

Configure FTD Remote Access VPN with MSCHAPv2 over RADIUS

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[Configure RA VPN with AAA/RADIUS Authentication via FMC](#)

[Configure ISE to Support MS-CHAPv2 as Authentication Protocol](#)

[Verify](#)

[Troubleshoot](#)

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.

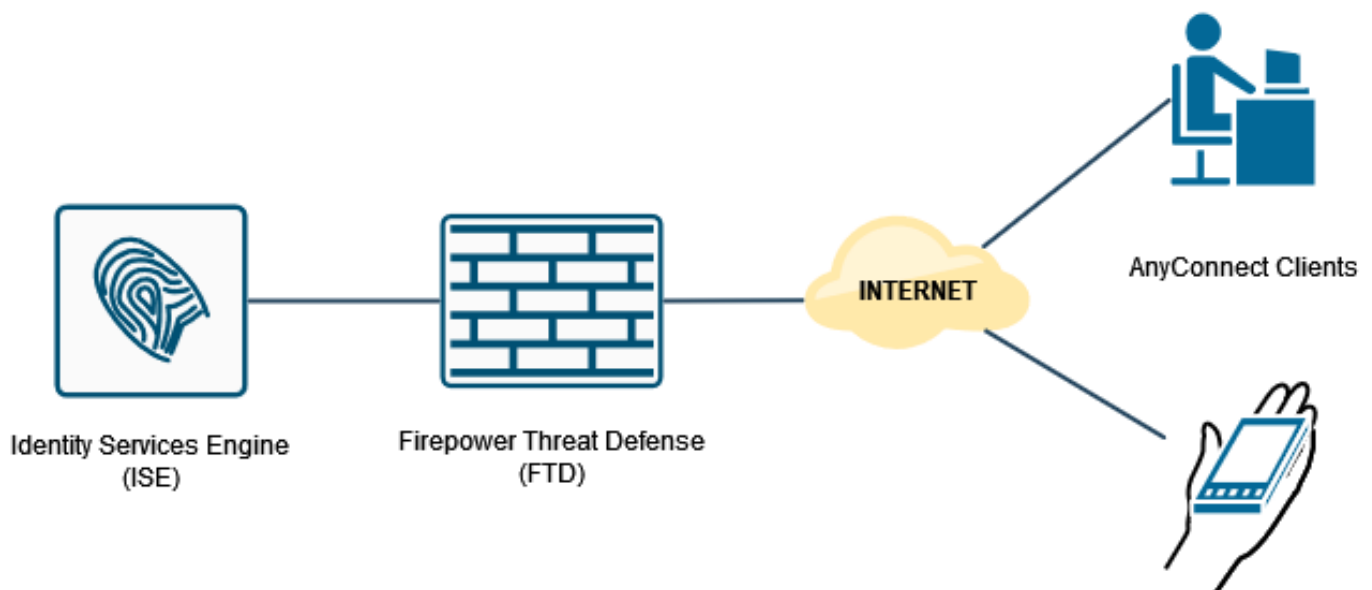
PAP provides a simple method for users to establish their identity with a two-way handshake. The PAP password is encrypted with a shared secret and is the least sophisticated authentication protocol. PAP is not a strong authentication method because it offers little protection from repeated trial-and-error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



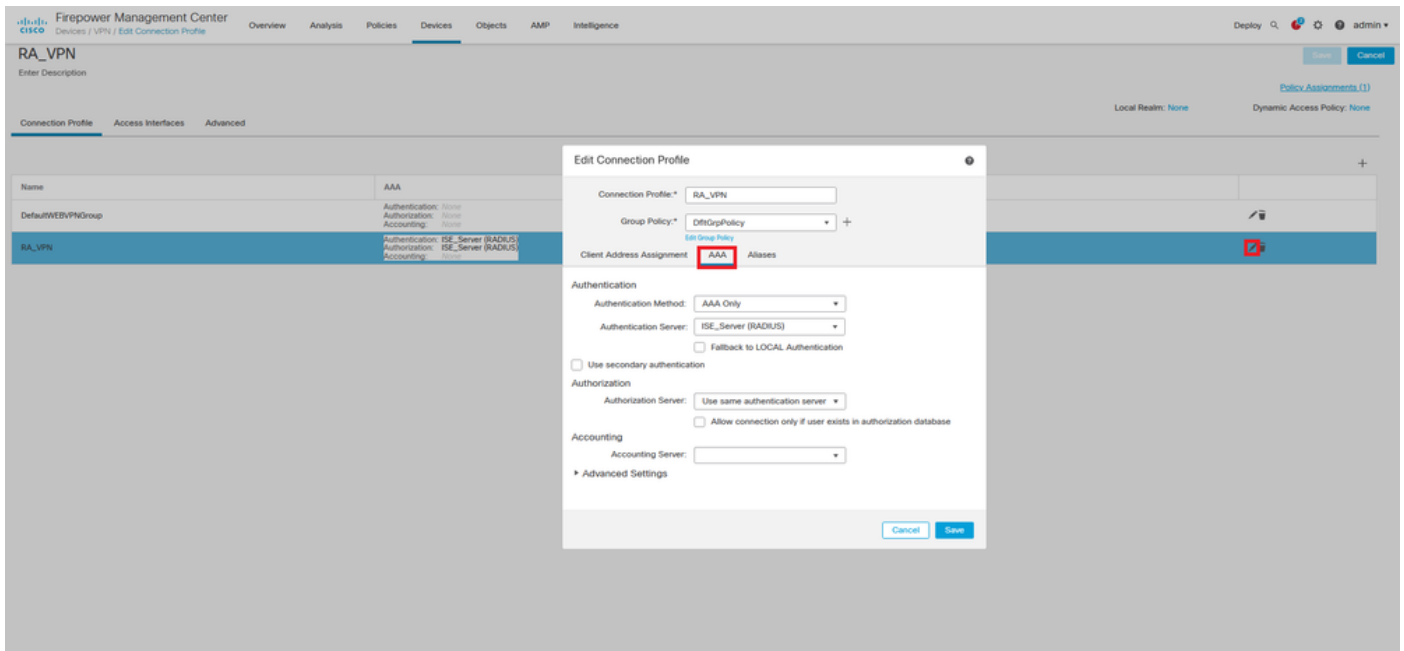
Configure RA VPN with AAA/RADIUS Authentication via FMC

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

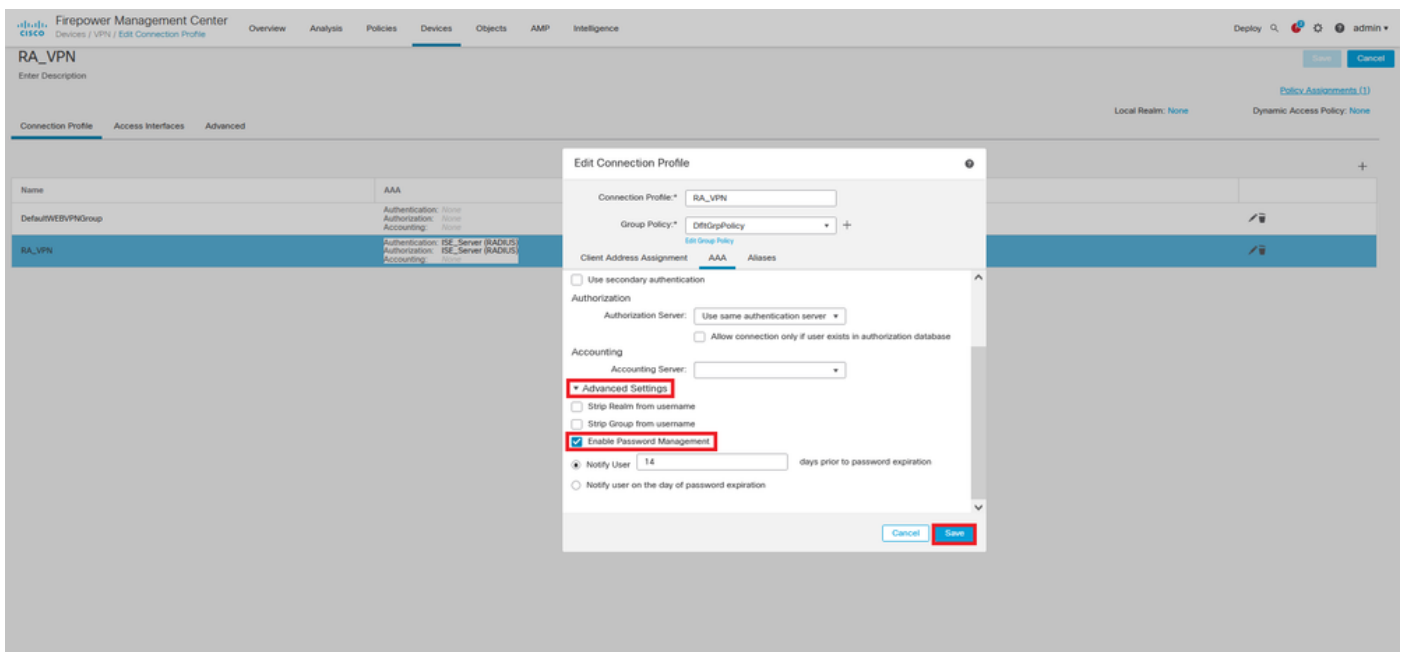
- [AnyConnect Remote Access VPN Configuration on FTD](#)

- [Initial AnyConnect Configuration for FTD Managed by FMC](#)

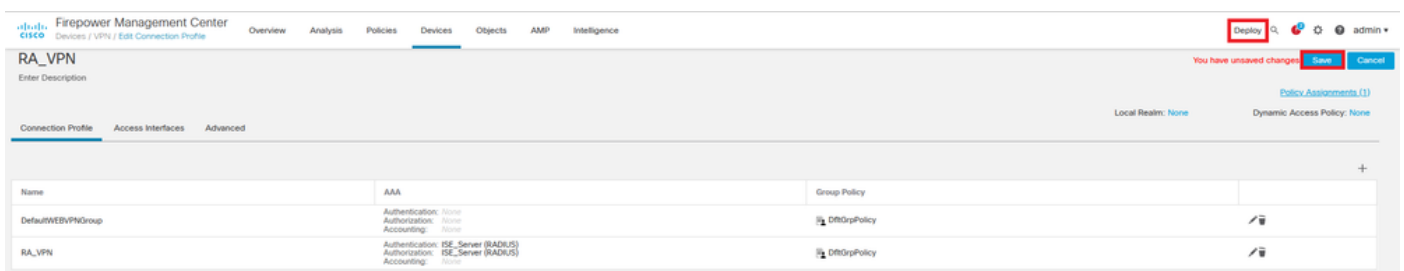
Step 1. Once Remote Access VPN is configured, navigate to **Devices > Remote Access**, edit the newly created Connection Profile and then navigate to the **AAA** tab.



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

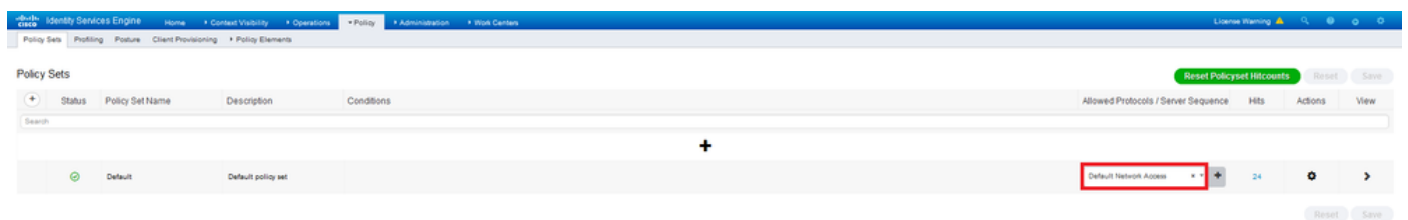
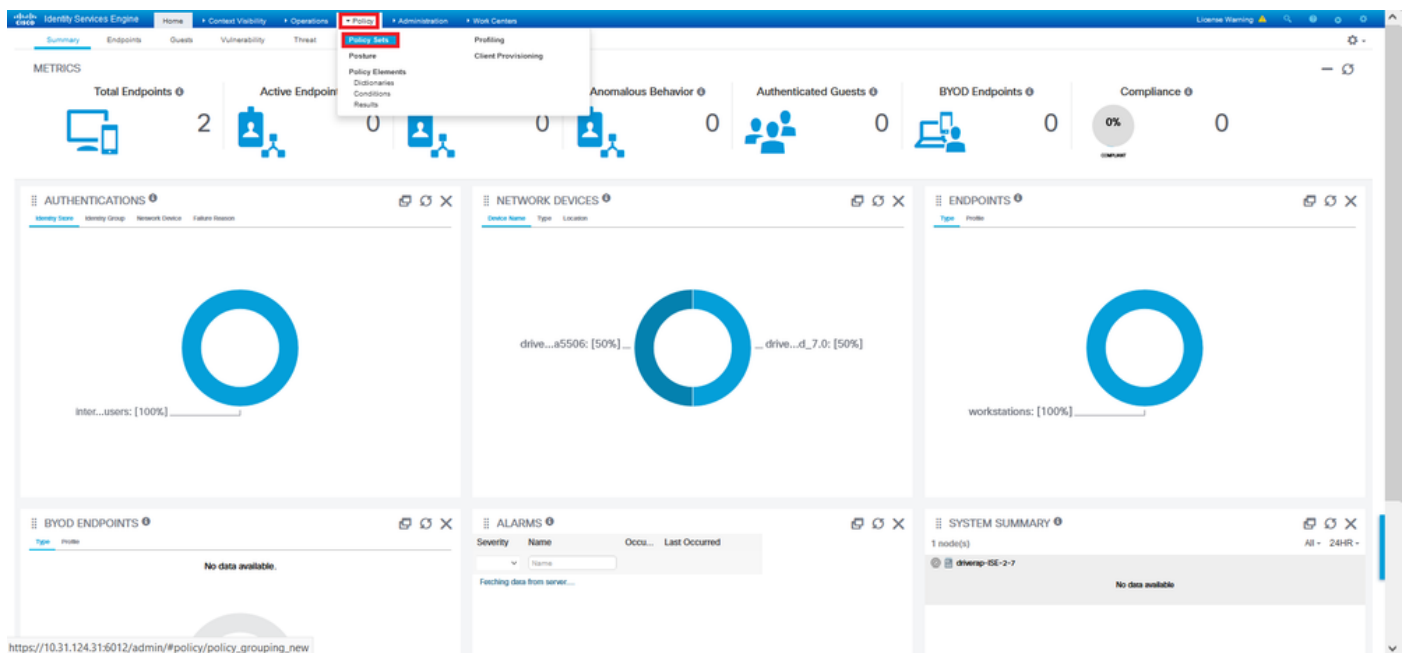
group-alias RA_VPN enable

Configure ISE to Support MS-CHAPv2 as Authentication Protocol

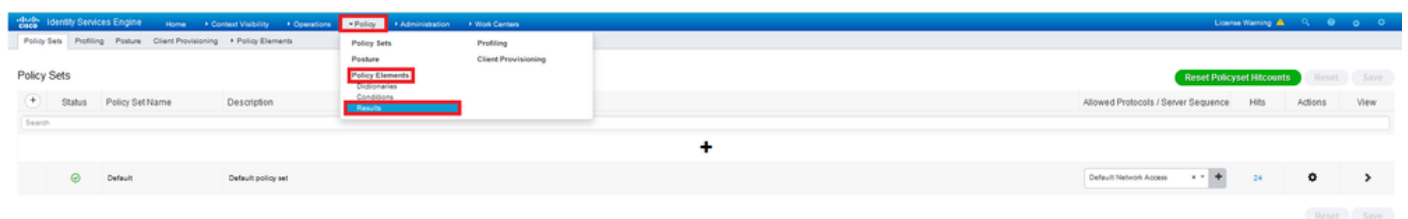
It is assumed that:

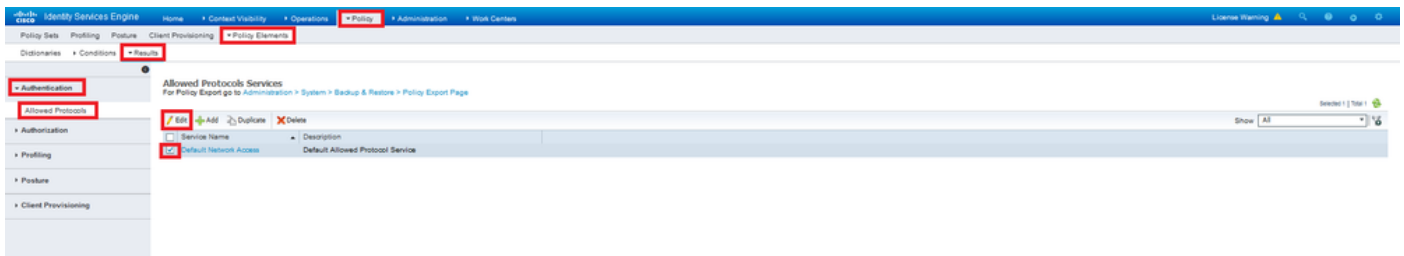
1. The FTD is already added as a Network Device on ISE so it can process RADIUS Access Requests from the FTD.
2. There is at least one user available for ISE to authenticate the AnyConnect client.

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*.

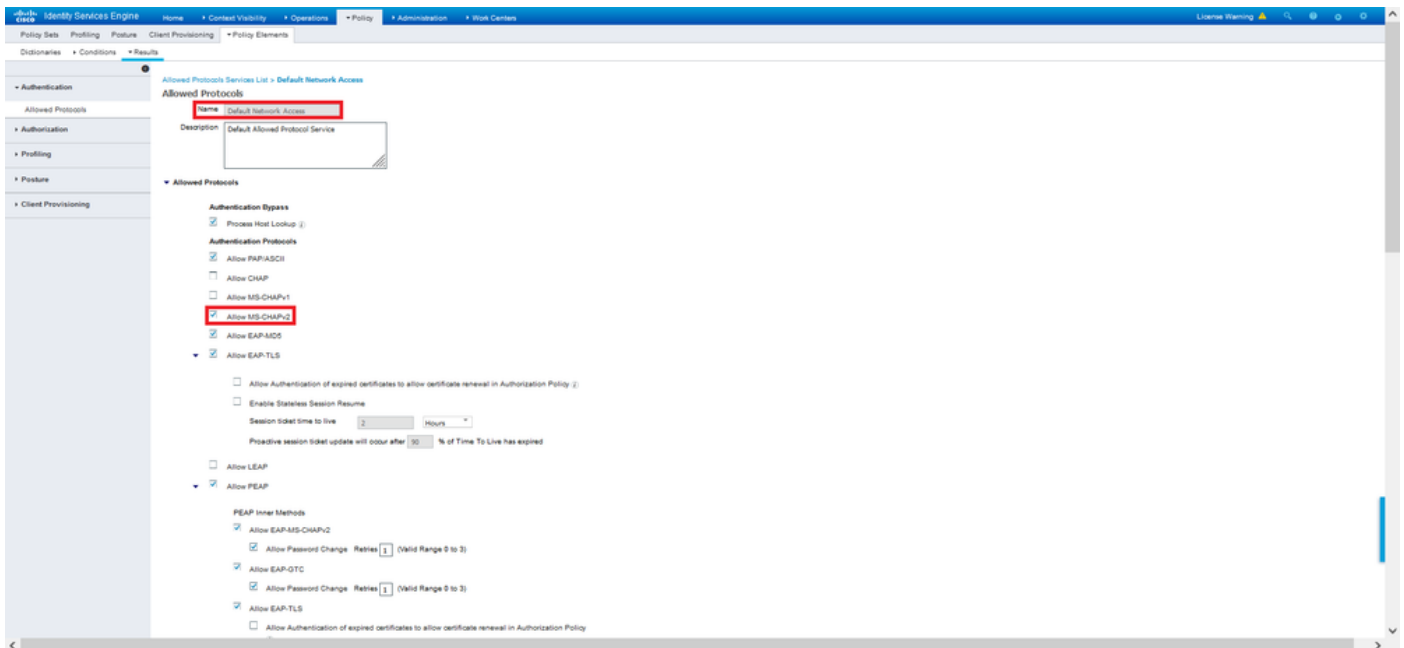


Step 3. Navigate to **Policy > Policy Elements > Results**. Under **Authentication > Allowed Protocols** choose and edit **Default Network Access**.



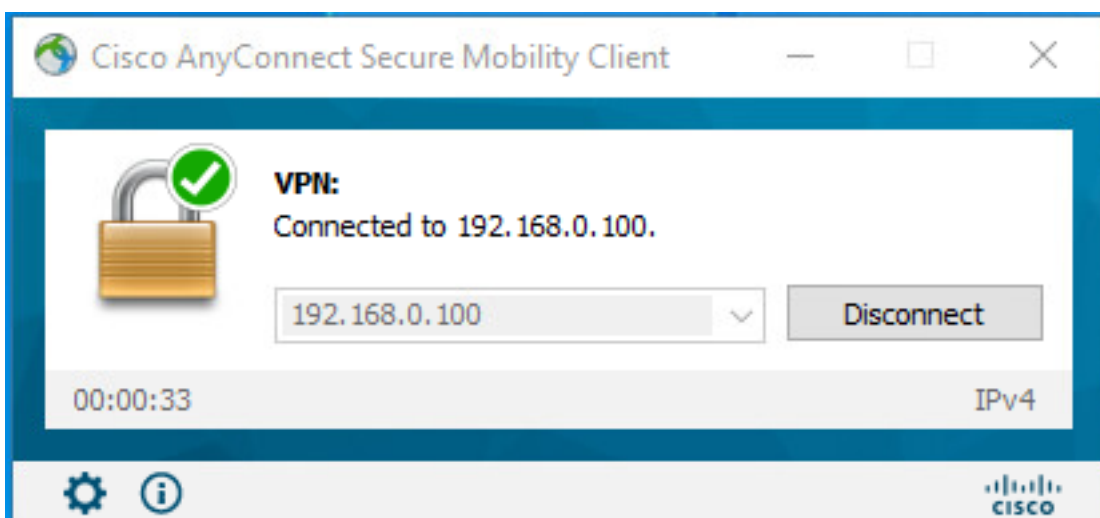


Make sure the **Allow MS-CHAPv2** check box is checked. Scroll all the way down and **Save** it.



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:

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
10048 Queried PIP - Normalised RADIUS RadiusForType (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
10048 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	drivrap-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 9F 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 50 99
CVPR3000ASAPROK7x Tunnel-Group-Name	RA_VPN
NetworkDeviceProfileId	b0099005-3150-4215-a80a-d753a45b850a
IsThirdPartyDeviceFlow	false
CVPR3000ASAPROK7x Client-Type	2
AcxSessionId	drivrap-ISE-2-71417494978-25
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
CiscoAPPar	<pre> mfm-dm-device-platform=main mfm-dm-device-manuf=00 50 50 90 40 0F 0 mfm-dm-device-platform-version=10.0.18.352 mfm-dm-device-public-manuf=00 50 50 90 40 0F 0 mfm-dm-device-agent=AnyConnect_VirtWpoc 4.10.02080 mfm-dm-device-type=VMware, Inc. VMware Virtual Platform mfm-dm-device-uid= globa=15878802C0F52F32C0E2431405F4BA2A2C0B3 mfm-dm-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 drivrap-ISE-2-71417494978-25
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 39 37 31 38 44 28 41 43 48 43 41
License Types	Basic license consumed

Session Events

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