Cisco Secure Desktop (CSD 3.1.x) em ASA 7.2.x para o exemplo de configuração de Windows usando o ASDM

Índice

Introdução

O Cisco Secure Desktop (CSD) estende a segurança da tecnologia de VPN SSL. O CSD fornece uma partição separada na estação de trabalho de um usuário para a atividade de sessão. Esta área de quarentena é criptografada durante as sessões e removida completamente quando a sessão de VPN SSL termina. O Windows pode ser configurado com todos os benefícios da segurança do CSD. Macintosh, Linux, e Windows CE têm acesso somente aos recursos de limpeza de cache, navegação na web e acesso a arquivos. O CSD pode ser configurado para dispositivos Windows, Macintosh, Windows CE e Linux nestas plataformas:

- 5500 Series adaptável da ferramenta de segurança de Cisco (ASA)
- Roteadores Cisco que executam as liberações 12.4(6)T do Cisco IOS ® Software e mais tarde

- Versão 4.7 e mais recente do Concentradores Cisco VPN série 3000
- Módulo de Cisco WebVPN no Roteadores do Catalyst 6500 e 7600 Series

Nota: A liberação 3.3 CSD deixa-o agora configurar o Cisco Secure Desktop para ser executado nos computadores remotos que executam a vista de Microsoft Windows. Previamente, o Cisco Secure Desktop foi limitado aos computadores que executaram Windows XP ou 2000. Refira o realce dos novos recursos - Secure Desktop na seção da vista dos Release Note para o Cisco Secure Desktop, liberação 3.3, para mais informação.

Este exemplo cobre primeiramente a instalação e a configuração do CSD no 5500 Series ASA para clientes do Windows. As configurações opcionais para Windows CE, o Mac, e os clientes Linux são adicionadas para a conclusão.

O CSD é usado conjuntamente com a tecnologia de VPN SSL (sem clientes SSL VPN, thin client SSL VPN, ou cliente VPN SSL (SVC)). O CSD adiciona o valor às sessões seguras da tecnologia de VPN SSL.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

Exigências para o dispositivo do theASA

- Liberação 3.1 de Cisco CSD ou mais atrasado
- Versão de software 7.1.1 de Cisco ASA ou mais atrasado
- Liberação 5.1.1 do Cisco Adaptive Security Device Manager (ASDM) ou mais atrasado**Nota:** Apoios da versão 3.2 CSD na versão ASA 8.x somente**Nota:** Consulte Habilitação de Acesso HTTPS para o ASDM para permitir que o ASA seja configurado pelo ASDM.

Exigências para computadores de cliente

- Os clientes remotos devem ter privilégios administrativos locais; não se exige, mas sugere-se altamente.
- Os clientes remotos devem ter a versão 1.4 ou mais recente do ambiente de tempo de execução de java (JRE).
- Navegadores de cliente remoto: Internet explorer 6.0, Netscape 7.1, Mozilla 1.7, safari 1.2.2, ou Firefox 1.0
- Cookie permitidos e pop-up permitidos em clientes remotos

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados neste documento começaram com uma

configuração limpa (padrão). Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando. Os endereços IP de Um ou Mais Servidores Cisco ICM NT usados nesta configuração são endereços do RFC 1918. Estes endereços IP de Um ou Mais Servidores Cisco ICM NT não são legais no Internet e devem ser usada somente em um ambiente de laboratório do teste.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

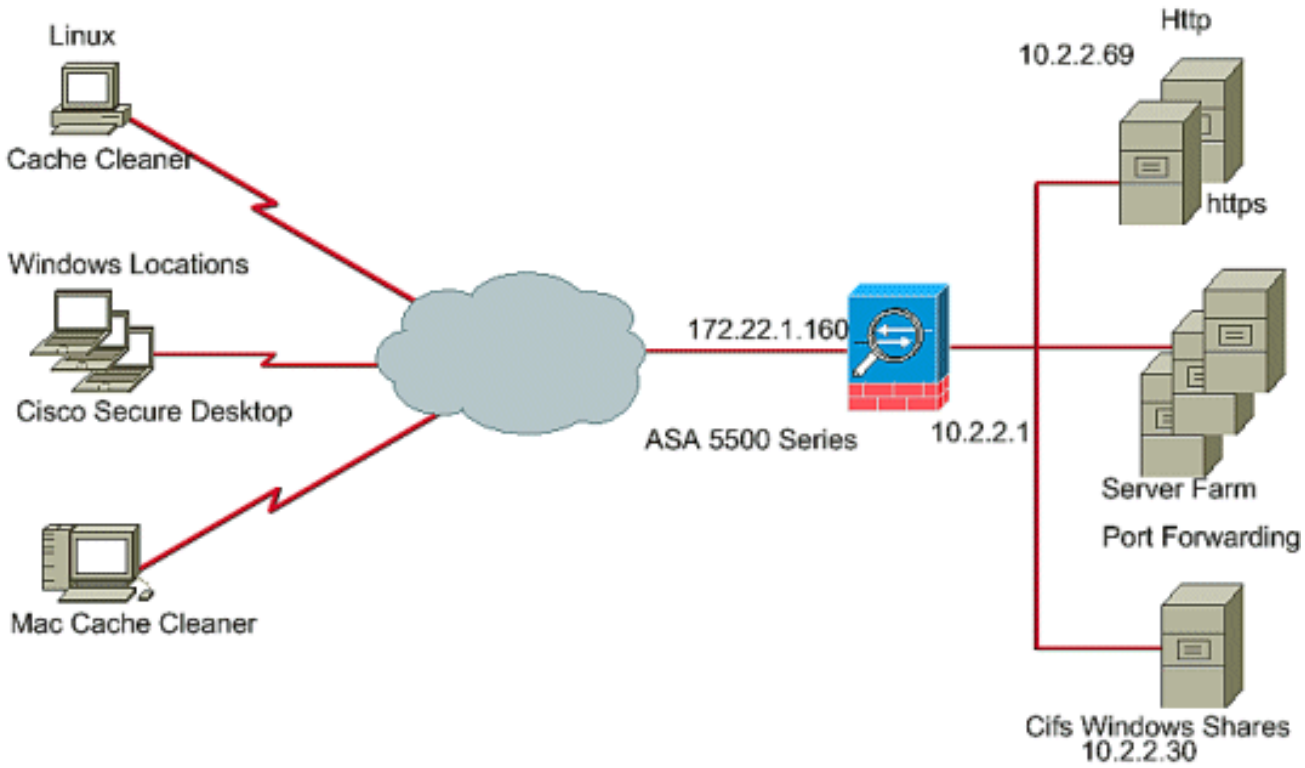
Informações de Apoio

O CSD opera-se com tecnologia de VPN SSL, assim que os sem clientes, o thin client, ou o SVC devem ser ativados antes da configuração do CSD.

Diagrama de Rede

Os lugar diferentes de Windows podem ser configurados com os aspectos da segurança total do CSD. Macintosh, Linux, e Windows CE têm o acesso somente ao líquido de limpeza do esconderijo e/ou a navegação na web e o acesso de arquivo.

Este documento utiliza a seguinte configuração de rede:



Configurar o CSD no ASA para clientes do Windows

Configurar o CSD no ASA para clientes do Windows com cinco etapas principal:

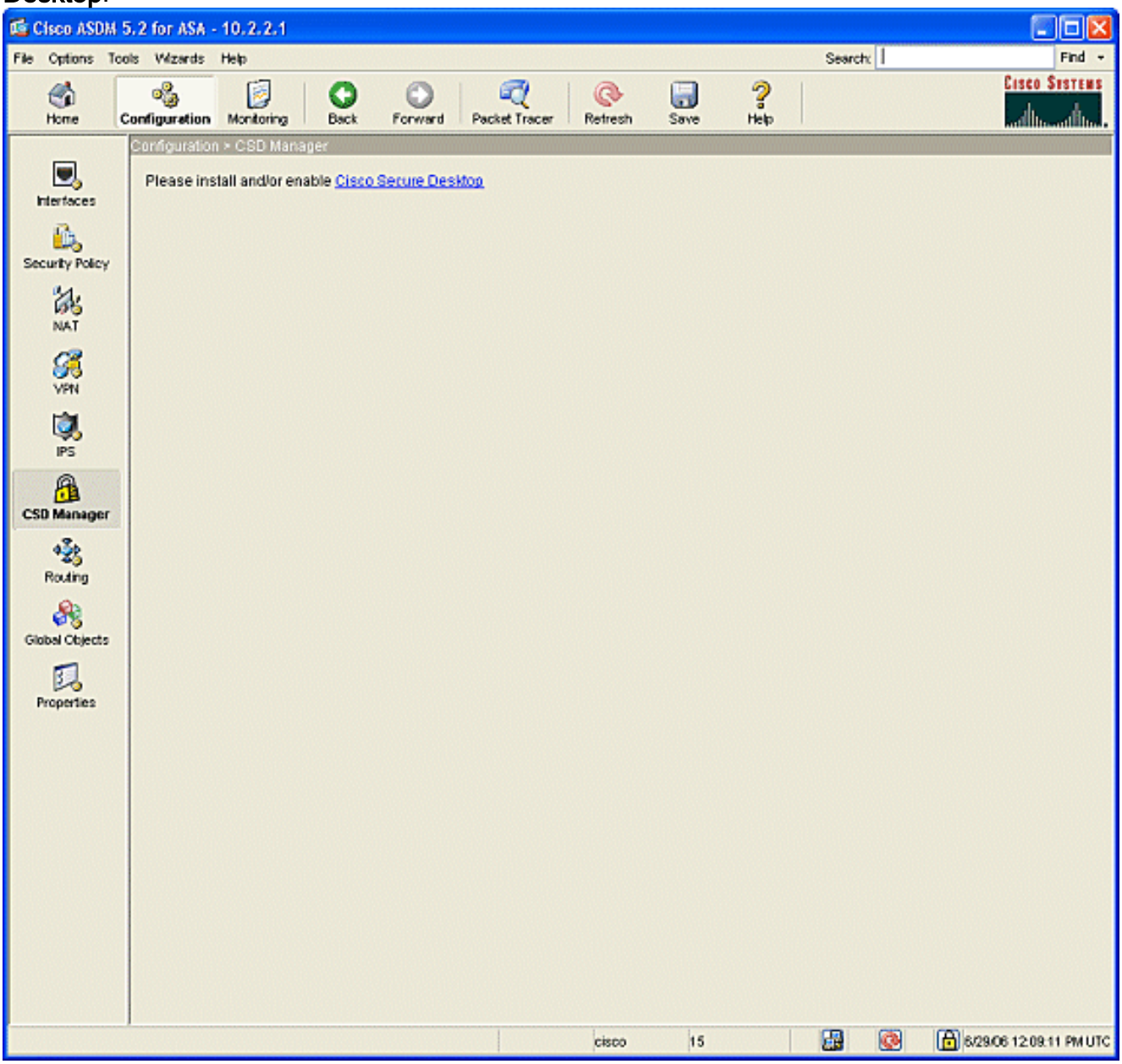
- Obtenha, instale, e permita o software CSD em Cisco ASA.

- Defina lugar de Windows.
- Defina a identificação de local de Windows.
- Configurar os módulos do lugar de Windows.
- Configurar características do lugar de Windows.
- Configuração opcional para Windows CE, Macintosh, e clientes Linux.

Obtenha, instale, e permita o software CSD

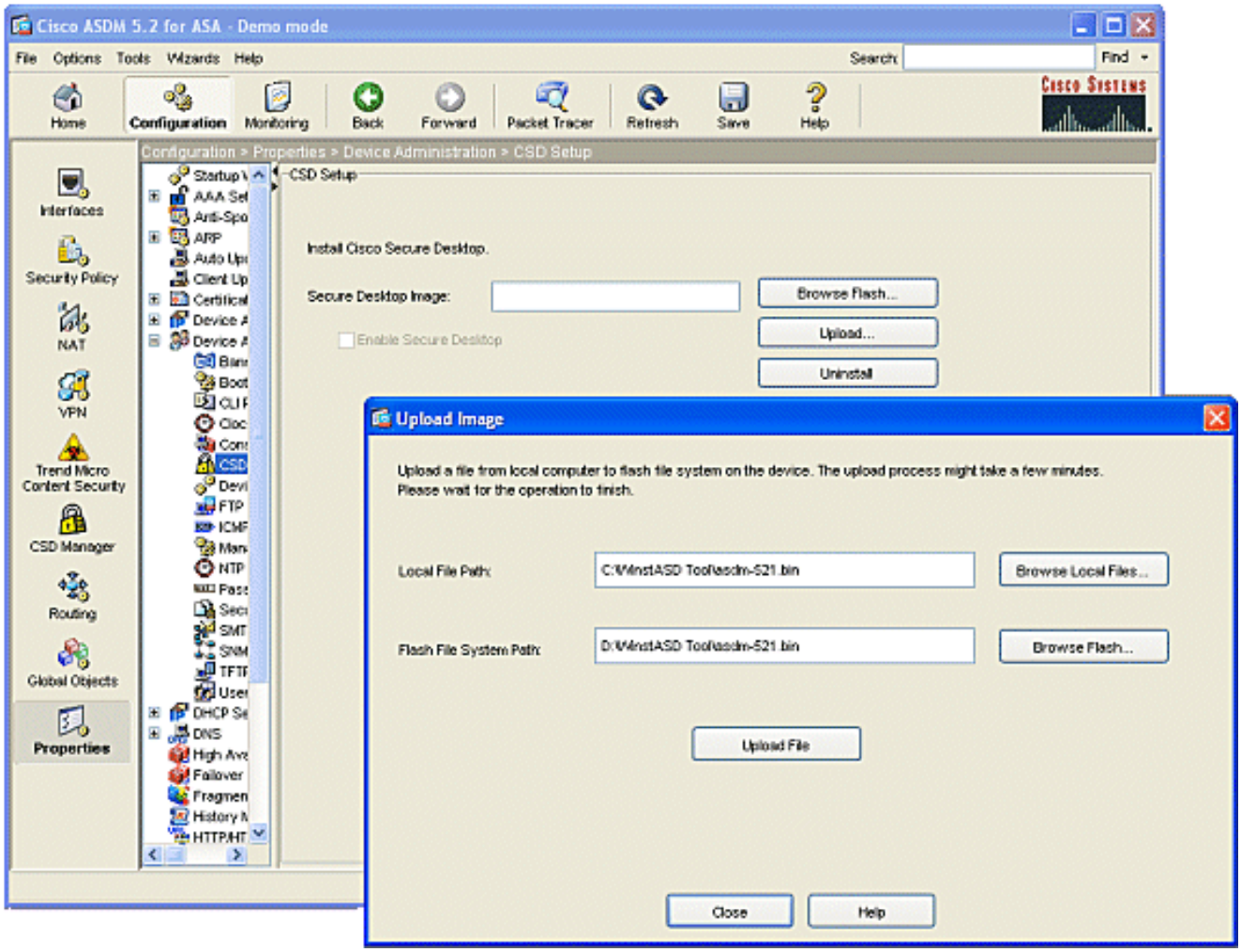
Termine estas etapas para obter, instalar, e permitir o software CSD em Cisco ASA.

1. Transfira o software securedesktop-asa*.package CSD e arquivos de leia-me em sua estação de gerenciamento do Web site da transferência de software Cisco.
2. Entre ao ASDM e clique o botão da **configuração**. Do menu esquerdo, clique o botão do **gerente CSD**, e clique o link do **Cisco Secure Desktop**.



3. Clique a **transferência de arquivo pela rede** para indicar o indicador da imagem da transferência de arquivo pela rede.Ou entre no trajeto do arquivo novo .package na estação de gerenciamento ou o clique **consulta arquivos locais** para encontrar o arquivo.Qualquer

um entra no lugar no flash em que para colocar o arquivo ou o clique **consulte o flash**.Clique o **arquivo da transferência de arquivo pela rede**.Quando alertado, clique a **APROVAÇÃO > próximo >**
APROVADO.

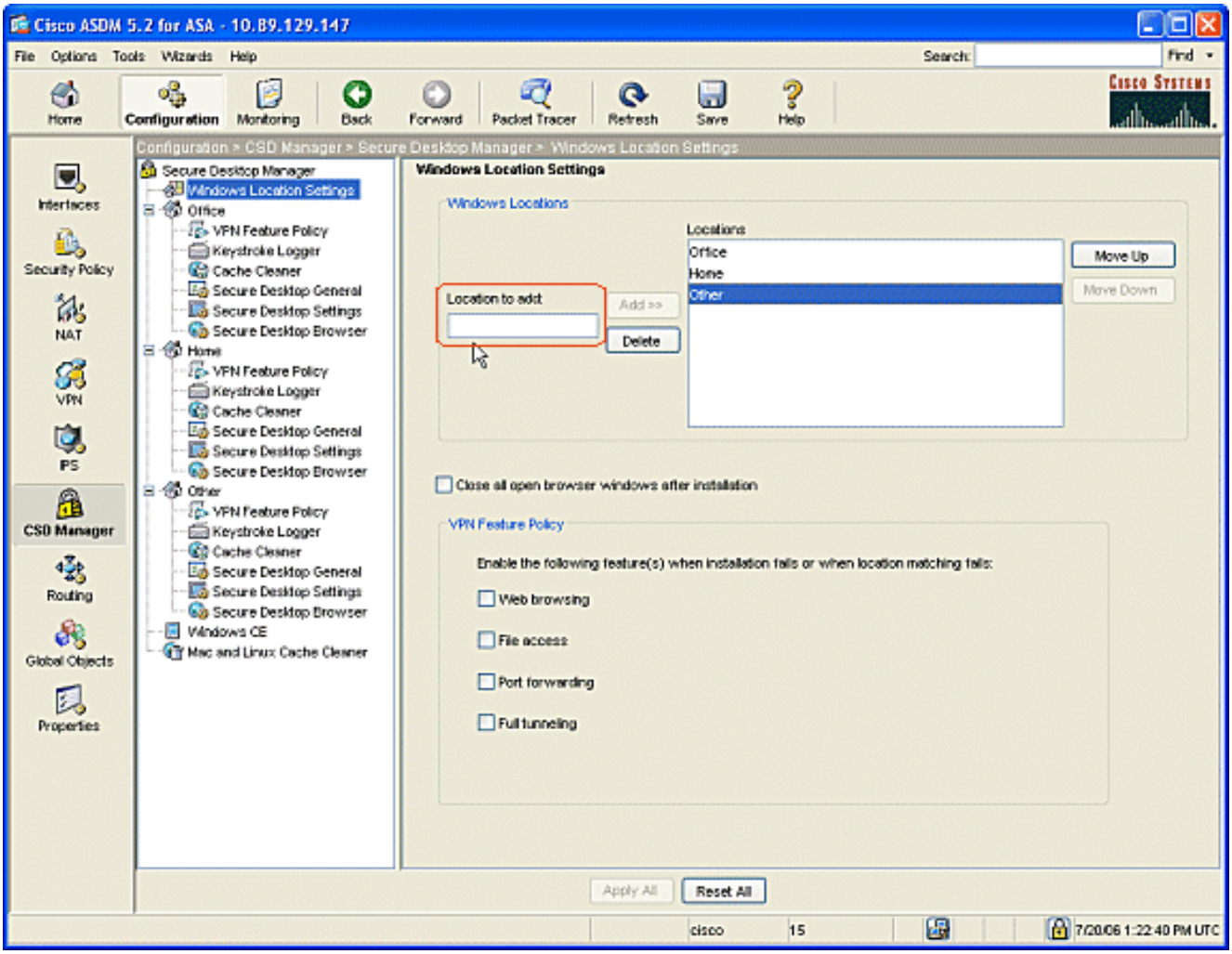


4. Uma vez que a imagem do cliente é carregada para piscar, verifique a caixa de verificação do **cliente VPN da possibilidade SSL**, e clique-a então **aplicam-se**.
5. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.

Defina lugar de Windows

Termine estas etapas para definir lugar de Windows.

1. Clique o botão da **configuração**.
2. Do menu esquerdo, clique o botão do **gerente CSD**, e clique o link do **Cisco Secure Desktop**.
3. Do painel de navegação, clique **configurações de local de Windows**.
4. Datilografe um nome do lugar no lugar para adicionar o campo e o clique **adiciona**.Note os três lugar neste exemplo: Escritório, HOME, e outro.O escritório representa as estações de trabalho que são situadas dentro do limite da Segurança do corporaçõ.A HOME representa os usuários que trabalham da HOME.Outro representa todo o lugar a não ser os dois lugar mencionados.

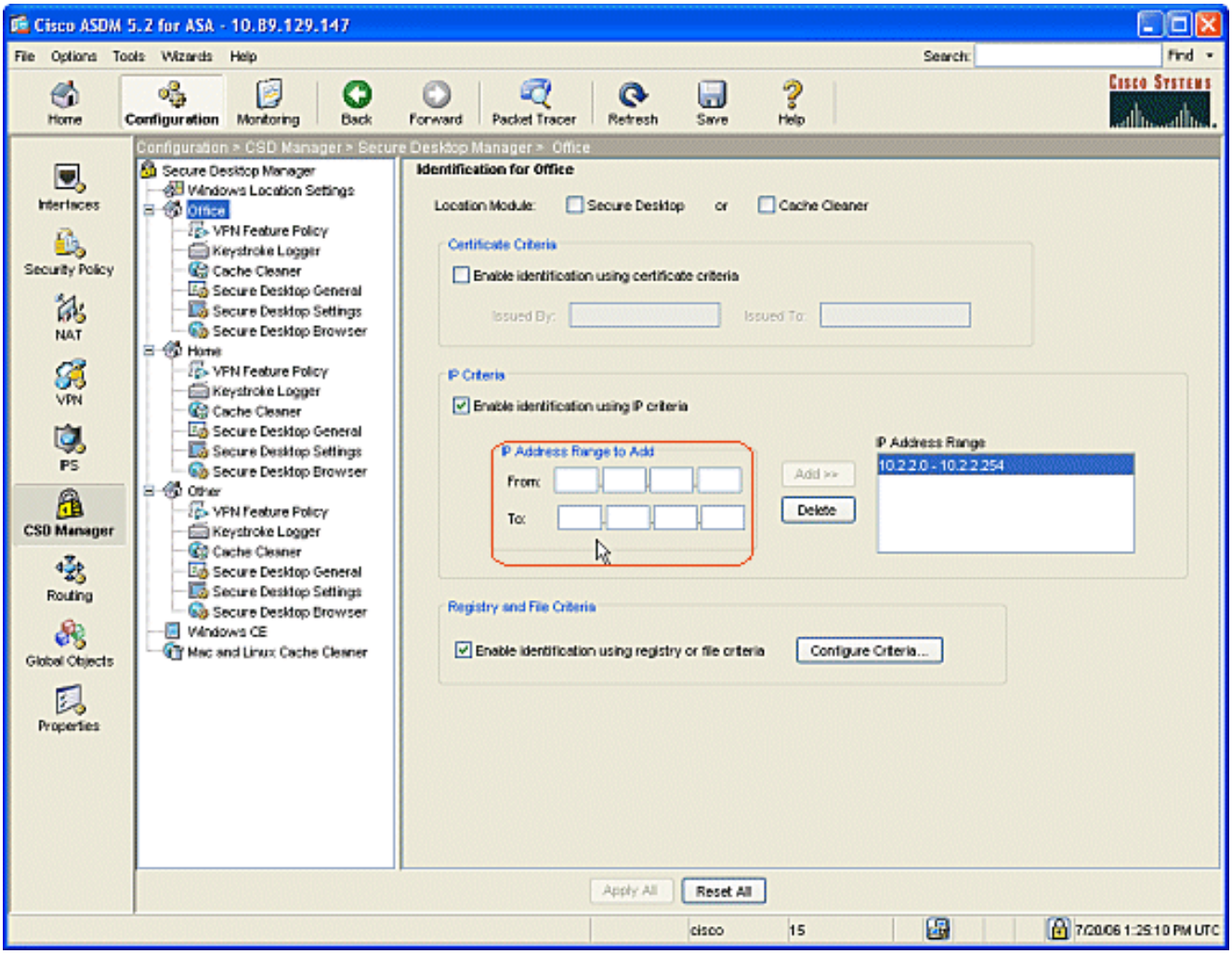


5. Crie seus próprios lugar dependentes da disposição de sua arquitetura de rede para vendas, convidados, Parceiros, e outro.
6. Porque você cria lugar de Windows, o painel de navegação expande com os módulos configuráveis para cada lugar novo. O clique **aplica tudo**.
7. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.

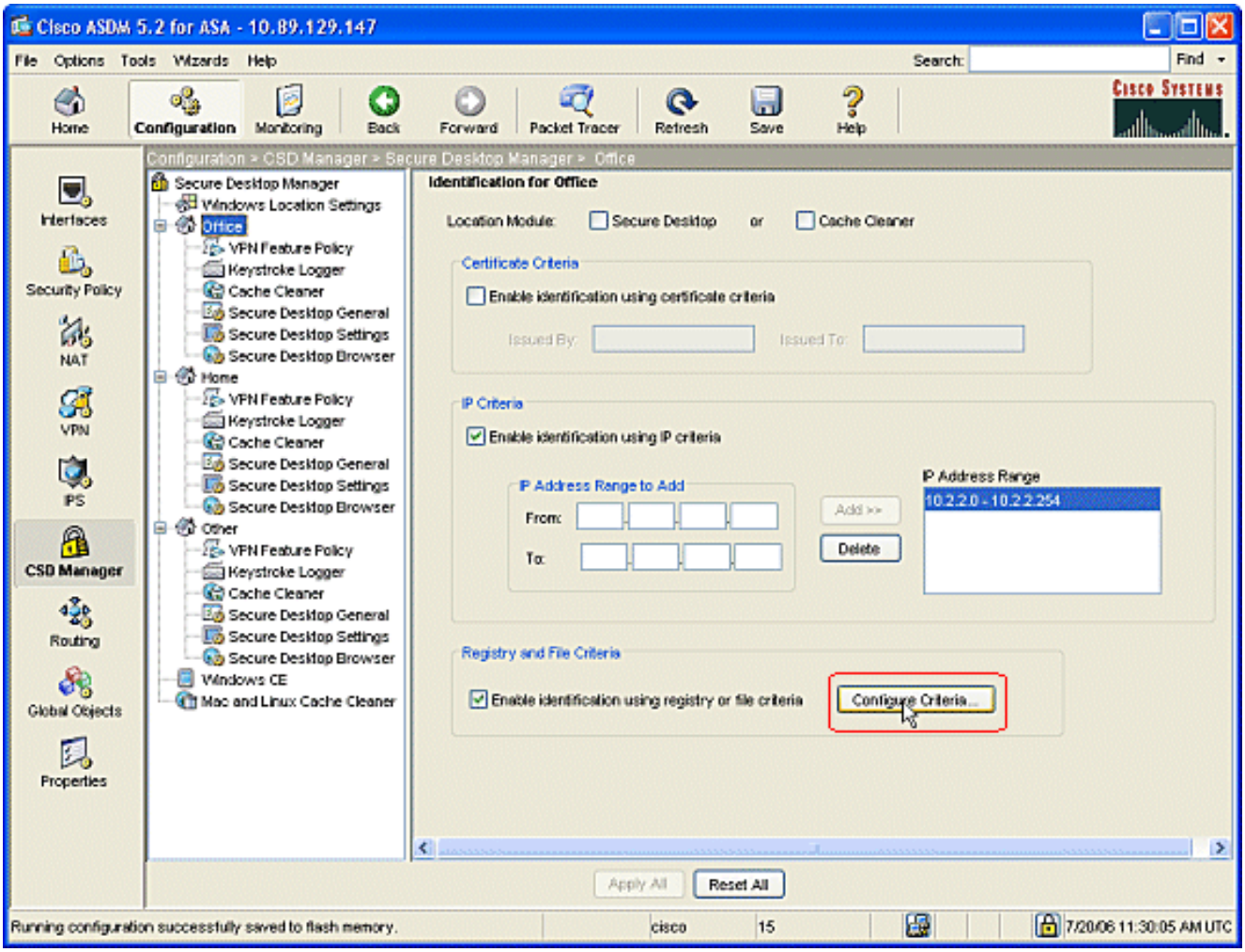
Identificação de local de Windows

Termine estas etapas para definir a identificação de local de Windows.

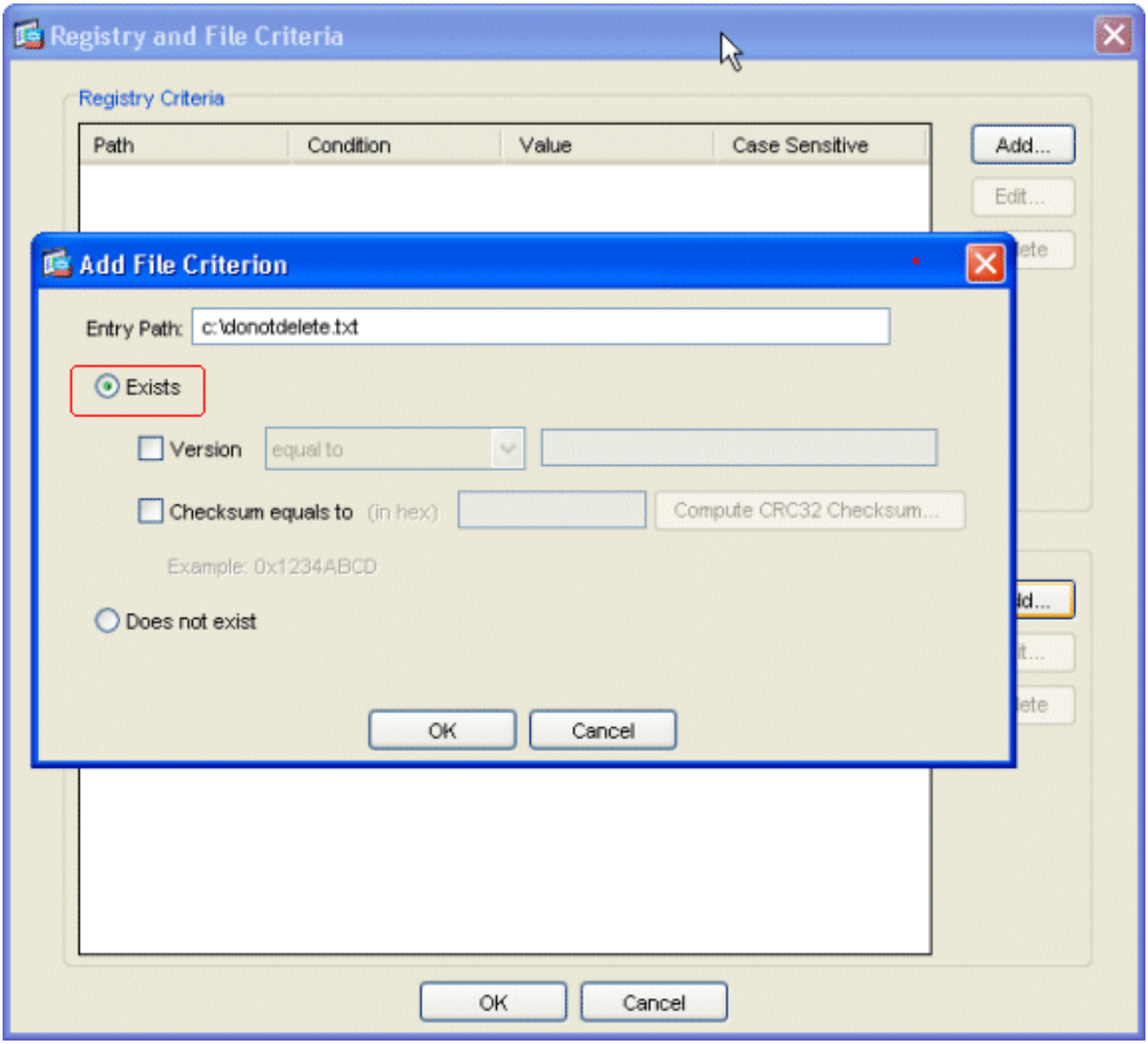
1. Identifique os lugar que foram criados dentro definem lugar de Windows.



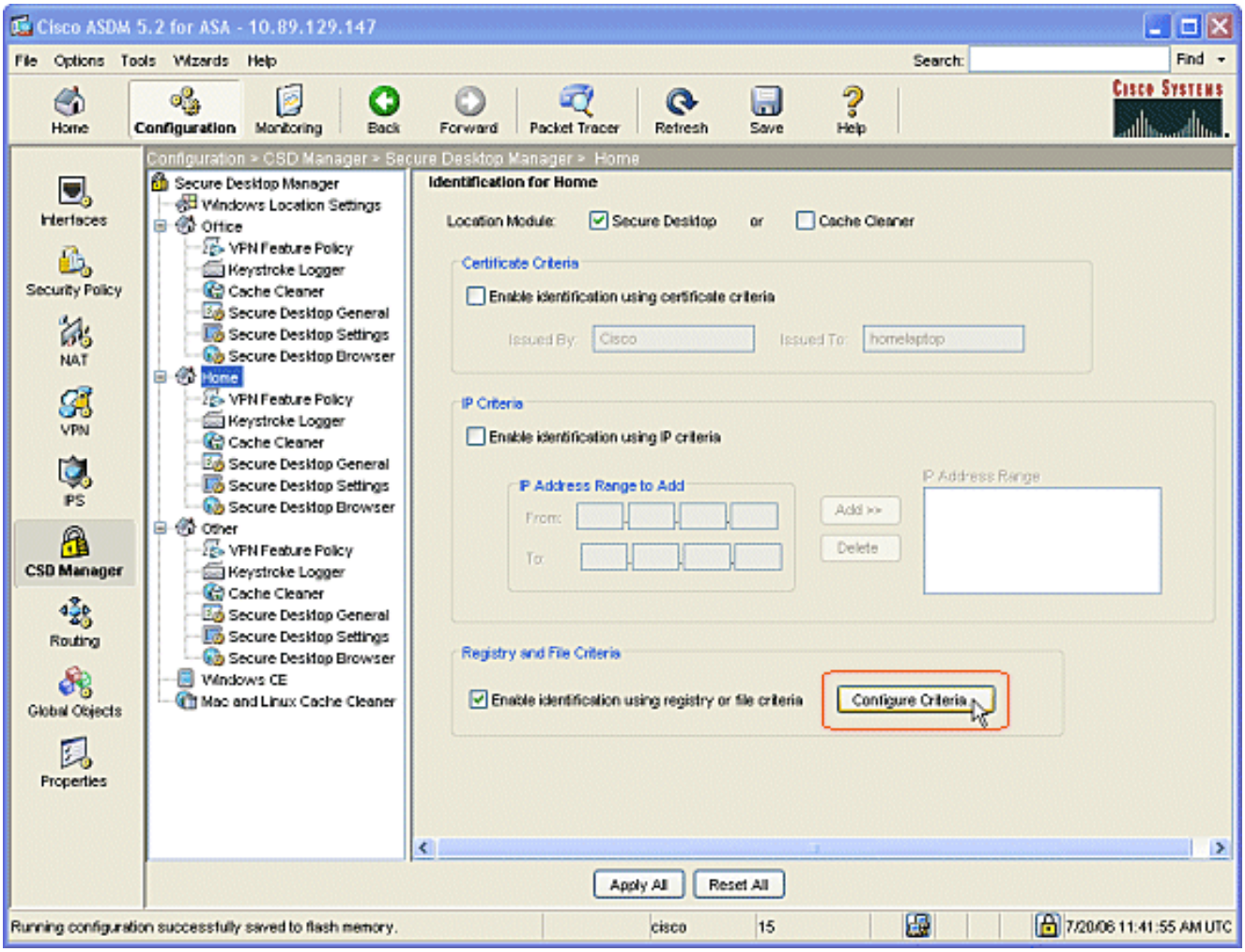
2. Para identificar o escritório do lugar, clique o **escritório no** painel de navegação.Desmarcar o **líquido de limpeza do Secure Desktop** e do **esconderijo** porque estes são computadores internos.A verificação **permite a identificação usando critérios IP**.Incorpore os intervalos de endereço IP de seus computadores internos.A verificação **permite a identificação usando o registro ou arquiva critérios**. Isto diferencia trabalhadores de escritório internos dos convidados ocasionais na
rede.



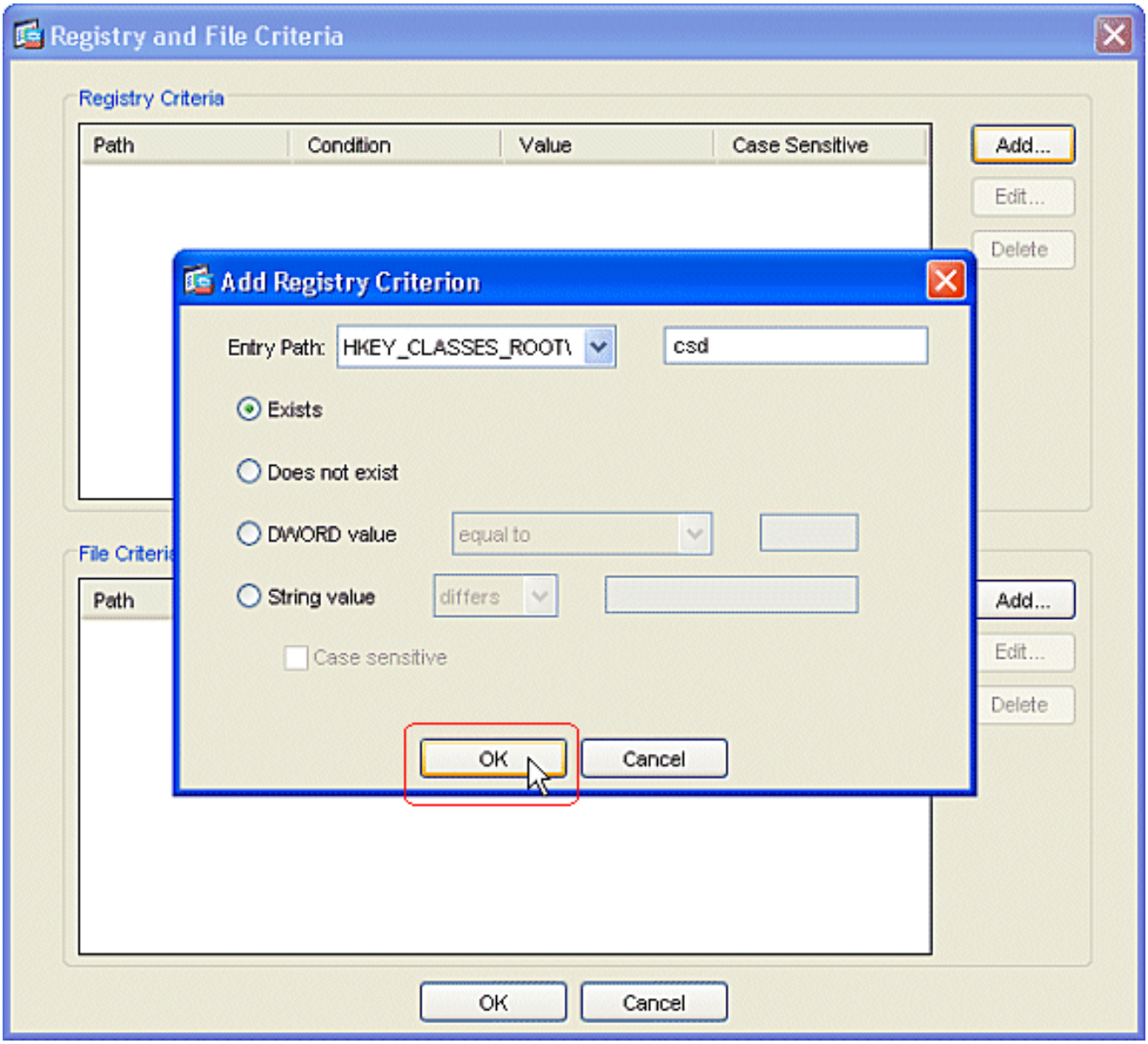
3. O clique **configura critérios**. Um exemplo simples de um arquivo “DoNotDelete.txt” é configurado. Este arquivo deve existir em seus computadores Windows internos e é simplesmente um placeholder. Você pode igualmente configurar uma chave do registro de Windows para identificar computadores de escritório internos. Clique OKIN o indicador do critério do arquivo adicionar. Clique OKIN o registro e arquive critérios do indicador.



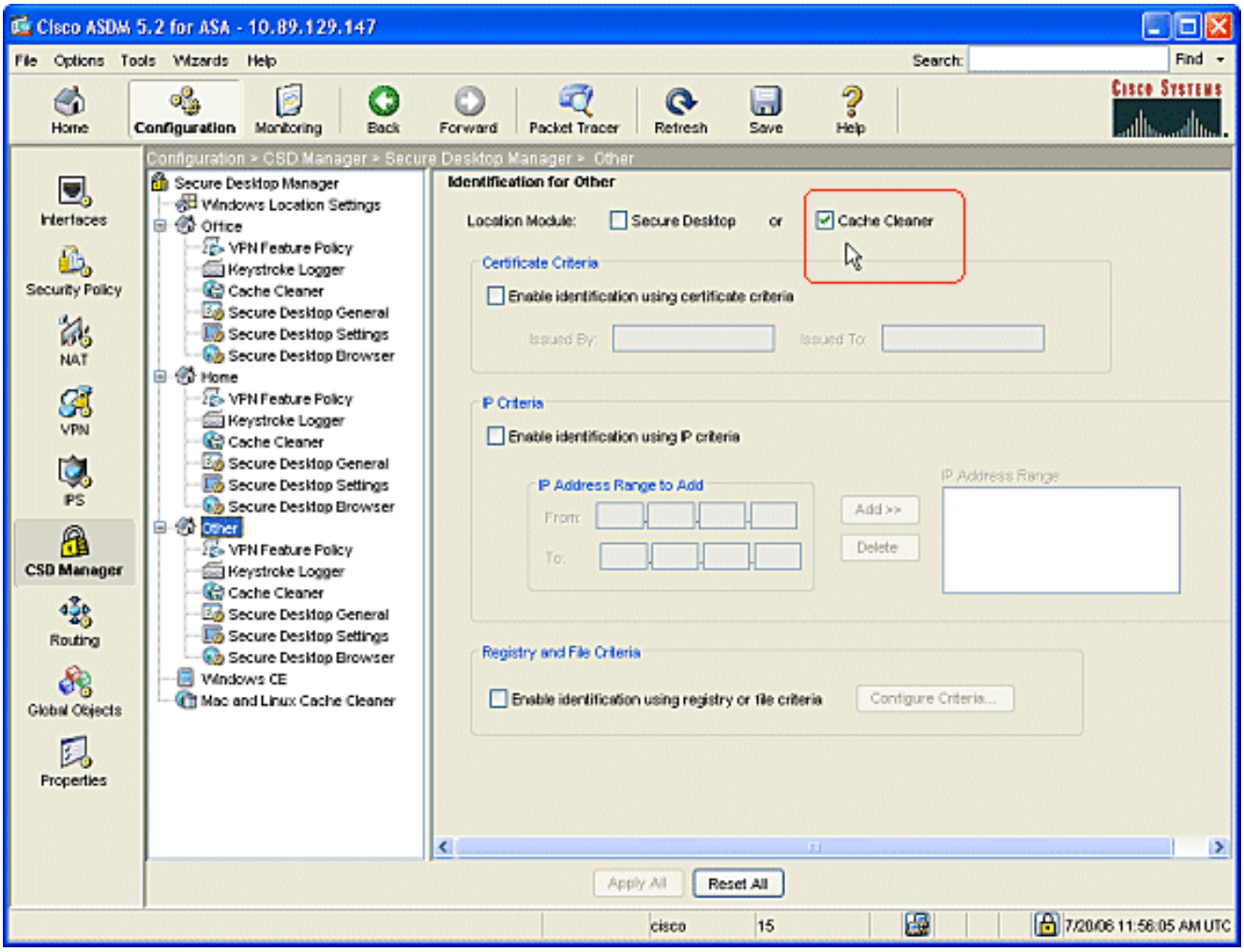
4. O clique **aplica tudo na** identificação para o indicador do escritório. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.
5. Para identificar a HOME do lugar, **HOME do** clique no painel de navegação.A verificação **permite a identificação usando o registro ou arquiva critérios**.O clique **configura critérios**.



6. Os clientes do computador doméstico devem ter sido configurados com esta chave de registro por um administrador. Clique a **APROVAÇÃO no** indicador do critério do registro adicionar. Clique a **APROVAÇÃO no** registro e arquive critérios do indicador.



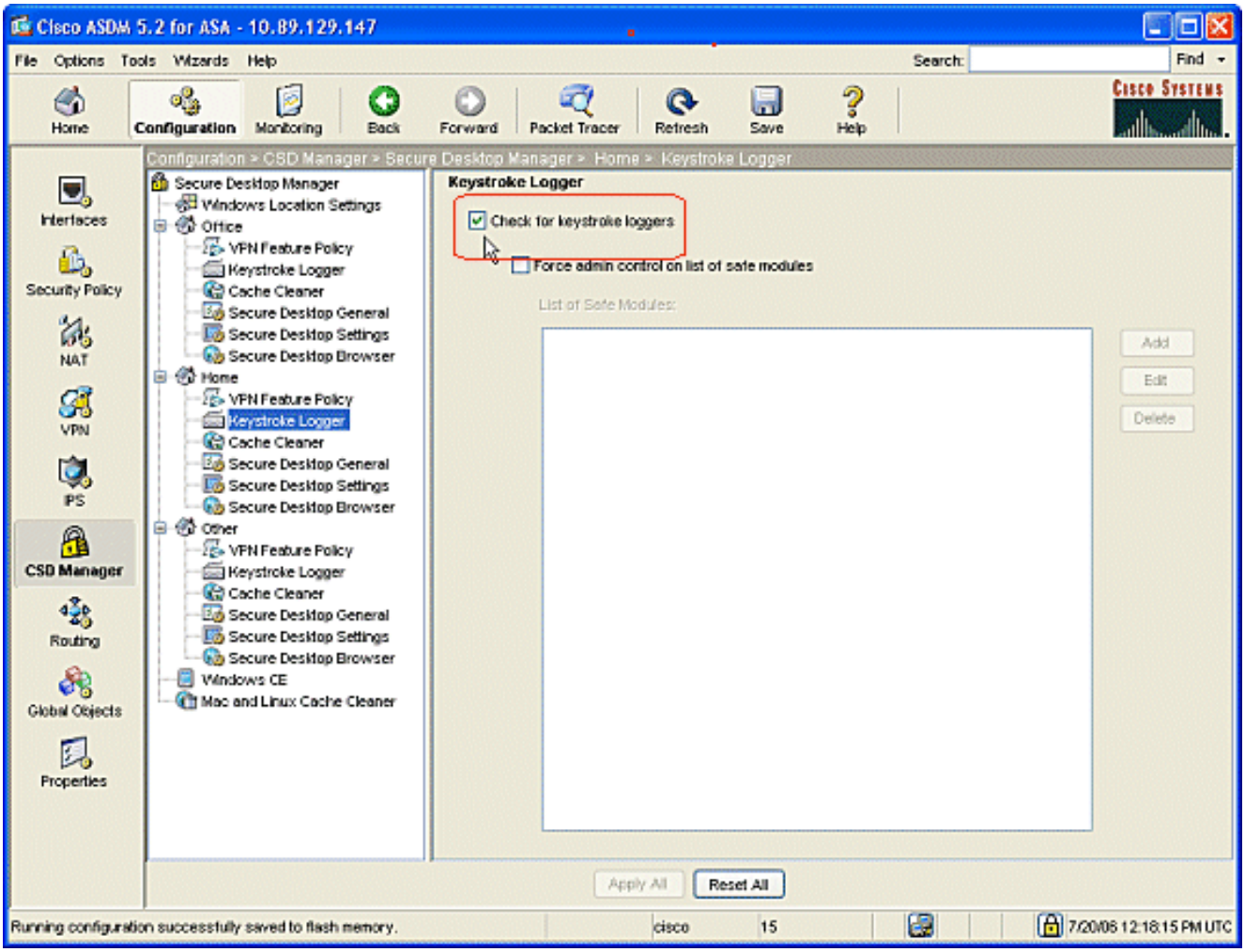
7. Sob o módulo do lugar, verifique o **Secure Desktop**. O clique **aplica tudo na** identificação para o indicador home. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.
8. Para identificar o lugar **outro**, clica **outro no** painel de navegação.Verifique somente a caixa do **líquido de limpeza do esconderijo** e desmarcar todas caixas restantes.O clique **aplica tudo na** identificação para o outro indicador.Clique em **Save** e, em seguida, clique em **Yes** para aceitar as
alterações.



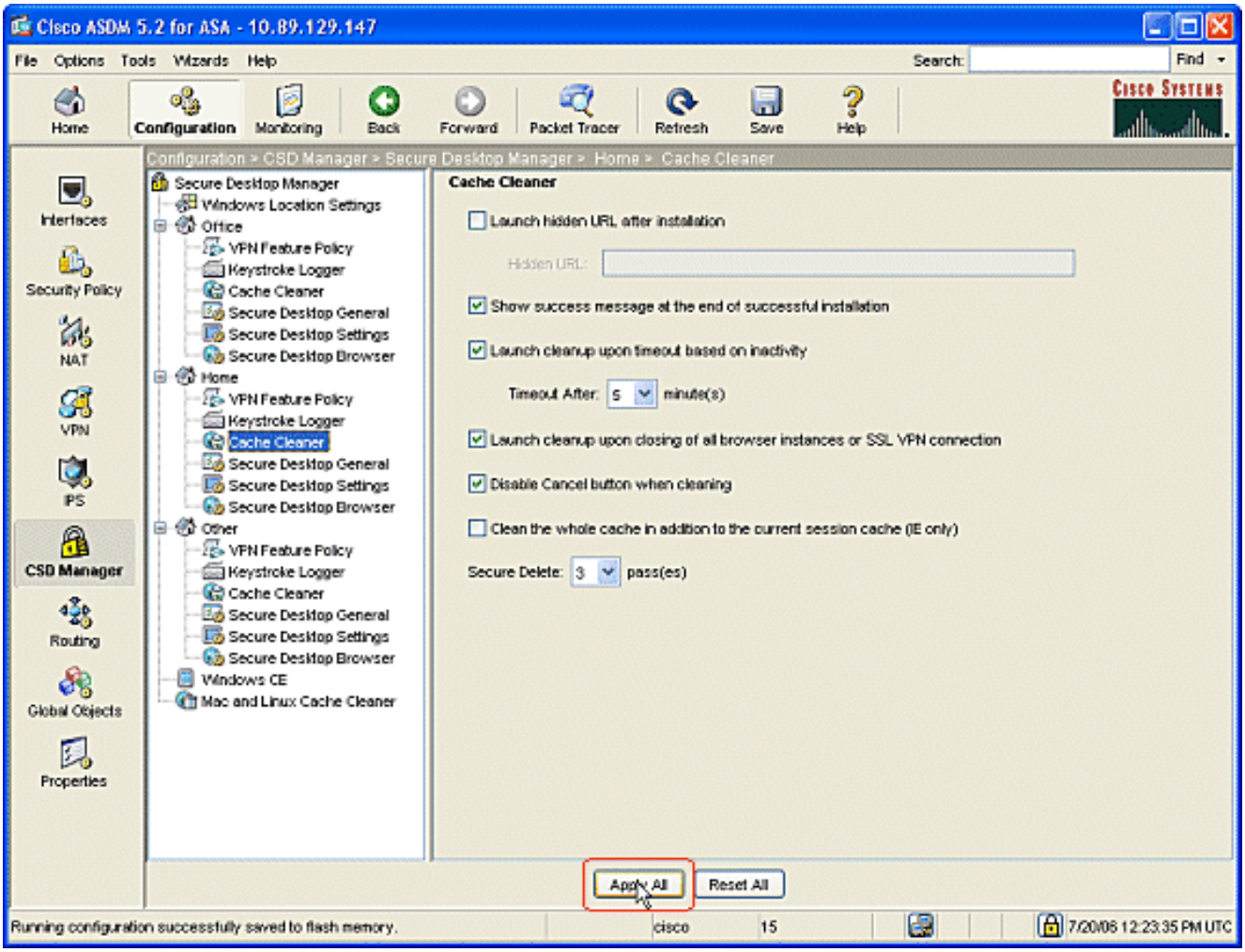
Configurar o módulo do lugar de Windows

Termine estas etapas para configurar os módulos sob cada um dos três lugar que você criou.

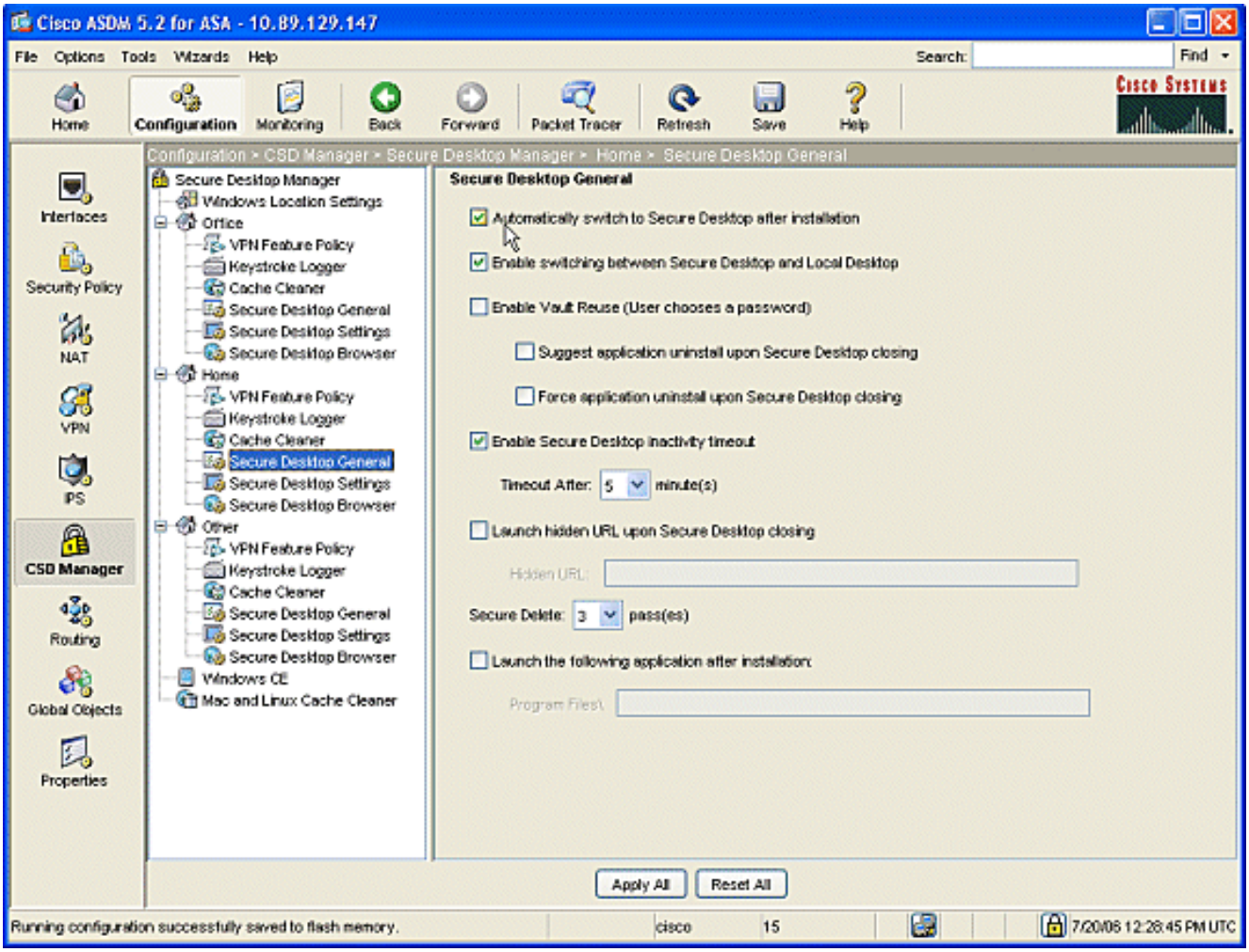
1. Para clientes do escritório, não faça nada desde que o líquido de limpeza do Secure Desktop e do esconderijo não foi escolhido nas etapas precedentes. O aplicativo ASDM permite que você configure o líquido de limpeza do esconderijo mesmo se não foi escolhido em uma etapa precedente. Mantenha as configurações padrão para os locais do escritório.**Nota:** A política da característica VPN não é discutida nesta etapa, mas será discutida em uma etapa subsequente para todos os lugar.
2. Para os clientes home, **HOME do** clique e **registador da introdução por teclado no** painel de navegação.No indicador do registador da introdução por teclado, verifique a **verificação para ver se há registadores de introdução por teclado**.O clique **aplica tudo no** indicador do registador da introdução por teclado.Clique em **Save** e, em seguida, clique em **Yes** para aceitar as
alterações.



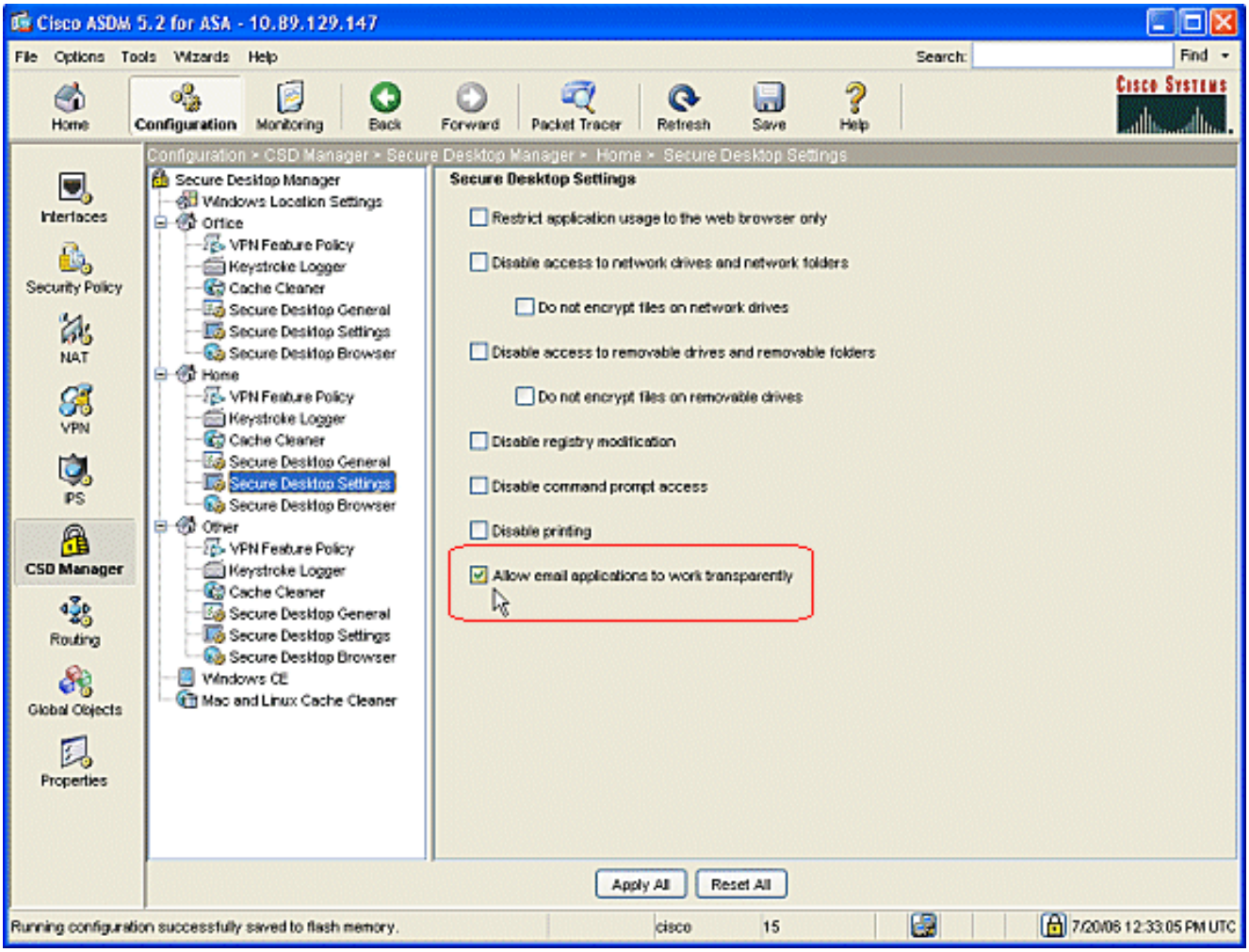
3. Sob a HOME, escolha o **líquido de limpeza do esconderijo** e os parâmetros serir seu ambiente.



4. Sob a HOME, escolha o **Secure Desktop geral** e os parâmetros serir seu ambiente.



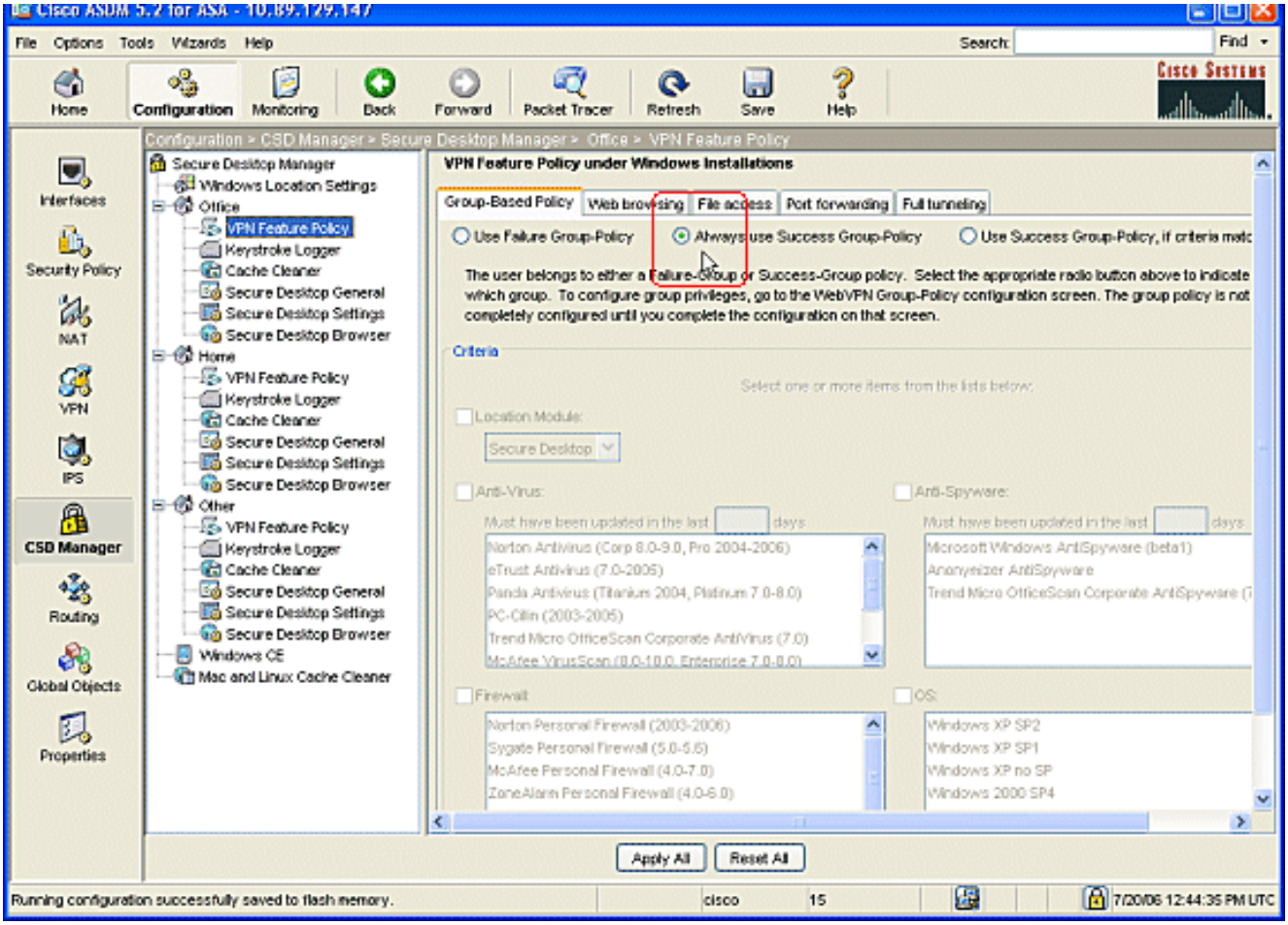
5. Sob a HOME, escolha **ajustes do Secure Desktop**.A verificação **permite aplicativos de e-mail trabalhar transparentemente**, e configura os outros ajustes para serir seu ambiente.O clique **aplica tudo**.Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.



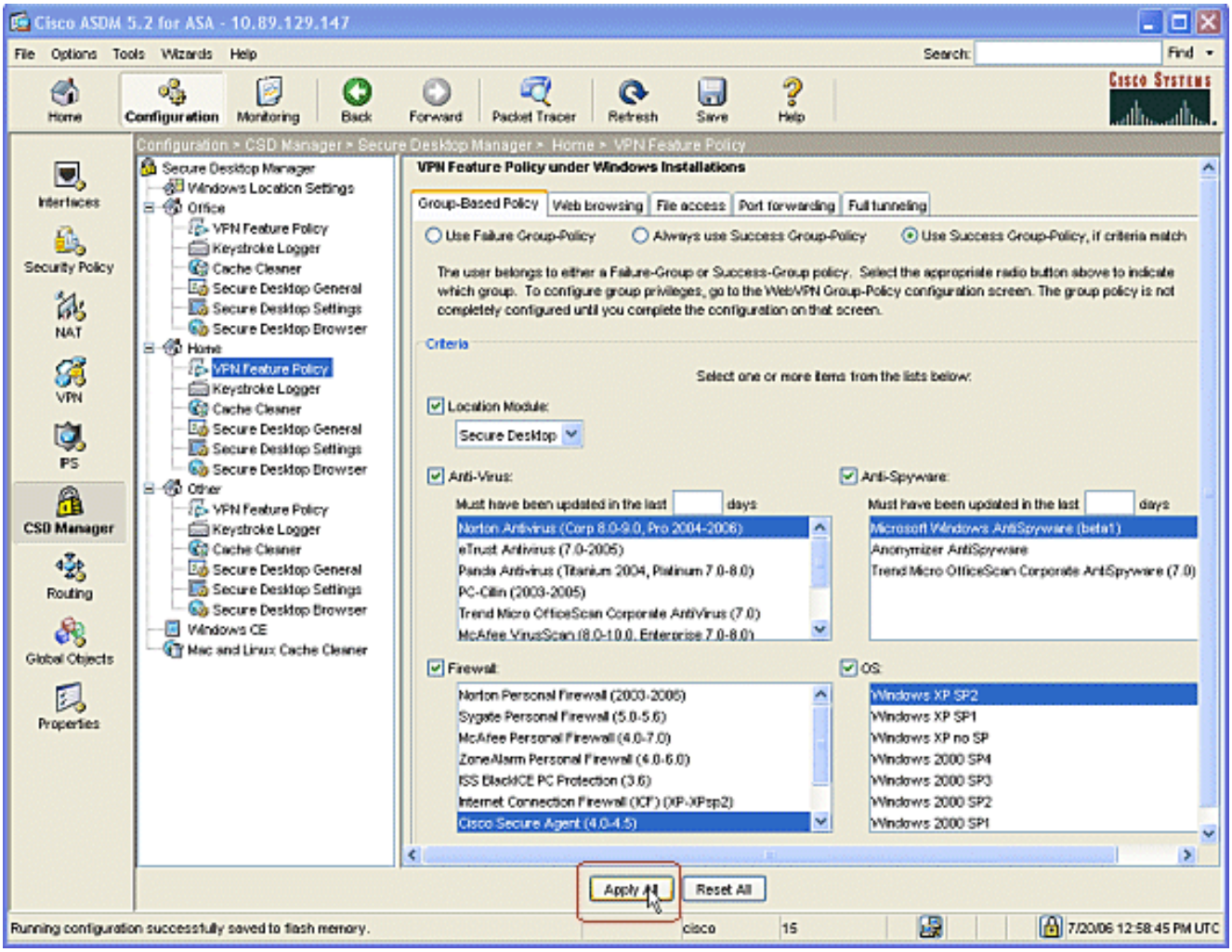
Configurar características do lugar de Windows

Configurar a política da característica VPN para cada um dos lugar que você criou.

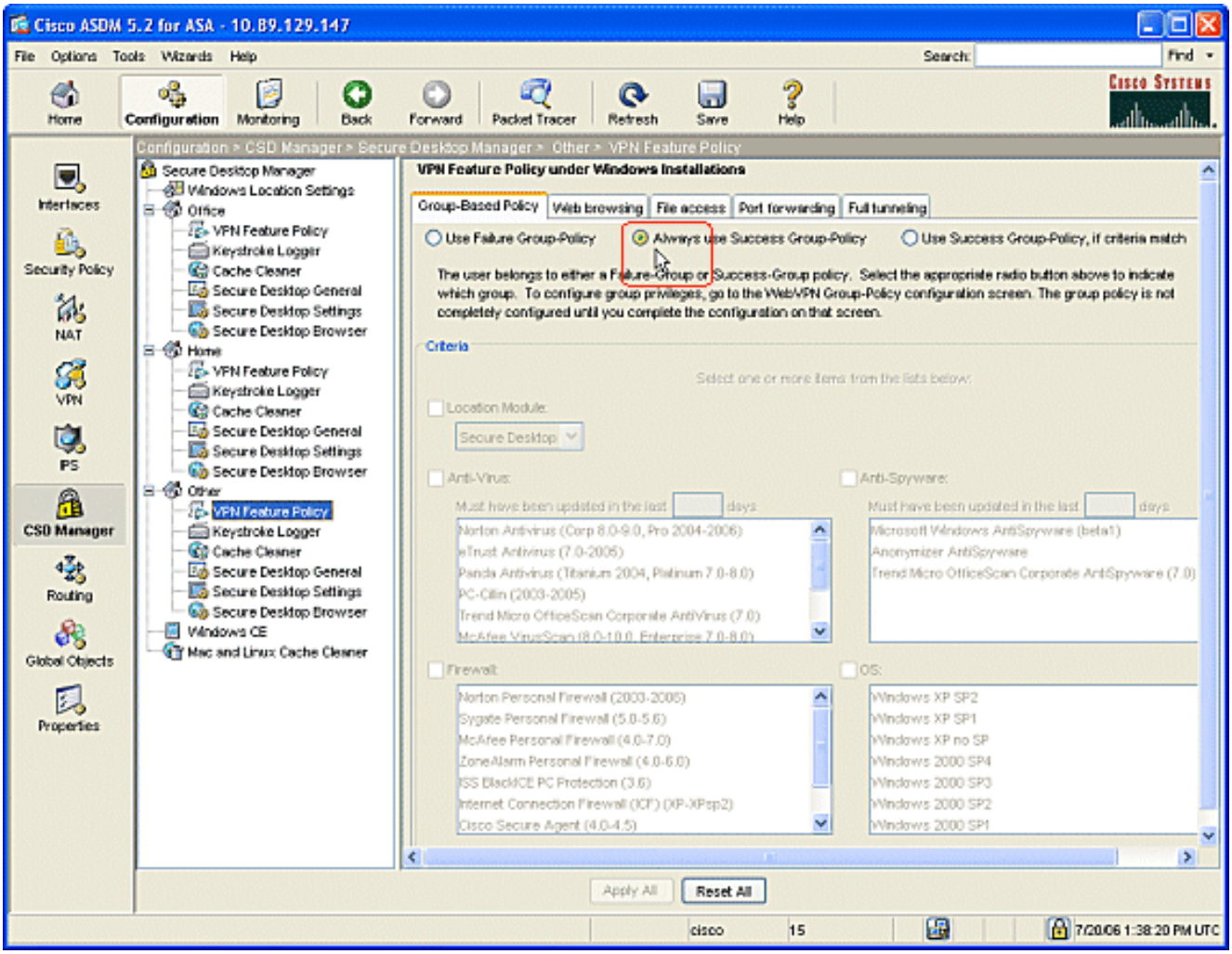
1. No painel de navegação, o clickOffice, e clica então a **política da característica VPN**.
2. Clique a aba Grupo-**baseada da política**.Clique **sempre o** botão de rádio da Grupo-**política do sucesso do uso**.Clique a aba da **navegação na web**, e verifique o botão de rádio **sempre permitido**.Siga o mesmo procedimento para a **transmissão do acesso de arquivo, da porta**, e abas **completas do Tunelamento**.O clique **aplica tudo**.Clique em **Save** e, em seguida, clique em **Yes** para aceitar as
alterações.



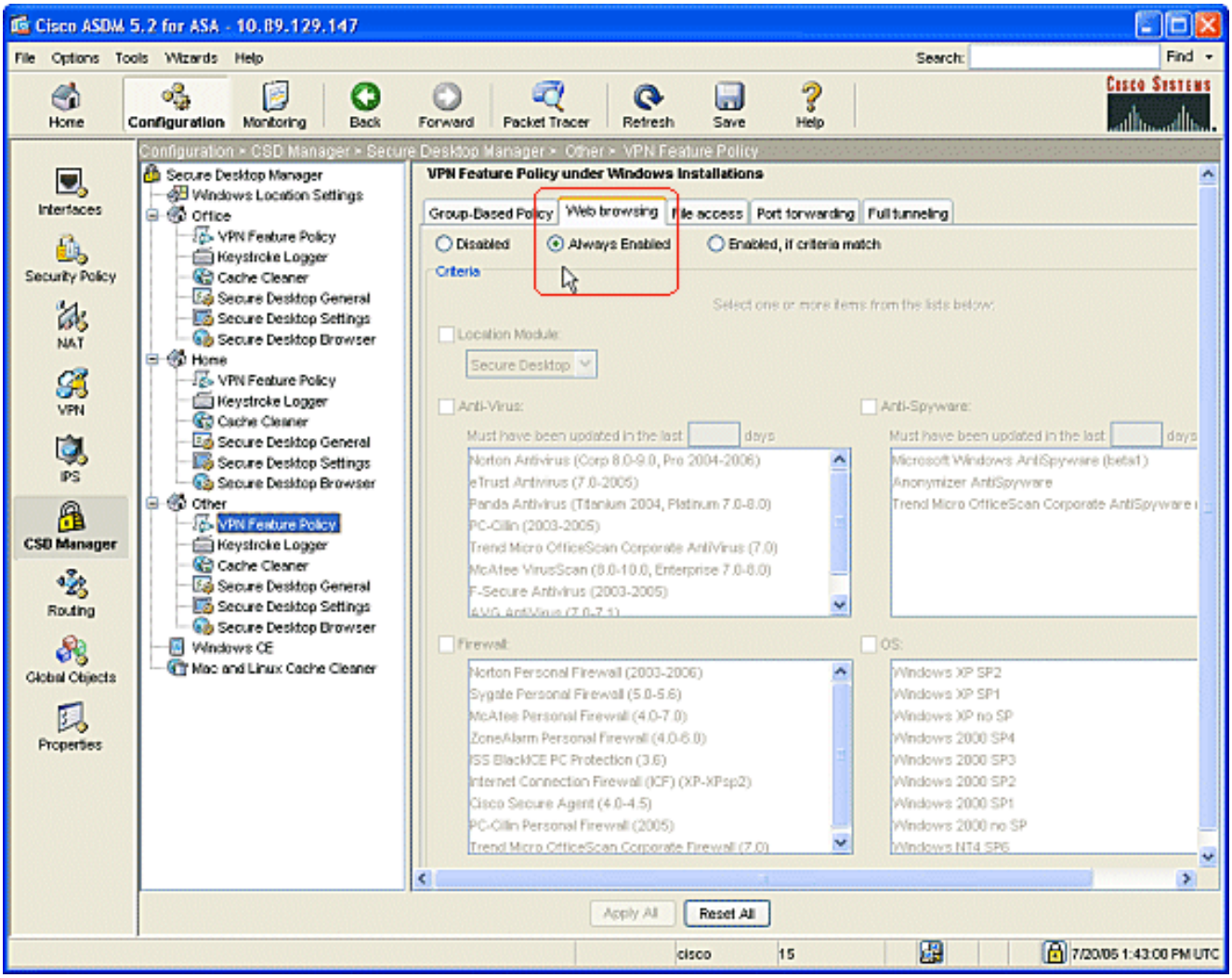
3. Para utilizadores domésticos, cada corporaçõ pode exigir políticas específicas antes que o acesso esteja permitido. No painel de navegação, clique **em casa**, e clique a **política da característica VPN**.Clique a aba Grupo-**baseada da política**.Clique o botão de rádio da Grupo-**política do sucesso do uso** se os critérios preconfigured combinam, como uma chave de registro específica, o nome de arquivo conhecido, ou o certificado digital.Verifique a caixa de seleção do **módulo do** theLocation e escolha o **Secure Desktop**.Escolha o **anti-vírus, o Anti-spyware, o Firewall**, e as áreas do **OS** de acordo com sua política de segurança da empresa. Não estarão permitidos aos utilizadores domésticos na rede a menos que seus computadores encontrarem seus critérios
configurados.



4. No painel de navegação, clique **outro** e clique a **política da característica VPN**.Clique a aba Grupo-**baseada da política**.Clique **sempre o** botão de rádio da Grupo-**política do sucesso do uso**.



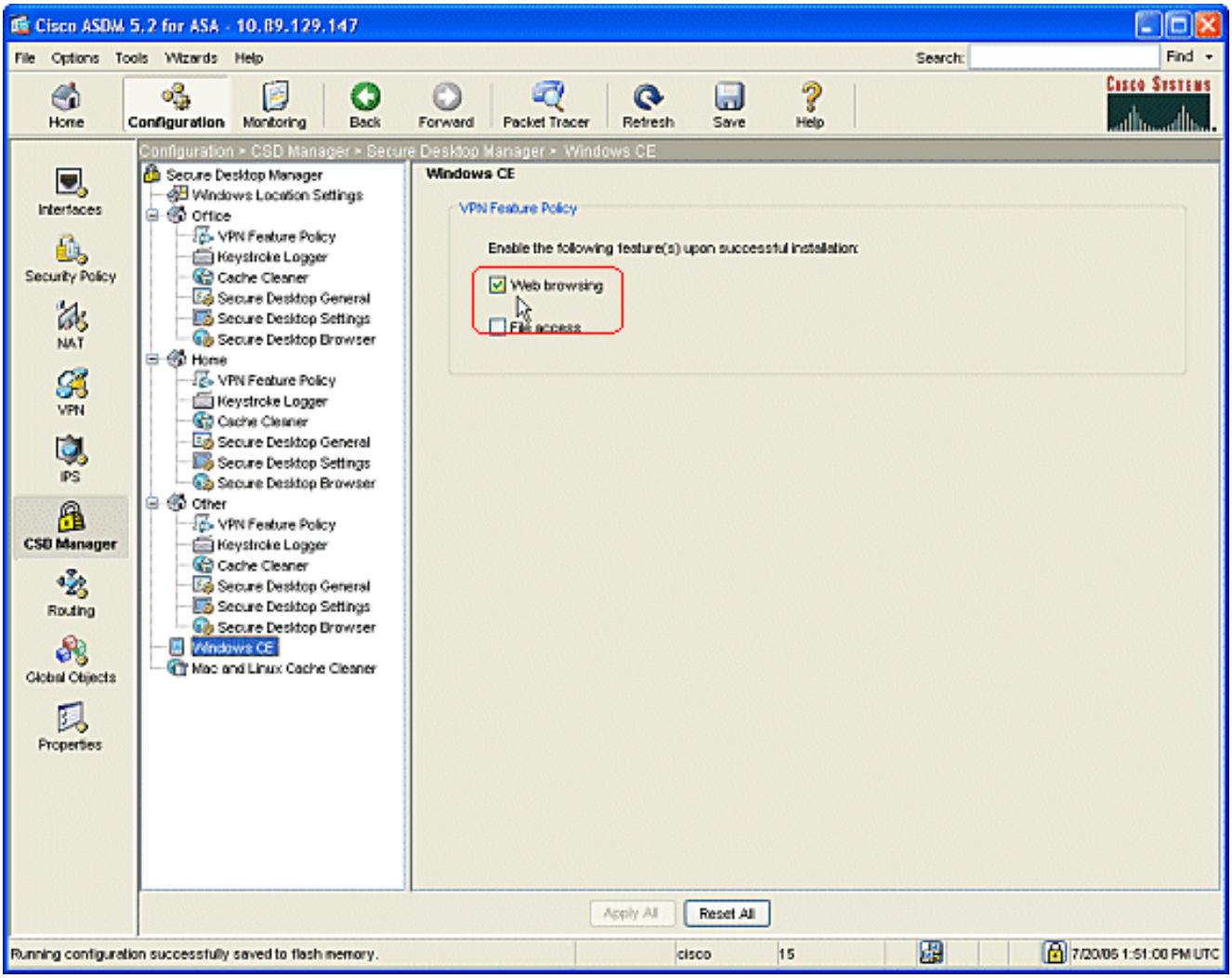
5. Para clientes neste lugar da **política da característica VPN**, clique a aba da **navegação na web**, e clique o seletor de rádio **sempre permitido**.Clique a aba do **acesso de arquivo**, e clique o botão de rádio do **desabilitação**.Repita a etapa com a **transmissão da porta** e as abas **completas do Tunelamento**.O clique **aplica tudo**.Clique em **Save** e, em seguida, clique em **Yes** para aceitar as
alterações.



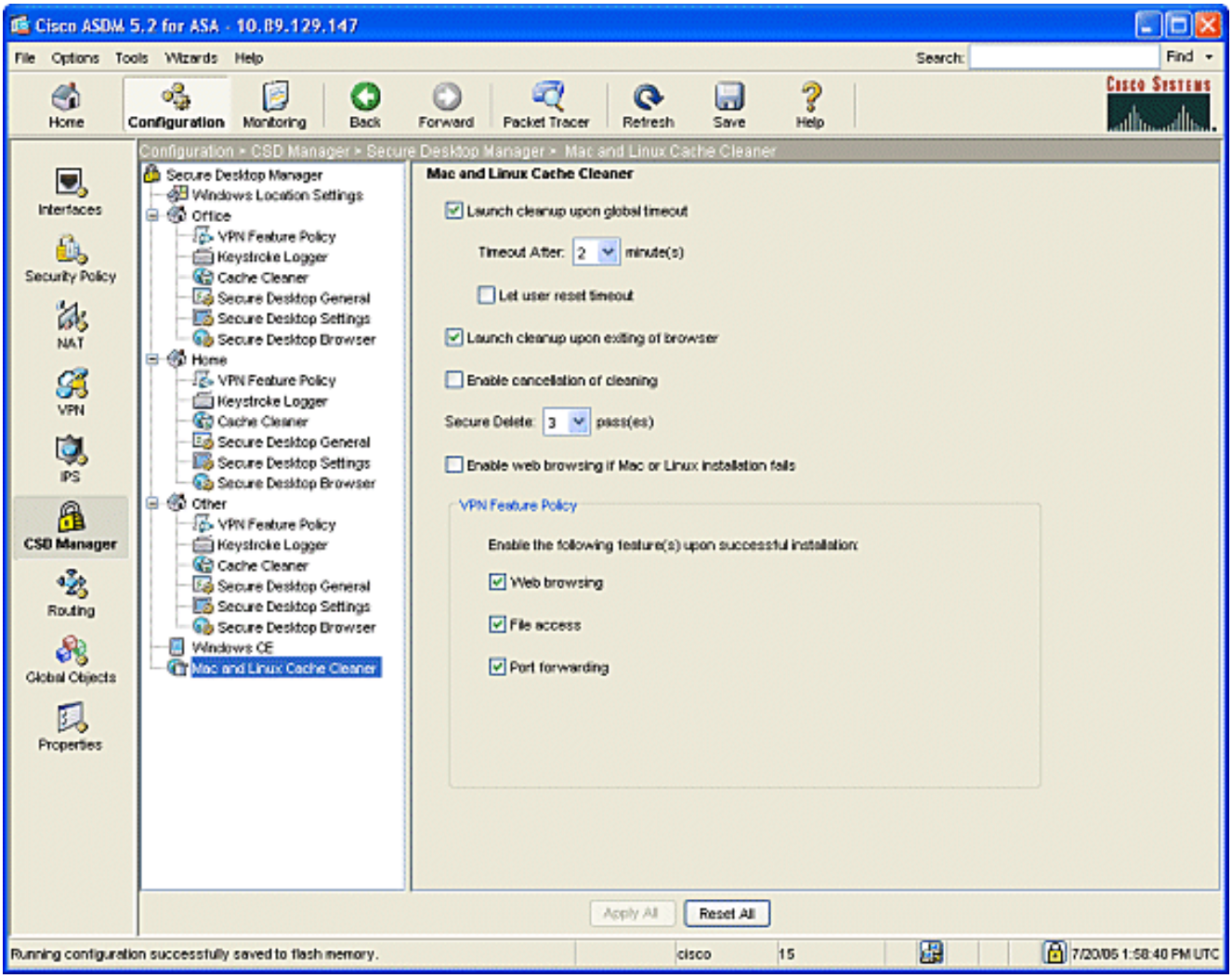
Configurações opcionais para Windows CE, Macintosh, e clientes Linux

Estas configurações são opcionais.

1. Se você escolhe **Windows CE do** painel de navegação, verifique a caixa de verificação da **navegação na web**.



2. Se você escolhe o **Mac e o líquido de limpeza do esconderijo de Linux do** painel de navegação, verifique a **limpeza do lançamento em cima do** seletor do rádio do **timeout global**.Mude o intervalo a sua especificação.Sob a área de **política da característica do** theVPN, verifique a **navegação na web, acesso de arquivo**, e o rádio da **transmissão da porta** disca para estes
clientes.



3. Se você escolhe Windows CE ou o Mac e o líquido de limpeza do esconderijo de Linux, o clique **aplica tudo**.
4. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.

Configurar

Configuração

Esta configuração reflete as mudanças ASDM feitas para permitir o CSD: A maioria das configurações CSD são mantidas em um arquivo separado no 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
```

Verificar

Use esta seção para confirmar que suas configurações para os sem clientes SSL VPN, o thin client SSL VPN, ou o cliente VPN SSL (SVC) se estão operando corretamente.

Teste o CSD com um PC que seja configurado com vários lugar de Windows. Cada teste deve fornecer um acesso diferente de acordo com as políticas que você configurou no exemplo acima.

Você pode mudar o número de porta e a relação onde Cisco ASA escuta conexões VPN da Web.

- A porta padrão é 443. Se você usa a porta padrão, o acesso é **endereço IP de Um ou Mais**

Servidores Cisco ICM NT de https://ASA.
- O uso de uma porta diferente muda o acesso ao **endereço IP de Um ou Mais Servidores Cisco ICM NT de https://ASA: newportnumber**.

Comandos

Vários **comandos show** estão associados ao WebVPN. Você pode executar estes comandos na interface de linha de comando (CLI) para mostrar estatísticas e outras informações. Para ver em detalhe o uso dos **comandos show**, refira a verificação da configuração WebVPN.

Nota: A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Se você tem problemas com o cliente remoto, verifique estes:

1. PNF-UPS, Javas, e/ou ActiveX são permitidos no navegador da Web? Estes podem precisar de ser permitido segundo o tipo de conexão de VPN SSL no uso.
2. O cliente deve aceitar os Certificados digitais apresentados no início da sessão.

Comandos

Vários **comandos debug** estão associados ao WebVPN. Para informações detalhadas sobre destes comandos, refira a utilização de comandos Debug WebVPN.

Nota: O uso de **comandos debug** pode afetar negativamente seu dispositivo Cisco. Antes de utilizar **comandos debug**, consulte Informações Importantes sobre Comandos Debug.

Informações Relacionadas

- Dispositivos de segurança adaptáveis Cisco ASA série 5500
- O ASA com WebVPN e escolhe Sinal-em usar o exemplo de configuração ASDM e NTLMv1
- Suporte Técnico e Documentação - Cisco Systems