

# عم FTD Remote Access VPN نيوكت مع RADIUS ربع MSCHAPv2

## تايوت حمل

[عم دق مل](#)

[عم ساس ال اابل ط مل](#)

[اابل ط مل](#)

[عم دخت س مل اانوك مل](#)

[عم ساس ااامل عم](#)

[نيوك مل](#)

[كك بش ل ل طي ط خ مل مسر](#)

[FMC ربع AAA/RADIUS عم داصم مادخت س ااب VPN RA عم كك بش نيوكت](#)

[عم داصم لوكوت وربك MS-CHAPv2 مع دل ISE نيوكت](#)

[عم حص ل ا نم قق ح مل](#)

[اه االص او اطا خ ال ا فاش ك س ا](#)

## عم دق مل

ي دحت ل ا عم يق ب ل ا ص ت ال ا دي ك ا ت ل عم داصم ل لوكوت ورب ني ك م ت عم في ك دن ت س مل ا اذ ه ح ض و ي FirePOWER (FMC) عم ر ا د ا ز ك رم ربع عم داصم عم ق ي ر ط ك (MS-CHAPv2) 2 ر ا د ص ل ا Microsoft ل مدخت س مل ل ا ص ت ا ب ل ط عم د خ عم داصم مادخت س ا ب د ع ب ن ع ل و ص و ل ل VPN عم كك بش ا ل م ع ل (RADIUS) دي ع ب ل ا .

## عم ساس ال اابل ط مل

### اابل ط مل

عم ل ا ت ل ا ع ي ض ا و م ل ا ب عم فر عم ك ي د ل نو ك ت ن ا ب Cisco ي ص و ت :

- Firepower Threat Defense (FTD)
- Firepower (FMC) عم ر ا د ا ز ك رم
- (ISE) عم ي و ه ل ا ت ا م د خ ك ح م
- Cisco AnyConnect Secure Mobility Client
- RADIUS لوكوت ورب

### عم دخت س مل اانوك مل

عم ل ا ت ل ا ح م ا ر ب ل ا ت ا ر ا د ص ا ل ا دن ت س مل ا اذ ه في عم ر ا و ل ا ت ا م و ل عم ل ا دن ت س ت :

- FMCv - 7.0.0 (عم ي ن ب 94)
- FTDv - 7.0.0 (عم ي ن ب ل ا 94)
- ISE - 2.7.0.356

- AnyConnect - 4.10.02086
- Windows 10 Pro لښغلش تال ماظن

ةصاخ ةي لم عم ةئي ب ي ف ةدوچوم ل ةزهجال نم دنن تسم ل اذه ي ف ةدراول تاملول عم ل ءاشن ا م ت تن ا ك اذ ا . (يضا رت ف ا) حوس م م ن ي و ك ت ب دنن تسم ل اذه ي ف ةمدختسم ل ةزهجال ا عي م ج ت ا د ب ر م ا ي ا ل م ت ح م ل ر ي ث ا ت ل ل ك م ه ف ن م د ك ا ت ف ، ل ي غ ش ت ل د ي ق ك ت ك ب ش

## ةي س ا س ا تاملول عم

م داو خ عم ةقداصم ةقيرطك (PAP) رورم ل ةم ل ك ةقداصم لوكوتورب FTD م دختسي ، ايضا رت ف ا RADIUS تالاصتال AnyConnect VPN.

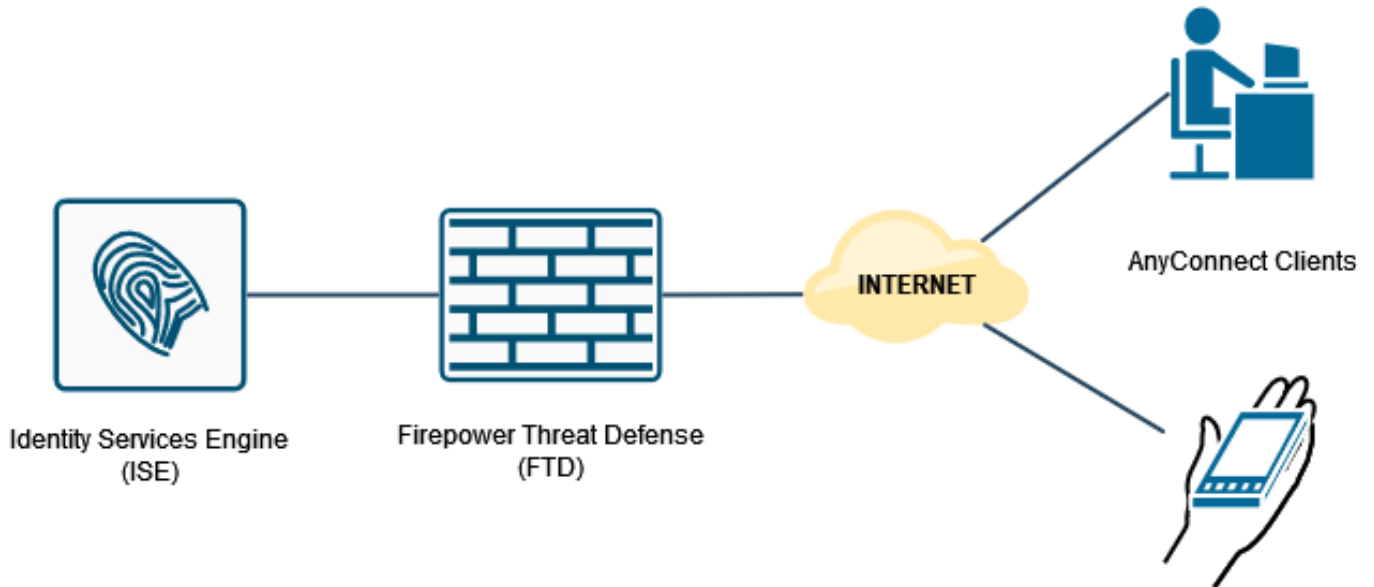
ةي ئانث ةحفاصم لال خ نم مه تي وه ت ا ب ث ا ل ن ي م دختسم ل ل ةطي س ب ةقيرط PAP رفوت ا روط ل ل ق ا ل ا ةقداصم ل لوكوتورب ي ه و ك رت شم رس ب PAP رورم ةم ل ك ر ي ف ش ت م ت ي . ه ا ج ت ا ل ا ط خ ل ا و ة ب ر ج ت ل ا ت ا م ج ه ن م ة ل ي ل ق ة ي ا م ح رفوت ا ه ا ن ا ل ة ي و ق ة ق د ا ص م ة ق ي ر ط ت س ي ل P A P . ة ر ر ك ت م ل ا

رورم ل ةم ل ك ر ي غ ت ة ز ي م و ن ا ر ق ا ل ا ن ي ب ة ل د ا ب ت م ة ق د ا ص م MS-CHAPv2 ة ق د ا ص م رفوت

ب ج ي ، VPN ل ا ص ت ا ل RADIUS م داخ و ASA ن ي ب م دختسم ل لوكوتورب ك MS-CHAPv2 ن ي ك م ت ل ي ل رورم ل ةم ل ك ة ر ا د ا ن ي ك م ت ي د و ي . ل ا ص ت ا ل ا ف ي ر ع ت ف ل م ي ف رورم ل ةم ل ك ة ر ا د ا ن ي ك م ت RADIUS م داخ ي ل FTD ن م MS-CHAPv2 ة ق د ا ص م ب ل ط ء ا ش ن ا

## ن ي و ك ت ل ا

### ة ك ب ش ل ل ي ط ي ط خ ت ل ا م س ر ل ا

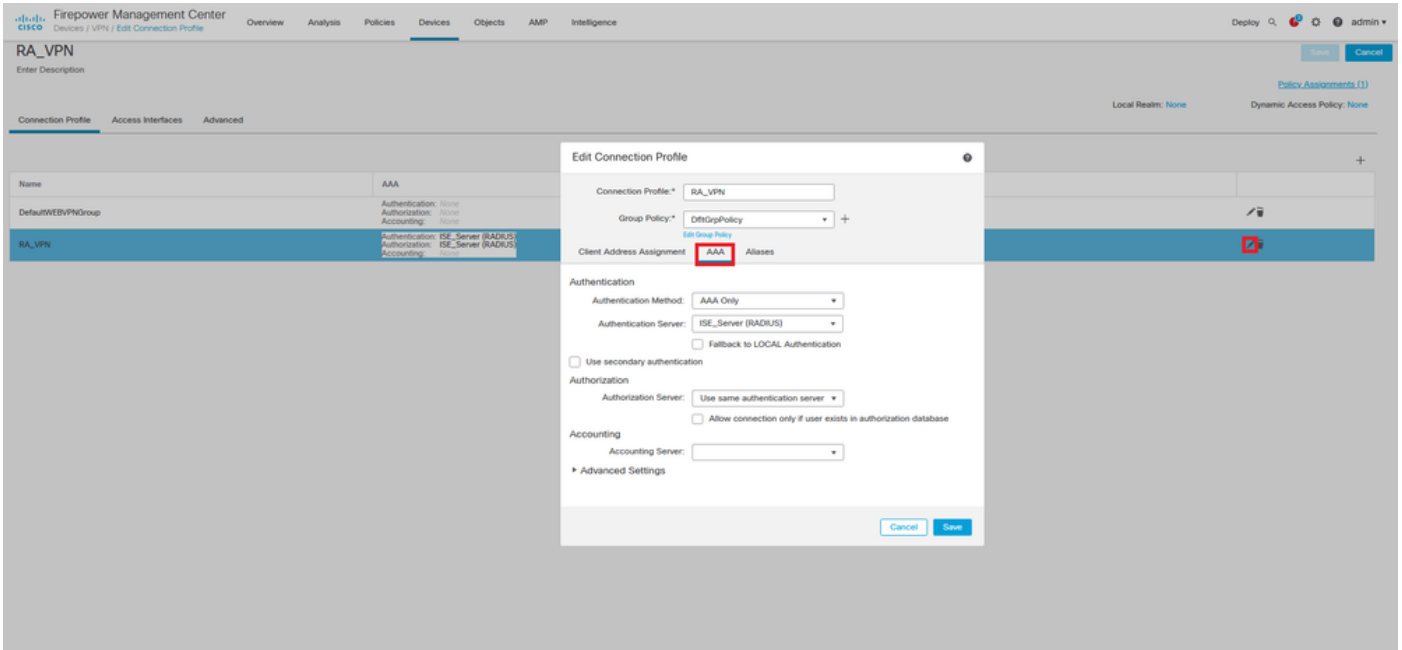


### FMC رب ع AAA/RADIUS ة ق د ا ص م م ا د خ ت س ا ب VPN RA ة ك ب ش ن ي و ك ت

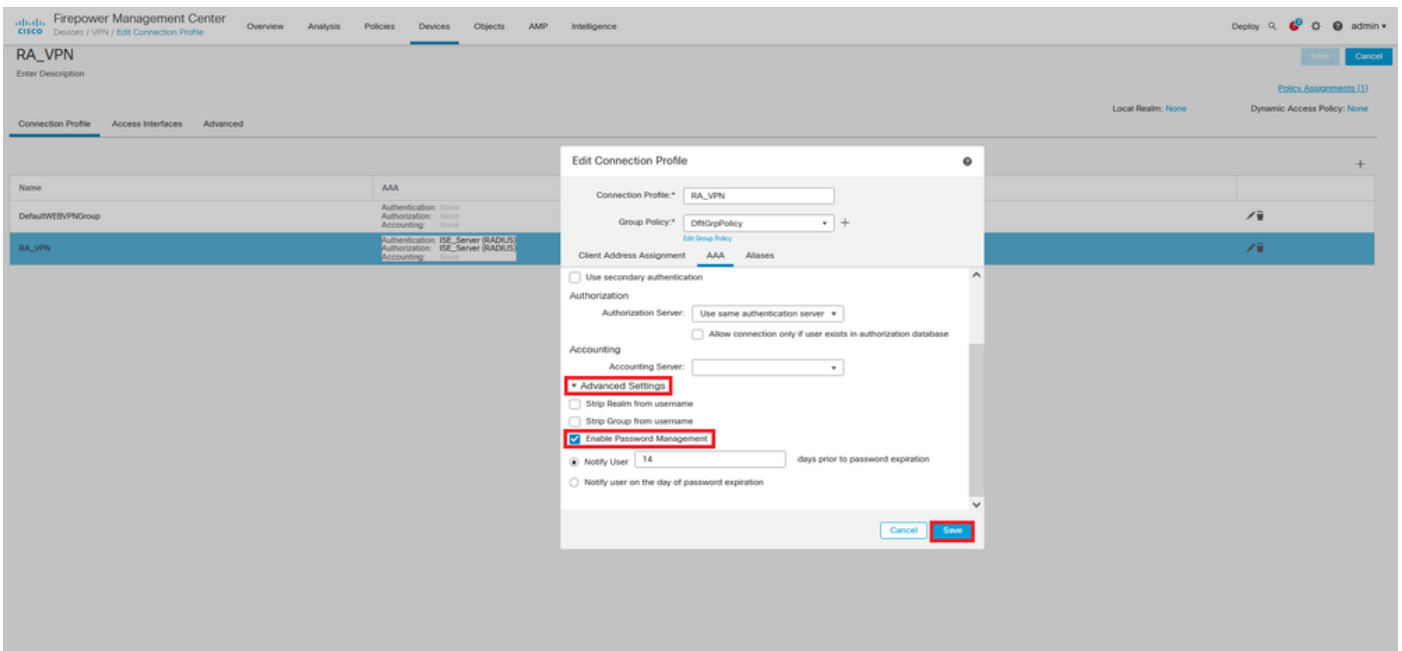
و ي د ي ف ا ل ا ذ ه و د ن ن ت س م ل ا ا ذ ه ي ل ا ع ج ر ا ، ة و ط خ ب ة و ط خ ل ص ف م ء ا ر ج ا ي ل ع ل و ص ح ل ل

- [FTD ي ل ع AnyConnect Remote Access VPN ن ي و ك ت](#)
- [FMC ة ط س ا و ب ر ا د م ل ا FTD ل ي ل و ا ل ا AnyConnect ن ي و ك ت](#)

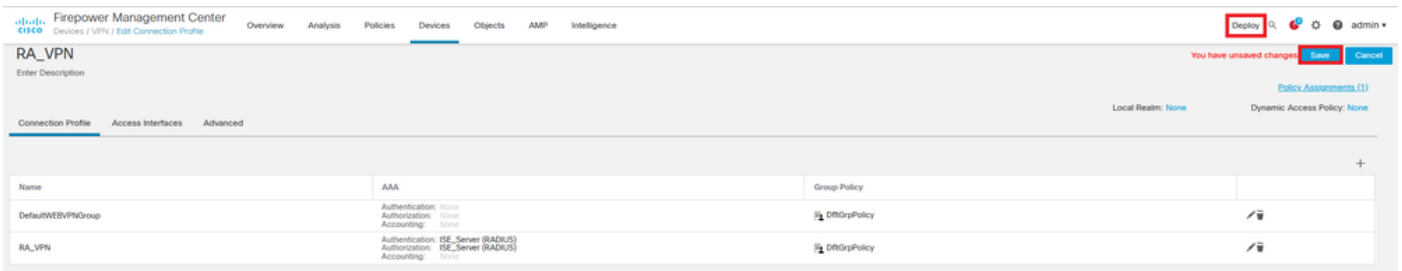
دع ب نع لوصولا > زهجالا لى لقتنا ،دع ب نع لوصولل VPN ةكبش نيوكت درجم ب 1. ةوطخل  
 AAA بيوبتل ةمالع لى لقتنا م ،اثيرح هؤاشنإ مت يذلا لاصتالا فيرعت فلم ررحو



ظفح ةقطق .قودنص قيقت ةرادا ةملك enable ل قطقطو مسق ةمدقتملا تاداعلال تادم



رشنو ظفح



FTD CLI لى دع ب نع لوصولل VPN نيوكت:

```
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

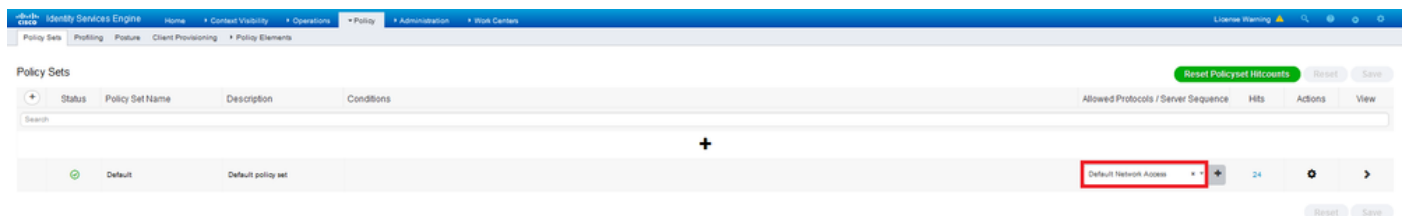
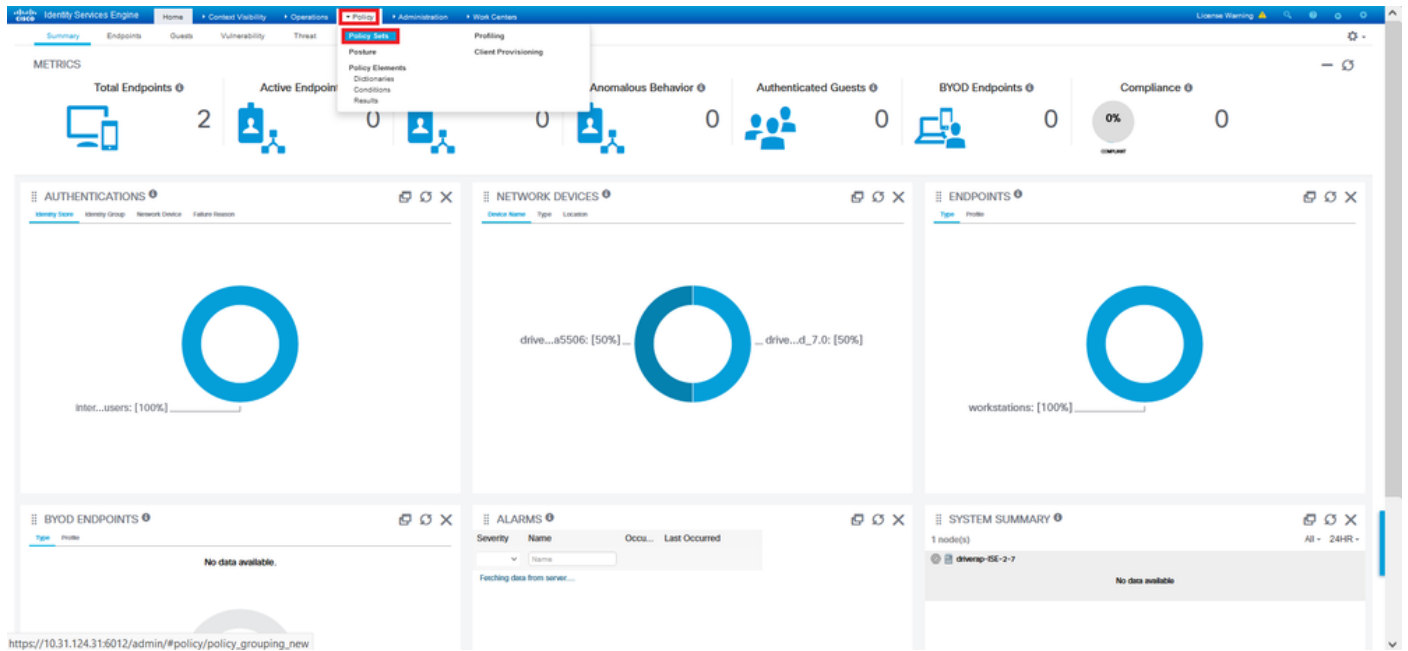
tunnel-group RA_VPN type remote-access
tunnel-group RA_VPN general-attributes
address-pool AC_Pool
authentication-server-group ISE_Server
password-management
tunnel-group RA_VPN webvpn-attributes
group-alias RA_VPN enable
```

# ةقداصم لوكوتوربك MS-CHAPv2 معدل ISE نيوكت

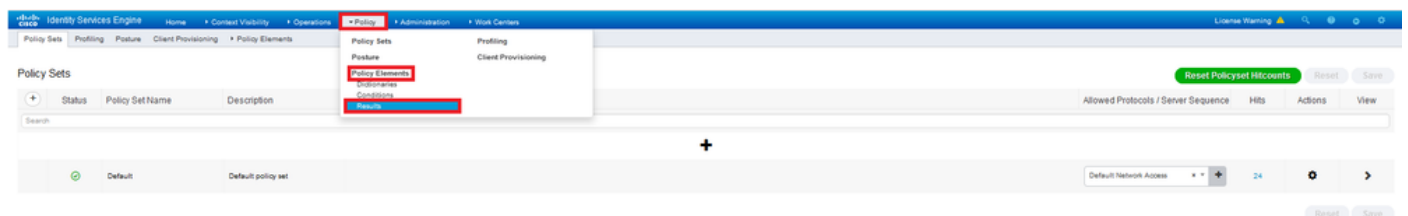
يلې ام ضررتفي:

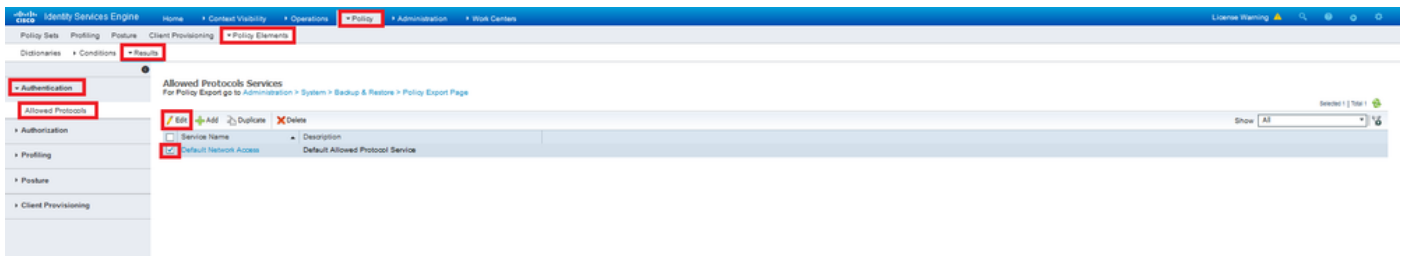
1. لوصولا تابلط ةجلاعم هنكمي ىتح ISE لىل ةكبش زاهجك لىل فلاب FTD ةفاضل تامت .
2. AnyConnect لىل ةقداصم ل ISE لىل رفوتم دحاو مدختسم لىل ةقلا لىل ةكانه .

اهب حومسمل تالوكوتوربلا جهن نع شحباو جهنلا تاعومجم > جهنلا لىل لقتنا . 2. ةوطخلا دجوت ،لاثلما اذه يف .كېدل AnyConnect يمدختسم ةقداصم متهې شېح جهنلا ةعومجم قفرملا Default Network Access وه شحبالا ديق جهنلا نوكي كلذل طقف ةدحاو جهن ةعومجم

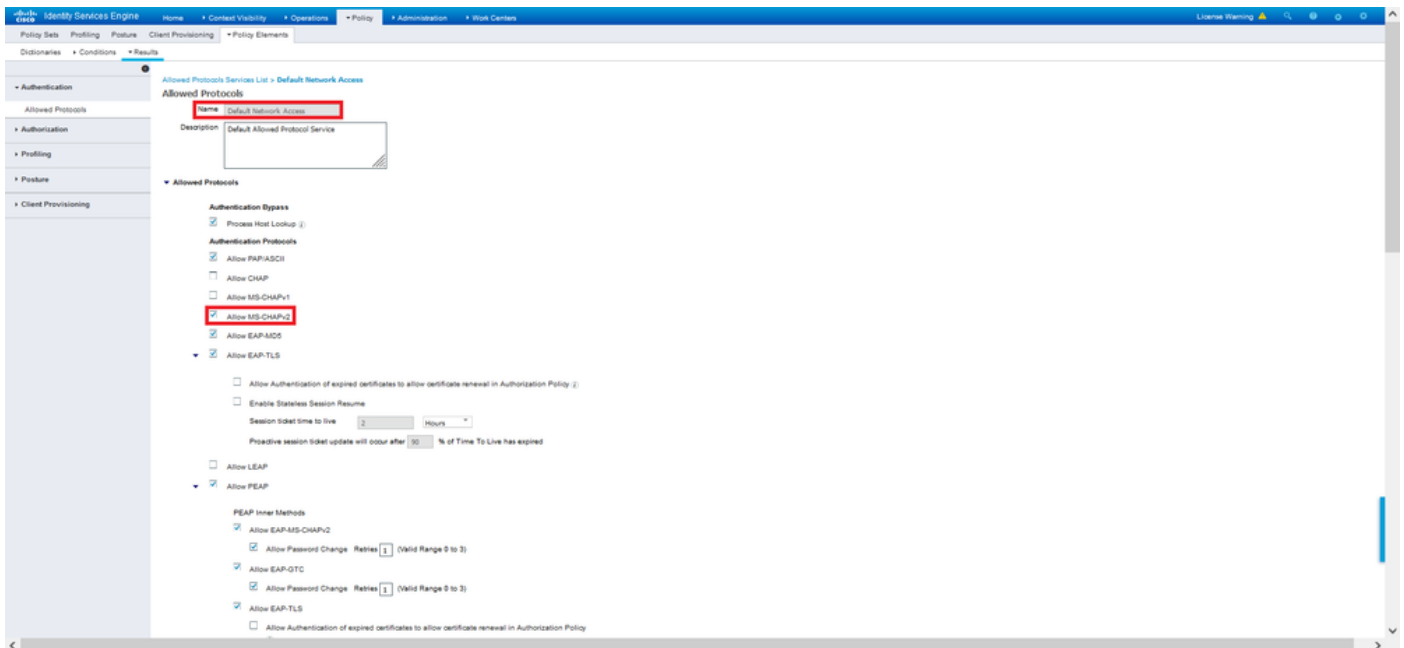


> ةقداصملا تحت .جئاتنلا > ةسايسلا رصانع > ةسايسلا لىل لقتنا . 3. ةوطخلا هريحتب مقويضارتفالا ةكبشلا لوصولا رتخأ اهب حومسمل تالوكوتوربلا



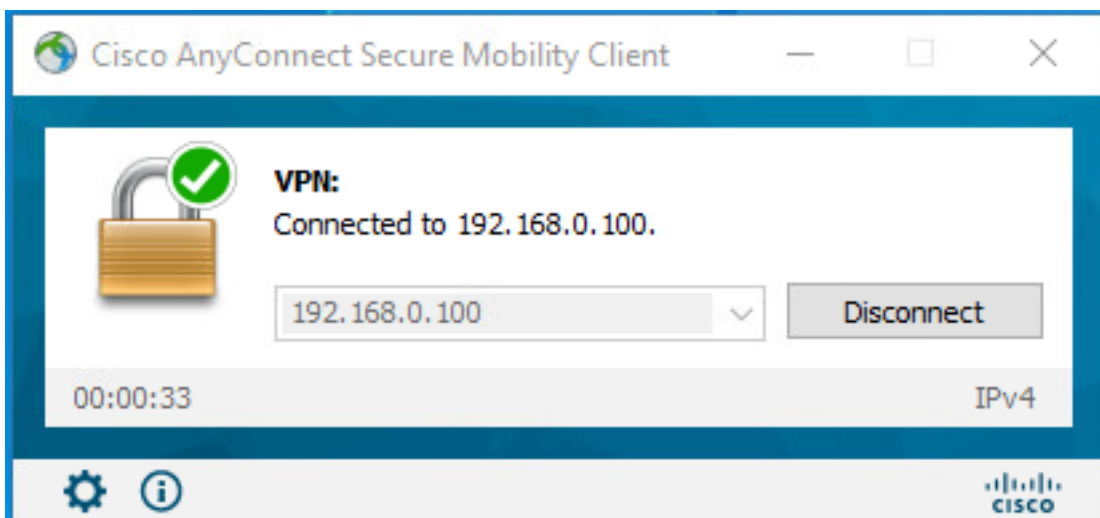


اهظ فحواو لفسألأى لى قلزنا MS-CHAPv2 ب حامسلا رايختالال ةناخ دي دجت نم دكأت



## ةحصلال نم ققحتلال

مق Cisco AnyConnect Secure Mobility Client تي بثت مت شيح ليمعلا زاهج لى لقتنا اذه ي ف Windows زاهج مادختسإ متي) "FTD ب ةصاخلا ثبلاو لابقسالا ةدحو" ب لاصتالاب مدختسملال دامتعا تانايب بكتاو (لاثلما)



ISE: ضرع لىع RADIUS Live لىجس

Overview	
Event	5200 Authentication succeeded
Username	user1
Endpoint Id	00 50 50 90 40 6F 0
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Static IP Address User 1
Authorization Result	StaticIPAddressUser1

Authentication Details	
Source Timestamp	2021-09-28 00:06:02.94
Received Timestamp	2021-09-28 00:06:02.94
Policy Server	drvrp-ISE-2-7
Event	5200 Authentication succeeded
Username	user1
User Type	User
Endpoint Id	00 50 50 90 40 6F 0
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	d8a30054000a000e1225a49
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

- 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 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
  - 24719 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

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 44 50 97 19 57 8e a8 08
MS-CHAP2-Response	00 00 00 00 40 20 44 45 8 12 0F 8a 20 0c a1 19 45 a0 00 00 00 00 00 00 00 00 00 00 4F 29 52 90 5a 2ca1 d9 a7 50 3c f0 8a 73 32 a9 50 54 27 00 5a 99
CVPR3000ASAPROTA Tunnel-Group-Name	RA_VPN
NetworkDeviceProfileId	b0099005-3150-4215-a80a-d753a45b850a
IsThirdPartyDeviceFlow	false
CVPR3000ASAPROTA Client-Type	2
AcxSessionId	drvrp-ISE-2-7-1417494978-25
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	All_AD_Icon_Points
SelectedAuthenticationIdentityStores	Guest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Static IP Address User 1
ISE Policy Set Name	Default
Identity Selection Matched Rule	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 DeviceNo
EnableFlag	Enabled
RADIUS Username	user1
Device IP Address	192.168.0.100
CPM Session ID	d8a30054000a000e1225a49
Called-Station-ID	192.168.0.100
CiscoAPPar	<pre> mgn-du-device-platform=main mgn-du-device-manage=00 50 50 90 40 6F 0 mgn-du-device-platform-version=10.0.18.352 mgn-du-device-public-manage=00 50 50 90 40 6F 0 mgn-du-manage-agent=AnyConnect_Windows 4.10.02080 mgn-du-device-type=VMware, Inc. VMware Virtual Platform, mgn-du-device-uid= globa=158788020F52F32C0E243405F4BA2AE2C0B3 mgn-du-device- user=3C3842717F80782F816F124621184408698C71E37D388C030F 944C8880344 audit-session-id=d8a30054000a000e1225a49 @source-ip=192.168.0.101, 00a-push@vive                     </pre>

Result	
Framed IP Address	10.0.50.101
Class	CACS-d8a30054000a000e1225a49 drvrp-ISE-2-7-1417494978-25
ctloc-av-gate	profile-name=Windows10-Workstation
MS-CHAP2-Success	00 53 3a 33 30 33 40 33 30 37 38 34 42 43 45 32 33 45 41 31 39 37 37 32 44 48 30 39 44 41 39 37 31 39 44 38 41 43 48 43 41
License Types	Base license consumed

Session Events	
----------------	--

مدخا لى ةقداصم لى ابل ط لاس رال PAP امئاد AAA-Server ةقداصم رم ا مدخت سي :ةظحال م

اذه مادختساب MS-CHAPv2 مادختسا لىل ع قىامحل راج راجل ع قىرط دجوت الو ، RADIUS رمل.

مكك Firepower# راب تخ | AAA-Server ISE\_Server Host 172.16.0.8 username user1 رورم XXXXXX  
ةل وناث 12 :ةلمل) IP (172.16.0.8) ناونع لىل ع قىاصم راب تخ | ةل وناث : تامول عم لىل  
ةحجان ةقداصم لىل : تامول عم لىل

ال ك لذ نأ ثىح Flex-config ربع ق فنل ة عومجمل PPP تامس لىل دع تب مق ت ال : ةظالم  
تالاصتال RADIUS ربع اه لىل ع صوافتل م تى لىل ةقداصم لىل تالوكوتورب لىل ع رثؤى  
AnyConnect VPN (SSL و IPsec).

تامس PPP Tunnel-group RA\_VPN  
ةقداصم ةمزح دجوت ال  
ةقداصم لىل CHAP لوكوتورب  
ةقداصم لىل ms-chap-v1  
ةقداصم دجوت ال ms-chap-v2  
ةقداصم لىل و دجوى ال

## اهال صا و اطاخ ال فاشكتسا

اهال صا و نىوكتل اطاخ فاشكتسا ال اهمادختسا لىل كنكم لىل تامول عم لىل مس ق ل اذو رفوى

ىل ع ف تى :

- debug radius all

ىل ع ISE:

- ةرشابم لىل RADIUS تال جس



ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن ت س م ل ا اذ ه Cisco ت مچرت  
م ل ا ل ا اء ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و  
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems ( ر ف و ت م ط ب ا ر ل ا ) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا