Exemple de configuration de Cisco Secure Desktop (CSD 3.1.x) sur ASA 7.2.x pour Windows à l'aide d'ASDM

Contenu

Introduction

Cisco Secure Desktop (CSD) améliore la sécurité de la technologie VPN SSL. CSD fournit une partition distincte sur le poste de travail d'un utilisateur pour l'activité de session. Cette voûte est chiffrée pendant les sessions et complètement retirée à la fin d'une session VPN SSL. Windows peut être configuré avec tous les avantages de sécurité du CSD. Macintosh, Linux, et Windows CE donnent seulement accès aux fonctionnalités de nettoyage de cache, de navigation Web et d'accès aux fichiers. Le CSD peut être configuré pour Windows, Macintosh, le Windows CE, et les périphériques de Linux sur ces Plateformes :

- Gamme 5500 de l'appliance de sécurité adaptable Cisco (ASA)
- Routeurs de Cisco qui exécutent des versions de logiciel 12.4(6)T et ultérieures de Cisco IOS®

- Version 4.7 et ultérieures de Concentrateurs de la gamme Cisco VPN 3000
- Module de webvpn de Cisco sur des Routeurs de gammes Catalyst 6500 et 7600

Remarque: La version 3.3 CSD vous permet maintenant de configurer le Cisco Secure Desktop pour fonctionner sur les ordinateurs distants qui exécutent la Microsoft Windows Vista. Précédemment, le Cisco Secure Desktop a été limité aux ordinateurs qui ont exécuté Windows XP ou 2000. Référez-vous à la nouvelle amélioration de caractéristique - Secure Desktop sur la section de vista des notes en version pour le Cisco Secure Desktop, version 3.3, pour en savoir plus.

Cet exemple couvre principalement l'installation et la configuration du CSD sur la gamme ASA 5500 pour des clients Windows. Des configurations facultatives pour le Windows CE, le MAC, et les clients Linux sont ajoutées pour la fin.

Le CSD est utilisé en même temps que la technologie de VPN SSL (VPN SSL sans client, client de VPN SSL de client léger, ou de VPN SSL (SVC)). Le CSD ajoute la valeur aux sessions sécurisées de la technologie de VPN SSL.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

Conditions requises pour le périphérique de theASA

- Version 3.1 de Cisco CSD ou plus tard
- Version de logiciel 7.1.1 de Cisco ASA ou plus tard
- Version 5.1.1 du Cisco Adaptive Security Device Manager (ASDM) ou plus tard**Remarque:** Supports de version 3.2 CSD sur la version 8.x ASA seulement**Remarque:** Référez-vous à Permettre l'accès HTTPS pour l'ASDM afin de permettre l'ASA d'être configuré par l'ASDM.

Conditions requises pour des ordinateurs client

- Les clients distants devraient avoir des privilèges d'administrateur locaux ; on ne l'exige pas, mais on lui suggère fortement.
- Les clients à distance doivent avoir la version 1.4 ou ultérieures de Java Runtime Environment (JRE).
- Navigateurs de client distant : Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, safari 1.2.2, ou Firefox 1.0
- Témoins activés et Popups permis sur des clients distants

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont commencé par une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande. Les adresses IP utilisées dans cette configuration sont les adresses RFC 1918. Ces adresses IP ne sont pas juridiques sur l'Internet et doivent être utilisées seulement dans un environnement de travaux pratiques de test.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

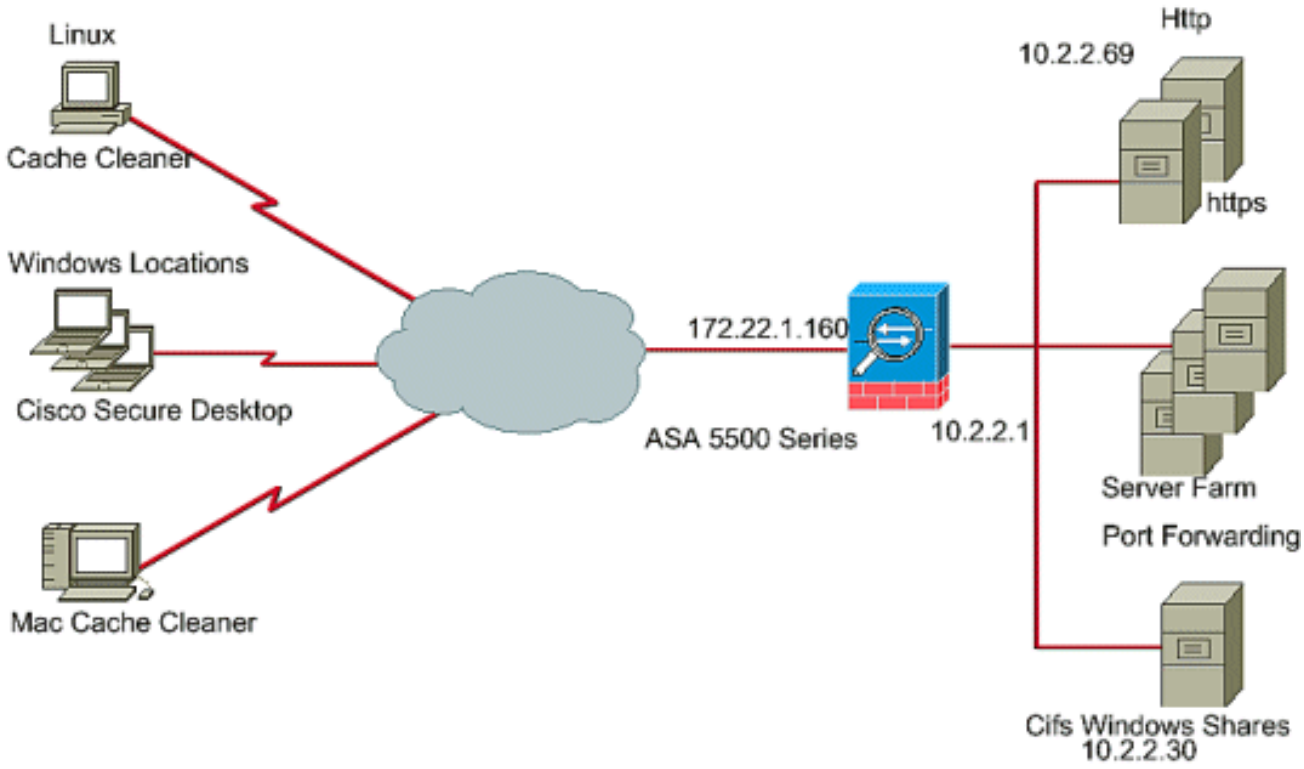
Informations générales

Le CSD fonctionne avec la technologie de VPN SSL, ainsi le sans client, le client léger, ou le SVC devraient être lancés avant la configuration du CSD.

Diagramme du réseau

Différents emplacements de Windows peuvent être configurés avec les pleins aspects de Sécurité du CSD. Macintosh, le Linux, et le Windows CE ont accès seulement au décapant de cache et/ou la navigation web et l'accès au fichier.

Ce document utilise la configuration réseau suivante :



Configurez le CSD sur l'ASA pour des clients Windows

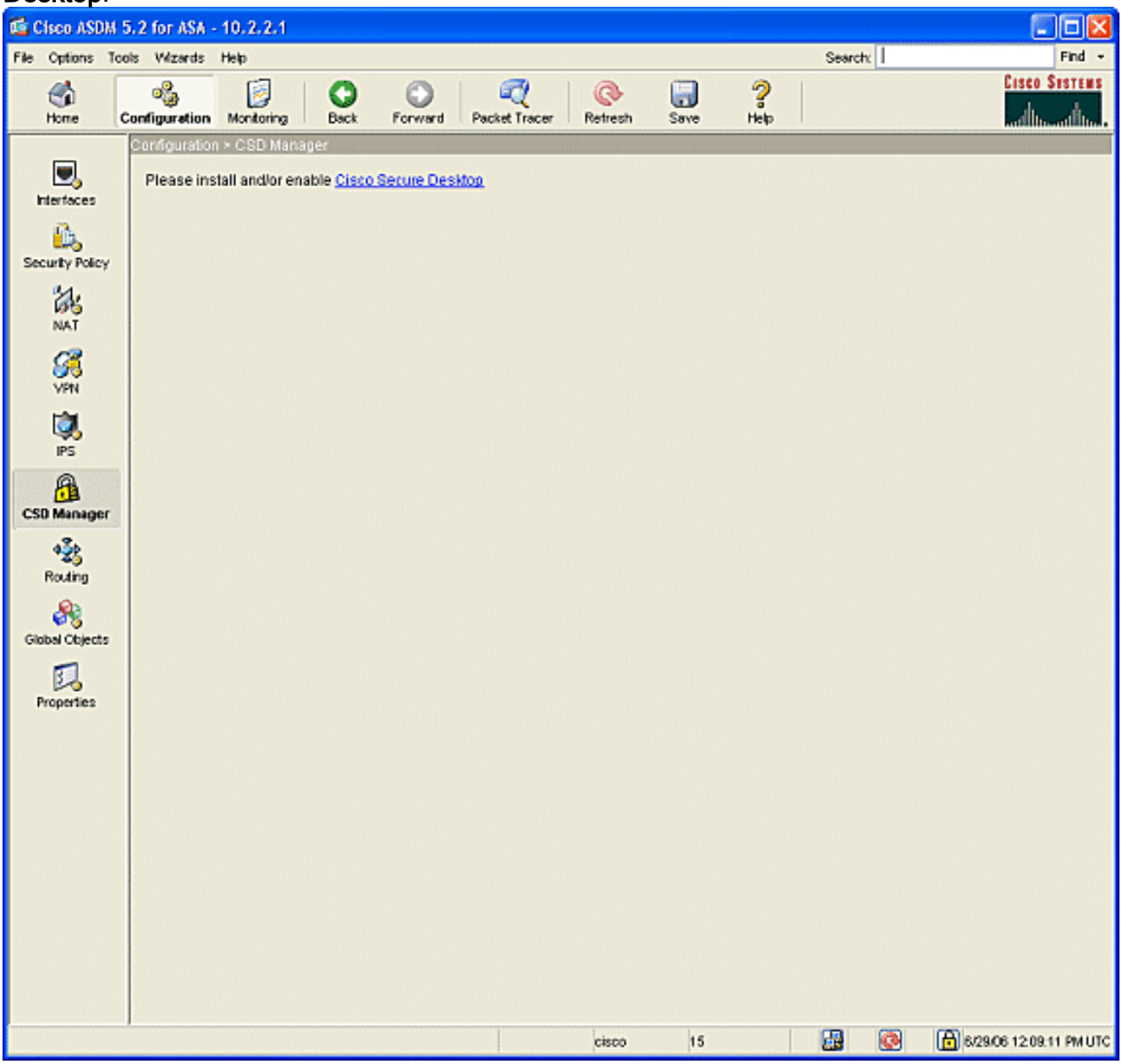
Configurez le CSD sur l'ASA pour des clients Windows avec cinq étapes principales :

- Obtenez, installez, et activez le logiciel CSD sur Cisco ASA.
- Définissez les emplacements de Windows.
- Définissez l'identification d'emplacement de Windows.
- Configurez les modules d'emplacement de Windows.
- Configurez les caractéristiques d'emplacement de Windows.
- Configuration facultative pour le Windows CE, le Macintosh, et les clients Linux.

Obtenez, installez, et activez le logiciel CSD

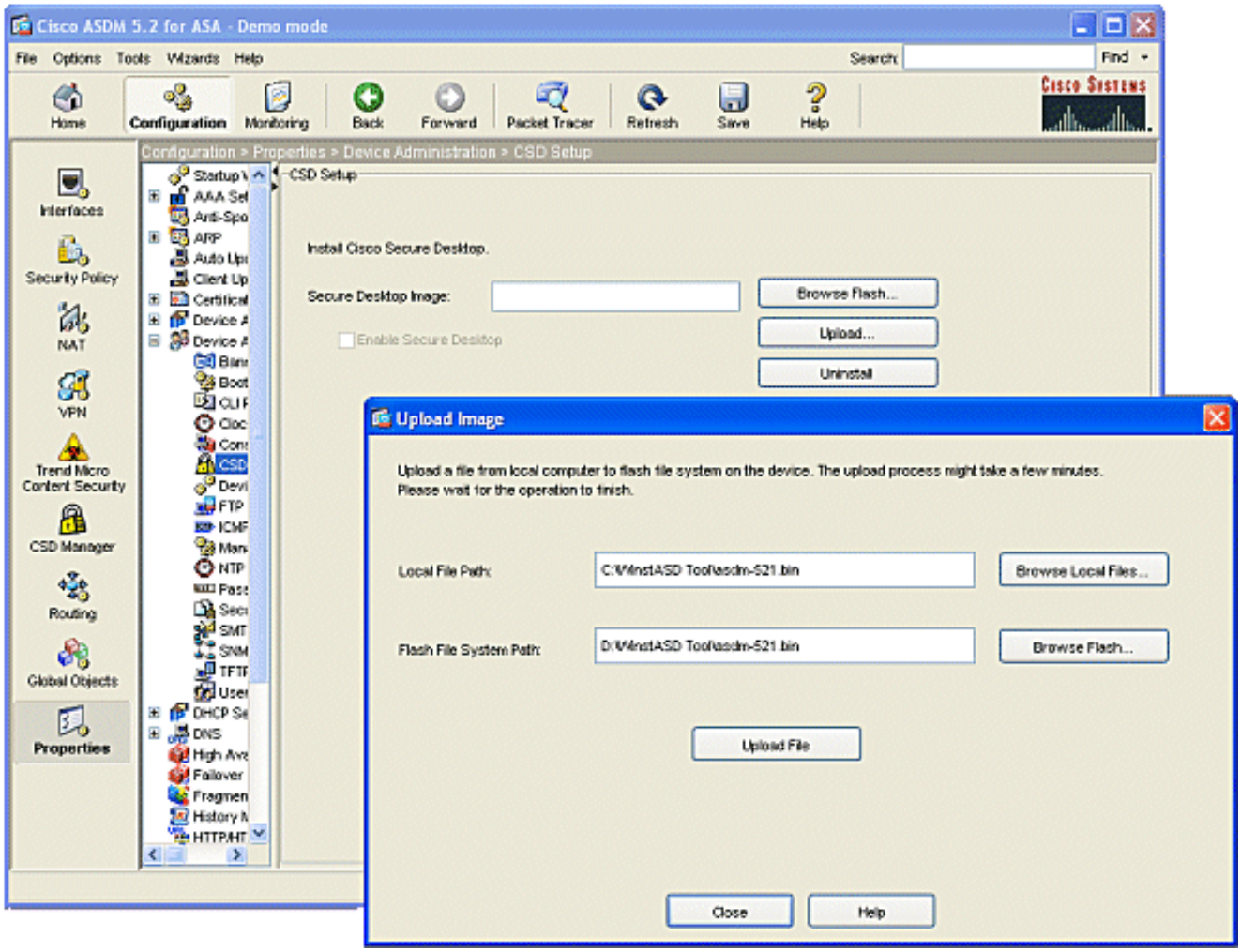
Terminez-vous ces étapes pour obtenir, installer, et activer le logiciel CSD sur Cisco ASA.

1. Téléchargez le logiciel securedesktop-asa*.package CSD et les fichiers readmes sur votre station de Gestion du site Web de téléchargement logiciel de Cisco.
2. Ouvrez une session à l'ASDM et cliquez sur le **bouton configuration**. Du menu de gauche, cliquez sur le bouton de **gestionnaire CSD**, et cliquez sur le lien de **Cisco Secure Desktop**.



3. Cliquez sur Upload pour afficher la fenêtre d'image de téléchargement.Ou entrez dans le chemin du nouveau fichier .package sur la station de Gestion ou le clic **parcourent des**

fichiers locaux pour localiser le fichier.L'un ou l'autre entre l'emplacement sur l'éclair dans lequel pour placer le fichier ou cliquer sur **Browse Flash**.Cliquez sur Upload le **fichier**.Une fois incité, cliquez sur OK **> étroit >**
CORRECT.

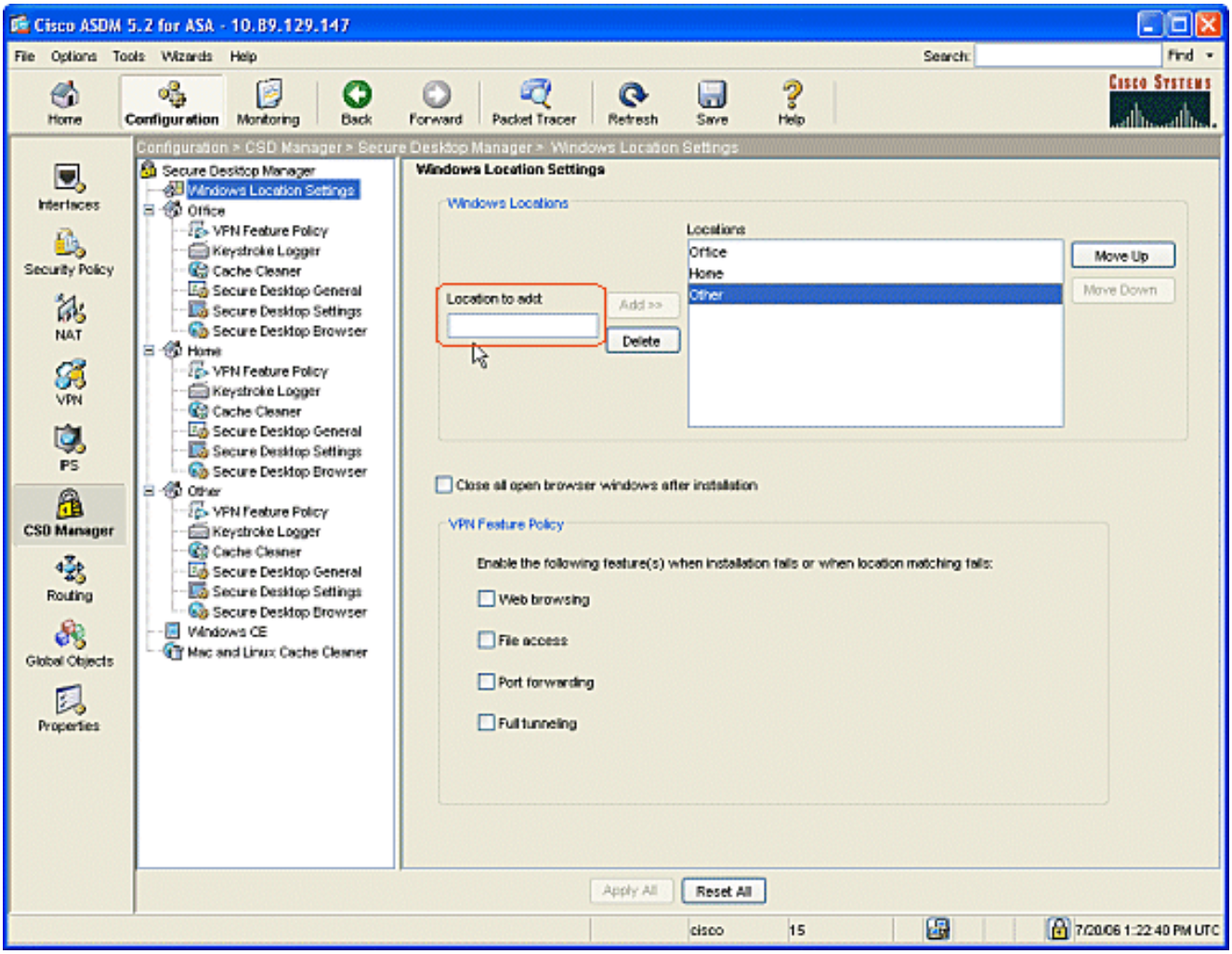


4. Une fois l'image client téléchargée sur flash, cochez la case **Enable SSL VPN Client**, puis cliquez sur **Apply**.
5. Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.

Définissez les emplacements de Windows

Terminez-vous ces étapes pour définir des emplacements de Windows.

1. Cliquez sur le **bouton configuration**.
2. Du menu de gauche, cliquez sur le bouton de **gestionnaire CSD**, et cliquez sur le lien de **Cisco Secure Desktop**.
3. Du volet de navigation, **configurations d'emplacement de Windows de** clic.
4. Introduisez un nom d'emplacement dans l'emplacement pour ajouter le champ et pour cliquer sur Add.Notez les trois emplacements dans cet exemple : Bureau, maison, et d'autres.Le bureau représente les postes de travail qui se trouvent à l'intérieur de la borne de Sécurité de la société.La maison représente les utilisateurs qui travaillent de la maison.Autre représente n'importe quel emplacement autre que les deux emplacements mentionnés.

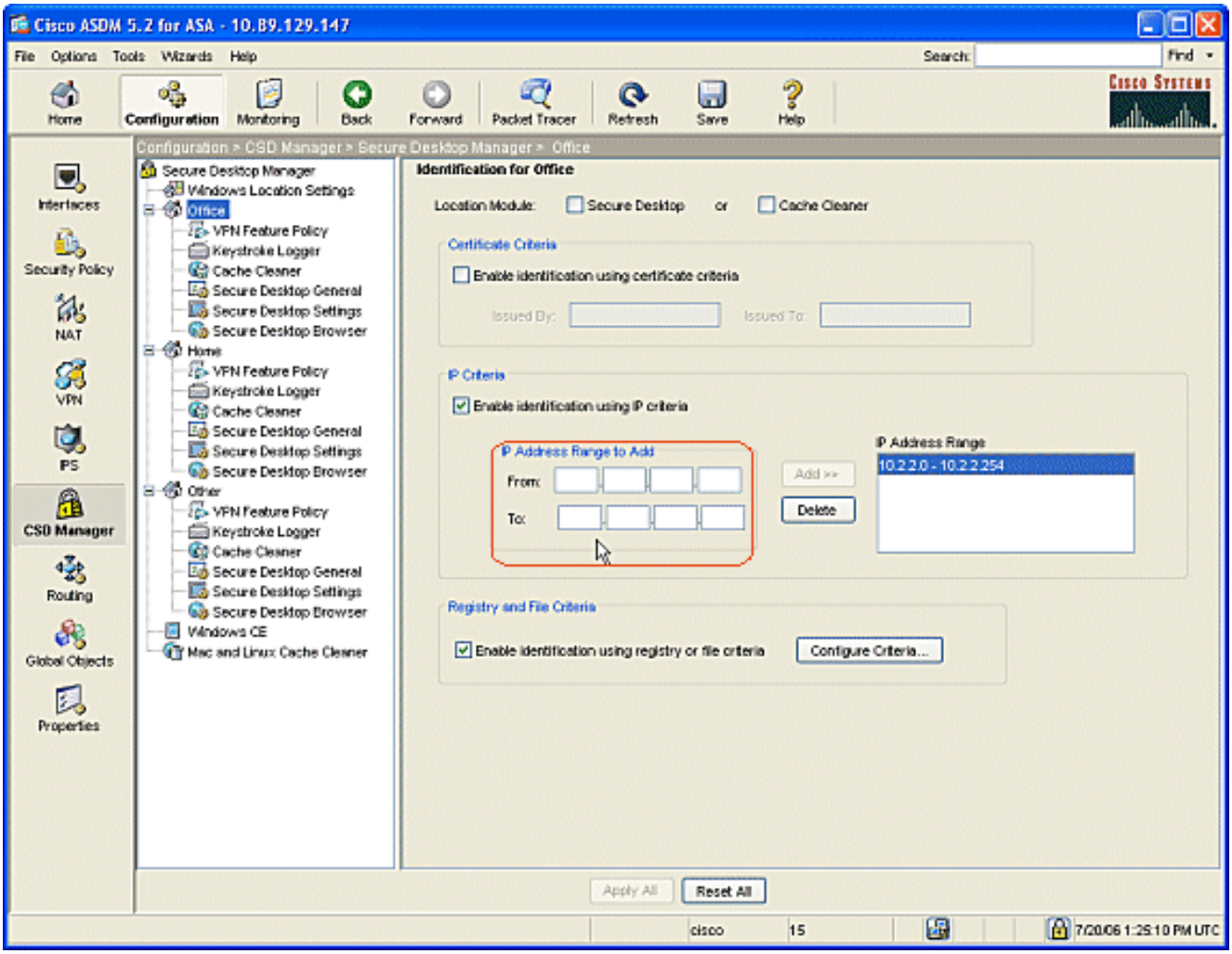


5. Créez vos propres emplacements dépendants de l'affichage de votre architecture de réseau à vendre, des invités, des Partenaires, et d'autres.
6. Car vous créez des emplacements de Windows, le volet de navigation développe avec les modules configurables pour chaque nouveau emplacement. Cliquez sur Apply **tous**.
7. Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.

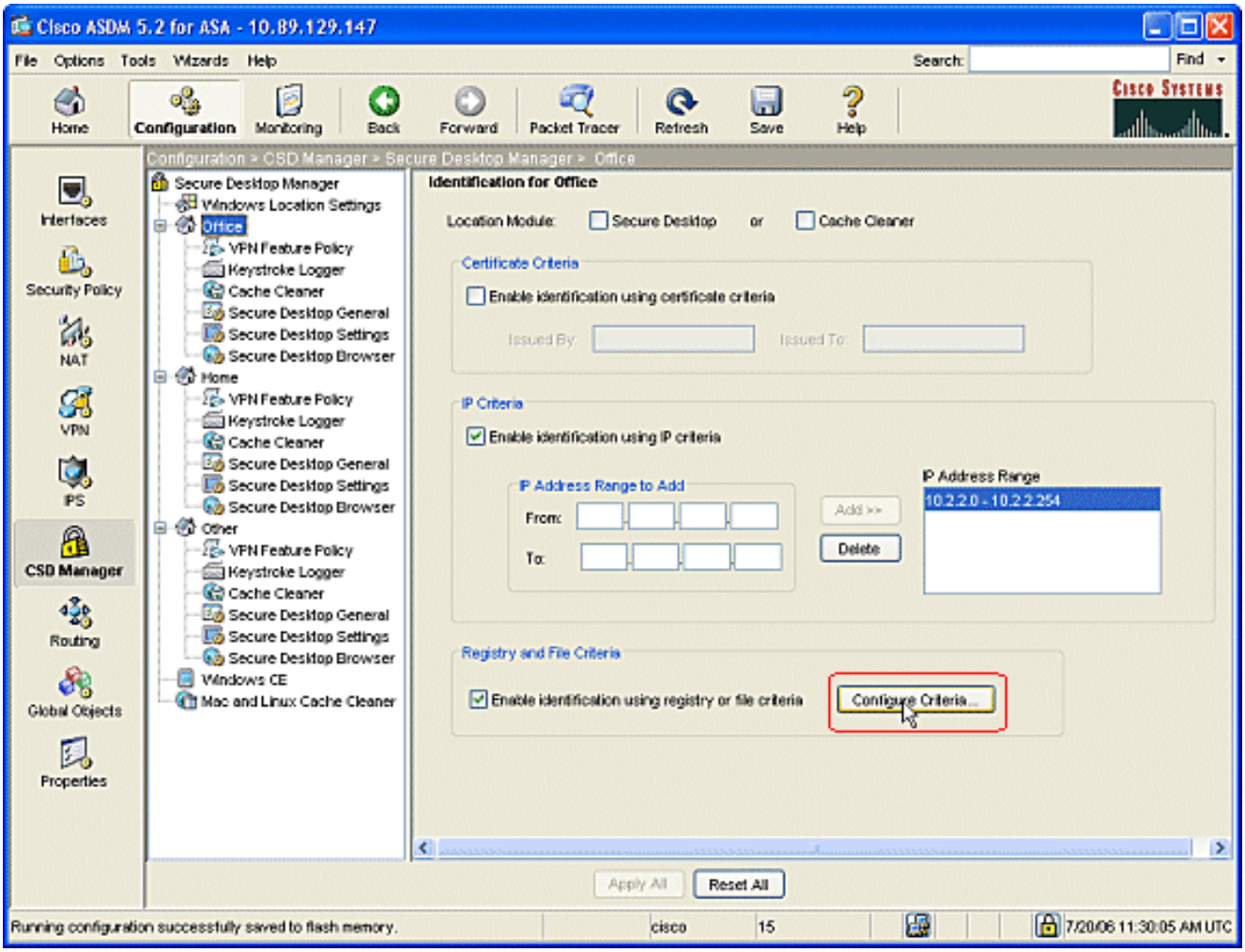
Identification d'emplacement de Windows

Terminez-vous ces étapes pour définir l'identification d'emplacement de Windows.

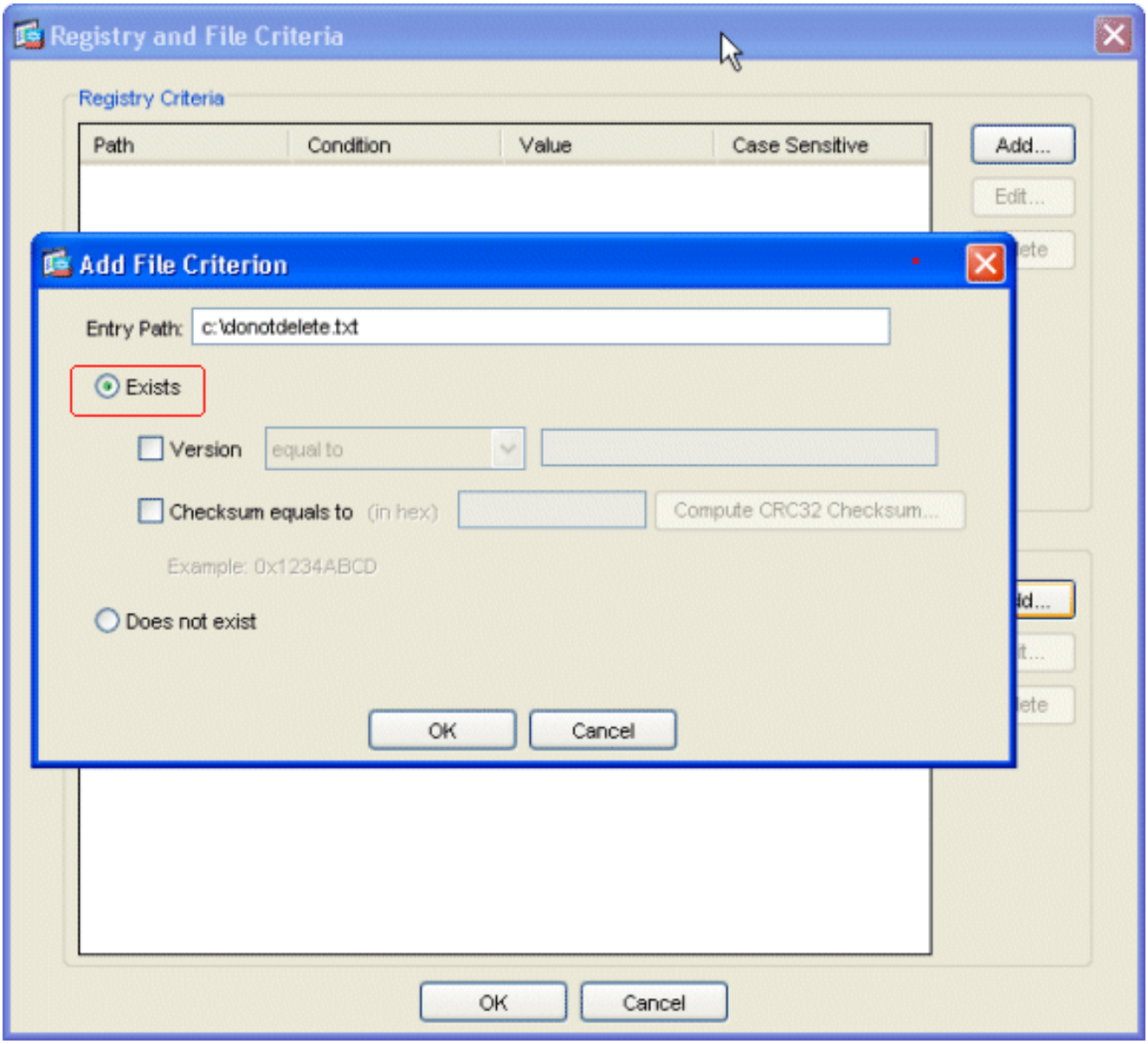
1. Identifiez les emplacements qui ont été créés dedans définissent des emplacements de Windows.



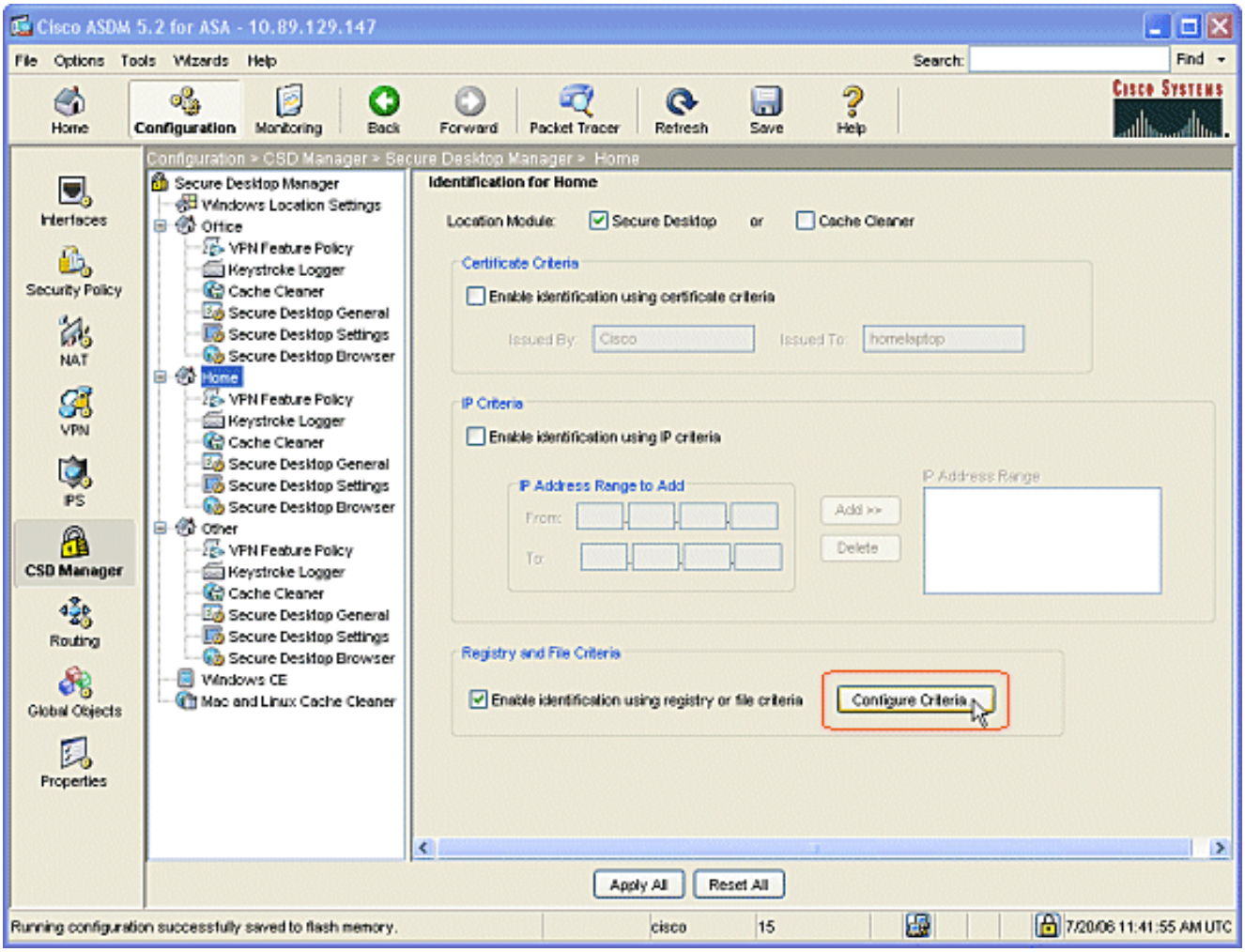
2. Pour identifier le bureau d'emplacement, **bureau de** clic dans le volet de navigation.Décochez le **décapant de Secure Desktop** et de **cache** parce que ce sont les ordinateurs internes.**Identification d'enable de** contrôle **utilisant des critères IP**.Écrivez les plages d'adresses IP de vos ordinateurs internes.Vérifiez l'**identification d'enable utilisant des critères de registre ou de fichier**. Ceci différencie les employés de bureau internes des invités occasionnels sur le
réseau.



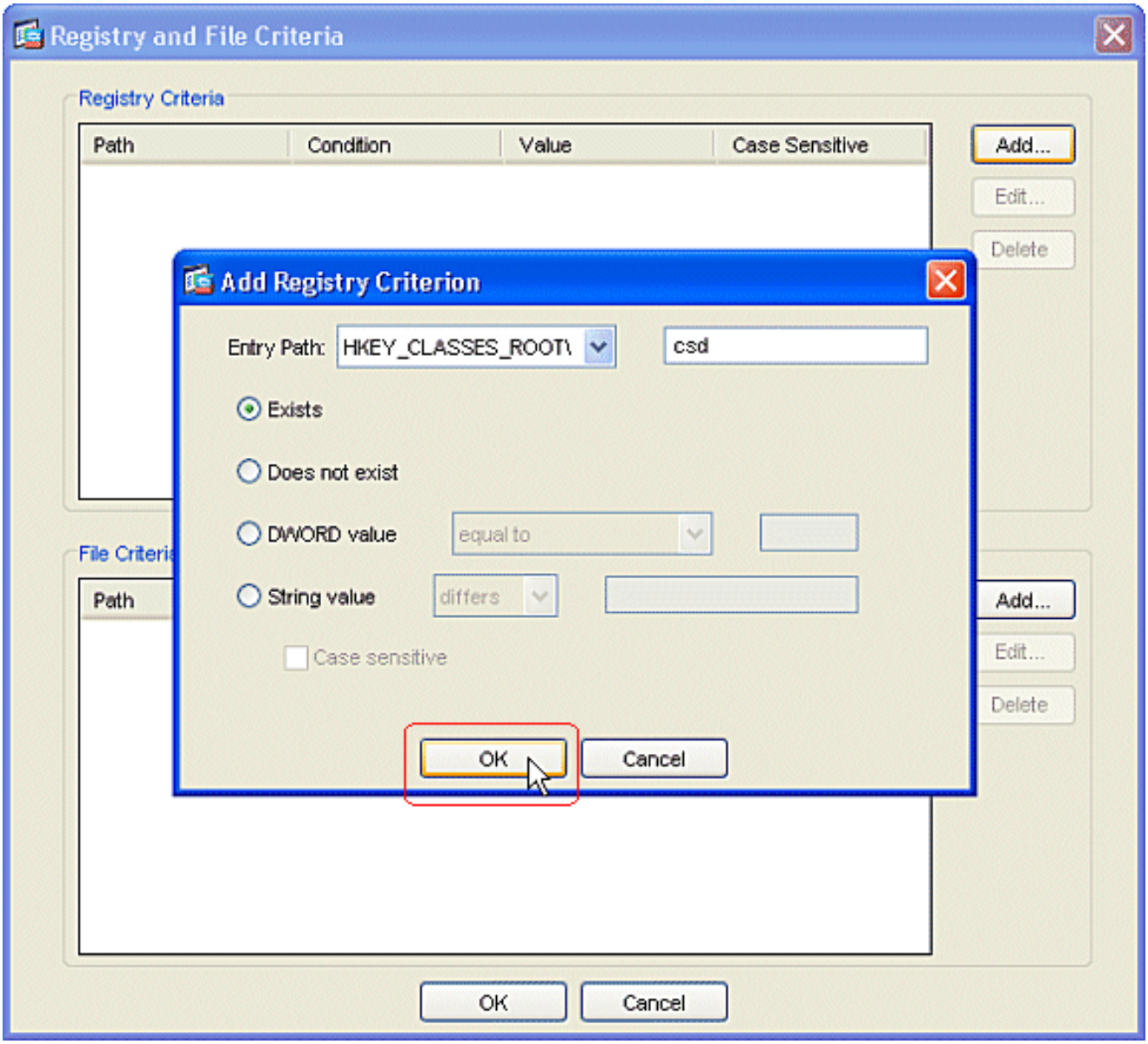
3. Cliquez sur Configure les **critères**. Un exemple simple d'un fichier « DoNotDelete.txt » est configuré. Ce fichier doit exister sur vos ordinateurs Windows internes et est simplement un texte d'attente. Vous pouvez également configurer une clé de registre de Windows pour identifier les ordinateurs de bureau internes. Clic OKIN la fenêtre de critère de fichier d'ajouter. Cliquez sur OKIN la fenêtre de critères de registre et de fichier.



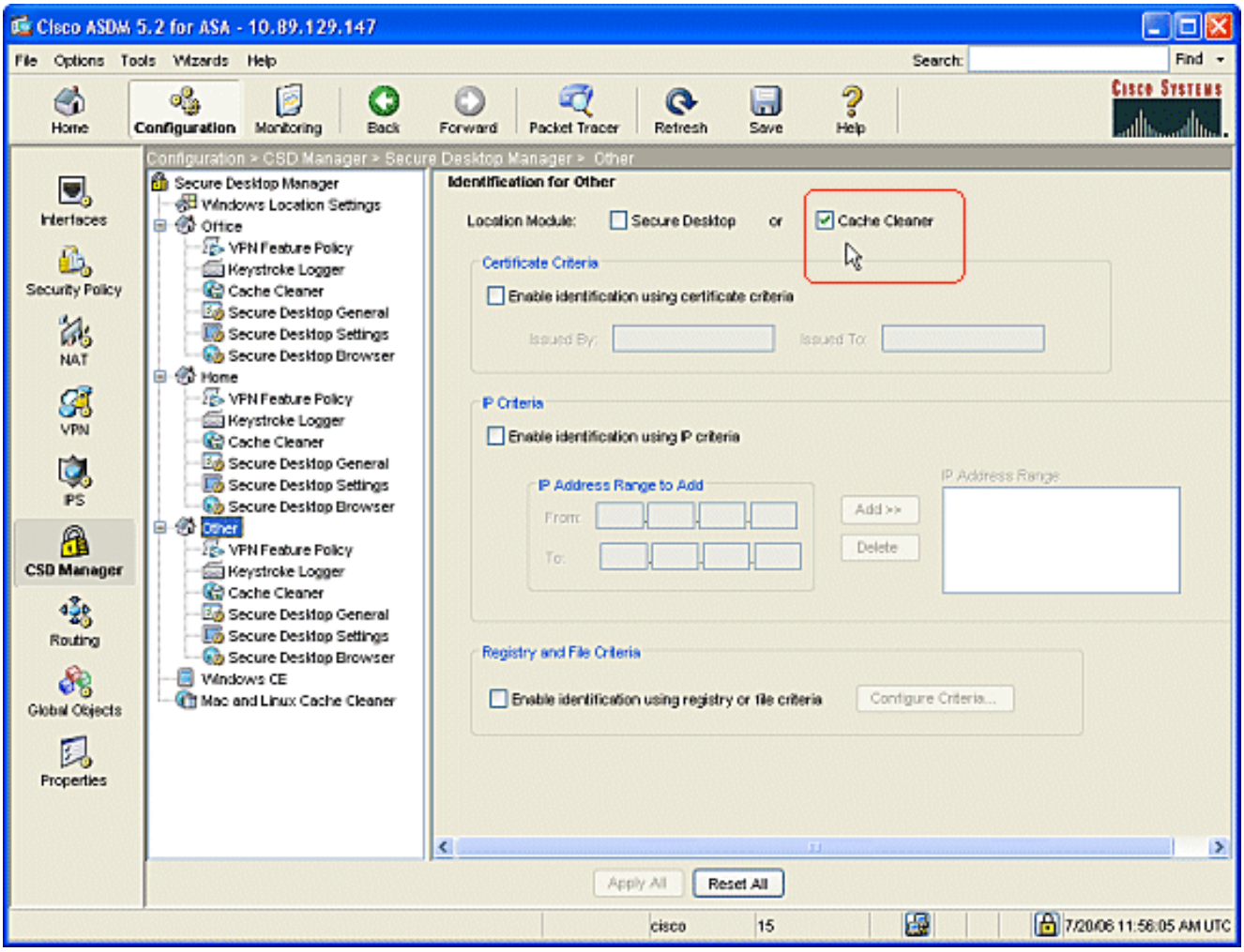
4. Cliquez sur Apply **tous** dans l'identification pour la fenêtre de bureau. Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.
5. Pour identifier la maison d'emplacement, **maison de** clic dans le volet de navigation.Vérifiez l'**identification d'enable utilisant des critères de registre ou de fichier**.Cliquez sur Configure les
critères.



6. Des clients d'ordinateur personnel doivent avoir été configurés avec cette clé de registre par un administrateur. Cliquez sur OK dans la fenêtre de critère de registre d'ajouter. Cliquez sur OK dans la fenêtre de critères de registre et de
fichier.



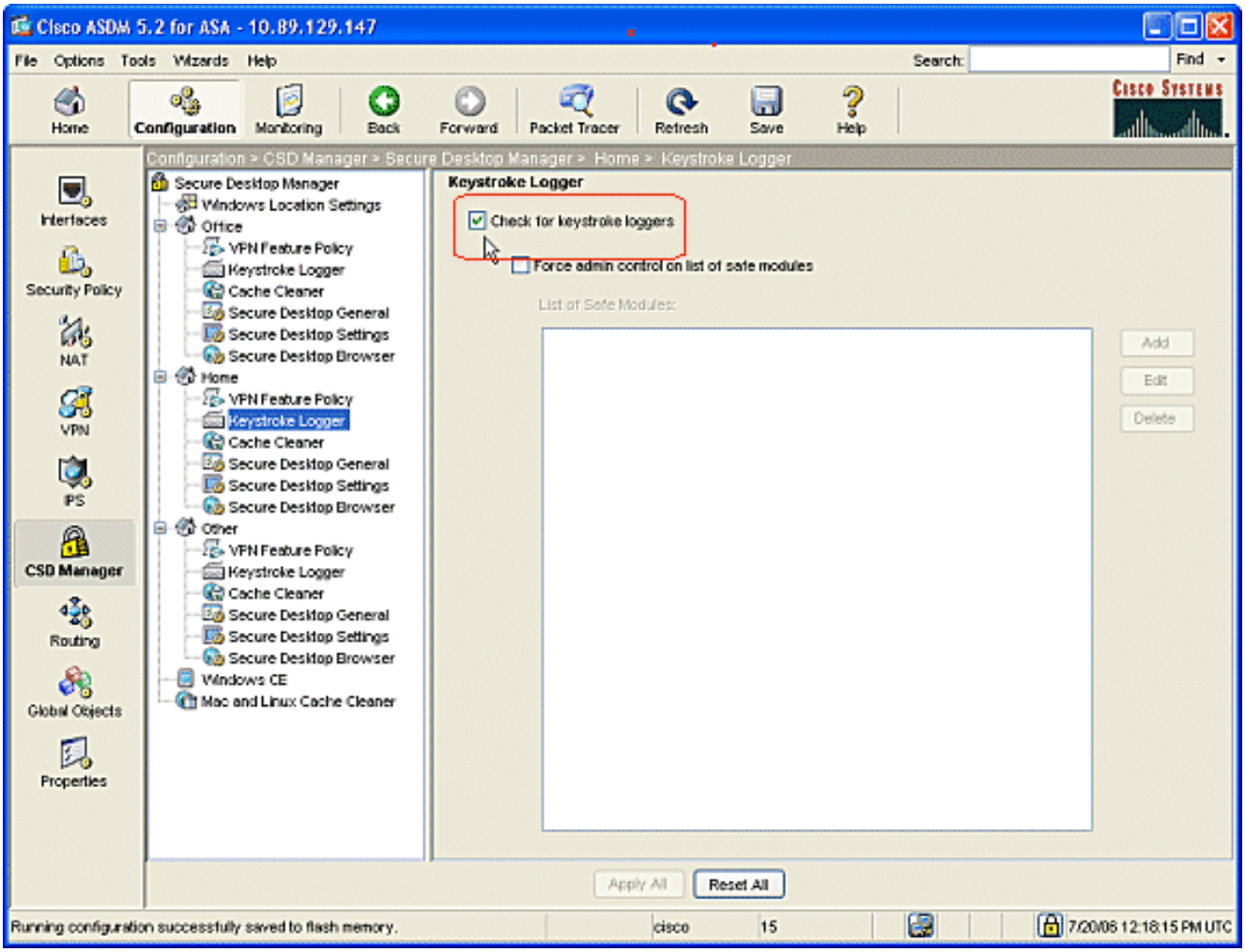
7. Sous le module d'emplacement, **Secure Desktop de** contrôle. Cliquez sur Apply **tous** dans l'identification pour la fenêtre d'accueil. Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.
8. Pour identifier l'emplacement **autre**, cliquent sur **autre** dans le volet de navigation.Cochez seulement la case de **décapant de cache** et décochez toutes autres cases.Cliquez sur Apply **tous** dans l'identification pour l'autre fenêtre.Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.



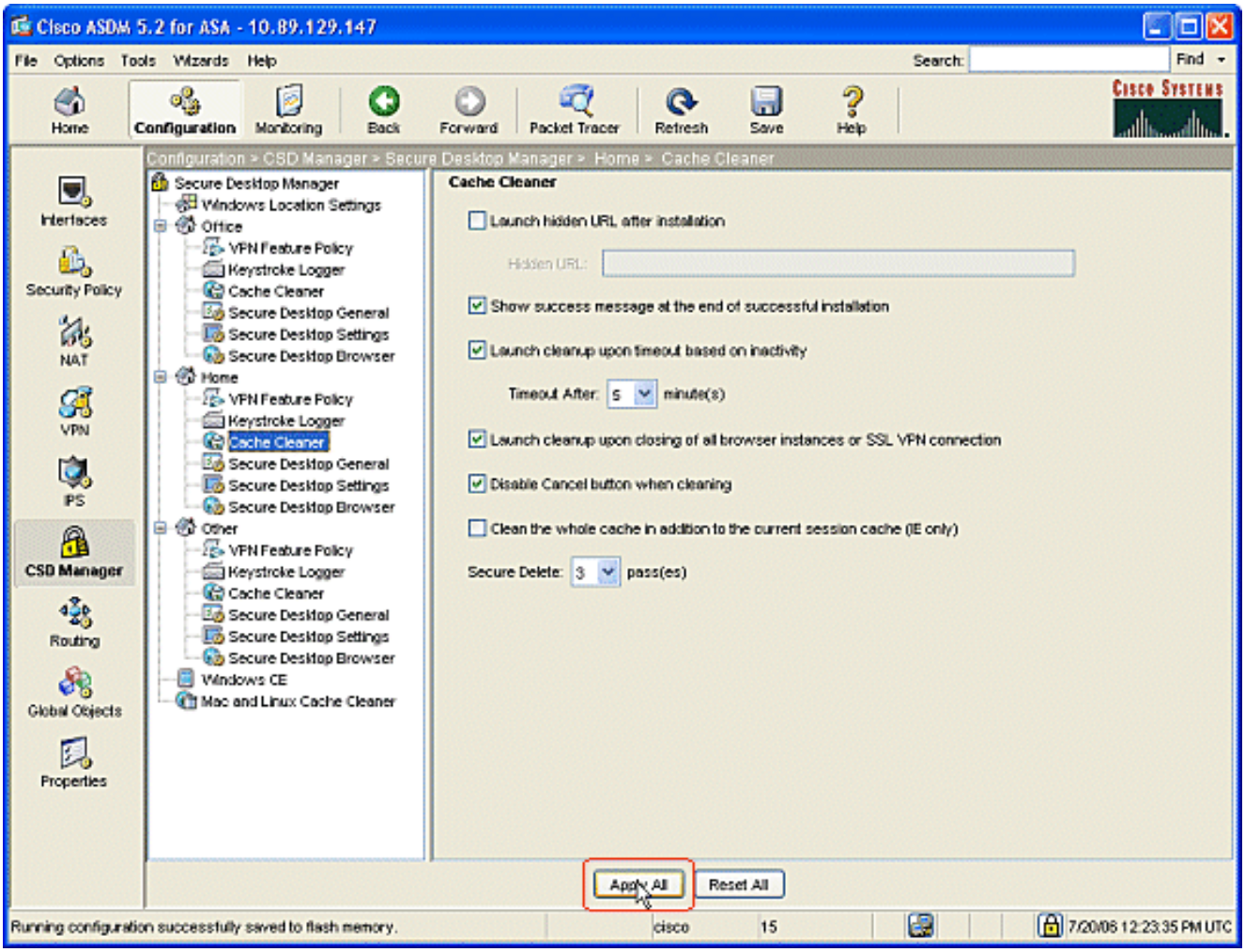
Configurez le module d'emplacement de Windows

Terminez-vous ces étapes pour configurer les modules sous chacun des trois emplacements que vous avez créés.

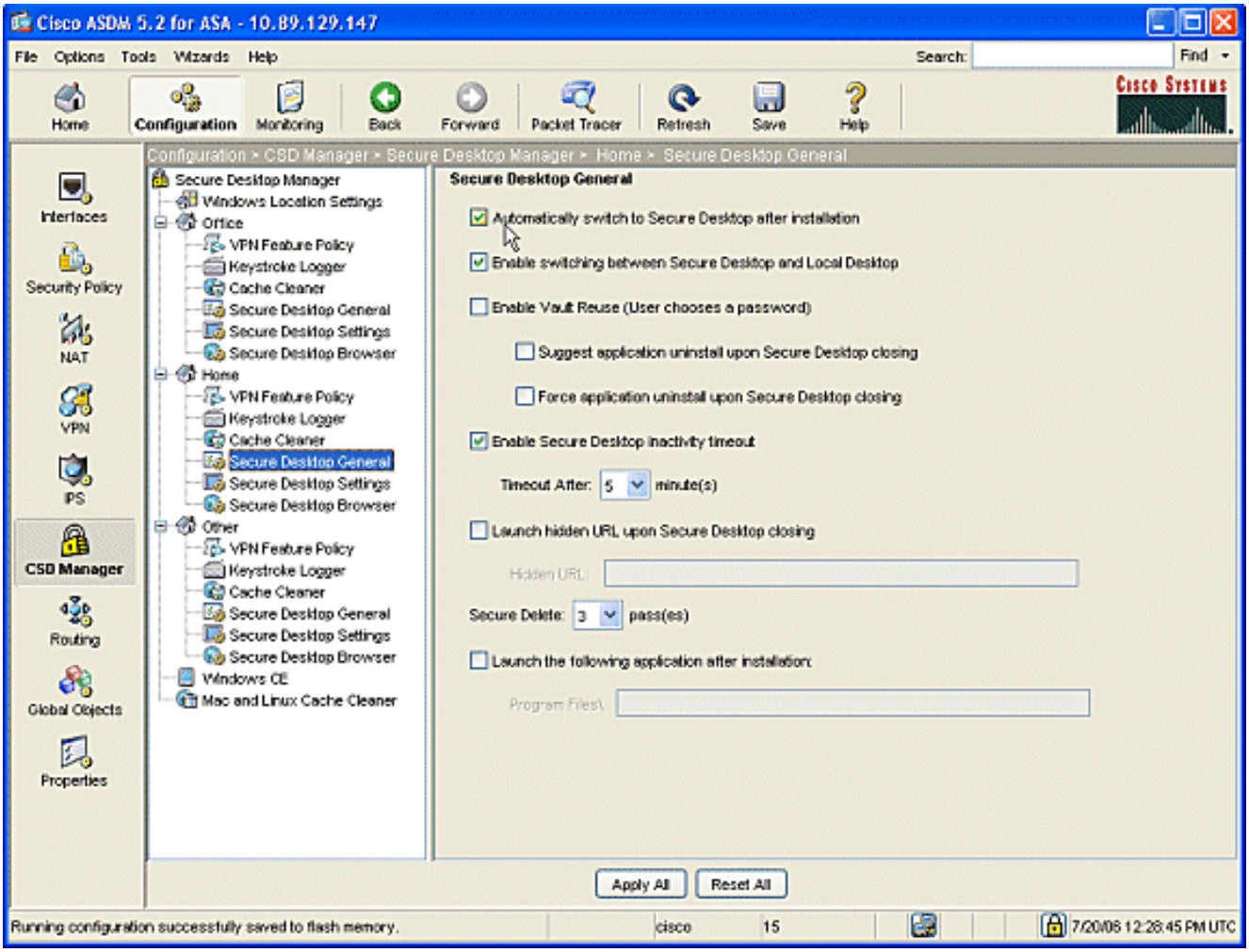
1. Pour des clients de bureau, ne faites rien puisque le décapant de Secure Desktop et de cache n'ont pas été choisis dans les étapes précédentes. L'application ASDM te permet pour configurer le décapant de cache même si elle n'ont pas été choisies dans une étape précédente. Gardez les valeurs par défaut pour les emplacements de bureau.**Remarque:** La stratégie de caractéristique VPN n'est pas discutée dans cette étape, mais elle sera discutée dans une étape ultérieure pour tous les emplacements.
2. Pour les clients à la maison, **maison de** clic et **enregistreur de touche** dans le volet de navigation.Dans la fenêtre d'enregistreur de touche, le contrôle **vérifient des enregistreurs de touche**.Cliquez sur Apply **tous** dans la fenêtre d'enregistreur de touche.Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.



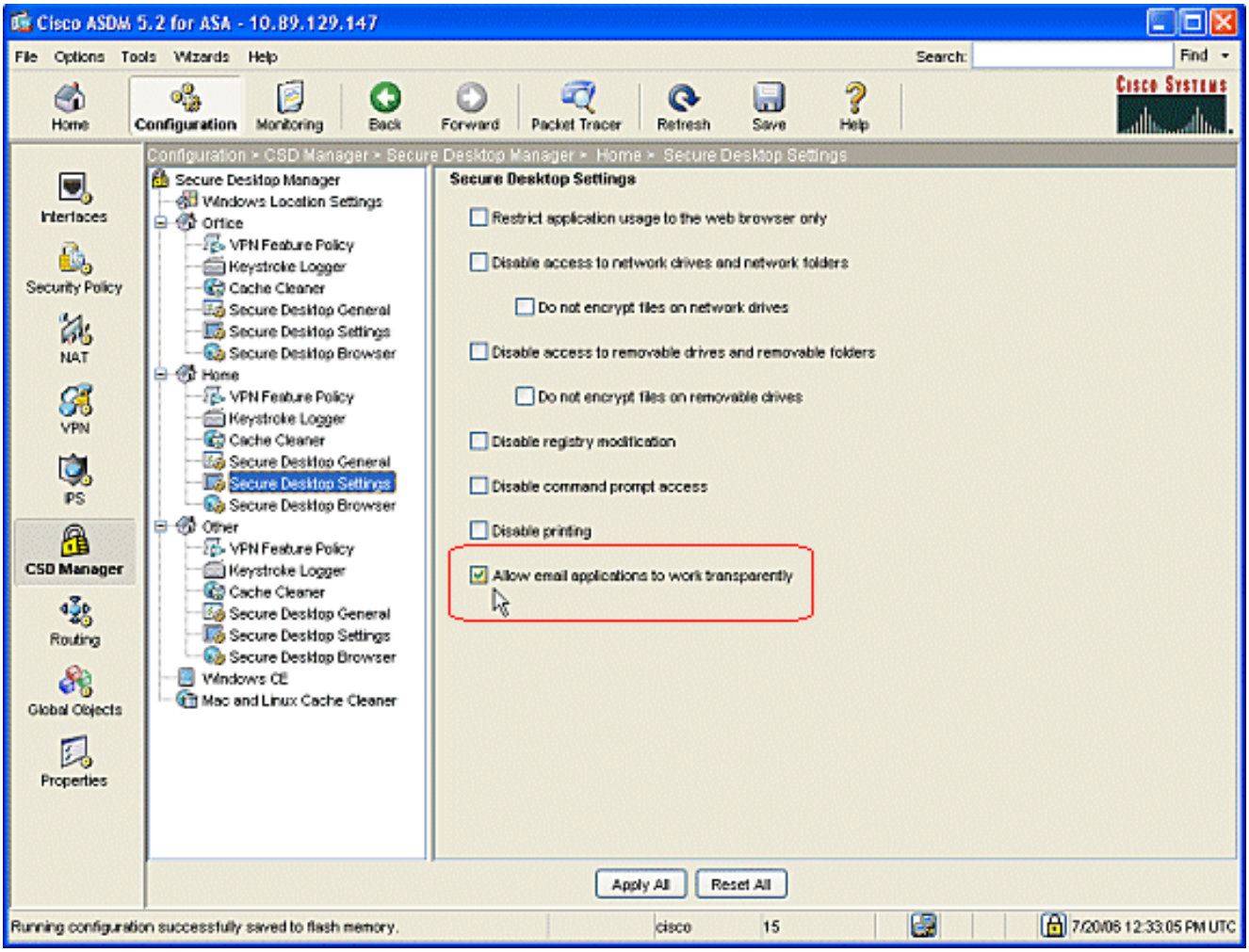
3. Sous la maison, choisissez le **décapant de cache** et les paramètres pour adapter à votre environnement.



4. Sous la maison, choisissez le **Secure Desktop général** et les paramètres pour adapter à votre
environnement.



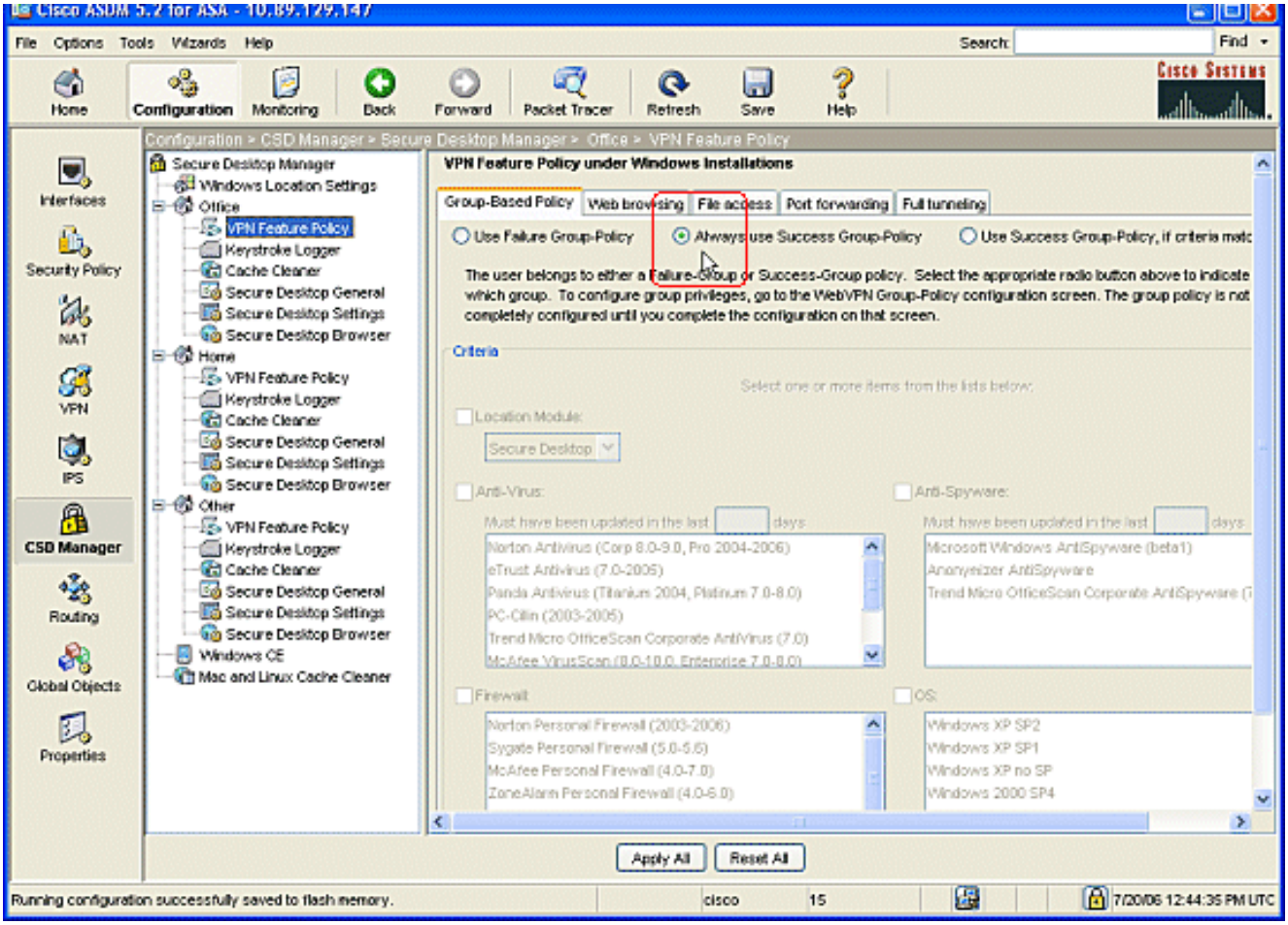
5. Sous la maison, choisissez les **configurations de Secure Desktop**.Vérifiez **permettent des applications de messagerie électronique de fonctionner d'une manière transparente**, et configurent les autres configurations pour adapter à votre environnement.Cliquez sur Apply **tous**.Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.



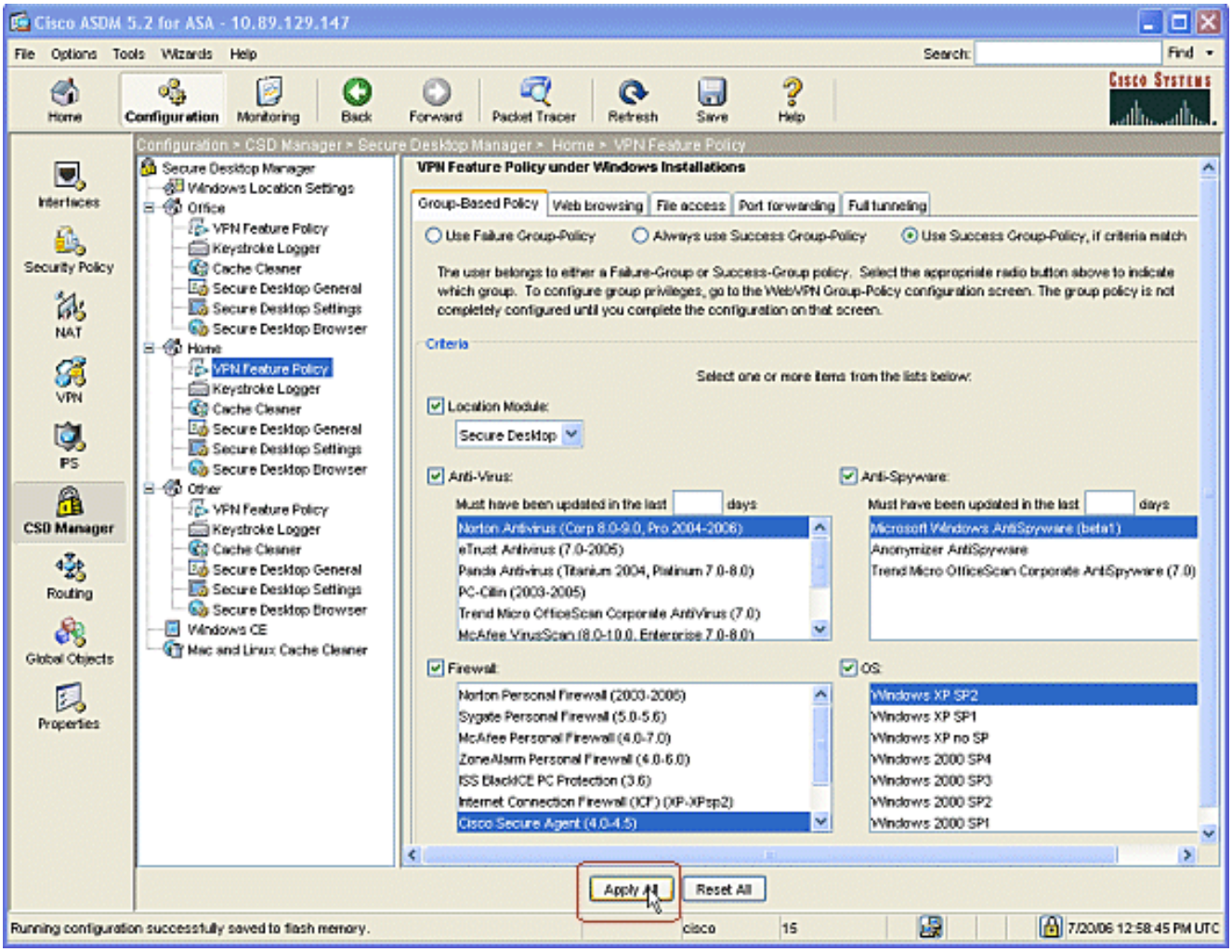
Configurez les caractéristiques d'emplacement de Windows

Configurez la stratégie de caractéristique VPN pour chacun des emplacements que vous avez créés.

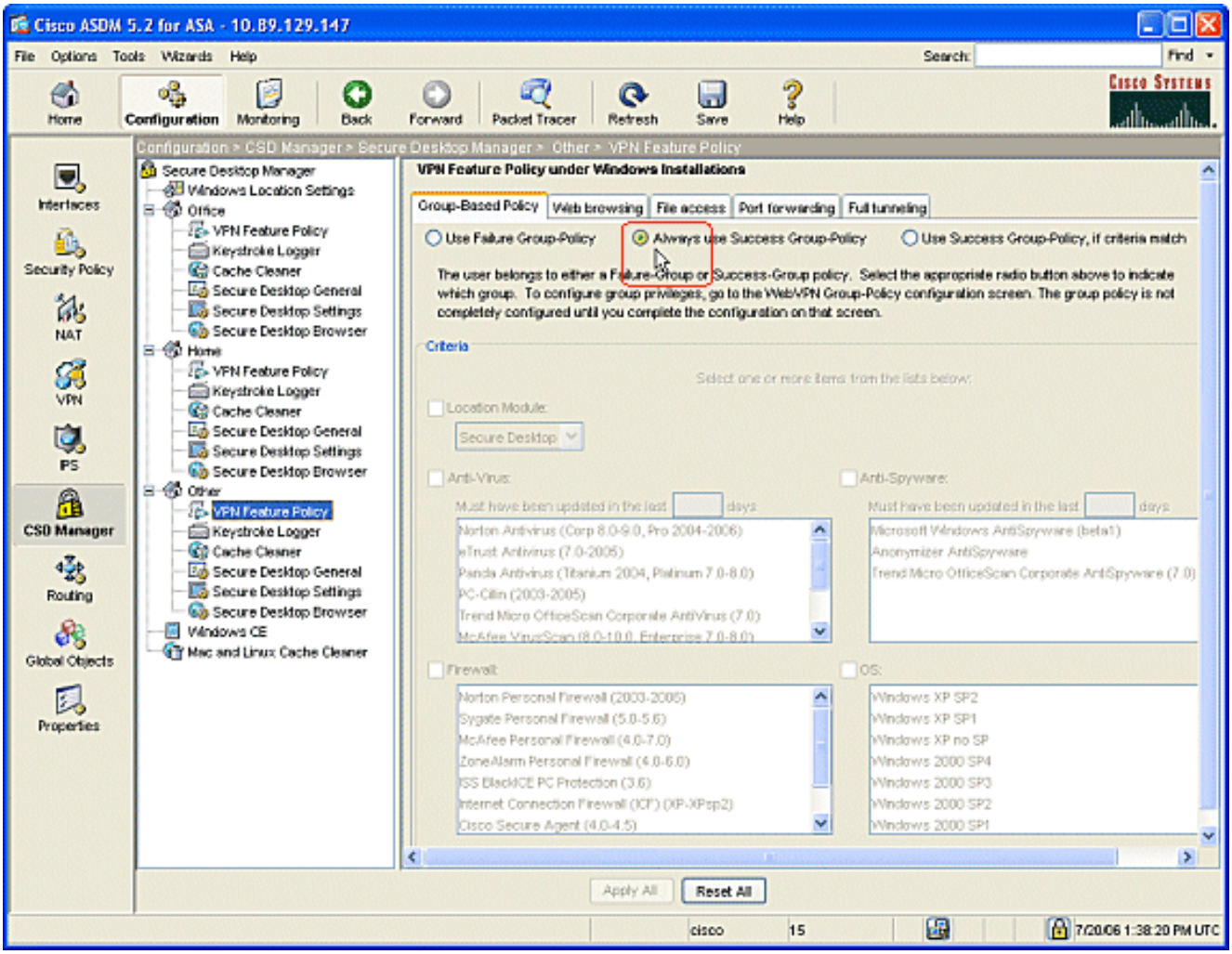
1. Dans le volet de navigation, le clickOffice, et cliquent sur alors la **stratégie de caractéristique VPN**.
2. Cliquez sur l'onglet **basé sur groupe de stratégie**.Cliquez sur **toujours la** case d'option de **stratégie de groupe de succès d'utilisation**.Cliquez sur l'onglet de **navigation web**, et vérifiez la case d'option **toujours activée**.Suivez la même procédure pour l'**accès au fichier, la transmission du port**, et les **pleins** onglets de **Tunnellisation**.Cliquez sur Apply **tous**.Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.



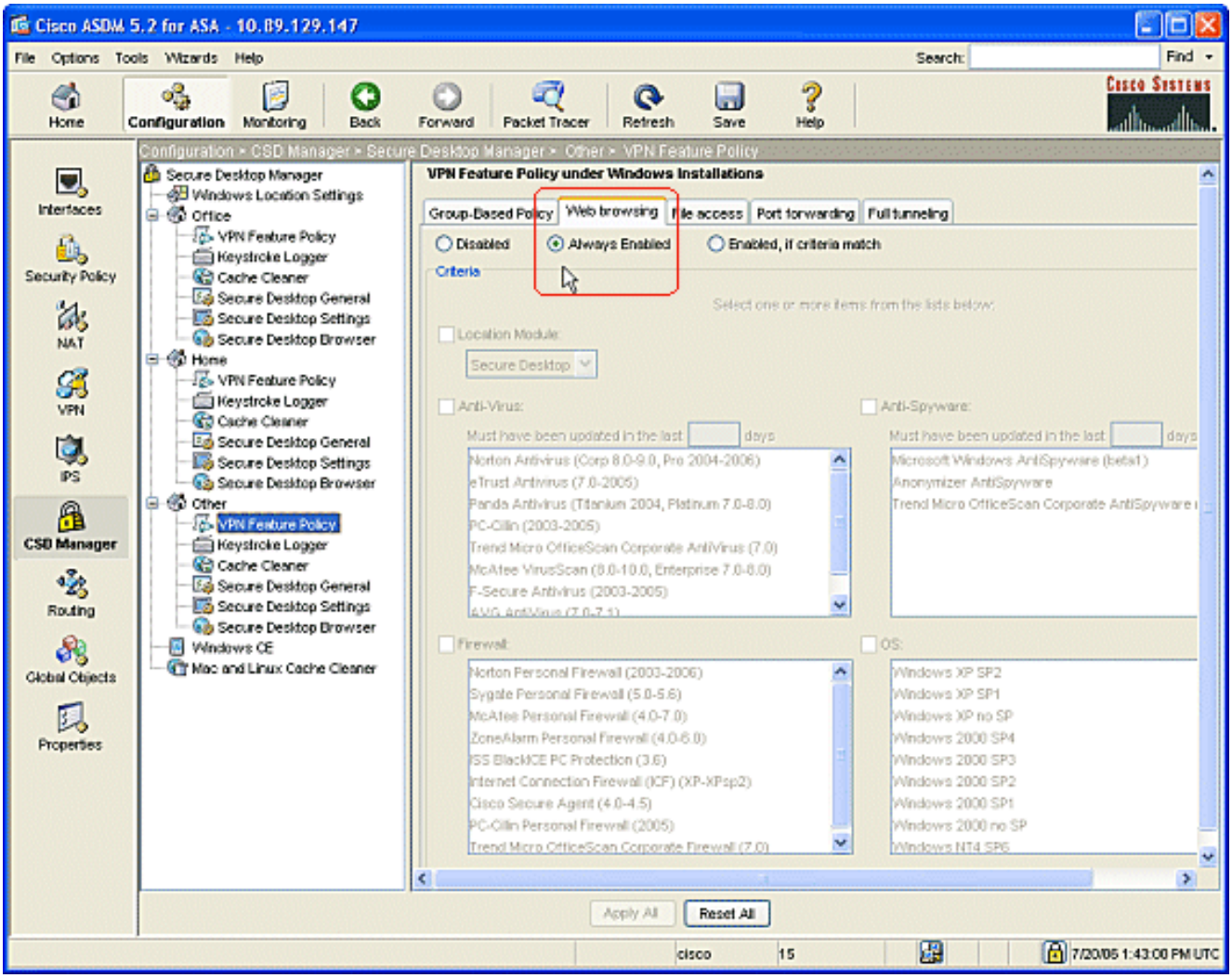
3. Pour des utilisateurs privés, chaque société peut exiger des stratégies spécifiques avant qu'on permette l'accès. Dans le volet de navigation, cliquez sur **à la maison**, et cliquez sur la **stratégie de caractéristique VPN**.Cliquez sur l'onglet **basé sur groupe de stratégie**.Cliquez sur la case d'option de **stratégie de groupe de succès d'utilisation** si les critères préconfigurés apparient, comme une clé de registre spécifique, le nom du fichier connu, ou le certificat numérique.Vérifiez la case à cocher de **module de** theLocation et choisissez le **Secure Desktop**.Choisissez l'**antivirus, l'anti-spyware, le Pare-feu**, et les zones de **SYSTÈME D'EXPLOITATION** selon votre stratégie de sécurité d'entreprise. On ne permettra pas des utilisateurs privés sur le réseau à moins que leurs ordinateurs répondent à vos critères configurés.



4. Dans le volet de navigation, cliquez sur **autre** et cliquez sur la **stratégie de caractéristique VPN**.Cliquez sur l'onglet **basé sur groupe de stratégie**.Cliquez sur **toujours la** case d'option de **stratégie de groupe de succès d'utilisation**.



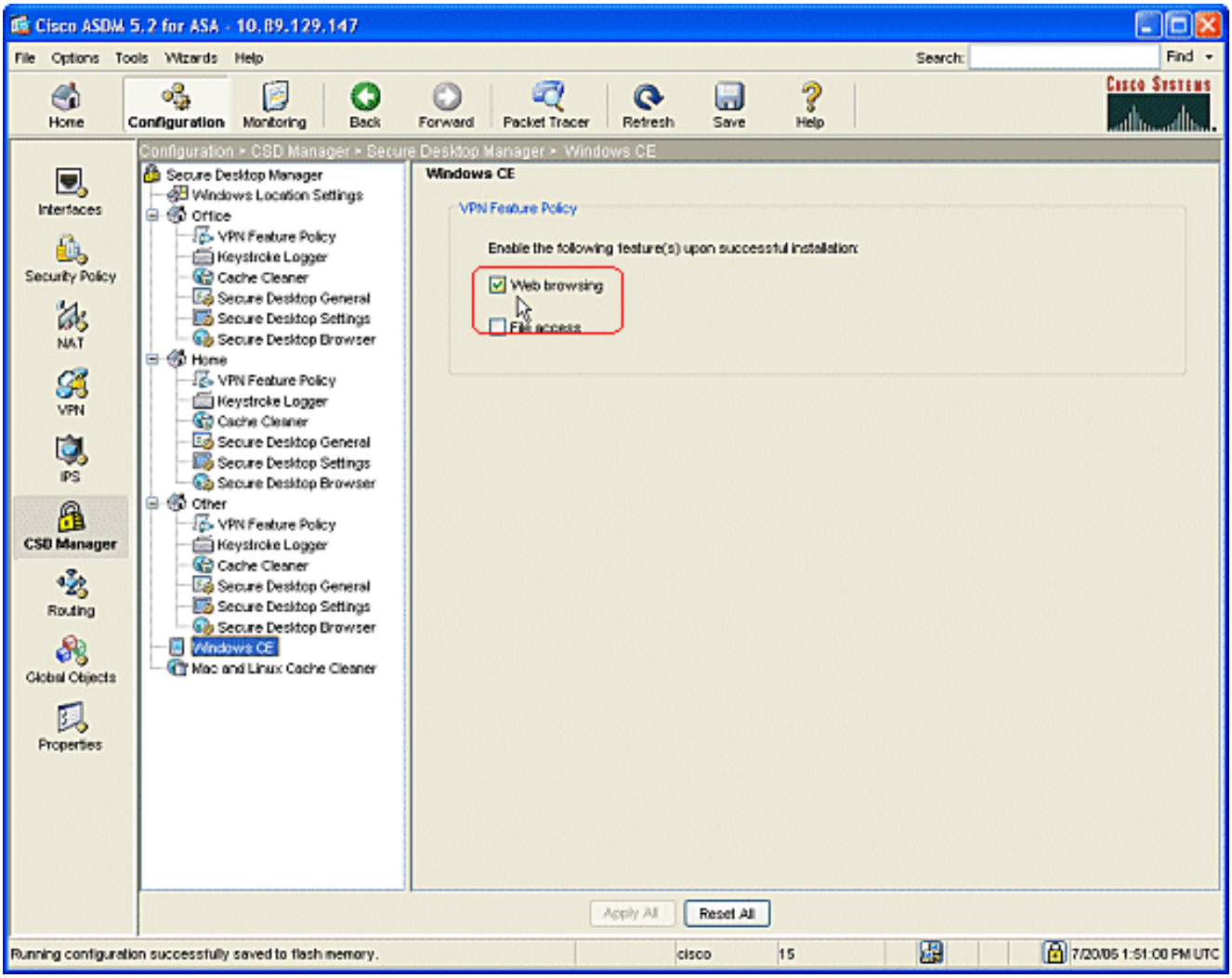
5. Pour des clients dans cet emplacement de **stratégie de caractéristique VPN**, cliquez sur l'onglet de **navigation web**, et cliquez sur le cadran par radio **toujours activé**.Cliquez sur l'onglet d'**accès au fichier**, et cliquez sur la case d'option de **débronchement**.Répétez l'étape avec la **transmission du port** et les **pleins** onglets de **Tunnellisation**.Cliquez sur Apply **tous**.Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.



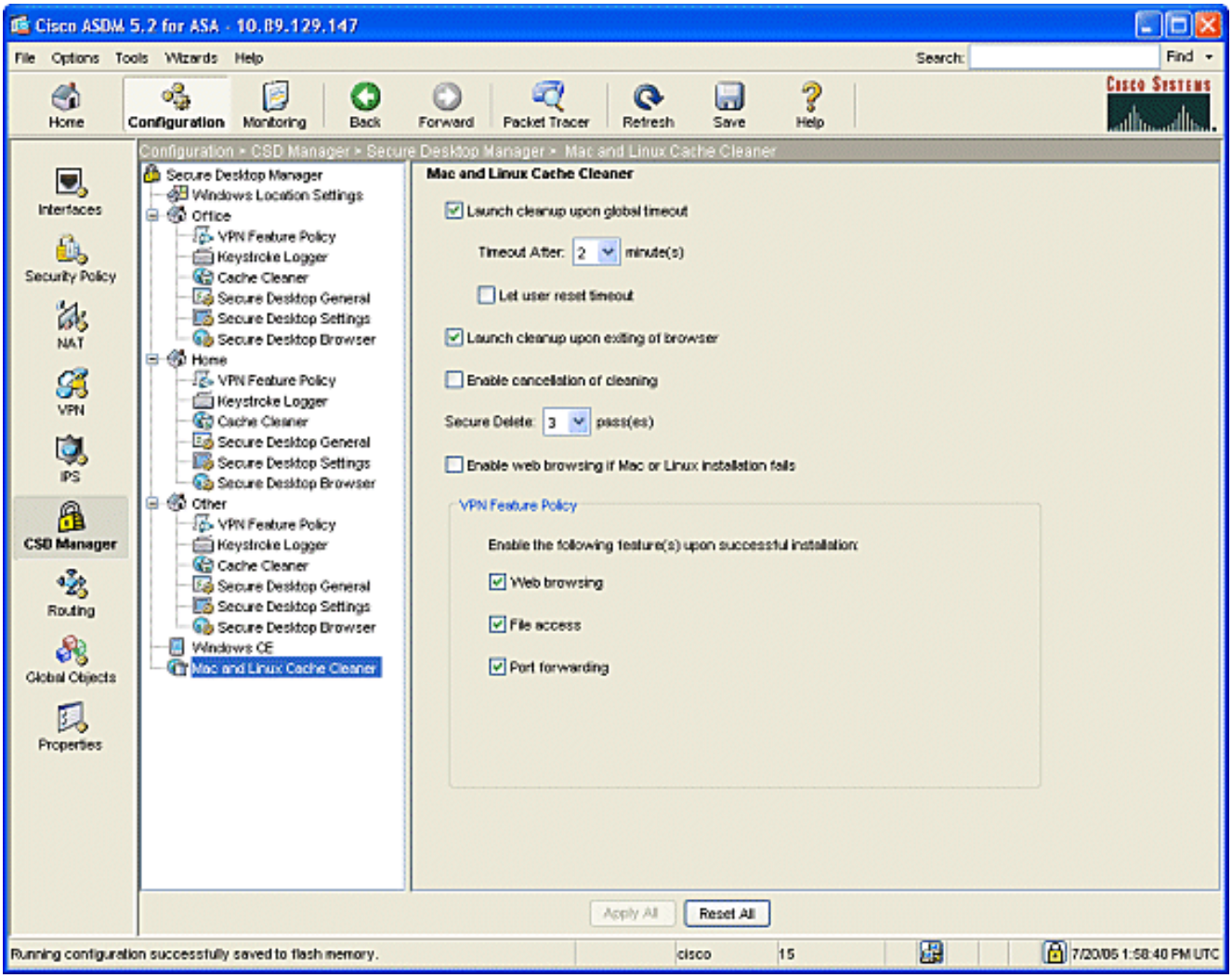
Configurations facultatives pour le Windows CE, le Macintosh, et les clients Linux

Ces configurations sont facultatives.

1. Si vous choisissez le **Windows CE du** volet de navigation, cochez la case de **navigation web**.



2. Si vous choisissez le **décapant de MAC et de cache de Linux du** volet de navigation, vérifiez le **nettoyage de lancement sur le** cadran **global de** radio de **délai d'attente**.Changez le délai d'attente à votre spécification.Sous la région de **stratégie de caractéristique de** theVPN, vérifiez les cadrans par radio de **navigation web, d'accès au fichier**, et de **transmission du port** pour ces
clients.



3. Si vous choisissez le Windows CE ou le décapant de MAC et de cache de Linux, cliquez sur Apply **tous**.
4. Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.

Configurez

Configuration

Cette configuration reflète les modifications ASDM apportées pour activer le CSD : La plupart des configurations CSD sont maintenues dans un fichier séparé sur l'éclair.

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
```

Vérifiez

Employez cette section pour confirmer que vos configurations le client sans client pour VPN SSL, de VPN SSL de client léger, ou de VPN SSL (SVC) fonctionnent correctement.

Testez le CSD avec un PC qui a été configuré avec de divers emplacements de Windows. Chaque test devrait fournir un accès différent selon les stratégies que vous avez configurées dans l'exemple ci-dessus.

Vous pouvez changer le numéro de port et l'interface où Cisco ASA écoute des connexions de webvpn.

- Le port par défaut est 443. Si vous utilisez le port par défaut, l'accès est **adresse IP de https://ASA**.
- L'utilisation d'un port différent change l'accès à l'**adresse IP de https://ASA : newportnumber**.

Commandes

Plusieurs commandes **show** sont associées au WebVPN. Vous pouvez exécuter ces commandes dans l'interface de ligne de commande (CLI) afin d'afficher les statistiques et autres informations. Pour voir l'utilisation des **commandes show** en détail, référez-vous à vérifier la configuration de webvpn.

Remarque: L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Si vous avez des problèmes avec le client distant, vérifiez ces derniers :

1. Bruit-UPS, Javas, et/ou ActiveX sont-ils activés dans le navigateur Web ? Ceux-ci peuvent devoir être activés selon le type de connexion de VPN SSL en service.
2. Le client doit recevoir les Certificats numériques présentés au début de la session.

Commandes

Plusieurs commandes **debug** sont associées à WebVPN. Pour des informations détaillées sur ces commandes, référez-vous en utilisant des commandes de debug de webvpn.

Remarque: L'utilisation des commandes **debug** peut avoir un impact négatif sur votre périphérique Cisco. Avant d'utiliser les commandes **debug**, référez-vous à la section **Informations importantes sur les commandes Debug**.

Informations connexes

- Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500
- Exemple de configuration d'ASA avec WebVPN et authentification unique à l'aide d'ASDM et de NTLMv1
- Support et documentation techniques - Cisco Systems