

# Configurar Mapa de Atributos LDAP para RAVPN no FTD Gerenciado pelo FDM

## Contents

- [Introdução](#)
- [Pré-requisitos](#)
- [Requisitos](#)
- [Componentes Utilizados](#)
- [Fluxo de autenticação](#)
- [Fluxo do mapa de atributos LDAP explicado](#)
- [Configurar](#)
- [Etapas de Configuração no FDM](#)
- [Etapas de Configuração para o Mapa de Atributos LDAP](#)
- [Verificar](#)
- [Troubleshooting](#)
- [Informações Relacionadas](#)

## Introdução

Este documento descreve o procedimento para usar um servidor Lightweight Directory Access Protocol (LDAP) para autenticar e autorizar usuários da VPN de Acesso Remoto (RA VPN) e conceder a eles acesso de rede diferente com base em sua associação de grupo no servidor LDAP.

## Pré-requisitos

### Requisitos

- Conhecimento básico da configuração de VPN RA no Gerenciador de Dispositivos de Firewall (FDM)
- Conhecimento básico da configuração do servidor LDAP no FDM
- Conhecimento básico da API REST (Application Program Interface) e do Explorador da API Rest do FDM
- Cisco FTD versão 6.5.0 ou mais recente gerenciado pelo FDM

### Componentes Utilizados

Foram usadas as seguintes versões de hardware e software de aplicativos/dispositivos:

- Cisco FTD versão 6.5.0, build 115
- Cisco AnyConnect versão 4.10
- Servidor do Microsoft Active Directory (AD)
- Postman ou qualquer outra ferramenta de desenvolvimento de API

---

Observação: o suporte de configuração para a ferramenta Microsoft AD Server and Postmal não é fornecido pela Cisco.

---

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório

específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Fluxo de autenticação



## Fluxo do mapa de atributos LDAP explicado

1. O usuário inicia uma conexão VPN de acesso remoto com o FTD e fornece um nome de usuário e uma senha para sua conta do Ative Diretory (AD).
2. O FTD envia uma solicitação LDAP ao servidor AD pela porta 389 ou 636 (LDAP sobre SSL)
3. O AD responde ao FTD com todos os atributos associados ao usuário.
4. O FTD corresponde aos valores de atributo recebidos com o Mapa de atributos LDAP criado no FTD. Este é o processo de Autorização.
5. Em seguida, o usuário conecta e herda as configurações da Política de grupo correspondente ao atributo **memberOf** no Mapa de atributos LDAP.

Para a finalidade deste documento, a autorização dos usuários do AnyConnect é feita usando o atributo LDAP **memberOf**.

- O atributo **memberOf** do servidor LDAP para cada usuário é mapeado para uma entidade **ldapValue** no FTD. Se o usuário pertencer ao grupo do AD correspondente, a Política de grupo associada a esse ldapValue será herdada pelo usuário.
- Se o valor do atributo **memberOf** de um usuário não corresponder a nenhuma entidade do **ldapValue** no FTD, a Política de Grupo padrão para o Perfil de Conexão selecionado será herdada. Neste exemplo, **NOACCESS** Group-Policy é herdada de .

## Configurar

O Mapa de Atributos LDAP para FTD gerenciado pelo FDM está configurado com a API REST.

### Etapas de Configuração no FDM

**Etapa 1.** Verifique se o Dispositivo está registrado no **Smart Licensing**.



<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>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 <a href="#">REQUEST FILE TO BE CREATED</a>
<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>

â€f

**Etapa 2.** Verifique se as licenas do AnyConnect esto habilitadas no 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**  Enabled **DISABLE**

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

Includes: Intrusion Policy

**Malware** Disabled by user **ENABLE**

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

Includes: File Policy

**URL License**  Enabled **DISABLE**

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

Includes: URL Reputation

**RA VPN License** 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

**Etapa 3.** Verifique se os **recursos de exportação controlada** estão **Habilitados** no token.

## Device Summary

## Smart License

**CONNECTED**  
SUFFICIENT LICENSEAssigned V  
Export-cont  
Go to Cisco

Last sync: 11 Oct 2019 09:33 A

Next sync: 11 Oct 2019 09:43 A

## 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

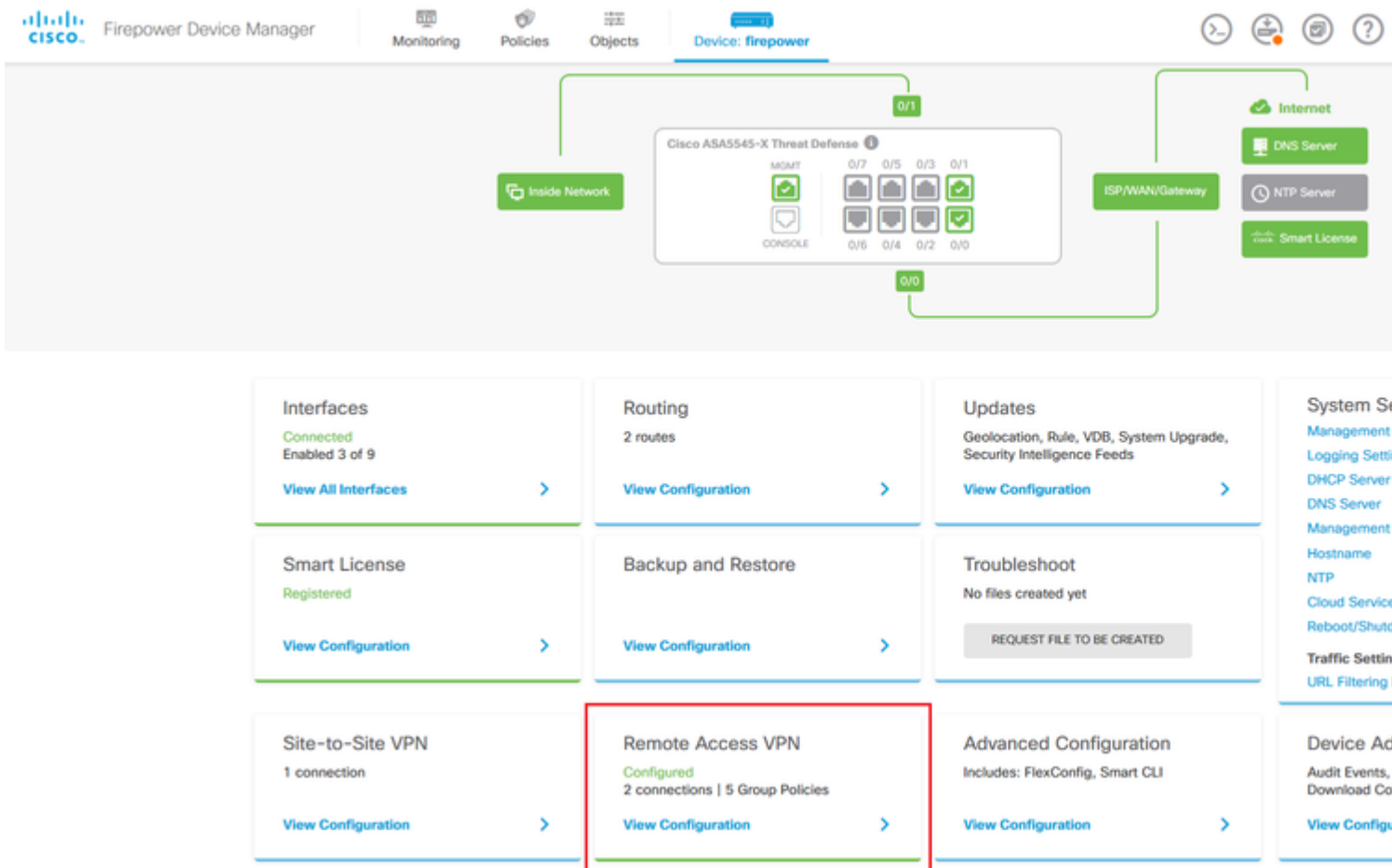
---

Observação: este documento pressupõe que o RA VPN já esteja configurado. Consulte o documento a seguir para obter mais informações sobre [Como configurar o RAVPN no FTD gerenciado pelo FDM](#).

---

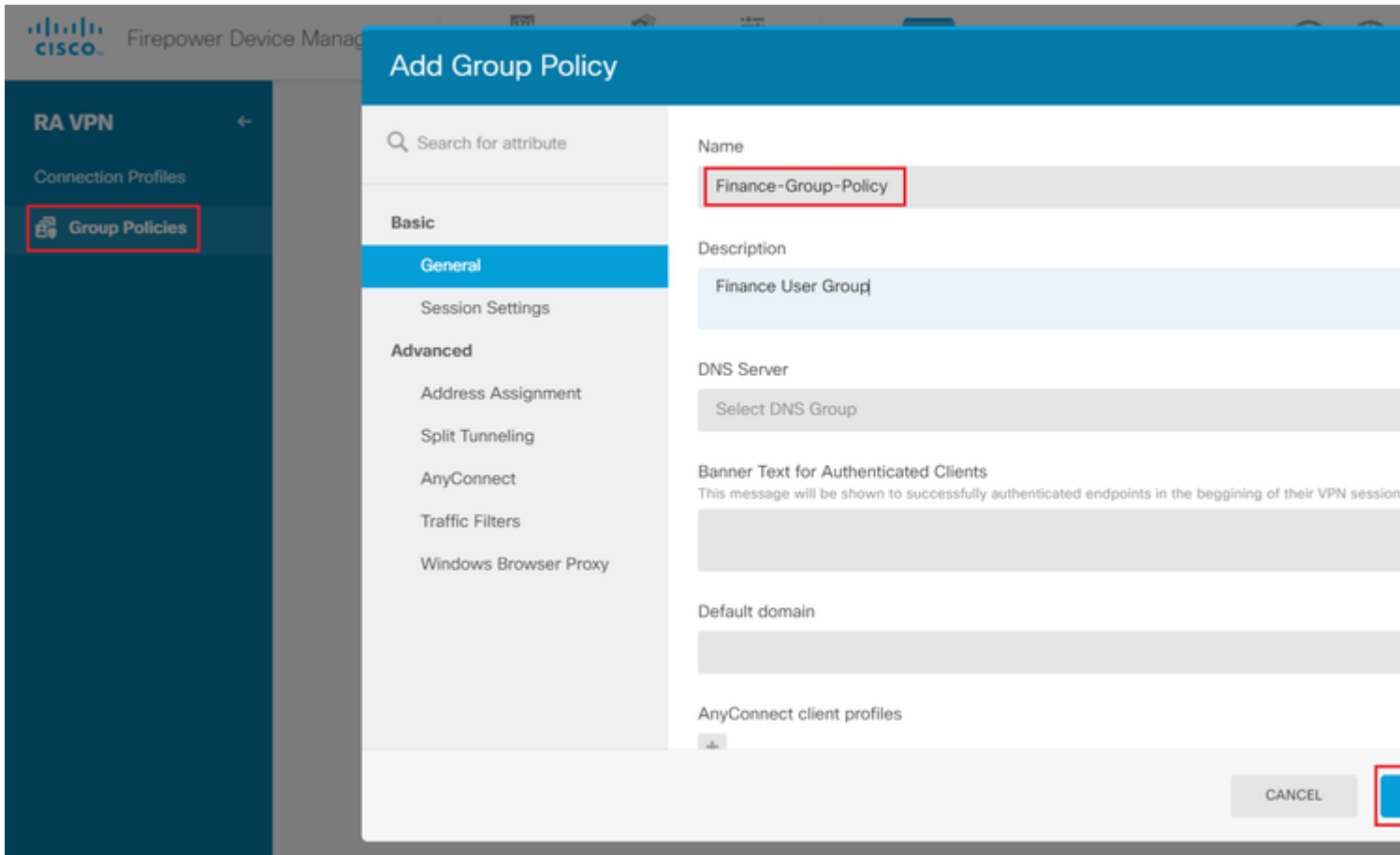
â€f

**Etapa 4.** Navegue até **Remote Access VPN** > Group Policies.



â€f

**Etapa 5.** Navegue até **Group Policies**. Clique em '+' para configurar as diretivas de grupo diferentes para cada grupo do AD. Neste exemplo, as pol ticas de grupo **Finance-Group-Policy**, **HR-Group-Policy** e **IT-Group-Policy** est o configuradas para ter acesso a diferentes sub-redes.



â€f

O **Finance-Group-Policy** tem as seguintes configurações:

```
<#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

Da mesma forma, **HR-Group-Policy** tem as configurações abaixo:

```
<#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

Por fim, **IT-Group-Policy** tem as próximas configurações:

```
<#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

**Etapa 6.** Crie uma política de grupo **NOACCESS**, navegue para **Configurações da sessão** e desmarque a opção **Logon simultâneo por usuário**. Isso define o valor **vpn-simultaneous-logins** como 0.

O valor **vpn-simultaneous-logins** na Política de Grupo quando definido como 0 termina imediatamente a conexão VPN do usuário. Este mecanismo é usado para impedir que os usuários que pertencem a qualquer Grupo de Usuários do AD que não os configurados (neste exemplo, Finanças, RH ou TI) estabeleçam conexões bem-sucedidas com o FTD e acessem recursos seguros disponíveis apenas para as contas de Grupo de Usuários permitidas.

Os usuários que pertencem a grupos de usuários do AD corretos correspondem ao mapa de atributos LDAP no FTD e herdam as políticas de grupo mapeadas, enquanto os usuários que não pertencem a nenhum dos grupos permitidos herdam a política de grupo padrão do perfil de conexão, que nesse caso é **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

A Diretiva de Grupo **NOACCESS** tem as seguintes configurações:

```
<#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
```

**Passo 7.** Navegue até **Perfis de conexão** e crie um Perfil de conexão. Neste exemplo, o nome do perfil é **Acesso remoto-LDAP**. Escolha **Primary Identity Source AAA Only** e crie um novo tipo de servidor de autenticação **AD**.

The screenshot shows the Cisco Firepower Device Manager interface for configuring a Connection Profile. The profile name is 'Remote-Access-LDAP'. The Primary Identity Source is set to 'AAA Only'. A dropdown menu is open for 'Primary Identity Source for User Authentication', showing 'LocalIdentitySource' and 'Special-Identities-Realm'. A 'Create new' button is visible, and a dropdown menu is open for 'AD'.

Insira as informações do servidor AD:

- Nome de usuário do diretório

- Senha do diretório
- DN base
- Domínio Primário do AD
- Nome de host/Endereço IP
- Porta
- Tipo de criptografia

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

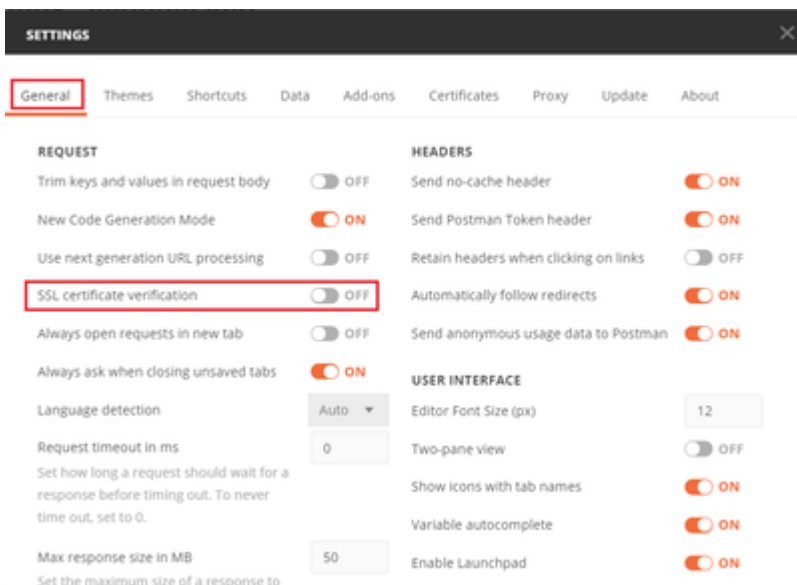
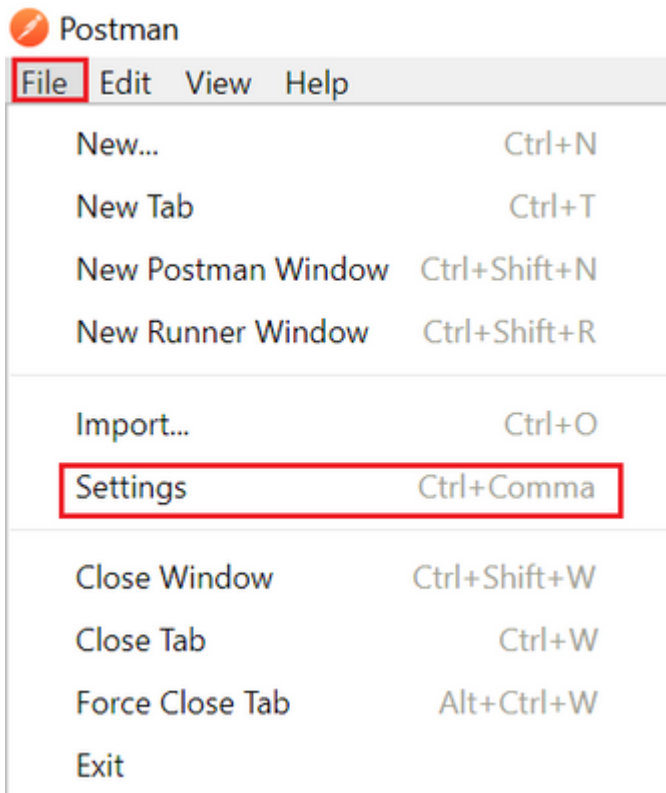
Please select a certificate

TEST

[Add another configuration](#)

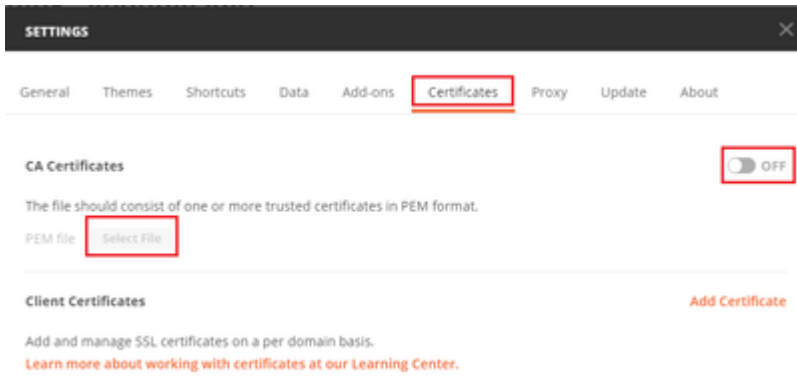
CANCEL

, desative a verificação de certificado SSL para evitar uma falha de handshake SSL ao enviar solicitações de API ao FTD. Isso é feito se o FTD usar um certificado autoassinado.



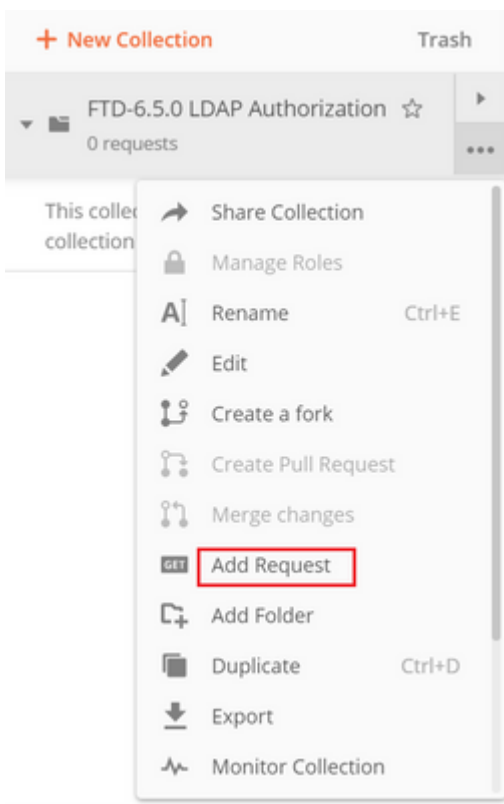
â€f

Como alternativa, o certificado usado pelo FTD pode ser adicionado como um certificado CA na seção Certificado das Configurações.

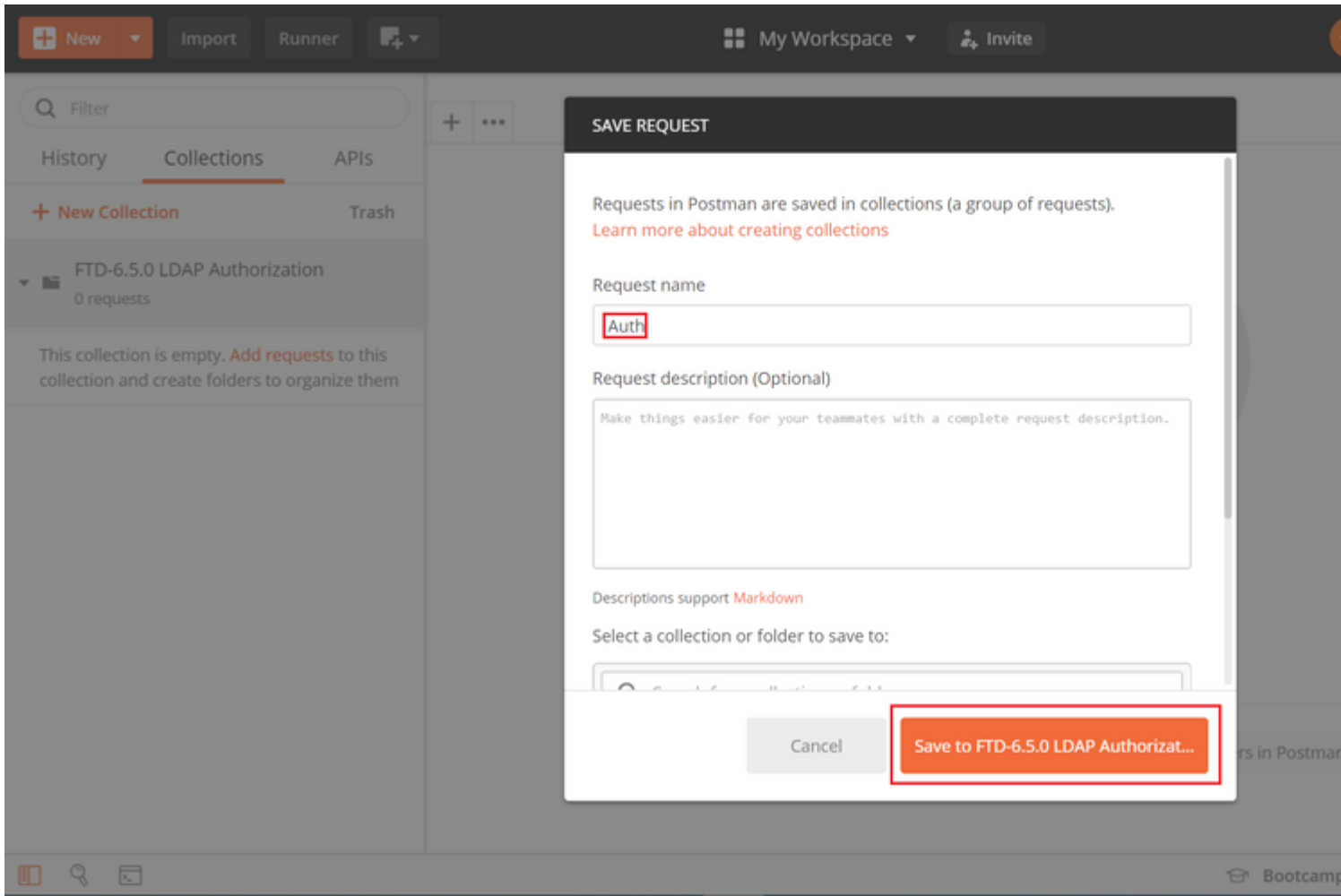


â€f

**Etapa 4.** Adicione uma nova solicitação POST **Auth** para criar uma solicitação POST de login para o FTD, para obter o token para autorizar qualquer solicitação POST/GET.







â€f

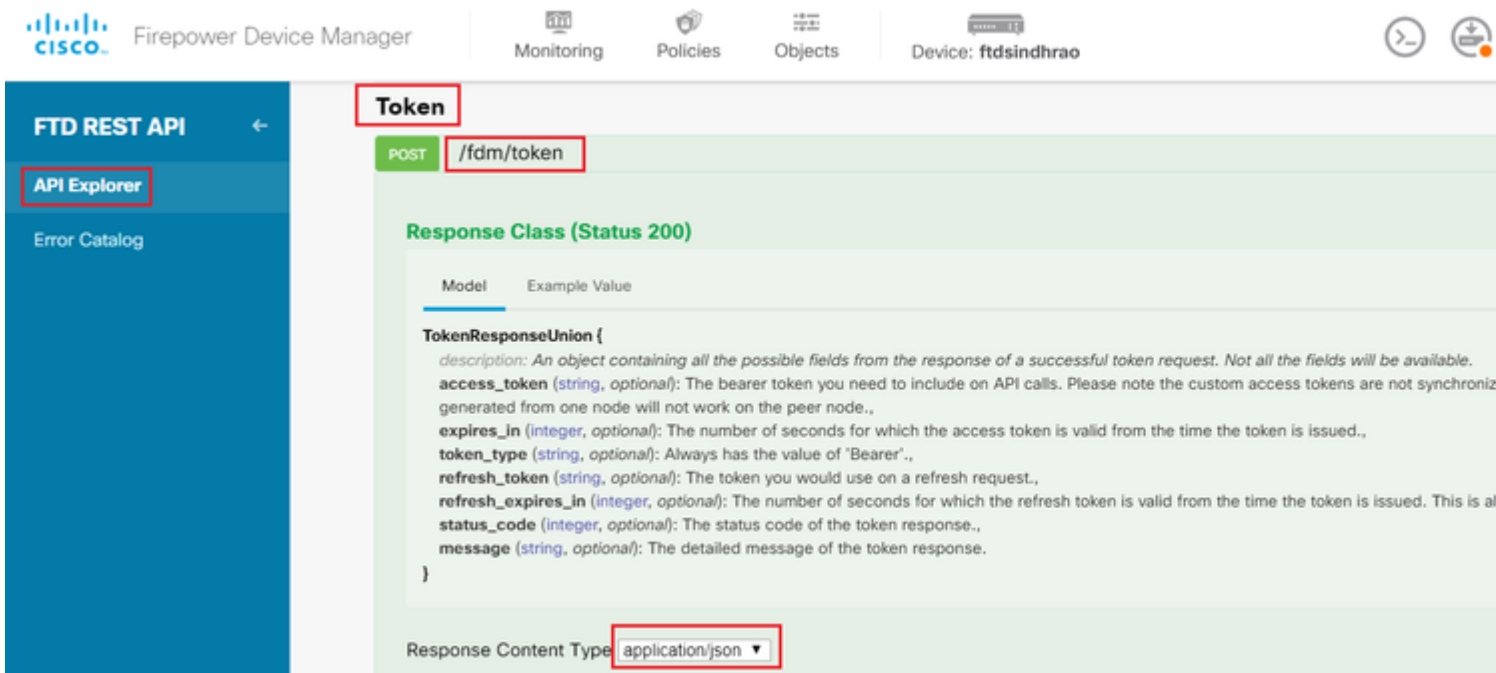
Todas as solicitações do Postman para esta coleção devem conter o seguinte:

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

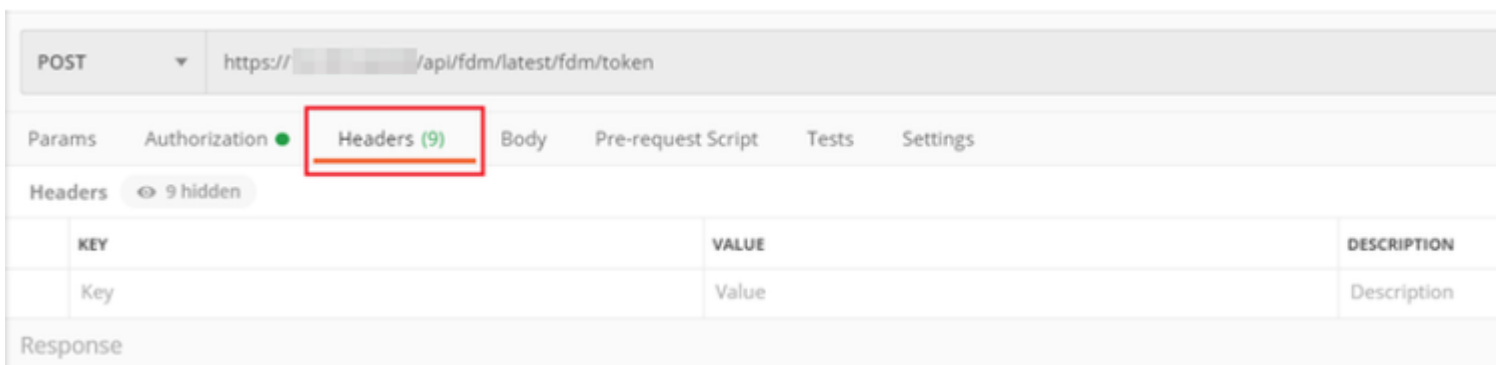
No URL de solicitação, anexe o URL base com os respectivos objetos que precisam ser adicionados ou modificados.

â€f

Aqui, uma solicitação de autenticação para um token é criada, referenciada de <https://<FTD Management IP>/api-explorer>. É necessário verificar se há outros objetos e fazer as alterações necessárias para eles.



Navegue até **Cabeçalhos** e clique em **Gerenciar Predefinições**.



â€f

Crie um novo **Cabeçalho** Predefinido-**LDAP** e adicione o seguinte par Chave-Valor:

Tipo de conteúdo	aplicativo/json
Aceitar	aplicativo/json

â€f

## MANAGE HEADER PRESETS

### Add Header Preset

Header-LDAP

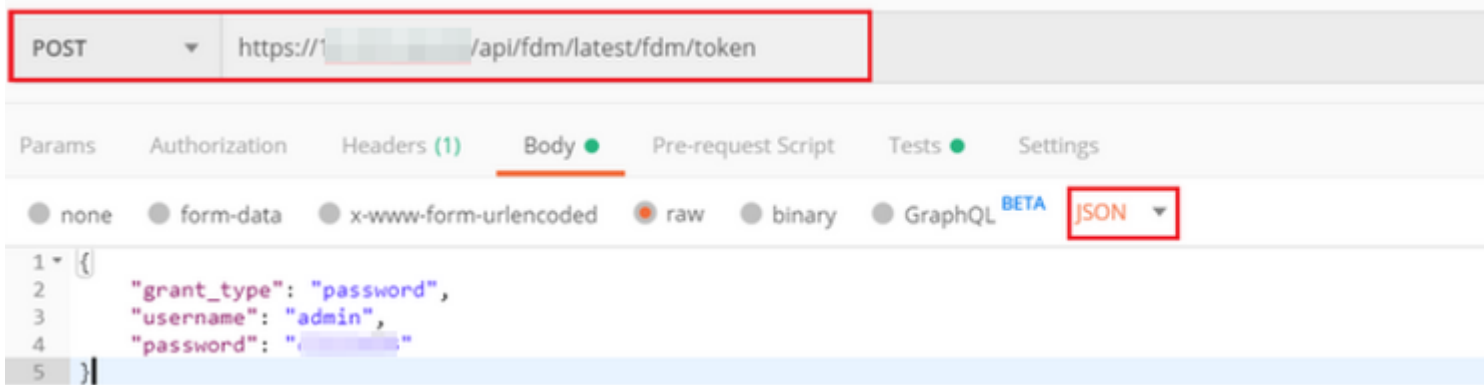
	KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/>	Content-Type	application/json	
<input checked="" type="checkbox"/>	Accept	application/json	
	Key	Value	Description

Para todas as outras solicitações, navegue até as respectivas guias Cabeçalho e selecione este valor de Cabeçalho Predefinido: **Cabeçalho-LDAP** para que as solicitações da API REST usem **json** como o tipo de dados principal.

O Corpo da Solicitação POST para obter o token deve conter o seguinte:

Tipo	Bruto - JSON (aplicativo/json)
grant_type	senha
nome do usuário	Admin Username para fazer login no FTD
senha	Senha associada à conta de usuário admin

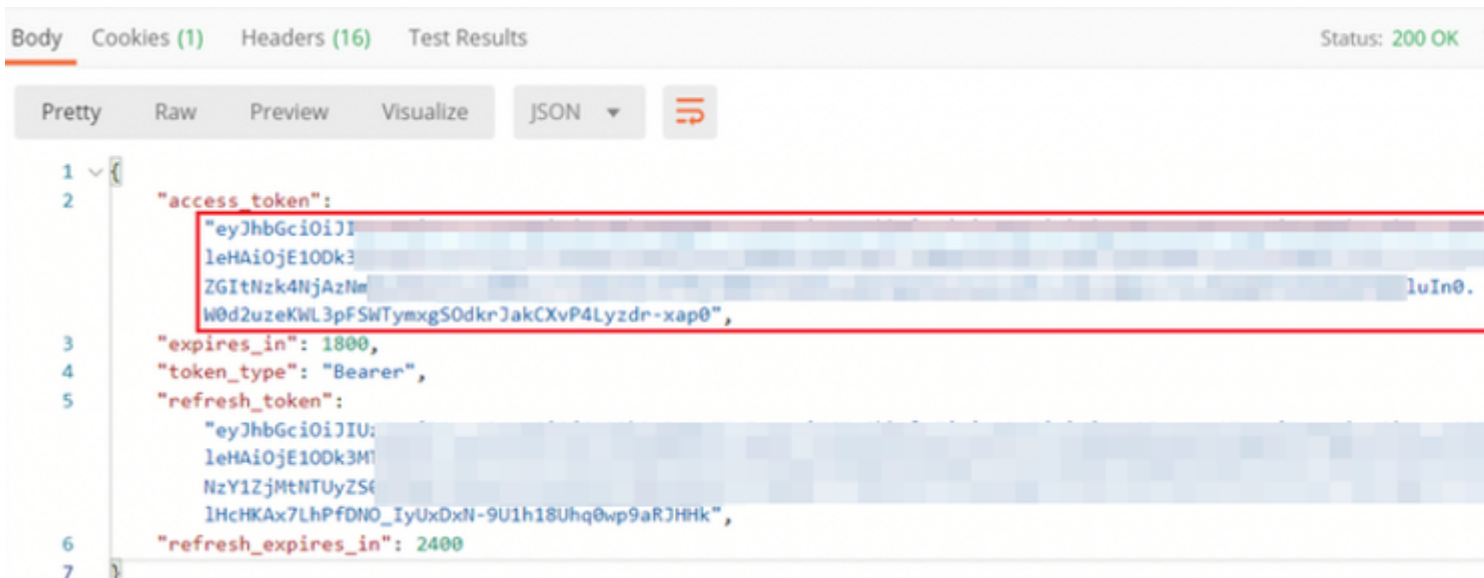
```
{
  "grant_type": "password",
  "username": "admin",
  "password": "<enter the password>"
}
```



â€f

Quando você clica em **enviar**, o corpo da resposta contém o token de acesso que é usado para enviar qualquer solicitação PUT/GET/POST ao FTD.

â€f



```
{
  "access_token": "eyJhbGciOiJIUzI1IiwiaXNjaWkiOiJkaXJkaXVpP4Lyzdr-xap0",
  "expires_in": 1800,
  "token_type": "Bearer",
  "refresh_token": "eyJhbGciOiJIUzI1IiwiaXNjaWkiOiJkaXJkaXVpP4Lyzdr-xap0",
  "refresh_expires_in": 2400
}
```

â€f

Esse token é usado para autorizar todas as solicitações subsequentes.

â€f

Navegue até a guia **Autorização** de cada nova solicitação e selecione a próxima:



```
58 {
59   "version": "2nidc13x12vu",
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   "enableGatewayOPD": false,
100  "gatewayOPDInterval": 30,
101  "enableClientOPD": false,
102  "clientOPDInterval": 30,
103  "clientProfiles": [],
104  "keepInstallerOnClient": false,
105  "vpnTrafficFilterACL": null,
106  "enableRestrictVPNTOVLAN": false,
107  "restrictVPNTOVLANId": null,
108  "clientFirewallPrivateNetworkRules": null,
109  "clientFirewallPublicNetworkRules": null,
110  "browserProxyType": "NO_PROXYIFY",
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

**Etapa 6.** Adicione uma nova solicitação POST **Create LDAP Attribute Map** para criar o mapa de atributos LDAP. Neste documento, o modelo **LdapAttributeMapping** é usado. Outros modelos também têm operações e métodos semelhantes para criar um mapa de atributos. Exemplos para esses modelos estão disponíveis no api-explorer, conforme mencionado anteriormente neste documento.

**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  
 }

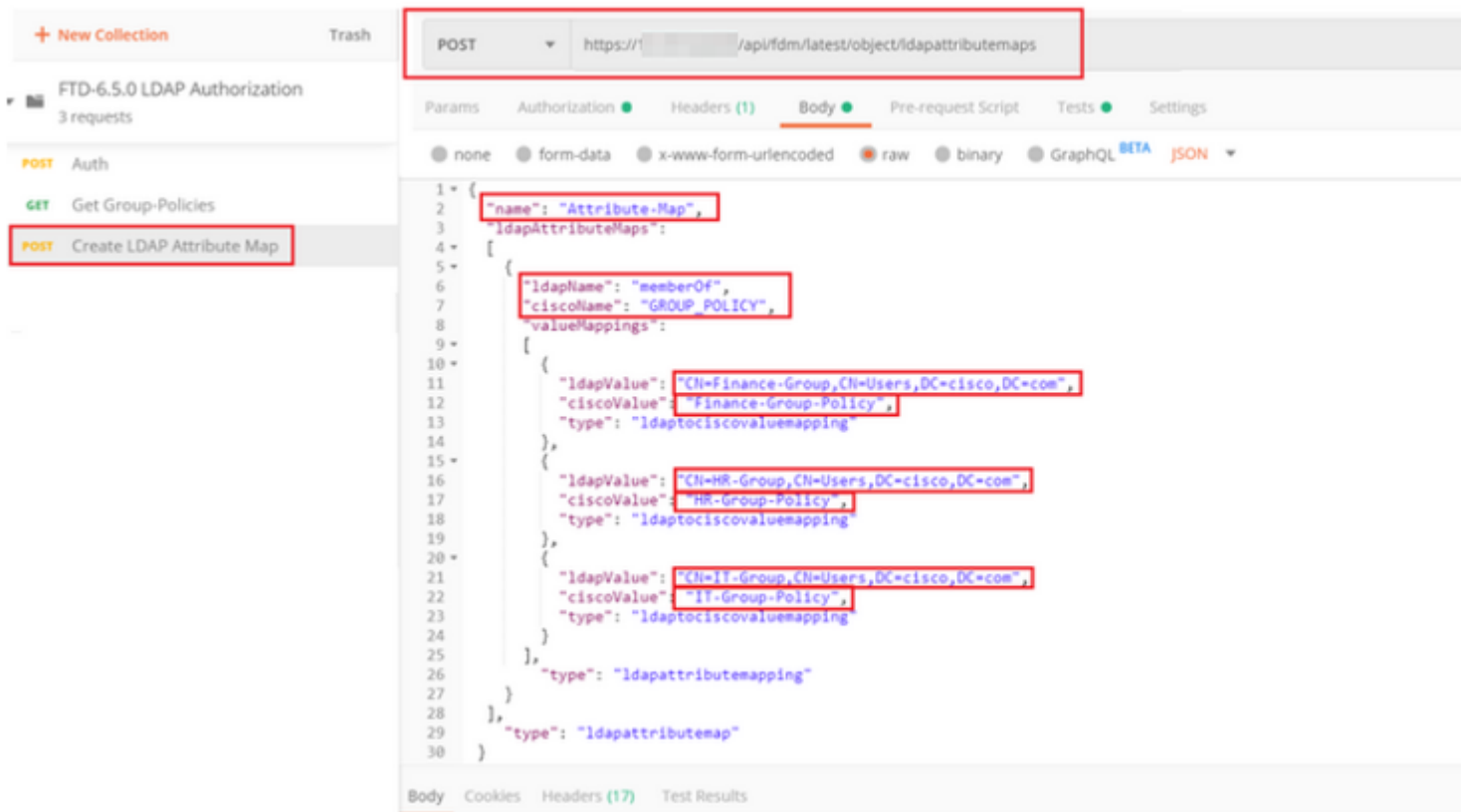
â€f

O URL para POSTAR o mapa de atributos LDAP é: <https://<FTD Management IP>/api/fdm/latest/object/ldapattributemaps>

O corpo da solicitação POST deve conter o seguinte:

nome	Nome do mapa de atributos LDAP
tipo	ldapattributemapping
ldapName	membroDe
ciscoName	GROUP_POLICY
ldapValue	valor memberOf para Usuário do AD
Valor da Cisco	Nome da Política de Grupo para cada Grupo de Usuários no FDM

â€f



â€f

O corpo da solicitação POST contém as informações do mapa de atributos LDAP que mapeia uma política de grupo específica para um grupo AD com base no valor **memberOf**:

```

{
  "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"
}

```

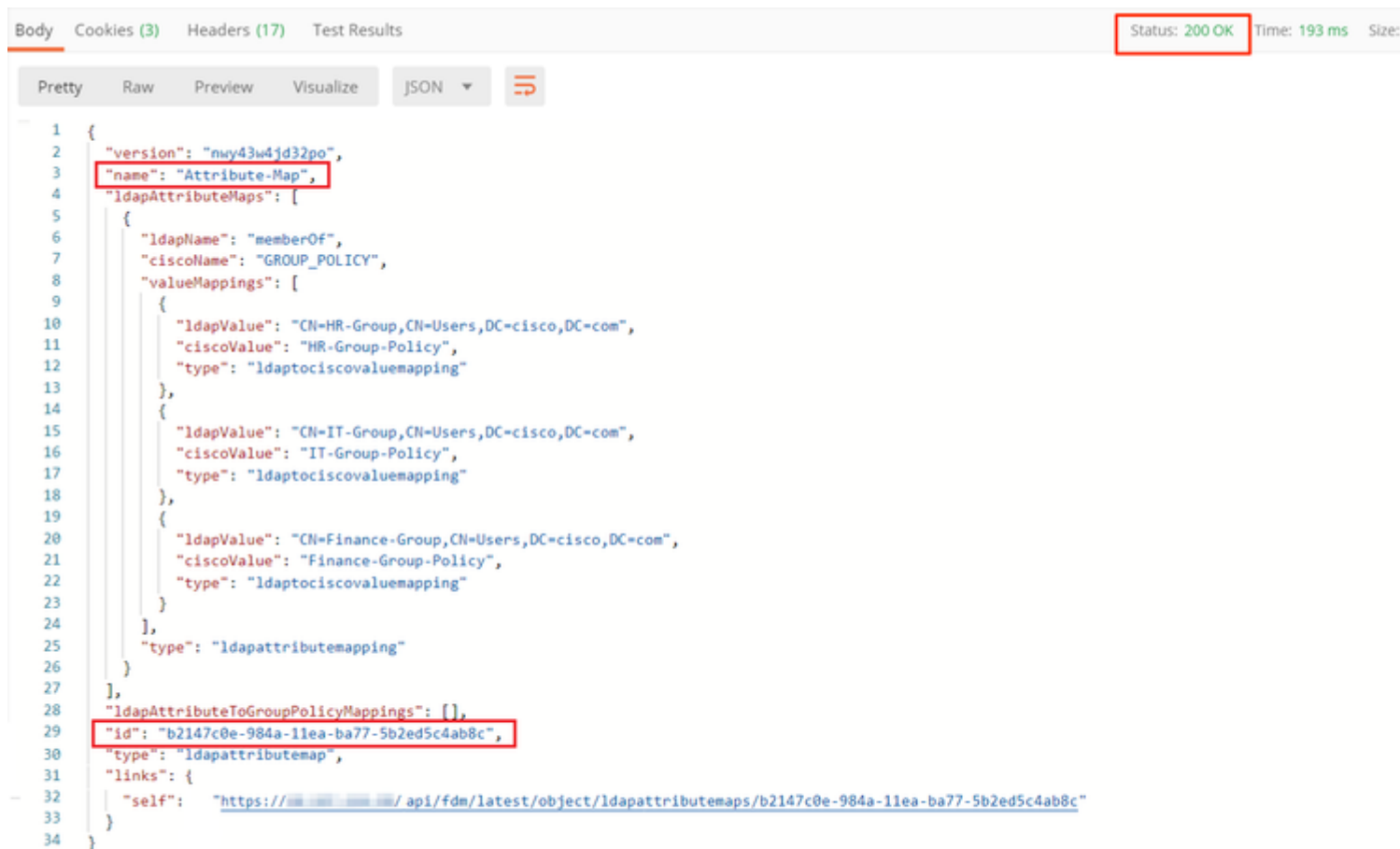


```
],  
  "type": "ldapattributemap"  
}
```

Observação: o campo **memberOf** pode ser recuperado do servidor AD com o comando **dsquery** ou pode ser buscado das depurações LDAP no FTD. Nos logs de depuração, procure o campo **memberOf value**:

â€f

A resposta desta solicitação POST é semelhante à próxima saída:

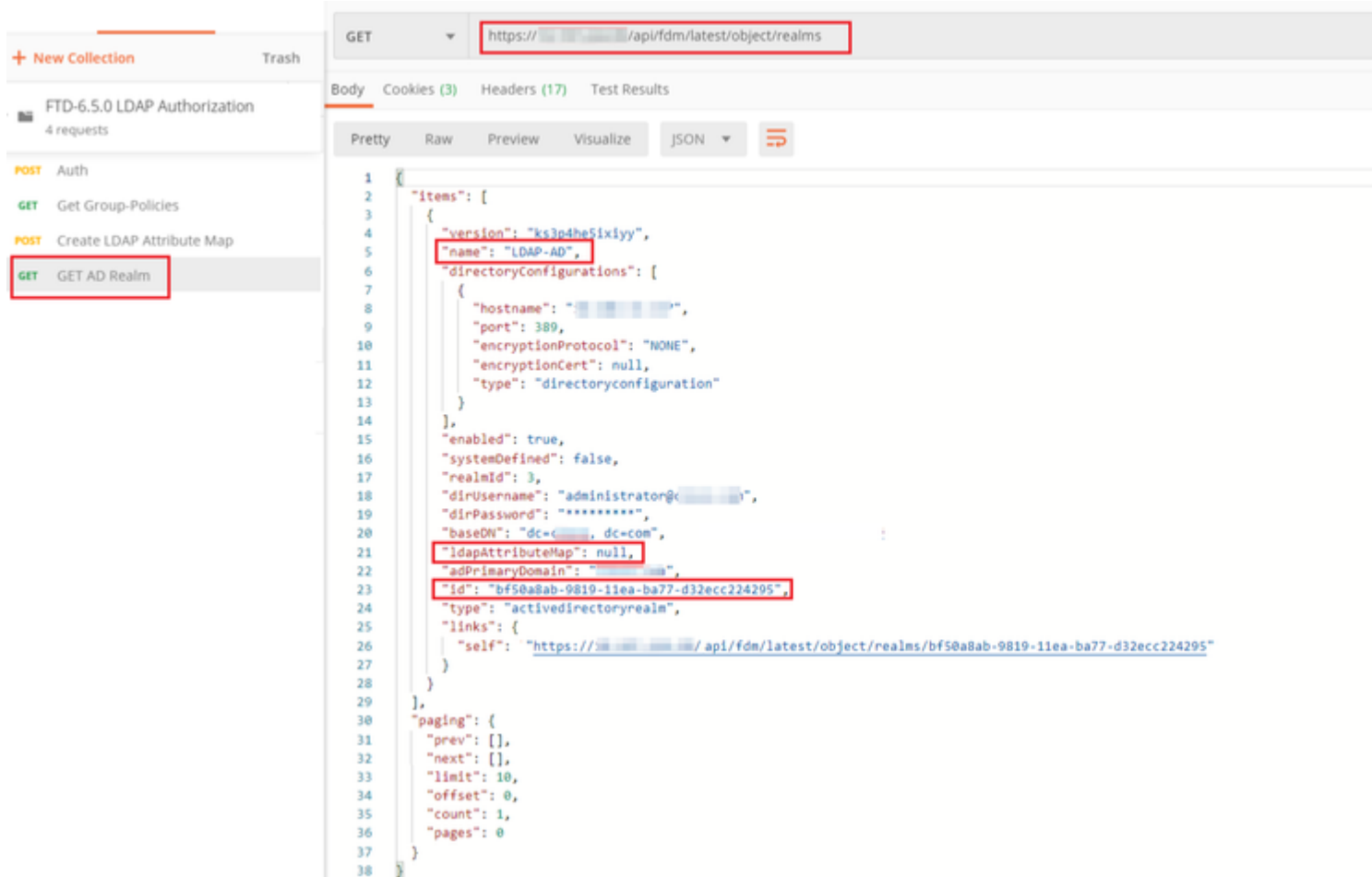


```
Body Cookies (3) Headers (17) Test Results Status: 200 OK Time: 193 ms Size:   
Pretty Raw Preview Visualize JSON   
1 {  
2   "version": "nwy43w4jd32po",  
3   "name": "Attribute-Map",  
4   "ldapAttributeMaps": [  
5     {  
6       "ldapName": "memberOf",  
7       "ciscoName": "GROUP_POLICY",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

**Passo 7.** Adicione uma nova solicitação GET para obter a configuração atual de realm do AD no FDM.

A URL para obter a configuração de realm do AD atual é: <https://<FTD Management IP>/api/fdm/latest/object/realms>

â€f



â€f

Observe que o valor da chave **ldapAttributeMap** é **null**.

â€f

**Etapa 8.** Crie uma nova solicitação **PUT** para editar o território AD. Copie a saída da resposta **GET** da etapa anterior e adicione-a ao Corpo desta nova solicitação **PUT**. Esta etapa pode ser usada para fazer modificações na configuração atual do Realm do AD, por exemplo: alterar a senha, o endereço IP ou adicionar um novo valor para qualquer chave, como **ldapAttributeMap**, neste caso.

Observação: é importante copiar o conteúdo da lista de itens em vez de copiar toda a saída da resposta GET. A URL de solicitação para a solicitação PUT deve ser anexada à ID do item do objeto para o qual as alterações são feitas. Neste exemplo, o valor é: bf50a8ab-9819-11ea-ba77-d32ecc224295

â€f

A URL para editar a configuração de realm atual do AD é: <https://<FTD Management IP>/api/fdm/latest/object/realms/<realm ID>>

O corpo da solicitação PUT deve conter o seguinte :

versão	versão obtida da resposta da solicitação GET anterior
id	ID obtida da resposta da solicitação GET anterior

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

O corpo da configuração neste exemplo é:

&lt;#root&gt;

```

{
  "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"

}
}
```

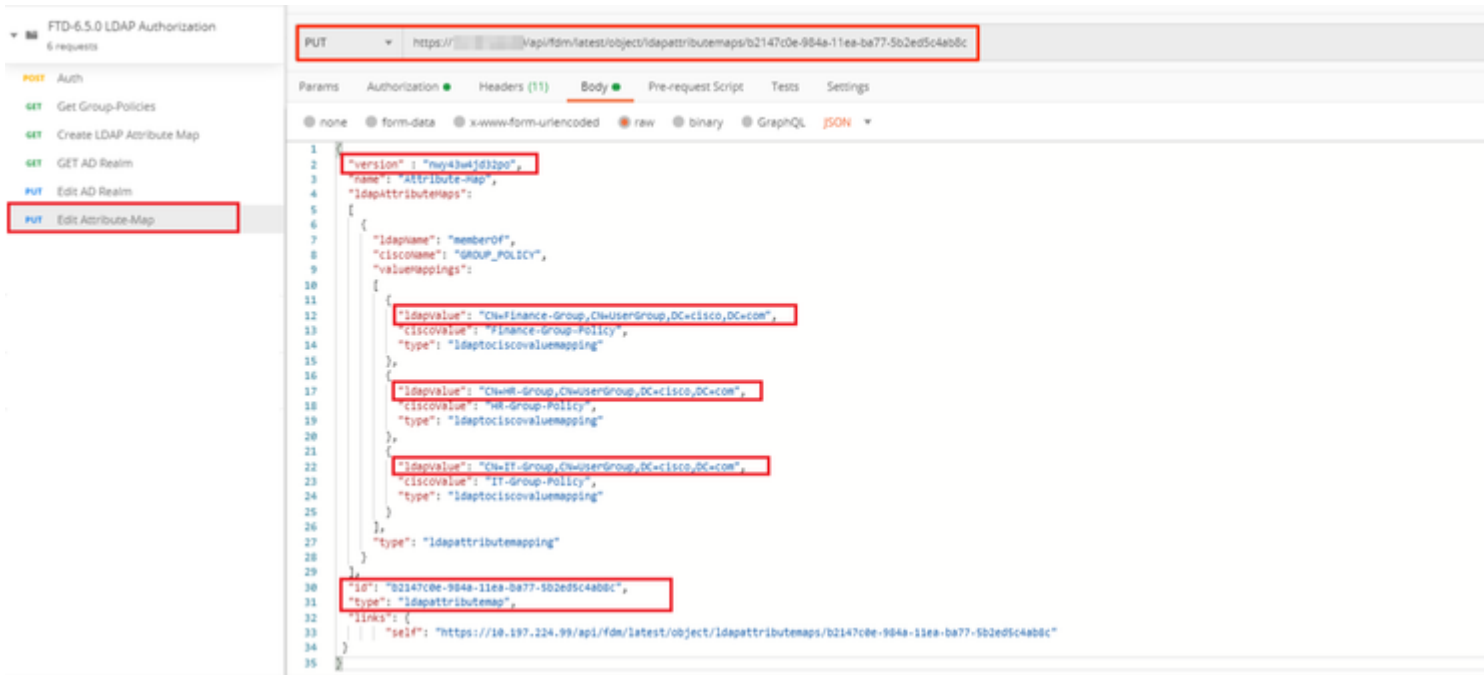
Verifique se a id de **ldapAttributeMap** corresponde ao Corpo da resposta para essa solicitação.

```
Body Cookies (3) Headers (17) Test Results Status: 200 OK
Pretty Raw Preview Visualize JSON
1 {
2   "version": "ksy7p574qfq7w",
3   "name": "LDAP-AD",
4   "directoryConfigurations": [
5     {
6       "hostname": ":",
7       "port": 389,
8       "encryptionProtocol": "NONE",
9       "encryptionCert": null,
10      "type": "directoryconfiguration"
11    }
12  ],
13  "enabled": true,
14  "systemDefined": false,
15  "realmId": 3,
16  "dirUsername": "administrator",
17  "dirPassword": "*****",
18  "baseDN": "dc=, dc=com",
19  "ldapAttributeMap": {
20    "version": "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:// / api/fdm/latest/object/realms/bf50a8ab-9819-11ea-ba77-d32ecc224295"
30  }
31 }
```

â€f

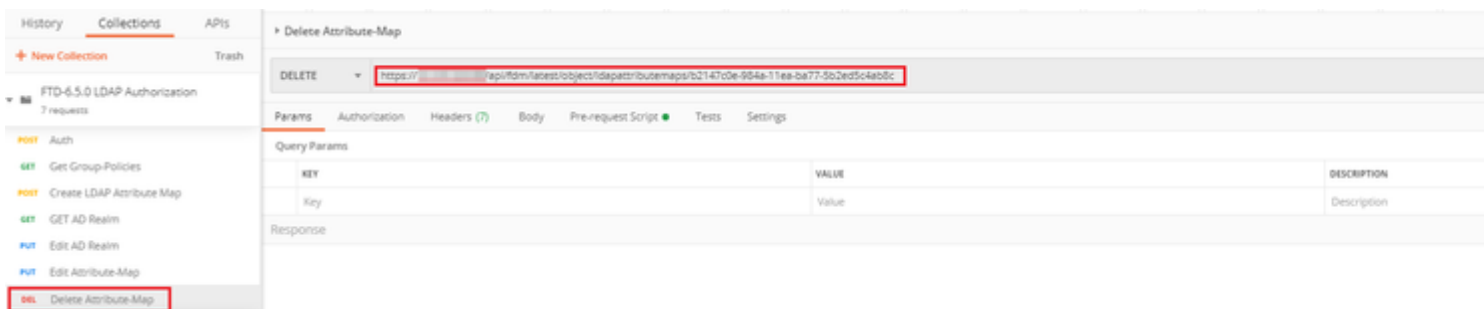
(Opcional). O mapa de atributos LDAP pode ser modificado com as solicitações **PUT**. Crie uma nova solicitação PUT **Edit Attribute-Map** e faça alterações como o nome do valor Attribute-Map ou memberOf. T

No próximo exemplo, o valor de **ldapvalue** foi modificado de **CN=Users** para **CN=UserGroup** para todos os três grupos.



â€f

**(Opcional).** Para excluir um mapa de atributos LDAP existente, crie uma solicitação DELETE **Delete Attribute-Map**. Inclua o **map-id** da resposta HTTP anterior e anexe com a URL base da solicitação de exclusão.



Observação: Se o atributo **memberOf** contiver espaços, ele deverá ser codificado por URL para que o Servidor Web o analise. Caso contrário, uma **Resposta HTTP de Solicitação 400 Inválida** é recebida. Para cadeias de caracteres que contêm espaços em branco, "%20" ou "+" podem ser usadas para evitar este erro.

â€f

**Etapa 9.** Volte para o FDM, selecione o ícone Implantação e clique em **Implantar Agora**.

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
+ <b>Idapattributemap Added: <i>Attribute-Map</i></b>	
-	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

✎ **Active Directory Realm Edited: *LDAP-AD***

ldapAttributeMap :	
-	Attribute-Map

MORE ACTIONS ▾

CANCEL

â€f

## Verificar

As alterações de implantação podem ser verificadas na seção **Histórico de Implantação** do FDM.

**Device Administration** ←

Audit Log

Download Configuration

Deployment Completed: User (admin) Triggered Deployment

Summary Differences View

Deployed Version	Pending Version
------------------	-----------------

+ Idapattributemap Added: Attribute-Map

Entity ID: b2147c8e-984a-11ea-ba77-5b2ed5c4ab8c

-	ldapAttributeMaps[0].ldap
-	ldapAttributeMaps[0].value
-	ldapAttributeMaps[0].value
-	ldapAttributeMaps[0].value
-	ldapAttributeMaps[0].value
-	ldapAttributeMaps[0].value
-	ldapAttributeMaps[0].value
-	ldapAttributeMaps[0].value
-	ldapAttributeMaps[0].cisco
-	name: Attribute-Map

Active Directory Realm Edited: LDAP-AD

Entity ID: bf50a8ab-9819-11ea-ba77-d32ecc224295

ldapAttributeMap:	
-	Attribute-Map

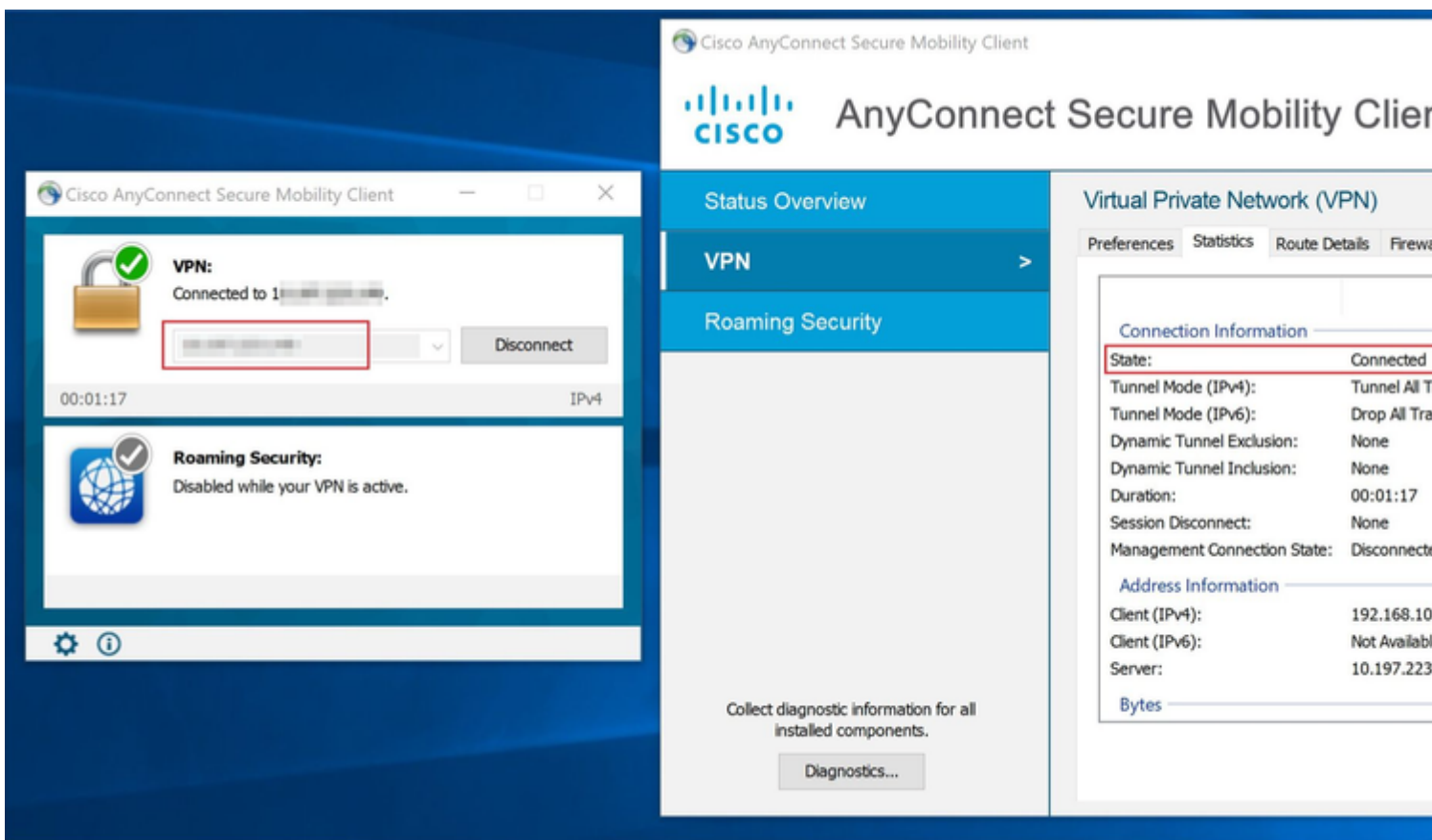
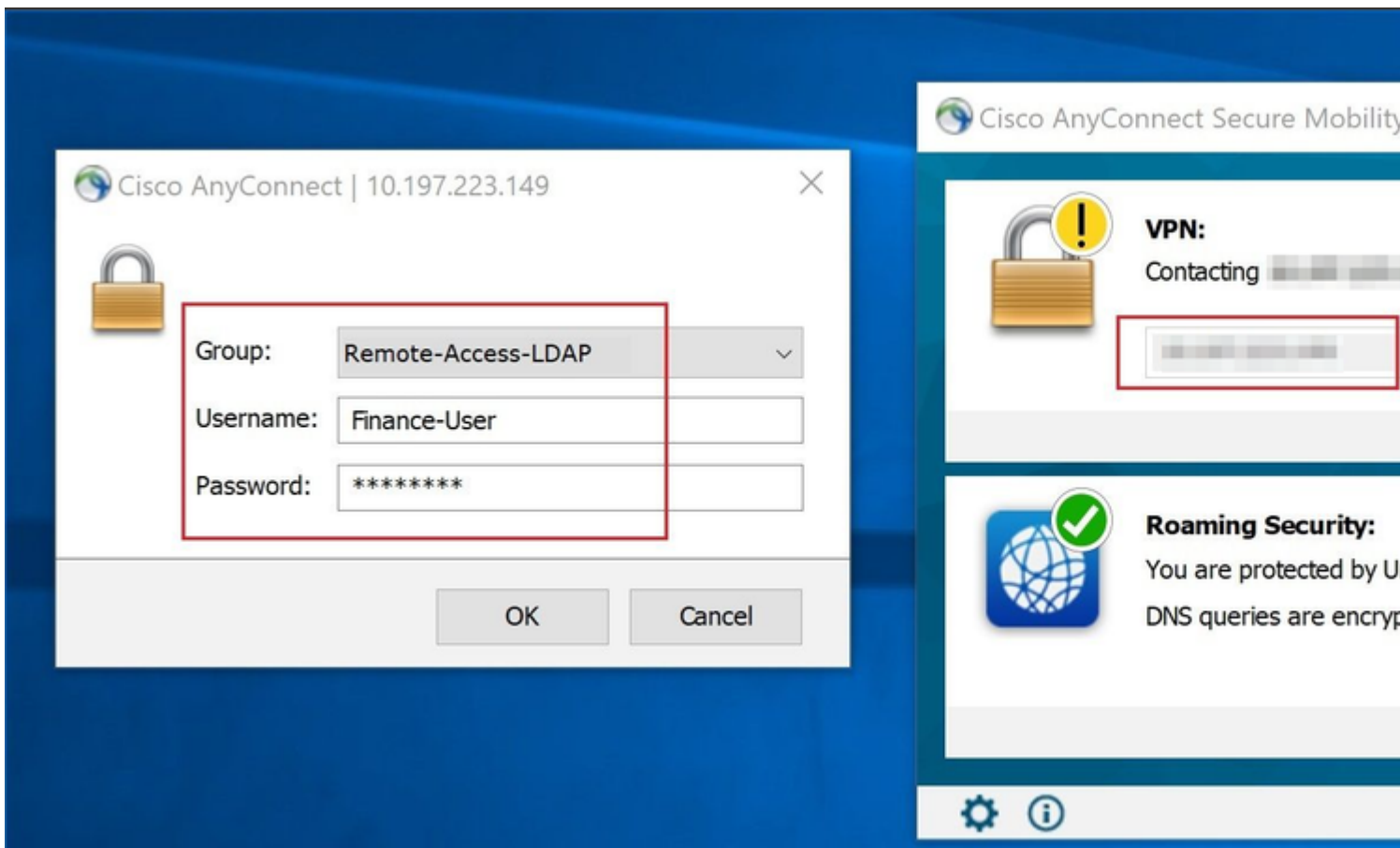
â€f

Para testar essa configuração, forneça as credenciais do AD nos campos **Nome de usuário** e **Senha**.

Quando um usuário que pertence ao grupo AD **Finance-Group** tenta fazer logon, a tentativa é bem-sucedida como esperado.

â€f

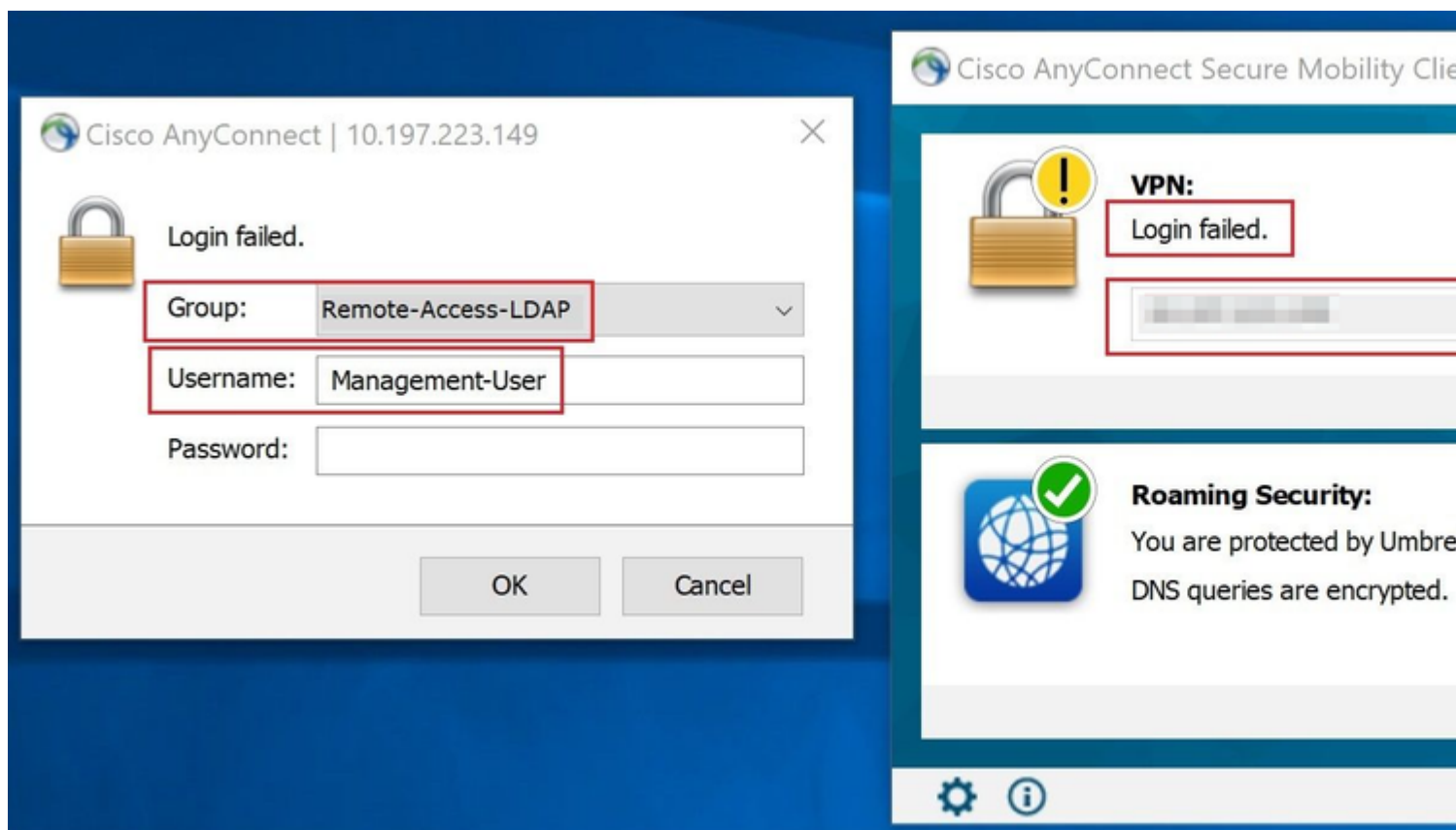




â€f

Quando um usu rio que pertence ao **Management-Group** no AD tenta se conectar ao Connection-Profile

**Remote-Access-LDAP**, já que nenhum Mapa de Atributos LDAP retornou uma correspondência, a Política de Grupo herdada por esse usuário no FTD é **NOACCESS** que tem vpn-simultaneous-logins definidos com o valor 0. Portanto, a tentativa de login para esse usuário falha.



â€f

A configuração pode ser verificada com os próximos comandos show da CLI do FTD:

```
<#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
Auds 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
```

## Troubleshooting

Um dos problemas mais comuns na configuração da API REST é renovar o token de transporte de tempos em tempos. O tempo de expiração do token é fornecido na Resposta para a solicitação de Autenticação. Se esse tempo expirar, um token de atualização adicional poderá ser usado por mais tempo. Depois que o token de atualização também expira, uma nova solicitação de Autenticação deve ser enviada para um novo token de acesso recuperado.

---

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

---

Você pode definir vários níveis de depuração. Por padrão, o nível 1 é usado. Se você alterar o nível de depuração, o detalhamento das depurações poderá aumentar. Faça isso com cuidado, especialmente em ambientes de produção.

---

As seguintes depurações no FTD CLI seriam úteis na solução de problemas relacionados ao mapa de atributos LDAP

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

Neste exemplo, as próximas depurações foram coletadas para demonstrar as informações recebidas do servidor AD quando os usuários de teste mencionados antes de se conectarem.

Depurações LDAP para **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 = 201910111094757.0Z  
[48] dSCorePropagationData: value = 201910111094614.0Z  
[48] dSCorePropagationData: value = 16010101000000.0Z  
[48] lastLogonTimestamp: value = 132153412825919405  
[48] Fiber exit Tx=538 bytes Rx=2720 bytes, status=1  
[48] Session End

## Depurações LDAP para **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

## Informações Relacionadas

Para obter assistência adicional, entre em contato com o Cisco Technical Assistance Center (TAC). É necessário um contrato de suporte válido: [Contatos de suporte da Cisco no mundo inteiro.](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.