RADIUS上のMSCHAPv2を使用したFTDリモートアクセスVPNの設定

内容

概要

このドキュメントでは、リモート認証ダイヤルインユーザサービス(RADIUS)認証を使用するリモートアクセスVPNクライアントのFirepower Management Center(FMC)を介した認証方式として、Microsoft Challenge Handshake Authentication Protocol(MS-CHAPv2)を有効にする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Firepower Threat Defense(FTD)
- Firepower Management Center（FMC）
- Identity Services Engine（ISE）
- Cisco AnyConnect セキュア モビリティ クライアント
- RADIUS プロトコル

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- FMCv - 7.0.0（ビルド94）
- FTDv - 7.0.0（ビルド94）
- ISE:2.7.0.356

- AnyConnect - 4.10.02086
- Windows 10 Pro

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

デフォルトでは、FTDはAnyConnect VPN接続用のRADIUSサーバの認証方式としてパスワード認証プロトコル(PAP)を使用します。

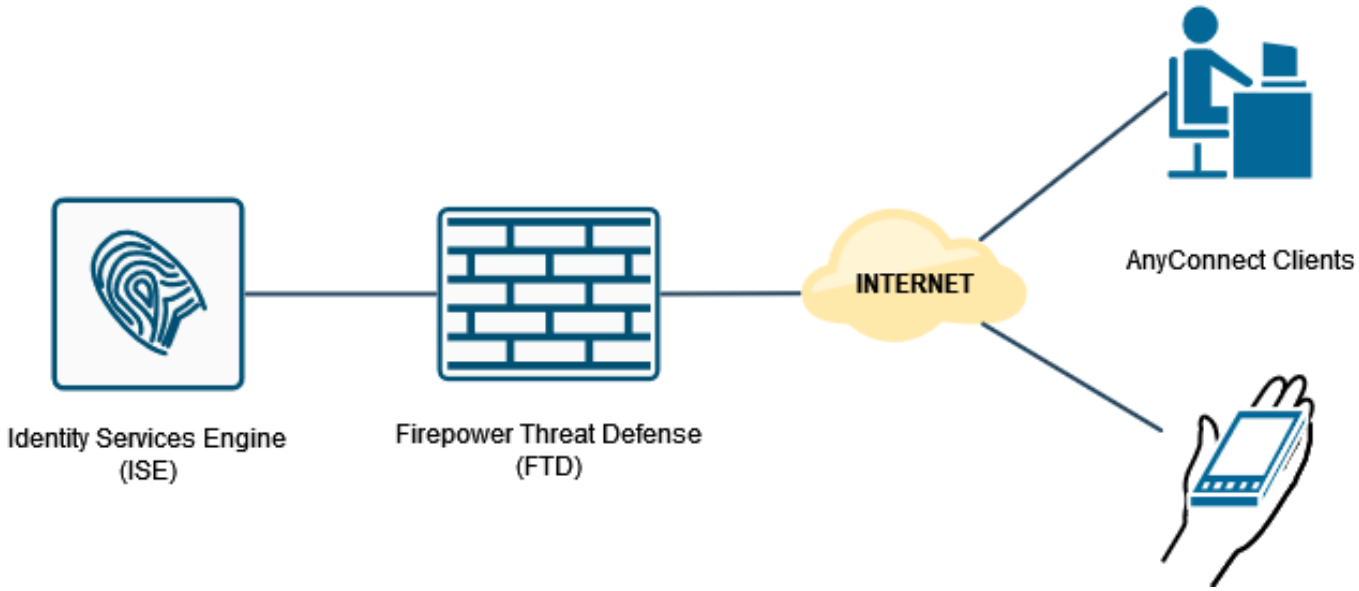
PAPは、ユーザが双方向ハンドシェイクでIDを確立するための簡単な方法を提供します。PAPパスワードは共有秘密で暗号化され、最も高度ではない認証プロトコルです。PAPは、繰り返し発生する試行錯誤からの保護をほとんど提供しないため、強力な認証方式ではありません。

MS-CHAPv2認証では、ピア間の相互認証とパスワード変更機能が導入されます。

VPN接続用にASAとRADIUSサーバ間で使用されるプロトコルとしてMS-CHAPv2を有効にするには、接続プロファイルでパスワード管理を有効にする必要があります。パスワード管理を有効にすると、FTDからRADIUSサーバへのMS-CHAPv2認証要求が生成されます。

設定

ネットワーク図

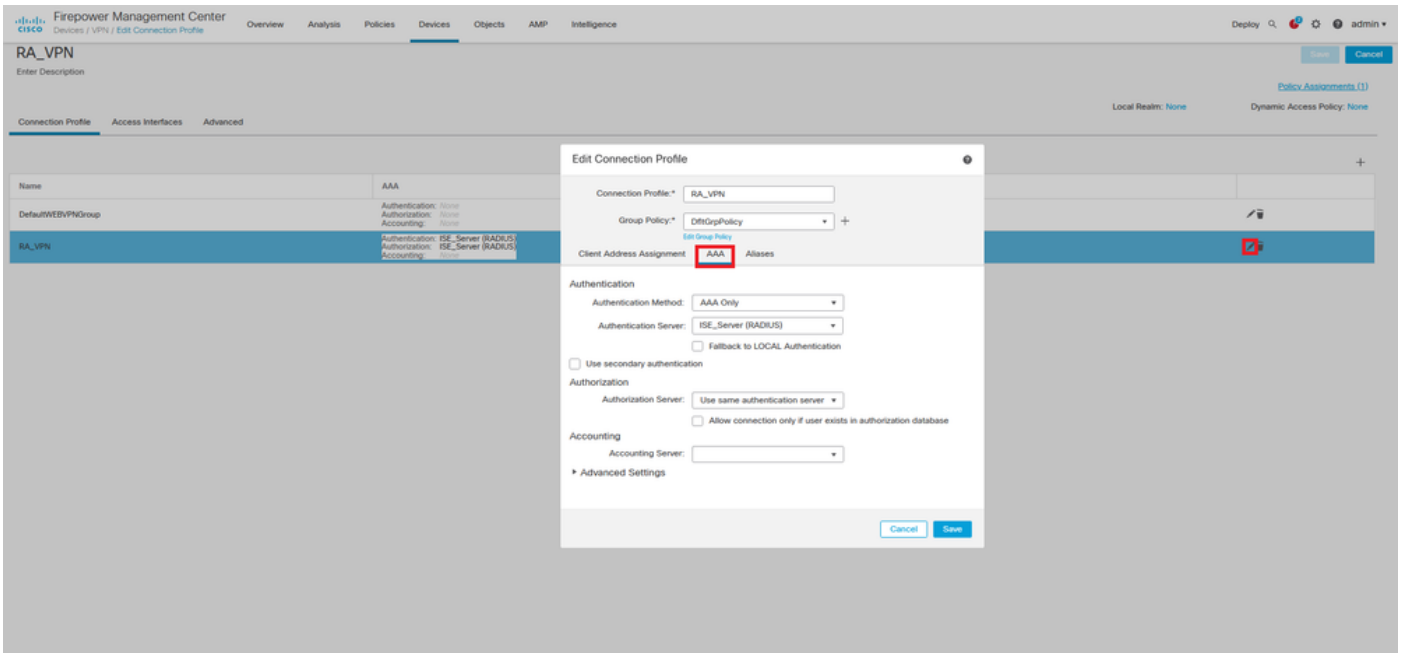


FMCによるAAA/RADIUS認証を使用したRA VPNの設定

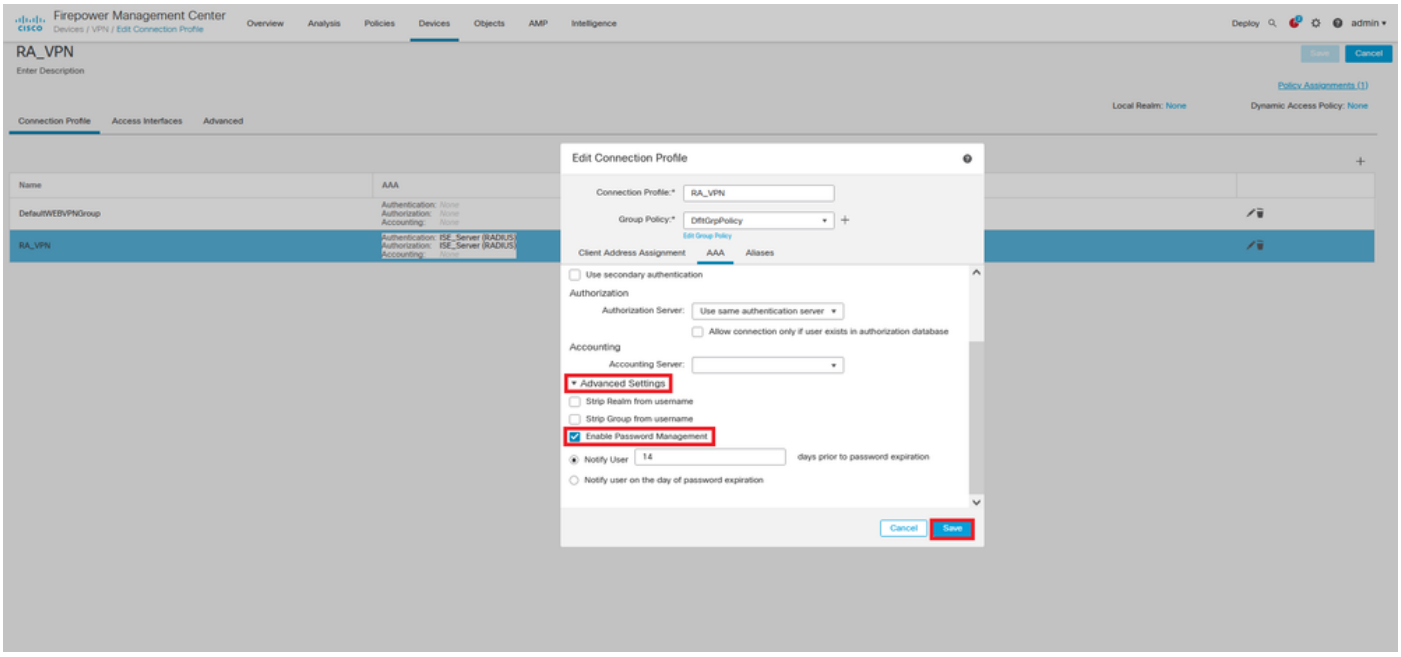
手順については、次のドキュメントとビデオを参照してください。

- FTD での AnyConnect Remote Access VPN の設定
- FMCによって管理されるFTDの初期AnyConnect設定

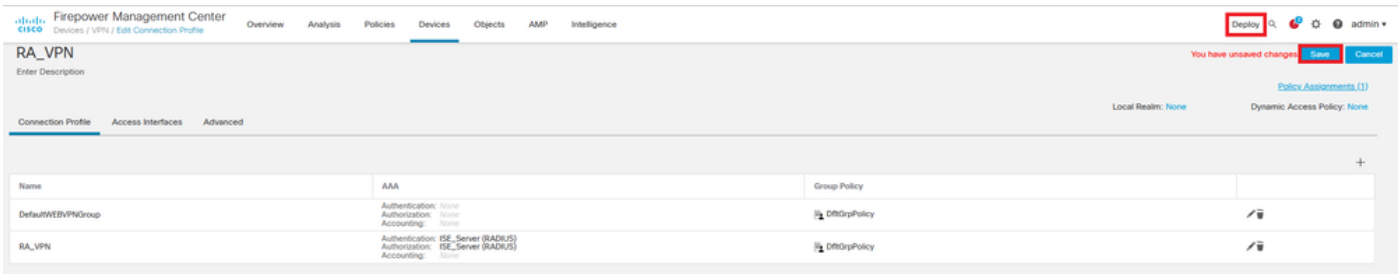
ステップ1：リモートアクセスVPNが設定されたら、[Devices] > [Remote Access]に移動し、新しく作成した接続プロファイルを編集して、[AAA]タブに移動します。



[詳細設定]セクションを展開し、[パスワード管理の有効]チェックボックスをオンにします。[Save] をクリックします。



保存して展開。



FTD CLIでのリモートアクセスVPNの設定は次のとおりです。

```
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
```

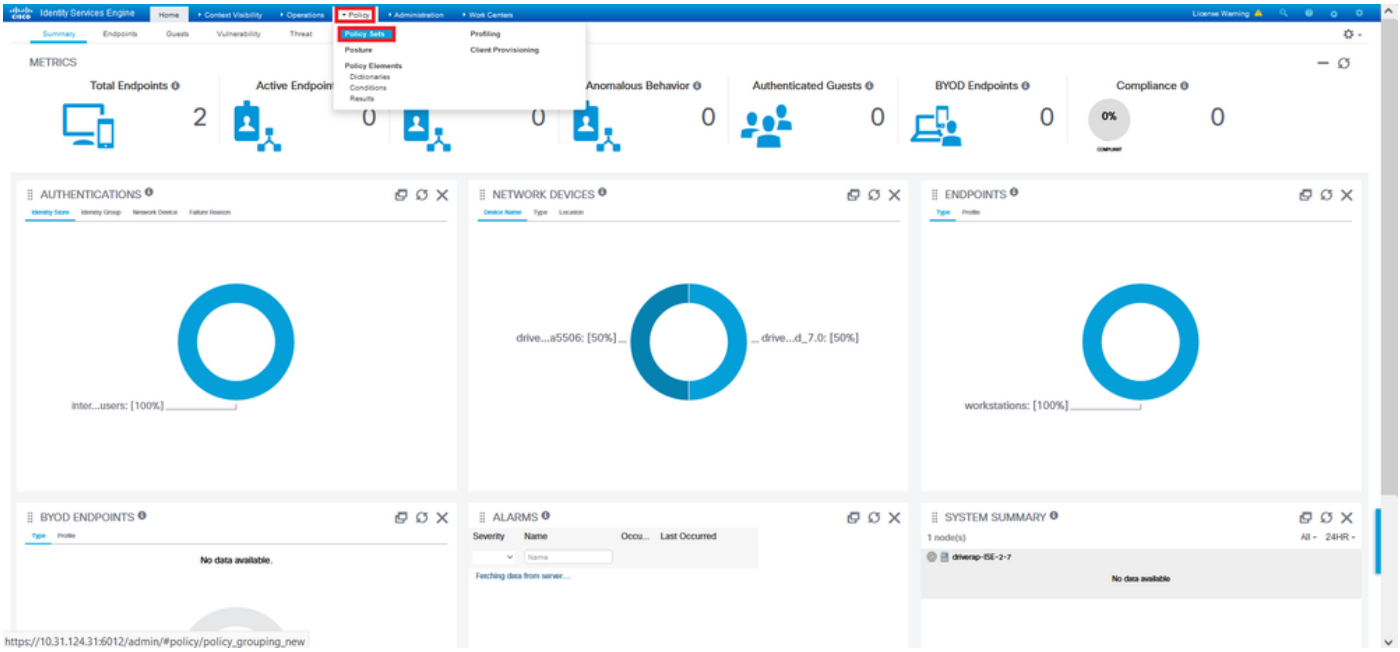
```
group-alias RA_VPN enable
```

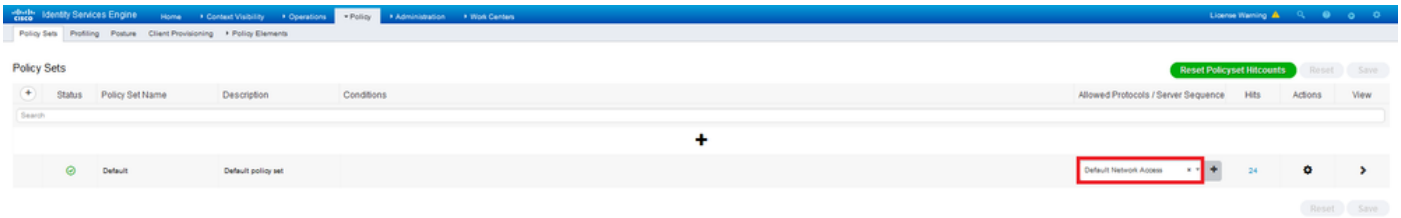
MS-CHAPv2を認証プロトコルとしてサポートするためのISEの設定

次のことを前提としています。

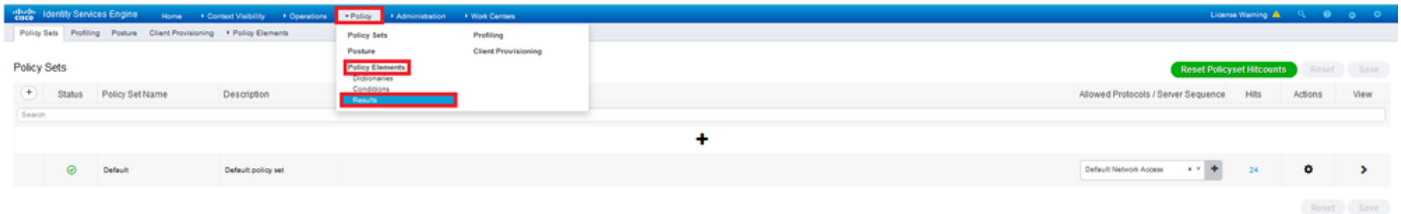
1. FTDはISEのネットワークデバイスとしてすでに追加されているため、FTDからRADIUSアクセス要求を処理できます。
2. ISEがAnyConnectクライアントを認証するために使用できるユーザが少なくとも1人あります。

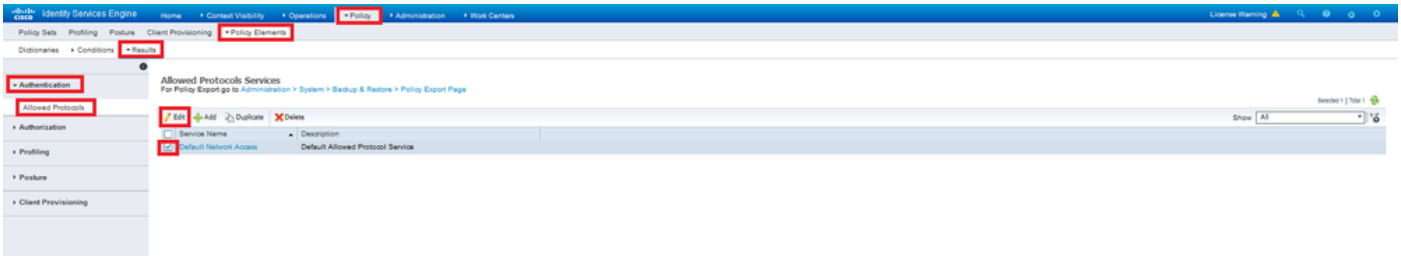
ステップ2:[**Policy**] > [Policy Sets]に移動し、AnyConnectユーザが認証されたポリシーセットに関連付けられている[Allowed Protocols]ポリシーを見つけます。この例では、1つのポリシーセットのみが存在するため、対象のポリシーは*Default Network Access*です。



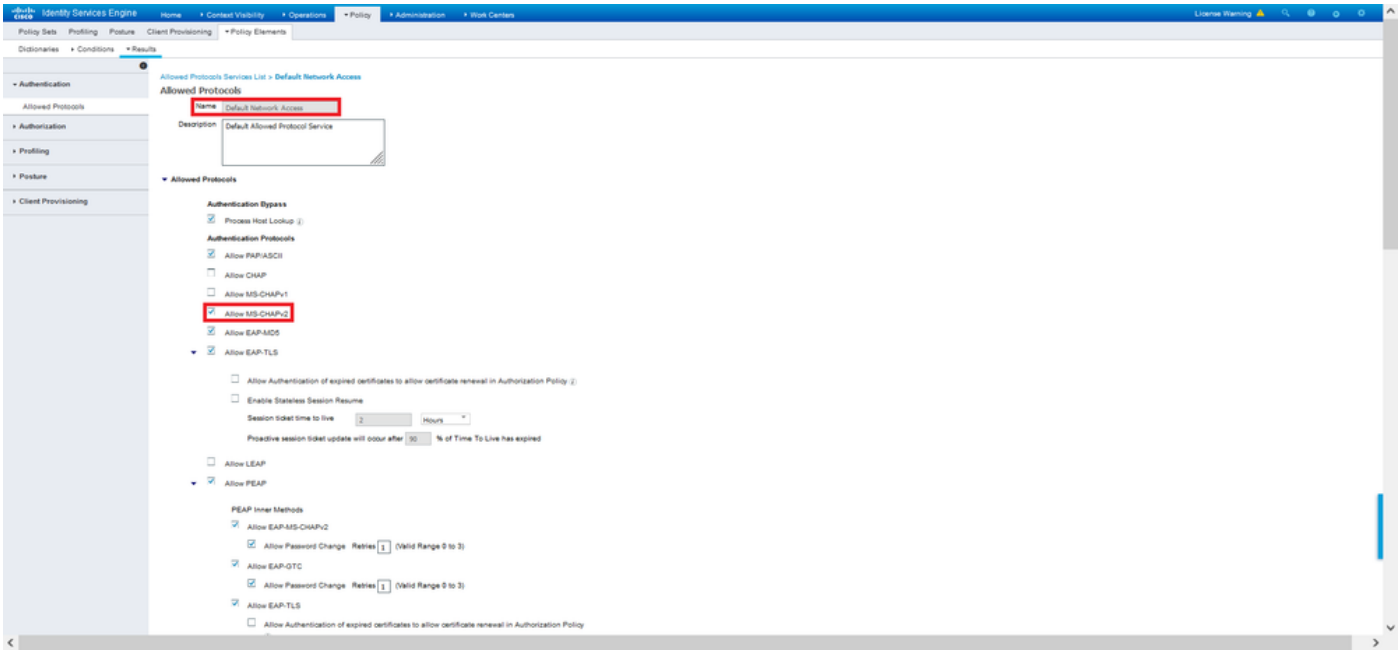


ステップ3:[Policy] > [**Policy Elements] > [Results]に移動します。**[Authentication] > [**Allowed Protocols]で、[Default Network Access]を選択して編集します。**



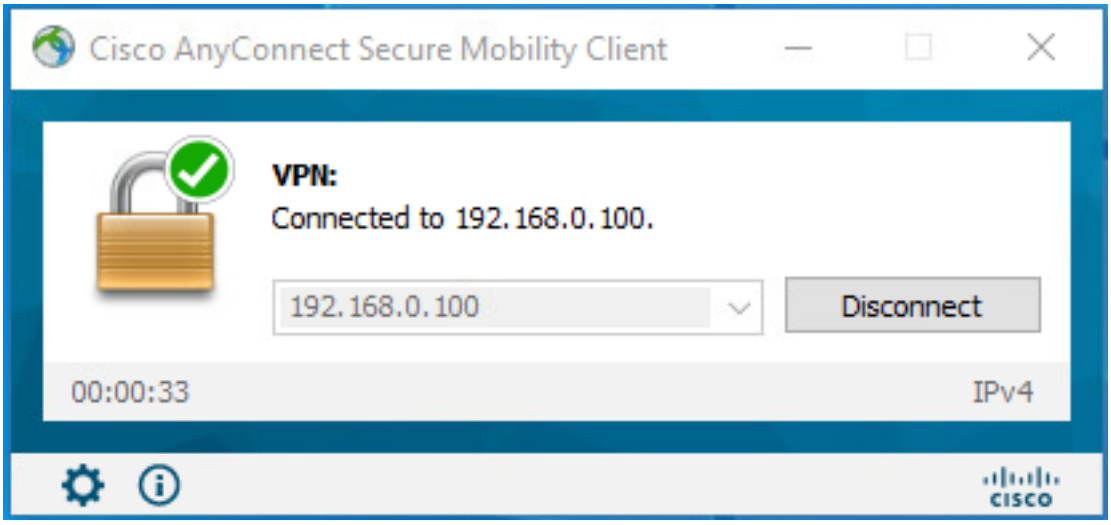


[Allow MS-CHAPv2]チェックボックスがオンになっていることを確認してください。下にスクロールして[保存]します。

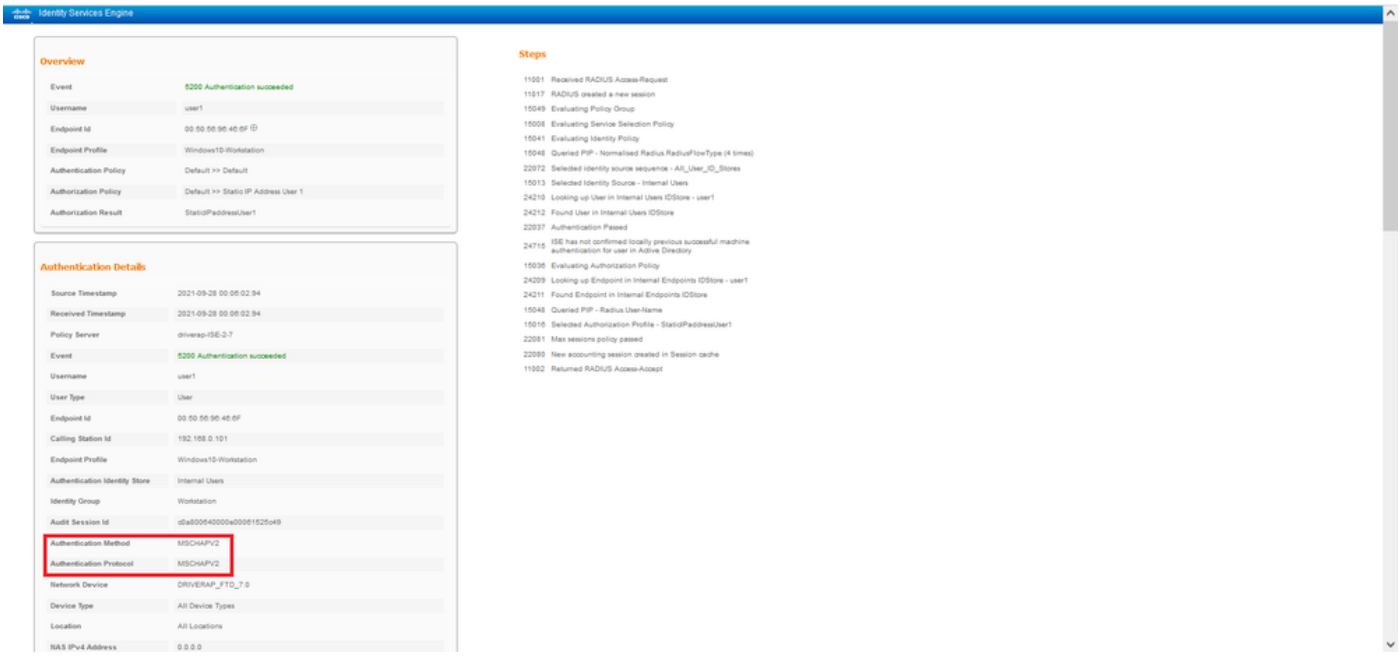


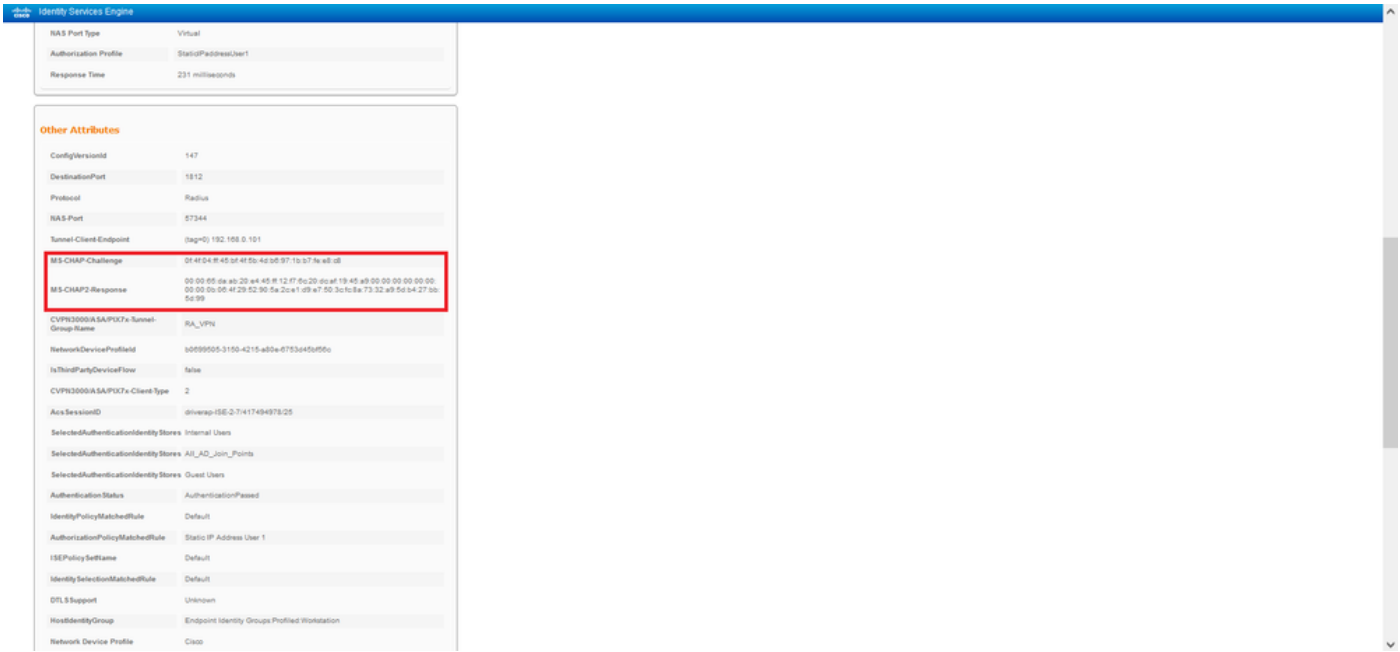
確認

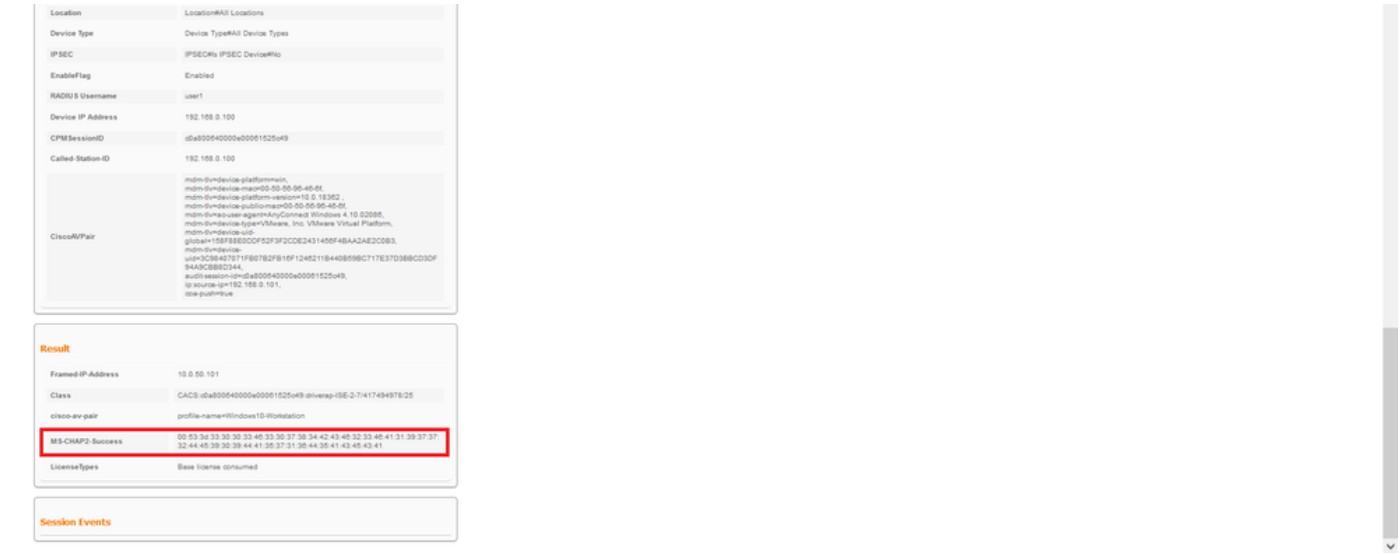
Cisco AnyConnectセキュアモビリティクライアントがインストールされているクライアントマシンに移動します。FTDヘッドエンド（この例ではWindowsマシンを使用）に接続し、ユーザクレデンシャルを入力します。



ISEのRADIUSライブログには次のように表示されます。







注:test aaa-server authenticationコマンドは、常にPAPを使用して認証要求をRADIUSサー

バに送信します。このコマンドを使用してファイアウォールにMS-CHAPv2を使用させる方法はありません。

firepower# **test aaa-server authentication ISE_Server host 172.16.0.8 username user1 password XXXXXX**
INFO:IPアドレス(172.16.0.8)への認証テストを試みています(タイムアウト：12 秒)
INFO:Authentication Successful

注：Flex-configを使用して**tunnel-group ppp-attributesを変更しないでください。これは、AnyConnect VPN（SSLおよびIPSec）接続のRADIUSでネゴシエートされた認証プロトコルには影響を与えません。**

tunnel-group RA_VPN ppp-attributes
 no authentication pap
 認証CHAP
 authentication ms-chap-v1
 no authentication ms-chap-v2
 no authentication eap-proxy

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

FTD:

- **debug radius all**

ISE:

- RADIUS ライブ ログ