# Cisco Secure Desktop (CSD 3.1.x) auf ASA 7.2.x für Windows - Konfigurationsbeispiel mit ASDM

## Inhalt



## Einführung

Cisco Secure Desktop (CSD) erweitert die Sicherheit der SSL VPN-Technologie. Der CSD stellt eine separate Partition auf der Workstation eines Benutzers für Sitzungsaktivitäten bereit. Dieser Vault-Bereich wird während der Sitzungen verschlüsselt und am Ende einer SSL VPN-Sitzung vollständig entfernt. Windows kann mit allen Sicherheitsvorteilen von CSD konfiguriert werden. Macintosh, Linux und Windows CE haben nur Zugriff auf die Funktionen Cache Cleaner, Web Browsing und Dateizugriff. Der CSD kann für Windows-, Macintosh-, Windows CE- und Linux-Geräte auf den folgenden Plattformen konfiguriert werden:

- Cisco Adaptive Security Appliance (ASA) der Serie 5500
- Cisco Router mit Cisco IOS® Software-Versionen 12.4(6)T und höher
- Cisco VPN Concentrators der Serie 3000, Version 4.7 und höher
- Cisco WebVPN-Modul für Catalyst Router der Serien 6500 und 7600

**Hinweis:** Mit CSD Release 3.3 können Sie jetzt Cisco Secure Desktop für die Ausführung auf

Remotecomputern konfigurieren, auf denen Microsoft Windows Vista ausgeführt wird. Bisher war Cisco Secure Desktop auf Computer beschränkt, auf denen Windows XP oder 2000 ausgeführt wurde. Weitere Informationen finden Sie im Abschnitt "Neue Funktionserweiterung - Sicherer Desktop unter Vista" in den Versionshinweisen für Cisco Secure Desktop, Version 3.3.

**In diesem Beispiel wird hauptsächlich die Installation und Konfiguration von CSD auf der ASA 5500-Serie für Windows-Clients beschrieben. Optionale Konfigurationen für Windows CE-, Mac- und Linux-Clients werden zur Fertigstellung hinzugefügt.**

Der CSD wird in Verbindung mit der SSL VPN-Technologie (Clientless SSL VPN, Thin-Client SSL VPN oder SSL VPN Client (SVC)) verwendet. CSD erhöht die Sicherheit von SSL VPN-Technologien.

# Voraussetzungen

## Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

### Anforderungen für das ASA-Gerät

- Cisco CSD Version 3.1 oder höher
- Cisco ASA Software Version 7.1.1 oder höher
- Cisco Adaptive Security Device Manager (ASDM) Version 5.1.1 oder höher**Hinweis:** CSD Version 3.2 unterstützt nur auf ASA Version 8.x**Hinweis:** Informationen zur Konfiguration der ASA durch den ASDM finden Sie unter Zulassen von HTTPS-Zugriff für ASDM.

### Anforderungen an Client-Computer

- Remote-Clients sollten über lokale Administratorberechtigungen verfügen. Sie ist nicht erforderlich, wird jedoch nachdrücklich empfohlen.
- Remote-Clients müssen über Java Runtime Environment (JRE) Version 1.4 oder höher verfügen.
- Remote-Client-Browser: Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 oder Firefox 1.0
- Cookies aktiviert und Popups auf Remote-Clients zugelassen

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte begannen mit einer leeren (Standard-)Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen. Bei den in dieser Konfiguration verwendeten

IP-Adressen handelt es sich um RFC 1918-Adressen. Diese IP-Adressen sind im Internet nicht legal und dürfen nur in einer Testlabor-Umgebung verwendet werden.

### Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

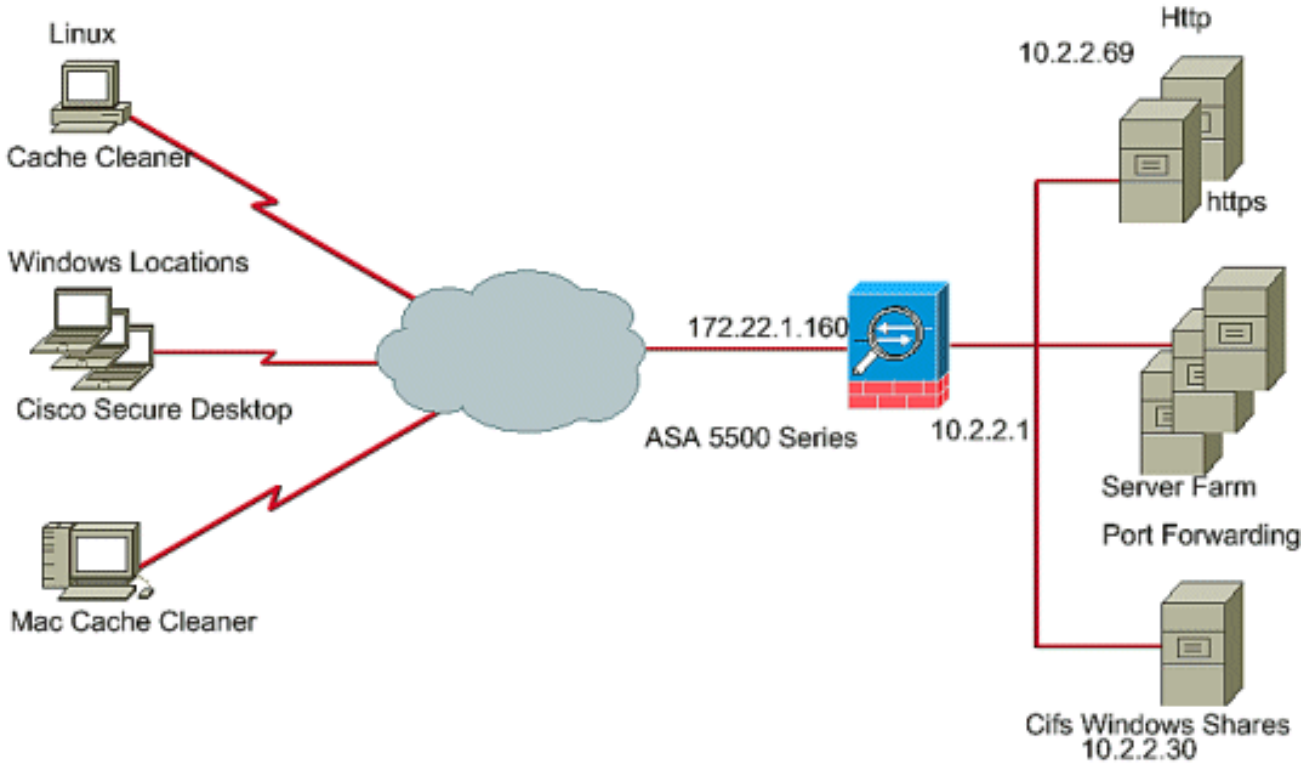
## Hintergrundinformationen

Der CSD arbeitet mit SSL VPN-Technologie, daher sollten vor der Konfiguration des CSD Clientless, Thin-Client oder SVC aktiviert werden.

### Netzwerkdiagramm

Verschiedene Windows-Standorte können mit allen Sicherheitsaspekten des CSD konfiguriert werden. Macintosh, Linux und Windows CE haben nur Zugriff auf den Cache Cleaner und/oder das Surfen im Internet und den Dateizugriff.

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:




## Konfigurieren des CSD auf der ASA für Windows-Clients

Konfigurieren Sie den CSD auf der ASA für Windows-Clients mit fünf Hauptschritten:

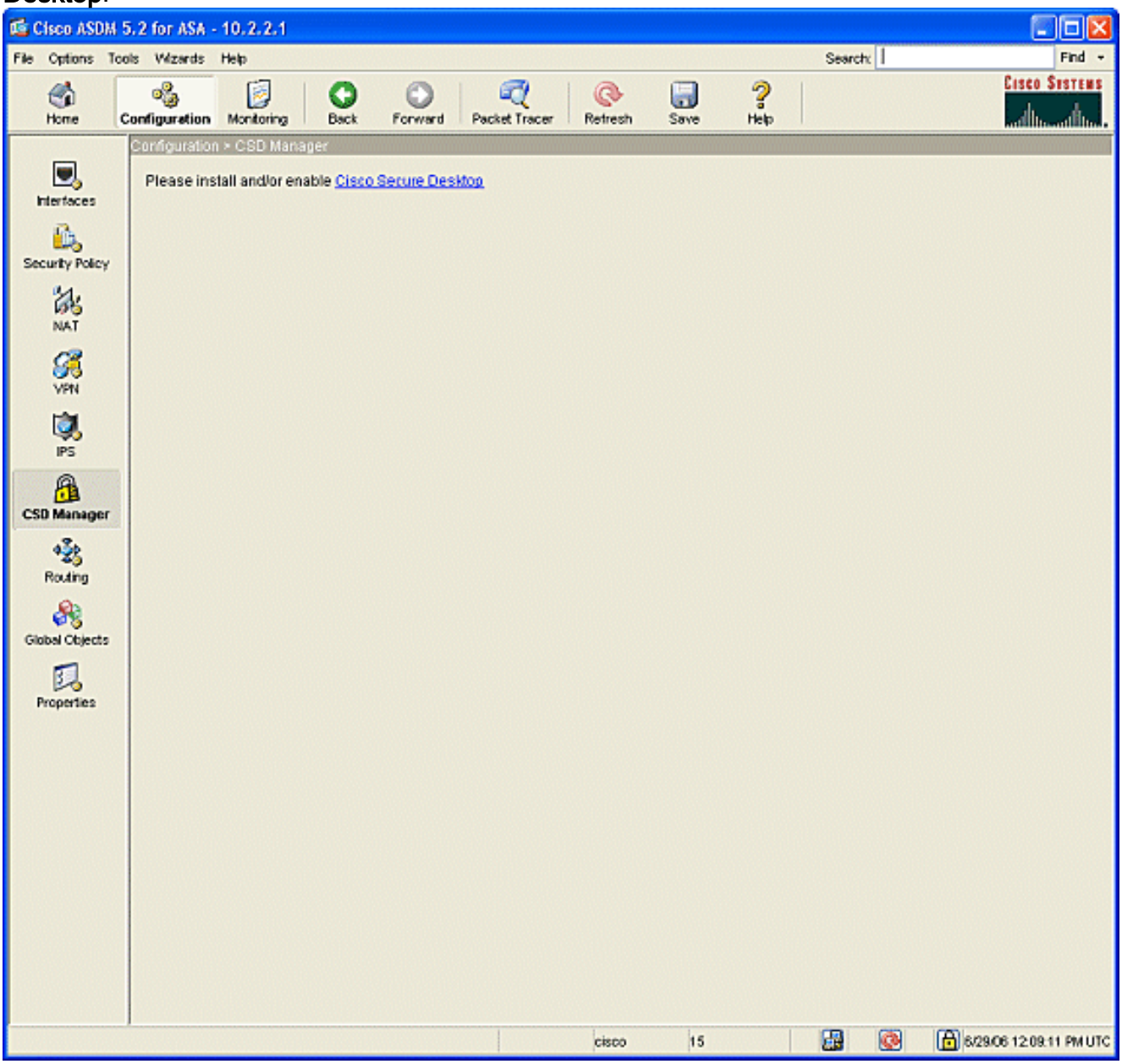
- Holen Sie die CSD-Software auf der Cisco ASA ein, installieren und aktivieren Sie sie.
- Definieren von Windows-Speicherorten.
- Definieren der Windows-Standortidentifizierung.
- Konfigurieren von Windows-Standortmodulen

- Konfigurieren der Standortfunktionen von Windows
- Optionale Konfiguration für Windows CE-, Macintosh- und Linux-Clients.

## CSD-Software beziehen, installieren und aktivieren

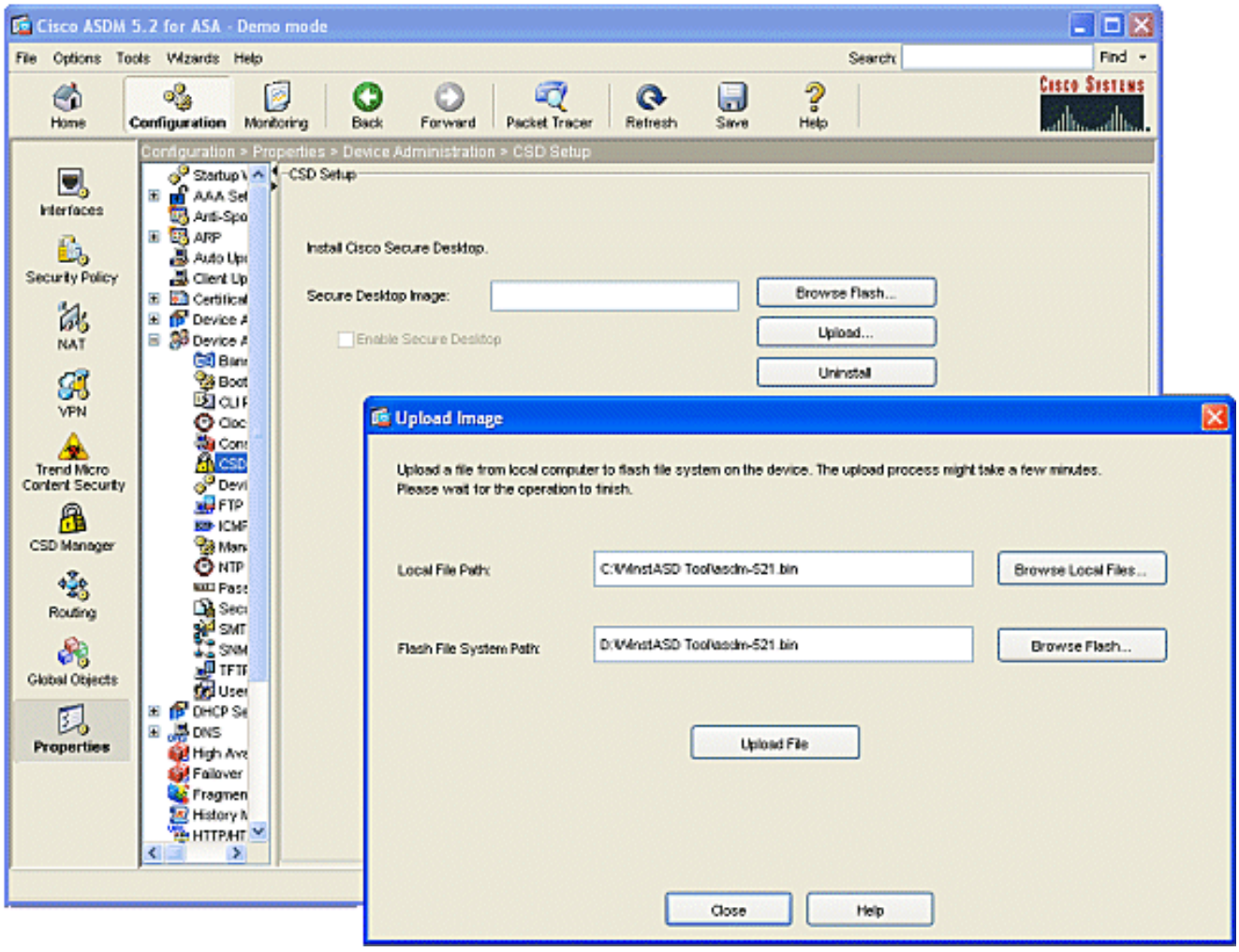
Gehen Sie wie folgt vor, um die CSD-Software auf der Cisco ASA zu erhalten, zu installieren und zu aktivieren.

1. Laden Sie die CSD Software securedesktop-asa*.pkg und die Readme-Dateien von der Cisco Software Download-Website auf Ihre Managementkonsole herunter.
2. Melden Sie sich bei ASDM an, und klicken Sie auf die Schaltfläche **Konfiguration**. Klicken Sie im linken Menü auf die Schaltfläche **CSD Manager**, und klicken Sie auf den Link **Cisco Secure Desktop**.




3. Klicken Sie auf **Hochladen**, um das Fenster Bild hochladen anzuzeigen.Geben Sie entweder den Pfad der neuen .pkg-Datei auf der Verwaltungsstation ein, oder klicken Sie auf **Lokale Dateien durchsuchen**, um die Datei zu suchen.Geben Sie entweder den Speicherort auf Flash ein, in dem die Datei gespeichert werden soll, oder klicken Sie auf **Flash**

**durchsuchen**.Klicken Sie auf **Datei hochladen**.Wenn Sie dazu aufgefordert werden, klicken Sie auf **OK > Schließen >**
**OK**.

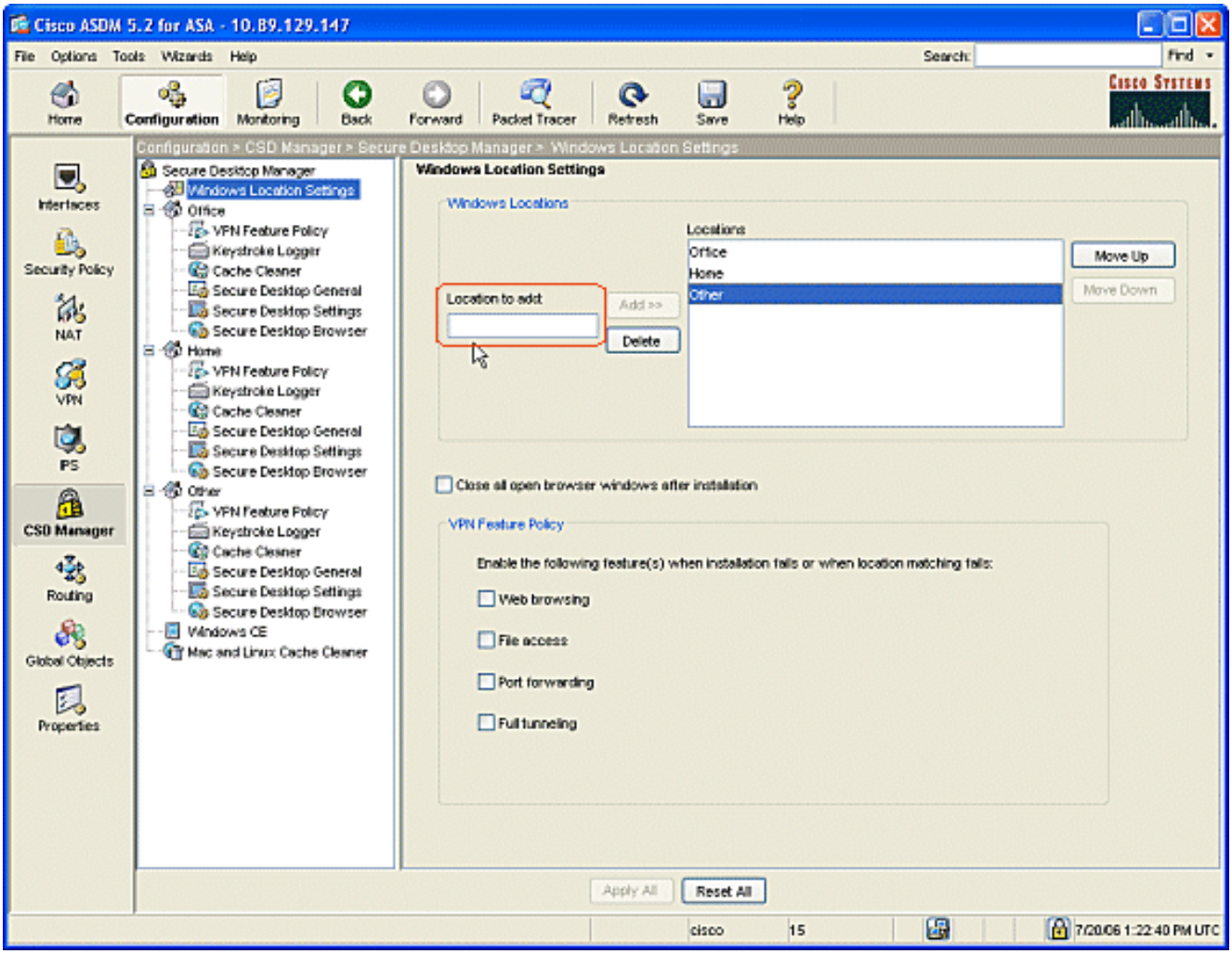



4. Wenn das Client-Image zum Flash geladen wurde, aktivieren Sie das Kontrollkästchen **SSL VPN-Client aktivieren**, und klicken Sie dann auf **Apply**.
5. Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.

## Definieren von Windows-Speicherorten

Führen Sie diese Schritte aus, um Windows-Speicherorte zu definieren.

1. Klicken Sie auf die Schaltfläche **Konfiguration**.
2. Klicken Sie im linken Menü auf die Schaltfläche **CSD Manager**, und klicken Sie auf den Link **Cisco Secure Desktop**.
3. Klicken Sie im Navigationsbereich auf **Windows Location Settings**.
4. Geben Sie einen Standortnamen in das Feld Speicherort zum Hinzufügen ein, und klicken Sie auf **Hinzufügen**.Beachten Sie die drei Standorte in diesem Beispiel: Büro, Home Office u. a.Office stellt Workstations dar, die sich innerhalb der Sicherheitsgrenze des Unternehmens befinden.Home repräsentiert Benutzer, die von zu Hause aus arbeiten.Andere repräsentieren einen beliebigen Standort, der nicht von den beiden genannten Standorten stammt.

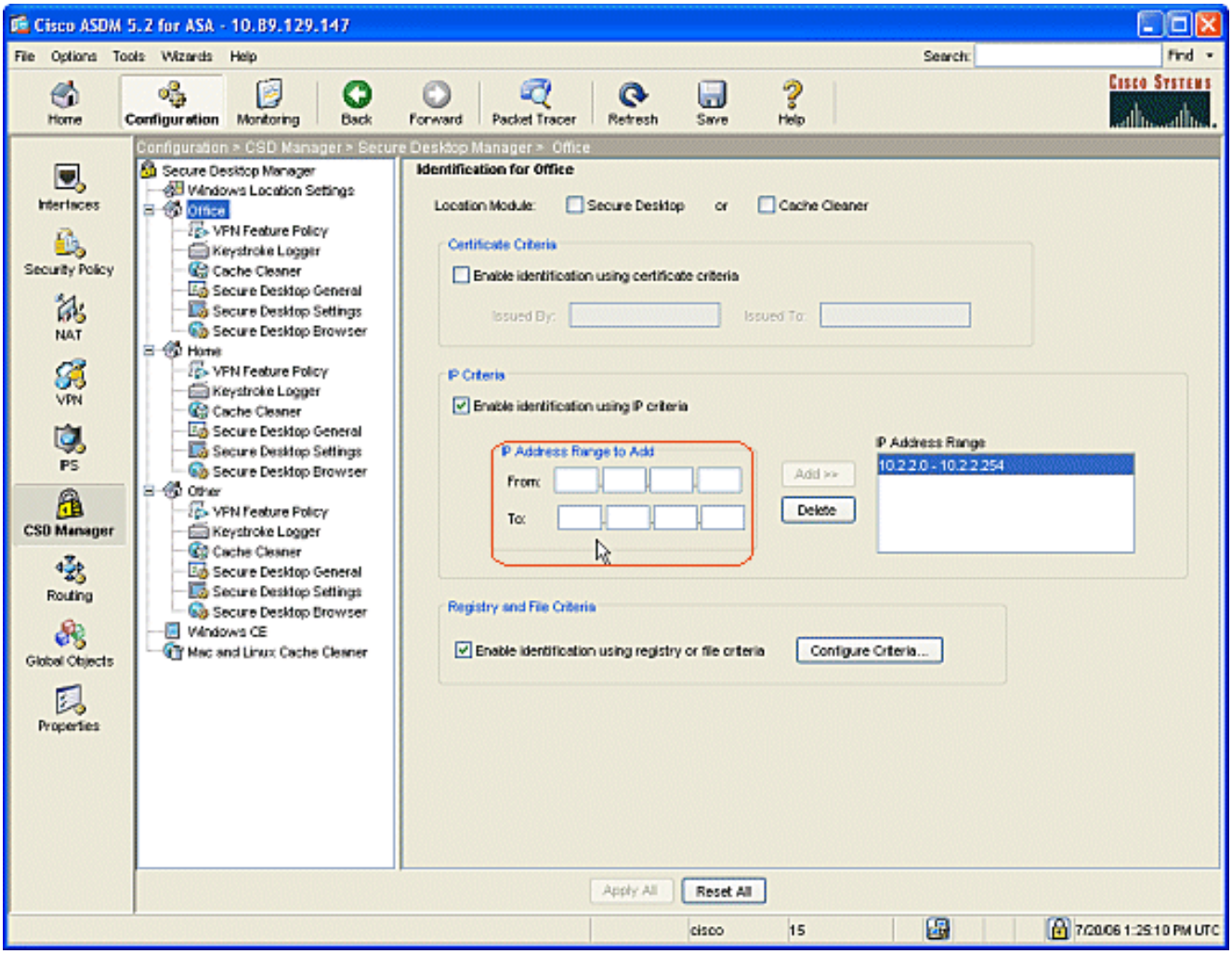



5. Erstellen Sie Ihre eigenen Standorte abhängig vom Layout Ihrer Netzwerkarchitektur für Vertrieb, Gäste, Partner und andere.
6. Wenn Sie Windows-Speicherorte erstellen, wird der Navigationsbereich mit konfigurierbaren Modulen für jeden neuen Speicherort erweitert. Klicken Sie auf **Alle anwenden**.
7. Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.

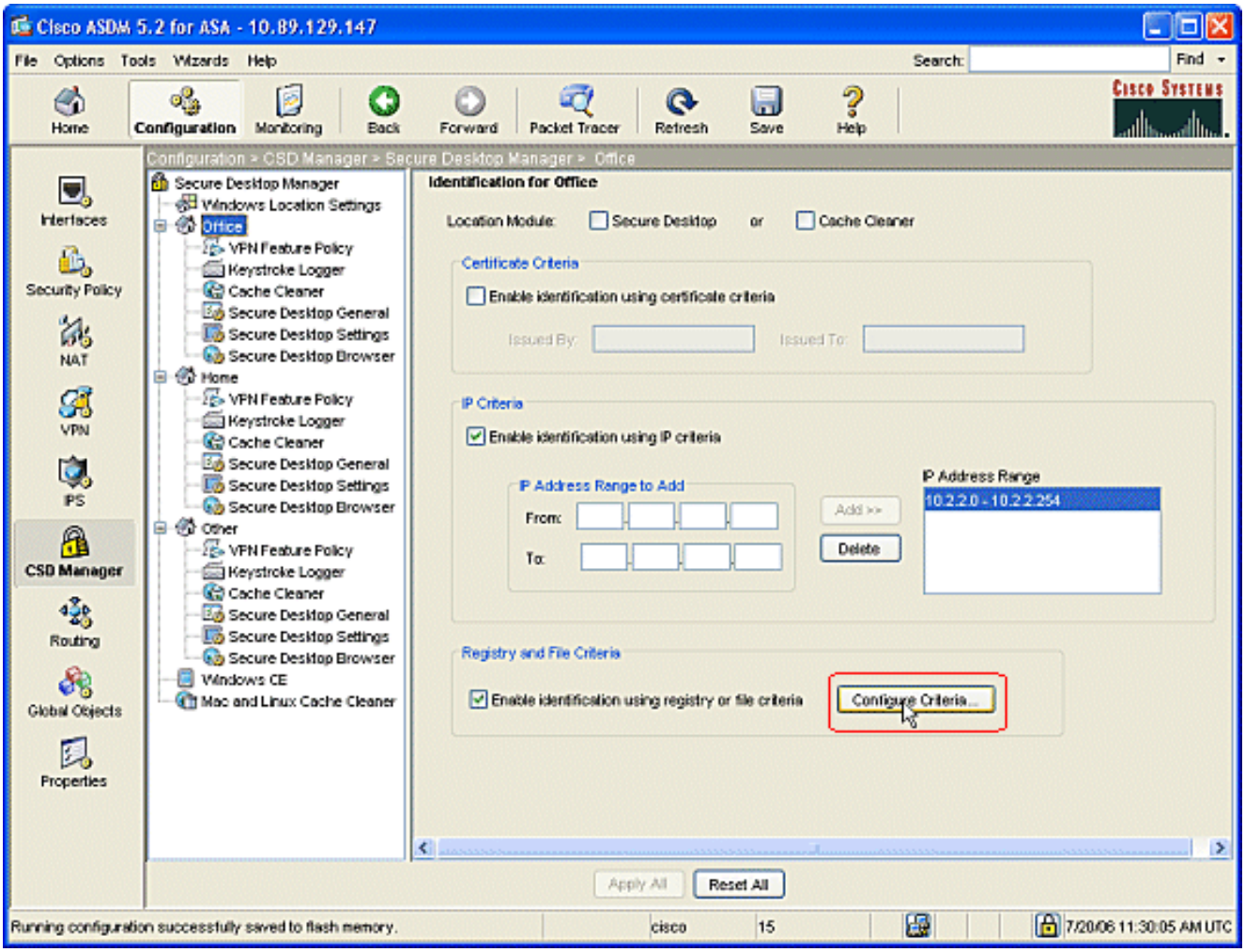
## Windows-Standortidentifizierung

Führen Sie diese Schritte aus, um die Windows-Standortidentifizierung zu definieren.

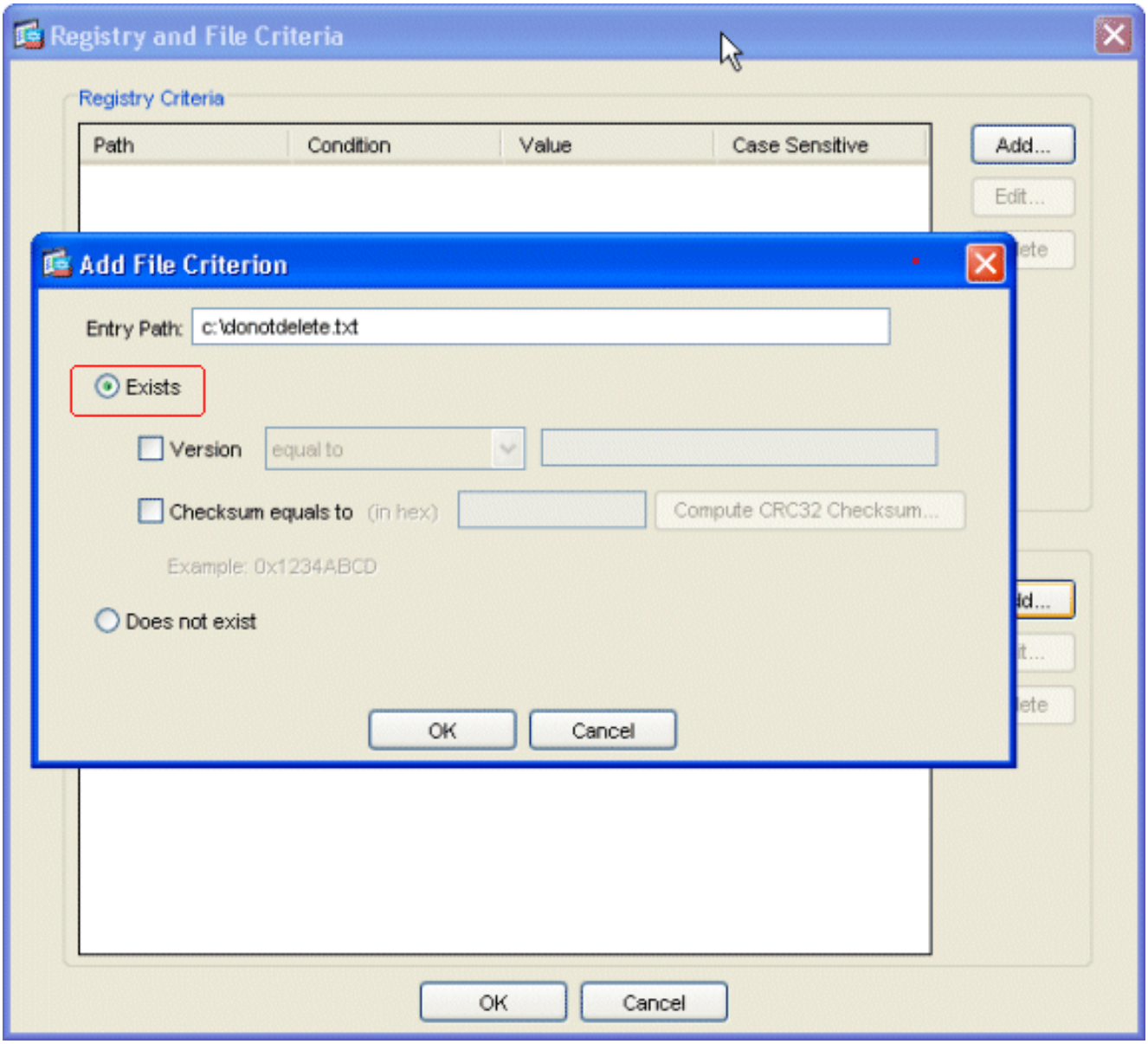
1. Identifizieren Sie die Speicherorte, die unter Windows-Speicherorte definieren erstellt wurden.



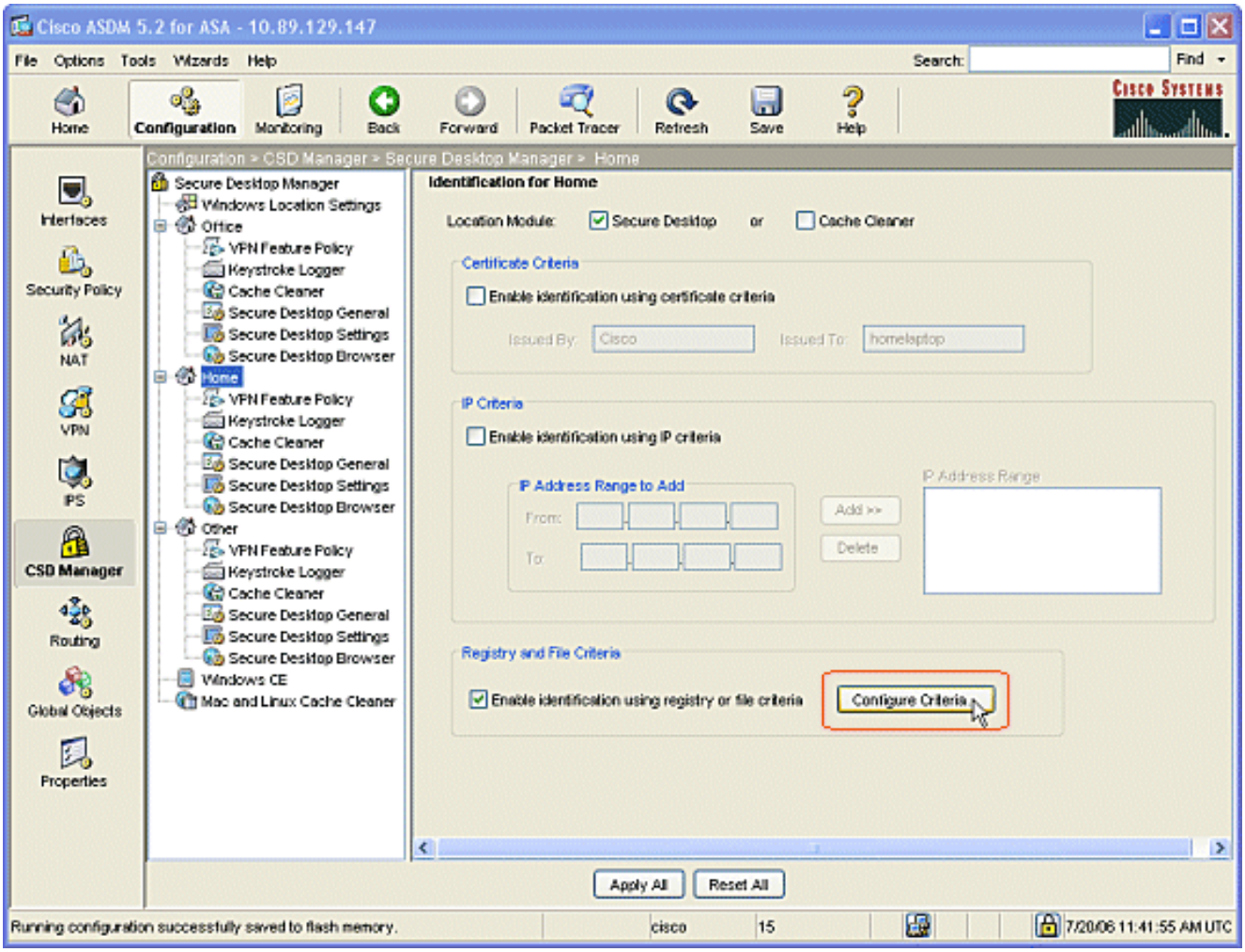

2. Um den Speicherort Office zu identifizieren, klicken Sie im Navigationsbereich auf **Office**.Deaktivieren Sie **Secure Desktop** und **Cache Cleaner**, da es sich um interne Computer handelt.Aktivieren Sie **Identifikation mithilfe von IP-Kriterien aktivieren**.Geben Sie die IP-Adressbereiche Ihrer internen Computer ein.Aktivieren Sie **Identifikation mithilfe von Registrierung oder Dateikriterien aktivieren**. Dies unterscheidet interne Büromitarbeiter von gelegentlichen Gästen im
Netzwerk.



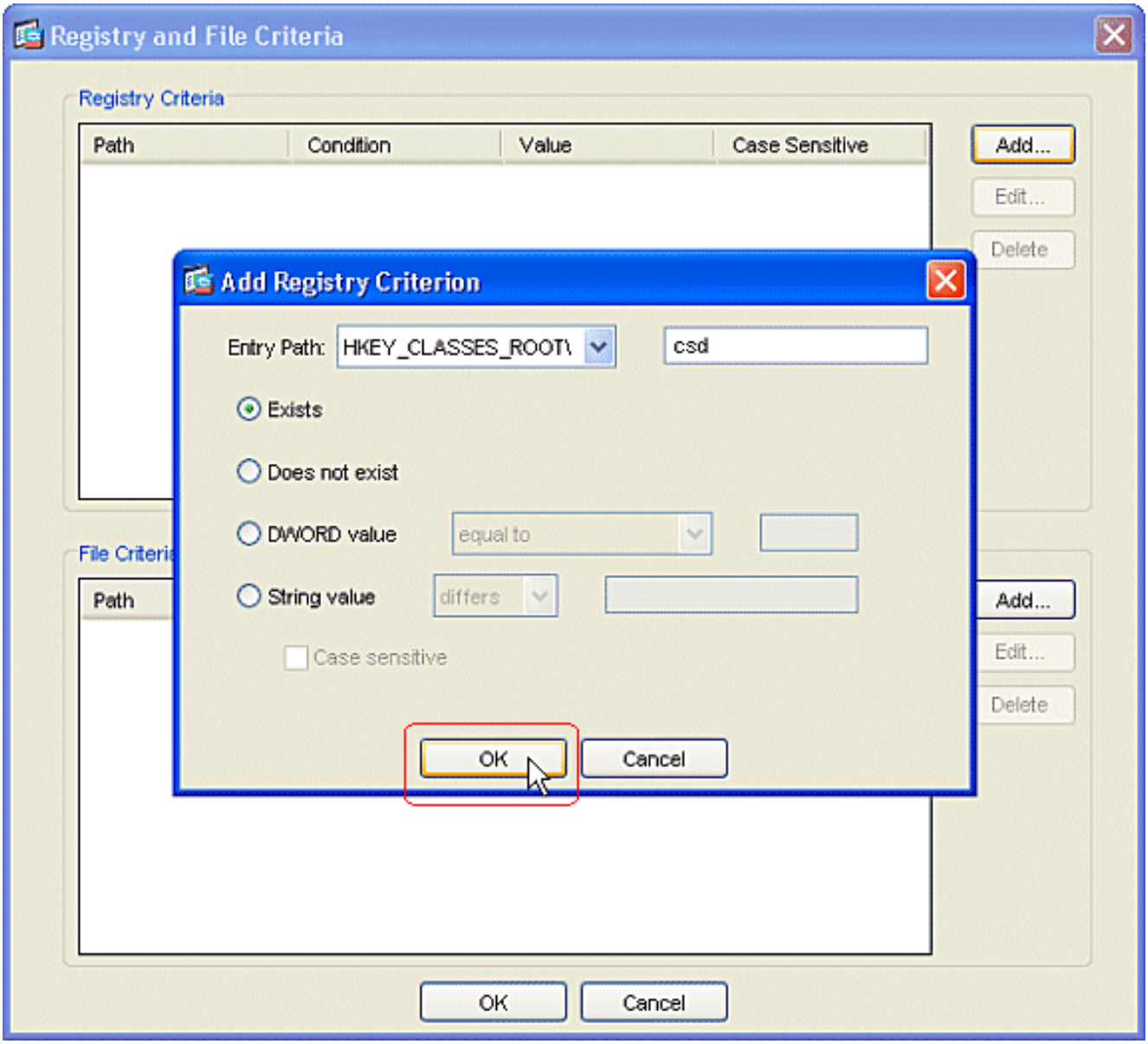

3. Klicken Sie auf **Kriterien konfigurieren**. Ein einfaches Beispiel für eine Datei "DoNotDelete.txt" ist konfiguriert. Diese Datei muss auf Ihren internen Windows-Computern vorhanden sein und ist lediglich ein Platzhalter. Sie können auch einen Windows-Registrierungsschlüssel konfigurieren, um interne Bürocomputer zu identifizieren. Klicken Sie im Fenster Dateikriterien hinzufügen auf **OK**. Klicken Sie im Fenster Registrierung und Dateikriterien auf
**OK**.



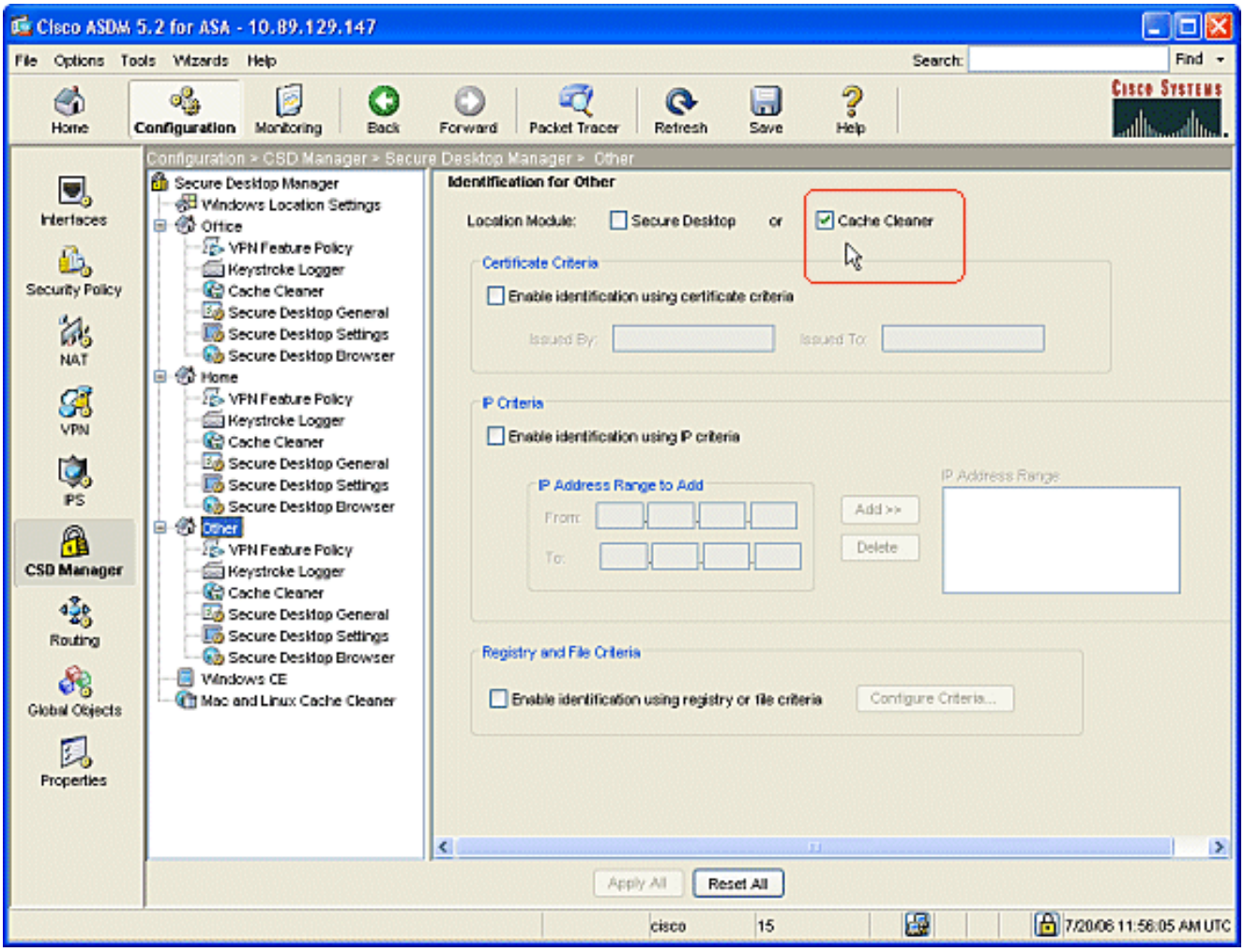

4. Klicken Sie im Fenster Identification for Office (Identifizierung für Office) **auf Alles anwenden**. Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.
5. Um den Speicherort Home zu identifizieren, klicken Sie im Navigationsbereich auf **Home**.Aktivieren Sie **Identifikation mithilfe von Registrierung oder Dateikriterien aktivieren**.Klicken Sie auf **Kriterien konfigurieren**.




6. Clients auf Heimcomputern müssen mit diesem Registrierungsschlüssel von einem Administrator konfiguriert worden sein. Klicken Sie im Fenster Registrierungskriterien hinzufügen auf **OK**. Klicken Sie im Fenster Registrierung und Dateikriterien auf **OK**.



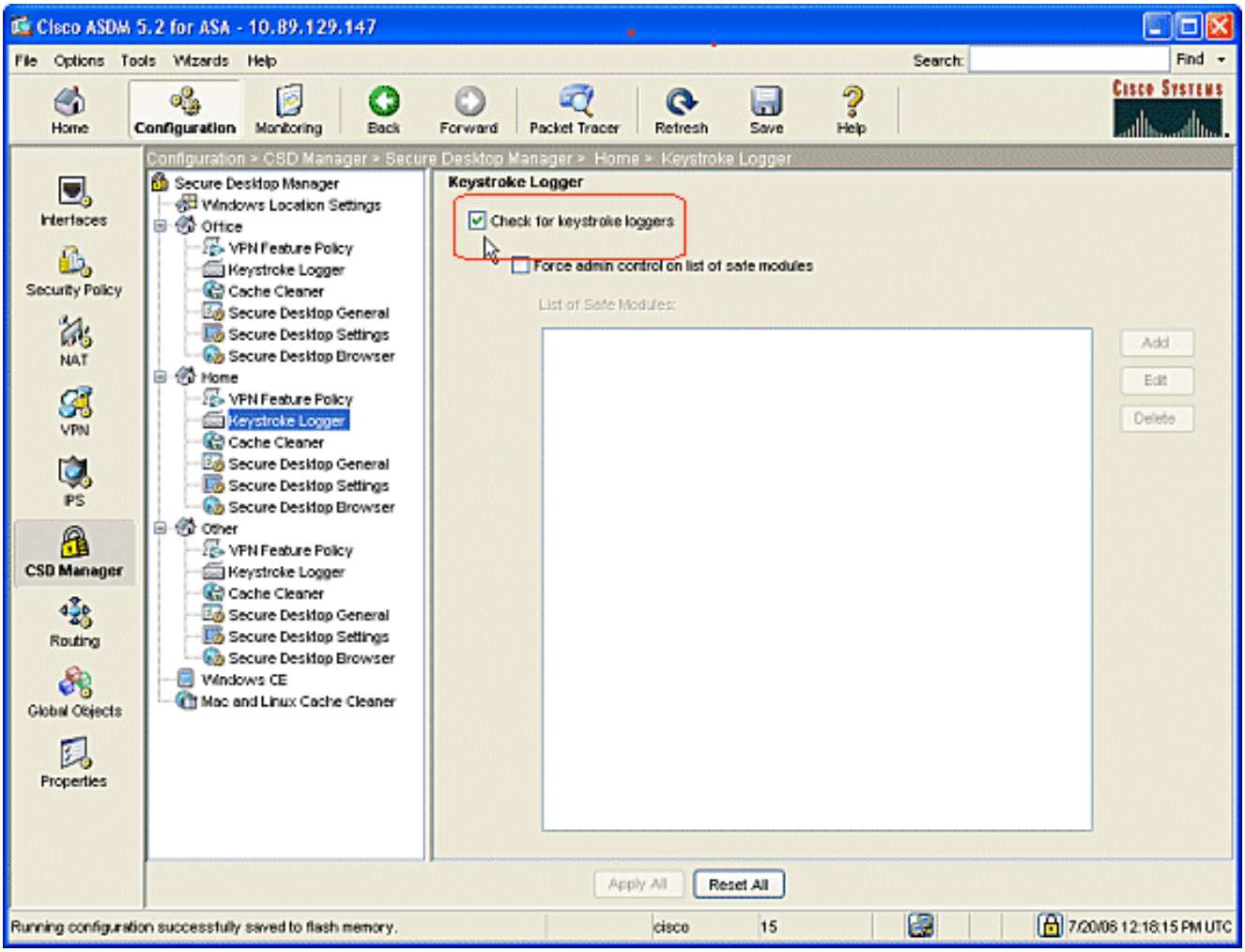

7. Aktivieren Sie unter Location Module (Standortmodul) die Option **Secure Desktop**. Klicken Sie im Fenster Identification for Home (Identifikation für die Startseite) auf **Apply All (Alle anwenden)**. Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.
8. Um den Speicherort **Andere** zu identifizieren, klicken Sie im Navigationsbereich auf **Andere**.Aktivieren Sie nur das Kontrollkästchen **Cache Cleaner**, und deaktivieren Sie alle anderen Kontrollkästchen.Klicken Sie im Fenster Identification for Other (Identifizierung für Andere) auf **Apply All (Alle anwenden)**.Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu
übernehmen.



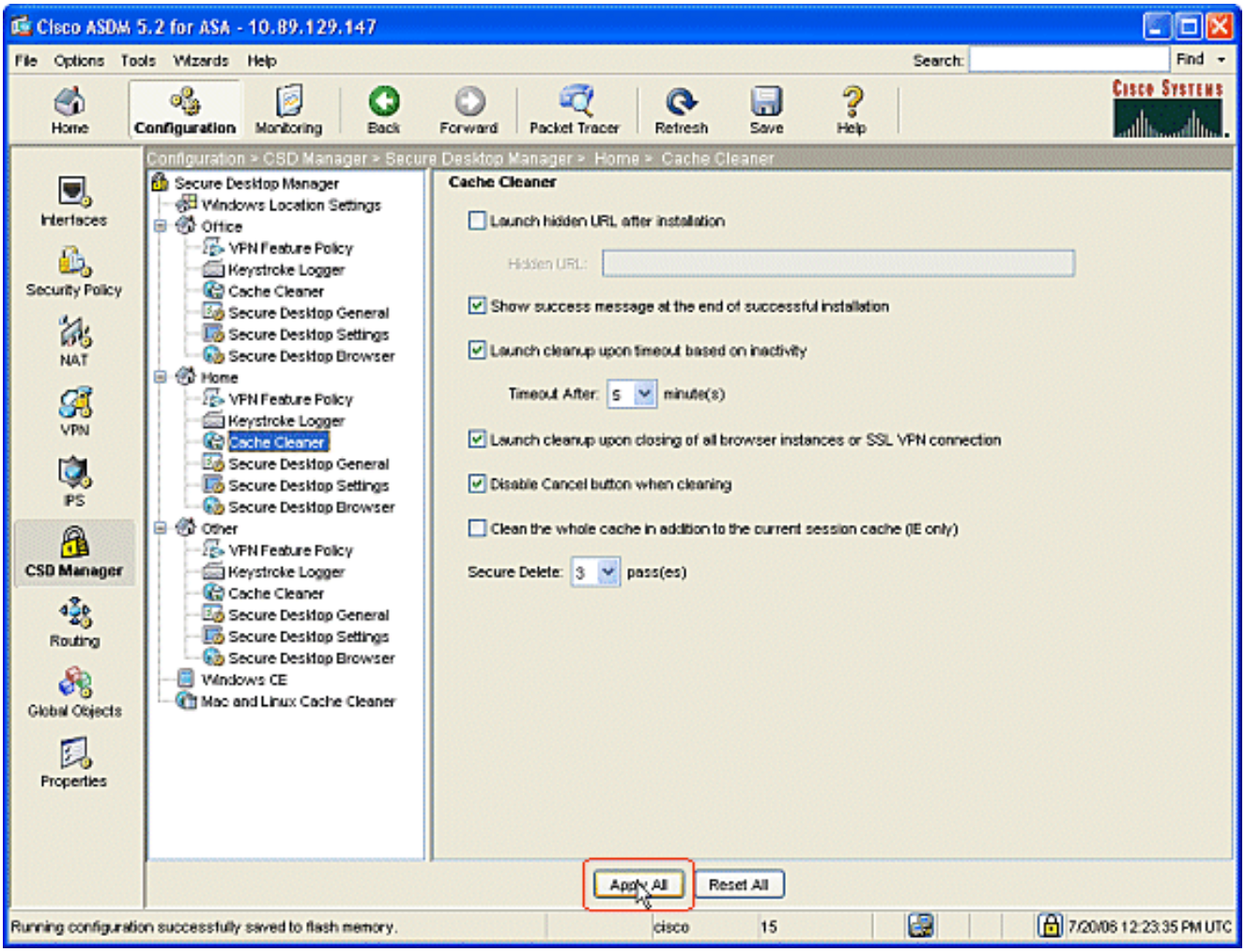

## Windows-Standortmodul konfigurieren

Führen Sie diese Schritte aus, um die Module an jedem der drei von Ihnen erstellten Speicherorte zu konfigurieren.

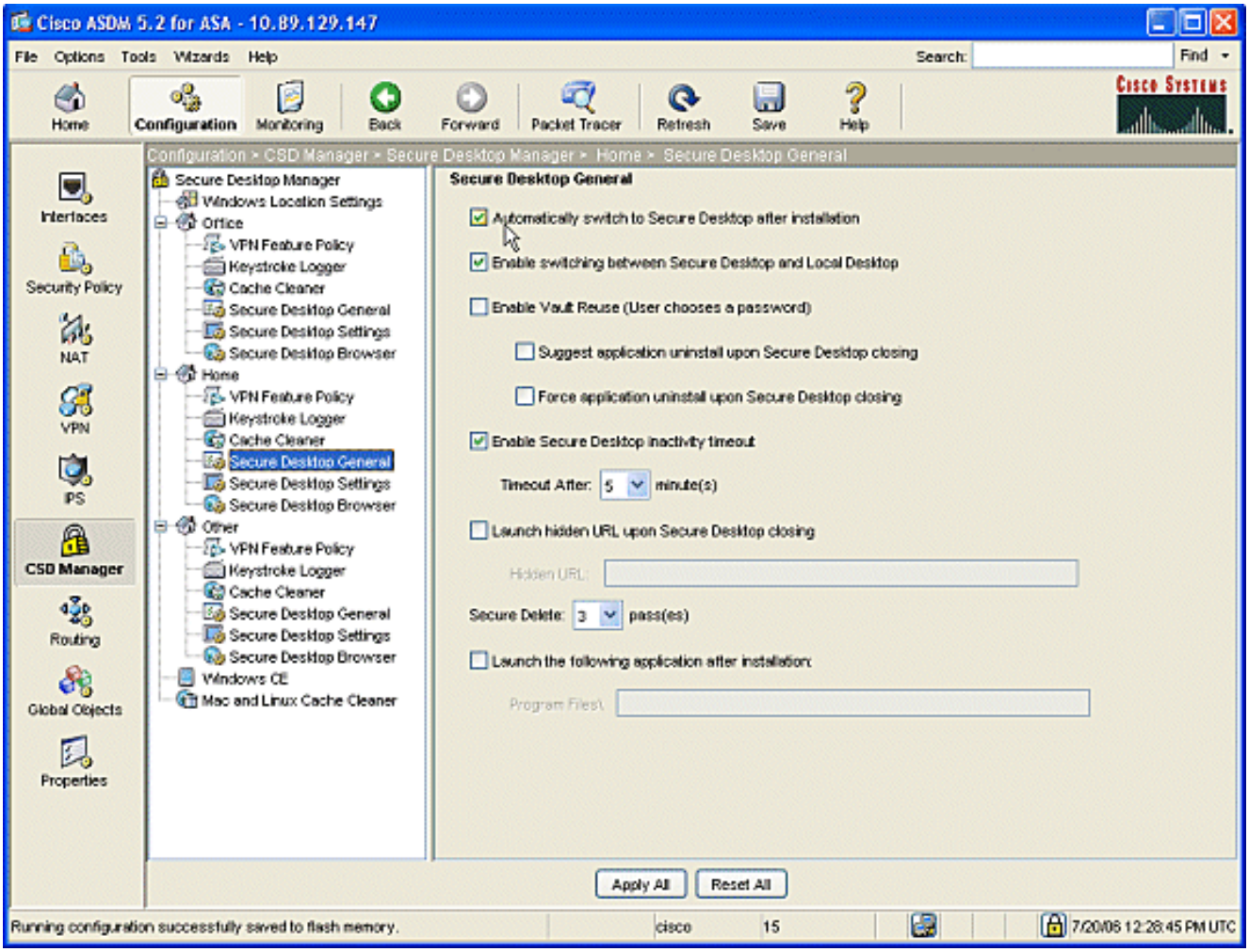
1. Für Office-Clients sollten Sie nichts tun, da Secure Desktop und Cache Cleaner in den vorherigen Schritten nicht ausgewählt wurden. Mit der ASDM-Anwendung können Sie den Cache Cleaner auch dann konfigurieren, wenn er in einem vorherigen Schritt nicht ausgewählt wurde. Behalten Sie die Standardeinstellungen für die Office-Speicherorte bei.**Hinweis:** Die VPN-Feature-Richtlinie wird in diesem Schritt nicht behandelt, wird jedoch in einem weiteren Schritt für alle Standorte besprochen.
2. Für Home-Clients klicken Sie im Navigationsbereich auf **Home** und **Keystroke Logger**.Aktivieren Sie im Fenster Keystroke Logger die Option **Check for keystroke Loggers (Tastenaufzeichner suchen)**.Klicken Sie im Fenster Keystroke Logger auf **Alles anwenden**.Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.



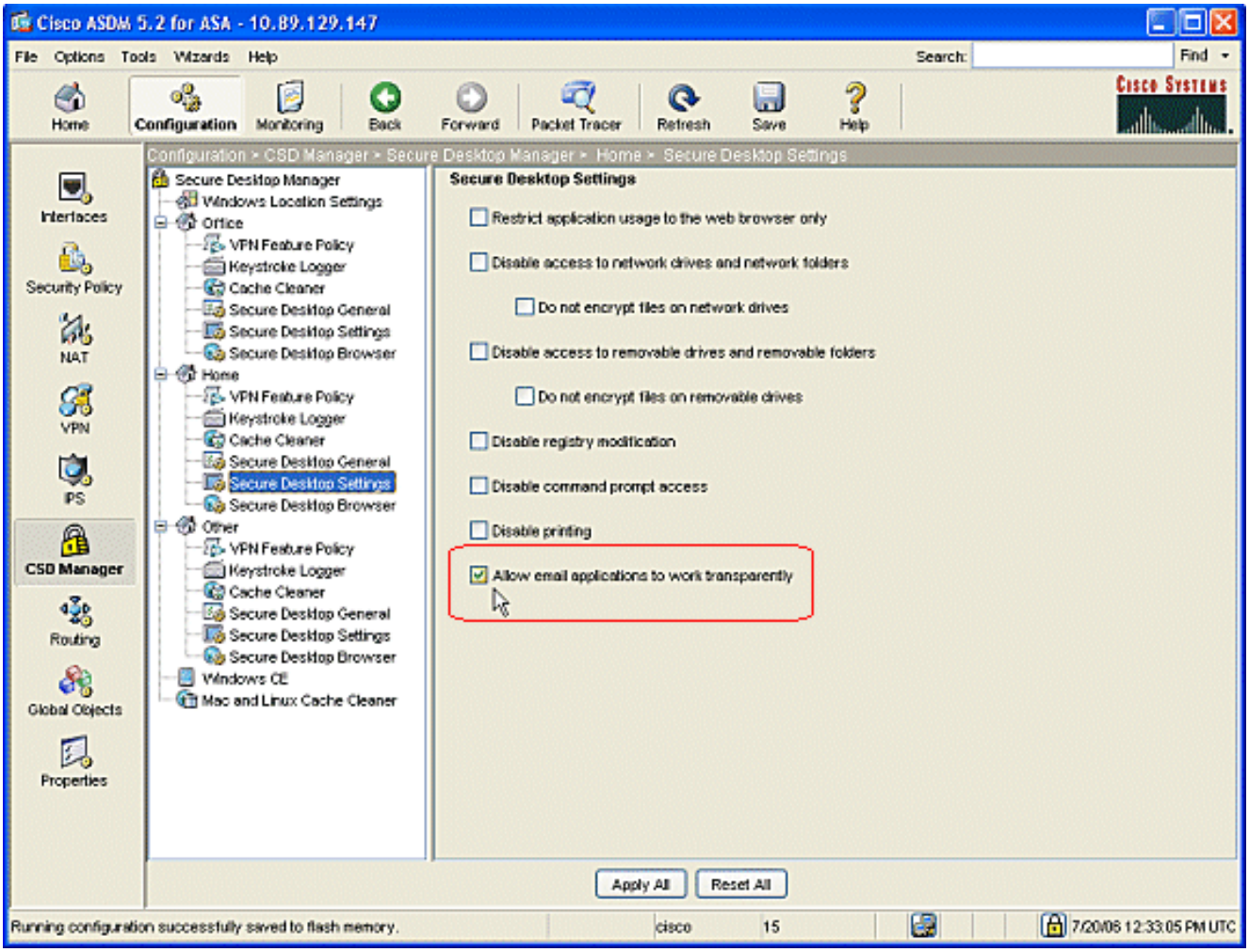

3. Wählen Sie unter Home **Cache Cleaner** und die Parameter für Ihre Umgebung aus.




4. Wählen Sie unter Home die Option **Secure Desktop General** und die Parameter für Ihre Umgebung
   aus.



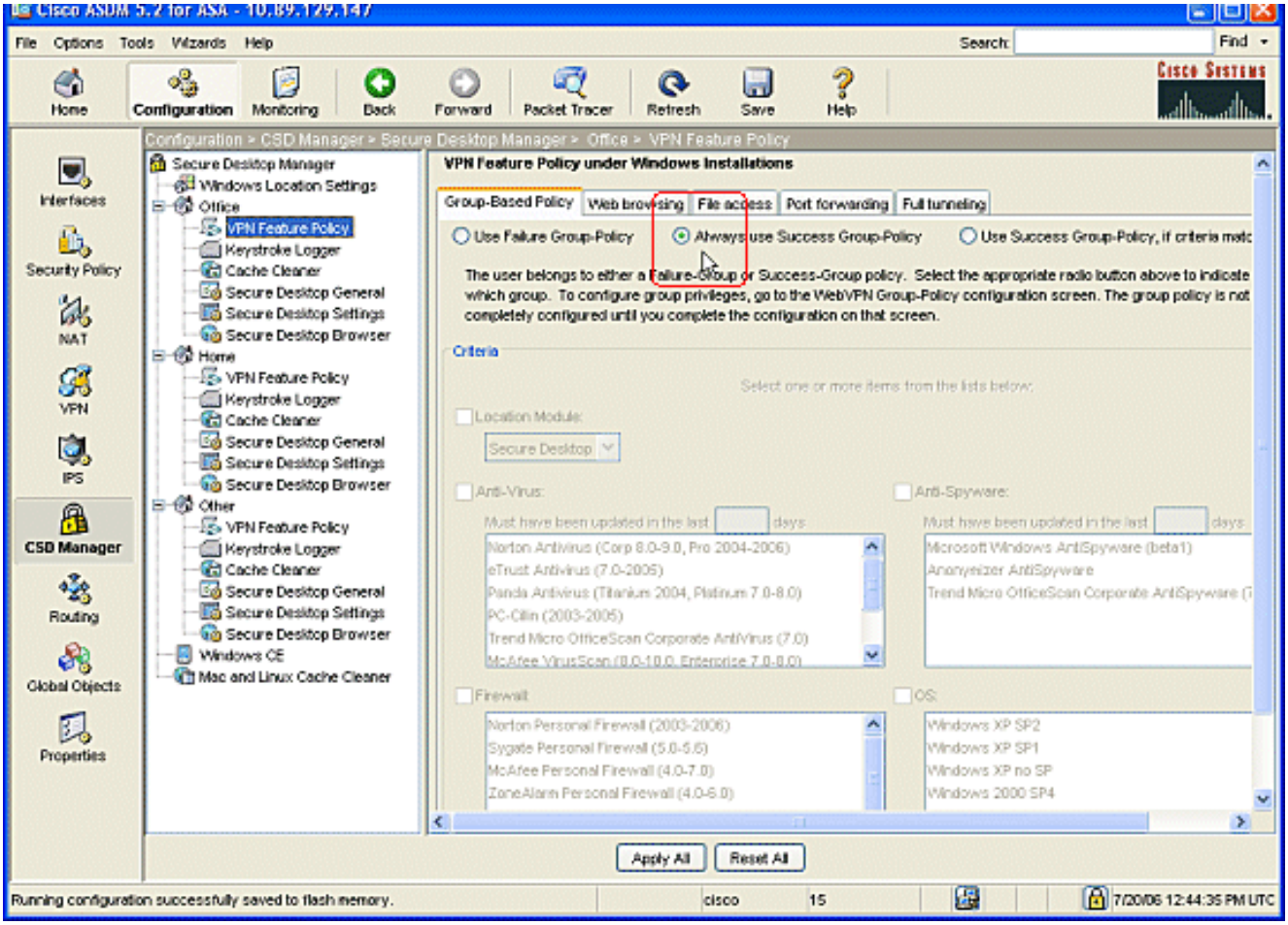

5. Wählen Sie unter Home die Option **Sichere Desktop-Einstellungen aus**.Aktivieren Sie **E-Mail-Anwendungen transparent arbeiten lassen**, und konfigurieren Sie die anderen Einstellungen für Ihre Umgebung.Klicken Sie auf **Alle anwenden**.Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.



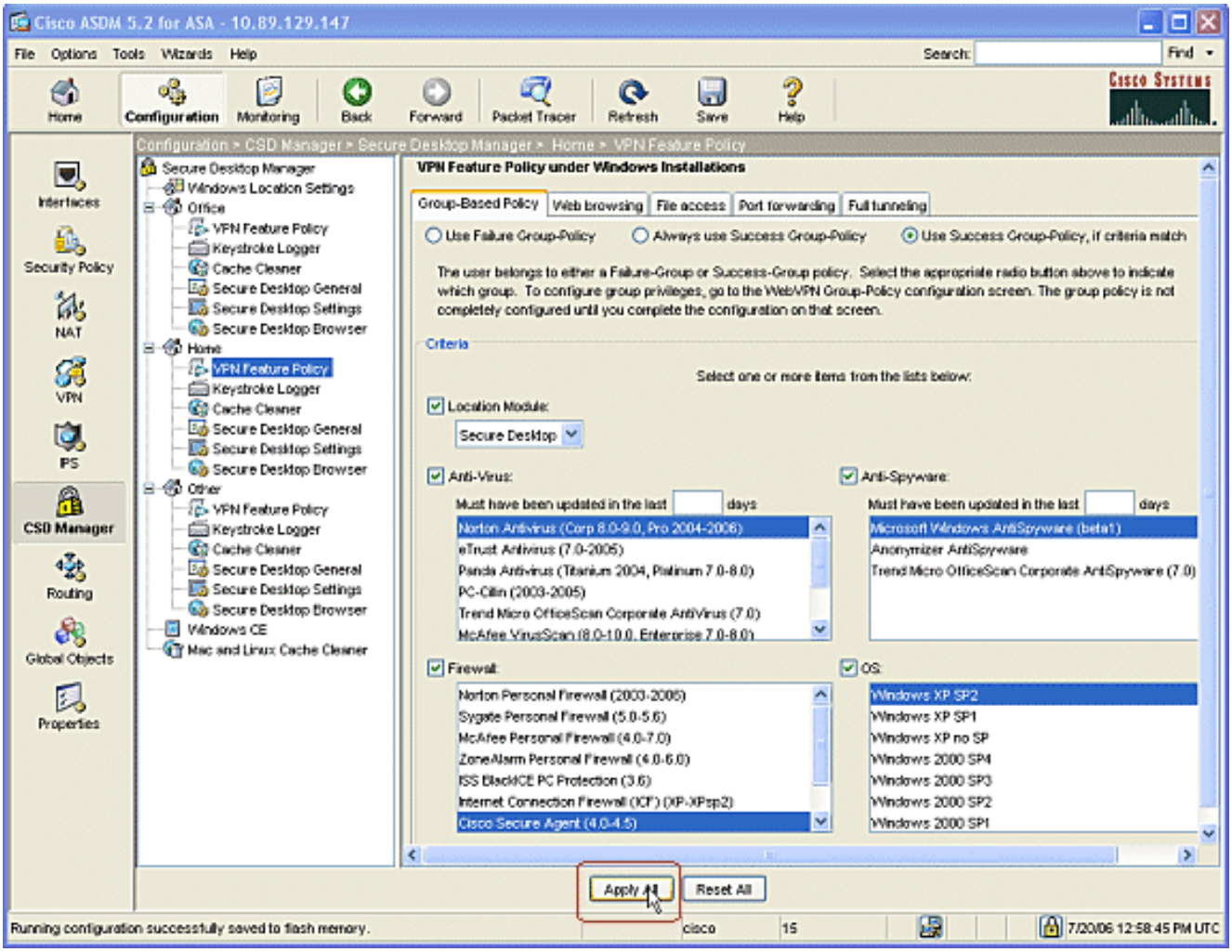

## Konfigurieren der Windows-Standortfunktionen

Konfigurieren Sie die VPN-Featurerichtlinie für die einzelnen von Ihnen erstellten Standorte.

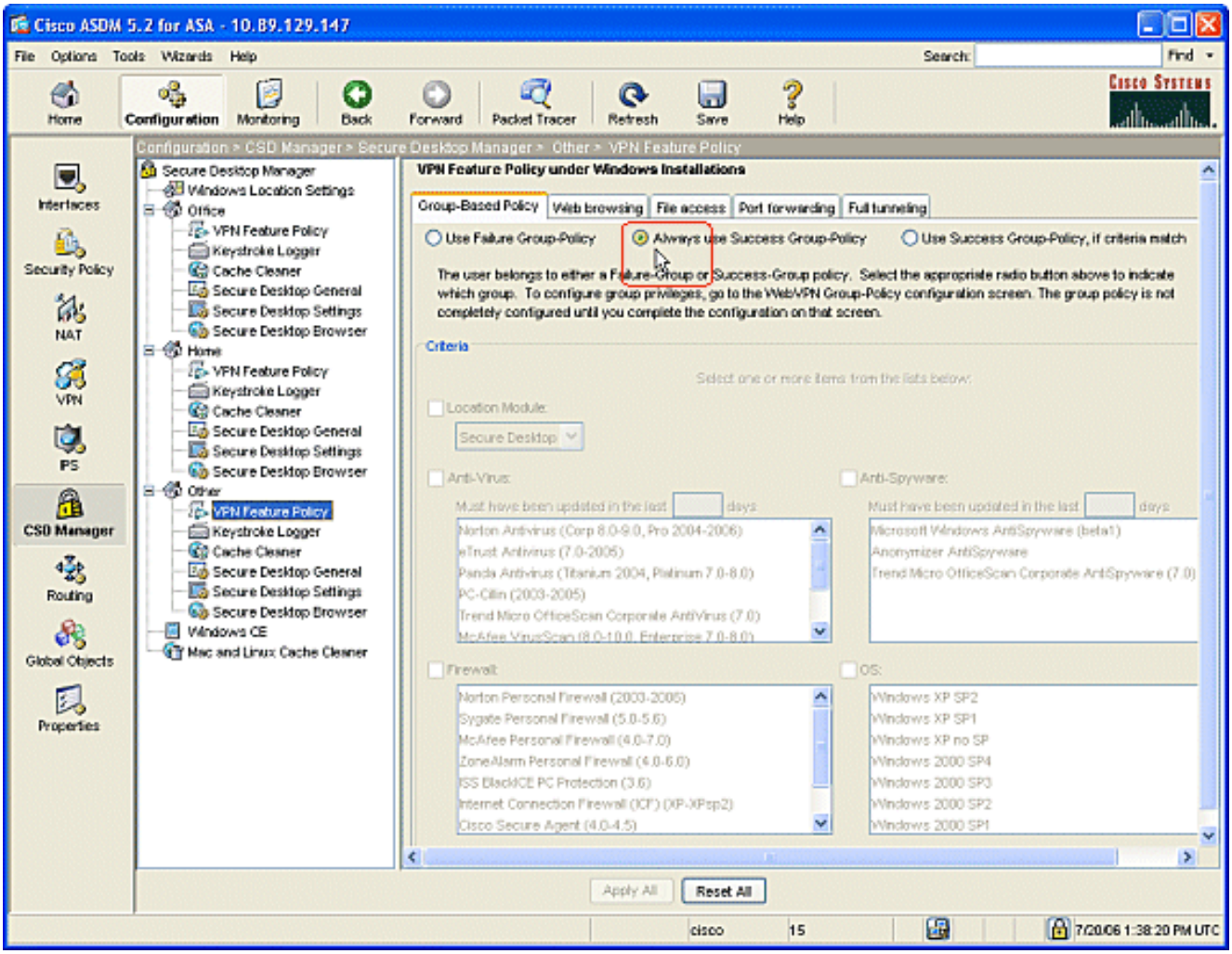
1. Klicken Sie im Navigationsbereich **auf Office** und dann auf **VPN Feature Policy (VPN-Featurerichtlinie)**.
2. Klicken Sie auf die Registerkarte **Gruppenbasierte Richtlinie**.Klicken Sie auf das Optionsfeld **Immer Erfolgsgruppenrichtlinie verwenden**.Klicken Sie auf die Registerkarte **Web Browsing**, und aktivieren Sie das Optionsfeld **Always Enabled (Immer aktiviert)**.Folgen Sie dem gleichen Verfahren für die Registerkarten **Dateizugriff, Portweiterleitung** und **Volltunneln**.Klicken Sie auf **Alle anwenden**.Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu
übernehmen.



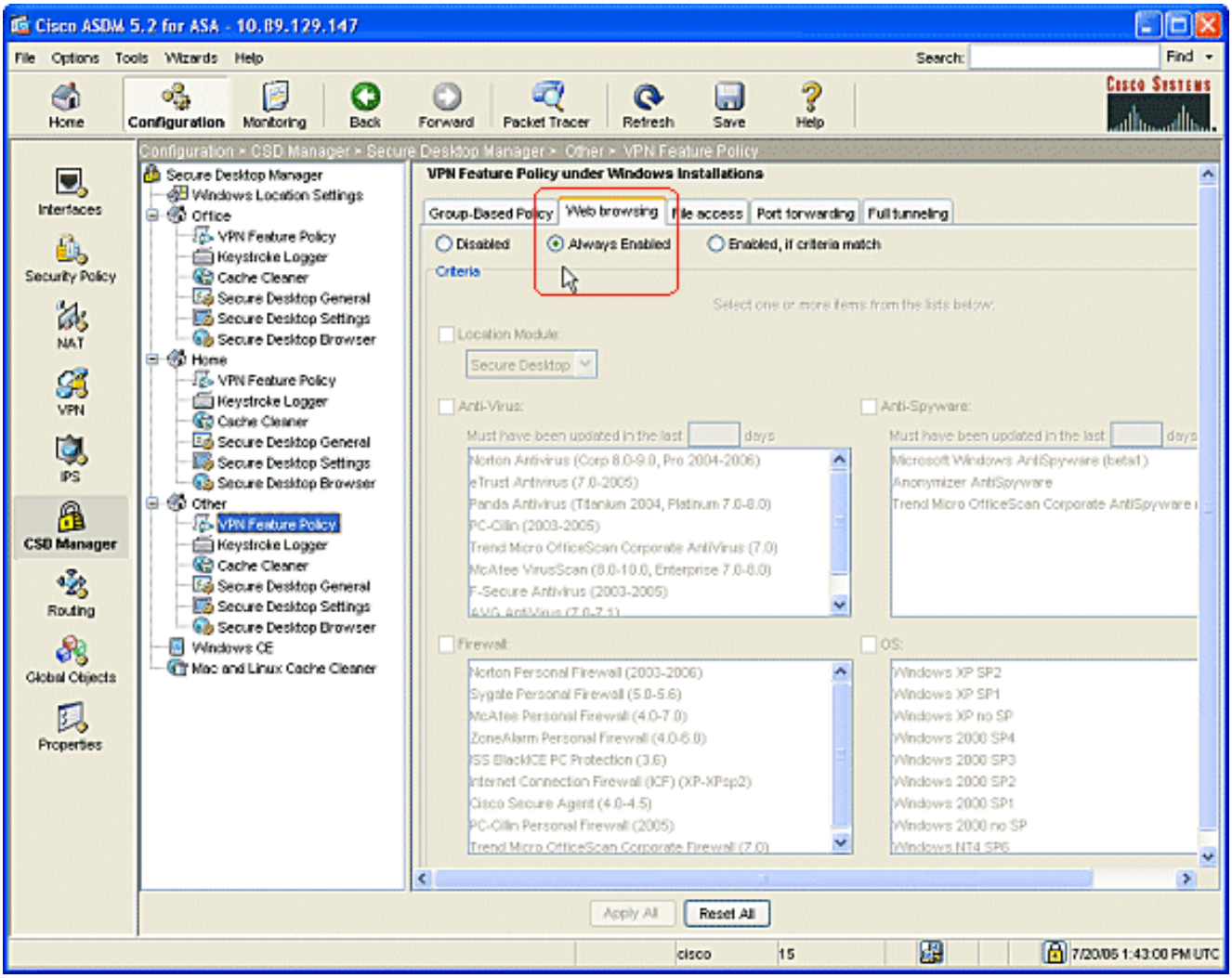

3. Für Privatanwender kann jedes Unternehmen spezifische Richtlinien vorschreiben, bevor der Zugriff erlaubt wird. Klicken Sie im Navigationsbereich auf **Home** und anschließend auf **VPN Feature Policy**.Klicken Sie auf die Registerkarte **Gruppenbasierte Richtlinie**.Klicken Sie auf das Optionsfeld **Erfolgsgruppen-Richtlinie verwenden**, wenn vorkonfigurierte Kriterien wie ein bestimmter Registrierungsschlüssel, ein bekannter Dateiname oder ein digitales Zertifikat übereinstimmen.Aktivieren Sie **das** Kontrollkästchen **Location Module (Standortmodul)**, und wählen Sie **Secure Desktop aus**.Wählen Sie die Sicherheitsrichtlinien Ihres Unternehmens **für die** Bereiche **Anti-Virus, Anti-Spyware**, Firewall und **Betriebssystem aus**. Privatanwender dürfen nur dann in das Netzwerk eindringen, wenn ihre Computer die konfigurierten Kriterien erfüllen.




4. Klicken Sie im Navigationsbereich auf **Andere** und anschließend auf **VPN Feature Policy**.Klicken Sie auf die Registerkarte **Gruppenbasierte Richtlinie**.Klicken Sie auf das Optionsfeld **Immer Erfolgsgruppenrichtlinie verwenden**.



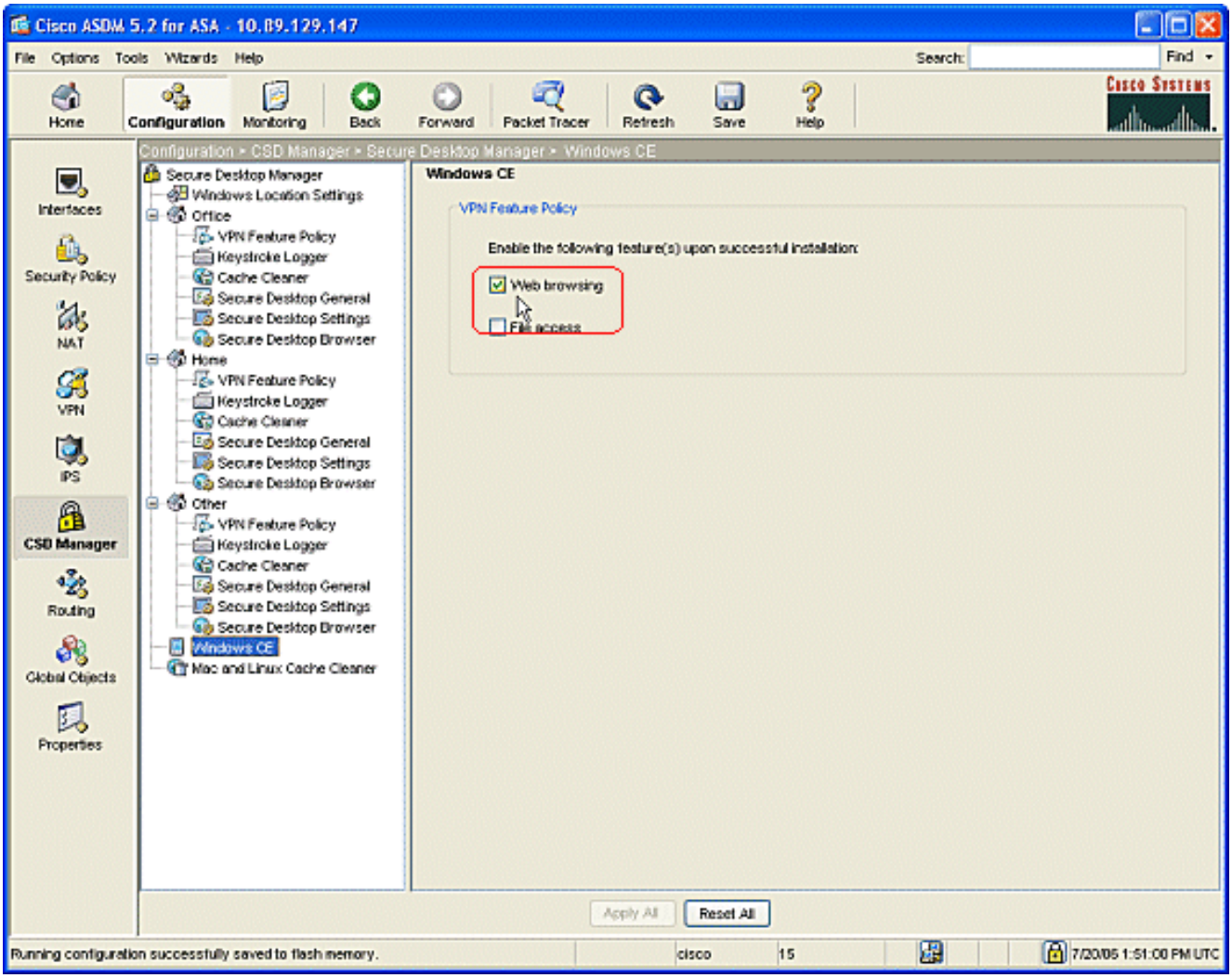

5. Für Clients in diesem Bereich **der VPN-Funktionsrichtlinie** klicken Sie auf die Registerkarte **Web Browsing** und anschließend auf das **immer aktivierte** Optionsfeld.Klicken Sie auf die Registerkarte **Dateizugriff** und anschließend auf das Optionsfeld **Deaktivieren**.Wiederholen Sie den Schritt mit den Registerkarten **Port Forwarding** und **Full Tunneling**.Klicken Sie auf **Alle anwenden**.Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.



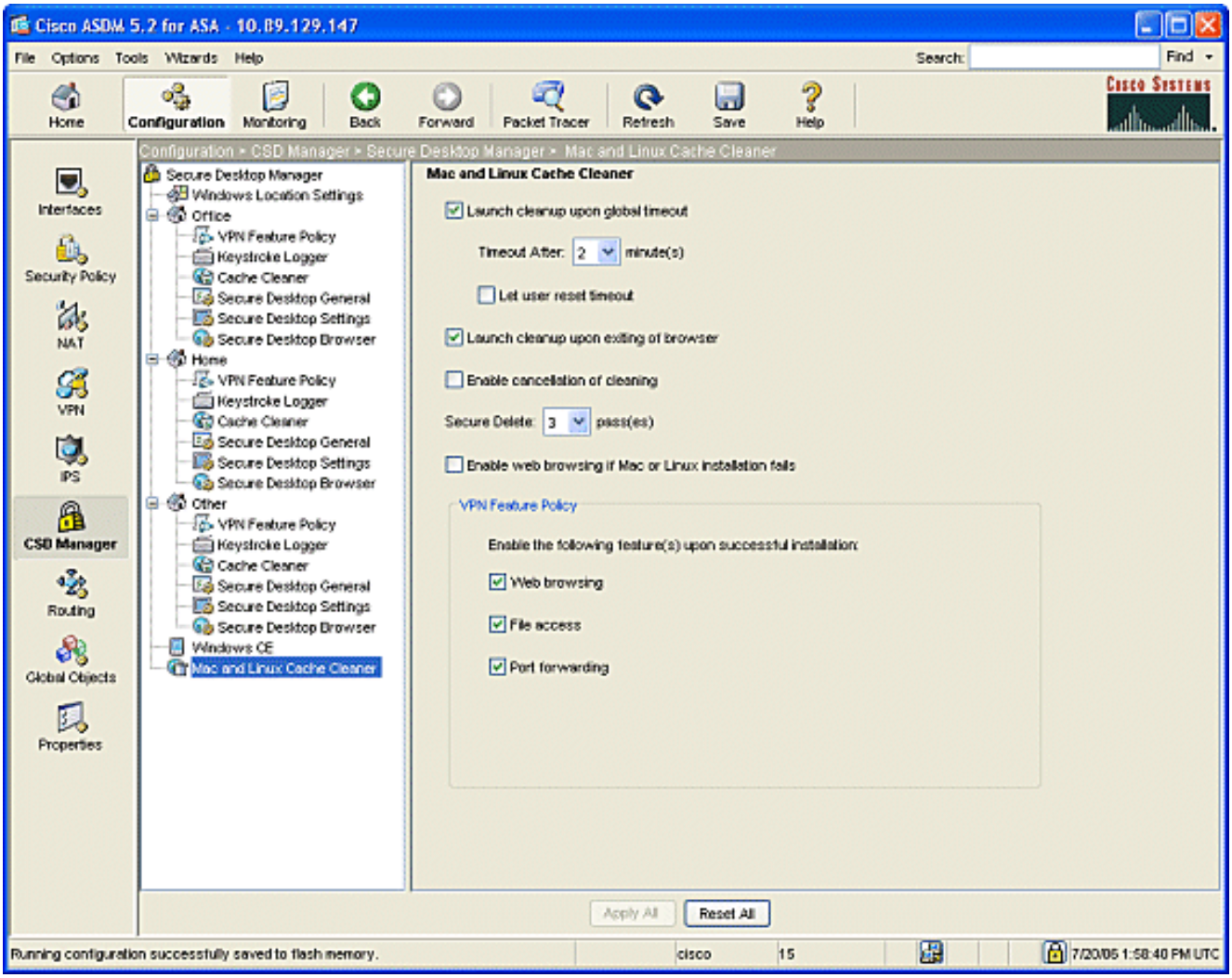

## Optionale Konfigurationen für Windows CE-, Macintosh- und Linux-Clients

Diese Konfigurationen sind optional.

1. Wenn Sie **Windows CE** im Navigationsbereich auswählen, aktivieren Sie das Kontrollkästchen **Webbrowsing**.




2. Wenn Sie **Mac und Linux Cache Cleaner** aus dem Navigationsbereich auswählen, überprüfen Sie die **Bereinigung bei globalem Timeout-**Funkwählverfahren.Ändern Sie das Timeout in Ihre Spezifikation.Im Bereich **VPN Feature Policy** (VPN-Featurerichtlinie) überprüfen Sie die Funknummern **Internetnutzung, Dateizugriff** und **Port Forwarding** für diese Clients.




3. Unabhängig davon, ob Sie Windows CE oder Mac und Linux Cache Cleaner wählen, klicken Sie auf **Alles anwenden**.
4. Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.

# Konfigurieren

## Konfiguration

Diese Konfiguration spiegelt die Änderungen wider, die ASDM zur Aktivierung von CSD vorgenommen hat: Die meisten CSD-Konfigurationen werden als separate Datei im Flash-Speicher gespeichert.

**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
```

# Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfigurationen für Clientless-SSL-VPN, Thin-Client-SSL-VPN oder SSL VPN-Client (SVC) ordnungsgemäß funktionieren.

Testen Sie den CSD mit einem PC, der mit verschiedenen Windows-Speicherorten konfiguriert wurde. Jeder Test sollte entsprechend der Richtlinien, die Sie im obigen Beispiel konfiguriert haben, einen anderen Zugriff bereitstellen.

Sie können die Portnummer und die Schnittstelle ändern, an der die Cisco ASA WebVPN-Verbindungen überwacht.

- Der Standard-Port ist 443. Wenn Sie den Standardport verwenden, ist der Zugriff **https://ASA IP Address**.
- Durch die Verwendung eines anderen Ports wird der Zugriff auf **https://ASA IP-Adresse:Portnummer** geändert.

### Befehle

Mehrere **show**-Befehle sind WebVPN zugeordnet. Sie können diese Befehle in der Befehlszeilenschnittstelle (CLI) ausführen, um Statistiken und andere Informationen anzuzeigen. Weitere Informationen zur Verwendung von **show**-Befehlen finden Sie unter Verifying WebVPN Configuration.

**Hinweis:** Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

## Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Wenn Sie Probleme mit dem Remote-Client haben, überprüfen Sie Folgendes:

1. Sind Popups, Java und/oder ActiveX im Webbrowser aktiviert? Diese müssen je nach verwendetem SSL VPN-Verbindungstyp möglicherweise aktiviert werden.
2. Der Kunde muss die zu Beginn der Sitzung präsentierten digitalen Zertifikate akzeptieren.

### Befehle

Dem WebVPN sind mehrere **Debugbefehle** zugeordnet. Ausführliche Informationen zu diesen Befehlen finden Sie unter Verwenden von WebVPN-Debug-Befehlen..

**Hinweis:** Die Verwendung von **Debug-**Befehlen kann sich negativ auf Ihr Cisco Gerät auswirken. Bevor Sie **Debug-**Befehle verwenden, lesen Sie die Informationen unter Wichtige Informationen über Debug-Befehle.

## Zugehörige Informationen

- Cisco Adaptive Security Appliances der Serie ASA 5500
- ASA mit WebVPN und Single Sign-On mit ASDM und NTLMv1 Konfigurationsbeispiel
- Technischer Support und Dokumentation - Cisco Systems