

FTD ىلج RAPN ل LDAP ةمس ةطيرخ نيوكت FDM ةطساوب ةرادملا

تايوتحمل

[ةمدقملا](#)

[ةيساسال تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةقداصملا قفدت](#)

[LDAP ةمس طاطخم قفدت حرش](#)

[نيوكتلا](#)

[FDM ىلج نيوكتلا تاوطخ](#)

[LDAP ةمس نييعةتل نيوكتلا تاوطخ](#)

[ةحصلا نم ققحتلا](#)

[اهجالص او عاخذال فاشكتسا](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

(LDAP) نزولا في فخ لي لدا لى ل لوصولا لوكوتورب م داخ مادختسا اراج دن تسملا اذه فصى مهليوختو (RA VPN) دع ب نع لوصول (RA VPN) ةكبش يمدختسم لىل ةقداصم ل ل LDAP م داخ لىل مةتعموم ةيوضع لىل اذانتسا فل تخم ةكبش لوصول.

ةيساسال تابلطتملا

تابلطتملا

- (FDM) ةياملال رادج ةزهجأ ري دم لىل RA VPN نيوكتب ةيساسال ةفرعم
- FDM لىل LDAP م داخ نيوكتب ةيساسال ةفرعم
- (API) (REST) ةيضا رتفالال ل ل ل ل قن قيبطت جم انرب ةهجاوب ةيساسال ةفرعم
FDM REST API فشكتسمو
- FDM ةطساوب ةرادملا ثدحال او Cisco FTD نم 6.5.0 رادصال

ةمدختسملا تانوكملا

ةزهجال/قيبطتلل ةيلا ل ل ل جم اربل او ةزهجال تارادصال مادختسا مت

- Cisco FTD، رادصال 6.5.0، build 115
- Cisco AnyConnect، رادصال 4.10
- Microsoft Active Directory (AD) م داخ
- API ريوطتل ىرخأ ةادأ ي او Postman

ديرب ال ةادأ Microsoft AD Server ل نيوكتل معد Cisco رفوت ال :ةظالم

ةصاخ ةي لمعم ةئي ي ف ةدوجومل ةزهأل نم دنن سمل اذه ي ف ةدراول تامولعمل عاشنإ مت تناك اذا .(يضا رتفا) حوسمم نيوكتب دنن سمل اذه ي ف ةمدختسمل ةزهأل عي مج تآدب رمأ يال لمحتحمل ريثأت لل كمهف نم دكأتف ،ليغشتل دي قكتك بيش

ةقداصملا قفدت



LDAP ةمس ططخم قفدت حرش

1. مدختسم مسا رفويو FTD ل دع ب نع لوصول VPN لاصتا ةئيه تب مدختسمل موق ي .
2. مدختسم مسا رفويو FTD ل سري (LDAP ربع SSL) 636 وأ 389 ذفنم ل ربع AD مداخ ل LDAP بلط FTD ل سري .
3. مدختسمل اب ةطبترملا تامسلا ل ك عم FTD ل AD بي جتسي .
4. FTD ل ع هؤاشنإ مت يذال LDAP ةمس نييعت عم ةملمتسمل ةمسلا مي ق FTD قباطي . لي وختلا ةي لمع يه هذه
5. قباطت يتل Group-Policy نم اهثرتو تاداعل اب لاصتال اب مدختسمل موق ي كلذ دع ب LDAP ةمس نييعت ي ف memberOf ةمسلا عم

LDAP وضع ةمس مادختساب AnyConnect ي مدختسم ضيوفت عارجإ متي ،دنن سمل اذه ضارغل

- FTD ل ع ldapValue نا ي ك ل مدختسم ل ك ل LDAP مداخ نم memberOf ةمسلا نييعت مت ب نرتقملا ةعومجمل جهن نإف ،ةقباطملا AD ةعومجمل ل يمتني مدختسمل نا ك اذا مدختسمل ل بق نم ثوروم اذه ldapValue
- ي ف ldapValue نا ي ك نم ي أ عم مدختسمل ل memberOf ةمس ةمي ق قباطت مدع ةلاح ي ف اذه ي ف . ددحمل لاصتال في رعت فلمل يضا رتفال ةعومجمل جهن ثيروت متي ، FTD ل ع ل NOACCESS Group-Policy ثيروت متي ، لاثملا

نيوكتل

ةجمرب ةهجاو مادختساب FDM ةسطاوب هترادا مت يذال FTD ل LDAP ةمس ططخم نيوكت مت REST تاق يبطت

FDM ل ع نيوكتل تاوطخ

ي كذل صيخرتل ي ف زاehl ليجست نم ققحت 1. ةوطخل



Interfaces Connected Enabled 3 of 9 View All Interfaces	Routing 2 routes View Configuration	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Server DNS Server Management Interface Hostname NTP Cloud Services Reboot/Shutdown Traffic Settings URL Filtering Preferences
Smart License Registered View Configuration	Backup and Restore View Configuration	Troubleshoot No files created yet REQUEST FILE TO BE CREATED	
Site-to-Site VPN 1 connection View Configuration	Remote Access VPN Configured 2 connections 5 Group Policies View Configuration	Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration	Device Administration Audit Events, Deployment History, Download Configuration View Configuration

FDM. AnyConnect صيخارت نيكمت نم ققحت 2. ةوطخلا

Smart License

CONNECTED SUFFICIENT LICENSE
 Last sync: 11 Oct 2019 09:33 AM
 Next sync: 11 Oct 2019 09:43 AM
[Go to Cloud Services](#)

SUBSCRIPTION LICENSES INCLUDED

- Threat** (Enabled) - Includes: Intrusion Policy
- Malware** (Disabled by user) - Includes: File Policy
- URL License** (Enabled) - Includes: URL Reputation
- RA VPN License** (Enabled) - Type: PLUS - Includes: RA-VPN

PERPETUAL LICENSES INCLUDED

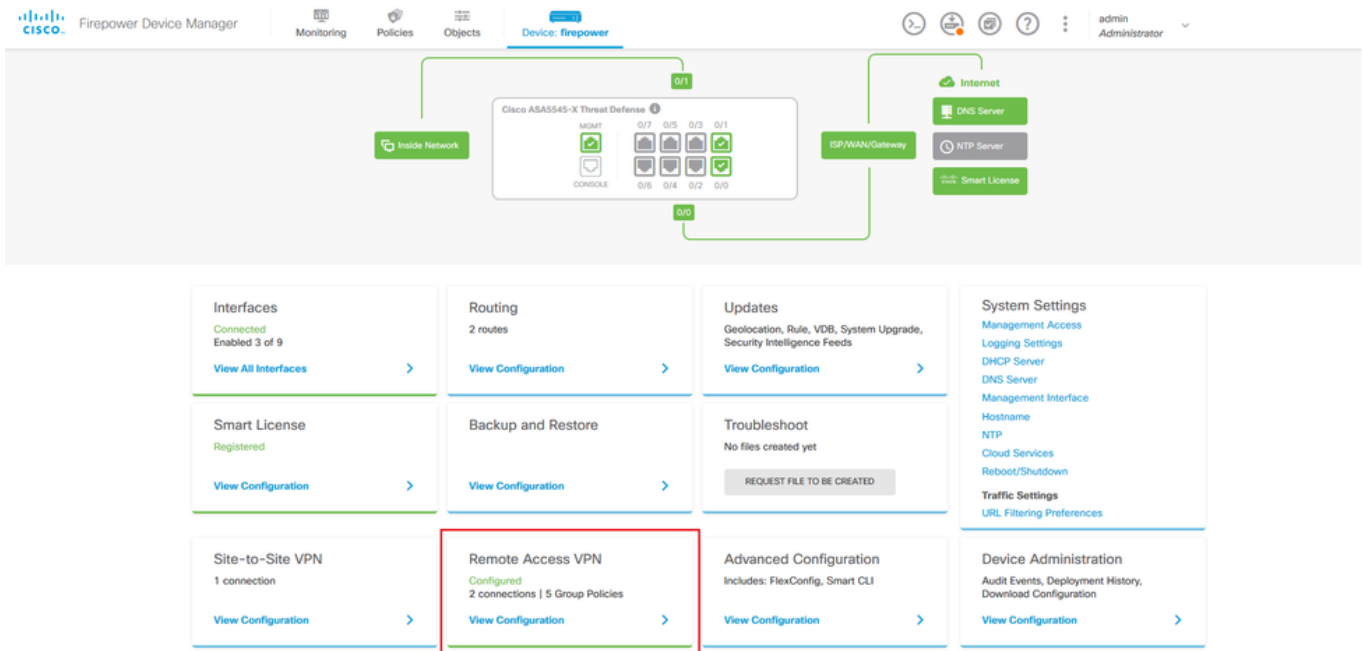
- Base License** (Enabled) - Includes: Base Firewall Capabilities, Application Visibility and Control

زمرلای ف ری دصت لای قی رط ن ع اهی ف مکحت لای م تی ی ت لای تازی م لای نی ک م ت ن م ق قحت 3. ة و ط خ لای ز ی م لای

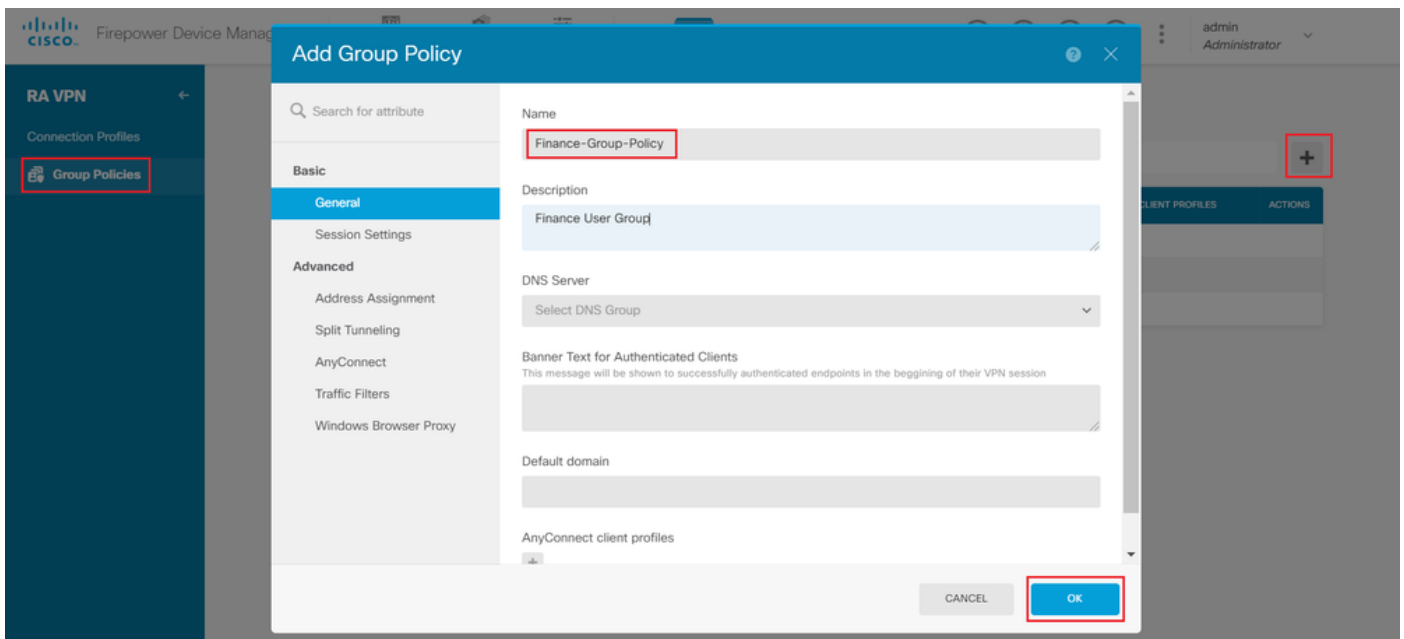
The screenshot displays the Cisco Firepower Device Manager interface for a device named 'firepower'. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: firepower'. The main content area is titled 'Device Summary Smart License'. A green checkmark indicates the device is 'CONNECTED SUFFICIENT LICENSE'. A tooltip shows 'Assigned Virtual Account: [redacted]', 'Export-controlled features: Enabled', and 'Go to Cisco Smart Software Manager.' Below this, sync times are listed: 'Last sync: 11 Oct 2019 09:33 AM' and 'Next sync: 11 Oct 2019 09:43 AM'. The 'SUBSCRIPTION LICENSES INCLUDED' section shows 'Threat' is 'Enabled' with a 'DISABLE' button. A description states: 'This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.' It includes 'Intrusion Policy'.

✎ لای ع و ج ر لای ی ج ر ی . ل ع ف ل ا ب ه ن ی و ک ت م ت RA VPN ن ا د ن ت س م لای ا ذ ه ض ر ت ف ی : ة ط خ لای م لای ع WAPN ن ی و ک ت ة ی ف ی ک ل و ح ت ا م و ل ع م لای ن م د ی ز م ی ل ع ل و ص ح ل ل ی ل ا ت لای د ن ت س م لای FDM. ة ط س ا و ب ه ت ر ا د ا م ت ت ی ذ لای FTD.

> Remote Access VPN ة و م ج م ج ه ن ی لای ل ق ت ن ا 4. ة و ط خ لای



لكل فئة لخدمات عمومية جهن نيوكتل '+' قوف رقنا .ةومجم ل جهن لى لقتنا 5 ةوطخل
 Finance-group-policy و HR-Group-Policy ةومجم ل تاسايس نيوكتل مت ، ل اثلما اذه يف ةومجم
 ةة ل تخم ةي عرف تاكبش لى لوصول ل IT-Group-Policy او



ةي ل ل اتاداع ل Finance-Group-Policy نمضتت

```
<#root>
```

```
firepower#
```

```
show run group-policy Finance-Group-Policy
```

```
group-policy Finance-Group-Policy internal
group-policy Finance-Group-Policy attributes
  banner value You can access Finance resource
  dhcp-network-scope none
  vpn-simultaneous-logins 3
  vpn-idle-timeout 30
  vpn-idle-timeout alert-interval 1
  vpn-session-timeout none
  vpn-session-timeout alert-interval 1
  vpn-filter none
  vpn-tunnel-protocol ssl-client
  split-tunnel-policy tunnelspecified
  ipv6-split-tunnel-policy tunnelall

split-tunnel-network-list value Finance-Group-Policy|splitAcl

split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
msie-proxy method no-modify
vlan none
address-pools none
ipv6-address-pools none
webvpn
<output omitted>
```

ةيلا لادادعإلا لىل عةيرشبلل دراوملل ةومجم جهن لم تشي، لثامم وحن لىل وعو:

<#root>

firepower#

```
show run group-policy HR-Group-Policy

group-policy HR-Group-Policy internal
group-policy HR-Group-Policy attributes
  banner value You can access Finance resource
  dhcp-network-scope none
  vpn-simultaneous-logins 3
  vpn-idle-timeout 30
  vpn-idle-timeout alert-interval 1
  vpn-session-timeout none
  vpn-session-timeout alert-interval 1
  vpn-filter none
  vpn-tunnel-protocol ssl-client
  split-tunnel-policy tunnelspecified
  ipv6-split-tunnel-policy tunnelall

split-tunnel-network-list value HR-Group-Policy|splitAcl

split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
msie-proxy method no-modify
vlan none
address-pools none
ipv6-address-pools none
```

```
webvpn
<output omitted>
```

ة:لالتا تاداعإلإىل ع تامولعملال ةنقت ةومجمهن يوتحي،اريخأو

```
<#root>
```

```
firepower#
```

```
show run group-policy IT-Group-Policy
```

```
group-policy IT-Group-Policy internal
group-policy IT-Group-Policy attributes
  banner value You can access Finance resource
  dhcp-network-scope none
  vpn-simultaneous-logins 3
  vpn-idle-timeout 30
  vpn-idle-timeout alert-interval 1
  vpn-session-timeout none
  vpn-session-timeout alert-interval 1
  vpn-filter none
  vpn-tunnel-protocol ssl-client
  split-tunnel-policy tunnelspecified
  ipv6-split-tunnel-policy tunnelall
```

```
split-tunnel-network-list value IT-Group-Policy|splitAcl
```

```
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
msie-proxy method no-modify
vlan none
address-pools none
ipv6-address-pools none
webvpn
<output omitted>
```

ءاغلاب مقو ةسلجل تاداعإلإىل لقتناو ةومجمهنل Noaccess ءاشنإب مق 6. ةوطخل تايلمع ةميقي نييعت لىل ع اذه لمعي .مدختسم لك نمازتمل لوخدل ليجست رايخ ديخت 0. لىل VPN ل ةنمازتمل لوخدل ليجست

(VPN) ةرهاظلا ةصاخلا ةكبشلاب ةصاخلا ةنمازتمل لوخدل ليجست تايلمع ةميقي موقت (VPN) ةرهاظلا ةصاخلا ةكبشلا لاصتا ءاهنإب 0 لىل ءهنييعت دنع "ةومجملا هن" يف أىل نومتنني نيلذلي نيمدختسملا عنمل ةيلآلا هذم ادختسإ متي .اروف مدختسملل نم (IT أو HR أو Finance لاثملا اذه يف) ةنوكملا تاعومجملا فالخ ب AD نيمدختسم ةومجم ةومجم تاباسحل طقف ةرفوتملا ةنمآلا دراوملا لىل لوصول او FTD ب ءجان تالاصتا ءاشنإ اهب حومسملا نيمدختسملا .

طبخم ةقباطم ب ةححص ال AD م دختسم تاعومجم لى ل نومتنى نى ذل نوم دختسم ل موقى ال نى ذل نوم دختسم ل شرى امنى ب ، ةنى عم ال ةومجم ل تاساى س نوثرى و FTD فى LDAP مسم فى رعت فللمل فى ضارته ال ةومجم ل جهن كل ذ دعب اهب حومسم ل تاعومجم ل نم فى لى ل نومتنى ال NOACCESS ةل ال هذه فى وه فى ذل او ، لاصل ال

Add Group Policy

Search for attribute

Basic

General

Session Settings

Advanced

Address Assignment

Split Tunneling

AnyConnect

Traffic Filters

Windows Browser Proxy

Name

NOACCESS

Description

To avoid users not belonging to correct AD group from connecting to VPN

DNS Server

Select DNS Group

Banner Text for Authenticated Clients

This message will be shown to successfully authenticated endpoints in the beginning of their VPN session

Default domain

AnyConnect client profiles

+ CANCEL OK

Edit Group Policy

Search for attribute

Basic

General

Session Settings

Advanced

Address Assignment

Split Tunneling

AnyConnect

Traffic Filters

Windows Browser Proxy

Maximum Connection Time
 minutes
 1-4473924

Idle Time
 minutes
 1-35791394; (Default: 30)

Simultaneous Login per User
 (Default: 3)

Connection Time Alert Interval
 minutes
 1-30; (Default: 1)

Idle Alert Interval
 minutes
 1-30; (Default: 1)

CANCEL OK

هذه هي الخطوات لإعداد NOACCESS على جهازك:

```
<#root>
```

```
firepower#
```

```
show run group-policy NOACCESS
```

```
group-policy NOACCESS internal
group-policy NOACCESS attributes
  dhcp-network-scope none
```

```
vpn-simultaneous-logins 0
```

```
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
msie-proxy method no-modify
vlan none
address-pools none
ipv6-address-pools none
webvpn
  anyconnect ssl dtls none
  anyconnect mtu 1406
```

```
anyconnect ssl keepalive 20
anyconnect ssl rekey time 4
anyconnect ssl rekey method new-tunnel
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect profiles none
anyconnect ssl df-bit-ignore disable
always-on-vpn profile-setting
```

مسا، لاثملا اذه في. لاصلت الل افي صوت ئشن أو لى صوت الل افي صوت إلى لقتنا. 7 ة ووطخ لا عاشن اب مقو طوق AAA يساس الة ايهو لا ردصم رتخأ. Remote-Access-LDAP وه فيرعت الل فلم AD. دي دجة قداصم مداخ عون

The screenshot shows the configuration page for a VPN connection profile in Cisco Firepower Device Manager. The profile name is 'Remote-Access-LDAP'. The authentication type is set to 'AAA Only'. The primary identity source for user authentication is 'LocalIdentitySource', and the fallback local identity source is 'Special-Identities-Realm'. The 'AD' option is selected in the 'Primary Identity Source' dropdown menu.

AD: تامولعم لخدأ

- لى لى لى مدختسم مسا
- لى لى لى رورم ةم لك
- يساس الة DN
- يساس الة AD لاجم
- IP ناو نع / فيضم لا مسا
- ذفنم لا
- رى فشنت لا عون

Add Identity Realm



! Identity Realm is used for Identity Policies and Remote Access VPN. Any changes impact all features that use this realm.

Name

LDAP-AD

Type

Active Directory (AD)

Directory Username

administrator@example.com

e.g. user@example.com

Directory Password

.....

Base DN

dc=example,dc=com

e.g. ou=user, dc=example, dc=com

AD Primary Domain

example.com

e.g. example.com

Directory Server Configuration

192.168.100.125:389

Hostname / IP Address

192.168.100.125

e.g. ad.example.com

Port

389

Interface

inside_25 (GigabitEthernet0/1)

Encryption

NONE

Trusted CA certificate

Please select a certificate

TEST

[Add another configuration](#)

CANCEL

OK

اذه لاصت الال فيرعت فللمل يضا رت فالال ة ومجم لال جهنك NOACCESS رتخاو يلات الال لى لى رونا

Firepower Device Manager

Monitoring Policies Objects Device: firepower

admin Administrator

Remote User Experience

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

View Group Policy

Filter	
Finance-Group-Policy	i
HR-Group-Policy	i
IT-Group-Policy	i
<input checked="" type="checkbox"/> NOACCESS	i
SSLVPN	i

Create new Group Policy

BACK NEXT

Maximum Connection Time / Alert Interval Unlimited / 1 Minutes

تحت ابيئرم نآل Remote-Access-LDAP لاصتال فيرعت فلم نوکي .تاريغتل ةفاک ظفح
تحت ابيئرم نآل Remote-Access-LDAP لاصتال فيرعت فلم نوکي .تاريغتل ةفاک ظفح
تحت ابيئرم نآل Remote-Access-LDAP لاصتال فيرعت فلم نوکي .تاريغتل ةفاک ظفح
تحت ابيئرم نآل Remote-Access-LDAP لاصتال فيرعت فلم نوکي .تاريغتل ةفاک ظفح
تحت ابيئرم نآل Remote-Access-LDAP لاصتال فيرعت فلم نوکي .تاريغتل ةفاک ظفح
تحت ابيئرم نآل Remote-Access-LDAP لاصتال فيرعت فلم نوکي .تاريغتل ةفاک ظفح
تحت ابيئرم نآل Remote-Access-LDAP لاصتال فيرعت فلم نوکي .تاريغتل ةفاک ظفح
تحت ابيئرم نآل Remote-Access-LDAP لاصتال فيرعت فلم نوکي .تاريغتل ةفاک ظفح
تحت ابيئرم نآل Remote-Access-LDAP لاصتال فيرعت فلم نوکي .تاريغتل ةفاک ظفح
تحت ابيئرم نآل Remote-Access-LDAP لاصتال فيرعت فلم نوکي .تاريغتل ةفاک ظفح

Firepower Device Manager

Monitoring Policies Objects Device: firepower

admin Administrator

RA VPN

Connection Profiles

Group Policies

Device Summary

Remote Access VPN Connection Profiles

1 object

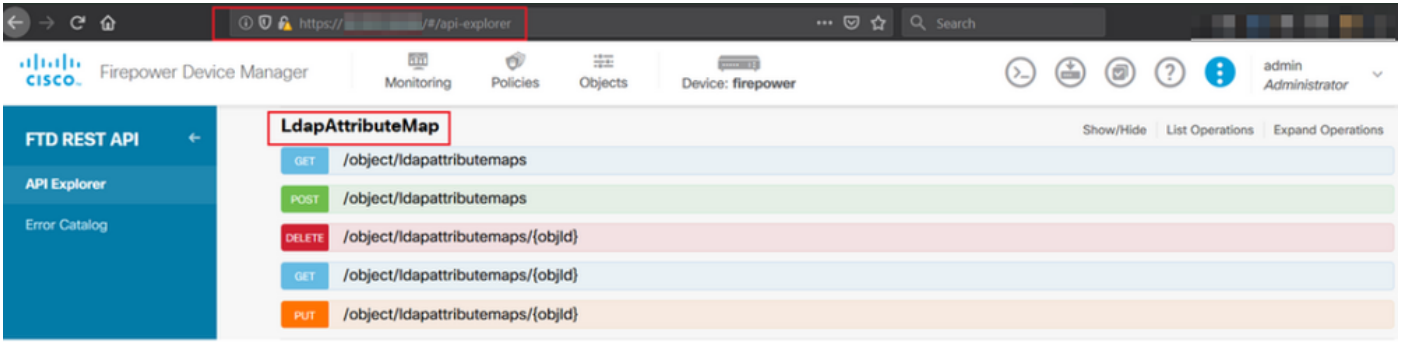
#	NAME	AAA	GROUP POLICY	ACTIONS
1	Remote-Access-LDAP	Authentication: AAA Only Authorization: None Accounting: None	NOACCESS	

LDAP ةمس نييغت ل نيوكتل تاوطخ

FTD ب صاخلا (API) تاقيبطتل ةجمرب ةهجاو فشكتسم ليغشت ادب 1 ةوطخلا

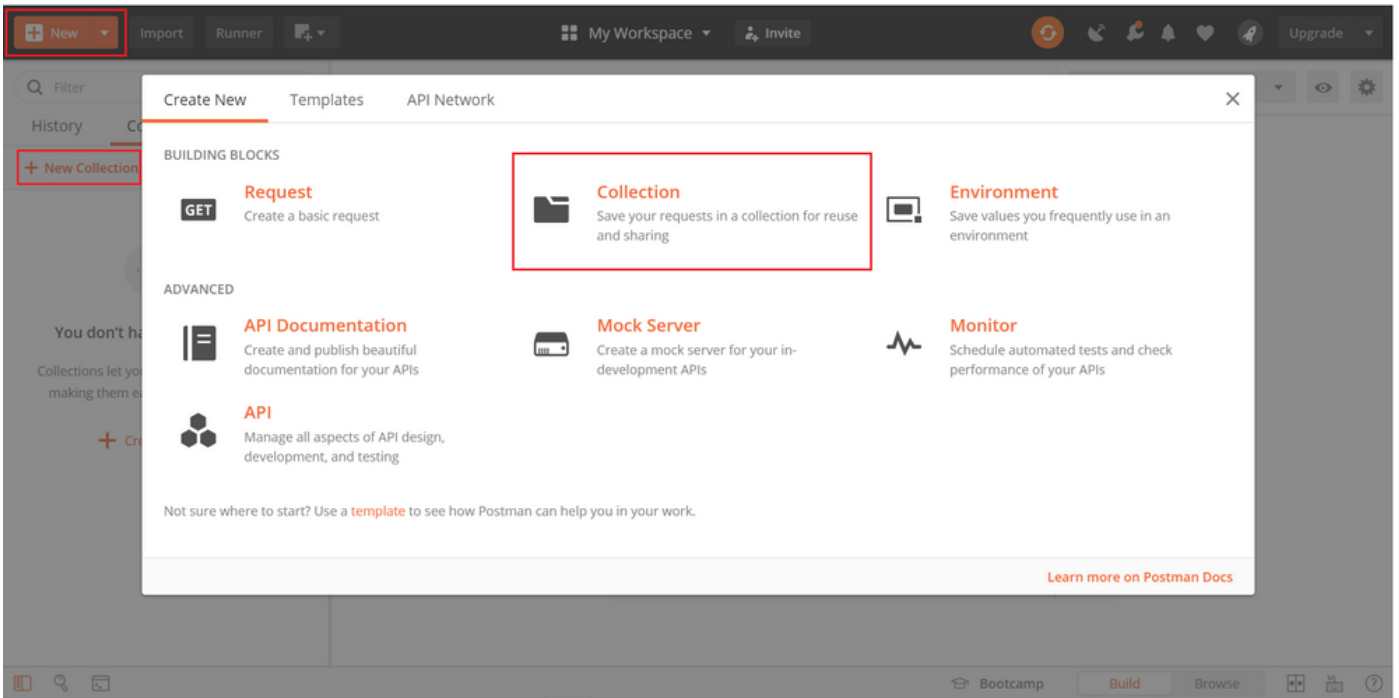
(API) تاقيبطتل ةجمرب ةهجاو ةمئاق لىع (API) تاقيبطتل ةجمرب ةهجاو فشكتسم يوتحي
https://<FTD Management IP>/API-Explorer لىل لقتنا .FTD لىع ةرفوتمل لمالكاب

تارايخل ايمج لىع عالطال لهي لىع رقناو LdapAttributeMap مسق لىل لفسأل ريرمتلاب مق
ةم وعدمل

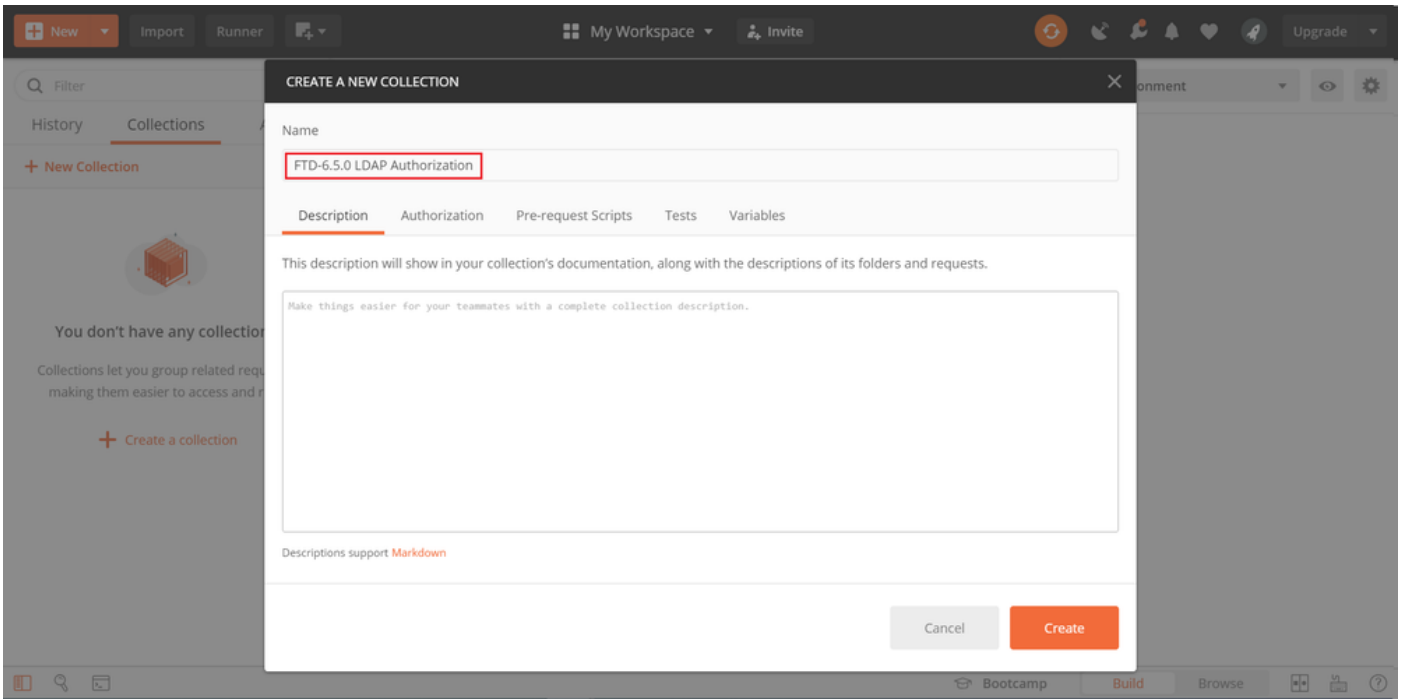


✎ عطيخ نيوكتل تاقيبطت ةجمررب ةهجاو ةادأك Postman مدختسن ،لاثملا اذه يف :ةظحالم ةمس LDAP.

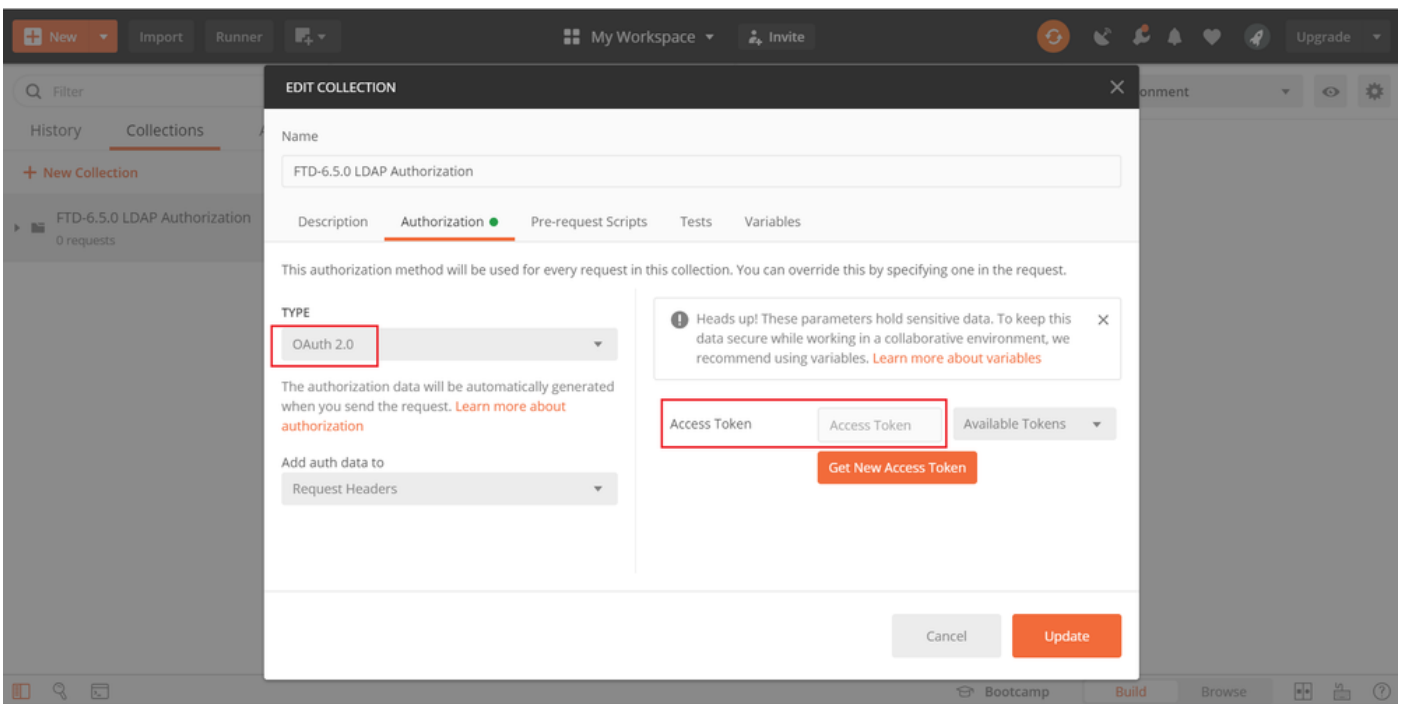
LDAP ضيوفتل ديربلا يعاس ةعومجم ةفاضلا 2. ةوطخلا



ةعومجملا هذهل امسا لخدا.



OAuth 2.0 عونلا ديحتو ةلودج دامت عال ريرحت



بنجتل SSL ةداهش نم ققحتل لايغشت فاقيا ب مق ، اتاداع | > فلم يلى لقتنا .3 ةئفل
مدختسي FTD ناك اذا كلذب مايقل المتوي . FTD يلى API تابلط لاسرا دنع SSL ةحفاصم لشف
اياتة عقوم ةداهش



Postman

File Edit View Help

New... Ctrl+N

New Tab Ctrl+T

New Postman Window Ctrl+Shift+N

New Runner Window Ctrl+Shift+R

Import... Ctrl+O

Settings Ctrl+Comma

Close Window Ctrl+Shift+W

Close Tab Ctrl+W

Force Close Tab Alt+Ctrl+W

Exit

SETTINGS ✕

General Themes Shortcuts Data Add-ons Certificates Proxy Update About

REQUEST

- Trim keys and values in request body OFF
- New Code Generation Mode ON
- Use next generation URL processing OFF
- SSL certificate verification** OFF
- Always open requests in new tab OFF
- Always ask when closing unsaved tabs ON
- Language detection
- Request timeout in ms
Set how long a request should wait for a response before timing out. To never time out, set to 0.
- Max response size in MB
Set the maximum size of a response to

HEADERS

- Send no-cache header ON
- Send Postman Token header ON
- Retain headers when clicking on links OFF
- Automatically follow redirects ON
- Send anonymous usage data to Postman ON

USER INTERFACE

- Editor Font Size (px)
- Two-pane view OFF
- Show icons with tab names ON
- Variable autocomplete ON
- Enable Launchpad ON

مسق في CA ةداهش ةئيه يلع FTD لبق نم ةمدختسمل ةداهشلا ةفاضل نكمي، كلذ نم الءب تاداءل نم ةداهشلا.

SETTINGS ✕

General Themes Shortcuts Data Add-ons **Certificates** Proxy Update About

CA Certificates OFF

The file should consist of one or more trusted certificates in PEM format.

PEM file

Client Certificates [Add Certificate](#)

Add and manage SSL certificates on a per domain basis.
[Learn more about working with certificates at our Learning Center.](#)

ىلإ لوخدلا لىجستل POST بىل طءاشنإل POST بىل طءدج ةقءاصم ةفاضب مق .4 ةوطخلا
POST/GET تابلط ألىوختل زىمملال زمرلا ىلع لوصحلل ،FTD.

+ New Collection

Trash

FTD-6.5.0 LDAP Authorization ☆

0 requests

This collec
collection



Share Collection



Manage Roles



Rename

Ctrl+E



Edit



Create a fork



Create Pull Request



Merge changes



Add Request



Add Folder



Duplicate

Ctrl+D



Export



Monitor Collection

لوبق | قبيطتال/json

MANAGE HEADER PRESETS

Add Header Preset

Header-LDAP

	KEY	VALUE	DESCRIPTION	...	Bulk Edit
<input checked="" type="checkbox"/>	Content-Type	application/json			
<input checked="" type="checkbox"/>	Accept	application/json			
	Key	Value	Description		

Cancel

Add

سأرمة مي ق دحو ولباقملا سأرلا تابي وبت لى لى لقتنا، رخألا تاب لطلال عي مجل ةبسن لابل تانا يبالا عونك json مادختس ال REST API تاب لطل Header-LDAP: هذه قبسملا دادعإلا يساسألا.

يلا تال لىل ع زي ممل زمرلا لىل لوصحلل POST بلط صن يوتحي نأ بجي:

عونلا	ماخ - JSON (قبيطتال/json)
grant_type	رورملا ةم لك
username	لىل لوخدلا لي جس تل لوؤسملا مدختسم مسأ
رورملا ةم لك	لوؤسملا مدختسملا باسحب ةنرتقملا رورملا ةم لك

```
{
  "grant_type": "password",
  "username": "admin",
  "password": "<enter the password>"
}
```

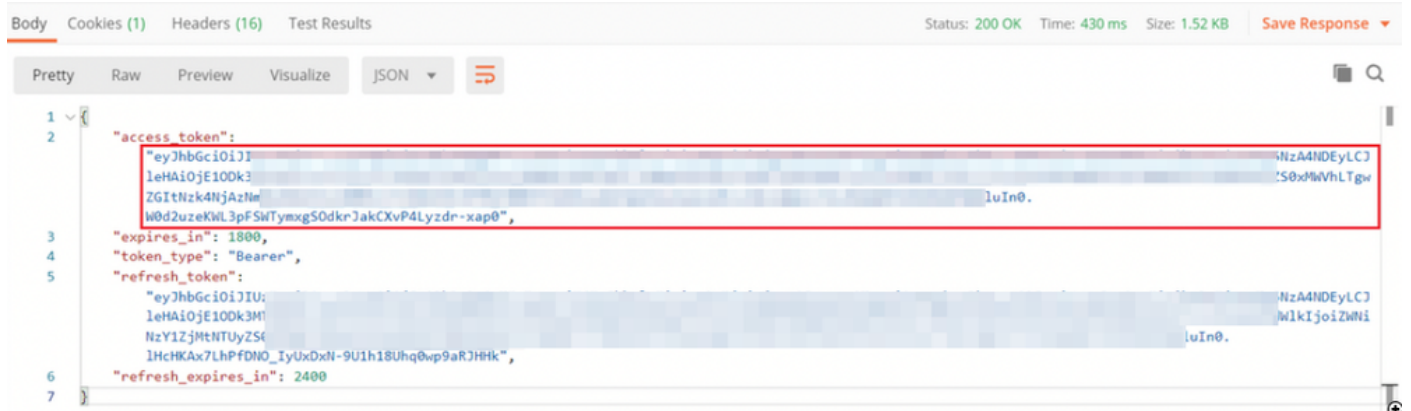
POST <https://1.../api/fdm/latest/fdm/token> Send

Params Authorization Headers (1) Body Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL BETA JSON

```
1 {
2   "grant_type": "password",
3   "username": "admin",
4   "password": "..."
5 }
```

م تي يذلا لوصولل زيمملا زمرلا ىلع ةباجتسالال صنيوتحي ،لاسرا قوف رقنلا درجمب
 لىل PUT/GET/POST تابلط ي لاسرال همادختسا

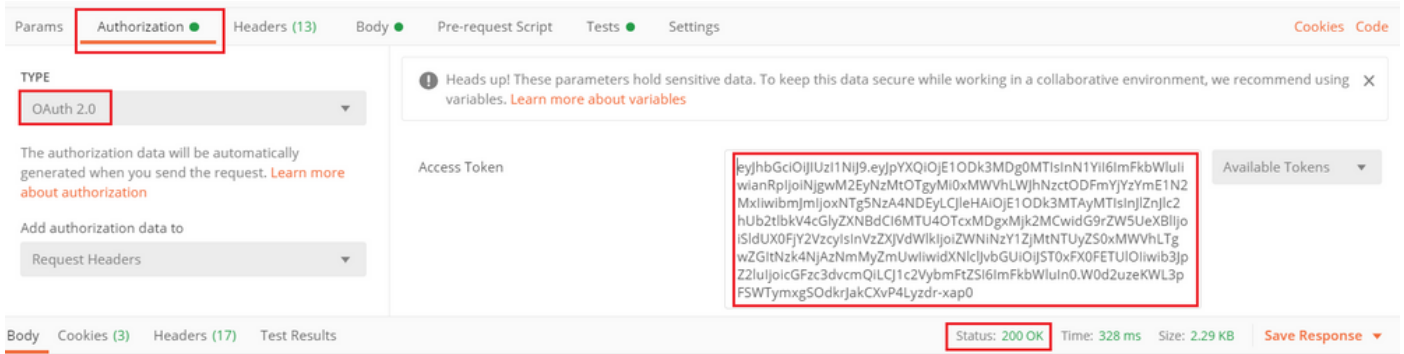


```
{
  "access_token": "eyJhbGciOiJIUzI1IiwiaXNjaW50eSI6ImVudC9kaXNjaW50eS00d2uzeKwL3pFShTymxgS0dkrJakCXvP4Lyzdr-xap0",
  "expires_in": 1800,
  "token_type": "Bearer",
  "refresh_token": "eyJhbGciOiJIUzI1IiwiaXNjaW50eSI6ImVudC9kaXNjaW50eS00d2uzeKwL3pFShTymxgS0dkrJakCXvP4Lyzdr-xap0",
  "refresh_expires_in": 2400
}
```

ةيلاتلا تابلطال عيجم ليوختل زيمملا زمرلا اذه مادختسا م تي م

يلاتلا ددحو ديدج بلط لكل ليوختلا بيوبتلا ةمالع ىل لقتنا

عونلا	OAuth 2.0
زمر	نم هيقلت م تي ذلا لوصولل زيمملا زمرلا
زيمم	POST لىل لوخدلا ليچست بلط ليغشت لالخ



جهن " ةلاح ىلع لوصحلل ةومجمل جهن ىلع لوصحلل ديدج GET بلط ةفاضل 5 ةوطخلل لاثمل اذه يف) هنيوكت مت ةومجمل جهن لكل فرعمل او مسالا عمجب مق . هتادادع او " ةومجمل ةيلاتل ةوطخلل يف هم ادختسالا (T-Group-Policy او HR-Group-Policy و Finance-Group-Policy

وانوع <https://<FTD Management IP>/API/FDM/latest/object/rootGroupPolicy> وه انهنيوكت مت يتل ةومجمل تاسايس ىلع لوصحلل URL ناونع

ةومجمل-ةيلاتل ةومجمل ةساييس ىلع ءوضلا طيلست متي ، يلاتل لاثمل يفو

```

+ New Collection  Trash  GET https://.../api/fdm/latest/object/ravngrouppolicies  Send
FTD-6.5.0 LDAP Authorization  Body  Cookies (3)  Headers (17)  Test Results  Status: 200 OK  Time: 129 ms  Size: 10.82 KB  Save
2 requests
POST Auth
GET Get Group-Policies
58 {
59   "version": "26d6c13b12p",
60   "name": "Finance-Group-Policy",
61   "banner": null,
62   "dnsServerGroup": null,
63   "defaultDomainName": null,
64   "simultaneousLogInPerUser": 3,
65   "maxConnectionTimeout": null,
66   "maxConnectionTimeAlertInterval": 1,
67   "vpnIdleTimeout": 30,
68   "vpnIdleTimeoutAlertInterval": 1,
69   "ipv4LocalAddressPool": [],
70   "ipv6LocalAddressPool": [],
71   "dhcpScope": null,
72   "ipv4SplitTunnelSetting": "TUNNEL_SPECIFIED",
73   "ipv6SplitTunnelSetting": "TUNNEL_ALL",
74   "ipv4SplitTunnelNetworks": [
75     {
76       "version": "ogalyil3higo",
77       "name": "ac11",
78       "id": "5ec790d-9836-11ea-ba77-37f667647b3e",
79       "type": "networkobject"
80     }
81   ],
82   "ipv6SplitTunnelNetworks": [],
83   "splitDNSRequestPolicy": "USE_SPLIT_TUNNEL_SETTING",
84   "splitDNSDomainList": "",
85   "scpeForwardingUrl": null,
86   "periodicClientCertAuthenticationInterval": 1,
87   "enableDTLS": false,
88   "enableDTLSCompression": false,
89   "sslCompression": "DISABLED",
90   "enableSSLrekey": false,
91   "rekeyMethod": "NEB_TUNNEL",
92   "rekeyInterval": 4,
93   "ignoreDFBit": false,
94   "bypassUnsupportedProtocol": false,
95   "mtuSize": 1400,
96   "useAlwaysOnVPNSettingInProfile": true,
97   "enableKeepAliveMessages": false,
98   "keepAliveMessageInterval": 20,
99   "enableGatewayDPO": false,
100  "gatewayDPOInterval": 30,
101  "enableClientDPO": false,
102  "clientDPOInterval": 30,
103  "clientProfiles": [],
104  "keepInstallerOnClient": false,
105  "vpnTrafficFilterACL": null,
106  "enableRestrictVPNToVLAN": false,
107  "restrictVPNToVLANs": null,
108  "clientFirewallPrivateNetworkRules": null,
109  "clientFirewallPublicNetworkRules": null,
110  "browserProxyType": "NO_PROXY",
111  "proxy": {
112    "serverHost": null,
113    "port": null,
114    "type": "serverhostandport"
115  },
116  "proxyExceptions": [],
117  "isEnablePeriodicClientCertAuthentication": false,
118  "id": "a5722b15-9836-11ea-ba77-6916f09acebc",
119  "type": "ravngrouppolicy",
120  "links": {
121    "self": "https://.../api/fdm/latest/object/ravngrouppolicies/a5722b15-9836-11ea-ba77-6916f09acebc"
122  }
123 },

```

في LDAP ةمس نييعت عاشنإل LDAP ةمس ططخم عاشنإ ديدج POST بلط ةفاضإ 6 ةوطخلإ
 لعل اضيأ ىرخألا جدامنلإ يوتحت .LdapAttributeMapping جذومنلإ مادختسإ متي ،دنتسمل اذه
 ةهجاو يف جدامنلإ هذهل ةلثمأ رفوتت .ةمسلا ةطيرخ عاشنإل ةهباشم بيلاس أو تاي لمع
 دنتسمل اذه يف اقباس روكذم وه امك (API-Explorer) تاقىبطلال ةجمررب

FTD REST API

API Explorer

Error Catalog

LdapAttributeMap

GET /object/ldapattributemaps

POST /object/ldapattributemaps

Implementation Notes
This API call is not allowed on the standby unit in an HA pair.

Response Class (Status 200)

Model Example Value

LdapAttributeMapping

description: Nested Entity which includes common objects for LdapAttributeMapping (Note: The field level constraints listed here might not cover all the constraints on the field. Additional constraints might exist.)

ldapName (string): The customer-specific LDAP attribute name that is being mapped.
Field level constraints: cannot be null, must match pattern ^((?:.)*\$). (Note: Additional constraints might exist).

ciscoName (string): An enum value that is the Cisco attribute name that maps to the customer-specific attribute name.
Field level constraints: cannot be null. (Note: Additional constraints might exist)

= ['ACCESS_HOURS', 'ALLOW_NETWORK_EXTENSION_MODE', 'AUTH_SERVICE_TYPE', 'AUTHENTICATED_USER_IDLE_TIMEOUT', 'AUTHORIZATION_REQUIRED', 'AUTHORIZATION_TYPE', 'BANNER1', 'BANNER2', 'CISCO_AV_PAIR', 'CISCO_IP_PHONE_BYPASS', 'CISCO_LEAP_BYPASS', 'CLIENT_BYPASS_PROTOCOL', 'CLIENT_INTERCEPT_DHCP_CONFIGURE_MSG', 'CLIENT_TYPE_VERSION_LIMITING', 'CONFIDENCE_INTERVAL', 'DHCP_NETWORK_SCOPE', 'DN_FIELD', 'DISABLE_ALWAYS_ON_VPN', 'FIREWALL_ACL_IN', 'FIREWALL_ACL_OUT', 'GATEWAY_FQDN', 'GROUP_POLICY', 'IE_PROXY_BYPASS_LOCAL', 'IE_PROXY_EXCEPTION_LIST', 'IE_PROXY_METHOD', 'IE_PROXY_SERVER', 'IETF_RADIUS_CLASS', 'IETF_RADIUS_FILTER_ID', 'IETF_RADIUS_FRAMED_IP_ADDRESS', 'IETF_RADIUS_FRAMED_IP_NETMASK', 'IETF_RADIUS_IPV6_PREFIX', 'IETF_RADIUS_IDLE_TIMEOUT', 'IETF_RADIUS_INTERFACE_ID', 'IETF_RADIUS_SERVICE_TYPE', 'IETF_RADIUS_SESSION_TIMEOUT', 'IKE DPD_Retry_Interval', 'IKE_KEEP_ALIVES', 'IPSEC_ALLOW_PASSWD_STORE', 'IPSEC_AUTH_ON_REKEY', 'IPSEC_AUTHENTICATION', 'IPSEC_BACKUP_SERVER_LIST', 'IPSEC_BACKUP_SERVERS', 'IPSEC_CLIENT_FIREWALL_FILTER_NAME', 'IPSEC_CLIENT_FIREWALL_FILTER_OPTIONAL', 'IPSEC_DEFAULT_DOMAIN', 'IPSEC_EXTENDED_AUTH_ON_REKEY', 'IPSEC_IKE_PEER_ID_CHECK', 'IPSEC_IP_COMPRESSION', 'IPSEC_IPV6_SPLIT_TUNNELING_POLICY', 'IPSEC_MODE_CONFIG', 'IPSEC_OVER_UDP', 'IPSEC_OVER_UDP_PORT', 'IPSEC_REQUIRED_CLIENT_FIREWALL_CAPABILITY', 'IPSEC_SPLIT_DNS_NAMES', 'IPSEC_SPLIT_TUNNEL_ALL_DNS', 'IPSEC_SPLIT_TUNNEL_LIST', 'IPSEC_SPLIT_TUNNELING_POLICY', 'IPSEC_TUNNEL_TYPE', 'IPSEC_USER_GROUP_LOCK', 'IPV6_PRIMARY_DNS', 'IPV6_SECONDARY_DNS', 'L2TP_ENCRYPTION', 'L2TP_MPPC_COMPRESSION', 'MS_CLIENT_SUBNET_MASK', 'PFS_REQUIRED', 'PPTP_ENCRYPTION', 'PPTP_MPPC_COMPRESSION', 'WEBVPN_VLAN']

valueMappings (Array[LdapToCiscoValueMapping]): A list of LdapToCiscoValueMapping objects, which specify the value mappings for this LDAP attribute.
Field level constraints: cannot be null. (Note: Additional constraints might exist).

type (string): ldapattributemapping

LdapAttributeToGroupPolicyMapping

description: An LDAP attribute to group policy mapping defines a customer-specific LDAP attribute name and maps it to a specific group policy object. Use this nested entity in an LDAP attribute map. (Note: The field level constraints listed here might not cover all the constraints on the field. Additional constraints might exist.)

ldapName (string): The customer-specific LDAP attribute name that is being mapped.
Field level constraints: cannot be null, must match pattern ^((?:.)*\$). (Note: Additional constraints might exist).

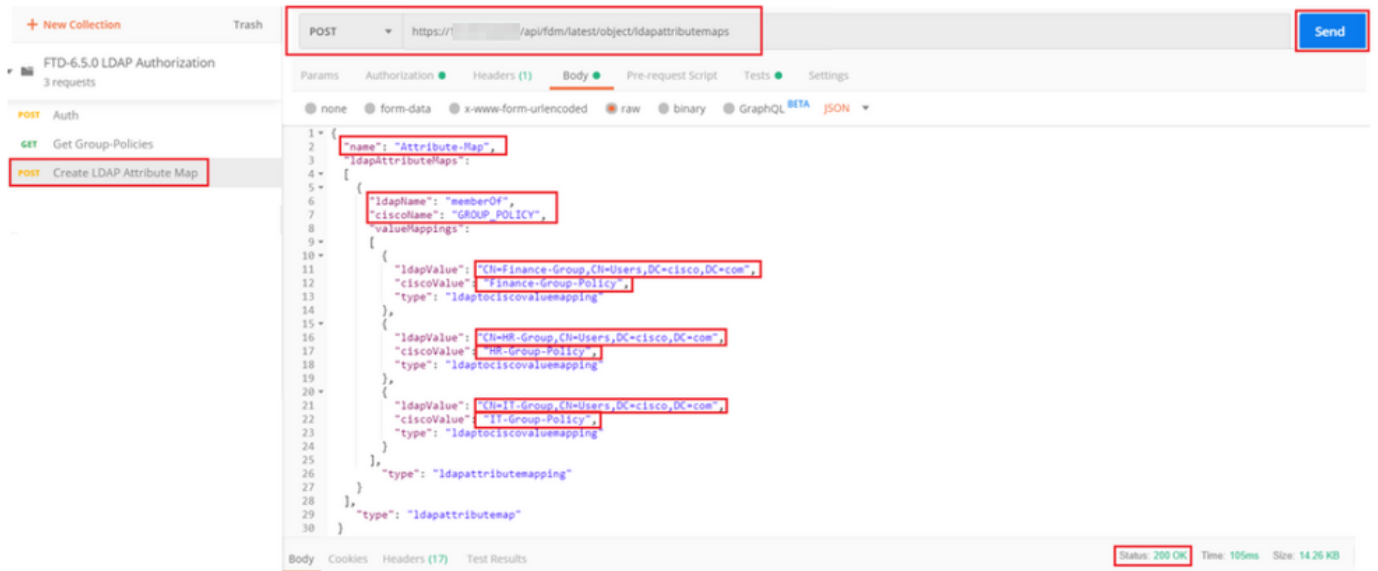
valueMappings (Array[LdapToGroupPolicyValueMapping]): A list of LdapToGroupPolicyValueMapping objects, which specify the value-to-group policy mappings for this LDAP attribute.
Field level constraints: cannot be null. (Note: Additional constraints might exist).

type (string): ldapattributetogrouppolicymapping

وهو LDAP ةمس ةطيرخ رشنل URL ناونع <https://<FTD Management IP>/API/FDM/latest/object/ldapattributeAps>

ي:لي ام ىلع رشنلا ةدام بلط صن يوتحي نأ بجي

م س ا ل ا	LDAP ةمس ني يع ت م س ا
ع و ن ل ا	ة ق ص ا ل ة ئ ز ج ت
ldapName	و ض ع
CiscoName	ة ع و م ج م ل ا ج ه ن
ldapValue	AD ن م م د خ ت س م ل ل و ض ع ل ا ة م ي ق
CiscoValue	ة ع و م ج م ل ل ة ع و م ج م ل ا ج ه ن م س ا FDM ي ف ن ي م د خ ت س م



ةومجم جهن نييغب موقت يال LDAP ةمس نييغت تامولعم لىع POST بلط صن يوتحي ةومجم لى ادانتسا AD ةومجم لى ددحم memberOf:

```
{
  "name": "Attribute-Map",
  "ldapAttributeMaps":
  [
    {
      "ldapName": "memberOf",
      "ciscoName": "GROUP_POLICY",
      "valueMappings":
      [
        {
          "ldapValue": "CN=Finance-Group,CN=Users,DC=cisco,DC=com",
          "ciscoValue": "Finance-Group-Policy",
          "type": "ldaptociscovaluemapping"
        },
        {
          "ldapValue": "CN=HR-Group,CN=Users,DC=cisco,DC=com",
          "ciscoValue": "HR-Group-Policy",
          "type": "ldaptociscovaluemapping"
        },
        {
          "ldapValue": "CN=IT-Group,CN=Users,DC=cisco,DC=com",
          "ciscoValue": "IT-Group-Policy",
          "type": "ldaptociscovaluemapping"
        }
      ],
      "type": "ldapattributemapping"
    }
  ],
  "type": "ldapattributemap"
}
```


نكمي وأ dsquery رمأل مادختساب AD م داخ نم memberOf ل قح دادرتسإ نكمي :ةظحال
نع شحبا ،ءاطخأل احيحصت تالچس يف .FTD لىع LDAP ءاطخأ احيحصت نم هراضح
memberOf value: field.

ةيلال ةطقنلل ةهباشم اذهرشنللا ةدام بلط ةباجتسإ نأ ودبي:

```
Body Cookies (3) Headers (17) Test Results Status: 200 OK Time: 193 ms Size: 1.46 KB Save Response
Pretty Raw Preview Visualize JSON
1 {
2   "version": "nuy43ud4d32po",
3   "name": "Attribute-Map",
4   "ldapAttributeMaps": [
5     {
6       "ldapName": "memberOf",
7       "ciscoName": "GROUP_POLICY",
8       "valueMappings": [
9         {
10          "ldapValue": "CN=HR-Group,CN=Users,DC=cisco,DC=com",
11          "ciscoValue": "HR-Group-Policy",
12          "type": "ldaptociscovaluemapping"
13        },
14        {
15          "ldapValue": "CN=IT-Group,CN=Users,DC=cisco,DC=com",
16          "ciscoValue": "IT-Group-Policy",
17          "type": "ldaptociscovaluemapping"
18        },
19        {
20          "ldapValue": "CN=Finance-Group,CN=Users,DC=cisco,DC=com",
21          "ciscoValue": "Finance-Group-Policy",
22          "type": "ldaptociscovaluemapping"
23        }
24      ],
25      "type": "ldapattributemapping"
26    }
27  ],
28  "ldapAttributeToGroupPolicyMappings": [],
29  "id": "b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c",
30  "type": "ldapattributemap",
31  "links": {
32    "self": "https://.../api/fdm/latest/object/ldapattributemaps/b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c"
33  }
34 }
```

FDM لىع يلالال AD قاطن نيوكت لىع لوصحلل ديدج GET بلط ةفاضاب مق 7. ةوطخال

وه يلالال نالعال قاطن نيوكت لىع لوصحلل URL ناوع
<https://<FTD Management IP>/API/FDM/latest/object/realms>

```

1 {
2   "realms": [
3     {
4       "version": "k3j0dha5ixyy",
5       "name": "LDAP-AD",
6       "directoryConfigurations": [
7         {
8           "hostname": "192.168.1.1",
9           "port": 389,
10          "encryptionProtocol": "NONE",
11          "encryptionCert": null,
12          "type": "directoryconfiguration"
13        }
14      ],
15      "enabled": true,
16      "systemDefined": false,
17      "realId": "",
18      "dirUsername": "administrator@192.168.1.1",
19      "dirPassword": "*****",
20      "baseDN": "dc=192.168.1, dc=com",
21      "ldapAttributeMap": null,
22      "adPrimaryDomain": "192.168.1",
23      "id": "bf50a8ab-9819-11ea-ba77-d32ecc224295",
24      "type": "activedirectoryrealm",
25      "links": {
26        "self": "https://192.168.1.1/api/fdm/latest/object/realms/bf50a8ab-9819-11ea-ba77-d32ecc224295"
27      }
28    }
29  ],
30  "paging": {
31    "prev": [],
32    "next": [],
33    "limit": 10,
34    "offset": 0,
35    "count": 1,
36    "pages": 0
37  }
38 }

```

نأ طحال null. يه لdapAttributeMap اجات فم ال م يق نأ طحال.

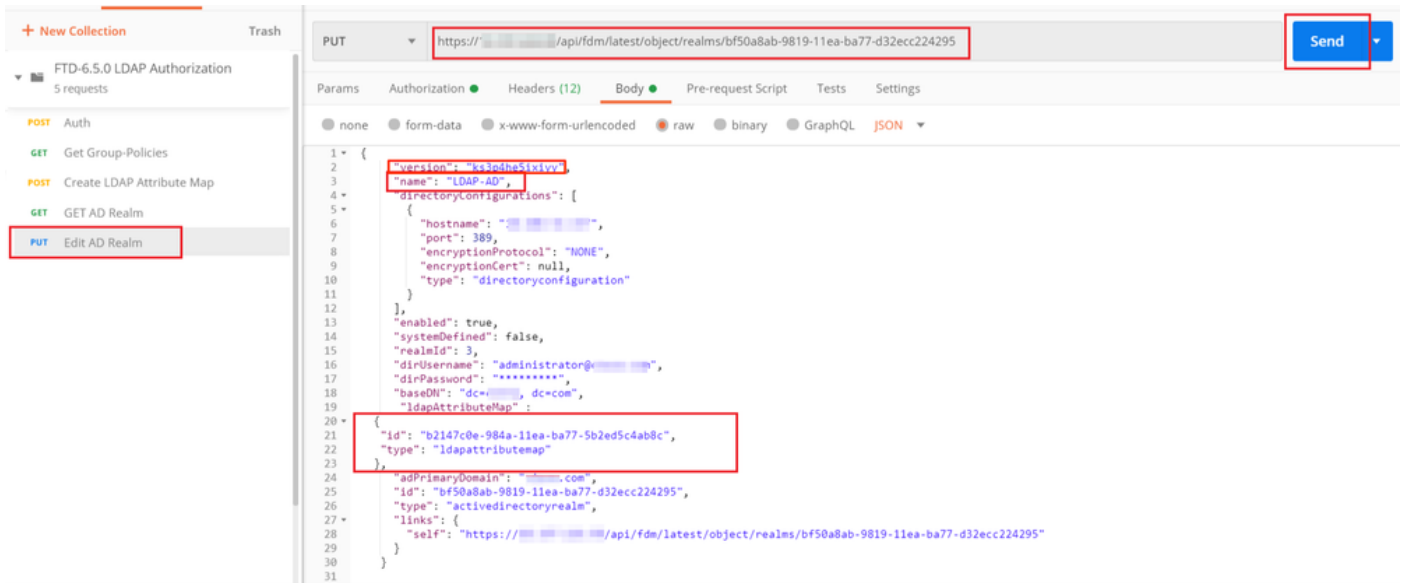
ة و طخال نم GET ة باجات سا جارخا خسنا AD. ل اجم ريرحتل ديدج PUT بلط عاشن اب مق 8. ة و طخال ا جارخا ة و طخال هذ م ادختسا نكمي. اذ ديدجل PUT بلط صن ل ا اتفاض او ق باسل او IP نا ونع او رورم ل ة ملك ريرغت: ل ا ثم ل ل بس ل ع، ل ا ل ا ل AD ق اطن دادع ل ع تال يدعت ة. ل ا ل ا هذ ف لdapAttributeMap ل ثم اجات فم ل ال ة ديدج ة م يق ة فاضا

لم الك اب GET ة باجات سا جارخا نم ال دب رصان ال ة م ئاق تايوتحم خسن م هم ل نم: ة طحال م. اراج م ت يذ ل ن ئا ك ل رصنع فرعم ب PUT بلط صاخ ل بل ط ل ل URL نا ونع ق ا ل ب ج ي. ه ب ة صاخ ل تار يرغت ل ل bf50a8ab-9819-11ea-ba77-d32ecc224295: يه ة م يق ل ل، ل ا ثم ل ا هذ ف. ه ب ة صاخ ل تار يرغت ل ل

وه ل ل ا ل ا ل ا ل ا ق اطن ن ي و ك ت ريرحتل URL نا ونع <https://<FTD Management IP>/API/FDM/latest/object/realms/<realm id>>

: ل ي ل ا م ل ع PUT بلط صن يوتح ل نأ ب ج ي

رادص ا ل ا	نم ه ي ل ع ل و ص ح ل م ت ي ذ ل رادص ا ل ا ق باسل ل GET بلط ة باجات سا
فرعم	نم ه ي ل ع ل و ص ح ل م ت ي ذ ل فرعم ل ا ق باسل ل GET بلط ة باجات سا
ldapAttributeMap	ل د ي ع ت عاشن ا بلط ة باجات سا نم LDAP-id ة م س LDAP



وهو لاثم ال اذه في نيوكتل صرن

<#root>

```

{
  "version": "ks3p4he5ixiyy",
  "name": "LDAP-AD",
  "directoryConfigurations": [
    {
      "hostname": "<IP Address>",
      "port": 389,
      "encryptionProtocol": "NONE",
      "encryptionCert": null,
      "type": "directoryconfiguration"
    }
  ],
  "enabled": true,
  "systemDefined": false,
  "realmId": 3,
  "dirUsername": "administrator@example.com",
  "dirPassword": "*****",
  "baseDN": "dc=example, dc=com",
  "ldapAttributeMap":
  {
    "id": "b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c",
    "type": "ldapattributemap"
  },
  "adPrimaryDomain": "example.com",
  "id": "bf50a8ab-9819-11ea-ba77-d32ecc224295",
  "type": "activedirectoryrealm",
  "links": {

```

```
"self": "https://
```

```
/api/fdm/latest/object/realms/bf50a8ab-9819-11ea-ba77-d32ecc224295"
```

```
}  
}
```

بطلال اذهل ةباجتسالال صرن يف id لdapAttributeMap قباطت نم ققحت

```
Body Cookies (3) Headers (17) Test Results Status: 200 OK Time: 657 ms Size: 1.37 KB Save Response  
Pretty Raw Preview Visualize JSON  
1 {  
2   "version": "ksy7p574fq7w",  
3   "name": "LDAP-AD",  
4   "directoryConfigurations": [  
5     {  
6       "hostname": " ",  
7       "port": 389,  
8       "encryptionProtocol": "NONE",  
9       "encryptionCert": null,  
10      "type": "directoryconfiguration"  
11    }  
12  ],  
13  "enabled": true,  
14  "systemDefined": false,  
15  "realmId": 3,  
16  "dirUsername": "administrator",  
17  "dirPassword": "*****",  
18  "baseDN": "dc= , dc=com",  
19  "ldapAttributeMap": {  
20    "version": "mwy43w4jd32po",  
21    "name": "Attribute-Map",  
22    "id": "b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c",  
23    "type": "ldapattributemap"  
24  },  
25  "adPrimaryDomain": ".com",  
26  "id": "bf50a8ab-9819-11ea-ba77-d32ecc224295",  
27  "type": "activedirectoryrealm",  
28  "links": {  
29    "self": "https:// /api/fdm/latest/object/realms/bf50a8ab-9819-11ea-ba77-d32ecc224295"  
30  }  
31 }
```

ةمس ططخم عاشناب مق PUT تابلط مادختساب LDAP ةمس نييعت ليدعت نكمي (يرايخا) MemberOf Value و Attribute-Map مسا لثم تاريخيغت ي اءراج مق و ديدج PUT بلط ريرحت

تاعومجملل cn=UserGroup لىل cn=Users نم ldapvalue ةمي ق ليدعت مت ،يلاتال لاثملال يف اهعيمج ثالثلال

```

1 PUT https://10.197.224.99/api/fdm/latest/object/ldapattributemaps/021470e-904a-11ea-ba77-5b2ed5c4abdc
2 {"description": "New LDAP Attribute Map",
3  "name": "MEMBER-ADP",
4  "ldapattributes":
5  {
6  {
7    "ldapname": "memberOf",
8    "ciscoName": "GROUP_POLICY",
9    "valueMappings":
10   {
11   {
12     "ldapvalue": "C=Finance-Group,C=UserGroup,DC=Cisco,DC=com",
13     "ciscoValue": "Finance-Group-POLICY",
14     "type": "LDAPtoCiscoValueMapping"
15   }
16   }
17   {
18     "ldapvalue": "C=HR-Group,C=UserGroup,DC=Cisco,DC=com",
19     "ciscoValue": "HR-Group-POLICY",
20     "type": "LDAPtoCiscoValueMapping"
21   }
22   {
23     "ldapvalue": "C=IT-Group,C=UserGroup,DC=Cisco,DC=com",
24     "ciscoValue": "IT-Group-POLICY",
25     "type": "LDAPtoCiscoValueMapping"
26   }
27   }
28 }
29 }
30 "id": "021470e-904a-11ea-ba77-5b2ed5c4abdc",
31 "type": "LDAPAttributeMap",
32 "links": {
33   "self": "https://10.197.224.99/api/fdm/latest/object/ldapattributemaps/021470e-904a-11ea-ba77-5b2ed5c4abdc"
34 }
35 }

```

فدحل بلطل لئسأسأل URL ناوئعب قحل أو ةقبأسل HTTP ةبأجتسإ نم ةطبرخل فرم نئمضتب مق . ةمس نئبعت فدحل بلط عاشنإب مق ، دوجوم LDAP ةمس ططخم فدحل . (برارتخا)

```

DELETE https://10.197.224.99/api/fdm/latest/object/ldapattributemaps/021470e-904a-11ea-ba77-5b2ed5c4abdc
{"id": "021470e-904a-11ea-ba77-5b2ed5c4abdc", "type": "LDAPAttributeMap"}

```

ارفشم URL نوئي نأ بجيف ، تافاسم لئع يوتحت memberOf ةمس لئناك اذا : ةطخال م مقرر بلطل لئسأسأل HTTP ةبأجتسإ يقلت متي ال أو . اه لئل لئسأسأل موقيل بيولا مداخل 20٪ ام امدختسإ نكمي ، ءاضي ب تافاسم لئع يوتحت يتل ةلسلسل ةبسنلاب . 400 أطلخا اذ بئجتل "+" وأ

نأل رشنل قوف رقناو رشنل زمر دجو ، FDM لئل ىرخأ ةرم لقتنا . 9 ةوطخل

Pending Changes



✓ Last Deployment Completed Successfully
17 May 2020 07:46 PM. [See Deployment History](#)

Deployed Version (17 May 2020 07:46 PM)	Pending Version
Idapattributemap Added: Attribute-Map	
-	ldapAttributeMaps[0].ldapName: memberOf
-	ldapAttributeMaps[0].valueMappings[0].ldapValue: CN=IT-Gr...
-	ldapAttributeMaps[0].valueMappings[0].ciscoValue: IT-Grou...
-	ldapAttributeMaps[0].valueMappings[1].ldapValue: CN=HR-Gr...
-	ldapAttributeMaps[0].valueMappings[1].ciscoValue: HR-Grou...
-	ldapAttributeMaps[0].valueMappings[2].ldapValue: CN=Finan...
-	ldapAttributeMaps[0].valueMappings[2].ciscoValue: Finance...
-	ldapAttributeMaps[0].ciscoName: GROUP_POLICY
-	name: Attribute-Map
Active Directory Realm Edited: LDAP-AD	
ldapAttributeMap:	
-	Attribute-Map

MORE ACTIONS ▾ CANCEL DEPLOY NOW ▾

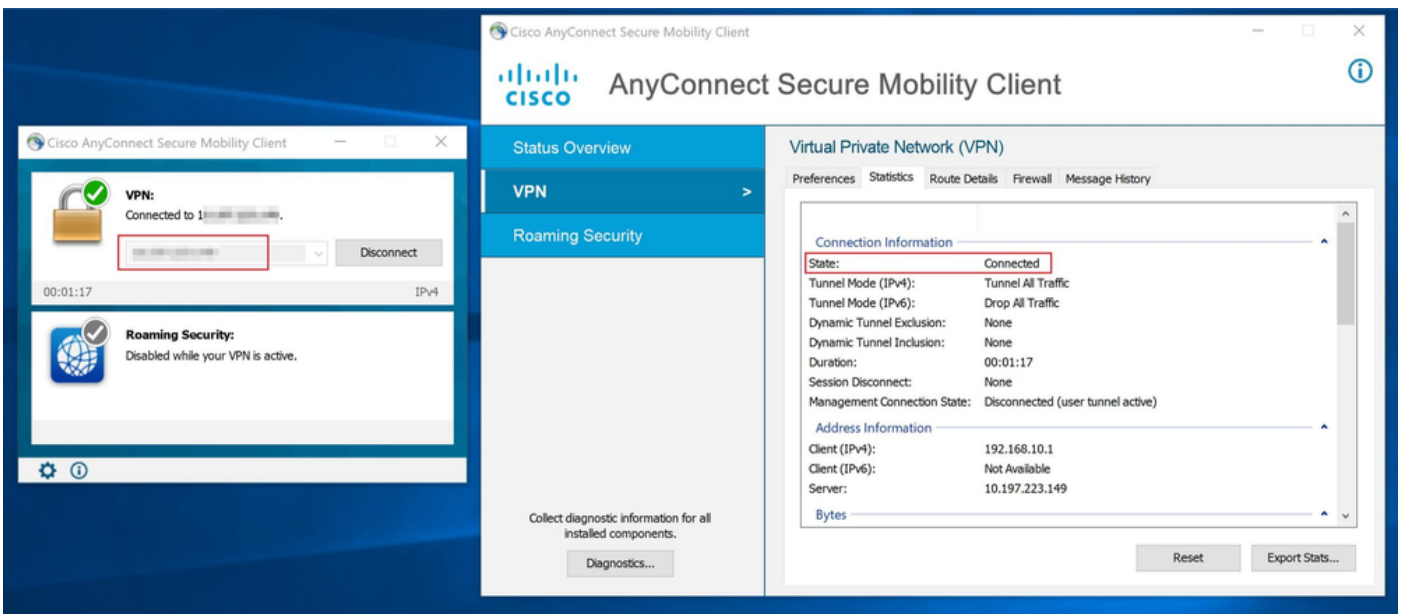
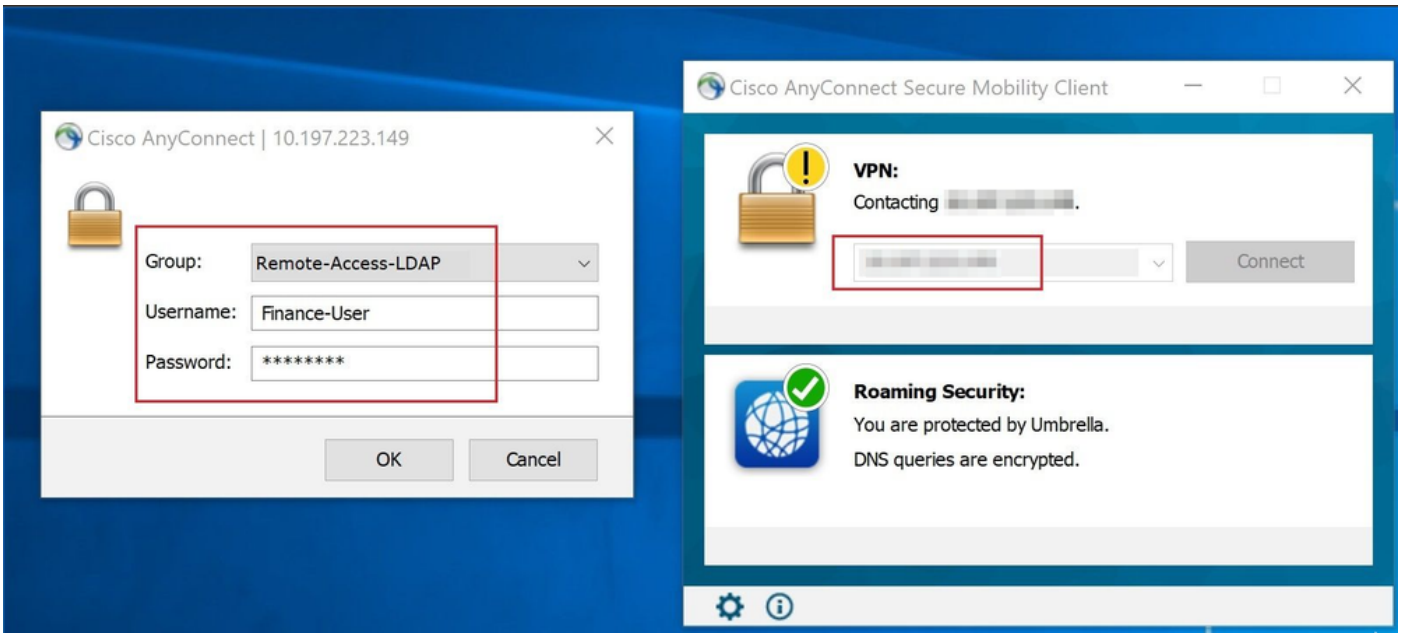
تحصيل نام ققحتلا

FDM يف رشنلا تاظوفحم مسق يف رشنلا تاريغيغ نم ققحتلا نكمي

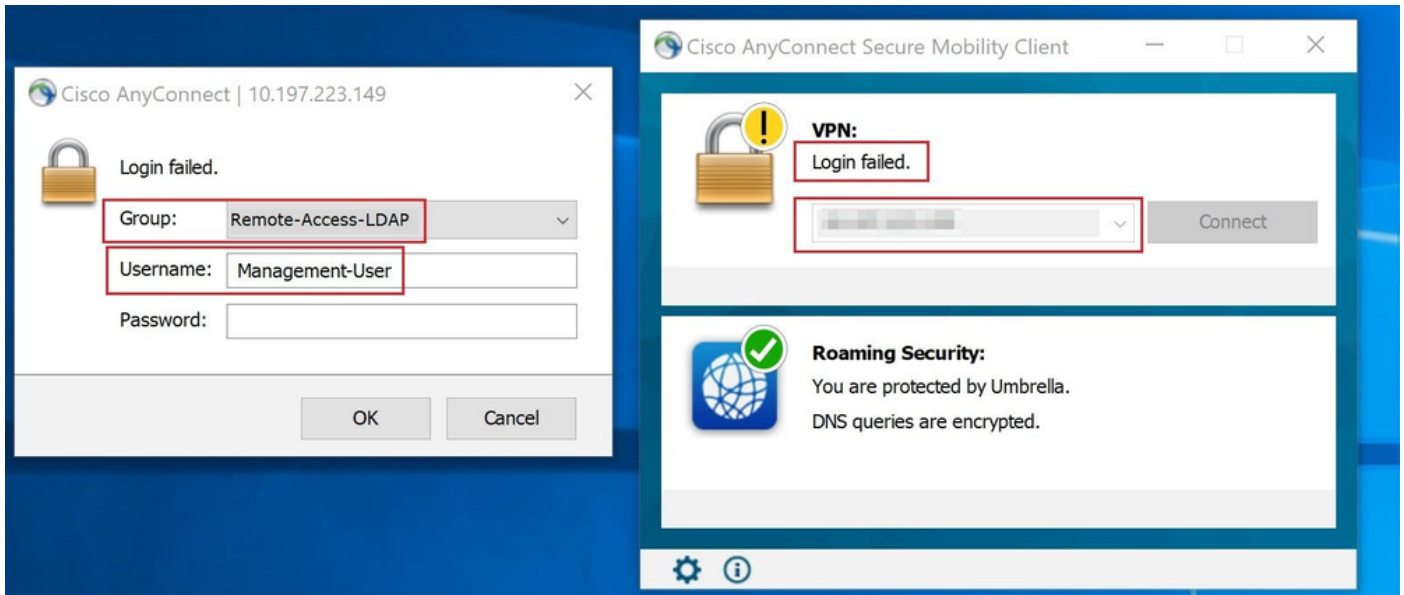
The screenshot shows the Cisco Firepower Device Manager interface. The top navigation bar includes 'Firepower Device Manager', 'Monitoring', 'Policies', 'Objects', and 'Device: firepower'. The user is logged in as 'admin Administrator'. The main content area displays a 'Deployment Completed' message for a 'User (admin) Triggered Deployment'. Below this, there are two sections: 'Idapattributemap Added: Attribute-Map' and 'Active Directory Realm Edited: LDAP-AD'. The 'Idapattributemap' section shows a comparison between the 'Deployed Version' and the 'Pending Version'. The 'Deployed Version' shows an empty list, while the 'Pending Version' shows a list of mappings for the 'Attribute-Map'.

عملكو مدختسمل مساق ققحتلا يف AD دامتعا تانايب ريفوتب مق، نيوكتلا اذه رابتخال رورمل.

وه امك ةلواحملا حجنت ،لوخذلا ليجست AD ةلالام ةومجم ىلإ يمتني مدختسم لواحي ام دنع عقوتم.



Connection-Profile ب لاصتال AD يف ةرادإلا ةومجم ىلإ يمتني مدختسم لواحي ام دنع ةومجملا جهن نوكي ،ةقباطم LDAP ةمس ةطيخ يأ عاچرا مدعل ارظن ، Remote-Access-LDAP ليجست تاي لمع نييعت مت يذل NOACCESS وه FTD ىل مدختسملا اذه لبق نم ثروملا لوخذلا ليجست ةلواحم لشفت ،يلالابو 0. ةميقلا ىل ع vpn ب ةصاخلا ةنمازتملا لوخذلا مدختسملا اذل.



ةصاخلا (CLI) رم اوألا رطس ةهجاو نم ةيلالاتلا show رم اوأ مادختسا ب نيوكتلا نم ققحتلا نكمي ب FTD:

<#root>

firepower#

show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username :

Finance-User

Index : 26
Assigned IP : 192.168.10.1 Public IP : 10.1.1.1
Protocol : AnyConnect-Parent SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384
Bytes Tx : 22491197 Bytes Rx : 14392
Group Policy :

Finance-Group-Policy

Tunnel Group : Remote-Access-LDAP
Login Time : 11:14:43 UTC Sat Oct 12 2019
Duration : 0h:02m:09s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 00000000001a0005da1b5a3
Security Grp : none Tunnel Zone : 0

<#root>


```
firepower#  
show run aaa-server LDAP-AD  
aaa-server LDAP-AD protocol ldap  
  realm-id 3  
aaa-server AD1 host 192.168.1.1  
  server-port 389  
  ldap-base-dn dc=example, dc=com  
  ldap-scope subtree  
  ldap-login-password *****  
  ldap-login-dn Administrator@example.com  
  server-type auto-detect
```

```
ldap-attribute-map Attribute-Map
```


```
<#root>
```

```
firepower#  
show run ldap attribute-map  
ldap attribute-map Attribute-Map  
  map-name memberOf Group-Policy  
  map-value memberOf CN=Finance-Group,CN=Users,DC=cisco,DC=com Finance-Group-Policy  
  map-value memberOf CN=HR-Group,CN=Users,DC=cisco,DC=com HR-Group-Policy  
  map-value memberOf CN=IT-Group,CN=Users,DC=cisco,DC=com IT-Group-Policy
```

اهحال صإو اءاطخأل فاشك ت سا

زيمم ل زمر ل دي دجت REST تاق ي ب ط ت ة ج م ر ب ة ج او ني و ك ت عم اعويش ل كاشم ل رثك أ نم بل ط ل ة ب ا ج ت س ا ل ا ي ف زيمم ل زمر ل ا ة ي ح ا ل ص ا ه ا ت ن ا ت ق و ر ي ف و ت م ت ي . ر خ آل ت ق و ن م ل م ا ح ل ل ة ر ت ف ل ي ف ا ض ا زيمم ث ي د ح ت زمر م ا د خ ت س ا ن ك م ي ، ة د م ل ه ذ ه ة ي ح ا ل ص ت ه ت ن ا ا ذ ا . ة ق د ا ص م ل ا ة د ا ع ا ل د ي د ج ة ق د ا ص م ب ل ط ل ا س ر ا ب ج ي ، ا ض ي ا ث ي د ح ت ل ل زيمم ل زمر ل ا ة ي ح ا ل ص ا ه ا ت ن ا د ع ب . ل و ط ا ة د ي د ج ل و ص و ل ل زيمم زمر ني ي ع ت .

 debug رماو ا م ا د خ ت س ا ل ب ق [ح ي ح ص ت ل ا ر م ا و ا ل و ح ة م ه م ت ا م و ل ع م](#) ي ل ا ع ج ر ا : ة ظ ح ا ل م .

 م ا د خ ت س ا م ت ي ، ي ض ا ر ت ف ا ل ك ش ب . ة ع و ن ت م ا ة ط خ ا ح ي ح ص ت ت ا ي و ت س م ط ب ض ك ن ك م ي ع س و ت ة ج ر د د ي ا ز ت د ق ف ، ا ة ط خ ا ل ا ح ي ح ص ت ي و ت س م ر ي ي غ ت ب ت م ق ا ذ ا . 1 . ي و ت س م ل ا ج ا ت ن ا ل ا ت ا ئ ي ب ي ف ة ص ا خ و ، ر ذ ح ب ك ل ذ ب م ق . ا ة ط خ ا ل ا ح ي ح ص ت

ة ق ل ع ت م ل ل ك ا ش م ل ا ف ا ش ك ت س ا ي ف ة د ي ف م F T D ل C L I ي ل ع ة ي ل ا ت ل ا ة ط خ ا ل ا ن و ك ت د ق ا ه ا ح ا ل ص ا و LDAP ة م س ة ط ي ر خ ب

```
debug ldap 255  
debug webvpn condition user <username>
```

```
debug webvpn anyconnect 255
debug aaa common 127
```

مت يتي الل تامول عمل احيضوتل ةي لالتل اءاطخأل احيحصت تايللمع عي مجت مت .لثاملا اذه ي في
ل.اصتالال لبق نيروكذمل رابتخالال يمدختسم مايق دنع AD مداخ نم اهيقلل

ل:ويومتل امدختسمل LDAP اءاطخأل احيحصت

```
<#root>
```

```
[48] Session Start
[48] New request Session, context 0x00002b0482c2d8e0, reqType = Authentication
[48] Fiber started
[48] Creating LDAP context with uri=ldap://192.168.1.1:389
[48] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[48] supportedLDAPVersion: value = 3
[48] supportedLDAPVersion: value = 2
[48] LDAP server192.168.1.1 is Active directory
[48] Binding as Administrator@cisco.com
[48] Performing Simple authentication for Administrator@example.com to192.168.1.1
[48] LDAP Search:
      Base DN = [dc=cisco, dc=com]
      Filter  = [sAMAccountName=Finance-User]
      Scope   = [SUBTREE]
[48] User DN = [CN=Finance-User,OU=Finance,OU=VPN,DC=cisco,DC=com]
[48] Talking to Active Directory server 192.168.1.1
[48] Reading password policy for Finance-User, dn:CN=Finance-User,OU=Finance,OU=VPN,DC=cisco,DC=com
[48] Read bad password count 0
[48] Binding as Finance-User
[48] Performing Simple authentication for Finance-User to 192.168.1.1
[48] Processing LDAP response for user Finance-User
[48] Message (Finance-User):
[48]
```

```
Authentication successful for Finance-User to 192.168.1.1
```

```
[48] Retrieved User Attributes:
[48]   objectClass: value = top
[48]   objectClass: value = person
[48]   objectClass: value = organizationalPerson
[48]   objectClass: value = user
[48]   cn: value = Finance-User
[48]   givenName: value = Finance-User
[48]   distinguishedName: value = CN=Finance-User,OU=Finance,OU=VPN,DC=cisco,DC=com
[48]   instanceType: value = 4
[48]   whenCreated: value = 20191011094454.0Z
[48]   whenChanged: value = 20191012080802.0Z
[48]   displayName: value = Finance-User
[48]   uSNCreated: value = 16036
[48]
```

```
memberOf: value = CN=Finance-Group,CN=Users,DC=cisco,DC=com
```

```
[48]
```

```
mapped to Group-Policy: value = Finance-Group-Policy
```

```
[48]
```

```
mapped to LDAP-Class: value = Finance-Group-Policy
```

```
[48] memberOf: value = CN=Users,CN=Builtin,DC=cisco,DC=com
[48] mapped to Group-Policy: value = CN=Users,CN=Builtin,DC=cisco,DC=com
[48] mapped to LDAP-Class: value = CN=Users,CN=Builtin,DC=cisco,DC=com
[48] uSNChanged: value = 16178
[48] name: value = Finance-User
[48] objectGUID: value = .J.2...N...X.0Q
[48] userAccountControl: value = 512
[48] badPwdCount: value = 0
[48] codePage: value = 0
[48] countryCode: value = 0
[48] badPasswordTime: value = 0
[48] lastLogoff: value = 0
[48] lastLogon: value = 0
[48] pwdLastSet: value = 132152606948243269
[48] primaryGroupID: value = 513
[48] objectSid: value = .....B...a5/ID.dT...
[48] accountExpires: value = 9223372036854775807
[48] logonCount: value = 0
[48] sAMAccountName: value = Finance-User
[48] sAMAccountType: value = 805306368
[48] userPrincipalName: value = Finance-User@cisco.com
[48] objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=cisco,DC=com
[48] dSCorePropagationData: value = 20191011094757.0Z
[48] dSCorePropagationData: value = 20191011094614.0Z
[48] dSCorePropagationData: value = 16010101000000.0Z
[48] lastLogonTimestamp: value = 132153412825919405
[48] Fiber exit Tx=538 bytes Rx=2720 bytes, status=1
[48] Session End
```

مدخست سمل-ةرادال LDAP ءاطخأ حيحصت

<#root>

```
[51] Session Start
[51] New request Session, context 0x00002b0482c2d8e0, reqType = Authentication
[51] Fiber started
[51] Creating LDAP context with uri=ldap://192.168.1.1:389
[51] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[51] supportedLDAPVersion: value = 3
[51] supportedLDAPVersion: value = 2
[51] LDAP server 192.168.1.1 is Active directory
[51] Binding as Administrator@cisco.com
[51] Performing Simple authentication for Administrator@example.com to 192.168.1.1
[51] LDAP Search:
      Base DN = [dc=cisco, dc=com]
      Filter = [sAMAccountName=Management-User]
      Scope = [SUBTREE]
[51] User DN = [CN=Management-User,OU=Management,OU=VPN,DC=cisco,DC=com]
[51] Talking to Active Directory server 192.168.1.1
[51] Reading password policy for Management-User, dn:CN=Management-User,OU=Management,OU=VPN,DC=cisco,DC=com
[51] Read bad password count 0
[51] Binding as Management-User
[51] Performing Simple authentication for Management-User to 192.168.1.1
[51] Processing LDAP response for user Management-User
[51] Message (Management-User):
[51]
```

Authentication successful for Management-User to 192.168.1.1

```
[51] Retrieved User Attributes:
[51]   objectClass: value = top
[51]   objectClass: value = person
[51]   objectClass: value = organizationalPerson
[51]   objectClass: value = user
[51]   cn: value = Management-User
[51]   givenName: value = Management-User
[51]   distinguishedName: value = CN=Management-User,OU=Management,OU=VPN,DC=cisco,DC=com
[51]   instanceType: value = 4
[51]   whenCreated: value = 20191011095036.0Z
[51]   whenChanged: value = 20191011095056.0Z
[51]   displayName: value = Management-User
[51]   uSNCreated: value = 16068
[51]
```

```
memberOf: value = CN=Management-Group,CN=Users,DC=cisco,DC=com
```

```
[51]
```

```
mapped to Group-Policy: value = CN=Management-Group,CN=Users,DC=cisco,DC=com
```

```
[51]
```

```
mapped to LDAP-Class: value = CN=Management-Group,CN=Users,DC=cisco,DC=com
```

```
[51]   memberOf: value = CN=Users,CN=Builtin,DC=cisco,DC=com
[51]     mapped to Group-Policy: value = CN=Users,CN=Builtin,DC=cisco,DC=com
[51]     mapped to LDAP-Class: value = CN=Users,CN=Builtin,DC=cisco,DC=com
[51]   uSNChanged: value = 16076
[51]   name: value = Management-User
[51]   objectGUID: value = i._(.E.O....Gig
[51]   userAccountControl: value = 512
[51]   badPwdCount: value = 0
[51]   codePage: value = 0
[51]   countryCode: value = 0
[51]   badPasswordTime: value = 0
[51]   lastLogoff: value = 0
[51]   lastLogon: value = 0
[51]   pwdLastSet: value = 132152610365026101
[51]   primaryGroupID: value = 513
[51]   objectSid: value = .....B...a5/ID.dW...
[51]   accountExpires: value = 9223372036854775807
[51]   logonCount: value = 0
[51]   sAMAccountName: value = Management-User
[51]   sAMAccountType: value = 805306368
[51]   userPrincipalName: value = Management-User@cisco.com
[51]   objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=cisco,DC=com
[51]   dSCorePropagationData: value = 20191011095056.0Z
[51]   dSCorePropagationData: value = 16010101000000.0Z
[51] Fiber exit Tx=553 bytes Rx=2688 bytes, status=1
[51] Session End
```

ةلص تاذا تامولعم

Cisco نم (TAC) ةينقتلا ةدعاسملا زكرمب لاصتالا ىجري، ةيفاضا ةدعاسم ىلع لوصحلل
[ملاعلا عاجنأ عيمج يف Cisco معد لاصتاتاهج](#): حلص معد دقع مزلي

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن م دخت س م ل ل م عد ي و ت ح م م ي دقت 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 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