

Konfigurieren der LDAP-Attributzuordnung für RAVPN auf von FDM verwaltetem FTD

Inhalt

- [Einleitung](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Authentifizierungsablauf](#)
- [LDAP-Attributzuordnungsablauf erklärt](#)
- [Konfigurieren](#)
- [Konfigurationsschritte bei FDM](#)
- [Konfigurationsschritte für die LDAP-Attributzuordnung](#)
- [Überprüfung](#)
- [Fehlerbehebung](#)
- [Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird das Verfahren zur Verwendung eines Lightweight Directory Access Protocol (LDAP)-Servers beschrieben, um Remote Access VPN-Benutzer (RA VPN) zu authentifizieren und zu autorisieren und ihnen je nach ihrer Gruppenmitgliedschaft auf dem LDAP-Server einen anderen Netzwerkzugriff zu gewähren.

Voraussetzungen

Anforderungen

- Grundkenntnisse der RA VPN-Konfiguration auf dem Firewall Device Manager (FDM)
- Grundkenntnisse der LDAP-Serverkonfiguration für FDM
- Grundkenntnisse von REpresentational State Transfer (REST) Application Program Interface (API) und FDM Rest API Explorer
- Cisco FTD Version 6.5.0 oder neuer, von FDM verwaltet

Verwendete Komponenten

Folgende Hardware- und Softwareversionen der Anwendung/Geräte wurden verwendet:

- Cisco FTD Version 6.5.0, Build 115
- Cisco AnyConnect Version 4.10
- Microsoft Active Directory (AD)-Server
- Postman oder jedes andere API-Entwicklungstool

Hinweis: Konfigurationsunterstützung für Microsoft AD Server und das Postmal-Tool wird von Cisco nicht bereitgestellt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Authentifizierungsablauf



LDAP-Attributzuordnungsablauf erklärt

1. Der Benutzer initiiert eine VPN-Verbindung für den Remote-Zugriff mit dem FTD und gibt einen Benutzernamen und ein Kennwort für sein Active Directory (AD)-Konto an.
2. Der FTD sendet eine LDAP-Anfrage an den AD-Server über Port 389 oder 636 (LDAP über SSL)
3. Das AD antwortet mit allen dem Benutzer zugeordneten Attributen auf das FTD.
4. Die FTD gleicht die empfangenen Attributwerte mit der LDAP-Attributzuordnung ab, die auf der FTD erstellt wurde. Dies ist der Autorisierungsprozess.
5. Der Benutzer stellt dann eine Verbindung her und übernimmt die Einstellungen der Gruppenrichtlinie, die mit dem **memberOf**-Attribut in der LDAP-Attributzuordnung übereinstimmt.

Für die Zwecke dieses Dokuments erfolgt die Autorisierung von AnyConnect-Benutzern mithilfe des **memberOf** LDAP-Attributs.

- Das **memberOf**-Attribut des LDAP-Servers für jeden Benutzer wird einer ldapValue-Entität im FTD zugeordnet. Wenn der Benutzer zur entsprechenden AD-Gruppe gehört, wird die diesem LDAP-Wert zugeordnete Gruppenrichtlinie vom Benutzer geerbt.
- Wenn der **memberOf**-Attributwert für einen Benutzer keiner der ldapValue-Entitäten im FTD entspricht, wird die Standardgruppenrichtlinie für das ausgewählte Verbindungsprofil vererbt. In diesem Beispiel wird **NOACCESS**-Gruppenrichtlinie auf geerbt.

Konfigurieren

Die LDAP-Attributzuordnung für das von FDM verwaltete FTD wird mit der REST-API konfiguriert.

Konfigurationsschritte bei FDM

Schritt 1: Überprüfen Sie, ob das Gerät für die **Smart Licensing-Funktion** registriert ist.

Model: Cisco ASA5545-X Threat Defense | Software: 6.5.0-115 | VDB: 309.0 | Rule Update: 2019-08-12-001-vrt | High Availability: Not Configured



<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

Schritt 2: Überprüfen Sie, ob **AnyConnect-Lizenzen** für den FDM aktiviert sind.

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

Schritt 3: Überprüfen Sie, ob im Token die **exportgesteuerten Funktionen** aktiviert sind.

Device Summary

Smart License

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

Last sync: 11 Oct 2019 09:33 A

Next sync: 11 Oct 2019 09:43 A

SUBSCRIPTION LICENSES INCLUDED

Threat

 Enabled

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

Includes:  Intrusion Policy

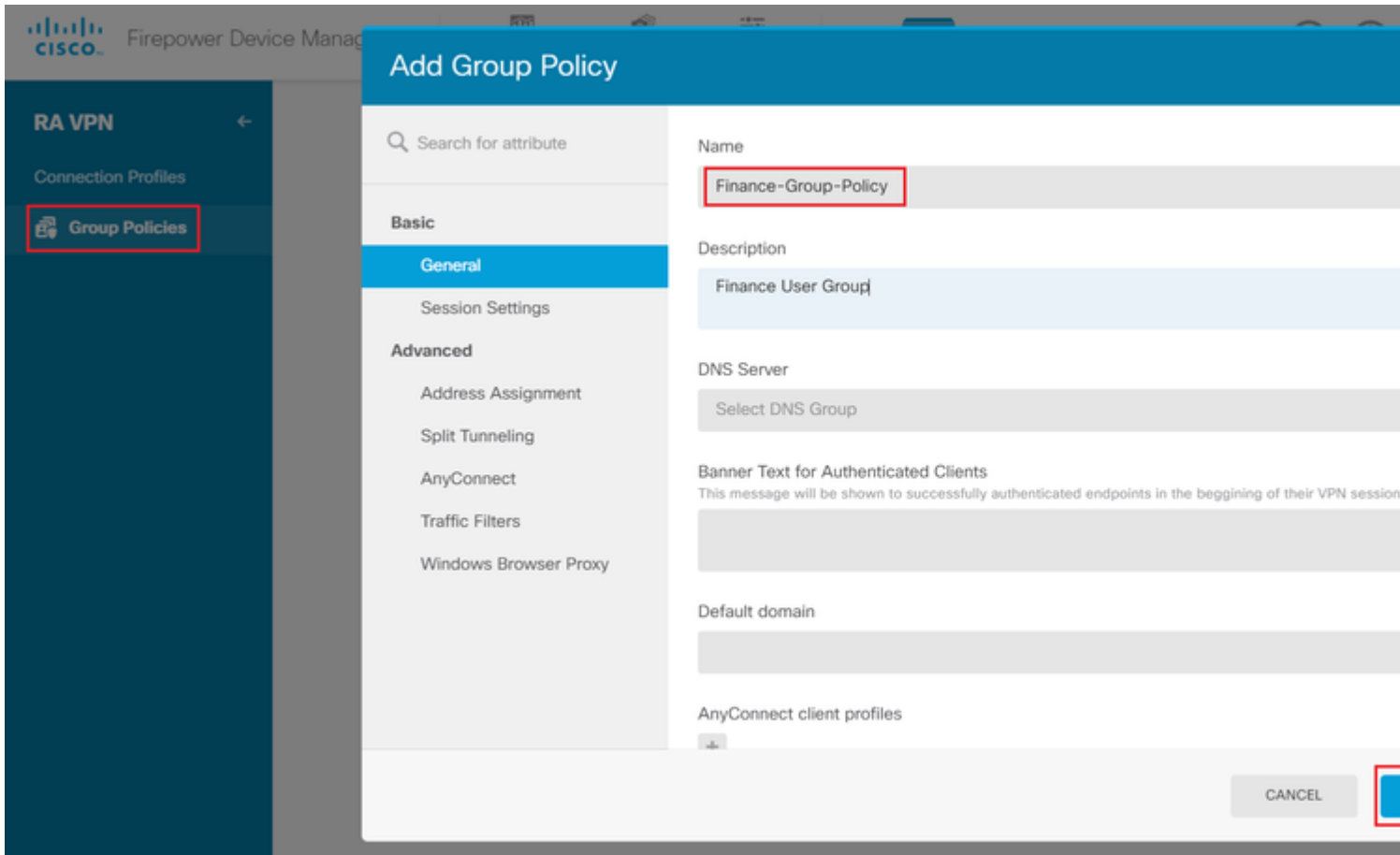
Hinweis: In diesem Dokument wird davon ausgegangen, dass RA VPN bereits konfiguriert ist. Im folgenden Dokument finden Sie weitere Informationen zur [RA VPN-Konfiguration auf FTD-Geräten, die von FDM verwaltet werden.](#)

â€f

Schritt 4: Navigieren Sie zu **Remotezugriff-VPN > Gruppenrichtlinien.**

â€f

Schritt 5: Navigieren Sie zu **Gruppenrichtlinien**. Klicken Sie auf '+', um die verschiedenen Gruppenrichtlinien f#r jede AD-Gruppe zu konfigurieren. In diesem Beispiel werden die Gruppenrichtlinien **Finance-Group-Policy**, **HR-Group-Policy** und **IT-Group-Policy** f#r den Zugriff auf verschiedene Subnetze konfiguriert.



â€f

Die **Finanzgruppenrichtlinie** hat folgende Einstellungen:

<#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

Ebenso hat **HR-Group-Policy** folgende Einstellungen:

```
<#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

Schließlich gibt es noch die folgenden Einstellungen für **IT-Gruppenrichtlinien**:

```
<#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

Schritt 6: Erstellen Sie einen Gruppenrichtlinien-**NOACCESS**, navigieren Sie zu **Session Settings**, und deaktivieren Sie die Option **Simultane Anmeldung pro Benutzer**. Damit wird der Wert **vpn-simultan-logins** auf 0 gesetzt.

Der Wert **vpn-simultan-login** in der Gruppenrichtlinie, wenn er auf 0 gesetzt ist, beendet die VPN-Verbindung des Benutzers sofort. Dieser Mechanismus wird verwendet, um zu verhindern, dass Benutzer, die zu einer anderen als den konfigurierten AD-Benutzergruppe gehören (in diesem Beispiel Finanzen, Personalverwaltung oder IT), erfolgreiche Verbindungen zum FTD herstellen und auf sichere Ressourcen zugreifen, die nur für die zulässigen Benutzergruppenkonten verfügbar sind.

Benutzer, die zu richtigen AD-Benutzergruppen gehören, stimmen mit der LDAP-Attributzuordnung im FTD überein und erben die zugeordneten Gruppenrichtlinien, während Benutzer, die keiner der zulässigen Gruppen angehören, dann die Standardgruppenrichtlinie des Verbindungsprofils erben, in diesem Fall **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

Die **NOACCESS**-Gruppenrichtlinie hat die folgenden Einstellungen:

```
<#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

```

Schritt 7. Navigieren Sie zu **Verbindungsprofile**, und erstellen Sie ein Verbindungsprofil. In diesem Beispiel lautet der Profilname "**Remote-Access-LDAP**". Wählen Sie Primary Identity Source **AAA Only** aus, und erstellen Sie einen neuen Authentifizierungsservertyp **AD**.

The screenshot shows the configuration interface for a VPN connection profile in Cisco Firepower Device Manager. The profile name is "Remote-Access-LDAP". The authentication type is set to "AAA Only". A dropdown menu for "Primary Identity Source for User Authentication" is open, showing "LocalIdentitySource" and "Special-Identities-Realm". A "Create new" button is visible, and a sub-menu is open with "AD" selected. The "NEXT" button is highlighted in blue.

Geben Sie die Informationen des AD-Servers ein:

- Verzeichnisbenutzername

- Verzeichniskennwort
- Basis-DN
- AD-Hauptdomäne
- Hostname/IP-Adresse
- Anschluss
- Verschlüsselungstyp

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

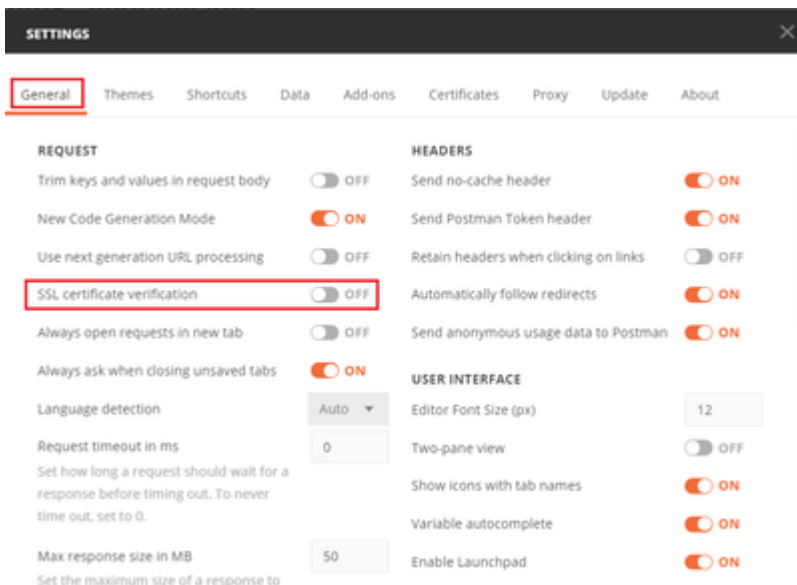
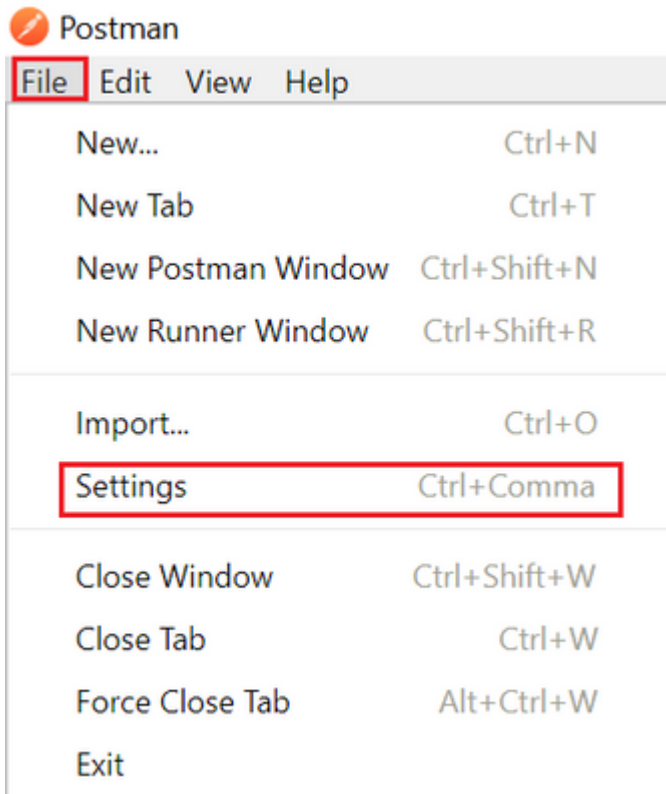
Please select a certificate

TEST

[Add another configuration](#)

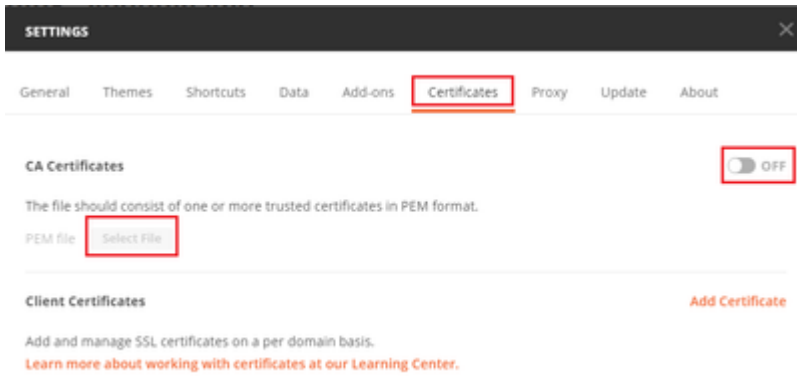
CANCEL

, und deaktivieren Sie die SSL-Zertifikatsüberprüfung, um einen SSL-Handshake-Fehler beim Senden von API-Anfragen an den FTD zu vermeiden. Dies geschieht, wenn die FTD ein selbstsigniertes Zertifikat verwendet.



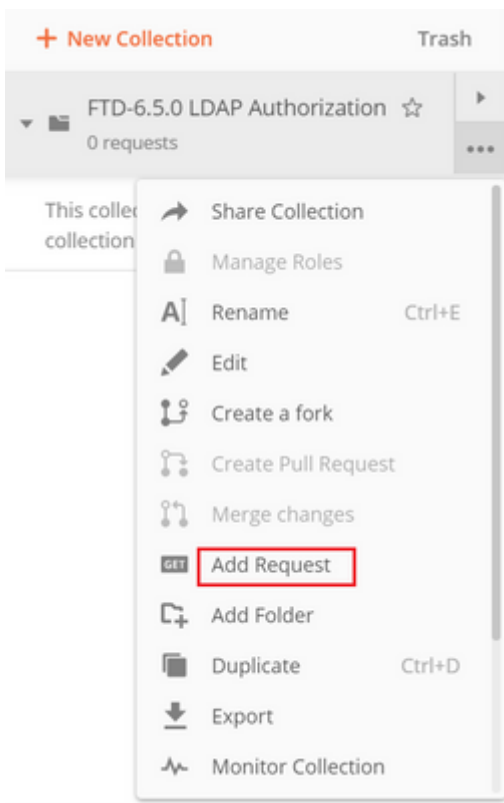
â€f

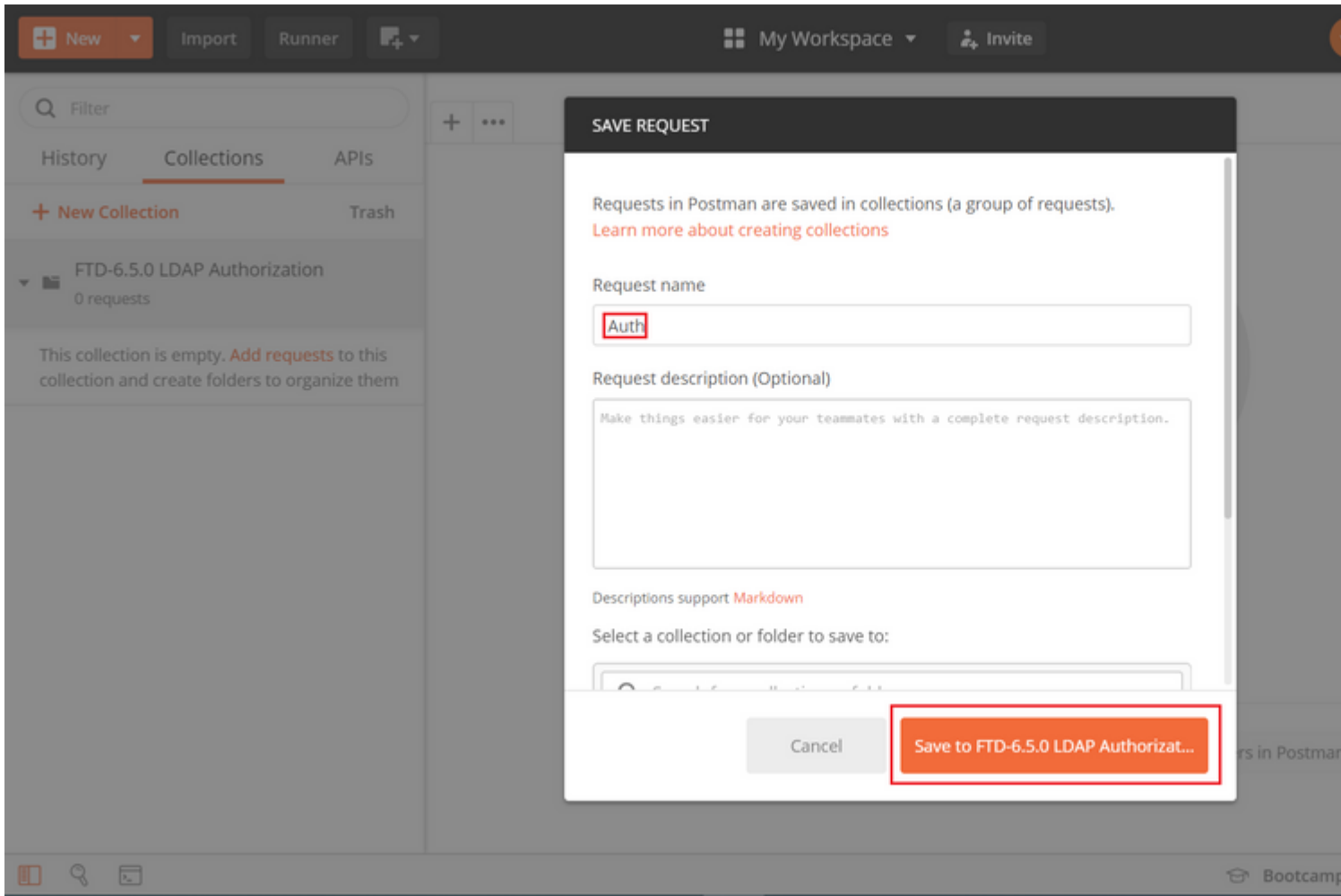
Alternativ dazu kann das vom FTD verwendete Zertifikat im Zertifikatabschnitt der Einstellungen als Zertifizierungsstellenzertifikat hinzugefügt werden.



â€f

Schritt 4: Fügen Sie eine neue POST-Anforderungsauthentifizierung hinzu, um eine Anmelde-POST-Anforderung an das FTD zu erstellen, damit das Token zur Autorisierung von POST-/GET-Anforderungen verwendet werden kann.





â€f

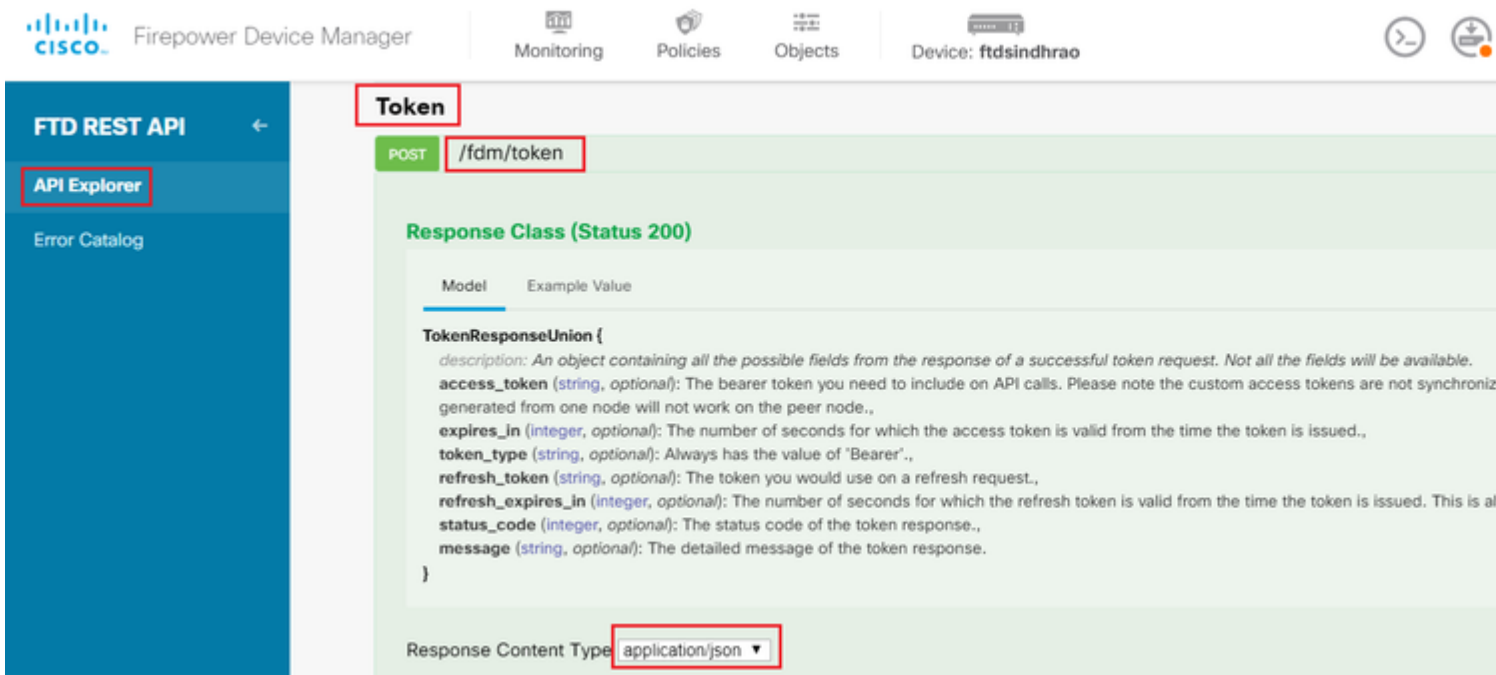
Alle Postman-Anforderungen für diese Sammlung müssen die folgenden Elemente enthalten:

Basis-URL: <https://<FTD Management IP>/api/fdm/neueste/>

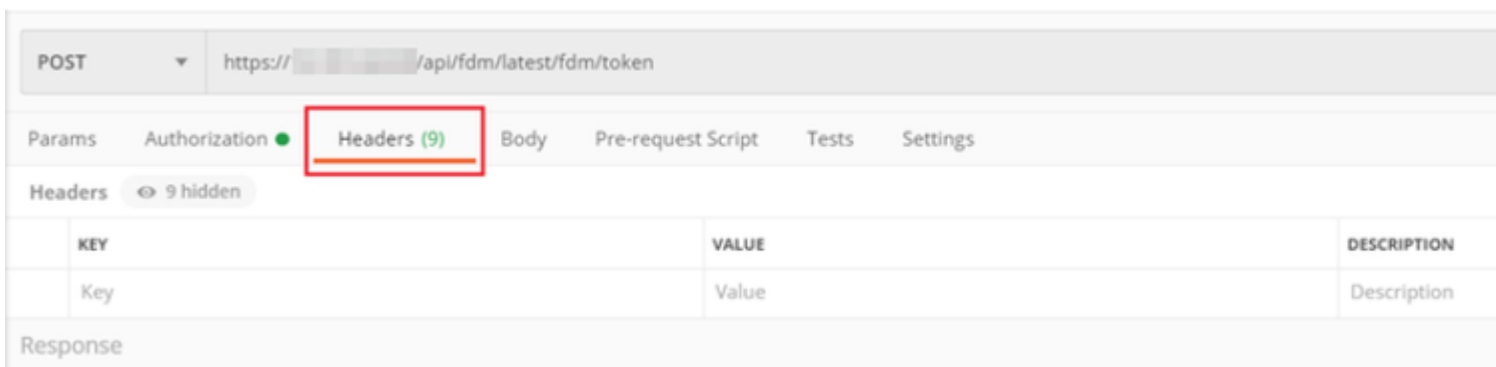
Hängen Sie in der Anforderungs-URL die Basis-URL mit den entsprechenden Objekten an, die hinzugefügt oder geändert werden müssen.

â€f

Hier wird eine Authentifizierungsanforderung für ein Token erstellt, die von <https://<FTD Management IP>/api-explorer> verwiesen wird. Dies muss auf andere Objekte überprüft werden und die notwendigen Änderungen müssen für diese vorgenommen werden.



Navigieren Sie zu **Headers**, und klicken Sie auf **Manage Presets (Voreinstellungen verwalten)**.



â€f

Erstellen Sie ein neues Voreingestelltes **Header-LDAP**, und fügen Sie das folgende Schlüssel-Wert-Paar hinzu:

Inhaltstyp	application/json
Akzeptieren	application/json

â€f

MANAGE HEADER PRESETS

Add Header Preset

Header-LDAP

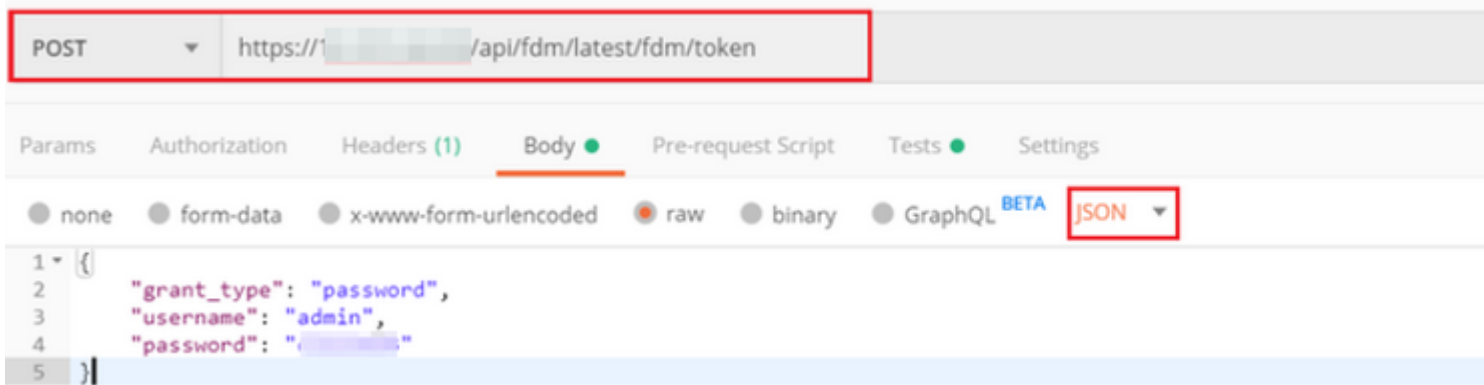
	KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/>	Content-Type	application/json	
<input checked="" type="checkbox"/>	Accept	application/json	
	Key	Value	Description

Navigieren Sie für alle anderen Anforderungen zu den entsprechenden Header-Registerkarten, und wählen Sie diesen Preset Header-Wert aus: **Header-LDAP** für die REST-API-Anforderungen, **json** als primären Datentyp zu verwenden.

Der Hauptteil der POST-Anforderung zum Abrufen des Tokens muss Folgendes enthalten:

Typ	raw - JSON (Anwendung/json)
Gewährungstyp	Kennwort
Benutzername	Admin-Benutzername zur Anmeldung beim FTD
Kennwort	Dem Administrator-Benutzerkonto zugeordnetes Kennwort

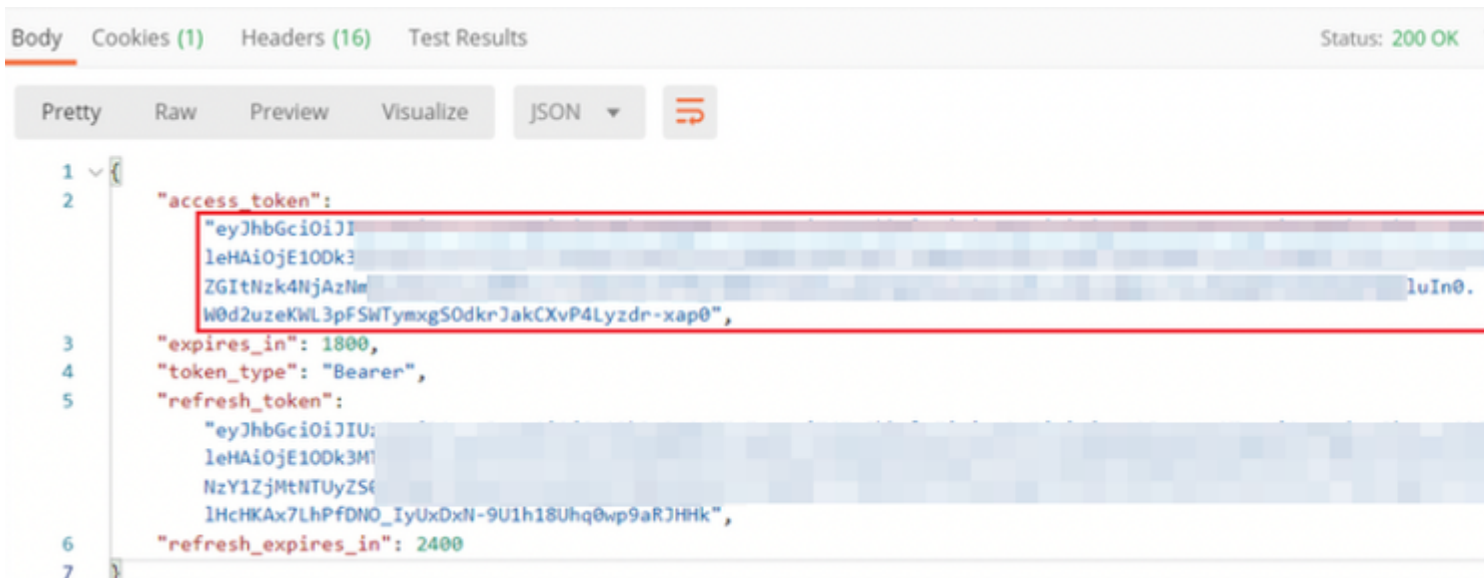
```
{
  "grant_type": "password",
  "username": "admin",
  "password": "<enter the password>"
}
```



â€f

Wenn Sie auf **Senden** klicken, enthält der Text der Antwort das Zugriffstoken, das verwendet wird, um PUT-/GET-/POST-Anfragen an den FTD zu senden.

â€f



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

â€f

Dieses Token wird dann verwendet, um alle nachfolgenden Anforderungen zu autorisieren.

â€f

Navigieren Sie zur Registerkarte "**Autorisierung**" für jede neue Anforderung, und wählen Sie die nächste aus:

â€f

Typ	OAuth 2.0
Token	Das Zugriffstoken, das beim Ausführen der POST-Anforderung für die Anmeldung empfangen wurde

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

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpYXBQIjE1ODk3MDg0MTwianRpljoiNjgwM2EyNzMtOTgyMi0xMwVhLWJhbnMxliwibmJmljoxNTg5NzA4NDYyLCJleHAiOiE1ODhUb2t1bkV4cGlyZXNBdCI6MTU4OTcxMDgxMjk2MjI0IiwiaWF0IjoiY2VzcyIsInVzZXJvdWlkijoiZWNIzY1ZjMwZGltNzk4NjAzNmMyZmUwliwidXNlcjlvbGUiOiJSZ2luIjoicGFzc3dvcmQILCJ1c2VybmFtZSI6ImFkbWwFSWYmXGSOdkrjakCXvP4Lyzdr-xap0
```

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

â€f

Schritt 5: Fügen Sie eine neue GET-Anforderung **Get Group-Policies** hinzu, um den Gruppenrichtlinienstatus und die Gruppenrichtlinieneinstellungen abzurufen. Sammeln Sie den Namen und die **ID** für jede konfigurierte Gruppenrichtlinie (in diesem Beispiel: **Finance-Group-Policy**, **HR-Group-Policy** und **IT-Group-Policy**), die Sie im nächsten Schritt verwenden möchten.

â€f

Die URL zum Abrufen der konfigurierten Gruppenrichtlinien lautet: <https://<FTD-Management-IP>/api/fdm/latest/object/ravpngrouppolicies>

â€f

Im nächsten Beispiel wird Group-Policy **Finance-Group-Policy** hervorgehoben.

â€f

```

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   "enableGatewayOPD": false,
100  "gatewayOPDInterval": 30,
101  "enableClientOPD": false,
102  "clientOPDInterval": 30,
103  "clientProfiles": [],
104  "keepInstallerOnClient": false,
105  "vpnTrafficFilterACL": null,
106  "enableRestrictVPNTOVLAN": false,
107  "restrictVPNTOVLANId": null,
108  "clientFirewallPrivateNetworkRules": null,
109  "clientFirewallPublicNetworkRules": null,
110  "browserProxyType": "NO_MODIFY",
111  "proxy": {
112    "serverHost": null,
113    "port": null,
114    "type": "serverhostandport"
115  },
116  "proxyExceptions": [],
117  "isDisablePeriodicClientCertAuthentication": false,
118  "id": "a5722b15-9836-11ea-ba77-6916f09ace0c",
119  "type": "ravpngrouppolicy",
120  "links": {
121    "self": "https://[redacted]/api/fdm/latest/object/ravpngrouppolicies/a5722b15-9836-11ea-ba77-6916f09ace0c"
122  }
123 },

```

â€š

Schritt 6: Fügen Sie eine neue POST-Anforderung hinzu. **Erstellen Sie eine LDAP-Attributzuordnung**, um die LDAP-Attributzuordnung zu erstellen. In diesem Dokument wird das Modell **LdapAttributeMapping** verwendet. Andere Modelle verfügen ebenfalls über ähnliche Operationen und Methoden zum Erstellen einer Attributzuordnung. Beispiele für diese Modelle sind im api-explorer verfügbar, wie bereits in diesem Dokument erwähnt.

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
 }

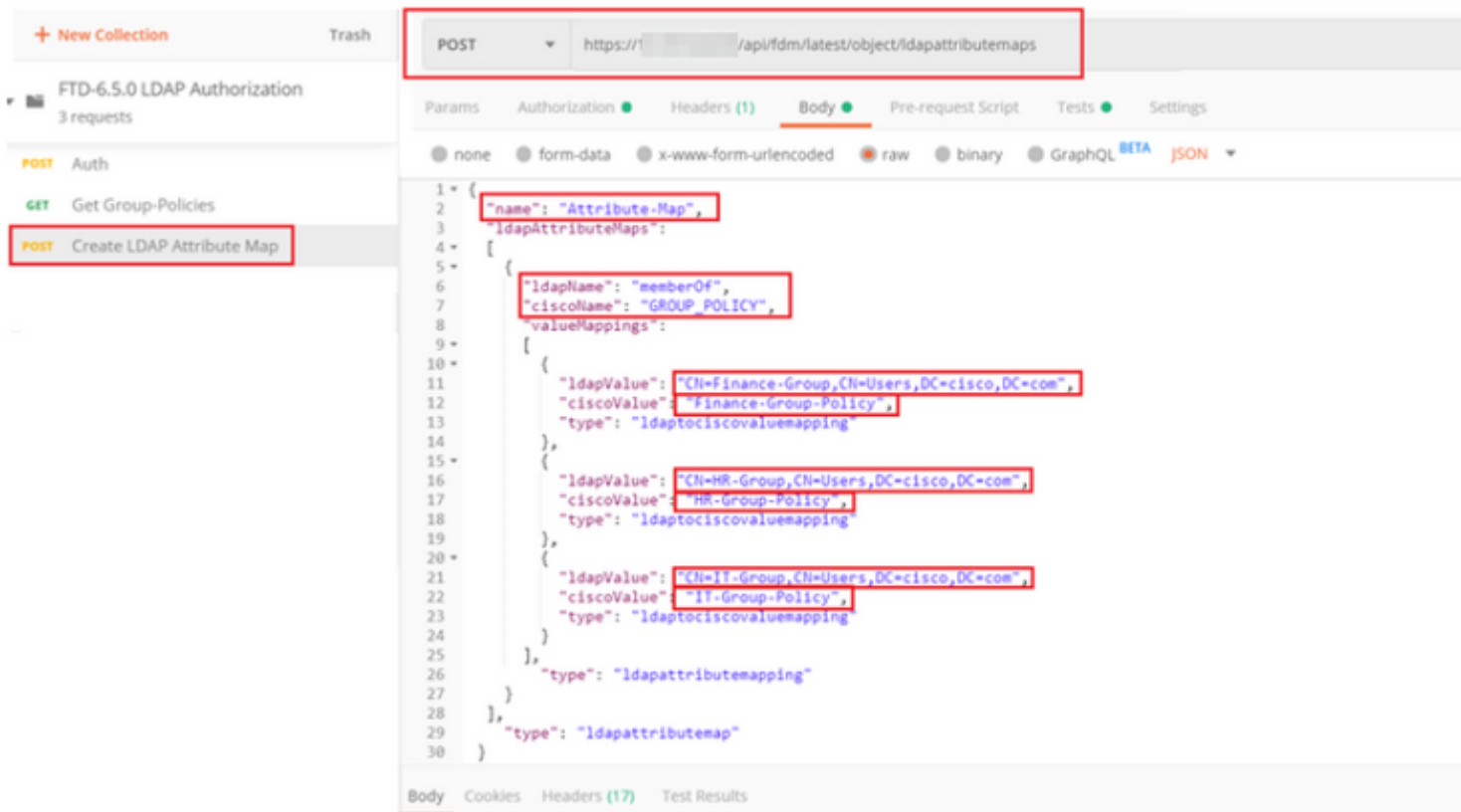
â€š

Die URL für den POST-Test der LDAP-Attributzuordnung lautet: <https://<FTD-Management-IP>/api/fdm/latest/object/ldapattributemaps>

Der Text der POST-Anforderung muss Folgendes enthalten:

name	Name für LDAP-Attributzuordnung
typ	ldapattributemapping
LDAP-Name	MitgliedVon
ciscoName	GRUPPENRICHTLINIE
ldapWert	memberOf-Wert für Benutzer von AD
CiscoWert	Gruppenrichtlinienname für jede Benutzergruppe in FDM

â€š



â€f

Der Text der POST-Anforderung enthält die LDAP-Attributzuordnungsinformationen, die eine bestimmte Gruppenrichtlinie einer AD-Gruppe basierend auf dem **memberOf**-Wert zuordnen:

```
{
  "name": "Attribute-Map",
  "ldapAttributeMaps":
  [
    {
      "ldapName": "memberOf",
      "ciscoName": "GROUP_POLICY",
      "valueMappings":
      [
        {
          "ldapValue": "CN=Finance-Group,CN=Users,DC=cisco,DC=com",
          "ciscoValue": "Finance-Group-Policy",
          "type": "ldaptociscovaluemapping"
        },
        {
          "ldapValue": "CN=HR-Group,CN=Users,DC=cisco,DC=com",
          "ciscoValue": "HR-Group-Policy",
          "type": "ldaptociscovaluemapping"
        },
        {
          "ldapValue": "CN=IT-Group,CN=Users,DC=cisco,DC=com",
          "ciscoValue": "IT-Group-Policy",
          "type": "ldaptociscovaluemapping"
        }
      ]
    },
    {
      "type": "ldapattributemapping"
    }
  ],
  "type": "ldapattributemap"
}
```

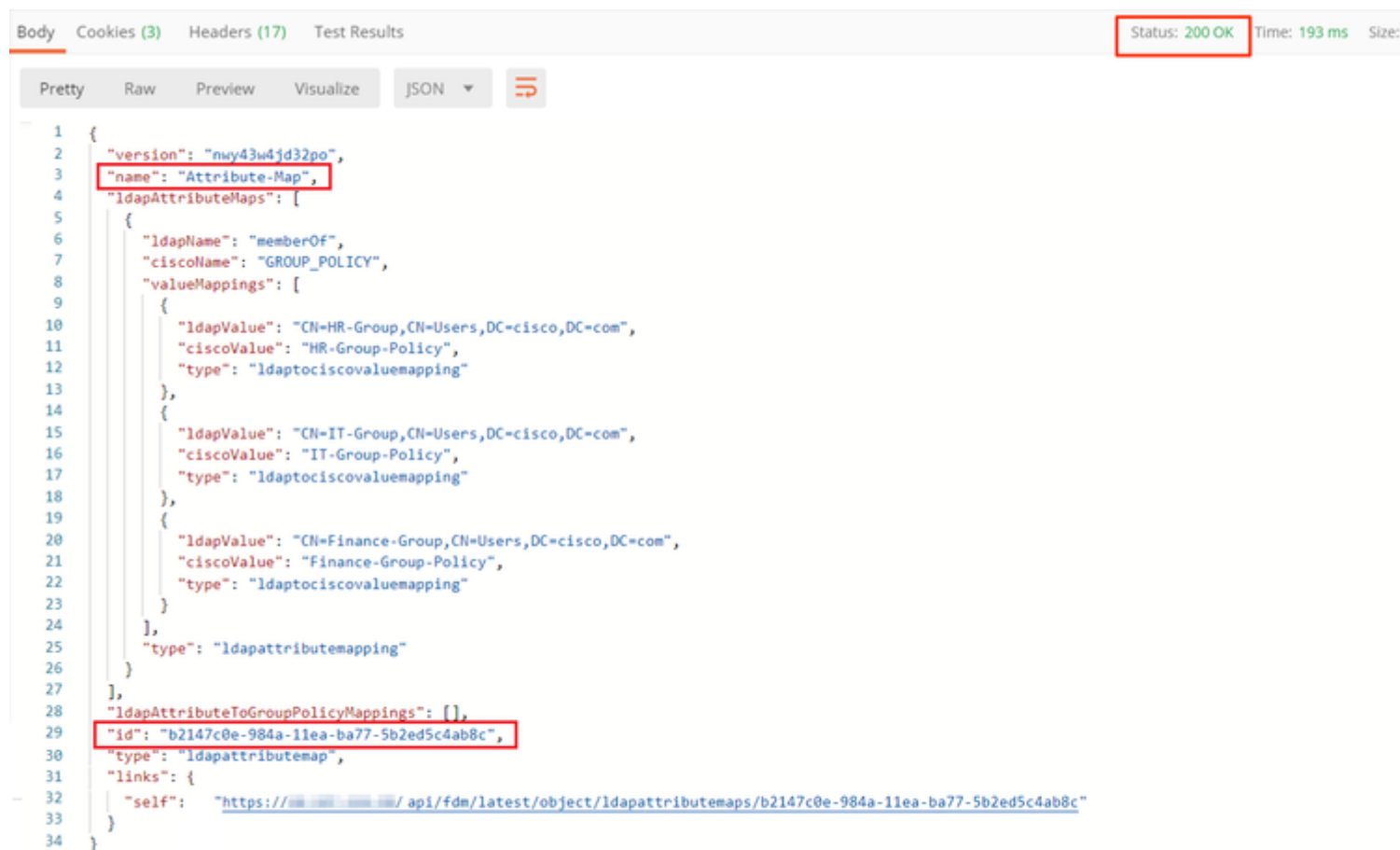


```
],  
  "type": "ldapattributemap"  
}
```

Hinweis: Das **memberOf**-Feld kann mit dem Befehl **dsquery** vom AD-Server abgerufen oder aus den LDAP-Debugs auf dem FTD abgerufen werden. Suchen Sie in den Debug-Protokollen nach **memberOf-Wert**.

â€f

Die Antwort auf diese POST-Anforderung sieht ähnlich aus wie die nächste Ausgabe:



```
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 }
```

Schritt 7. Fügen Sie eine neue GET-Anforderung hinzu, um die aktuelle AD-Bereichskonfiguration für FDM abzurufen.

Die URL zum Abrufen der aktuellen AD-Bereichskonfiguration lautet: <https://<FTD Management IP>/api/fdm/latest/object/realms>

â€f

```

1  {
2    "items": [
3      {
4        "version": "ks3pd4he5ixiyy",
5        "name": "LDAP-AD",
6        "directoryConfigurations": [
7          {
8            "hostname": "10.10.10.10",
9            "port": 389,
10           "encryptionProtocol": "NONE",
11           "encryptionCert": null,
12           "type": "directoryconfiguration"
13         }
14       ],
15       "enabled": true,
16       "systemDefined": false,
17       "realId": 3,
18       "dirUsername": "administrator@10.10.10.10",
19       "dirPassword": "*****",
20       "baseDN": "dc=10.10.10.10, dc=com",
21       "ldapAttributeMap": null,
22       "adPrimaryDomain": "10.10.10.10",
23       "id": "bf50a8ab-9819-11ea-ba77-d32ecc224295",
24       "type": "activedirectoryrealm",
25       "links": {
26         "self": "https://10.10.10.10/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

Beachten Sie, dass der Wert für key **ldapAttributeMap** null ist.

â€f

Schritt 8: Erstellen Sie eine neue **PUT**-Anforderung, um den AD-Bereich zu bearbeiten. Kopieren Sie die **GET**-Antwortausgabe aus dem vorherigen Schritt, und fügen Sie sie dem Hauptteil dieser neuen **PUT**-Anforderung hinzu. Dieser Schritt kann verwendet werden, um Änderungen an der aktuellen AD Realm-Konfiguration vorzunehmen, z. B.: Ändern des Kennworts, der IP-Adresse oder Hinzufügen eines neuen Werts für einen beliebigen Schlüssel wie **ldapAttributeMap** in diesem Fall.

Hinweis: Es ist wichtig, den Inhalt der Elementliste zu kopieren, anstatt die gesamte GET-Antwortausgabe. Die Anforderungs-URL für die PUT-Anforderung muss an die Element-ID des Objekts angehängt werden, für das Änderungen vorgenommen werden. In diesem Beispiel lautet der Wert: bf50a8ab-9819-11ea-ba77-d32ecc224295

â€f

Die URL zum Bearbeiten der aktuellen AD-Bereichskonfiguration lautet: <https://<FTD-Management-IP>/api/fdm/latest/object/realms/<Bereichskennung>>

Der Text der PUT-Anforderung muss Folgendes enthalten:

version	Version, die aus der Antwort auf die vorherige GET-Anforderung ermittelt wurde
---------	--

ID	ID, die aus der Antwort der vorherigen GET-Anforderung ermittelt wurde.
ldapAttributeMap	ldap-id aus Antwort auf Anforderung LDAP-Attributzuordnung erstellen

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:

```

1 {
2   "version": "ks3pdhe5ixivy",
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

Der Text für die Konfiguration in diesem Beispiel lautet:

<#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"

  }
}
```

Überprüfen Sie, ob die **ldapAttributeMap-ID** mit dem Antworttext für diese Anforderung übereinstimmt.

```
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

(Optional) Die LDAP-Attributzuordnung kann mit **PUT**-Anforderungen geÃ¤ndert werden. Erstellen Sie eine neue PUT-Anforderung **Edit Attribute-Map** und nehmen Sie alle Ã¤nderungen vor, z. B. den Namen der Attribute-Map oder memberOf-Wert. T

Im nÃ¤chsten Beispiel wurde der Wert von **ldapvalue** fÃ¼r alle drei Gruppen von **CN=Users** in **CN=UserGroup** geÃ¤ndert.

```

1 PUT https://10.197.224.99/api/fdm/latest/object/idapattributemaps/b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c
2
3 Params Authorization Headers (11) Body Pre-request Script Tests Settings
4
5 none form-data x-www-form-urlencoded raw binary GraphQL JSON
6
7 1
8 2 "version": "my43edf032po",
9 3 "name": "Attribute-map",
10 4 "idapattributemaps":
11 5 {
12 6   "ldapname": "memberOf",
13 7   "cisconame": "GROUP_POLICY",
14 8   "valuemappings":
15 9   [
16 10     {
17 11       "ldapvalue": "CisFinance-Group,CisUserGroup,DC=cisco,DC=com",
18 12       "ciscoverse": "Finance-Group-Policy",
19 13       "type": "ldaptociscovaluemapping"
20 14     },
21 15     {
22 16       "ldapvalue": "CisM-Group,CisUserGroup,DC=cisco,DC=com",
23 17       "ciscoverse": "M-Group-Policy",
24 18       "type": "ldaptociscovaluemapping"
25 19     },
26 20     {
27 21       "ldapvalue": "CisIT-Group,CisUserGroup,DC=cisco,DC=com",
28 22       "ciscoverse": "IT-Group-Policy",
29 23       "type": "ldaptociscovaluemapping"
30 24     }
31 25   ],
32 26   "type": "ldapattributemapping"
33 27 }
34 28
35 29 "id": "b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c",
36 30 "type": "ldapattributemap",
37 31 "links": {
38 32   "self": "https://10.197.224.99/api/fdm/latest/object/idapattributemaps/b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c"
39 33 }
40 34
41 35

```

â€f

(Optional) Um eine vorhandene LDAP-Attributzuordnung zu löschen, erstellen Sie eine DELETE-Anforderung, **Attributzuordnung löschen**. Schließen Sie die **Map-ID** der vorherigen HTTP-Antwort ein, und fügen Sie die Basis-URL der Löschanforderung an.

```

DELETE https://10.197.224.99/api/fdm/latest/object/idapattributemaps/b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c

```

Hinweis: Wenn das **memberOf**-Attribut Leerzeichen enthält, muss es URL-codiert sein, damit der Webserver es analysieren kann. Andernfalls wird eine **400 Bad Request HTTP Response** empfangen. Bei einer Zeichenfolge mit Leerzeichen kann entweder **"%20"** oder **"+"** verwendet werden, um diesen Fehler zu vermeiden.

â€f

Schritt 9. Navigieren Sie zurück zu FDM, wählen Sie das Bereitstellungssymbol aus, und klicken Sie auf **Jetzt bereitstellen**.

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

Überprüfung

Die Änderungen an der Bereitstellung können im Abschnitt **Bereitstellungsverlauf** des FDM überprüft werden.

Device Administration ←

Audit Log

Download Configuration

Deployment Completed: User (admin) Triggered Deployment

Summary Differences View

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

Idapattributemap Added: Attribute-Map

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

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

Active Directory Realm Edited: LDAP-AD

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

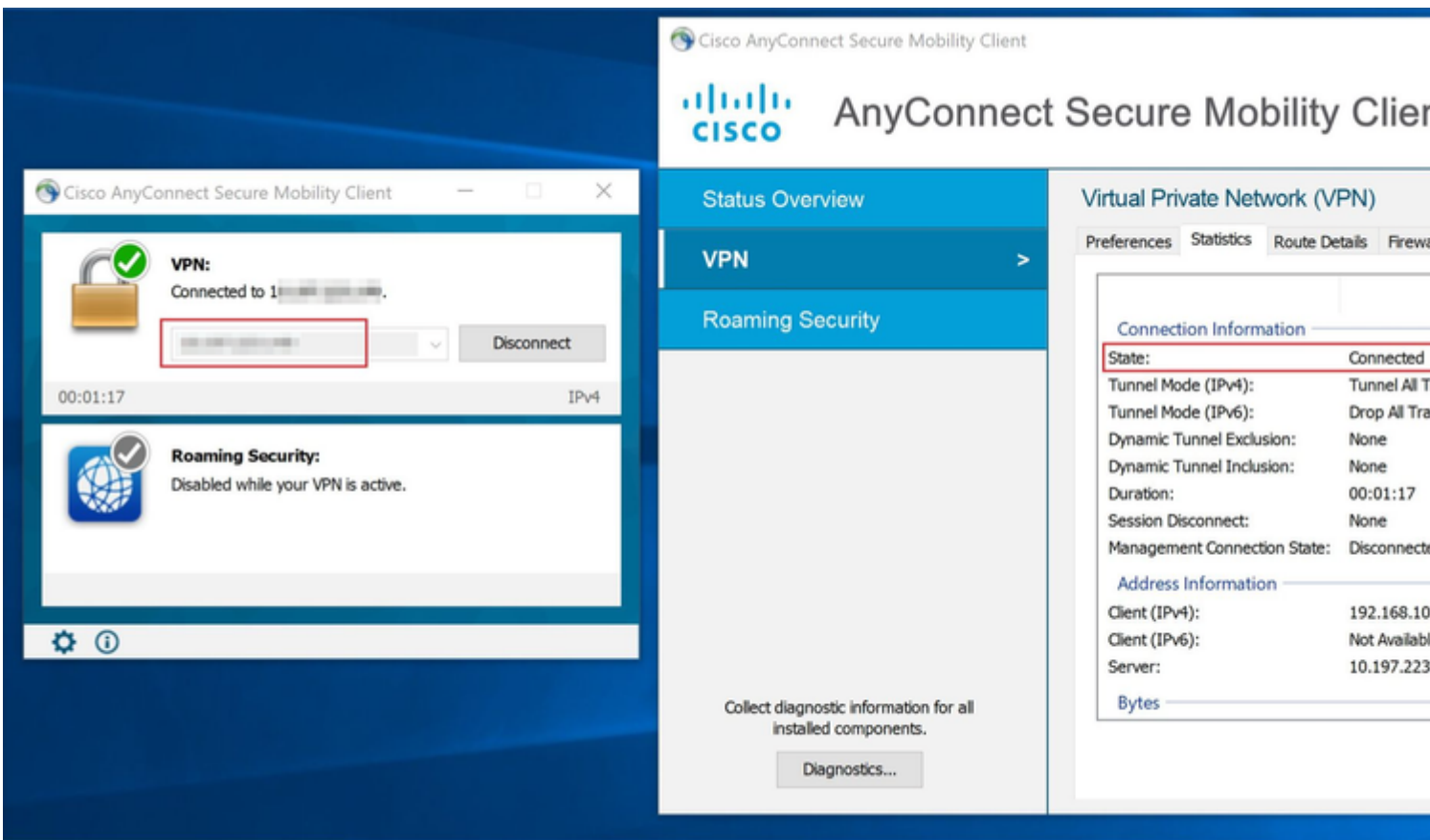
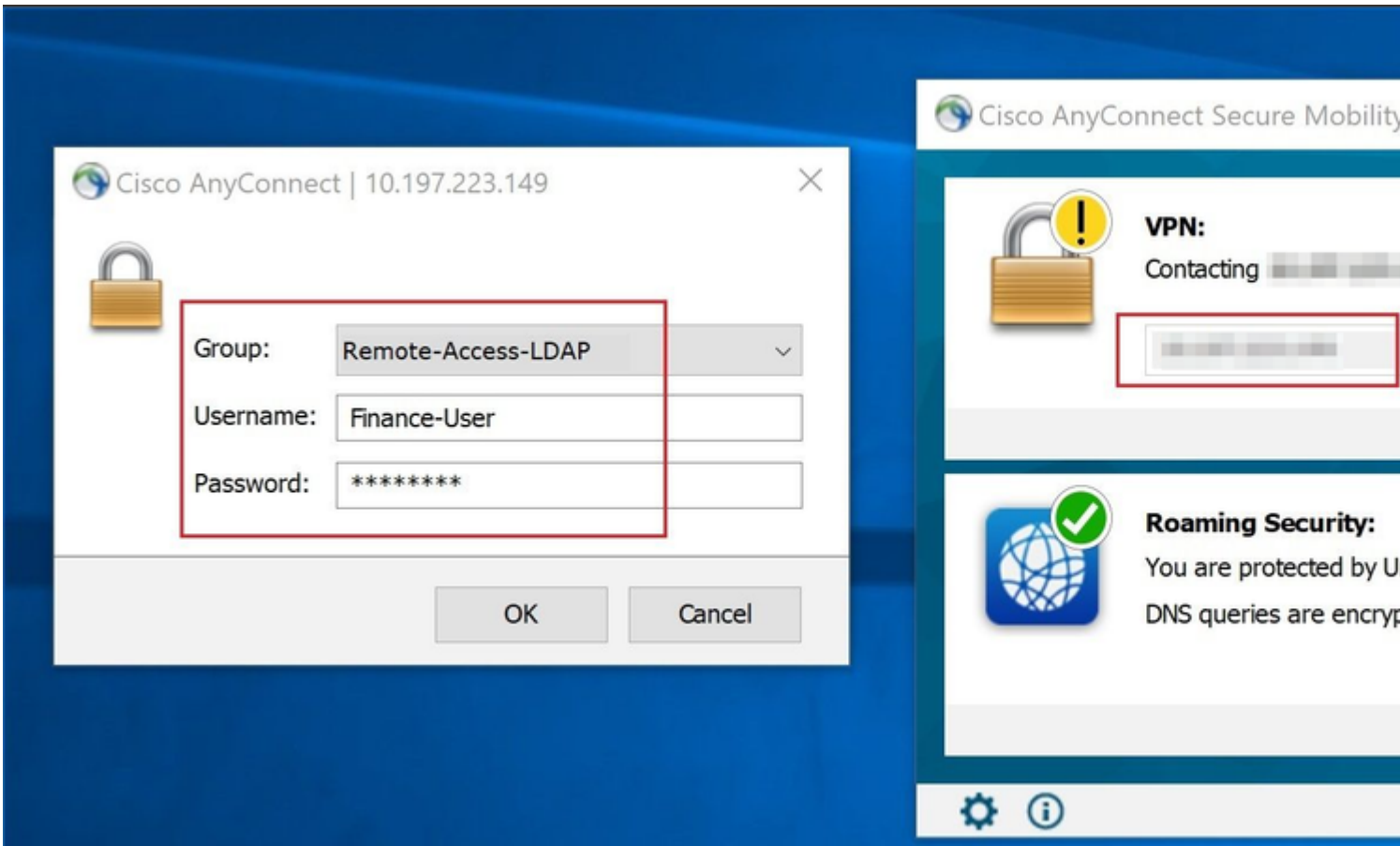
ldapAttributeMap:	
-	Attribute-Map

â€f

Um diese Konfiguration zu testen, geben Sie die AD-Anmeldeinformationen in den Feldern **Benutzername** und **Kennwort ein**.

Wenn ein Benutzer, der zur AD-Gruppe **Finance-Group** gehört, versucht, sich anzumelden, ist der Versuch wie erwartet erfolgreich.

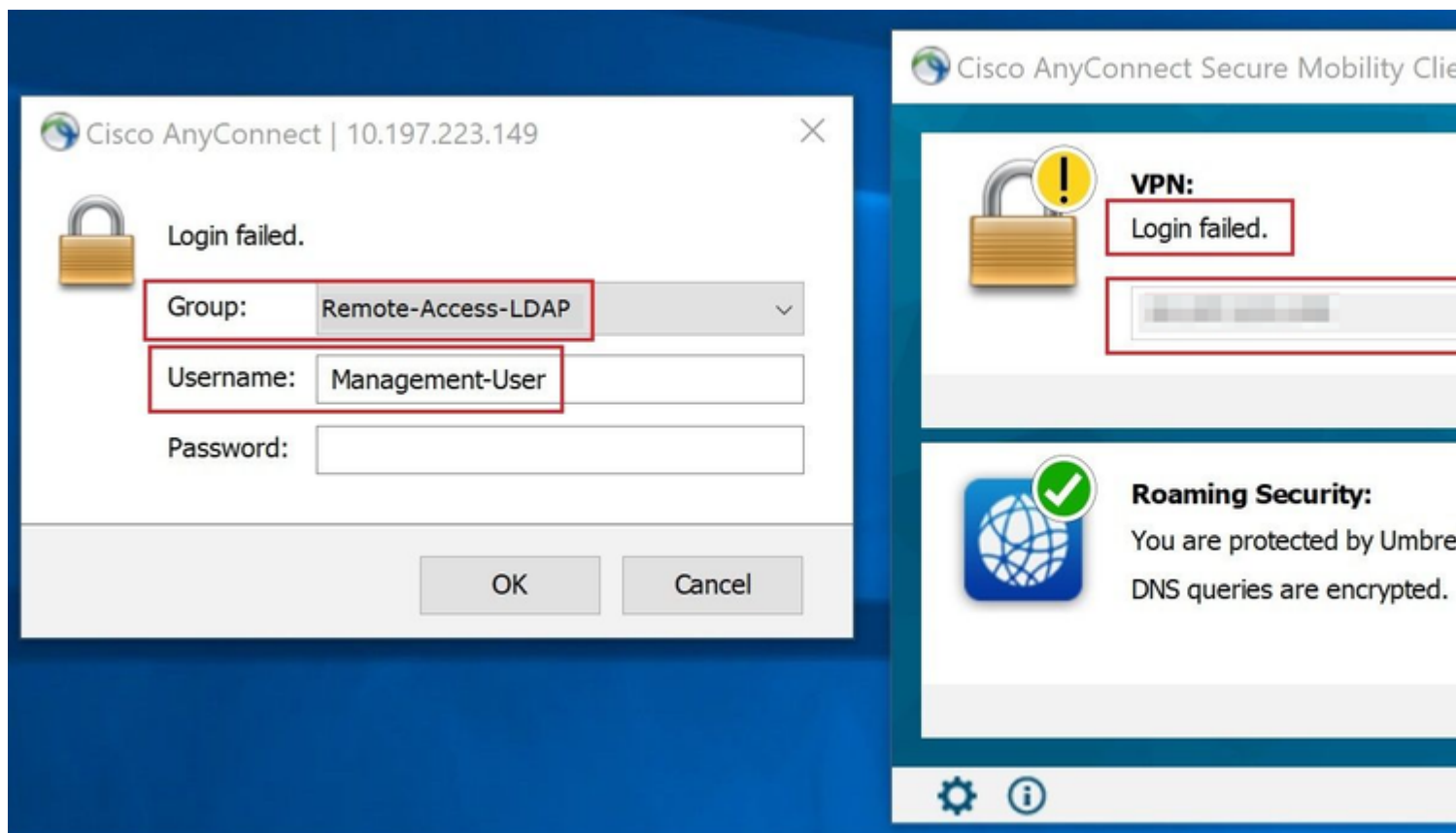
â€f



â€f

Wenn ein Benutzer, der zu der **Verwaltungsgruppe** in AD gehÃ¶rt, versucht, eine Verbindung mit dem

Verbindungsprofil-**RAS-LDAP** herzustellen, da keine LDAP-Attributzuordnung eine Übereinstimmung zurückgegeben hat, ist die von diesem Benutzer auf dem FTD geerbte Gruppenrichtlinie **NOACCESS**, die den Wert 0 für die gleichzeitige VPN-Anmeldung hat. Daher schlägt der Anmeldeversuch für diesen Benutzer fehl.



â€f

Die Konfiguration kann mit den nächsten Befehlen zum Anzeigen über die FTD-CLI überprüft werden:

```
<#root>
```

```
firepower#
```

```
show vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect
```

```
Username      :
```

```
Finance-User
```

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

```
Finance-Group-Policy
```

```
  Tunnel Group : Remote-Access-LDAP
```

```
Login Time    : 11:14:43 UTC Sat Oct 12 2019
Duration     : 0h:02m:09s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                VLAN           : none
Auds Sess ID : 000000000001a0005da1b5a3
Security Grp : none                Tunnel Zone    : 0
```

<#root>

firepower#

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

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

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

<#root>

firepower#

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

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

Fehlerbehebung

Eines der häufigsten Probleme bei der Konfiguration der REST-API ist die gelegentliche Erneuerung des Trägertokens. Die Ablaufzeit des Tokens wird in der Antwort für die Authentifizierungsanforderung angegeben. Wenn diese Zeit abläuft, kann ein zusätzliches Aktualisierungstoken für einen längeren Zeitraum verwendet werden. Wenn das Aktualisierungstoken ebenfalls abläuft, muss eine neue Auth-Anforderung gesendet werden, um ein neues Zugriffstoken abzurufen.

Hinweis: Lesen Sie [Wichtige Informationen](#) zu [Debug-Befehlen](#), bevor Sie **Debug**-Befehle verwenden.

Sie können verschiedene Debugstufen festlegen. Standardmäßig wird Ebene 1 verwendet. Wenn Sie die Debug-Ebene ändern, kann die Ausführlichkeit der Debugs zunehmen. Gehen Sie dabei besonders in Produktionsumgebungen vorsichtig vor.

Die folgenden Fehlerbehebungen in der FTD-CLI sind hilfreich bei der Behebung von Problemen mit der LDAP-Attributzuordnung.

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

In diesem Beispiel wurden die nächsten Debugs gesammelt, um die Informationen zu veranschaulichen, die vom AD-Server empfangen wurden, wenn die Testbenutzer vor dem Herstellen der Verbindung eine Verbindung hergestellt haben.

LDAP-Debugging für **Finance-User**:

```
<#root>
```

```
[48] Session Start
[48] New request Session, context 0x00002b0482c2d8e0, reqType = Authentication
[48] Fiber started
[48] Creating LDAP context with uri=ldap://192.168.1.1:389
[48] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[48] supportedLDAPVersion: value = 3
[48] supportedLDAPVersion: value = 2
[48] LDAP server192.168.1.1 is Active directory
[48] Binding as Administrator@cisco.com
[48] Performing Simple authentication for Administrator@example.com to192.168.1.1
[48] LDAP Search:
      Base DN = [dc=cisco, dc=com]
      Filter  = [sAMAccountName=Finance-User]
      Scope   = [SUBTREE]
[48] User DN = [CN=Finance-User,OU=Finance,OU=VPN,DC=cisco,DC=com]
[48] Talking to Active Directory server 192.168.1.1
[48] Reading password policy for Finance-User, dn:CN=Finance-User,OU=Finance,OU=VPN,DC=cisco,DC=com
[48] Read bad password count 0
[48] Binding as Finance-User
[48] Performing Simple authentication for Finance-User to 192.168.1.1
[48] Processing LDAP response for user Finance-User
[48] Message (Finance-User):
[48]
```

Authentication successful for Finance-User to 192.168.1.1

```
[48] Retrieved User Attributes:
[48]   objectClass: value = top
[48]   objectClass: value = person
[48]   objectClass: value = organizationalPerson
[48]   objectClass: value = user
[48]   cn: value = Finance-User
[48]   givenName: value = Finance-User
[48]   distinguishedName: value = CN=Finance-User,OU=Finance,OU=VPN,DC=cisco,DC=com
[48]   instanceType: value = 4
[48]   whenCreated: value = 20191011094454.0Z
[48]   whenChanged: value = 20191012080802.0Z
[48]   displayName: value = Finance-User
[48]   uSNCreated: value = 16036
[48]
```

```

memberOf: value = CN=Finance-Group,CN=Users,DC=cisco,DC=com
[48]
mapped to Group-Policy: value = Finance-Group-Policy
[48]
mapped to LDAP-Class: value = Finance-Group-Policy
[48]   memberOf: value = CN=Users,CN=Builtin,DC=cisco,DC=com
[48]         mapped to Group-Policy: value = CN=Users,CN=Builtin,DC=cisco,DC=com
[48]         mapped to LDAP-Class: value = CN=Users,CN=Builtin,DC=cisco,DC=com
[48]   uSNChanged: value = 16178
[48]   name: value = Finance-User
[48]   objectGUID: value = .J.2...N...X.0Q
[48]   userAccountControl: value = 512
[48]   badPwdCount: value = 0
[48]   codePage: value = 0
[48]   countryCode: value = 0
[48]   badPasswordTime: value = 0
[48]   lastLogoff: value = 0
[48]   lastLogon: value = 0
[48]   pwdLastSet: value = 132152606948243269
[48]   primaryGroupID: value = 513
[48]   objectSid: value = .....B...a5/ID.dT...
[48]   accountExpires: value = 9223372036854775807
[48]   logonCount: value = 0
[48]   sAMAccountName: value = Finance-User
[48]   sAMAccountType: value = 805306368
[48]   userPrincipalName: value = Finance-User@cisco.com
[48]   objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=cisco,DC=com
[48]   dSCorePropagationData: value = 20191011094757.0Z
[48]   dSCorePropagationData: value = 20191011094614.0Z
[48]   dSCorePropagationData: value = 16010101000000.0Z
[48]   lastLogonTimestamp: value = 132153412825919405
[48] Fiber exit Tx=538 bytes Rx=2720 bytes, status=1
[48] Session End

```

LDAP-Debugging für **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

Zugehörige Informationen

Wenden Sie sich für weitere Unterstützung an das Cisco Technical Assistance Center (TAC). Ein gültiger Supportvertrag ist erforderlich: [Weltweiter Kontakt zum Cisco Support](#).

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.