ASDM을 사용하는 Windows용 ASA 7.2.x의 Cisco Secure Desktop(CSD 3.1.x) 구성 예

목차

소개

CSD(Cisco Secure Desktop)는 SSL VPN 기술의 보안을 확장합니다.CSD는 세션 활동을 위해 사용자의 워크스테이션에 별도의 파티션을 제공합니다.이 볼트(Vault) 영역은 세션 중에 암호화되며 SSL VPN 세션이 끝날 때 완전히 제거됩니다.Windows는 CSD의 모든 보안 이점을 통해 구성할 수 있습니다.Macintosh, Linux 및 Windows CE는 캐시 클리너, 웹 브라우징 및 파일 액세스 기능에만 액세스할 수 있습니다.CSD는 다음 플랫폼에서 Windows, Macintosh, Windows CE 및 Linux 디바이스에 대해 구성할 수 있습니다.

- Cisco ASA(Adaptive Security Appliance) 5500 시리즈
- Cisco IOS® Software 릴리스 12.4(6)T 이상을 실행하는 Cisco 라우터
- Cisco VPN 3000 Series Concentrator 버전 4.7 이상
- Catalyst 6500 및 7600 Series 라우터의 Cisco WebVPN Module

참고: 이제 CSD Release 3.3에서는 Microsoft Windows Vista를 실행하는 원격 컴퓨터에서 Cisco Secure Desktop을 실행하도록 구성할 수 있습니다.이전에는 Cisco Secure Desktop이 Windows

XP 또는 2000을 실행하는 컴퓨터로 제한되었습니다.자세한 내용은 Cisco Secure Desktop 릴리스 정보, 릴리스 3.3의 Vista에서 새로운 기능 개선 - Secure Desktop on Vista 섹션을 참조하십시오.

이 예에서는 주로 ASA 5500 Series for Windows 클라이언트에서 CSD를 설치하고 구성하는 방법을 다룹니다.Windows CE, Mac 및 Linux 클라이언트에 대한 선택적 컨피그레이션이 추가되어 완료됩니다.

CSD는 SSL VPN 기술(클라이언트리스 SSL VPN, 씬 클라이언트 SSL VPN 또는 SSL VPN 클라이언트(SVC))과 함께 사용됩니다.CSD는 SSL VPN 기술의 보안 세션에 가치를 더합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

ASA 디바이스의 요구 사항

- Cisco CSD 릴리스 3.1 이상
- Cisco ASA 소프트웨어 버전 7.1.1 이상
- Cisco ASDM(Adaptive Security Device Manager) 릴리스 5.1.1 이상**참고:** CSD 버전 3.2는 ASA 버전 8.x에서만 지원됩니다.**참고:** ASDM에서 ASA를 구성할 수 있도록 허용하려면 ASDM에 대한 HTTPS 액세스 허용을 참조하십시오.

클라이언트 컴퓨터의 요구 사항

- 원격 클라이언트에는 로컬 관리 권한이 있어야 합니다.필수 사항은 아니지만, 매우 권장됩니다.
- 원격 클라이언트에는 JRE(Java Runtime Environment) 버전 1.4 이상이 있어야 합니다.
- 원격 클라이언트 브라우저:Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 또는 Firefox 1.0
- 원격 클라이언트에서 쿠키 사용 및 팝업 허용

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASDM 버전 5.2(1)
- Cisco ASA 버전 7.2(1)
- Cisco CSD 버전 보안 데스크톱-asa-3.1.1.32-k9.pkg

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 지워진(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.이 구성에 사용되는 IP 주소는 RFC 1918 주소입니다.이러한 IP 주소는 인터넷에서 사용할 수 없으며 테스트 랩 환경에서만 사용됩니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

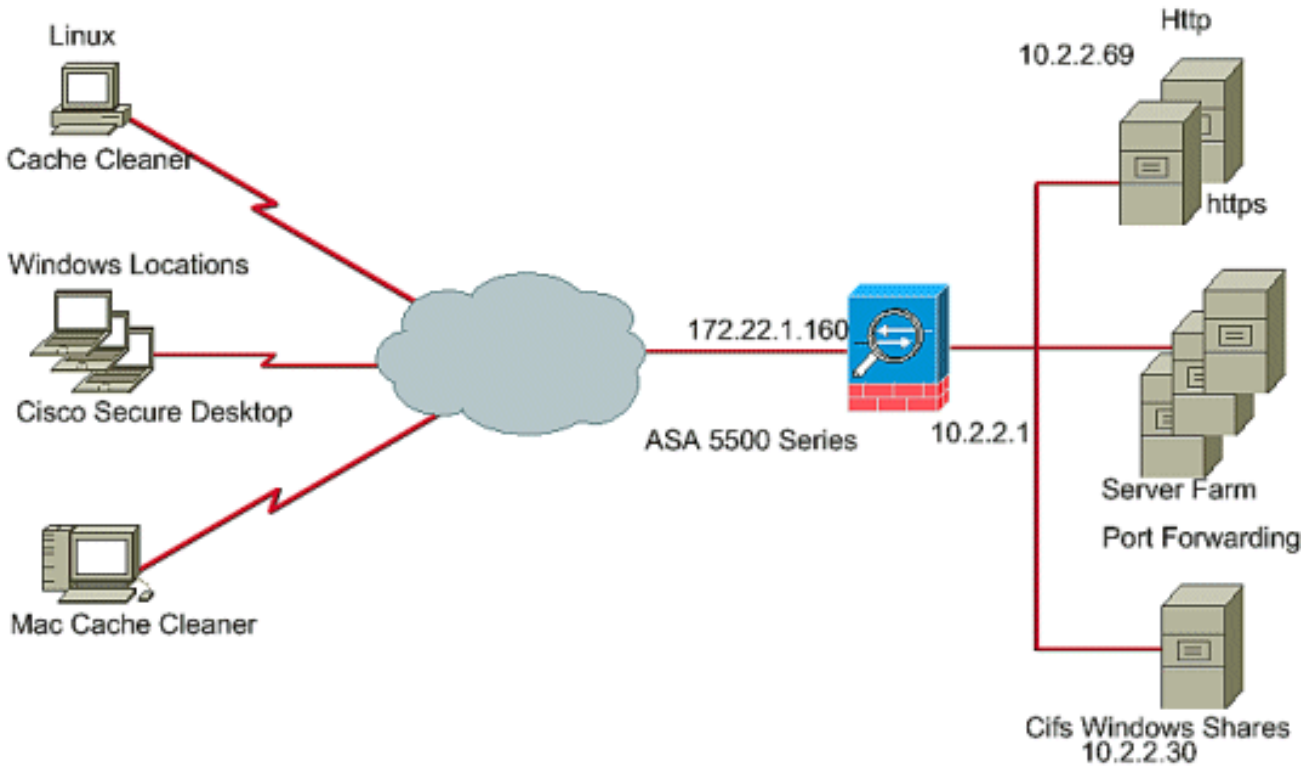
배경 정보

CSD는 SSL VPN 기술을 사용하여 작동하므로 CSD를 구성하기 전에 클라이언트리스, 씬 클라이언트 또는 SVC를 활성화해야 합니다.

네트워크 다이어그램

CSD의 전체 보안 측면을 사용하여 다양한 Windows 위치를 구성할 수 있습니다.Macintosh, Linux 및 Windows CE는 캐시 클리너 및/또는 웹 검색 및 파일 액세스에만 액세스할 수 있습니다.

이 문서에서는 다음 네트워크 설정을 사용합니다.



Windows 클라이언트용 ASA에서 CSD 구성

ASA for Windows Clients에 다음 5가지 주요 단계로 CSD를 구성합니다.

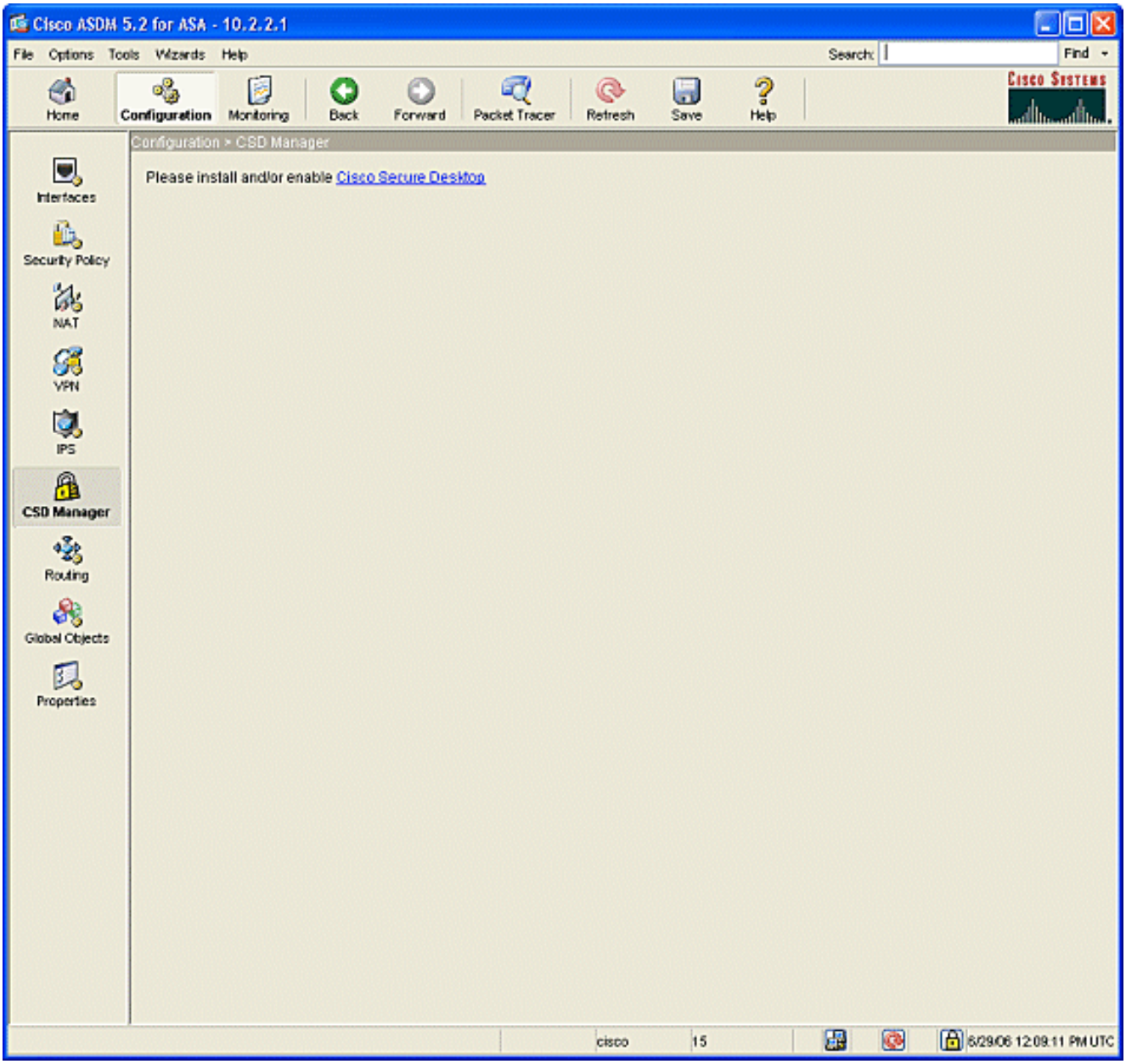
- Cisco ASA에서 CSD 소프트웨어를 확보, 설치 및 활성화합니다.
- Windows 위치를 정의합니다.
- Windows 위치 ID를 정의합니다.
- Windows 위치 모듈을 구성합니다.
- Windows 위치 기능을 구성합니다.
- Windows CE, Macintosh 및 Linux 클라이언트에 대한 선택적 구성

CSD 소프트웨어 가져오기, 설치 및 활성화

Cisco ASA에서 CSD 소프트웨어를 가져오고 설치하고 활성화하려면 다음 단계를 완료하십시오.

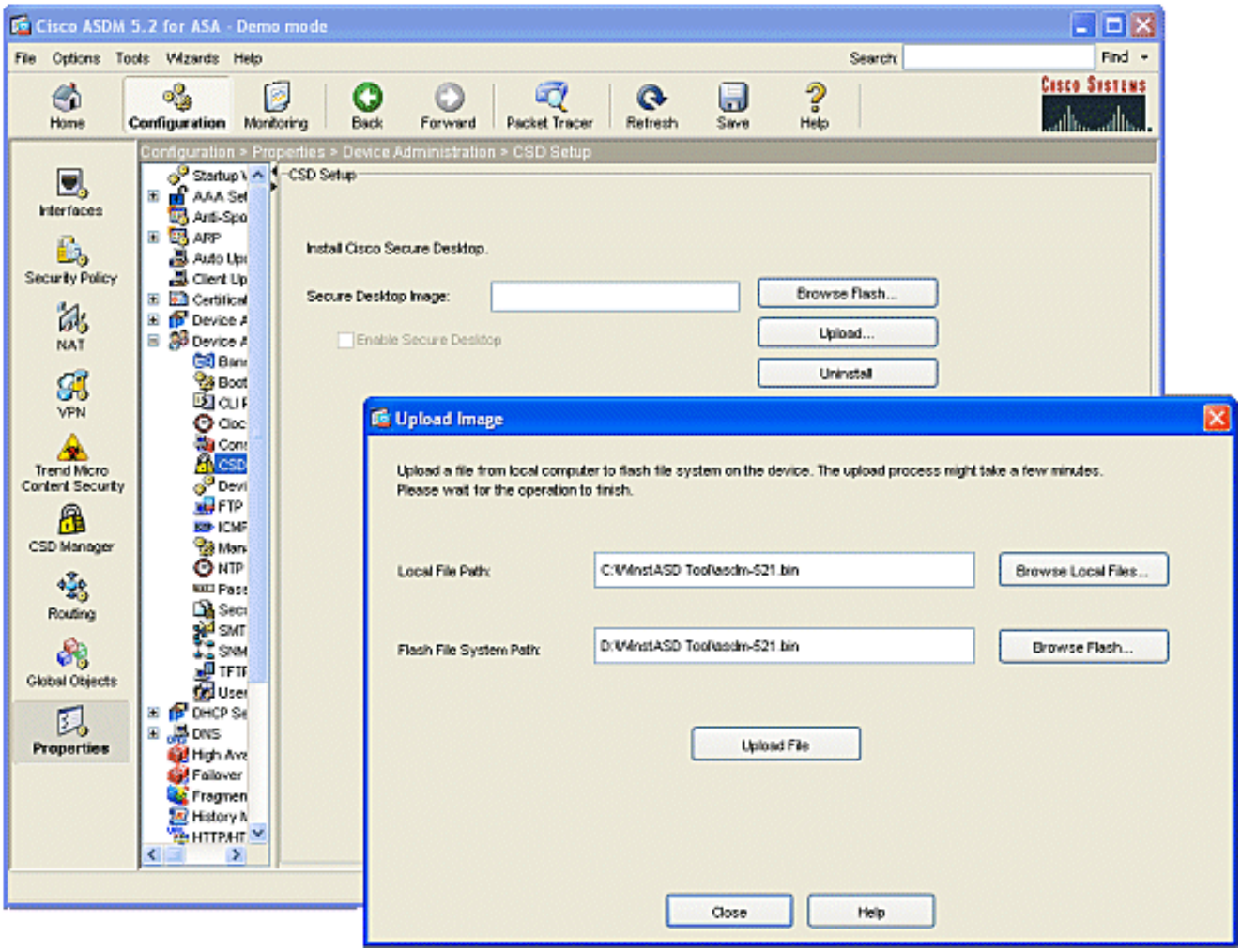
1. Cisco 소프트웨어 다운로드 웹 사이트에서 관리 스테이션에 CSD 소프트웨어 securedesktop-asa*.pkg 및 readme 파일을 다운로드합니다.
2. ASDM에 로그인하고 **Configuration** 버튼을 클릭합니다.왼쪽 메뉴에서 CSD **Manager** 버튼을 클릭하고 **Cisco Secure Desktop** 링크를 클릭합니다

.



3. Upload(**업로드**)를 클릭하여 Upload Image(이미지 업로드) 창을 표시합니다.관리 스테이션에서 새 .pkg 파일의 경로를 입력하거나 Browse Local **Files(로컬 파일 찾아보기)를** 클릭하여 파일을 찾습니다.파일을 배치할 플래시 위치를 입력하거나 **Browse Flash**(플래시 찾아보기)를 클릭합니다.Upload **File을 클릭합니다**.프롬프트가 표시되면 **확인 > 닫기 > 확인을** 클릭합니다

.

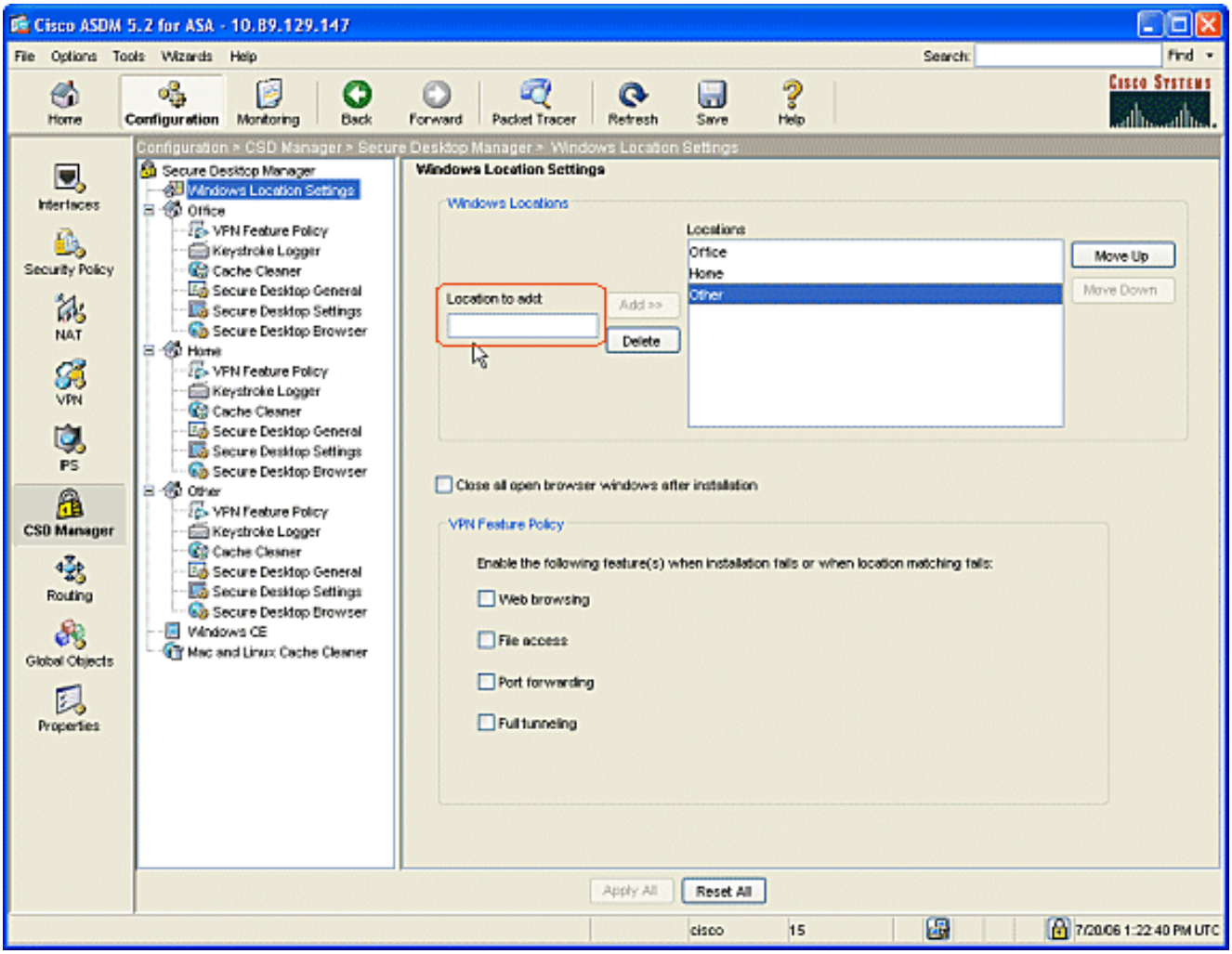


4. 클라이언트 이미지가 플래시에 로드되면 Enable SSL **VPN Client(SSL VPN 클라이언트 활성화)** 확인란을 선택한 다음 Apply(적용)를 **클릭합니다**.
5. Save(**저장**)를 클릭한 다음 **Yes(예)**를 클릭하여 변경 사항을 적용합니다.

Windows 위치 정의

Windows 위치를 정의하려면 다음 단계를 완료하십시오.

1. Configuration(컨피그레이션) 버튼**을** 클릭합니다.
2. 왼쪽 메뉴에서 CSD **Manager** 버튼을 클릭하고 **Cisco Secure Desktop** 링크를 클릭합니다.
3. 탐색 창에서 **Windows 위치 설정**을 클릭합니다.
4. 추가할 위치 필드에 위치 이름을 입력하고 추가를 **클릭합니다**.이 예에서는 3개의 위치에 유의하십시오.사무실, 집 및 기타Office는 회사의 보안 경계 내에 있는 워크스테이션을 나타냅니다.홈은 재택 근무 사용자를 나타냅니다.기타(Other)는 언급된 두 위치 외의 위치를 나타냅니다.

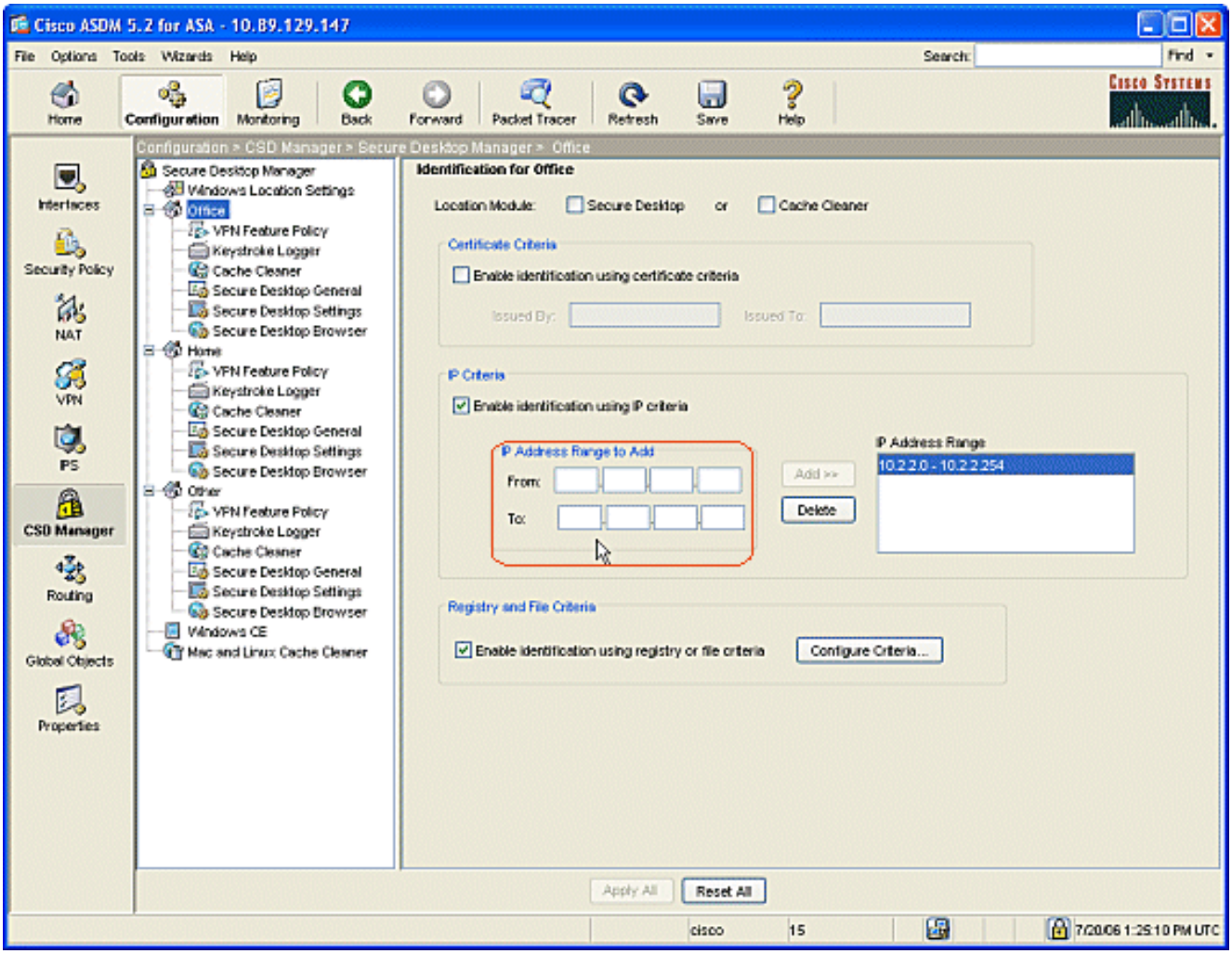


5. 영업 팀, 게스트, 파트너 및 기타 사용자를 위한 네트워크 아키텍처의 레이아웃에 따라 고유한 위치를 생성합니다.
6. Windows 위치를 만들 때 탐색 창은 각 새 위치에 대해 구성 가능한 모듈로 확장됩니다.**Apply All을 클릭합니다**.
7. Save(**저장**)를 클릭한 다음 **Yes(예)**를 클릭하여 변경 사항을 적용합니다.

Windows 위치 식별

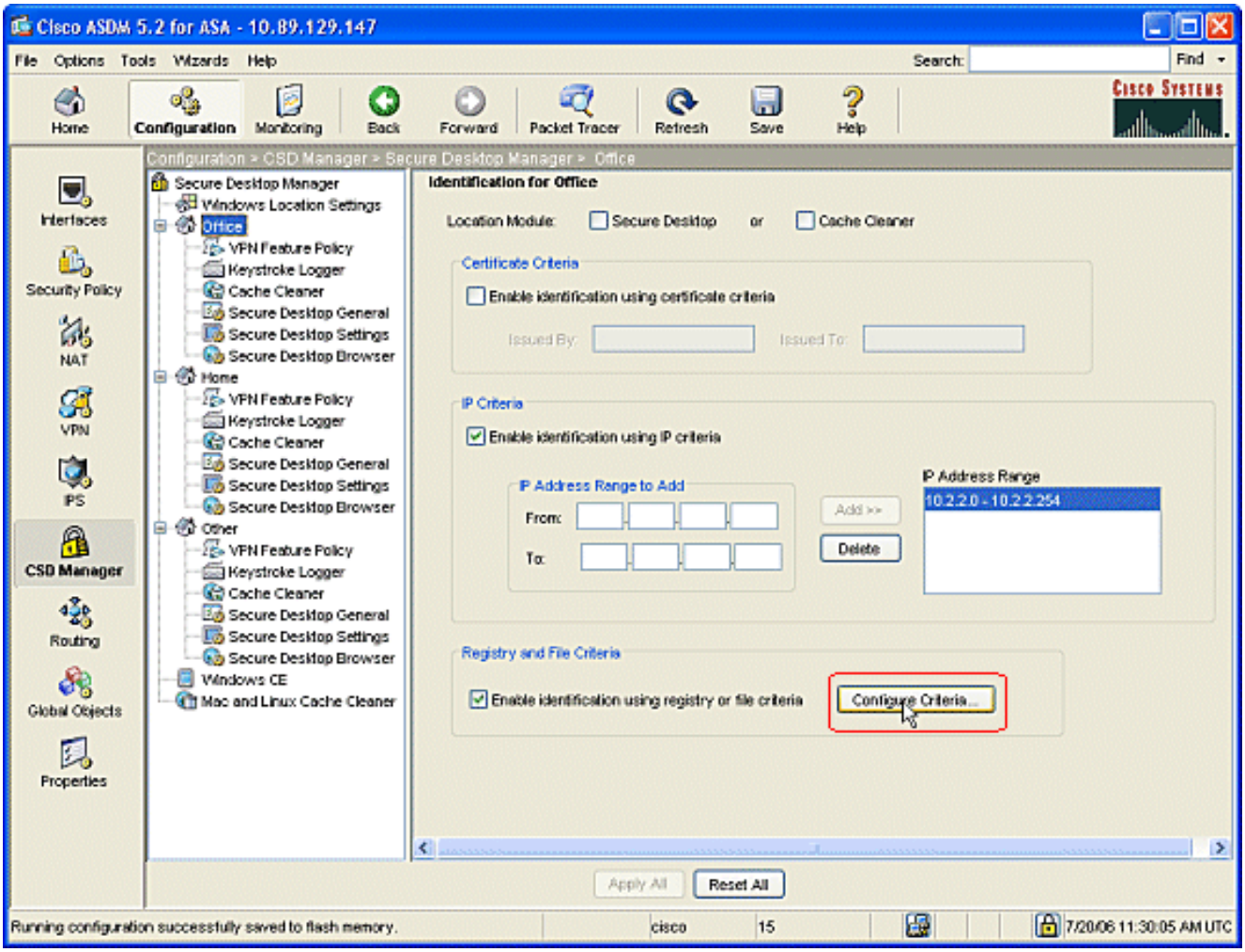
Windows 위치 ID를 정의하려면 다음 단계를 완료하십시오.

1. Windows 위치 정의에서 만든 위치를 식별합니다
   .



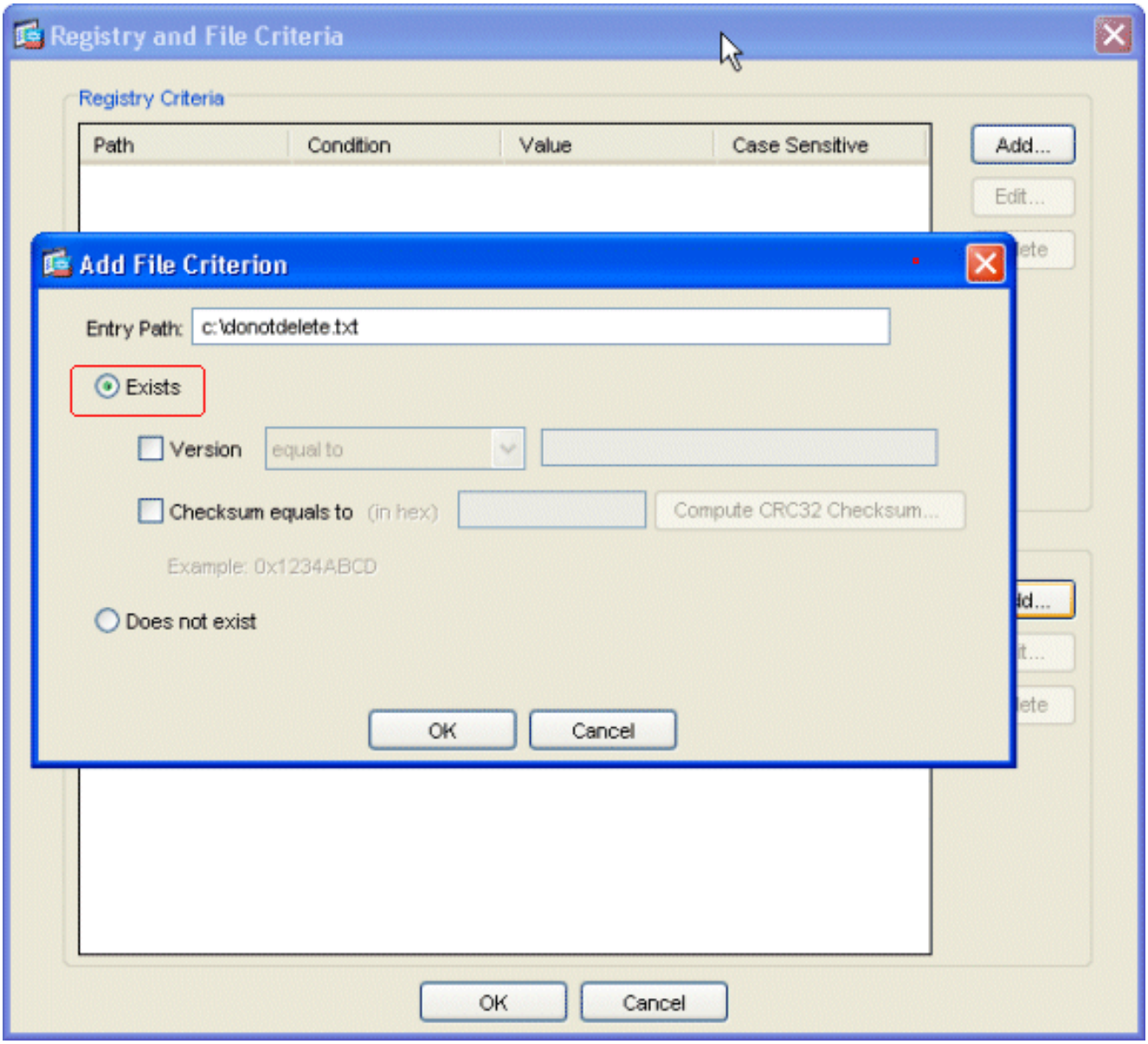
2. Office 위치를 확인하려면 탐색 창에서 Office를 클릭합니다.**보안 데스크톱** 및 **캐시 클리너**는 내부 컴퓨터이므로 선택을 취소합니다.Enable identification using **IP criteria(IP 기준을 사용하여 식별 활성화)를 선택합니다**.내부 컴퓨터의 IP 주소 범위를 입력합니다.**레지스트리 또는 파일 기준을 사용하여 식별 사용을 선택합니다**.이렇게 하면 내부 사무실 직원이 네트워크에 가끔 오는 게스트와 구별됩니다

.



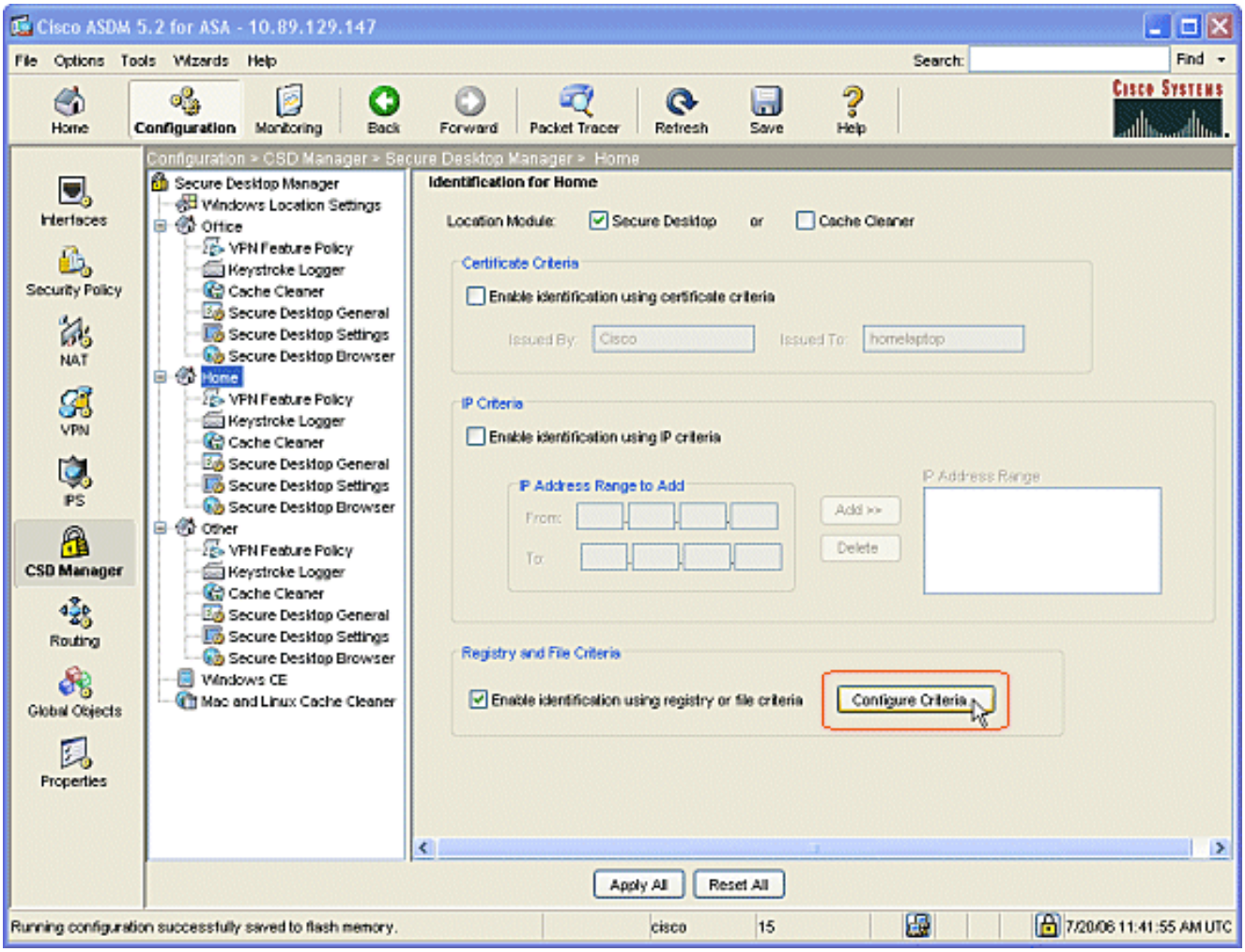
3. Configure **Criteria를 클릭합니다**."DoNotDelete.txt" 파일의 간단한 예가 구성됩니다.이 파일은 내부 Windows 컴퓨터에 있어야 하며 자리 표시자입니다.내부 사무실 컴퓨터를 식별하도록 Windows 레지스트리 키를 구성할 수도 있습니다.Add File Criterion 창에서 OK를 클릭합니다 .레지스트리 및 파일 조건 창에서 확인을 클릭합니다

.

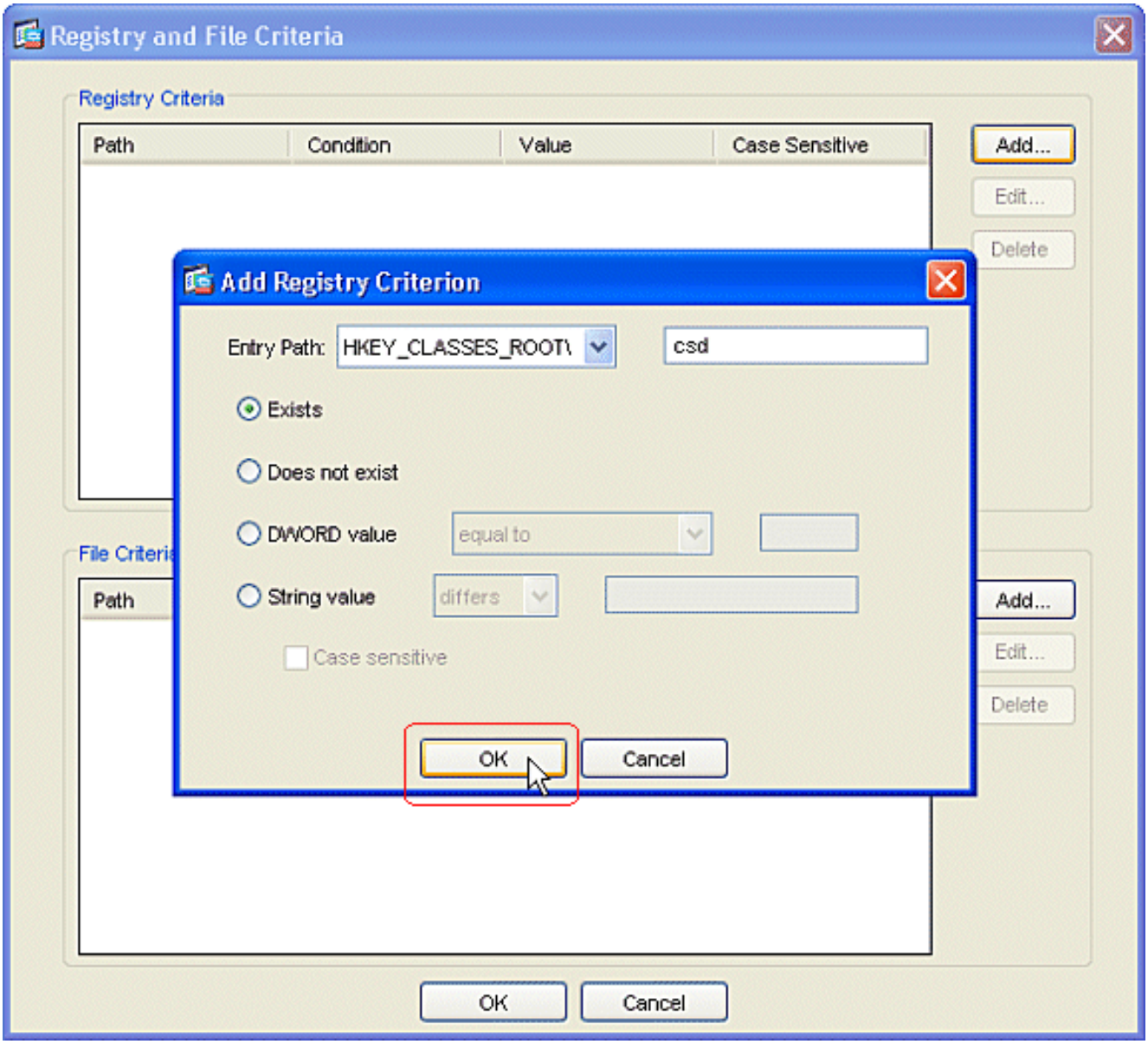


4. Office**용** 식별 창에서 모두 적용을 클릭합니다.Save(**저장**)를 클릭한 다음 **Yes(예)**를 클릭하여 변경 사항을 적용합니다.
5. 홈 위치를 식별하려면 탐색 창에서 **홈**을 클릭합니다.**레지스트리 또는 파일 기준을 사용하여 식별 사용을 선택합니다**.Configure **Criteria를 클릭합니다**

.

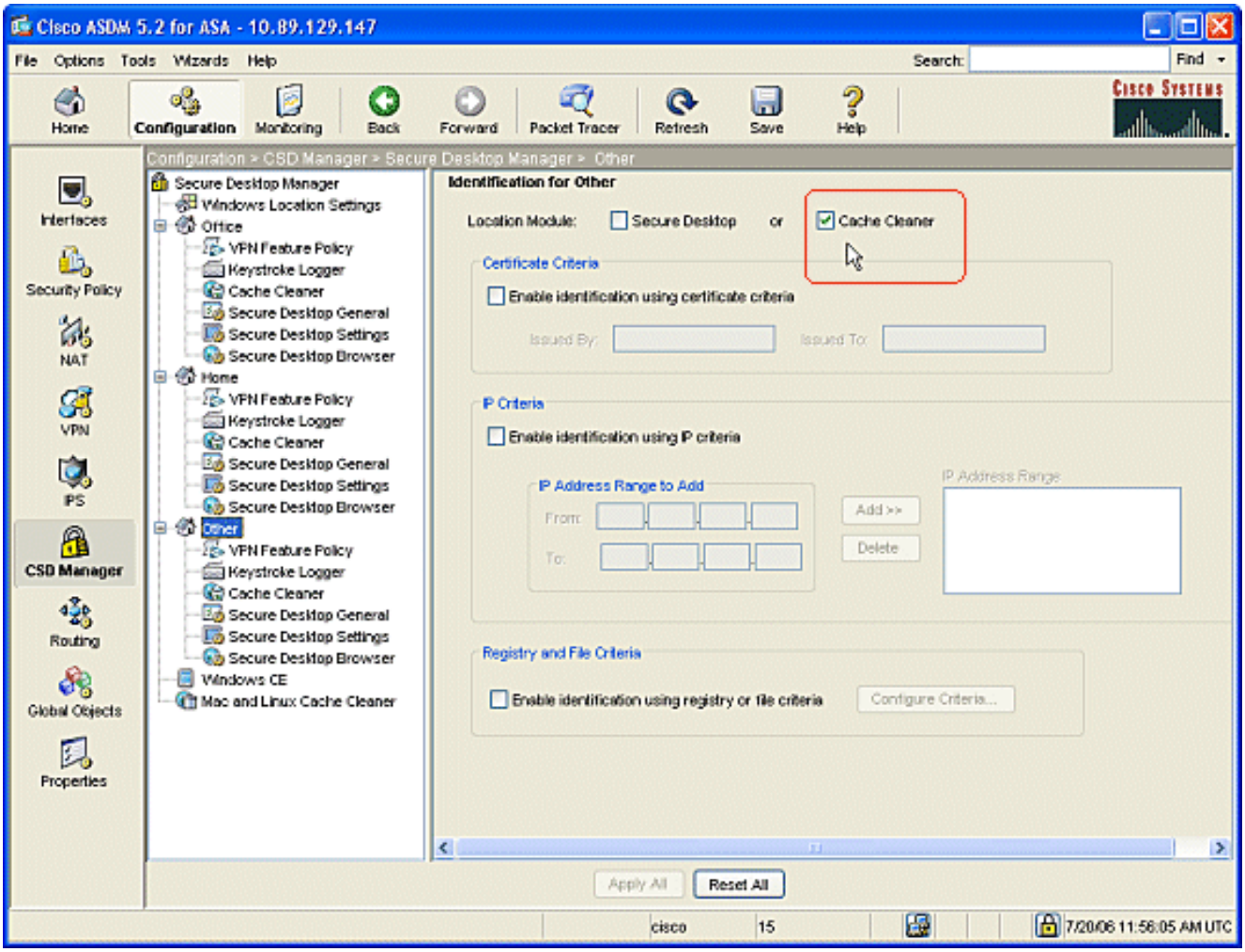


6. 관리자가 이 레지스트리 키로 홈 컴퓨터 클라이언트를 구성했어야 합니다.Add Registry Criterion 창에서 OK를 클릭합니다.레지스트리 및 파일 조건 창에서 확인을 클릭합니다
.



7. Location Module(위치 모듈)에서 Secure **Desktop(보안 데스크톱)을** 선택합니다.Identification for Home(홈 식별) 창에서 Apply All(모두 적용)을 클릭합니다.Save(**저장**)를 클릭한 다음 **Yes(예**)를 클릭하여 변경 사항을 적용합니다.
8. 위치를 확인하려면 **기타**를 클릭하고 탐색 창에서 기타를 클릭합니다.Cache Cleaner(캐시 클리너) 상자만 선택하고 다른 모든 상자의 선택을 취소합니다.Identification for Other(기타 식별) 창에서 Apply All(모두 적용)을 클릭합니다.Save(**저장**)를 클릭한 다음 **Yes(예**)를 클릭하여 변경 사항을 적용합니다

.

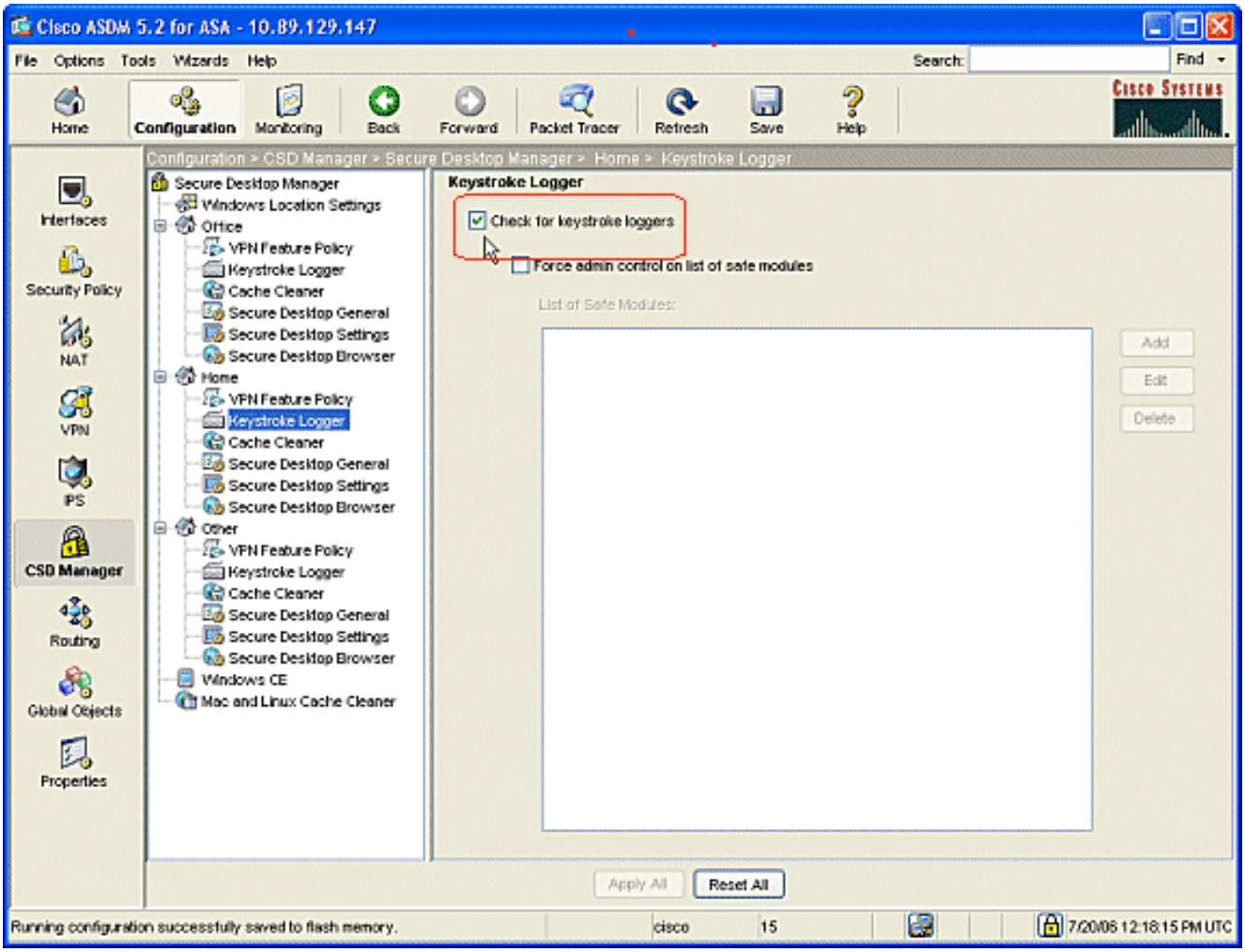


Windows 위치 구성 모듈

생성한 세 위치 아래에 모듈을 구성하려면 다음 단계를 완료하십시오.

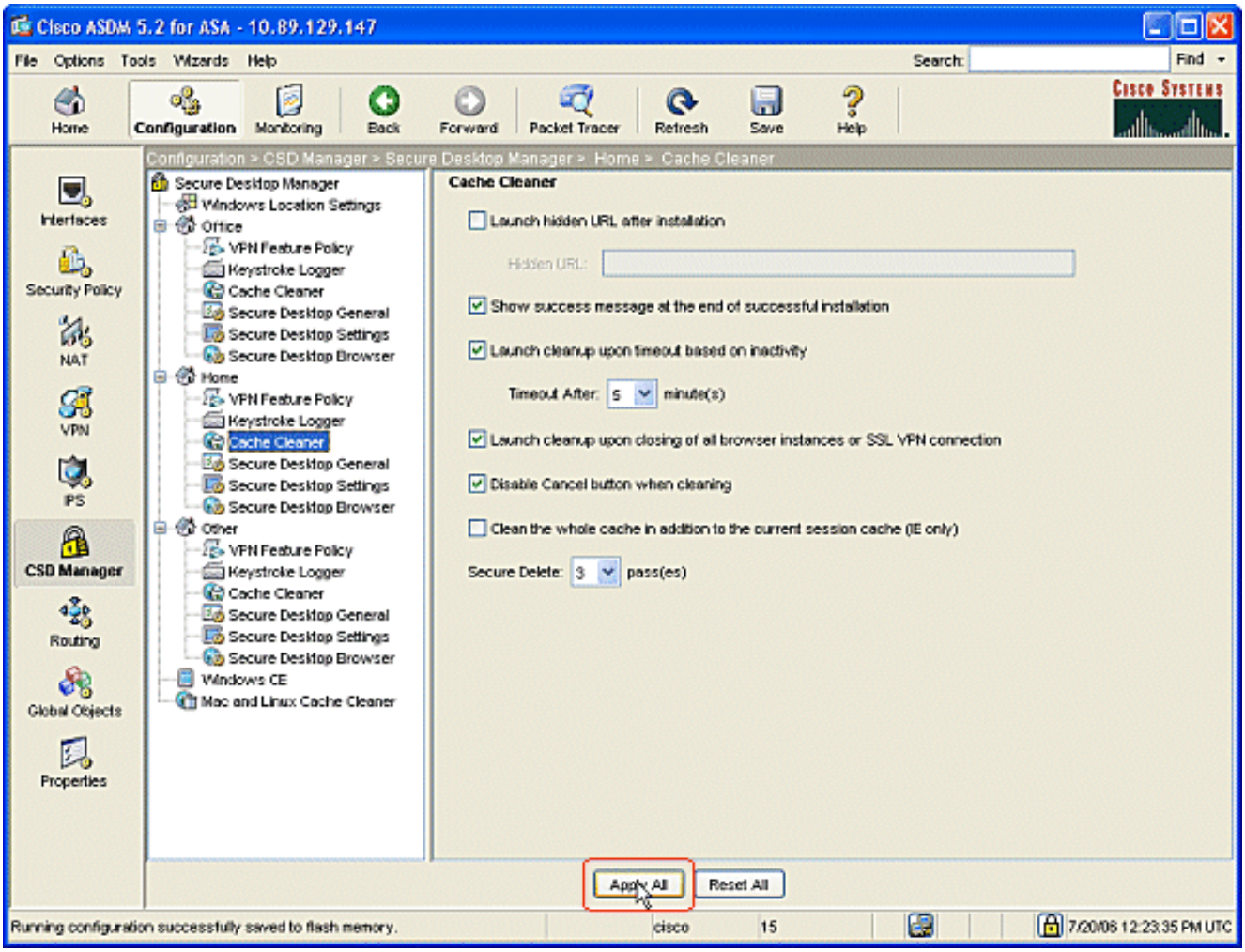
1. 이전 단계에서 보안 데스크톱 및 캐시 클리너를 선택하지 않았으므로 Office 클라이언트의 경우 아무 작업도 수행하지 않습니다.ASDM 애플리케이션을 사용하면 이전 단계에서 선택하지 않은 경우에도 캐시 클리너를 구성할 수 있습니다.Office 위치의 기본 설정을 유지합니다.**참고:** VPN 기능 정책은 이 단계에서 논의되지 않지만 모든 위치의 후속 단계에서 설명됩니다.
2. 홈 클라이언트의 경우 탐색 창**에서 홈** 및 **키 입력 로거**를 클릭합니다.Keystroke Logger(키 입력 로거) 창에서 Check for keystroke loggers(**키 입력 로거 확인)를** 선택합니다.Keystroke **Logger** 창에서 Apply All을 클릭합니다.Save(**저장**)를 클릭한 다음 **Yes(예**)를 클릭하여 변경 사항을 적용합니다

.



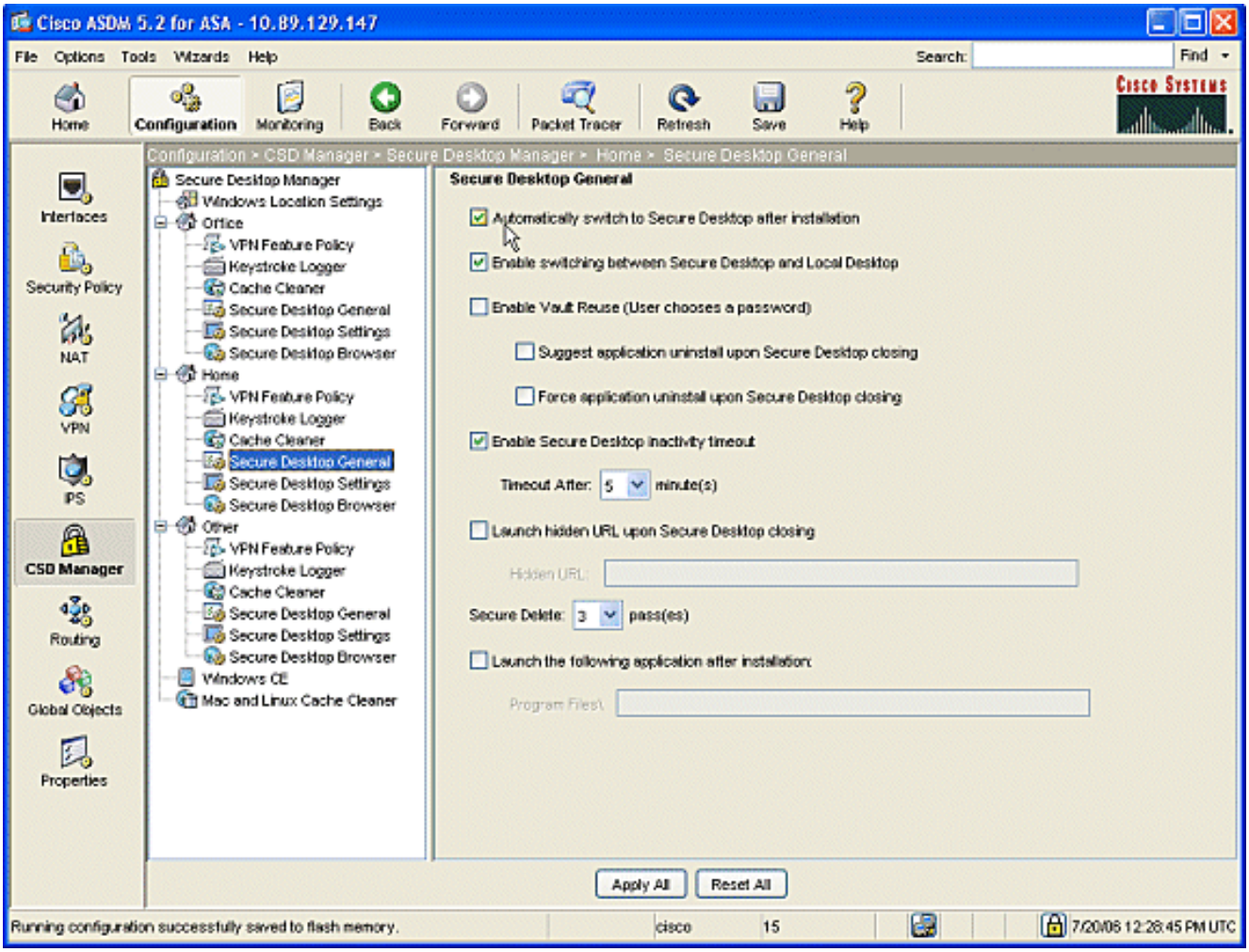
3. 홈에서 **캐시 클리너** 및 환경에 맞는 매개변수를 선택합니다

.



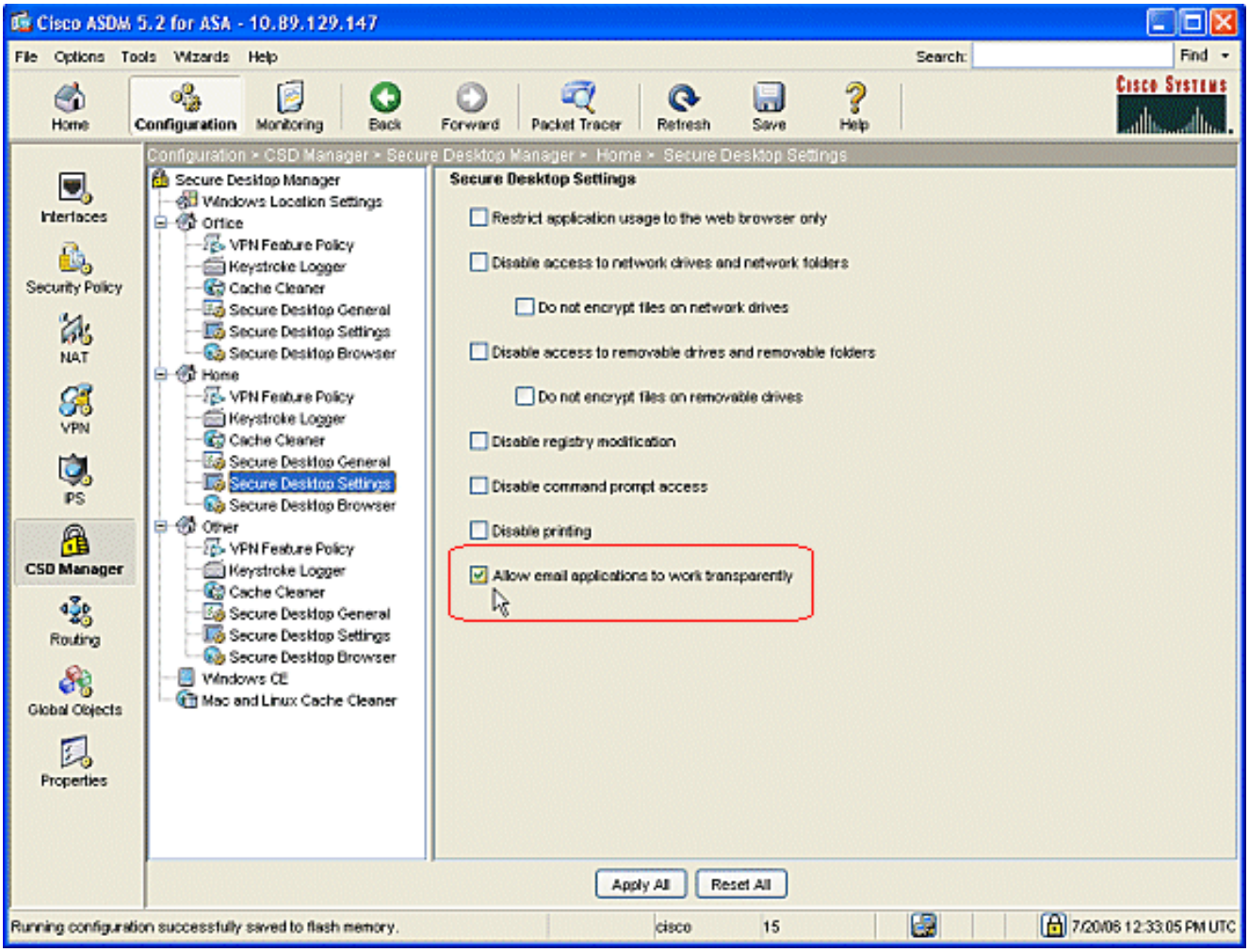
4. 홈에서 **Secure Desktop General(보안 데스크톱 일반)**과 사용자 환경에 맞는 매개변수를 선택합니다

.



5. Home(홈)에서 Secure **Desktop Settings(데스크톱 설정 보안)를 선택합니다**.Allow **email applications to work transparently(이메일 애플리케이션이 투명하게 작동하도록 허용)를 선택하고** 환경에 맞게 다른 설정을 구성합니다.Apply **All을 클릭합니다**.Save(**저장**)를 클릭한 다음 **Yes(예)**를 클릭하여 변경 사항을 적용합니다

.

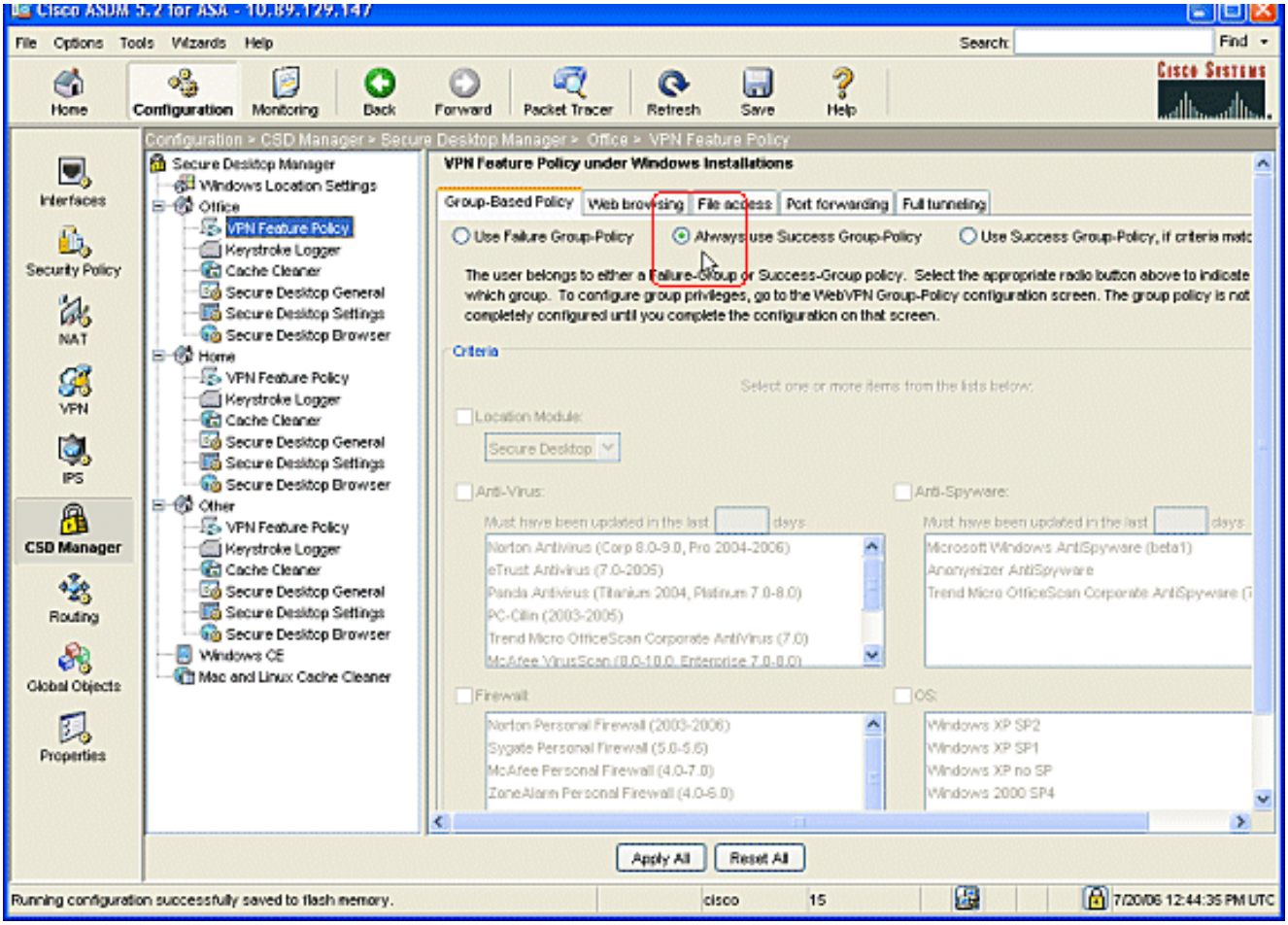


Windows 위치 기능 구성

생성한 각 위치에 대해 VPN 기능 정책을 구성합니다.

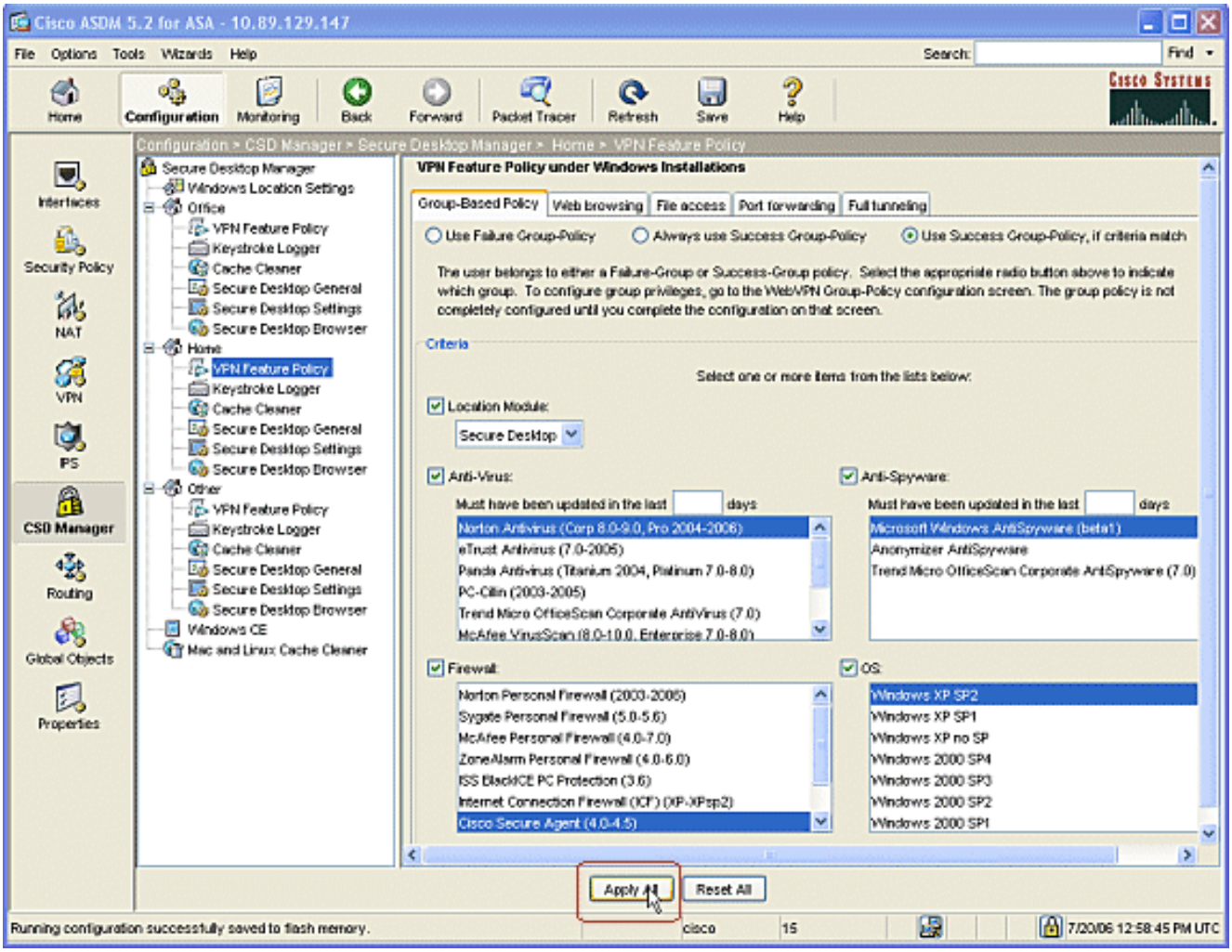
1. 탐색 창에서 Office를 **클릭한** 다음 **VPN Feature Policy(VPN 기능 정책)를 클릭합니다**.
2. **Group-Based Policy** 탭을 클릭합니다.Always use **Success Group-Policy(항상 성공 그룹-정책 사용)** 라디오 버튼을 클릭합니다.**웹 검색** 탭을 클릭하고 Always Enabled(**항상 사용**) 라디오 버튼을 선택합니다.**파일 액세스, 포트 전달** 및 **전체 터널링** 탭에 대해 동일한 절차를 수행합니다.Apply **All을 클릭합니다**.Save(**저장**)를 클릭한 다음 **Yes(예)**를 클릭하여 변경 사항을 적용합니다

.



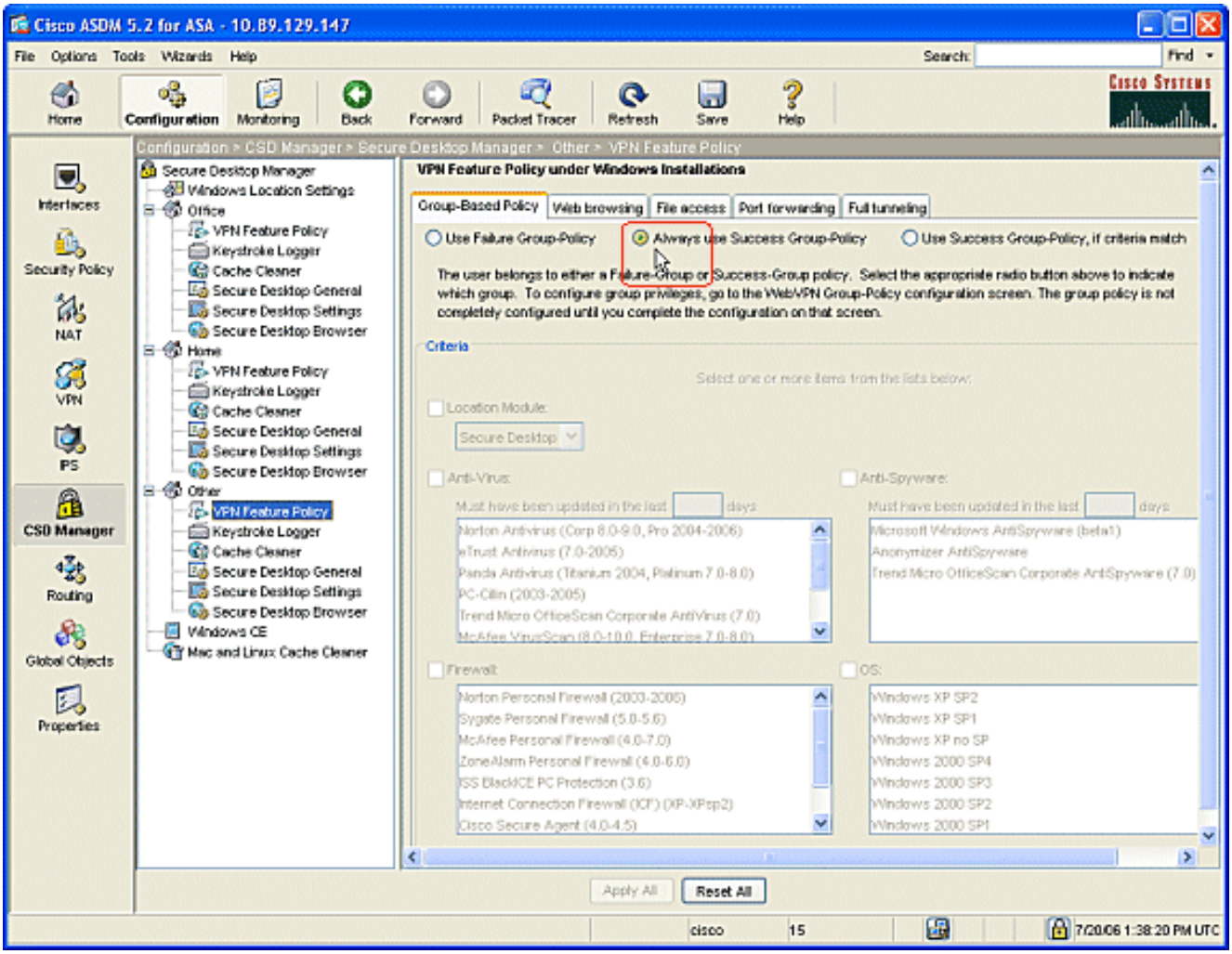
3. 홈 사용자의 경우, 각 기업은 액세스를 허용하기 전에 특정 정책을 요구할 수 있습니다.탐색 창에서 **Home(홈)**을 클릭하고 **VPN Feature Policy(VPN 기능 정책)를 클릭합니다.Group-Based Policy** 탭을 클릭합니다.특정 레지스트리 키, 알려진 파일 이름, 디지털 인증서 등 사전 구성된 기준이 일치하면 **Use Success Group-Policy** 라디오 버튼을 클릭합니다.Location **Module(위치 모듈)** 확인란을 선택하고 Secure **Desktop을 선택합니다**.회사 보안 정책에 따라 **안티바이러스, 안티스파이웨어, 방화벽** 및 **OS** 영역을 선택합니다.컴퓨터가 구성된 기준을 충족하지 않는 한 홈 사용자는 네트워크에 연결할 수 없습니다

.



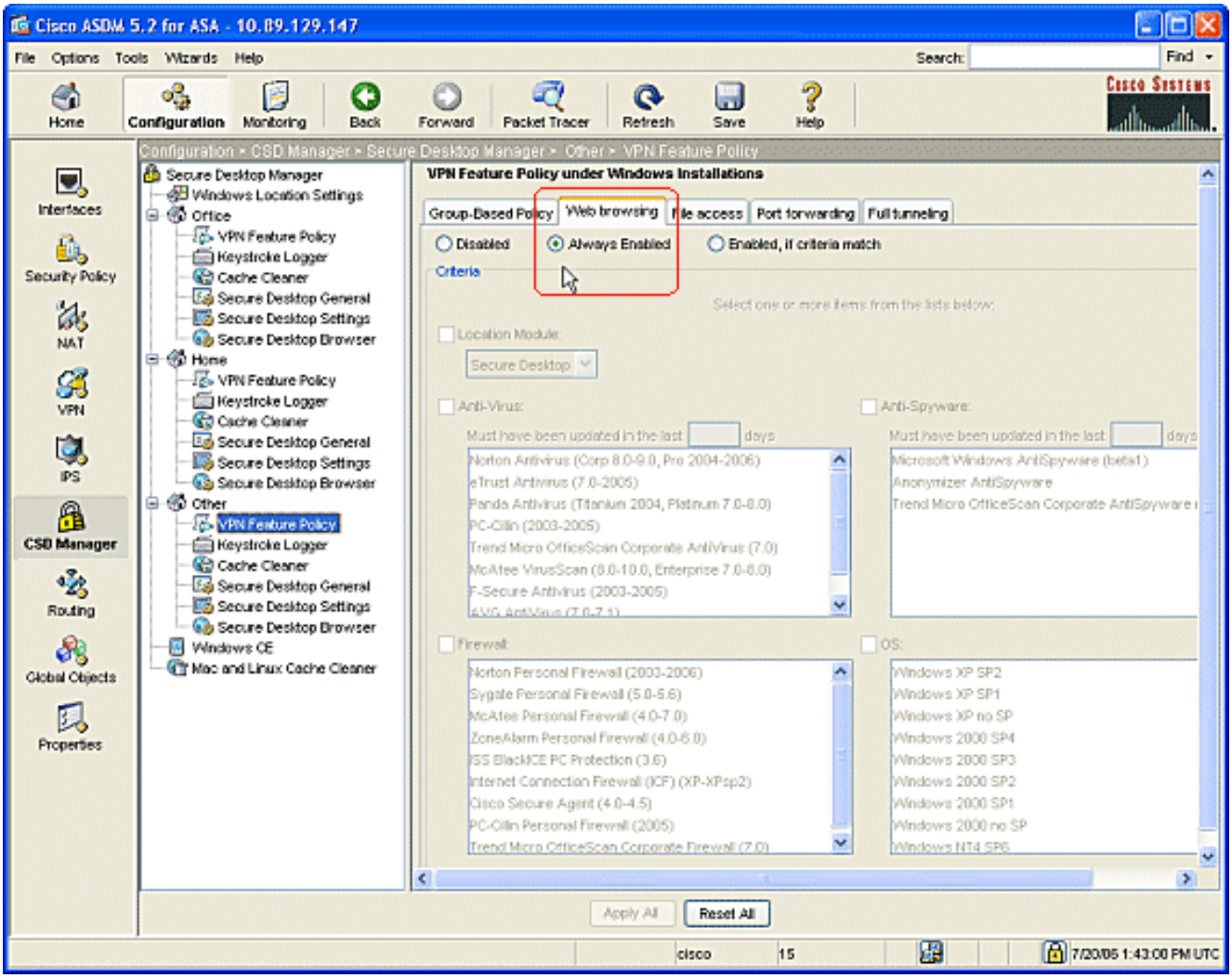
4. 탐색 창에서 **Other**(기타)를 클릭하고 **VPN Feature Policy(VPN 기능 정책)를 클릭합니다** .**Group-Based Policy** 탭을 클릭합니다.Always use **Success Group-Policy(항상 성공 그룹-정책 사용)** 라디오 버튼을 클릭합니다

.



5. 이 **VPN Feature Policy** 위치에 있는 클라이언트의 경우 **Web Browsing** 탭을 클릭하고 **Always Enabled** 라디오 다이얼을 클릭합니다.**File Access** 탭을 클릭하고 Disable 라디오 버튼을 클릭합니다.Port Forwarding(포트 전달) 및 **Full Tunneling(전체 터널링)** 탭을 사용하여 단계를 반복합니다.Apply **All을 클릭합니다**.Save(**저장**)를 클릭한 다음 **Yes(예)**를 클릭하여 변경 사항을 적용합니다

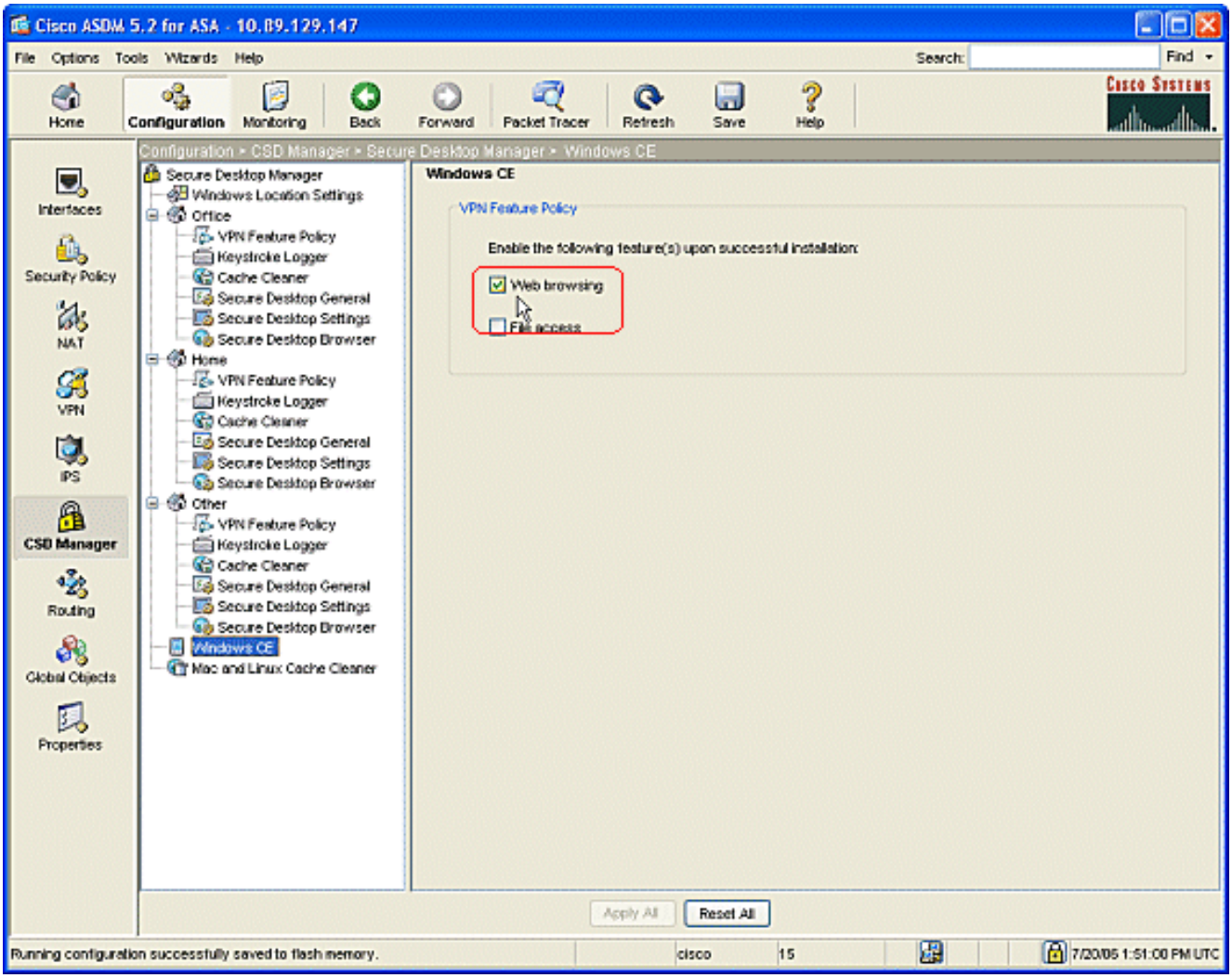
.



Windows CE, Macintosh 및 Linux 클라이언트에 대한 선택적 구성

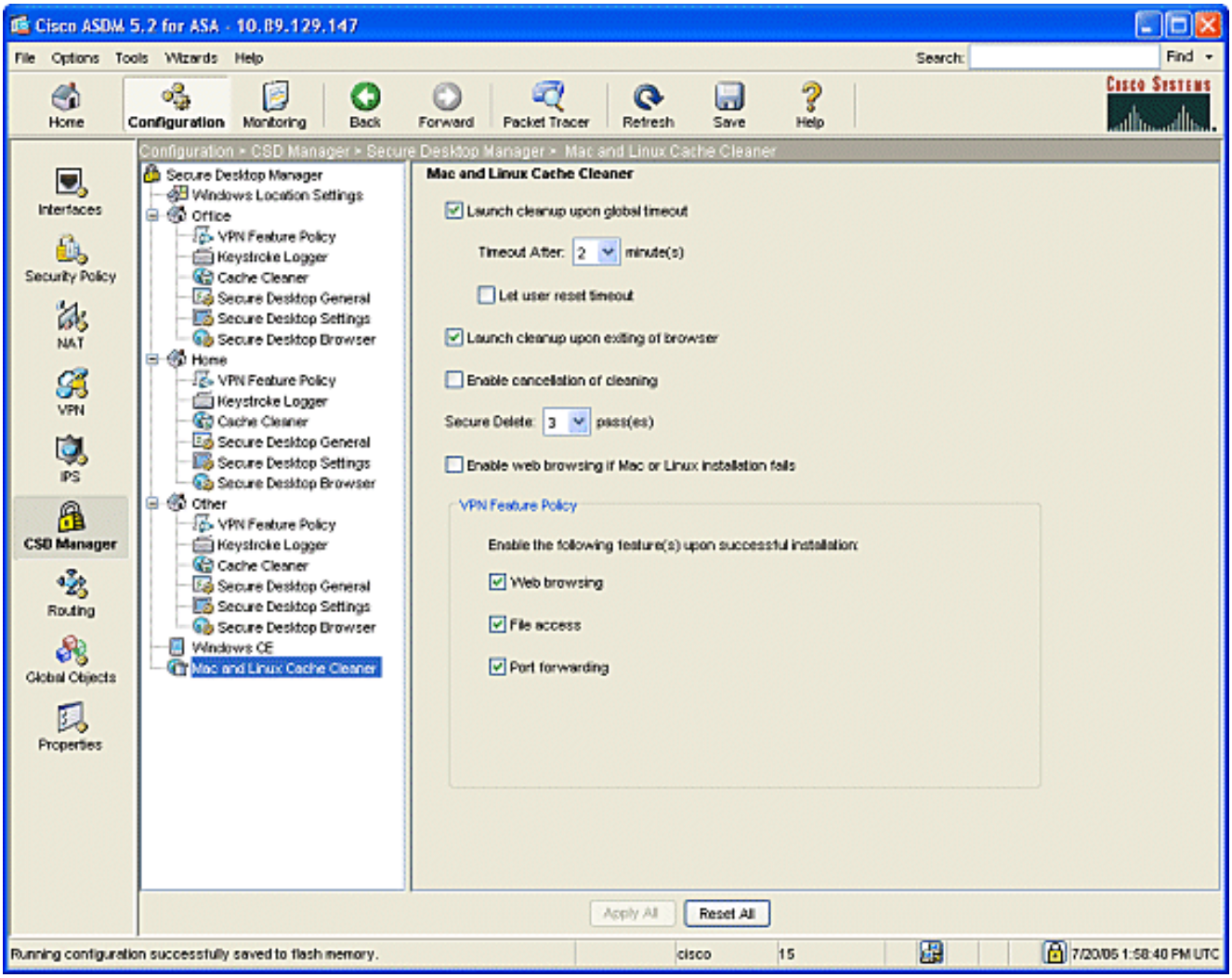
이러한 구성은 선택 사항입니다.

1. 탐색 창에서 **Windows CE**를 선택한 경우 **웹 검색** 확인란을 선택합니다
   .



2. 탐색 창에서 **Mac 및 Linux Cache Cleaner**를 선택한 경우 **전역 시간 제한** 라디오 다이얼 **시 실행 정리**를 선택합니다.시간 제한을 사양에 변경합니다.VPN **Feature Policy(VPN 기능 정책**) 영역에서 **웹 브라우징, 파일 액세스** 및 **포트 전달** 라디오 다이얼을 확인합니다

.



3. Windows CE 또는 Mac 및 Linux Cache Cleaner를 선택하든 Apply **All**(모두 적용)을 클릭합니다.
4. Save(**저장**)를 클릭한 다음 **Yes(예)**를 클릭하여 변경 사항을 적용합니다.

구성

구성

이 컨피그레이션은 CSD를 활성화하기 위해 ASDM이 변경한 사항을 반영합니다.대부분의 CSD 컨피그레이션은 플래시에 별도의 파일에 보관됩니다.

시스코아사

```
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
```

다음을 확인합니다.

이 섹션에서는 클라이언트리스 SSL VPN, 씬 클라이언트 SSL VPN 또는 SSL VPN 클라이언트(SVC)에 대한 컨피그레이션이 제대로 작동하고 있는지 확인합니다.

다양한 Windows 위치로 구성된 PC로 CSD를 테스트합니다.각 테스트에서는 위의 예에서 구성한 정책에 따라 다른 액세스를 제공해야 합니다.

포트 번호와 Cisco ASA가 WebVPN 연결을 수신하는 인터페이스를 변경할 수 있습니다.

- 기본 포트는 443입니다. 기본 포트를 사용하는 경우 액세스 권한은 https://ASA **IP Address입니다**.
- 다른 포트를 사용하면 https://ASA **IP Address:newportnumber**에 대한 액세스**가 변경됩니다**.

명령

여러 **show** 명령이 WebVPN과 연결되어 있습니다.CLI(Command Line Interface)에서 이러한 명령을 실행하여 통계 및 기타 정보를 표시할 수 있습니다.**show 명령**의 사용을 자세히 보려면 WebVPN 구성 확인을 참조하십시오.

참고: Output Interpreter Tool(등록된 고객만 해당)(OIT)은 특정 **show** 명령을 **지원합니다**.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

원격 클라이언트에 문제가 있는 경우 다음 사항을 확인하십시오.

1. 웹 브라우저에서 팝업, Java 및/또는 ActiveX가 활성화되어 있습니까?사용 중인 SSL VPN 연결 유형에 따라 이러한 연결을 활성화해야 할 수 있습니다.
2. 클라이언트는 세션 시작 시 표시되는 디지털 인증서를 수락해야 합니다.

명령

여러 **디버그** 명령이 WebVPN과 연결됩니다.이러한 명령에 대한 자세한 내용은 WebVPN 디버그 명령 사용을 참조하십시오.

참고: debug 명령을 사용하면 Cisco 디바이스에 부정적인 영향을 미칠 수 있습니다.debug 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance
- ASDM 및 NTLMv1 컨피그레이션을 사용하는 ASA with WebVPN 및 Single Sign-on 예
- 기술 지원 및 문서 – Cisco Systems