Cisco Secure Desktop (CSD 3.1.x) على ASA مادختساب Windows نيوكت لاثمل 7.2.x ASDM

المحتويات

المقدمة

يعمل Cisco Secure Desktop (CSD) على زيادة أمان تقنية SSL VPN. يوفر CSD تقسيما منفصلا على محطة عمل مستخدم لنشاط جلسة العمل. يتم تشفير مساحة التخزين هذه أثناء جلسات العمل وتتم إزالتها بالكامل في نهاية جلسة SSL VPN. يمكن تكوين Windows باستخدام ميزات الأمان الكاملة ل CSD. يمكن لمنتجات Macintosh و Linux و Windows CE الوصول فقط إلى ميزات تنظيف ذاكرة التخزين المؤقت وتصفح الويب والوصول إلى الملفات. يمكن تهيئة CSD لأجهزة Windows و Macintosh و Windows CE و Linux على هذه الأنظمة الأساسية:

- سلسلة أجهزة الأمان المعدلة Cisco Adaptive Security Appliance (ASA) 5500 Series
- cisco مسحاج تخديد أن يركض cisco ios ® برمجية إطلاق T(6)12.4 وفيما بعد
- Cisco VPN 3000 Series Concentrators، الإصدار 4.7 والإصدارات الأحدث
- الوحدة النمطية Cisco WebVPN Module على موجهات سلسلة Catalyst 6500 و 7600

ملاحظة: يتيح لك الإصدار 3.3 من CSD الآن تكوين Cisco Secure Desktop للتشغيل على أجهزة الكمبيوتر البعيدة التي تعمل بنظام التشغيل Microsoft Windows Vista. في السابق، كان "سطح المكتب الآمن من Cisco" محدودا بأجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows XP أو 2000. راجع قسم تحسين الميزة الجديدة - تأمين

سطح المكتب على Vista من ملاحظات الإصدار الخاصة ب Cisco Secure Desktop، الإصدار 3.3، للحصول على مزيد من المعلومات.

يغطي هذا المثال بشكل أساسي تثبيت CSD وتكوينه على سلسلة ASA 5500 لعملاء Windows. تتم إضافة التكوينات الاختيارية لعملاء Windows CE و Mac و Linux من أجل الاكتمال.

يتم إستخدام CSD بالاقتران مع تقنية SSL VPN (الشبكة الخاصة الظاهرية (VPN) الخاصة ب SSL دون عميل، أو شبكة VPN الخاصة ب SSL أو SVPN الخاصة ب SSL). يضيف CSD قيمة إلى الجلسات الآمنة لتقنية SSL VPN.

المتطلبات الأساسية

المتطلبات

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

متطلبات جهاز ASA

- Cisco CSD الإصدار 3.1 أو إصدار أحدث
- برنامج ASA الإصدار 7.1.1 من Cisco أو إصدار أحدث
- مدير أجهزة الأمان المعدلة (ASDM) من Cisco، الإصدار 5.1.1 أو إصدار أحدث**ملاحظة:** يدعم CSD الإصدار 3.2 على ASA الإصدار x.8 فقط**ملاحظة:** ارجع إلى السماح بوصول HTTPS إلى ASDM للسماح بتكوين ASA بواسطة ASDM.

متطلبات أجهزة الكمبيوتر العميلة

- يجب أن يتمتع العملاء البعيدين بامتيازات إدارية محلية؛ وهذا غير مطلوب، ولكنه مقترح بشدة.
- يجب أن يكون لدى العملاء البعيدين الإصدار 1.4 أو أعلى من بيئة وقت تشغيل Java (JRE).
- مستعرضات الأجهزة العميلة البعيدة: Internet Explorer 6.0 أو Netscape 7.1 أو Mozilla 1.7 أو Safari 1.2.2 أو Firefox 1.0
- تم تمكين ملفات تعريف الارتباط والإطارات المنبثقة المسموح بها على العملاء البعيدين

المكونات المستخدمة

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

- Cisco ASDM، الإصدار 5.2(1)
- Cisco ASA، الإصدار 7.2(1)
- Cisco CSD Version-Secure Desktop-asa-3.1.1.32-k9.pkg

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. عناوين IP المستخدمة في هذا التكوين هي عناوين RFC 1918. عناوين IP هذه غير قانونية على الإنترنت ويجب إستخدامها فقط في بيئة مختبر الاختبار.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

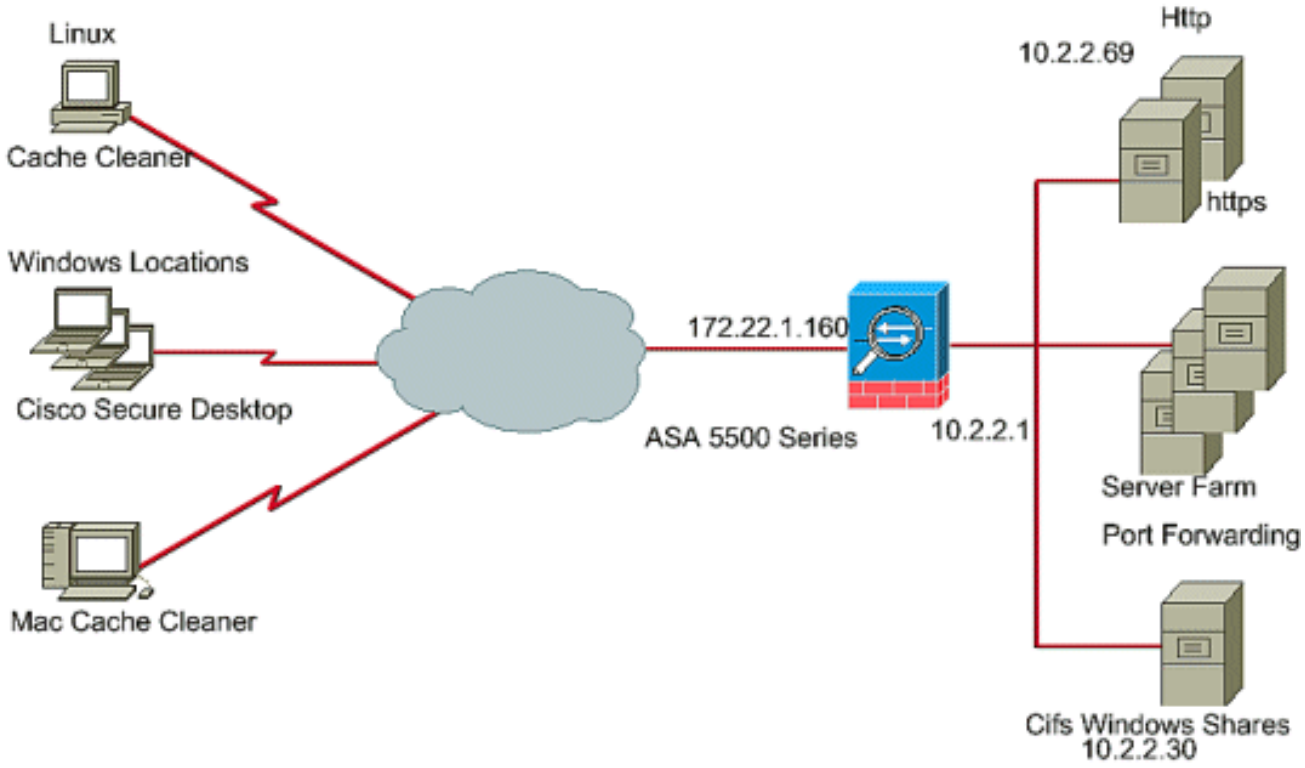
معلومات أساسية

يعمل CSD باستخدام تقنية SSL VPN، لذلك يجب تنشيط البرامج دون عملاء أو برامج عميلة قليلة السمك أو بطاقات SVC قبل تكوين CSD.

الرسم التخطيطي للشبكة

يمكن تكوين مواقع Windows مختلفة باستخدام جوانب الأمان الكاملة ل CSD. تمتلك Macintosh و Linux و Windows CE إمكانية الوصول فقط إلى جهاز تنظيف ذاكرة التخزين المؤقت و/أو إستعراض الويب والوصول إلى الملفات.

يستخدم هذا المستند إعداد الشبكة التالي:



تكوين CSD على ASA لعملاء Windows

قم بتكوين CSD على ASA لعملاء Windows بخمس خطوات رئيسية:

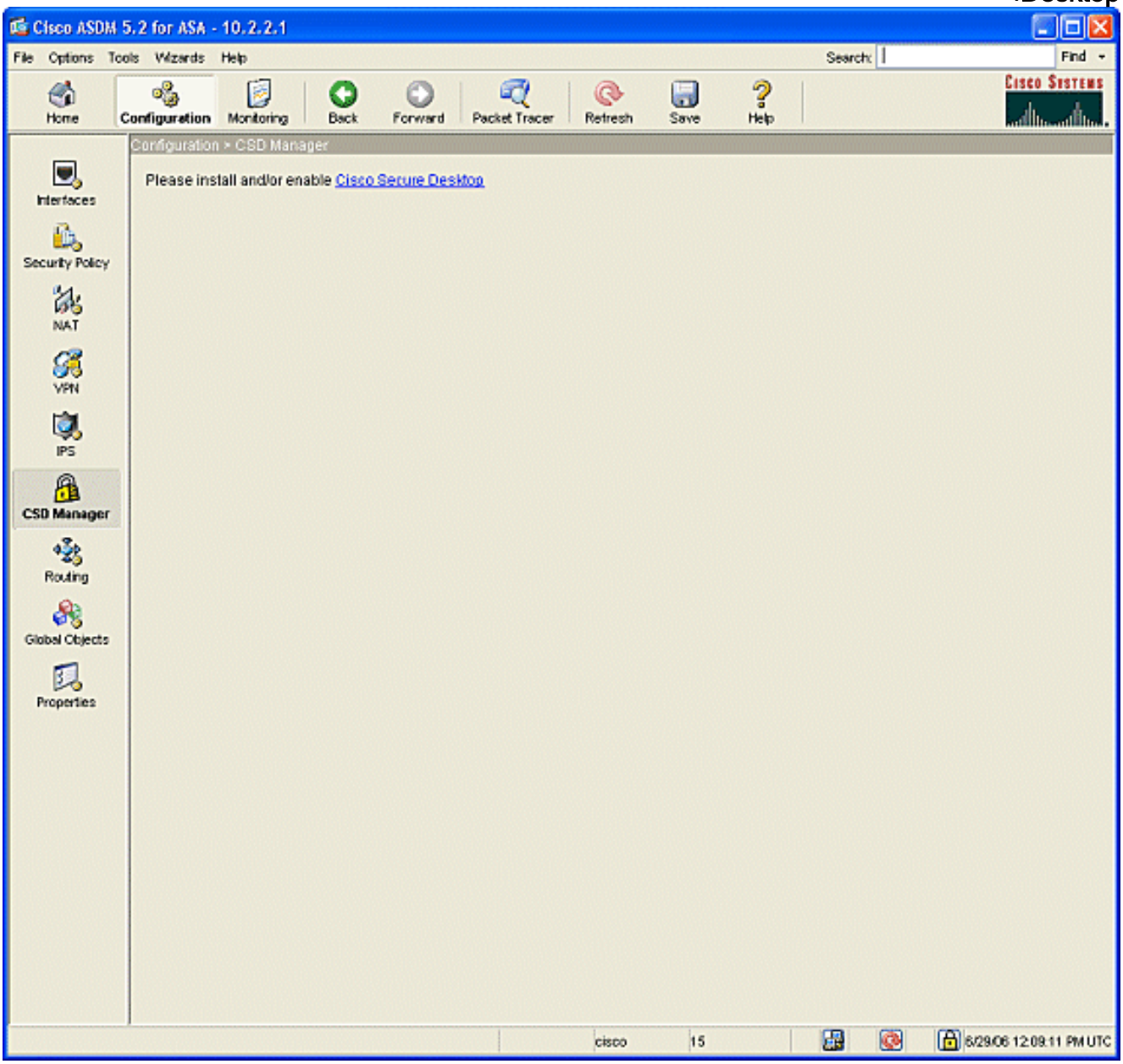
- الحصول على برنامج CSD على Cisco ASA وتثبيته وتمكينه.
- تعريف مواقع Windows.
- تعريف موقع Windows.
- تكوين الوحدات النمطية لموقع Windows.
- تكوين ميزات موقع Windows.
- تهيئة إختيارية لعملاء Windows CE و Macintosh و Linux.

الحصول على برنامج CSD وتثبيته وتمكينه

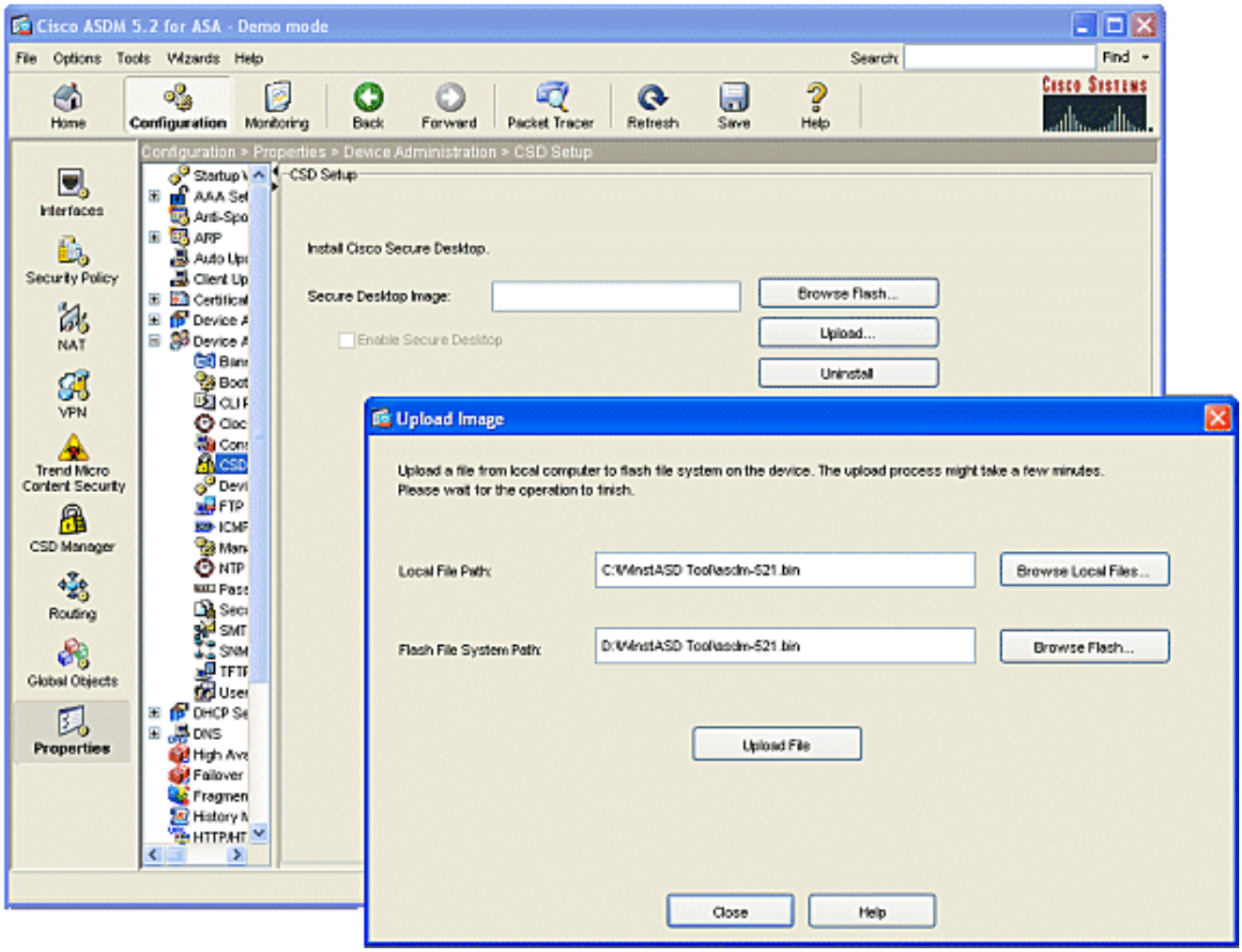
أكمل الخطوات التالية للحصول على برنامج CSD على Cisco ASA وتثبيته وتمكينه.

1. تنزيل برنامج CSD Secure Desktop-asa*.pkg وتصحيح الملفات على محطة الإدارة الخاصة بك من موقع تنزيل برامج Cisco على الويب.
2. سجل الدخول إلى ASDM وانقر فوق الزر **تكوين**. من القائمة اليسرى، انقر فوق الزر **CSD Manager**، وانقر

فوق إرتباط **Cisco Secure Desktop**.



3. انقر فوق **تحميل** لعرض نافذة تحميل الصورة.قم بإدخال مسار ملف .pkg الجديد على محطة الإدارة أو انقر **تصفح الملفات المحلية** لتحديد موقع الملف.إما أن تدخل الموقع على Flash الذي تريد وضع الملف فيه أو انقر على **تصفح Flash**.انقر فوق **تحميل الملف**.عندما يطلب منك، انقر **موافق > إغلاق > موافق**.

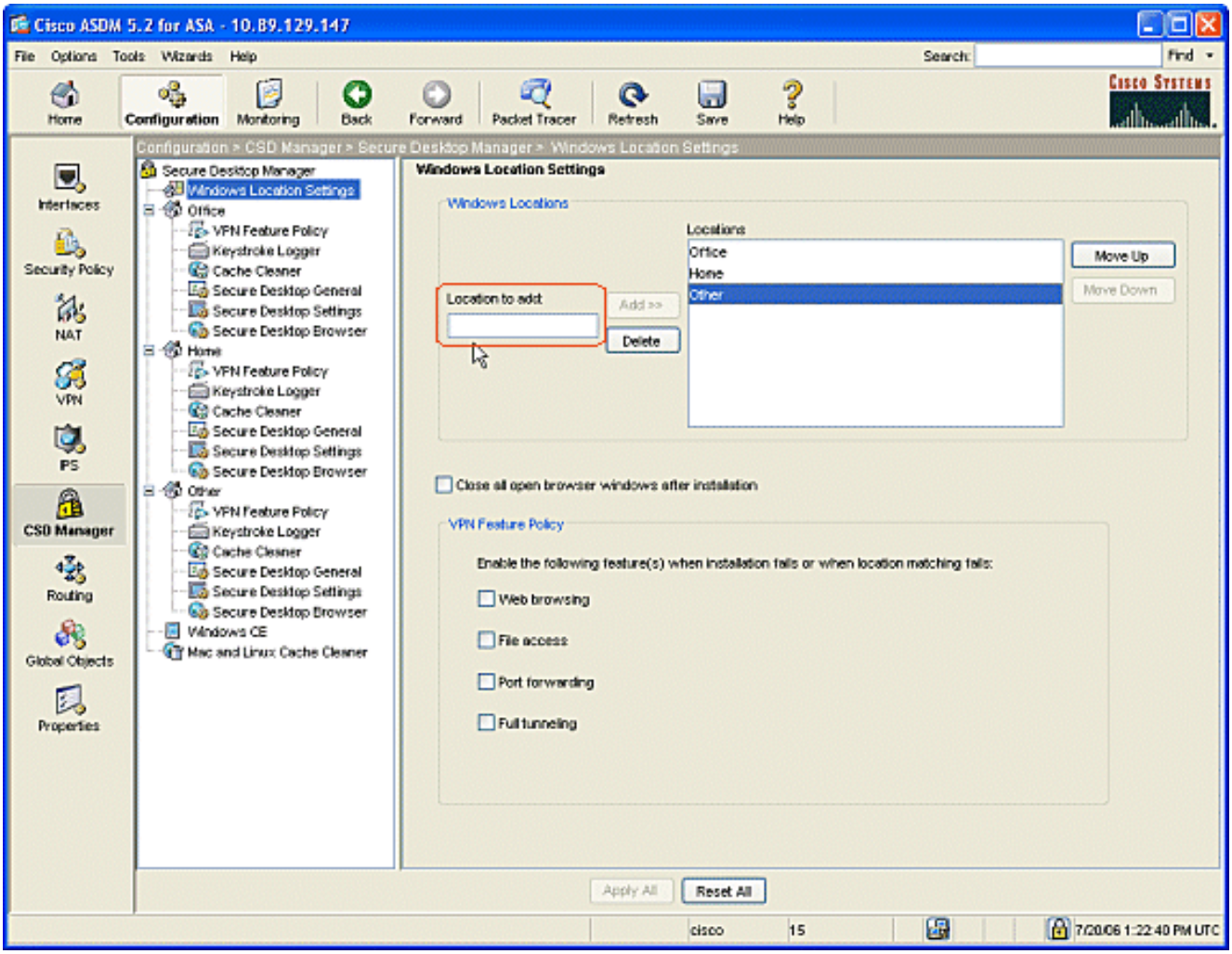


4. بمجرد تحميل صورة العميل إلى ذاكرة Flash (الذاكرة المؤقتة)، حدد خانة الاختيار **تمكين SSL VPN Client**، ثم انقر فوق **تطبيق**.
5. انقر فوق **حفظ**، ثم انقر فوق **نعم** لقبول التغييرات.

تعريف مواقع Windows

أكمل الخطوات التالية لتعريف مواقع Windows.

1. طقطقت **التشكيل** زر.
2. من القائمة اليسرى، انقر فوق الزر **CSD Manager**، وانقر فوق إرتباط **Cisco Secure Desktop**.
3. من جزء التنقل، انقر فوق **إعدادات موقع Windows**.
4. اكتب اسم موقع في حقل "الموقع المراد إضافته" وانقر فوق **إضافة**.لاحظ المواقع الثلاثة في هذا المثال: Office و Home و Others.يمثل Office محطات العمل الموجودة داخل الحدود الأمنية للشركة.يمثل Home المستخدمين الذين يعملون من المنزل.وتمثل مواقع أخرى أي موقع آخر غير الموقعين المذكورين.

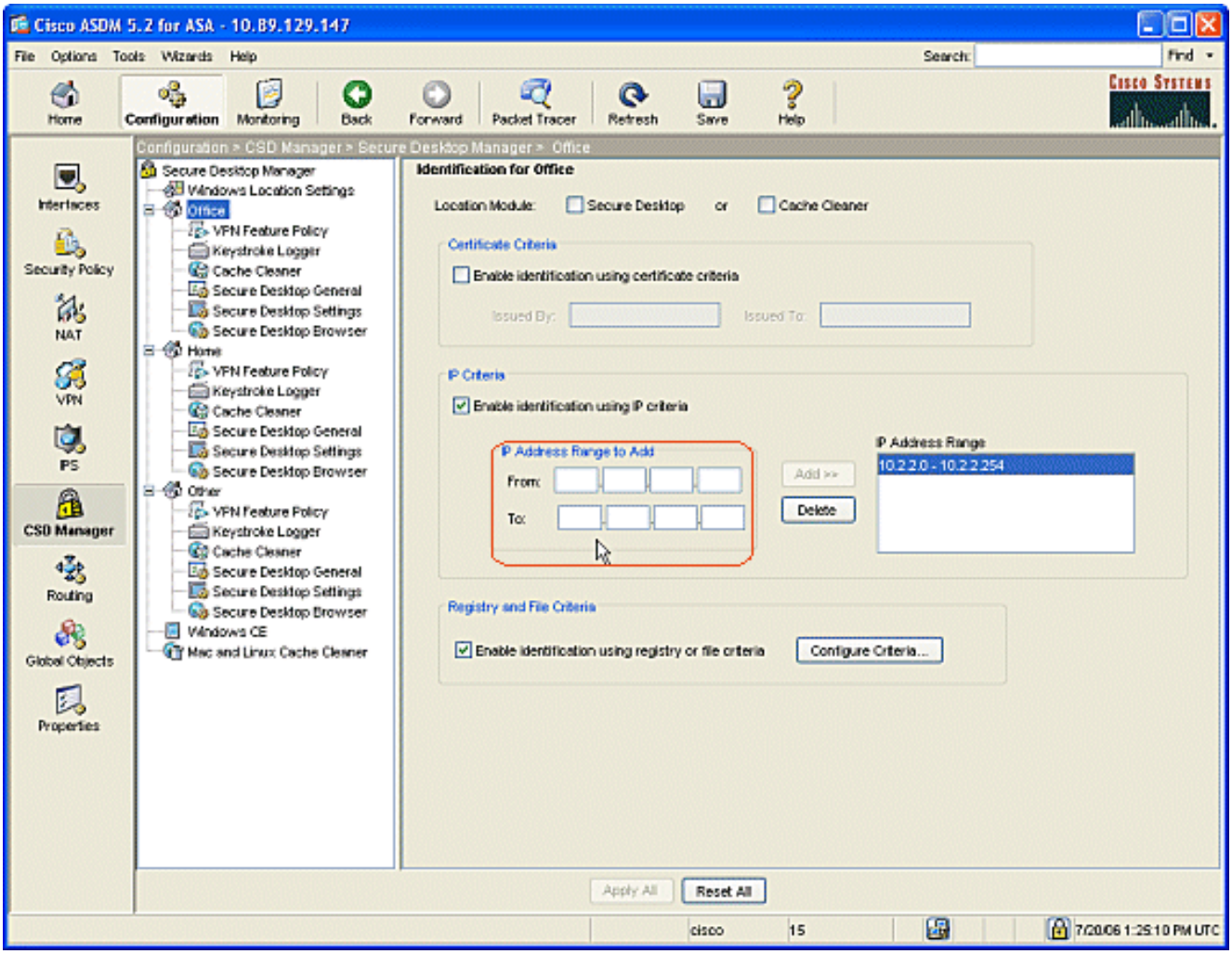


5. قم بإنشاء المواقع الخاصة بك وفقا لتخطيط بنية الشبكة الخاصة بك للمبيعات والضيوف والشركاء وغيرهم.
6. أثناء قيامك بإنشاء مواقع Windows، يتم توسيع جزء التنقل باستخدام وحدات قابلة للتكوين لكل موقع جديد.
   انقر فوق **تطبيق الكل**.
7. انقر فوق **حفظ**، ثم انقر فوق **نعم** لقبول التغييرات.

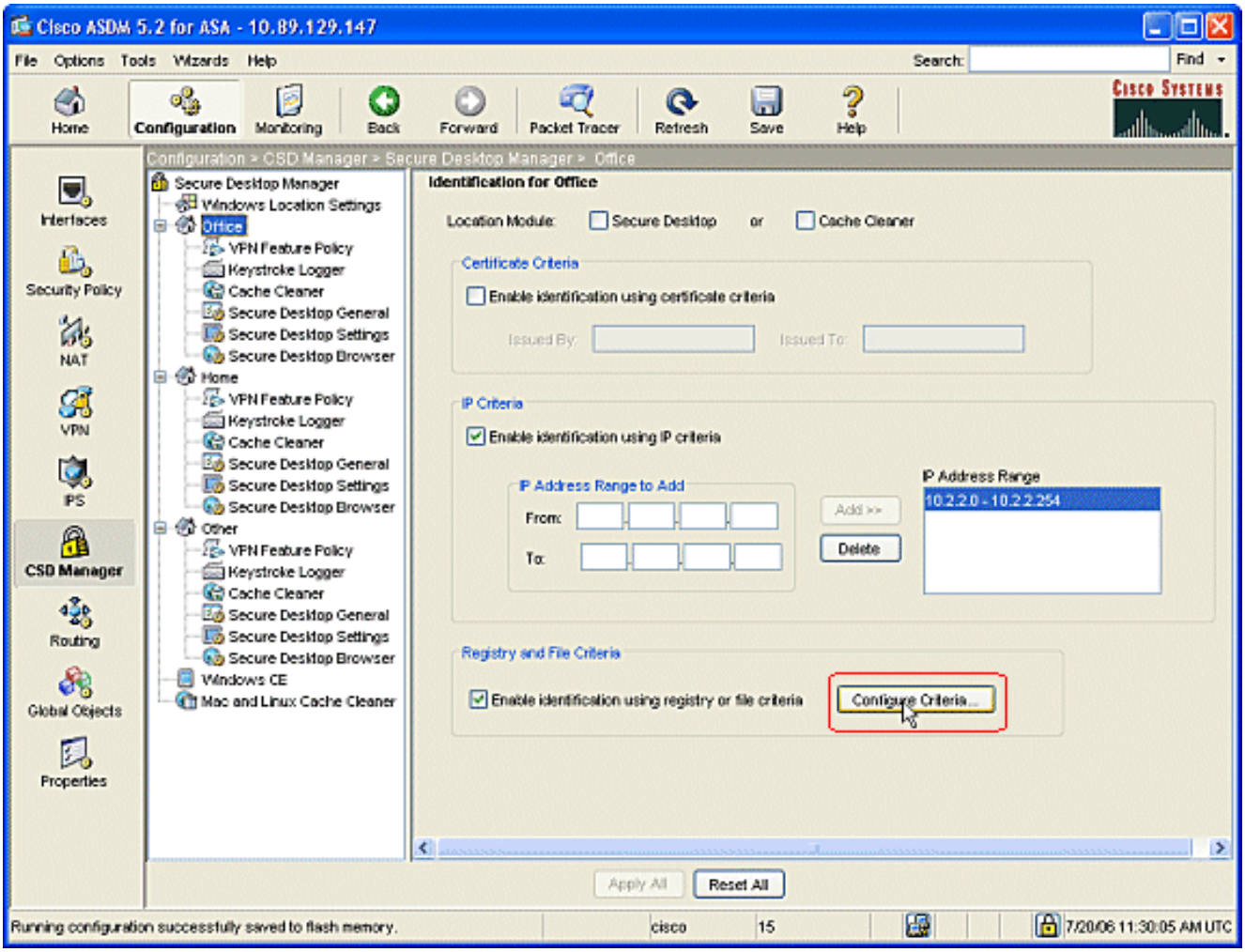
تعريف موقع Windows

أكمل الخطوات التالية لتعريف تعريف موقع Windows.

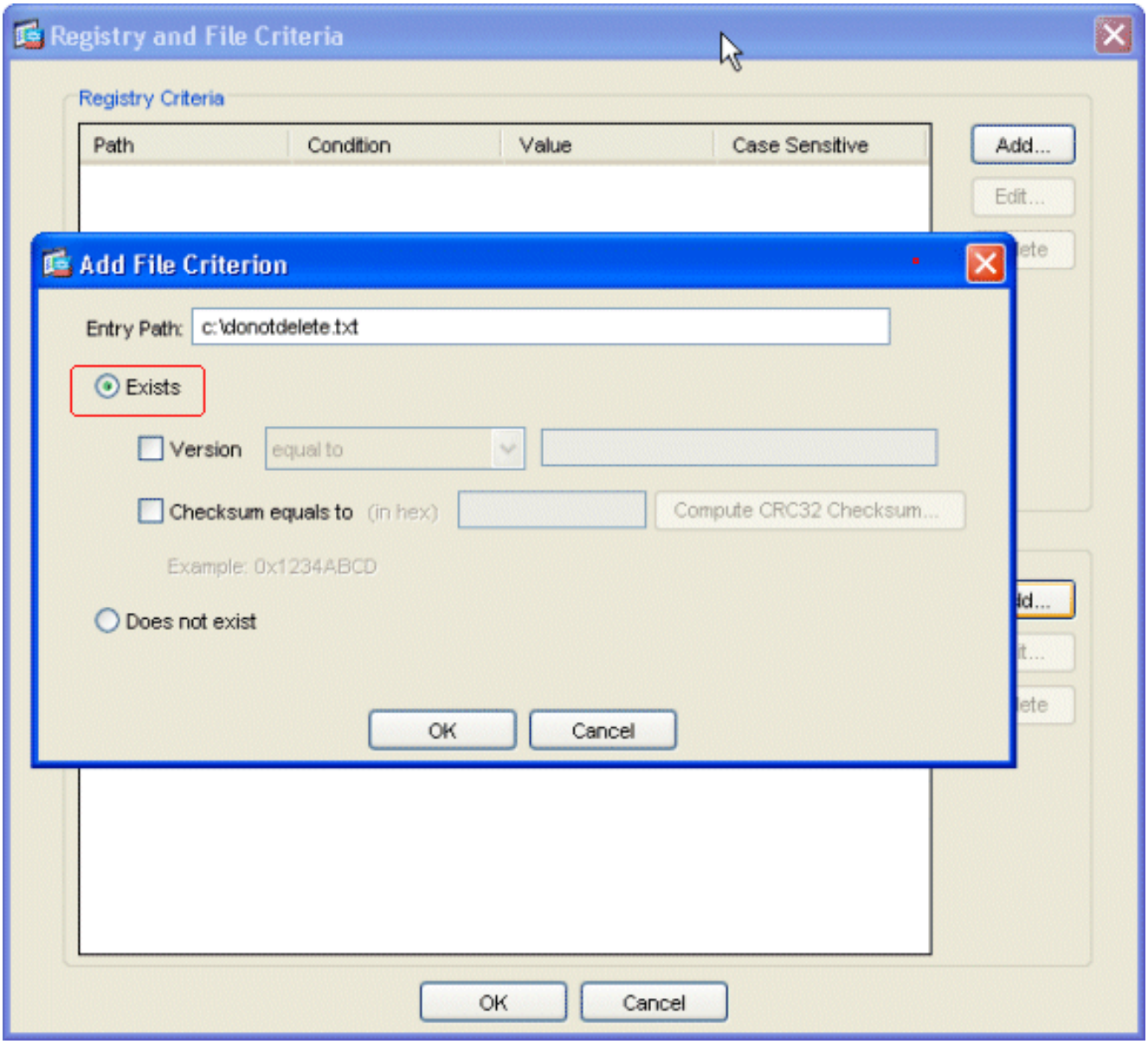
1. تحديد المواقع التي تم إنشاؤها في تعريف مواقع Windows.



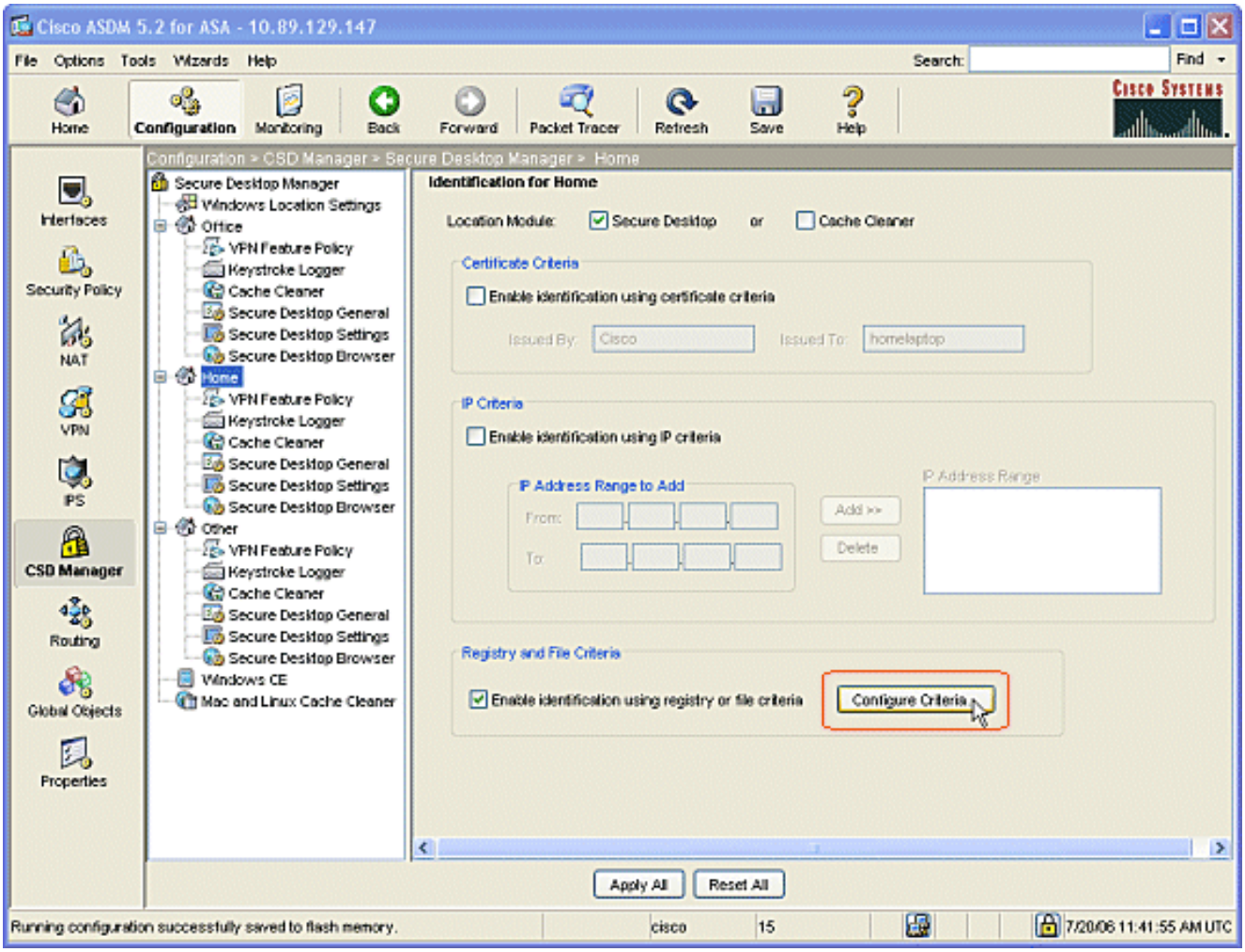
2. لتحديد موقع Office، انقر فوق **Office** في جزء التنقل.قم بإلغاء تحديد **Secure Desktop** و**Cache Clean** لأن هذه هي أجهزة كمبيوتر داخلية.تحقق من **تمكين التعريف باستخدام معايير IP**.أدخل نطاقات عناوين IP الخاصة بأجهزة الكمبيوتر الداخلية لديك.تحقق من **تمكين التعريف باستخدام معايير التسجيل أو الملف**. ويميز هذا الأمر بين موظفي المكاتب الداخلية والضيوف في بعض الأحيان على الشبكة.



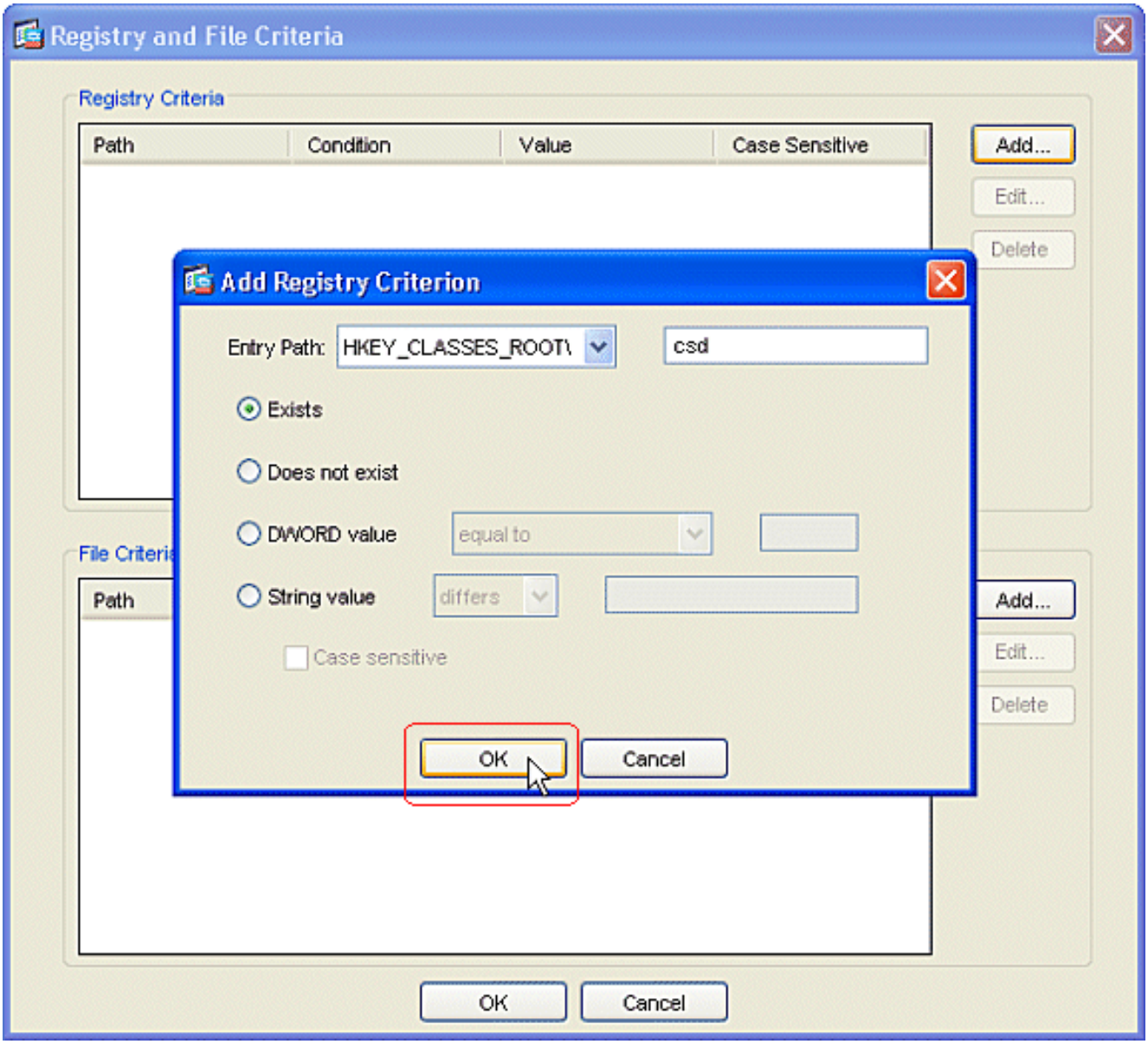
3. انقر فوق **تكوين المعايير**. تم تكوين مثال بسيط لملف "DoNotDelete.txt". يجب أن يكون هذا الملف موجودا على أجهزة الكمبيوتر الداخلية الخاصة بك في Windows وهو مجرد عنصر نائب. يمكنك أيضا تكوين مفتاح تسجيل Windows لتعريف أجهزة الكمبيوتر الداخلية في المكتب. انقر فوق **موافق** في الإطار إضافة معيار الملف. انقر فوق **موافق** في الإطار معايير السجل والملف.



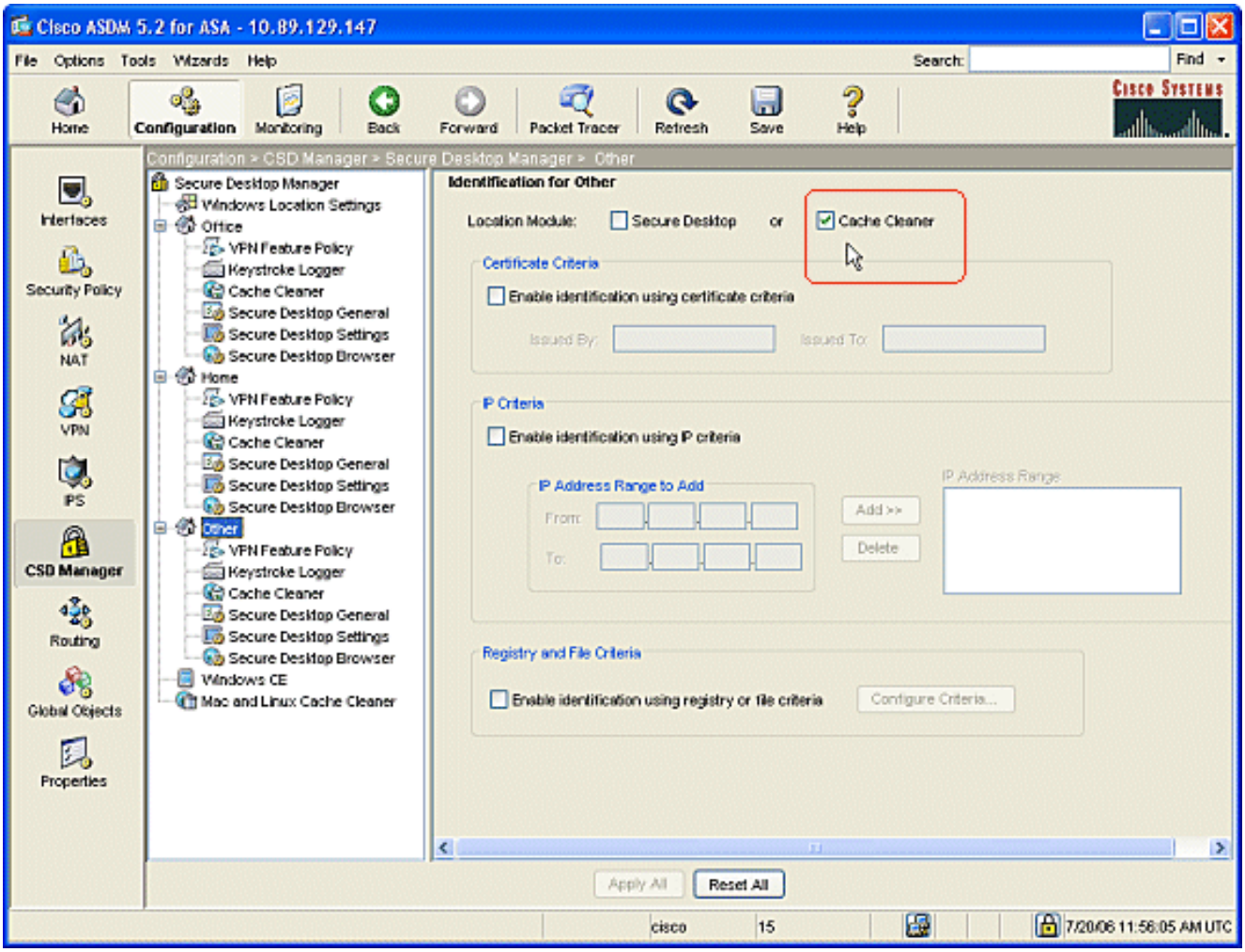
4. انقر فوق **تطبيق الكل** في تعريف إطار Office. انقر فوق **حفظ**، ثم انقر فوق **نعم** لقبول التغييرات.
5. لتحديد الموقع الرئيسي، انقر فوق **الصفحة الرئيسية** في جزء التنقل.تحقق من **تمكين التعريف باستخدام معايير التسجيل أو الملف**.انقر فوق **تكوين المعايير**.



6. يجب أن يكون المسؤول قد قام بتكوين عملاء الكمبيوتر المنزلي باستخدام مفتاح التسجيل هذا. انقر فوق **موافق** في الإطار "إضافة معيار تسجيل". انقر فوق **موافق** في الإطار معايير السجل والملف.



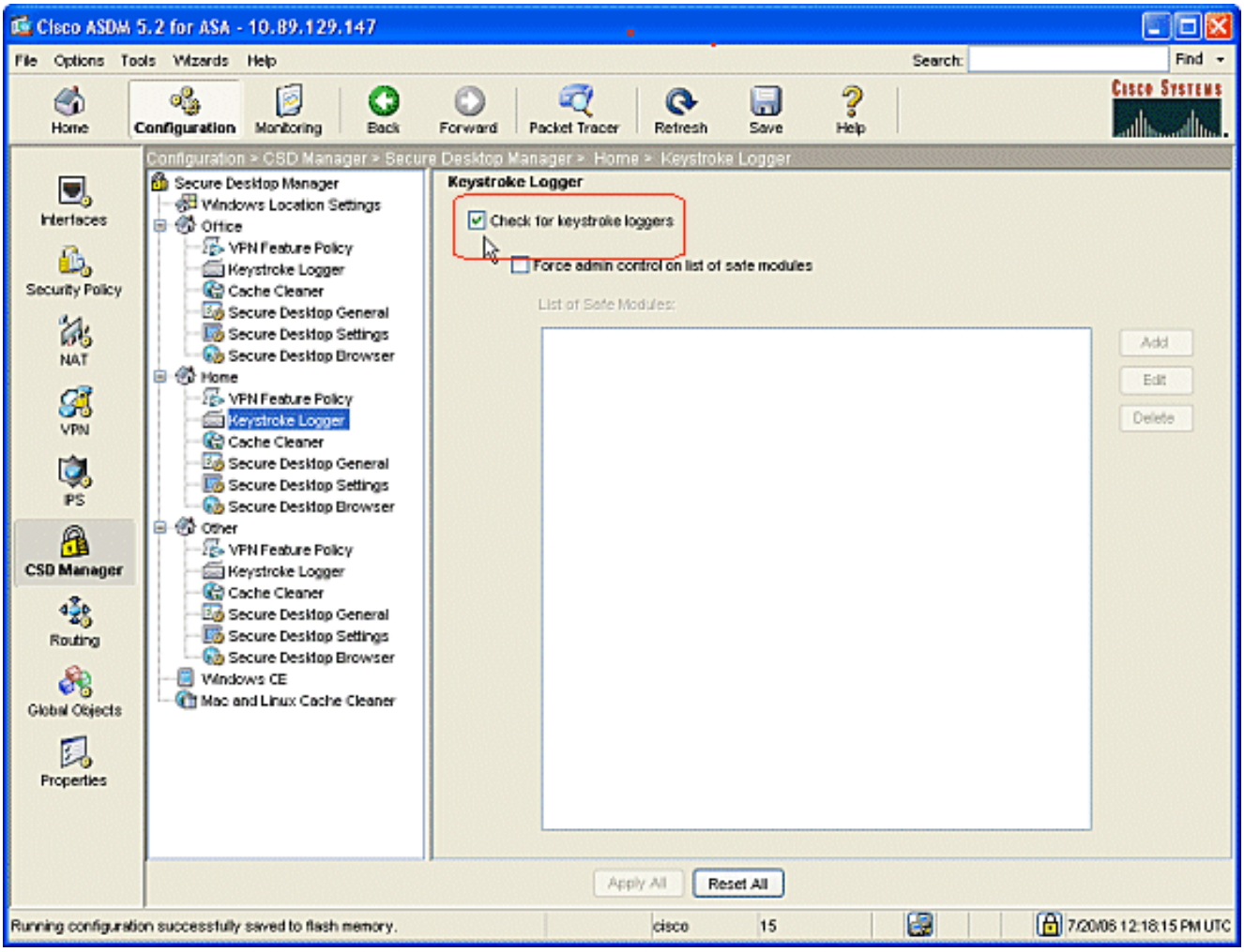
7. تحت وحدة الموقع، تحقق من **سطح المكتب الآمن**. طقطقة **يطبق all** في التعريف لنافذة منزل. انقر فوق **حفظ**، ثم انقر فوق **نعم** لقبول التغييرات.
8. لتعريف الموقع **آخر**، انقر **آخر** في جزء التنقل.حدد فقط مربع **تنظيف ذاكرة التخزين المؤقت** وألغي تحديد كافة المربعات الأخرى.طقطقة **يطبق all** في التعريف لنافذة آخر.انقر فوق **حفظ**، ثم انقر فوق **نعم** لقبول التغييرات.



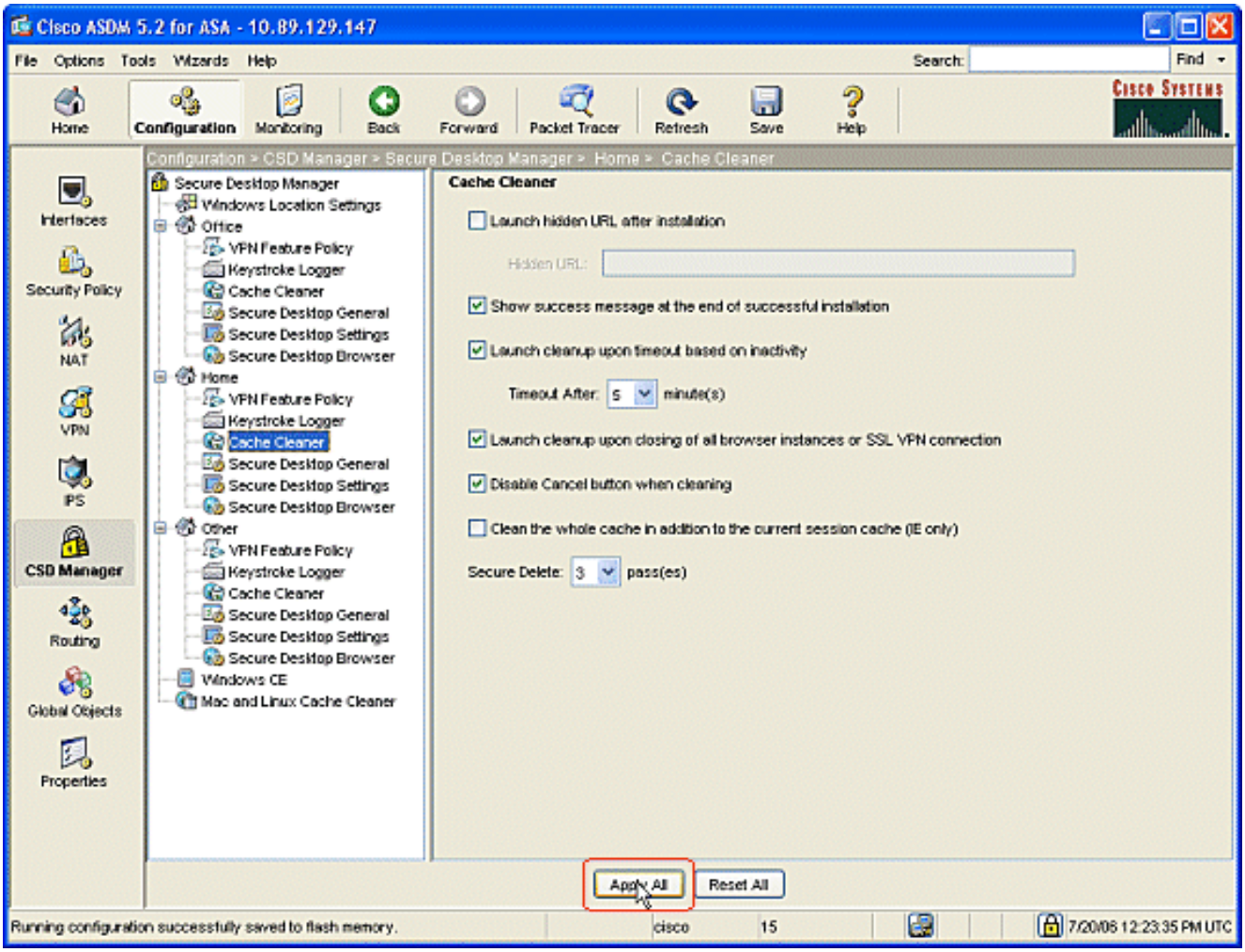
تكوين الوحدة النمطية لموقع Windows

أكمل هذه الخطوات لتكوين الوحدات النمطية ضمن كل موقع من المواقع الثلاثة التي قمت بإنشائها.

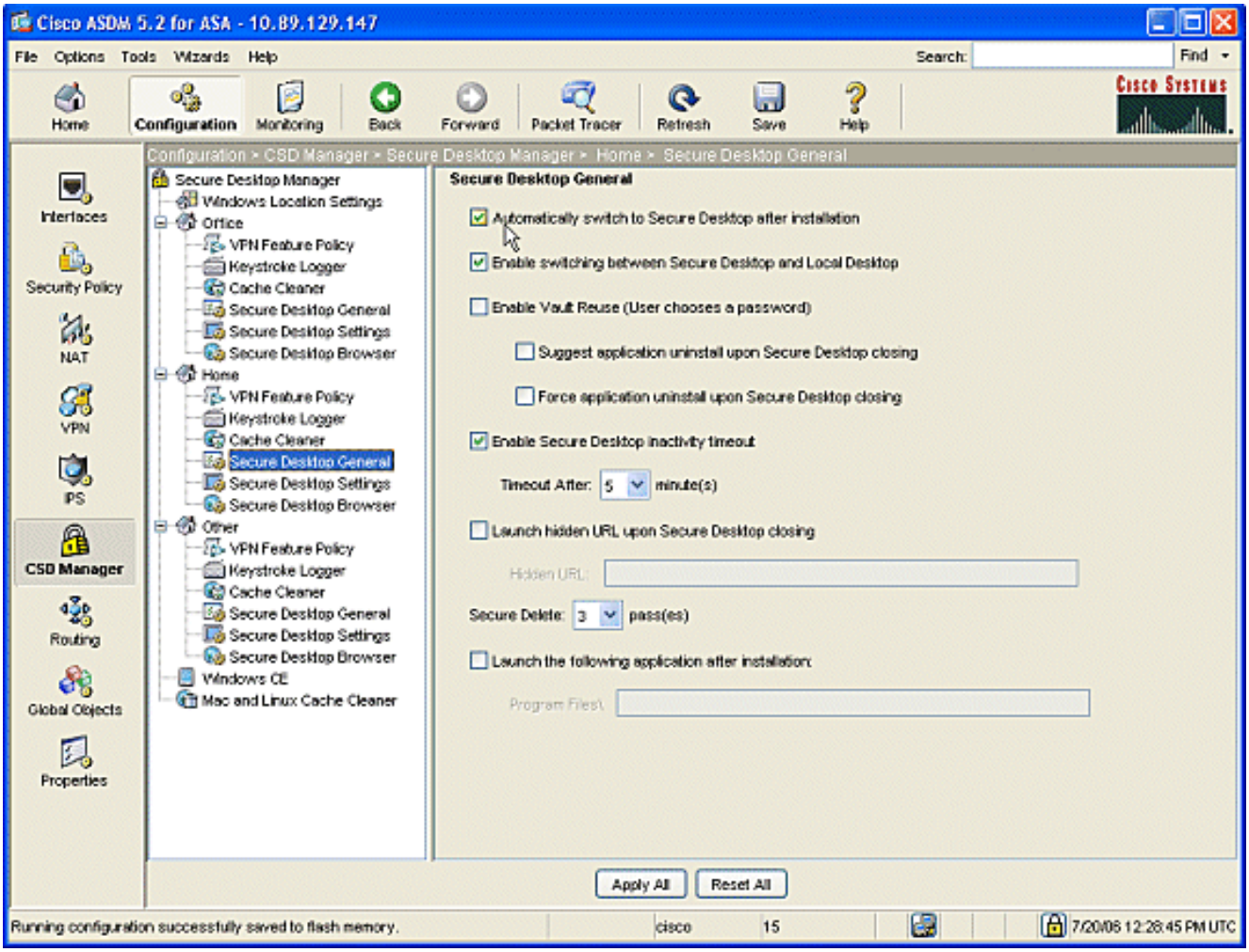
1. بالنسبة لعملاء Office، لا تفعل شيئا حيث لم يتم إختيار "منظف سطح المكتب الآمن وذاكرة التخزين المؤقت" في الخطوات السابقة. يسمح لك تطبيق ASDM بتكوين "منظف ذاكرة التخزين المؤقت" حتى في حالة عدم إختياره في خطوة سابقة. الاحتفاظ بالإعدادات الافتراضية لمواقع Office.**ملاحظة:** لا يتم مناقشة سياسة ميزة الشبكة الخاصة الظاهرية (VPN) في هذه الخطوة، ولكن ستتم مناقشتها في خطوة تالية لجميع المواقع.
2. بالنسبة للعملاء المنزليين، انقر فوق **الصفحة الرئيسية** و**مسجل ضغطات المفاتيح** في جزء التنقل.في نافذة مسجل ضربات المفاتيح، تحقق **من مشغلات ضغطات المفاتيح**.انقر **تطبيق الكل** في نافذة مسجل ضربات المفاتيح.انقر فوق **حفظ**، ثم انقر فوق **نعم** لقبول التغييرات.



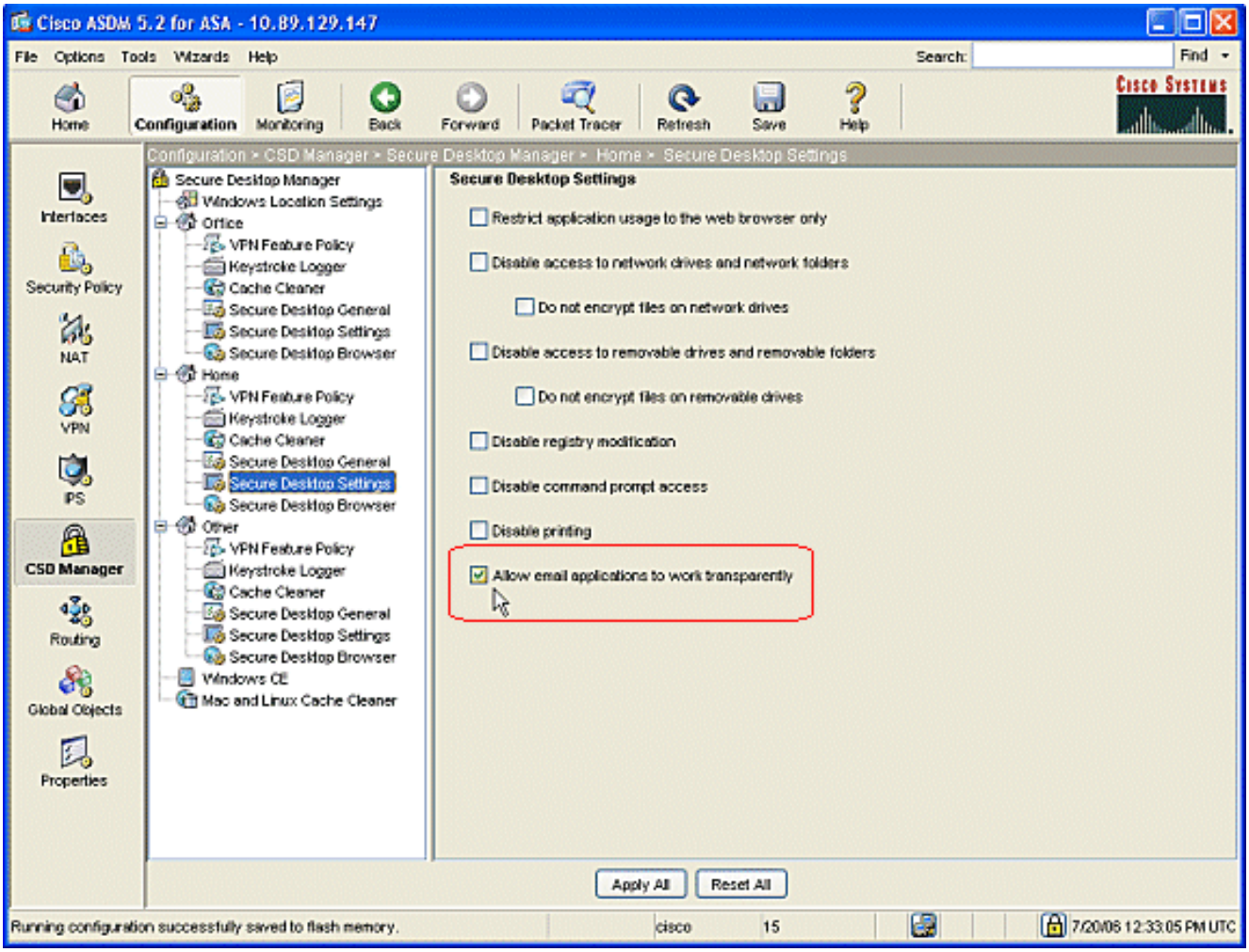
3. تحت الصفحة الرئيسية، أختر **منظف ذاكرة التخزين المؤقت** والمعلمات التي تناسب بيئتك.



4. تحت الصفحة الرئيسية، أختر **Secure Desktop General** والمعلمات التي تلائم بيئتك.



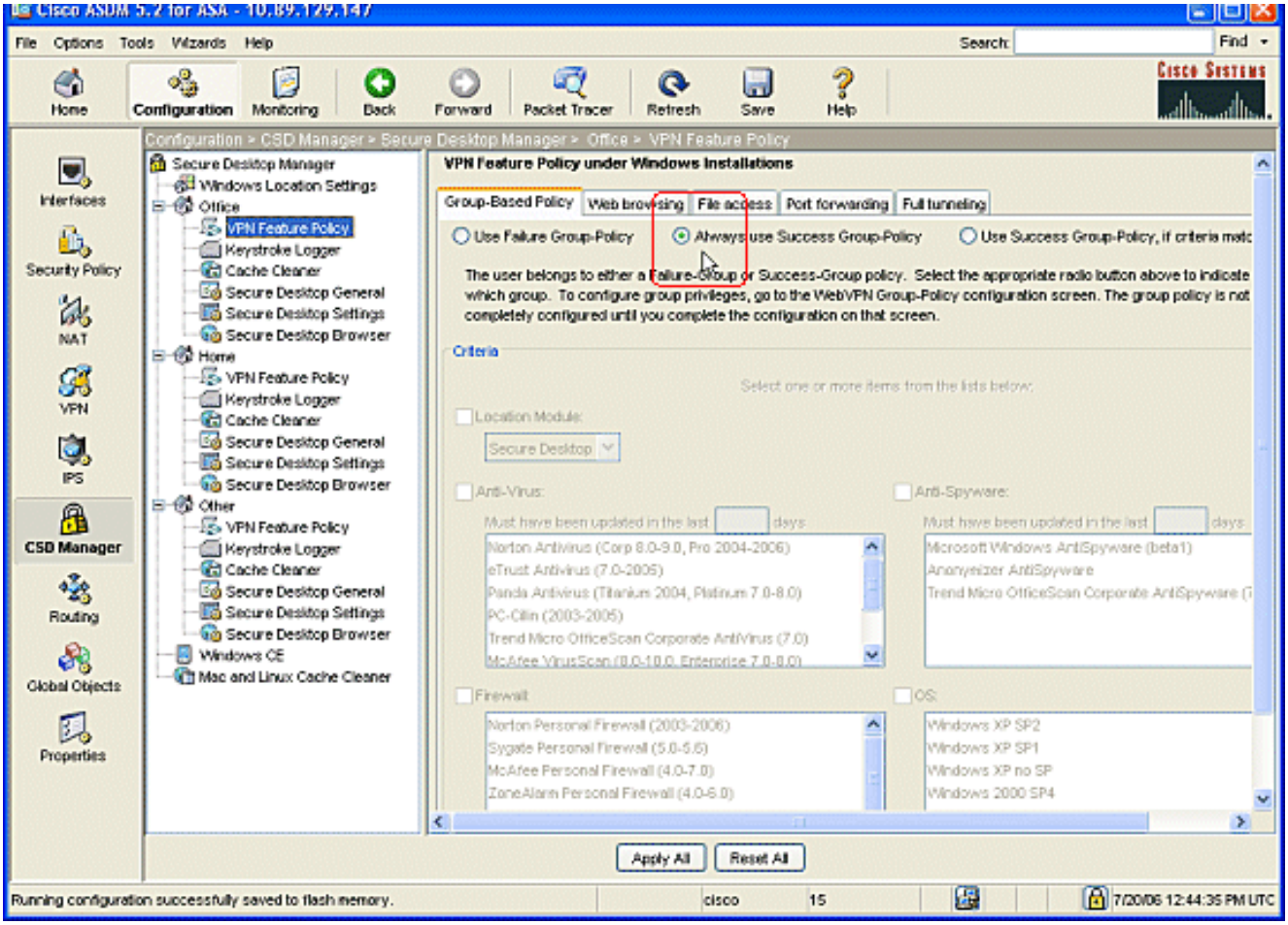
5. تحت المنزل، أختر **إعدادات سطح المكتب الآمنة**.حدد **السماح لتطبيقات البريد الإلكتروني بالعمل بشفافية**، وقم بتكوين الإعدادات الأخرى لتناسب بيئتك.انقر فوق **تطبيق الكل**.انقر فوق **حفظ**، ثم انقر فوق **نعم** لقبول التغييرات.



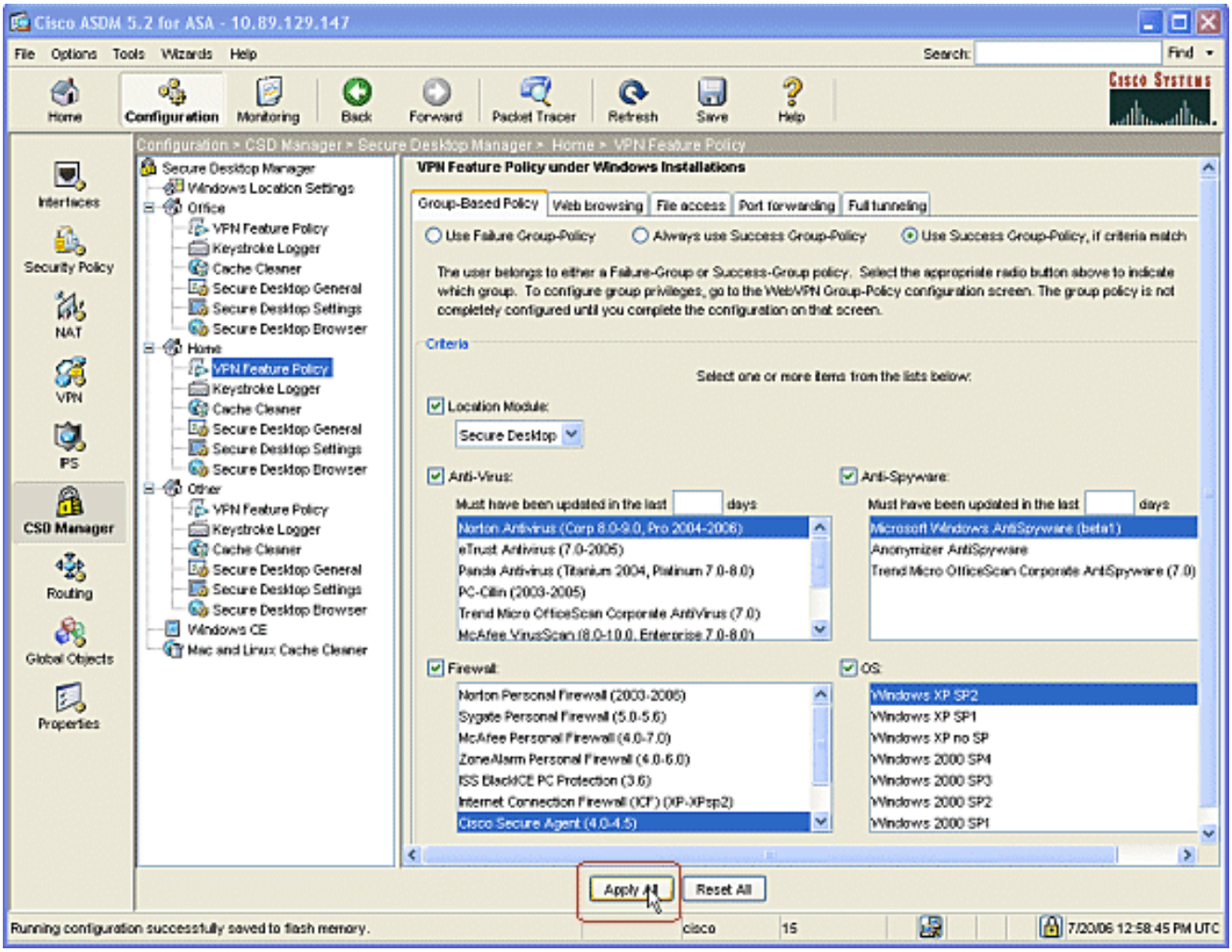
تكوين ميزات موقع Windows

قم بتكوين نهج ميزة VPN لكل موقع من المواقع التي قمت بإنشائها.

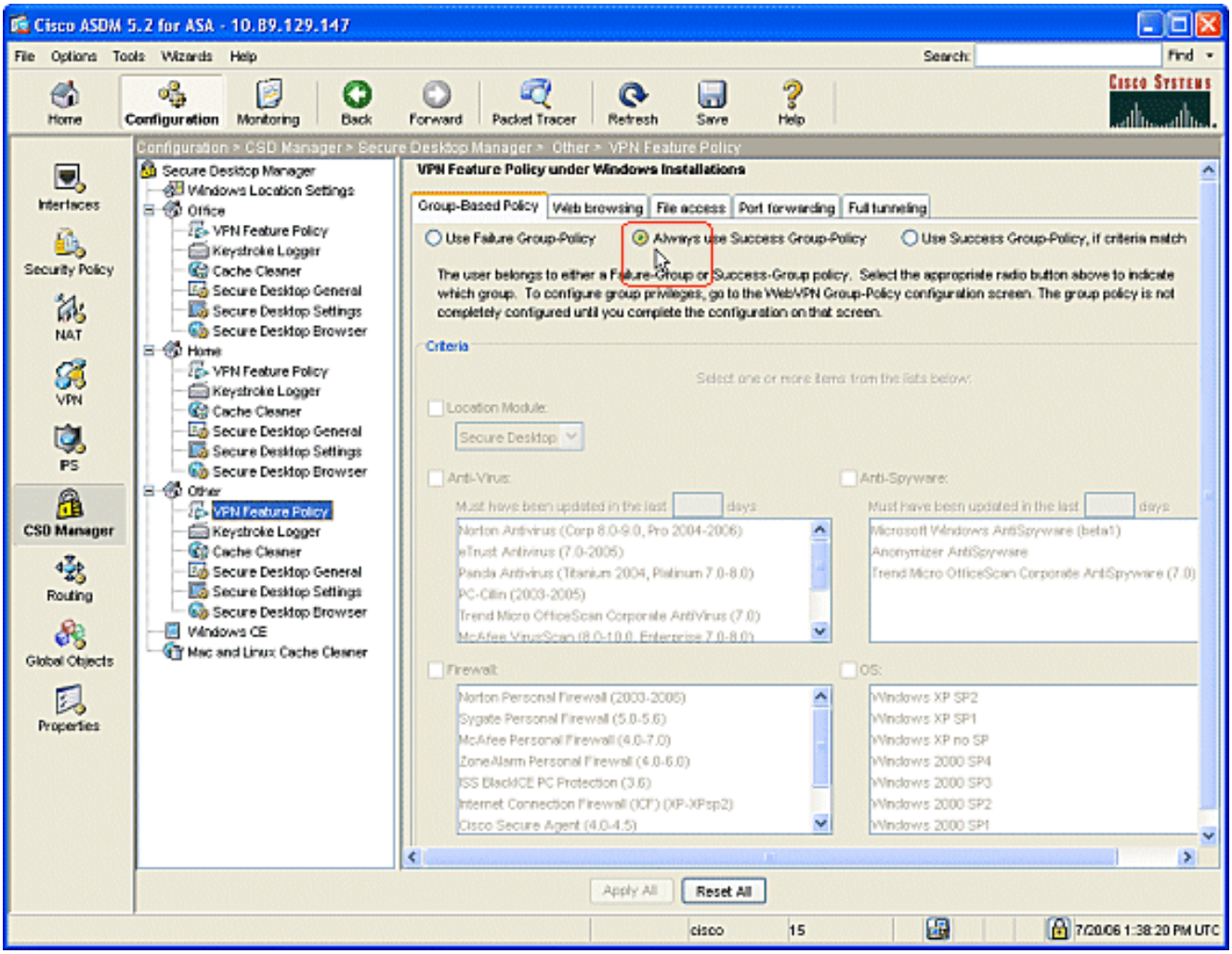
1. في جزء التنقل، انقر فوق **Office**، ثم انقر فوق **نهج ميزة VPN**.
2. انقر فوق علامة التبويب **نهج مستند إلى مجموعة**.انقر فوق الزر **إستخدام** راديو **نهج مجموعة النجاح دائما**.انقر على علامة التبويب **إستعراض الويب**، وحدد زر الخيار **تمكين** دائما.اتبع الإجراء نفسه لعلامات التبويب **الوصول إلى الملف وإعادة توجيه المنفذ والاتصال النفقي الكامل**.انقر فوق **تطبيق الكل**.انقر فوق **حفظ**، ثم انقر فوق **نعم** لقبول
التغييرات.



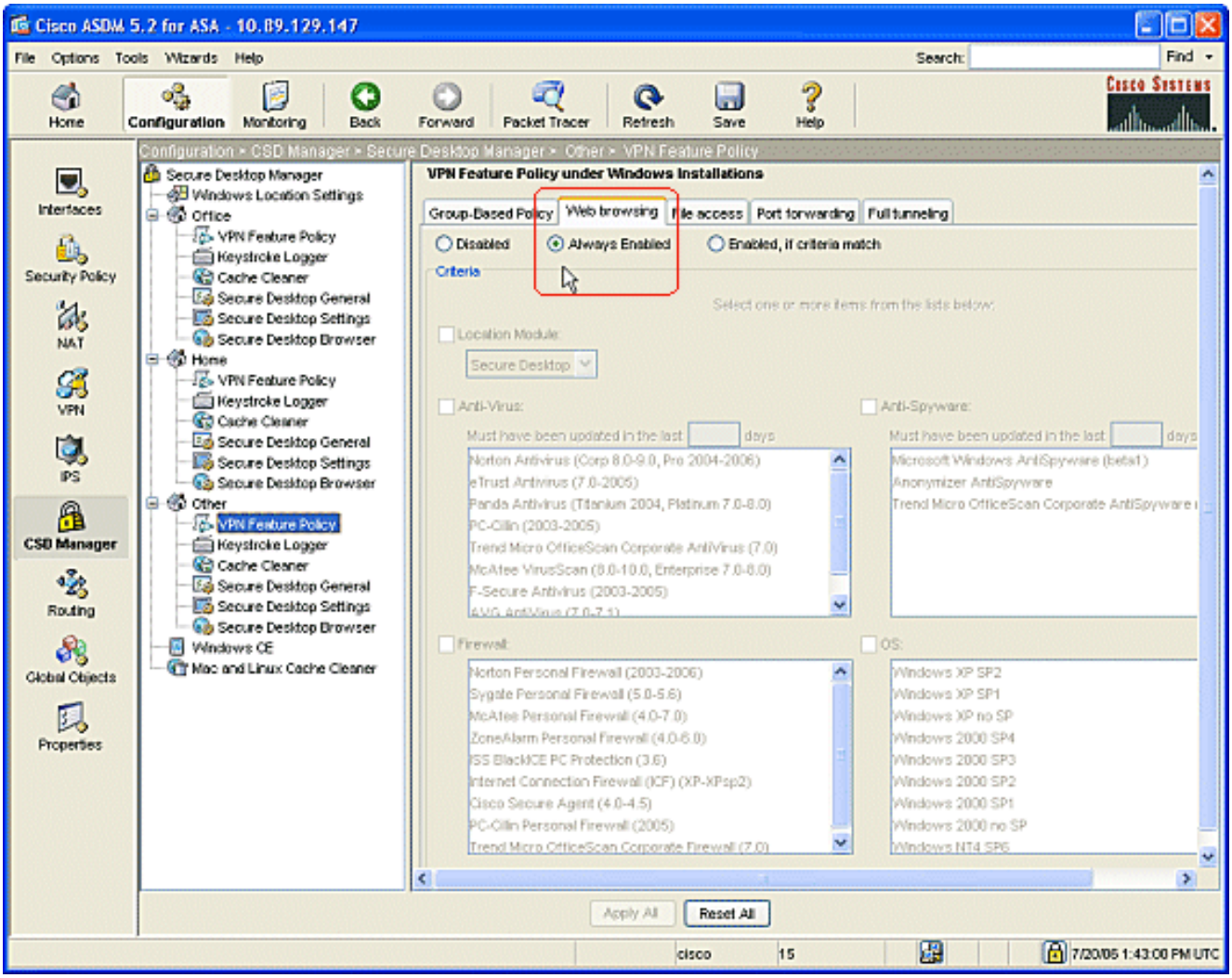
3. بالنسبة لمستخدمي المنازل، يمكن لكل شركة طلب سياسات محددة قبل السماح بالوصول. في جزء التنقل، انقر فوق **الصفحة الرئيسية**، ثم انقر فوق **نهج ميزة VPN**.انقر فوق علامة التبويب **نهج مستند إلى مجموعة**.انقر فوق زر **إستخدام نهج مجموعة النجاح** في حالة تطابق معايير تم تكوينها مسبقا، مثل مفتاح تسجيل محدد أو اسم ملف معروف أو شهادة رقمية.حدد خانة الاختيار **وحدة الموقع النمطية** واختر **سطح المكتب الآمن**.أختر مناطق **مكافحة الفيروسات وبرامج مكافحة التجسس وجدار الحماية** و**نظام التشغيل** وفقا لسياسة أمان الشركة. لن يسمح للمستخدمين المنزليين بالدخول إلى الشبكة ما لم تكن أجهزة الكمبيوتر الخاصة بهم تفي بالمعايير التي تم
تكوينها.



4. في جزء التنقل، انقر فوق **آخر** وانقر فوق **نهج ميزة VPN**.انقر فوق علامة التبويب **نهج مستند إلى مجموعة**.انقر فوق الزر **إستخدام** راديو **نهج مجموعة النجاح دائما**.



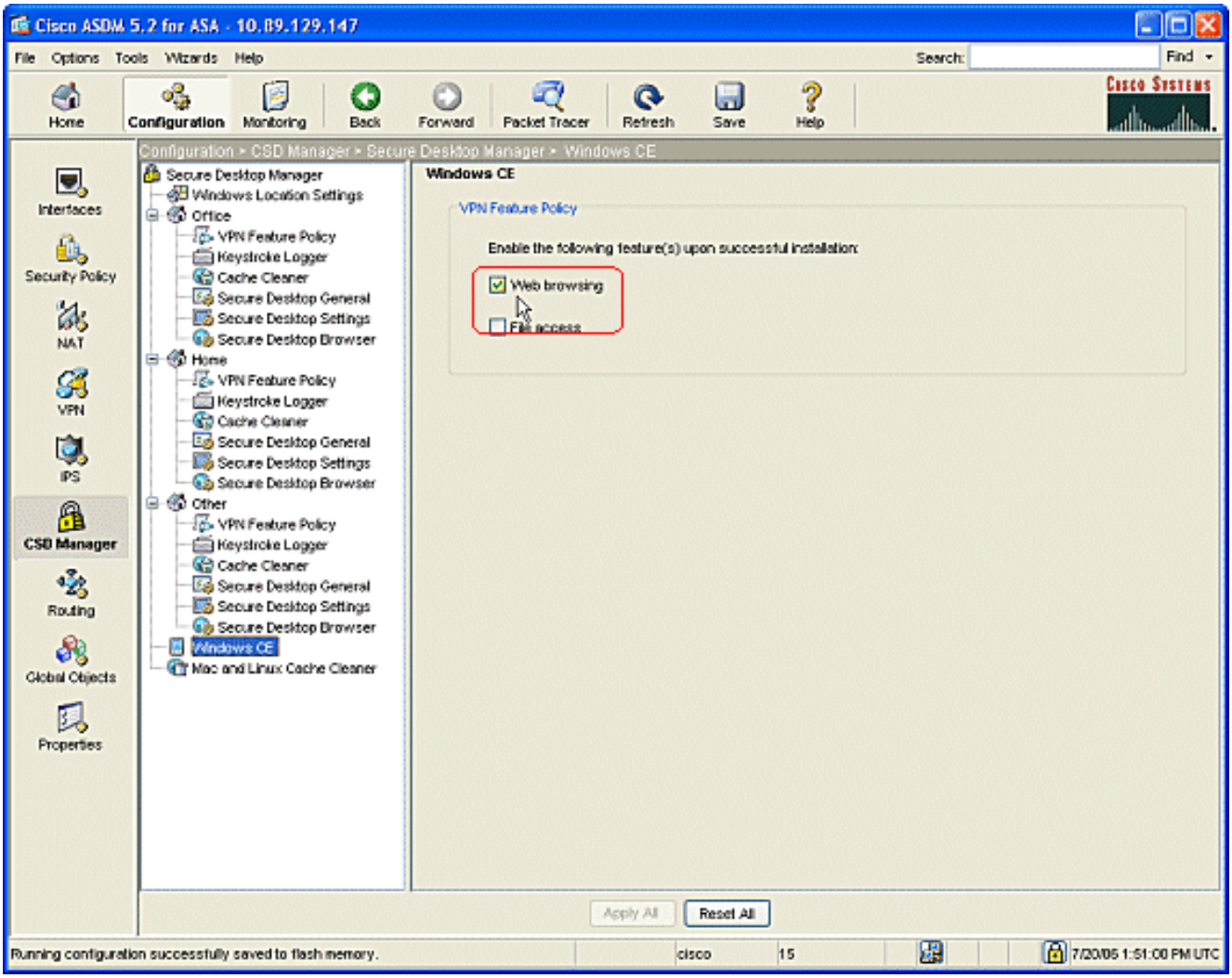
5. بالنسبة للعملاء في موقع **نهج ميزة VPN** هذا، انقر فوق علامة التبويب **إستعراض الويب**، وانقر فوق الطلب اللاسلكي **الذي يتم تمكينه دائما**.انقر فوق علامة التبويب **الوصول إلى الملف**، وانقر فوق الزر **تعطيل** الراديو.كرر الخطوة باستخدام علامات التبويب **إعادة توجيه المنفذ** و**الاتصال النفقي الكامل**.انقر فوق **تطبيق الكل**.انقر فوق **حفظ**، ثم انقر فوق **نعم** لقبول التغييرات.



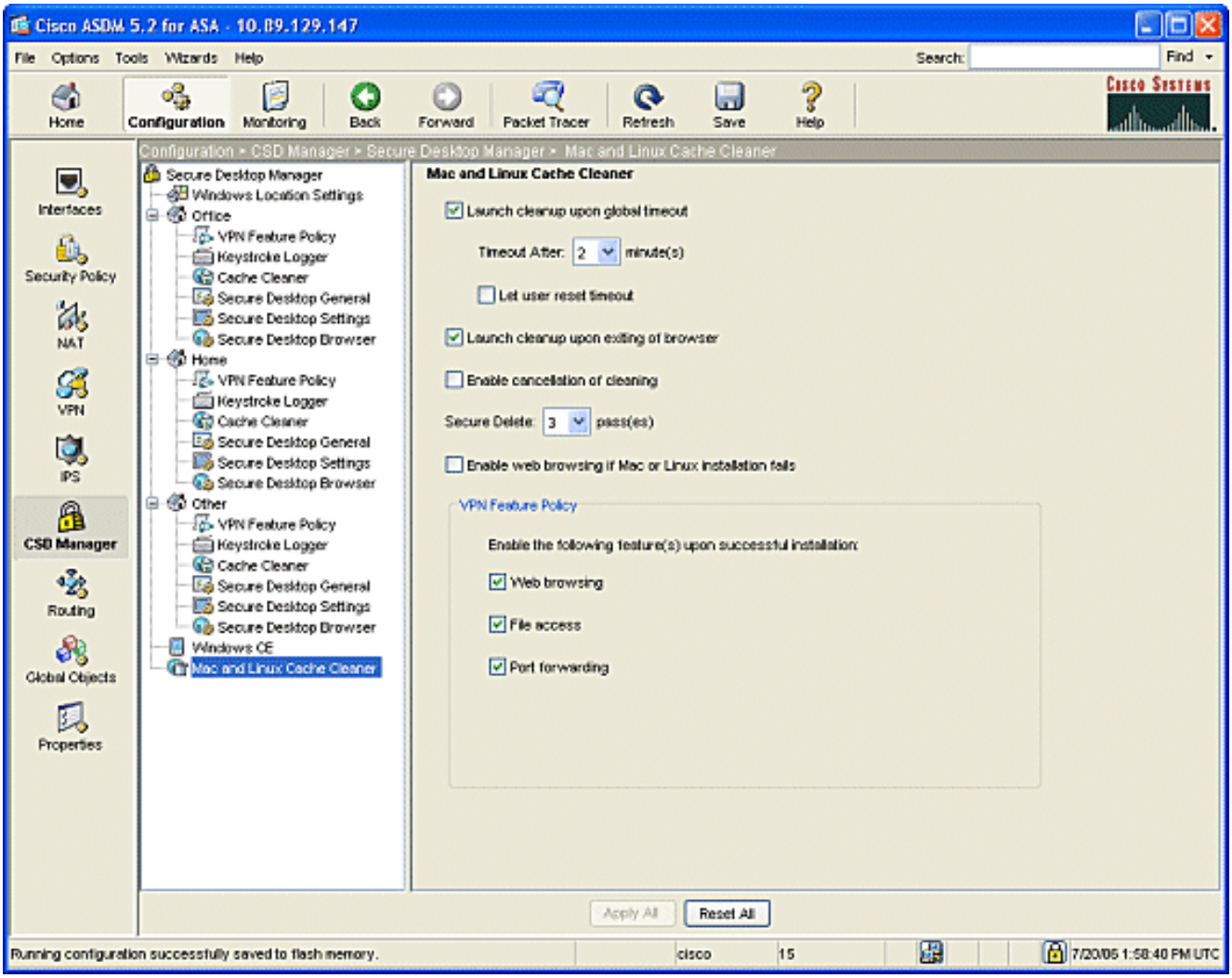
عمليات تهيئة إختيارية لعملاء Windows CE و Macintosh و Linux

وهذه التكوينات إختيارية.

1. إذا أخترت **Windows CE** من لوحة التصفح، حدد خانة الاختيار **إستعراض الويب**.



2. إذا أخترت **منظف لذاكرة التخزين المؤقت من Mac و Linux** من لوح التصفح، فتحقق من **تنظيف الإطلاق على** اتصال لاسلكي **للمهلة العالمية**.قم بتغيير المهلة إلى مواصفاتك.ضمن منطقة **نهج ميزة VPN**، تحقق من **إستعراض الويب والوصول إلى الملفات** ورسائل **إعادة توجيه المنافذ** لهؤلاء العملاء.



3. سواء أخترت نظام التشغيل Windows CE أو Mac أو Linux Cache Clean، انقر **تطبيق الكل**.
4. انقر فوق **حفظ**، ثم انقر فوق **نعم** لقبول التغييرات.

التكوين

التكوين

يعكس هذا التكوين التغييرات التي تم إجراؤها على ASDM لتمكين CSD: يتم الاحتفاظ بمعظم تكوينات CSD في ملف منفصل على ذاكرة Flash (الذاكرة المؤقتة).

سيسكوسا

```
ciscoasa#show running-config
...Building configuration
(ASA Version 7.2(1

!

hostname ciscoasa

domain-name cisco.com

enable password 2KFQnbNIdI.2KYOU encrypted

names
```

```
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 10.2.2.1 255.255.255.0
!
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name cisco.com
no pager
logging enable
logging asdm informational
mtu outside 1500
```

```
mtu inside 1500

                                        ASDM location on disk0 asdm image ---!
   disk0:/asdm521.bin no asdm history enable arp timeout
    14400 nat-control timeout xlate 3:00:00 timeout conn
    1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
   timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
  0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media
       0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
   timeout uauth 0:05:00 absolute !--- some group policy
    attributes group-policy GroupPolicy1 internal group-
policy GroupPolicy1 attributes vpn-tunnel-protocol IPSec
l2tp-ipsec webvpn webvpn functions url-entry file-access
        file-entry file-browsing username user1 password
  mbO2jYs13AXlIAGa encrypted privilege 15 username user1
 attributes vpn-group-policy GroupPolicy1 username cisco
        password 3USUcOPFUiMCO4Jk encrypted privilege 15
username cisco attributes vpn-group-policy DfltGrpPolicy
        webvpn port-forward none port-forward-name value
     Application Access http server enable http 10.2.2.0
   255.255.255.0 inside no snmp-server location no snmp-
           server contact snmp-server enable traps snmp
    authentication linkup linkdown coldstart !--- tunnel
       group information tunnel-group DefaultWEBVPNGroup
    general-attributes default-group-policy GroupPolicy1
  tunnel-group DefaultWEBVPNGroup webvpn-attributes hic-
    fail-group-policy GroupPolicy1 nbns-server 10.2.2.30
timeout 2 retry 2 telnet timeout 5 ssh timeout 5 console
 timeout 0 ! class-map inspection_default match default-
      inspection-traffic ! ! policy-map type inspect dns
    preset_dns_map parameters message-length maximum 512
       policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
    inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
      policy global_policy global !--- webvpn parameters
  webvpn port 1443 enable outside enable inside !--- csd
   location csd image disk0:/securedesktop-asa-3.1.1.32-
 k9.pkg csd enable customization DfltCustomization title
          text YOUR-COMPANY SSL VPN Services title style
background-color: rgb(204,204,255);color: rgb(51,0,255);
                  border-bottom:5px groove #669999;font-
size:larger;vertical-align:middle;text-align: left;font-
        weight:bold url-list ServerList "Windows Shares"
  cifs://10.2.2.30 1 url-list ServerList "Tacacs Server"
 http://10.2.2.69:2002 2 tunnel-group-list enable prompt
                                        hostname context
 Cryptochecksum:a840d81f0af21d869db4fa559e83d6d0 : end !
                                                    end
```

التحقق من الصحة

أستخدم هذا القسم للتأكد من أن التكوينات الخاصة بك ل SSL VPN بدون عملاء أو SSL VPN للعميل الدقيق أو SSL VPN Client (SVC) تعمل بشكل صحيح.

اختبر CSD باستخدام جهاز كمبيوتر تم تكوينه باستخدام مواقع Windows مختلفة. يجب أن يوفر كل إختبار وصولا مختلفا بما يتوافق مع السياسات التي قمت بتكوينها في المثال أعلاه.

يمكنك تغيير رقم المنفذ والواجهة حيث يستمع Cisco ASA إلى إتصالات WebVPN.

- المنفذ الافتراضي هو 443. إن يستعمل أنت التقصير ميناء، الوصول هو **https://ASA ip عنوان**.
- يؤدي إستخدام منفذ مختلف إلى تغيير الوصول إلى **https://ASA IP address:newPortNumber**.

الأوامر

يتم إقران العديد من أوامر **العرض** مع WebVPN. يمكنك تنفيذ هذه الأوامر في واجهة سطر الأوامر (CLI) لإظهار الإحصائيات ومعلومات أخرى. للاطلاع على إستخدام أوامر **show** بالتفصيل، ارجع إلى التحقق من تكوين WebVPN.

ملاحظة: الإنتاج مترجم بساند أداة (يسجل زبون فقط) (OIT) مؤكد **عرض** أمر. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

إذا واجهت مشاكل مع العميل البعيد، فتحقق مما يلي:

1. هل تم تمكين الإطارات المنبثقة و/أو Java و/أو ActiveX في مستعرض الويب؟ قد يلزم تمكين هذه الشبكات بناء على نوع اتصال SSL VPN قيد الاستخدام.
2. يجب أن يقبل العميل الشهادات الرقمية المقدمة في بداية الجلسة.

الأوامر

تقترن العديد من أوامر **تصحيح الأخطاء** ب WebVPN. للحصول على معلومات تفصيلية حول هذه الأوامر، ارجع إلى إستخدام أوامر تصحيح الأخطاء ل WebVPN..

ملاحظة: يمكن أن يؤثر إستخدام أوامر **تصحيح الأخطاء سلبا** على جهاز Cisco الخاص بك. قبل إستخدام أوامر **debug**، ارجع إلى معلومات مهمة عن أوامر تصحيح الأخطاء.

معلومات ذات صلة

- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- ASA مع WebVPN وتسجيل دخول أحادي باستخدام مثال تكوين ASDM و NTLMv1
- الدعم التقني والمستندات - Cisco Systems

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).