Cisco Secure-desktop (CSD 3.1.x) op ASA 7.2.x voor Windows Configuration-voorbeeld met ASDM

Inhoud

Inleiding

Cisco Secure Desktop (CSD) breidt de beveiliging van SSL VPN-technologie uit. CSD biedt een afzonderlijke verdeling op het werkstation van een gebruiker voor sessieactiviteit. Dit volwassen gebied wordt versleuteld tijdens sessies en volledig verwijderd aan het einde van een SSL VPN-sessie. Windows kan worden ingesteld met de volledige veiligheidsvoordelen van CSD. Macintosh, Linux en Windows CE hebben alleen toegang tot de functies voor cache, webBrowsing en bestandstoegang. CSD kan op deze platforms worden ingesteld voor Windows-, Macintosh-, Windows CE- en Linux-apparaten:

- Cisco adaptieve security applicatie (ASA) 5500 Series switches
- Cisco-routers die Cisco IOS-softwarereleases 12.4(6)T en hoger uitvoeren
- Cisco VPN 3000 Series concentrators versie 4.7 en hoger

- Cisco Webex VPN-module op Catalyst 6500 en 7600 Series routers

Opmerking: u kunt nu Cisco Secure Desktop configureren om te draaien op externe computers waarop Microsoft Windows Vista-software is geïnstalleerd. Eerder, was Cisco Secure Desktop beperkt tot computers die Windows XP of 2000 hebben uitgevoerd. Raadpleeg het gedeelte Nieuwe functies - Secure-desktop met Vista van de release Notes voor Cisco Secure Desktop, release 3.3, voor meer informatie.

Dit voorbeeld heeft hoofdzakelijk betrekking op de installatie en configuratie van CSD's op de ASA 5500 Series voor Windows-cliënten. Optionele configuraties voor Windows CE, Mac en Linux-clients worden toegevoegd voor voltooiing.

CSD wordt gebruikt in combinatie met SSL VPN-technologie (Clientless SSL VPN, Thin-Client SSL VPN of SSL VPN-client (SVC). CSD voegt waarde toe aan de veilige sessies van SSL VPN-technologie.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

Eisen voor de ASA-apparatuur

- Cisco CSD release 3.1 of hoger
- Cisco ASA-softwareversie 7.1.1 of hoger
- Cisco Adaptieve Security Devices Manager (ASDM) release 5.1.1 of hoger**Opmerking:** CSD versie 3.2 ondersteunt alleen op ASA versie 8.x**Opmerking:** Raadpleeg HTTPS-toegang voor ASDM om de ASA te kunnen configureren door de ASDM.

Eisen voor clientcomputers

- Afstandsklanten dienen lokale administratieve rechten te hebben; het is niet nodig , maar het is zeer gesuggereerd .
- Afstandsklanten moeten beschikken over Java Runtime Environment (JRE) versie 1.4 of hoger.
- Afstandsbrowsers: Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 of Firefox 1.0
- Gebruikte koekjes en populaties toegestaan op externe klanten

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASDM versie 5.2(1)
- Cisco ASA versie 7.2(1)
- Cisco CSD, versie-veilig bureaublad-asa-3.1.1.32-k9.pkg

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden gebruikt, begonnen met een gewiste (standaard) configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen. De IP adressen die in deze configuratie worden gebruikt zijn RFC 1918 adressen. Deze IP-adressen zijn niet legaal op internet en moeten alleen in een testlabomgeving

worden gebruikt.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

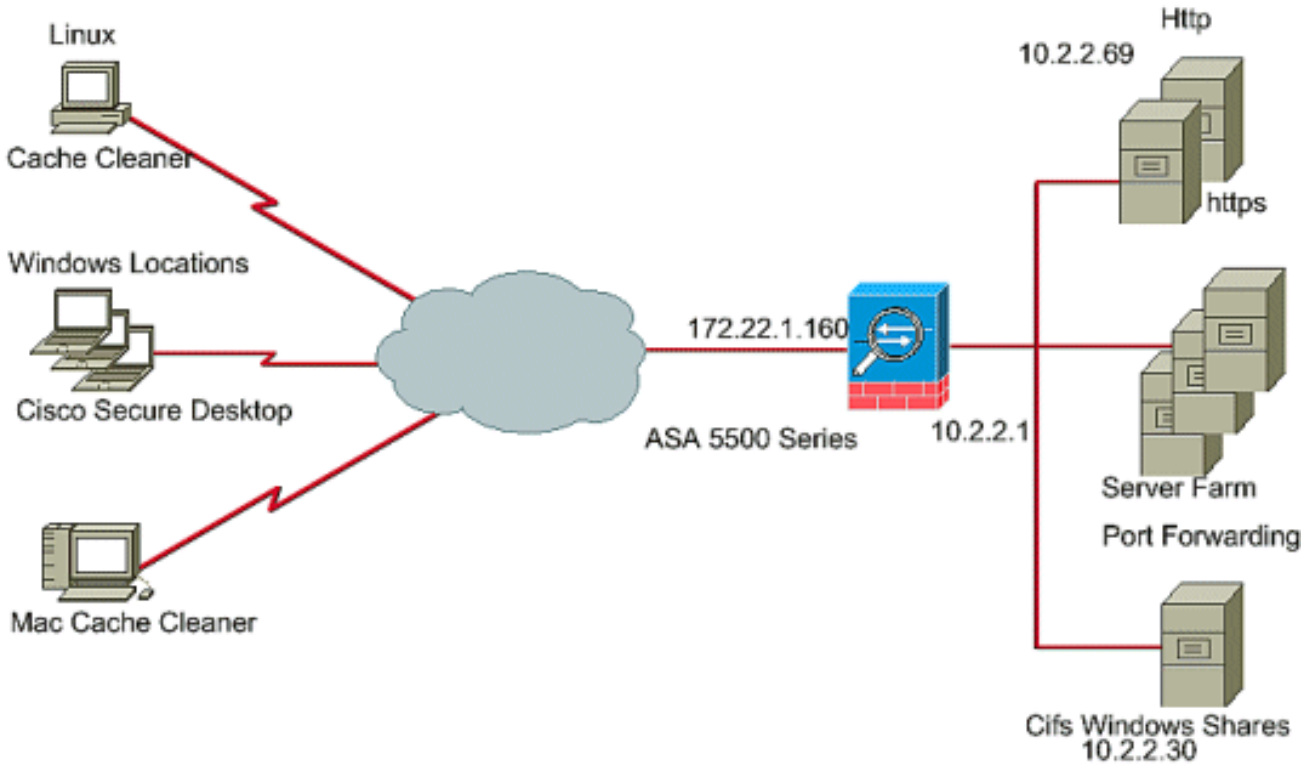
Achtergrondinformatie

CSD werkt met SSL VPN-technologie, zodat de Clientless, Thin-Client of SVC moeten worden geactiveerd voordat de CSD wordt ingesteld.

Netwerkdiagram

Verschillende Windows-locaties kunnen worden ingesteld met de volledige beveiligingsaspecten van CSD. Macintosh, Linux en Windows CE hebben alleen toegang tot de Cache Cleaner en/of web browsing en bestandstoegang.

Het netwerk in dit document is als volgt opgebouwd:



CSD op de ASA for Windows Clients configureren

CSD op de ASA for Windows Clients configureren met vijf belangrijke stappen:

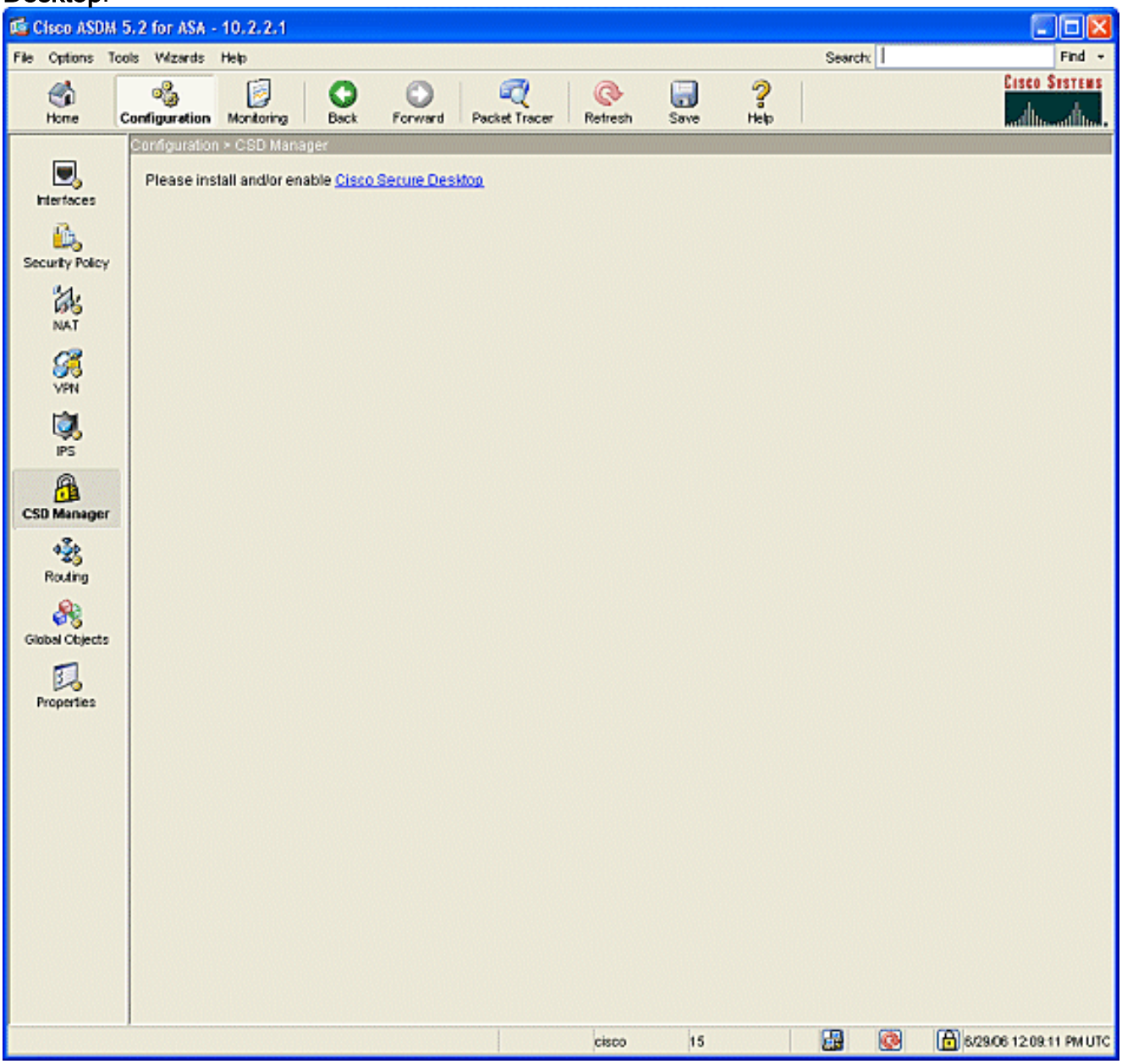
- Verkrijg, installeer en laat de CSD-software op Cisco ASA toe.
- Windows locaties definiëren
- Identificatie van Windows-locatie definiëren
- Configuratie van de Plaats van Windows modules.
- Functies voor Windows-locatie configureren

- Optionele configuratie voor Windows CE-, Macintosh- en Linux-clients.

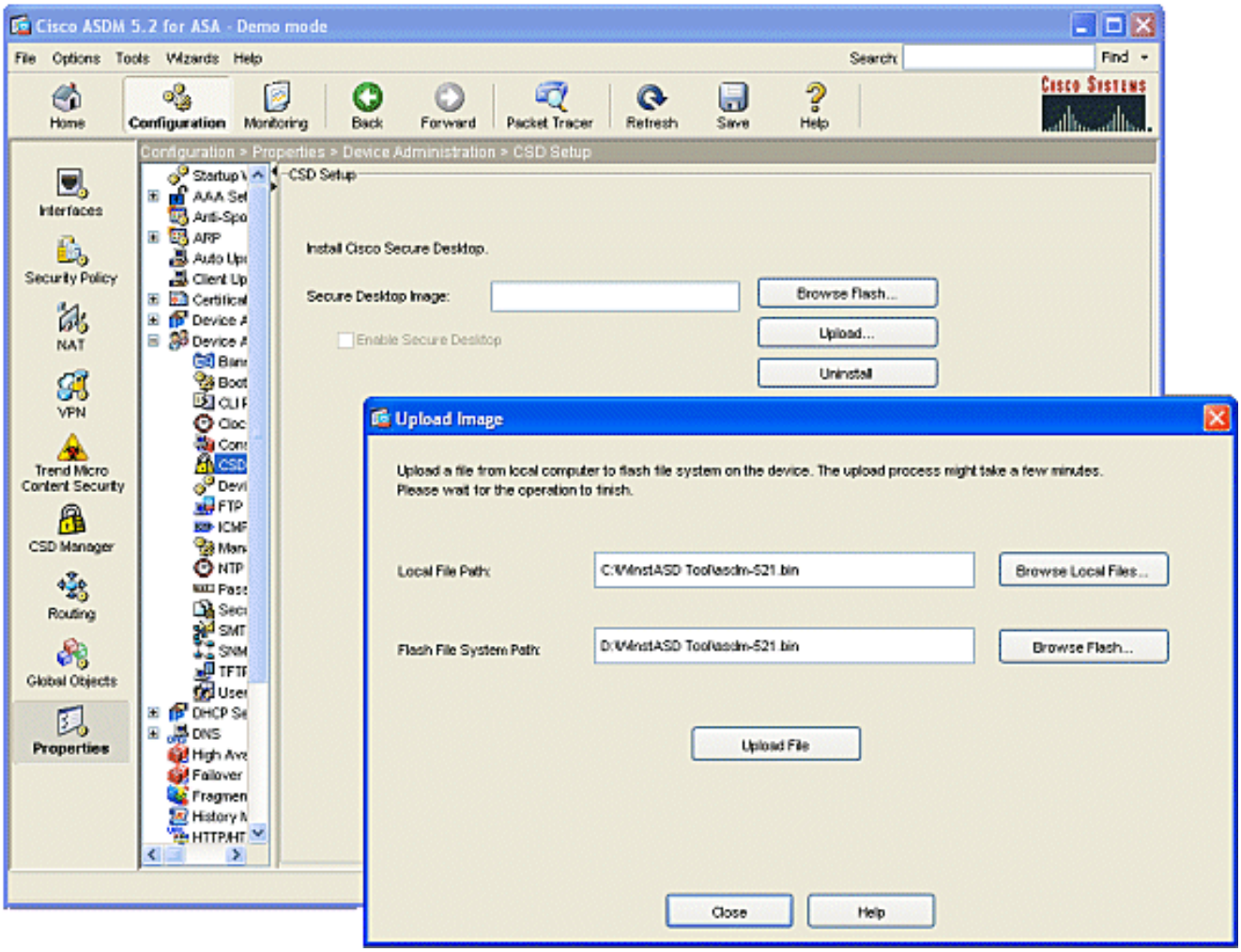
De CSD-software verkrijgen, installeren en inschakelen

Voltooi deze stappen om de CSD-software van Cisco ASA te verkrijgen, installeren en inschakelen.

1. Download de CSD-softwarebeveiliging bureaublad-asa*.pkg en leesmij bestanden op uw beheerstation van de Cisco Software Download website.
2. Meld u aan bij ASDM en klik op de knop **Configuration**. Klik in het linkermenu op de knop **CSD Manager** en klik op de link **Cisco Secure Desktop**.



3. Klik op **Upload** om het Afbeeldingsvenster uploaden.Voer het pad van het nieuwe .pkg-bestand in op het beheerstation of klik op **Bladeren** in **Local Files** om bestand te vinden.Voer de locatie op flitser in om het bestand te plaatsen of klik op **Bladeren**.Klik op **Upload File**.Klik na ontvangst op **OK > Sluiten > OK**.

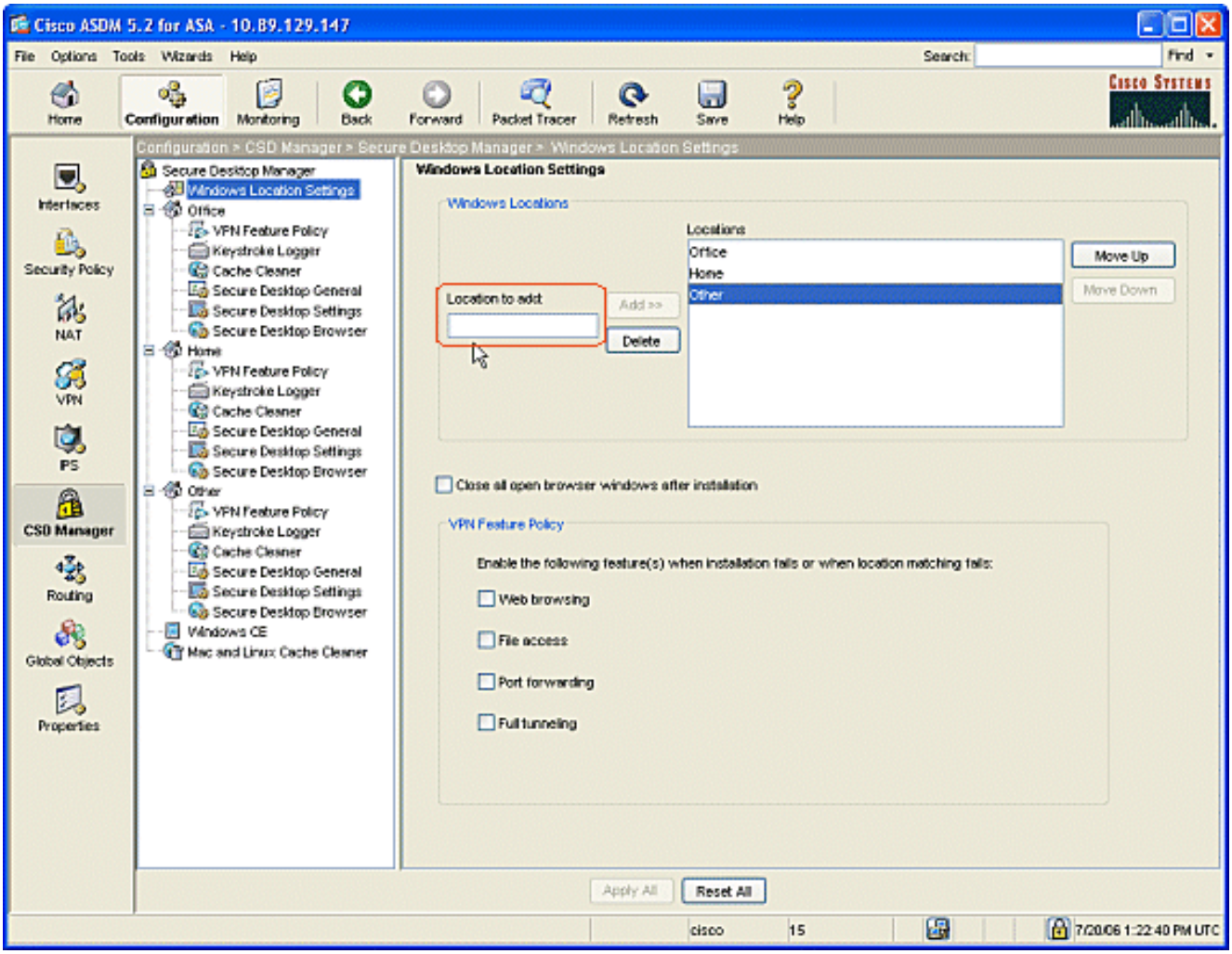


4. Nadat het clientbeeld naar flitser is geladen, controleert u het vakje **SSL VPN-client inschakelen** en vervolgens klikt u op **Toepassen**.
5. Klik op **Opslaan** en vervolgens op **Ja** om de wijzigingen te aanvaarden.

Windows-locaties definiëren

Voltooi deze stappen om Windows-locaties te definiëren.

1. Klik op de knop **Configuration**.
2. Klik in het linkermenu op de knop **CSD Manager** en klik op de link **Cisco Secure Desktop**.
3. Klik in het navigatiedeelvenster op **Windows-instellingen voor locatie**.
4. Typ een plaatsnaam in het veld Locatie om toe te voegen en klik op **Toevoegen**.Let op de drie locaties in dit voorbeeld: Office, Thuis en anderen.Office vertegenwoordigt werkstations die zich binnen de veiligheidsgrens van het bedrijf bevinden.Thuis staat voor gebruikers die thuis werken.Ander representeert elke andere locatie dan de twee vermelde locaties.

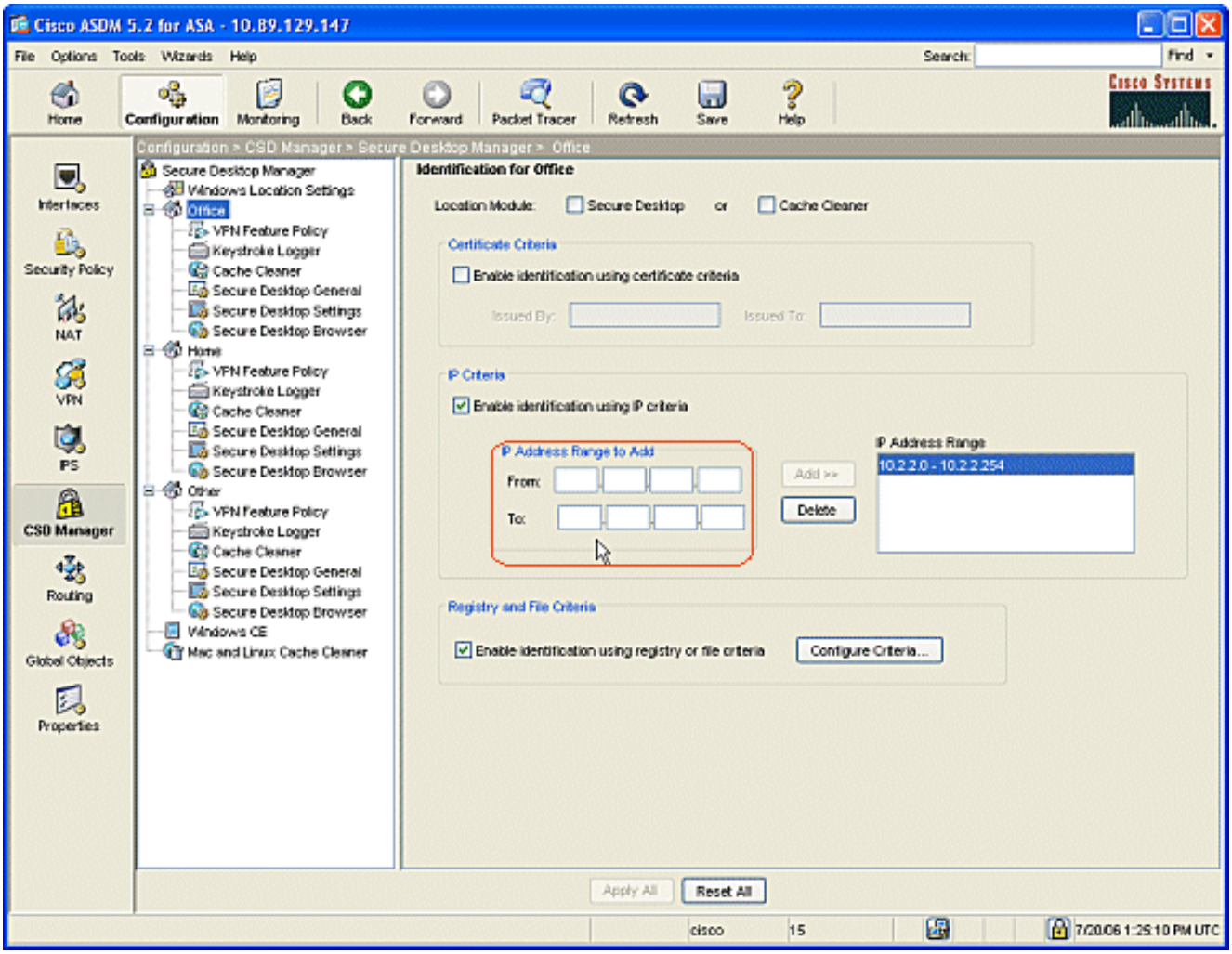


5. Maak uw eigen locaties afhankelijk van de lay-out van uw netwerkarchitectuur voor verkoop, gasten, partners en anderen.
6. Als u Windows-locaties maakt, wordt het navigatiedeelvenster met configureerbare modules voor elke nieuwe locatie uitgebreid. Klik op **Alles toepassen**.
7. Klik op **Opslaan** en vervolgens op **Ja** om de wijzigingen te aanvaarden.

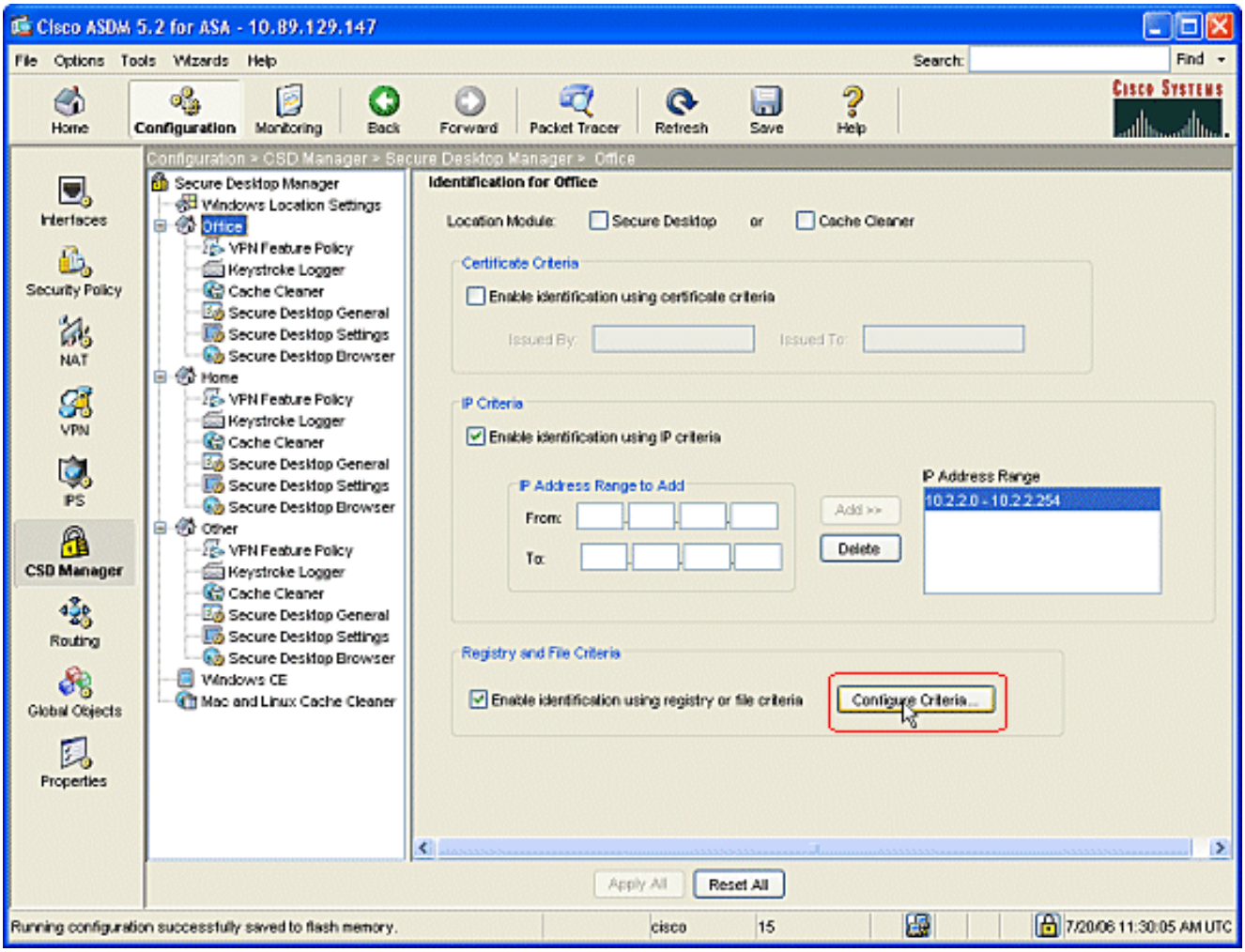
Identificatie van Windows-locatie

Voltooi deze stappen om de identificatie van Windows-locatie te definiëren.

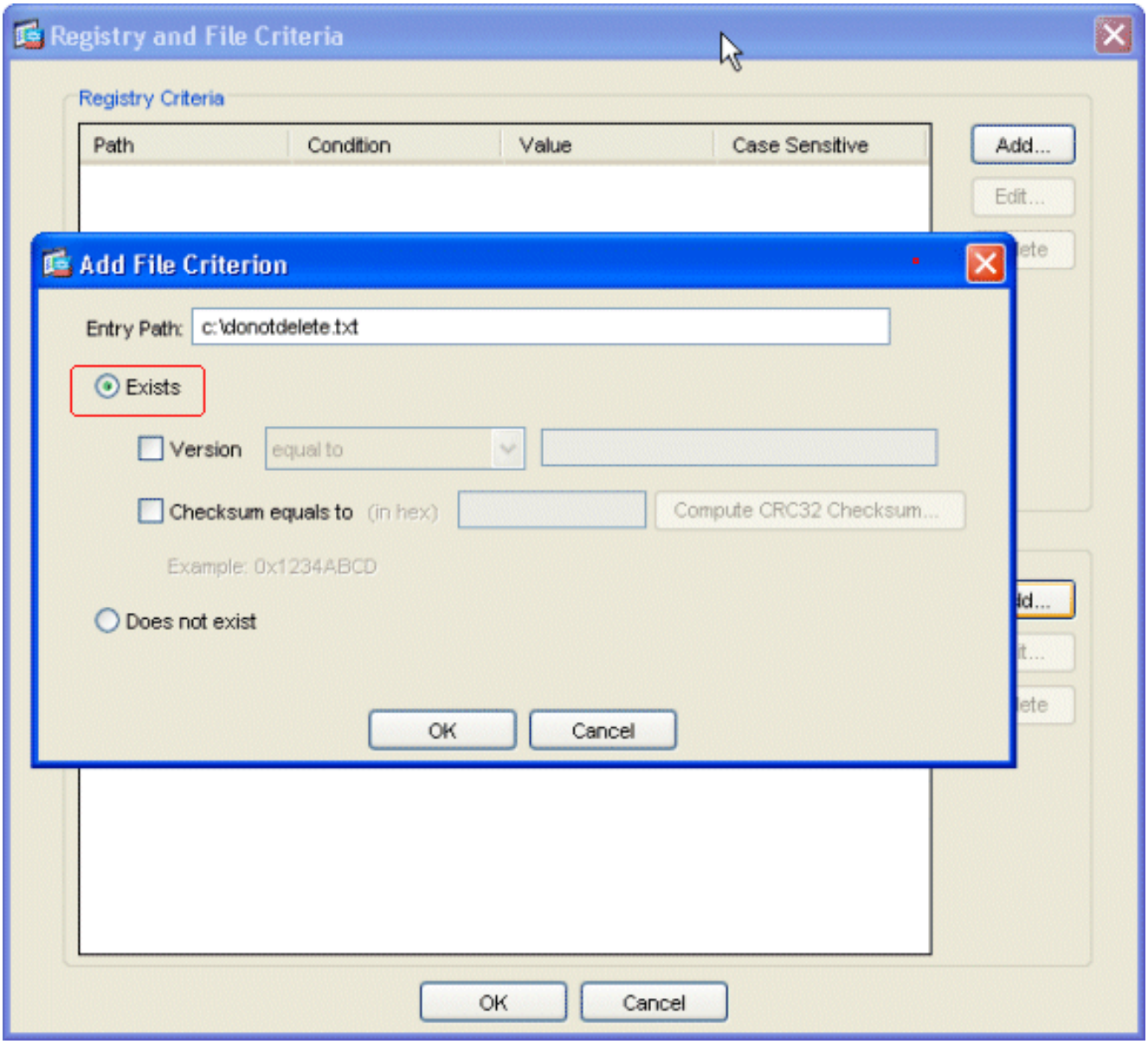
1. Identificeer de locaties die werden gecreëerd in Windows locaties definiëren.



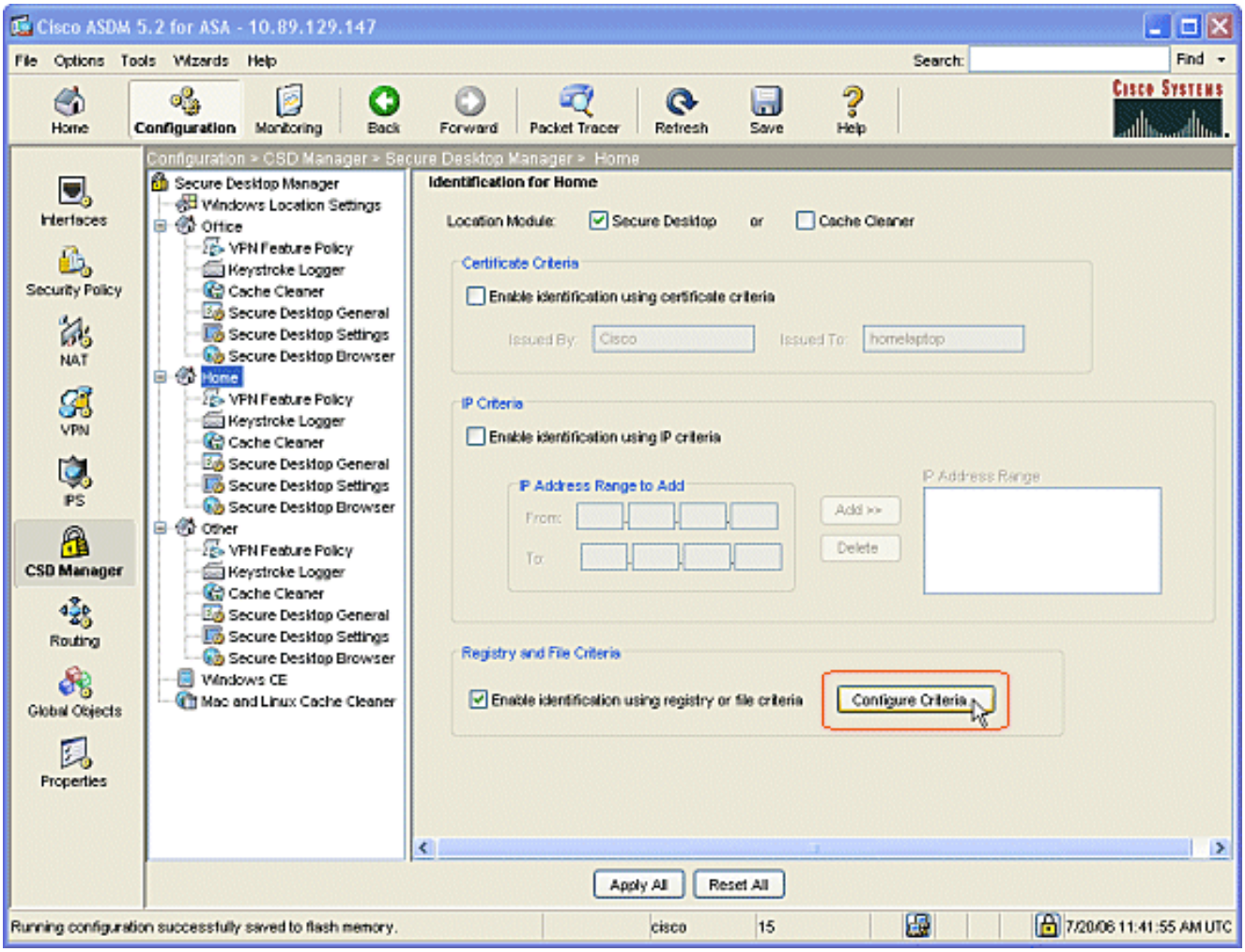
2. Wilt u het locatie-kantoor identificeren, dan klikt u op **Office** in het navigatiedeelvenster.**Secure Desktop** en **Cache Cleaner** uit te schakelen omdat dit interne computers zijn.Controleer **identificatie met behulp van IP-criteria inschakelen**.Voer de IP-adresbereik van uw interne computers in.Controleer **Identificatie inschakelen met behulp van registratie- of bestandscriteria**. Dit maakt onderscheid tussen interne kantoormedewerkers en de incidentele gasten op het
netwerk.



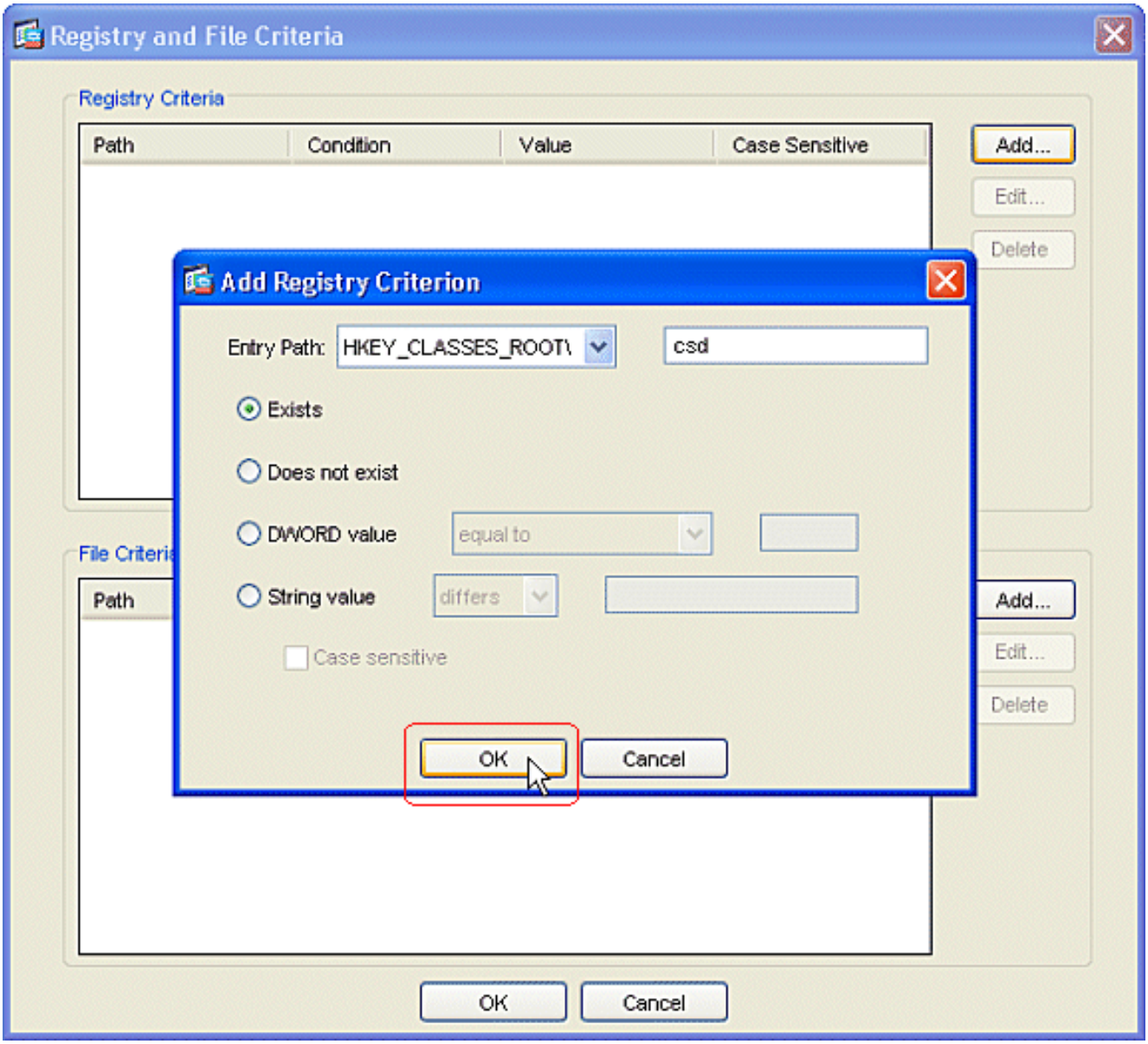
3. Klik op **Criteria configureren**. Een eenvoudig voorbeeld van een bestand "DoNotDelete.txt" wordt ingesteld. Dit bestand moet op uw interne Windows-computers bestaan en is alleen een plaatsaanduiding. U kunt ook een Windows-registratiesleutel configureren om interne kantoorcomputers te identificeren. Klik op **OK** in het venster Bestand toevoegen met criterium. Klik op **OK** in het venster Registratie- en bestandscriteria.



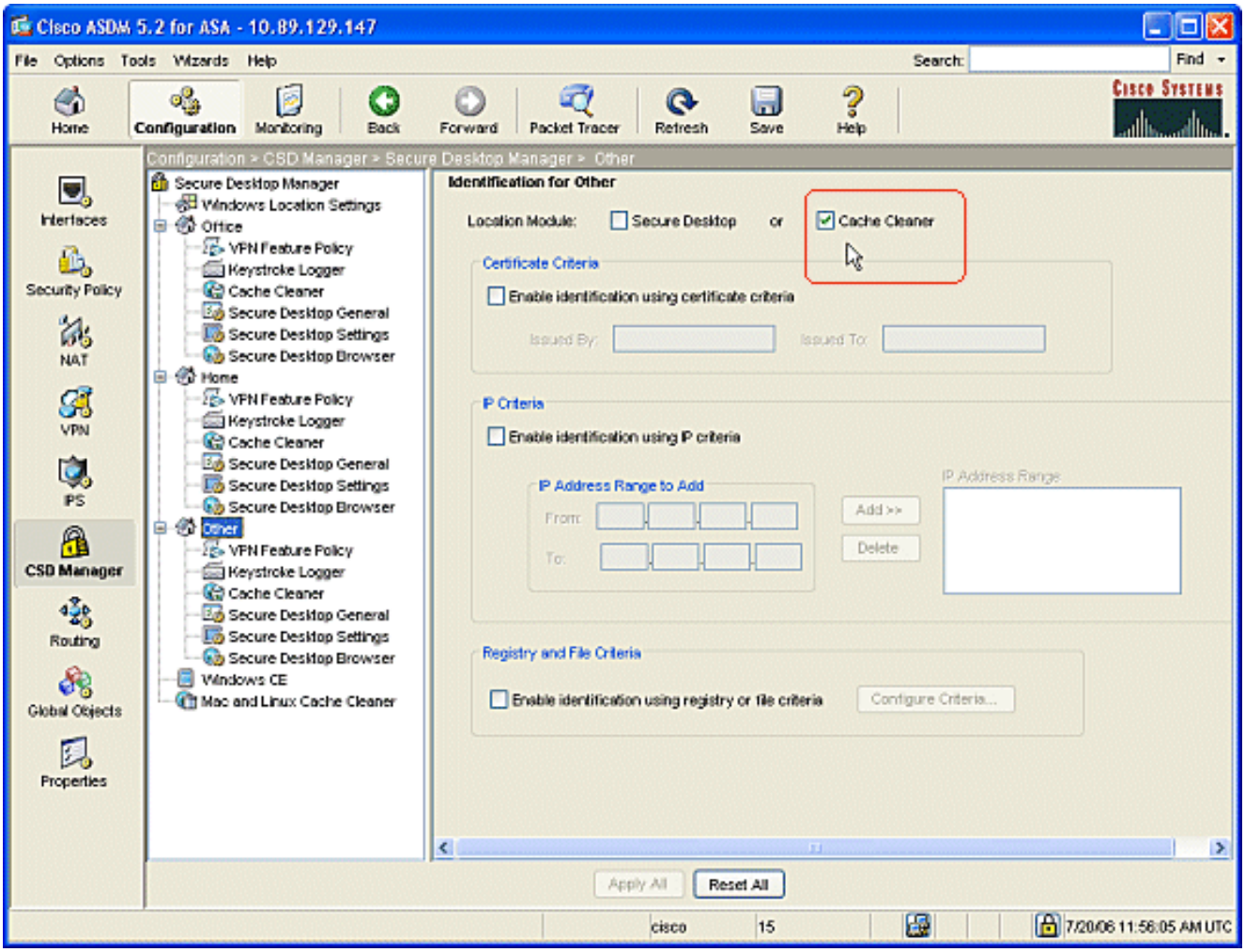
4. Klik op **Alles toepassen** in het venster Identificatie voor Office. Klik op **Opslaan** en vervolgens op **Ja** om de wijzigingen te aanvaarden.
5. Wilt u de locatie-startpunt identificeren, dan klikt u op **startpunt** in het navigatiedeelvenster.Controleer **Identificatie inschakelen met behulp van registratie- of bestandscriteria**.Klik op **Criteria configureren**.



6. Clients voor de thuiscomputer moeten door een beheerder met deze registersleutel zijn geconfigureerd. Klik op **OK** in het venster Registratiecriterium toevoegen. Klik op **OK** in het venster Registratie- en bestandscriteria.



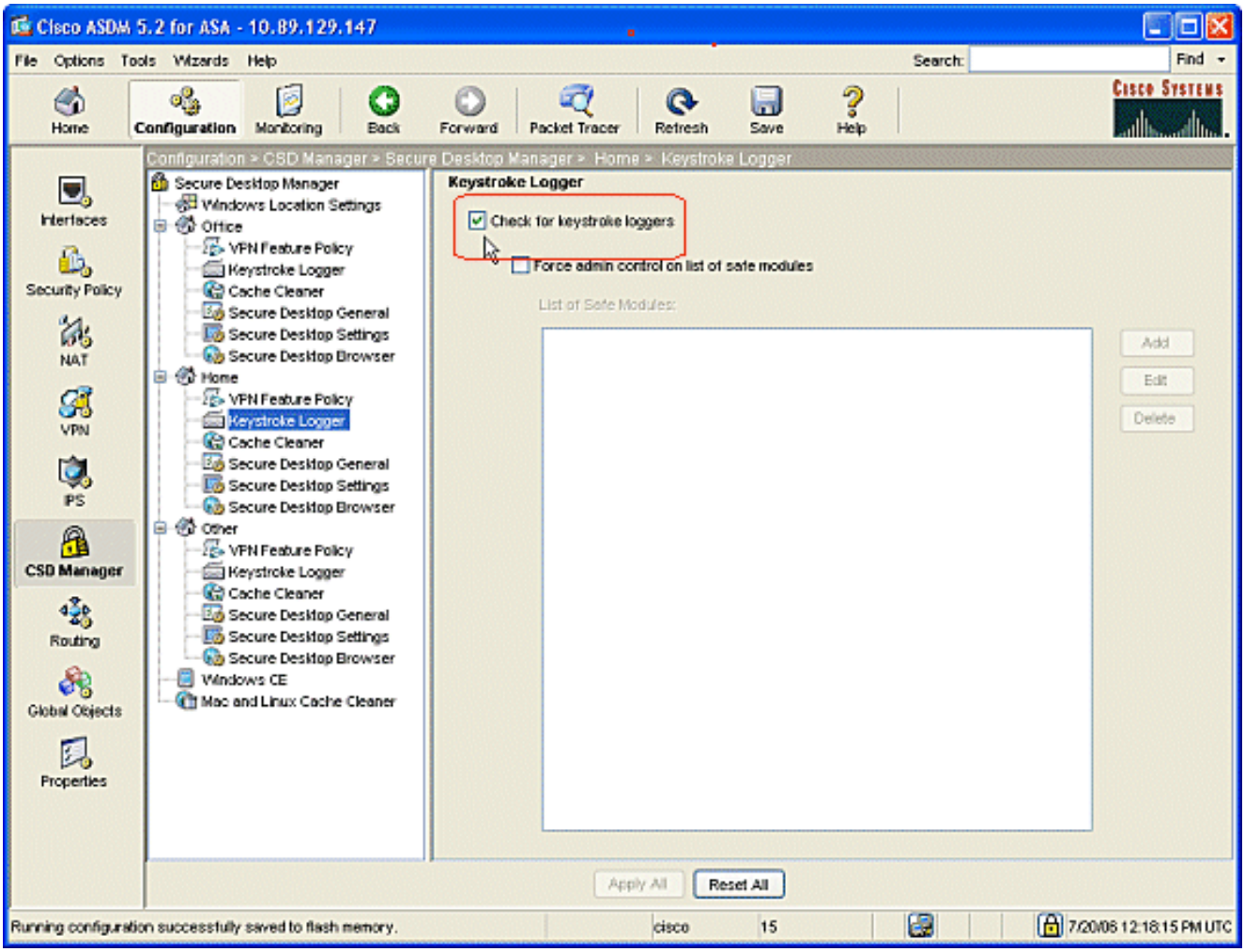
7. Controleer onder Locatiemodule **het beveiligde bureaublad**. Klik op **Alles toepassen** in het venster Identificatie voor startpunt. Klik op **Opslaan** en vervolgens op **Ja** om de wijzigingen te aanvaarden.
8. Als u de locatie **anders** wilt identificeren, klikt u op **Ander** in het navigatiedeelvenster.Controleer alleen het vakje **Cache Cleaner** en koppel alle andere vakjes los.Klik op **Alles toepassen** in het venster Identificatie voor Ander venster.Klik op **Opslaan** en vervolgens op **Ja** om de wijzigingen te aanvaarden.



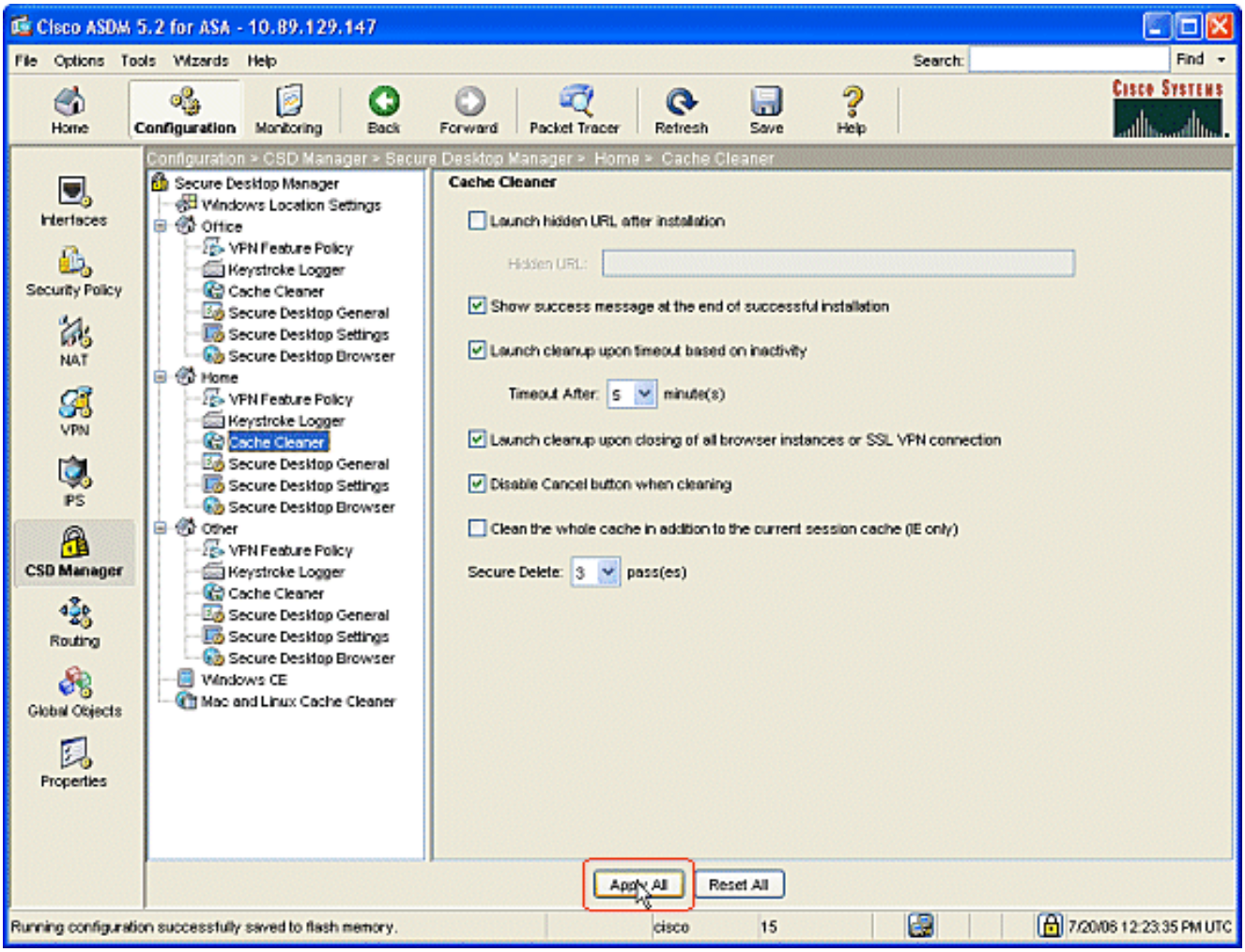
Windows-locatiemodule configureren

Voltooi deze stappen om de modules onder elk van de drie plaatsen te configureren die u hebt gemaakt.

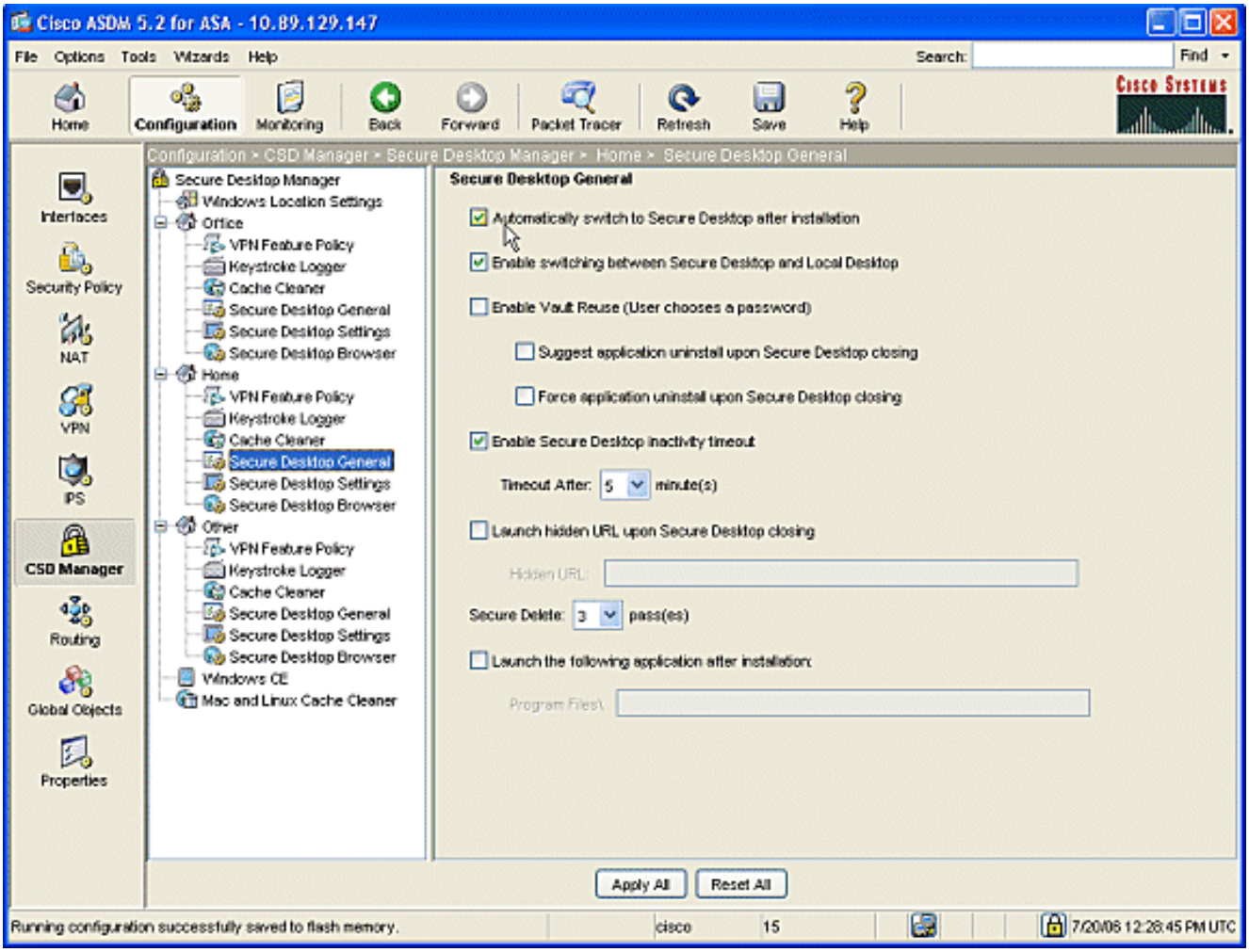
1. Voor Office-klanten doet u niets omdat in de vorige stappen geen Secure Desktop en Cache Cleaner is geselecteerd. Met de ASDM-toepassing kunt u de Cache Cleaner configureren, zelfs als dit niet in een vorige stap is geselecteerd. Bewaar de standaardinstellingen voor de kantoorlocaties.**Opmerking:** Het VPN-functiebeleid wordt in deze stap niet besproken, maar het wordt in een volgende stap voor alle locaties besproken.
2. Klik voor thuisclients op **Start** en **Trefberoerte** in het navigatiedeelvenster.Controleer in het venster Trefslag Logger op **vinkloggers**.Klik op **Alles toepassen** in het venster Trefberoerte logger.Klik op **Opslaan** en vervolgens op **Ja** om de wijzigingen te aanvaarden.



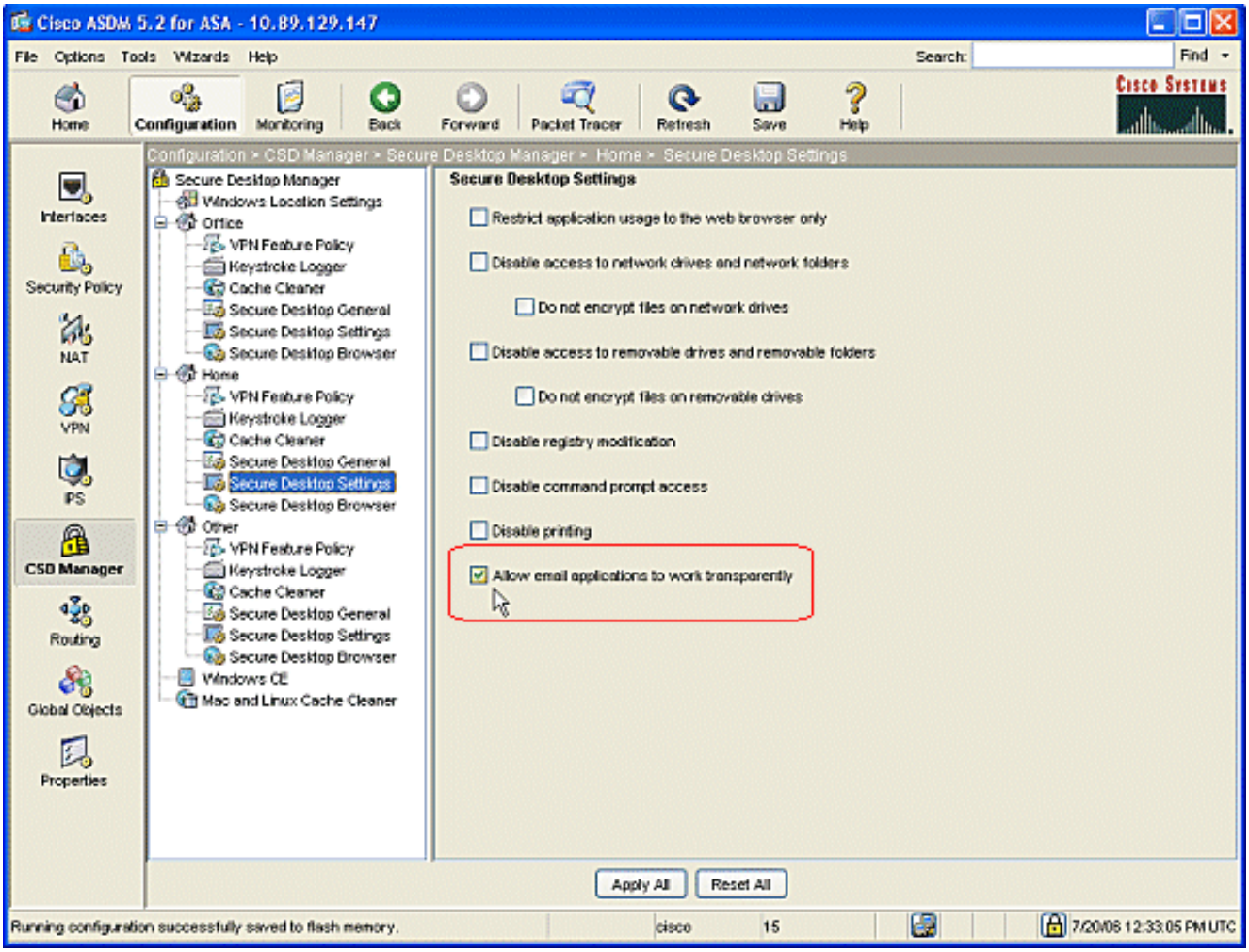
3. Selecteer onder Home **Cache Cleaner** en de parameters die bij uw omgeving passen.



4. Selecteer onder Home de optie **Secure Desktop General** en de parameters die bij uw omgeving
passen.



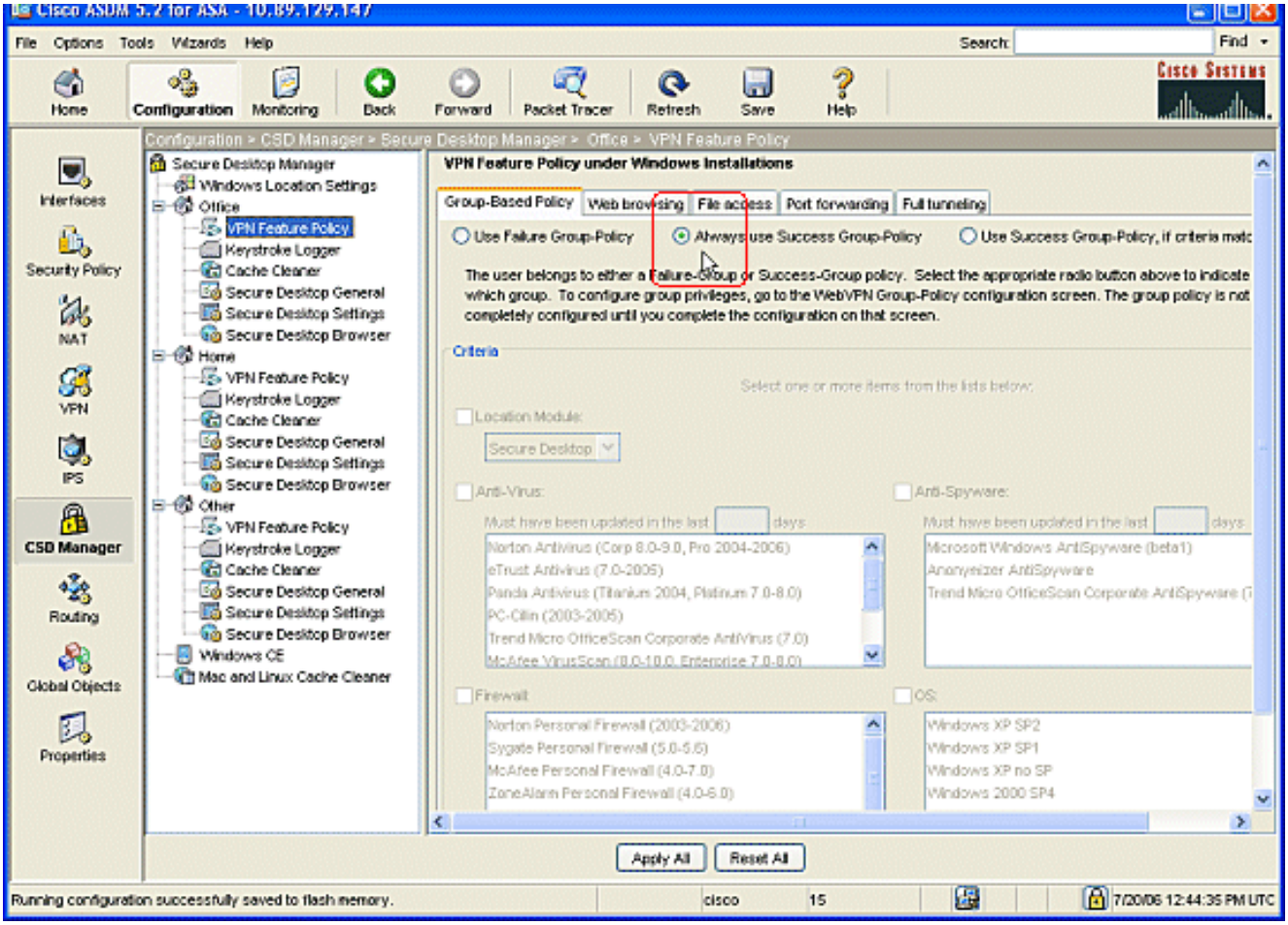
5. Kies onder Start **Beveiligde desktopinstellingen**.Controleer **E-mailtoepassingen op transparante wijze laten werken** en stel de andere instellingen in die passen bij uw omgeving.Klik op **Alles toepassen**.Klik op **Opslaan** en vervolgens op **Ja** om de wijzigingen te aanvaarden.



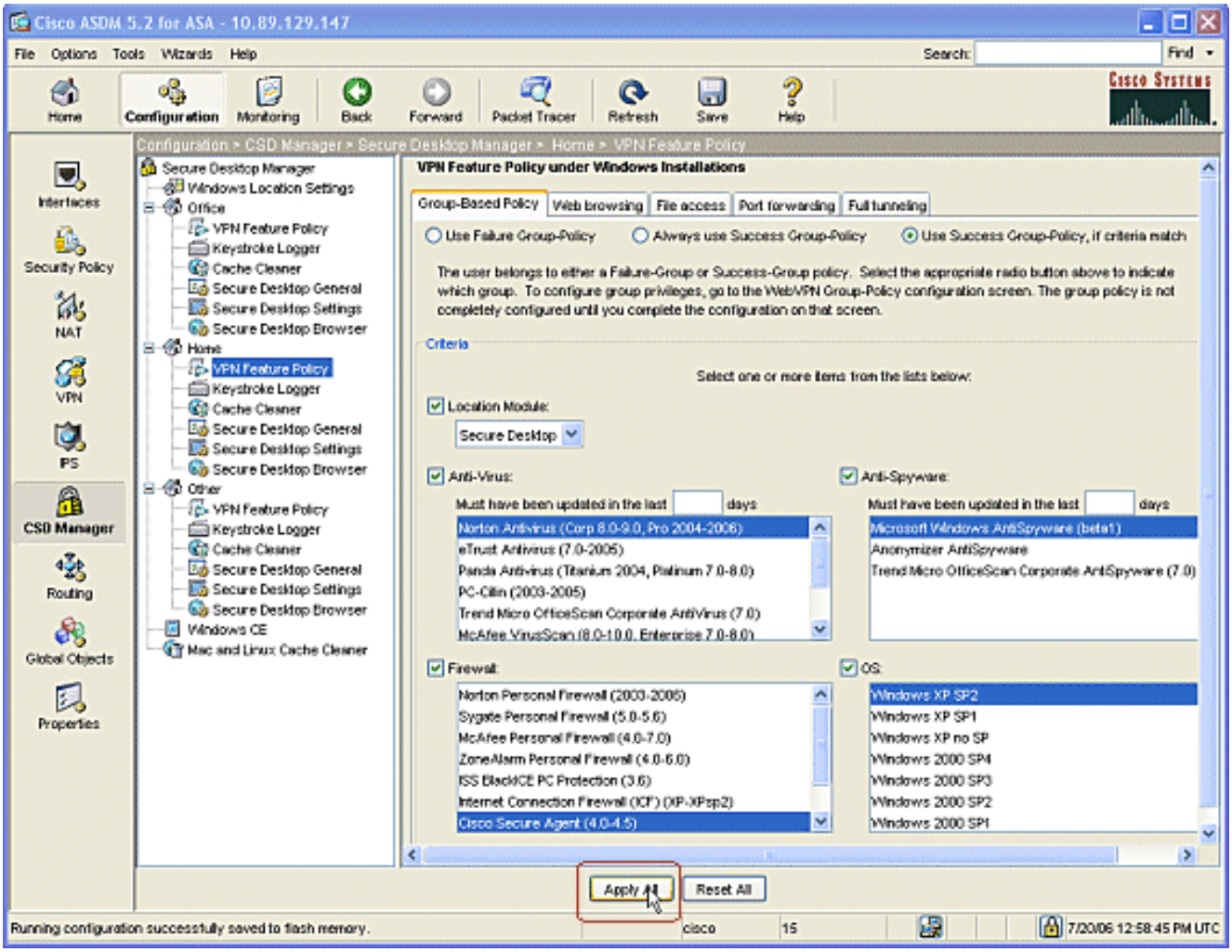
Functies voor Windows-locatie configureren

Configureer het beleid van de VPN-functie voor elk van de locaties die u hebt gemaakt.

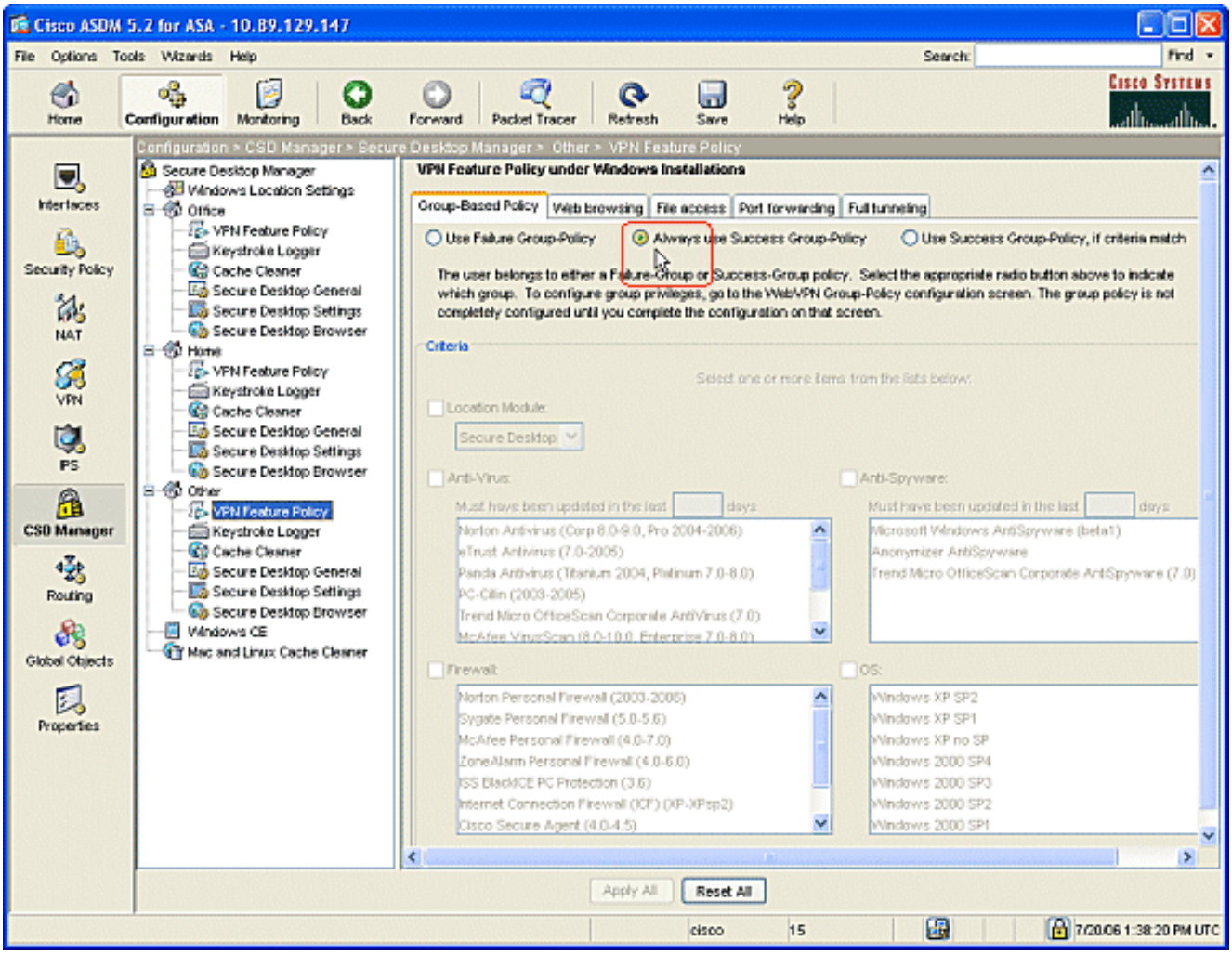
1. Klik in het navigatiedeelvenster **op Office** en vervolgens op **VPN-functiebeleid**.
2. Klik op het tabblad **Groepsgebaseerd beleid**.Klik op de radioknop **Altijd Success Group-Policy gebruiken**.Klik op het tabblad **Web browsen** en controleer de radioknop **Altijd ingeschakeld**.Volg dezelfde procedure voor de tabbladen **Bestandstoegang, Poortverzending** en **Volledig tunnelen**.Klik op **Alles toepassen**.Klik op **Opslaan** en vervolgens op **Ja** om de wijzigingen te
aanvaarden.



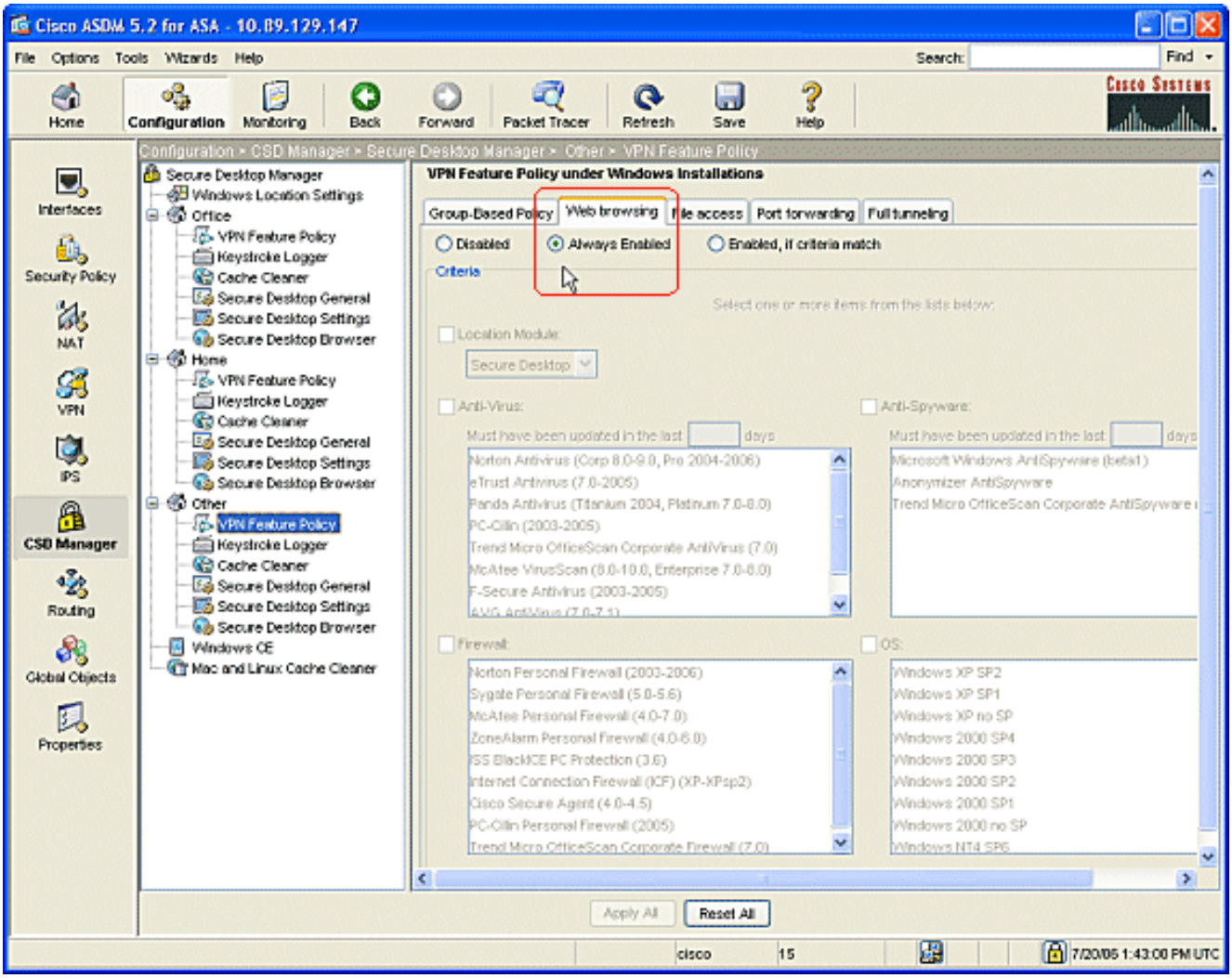
3. Voor thuisgebruikers kan elk bedrijf een specifiek beleid vereisen voordat toegang wordt toegestaan. Klik in het navigatiedeelvenster op **Start** en klik op **VPN-functiebeleid**.Klik op het tabblad **Groepsgebaseerd beleid**.Klik op de radioknop **Use Success Group-Policy** als vooraf ingestelde criteria overeenkomen, zoals een specifieke registratiesleutel, een bekende bestandsnaam of een digitaal certificaat.Controleer **het** selectieknop **Locatiemodule** en kies **Secure Desktop**.Kies de gebieden **tegen virussen, anti-spyware, firewall** en **OS** in overeenstemming met uw bedrijfsbeveiligingsbeleid. Thuisgebruikers mogen alleen op het netwerk aanwezig zijn als hun computers aan de criteria voldoen.



4. Klik in het navigatiedeelvenster op **Ander** en klik op **VPN-functiebeleid**.Klik op het tabblad **Groepsgebaseerd beleid**.Klik op de radioknop **Altijd Success Group-Policy gebruiken**.



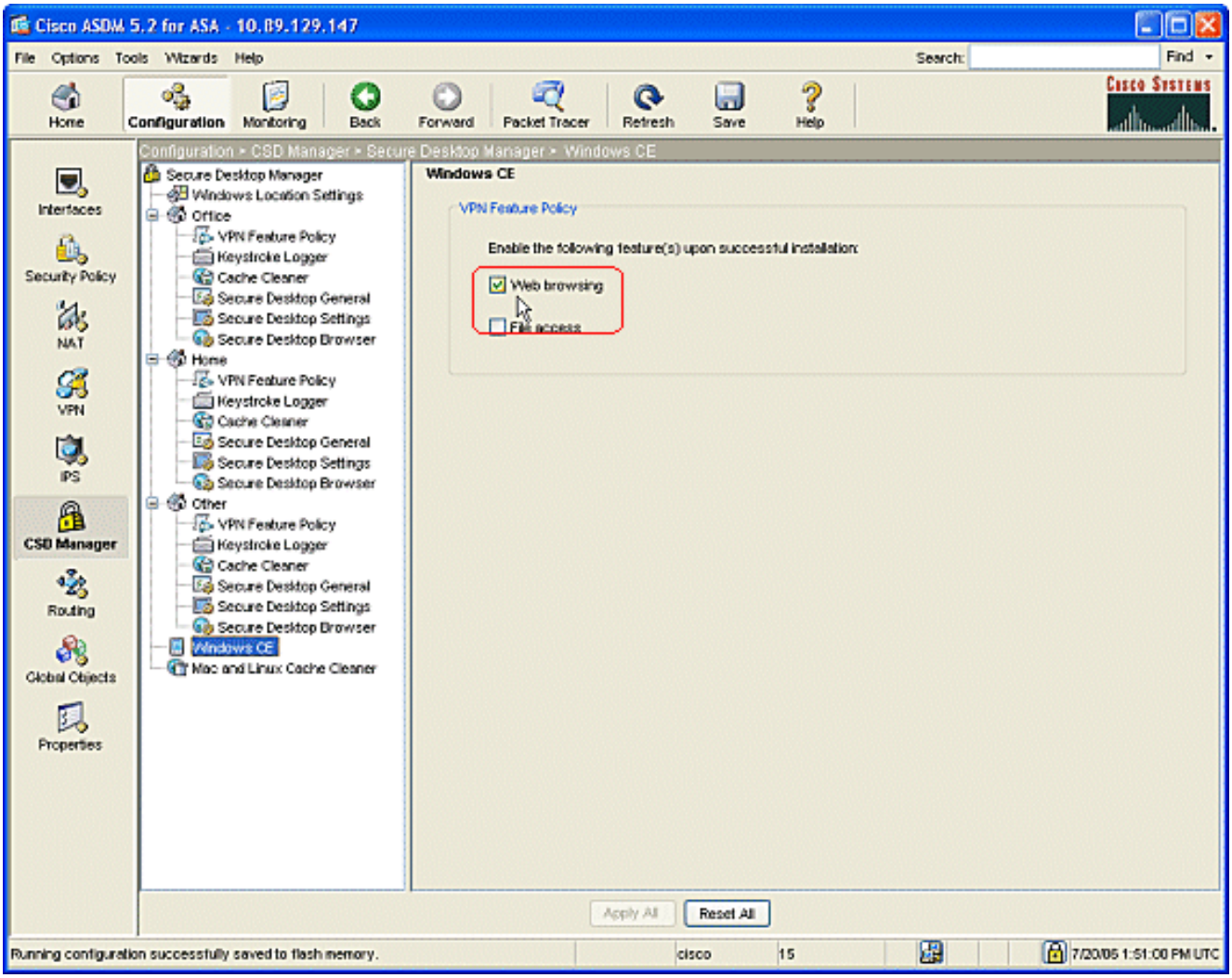
5. Voor klanten in deze plaats **van het** Functiebeleid van **VPN**, klik het **Web Browsing** tabblad, en klik de **altijd Ingeschakelde** radioknop.Klik op het tabblad **File Access** en klik op de knop **Uitschakelen**.Herhaal de stap met de tabbladen **Port Forwarding** en **Full Tunneling**.Klik op **Alles toepassen**.Klik op **Opslaan** en vervolgens op **Ja** om de wijzigingen te aanvaarden.



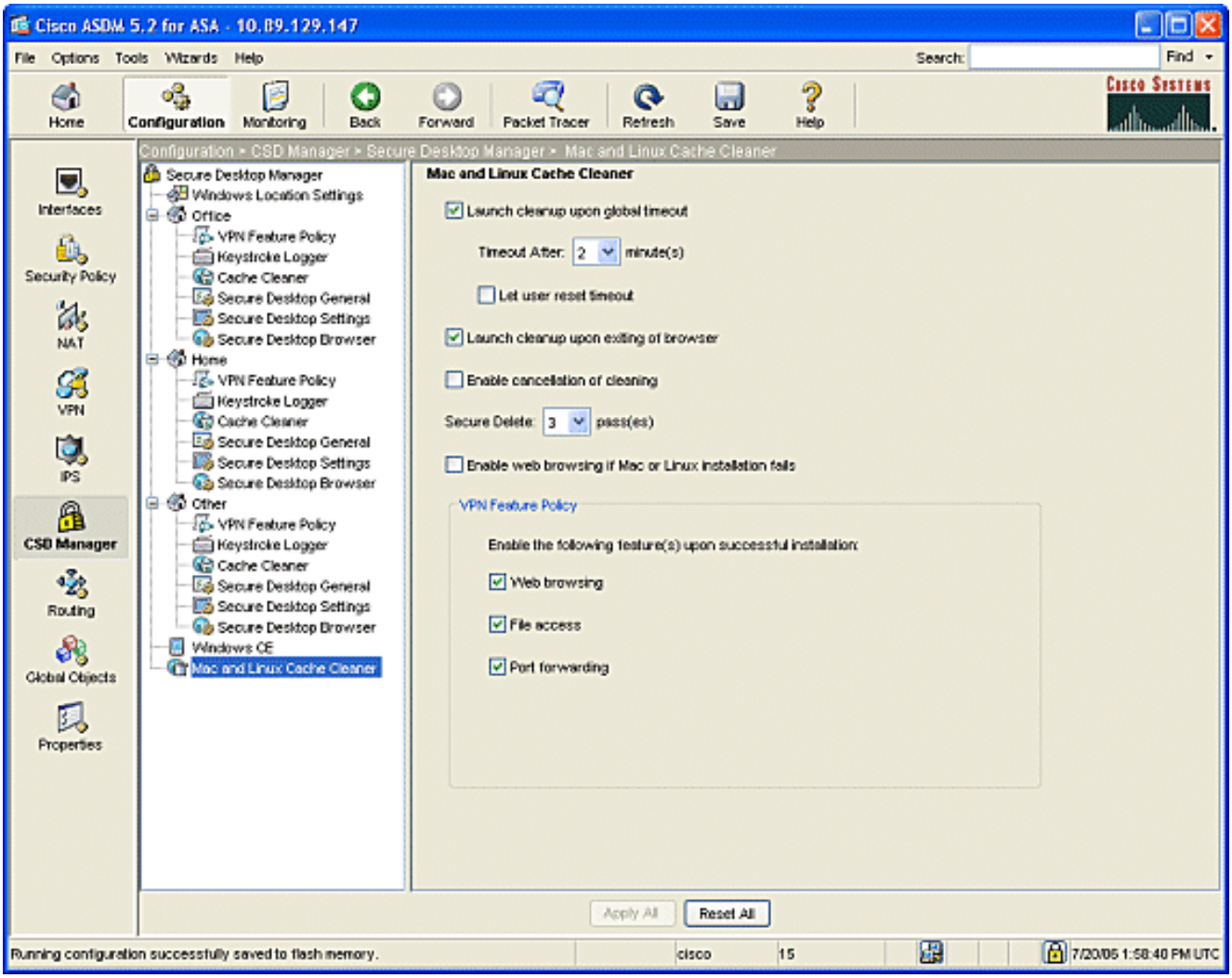
Optionele configuraties voor Windows CE, Macintosh en Linux-clients

Deze configuraties zijn optioneel.

1. Als u **Windows CE** uit het navigatiedeelvenster kiest, controleert u het vakje **Web browsing**.



2. Als u **Mac en Linux Cache Cleaner** kiest uit het navigatiedeelvenster, controleert u de **Start clean-up bij de** radioknop **van de global timeout**.Verander de tijd in de specificatie.Controleer onder **het** gebied **van het** Functiebeleid van **VPN**, de **Webbrowsing, de Toegang van het Bestand**, en de **Port** het **verzenden** van radiokalen voor deze klanten.



3. Of u Windows CE of Mac en Linux Cache Cleaner kiest, klik op **Toepassen**.
4. Klik op **Opslaan** en vervolgens op **Ja** om de wijzigingen te aanvaarden.

Configureren

Configuratie

Deze configuratie weerspiegelt de wijzigingen die ASDM heeft aangebracht om CSD in staat te stellen: De meeste CSD-configuraties worden op flitser in een afzonderlijk bestand bewaard.

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
```

Verifiëren

Gebruik deze sectie om te bevestigen dat uw configuraties voor Clientless SSL VPN, Thin-Client SSL VPN of SSL VPN-client (SVC) correct werken.

Test CSD met een PC die bij verschillende Windows-locaties is ingesteld. Elke test moet een andere toegang bieden in overeenstemming met het beleid dat u in het bovenstaande voorbeeld hebt ingesteld.

U kunt het poortnummer en de interface wijzigen waar Cisco ASA naar WebVPN-verbindingen luistert.

- De standaardpoort is 443. Als u de standaardpoort gebruikt is de toegang **https://ASA IP-adres**.
- Het gebruik van een andere poort verandert de toegang tot **https://ASA IP Address:newportnumber**.

Opdrachten

Verschillende **tonen** opdrachten worden geassocieerd met WebVPN. U kunt deze opdrachten uitvoeren op de opdrachtregel-interface (CLI) om statistieken en andere informatie weer te geven. Zie WebVPN-configuratie controleren van het gebruik van de opdrachten in detail controleren.

Opmerking: Uitvoer Tolk (alleen geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Als u problemen hebt met de externe client, controleert u deze:

1. Zijn pop-ups, Java en/of ActiveX ingeschakeld in de webbrowser? Deze moeten mogelijk worden ingeschakeld, afhankelijk van het type SSL VPN-verbinding dat in gebruik is.
2. De klant moet de bij het begin van de sessie gepresenteerde digitale certificaten accepteren.

Opdrachten

Meerdere **debug** opdrachten zijn gekoppeld aan WebVPN. Raadpleeg voor gedetailleerde informatie over deze opdrachten de optie Opdrachtinterinstructies gebruiken op WebVPN.

Opmerking: het gebruik van **debug-**opdrachten kan een negatieve invloed hebben op uw Cisco-apparaat. Voordat u **debug**-opdrachten gebruikt, raadpleegt u Belangrijke informatie over Debug Commands.

Gerelateerde informatie

- Cisco ASA 5500 Series adaptieve security applicaties
- ASA met WebVPN en Single aanmelding bij gebruik van ASDM en NTLMv1 Configuration Voorbeeld
- Technische ondersteuning en documentatie – Cisco Systems