Configurare la VPN ad accesso remoto FTD con MSCHAPv2 su RADIUS

Sommario

Introduzione

In questo documento viene descritto come abilitare il protocollo MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol versione 2) come metodo di autenticazione tramite Firepower Management Center (FMC) per client VPN ad accesso remoto con autenticazione RADIUS (Remote Authentication Dial-In User Service).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- FMCv - 7.0.0 (build 94)
- FTDv - 7.0.0 (Build 94)
- ISE - 2.7.0.356

- AnyConnect - 4.10.02086
- Windows 10 Pro

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Per impostazione predefinita, il protocollo FTD utilizza il protocollo PAP (Password Authentication Protocol) come metodo di autenticazione con i server RADIUS per le connessioni VPN AnyConnect.

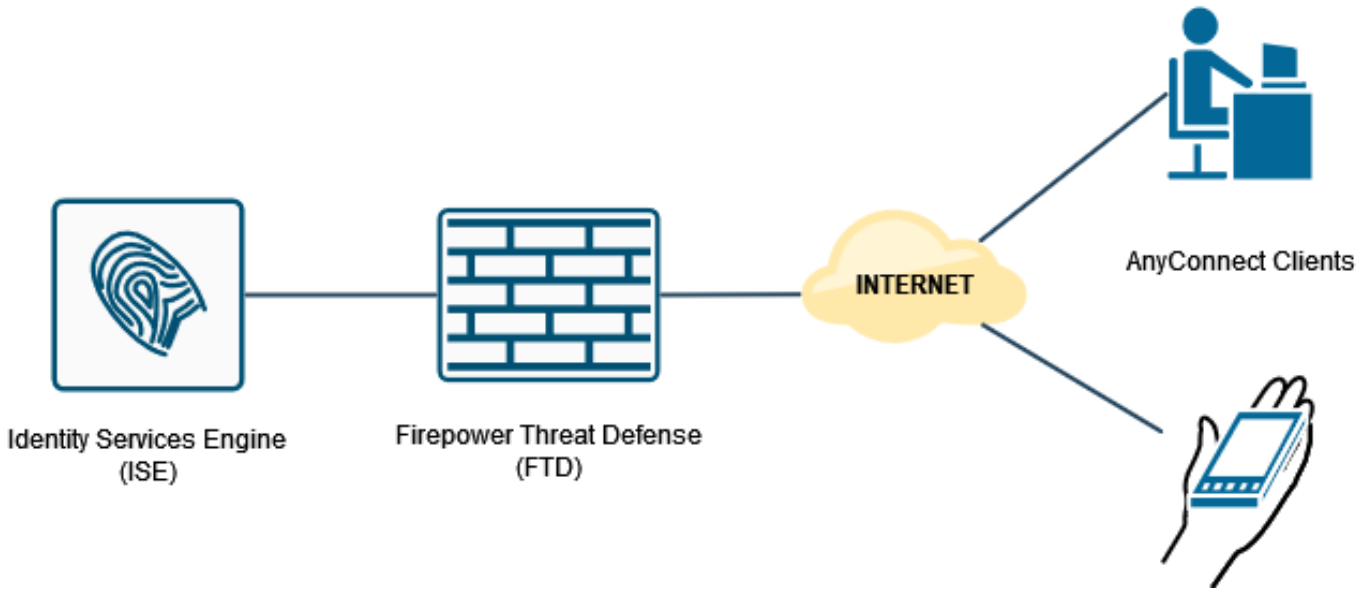
Il protocollo PAP fornisce agli utenti un metodo semplice per stabilire la propria identità con un handshake bidirezionale. La password PAP è crittografata con un segreto condiviso ed è il protocollo di autenticazione meno sofisticato. Il protocollo PAP non è un metodo di autenticazione avanzato in quanto offre una protezione ridotta da attacchi ripetuti di tipo prova ed errore.

L'autenticazione MS-CHAPv2 introduce l'autenticazione reciproca tra peer e una funzione di modifica della password.

Per abilitare MS-CHAPv2 come protocollo utilizzato tra l'ASA e il server RADIUS per una connessione VPN, è necessario abilitare la gestione delle password nel profilo di connessione. L'abilitazione della gestione delle password genera una richiesta di autenticazione MS-CHAPv2 da FTD al server RADIUS.

Configurazione

Esempio di rete

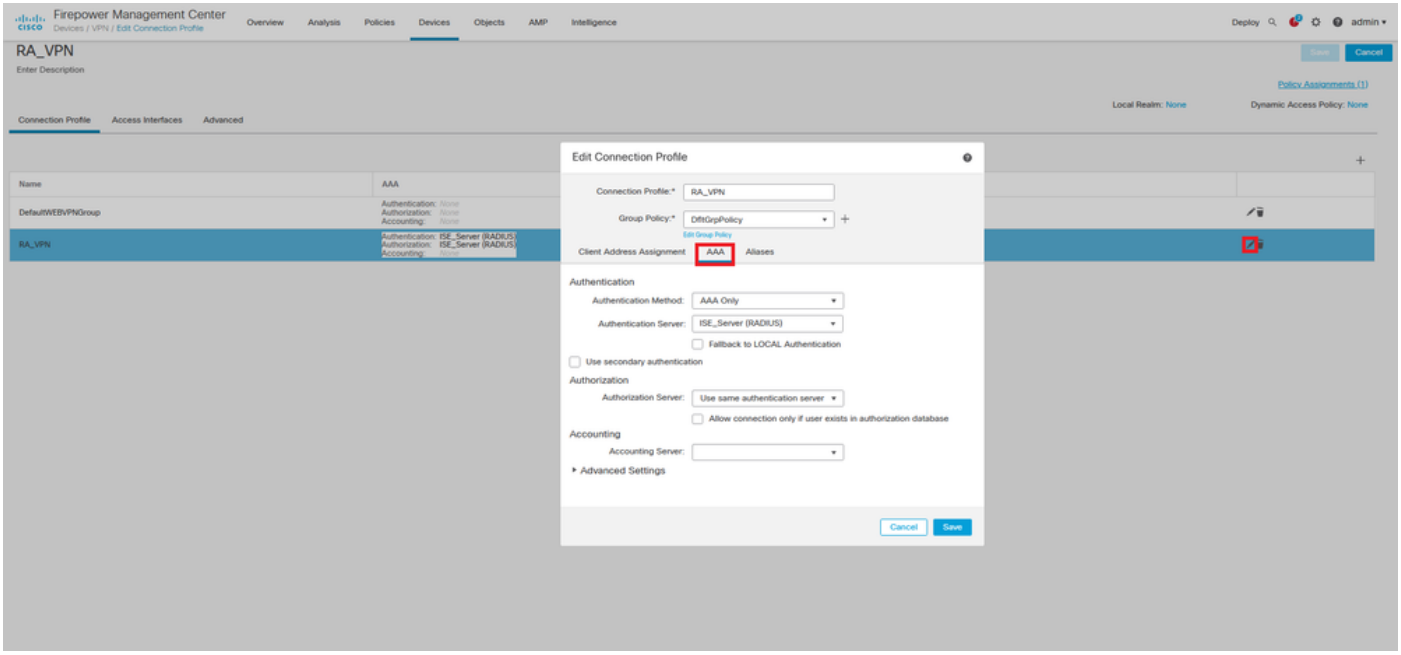


Configurazione di RSA VPN con autenticazione AAA/RADIUS tramite FMC

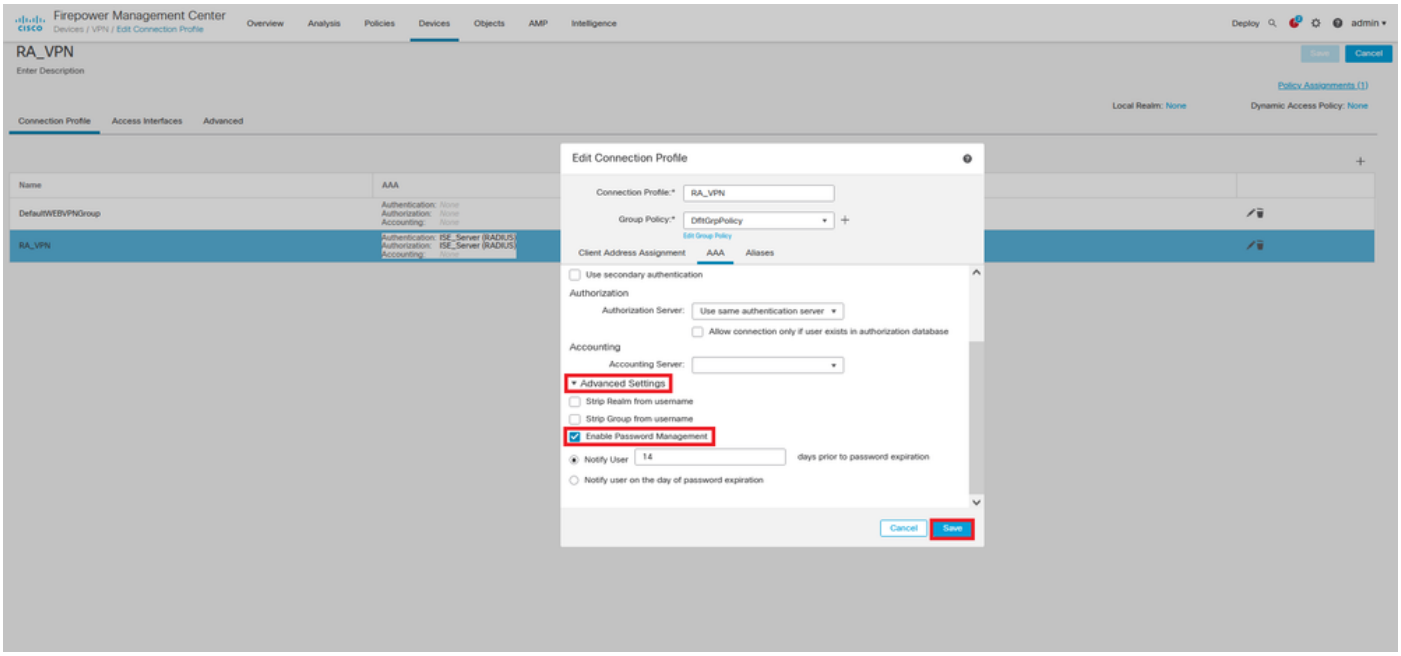
Per una procedura dettagliata, fare riferimento a questo documento e a questo video:

- Configurazione VPN ad accesso remoto AnyConnect su FTD
- Configurazione iniziale di AnyConnect per FTD gestito da FMC

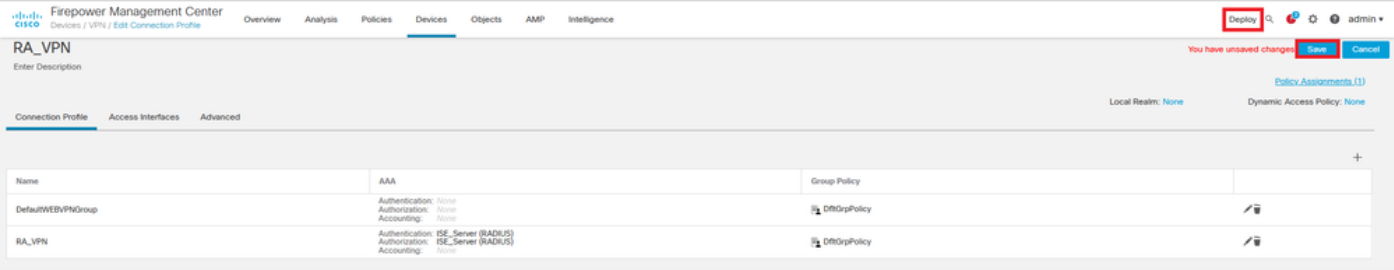
Passaggio 1. Una volta configurata la VPN ad accesso remoto, selezionare **Dispositivi > Accesso remoto**, modificare il profilo di connessione appena creato e passare alla scheda **AAA**.



Espandere la sezione **Impostazioni avanzate** e fare clic sulla casella di controllo **Abilita gestione password**. Fare clic su **Salva**.



Salvataggio e **distribuzione**.



La configurazione VPN ad accesso remoto nella CLI FTD è:

```
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
```

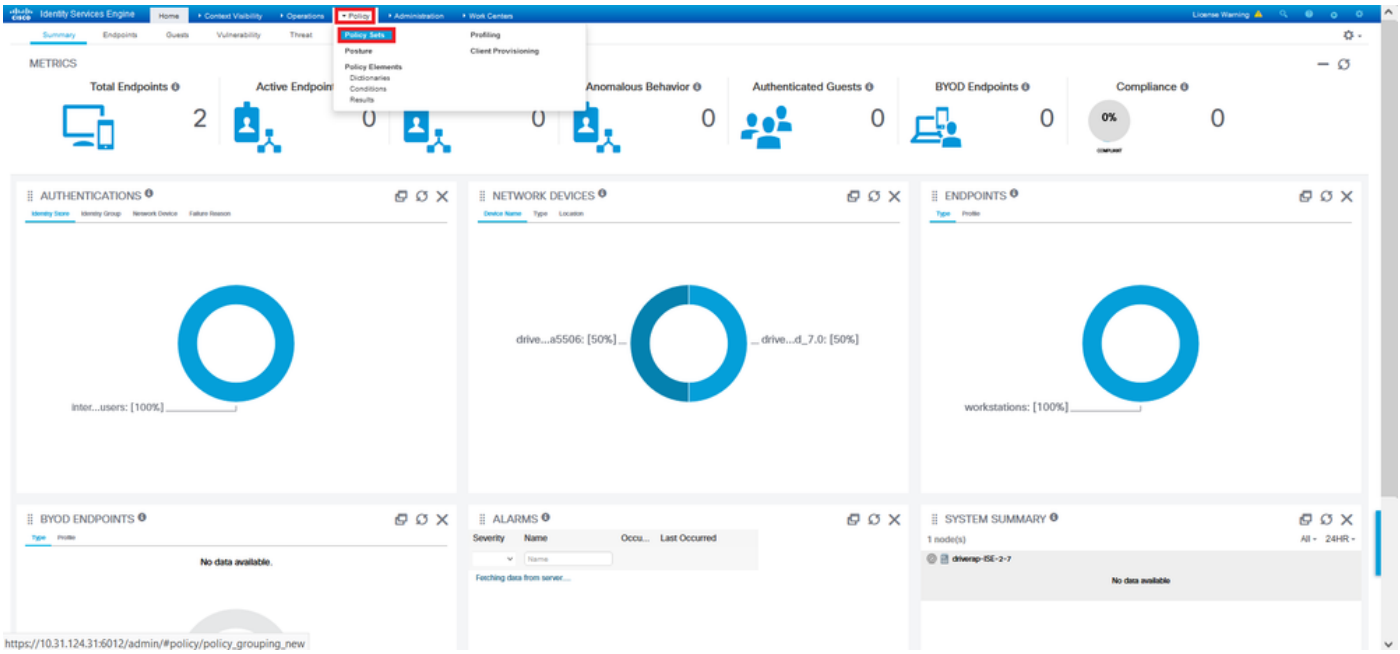
```
file-entry disable
file-browsing disable
url-entry disable
deny-message none

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
```

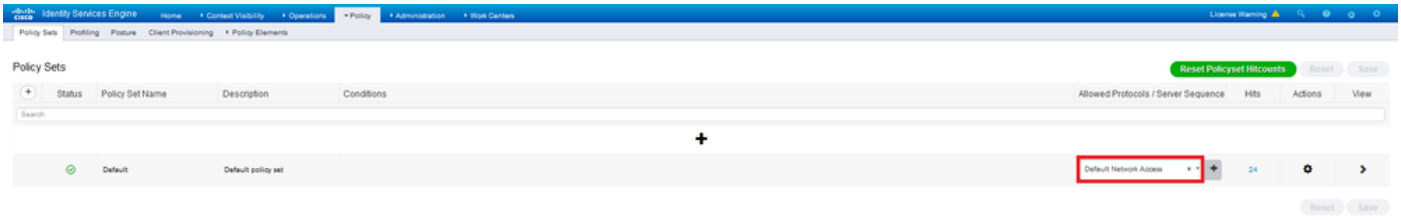
Configurazione di ISE per il supporto di MS-CHAPv2 come protocollo di autenticazione

Si presume che:

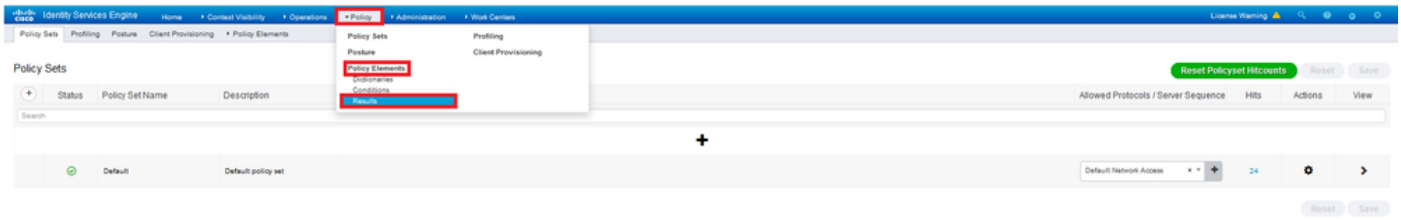
1. L'FTD è già stato aggiunto come dispositivo di rete su ISE in modo che possa elaborare le richieste di accesso RADIUS dall'FTD.
2. Per autenticare il client AnyConnect, ISE può usare almeno un utente.

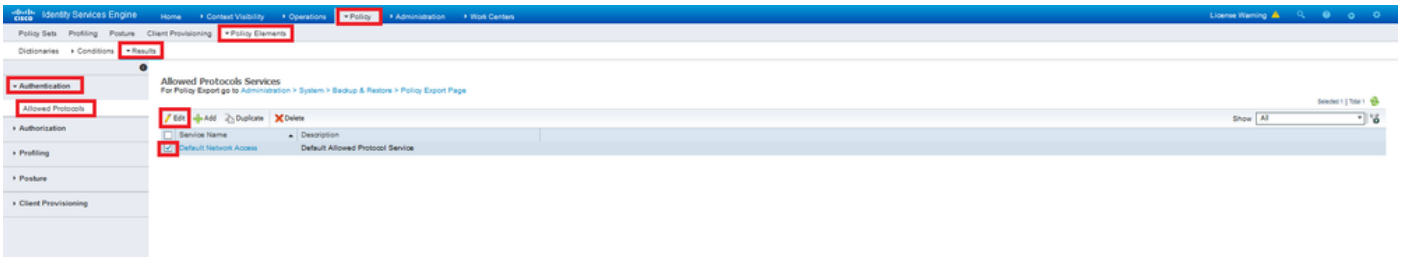
Passaggio 2. Passare a **Criterio > Set di criteri** e individuare il criterio **Protocolli autorizzati** associato al set di criteri in cui sono autenticati gli utenti AnyConnect. In questo esempio è presente un solo set di criteri, pertanto il criterio in questione è *Accesso di rete predefinito*.



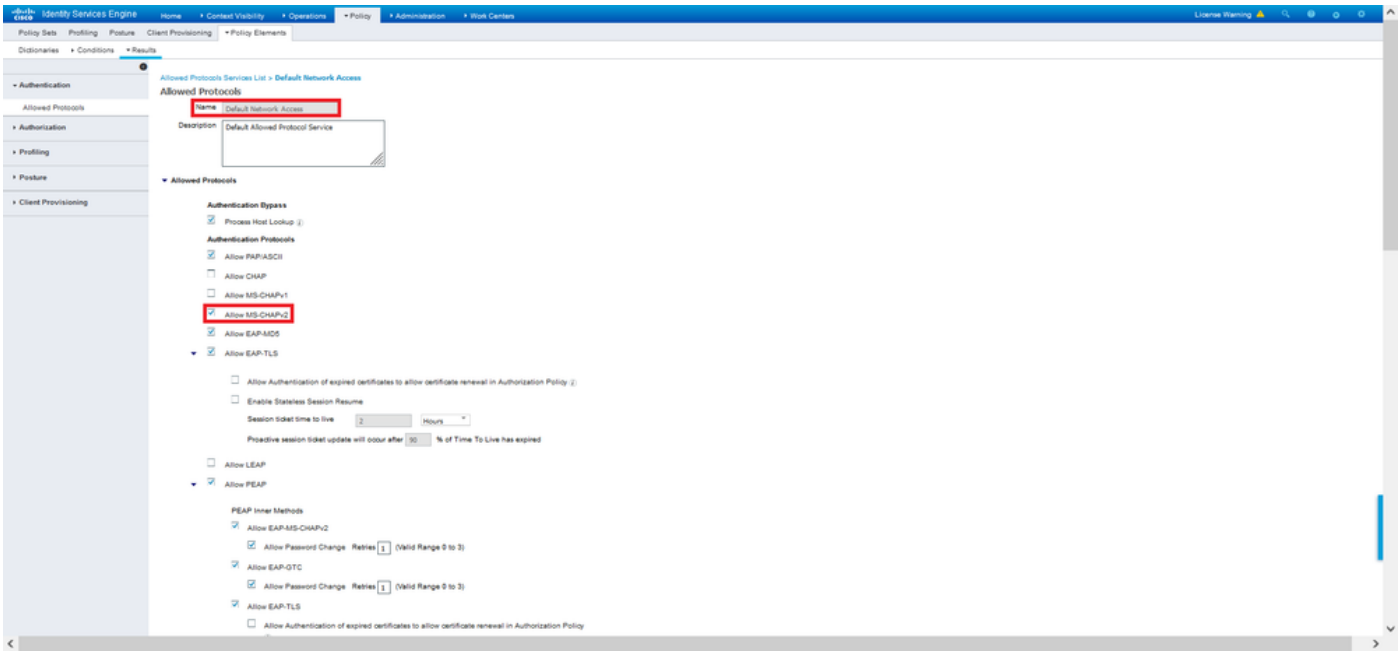


Passaggio 3. Passare a **Criterio > Elementi criteri > Risultati.** In **Autenticazione > Protocolli consentiti** scegliere e modificare **Accesso alla rete predefinito**.



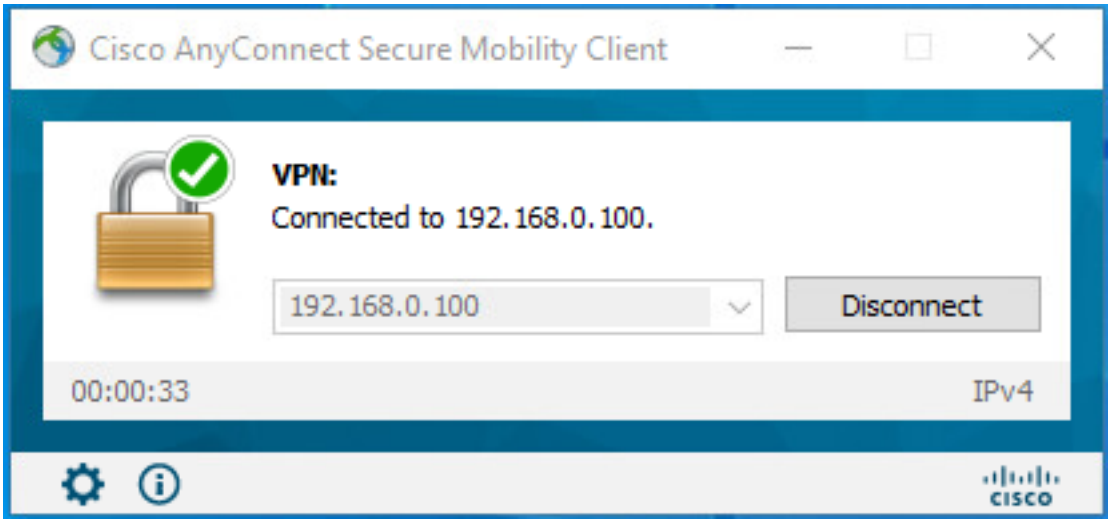


Verificare che la casella di controllo **Consenti MS-CHAPv2** sia selezionata. Scorri fino in fondo e **salva**.

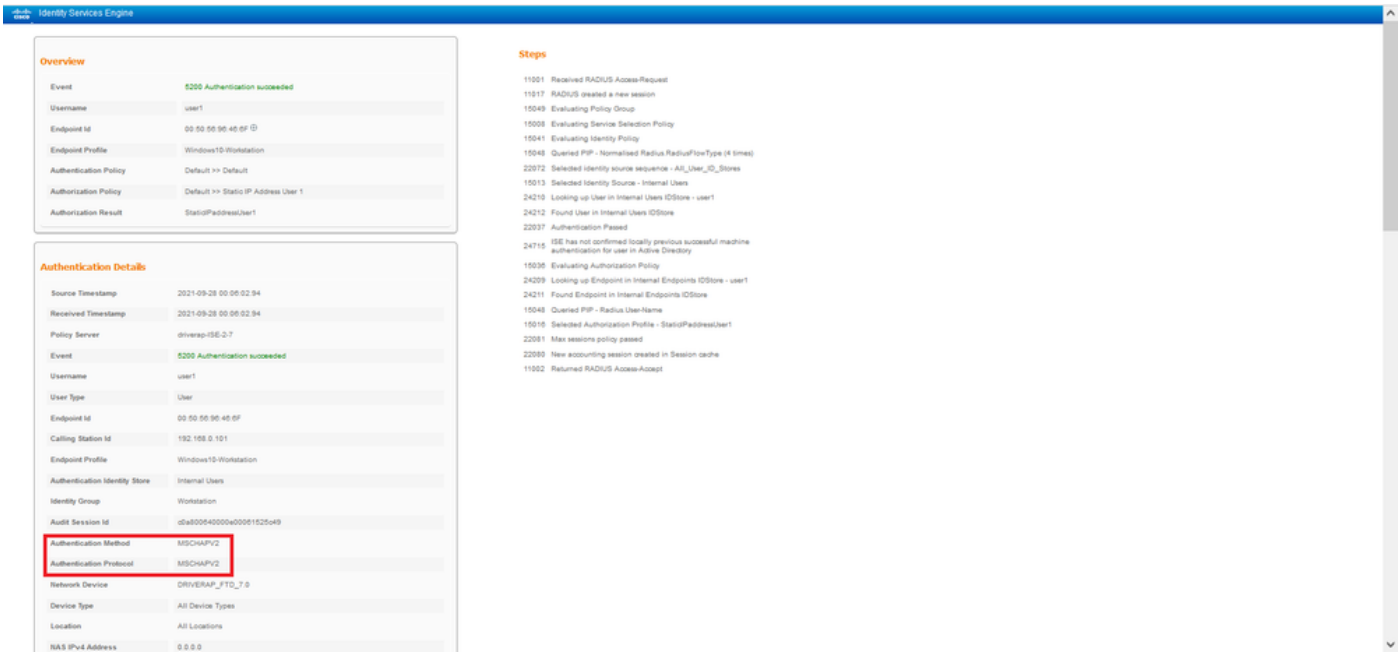


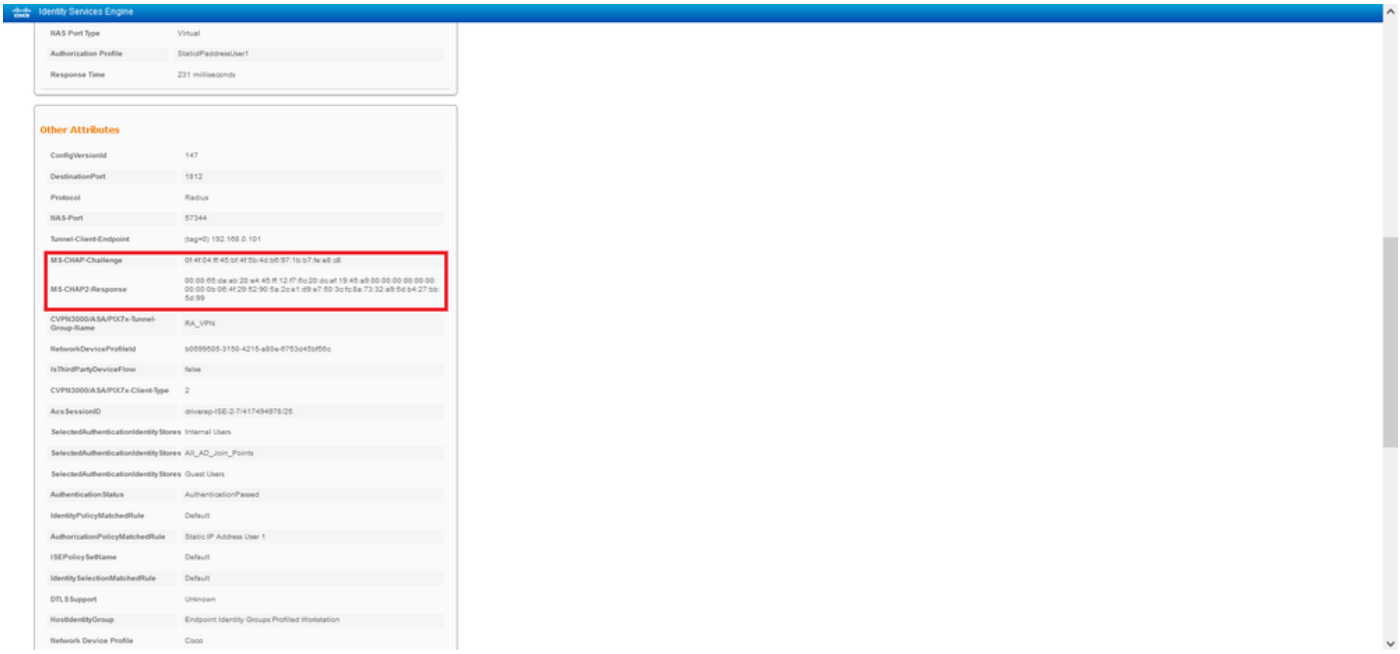
Verifica

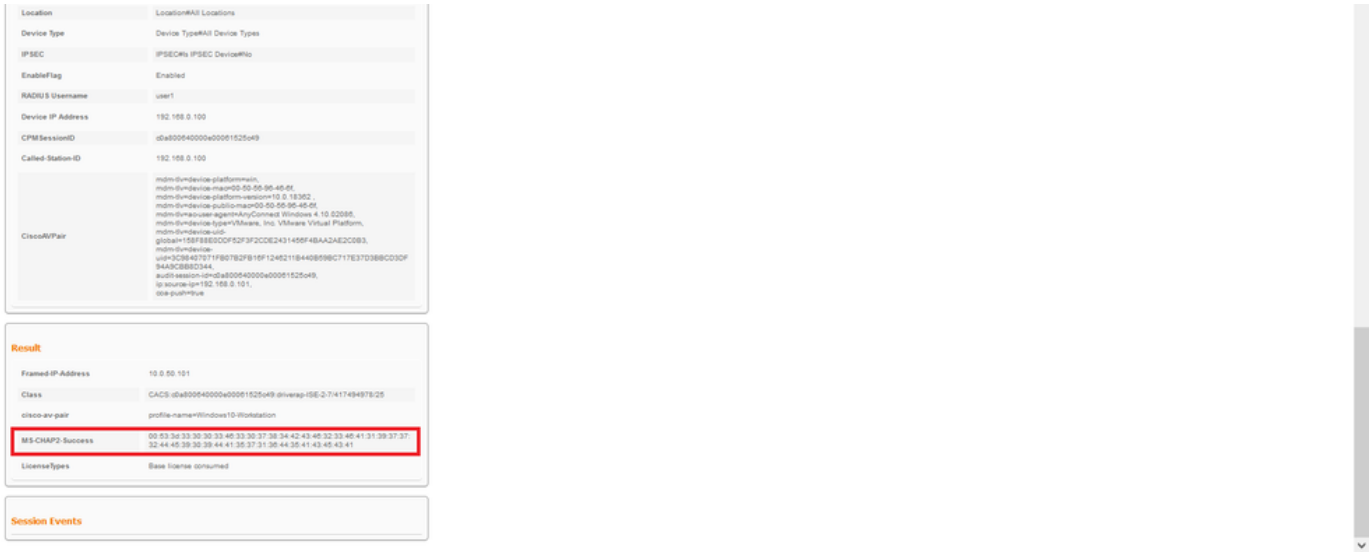
Passare al computer client in cui è installato il client Cisco AnyConnect Secure Mobility. Connettersi all'headend FTD (nell'esempio riportato viene utilizzato un computer Windows) e digitare le credenziali dell'utente.



I login RADIUS Live ad ISE mostrano:







Nota: il comando **test di autenticazione aaa-server** utilizza sempre PAP per inviare le richieste di autenticazione al server RADIUS. Non è possibile forzare il firewall a utilizzare MS-CHAPv2 con questo comando.

firepower# **test di autenticazione aaa-server ISE_Server host 172.16.0.8 nomeutente user1 password XXXXXX**
INFORMAZIONI: Tentativo di verifica dell'autenticazione sull'indirizzo IP (172.16.0.8) (timeout: 12 secondi)
INFORMAZIONI: Autenticazione riuscita

Nota: Non modificare **gli attributi ppp del gruppo di tunnel** tramite Flex-config perché non ha effetto sui protocolli di autenticazione negoziati su RADIUS per le connessioni AnyConnect VPN (SSL e IPSec).

tunnel-group RA_VPN ppp-attributes
 nessuna pagina di autenticazione
 autenticazione chap
 autenticazione ms-chap-v1
 nessuna autenticazione ms-chap-v2
 nessuna autenticazione eap-proxy

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Su FTD

- **debug radius all**

ISE:

- Registri attivi RADIUS