

Configuración del mapa de atributos LDAP para RAVPN en FTD administrado por FDM

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Flujo de autenticación](#)

[Explicación del Flujo de Mapa de Atributos LDAP](#)

[Configurar](#)

[Pasos de configuración en FDM](#)

[Pasos de Configuración para el Mapa de Atributos LDAP](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe el procedimiento para utilizar un servidor de Protocolo ligero de acceso a directorios (LDAP) para autenticar y autorizar a los usuarios de VPN de acceso remoto (RA VPN), y concederles un acceso a la red diferente en función de su pertenencia al grupo en el servidor LDAP.

Prerequisites

Requirements

- Conocimientos básicos de la configuración de VPN de RA en el administrador de dispositivos de firewall (FDM)
- Conocimiento básico de la configuración del servidor LDAP en FDM
- Conocimientos básicos de REpresentational State Transfer (REST) Application Program Interface (API) y FDM Rest API Explorer
- FDM administra Cisco FTD versión 6.5.0 o posterior

Componentes Utilizados

Se utilizaron las siguientes versiones de hardware y software de las aplicaciones/dispositivos:

- Cisco FTD versión 6.5.0, compilación 115
- Cisco AnyConnect versión 4.10
- Servidor de Microsoft Active Directory (AD)
- Postman o cualquier otra herramienta de desarrollo de API

Nota: Cisco no proporciona compatibilidad con la configuración de Microsoft AD Server y la herramienta Postmal.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de

laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Flujo de autenticación



Explicación del Flujo de Mapa de Atributos LDAP

1. El usuario inicia una conexión VPN de acceso remoto al FTD y proporciona un nombre de usuario y una contraseña para su cuenta de Active Directory (AD).
2. El FTD envía una solicitud LDAP al servidor AD a través del puerto 389 o 636 (LDAP sobre SSL)
3. El AD responde al FTD con todos los atributos asociados con el usuario.
4. El FTD hace coincidir los valores de atributo recibidos con el mapa de atributo LDAP creado en el FTD. Este es el proceso de autorización.
5. A continuación, el usuario se conecta y hereda la configuración de la directiva de grupo que coincide con el atributo **memberOf** en el mapa de atributos LDAP.

A los efectos de este documento, la autorización de usuarios de AnyConnect se realiza mediante el atributo **memberOf** LDAP.

- El atributo **memberOf** del servidor LDAP para cada usuario se asigna a una entidad **ldapValue** en el FTD. Si el usuario pertenece al grupo de AD coincidente, el usuario hereda la directiva de grupo asociada a **ldapValue**.
- Si el valor del atributo **memberOf** para un usuario no coincide con ninguna de las entidades **ldapValue** del FTD, se hereda la directiva de grupo predeterminada para el perfil de conexión seleccionado. En este ejemplo, la política de grupo **NOACCESS** se hereda a .

Configurar

El mapa de atributos LDAP para FTD administrado por FDM se configura con la API REST.

Pasos de configuración en FDM

Paso 1. Verifique que el dispositivo esté registrado en **Smart Licensing**.



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

â€f

Paso 2. Verifique que las **licencias de AnyConnect** est n habilitadas en FDM.

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

Device Summary
Smart License

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

SUBSCRIPTION LICENSES INCLUDED

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

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

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

RA VPN License Type PLUS DISABLE
Enabled
Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager does not support any of the advanced features covered by the Apex license.
Includes: RA-VPN

PERPETUAL LICENSES INCLUDED

Base License ENABLED ALWAYS
Enabled
This perpetual license is included with the purchase of the system. You must have this license to configure and use the device. It covers all features not covered by subscription licenses.
Includes: Base Firewall Capabilities, Application Visibility and Control

â€f

Paso 3. Verifique que las funciones controladas por exportaci3n est3n habilitadas en el token.

Device Summary
Smart License



CONNECTED
SUFFICIENT LICENSE

Assigned V
Export-cont
Go to Cisco

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

SUBSCRIPTION LICENSES INCLUDED

Threat

 Enabled

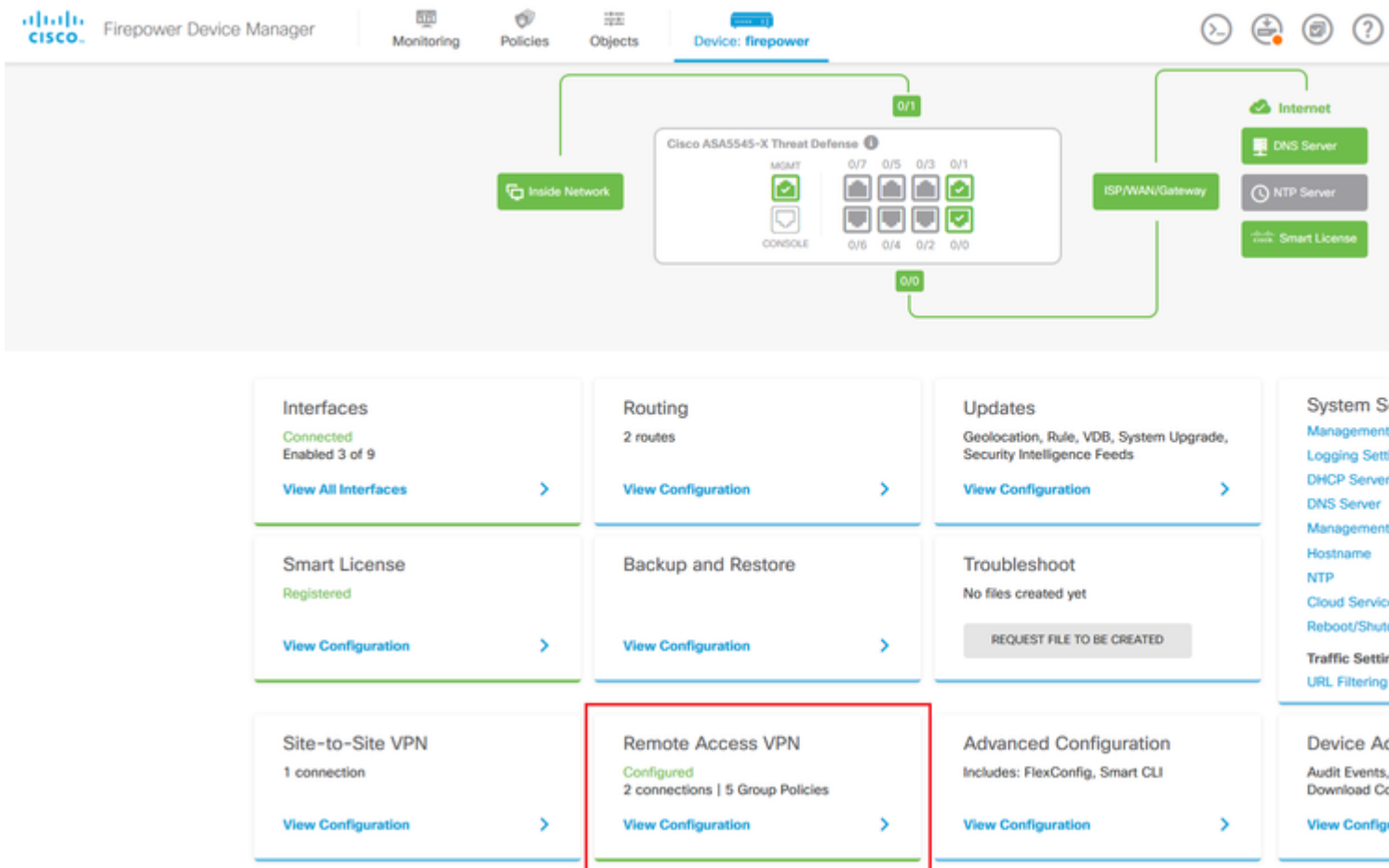
This License allows you to perform intrusion detection and prevention. You must have this license to apply intrusion policies in access rules. You also need this license to apply file policies that control files based on file type.

Includes:  Intrusion Policy

Nota: Este documento asume que RA VPN ya está configurado. Consulte el siguiente documento para obtener más información sobre [Cómo configurar RAVPN en FTD administrado por FDM](#).

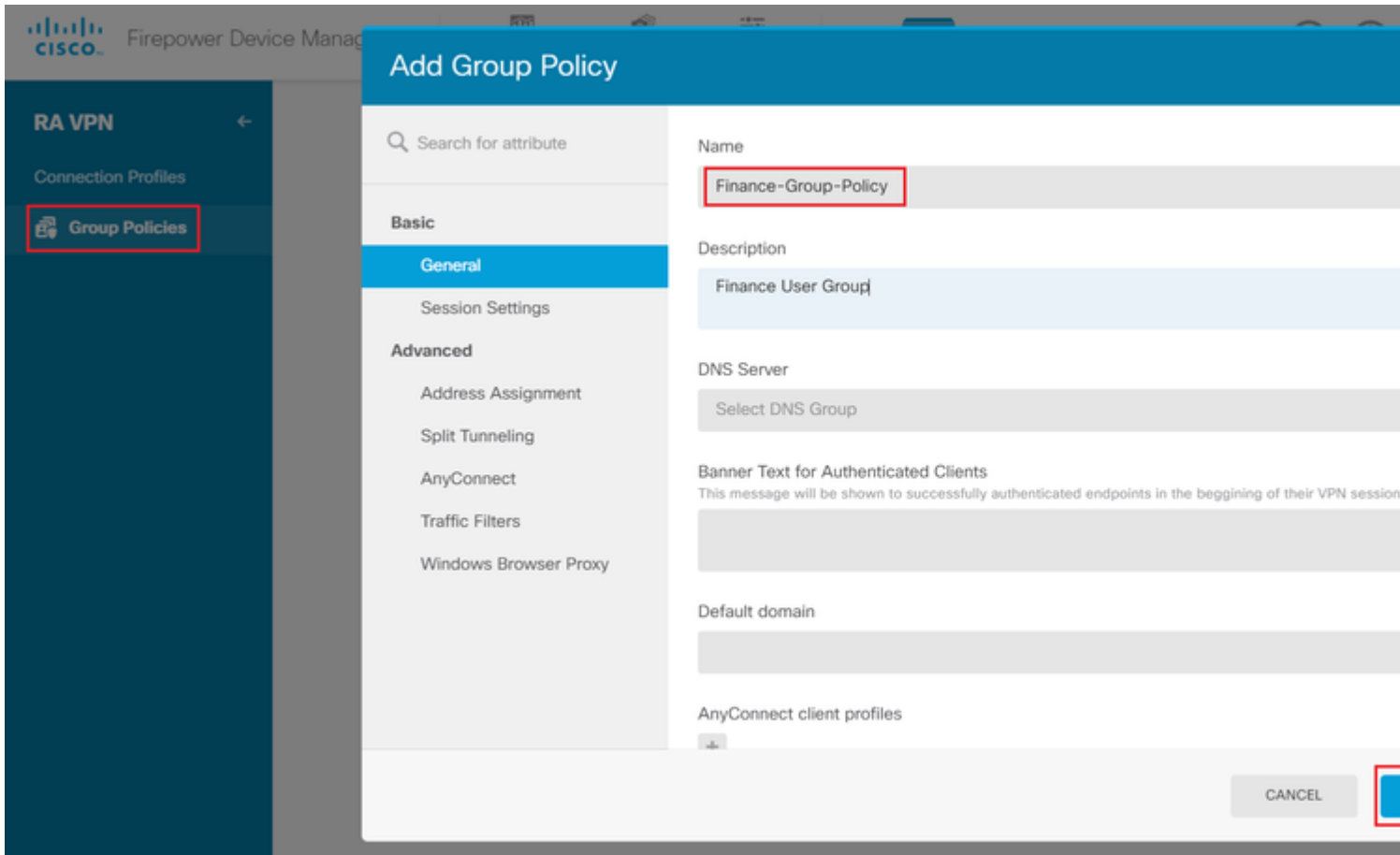
â€f

Paso 4. Vaya a **Remote Access VPN > Group Policies** .



â€f

Paso 5. Vaya a **Políticas de grupo**. Haga clic en '+' para configurar las distintas políticas de grupo para cada grupo de AD. En este ejemplo, las políticas de grupo **Finance-Group-Policy**, **HR-Group-Policy** y **IT-Group-Policy** se configuran para tener acceso a diferentes subredes.



â€f

La **Política de grupo de finanzas** tiene la siguiente configuración:

```
<#root>
```

```
firepower#
```

```
show run group-policy Finance-Group-Policy
```

```
group-policy Finance-Group-Policy internal
group-policy Finance-Group-Policy attributes
banner value You can access Finance resource
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
ipv6-split-tunnel-policy tunnelall
```

```
split-tunnel-network-list value Finance-Group-Policy|splitAc1
```

```
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
msie-proxy method no-modify
vlan none
address-pools none
```

```
ipv6-address-pools none
webvpn
<output omitted>
```

â€f

De manera similar, **HR-Group-Policy** tiene la siguiente configuración:

```
<#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

Finalmente, **IT-Group-Policy** tiene la siguiente configuración:

```
<#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

Paso 6. Cree una política de grupo **NOACCESS** y navegue hasta **Configuración de sesión** y desmarque la opción **Inicio de sesión simultáneo por usuario**. Esto configura el valor **vpn-simultaneous-logins** en 0.

El valor de **vpn-simultaneous-logins** en la política de grupo cuando se establece en 0 termina la conexión VPN del usuario inmediatamente. Este mecanismo se utiliza para evitar que los usuarios que pertenecen a cualquier grupo de usuarios de AD distinto de los configurados (en este ejemplo, Finanzas, RR. HH. o TI) establezcan conexiones satisfactorias con el FTD y accedan a recursos seguros disponibles únicamente para las cuentas de grupo de usuarios permitidas.

Los usuarios que pertenecen a grupos de usuarios AD correctos coinciden con el mapa de atributos LDAP en el FTD y heredan las políticas de grupo asignadas, mientras que los usuarios que no pertenecen a ninguno de los grupos permitidos heredan la política de grupo predeterminada del perfil de conexión, que en este caso es **NOACCESS**.

â€f

Add Group Policy

🔍 Search for attribute

Basic

General

Session Settings

Advanced

Address Assignment

Split Tunneling

AnyConnect

Traffic Filters

Windows Browser Proxy

Name

NOACCESS

Description

To avoid users not belonging to correct AD group from connecting

DNS Server

Select DNS Group

Banner Text for Authenticated Clients

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

Default domain

AnyConnect client profiles



Edit Group Policy

Search for attribute

Basic

General

Session Settings

Advanced

Address Assignment

Split Tunneling

AnyConnect

Traffic Filters

Windows Browser Proxy

Maximum Connection Time

Unlimited

minutes

1-4473924

Idle Time

30

minutes

1-35791394; (Default: 30)

Connection Time

1

1-30; (Default: 1)

Idle Alert Interval

1

1-30; (Default: 1)

Simultaneous Login per User

1-2147483647; (Default: 3)

â€f

La política de grupo **NOACCESS** tiene la siguiente configuración:

```
<#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

```

Paso 7. Navegue hasta **Perfiles de conexión** y cree un perfil de conexión. En este ejemplo, el nombre del perfil es **Remote-Access-LDAP**. Elija **Primary Identity Source AAA Only** y cree un nuevo tipo de servidor de autenticación **AD**.

The screenshot shows the configuration page for a VPN connection profile in the Cisco Firepower Device Manager. The interface includes a navigation bar at the top with 'Monitoring', 'Policies', 'Objects', and 'Device: firepower'. The main configuration area is titled 'Connection Profile Name' and contains the following fields and options:

- Connection Profile Name:** Remote-Access-LDAP (highlighted with a red box).
- Group Alias (one per line, up to 5):** Remote-Access-LDAP
- Group URL (one per line, up to 5):** (empty field)
- Primary Identity Source:** AAA Only (highlighted with a red box). Other options include Client Certificate Only and AAA and Client Certificate.
- Primary Identity Source for User Authentication:** A dropdown menu showing 'LocalIdentitySource' (selected), 'Special-Identities-Realm', and 'Create new'. A sub-menu for 'Create new' is open, showing 'AD' (highlighted with a red box) and 'RADIUS Server Group'.
- Fallback Local Identity Source:** Please Select Local Identity Source (with a warning icon).

At the bottom of the configuration area, there are 'CANCEL' and 'NEXT' buttons.

Introduzca la información del servidor de AD:

- Nombre de usuario del directorio

- Contraseña del directorio
- DN base
- Dominio principal de AD
- Nombre de host/dirección IP
- Puerto
- Tipo de cifrado

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

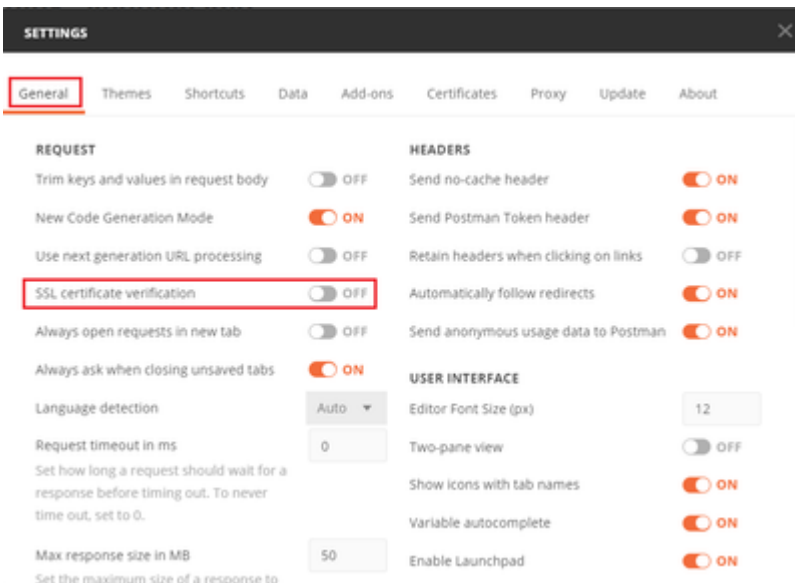
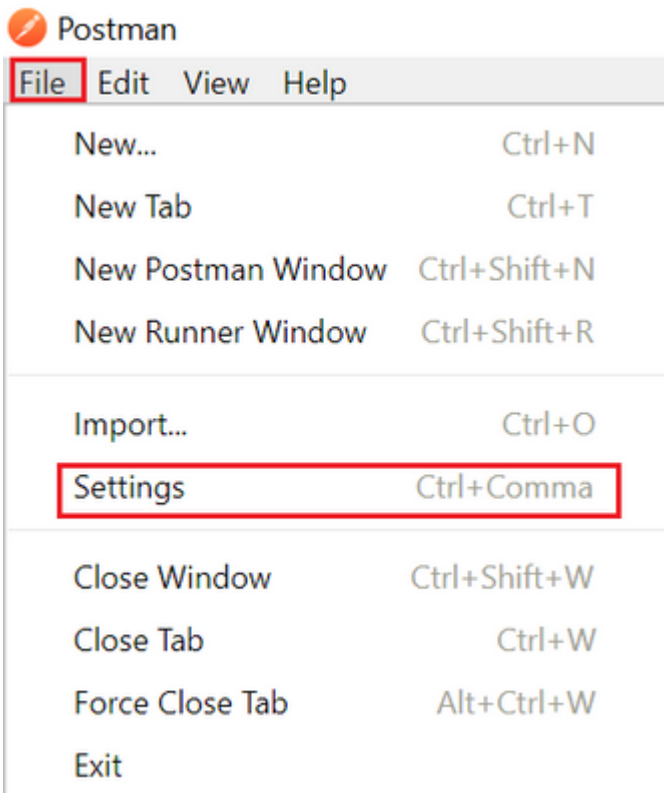
Please select a certificate

TEST

[Add another configuration](#)

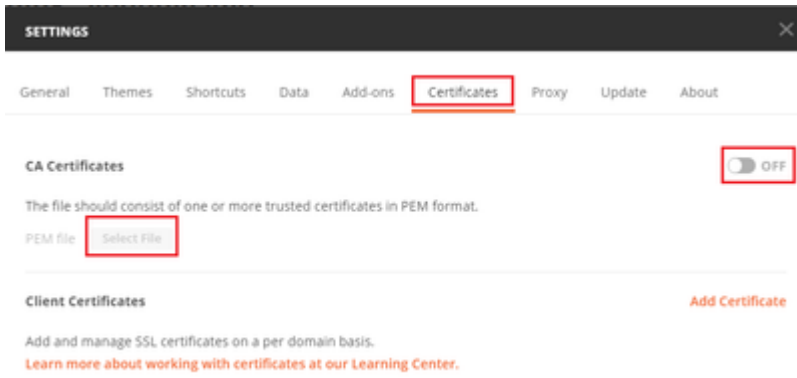
CANCEL

, desactive la verificación del certificado SSL para evitar una falla de intercambio de señales SSL cuando envíe solicitudes de API al FTD. Esto se hace si el FTD utiliza un certificado autofirmado.



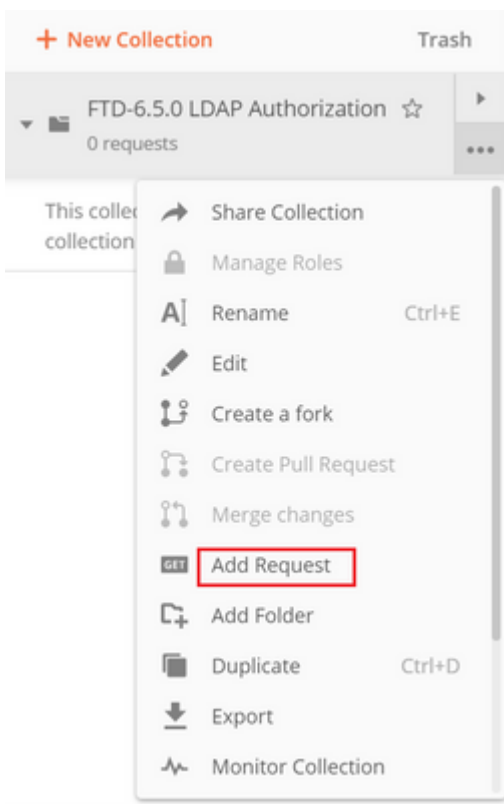
â€f

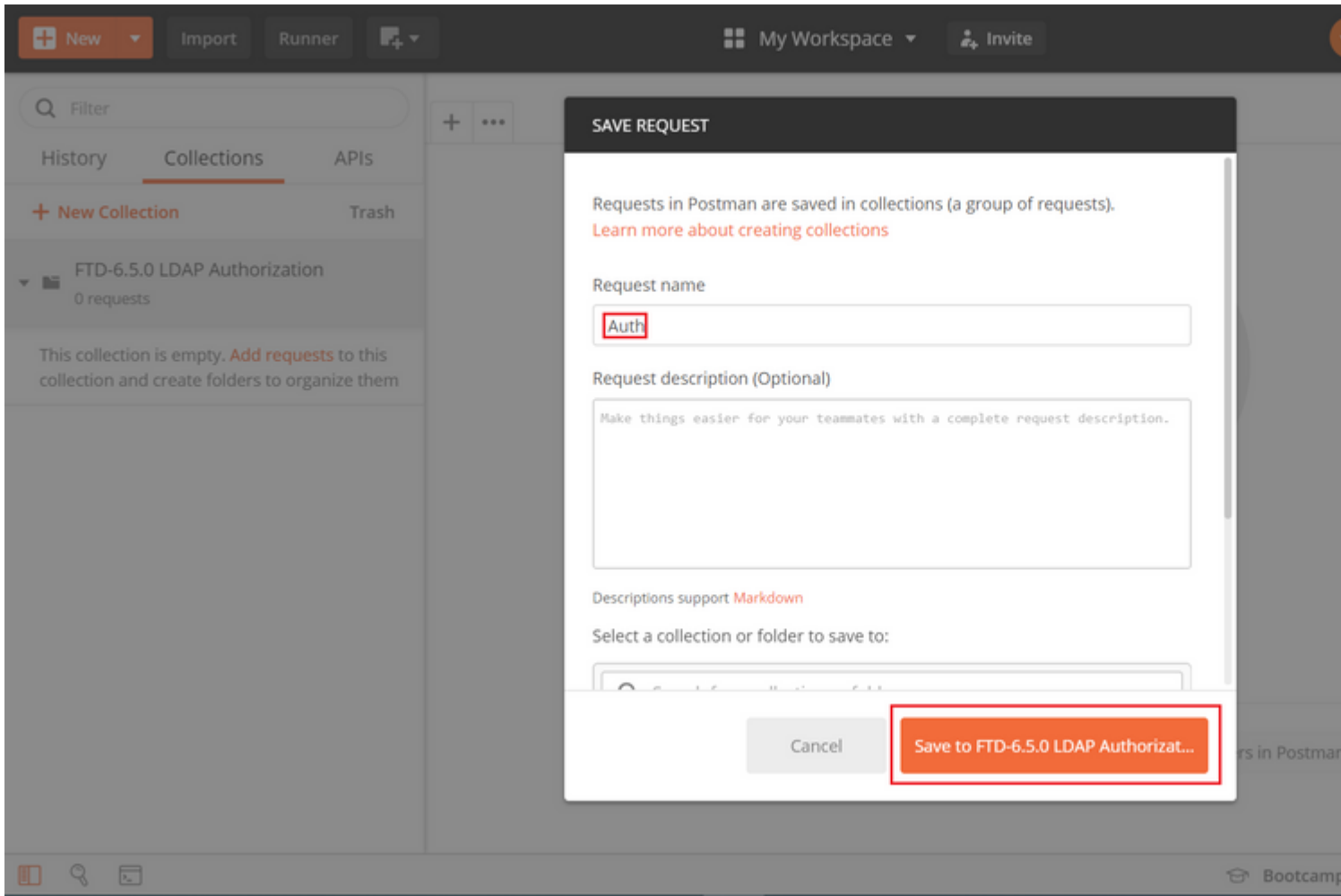
Como alternativa, el certificado utilizado por el FTD se puede agregar como certificado de CA en la sección Certificado de la configuración.



â€f

Paso 4. Agregue una nueva **autenticaci3n** de solicitud POST para crear una solicitud POST de inicio de sesi3n al FTD, para obtener el token para autorizar cualquier solicitud POST/GET.





â€f

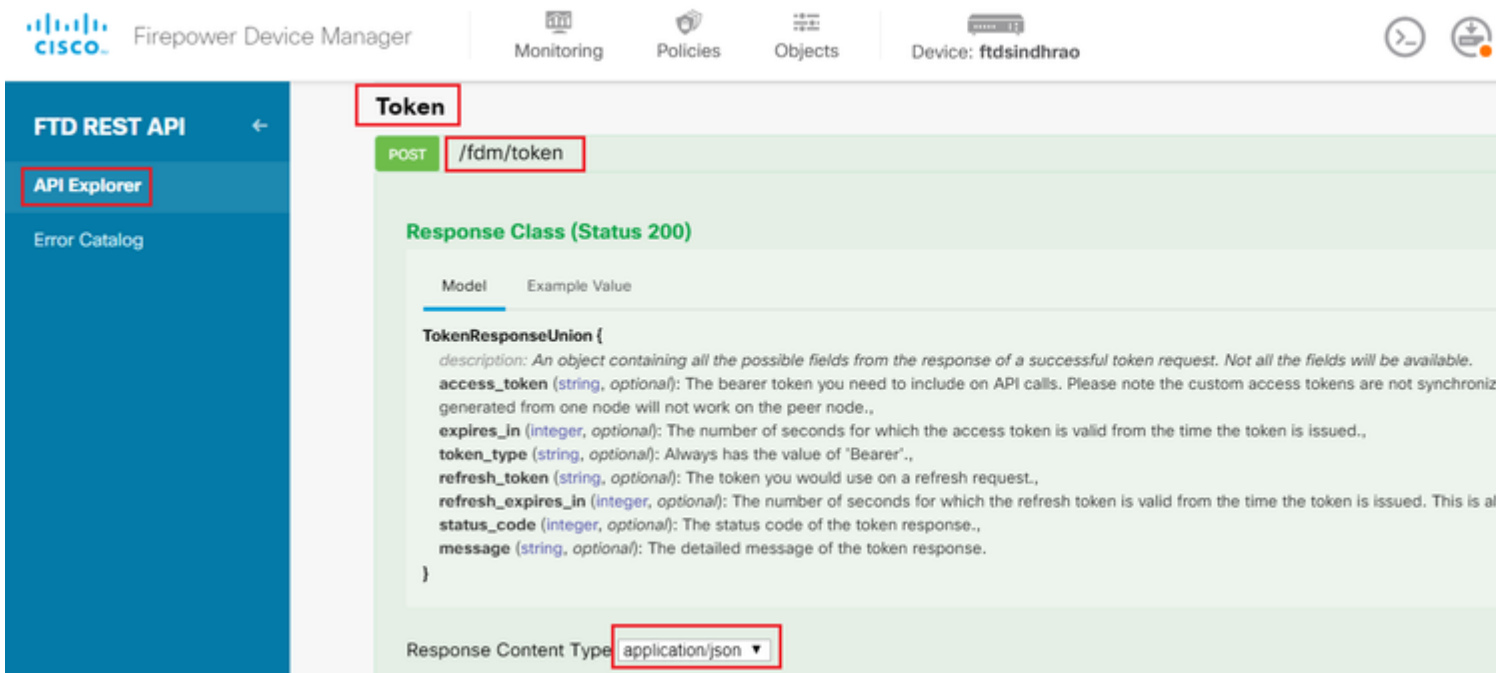
Todas las solicitudes de Postman para esta colecci3n deben contener la siguiente informaci3n:

URL base: <https://<FTD Management IP>/api/fdm/latest/>

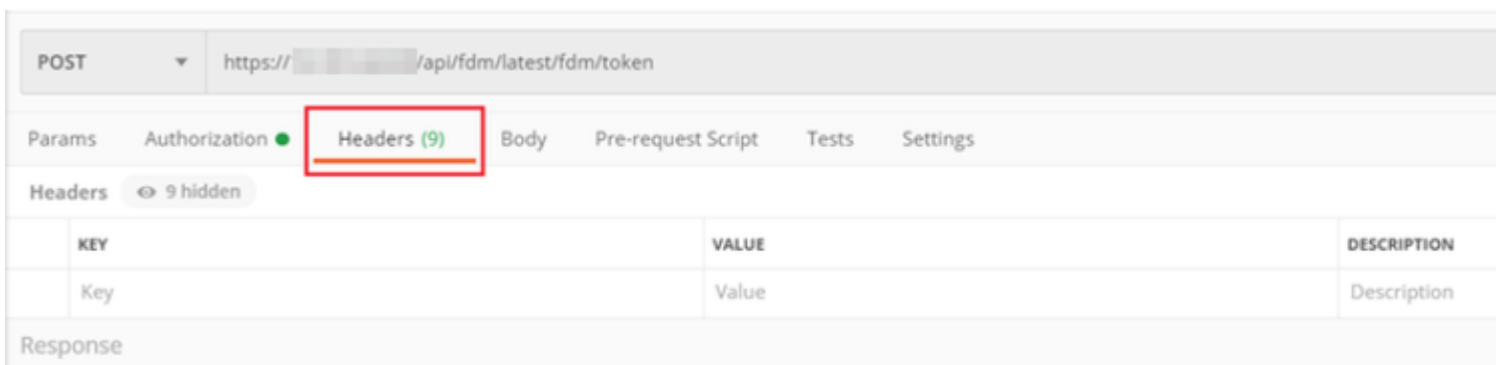
En la URL de solicitud, aãada la URL base con los objetos respectivos que se deben agregar o modificar.

â€f

Aqu3, se crea una solicitud de autenticaci3n para un token, referida desde <https://<FTD Management IP>/api-explorer>. Esto debe comprobarse para otros objetos y deben realizarse los cambios necesarios para ellos.



Navegue hasta **Encabezados** y haga clic en **Administrar ajustes preestablecidos**.



â€f

Cree un nuevo **encabezado** predeterminado-**LDAP** y agregue el siguiente par clave-valor:

Tipo de contenido	Aplicaci3n/JSON
Aceptar	Aplicaci3n/JSON

â€f

MANAGE HEADER PRESETS

Add Header Preset

Header-LDAP

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

Para todas las demás solicitudes, navegue hasta las respectivas pestañas de encabezado y seleccione este valor de encabezado preestablecido: **Header-LDAP** para que las solicitudes de API REST utilicen **json** como tipo de datos principal.

El cuerpo de la solicitud POST para obtener el token debe contener el siguiente elemento:

Tipo	raw - JSON (application/json)
grant_type	contraseña
Nombre de usuario	Nombre de usuario del administrador para iniciar sesión en el FTD
contraseña	Contraseña asociada a la cuenta del usuario administrador

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



```
+ 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": "2nidc13x12vu",
60   "name": "Finance-Group-Policy",
61   "banner": null,
62   "dnsServerGroup": null,
63   "defaultDomainName": null,
64   "simultaneousLoginPerUser": 3,
65   "maxConnectionTimeout": null,
66   "maxConnectionTimeAlertInterval": 1,
67   "vpnIdleTimeout": 30,
68   "vpnIdleTimeoutAlertInterval": 1,
69   "ipv4LocalAddressPool": [],
70   "ipv6LocalAddressPool": [],
71   "dhcpScope": null,
72   "ipv4SplitTunnelSetting": "TUNNEL_SPECIFIED",
73   "ipv6SplitTunnelSetting": "TUNNEL_ALL",
74   "ipv4SplitTunnelNetworks": [
75     {
76       "version": "ogaly1l3hgigo",
77       "name": "acl1",
78       "id": "9ec77902-9836-11ea-ba77-37fd67647b3e",
79       "type": "networkobject"
80     }
81   ],
82   "ipv6SplitTunnelNetworks": [],
83   "splitDNSRequestPolicy": "USE_SPLIT_TUNNEL_SETTING",
84   "splitDNSDomainList": "",
85   "scepForwardingUrl": null,
86   "periodicClientCertAuthenticationInterval": 1,
87   "enableDTLS": false,
88   "enableDTLSCompression": false,
89   "sslCompression": "DISABLED",
90   "enableSSLrekey": false,
91   "rekeyMethod": "NEW_TUNNEL",
92   "rekeyInterval": 4,
93   "ignoreDFBit": false,
94   "bypassUnsupportedProtocol": false,
95   "mtuSize": 1406,
96   "useAlwaysOnVPNSettingInProfile": true,
97   "enableKeepAliveMessages": false,
98   "keepAliveMessageInterval": 20,
99   "enableGatewayOPD": false,
100  "gatewayOPDInterval": 30,
101  "enableClientOPD": false,
102  "clientOPDInterval": 30,
103  "clientProfiles": [],
104  "keepInstallerOnClient": false,
105  "vpnTrafficFilterACL": null,
106  "enableRestrictVPNTOVLAN": false,
107  "restrictVPNTOVLANId": null,
108  "clientFirewallPrivateNetworkRules": null,
109  "clientFirewallPublicNetworkRules": null,
110  "browserProxyType": "NO_PROXY",
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

Paso 6. Agregue una nueva solicitud POST **Create LDAP Attribute Map** para crear el mapa de atributo LDAP. En este documento, se utiliza el modelo **LdapAttributeMapping**. Otros modelos también tienen operaciones y métodos similares para crear el mapa de atributo. Como se mencionó anteriormente en este documento, hay ejemplos de estos modelos disponibles en el explorador API.

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
 }

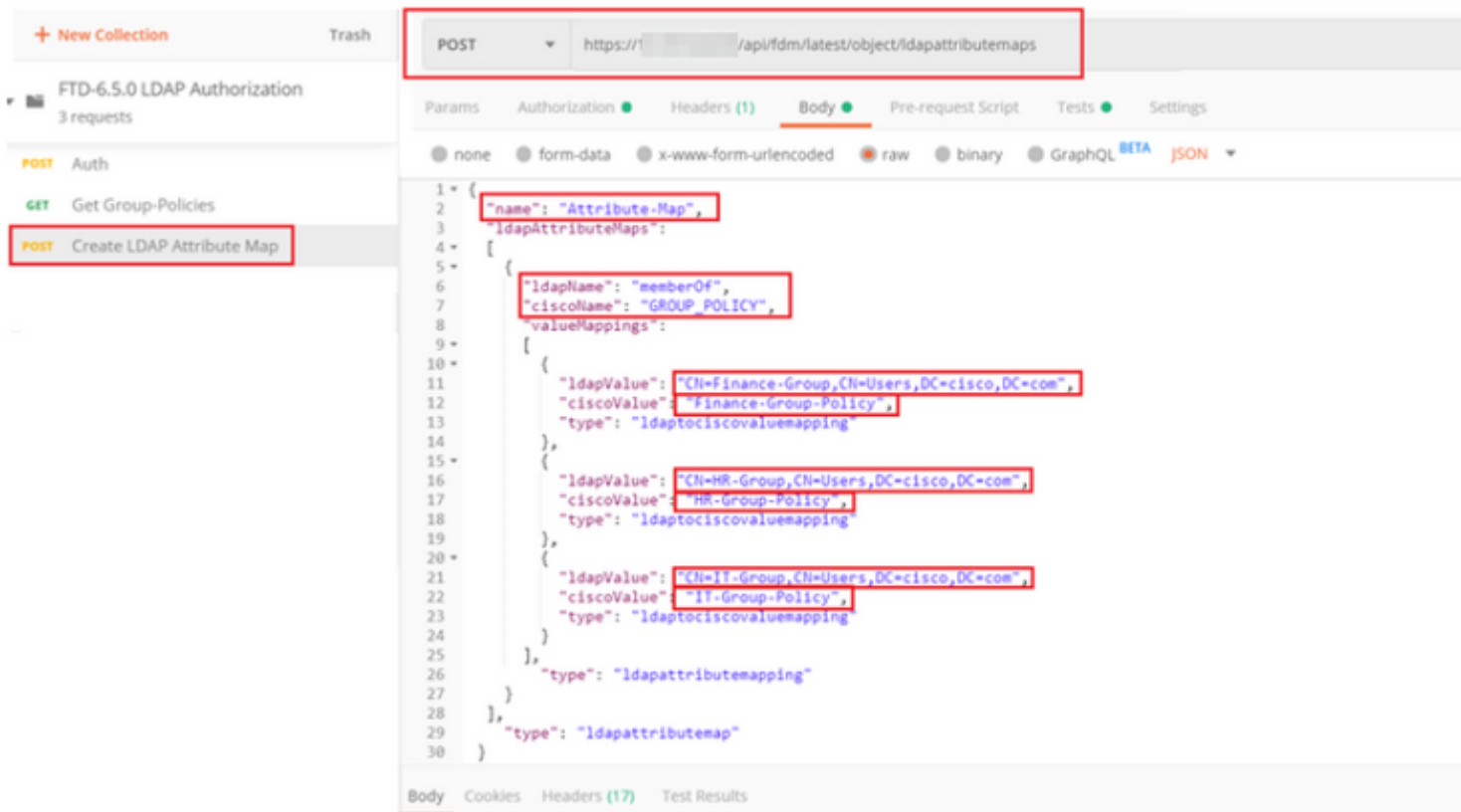
â€š

La URL para publicar el mapa de atributos LDAP es: <https://<IP de administración de FTD>/api/fdm/latest/object/ldapattributeMaps>

El cuerpo de la solicitud POST debe contener lo siguiente:

nombre	Nombre para LDAP Attribute-Map
tipo	ldapattributeMapping
ldapName	memberOf
ciscoName	POLÍTICA_DE_GRUPO
valorLDAP	valor memberOf para el usuario de AD
ciscoValue	Nombre de directiva de grupo para cada grupo de usuarios en FDM

â€š



â€f

El cuerpo de la solicitud POST contiene la informaci3n de mapa de atributo LDAP que mapea una pol3tica de grupo espec3fica a un grupo AD seg3n el valor **memberOf**:

```

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

```

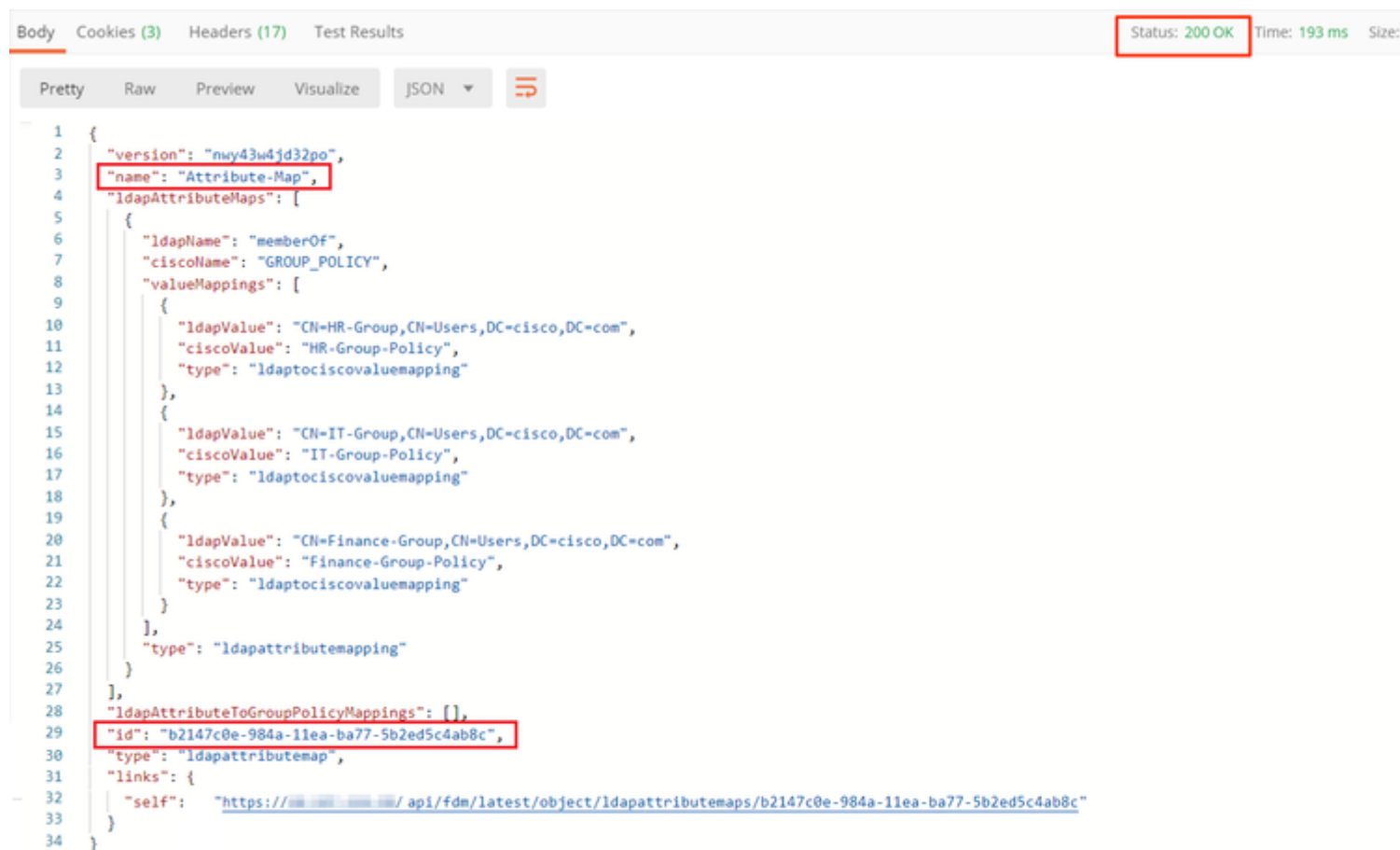


```
],
  "type": "ldapattributemap"
}
```

Nota: El campo **memberOf** se puede recuperar desde el servidor AD con el comando **dsquery** o se puede recuperar desde los debugs LDAP en el FTD. En los logs de debug, busque el campo **memberOf value**:

â€f

La respuesta de esta solicitud POST es similar a la siguiente salida:

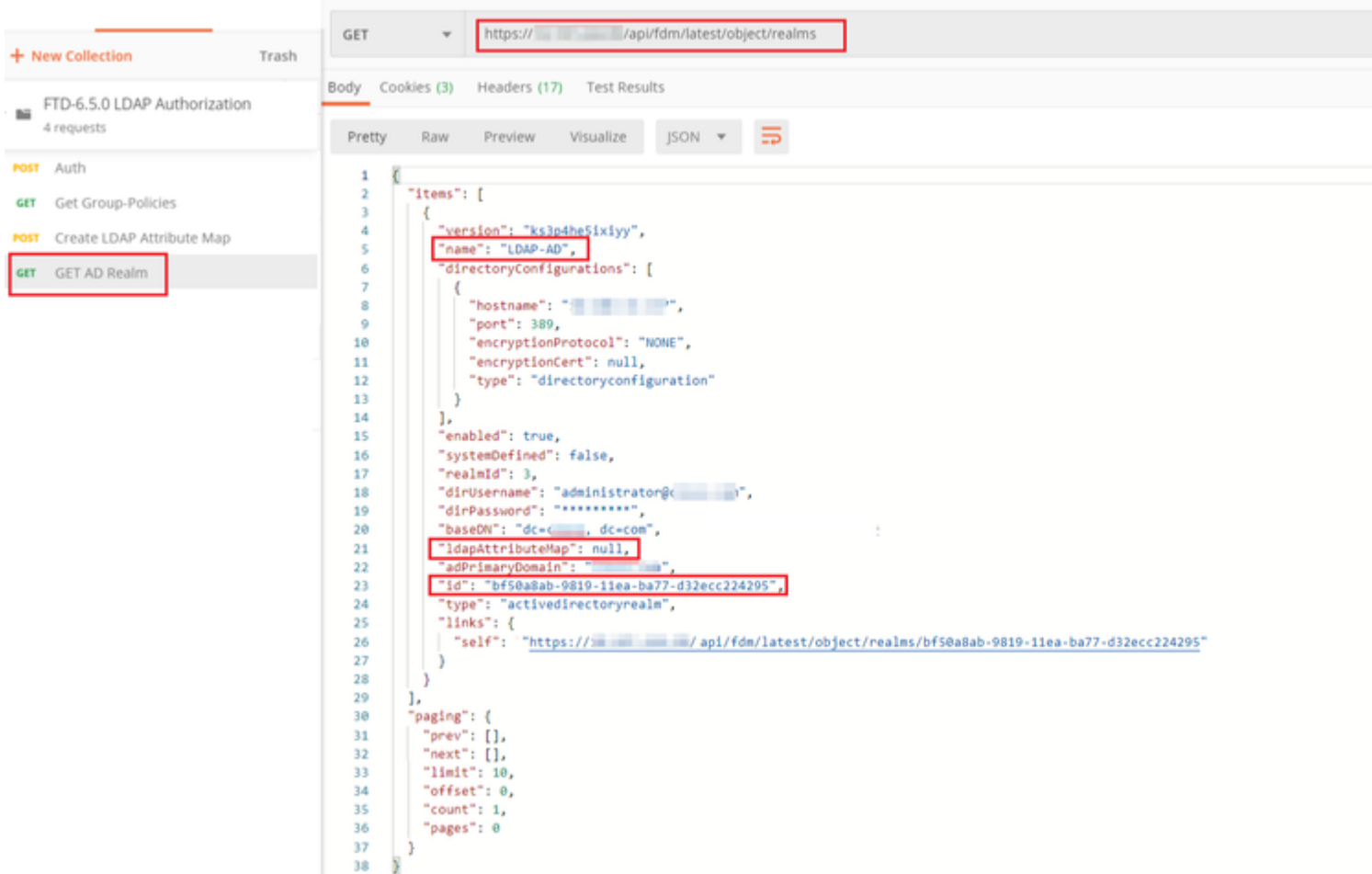


```
Body Cookies (3) Headers (17) Test Results Status: 200 OK Time: 193 ms Size:
Pretty Raw Preview Visualize JSON
1 {
2   "version": "nwy43w4jd32po",
3   "name": "Attribute-Map",
4   "ldapAttributeMaps": [
5     {
6       "ldapName": "memberOf",
7       "ciscoName": "GROUP_POLICY",
8       "valueMappings": [
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 }
```

Paso 7. Agregue una nueva solicitud GET para obtener la configuración de dominio kerberos de AD actual en FDM.

La URL para obtener la configuración de dominio de AD actual es: <https://<IP de administración de FTD>/api/fdm/latest/object/realms>

â€f



â€f

Observe que el valor de la clave **ldapAttributeMap** es **nulo**.

â€f

Paso 8. Cree una nueva solicitud **PUT** para editar el rango de AD. Copie el resultado de la respuesta **GET** del paso anterior y agréguelo al cuerpo de esta nueva solicitud **PUT**. Este paso se puede utilizar para realizar cualquier modificación en la configuración actual de AD Realm, por ejemplo: cambiar la contraseña, la dirección IP o agregar un nuevo valor para cualquier clave como **ldapAttributeMap** en este caso.

Nota: Es importante copiar el contenido de la lista de elementos en lugar de la salida de respuesta GET completa. La URL de solicitud para la solicitud PUT debe anexarse con el id. de elemento del objeto para el que se realizan cambios. En este ejemplo, el valor es: bf50a8ab-9819-11ea-ba77-d32ecc224295

â€f

La URL para editar la configuración actual del rango de AD es: <https://<IP de administración de FTD>/api/fdm/latest/object/realms/<ID de rango>>

El cuerpo de la solicitud PUT debe contener lo siguiente:

versión	versión obtenida de la respuesta a una solicitud GET anterior
id	ID obtenida de la respuesta de una solicitud

	GET anterior
ldapAttributeMap	ldap-id from Response of Create LDAP Attribute Map request

â€f

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

```

1 {
2   "version": "ks3pdhe5ixiyy",
3   "name": "LDAP-AD",
4   "directoryConfigurations": [
5     {
6       "hostname": "<IP Address>",
7       "port": 389,
8       "encryptionProtocol": "NONE",
9       "encryptionCert": null,
10      "type": "directoryconfiguration"
11    }
12  ],
13  "enabled": true,
14  "systemDefined": false,
15  "realmId": 3,
16  "dirUsername": "administrator@...com",
17  "dirPassword": "*****",
18  "baseDN": "dc=..., dc=com",
19  "ldapAttributeMap":
20  {
21    "id": "b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c",
22    "type": "ldapattributemap"
23  },
24  "adPrimaryDomain": "...com",
25  "id": "bf50a8ab-9819-11ea-ba77-d32ecc224295",
26  "type": "activedirectoryrealm",
27  "links": {
28    "self": "https://.../api/fdm/latest/object/realms/bf50a8ab-9819-11ea-ba77-d32ecc224295"
29  }
30 }
31

```

â€f

El cuerpo de la configuración de este ejemplo es:

<#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"

  }
}
```

Verifique que el id. de **LdapAttributeMap** coincida en el Cuerpo de Respuesta para esta solicitud.

```
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€¦

(Opcional) . El mapa de atributo LDAP se puede modificar con solicitudes **PUT**. Cree una nueva solicitud **PUT Edit Attribute-Map** y realice cambios como el nombre del valor Attribute-Map o memberOf. T

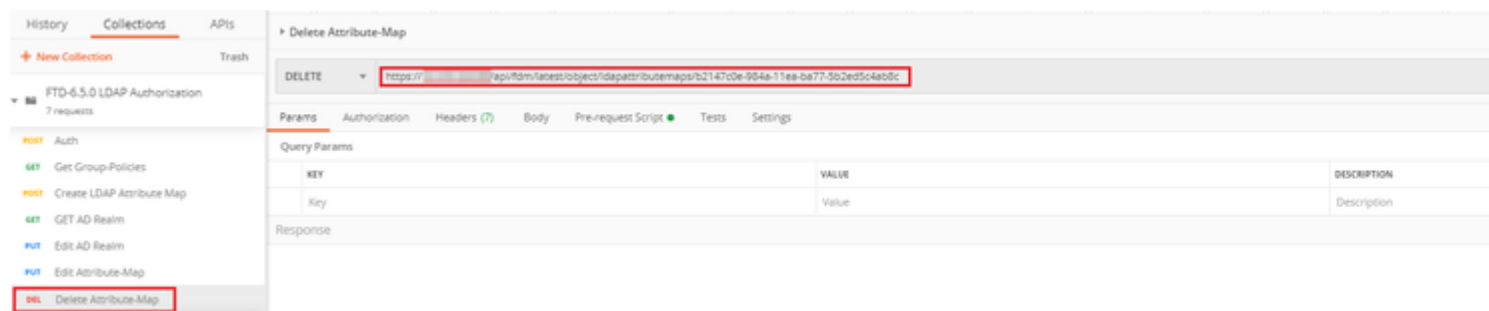
En el siguiente ejemplo, el valor de **ldapvalue** se ha modificado de **CN=Users** a **CN=UserGroup** para los tres grupos.

```
FTD-6.5.0 LDAP Authorization
6 requests
Auth
POST
GET Get Group-Policies
GET Create LDAP Attribute Map
GET GET AD Realm
PUT Edit AD Realm
PUT Edit Attribute-Map

PUT https:// / api/fdm/latest/object/ldapattributemaps/b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c
Params Authorization Headers (11) Body Pre-request Script Tests Settings
none form-data x-www-form-urlencoded raw binary GraphQL JSON
1 {
2   "version": "nwy43w4jd32po",
3   "name": "Attribute-Map",
4   "ldapattributemaps": [
5     {
6       "ldapname": "memberOf",
7       "ciscaname": "GROUP_POLICY",
8       "valuemappings": [
9         {
10          "ldapvalue": "CN=Finance-Group,CN=UserGroup,DC=cisco,DC=com",
11          "ciscovalue": "Finance-Group-Policy",
12          "type": "ldaptociscovaluemapping"
13        },
14        {
15          "ldapvalue": "CN=HR-Group,CN=UserGroup,DC=cisco,DC=com",
16          "ciscovalue": "HR-Group-Policy",
17          "type": "ldaptociscovaluemapping"
18        },
19        {
20          "ldapvalue": "CN=IT-Group,CN=UserGroup,DC=cisco,DC=com",
21          "ciscovalue": "IT-Group-Policy",
22          "type": "ldaptociscovaluemapping"
23        }
24      ]
25    }
26  ],
27  "type": "ldapattributemap"
28 }
29
30 "id": "b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c",
31 "type": "ldapattributemap",
32 "links": {
33   "self": "https://10.197.224.99/api/fdm/latest/object/ldapattributemaps/b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c"
34 }
35 }
```

â€f

(Opcional) . Para eliminar un Attribute-Map LDAP existente, cree una solicitud DELETE **Delete Attribute-Map**. Incluya el **map-id** de la respuesta HTTP anterior y añada con la URL base de la solicitud de eliminación.



Nota: Si el atributo **memberOf** contiene espacios, debe estar codificado en URL para que el servidor web lo analice. De lo contrario, se recibe **una respuesta HTTP de solicitud 400 incorrecta**. Para las cadenas que contienen espacios en blanco, se puede utilizar **"%20"** o **"+"** para evitar este error.

â€f

Paso 9. Vuelva a FDM, seleccione el icono de implementación y haga clic en **Desplegar ahora**.

â€f

Pending Changes

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

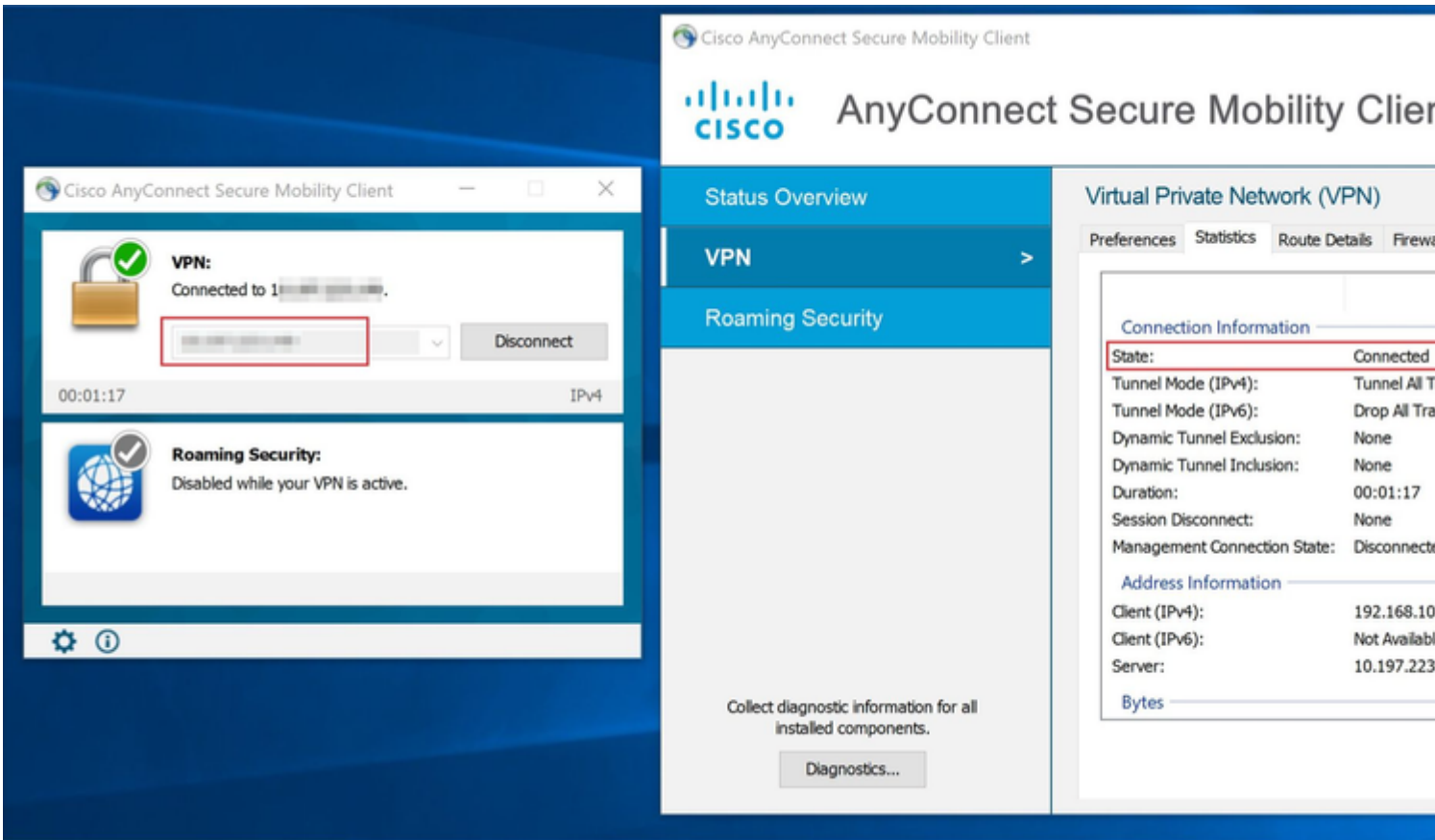
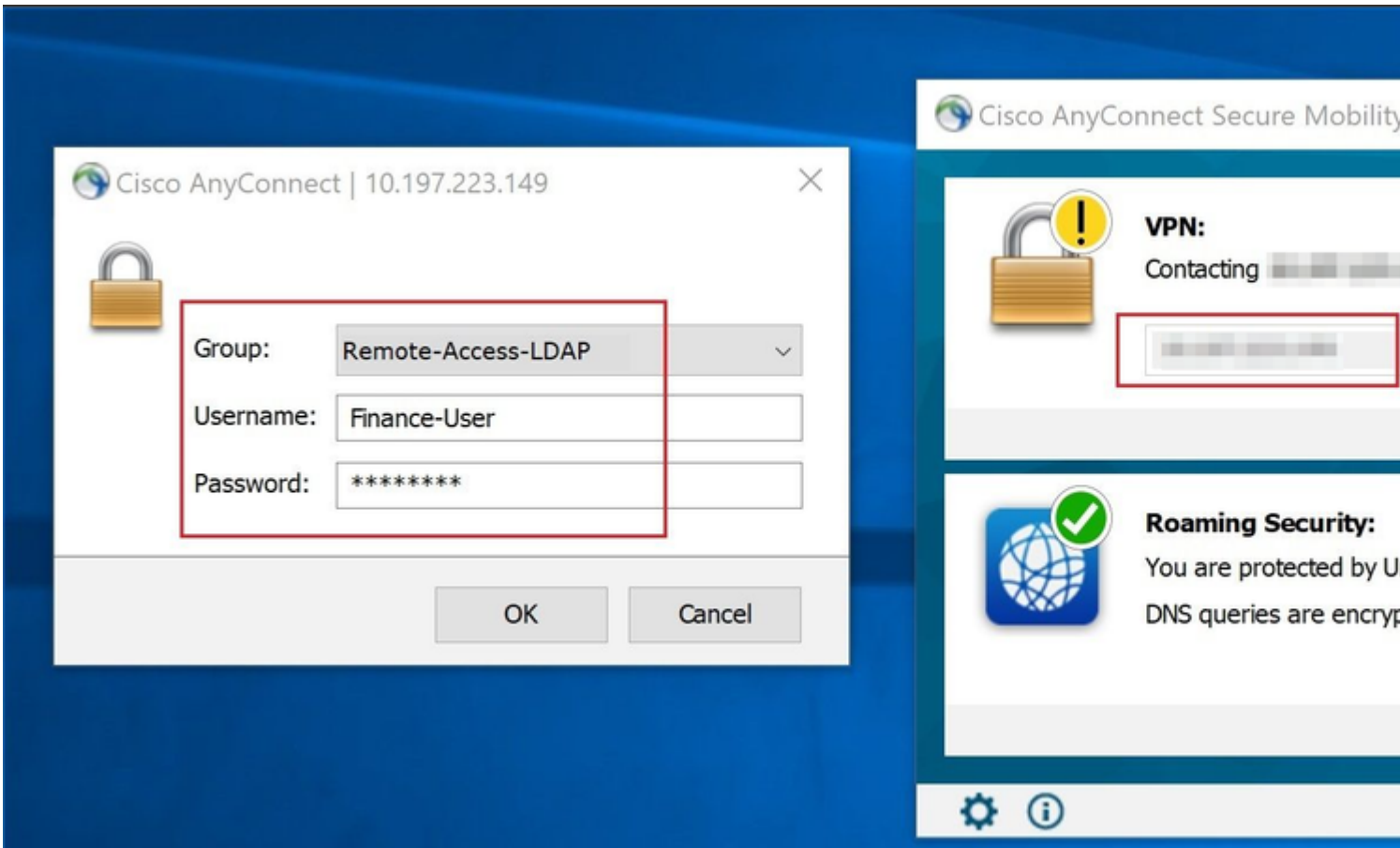
Deployed Version (17 May 2020 07:46 PM)	Pending Version
+ Idapattributemap Added: <i>Attribute-Map</i>	
<pre>- - - - - - - - -</pre>	<pre>ldapAttributeMaps[0].ldapName : ldapAttributeMaps[0].valueMappi ldapAttributeMaps[0].valueMappi ldapAttributeMaps[0].valueMappi ldapAttributeMaps[0].valueMappi ldapAttributeMaps[0].valueMappi 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

Verificación

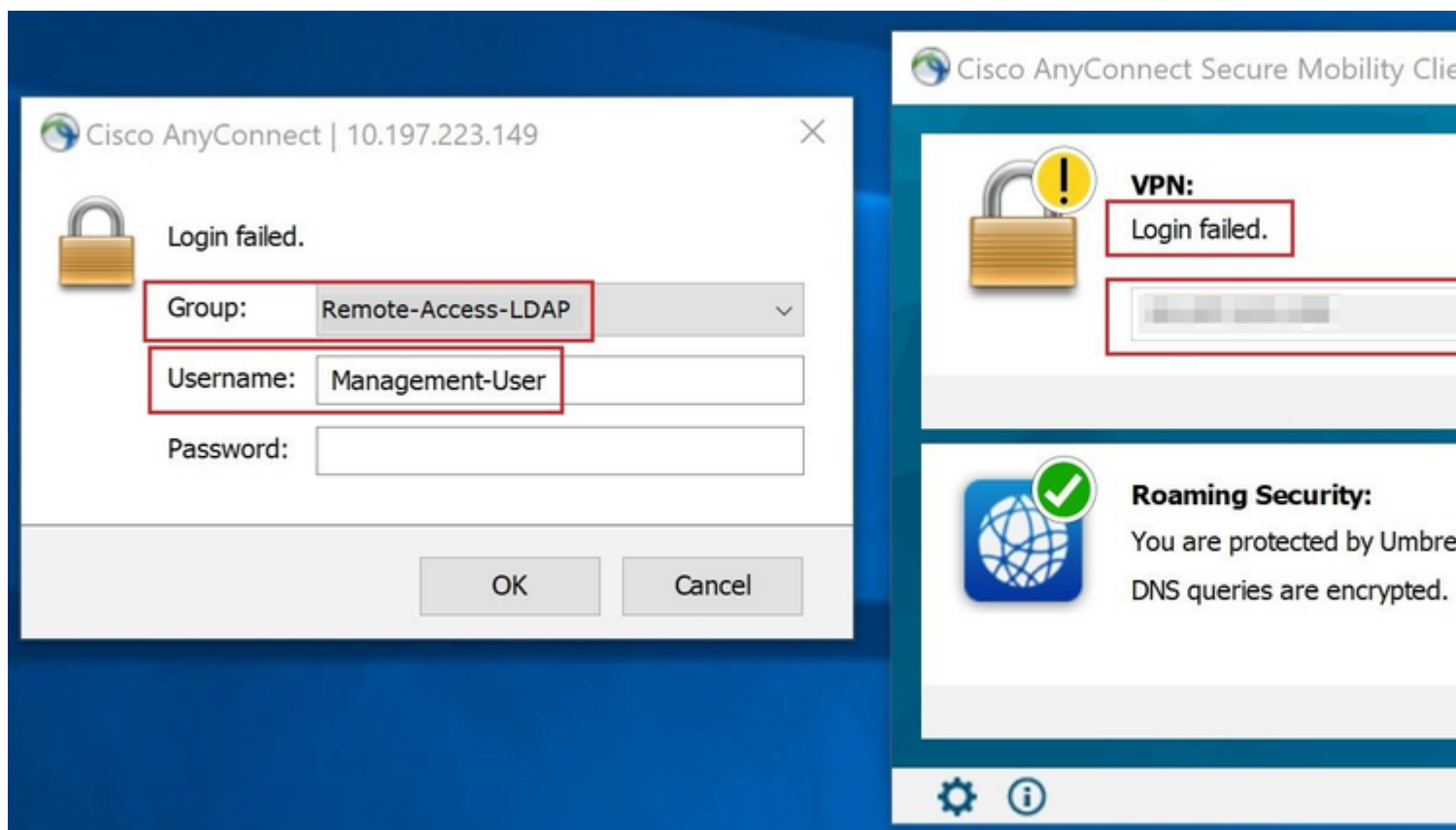
Los cambios de implementación se pueden verificar en la sección **Historial de implementación** de FDM.



â€f

Quando un usuario que pertenece al **Management-Group** en AD intenta conectarse a Connection-Profile

Remote-Access-LDAP, ya que ningún mapa de atributo LDAP devolvió una coincidencia, la política de grupo heredada por este usuario en el FTD es **NOACCESS**, que tiene los inicios de sesión simultáneos de vpn establecidos en el valor 0. Por lo tanto, el intento de inicio de sesión para este usuario falla.



â€f

La configuración se puede verificar con los siguientes comandos show de la CLI de FTD:

```
<#root>
```

```
firepower#
```

```
show vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect
```

```
Username      :
```

```
Finance-User
```

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

```
Finance-Group-Policy
```

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

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

```
<#root>
```

```
firepower#
```

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

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

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

```
<#root>
```

```
firepower#
```

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

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

Troubleshoot

Uno de los problemas más comunes con la configuración de la API REST es renovar el token portador de vez en cuando. El tiempo de vencimiento del token se indica en la Respuesta para la solicitud de autenticación. Si vence este tiempo, se puede utilizar un token de actualización adicional durante un tiempo más largo. Después de que el token de actualización también caduque, se debe enviar una nueva solicitud de autenticación para recuperar un nuevo token de acceso.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.

Puede establecer varios niveles de depuración. De forma predeterminada, se utiliza el nivel 1. Si cambia el nivel de depuración, puede aumentar la verbosidad de los depuradores. Hágalo con precaución, especialmente en entornos de producción.

Las siguientes depuraciones en la CLI de FTD serían útiles para solucionar problemas relacionados con el mapa de atributos LDAP

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

En este ejemplo, se recopilaron las siguientes depuraciones para mostrar la información recibida del servidor AD cuando los usuarios de prueba mencionados antes se conectaron.

Depuraciones LDAP para **Finance-User**:

```
<#root>
```

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

Authentication successful for Finance-User to 192.168.1.1

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

memberOf: value = CN=Finance-Group,CN=Users,DC=cisco,DC=com

[48]

mapped to Group-Policy: value = Finance-Group-Policy

[48]

mapped to LDAP-Class: value = Finance-Group-Policy

[48] memberOf: value = CN=Users,CN=Builtin,DC=cisco,DC=com
[48] mapped to Group-Policy: value = CN=Users,CN=Builtin,DC=cisco,DC=com
[48] mapped to LDAP-Class: value = CN=Users,CN=Builtin,DC=cisco,DC=com
[48] uSNChanged: value = 16178
[48] name: value = Finance-User
[48] objectGUID: value = .J.2...N...X.0Q
[48] userAccountControl: value = 512
[48] badPwdCount: value = 0
[48] codePage: value = 0
[48] countryCode: value = 0
[48] badPasswordTime: value = 0
[48] lastLogoff: value = 0
[48] lastLogon: value = 0
[48] pwdLastSet: value = 132152606948243269
[48] primaryGroupID: value = 513
[48] objectSid: value =B...a5/ID.dT...
[48] accountExpires: value = 9223372036854775807
[48] logonCount: value = 0
[48] sAMAccountName: value = Finance-User
[48] sAMAccountType: value = 805306368
[48] userPrincipalName: value = Finance-User@cisco.com
[48] objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=cisco,DC=com
[48] dSCorePropagationData: value = 201910111094757.0Z
[48] dSCorePropagationData: value = 201910111094614.0Z
[48] dSCorePropagationData: value = 16010101000000.0Z
[48] lastLogonTimestamp: value = 132153412825919405
[48] Fiber exit Tx=538 bytes Rx=2720 bytes, status=1
[48] Session End

Depuraciones LDAP para **Management-User**:

<#root>

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

[51] Performing Simple authentication for Management-User to 192.168.1.1
[51] Processing LDAP response for user Management-User
[51] Message (Management-User):
[51]

Authentication successful for Management-User to 192.168.1.1

[51] Retrieved User Attributes:
[51] objectClass: value = top
[51] objectClass: value = person
[51] objectClass: value = organizationalPerson
[51] objectClass: value = user
[51] cn: value = Management-User
[51] givenName: value = Management-User
[51] distinguishedName: value = CN=Management-User,OU=Management,OU=VPN,DC=cisco,DC=com
[51] instanceType: value = 4
[51] whenCreated: value = 20191011095036.0Z
[51] whenChanged: value = 20191011095056.0Z
[51] displayName: value = Management-User
[51] uSNCreated: value = 16068
[51]

memberOf: value = CN=Management-Group,CN=Users,DC=cisco,DC=com

[51]

mapped to Group-Policy: value = CN=Management-Group,CN=Users,DC=cisco,DC=com

[51]

mapped to LDAP-Class: value = CN=Management-Group,CN=Users,DC=cisco,DC=com

[51] memberOf: value = CN=Users,CN=Builtin,DC=cisco,DC=com
[51] mapped to Group-Policy: value = CN=Users,CN=Builtin,DC=cisco,DC=com
[51] mapped to LDAP-Class: value = CN=Users,CN=Builtin,DC=cisco,DC=com
[51] uSNChanged: value = 16076
[51] name: value = Management-User
[51] objectGUID: value = i._(.E.O....Gig
[51] userAccountControl: value = 512
[51] badPwdCount: value = 0
[51] codePage: value = 0
[51] countryCode: value = 0
[51] badPasswordTime: value = 0
[51] lastLogoff: value = 0
[51] lastLogon: value = 0
[51] pwdLastSet: value = 132152610365026101
[51] primaryGroupID: value = 513
[51] objectSid: value =B...a5/ID.dW...
[51] accountExpires: value = 9223372036854775807
[51] logonCount: value = 0
[51] sAMAccountName: value = Management-User
[51] sAMAccountType: value = 805306368
[51] userPrincipalName: value = Management-User@cisco.com
[51] objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=cisco,DC=com
[51] dSCorePropagationData: value = 20191011095056.0Z
[51] dSCorePropagationData: value = 16010101000000.0Z
[51] Fiber exit Tx=553 bytes Rx=2688 bytes, status=1
[51] Session End

Información Relacionada

Para obtener asistencia adicional, póngase en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC). Se necesita un contrato de soporte válido: [Contactos de soporte a nivel mundial de Cisco](#).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).