ASDM を使用した ASA 7.2.x for Windows 上の Cisco Secure Desktop（CSD3.1.x）の設定例

目次

概要

Cisco Secure Desktop（CSD）は、SSL VPN テクノロジーのセキュリティを拡張します。 CSD では、ユーザのワークステーションでセッション アクティビティ用に個別のパーティションが設定されます。 この領域はセッション中は暗号化されており、SSL VPN セッションの終了時に完全に削除されます。 Windows は、CSD のセキュリティ上の恩恵をフルに受けるように設定できます。 Macintosh、Linux、および Windows CE で利用できるのは、キャッシュ クリーナ、Web ブラウジング、およびファイル アクセス機能だけです。 次のプラットフォームでは、Windows、Macintosh、Windows CE、および Linux のデバイスに対して CSD を設定できます。

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco IOS ® ソフトウェアリリース 12.4(6)T およびそれ以降を実行する Ciscoルータ
- Cisco VPN 3000 シリーズ コンセントレータ バージョン 4.7 以降
- Catalyst 6500 および 7600 シリーズ ルータ上の Cisco WebVPN モジュール

注: CSD リリース 3.3 では、Microsoft Windows Vista が稼働するリモート コンピュータ上で

Cisco Secure Desktop を設定できるようになりました。 以前は、Cisco Secure Desktop を稼働できるのは Windows XP または 2000 が動作するコンピュータに限られていました。 詳細は、Cisco Secure Desktop リリース 3.3 のリリース ノートの『新しい機能拡張：Vista 上の Secure Desktop』を参照してください。

この例では、Windows 用 ASA 5500 シリーズのクライアントでの CSD のインストールと設定について主に説明しています。 全体を網羅するために、Windows CE、Mac、および Linux クライアント用のオプションの設定も追加されています。

CSD は SSL VPN テクノロジー（クライアントレス SSL VPN、シンクライアント SSL VPN、または SSL VPN クライアント（SVC））とともに使用します。 CSD は SSL VPN テクノロジーのセキュア セッションに付加価値を与えます。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

ASA デバイスの要件

- Cisco CSD リリース 3.1 以降
- Cisco ASA ソフトウェア バージョン 7.1.1 以降
- Cisco Adaptive Security Device Manager（ASDM）リリース 5.1.1 以降**注:** CSD バージョン 3.2 でサポートされるのは、ASA バージョン 8.x だけです。**注:** ASA を ASDM で設定できるようにするには、『ASDM 用の HTTPS アクセスの許可』を参照してください。

クライアント コンピュータの要件

- リモート クライアントには、ローカルの管理者権限があること。 これは必須事項ではありませんが、重要な推奨事項です。
- リモート クライアントには、Java Runtime Environment（JRE）バージョン 1.4 以降が必要です。
- リモート クライアント ブラウザ： Internet Explorer 6.0、Netscape 7.1、Mozilla 1.7、Safari 1.2.2、Firefox 1.0 のいずれか
- リモート クライアントでクッキーがイネーブルにされており、ポップアップが許可されていること。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。 この設定で使用されている IP アドレスは、RFC 1918 の定義で使用されているアドレスです。 これらの IP アドレスは、実際のインターネット上で有効なものではなく、テ

スト用のラボ環境だけで使用されるものです。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

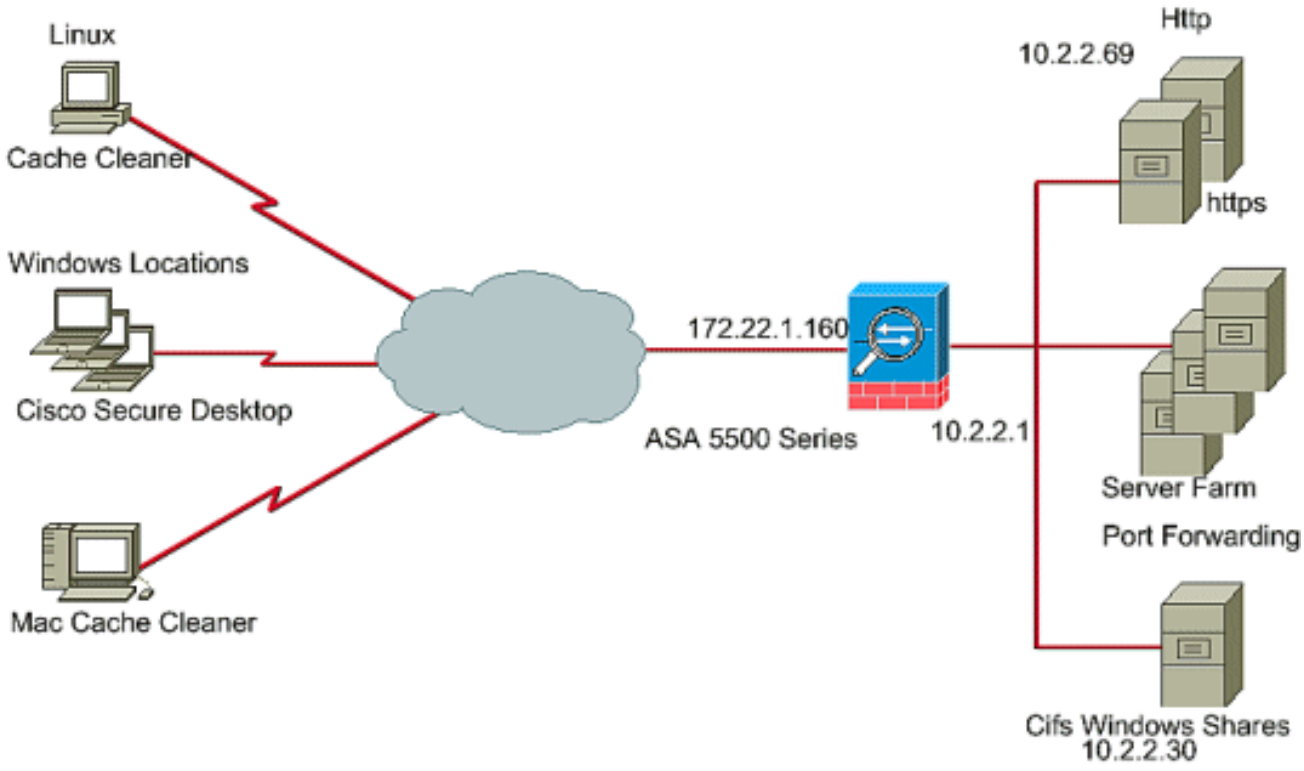
背景説明

CSD は SSL VPN テクノロジーを使用して動作するため、CSD を設定する前に、クライアントレス、シンクライアント、または SVC をアクティブにしておく必要があります。

ネットワーク図

さまざまな Windows のロケーションで、CSD のセキュリティ機能をすべて設定できます。Macintosh、Linux、および Windows CE では、キャッシュ クリーナと Web ブラウジングのどちらかまたは両方、およびファイル アクセスだけにアクセスできます。

このドキュメントでは、次のネットワーク構成を使用しています。



ASA での Windows クライアント用の CSD の設定

次の 5 つの主要手順により、ASA で Windows クライアント用の CSD を設定します。

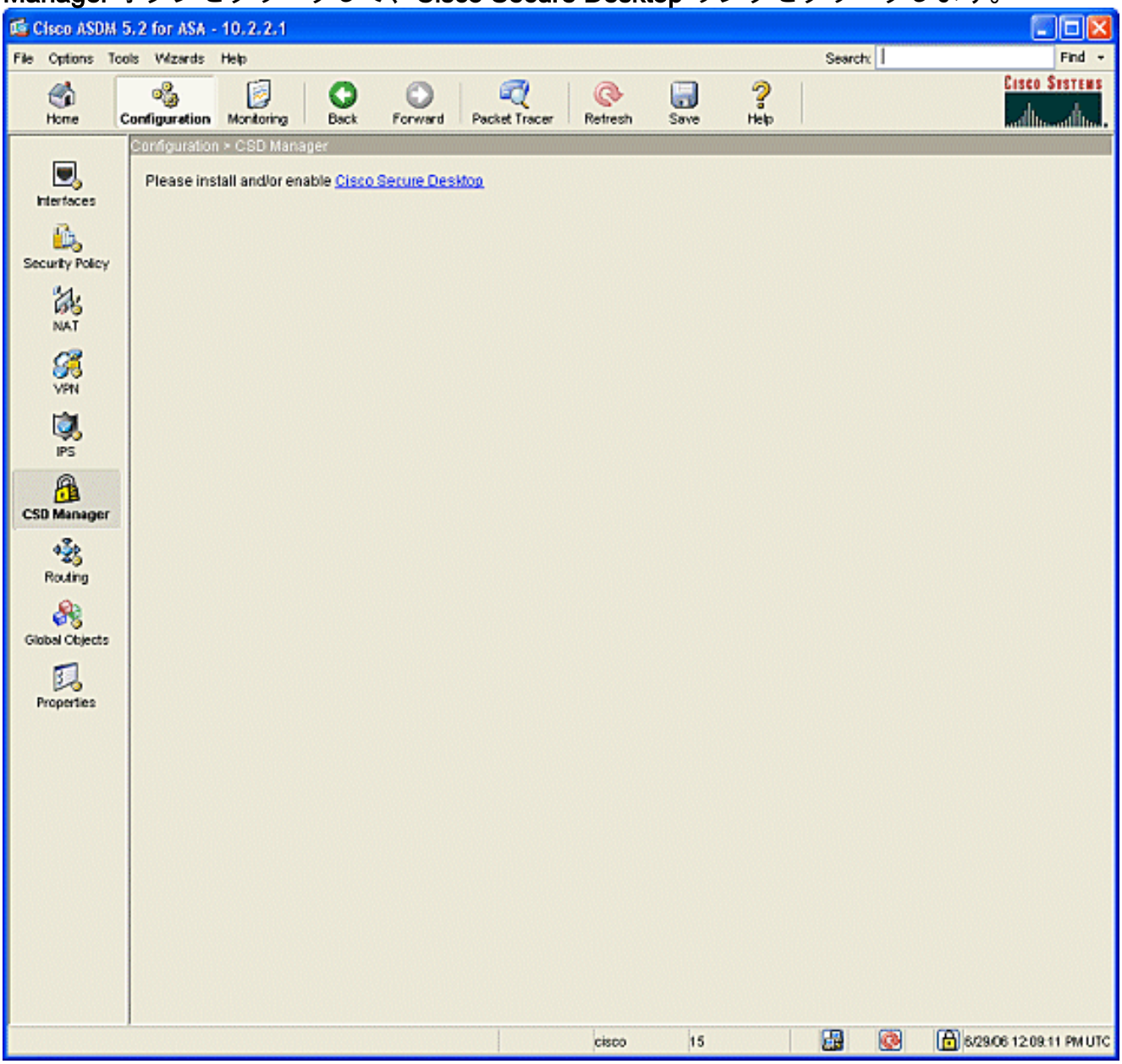
- Cisco ASA 上で CSD ソフトウェアを入手し、インストールして、イネーブルにする。
- Windows のロケーションを定義する。
- Windows のロケーション識別情報を定義する。
- Windows のロケーション モジュールを設定する。
- Windows のロケーション機能を設定する。

- オプションで、Windows CE、Macintosh、および Linux クライアント用に設定する。

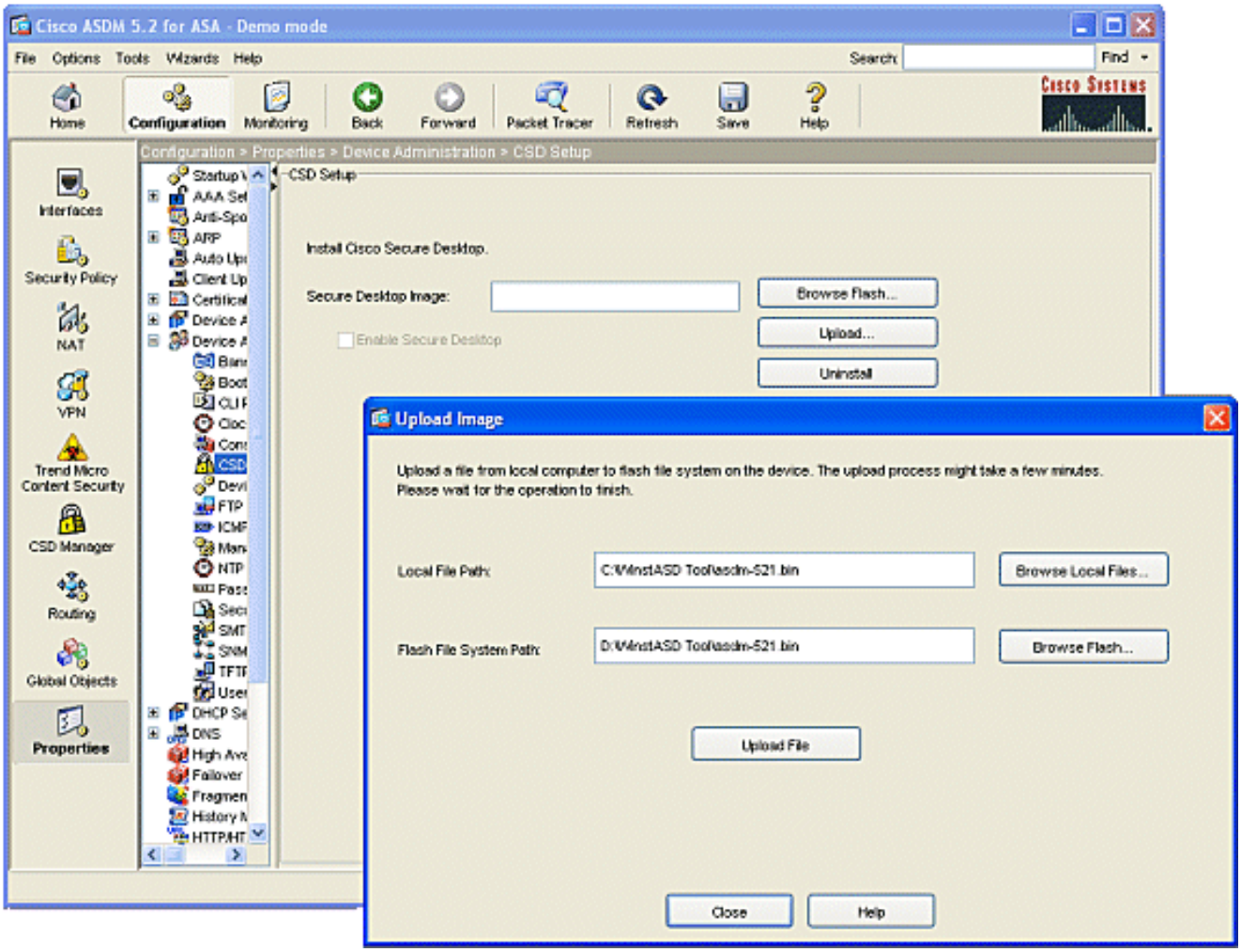
CSD ソフトウェアの入手、インストール、およびイネーブル

次の手順を実行して、Cisco ASA 上で CSD ソフトウェアを入手し、インストールして、イネーブルにします。

1. Cisco ソフトウェア ダウンロード Web サイトから CSD ソフトウェア securedesktop-asa*.pkg と readme ファイルを管理ステーションにダウンロードします。
2. ASDM にログインして、**Configuration** ボタンをクリックします。 左側のメニューから **CSD Manager** ボタンをクリックして、**Cisco Secure Desktop** リンクをクリックします。



3. **Upload** をクリックして、Upload Image ウィンドウを表示します。管理ステーションにある新しい .pkg ファイルのパスを入力するか、**Browse Local Files** をクリックしてファイルの場所を指定します。ファイルを配置するフラッシュの場所を入力するか **Browse Flash** をクリックします。[Upload File] をクリックします。確認を求められたら、**OK > Close > OK** の順にクリックします。

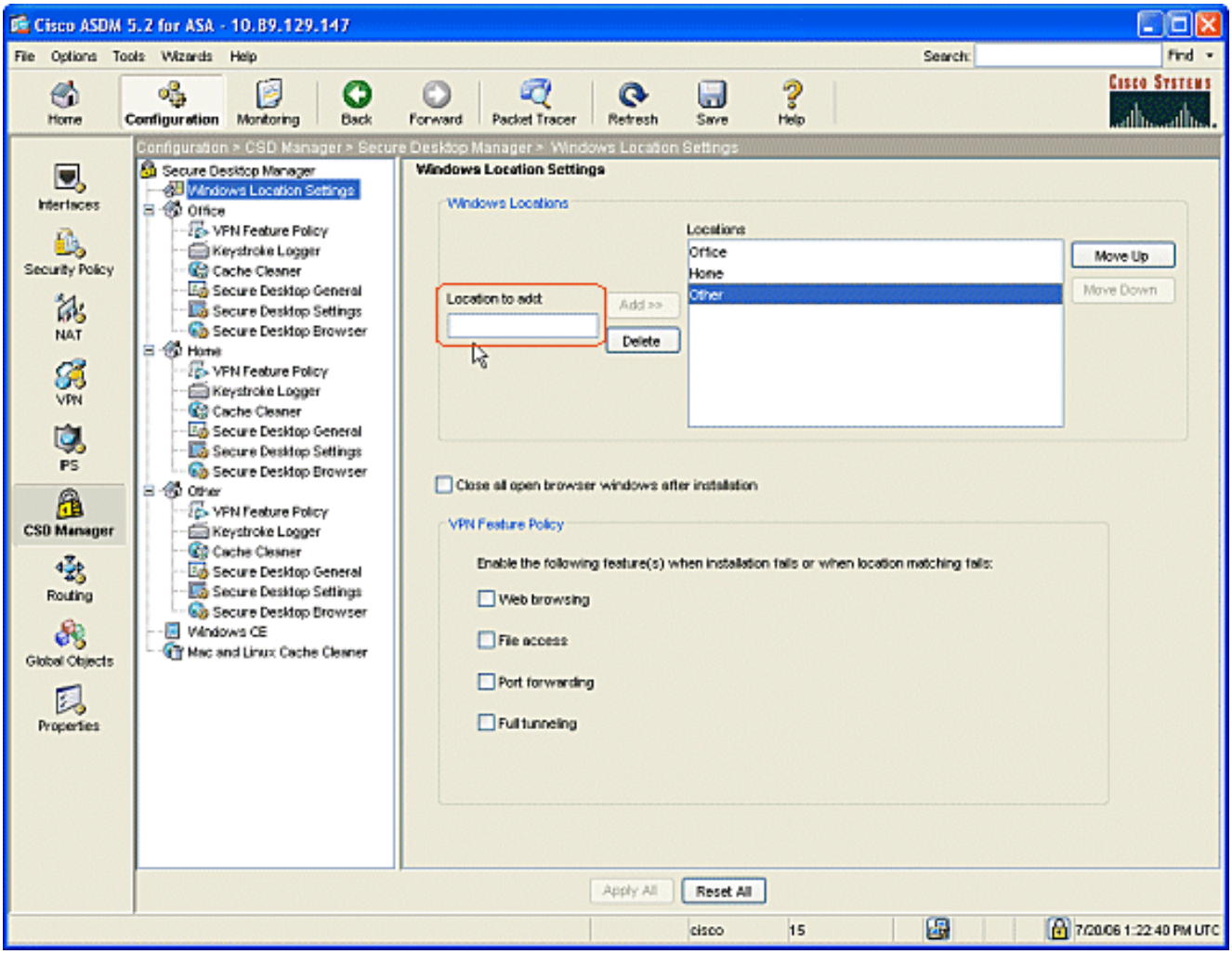


4. クライアント イメージがフラッシュにロードされたら、**Enable SSL VPN Client** チェックボックスにチェックマークを入れてから、**Apply** をクリックします。
5. [Save] をクリックし、[Yes] をクリックして変更を確定します。

Windows のロケーションの定義

次の手順を実行して、Windows のロケーションを定義します。

1. **Configuration** ボタンをクリックします。
2. 左側のメニューから **CSD Manager** ボタンをクリックして、**Cisco Secure Desktop** リンクをクリックします。
3. ナビゲーション ペインで **Windows Location Settings** をクリックします。
4. Location to Add フィールドにロケーション名を入力して、**Add** をクリックします。この例の 3 つの場所に注意して下さい: オフィス、ホーム、および他。Office は、会社のセキュリティ境界内にあるワークステーションを表しています。Home は、自宅から作業するユーザを表しています。Other は、上記の 2 つ以外のロケーションを表しています。

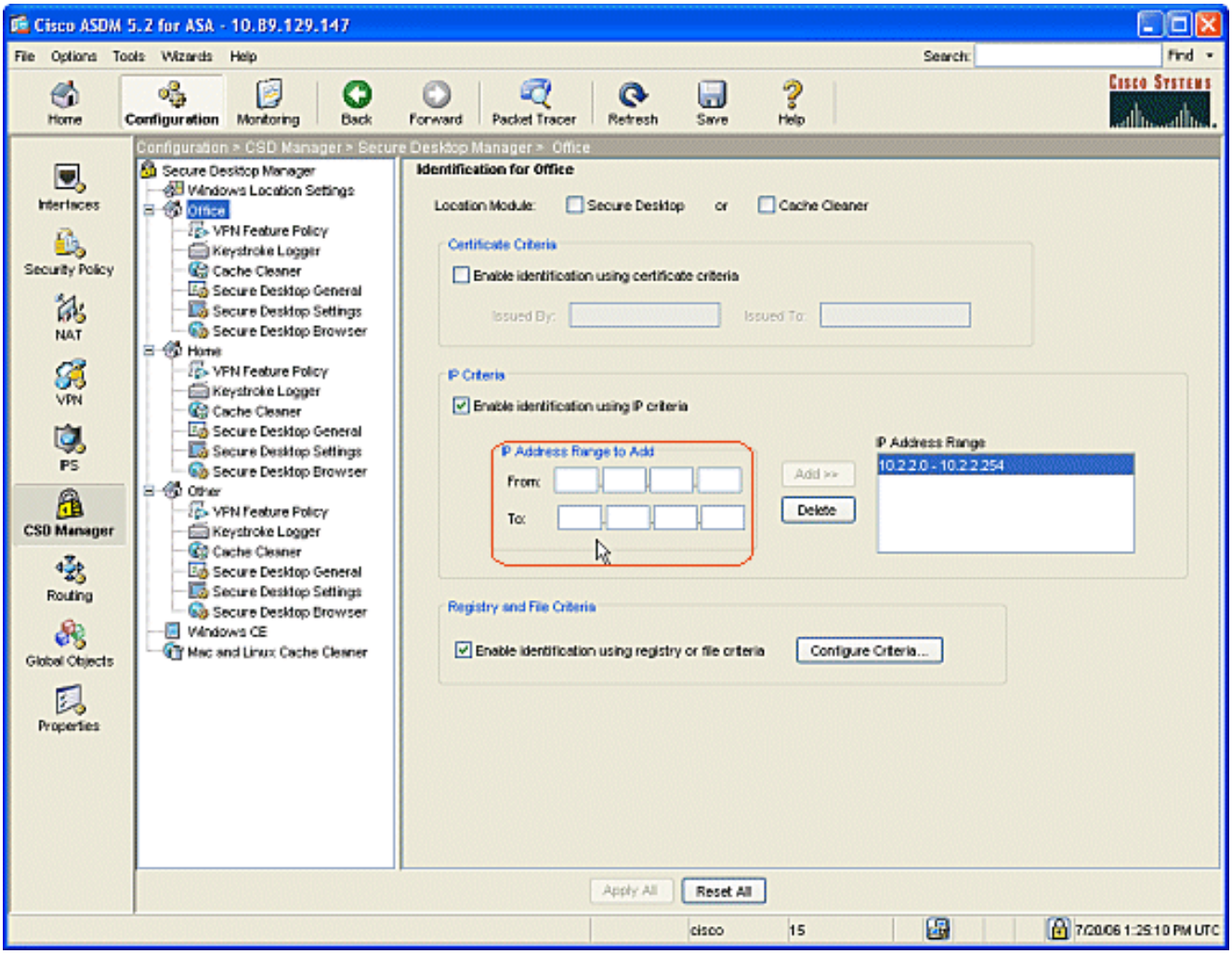


5. ネットワーク アーキテクチャのレイアウトに応じて、営業、ゲスト、パートナー、その他用の口ケーションを作成します。
6. Windows の口ケーションを作成していくと、ナビゲーション ペインが拡張されて、それぞれの新しい口ケーションに設定可能なモジュールが表示されます。 [Apply All] をクリックします。
7. [Save] をクリックし、[Yes] をクリックして変更を確定します。

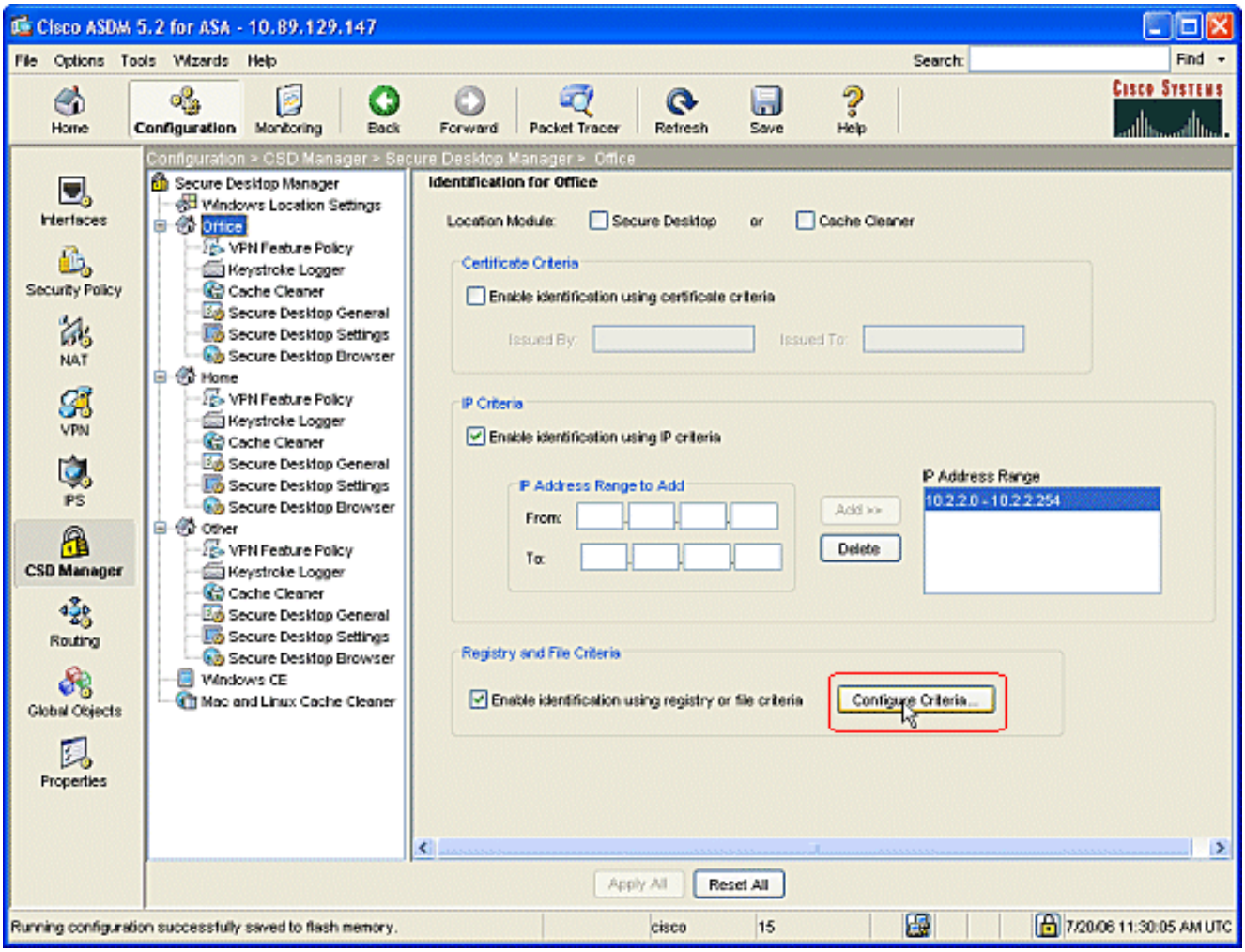
Windows の口ケーション識別情報

次の手順を実行して、Windows の口ケーション識別情報を定義します。

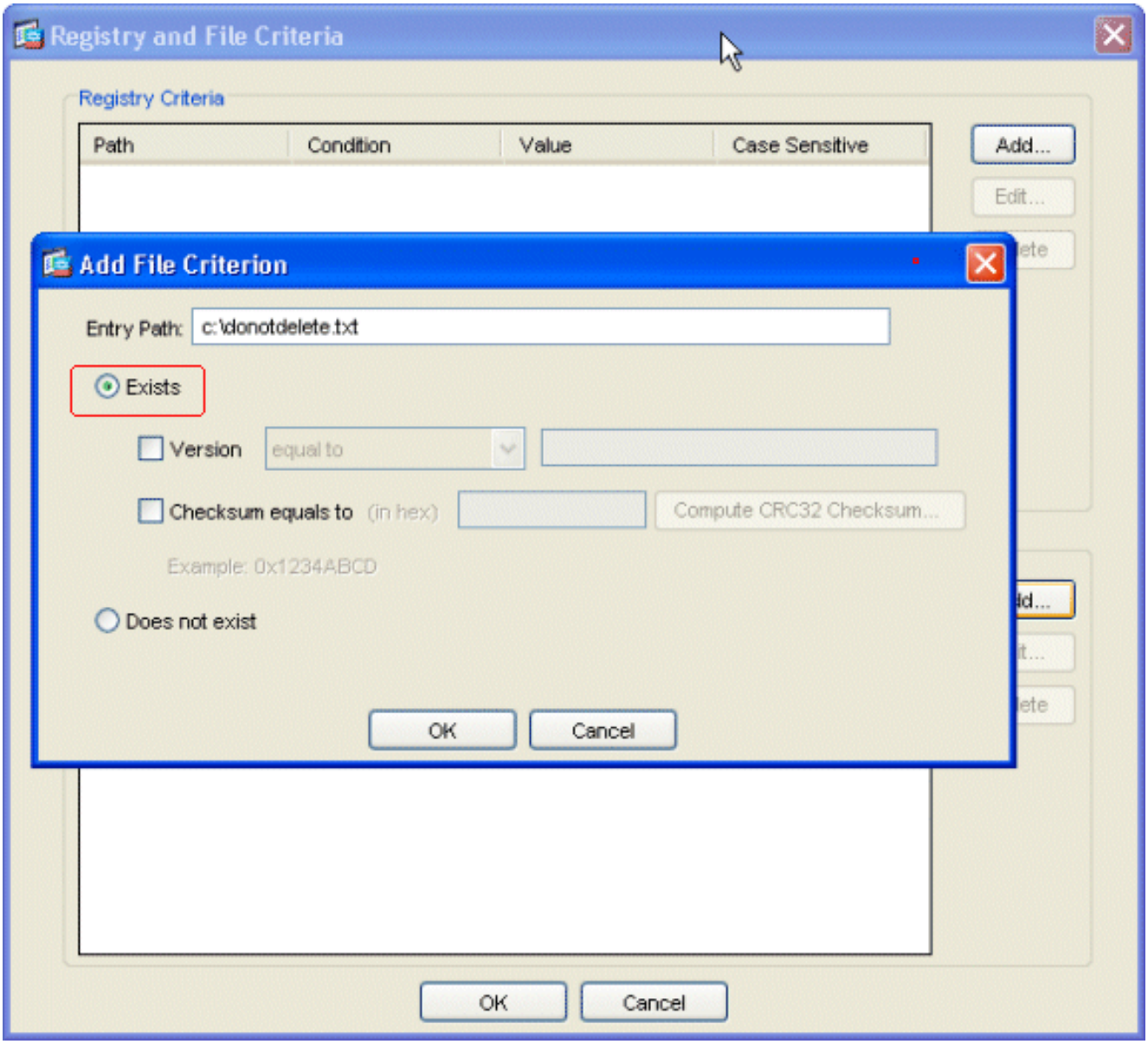
1. 「 Windows の口ケーションの定義」で作成した口ケーションを識別します。



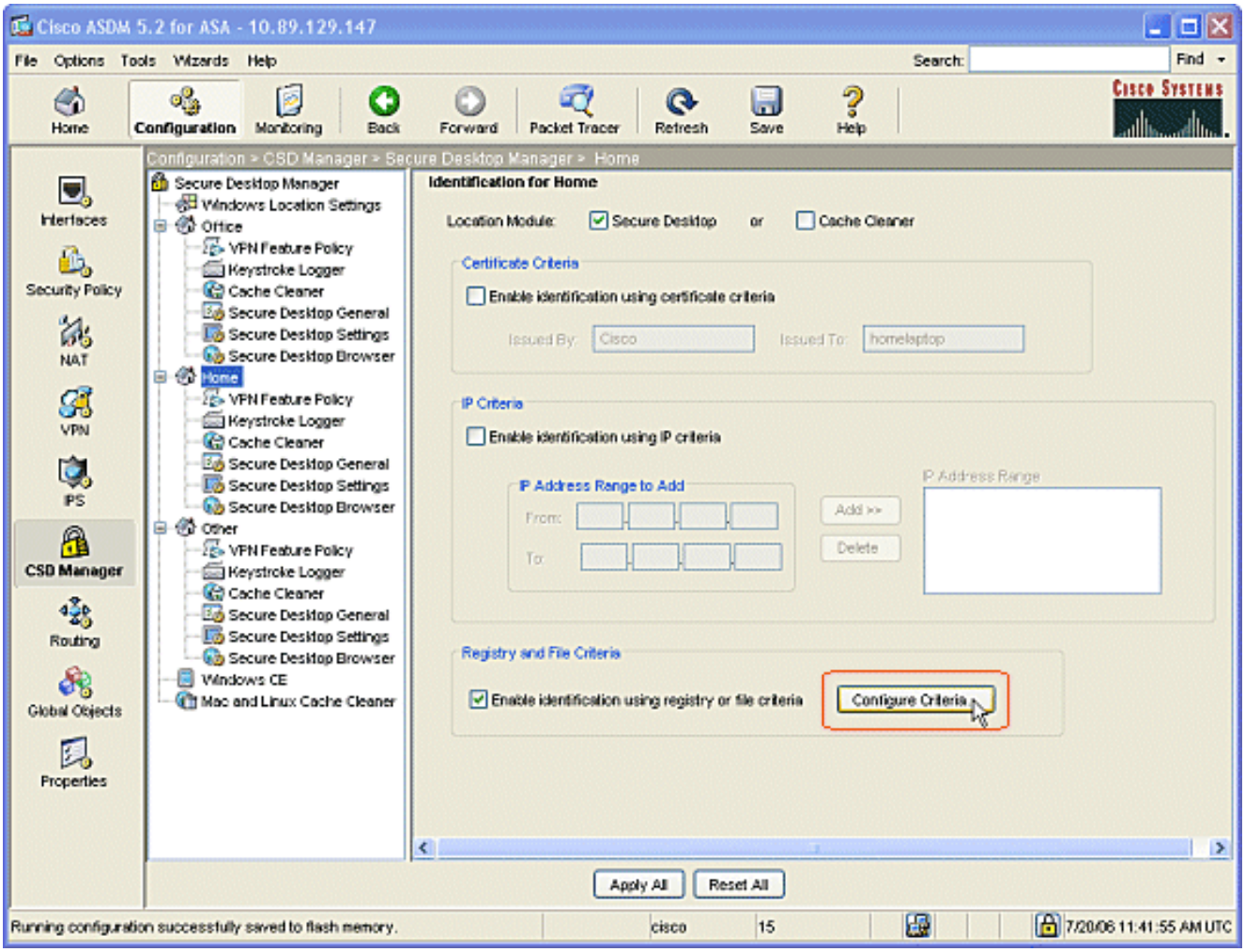
2. Office という口ケーションを識別するために、ナビゲーション ペインで **Office** をクリックします。これらは内部コンピュータなので、**Secure Desktop** チェック ボックスと **Cache Cleaner** チェック ボックスのチェックマークを外します。**Enable identification using IP criteria** チェック ボックスにチェックマークを入れます。内部コンピュータの IP アドレス範囲を入力します。**Enable identification using registry or file criteria** チェック ボックスにチェックマークを入れます。 この設定により、内部のオフィス ワーカーとネットワーク上の一時的なゲストを区別できます。



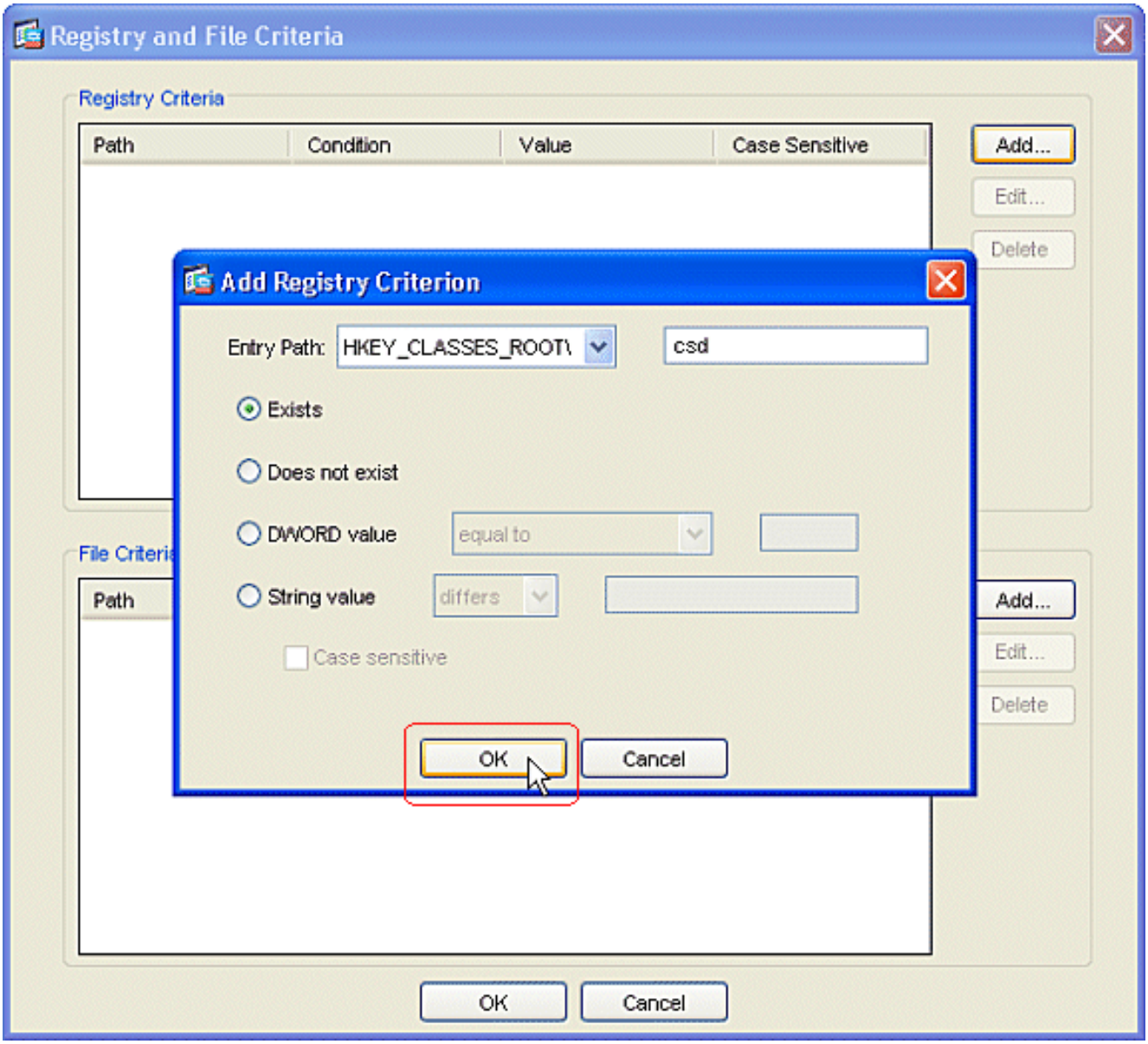
3. **Configure Criteria** をクリックします。 簡単なサンプル ファイル「DoNotDelete.txt」が設定されます。 このファイルは、内部の Windows コンピュータに存在する必要がある、単なるプレースホルダです。 Windows レジストリ キーを設定して、内部オフィスのコンピュータを識別することもできます。 OKIN をウィンドウ追加ファイル 基準のクリックして下さい。 OKIN をレジストリおよびファイル 基準のウィンドウ クリックして下さい。



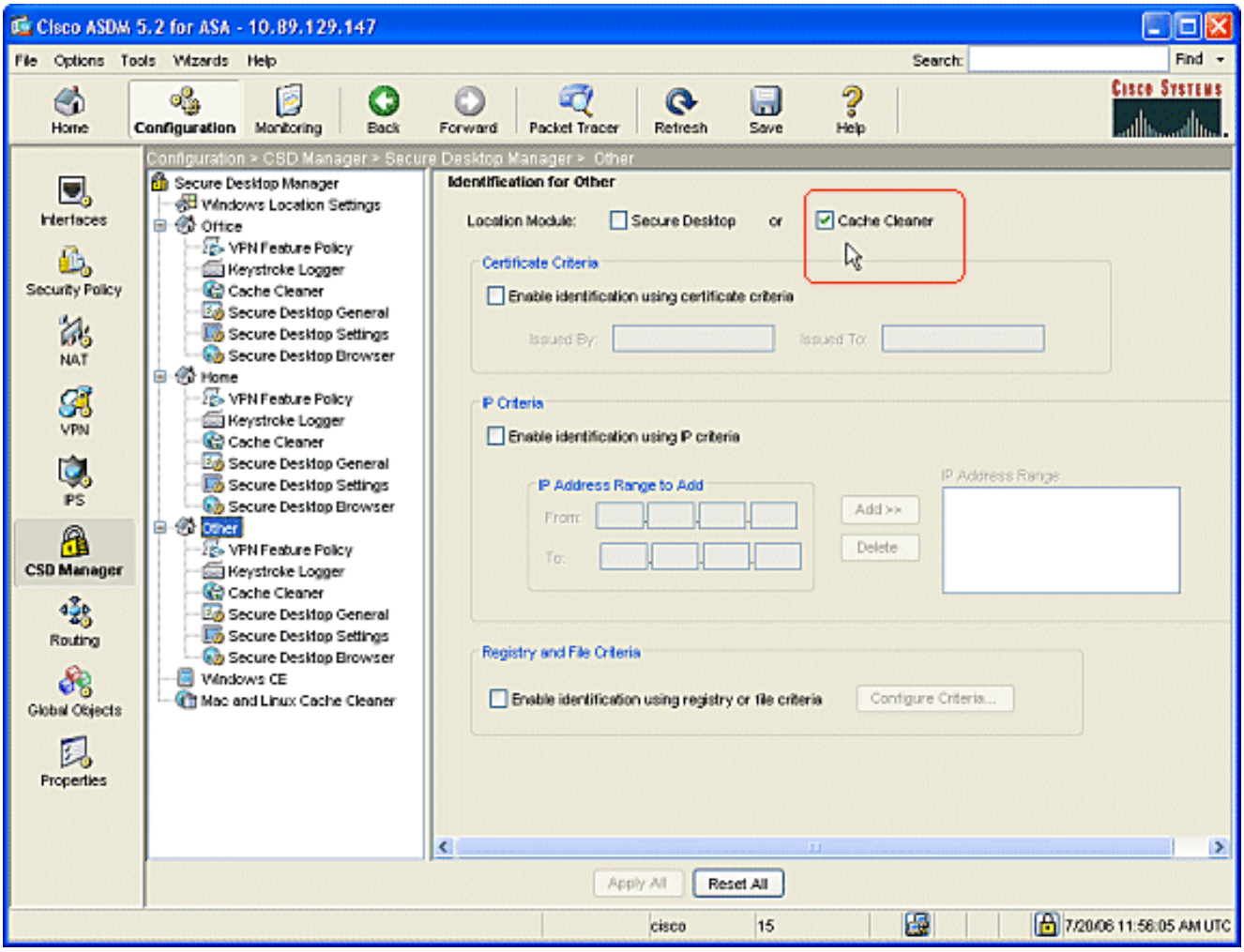
4. Identification for Office ウィンドウで **Apply All** をクリックします。 [Save] をクリックし、[Yes] をクリックして変更を確定します。
5. Home という口ケーションを識別するために、ナビゲーション ペインで **Home** をクリックします。**Enable identification using registry or file criteria** チェック ボックスにチェックマークを入れます。**Configure Criteria** をクリックします。



6. Home コンピュータのクライアントは、このレジストリ キーを使用して管理者が設定しておく必要があります。 Add Registry Criterion ウィンドウで **OK** をクリックします。 Registry and File Criteria ウィンドウで **OK** をクリックします。



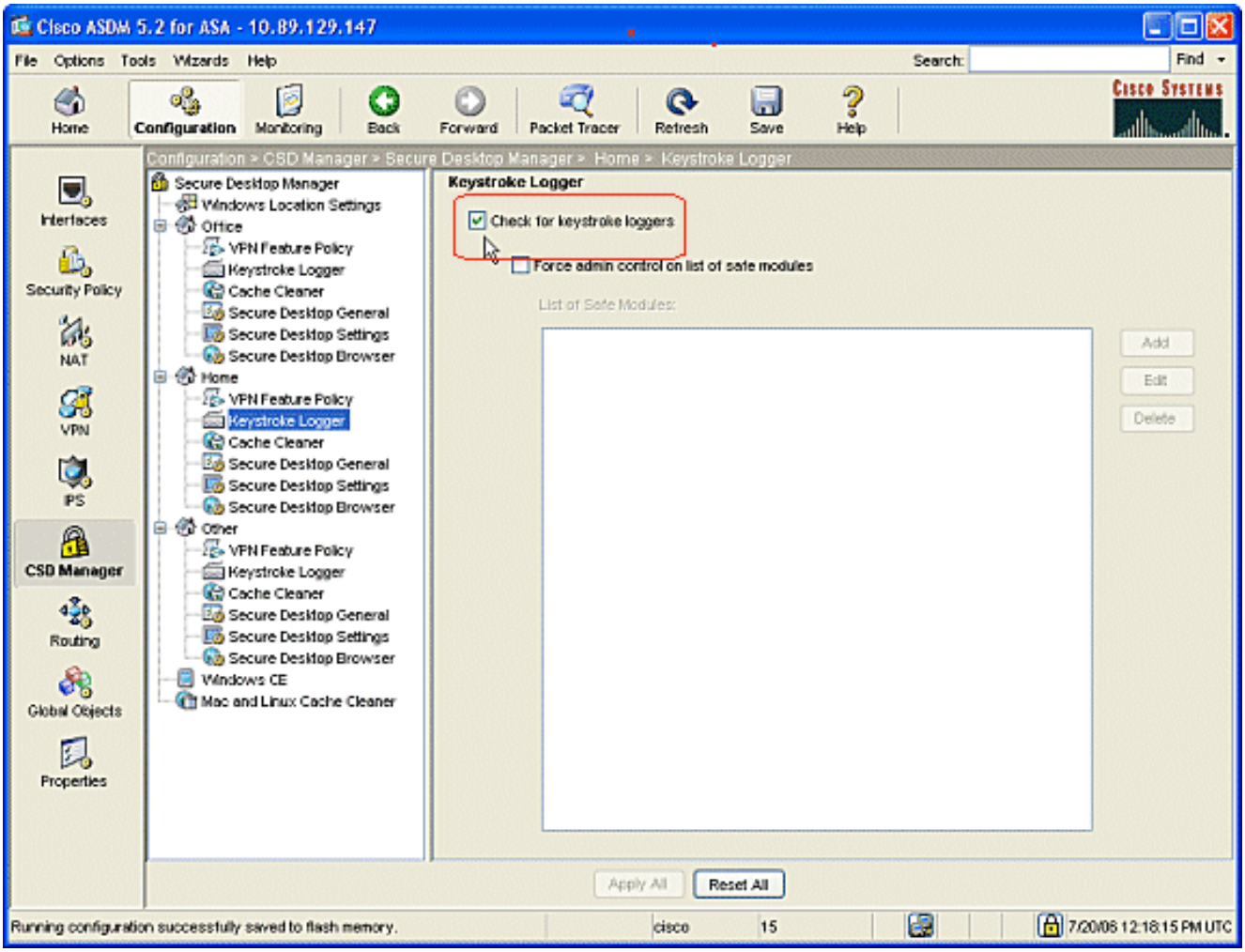
7. Location Module で **Secure Desktop** チェック ボックスにチェックマークを入れます。Identification for Home ウィンドウで **Apply All** をクリックします。 [Save] をクリックし、[Yes] をクリックして変更を確定します。
8. **Other** という口ケーションを識別するために、ナビゲーション ペインで **Other** をクリックします。**Cache Cleaner** チェック ボックスだけにチェックマークを入れて、他のチェック ボックスはすべてチェックマークを外します。Identification for Other ウィンドウで **Apply All** をクリックします。[Save] をクリックし、[Yes] をクリックして変更を確定します。



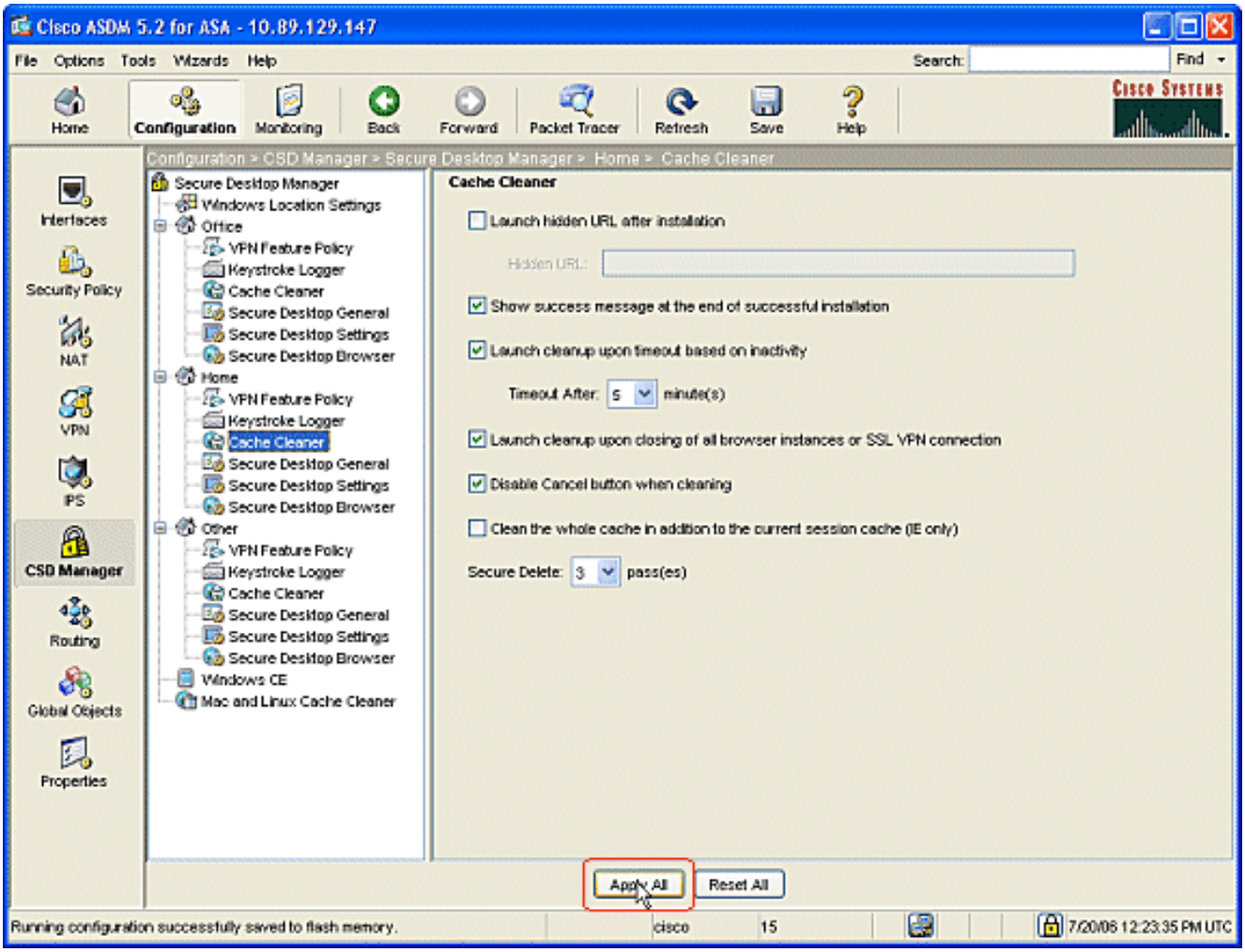
Windows のロケーション モジュールの設定

次の手順を実行して、作成した 3 つのロケーションそれぞれにモジュールを設定します。

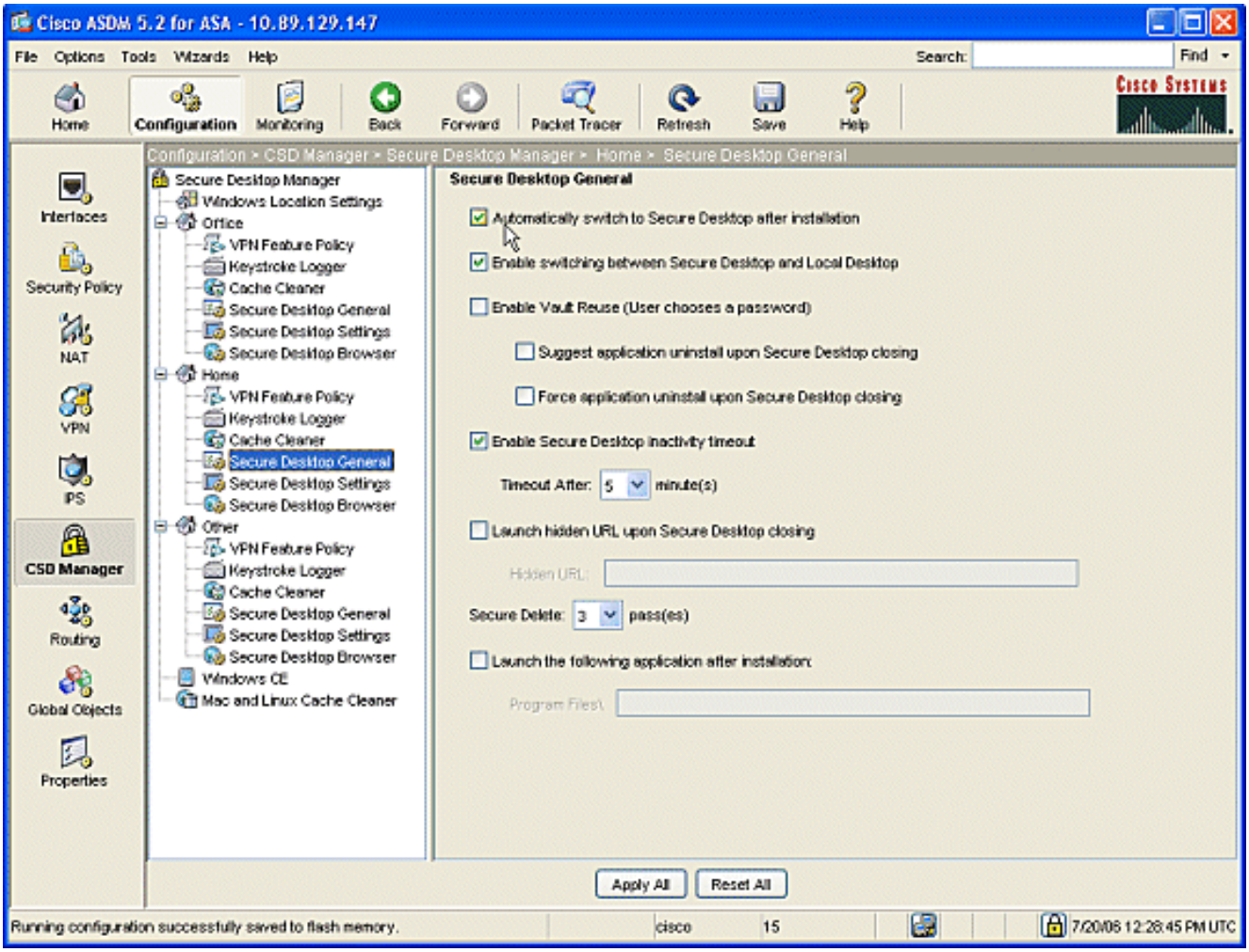
1. Office クライアントの場合は、以前の手順で Secure Desktop と Cache Cleaner を選択しなかったので、何の作業もしません。 ASDM アプリケーションでは、以前の手順で Cache Cleaner を選択しなかった場合でも、Cache Cleaner を設定できます。 Office ロケーション用のデフォルト設定をそのまま使用します。**注:** この手順では VPN Feature Policy について説明していませんが、この後のすべてのロケーション用の手順で説明します。
2. Home クライアントの場合は、ナビゲーション ペインで **Home** と **Keystroke Logger** をクリックします。Keystroke Logger ウィンドウで、**Check for keystroke loggers** チェック ボックスをオンにします。Keystroke Logger ウィンドウで **Apply All** をクリックします。[Save] をクリックし、[Yes] をクリックして変更を確定します。



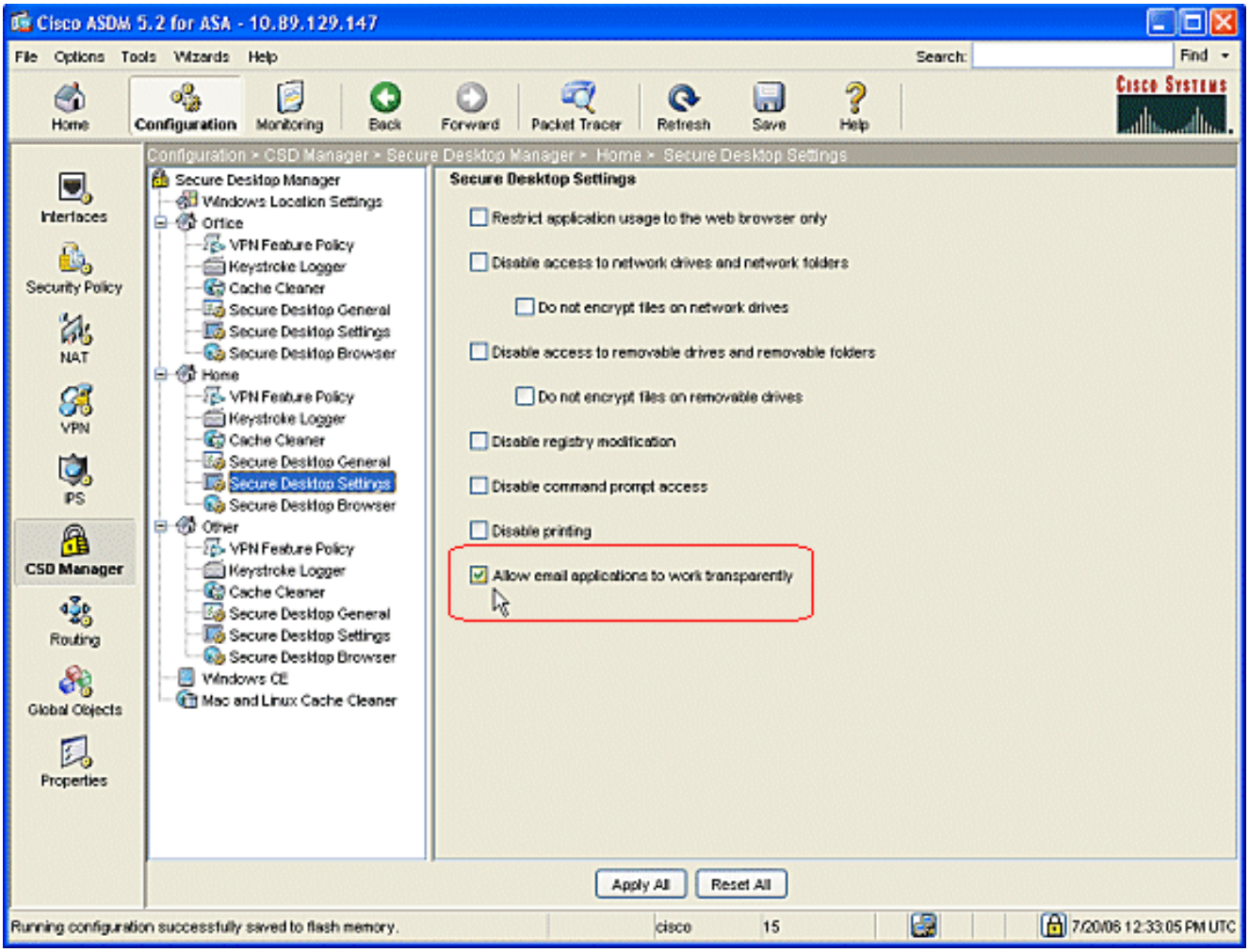
3. Home で、**Cache Cleaner** と環境に適したパラメータを選択します。



4. Home で、**Secure Desktop General** と環境に適したパラメータを選択します。



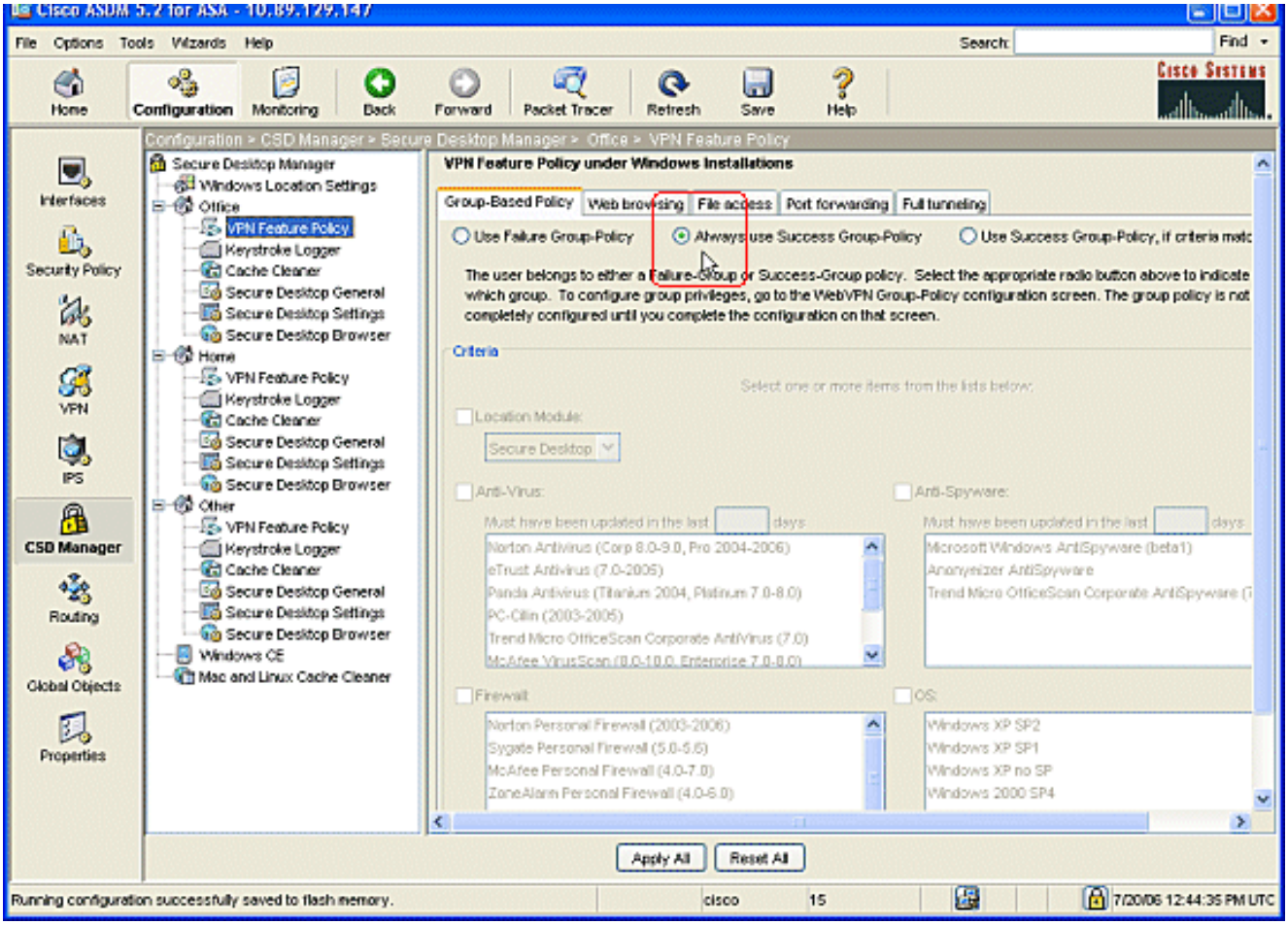
5. Home で **Secure Desktop Settings** を選択します。**Allow email applications to work transparently** チェック ボックスにチェックマークを入れて、環境に合わせて他の設定をします。[Apply All] をクリックします。[Save] をクリックし、[Yes] をクリックして変更を確定します。



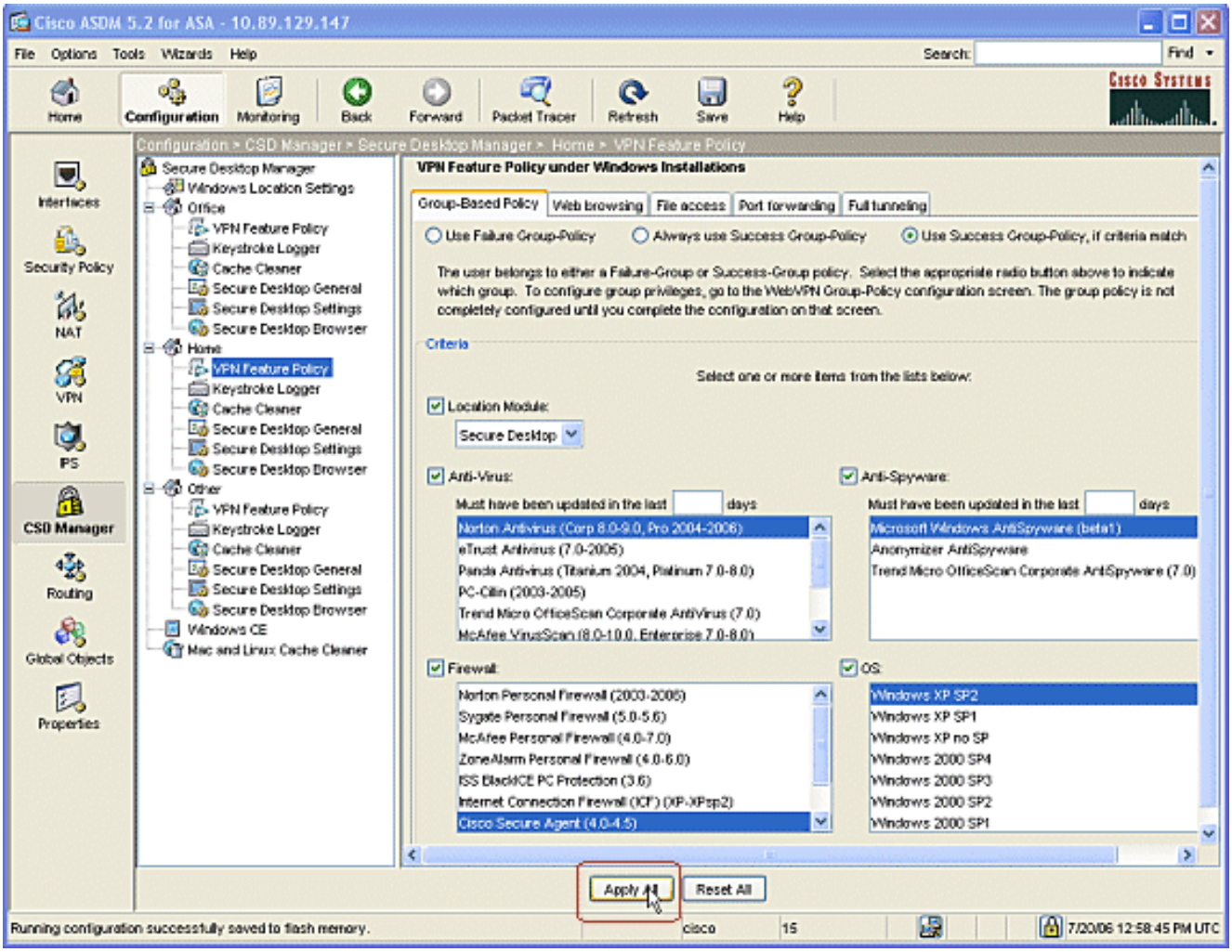
Windows のロケーション機能の設定

作成した各ロケーションの VPN Feature Policy を設定します。

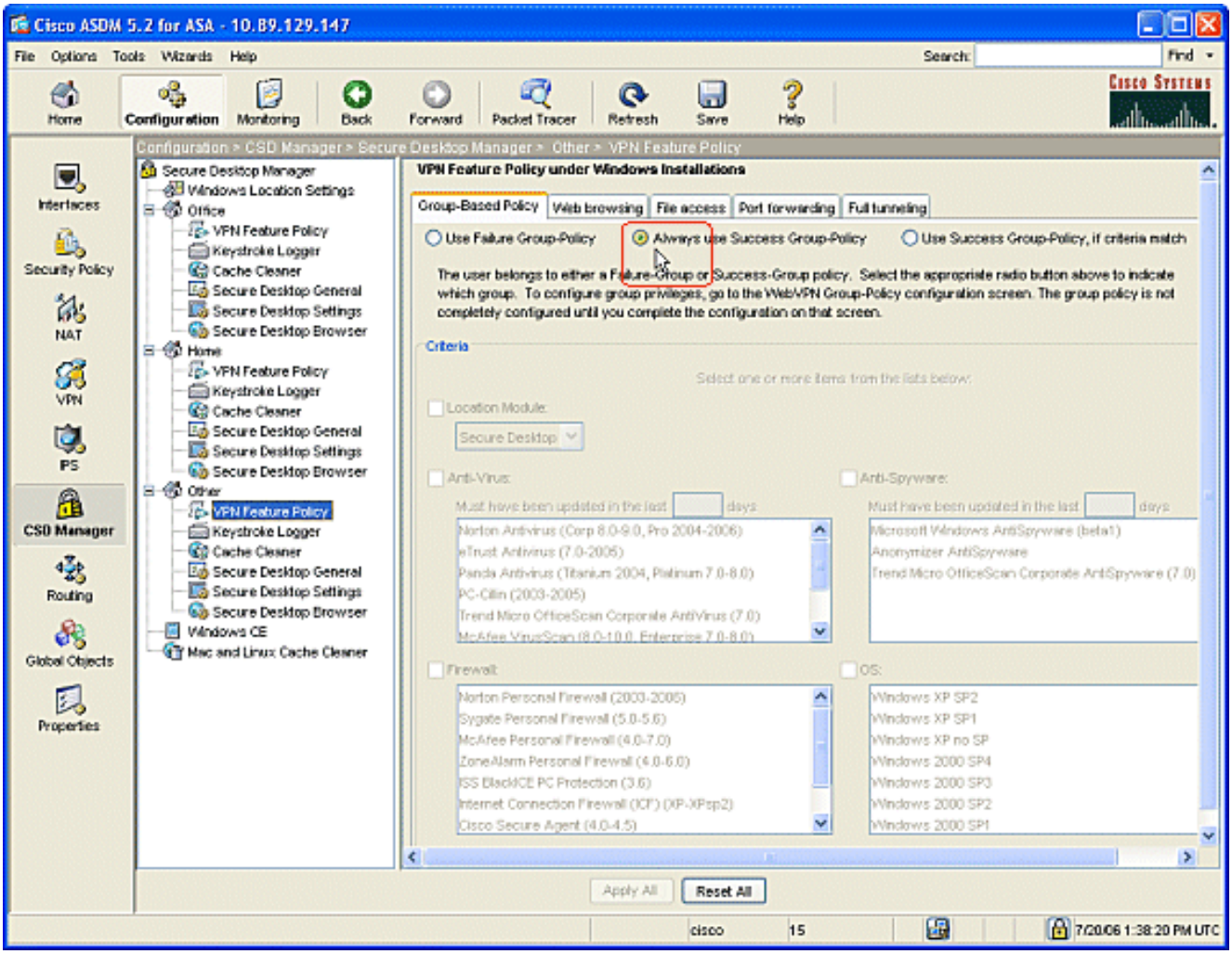
1. ナビゲーション ペインで **Office**、**VPN Feature Policy** の順にクリックします。
2. **Group-Based Policy** タブをクリックします。**Always use Success Group-Policy** オプション ボタンをクリックします。**Web browsing** タブをクリックして、**Always Enabled** オプション ボタンをオンにします。**File access** タブ、**Port forwarding** タブ、および **Full tunneling** タブでも同じ手順を実行します。[Apply All] をクリックします。[Save] をクリックし、[Yes] をクリックして変更を確定します。



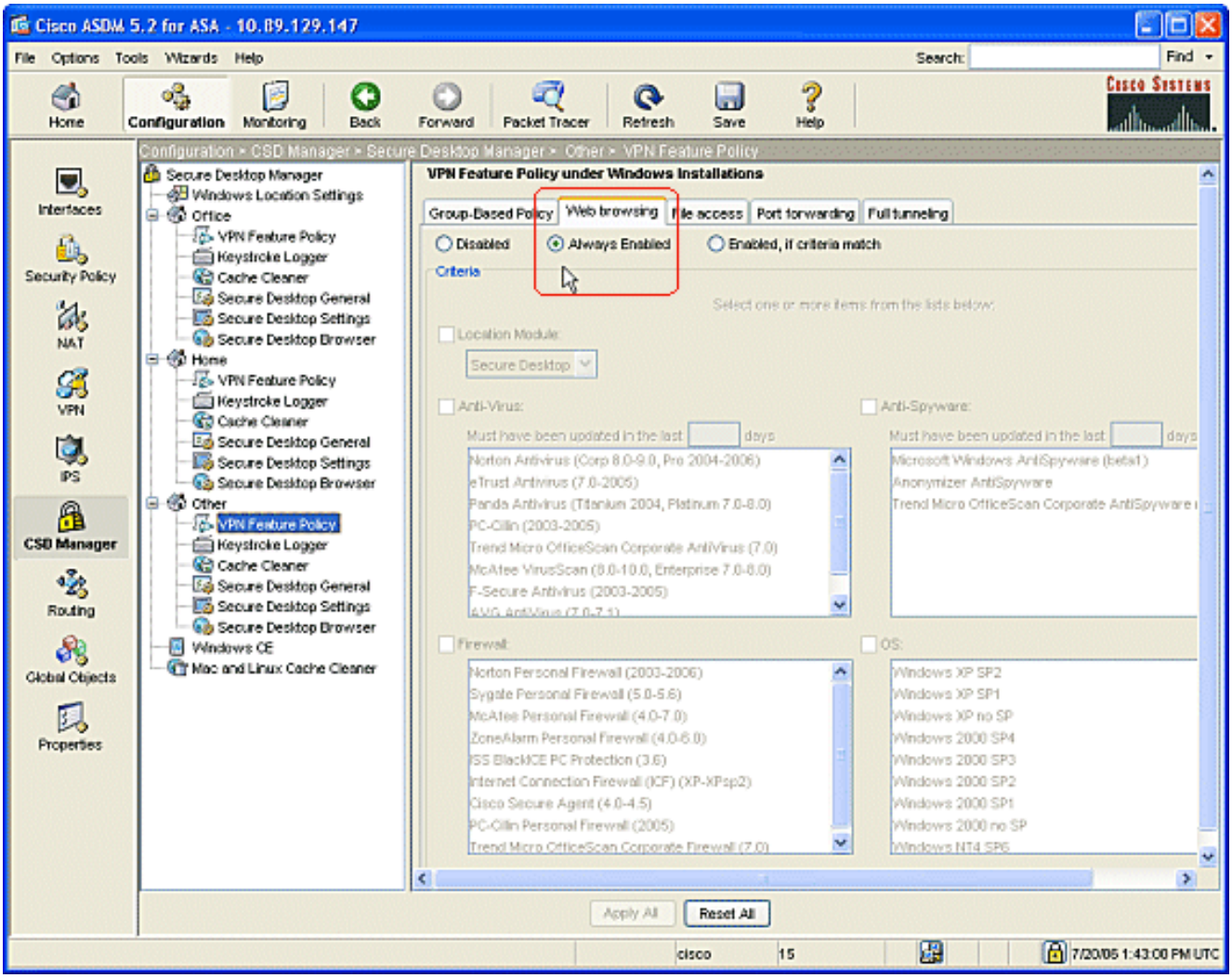
3. Home ユーザの場合は、アクセスが許可される前に、会社ごとに特定のポリシーが必要になる場合があります。 ナビゲーション ペインで **Home**、**VPN Feature Policy** の順にクリックします。**Group-Based Policy** タブをクリックします。特定のレジストリ キー、既知のファイル名、デジタル証明書などの事前に設定された条件が一致する場合は、**Use Success Group-Policy** オプション ボタンをオンにします。**Location Module** チェック ボックスにチェックマークを入れて、**Secure Desktop** を選択します。**Anti-Virus**、**Anti-Spyware**、**Firewall**、および **OS** の各領域を、会社のセキュリティ ポリシーに従って選択します。 Home ユーザのコンピュータが設定された条件に一致しない場合、Home ユーザはネットワークへのアクセスを許可されません。



4. ナビゲーション ペインで Other、VPN Feature Policy の順にクリックします。Group-Based Policy タブをクリックします。Always use Success Group-Policy オプション ボタンをクリックします。



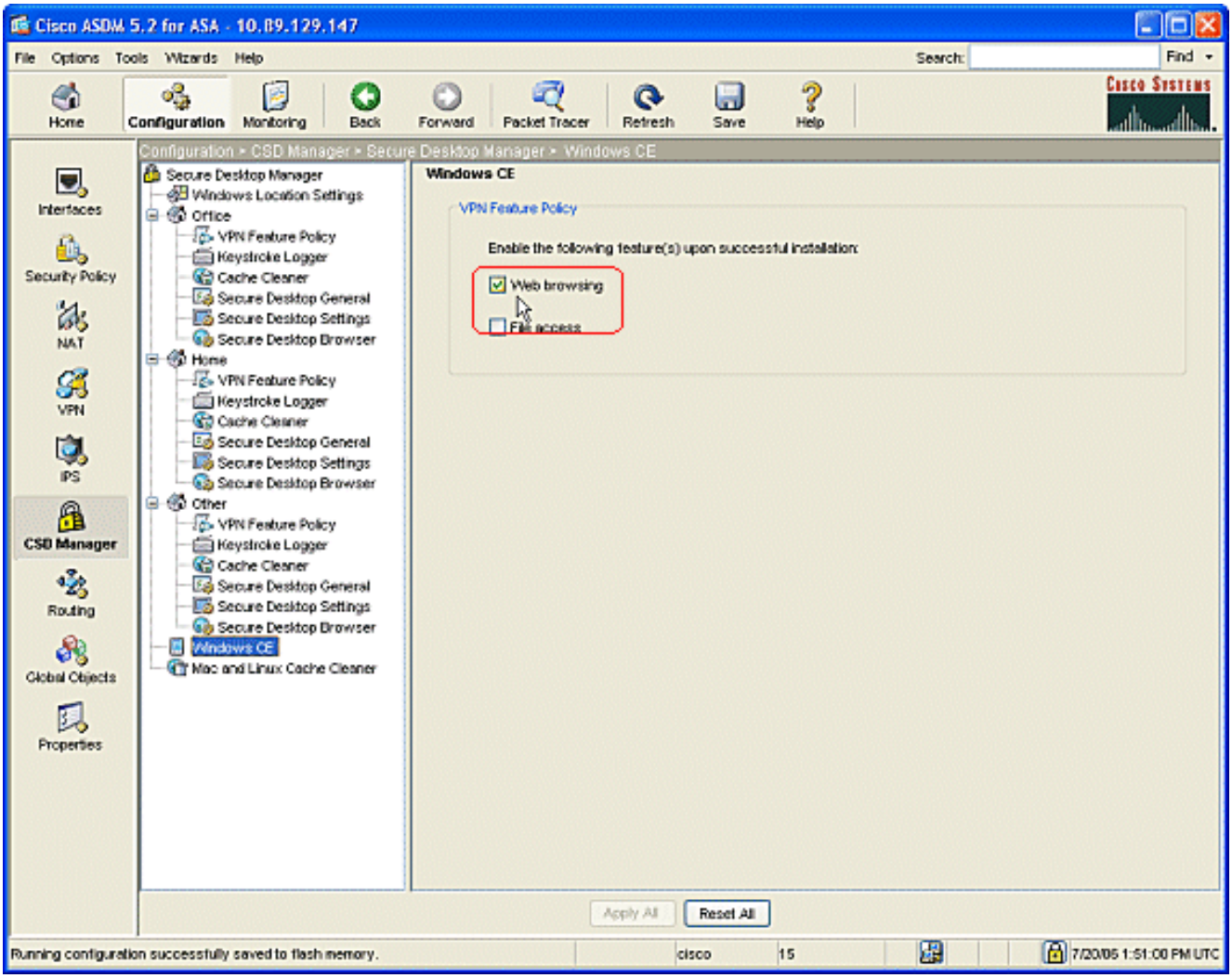
5. この VPN Feature Policy ロケーションにあるクライアントに対して、Web Browsing タブをクリックして、Always Enabled オプション ボタンをクリックします。File Access タブをクリックして、Disable オプション ボタンをオンにします。Port Forwarding タブと Full Tunneling タブでもこの手順を繰り返します。[Apply All] をクリックします。[Save] をクリックし、[Yes] をクリックして変更を確定します。



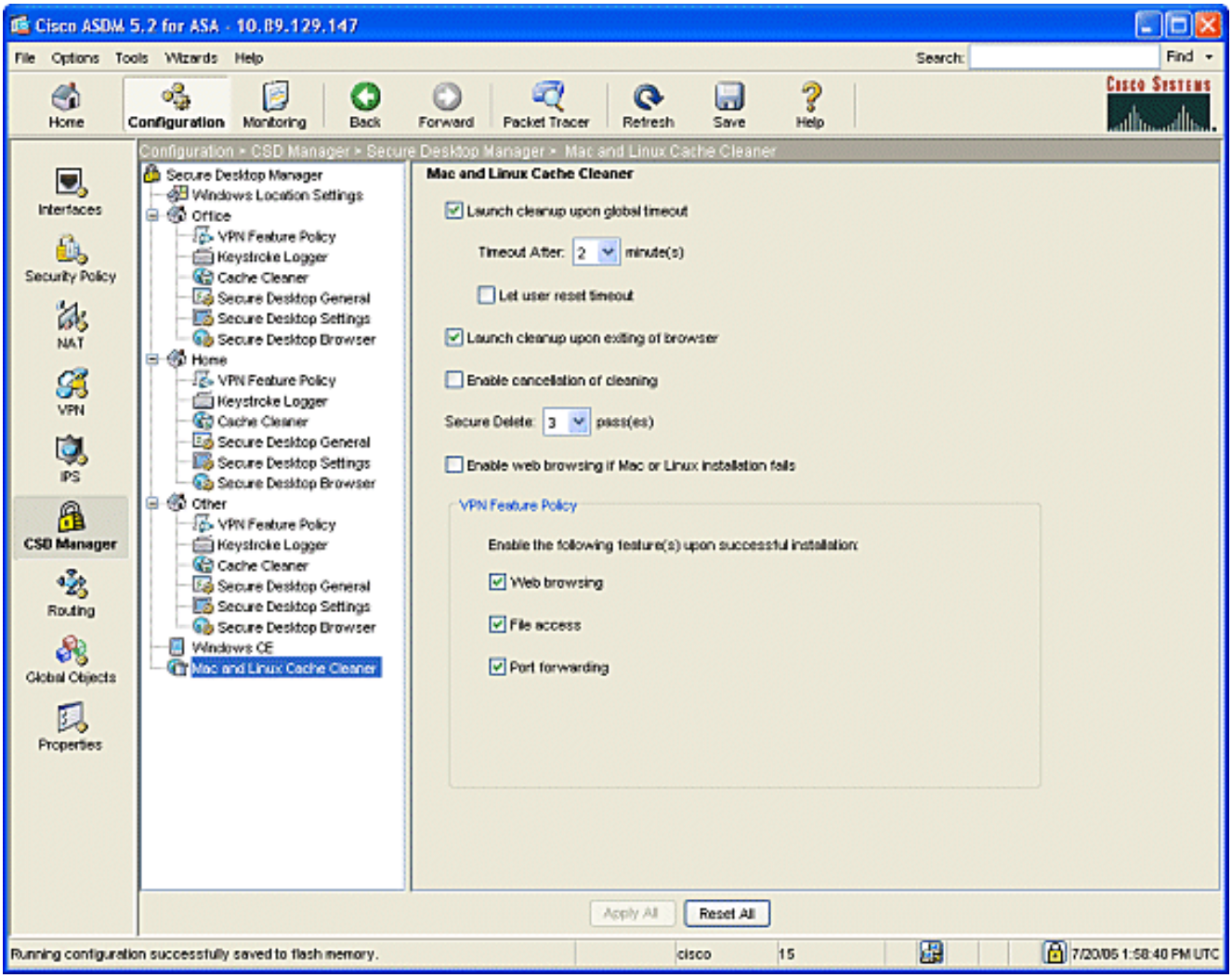
Windows CE、Macintosh、および Linux クライアント用のオプション設定

次の設定はオプションです。

1. ナビゲーション ペインから Windows CE を選択する場合は、Web browsing チェック ボックスにチェックマークを入れます。



2. ナビゲーション ペインから Mac and Linux Cache Cleaner を選択する場合は、Launch cleanup upon global timeout チェック ボックスにチェックマークを入れます。仕様に合わせてタイムアウトを変更します。VPN Feature Policy 領域で、これらのクライアントの Web browsing、File access、Port forwarding の各チェック ボックスをオンにします。



3. Windows CE と Mac and Linux Cache Cleaner のどちらを選択した場合でも、**Apply All** をクリックします。
4. [Save] をクリックし、[Yes] をクリックして変更を確定します。

設定

設定

この設定では、ASDM で行った変更を反映して、CSD をイネーブルにします。 ほとんどの CSD 設定は、フラッシュにある別のファイルに保存されています。

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
```

確認

このセクションでは、クライアントレス SSL VPN、シンクライアント SSL VPN または SSL VPN クライアント（SVC）が正しく動作していることを確認します。

さまざまな Windows の口ケーションが設定された PC を使用して CSD をテストします。 各テストでは、上記の例で設定したポリシーに従ってさまざまなアクセスが行われます。

Cisco ASA が WebVPN 接続をリッスンするポート番号とインターフェイスを変更できます。

- デフォルト ポートは 443 です。 デフォルト ポートを使用する場合、アクセスは **https://ASA**

IP Address になります。
- 異なるポートの使用は https://ASA IP アドレスにアクセスを変更します: newportnumber。

コマンド

いくつかの **show** コマンドは WebVPN に関連しています。 これらのコマンドをコマンドライン インターフェイス（CLI）で実行して、統計情報や他の情報を表示できます。 **show** コマンドの使用方法についての詳細は、『WebVPN 設定の確認』を参照してください。

注: Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

リモート クライアントで問題が発生する場合は、次の点を調べます。

1. ポップアップ、Java、ActiveX のいずれかまたはすべてが Web ブラウザでイネーブルになっていますか。 使用する SSL VPN 接続のタイプによっては、これらをイネーブルにすることが必要な場合があります。
2. クライアントは、セッションの開始時に提示されるデジタル証明書を受け入れる必要があります。

コマンド

いくつかの **debug** コマンドは、WebVPN に関連しています。 これらのコマンドについての詳細は、『WebVPN Debug コマンドの使用』を参照してください。

注: debug コマンドを使用すると、Cisco デバイスに悪影響が及ぶ可能性があります。 **debug** コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

関連情報

- Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンス
- ASDM および NTLMv1 を使用した WebVPN およびシングル サインオン機能付き ASA の設定例
- テクニカルサポートとドキュメント - Cisco Systems