Configure FTD Remote Access VPN with MSCHAPv2 over RADIUS

Contents

Introduction

This document describes how to enable Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) as the authentication method via Firepower Management Center (FMC) for Remote Access VPN clients with Remote Authentication Dial-In User Service (RADIUS) authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

The information in this document is based on these software versions:

- FMCv - 7.0.0 (build 94)
- FTDv - 7.0.0 (Build 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

By default, FTD uses Password Authentication Protocol (PAP) as the authentication method with RADIUS servers for AnyConnect VPN connections.

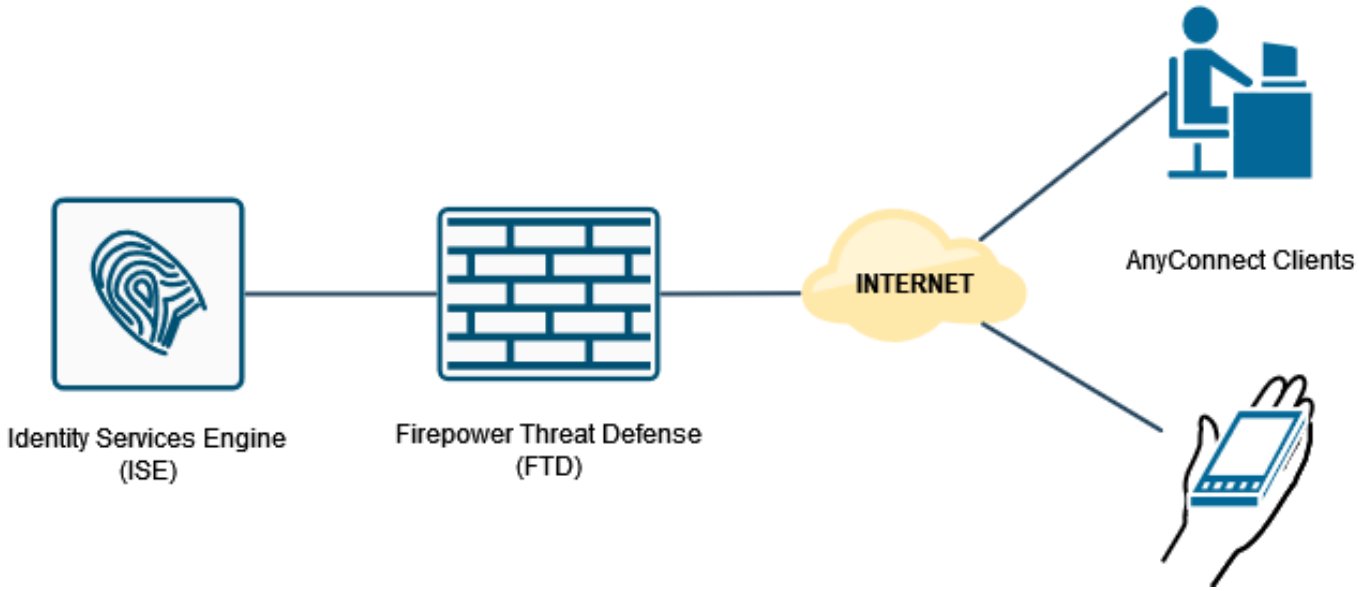
PAP provides a simple method for users to establish their identity with a two-way handshake. The PAP password is encrypted with a shared secret and is the least sophisticated authentication protocol. PAP is not a strong authentication method because it offers little protection from repeated trial-and-error attacks.

MS-CHAPv2 authentication introduces mutual authentication between peers and a change password feature.

In order to enable MS-CHAPv2 as the protocol used between the ASA and the RADIUS server for a VPN connection, password management must be enabled in the Connection Profile. Enabling password management generates an MS-CHAPv2 authentication request from the FTD to the RADIUS server.

Configure

Network Diagram



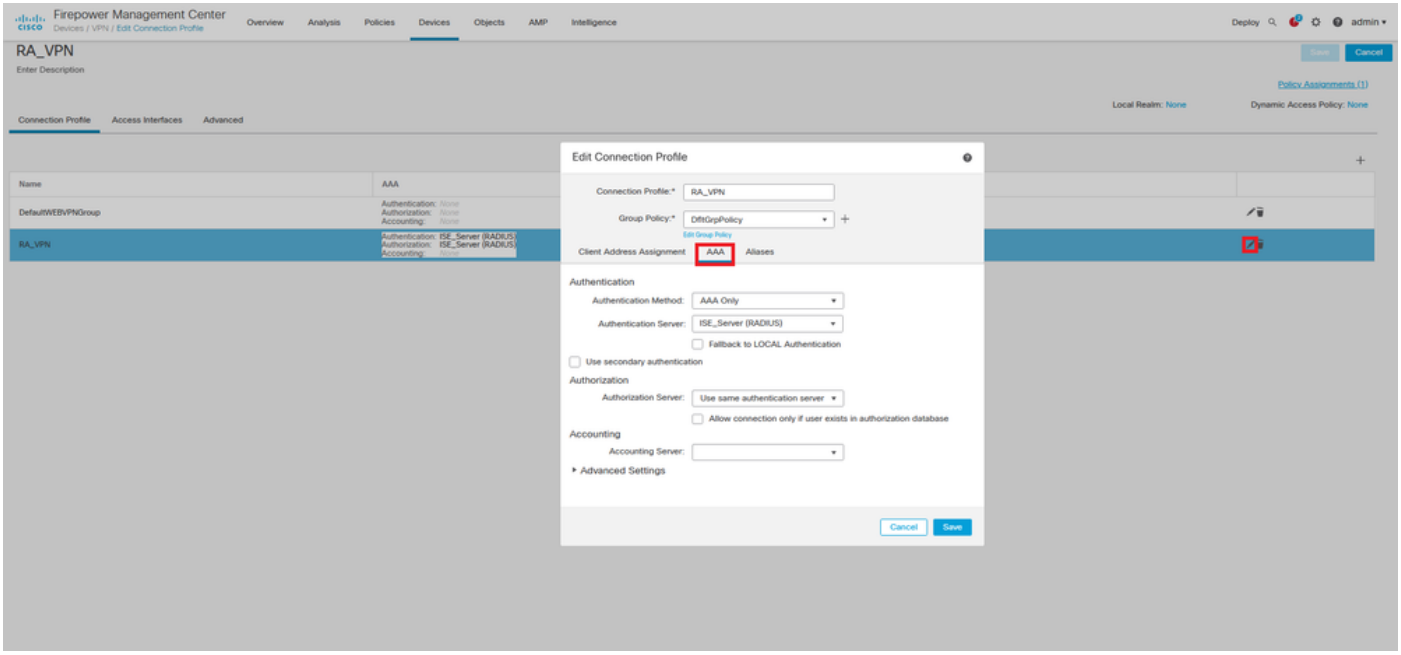
Configure RA VPN with AAA/RADIUS Authentication via FMC

For a step-by-step procedure, refer to this document and this video:

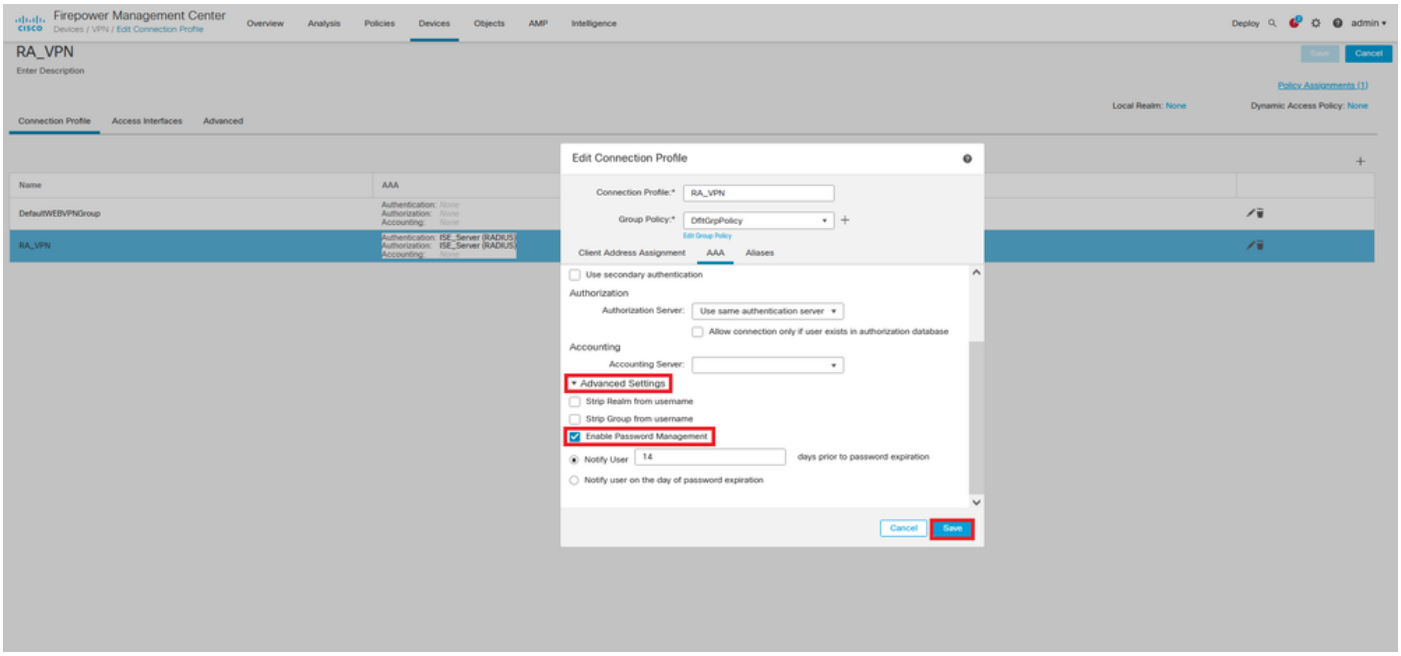
- AnyConnect Remote Access VPN Configuration on FTD

- [Initial AnyConnect Configuration for FTD Managed by FMC]

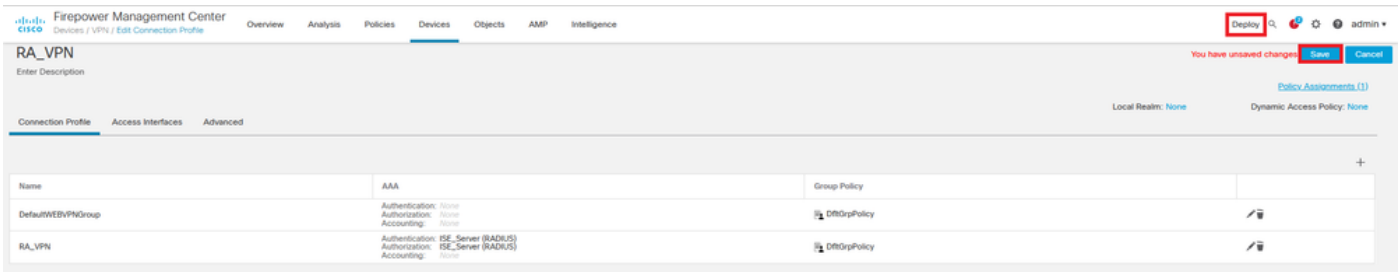
Step 1. Once Remote Access VPN is configured, navigate to **Devices > Remote Access**, edit the newly created Connection Profile and then navigate to the **AAA** tab.



Expand the **Advanced Settings** section and click the **Enable Password Management** check box. Click **Save**.



Save and **Deploy**.



Remote Access VPN configuration on 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
```

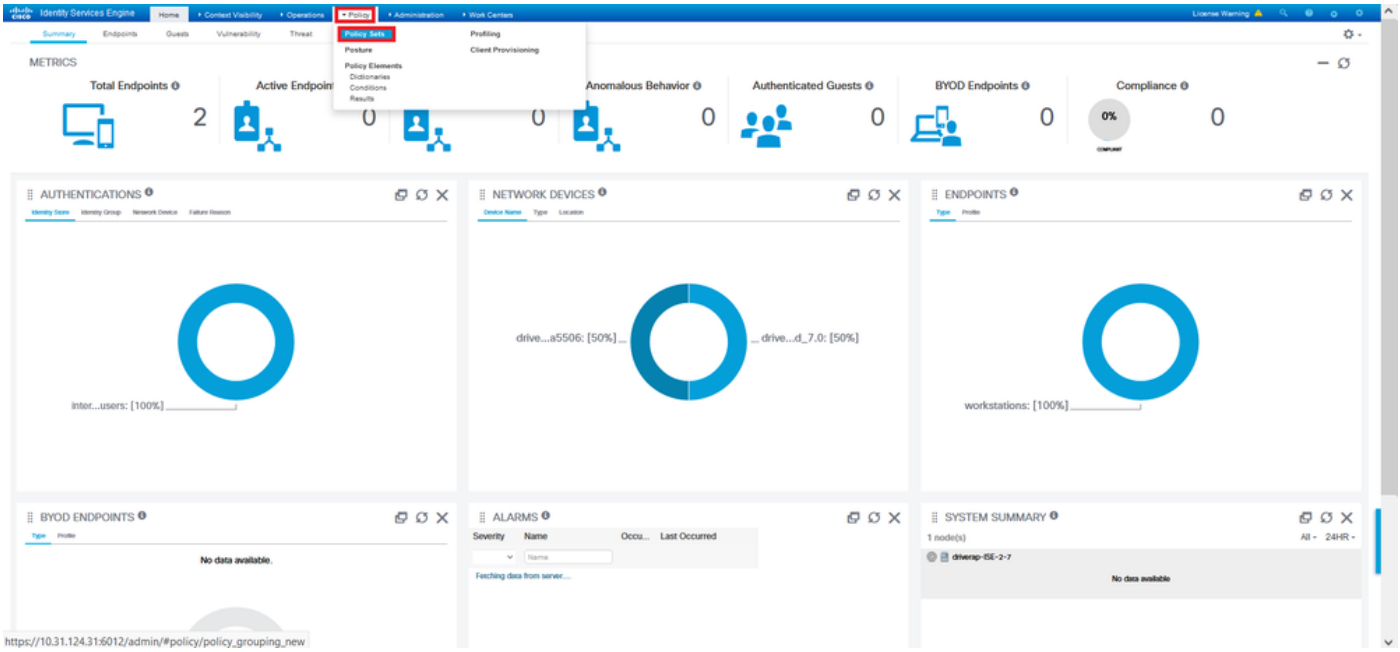
```
password-management
tunnel-group RA_VPN webvpn-attributes
group-alias RA_VPN enable
```

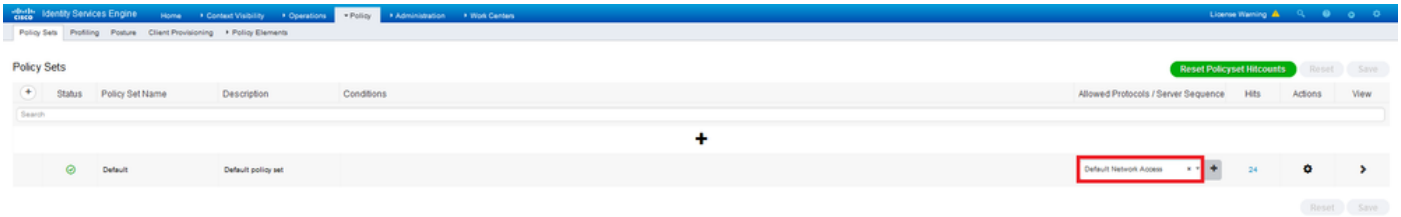
Configure ISE to Support MS-CHAPv2 as Authentication Protocol

It is assumed that:

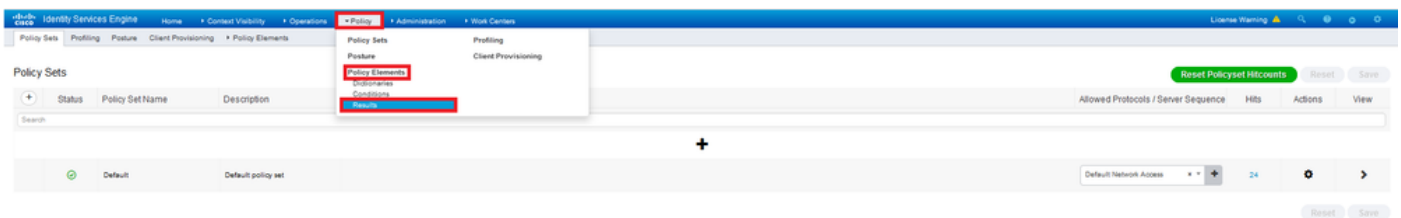
1. The FTD is already added as a Network Device on ISE so it can proccess RADIUS Access Requests from the FTD.
2. There is at least one user available for ISE to authenticate the AnyConnect client.

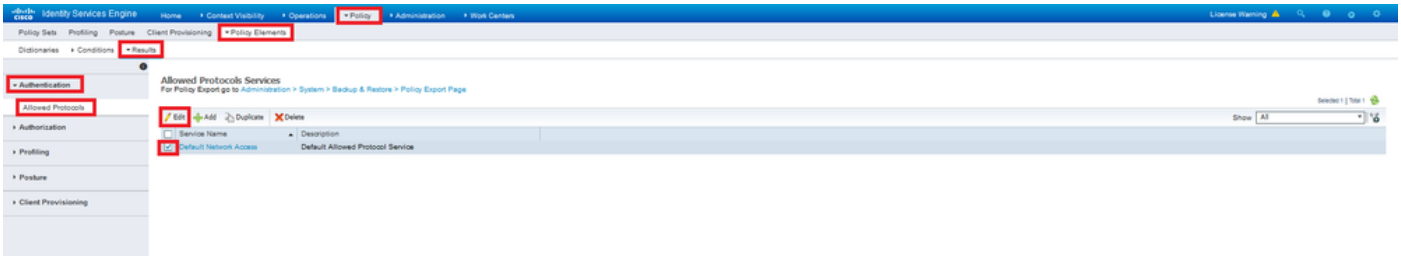
Step 2. Navigate to **Policy > Policy Sets** and find the **Allowed Protocols** policy attached to the Policy Set where your AnyConnect Users are authenticated. In this example, only one Policy Set is present so the policy in question is *Default Network Access*.



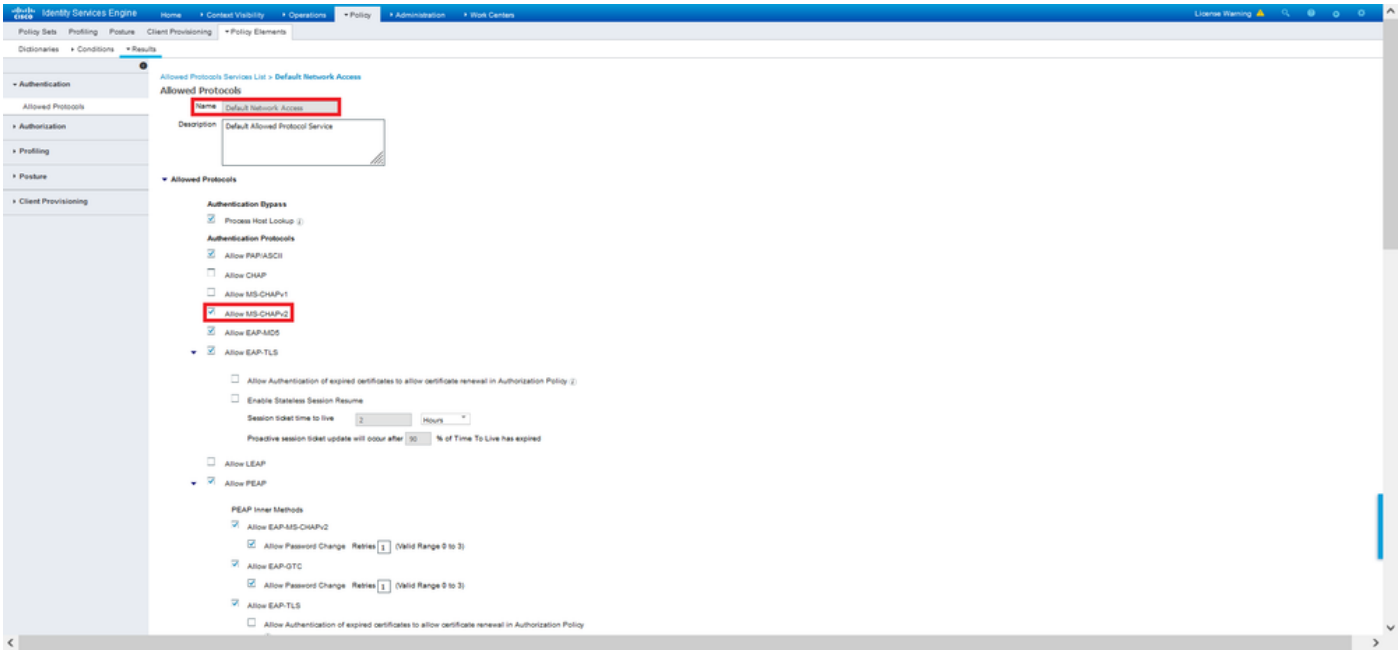


Step 3. Navigate to **Policy > Policy Elements > Results.** Under **Authentication > Allowed Protocols** choose and edit **Default Network Access**.



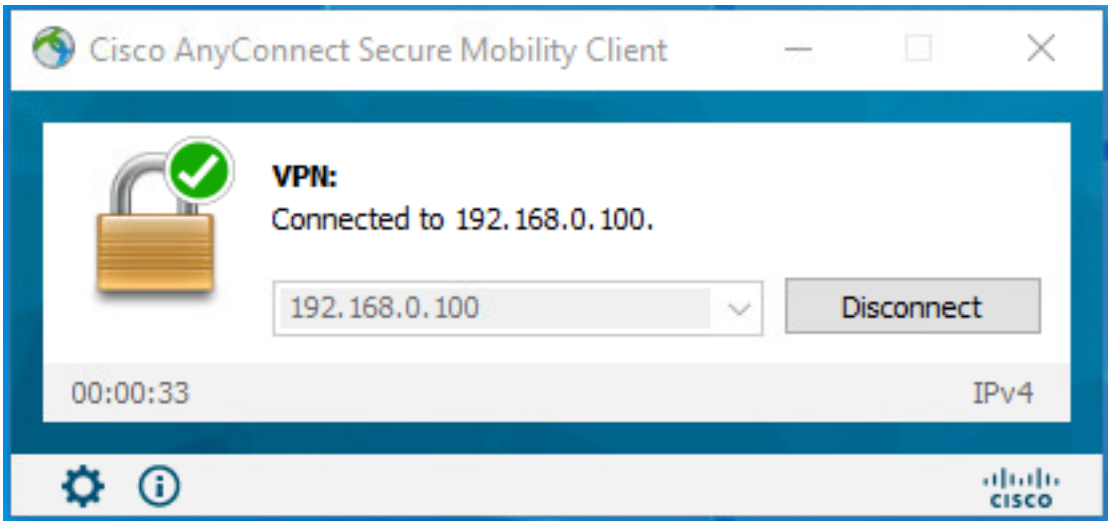


Make sure the **Allow MS-CHAPv2** check box is checked. Scroll all the way down and **Save** it.

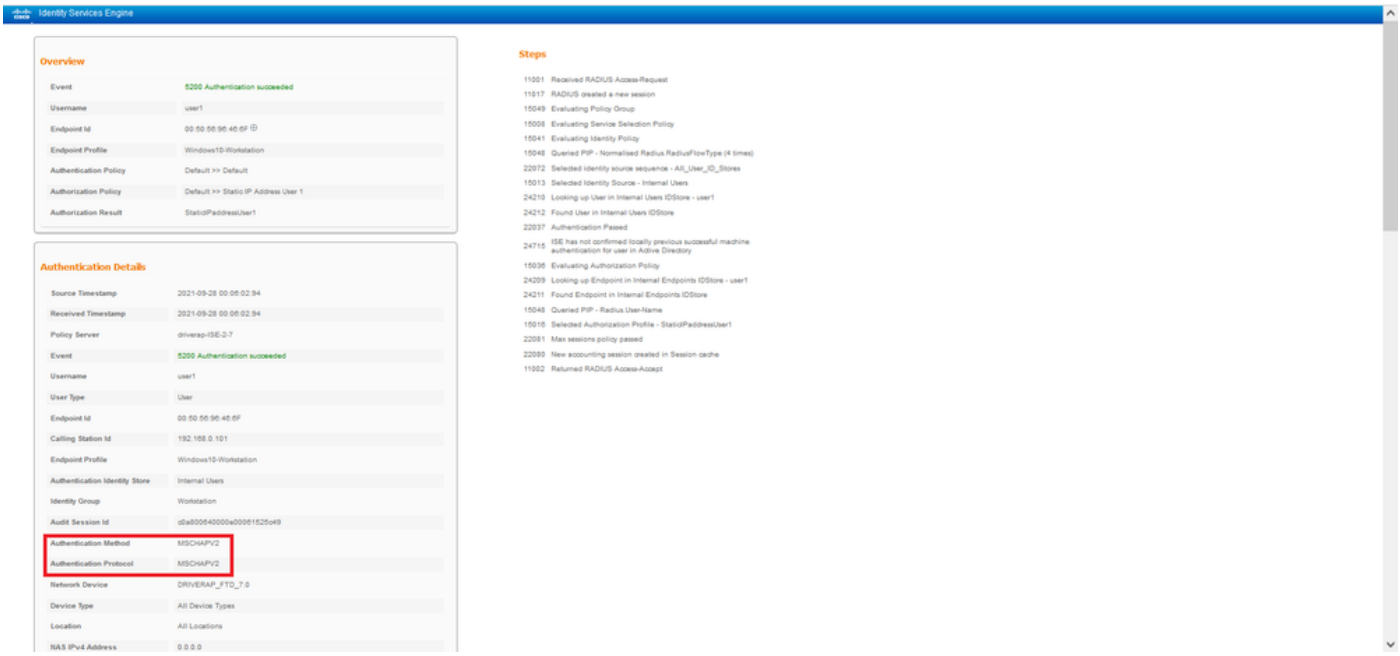


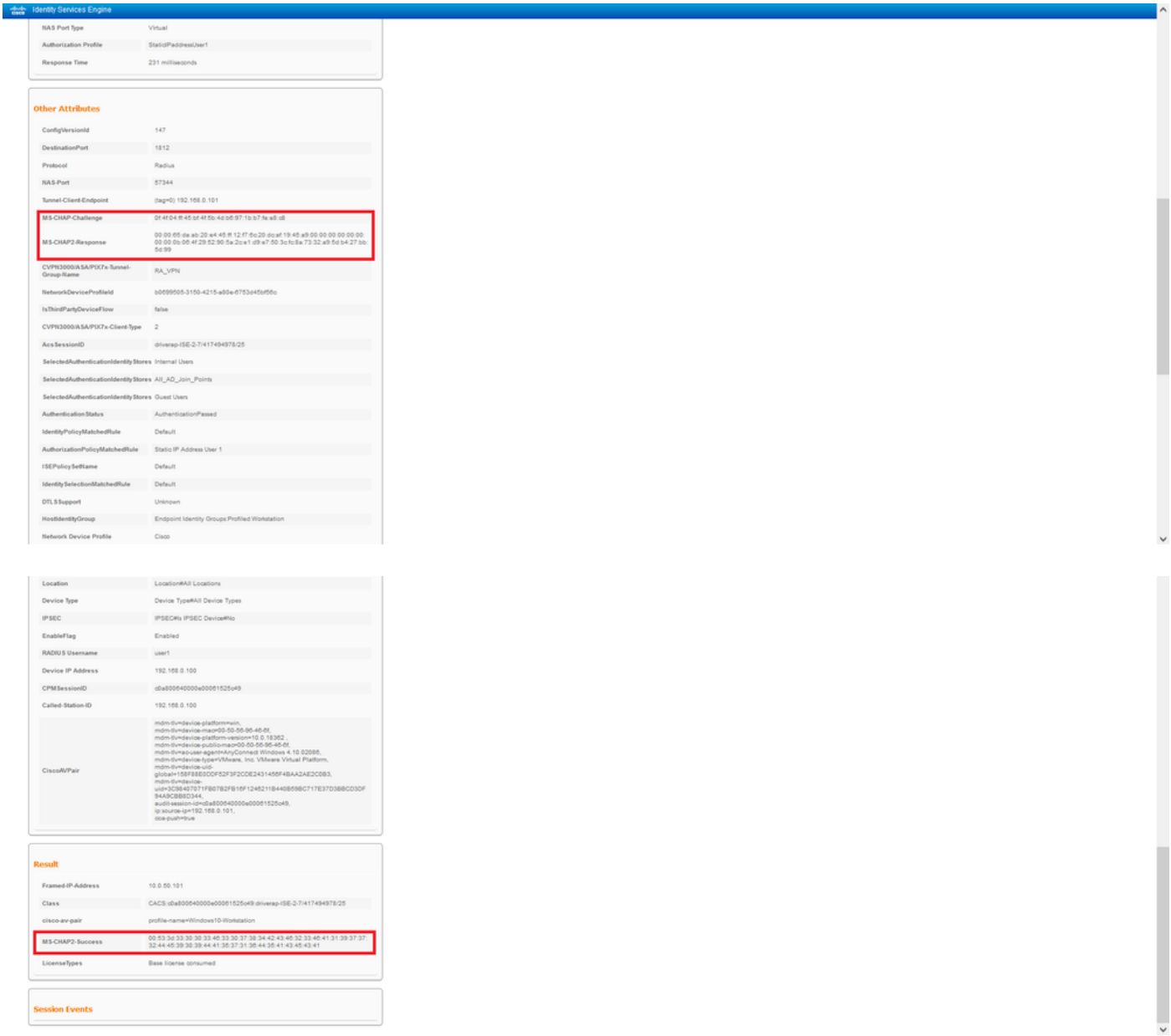
Verify

Navigate to your client machine where the Cisco AnyConnect Secure Mobility client is installed. Connect to the FTD headend (a Windows machine is used in this example) and type the user credentials.



The RADIUS Live Logs on ISE show:





Note: The **test aaa-server authentication** command always uses PAP to send

authentication requests to the RADIUS server, there is no way to force the firewall to use MS-CHAPv2 with this command.

firepower# **test aaa-server authentication ISE_Server host 172.16.0.8 username user1 password XXXXXX**
INFO: Attempting Authentication test to IP address (172.16.0.8) (timeout: 12 seconds)
INFO: Authentication Successful

Note: Do not modify **tunnel-group ppp-attributes** via Flex-config as this takes no effect on the Authentication Protocols negotiated over RADIUS for AnyConnect VPN (SSL and IPSec) connections.

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

This section provides the information you can use in order to troubleshoot your configuration.

On FTD:

- **debug radius all**

On ISE:

- RADIUS live logs