

# Configuración de FTD Remote Access VPN con MSCHAPv2 sobre RADIUS

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración de RA VPN con autenticación AAA/RADIUS a través de FMC](#)

[Configuración de ISE para Soportar MS-CHAPv2 como protocolo de autenticación](#)

[Verificación](#)

[Troubleshoot](#)

## 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.

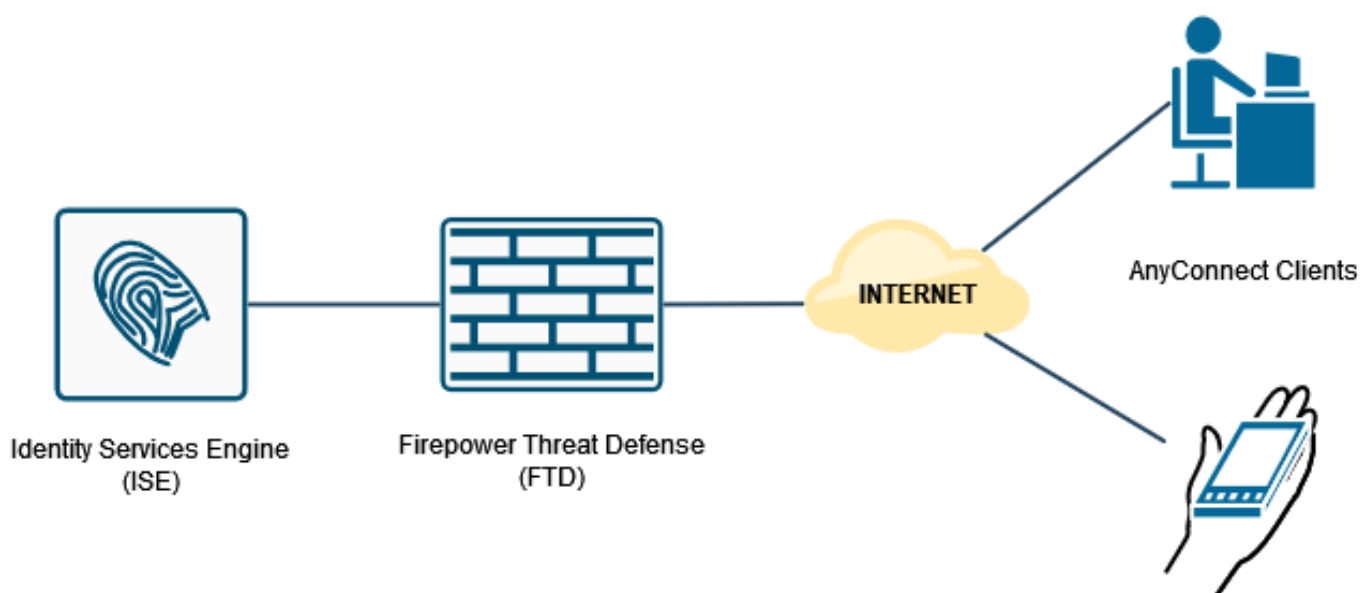
PAP proporciona un método sencillo para que los usuarios establezcan su identidad con un intercambio de señales bidireccional. La contraseña PAP se cifra con un secreto compartido y es el protocolo de autenticación menos sofisticado. PAP no es un método de autenticación sólido porque ofrece poca protección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



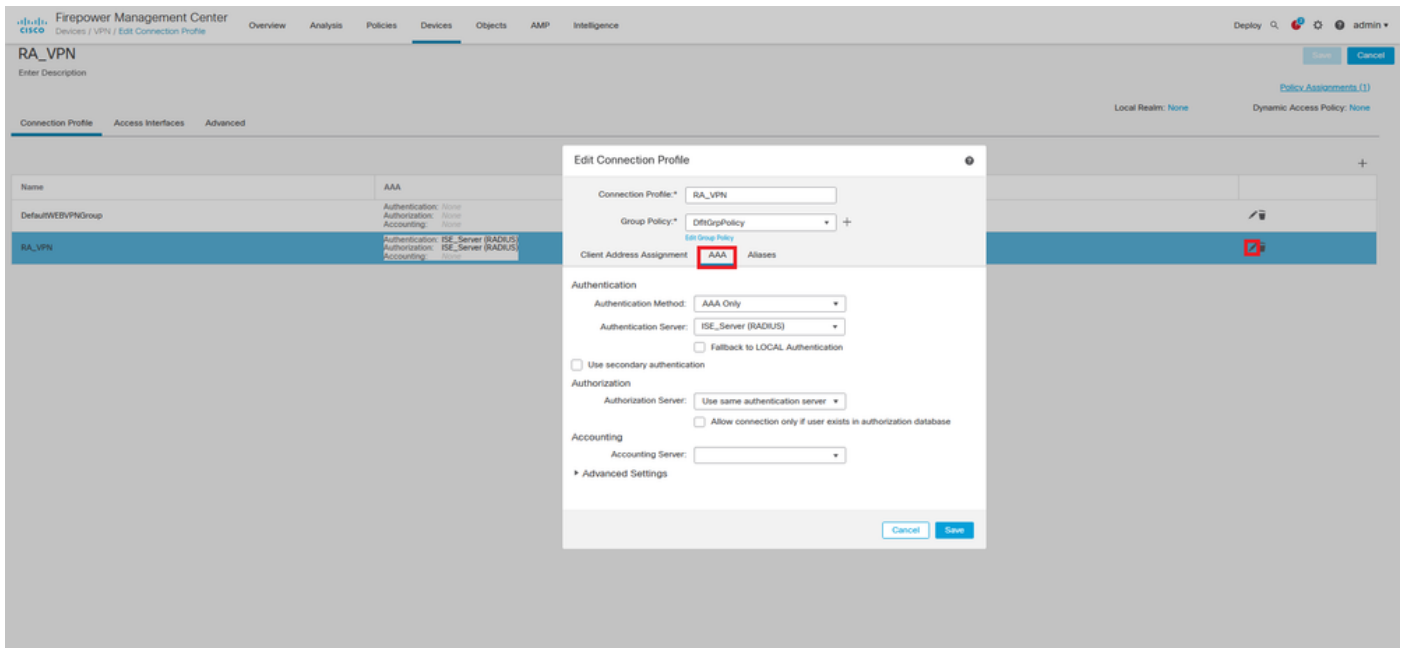
### Configuración de RA VPN con autenticación AAA/RADIUS a través de FMC

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

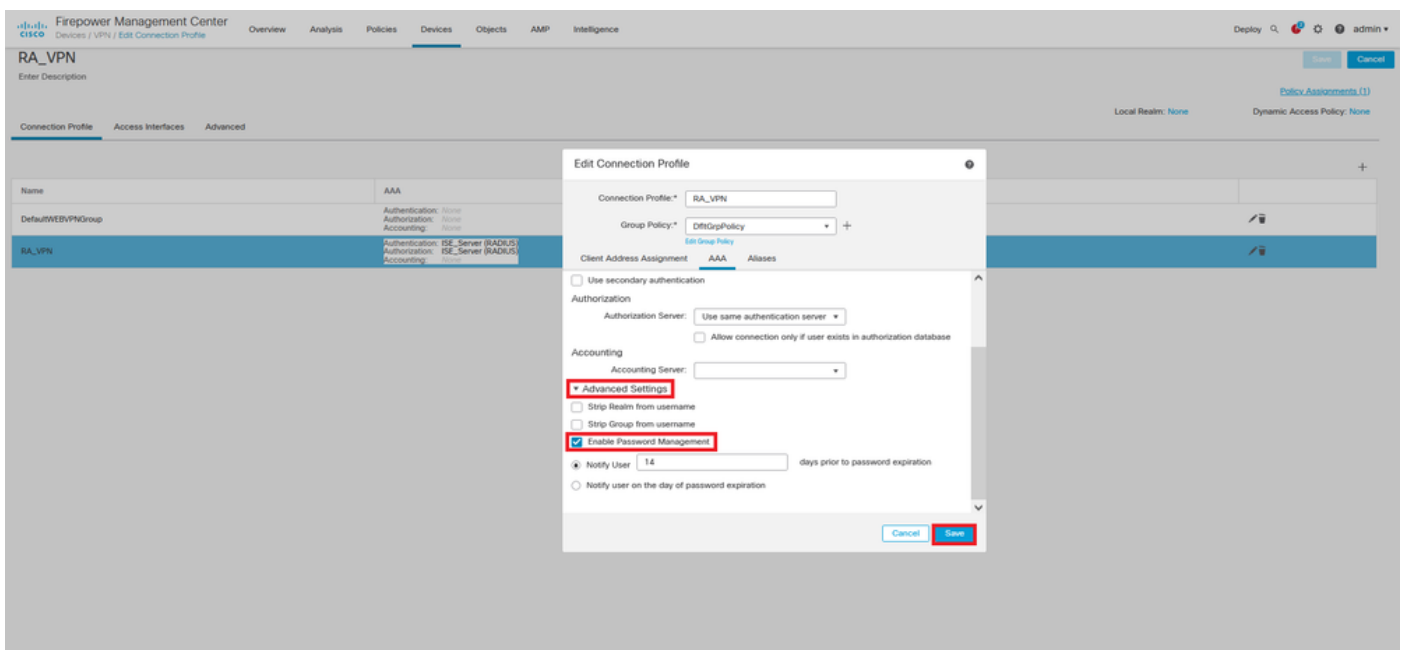
- [Configuración de VPN de acceso remoto AnyConnect en FTD](#)

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

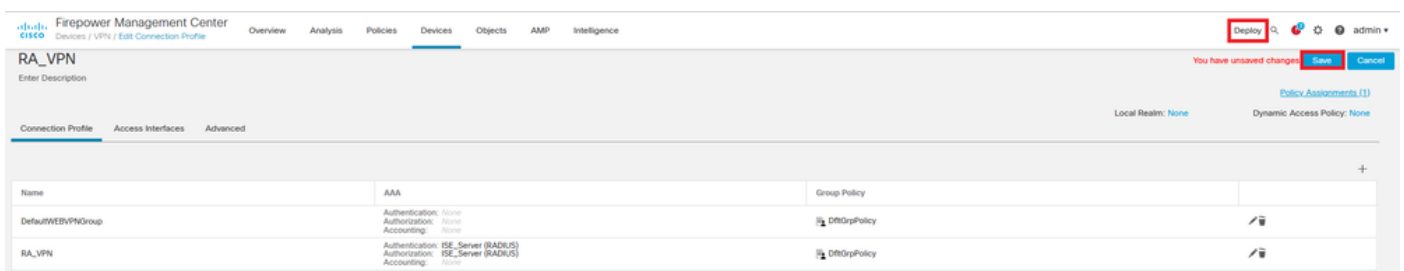
Paso 1. Una vez configurada la VPN de acceso remoto, navegue hasta **Dispositivos > Acceso remoto**, edite el perfil de conexión recién creado y luego navegue a la pestaña **AAA**.



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*.

The screenshot displays the Cisco Identity Services Engine (ISE) dashboard. At the top, there are navigation tabs for Summary, Endpoints, Guests, Vulnerability, Threat, Policy Sets, Profiling, and Client Provisioning. The main area features several metrics: Total Endpoints (2), Active Endpoints (0), Anomalous Behavior (0), Authenticated Guests (0), BYOD Endpoints (0), and Compliance (0%). Below these are three donut charts: 'Authentications' showing 'Intr...users: [100%]', 'Network Devices' showing 'drive...a5506: [50%]' and 'drive...d\_7.0: [50%]', and 'Endpoints' showing 'workstations: [100%]'. There are also sections for BYOD Endpoints (No data available), Alarms (Fetching data from server...), and System Summary (1 node(s), All - 24HR - No data available).

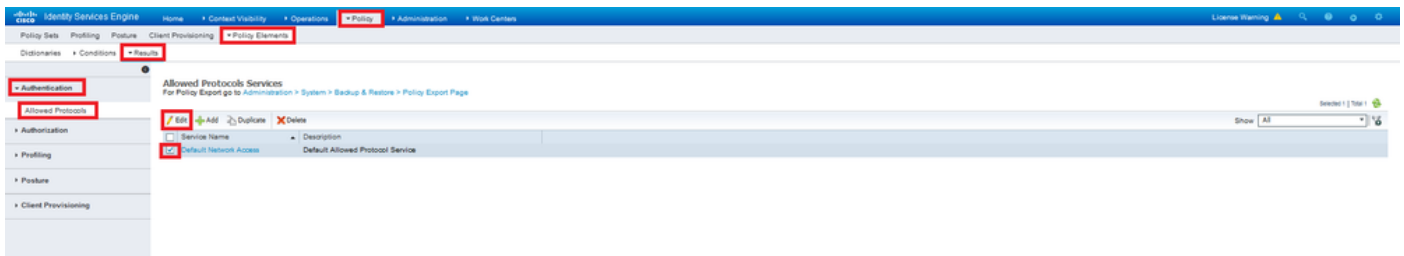
The screenshot shows the 'Policy Sets' configuration page in Cisco ISE. A table lists the policy sets:

| Status  | Policy Set Name    | Description | Conditions | Allowed Protocols / Server Sequence | HHS | Actions | View |
|---------|--------------------|-------------|------------|-------------------------------------|-----|---------|------|
| Default | Default policy set |             |            | Default Network Access              | 24  |         |      |

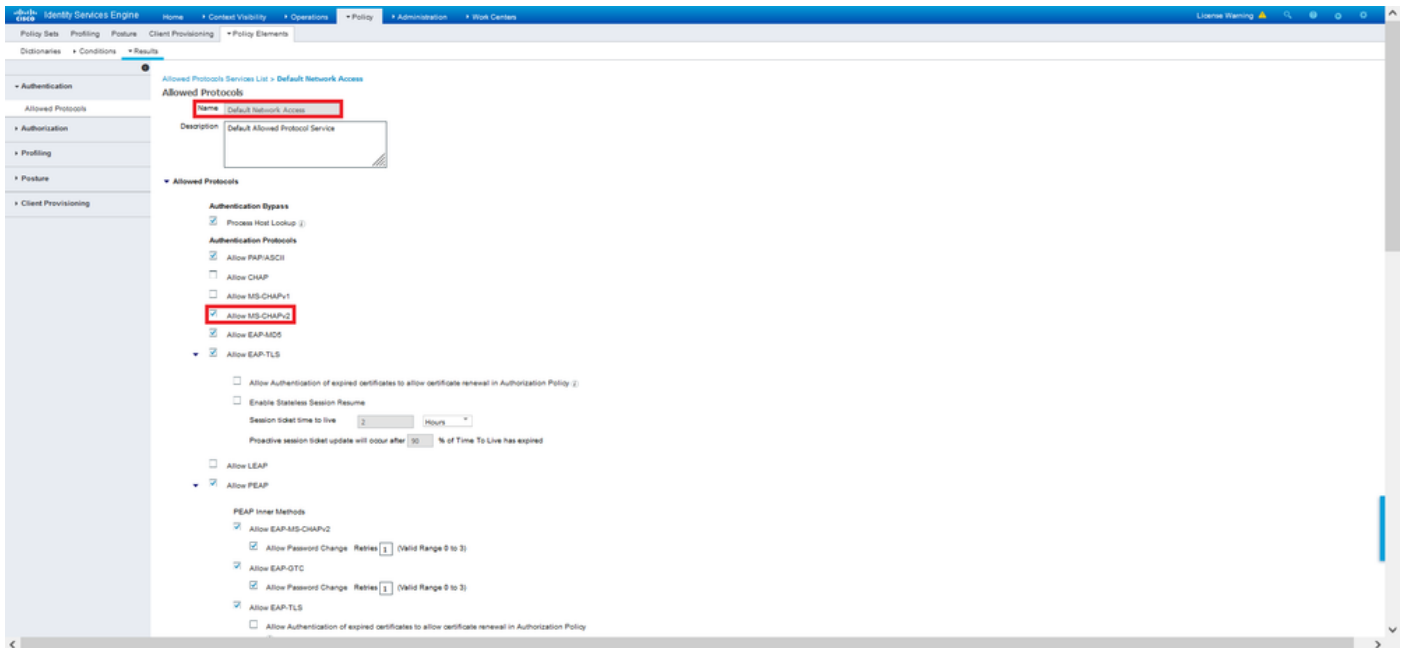
Paso 3. Vaya a **Política > Elementos de política > Resultados**. En **Authentication > Allowed Protocols** elija y edite **Default Network Access**.

The screenshot shows the 'Policy Elements' configuration page in Cisco ISE. A table lists the policy elements:

| Status  | Policy Set Name    | Description | Conditions | Allowed Protocols / Server Sequence | HHS | Actions | View |
|---------|--------------------|-------------|------------|-------------------------------------|-----|---------|------|
| Default | Default policy set |             |            | Default Network Access              | 24  |         |      |

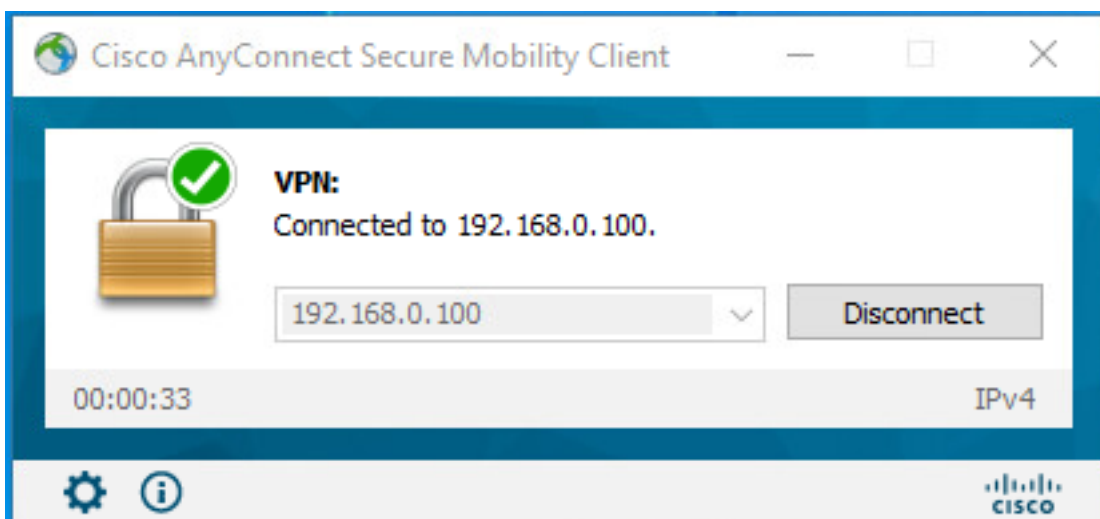


Asegúrese de que la casilla de verificación **Allow MS-CHAPv2** esté marcada. Desplácese hasta abajo y **guárdelo**.



## 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:

**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
10049 Evaluating Policy Group
10008 Evaluating Service Selection Policy
10041 Evaluating Identity Policy
10043 Queried PIP - Normalised RADIUS Radius/ForType (4 times)
22072 Selected Identity source sequence - All_User_ID_Stores
10019 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore - user1
24212 Found User in Internal Users IDStore
22037 Authentication Passed
24716 ISE has not confirmed locally previous successful machine authentication for user in Active Directory
10036 Evaluating Authorization Policy
24209 Looking up Endpoint in Internal Endpoints IDStore - user1
24211 Found Endpoint in Internal Endpoints IDStore
10043 Queried PIP - RADIUS User-Name
10018 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 00:06:02.94        |
| Received Timestamp            | 2021-09-28 00:06:02.94        |
| Policy Server                 | driverap-ISE-2-7              |
| 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 4F 45 0F 4F 50 42 50 97 19 57 56 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 2c a1 d9 a7 50 3c fc 8a 73 32 a9 50 54 27 00 5d 99 |
| CVPR3000ASAP307x Tunnel-Group-Name   | RA_VPN  |
| NetworkDeviceProfileId               | b0099005-3150-4215-a80a-d753a45b850a  |
| IsThirdPartyDeviceFlow               | false   |
| CVPR3000ASAP307x Client-Type         | 2   |
| AcxSessionId                         | driverap-ISE-2-7-1417494978-25  |
| SelectedAuthenticationIdentityStores | Internal Users  |
| SelectedAuthenticationIdentityStores | All_AD_Join_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  |
| CiscoRTPair       | <pre> mfm-du=device-platformmain mfm-du=device-manage00-50-50-90-40-0f mfm-du=device-platform-version10.0.18.352 mfm-du=device-publicname00-50-50-90-40-0f mfm-du=mac-user-agentAnyConnect-Windows 4.10.02080 mfm-du=device-typeVMware, Inc. VMware Virtual Platform mfm-du=device-uid globa=15878802C0F52F32C0E2431405F4BA2A2C0B8 mfm-du=device- user=3C38427071F90782F816F124621184408698C71E37D388CC03DF 944AC8880344 audit-session-id=d8a30054000a000e1025c49 @source-ip=192.168.0.101, 00a-push@vive </pre> |

|                   |  |
|-------------------|--|
| 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  |
| CiscoRTPair       | <pre> mfm-du=device-platformmain mfm-du=device-manage00-50-50-90-40-0f mfm-du=device-platform-version10.0.18.352 mfm-du=device-publicname00-50-50-90-40-0f mfm-du=mac-user-agentAnyConnect-Windows 4.10.02080 mfm-du=device-typeVMware, Inc. VMware Virtual Platform mfm-du=device-uid globa=15878802C0F52F32C0E2431405F4BA2A2C0B8 mfm-du=device- user=3C38427071F90782F816F124621184408698C71E37D388CC03DF 944AC8880344 audit-session-id=d8a30054000a000e1025c49 @source-ip=192.168.0.101, 00a-push@vive </pre> |

### Result

|                   |  |
|-------------------|--|
| Framed IP Address | 10.0.50.101  |
| Class             | CACS-d8a30054000a000e1025c49 driverap-ISE-2-7-1417494978-25  |
| class-av-pair     | profile-name=Windows10-Workstation   |
| MS-CHAP2-Success  | 00 23 3a 33 30 33 40 33 30 37 38 34 42 43 45 32 33 45 41 31 39 37 37 32 44 48 39 38 44 41 38 37 31 38 44 28 41 43 48 43 41 |
| LicenseTypes      | Basic license consumed   |

### Session Events

**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