

# FDM에서 관리하는 FTD에서 RAVPN에 대한 LDAP 특성 맵 구성

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[인증 흐름](#)

[LDAP 특성 맵 흐름 설명](#)

[구성](#)

[FDM의 구성 단계](#)

[LDAP 특성 맵에 대한 컨피그레이션 단계](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

---

## 소개

이 문서에서는 LDAP(Lightweight Directory Access Protocol) 서버를 사용하여 RA VPN(Remote Access VPN) 사용자를 인증 및 인증하고 LDAP 서버의 그룹 멤버십에 따라 서로 다른 네트워크 액세스 권한을 부여하는 절차에 대해 설명합니다.

## 사전 요구 사항


### 요구 사항

- 방화벽 장치 관리자(FDM)의 RA VPN 구성에 대한 기본 지식
- FDM의 LDAP 서버 구성에 대한 기본 지식
- REST(Presentational State Transfer) API(Application Program Interface) 및 FDM Rest API 탐색기에 대한 기본 지식
- FDM에서 관리하는 Cisco FTD 버전 6.5.0 이상

### 사용되는 구성 요소

다음 하드웨어 및 소프트웨어 버전의 애플리케이션/장치가 사용되었습니다.

- Cisco FTD 버전 6.5.0, 빌드 115
- Cisco AnyConnect 버전 4.10
- Microsoft AD 서버
- Postman 또는 기타 API 개발 툴

 참고: Microsoft AD Server 및 Postmal 틀에 대한 컨피그레이션 지원은 Cisco에서 제공하지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 인증 흐름



## LDAP 특성 맵 흐름 설명

1. 사용자는 FTD에 대한 원격 액세스 VPN 연결을 시작하고 AD(Active Directory) 계정의 사용자 이름 및 비밀번호를 제공합니다.
2. FTD는 포트 389 또는 636(LDAP over SSL)을 통해 AD 서버에 LDAP 요청을 보냅니다.
3. AD는 사용자와 연결된 모든 특성을 사용하여 FTD에 다시 응답합니다.
4. FTD는 수신된 특성 값을 FTD에 생성된 LDAP 특성 맵과 일치시킵니다. 이것은 승인 프로세스입니다.
5. 그런 다음 사용자는 LDAP 특성 맵의 memberOf 특성과 일치하는 Group-Policy의 설정을 연결하고 상속합니다.

이 문서에서는 AnyConnect 사용자의 권한 부여가 memberOf LDAP 특성을 사용하여 수행됩니다.

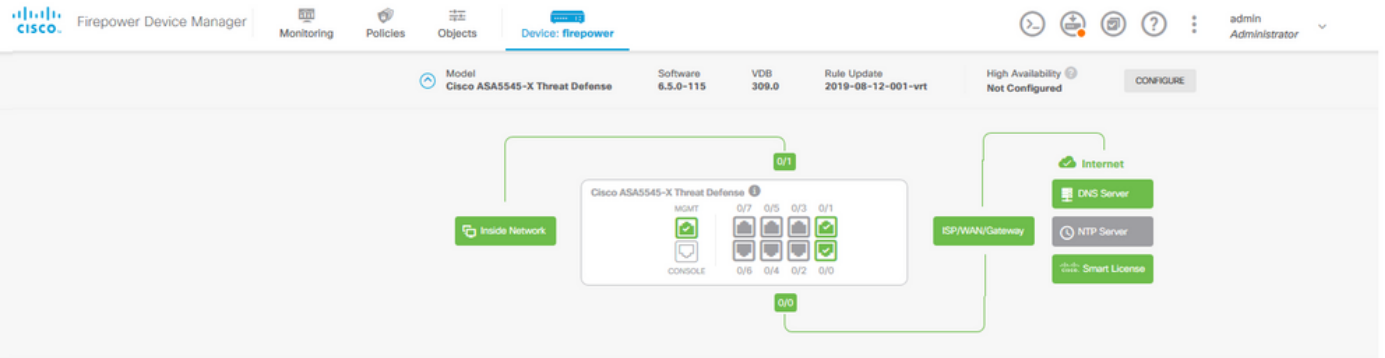
- 각 사용자에게 대한 LDAP 서버의 memberOf 특성은 FTD의 IdapValue 엔터티에 매핑됩니다. 사용자가 일치하는 AD 그룹에 속하는 경우, 해당 IdapValue와 연결된 그룹 정책은 사용자가 상속합니다.
- 사용자의 memberOf 특성 값이 FTD의 IdapValue 엔터티와 일치하지 않는 경우 선택한 연결 프로파일에 대한 기본 그룹 정책이 상속됩니다. 이 예에서는 NOACCESS Group-Policy가 상속됩니다.

## 구성

FDM에서 관리하는 FTD에 대한 LDAP 속성 맵이 REST API로 구성됩니다.

### FDM의 구성 단계

1단계. 디바이스가 Smart Licensing에 등록되었는지 확인합니다.



<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>

2단계. FDM에서 AnyConnect 라이선스가 활성화되어 있는지 확인합니다.

**Smart License**

CONNECTED SUFFICIENT LICENSE  
 Last sync: 11 Oct 2019 09:33 AM  
 Next sync: 11 Oct 2019 09:43 AM

**SUBSCRIPTION LICENSES INCLUDED**


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

**PERPETUAL LICENSES INCLUDED**

- Base License**: Enabled ALWAYS. Includes: Base Firewall Capabilities, Application Visibility and Control.

3단계. 토큰에서 Export-controlled 기능이 활성화되었는지 확인합니다.

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

 참고: 이 문서에서는 RA VPN이 이미 구성되어 있다고 가정합니다. FDM에서 관리하는 FTD에서 RAVPN을 구성하는 [방법에 대한 자세한 내용은 다음 문서를 참조하십시오.](#)

4단계. Remote Access VPN(원격 액세스 VPN) > Group Policies(그룹 정책)로 이동합니다.



<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>

5단계. Group Policies(그룹 정책)로 이동합니다. 각 AD 그룹에 대해 다른 그룹 정책을 구성하려면 '+'를 클릭합니다. 이 예에서는 Group-policies Finance-Group-Policy, HR-Group-Policy 및 IT-Group-Policy가 다른 서브넷에 액세스하도록 구성됩니다.

The screenshot shows the 'Add Group Policy' configuration window. The 'Name' field is set to 'Finance-Group-Policy' and is highlighted with a red box. The 'Description' field contains 'Finance User Group'. The 'DNS Server' dropdown is set to 'Select DNS Group'. The 'Banner Text for Authenticated Clients' field contains a message: 'This message will be shown to successfully authenticated endpoints in the beginning of their VPN session'. The 'Default domain' field is empty. The 'AnyConnect client profiles' dropdown is set to 'All'. The 'OK' button is highlighted with a red box. In the background, the 'Group Policies' menu item is highlighted with a red box, and a '+' icon is also highlighted with a red box.

Finance-Group-Policy에는 다음 설정이 있습니다.

```
<#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>
```

마찬가지로, HR-Group-Policy에는 다음 설정이 있습니다.

<#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>
```

마지막으로, IT 그룹 정책에는 다음 설정이 있습니다.

```
<#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>
```

6단계. Group-Policy NOACCESS(그룹 정책 NOACCESS)를 생성하고 Session Settings(세션 설정)로 이동하고 Simultaneous Login per User(사용자당 동시 로그인) 옵션의 선택을 취소합니다. 이렇게 하면 vpn-simultaneous-logins 값이 0으로 설정됩니다.

0으로 설정된 경우 Group-Policy의 vpn-simultaneous-logins 값은 사용자의 VPN 연결을 즉시 종료합니다. 이 메커니즘은 구성된 AD 사용자 그룹(이 예에서는 Finance, HR 또는 IT)이 아닌 다른 AD 사용자 그룹에 속한 사용자가 FTD에 성공적으로 연결하고 허용된 사용자 그룹 계정에만 사용할 수 있는 보안 리소스에 액세스하는 것을 방지하기 위해 사용됩니다.

올바른 AD 사용자 그룹에 속한 사용자는 FTD의 LDAP 특성 맵과 일치하고 매핑된 그룹 정책을 상속하며, 허용된 그룹에 속하지 않은 사용자는 연결 프로파일의 기본 그룹 정책을 상속합니다. 이 경

우 NOACCESS입니다.

### 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 그룹 정책의 설정은 다음과 같습니다.

```
<#root>
```

```
firepower#
```

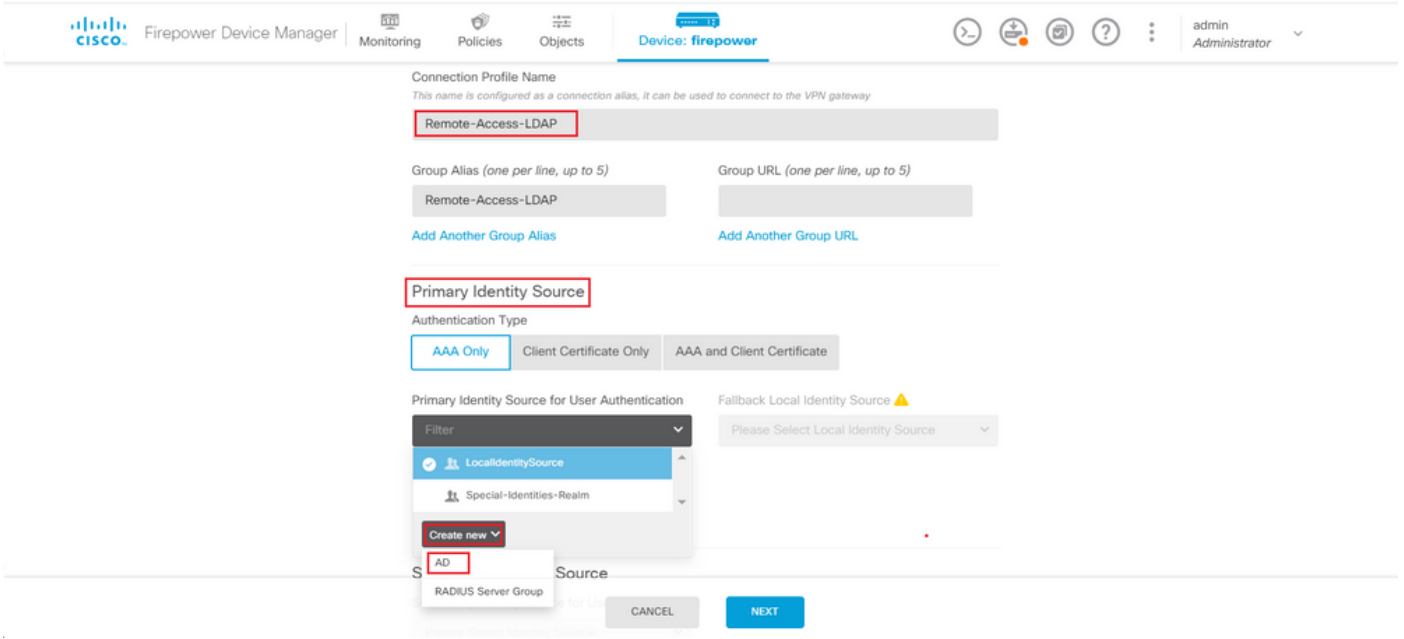
```
show run group-policy NOACCESS
```

```
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
```

7단계. Connection Profiles(연결 프로파일)로 이동하여 Connection-Profile(연결 프로파일)을 생성합니다. 이 예에서 프로파일 이름은 Remote-Access-LDAP입니다. Primary Identity Source AAA Only를 선택하고 새 인증 서버 유형 AD를 만듭니다.



AD 서버의 정보를 입력합니다.

- 디렉토리 사용자 이름
- 디렉터리 암호
- 기본 DN
- AD 주 도메인
- 호스트 이름/IP 주소
- 포트
- 암호화 유형

# 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

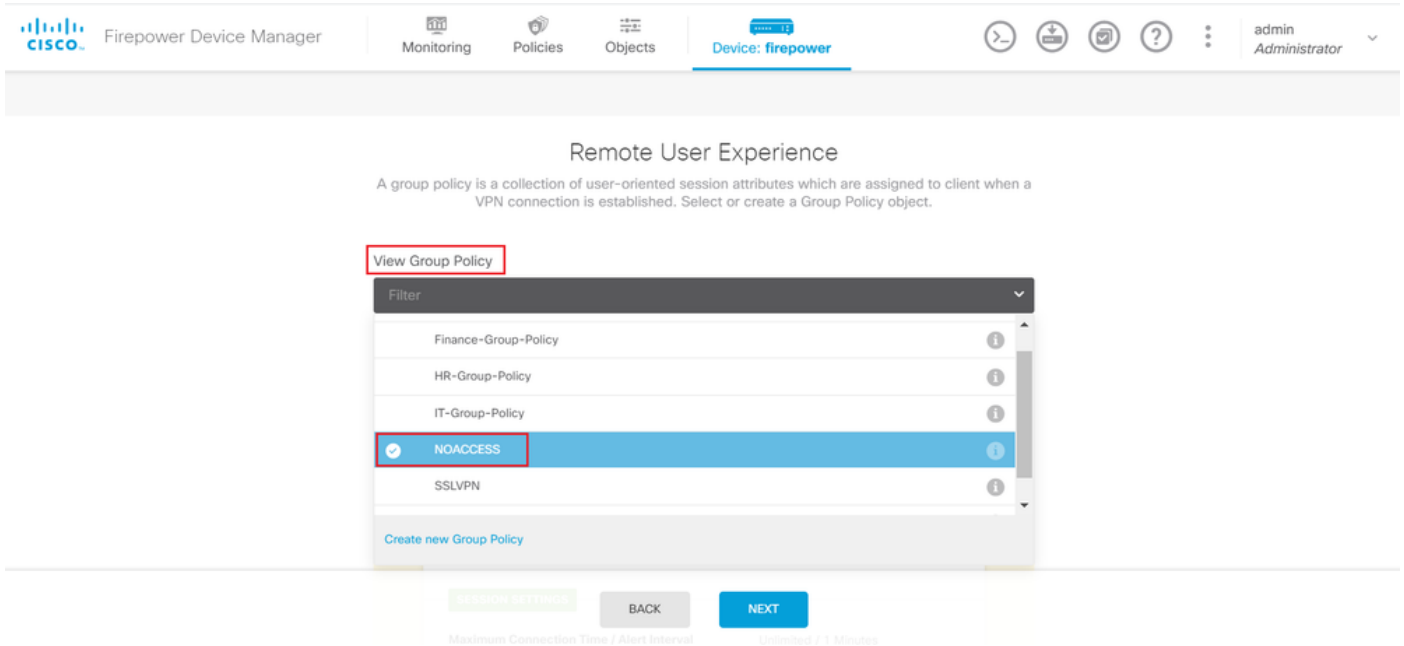
TEST

[Add another configuration](#)

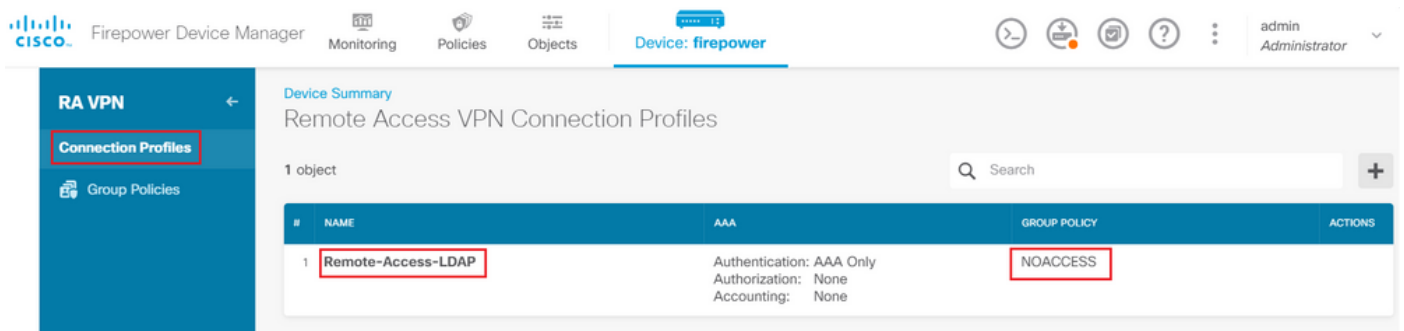
CANCEL

OK

Next(다음)를 클릭하고 이 연결 프로파일의 기본 Group-Policy(그룹 정책)로 NOACCESS를 선택합니다.



모든 변경 사항을 저장합니다. 이제 RA VPN 컨피그레이션에서 연결 프로파일 Remote-Access-LDAP를 볼 수 있습니다.

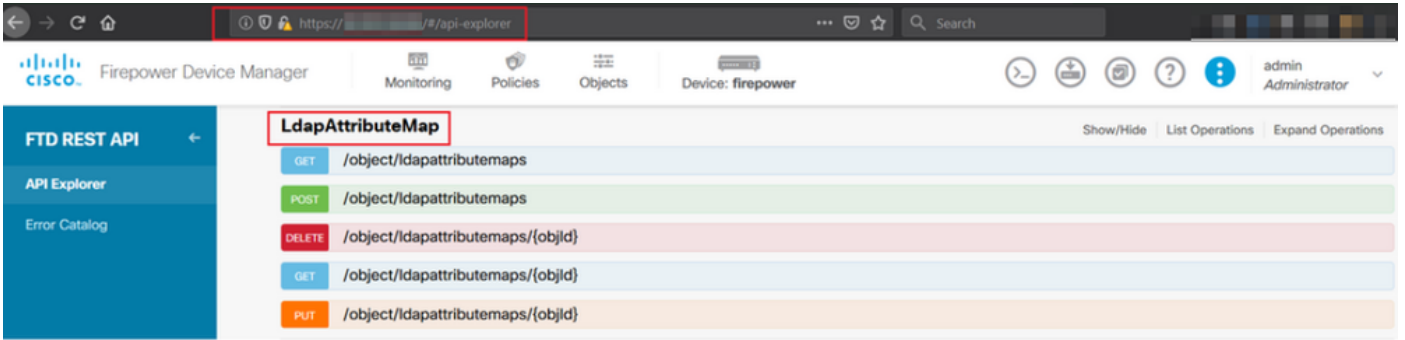


LDAP 특성 맵에 대한 컨피그레이션 단계

1단계. FTD의 API Explorer를 시작합니다.

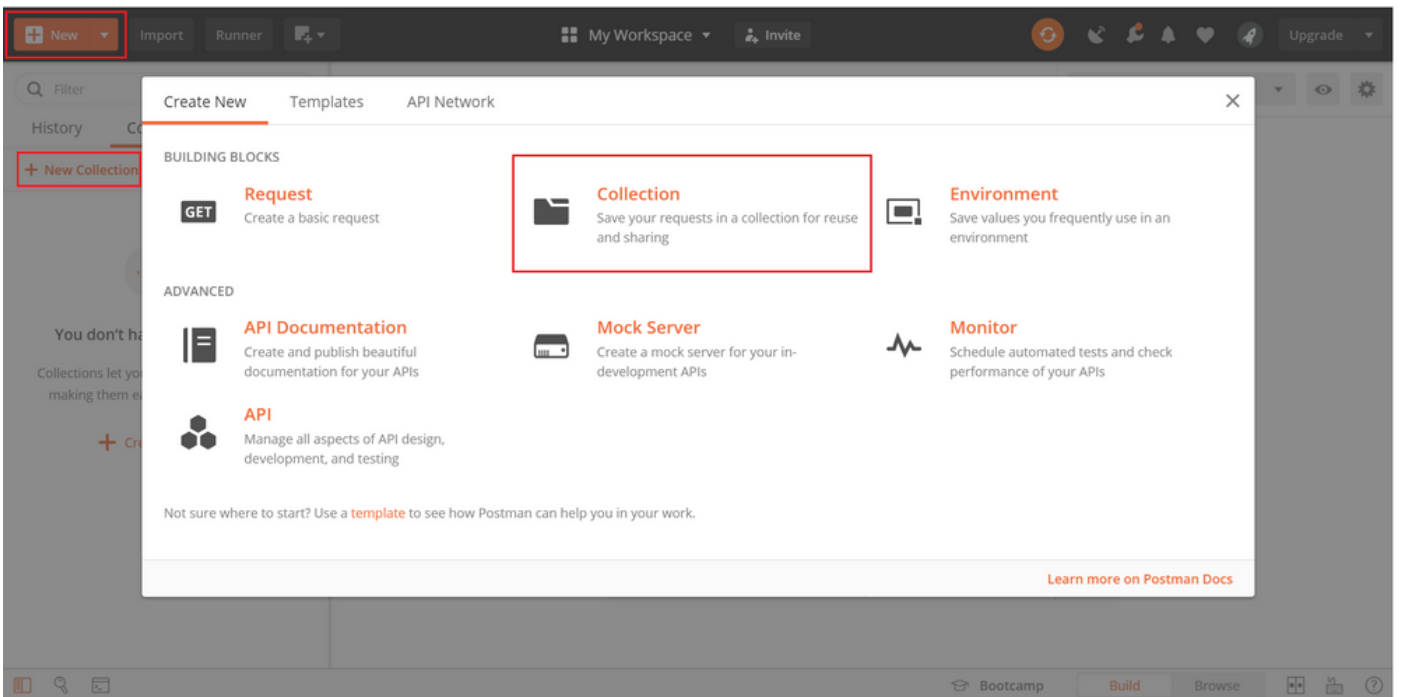
API 탐색기에는 FTD에서 사용 가능한 API의 전체 목록이 포함됩니다. <https://<FTD Management IP>/api-explorer>로 이동합니다.

아래로 스크롤하여 LdapAttributeMap 섹션으로 이동한 다음 클릭하여 지원되는 모든 옵션을 확인합니다.

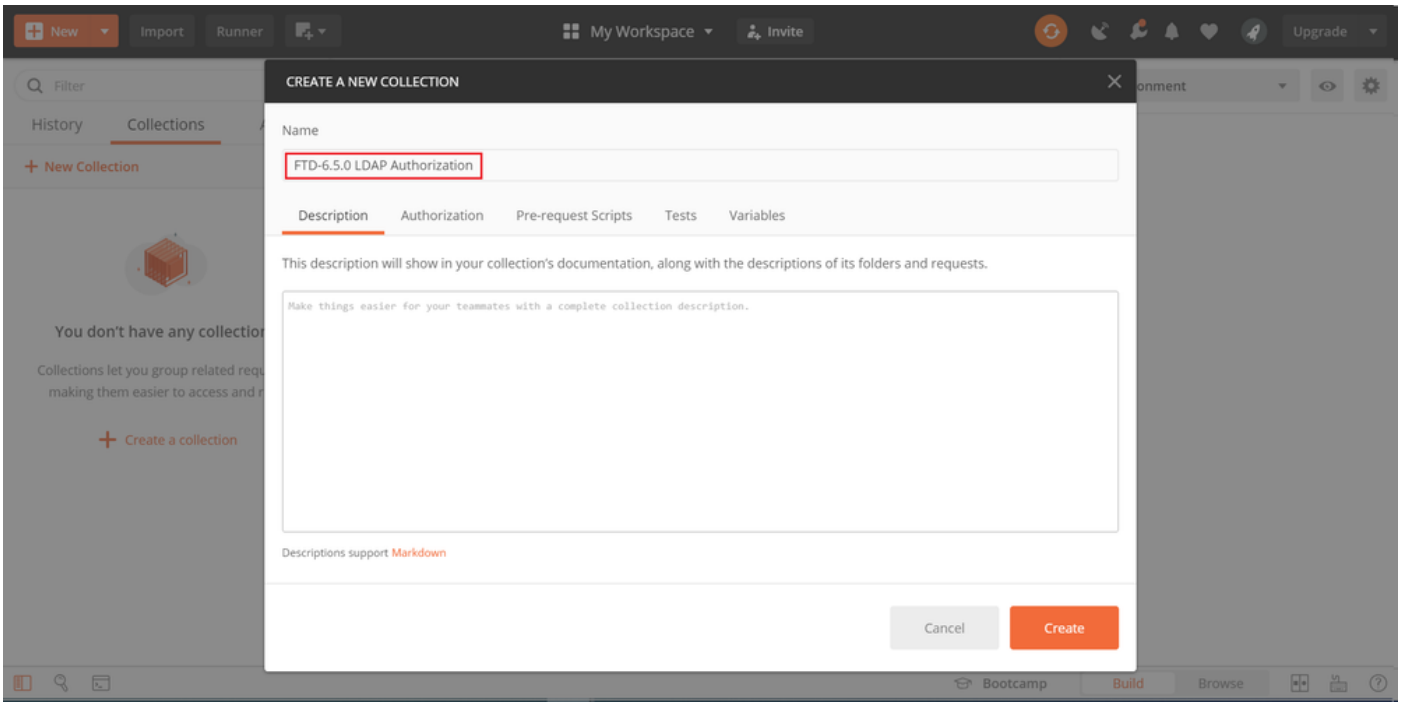


참고: 이 예에서는 API 툴로 Postman을 사용하여 LDAP 특성 맵을 구성합니다.

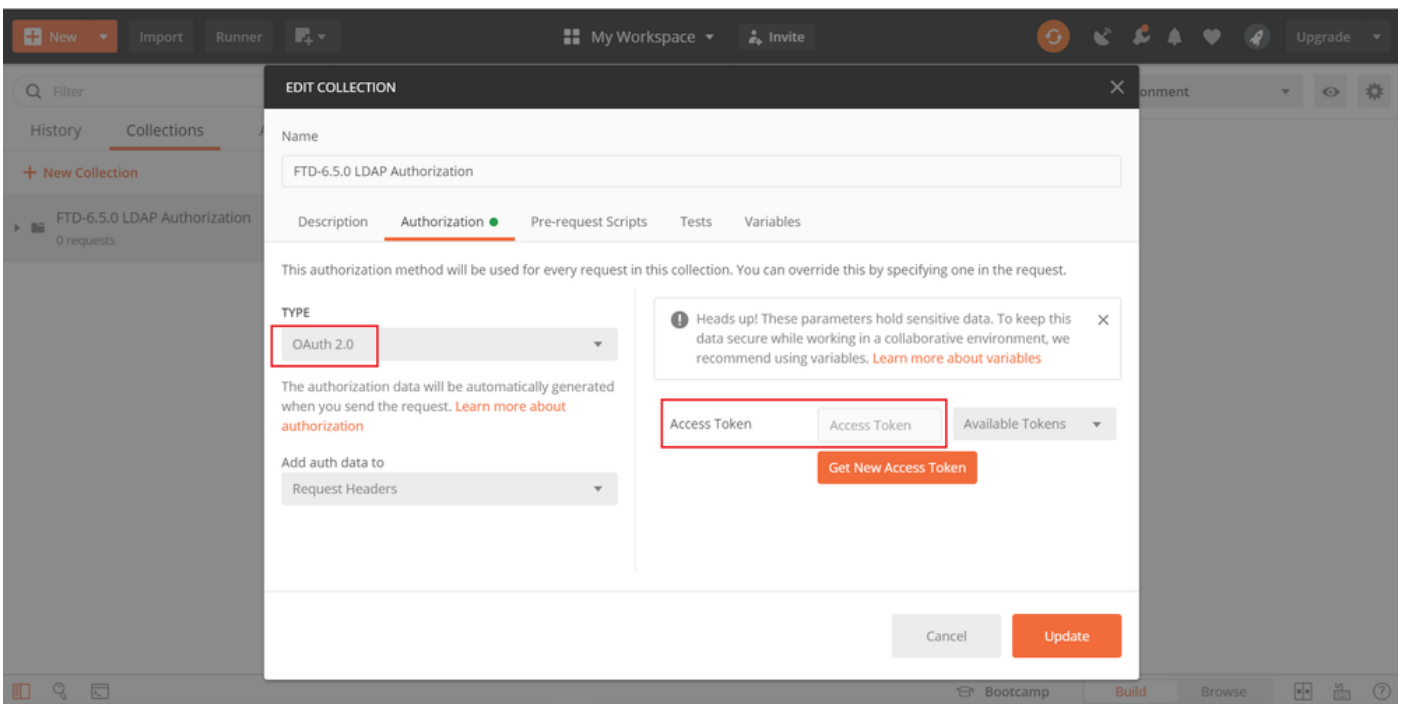
2단계.LDAP 권한 부여를 위한 Postman 컬렉션을 추가합니다.



이 컬렉션의 이름을 입력하십시오.



### 편집 Authorization(권한 부여) 탭 및 선택 OAuth 2.0 유형



3단계. File(파일) > Settings(설정)로 이동하여 FTD로 API 요청을 전송할 때 SSL 핸드셰이크 오류가 발생하지 않도록 SSL 인증서 검증을 끕니다. 이는 FTD가 자체 서명 인증서를 사용하는 경우에 수행됩니다.



# 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

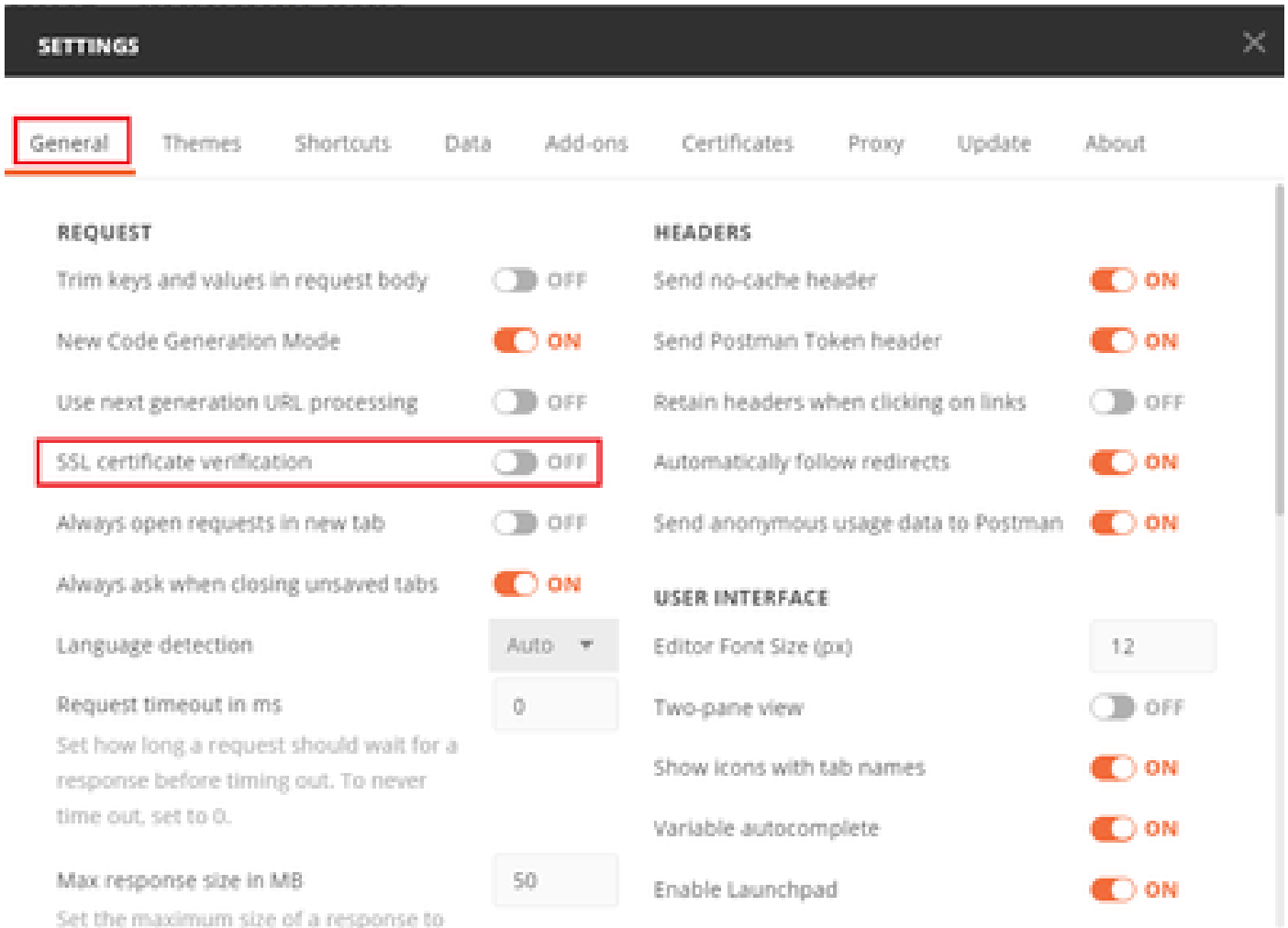
Settings Ctrl+Comma

Close Window Ctrl+Shift+W

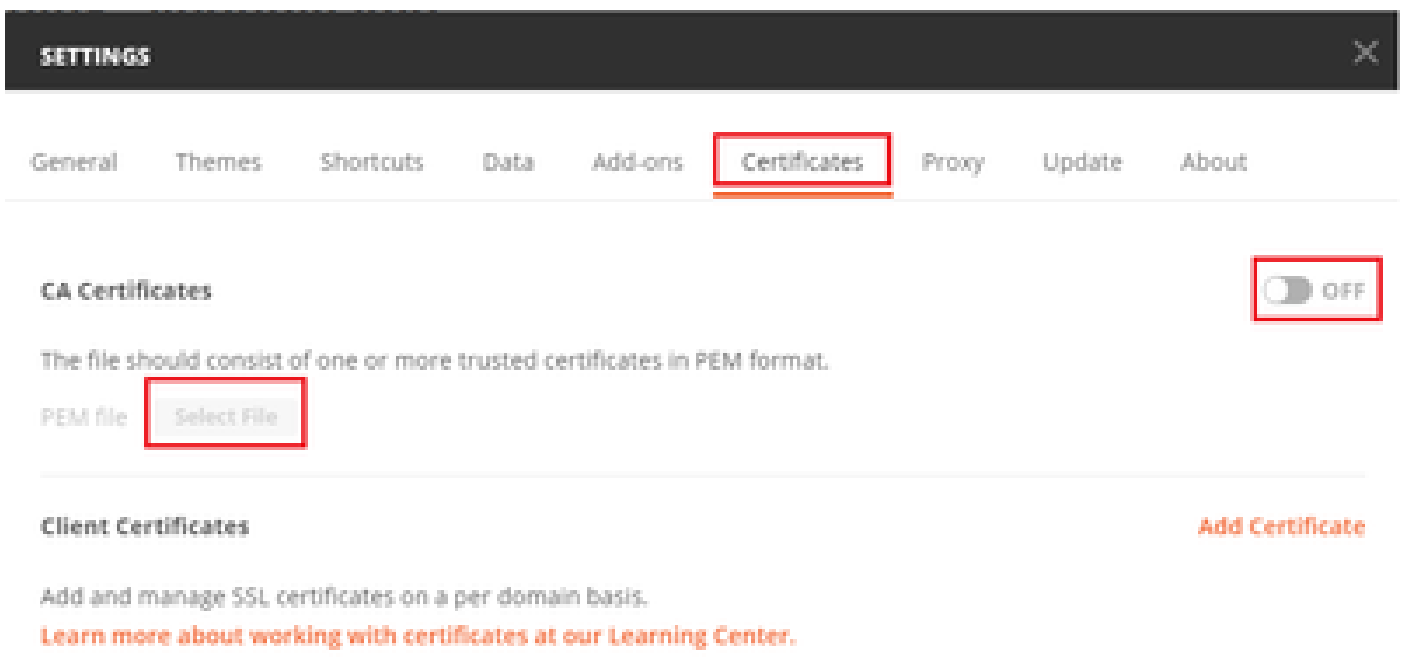
Close Tab Ctrl+W

Force Close Tab Alt+Ctrl+W

Exit



또는 FTD에서 사용하는 인증서를 Settings(설정)의 Certificate(인증서) 섹션에서 CA 인증서로 추가할 수 있습니다.





4단계. 모든 POST/GET 요청을 승인하는 토큰을 얻기 위해 FTD에 로그인 POST 요청을 생성하려면 새 POST 요청 인증을 추가합니다.

**+ 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

수락 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

다른 모든 요청의 경우 각 Header(헤더) 탭으로 이동하고 json을 기본 데이터 유형으로 사용할 REST API 요청에 대한 Preset Header-LDAP(Header-LDAP) 값을 선택합니다.

토큰을 얻기 위한 POST 요청의 본문에는 다음 항목이 포함되어야 합니다.

유형	raw - JSON(애플리케이션/json)
부여_유형	암호
사용자 이름	FTD에 로그인하기 위한 관리자 사용자 이름
암호	관리자 사용자 계정과 연결된 비밀번호

```
{
  "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

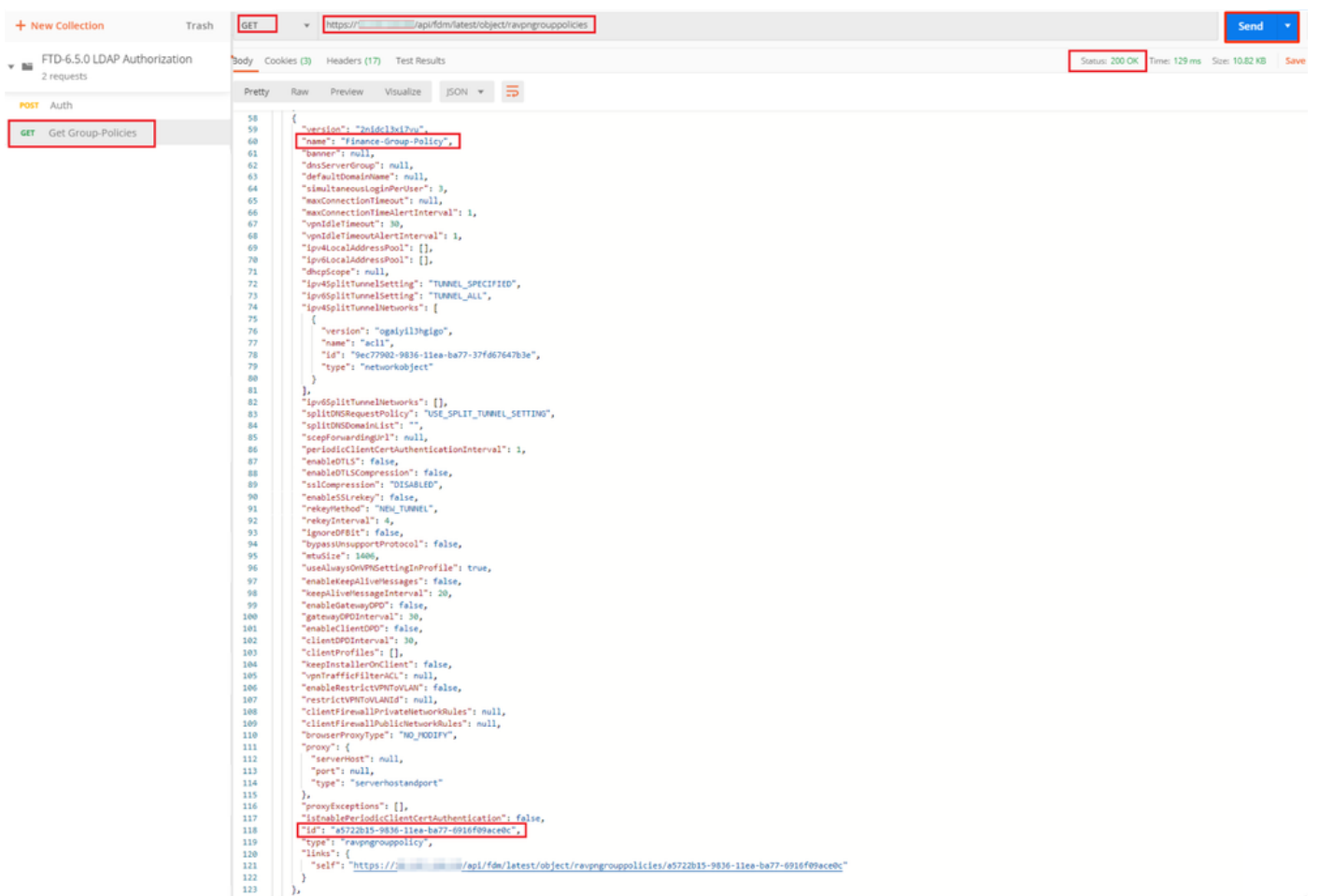
```
1 {
2   "grant_type": "password",
3   "username": "admin",
4   "password": "..."
5 }
```



5단계. 새 GET 요청 Get Group-Policies를 추가하여 Group-Policy 상태 및 설정을 가져옵니다. 구성된 각 그룹 정책(이 예에서는 Finance-Group-Policy, HR-Group-Policy 및 IT-Group-Policy)에 대해 다음 단계에서 사용할 이름 및 ID를 수집합니다.

구성된 그룹 정책을 가져오는 URL은 다음과 같습니다. <https://<FTD Management IP>/api/fdm/latest/object/ravpngrouppolicies>

다음 예에서는 Group-Policy Finance-Group-Policy가 강조 표시됩니다.



6단계. LDAP 특성 맵을 생성하려면 새 POST 요청을 추가하고 LDAP 특성 맵을 만듭니다. 이 문서에서는 LdapAttributeMapping 모델이 사용됩니다. 다른 모델에서도 유사한 작업 및 방법으로 특성 맵을 만들 수 있습니다. 이러한 모델의 예는 이 문서의 앞부분에서 설명한 api-explorer에서 사용할 수 있습니다.

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.

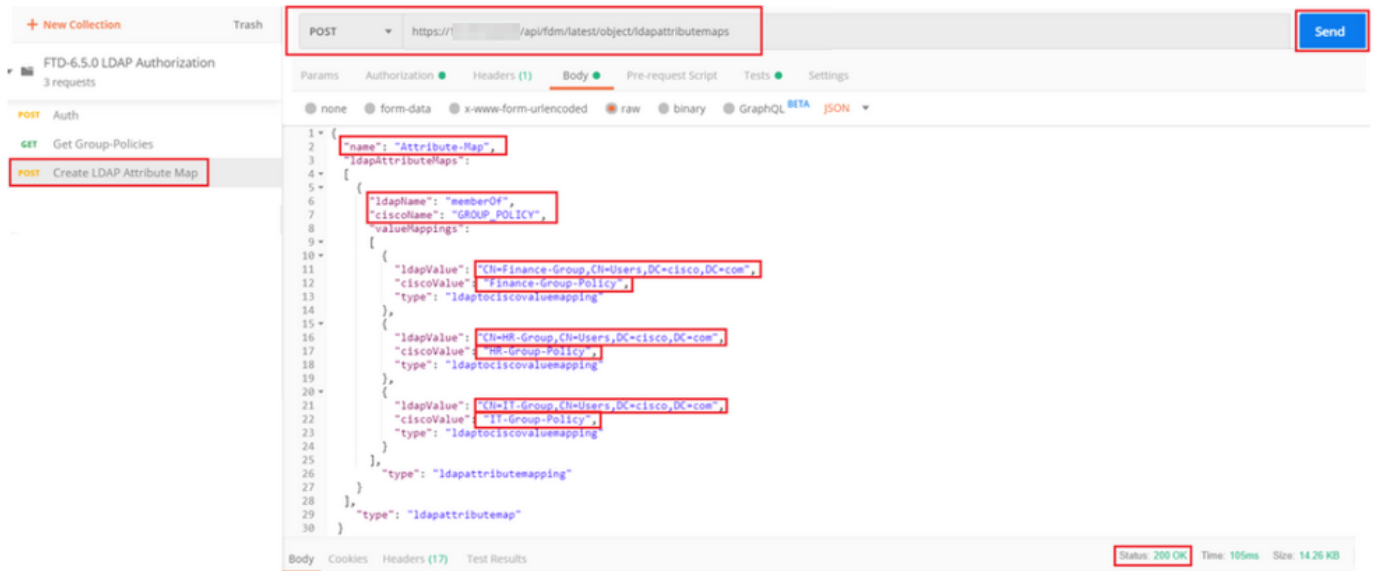
**Response Class (Status 200)**

Model	Example Value
<p><b>LdapAttributeMapping</b></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><b>ldapName</b> (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><b>ciscoName</b> (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><b>valueMappings</b> (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><b>type</b> (string): ldapattributemapping</p>	
<p><b>LdapAttributeToGroupPolicyMapping</b></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><b>ldapName</b> (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><b>valueMappings</b> (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><b>type</b> (string): ldapattributetogrouppolicymapping</p>	

LDAP 특성 맵을 게시하는 URL은 다음과 같습니다. <https://<FTD Management IP>/api/fdm/latest/object/ldapattributemaps>

POST 요청의 본문에는 다음이 포함되어야 합니다.

이름	LDAP Attribute-Map 이름
유형	ldap특성매핑
ldap이름	구성원
시스코 이름	그룹 정책
ldap값	AD의 사용자에게 대한 memberOf 값
시스코 밸류	FTD의 각 사용자 그룹에 대한 그룹 정책 이름




POST 요청의 본문에는 memberOf 값을 기반으로 특정 그룹 정책을 AD 그룹에 매핑하는 LDAP 특성 맵 정보가 포함됩니다.

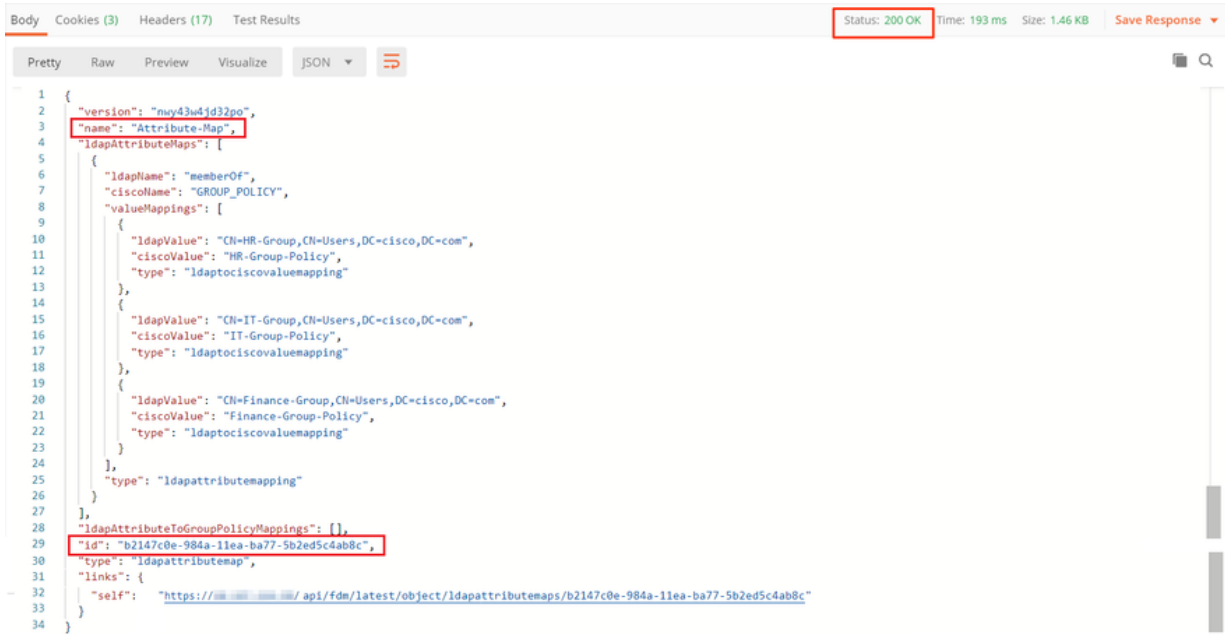
```

{
  "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"
}

```

 참고: memberOf 필드는 dsquery 명령을 사용하여 AD 서버에서 검색되거나 FTD의 LDAP 디버거에서 가져올 수 있습니다. 디버그 로그에서 memberOf value: 필드를 찾습니다.

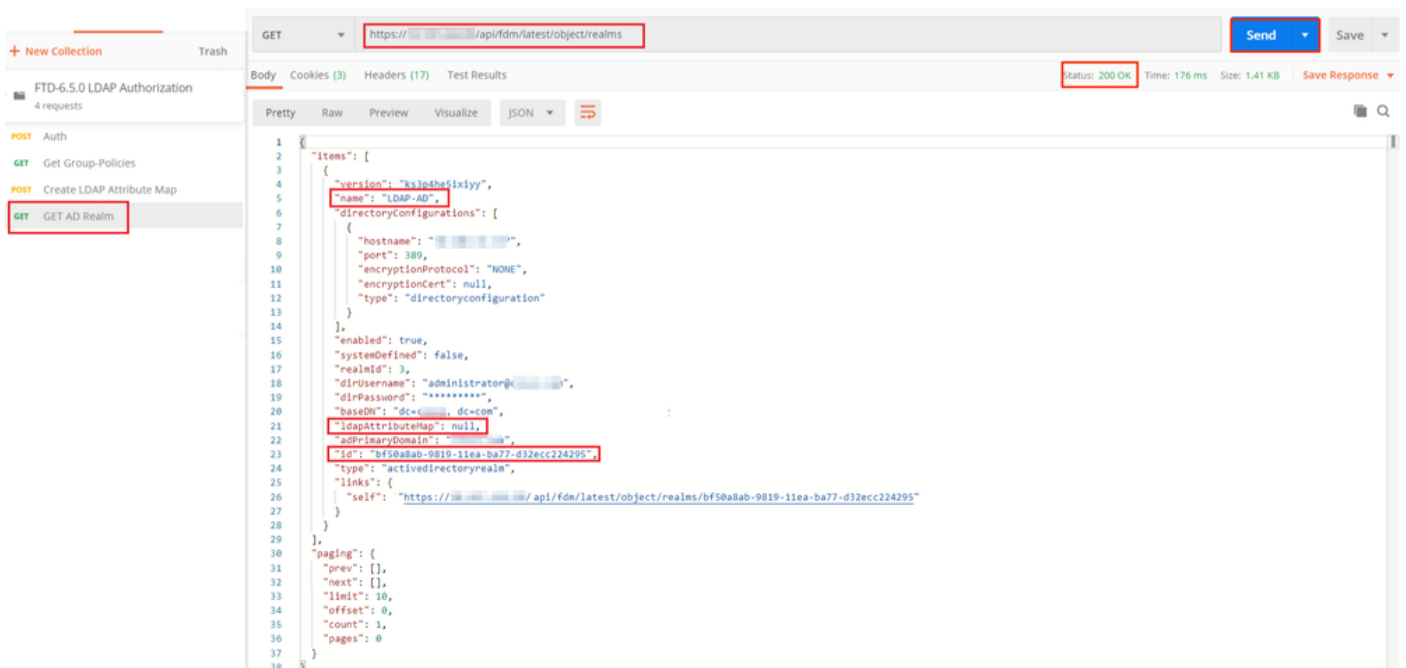
이 POST 요청의 응답은 다음 출력과 유사합니다.



```
1 {
2   "version": "nv43u4d32po",
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 }
```

7단계. FDM에서 현재 AD 영역 구성을 가져오려면 새 GET 요청을 추가합니다.

현재 AD 영역 컨피그레이션을 가져오는 URL은 다음과 같습니다. <https://<FTD Management IP>/api/fdm/latest/object/realms>




```
1 GET https://.../api/fdm/latest/object/realms
2 Status: 200 OK Time: 176 ms Size: 1.41 KB Save Response
3
4 Body
5 Pretty Raw Preview Visualize JSON
6
7 {
8   "items": [
9     {
10      "version": "ksjodshatixiyy",
11      "name": "LDAP-AD",
12      "directoryConfigurations": [
13        {
14          "hostname": "...",
15          "port": 389,
16          "encryptionProtocol": "NONE",
17          "encryptionCert": null,
18          "type": "directoryconfiguration"
19        }
20      ],
21      "enabled": true,
22      "systemDefined": false,
23      "realmId": 9,
24      "dirUsername": "administrator@...",
25      "dirPassword": "*****",
26      "baseDN": "dc=...,dc=com",
27      "ldapAttributeMap": null,
28      "adPrimaryDomain": "...",
29      "id": "bf50a8ab-9819-11ea-ba77-d32ecc224295",
30      "type": "activedirectoryrealm",
31      "links": {
32        "self": "https://.../api/fdm/latest/object/realms/bf50a8ab-9819-11ea-ba77-d32ecc224295"
33      }
34    }
35  ],
36  "paging": {
37    "prev": [],
38    "next": [],
39    "limit": 10,
40    "offset": 0,
41    "count": 1,
42    "pages": 0
43  }
44 }
```



키 ldapAttributeMap의 값이 null임을 확인합니다.

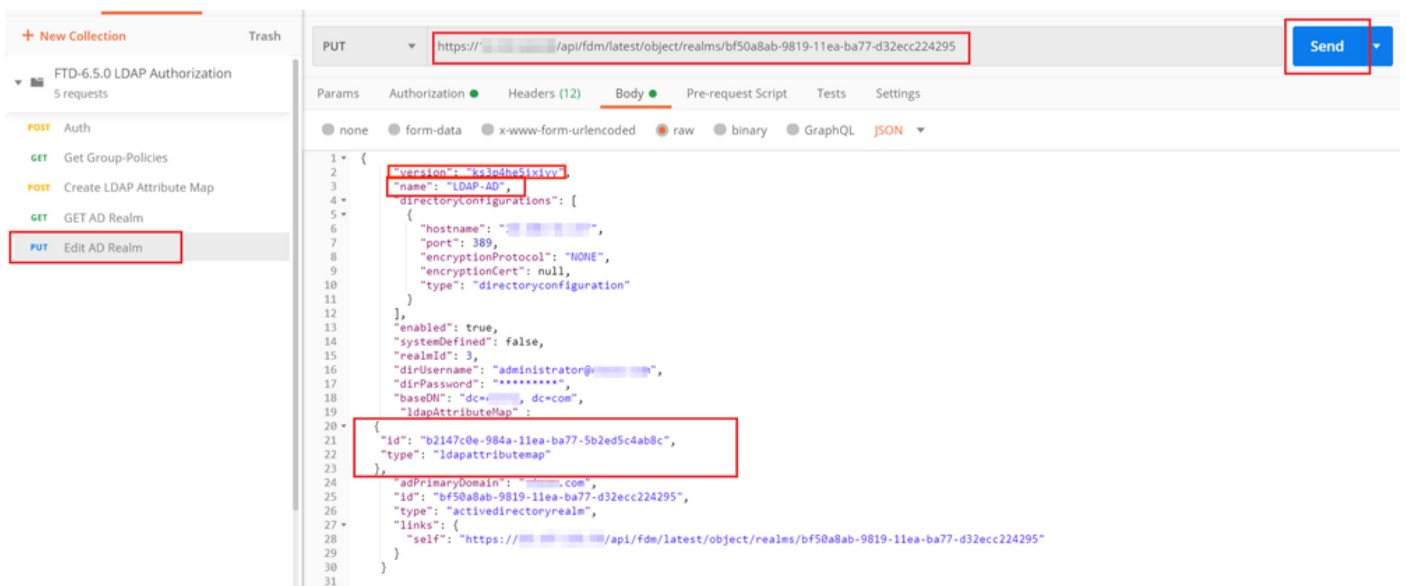
8단계. AD 영역을 편집할 새 PUT 요청을 생성합니다. 이전 단계의 GET 응답 출력을 복사하여 이 새 PUT 요청의 본문에 추가합니다. 이 단계는 현재 AD 영역 설정을 수정하는 데 사용할 수 있습니다. 예를 들어 비밀번호 변경, IP 주소 또는 ldapAttributeMap과 같은 키에 새 값을 추가할 수 있습니다.

 참고: 전체 GET 응답 출력이 아닌 항목 목록의 내용을 복사하는 것이 중요합니다. PUT 요청의 요청 URL에는 변경이 수행되는 객체의 항목 ID가 추가되어야 합니다. 이 예에서 값은 bf50a8ab-9819-11ea-ba77-d32ecc224295입니다

현재 AD 영역 구성을 편집할 URL은 <https://<FTD Management IP>/api/fdm/latest/object/realms/<realm ID>>입니다.

PUT 요청의 본문에는 다음이 포함되어야 합니다.

버전	이전 GET 요청의 응답에서 얻은 버전
ID	이전 GET 요청의 응답에서 얻은 ID
ldap특성맵	ldap-id from Response of Create LDAP Attribute Map request(LDAP 특성 맵 생성 요청의 응답)



```

1 * {
2   {
3     "version": "ks3dha5iviv",
4     "name": "LDAP-AD",
5     "directoryConfigurations": [
6       {
7         "hostname": "10.10.10.10",
8         "port": 389,
9         "encryptionProtocol": "NONE",
10        "encryptionCert": null,
11        "type": "directoryconfiguration"
12      }
13    ],
14    "enabled": true,
15    "systemDefined": false,
16    "realmId": 3,
17    "dirUsername": "administrator@10.10.10.10",
18    "dirPassword": "*****",
19    "baseDN": "dc=10.10.10.10, dc=com",
20    "ldapAttributeMap": {
21      "id": "b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c",
22      "type": "ldapattributemap"
23    },
24    "adPrimaryDomain": "10.10.10.10.com",
25    "id": "bf50a8ab-9819-11ea-ba77-d32ecc224295",
26    "type": "activedirectoryrealm",
27    "links": {
28      "self": "https://10.10.10.10/api/fdm/latest/object/realms/bf50a8ab-9819-11ea-ba77-d32ecc224295"
29    }
30  }
31 }
  
```

이 예의 컨피그레이션 본문은 다음과 같습니다.

```
<#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"

  }
}
```

이 요청에 대한 응답 본문에서 ldapAttributeMap ID가 일치하는지 확인합니다.

```

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": "200.100.100.100",
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://200.100.100.100/api/fdm/latest/object/realm/bf50a8ab-9819-11ea-ba77-d32ecc224295"
30  }
31 }

```

(선택 사항). LDAP 특성 맵은 PUT 요청으로 수정할 수 있습니다. 새 PUT 요청 Edit Attribute-Map을 생성하고 Attribute-Map 또는 memberOf 값의 이름과 같은 변경 사항을 적용합니다. T

다음 예에서 Idapvalue 값은 세 그룹 모두에 대해 CN=Users에서 CN=UserGroup으로 수정되었습니다.

```

FTD-6.5.0 LDAP Authorization
PUT https://200.100.100.100/api/fdm/latest/object/ldapattributemaps/b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c
Params Authorization Headers (11) Body Pre-request Scripts Tests Settings
none form-data x-www-form-urlencoded raw binary GraphQL JSON
1 {
2   "version": "nwy43w4jd32po",
3   "name": "Attribute-Map",
4   "ldapAttributeMap": {
5     "ldapname": "memberOf",
6     "cisname": "memberOf",
7     "valueMappings": [
8       {
9         "idapvalue": "Cwiflance-group,Cwiflance-group,Cwiflance-group,Cwiflance-group",
10        "cisvalue": "memberOf-policy",
11        "type": "ldaptoctisovalmapping"
12      },
13      {
14        "idapvalue": "Cwifl-group,Cwifl-group,Cwifl-group,Cwifl-group",
15        "cisvalue": "memberOf-policy",
16        "type": "ldaptoctisovalmapping"
17      },
18      {
19        "idapvalue": "Cwifl-group,Cwifl-group,Cwifl-group,Cwifl-group",
20        "cisvalue": "memberOf-policy",
21        "type": "ldaptoctisovalmapping"
22      },
23      {
24        "idapvalue": "Cwifl-group,Cwifl-group,Cwifl-group,Cwifl-group",
25        "cisvalue": "memberOf-policy",
26        "type": "ldaptoctisovalmapping"
27      }
28    ]
29  },
30  "id": "b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c",
31  "type": "ldapattributemap",
32  "links": {
33    "self": "https://200.100.100.100/api/fdm/latest/object/ldapattributemaps/b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c"
34  }
35 }


```

(선택 사항). 기존 LDAP Attribute-Map을 삭제하려면 DELETE Request Delete Attribute-Map을 생성합니다. 이전 HTTP 응답의 map-id를 포함하고 삭제 요청의 기본 URL에 추가합니다.

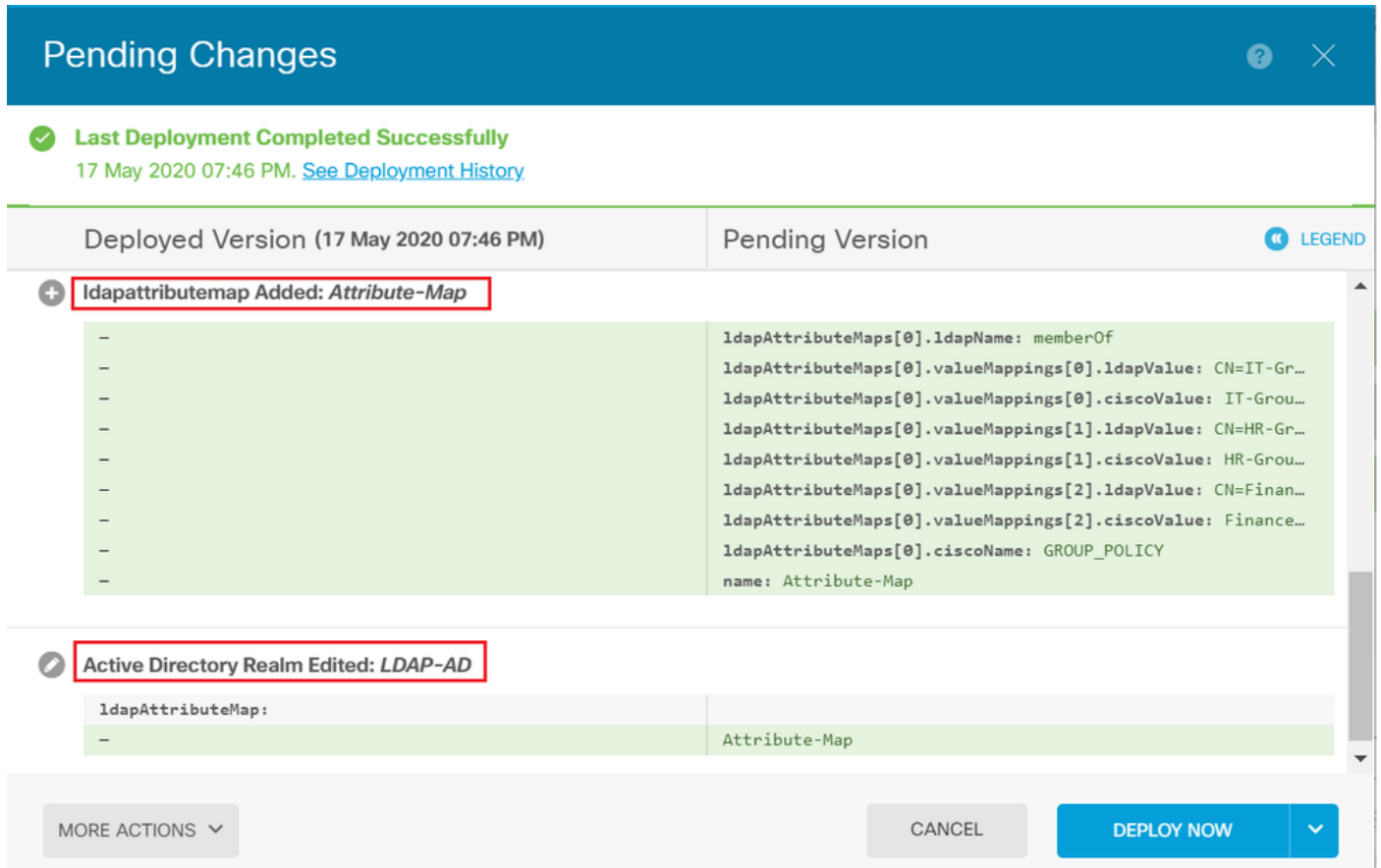
```

History Collections APIs
Delete Attribute-Map
DELETE https://200.100.100.100/api/fdm/latest/object/ldapattributemaps/b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c
Params Authorization Headers (7) Body Pre-request Scripts Tests Settings
Query Params
KEY VALUE DESCRIPTION
Key Value Description
Response

```

 참고: memberOf 특성에 공백이 포함되어 있으면 웹 서버에서 구문 분석하기 위해 URL로 인코딩되어야 합니다. 그렇지 않으면 400 잘못된 요청 HTTP 응답이 수신됩니다. 공백을 포함하는 문자열의 경우 이 오류를 방지하기 위해 "%20" 또는 "+" 중 하나를 사용할 수 있습니다.

9단계. FDM으로 다시 이동하여 [배포] 아이콘을 선택하고 [지금 배포]를 클릭합니다.



**Pending Changes**

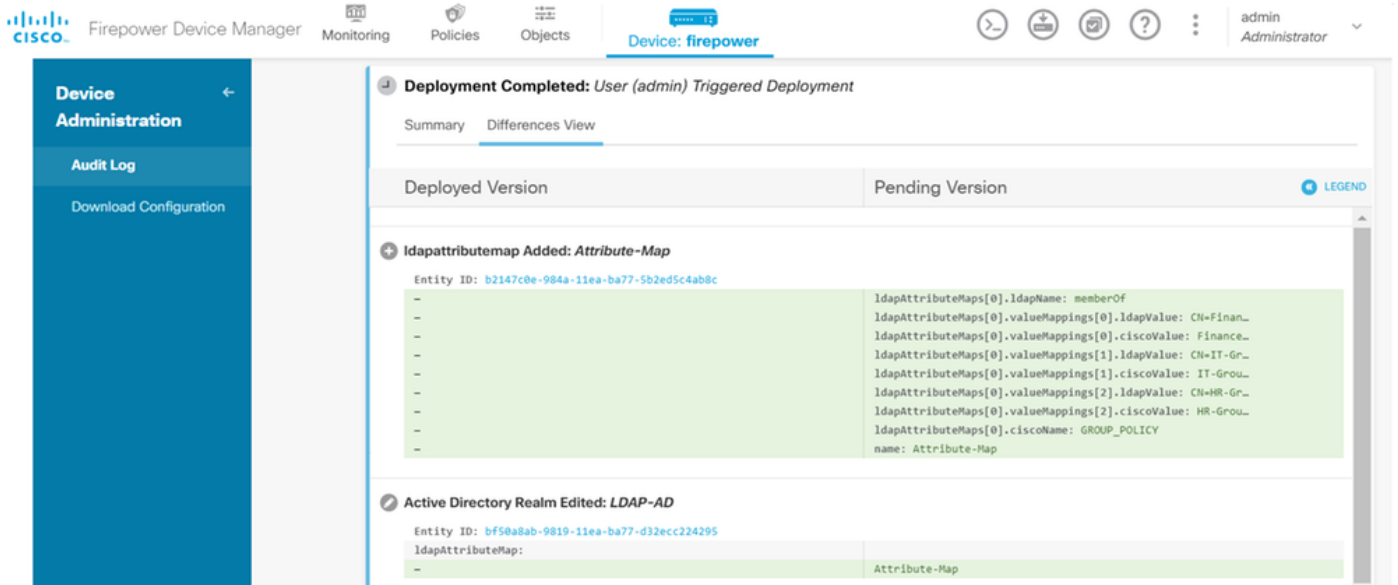
✓ Last Deployment Completed Successfully  
17 May 2020 07:46 PM. [See Deployment History](#)

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

MORE ACTIONS ▾ CANCEL DEPLOY NOW ▾

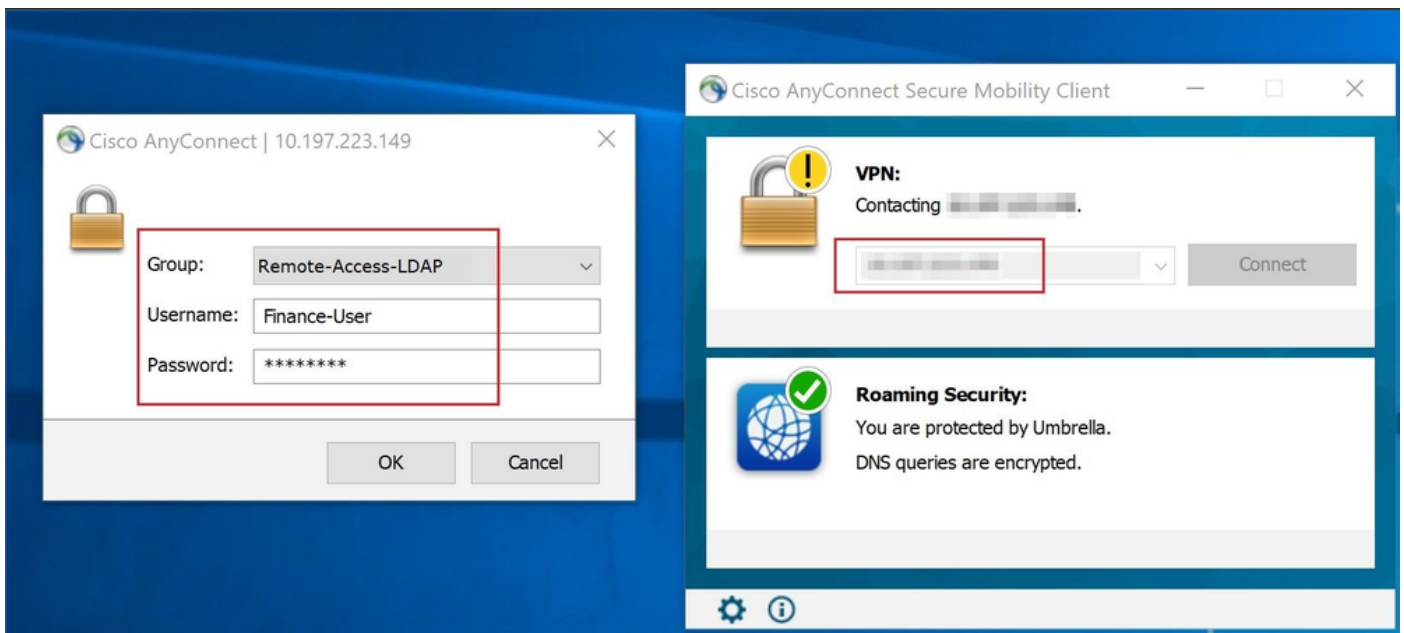
다음을 확인합니다.

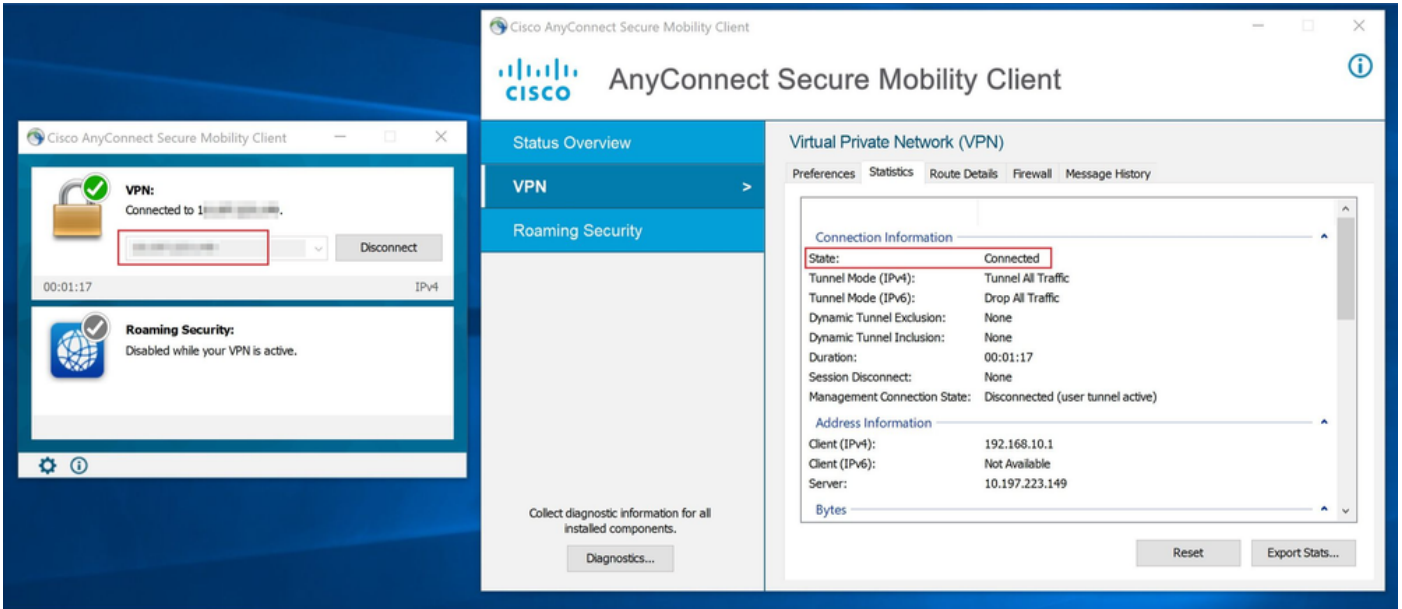
배포 변경 사항은 FDM의 [배포 기록] 섹션에서 확인할 수 있습니다.



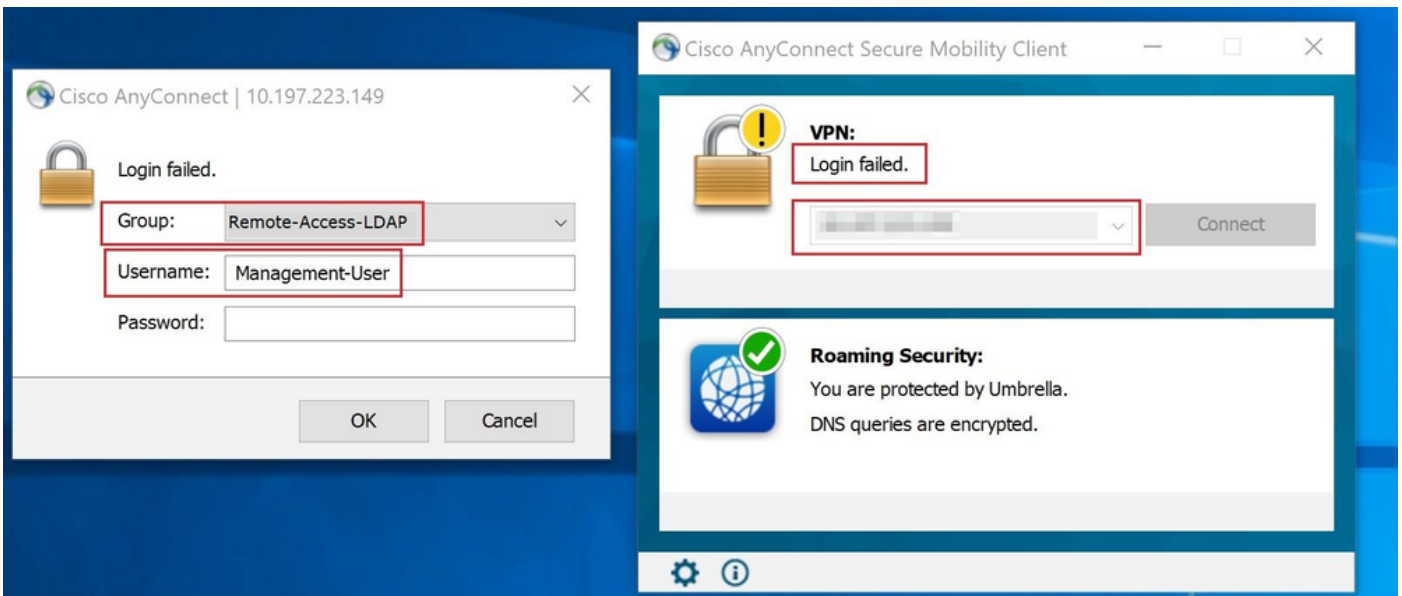
이 컨피그레이션을 테스트하려면 Username(사용자 이름) 및 Password(비밀번호) 필드에 AD 자격 증명을 제공합니다.

AD 그룹 Finance-Group에 속한 사용자가 로그인을 시도하면 예상대로 성공합니다.





AD의 Management-Group에 속한 사용자가 Connection-Profile Remote-Access-LDAP에 연결하려고 시도할 때 LDAP 특성 맵이 일치를 반환하지 않으므로 FTD에서 이 사용자가 상속한 Group-Policy는 vpn 동시 로그인 값 0으로 설정된 NOACCESS입니다. 따라서 이 사용자에게 대한 로그인 시도가 실패합니다.



FTD CLI의 다음 show 명령을 사용하여 컨피그레이션을 확인할 수 있습니다.

```
<#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
```


## 문제 해결

REST API를 구성하는 가장 일반적인 문제 중 하나는 전달자 토큰을 수시로 갱신하는 것입니다. 토큰 만료 시간은 인증 요청에 대한 응답에서 제공됩니다. 이 시간이 만료되면 추가 새로 고침 토큰을 더 오래 사용할 수 있습니다. 새로 고침 토큰도 만료되면 새 액세스 토큰을 검색하려면 새 인증 요청을 전송해야 합니다.

---

 참고: debug 명령을 사용하기 [전에 Debug 명령](#)에 대한 중요 정보를 참조하십시오.

---

 다양한 디버그 레벨을 설정할 수 있습니다. 기본적으로 레벨 1이 사용됩니다. 디버그 수준을 변경하면 디버그의 세부 정도가 증가할 수 있습니다. 특히 프로덕션 환경에서는 이 작업을 신중하게 수행해야 합니다.

---

FTD CLI에서 다음 디버그는 LDAP 특성 맵과 관련된 문제를 해결하는 데 도움이 됩니다

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

이 예에서는 연결되기 전에 언급한 테스트 사용자가 AD 서버에서 받은 정보를 보여 주기 위해 다음 디버그를 수집했습니다.

Finance-User용 LDAP 디버그:

<#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.OQ  
[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-User용 LDAP 디버그:

<#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
```

## 관련 정보

추가 지원이 필요한 경우 Cisco Technical Assistance Center(TAC)에 문의하십시오. 유효한 지원 계약이 필요합니다. [Cisco 전 세계 지원 문의처](#).

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.