

FDMによって管理されるFTDでのRAVPNのLDAP属性マップの構成

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[認証フロー](#)

[LDAP属性マップフローの説明](#)

[設定](#)

[FDMでの構成手順](#)

[LDAP属性マップの設定手順](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

はじめに

このドキュメントでは、Lightweight Directory Access Protocol(LDAP)サーバを使用してリモートアクセスVPN(RA VPN)ユーザを認証および許可し、LDAPサーバ上のグループメンバーシップに基づいて異なるネットワークアクセスをユーザに付与する手順について説明します。

前提条件

要件


- ファイアウォールデバイスマネージャ(FDM)でのRA VPN設定に関する基本的な知識
- FDMでのLDAPサーバ設定に関する基本的な知識
- REST(Representational State Transfer)アプリケーション・プログラム・インタフェース(API)およびFDM Rest APIエクスプローラの基礎知識
- FDMで管理されるCisco FTDバージョン6.5.0以降

使用するコンポーネント

次のハードウェアおよびソフトウェアバージョンのアプリケーション/デバイスが使用されました。

- Cisco FTDバージョン6.5.0、ビルド115
- Cisco AnyConnectバージョン4.10
- Microsoft Active Directory (AD) サーバ

- Postmanまたはその他のAPI開発ツール

 注：Microsoft AD Server and Postmalツールの設定サポートは、シスコから提供されません。

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、クリアな（デフォルト）設定で作業を開始しています。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。

認証フロー



LDAP属性マップフローの説明

1. ユーザはFTDへのリモートアクセスVPN接続を開始し、Active Directory(AD)アカウントにユーザ名とパスワードを提供します。
2. FTDがADサーバにポート389または636(LDAP over SSL)でLDAP要求を送信します
3. ADは、ユーザに関連付けられているすべての属性を使用してFTDに応答します。
4. FTDは、受信した属性値を、FTDで作成されたLDAP属性マップと照合します。これは許可プロセスです。
5. 次に、ユーザはLDAP属性マップのmemberOf属性に一致するグループポリシーの設定に接続し、継承します。

このドキュメントの目的に従い、AnyConnectユーザの許可はmemberOf LDAP属性を使用して行われます。

- 各ユーザのLDAPサーバのmemberOf属性は、FTDのldapValueエンティティにマッピングされます。ユーザが一致するADグループに属している場合、そのldapValueに関連付けられているグループポリシーがユーザに継承されます。
- ユーザのmemberOf属性値がFTDのldapValueエンティティのいずれとも一致しない場合、選択した接続プロファイルのデフォルトのグループポリシーが継承されます。この例では、NOACCESSグループポリシーがに継承されます。

設定

FDMによって管理されるFTDのLDAP属性マップは、REST APIを使用して設定されます。

FDMでの構成手順

ステップ 1 : デバイスがSmart Licensingに登録されていることを確認します。

The screenshot displays the Cisco Firepower Device Manager (FDM) interface for a Cisco ASA5545-X Threat Defense device. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: firepower'. The main content area shows a network diagram with 'Inside Network' and 'ISP/WAN/Gateway' connected to the device. Below the diagram, a grid of configuration tiles is visible. The 'Smart License' tile is highlighted with a red border and shows a 'Registered' status. Other tiles include 'Interfaces', 'Routing', 'Updates', 'System Settings', 'Backup and Restore', 'Troubleshoot', 'Site-to-Site VPN', 'Remote Access VPN', 'Advanced Configuration', and 'Device Administration'.

Category	Status	Action
Interfaces	Connected Enabled 3 of 9	View All Interfaces
Smart License	Registered	View Configuration
Site-to-Site VPN	1 connection	View Configuration

ステップ 2 : FDMでAnyConnectライセンスが有効になっていることを確認します。

Monitoring Policies Objects **Device: firepower** admin Administrator

Device Summary
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 **DISABLE**

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.

Includes: Intrusion Policy

Malware Disabled by user **ENABLE**

This License allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for Firepower and AMP Threat Grid. You must have this license to apply file policies that detect and block malware in files transmitted over your network.

Includes: File Policy

URL License Enabled **DISABLE**

This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.

Includes: URL Reputation

RA VPN License Enabled Type PLUS **DISABLE**

Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager does not support any of the advanced features covered by the Apex license.

Includes: RA-VPN

PERPETUAL LICENSES INCLUDED

Base License Enabled **ENABLED ALWAYS**

This perpetual license is included with the purchase of the system. You must have this license to configure and use the device. It covers all features not covered by subscription licenses.

Includes: Base Firewall Capabilities, Application Visibility and Control

ステップ 3 : トークンでエクスポート制御機能が有効になっていることを確認します。

Device Summary
Smart License

✔ **CONNECTED**
SUFFICIENT LICENSE

Assigned Virtual Account: ██████
Export-controlled features: Enabled
Go to [Cisco Smart Software Manager](#).

Last sync: 11 Oct 2019 09:33 AM
Next sync: 11 Oct 2019 09:43 AM

SUBSCRIPTION LICENSES INCLUDED

Threat

DISABLE

✔ Enabled

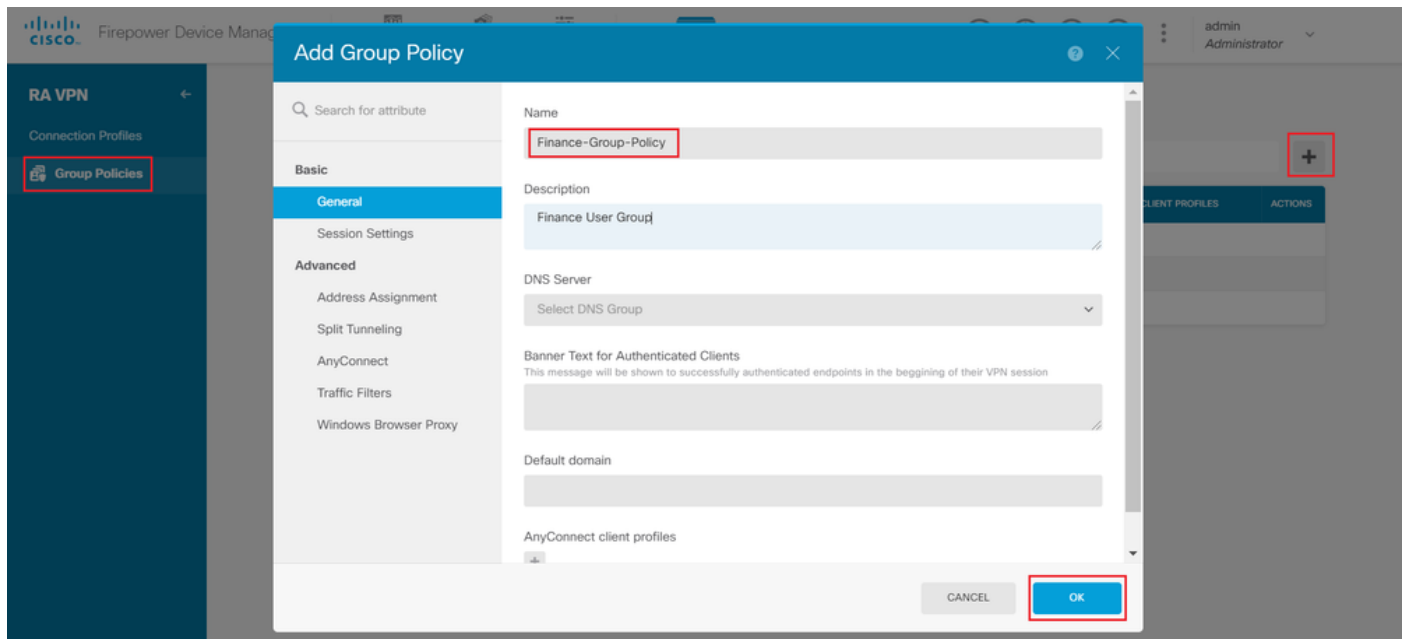
This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.

Includes: Intrusion Policy

注：このドキュメントでは、RA VPNがすでに設定されていることを前提としています。FDMによって管理されるFTDでRAVPNを設定する方法の詳細については、次のドキュメントを参照してください。

ステップ 4 : Remote Access VPN > Group Policiesの順に移動します。

ステップ 5 : Group Policiesに移動します。ADグループごとに異なるグループポリシーを設定するには、「+」をクリックします。この例では、グループポリシーFinance-Group-Policy、HR-Group-Policy、およびIT-Group-Policyが、異なるサブネットにアクセスできるように設定されています。



Finance-Group-Policyの設定は次のとおりです。

```
<#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>
```

同様に、HR-Group-Policyの設定は次のとおりです。

```
<#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>
```

最後に、IT-Group-Policyには次の設定があります。

```
<#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>
```

手順 6 : グループポリシーNOACCESSを作成し、Session Settingsに移動して、Simultaneous Login per Userオプションのチェックマークを外します。これにより、vpn-simultaneous-loginsの値が0に設定されます。

グループポリシーのvpn-simultaneous-logins値を0に設定すると、ユーザのVPN接続がただちに終了します。このメカニズムを使用して、設定済みグループ(この例ではFinance、HR、またはIT)以外のADユーザグループに属するユーザがFTDへの接続を正常に確立し、許可されたユーザグループアカウントだけに使用できるセキュアなリソースにアクセスすることを防止します。

正しいADユーザグループに属するユーザは、FTDのLDAP属性マップに一致し、マッピングされたグループポリシーを継承しますが、許可されたグループのいずれにも属さないユーザは、接続プロファイルのデフォルトのグループポリシー(この場合はNOACCESS)を継承します。

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: Unlimited minutes (1-4473924)

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

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

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

Simultaneous Login per User (1-2147483647; Default: 3)

CANCEL OK

NOACCESSグループポリシーの設定は次のとおりです。

<#root>

firepower#

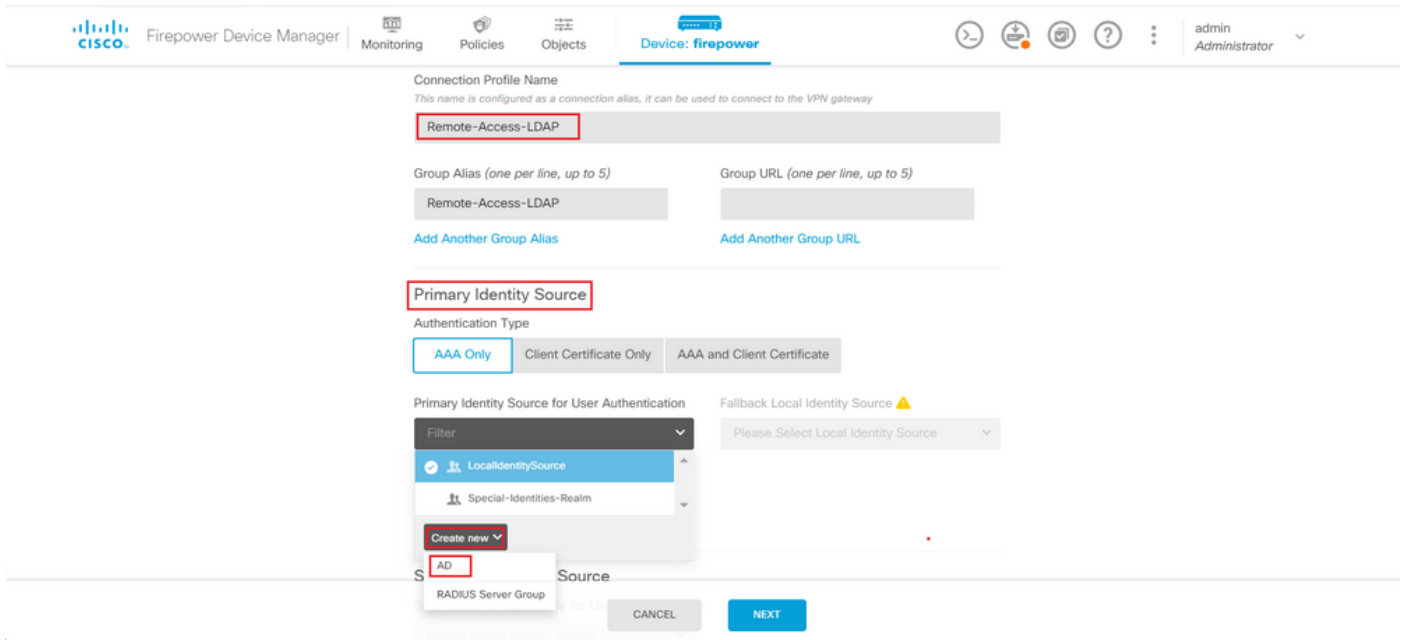
show run group-policy NOACCESS

```
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
```

手順 7 : Connection Profilesに移動し、Connection-Profileを作成します。この例では、プロファイル名はRemote-Access-LDAPです。Primary Identity Source AAA Onlyを選択し、新しい認証サーバタイプADを作成します。



ADサーバの情報を入力します。

- ディレクトリユーザ名
- ディレクトリパスワード
- ベース DN
- ADプライマリドメイン
- ホスト名/IPアドレス
- ポート
- 暗号化タイプ

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

Nextをクリックし、この接続プロファイルのデフォルトのグループポリシーとしてNOACCESSを選択します。

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
- HR-Group-Policy
- IT-Group-Policy
- NOACCESS
- SSLVPN

Create new Group Policy

BACK NEXT

Maximum Connection Time / Alert Interval Unlimited / 1 Minutes

すべての変更を保存します。これで、接続プロファイルRemote-Access-LDAPがRA VPN設定に表示されるようになります。

RA VPN

Connection Profiles

Group Policies

Device Summary

Remote Access VPN Connection Profiles

1 object

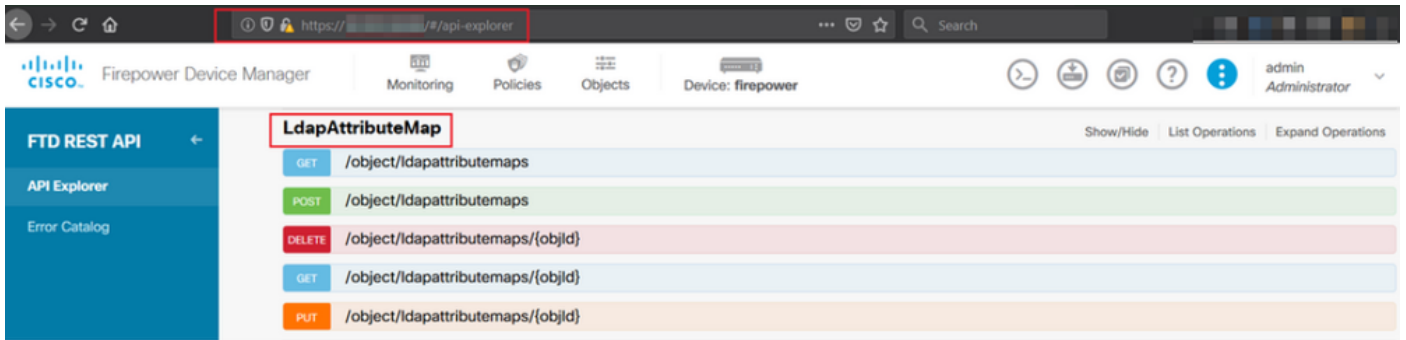
#	NAME	AAA	GROUP POLICY	ACTIONS
1	Remote-Access-LDAP	Authentication: AAA Only Authorization: None Accounting: None	NOACCESS	


LDAP属性マップの設定手順

ステップ 1 : FTDのAPI Explorerを起動します。

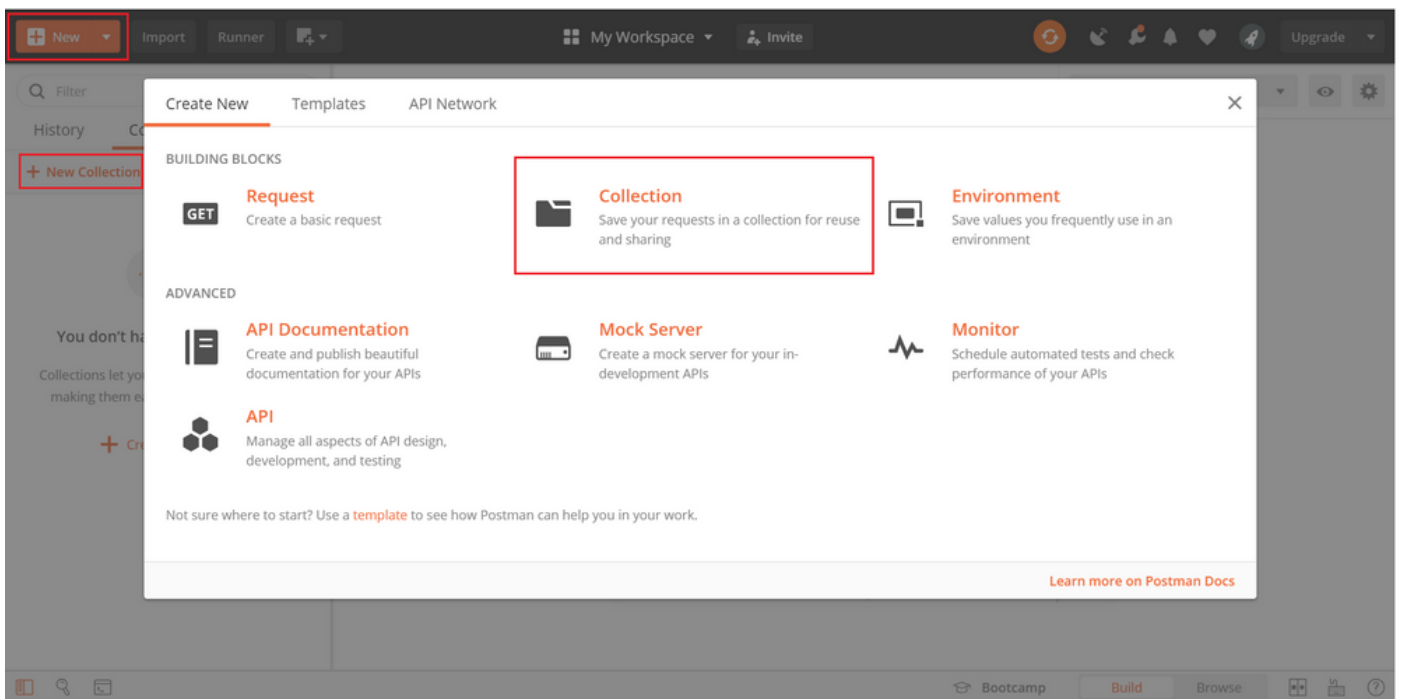
APIエクスプローラには、FTDで使用可能なAPIの全リストが含まれています。https://<FTD Management IP>/api-explorerに移動します。

LdapAttributeMapセクションまでスクロールダウンして、このセクションをクリックすると、サポートされているすべてのオプションが表示されます。

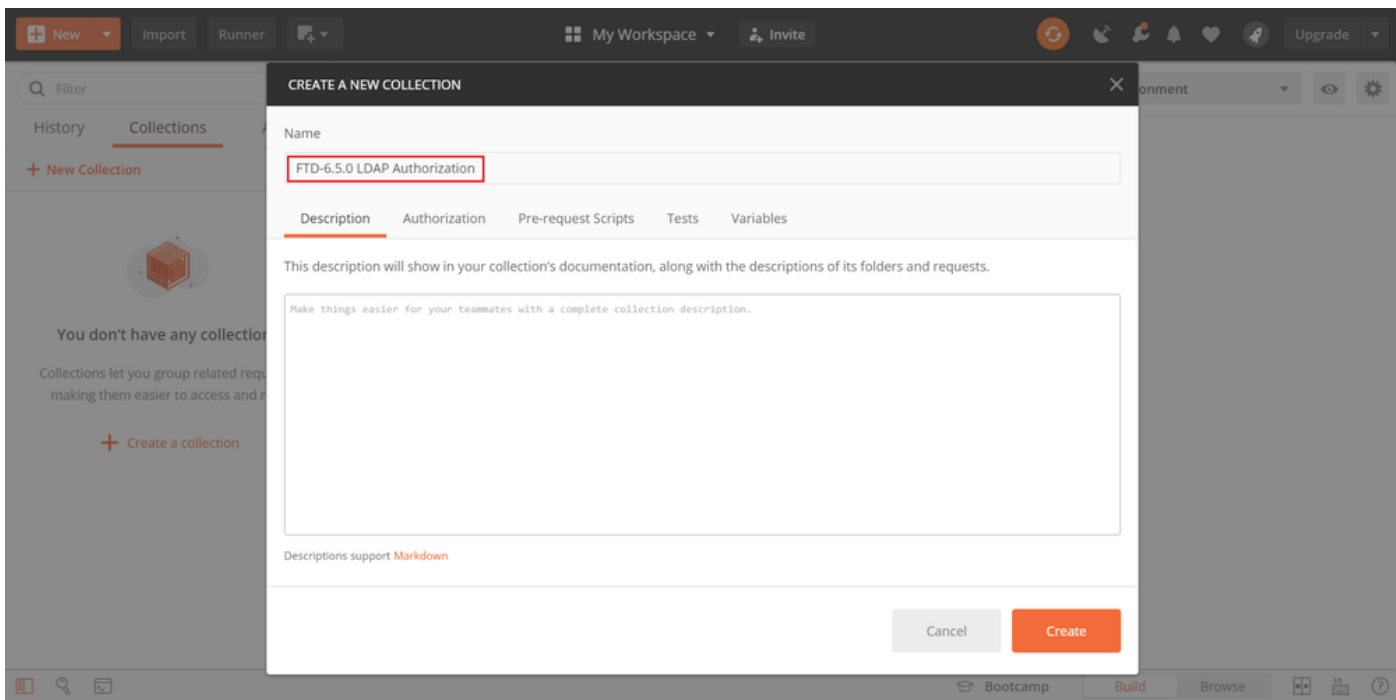


 注：この例では、LDAP属性マップを設定するためのAPIツールとしてPostmanを使用します。

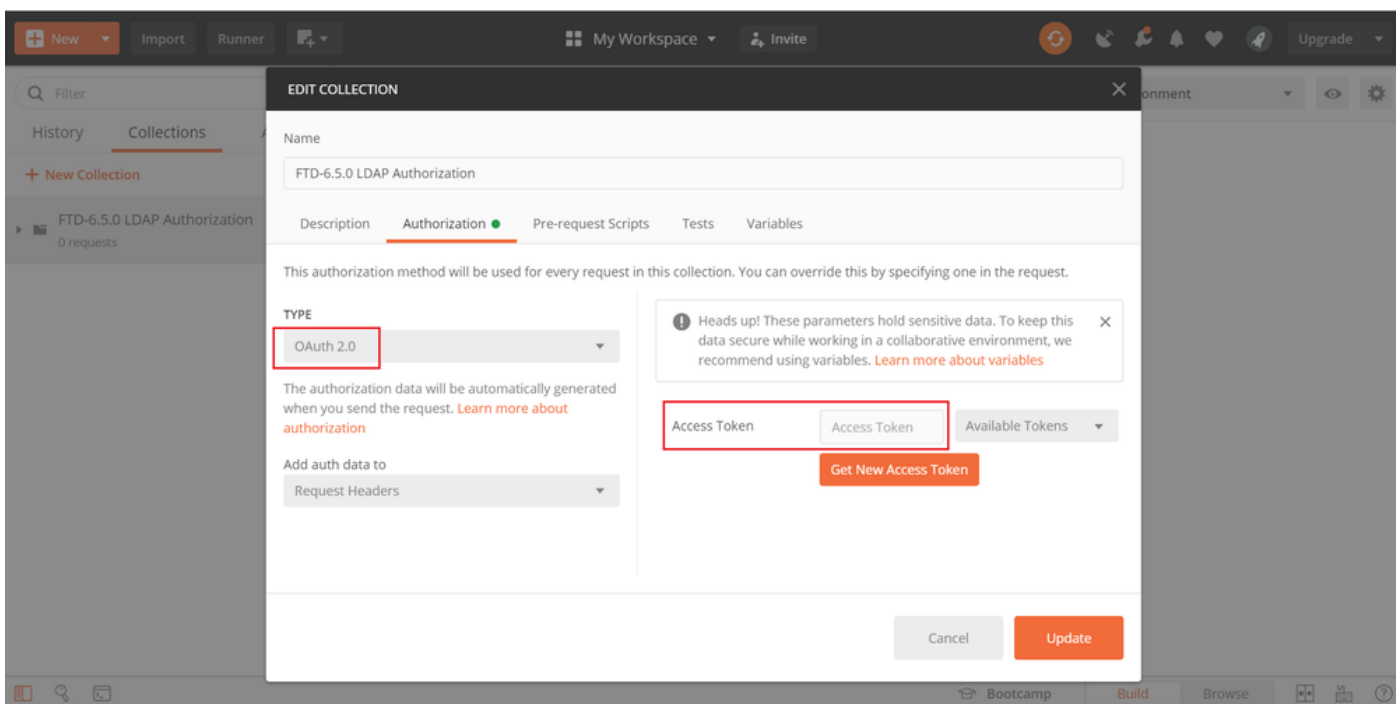
ステップ 2：LDAP許可用のPostmanコレクションを追加します。



このコレクションの名前を入力します。



を編集します 許可 tabキーを押して選択します タイプ OAuth 2.0



手順3: API要求をFTDに送信するときにSSLハンドシェイクの失敗を回避するには、File > Settingsの順に移動し、SSL証明書検証をオフにします。これは、FTDが自己署名証明書を使用する場合に実行されます。



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

または、FTDで使用される証明書をCA証明書として設定の証明書セクションに追加できます。

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.](#)

ステップ 4：新しいPOST要求Authを追加してFTDにログインPOST要求を作成し、トークンがPOST/GET要求を承認できるようにします。

+ 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

Accept application/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

その他のすべてのリクエストについては、それぞれのヘッダータブに移動し、REST APIリクエストでプライマリデータタイプとしてjsonを使用するために、このプリセットヘッダー値Header-LDAPを選択します。

トークンを取得するためのPOST要求の本文には、次の内容が含まれている必要があります。

Type	raw:JSON(application/json)
grant_type (認可タイプ)	password
username	FTDにログインするための管理者ユーザ名
password	管理者ユーザアカウントに関連付けられたパスワード

```
{  
  "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 }
```

sendをクリックすると、応答の本文に、FTDにPUT/GET/POST要求を送信するために使用されるアクセストークンが含まれます。

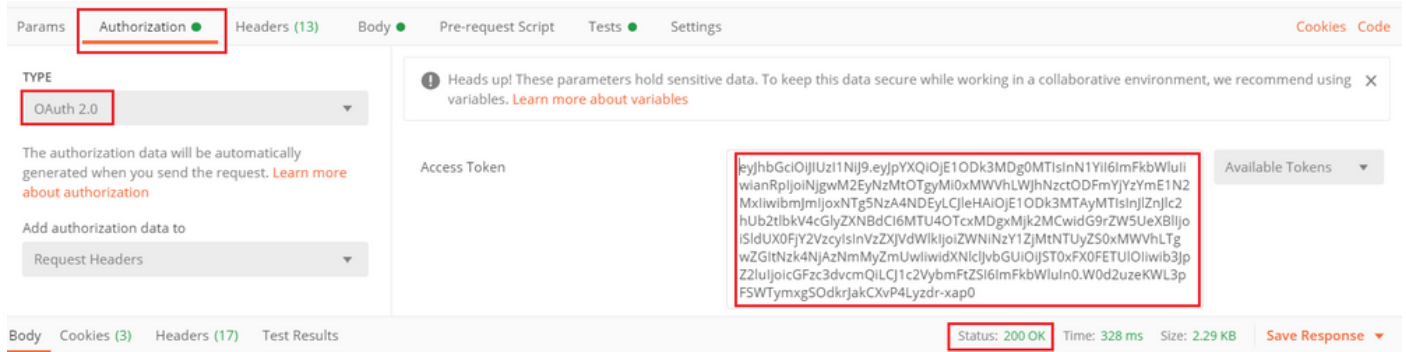


```
{
  "access_token": "eyJhbGciOiJIUzI1IiwiaXN0IjoiOiJkaXJlbnR5dXN0IiwiaWF0IjoiIj09d29zeKwL3pFShTymxgS0dkrJakCXvP4Lyzdr-xap0",
  "expires_in": 1800,
  "token_type": "Bearer",
  "refresh_token": "eyJhbGciOiJIUzI1IiwiaXN0IjoiOiJkaXJlbnR5dXN0IiwiaWF0IjoiIj09d29zeKwL3pFShTymxgS0dkrJakCXvP4Lyzdr-xap0",
  "refresh_expires_in": 2400
}
```

このトークンは、後続のすべての要求を承認するために使用されます。

すべての新しい要求のAuthorizationタブに移動し、次のいずれかを選択します。

Type	OAuth 2.0
トークン	ログインPOST要求の実行によって受信されたアクセストークン



ステップ 5 : 新しいGET要求Get Group-Policiesを追加して、グループポリシーのステータスと設定を取得します。次のステップで使用する、設定済みの各グループポリシー(この例ではFinance-Group-Policy、HR-Group-Policy、およびIT-Group-Policy)の名前とIDを収集します。

設定済みのグループポリシーを取得するURLは、<https://<FTD Management IP>/api/fdm/latest/object/ravpngroupolicies>です。

次の例では、Group-Policy Finance-Group-Policyが強調表示されています。

```
+ New Collection  Trash GET https://.../api/fdm/latest/object/ravprgrouppolicies Send
FTD-6.5.0 LDAP Authorization 2 requests Status: 200 OK Time: 129 ms Size: 10.82 KB Save
POST Auth
GET Get Group-Policies

58 {
59   "version": "26dc1b32p",
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   "scpfForwardingUrl": null,
86   "periodicClientCertAuthenticationInterval": 1,
87   "enableDTLS": false,
88   "enableDTLSCompression": false,
89   "sslCompression": "DISABLED",
90   "enableSSLrekey": false,
91   "rekeyMethod": "NEH_TUNNEL",
92   "rekeyInterval": 4,
93   "ignoreDFBit": false,
94   "bypassUnsupportedProtocol": false,
95   "mtuSize": 1400,
96   "useAlwaysOnVPNSettingInProfile": true,
97   "enableKeepAliveMessages": false,
98   "keepAliveMessageInterval": 30,
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": "ravprgrouppolicy",
120  "links": {
121    "self": "https://.../api/fdm/latest/object/ravprgrouppolicies/a5722b15-9836-11ea-ba77-6916f09acebc"
122  }
123 }
```

手順 6 : 新しいPOST要求Create LDAP Attribute Mapを追加して、LDAP Attribute Mapを作成します。このドキュメントでは、モデルLdapAttributeMappingを使用します。他のモデルにも、アトリビュートマップを作成するための同様の操作とメソッドがあります。これらのモデルの例は、このドキュメントで前述したようにapi-explorerで入手できます。

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.

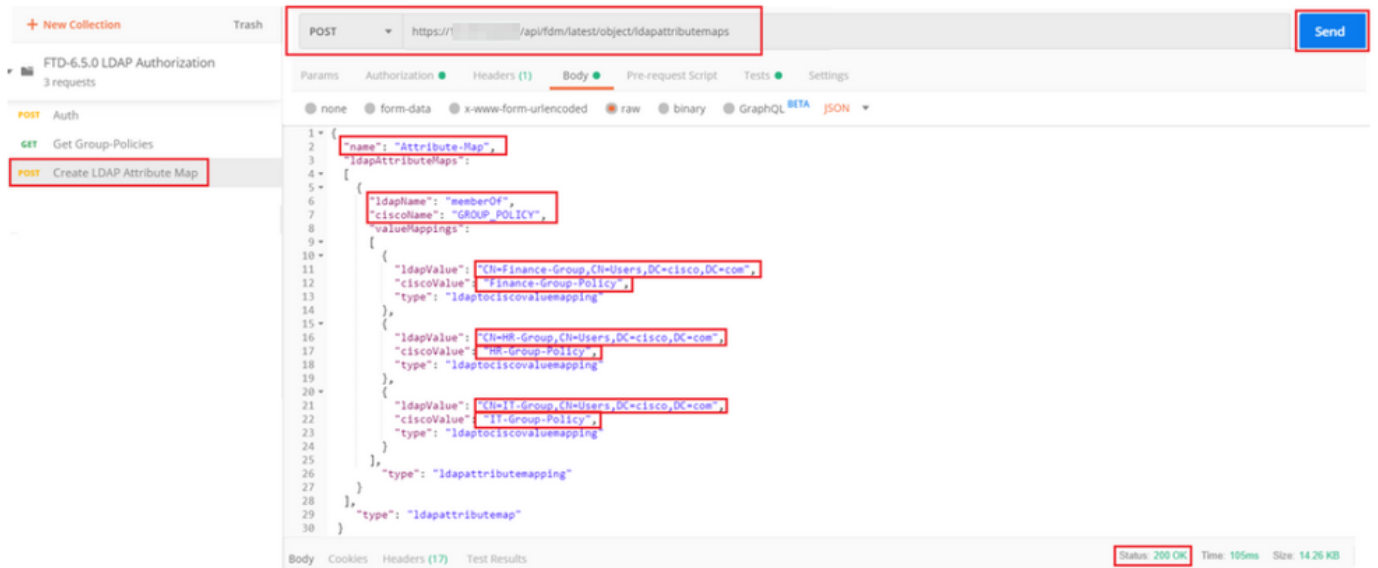
Response Class (Status 200)

Model	Example Value
<p>LdapAttributeMapping</p> <p><i>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.)</i></p> <p>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),</p> <p>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)</p> <p>= ['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'],</p> <p>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),</p> <p>type (string): ldapattributemapping</p>	
<p>LdapAttributeToGroupPolicyMapping</p> <p><i>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.)</i></p> <p>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),</p> <p>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),</p> <p>type (string): ldapattributetogrouppolicymapping</p>	

LDAP属性マップをPOSTするURLは、<https://<FTD Management IP>/api/fdm/latest/object/ldapattributemaps>です。


POST要求の本文には、次の情報が含まれている必要があります。

name	LDAP属性マップの名前
種類	ldapattributemapping
ldapName	memberOf
シスコ名	GROUP_POLICY (グループポリシー)
ldap値	ADからのユーザのmemberOf値
シスコの値	FTDでの各ユーザー・グループのグループ・ポリシー名

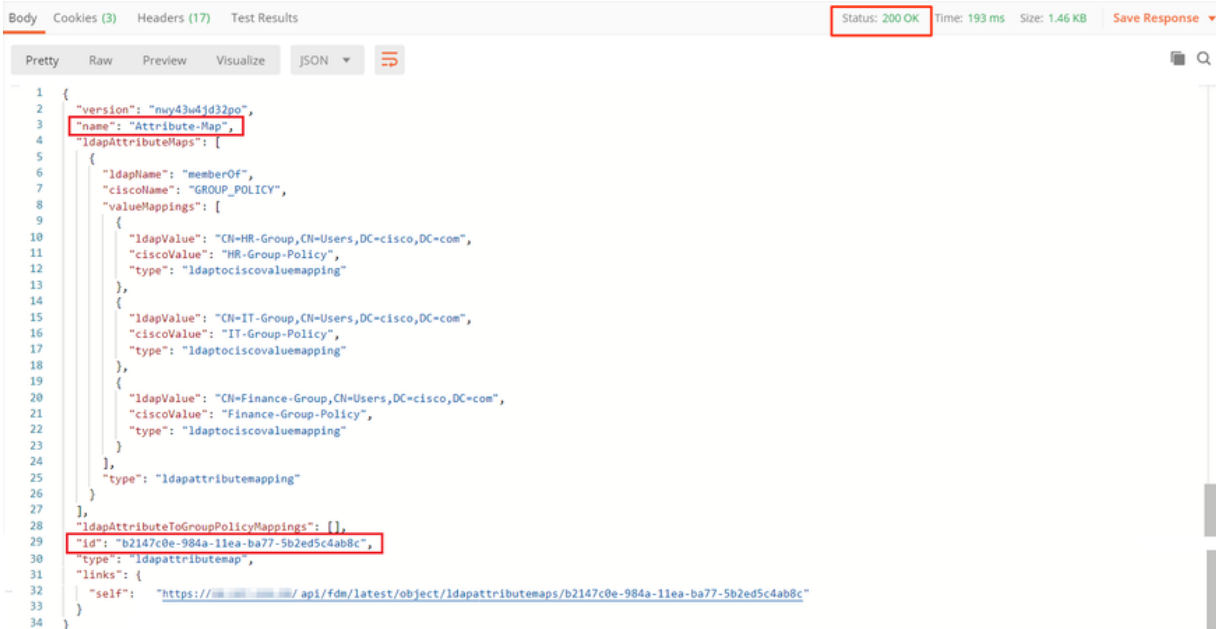


POST要求の本文には、memberOf値に基づいて特定のグループポリシーをADグループにマッピングするLDAP属性マップ情報が含まれています。

```
{
  "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"
  ]
}
```

 注：memberOfフィールドは、dsqueryコマンドを使用してADサーバから取得するか、FTDのLDAPデバッグからフェッチできます。デバッグログで、memberOf value:フィールドを探します。

このPOST要求の応答は、次の出力のようになります。



```
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 }
```

手順 7：FDMで現在のADレルム構成を取得するための新しいGET要求を追加します。

現在のADレルム設定を取得するURLは、<https://<FTD Management IP>/api/fdm/latest/object/realms>です。


```

1 {
2   "items": [
3     {
4       "version": "ksj3d8e5ixyy",
5       "name": "LDAP-AD",
6       "directoryConfigurations": [
7         {
8           "hostname": "...",
9           "port": 389,
10          "encryptionProtocol": "NONE",
11          "encryptionCert": null,
12          "type": "directoryconfiguration"
13        }
14      ],
15      "enabled": true,
16      "systemDefined": false,
17      "realmId": 3,
18      "dirUsername": "administrator@...",
19      "dirPassword": "*****",
20      "baseDN": "dc=...,dc=com",
21      "ldapAttributeMap": null,
22      "adPrimaryDomain": "...",
23      "id": "bf50a8ab-9819-11ea-ba77-d32ecc224295",
24      "type": "activedirectoryrealm",
25      "links": {
26        "self": "https://.../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 }

```

キーldapAttributeMapの値がnullであることに注意してください。

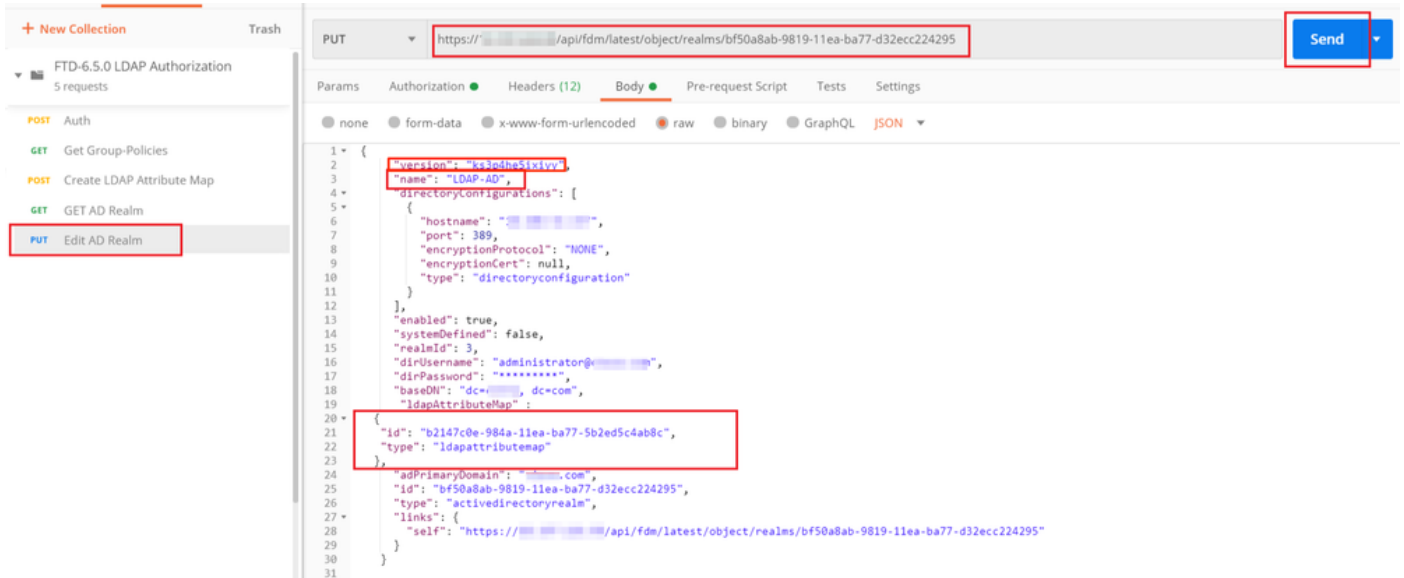
ステップ 8 : ADレルムを編集するための新しいPUT要求を作成します。前のステップで出力したGET応答をコピーして、この新しいPUT要求の本文に追加します。この手順を使用して、現在のADレルムの設定を変更できます。たとえば、パスワード、IPアドレスを変更したり、この場合のldapAttributeMapなどの任意のキーに新しい値を追加したりできます。

 **注意** : GET応答の出力全体ではなく、項目リストの内容をコピーすることが重要です。PUT要求の要求URLには、変更を行うオブジェクトの項目IDを追加する必要があります。この例では、値はbf50a8ab-9819-11ea-ba77-d32ecc224295です。

現在のADレルム設定を編集するURLは、<https://<FTD Management IP>/api/fdm/latest/object/realms/<realm ID>>です。

PUT要求の本文には、次のものが含まれている必要があります。

version	以前のGET要求の応答から取得されたバージョン
[id]	前のGET要求の応答から取得されたID
ldapAttributeMap	LDAP属性マップの作成要求の応答からのLDAP-ID



この例の設定の本文は次のとおりです。

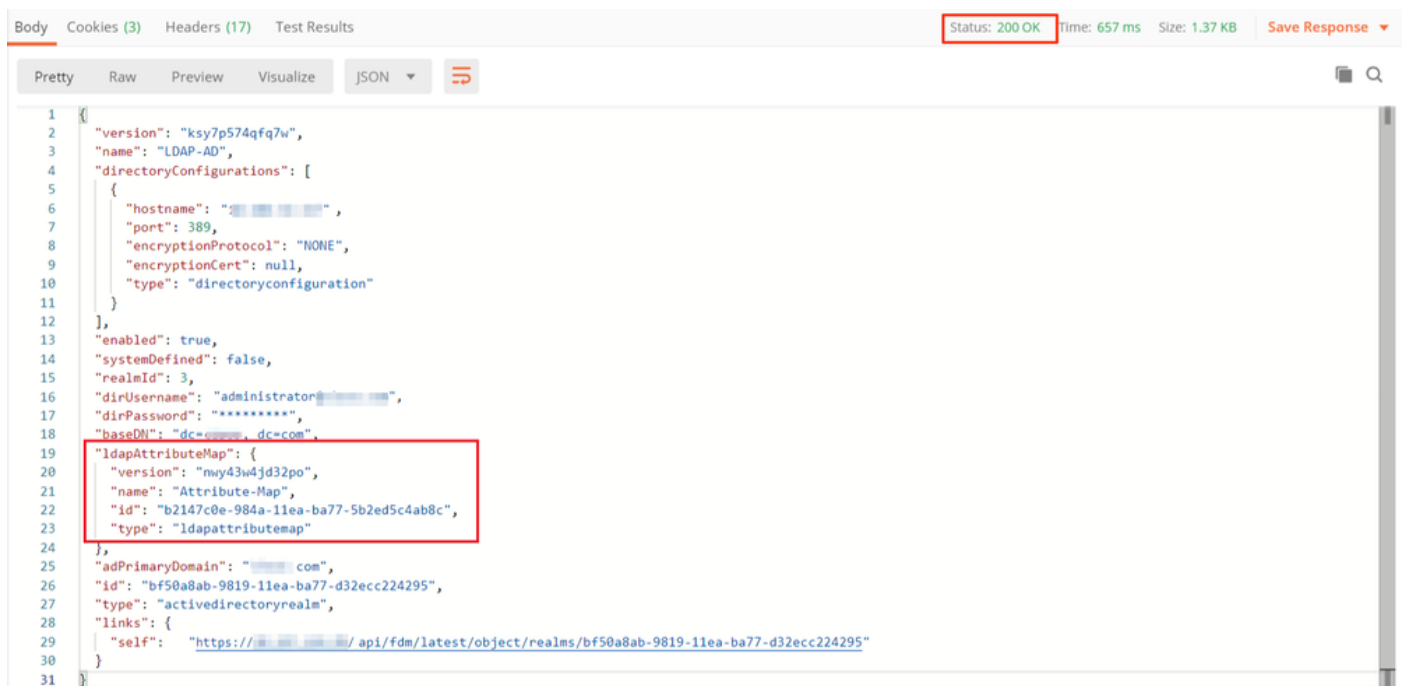
<#root>

```
{
  "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"
```

```
}  
}
```

この要求の応答本文のldapAttributeMap idが一致することを確認します。



```
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": "ksy7p574qfq7w",  
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 }
```


(オプション)。LDAP属性マップは、PUT要求を使用して変更できます。新しいPUT要求Edit Attribute-Mapを作成し、Attribute-Mapの名前やmemberOf値などの変更を行います。T

次の例では、3つすべてのグループについて、ldapvalueの値がCN=UsersからCN=UserGroupに変更されています。

```
1 {"description": "memberOf",
2 "name": "memberOf-map",
3 "ldapattributemaps":
4 {
5   [
6     {
7       "ldapname": "memberOf",
8       "ciscovalue": "group-policy",
9       "valuemappings":
10      [
11        [
12          {
13            "ldapvalue": "CiscoFinance-Group_CiscoGroup_OC=cisco_OC=com",
14            "ciscovalue": "Finance-Group-POLICY",
15            "type": "ldapciscovaluemapping"
16          }
17        ],
18        [
19          {
20            "ldapvalue": "CiscoHR-Group_CiscoGroup_OC=cisco_OC=com",
21            "ciscovalue": "HR-Group-POLICY",
22            "type": "ldapciscovaluemapping"
23          }
24        ],
25        [
26          {
27            "ldapvalue": "CiscoIT-Group_CiscoGroup_OC=cisco_OC=com",
28            "ciscovalue": "IT-Group-POLICY",
29            "type": "ldapciscovaluemapping"
30          }
31        ]
32      ]
33    }
34  ]
35 }
36
37 {"id": "021470e-904a-11ea-ba77-5b2ed5c4a8dc",
38 "type": "ldapattributemap",
39 "links": {
40   "self": "https://18.197.224.99/api/fdm/latest/object/ldapattributemaps/021470e-904a-11ea-ba77-5b2ed5c4a8dc"
41 }
42 }
```

(オプション)。既存のLDAP属性マップを削除するには、DELETE要求のDelete Attribute-Mapを作成します。前のHTTP応答のmap-idを含め、削除要求のベースURLを付加します。

```
DELETE https://18.197.224.99/api/fdm/latest/object/ldapattributemaps/021470e-904a-11ea-ba77-5b2ed5c4a8dc
```

 注：memberOf属性にスペースが含まれている場合、Webサーバで解析するにはURLでエンコードする必要があります。それ以外の場合は、400 Bad Request HTTP Responseが受信されます。空白文字を含む文字列の場合、このエラーを回避するには%20または+を使用できます。

ステップ 9：FDMに戻り、「配置」アイコンを選択して「今すぐ配置」をクリックします。

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

Deployed Version	Pending Version
Active Directory Realm Edited: LDAP-AD	
ldapAttributeMap:	
-	Attribute-Map

MORE ACTIONS ▾ CANCEL DEPLOY NOW ▾

確認

配置の変更は、FDMの「配置履歴」セクションで確認できます。

Device Administration

Audit Log

Download Configuration

Deployment Completed: User (admin) Triggered Deployment

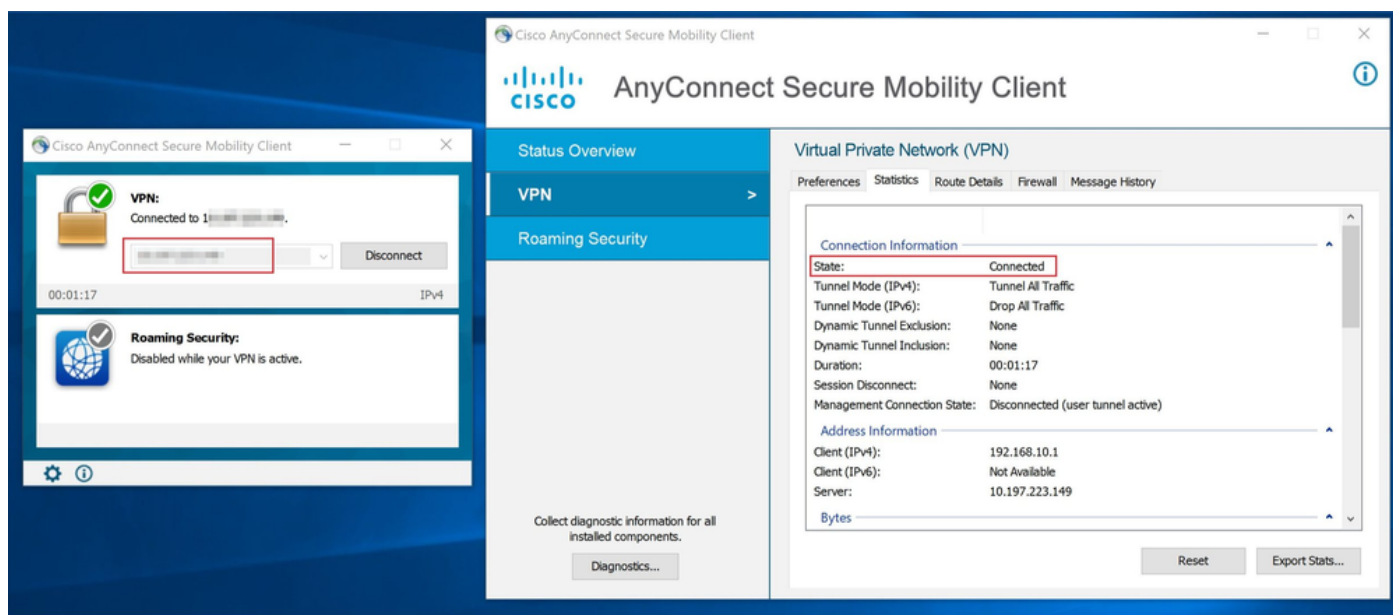
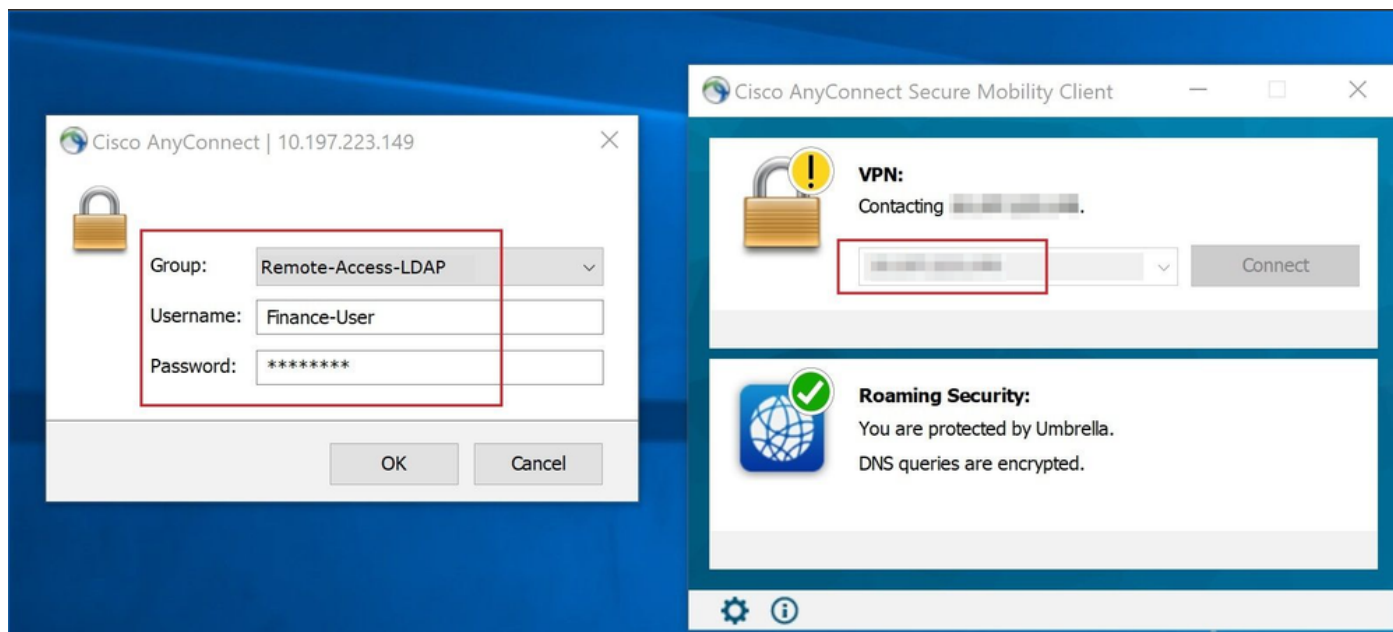
Summary Differences View

Deployed Version	Pending Version
Idapattributemap Added: Attribute-Map	
Entity ID: b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c	
-	ldapAttributeMaps[0].ldapName: memberOf
-	ldapAttributeMaps[0].valueMappings[0].ldapValue: CN=Finan...
-	ldapAttributeMaps[0].valueMappings[0].ciscoValue: Finance...
-	ldapAttributeMaps[0].valueMappings[1].ldapValue: CN=IT-Gr...
-	ldapAttributeMaps[0].valueMappings[1].ciscoValue: IT-Grou...
-	ldapAttributeMaps[0].valueMappings[2].ldapValue: CN=HR-Gr...
-	ldapAttributeMaps[0].valueMappings[2].ciscoValue: HR-Grou...
-	ldapAttributeMaps[0].ciscoName: GROUP_POLICY
-	name: Attribute-Map

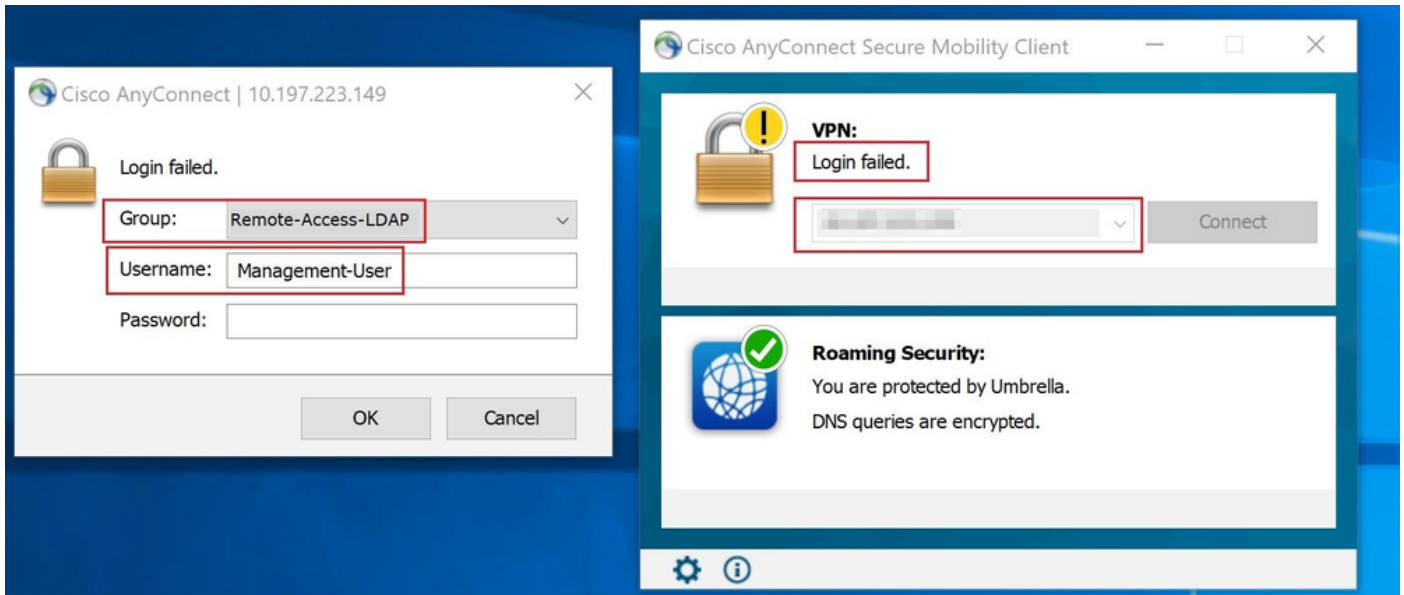
Deployed Version	Pending Version
Active Directory Realm Edited: LDAP-AD	
Entity ID: b5f9a8ab-9819-11ea-ba77-d32ecc224295	
ldapAttributeMap:	
-	Attribute-Map

この設定をテストするには、UsernameフィールドとPasswordフィールドにADクレデンシャルを入力します。

ADグループFinance-Groupに属するユーザがログインを試みると、期待どおりにログイン試行が成功します。



ADのManagement-Groupに属するユーザがConnection-Profile Remote-Access-LDAPに接続しようとする時、一致するLDAP属性マップが返されないため、このユーザがFTDで継承するグループポリシーは、vpn-simultaneous-loginsの値が0に設定されているNOACCESSです。したがって、このユーザに対するログイン試行は失敗します。



設定は、FTD CLIから次のshowコマンドを使用して確認できます。

```
<#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 : 000000000001a0005da1b5a3
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
```

トラブルシューティング

REST APIの設定に関する最も一般的な問題の1つは、ベアラートークンを適宜更新することです。トークンの有効期限は、認証要求の応答で指定されます。この時間が経過すると、追加の更新トークンをより長く使用できます。更新トークンも期限切れになると、新しいアクセストークンを取得するために新しい認証要求を送信する必要があります。

 注：debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

 さまざまなデバッグレベルを設定できます。デフォルトでは、レベル 1 が使用されます。デバッグレベルを変更すると、デバッグの冗長性が高くなる場合があります。特に実稼働環境では、注意して実行してください。

LDAP属性マップに関連する問題のトラブルシューティングには、FTD CLIでの次のデバッグが役立ちます

```
debug ldap 255
debug webvpn condition user <username>
debug webvpn anyconnect 255
debug aaa common 127
```

この例では、前に説明したテストユーザが接続したときにADサーバから受信した情報を示すために、次のデバッグが収集されました。

Finance-UserのLDAPデバッグ

<#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
```

Management-UserのLDAPデバッグ

<#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
```

関連情報

詳細については、Cisco Technical Assistance Center(TAC)にお問い合わせください。有効なサポート契約が必要です。 [各国のシスコ サポートの連絡先](#)。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。