使用 ASDM 在 ASA 7.2.x 上配置适用于 Windows 的 Cisco Secure Desktop (CSD 3.1.x) 的配置示例

目录

简介

Cisco Secure Desktop (CSD) 扩展了 SSL VPN 技术的安全。CSD 在用户工作站上为会话活动提供了一个单独的分区。此保管库区域将在会话期间加密，并在 SSL VPN 会话结束后彻底删除。可以对 Windows 进行配置，使其具备 CSD 的所有安全优势。Macintosh、Linux 和 Windows CE 只能访问 Cache Cleaner、Web 浏览和文件访问功能。可以在以下平台上为 Windows、Macintosh、Windows CE 和 Linux 设备配置 CSD：

- Cisco 自适应安全设备 (ASA) 5500 系列
- 运行Cisco IOS软件版本12.4(6)T和以后的Cisco路由器
- Cisco VPN 3000 系列集中器 4.7 版及更高版本
- Catalyst 6500 和 7600 系列路由器上的 Cisco WebVPN 模块

注意： CSD 3.3 版本现在允许您将 Cisco Secure Desktop 配置为在运行 Microsoft Windows Vista

的远程计算机上运行。Cisco Secure Desktop 过去仅限于运行 Windows XP 或 2000 的计算机。有关详细信息，请参阅《Cisco Secure Desktop 发行版本注释（3.3 版）》的新增强功能 - Vista 上的 Secure Desktop 部分。

本示例主要包括如何在 ASA 5500 系列上为 Windows 客户端安装和配置 CSD。本文添加了 Windows CE、Mac 和 Linux 客户端的可选配置，以便补充完善。

CSD 与 SSL VPN 技术（无客户端 SSL VPN、瘦客户端 SSL VPN 或 SSL VPN 客户端 (SVC)）一起使用。CSD 为 SSL VPN 技术的安全会话创造了价值。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

ASA 设备要求

- Cisco CSD 3.1 版或更高版本
- Cisco ASA 软件版本 7.1.1 或更高版本
- Cisco 自适应安全设备管理器 (ASDM) 5.1.1 版或更高版本**注意：** 仅在 ASA 8.x 版上支持 CSD 3.2 版**注意：** 要使 ASDM 可配置 ASA，请参阅允许 ASDM 进行 HTTPS 访问。

客户端计算机要求

- 远程客户端应当具有本地管理特权；这不是必需的，但强烈建议进行此设置。
- 远程客户端必须安装有 Java Runtime Environment (JRE) 1.4 或更高版本。
- 远程客户端浏览器：Internet Explorer 6.0、Netscape 7.1、Mozilla 1.7、Safari 1.2.2 或 Firefox 1.0
- 已在远程客户端上启用 Cookie，并允许弹出窗口

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。此配置使用的 IP 地址为 RFC 1918 地址。这些 IP 地址不能在 Internet 上合法使用，只能在测试实验室环境中使用。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

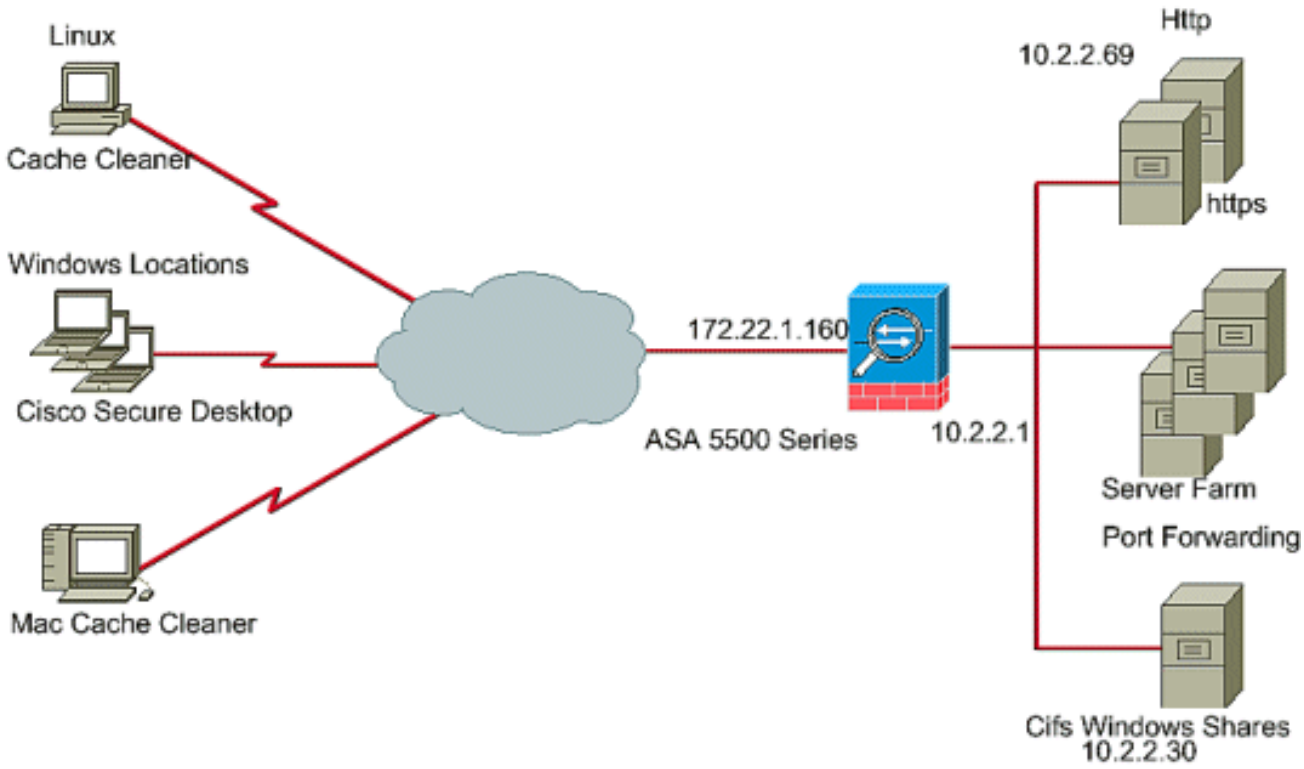
背景信息

CSD 与 SSL VPN 技术配合运行，因此应当在配置 CSD 之前激活无客户端、瘦客户端或 SVC。

网络图

可以对不同 Windows 位置进行配置，使 Windows 在所有层面上都具备 CSD 安全。Macintosh、Linux 和 Windows CE 只能访问 Cache Cleaner 和/或 Web 浏览和文件访问功能。

本文档使用以下网络设置：



在 ASA 上为 Windows 客户端配置 CSD

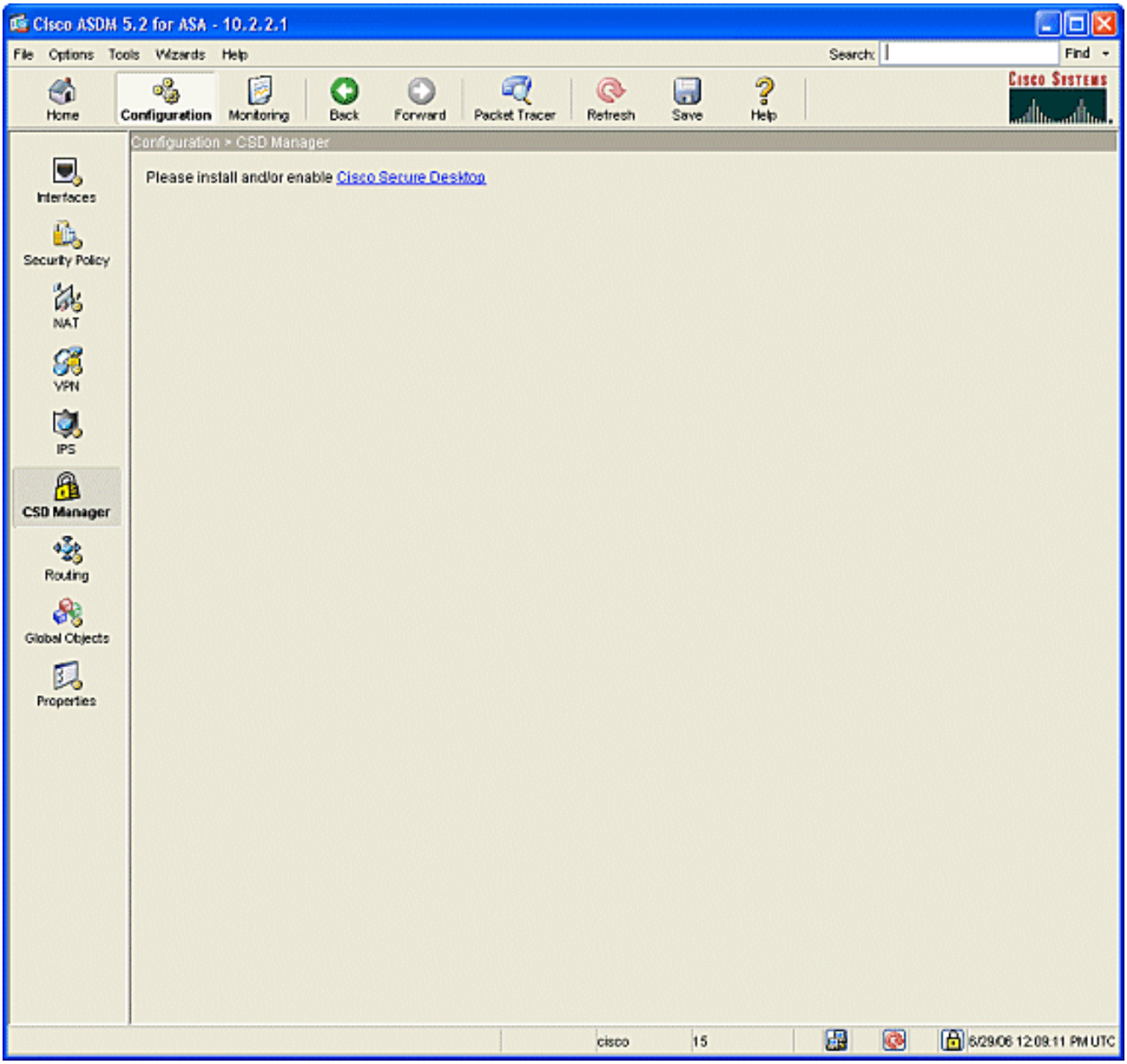
通过以下五个主要步骤，在 ASA 上为 Windows 客户端配置 CSD：

- 在 Cisco ASA 上获取、安装和启用 CSD 软件。
- 定义 Windows 位置。
- 定义 Windows 位置标识。
- 配置 Windows 位置模块。
- 配置 Windows 位置功能。
- Windows CE、Macintosh 和 Linux 客户端的可选配置。

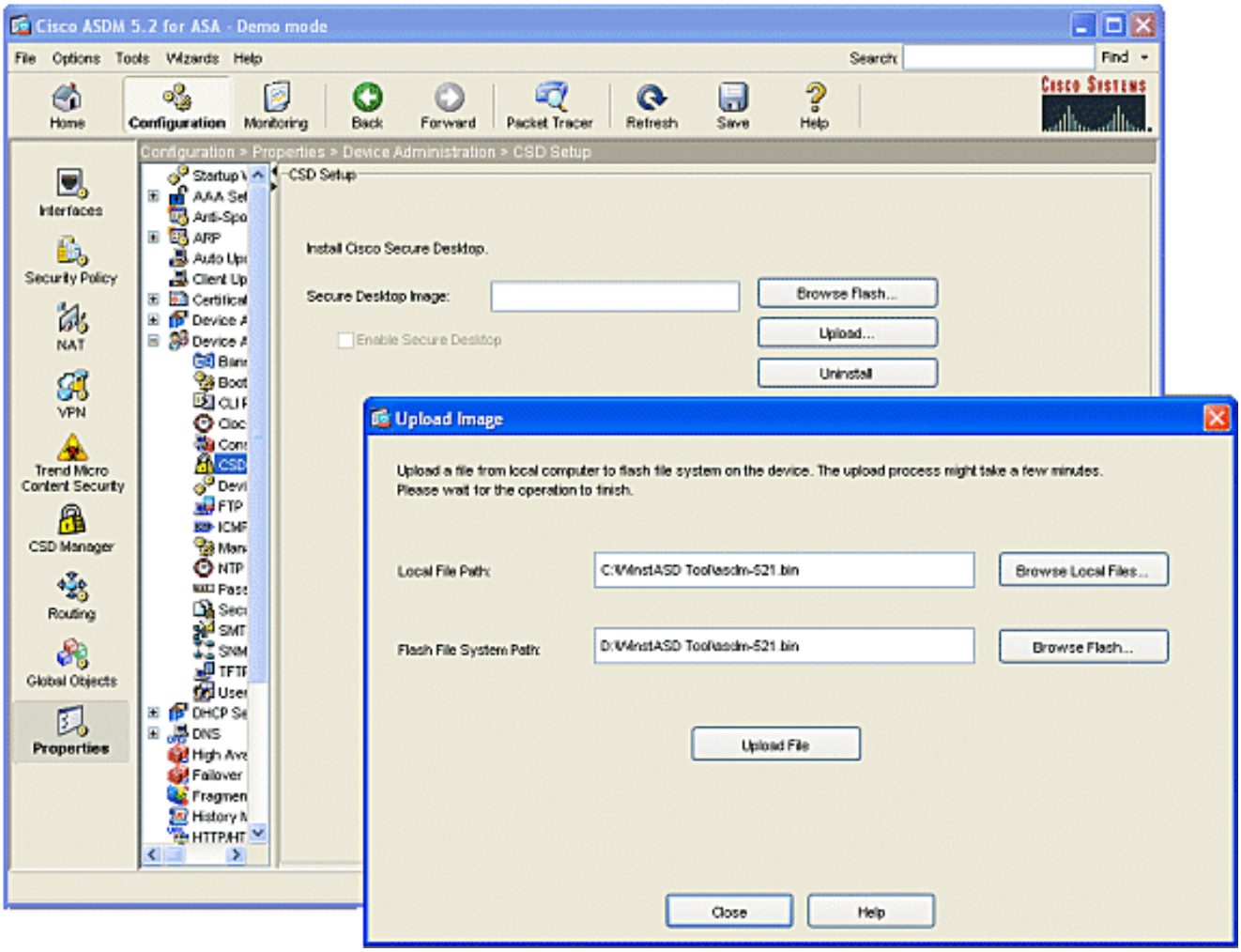
获取、安装和启用 CSD 软件

完成以下步骤，以便在 Cisco ASA 上获取、安装和启用 CSD 软件。

1. 在 Cisco 软件下载网站上，将 CSD 软件 securedesktop-asa*.pkg 和自述文件下载到您的管理站。
2. 登录 ASDM 并单击 **Configuration** 按钮。在左菜单中，单击 **CSD Manager** 按钮，然后单击“Cisco Secure Desktop”链接。



3. 单击 **Upload** 显示“Upload Image”窗口。输入新 .pkg 文件在管理站上的路径，或者单击 **Browse Local Files** 查找文件。输入要在闪存上存放文件的位置，或者单击 **Browse Flash**。单击 **Upload File**。出现提示时，单击 **OK > Close > OK**。

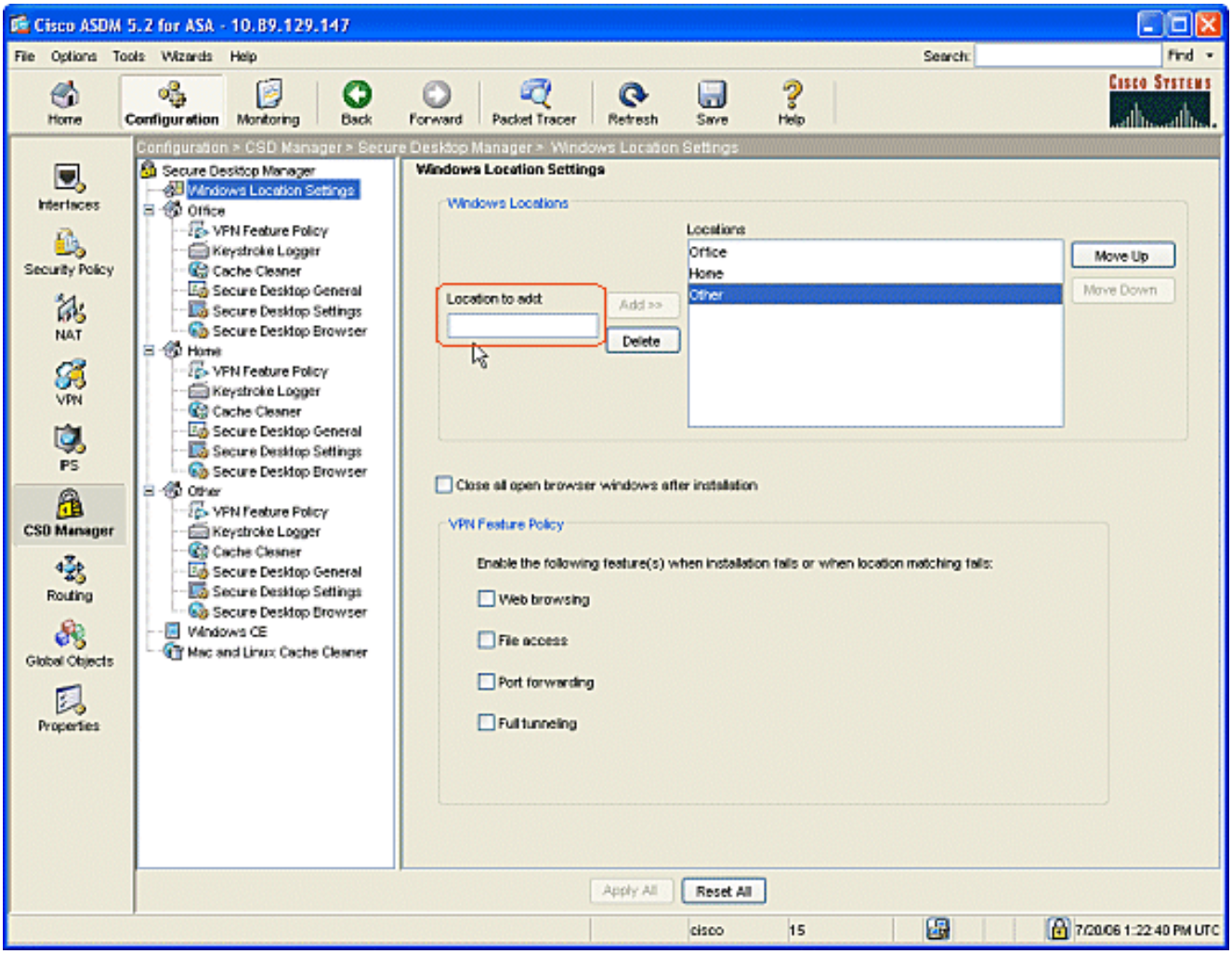


4. 客户端映像加载到闪存后，选中 **Enable SSL VPN Client** 复选框，然后单击 Apply。
5. 单击 **Save**，然后单击 **Yes** 接受更改。

定义 Windows 位置

完成以下步骤，以便定义 Windows 位置。

1. 单击 **Configuration** 按钮。
2. 在左菜单中，单击 **CSD Manager** 按钮，然后单击“Cisco Secure Desktop”链接。
3. 在导航窗格中，单击 **Windows Location Settings**。
4. 在“Location to Add”字段中键入位置名称，然后单击 **Add**。请注意本示例中的三个位置：“Office”、“Home”和“Others”。“Office”表示位于公司安全范围内的工作站。“Home”表示在家工作的用户。“Other”表示除上述两个位置以外的任何位置。

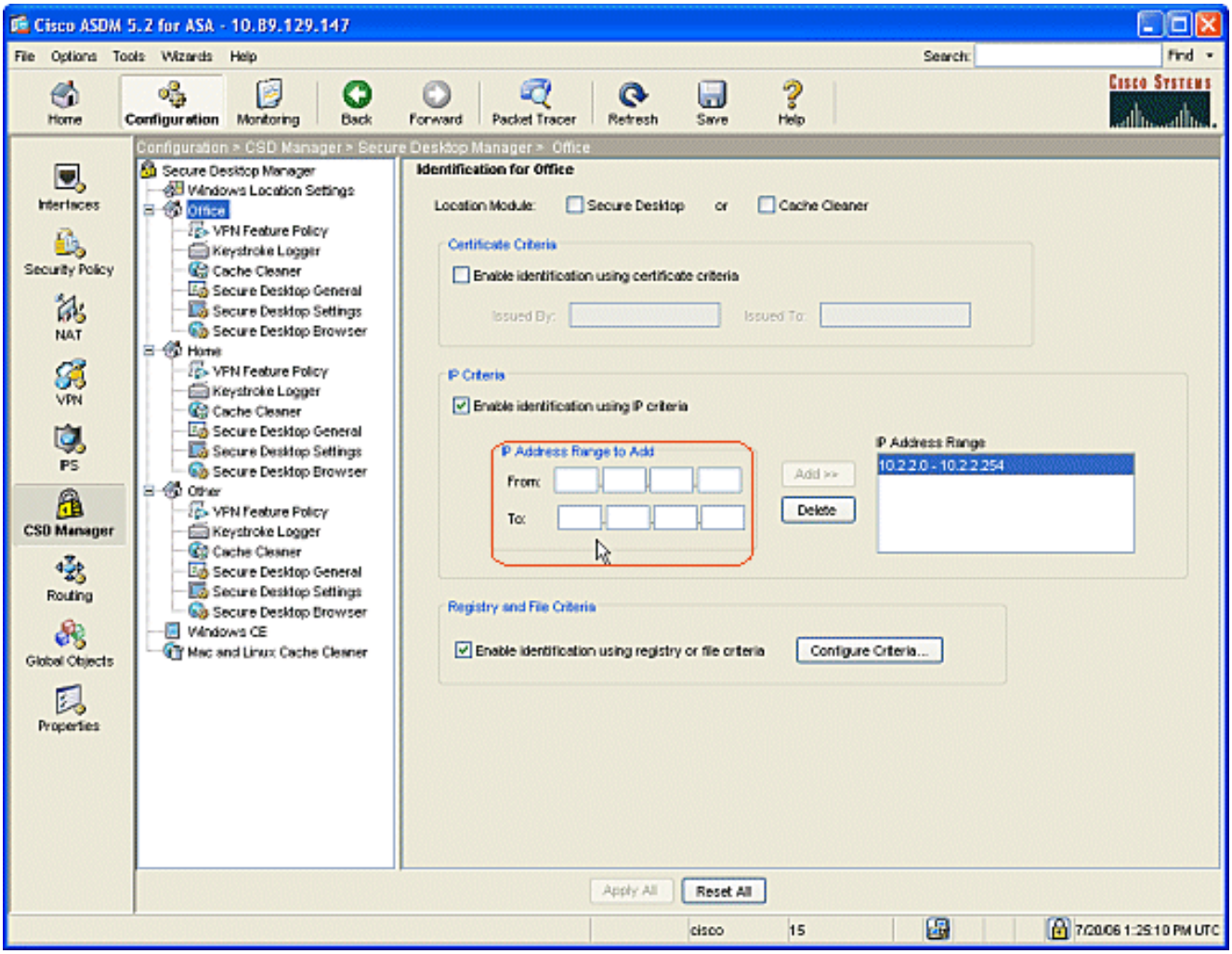


5. 根据网络体系结构布局，为销售、访客、合作伙伴或其他人员创建您自己的位置。
6. 在创建 Windows 位置时，导航窗格将随每个新位置的可配置模块扩展。单击 **Apply All**。
7. 单击 **Save**，然后单击 **Yes** 接受更改。

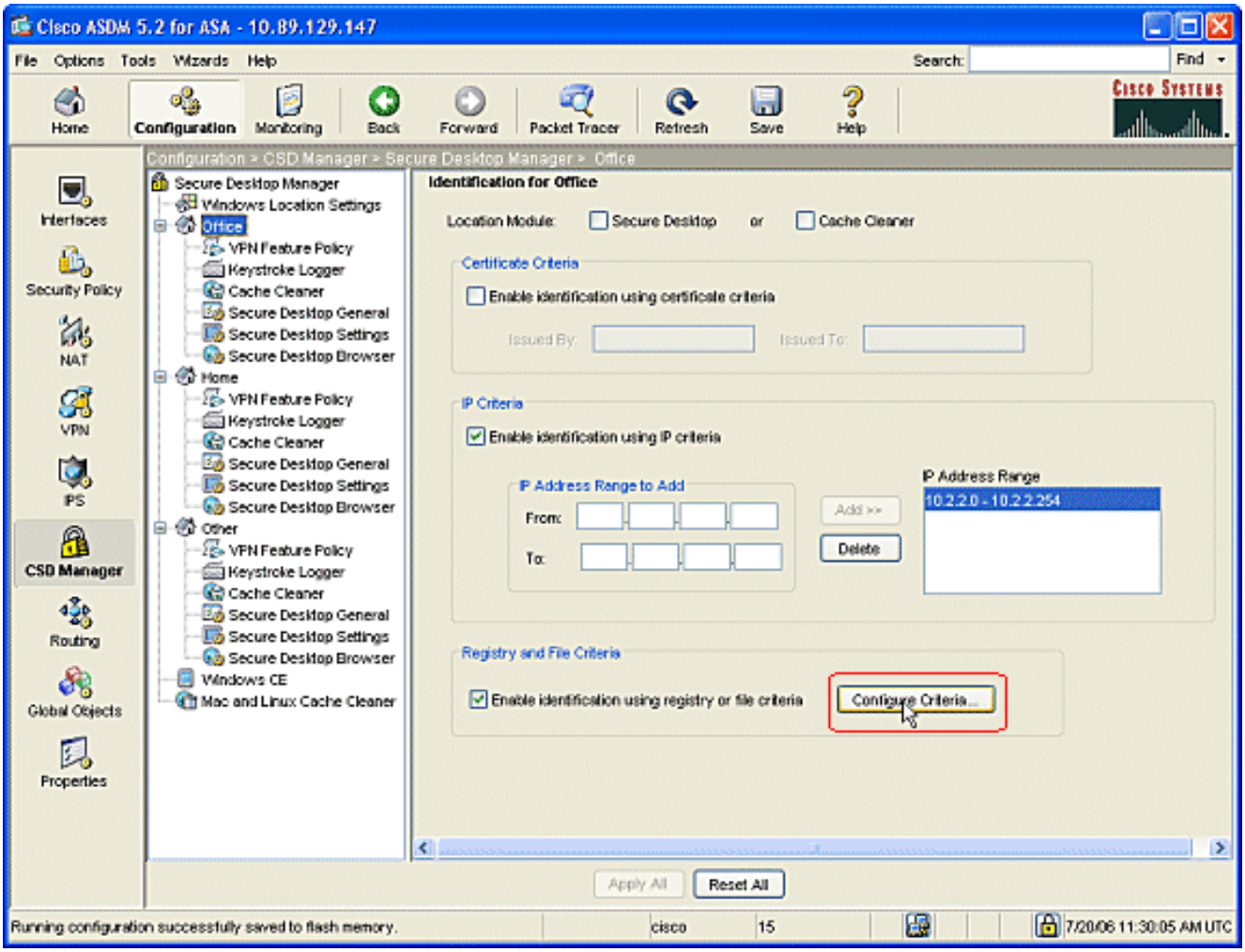
Windows 位置标识

完成以下步骤，以便定义 Windows 位置标识。

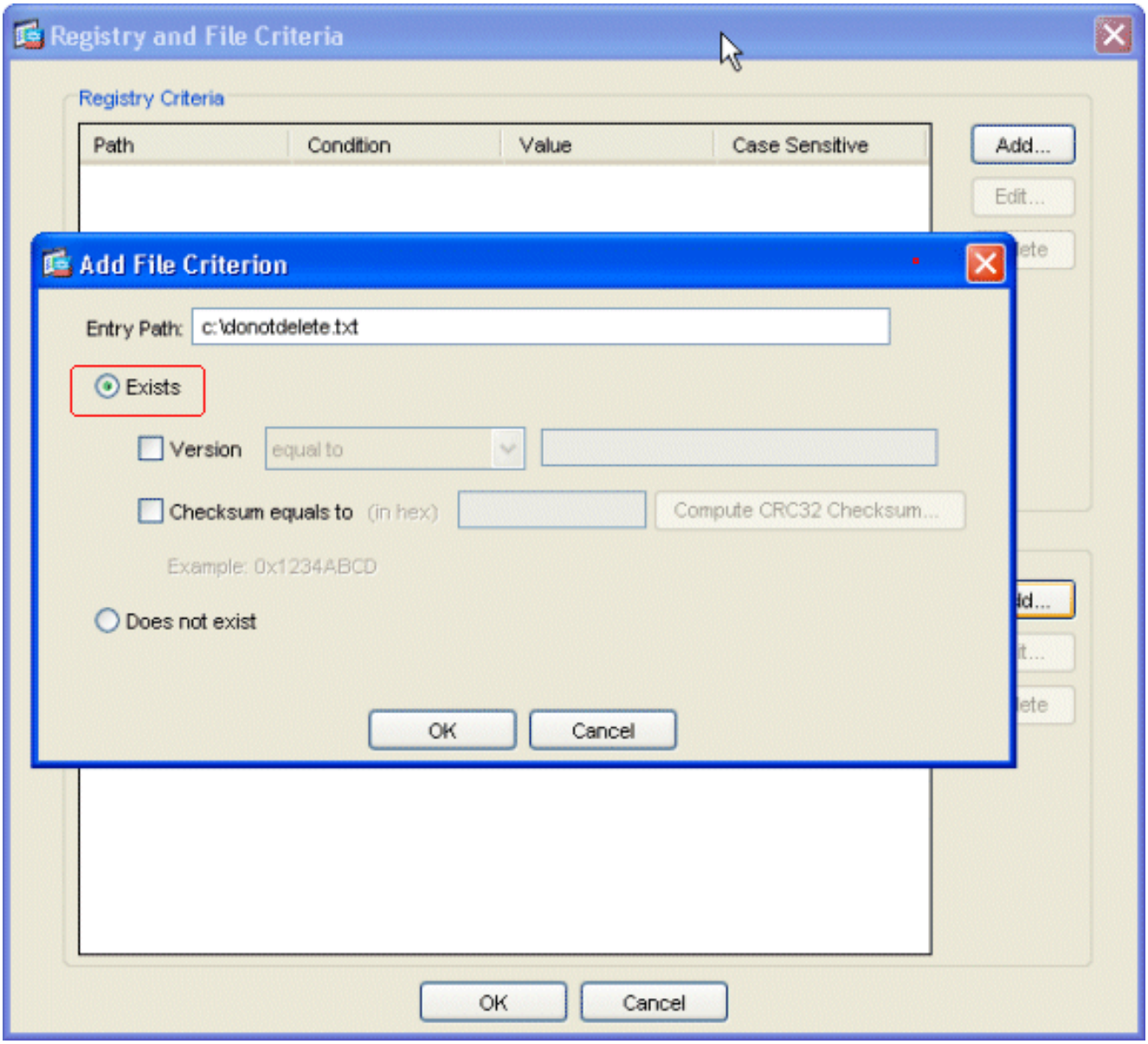
1. 标识在定义 Windows 位置中创建的位置。



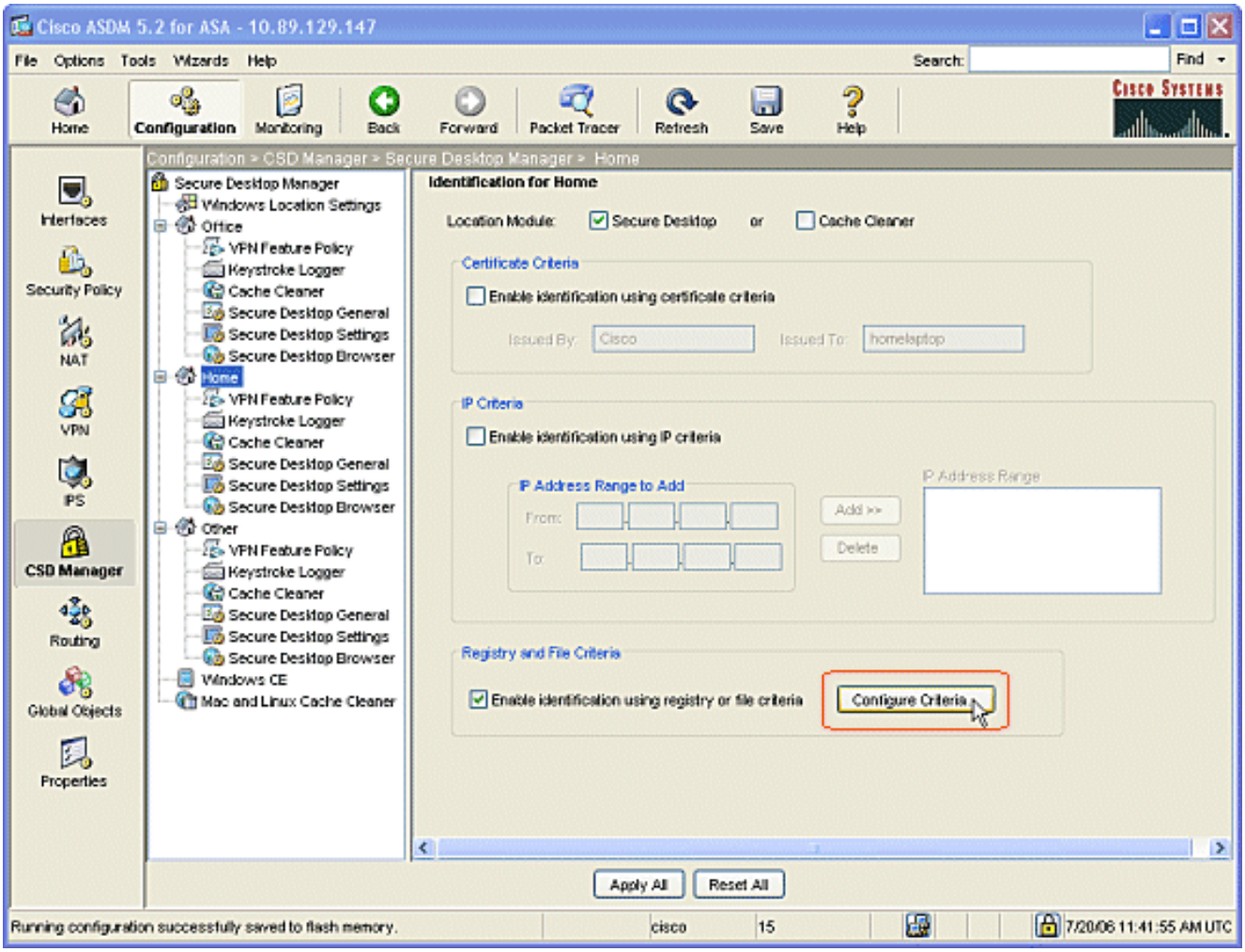
2. 要标识位置“Office”，请在导航窗格中单击 **Office**。取消选中 **Secure Desktop** 和“Cache Cleaner”，这是因为它们不是内部计算机。选中 **Enable identification using IP criteria**。输入内部计算机的 IP 地址范围。选中 **Enable identification using registry or file criteria**。这可以将内部办公人员同网络上的偶尔访客区分开来。



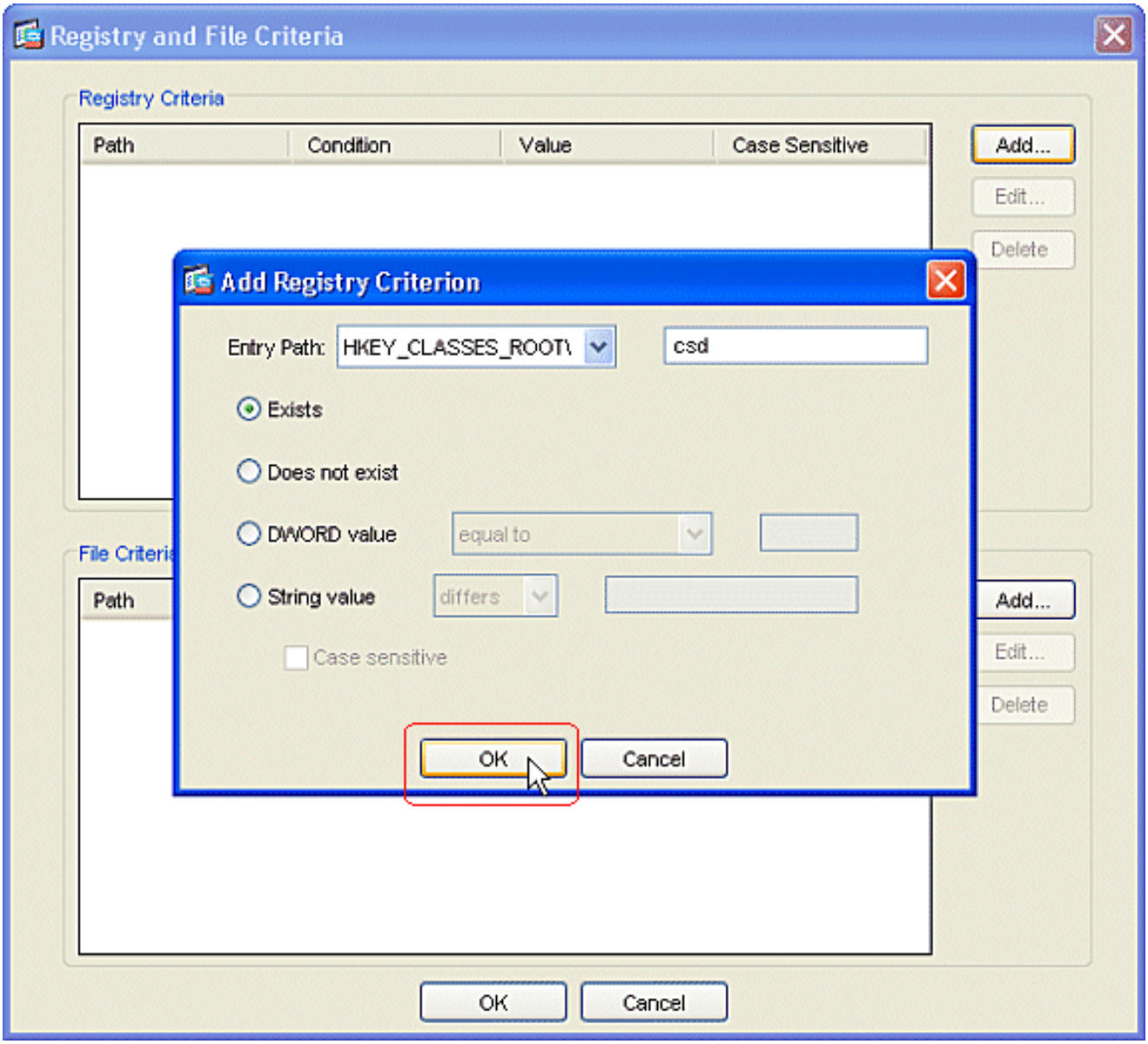
3. 单击 **Configure Criteria**。配置“DoNotDelete.txt”文件的简单示例。此文件必须位于内部 Windows 计算机上，并且仅用作占位符。也可以通过配置 Windows 注册表项来标识内部办公室计算机。点击OKIN添加文件标准窗口。点击OKIN注册和文件标准窗口。



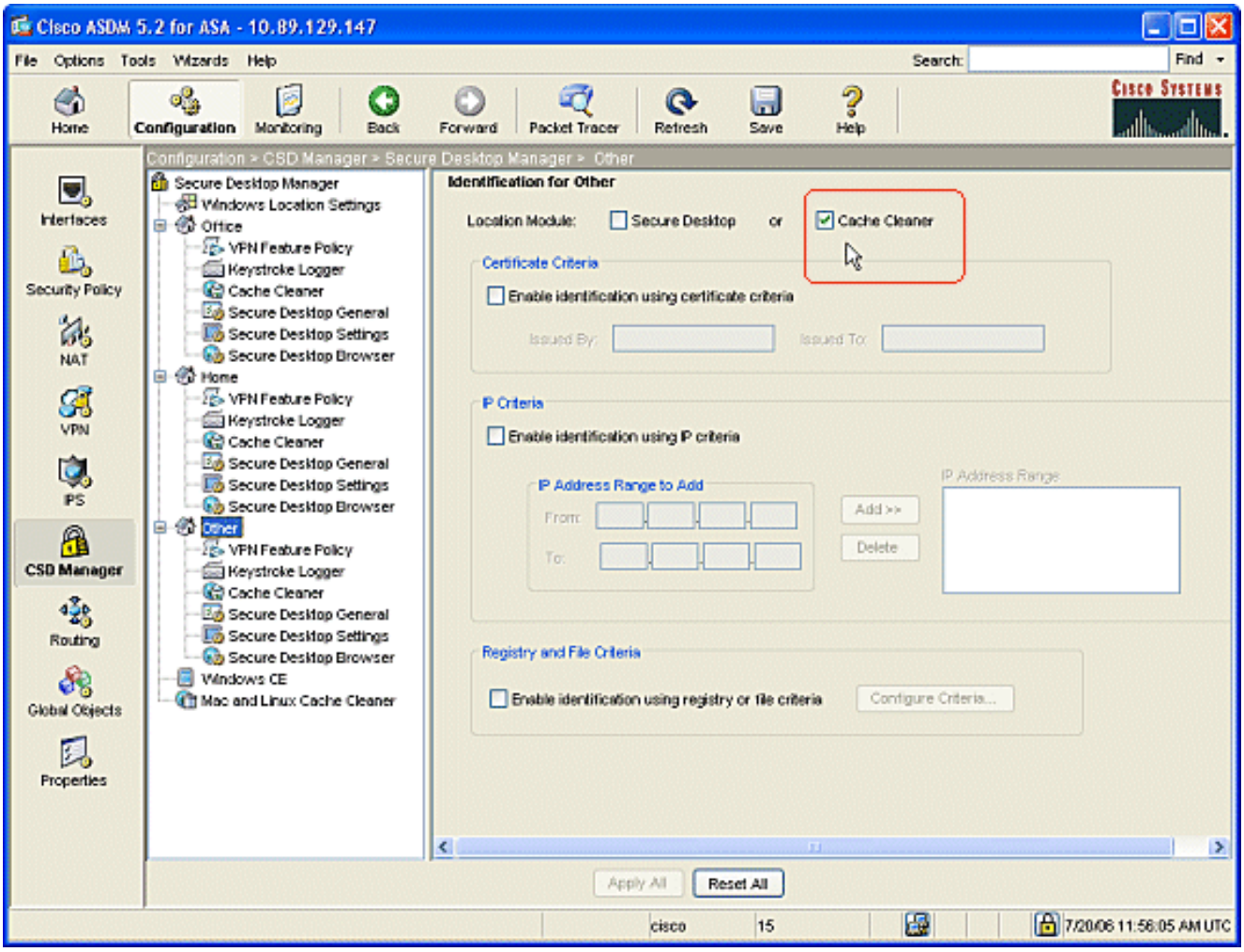
4. 在“Identification for Office”窗口中单击 **Apply All**。单击 **Save**，然后单击 **Yes** 接受更改。
5. 要标识位置“Home”，请在导航窗格中单击 **Home**。选中 **Enable identification using registry or file criteria**。单击 **Configure Criteria**。



6. 管理员必须使用此注册表项配置“Home”计算机客户端。在“Add Registry Criterion”窗口中单击 **OK**。在“Registry and File Criteria”窗口中单击 **OK**。



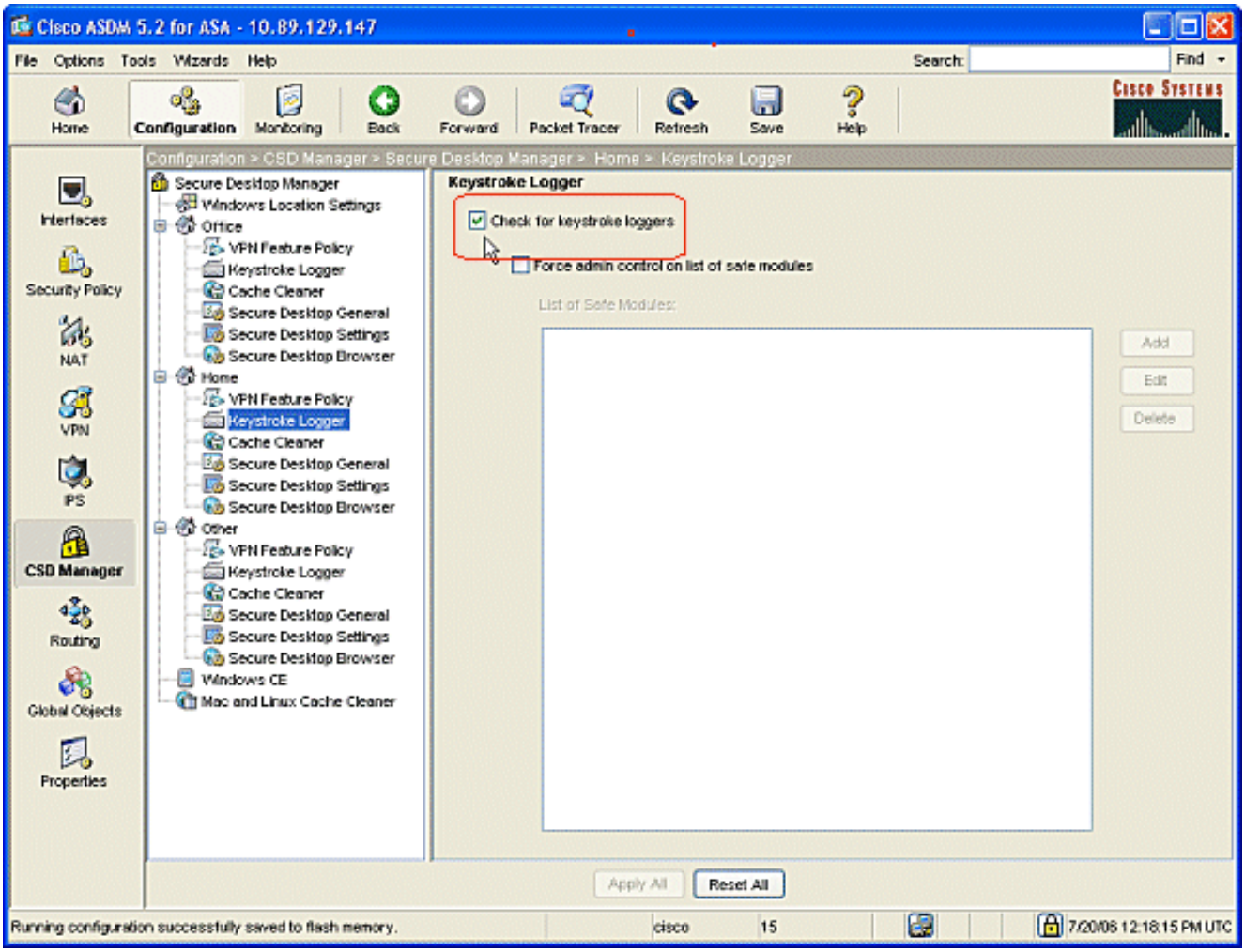
7. 在“Location Module”下，选中 **Secure Desktop**。在“Identification for Home”窗口中单击 **Apply All**。单击 **Save**，然后单击 **Yes** 接受更改。
8. 要标识位置 **Other**，请在导航窗格中单击“Other”。仅选中 **Cache Cleaner** 框，并取消选中所有其他框。在“Identification for Other”窗口中单击 **Apply All**。单击 **Save**，然后单击 **Yes** 接受更改。



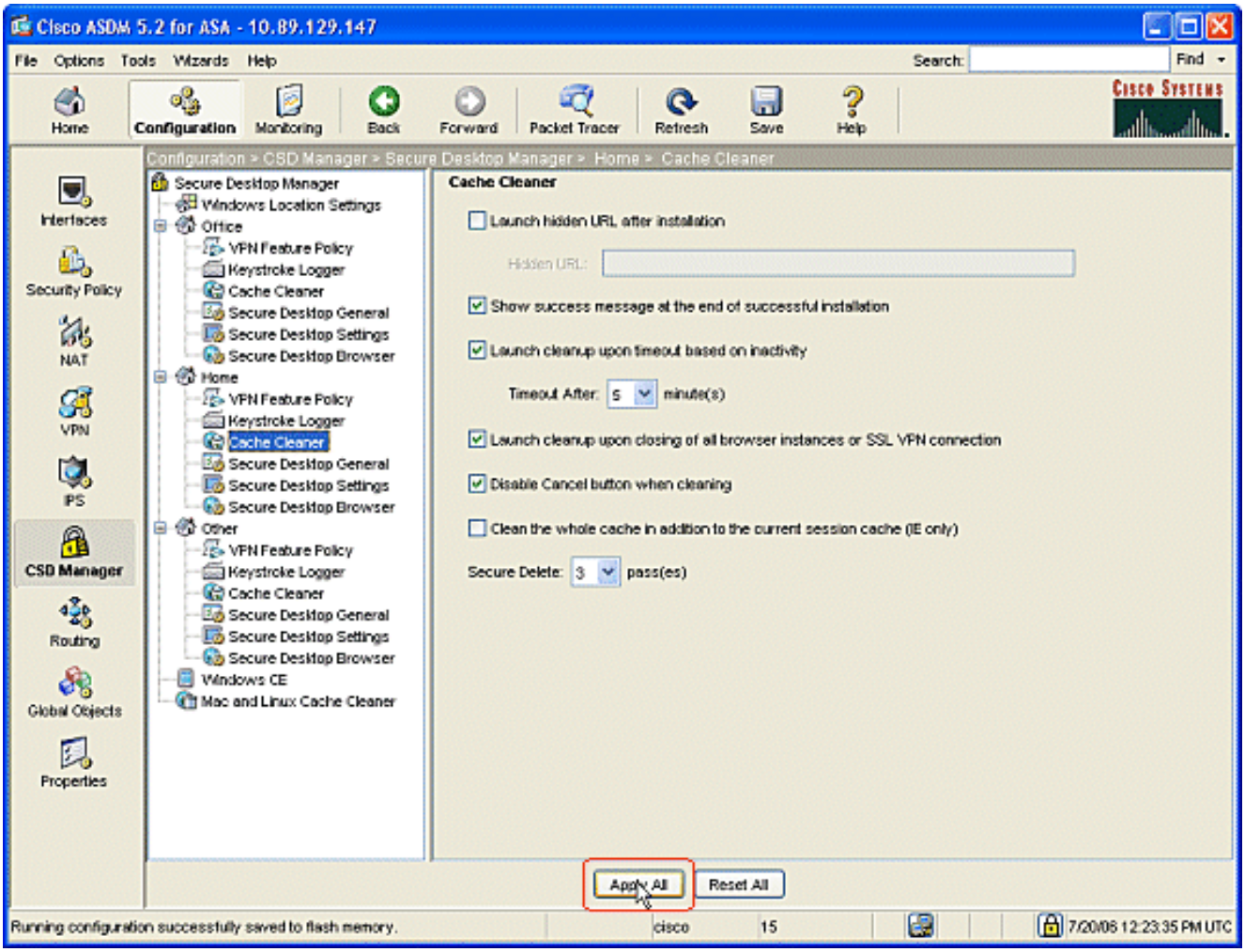
配置 Windows 位置模块

完成以下步骤，以便在创建的三个位置中的每个位置下配置模块。

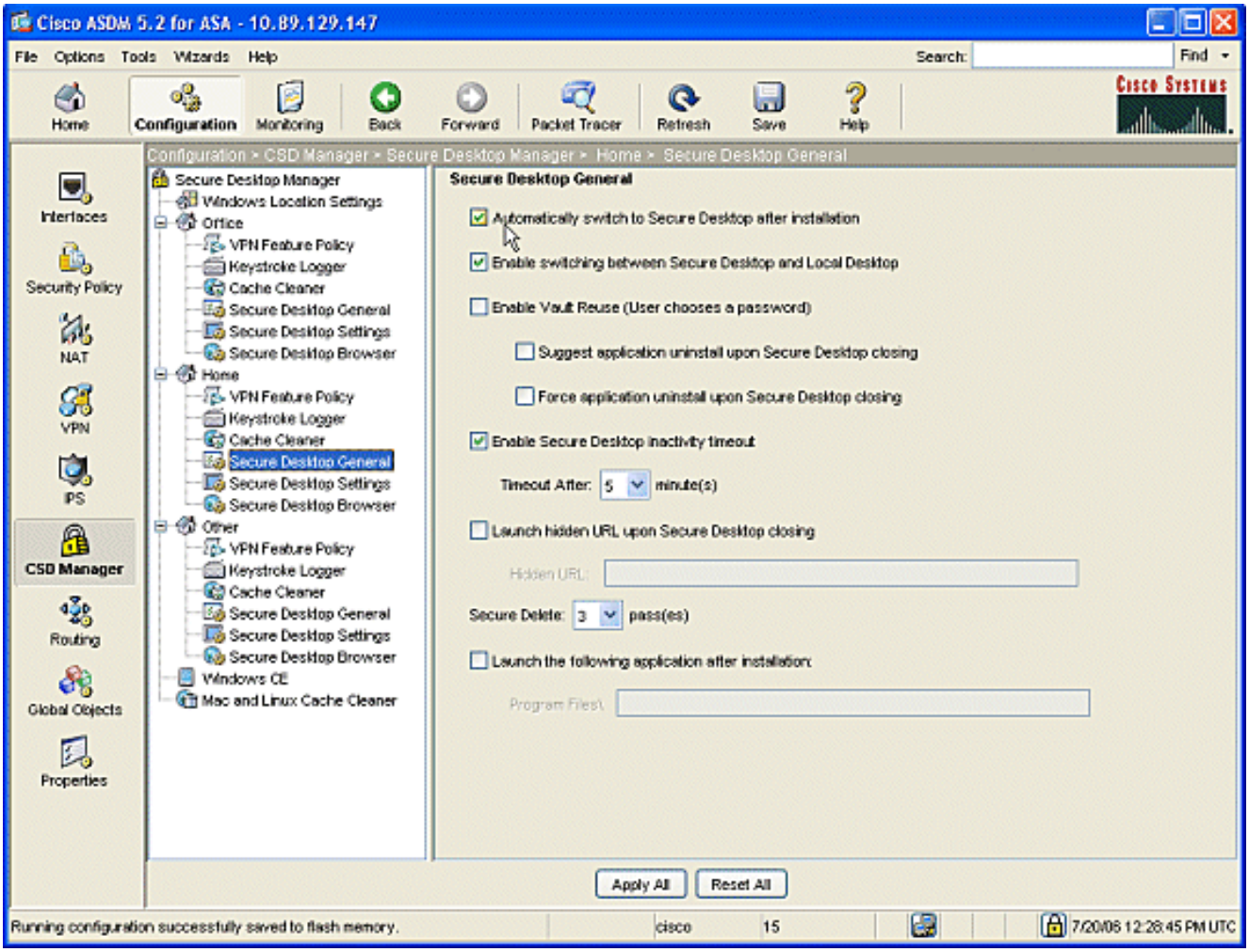
1. 对于“Office”客户端，由于未在上一步骤中选择“Secure Desktop”和“Cache Cleaner”，因此请勿执行任何操作。通过 ASDM 应用程序，您可以配置缓存清理软件，即使未在上一步骤中选择它也是如此。保持“Office”位置的默认设置。**注意：** 本步骤未讨论 VPN 功能策略，该策略将在所有位置的后续步骤中进行讨论。
2. 对于“Home”客户端，请在导航窗格中单击 **Home** 和“Keystroke Logger”。在“Keystroke Logger”窗口中，选中 **Check for keystroke loggers**。在“Keystroke Logger”窗口中单击 **Apply All**。单击 **Save**，然后单击 **Yes** 接受更改。



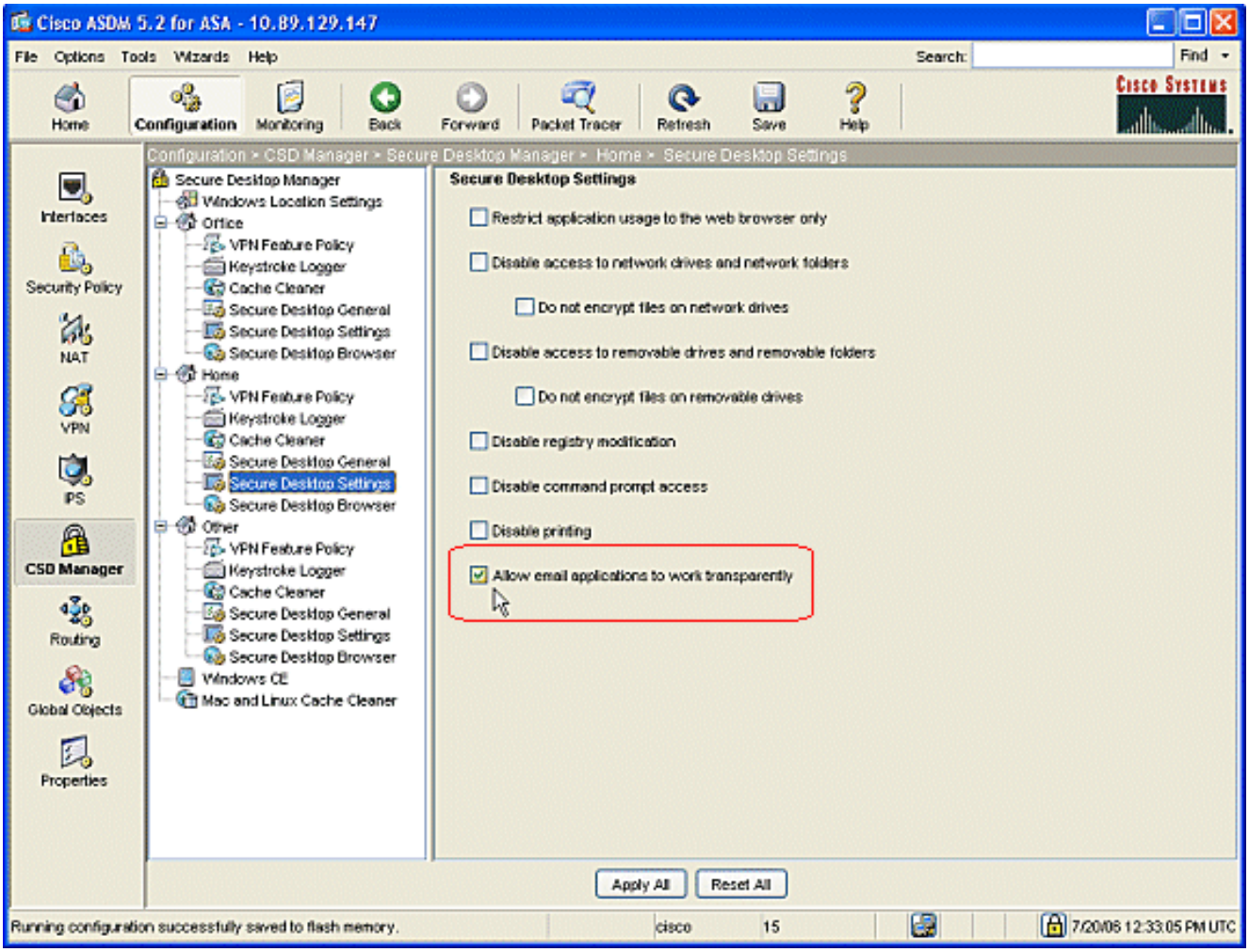
3. 在“Home”下选择 **Cache Cleaner** 和适合您的环境的参数。



4. 在“Home”下选择 **Secure Desktop General** 和适合您的环境的参数。



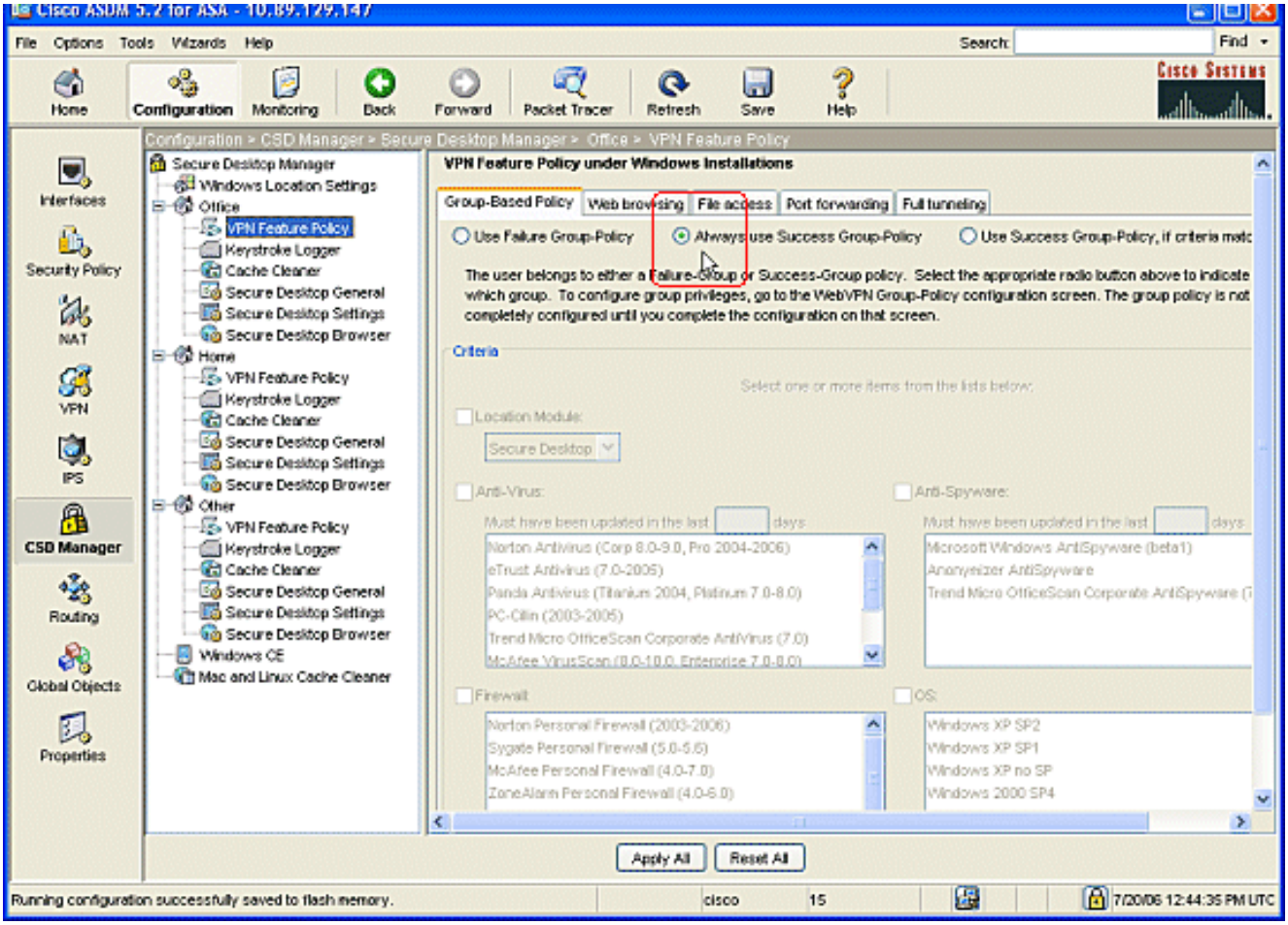
5. 在“Home”下选择 **Secure Desktop Settings**。选中 **Allow email applications to work transparently**，并配置适合您的环境的其他设置。单击 **Apply All**。单击 **Save**，然后单击 **Yes** 接受更改。



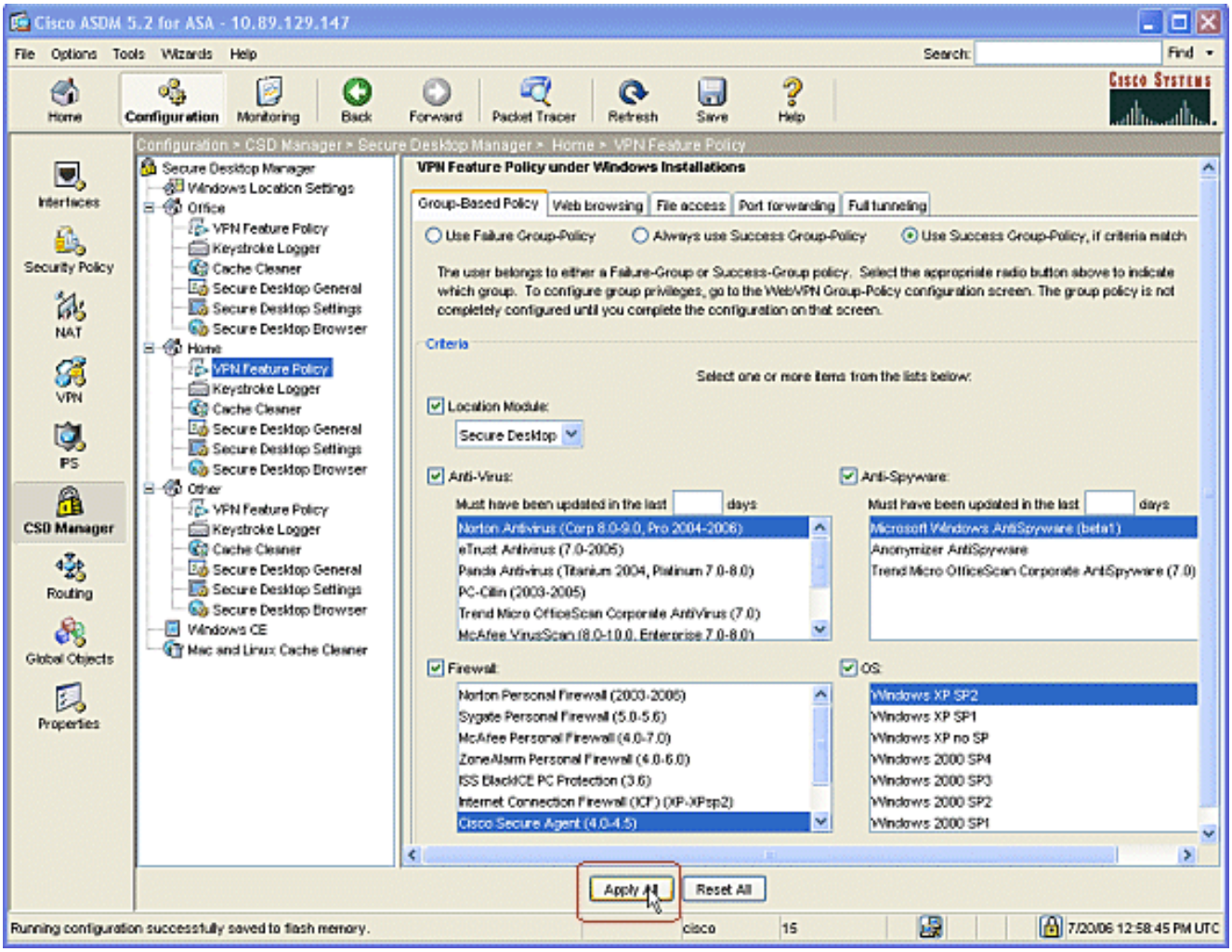
配置 Windows 位置功能

为创建的每个位置配置 VPN 功能策略。

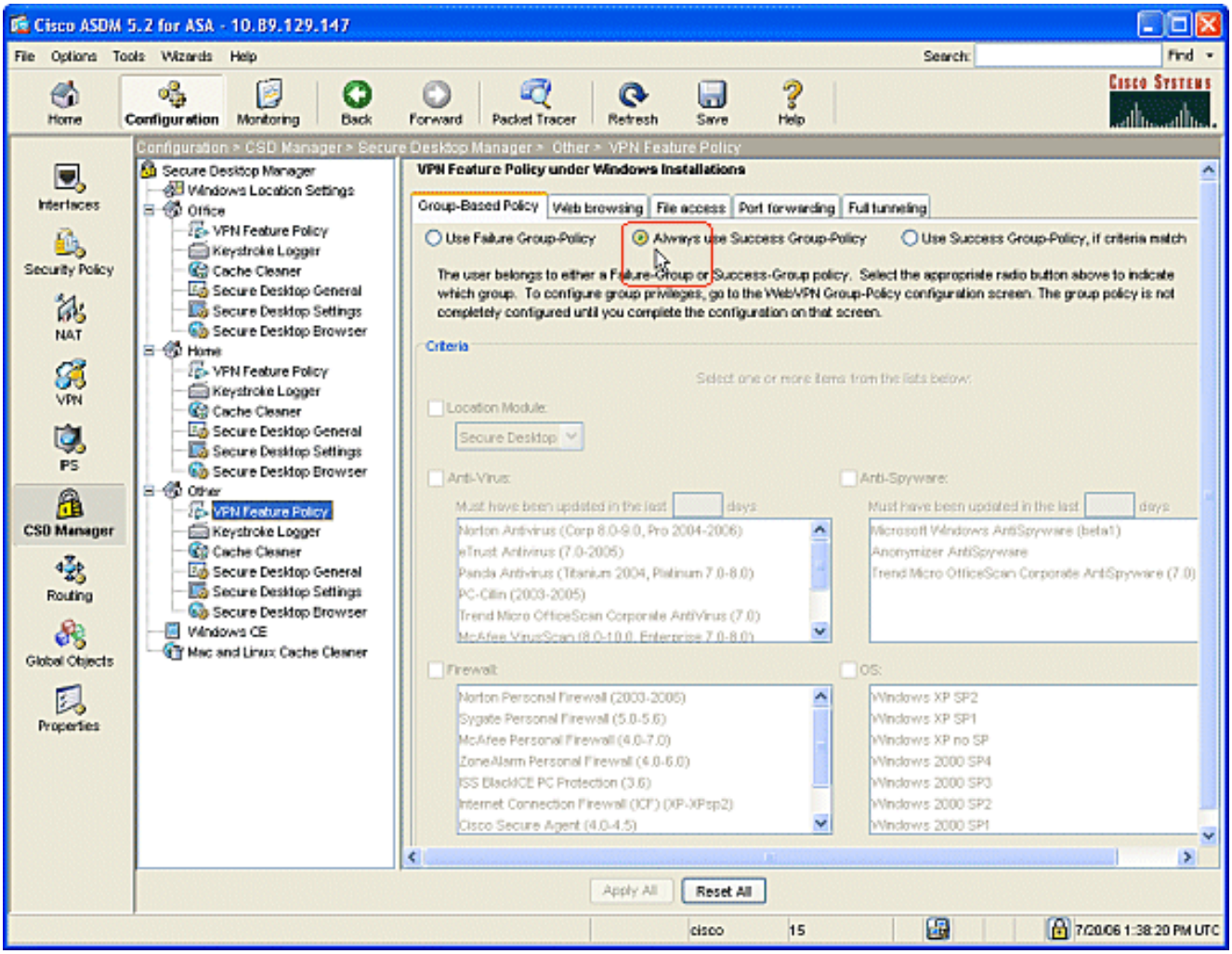
1. 在导航窗格中，单击“Office”，然后单击 **VPN Feature Policy**。
2. 单击 **Group-Based Policy** 选项卡。单击 **Always use Success Group-Policy** 单选按钮。单击 **Web browsing** 选项卡，并选中“Always Enabled”单选按钮。针对**“File access”**、**“Port forwarding”**和“Full tunneling”选项卡执行相同步骤。单击 **Apply All**。单击 **Save**，然后单击 **Yes** 接受更改。



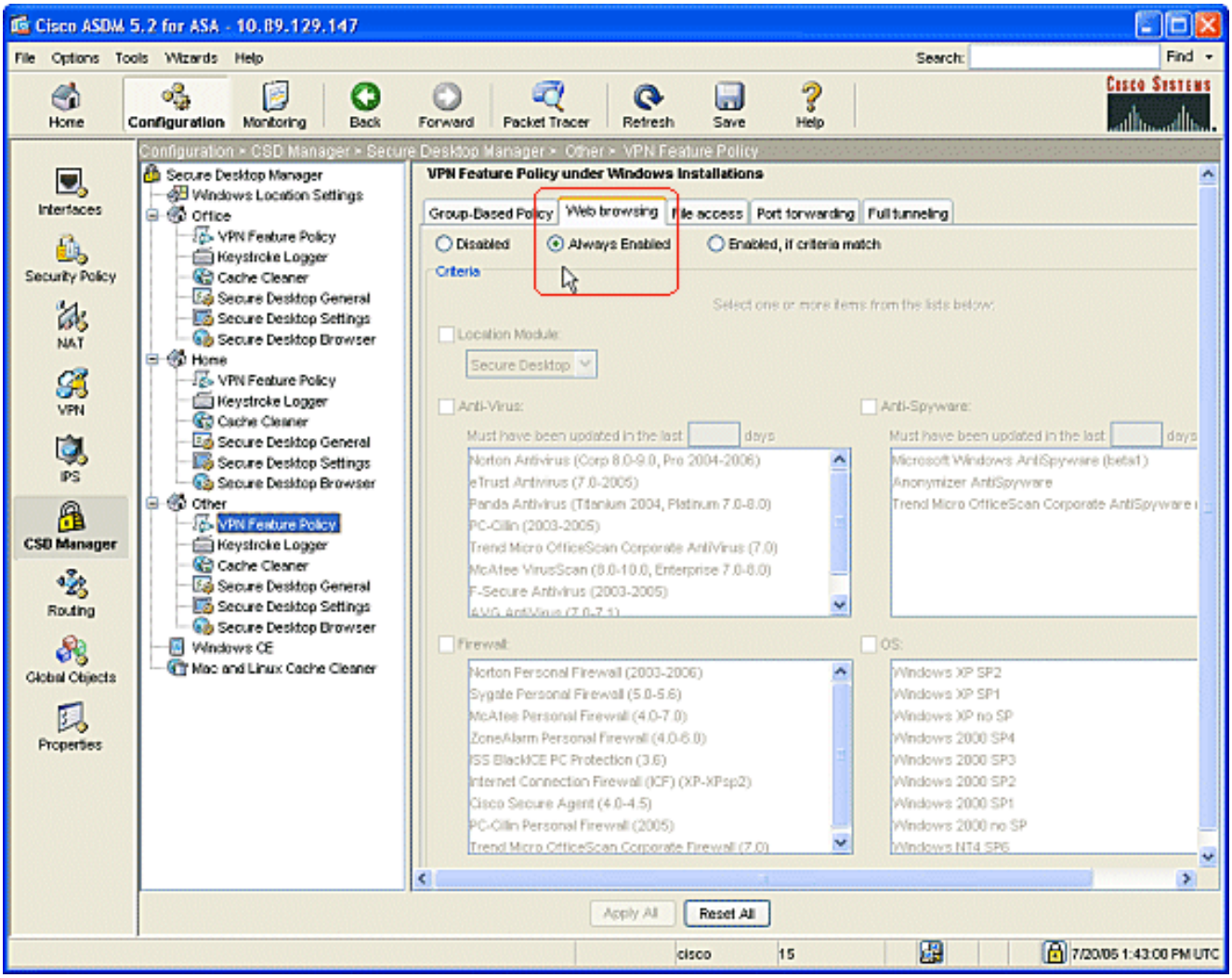
3. 在允许“Home”用户访问之前，各个公司可以要求采用特定策略。在导航窗格中，单击 **Home**，然后单击“VPN Feature Policy”。单击 **Group-Based Policy** 选项卡。如果预先配置的标准（如特定注册表项、已知文件名或数字证书）匹配，请单击 **Use Success Group-Policy** 单选按钮。选中 **Location Module** 复选框，然后选择“Secure Desktop”。根据公司安全策略，选择 **Anti-Virus, Anti-Spyware, Firewall** 和“OS”区域。除非“Home”用户的计算机符合已配置的标准，否则禁止“Home”用户访问网络。



4. 在导航窗格中，单击 **Other**，然后单击“VPN Feature Policy”。单击 **Group-Based Policy** 选项卡。单击 **Always use Success Group-Policy** 单选按钮。



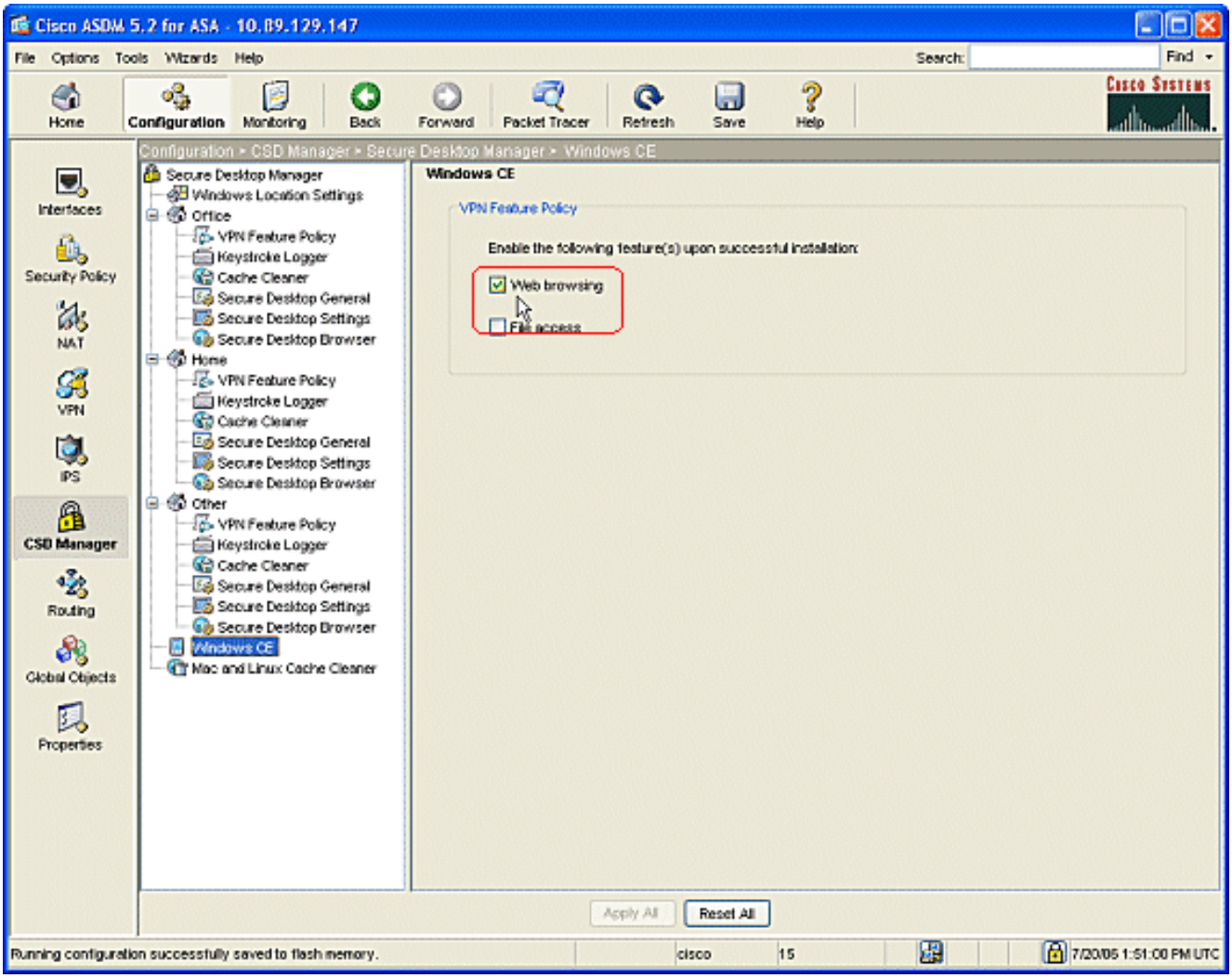
5. 对于此 **VPN Feature Policy** 位置中的客户端，请单击“Web Browsing”选项卡，然后单击“Always Enabled”单选按钮。单击 **File Access** 选项卡，然后单击“Disable”单选按钮。请对 **Port Forwarding** 和“Full Tunneling”选项卡重复此步骤。单击 **Apply All**。单击 **Save**，然后单击 **Yes** 接受更改。



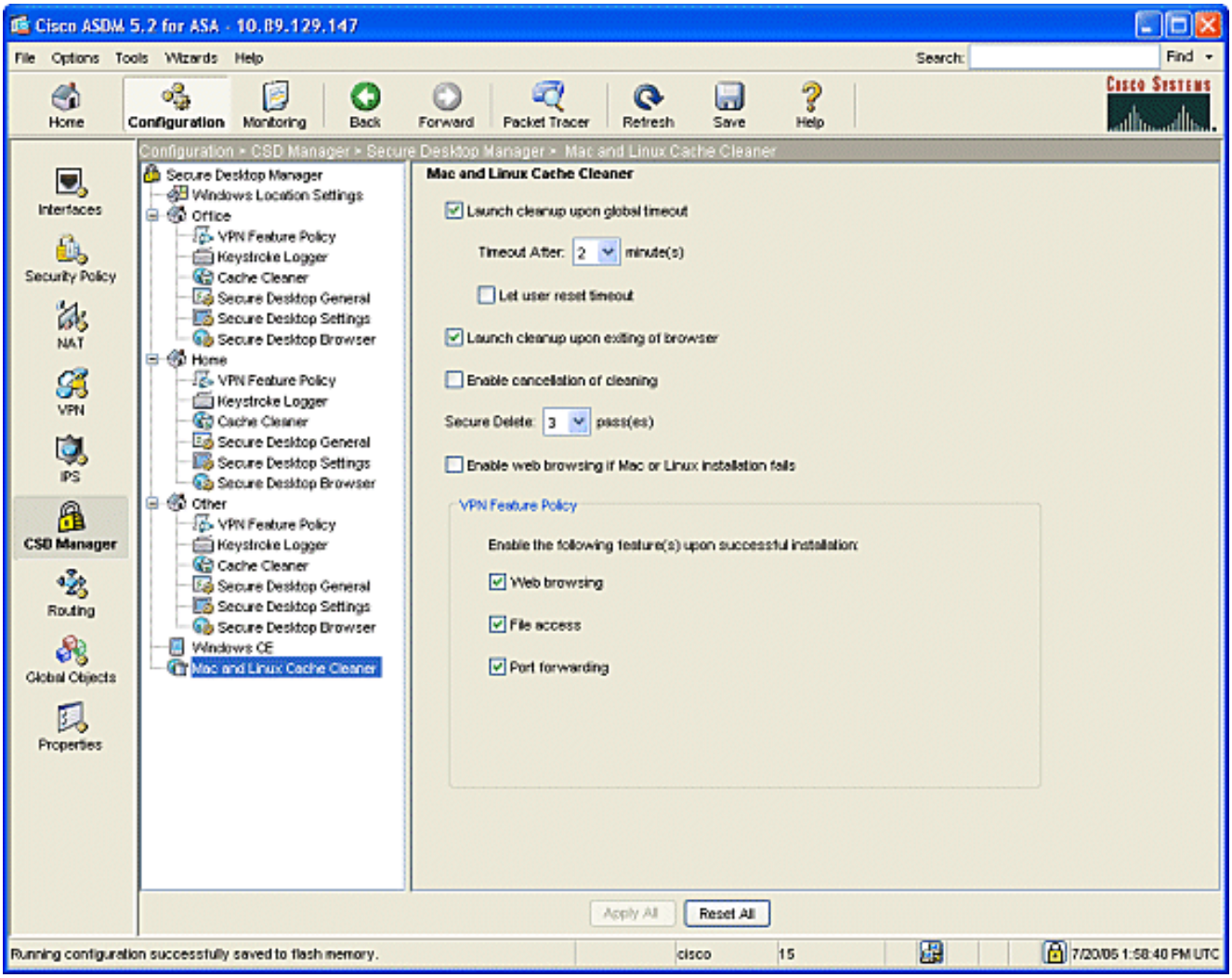
Windows CE、Macintosh 和 Linux 客户端的可选配置

这些配置是可选的。

1. 如果在导航窗格选择了 **Windows CE**，请选中“Web browsing”复选框。



2. 如果在导航窗格选择了 **Mac and Linux Cache Cleaner**，请选中“Launch cleanup upon global timeout”单选按钮。根据指定内容更改超时。在 **VPN Feature Policy** 区域下，为这些客户端选中“Web browsing”、“File access”和“Port forwarding”单选按钮。



3. 无论您选择是“ Windows CE”还是“Mac and Linux Cache Cleaner”，请单击 **Apply All**。
4. 单击 **Save**，然后单击 **Yes** 接受更改。

配置

配置

此配置反映了 ASDM 为启用 CSD 而进行的更改：大多数 CSD 配置将在闪存上保留在单独的文件中。

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
```

验证

使用此部分确认无客户端 SSL VPN、瘦客户端 SSL VPN 或 SSL VPN 客户端 (SVC) 的配置是否正常运行。

使用配置有不同 Windows 位置的 PC 测试 CSD。每次测试应根据您在上述示例中配置的策略提供不同的访问。

可更改 Cisco ASA 侦听 WebVPN 连接的端口号和接口。

- 默认端口为 443。如果使用默认端口，则访问地址为 **https://ASA IP 地址**。
- 使用不同端口可将访问地址更改为 **https://ASA IP 地址:newportnumber**。

命令

有若干 **show** 命令与 WebVPN 关联。可以在命令行界面 (CLI) 上执行这些命令以显示统计信息和其他信息。要详细查看 **show** 命令的用法，请参阅验证 WebVPN 配置。

注意： 命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

故障排除

本部分提供的信息可用于对配置进行故障排除。

如果远程客户端发生问题，请检查以下各项：

1. 是否已在 Web 浏览器中启用弹出窗口、Java 和/或 ActiveX？可根据使用的 SSL VPN 连接的类型启用这些设置。
2. 客户端必须接受在会话开始时提供的数字证书。

命令

有若干 **debug** 命令与 WebVPN 关联。有关这些命令的详细信息，请参阅使用 WebVPN Debug 命令。

注意： 使用 **debug** 命令可能会对 Cisco 设备造成负面影响。使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

相关信息

- Cisco ASA 5500 系列自适应安全设备
- 使用 ASDM 和 NTLMv1 配置具有 WebVPN 和单点登录的 ASA 示例
- 技术支持和文档 - Cisco Systems