Esempio di configurazione di Cisco Secure Desktop (CSD 3.1.x) su ASA 7.2.x per Windows con ASDM

Sommario

Introduzione

Cisco Secure Desktop (CSD) estende la sicurezza della tecnologia VPN SSL. CSD fornisce una partizione separata sulla workstation di un utente per l'attività della sessione. Quest'area di vaulting viene crittografata durante le sessioni e completamente rimossa al termine di una sessione VPN SSL. Windows può essere configurato con tutti i vantaggi di sicurezza di CSD. Macintosh, Linux e Windows CE hanno accesso solo alle funzioni Cache Cleaner, Web Browsing e File Access. CSD può essere configurato per i dispositivi Windows, Macintosh, Windows CE e Linux sulle seguenti piattaforme:

- Cisco Adaptive Security Appliance (ASA) serie 5500
- Router Cisco con software Cisco IOS® versione 12.4(6)T e successive
- Cisco VPN serie 3000 concentrator versione 4.7 e successive

- Cisco WebVPN Module sui router Catalyst serie 6500 e 7600

Nota: CSD release 3.3 consente ora di configurare Cisco Secure Desktop per l'esecuzione su computer remoti che eseguono Microsoft Windows Vista. In precedenza, Cisco Secure Desktop era limitato ai computer che eseguivano Windows XP o 2000. Per ulteriori informazioni, consultare la sezione Miglioramento delle nuove funzionalità - Secure Desktop on Vista nelle Note sulla versione di Cisco Secure Desktop, versione 3.3.

Questo esempio riguarda principalmente l'installazione e la configurazione di CSD sull'appliance ASA serie 5500 per client Windows. Sono state aggiunte configurazioni opzionali per i client Windows CE, Mac e Linux da completare.

CSD viene utilizzato in combinazione con la tecnologia VPN SSL (Client less SSL VPN, Thin-Client SSL VPN o SSL VPN Client (SVC)). CSD aggiunge valore alle sessioni sicure della tecnologia VPN SSL.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

Requisiti per il dispositivo ASA

- Cisco CSD release 3.1 o successive
- Software Cisco ASA versione 7.1.1 o successive
- Cisco Adaptive Security Device Manager (ASDM) versione 5.1.1 o successive**Nota:** CSD versione 3.2 supporta solo ASA versione 8.x**Nota:** per consentire all'ASDM di configurare l'appliance ASA, consultare il documento sull'autorizzazione dell'accesso HTTPS per ASDM.

Requisiti per i computer client

- I client remoti devono disporre di privilegi amministrativi locali; non è obbligatorio, ma è altamente suggerito.
- I client remoti devono disporre di Java Runtime Environment (JRE) versione 1.4 o successiva.
- Browser client remoti: Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 o Firefox 1.0
- Cookie attivati e popup consentiti su client remoti

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi. Gli indirizzi IP utilizzati in questa configurazione sono

gli indirizzi RFC 1918. Questi indirizzi IP non sono validi su Internet e devono essere utilizzati solo in un ambiente di prova.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

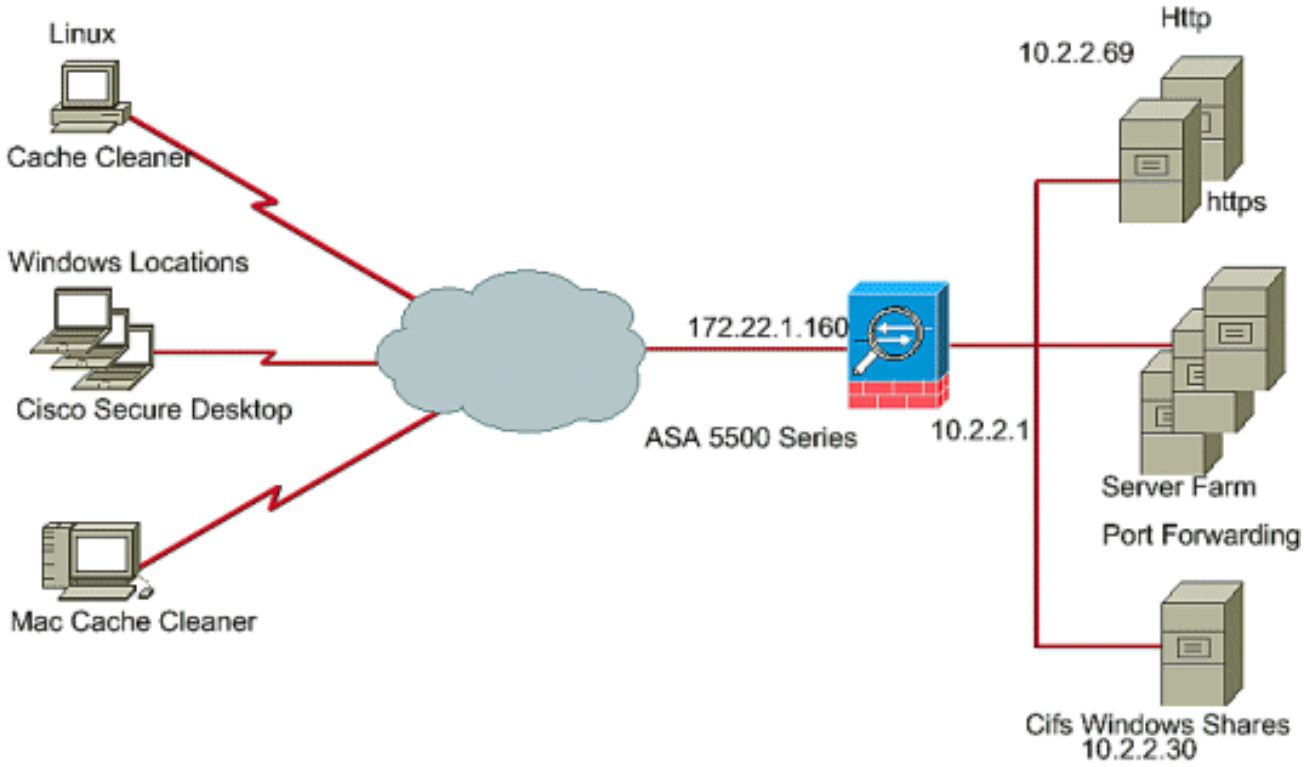
Premesse

CSD opera con la tecnologia VPN SSL, quindi il client senza client, thin client o SVC deve essere attivato prima della configurazione di CSD.

Esempio di rete

Èpossibile configurare percorsi Windows diversi con gli aspetti di protezione completa di CSD. Macintosh, Linux e Windows CE hanno accesso solo a Cache Cleaner e/o alla navigazione sul Web e all'accesso ai file.

Nel documento viene usata questa impostazione di rete:



Configurazione di CSD sull'appliance ASA per client Windows

Configurare CSD sull'appliance ASA per client Windows in cinque passaggi principali:

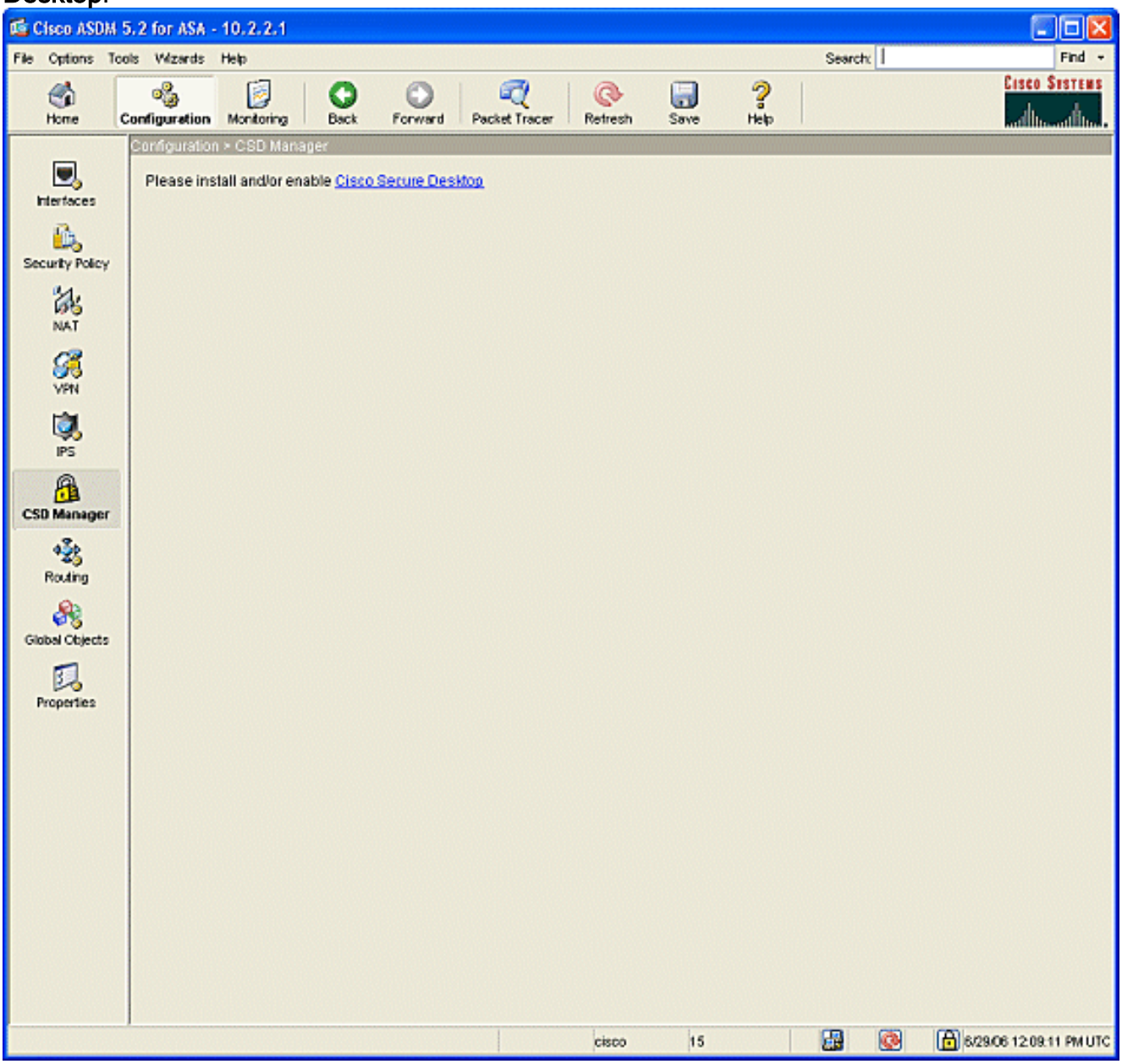
- Ottenere, installare e abilitare il software CSD sull'appliance Cisco ASA.
- Definire i percorsi di Windows.
- Definire l'identificazione del percorso di Windows.
- Configurare i moduli percorsi Windows.

- Configurare le funzionalità di posizione di Windows.
- Configurazione opzionale per client Windows CE, Macintosh e Linux.

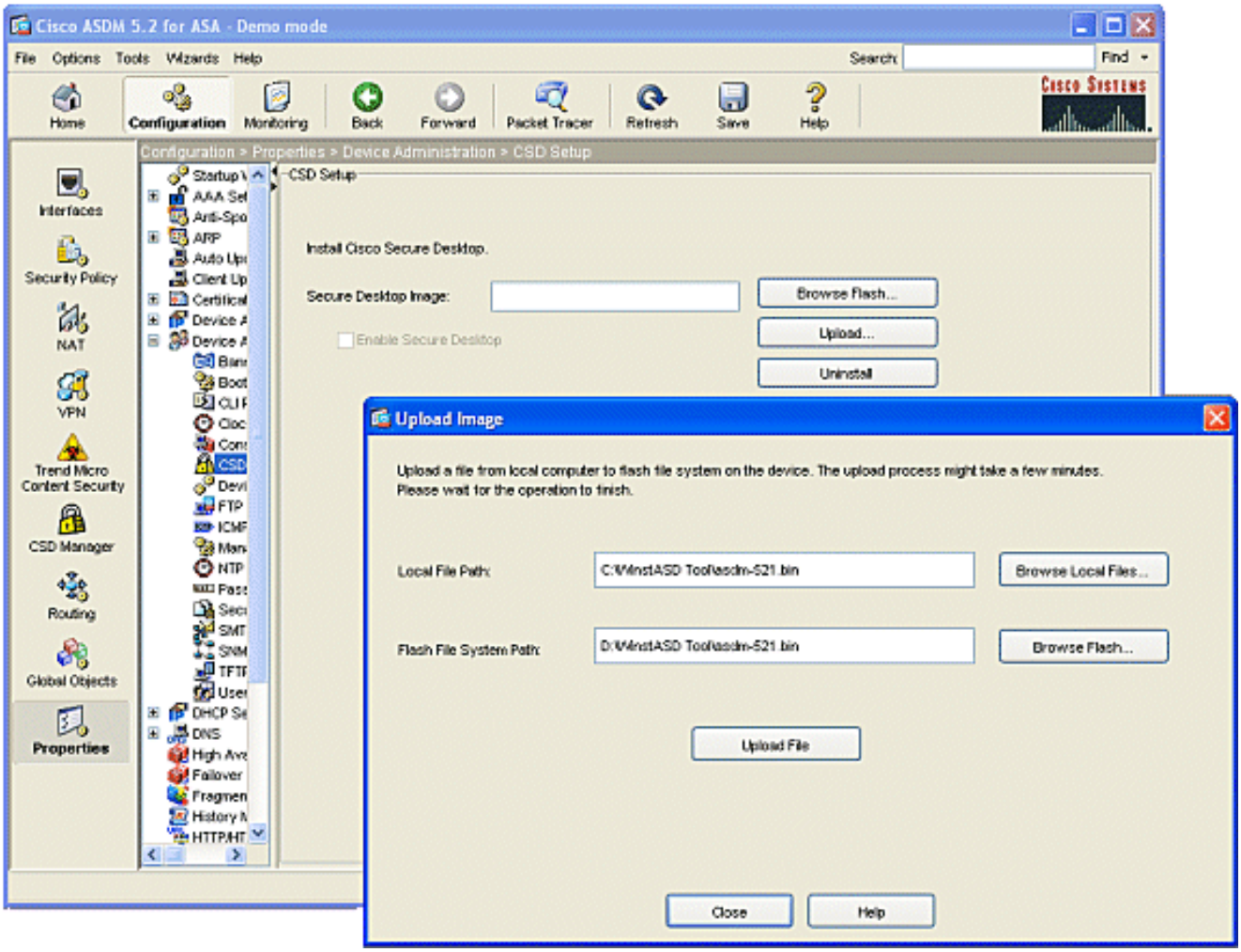
Ottenere, installare e abilitare il software CSD

Completare questa procedura per ottenere, installare e abilitare il software CSD sull'appliance Cisco ASA.

1. Scaricare il software CSD securedesktop-asa*.pkg e i file Leggimi nella stazione di gestione dal sito Web di download del software Cisco.
2. Accedere ad ASDM e fare clic sul pulsante **Configuration** (Configurazione). Dal menu a sinistra, fare clic sul pulsante **CSD Manager**, quindi fare clic sul collegamento **Cisco Secure Desktop**.



3. Fare clic su **Upload** per visualizzare la finestra Upload Image (Carica immagine).Immettere il percorso del nuovo file .pkg sulla stazione di gestione o fare clic su **Sfoglia file locali** per individuare il file.Immettere il percorso su flash in cui inserire il file o fare clic su **Sfoglia Flash**.Fare clic su **Upload File**.Quando richiesto, fate clic su **OK > Chiudi (Close) > OK**.

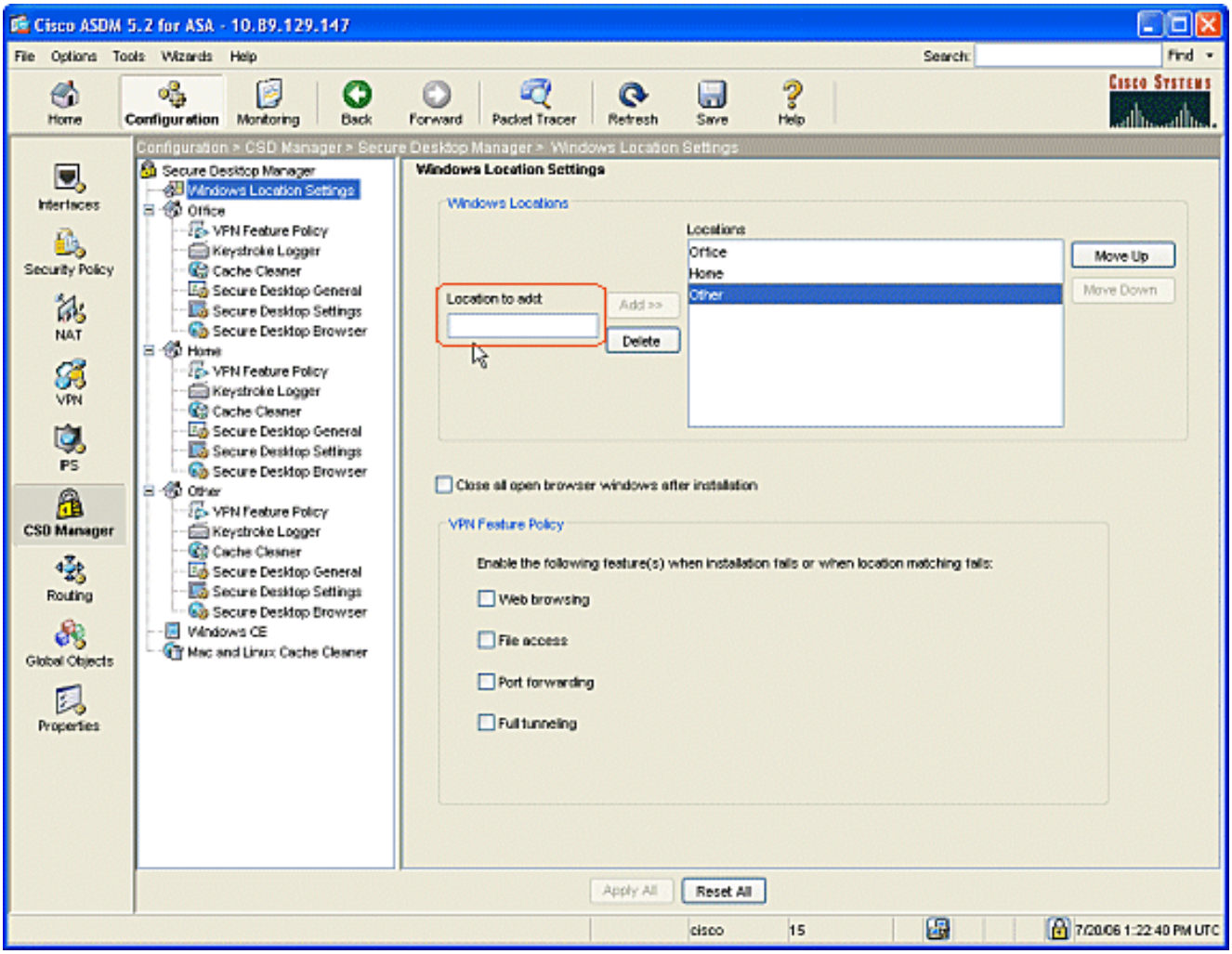


4. Una volta caricata l'immagine client per la memoria flash, selezionare la casella di controllo **Abilita client VPN SSL** e quindi fare clic su **Applica**.
5. Fare clic su **Salva** e quindi su **Sì** per accettare le modifiche.

Definisci percorsi Windows

Completare la procedura seguente per definire le posizioni di Windows.

1. Fare clic sul pulsante **Configuration** (Configurazione).
2. Dal menu a sinistra, fare clic sul pulsante **CSD Manager**, quindi fare clic sul collegamento **Cisco Secure Desktop**.
3. Nel riquadro di spostamento fare clic su **Impostazioni percorso di Windows**.
4. Digitare un nome di percorso nel campo Percorso da aggiungere e fare clic su **Aggiungi**.Prendere nota delle tre posizioni riportate nell'esempio: Office, Home e Altri.Office rappresenta le workstation che si trovano all'interno dei limiti di sicurezza dell'azienda.Home rappresenta gli utenti che lavorano da casa.Altro rappresenta un percorso diverso dai due percorsi
menzionati.

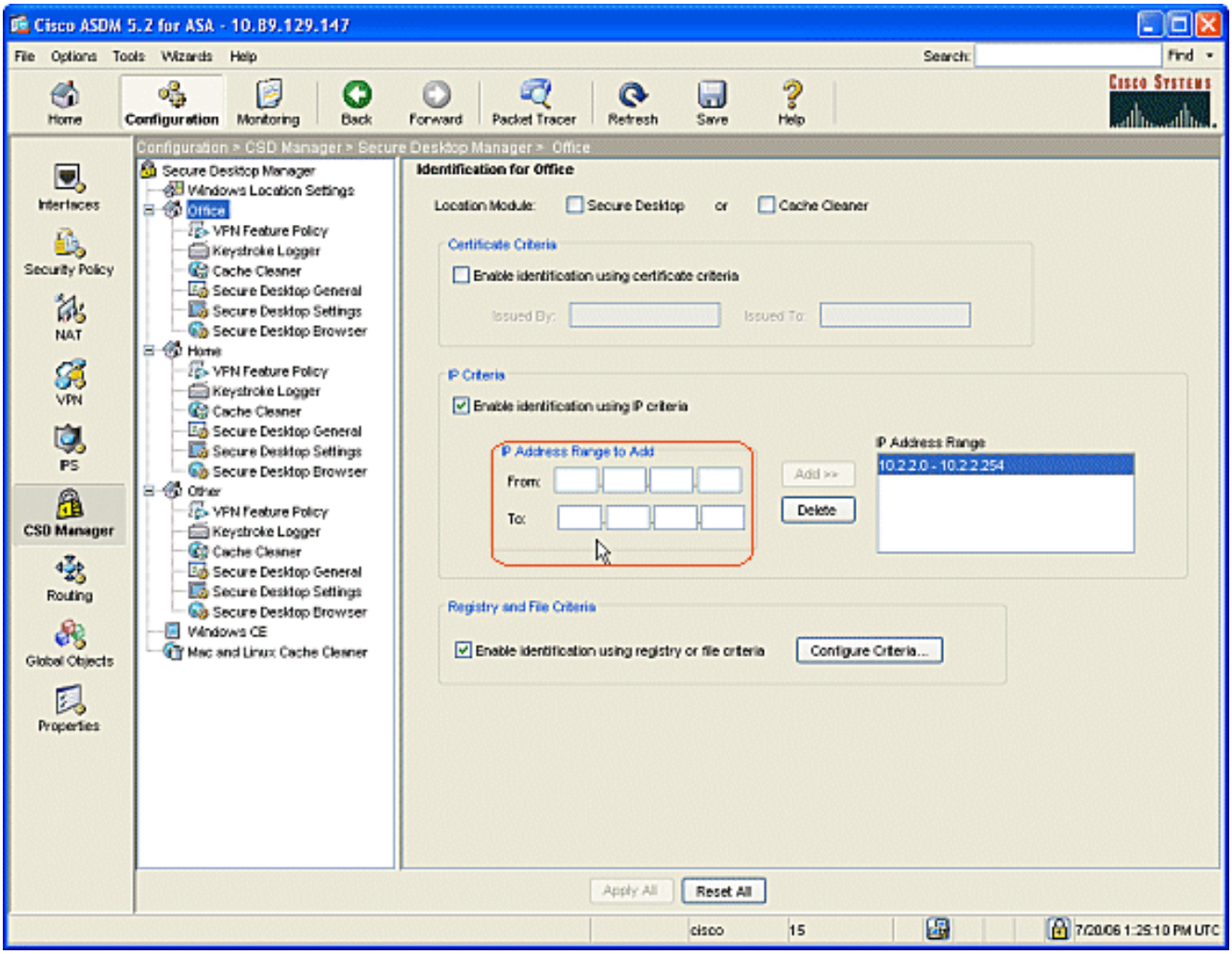


5. Èpossibile creare ubicazioni personalizzate in base al layout dell'architettura di rete per vendite, ospiti, partner e altri.
6. Durante la creazione dei percorsi di Windows, il riquadro di spostamento si espande con moduli configurabili per ogni nuovo percorso. Fare clic su **Applica tutto**.
7. Fare clic su **Salva** e quindi su **Sì** per accettare le modifiche.

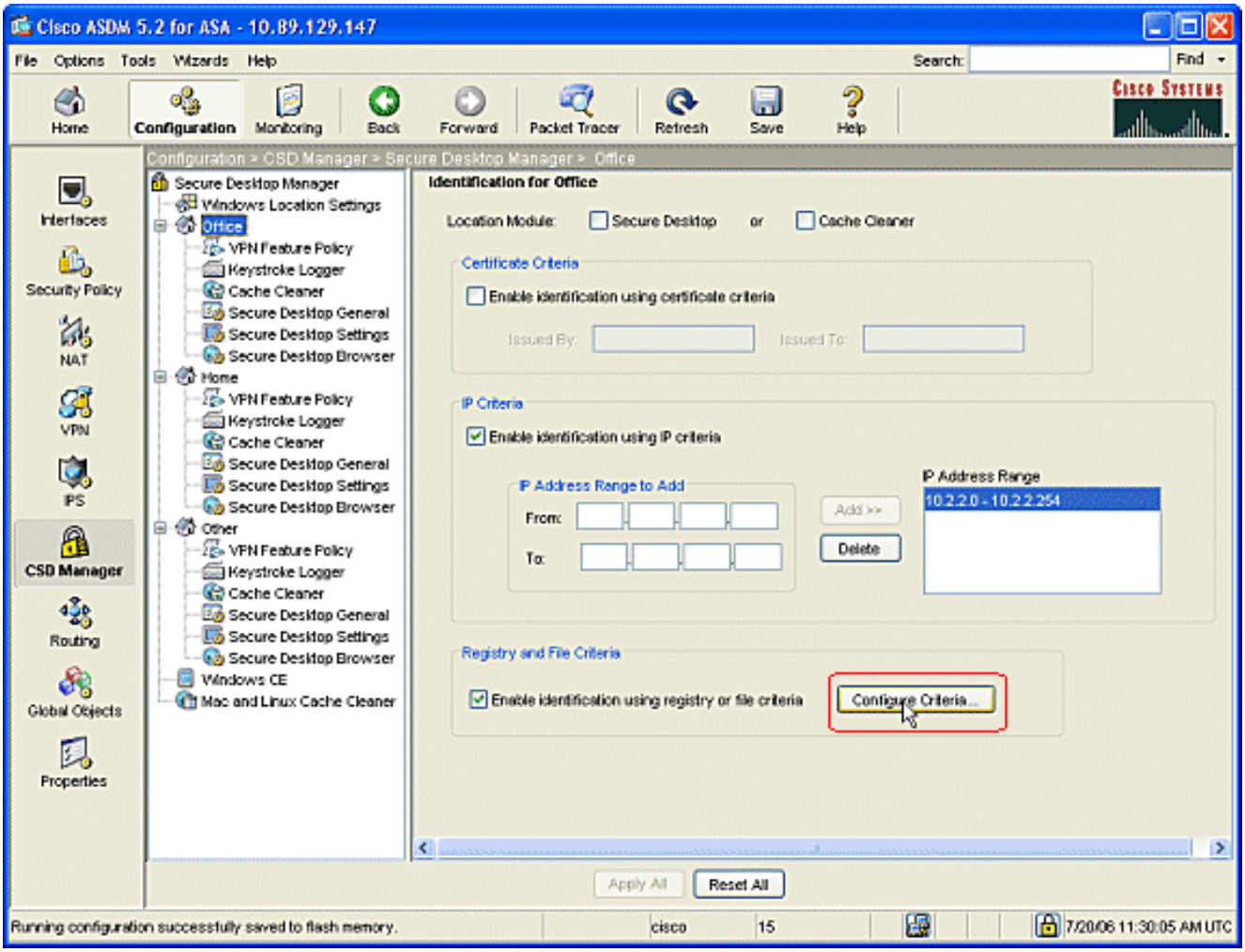
Identificazione percorso Windows

Completare la procedura seguente per definire l'identificazione del percorso di Windows.

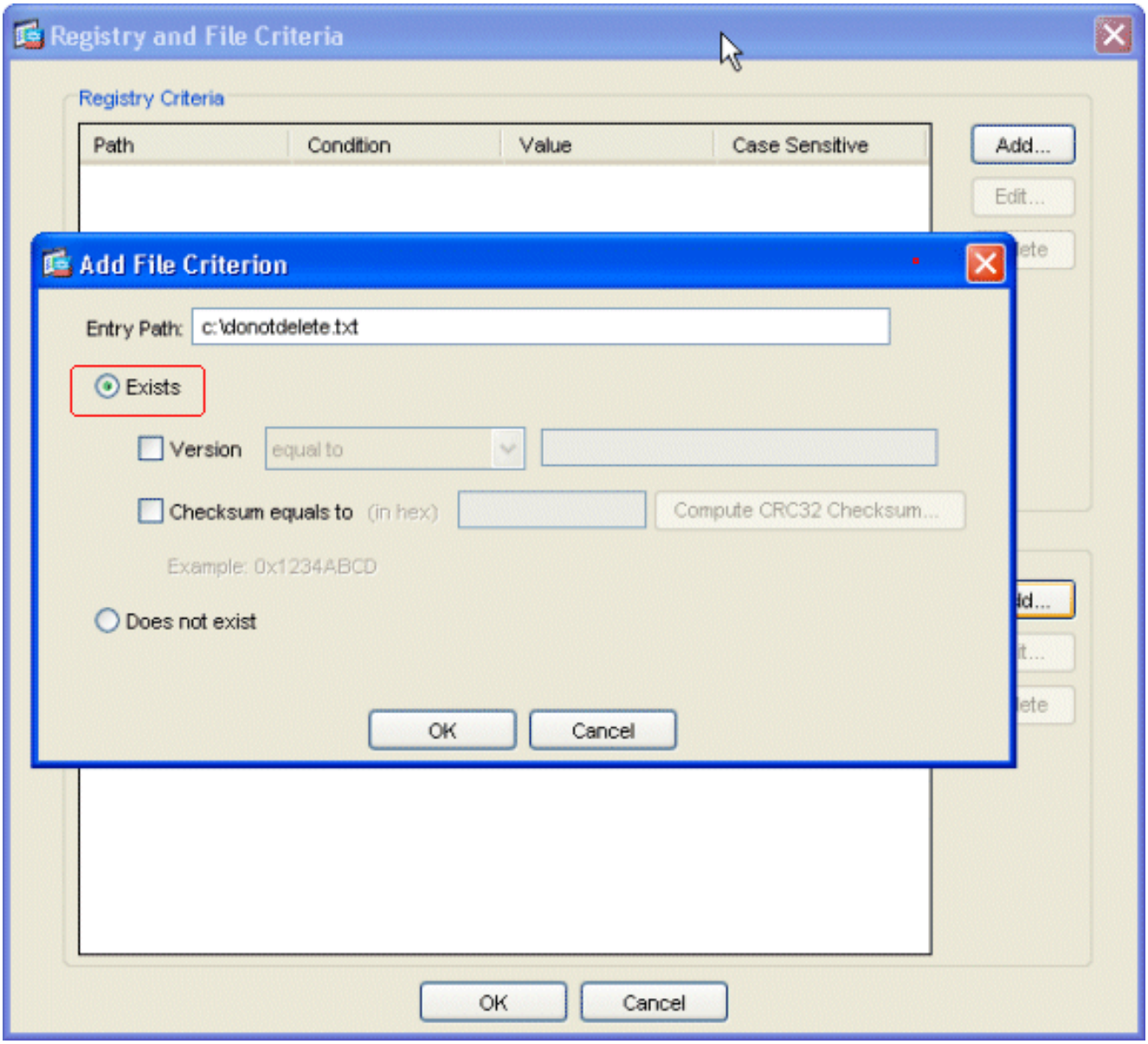
1. Identificare i percorsi creati in Definisci percorsi Windows.



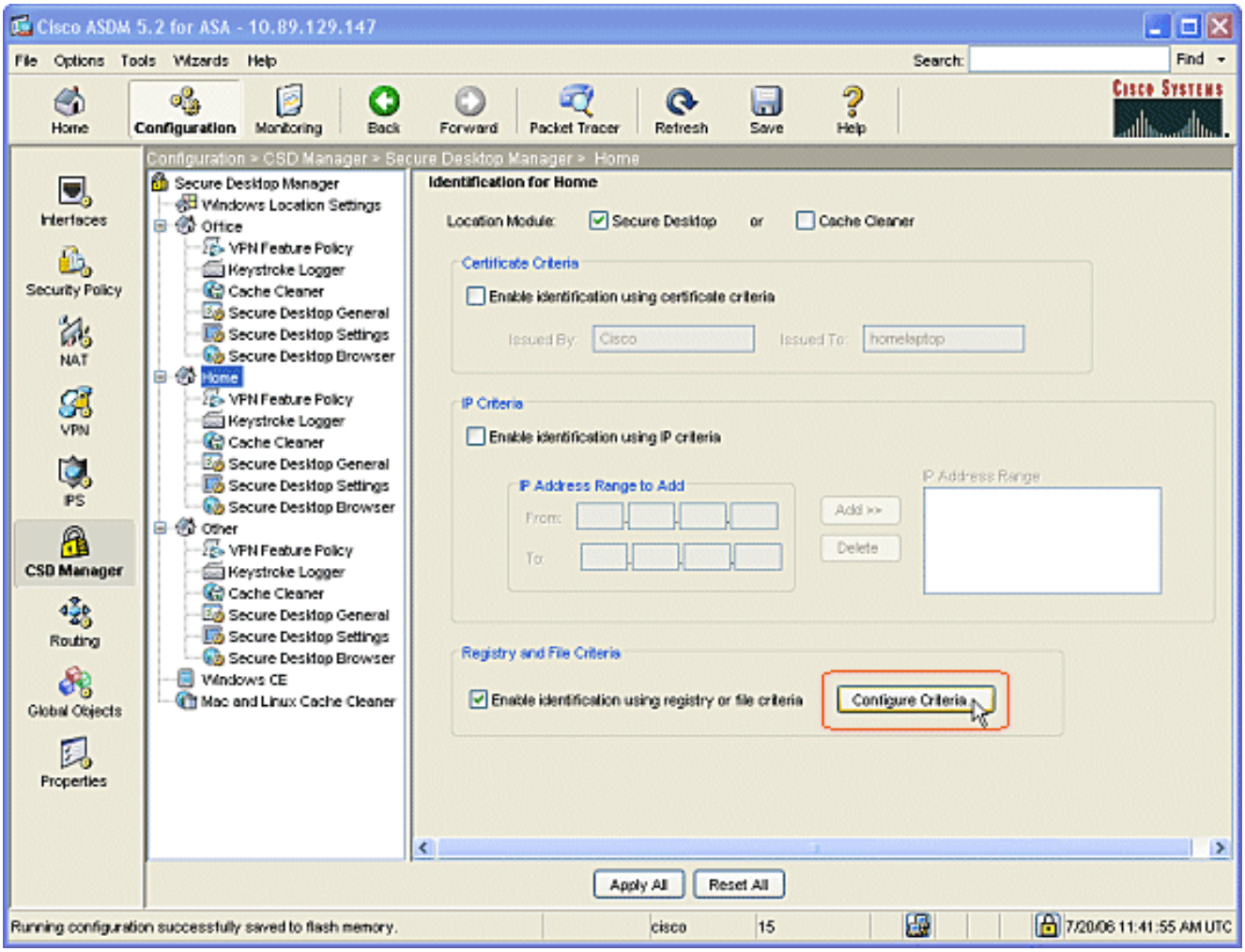
2. Per identificare il percorso di Office, fare clic su **Office** nel riquadro di spostamento.Deselezionare **Secure Desktop** and **Cache Cleaner** in quanto si tratta di computer interni.Selezionare **Abilita identificazione utilizzando criteri IP**.Immettere gli intervalli di indirizzi IP dei computer interni.Selezionare **Abilita identificazione utilizzando i criteri del Registro di sistema o del file**. Ciò consente di distinguere gli impiegati interni dagli ospiti occasionali della
rete.



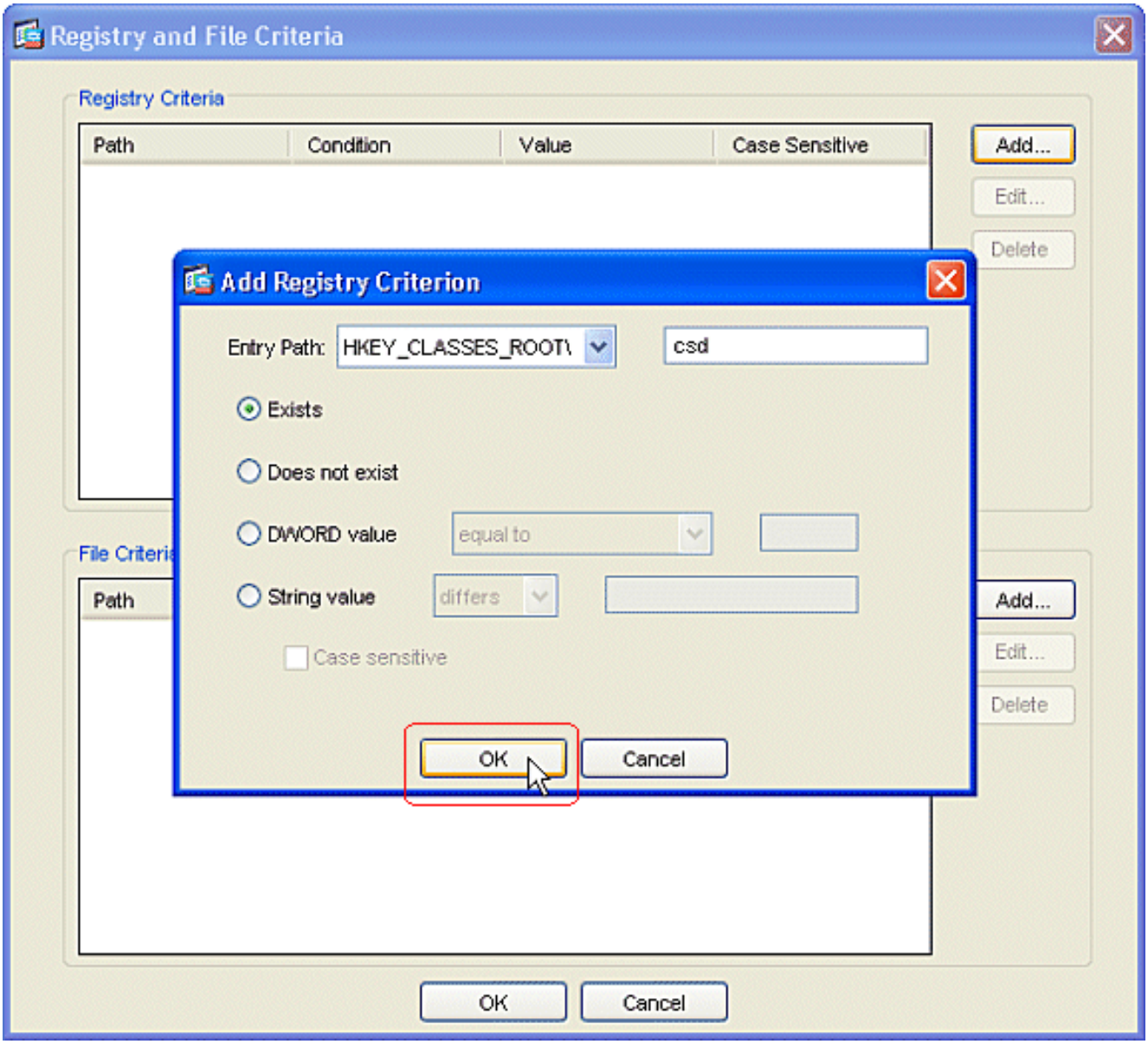
3. Fare clic su **Configura criteri**. Viene configurato un semplice esempio di file "DoNotDelete.txt". Questo file deve esistere nei computer Windows interni ed è semplicemente un segnaposto. È inoltre possibile configurare una chiave del Registro di sistema di Windows per identificare i computer dell'ufficio interno. Fare clic su **OK** nella finestra Aggiungi criterio file. Fare clic su **OK** nella finestra Criteri file e Registro di sistema.



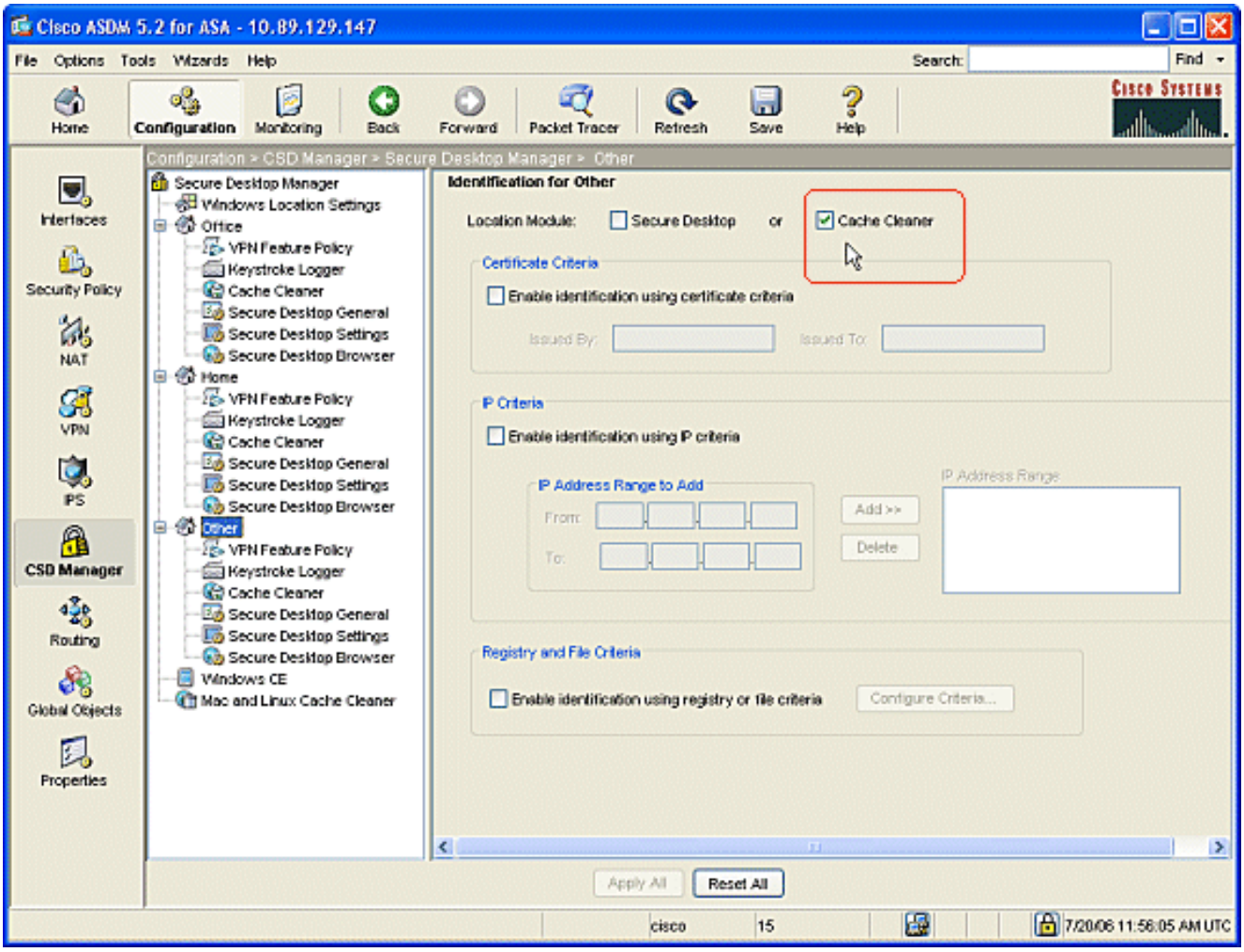
4. Fare clic su **Applica tutto** nella finestra Identificazione per Office. Fare clic su **Salva** e quindi su **Sì** per accettare le modifiche.
5. Per identificare la posizione Home, fare clic su **Home page** nel riquadro di navigazione.Selezionare **Abilita identificazione utilizzando i criteri del Registro di sistema o del file**.Fare clic su **Configura criteri**.



6. I client del computer di casa devono essere stati configurati con questa chiave del Registro di sistema da un amministratore. Fare clic su **OK** nella finestra Aggiungi criterio del Registro di sistema. Fare clic su **OK** nella finestra Criteri file e Registro di sistema.



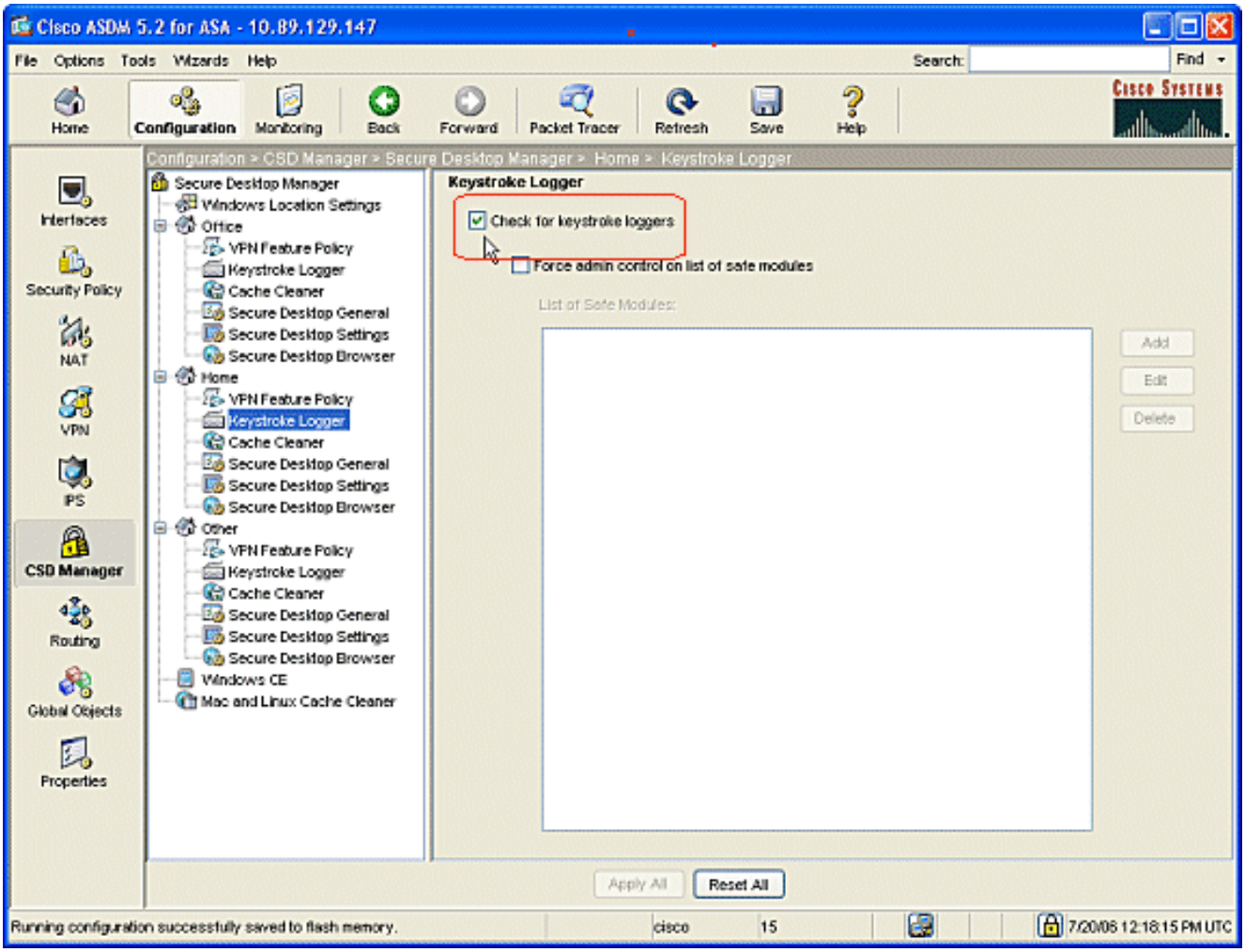
7. In Modulo posizione selezionare **Secure Desktop**. Fare clic su **Applica tutto** nella finestra Identificazione per la home page. Fare clic su **Salva** e quindi su **Sì** per accettare le modifiche.
8. Per identificare il percorso **Altro**, fare clic su **Altro** nel riquadro di spostamento.Selezionare solo la casella **Cache Cleaner** e deselezionare tutte le altre caselle.Fare clic su **Applica tutto** nella finestra Identificazione per altro.Fare clic su **Salva** e quindi su **Sì** per accettare le modifiche.



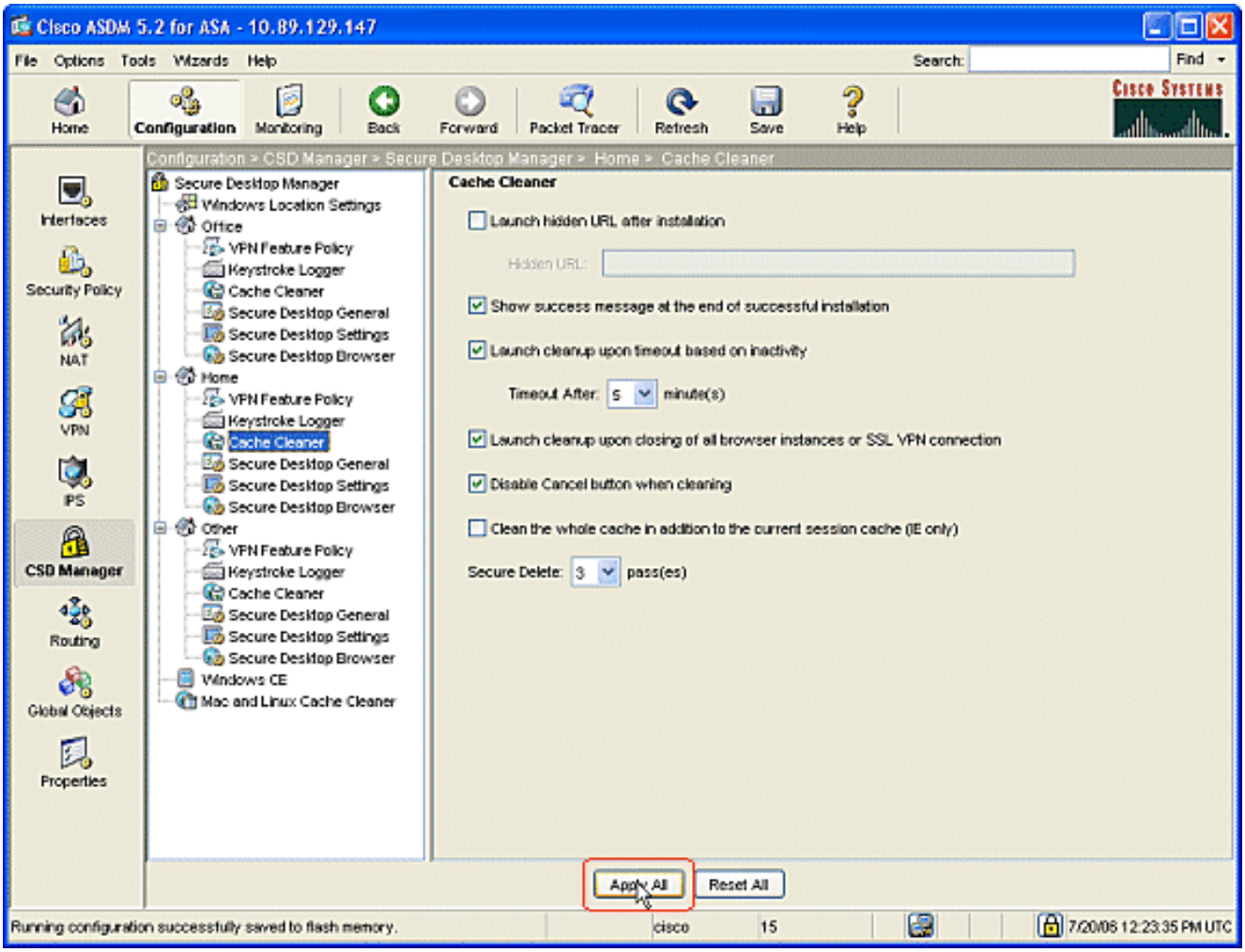
Configura Windows Location Module

Completare questi passaggi per configurare i moduli in ognuna delle tre posizioni create.

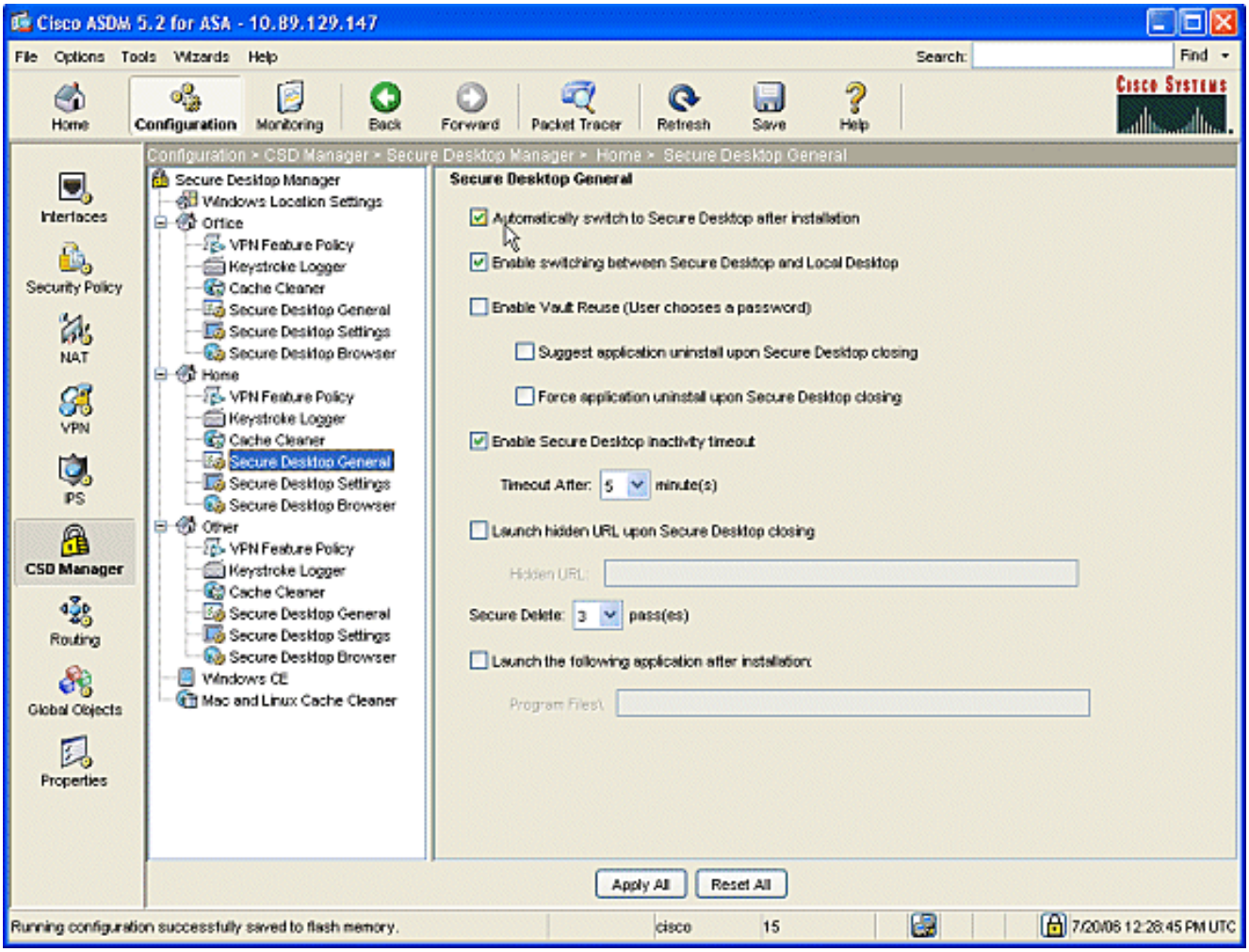
1. Per i client Office, non eseguire alcuna operazione poiché nella procedura precedente non sono stati scelti Secure Desktop e Cache Cleaner. L'applicazione ASDM consente di configurare Cache Cleaner anche se non è stato scelto in un passaggio precedente. Mantenere le impostazioni predefinite per i percorsi di Office.**Nota:** la policy sulle funzionalità VPN non viene discussa in questo passaggio, ma verrà discussa in un passaggio successivo per tutte le posizioni.
2. Per i client privati, fare clic su **Home page** e su **Registratore tasti** nel riquadro di navigazione.Nella finestra Registratore tasti, selezionare **Controlla registratori di tasti**.Fare clic su **Applica tutto** nella finestra Registratore tasti.Fare clic su **Salva** e quindi su **Sì** per accettare le
modifiche.



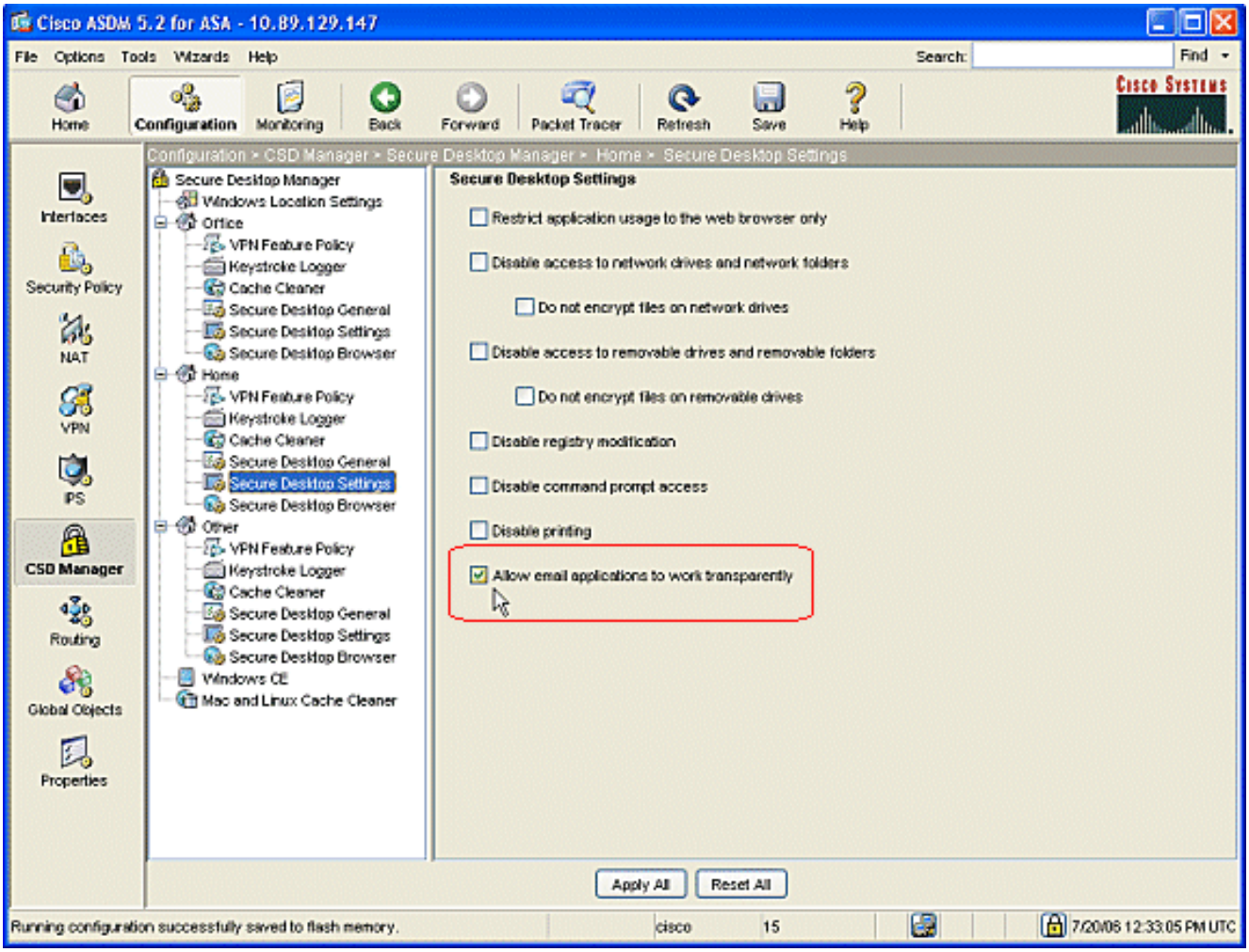
3. In Home, scegliere **Cache Cleaner** e i parametri che si adattano al proprio ambiente.



4. In Home (Principale), scegliere **Secure Desktop General** (Desktop sicuro) e i parametri adatti al proprio
ambiente.



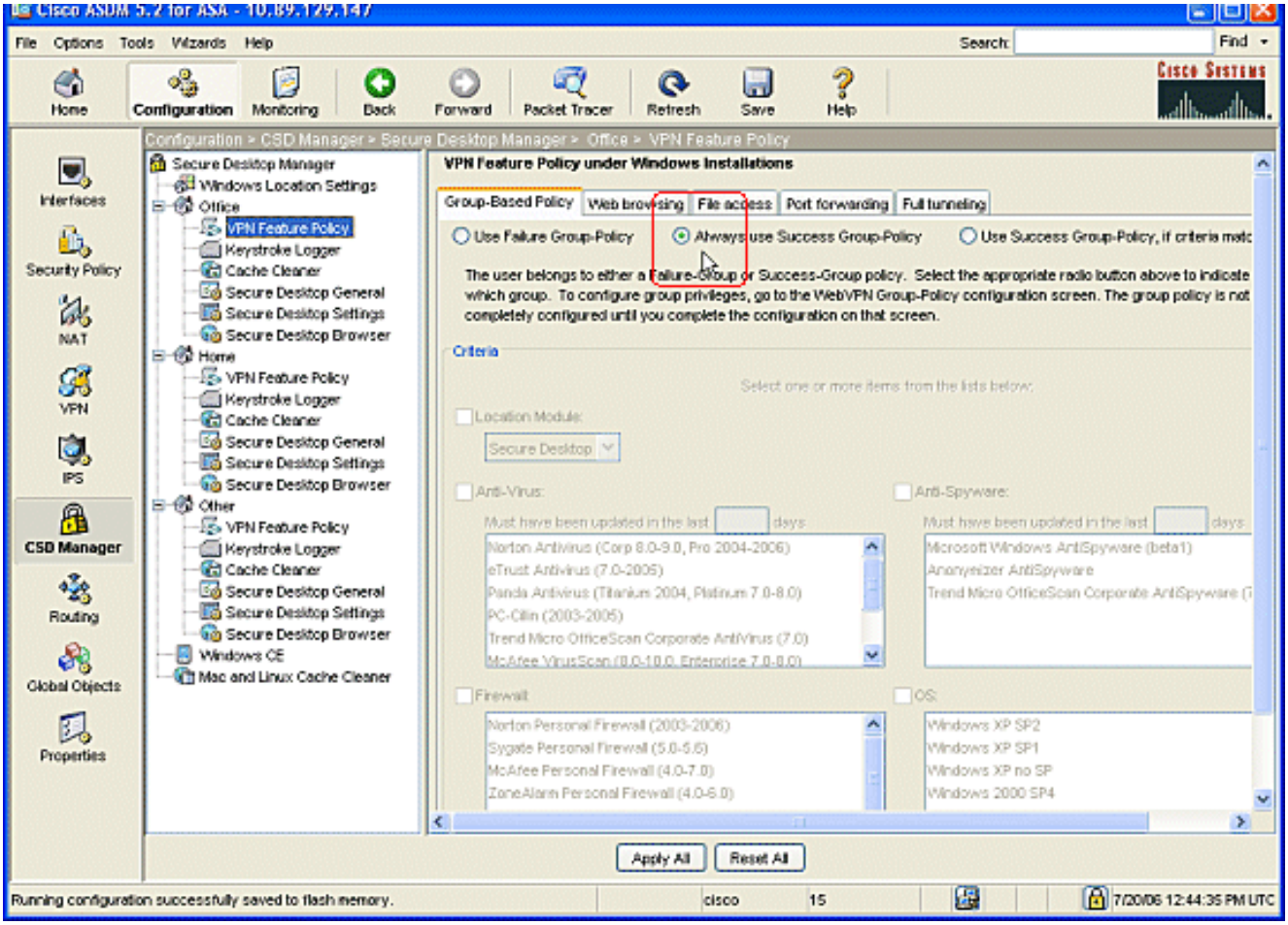
5. In Home, scegliere **Impostazioni desktop sicuro**.Selezionare **Consenti alle applicazioni di posta elettronica di funzionare in modo trasparente** e configurare le altre impostazioni in base al proprio ambiente.Fare clic su **Applica tutto**.Fare clic su **Salva** e quindi su **Sì** per accettare le
modifiche.



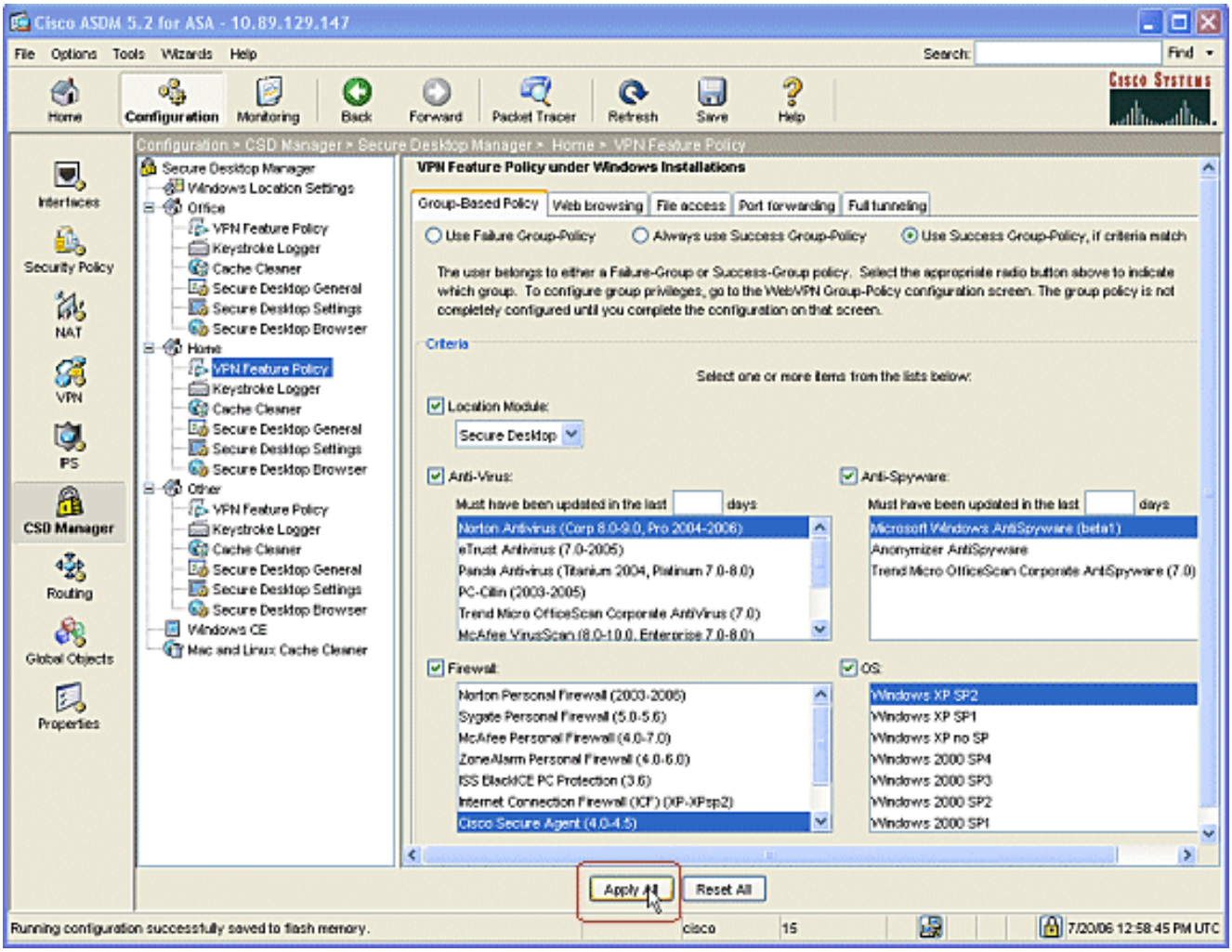
Configura funzionalità di posizione di Windows

Configurare i criteri delle funzionalità VPN per ogni percorso creato.

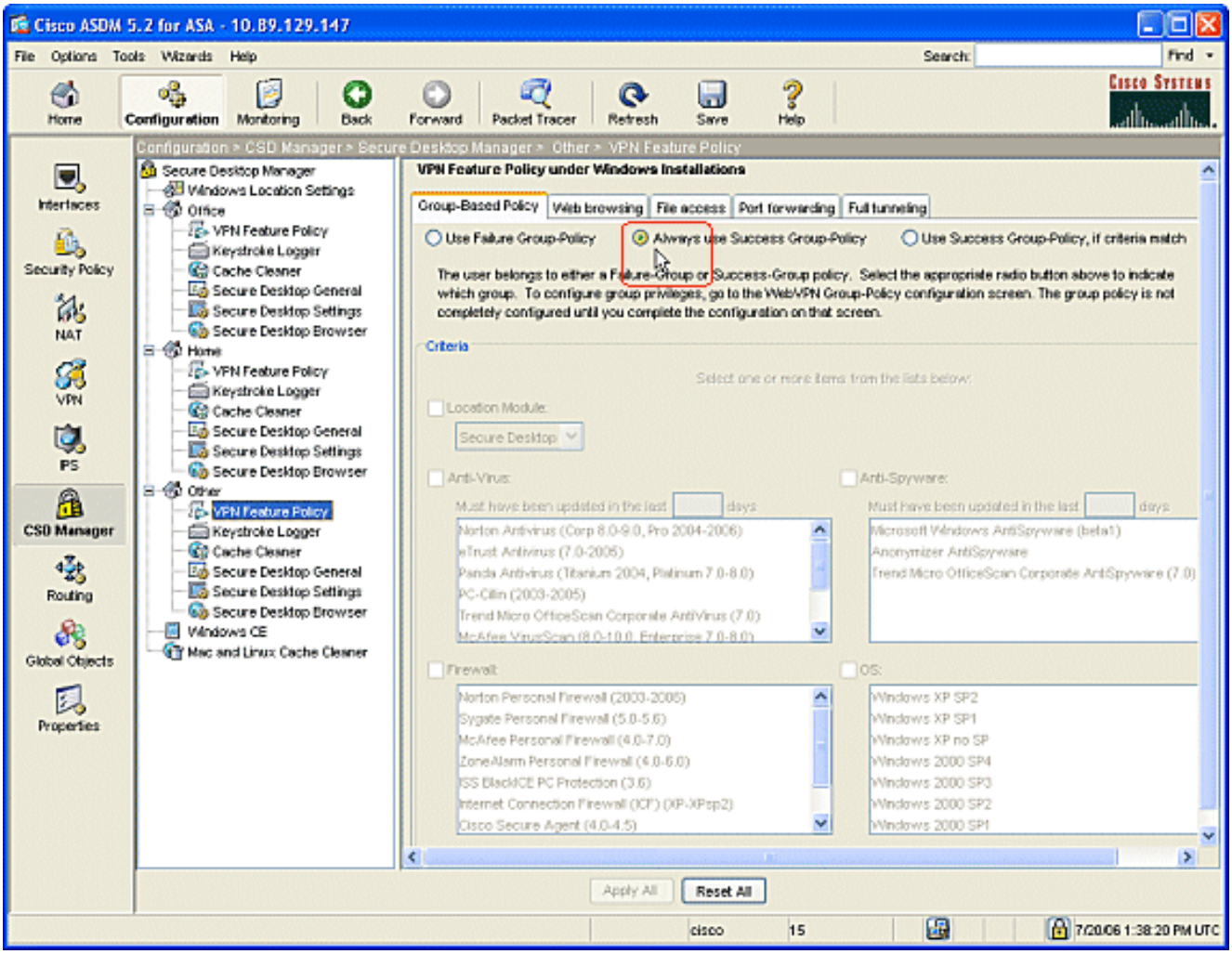
1. Nel riquadro di spostamento **fare clic su Office** e quindi su **Criteri funzionalità VPN**.
2. Fare clic sulla scheda **Criteri di gruppo**.Fare clic sul pulsante di opzione **Utilizza sempre criteri di gruppo riusciti**.Fare clic sulla scheda **Esplorazione Web** e selezionare il pulsante di opzione **Sempre abilitato**.Seguire la stessa procedura per le schede **Accesso file, Inoltro porta** e **Tunneling completo**.Fare clic su **Applica tutto**.Fare clic su **Salva** e quindi su **Sì** per accettare le
modifiche.



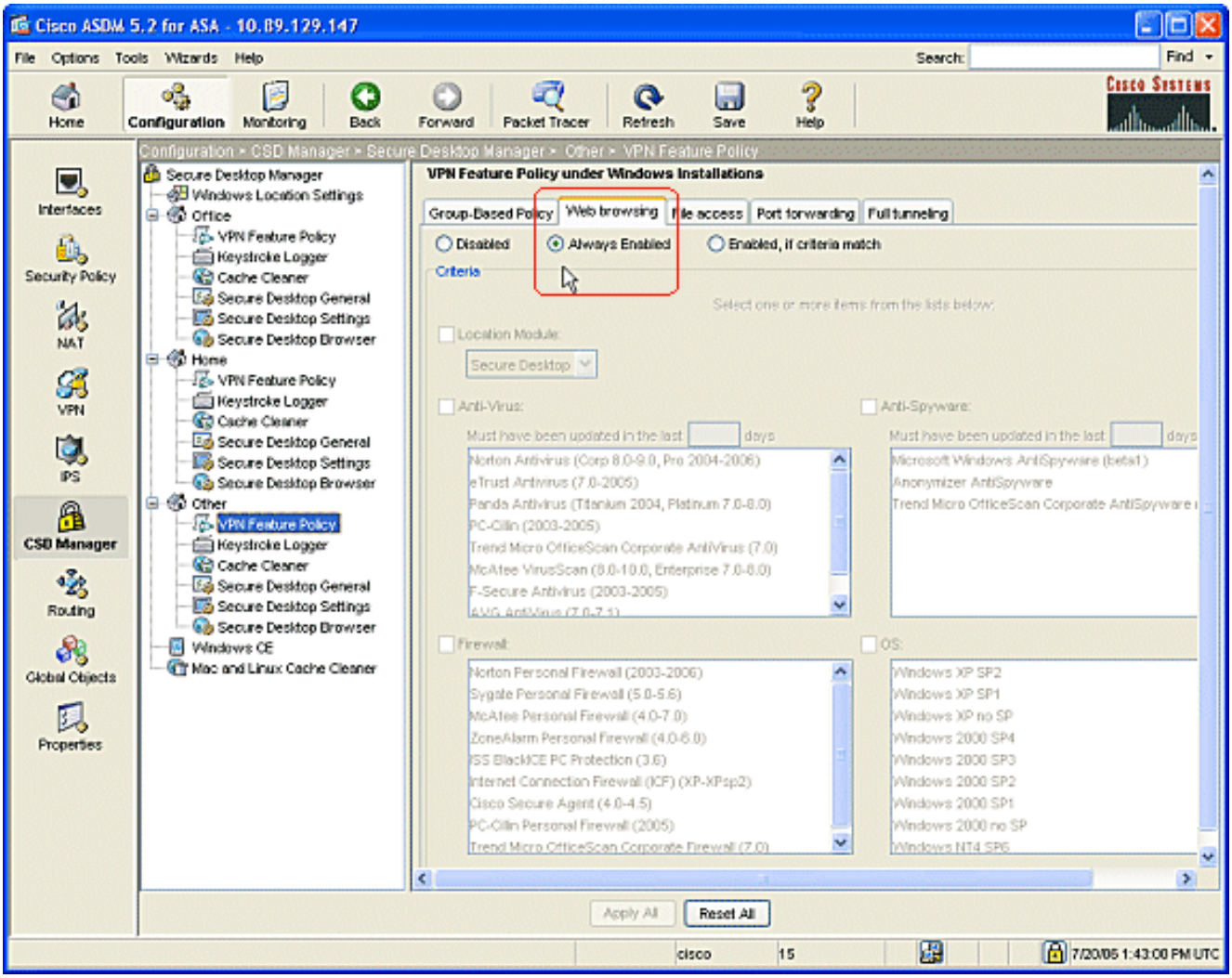
3. Per gli utenti privati, ogni azienda può richiedere criteri specifici prima di poter accedere. Nel riquadro di spostamento fare clic su **Home page** e quindi su **Criteri funzionalità VPN**.Fare clic sulla scheda **Criteri di gruppo**.Fare clic sul pulsante di opzione **Utilizza criteri di gruppo riusciti** se i criteri preconfigurati corrispondono, ad esempio una chiave specifica del Registro di sistema, un nome di file noto o un certificato digitale.Selezionare **la** casella di controllo **Modulo percorso** e scegliere **Desktop sicuro**.Scegliere le aree **Antivirus, Antispyware**, **Firewall** e **SO** in base ai criteri di sicurezza aziendali. Gli utenti privati non potranno accedere alla rete se i loro computer non soddisfano i criteri configurati.



4. Nel riquadro di spostamento fare clic su **Altro** e quindi su **Criteri funzionalità VPN**.Fare clic sulla scheda **Criteri di gruppo**.Fare clic sul pulsante di opzione **Utilizza sempre criteri di gruppo riusciti**.



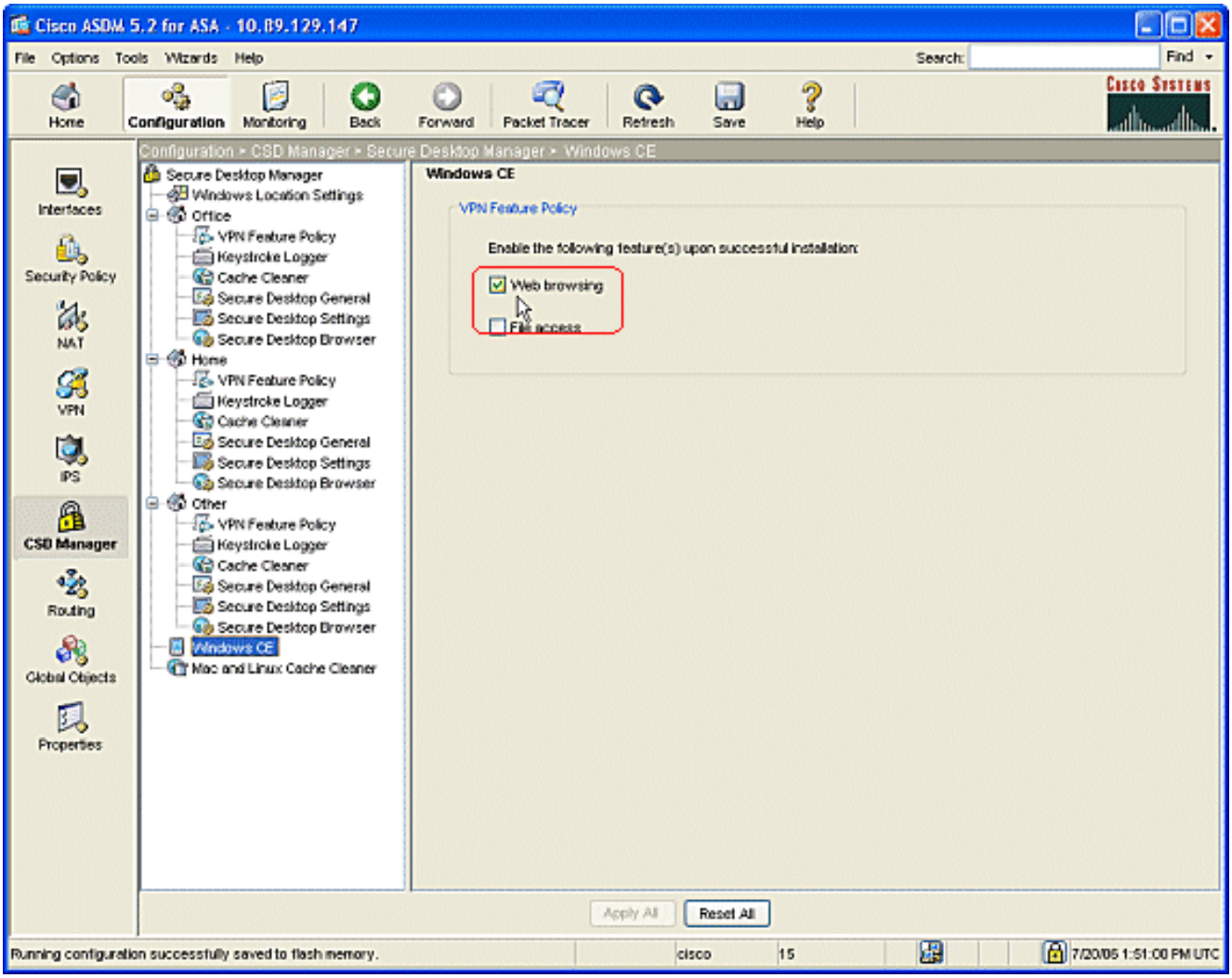
5. Per i client in questa posizione dei **criteri per le funzionalità VPN**, fare clic sulla scheda **Esplorazione Web** e quindi sulla composizione radio **Sempre attivata**.Fare clic sulla scheda **Accesso file**, quindi sul pulsante di opzione **Disabilita**.Ripetere il passaggio con le schede **Port Forwarding** e **Full Tunneling**.Fare clic su **Applica tutto**.Fare clic su **Salva** e quindi su **Sì** per accettare le
modifiche.



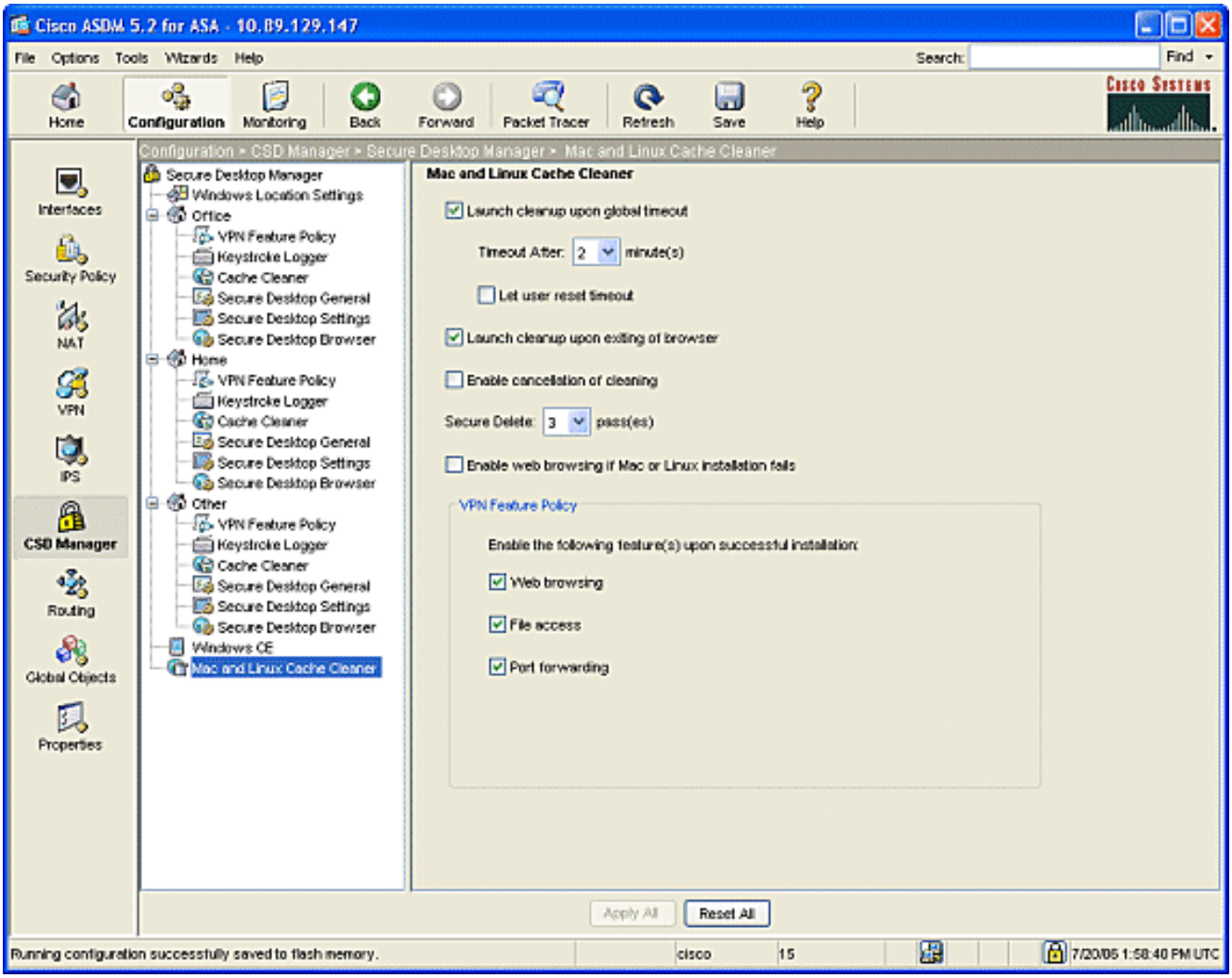
Configurazioni opzionali per client Windows CE, Macintosh e Linux

Queste configurazioni sono opzionali.

1. Se si sceglie **Windows CE** dal riquadro di spostamento, selezionare la casella di controllo **Esplorazione Web**.



2. Se si sceglie **Mac e Linux Cache Cleaner** dal pannello di navigazione, controllare la **funzione di pulizia Avvia al timeout globale della** radio.Modificare il timeout in base alle specifiche.Nell'area **Criteri funzionalità VPN** controllare le **chiamate** radio per **esplorazione Web**, **accesso ai file** e **inoltro porte** per questi
client.



3. Se scegliete Windows CE o Mac e Pulizia cache Linux, fate clic su **Applica tutto**.
4. Fare clic su **Salva** e quindi su **Sì** per accettare le modifiche.

Configurazione

Configurazione

Questa configurazione riflette le modifiche apportate da ASDM per abilitare CSD: La maggior parte delle configurazioni CSD è conservata in un file separato su 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
```

Verifica

Utilizzare questa sezione per verificare che le configurazioni per VPN SSL senza client, VPN SSL thin-client o client VPN SSL (SVC) funzionino correttamente.

Verificare il CSD con un PC configurato con diverse posizioni Windows. Ogni test deve fornire un accesso diverso in base ai criteri configurati nell'esempio precedente.

È possibile modificare il numero di porta e l'interfaccia su cui Cisco ASA resta in ascolto delle

connessioni WebVPN.

- La porta predefinita è 443. Se si utilizza la porta predefinita, l'accesso è **https://ASA indirizzo IP**.
- L'uso di una porta diversa modifica l'accesso a **https://ASA IP Address:newportnumber**.

Comandi

Diversi comandi **show** sono associati a WebVPN. È possibile eseguire questi comandi dall'interfaccia della riga di comando (CLI) per visualizzare le statistiche e altre informazioni. Per ulteriori informazioni sull'utilizzo dei comandi **show**, consultare il documento sulla verifica della configurazione di WebVPN.

Nota: lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

In caso di problemi con il client remoto, verificare quanto segue:

1. I popup, Java e/o ActiveX sono abilitati nel browser Web? A seconda del tipo di connessione VPN SSL in uso, potrebbe essere necessario attivare tali connessioni.
2. Il client deve accettare i certificati digitali presentati all'inizio della sessione.

Comandi

Diversi comandi **debug** sono associati a WebVPN. Per informazioni dettagliate su questi comandi, consultare il documento sull'uso dei comandi di debug di WebVPN..

Nota: l'uso dei comandi di **debug** può avere un impatto negativo sul dispositivo Cisco. Prima di usare i comandi di **debug**, consultare le informazioni importanti sui comandi di debug.

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- Esempio di configurazione di ASA con WebVPN e Single Sign-On con ASDM e NTLMv1
- Documentazione e supporto tecnico – Cisco Systems