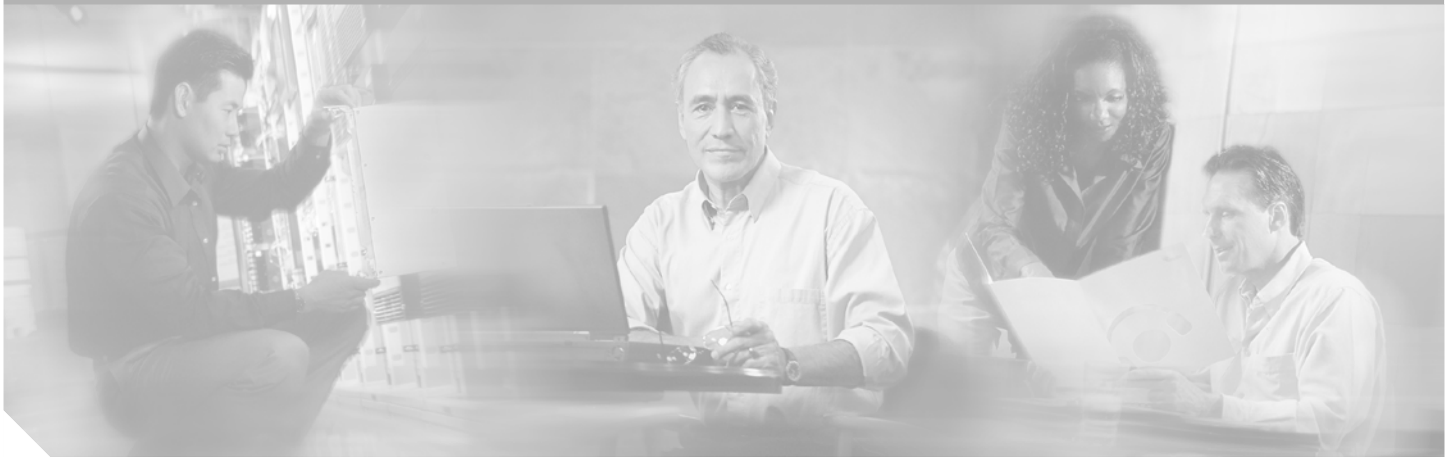


Cisco Secure Desktop Configuration Guide

for Cisco ASA 5500 Series Administrators

Software Release 3.1.1
October 2006

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-8607-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Secure Desktop Configuration Guide

CONTENTS

About This Guide

Refer to the following sections to understand the audience, topics, and conventions in this guide, and the titles of related documents. Subsequent sections describe how to obtain documentation, provide feedback, learn about Cisco product security, report security problems, and obtain technical assistance.

Audience and Scope

Written for network managers and administrators, this guide describes how to install, configure, and enable Cisco Secure Desktop (CSD) on a Cisco ASA 5500 Series security appliance to provide a safe computing environment through which clients can connect from a variety of locations.

This guide describes how to specify the types of locations from which Microsoft® Windows users connect, the criteria used to identify those locations, and the access rights and restrictions to assign to clients that match the location criteria. It also describes how to configure features to support Windows CE, Macintosh, and Linux clients.

Organization and Use

Table 1 describes the contents of this guide.

Table 1 Document Organization

Topic	Purpose
Installing or Upgrading the CSD Software	Describes how to obtain the CSD software, and install or upgrade it.
Enabling and Disabling CSD	Describes how to enable or disable remote client access to CSD.
Introduction	Describes CSD capabilities, how to access the Secure Desktop Manager (the browser-enabled interface for CSD administrators), how to navigate the Secure Desktop Manager, and how to save configuration changes.
Tutorial	Steps you through an example configuration to provide an overview of how to deploy CSD, and introduces you to the security decisions that you need to make to best accommodate your users and secure your network.

Table 1 Document Organization (continued)

Topic	Purpose
Setting Up CSD for Microsoft Windows Clients	Describes how to configure Secure Desktop and Cache Cleaner support for remote clients running Microsoft Windows.
Setting Up CSD for Microsoft Windows CE Clients	Describes how to configure a VPN feature policy to enable or restrict web browsing and file access for remote clients running Microsoft Windows CE.
Setting Up CSD for Macintosh and Linux Clients	Describes how to configure the Cache Cleaner and VPN feature policy for clients running Macintosh or Linux.
Frequently Asked Questions	Provides questions and answers on a broad range of CSD functions.

Conventions

This document uses the following conventions:

- **Boldface** indicates commands and keywords that you enter literally as shown, menu options you choose, or buttons and check boxes you click.
- *Italics* indicate arguments for which you supply values.
- Examples show screen displays and the command line in `screen` font.

Note Means *reader take note*. Notes contain helpful suggestions, or references to material not covered in the manual.

Caution Means *reader be careful*. Cautions alert you to actions or conditions that could result in equipment damage or loss of data.

Related Documentation

For more information, refer to the following documentation:

- *Release Notes for Cisco Secure Desktop*
- *Cisco ASA 5500 Series Release Notes*
- *Cisco ASDM Release Notes*
- *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*
- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Migrating to ASA for VPN 3000 Concentrator Series Administrators*
- Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide for the ASA 5510, ASA 5520, and ASA 5540
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*

- *Selected ASDM VPN Configuration Procedures for the Cisco ASA 5500 Series*
- *Cisco Security Appliance Logging Configuration and System Log Messages*

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security

Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting

show command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Installing or Upgrading the CSD Software

CSD Release 3.1 requires that you install ASA Release 7.1.1 and ASDM Release 5.1.1 or later.

Note You do not need to boot the security appliance after you install the CSD software.

Install or upgrade the Cisco Secure Desktop (CSD) software as follows:

Step 1 Use your Internet browser to access the following URL and download the **securedesktop_asa_<*n*>_<*n*>*.pkg** file to any location on your PC:

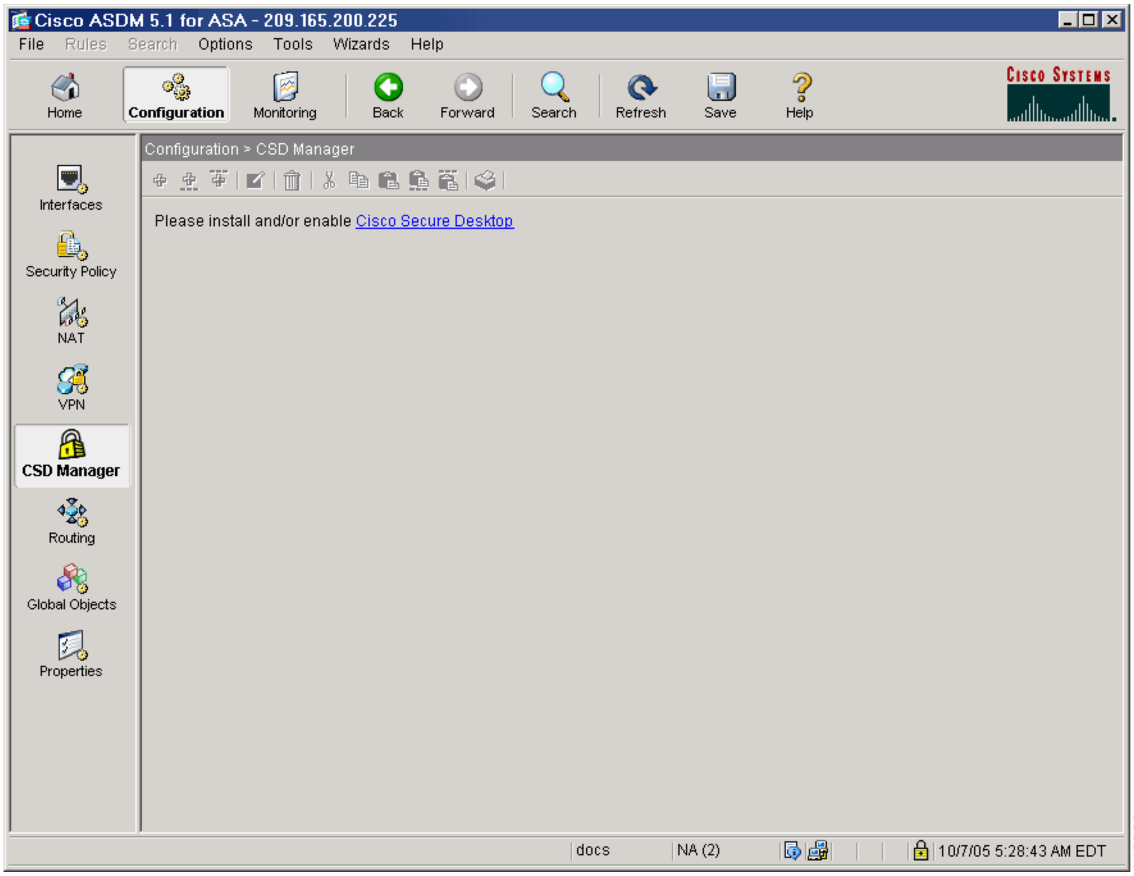
http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

Step 2 Use your Internet browser to log in to ASDM.

Step 3 Choose **Configuration** > **CSD Setup**.

The pane displays the message "Please install and/or enable Cisco Secure Desktop" if CSD is not installed (Figure 1-1).

Figure 1-1 CSD Manager Not Installed



Cisco ASDM 5.1 for ASA - 209.165.200.225

Configuration > CSD Manager

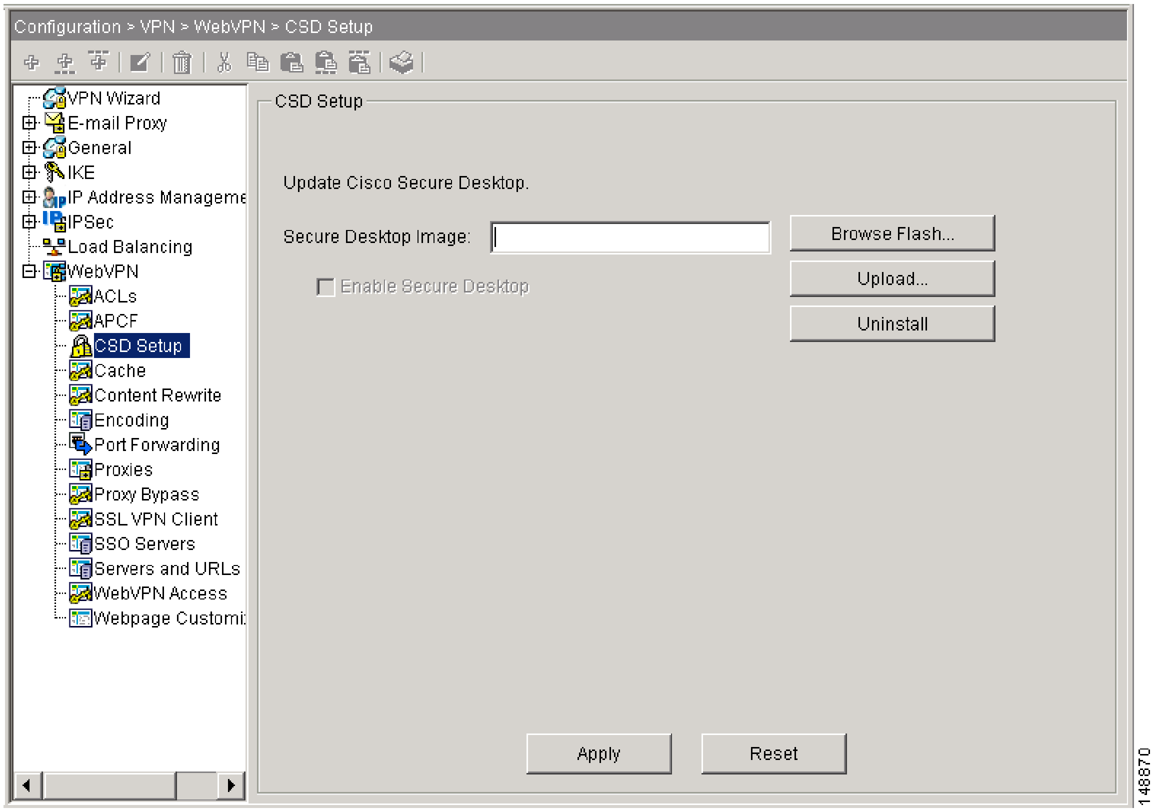
Please install and/or enable Cisco Secure Desktop

10/7/05 5:28:43 AM EDT

Step 4 Click the "Cisco Secure Desktop" link.

ASDM opens the Configuration > VPN > WebVPN > CSD Setup pane (Figure 1-2).

Figure 1-2 CSD Setup (Installation)



Update Cisco Secure Desktop.

Secure Desktop Image:

□ Enable Secure Desktop

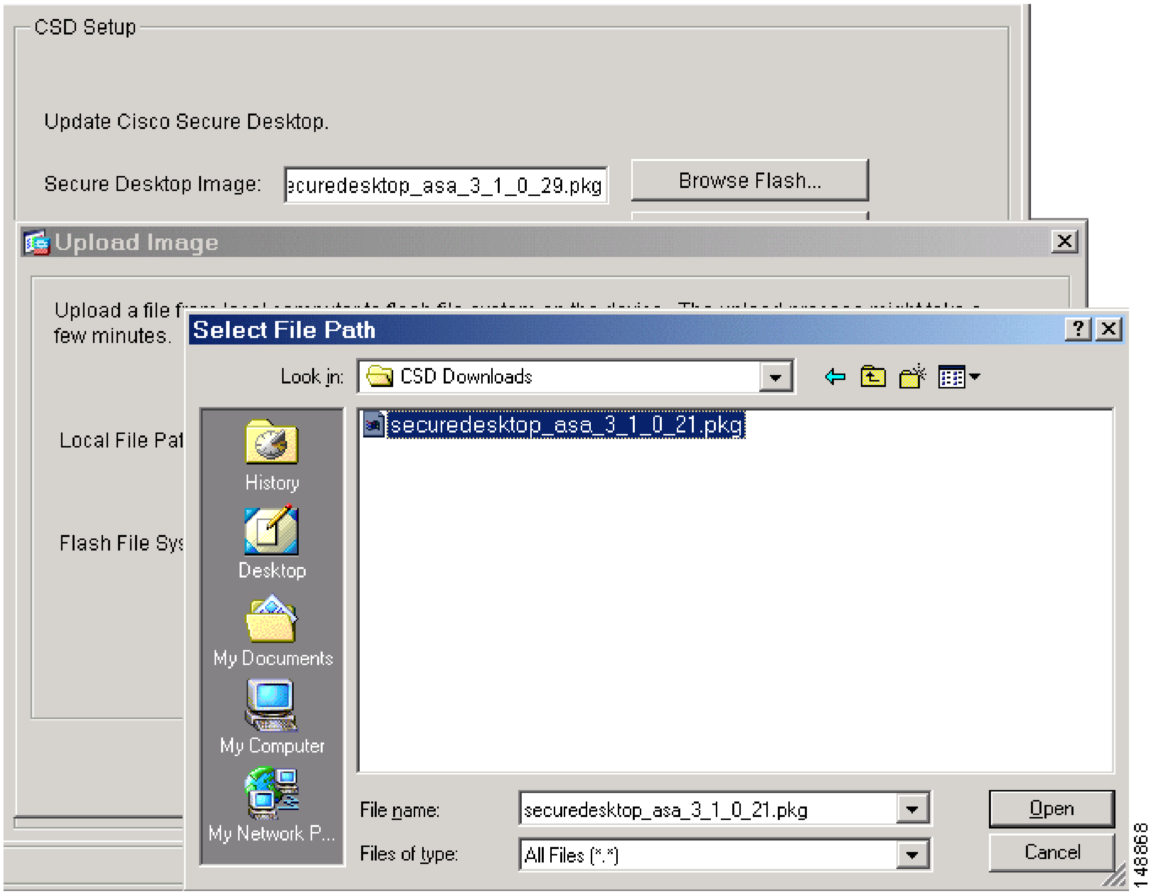
Step 5 Click **Upload** to prepare to transfer a copy of the CSD software from your local PC to the flash card installed in the ASA 5500.

ASDM opens the Upload Image dialog box.

Step 6 Click **Browse Local** to prepare to select the file on your local PC.

The Selected File Path dialog box displays the contents of the latest, local folder you accessed (Figure 1-3).

Figure 1-3 Select File Path (Upload Image)



CSD Setup

Update Cisco Secure Desktop.

Secure Desktop Image: ecuredesktop_asa_3_1_0_29.pkg

Upload Image

Upload a file f
few minutes.

Select File Path

Look in: CSD Downloads

securedesktop_asa_3_1_0_21.pkg

File name: securedesktop_asa_3_1_0_21.pkg

Files of type: All Files (*.*)

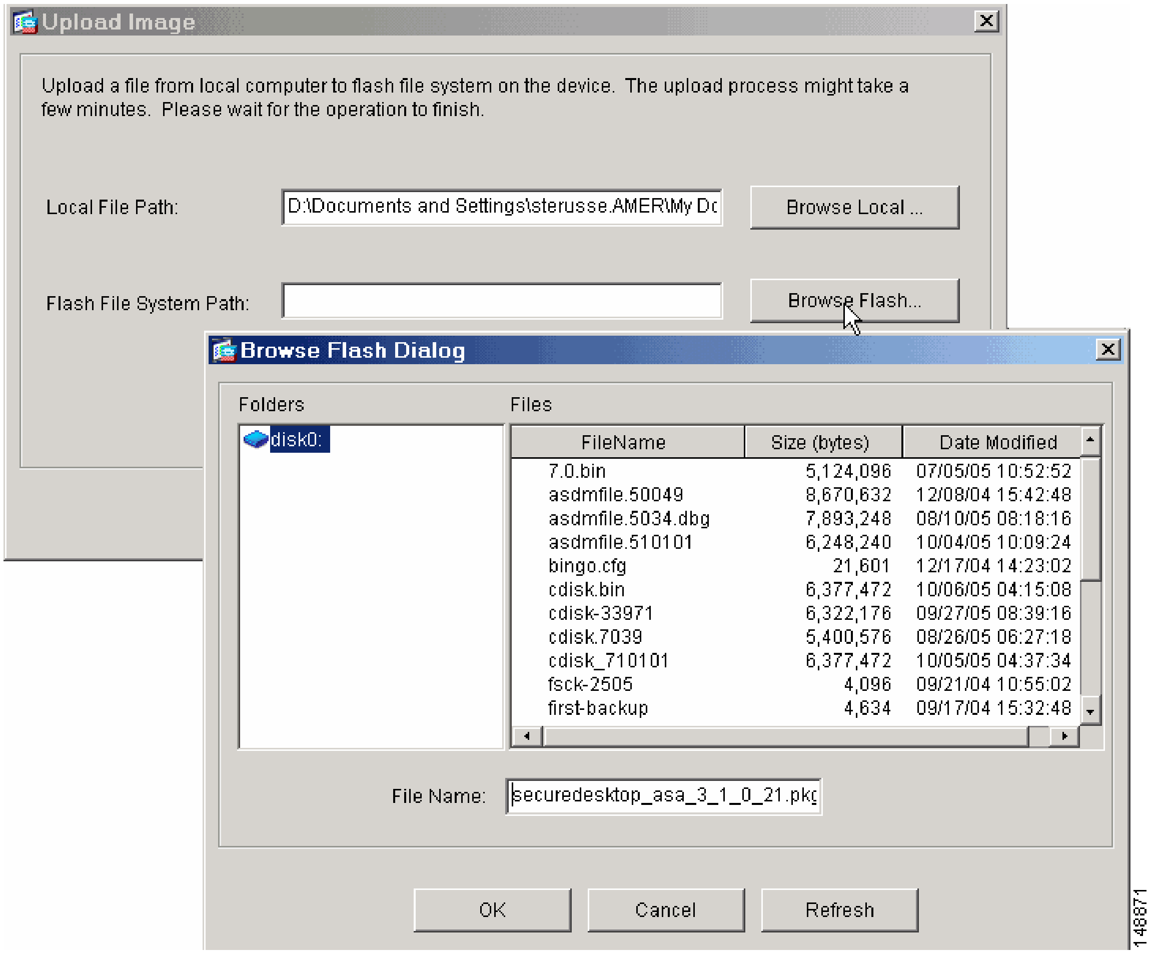
Step 7 Choose the **securedesktop_asa_<*n*>_<*n*>*.pkg** you downloaded in Step 1 and click **Open**.

ASDM closes the Select File Path dialog box and displays the file in the Local File Path field.

Step 8 Click Browse Flash to specify the target directory for the file.

Step 9 The Browse Flash Dialog box displays the contents of the flash card (Figure 1-4).

Figure 1-4 Browse Flash Dialog



Upload a file from local computer to flash file system on the device. The upload process might take a few minutes. Please wait for the operation to finish.

Local File Path: D:\Documents and Settings\sterusse.AMER\My Dc

Flash File System Path:

FileName	Size (bytes)	Date Modified
7.0.bin	5,124,096	07/05/05 10:52:52
asdmfile.50049	8,670,632	12/08/04 15:42:48
asdmfile.5034.dbg	7,893,248	08/10/05 08:18:16
asdmfile.510101	6,248,240	10/04/05 10:09:24
bingo.cfg	21,601	12/17/04 14:23:02
cdisk.bin	6,377,472	10/06/05 04:15:08
cdisk-33971	6,322,176	09/27/05 08:39:16
cdisk.7039	5,400,576	08/26/05 06:27:18
cdisk_710101	6,377,472	10/05/05 04:37:34
fsck-2505	4,096	09/21/04 10:55:02
first-backup	4,634	09/17/04 15:32:48

File Name: securedesktop_asa_3_1_0_21.pk

Note The File Name field at the bottom of the dialog box displays the target filename. By default, it matches the name of the source file you selected on your local PC. We recommend that you use the default name.

Step 10 (Optional) Choose the target folder in the Folders box.

Step 11 Click **OK**.

ASDM closes the Browse Flash Dialog box and displays the file in the Flash File System Path field.

Step 12 Click **Upload File** and click **OK**.

An Information dialog box displays the following message:

```
File is uploaded to flash successfully.
```

Step 13 Click **OK**.

ASDM closes the dialog box, transfers a copy of the file to the flash card, and removes the text from the fields in the Upload Image dialog box.

Step 14 Click **Close**.

The Use Uploaded Image dialog box displays the following message:

```
Use disk0:/securedesktop_asa_n_n.pkg as your new current image?
```

Step 15 Click **OK** to install the CSD software.

The Uninstall CSD dialog box opens if you upgraded from an earlier version of CSD, and displays the following message:

```
Do you want to delete disk0:securedesktop_asa_<Previous_Version>.pkg?
```

Step 16 Click **Yes** unless you want to keep the previous version.

ASDM closes the dialog box, revealing the installed image in the Secure Desktop Image field.

Refer to "Enabling and Disabling CSD" to continue.

CHAPTER 2

Enabling and Disabling CSD

You can use CLI or ASDM to enable or disable CSD. Refer to the section that names your preference.

- Using CLI to Enable or Disable CSD
- Using ASDM to Enable or Disable CSD

Using CLI to Enable or Disable CSD

Enabling CSD loads the CSD configuration file (data.xml) from the flash device to the running configuration. If you transfer or replace the data.xml file, disable and then enable CSD to load the file.

You can enter the following CLI command in privileged EXEC mode to display the status of the CSD image:

show webvpn csd

EXAMPLE

```
F1-asa1(config)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
```

Note Disabling CSD does not alter the CSD configuration.

Use the CLI to enable or disable CSD as follows:

Step 1 Log in to the CLI and enter the **config t** command.

Step 2 Enter **webvpn** to access the webvpn command mode.

For example,

```
F1-asa1(config)# webvpn
```

Step 3 Enter the following command to identify the disk that contains the securedesktop_asa_<*Version*>.pkg file and display the name of the that file.

For example,

```
F1-asa1(config-webvpn)# show disk all
-#- --length-- -----date/time------ path
  6 8543616    Nov 02 2005 08:25:36 PDM
  9 6414336    Nov 02 2005 08:49:50 cdisk.bin
 10 4634       Sep 17 2004 15:32:48 first-backup
 11 4096       Sep 21 2004 10:55:02 fsck-2451
 12 4096       Sep 21 2004 10:55:02 fsck-2505
 13 21601      Nov 23 2004 15:51:46 shirley.cfg
 14 9367       Nov 01 2004 17:15:34 still.jpg
 15 6594064    Nov 04 2005 09:48:14 asdmfile.510106.rls
 16 21601      Dec 17 2004 14:20:40 tftp
 17 21601      Dec 17 2004 14:23:02 bingo.cfg
 18 9625       May 03 2005 11:06:14 wally.cfg
 19 16984      Oct 19 2005 03:48:46 tomm_backup.cfg
 20 319662     Jul 29 2005 09:51:28 sslclient-win-1.0.2.127.pkg
 21 0          Oct 07 2005 17:33:48 sdesktop
 22 5352       Oct 28 2005 15:09:20 sdesktop/data.xml
 23 369182     Oct 10 2005 05:27:58 sslclient-win-1.1.0.133.pkg
 24 1836392    Oct 26 2005 09:15:26 securedesktop_asa_3_1_0_24.pkg

38600704 bytes available (24281088 bytes used)

******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155

F1-asa1(config-webvpn)#
```

Step 4 To install the image, enter the following command:

```
csd image securedesktop_asa_<Version>.pkg
```

For example,

```
F1-asa1(config-webvpn)# csd image securedesktop_asa_3_1_0_25.pkg
```

Step 5 Enter one of the following commands:

- **csd enable** to enable CSD
- **no csd enable** to disable CSD

For example,

```
F1-asa1(config-webvpn)# csd enable
F1-asa1(config-webvpn)#
```

Step 6 Enter **write memory** to save the running configuration.

For example,

```
F1-asa1(config-webvpn)# F1-asa1(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 71fa1950 45b7f82f 12b4e7c1 934111bb
```

```
15585 bytes copied in 3.710 secs (5195 bytes/sec)
[OK]
F1-asa1(config-webvpn)#
```

Using ASDM to Enable or Disable CSD

Enabling CSD loads the CSD configuration file (data.xml) from the flash device to the running configuration. If you transfer or replace the data.xml, disable and then enable CSD to load the file.

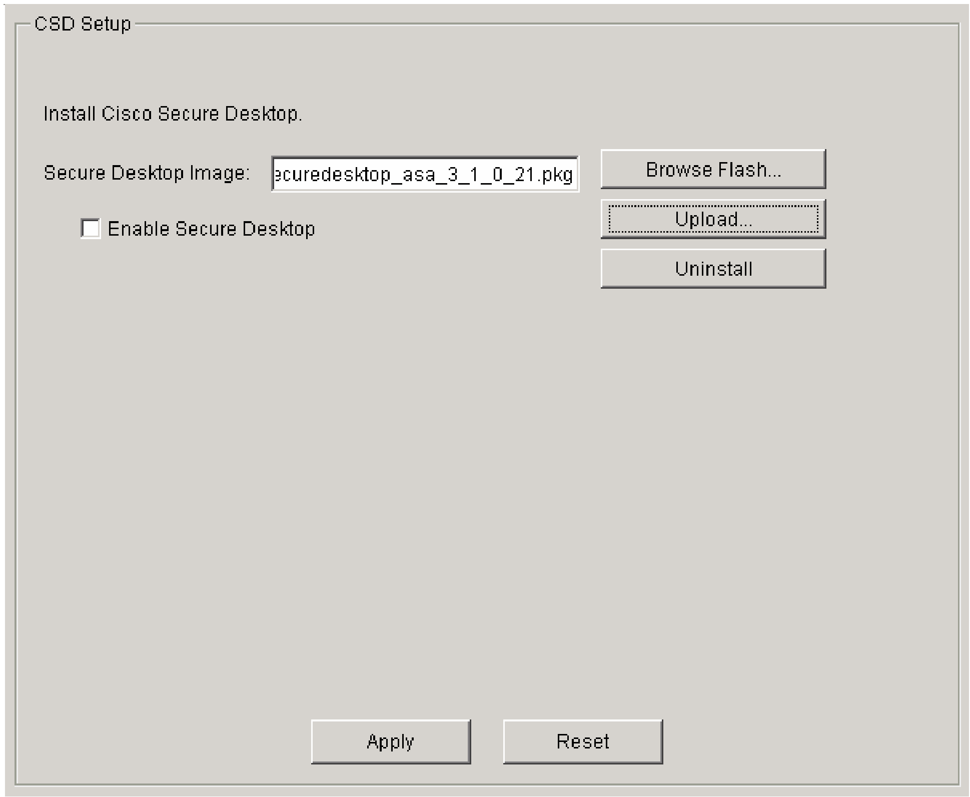
Disabling CSD does not alter the CSD configuration.

Use ASDM to enable or disable CSD as follows:

Step 1 Choose **Configuration** > **VPN** > **WebVPN** > **CSD Setup**.

The CSD Setup pane opens (Figure 2-1).

Figure 2-1 CSD Setup (Enable/Disable)



CSD Setup

Install Cisco Secure Desktop.

Secure Desktop Image: ecuredesktop_asa_3_1_0_21.pkg

□ Enable Secure Desktop

Note The Secure Desktop Image field displays the image (and version) that is currently installed. The Enable Secure Desktop check box indicates whether CSD is enabled.

Step 2 Check or uncheck **Enable Secure Desktop** and click **Apply**.

ASDM enables or disables CSD.

CHAPTER 3

Introduction

The following sections describe the capabilities of Cisco Secure Desktop (CSD), introduce the Cisco Secure Desktop Manager (CSDM) interface, and describe how to save configuration changes:

- CSD Capabilities
- Navigation
- Saving and Resetting the Running CSD Configuration

CSD Capabilities

CSD seeks to minimize the risk of information being left after an SSL VPN session terminates. CSD's goal is to reduce the possibility that cookies, browser history, temporary files, and downloaded content will not remain on a system after a remote user logs out or an SSL VPN session times out. CSD encrypts data and files associated with, or downloaded, during the SSL VPN session.

The protection provided by CSD is valuable in case of an abrupt session termination, or if a session times out due to inactivity. Furthermore, CSD stores session information in the secure vault desktop partition; when the session closes, CSD overwrites and attempts to remove session data using a U.S. Department of Defense (DoD) sanitation algorithm to provide endpoint security protection.

CSD allows full customization of when and where it is downloaded. It supports profiles of network element connection types (corporate laptop, home PC, or Internet kiosk) and applies a different security policy to each type. These policies include *System Detection*, which is the definition, enforcement, and restoration of client security in order to secure enterprise networks and data. You can configure System Detection to confirm the presence of the CSD modules Secure Desktop or Cache Cleaner; and antivirus software, antispyware software, personal firewall software, and/or the Microsoft® Windows operating system and service packs on the user's computer as conditions for enabling particular features.

Cisco SSL VPN solutions provide organizations with robust and flexible products for protecting the security and privacy of information, and can play an important part in an organization's compliance strategies. No single technology today addresses all security requirements under the proposed standards. In addition, given limitations of the Microsoft operating system, no technology that interoperates with the operating system can ensure the total removal of all data, especially from an untrusted system with potentially malicious third party software installed. However, deployments of Cisco SSL VPN using CSD, when combined with other security controls and mechanisms within the context of an effective risk management strategy and policy, can help to reduce risks associated with using such technologies.

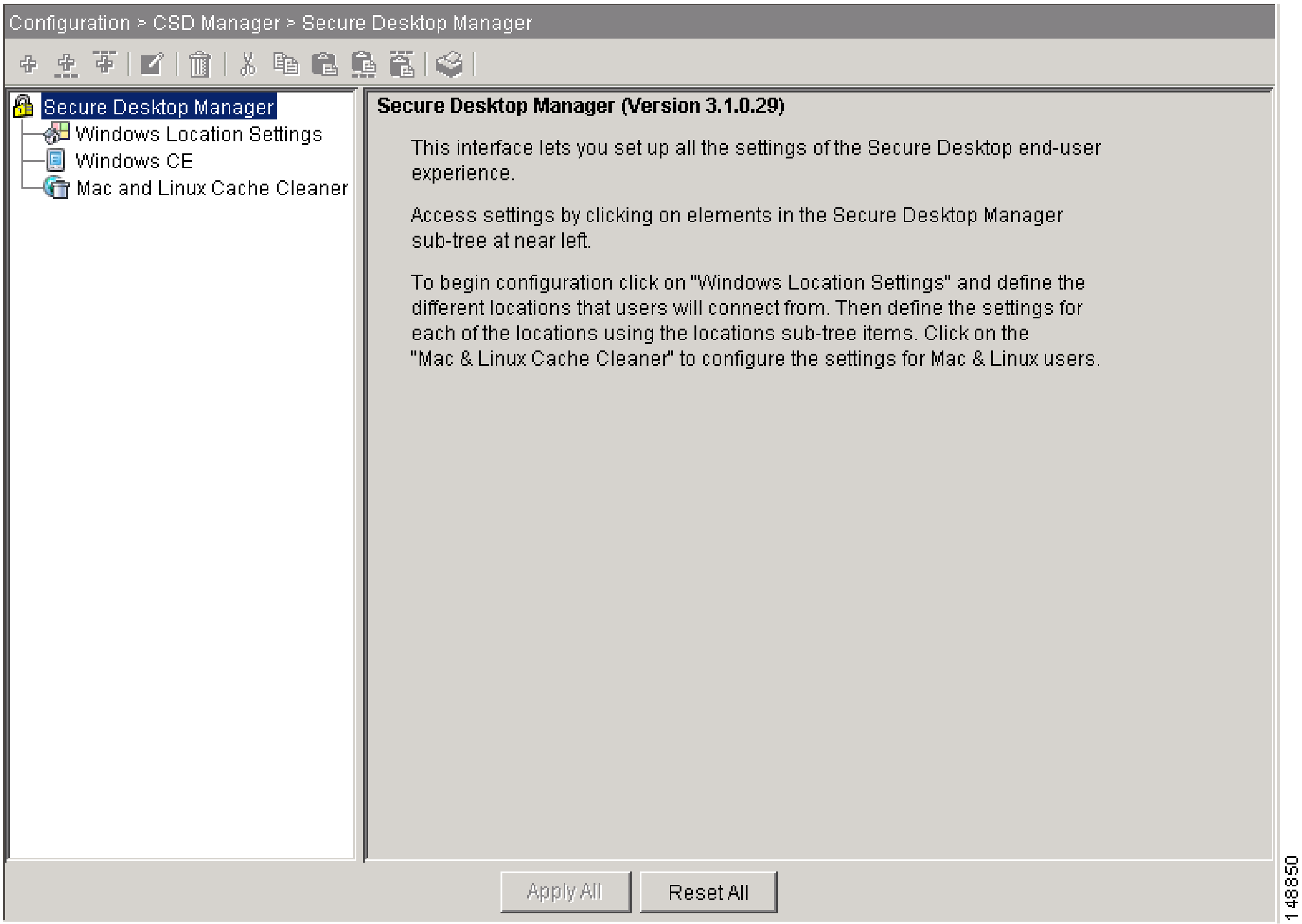
Navigation

To access the Secure Desktop Manager to configure CSD for remote clients, choose **Configuration** > **CSD Manager** > **Secure Desktop Manager**.

The Secure Desktop Manager pane opens.

Figure 3-1 shows the default menu and the Secure Desktop Manager pane.

Figure 3-1 Secure Desktop Manager (Initial)



Configuration > CSD Manager > Secure Desktop Manager
Secure Desktop Manager
Windows Location Settings
Windows CE
Mac and Linux Cache Cleaner
Apply All
Reset All
148850

Secure Desktop Manager (Version 3.1.0.29)

This interface lets you set up all the settings of the Secure Desktop end-user experience.

Access settings by clicking on elements in the Secure Desktop Manager sub-tree at near left.

To begin configuration click on "Windows Location Settings" and define the different locations that users will connect from. Then define the settings for each of the locations using the locations sub-tree items. Click on the "Mac & Linux Cache Cleaner" to configure the settings for Mac & Linux users.

The following initial options are available in the CSDM menu:

- Windows Location Settings — Click to create a group of settings for Windows clients connecting from a particular type of location, such as Work, Home, or Insecure. Once you create a location, you can specify how to determine that clients are connecting from that particular location. For example, clients with DHCP-assigned IP addresses within a corporate address range connect from the Work location.

  After you create a location, you can configure the VPN Feature Policy, Keystroke Logger, Cache Cleaner, and Secure Desktop features for that location.

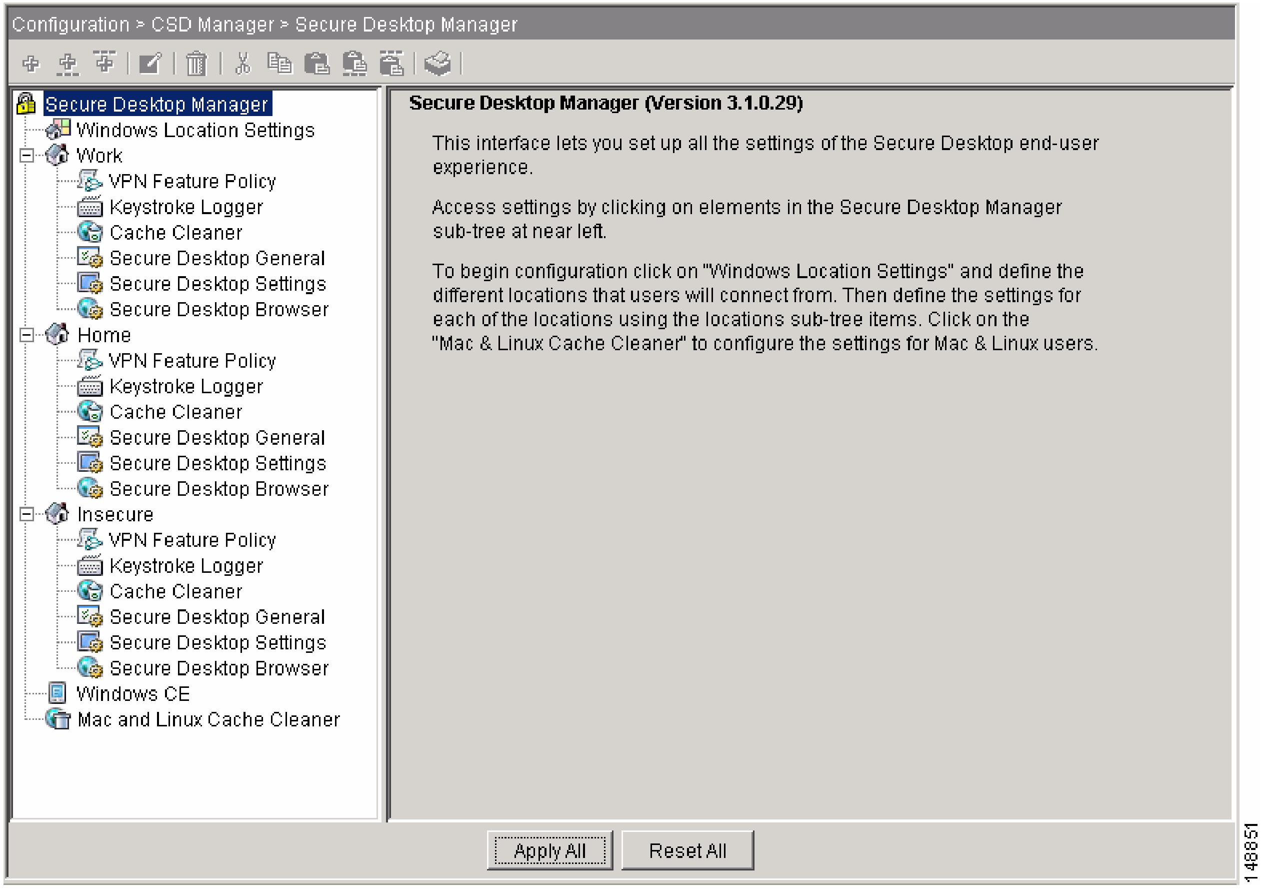
- Windows CE — Click to enable or restrict web browsing and file access for Windows CE clients. CSD does not support location entries for Windows CE clients, but does let you enable or restrict web browsing and remote server file access for them.
- Mac & Linux Cache Cleaner — Click to configure the Cache Cleaner and a VPN Feature Policy (enable or restrict web browsing, remote server file access, and port forwarding) for Macintosh and Linux clients.

Note *Port forwarding* permits the use of the Secure Desktop to connect a client application installed on the local PC to the TCP/IP port of a peer application on a remote server.

CSD does not support location entries for Macintosh and Linux clients; however, it does support a limited set of security features for these platforms.

Figure 3-2 shows a CSD menu populated with locations.

Figure 3-2 Navigating the Secure Desktop Manager



Secure Desktop Manager (Version 3.1.0.29)

This interface lets you set up all the settings of the Secure Desktop end-user experience.

Access settings by clicking on elements in the Secure Desktop Manager sub-tree at near left.

To begin configuration click on "Windows Location Settings" and define the different locations that users will connect from. Then define the settings for each of the locations using the locations sub-tree items. Click on the "Mac & Linux Cache Cleaner" to configure the settings for Mac & Linux users.

A *location* is a security profile you can assign to Microsoft Windows clients as they connect to the corporate network. (Locations apply to Microsoft Windows users only.) As an administrator, you specify the criteria to match the client to the location. Eligible matching criteria include certificate name and authority, IP address range, and local file or registry requirements. Each location also contains a set of user access rights. For example, as an administrator, you might configure a secure location to provide full access rights – web browsing, remote server file access, port forwarding, and full VPN tunneling – but limit an insecure location to web browsing.

Windows locations allow deployment of the Secure Desktop functions on a location-specific basis. Typical location types include Work, Home, and Insecure (for such client connection sites as an Internet cafe). You can use Secure Desktop Manager to define as many locations as needed. Each location has its own settings and options that make up its security profile.

When you add a location to the configuration, the Desktop Manager displays the name of the location in the menu, and displays the following options for configuring privileges and restrictions for that location only:

- VPN Feature Policy—Provides System Detection before allowing the following remote access functions: web browsing, remote server file access, port forwarding, and full tunneling using the SSL VPN Client. It can require and verify the presence of certain safeguards such as antivirus software, antispyware software, firewall software, and the operating system version and patch.
- Keystroke Logger—Scans the client PC for a keystroke logging application. You can configure a location type to require a scan for keystroke logging applications on the client PC. You can list the keystroke logging applications that are safe or let the remote user approve of the applications the scan identifies. Secure Desktop and Cache Cleaner launch only if the scan is clear, or only if you assign administrative control to the user and the user approves of the applications the scan identifies. Cisco Secure Desktop may be unable to detect every potentially malicious keystroke logger, including but not limited to hardware keystroke logging devices.
- Cache Cleaner—Attempts to disable or erase data that a user downloaded, inserted, or created in the browser, including cached files, configuration changes, cached browser information, passwords entered, and auto-completed information. The Cache Cleaner works with Microsoft Internet Explorer 5.0 or later on Windows 98, ME, NT 4, 2000, and XP; Internet Explorer 5.2 or later, or Safari 1.0 or later, on Macintosh (MacOS X); and Mozilla 1.1 or later on Red Hat Linux v9.
- Secure Desktop General—Provides an encrypted space for Windows 2000 and Windows XP users, within which the user has an online session using a browser. It is transparent, requiring only a browser for access. The Secure Desktop does not encrypt or clean system memory information, including that which may be left on the disk by the operating system in the Windows virtual memory file, commonly referred to as the paging file. There may also be instances where, if local printing is permitted, that data can remain in the local system print spool. CSD does provide an option that seeks to disable printing from within a CSD session.
- Secure Desktop Settings—Lets you place restrictions on the Secure Desktop.
- Secure Desktop Browser—Specifies the home page to which the browser connects when the remote user establishes a CSD session. This option also lets you specify the folders and bookmarks (or “favorites”) to insert into the respective browser menu during the CSD session.

Saving and Resetting the Running CSD Configuration

CSD saves all CSD configuration data to disk0:/sdesktop/data.xml.

Note To copy the configuration settings from one security appliance to another, transfer a copy of the disk0:/sdesktop/data.xml file to the flash device of the target security appliance. Disable and reenable CSD to read the disko:/sdesktop/data.xml file into the running CSD configuration.

CSD displays two buttons at the bottom of the CSD panes that interact with the disk0:/sdesktop/data.xml file. Use these buttons as follows:

- To save the running CSD configuration to the data.xml file, click **Apply All**.
- To overwrite all settings in the running CSD configuration with those stored in the data.xml file, click **Reset All**.

CHAPTER 4

Tutorial

CSD is a highly customizable suite of security tools that you can deploy in many different ways to secure remote systems and enforce your company's network security polices. Becoming familiar with the configuration procedure can help you understand the following:

- How to deploy CSD
- Which security decisions you need to make to best accommodate your users and secure your network

Note This tutorial introduces you to the CSD configuration settings. Subsequent sections reinforce the instructions with detailed descriptions.

The following sections guide you through the CSD configuration sequence:

- Step One: Define Windows Locations
- Step Two: Define Windows Location Identification
- Step Three: Configure Windows Location Modules
- Step Four: Configure Windows Location Features
- Step Five: Configure Windows CE Features
- Step Six: Configure Macintosh and Linux Features

Step One: Define Windows Locations

Begin configuring CSD by defining Windows locations. Windows locations apply to supported Microsoft Windows clients only; they do not apply to Windows CE, Macintosh, and Linux clients.

Locations let you deploy an appropriately secure environment to hosts that connect through the VPN. They let you increase security on hosts that you determine are likely to be insecure, and offer flexibility to clients you determine are secure. You can restrict user privileges when they connect from unknown computers. You can also deploy the Secure Desktop and Cache Cleaner modules on insecure hosts to minimize session information that might contain confidential company information. We recommend that you consider the different types of hosts that will connect through the VPN before you determine the criteria needed to secure those hosts and the security policies to assign to those criteria. In addition, because it is physically impossible to ensure 100 percent removal of all data sent to a remote system, organizations may use Cisco Secure Desktop to minimize access to trusted assets.

This tutorial describes how to configure three example locations: “Work,” “Home,” and “Insecure.” “Work” is for those connecting to the VPN from a workstation in the office, “Home” is for those working from home, and “Insecure” is for those who do not meet the criteria for either, such as those connecting from a cybercafé.

In this tutorial, “Work” provides clients with full access, “Home” provides some flexibility, and “Insecure” restricts access. This tutorial defines the locations as follows:

- Work
  - Identified by a registry entry
  - Secure Desktop and Cache Cleaner are disabled
  - Full access: all features ON
- Home
  - Identified by a certificate given by the administrator
  - Secure Desktop and Vault Reuse are enabled, with no timeout

    Vault Reuse lets users close the Secure Desktop and open it again at a later time, creating a persistent desktop that is available from one session to the next. If you enable this option, users must enter a password (up to 127 characters in length) when CSD creates the Secure Desktop.
  - Advanced features require company antivirus software, company antispyware, company firewall, and Windows 2000 Service Pack 4 or Windows XP
  - Check for keystroke logger
- Insecure
  - No identification
  - Cache Cleaner
  - All features disabled except web browsing

To create the three locations:

Step 1 Choose **Windows Location Settings** in the CSD menu.

The Windows Location Settings pane appears.

Step 2 Type the following names in the **Location name** field, and click **Add** after typing each one:

- `Work`
- `Home`
- `Insecure`

CSD evaluates client connections against the location entries in the order listed on the Windows Location Settings pane. CSD grants privileges to a client PC based on the first location definition it matches. Our example includes “Work,” “Home,” and “Insecure” in that order; to assign privileges to a host, CSD first determines whether it is a “Work” host. If it is not, it determines whether it is a “Home” host. If it is not, it assigns the privileges associated with the “Insecure” location.

To change the order of the evaluation, choose a location name and click **Move Up** or **Move Down**.

Click **Apply All** to save the running CSD configuration to the flash device.

Note An "Unapplied Changes" dialog box prompts you to save the CSD configuration if you try to navigate away from it or exit without having saved the configuration. Clicking **Apply Changes** in that window is equivalent to clicking the Apply All button.

Step Two: Define Windows Location Identification

For each Windows location, define the criteria used to identify the location and the security modules to be deployed for that location. Specify this information by clicking on the location name in the menu on the left side of the CSD Manager. An Identification pane lets you enable the identification criteria for the location: certificate, IP address range, and file/registry. The "Use Module" attribute at the bottom of the pane lets you enable or disable the Secure Desktop or Cache Cleaner modules for the associated location.

Work

Identify clients in the "Work" location by registry entry as follows:

Step 1 Click the name **Work** in the menu on the left.

The Identification pane opens.

Step 2 Check **Enable identification using Registry or File criteria**.

Step 3 Add a registry criteria such as, "HKEY_LOCAL_MACHINE\SOFTWARE\Company exists."

Step 4 Do not deploy a security module because the hosts in this location are inside the office; uncheck both **Secure Desktop** and **Cache Cleaner** next to "Use Module."

Home

Identify clients in the "Home" location by a certificate given by the administrator to users who connect from home, as follows:

Step 1 Click the name **Home** in the menu on the left.

Step 2 Check **Enable identification using certificate criteria**.

Step 3 Complete the **Issued to** and **Issued By** fields of the certificate.

Step 4 Check **Secure Desktop** next to "Use Module."

Insecure

Do not specify any criteria for the final location entry, “Insecure.” It applies to all clients that do not match the criteria specified in the previous location entries. Enable the Cache Cleaner module for these clients, as follows:

Step 1 Click the name **Insecure** in the menu on the left.

Step 2 Check **Cache Cleaner** next to “Use Module.”

Click **Apply All** to save the running CSD configuration to the flash device.

Step Three: Configure Windows Location Modules

This section describes how to customize the CSD deployment for each location. Each location in the menu has six options: VPN Feature Policy, Keystroke Logger, Cache Cleaner, Secure Desktop General, Secure Desktop Settings, and Secure Desktop Browser.

If you selected **Cache Cleaner** next to “Use Module” in the location configuration, configure the Cache Cleaner. If you selected **Secure Desktop**, configure both the Secure Desktop and Cache Cleaner because CSD supports only the Cache Cleaner on Windows 98 machines.

Work

Because you assigned neither the Secure Desktop and Cache Cleaner security modules to the location entry named “Work,” do not configure the associated VPN Feature Policy, Keystroke Logger, Cache Cleaner, Secure Desktop General, Secure Desktop Settings, and Secure Desktop Browser settings.

Home

Use the Secure Desktop for the “Home” location and allow vault reuse, no timeout, access to printing, and the command prompt. Also, allow connections using the Cache Cleaner for Windows 98 hosts. Set up the “Home” location with these settings as follows:

Step 1 Click **Cache Cleaner** under “Home.”

The Cache Cleaner pane opens.

Step 2 Uncheck **Launch cleanup upon inactivity timeout**.

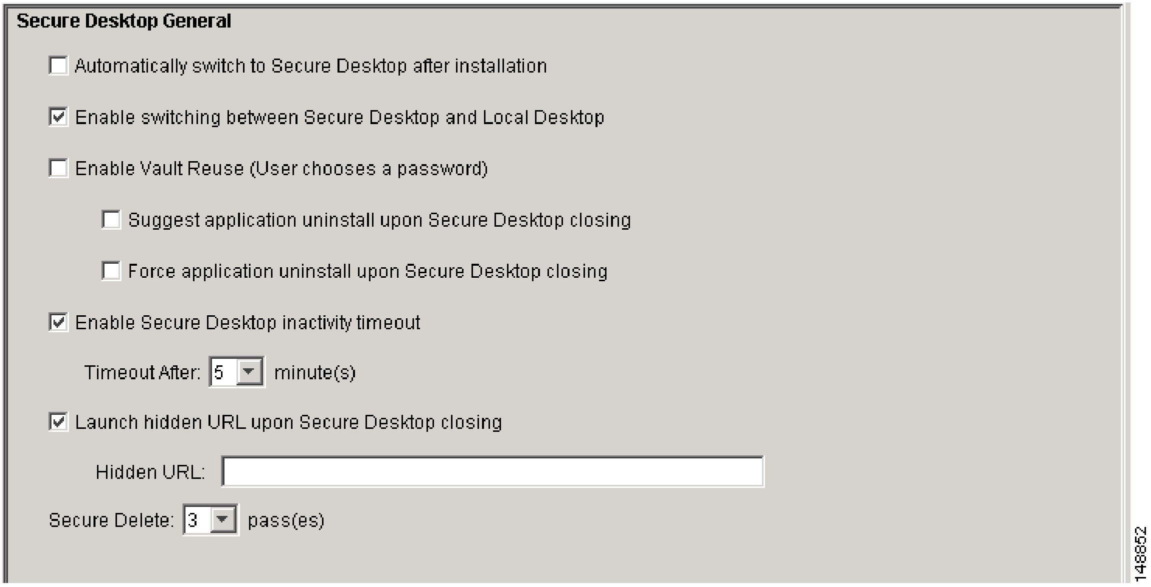
Step 3 Uncheck **Disable cancellation of cleaning**.

See the option descriptions in “Configuring Cache Cleaner for a Location” for more information about the settings on this pane.

Step 4 Click **Secure Desktop General** under “Home.”

The Secure Desktop General pane appears (Figure 4-1).

Figure 4-1 Secure Desktop General



Secure Desktop General

□ Automatically switch to Secure Desktop after installation

☑ Enable switching between Secure Desktop and Local Desktop

□ Enable Vault Reuse (User chooses a password)

□ Suggest application uninstall upon Secure Desktop closing

□ Force application uninstall upon Secure Desktop closing

☑ Enable Secure Desktop inactivity timeout

Timeout After: 5 minute(s)

☑ Launch hidden URL upon Secure Desktop closing

Hidden URL:

Secure Delete: 3 pass(es)

Step 5 Check **Enable switching between Secure Desktop and Local Desktop**.

Step 6 Check **Enable Vault Reuse**.

Step 7 Uncheck **Enable Secure Desktop inactivity timeout**.

With this attribute unchecked, the timeout has no effect.

See the option descriptions in "Configuring Secure Desktop General for a Location" for more information about the settings on this pane.

Step 8 Click **Secure Desktop Settings** under "Home."

The Secure Desktop pane appears.

Uncheck all options except for **Allow e-mail applications to work transparently**.

See the option descriptions in "Configuring Secure Desktop Settings for a Location" for more information about the settings on this pane.

Insecure

Use the default Cache Cleaner settings for the "Insecure" location. Assign or confirm the associated Cache Cleaner settings as follows:

Step 1 Click **Cache Cleaner** under "Insecure."

The Cache Cleaner pane appears.

Step 2 Check **Launch cleanup upon inactivity timeout**.

When checked, this option forces a timeout if the user leaves the computer without logging out.

Step 3 Set **Timeout after** to **5 minutes**.

Click **Apply All** to save the running CSD configuration to the flash device.

Step Four: Configure Windows Location Features

CSD creates security modules for each location when you create it. Refer to the following sections to specify the level of access for each location.

Work

Provide full access to users in the “Work” location as follows:

Step 1 Click **VPN Feature Policy** under “Work.”

Step 2 Set the following attributes to **ON** to ensure users connecting from the office environment have access to all of the VPN features:

- **Web Browsing**
- **File Access**
- **Port Forwarding**
- **Full Tunneling**

Home

Users connecting from home have advanced features like File Access, Port Forwarding, and Full Tunneling only if they meet the company network policies for antivirus software, antispyware, firewall software, and Windows 2000 Service Pack 4 or Windows XP. Provide users in the “Home” location with this level of access as follows:

Step 1 Click **VPN Feature Policy** under “Home.”

Step 2 Set **Web Browsing** to **ON**.

Step 3 Set **File Access** to **ON if criteria are matched**.

Step 4 Click the ellipsis (**...**) button under “Web Browsing.”

A dialog box opens.

Step 5 Check **AntiVirus** and choose the antivirus software.

Note To choose multiple options for a given field, Control-click them.

Step 6 Check **Anti-spyware** and choose the antispyware software.

Step 7 Check **Firewall** and choose the firewall software.

Step 8 Check **OS** and choose **2000 SP4**, **XP no SP**, **XP SP1**, and **XP SP2**.

Step 9 Click **OK**.

Step 10 Repeat Steps 3 to 9 for **Port Forwarding** and **Full Tunneling**.

Insecure

These instructions grant web browsing access only, and only if the Secure Desktop is active. Provide this level of access to users in the "Insecure" location as follows:

Step 1 Click **VPN Feature Policy** under "Insecure."

Step 2 Set **Web Browsing** to **ON if criteria are matched**.

Step 3 Click the ellipses (**...**) button under "Web Browsing."

A dialog box opens.

Step 4 Check **AntiVirus** and choose the antivirus software.

Note To choose multiple options for a given field, Control-click them.

Step 5 Check **Firewall** and choose the company firewall software.

Step 6 Check **Anti-spyware** and choose the antispyware software.

Step 7 Check **OS** and choose **2000 SP4**, **XP no SP**, **XP SP1**, and **XP SP2**.

Step 8 Check **Feature** and choose **Cache Cleaner**.

Step 9 Click **OK**.

Step 10 Make sure **File Access**, **Port Forwarding**, and **Full Tunneling** are unchecked.

Step 11 Click **OK**.

See the option descriptions in "Configuring a VPN Feature Policy for a Location" for more information.

Click **Apply All** to save the running CSD configuration to the flash device.

Step Five: Configure Windows CE Features

CSD provides limited features and restrictions for Windows CE clients. The following instructions explain how to grant or restrict web browsing and file access privileges to these clients.

Configure CSD for Windows CE clients as follows:

Step 1 Click **Windows CE**.

The Windows CE pane appears.

Step 2 Set **Web Browsing** to **ON**.

Step 3 Set **File Access** to **ON**.

See the option descriptions in "Setting Up CSD for Microsoft Windows CE Clients" for more information about the settings in this window.

Click **Apply All** to save the running CSD configuration to the flash device.

Step Six: Configure Macintosh and Linux Features

CSD handles Macintosh and Linux systems differently from Windows. Instead of using different settings per location, all Macintosh and Linux hosts use the same settings. (Hosts connecting from both secure and insecure locations connect with the same settings.) The following instructions explain how to grant only web browsing access privileges with a global timeout.

Configure the Macintosh and Linux cache cleaner as follows:

Step 1 Click **Mac & Linux Cache Cleaner**.

The Cache Cleaner - Mac & Linux pane appears.

Step 2 Check **Launch cleanup upon global timeout**.

Step 3 Set the **Timeout after** value to **5 minutes**.

Step 4 Check **Let user reset timeout**.

Step 5 Set **Web Browsing** to **ON**.

Step 6 Set **File Access** to **ON**.

Step 7 Set **Port Forwarding** to **OFF**.

See the option descriptions in "Setting Up CSD for Macintosh and Linux Clients" for more information about the settings in this window.

Click **Apply All** to save the running CSD configuration to the flash device.

Setting Up CSD for Microsoft Windows Clients

See the following sections to configure CSD for remote clients running Microsoft Windows:

- Creating Windows Locations
- Defining Location Criteria
- Configuring the Secure Desktop for Clients that Match Location Criteria

Creating Windows Locations

Windows locations let you determine how clients connect to your virtual private network, and protect it accordingly.

For example, clients connecting from within a workplace LAN on a 10.*x.x.x* network behind a NAT device are an unlikely risk for exposing confidential information. For these clients, you might set up a CSD Windows Location named Work that is specified by IP addresses on the 10.*x.x.x* network, and disable both the Cache Cleaner and the Secure Desktop function for this location.

In contrast, users' home PCs might be considered more at risk to viruses due to their mixed use. For these clients, you might set up a location named Home that is specified by a corporate-supplied certificate that employees install on their home PCs. This location would require the presence of antivirus software and specific, supported operating systems to grant full access to the network.

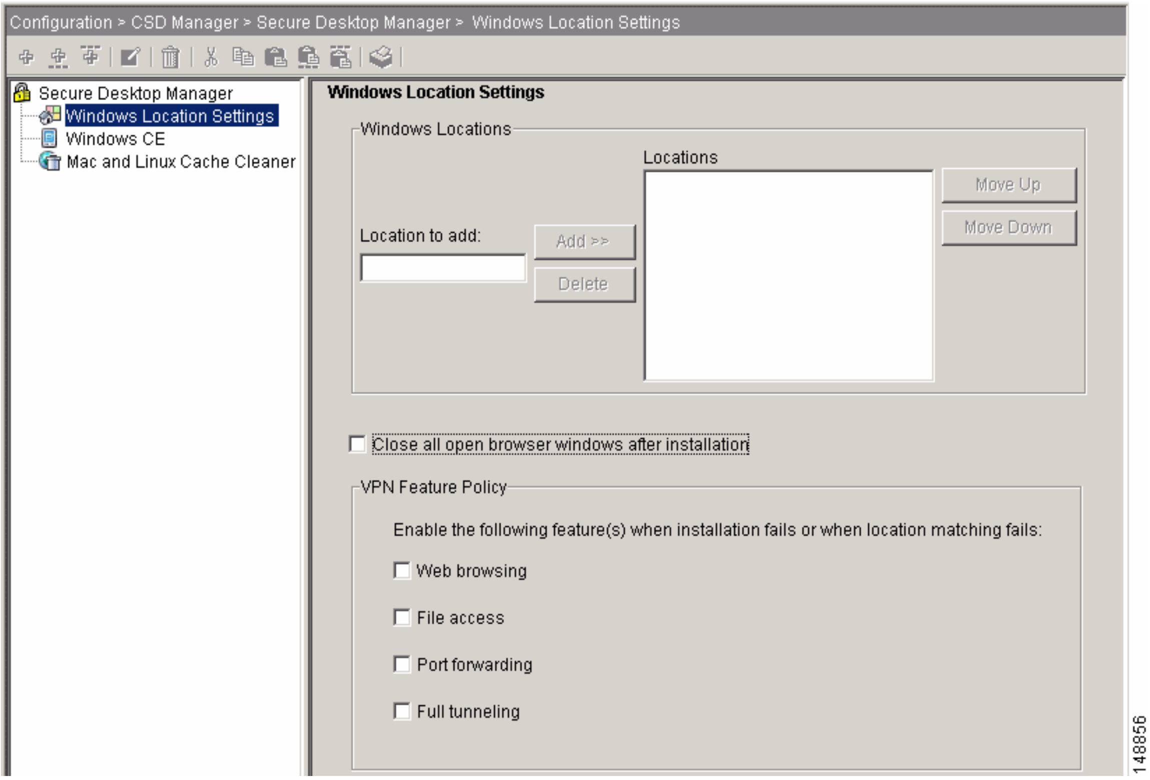
Finally, for untrusted locations such as Internet cafes, you might set up a location named "Insecure" that has no matching criteria (thus making it the default for clients that do not match other locations). This location would require full Secure Desktop functions, and include a short timeout period to prevent access by unauthorized users.

CSD evaluates remote client PCs against the locations in the order listed on the Windows Location Settings pane, and grants privileges based on the first location definition that matches.

Examine the Windows Location attribute descriptions to plan a configuration that meets the security requirements of your network.

Click **Windows Location Settings** in the menu on the left to define the location-based settings (also called adaptive policies) for CSD. Figure 5-1 shows the default settings.

Figure 5-1 Windows Location Settings


Configuration > CSD Manager > Secure Desktop Manager > Windows Location Settings
Secure Desktop Manager
Windows Location Settings
Windows CE
Mac and Linux Cache Cleaner
Windows Location Settings
Windows Locations
Locations
Move Up
Move Down
Location to add:
Add >>
Delete
VPN Feature Policy
148856

□ Close all open browser windows after installation

Enable the following feature(s) when installation fails or when location matching fails:

□ Web browsing

□ File access

□ Port forwarding

□ Full tunneling

The elements on this pane are as follows:

- Location to add and Add button—To add a location from which users can connect, type a new location name in the Location to add field and click Add. As you add locations, the Secure Desktop Manager adds their names to the CSD menu and to the list of “Locations” on this pane.
- Delete—Select an entry in the Locations box and click Delete to discard it.
- Locations—Lists the locations in the CSD configuration. When a remote client PC connects, the Secure Desktop Installer attempts to match it to a location in the sequence shown in this box.

⚠

Caution If you create a location and do not specify criteria, make sure it is the last entry in the “Locations” list.

- Move Up and Move Down—Select an entry in the Locations box and click one of these buttons to change its priority.

  CSD evaluates clients against the locations in the order of their appearance in this list.
- Close all open browser windows upon installation—Check to remove unsecured web browser sessions from the client when CSD is installed. This option prevents confusion over whether CSD secures the data. This option applies to all Windows Locations.
- Web browsing—Check to let the remote user browse the web if the Secure Desktop installation fails or the remote client PC does not match any of the configured locations criteria. In the interest of security, we recommend that you do not check this option.

  By default, this attribute is unchecked.

- File access—Check to let the remote user access files on a remote server if the Secure Desktop installation fails or the remote client PC does not match any of the configured locations criteria. In the interest of security, we recommend that you do not check this option.

  By default, this attribute is unchecked.
- Port forwarding—Check to let the remote user connect a client application installed on the local PC to the TCP/IP port of a peer application on a remote server if the Secure Desktop installation fails or the remote client PC does not match any of the configured locations criteria. In the interest of security, we recommend that you do not check this option.

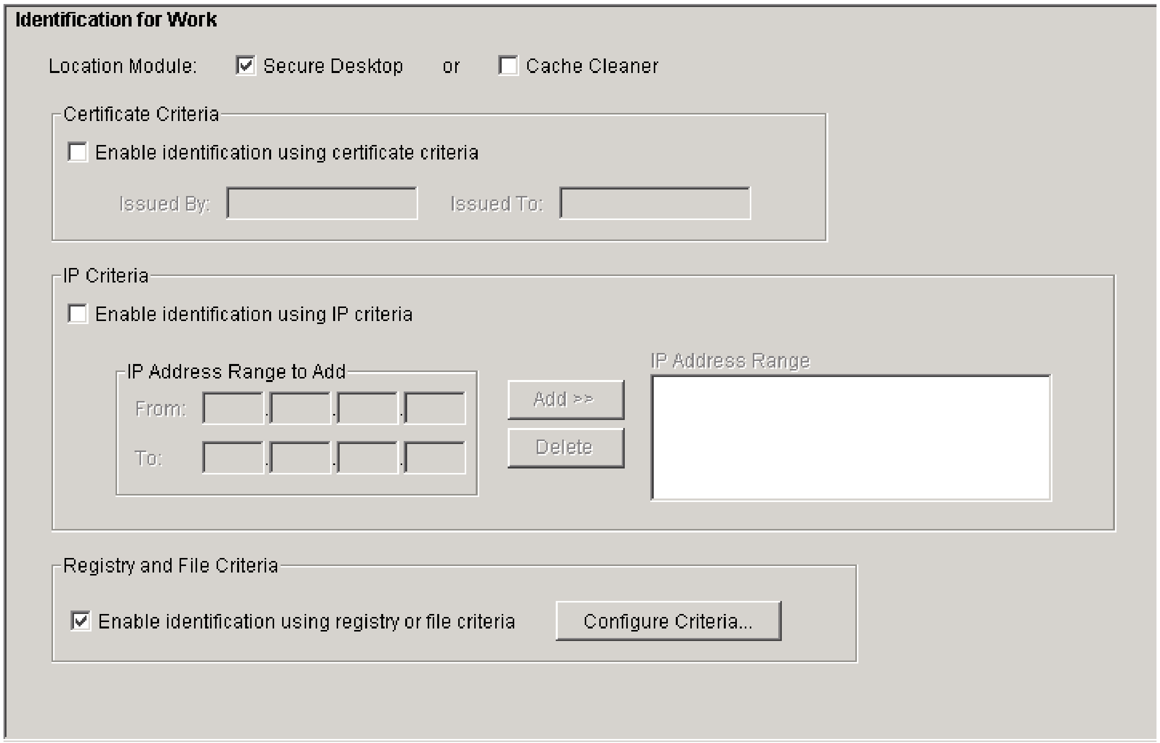
  By default, this attribute is unchecked.
- Full tunneling—Check to let the remote user establish a VPN tunnel with the SSL VPN Client if the Secure Desktop installation fails or the remote client PC does not match any of the configured locations criteria. In the interest of security, we recommend that you do not check this option.

  By default, this attribute is unchecked.

Defining Location Criteria

To configure the settings for a location, click the location name in the menu on the left. The Identification for <*Location*> pane appears (Figure 5-2).

Figure 5-2 Identification for <Location>



Identification for Work

Location Module: ☑ Secure Desktop or ☐ Cache Cleaner

Certificate Criteria

☐ Enable identification using certificate criteria

Issued By:
Issued To:

IP Criteria

☐ Enable identification using IP criteria

IP Address Range to Add

From:
To:

IP Address Range

Registry and File Criteria

☑ Enable identification using registry or file criteria

This pane lets you specify the criteria that define the location. A location can be based on any of the following matching criteria:

- Certificate name and issuer
- IP address range
- Presence or absence of a particular file or registry key.

Note To push the Secure Desktop to all remote client PCs regardless of their status, configure only one location and do not specify a certificate, IP address range, or file or registry criteria. This default location pushes the Secure Desktop to all computers from which users connect.

CSD considers the three location criteria in a logical "AND" relationship. For example, if you specify an IP address range under "Enable identification using IP criteria," and you specify "File company_software.exe #does exist#" under "Enable identification using File or Registry criteria," the client must meet both of these conditions to match the location.

Within each area in the pane, only one of the criteria you specify must match; that is, CSD considers the criteria in a logical "OR" relationship. For example, if you specify several files under "Enable identification using File or Registry criteria," only one of these files must be present.

Refer to the sections that name the location criteria you want to configure:

- Location Module
- Certificate Criteria
- IP Criteria
- Registry and File Criteria

Location Module

The Location Module attribute in the Identification for <*Location*> pane (Figure 5-2) permits one of the following options:

- Secure Desktop—Check if you want to require the Secure Desktop to be present on the remote client as a criterion for assigning this location entry.

  Note If you check Secure Desktop and configure the Secure Desktop settings, you should still configure the Cache Cleaner as well. The Cache Cleaner serves as a fall-back security solution for older Windows operating systems such as Windows 98, which the full Secure Desktop functions do not support.

- Cache Cleaner—Check if you want to require the Cache Cleaner to be present on the remote client as a criterion for assigning this location entry.
- Both Secure Desktop and Cache Cleaner—Leave unchecked to let CSD apply the configured VPN feature policy.

Certificate Criteria

Check **Enable identification using certificate criteria** in the Identification for <*Location*> pane (Figure 5-2) to specify values of a digital certificate on the remote client PC as a criterion for assigning the properties of the location to the remote client.

Note For information about setting up your server to work with client certificates, see the "Frequently Asked Questions" section on page A-1.

Use one of the following instructions to examine the certificate Subject and Issuer fields to identify the values to be completed in the "Issued By" and "Issued To" fields:

- Using a Certificate File to Specify Certificate Criteria
- Using a Signed File to Specify Certificate Criteria
- Using the Certificates in Your Store to Specify Certificate Criteria

Using a Certificate File to Specify Certificate Criteria

To specify certificate criteria if you have a certificate file (for example, a *.cer or *.pfx file),

Step 1 Double-click the certificate.

The Certificate window opens.

Step 2 Click the **Details** tab.

Step 3 Complete both of the fields in the "Certificate Criteria" area of the Identification for <*Location*> pane (Figure 5-2), as follows:

- **Issued By—**Click **Subject** in the Field column under the Details tab of the Certificate window. The area below the Field column displays the subordinate fields and values assigned to the Subject field of the certificate. The subordinate fields include such names as "CN" for common name, "O" for organization unit name, and "E" for e-mail address. Type the value of one of these subfields in the **Issued By** field on the Identification for <*Location*> pane to match it against the Subject field of the certificate.

Note Specify the value of the subfield. For example, type the value of the "O" field, not the "O" itself.

- **Issued To—**Click **Issuer** in the Field column under the Details tab of the Certificate window. The area below the Field column displays the subordinate fields and values assigned to the Issuer field of the certificate. The subordinate fields include such names as "CN" for common name, "O" for organization unit name, and "E" for e-mail address. Type the value of one of these subordinate fields in the **Issued To** field on the Identification for <*Location*> pane to match it against the Issuer field of the certificate.

CSD assigns the location to the client only if it has a certificate that contains *both* of the following, and only if it matches at least one criterion in each of the completed areas in the Identification for <*Location*> pane:

- Value in the Subject field that matches the value you specified in the "Issued By" field
- Value in the Issuer field that matches the value you specified in the "Issued To" field

Using a Signed File to Specify Certificate Criteria

To specify certificate criteria if you have a signed file (that is, the file is not a certificate file, but contains a certificate):

Step 1 Right click the file and choose **Properties**.

The Properties window opens.

Step 2 Click the **Digital Signatures** tab (which appears only if the file is signed).

Step 3 Click **Details**.

Step 4 Click **View Certificate**.

The Certificate window opens.

Step 5 Click the **Details** tab.

Step 6 Complete both of the fields in the "Certificate Criteria" area of the Identification for <*Location*> pane (Figure 5-2), as follows:

– **Issued By—**Click **Subject** in the Field column under the Details tab of the Certificate window. The area below the Field column displays the subordinate fields and values assigned to the Subject field of the certificate. The subordinate fields include such names as "CN" for common name, "O" for organization unit name, and "E" for e-mail address. Type the value of one of these subfields in the **Issued By** field on the Identification for <*Location*> pane to match it against the Subject field of the certificate.

Note Specify the value of the subfield. For example, type the value of the "O" field, not the "O" itself.

– **Issued To—**Click **Issuer** in the Field column under the Details tab of the Certificate window. The area below the Field column displays the subordinate fields and values assigned to the Issuer field of the certificate. The subordinate fields include such names as "CN" for common name, "O" for organization unit name, and "E" for e-mail address. Type the value of one of these subordinate fields in the **Issued To** field on the Identification for <*Location*> pane to match it against the Issuer field of the certificate.

CSD assigns the location to the client only if it has a certificate that contains *both* of the following, and only if it matches at least one criterion in each of the completed areas in the Identification for <*Location*> pane:

- Value in the Subject field that matches the value you specified in the "Issued By" field
- Value in the Issuer field that matches the value you specified in the "Issued To" field

Using the Certificates in Your Store to Specify Certificate Criteria

To specify certificate criteria if you have neither a certificate file nor a signed file, go to the certificates in your *store* (your computer) to retrieve the data you need, as follows:

Step 1 Open the **Control Panel**.

Step 2 Choose **Internet Options**.

Step 3 Click the **Content** tab.

Step 4 Click **Certificates**.

Step 5 Choose a certificate and click **View**.

The Certificate window opens.

Step 6 Click the **Details** tab.

Step 7 Complete both of the fields in the "Certificate Criteria" area of the Identification for <*Location*> pane (Figure 5-2), as follows:

- **Issued By—**Click **Subject** in the Field column under the Details tab of the Certificate window. The area below the Field column displays the subordinate fields and values assigned to the Subject field of the certificate. The subordinate fields include such names as "CN" for common name, "O" for organization unit name, and "E" for e-mail address. Type the value of one of these subfields in the **Issued By** field on the Identification for <*Location*> pane to match it against the Subject field of the certificate.

Note Specify the value of the subfield. For example, type the value of the "O" field, not the "O" itself.

- **Issued To—**Click **Issuer** in the Field column under the Details tab of the Certificate window. The area below the Field column displays the subordinate fields and values assigned to the Issuer field of the certificate. The subordinate fields include such names as "CN" for common name, "O" for organization unit name, and "E" for e-mail address. Type the value of one of these subordinate fields in the **Issued To** field on the Identification for <*Location*> pane to match it against the Issuer field of the certificate.

CSD assigns the location to the client only if it has a certificate that contains *both* of the following, and only if it matches at least one criterion in each of the completed areas in the Identification for <*Location*> pane:

- Value in the Subject field that matches the value you specified in the "Issued By" field
- Value in the Issuer field that matches the value you specified in the "Issued To" field

IP Criteria

Check **Enable identification using IP criteria** in the Identification for <*Location*> pane (Figure 5-2) to use the IP address of the remote client PC as a criterion for assigning a location to the remote client, then click **Add** to enter one or more IP address ranges.

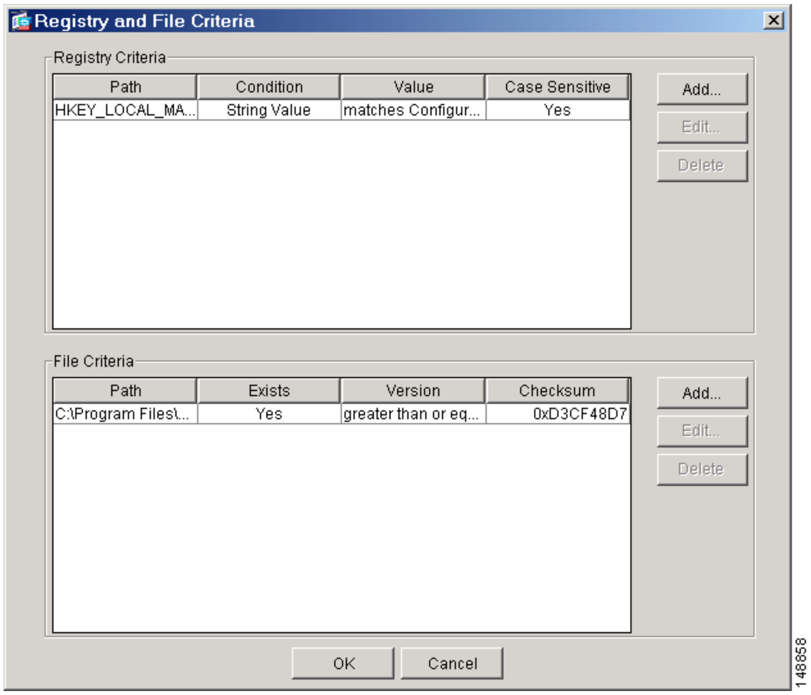
CSD checks the IP addresses of remote client PCs trying to connect. If a client has an address within the specified range, CSD assigns the properties of the location to the remote client.

Note If the client has more than one network card, CSD uses only the address of the first card detected.

Registry and File Criteria

Check **Enable identification using registry or file criteria** in the Identification for <*Location*> pane (Figure 5-2) if you want to specify registry key or file criteria to match to qualify a remote client PC to obtain the access rights associated with the location you are configuring, and click **Configure Criteria**. The Registry and File Criteria dialog box opens (Figure 5-3).

Figure 5-3 Registry and File Criteria



Registry Criteria

Path	Condition	Value	Case Sensitive
HKEY_LOCAL_MA...	String Value	matches Configur...	Yes

File Criteria

Path	Exists	Version	Checksum
C:\Program Files\...	Yes	greater than or eq...	0xD3CF48D7

The tables in this window list any registry key and file requirements needed to qualify a remote client to obtain the access rights associated with the location you are configuring. Each entry is a logical OR operator (that is, the evaluation result for any entry must be TRUE to assign the location.

Note To view details in the Registry Criteria or File Criteria tables, float the cursor over the column header divider. As you do so, it becomes a double, horizontal arrow. Drag the arrow to the left or right to expose the contents of the column.

Refer to the section that identifies the type of criteria you would like to configure:

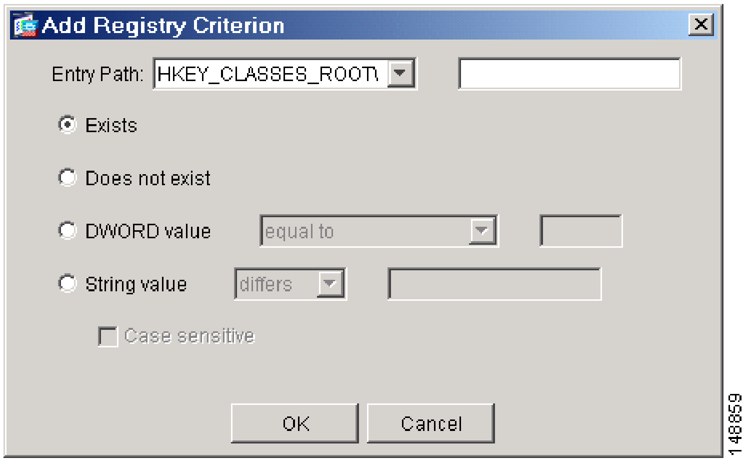
- Registry Criteria
- File Criteria

Registry Criteria

In the Registry Criteria area of the Registry and File Criteria dialog box (Figure 5-3), click **Add** if you want to confirm the presence or absence of a specific registry key as a criterion, or choose a criterion to be modified from the Registry Criteria area and click **Edit**.

The Add or Edit Registry Criterion dialog box opens. Figure 5-4 shows the Add Registry Criterion dialog box.

Figure 5-4 Add Registry Criterion



Entry Path: HKEY_CLASSES_ROOT\

● Exists

○ Does not exist

○ DWORD value equal to

○ String value differs

□ Case sensitive

Note You can use the value types to be specified in this window as a guide to set up one or more secret criteria within the remote client's system to match those specified for this location. For example, you can add a DWORD (double word, an unsigned 32-bit integer) value or string value to a registry key on client computers to qualify them for the location you are configuring.

Step 1 Assign values to the mandatory attributes in the Add or Edit Registry Criterion dialog box as follows:

- **Entry Path** menu—Choose the *hive*, the initial directory path of a registry key. The options are as follows:

```
HKEY_CLASSES_ROOT\
HKEY_CURRENT_USER\
HKEY_LOCAL_MACHINE\
HKEY_USERS\
```

  Each string references a registry base that stores different information. The `HKEY_LOCAL_MACHINE\` path is the most commonly used one because it contains the machine-specific registry files.

- **Entry Path** field—Enter the name of the registry key required to be present on or absent from the client system.

  Note Refer to the subsequent attribute descriptions for examples of Entry Path strings.

Step 2 Click one radio button from the following list and assign the associated values:

- **Exists**—Click if the mere presence of the named registry key on the remote client PC is sufficient to match the location you are configuring.

EXAMPLE Click **Exists** if you want to require the following registry key to be present to match a criterion for assigning a location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\<Protective_Software>
```

- **Does not exist**—Click if the absence of the named registry key from the remote client PC is sufficient to match the location you are configuring.

  EXAMPLE Click **Does not exist** if you want to require the following registry key to be absent to match a criterion for assigning a location:

  ```
      HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\<Evil_SpyWare>
  ```

- **DWORD value** radio button—Click if the registry key includes a "Dword" ("double word," a 32-bit integer) and you want to specify its value as a criterion.

  "DWORD" refers to the attribute in the Add/Edit Registry Criterion dialog box. "Dword" refers to the attribute as it appears in the registry key.

  Note Use the regedit application, accessed on the Windows command line, to view the Dword value of a registry key, or use it to add a Dword value to the registry key to satisfy the requirement you are configuring.

  DWORD value menu—Choose one of the following options next to **DWORD value** to specify the relationship of the Dword value of the registry key to the value to be entered to the right:

  - different from
  - equal to
  - greater than
  - greater than or equal to
  - less than
  - less than or equal to

  DWORD value field—Enter a decimal to compare with the Dword value of the registry key on the client computer.

  EXAMPLE Choose **greater than or equal to** and enter an integer if you want to require that the following protective software application meet a minimum version requirement:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\<Protective_Software>\Version
  ```

- **String value** radio button—Click if the registry key includes a string and you want to specify its value as a criterion.

  Note Use the regedit application, accessed on the Windows command line, to view the String value of a registry key, or use it to add a String value to the registry key to satisfy the requirement you are configuring.

  String value menu—Choose one of the following options to specify the relationship of the String value of the registry key to the value to be entered to the right:

  - contains
  - differs
  - matches

String value field—Enter a string to compare with the String value of the registry key on the client computer.

EXAMPLE Choose **matches** and enter Active if you want to ensure the following protective software application is active:

```
HKEY_LOCAL_MACHINE\SOFTWARE\<Protective_Software>\Status
```

Case sensitive—Check to require the String value of the registry key on the client computer to match the case used in the String value field to satisfy the criterion.

Step 3 Click **OK**.

The dialog box closes and the new criterion appears as an entry in the Registry Criteria window inside the Registry and File Criteria dialog box.

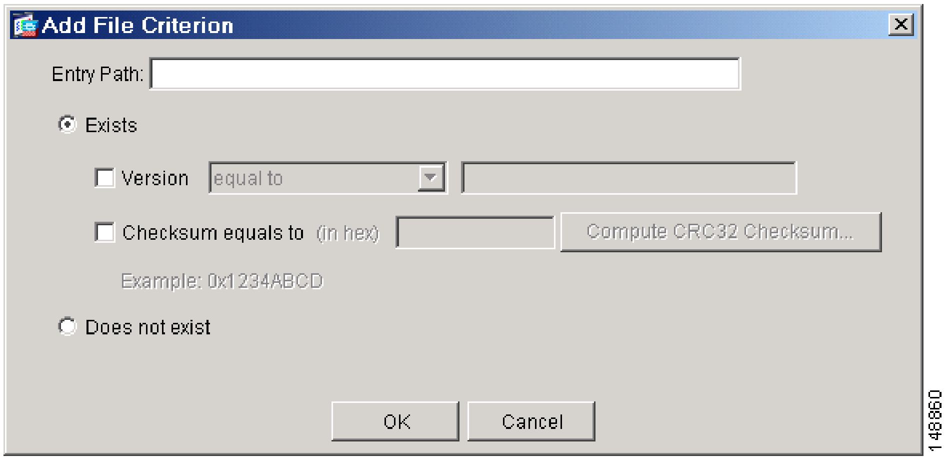
Step 4 Click **Add** if you want to specify another registry key, refer to the next section if you want to specify a file criterion, or click **OK** to return to the Identification for <*Location*> pane.

File Criteria

In the File Criteria area of the Registry and File Criteria dialog box (Figure 5-3), click **Add** if you want to confirm the presence or absence of a specific file as a criterion for assigning the location you are configuring for the remote client, or choose a criterion to be modified from the File Criteria area and click **Edit**.

The Add or Edit File Criterion dialog box opens. Figure 5-5 shows the Add File Criterion dialog box.

Figure 5-5 Add File Criterion



Add File Criterion

Entry Path:

● Exists

☐ Version equal to

☐ Checksum equals to (in hex)

Example: 0x1234ABCD

○ Does not exist

Configure a file criterion as follows:

Step 1 Assign a value to the following mandatory attribute:

- **Entry Path**—Enter the directory path of the file required to be present on or absent from the client system.

Note Refer to the subsequent attribute descriptions for examples File paths.

Step 2 Click one radio button from the following list and assign the associated values:

- **Exists**—Click if the file must be present on the remote client PC to assign the location you are configuring.

  EXAMPLE Click **Exists** to ensure the following security application is installed:

  ```
  C:\Program Files\<Security Application>\<Protective_Application.exe>
  ```

  You can specify a version, checksum, both, or neither in conjunction with the "Exists" radio button.

  (Optional) **Version** check box—Check if you want to specify the version of the file as a criterion. Use this criterion to require that a specific application is a particular version.

  Note To display the version of an .exe file, use Windows Explorer to right-click the file, choose **Properties**, and click the **Version** tab.

  (Optional) **Version** menu—Choose one of the following options to specify the relationship of the "Version value" of the file to the number to be entered to the right:

  - less than
  - less than or equal to
  - equal to
  - different from
  - greater than
  - greater than or equal to

  (Optional) **Version** field—Type a string (typically in dotted decimal notation) to compare with the version of the file on the client computer.

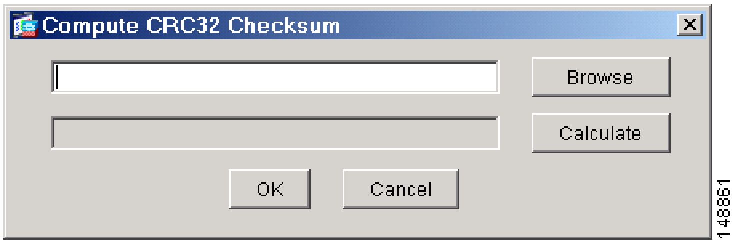
  (Optional) **Checksum equals to** check box—Check to specify a checksum to authenticate the file named in the Path field.

  (Optional) **Checksum equals to** field—Enter a checksum in hexadecimal format, beginning with 0x, to authenticate the file named in the Path field, or click **Compute CRC32 Checksum** to calculate and insert the value automatically.

  (Optional) **Compute CRC32 Checksum**—Click to calculate the checksum of the file stored locally and insert the value in the **Checksum equals to** field.

  The Compute CRC32 Checksum dialog box opens (Figure 5-6).

Figure 5-6 Compute CRC32 Checksum



Retrieve the checksum as follows:

a. Click **Browse** and choose the file on which to calculate the checksum.

The field at the top of the Compute CRC32 Checksum dialog box displays the path to the file you chose.

b. Click **Calculate**.

The field at the bottom of the Compute CRC32 Checksum dialog box displays the checksum in hexadecimal format.

c. Click **OK**.

The Compute CRC32 Checksum dialog box closes and the hexadecimal value appears in the **Checksum equals to** field.

Step 3 Click **OK** in the Add or Edit File Information dialog box.

The dialog box closes and the new criterion appears as an entry in the File Criteria window inside the Registry and File Criteria dialog box.

Step 4 Click the associated **Add** button if you want to specify another registry or file criterion, or click **OK** to return to the Identification for <*Location*> pane.

Configuring the Secure Desktop for Clients that Match Location Criteria

Refer to the following sections to define the Secure Desktop experience for clients that match the criteria defined for a specific location:

- Configuring a VPN Feature Policy for a Location
- Configuring Keystroke Logger for a Location
- Configuring Cache Cleaner for a Location
- Configuring Secure Desktop General for a Location
- Configuring Secure Desktop Settings for a Location
- Configuring Secure Desktop Browser for a Location

Configuring a VPN Feature Policy for a Location

CSD applies the configured VPN feature policy if you choose neither the Secure Desktop nor the Cache Cleaner location modules in the Identification for <*Location*> pane (Figure 5-2). Use the instructions in the following sections to configure the VPN feature policy for each location for which neither option is chosen:

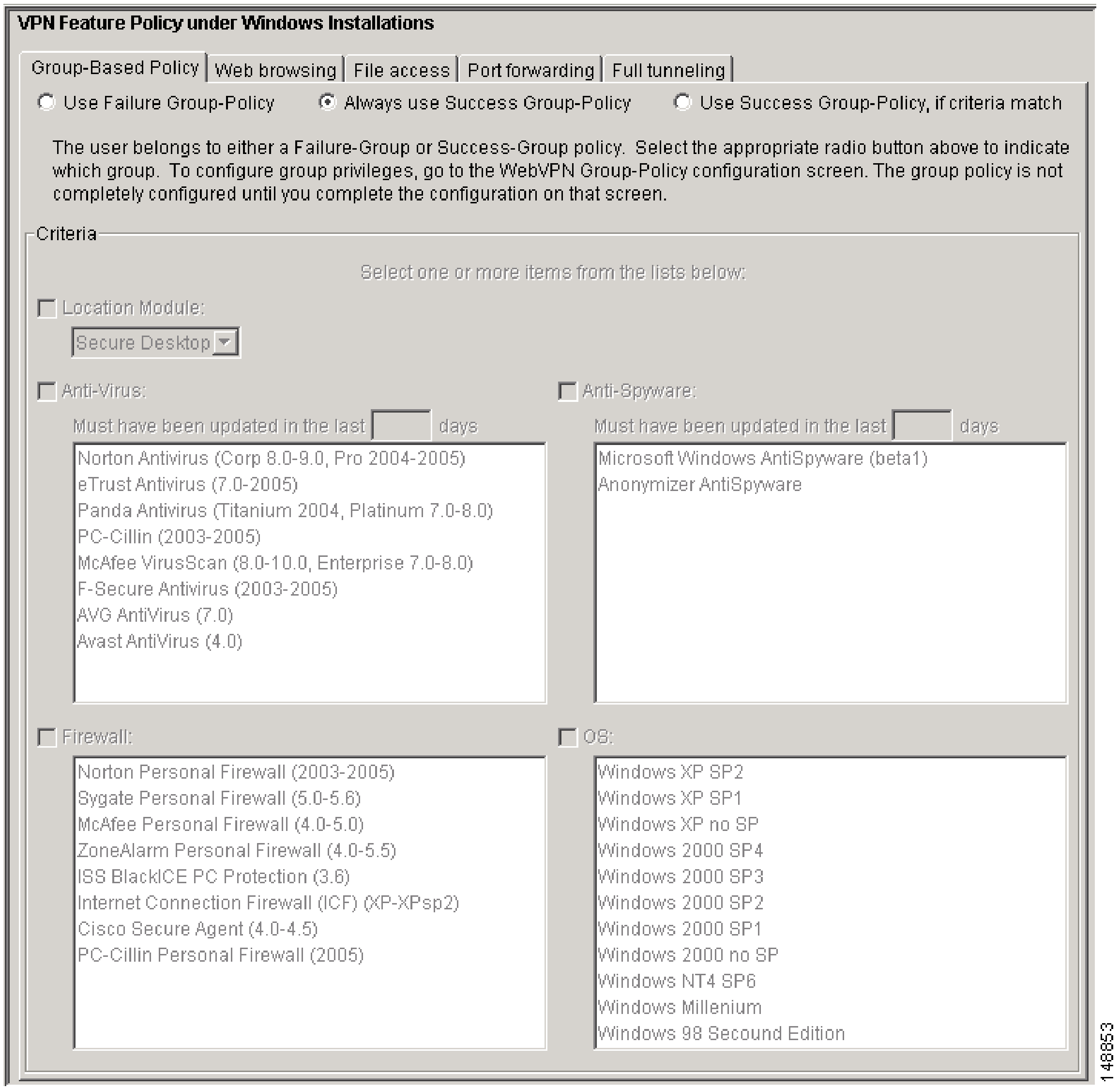
Configuring a Group-based Policy for a Location

Configure a group-based VPN feature-based policy as follows:

Step 1 Click **VPN Feature Policy** under the name of the location you are configuring in the menu on the left.

The Group-Based Policy tab opens (Figure 5-7).

Figure 5-7 VPN Group-based Policy under Windows Installations



○ Use Failure Group-Policy ● Always use Success Group-Policy ○ Use Success Group-Policy, if criteria match

The user belongs to either a Failure-Group or Success-Group policy. Select the appropriate radio button above to indicate which group. To configure group privileges, go to the WebVPN Group-Policy configuration screen. The group policy is not completely configured until you complete the configuration on that screen.

Criteria

Select one or more items from the lists below:

□ Location Module:

Secure Desktop

□ Anti-Virus:

Must have been updated in the last ____ days

Norton Antivirus (Corp 8.0-9.0, Pro 2004-2005)
eTrust Antivirus (7.0-2005)
Panda Antivirus (Titanium 2004, Platinum 7.0-8.0)
PC-Cillin (2003-2005)
McAfee VirusScan (8.0-10.0, Enterprise 7.0-8.0)
F-Secure Antivirus (2003-2005)
AVG AntiVirus (7.0)
Avast AntiVirus (4.0)

□ Anti-Spyware:

Must have been updated in the last ____ days

Microsoft Windows AntiSpyware (beta1)
Anonymizer AntiSpyware

□ Firewall:

Norton Personal Firewall (2003-2005)
Sygate Personal Firewall (5.0-5.6)
McAfee Personal Firewall (4.0-5.0)
ZoneAlarm Personal Firewall (4.0-5.5)
ISS BlackICE PC Protection (3.6)
Internet Connection Firewall (ICF) (XP-XPsp2)
Cisco Secure Agent (4.0-4.5)
PC-Cillin Personal Firewall (2005)

□ OS:

Windows XP SP2
Windows XP SP1
Windows XP no SP
Windows 2000 SP4
Windows 2000 SP3
Windows 2000 SP2
Windows 2000 SP1
Windows 2000 no SP
Windows NT4 SP6
Windows Millenium
Windows 98 Secound Edition

Step 2 Click one of the following radio buttons:

- **Use Failure Group-Policy** if you want to apply the "Alternative group policy" to any remote client matched to this location.

  This option lets you apply an alternative to the default group policy so you can differentiate access rights. Typically, you would use the failure group policy to apply access rights that are more limited than those associated with the success group policy.

  With this option set, CSDM dims the attributes in the Criteria area. If you click this radio button, you cannot change other settings on this tab.

Note If you click this radio button, change the alternative group policy setting for the WebVPN tunnel group to a group policy that has access rights that are different than the default group policy. To do so, choose the **Configuration > VPN > General > Tunnel Group > Add/Edit Tunnel Group > WebVPN Access > WebVPN** tab. Change the policy assigned to the **Alternative group policy** attribute to apply a policy to all clients who match this location.

- **Always use Success Group-Policy** if you want to apply the default WebVPN group policy to any remote client matched to this location.

  This option is the default group-based policy setting. If you click this radio button, CSDM dims the attributes in the Criteria area; you cannot change other settings on this tab. Your configuration of a group-based policy ends with this step.

- **Use Success Group-Policy if criteria match** if you want to apply the following group policy to the remote client matched to this location:
  - WebVPN default group policy if the client PC satisfies the criteria specified on this tab.
  - WebVPN failure group policy if the client PC fails to satisfy the criteria specified on this tab.

  Note If you click this radio button, choose the **Configuration > VPN > General > Tunnel Group > Add/Edit Tunnel Group > WebVPN Access > WebVPN** tab. Change the policy assigned to the **Alternative group policy** attribute to apply a policy to clients that fail to satisfy the criteria.

  If you click this radio button, CSDM activates the check boxes in the criteria area.

  Note A “Use Success Group-Policy if criteria match,” setting without criteria is equivalent to “Always use Success Group-Policy.”

  Continue with the following steps.

Step 3 Check **Location Module** if you want to require the presence of Secure Desktop or Cache Cleaner as a criterion for assigning the success group policy, then choose the module to require: Secure Desktop or Cache Cleaner.

Note If the feature you choose is not active, the client fails the VPN feature policy criteria check.

Step 4 Check **Anti-Virus**, **Anti-Spyware**, **Firewall**, and **OS** if you want to require their presence as conditions for assigning the success group policy.

If you enable more than one category, the end user's computer must pass in each category to pass the System Detection check. An “AND” relationship is present among the enabled categories.

The options within each category have an “OR” relationship. For example, you can specify that any one of a list of antivirus software programs be running, and even if you have checked all of them as possible candidates, having just one of them running is enough to satisfy the antivirus software requirement.

The security categories are as follows:

- **Anti-Virus**—Check to enable System Detection for the presence of antivirus software. CSD requires one of the applications highlighted to be running on the remote client PC to satisfy the anti-virus requirement.
- **Anti-Spyware**—Check to enable System Detection for the presence of antispyware software. CSD requires one of the applications highlighted to be running on the remote client PC to satisfy the anti-virus requirement.
- **Firewall**—Check to enable System Detection for the presence of a personal firewall that is running. CSD requires one of the applications highlighted to be running on the remote client PC to satisfy the personal firewall requirement.
- **OS**—Check to enable System Detection for the presence of a particular operating system and service pack. CSD requires one of the operating systems highlighted to be running on the remote client PC to satisfy the operating system requirement.

Step 5 (Optional) Enter an integer in the range 0 - 999999 in the **Must have been updated in the last ___ days** fields.

CSDM includes this two such fields, one above the Anti-Virus window and the other above the Anti-Spyware window.

Step 6 For each enabled security category you check, click one of the options or control-click multiple options.

Note For the complete list of applications checked by System Detection, see Figure 5-7 or refer to "System Detection Questions."

Click **Apply All** to save the running CSD configuration.

Configuring Web Browsing, File Access, Port Forwarding, and Full Tunneling VPN Policies for a Location

This section describes how to configure permissions and system detection conditions for web browsing, file access, port forwarding, and full tunneling when the remote client satisfies the configured location criteria.

Note To configure settings when remote clients running Microsoft Windows do *not* satisfy configured location criteria, see "Creating Windows Locations."

Step 1 Click **VPN Feature Policy** under the name of the location you are configuring in the menu on the left.

The VPN Feature Policy pane displays the default Group-Based Policy tab (described in "Configuring a Group-based Policy for a Location").

Step 2 Click the tab that names the application for which you would like to configure a policy. The tabs after the Group-Based Policy tab are as follows:

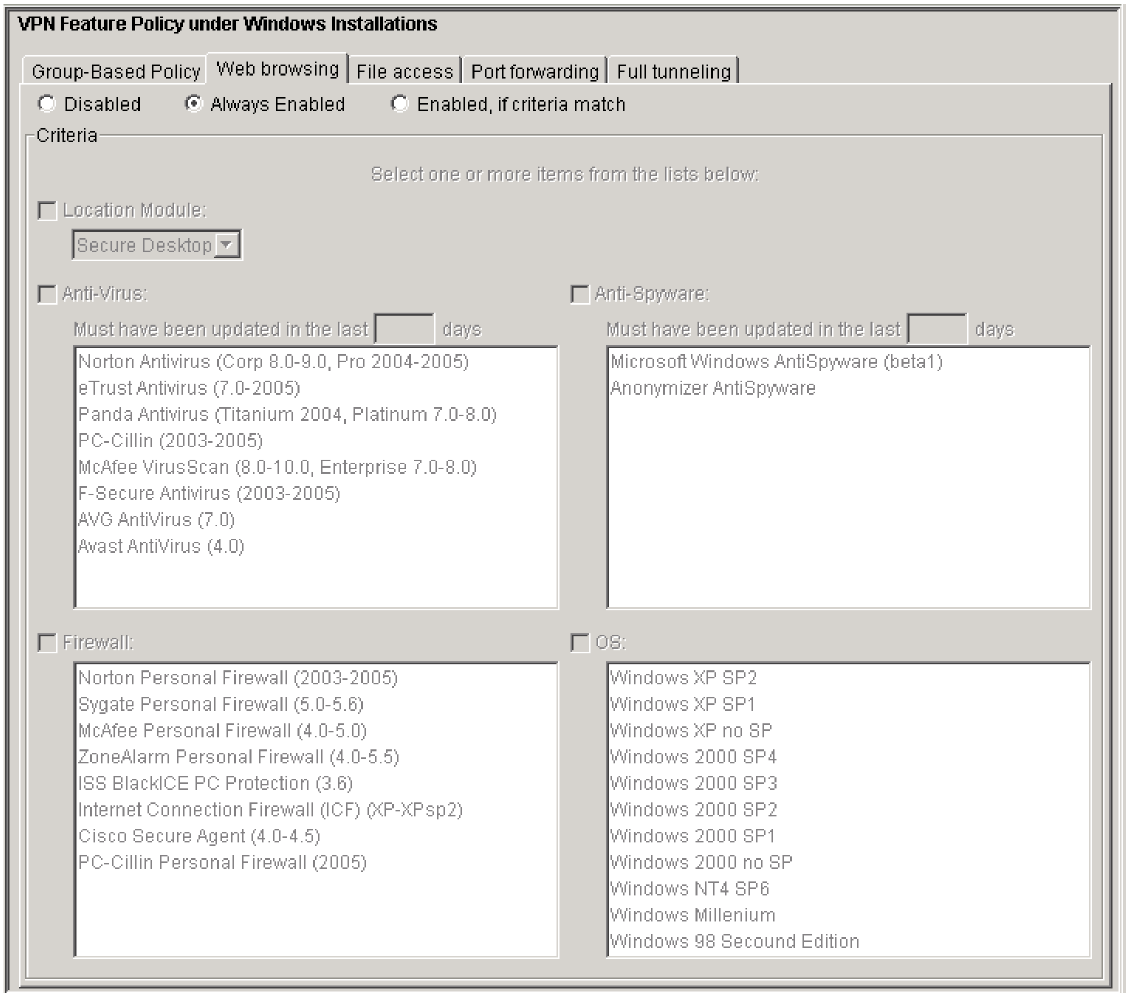
- Web browsing—Permits the client to use the Secure Desktop to browse the web.
- File access—Permits the use of the Secure Desktop to access files on a remote server.
- Port forwarding—Permits the use of the Secure Desktop to connect a client application installed on the local PC to the TCP/IP port of a peer application on a remote server.

- Full tunneling—Lets the SSL VPN Client establish a VPN tunnel.

Note The default setting for each of these attributes is “OFF.”

Figure 5-8 shows the Web browsing tab.

Figure 5-8 VPN Web Browsing Policy under Windows Installations



VPN Feature Policy under Windows Installations

○ Disabled ● Always Enabled ○ Enabled, if criteria match

Criteria

Select one or more items from the lists below:

□ Location Module:

Secure Desktop

□ Anti-Virus:

Must have been updated in the last [ ] days

Norton Antivirus (Corp 8.0-9.0, Pro 2004-2005)
eTrust Antivirus (7.0-2005)
Panda Antivirus (Titanium 2004, Platinum 7.0-8.0)
PC-Cillin (2003-2005)
McAfee VirusScan (8.0-10.0, Enterprise 7.0-8.0)
F-Secure Antivirus (2003-2005)
AVG AntiVirus (7.0)
Avast AntiVirus (4.0)

□ Anti-Spyware:

Must have been updated in the last [ ] days

Microsoft Windows AntiSpyware (beta1)
Anonymizer AntiSpyware

□ Firewall:

Norton Personal Firewall (2003-2005)
Sygate Personal Firewall (5.0-5.6)
McAfee Personal Firewall (4.0-5.0)
ZoneAlarm Personal Firewall (4.0-5.5)
ISS BlackICE PC Protection (3.6)
Internet Connection Firewall (ICF) (XP-XPsp2)
Cisco Secure Agent (4.0-4.5)
PC-Cillin Personal Firewall (2005)

□ OS:

Windows XP SP2
Windows XP SP1
Windows XP no SP
Windows 2000 SP4
Windows 2000 SP3
Windows 2000 SP2
Windows 2000 SP1
Windows 2000 no SP
Windows NT4 SP6
Windows Millenium
Windows 98 Secound Edition

148862

Note Except for the tab name, the last four tabs are identical. Also, except for the row of radio buttons near the top, they are also identical to the Group-Based Policy tab (Figure 5-7).

Step 3 Click one of the following radio buttons:

- **Disabled** to make the feature unavailable to the remote client that matches the location criteria.

  This option is the default VPN policy setting for web browsing, file access, port forwarding, and full tunneling. If set, CSDM dims the attributes in the Criteria area. If you click this radio button, you cannot change other settings on this tab; your configuration of a VPN policy for this feature ends at this step.

- **Always Enabled** to make the feature available to the remote client that matches the location criteria.

  If you click this radio button, CSDM dims the attributes in the Criteria area. If set, you cannot change other settings on this tab; your configuration of a VPN policy for this feature ends at this step.

- **Enabled if criteria match** to make the feature available to the remote client that matches the location criteria and satisfies the conditions set below. If you click this radio button, CSDM activates the check boxes in the criteria area.

  Note An "Enabled if criteria match," setting without criteria is equivalent to "Always Enabled."

Step 4 Check **Location Module** if you want to require the presence of Secure Desktop or Cache Cleaner as a criterion for enabling the feature identified in the tab, then choose the module to require: Secure Desktop or Cache Cleaner.

Note If the feature you choose is not active, the client fails the VPN feature policy criteria check.

Step 5 Click one or more security categories to require their presence as a condition to enable the location module you chose in Step 4.

If you enable more than one category, the end user's computer must pass in each category to pass the System Detection check. An "AND" relationship is present among the enabled categories.

The options within each category have an "OR" relationship. For example, you can specify that any one of a list of antivirus software programs be running, and even if you have checked all of them as possible candidates, having just one of them running is enough to satisfy the antivirus software requirement.

The security categories are as follows:

- **Anti-Virus**—Check to enable System Detection for the presence of antivirus software. CSD requires one of the applications highlighted to be running on the remote client PC to satisfy the anti-virus requirement.
- **Anti-Spyware**—Check to enable System Detection for the presence of antispyware software. CSD requires one of the applications highlighted to be running on the remote client PC to satisfy the anti-virus requirement.
- **Firewall**—Check to enable System Detection for the presence of a personal firewall that is running. CSD requires one of the applications highlighted to be running on the remote client PC to satisfy the personal firewall requirement.
- **OS**—Check to enable System Detection for the presence of a particular operating system and service pack. CSD requires one of the operating systems highlighted to be running on the remote client PC to satisfy the operating system requirement.

Step 6 (Optional) Enter an integer in the range 0 - 999999 in the **Must have been updated in the last ___ days** fields.

CSDM includes this two such fields, one above the Anti-Virus window and the other above the Anti-Spyware window.

Step 7 For each enabled security category you check, click one of the options or control-click multiple options.

Note For the complete list of applications checked by System Detection, see Figure 5-8 or refer to "System Detection Questions."

Configuring Keystroke Logger for a Location

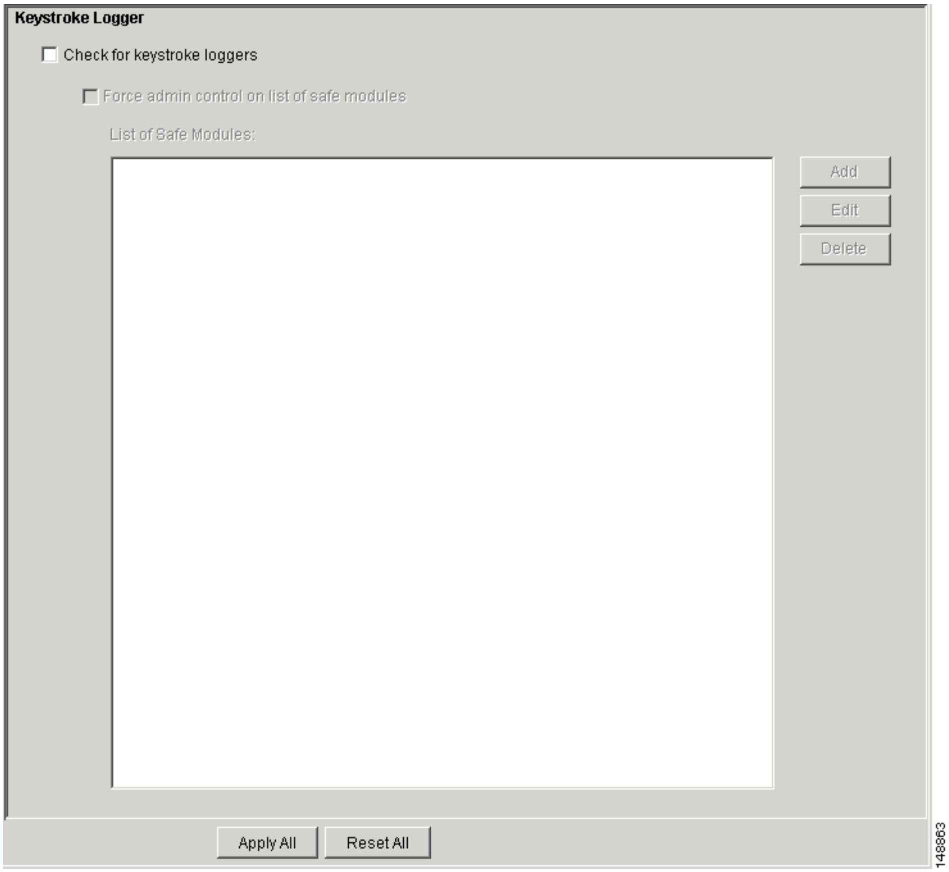
You can configure a location type to scan for keystroke logging applications on the remote client. You can list the keystroke logging applications that are safe or let the remote user approve of the applications the scan identifies. Secure Desktop and Cache Cleaner launch only if the scan is clear, or only if you assign administrative control to the user and the user approves of the applications the scan identifies. It may not be possible for CSD to detect all keystroke loggers present, including hardware keystroke logging devices.

By default, System Detection does not scan for keystroke loggers. Configure scanning for keystroke loggers as follows:

Step 1 Click **Keystroke Logger** under the name of the location you are configuring in the menu on the left.

The Keystroke Logger window opens (Figure 5-9).

Figure 5-9 Keystroke Logger Window



Keystroke Logger

□ Check for keystroke loggers

□ Force admin control on list of safe modules

List of Safe Modules:

The “List of Safe Modules” window lists the paths to program applications on the remote client that have keystroke logging capabilities, but are safe to use, as determined by the administrator. Such programs, such as Corel (previously Jasc) Paint Shop Pro, typically invoke functions when the user presses particular keystroke combinations from within another application.

Step 2 Check **Check for keystroke loggers** to scan for a keystroke logging application on the remote client PC and make sure one is not running, before creating the Secure Desktop space on the remote client.

By default, this attribute is not checked, and the other attributes and buttons are grayed out. If you check this attribute, the “Force admin control on list of safe modules” attribute becomes active.

Step 3 Check **Force admin control on list of safe modules** to give yourself control over which key loggers are exempt from scanning, or uncheck it to give the remote user this control.

If you check this attribute, the **Add** button become active.

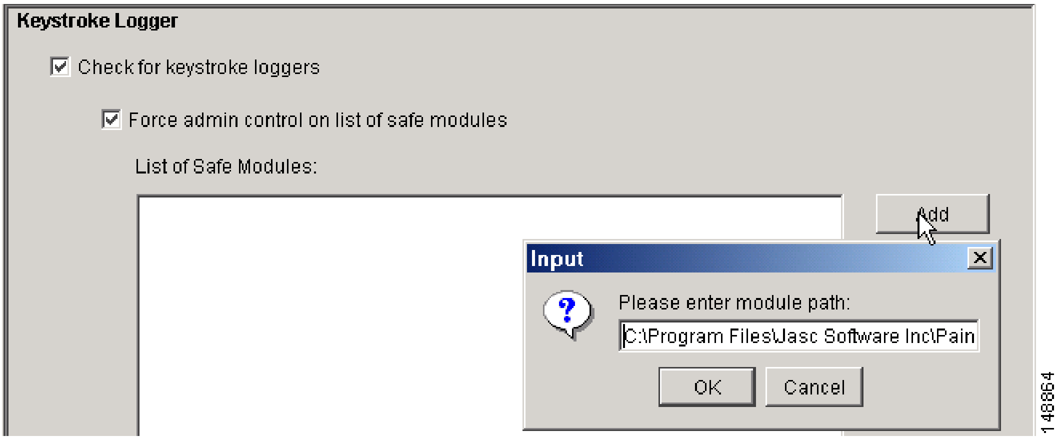
Uncheck this attribute if you want to give the remote user the right to determine if any detected keystroke logger is safe. If this attribute is unchecked, CSD lists the keystroke loggers discovered on the client computer. To access the Secure Desktop, the user must insert a check next to all of the keystroke loggers in the list to indicate they are safe. Otherwise, the user must terminate the session.

Note Unchecking this attribute deactivates but does not delete the contents of the “List of Safe Modules” window.

Step 4 Click **Add** to specify a module as safe, or choose an entry in the List of Safe Modules window and click **Edit** if you want to modify its path.

CSDM opens the Input dialog box.

Figure 5-10 Input (for Keystroke Logger)



Keystroke Logger

☑ Check for keystroke loggers

☑ Force admin control on list of safe modules

List of Safe Modules:

Input

Please enter module path: C:\Program Files\Jasc Software Inc\Pain

Step 5 Type the path and name of the module or application in the **Please enter module path** field, then click **OK**.

CSDM closes the dialog box and lists the entry in the List of Safe Modules window.

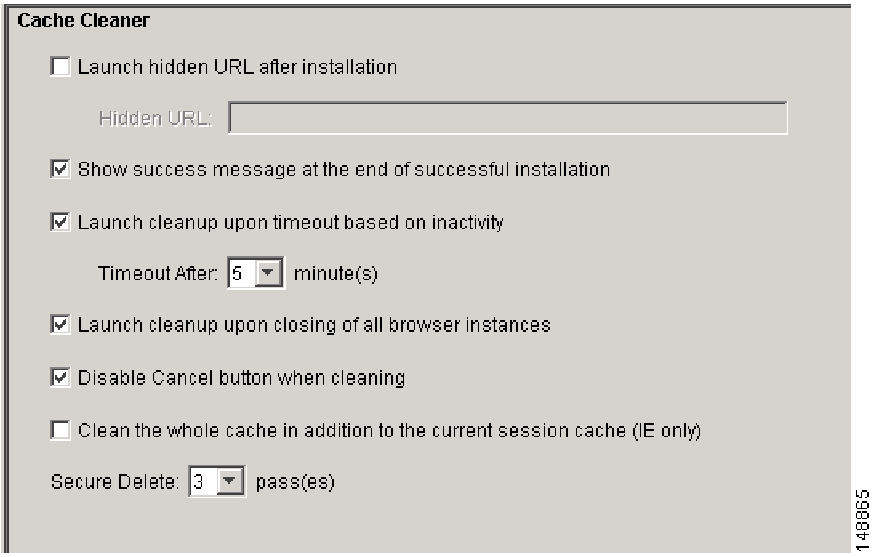
Note To remove a program from the list, click the entry in the "Path of safe modules" list, then click **Delete**.

Step 6 Click **Apply All** to save the configuration changes.

Configuring Cache Cleaner for a Location

For each location for which the Cache Cleaner is enabled, click **Cache Cleaner** under the location you are configuring to configure Cache Cleaner for Windows. The Cache Cleaner pane appears. Figure 5-11 shows the default settings.

Figure 5-11 Cache Cleaner for Windows



Cache Cleaner

□ Launch hidden URL after installation

Hidden URL:

☑ Show success message at the end of successful installation

☑ Launch cleanup upon timeout based on inactivity

Timeout After: 5 minute(s)

☑ Launch cleanup upon closing of all browser instances

☑ Disable Cancel button when cleaning

□ Clean the whole cache in addition to the current session cache (IE only)

Secure Delete: 3 pass(es)

This window lets you configure the Cache Cleaner for the associated location only. Check the following fields as required by your security policy:

- Launch hidden URL after installation—Check to use a URL for administrative purposes, hidden from the remote client, so that you know that the user has the Cache Cleaner installed. For example, you could place a cookie file on the user's computer, and later check for the presence of that cookie.
- Hidden URL—Type the URL to use for administrative purposes, if you checked “Launch hidden URL after installation.”
- Show success message at the end of successful installation—Check to display a dialog box on remote client PCs informing the user when the Cache Cleaner installation is successful.
- Launch cleanup upon timeout based on inactivity—Check to set a specific timeout period after which the cleanup begins.
- Timeout after—Choose the number of minutes (1, 2, 5, 10, 15, 30, or 60) to set the timeout period if you checked the “Launch cleanup upon timeout based on inactivity” attribute. This attribute is the inactivity timer. Its default value is 5.
- Launch cleanup upon closing of all browser instances—Check to clean up the cache when all browser windows are closed.
- Disable Cancel button when cleaning—Check to prevent the remote user from canceling the deletion of the cache.
- Clean the whole cache in addition to the current session cache (IE only)—Check to remove data from the Internet Explorer cache upon activation, including files generated before the client’s CSD session began.

- Secure Delete—CSD encrypts and writes the cache to the remote client's disk. Upon termination of the Secure Desktop, CSD converts all bits occupied by the cache to all 0's, then to all 1's, and then to randomized 0's and 1's. Choose the number of times for CSD to perform this cleanup task. The default setting, 1 pass, meets the US Department of Defense (DoD) standard for securely deleting files. Following the completion of the task the number of times specified, CSD removes the pointer to the file (that is, performs a "Windows-delete").

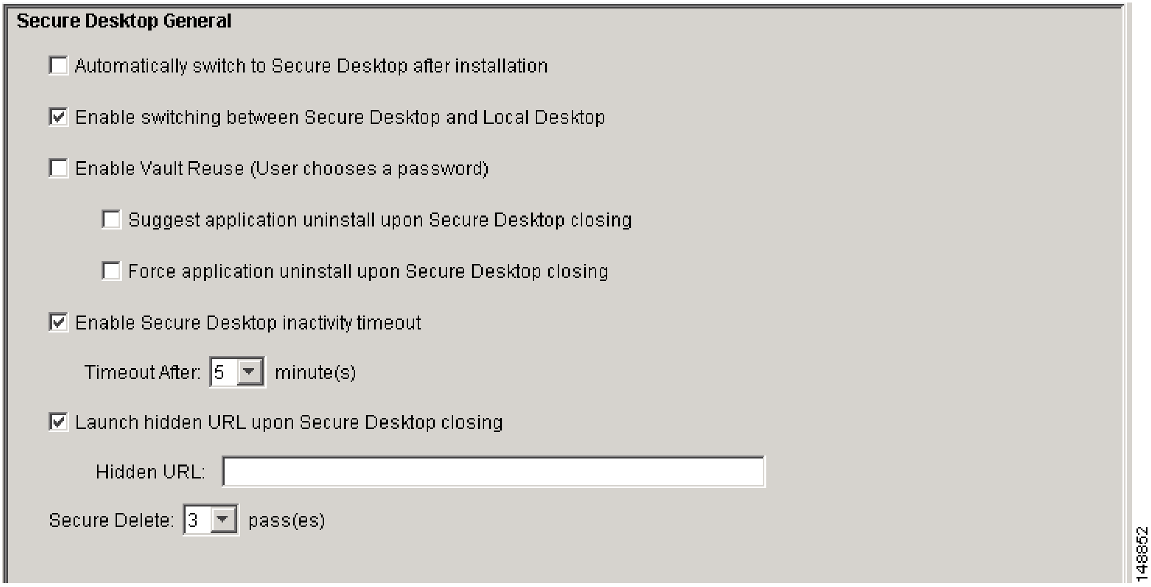
Note Click **Apply All** to save the running CSD configuration.

Configuring Secure Desktop General for a Location

Click **Secure Desktop General** under the location name to enable or disable the Secure Desktop features and customize the user experience.

The Secure Desktop General pane appears. Figure 5-12 shows the default settings.

Figure 5-12 Secure Desktop General



Secure Desktop General

☐ Automatically switch to Secure Desktop after installation

☑ Enable switching between Secure Desktop and Local Desktop

☐ Enable Vault Reuse (User chooses a password)

☐ Suggest application uninstall upon Secure Desktop closing

☐ Force application uninstall upon Secure Desktop closing

☑ Enable Secure Desktop inactivity timeout

Timeout After: 5 minute(s)

☑ Launch hidden URL upon Secure Desktop closing

Hidden URL:

Secure Delete: 3 pass(es)

Check the following attributes to configure the Secure Desktop General settings for the location you are configuring, as required by your security policy:

- Automatically switch to Secure Desktop after installation—Check to set the Secure Desktop to load automatically after installation. This option forces users into the Secure Desktop.
- Enable switching between Secure Desktop and Local Desktop—We strongly recommend that you check this attribute to let users switch between Secure Desktop and the untrusted desktop. Called *desktop switching*, this feature provides users with the flexibility they might need to respond to a prompt from another application requiring an OK to let CSD continue processing. (The Cisco Secure Tunneling Client is *not* one of those applications; it is accessible on both the local desktop and the CSD.) Unchecking this attribute minimizes the potential security risk posed by a user who leaves traces on the untrusted desktop. Thus, you might choose to uncheck this option if the security

risk is a bigger issue than the deployment advantages of the alternative. Operating System limitations may prevent CSD from enforcing prevention of desktop switching, even if you disable this feature.

You can configure both the Secure Desktop component of CSD and Cisco SSL VPN Client (SVC) to run simultaneously on client PCs. If you check this attribute, the SVC connection becomes available to both.

- Enable Vault Reuse—Check to allow users to close the Secure Desktop and open it again at a later time. The Vault is a persistent desktop that is available from one session to the next. If you enable this option, users must enter a password (up to 127 characters in length) when CSD creates the Secure Desktop. This is useful if users are running the Secure Desktop on computers that are likely to be reused; for example, a home computer. When a user closes the Secure Desktop, CSD does not destroy the Vault. If you do not enable this option, CSD automatically destroys the Vault at the end of each Secure Desktop session.

  If unchecked, this attribute activates the following two attributes.

- Suggest application uninstall upon Secure Desktop closing—Check to prompt the user and recommend that the Secure Desktop be uninstalled when it closes. In contrast to the option below, the user has the choice to refuse the uninstallation.

  Note Leave this option disabled if you want users to be able to use the Vault. Checking this option uninstalls the Vault from the user's computer when the Secure Desktop closes.

- Force application uninstall upon Secure Desktop closing—Check if you do not want to leave the Secure Desktop application on untrusted computers after users are done using it. The Secure Desktop uninstalls when it closes.

  Note Leave this option disabled if you want users to be able to use the Vault. Checking this option uninstalls the Vault from the user's computer when the Secure Desktop closes.

- Enable Secure Desktop inactivity timeout—Check to close the Secure Desktop automatically after a period of inactivity.

  Because CSD runs on the client machine, it detects real inactivity and closes the Secure Desktop to avoid leaving anything behind.

  If checked, this attribute activates the following attribute.

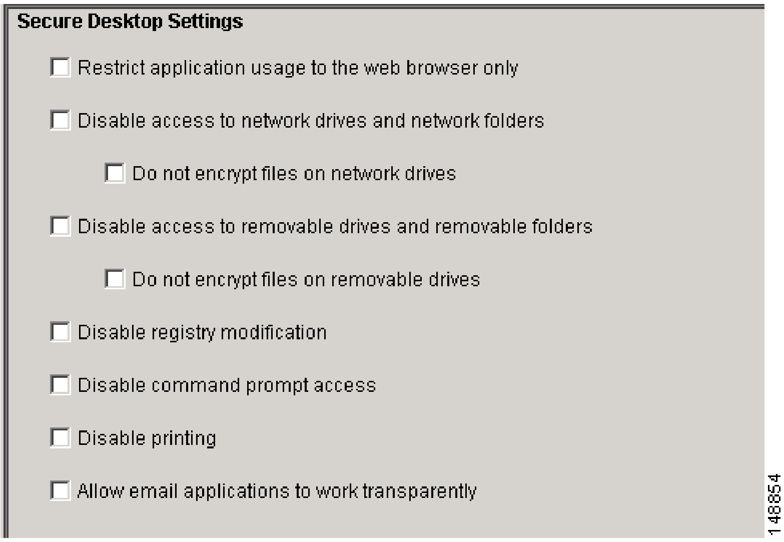
- Timeout After—Choose the number of minutes (1, 2, 5, 10, 15, 30, or 60) to set the timeout period if you checked the “Enable Secure Desktop inactivity timeout” attribute. This attribute is the associated inactivity timer.
- Launch hidden URL upon Secure Desktop closing—Check this box and enter a URL in the field to make CSD automatically open a web page when the Secure Desktop closes.
- Secure Delete—CSD encrypts and writes the Secure Desktop to the remote client’s disk. Upon termination of the Secure Desktop, CSD converts all bits occupied by the Secure Desktop to all 0’s, then to all 1’s, and then to randomized 0’s and 1’s. Choose the number of times for CSD to perform this cleanup task. The default setting, 1 pass, meets the US Department of Defense (DoD) standard for securely deleting files. Following the completion of the task the number of times specified, CSD removes the pointer to the file (that is, performs a “Windows-delete”).

Note Click **Apply All** to save the running CSD configuration.

Configuring Secure Desktop Settings for a Location

Click **Secure Desktop Settings** under the location name to place restrictions on the Secure Desktop. The Secure Desktop Settings pane appears. Figure 5-13 shows the default settings.

Figure 5-13 Secure Desktop Settings



Secure Desktop Settings

- □ Restrict application usage to the web browser only
- □ Disable access to network drives and network folders
  - □ Do not encrypt files on network drives
- □ Disable access to removable drives and removable folders
  - □ Do not encrypt files on removable drives
- □ Disable registry modification
- □ Disable command prompt access
- □ Disable printing
- □ Allow email applications to work transparently

Check the boxes to apply the associated restrictions. The restrictions are as follows:

- Restrict application usage to the web browser only—Check to let only the originating browser run on the Secure Desktop. If you choose this option, the browser that started CSD (Internet Explorer, Netscape, Firefox, etc.) is the only browser permitted to run in Secure Desktop mode. Choosing this option limits the user's ability to use other applications, but increases the level of security.
- Disable access to network drives and network folders—Check to prevent the user from accessing network resources and network drives while on the Secure Desktop. The network resources are those that use the Server Message Block (SMB) client/server, request-response protocol to share such resources as files, printers, and APIs. For maximum security, we recommend that you check this attribute. If you do, the Secure Desktop Manager dims the following attribute.
- Do not encrypt files on network drives—Check to prevent the user from saving encrypted files to drives onto the network while on the Secure Desktop. The Secure Desktop Manager dims this attribute if you check the previous attribute.
- Disable access to removable drives and removable folders**—**Check to prevent the user from accessing portable drives while on the Secure Desktop. Otherwise, the user can save files to a removable drive and remove the drive before closing the CSD session. After closing the CSD session, the user could forget to take the removable drive. For maximum security, we recommend that you check this attribute. If you do, the Secure Desktop Manager dims the next attribute.

  This attribute applies only to the drives that Microsoft names “Removable” in the Windows Explorer “My Computer” window.
- Do not encrypt files on removable drives—Check to prevent the user from saving encrypted files onto portable drives while on the Secure Desktop. The Secure Desktop Manager dims this attribute if you check the previous attribute.

This attribute applies only to the drives that Microsoft names “Removable” in the Windows Explorer “My Computer” window.

- Disable registry modification—Check to prevent the user from modifying the registry from within the Secure Desktop. For maximum security, we recommend that you check this attribute.
- Disable command prompt access—Check to prevent the user running the DOS command prompt from within the Secure Desktop. For maximum security, we recommend that you check this attribute.
- Disable printing—Check to prevent the user from printing while using the Secure Desktop space. For maximum security of sensitive data, check this option.
- Allow email applications to work transparently—Check to let the user open e-mail while on the Secure Desktop and to prevent CSD from deleting e-mail upon the termination of the CSD session. The use of the term *transparent* means that the Secure Desktop handles e-mail the same way that the local desktop handles it. Transparent handling works for the following e-mail applications:
  - Microsoft Outlook Express
  - Microsoft Outlook
  - Eudora
  - Lotus Notes

  If this attribute is checked and the remote user uses an e-mail application to save an attachment to the “My Documents” folder, it is visible from both the Secure Desktop and the local desktop. Similarly, deleting such a file from within the e-mail application running on a Secure Desktop removes the file from both desktops.

Note Deleting transparent or nontransparent files from outside of Outlook, such as from a Windows Explorer window, during a Secure Desktop session removes the file only from the Secure Desktop.

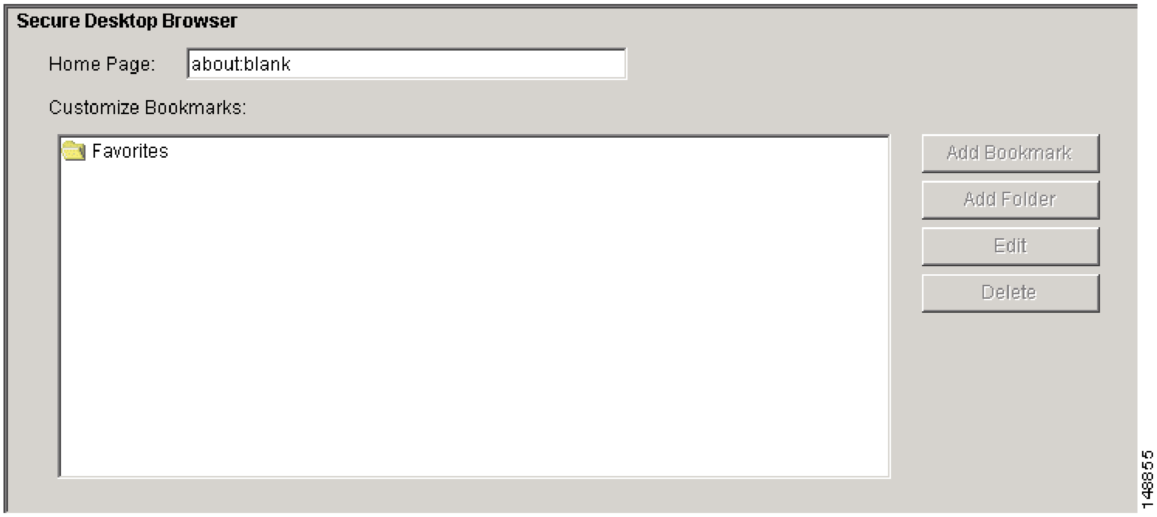
Click **Apply All** to save the running CSD configuration.

Configuring Secure Desktop Browser for a Location

Click **Secure Desktop Browser** under the location name to specify the Home Page to which the browser connects when the remote user establishes a CSD session. This option also lets you specify the folders and URLs that populate the Bookmarks or Favorites menu during the CSD session.

The Secure Desktop Browser pane appears. Figure 5-14 shows the default settings.

Figure 5-14 Secure Desktop Browser



Secure Desktop Browser

Home Page: about:blank

Customize Bookmarks:

For the duration of the CSD session, the browser does not list the user's bookmarks or favorites. It lists only the ones shown in this pane.

Configure the Secure Desktop Browser as follows:

Step 1 Type the URL of the page that you want to open when the remote user establishes a CSD session into the **Home Page** field.

The Customized Bookmarks pane lists the folders and URLs that populate the browser Bookmarks or Favorites menu.

Step 2 Use the following guidelines to add, modify, and delete entries in the Customized Bookmarks pane:

- To add a folder, choose the folder to contain it, click **Add Folder**, type the new folder in the dialog box, then click OK.
- To add a bookmark to the list, choose the folder to contain it, click **Add Bookmark**, type the URL in the dialog box, then click **OK**.
- To modify a URL, choose it, click **Edit**, type the new URL in the dialog box, then click **Edit**.
- To remove a folder or a URL, choose it and click **Delete**.

Note Click **Apply All** to save the running CSD configuration.

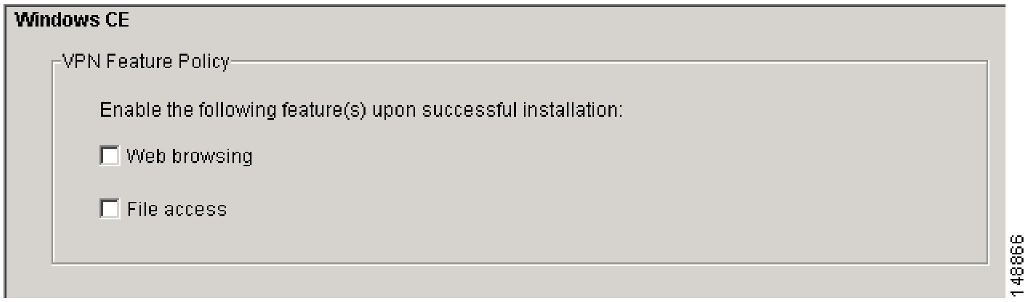
CHAPTER 6

Setting Up CSD for Microsoft Windows CE Clients

CSD lets you configure a VPN feature policy to enable or restrict both web browsing and remote server file access for remote clients running Microsoft Windows CE. To do so, click **Windows CE** in the menu on the left.

The Windows CE pane appears (Figure 6-1).

Figure 6-1 Windows CE



Windows CE

VPN Feature Policy

Enable the following feature(s) upon successful installation:

☐ Web browsing

☐ File access

Set the attributes as follows:

- Web Browsing—Check to let the remote user use the Secure Desktop to browse the web.

Note To ensure security, the Secure Desktop Manager supports only web browsing by clients in unknown locations and access outside of the CSD environment.

- File Access**—**Check to let the remote user use the Secure Desktop to access files on a remote server.

Click **Apply All** to save the running configuration to the flash device.

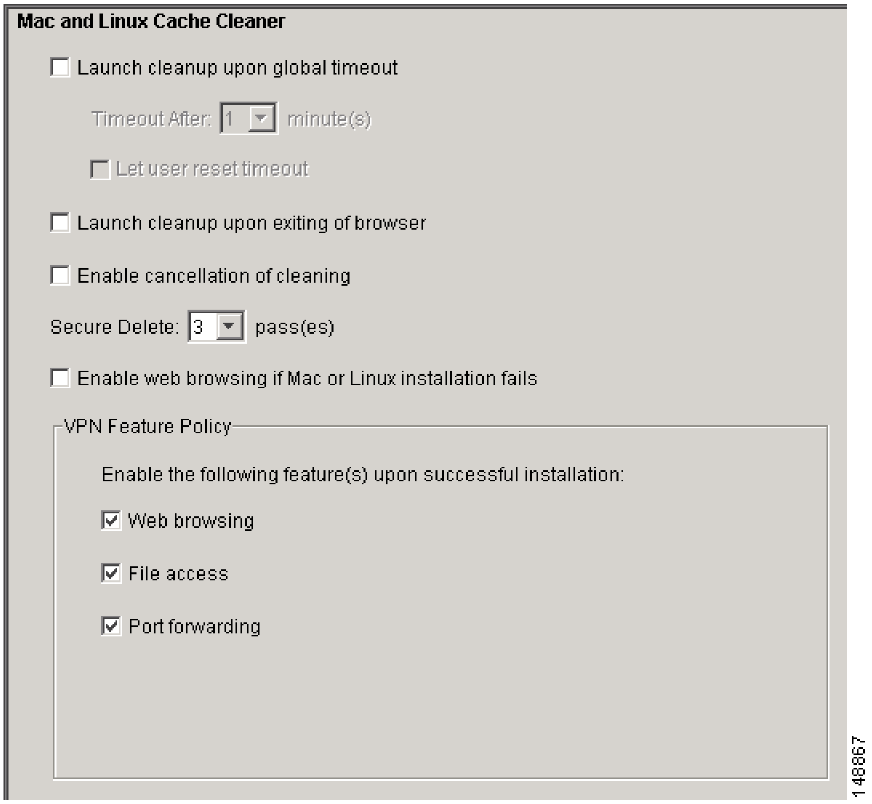
CHAPTER 7

Setting Up CSD for Macintosh and Linux Clients

CSD supports the Cache Cleaner and VPN feature policy for remote clients running Macintosh or Linux. To configure the Secure Desktop experience for these clients, click **Mac & Linux Cache Cleaner** in the menu on the left.

The Mac and Linux Cache Cleaner pane appears (Figure 7-1).

Figure 7-1 Cache Cleaner — Mac and Linux Cache Cleaner



Mac and Linux Cache Cleaner

□ Launch cleanup upon global timeout

Timeout After: 1 minute(s)

□ Let user reset timeout

□ Launch cleanup upon exiting of browser

□ Enable cancellation of cleaning

Secure Delete: 3 pass(es)

□ Enable web browsing if Mac or Linux installation fails

VPN Feature Policy

Enable the following feature(s) upon successful installation:

☑ Web browsing

☑ File access

☑ Port forwarding

Note This pane lets you configure both the Cache Cleaner and VPN feature policy for all Mac and Linux clients.

Set the attributes as follows:

- Launch cleanup upon global timeout and Timeout after—Check to set a global timeout after which CSD launches the Cache Cleaner. Use the drop-down list to set the timeout period.
- Let user reset timeout—Check to allow the user to reset the timeout period.
- Launch cleanup upon exiting of browser—Check to launch cache cleaning when the user closes all browser instances.
- Enable cancellation of cleaning—Check to allow the user to cancel the cache cleaning.
- Secure Delete—CSD encrypts and writes the cache to the remote client's disk. Upon termination of the Secure Desktop, CSD converts all bits occupied by the cache to all 0's, then to all 1's, and then to randomized 0's and 1's. Choose the number of times for CSD to perform this cleanup task. The default setting, 1 pass, meets the US Department of Defense (DoD) standard for securely deleting files. Following the completion of the task the number of times specified, CSD removes the pointer to the file.
- Enable web browsing if Mac or Linux installation fails—Check to allow web browsing (but disable other remote-access features) if Cache Cleaner installation fails.
- Web Browsing—Check to permit the use of the Secure Desktop to browse the web.

Note To ensure security, the Secure Desktop Manager supports only web browsing by clients in unknown locations and access outside of the CSD environment.

- File Access—Check to permit the use of the Secure Desktop to access files on a remote server.
- Port Forwarding—Check to permit the use of the Secure Desktop to connect a client application installed on the local PC to the TCP/IP port of a peer application on a remote server.

Click **Apply All** to save the running configuration to the flash device.

Frequently Asked Questions

The following sections address the CSD FAQs:

- General Questions
- Timeout Questions
- Vault and Secure Desktop Questions
- System Detection Questions
- Security Questions
- Networking and Firewall Questions

General Questions

The following questions address a broad range of CSD functions:

Can I use Fast User Switching on Windows XP?

The Secure Desktop does not support Fast User Switching because only one instance of the CSD software can run on the same computer.

Which Java Virtual Machine is used by the Secure Desktop and the Cache Cleaner?

CSD checks Internet Explorer to determine which Java Virtual Machine (JVM) has been configured for that particular machine, and uses JVM to install the CSD components.

When do modified settings apply to the Cache Cleaner and the Secure Desktop?

When you modify the settings in the Secure Desktop Manager, you must deploy those settings by clicking the Apply All button in CSDM. The settings take effect the next time that a user starts either the Cache Cleaner application or the Secure Desktop application.

Do I need Administrator privileges to use the CSD features?

Administrator privileges are not required, but they are recommended.

Does the Secure Desktop Manager support Japanese character encodings?

The Secure Desktop Manager supports encoding such as the Shift_JIS, provided that you configure support for it using ASDM (Configuration > VPN > WebVPN > Encoding) or the remote user configures encoding using the browser (View > Encoding or View > Character Encoding).

What does transparent handling of e-mail applications mean?

The use of the term *transparent* means that the Secure Desktop handles e-mail the same way that the local desktop handles it. Transparent handling works for the following e-mail applications:

- Microsoft Outlook Express
- Microsoft Outlook
- Eudora
- Lotus Notes

Which applications does the Secure Desktop handle transparently?

Secure Desktop provides transparent handling of Outlook, Outlook Express, Eudora, and Notes.

Timeout Questions

The following questions address timeout settings with the Secure Desktop and the Cache Cleaner:

How does the timeout setting work on the Secure Desktop?

The timeout setting is independent of the desktop on which the user is operating. If you set a timeout of 1 minute and the remote user switches to the Local Desktop and works there beyond the 1-minute setting, the Secure Desktop closes at the end of the minute. Depending upon other settings, CSD saves the data to a Vault or erases it from the disk. Also, CSD uninstalls the Secure Desktop software if you configure it to do so.

Do Macintosh and Linux have a timeout setting?

Yes, you can set a time-out for the Macintosh & Linux Cache Cleaner.

Vault and Secure Desktop Questions

The following questions address the use of the Secure Desktop and Vault features:

Does Secure Desktop completely eliminate the risk that data will be left behind on a system?

No. CSD diligently works to remove data from a remote system. However, Microsoft operating system limitations or installed malicious software may prevent CSD from completely removing all traces of a session from a remote system.

Can I use uninstallation and Vault reuse with the Secure Desktop?

No; if you uninstall the application, the Secure Desktop always automatically deletes the vault. To avoid unintended results, do not configure both of these options simultaneously.

If I enable Vault reuse, how large is the download the second time?

When you enable Vault reuse, the majority of the program is downloaded. The next time the remote user reaches the site, only a small application downloads (approximately 40 KB in size).

How does an end user use the Vault after downloading it the first time?

Once you have downloaded and installed the Secure Desktop, it appears as an entry in the Start menu. Users who want to reuse the Vault can click **Start** > **Programs** > **Cisco Secure Desktop** and enter the password with which they protected the Vault.

Can I run multiple Secure Desktops at the same time?

The current release does not support multiple Secure Desktops.

System Detection Questions

The following questions address System Detection:

Can CSD detect all keystroke loggers?

CSD works diligently to detect keystroke loggers. There may be instances where CSD is unable to detect a particular keystroke logger, including but not limited to hardware keystroke logging devices.

For System Detection, what is the AND/OR relationship among the various settings?

System Detection is either enabled or disabled. If it is enabled, you can then enable or disable each of following categories:

- Antivirus software
- Antispyware software
- Personal firewall software
- Service packs

If you enable more than one category, the end user's computer must pass in each category to pass the System Detection check. An "AND" relationship is present among the enabled categories.

The options within each category have an "OR" relationship. For example, you can specify that any one of a list of antivirus software programs be running, and even if you have checked all of them as possible candidates, having just one of them running is enough to satisfy the antivirus software requirement.

Which antivirus applications does System Detection support?

The antivirus applications that System Detection checks for includes:

- Avast AntiVirus (4.0)
- AVG AntiVirus (7.0)
- eTrust Antivirus (7.0 to 2005)
- F-Secure Antivirus (2003 to 2005)
- McAfee VirusScan (8.0 to 10.0, Enterprise 7.0 to 8.0)
- Norton AntiVirus For Windows (Corporate 8.0 to 9.0, Professional 2004 to 2005)
- Panda AntiVirus (Titanium 2004 or Platinum 7.0 to 8.0)
- PC-cillin 2003 or 2004

Which antispyware applications does System Detection support?

The antispyware applications that System Detection checks for includes:

- Microsoft Anti-Spyware
- Anonymizer AntiSpyware

Which personal firewall applications does System Detection support?

The personal firewall applications that System Detection checks for includes:

- Cisco Security Agent (4.0 to 4.5)
- Internet Connection Firewall (ICF) (Windows XP to XP SP2)
- ISS BlackICE PC Protection (3.6)
- McAfee Personal Firewall (4.0 to 5.0)

- Norton Personal Firewall (2003 to 2005)
- Sygate Personal Firewall (5.0 to 5.6)
- ZoneAlarm Personal Firewall (4.0 to 5.5)

Which personal operating systems does System Detection support?

The operating systems and service packs that System Detection checks for include:

- Windows XP Service Pack 2
- Windows XP Service Pack 1
- Windows XP (no service pack)
- Windows 2000 Service Pack 4
- Windows 2000 Service Pack 3
- Windows 2000 Service Pack 2
- Windows 2000 Service Pack 1
- Windows 2000 (no service pack)
- Windows NT Service Pack 6
- Windows Millennium Edition
- Windows 98 Second Edition

Security Questions

The following questions address the Secure Desktop and the Cache Cleaner security settings and encryption level.

What security settings do I need to set on user computers?

The following Internet Explorer settings are required for CSD. Use these settings as a guideline for other browsers:

To access and launch the executable page:

- Scripting > Active scripting > Enable
- Downloads > File download > Enable

To launch ActiveX:

- Scripting > Active scripting > Enable
- ActiveX controls and plug-ins > Download signed ActiveX controls > Enable
- ActiveX controls and plug-ins > Run ActiveX controls and plug-ins > Enable

To launch Java using the Microsoft Virtual Machine:

- Scripting > Active scripting > Enable
- Scripting > Scripting of Java applets > Enable
- ActiveX controls and plug-ins > Download signed ActiveX controls > Enable

- Microsoft VM > Java permissions > High, medium or low safety

What kind of encryption do the Secure Desktop and Cache Cleaner use?

CSD encrypts data with 168-bit 3DES. Erasure of the cache meets U.S. Department of Defense standards.

Data Encryption Standard (DES) is an algorithm for protecting data using private encryption keys. DES-CBC is the Cipher Block Chaining (CBC) mode of DES, a stronger form of encryption; it applies an exclusive OR to each block of data with the previous block and then encrypts the data using the DES encryption key. 3DES or Triple DES, the strongest form of encryption, uses different keys to encrypt each data block three times.

How long can the password be for Vault reuse?

The password can be up to 127 characters, and can include any combination of upper and lower case letters, plus numbers and punctuation symbols, including spaces.

What happens when the cache is cleaned, either by the Cache Cleaner or the Secure Desktop?

The Cache Cleaner or the Secure Desktop sanitizes the system, disabling or erasing all data that was downloaded, inserted, or created in the browser including file downloads, configuration changes, cached browser information, entered passwords, and auto-completed information.

Networking and Firewall Questions

The following questions address networking aspects of the Secure Desktop and the Cache Cleaner, and their interaction with personal firewalls such as Sygate Security Agent and Sygate Personal Firewall:

Does the Secure Desktop or Cache Cleaner detect a second network card for location determination?

No, they detect only the IP address of the first network card.

I am using a personal firewall. What application must I “Allow” to access the network?

You must allow the program main.exe to access the network.

INDEX