

# 為FDM管理的FTD上的RAVPN配置LDAP屬性對映

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[身份驗證流程](#)

[LDAP屬性對映流說明](#)

[設定](#)

[FDM的配置步驟](#)

[LDAP屬性對映的配置步驟](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

---

## 簡介

本文檔介紹使用輕量級目錄訪問協定(LDAP)伺服器對遠端訪問VPN(RA VPN)使用者進行身份驗證和授權，並根據使用者在LDAP伺服器上的組成員資格授予他們不同的網路訪問許可權的過程。

## 必要條件

### 需求

- 防火牆裝置管理器(FDM)上的RA VPN配置基礎知識
- 有關FDM上的LDAP伺服器配置的基本知識
- 演示狀態傳輸(REST)應用程式介面(API)和FDM Rest API資源管理器的基本知識
- 由FDM管理的Cisco FTD 6.5.0版或更高版本

### 採用元件

使用了下列應用程式/裝置的硬體和軟體版本：

- Cisco FTD版本6.5.0，內部版本115
- Cisco AnyConnect版本4.10
- Microsoft Active Directory(AD)伺服器
- Postman或任何其他API開發工具



注意：思科不提供對Microsoft AD Server和Postmal工具的配置支援。

---

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 身份驗證流程



### LDAP屬性對映流說明

1. 使用者發起與FTD的遠端存取VPN連線，並為其Active Directory(AD)帳戶提供使用者名稱和密碼。
2. FTD透過連線埠389或636（透過SSL的LDAP）將LDAP要求傳送到AD伺服器
3. AD會使用與該使用者相關聯的所有屬性回覆FTD。
4. FTD將接收的屬性值與在FTD上建立的LDAP屬性對映相匹配。這是授權過程。
5. 然後，使用者連線並繼承與LDAP屬性對映中的memberOf屬性匹配的Group-Policy的設定。

在本文檔中，使用memberOf LDAP屬性對AnyConnect使用者進行授權。

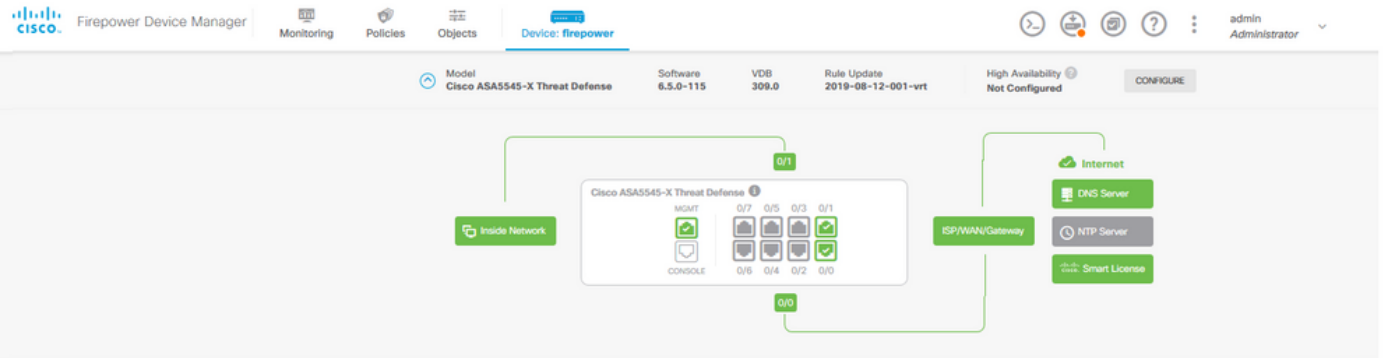
- 每個使用者的LDAP伺服器中的memberOf屬性被對映到FTD上的ldapValue實體。如果使用者屬於匹配的AD組，則使用者將繼承與該ldapValue關聯的組策略。
- 如果使用者的memberOf屬性值與FTD上的任何ldapValue實體不匹配，則會繼承所選連線配置檔案的預設Group-Policy。在本示例中，NOACCESS Group-Policy繼承到。

### 設定

FDM管理的FTD的LDAP屬性對映配置了REST API。

#### FDM的配置步驟

步驟 1. 驗證裝置是否已註冊到智慧許可。



<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>

步驟 2. 驗證FDM上是否已啟用AnyConnect許可證。

步驟 3. 驗證權杖中是否啟用匯出控制功能Enabled。

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

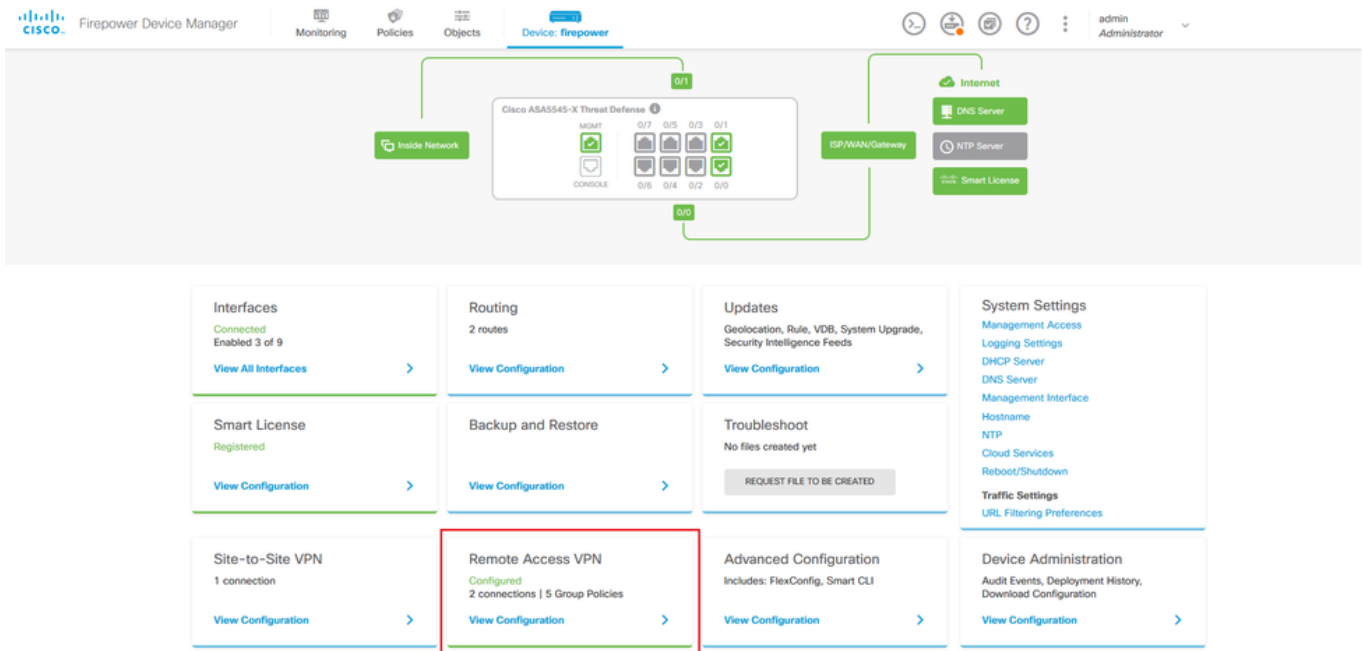
Enabled

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.

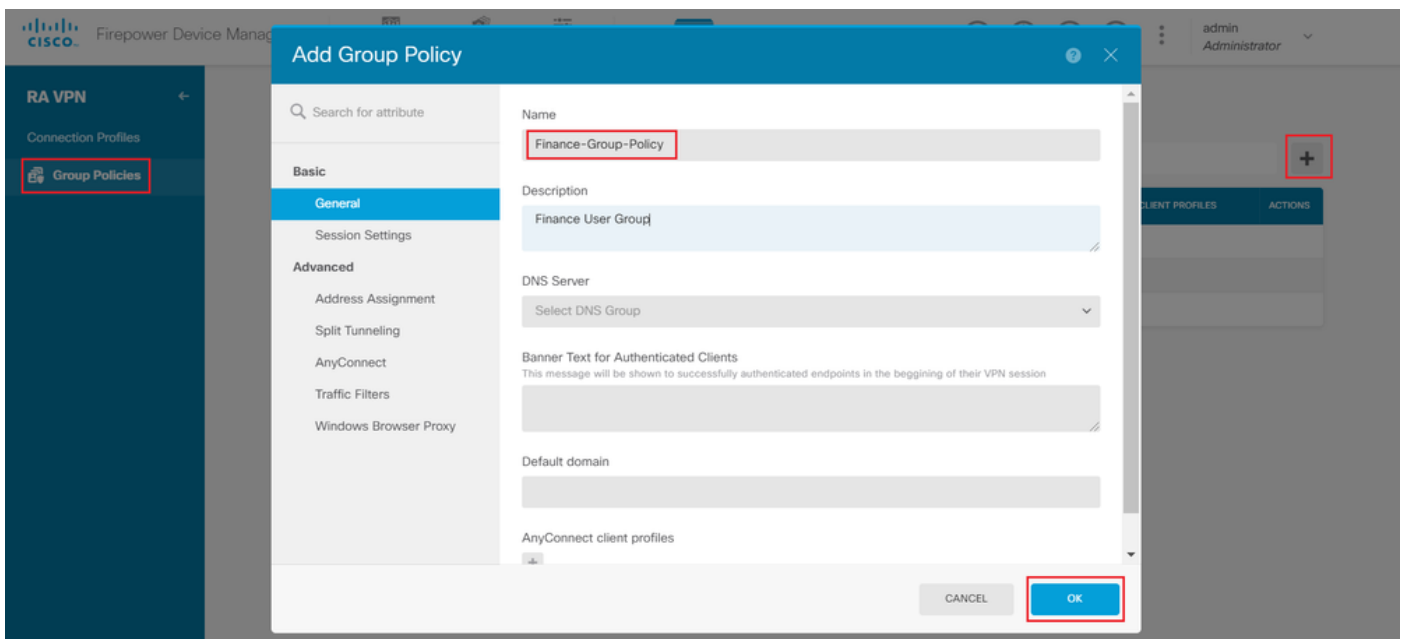
Includes: Intrusion Policy

注意：本文檔假設RA VPN已配置。有關如何在FDM管理的FTD上配置RA VPN的詳細資訊，請參閱以下文檔。

步驟 4. 導航到Remote Access VPN > Group Policies。



步驟 5. 導航到組策略。按一下「+」為每個AD組配置不同的組策略。在本示例中，將組策略 Finance-Group-Policy、HR-Group-Policy和IT-Group-Policy配置為可以訪問不同的子網。



Finance-Group-Policy具有以下設定：

```
<#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>
```

同樣，HR-Group-Policy具有以下設定：

```
<#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，IT-Group-Policy具有下一個設定：

<#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>
```

步驟 6. 建立組策略NOACCESS並導航到Session Settings，然後取消選中Simultaneous Login per User選項。這會將vpn-simultaneous-logins值設定為0。

設定為0時，Group-Policy中的vpn-simultaneous-logins值將立即終止使用者的VPN連線。此機制用於防止屬於任何AD使用者組（已配置使用者組除外）（在本例中為Finance、HR或IT）的使用者建立到FTD的成功連線，並訪問僅可用於允許的使用者組帳戶的安全資源。

屬於正確AD使用者組的使用者匹配FTD上的LDAP屬性對映並繼承對映的組策略，而不屬於任何允許組的使用者則繼承連線配置檔案的預設組策略，在本例中為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 Group-Policy具有以下設定：



```
<#root>
```

```
firepower#
```

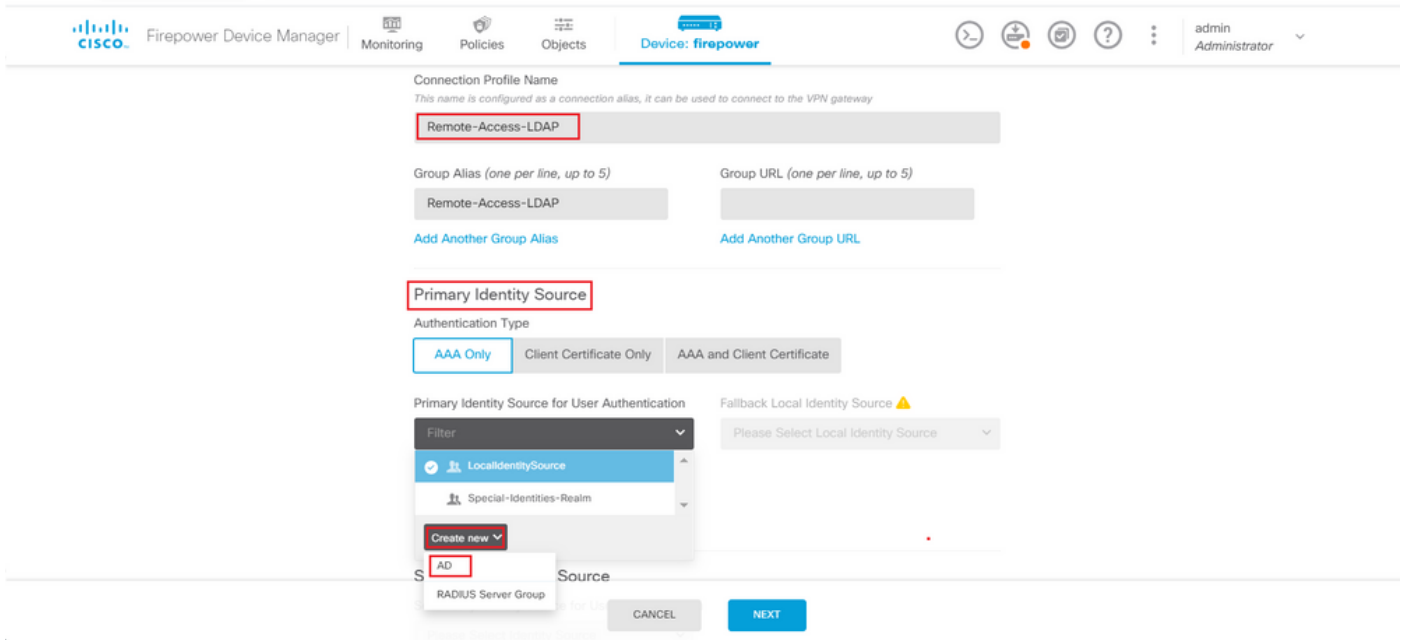
```
show run group-policy NOACCESS
```

```
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
```

步驟 7. 導航到 Connection Profiles 並建立 Connection-Profile。在此示例中，配置檔名稱為 Remote-Access-LDAP。選擇 Primary Identity Source AAA Only，然後建立新的身份驗證伺服器類型 AD。



輸入AD伺服器的資訊：

- 目錄使用者名稱
- 目錄密碼
- 基本DN
- AD主域
- 主機名/IP地址
- 連接埠
- 加密型別

# 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

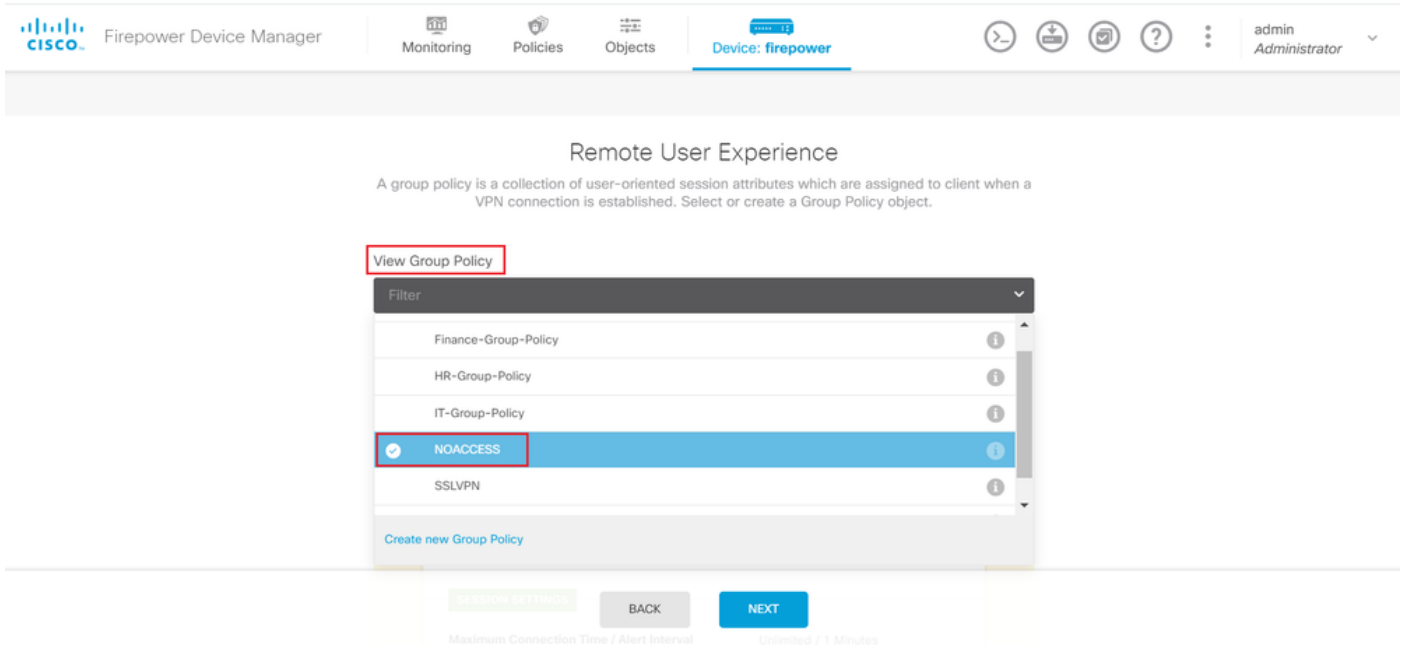
TEST

[Add another configuration](#)

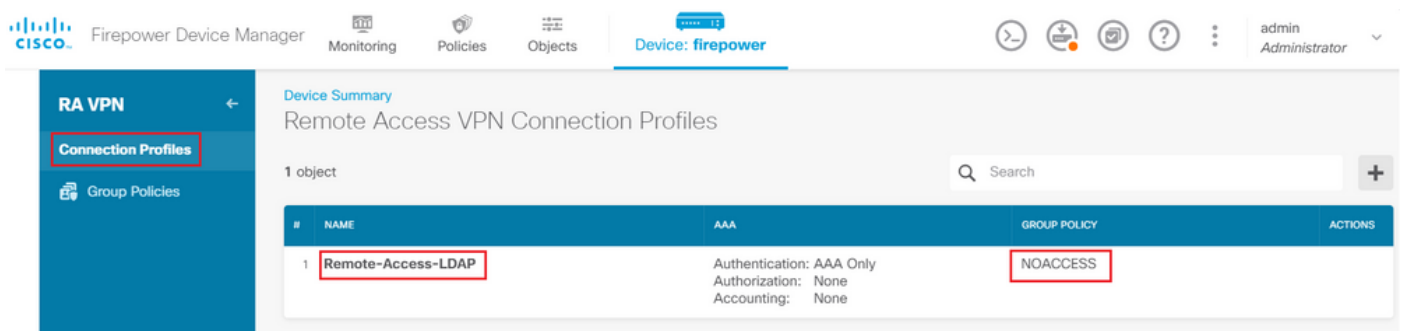
CANCEL

OK

按一下Next，然後選擇NOACCESS作為此連線配置檔案的預設組策略。



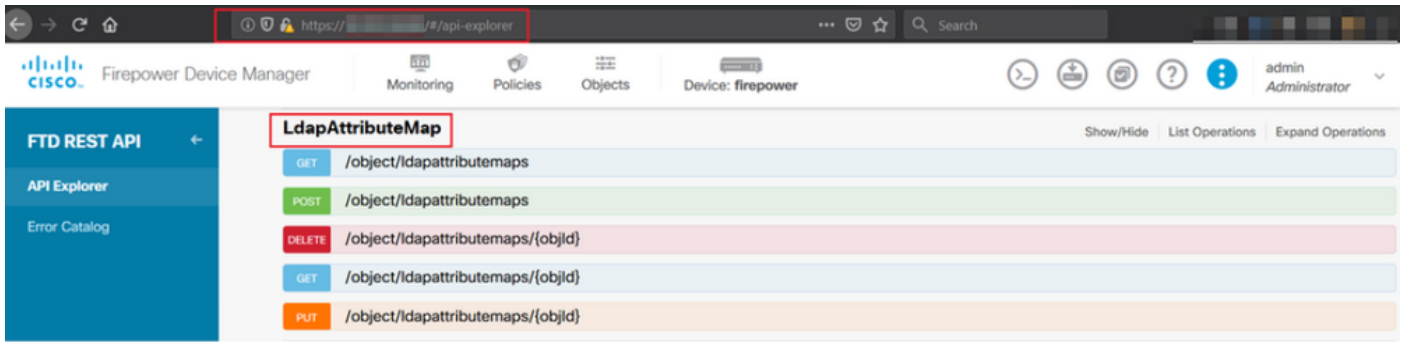
儲存所有更改。連線配置檔案Remote-Access-LDAP現在在RA VPN配置下可見。



## LDAP屬性對映的配置步驟

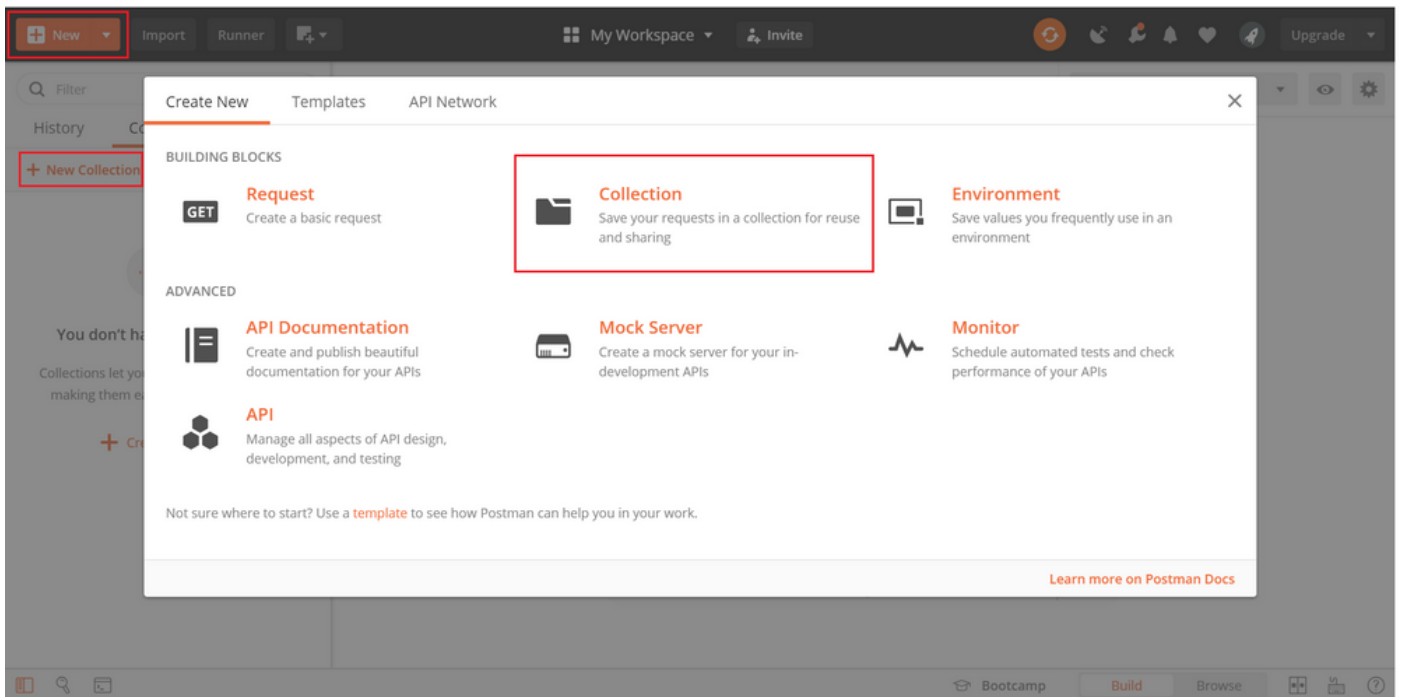
步驟 1. 啟動FTD的API Explorer。

API Explorer包含FTD上可用的API的完整清單。導覽至<https://<FTD Management IP>/api-explorer> 向下滾動到LdapAttributeMap部分，然後按一下它以檢視所有支援的選項。

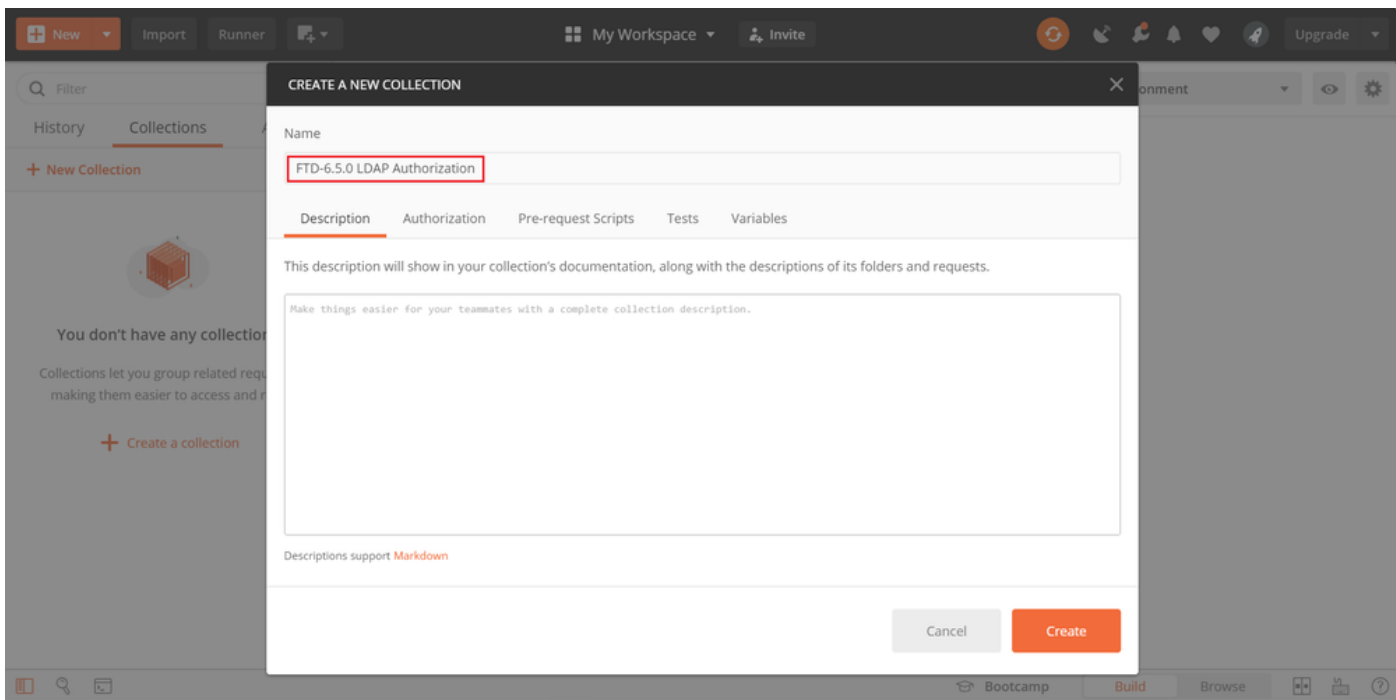


 注意：在本示例中，我們使用Postman作為API工具來配置LDAP屬性對映。

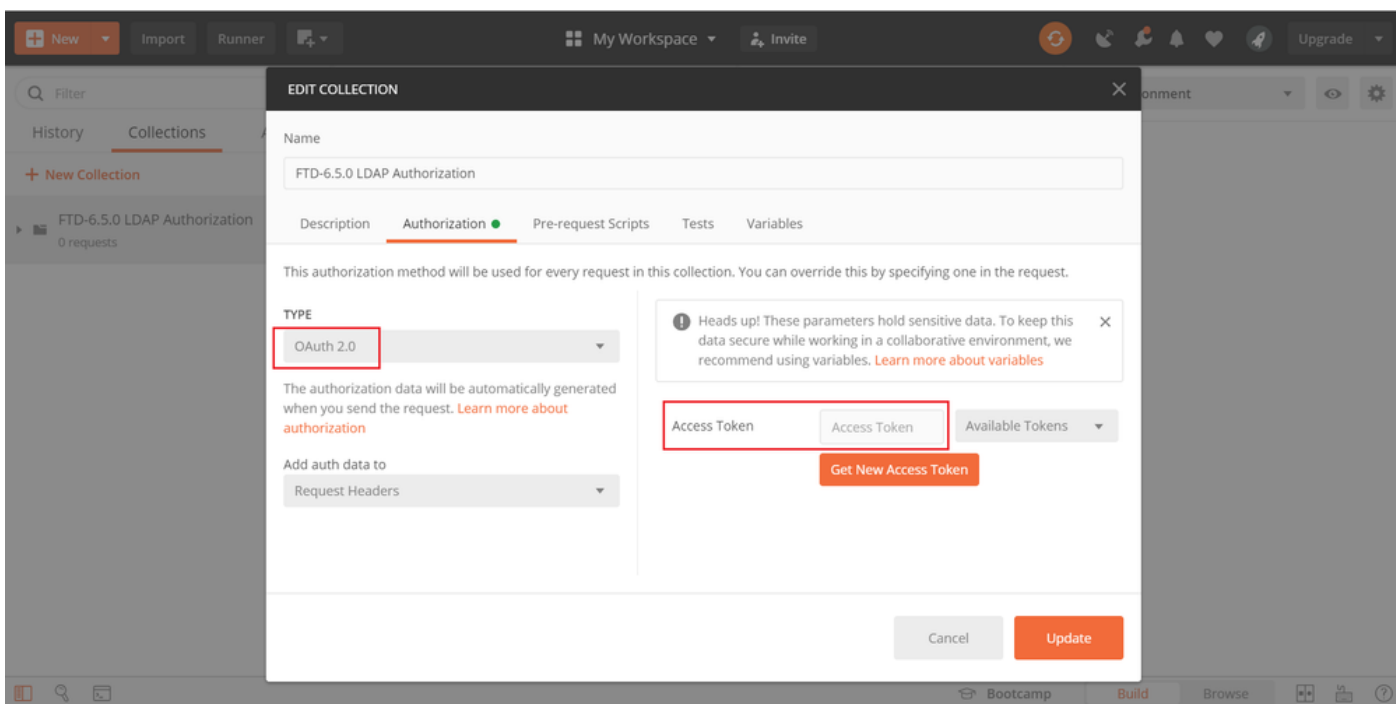
步驟 2. 為LDAP授權新增Postman集合。



輸入此集合的名稱。



編輯 Authorization 頁籤並選擇 OAuth 2.0 型別



步驟3. 導覽至File > Settings，關閉SSL憑證驗證，以避免在向FTD傳送API要求時發生SSL交握失敗。如果FTD使用自簽名的憑證，則會完成此操作。



# 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

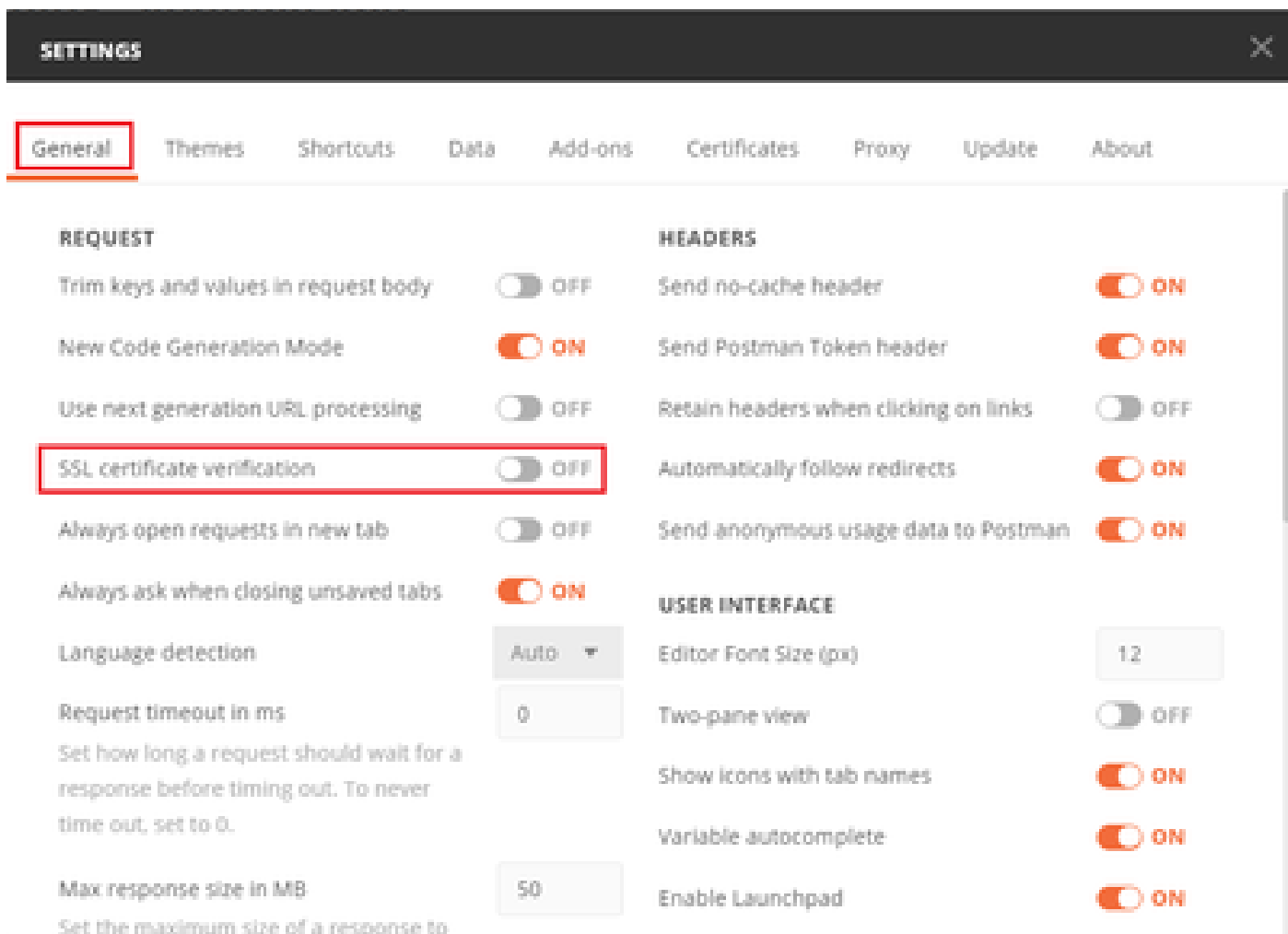
Settings Ctrl+Comma

Close Window Ctrl+Shift+W

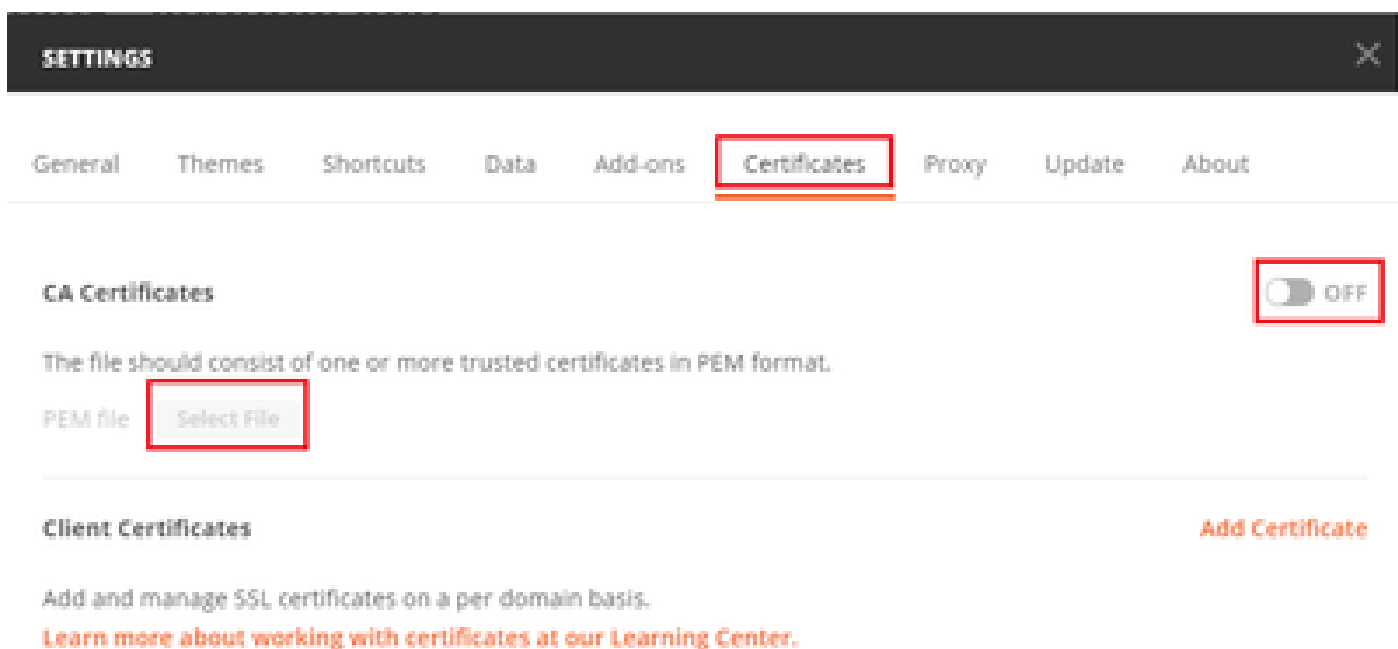
Close Tab Ctrl+W

Force Close Tab Alt+Ctrl+W

Exit



或者，FTD使用的憑證可以作為CA憑證新增到設定的「憑證」一節中。





步驟 4. 新增一個POST要求Auth，以建立到FTD的登入POST要求，從而取得權杖來授權任何POST/GET要求。

**+ 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

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

對於所有其他請求，請導航到相應的報頭頁籤，然後選擇此「預設報頭」值：Header-LDAP，使 REST API 請求使用 json 作為主要資料型別。

要獲取令牌的 POST 請求正文必須包含下一個：

類型	raw - JSON(application/json)
grant_type	密碼
使用者名稱	用於登入 FTD 的管理員使用者名稱
密碼	與管理員使用者帳戶關聯的密碼

```
{  
  "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

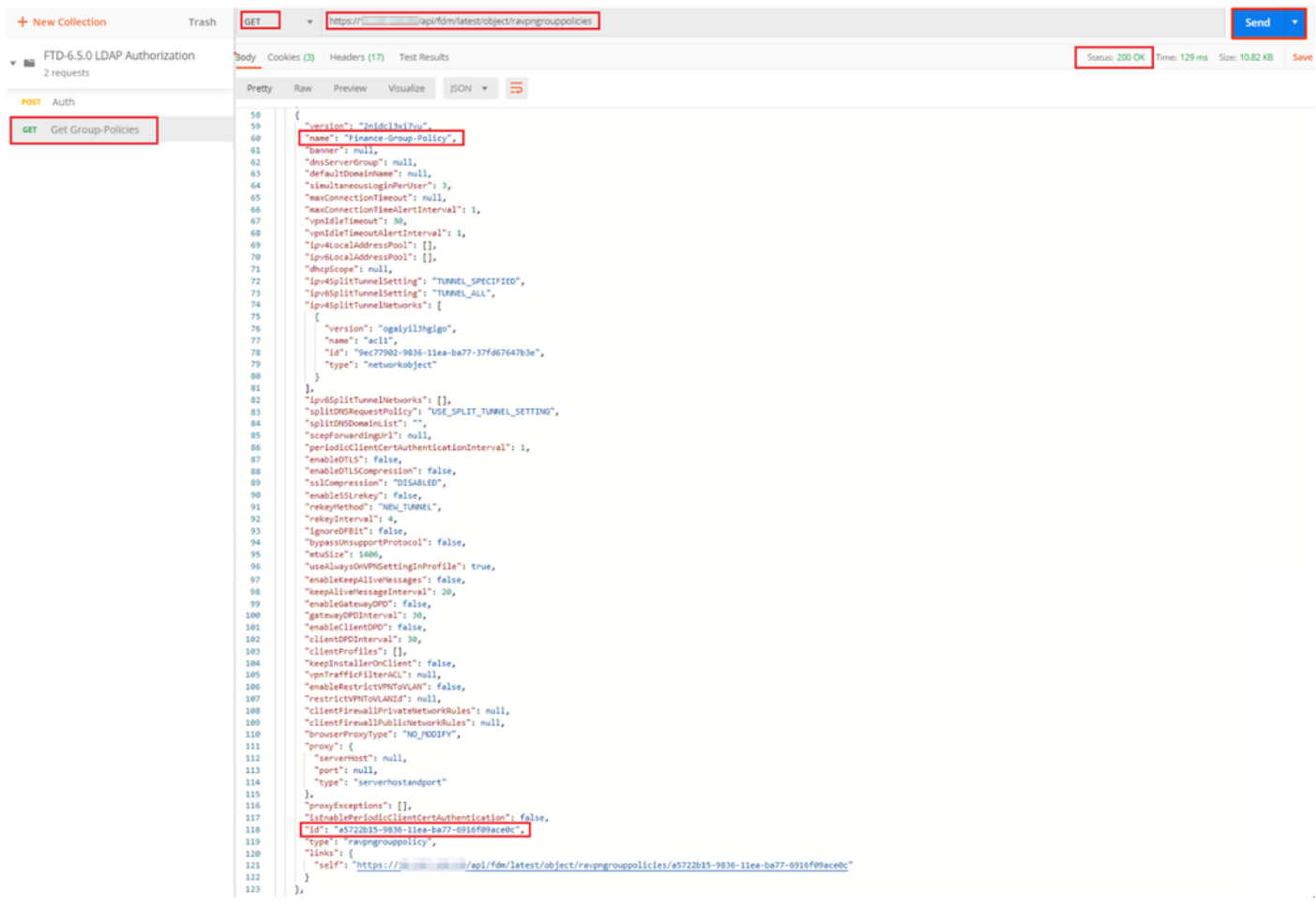
```
1 {  
2   "grant_type": "password",  
3   "username": "admin",  
4   "password": "  
5 }
```



步驟 5. 新增新的GET請求Get Group-Policies以獲取Group-Policy狀態和設定。收集每個已配置的組策略的名稱和ID(在本例中為：Finance-Group-Policy、HR-Group-Policy和IT-Group-Policy)，以便在下一步中使用。

獲取已配置的組策略的URL為：<https://<FTD Management IP>/api/fdm/latest/object/ravpngrouppolicies>

在下一個示例中，將突出顯示Group-Policy Finance-Group-Policy。



步驟 6. 新增新的POST請求建立LDAP屬性對映以建立LDAP屬性對映。在本文檔中，使用模型LdapAttributeMapping。其他模型也有類似的操作和方法，用於建立屬性對映。這些型號的示例可以在本文檔前面提到的api-explorer中找到。

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

LDAP屬性對映的URL為：<https://<FTD Management IP>/api/fdm/latest/object/ldapattributemaps>

POST請求正文必須包含以下內容：

名稱	LDAP屬性對映的名稱
類型	ldapattributemapping
ldap名稱	memberOf
ciscoName	GROUP_POLICY
ldap值	來自AD的使用者的memberOf值
ciscoValue	FDM中每個使用者組的組策略名稱

```

POST https://.../api/fdm/latest/object/ldapattributemaps
Body
1 {
2   "name": "Attribute-Map",
3   "ldapAttributeMaps":
4   [
5     {
6       "ldapName": "memberOf",
7       "ciscoName": "GROUP_POLICY",
8       "valueMappings":
9       [
10      {
11        "ldapValue": "CN=Finance-Group,CN=Users,DC=cisco,DC=com",
12        "ciscoValue": "Finance-Group-Policy",
13        "type": "ldaptociscovaluemapping"
14      },
15      {
16        "ldapValue": "CN=HR-Group,CN=Users,DC=cisco,DC=com",
17        "ciscoValue": "HR-Group-Policy",
18        "type": "ldaptociscovaluemapping"
19      },
20      {
21        "ldapValue": "CN=IT-Group,CN=Users,DC=cisco,DC=com",
22        "ciscoValue": "IT-Group-Policy",
23        "type": "ldaptociscovaluemapping"
24      }
25      ],
26       "type": "ldapattributemapping"
27     }
28   ],
29   "type": "ldapattributemap"
30 }
Status: 200 OK Time: 105ms Size: 14.26 KB

```

POST請求的主體包含根據memberOf值將特定組策略對映到AD組的LDAP屬性映射信息：

```

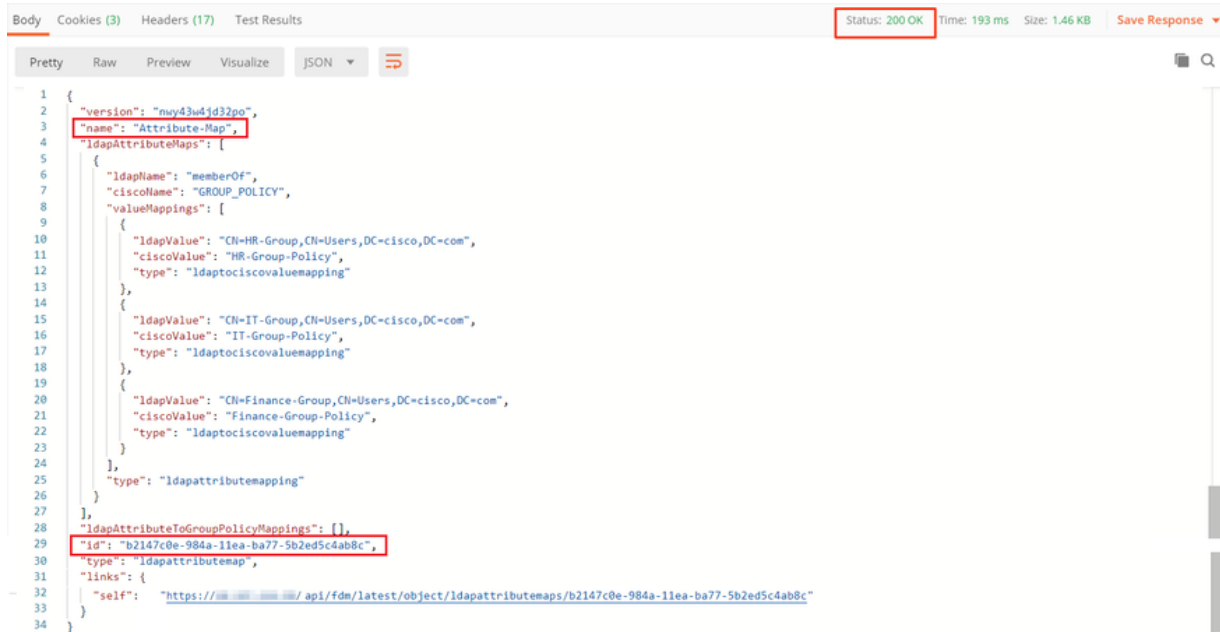
{
  "name": "Attribute-Map",
  "ldapAttributeMaps":
  [
    {
      "ldapName": "memberOf",
      "ciscoName": "GROUP_POLICY",
      "valueMappings":
      [
        {
          "ldapValue": "CN=Finance-Group,CN=Users,DC=cisco,DC=com",
          "ciscoValue": "Finance-Group-Policy",
          "type": "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命令從AD伺服器檢索memberOf欄位，或從FTD上的LDAP調試中讀

取該欄位。在調試日誌中，查詢memberOf value：字段。

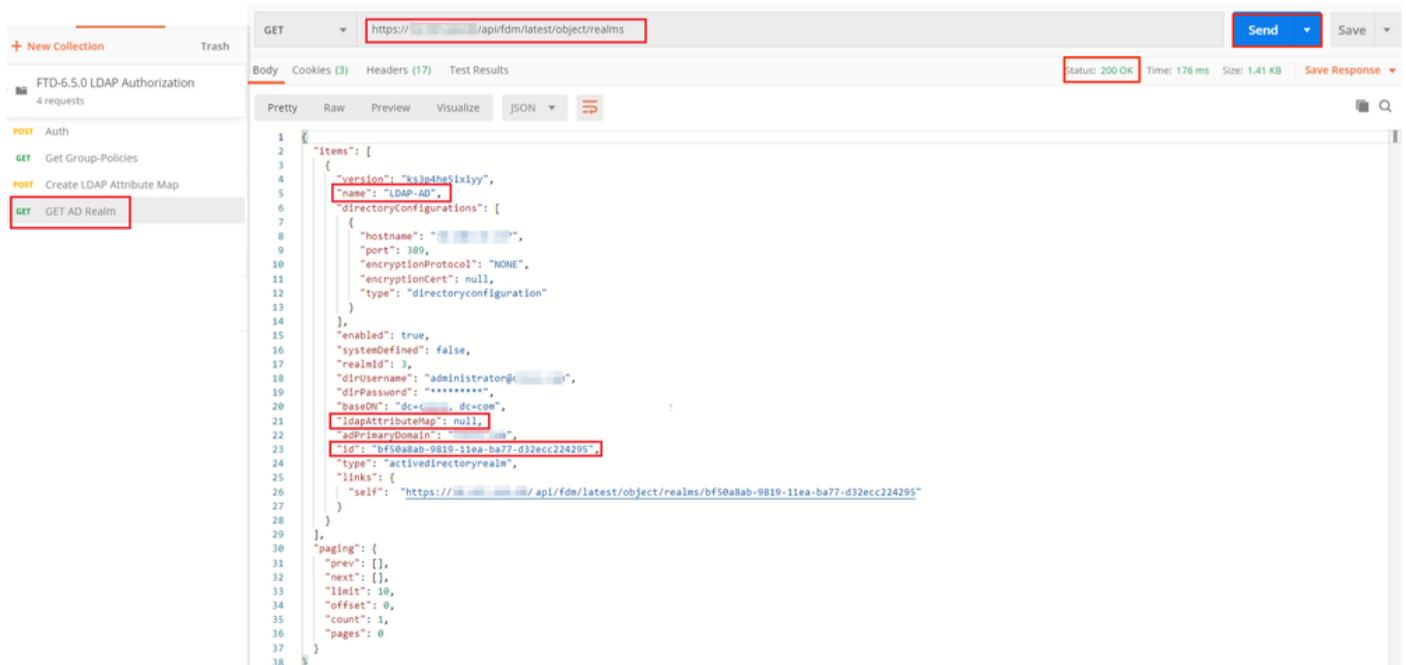
此POST請求的響應看起來與下一個輸出類似：



```
1 {
2   "version": "my43w4d32po",
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 }
```

步驟 7. 新增新的GET請求以獲取FDM上的當前AD領域配置。

獲取當前AD領域配置的URL為：<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      "realmId": 3,
18      "dirUsername": "administrator@...",
19      "dirPassword": "*****",
20      "baseDN": "dc=...,dc=com",
21      "ldapAttributeMap": null,
22      "adPrinmgDomain": "...",
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 }
```



請注意，關鍵字ldapAttributeMap的值為null。

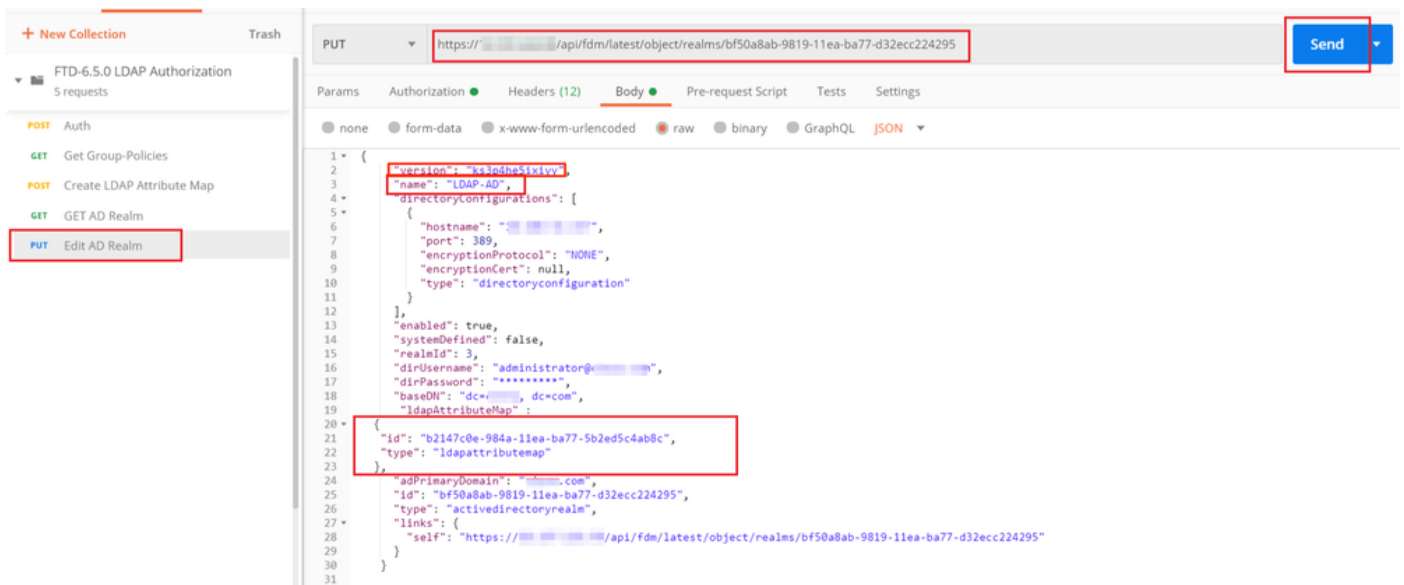
步驟 8. 建立新的PUT請求以編輯AD領域。複製上一步的GET響應輸出，並將其新增到此新PUT請求的正文中。此步驟可用於對當前AD領域設定進行任何修改，例如：更改密碼、IP地址或新增任何鍵(如ldapAttributeMap)的新值。

 注意：複製專案清單的內容，而不是複製整個GET響應輸出非常重要。PUT請求的「請求URL」必須附加有對其進行了更改的對象的專案ID。在本例中，值為：bf50a8ab-9819-11ea-ba77-d32ecc224295

用於編輯當前AD領域配置的URL為：<https://<FTD Management IP>/api/fdm/latest/object/realms/<realm ID>>

PUT請求的主體必須包含以下內容：

版本	從之前的GET請求的響應獲取的版本
id	從之前的GET請求的響應獲取的ID
ldap屬性對映	來自建立LDAP屬性對映請求的響應的ldap-id



此範例中的組態主體為：

<#root>

{



```
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@10.10.10.10",
17  "dirPassword": "*****",
18  "baseDN": "dc=example,dc=com",
19  "ldapAttributeMap": {
20    "version": "nwy43w4jd32po",
21    "name": "Attribute-Map",
22    "id": "b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c",
23    "type": "ldapattributemap"
24  },
25  "adPrimaryDomain": "example.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 }
```


( 可選 )。可以使用PUT請求修改LDAP屬性對映。建立新的PUT請求Edit Attribute-Map，並進行任何更改，如Attribute-Map或memberOf值的名稱。T

在下一個示例中，所有三個組的Idapvalue的值都已從CN=Users更改為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 Params Authorization Headers (11) Body Pre-request Script Tests Settings
1 {
2   "version": "nwy43w4jd32po",
3   "name": "Attribute-Map",
4   "ldapattributemaps": [
5     {
6       "idapname": "memberOf",
7       "ciscoName": "GROUP_POLICY",
8       "valueMappings": [
9         {
10          "idapvalue": "CN=Finance-group,CN=usersgroup,DC=example,DC=com",
11          "ciscoValue": "Finance-Group-Policy",
12          "type": "IdaptoCiscovalueMapping"
13        },
14        {
15          "idapvalue": "CN=HR-group,CN=usersgroup,DC=example,DC=com",
16          "ciscoValue": "HR-Group-Policy",
17          "type": "IdaptoCiscovalueMapping"
18        },
19        {
20          "idapvalue": "CN=IT-group,CN=usersgroup,DC=example,DC=com",
21          "ciscoValue": "IT-Group-Policy",
22          "type": "IdaptoCiscovalueMapping"
23        }
24      ]
25    },
26    {
27      "type": "ldapattributemapping"
28    }
29  ],
30  "id": "b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c",
31  "type": "ldapattributemap",
32  "links": {
33    "self": "https://10.10.10.10/api/fdm/latest/object/ldapattributemaps/b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c"
34  }
35 }
```

( 可選 )。要刪除現有LDAP屬性對映，請建立DELETE請求刪除屬性對映。包括來自上一個HTTP響應的map-id，並將其與刪除請求的基本URL附加。

```
History Collections APIs Delete Attribute-Map DELETE https://10.10.10.10/api/fdm/latest/object/ldapattributemaps/b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c
Auth Params Authorization Headers (7) Body Pre-request Script Tests Settings
KEY VALUE DESCRIPTION
Key Value Description
Response
```

 註：如果memberOf屬性包含空格，則必須對屬性進行URL編碼，以便Web伺服器對其進行分析。否則會收到400錯誤要求HTTP回應。對於包含空格字元的字串，「%20」或「+」可用於避免此錯誤。

步驟 9. 導航回到FDM，選擇「部署」圖示，然後按一下「立即部署」。

## Pending Changes ? ×

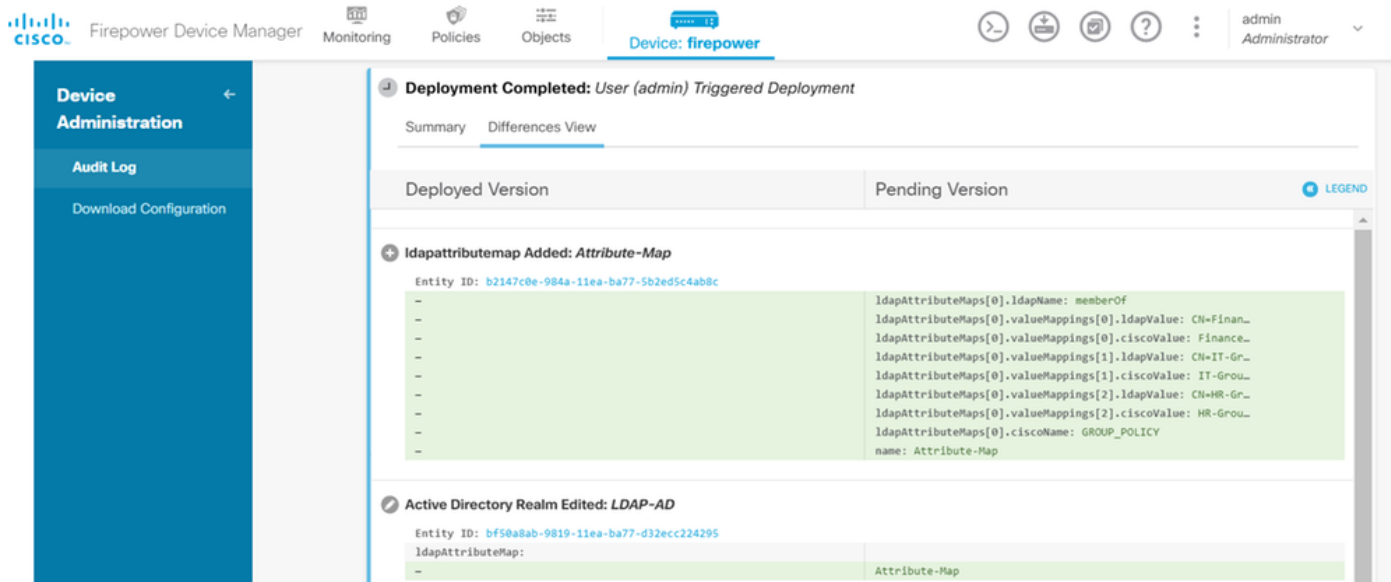
✓ **Last Deployment Completed Successfully**  
17 May 2020 07:46 PM. [See Deployment History](#)

Deployed Version (17 May 2020 07:46 PM)	Pending Version <span>◀ LEGEND</span>
<span>+</span> <b>Idapattributemap Added: Attribute-Map</b>	<pre>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</pre>
<span>⊖</span> <b>Active Directory Realm Edited: LDAP-AD</b>	<pre>ldapAttributeMap: - Attribute-Map</pre>

MORE ACTIONS ▼ CANCEL DEPLOY NOW ▼

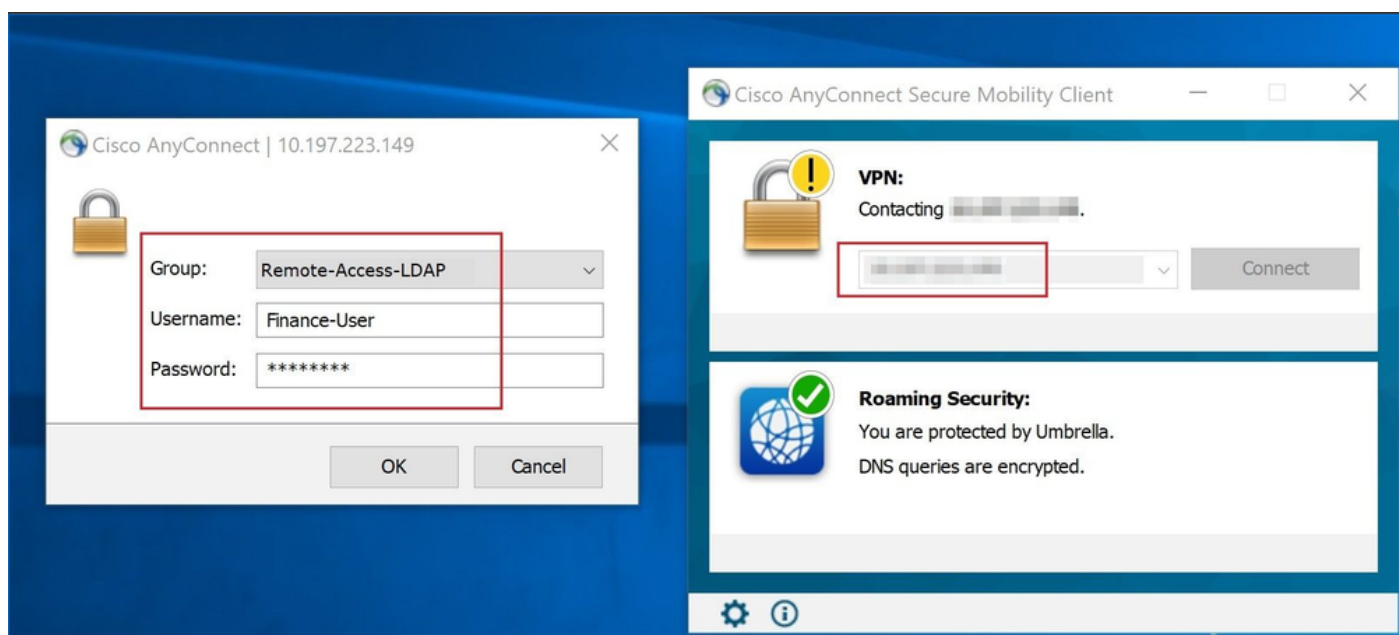
## 驗證

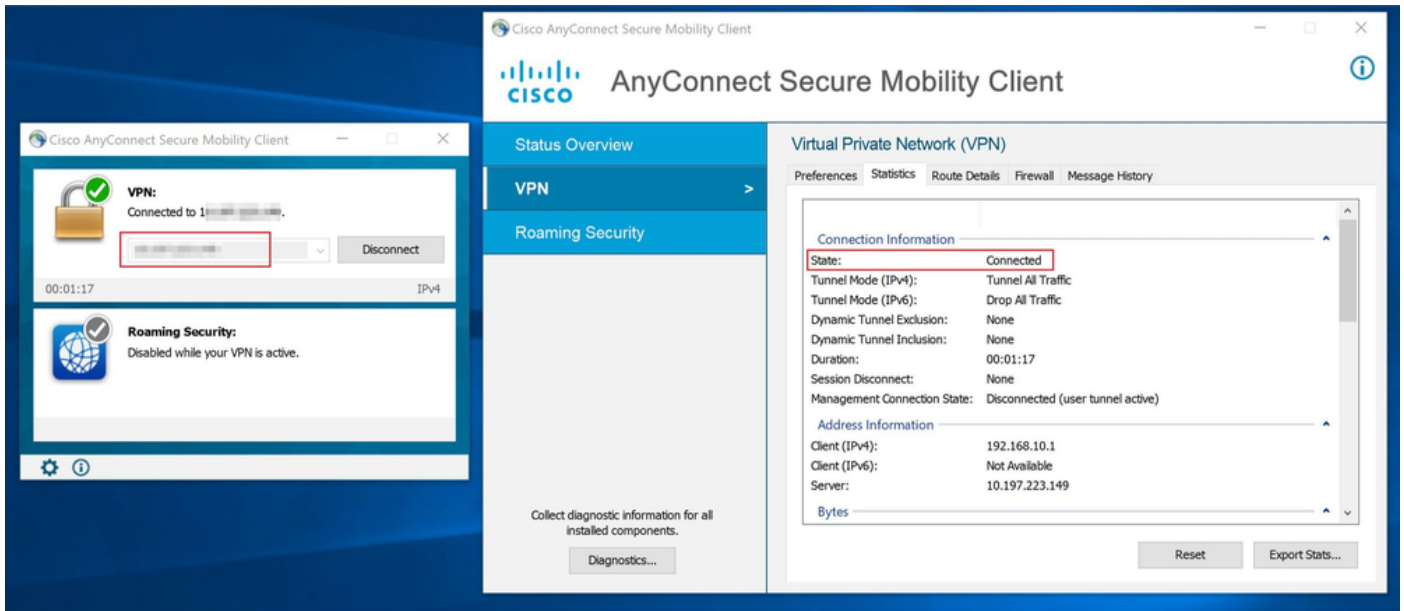
可以在FDM的部署歷史記錄部分驗證部署更改。



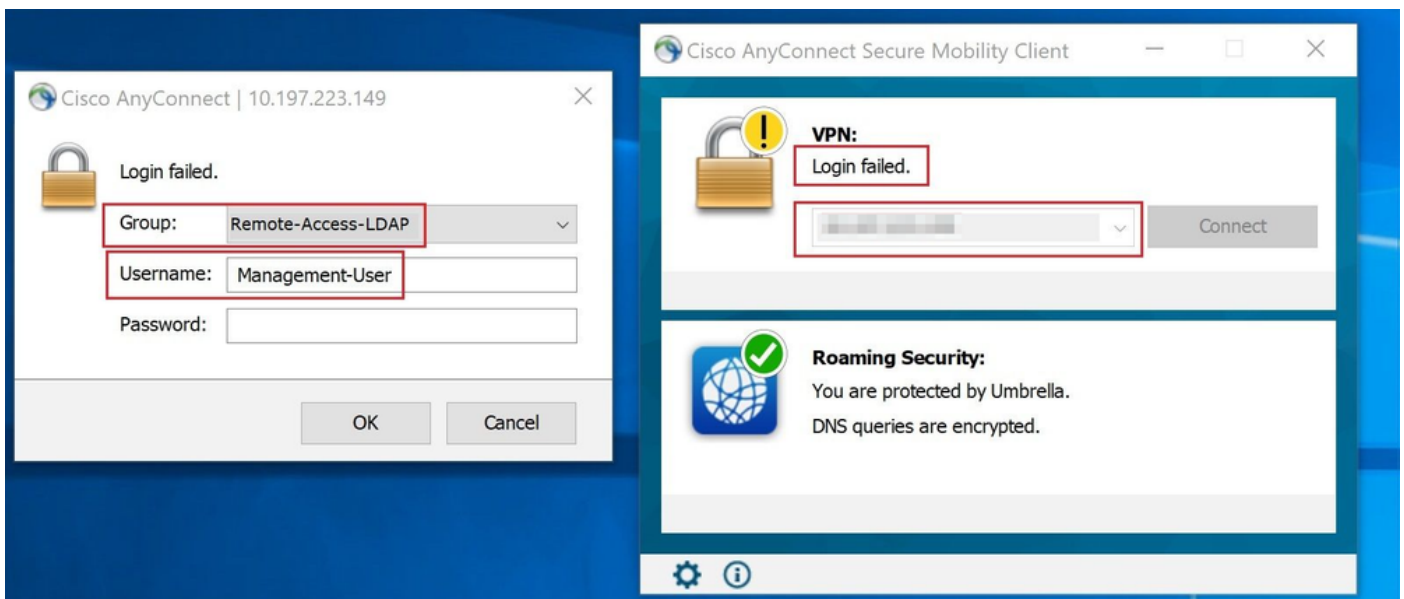
為了測試此配置，請在使用者名稱和密碼欄位中提供AD憑據。

當屬於AD組Finance-Group的使用者嘗試登入時，該嘗試按預期成功。





當屬於AD中Management-Group的使用者嘗試連線到Connection-Profile Remote-Access-LDAP時，由於沒有LDAP屬性對映返回匹配項，因此此使用者在FTD上繼承的組策略是NOACCESS，其vpn-simultaneous-logins設定為0。因此，此使用者的登入嘗試失敗。



可從FTD CLI使用下一個show命令驗證設定：

```
<#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
```


## 疑難排解

配置REST API的最常見問題之一就是不時更新持有者令牌。令牌到期時間在身份驗證請求的響應中給出。如果此時間過期，則可以使用額外的刷新令牌更長時間。刷新令牌也到期後，必須傳送新的身份驗證請求，以檢索新的訪問令牌。

---

 附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

---

 您可以設定各種偵錯層級。預設情況下，使用級別1。如果更改調試級別，調試的詳細程度可能會增加。請謹慎執行此操作，尤其是在生產環境中。

---

FTD CLI上的以下調試有助於解決與LDAP屬性對映相關的問題

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

在此示例中，收集了下一個調試，以演示連線前提及測試使用者時從AD伺服器接收的資訊。

Finance-User的LDAP調試:

<#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調試:

```
<#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
```

## 相關資訊

如需其他協助，請聯絡思科技術協助中心(TAC)。需要有效的支援合約：[思科全球支援聯絡人](#)。

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。