

Configure LDAP Attribute Map for RA VPN on FTD Managed by FDM

Contents

- [Introduction](#)
- [Prerequisites](#)
- [Requirements](#)
- [Components Used](#)
- [Authentication Flow](#)
- [LDAP Attribute Map Flow Explained](#)
- [Configure](#)
- [Configuration Steps on FDM](#)
- [Configuration Steps for LDAP Attribute Map](#)
- [Verify](#)
- [Troubleshoot](#)
- [Related Information](#)

Introduction

This document describes the procedure to use a Lightweight Directory Access Protocol (LDAP) server to authenticate and authorize Remote Access VPN (RA VPN) users, and grant them different network access based on their group membership on the LDAP server.

Prerequisites

Requirements

- Basic knowledge of RA VPN configuration on Firewall Device Manager (FDM)
- Basic knowledge of LDAP server configuration on FDM
- Basic knowledge of REpresentational State Transfer (REST) Application Program Interface (API) and FDM Rest API Explorer
- Cisco FTD version 6.5.0 or newer managed by FDM

Components Used

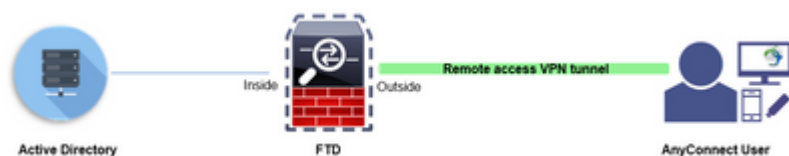
The following hardware and software versions of application/devices were used:

- Cisco FTD version 6.5.0, build 115
- Cisco AnyConnect version 4.10
- Microsoft Active Directory (AD) Server
- Postman or any other API development tool

Note: Configuration support for the Microsoft AD Server and Postmal tool is not provided by Cisco.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Authentication Flow



LDAP Attribute Map Flow Explained

1. The user initiates a remote access VPN connection to the FTD and provides a username and password for their Active Directory (AD) account.
2. The FTD sends a LDAP request to the AD server over port 389 or 636 (LDAP over SSL)
3. The AD responds back to the FTD with all attributes associated with the user.
4. The FTD matches the received attribute values with the LDAP Attribute Map created on the FTD. This is the Authorization process.
5. The user then connects and inherits settings from the Group-Policy matched with the **memberOf** attribute in the LDAP Attribute Map.

For the purpose of this document, the Authorization of AnyConnect users is done using the **memberOf** LDAP attribute.

- The **memberOf** attribute from the LDAP Server for each user is mapped to a **ldapValue** entity on the FTD. If the user belongs to the matching AD group, the Group-Policy associated with that ldapValue is inherited by the user.
- If the **memberOf** attribute value for a user is not matched with any of the **ldapValue** entity on the FTD, the default Group-Policy for the selected Connection Profile is inherited. In this example, **NOACCESS** Group-Policy is inherited to .

Configure

LDAP Attribute Map for FTD managed by FDM is configured with REST API.

Configuration Steps on FDM

Step 1. Verify Device is registered to **Smart Licensing**.



Interfaces Connected Enabled 3 of 9 View All Interfaces	Routing 2 routes View Configuration	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration
Smart License Registered View Configuration	Backup and Restore View Configuration	Troubleshoot No files created yet REQUEST FILE TO BE CREATED
Site-to-Site VPN 1 connection View Configuration	Remote Access VPN Configured 2 connections 5 Group Policies View Configuration	Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration

â€f

Step 2. Verify **AnyConnect Licenses** are enabled on the FDM.

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

Device Summary
Smart License

CONNECTED SUFFICIENT LICENSE Last sync: 11 Oct 2019 09:33 AM Next sync: 11 Oct 2019 09:43 AM Go to Cloud Services

SUBSCRIPTION LICENSES INCLUDED

Threat ENABLE
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

Malware ENABLE
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

URL License DISABLE
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

RA VPN License Type PLUS DISABLE
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

Base License ENABLED ALWAYS
Enabled
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

â€f

Step 3. Verify Export-controlled features is Enabled in the token.



Device Summary

Smart License



CONNECTED
SUFFICIENT LICENSE

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

Assigned V
Export-cont
Go to Cisco

SUBSCRIPTION LICENSES INCLUDED

Threat

Enabled

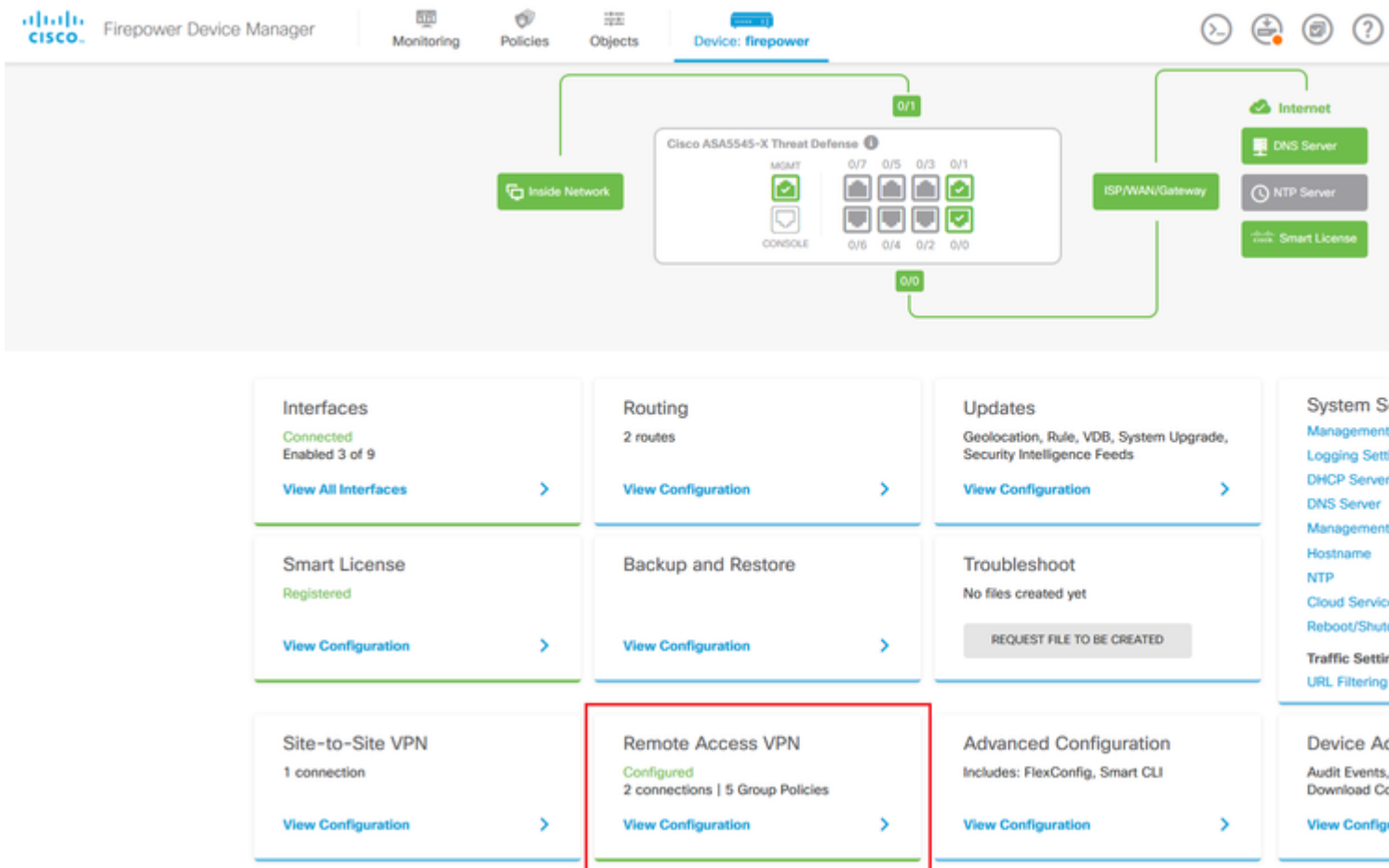
This License allows you to perform intrusion detection and prevention. You must have this license to apply intrusion policies in access rules. You also need this license to apply file policies that control files based on file type.

Includes: Intrusion Policy

Note: This document assumes that RA VPN is already configured. Please refer to the following document for more information on [How to configure RAVPN on FTD managed by FDM](#).

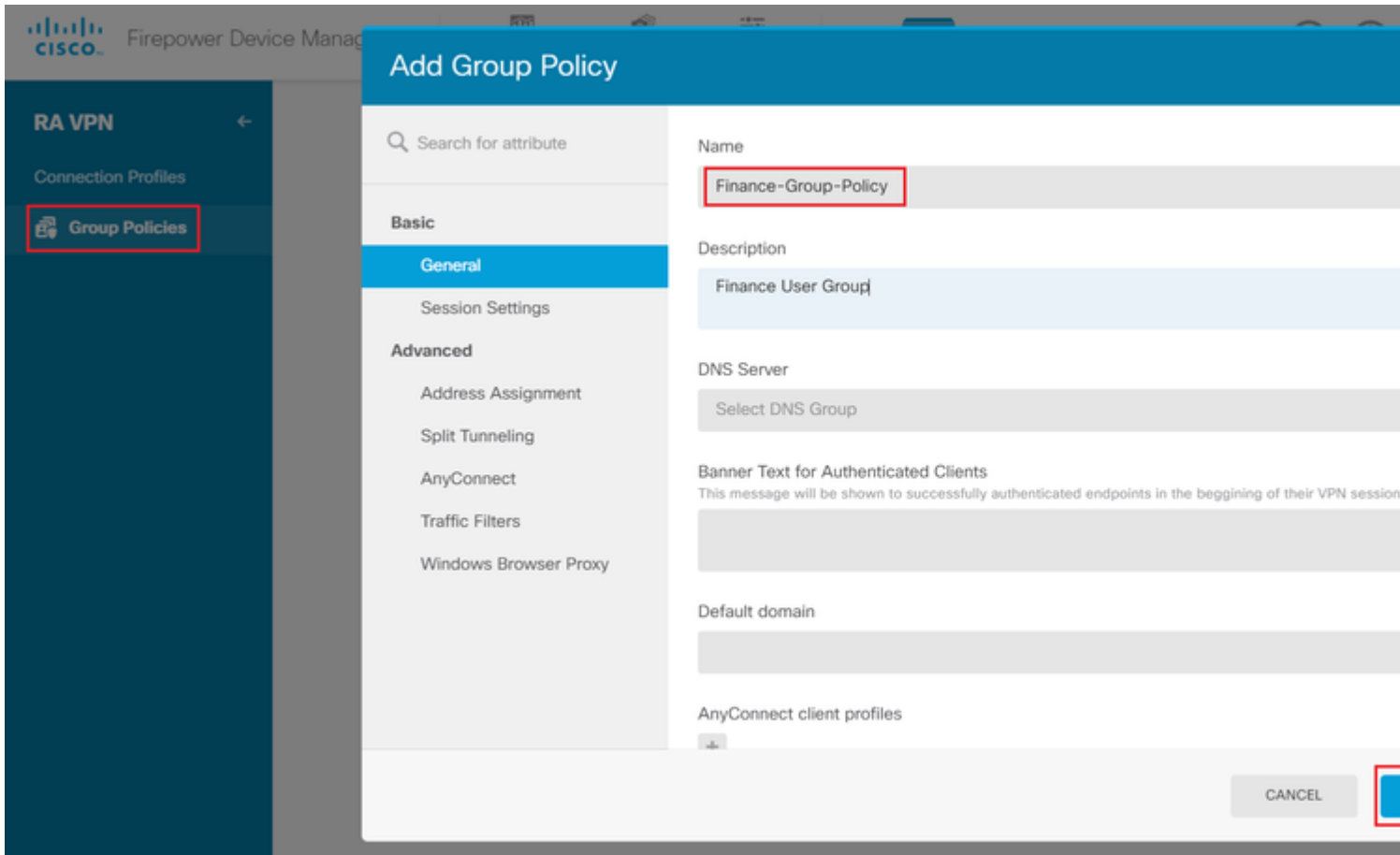
â€f

Step 4. Navigate to **Remote Access VPN > Group Policies**.



â€f

Step 5. Navigate to **Group Policies**. Click on '+' to configure the different Group-Policies for each AD group. In this example, the Group-policies **Finance-Group-Policy**, **HR-Group-Policy** and **IT-Group-Policy** are configured to have access to different subnets.



â€f

The **Finance-Group-Policy** has the following settings:

<#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|splitAc1

```
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>
```

â€f

Similarly, **HR-Group-Policy** has below settings:

```
<#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>
```

â€f

Finally, **IT-Group-Policy** has the next settings:

```
<#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>
```

â€f

Step 6. Create a Group-Policy **NOACCESS** and navigate to **Session Settings** and uncheck the **Simultaneous Login per User** option. This sets the **vpn-simultaneous-logins** value to 0.

The **vpn-simultaneous-logins** value in the Group-Policy when set to 0 terminates the VPN connection of the user immediately. This mechanism is used to prevent users that belong to any AD User-Group other than the configured ones (in this example Finance, HR or IT) from establishing successful connections to the FTD and accessing secure resources available only for the allowed User-Group accounts.

Users that belong to correct AD User-Groups match the LDAP Attribute Map on the FTD and inherit the mapped Group-Policies, while users that do not belong to any of the allowed groups then inherit the default Group-Policy of the connection profile, which in this case is **NOACCESS**.

â€f

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

DNS Server

Select DNS Group

Banner Text for Authenticated Clients

This message will be shown to successfully authenticated endpoints in the begg

Default domain

AnyConnect client profiles



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

Idle Time

30

minutes

1-35791394; (Default: 30)

Connection Time

1

1-30; (Default: 1)

Idle Alert Interval

1

1-30; (Default: 1)

Simultaneous Login per User

1-2147483647; (Default: 3)

â€f

The **NOACCESS** Group-Policy has the following settings:

```
<#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

```

Step 7. Navigate to **Connection Profiles** and create a Connection-Profile. In this example the profile name is **Remote-Access-LDAP**. Choose Primary Identity Source **AAA Only** and create a new Authentication Server type **AD**.

The screenshot shows the Cisco Firepower Device Manager interface for configuring a Connection Profile. The profile name is **Remote-Access-LDAP**. The Group Alias is also **Remote-Access-LDAP**. The Primary Identity Source is set to **AAA Only**. The Primary Identity Source for User Authentication dropdown is open, showing **LocalIdentitySource** and **Special-Identities-Realm**. A **Create new** dropdown is also open, showing **AD** as an option. The Fallback Local Identity Source is set to **Please Select Local Identity Source**. The **NEXT** button is visible at the bottom right.

Enter the information of the AD server:

- Directory Username

- Directory Passowrd
- Base DN
- AD Primary Domain
- Hostname / IP Address
- Port
- Encryption type

â€f

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

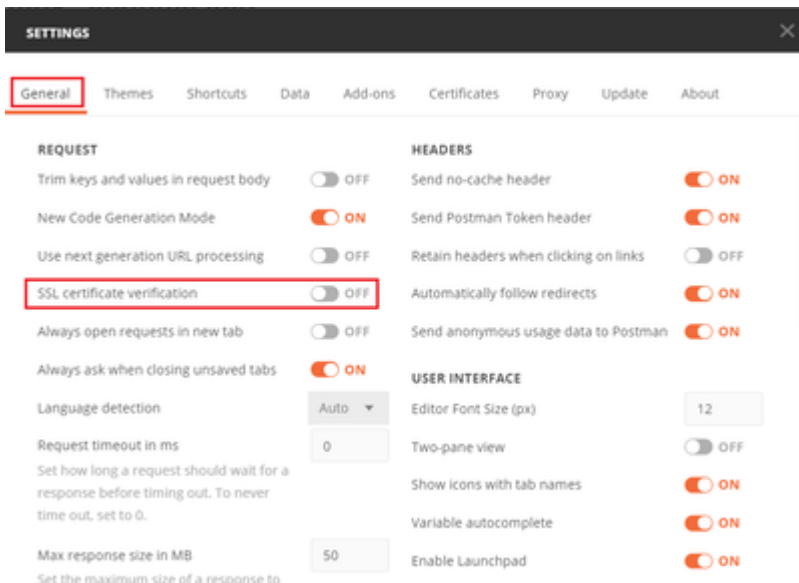
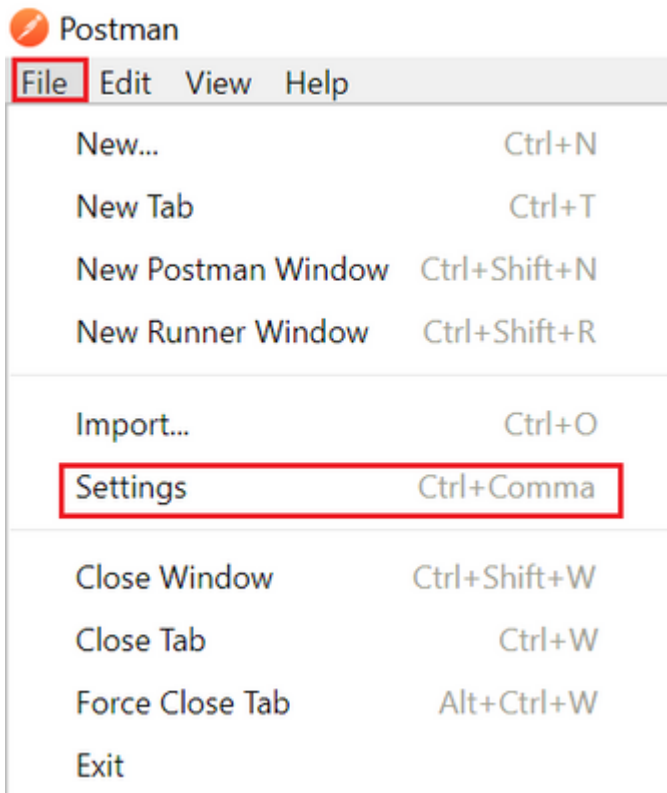
Please select a certificate

TEST

[Add another configuration](#)

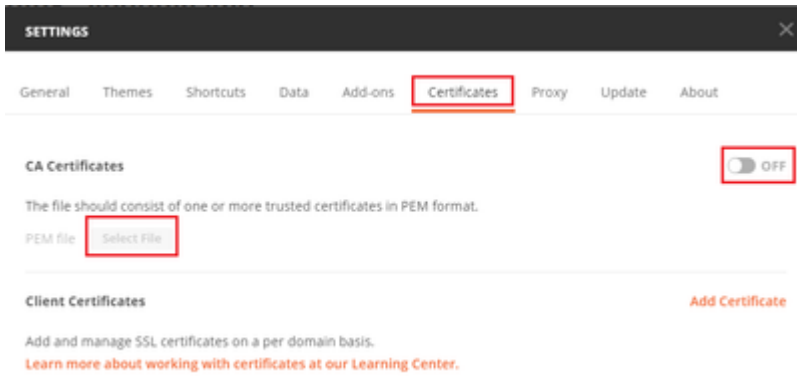
CANCEL

, turn off the SSL certificate verification to avoid a SSL handshake failure when sending API requests to the FTD. This is done if the FTD uses a self-signed certificate.



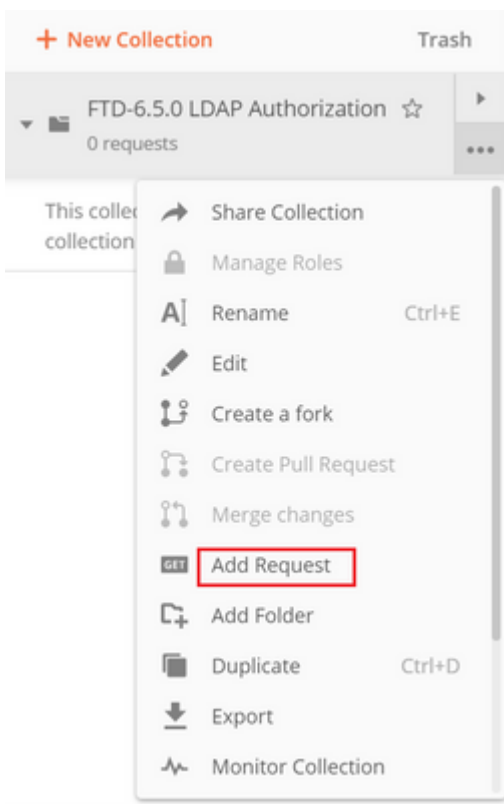
â€f

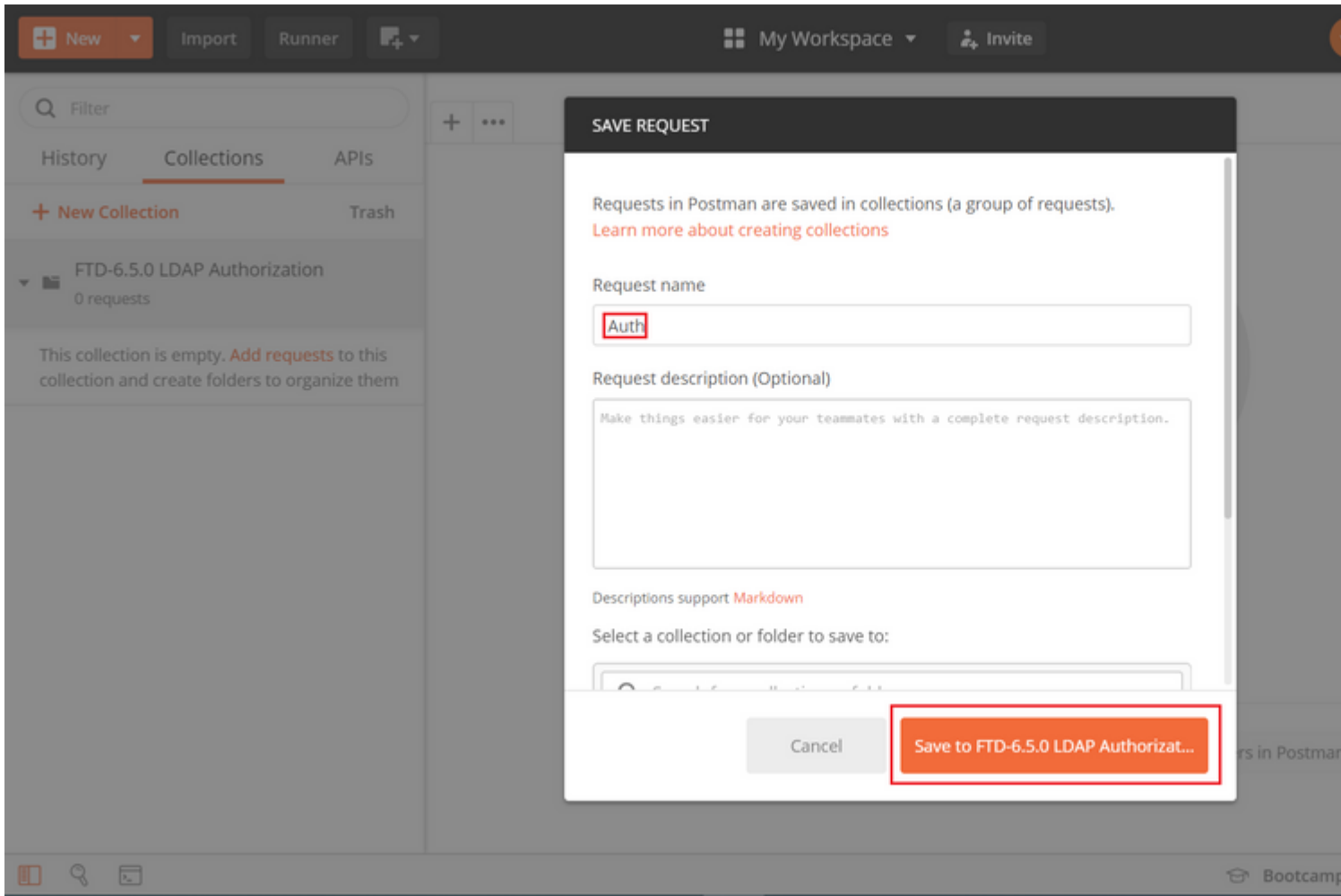
Alternatively, the certificate used by the FTD can be added as a CA certificate in the Certificate section of the Settings.



â€f

Step 4. Add a new POST request **Auth** to create a login POST request to the FTD, in order to get the token to authorize any POST/GET requests.





â€f

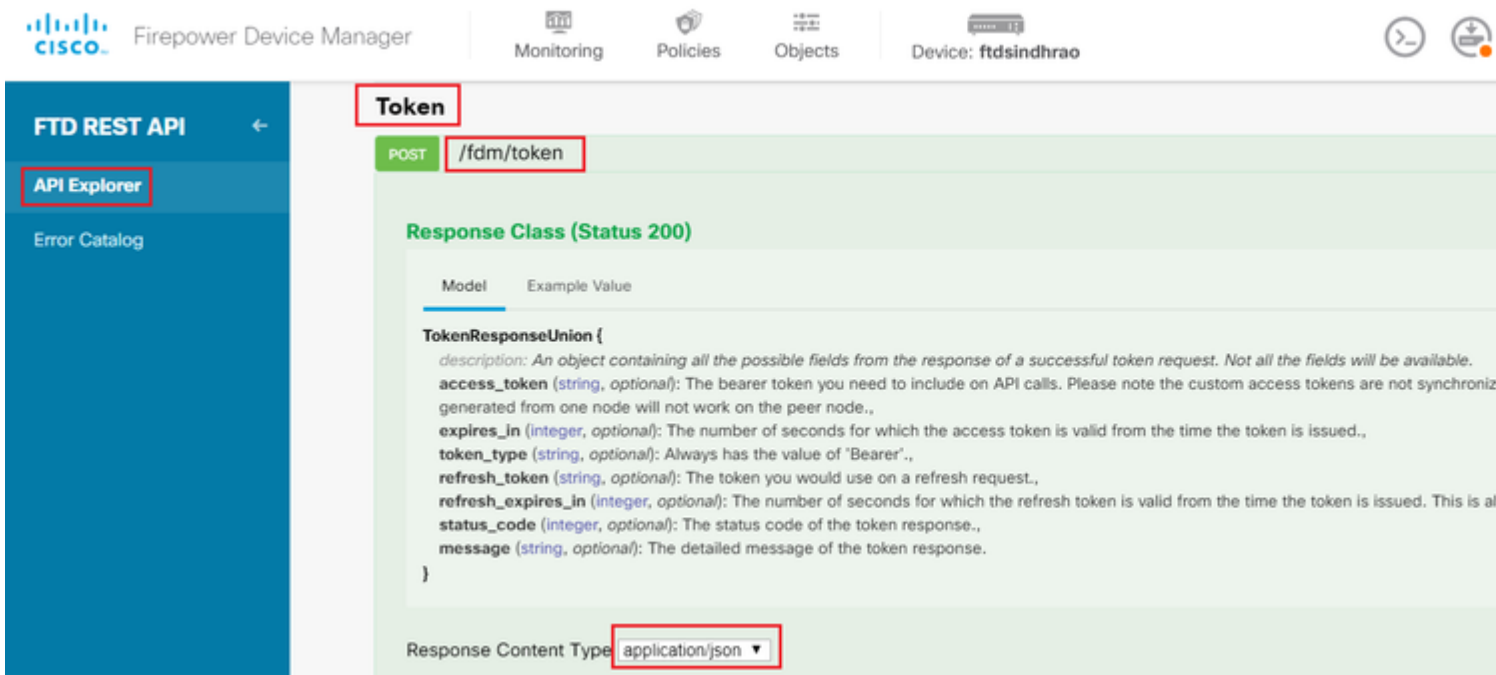
All Postman requests for this collection must contain the next:

BaseURL: <https://<FTD Management IP>/api/fdm/latest/>

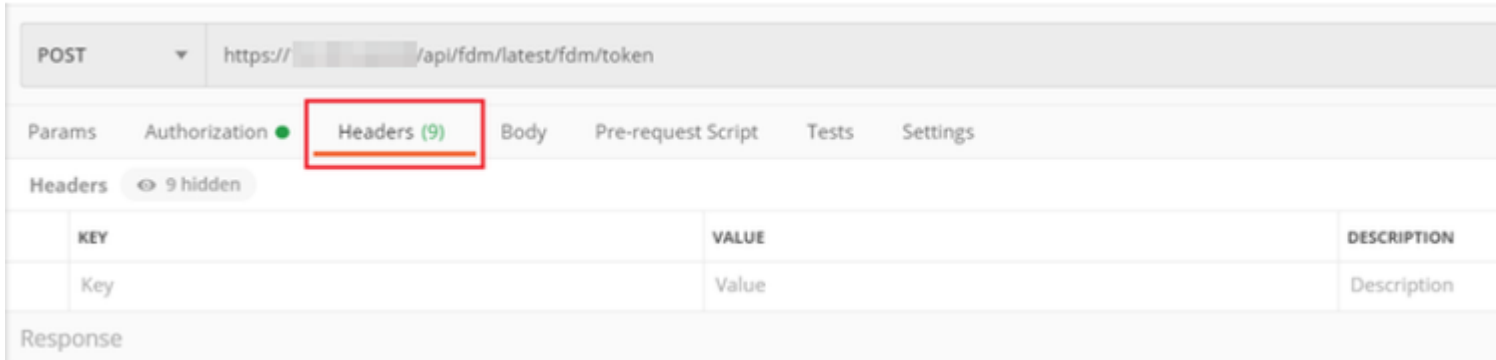
In the request URL, append the base URL with the respective objects that need to be added or modified.

â€f

Here, an authentication request for a token is created, referred from <https://<FTD Management IP>/api-explorer>. This needs to be checked for other objects and the necessary changes need to be made for them.



Navigate to **Headers** and click on **Manage Presets**.



â€f

Crte a new Preset **Header-LDAP** and add the below Key-Value pair:

Content-Type	application/json
Accept	application/json

â€f

MANAGE HEADER PRESETS

Add Header Preset

Header-LDAP

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

For all other requests, navigate to respective Header tabs and select this Preset Header value: **Header-LDAP** for the REST API requests to use **json** as the primary data type.

The Body of the POST Request to get the token must contain the next:

Type	raw - JSON (application/json)
grant_type	password
username	Admin Username in order to log in to the FTD
password	Password associated with the admin user account

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



```

58 {
59   "version": "2nid13x12vu",
60   "name": "Finance-Group-Policy",
61   "banner": null,
62   "dnsServerGroup": null,
63   "defaultDomainName": null,
64   "simultaneousLoginPerUser": 3,
65   "maxConnectionTimeout": null,
66   "maxConnectionTimeAlertInterval": 1,
67   "vpnIdleTimeout": 30,
68   "vpnIdleTimeoutAlertInterval": 1,
69   "ipv4LocalAddressPool": [],
70   "ipv6LocalAddressPool": [],
71   "dhcpScope": null,
72   "ipv4SplitTunnelSetting": "TUNNEL_SPECIFIED",
73   "ipv6SplitTunnelSetting": "TUNNEL_ALL",
74   "ipv4SplitTunnelNetworks": [
75     {
76       "version": "ogaly1l3hgigo",
77       "name": "acl1",
78       "id": "9ec77902-9836-11ea-ba77-37fd67647b3e",
79       "type": "networkobject"
80     }
81   ],
82   "ipv6SplitTunnelNetworks": [],
83   "splitDNSRequestPolicy": "USE_SPLIT_TUNNEL_SETTING",
84   "splitDNSDomainList": "",
85   "scepForwardingUrl": null,
86   "periodicClientCertAuthenticationInterval": 1,
87   "enableDTLS": false,
88   "enableDTLSCompression": false,
89   "sslCompression": "DISABLED",
90   "enableSSLrekey": false,
91   "rekeyMethod": "NEW_TUNNEL",
92   "rekeyInterval": 4,
93   "ignoreDFBit": false,
94   "bypassUnsupportedProtocol": false,
95   "mtuSize": 1406,
96   "useAlwaysOnVPNSettingInProfile": true,
97   "enableKeepAliveMessages": false,
98   "keepAliveMessageInterval": 20,
99   "enableGatewayDPD": false,
100  "gatewayDPDInterval": 30,
101  "enableClientDPD": false,
102  "clientDPDInterval": 30,
103  "clientProfiles": [],
104  "keepInstallerOnClient": false,
105  "vpnTrafficFilterACL": null,
106  "enableRestrictVPNTOVLAN": false,
107  "restrictVPNTOVLANId": null,
108  "clientFirewallPrivateNetworkRules": null,
109  "clientFirewallPublicNetworkRules": null,
110  "browserProxyType": "NO_MODIFY",
111  "proxy": {
112    "serverHost": null,
113    "port": null,
114    "type": "serverhostandport"
115  },
116  "proxyExceptions": [],
117  "isDisablePeriodicClientCertAuthentication": false,
118  "id": "a5722b15-9836-11ea-ba77-6916f09ace0c",
119  "type": "ravpngrouppolicy",
120  "links": {
121    "self": "https://[redacted]/api/fdm/latest/object/ravpngrouppolicies/a5722b15-9836-11ea-ba77-6916f09ace0c"
122  }
123 },

```

â€š

Step 6. Add a new POST request **Create LDAP Attribute Map** to create the LDAP Attribute Map. In this document, the model **LdapAttributeMapping** is used. Other models also have similar operations and methods to create Attribute map. Examples for these models is available in the api-explorer as mentioned earlier in this document.

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', 'BANNER1', 'BANNER2', 'CISCO_AV_PAIR', 'CISCO_IP_PHONE_BYPASS', 'CISCO_LEAP_BYPASS', 'CLIENT_BYPASS_PROTOCOL', 'CLIENT_TYPE_VERSION_LIMITING', 'CONFIDENCE_INTERVAL', 'DHCP_NETWORK_SCOPE', 'DN_FIELD', 'DISABLE_ALWAYS_ON_VPN_GATEWAY_FQDN', 'GROUP_POLICY', 'IE_PROXY_BYPASS_LOCAL', 'IE_PROXY_EXCEPTION_LIST', 'IE_PROXY_METHOD', 'IE_PROXY_PREF', 'IETF_RADIUS_FILTER_ID', 'IETF_RADIUS_FRAMED_IP_ADDRESS', 'IETF_RADIUS_FRAMED_IP_NETMASK', 'IETF_RADIUS_IPV6_PREF', 'IETF_RADIUS_INTERFACE_ID', 'IETF_RADIUS_SERVICE_TYPE', 'IETF_RADIUS_SESSION_TIMEOUT', 'IKE DPD_Retry_Interval', 'IKE_PEER_AUTH_ON_REKEY', 'IPSEC_AUTHENTICATION', 'IPSEC_BACKUP_SERVER_LIST', 'IPSEC_BACKUP_SERVERS', 'IPSEC_CLIENT_FIREWALL_FILTER_OPTIONAL', 'IPSEC_CLIENT_FIREWALL_FILTER_OPTIONAL', 'IPSEC_DEFAULT_DOMAIN', 'IPSEC_EXTENDED_AUTH_ON_REKEY', 'IPSEC_IKE_PEER_AUTH_ON_REKEY', 'IPSEC_IPV6_SPLIT_TUNNELING_POLICY', 'IPSEC_MODE_CONFIG', 'IPSEC_OVER_UDP', 'IPSEC_OVER_UDP_PORT', 'IPSEC_REQUIRE_SPLIT_TUNNELING', 'IPSEC_SPLIT_DNS_NAMES', 'IPSEC_SPLIT_TUNNEL_ALL_DNS', 'IPSEC_SPLIT_TUNNEL_LIST', 'IPSEC_SPLIT_TUNNELING_POLICY', 'IPV6_PRIMARY_DNS', 'IPV6_SECONDARY_DNS', 'L2TP_ENCRYPTION', 'L2TP_MPPC_COMPRESSION', 'MS_CLIENT_SUBNET_MASK', 'PPTP_MPPC_COMPRESSION', 'WEBVPN_VLAN'],
valueMappings (Array[LdapToCiscoValueMapping]): A list of LdapToCiscoValueMapping objects, which specify the value mappings for the 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. (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 mappings for the attribute.
 Field level constraints: cannot be null. (Note: Additional constraints might exist),
type (string): ldapattributetogrouppolicymapping
 }

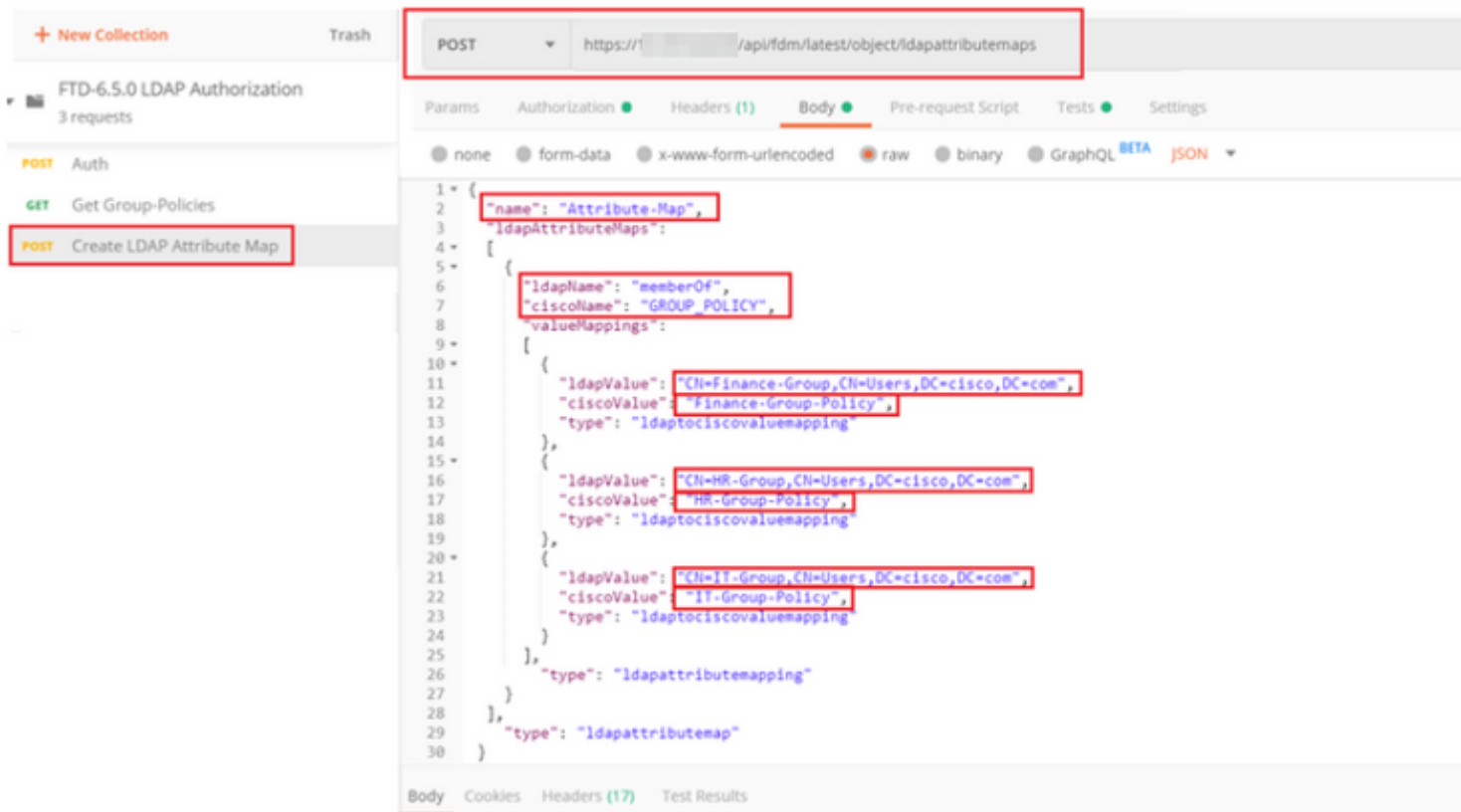
â€f

The URL to POST the LDAP Attribute Map is: <https://<FTD Management IP>/api/fdm/latest/object/ldapattributemaps>

The body of POST request must contain the following:

name	Name for LDAP Attribute-Map
type	ldapattributemapping
ldapName	memberOf
ciscoName	GROUP_POLICY
ldapValue	memberOf value for User from AD
ciscoValue	Group-Policy name for each User Group in FDM

â€f



â€f

The body of the POST request contains the LDAP Attribute map information that maps a specific Group-Policy to an AD group based on the **memberOf** value:

```
{
  "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"
}
```

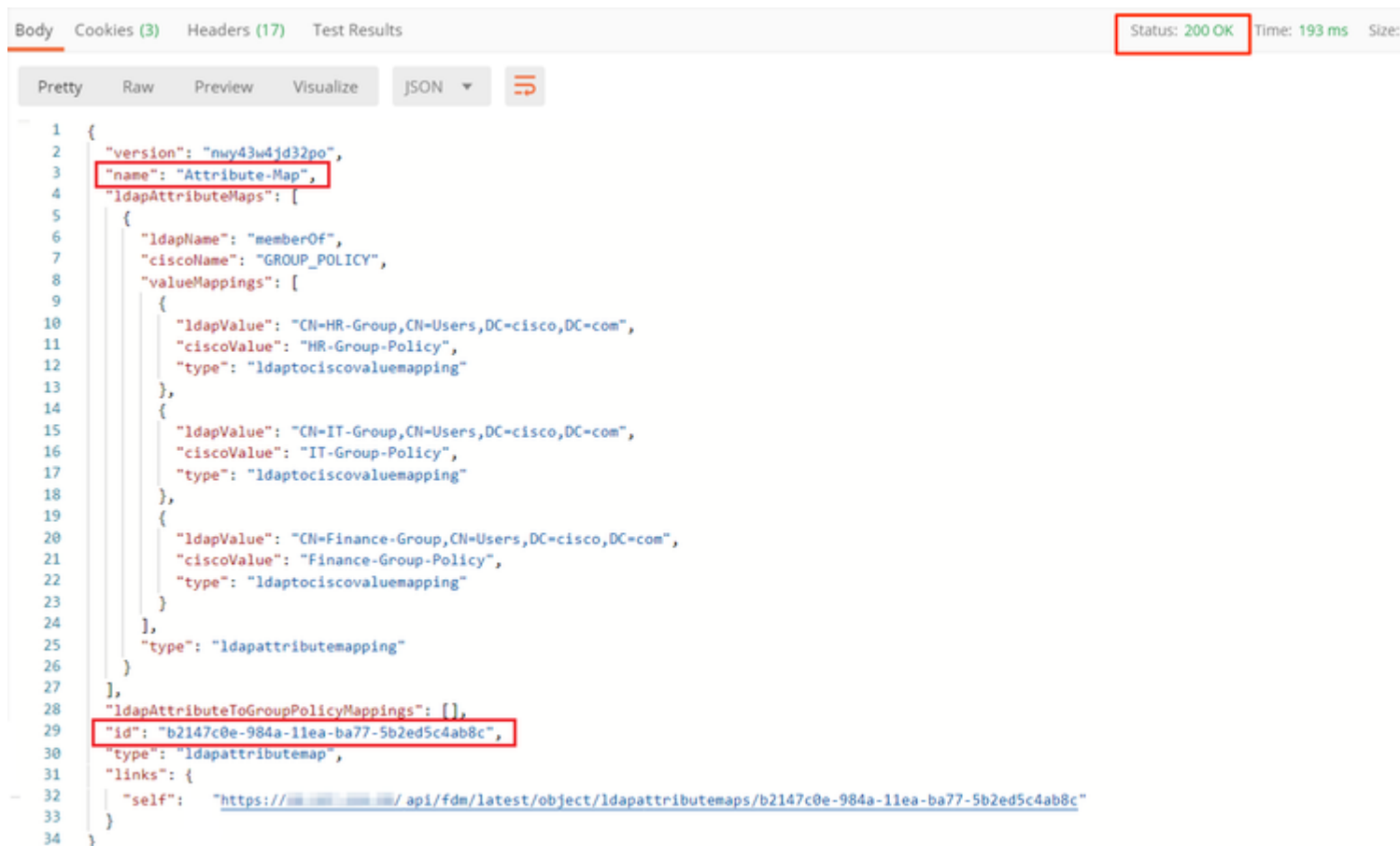


```
],
  "type": "ldapattributemap"
}
```

Note: The **memberOf** field can be retrieved from AD server with the **dsquery** command or can be fetched from the LDAP debugs on the FTD. In the debug logs, look for **memberOf value:** field.

â€f

The Response of this POST request looks similar to the next output:

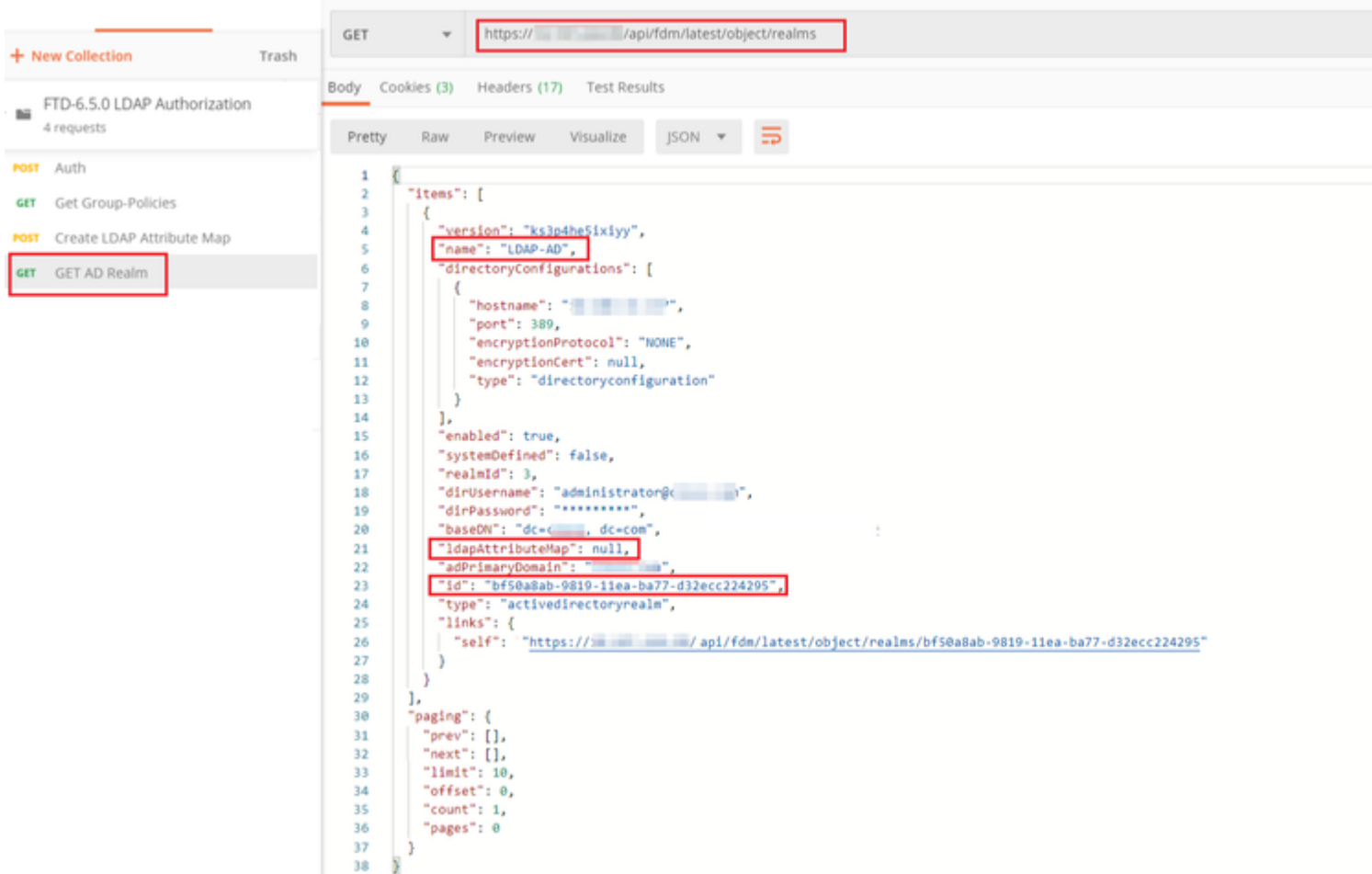


```
Body Cookies (3) Headers (17) Test Results Status: 200 OK Time: 193 ms Size:
Pretty Raw Preview Visualize JSON
1 {
2   "version": "nwy43w4jd32po",
3   "name": "Attribute-Map",
4   "ldapAttributeMaps": [
5     {
6       "ldapName": "memberOf",
7       "ciscoName": "GROUP_POLICY",
8       "valueMappings": [
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://<IP>/api/fdm/latest/object/ldapattributemaps/b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c"
33  }
34 }
```

Step 7. Add a new GET request to obtain the current AD realm configuration on FDM.

The URL to get the current AD realm configuration is: <https://<FTD Management IP>/api/fdm/latest/object/realms>

â€f



â€f

Notice that the value for key **ldapAttributeMap** is **null**.

â€f

Step 8. Create a new **PUT** request to edit the AD Realm. Copy the **GET** response output from previous step and add it to the Body of this new **PUT** request. This step can be used to make any modifications to the current AD Realm setup, for example: change password, IP address or add new value for any key like **ldapAttributeMap** in this case.

Note: It is important to copy the contents of the item list rather than the whole GET response output. The Request URL for the PUT request has to be appended with the item id of the object for which changes are made. In this example, the value is: bf50a8ab-9819-11ea-ba77-d32ecc224295

â€f

The URL to edit the current AD realm configuration is: <https://<FTD Management IP>/api/fdm/latest/object/realms/<realm ID>>

The body of the PUT request must contain the following :

version	version obtained from response of previous GET request
id	id obtained from response of previous GET request

â€f

The screenshot shows a REST client interface with a PUT request to the URL `https://.../api/fdm/latest/object/realms/bf50a8ab-9819-11ea-ba77-d32ecc224295`. The request body is a JSON object:

```

1 {
2   "version": "ks3p4he5ixiyy",
3   "name": "LDAP-AD",
4   "directoryConfigurations": [
5     {
6       "hostname": "<IP Address>",
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@...com",
17  "dirPassword": "*****",
18  "baseDN": "dc=..., dc=com",
19  "ldapAttributeMap":
20  {
21    "id": "b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c",
22    "type": "ldapattributemap"
23  },
24  "adPrimaryDomain": "...com",
25  "id": "bf50a8ab-9819-11ea-ba77-d32ecc224295",
26  "type": "activedirectoryrealm",
27  "links": {
28    "self": "https://.../api/fdm/latest/object/realms/bf50a8ab-9819-11ea-ba77-d32ecc224295"
29  }
30 }
31

```

â€f

The body for the configuration in this example is:

<#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://<FTD Management IP Address>/api/fdm/latest/object/realms/bf50a8ab-9819-11ea-ba77-d32ecc224295"
  }
}

```

Verify that the **ldapAttributeMap id** matches in the Response Body for this request.

The screenshot shows a REST client interface with the following elements:

- Top bar: "Body", "Cookies (3)", "Headers (17)", "Test Results", and "Status: 200 OK" (highlighted in red).
- Navigation tabs: "Pretty", "Raw", "Preview", "Visualize", "JSON", and a menu icon.
- JSON response body (lines 1-31):


```

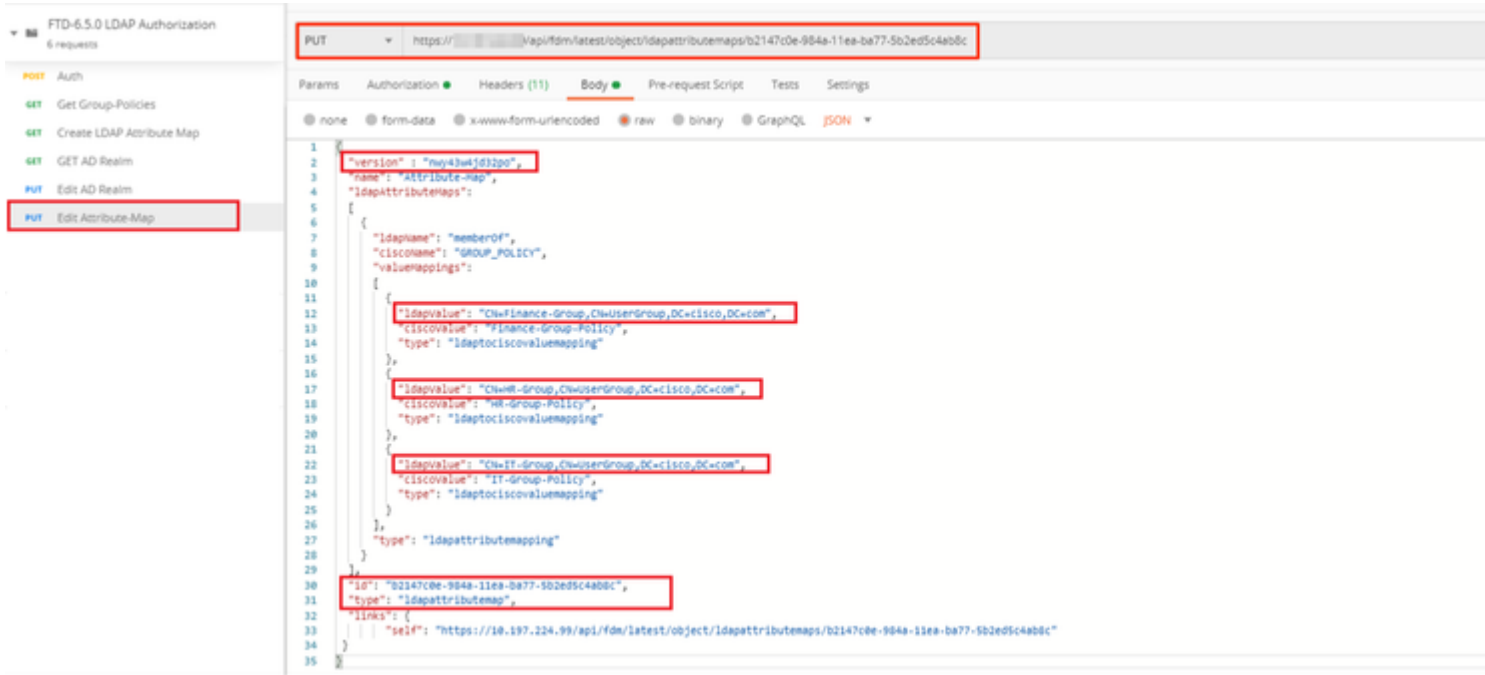
1 {
2   "version": "ksy7p574qfq7w",
3   "name": "LDAP-AD",
4   "directoryConfigurations": [
5     {
6       "hostname": "10.10.10.10",
7       "port": 389,
8       "encryptionProtocol": "NONE",
9       "encryptionCert": null,
10      "type": "directoryconfiguration"
11    }
12  ],
13  "enabled": true,
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/realms/bf50a8ab-9819-11ea-ba77-d32ecc224295"
30  }
31 }

```

â€¦

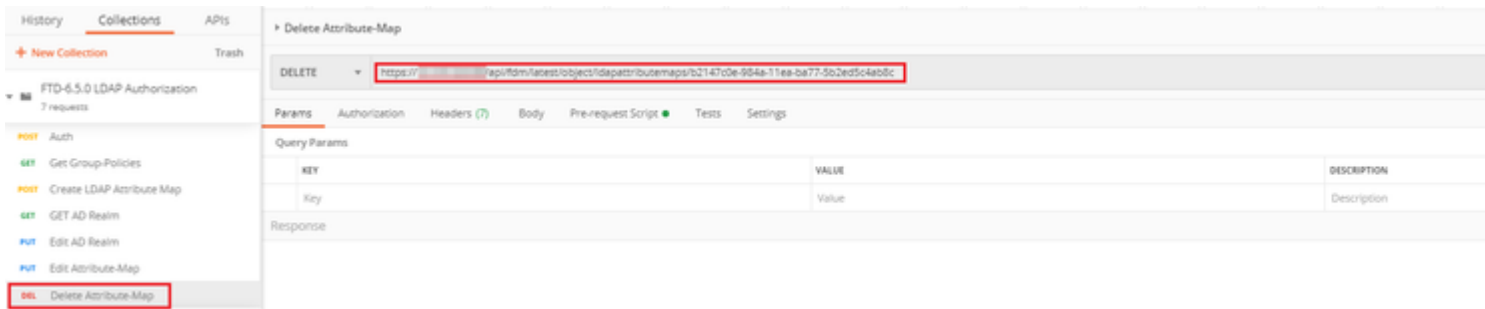
(Optional). The LDAP attribute map can be modified with **PUT** requests. Create a new PUT request **Edit Attribute-Map** and make any changes like the name of the Attribute-Map or memberOf value. T

In the next example, the value of **ldapvalue** has been modified from **CN=Users** to **CN=UserGroup** for all three groups.



â€f

(Optional). To delete an existing LDAP Attribute-Map, create a DELETE Request **Delete Attribute-Map**. Include the **map-id** from the previous HTTP response and append with the base URL of the delete request.



Note: If the **memberOf** attribute contains spaces, it must be URL encoded for the Web Server to parse it. Otherwise a **400 Bad Request HTTP Response** is received. For string containing white-spaces spaces, either "%20" or "+" can be used to avoid this error.

â€f

Step 9. Navigate back to FDM, select the Deployment icon and click on **Deploy Now**.

â€f

Pending Changes

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

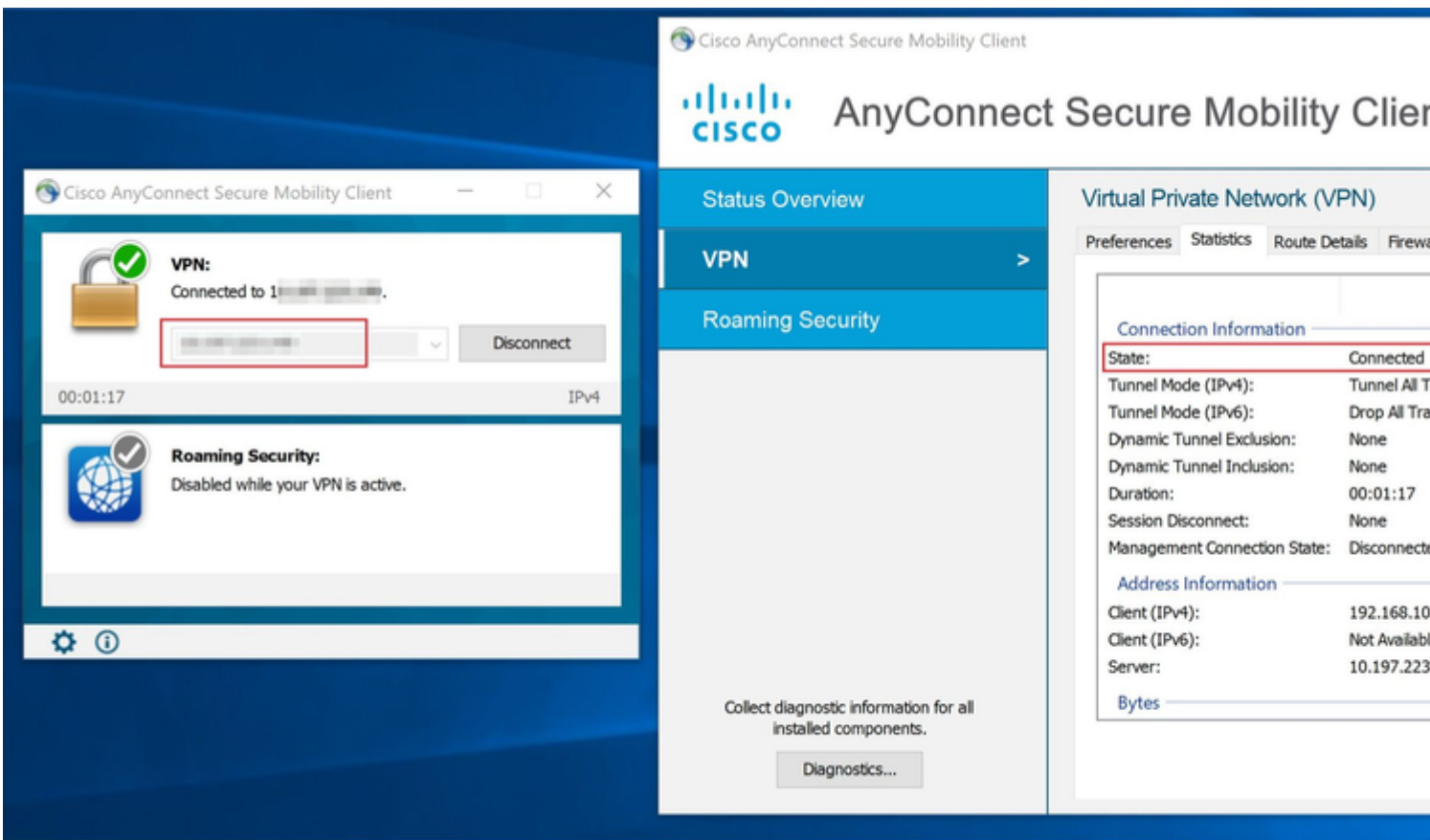
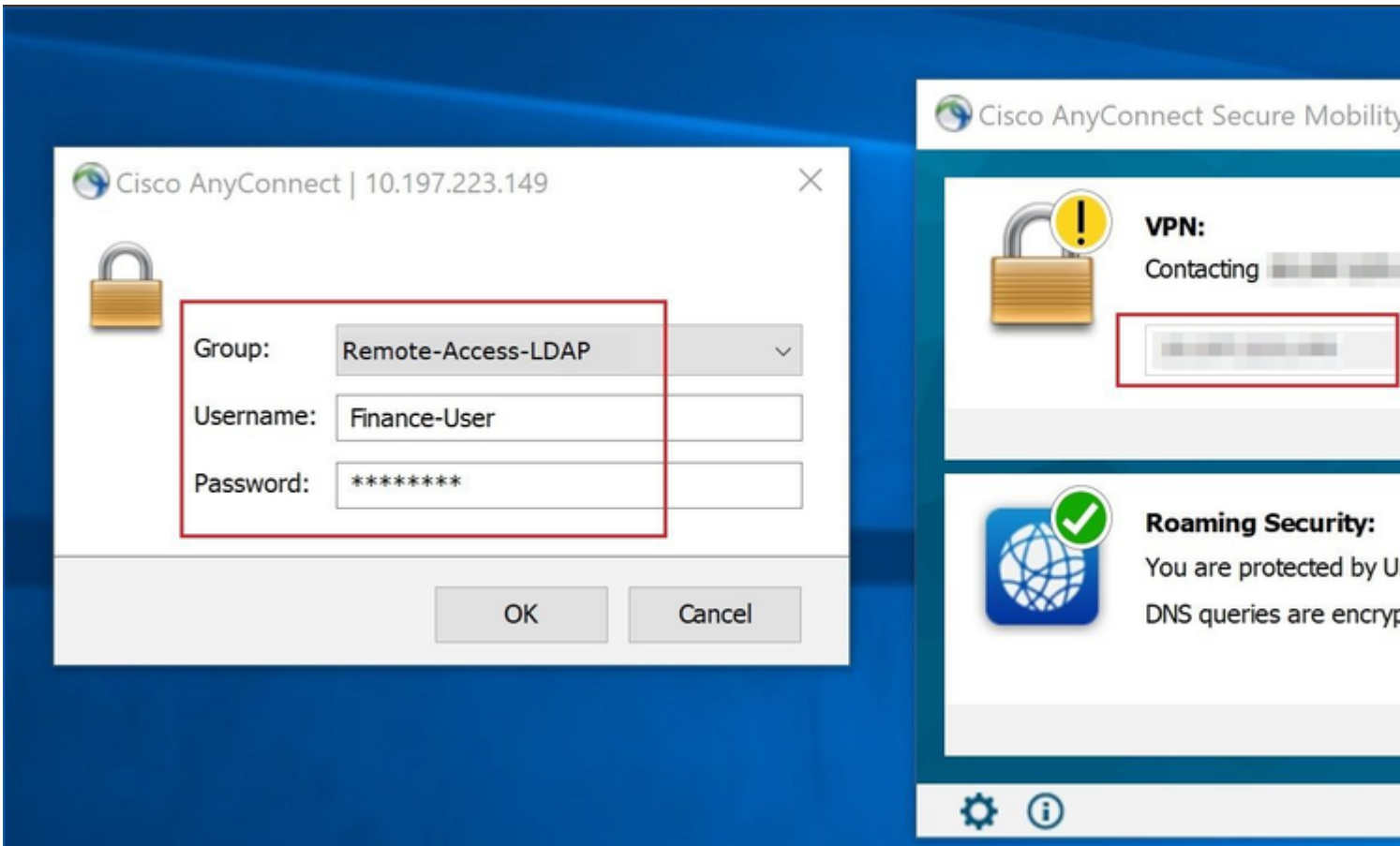
Deployed Version (17 May 2020 07:46 PM)	Pending Version
+ Idapattributemap Added: <i>Attribute-Map</i>	
<pre>- - - - - - - - -</pre>	<pre>ldapAttributeMaps[0].ldapName : ldapAttributeMaps[0].valueMappi ldapAttributeMaps[0].valueMappi ldapAttributeMaps[0].valueMappi ldapAttributeMaps[0].valueMappi ldapAttributeMaps[0].valueMappi ldapAttributeMaps[0].valueMappi ldapAttributeMaps[0].valueMappi ldapAttributeMaps[0].ciscoName : name: Attribute-Map</pre>
🔍 Active Directory Realm Edited: <i>LDAP-AD</i>	
<pre>ldapAttributeMap : -</pre>	<pre>Attribute-Map</pre>

MORE ACTIONS ▾ CANCEL

â€f

Verify

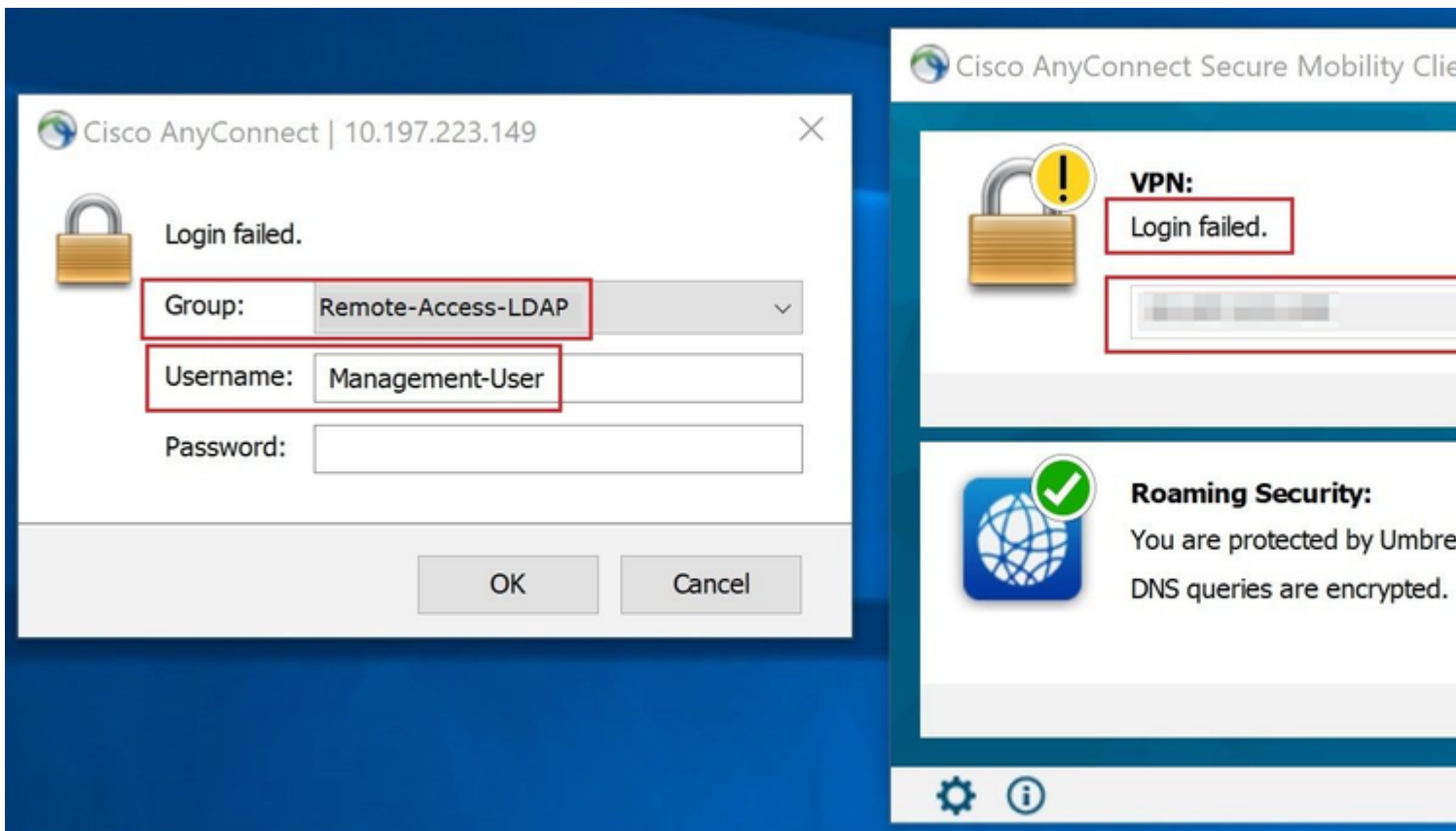
The deployment changes can be verified in the **Deployment History** section of the FDM.



â€f

When a user that belongs to the **Management-Group** in AD tries to connect to Connection-Profile **Remote-**

Access-LDAP, since no LDAP Attribute Map returned a match, the Group-Policy inherited by this user on the FTD is **NOACCESS** which has vpn-simultaneous-logins set to value 0. Hence, the login attempt for this user fails.



â€f

The configuration can be verified with the next show commands from the FTD CLI:

```
<#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
```

Troubleshoot

One of the most common issues with configuring REST API is to renew the bearer token from time to time. The token expiry time is given in the Response for the Auth request. If this time expires, an additional refresh token can be used for a longer time. After the refresh token also expires, a new Auth request has to be sent to retrieve a new access token.

Note: Refer to [Important Information on Debug Commands](#) before you use **debug** commands.

You can set various debug levels. By default, level 1 is used. If you change the debug level, the verbosity of the debugs might increase. Do this with caution, especially in production environments.

The following debugs on the FTD CLI would be helpful in troubleshooting problems related to LDAP Attribute Map

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

In this example. the next debugs were collected to demonstrate the information received from the AD server when the test users mentioned before connected.

LDAP debugs for **Finance-User**:

<#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

LDAP debugs for Management-User:

<#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
```

Related Information

For additional assistance, please contact Cisco Technical Assistance Center (TAC). A valid support contract is required: [Cisco Worldwide Support Contacts](#).