Configuración de FTD Remote Access VPN con MSCHAPv2 sobre RADIUS

Contenido

Introducción

Este documento describe cómo habilitar Microsoft Challenge Handshake Authentication Protocol versión 2 (MS-CHAPv2) como el método de autenticación a través de Firepower Management Center (FMC) para clientes VPN de acceso remoto con autenticación RADIUS (servicio de usuario de acceso telefónico de autenticación remota).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- FMCv - 7.0.0 (compilación 94)
- FTDv - 7.0.0 (Compilación 94)
- ISE - 2.7.0.356

- AnyConnect: 4.10.02086
- Windows 10 Pro

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

De forma predeterminada, FTD utiliza el protocolo de autenticación de contraseña (PAP) como método de autenticación con los servidores RADIUS para las conexiones VPN de AnyConnect.

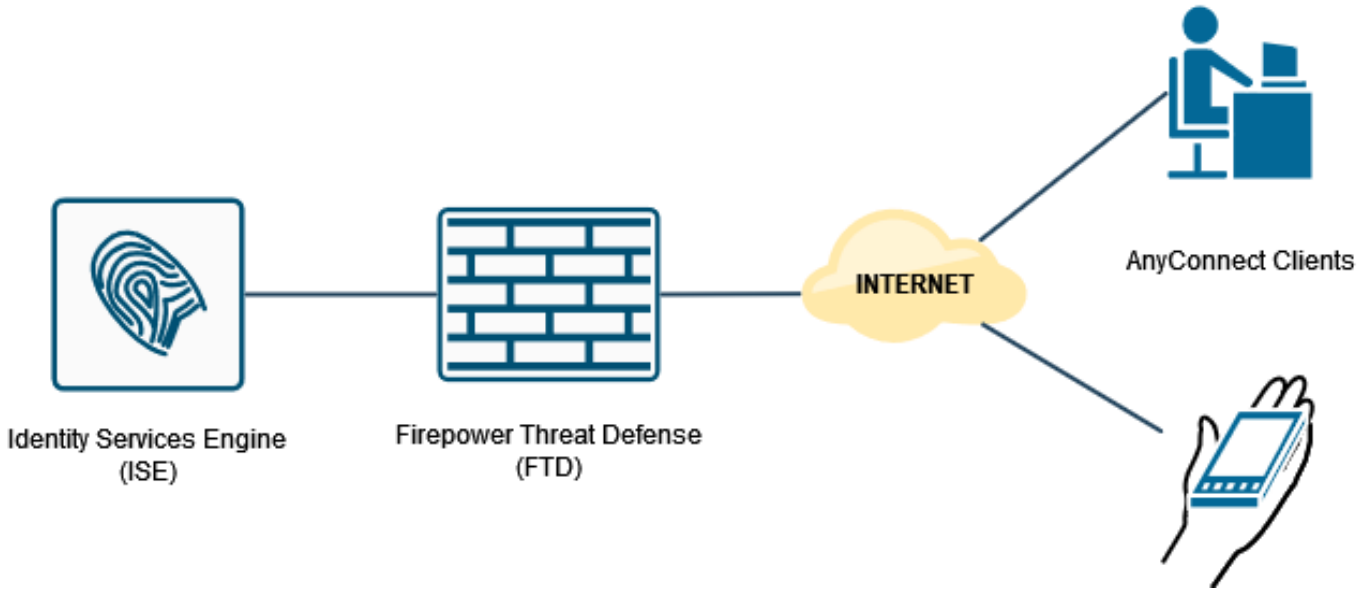
PAP proporciona un método sencillo para que los usuarios establezcan su identidad con un intercambio de señales bidireccional. La contraseña PAP se cifra con un secreto compartido y es el protocolo de autenticación menos sofisticado. PAP no es un método de autenticación sólido porque ofrece poca protección contra los repetidos ataques de prueba y error.

La autenticación MS-CHAPv2 introduce la autenticación mutua entre pares y una función de cambio de contraseña.

Para habilitar MS-CHAPv2 como el protocolo utilizado entre el ASA y el servidor RADIUS para una conexión VPN, la administración de contraseñas debe estar habilitada en el perfil de conexión. Al habilitar la administración de contraseñas, se genera una solicitud de autenticación MS-CHAPv2 desde el FTD al servidor RADIUS.

Configurar

Diagrama de la red



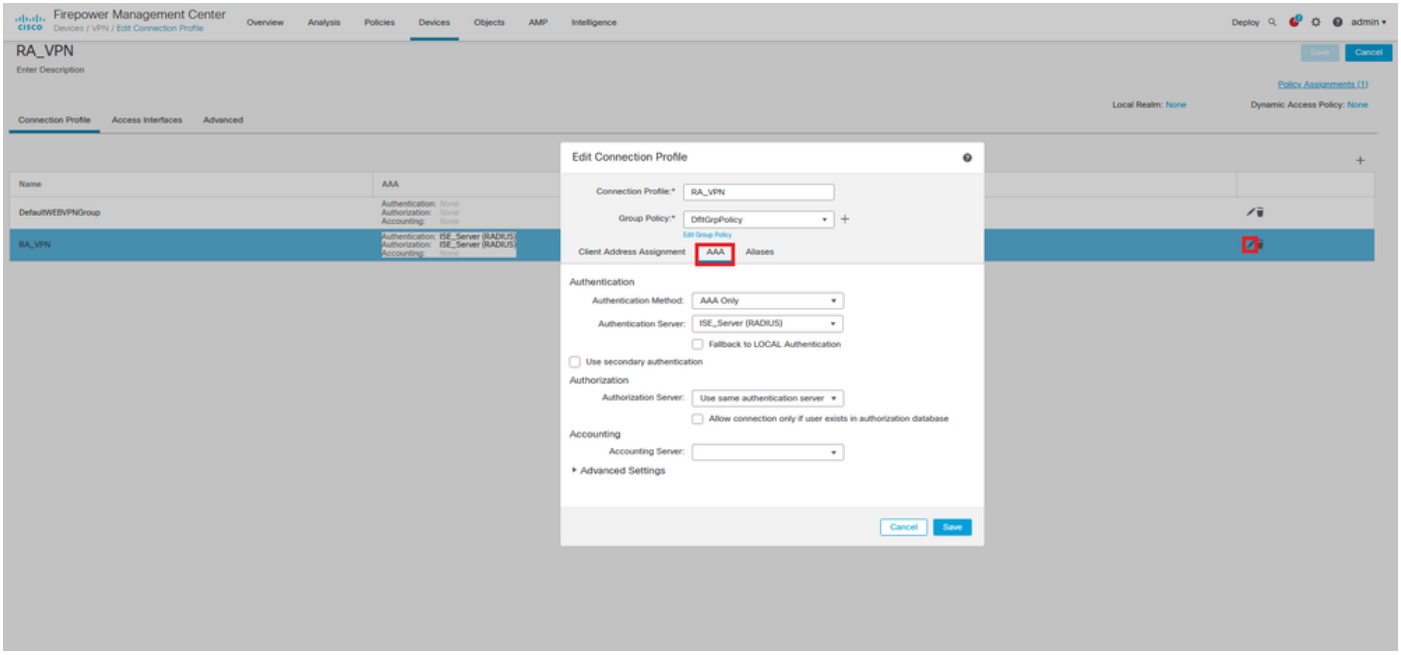
Configuración de RA VPN con autenticación AAA/RADIUS a través de FMC

Para ver un procedimiento paso a paso, consulte este documento y este vídeo:

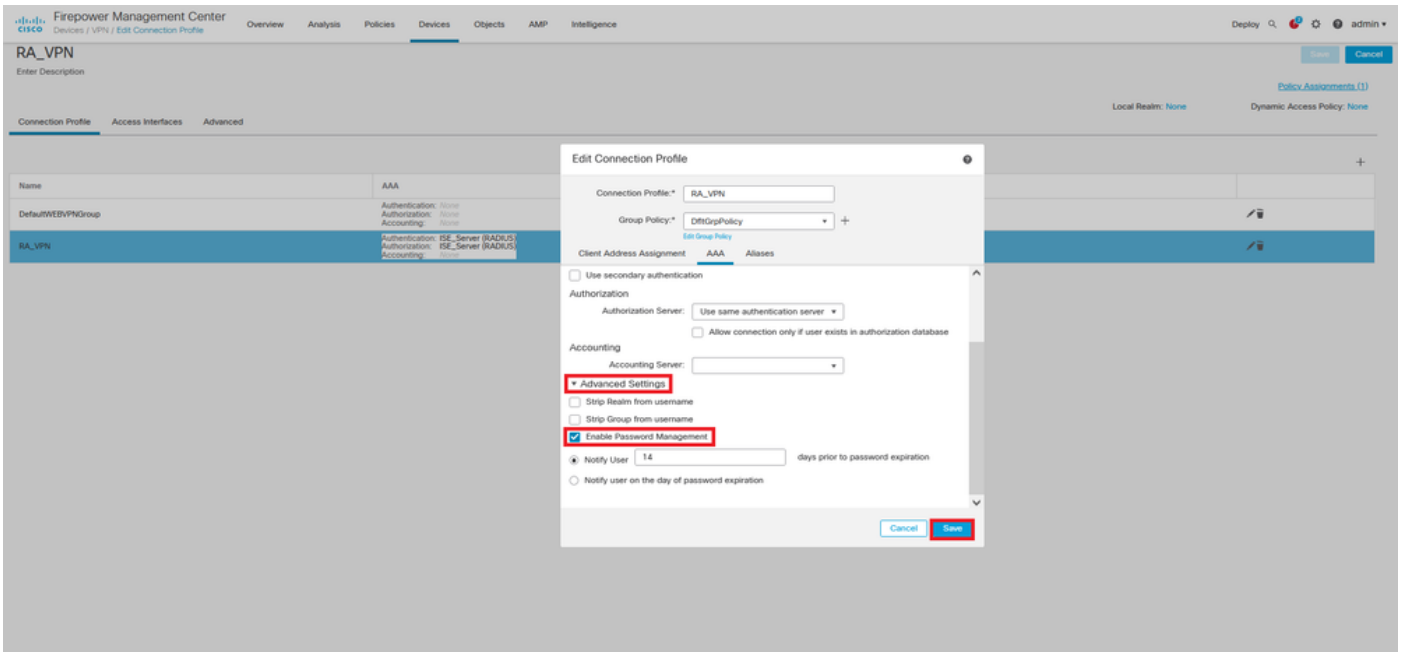
- Configuración de VPN de acceso remoto AnyConnect en FTD

- [Configuración de AnyConnect inicial para FTD gestionada por FMC]

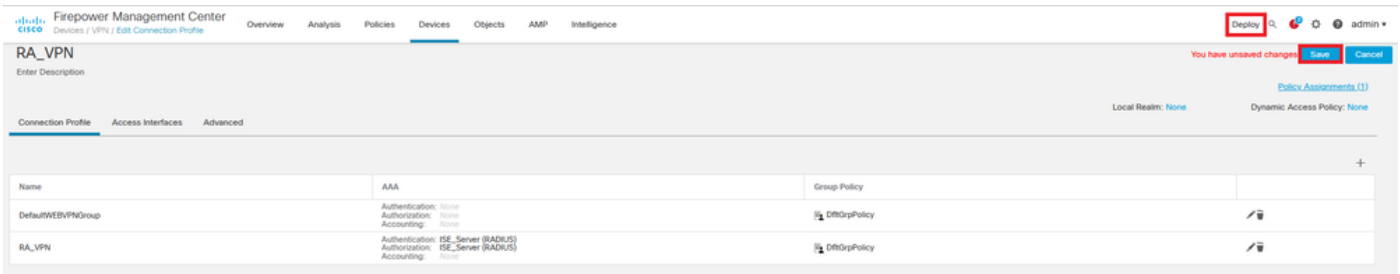
Paso 1. Una vez configurada la VPN de acceso remoto, navegue hasta **Dispositivos > Acceso remoto**, edite el perfil de conexión recién creado y luego navegue a la pestaña **AAA**.



Expanda la sección **Advanced Settings** y haga clic en la **casilla de verificación Enable Password Management** . Click **Save**.



Guardar e **implementar**.



La configuración de VPN de acceso remoto en la CLI de FTD es:

```
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
```

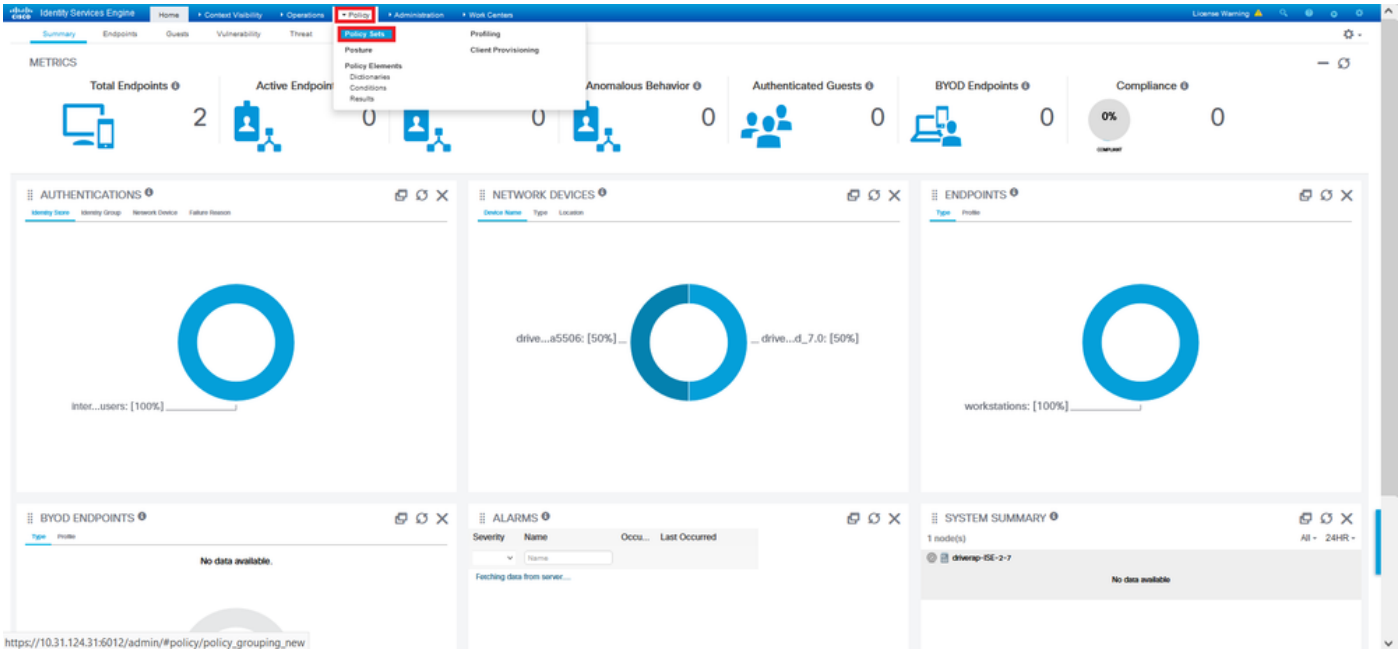
```
password-management
tunnel-group RA_VPN webvpn-attributes
group-alias RA_VPN enable
```

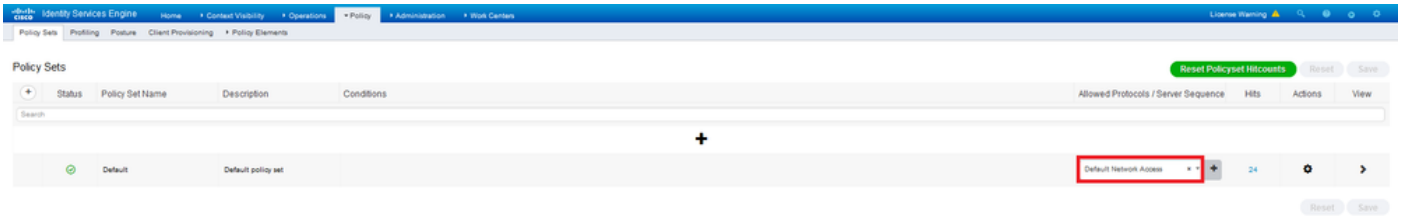
Configuración de ISE para Soportar MS-CHAPv2 como protocolo de autenticación

Se supone que:

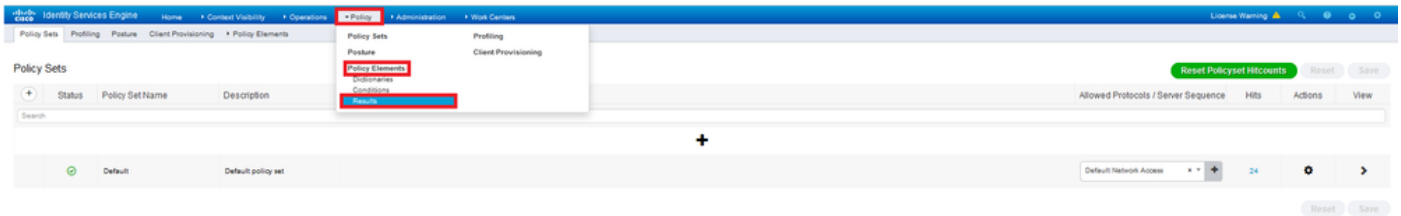
1. El FTD ya se agrega como dispositivo de red en ISE para que pueda procesar las solicitudes de acceso RADIUS desde el FTD.
2. ISE dispone de al menos un usuario para autenticar el cliente AnyConnect.

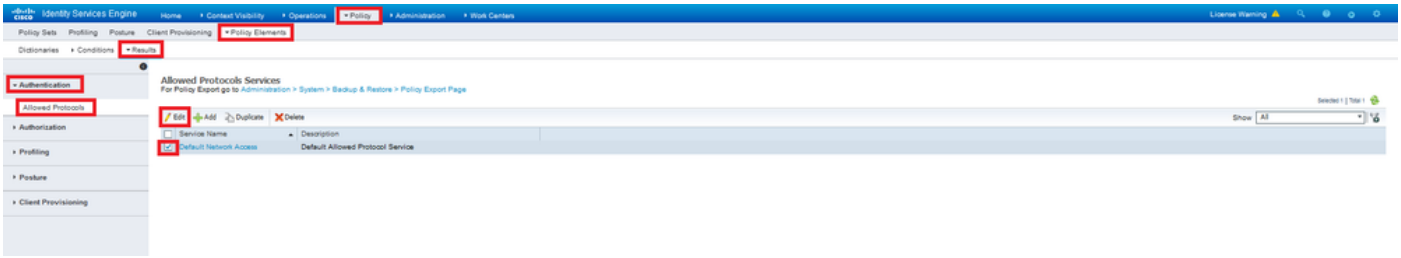
Paso 2. Navegue hasta **Política > Conjuntos de políticas** y busque la política de **Protocolos permitidos** asociada al Conjunto de políticas donde se autentican los usuarios de AnyConnect. En este ejemplo, sólo hay un conjunto de políticas, por lo que la política en cuestión es *Acceso de red predeterminado*.



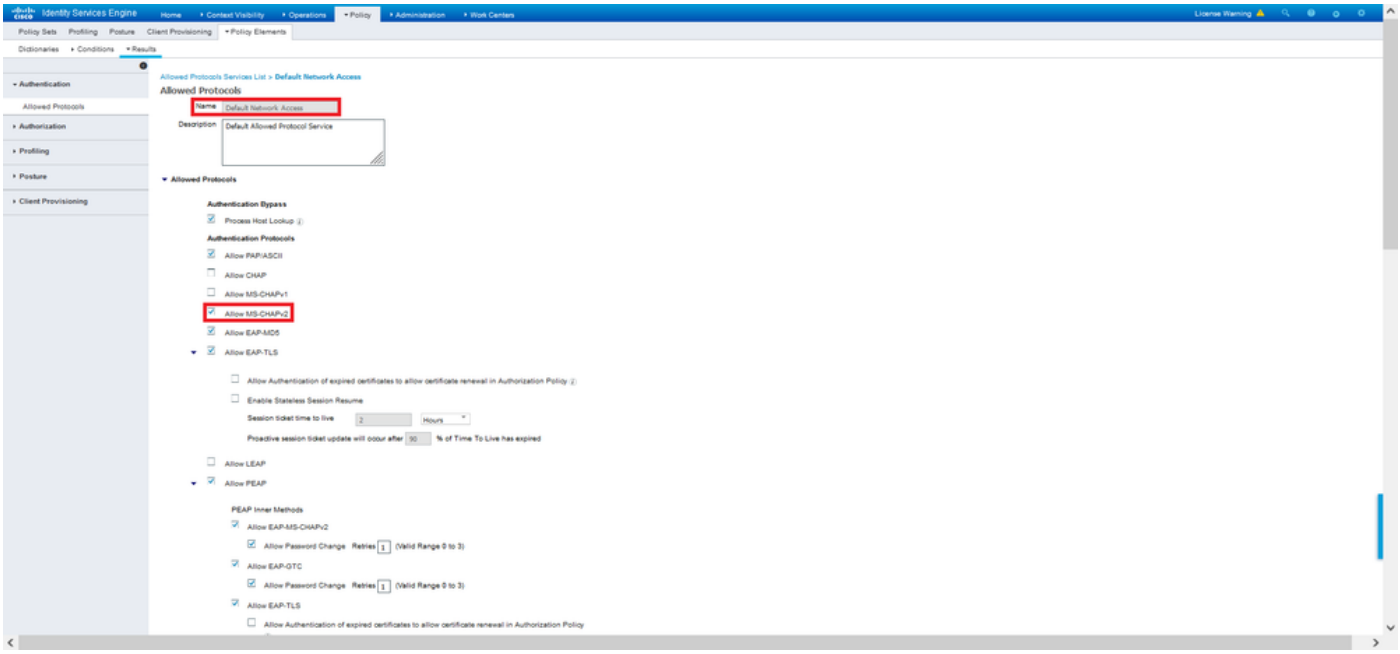


Paso 3. Vaya a **Política > Elementos de política > Resultados.** En **Authentication > Allowed Protocols** elija y edite **Default Network Access**.



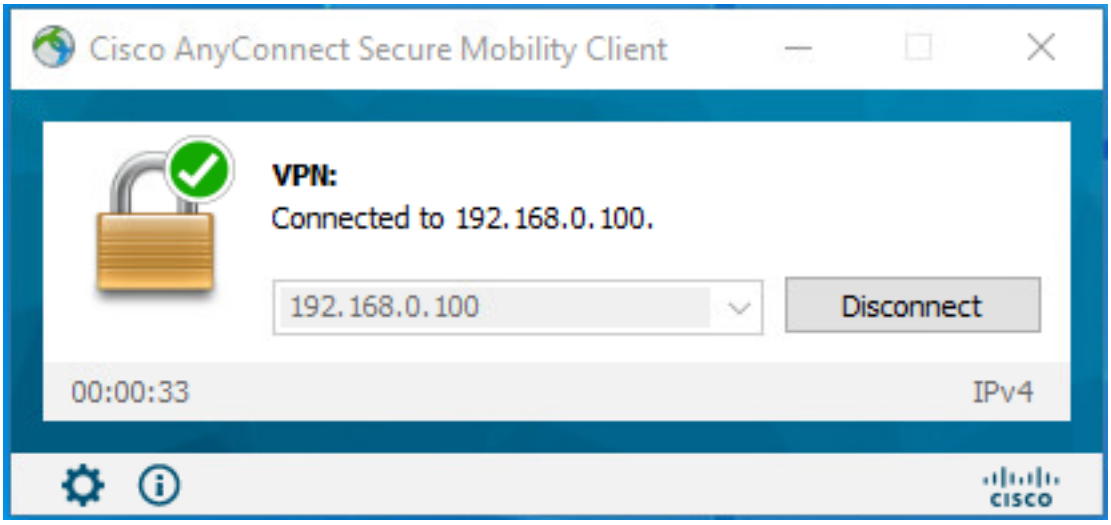


Asegúrese de que la casilla de verificación **Allow MS-CHAPv2** esté marcada. Desplácese hasta abajo y **guárdelo**.

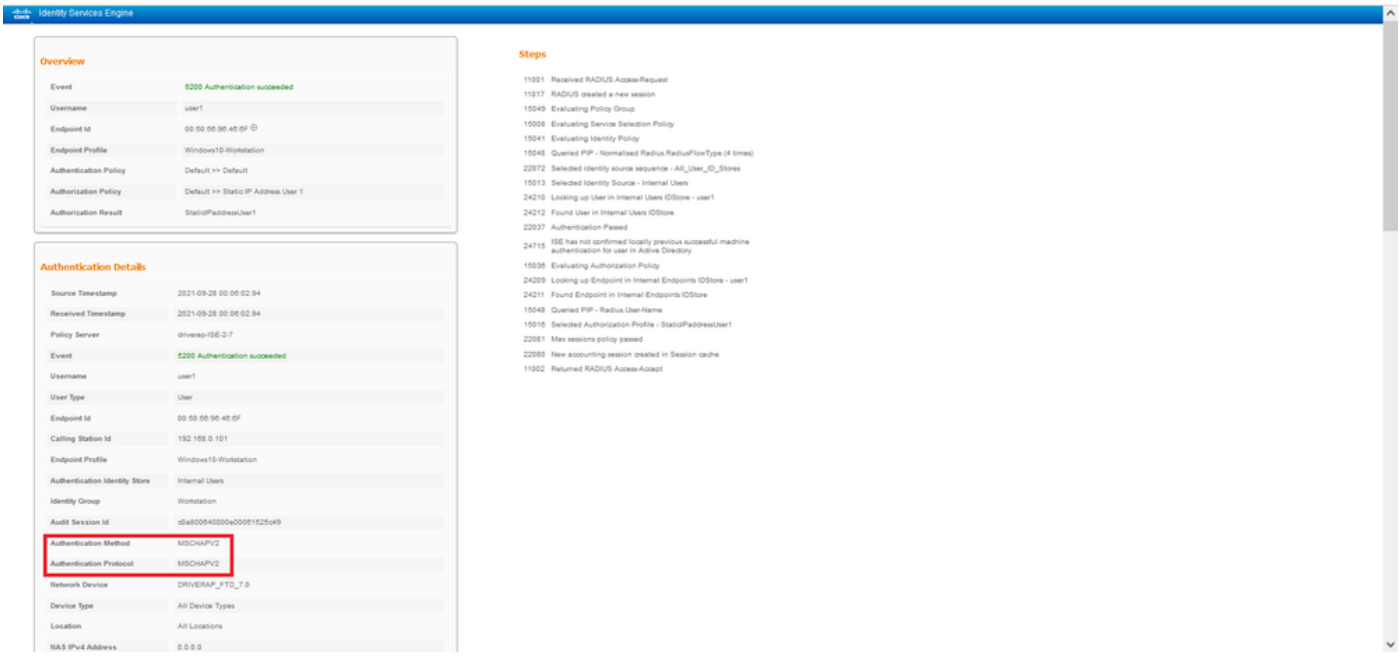


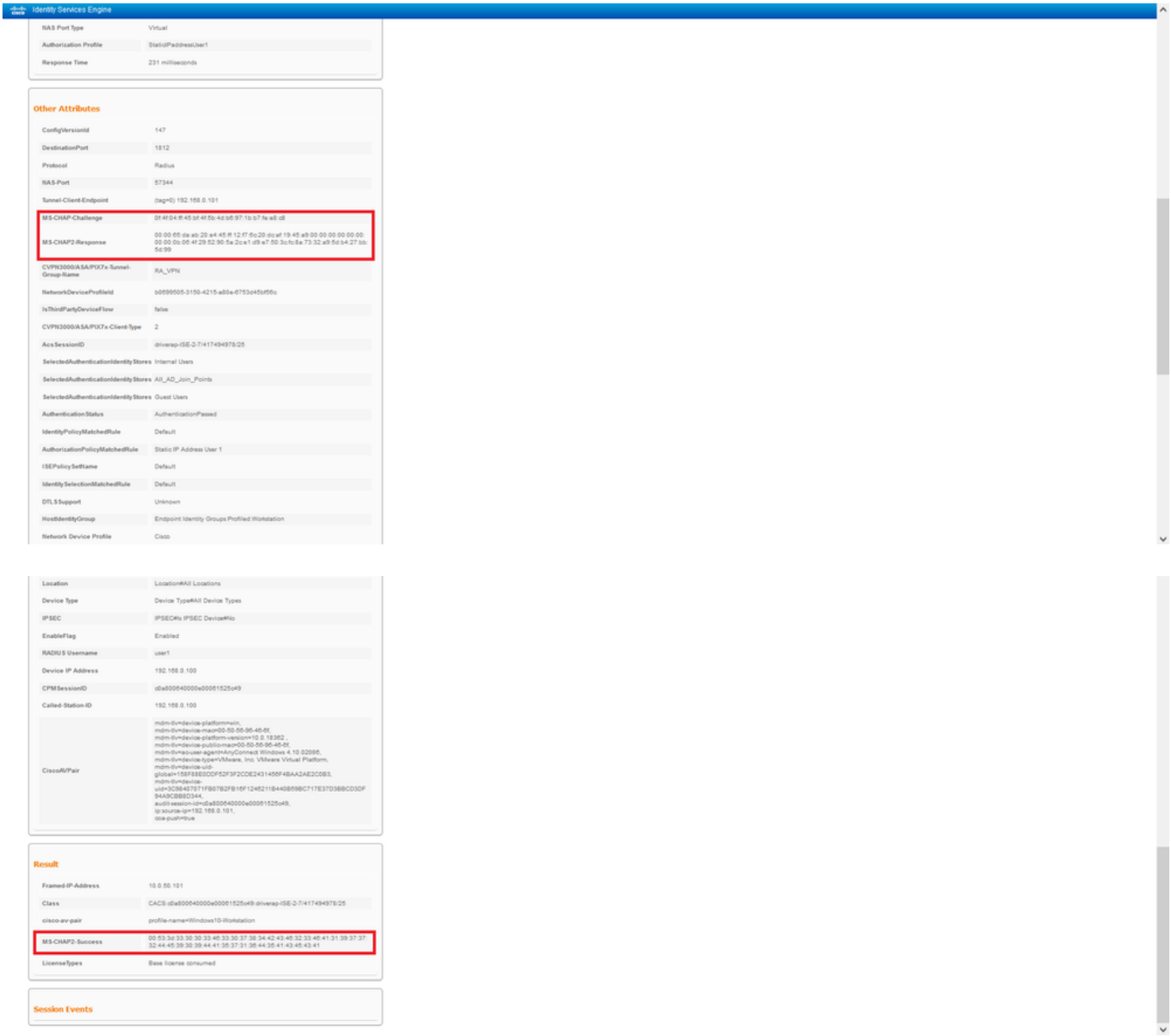
Verificación

Desplácese hasta el equipo cliente en el que está instalado el cliente Cisco AnyConnect Secure Mobility. Conéctese a la cabecera FTD (en este ejemplo se utiliza una máquina Windows) y escriba las credenciales del usuario.



Los registros en directo de RADIUS en ISE muestran:





Nota: El comando **test aaa-server authentication** siempre utiliza PAP para enviar solicitudes

de autenticación al servidor RADIUS, no hay forma de forzar al firewall a utilizar MS-CHAPv2 con este comando.

firepower# **test aaa-server authentication ISE_Server host 172.16.0.8 username user1 password XXXXXX**
INFO: Intentando la prueba de autenticación a la dirección IP (172.16.0.8) (tiempo de espera: 12 segundos)
INFO: Authentication Successful (Autenticación exitosa)

Nota: No modifique **los atributos ppp del grupo de túnel** mediante Flex-config, ya que esto no tiene efecto en los protocolos de autenticación negociados sobre RADIUS para las conexiones VPN de AnyConnect (SSL e IPSec).

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

Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

On FTD:

- **debug radius all**

En ISE:

- Registros activos RADIUS