適用於Windows的ASA 7.2.x上的Cisco Secure Desktop(CSD 3.1.x)使用ASDM的配置示例

目錄

簡介

Cisco Secure Desktop(CSD)擴展了SSL VPN技術的安全性。CSD在使用者的工作站上為會話活動提供一個單獨的分割槽。此保管庫區域在會話期間加密，並在SSL VPN會話結束時完全刪除。Windows可以配置CSD的全部安全優勢。Macintosh 、 Linux和Windows CE只能訪問Cache Cleaner 、 Web Browsing和File Access功能。可以在以下平台上為Windows、Macintosh、Windows CE和Linux裝置配置CSD:

- 思科調適型安全裝置(ASA)5500系列
- 執行Cisco IOS®軟體版本12.4(6)T和更新版本的思科路由器
- Cisco VPN 3000系列集中器版本4.7及更高版本
- Catalyst 6500和7600系列路由器上的Cisco WebVPN模組

注意：CSD 3.3版現在允許您將Cisco Secure Desktop配置為在運行Microsoft Windows Vista的遠端電腦上運行。以前，Cisco Secure Desktop僅限於運行Windows XP或2000的電腦。如需詳細資訊，請參閱Cisco Secure Desktop 3.3版版本說明的新功能增強 — Vista上的安全案頭一節。

本示例主要介紹在ASA 5500系列上為Windows客戶端安裝和配置CSD。新增了Windows CE、Mac和Linux客戶端的可選配置以完成。

CSD與SSL VPN技術(無客戶端SSL VPN、瘦客戶端SSL VPN或SSL VPN客戶端(SVC))結合使用。CSD為SSL VPN技術的安全會話增加了價值。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

ASA裝置的要求

- Cisco CSD 3.1版或更高版本
- Cisco ASA軟體7.1.1版或更高版本
- 思科自適應安全裝置管理器(ASDM)5.1.1版或更高版本**注意：**僅ASA 8.x版支援CSD 3.2版**註**：請參閱允許ASDM進行HTTPS訪問，以便允許ASDM配置ASA。

客戶端電腦的要求

- 遠端客戶端應具有本地管理許可權；這不是必需的，但強烈建議這樣做。
- 遠端客戶端必須具有Java Runtime Environment(JRE)1.4版或更高版本。
- 遠端客戶端瀏覽器：Internet Explorer 6.0、Netscape 7.1、Mozilla 1.7、Safari 1.2.2或Firefox 1.0
- 在遠端客戶端上啟用Cookie和允許彈出視窗

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ASDM版本5.2(1)
- Cisco ASA版本7.2(1)
- Cisco CSD版本securedesktop-asa-3.1.1.32-k9.pkg

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態開始。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。此配置中使用的IP地址為RFC 1918地址。這些IP地址在Internet上不合法，只能在測試實驗室環境中使用。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

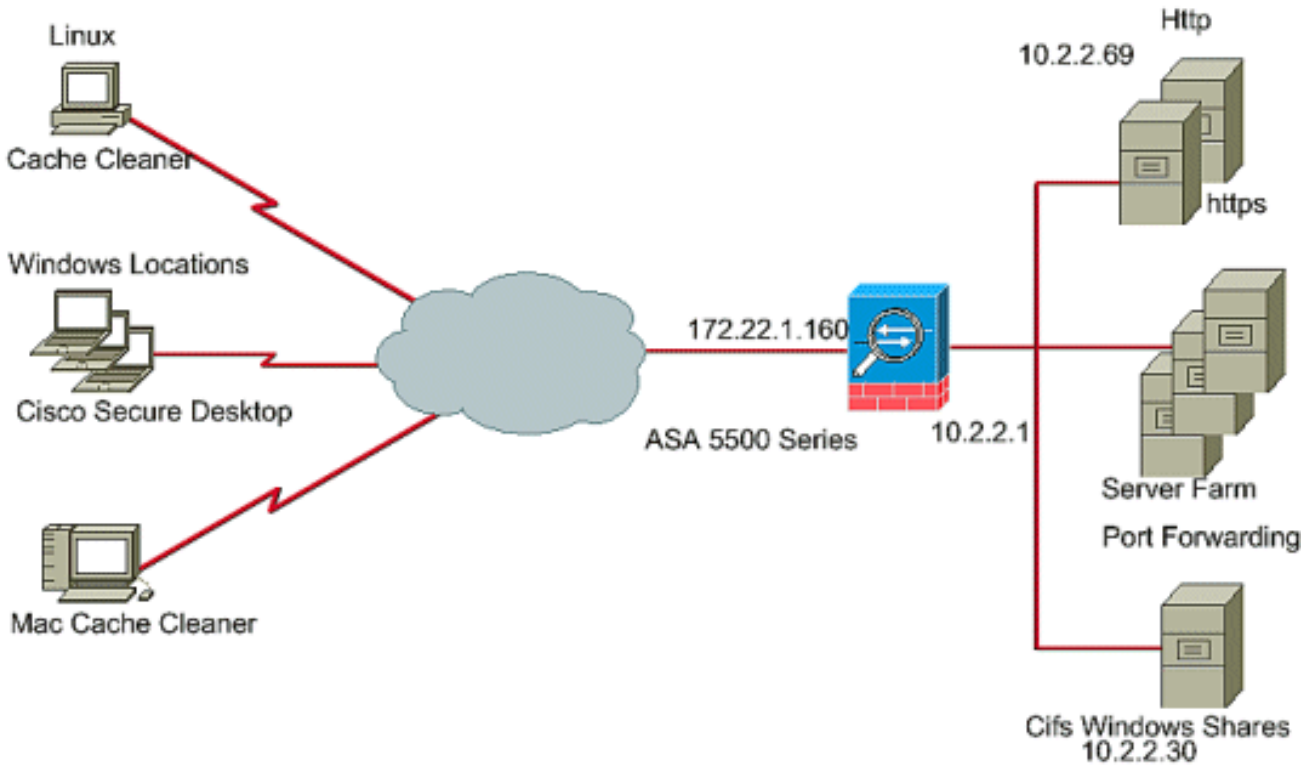
背景資訊

CSD使用SSL VPN技術運行，因此應在配置CSD之前啟用無客戶端、瘦客戶端或SVC。

網路圖表

可以利用CSD的完整安全功能配置不同的Windows位置。Macintosh、Linux和Windows CE只能訪問Cache Cleaner和/或Web瀏覽和檔案訪問。

本檔案會使用以下網路設定：



在ASA上為Windows客戶端配置CSD

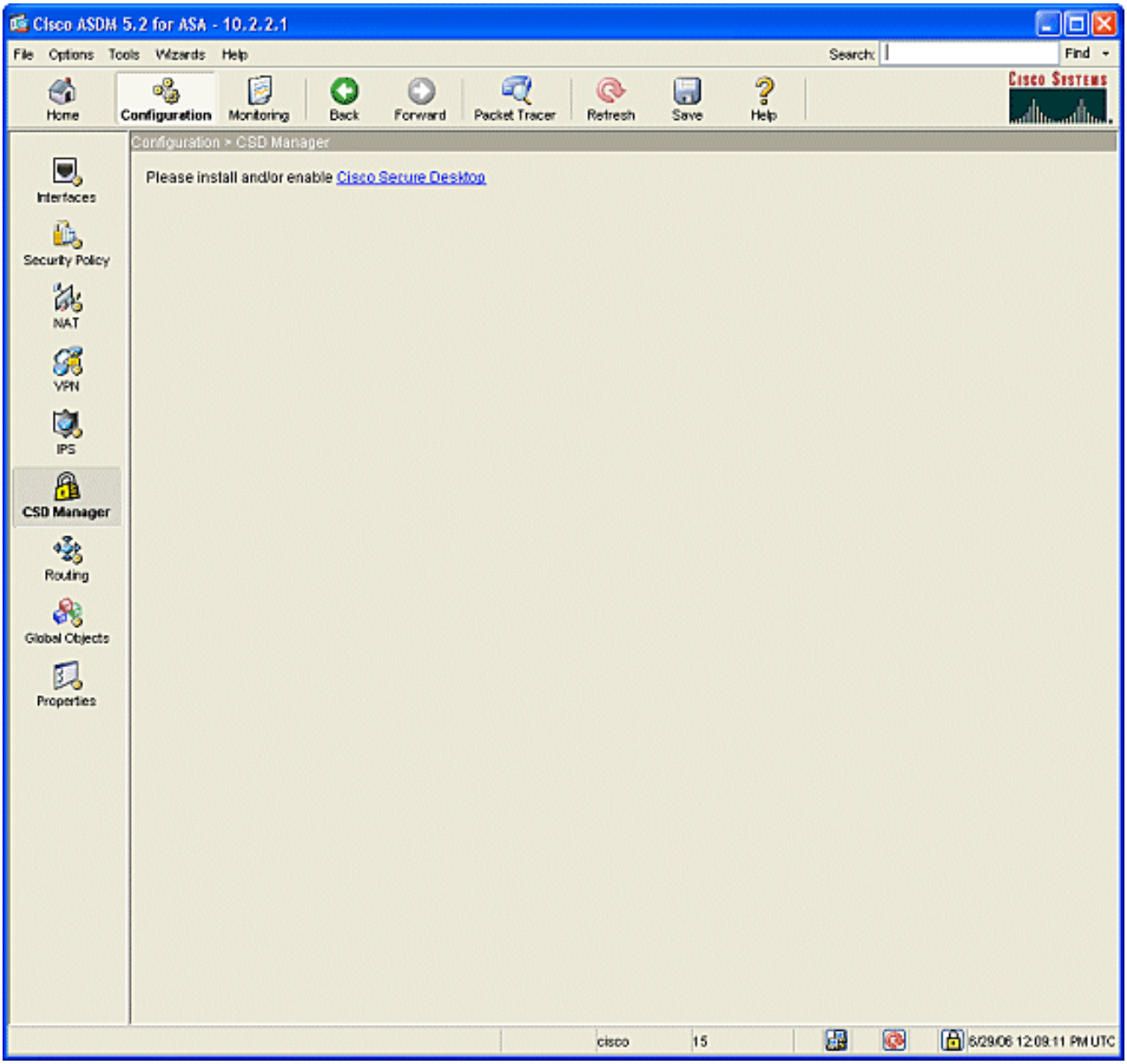
在ASA上為Windows客戶端配置CSD，主要步驟有五個：

- 在Cisco ASA上獲取、安裝並啟用CSD軟體。
- 定義Windows位置。
- 定義Windows位置標識。
- 配置Windows位置模組。
- 配置Windows位置功能。
- Windows CE、Macintosh和Linux客戶端的可選配置。

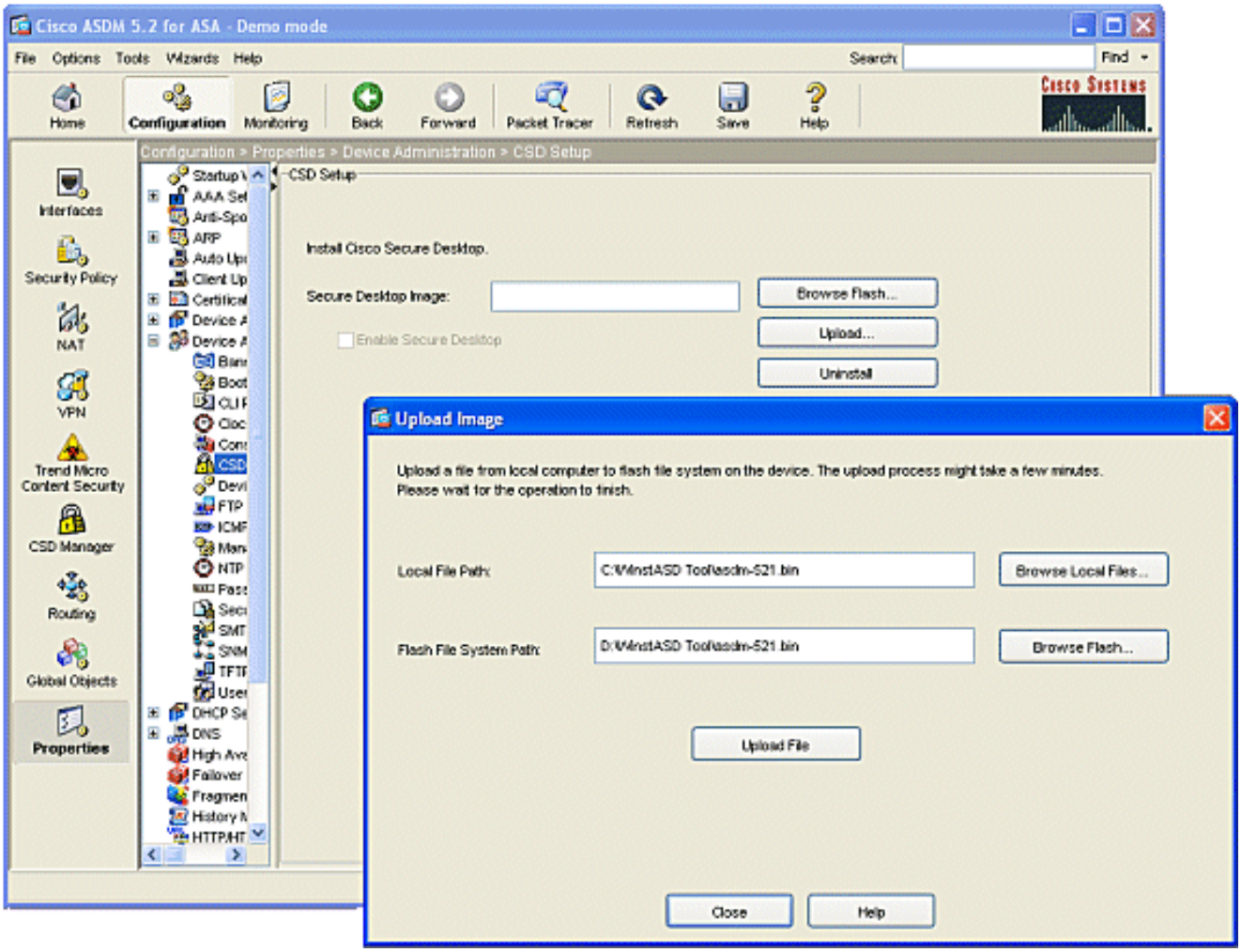
獲取、安裝和啟用CSD軟體

完成以下步驟，在Cisco ASA上獲取、安裝和啟用CSD軟體。

1. 從思科軟體下載網站將CSD軟體securedesktop-asa*.pkg和自述檔案下載到您的管理站。
2. 登入到ASDM，然後按一下**Configuration**按鈕。在左側選單中，按一下**CSD Manager**按鈕，然後按一下**Cisco Secure Desktop**連結。



3. 按一下**Upload**以顯示Upload Image視窗。輸入管理站上新的.pkg檔案的路徑，或按一下**Browse Local Files**以查詢檔案。輸入快閃記憶體上放置檔案的位置，或按一下**Browse Flash**。按一下「**Upload File**」。出現提示時，按一下**OK > Close > OK**。

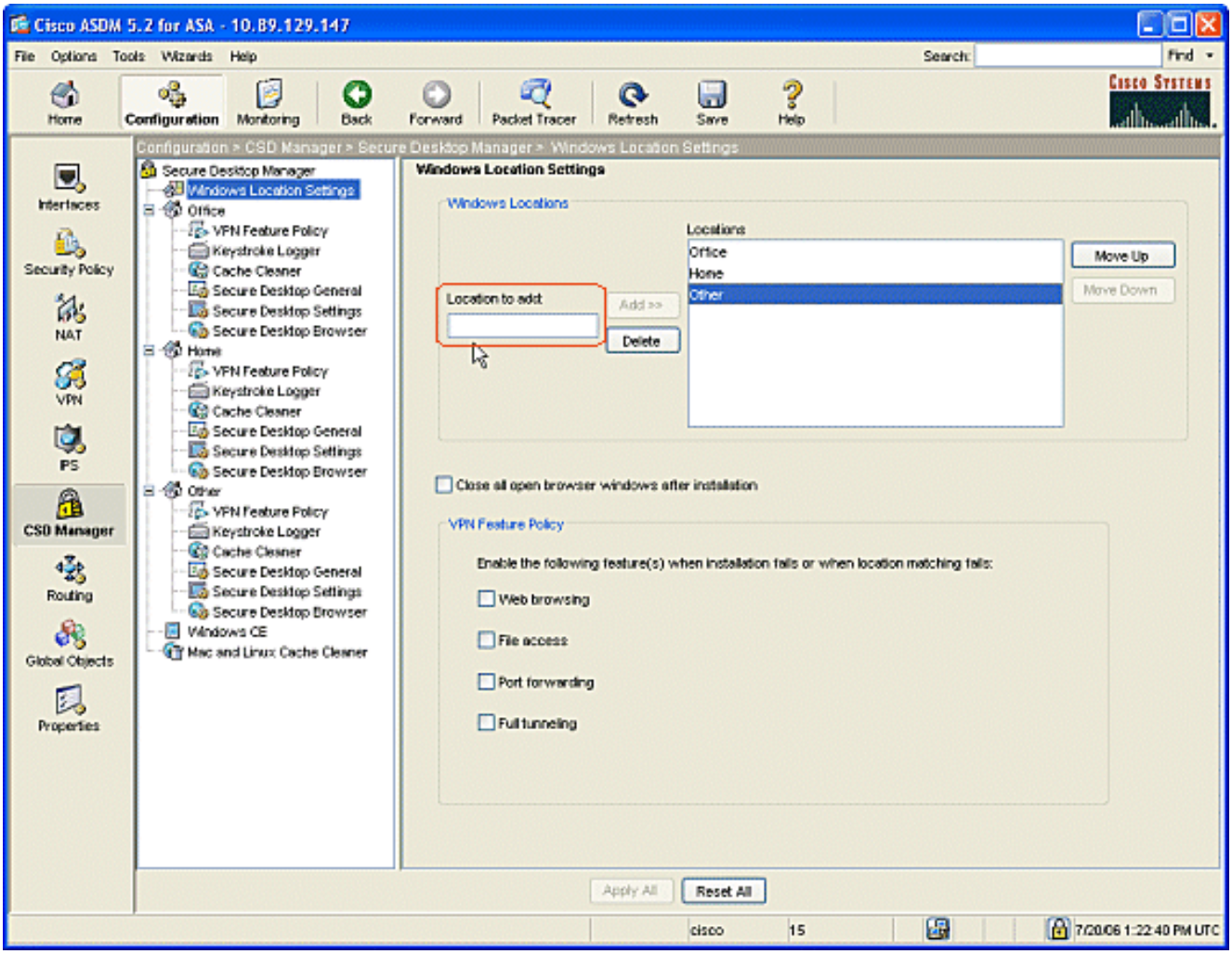


4. 將客戶端映像載入到快閃記憶體後，選中**Enable SSL VPN Client**覈取方塊，然後按一下**Apply**。
5. 按一下**Save**，然後按一下**Yes**接受更改。

定義Windows位置

完成以下步驟以定義Windows位置。

1. 按一下**Configuration**按鈕。
2. 在左側選單中，按一下**CSD Manager**按鈕，然後按一下**Cisco Secure Desktop**連結。
3. 在導航窗格中，按一下**Windows位置設定**。
4. 在「要新增的位置」欄位中鍵入位置名稱，然後按一下**新增**。請注意本示例中的三個位置：Office、Home等。Office表示位於公司安全邊界內的工作站。Home表示在家工作的使用者。Other表示除上述兩個位置以外的任何位置。

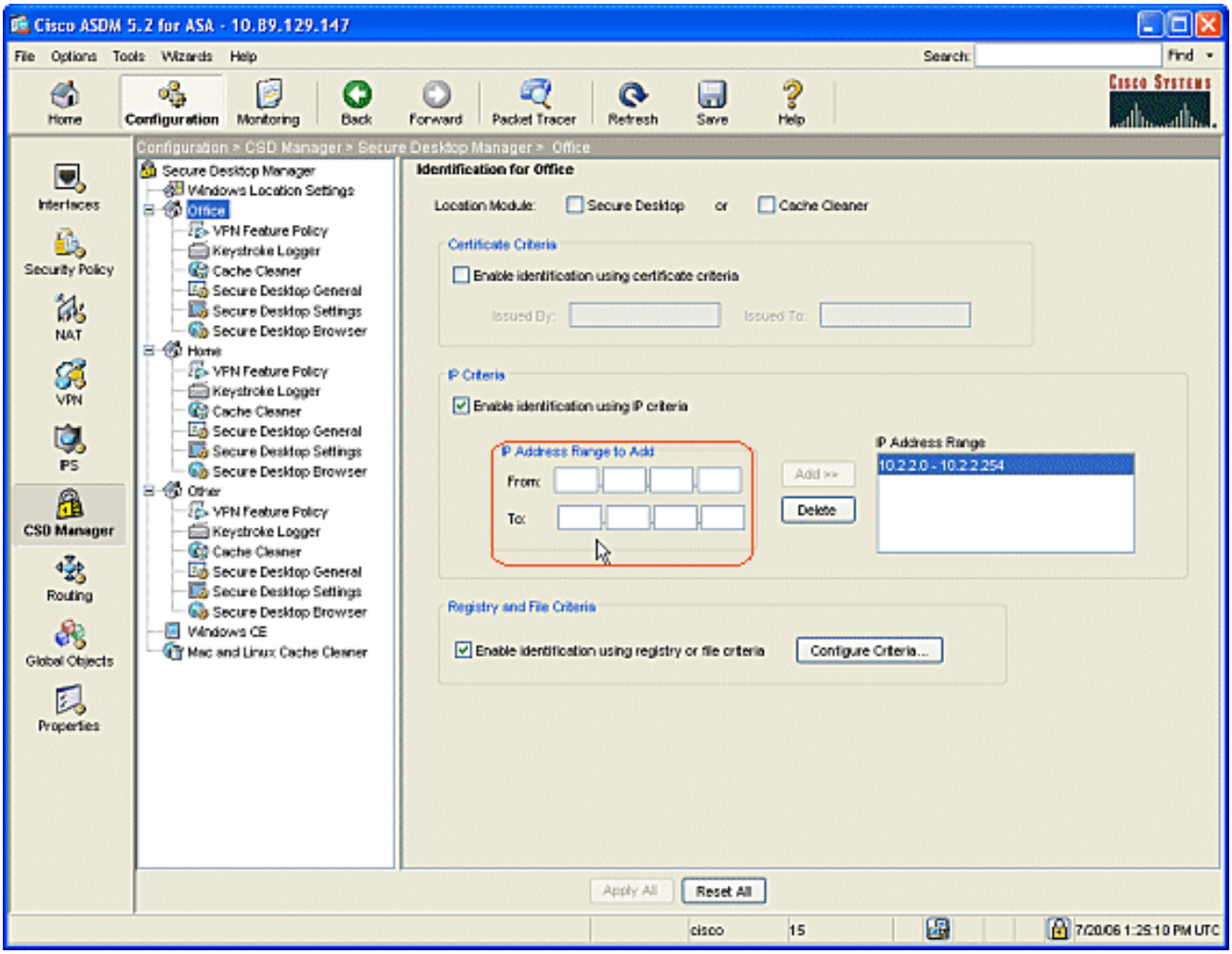


5. 根據銷售人員、訪客、合作夥伴和其他人的網路架構佈局，建立您自己的位置。
6. 建立Windows位置時，導航窗格會展開，每個新位置都包含可配置的模組。按一下「**Apply All**」。
7. 按一下**Save**，然後按一下**Yes**接受更改。

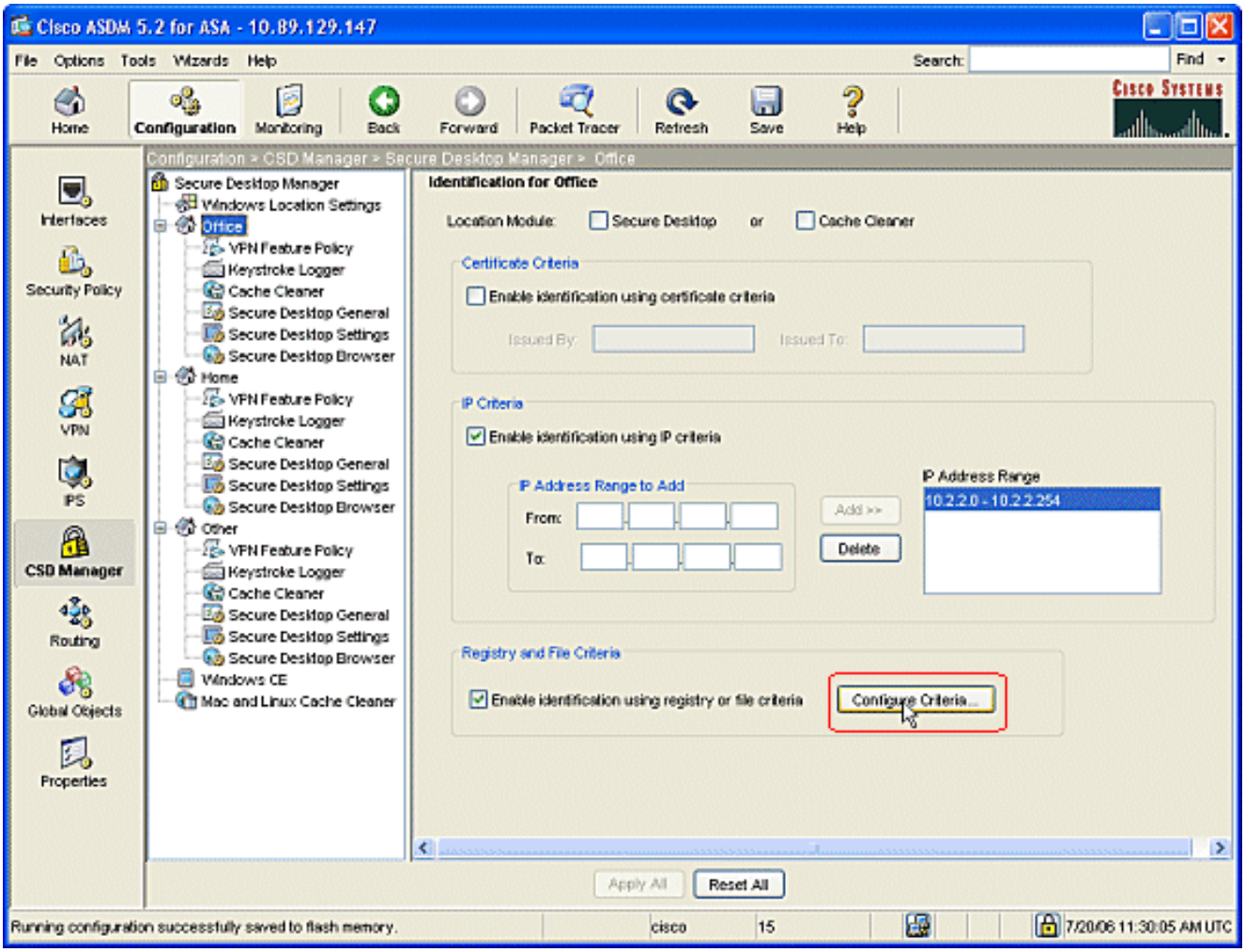
Windows位置標識

完成以下步驟以定義Windows位置標識。

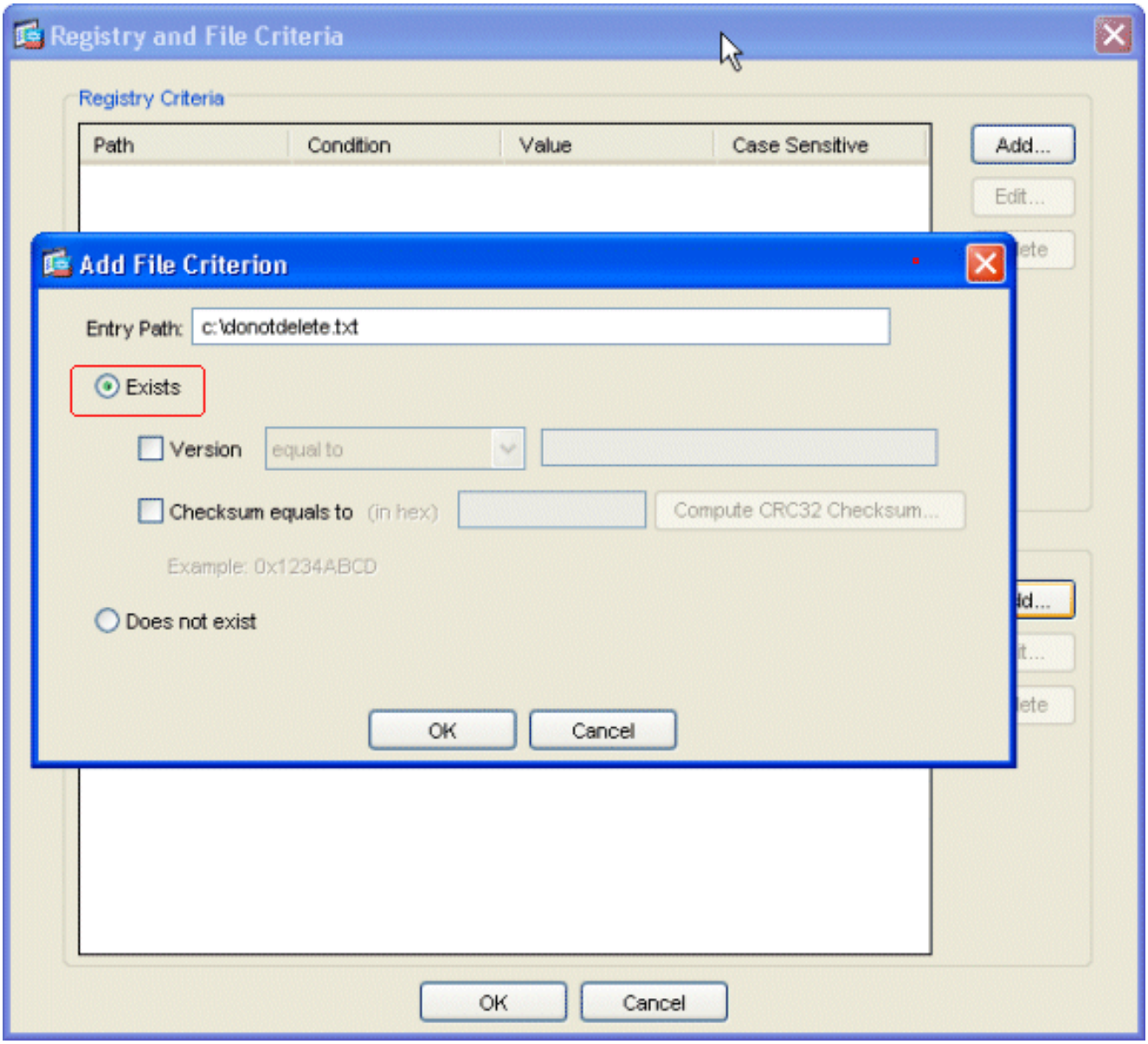
1. 確定在定義Windows位置中建立的位置。



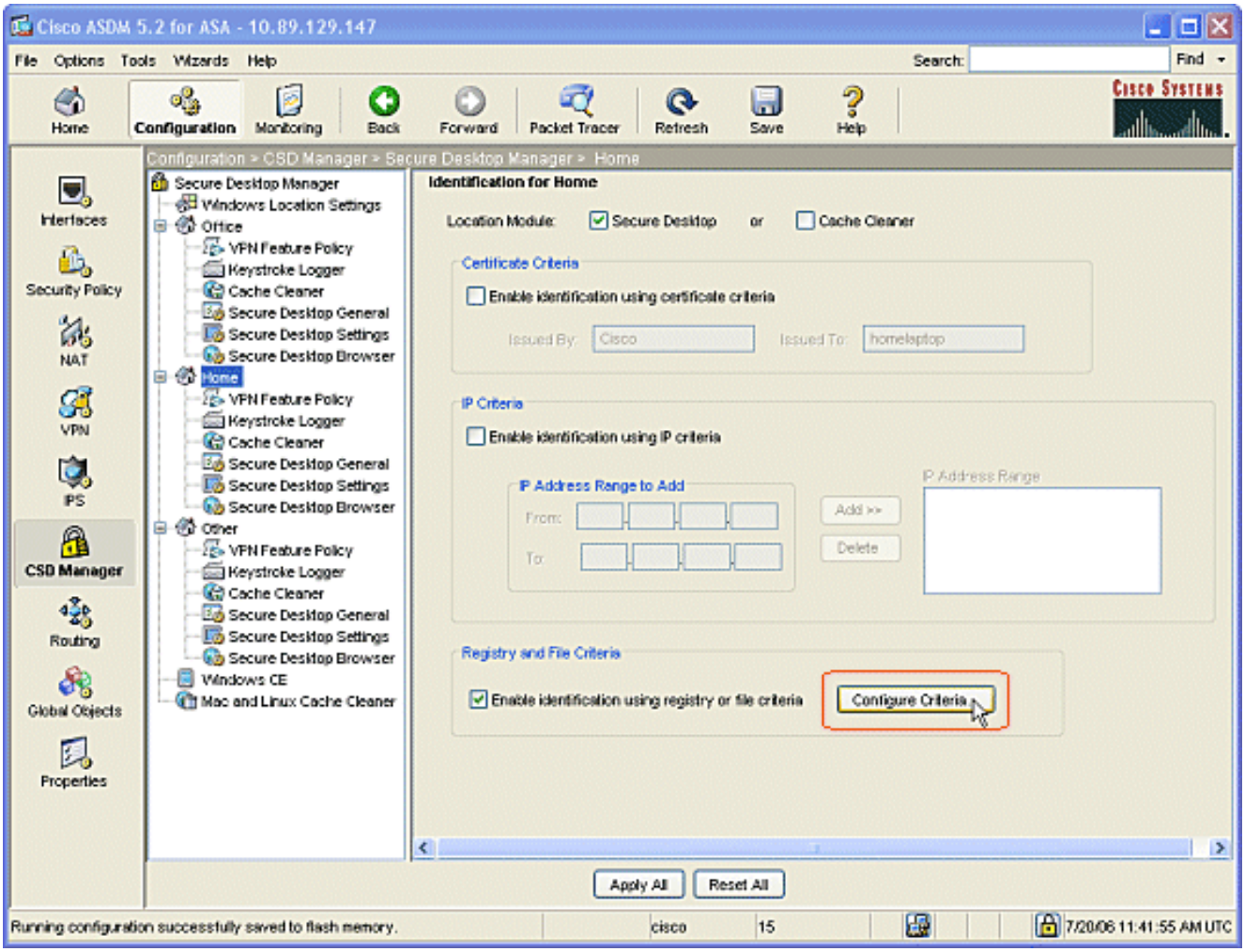
2. 要確定Office的位置，請在導航窗格中按一下**Office**。取消選中**Secure Desktop**和**Cache Cleaner**，因為這些是內部電腦。選中**Enable identification using IP criteria**。輸入內部電腦的IP地址範圍。選中**Enable identification using registry or file criteria**。這就將內部辦公室員工與網路中的臨時訪客區分開來。



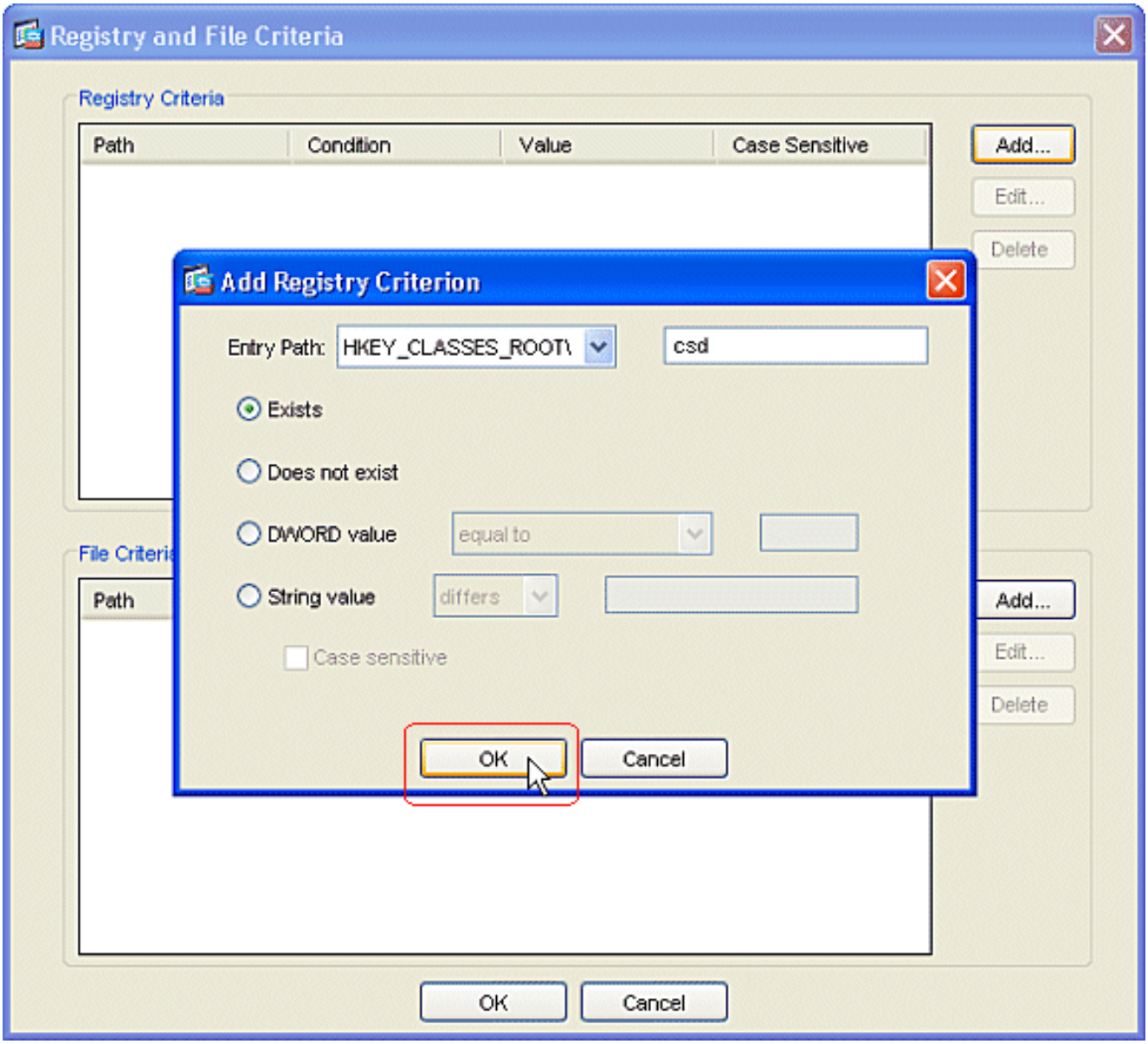
3. 按一下**Configure Criteria**。配置了一個簡單的檔案「DoNotDelete.txt」示例。此檔案必須存在於您的內部Windows電腦上，並且只是一個佔位符。您還可以配置Windows登錄檔項以識別內部辦公室電腦。在「Add File Criterion」視窗中按一下**OK**。在「Registry and File Criteria（登錄檔和檔案標準）」視窗中按一下**OK**。



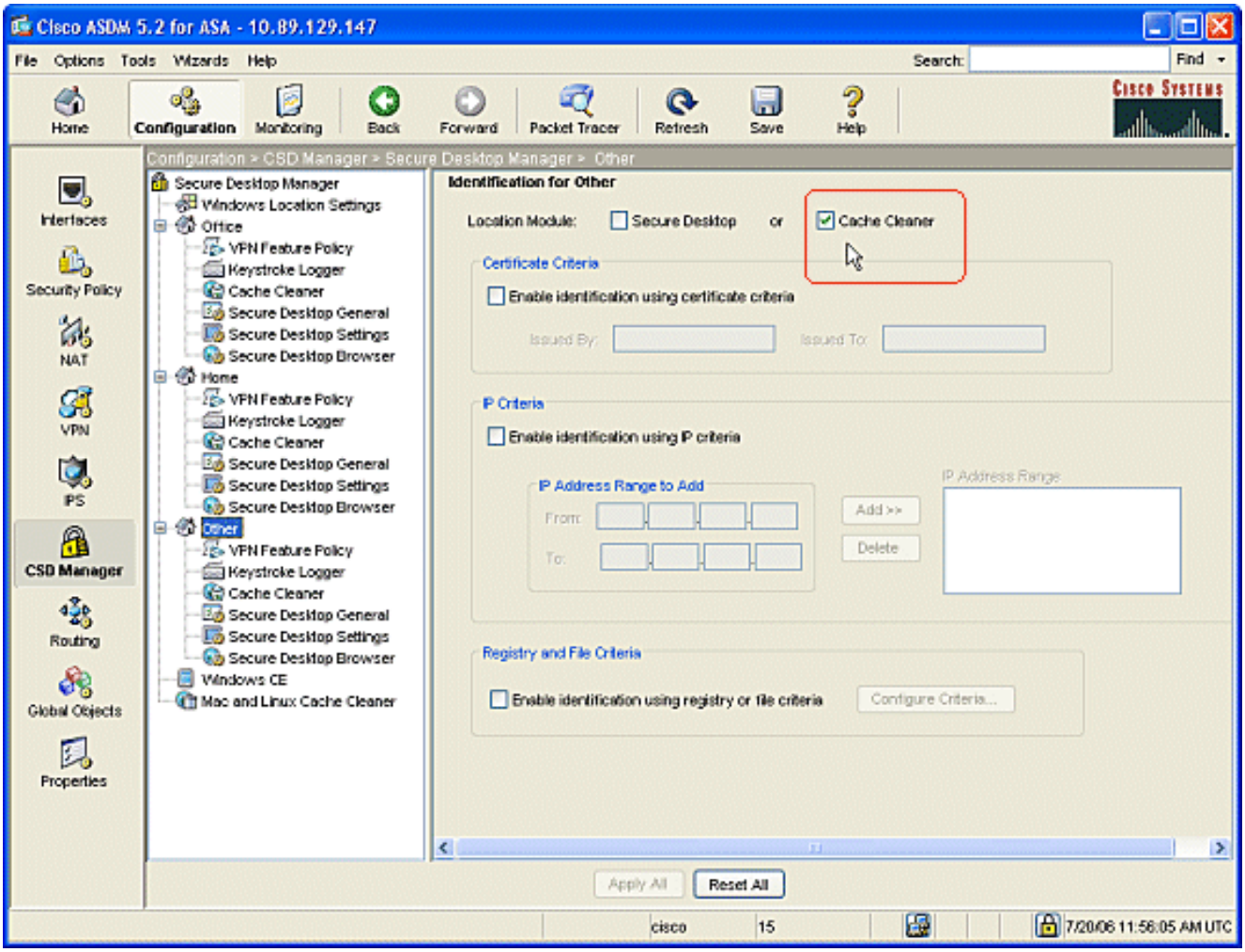
4. 在「Identification for Office（Office標識）」視窗中按一下**Apply All**。按一下**Save**，然後按一下**Yes**接受更改。
5. 要標識位置Home，請在導航窗格中按一下**Home**。選中**Enable identification using registry or file criteria**。按一下**Configure Criteria**。



6. 必須由管理員使用此登錄檔項配置家庭電腦客戶端。在「Add Registry Criterion」視窗中按一下**OK**。在「Registry and File Criteria（登錄檔和檔案標準）」視窗中按一下**OK**。



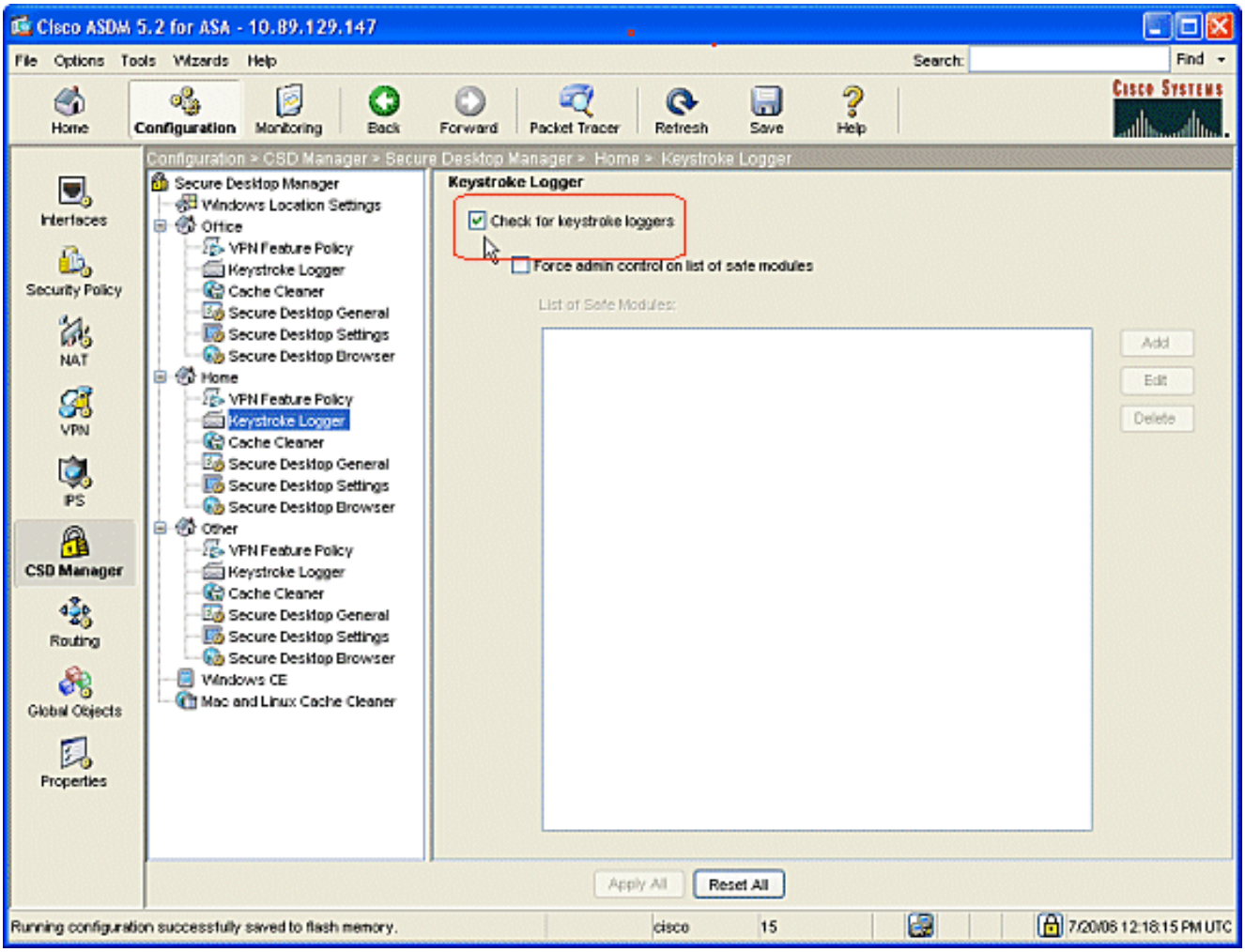
7. 在Location Module下，選中**Secure Desktop**。在「Identification for Home（主目錄標識）」視窗中按一下**Apply All**。按一下**Save**，然後按一下**Yes**接受更改。
8. 要標識位置**其他**，請在導航窗格中按一下**其他**。僅選中**Cache Cleaner**框並取消選中所有其他框。按一下「Identification for Other（其它標識）」視窗中的**Apply All**。按一下**Save**，然後按一下**Yes**接受更改。



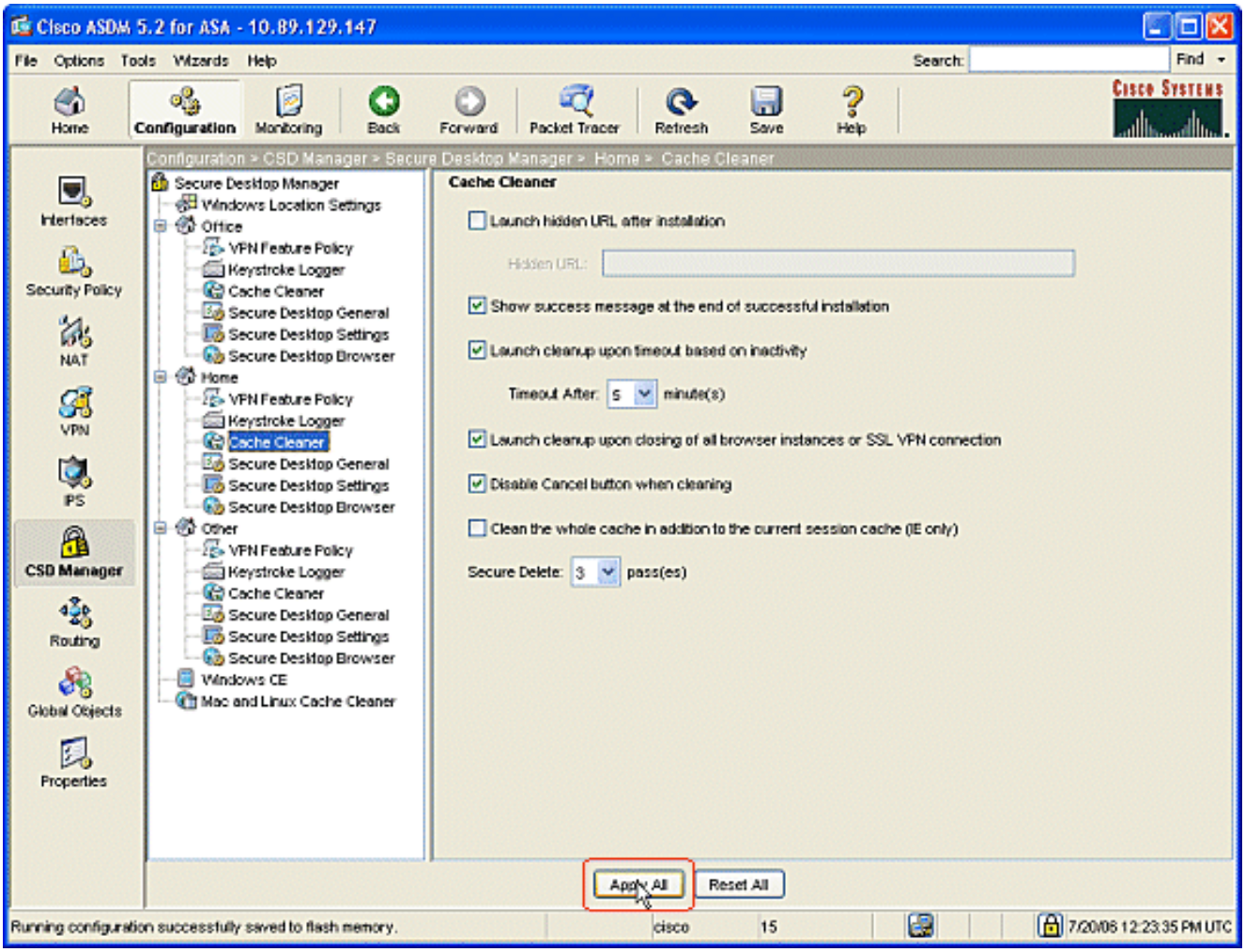
配置Windows位置模組

完成以下步驟，配置您建立的三個位置下方的模組。

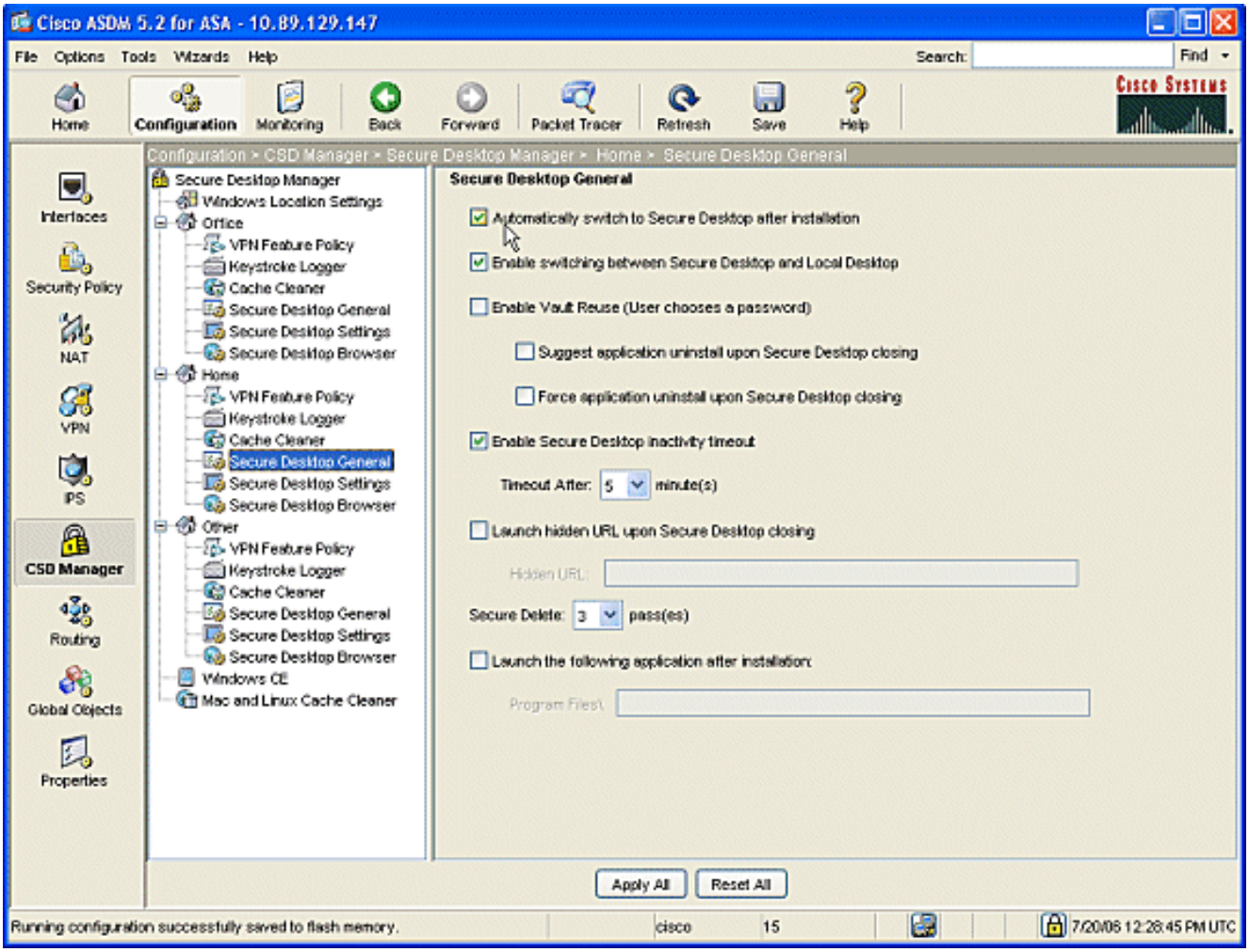
1. 對於Office客戶端，不要執行任何操作，因為在上面的步驟中未選擇Secure Desktop和Cache Cleaner。ASDM應用程式允許您配置快取清理程式，即使在上一步中未選擇它。保留Office位置的預設設定。**注意**：此步驟中未討論VPN功能策略，但將在後續步驟中對所有位置進行討論。
2. 對於Home客戶端，請在導航窗格中按一下**Home**和**Keystroke Logger**。在「按鍵記錄器」視窗中，選中**檢查按鍵記錄器**。在「按鍵記錄器」視窗中按一下**Apply All**。按一下**Save**，然後按一下**Yes**接受更改。



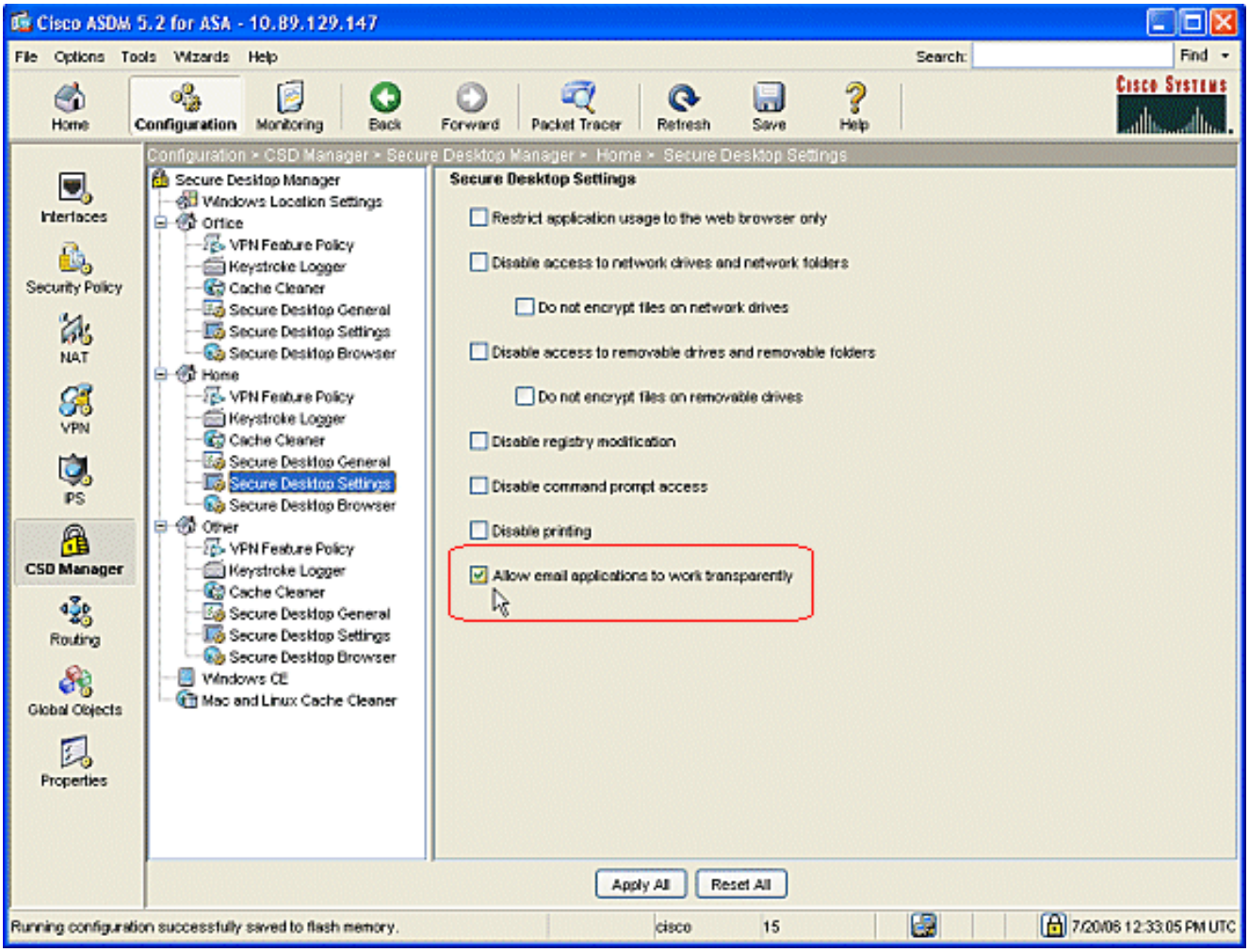
3. 在Home下，選擇**Cache Cleaner**並根據您的環境選擇引數。



4. 在「Home」下，選擇**Secure Desktop General**並根據您的環境選擇引數。



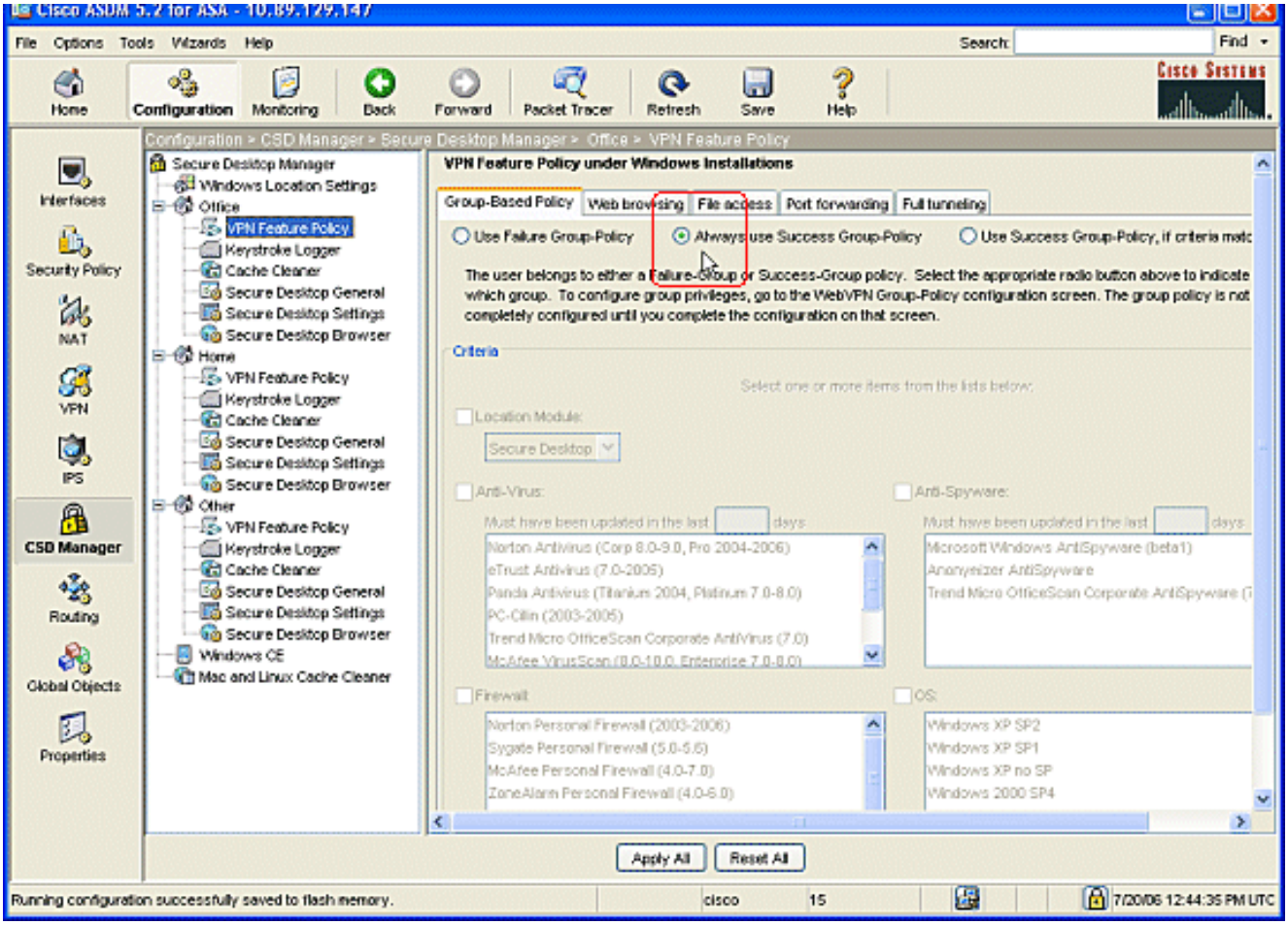
5. 在「首頁」下，選擇**「安全案頭設定」**。選中**Allow email applications to work transparent**，然後根據您的環境配置其他設定。按一下「**Apply All**」。按一下**Save**，然後按一下**Yes**接受更改。



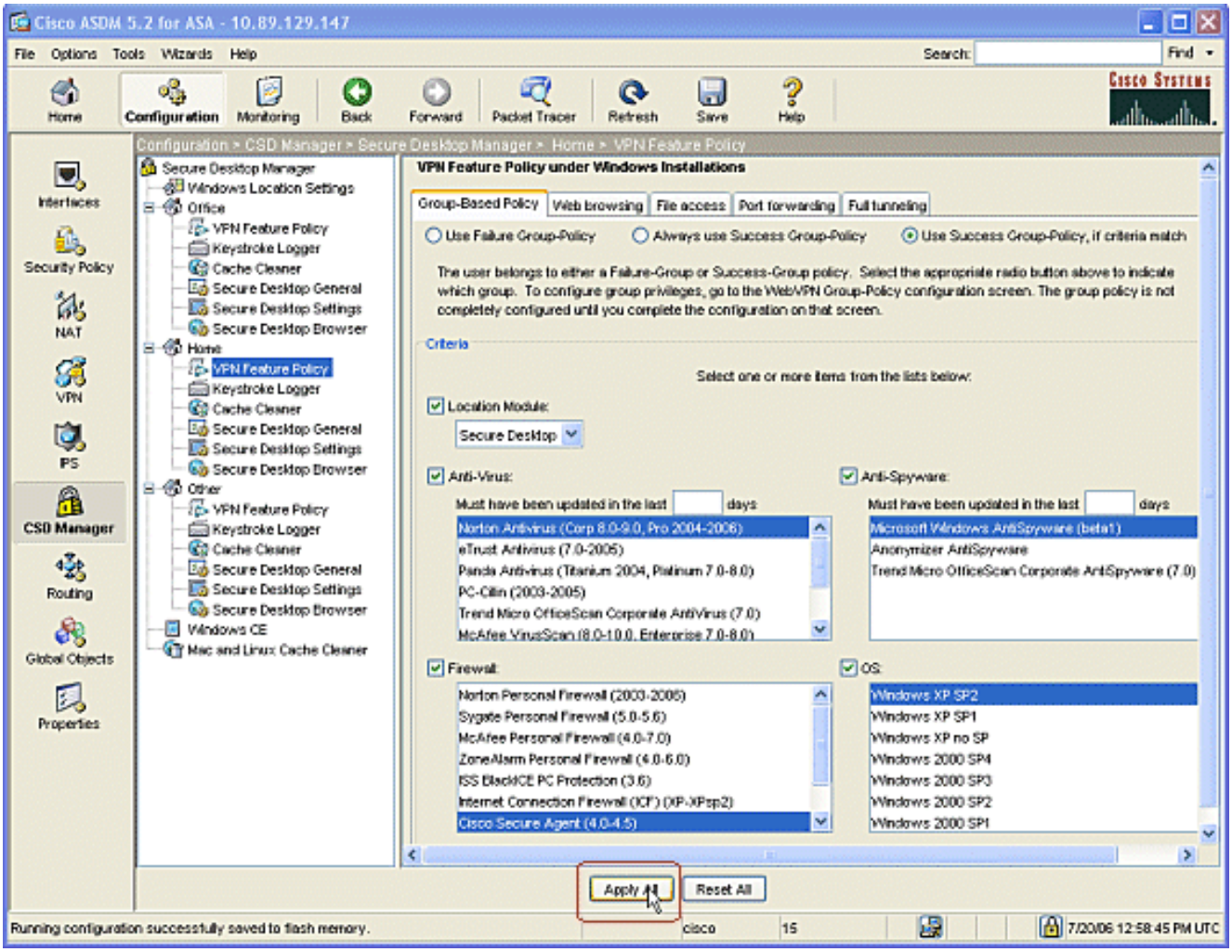
配置Windows位置功能

為建立的每個位置配置VPN功能策略。

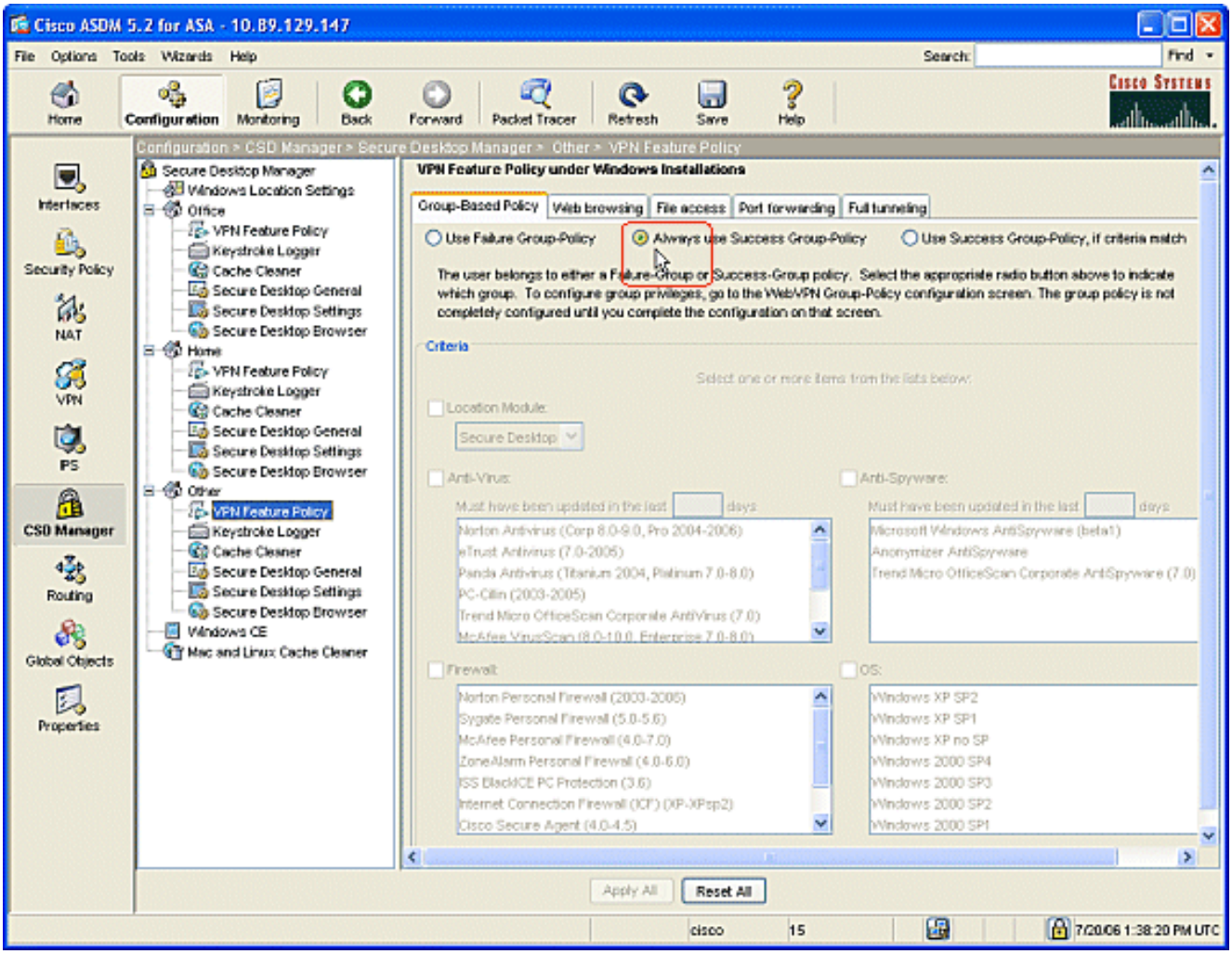
1. 在導航窗格中，單擊Office，然後按一下VPN Feature Policy。
2. 按一下Group-Based Policy選項卡。按一下Always use Success Group-Policy單選按鈕。按一下Web browsing頁籤，並選中Always Enabled單選按鈕。請按照File access、Port forwarding和Full tunneling索引標籤的相同程式操作。按一下「Apply All」。按一下Save，然後按一下Yes接受更改。



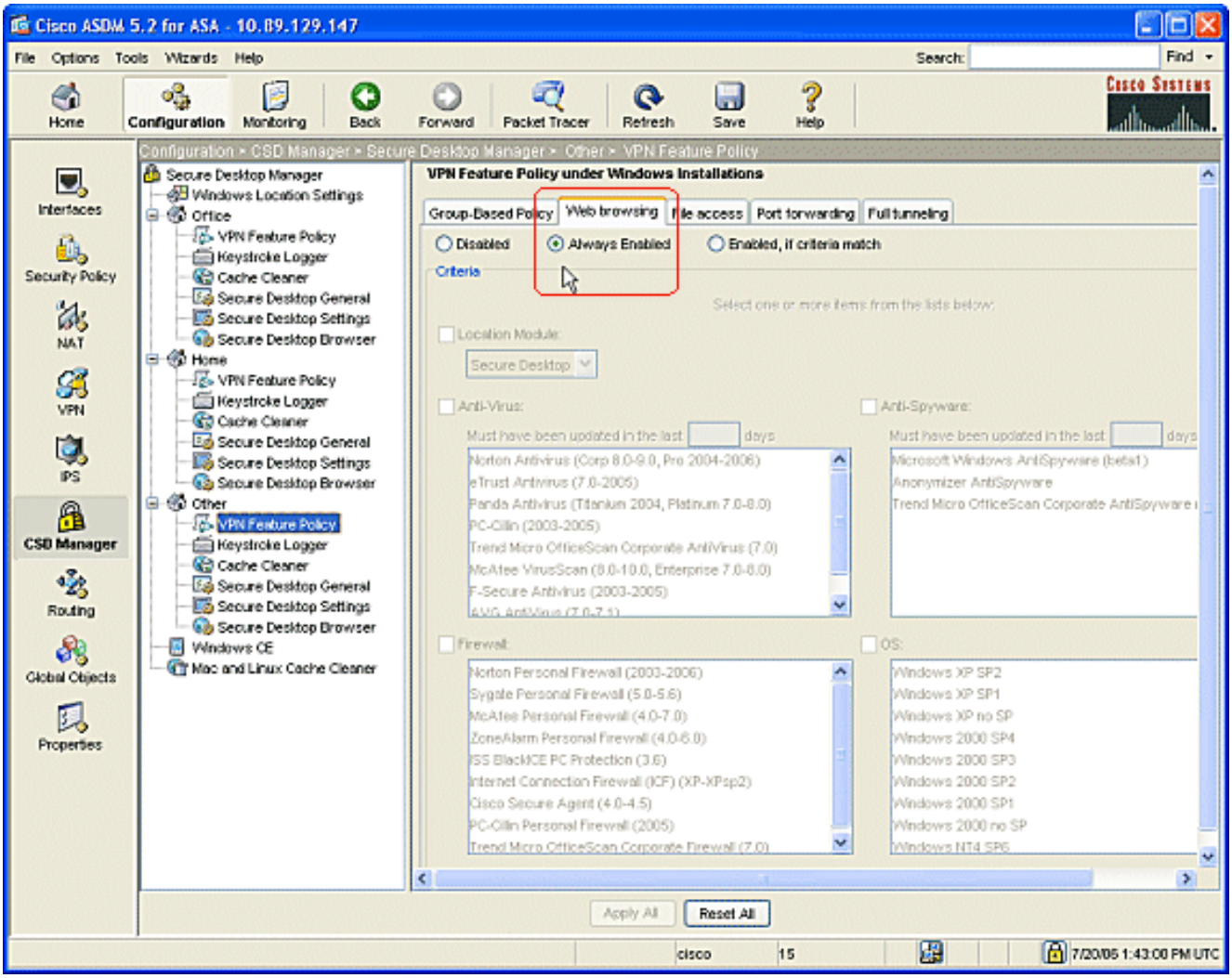
3. 對於家庭使用者，每個公司都可以在允許訪問之前要求特定的策略。在導航窗格中，按一下**Home**，然後按一下**VPN Feature Policy**。按一下**Group-Based Policy選項**卡。如果預配置的條件匹配（例如特定登錄檔項、已知檔名或數位證書），請按一下**Use Success Group-Policy**單選按鈕。選中**Location Module**覈取方塊並選擇**Secure Desktop**。根據您**公司的安全策略，選擇防病毒**、防間**諜**軟體、防火牆和作業系統區域。除非家庭使用者的電腦符合您配置的標準，否則不允許其訪問網路。



4. 在導航窗格中，按一下**Other**，然後按一下**VPN Feature Policy**。按一下**Group-Based Policy選項卡**。按一下**Always use Success Group-Policy**單選按鈕。



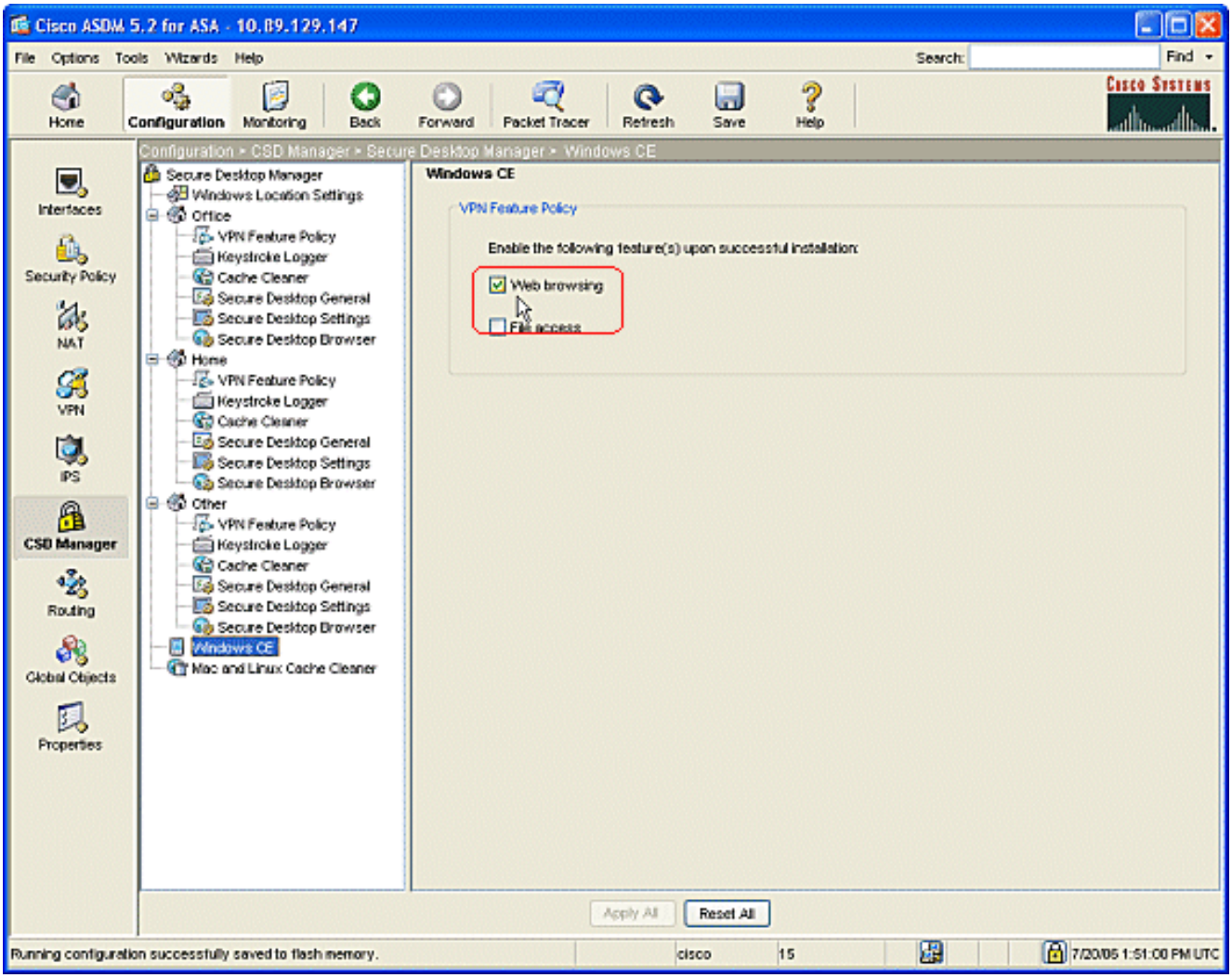
5. 對於此VPN Feature Policy位置的客戶端，按一下Web Browsing頁籤，然後按一下Always Enabled單選撥號。按一下File Access頁籤，然後按一下Disable單選按鈕。使用Port Forwarding和Full Tunneling索引標籤重複此步驟。按一下「Apply All」。按一下Save，然後按一下Yes接受更改。



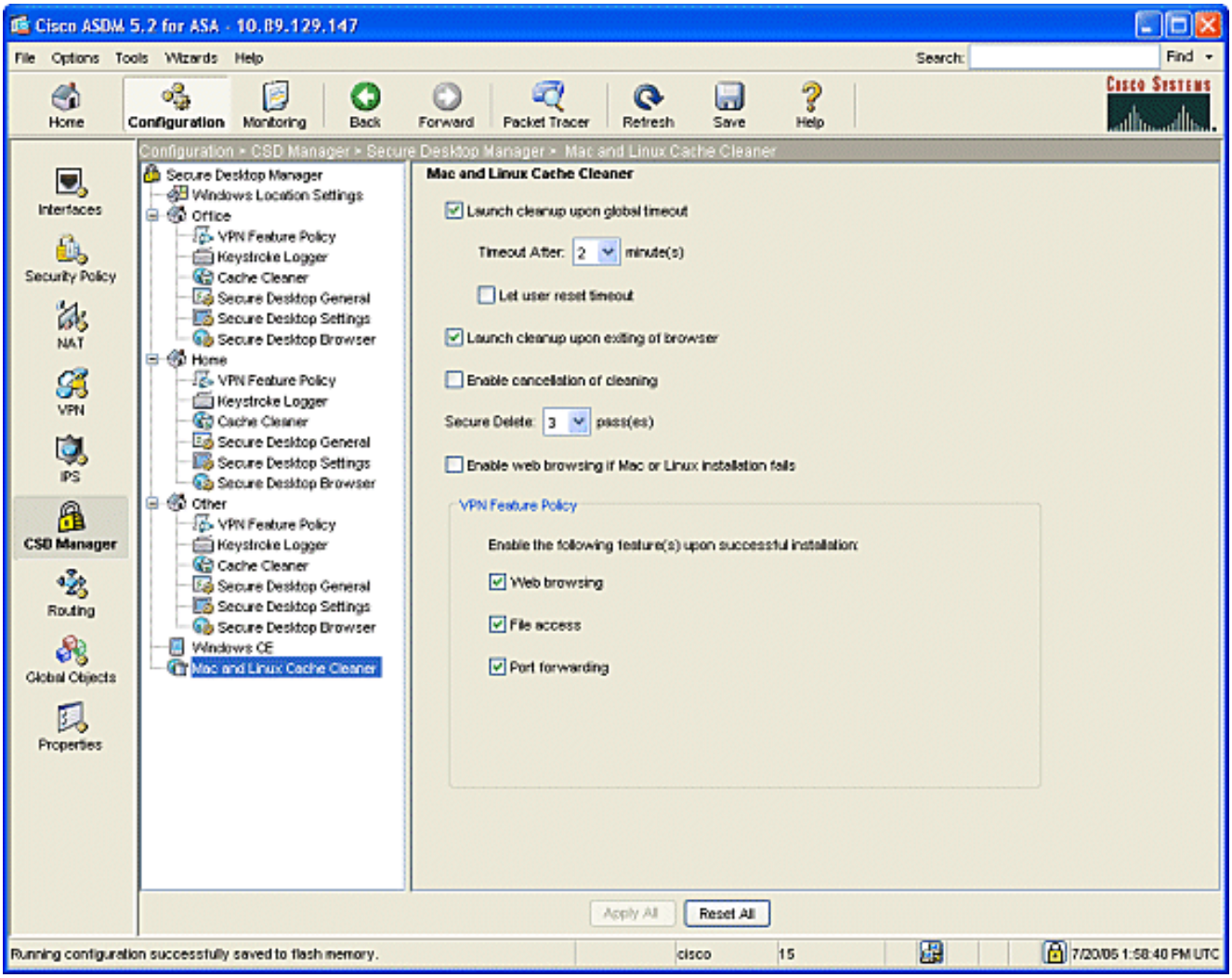
Windows CE、Macintosh和Linux客戶端的可選配置

這些配置是可選的。

1. 如果從導航窗格中選擇Windows CE，請選中Web browsing覈取方塊。



2. 如果從導航窗格中選擇Mac and Linux Cache Cleaner，請選中Launch cleanup upon global timeout單選撥號。根據您的規範更改超時。在VPN Feature Policy區域下，檢查這些客戶端的Web瀏覽、檔案訪問和埠轉發無線電撥號。



3. 無論您選擇Windows CE還是Mac and Linux Cache Cleaner，均可按一下**Apply All**。
4. 按一下**Save**，然後按一下**Yes**接受更改。

設定

組態

此配置反映了ASDM為啟用CSD所做的更改：大多數CSD配置儲存在快閃記憶體上的單獨檔案中。

Ciscoasa

```
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
```

驗證

使用本節內容，確認您的無客戶端SSL VPN、瘦客戶端SSL VPN或SSL VPN客戶端(SVC)配置是否正常運行。

使用配置有各種Windows位置的PC測試CSD。每個測試都應該根據您在上例中配置的策略提供不同的訪問許可權。

您可以更改Cisco ASA監聽WebVPN連線的埠號和介面。

- 預設埠為443。如果使用預設埠，則訪問地址為**https://ASA IP Address**。
- 使用不同的埠會更改對**https://ASA IP Address:newportnumber**的訪問。

指令

有幾個**show**命令與WebVPN關聯。您可以在命令列介面(CLI)上執行這些命令，以顯示統計資訊和其他資訊。要詳細瞭解**show**命令的用法，請參閱驗證WebVPN配置。

註：Output Interpreter Tool(僅限註冊客戶)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

如果遠端客戶端出現問題，請檢查以下項：

1. 是否在Web瀏覽器中啟用彈出視窗、Java和/或ActiveX?可能需要根據正在使用的SSL VPN連線型別啟用這些功能。
2. 客戶端必須接受會話開始時顯示的數位證書。

指令

有幾個**debug**命令與WebVPN關聯。有關這些命令的詳細資訊，請參閱使用WebVPN Debug命令。

注意：使用**debug**指令可能會對思科裝置造成負面影響。使用**debug**指令之前，請先參閱有關Debug指令的重要資訊。

相關資訊

- **Cisco ASA 5500系列調適型安全裝置**
- **使用ASDM和NTLMv1的WebVPN和單一登入的ASA配置示例**
- **技術支援與文件 - Cisco Systems**