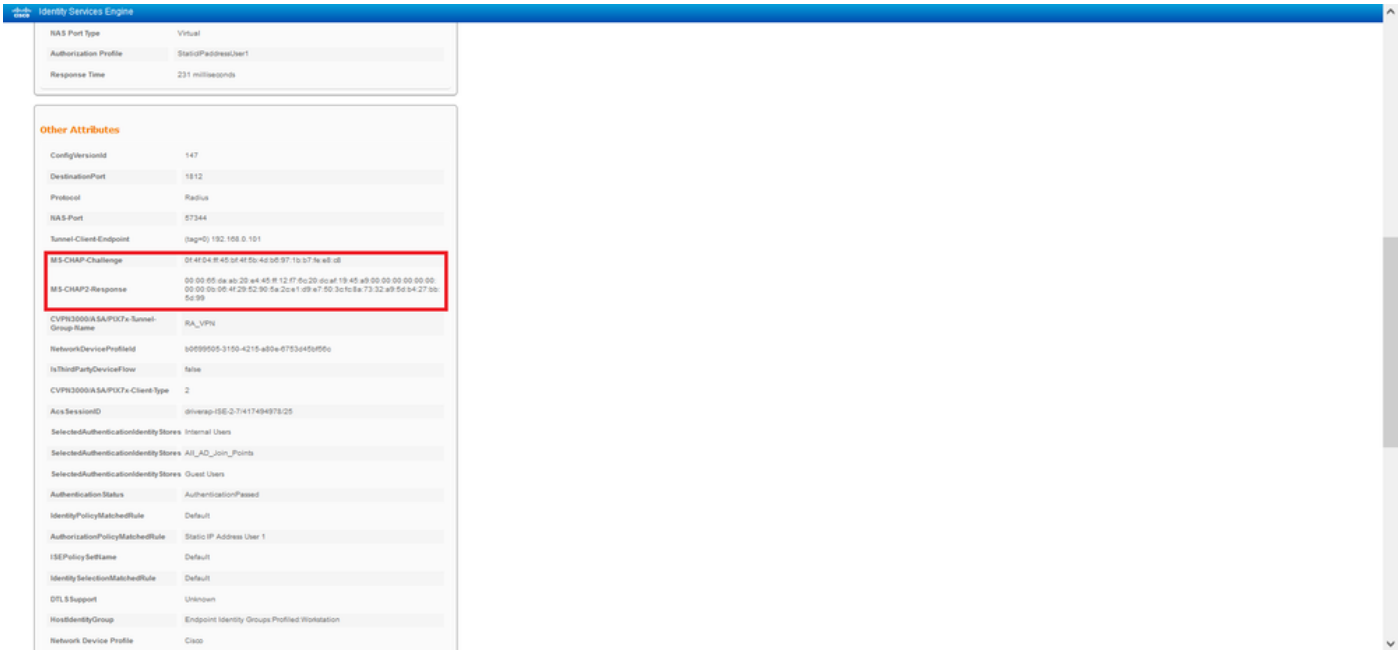
Verifiëren

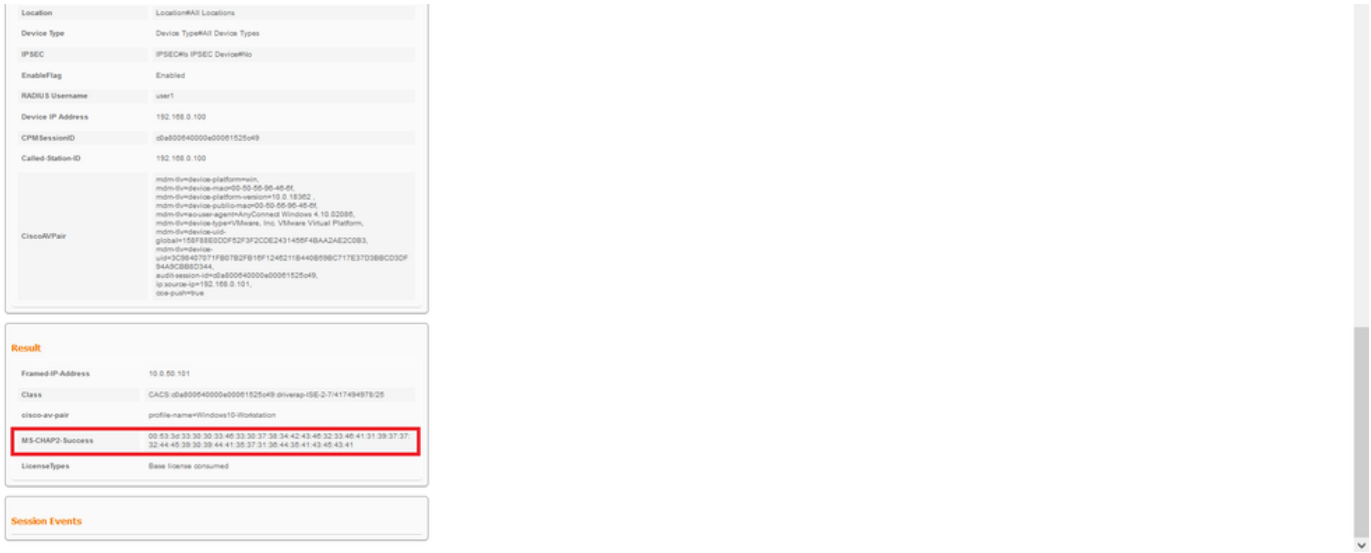
Navigeer naar uw clientmachine waar Cisco AnyConnect Secure Mobility client is geïnstalleerd. Sluit aan op het FTD head-end (een Windows-machine wordt in dit voorbeeld gebruikt) en typt de gebruikersreferenties.



De RADIUS Live Logs op ISE laten zien:







Opmerking: de opdracht **voor** verificatie **op** de **testaaa-server** gebruikt PP altijd om authenticatieverzoeken naar de RADIUS-server te verzenden, er is geen manier om de firewall te dwingen MS-CHAPv2 met deze opdracht te gebruiken.

Firepower# **test AAA-server verificatie ISE_Server host 172.16.0.8 gebruikersnaam1 wachtwoord XXXXXX**
INFORMATIE: Probeert de verificatietest naar IP-adres (172.16.0.8) (tijdelijke oplossing: 12 seconden)
INFORMATIE: Verificatiesucces

Opmerking: Wijzig geen **tunnels-group PPP-eigenschappen** via Flex-fig **omdat** dit geen effect heeft op de verificatieprotocollen die via RADIUS zijn onderhandeld voor AnyConnect VPN-verbindingen (SSL en IPSec).

tunnelgroep RA_VPN ppp-eigenschappen
geen authenticatiepagina
legalisatietak
Verificatie ms-chap-v1
geen authenticatie ms-chap-v2
geen authenticatie-eap-proxy

Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

AanTD:

- **Straal verwijderen**

Op ISE:

- RADIUS-live logbestanden