

# دليل (WebVPN) لجمع نودب SSL VPN نيوكت ASA

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [التكوين](#)
- [الرسم التخطيطي للشبكة](#)
- [معلومات أساسية](#)
- [التكوين](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [الإجراءات المستخدمة لاستكشاف الأخطاء وإصلاحها](#)
- [الأوامر المستخدمة لاستكشاف الأخطاء وإصلاحها](#)
- [مشاكل مشتركة](#)
- [تتعد على المستخدم تسجيل الدخول](#)
- [تتعدر توصيل أكثر من ثلاثة مستخدمي WebVPN ب ASA](#)
- [تتعدر على عملاء WebVPN الوصول إلى الإشارات المرجعية ويتم سحبها للخارج](#)
- [اتصال Citrix من خلال WebVPN](#)
- [كيفية تجنب الحاجة إلى مصادقة ثانية للمستخدمين](#)
- [معلومات ذات صلة](#)

## المقدمة

يقدم هذا المستند تكوين مباشر لسلسلة جهاز الأمان القابل للتكيف (ASA 5500) من Cisco للسماح بوصول طبقة مأخذ التوصيل الأمانة (SSL) الخاصة الظاهرية (VPN) دون عميل إلى موارد الشبكة الداخلية. تسمح الشبكة الخاصة الظاهرية (WebVPN) لشبكة SSL التي لا تحتوي على عملاء بالوصول المحدود والأمن في الوقت نفسه من أي موقع إلى شبكة الشركة. يستطيع المستخدمون تحقيق وصول آمن قائم على المستعرض إلى موارد الشركة في أي وقت. لا حاجة إلى عميل إضافي للحصول على إمكانية الوصول إلى الموارد الداخلية. يتم توفير الوصول باستخدام بروتوكول نقل النص التشعبي عبر اتصال SSL.

يوفر SSL VPN الذي لا يحتاج إلى عملاء إمكانية الوصول الآمن والسهل إلى مجموعة كبيرة من موارد الويب والتطبيقات التي تم تمكين الويب بها والتطبيقات القديمة من أي كمبيوتر تقريبا يمكنه الوصول إلى مواقع بروتوكول نقل النص التشعبي على الإنترنت (HTTP). ويشمل ذلك ما يلي:

- مواقع ويب داخلية
- Microsoft SharePoint 2003 و 2007 و 2010
- Microsoft Outlook Web Access 2003 و 2007 و 2013

- Microsoft Outlook Web App 2010
- 8.5.1 و Domino Web Access (DWA) 8.5
- Citrix Metaframe Presentation Server 4.x
- Citrix XenApp الإصدار 5 إلى 6.5
- Citrix XenDesktop الإصدار 5 إلى 5.6 و 7.5
- VMware View 4

يمكن العثور على قائمة بالبرامج المدعومة في [أنظمة VPN الأساسية المدعومة، سلسلة Cisco ASA 5500](#).

## المتطلبات الأساسية

### المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- المستعرض الذي يدعم SSL
  - ASA مع الإصدار 7.1 أو أعلى
  - تم إصدار شهادة X.509 إلى اسم مجال ASA
  - منفذ TCP رقم 443، والذي يجب ألا يتم حظره على طول المسار من العميل إلى ASA
- يمكن العثور على القائمة الكاملة للمتطلبات في [أنظمة VPN الأساسية المدعومة، سلسلة Cisco ASA 5500](#).

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- ASA، الإصدار 9.4(1)
- Adaptive Security Device Manager (ASDM)، الإصدار 7.4(2)
- ASA 5515-X

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

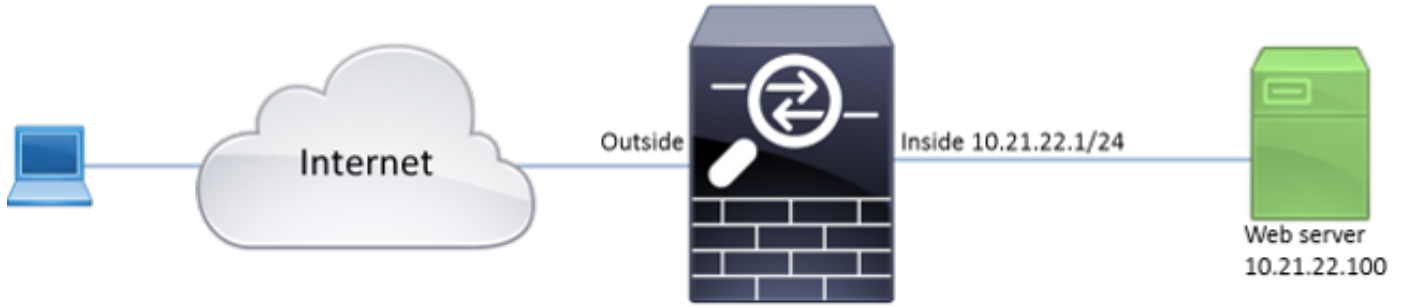
## التكوين

تصف هذه المقالة عملية التكوين لكل من ASDM و CLI. يمكنك إختيار اتباع أي من الأدوات لتكوين WebVPN، ولكن يمكن تحقيق بعض خطوات التكوين فقط باستخدام ASDM.

ملاحظة: أستخدم [أداة بحث الأوامر](#) (للعلماء [المسجلين](#) فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

### الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



## معلومات أساسية

يستخدم WebVPN بروتوكول SSL لتأمين البيانات التي تم نقلها بين العميل والخادم. عندما يقوم المستعرض بتهيئة اتصال مع ASA، يقدم ASA شهادته لمصادقة نفسه على المستعرض. لضمان تأمين الاتصال بين العميل و ASA، يلزمك تزويد ASA بالشهادة الموقعة من قبل المرجع المصدق والتي يثق فيها العميل بالفعل. وإلا فلن يكون لدى العميل الوسائل التي تمكنه من التحقق من أصالة ASA مما يؤدي إلى احتمال هجوم الدخيل وتجربة المستخدم الضعيفة، وذلك لأن المستعرض يصدر تحذيراً بأن الاتصال غير موثوق به.

**ملاحظة:** يقوم ASA بشكل افتراضي بإنشاء شهادة X.509 ذاتية التوقيع عند بدء التشغيل. يتم استخدام هذه الشهادة لخدمة اتصالات العميل بشكل افتراضي. لا يوصى باستخدام هذه الشهادة لأنه لا يمكن التحقق من أصالتها بواسطة المستعرض. علاوة على ذلك، يتم إعادة إنشاء هذه الشهادة على كل عملية إعادة تشغيل. حيث تتغير بعد كل عملية إعادة تشغيل.

تثبيت الشهادة خارج نطاق هذا المستند.

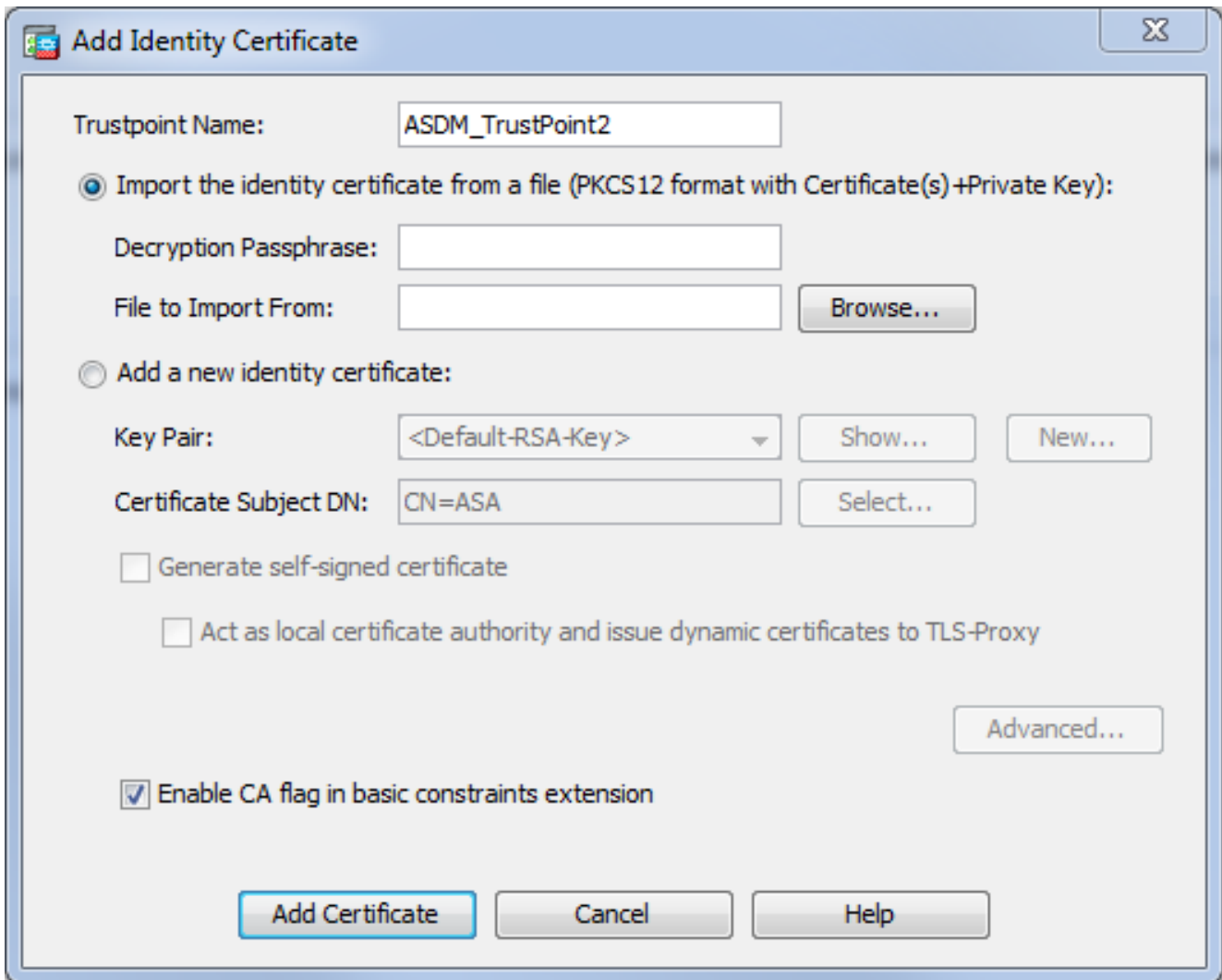
## التكوين

قم بتكوين WebVPN على ASA بخمس خطوات رئيسية:

- قم بتكوين الشهادة التي سيتم استخدامها من قبل ASA.
- تمكين WebVPN على واجهة ASA.
- قم بإنشاء قائمة بالخوادم و/أو محدد موقع الموارد الموحد (URL) للوصول إلى WebVPN.
- إنشاء نهج مجموعة لمستخدمي WebVPN.
- تطبيق نهج المجموعة الجديد على مجموعة نفق.

**ملاحظة:** في إصدارات ASA الأحدث من الإصدار 9.4، تم تغيير الخوارزمية المستخدمة لاختيار شفرة SSL (راجع [ملاحظات الإصدار الخاصة بسلسلة Cisco ASA، الإصدار 9.4\(x\)](#)). إذا كان سيتم استخدام العملاء القادرين على المنحنى الاهليلجي فقط، فمن الأمان استخدام مفتاح المنحنى الاهليلجي الخاص للشهادة. وإلا يجب استخدام مجموعة التشفير المخصصة لتجنب تقديم ASA لشهادة مؤقتة موقعة ذاتياً. يمكنك تكوين ASA لاستخدام شفرة RSA فقط مع تشفير SSL التشفير "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5".

1. الخيار 1 - إستيراد الشهادة مع ملف PKCS12. أخطر تشكيل < جدار الحماية > متقدم < إدارة الشهادات > شهادات الهوية < إضافة >. يمكنك تثبيته باستخدام ملف PKCS12 أو لصق المحتويات في تنسيق "البريد المحسن للخصوصية" (PEM).



:CLI

```
"ASA(config)# crypto ca import TrustPoint-name pkcs12 "password
```

```

        .Enter the base 64 encoded pkcs12
        :End with the word "quit" on a line by itself
MIIJUQIBAzCCCRcGCSqGSIb3DQEHAaCCCQgEggkEMIIJADCCBF8GCSqGSIb3DQEH
BqCCBFawggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI8F3N
vkvjUgCAggAgIIFuHFrv6enVflNv3sBByB/yZswhELY5KpeALbXhfrFDpLNncAB+
/z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x3Ozo0JjxSAafmTWqDOEOS
7mHsaKMoao+pv2LqKTWh007No4Ycx75Y5sOhyuQGPhLJRdionbils1ioe4Dplx1b

```

--- output omitted ---

```

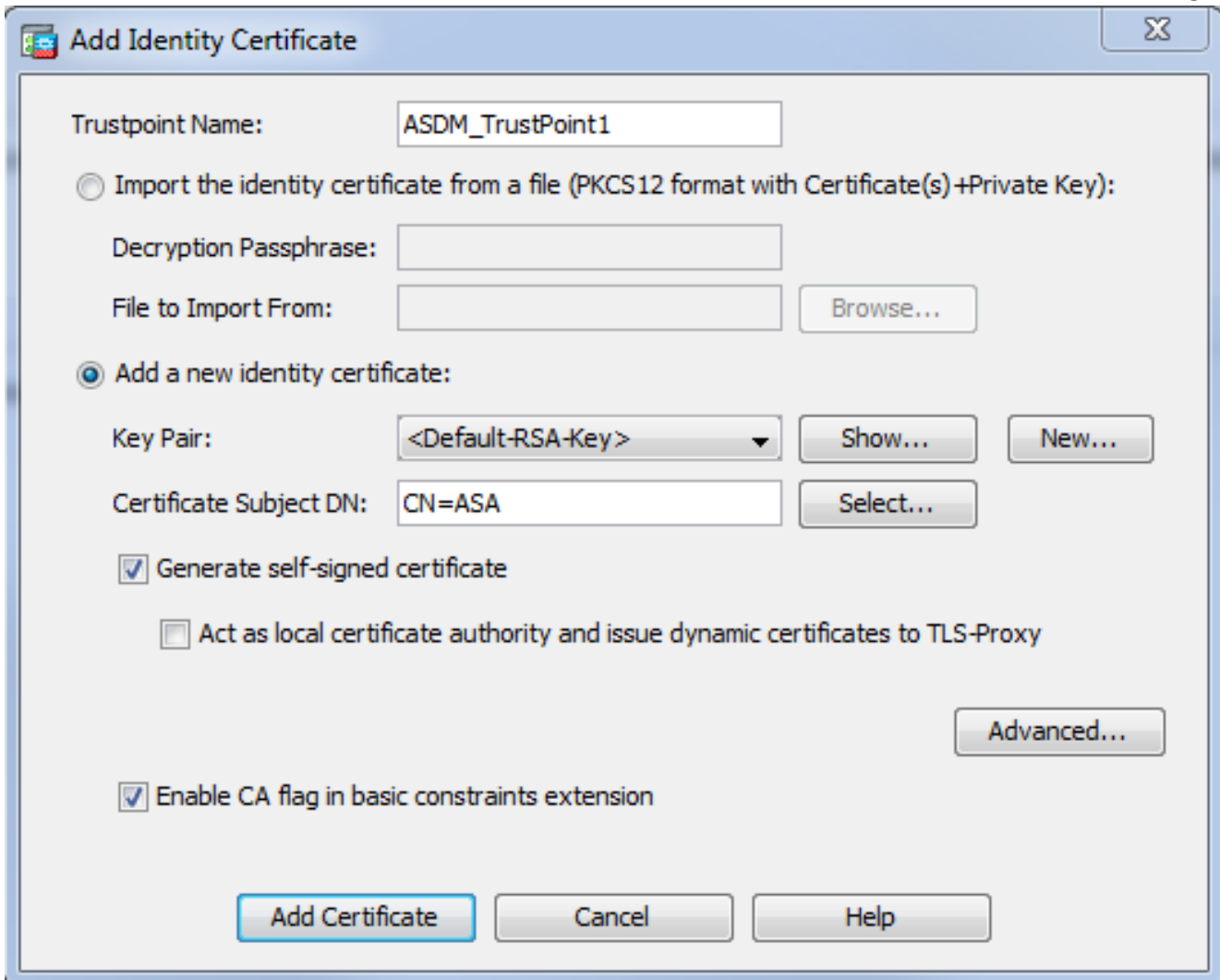
        .Enter the base 64 encoded pkcs12
        :End with the word "quit" on a line by itself
MIIJUQIBAzCCCRcGCSqGSIb3DQEHAaCCCQgEggkEMIIJADCCBF8GCSqGSIb3DQEH
BqCCBFawggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI8F3N
vkvjUgCAggAgIIFuHFrv6enVflNv3sBByB/yZswhELY5KpeALbXhfrFDpLNncAB+
/z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x3Ozo0JjxSAafmTWqDOEOS
7mHsaKMoao+pv2LqKTWh007No4Ycx75Y5sOhyuQGPhLJRdionbils1ioe4Dplx1b

```

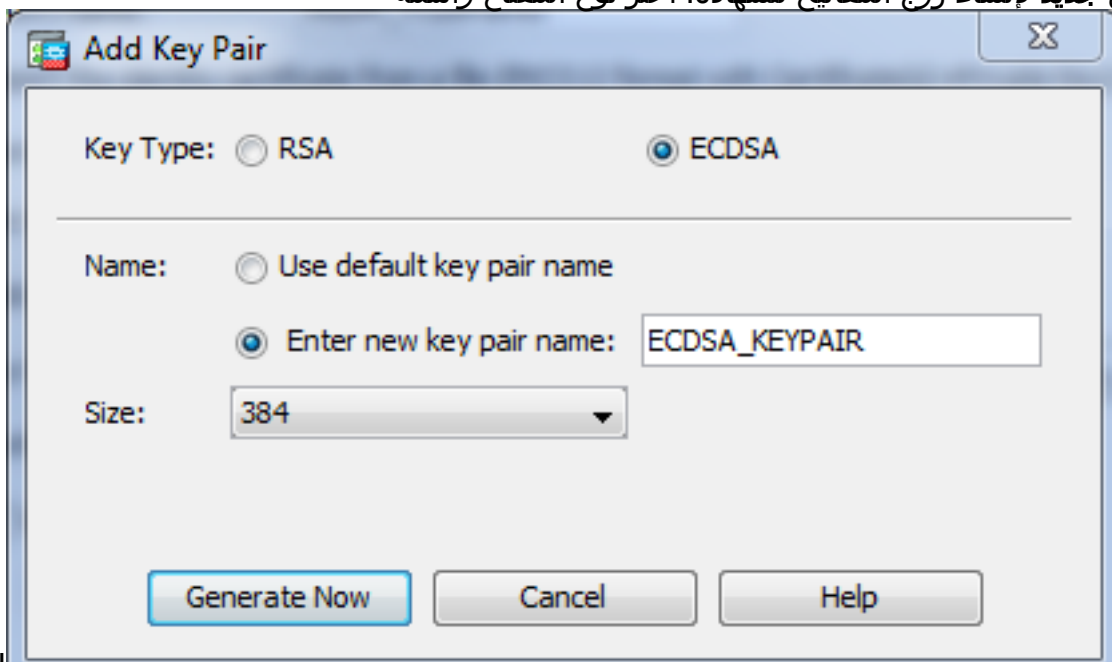
quit

INFO: Import PKCS12 operation completed successfully

الخيار 2 - إنشاء شهادة موقعة ذاتيا.أختر تشكيل < جدار الحماية < متقدم < إدارة الشهادات < شهادات الهوية < إضافة.انقر على زر إضافة شهادة هوية جديدة. حدد خانة الاختيار إنشاء شهادة موقعة ذاتيا. اخترت اسم مشترك (CN) أن يطابق domain name من ال .ASA



انقر فوق جديد لإنشاء زوج المفاتيح للشهادة. اختر نوع المفتاح واسمه



:CLI

وحجمه.

```
ASA(config)# crypto key generate ecdsa label ECDSA_KEYPAIR noconfirm
```

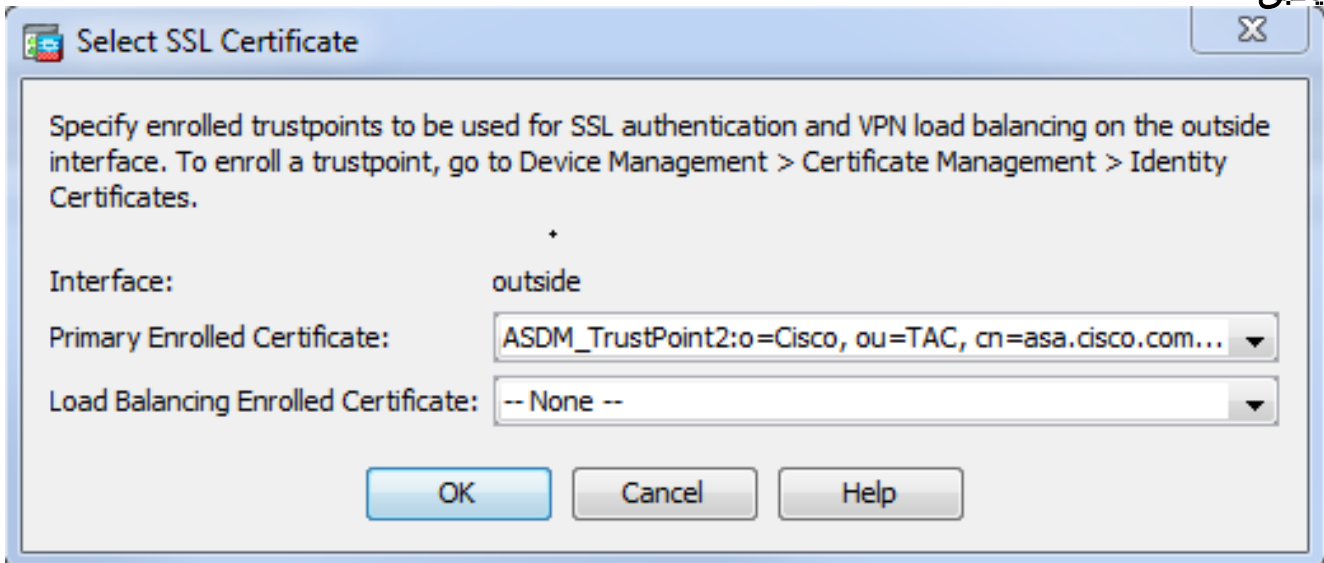
```

ASA(config)# crypto ca trustpoint TrustPoint1
ASA(config-ca-trustpoint)# revocation-check none
ASA(config-ca-trustpoint)# id-usage ssl-ipsec
ASA(config-ca-trustpoint)# no fqdn
ASA(config-ca-trustpoint)# subject-name CN=ASA
ASA(config-ca-trustpoint)# enrollment self
ASA(config-ca-trustpoint)# keypair ECDSA_KEYPAIR
ASA(config-ca-trustpoint)# exit
ASA(config)# crypto ca enroll TrustPoint1 noconfirm

```

2. أختار الشهادة التي سيتم استخدامها لخدمة إتصالات WebVPN. أخترت تشكيل <وصول عن بعد VPN> متقدم <SSL عملية إعداد. من قائمة الشهادات، أختار TrustPoint المرتبطة بالشهادة المطلوبة للواجهة الخارجية. طقطقة.

يطبق.



CLI مكافئ تشكيل:

```
ASA(config)# ssl trust-point
```

3. (إختياري) قم بتمكين عمليات بحث خادم اسم المجال (DNS). يعمل خادم WebVPN كوكيل لاتصالات العميل. هذا يعني أن ASA يقوم بإنشاء إتصالات بالموارد نيابة عن العميل. إذا كان العملاء يحتاجون إلى إتصالات بالموارد التي تستخدم أسماء المجالات، فيحتاج ASA إلى إجراء البحث عن DNS. أختار تكوين < Remote Access VPN (الوصول عن بعد) > DNS. قم بتكوين خادم DNS واحد على الأقل وتمكين عمليات بحث DNS على الواجهة التي تواجه خادم

## Configuration > Remote Access VPN > DNS

Specify how to resolve DNS requests.

### DNS Setup

Configure one DNS server group  Configure multiple DNS server groups

Primary DNS Server:

10.11.12.101

Secondary Servers:

+

Domain Name:

cisco.com

### DNS.

#### DNS Lookup

To configure DNS, enable DNS lookup on at least one interface.

Interface	DNS Enabled
inside	True
outside	False

#### DNS Guard

This function enforces one DNS response per query. If DNS inspection is configured, this option is ignored on that interface.

Enable DNS Guard on all interfaces.

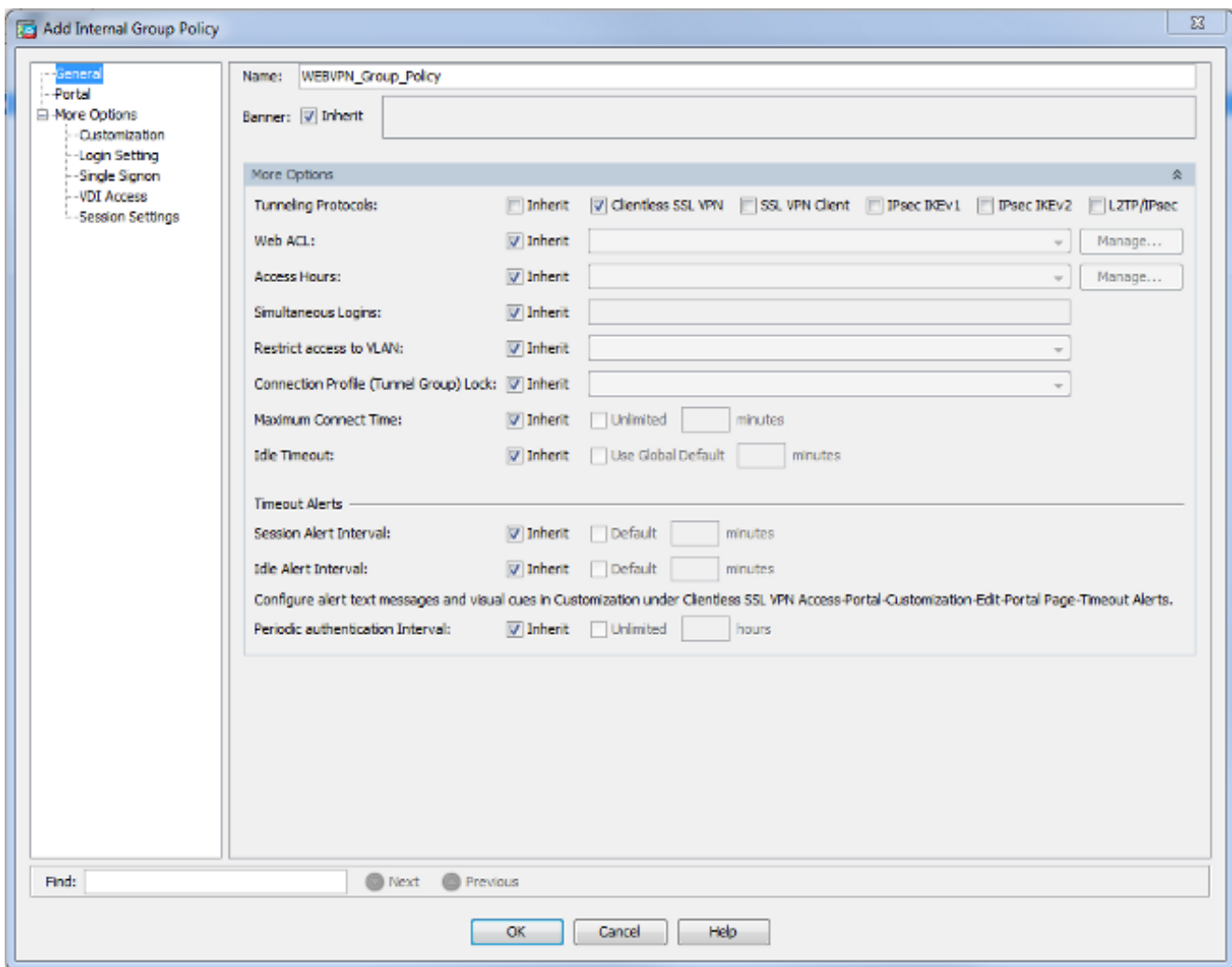
:CLI

```
ASA(config)# dns domain-lookup inside
```

```
ASA(config)# dns server-group DefaultDNS
```

```
ASA(config-dns-server-group)# name-server 10.11.12.101
```

4. (إختياري) قم بإنشاء نهج مجموعة لاتصالات WebVPN. أختار تكوين < Remote Access VPN (الوصول عن بعد) < Client Less SSL VPN Access < نهج المجموعة < إضافة نهج مجموعة داخلي. تحت الخيارات العامة، قم بتغيير قيمة بروتوكولات التوليف إلى "SSL VPN بدون عملاء".



:CLI

```
ASA(config)# group-policy WEBVPN_Group_Policy internal
ASA(config)# group-policy WEBVPN_Group_Policy attributes
ASA(config-group-policy)# vpn-tunnel-protocol ssl-clientless
```

5. تشكيل توصيف التوصليل في ASDM، أخطر تكوين < Remote Access VPN للوصول عن بعد > وصول SSL VPN بدون عملاء < ملفات تعريف الاتصال.

للحصول على نظرة عامة على ملفات تعريف الاتصال ونهج المجموعة، راجع [دليل تكوين واجهة سطر الأوامر من Cisco ASA Series VPN، الإصدار 9.4 - ملفات تعريف الاتصال، نهج المجموعة، والمستخدمين](#). تستخدم إتصالات WebVPN بشكل افتراضي ملف تعريف DefaultWEBVPNGgroup. يمكنك إنشاء توصيفات إضافية. ملاحظة: هناك طرق مختلفة لتعيين مستخدمين إلى ملفات تعريف أخرى.

- يمكن للمستخدمين تحديد ملف تعريف الاتصال يدويا من القائمة المنسدلة أو باستخدام عنوان URL محدد. راجع [ASA 8.x: السماح للمستخدمين بتحديد مجموعة في تسجيل الدخول إلى WebVPN من خلال أسلوب الاسم المستعار للمجموعة و أسلوب URL للمجموعة](#).

- عند استخدام خادم LDAP، يمكنك تعيين ملف تعريف المستخدم استنادا إلى السمات التي تم تلقيها من خادم LDAP، راجع [استخدام ASA لمخطط سمات LDAP كمثال تكوين](#).

- عند استخدام مصادقة العملاء المستندة إلى الشهادات، يمكنك تعيين المستخدم إلى ملفات التعريف استنادا إلى الحقول الموجودة في الشهادة، راجع [دليل تكوين واجهة سطر الأوامر ل Cisco ASA Series VPN، الإصدار 9.4 - تكوين مطابقة مجموعة الشهادات ل IKEv1](#).

- لتعيين المستخدمين يدويا إلى سياسة المجموعة، راجع [دليل تكوين واجهة سطر الأوامر من السلسلة Cisco ASA Series VPN، الإصدار 9.4 - تكوين السمات للمستخدمين الفرديينم بتحرير ملف تعريف](#)



DefaultWEBVPNGroup واختر WEBvpn\_Group\_Policy ضمن نهج المجموعة الافتراضي.

Edit Clientless SSL VPN Connection Profile: DefaultWEBVPNGroup

Basic  
Advanced

Name: DefaultWEBVPNGroup  
Aliases:

Authentication  
Method:  AAA  Certificate  Both  
AAA Server Group: LOCAL Manage...  
 Use LOCAL if Server Group fails

DNS  
Server Group: DefaultDNS Manage...  
(Following fields are attributes of the DNS server group selected above.)  
Servers: 10.21.22.101  
Domain Name: cisco.com

Default Group Policy  
Group Policy: WEBVPN\_Group\_Policy Manage...  
(Following field is an attribute of the group policy selected above.)  
 Enable clientless SSL VPN protocol

Find: Next Previous

OK Cancel Help

:CLI

```
ASA(config)# tunnel-group DefaultWEBVPNGroup general-attributes  
ASA(config-tunnel-general)# default-group-policy WEBVPN_Group_Policy
```

6. أخترت in order to مكنت WebVPN على القارن خارجي، تشكيل Clientless VPN Remote Access SSL VPN منفذ توصيل توصيفات. حدد خانة الاختيار السماح بالوصول بجوار الواجهة الخارجية.

Access Interfaces

Enable interfaces for clientless SSL VPN access.

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

Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Device Certificate ...

Port Setting ...

:CLI

ASA(config)# **webvpn**

ASA(config-webvpn)# **enable outside**

7. (إختياري) قم بإنشاء إشارات مرجعية للمحتوى. تسمح الإشارات المرجعية للمستخدم باستعراض الموارد الداخلية بسهولة بدون الحاجة إلى تذكر عناوين الربط URL. أخترت in order to خلقت إشارة مرجعية، تشكيل < Remote Access VPN>Client SSL VPN منفذ < مدخل < إشارات مرجعية < إضافة.

Add Bookmark List

Bookmark List Name: MyBookmarks

Bookmark Title	URL
----------------	-----

Add

Edit

Delete

Move Up

Move Down

Find:     Match Case

OK Cancel Help

أختر إضافة لإضافة إشارة مرجعية معينة.

Bookmark Title: Example bookmark

URL: http:// www.cisco.com Assistant...

Preload Page (Optional)

Preload URL: http://

Wait Time: (seconds)

Other Settings (Optional)

Subtitle:

Thumbnail: -- None -- Manage

Place this bookmark on the VPN home page

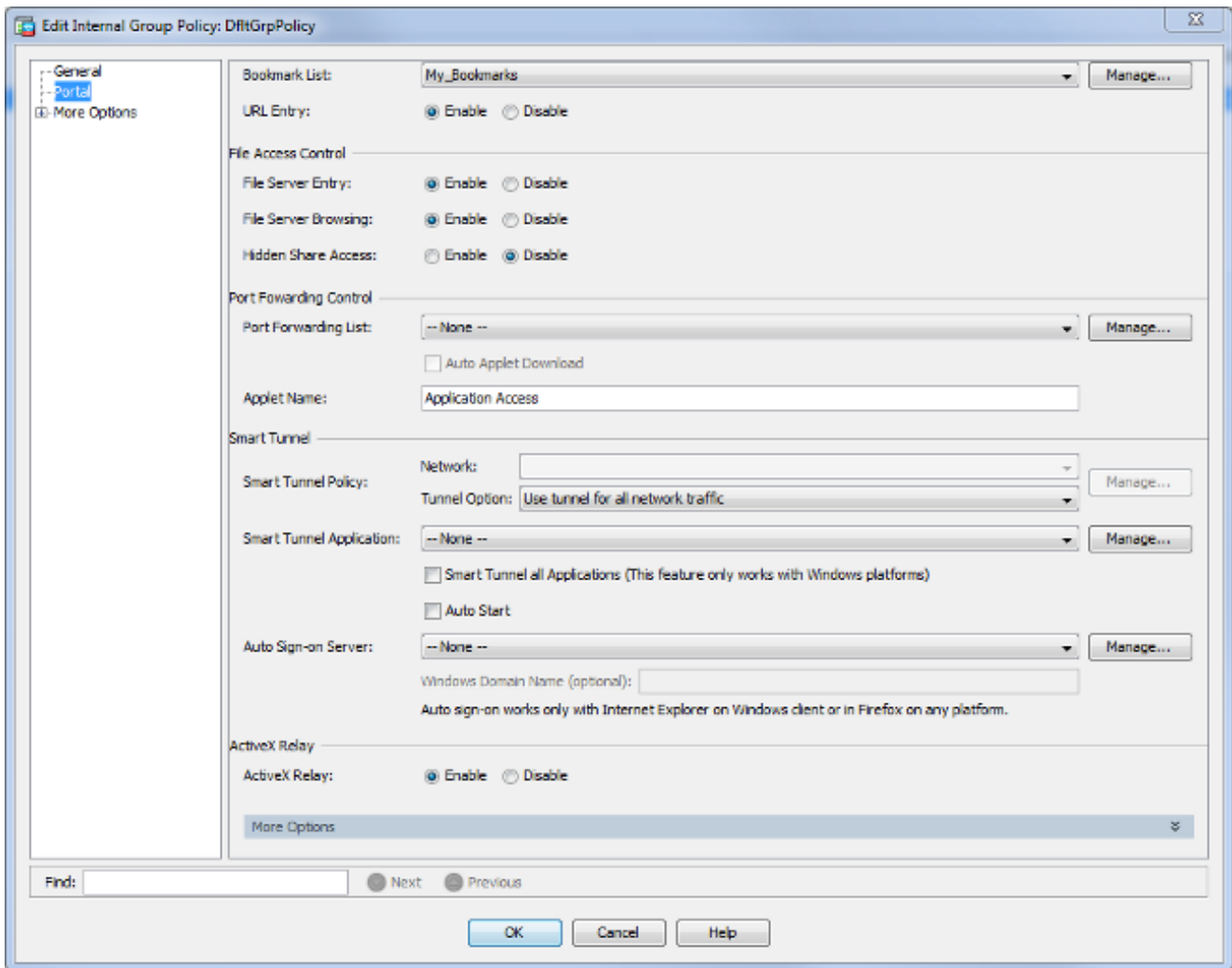
Enable Smart Tunnel

Advanced Options

OK Cancel Help

CLI: من المستحيل إنشاء إشارات مرجعية من خلال واجهة سطر الأوامر لأنها يتم إنشاؤها على هيئة ملفات XML.

8. (إختياري) قم بتعيين إشارات مرجعية لنهج مجموعة معين. أختار تكوين < Remote Access VPN (الوصول عن بعد) < Group Policy > Client Ssl VPN Access (نهج المجموعة) < Edit (تحرير) < Portal (المدخل) < قائمة الإشارات المرجعية.

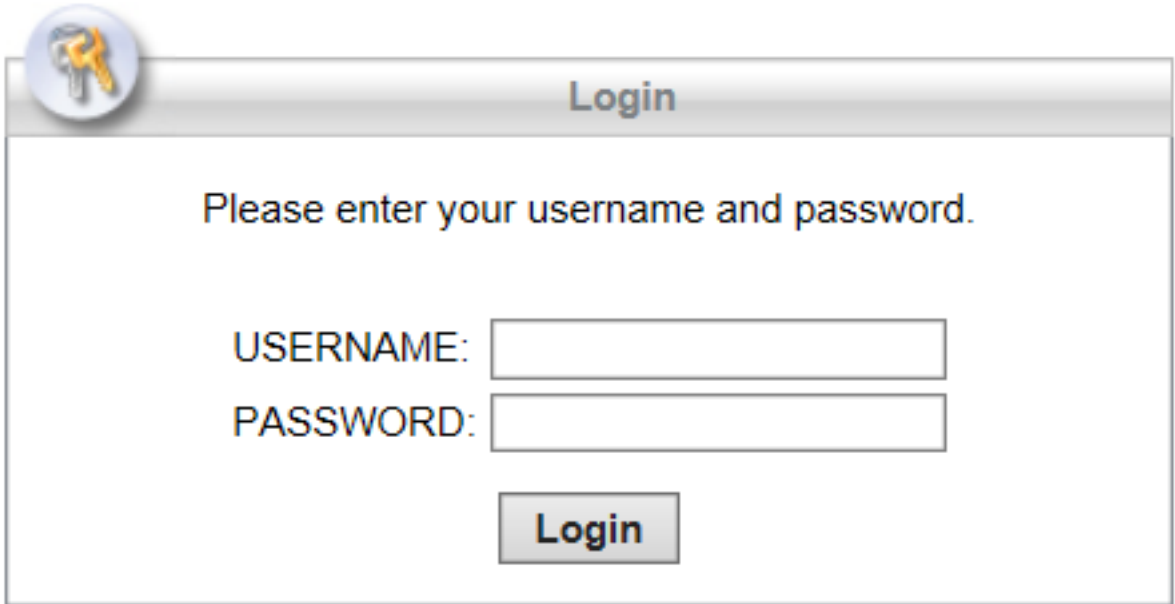


:CLI

```
ASA(config)# group-policy DfltGrpPolicy attributes
                ASA(config-group-policy)# webvpn
                ASA(config-group-webvpn)# url-list value My_Bookmarks
```

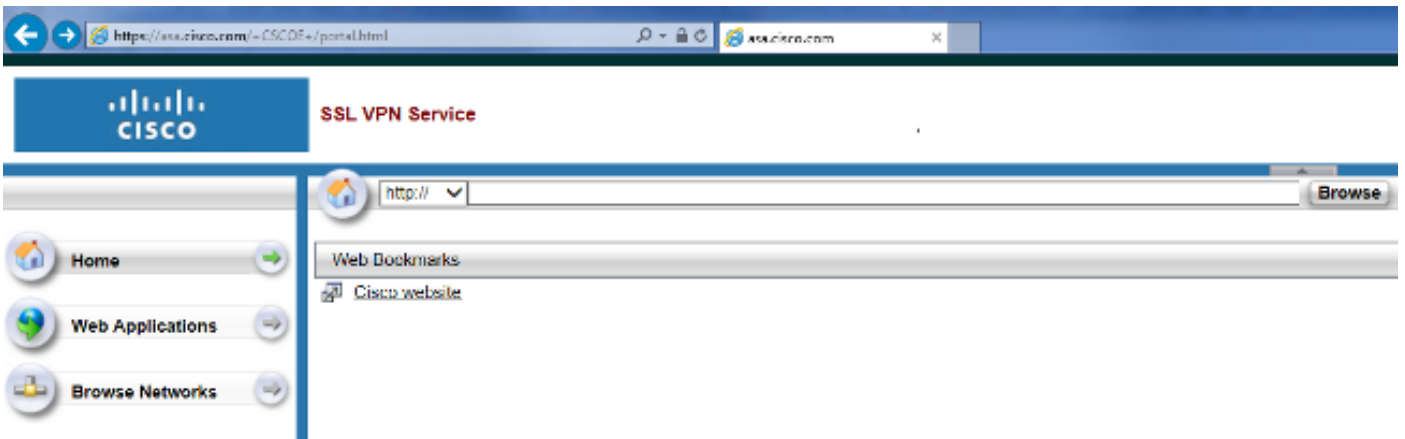
## التحقق من الصحة

بمجرد تكوين WebVPN، أستخدم العنوان `https://<FQDN>` الخاص بـ ASA في المستعرض.



The image shows a login window titled "Login" with a key icon in the top left corner. The text inside the window reads "Please enter your username and password." Below this text are two input fields: "USERNAME:" and "PASSWORD:". A "Login" button is positioned below the password field.

بعد تسجيل الدخول، يجب أن تكون قادرا على رؤية شريط العناوين المستخدم للتنقل إلى مواقع الويب والإشارات المرجعية.



## استكشاف الأخطاء وإصلاحها

### الإجراءات المستخدمة لاستكشاف الأخطاء وإصلاحها

اتبع هذه التعليمات لاستكشاف أخطاء عملية التكوين لديك وإصلاحها.

في ASDM، أختار المراقبة < التسجيل < عارض السجل في الوقت الفعلي < العرض. عند اتصال عميل ب ASA، لاحظ إنشاء جلسة TLS، وتحديد سياسة المجموعة، والمصادقة الناجحة للمستخدم.

```

Device completed SSL handshake with client outside:10.229.20.77/61307 to 10.48.66.179/443 for TLSv1.2 session
Device completed SSL handshake with client outside:10.229.20.77/61306 to 10.48.66.179/443 for TLSv1.2 session
SSL client outside:10.229.20.77/61307 to 10.48.66.179/443 request to resume previous session
Starting SSL handshake with client outside:10.229.20.77/61307 to 10.48.66.179/443 for TLS session
SSL client outside:10.229.20.77/61306 to 10.48.66.179/443 request to resume previous session
Starting SSL handshake with client outside:10.229.20.77/61306 to 10.48.66.179/443 for TLS session
Built inbound TCP connection 107 for outside:10.229.20.77/61307 (10.229.20.77/61307) to identity:10.48.66.179/443 (10.48.66.179/443)
Built inbound TCP connection 106 for outside:10.229.20.77/61306 (10.229.20.77/61306) to identity:10.48.66.179/443 (10.48.66.179/443)
Group <WEBVPN_Group_Policy> User <admin> IP <10.229.20.77> Authentication: successful, Session Type: WebVPN.
Device selects trust-point ASA-self-signed for client outside:10.229.20.77/53047 to 10.48.66.179/443
Group <WEBVPN_Group_Policy> User <admin> IP <10.229.20.77> WebVPN session started.
DAP: User admin, Addr 10.229.20.77, Connection Clientless: The following DAP records were selected for this connection: DfltAccessPolicy
AAA transaction status ACCEPT : user = admin
AAA retrieved default group policy (WEBVPN_Group_Policy) for user = admin
AAA user authentication Successful : local database : user = admin
Device completed SSL handshake with client outside:10.229.20.77/61304 to 10.48.66.179/443 for TLSv1.2 session
Device completed SSL handshake with client outside:10.229.20.77/61303 to 10.48.66.179/443 for TLSv1.2 session

```

:CLI

```

ASA(config)# logging buffered debugging
ASA(config)# show logging

```

في ASDM، أخطر مراقبة <VPN> <إحصائيات VPN> <جلسات العمل> تصفية حسب: SSL VPN بدون عملاء. ابحث عن جلسة عمل WebVPN الجديدة. تأكد من إختيار عامل تصفية WebVPN وانقر فوق عامل التصفية. إذا حدثت مشكلة، فعليك تجاوز جهاز ASA مؤقتا لضمان أن العملاء يمكنهم الوصول إلى موارد الشبكة المطلوبة. راجع خطوات التكوين المدرجة في هذا المستند.

Username IP Address	Group Policy Connection Profile	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx	Cer Auth Int	Cer Auth Left
admin 10.229.20.77	WEBVPN_Group_Policy DefaultWEBVPNGroup	Clientless Clientless: (1)AES128	10:40:04 UTC Tue May 26 2015 0h:02m:50s	63991 166375		

:CLI

```

ASA(config)# show vpn-sessiondb webvpn

```

```

Session Type: WebVPN

Username : admin Index : 3
Public IP : 10.229.20.77
Protocol : Clientless
License : AnyConnect Premium
Encryption : Clientless: (1)AES128 Hashing : Clientless: (1)SHA256
Bytes Tx : 72214 Bytes Rx : 270241
Group Policy : WEBVPN_Group_Policy Tunnel Group : DefaultWEBVPNGroup
Login Time : 10:40:04 UTC Tue May 26 2015
Duration : 0h:05m:21s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a1516010000300055644d84
Security Grp : none

```

## الأوامر المستخدمة لاستكشاف الأخطاء وإصلاحها

تدعم أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر `show`. استخدم أداة مترجم الإخراج (OIT) لعرض

تحليل مخرَج الأمر show .

ملاحظة: ارجع إلى [معلومات مهمة حول أوامر التصحيح](#) قبل استخدام أوامر debug.

- show webVPN - هناك العديد من أوامر show المقترنة ب WebVPN. رأيت in order to رأيت الإستعمال من عرض أمر بالتفصيل، [الأمر مرجع](#) قسم من ال cisco أمن جهاز.
- debug webVPN - يمكن أن يؤثر استخدام أوامر debug سلبا على ASA. رأيت in order to رأيت الإستعمال من يضبط أمر في كثير تفصيل، [الأمر مرجع](#) قسم من ال cisco أمن جهاز.

## مشاكل مشتركة

### يتعذر على المستخدم تسجيل الدخول

#### المشكلة

لا يسمح بوصول الرسالة "ClientWithout (browser) SSL VPN". تظهر الرسالة في المستعرض بعد محاولة تسجيل دخول غير ناجحة. لم يتم تثبيت ترخيص AnyConnect Premium على ASA أو أنه غير مستخدم كما هو موضح "لم يتم تمكين ترخيص AnyConnect Premium على ASA".

#### الحل

تمكين ترخيص Premium AnyConnect باستخدام الأوامر التالية:

```
ASA(config)# webvpn
ASA(config-webvpn)# no anyconnect-essentials
```

#### المشكلة

تظهر الرسالة "فشل تسجيل الدخول" في المستعرض بعد محاولة تسجيل دخول غير ناجحة. تم تجاوز حد ترخيص AnyConnect.

#### الحل

ابحث عن هذه الرسالة في السجلات:

```
<ASA-4-716023: Group <DfltGrpPolicy> User <cisco> IP <192.168.1.100%
.Session could not be established: session limit of 2 reached
```

تحقق أيضا من حد الترخيص الخاص بك:

```
ASA(config)# show version | include Premium
AnyConnect Premium Peers : 2 perpetual
```

#### المشكلة

تظهر الرسالة "لم يتم تمكين AnyConnect على خادم VPN" في المستعرض بعد محاولة تسجيل دخول غير ناجحة. لم يتم تمكين بروتوكول VPN بدون عملاء في نهج المجموعة.

#### الحل

ابحث عن هذه الرسالة في السجلات:

```
<ASA-6-716002: Group <DfltGrpPolicy> User <cisco> IP <192.168.1.100%
.WebVPN session terminated: Client type not supported
تأكد من تمكين بروتوكول VPN بدون عميل لنهج المجموعة المطلوب:
```

```
ASA(config)# show run all group-policy | include vpn-tunnel-protocol
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-clientless
```

## يتعذر توصيل أكثر من ثلاثة مستخدمي WebVPN بـ ASA

### المشكلة

يمكن لثلاثة عملاء WebVPN فقط الاتصال بـ ASA. فشل اتصال العميل الرابع.

### الحل

في معظم الحالات، تكون هذه المشكلة مرتبطة بإعداد تسجيل دخول متزامن ضمن نهج المجموعة. أستخدم هذا الرسم التوضيحي لتكوين العدد المطلوب من عمليات تسجيل الدخول المتزامنة. في هذا المثال، القيمة المطلوبة هي 20.

```
ASA(config)# group-policy Cisco attributes
ASA(config-group-policy)# vpn-simultaneous-logins 20
```

## يتعذر على عملاء WebVPN الوصول إلى الإشارات المرجعية ويتم سحبها للخارج

### المشكلة

إذا كانت هذه الإشارات المرجعية قد تم تكوينها للمستخدمين لتسجيل الدخول إلى شبكة VPN التي ليس لها عملاء، ولكن على الشاشة الرئيسية تحت "تطبيقات ويب" تظهر كما هي، فكيف يمكنني تمكين إرتباطات HTTP هذه بحيث يتمكن المستخدمون من النقر فوقها والانتقال إلى عنوان URL معين؟

### الحل

يجب أولاً التأكد من قدرة ASA على حل مواقع الويب من خلال DNS. حاول إختبار اتصال مواقع الويب بالاسم. إذا لم يتمكن ASA من حل الاسم، سيتم قطع الارتباط. إذا كانت خوادم DNS داخلية في شبكتك، فقم بتكوين الواجهة الخاصة لنطاق بحث DNS.

## اتصال Citrix من خلال WebVPN

### المشكلة

تحدث رسالة الخطأ عميل ICA الذي تلقى ملف ICA تالف. ل Citrix عبر WebVPN.

### الحل

إذا كنت تستخدم وضع العبارة الآمنة لاتصال Citrix من خلال WebVPN، فيمكن أن يتلف ملف ICA. نظراً لأن ASA غير متوافق مع وضع العملية هذا، قم بإنشاء ملف ICA جديد في الوضع المباشر (الوضع غير الآمن).



## كيفية تجنب الحاجة إلى مصادقة ثانية للمستخدمين

### المشكلة

عندما تصل إلى روابط CIFS على مدخل WebVPN بدون عملاء، سيطلب منك بيانات الاعتماد بعد أن تنقر الإشارة المرجعية. يستخدم البروتوكول الخفيف للوصول للدليل (LDAP) لمصادقة كل من الموارد والمستخدمين الذين دخلوا بالفعل بيانات اعتماد LDAP لتسجيل الدخول إلى جلسة عمل شبكة VPN.

### الحل

يمكنك استخدام ميزة الموقع التلقائي في هذه الحالة. تحت نهج المجموعة المحدد الجاري استخدامه وتحت سمات WebVPN الخاصة به، قم بتكوين ما يلي:

```
ASA(config)# group-policy WEBVPN_Group_Policy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# auto-signon allow uri cifs://X.X.X.X/* auth-type all
حيث X.X.X.X=IP الخاص بخادم CIFS و* = للوصول إلى ملف/مجلد المشاركة المعني.
```

يتم عرض قصاصة تكوين هنا:

```
ASA(config)# group-policy ExamplePolicy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# auto-signon allow uri
https://*.example.com/* auth-type all
```

لمزيد من المعلومات حول هذا الأمر، راجع [تكوين SSO باستخدام مصادقة HTTP الأساسية أو مصادقة NTLM](#).

## معلومات ذات صلة

- [ASA: النفق الذكي باستخدام مثال تكوين ASDM](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت  
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبل او  
امك ةقيد نوك تنل ةللأل ةمچرت لصف انءمچم اءمچرئى. ةصاأل مءتبل ب  
Cisco يلخت. فرتحم مچرت مءم دقي يتل ةيفارتحال ةمچرتل عم لاعل او  
ىل اءمءاد ةوچرلاب يصوءو تامچرتل هذه ةقदनء اهتيل وئسم Cisco  
Systems (رفوتم طبارل) يلصلأل يزىلچنل دن تسمل