在Firepower威脅防禦(FTD)上配置AnyConnect LDAP對映

目錄

簡介

本文提供使用Firepower管理中心(FMC)FlexConfig策略對Firepower威脅防禦(FTD)上的AnyConnect使用者進行輕量級目錄訪問協定(LDAP)對映的配置示例。此配置用於允許屬於Active Directory(AD)組的特定使用者建立虛擬專用網路(VPN)連線。來自未在對映中定義的不同AD組的使用者將無法使用同一配置檔案進行連線。

必要條件

需求

思科建議您瞭解以下主題：

- FMC上的AD領域配置
- Windows Active Directory
- FMC上的AnyConnect(SSLVPN)配置
- FMC上FlexConfig對象的基本知識

採用元件

- FirePower管理器中心(FMC)版本6.2.3和6.5.0
- FirePower威脅防禦(FTD)版本6.2.3和6.5.0
- 帶有Active Directory的Windows Server

設定

FTD上的組態

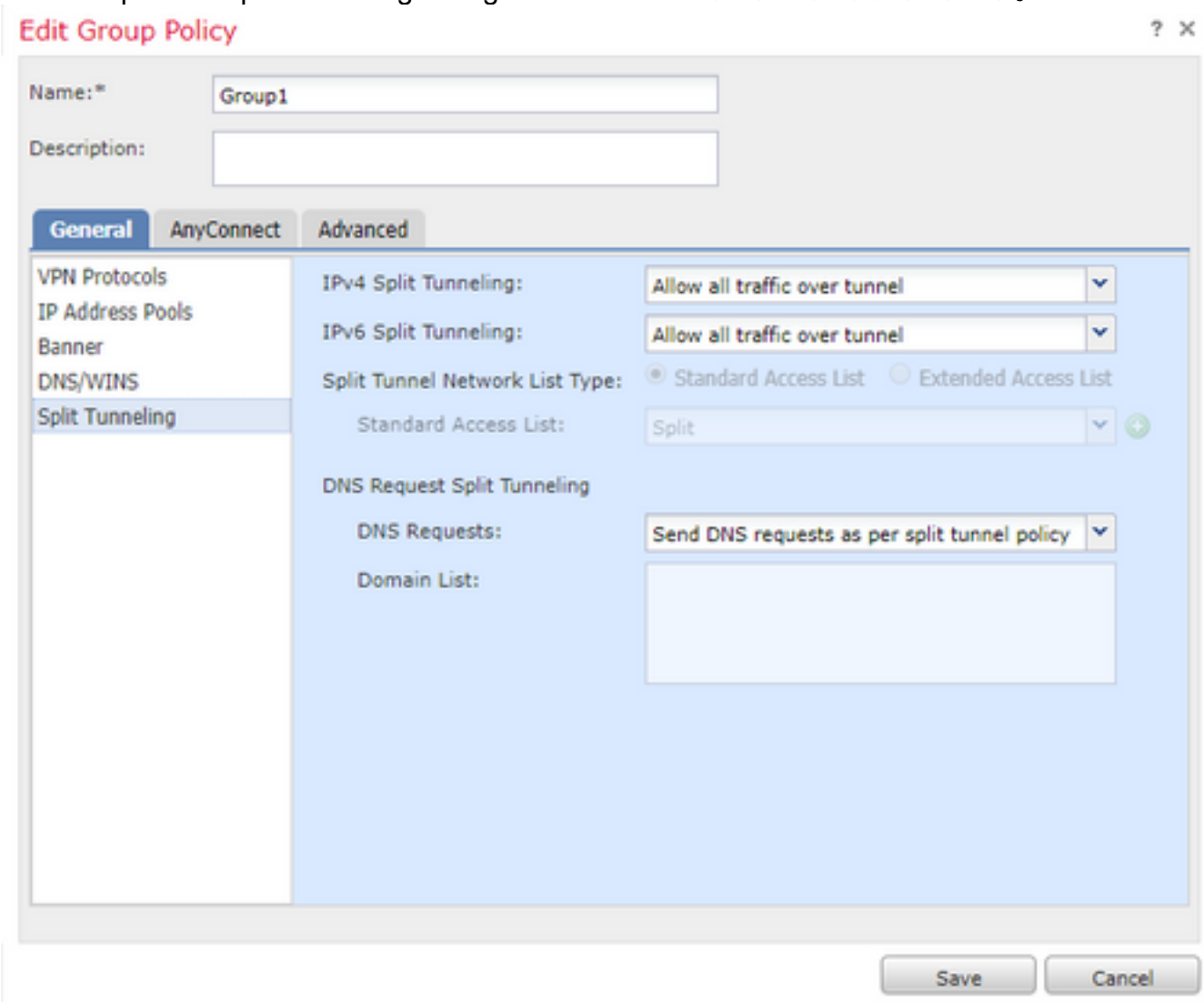
在本例中，屬於AD組1的使用者使用全隧道配置，而屬於AD組2的使用者對特定主機的訪問許可權有限。不屬於這些組的所有其他使用者均無法進行身份驗證。

步驟1.使用LDAP身份驗證配置AnyConnect並部署更改。本指南中有一個示例。

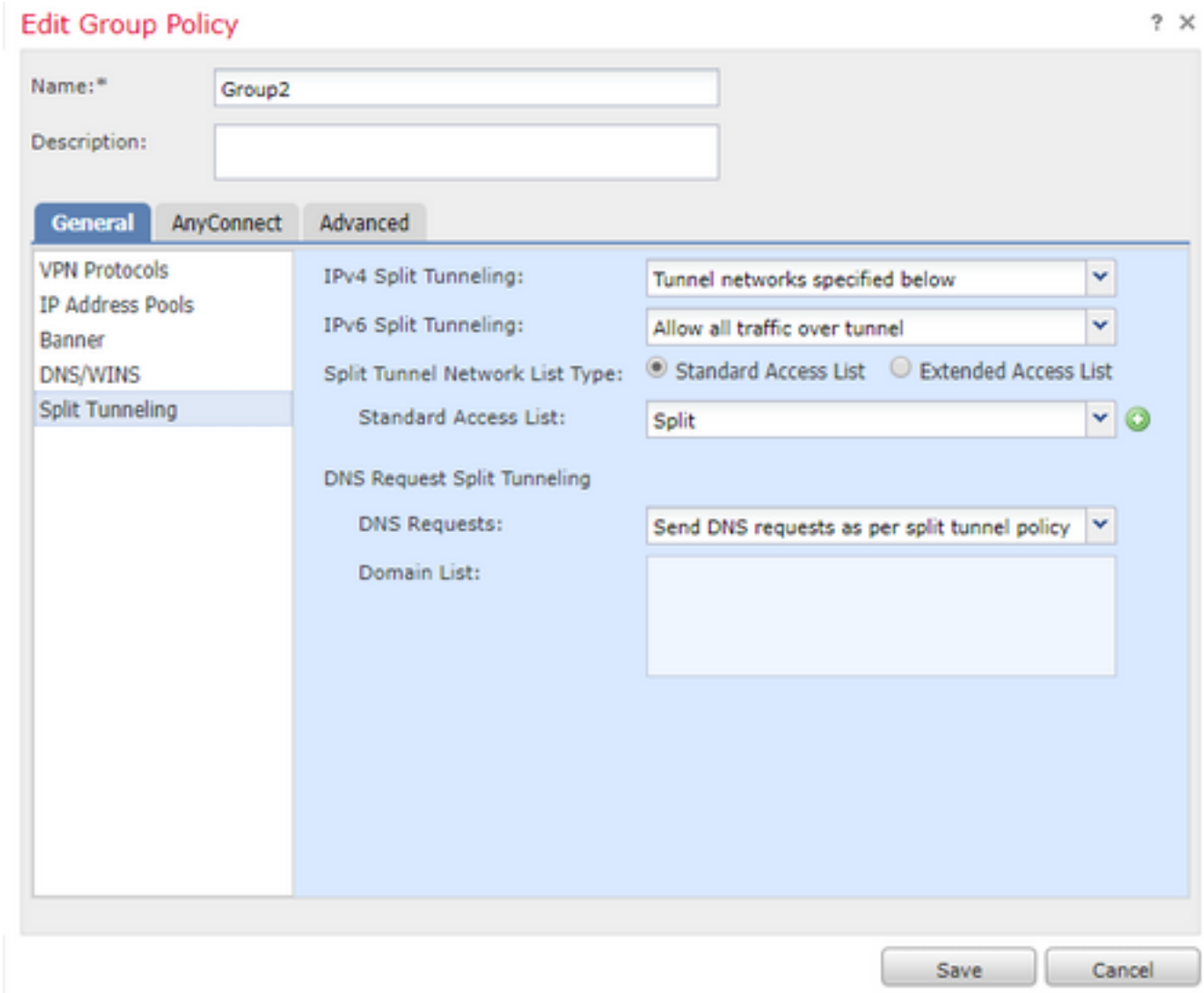
步驟2.導航到Devices > Remote Access > Edit AnyConnect Policy > Advanced > Group Policies。

步驟3.建立3個不同的組策略：

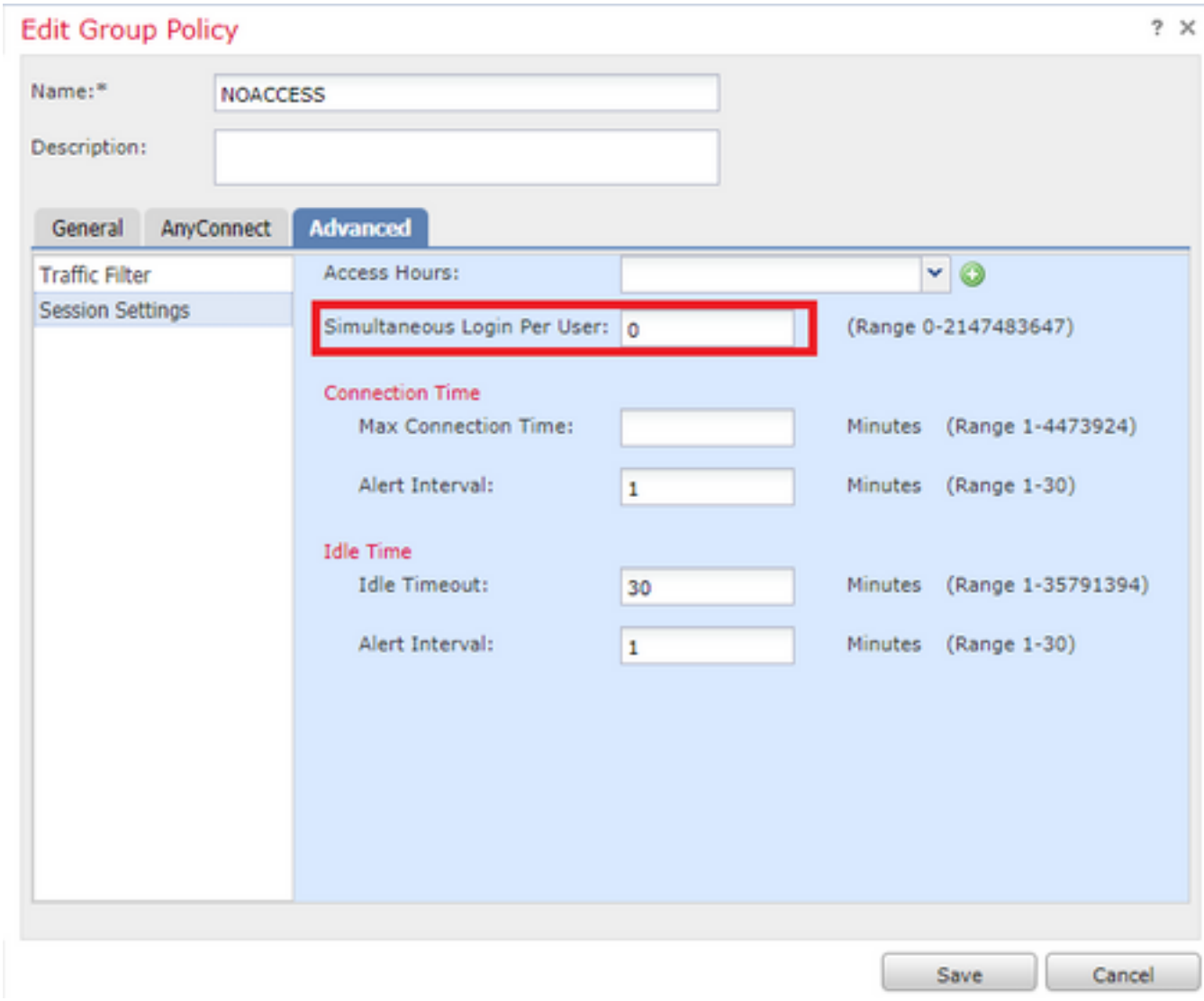
- Group1 with Split Tunneling configuration set to **Allow all traffic over tunnel。**



- 「分割隧道」配置設定為**Split**的Group2。



- 不屬於任何先前組的使用者的NOACCESS組。「**Simultaneous Login Per User**」欄位必須設定為0。



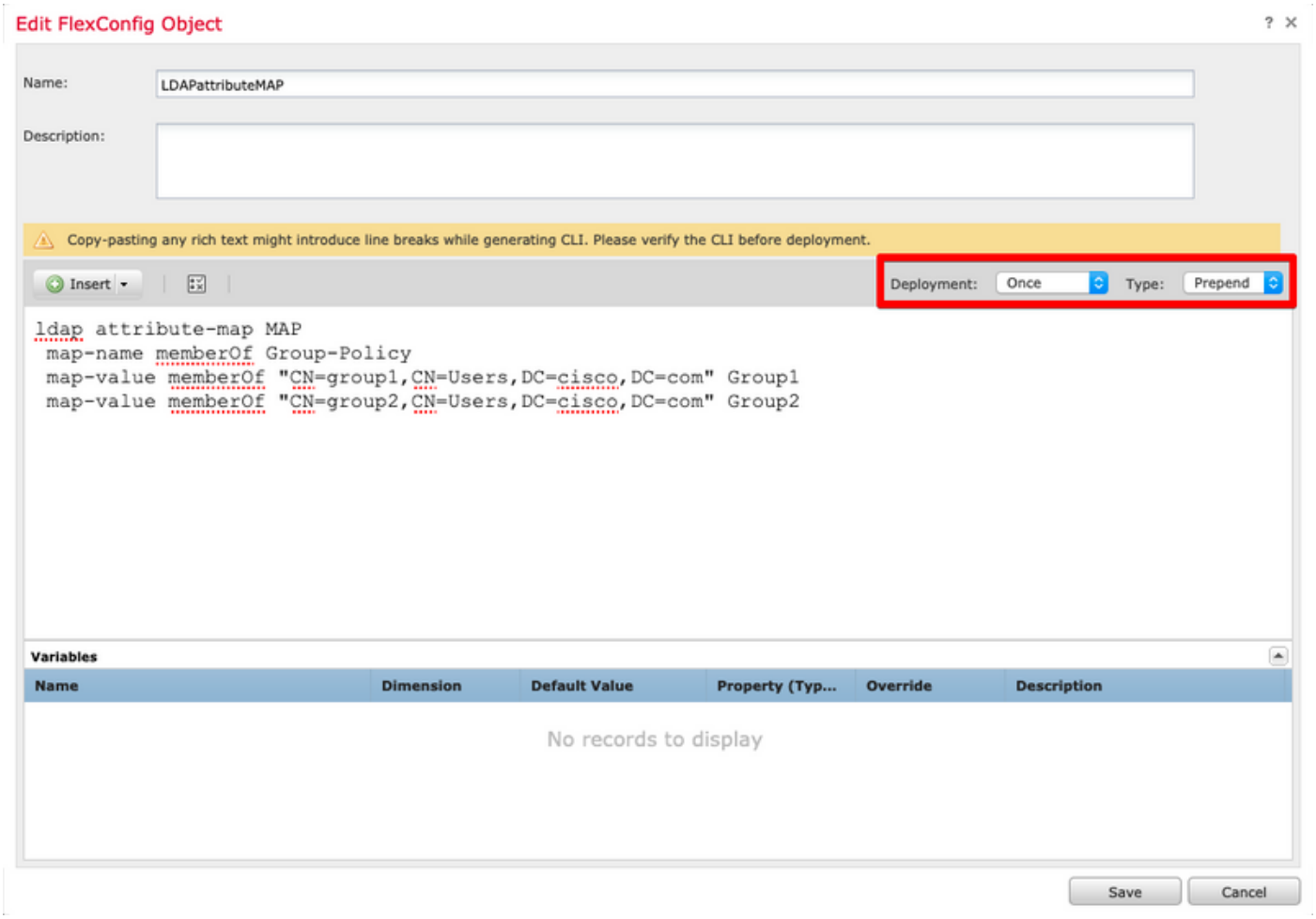
步驟4.將NOACCESS組策略分配給連線配置檔案。

步驟5.導覽至Object > Object Management t> FlexConfig > FlexConfig Object > Add FlexConfig Object。

步驟6.新增LDAP屬性對映配置所需的必要memberOf值。要從伺服器獲取組DN，可以使用命令「dsquery samid -group <group-name>」。

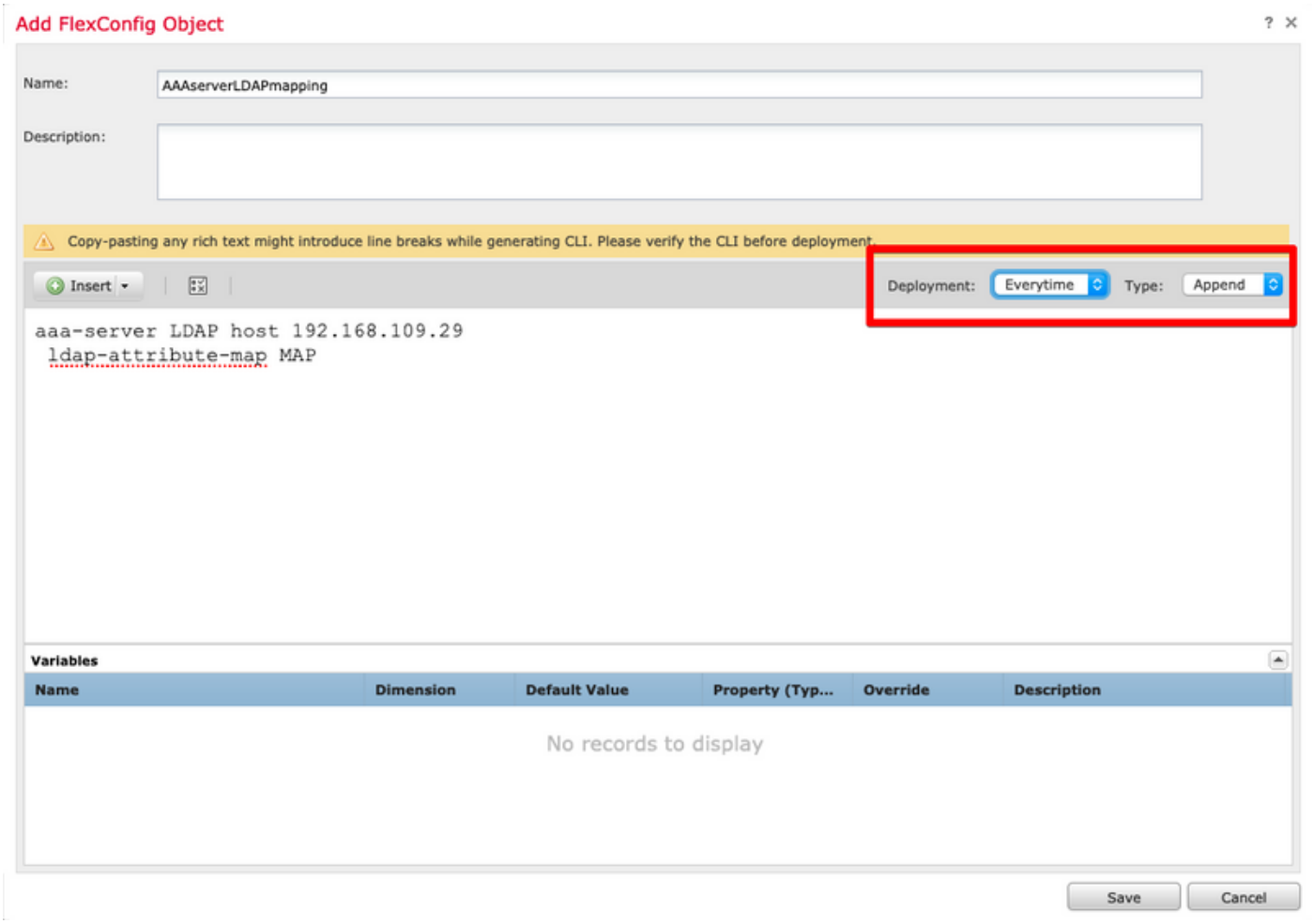
部署需要設定為*Once*，型別設定為*Prepend*。

提示：屬性名稱和值區分大小寫。如果對映未正確執行，請確保在LDAP屬性對映中對Cisco和LDAP屬性名稱和值使用了正確的拼寫和大寫。



步驟7.建立另一個 名為AAAserverLDAP對映的FlexConfig對象。此對象將屬性對映附加到aaa伺服器配置。

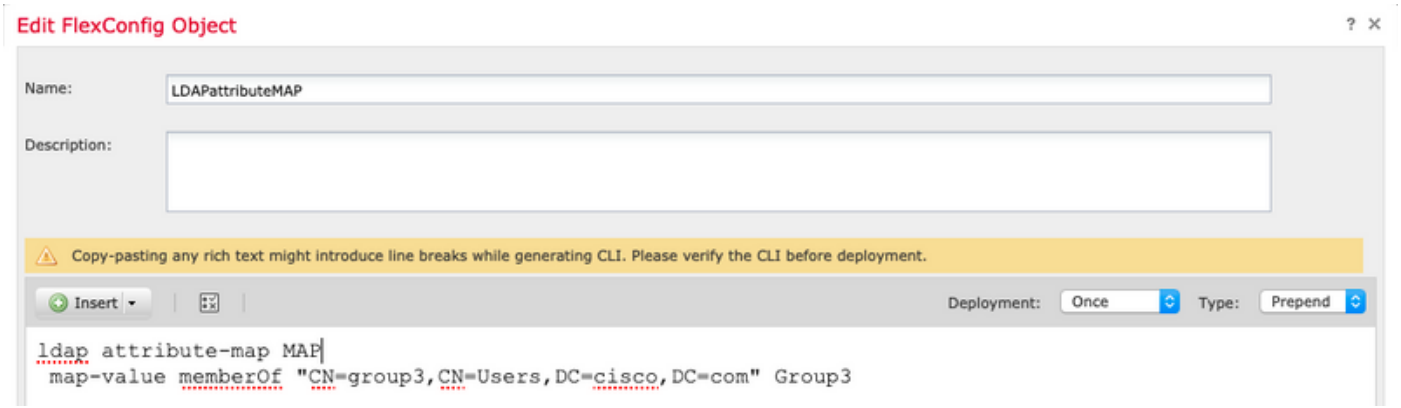
需要將Deployment值設定為*Everytime*，將Type設定為*Append*。



步驟8.導覽至Devices > FlexConfig > Edit current FlexConfig。 確保FlexConfig策略中FlexConfig對象的順序首先是LDAP屬性對映FlexConfig對象，然後是AAA伺服器對象。

步驟9.將配置部署到裝置，以將此配置傳送到受管裝置。

為了在LDAP對映中新增額外條目，請將現有的FlexConfig LDAPAtributeMAP對象修改為ONLY以包括新的對映值。



驗證

連線到FTD CLISH並發出這些命令，以確保已定義組上的使用者能夠連線。

```
> show vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect

Username     : cisco1                 Index        : 25
Assigned IP  : 10.10.10.1             Public IP    : 192.168.109.80
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 15820                  Bytes Rx     : 160
Group Policy : Group1                 Tunnel Group : AnyConnect
Login Time   : 16:02:45 UTC Tue Oct 9 2018
Duration     : 0h:00m:38s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 00000000000190005bbcd125
Security Grp : none                   Tunnel Zone  : 0


> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : cisco2                 Index        : 26
Assigned IP  : 11.11.11.1             Public IP    : 192.168.109.80
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 15820                  Bytes Rx     : 442
Group Policy : Group2                 Tunnel Group : AnyConnect
Login Time   : 16:04:12 UTC Tue Oct 9 2018
Duration     : 0h:00m:14s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 000000000001a0005bbcd17c
Security Grp : none                   Tunnel Zone  : 0
```

疑難排解

調試：

為了檢查LDAP事務，您可以使用這些debug命令。

```
> system support diagnostic-cli
debug ldap 250
debug aaa common 250
```

以下是每個debug命令成功輸出的範例。

```
firepower# debug ldap 250
debug ldap  enabled at level 250
firepower#
[49] Session Start
[49] New request Session, context 0x00002aaad332f100, reqType = Authentication
[49] Fiber started
[49] Creating LDAP context with uri=ldap://192.168.109.29:389
[49] Connect to LDAP server: ldap://192.168.109.29:389, status = Successful
[49] supportedLDAPVersion: value = 3
[49] supportedLDAPVersion: value = 2
```

```
[49] LDAP server 192.168.109.29 is Active directory
[49] Binding as AdminFTD
[49] Performing Simple authentication for AdminFTD to 192.168.109.29
[49] LDAP Search:
        Base DN = [DC=cisco,DC=com]
        Filter  = [samaccountname=cisco1]
        Scope   = [SUBTREE]
[49] User DN = [CN=cisco1,CN=Users,DC=cisco,DC=com]
[49] Talking to Active Directory server 192.168.109.29
[49] Reading password policy for cisco1, dn:CN=cisco1,CN=Users,DC=cisco,DC=com
[49] Read bad password count 1
[49] Binding as cisco1
[49] Performing Simple authentication for cisco1 to 192.168.109.29
[49] Processing LDAP response for user cisco1
[49] Message (cisco1):
[49] Authentication successful for cisco1 to 192.168.109.29
[49] Retrieved User Attributes:
[49]    objectClass: value = top
[49]    objectClass: value = person
[49]    objectClass: value = organizationalPerson
[49]    objectClass: value = user
[49]    cn: value = cisco1
[49]    givenName: value = cisco1
[49]    distinguishedName: value = CN=cisco1,CN=Users,DC=cisco,DC=com
[49]    instanceType: value = 4
[49]    whenCreated: value = 20181009153032.0Z
[49]    whenChanged: value = 20181009154032.0Z
[49]    displayName: value = cisco1
[49]    uSNCreated: value = 856333
[49]    memberOf: value = CN=group1,CN=Users,DC=cisco,DC=com
[49]            mapped to Group-Policy: value = Group1
[49]            mapped to LDAP-Class: value = Group1
[49]    uSNChanged: value = 856372
[49]    name: value = cisco1
[49]    objectGUID: value = .K.'..3N....Q...
[49]    userAccountControl: value = 66048
[49]    badPwdCount: value = 1
[49]    codePage: value = 0
[49]    countryCode: value = 0
[49]    badPasswordTime: value = 131835752510299209
[49]    lastLogoff: value = 0
[49]    lastLogon: value = 131835733331105504
[49]    pwdLastSet: value = 131835726324409149
[49]    primaryGroupID: value = 513
[49]    objectSid: value = .............E1.E.G..9..@s...
[49]    adminCount: value = 1
[49]    accountExpires: value = 9223372036854775807
[49]    logonCount: value = 0
[49]    sAMAccountName: value = cisco1
[49]    sAMAccountType: value = 805306368
[49]    userPrincipalName: value = cisco1@cisco.com
[49]    objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=cisco,DC=com
[49]    dSCorePropagationData: value = 20181009153316.0Z
[49]    dSCorePropagationData: value = 16010101000000.0Z
[49]    lastLogonTimestamp: value = 131835732321783732
[49] Fiber exit Tx=551 bytes Rx=2628 bytes, status=1
[49] Session End

firepower# debug aaa common 250
debug aaa common enabled at level 250
firepower# AAA API: In aaa_open
AAA session opened: handle = 31
AAA API: In aaa_process_async
```

```
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(0x00002b4ad7423b20) received message type 0
[31] AAA FSM: In AAA_StartAAATransaction
[31] AAA FSM: In AAA_InitTransaction

Initiating authentication to primary server (Svr Grp: LDAP-29)
-----------------------------------------------
[31] AAA FSM: In AAA_BindServer
[31] AAA_BindServer: Using server: 192.168.109.29
[31] AAA FSM: In AAA_SendMsg
User: cisco1
Resp:
callback_aaa_task: status = 1, msg =
[31] AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 31, pAcb = 0x00002aaad352bc80
AAA task: aaa_process_msg(0x00002b4ad7423b20) received message type 1
[31] AAA FSM: In AAA_ProcSvrResp

Back End response:
------------------
Authentication Status: 1 (ACCEPT)

[31] AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_PRIM_AUTHENTICATE, auth_status = ACCEPT
AAA_NextFunction: authen svr = LDAP-29, author svr = <none>, user pol = Group1, tunn pol =
NOACCESS
AAA_NextFunction: New i_fsm_state = IFSM_USER_GRP_POLICY,
[31] AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(Group1)
Got server ID 0 for group policy DB

Initiating user group policy lookup (Svr Grp: GROUP_POLICY_DB)
-----------------------------------------------
[31] AAA FSM: In AAA_BindServer
[31] AAA_BindServer: Using server: <Internal Server>
[31] AAA FSM: In AAA_SendMsg
User: Group1
Resp:
grp_policy_ioctl(0x00002b4ad31fd460, 114698, 0x00002b4ad7423430)
grp_policy_ioctl: Looking up Group1
callback_aaa_task: status = 1, msg =
[31] AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 31, pAcb = 0x00002aaad352bc80
AAA task: aaa_process_msg(0x00002b4ad7423b20) received message type 1
[31] AAA FSM: In AAA_ProcSvrResp

Back End response:
------------------
User Group Policy Status: 1 (ACCEPT)

[31] AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_USER_GRP_POLICY, auth_status = ACCEPT
AAA_NextFunction: New i_fsm_state = IFSM_TUNN_GRP_POLICY,
[31] AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(NOACCESS)
Got server ID 0 for group policy DB

Initiating tunnel group policy lookup (Svr Grp: GROUP_POLICY_DB)
-----------------------------------------------
[31] AAA FSM: In AAA_BindServer
[31] AAA_BindServer: Using server: <Internal Server>
[31] AAA FSM: In AAA_SendMsg
User: NOACCESS
Resp:
```

```
grp_policy_ioctl(0x00002b4ad31fd460, 114698, 0x00002b4ad7423430)
grp_policy_ioctl: Looking up NOACCESS
callback_aaa_task: status = 1, msg =
[31] AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 31, pAcb = 0x00002aaad352bc80
AAA task: aaa_process_msg(0x00002b4ad7423b20) received message type 1
[31] AAA FSM: In AAA_ProcSvrResp

Back End response:
------------------
Tunnel Group Policy Status: 1 (ACCEPT)

[31] AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY, auth_status = ACCEPT
dACL processing skipped: no ATTR_FILTER_ID found
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
[31] AAA FSM: In AAA_ProcessFinal
Checking simultaneous login restriction (max allowance=3) for user cisco1
Class attribute created from LDAP-Class attribute
[31] AAA FSM: In AAA_Callback
user attributes:
  1     User-Name(1)      6    "cisco1"
  2     User-Password(2)     13    (hidden)
  3     Group-Policy(4121)      6    "Group1"
  4     AAA-AVP-Table(4243)    1639    "g[06][00][00]$[00][00][00]x[01][00][00][8F][01][00][00]"
  5     DAP class attribute required(20510)      4    1
  6     LDAP-Class(20520)      7    "Group1[00]"

User Access-Lists:
user_acl[0] = NULL
user_acl[1] = NULL
user policy attributes:                              <--- Group-Policy Configuration (Group1)
  1     Filter-Id(11)      8    ""
  2     Session-Timeout(27)      4    0
  3     Idle-Timeout(28)      4    30
  4     Simultaneous-Logins(4098)      4    3
  5     Primary-DNS(4101)      4    IP: 0.0.0.0
  6     Secondary-DNS(4102)      4    IP: 0.0.0.0
  7     Primary-WINS(4103)      4    IP: 0.0.0.0
  8     Secondary-WINS(4104)      4    IP: 0.0.0.0
  9     Tunnelling-Protocol(4107)      4    96
 10     Banner(4111)      0    0x00002aaad49daa38   ** Unresolved Attribute **
 11     Split-Tunnel-Inclusion-List(4123)      8    ""
 12     Default-Domain-Name(4124)      0    0x00002aaad49daa41   ** Unresolved Attribute **
 13     Secondary-Domain-Name-List(4125)      0    0x00002aaad49daa42   ** Unresolved Attribute
**
 14     Split-Tunneling-Policy(4151)      4    0
 15     Group-giaddr(4157)      4    IP: 0.0.0.0
 16     WebVPN SVC Keepalive interval(4203)      4    20
 17     WebVPN SVC Client DPD period(4204)      4    30
 18     WebVPN SVC Gateway DPD period(4205)      4    30
 19     WebVPN SVC Rekey period(4206)      4    0
 20     WebVPN SVC Rekey method(4207)      4    0
 21     WebVPN SVC Compression(4208)      4    0
 22     WebVPN SVC Firewall Rule(4211)     17    "public#,private#,"
 23     WebVPN SVC DTLS Compression(4213)      4    0
 24     WebVPN SVC DTLS enable(4219)      4    1
 25     WebVPN SVC MTU(4221)      4    1406
 26     CVC-Modules(4223)      4    "dart"
 27     CVC-Profile(4224)     11    "FTD03#user,"
 28     CVC-Ask(4227)      4    2
 29     CVC-Ask-Timeout(4228)      4    0
 30     VLAN ID(4236)      4    0
 31     WebVPN Idle timeout alert interval(4244)      4    1
```

```
 32     WebVPN Session timeout alert interval(4245)      4    1
 33     List of address pools to assign addresses from(4313)      3    "SSL"
 34     SVC ignore DF bit(4326)      4    0
 35     Configure the behaviour of DNS queries by the client when Split tunneling is
enabled(4328)      4    0
 36     Primary-IPv6-DNS(4329)     16    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  37
Secondary-IPv6-DNS(4330)     16    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  38
Client Bypass Protocol(4331)      4    0
 39     IPv6-Split-Tunneling-Policy(4332)      4    0

User Policy Access-Lists:
user_acl[0] = NULL
user_acl[1] = NULL
tunnel policy attributes:                                    <--- Default Group-Policy
attributes (NOACCESS)
  1     Filter-Id(11)      8    ""
  2     Session-Timeout(27)      4    0
  3     Idle-Timeout(28)      4    30
  4     Simultaneous-Logins(4098)      4    0
  5     Primary-DNS(4101)      4    IP: 0.0.0.0
  6     Secondary-DNS(4102)      4    IP: 0.0.0.0
  7     Primary-WINS(4103)      4    IP: 0.0.0.0
  8     Secondary-WINS(4104)      4    IP: 0.0.0.0
  9     Tunnelling-Protocol(4107)      4    96
 10     Banner(4111)      0    0x00002aaad2580328   ** Unresolved Attribute **
 11     Group-Policy(4121)      8    "NOACCESS"
 12     Split-Tunnel-Inclusion-List(4123)      8    ""
 13     Default-Domain-Name(4124)      0    0x00002aaad2580331   ** Unresolved Attribute **
 14     Secondary-Domain-Name-List(4125)      0    0x00002aaad2580332   ** Unresolved Attribute
**
 15     Split-Tunneling-Policy(4151)      4    0
 16     Group-giaddr(4157)      4    IP: 0.0.0.0
 17     WebVPN SVC Keepalive interval(4203)      4    20
 18     WebVPN SVC Client DPD period(4204)      4    30
 19     WebVPN SVC Gateway DPD period(4205)      4    30
 20     WebVPN SVC Rekey period(4206)      4    0
 21     WebVPN SVC Rekey method(4207)      4    0
 22     WebVPN SVC Compression(4208)      4    0
 23     WebVPN SVC Firewall Rule(4211)     17    "public#,private#,"
 24     WebVPN SVC DTLS Compression(4213)      4    0
 25     WebVPN SVC DTLS enable(4219)      4    1
 26     WebVPN SVC MTU(4221)      4    1406
 27     CVC-Modules(4223)      4    "dart"
 28     CVC-Profile(4224)     11    "FTD03#user,"
 29     CVC-Ask(4227)      4    2
 30     CVC-Ask-Timeout(4228)      4    0
 31     VLAN ID(4236)      4    0
 32     WebVPN Idle timeout alert interval(4244)      4    1
 33     WebVPN Session timeout alert interval(4245)      4    1
 34     SVC ignore DF bit(4326)      4    0
 35     Configure the behaviour of DNS queries by the client when Split tunneling is
enabled(4328)      4    0
 36     Primary-IPv6-DNS(4329)     16    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  37
Secondary-IPv6-DNS(4330)     16    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  38
Client Bypass Protocol(4331)      4    0
 39     IPv6-Split-Tunneling-Policy(4332)      4    0

Tunnel Policy Access-Lists:
user_acl[0] = NULL
user_acl[1] = NULL

Auth Status = ACCEPT
aaai_internal_cb: handle is 31, pAcb is 0x00002aaad352bc80, pAcb->tq.tqh_first is
0x0000000000000000
```

```
AAA API: In aaa_close
Checking simultaneous login restriction (max allowance=3) for user cisco1
AAA task: aaa_process_msg(0x00002b4ad7423b20) received message type 2
In aaai_close_session (31)
AAA API: In aaa_send_acct_start
```