

Configura mappa attributi LDAP per RAVPN su FTD Gestito da FDM

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Flusso di autenticazione](#)

[Spiegazione del flusso della mappa degli attributi LDAP](#)

[Configurazione](#)

[Procedura di configurazione in FDM](#)

[Procedura di configurazione per la mappa degli attributi LDAP](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritta la procedura per utilizzare un server LDAP (Lightweight Directory Access Protocol) per autenticare e autorizzare gli utenti della VPN ad accesso remoto (RA VPN) e concedere loro un accesso di rete diverso in base all'appartenenza ai gruppi sul server LDAP.

Prerequisiti

Requisiti


- Conoscenze base della configurazione di RMA VPN in Gestione dispositivi firewall
- Conoscenze base della configurazione del server LDAP in FDM
- Conoscenze base di REpresentational State Transfer (REST) Application Program Interface (API) e FDM Rest API Explorer
- Cisco FTD versione 6.5.0 o successiva gestito da FDM

Componenti usati

Sono state utilizzate le seguenti versioni hardware e software di applicazioni/dispositivi:

- Cisco FTD versione 6.5.0, build 115
- Cisco AnyConnect versione 4.10
- Server Microsoft Active Directory (AD)

- Postman o qualsiasi altro strumento di sviluppo API

 Nota: il supporto per la configurazione di Microsoft AD Server and Postmal Tool non è fornito da Cisco.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Flusso di autenticazione



Spiegazione del flusso della mappa degli attributi LDAP

1. L'utente avvia una connessione VPN di accesso remoto all'FTD e fornisce un nome utente e una password per l'account di Active Directory (AD).
2. L'FTD invia una richiesta LDAP al server AD tramite la porta 389 o 636 (LDAP su SSL)
3. AD risponde all'FTD con tutti gli attributi associati all'utente.
4. L'FTD corrisponde ai valori degli attributi ricevuti con la mappa degli attributi LDAP creata sull'FTD. Processo di autorizzazione.
5. L'utente quindi si connette ed eredita le impostazioni dai Criteri di gruppo corrispondenti all'attributo memberOf nella mappa degli attributi LDAP.

Ai fini del presente documento, l'autorizzazione degli utenti AnyConnect viene effettuata usando l'attributo LDAP memberOf.

- L'attributo memberOf del server LDAP per ciascun utente è mappato a un'entità ldapValue sull'FTD. Se l'utente appartiene al gruppo AD corrispondente, i Criteri di gruppo associati a tale valore ldapValue vengono ereditati dall'utente.
- Se il valore dell'attributo memberOf di un utente non corrisponde a nessuna delle entità ldapValue nell'FTD, viene ereditato il criterio di gruppo predefinito per il profilo di connessione selezionato. In questo esempio, i Criteri di gruppo NOACCESS vengono ereditati da .

Configurazione

La mappa degli attributi LDAP per FTD gestita da FDM è configurata con l'API REST.

Procedura di configurazione in FDM

Passaggio 1. Verificare che il dispositivo sia registrato in Smart Licensing.

The screenshot displays the Cisco Firepower Device Manager (FDM) interface for a Cisco ASA5545-X Threat Defense device. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: firepower'. The main content area shows a network diagram with 'Inside Network', 'ISP/WAN/Gateway', and 'Internet' components. Below the diagram is a grid of configuration sections:

- Interfaces:** Connected, Enabled 3 of 9. [View All Interfaces](#)
- Smart License:** Registered. [View Configuration](#) (highlighted with a red border)
- Routing:** 2 routes. [View Configuration](#)
- Updates:** Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds. [View Configuration](#)
- Backup and Restore:** [View Configuration](#)
- Troubleshoot:** No files created yet. [REQUEST FILE TO BE CREATED](#)
- System Settings:** Management Access, Logging Settings, DHCP Server, DNS Server, Management Interface, Hostname, NTP, Cloud Services, Reboot/Shutdown, Traffic Settings, URL Filtering Preferences.
- Site-to-Site VPN:** 1 connection. [View Configuration](#)
- Remote Access VPN:** Configured, 2 connections | 5 Group Policies. [View Configuration](#)
- Advanced Configuration:** Includes: FlexConfig, Smart CLI. [View Configuration](#)
- Device Administration:** Audit Events, Deployment History, Download Configuration. [View Configuration](#)

Passaggio 2. Verificare che le licenze AnyConnect siano abilitate su 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

Passaggio 3. Verificare che le funzionalità controllate per l'esportazione siano abilitate nel token.



Device Summary Smart License

CONNECTED
SUFFICIENT LICENSE

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

Assigned Virtual Account: ██████
Export-controlled features: Enabled
Go to [Cisco Smart Software Manager](#).

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

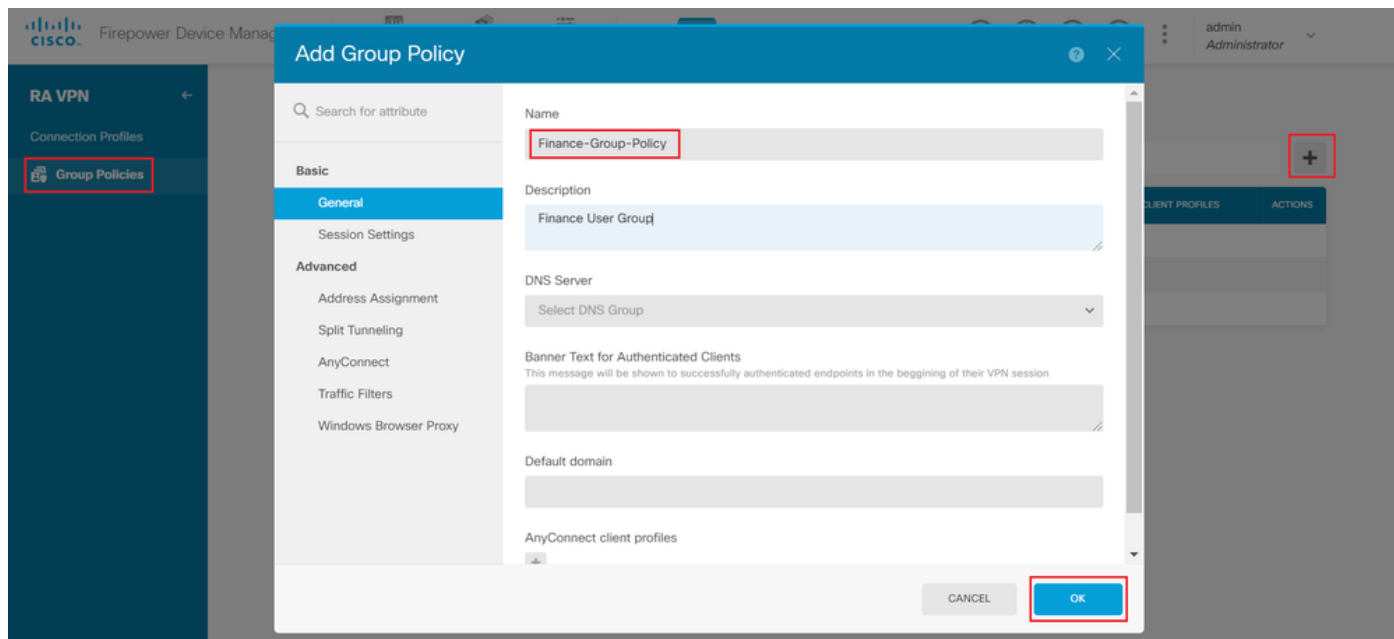
Nota: in questo documento si presume che RSA VPN sia già configurato. Fare riferimento al documento seguente per ulteriori informazioni su [come configurare RAVPN su FTD gestito da FDM](#).

Passaggio 4. Passare a VPN accesso remoto > Criteri di gruppo.

The screenshot shows the Firepower Device Manager interface for a device named 'firepower'. At the top, there are navigation tabs for Monitoring, Policies, Objects, and Device: firepower. Below the navigation, there is a network diagram showing connections between an Inside Network, a Cisco ASA5545-X Threat Defense device, and an ISP/WAN/Gateway. The Threat Defense device has several status indicators for MGMT and CONSOLE ports. To the right of the diagram, there are icons for Internet, DNS Server, NTP Server, and Smart License. Below the diagram, there is a grid of configuration options:

Interfaces Connected Enabled 3 of 9 View All Interfaces	Routing 2 routes View Configuration	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Server DNS Server Management Interface Hostname NTP Cloud Services Reboot/Shutdown Traffic Settings URL Filtering Preferences
Smart License Registered View Configuration	Backup and Restore View Configuration	Troubleshoot No files created yet REQUEST FILE TO BE CREATED	Device Administration Audit Events, Deployment History, Download Configuration View Configuration
Site-to-Site VPN 1 connection View Configuration	Remote Access VPN Configured 2 connections 5 Group Policies View Configuration	Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration	

Passaggio 5. Passare a Criteri di gruppo. Fare clic su '+' per configurare i diversi Criteri di gruppo per ogni gruppo AD. In questo esempio, i criteri di gruppo Finance-Group-Policy, HR-Group-Policy e IT-Group-Policy sono configurati per avere accesso a subnet diverse.



Per Finance-Group-Policy sono disponibili le impostazioni seguenti:

```
<#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|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>
```

Analogamente, HR-Group-Policy dispone delle impostazioni seguenti:

```
<#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>
```

Infine, IT-Group-Policy dispone delle impostazioni seguenti:

```
<#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>
```

Passaggio 6. Creare un oggetto NOACCESS di Criteri di gruppo, passare a Impostazioni sessione e deselezionare l'opzione Accesso simultaneo per utente. In questo modo il valore vpn-simultous-logins viene impostato su 0.

Il valore vpn-simultous-logins in Criteri di gruppo quando impostato su 0 interrompe immediatamente la connessione VPN dell'utente. Questo meccanismo viene utilizzato per impedire agli utenti che appartengono a un gruppo di utenti AD diverso da quelli configurati (in questo esempio, Finanza, HR o IT) di stabilire connessioni riuscite all'FTD e di accedere a risorse sicure disponibili solo per gli account del gruppo di utenti consentiti.

Gli utenti che appartengono ai gruppi di utenti AD corretti corrispondono alla mappa degli attributi LDAP nel FTD ed ereditano i Criteri di gruppo mappati, mentre gli utenti che non appartengono ad alcuno dei gruppi consentiti ereditano i Criteri di gruppo predefiniti del profilo di connessione, che in questo caso è NOACCESS.

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 to VPN

DNS Server

Select DNS Group

Banner Text for Authenticated Clients

This message will be shown to successfully authenticated endpoints in the beginning of their VPN session

Default domain

AnyConnect client profiles

+

CANCEL OK

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

Connection Time Alert Interval

1 minutes
1-30; (Default: 1)

Idle Time

30 minutes
1-35791394; (Default: 30)

Idle Alert Interval

1 minutes
1-30; (Default: 1)

Simultaneous Login per User

1-2147483647; (Default: 3)

CANCEL OK

I Criteri di gruppo NOACCESS dispongono delle impostazioni seguenti:

<#root>

firepower#

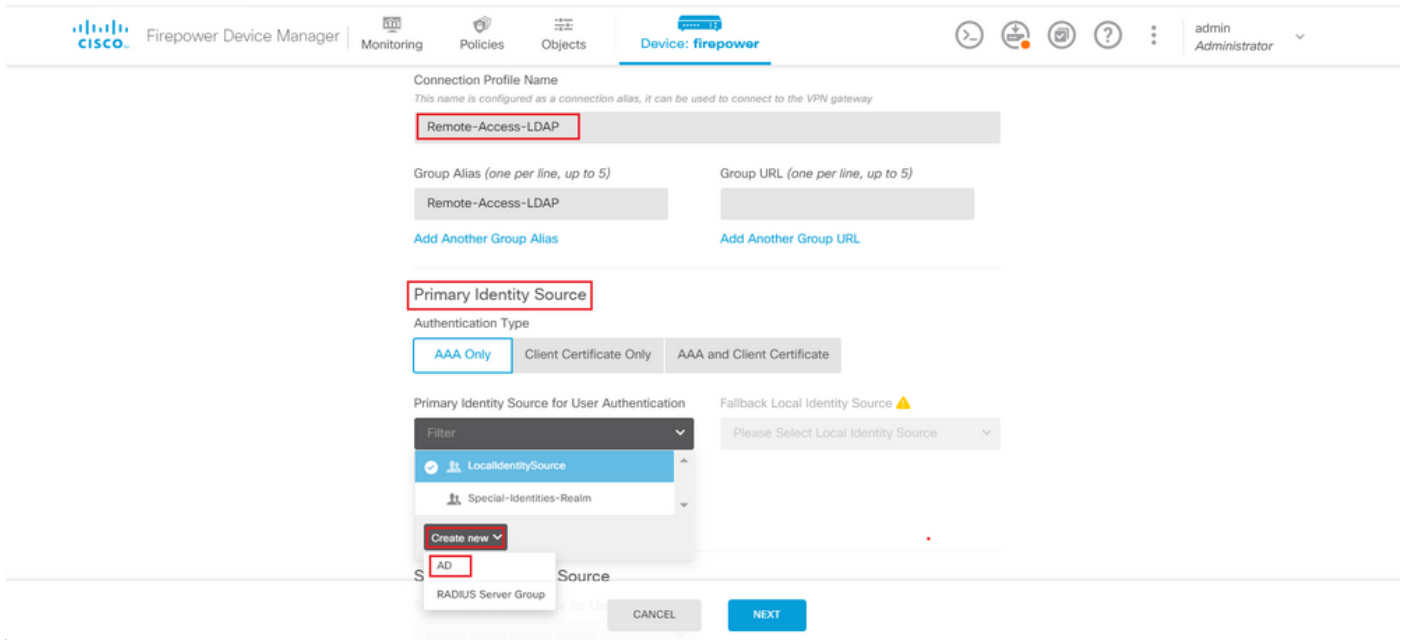
show run group-policy NOACCESS

```
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
```

Passaggio 7. Passare a Profili di connessione e creare un profilo di connessione. In questo esempio il nome del profilo è Accesso remoto-LDAP. Scegliere Solo AAA origine identità primaria e creare un nuovo tipo di server di autenticazione AD.



Immettere le informazioni sul server AD:

- Nome utente directory
- Password directory
- DN di base
- Dominio primario AD
- Nome host / Indirizzo IP
- Port
- Tipo di crittografia

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

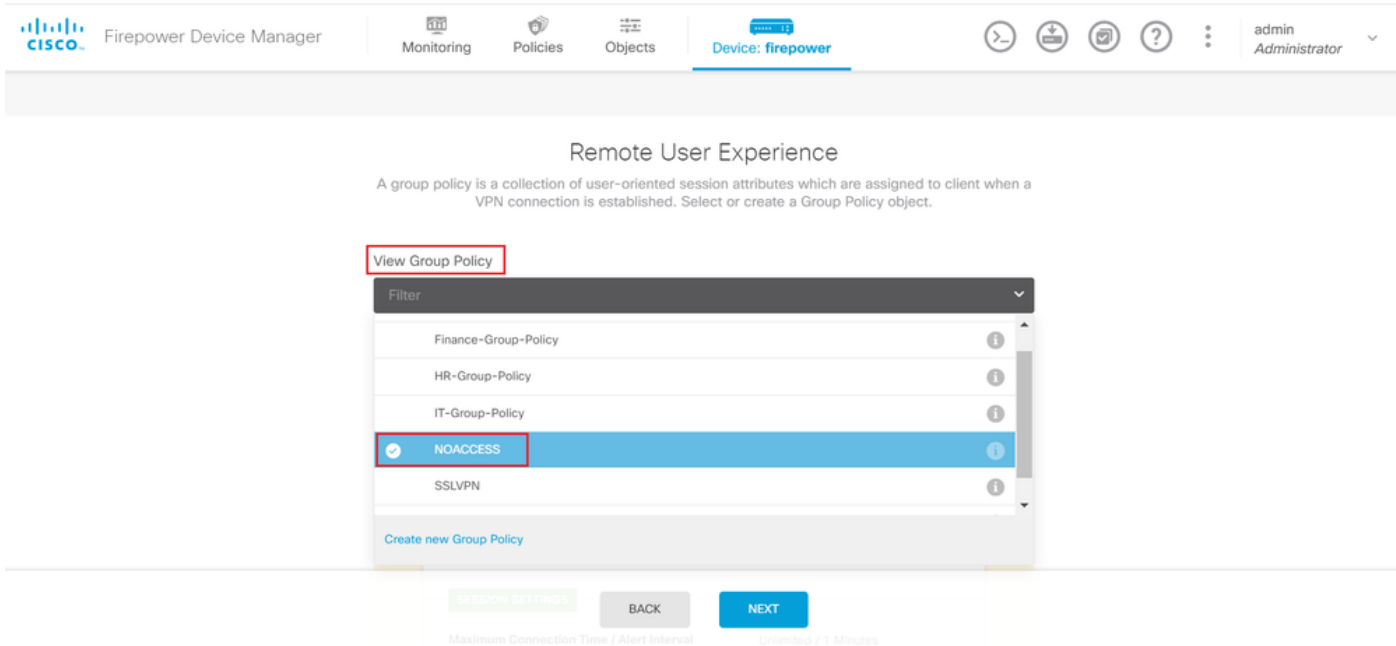
TEST

[Add another configuration](#)

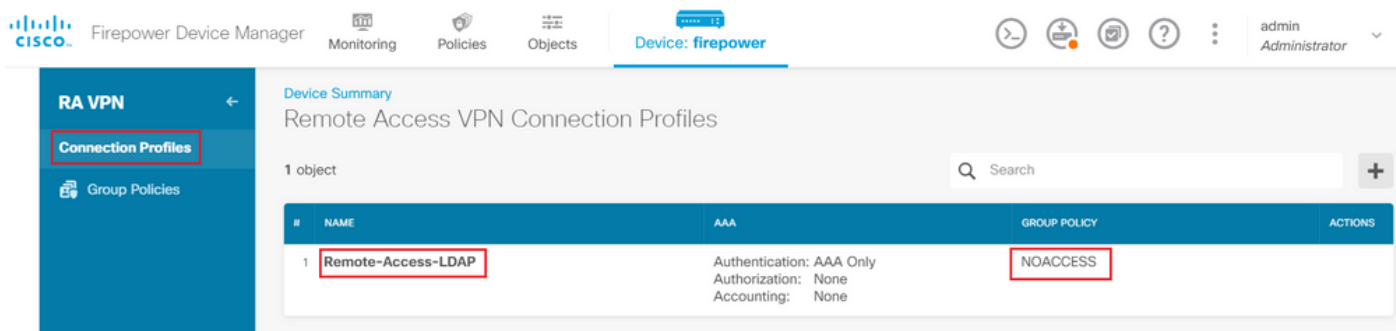
CANCEL

OK

Fare clic su Avanti e scegliere NOACCESS come criterio di gruppo predefinito per il profilo di connessione.



Salva tutte le modifiche. Il profilo di connessione Accesso remoto-LDAP è ora visibile nella configurazione VPN di Accesso remoto.

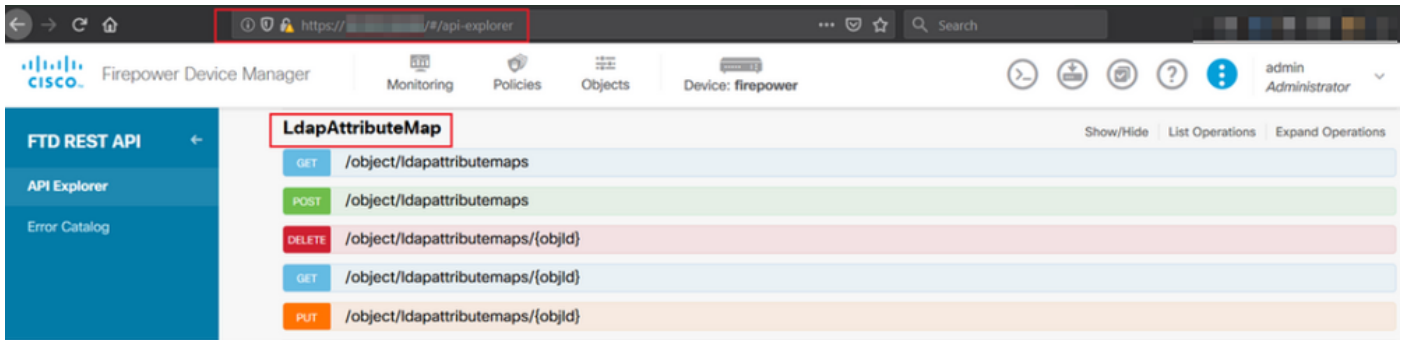


Procedura di configurazione per la mappa degli attributi LDAP

Passaggio 1. Avviare API Explorer dell'FTD.

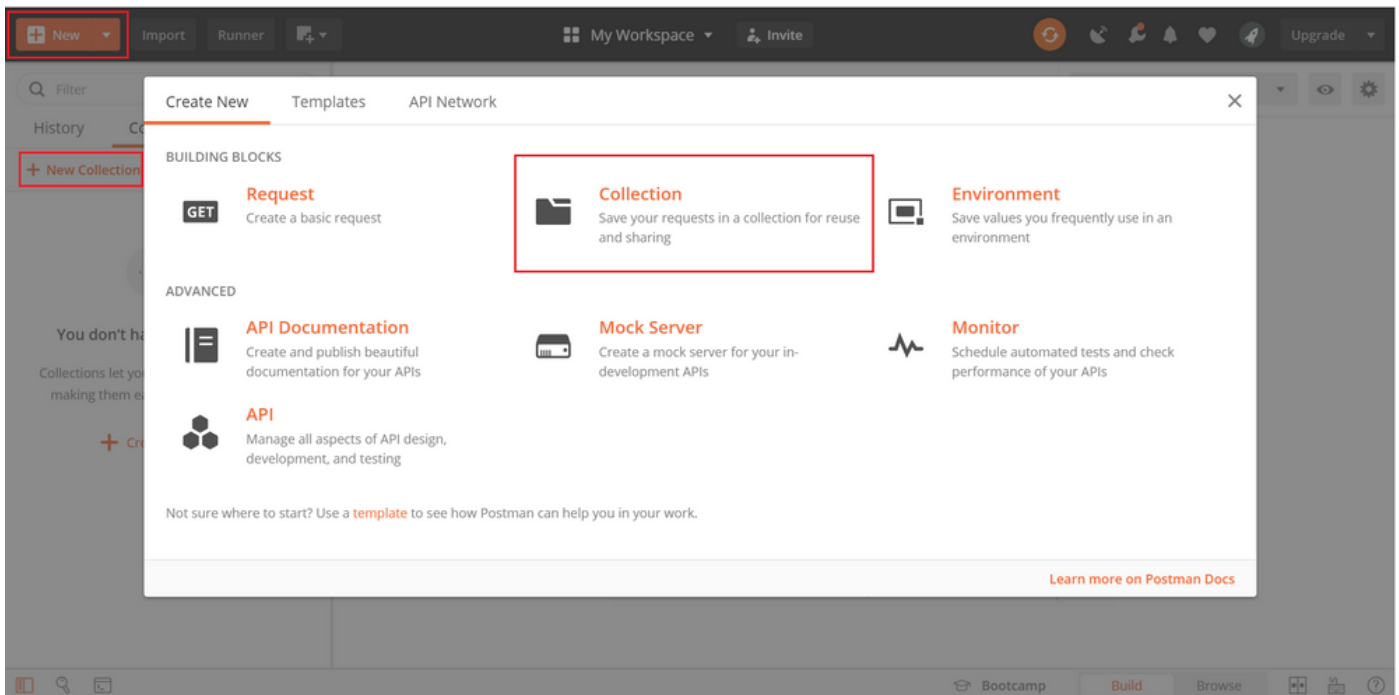
API Explorer contiene l'intero elenco di API disponibili sull'FTD. Passare a <https://<FTD Management IP>/api-explorer>

Scorrere fino alla sezione LdapAttributeMap e fare clic su di essa per visualizzare tutte le opzioni supportate.

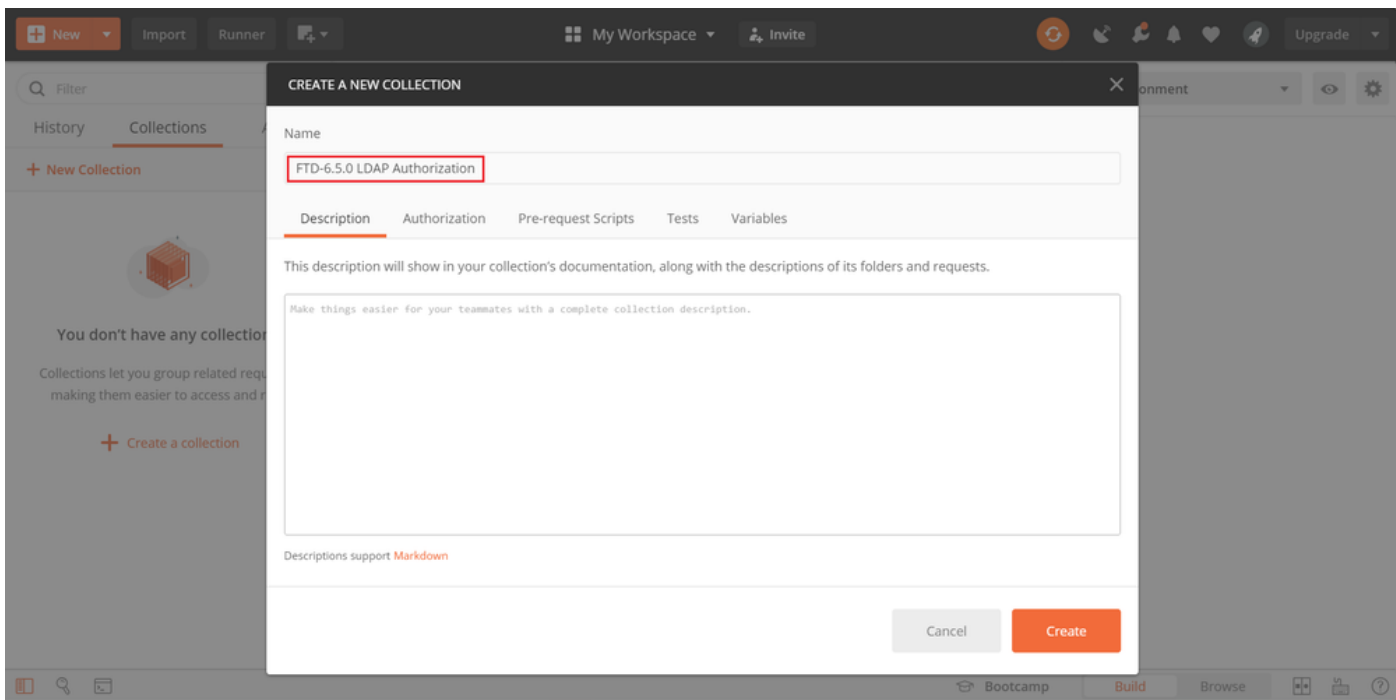


✎ Nota: in questo esempio, viene utilizzato Postman come strumento API per configurare la mappa degli attributi LDAP.

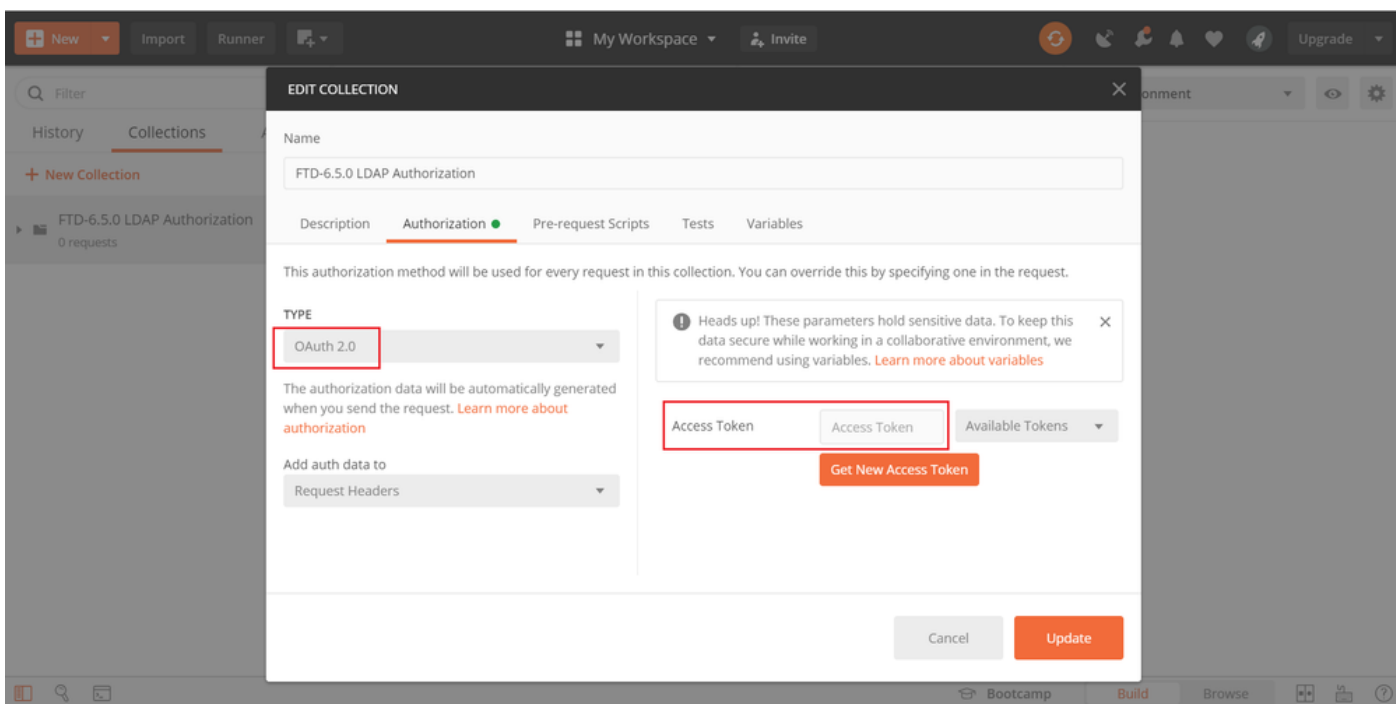
Passaggio 2. Aggiungere una raccolta Postman per l'autorizzazione LDAP.



Immettere un nome per la raccolta.



Modifica Authorization e selezionare il tipo OAuth 2.0



Punto 3. Passare a File > Impostazioni, disattivare la verifica del certificato SSL per evitare errori di handshake SSL durante l'invio di richieste API all'FTD. Ciò avviene se l'FTD utilizza un certificato autofirmato.



Postman

File Edit View Help

New... Ctrl+N

New Tab Ctrl+T

New Postman Window Ctrl+Shift+N

New Runner Window Ctrl+Shift+R

Import... Ctrl+O

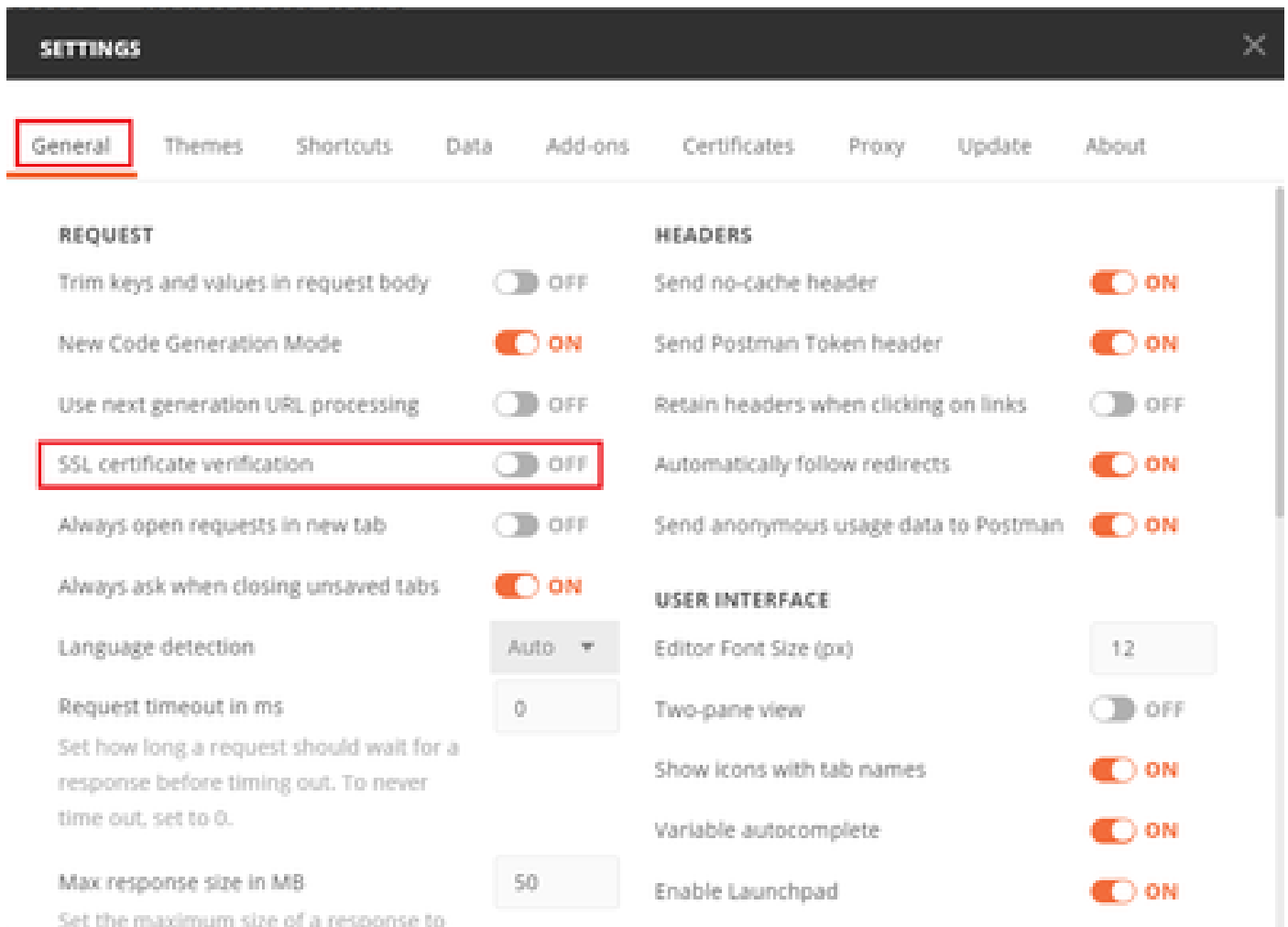
Settings Ctrl+Comma

Close Window Ctrl+Shift+W

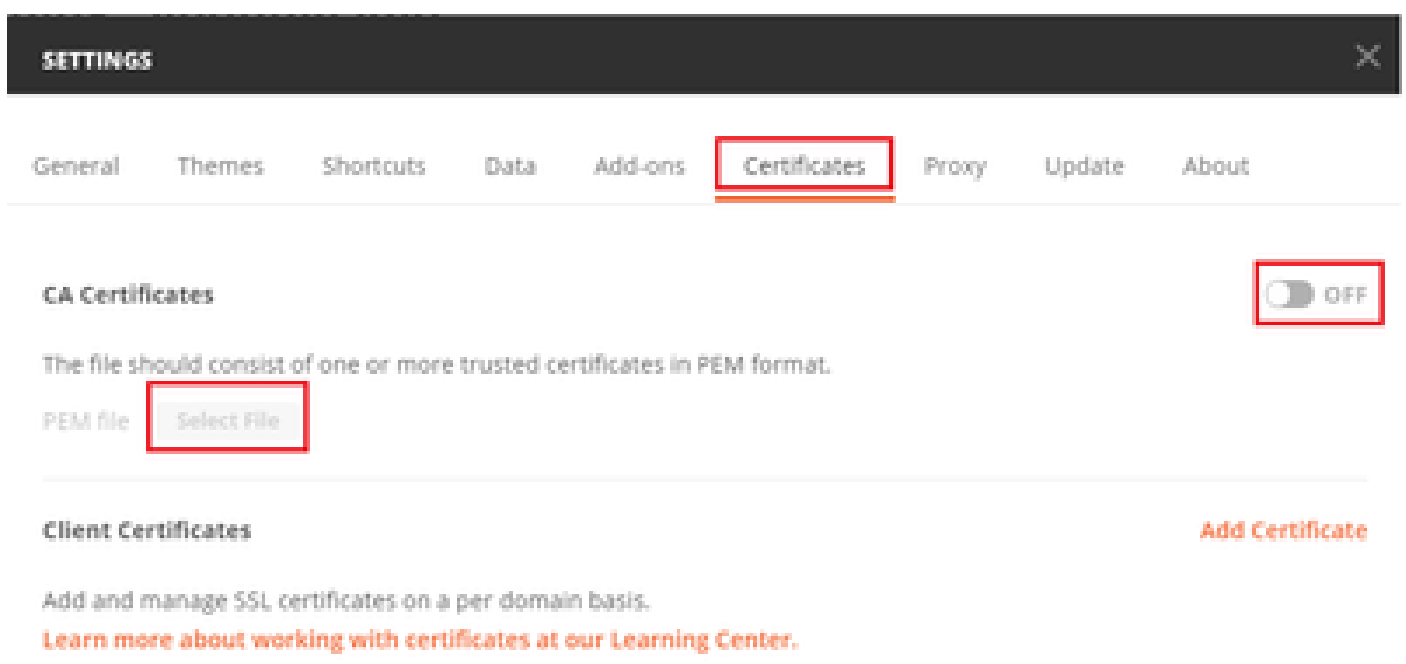
Close Tab Ctrl+W

Force Close Tab Alt+Ctrl+W

Exit



In alternativa, il certificato utilizzato dall'FTD può essere aggiunto come certificato CA nella sezione Certificato delle impostazioni.



Passaggio 4. Aggiungere una nuova richiesta POST Auth per creare una richiesta POST di accesso all'FTD, in modo da ottenere il token per autorizzare qualsiasi richiesta POST/GET.

+ New Collection

Trash

FTD-6.5.0 LDAP Authorization ☆

0 requests

This collec
collection



Share Collection



Manage Roles



Rename

Ctrl+E



Edit



Create a fork



Create Pull Request



Merge changes



Add Request



Add Folder



Duplicate

Ctrl+D



Export



Monitor Collection

Accetta application/json

MANAGE HEADER PRESETS

Add Header Preset

Header-LDAP

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

Cancel Add

Per tutte le altre richieste, passare alle rispettive schede Intestazione e selezionare il seguente valore Intestazione preimpostata: Intestazione-LDAP per le richieste API REST in modo da utilizzare json come tipo di dati primario.

Il corpo della richiesta POST per ottenere il token deve contenere:

Tipo	raw - JSON (application/json)
tipo_concessione	password
username	Per accedere al file FTD, usare il nome utente Admin
password	Password associata all'account utente admin

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

POST https://1.../api/fdm/latest/fdm/token Send

Params Authorization Headers (1) Body Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL BETA JSON

```
1 {  
2   "grant_type": "password",  
3   "username": "admin",  
4   "password": "  
5 }
```

Dopo aver fatto clic su invia, il corpo della risposta contiene il token di accesso utilizzato per inviare eventuali richieste PUT/GET/POST all'FTD.



```
{
  "access_token": "eyJhbGciOiJIUzI1IiwiaXN0IjoiOiJ0d2UzeKwL3pFShTymxgS0dkrJakCXvP4Lyzdr-xap0",
  "expires_in": 1800,
  "token_type": "Bearer",
  "refresh_token": "eyJhbGciOiJIUzI1IiwiaXN0IjoiOiJ0d2UzeKwL3pFShTymxgS0dkrJakCXvP4Lyzdr-xap0",
  "refresh_expires_in": 2400
}
```

Questo token viene quindi utilizzato per autorizzare tutte le richieste successive.

Passare alla scheda Autorizzazione di ogni nuova richiesta e selezionare la richiesta successiva:

Tipo	OAuth 2.0
Token	Token di accesso ricevuto eseguendo la richiesta di accesso POST


```
58 {
59   "version": "26dc13129",
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": "ogalyil3higo",
77       "name": "acl1",
78       "id": "5ec790d-9836-11ea-ba77-37f667647b3e",
79       "type": "networkobject"
80     }
81   ],
82   "ipv6SplitTunnelNetworks": [],
83   "splitDNSRequestPolicy": "USE_SPLIT_TUNNEL_SETTING",
84   "splitDNSDomainList": "",
85   "scpfForwardingUrl": null,
86   "periodicClientCertAuthenticationInterval": 1,
87   "enableDTLS": false,
88   "enableDTLSCompression": false,
89   "sslCompression": "DISABLED",
90   "enableSSLrekey": false,
91   "rekeyMethod": "NEB_TUNNEL",
92   "rekeyInterval": 4,
93   "ignoreDFBit": false,
94   "bypassUnsupportedProtocol": false,
95   "mtuSize": 1400,
96   "useAlwaysOnVPNSettingInProfile": true,
97   "enableKeepAliveMessages": false,
98   "keepAliveMessageInterval": 20,
99   "enableGatewayDPO": false,
100  "gatewayDPOInterval": 30,
101  "enableClientDPO": false,
102  "clientDPOInterval": 30,
103  "clientProfiles": [],
104  "keepInstallerOnClient": false,
105  "vpnTrafficFilterACL": null,
106  "enableRestrictVPNToVLAN": false,
107  "restrictVPNToVLANs": 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  "isEnablePeriodicClientCertAuthentication": false,
118  "id": "a5722b15-9836-11ea-ba77-6916f09acebc",
119  "type": "ravprgrouppolicy",
120  "links": {
121    "self": "https://.../api/fdm/latest/object/ravprgrouppolicies/a5722b15-9836-11ea-ba77-6916f09acebc"
122  }
123 }
```

Passaggio 6. Aggiungere una nuova richiesta POST Crea mappa attributi LDAP per creare la mappa attributi LDAP. Nel presente documento viene utilizzato il modello LdapAttributeMapping. Anche altri modelli hanno operazioni e metodi simili per creare la mappa degli attributi. Gli esempi di questi modelli sono disponibili in api-explorer come accennato in precedenza in questo documento.

FTD REST API

API Explorer

Error Catalog

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', 'AUTHORIZATION_REQUIRED', 'AUTHORIZATION_TYPE', 'BANNER1', 'BANNER2', 'CISCO_AV_PAIR', 'CISCO_IP_PHONE_BYPASS', 'CISCO_LEAP_BYPASS', 'CLIENT_BYPASS_PROTOCOL', 'CLIENT_INTERCEPT_DHCP_CONFIGURE_MSG', 'CLIENT_TYPE_VERSION_LIMITING', 'CONFIDENCE_INTERVAL', 'DHCP_NETWORK_SCOPE', 'DN_FIELD', 'DISABLE_ALWAYS_ON_VPN', 'FIREWALL_ACL_IN', 'FIREWALL_ACL_OUT', 'GATEWAY_FQDN', 'GROUP_POLICY', 'IE_PROXY_BYPASS_LOCAL', 'IE_PROXY_EXCEPTION_LIST', 'IE_PROXY_METHOD', 'IE_PROXY_SERVER', 'IETF_RADIUS_CLASS', 'IETF_RADIUS_FILTER_ID', 'IETF_RADIUS_FRAMED_IP_ADDRESS', 'IETF_RADIUS_FRAMED_IP_NETMASK', 'IETF_RADIUS_IPV6_PREFIX', 'IETF_RADIUS_IDLE_TIMEOUT', 'IETF_RADIUS_INTERFACE_ID', 'IETF_RADIUS_SERVICE_TYPE', 'IETF_RADIUS_SESSION_TIMEOUT', 'IKE DPD_Retry_Interval', 'IKE_KEEP_ALIVES', 'IPSEC_ALLOW_PASSWD_STORE', 'IPSEC_AUTH_ON_REKEY', 'IPSEC_AUTHENTICATION', 'IPSEC_BACKUP_SERVER_LIST', 'IPSEC_BACKUP_SERVERS', 'IPSEC_CLIENT_FIREWALL_FILTER_NAME', 'IPSEC_CLIENT_FIREWALL_FILTER_OPTIONAL', 'IPSEC_DEFAULT_DOMAIN', 'IPSEC_EXTENDED_AUTH_ON_REKEY', 'IPSEC_IKE_PEER_ID_CHECK', 'IPSEC_IP_COMPRESSION', 'IPSEC_IPV6_SPLIT_TUNNELING_POLICY', 'IPSEC_MODE_CONFIG', 'IPSEC_OVER_UDP', 'IPSEC_OVER_UDP_PORT', 'IPSEC_REQUIRED_CLIENT_FIREWALL_CAPABILITY', 'IPSEC_SPLIT_DNS_NAMES', 'IPSEC_SPLIT_TUNNEL_ALL_DNS', 'IPSEC_SPLIT_TUNNEL_LIST', 'IPSEC_SPLIT_TUNNELING_POLICY', 'IPSEC_TUNNEL_TYPE', 'IPSEC_USER_GROUP_LOCK', 'IPV6_PRIMARY_DNS', 'IPV6_SECONDARY_DNS', 'L2TP_ENCRYPTION', 'L2TP_MPPC_COMPRESSION', 'MS_CLIENT_SUBNET_MASK', 'PFS_REQUIRED', 'PPTP_ENCRYPTION', 'PPTP_MPPC_COMPRESSION', 'WEBVPN_VLAN'],

valueMappings (Array[LdapToCiscoValueMapping]): A list of LdapToCiscoValueMapping objects, which specify the value mappings for this LDAP 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 object. Use this nested entity in an LDAP attribute map. (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),

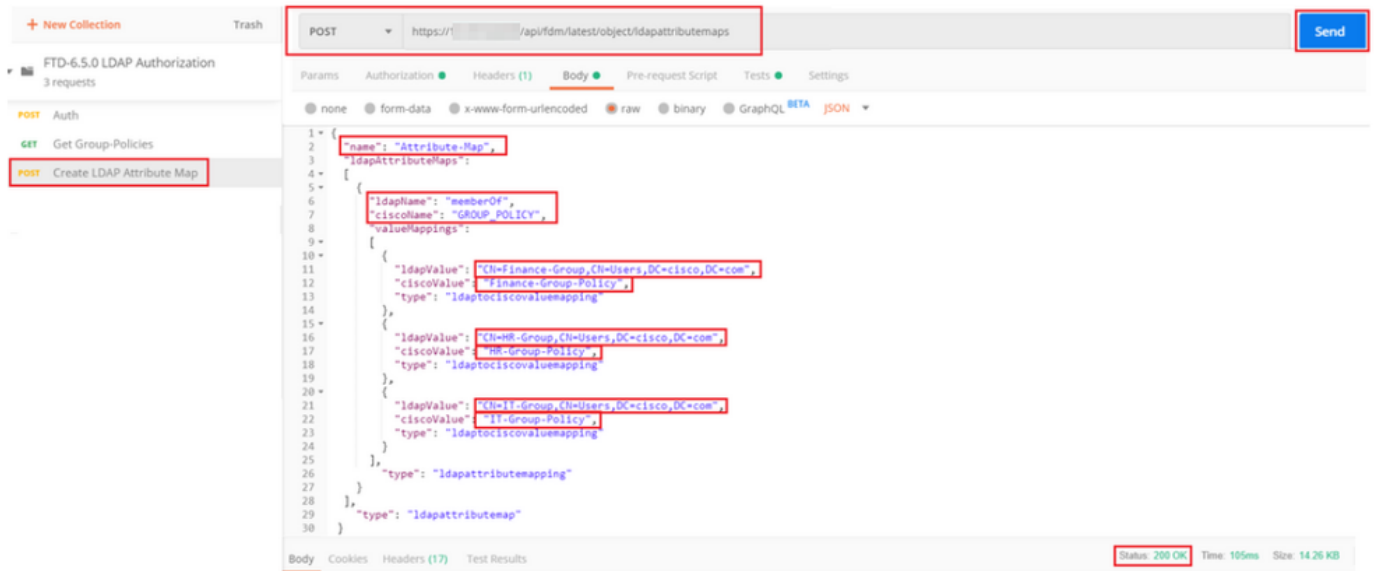
valueMappings (Array[LdapToGroupPolicyValueMapping]): A list of LdapToGroupPolicyValueMapping objects, which specify the value-to-group policy mappings for this LDAP attribute.
Field level constraints: cannot be null. (Note: Additional constraints might exist),

type (string): ldapattributetogrouppolicymapping

L'URL da INSERIRE nella mappa degli attributi LDAP è: <https://<FTD Management IP>/api/fdm/last/object/ldapattributemaps>

Il corpo della richiesta POST deve contenere quanto segue:

nome	Nome per la mappa degli attributi LDAP
tipo	ldapattributemapping
NomeLDAP	memberOf
NomeCisco	CRITERI_GRUPPO
ValoreLDAP	Valore memberOf per l'utente da AD
Valore cisco	Nome di Criteri di gruppo per ogni gruppo di utenti in FDM




Il corpo della richiesta POST contiene le informazioni sulla mappa degli attributi LDAP che mappa un criterio di gruppo specifico a un gruppo AD in base al valore memberOf:

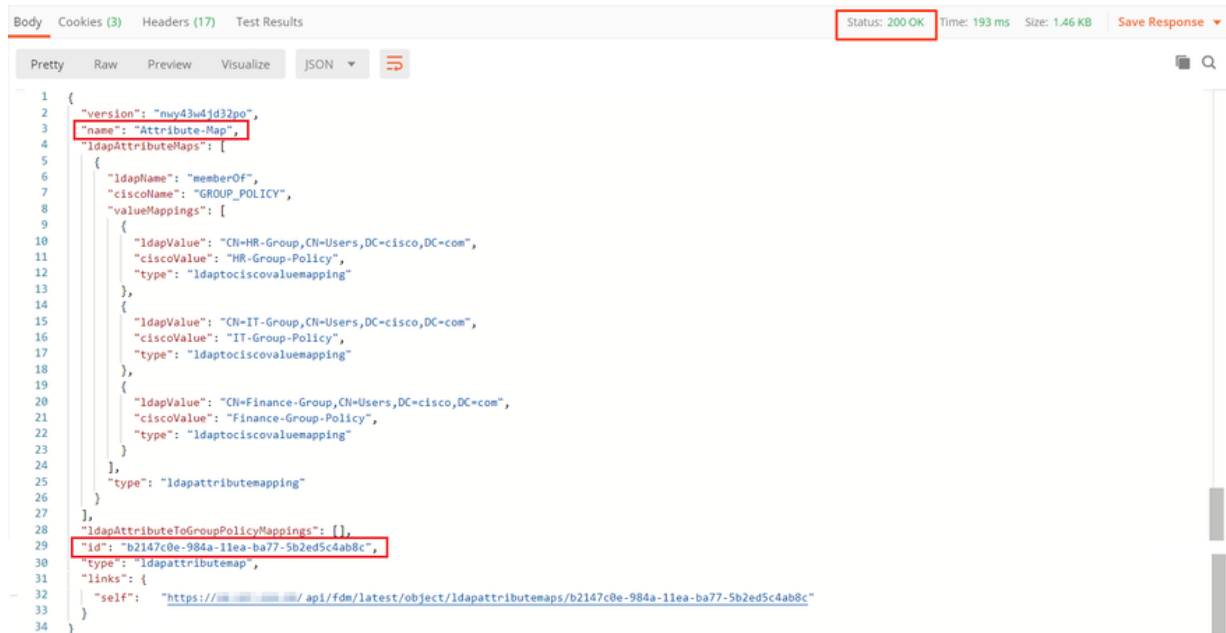
```

{
  "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: il campo memberOf può essere recuperato dal server AD con il comando dsquery oppure recuperato dai debug LDAP sull'FTD. Nel campo memberOf value: dei log di debug.

La risposta di questa richiesta POST è simile all'output successivo:



```
1 {
2   "version": "nv43u4d32po",
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://<FTD Management IP>/api/fdm/latest/object/ldapattributemaps/b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c"
33  }
34 }
```

Passaggio 7. Aggiungere una nuova richiesta GET per ottenere la configurazione corrente dell'area di autenticazione AD in FDM.

L'URL per ottenere la configurazione corrente del realm AD è: <https://<FTD Management IP>/api/fdm/latest/object/realms>


```

1 {
2   "items": [
3     {
4       "version": "k3j0dha5ixyy",
5       "name": "LDAP-AD",
6       "directoryConfigurations": [
7         {
8           "hostname": "192.168.1.1",
9           "port": 389,
10          "encryptionProtocol": "NONE",
11          "encryptionCert": null,
12          "type": "directoryconfiguration"
13        }
14      ],
15      "enabled": true,
16      "systemDefined": false,
17      "realId": 3,
18      "dirUsername": "administrator@192.168.1.1",
19      "dirPassword": "*****",
20      "baseDN": "dc=192.168.1, dc=com",
21      "ldapAttributeMap": null,
22      "adPrimaryDomain": "192.168.1.1",
23      "id": "bf50a8ab-9819-11ea-ba77-d32ecc224295",
24      "type": "activedirectoryrealm",
25      "links": {
26        "self": "https://192.168.1.1/api/fdm/latest/object/realms/bf50a8ab-9819-11ea-ba77-d32ecc224295"
27      }
28    }
29  ],
30  "paging": {
31    "prev": [],
32    "next": [],
33    "limit": 10,
34    "offset": 0,
35    "count": 1,
36    "pages": 0
37  }
38 }

```

Si noti che il valore della chiave ldapAttributeMap è null.

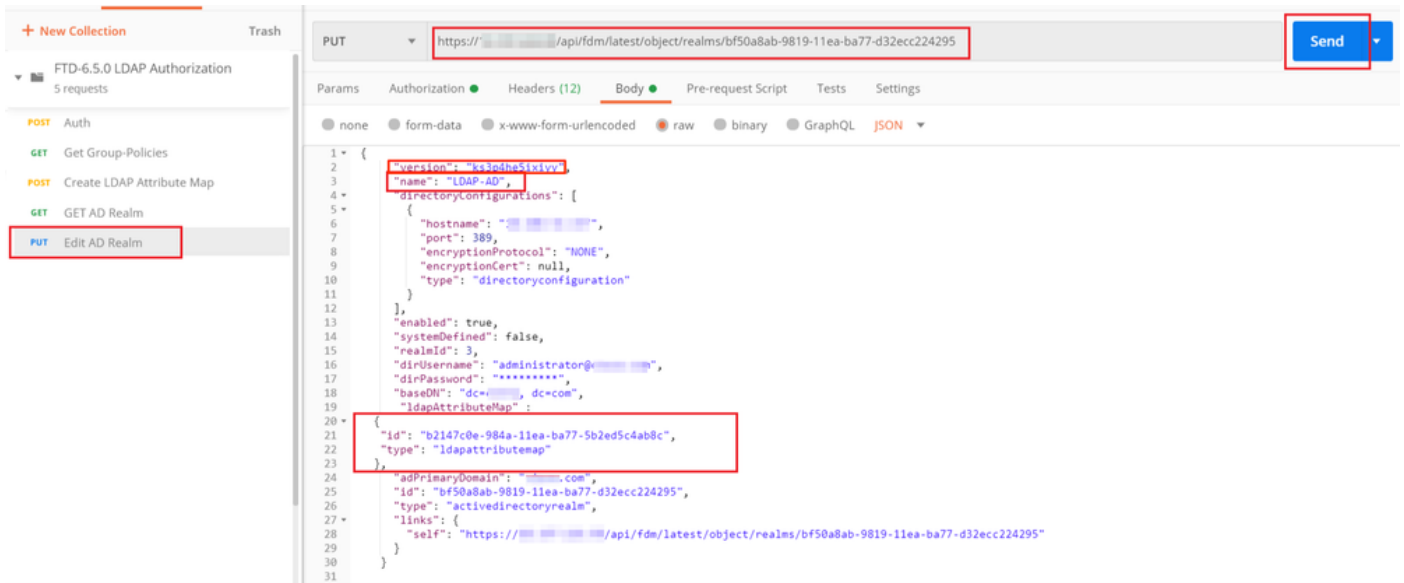
Passaggio 8. Creare una nuova richiesta PUT per modificare il realm AD. Copiare l'output della risposta GET dal passaggio precedente e aggiungerlo al corpo di questa nuova richiesta PUT. Questo passaggio può essere utilizzato per apportare modifiche all'impostazione corrente del realm di Active Directory, ad esempio: modificare la password, l'indirizzo IP o aggiungere un nuovo valore per una chiave come ldapAttributeMap in questo caso.

 Nota: è importante copiare il contenuto dell'elenco di elementi anziché l'intero output della risposta GET. L'URL della richiesta PUT deve essere aggiunto all'ID articolo dell'oggetto per il quale sono state apportate modifiche. Nell'esempio il valore è: bf50a8ab-9819-11ea-ba77-d32ecc224295

L'URL per modificare la configurazione corrente del realm AD è: <https://<FTD Management IP>/api/fdm/latest/object/realms/<realm ID>>

Il corpo della richiesta PUT deve contenere:

version	versione ottenuta dalla risposta di una richiesta GET precedente
ID	ID ottenuto dalla risposta di una richiesta GET precedente
ldapAttributeMap	ldap-id da risposta della richiesta Crea mappa attributi LDAP



Il corpo della configurazione in questo esempio è:

<#root>

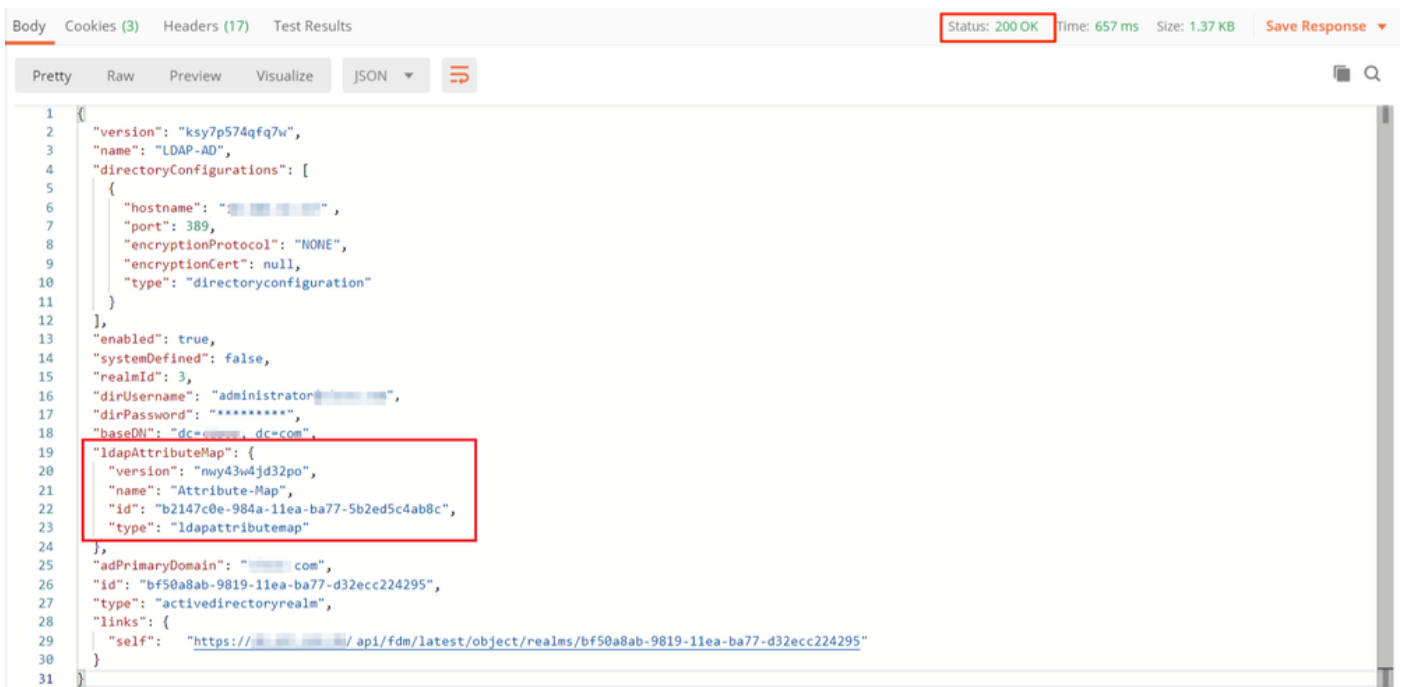
```
{
  "version": "ks3p4he5ixiyy",
  "name": "LDAP-AD",
  "directoryConfigurations": [
    {
      "hostname": "<IP Address>",
      "port": 389,
      "encryptionProtocol": "NONE",
      "encryptionCert": null,
      "type": "directoryconfiguration"
    }
  ],
  "enabled": true,
  "systemDefined": 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"
```

```
}  
}
```

Verificare che l'ID ldapAttributeMap corrisponda nel corpo della risposta per questa richiesta.



The screenshot shows a REST client interface with a JSON response. The status bar at the top indicates "Status: 200 OK", "Time: 657 ms", and "Size: 1.37 KB". The response body is displayed in a "Pretty" view. A red box highlights the "ldapAttributeMap" field, which contains the following JSON object:

```
{  
  "version": "mwy43w4jd32po",  
  "name": "Attribute-Map",  
  "id": "b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c",  
  "type": "ldapattributemap"  
}
```


(Facoltativo). La mappa degli attributi LDAP può essere modificata con le richieste PUT. Creare una nuova richiesta PUT Modifica mappa attributi e apportare le modifiche desiderate, ad esempio il nome della mappa attributi o il valore memberOf. T

Nell'esempio seguente, il valore di ldapvalue è stato modificato da CN=Users a CN=UserGroup per tutti e tre i gruppi.

```
1 PUT https://10.197.224.99/api/fdm/latest/object/ldapattributemaps/021470e-904a-11ea-ba77-5b2e5c4a8dc
2 {"description": "NewKad51200",
3  "name": "MEM10UE-ldap",
4  "ldapattributemaps":
5  {
6    {
7      "idpname": "memberOf",
8      "ciscoName": "GROUP_POLICY",
9      "valueMappings":
10     {
11       {
12         "idpname": "CiwFinance-Group_CwuserGroup_DC=cisco_DC=com",
13         "ciscoName": "Finance-Group-Policy",
14         "type": "ldaptoiscisovaluemapping"
15       },
16       {
17         "idpname": "CiwHR-Group_CwuserGroup_DC=cisco_DC=com",
18         "ciscoName": "HR-Group-Policy",
19         "type": "ldaptoiscisovaluemapping"
20       },
21       {
22         "idpname": "CiwIT-Group_CwuserGroup_DC=cisco_DC=com",
23         "ciscoName": "IT-Group-Policy",
24         "type": "ldaptoiscisovaluemapping"
25       }
26     }
27   }
28 }
29
30 {"id": "021470e-904a-11ea-ba77-5b2e5c4a8dc",
31  "type": "ldapattributemap",
32  "links": {
33    "self": "https://10.197.224.99/api/fdm/latest/object/ldapattributemaps/021470e-904a-11ea-ba77-5b2e5c4a8dc"
34  }
35 }
```

(Facoltativo). Per eliminare una Mappa attributi LDAP esistente, creare una Mappa attributi eliminazione richiesta DELETE. Includere l'id-mapping della risposta HTTP precedente e aggiungerlo all'URL di base della richiesta di eliminazione.

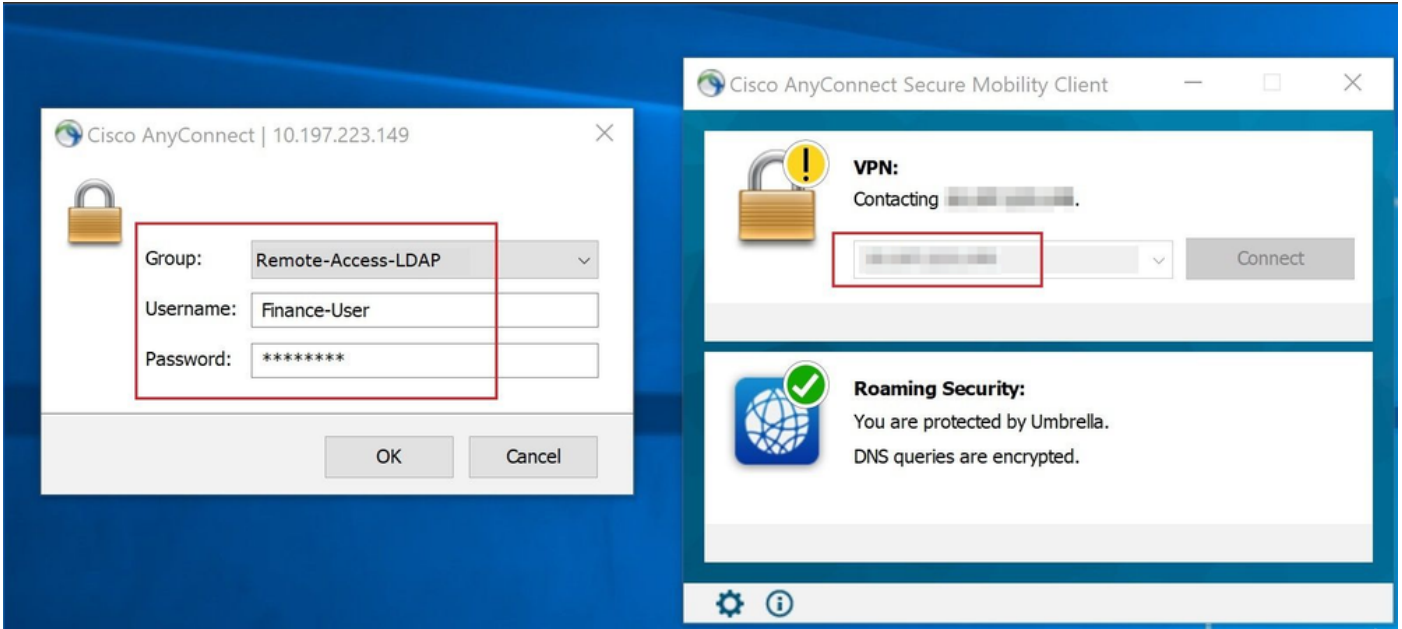
```
DELETE https://10.197.224.99/api/fdm/latest/object/ldapattributemaps/021470e-904a-11ea-ba77-5b2e5c4a8dc
```

 **Nota:** se l'attributo `memberOf` contiene spazi, è necessario che sia codificato tramite URL affinché il server Web possa analizzarlo. In caso contrario, viene ricevuta una risposta HTTP di richiesta non valida 400. Per evitare questo errore, è possibile utilizzare "%20" o "+" per la stringa contenente spazi vuoti.

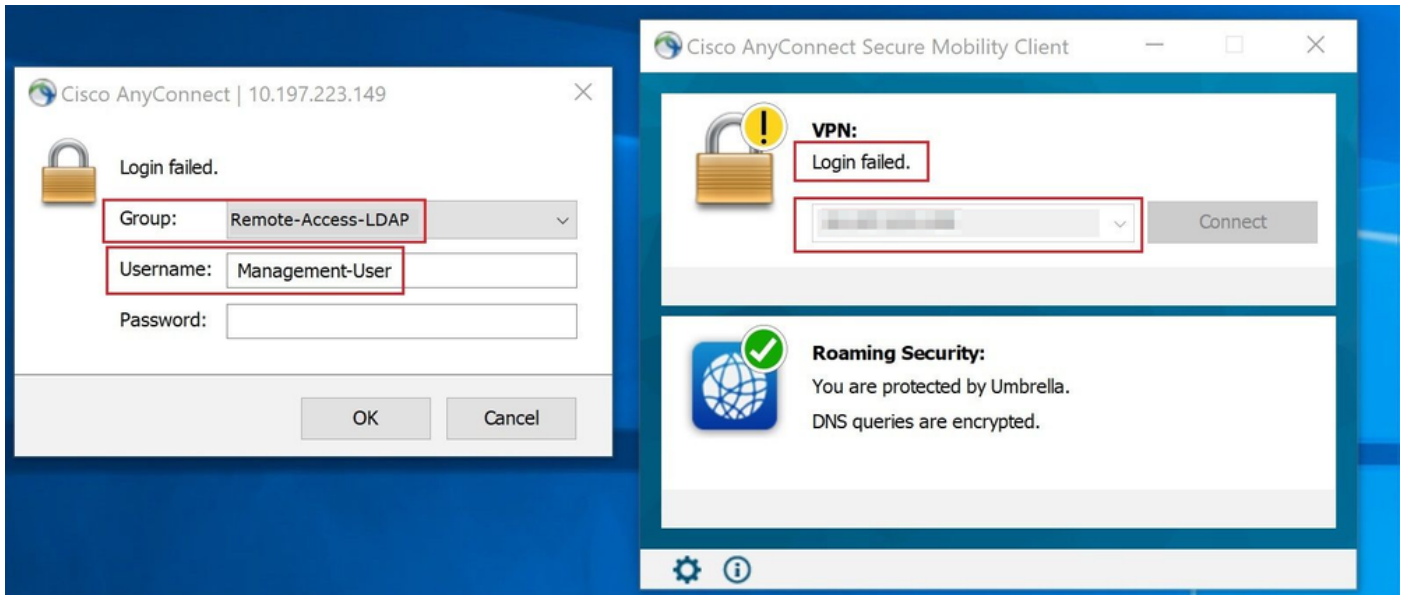
Passaggio 9. Tornare a FDM, selezionare l'icona Distribuzione e fare clic su Distribuisci ora.

utente e Password.

Quando un utente che appartiene al gruppo Finance di AD tenta di eseguire l'accesso, il tentativo ha esito positivo come previsto.



Quando un utente che appartiene al gruppo di gestione in Active Directory tenta di connettersi a Connection-Profile Remote-Access-LDAP, poiché nessuna mappa degli attributi LDAP ha restituito una corrispondenza, il criterio di gruppo ereditato dall'utente nel FTD è NOACCESS con il valore di vpn-simultous-logins impostato su 0. Il tentativo di accesso dell'utente non riesce.



La configurazione può essere verificata con i successivi comandi show dalla CLI di 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
```

Risoluzione dei problemi

Uno dei problemi più comuni nella configurazione dell'API REST è il rinnovo del token di connessione di volta in volta. Il tempo di scadenza del token è specificato nella risposta per la richiesta Auth. Se questo tempo scade, è possibile utilizzare un token di aggiornamento aggiuntivo per un periodo di tempo più lungo. Dopo la scadenza anche del token di aggiornamento, è necessario inviare una nuova richiesta Auth per recuperare un nuovo token di accesso.

 Nota: consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di debug.

 È possibile impostare vari livelli di debug. Per impostazione predefinita, viene utilizzato il livello 1. Se si modifica il livello di debug, il livello di dettaglio dei debug potrebbe aumentare. Procedere con cautela, soprattutto negli ambienti di produzione.

I seguenti debug sulla CLI FTD sono utili per la risoluzione dei problemi relativi alla mappa degli attributi LDAP

```
debug ldap 255
debug webvpn condition user <username>
debug webvpn anyconnect 255
```

debug aaa common 127

In questo esempio sono stati raccolti i debug successivi per illustrare le informazioni ricevute dal server AD quando gli utenti di test menzionati prima della connessione sono stati connessi.

Debug LDAP per 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
```

Debug LDAP per 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
```

Informazioni correlate

Per ulteriore assistenza, contattare il Cisco Technical Assistance Center (TAC). È necessario un contratto di supporto valido: [Contatti del supporto Cisco internazionali](#).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).