



## تكوين اسم مستعار وتمكين القائمة المنسدلة

في هذا القسم، تقدم لك معلومات تكوين اسم مستعار لملف تعريف اتصال (مجموعة أنفاق) ثم تكوين هذه الأسماء المستعارة لتظهر في القائمة المنسدلة "مجموعة" في صفحة تسجيل الدخول إلى WebVPN.

### ASDM

أكمل هذه الخطوات لتكوين اسم مستعار لملف تعريف اتصال (مجموعة نفق) في ASDM. كرر حسب الضرورة لكل مجموعة تريد تكوين اسم مستعار لها.

1. أختار تكوين < وصول SSL VPN دون عميل < توصيفات الاتصال.
2. حدد توصيف توصيل وانقر على تحرير.
3. أدخل اسما مستعارا في حقل الأسماء المستعارة.

The screenshot shows the 'Edit Clientless SSL VPN Connection Profile' dialog box for 'ExampleGroup1'. The 'Name' field contains 'ExampleGroup1' and the 'Aliases' field contains 'Group1'. Under the 'Authentication' section, the 'Method' is set to 'AAA'. The 'AAA Server Group' is set to 'LOCAL'. There is a checkbox for 'Use LOCAL if Server Group fails' which is currently unchecked. Under the 'Default Group Policy' section, the 'Group Policy' is set to 'DfltGrpPolicy'. The 'Clientless SSL VPN Protocol' is checked and set to 'Enabled'. The dialog has 'OK', 'Cancel', and 'Help' buttons at the bottom.

4. طقطقت OK وطبقت التغيير.
5. في إطار توصيفات التوصيل، تحقق من السماح للمستخدم بتحديد اتصال معرف باسم مستعار في الجدول أعلاه في صفحة تسجيل الدخول.

**Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**

Configure Clientless SSL VPN access parameters.

**Access Interfaces**  
Enable interfaces for clientless SSL VPN access, and indicate whether to require a certificate for access.

Interface	Allow Access	Require Client Certificate
outside	<input checked="" type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

Access Port:

Click here to [Assign Certificate to Interface](#).

**Connection Profiles**  
Connection profile (tunnel group) table below contains records that determine connection policies. A record identifies a default group policy for the connection and contains protocol-specific connection parameters.

Name	Aliases	Clientless SSL VPN Protocol	Group Policy
DefaultRAGroup		Enabled	DfltGrpPolicy
DefaultWEBVPNGroup		Enabled	DfltGrpPolicy
ExampleGroup1	Group1	Enabled	DfltGrpPolicy
ExampleGroup2	Group2	Enabled	DfltGrpPolicy

Allow user to select connection, identified by alias in the table above, at login page  
 Allow user to enter internal password at login page

## CLI

أستخدم هذه الأوامر في سطر الأوامر لتكوين اسم مستعار لملف تعريف اتصال (مجموعة النفق) وتمكين القائمة المنسدلة لمجموعة النفق. كرر حسب الضرورة لكل مجموعة تريد تكوين اسم مستعار لها.

```

ciscoasa#configure terminal
ciscoasa(config)#tunnel-group ExampleGroup1 webvpn-att
ciscoasa(config-tunnel-webvpn)#group-alias Group1 enable
ciscoasa(config-tunnel-webvpn)#exit
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#tunnel-group-list enable

```

## تكوين عنوان URL وتمكين القائمة المنسدلة

في هذا القسم، تقدم لك معلومات تكوين عنوان URL لملف تعريف اتصال (مجموعة أنفاق) ثم تكوين عناوين URL هذه للظهور في القائمة المنسدلة "مجموعة" في صفحة تسجيل الدخول إلى WebVPN. إحدى ميزات استخدام عنوان URL الخاص بالمجموعة عبر الاسم المستعار للمجموعة (القائمة المنسدلة للمجموعة) هي أنك لا تكشف أسماء المجموعة كما هو الحال بالنسبة للأسلوب الأخير.

## ASDM



```
ciscoasa(config)#tunnel-group Trusted-Employees type remote-access
ciscoasa(config)#tunnel-group Trusted-Employees general-attributes
ciscoasa(config)#authentication-server-group (inside) LDAP-AD11
ciscoasa(config)#accounting-server-group RadiusACS12
ciscoasa(config)#default-group-policy Employees
ciscoasa(config)#tunnel-group Trusted-Employees webvpn-attributes
ciscoasa(config)#group-url https://asa-vpn1.companyA.com/Employees enable
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#tunnel-group-list enable
```

## س و أ

سؤال:

كيف يمكنك تكوين عنوان URL الخاص بالمجموعة إذا كانت عبارة ASA VPN خلف جهاز nat؟

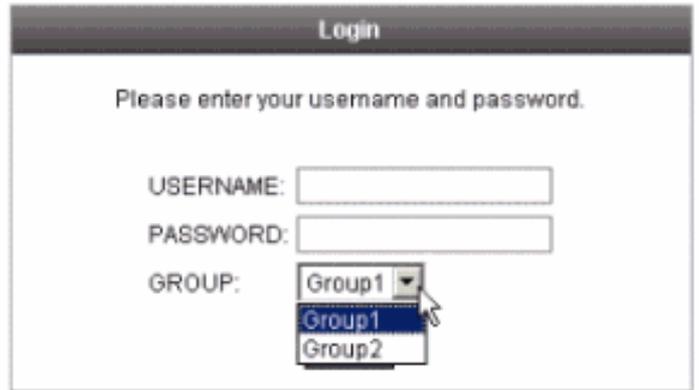
الجواب:

سيتم استخدام المضيف/عنوان URL الذي يقوم المستخدم بإدخاله لتعيين المجموعة. لذلك، أنت ينبغي استعملت ال nat\_d عنوان، ليس العنوان حقيقي على ال ASA قارن خارجي. أفضل بديل هو استخدام FQDN بدلا من عنوان IP لتعيين عنوان URL الخاص بالمجموعة.

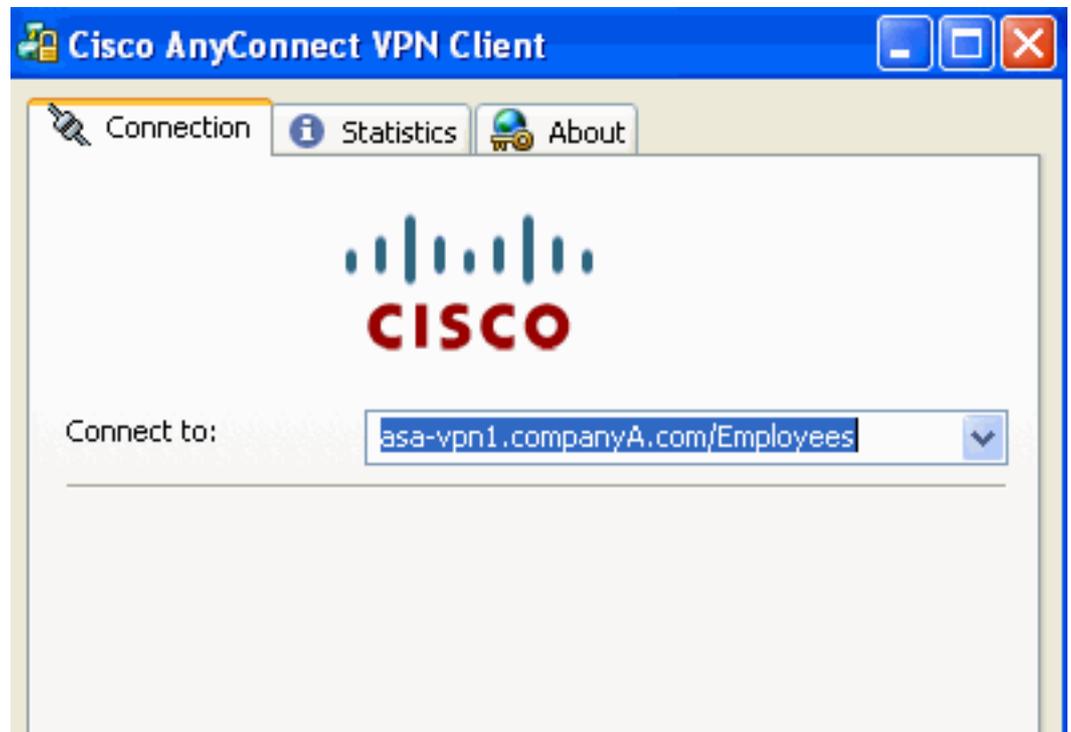
يتم تنفيذ كافة التعيينات على مستوى بروتوكول HTTP (استنادا إلى المعلومات التي يرسلها المستعرض) ويتم تكوين URL لتعيين من المعلومات الموجودة في رؤوس HTTP الواردة. يتم أخذ اسم المضيف أو IP من رأس المضيف وبقيّة عنوان URL من سطر طلب HTTP. هذا يعني أنه سيتم استخدام المضيف/عنوان URL الذي يقوم المستخدم بإدخاله لتعيين المجموعة.

## التحقق من الصحة

انتقل إلى صفحة تسجيل الدخول إلى WebVPN الخاصة ب ASA للتحقق من تمكين القائمة المنسدلة ومن ظهور الأسماء المستعارة.



انتقل إلى صفحة تسجيل الدخول إلى WebVPN الخاصة بـ ASA للتحقق من تمكين القائمة المنسدلة ومن ظهور عنوان URL.



### استكشاف الأخطاء وإصلاحها

- إذا لم تظهر القائمة المنسدلة، تأكد من تمكينها ومن تكوين الأسماء المستعارة. غالباً ما يقوم المستخدمون بأحد هذه الأشياء، لكن ليس الآخر.
- تأكد من إتصالك بعنوان URL الأساسي لـ ASA. لا تظهر القائمة المنسدلة إذا قمت بالاتصال بـ ASA باستخدام

عنوان URL لمجموعة، حيث أن الغرض من عنوان URL للمجموعة هو تنفيذ تحديد المجموعة.

## معلومات ذات صلة

- [أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن مة و مچم مادخت ساب دن تسمل اذ ه Cisco ت مچرت  
ملاعلاء ان أ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ي رش ب ل و  
امك ة ق ي قد ن و ك ت ن ل ة ل آل ة مچرت ل ض ف أن ة ظ حال م ي ج ر ي . ة ص ا خ ل 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 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 أ ل ا ي ز ي ل ج ن إ ل ا دن تسمل ا