

# Configurer le mappage d'attributs LDAP pour RAVPN sur FTD géré par FDM

## Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Flux d'authentification](#)

[Flux de mappage d'attribut LDAP expliqué](#)

[Configurer](#)

[Étapes de configuration sur FDM](#)

[Étapes de configuration du mappage d'attributs LDAP](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

## Introduction

Ce document décrit la procédure d'utilisation d'un serveur LDAP (Lightweight Directory Access Protocol) pour authentifier et autoriser les utilisateurs VPN d'accès à distance (RA VPN), et leur accorder un accès réseau différent en fonction de leur appartenance à un groupe sur le serveur LDAP.

## Conditions préalables

### Exigences

- Connaissances de base de la configuration VPN RA sur Firewall Device Manager (FDM)
- Connaissance de base de la configuration du serveur LDAP sur FDM
- Connaissances de base de l'API REST (REpresentational State Transfer) et de l'explorateur d'API FDM Rest
- Cisco FTD version 6.5.0 ou ultérieure gérée par FDM

### Composants utilisés

Les versions matérielles et logicielles suivantes des applications/périphériques ont été utilisées :

- Cisco FTD version 6.5.0, build 115
- Cisco AnyConnect version 4.10
- Serveur Microsoft Active Directory (AD)
- Postman ou tout autre outil de développement d'API

---

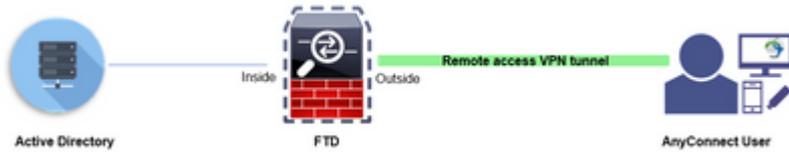
Remarque : la prise en charge de la configuration du serveur Microsoft AD et de l'outil Courrier postal n'est pas fournie par Cisco.

---

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. Si votre réseau est en ligne,

assurez-vous de bien comprendre l'incidence possible des commandes.

## Flux d'authentification



### Flux de mappage d'attribut LDAP expliqué

1. L'utilisateur initie une connexion VPN d'accès à distance au FTD et fournit un nom d'utilisateur et un mot de passe pour son compte Active Directory (AD).
2. Le FTD envoie une requête LDAP au serveur AD via le port 389 ou 636 (LDAP via SSL)
3. La DA répond au FTD avec tous les attributs associés à l'utilisateur.
4. Le FTD fait correspondre les valeurs d'attribut reçues avec le mappage d'attribut LDAP créé sur le FTD. Il s'agit du processus d'autorisation.
5. L'utilisateur se connecte ensuite et hérite des paramètres de la stratégie de groupe correspondant à l'attribut **memberOf** dans le mappage d'attributs LDAP.

Dans le cadre de ce document, l'autorisation des utilisateurs AnyConnect est effectuée à l'aide de l'attribut **memberOf** LDAP.

- L'attribut **memberOf** du serveur LDAP pour chaque utilisateur est mappé à une entité **ldapValue** sur le FTD. Si l'utilisateur appartient au groupe AD correspondant, la stratégie de groupe associée à cette valeur ldap est héritée par l'utilisateur.
- Si la valeur de l'attribut **memberOf** pour un utilisateur ne correspond à aucune entité **ldapValue** sur le FTD, la stratégie de groupe par défaut pour le profil de connexion sélectionné est héritée. Dans cet exemple, **NOACCESS** Group-Policy est hérité de .

### Configurer

Le mappage d'attributs LDAP pour FTD géré par FDM est configuré avec l'API REST.

#### Étapes de configuration sur FDM

**Étape 1.** Vérifiez que le périphérique est enregistré dans **Smart Licensing**.



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

â€f

**Étape 2.** Vérifiez que les **licences AnyConnect** sont activées sur 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** DISABLE  
Enabled  
This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.  
Includes: Intrusion Policy

**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

**Étape 3.** Vérifiez que les fonctions d'exportation contrôlée sont activées dans le jeton.

Device Summary  
Smart License



**CONNECTED**  
**SUFFICIENT LICENSE**

Assigned 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

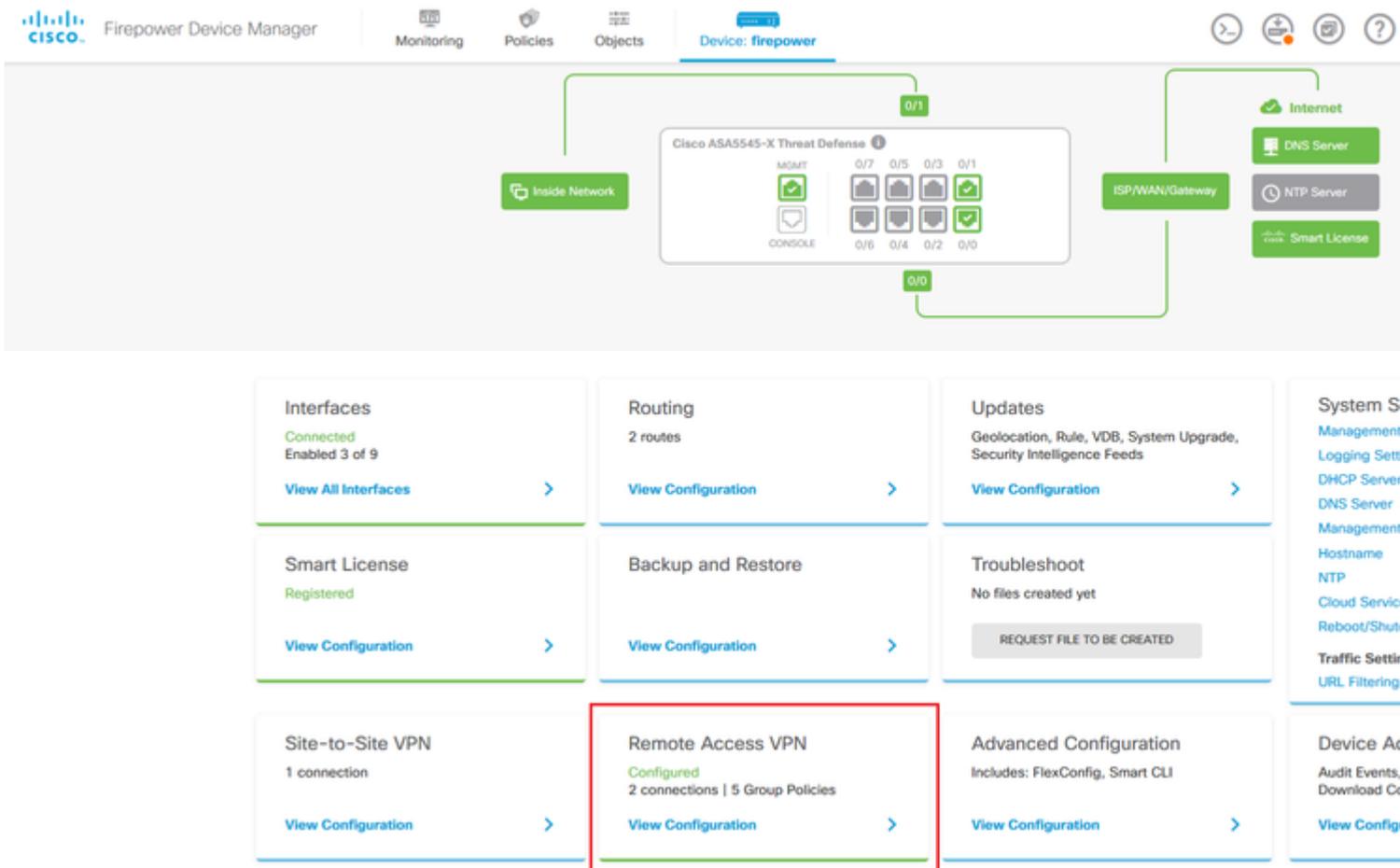
---

Remarque : ce document suppose que RA VPN est déjà configuré. Reportez-vous au document suivant pour plus d'informations sur la [façon de configurer RAVPN sur FTD géré par FDM](#).

---

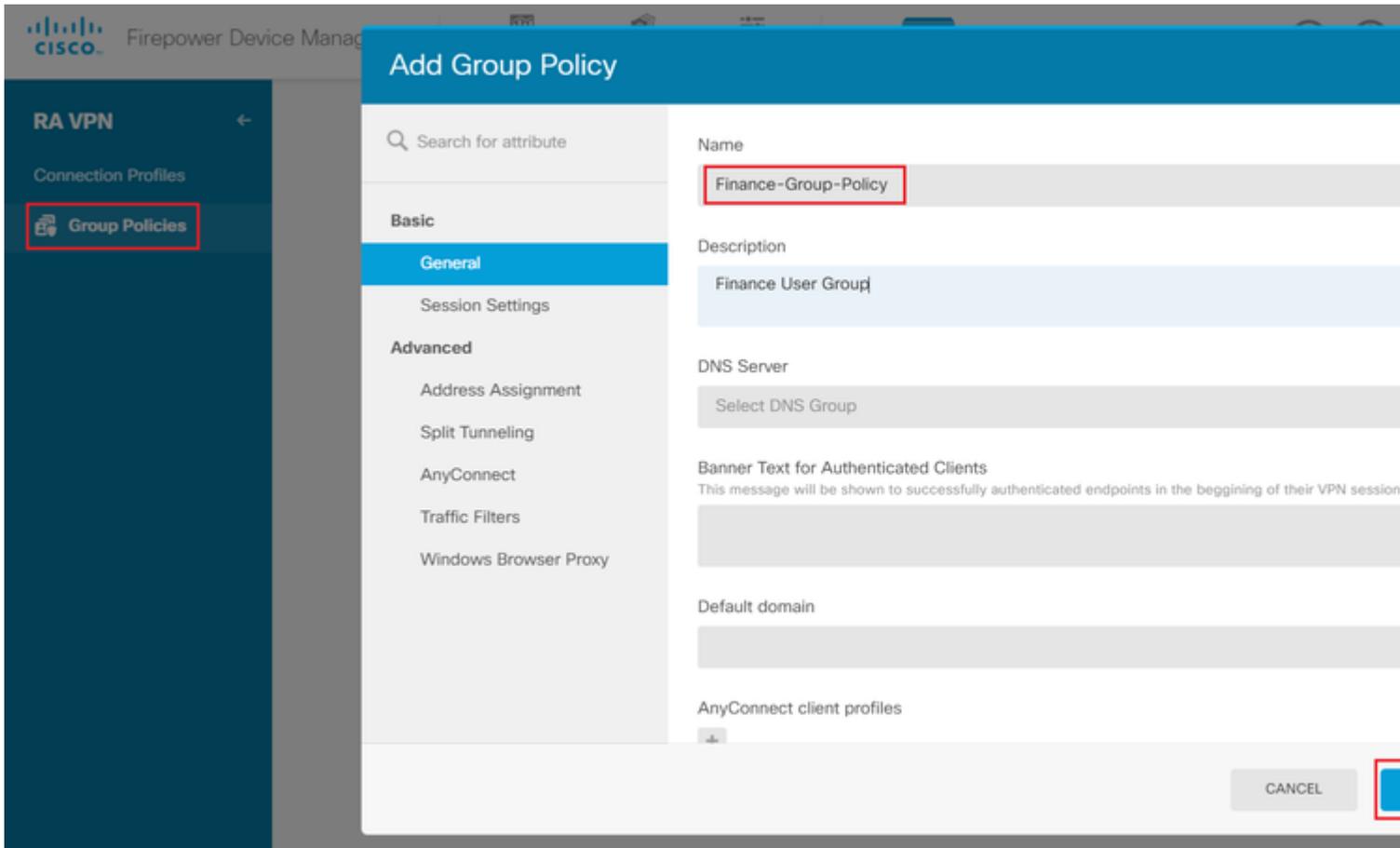
â€f

**Étape 4.** Accédez à **Remote Access VPN > Group Policies**.



â€f

**Étape 5.** Accédez à **Stratégies de groupe**. Cliquez sur « + » pour configurer les différentes stratégies de groupe pour chaque groupe Active Directory. Dans cet exemple, les stratégies de groupe **Finance-Group-Policy**, **HR-Group-Policy** et **IT-Group-Policy** sont configurées pour avoir accès à différents sous-réseaux.



â€f

La **stratégie de groupe Finance** comporte les paramètres suivants :

<#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

De même, **HR-Group-Policy** a les paramètres suivants :

```
<#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

Enfin, **IT-Group-Policy** dispose des paramètres suivants :

```
<#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

**Étape 6.** Créez une stratégie de groupe **NOACCESS**, accédez à **Paramètres de session** et décochez l'option **Connexion simultanée par utilisateur**. Cela définit la valeur **vpn-simultanément-logins** à 0.

La valeur **vpn-simultanée-logins** dans la stratégie de groupe lorsqu'elle est définie sur 0 met fin immédiatement à la connexion VPN de l'utilisateur. Ce mécanisme est utilisé pour empêcher les utilisateurs qui appartiennent à un groupe d'utilisateurs AD autre que ceux configurés (dans cet exemple, Finance, RH ou IT) d'établir des connexions réussies au FTD et d'accéder aux ressources sécurisées disponibles uniquement pour les comptes de groupe d'utilisateurs autorisés.

Les utilisateurs qui appartiennent aux groupes d'utilisateurs AD corrects correspondent au mappage d'attribut LDAP sur le FTD et héritent des stratégies de groupe mappées, tandis que les utilisateurs qui n'appartiennent à aucun des groupes autorisés héritent de la stratégie de groupe par défaut du profil de connexion, qui dans ce cas est **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

La stratégie de groupe **NOACCESS** a les paramètres suivants :

```
<#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
```

**Étape 7.** Accédez à **Profils de connexion** et créez un profil de connexion. Dans cet exemple, le nom du profil est **Remote-Access-LDAP**. Choisissez Primary Identity Source **AAA Only** et créez un nouveau type de serveur d'authentification **AD**.

The screenshot shows the Cisco Firepower Device Manager interface for configuring a connection profile. The profile name is 'Remote-Access-LDAP'. The authentication type is set to 'AAA Only'. The primary identity source for user authentication is 'LocalIdentitySource', and a new source 'AD' is being created. The fallback local identity source is 'Please Select Local Identity Source'. The 'NEXT' button is visible at the bottom right.

Entrez les informations du serveur AD :

- Nom d'utilisateur

- Mot de passe du répertoire
- DN de base
- Domaine principal AD
- Nom d'hôte / Adresse IP
- Port
- Type de chiffrement

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

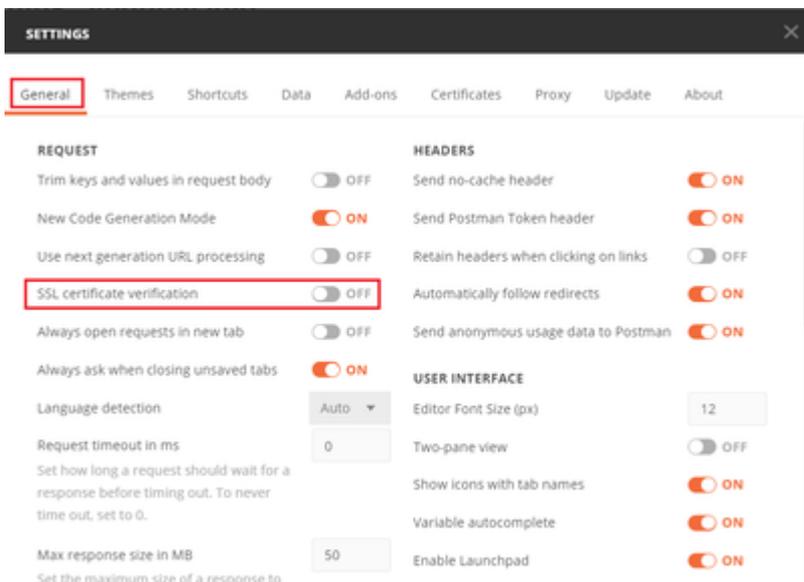
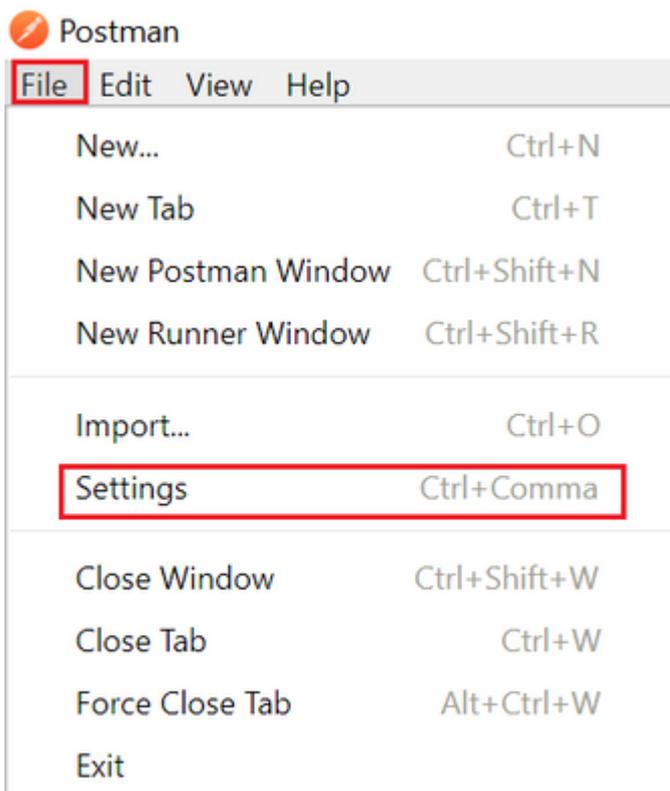
Please select a certificate

TEST

[Add another configuration](#)

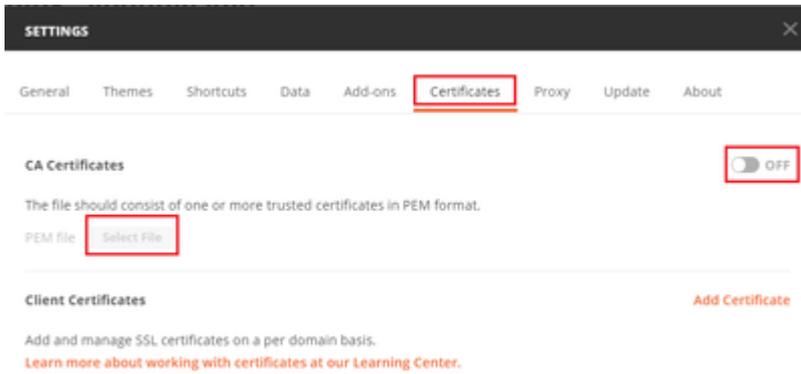
CANCEL

, désactivez la vérification du certificat SSL pour éviter un échec de connexion SSL lors de l'envoi de requêtes API au FTD. Cette opération est effectuée si le FTD utilise un certificat auto-signé.



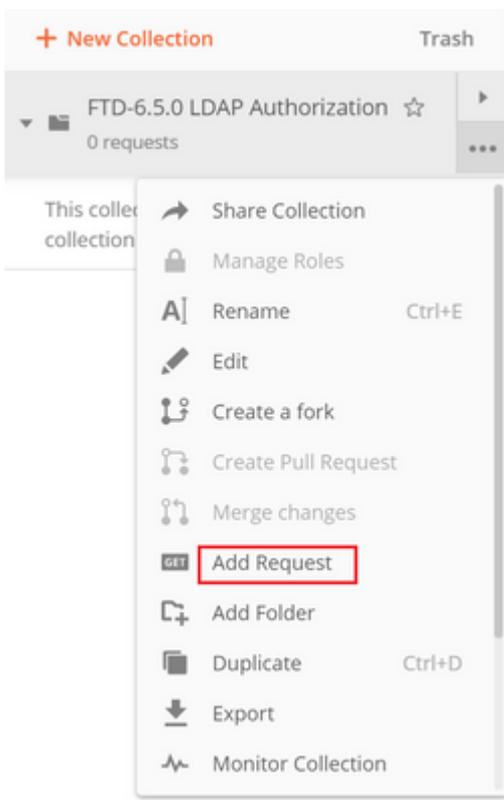
â€f

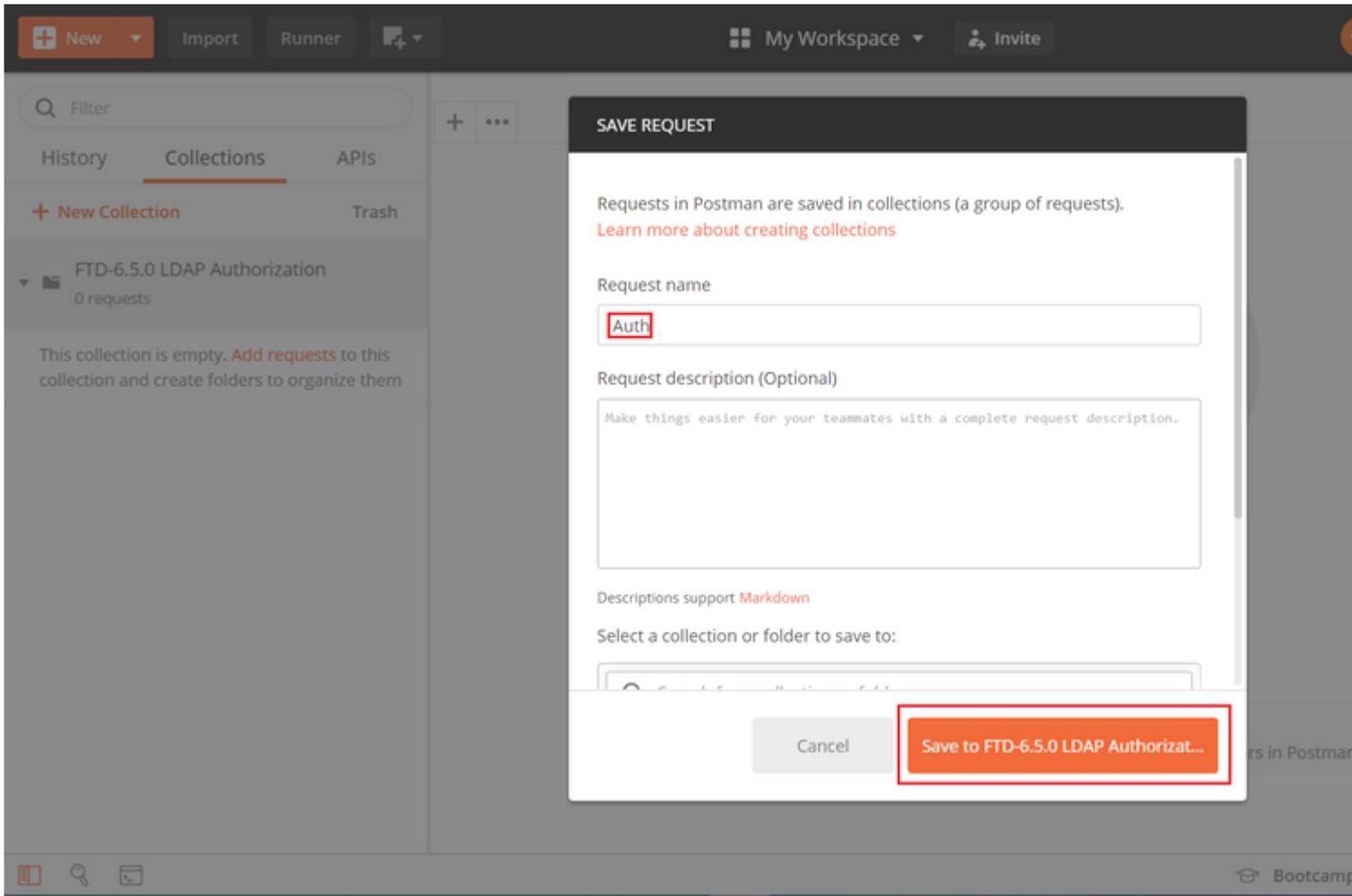
Vous pouvez également ajouter le certificat utilisé par le FTD en tant que certificat CA dans la section Certificate des paramètres.



â€f

**Étape 4.** Ajoutez une nouvelle demande POST **Auth** pour créer une demande POST de connexion au FTD, afin d'obtenir le jeton pour autoriser toute demande POST/GET.





â€f

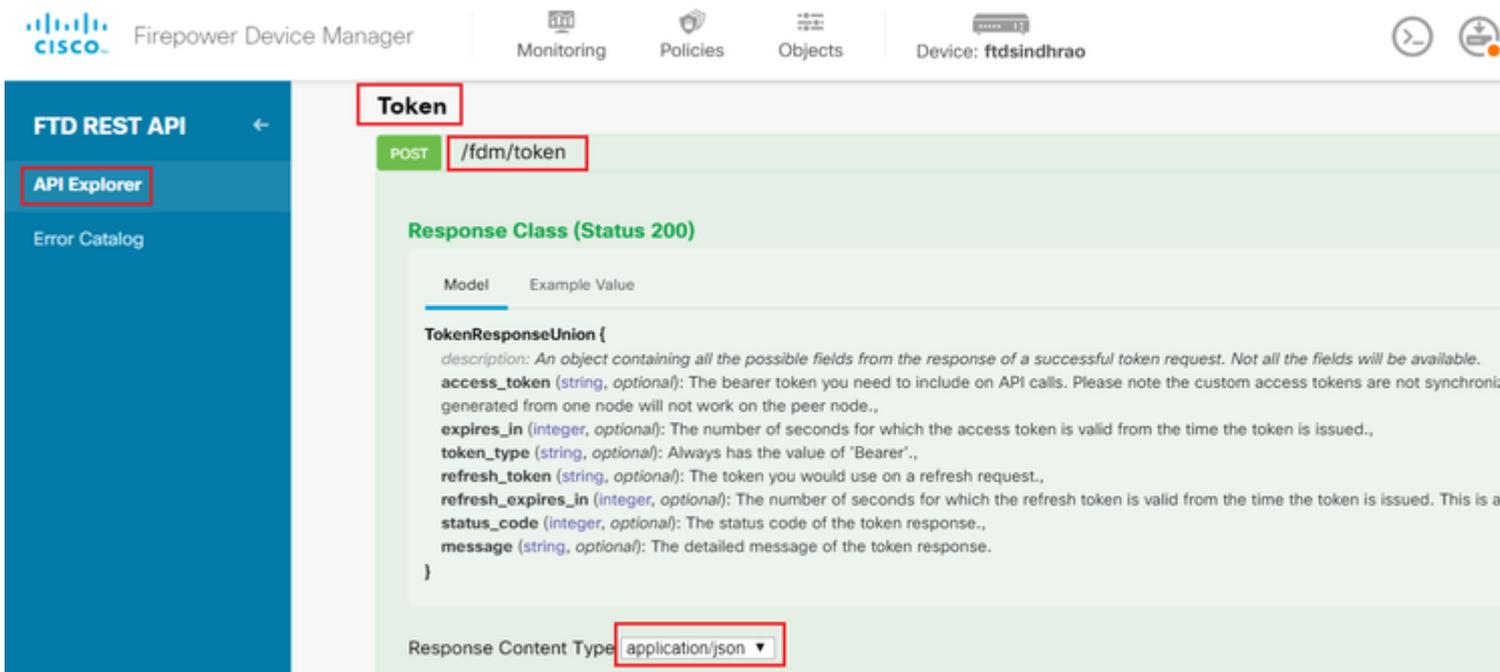
Toutes les requêtes Postman pour cette collection doivent contenir les éléments suivants :

URL de base : <https://<IP de gestion FTD>/api/fdm/last/>

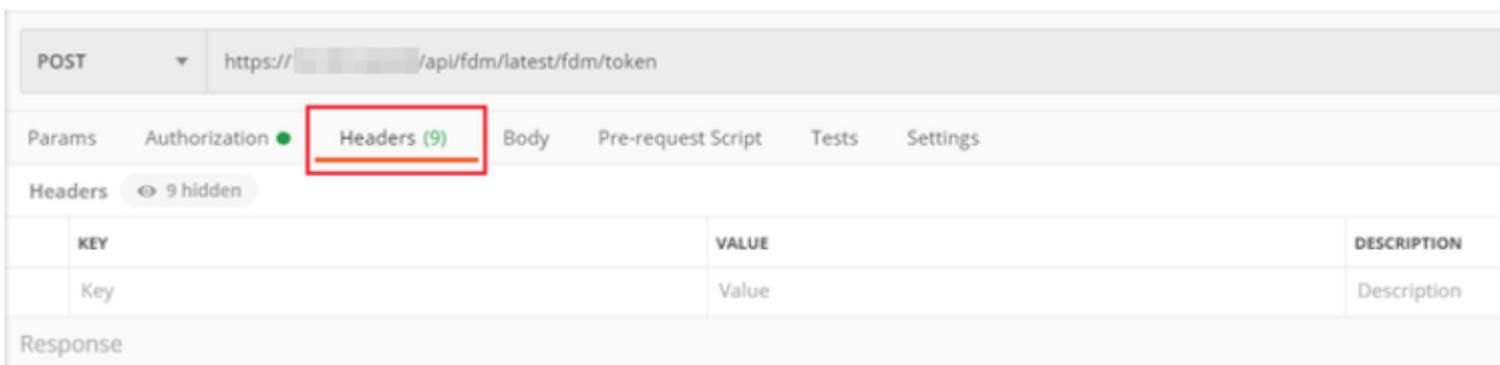
Dans l'URL de requête, ajoutez l'URL de base avec les objets respectifs qui doivent être ajoutés ou modifiés.

â€f

Ici, une demande d'authentification pour un jeton est créée, référencée à partir de <https://<FTD Management IP>/api-explorer>. Vous devez vérifier si d'autres objets sont présents et apporter les modifications nécessaires.



Accédez à **Headers** et cliquez sur **Manage Presets**.



â€f

Créez un nouvel **en-tête** prédéfini-**LDAP** et ajoutez la paire clé-valeur ci-dessous :

Content-Type (Type de contenu)	application/json
Accept (accepter)	application/json

â€f

## MANAGE HEADER PRESETS

### Add Header Preset

Header-LDAP

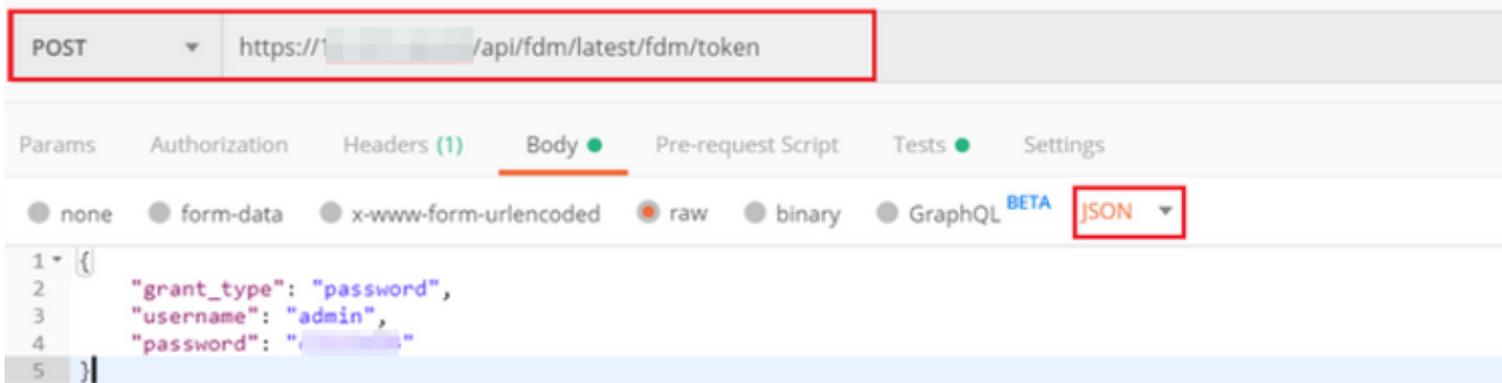
	KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/>	Content-Type	application/json	
<input checked="" type="checkbox"/>	Accept	application/json	
	Key	Value	Description

Pour toutes les autres demandes, accédez aux onglets d'en-tête respectifs et sélectionnez cette valeur d'en-tête prédéfinie : **Header-LDAP** pour les demandes d'API REST à utiliser **json** comme type de données principal.

Le corps de la requête POST pour obtenir le jeton doit contenir les éléments suivants :

Type	brut - JSON (application/json)
grant_type	mot de passe
nom d'utilisateur	Nom d'utilisateur Admin afin de se connecter au FTD
mot de passe	Mot de passe associé au compte utilisateur admin

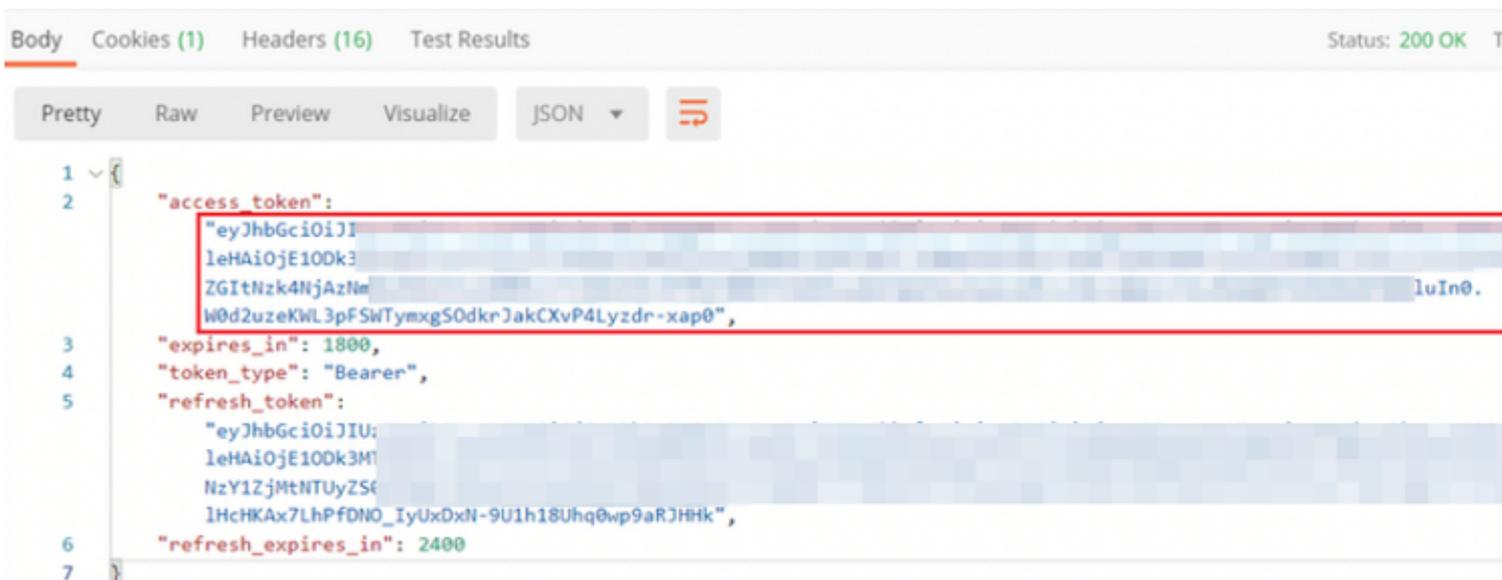
```
{
  "grant_type": "password",
  "username": "admin",
  "password": "<enter the password>"
}
```



â€f

Une fois que vous cliquez sur **send**, le corps de la réponse contient le jeton d'accès qui est utilisé afin d'envoyer toute demande PUT/GET/POST au FTD.

â€f



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

â€f

Ce jeton est ensuite utilisé pour autoriser toutes les requêtes suivantes.

â€f

Accédez à l'onglet **Autorisation** de chaque nouvelle demande et sélectionnez le suivant :



```
+ New Collection  Trash  GET  https://[redacted]/api/fdm/latest/object/ravpngrouppolicies

FTD-6.5.0 LDAP Authorization
2 requests

POST Auth
GET Get Group-Policies

58 {
59   "version": "2nidc13x12yv",
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": "ogalyil3hgigo",
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€¦

**Étape 6.** Ajoutez une nouvelle demande POST **Create LDAP Attribute Map** pour créer la carte d'attributs LDAP. Dans ce document, le modèle **LdapAttributeMapping** est utilisé. D'autres modèles ont également des opérations et des méthodes similaires pour créer une carte d'attribut. Des exemples pour ces modèles sont disponibles dans l'explorateur d'API comme mentionné précédemment dans ce document.

â€f

L'URL pour POST le mappage d'attribut LDAP est : <https://<FTD Management IP>/api/fdm/last/object/ldapattributemaps>

Le corps de la requête POST doit contenir les éléments suivants :

nom	Nom du mappage d'attributs LDAP
type	mappage des attributs ldap
NomLDAP	membrDe
NomCisco	STRATÉGIE_DE_GROUPE
ValeurLDAP	valeur memberOf pour l'utilisateur d'AD
CiscoValue	Nom de stratégie de groupe pour chaque groupe d'utilisateurs dans FDM

â€f

The screenshot shows a REST client interface with a POST request to `https://[redacted]/api/fdm/latest/object/ldapattributemaps`. The request body is a JSON object:

```

1 {
2   "name": "Attribute-Map",
3   "ldapAttributeMaps":
4   [
5     {
6       "ldapName": "memberOf",
7       "ciscoName": "GROUP_POLICY",
8       "valueMappings":
9       [
10      {
11        "ldapValue": "CN=Finance-Group,CN=Users,DC=cisco,DC=com",
12        "ciscoValue": "Finance-Group-Policy",
13        "type": "ldaptociscovaluemapping"
14      },
15      {
16        "ldapValue": "CN=HR-Group,CN=Users,DC=cisco,DC=com",
17        "ciscoValue": "HR-Group-Policy",
18        "type": "ldaptociscovaluemapping"
19      },
20      {
21        "ldapValue": "CN=IT-Group,CN=Users,DC=cisco,DC=com",
22        "ciscoValue": "IT-Group-Policy",
23        "type": "ldaptociscovaluemapping"
24      }
25    ],
26     "type": "ldapattributemapping"
27   }
28 ],
29 "type": "ldapattributemap"
30 }

```

â€f

Le corps de la requête POST contient les informations de mappage d'attribut LDAP qui mappent une stratégie de groupe spécifique à un groupe AD basé sur la valeur **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"
  ]
}

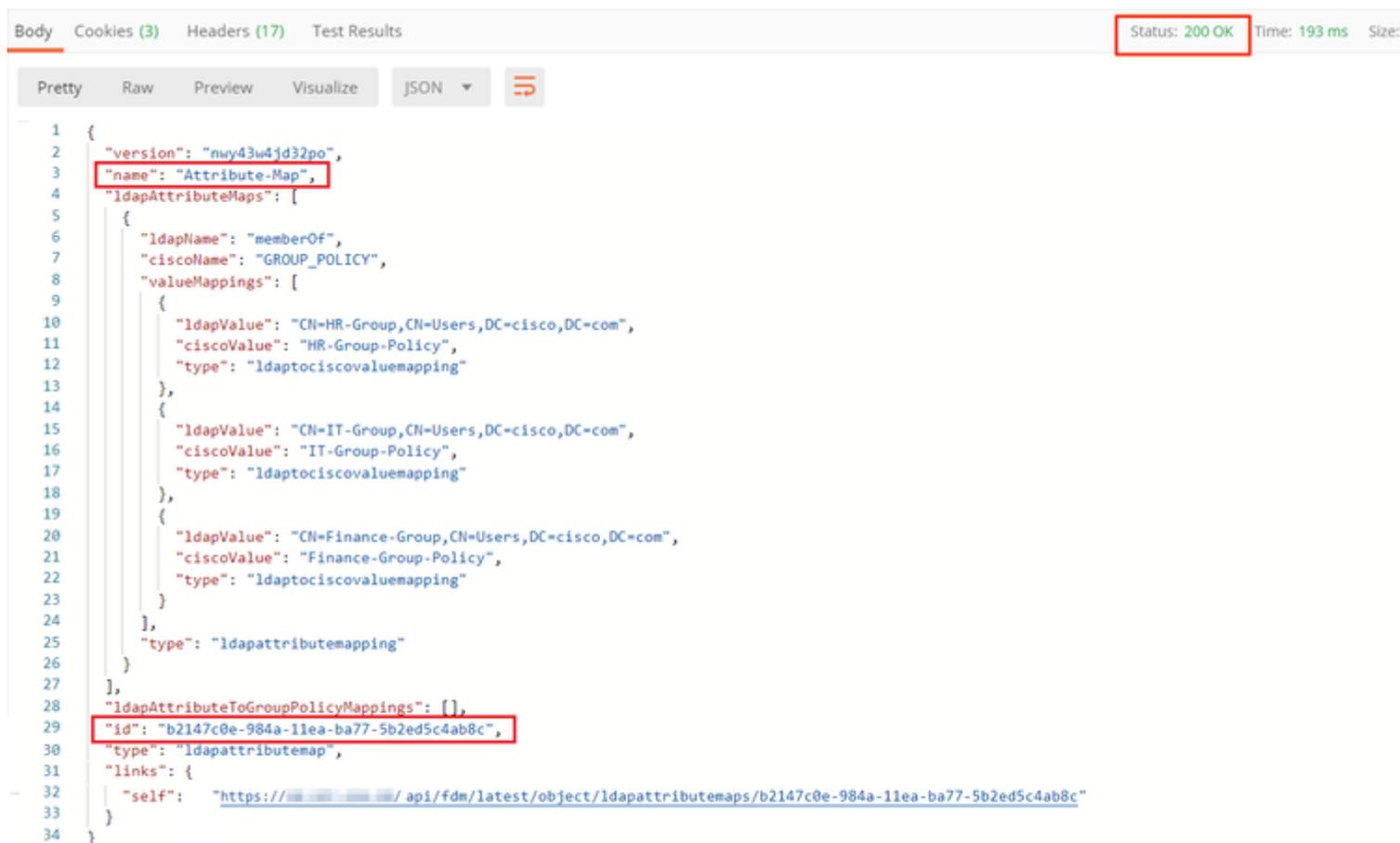
```

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

Remarque : le champ **memberOf** peut être récupéré à partir du serveur AD à l'aide de la commande **dsquery** ou peut être récupéré à partir des débogages LDAP sur le FTD. Dans les journaux de débogage, recherchez le champ **memberOf value**.

â€f

La réponse de cette requête POST ressemble à la sortie suivante :



```
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 }
```

**Étape 7.** Ajoutez une nouvelle requête GET pour obtenir la configuration actuelle du domaine AD sur FDM.

L'URL pour obtenir la configuration actuelle du domaine AD est : <https://<FTD Management IP>/api/fdm/last/object/realm>

â€f

```

1  {
2    "items": [
3      {
4        "version": "ks3pd4he5ixiyy",
5        "name": "LDAP-AD",
6        "directoryConfigurations": [
7          {
8            "hostname": "192.168.1.1",
9            "port": 389,
10           "encryptionProtocol": "NONE",
11           "encryptionCert": null,
12           "type": "directoryconfiguration"
13         }
14       ],
15       "enabled": true,
16       "systemDefined": false,
17       "realmId": 3,
18       "dirUsername": "administrator@192.168.1.1",
19       "dirPassword": "*****",
20       "baseDN": "dc=192.168.1, dc=com",
21       "ldapAttributeMap": null,
22       "adPrimaryDomain": "192.168.1.1",
23       "id": "bf50a8ab-9819-11ea-ba77-d32ecc224295",
24       "type": "activedirectoryrealm",
25       "links": {
26         "self": "https://192.168.1.1/api/fdm/latest/object/realms/bf50a8ab-9819-11ea-ba77-d32ecc224295"
27       }
28     }
29   ],
30   "paging": {
31     "prev": [],
32     "next": [],
33     "limit": 10,
34     "offset": 0,
35     "count": 1,
36     "pages": 0
37   }
38 }

```

â€f

Notez que la valeur de la clé **ldapAttributeMap** est **Null**.

â€f

**Étape 8.** Créez une nouvelle demande **PUT** pour modifier le domaine AD. Copiez la sortie de la réponse **GET** de l'étape précédente et ajoutez-la au corps de cette nouvelle demande **PUT**. Cette étape peut être utilisée pour apporter des modifications à la configuration actuelle du domaine Active Directory, par exemple : changer le mot de passe, l'adresse IP ou ajouter une nouvelle valeur pour une clé comme **ldapAttributeMap** dans ce cas.

---

Remarque : il est important de copier le contenu de la liste d'éléments plutôt que l'ensemble du résultat de la réponse GET. L'URL de requête de la requête PUT doit être ajoutée avec l'ID d'élément de l'objet pour lequel des modifications sont apportées. Dans cet exemple, la valeur est : bf50a8ab-9819-11ea-ba77-d32ecc224295

---

â€f

L'URL pour modifier la configuration actuelle du domaine AD est : <https://<FTD Management IP>/api/fdm/latest/object/realms/<ID du domaine>>

Le corps de la demande PUT doit contenir les éléments suivants :

version	version obtenue à partir de la réponse de la requête GET précédente
---------	---

id	ID obtenu à partir de la réponse de la requête GET précédente.
MappageAttributLDAP	ldap-id de la réponse à la demande <b>Create LDAP Attribute Map</b>

â€f

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

```

{
  "version": "ks3pdhe5ixivv",
  "name": "LDAP-AD",
  "directoryConfigurations": [
    {
      "hostname": "<IP Address>",
      "port": 389,
      "encryptionProtocol": "NONE",
      "encryptionCert": null,
      "type": "directoryconfiguration"
    }
  ],
  "enabled": true,
  "systemDefined": false,
  "realmId": 3,
  "dirUsername": "administrator@[redacted].com",
  "dirPassword": "*****",
  "baseDN": "dc=[redacted], dc=com",
  "ldapAttributeMap": {
    "id": "b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c",
    "type": "ldapattributemap"
  }
}

```

The response body is a JSON object:

```

{
  "adPrimaryDomain": "[redacted].com",
  "id": "bf50a8ab-9819-11ea-ba77-d32ecc224295",
  "type": "activedirectoryrealm",
  "links": {
    "self": "https://[redacted]/api/fdm/latest/object/realms/bf50a8ab-9819-11ea-ba77-d32ecc224295"
  }
}

```

â€f

Le corps de la configuration dans cet exemple est :

<#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"

  }
}
```

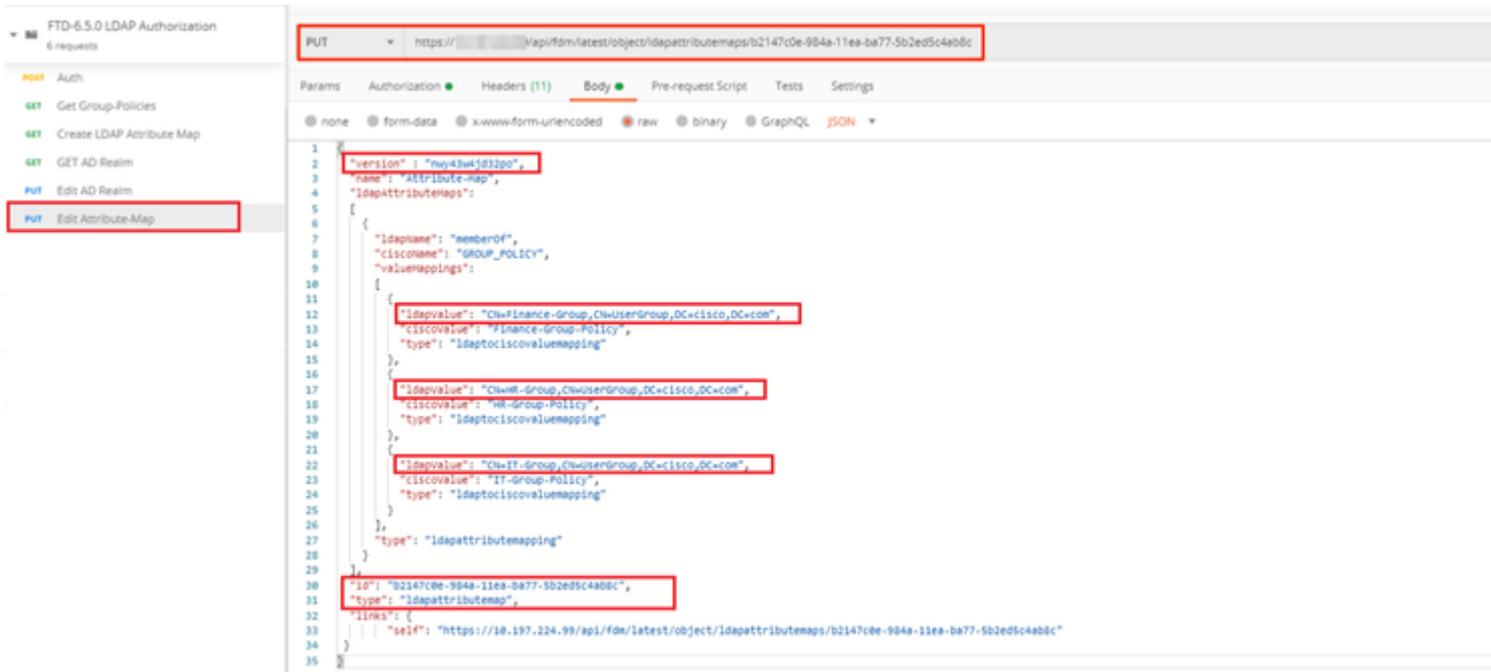
Vérifiez que l'ID **ldapAttributeMap** correspond dans le corps de réponse pour cette demande.

```
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

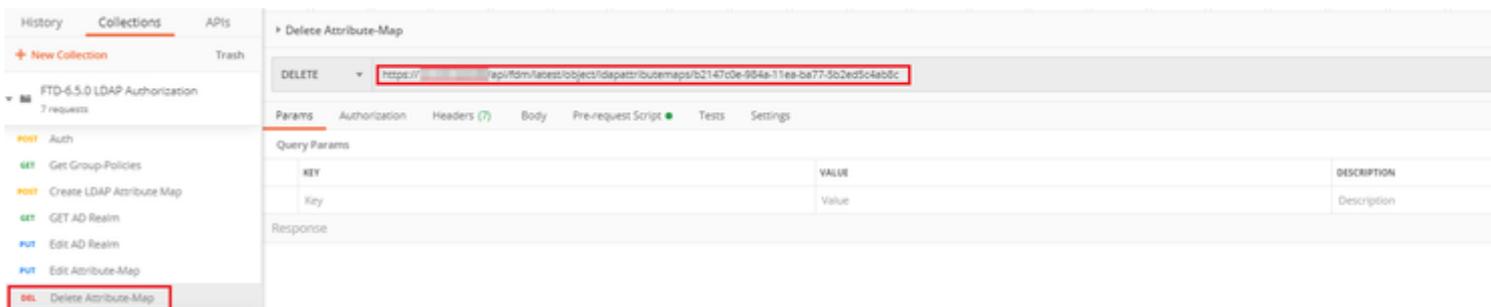
(facultatif). La carte d'attributs LDAP peut être modifiée avec des demandes **PUT**. Créez une nouvelle demande PUT **Edit Attribute-Map** et apportez toutes les modifications comme le nom de la valeur Attribute-Map ou memberOf. T

Dans l'exemple suivant, la valeur de **ldapvalue** a été modifiée de **CN=Users** à **CN=UserGroup** pour les trois groupes.



â€f

**(facultatif).** Pour supprimer un mappage d'attributs LDAP existant, créez un mappage d'attributs DELETE Request **Delete**. Incluez l'**id de mappage** de la réponse HTTP précédente et ajoutez l'URL de base de la demande de suppression.



Remarque : si l'attribut **memberOf** contient des espaces, il doit être codé en URL pour que le serveur Web puisse l'analyser. Sinon, une **réponse HTTP de 400 requêtes incorrectes** est reçue. Pour les chaînes contenant des espaces, "%20" ou "+" peuvent être utilisés pour éviter cette erreur.

â€f

**Étape 9.** Revenez à FDM, sélectionnez l'icône Déploiement et cliquez sur **Déployer maintenant**.

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>	
<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>
<b>✎ Active Directory Realm Edited: <i>LDAP-AD</i></b>	
<pre>ldapAttributeMap : -</pre>	<pre>Attribute-Map</pre>

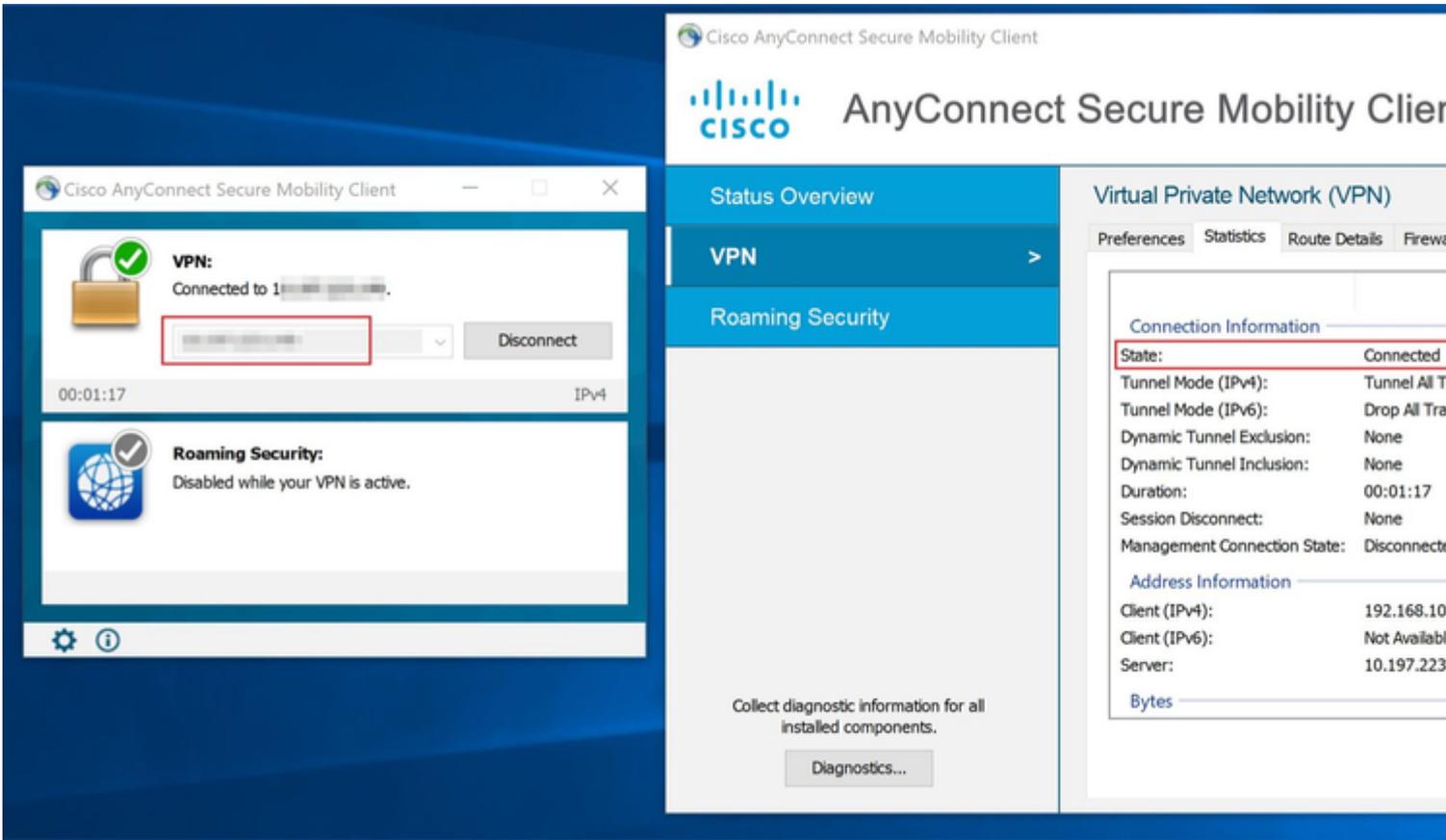
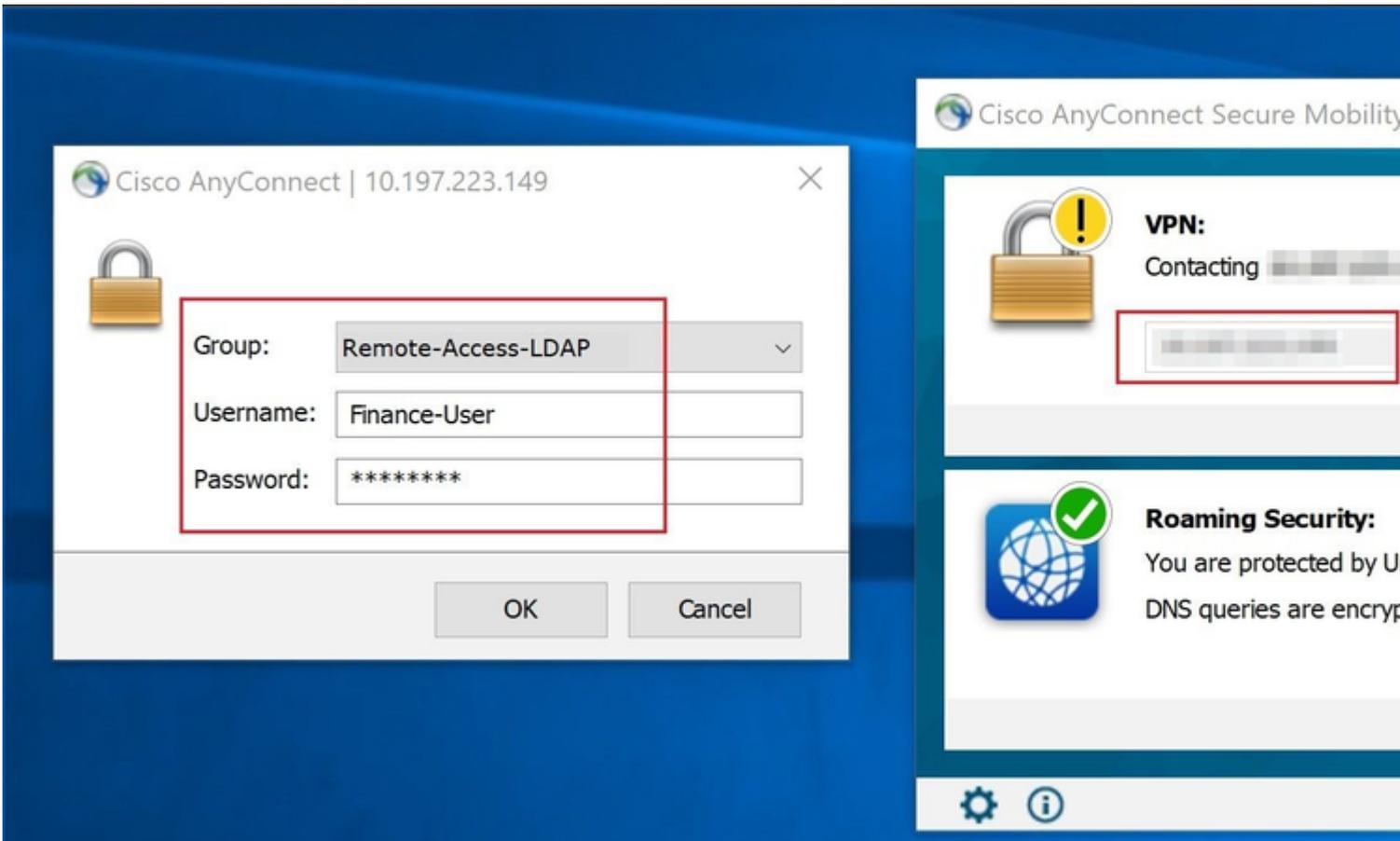
MORE ACTIONS ▾ CANCEL

â€f

## Vérifier

Les modifications de déploiement peuvent être vérifiées dans la section **Historique de déploiement** de FDM.

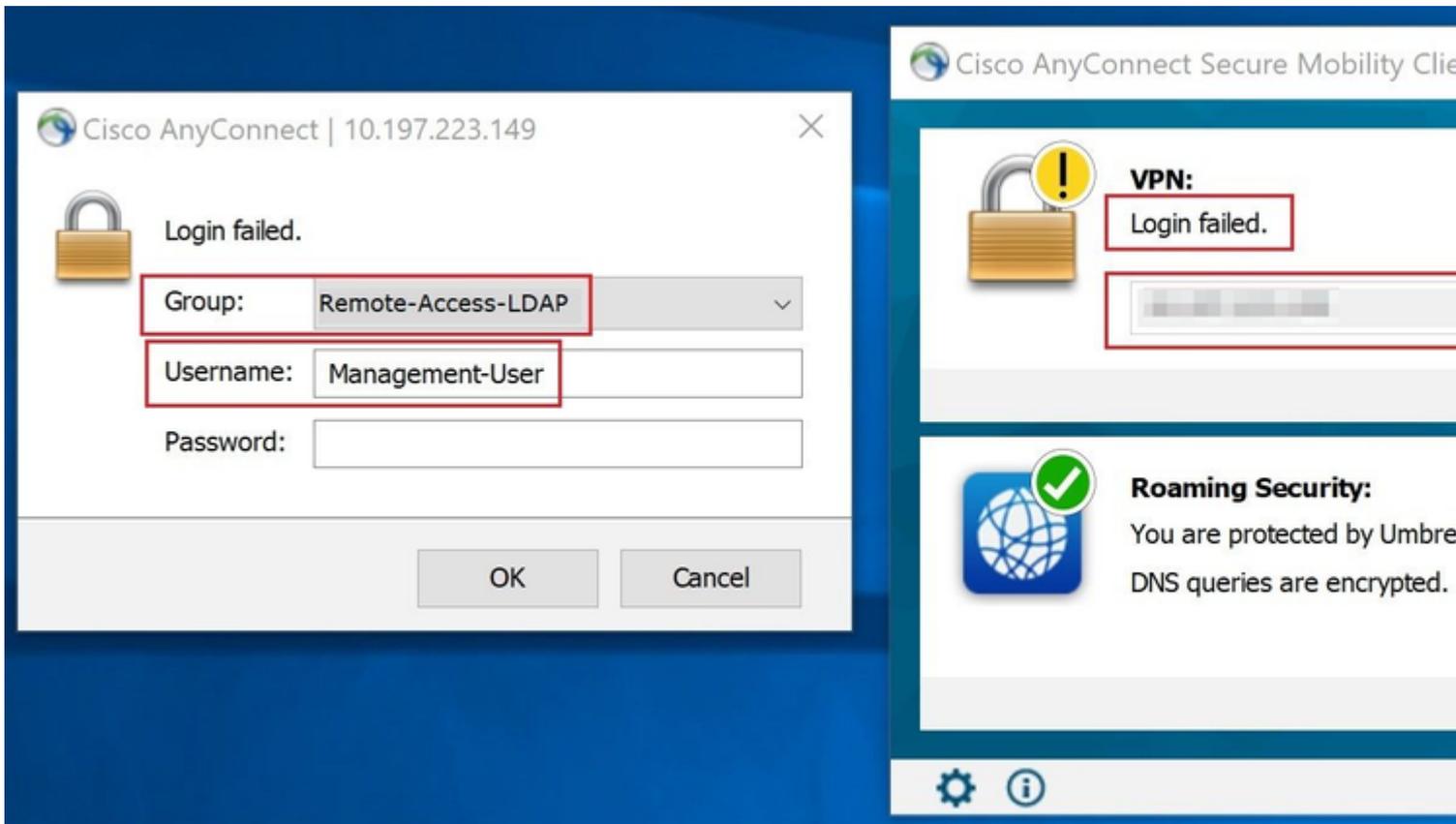




â€f

Lorsqu'un utilisateur qui appartient au **groupe de gestion** dans Active Directory tente de se connecter à

Connection-Profile **Remote-Access-LDAP**, puisqu'aucun mappage d'attribut LDAP n'a renvoyé de correspondance, la stratégie de groupe héritée par cet utilisateur sur le FTD est **NOACCESS**, pour lequel vpn-simultané-logins est défini sur la valeur 0. Par conséquent, la tentative de connexion pour cet utilisateur échoue.



â€f

La configuration peut être vérifiée à l'aide des commandes show suivantes de l'interface de ligne de commande 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
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
```

## Dépannage

L'un des problèmes les plus courants lors de la configuration de l'API REST est le renouvellement périodique du jeton support. Le délai d'expiration du jeton est indiqué dans la réponse à la demande d'authentification. Si ce délai expire, un jeton d'actualisation supplémentaire peut être utilisé pendant une période plus longue. Une fois que le jeton d'actualisation a également expiré, une nouvelle demande d'authentification doit être envoyée pour recevoir un nouveau jeton d'accès.

---

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de débogage.

---

Vous pouvez définir différents niveaux de débogage. Par défaut, le niveau 1 est utilisé. Si vous modifiez le niveau de débogage, le niveau de détail des débogages peut augmenter. Faites-le avec

---

---

prudence, en particulier dans les environnements de production.

---

Les débogages suivants sur l'interface de ligne de commande de FTD seraient utiles pour résoudre les problèmes liés à la carte d'attributs LDAP

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

Dans cet exemple, les débogages suivants ont été collectés pour démontrer les informations reçues du serveur AD lorsque les utilisateurs de test mentionnés précédemment se sont connectés.

Débogages LDAP pour **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

## Débugages LDAP pour **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

## Informations connexes

Pour obtenir de l'aide supplémentaire, contactez le centre d'assistance technique de Cisco. Un contrat d'assistance valide est requis : [Coordonnées du service d'assistance Cisco à l'échelle mondiale](#).

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.