

# 为FDM管理的FTD上的RAVPN配置LDAP属性映射

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[身份验证流程](#)

[LDAP属性映射流说明](#)

[配置](#)

[FDM的配置步骤](#)

[LDAP属性映射的配置步骤](#)

[验证](#)

[故障排除](#)

[相关信息](#)

---

## 简介

本文档介绍使用轻量级目录访问协议(LDAP)服务器对远程访问VPN(RA VPN)用户进行身份验证和授权，并根据用户在LDAP服务器上的组成员资格授予他们不同的网络访问权限的过程。

## 先决条件

### 要求

- 防火墙设备管理器(FDM)上的RA VPN配置基础知识
- 基本了解FDM上的LDAP服务器配置
- 演示状态传输(REST)应用程序接口(API)和FDM Rest API资源管理器的基础知识
- 由FDM管理的Cisco FTD 6.5.0版或更高版本

### 使用的组件

使用了以下应用程序/设备的硬件和软件版本：

- Cisco FTD版本6.5.0，内部版本115
- Cisco AnyConnect版本4.10
- Microsoft Active Directory(AD)服务器
- Postman或任何其他API开发工具



注意：思科不提供对Microsoft AD服务器和Postmal工具的配置支持。

---

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 身份验证流程



### LDAP属性映射流说明

1. 用户启动到FTD的远程访问VPN连接，并为其Active Directory(AD)帐户提供用户名和密码。
2. FTD通过端口389或636 ( SSL上的LDAP ) 向AD服务器发送LDAP请求
3. AD使用与用户相关联的所有属性回响应FTD。
4. FTD将收到的属性值与在FTD中创建的LDAP属性映射相匹配。这是授权过程。
5. 然后，用户从与LDAP属性映射中的memberOf属性匹配的组策略连接和继承设置。

在本文档中，AnyConnect用户的授权是使用memberOf LDAP属性完成。

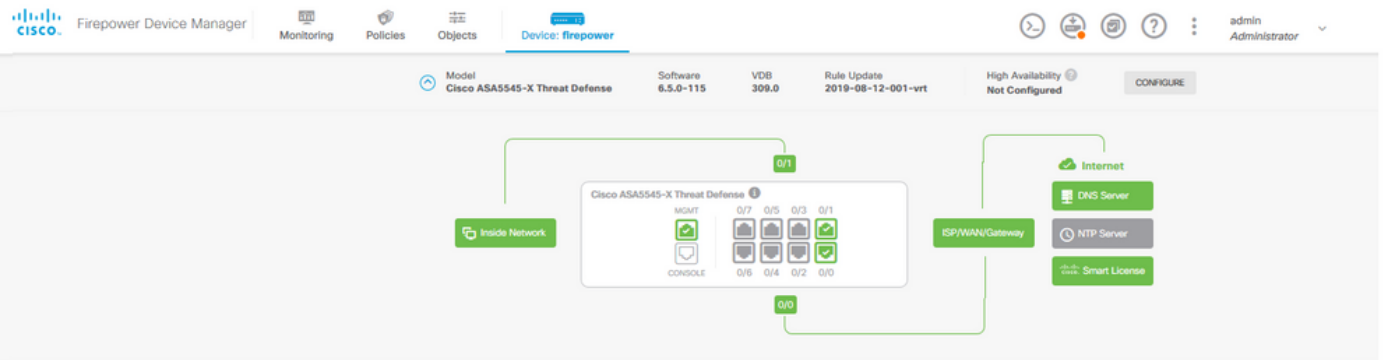
- 每个用户的LDAP服务器中的memberOf属性映射到FTD上的ldapValue实体。如果用户属于匹配的AD组，则用户将继承与该ldapValue关联的组策略。
- 如果用户的memberOf属性值与FTD上的任何ldapValue实体不匹配，则会继承所选连接配置文件的默认Group-Policy。在本示例中，NOACCESS Group-Policy继承到。

## 配置

FDM管理的FTD的LDAP属性映射配置有REST API。

### FDM的配置步骤

步骤1:验证设备是否已注册到智能许可。



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

第二步：验证FDM上是否启用了AnyConnect许可证。

**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**

<b>Threat</b> 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	<b>Malware</b> Disabled by user 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
<b>URL License</b> Enabled 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	<b>RA VPN License</b> Type: PLUS Enabled 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**

<b>Base License</b> 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
---

第三步：验证令牌中的导出控制功能是否已启用。

Device Summary  
Smart License

CONNECTED  
SUFFICIENT LICENSE

Assigned Virtual Account: [redacted]  
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

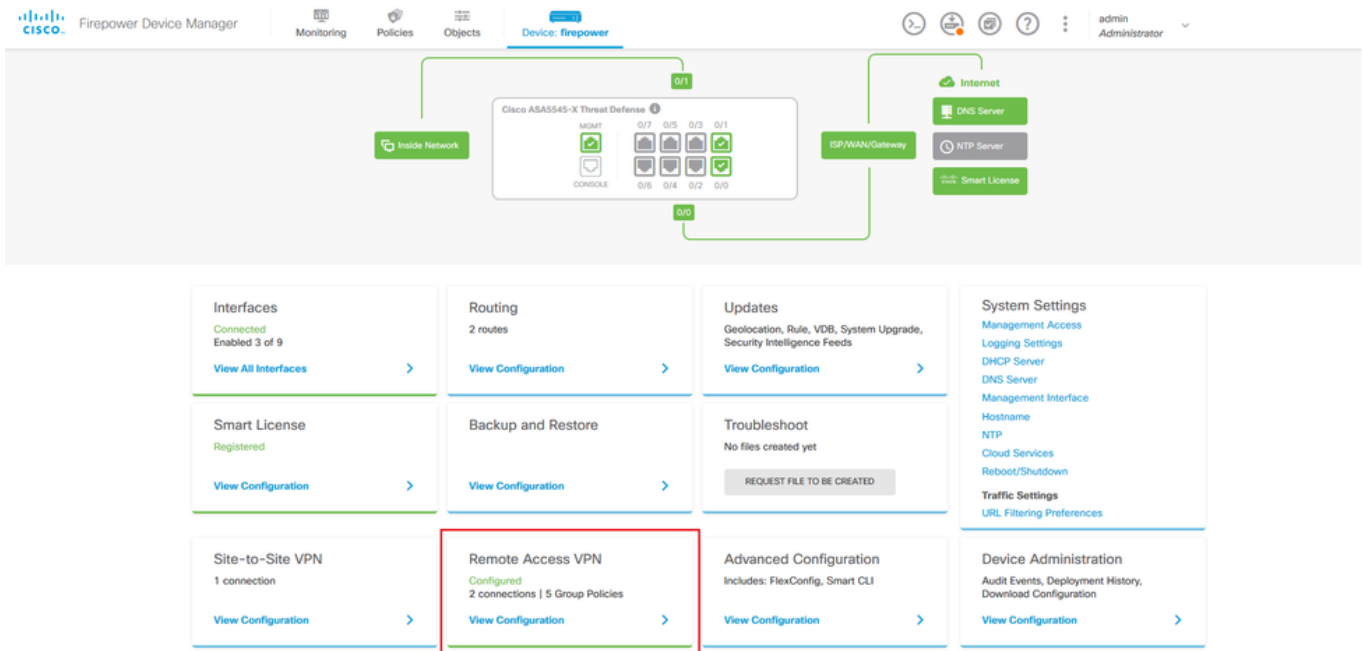
Enabled

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.

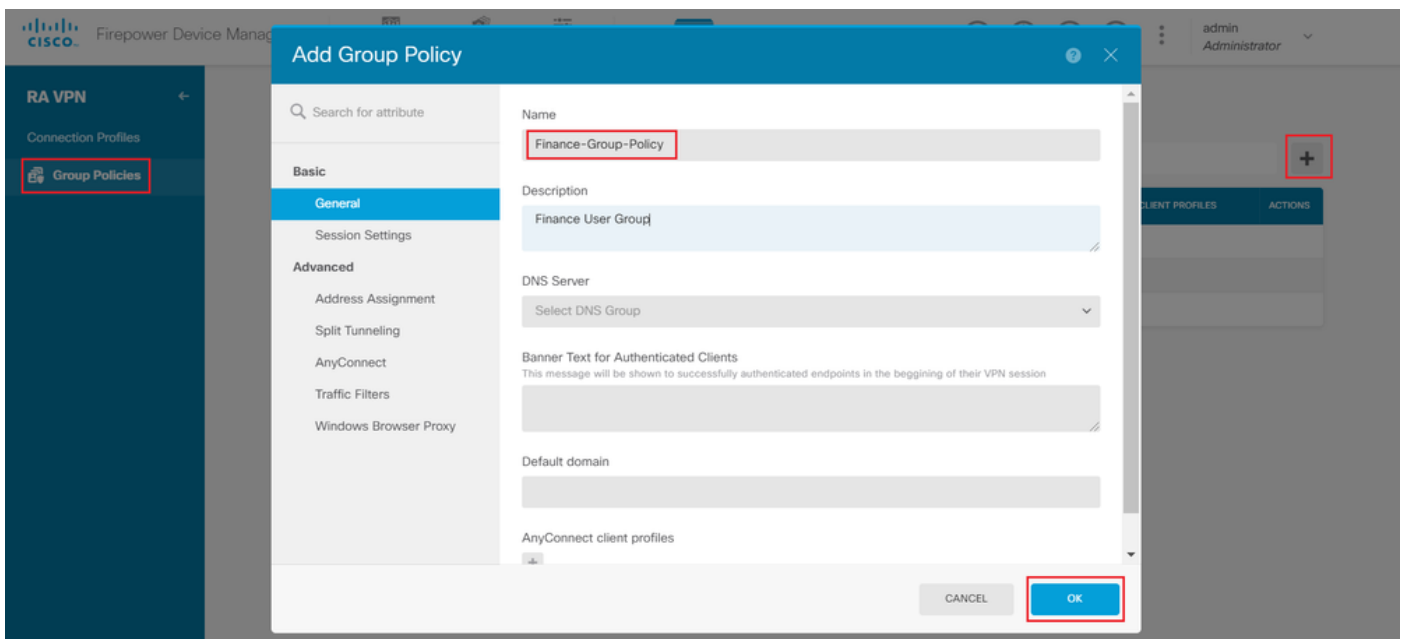
Includes: Intrusion Policy

注意：本文档假设RA VPN已配置。有关如何在FDM管理的FTD上配置RAVPN的详细信息，请参阅以下文档。

第四步：导航到Remote Access VPN > Group Policies。



第五步：导航到组策略。点击“+”为每个AD组配置不同的组策略。在本例中，将组策略Finance-Group-Policy、HR-Group-Policy和IT-Group-Policy配置为可以访问不同的子网。



Finance-Group-Policy具有以下设置：

```
<#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>
```

同样，HR-Group-Policy有以下设置：

```
<#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>

最后，IT-Group-Policy有以下设置：

<#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>
```

第六步：创建组策略NOACCESS并导航到会话设置，然后取消选中Simultaneous Login per User选项。这会将vpn-simultaneous-logins值设置为0。

设置为0时，Group-Policy中的vpn-simultaneous-logins值将立即终止用户的VPN连接。此机制用于防止属于除已配置用户组以外的任何AD用户组的用户（在本示例中为Finance、HR或IT）成功建立到FTD的连接，并访问仅可用于允许的用户组帐户的安全资源。

属于正确AD用户组的用户匹配FTD上的LDAP属性映射并继承映射的组策略，而不属于任何允许组的用户则继承连接配置文件的默认组策略，在本例中为NOACCESS。

## 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组策略具有以下设置：



```
<#root>
```

```
firepower#
```

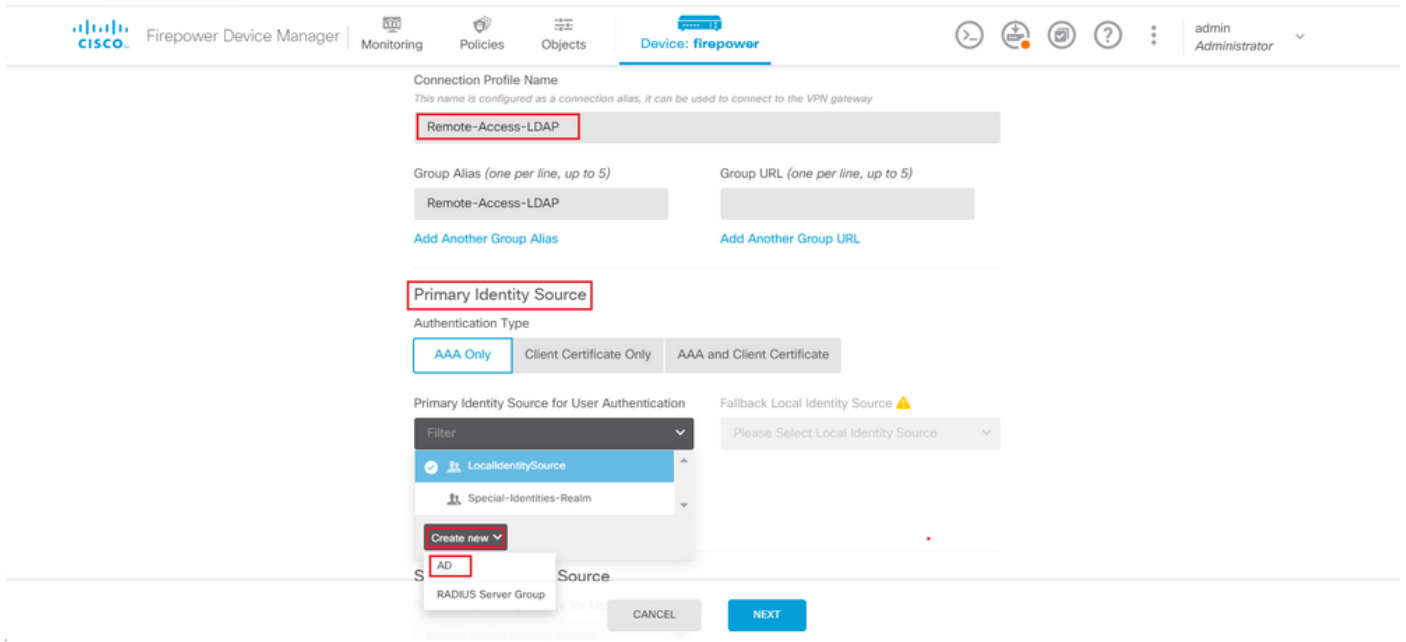
```
show run group-policy NOACCESS
```

```
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
```

步骤 7. 导航到连接配置文件并创建连接配置文件。在本示例中，配置文件名称为Remote-Access-LDAP。选择Primary Identity Source AAA Only，然后创建新的身份验证服务器类型AD。



输入AD服务器的信息：

- 目录用户名
- 目录密码
- 基准 DN
- AD主域
- 主机名/IP地址
- 端口
- 加密类型

# 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

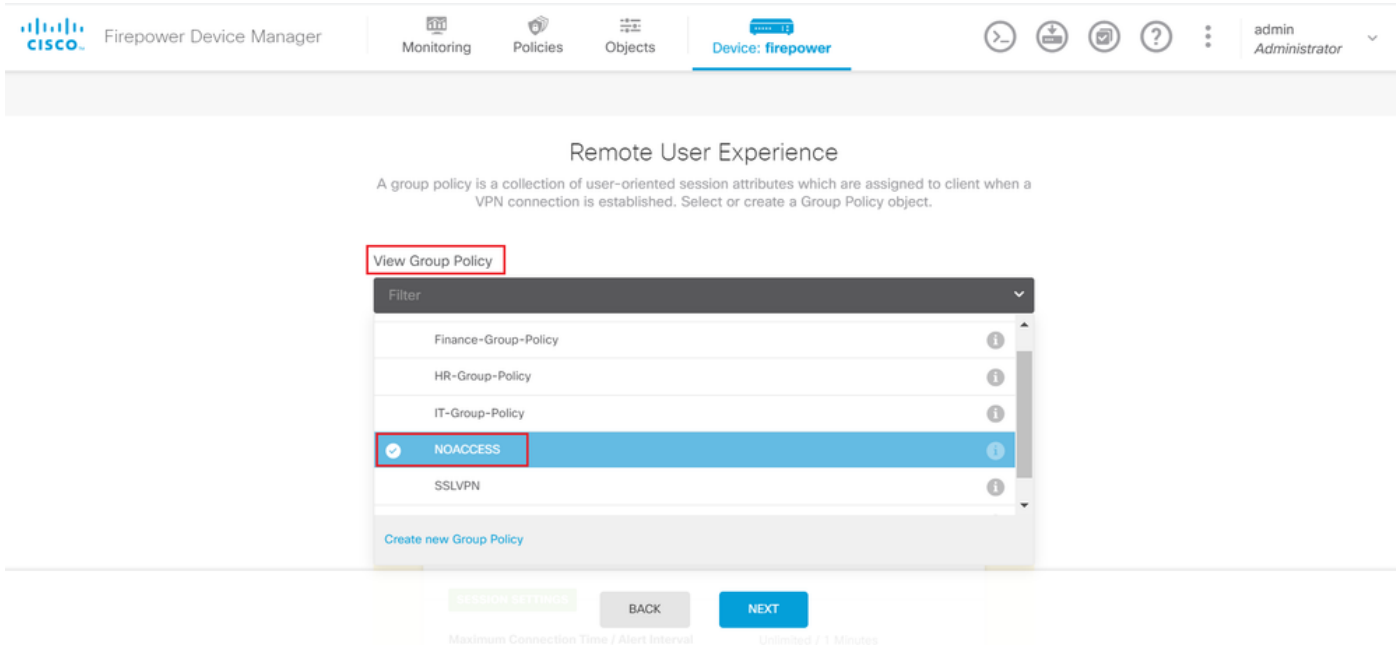
TEST

[Add another configuration](#)

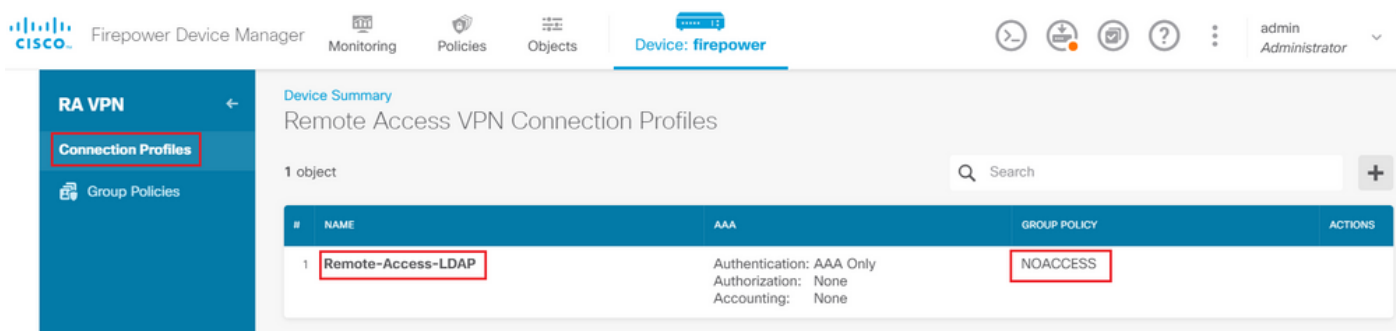
CANCEL

OK

单击Next并选择NOACCESS作为此连接配置文件的默认组策略。



保存所有更改。连接配置文件Remote-Access-LDAP现在在RA VPN配置下可见。

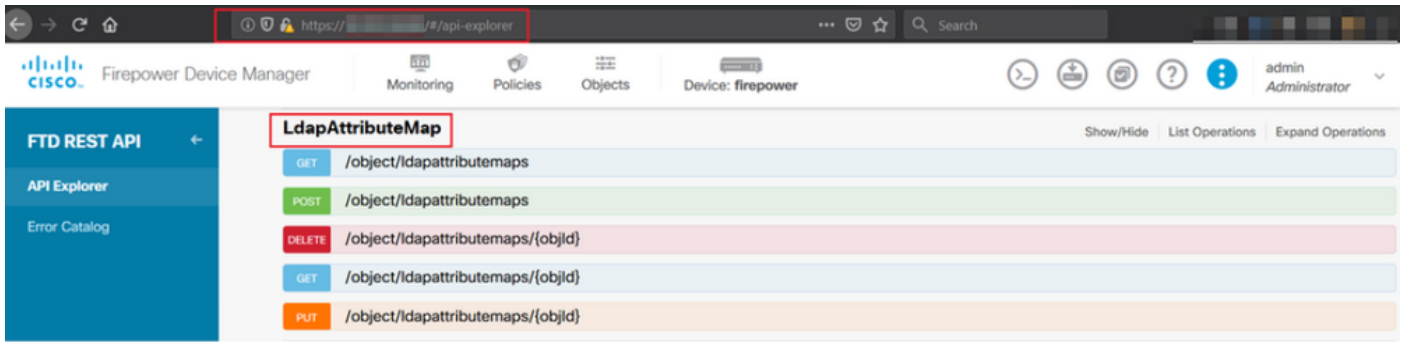


## LDAP属性映射的配置步骤

步骤1:启动FTD的API资源管理器。

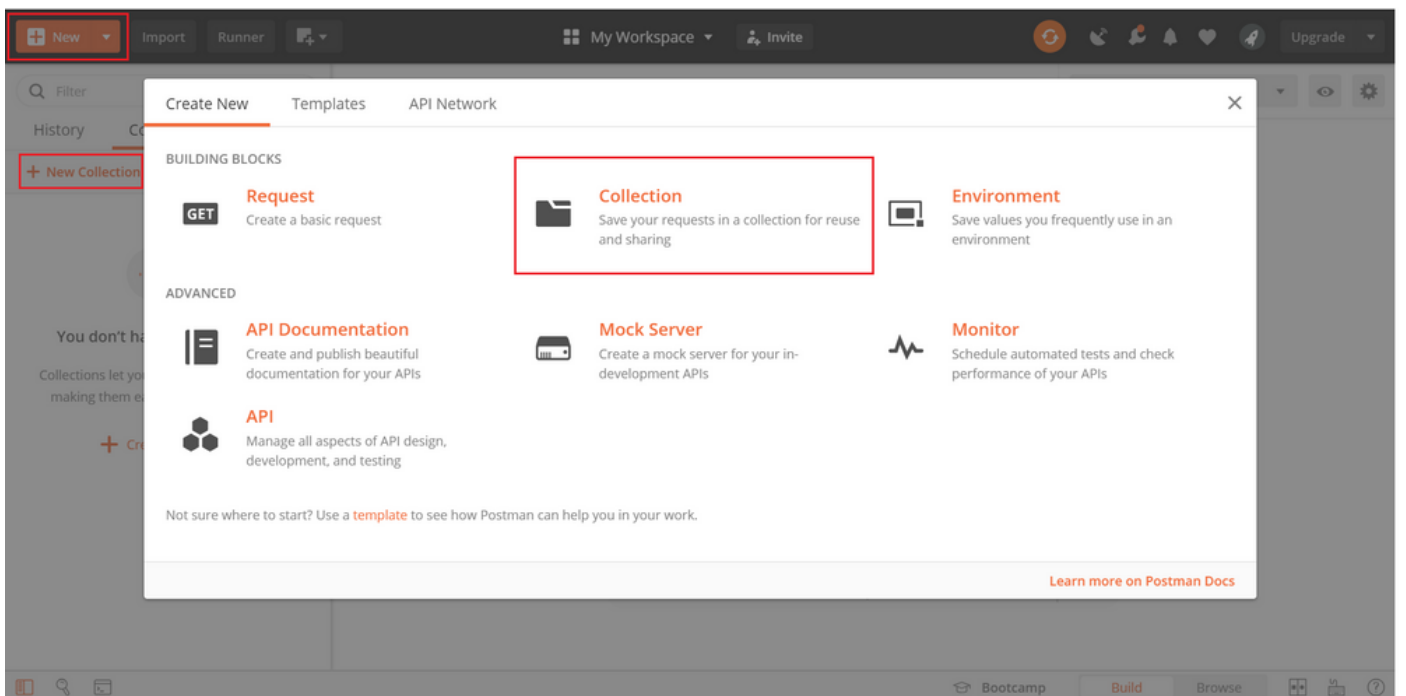
API资源管理器包含FTD上可用的API的完整列表。导航至<https://<FTD Management IP>/api-explorer>

向下滚动到LdapAttributeMap部分，然后单击它以查看所有受支持的选项。

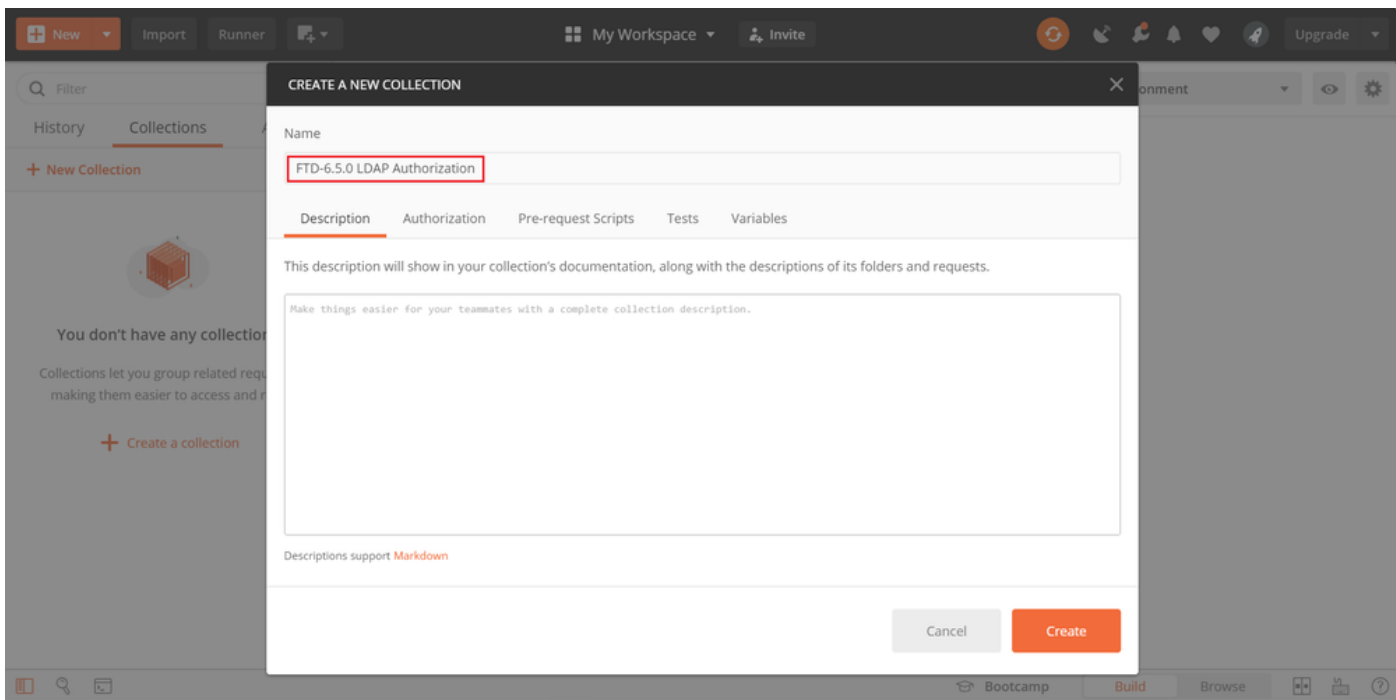


 注意：在本示例中，我们使用Postman作为API工具来配置LDAP属性映射。

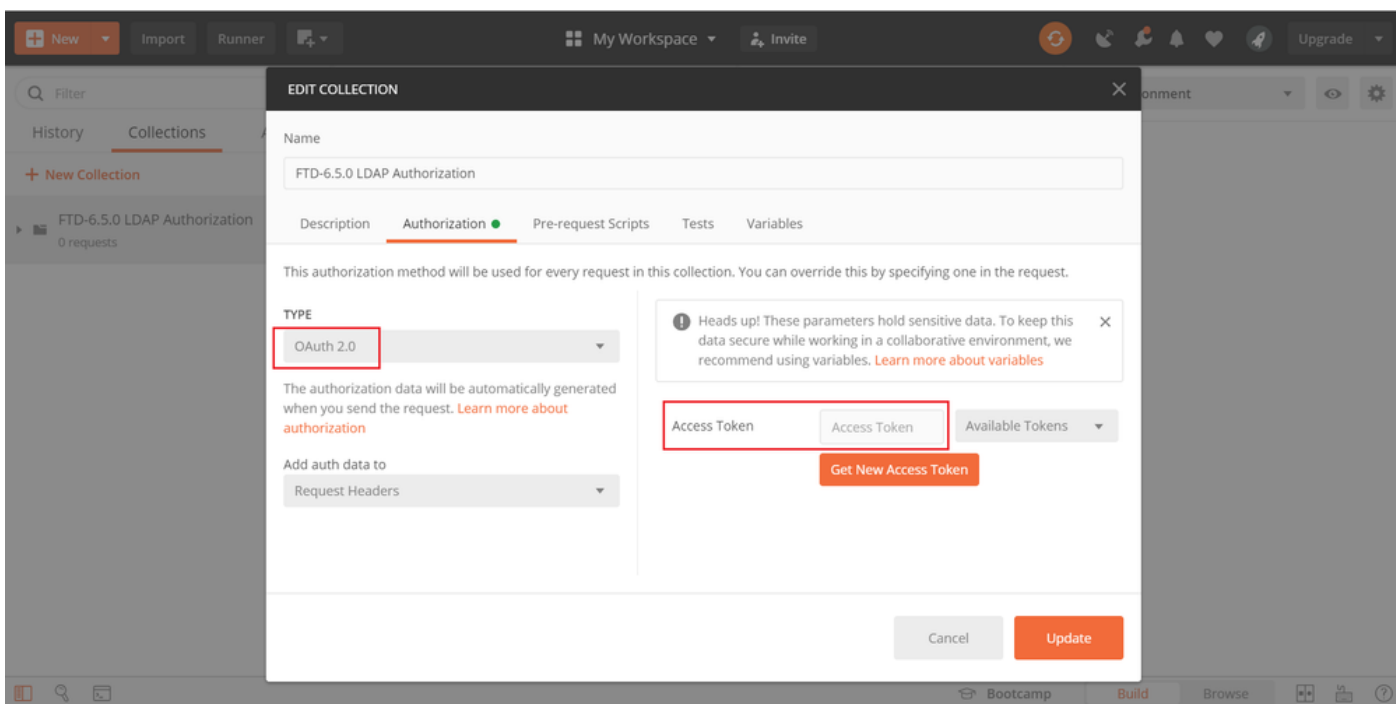
第二步：为LDAP授权添加Postman集合。



输入此集合的名称。



编辑 授权 选项卡并选择 OAuth 2.0类型



步骤3. 导航到File > Settings，关闭SSL证书验证，以避免在向FTD发送API请求时发生SSL握手故障。如果FTD使用自签名证书，则会完成此操作。



# 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

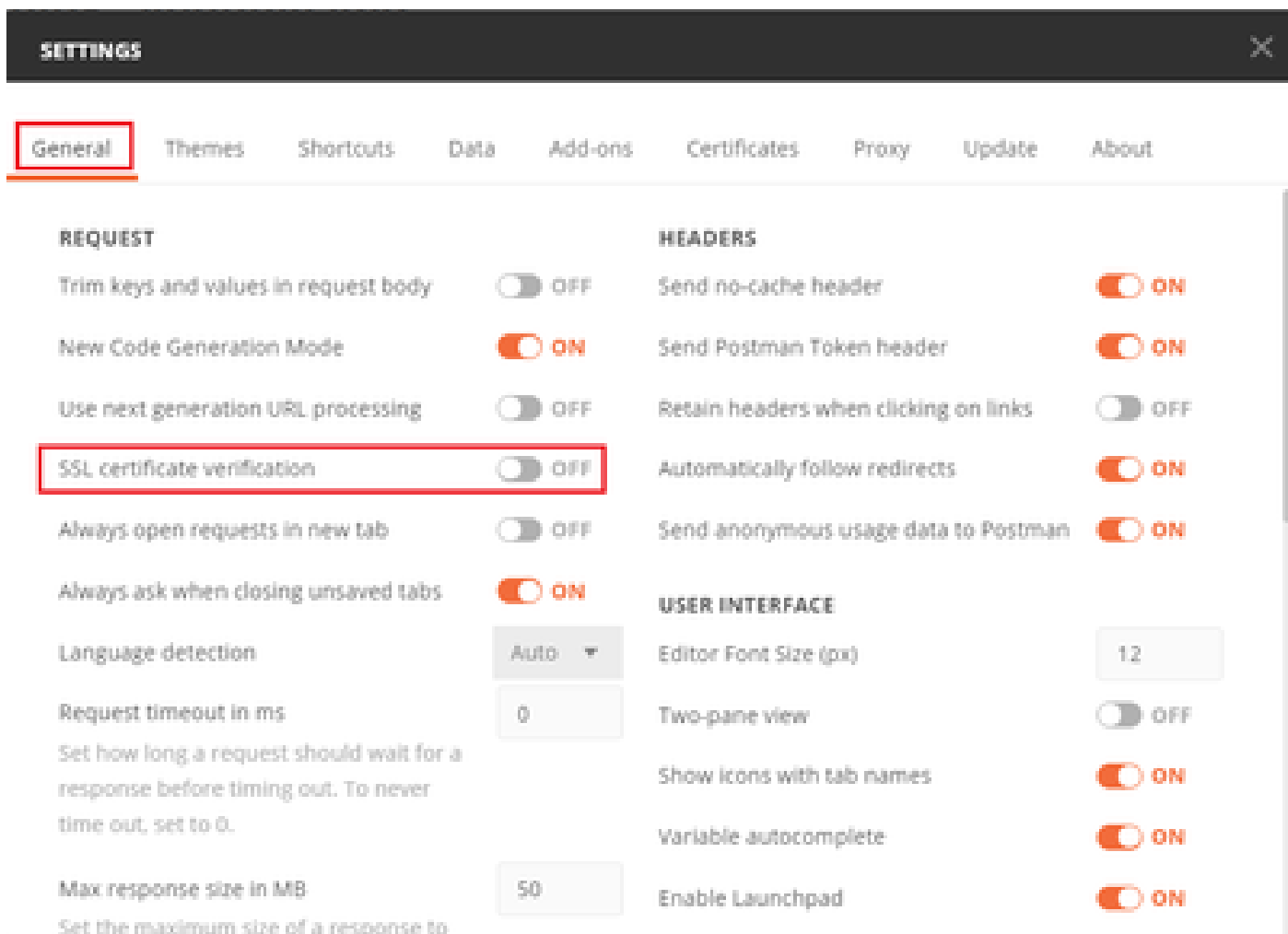
Settings Ctrl+Comma

Close Window Ctrl+Shift+W

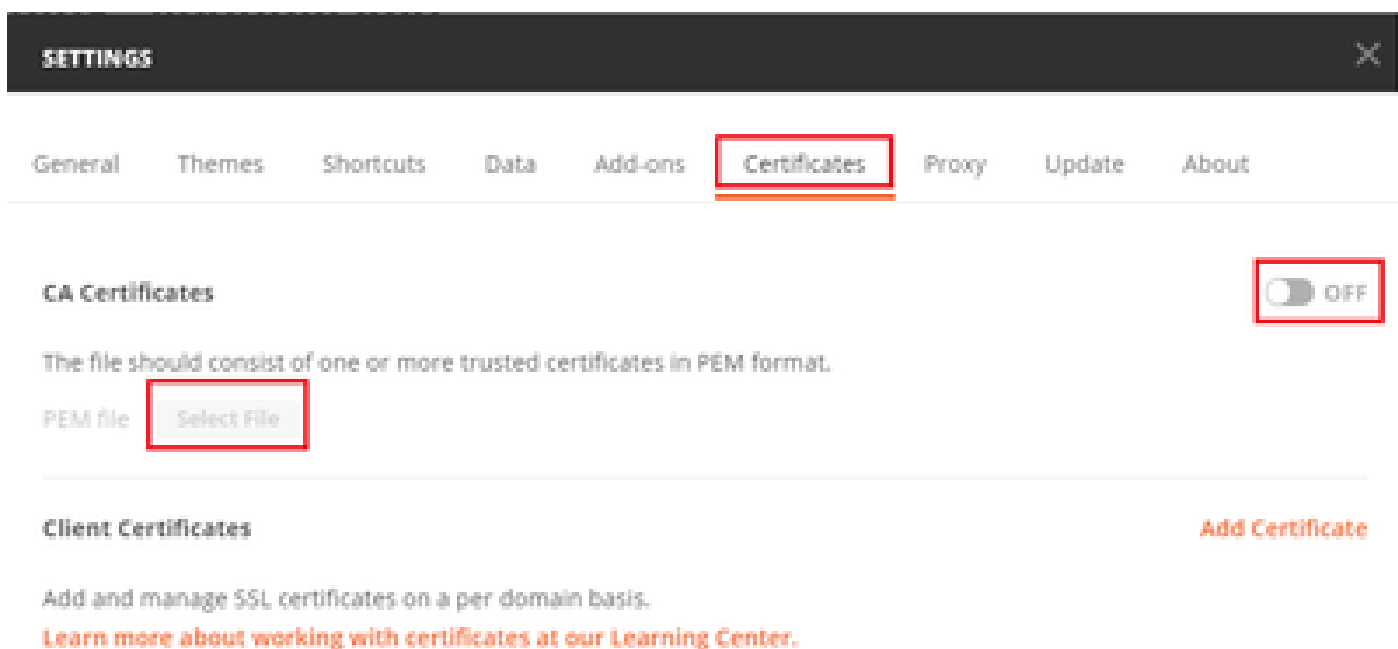
Close Tab Ctrl+W

Force Close Tab Alt+Ctrl+W

Exit



或者，FTD使用的证书可以作为CA证书添加到设置的Certificate部分。





第四步：添加新的POST请求Auth，以创建到FTD的登录POST请求，从而获取令牌以授权任何POST/GET请求。

**+ 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 ( 接受 ) 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

对于所有其他请求，导航到相应的报头选项卡，并选择此Preset Header值：Header-LDAP，使REST API请求使用json作为主要数据类型。

要获取令牌的POST请求正文必须包含以下内容：

类型	raw - JSON ( 应用/json )
grant_type	密码
用户名	管理员用户名以登录到FTD
密码	与管理员用户帐户关联的密码

```
{
  "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 }
```

单击send后，响应的主体包含用于向FTD发送任何PUT/GET/POST请求的访问令牌。

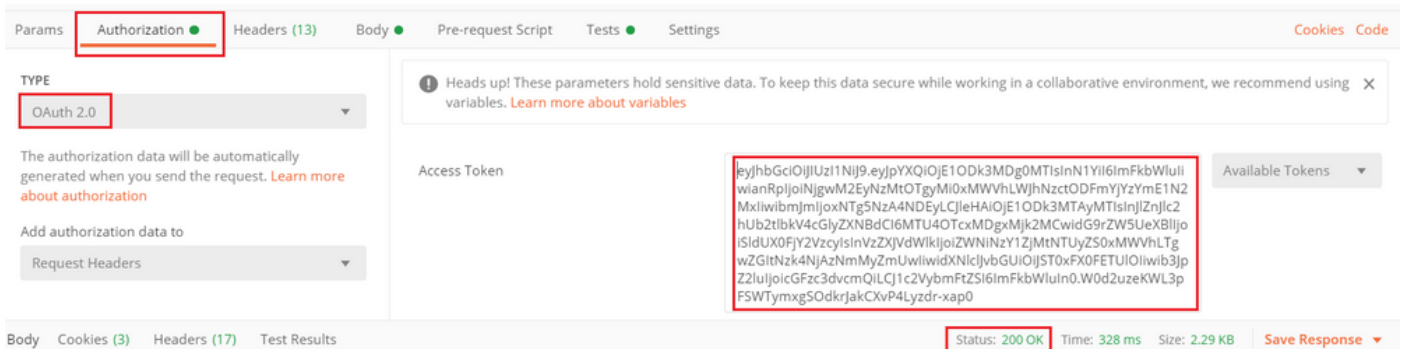


```
{
  "access_token": "eyJhbGciOiJIUzI1NiIsInR5cGU6IjY9LmVhbnQ6ImF1dG8iLCJ1e28xMWhLTGw",
  "expires_in": 1800,
  "token_type": "Bearer",
  "refresh_token": "eyJhbGciOiJIUzI1NiIsInR5cGU6IjY9LmVhbnQ6ImF1dG8iLCJ1e28xMWhLTGw",
  "refresh_expires_in": 2400
}
```

然后，此令牌用于授权所有后续请求。

导航到每个新请求的Authorization选项卡，然后选择下一个请求：

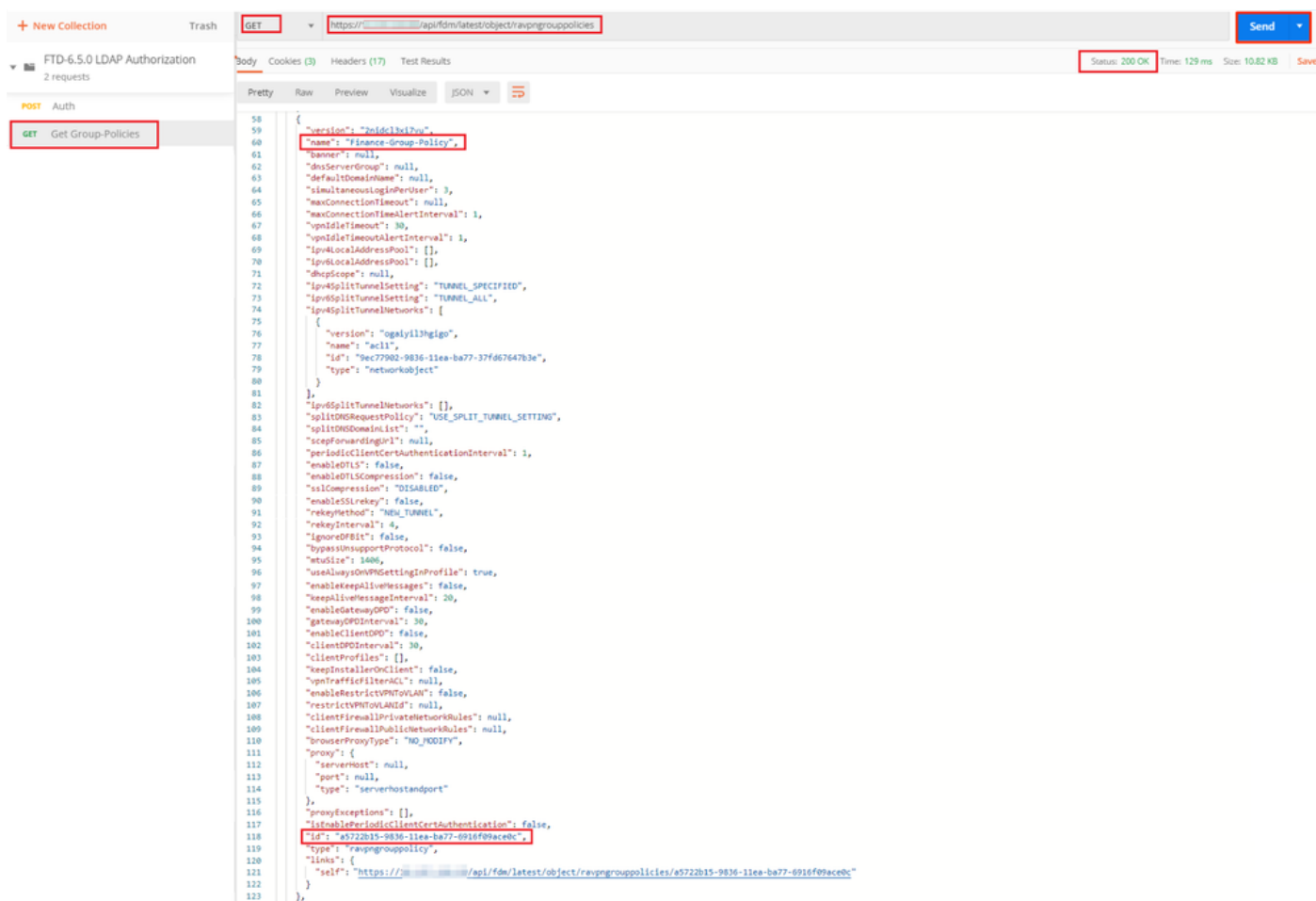
类型	OAuth 2.0
令牌	通过运行登录POST请求接收的访问令牌



第五步：添加新的GET请求Get Group-Policies以获取组策略状态和设置。收集每个已配置的组策略 (在本例中为Finance-Group-Policy、HR-Group-Policy和IT-Group-Policy)的名称和ID，以便在下一步中使用。

获取已配置的组策略的URL为：<https://<FTD Management IP>/api/fdm/latest/object/ravpngrouppolicies>

在下一个示例中，Group-Policy Finance-Group-Policy突出显示。



第六步：添加新的POST请求创建LDAP属性映射以创建LDAP属性映射。在本文档中，使用模型LdapAttributeMapping。其他模型也有类似的操作和方法，用于创建属性映射。这些型号的示例在本文档前面提到的api-explorer中提供。

FTD REST API

API Explorer

Error Catalog

**LdapAttributeMap**

GET /object/ldapattributemaps

POST /object/ldapattributemaps

Show/Hide | List Operations | Expand Operations

**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),

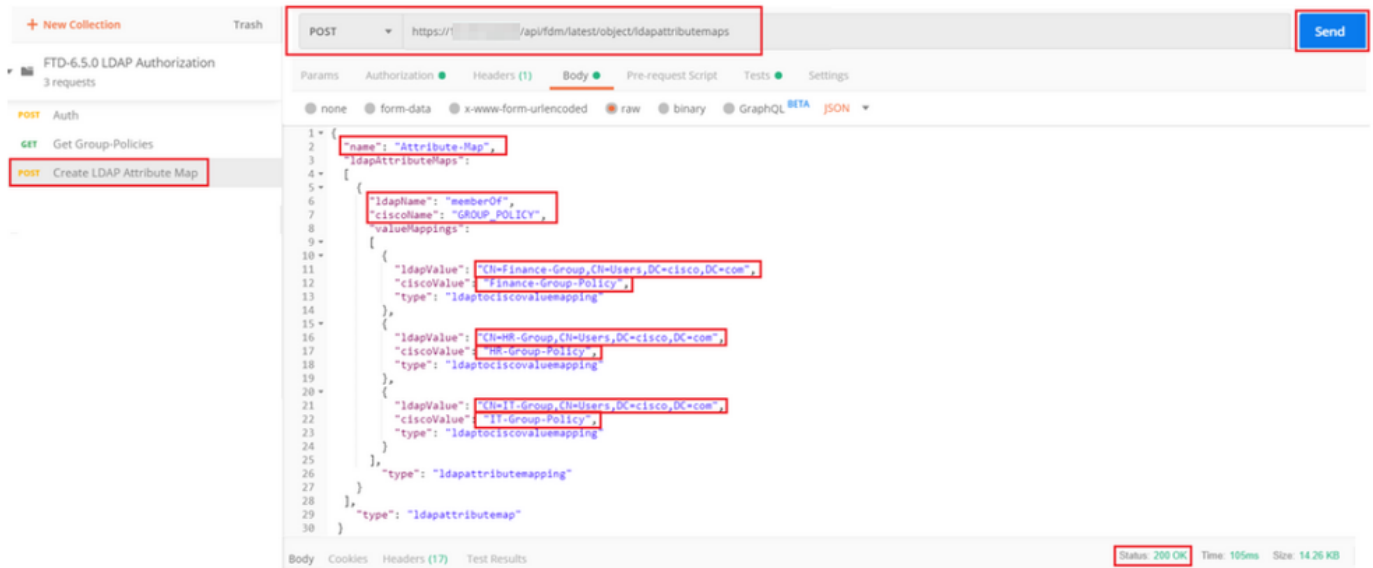
**valueMappings** (Array[LdapToGroupPolicyValueMapping]): A list of LdapToGroupPolicyValueMapping objects, which specify the value-to-group policy mappings for this LDAP attribute.  
Field level constraints: cannot be null. (Note: Additional constraints might exist),

**type** (string): ldapattributetogrouppolicymapping

发布LDAP属性映射的URL为：<https://<FTD Management IP>/api/fdm/latest/object/ldapattributemaps>

POST请求正文必须包含以下内容：


名称	LDAP属性映射的名称
类型	ldapattributemapping
ldapName	成员
ciscoName	GROUP_POLICY
ldapValue	来自AD的用户的memberOf值
思科价值	FDM中每个用户组的组策略名称



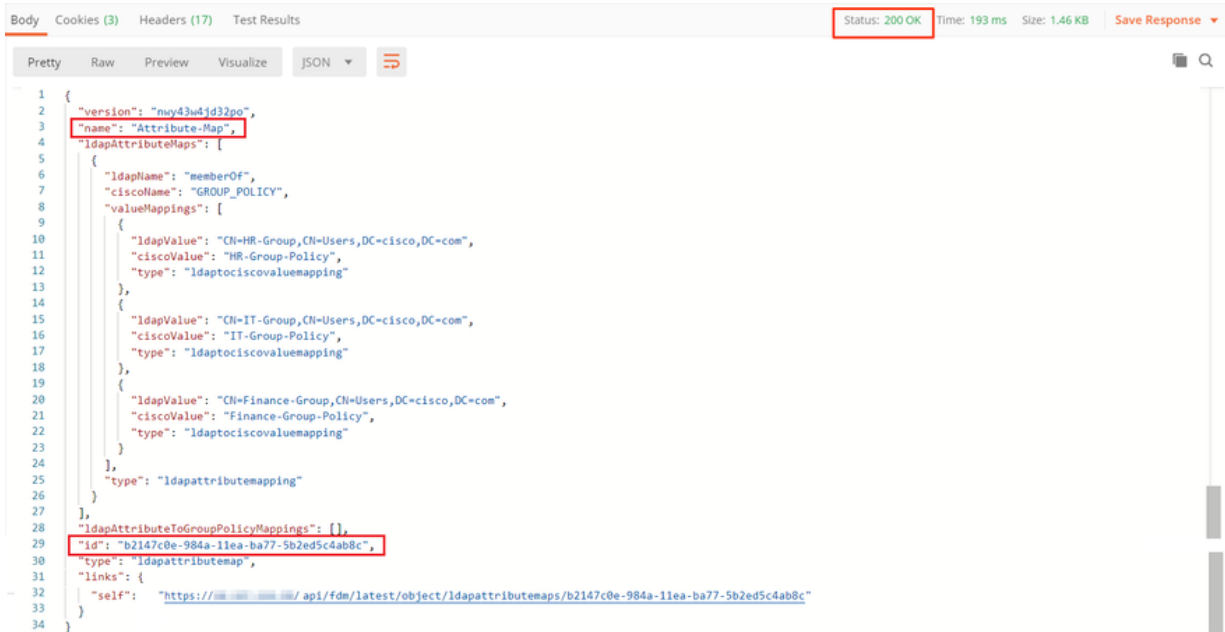
POST请求的主体包含根据memberOf值将特定组策略映射到AD组的LDAP属性映射信息：

```
{
  "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"
}
```

 注意：可以使用dsquery命令从AD服务器检索memberOf字段，也可以从FTD上的LDAP调试

 中检索该字段。在调试日志中，查找memberOf value:字段。

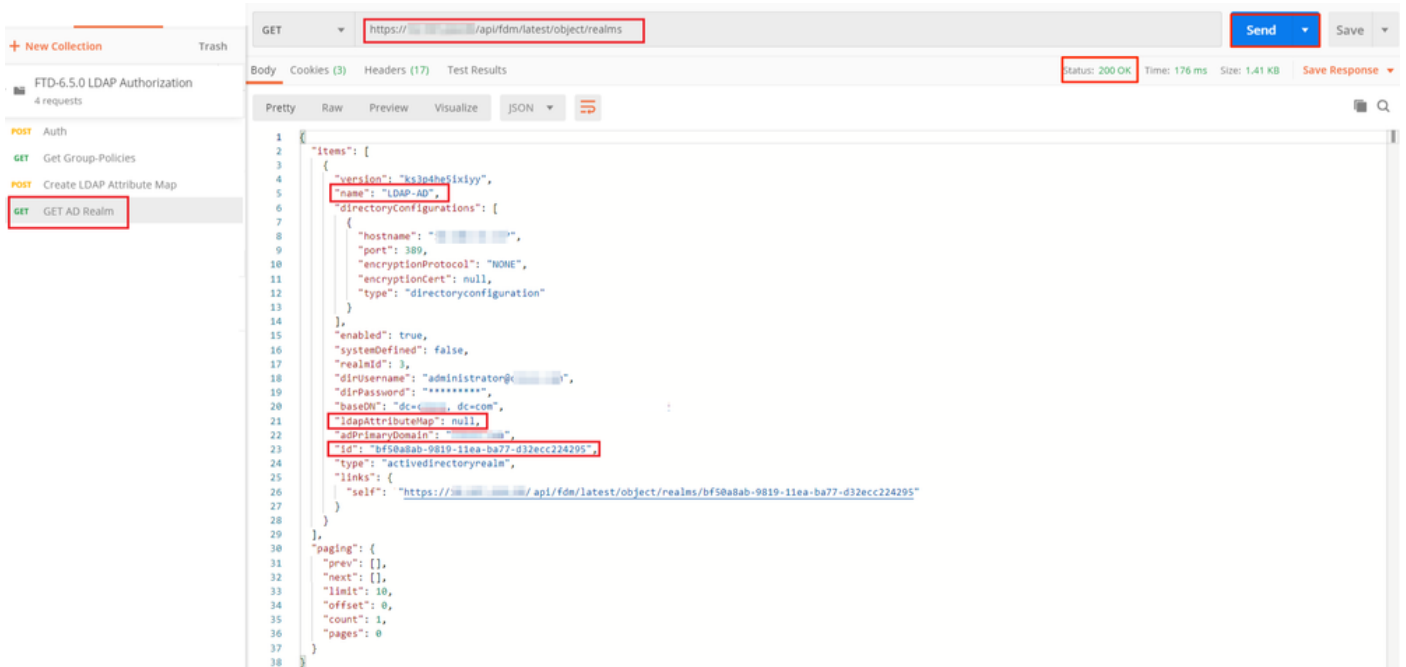
此POST请求的响应看起来与下一个输出类似：



```
1 {
2   "version": "muy43w4jd32po",
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 }
```

步骤 7.添加新的GET请求以获取FDM上的当前AD领域配置。

获取当前AD领域配置的URL为：<https://<FTD Management IP>/api/fdm/latest/object/realms>




```
1 {
2   "items": [
3     {
4       "version": "k3jcdh6ixiy",
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      "realId": {},
18      "dirUsername": "administrator@...",
19      "dirPassword": "*****",
20      "baseDN": "dc=...,dc=com",
21      "ldapAttributeMap": null,
22      "dirPrincipalDomain": "...",
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 }
```



请注意，关键字ldapAttributeMap的值为null。

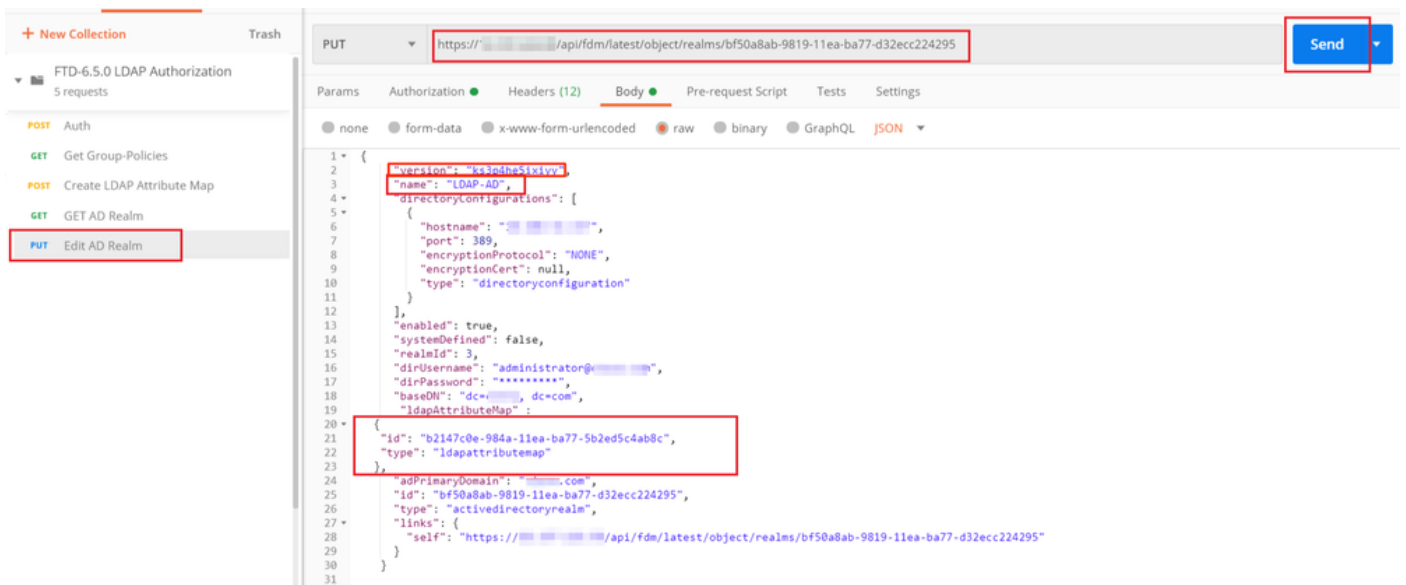
步骤 8创建新的PUT请求以编辑AD领域。复制上一步的GET响应输出，并将其添加到此新PUT请求的正文中。此步骤可用于对当前AD领域设置进行任何修改，例如：更改密码、IP地址或添加任何密钥(例如ldapAttributeMap)的新值。

 注意：复制项目列表的内容，而不是复制整个GET响应输出非常重要。PUT请求的请求URL必须附加有已进行更改的对象的项目ID。在本示例中，值为：bf50a8ab-9819-11ea-ba77-d32ecc224295

用于编辑当前AD领域配置的URL为：<https://<FTD Management IP>/api/fdm/latest/object/realms/<realm ID>>

PUT请求的主体必须包含以下内容：

version	从之前的GET请求的响应获取的版本
ID	从之前的GET请求的响应获取的ID
ldapAttributeMap	来自创建LDAP属性映射请求的响应的Idap-id



本示例中配置的正文为：

<#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"

}
}
```

验证ldapAttributeMap id是否与此请求的响应正文匹配。

```
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": "10.10.10.10",
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=com, dc=com",
19  "ldapAttributeMap": {
20    "version": "nwy43w4jd32po",
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://10.10.10.10/api/fdm/latest/object/realm/bf50a8ab-9819-11ea-ba77-d32ecc224295"
30  }
31 }
```


( 可选 )。可以使用PUT请求修改LDAP属性映射。创建新的PUT请求Edit Attribute-Map，并进行任何更改，例如Attribute-Map或memberOf值的名称。 T

在下一个示例中，所有三个组的值ldapvalue都已从CN=Users修改为CN=UserGroup。

```
FTD-6.5.0 LDAP Authorization 6 requests PUT https://10.10.10.10/api/fdm/latest/object/ldapattributemaps/b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c
Auth
POST Get Group-Policies
GET Create LDAP Attribute-Map
GET GET AD Realm
PUT Edit AD Realm
PUT Edit Attribute-Map
PUT Edit Attribute-Map
Params Authorization Headers (11) Body Pre-request Script Tests Settings
@ none @ form-data @ x-www-form-urlencoded @ raw @ binary @ GraphQL JSON
1 {
2   "version": "nwy43w4jd32po",
3   "name": "Attribute-Map",
4   "ldapattributemaps": [
5     {
6       "ldapname": "memberOf",
7       "ciscosname": "GROUP_POLICY",
8       "value": "CN=Users",
9       "valueMappings": [
10        {
11          "ldapvalue": "CN=UserGroup",
12          "ciscosname": "Finance-Group-Policy",
13          "type": "ldaptoiscosvaluemapping"
14        },
15        {
16          "ldapvalue": "CN=UserGroup",
17          "ciscosname": "HR-Group-Policy",
18          "type": "ldaptoiscosvaluemapping"
19        },
20        {
21          "ldapvalue": "CN=UserGroup",
22          "ciscosname": "IT-Group-Policy",
23          "type": "ldaptoiscosvaluemapping"
24        }
25      ],
26      "type": "ldapattributemapping"
27    }
28  ],
29  "id": "b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c",
30  "type": "ldapattributemap",
31  "links": {
32    "self": "https://10.10.10.10/api/fdm/latest/object/ldapattributemaps/b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c"
33  }
34 }
35 }
```

( 可选 )。要删除现有LDAP属性映射，请创建DELETE Request Delete Attribute-Map。包括上一个HTTP响应中的map-id，并附加删除请求的基本URL。

```
History Collections APIs Delete Attribute-Map
+ New Collection Trash
FTD-6.5.0 LDAP Authorization 7 requests
Auth
POST Get Group-Policies
GET Create LDAP Attribute-Map
GET GET AD Realm
PUT Edit AD Realm
PUT Edit Attribute-Map
DELETE Delete Attribute-Map
DELETE https://10.10.10.10/api/fdm/latest/object/ldapattributemaps/b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c
Params Authorization Headers (7) Body Pre-request Script Tests Settings
Query Params
KEY VALUE DESCRIPTION
Key Value Description
Response
```

 注：如果memberOf属性包含空格，则必须使用URL编码才能让Web服务器对其进行分析。否则，会收到400错误请求HTTP响应。对于包含空格的字符串，可使用“%20”或“+”来避免此错误。

步骤 9 导航回FDM，选择“部署”图标，然后点击立即部署。

## Pending Changes ? ×

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

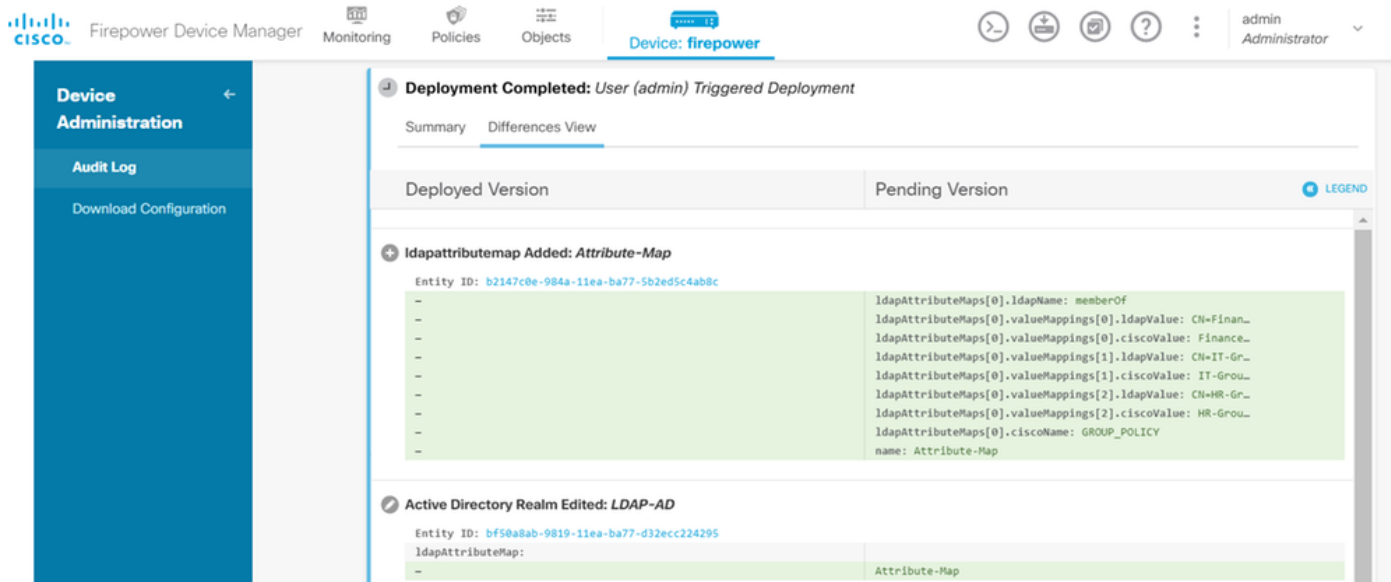
Deployed Version (17 May 2020 07:46 PM)	Pending Version <span>⏪</span> <b>LEGEND</b>
<b>+ Idapattributemap Added: <i>Attribute-Map</i></b>	
-	ldapAttributeMaps[0].ldapName: memberOf
-	ldapAttributeMaps[0].valueMappings[0].ldapValue: CN=IT-Gr...
-	ldapAttributeMaps[0].valueMappings[0].ciscoValue: IT-Grou...
-	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 ▼

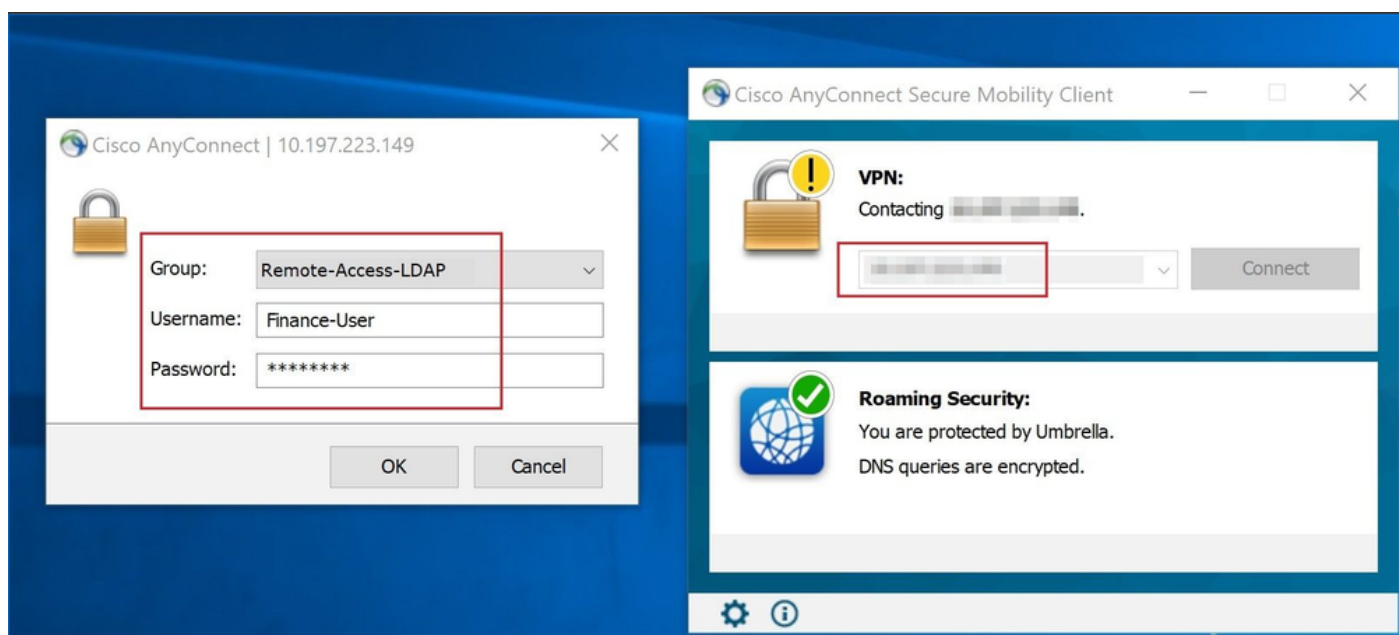
## 验证

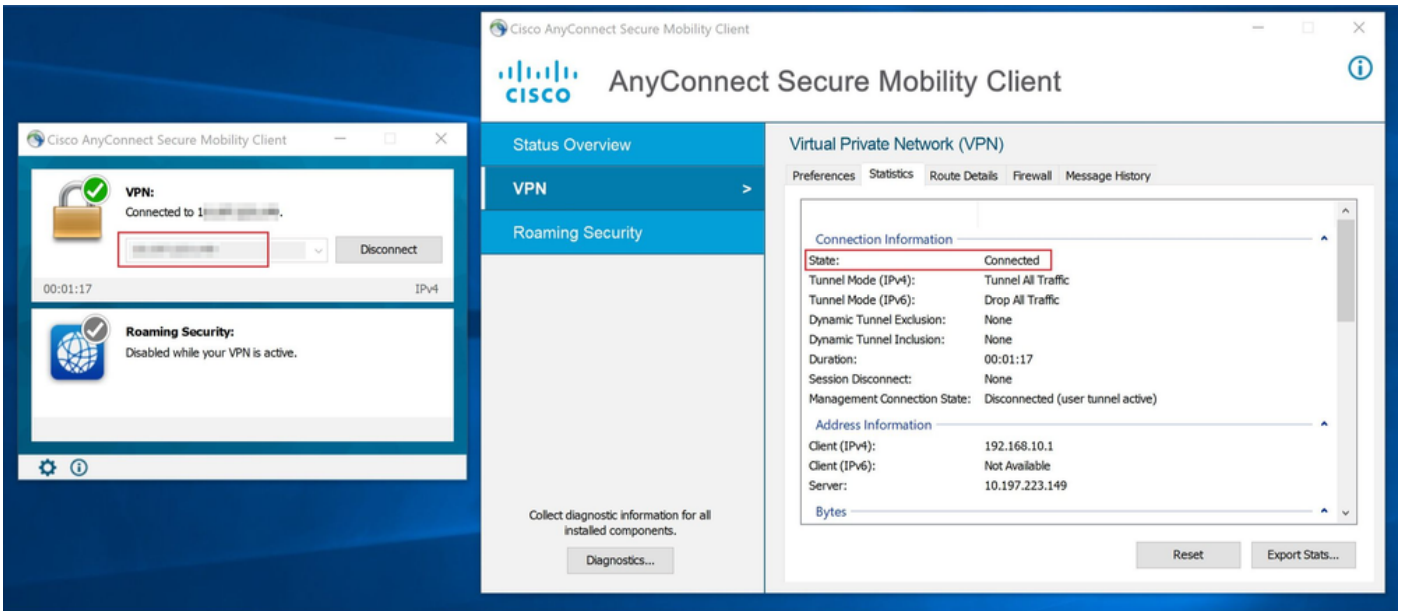
可以在FDM的部署历史记录部分中验证部署更改。



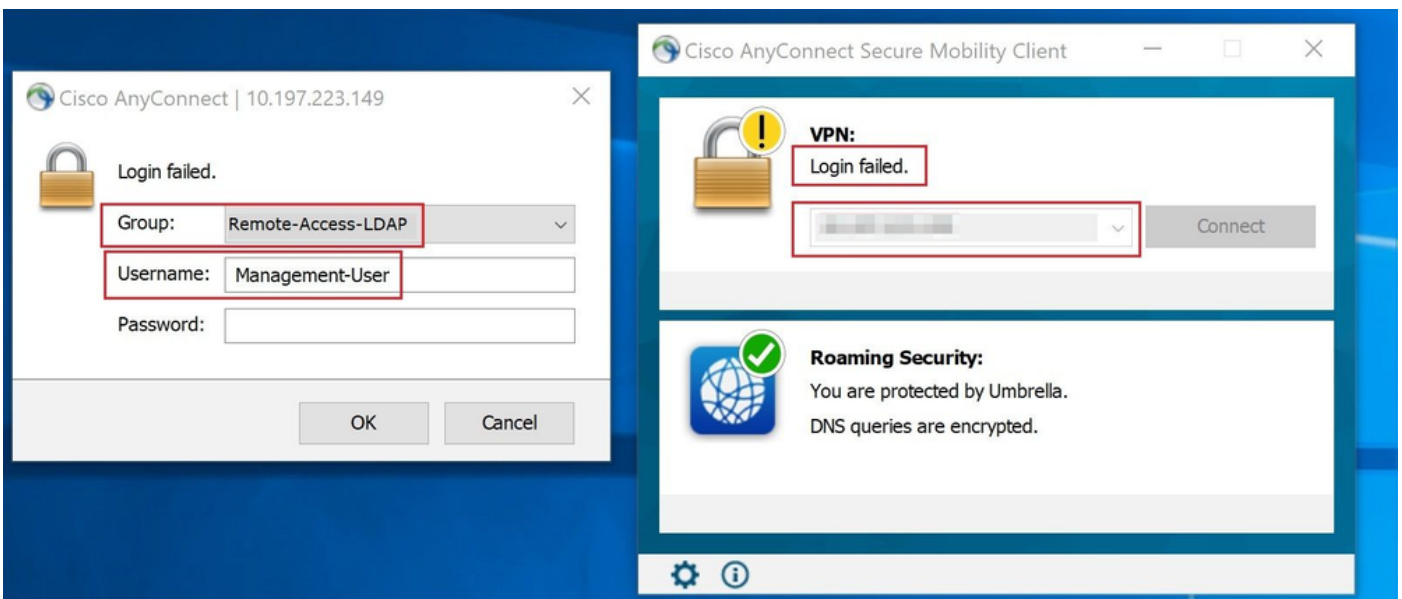
要测试此配置，请在用户名和密码字段中提供AD凭证。

当属于AD组Finance-Group的用户尝试登录时，尝试按预期成功。





当AD中属于Management-Group的用户尝试连接到Connection-Profile Remote-Access-LDAP时，由于没有LDAP属性映射返回匹配项，因此该用户在FTD上继承的组策略是NOACCESS，其vpn-simultaneous-logins值设置为0。因此，此用户的登录尝试失败。



可以通过FTD CLI的下一条show命令验证配置：

```
<#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
```


## 故障排除

配置REST API最常见的问题之一是不时更新承载令牌。身份验证请求的响应中提供了令牌到期时间。如果此时间过期，则可以使用其他刷新令牌更长时间。刷新令牌也到期后，必须发送新的身份验证请求以检索新的访问令牌。

---

 注意：使用[debug命令之前](#)，请参阅有关Debug命令的重要信息。

---

 您可以设置各种调试级别。默认情况下，使用级别1。如果更改调试级别，调试的详细程度可能会增加。请谨慎执行此操作，尤其是在生产环境中。

---

FTD CLI上的以下调试有助于排除与LDAP属性映射相关的问题

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

在本例中，收集了下一个调试，以演示在连接之前提及测试用户时从AD服务器接收的信息。

Finance-User的LDAP调试:

<#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的LDAP调试:

```
<#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
```

## 相关信息

如需其他帮助，请联系思科技术支持中心(TAC)。需要有效的支持合同：[思科全球支持联系方式](#)。

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。