Cisco Secure Desktop (CSD 3.1.x) en ASA 7.2.x para el ejemplo de configuración de Windows usando el ASDM

Contenido

Introducción

Cisco Secure Desktop (CSD) amplía la seguridad de la tecnología VPN SSL. CSD proporciona una partición separada en la estación de trabajo de un usuario para la actividad de sesión. Este área de seguridad se cifra durante las sesiones y se elimina por completo al final de una sesión de VPN SSL. Windows se puede configurar con las ventajas de seguridad total del CSD. Macintosh, Linux,y Windows CE tienen acceso solamente a las funciones de Limpieza de Caché, Exploración de la Web y Acceso a Archivos. CSD se puede configurar para dispositivos Windows, Macintosh, Windows CE y Linux en estas plataformas:

- 5500 Series adaptantes del dispositivo de seguridad de Cisco (ASA)
- Routeres Cisco que funcionan con las versiones 12.4(6)T del Cisco IOS ® Software y posterior

- Versión 4.7 y posterior del Concentradores Cisco VPN de la serie 3000
- Módulo del WebVPN de Cisco en el Routers de las Catalyst 6500 y 7600 Series

Nota: La versión 3.3 CSD ahora le deja configurar el Cisco Secure Desktop para ejecutarse en las computadoras remotas que ejecutan Microsoft Windows Vista. Previamente, el Cisco Secure Desktop fue limitado a los ordenadores que ejecutaron Windows XP o 2000. Refiera a la mejora de la nueva función - Secure Desktop en la sección de Vista de los Release Note para el Cisco Secure Desktop, versión 3.3, para más información.

Este ejemplo cubre sobre todo la instalación y la configuración del CSD en las 5500 Series ASA para los clientes de Windows. Las configuraciones optativas para Windows CE, el mac, y los clientes de Linux se agregan para la realización.

El CSD se utiliza conjuntamente con la tecnología VPN SSL (clientless SSL VPN, cliente “liviano” SSL VPN, o (SVC) del cliente VPN SSL). El CSD agrega el valor a las sesiones seguras de la tecnología VPN SSL.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

Requisitos para el dispositivo del theASA

- Versión 3.1 de Cisco CSD o más adelante
- Versión de software 7.1.1 de Cisco ASA o más adelante
- Versión 5.1.1 del Cisco Adaptive Security Device Manager (ASDM) o más adelante**Nota:** Soportes de la versión 3.2 CSD en la Versión de ASA 8.x solamente**Nota:** Consulte Cómo Permitir el Acceso HTTPS para el ASDM para que el ASA sea configurado por el ASDM.

Requisitos para las computadoras cliente

- Los clientes remotos deben tener privilegios administrativos locales; no se requiere, sino que se sugiere altamente.
- Los clientes remotos deben tener versión 1.4 o posterior del Entorno de tiempo de ejecución Java (JRE).
- Navegadores de cliente remoto: Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, safari 1.2.2, o Firefox 1.0
- Cookie habilitados y popups permitido en los clientes remotos

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ASDM versión 5.2(1)
- Versión de ASA de Cisco 7.2(1)
- Cisco CSD Version-securedesktop-asa-3.1.1.32-k9.pkg

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos usados en este documento comenzaron con una configuración despejada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando. Los IP Addresses usados en esta configuración son direccionamientos del RFC 1918. Estos IP Addresses no son legales en Internet y deben ser utilizados solamente en un ambiente de laboratorio de la prueba.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

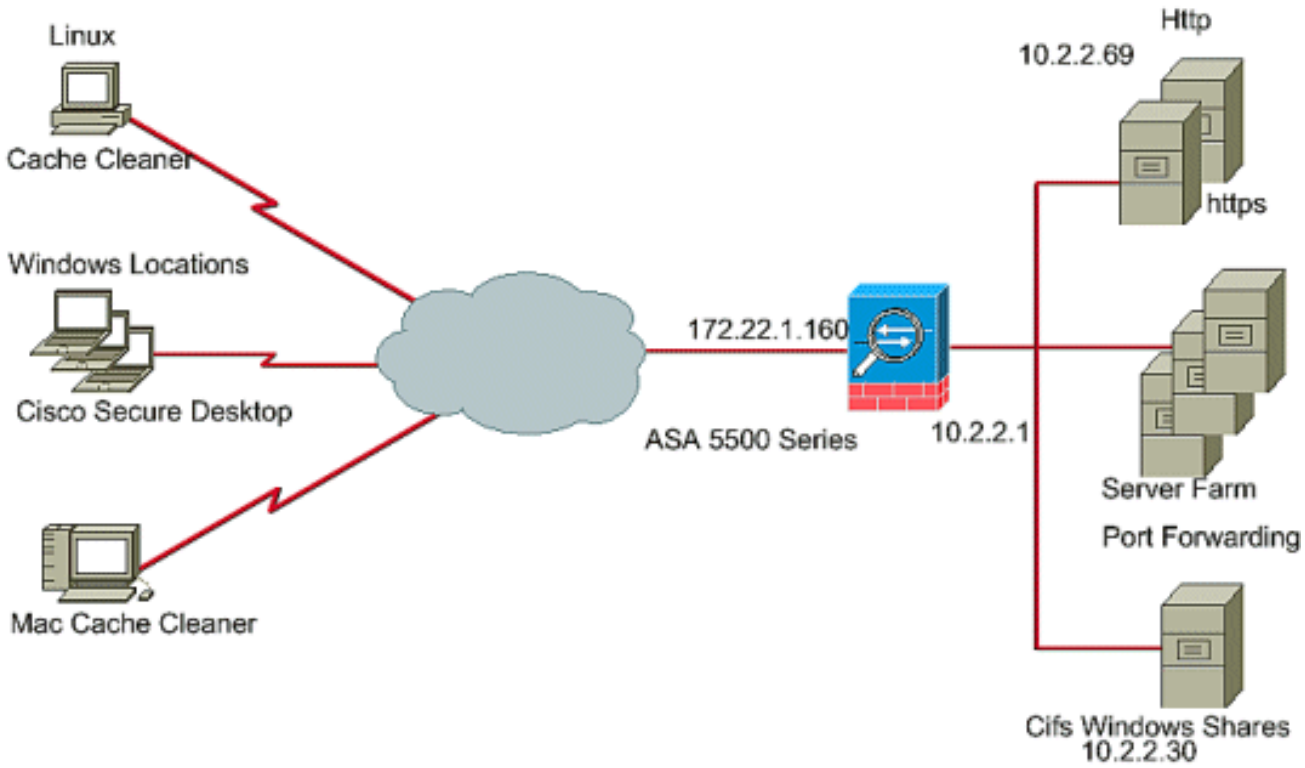
Antecedentes

El CSD actúa con la tecnología VPN SSL, así que el clientless, el cliente “liviano”, o SVC se deben activar antes de la configuración del CSD.

Diagrama de la red

Diversas ubicaciones de Windows se pueden configurar con los aspectos de la seguridad total del CSD. Macintosh, Linux, y Windows CE tienen acceso solamente al producto de limpieza de discos del caché y/o exploración de la Web y al acceso al archivo.

En este documento, se utiliza esta configuración de red:



Configuración CSD en el ASA para los clientes de Windows

Configuración CSD en el ASA para los clientes de Windows con cinco pasos principales:

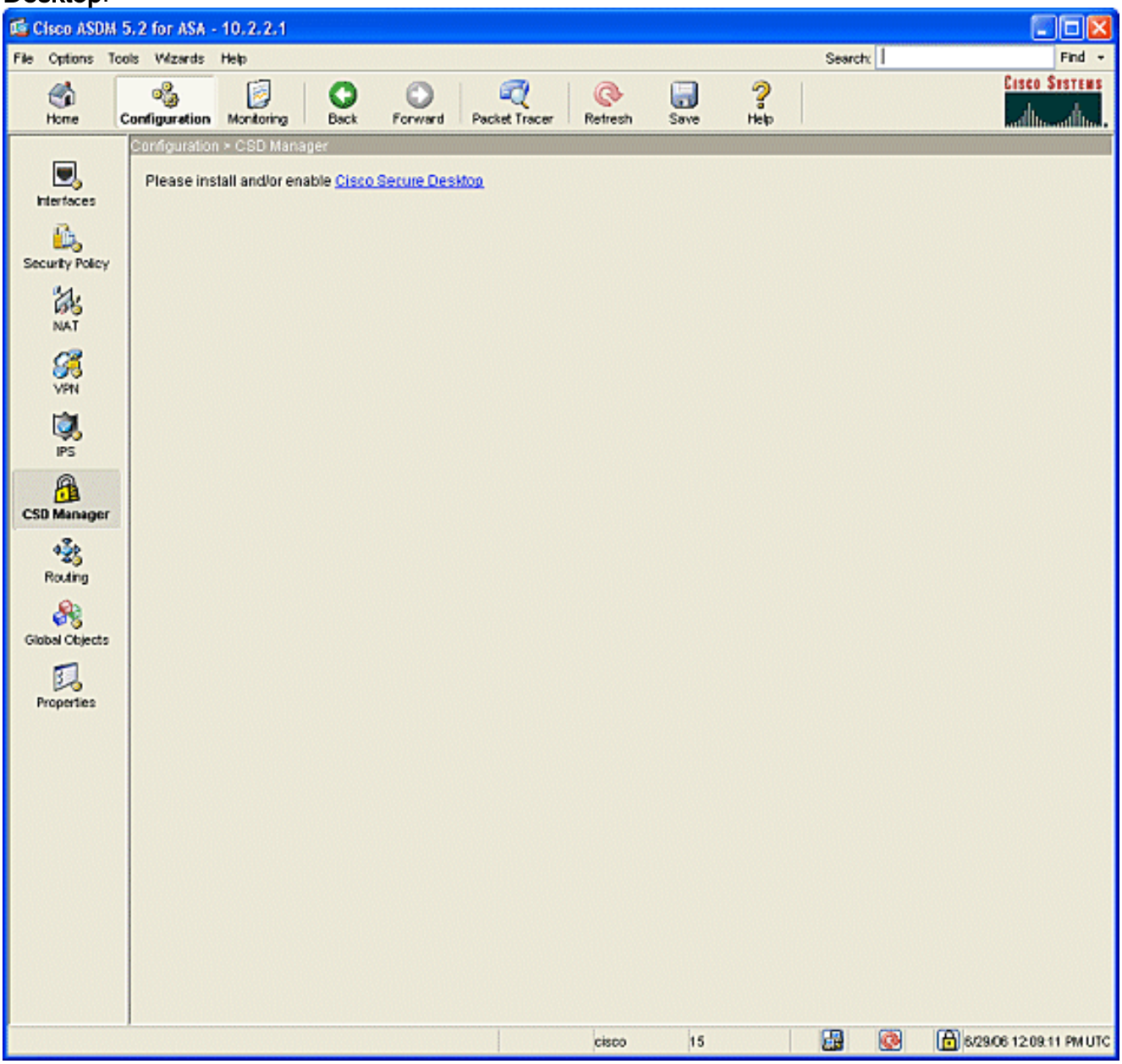
- Obtenga, instale, y habilite el software CSD en Cisco ASA.

- Defina las ubicaciones de Windows.
- Defina la identificación de la ubicación de Windows.
- Configure los módulos de la ubicación de Windows.
- Configure las características de la ubicación de Windows.
- Configuración optativa para Windows CE, Macintosh, y los clientes de Linux.

Obtenga, instale, y habilite el software CSD

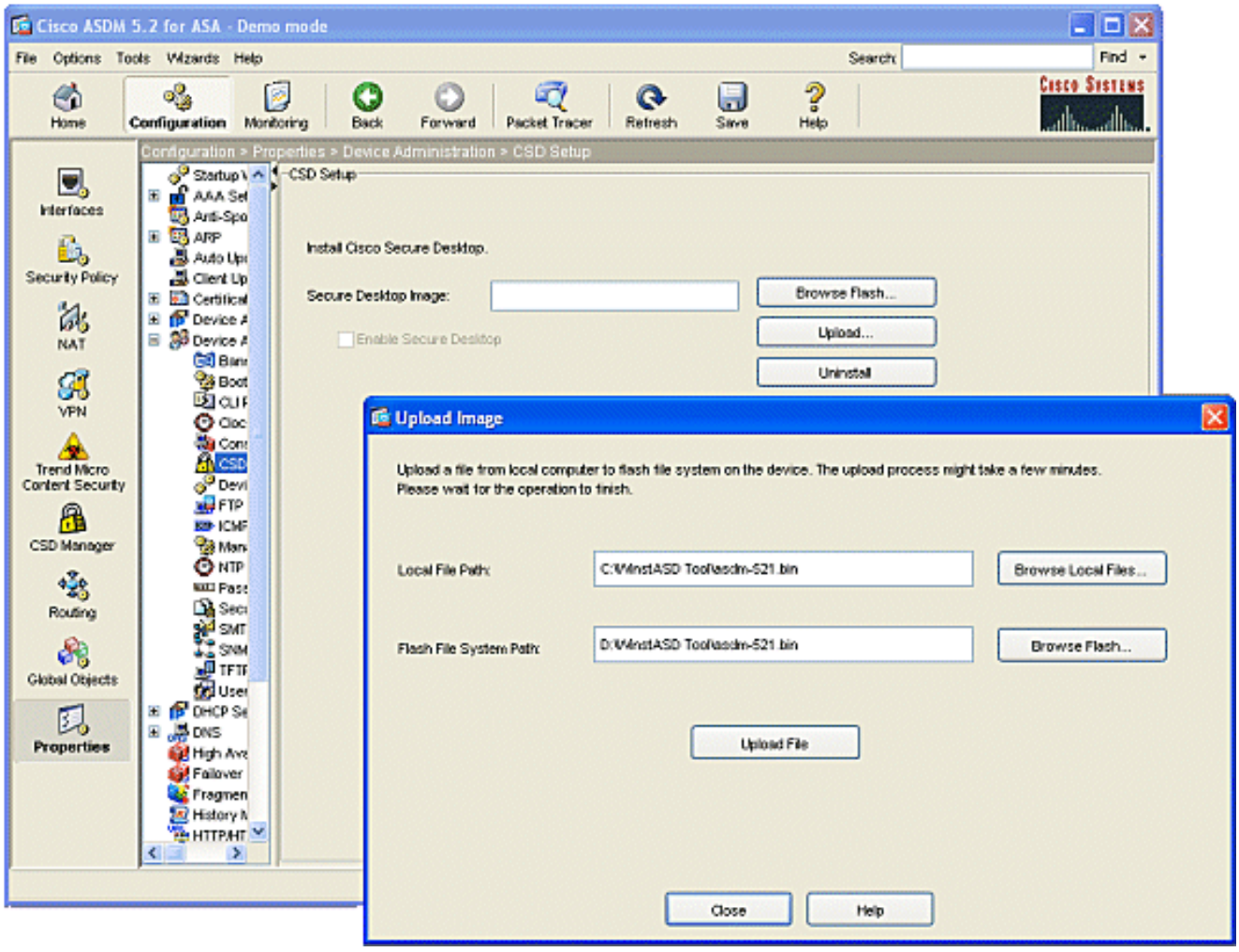
Complete estos pasos para obtener, para instalar, y para habilitar el software CSD en Cisco ASA.

1. Descargue el software securedesktop-asa*.package CSD y los archivos Léame sobre su estación de administración del sitio web de la descarga de software de Cisco.
2. Inicie sesión al ASDM y haga clic el botón de la **configuración**. Del menú izquierdo, haga clic el botón del **administrador CSD**, y haga clic el link del **Cisco Secure Desktop**.



3. Haga clic la **carga** para visualizar la ventana de la imagen de la carga.O ingrese la trayectoria del nuevo archivo .package en la estación de administración o el tecleo **hojea los archivos locales** para localizar el archivo.Cualquiera ingresa la ubicación en el flash en el

cual poner el archivo o el tecleo **hojee el Flash**.Haga clic el **archivo de la carga**.Cuando se le pregunte, **AUTORIZACIÓN del** tecleo **> cercano > ACEPTABLE**.

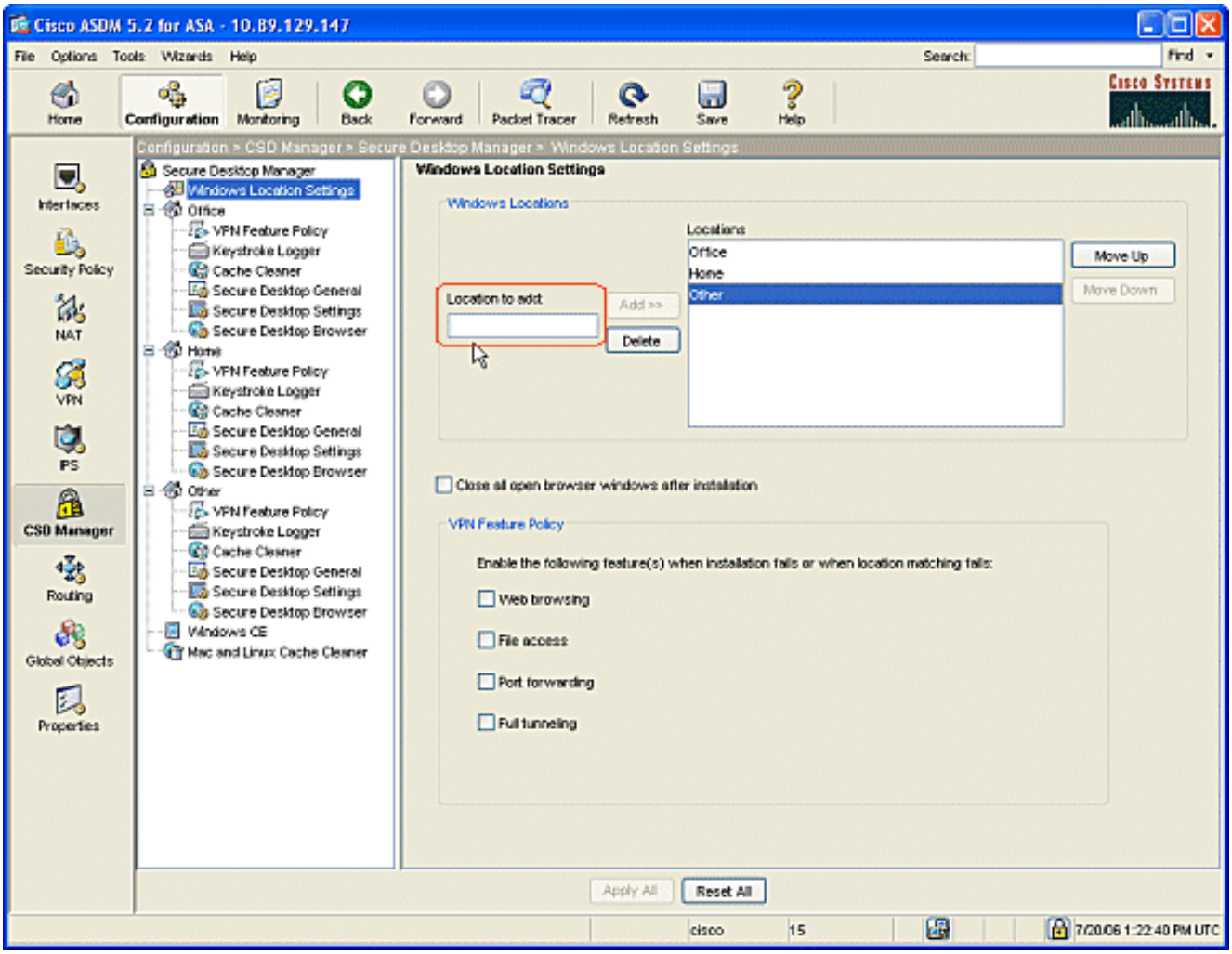


4. Una vez que la imagen del cliente se carga para contellear, marque la casilla de verificación del **cliente VPN del permiso SSL**, y después haga clic **se aplican**.
5. Haga clic la **salvaguardia**, y después haga clic **sí** para validar los cambios.

Defina las ubicaciones de Windows

Complete estos pasos para definir las ubicaciones de Windows.

1. Haga clic el botón de la **configuración**.
2. Del menú izquierdo, haga clic el botón del **administrador CSD**, y haga clic el link del **Cisco Secure Desktop**.
3. Del SCR_INVALID, haga clic las **configuraciones de ubicación de Windows**.
4. Teclee un nombre de la ubicación en la ubicación para agregar el campo y el haga click en AddObserve las tres ubicaciones en este ejemplo: Oficina, hogar, y otros.La oficina representa los puestos de trabajo que están situados dentro del límite de la Seguridad de la sociedad.El hogar representa a los usuarios que trabajan del hogar.Otro representa cualquier ubicación con excepción de las dos ubicaciones mencionadas.

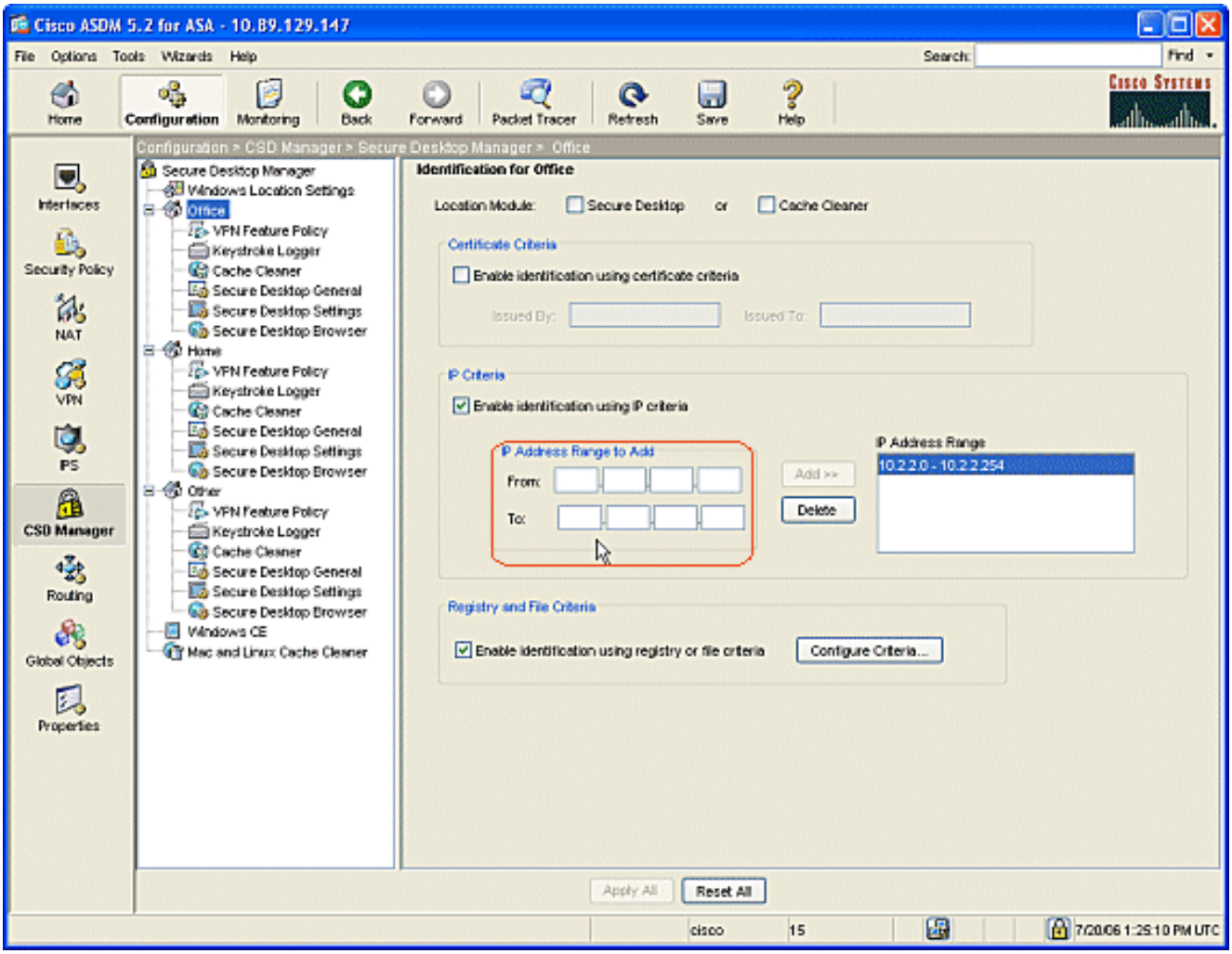


5. Cree sus propias ubicaciones dependientes en la disposición de su arquitectura de red para las ventas, los invitados, los Partners, y otros.
6. Pues usted crea las ubicaciones de Windows, el SCR_INVALID se amplía con los módulos configurables para cada nueva ubicación. El tecleo **aplica todos**.
7. **La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los cambios.

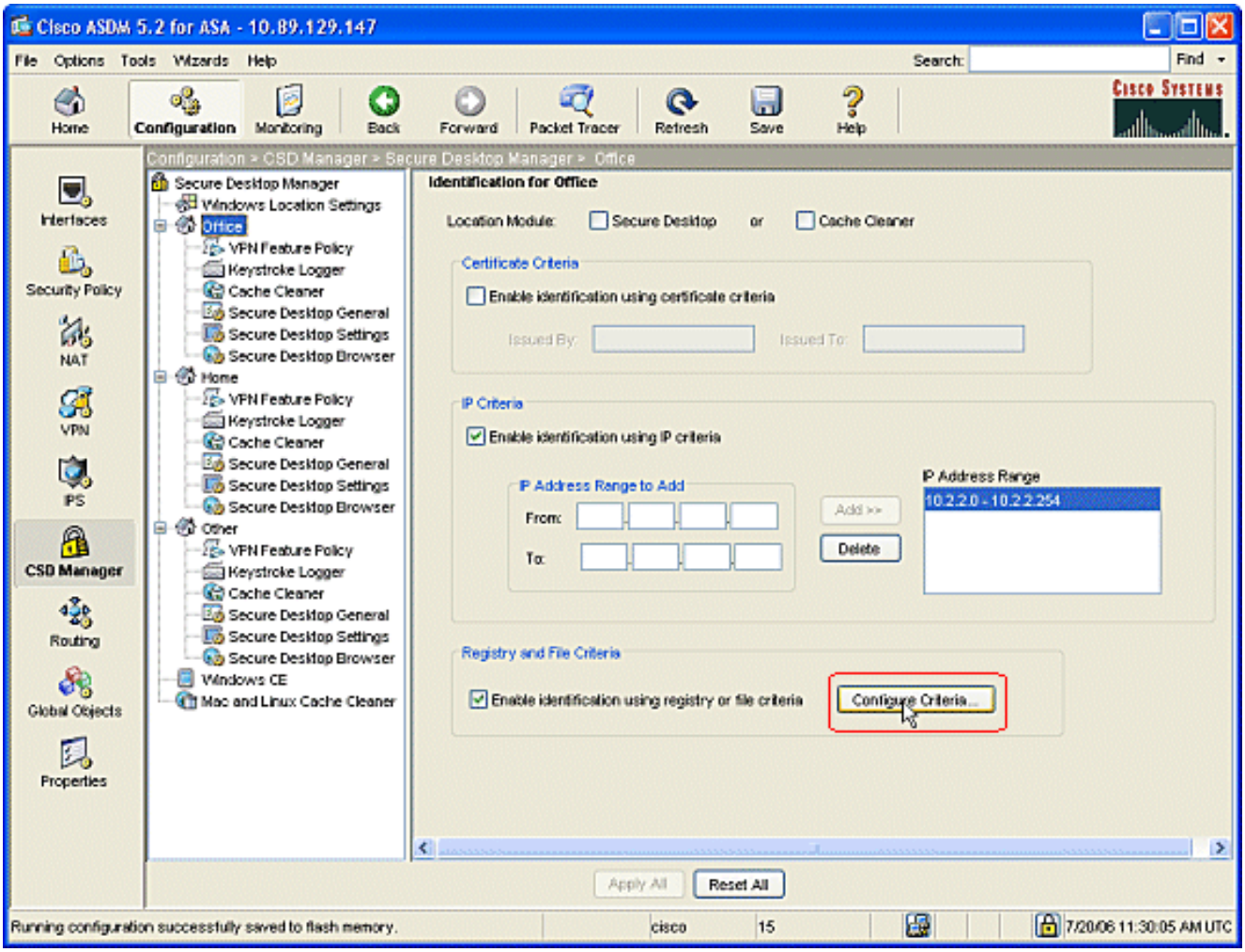
Identificación de la ubicación de Windows

Complete estos pasos para definir la identificación de la ubicación de Windows.

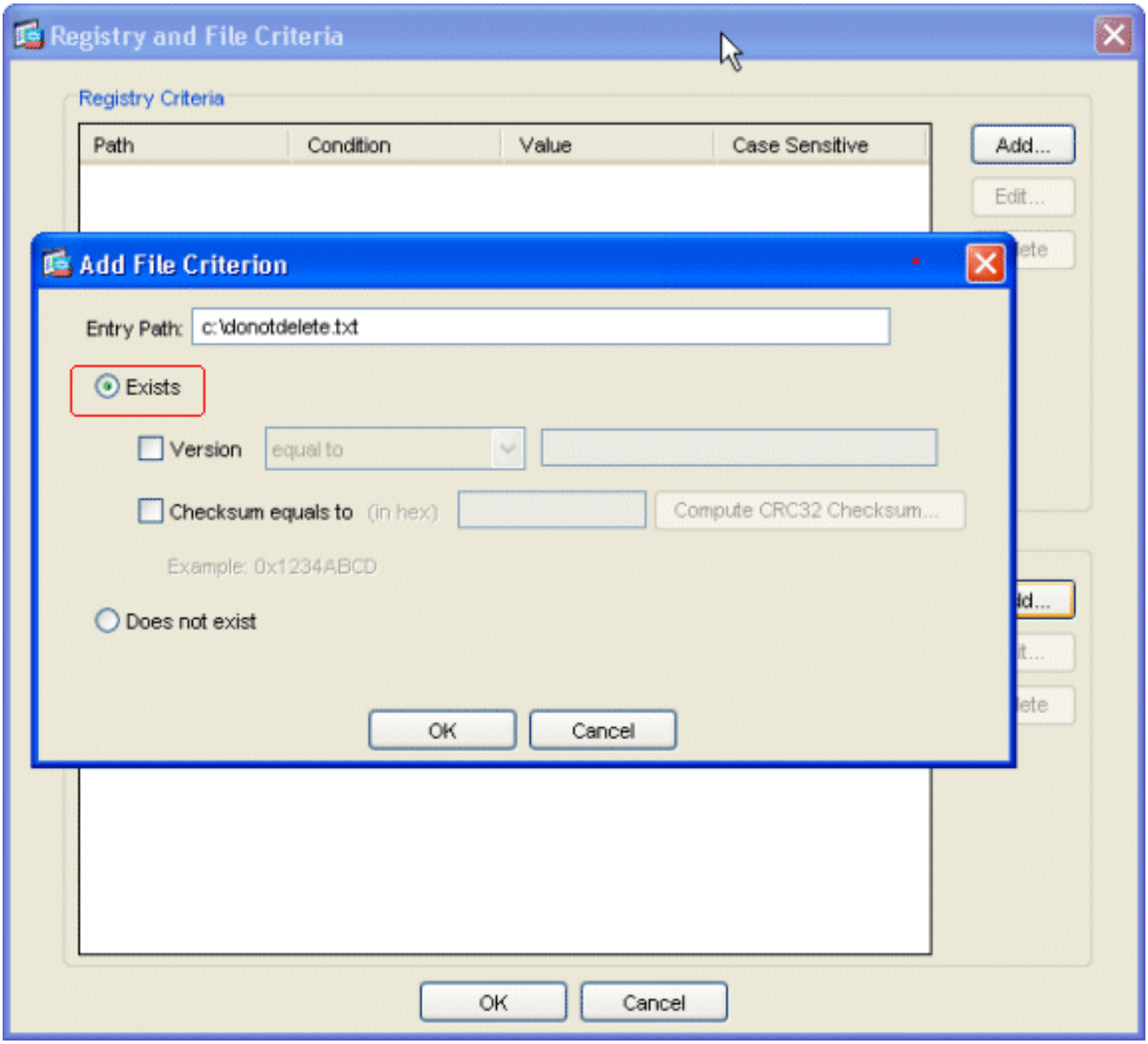
1. Identifique las ubicaciones que fueron creadas adentro definen las ubicaciones de Windows.



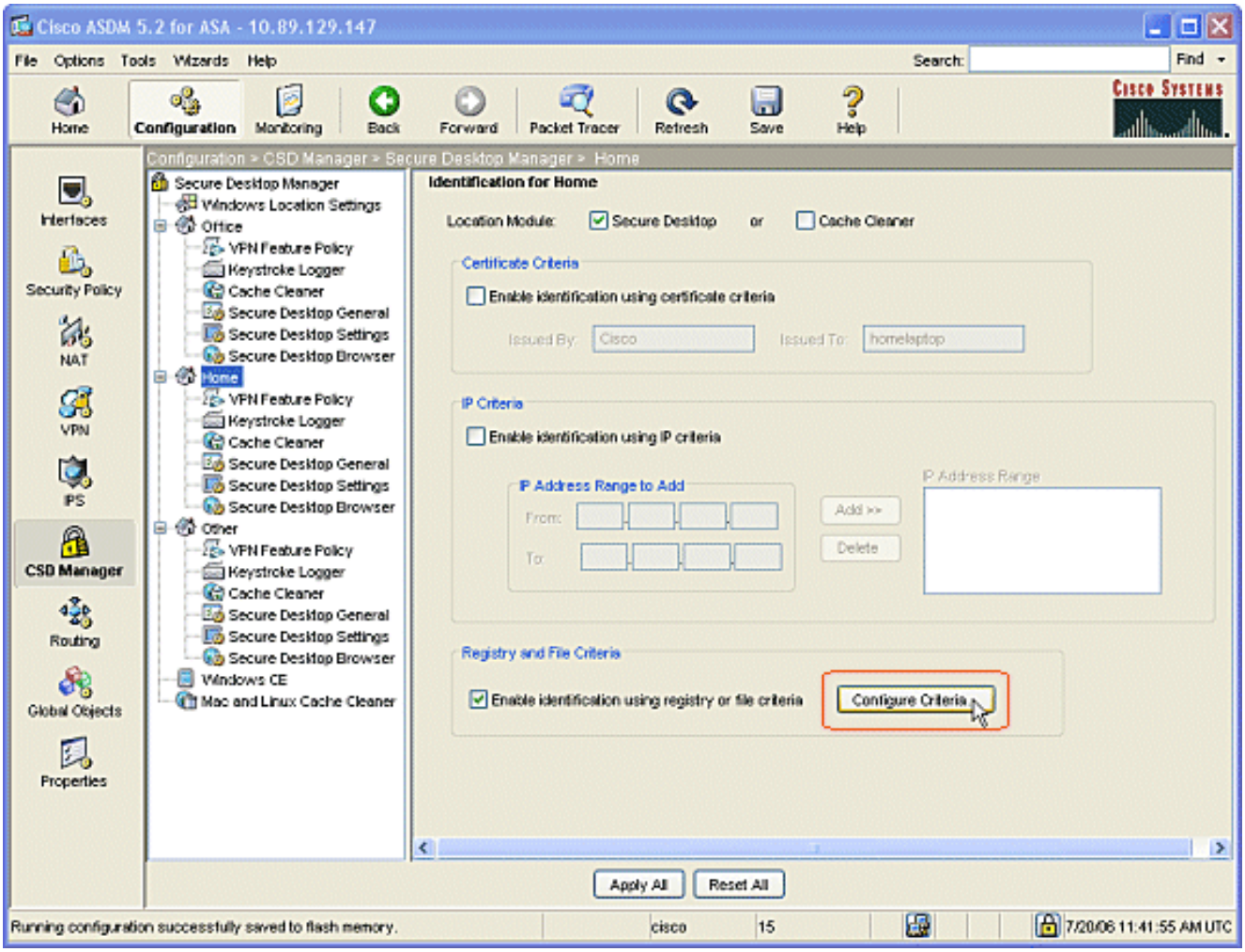
2. Para identificar la oficina de la ubicación, haga clic la **oficina** en el SCR_INVALID.Desmarque el **Secure Desktop** y **oculte el producto de limpieza de discos** porque éstos son ordenadores internos.Marque la **identificación del permiso usando los criterios IP**.Ingrese los alcances del IP Address de sus ordenadores internos.Marque la **identificación del permiso usando el registro o clasifíe los criterios**. Esto distingue a los oficinistas internos de los invitados ocasionales en la
red.



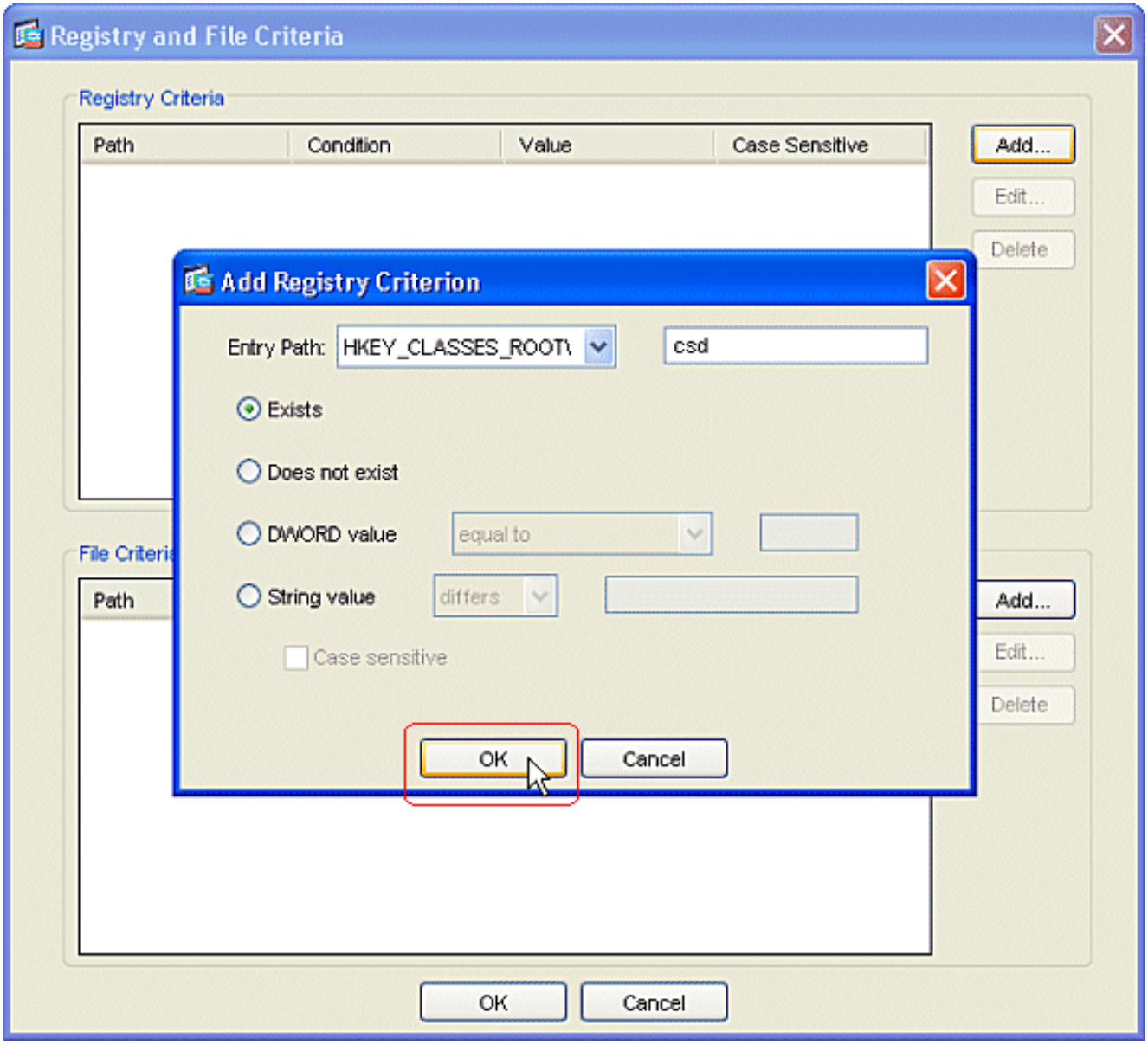
3. **Criterios de la configuración del** tecleo. Un ejemplo simple de un archivo “DoNotDelete.txt” se configura. Este archivo debe existir en sus computadores con Windows internos y es simplemente un placeholder. Usted puede también configurar una clave del registro de Windows para identificar los ordenadores de oficina internos. Tecleo OKIN la ventana del criterio del archivo del agregar. Haga clic OKIN el registro y clasifíe la ventana de los criterios.



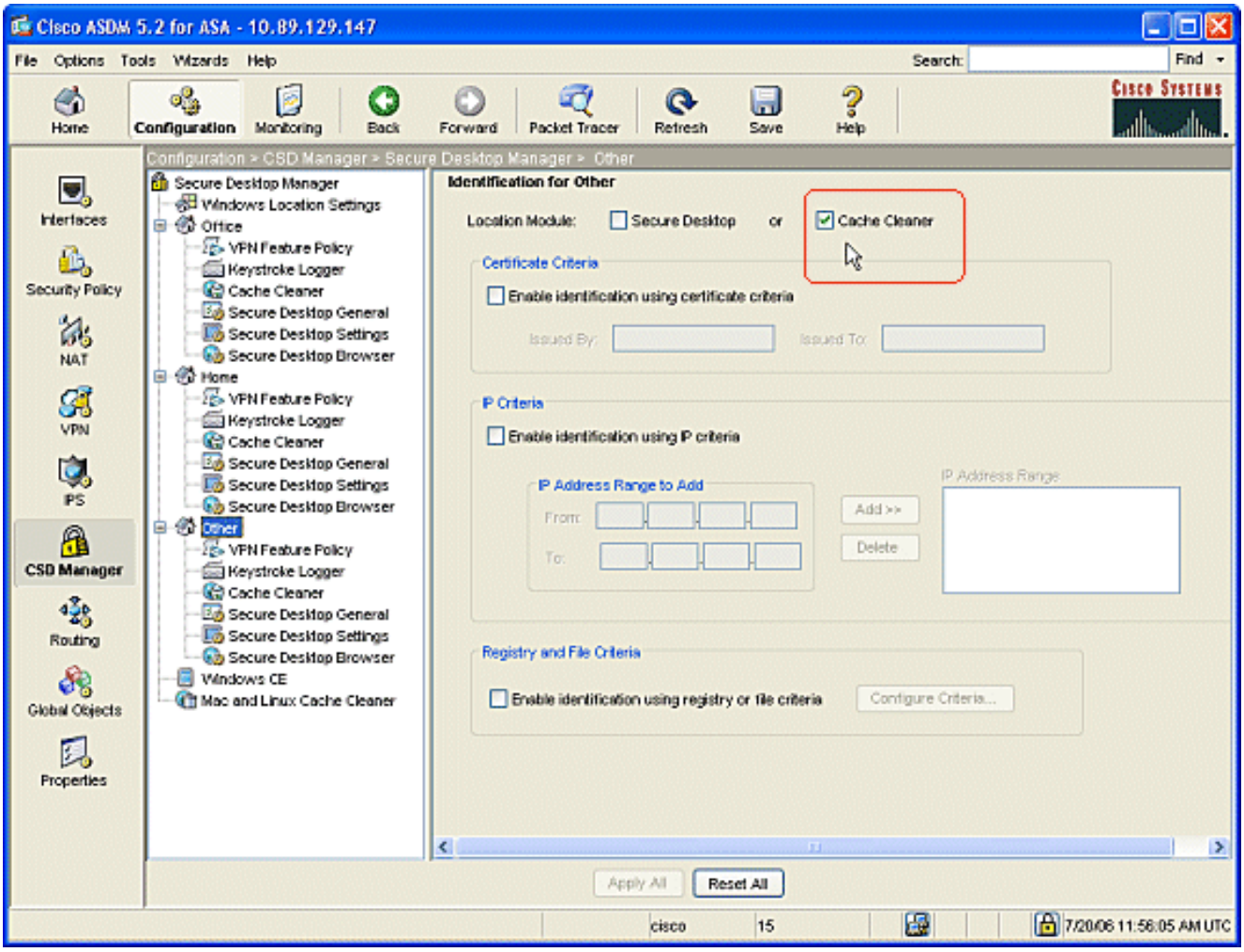
4. El tecleo **aplica todos** en la identificación para la ventana de la oficina. **La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los cambios.
5. Para identificar el hogar de la ubicación, **hogar del** tecleo en el SCR_INVALID.Marque la **identificación del permiso usando el registro o clasifíe los criterios**.Haga clic los **criterios de la configuración**.



6. Las computadoras cliente caseras deben haber sido configuradas con esta clave de registro por un administrador. Haga Click en OK en la ventana del criterio del registro del agregar. Haga Click en OK en la ventana de los criterios del registro y del archivo.



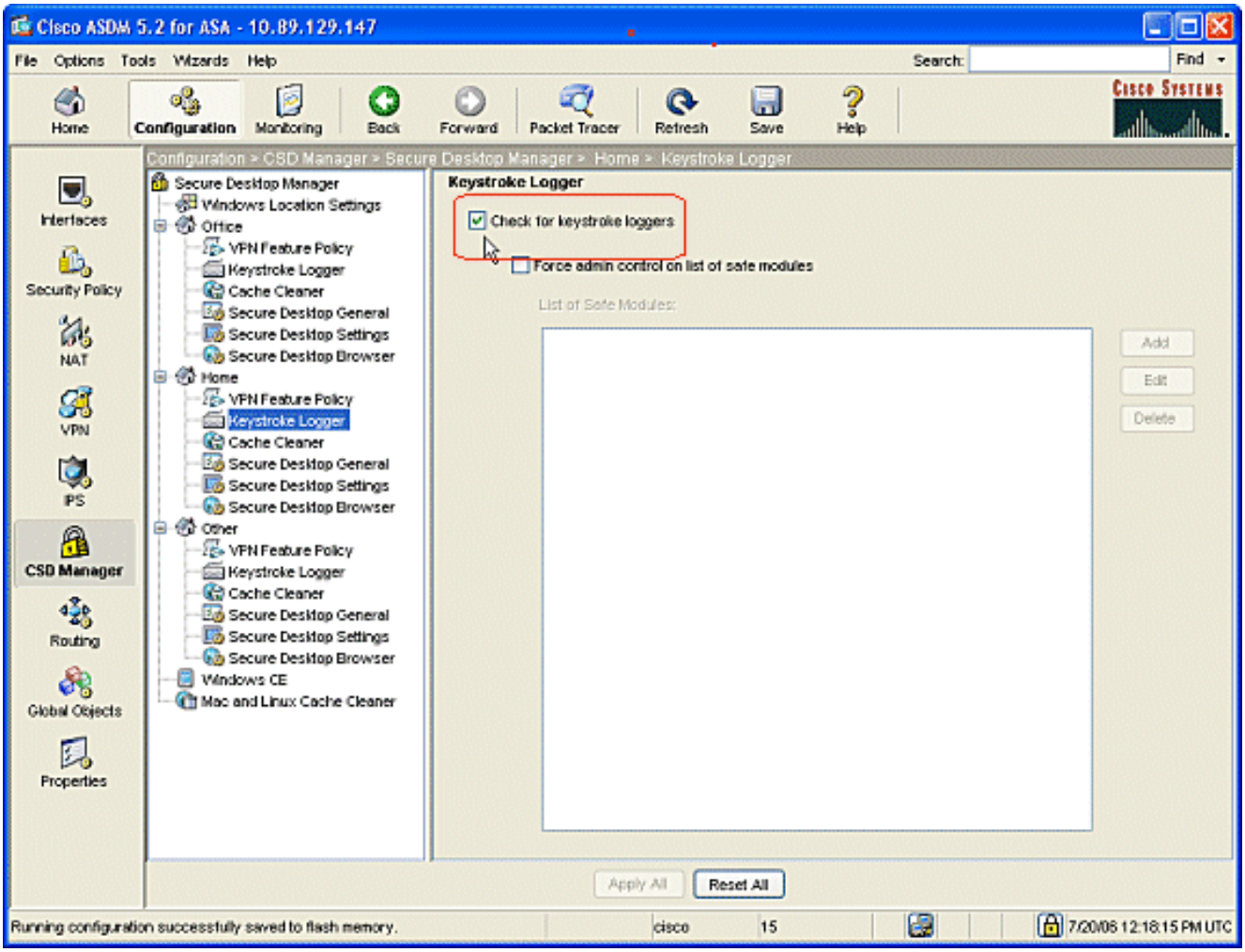
7. Bajo el módulo de la ubicación, **Secure Desktop del** control. El tecleo **aplica todos** en la identificación para la ventana casera. **La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los cambios.
8. Para identificar la ubicación **otro**, hace clic **otro** en el SCR_INVALID.Marque solamente el cuadro del **producto de limpieza de discos del caché** y desmarque el resto de los cuadros.El tecleo **aplica todos** en la identificación para la otra ventana.**La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los
cambios.



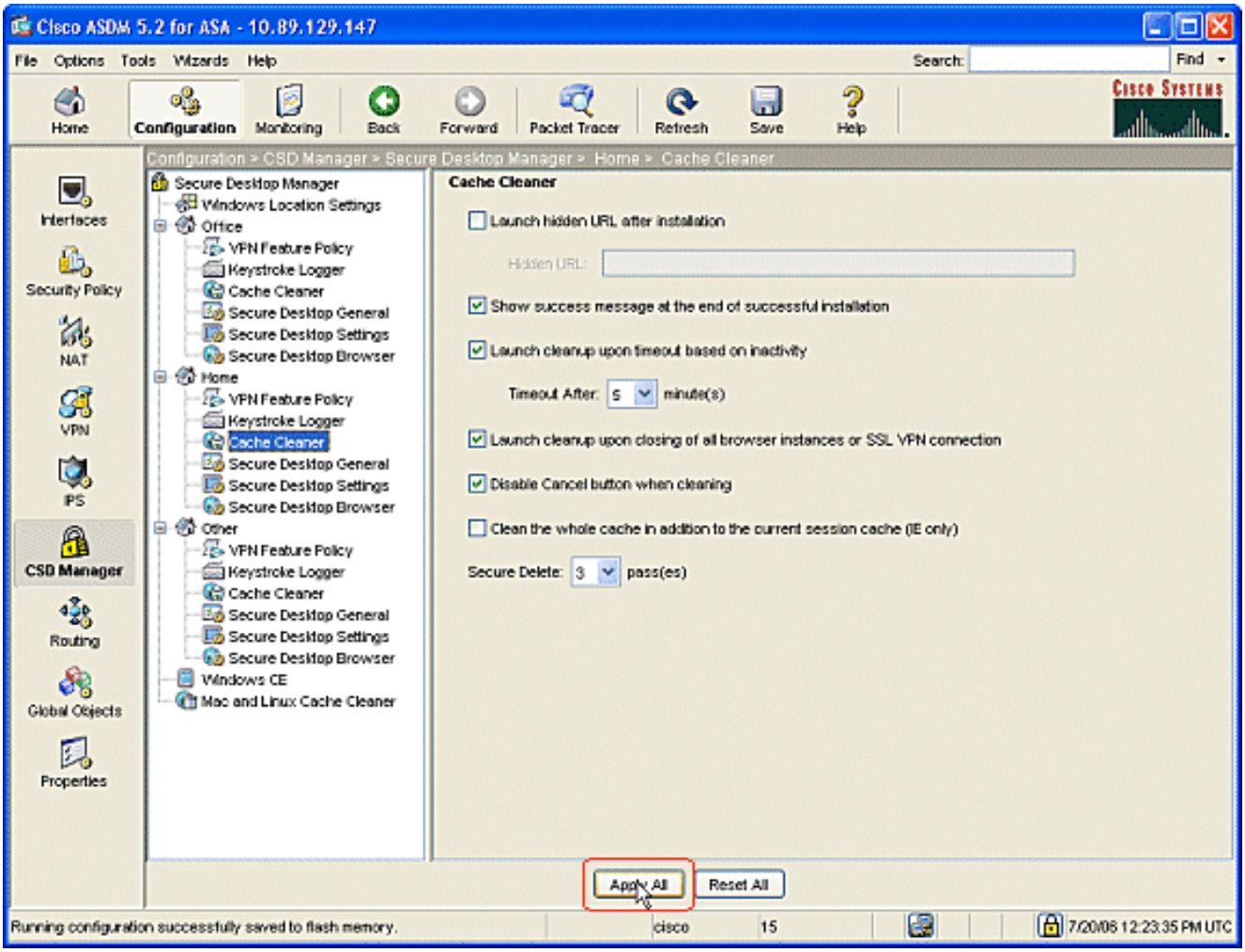
Módulo de la ubicación de Windows de la configuración

Complete estos pasos para configurar los módulos bajo cada uno de las tres ubicaciones que usted creó.

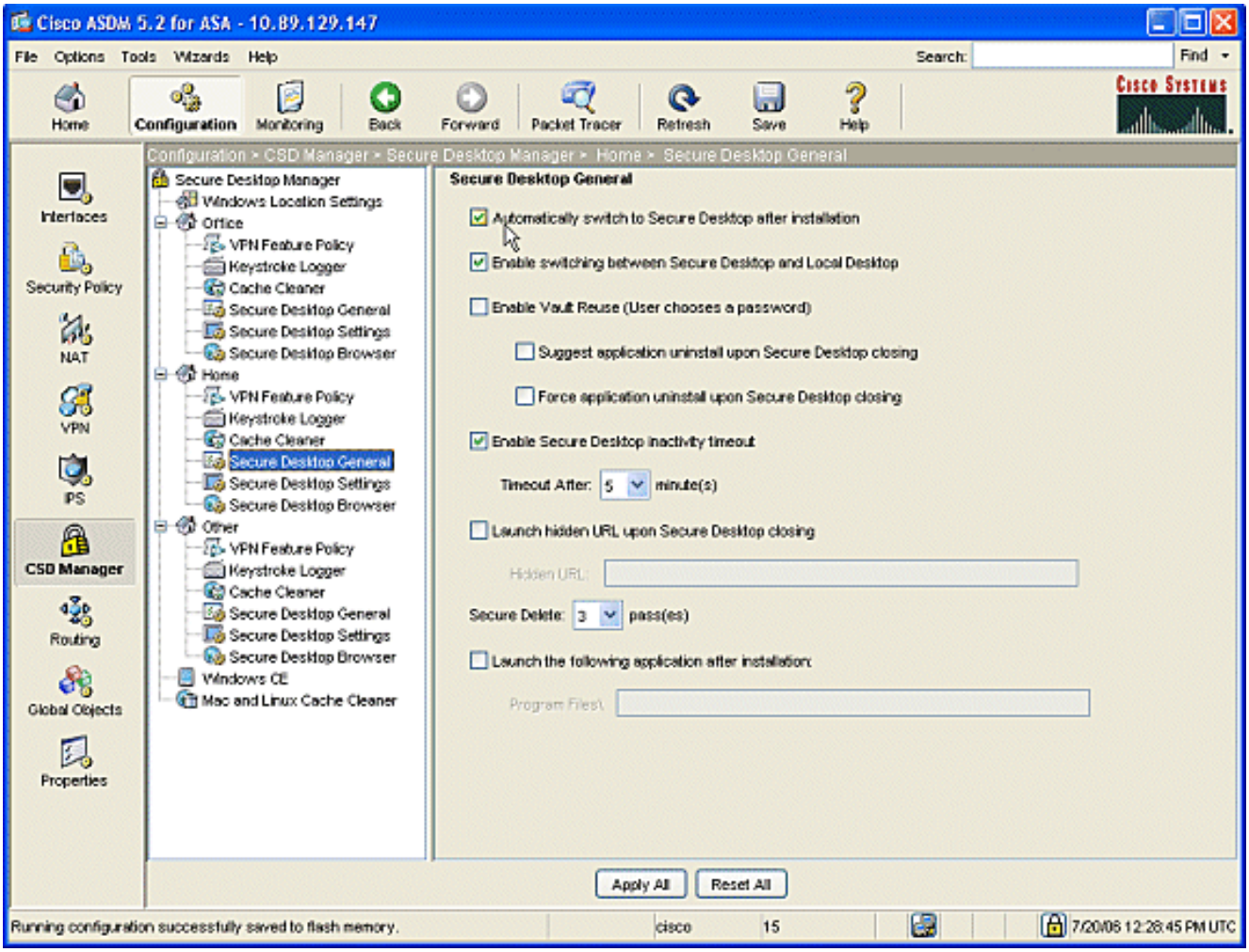
1. Para los clientes de la oficina, no haga nada puesto que el producto de limpieza de discos del Secure Desktop y del caché no fue elegido en los pasos anteriores. La aplicación ASDM permite que usted configure el producto de limpieza de discos del caché incluso si no fue elegida en un paso anterior. Guarde las configuraciones predeterminadas para las ubicaciones de las instalaciones.**Nota:** La directiva de la característica VPN no se discute en este paso, sino que será discutida en un paso subsiguiente para todas las ubicaciones.
2. Para los clientes caseros, **hogar del** tecleo y **maderero del golpe de teclado** en el SCR_INVALID.En la ventana del maderero del golpe de teclado, **comprobación para del** control los **madereros del golpe de teclado**.El tecleo **aplica todos** en la ventana del maderero del golpe de teclado.**La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los cambios.



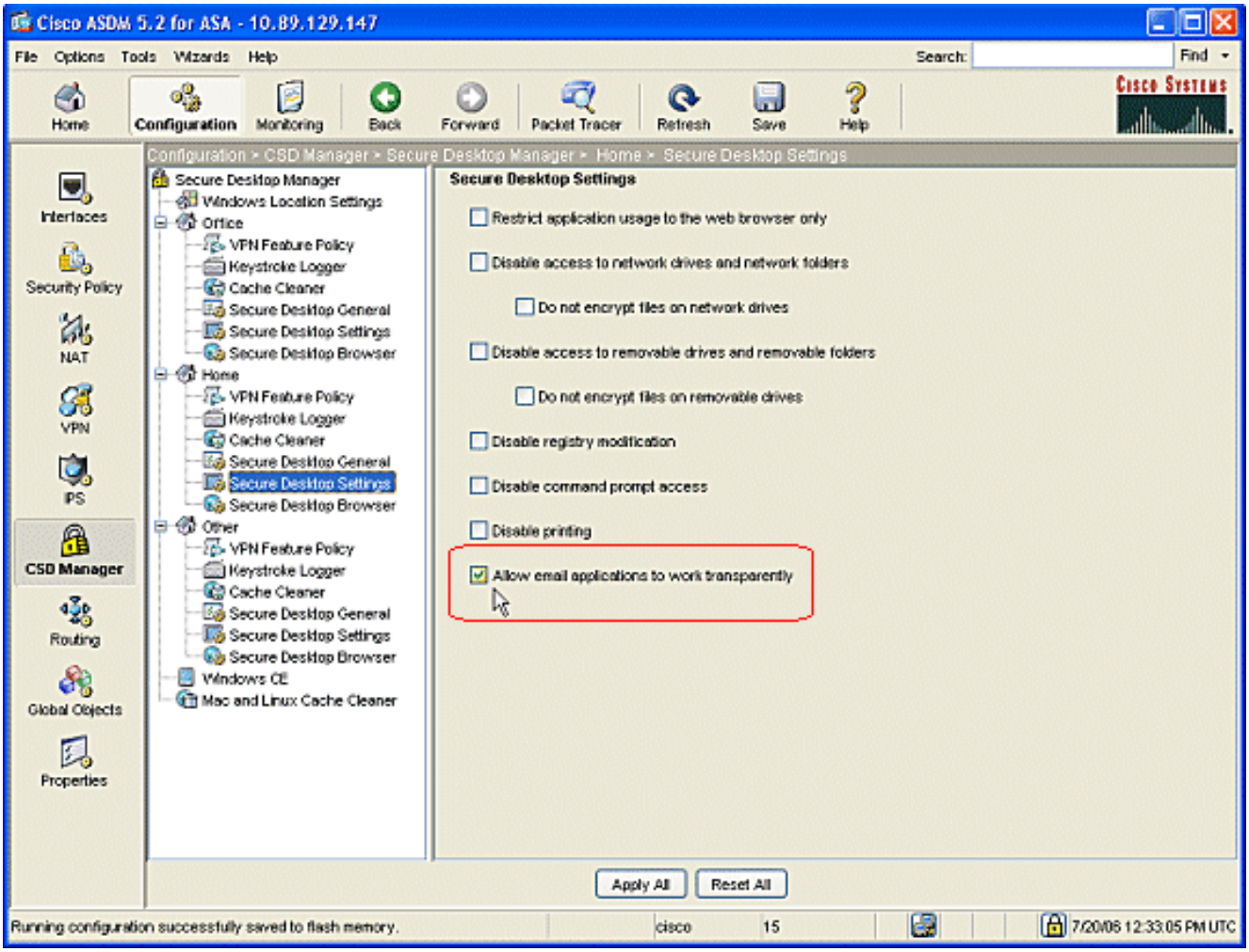
3. Bajo hogar, elija el **producto de limpieza de discos del caché** y los parámetros para adaptarse a su
entorno.



4. Bajo hogar, elija el **Secure Desktop general** y los parámetros para adaptarse a su entorno.



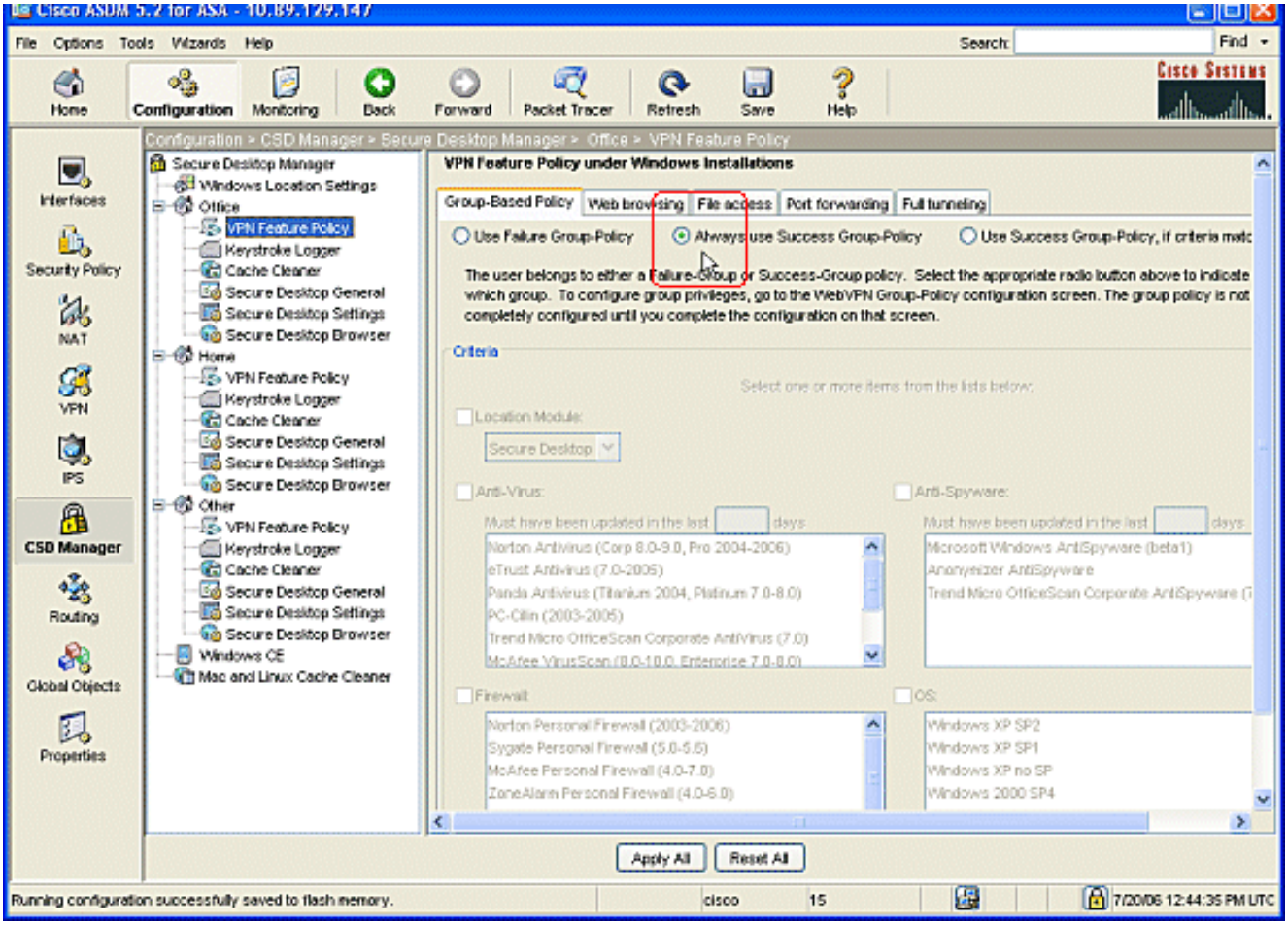
5. Bajo hogar, elija las **configuraciones del Secure Desktop**.El control **permite las aplicaciones de correo electrónico para trabajar transparente**, y configura las otras configuraciones para adaptarse a su entorno.El tecleo **aplica todos**.**La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los
cambios.



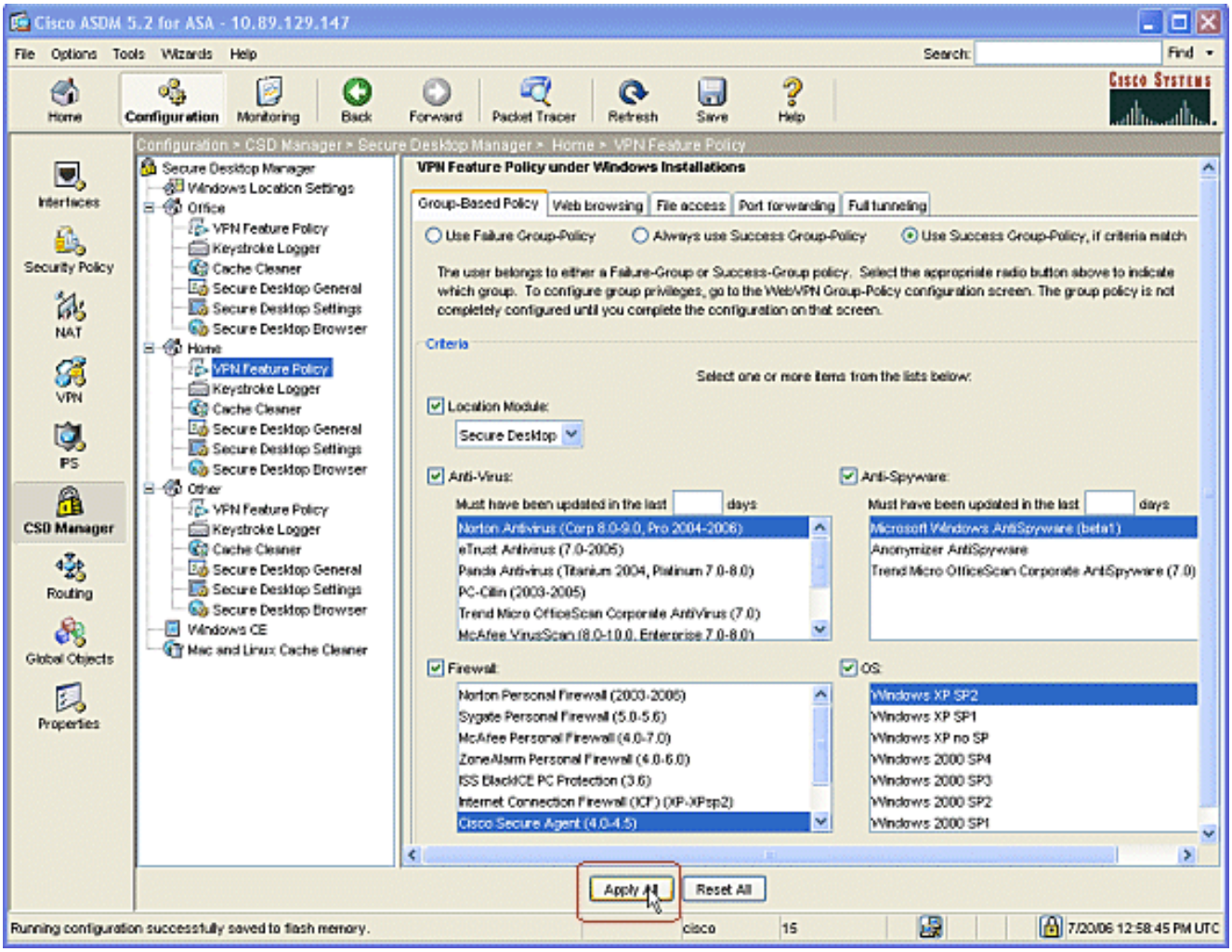
Características de la ubicación de Windows de la configuración

Configure la directiva de la característica VPN para cada uno de las ubicaciones que usted creó.

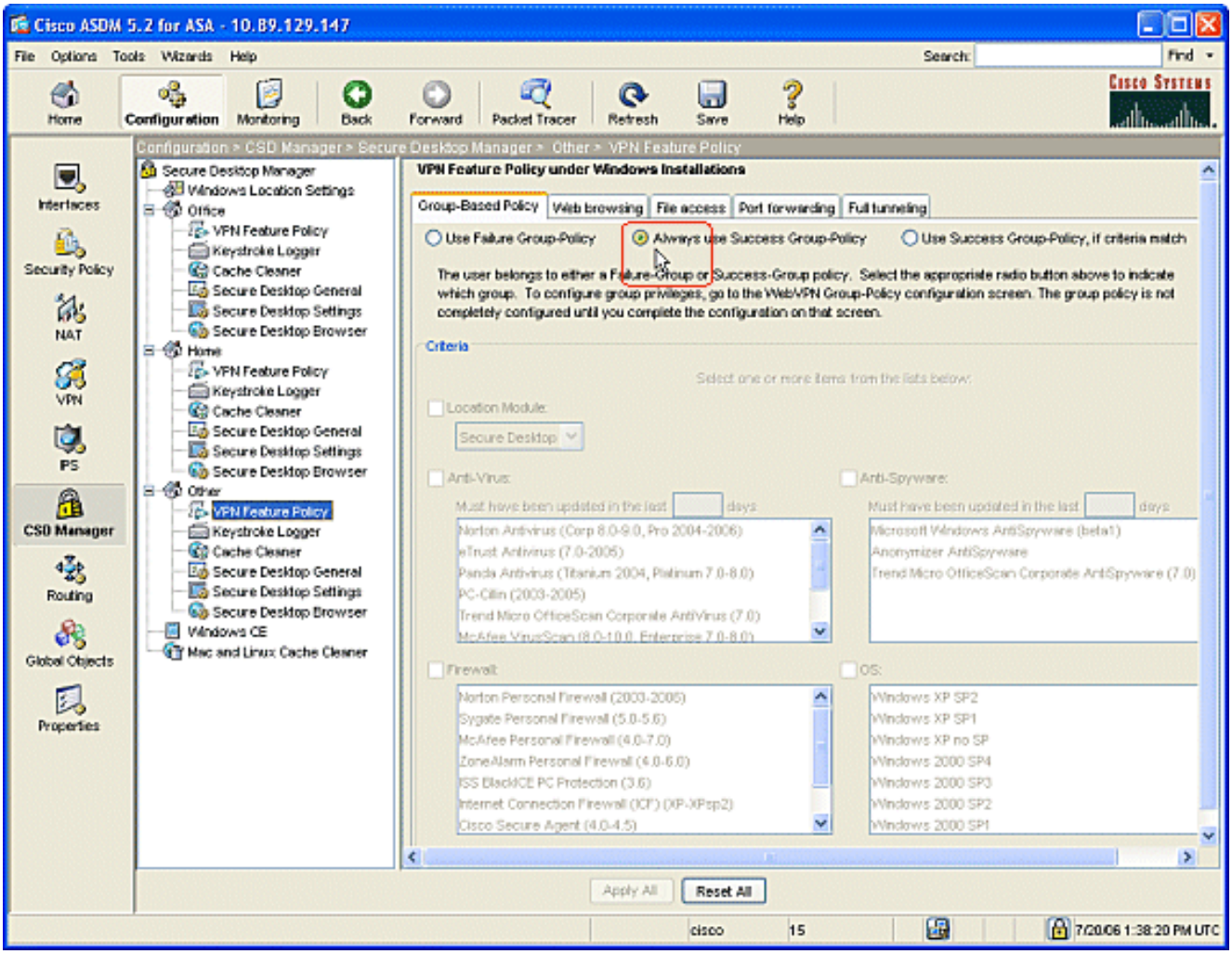
1. En el SCR_INVALID, el clickOffice, y entonces hace clic la **directiva de la característica VPN**.
2. Haga clic la lengueta **basada en el grupo de la directiva**.Haga clic **siempre el** botón de radio de la Grupo-**directiva del éxito del uso**.Haga clic **exploración de la Web la** lengueta, y marque el botón de radio **siempre habilitado**.Siga el mismo procedimiento para la **expedición del acceso al archivo, del puerto**, y las lengüetas **completas del Tunelización**.El tecleo **aplica todos**.**La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los cambios.



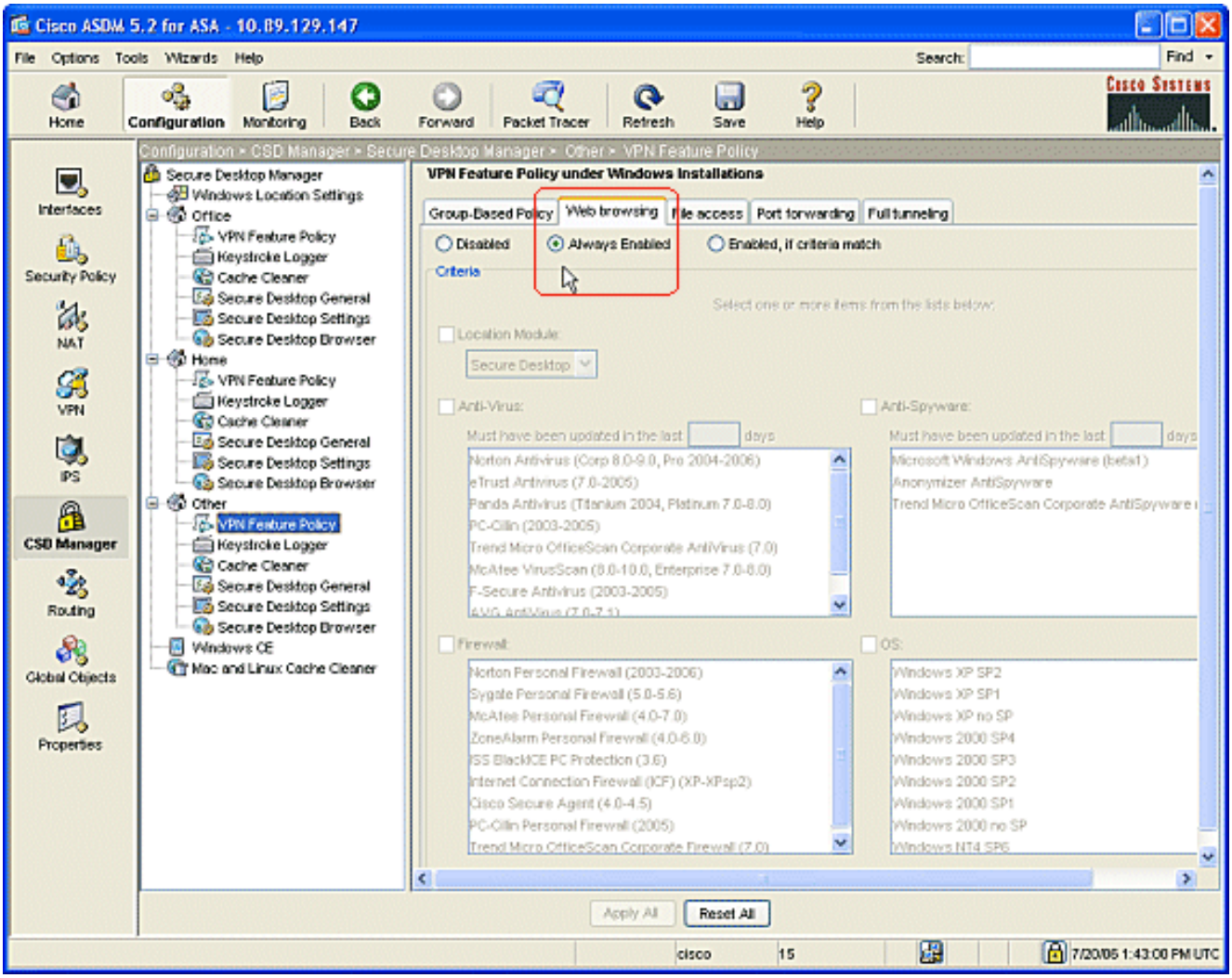
3. Para los usuarios caseros, cada sociedad puede requerir las directivas específicas antes de que se permita el acceso. En el SCR_INVALID, haga clic **a casa**, y haga clic la **directiva de la característica VPN**.Haga clic la lengueta **basada en el grupo de la directiva**.Haga clic el botón de radio de la Grupo-**directiva del éxito del uso** si los criterios preconfigurados hacen juego, por ejemplo una clave de registro específica, el nombre del archivo sabido, o el certificado digital.Marque el checkbox del **módulo del** theLocation y elija el **Secure Desktop**.Elija el **contra virus, el Anti-Spyware, el Firewall**, y las áreas **OS** de acuerdo con su política de seguridad de la compañía. No se permitirá a los usuarios caseros sobre la red a menos que sus ordenadores cumplan sus criterios configurados.



4. En el SCR_INVALID, haga clic **otro** y haga clic la **directiva de la característica VPN**.Haga clic la lengueta **basada en el grupo de la directiva**.Haga clic **siempre el** botón de radio de la Grupo-**directiva del éxito del uso**.



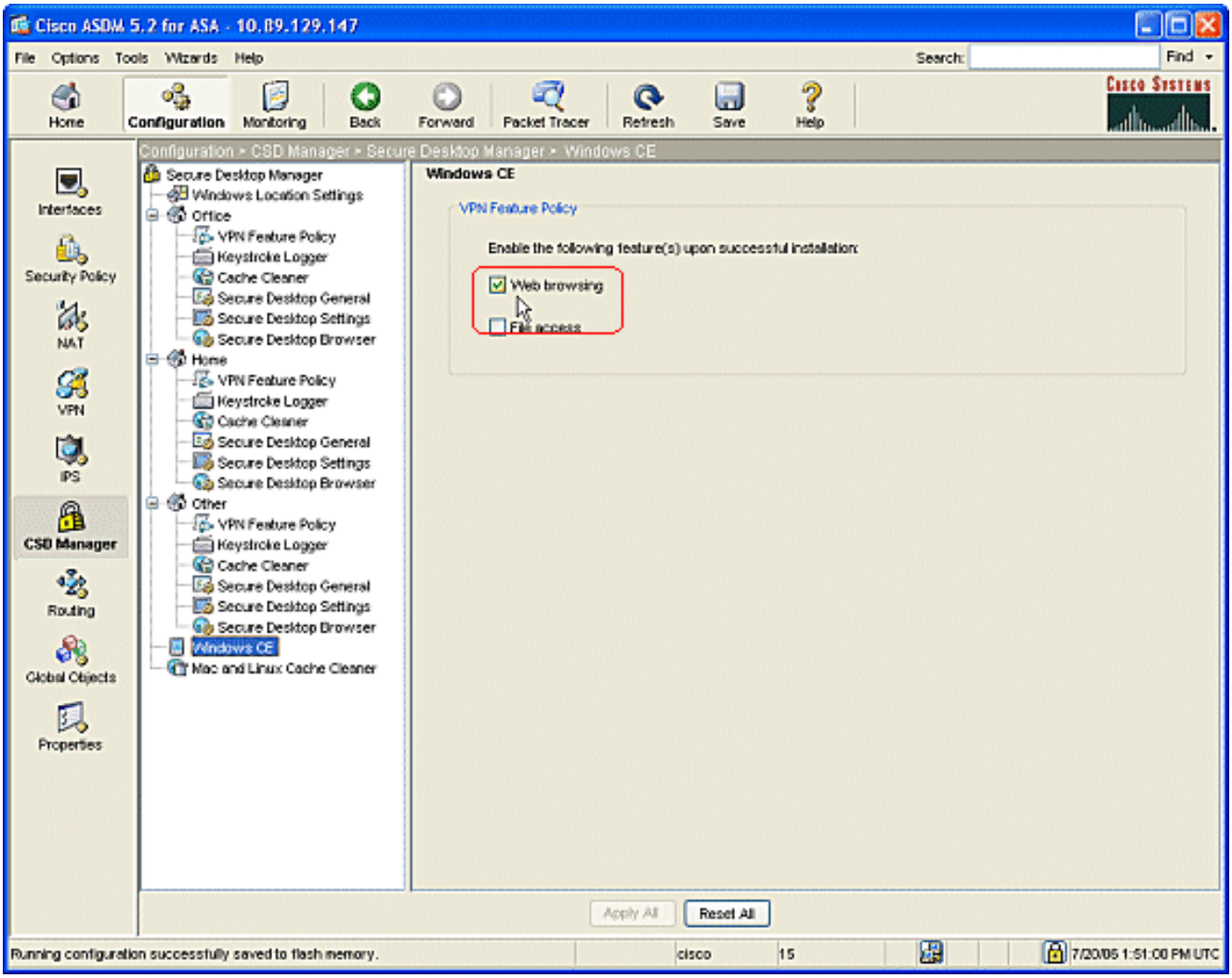
5. Para los clientes en esta ubicación de la **directiva de la característica VPN**, haga clic **exploración de la Web la** lengueta, y haga clic el dial de radio **siempre habilitado**.Haga clic la lengueta del **acceso al archivo**, y haga clic el botón de radio de la **neutralización**.Relance el paso con la **expedición del puerto** y las lenguetas **completas del Tunelización**.El tecleo **aplica todos**.**La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los cambios.



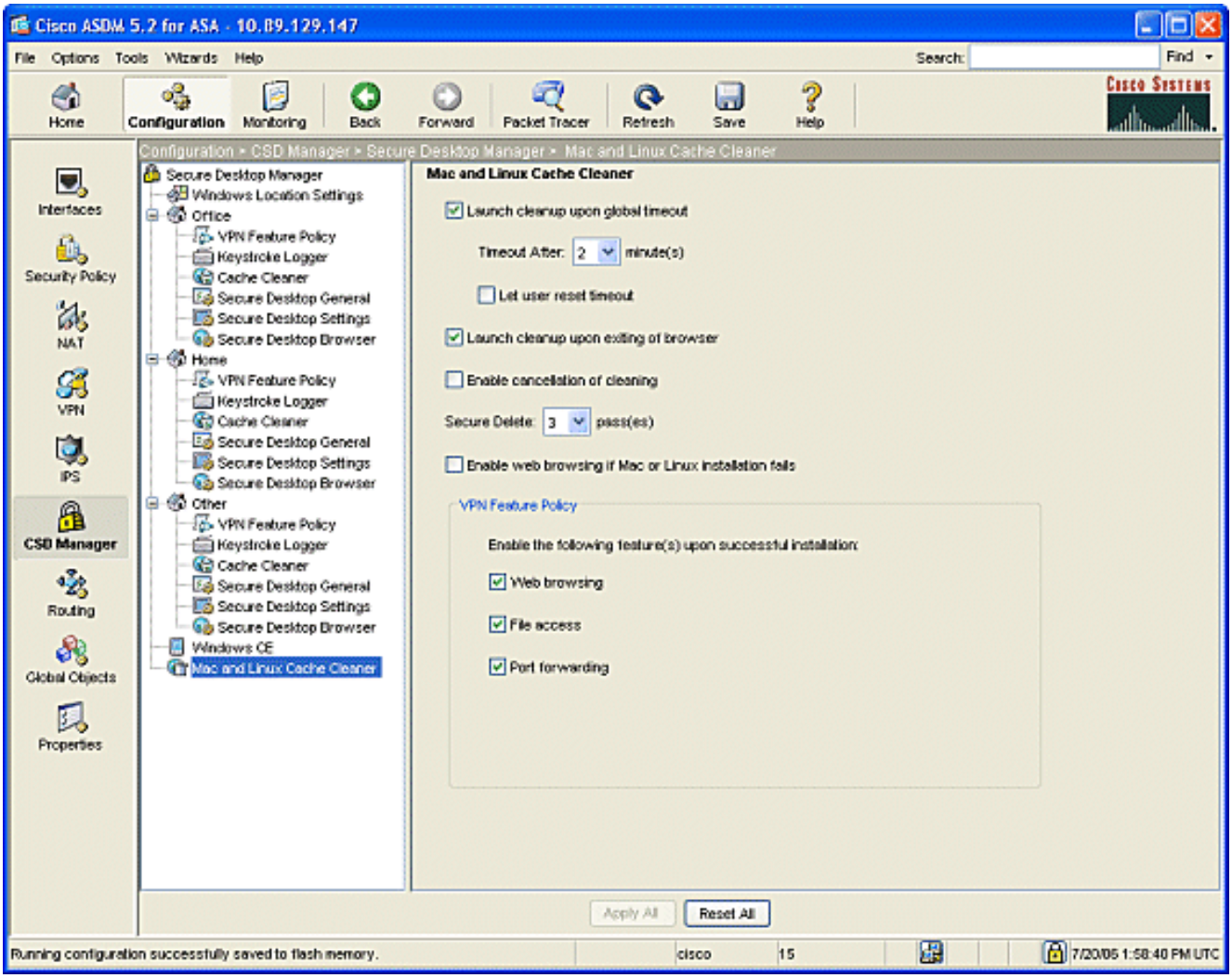
Configuraciones optativas para Windows CE, Macintosh, y los clientes de Linux

Estas configuraciones son opcionales.

1. Si usted elige **Windows CE del** SCR_INVALID, marque **exploración de la Web la** casilla de verificación.



2. Si usted elige el **mac y el producto de limpieza de discos del caché de Linux del** SCR_INVALID, marque la **limpieza del lanzamiento sobre el** dial de la radio del **tiempo de espera global agotado**.Cambie el descanso a su especificación.Bajo área de **directiva de la característica del** theVPN, marque los diales de la radio de la **expedición exploración de la Web, del acceso al archivo**, y del **puerto** para estos clientes.



3. Si usted elige Windows CE o el mac y el producto de limpieza de discos del caché de Linux, el tecleo **aplica todos**.
4. **La salvaguardia del** tecleo, y entonces hace clic **sí** para validar los cambios.

Configurar

Configuración

Esta configuración refleja el ASDM de los cambios hecho para habilitar el CSD: La mayor parte de las configuraciones CSD se mantienen un archivo distinto en el flash.

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
```

Verificación

Utilice esta sección para confirmar que sus configuraciones para el clientless SSL VPN, el cliente “liviano” SSL VPN, o (SVC) del cliente VPN SSL están actuando correctamente.

Pruebe el CSD con un PC que se ha configurado con las diversas ubicaciones de Windows. Cada prueba debe proporcionar un diverso acceso de acuerdo con las directivas que usted ha configurado en el ejemplo antedicho.

Usted puede cambiar el número del puerto y la interfaz donde Cisco ASA está atentas las conexiones WebVPN.

- El puerto predeterminado es 443. Si usted utiliza el puerto predeterminado, el acceso es **dirección IP de https://ASA**.
- El uso de un diverso puerto cambia el acceso a la **dirección IP de https://ASA: newportnumber**.

Comandos

Varios **comandos show se asocian a** WebVPN. Puede ejecutar estos comandos en command-line interface (CLI) para mostrar las estadísticas y otra información. Para ver el uso de los **comandos show** detalladamente, refiera a verificar la configuración del WebVPN.

Nota: La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Si usted tiene problemas con el cliente remoto, marque éstos:

1. ¿Estallido-UPS, las Javas, y/o ActiveX se habilitan en el buscador Web? Éstos pueden necesitar ser habilitado dependiendo del tipo de conexión VPN SSL funcionando.
2. El cliente debe validar los Certificados digitales presentados al inicio de la sesión.

Comandos

Varios **comandos debug se asocian a** WebVPN. Para información detallada sobre estos comandos, refiérase con los comandos Debug del WebVPN.

Nota: El uso de los **comandos debug** puede afectar negativamente su dispositivo de Cisco. Antes de que utilice los **comandos debug**, consulte Información Importante sobre los Comandos Debug.

Información Relacionada

- Dispositivos de seguridad adaptable Cisco ASA de la serie 5500
- Ejemplo de Configuración de ASA con WebVPN y Single Sign-on con ASDM y NTLMv1
- Soporte Técnico y Documentación - Cisco Systems