# تكوين تخطيط AnyConnect LDAP على الدفاع عن تهديد FirePOWER (FTD)

## المحتويات



## المقدمة

يقدم هذا المستند مثال لتكوين تخطيط بروتوكول الوصول إلى الدليل (LDAP) في الوضع Lightweight لمستخدمي AnyConnect على برنامج الدفاع عن تهديد FirePOWER (FTD) باستخدام سياسة FlexConfig لمركز إدارة Firepower (FMC). يتم إستخدام هذا التكوين للسماح للمستخدمين المحددين الذين ينتمون إلى مجموعة Active Directory (AD) بإنشاء اتصال شبكة خاصة ظاهرية (VPN). لن يتمكن المستخدمون من مجموعات AD المختلفة غير المعرفة على الخريطة من الاتصال بنفس ملف التعريف.

## المتطلبات الأساسية

### المتطلبات

cisco يوصي أن يتلقى أنت معرفة على هذا موضوع:

- تكوين نطاق الإعلان على FMC
- Windows Active Directory
- تكوين AnyConnect (SSLVPN) على FMC
- معرفة أساسية بكائنات FlexConfig على FMC

### المكونات المستخدمة

- FirePower Manager Center (FMC)، الإصدار 6.5.0 و 6.2.3
- FirePOWER Threat Defense (FTD)، الإصدار 6.5.0 و 6.2.3
- Windows Server مع Active Directory

## التكوين

### التكوين على FTD

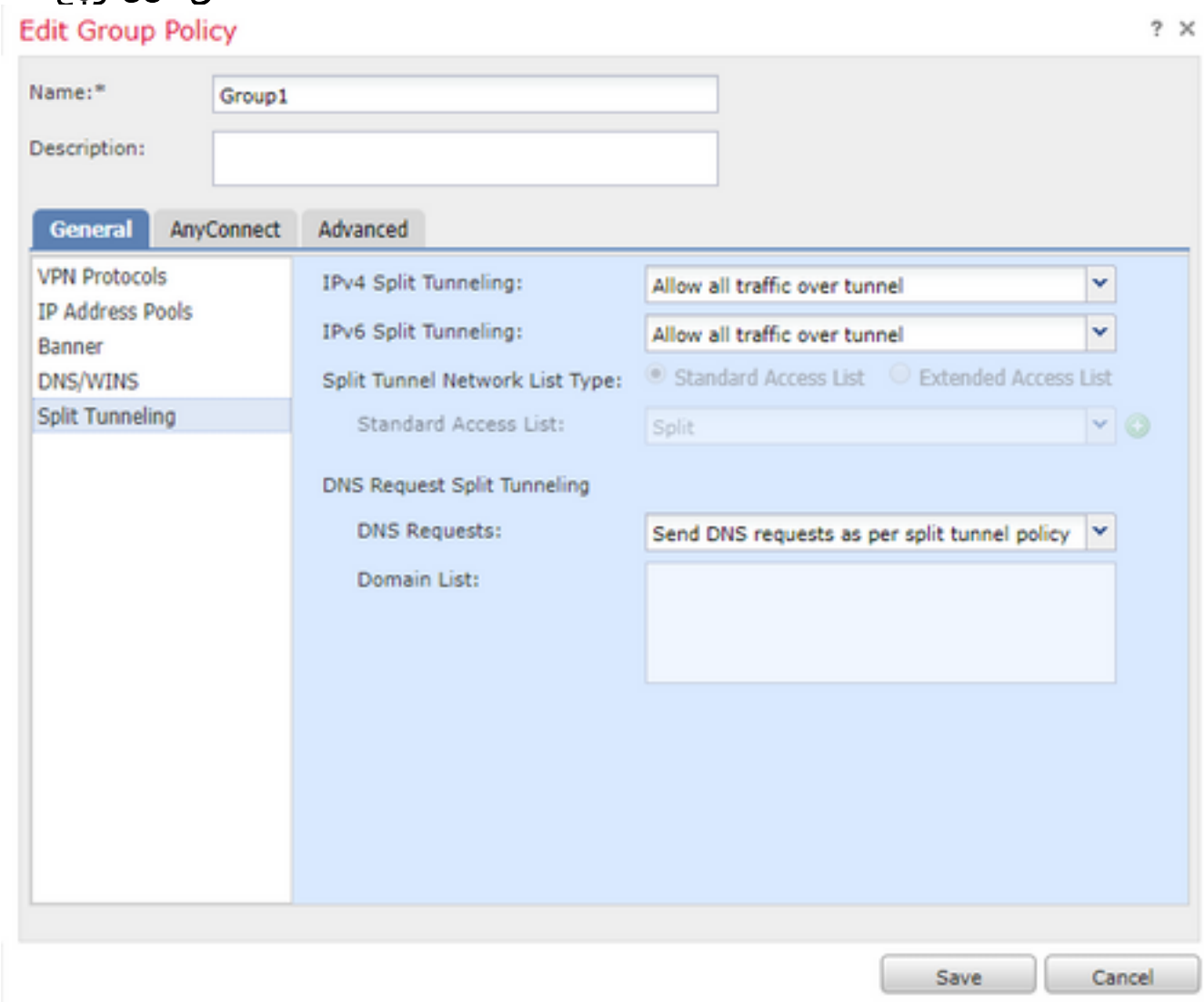
في هذا المثال، يستخدم المستخدمون الذين ينتمون إلى AD Group1 تكوين tunnel-all، بينما يملك المستخدمون الذين ينتمون إلى AD Group2 وصول محدود إلى مضيفين محددين. لا يمكن مصادقة كافة المستخدمين الآخرين الذين لا ينتمون إلى هذه المجموعات.

الخطوة 1. قم بتكوين AnyConnect باستخدام مصادقة LDAP ونشر التغييرات. يمكن العثور على مثال على هذا الدليل.

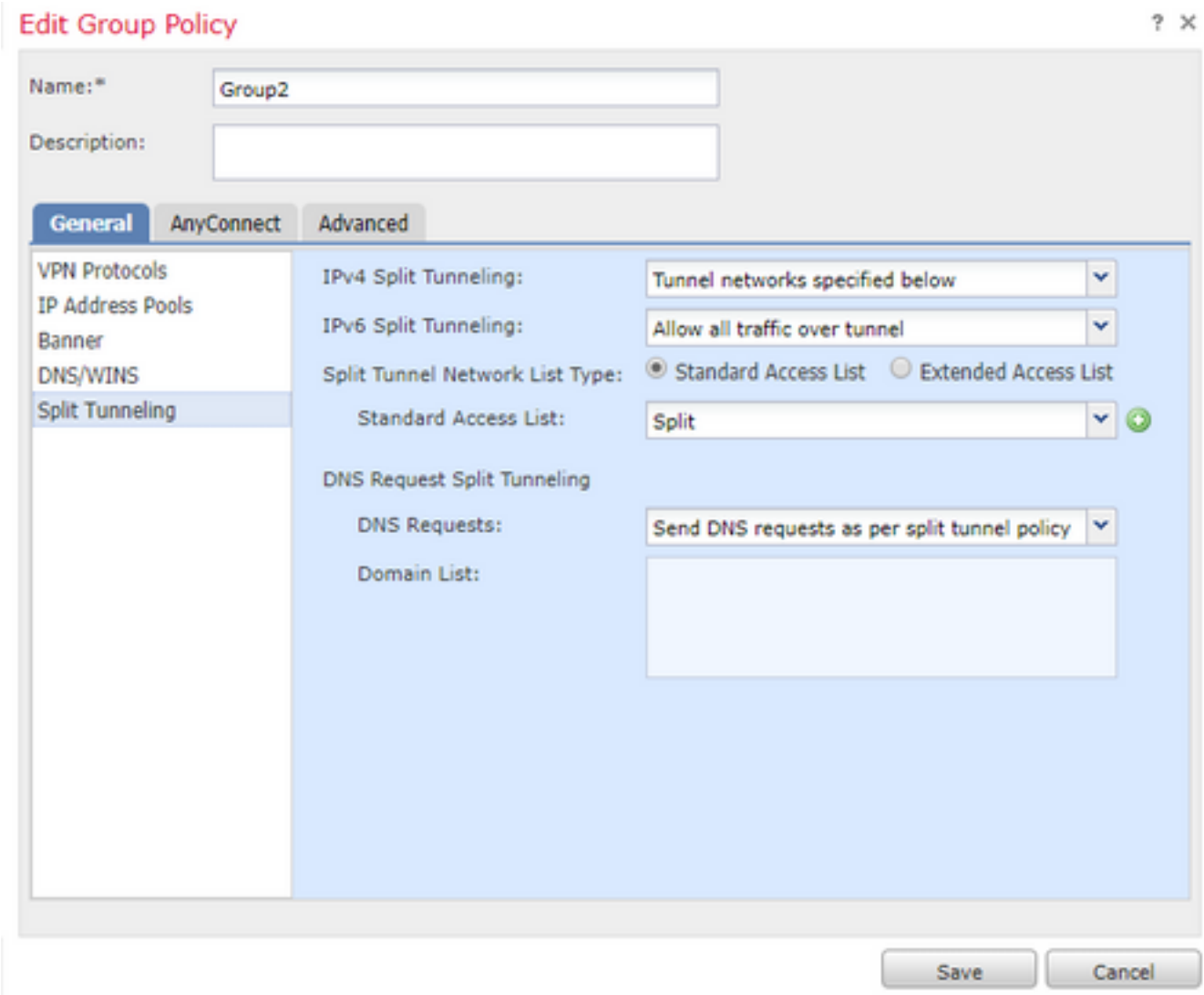
الخطوة 2. انتقل إلى الأجهزة > الوصول عن بعد > تحرير نهج AnyConnect > متقدم > نهج المجموعة.

الخطوة 3. إنشاء 3 نهج مجموعات مختلفة:

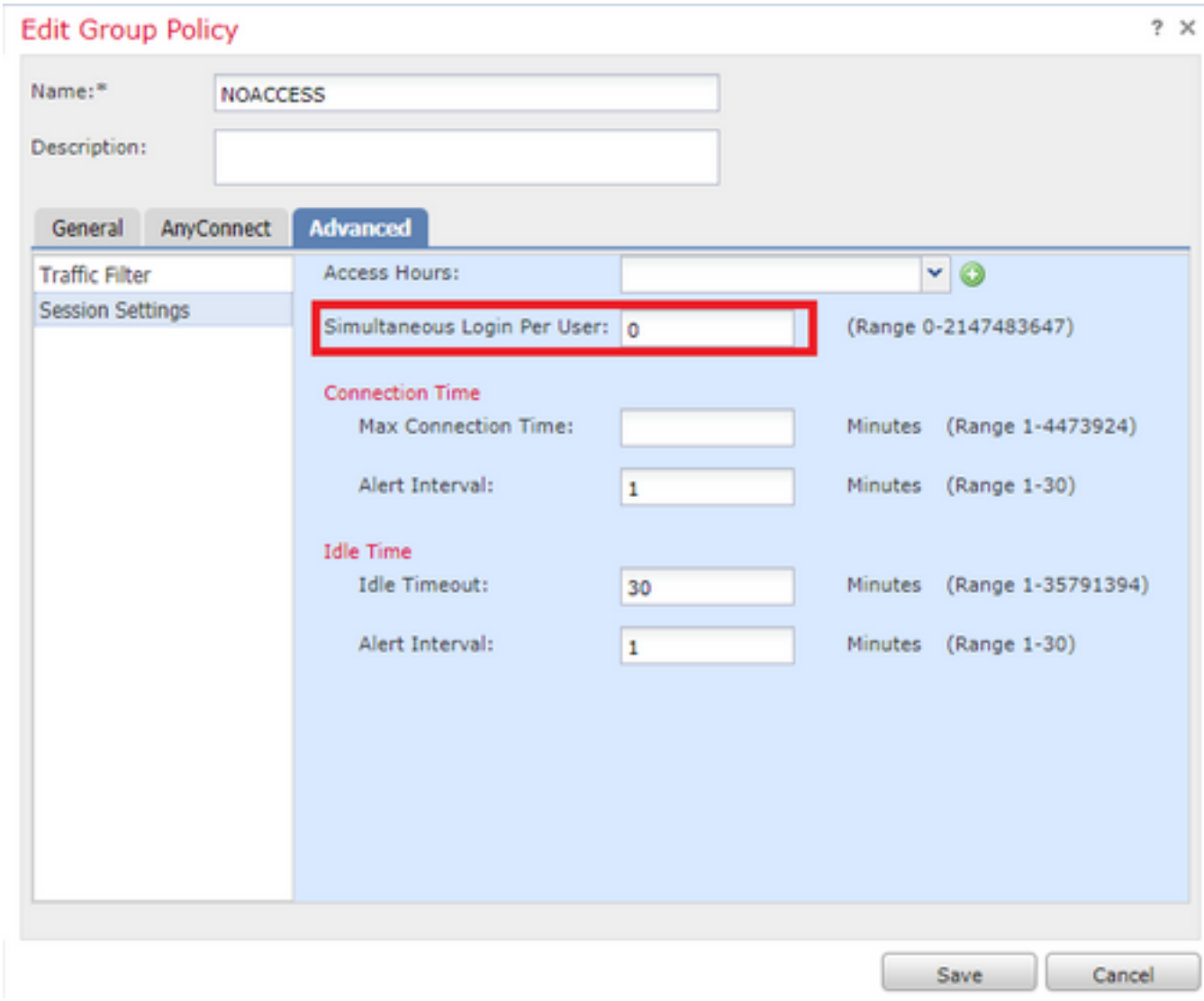
- تم تعيين المجموعة 1 مع تكوين انقسام الاتصال النفقي **للسماح لجميع حركة المرور عبر النفق.**




- تم تعيين المجموعة 2 مع تكوين تقسيم الاتصال النفقي إلى **انقسام.**




- مجموعة NoAccess للمستخدمين الذين لا ينتمون إلى أي من المجموعات السابقة. يجب تعيين **تسجيل الدخول المتزامن** للحقل **لكل مستخدم** على 0.



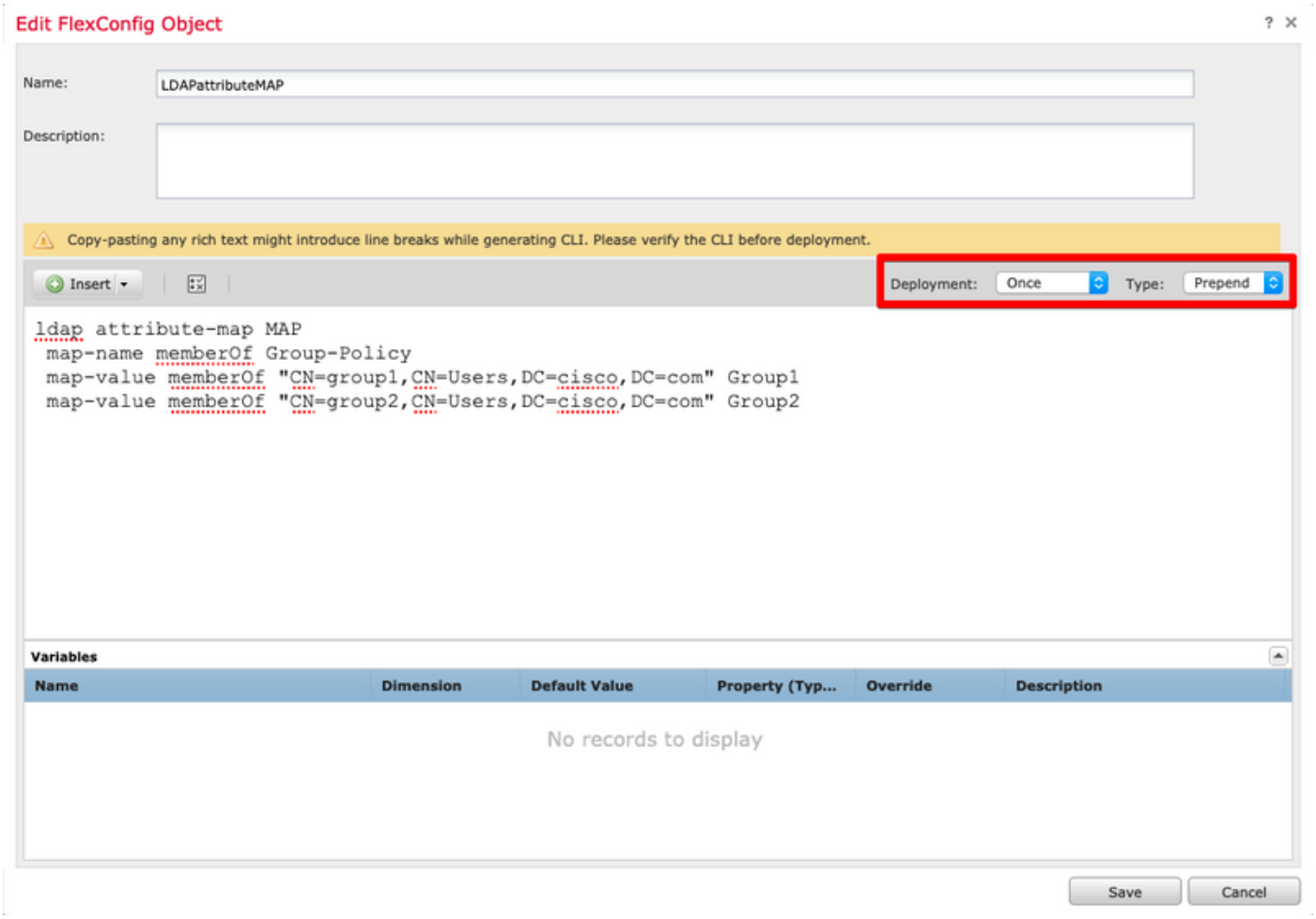

الخطوة 4. قم بتعيين نهج مجموعة NOACCESS لملف تعريف الاتصال.


الخطوة 5. انتقل إلى Object > Object Management T> FlexConfig > FlexConfig Object > إضافة FlexConfig Object.

الخطوة 6. قم بإضافة قيم memberOf الضرورية لتكوين تعيين سمة LDAP. للحصول على DN المجموعة من الخادم، يمكنك إستخدام الأمر "dsquery samid -group <group-name>".

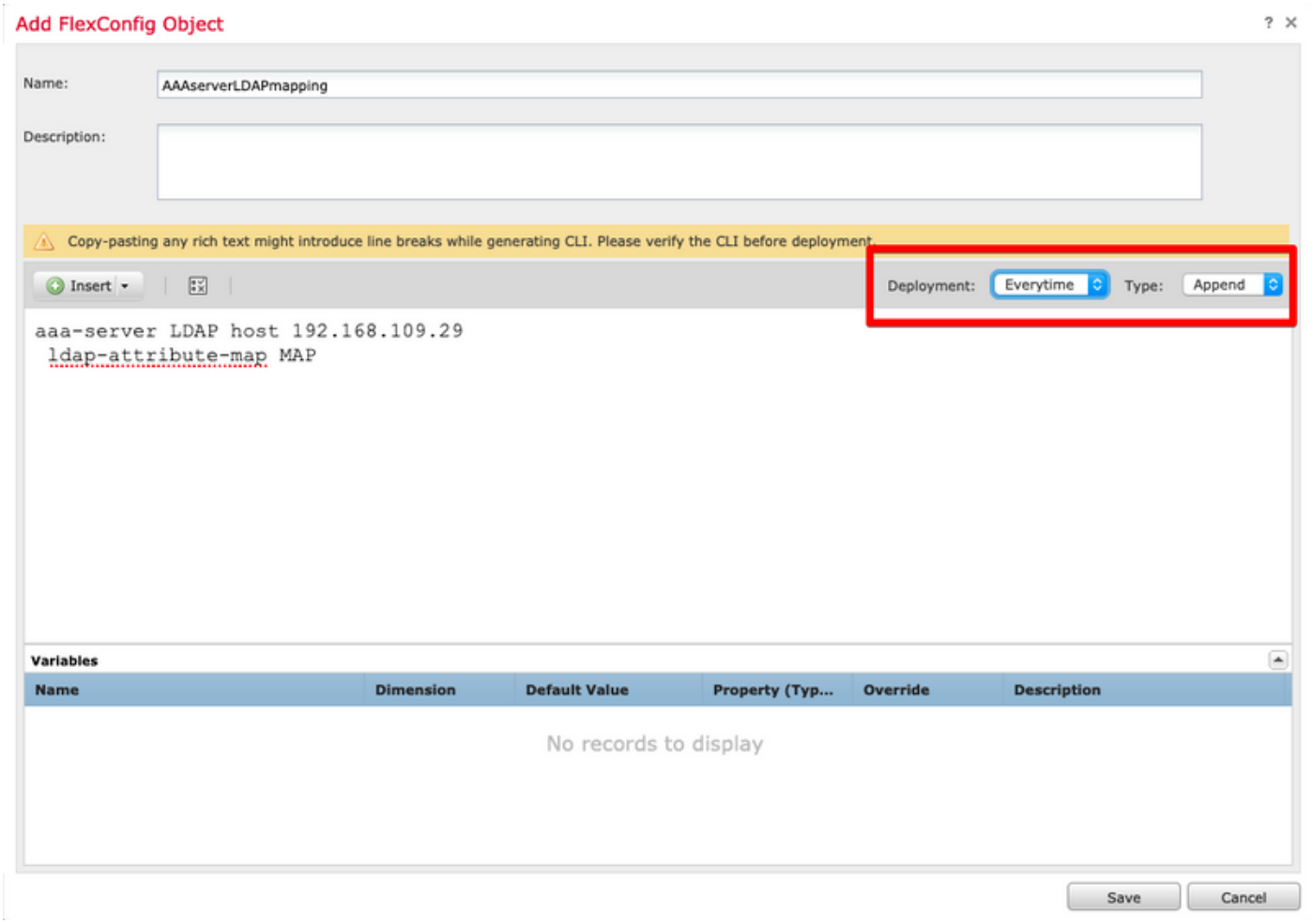
يجب تعيين النشر *مرة واحدة* وكتابة *مسبقا*.

**تلميح: أسماء السمات والقيم حساسة لحالة الأحرف. إذا لم يحدث التعيين بشكل صحيح، تأكد من إستخدام الإملاء الصحيح والتكبير في خريطة سمة LDAP لأسماء وقيم سمات Cisco و LDAP.**




الخطوة 7. إنشاء آخر FlexConfig Object المسمى AAAserverLDAPmapping. يقوم هذا الكائن بإرفاق مخطط السمة بتكوين AAA-server.

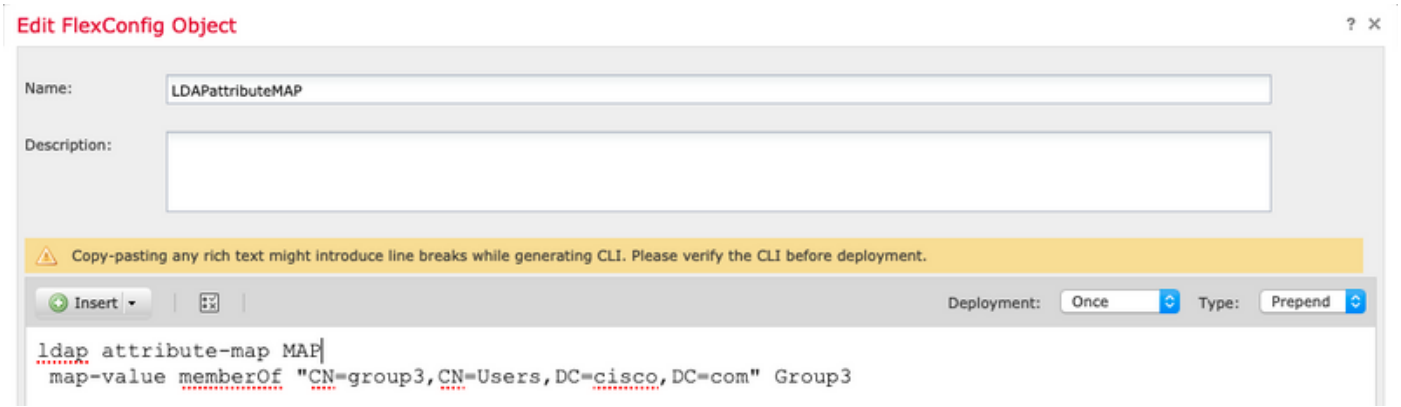
يجب تعيين قيم النشر على أنها *كل مرة* وكتابة على هيئة *إضافة*.




الخطوة 8. انتقل إلى الأجهزة > FlexConfig > Edit FlexConfig الحالي. تأكد من أن ترتيب كائنات FlexConfig في نهج FlexConfig هو أولا كائن FlexConfig الخاص بسمة LDAP المتبع بكائن AAA-server.

الخطوة 9. قم بنشر التكوين على الجهاز لإرسال هذا التكوين إلى الجهاز المدار.

لإضافة إدخال إضافي على خريطة LDAP، قم بتعديل كائن FlexConfig LDAPAtributeMAP الموجود لتضمين قيمة الخريطة الجديدة فقط.




# التحقق من الصحة

قم بالاتصال ب FTD CLISH وأصدر هذه الأوامر لضمان قدرة المستخدمين على المجموعات المحددة على الاتصال.

```
> 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
```

# استكشاف الأخطاء وإصلاحها

### تصحيح الأخطاء:

للتحقق من حركة LDAP، يمكنك إستخدام أوامر تصحيح الأخطاء هذه.

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

هذه أمثلة على الإخراج الناجح لكل أمر تصحيح أخطاء.

```
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
```

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).