

Configureer LDAP Attribute Map voor RAVPN op FTD beheerd door FDM

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Verificatiestroom](#)

[LDAP Attribute Map Flow toegelicht](#)

[Configureren](#)

[Configuratiestappen op FDM](#)

[Configuratiestappen voor LDAP-kenmerkaart](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de procedure voor het gebruik van een Lichtgewicht Directory Access Protocol (LDAP) server voor het verifiëren en autoriseren van gebruikers van Remote Access VPN (RA VPN) en het verlenen van verschillende netwerktoegang op basis van hun groepslidmaatschap op de LDAP-server.

Voorwaarden

Vereisten

- Basiskennis van RA VPN-configuratie op Firewall Device Manager (FDM)
- Basiskennis van LDAP-serverconfiguratie op FDM
- Basiskennis van REpresentational State Transfer (REST) Application Program Interface (API) en FDM Rest API Explorer
- Cisco FTD versie 6.5.0 of nieuwer beheerd door FDM

Gebruikte componenten

De volgende hardware- en softwareversies van toepassingen/apparaten werden gebruikt:

- Cisco FTD versie 6.5.0, build 115
- Cisco AnyConnect versie 4.10
- Microsoft Active Directory (AD)-server
- Postman of een andere API-ontwikkeltool

Opmerking: Cisco biedt geen ondersteuning voor configuratie van de Microsoft AD Server- en Postmal-tool.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als

uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Verificatiestroom



LDAP Attribute Map Flow toegelicht

1. De gebruiker initieert een externe VPN-verbinding met de FTD en geeft een gebruikersnaam en wachtwoord voor hun Active Directory (AD)-account.
2. De FTD stuurt een LDAP-verzoek naar de AD-server via poort 389 of 636 (LDAP over SSL)
3. De AD reageert terug op de FTD met alle attributen die aan de gebruiker zijn gekoppeld.
4. De FTD past de ontvangen attribuutwaarden aan met de LDAP Attribute Map die op de FTD is gemaakt. Dit is het autorisatieproces.
5. De gebruiker verbindt en erft vervolgens instellingen van de groep-beleid die worden afgestemd met de **memberOf** attributen in de LDAP Attribute Map.

Voor de toepassing van dit document wordt de autorisatie van AnyConnect-gebruikers uitgevoerd met behulp van het kenmerk **memberOf** LDAP.

- Het **memberOf** attribuut van de LDAP Server voor elke gebruiker wordt in kaart gebracht aan een **ldapValue**-entiteit op de FTD. Als de gebruiker tot de overeenkomende AD-groep behoort, wordt het Groepsbeleid dat aan die ldapValue is gekoppeld, geërfd door de gebruiker.
- Als de attribuutwaarde **memberOf** voor een gebruiker niet overeenkomt met een van de **ldapValue**-entiteiten op de FTD, wordt het standaardgroepsbeleid voor het geselecteerde verbindingsprofiel geërfd. In dit voorbeeld is **NOACCESS** Group-Policy geërfd naar .

Configureren

LDAP Attribute Map voor FTD beheerd door FDM wordt geconfigureerd met REST API.

Configuratiestappen op FDM

Stap 1. Controleer of apparaat is geregistreerd voor **slimme licenties**.



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

â€f

Stap 2. Controleer of **AnyConnect-licenties** zijn ingeschakeld op de 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
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
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
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
 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

Stap 3. Controleer of **door export gecontroleerde functies** in het token zijn **ingeschakeld**.



Device Summary
Smart License



CONNECTED
SUFFICIENT LICENSE

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

Assigned V
Export-cont
Go to Cisco

SUBSCRIPTION LICENSES INCLUDED

Threat

✓ Enabled

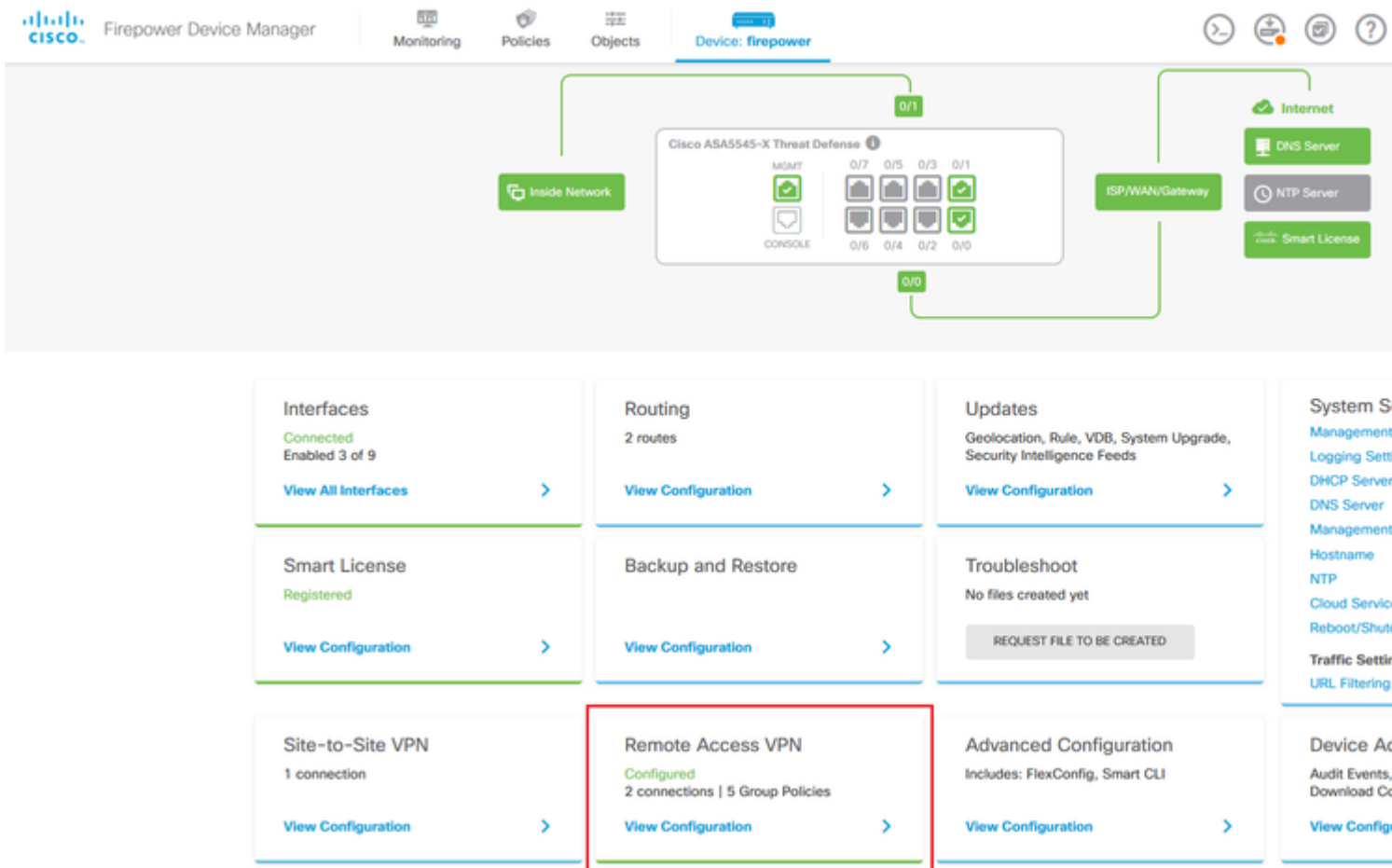
This License allows you to perform intrusion detection and prevention. You must have this license to apply intrusion policies in access rules. You also need this license to apply file policies that control files based on file type.

Includes: Intrusion Policy

Opmerking: in dit document wordt ervan uitgegaan dat RA VPN al is geconfigureerd. Raadpleeg het volgende document voor meer informatie over [hoe u RAVPN kunt configureren op FTD die wordt beheerd door FDM](#).

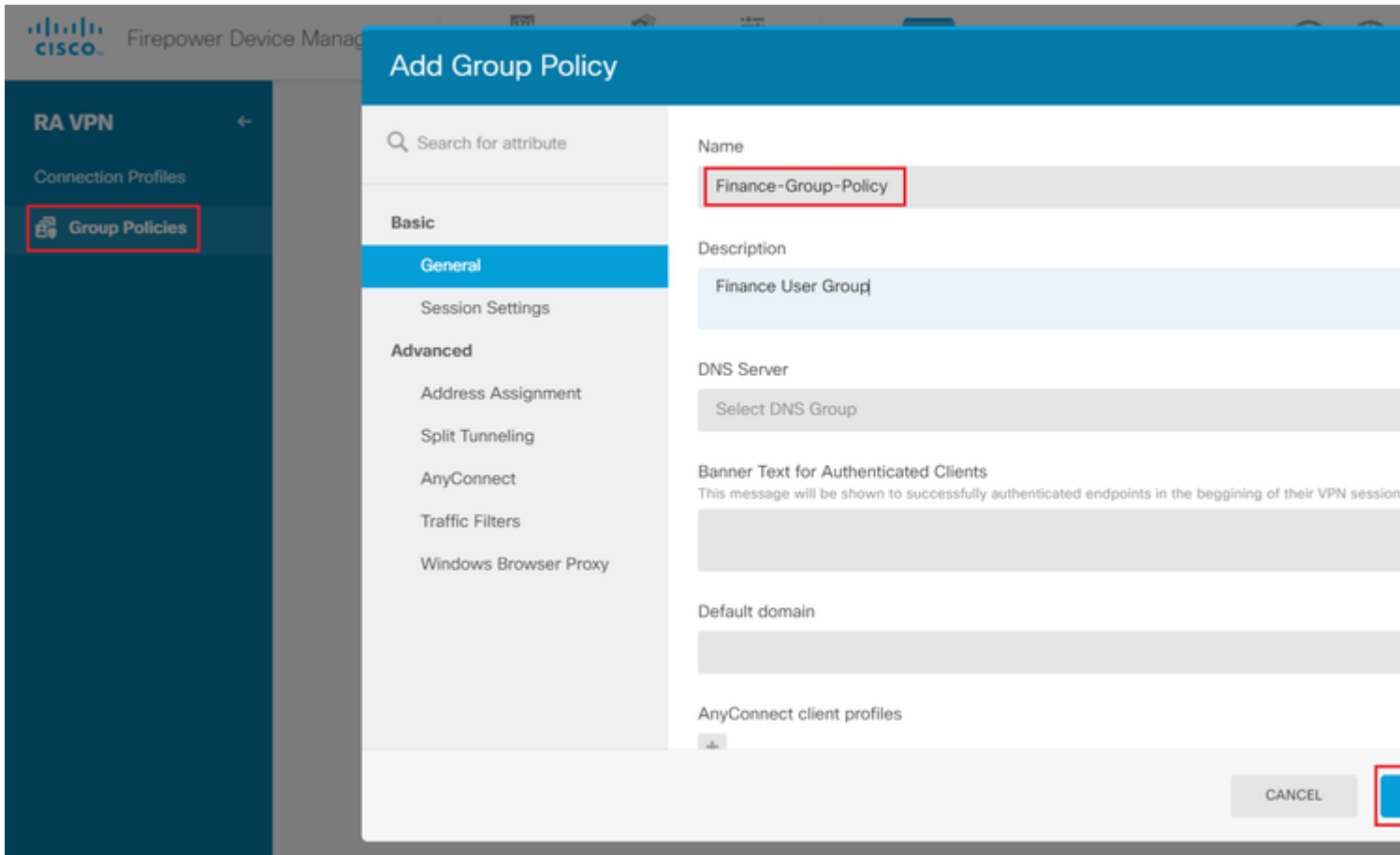
â€f

Stap 4. Navigeer naar **beleid voor externe toegang > VPN-groep**.



â€f

Stap 5. Ga naar **Groepsbeleid**. Klik op '+' om de verschillende Groepsbeleid voor elke AD-groep te configureren. In dit voorbeeld zijn de **financiën-groep-beleid**, **HR-groep-beleid** en **IT-groep-beleid** geconfigureerd om toegang te hebben tot verschillende subnetten.



â€f

Het **Finance-Group-Policy** heeft de volgende instellingen:

<#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

Op dezelfde manier heeft **HR-Group-Policy** onderstaande instellingen:

```
<#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

Tenslotte heeft **IT-Group-Policy** de volgende instellingen:

```
<#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

Stap 6. Maak een Group-Policy **NOACCESS** en navigeer naar **Session-instellingen** en deselecteer de optie **Gelijktijdige aanmelding per gebruiker**. Hiermee wordt de waarde van de **VPN-simultaan-logins** op 0 ingesteld.

De waarde voor **VPN-simultane aanmeldingen** in het groepsbeleid wanneer deze op 0 is ingesteld, beëindigt de VPN-verbinding van de gebruiker onmiddellijk. Dit mechanisme wordt gebruikt om te voorkomen dat gebruikers die tot een andere AD-gebruikersgroep behoren dan de geconfigureerde gebruikers (in dit voorbeeld Finance, HR of IT) succesvolle verbindingen met het FTD tot stand brengen en toegang krijgen tot beveiligde bronnen die alleen beschikbaar zijn voor de toegestane gebruikersgroeprekeningen.

Gebruikers die behoren tot de juiste AD-gebruikersgroepen passen de LDAP-kenmerkaart op de FTD aan en erven het in kaart gebrachte groepsbeleid, terwijl gebruikers die niet tot een van de toegestane groepen behoren, het standaard groepsbeleid van het verbindingsprofiel erven, dat in dit geval **NOACCESS** is.

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

Het **NOACCESS** Group-Policy heeft de volgende instellingen:

```
<#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
```

Stap 7. Navigeer naar **verbindingprofielen** en maak een verbindingprofiel aan. In dit voorbeeld is de profielnaam **Remote-Access-LDAP**. Kies **alleen** primaire identiteitsbron **AAA** en maak een nieuw verificatieservertype **AD**.

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

Voer de gegevens van de AD-server in:

- Gebruikersnaam map

- Directory-wachtwoord
- Basis-DN
- AD Primair domein
- Hostnaam/IP-adres
- Port
- Type encryptie

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

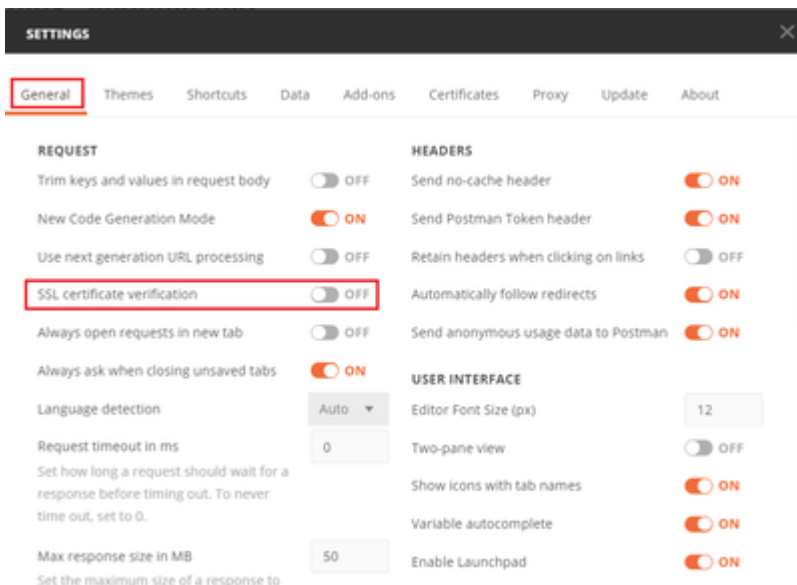
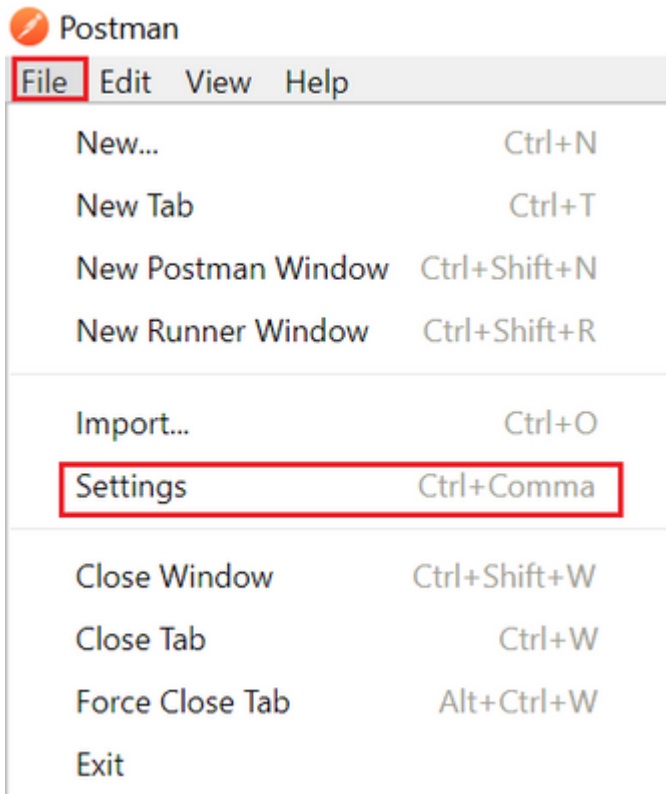
Please select a certificate

TEST

[Add another configuration](#)

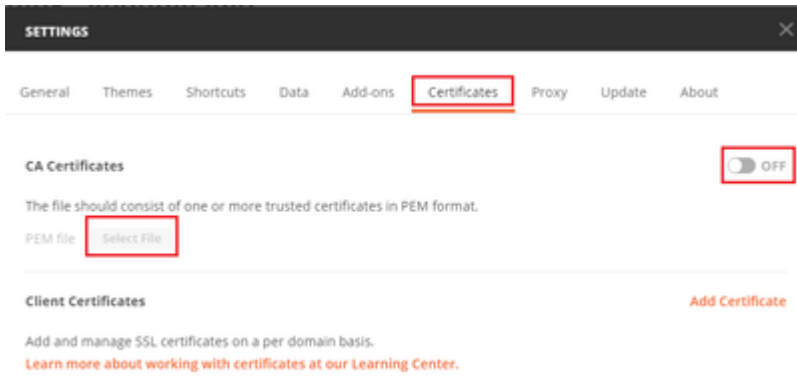
CANCEL

, schakel de SSL-certificaatverificatie uit om te voorkomen dat er een SSL-handdruk fout optreedt bij het verzenden van API-aanvragen naar de FTD. Dit gebeurt als het FTD een zelfondertekend certificaat gebruikt.



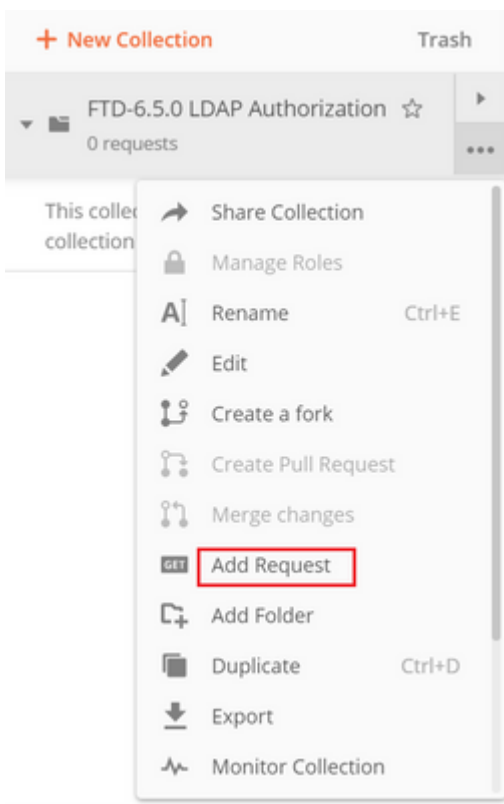
â€f

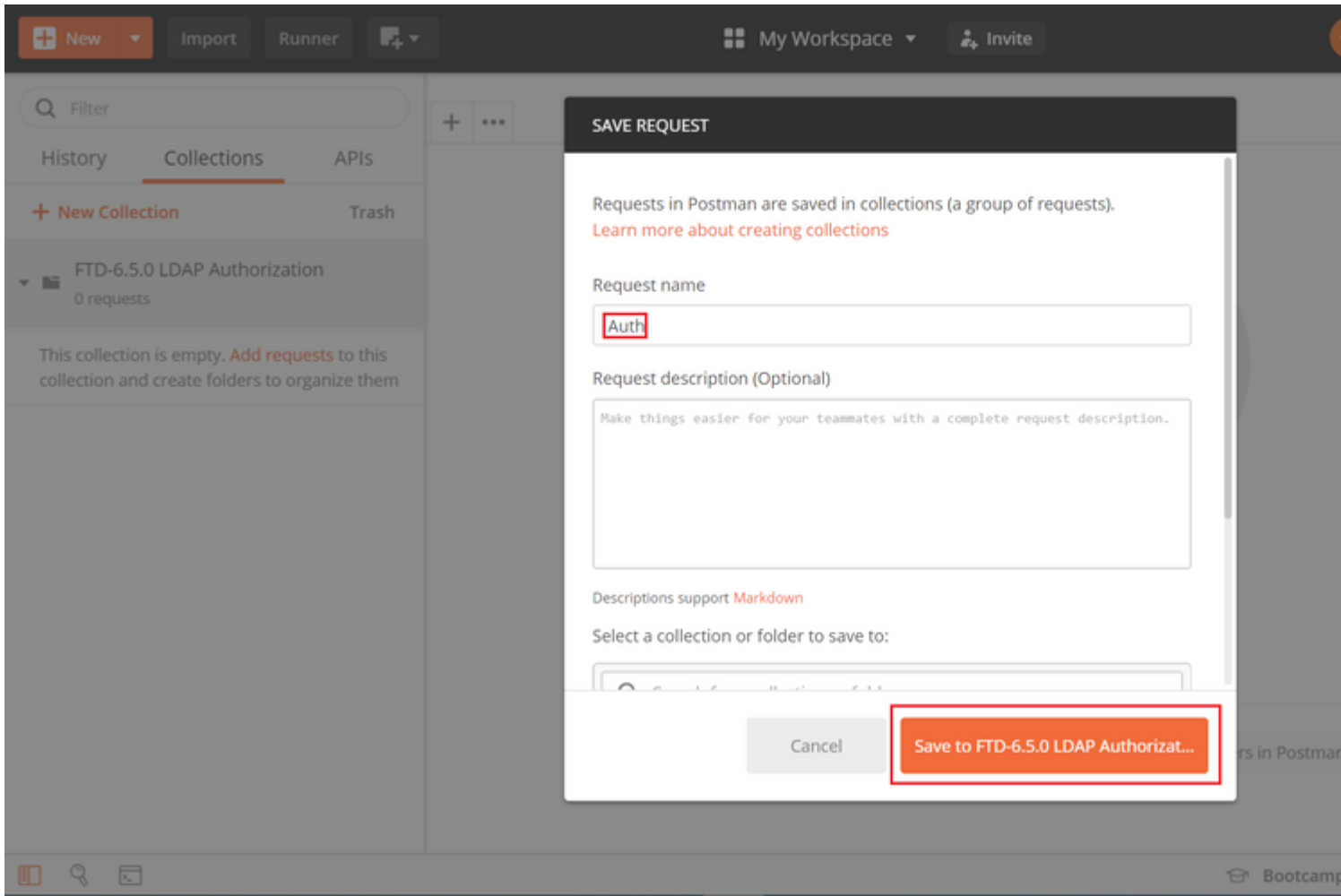
Het door de FTD gebruikte certificaat kan ook worden toegevoegd als CA-certificaat in het vak Certificaat van de instellingen.



â€f

Stap 4. Voeg een nieuwe POST aanvraag **Auth** toe om een login POST aanvraag te creëren aan de FTD, om het token te krijgen om eventuele POST/GET verzoeken te autoriseren.





â€f

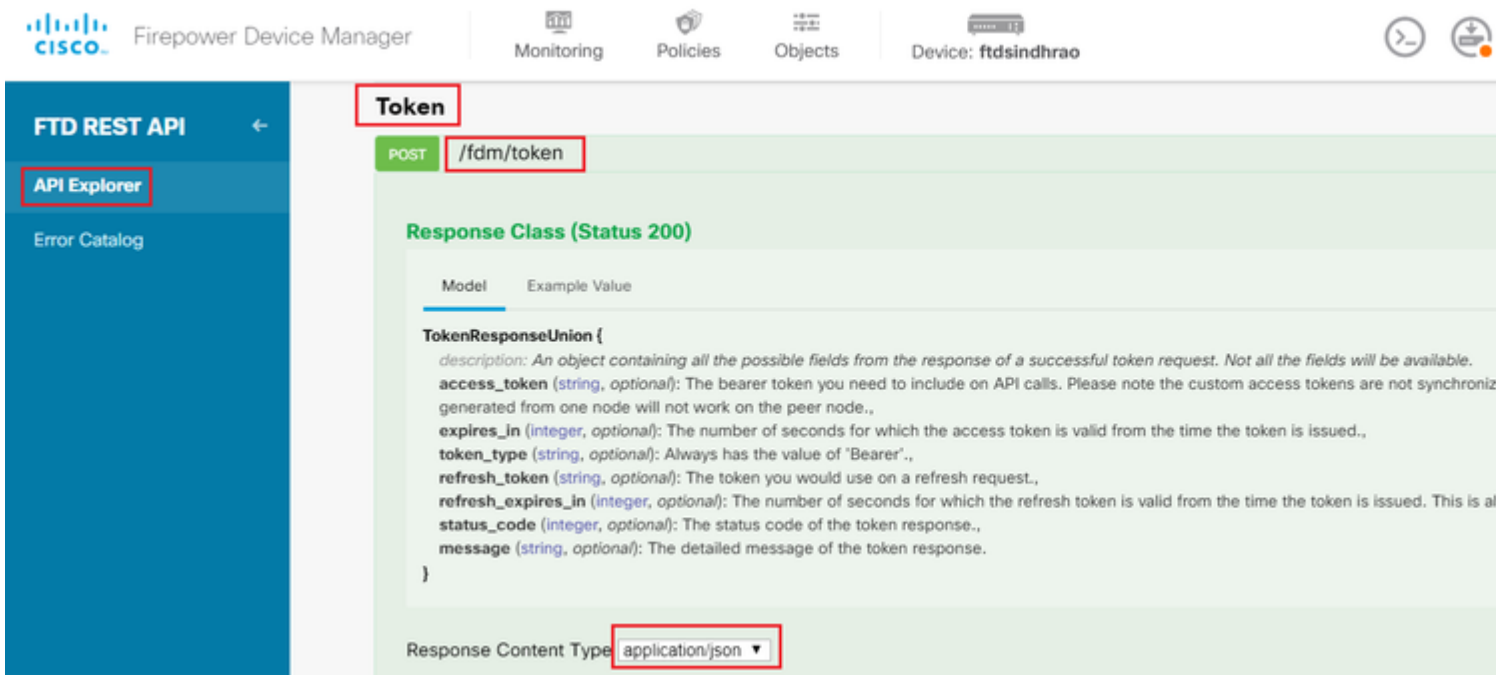
Alle Postman verzoeken voor deze collectie moeten het volgende bevatten:

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

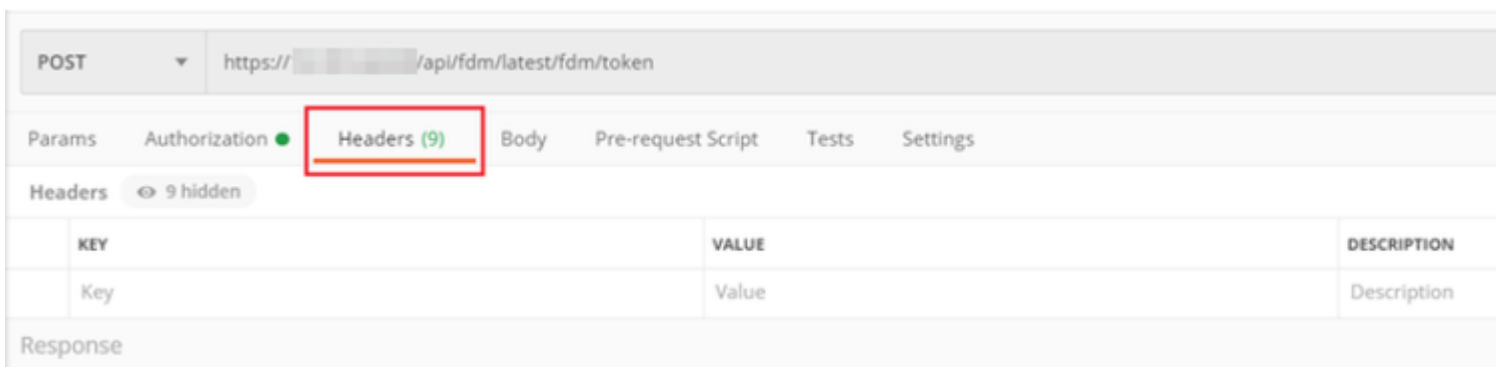
In de aanvraag URL, voeg de basis URL toe met de respectievelijke objecten die moeten worden toegevoegd of aangepast.

â€f

Hier wordt een verificatieaanvraag voor een token gemaakt, via <https://<FTD Management IP>/API-Explorer>. Dit moet worden gecontroleerd op andere objecten en daarvoor moeten de nodige wijzigingen worden aangebracht.



Navigeer naar **koppen** en klik op **Voorinstellingen beheren**.



â€f

Maak een nieuwe voorgeprogrammeerde **Kop-LDAP** en voeg het onderstaande Key-Value-paar toe:

Content-Type	application/json
accepteren	application/json

â€f

MANAGE HEADER PRESETS

Add Header Preset

Header-LDAP

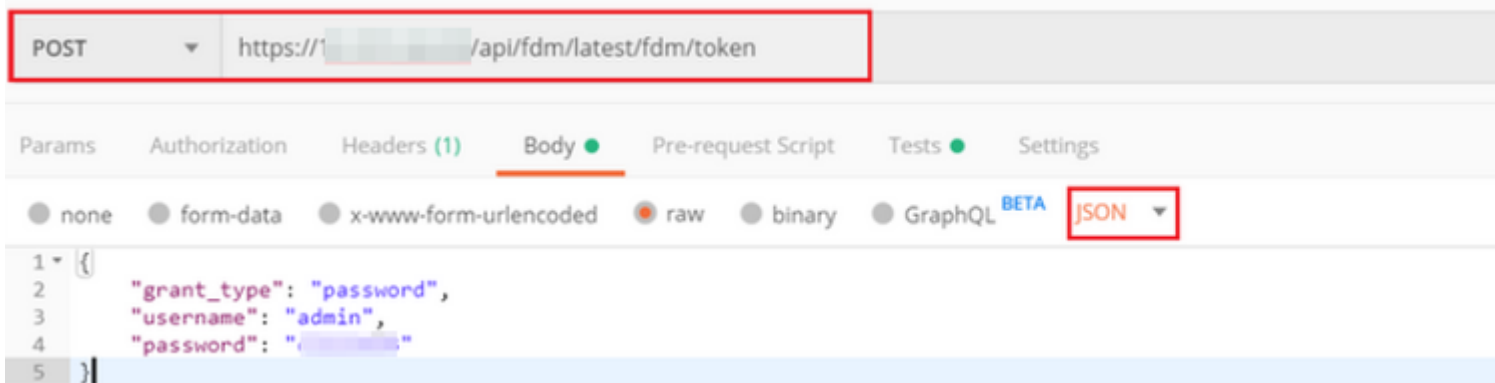
	KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/>	Content-Type	application/json	
<input checked="" type="checkbox"/>	Accept	application/json	
	Key	Value	Description

Voor alle andere aanvragen, navigeer naar de respectievelijke Kop tabbladen en selecteer deze Vooraf ingestelde Kop waarde: **Kop-LDAP** voor de REST API verzoeken om **json** als het primaire gegevenstype te gebruiken.

De Body of the POST Verzoek om het token te krijgen moet het volgende bevatten:

Type	Raw - JSON (application/json)
subsidie_type	wachtwoord
username	Gebruikersnaam Admin om in te loggen op het FTD
wachtwoord	Wachtwoord geassocieerd met de admin-gebruikersaccount

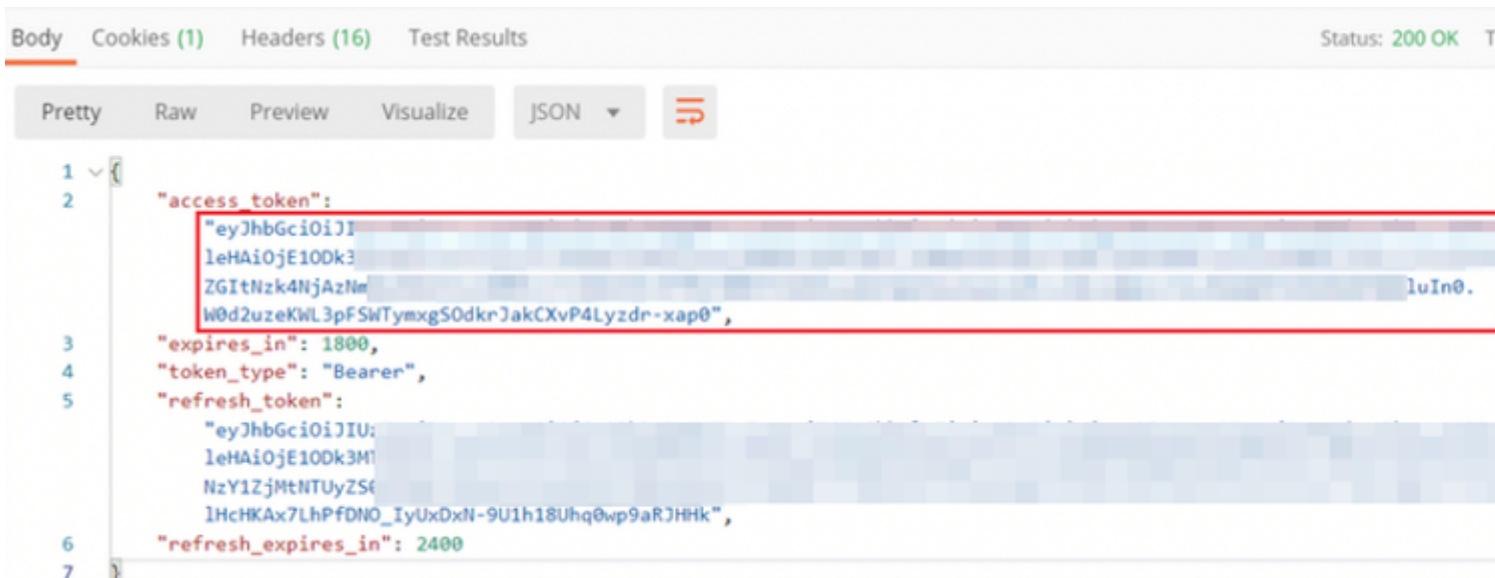
```
{
  "grant_type": "password",
  "username": "admin",
  "password": "<enter the password>"
}
```



â€f

Zodra u op **verzenden** klikt, bevat de inhoud van het antwoord het toegangsteken dat wordt gebruikt om PUT/GET/POST-verzoeken naar het FTD te verzenden.

â€f



```
{
  "access_token": "eyJhbGciOiJIUzI1NiIsInR5cGU6IjY9bnVudC54aW50IiwiaWF0IjoiYXNjaW50Lm9uIn0.",
  "expires_in": 1800,
  "token_type": "Bearer",
  "refresh_token": "eyJhbGciOiJIUzI1NiIsInR5cGU6IjY9bnVudC54aW50IiwiaWF0IjoiYXNjaW50Lm9uIn0.",
  "refresh_expires_in": 2400
}
```

â€f

Deze token worden vervolgens gebruikt voor de autorisatie van alle volgende aanvragen.

â€f

Navigeer naar het tabblad **Autorisatie** van elk nieuw verzoek en selecteer het volgende:

â€f

Type	OAuth 2.0
Token	Het toegangsteken dat is ontvangen door de aanvraag voor aanmelding na aanmelding uit te voeren

Params **Authorization** Headers (13) Body Pre-request Script Tests Settings

TYPE
OAuth 2.0

The authorization data will be automatically generated when you send the request. [Learn more about authorization](#)

Add authorization data to
Request Headers

Heads up! These parameters hold sensitive data. To keep this data secure while working in a c... variables. [Learn more about variables](#)

Access Token

```
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOiE1ODk3MDg0MTwianRpljoiNjgwM2EyNzMtOTgyMi0xMwVhLWJhbnMxliwibmJmljoxNTg5NzA4NDYyLCJleHAiOiE1ODhUb2t1bkV4cGlyZXNBdCI6MTU4OTcxMDgxMjk2NiIsIldlUX0FjY2VzcyIsInVzZXJvdWlkijoiZWNIzY1ZjMwZGltNzk4NjAzNmMyZmUwliwidXNlcljvbiUOIjS2Z2luIjoicGFzc3dvcmQILCJ1c2VybmFtZSI6ImFkbWFSWWTymxgSOdkrjakCXvP4Lyzdr-xap0
```

Body Cookies (3) Headers (17) Test Results **Status: 200 OK**

â€f

Stap 5. Voeg een nieuw GET aanvraag **Get Group-Policies** om de Group-Policy status en instellingen te krijgen. Verzamel de naam en **id** voor elk geconfigureerd Group-Policy (in dit voorbeeld: **Finance-Group-Policy**, **HR-Group-Policy** en **IT-Group-Policy**) om in de volgende stap te gebruiken.

â€f

De URL voor het geconfigureerd groepsbeleid is: <https://<FTD Management IP>/api/fdm/last/object/ravpngrouppolicies>

â€f

In het volgende voorbeeld wordt Group-Policy **Finance-Group-Policy** gemarkeerd.

â€f

```
+ 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": "2nid13x12vu",
60   "name": "Finance-Group-Policy",
61   "banner": null,
62   "dnsServerGroup": null,
63   "defaultDomainName": null,
64   "simultaneousLoginPerUser": 3,
65   "maxConnectionTimeout": null,
66   "maxConnectionTimeAlertInterval": 1,
67   "vpnIdleTimeout": 30,
68   "vpnIdleTimeoutAlertInterval": 1,
69   "ipv4LocalAddressPool": [],
70   "ipv6LocalAddressPool": [],
71   "dhcpScope": null,
72   "ipv4SplitTunnelSetting": "TUNNEL_SPECIFIED",
73   "ipv6SplitTunnelSetting": "TUNNEL_ALL",
74   "ipv4SplitTunnelNetworks": [
75     {
76       "version": "ogaly1l3hgigo",
77       "name": "acl1",
78       "id": "9ec77902-9836-11ea-ba77-37fd67647b3e",
79       "type": "networkobject"
80     }
81   ],
82   "ipv6SplitTunnelNetworks": [],
83   "splitDNSRequestPolicy": "USE_SPLIT_TUNNEL_SETTING",
84   "splitDNSDomainList": "",
85   "scepForwardingUrl": null,
86   "periodicClientCertAuthenticationInterval": 1,
87   "enableDTLS": false,
88   "enableDTLSCompression": false,
89   "sslCompression": "DISABLED",
90   "enableSSLrekey": false,
91   "rekeyMethod": "NEW_TUNNEL",
92   "rekeyInterval": 4,
93   "ignoreDFBit": false,
94   "bypassUnsupportedProtocol": false,
95   "mtuSize": 1406,
96   "useAlwaysOnVPNSettingInProfile": true,
97   "enableKeepAliveMessages": false,
98   "keepAliveMessageInterval": 20,
99   "enableGatewayDPD": false,
100  "gatewayDPDInterval": 30,
101  "enableClientDPD": false,
102  "clientDPDInterval": 30,
103  "clientProfiles": [],
104  "keepInstallerOnClient": false,
105  "vpnTrafficFilterACL": null,
106  "enableRestrictVPNTOVLAN": false,
107  "restrictVPNTOVLANId": null,
108  "clientFirewallPrivateNetworkRules": null,
109  "clientFirewallPublicNetworkRules": null,
110  "browserProxyType": "NO_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

Stap 6. Voeg een nieuwe POST aanvraag **Maak LDAP Attribute Map** om de LDAP Attribute Map te maken. In dit document wordt het model **LdapAttributeMapping** gebruikt. Andere modellen hebben ook vergelijkbare bewerkingen en methoden om Attribute map te maken. Voorbeelden voor deze modellen zijn beschikbaar in de api-explorer zoals eerder vermeld in dit document.

LdapAttributeMap

GET /object/ldapattributemaps

POST /object/ldapattributemaps

Implementation Notes
This API call is not allowed on the standby unit in an HA pair.

Response Class (Status 200)

Model Example Value

LdapAttributeMapping
description: Nested Entity which includes common objects for LdapAttributeMapping (Note: The field level constraints listed here might not cover all the constraints on the field. Additional constraints might exist.)
ldapName (string): The customer-specific LDAP attribute name that is being mapped.
 Field level constraints: cannot be null, must match pattern `^(?!:).*`. (Note: Additional constraints might exist),
ciscoName (string): An enum value that is the Cisco attribute name that maps to the customer-specific attribute name.
 Field level constraints: cannot be null. (Note: Additional constraints might exist)
 = ['ACCESS_HOURS', 'ALLOW_NETWORK_EXTENSION_MODE', 'AUTH_SERVICE_TYPE', 'AUTHENTICATED_USER_IDLE_TIMEOUT', 'BANNER1', 'BANNER2', 'CISCO_AV_PAIR', 'CISCO_IP_PHONE_BYPASS', 'CISCO_LEAP_BYPASS', 'CLIENT_BYPASS_PROTOCOL', 'CLIENT_TYPE_VERSION_LIMITING', 'CONFIDENCE_INTERVAL', 'DHCP_NETWORK_SCOPE', 'DN_FIELD', 'DISABLE_ALWAYS_ON_VPN_GATEWAY_FQDN', 'GROUP_POLICY', 'IE_PROXY_BYPASS_LOCAL', 'IE_PROXY_EXCEPTION_LIST', 'IE_PROXY_METHOD', 'IE_PROXY_PREF', 'IETF_RADIUS_FILTER_ID', 'IETF_RADIUS_FRAMED_IP_ADDRESS', 'IETF_RADIUS_FRAMED_IP_NETMASK', 'IETF_RADIUS_IPV6_PREF', 'IETF_RADIUS_INTERFACE_ID', 'IETF_RADIUS_SERVICE_TYPE', 'IETF_RADIUS_SESSION_TIMEOUT', 'IKE DPD_Retry_Interval', 'IKE_PEER_AUTH_ON_REKEY', 'IPSEC_AUTHENTICATION', 'IPSEC_BACKUP_SERVER_LIST', 'IPSEC_BACKUP_SERVERS', 'IPSEC_CLIENT_FIREWALL_FILTER_OPTIONAL', 'IPSEC_CLIENT_FIREWALL_FILTER_OPTIONAL', 'IPSEC_DEFAULT_DOMAIN', 'IPSEC_EXTENDED_AUTH_ON_REKEY', 'IPSEC_IKE_PEER_AUTH_ON_REKEY', 'IPSEC_IPV6_SPLIT_TUNNELING_POLICY', 'IPSEC_MODE_CONFIG', 'IPSEC_OVER_UDP', 'IPSEC_OVER_UDP_PORT', 'IPSEC_REQUIRE_SPLIT_TUNNELING', 'IPSEC_SPLIT_DNS_NAMES', 'IPSEC_SPLIT_TUNNEL_ALL_DNS', 'IPSEC_SPLIT_TUNNEL_LIST', 'IPSEC_SPLIT_TUNNELING_POLICY', 'IPV6_PRIMARY_DNS', 'IPV6_SECONDARY_DNS', 'L2TP_ENCRYPTION', 'L2TP_MPPC_COMPRESSION', 'MS_CLIENT_SUBNET_MASK', 'PPTP_MPPC_COMPRESSION', 'WEBVPN_VLAN'],
valueMappings (Array[LdapToCiscoValueMapping]): A list of LdapToCiscoValueMapping objects, which specify the value mappings for the attribute.
 Field level constraints: cannot be null. (Note: Additional constraints might exist),
type (string): ldapattributemapping
 }

LdapAttributeToGroupPolicyMapping
description: An LDAP attribute to group policy mapping defines a customer-specific LDAP attribute name and maps it to a specific group policy. (Note: The field level constraints listed here might not cover all the constraints on the field. Additional constraints might exist.)
ldapName (string): The customer-specific LDAP attribute name that is being mapped.
 Field level constraints: cannot be null, must match pattern `^(?!:).*`. (Note: Additional constraints might exist),
valueMappings (Array[LdapToGroupPolicyValueMapping]): A list of LdapToGroupPolicyValueMapping objects, which specify the value mappings for the attribute.
 Field level constraints: cannot be null. (Note: Additional constraints might exist),
type (string): ldapattributetogrouppolicymapping
 }

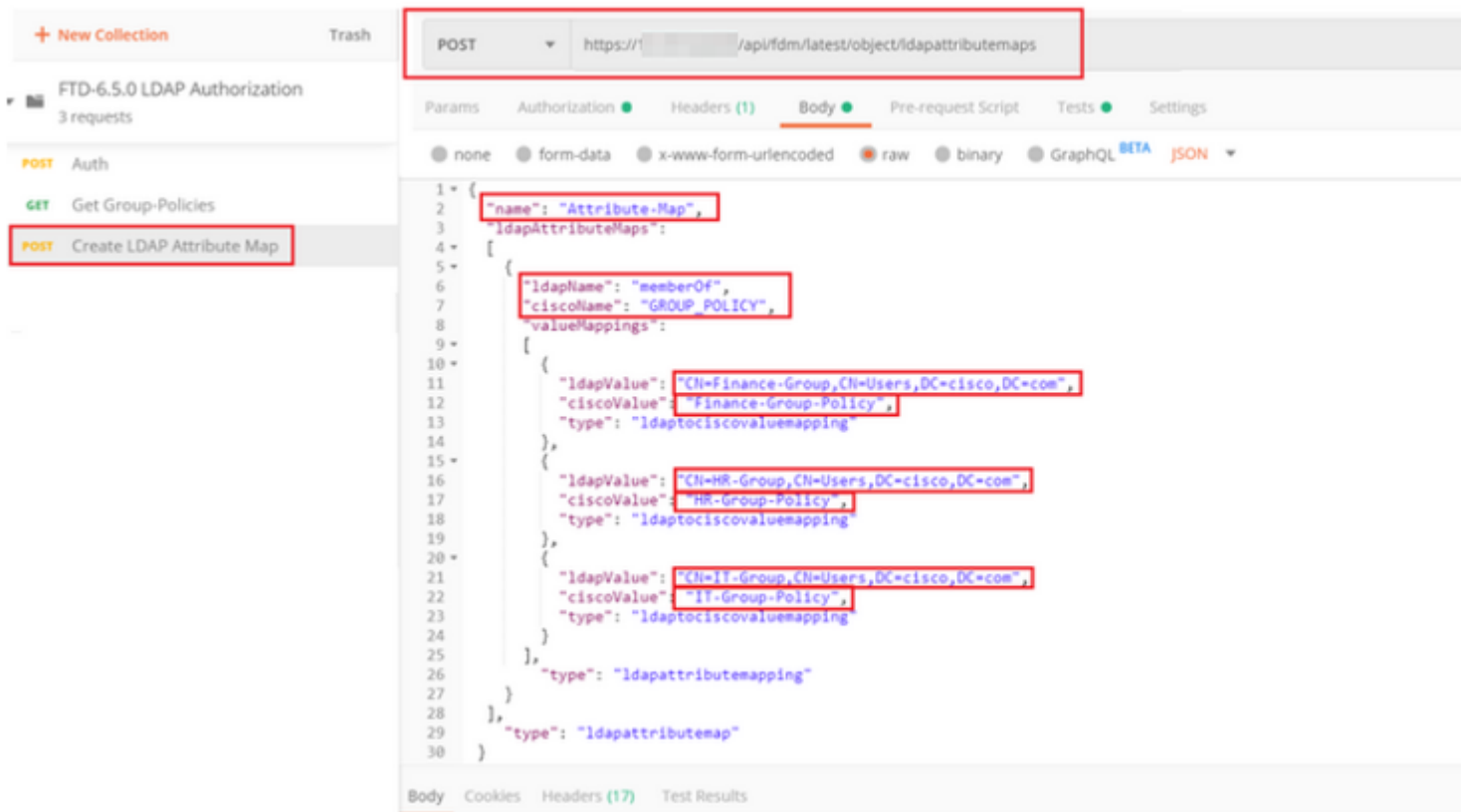
â€f

De URL voor het posten van de LDAP Attribute Map is: <https://<FTD Management IP>/api/fdm/last/object/ldapattributemaps>

Het corpus van de POST-aanvraag moet het volgende bevatten:

name	Naam voor LDAP Attribute-Map
type	ldapattributemapping
LDPnaam	lid van
CiscoName	GROEP_BELEID
LDPwaarde	MemberOfValue voor Gebruiker van AD
Cisco-waarde	Groepsbeleidsnaam voor elke gebruikersgroep in FDM

â€f



â€f

De hoofdtekst van het POST-verzoek bevat de LDAP Attribute map-informatie die een specifiek Group-Policy toewijst aan een AD-groep op basis van de waarde **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"
  ]
}

```

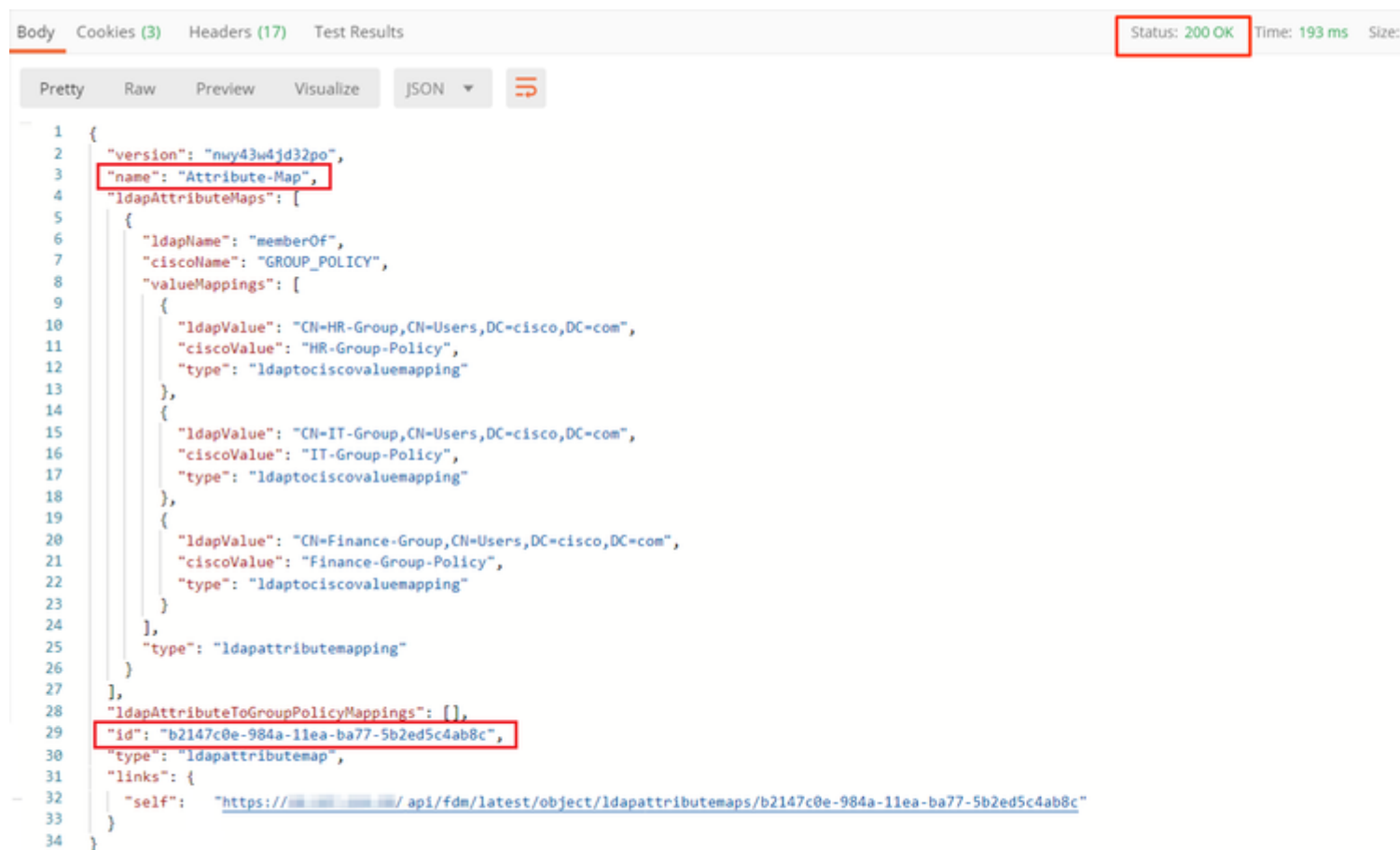


```
],
  "type": "ldapattributemap"
}
```

Opmerking: Het veld **memberOf** kan met de **dsquery**-opdracht worden opgehaald van de AD-server of kan worden gehaald uit de LDAP-debuglogs op de FTD. In de debug logbestanden zoekt u **naar memberOf value: field**.

â€f

Het antwoord op dit POST-verzoek lijkt op de volgende output:



```
Body Cookies (3) Headers (17) Test Results Status: 200 OK Time: 193 ms Size:
Pretty Raw Preview Visualize JSON
1 {
2   "version": "nwy43w4jd32po",
3   "name": "Attribute-Map",
4   "ldapAttributeMaps": [
5     {
6       "ldapName": "memberOf",
7       "ciscoName": "GROUP_POLICY",
8       "valueMappings": [
9         {
10        "ldapValue": "CN=HR-Group,CN=Users,DC=cisco,DC=com",
11        "ciscoValue": "HR-Group-Policy",
12        "type": "ldaptociscovaluemapping"
13      },
14      {
15        "ldapValue": "CN=IT-Group,CN=Users,DC=cisco,DC=com",
16        "ciscoValue": "IT-Group-Policy",
17        "type": "ldaptociscovaluemapping"
18      },
19      {
20        "ldapValue": "CN=Finance-Group,CN=Users,DC=cisco,DC=com",
21        "ciscoValue": "Finance-Group-Policy",
22        "type": "ldaptociscovaluemapping"
23      }
24    ],
25    "type": "ldapattributemapping"
26  }
27 ],
28 "ldapAttributeToGroupPolicyMappings": [],
29 "id": "b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c",
30 "type": "ldapattributemap",
31 "links": {
32   "self": "https://.../api/fdm/latest/object/ldapattributemaps/b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c"
33 }
34 }
```

Stap 7. Voeg een nieuw GET-verzoek toe om de huidige AD-realm-configuratie op FDM te verkrijgen.

De URL voor de huidige AD-[realmconfiguratie](https://<FTD Management IP>/api/fdm/latest/object/realms) is: <https://<FTD Management IP>/api/fdm/latest/object/realms>

â€f

The screenshot shows a REST client interface with a GET request to `https://.../api/fdm/latest/object/realms`. The response is a JSON object with the following structure:

```

1 {
2   "items": [
3     {
4       "version": "ks3pdhe5ixiyy",
5       "name": "LDAP-AD",
6       "directoryConfigurations": [
7         {
8           "hostname": "...",
9           "port": 389,
10          "encryptionProtocol": "NONE",
11          "encryptionCert": null,
12          "type": "directoryconfiguration"
13        }
14      ],
15      "enabled": true,
16      "systemDefined": false,
17      "realmId": 3,
18      "dirUsername": "administrator@...",
19      "dirPassword": "*****",
20      "baseDN": "dc=..., dc=com",
21      "ldapAttributeMap": null,
22      "adPrimaryDomain": "...",
23      "id": "bf50a8ab-9819-11ea-ba77-d32ecc224295",
24      "type": "activedirectoryrealm",
25      "links": {
26        "self": "https://.../api/fdm/latest/object/realms/bf50a8ab-9819-11ea-ba77-d32ecc224295"
27      }
28    }
29  ],
30  "paging": {
31    "prev": [],
32    "next": [],
33    "limit": 10,
34    "offset": 0,
35    "count": 1,
36    "pages": 0
37  }
38 }

```

â€f

Bericht dat de waarde voor zeer belangrijke **ldapAttributeMap** ongeldig is.

â€f

Stap 8. Maak een nieuwe **PUT** aanvraag om het AD-domein te bewerken. Kopieer de **GET** response output van de vorige stap en voeg deze toe aan de Body van deze nieuwe **PUT** request. Deze stap kan worden gebruikt om wijzigingen aan te brengen in de huidige instellingen van AD Realm, bijvoorbeeld: wachtwoord wijzigen, IP-adres of nieuwe waarde toevoegen voor een sleutel zoals **ldapAttributeMap** in dit geval.

Opmerking: het is belangrijk om de inhoud van de lijst met items te kopiëren in plaats van de hele GET response-output. De URL van het verzoek voor het PUT-verzoek moet worden toegevoegd aan de item-id van het object waarvoor wijzigingen worden aangebracht. In dit voorbeeld is de waarde: `bf50a8ab-9819-11ea-ba77-d32ecc224295`

â€f

De URL voor het bewerken van de huidige AD-[realmconfiguratie](#) is: <https://<FTD Management IP>/api/fdm/latest/object/realms/<realm ID>>

De tekst van het PUT request dient het volgende te bevatten:

versie	versie die is verkregen uit antwoord op vorige GET-aanvraag
id	id verkregen uit reactie op eerder GET verzoek

â€f

The screenshot shows a REST client interface with a PUT request to the URL `https://[redacted]/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@[redacted].com",
17  "dirPassword": "*****",
18  "baseDN": "dc=[redacted], dc=com",
19  "ldapAttributeMap":
20  {
21    "id": "b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c",
22    "type": "ldapattributemap"
23  },
24  "adPrimaryDomain": "[redacted].com",
25  "id": "bf50a8ab-9819-11ea-ba77-d32ecc224295",
26  "type": "activedirectoryrealm",
27  "links": {
28    "self": "https://[redacted]/api/fdm/latest/object/realms/bf50a8ab-9819-11ea-ba77-d32ecc224295"
29  }
30 }
31

```

â€f

De body voor de configuratie in dit voorbeeld is:

<#root>

```

{
  "version": "ks3p4he5ixiyy",
  "name": "LDAP-AD",
  "directoryConfigurations": [
    {
      "hostname": "<IP Address>",
      "port": 389,
      "encryptionProtocol": "NONE",
      "encryptionCert": null,
      "type": "directoryconfiguration"
    }
  ],
  "enabled": true,
  "systemDefined": false,
  "realmId": 3,
  "dirUsername": "administrator@example.com",
  "dirPassword": "*****",
  "baseDN": "dc=example, dc=com",
  "ldapAttributeMap":
  {

```

```
"id": "b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c",
"type": "ldapattributemap"
},
"adPrimaryDomain": "example.com",
"id": "bf50a8ab-9819-11ea-ba77-d32ecc224295",
"type": "activedirectoryrealm",
"links": {
  "self": "https://

/api/fdm/latest/object/realms/bf50a8ab-9819-11ea-ba77-d32ecc224295"

}
}
```

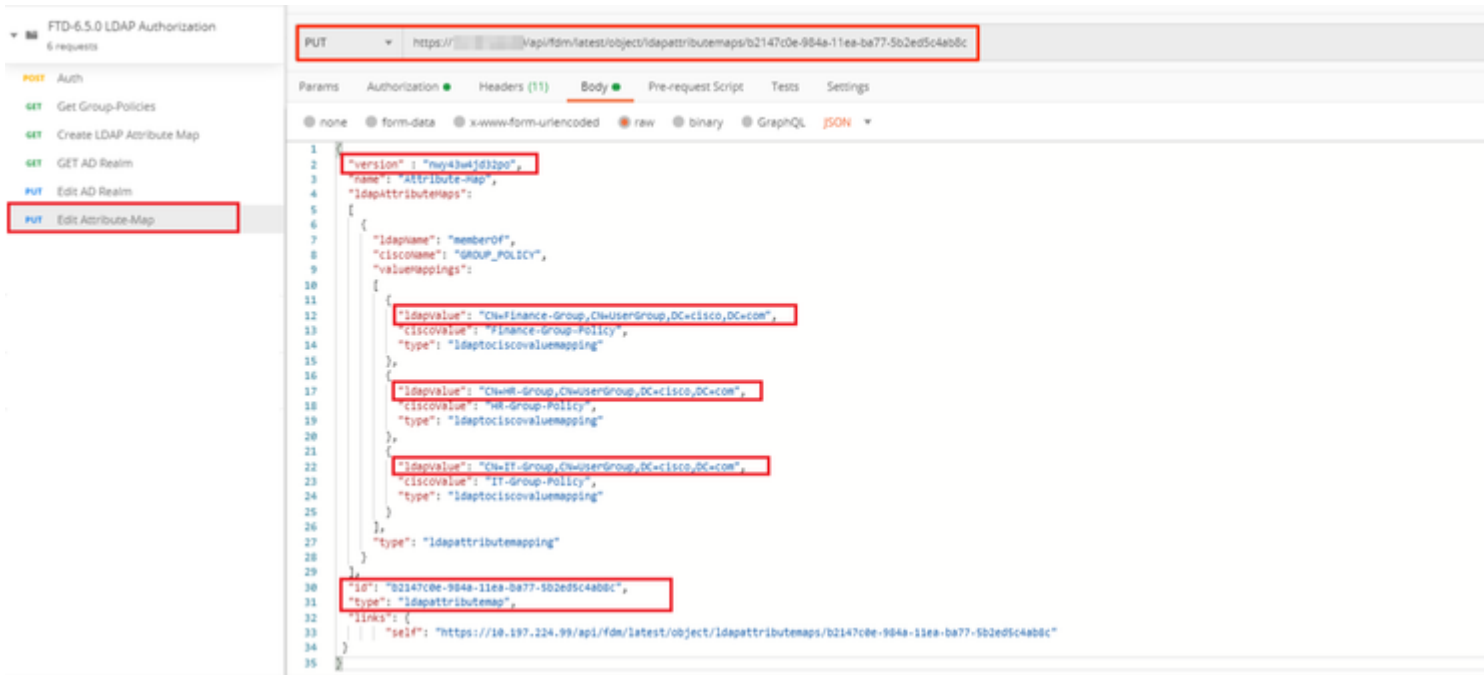
Controleer of de **ldapAttributeMap-id** overeenkomt in het antwoordorgaan voor dit verzoek.

```
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/realm/bf50a8ab-9819-11ea-ba77-d32ecc224295"
30  }
31 }
```

â€f

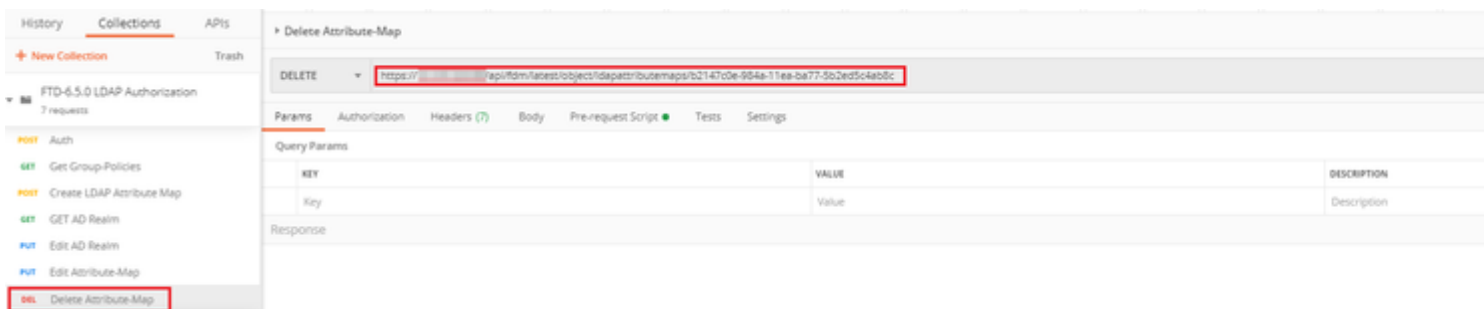
(Optioneel). De LDAP attributenkaart kan met **PUT** verzoeken worden gewijzigd. Maak een nieuwe PUT aanvraag **Bewerk Attribute-Map** en breng wijzigingen aan zoals de naam van de Attribute-Map of memberOf waarde. T

In het volgende voorbeeld is de waarde van **ldapvalue** gewijzigd van **CN=User** naar **CN=UserGroup** voor alle drie de groepen.



â€f

(Optioneel). Als u een bestaande LDAP Attribute-Map wilt verwijderen, maakt u een Delete Verzoek **Delete Attribute-Map**. Neem de **map-id** van de vorige HTTP-respons op en voeg deze toe met de basis-URL van het verwijderingsverzoek.



Opmerking: Als het attribuut **memberOf** spaties bevat, moet het URL zijn gecodeerd voor de Web Server om het te parsen. Anders wordt een **400 Slecht Verzoek HTTP-antwoord** ontvangen. Voor een string die spaties met witte spaties bevat, kan "%20" of "+" gebruikt worden om deze fout te voorkomen.

â€f

Stap 9. Navigeer terug naar FDM, selecteer het implementatiepictogram en klik op **Nu implementeren**.

â€f

Pending Changes

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

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

â€f

Verifiëren

De implementatiewijzigingen kunnen worden geverifieerd in de sectie **Implementatiegeschiedenis** van de 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].value
-	ldapAttributeMaps[0].cisco
-	name: Attribute-Map

Active Directory Realm Edited: LDAP-AD

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

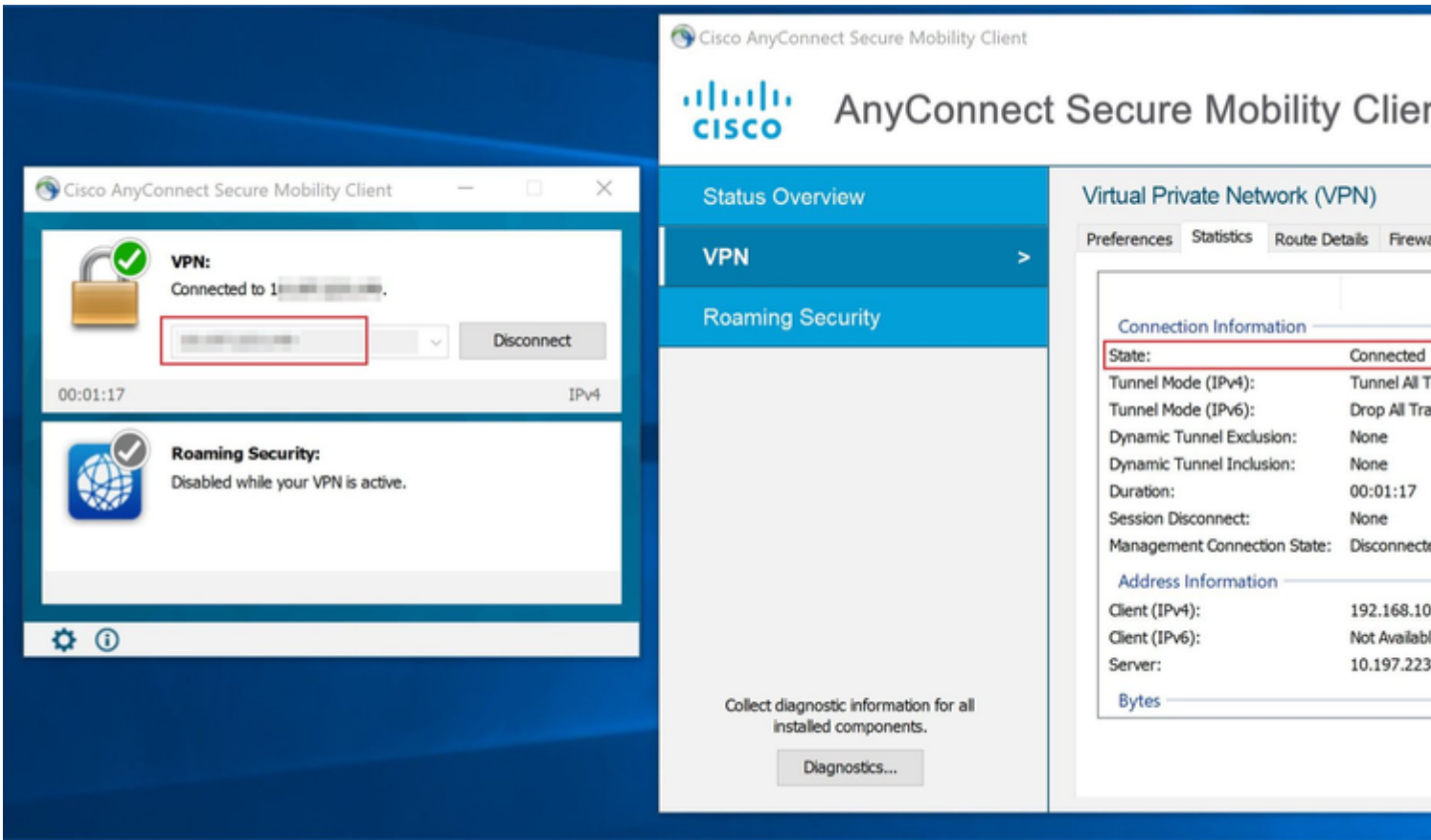
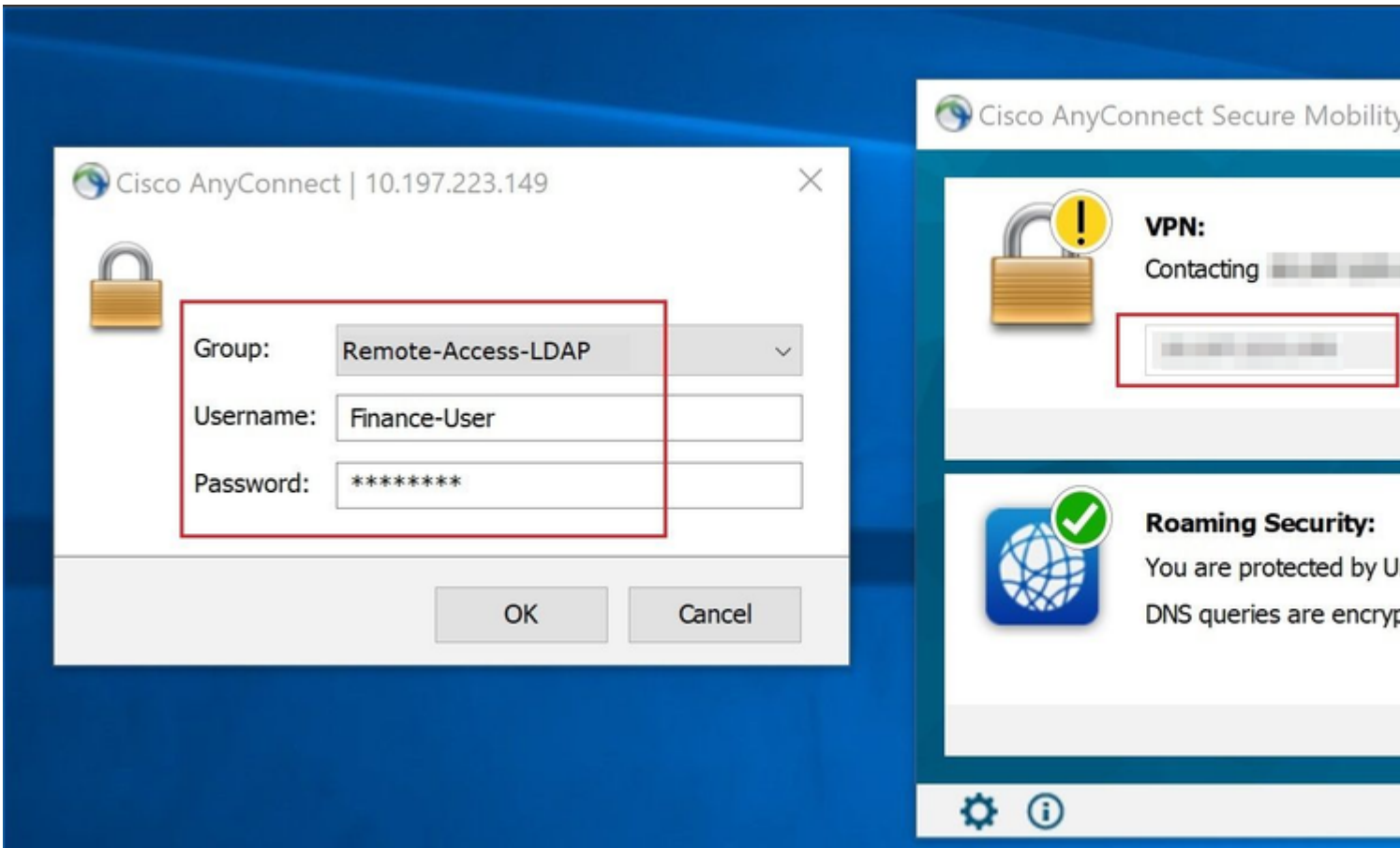
ldapAttributeMap:	
-	Attribute-Map

â€f

Om deze configuratie te testen, specificeert u de AD-referenties in de velden **Gebruikersnaam** en **Wachtwoord**.

Wanneer een gebruiker die tot de AD-groep **Finance-Group** behoort probeert in te loggen, is de poging succesvol zoals verwacht.

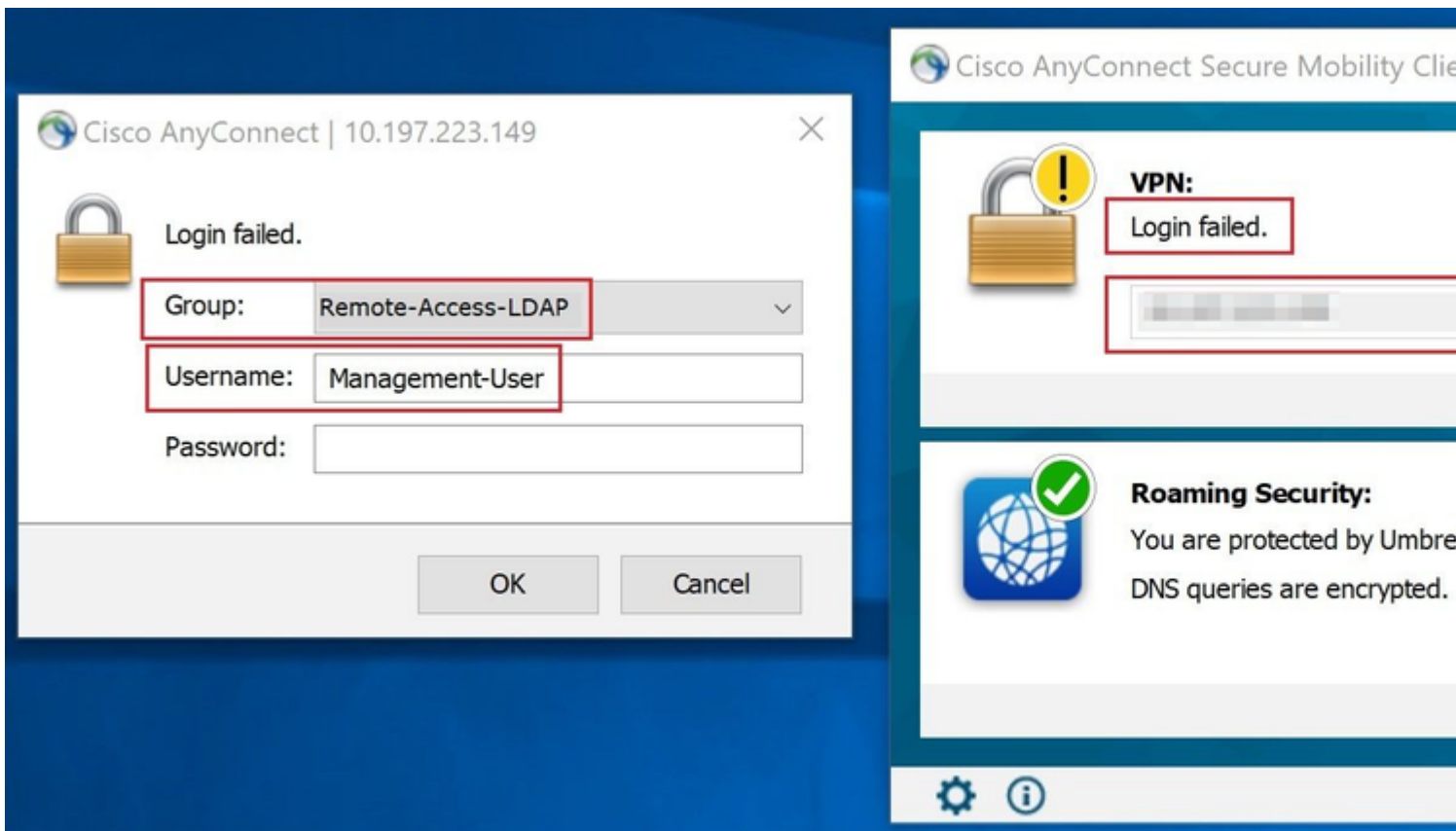
â€f



â€f

Wanneer een gebruiker die behoort tot de **Management-Group** in AD probeert verbinding te maken met

Connection-Profile **Remote-Access-LDAP**, omdat geen LDAP Attribute Map een match heeft teruggegeven, is het Group-Policy dat door deze gebruiker op de FTD wordt geërfd **NOACCESS** dat VPN-simultane-logins op waarde 0 heeft ingesteld. De inlogpoging voor deze gebruiker mislukt dus.



â€f

De configuratie kan worden geverifieerd met de volgende showopdrachten van de FTD CLI:

```
<#root>
```

```
firepower#
```

```
show vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect
```

```
Username      :
```

```
Finance-User
```

```
      Index      : 26
Assigned IP    : 192.168.10.1      Public IP      : 10.1.1.1
Protocol      : AnyConnect-Parent SSL-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384
Bytes Tx      : 22491197          Bytes Rx      : 14392
Group Policy  :
```

```
Finance-Group-Policy
```

```
      Tunnel Group : Remote-Access-LDAP
Login Time       : 11:14:43 UTC Sat Oct 12 2019
```

```
Duration      : 0h:02m:09s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A          VLAN      : none
Audt Sess ID  : 000000000001a0005da1b5a3
Security Grp  : none         Tunnel Zone : 0
```

<#root>

firepower#

```
show run aaa-server LDAP-AD
```

```
aaa-server LDAP-AD protocol ldap
  realm-id 3
aaa-server AD1 host 192.168.1.1
  server-port 389
  ldap-base-dn dc=example, dc=com
  ldap-scope subtree
  ldap-login-password *****
  ldap-login-dn Administrator@example.com
  server-type auto-detect
```

```
ldap-attribute-map Attribute-Map
```

<#root>

firepower#

```
show run ldap attribute-map
```

```
ldap attribute-map Attribute-Map
  map-name memberOf Group-Policy
  map-value memberOf CN=Finance-Group,CN=Users,DC=cisco,DC=com Finance-Group-Policy
  map-value memberOf CN=HR-Group,CN=Users,DC=cisco,DC=com HR-Group-Policy
  map-value memberOf CN=IT-Group,CN=Users,DC=cisco,DC=com IT-Group-Policy
```

Problemen oplossen

Een van de meest voorkomende problemen bij het configureren van REST API is om het token aan toonder van tijd tot tijd te verlengen. De symbolische verlooptijd wordt gegeven in het antwoord op het verzoek om toestemming. Als deze tijd verstrijkt, kan een extra verversen token voor een langere tijd worden gebruikt. Als het verversen-token ook verloopt, moet er een nieuw autorisatieverzoek worden verstuurd naar een nieuw toegangstoken.

N.B.: Raadpleeg [Belangrijke informatie over debug-opdrachten](#) voordat u **debug**-opdrachten gebruikt.

U kunt verschillende debug-niveaus instellen. Standaard wordt niveau 1 gebruikt. Als u het debug-niveau wijzigt, kan de hoeveelheid debug-informatie toenemen. Wees hier voorzichtig mee, vooral in productieomgevingen.

De volgende debugs op de FTD CLI zou nuttig zijn bij problemen met betrekking tot LDAP Attribute Map

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

In dit voorbeeld, de volgende debugs werden verzameld om de informatie aan te tonen die van de AD server werd ontvangen toen de testgebruikers noemden alvorens te verbinden.

LDAP-debuggs voor **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

LDAP-debugg voor **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

Gerelateerde informatie

Neem voor extra assistentie contact op met het Cisco Technical Assistance Center (TAC). Een geldig ondersteuningscontract is vereist: [Cisco's wereldwijde contactgegevens voor ondersteuning](#).

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.