

ASA J Secure Client VPN ىل ع LDAP ةم س ني عت ني وكت

تايوت حمل

ةمدقم

[تابلطت](#)

[Cisco نم ASA تابلطت](#)

[ةكبش ل تابلطت](#)

[لي م ع ل تابلطت](#)

[ةمدخت س م ل تان وكت](#)

[ني وكت ل ت اوطخ](#)

[ةومجم ل تاسا س دي دحت 1. ةوطخ](#)

[LDAP ةم س ني عت ني وكت 2. ةوطخ](#)

[LDAP AAA م داخ ني وكت 3. ةوطخ](#)

[قاف ن أ ل ةومجم دي دحت 4. ةوطخ](#)

[ةحص ل ت م ق قحت](#)

[VPN ةكبش ةس ل ج ني عت ت م ق قحت](#)

[اه ج ل ص او عا ط خ أ ل فاش ك ت س](#)

[LDAP عا ط خ أ ج ح ص ت ني ك م ت](#)

[VPN ل ا ص ت ا ع ب](#)

[عا ط خ أ ل ج ح ص ت ج ا ر خ ة ع ج ا ر م](#)

[ق قحت ل ا د ع ب عا ط خ أ ل ج ح ص ت ل ي ط ع ت](#)

[ة ع ي ا ش ل ا ت ا ل ك ش م ل](#)

ةمدقم

ةومجم تاسا س ني عت ل Cisco ASA ىل ع LDAP ةم س ني عت ني وكت دنت س م ل ا اذه فص ي Active Directory تاعومجم ل ا ا د ا ن ت س ا VPN.

تابلطت

Cisco نم ASA تابلطت

- موعدم جم ان رب رادص ل غ ش ي ذل ا Cisco نم ASA.
- ASA زا ه ج ل ا ي ر ا د ا ل ا ل و ص و ل ا.

ةكبش ل تابلطت

- ASA ل ب ق ن م ه ي ل ا ل و ص و ل ا ن ك م ي ي ذل ا (AD) Active Directory ل ا ج م .
- (636 ي ض ا ر ت ف ا ل ا ذ ف ن م ل ا) AD م داخ ىل ع ه ن ي و ك ت م ت (LDAPs) SSL ر ب ع LDAP .

ليعمل التابلت

- ليعمل أجهز على Secure Client تثبيت مت

مقدمة التابلت

عندما يتم تثبيت التابلت على جهازك، فإنه ينفذ عمليات التابلت.

عندما يتم تثبيت التابلت على جهازك، فإنه ينفذ عمليات التابلت. (يشار إليها). هناك إذا. حوسبة التابلت على جهازك، فإنه ينفذ عمليات التابلت. (يشار إليها). هناك إذا. حوسبة التابلت على جهازك، فإنه ينفذ عمليات التابلت.

تثبيت التابلت

مقدمة التابلت 1. التابلت

تاسيس التابلت على جهازك، فإنه ينفذ عمليات التابلت. (يشار إليها). هناك إذا. حوسبة التابلت على جهازك، فإنه ينفذ عمليات التابلت.

تاسيس التابلت على جهازك، فإنه ينفذ عمليات التابلت.

```
group-policy VPN_User_Policy internal
group-policy VPN_User_Policy attributes
  vpn-simultaneous-logins 3
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value SPLIT_TUNNEL_ACL
```

تاسيس التابلت على جهازك، فإنه ينفذ عمليات التابلت.

```
group-policy No_Access_Policy internal
group-policy No_Access_Policy attributes
  vpn-simultaneous-logins 0
```

LDAP التابلت 2. التابلت

تاسيس التابلت على جهازك، فإنه ينفذ عمليات التابلت. (يشار إليها). هناك إذا. حوسبة التابلت على جهازك، فإنه ينفذ عمليات التابلت.

```
ldap attribute-map VPN_Access_Map
  map-name memberOf Group-Policy
  map-value memberOf "CN=VPN_Users,OU=Groups,DC=example,DC=com" VPN_User_Policy
```

صيصنت تامالع يف LDAP ةومحمل (DN) زيمملا مسالا نيمضت امئاد بجي :ةظحالم
لا يف حيحص لكشب ةصاخ فورحو تافاسم رس في ASA لا نأ نمضي اذهو. (" ةجودزم
DN.

LDAP AAA مداخل نيوكت 3. ةوطخلا

ةومحمل لطختو ةقداصلل AD مداخل لاصلتالل ASA دادعاب مق

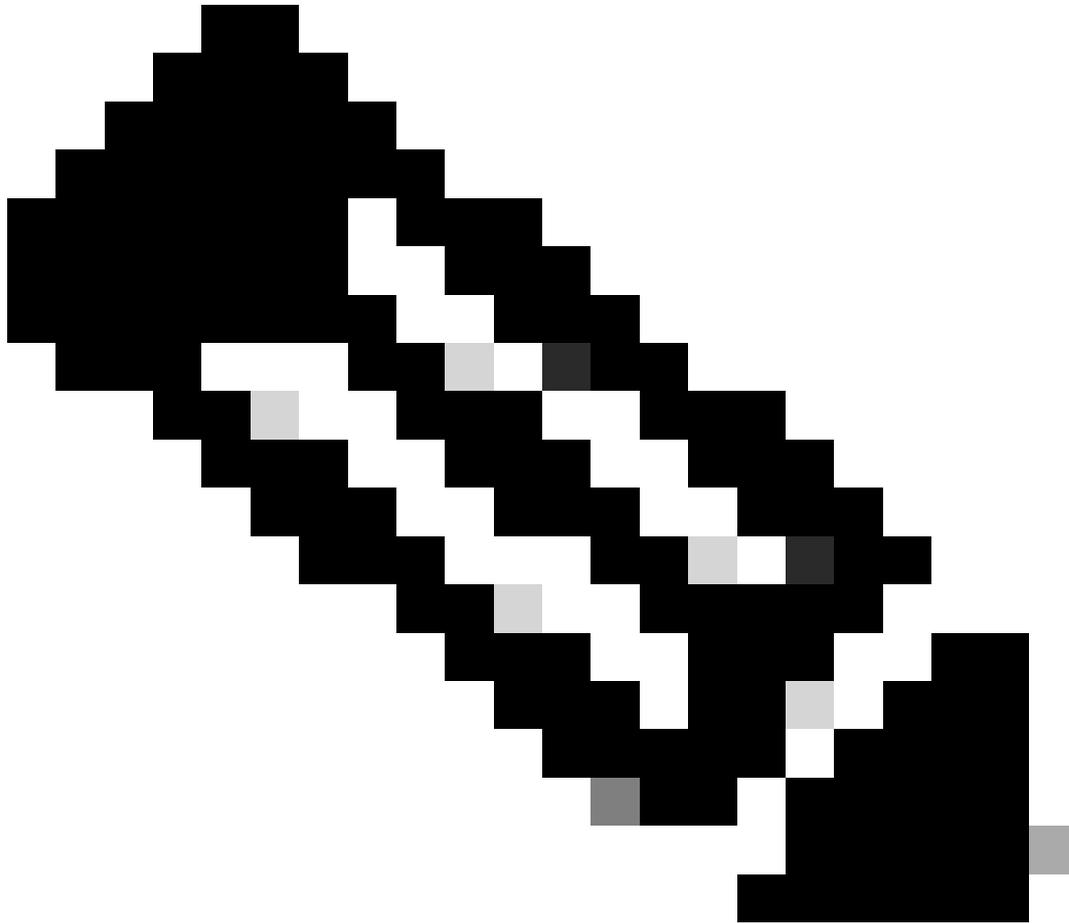
```
aaa-server AD_LDAP_Server protocol ldap
aaa-server AD_LDAP_Server (inside) host 192.168.1.10
  ldap-base-dn dc=example,dc=com
  ldap-scope subtree
  ldap-naming-attribute sAMAccountName
  ldap-login-password *****
  ldap-login-dn CN=ldap_bind_user,OU=Service Accounts,DC=example,DC=com
  ldap-over-ssl enable
  ldap-attribute-map VPN_Access_Map
```

قافنألة ةومجم ءي ءت 4. ةوطأل

LDAP مءاآب ةقءاصمءا طبرو VPN ءامءم ءي رءب قفنللة ةومجم موقت

```
tunnel-group VPN_Tunnel type remote-access
tunnel-group VPN_Tunnel general-attributes
  address-pool VPN_Pool
  authentication-server-group AD_LDAP_Server
  default-group-policy No_Access_Policy

tunnel-group VPN_Tunnel webvpn-attributes
  group-alias VPN_Tunnel enable
```



ضفر عم NO_ACCESS_POLICY لى ءي ضارءة فاللة ةومجمءا ءهن نبي ءمءة: ةظءالم LDAP ةمسل ةطيرء ربي ءم ءي ءم نوباطءي ال نبيءل نبيءءءسمءا لوصو

ةحصلا نم ققحتلا

ةومجملا جهن نييعة نم وحيحص لكشب ني مدختسملا ةقداصم نم ققحت ،دادعإلا لامكإ دعب ةبسانملا

VPN ةكبش ةسلج نييعة نم ققحتلا

```
show vpn-sessiondb anyconnect filter name
```

يلعفل رابتخال باسحب <username> لدبتسا

اهحالصإو اءاخألا فاشكتسا

اهحالصإو نيوكتلا اءاخأ فاشكتسال مسقلا اذه مدختسأ

LDAP اءاخأ حيحصت نيكمت

ءاخألا حيحصت نيكمتب مقف ،ةعقوتملا ةومجملا جهن نوقلتي نومدختسملا نكي مل اذإ لكاشملا ديدحتل

```
debug ldap 255
debug aaa common 255
debug aaa shim 255
```

VPN لاصتا ادب

Cisco Secure Client مادختساب لاصتال رابتخال مدختسم ةلواحم اءارحإ

ءاخألا حيحصت اءارحإ ةءءارم

ادانتسا حيحصلا ةومجملا جهنل مدختسملا نييعة نم دكأتلل Cisco ASA تالجم نم ققحت هب ةصاخلا Active Directory (AD) ةومجم ةيوضع ىلا

ققحتلا دعب اءاخألا حيحصت ليطعت

```
undebug all
```

ةعئاشللال تالكشملال

ةمقق تارابع يف AD ةومجم ءامسأ نأ نم دكأت . فرألال ةلأجل ةساسح LDAP ةمس تانققعت ةلأجل ةساسح كذل يف امب ، امامت ةقباطم ةطققلال

امئاد فرقتلال مقق ال . ةددملال AD تاعومجم يف نورشابم ءاضأ مه نققم دقتسملال نأ نم ققتت لقققتلال يف لكاشم ثودح للاق دؤقق امم ، ةلأدملال ةومجملال تاقوضع لعل

ةومجملال ةساقس ةطققلال ةمقق رققاقم نم يقأ عم نوقباطتق ال نققذل نوم دقتسملال لقققتللق لوصولل عنمقق امم ، (ةلأجل هذقق يف NO_ACCESS_POLICY) ةققضارتقال

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا