



Cisco Secure Desktop Configuration Guide

for Cisco ASA 5500 Series Administrators

Software Release 3.2
June 2007

Americas 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: 408 527-0883

Text Part Number: OL-8607-03

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.

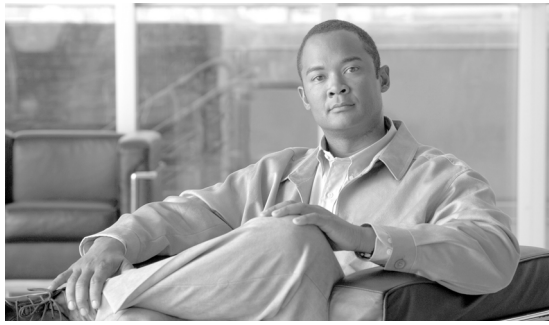
CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

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

© 2007 Cisco Systems, Inc. All rights reserved.



CONTENTS

About This Guide	vii
Audience and Scope	vii
Organization and Use	vii
Conventions	viii
Related Documentation	viii
Obtaining Documentation, Obtaining Support, and Security Guidelines	viii

CHAPTER 1

Introduction	1-1
Cisco Secure Desktop Capabilities	1-1
About Endpoint Profiles	1-2
Introduction to Secure Desktop Manager	1-3
Saving and Resetting the Running Configuration	1-6
Interoperability	1-7
Operating Systems	1-7
OS Detection	1-7
OS Interoperability	1-8
Browsers	1-8
Clientless SSL VPN	1-8
AnyConnect Client	1-9

CHAPTER 2

Installing and Enabling Cisco Secure Desktop	2-1
Installing or Upgrading Cisco Secure Desktop	2-1
Enabling or Disabling Cisco Secure Desktop	2-3
Entering an Activation Key to Support Advanced Endpoint Assessment	2-4
Configuring CSA Interoperability with the AnyConnect Client and Cisco Secure Desktop	2-4
Uninstalling Cisco Secure Desktop	2-5

CHAPTER 3

Configuring Cisco Secure Desktop for Microsoft Windows Computers	3-1
Understanding Prelogin Assessments and Endpoint Profiles	3-1
Configuring the Prelogin Assessment	3-4
Checking for a Registry Key	3-4
Checking for a File	3-7

- Checking for a Certificate 3-9
- Checking for the Windows Version 3-11
- Checking for an IP Address 3-12
- Modifying the Prelogin Assessment Configuration 3-13
- Assigning Settings to an Endpoint Profile 3-13
- Configuring Secure Session and Cache Cleaner for an Endpoint Profile 3-14
 - Configuring Keystroke Logger and Host Emulator Scanning for an Endpoint Profile 3-14
 - Configuring Cache Cleaner for an Endpoint Profile 3-17
 - Configuring Secure Desktop (Secure Session) General for an Endpoint Profile 3-19
 - Configuring Secure Desktop (Secure Session) Settings for an Endpoint Profile 3-21
 - Configuring the Secure Session Browser for an Endpoint Profile 3-23
- Configuring Host Scan 3-24
 - Configuring Basic Host Scan Entries 3-25
 - Adding a File Check to the Basic Host Scan 3-25
 - Adding a Registry Key Check to the Basic Host Scan 3-26
 - Adding a Process Check to the Basic Host Scan 3-27
 - Enabling and Disabling Host Scan Extensions 3-28
 - Configuring Advanced Endpoint Assessment 3-28
 - Configuring Personal Firewall Rules 3-31
- Configuring a Dynamic Access Policy 3-32

CHAPTER 4

Configuring Cache Cleaner for Mac OS X and Linux Computers 4-1

APPENDIX A

Tutorial A-1

- Tutorial Overview A-1
- Configuring a Prelogin Assessment A-2
 - Configuring an Endpoint Profile and Prelogin Assessment for a Secure Computer A-2
 - Configuring an Endpoint Profile and Prelogin Assessment for a Home Computer A-6
 - Configuring an Endpoint Profile and Prelogin Assessment for a Public Computer A-8
- Assigning Secure Session and Cache Cleaner Settings for Each Endpoint Profile A-9
 - Enabling or Disabling Secure Session and Cache Cleaner A-9
 - Configuring Keystroke Logger Scanning A-10
- Configuring Cache Cleaner Support for Mac OS X and Linux A-13
- Assigning a DAP for Each Endpoint Profile A-13

APPENDIX B**Frequently Asked Questions B-1**

New Questions for Cisco Secure Desktop Release 3.2 **B-1**

What happened to the VPN feature policies? **B-1**

What are the minimum rights for Secure Session, Cache Cleaner, Host Scan, and KeyStroke Logger Scanning? **B-1**

What is the sequence of events when a remote computer connects? **B-1**

Must Secure Session install to check for malware? **B-2**

How does Host Scan work with dynamic access policies? **B-2**

What happened to Windows CE? **B-3**

Timeout Questions **B-3**

How does the timeout setting work on Secure Session? **B-3**

Do Mac OS X and Linux have a timeout setting? **B-3**

Which antivirus, antispware, and firewall applications does Host Scan support? **B-3**

Secure Session and Cache Cleaner Questions **B-4**

Does Secure Session completely eliminate the risk that data will be left behind on a system? **B-4**

If I enable Secure Session reuse, how large is the download the second time? **B-4**

How does an end user use Secure Session after downloading it the first time? **B-4**

Can I run multiple instances of Secure Session at the same time? **B-4**

Can Cisco Secure Desktop detect all keystroke loggers? **B-4**

What security settings do I need to set on user computers? **B-4**

What kind of encryption do Secure Session and Cache Cleaner use? **B-5**

How long can the password be for Secure Session reuse? **B-5**

What happens when the cache is cleaned, either by Secure Session or Cache Cleaner? **B-5**

Can I use fast user switching on Windows XP? **B-5**

Which Java Virtual Machine is used by Secure Session and Cache Cleaner? **B-6**

When do modified settings apply to Cache Cleaner and Secure Session? **B-6**

Does Secure Session support Japanese character encodings? **B-6**

What does transparent handling of e-mail applications mean? **B-6**

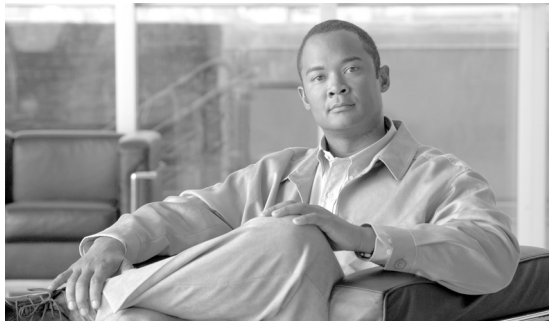
Which applications does the Secure Session handle transparently? **B-6**

Networking and Firewall Questions **B-6**

Does the Secure Session or Cache Cleaner detect a second network card for endpoint profile determination? **B-6**

I am using a personal firewall. What application must I "Allow" to access the network? **B-7**

INDEX



About This Guide

Refer to the following sections to understand the audience, topics, and conventions in this guide, and the titles of related documents.

Audience and Scope

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

Organization and Use

Table 1 describes the contents of this guide.

Table 1 **Document Organization**

Topic	Purpose
Introduction	Describes Cisco Secure Desktop capabilities, how to access the Cisco Secure Desktop Manager (the browser-enabled interface for Cisco Secure Desktop administrators).
Installing and Enabling Cisco Secure Desktop	Describes how to obtain the Cisco Secure Desktop software, and install or upgrade it.
Configuring Cisco Secure Desktop for Microsoft Windows Computers	Describes how to configure the prelogin assessment, Host Scan options, Secure Session, and Cache Cleaner for remote computers running Microsoft® Windows.
Configuring Cache Cleaner for Mac OS X and Linux Computers	Describes how to configure the Cache Cleaner for remote computers running Mac OS X or Linux.
Tutorial	Provides examples showing how to configure Cisco Secure Desktop.
Frequently Asked Questions	Provides questions and answers on a broad range of Cisco Secure Desktop 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*
- *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*
- *Cisco Security Appliance Logging Configuration and System Log Messages*

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>



Introduction

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

- [Cisco Secure Desktop Capabilities](#)
- [About Endpoint Profiles](#)
- [Introduction to Secure Desktop Manager](#)
- [Saving and Resetting the Running Configuration](#)
- [Interoperability](#)

Cisco Secure Desktop Capabilities

Cisco Secure Desktop seeks to minimize the risks posed by the use of noncorporate computers to establish a Cisco clientless SSL VPN or AnyConnect Client session. It does so by performing checks and scans that assess the safety of Microsoft Windows computers that attempt to establish a session, and associating dynamic access policies (DAPs) to the results.

As a condition for a VPN connection, the remote computer scans for a large collection of antivirus and antispyware applications, firewalls, operating systems, and associated updates. It also scans for any registry entries, filenames, and process names, collectively called a *basic host scan*, that you specify for Microsoft Windows computers. It sends the scan results to the security appliance. The security appliance uses the user's login credentials, the computer scan results, and endpoint profile match to assign a DAP.

With an Advanced Endpoint Assessment License, you can enhance the basic host scan by configuring an attempt to update noncompliant, Microsoft Windows computers to meet version requirements.

Secure Session (named "Secure Desktop" on the remote user interface) encrypts data and files associated with or downloaded during a remote session, into a secure desktop partition. Upon session termination, a U.S. Department of Defense (DoD) sanitation algorithm removes the partition. The protection provided by Secure Session is valuable in case of an abrupt session termination, or if the session times because of inactivity. Secure Session attempts to reduce the possibility that cookies, browser history, temporary files, and downloaded content remain after a remote user logs out or a session times out.

Secure Desktop Manager allows full customization of the conditions on which Secure Session and the other Cisco Secure Desktop features described in this chapter are loaded. It supports profiles of network element connection types (e.g., corporate laptop, home PC, or Internet kiosk) and applies different settings to each type if it is configured to do so. A simplified, graphical view simplifies the configuration of prelogin and periodic assessments of remote Microsoft Windows computers. As you use this graphical view to configure sequences of checks, link them to branches, deny logins, and assign endpoint profiles

to the results, Secure Desktop Manager records the changes to an XML file. You can configure the security appliance to use returned results in combination with many other types of data, such as the connection type and multiple group settings, to generate and apply a DAP to the session.

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 using Cisco Secure Desktop, 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.

About Endpoint Profiles

An *endpoint profile* specifies access rights you can assign to Microsoft Windows computers as they connect to the corporate network, depending on the results of prelogin assessments.

Endpoint profiles let you determine how PCs running Windows operating systems connect to your virtual private network, and protect it accordingly.

For example, PCs 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 PCs, you might set up an endpoint profile named Secure to match the IP addresses on the 10.x.x.x network, and disable the endpoint profile settings that enable the installation of Secure Session or Cache Cleaner.

In contrast, users' home PCs might be considered more at risk to viruses because of their mixed use. For these PCs, you might set up an endpoint profile named Home that is specified by a corporate-supplied certificate that employees install on their home PCs. This profile, when configured as one of the criteria of a DAP, would require the presence of antivirus and antispyware software to grant full access to the network.

Finally, for untrusted locations such as Internet cafes, you might set up an endpoint profile named "Public" that has either no matching criteria, thus making it the default profile for remote access devices that do not meet the requirements of more secure profiles; or you might define criteria that are less stringent. This profile would require a Secure Session installation, and include a short timeout period to prevent access by unauthorized users.

Cisco Secure Desktop evaluates remote access devices against the criteria in the sequence presented on the Windows Location Settings pane, and in combination with the configuration of dynamic access policies, grants privileges based on the first endpoint profile associated with the matched criteria.

Before configuring Cisco Secure Desktop, examine the Secure Desktop (Secure Session), Cache Cleaner, and DAP attribute descriptions to plan a configuration that meets the security requirements of your network policies.

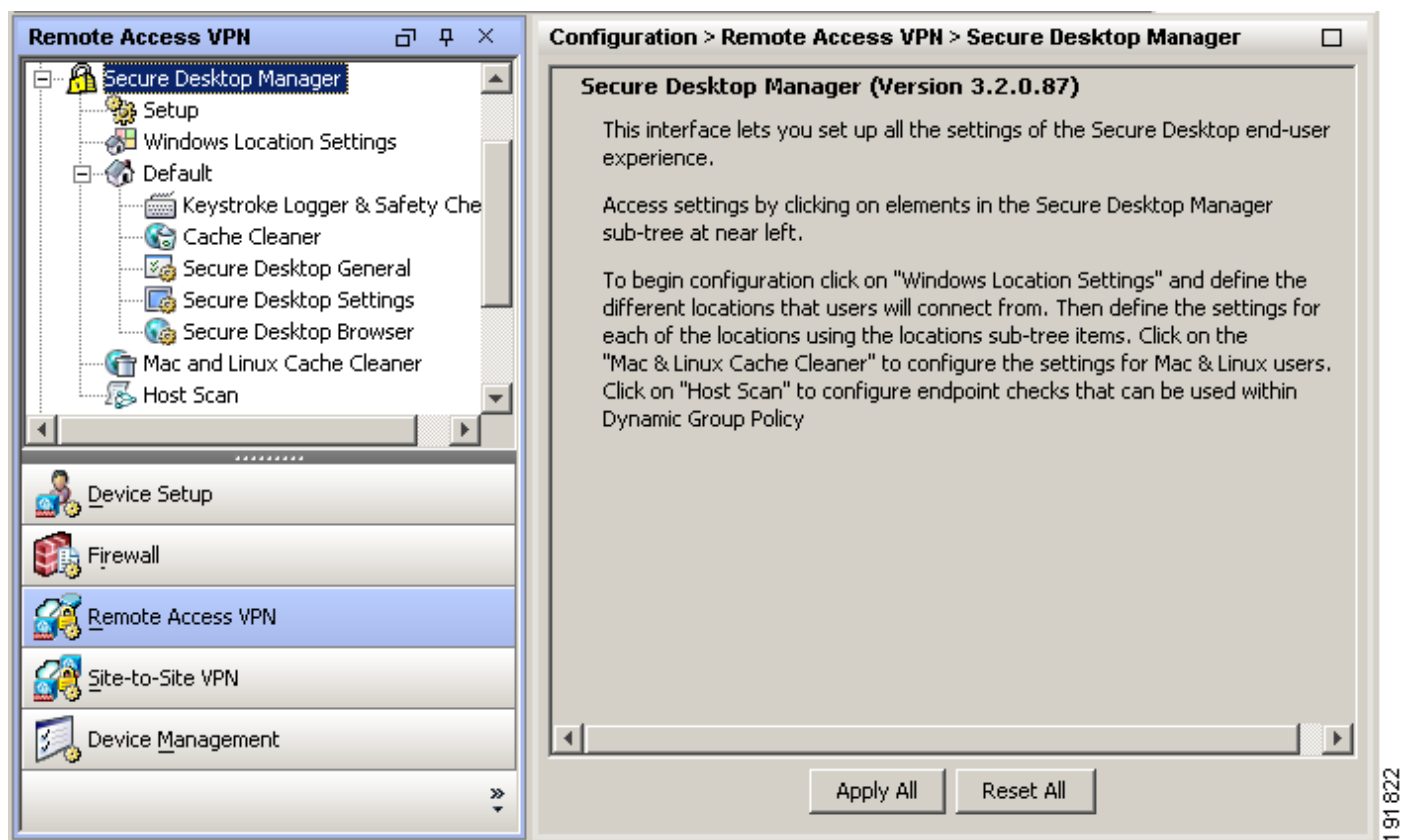
Introduction to Secure Desktop Manager

Use Secure Desktop Manager to configure Cisco Secure Desktop on the security appliance. After installing and enabling Cisco Secure Desktop, choose **Configuration > Remote Access VPN > Secure Desktop Manager**.

The Secure Desktop Manager pane opens. When Cisco Secure Desktop is disabled, only the Setup menu option is present. This option lets you enable Cisco Secure Desktop.

Figure 1-1 shows the fully-expanded, default menu and the Secure Desktop Manager pane, which appears after you install and enable Secure Desktop, exit the ASDM connection, and establish a new ASDM connection.

Figure 1-1 Secure Desktop Manager (Initial)



The following options are present in the Secure Desktop Manager menu:

- **Setup**—Lets you retrieve a Cisco Secure Desktop image from your computer and install the image, replace and install the existing image with a newer or older one, uninstall the image, and enable or disable Cisco Secure Desktop.
- **Windows Location Settings** — Click to specify or view the prelogin assessment of Microsoft Windows computers, and add, view, rename, or remove the endpoint profiles to be applied to remote computers that pass the prelogin assessment.

By default, the Windows Location Settings diagram has only one endpoint profile named Default. For every endpoint profile in the Windows Location Setting diagram, Secure Desktop Manager adds a tree of the same name to the menu on the left. You can view and change the settings assigned to an endpoint profile by clicking its name in the menu and by clicking any options below and indented to the right of the Default option.

Computers connecting from remote locations typically have or lack properties that signify their security state. Thus, you may want to create endpoint profiles such as “Secure,” “Home,” and “Public” to provide network access that is appropriate for the degree to which the connecting PC complies with your safety requirements. Use the Windows Location Settings option to not only create the endpoint profiles, but specify the conditions the remote PC must satisfy to qualify for an endpoint profile assignment. For example, you can configure the assignment of the Secure endpoint profile to remote computers with DHCP-assigned IP addresses within the corporate address range.

After you create an endpoint profile, you can configure the Keystroke Logger and Safety Checks, and Secure Desktop (Secure Session) or Cache Cleaner settings for that profile.

- Mac & Linux Cache Cleaner — Click to configure the Cache Cleaner for remote computers running Mac OS X or Linux operating systems.

Cisco Secure Desktop does not support endpoint profiles for computers running Mac OS X or Linux operating systems; however, it does support a limited set of security features for those platforms.

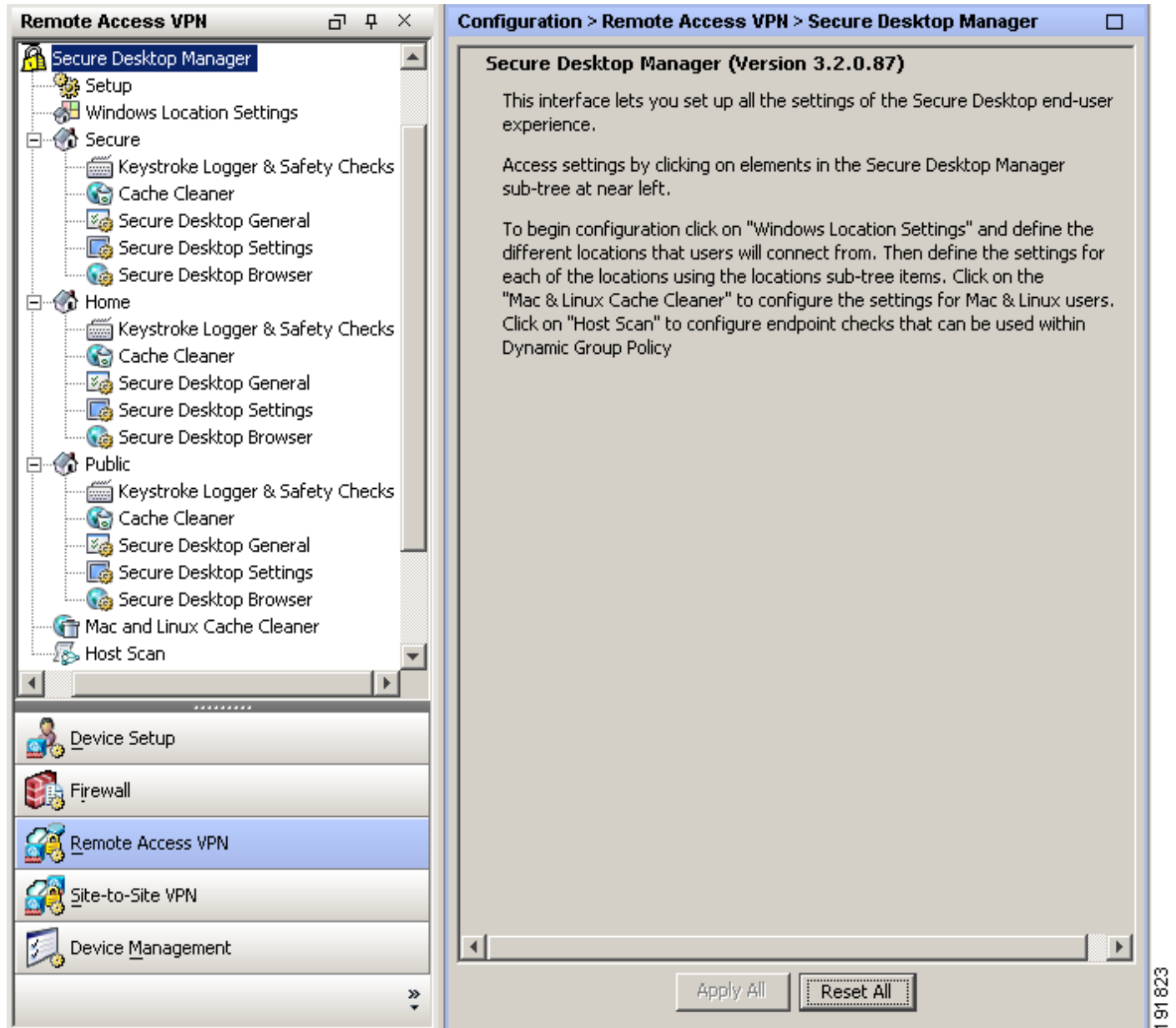
- Host Scan—Click to specify the registry entries, files, and processes to scan for following the prelogin assessment; also click to include a scan for antivirus, personal firewall, and antispyware applications and updates that are running on the remote PC. The scan for these items is called a *Basic Host Scan*. Finally, you can click this option to configure updates of noncompliant PCs if you have an Advanced Endpoint Assessment License. The enforcement of updates, combined with the Basic Host Scan, is called *Host Scan Extensions*. Both the Basic Host Scan and Host Scan Extensions require the endpoint to run Microsoft Windows.

Following the configuration of the endpoint profiles and host scan options, you can configure a match of any one or any combination of the following Host Scan results to assign a dynamic access policy following the user login:

- operating system
- endpoint profile (also called a policy)
- registry key
- file
- process
- antivirus application
- personal firewall application
- antispyware application

Figure 1-2 shows a Secure Desktop Manager menu populated with endpoint profiles named Secure, Home, and Public.

Figure 1-2 Navigating the Secure Desktop Manager



A *endpoint profile* is a security profile you can assign to computers running Microsoft Windows as they connect to the corporate network. (Endpoint profiles apply to Microsoft Windows users only.) As an administrator, you specify the criteria to match the remote computer to the endpoint profile. Eligible matching criteria include certificate name and authority, IP address range, and local file or registry requirements. As an administrator, you can assign a dynamic access policy (DAP) specifying user access rights to remote computers that match the criteria of an endpoint profile.

Endpoint profiles allow deployment of the Cisco Secure Desktop functions on a location-specific basis. Typical location types include Secure, Home, and Public (for such connection sites as an Internet cafe). You can use Secure Desktop Manager to define as many endpoint profiles as needed. Each profile has its own options and settings.

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

- **Keystroke Logger & Safety Checks**—Enables and disables scans of the remote PC for keystroke logging applications and a host emulator. You can configure an endpoint profile to require a scan for keystroke logging applications and a host emulator on the remote PC. You can list the keystroke logging applications that are safe or let the remote user interactively approve of the applications the scan identifies. Secure Session 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. The keystroke logger detection 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. Cache Cleaner supports the following:
 - WebLaunch of Cisco AnyConnect on a PC running Windows 2000 or XP.
 - Clientless (browser-based) SSL VPN connections with Microsoft Internet Explorer 5.0 or later on Windows 98, 2000, XP, and Vista.
 - Clientless SSL VPN connections with Internet Explorer 5.2 or later, or Safari 1.0 or later, on Mac OS X.
 - Clientless SSL VPN connections with Mozilla 1.7 or later on Red Hat Linux v9.

Cache Cleaner does not support the standalone startup of AnyConnect Client from any computer.

- **Secure Desktop General**—Provides an encrypted space (Secure Session) for Windows 2000 and Windows XP users, within which the user has an online session using a browser. Secure Session 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. Secure Desktop Manager does provide an option that seeks to disable printing from within a user session.
- **Secure Desktop Settings**—Lets you place restrictions on the Secure Session.
- **Secure Desktop Browser**—Specifies the home page to which the browser connects when the remote user establishes a session. This option also lets you specify the folders and bookmarks (or “favorites”) to insert into the respective browser menu during the session.

Saving and Resetting the Running Configuration

Secure Desktop Manager saves all Cisco Secure Desktop 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 Cisco Secure Desktop to copy the `disk0:/sdesktop/data.xml` file into the running configuration.

The security appliance stores the settings displayed in the Secure Desktop Manager > Setup pane. Secure Desktop Manager stores the remaining settings in the `disk0:/sdesktop/data.xml` file. Secure Desktop Manager displays two buttons at the bottom of the panes beginning with Secure Desktop Manager > Windows Location Settings for interacting with that file. Use these buttons as follows:

- To save the running Cisco Secure Desktop configuration to the `data.xml` file, click **Apply All**.

- To overwrite all settings in the running Cisco Secure Desktop configuration with those stored in the data.xml file, click **Reset All**.

An “Unapplied Changes” dialog box prompts you to save the Cisco Secure Desktop 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.

Interoperability

The following sections list the operating systems and browsers the Cisco Secure Desktop components support on clientless SSL VPN and AnyConnect sessions:

- [Operating Systems](#)
- [Browsers](#)
- [Clientless SSL VPN](#)
- [AnyConnect Client](#)

Operating Systems

The following sections list the operating systems identified by the OS Detection module of Cisco Secure Desktop, and list which ones the other Secure Desktop modules support.

OS Detection

OS Detection reports the following operating systems and service packs for DAP assignment:

- Microsoft Windows Vista
- Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Service Pack 1
- Microsoft Windows XP (no service pack)
- Microsoft Windows Server 2003
- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows 2000 Service Pack 3
- Microsoft Windows 2000 Service Pack 2
- Microsoft Windows 2000 Service Pack 1
- Microsoft Windows 2000 (no service pack)
- Microsoft Windows 98 Second Edition
- Linux
- MacOS X

OS Interoperability

Table 1-1 shows which operating systems the Cisco Secure Desktop modules support.

Table 1-1 *Operating Systems Supported by Cisco Secure Desktop*

Operating Systems ¹	Prelogin Assessment	Host Scan	Secure Session	Cache Cleaner ²
Microsoft Windows Vista	Y	–	–	Y
Microsoft Windows XP	Y	Y	Y	Y
Microsoft Windows 2000	Y	Y	Y	Y
Apple Macintosh OS X 10.4 (PowerPC or Intel)	–	–	–	Y
Linux	–	–	–	Y

1. Includes both English and non-English support for 32-bit Microsoft operating systems. Cisco Secure Desktop does not support the 64-bit versions.
2. Cache Cleaner also supports WebLaunch of Cisco AnyConnect on a PC running Windows 2000 or XP.

Browsers

Table 1-2 shows the Internet browsers that Secure Session and Cache Cleaner support. These modules may also work with other browsers.

Table 1-2 *Browsers Supported by Secure Session and Cache Cleaner*

Browsers	Secure Session	Cache Cleaner ¹
Internet Explorer 6.0 Service Pack 1	Y	Y
Internet Explorer 7.0	Y	Y
Mozilla 1.7. to 1.7.13	Y	Y
Mozilla Firefox 1.0	Y	–
Mozilla Firefox 1.5	Y	–
Mozilla Firefox 2.0	Y	–
Safari 1.0 to 1.3	–	Y
Safari 2.0	–	Y

1. Cache Cleaner also supports Clientless SSL VPN connections with Microsoft Internet Explorer 5.0 or later on Windows Vista, XP, 2000, and 98.

Clientless SSL VPN

Table 1-3 shows the interoperability of the Cisco Secure Desktop modules on remote computers establishing clientless (browser-based) SSL VPN sessions.

Table 1-3 *Clientless SSL VPN and Cisco Secure Desktop Interoperability*

Operating System ¹	Cisco Secure Desktop Remote Module			
	Prelogin Assessment	Host Scan	Secure Session	Cache Cleaner
Microsoft Windows Vista	Yes	Yes	–	Yes
Microsoft Windows XP	Yes	Yes	Yes	Yes
Microsoft Windows 2000	Yes	Yes	Yes	Yes
Apple Macintosh OS X 10.4 (PowerPC or Intel)	–	–	–	Yes
Linux	–	–	–	Yes

1. Includes both English and non-English support for 32-bit Microsoft operating systems. Cisco Secure Desktop does not support the 64-bit versions.

AnyConnect Client

Table 1-4 shows the interoperability of the AnyConnect Client modes with Cisco Secure Desktop modules on remote computers.

Table 1-4 *AnyConnect Client and Cisco Secure Desktop Interoperability*

AnyConnect Client Mode (SBL must not be enabled) ¹	Operating System ²	Cisco Secure Desktop Remote Module			
		Prelogin Assessment	Host Scan	Secure Session	Cache Cleaner
Standalone	Microsoft Windows Vista	Yes	Yes	–	–
	Microsoft Windows XP	Yes	Yes	Yes	–
	Microsoft Windows 2000	Yes	Yes	Yes	–
	Apple Macintosh OS X 10.4 (PowerPC or Intel)	–	–	–	–
	Linux	–	–	–	–
WebLaunch	Microsoft Windows Vista	Yes	Yes	–	Yes
	Microsoft Windows XP	Yes	Yes	Yes	Yes
	Microsoft Windows 2000	Yes	Yes	Yes	Yes
	Apple Macintosh OS X 10.4 (PowerPC or Intel)	–	–	–	Yes
	Linux	–	–	–	Yes

1. By default, the Start Before Logon (SBL) feature of AnyConnect Client is disabled. Cisco Secure Desktop modules are not interoperable with AnyConnect Client if SBL is enabled.
2. Includes both English and non-English support for 32-bit Microsoft operating systems. Cisco Secure Desktop does not support the 64-bit versions.



Installing and Enabling Cisco Secure Desktop

This chapter describes how to perform the following tasks on the security appliance.

- [Installing or Upgrading Cisco Secure Desktop](#)
- [Enabling or Disabling Cisco Secure Desktop](#)
- [Entering an Activation Key to Support Advanced Endpoint Assessment](#)
- [Configuring CSA Interoperability with the AnyConnect Client and Cisco Secure Desktop](#)
- [Uninstalling Cisco Secure Desktop](#)

Installing or Upgrading Cisco Secure Desktop

Cisco Secure Desktop Release 3.2 requires ASA Release 8.0(2). You do not need to restart the security appliance after you install or upgrade Cisco Secure Desktop, however, you must exit and restart your ASDM connection to access Secure Desktop Manager.



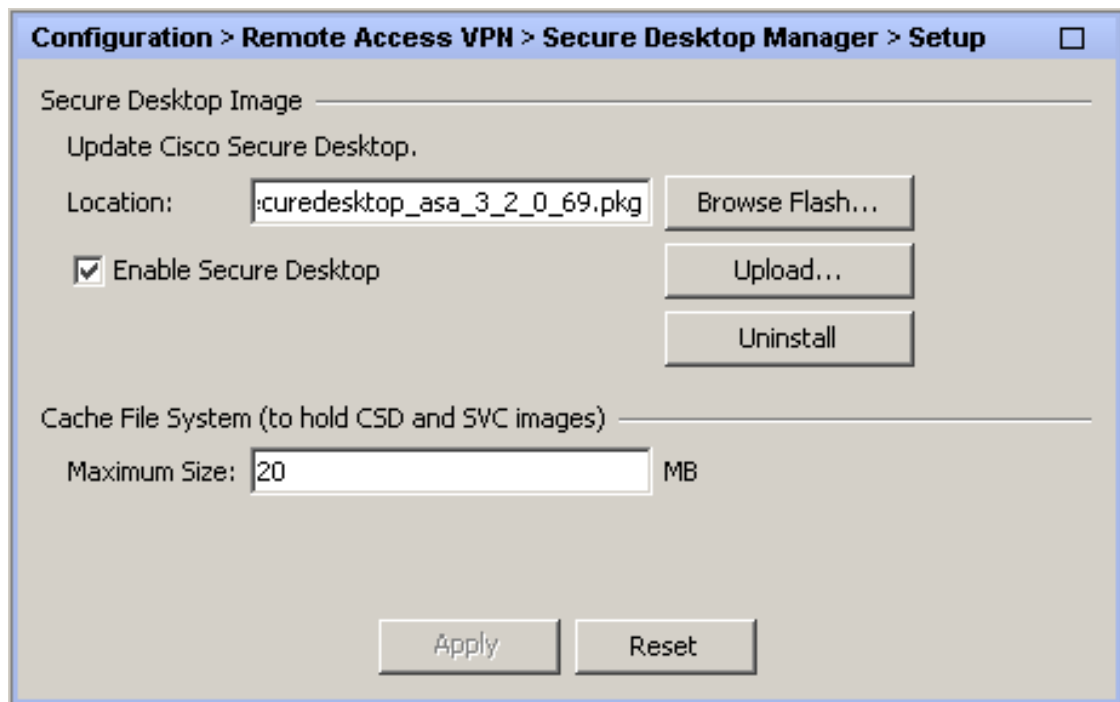
Note Archive and delete the Secure Desktop `desktop/data.xml` configuration file before upgrading to Cisco Secure Desktop 3.2. To create a clean configuration file, uninstall Cisco Secure Desktop before reinstalling it.

The expanded flexibility provided by a prelogin assessment sequence editor, and replacement of the Cisco Secure Desktop feature policies with a dynamic access policy (DAP) configured on the security appliance, are incompatible with Cisco Secure Desktop 3.1.1 configurations. Cisco Secure Desktop automatically inserts a new, default configuration file when it detects that one is not present.

Install or upgrade the Cisco Secure Desktop software on the security appliance as follows:

-
- Step 1** Use your Internet browser to access the following URL and download the `securedesktop_asa_<n>_<n>*.pkg` file to “My Documents” on your PC:
<http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop>
- Step 2** Establish an ASDM session with the security appliance.
- Step 3** Choose **Configuration > Remote Access VPN > Secure Desktop Manager > Setup**.
ASDM opens the Setup pane ([Figure 2-1](#)).

Figure 2-1 Setup



Step 4 Click **Upload** to prepare to transfer a copy of the Cisco Secure Desktop software from your local PC to the flash card installed in the ASA 5500.

ASDM opens the Upload Image dialog box.

Step 5 Click **Browse Local** to prepare to select the file on your local PC.

By default, the Selected File Path dialog box displays the contents of the My Documents folder.

Step 6 Choose the **securedesktop_asa_<n>_<n>*.pkg** you downloaded in Step 1 and click **Select**.

ASDM closes the Select File Path dialog box.

Step 7 Click **Browse Flash** and enter the name of the **securedesktop_asa_<n>_<n>*.pkg** file you are uploading in the File Name field, then click **OK**.

Step 8 Click **Upload File**.



Caution Avoid opening other windows until you complete the remaining steps.

ASDM transfers a copy of the file to the flash card. An Information dialog box displays the following message:

File has been uploaded to flash successfully.

Step 9 Click **OK**.

ASDM clears the fields in the Upload Image dialog box.

Step 10 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 11 Click **OK**.

Step 12 Check **Enable Secure Desktop** if it is not already checked.

Step 13 Click **Apply**.

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

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

Step 14 Click **Yes** to remove the previous version from the flash memory card, and click **Proceed** in the Refresh Needed window.

If you choose to downgrade later, you can use the same method you used to upgrade (that is, upload and install it).

An ASDM Restart Confirmation window displays the following message:

```
The Secure Desktop image is successfully updated. The new features can be accessed after ASDM is restarted.
```

Step 15 Click **OK**.

Step 16 The Secure Desktop Manager menu closes.

If you reopen the menu, it shows only the Setup option.

Step 17 Click the **X** in the upper right corner of the ASDM window to exit.

A window displays the following message:

```
The configuration has been modified. Do you want to save the running configuration to flash memory?
```

Step 18 Click **Save**.

ASDM saves the configuration and closes.

Step 19 Establish a new ASDM session with the security appliance to customize the Secure Desktop Manager configuration.

Enabling or Disabling Cisco Secure Desktop

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

Disabling Cisco Secure Desktop does not alter the Cisco Secure Desktop configuration.

Use ASDM to enable or disable Cisco Secure Desktop as follows:

Step 1 Choose **Configuration > Clientless SSL VPN > Secure Desktop > Setup**.

ASDM opens the Setup pane (Figure 2-1).



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

- Step 2** Check or uncheck **Enable Secure Desktop** and click **Apply**.
ASDM enables or disables Cisco Secure Desktop.
-

Entering an Activation Key to Support Advanced Endpoint Assessment

Advanced Endpoint Assessment includes all of the Endpoint Assessment features, and lets you configure an attempt to update noncompliant computers to meet version requirements. You can use ASDM to activate a key to support Advanced Endpoint Assessment after acquiring it from Cisco, as follows:

- Step 1** Choose **Device Management > System Image/Configuration > Activation Key**.
Step 2 Enter the key in the New Activation Key field.
Step 3 Click **Update Activation Key**.
Step 4 Choose **File > Save Running Configuration to Flash**.

An Advanced Endpoint Assessment entry appears and the Configure button becomes active in the Host Scan Extensions area of the **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan** pane, which is accessible only if Cisco Secure Desktop is enabled.

Configuring CSA Interoperability with the AnyConnect Client and Cisco Secure Desktop

If your remote users have Cisco Security Agent (CSA) installed, you must import new CSA policies to the remote users to enable the AnyConnect VPN Client and Cisco Secure Desktop to interoperate with the security appliance.

To do this, follow these steps:

- Step 1** Retrieve the CSA policies for the AnyConnect client and Cisco Secure Desktop. You can get the files from:
- The CD shipped with the security appliance.
 - The software download page for the ASA 5500 Series Adaptive Security Appliance at <http://www.cisco.com/cgi-bin/tablebuild.pl/asa>.
- The filenames are AnyConnect-CSA.zip and CSD-for-CSA-updates.zip
- Step 2** Extract the .export files from the .zip package files.
- Step 3** Choose the correct version of the .export file to import. The Version 5.2 export files work for CSA Versions 5.2 and higher. The 5.x export files are for CSA Versions 5.0 and 5.1.
- Step 4** Import the file using the Maintenance > Export/Import tab on the CSA Management Center.

Step 5 Attach the new rule module to your VPN policy and generate rules.

For more information, see the CSA document *Using Management Center for Cisco Security Agents 5.2*. Specific information about exporting policies is located in the section *Exporting and Importing Configurations*.

Uninstalling Cisco Secure Desktop

Uninstalling Cisco Secure Desktop removes the Cisco Secure Desktop configuration file (data.xml) from the sdesktop directory on the flash card. If you want to retain the file, copy it using an alternative name or download it to your workstation before you uninstall Cisco Secure Desktop.

Uninstall Cisco Secure Desktop on the security appliance as follows:

Step 1 Establish an ASDM session with the security appliance.

Step 2 Choose **Configuration > Remote Access VPN > Secure Desktop Manager > Setup**.

ASDM opens the Setup pane ([Figure 2-1](#)).

Step 3 Click **Uninstall**.

A confirmation window displays the following message:

```
Do you want to delete disk0:/securedesktop_asa_3_2_0_87.pkg and all CSD data files?
```

Step 4 Click **Yes**.

ASDM removes the text from the Location text box and removes the Secure Desktop Manager menu options below Setup.



Configuring Cisco Secure Desktop for Microsoft Windows Computers

See the following sections to configure Cisco Secure Desktop for remote PCs running Microsoft Windows:

- [Understanding Prelogin Assessments and Endpoint Profiles](#)
- [Configuring the Prelogin Assessment](#)
- [Assigning Settings to an Endpoint Profile](#)
- [Configuring Secure Session and Cache Cleaner for an Endpoint Profile](#)
- [Configuring Host Scan](#)
- [Configuring a Dynamic Access Policy](#)

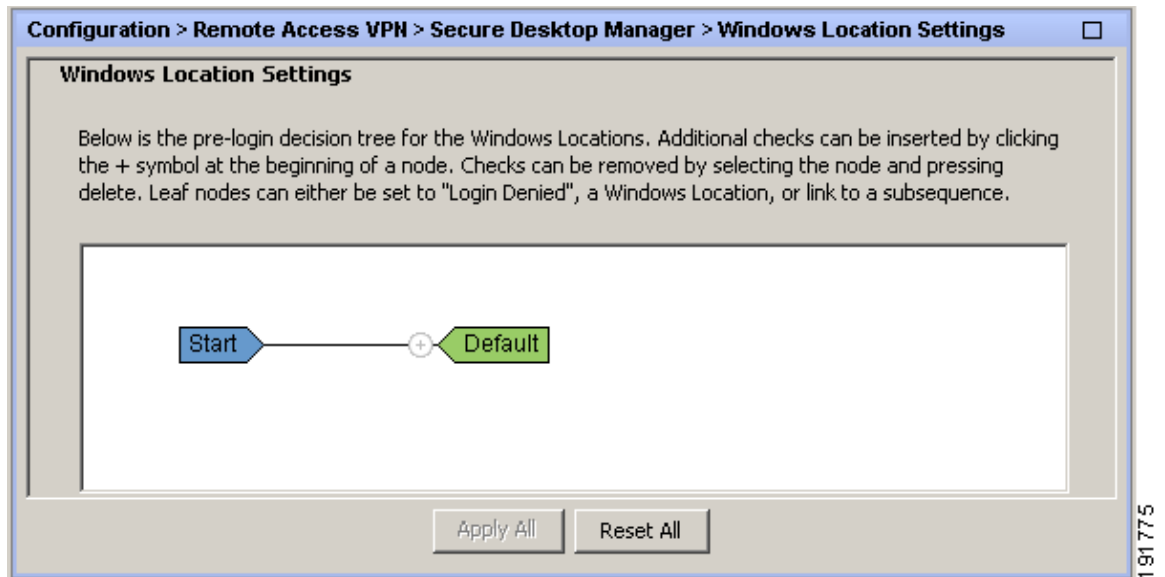
Understanding Prelogin Assessments and Endpoint Profiles

Secure Desktop Manager lets you specify the checks to be performed between the time the user establishes a connection with the security appliance and the time the user enters the login credentials. These checks determine whether to assign an endpoint profile or whether to display a “Login Denied” message for the remote user. The settings of the matched endpoint profile determine whether Secure Session or Cache Cleaner loads. The incorporation of the endpoint profile in a dynamic access policy (DAP) determines the access rights and restrictions placed on the connection.

To view the prelogin assessments present in the configuration, choose **Secure Desktop Manager > Windows Locations Settings**.

Figure 3-1 shows the default prelogin assessment configuration, including the default endpoint profile named “Default.”

Figure 3-1 Default Elements in the Windows Location Settings Pane



By default, the Windows Location Settings pane displays the following elements:

- **Start**—Displayed in blue, this node provides a visual indication of the beginning of the sequence of checks to be performed. You cannot edit the start node.
- **Line**—Provides a visual indication of the conditional relationship of the node to its left and the one that follows. You cannot move or remove a line.
- **Plus sign**—Click to insert a prelogin check between the two nodes on either side of the line. Secure Desktop Manager lets you insert the following types of checks:
 - **Registry**—Lets you detect the presence or absence of a registry key.
 - **File**—Lets you specify the presence or absence of a particular file, its version, and its checksum.
 - **Certificate**—Lets you specify the issuer of a certificate and one certificate attribute and value to match.

For each additional attribute of a single certificate that you want to match, create another prelogin check that specifies that attribute and value.
 - **Windows Version**—Creates two login checks; Windows 2000, XP, and Vista; and Win 9x (for Windows 98). The editor inserts a Failure line and Login Denied end node for remote connections that fail both operating system checks.
 - **IP Address**—Lets you specify an IP address range or subnet mask.
- **Default Location Type**—Displayed in green, this end node assigns the endpoint profile named “Default.” By default, Cisco Secure Desktop assigns this profile to every remote computer running Windows Vista, XP, 2000, and 98.

If you insert a check before an end node, Secure Desktop Manager automatically assigns at least one instance of each of the following:

- **Success tag** to the line leading from the new check to the endpoint profile that is already present.
- **Failure tag** to a second line leading from the new check to a “Login Denied” node. This node, displayed in brown, indicates that a “Login Denied” response appears after the user enters the login credentials; Cisco Secure Desktop denies the user access to the security appliance.

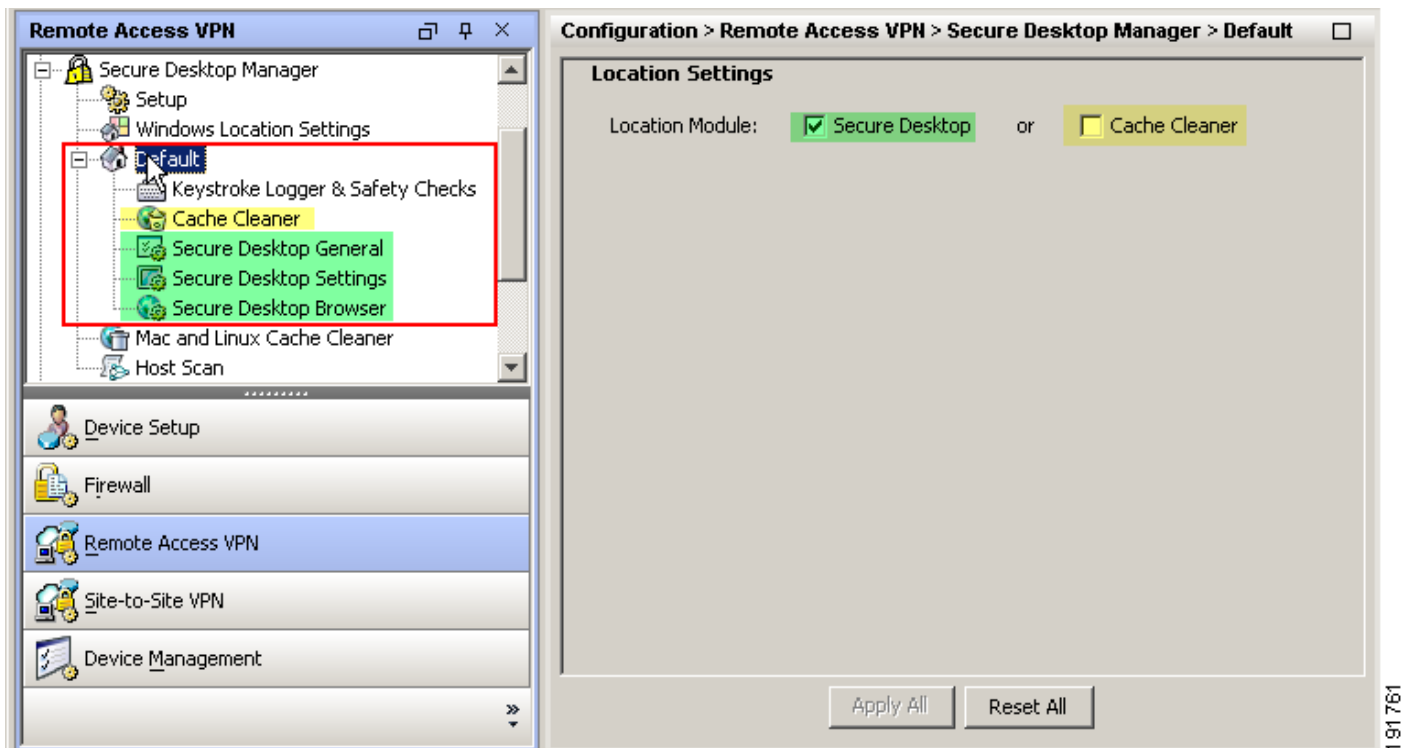
You can change the name or type of any node except for the Start node. You can change an end node following a Success tag to be a Login Denied node, and the end node following a Failure tag to be an endpoint profile. You can also change either type of end node to a *subsequence* node. Displayed in blue, this node indicates a continuation to another blue node vertically aligned under the Start node. To assign a subsequence to a set of conditions, click an end node, then click Subsequence. You must assign a unique name to each subsequence you create. Secure Desktop Manager assigns the name to both instances of the subsequence node—the one at the end of the branch—and the one at the beginning of the new branch. You might want to create a subsequence for any of the following reasons:

- Restart a branch on the left side to reduce horizontal scrolling.
- Create a set of conditions that have an overall purpose that you want to document by using the subsequence name.
- Reuse a subsequence.

To do so, type the name of the subsequence that is already present when you are changing an end node to a subsequence node.

An endpoint profile determines the desktop experience. To view the settings assigned to an endpoint profile, note its name in the green end node of the Windows Location Settings pane, click an option with the same name in the Secure Desktop Manager menu, note the location module that is enabled in the Location Settings pane (Figure 3-2), then click **KeyStroke Logger & Safety Checks** and any options associated with the enabled location module.

Figure 3-2 Location Settings



You can rename any endpoint profile, including the one named “Default.” To do so, return to the Windows Location Settings pane and click the “Default” node. Replace the text in the Label field with a name for an endpoint profile that is meaningful to you. For example, you may want to rename it “Secure” to indicate the profile applies to corporate PCs (that is, those that meet the most stringent

requirements, as determined by the checks to be inserted). Secure Desktop Manager automatically renames the node in the associated menu. You can then adjust the settings for the endpoint profile accordingly.

Configuring the Prelogin Assessment

When a remote PC attempts to establish a remote VPN connection, Cisco Secure Desktop automatically checks for the conditions you configure, and assigns the attribute settings of the endpoint profile associated with the result of the checks to the connection, or issues a Login Denied message.

Use the following sections to configure a prelogin assessment to be downloaded to the remote PC:

- [Checking for a Registry Key](#)
- [Checking for a File](#)
- [Checking for a Certificate](#)
- [Checking for the Windows Version](#)
- [Checking for an IP Address](#)
- [Modifying the Prelogin Assessment Configuration](#)

Checking for a Registry Key

Insert a check for a specific registry key on the remote host as follows:

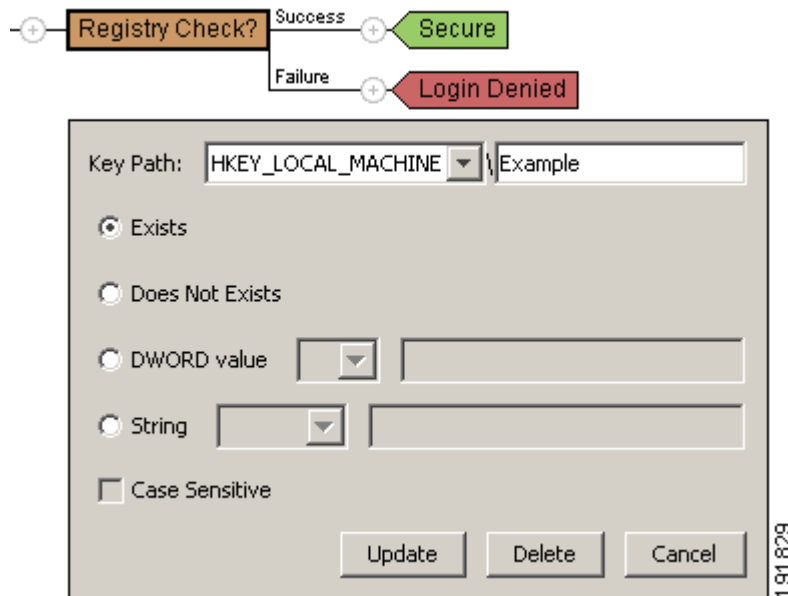
Step 1 Choose **Windows Location Settings**.

Step 2 Determine the position of the registry check to be inserted and click the associated plus sign. A window opens below the diagram, prompting you to select the type of check to be inserted.

Step 3 Choose **Registry Check** and click **Add**.

Secure Desktop Manager inserts the Registry Check node into the window and opens the Registry Check window ([Figure 3-3](#)).

Figure 3-3 Add Registry Check

**Tip**

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

Step 4 Assign values to the mandatory attributes in the Registry Check window as follows:

- **Key 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.

- **Key Path** field—Enter the name of the registry key required to be present on or absent from the remote PC.



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

Step 5 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 PC is sufficient to match the endpoint profile you are configuring.

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

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

- **Does not exist**—Click if the absence of the named registry key from the remote PC is sufficient to match the endpoint profile 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 an endpoint profile:

```
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 an option (<, <=, =, >, or >=) to specify the relationship of the Dword value of the registry key to the value to be entered to the right.
- **DWORD value** field—Enter a decimal to compare with the Dword value of the registry key on the remote PC.

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
 - matches
 - differs
- **String value** field—Enter a string to compare with the String value of the registry key on the remote PC.

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 remote PC to match the case used in the String value field to satisfy the criterion.

Step 6 Click **Update**.

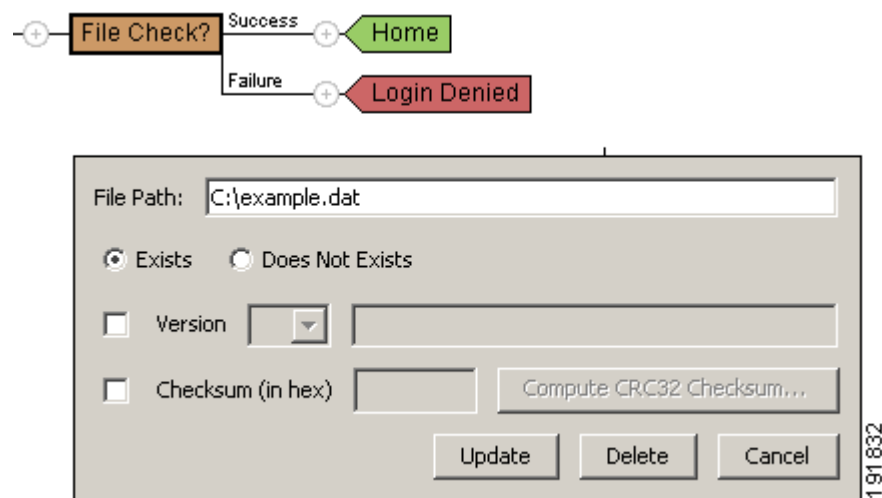
Checking for a File

The file criterion prelogin check lets you specify that a certain file must or must not exist to be eligible for the associated endpoint profile. For example, you might want to use a file prelogin check to ensure a corporate file is present or one or more peer-to-peer file-sharing programs containing malware are not present before assigning an endpoint profile.

Use the following procedure to insert a prelogin assessment for files on the remote PC:

-
- Step 1** Choose **Windows Location Settings**.
- Step 2** Determine the position of the file check to be inserted and click the associated plus sign. A window prompts you to select the type of check to be inserted.
- Step 3** Choose **File Check** and click **Add**. Secure Desktop Manager inserts the File Check node into the window and opens the File Check window (Figure 3-4).

Figure 3-4 File Check



- Step 4** Assign a value to the following mandatory attribute:
- **File Path**—Enter the directory path of the file.
For example,
`C:\Program Files\Cisco Systems\CSAgent\bin\okclient.exe`
- Step 5** Click one of the following mandatory radio buttons:
- **Exists**—Click if the file must be present on the remote PC.
 - **Does not exist**—Click if the file must be absent from the remote PC, then go to Step 7.
- Step 6** Use the following attributes if you want to specify the file version.
- **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 or is not a particular version.

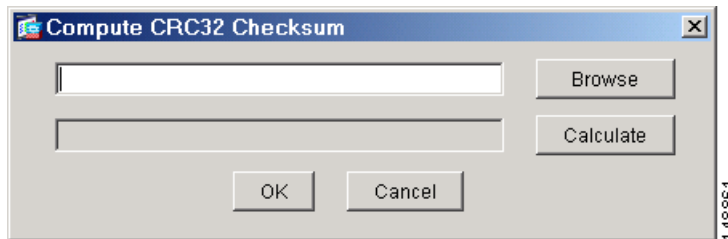


Note To display the version of an .exe file, use Windows Explorer to right-click the file, choose **Properties**, and click the **Version** tab.

- **Version** drop-down list—Choose an option (<, <=, =, >, or >=) to specify the relationship of the version of the file to the string to be entered to the right.
- **Version** field—Type a string to compare with the version of the file on the remote PC.
- **Checksum** check box—Check to specify a checksum to authenticate the file named in the Path field.
- **Checksum** field—Enter a checksum in hexadecimal format, beginning with 0x, or click **Compute CRC32 Checksum** to calculate the checksum of a file stored locally and insert the value in this field.

The Compute CRC32 Checksum dialog box opens (Figure 3-5).

Figure 3-5 Compute CRC32 Checksum



Retrieve the checksum as follows:

- 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.
- Click **Calculate**.
The field at the bottom of the Compute CRC32 Checksum dialog box displays the checksum in hexadecimal format.
- Click **OK**.
The Compute CRC32 Checksum dialog box closes and the hexadecimal value appears in the **Checksum** field.

Step 7 Click **Update** in the File Check window.

Checking for a Certificate

Insert a check for a specific certificate on the remote host as follows:

- Step 1** Use [Table 3-1](#) to prepare to identify the attribute and value to require, and to identify the issuer of the certificate. This table contains three procedures. Use the procedure in the column associated with the certificate you want to require.
- Column 1 shows how to view the values if you have a certificate file (such as one with a .cer or .pfx file extension).
 - Column 2 shows how to view the values if you have a signed file (that is, the file is not a certificate file, but contains a certificate).
 - Column 3 shows how to view the values if you have neither a certificate file nor a signed file.

Table 3-1 Viewing Certificate Attributes and Values

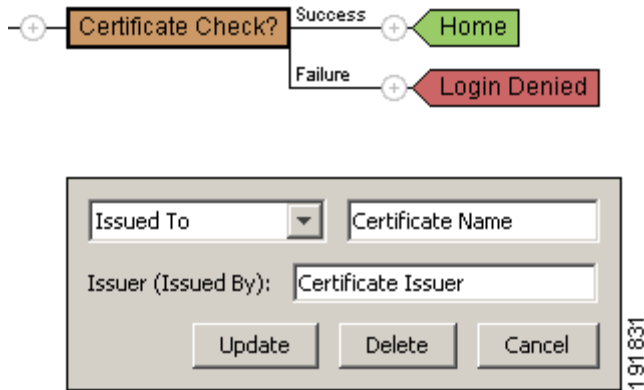
	Certificate File	Signed File	Your Store (your PC)
Step 1	Double-click the certificate.	Right click the file and choose Properties .	Open the Control Panel .
Step 2	Click the Details tab.	Click the Digital Signatures tab (which appears only if the file is signed).	Choose Internet Options .
Step 3	—	Click Details .	Click the Content tab.
Step 4	—	Click View Certificate .	Click Certificates .
Step 5	—	Click the Details tab.	Choose a certificate and click View .
Step 6	—	—	Click the Details tab.

Step 2 Go to the Secure Desktop Manager menu on ASDM and choose **Windows Location Settings**.

Step 3 Determine the position of the certificate check to be inserted and click the associated plus sign. A window opens below the diagram, prompting you to select the type of check to be inserted.

Step 4 Choose **Certificate Check** and click **Add**.

Secure Desktop Manager inserts the Certificate Check node into the window and opens the Certificate Check window ([Figure 3-6](#)).

Figure 3-6 Add Certificate Check

- Using the untitled drop-down list, choose the certificate attribute for which you want to specify a value to match to the certificate on the remote host.



Note Insert more than one certificate check if you want to require more than one attribute value match.

The options name the attributes in the Field column of the Details tab, as follows:

- Issued To
- Common Name
- Given Name
- Surname
- Country
- Locality
- State or Province
- Street Address
- Organization
- Organizational Unit
- Title
- Description
- Business Category
- Postal Address
- Postal Code
- Member
- Owner
- Role Occupant
- Initials
- Dn Qualifier

- Domain Component

- Step 5** Copy the string in the Value column to the right of the attribute name from the Details tab to the unnamed text box in the ASDM Add Certificate window.
- Step 6** Copy the string in the Value column to the right of Issuer from the Details tab to the Issuer text box in the ASDM Add Certificate window.
- Step 7** Click **Update**.

Checking for the Windows Version

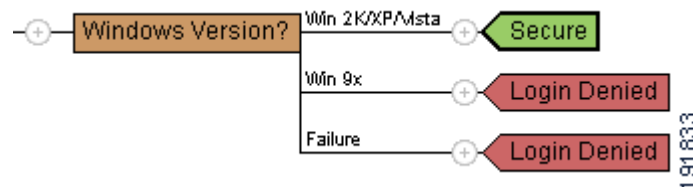
The prelogin assessment includes a check for the version of Windows running on a remote PC attempting to establish a VPN connection. When the user attempts to connect, however, Cisco Secure Desktop automatically checks for the Windows version, regardless of whether you insert a Windows version prelogin check. If the endpoint profile assigned to the connection has Secure Desktop (Secure Session) enabled and if the remote PC is running Windows 2000 or XP, it installs Secure Session, regardless of whether you insert a Windows version prelogin check. If the endpoint profile has Secure Desktop enabled and the operating system is Windows 98, or Vista, Windows Cache Cleaner runs instead because Secure Desktop supports only Windows 2000 and XP. Therefore, you should make sure the Cache Cleaner settings are appropriate for an endpoint profile, even if you configure Secure Desktop to run instead.

Although Cisco Secure Desktop automatically checks for the version of Windows, you may want to insert a Windows Version prelogin check as a condition for applying an endpoint profile.

Use the following procedure to insert a Windows version check:

- Step 1** Choose **Windows Location Settings**.
- Step 2** Determine the position of the Windows check to be inserted and click the associated plus sign.
A window prompts you to select the type of check to be inserted.
- Step 3** Choose **Windows Version Check** and click **Add**.
Secure Desktop Manager inserts the Windows Version check node into the diagram (Figure 3-7).

Figure 3-7 Windows Version Check



If you wish, you can click any Login Denied node to change it to an endpoint profile or a subsequence node.

Checking for an IP Address

You can insert a check for the IP address of the remote host attempting a VPN connection, into the prelogin assessment. If the IP address is within the number range or the range specified by the subnet mask you enter, the remote host passes the check; otherwise, it fails. For example, PCs 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 PCs, you might set up an endpoint profile named Secure that is specified by IP addresses on the 10.x.x.x network, and disable the endpoint profile settings that enable the installation of Cache Cleaner and Secure Session.



Note

If the PC has more than one IP address, Cisco Secure Desktop uses only the first address detected.

Use the following procedure to check for an IP address as part of a prelogin assessment:

Step 1 Choose **Windows Location Settings**.

Step 2 Determine the position of the IP address check to be inserted and click the associated plus sign.

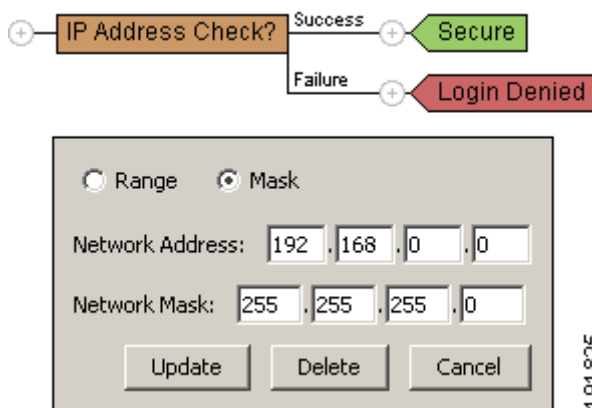
A window prompts you to select the type of check to be inserted.

Step 3 Choose **File Check** and click **Add**.

Step 4 Select **IP Address Check** and click **Add**.

Secure Desktop Manager inserts the IP Address Check node and opens the IP address check window below the diagram (Figure 3-8).

Figure 3-8 IP Address Check



Step 5 Choose one of the following options to indicate the type of IP address check:

- Click **Range** and enter the IP address in the Network Address field, leaving a 0 in one or more of the left-most fields to indicate the range.
- Click **Mask** and enter the subnet mask in the Network Mask field, leaving a 0 in one or more of the left-most fields to indicate the range.

Step 6 Click **Update**.

Modifying the Prelogin Assessment Configuration

To modify or delete any node in the Windows Location Settings window, click the node. With the exception of the Start and Windows Version nodes, Secure Desktop Manager inserts the window associated with the node type that opened when you created the node. Make the changes as needed and click **Update**, or click **Delete** to remove the node from the configuration.

To delete a Windows version node, click the node, select the option (Win2k/XP/Vista, Win 9x, or Failure) next to the “Which branch should replace node attribute,” then click **Delete**.

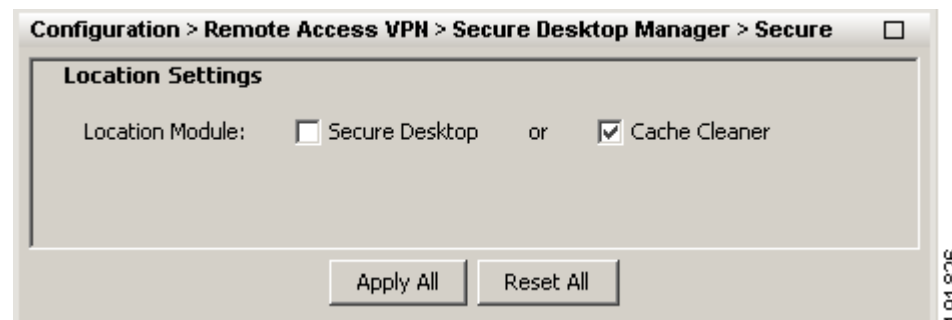
To insert a prelogin check, click the plus sign located in the position where you want to insert the check. Secure Desktop Manager inserts the window that lets you specify the check you want to insert. After doing so, click **Add**. Use the instructions in the previous section to set the attributes in the check type window and click **Update**.

To change the type and name of any end node, double click the end node, click **Login Denied**, **Location**, or **Subsequence** to change the node type, type the name of the node in the Label field if it is of type Location or Subsequence, and click **Update**.

Assigning Settings to an Endpoint Profile

Click the name of the endpoint profile in the Secure Desktop Manager menu. The Location Settings pane opens (Figure 3-9).

Figure 3-9 Location Settings



This pane lets you specify the main settings for an endpoint profile.

Check one of the following:

- Secure Desktop—To install Secure Session on the remote PC.



Note If you check Secure Desktop and configure Secure Desktop settings, you should still configure the Cache Cleaner as well. The Cache Cleaner serves as a fall-back security solution for Windows 98 and Vista, which Secure Session does not support.

- Cache Cleaner—To install Cache Cleaner on the remote PC.
- Neither Secure Desktop nor Cache Cleaner—Uncheck both options if the PC is secure (for example, if the PC is a corporate computer) or you do not want either module to load.

Regardless of which option you check, Host Scan loads if it contains Basic Host Scan entries or one or both Host Scan extensions are checked.

Configuring Secure Session and Cache Cleaner for an Endpoint Profile

Refer to the following sections to define the Cisco Secure Desktop experience for PCs that match the criteria defined for a specific endpoint profile:

- [Configuring Keystroke Logger and Host Emulator Scanning for an Endpoint Profile](#)
- [Configuring Cache Cleaner for an Endpoint Profile](#)
- [Configuring Secure Desktop \(Secure Session\) General for an Endpoint Profile](#)
- [Configuring Secure Desktop \(Secure Session\) Settings for an Endpoint Profile](#)
- [Configuring the Secure Session Browser for an Endpoint Profile](#)

Configuring Keystroke Logger and Host Emulator Scanning for an Endpoint Profile

Keystroke logger scanning is disabled by default for each endpoint profile. If you enable scanning and a scan detects unapproved keystroke loggers, neither Secure Session nor Cache Cleaner launches. Alternatively, the keystroke logger scanning configuration lets you determine whether the user can interactively approve of applications the scan identifies. It also lets you create an exception list which lists applications to ignore when scanning for keystroke loggers.

Host emulation detection is also disabled by default for each endpoint profile. If you enable host emulation detection and a scan determines that the remote operating system is running over virtualization software, neither Secure Session nor Cache Cleaner launches. Alternatively, you can configure the Cisco Secure Desktop to alert the user about the host emulator and let the user opt to prevent Secure Session or Cache Cleaner from installing.

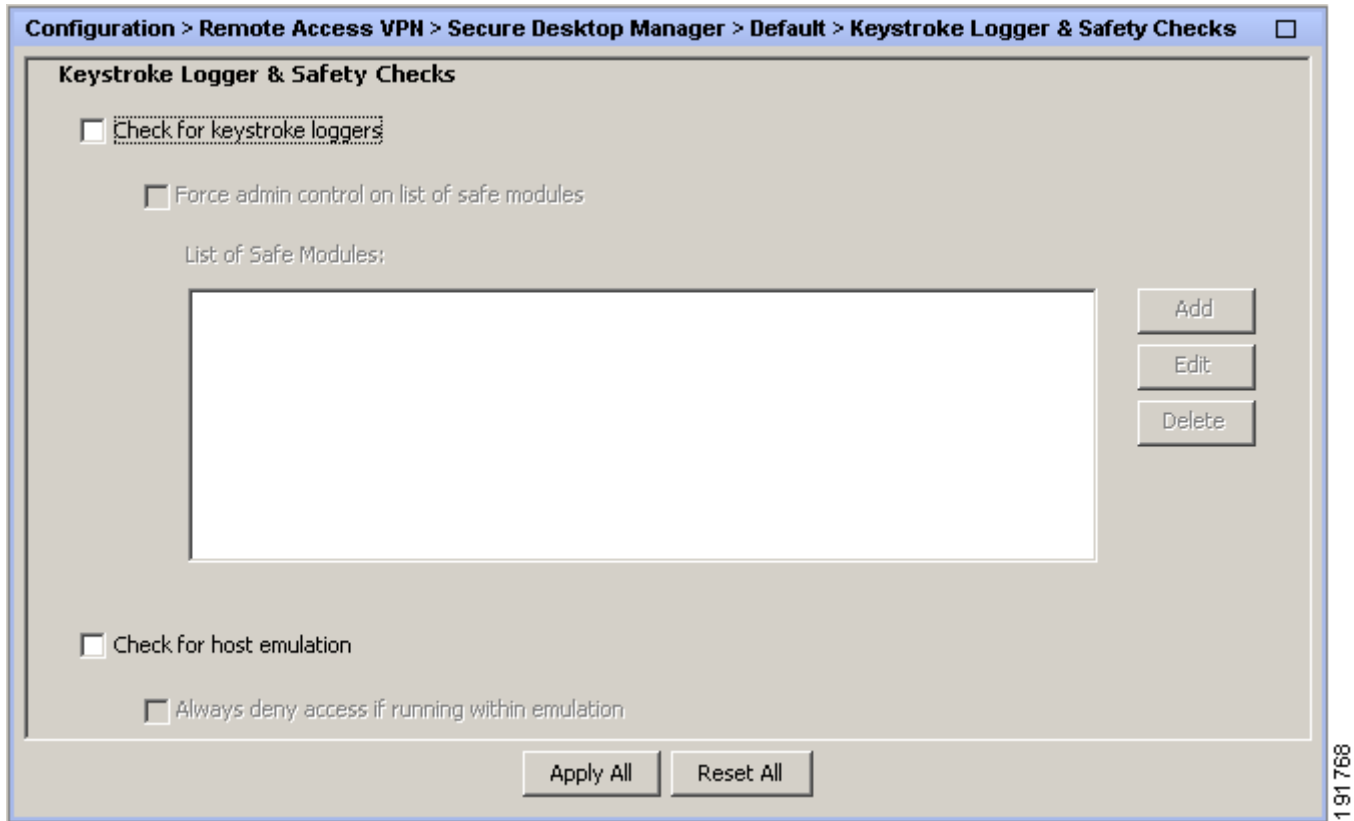
It may not be possible to detect all keystroke loggers present, including hardware keystroke logging devices, and all host emulators.

Configure scanning for keystroke loggers as follows:

-
- Step 1** Click **Keystroke Logger & Safety Checks** under the name of the endpoint profile you are configuring in the menu on the left.

The Keystroke Logger window opens ([Figure 3-10](#)).

Figure 3-10 Keystroke Logger Window



The “List of Safe Modules” window lists the paths to program applications on the remote PC 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 PC and make sure one is not running, before installing Secure Session.

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, Cisco Secure Desktop lists the keystroke loggers discovered on the remote PC. To access Secure Session, 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.

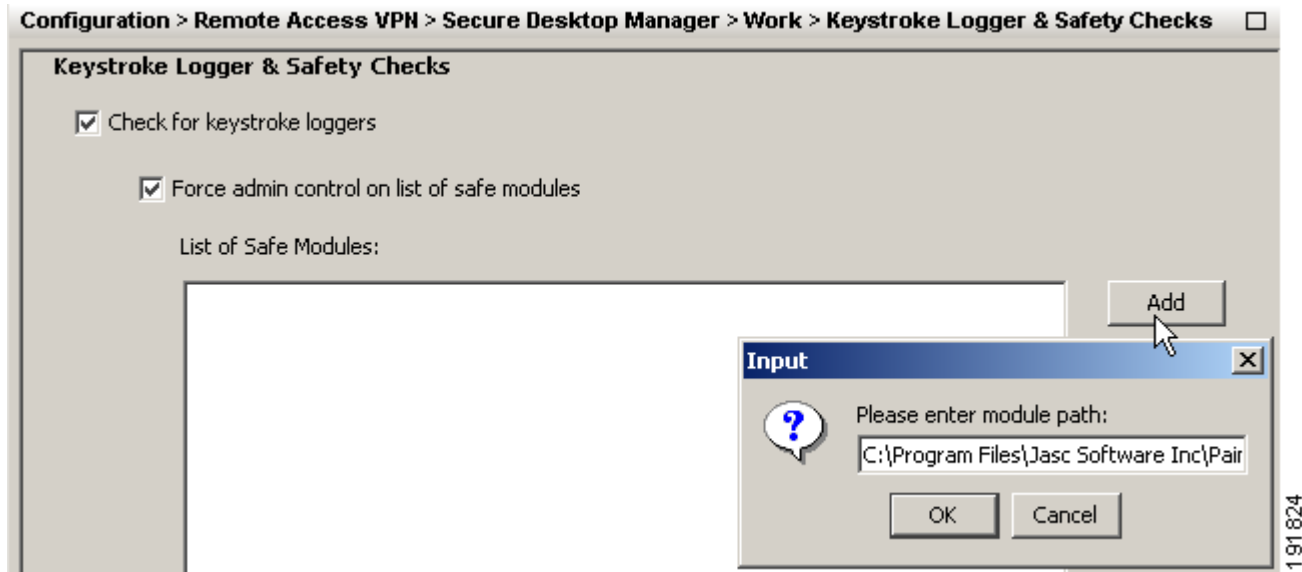


Note Unchecking this attribute deactivates but does not delete the contents of the “List of Safe Modules” window.

- 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.

Cisco Secure Desktop Manager opens the Input dialog box (Figure 3-11).

Figure 3-11 Input (for Keystroke Logger)



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

Cisco Secure Desktop Manager 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** Check **Check for host emulation** if you want to determine whether the operating system is running over virtualization software, such as VMWare.
- Step 7** Check **Always deny access if running within emulation** to prevent Secure Session or Cache Cleaner from installing if Cisco Secure Desktop detects that the operating system is running over virtualization software. Uncheck this attribute to alert the user about the host emulation software and let the user opt to prevent Secure Session or Cache Cleaner from installing.
- Step 8** Click **Apply All** to save the configuration changes.

Configuring Cache Cleaner for an Endpoint Profile

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. Cache Cleaner for Windows supports the following:

- WebLaunch of Cisco AnyConnect on a PC running Windows 2000 or XP.
- Clientless (browser-based) SSL VPN connections with Microsoft Internet Explorer 5.0 or later on Windows Vista, XP, 2000, and 98.

Cache Cleaner does not support the standalone startup of AnyConnect Client from any computer.

For each endpoint profile for which either Secure Desktop (Secure Session) or Cache Cleaner is enabled, click **Cache Cleaner** under the profile you are configuring. The Cache Cleaner pane appears.

Figure 3-12 shows the default settings.

Figure 3-12 Cache Cleaner for Windows

Configuration > Remote Access VPN > Secure Desktop Manager > Default > Cache Cleaner

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: minute(s)

Launch cleanup upon closing of all browser instances or SSL VPN connection

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

Secure Delete: pass(es)

This window lets you configure the Cache Cleaner for the associated endpoint profile. 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 PC, so that you know that the user has the Cache Cleaner installed. For example, you could place a cookie file on the user's PC, 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 the remote PC 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.
- 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 session begins.
- Secure Delete—Secure Session writes the cache to the remote PC disk. Upon termination, it converts bits occupied by the cache to 0’s, then to 1’s, and finally to randomized 1’s and 0’s. Choose the number of times to perform this cleanup task. The default setting, 3 passes, meets the US Department of Defense (DoD) standard for securely deleting files. Following the completion of the task the number of times specified, Secure Session removes the pointer to the file (that is, performs a “Windows-delete”).

**Note**

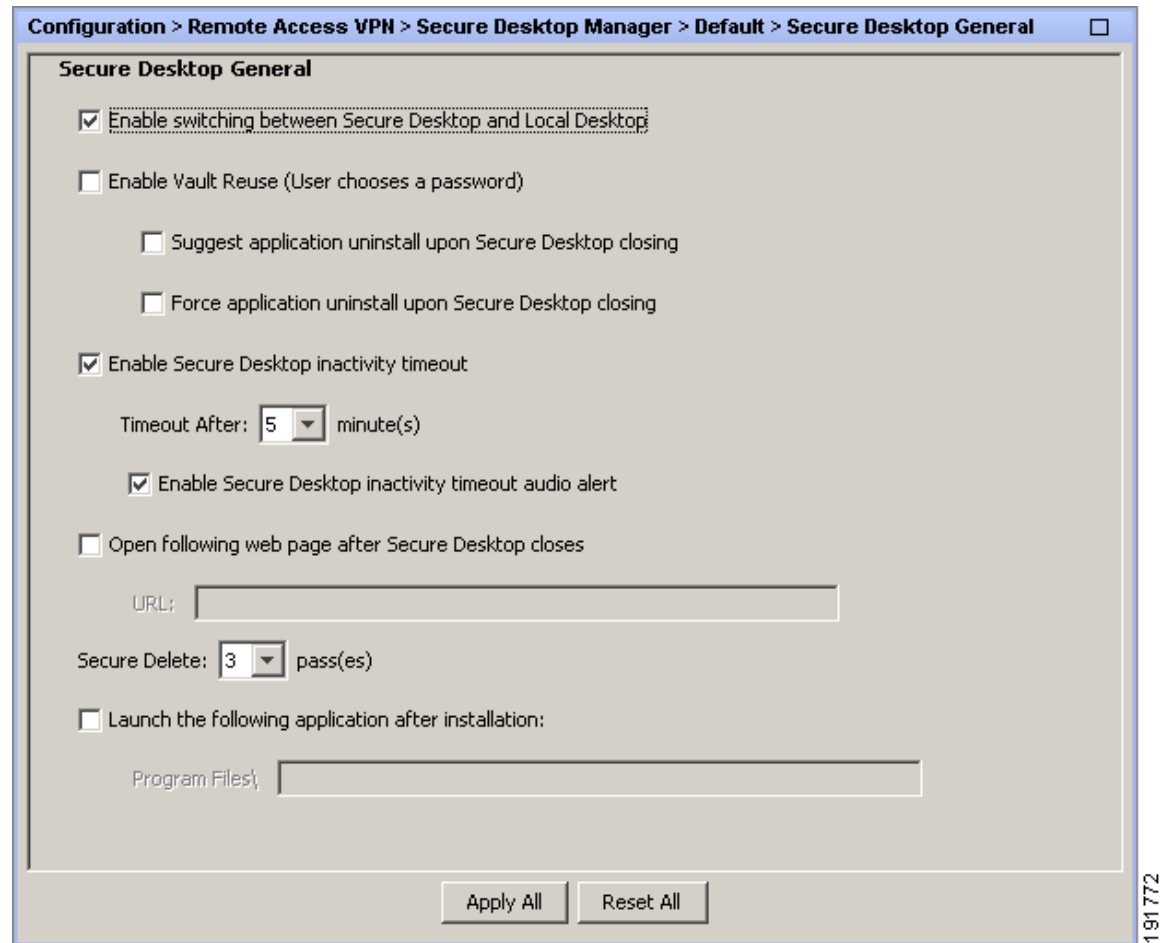
Click **Apply All** to save the running Cisco Secure Desktop configuration.

Configuring Secure Desktop (Secure Session) General for an Endpoint Profile

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

The Secure Desktop General pane appears. [Figure 3-13](#) shows the default settings.

Figure 3-13 Secure Desktop General



Check the following attributes to configure the general Secure Session settings for the endpoint profile you are configuring, as required by your security policy:

- **Enable switching between Secure Desktop and Local Desktop**—We strongly recommend that you check this attribute to let users switch between Secure Session 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 Secure Session continue processing. 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 Secure Session from enforcing prevention of desktop switching, even if you disable this feature.

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

- **Enable Vault Reuse**—Check to allow users to close Secure Session and open it again at a later time. Secure Session becomes 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) to restart Secure Session. This option is useful if users are running Secure Session on PCs that are likely to be reused; for example, a home PC. When a user closes Secure Session, it does not self-destruct. If you do not enable this option, Secure Session automatically self-destructs upon termination.

If unchecked, this attribute activates the following two attributes.

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



Note Checking this option uninstalls Secure Session from the remote PC when the user session closes, so leave this option disabled if access to the Secure Session is important.

- **Force application uninstall upon Secure Desktop closing**—Check if you do not want to leave Secure Session on untrusted PCs after users finish using it. Secure Session uninstalls when it closes.



Note Checking this option uninstalls Secure Session from the remote PC when the session closes, so leave this option disabled if access to Secure Session is important.

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

Secure Session detects inactivity and closes 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.
- **Open following web page after Secure Desktop closes**—Check this box and enter a URL in the field to make Secure Session automatically open a web page when it closes.
- **Secure Delete**—Secure Session encrypts and writes itself to the remote PC disk. Upon termination, Secure Session converts all bits it occupies to all 0’s, then to all 1’s, and then to randomized 0’s and 1’s. Choose the number of times 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, Secure Session removes the pointer to the file (that is, performs a “Windows-delete”).



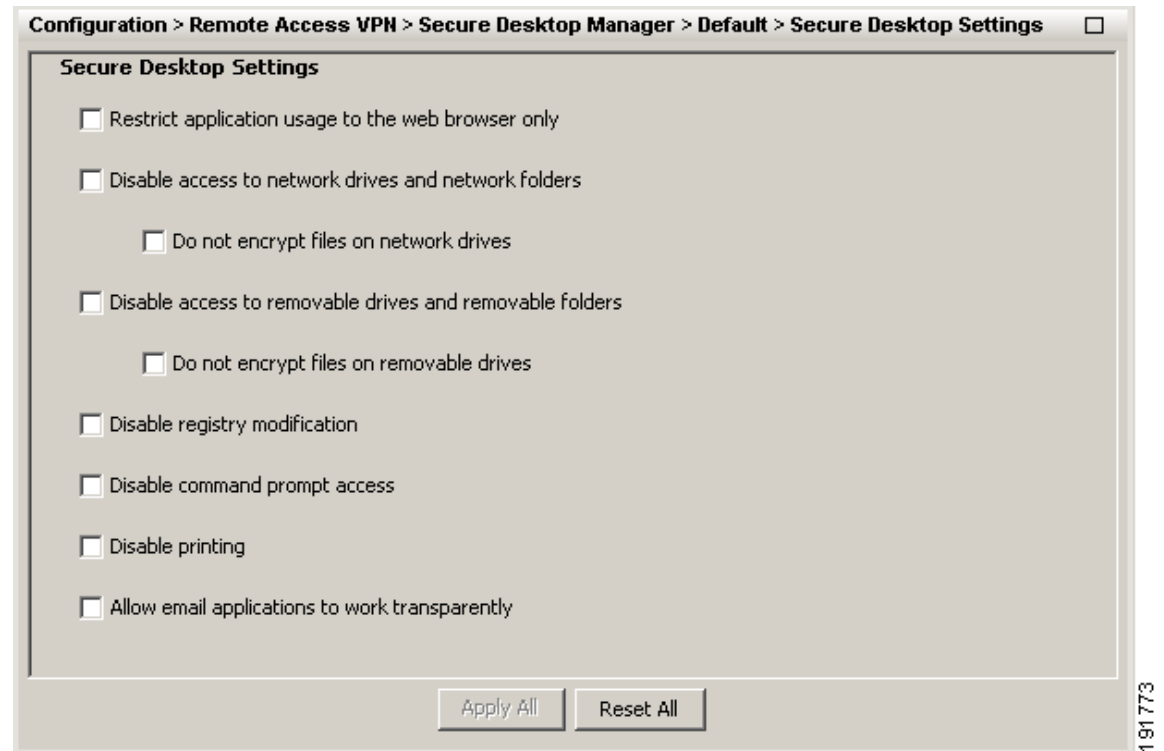
Note

Click **Apply All** to save the running Cisco Secure Desktop configuration.

Configuring Secure Desktop (Secure Session) Settings for an Endpoint Profile

Click **Secure Desktop Settings** under the endpoint profile name to place restrictions on Secure Session. The Secure Desktop Settings pane appears. [Figure 3-14](#) shows the default settings.

Figure 3-14 Secure Desktop Settings



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 Secure Session. If you choose this option, the browser that initiated the connection (Internet Explorer, Netscape, Firefox, etc.) is the only browser permitted to run. 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 running Secure Session. 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, Secure Desktop Manager dims the following attribute.
- Do not encrypt files on network drives—Check to let the user save files to network drives. Secure Session does not encrypt the files and leaves the files behind after the session ends. If you uncheck “Disable access to network drives and network folders” and this attribute, Secure Session encrypts the files the user saves to network drives, then removes them upon Secure Session termination. Secure Desktop Manager dims this attribute if you check the previous attribute.

191773

- Disable access to removable drives and removable folders—Check to prevent the user from accessing portable drives while running Secure Session. Otherwise, the user can save files to a removable drive and remove the drive before closing the session. After closing the session, the user could forget to take the removable drive. For maximum security, we recommend that you check this attribute. If you do, 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 let the user save files to portable drives that Microsoft names “Removable” in the Windows Explorer “My Computer” window. Secure Session does not encrypt the files and leaves the files behind after the session ends. If you uncheck both “Disable access to removable drives and removable folders” and this attribute, Secure Session encrypts the files the user saves to portable drives, then removes them upon session termination. Secure Desktop Manager dims this attribute if you check the previous attribute.
- Disable registry modification—Check to prevent the user from modifying the registry from within Secure Session. For maximum security, we recommend that you check this attribute.
- Disable command prompt access—Check to prevent the user from running the DOS command prompt from within Secure Session. For maximum security, we recommend that you check this attribute.
- Disable printing—Check to prevent the user from printing while using Secure Session. 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 Secure Session and to prevent it from deleting e-mail upon the termination of the session. The use of the term *transparent* means that Secure Session 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 Secure Session and the local desktop. Similarly, deleting such a file from within the e-mail application running over Secure Session removes the file from both desktops.



Note Deleting transparent or nontransparent files from outside of Outlook, such as from a Windows Explorer window, while in a Secure Session removes the file only from Secure Session.

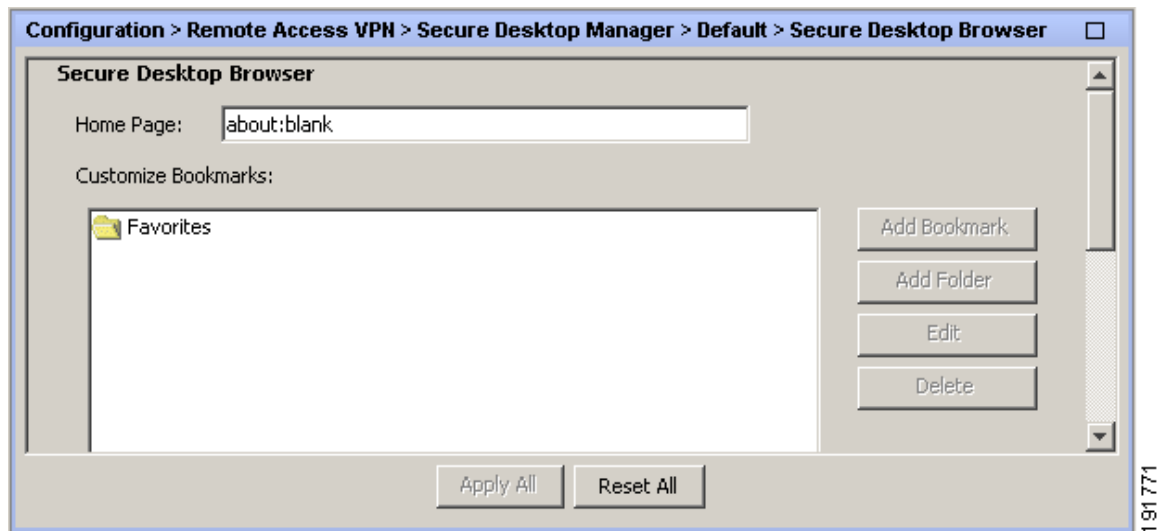
Click **Apply All** to save the running Cisco Secure Desktop configuration.

Configuring the Secure Session Browser for an Endpoint Profile

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

The Secure Desktop Browser pane appears. [Figure 3-15](#) shows the default settings.

Figure 3-15 Secure Desktop Browser



For the duration of the Secure 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 Secure 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

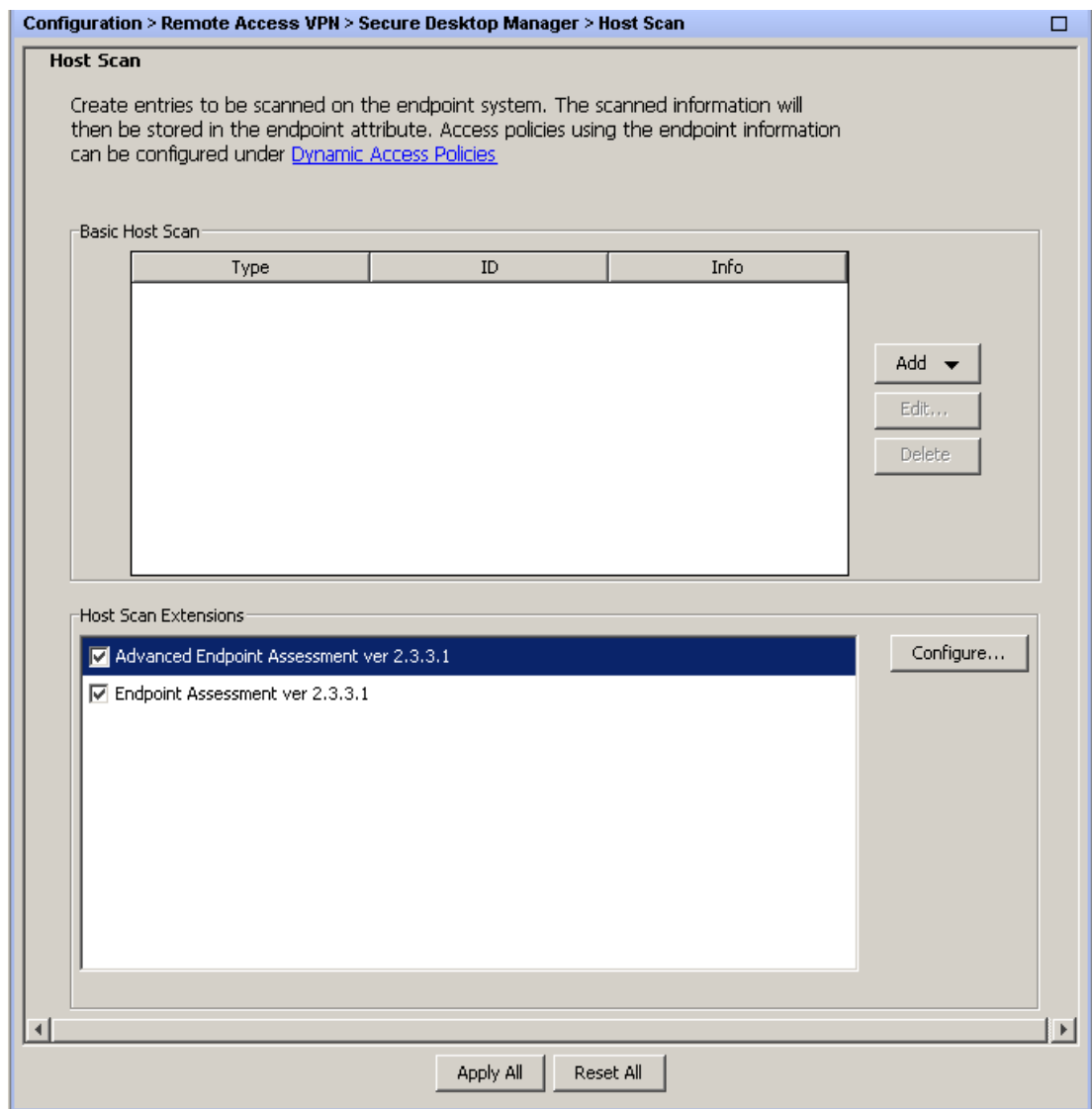
Click **Apply All** to save the running Cisco Secure Desktop configuration.

Configuring Host Scan

The **Secure Desktop Manager > Host Scan** window shown in [Figure 3-16](#) lets you do the following:

- To configure and view the registry entries, filenames, and process names for which to scan, see “[Configuring Basic Host Scan Entries.](#)”
- To enable or disable scanning for antispymware, antivirus, and personal firewall applications and updates, see “[Enabling and Disabling Host Scan Extensions.](#)”
- To configure enforcement of the antispymware, antivirus, and personal firewall applications and updates of your choice, see “[Configuring Advanced Endpoint Assessment](#)” and “[Configuring Personal Firewall Rules.](#)” This option requires an Advanced Endpoint Assessment license.

Figure 3-16 Host Scan



**Note**

Regardless of whether you have an Advanced Endpoint Assessment license, you can use ASDM to configure Dynamic Access Policies for making policy decisions based on the scan results.

Configuring Basic Host Scan Entries

You can specify a set of registry entries, filenames, and process names, collectively called a *basic host scan*. The host scan, which includes the basic host scan and the endpoint assessment, or advanced, endpoint assessment; occurs after the prelogin assessment but before the assignment of a DAP. Following the basic host scan, the security appliance uses the login credentials, the host scan results, endpoint profile, and other criteria you configure to assign a DAP.

See the sections that name the types of basic host scan entries you would like to configure:

- [Adding a File Check to the Basic Host Scan](#)
- [Adding a Registry Key Check to the Basic Host Scan](#)
- [Adding a Process Check to the Basic Host Scan](#)

Adding a File Check to the Basic Host Scan

Add a check for a specific file to the basic host scan as follows:

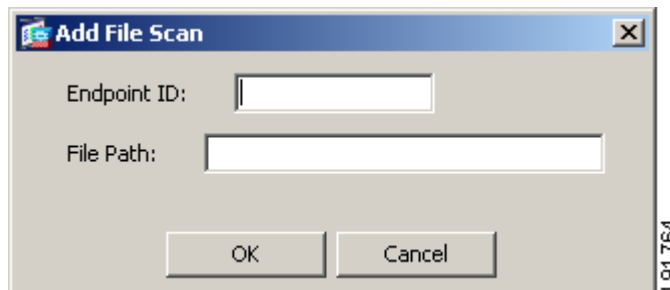
Step 1 Choose **Secure Desktop Manager > Host Scan**.

The Host Scan pane opens (Figure 3-16).

Step 2 Click **Add > File Scan**.

The Add File Scan pane opens (Figure 3-17).

Figure 3-17 Add File Scan



Step 3 Assign values to the following attributes:

- **Endpoint ID**—Enter a unique and meaningful string to serve as an index to this entry. After completing the Host Scan configuration, specify the same index when you assign this entry as an endpoint attribute when configuring a DAP. The string is case-sensitive.

For example,

`file-okclient.exe`

- **File Path**—Enter the directory path of the file.

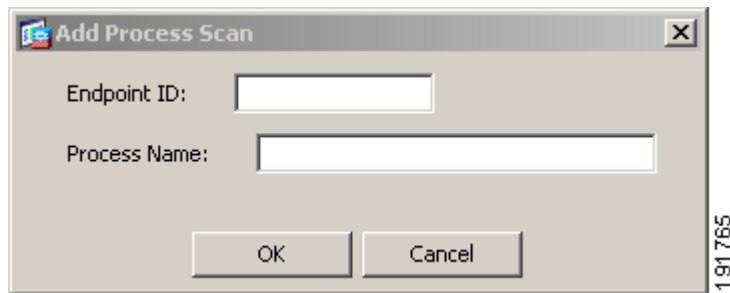
- Step 4** Click **OK**.
ASDM closes the Add Registry Scan window and inserts the entry into the Basic Host Scan table.
-

Adding a Process Check to the Basic Host Scan

Add a check for a specific process to the basic host scan as follows:

- Step 1** Choose **Secure Desktop Manager > Host Scan**.
The Host Scan pane opens (Figure 3-16).
- Step 2** Click **Add > Process Scan**.
The Add Process Scan pane opens (Figure 3-19).

Figure 3-19 Add Process Scan



- Step 3** Assign values to the following attributes:
- **Endpoint ID**—Enter a unique and meaningful string to serve as an index to this entry. After completing the Host Scan configuration, specify the same index when you assign this entry as an endpoint attribute when configuring a DAP. The string is case-sensitive.
For example,
Process-Agent.exe
 - **Process Name**—Enter the name of the process. You can display it in Microsoft Windows by opening the Windows Task Manager window and clicking the Processes tab.
For example,
Agent.exe
- Step 4** Click **OK**.
ASDM closes the Add Process Scan window and inserts the entry into the Basic Host Scan table.
-

Enabling and Disabling Host Scan Extensions

You can configure a scan for antivirus, personal firewall, and antispyware applications and updates as a condition for the completion of a Cisco AnyConnect or clientless SSL VPN connection. Following the prelogin assessment, Cisco Secure Desktop loads the endpoint assessment checks and reports the results back to the security appliance for use in assigning a DAP.

To enable or disable Host Scan Extensions,

Step 1 Choose **Secure Desktop Manager > Host Scan**

The Host Scan window opens (Figure 3-16).

Step 2 Check one of the following options in the Host Extensions area of the Host Scan window:

- **Endpoint Assessment**—If you check this option the remote PC scans for a large collection of antivirus, antispyware, and personal firewall applications, and associated updates.
- **Advanced Endpoint Assessment**—This option is present only if the configuration includes a key for an Advanced Endpoint Assessment license. It includes all of the Endpoint Assessment features, and lets you configure an attempt to update noncompliant PCs to meet the version requirements you specify. To turn on this option after acquiring a key from Cisco, choose **Device Management > System Image/Configuration > Activation Key**, enter the key in the New Activation Key field, and click **Update Activation Key**.

When you check this option, Secure Desktop Manager inserts a check mark next to both options.

To disable the host scan extensions, uncheck both options in the Host Extensions area of the Host Scan window.

Configuring Advanced Endpoint Assessment

Advanced Endpoint Assessment lets you configure an attempt to update noncompliant PCs to meet the version requirements you specify.

To configure Advanced Endpoint Assessment,

Step 1 Choose **Secure Desktop Manager > Host Scan**.

The Host Scan window opens (Figure 3-16).

Step 2 Check or click **Advanced Endpoint Assessment**.

If this option is unavailable, you need to get an Advanced Endpoint Assessment license and enter the key, as described in the previous section. Otherwise, Secure Desktop Manager activates the Configure button.

Step 3 Click **Configure** after checking Advanced Endpoint Assessment.

The Advanced Endpoint Assessment window displays the configuration settings. Figure 3-20 shows the default settings in this window.

Figure 3-20 Advanced Endpoint Assessment

**Note**

You must check an Enforce button to activate the corresponding drop-down lists of companies and applications. Secure Desktop Manager activates attributes and buttons in response to a selection only if the application supports the attributes and button functions. For example, you can click Add to add a personal firewall rule only if the selected personal firewall application supports rules.

Step 4

Use the descriptions of the attributes in the Antivirus area if you want to attempt to update noncompliant PCs with an antivirus application:

- **Enforce Antivirus** checkbox—Check to attempt to force an update of the application to be selected.
- **Enforce Antivirus** drop-down list—Select the company that produces the antivirus application.
- (Unnamed) drop-down list—When you select the company, this list displays the versions of antivirus applications that this company supports and that Host Scan supports. Select the version you want to require on the remote host.
- **Force File System Protection**—(Enabled only if the selected antivirus application supports this feature) Check to turn on ongoing background scanning by the antivirus application. The application checks files as they are received and blocks access to files that are likely to contain viruses.
- **Force Virus Definitions Update**—Check to require the remote host to check for a virus definitions update for the selected application. If you check this option, you must specify the number of days.
- **if not updated in last**— Enter the age in days of the last update that triggers a new update.

Step 5 Use the descriptions of the attributes in the Personal Firewall area if you want to attempt to update noncompliant PCs with an personal firewall application.

- **Enforce Personal Firewall** checkbox—Check to attempt to enable the application to be selected.
- **Enforce Personal Firewall** drop-down list—Select the company that produces the personal firewall application.
- (Unnamed) drop-down list—When you select the company, this list displays the versions of personal firewall applications that this company supports and that Host Scan supports. Select the version you want to require on the remote host.
- **Firewall Action**—The contents of this drop-down list depend on the options available to the selected personal firewall. Select None, Force Enable to enable the firewall, or Force Disable to disable the firewall.
- **Rules**—This table is available only if the selected personal firewall supports rules. It lets you specify applications and ports for which the firewall allows or blocks ports or applications. See [“Configuring Personal Firewall Rules”](#) to set the attributes in the Add or Edit window.

Step 6 Use the descriptions of the attributes in the Antispyware area if you want to attempt to update noncompliant PCs with an antispyware application.

- **Enforce Antispyware** checkbox—Check to attempt to force an update of the application to be selected.
- **Enforce Antispyware** drop-down list—Select the company that produces the antispyware application.
- (Unnamed) drop-down list—When you select the company, this list displays the versions of antispyware applications that this company supports and that Host Scan supports. Select the version you want to require on the remote host.
- **Force Spyware Definitions Update**—Check to require the remote host to check for a spyware definitions update for the selected application. If you check this option, you must specify the number of days.
- **if not updated in last**— Enter the age in days of the last update that triggers a new update.

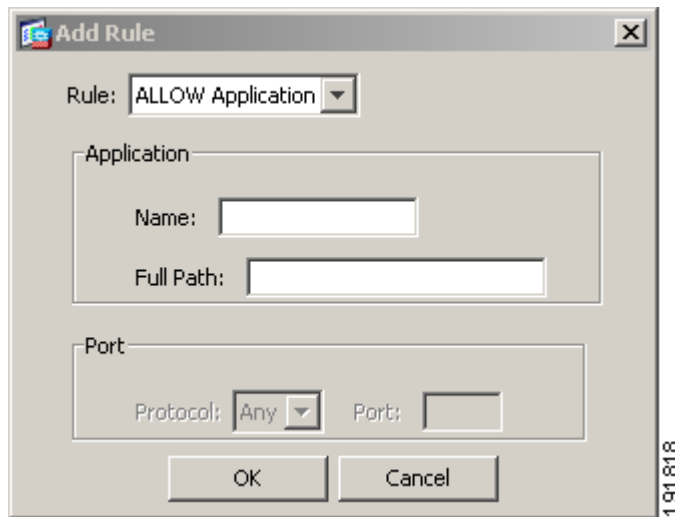
Step 7 Click **OK**.

Configuring Personal Firewall Rules

Personal firewall rules let you specify applications and ports for the firewall to allow or block. The Add, Edit, and Delete buttons next to the Rules table in the Advanced Endpoint Assessment window (Figure 3-20) are active only if the selected personal firewall supports rules. For example, the applications that appear under the Internet Security Systems, Inc. option support personal firewall rules.

If you configure Advance Endpoint Assessment as described in the previous section and click **Add** or **Edit** next to the Rules table, the Add or Edit Rule window opens (Figure 3-21).

Figure 3-21 Add Personal Firewall Rule



To set the attributes in the Add or Edit Rule window,

-
- Step 1** Use the following attribute description to select the rule.
- Rule—Choose the action of this rule. The options are ALLOW Application, BLOCK Application, ALLOW Port, and Block Port.
- Step 2** Go to the Application area and set the following attributes if you selected ALLOW Application or BLOCK Application.
- Name—Enter the full file name and extension of the application to be allowed or blocked.
 - Full path—Enter the entire path to the application file.
- Step 3** Go to the Port area and set the following attributes if you selected ALLOW Port or BLOCK Port.
- Protocol—Select the protocols to be allowed or blocked. The options are Any, UDP, and TCP.
 - Port—Enter the port number to be allowed or blocked.
- Step 4** Click **OK**.

Repeat this procedure for each personal firewall rule you want to configure.

Configuring a Dynamic Access Policy

You can use a match of an endpoint profile, basic Host Scan entry, host scan extension, or any combination of these and any other policy attributes to assign access rights and restrictions. At minimum, configure dynamic access policies (DAP) to assign to each endpoint profile and basic host scan entry.

Configure DAPs as follows:

- Step 1** Choose **Configuration > Network (Client) Access** or **Clientless SSL VPN Access > Dynamic Access Policies > Add** or **Edit**.

The Add or Edit Dynamic Policy window opens (Figure 3-22).

Figure 3-22 Add Dynamic Access Policy

The screenshot shows the 'Add Dynamic Access Policy' dialog box. At the top, there are fields for 'Policy Name', 'Description', and 'Priority' (set to 0). Below this is the 'Selection Criteria' section, which includes a dropdown menu currently set to 'User has ANY of the following AAA Attributes values...'. There are two tables for defining criteria: one for AAA Attributes and one for Endpoint Attributes. Each table has 'Add', 'Edit', and 'Delete' buttons. Below the tables is an 'Advanced' section that is currently collapsed. The 'Access Policy Attributes' section is expanded, showing tabs for 'Action', 'Network ACL Filters', 'Web-Type ACL Filters', 'Functions', 'Port Forwarding Lists', 'URL Lists', and 'Access Method'. The 'Action' tab is selected, showing radio buttons for 'Continue' (selected) and 'Terminate'. Below this is a 'User Message' text area. At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.

- Step 2** Name the policy and assign a priority to the policy using the fields near the top of the window.

- Step 3** Select the ANY, ALL, or NONE option in the drop-down list on the left side of the Selection Criteria area.

- Step 4** Click the **Add** button on the left to specify AAA attribute type and values, then click OK. Repeat for each AAA attribute to use for this DAP.
- Step 5** Move the mouse to the right of the Endpoint Attribute table and click **Add**.
The Add Endpoint Attribute window opens (Figure 3-23).

Figure 3-23 Add Endpoint Attribute

The screenshot shows a dialog box titled "Add Endpoint Attribute". It has a title bar with a close button. Inside, there is a dropdown menu for "Endpoint Attribute Type" with "Anti-Spyware" selected. Below it are two radio buttons: "Exists" (selected) and "Does not exist". There are three input fields: "Vendor ID", "Vendor Description", and "Version" (with a dropdown set to "="). Below these are two more input fields: "Last Update" (with a dropdown set to "<") and "days". At the bottom are three buttons: "OK", "Cancel", and "Help". A vertical number "191817" is visible on the right side of the dialog box.



Note If the Endpoint Assessment or Advanced Endpoint Assessment option on the Secure Desktop Manager > Host Scan pane is checked and you select Antispyware, Antivirus, or Personal Firewall, ASDM populates the Vendor ID and Vendor Description drop-down menus. Otherwise, it shows blank fields next to the Vendor ID and Vendor Description attribute names.

- Step 6** Choose one or more of the methods in Table 3-2 to match the endpoint:

Table 3-2 Endpoint Attribute Types Associated with Cisco Secure Desktop

To Match this Secure Desktop Manager object	Select this Endpoint Attribute Type	And do this
Endpoint profile present in the Secure Desktop Manager > Windows Location Settings pane	Policy	Enter the name of the endpoint profile in the Location field.
File specified in the Basic Host Scan table in the Secure Desktop Manager > Host Scan pane	File	Select the Endpoint ID that matches the Basic Host Scan file entry ID from the drop-down list.
Process specified in the Basic Host Scan table in the Secure Desktop Manager > Host Scan pane	Process	Select the Endpoint ID that matches the Basic Host Scan process entry ID from the drop-down list.

Table 3-2 *Endpoint Attribute Types Associated with Cisco Secure Desktop*

To Match this Secure Desktop Manager object	Select this Endpoint Attribute Type	And do this
Registry key specified in the Basic Host Scan table in the Secure Desktop Manager > Host Scan pane	Registry	Select the Endpoint ID that matches the Basic Host Scan registry entry ID from the drop-down list.
Antispyware application of interest, applicable only if the Endpoint Assessment or Advanced Endpoint Assessment option on the Secure Desktop Manager > Host Scan pane is checked.	Antispyware	Select the options in the Vendor ID and Vendor Description drop-down lists.
Antivirus application of interest, applicable only if the Endpoint Assessment or Advanced Endpoint Assessment option on the Secure Desktop Manager > Host Scan pane is checked.	Antivirus	Select the options in the Vendor ID and Vendor Description drop-down lists.
Personal firewall application of interest, applicable only if the Endpoint Assessment or Advanced Endpoint Assessment option on the Secure Desktop Manager > Host Scan pane is checked.	Personal Firewall	Select the options in the Vendor ID and Vendor Description drop-down lists.

Step 7 Click **OK**.

The Add or Edit Endpoint Attribute window closes, leaving the Add or Edit Dynamic Policy window open.

Step 8 Complete the configuration of any other endpoint attributes to specify any other criteria you want to use to identify the remote access devices for which the DAP applies.**Step 9** Set the access policy attributes in the tabs at the bottom of the window to provide access rights and restrictions, then click **OK**.



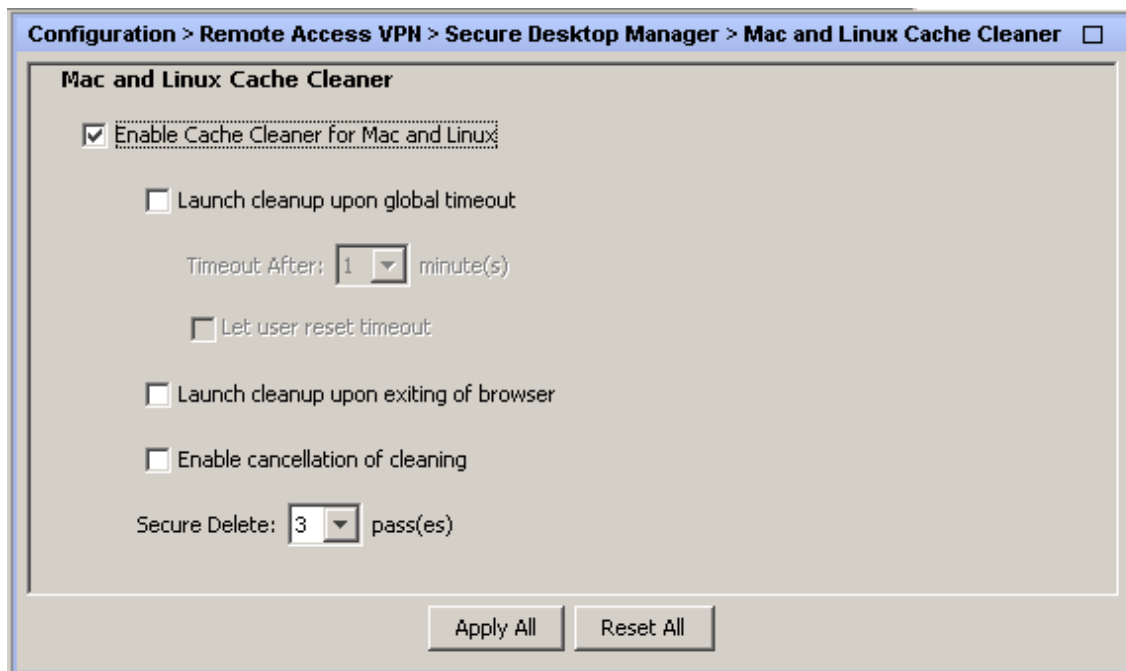
Configuring Cache Cleaner for Mac OS X and Linux Computers

Cache Cleaner for Mac OS X and Linux supports Clientless SSL VPN connections with remote computers running those operating systems.

To configure Cache Cleaner for these computers, click **Mac & Linux Cache Cleaner** in the menu on the left.

The Mac and Linux Cache Cleaner pane appears (Figure 4-1).

Figure 4-1 Cache Cleaner — Mac and Linux Cache Cleaner



Note

This pane lets you configure Cache Cleaner for all Mac and Linux computers.

Set the attributes as follows:

- **Enable Cache Cleaner for Mac and Linux**—Check to install Cache Cleaner when a Macintosh or PC running Linux connects to the security appliance. Uncheck to not install it.
- **Launch cleanup upon global timeout and Timeout after**—Check to set a global timeout after which to launch 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**—Cache Cleaner writes the cache to the remote computer disk. Upon termination, Cache Cleaner converts bits occupied by the cache to 0's, then to 1's, and finally to randomized 1's and 0's. Choose the number of times 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, Cache Cleaner removes the pointer to the file.

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



Tutorial

This tutorial provides an overview of the Cisco Secure Desktop configuration sequence. It does not provide detailed instructions on the attributes. The sections are as follows:

- [Tutorial Overview](#)
- [Configuring a Prelogin Assessment](#)
- [Assigning Secure Session and Cache Cleaner Settings for Each Endpoint Profile](#)
- [Configuring Cache Cleaner Support for Mac OS X and Linux](#)
- [Assigning a DAP for Each Endpoint Profile](#)

Tutorial Overview

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



Note

This tutorial is only an example; we recommend that you choose profile names and configuration settings in your actual deployment that reflect your VPN security policies.

In this tutorial, “Secure” provides clients with full access, “Home” provides some flexibility, and “Public” requires restricts access. This tutorial defines the endpoint profiles as follows:

- Secure
 - Assign a prelogin assessment to recognize a corporate computer attempting to establish a VPN connection by identifying the Windows version, that the IP address is within a specific range, and that it has a specified registry entry.
 - Disable Secure Desktop (Secure Session) and Cache Cleaner.
 - Use the dynamic access policy (DAP) configuration to assign access rights.
- Home
 - Identify using a certificate given by the administrator and a file check.
 - Enable Secure Desktop (Secure Session) and Vault Reuse with no timeout.

Vault Reuse lets users close the Secure Session 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) before the establishment of a Secure Session.

- Advanced features require company antivirus software, company antispayware, company firewall, and Windows 2000 Service Pack 4 or Windows XP.
- Check for keystroke logger.
- Use the DAP configuration to assign access rights.
- Public profile
 - Check for malware file.
 - Check for keystroke logger file.
 - Install Cache Cleaner.
 - Use the DAP configuration to assign access rights.

Our example includes “Secure,” “Home,” and “Public” in that order; to assign privileges to a host, Cisco Secure Desktop first determines whether it is a “Secure” host. If it is not, it determines whether it is a “Home” host. If it is not, it performs several file checks and assigns the privileges associated with the “Public” endpoint profile.

Configuring a Prelogin Assessment

These instructions assume that Secure Desktop Manager has loaded the default configuration. To reload the default configuration, rename the sdesktop/data.xml file, disable Cisco Secure Desktop, re-enable it, exit ASDM, then start a new ASDM session.

Use the following sections to configure the prelogin assessment and assign names to the endpoint profiles:

- [Configuring an Endpoint Profile and Prelogin Assessment for a Secure Computer](#)
- [Configuring an Endpoint Profile and Prelogin Assessment for a Home Computer](#)
- [Configuring an Endpoint Profile and Prelogin Assessment for a Public Computer](#)

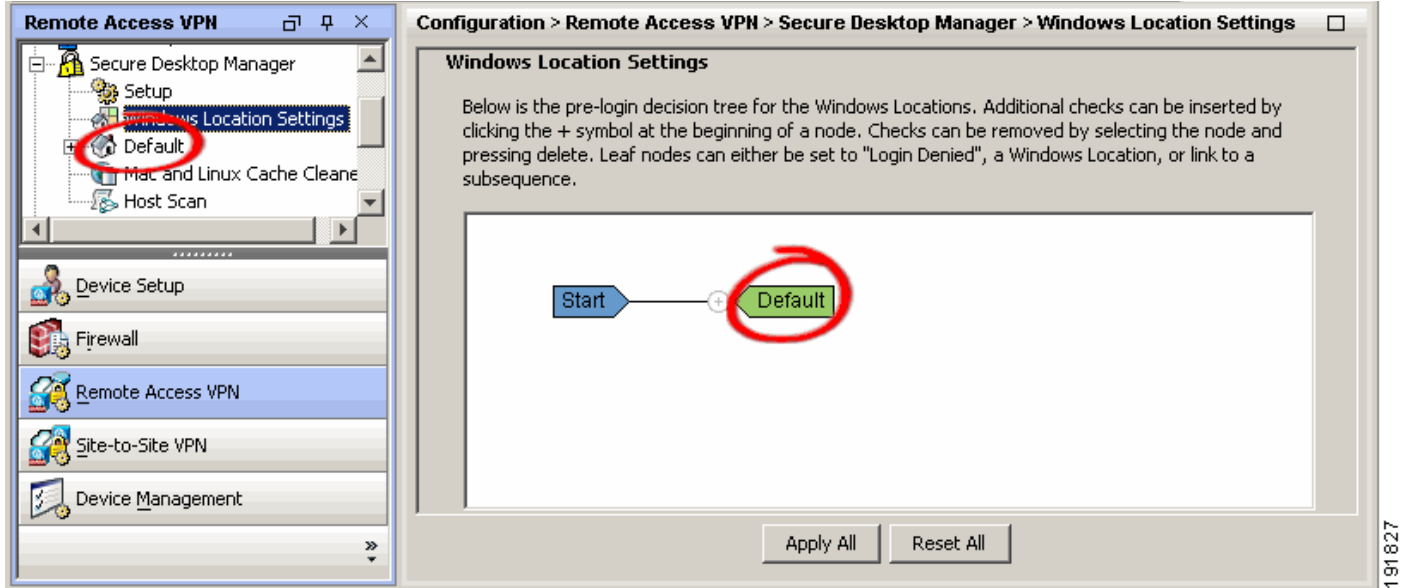
Configuring an Endpoint Profile and Prelogin Assessment for a Secure Computer

Use the following instructions to create an example endpoint profile named “Secure” and assign a prelogin assessment to qualify PCs attempting remote access VPN connections:

Step 1 Choose **Windows Location Settings**.

The Windows Location Settings pane shows the default endpoint profile named “Default.” The menu shows the same profile name, indicating the place where you assign settings to that profile ([Figure A-1](#)).

Figure A-1 Windows Location Settings (Default Prelogin Configuration)

**Tip**

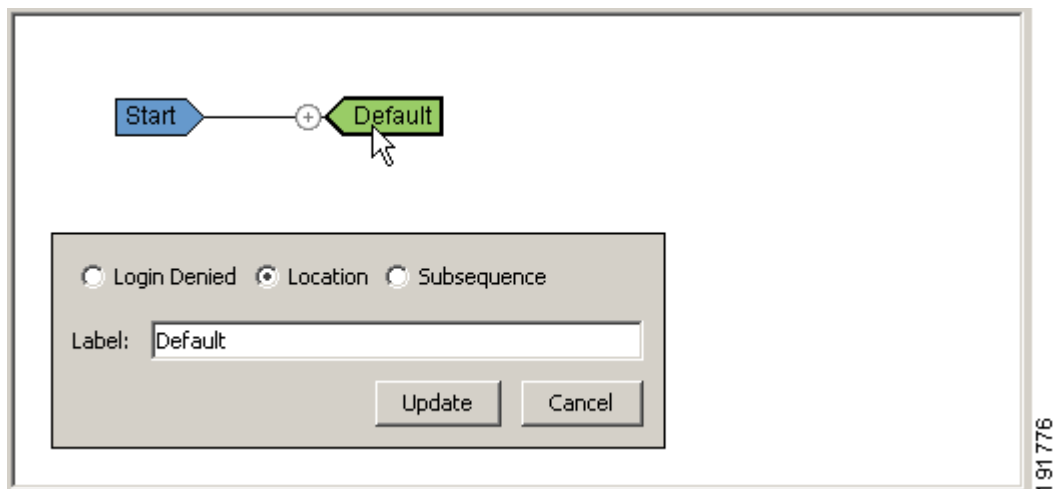
If you would like to explore the options available in the prelogin assessment sequence editor without making permanent changes to the Cisco Secure Desktop configuration file, make the changes, then choose an ASDM option outside the Secure Desktop Manager menu, and click **Discard Changes**.

Step 2 Click the end node named **Default**.

This end node represents an endpoint profile. Note that Secure Desktop Manager displays the name of this end node in its menu.

Secure Desktop Manager inserts a window that lets you change the type and name of the end node (Figure A-2).

Figure A-2 Change End Node Window

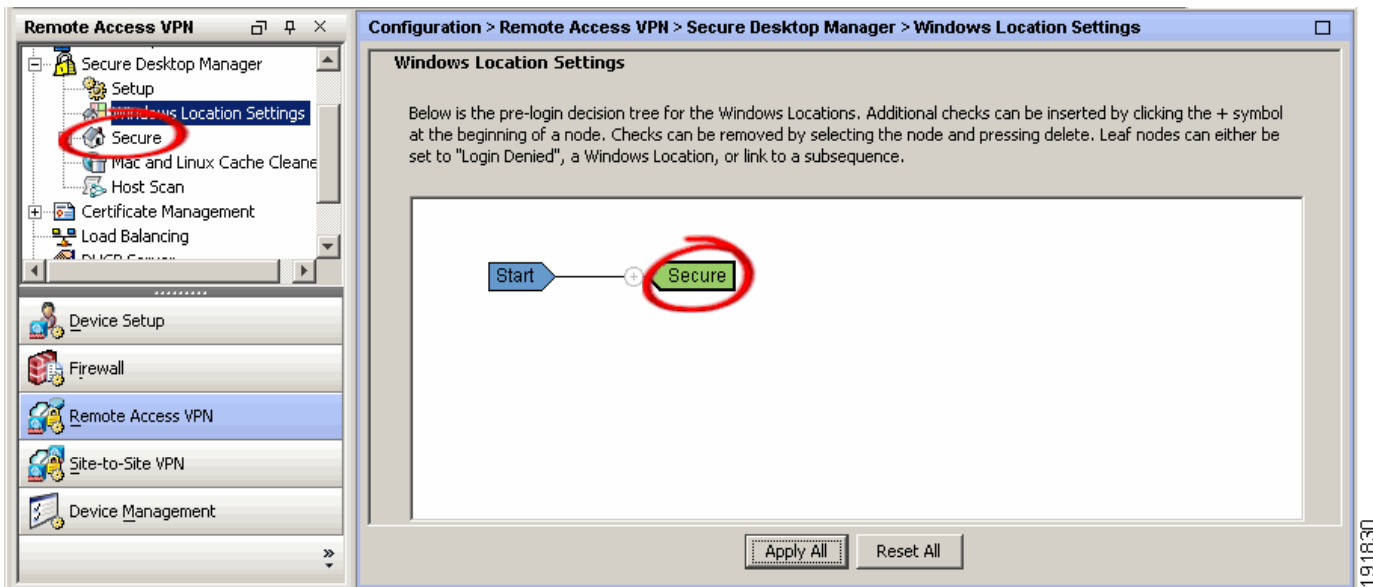


Note that the Location option is already selected. In this case, you only need to change the name.

- Step 3** Replace the name Default in the text box with the name Secure, as shown.
- Step 4** Click **Update**.

Secure Desktop Manager closes the change end node window, and changes both the name of the end node and the associated menu option in the Secure Desktop Manager menu (Figure A-3).

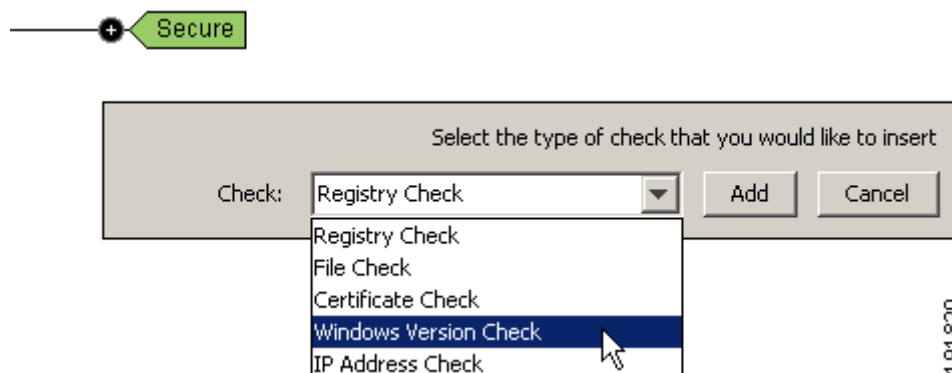
Figure A-3 Default Location Changed to Secure



- Step 5** Click the plus sign in the diagram.

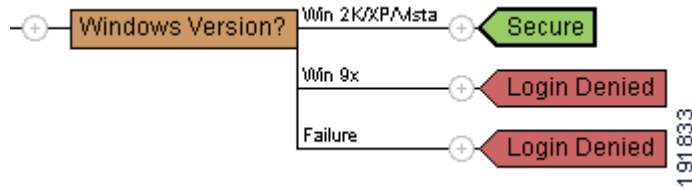
A window opens below the diagram, prompting you to select the type of check to be inserted (Figure A-4).

Figure A-4 Prelogin Assessment Options



- Step 6** Choose **Windows Version Check** and click **Add**.

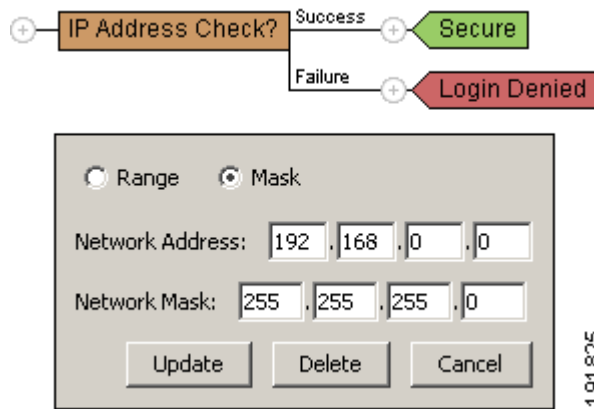
Secure Desktop Manager inserts the Windows Version check node into the diagram (Figure A-5).

Figure A-5 Windows Version Check

Step 7 Click the plus sign to the left of the Secure node.

Step 8 Select **IP Address Check** and click **Add**.

Secure Desktop Manager inserts the IP Address Check node and opens the IP address check window below the diagram (Figure A-6).

Figure A-6 IP Address Check

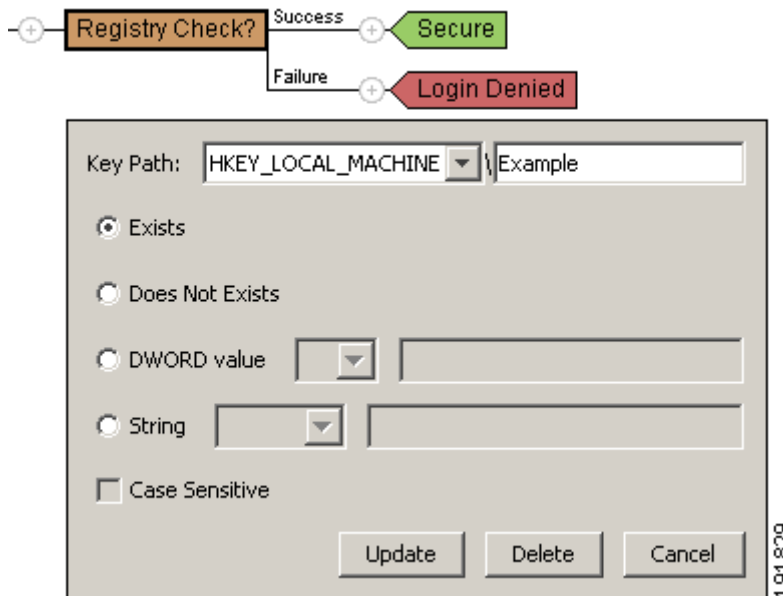
Step 9 Click **Range** to indicate the type of IP address check, enter the IP address range, and click **Update**.

Step 10 Click the plus sign to the left of the Secure node.

Step 11 Select **Registry Check** and click **Add**.

Secure Desktop Manager inserts the Registry Check node and opens the Registry check window below the diagram (Figure A-7).

Figure A-7 Registry Check



- Step 12** Select an option next to the Key Path drop-down menu such as HKEY_LOCAL_MACHINE,” type the string to indicate the remainder or the path such as “SOFTWARE\Company-Name,” select a radio button such as Exists, and click **Update**.

This step completes the instructions for creating checks for the example Secure node.

Configuring an Endpoint Profile and Prelogin Assessment for a Home Computer

Use the following instructions to create an example endpoint profile named “Home” and assign a prelogin assessment to qualify Windows computers for a Secure Session installation. The prelogin assessment verifies the presence of a certificate given by the administrator to users who connect from home and verifies the presence or absence of a specific file. Complete the example prelogin assessment for home computers as follows:



Note These instructions assume you have followed the instructions in the previous section.

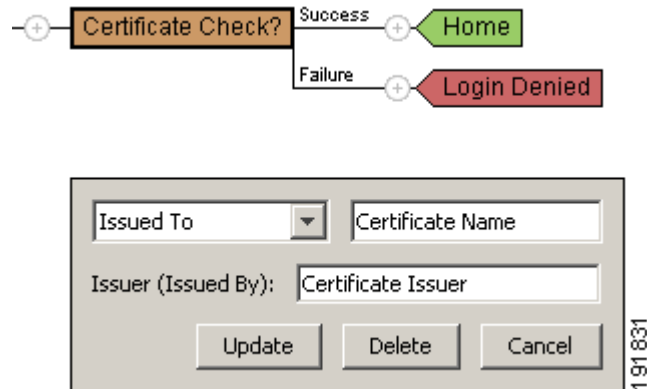
- Step 1** Choose **Windows Location Settings**.
- Step 2** Click the Login Denied end node that follows the IP Address Failure branch.
Secure Desktop Manager inserts a window that lets you change the type and name of the end node.
- Step 3** Click the Subsequence radio button, replace the text in the box with the name Home Check, and click **Update**.
Secure Desktop Manager inserts a window that lets you change the type and name of the end node.
- Step 4** Scroll to the Home Check node on the left side of the diagram and click the Login Denied end node to its right.
- Step 5** Click the **Location** radio button and replace the text in the box with the word Home.

Step 6 Click the plus sign to the left of the end node labeled Home.

Step 7 Select **Certificate Check**, and click **Add**.

Secure Desktop Manager inserts the Certificate Check node and opens the Certificate check window below the diagram (Figure A-8).

Figure A-8 Certificate Check



Step 8 Select an option from the drop-down box to specify the certificate field to be checked, enter the value of the field to match in the adjacent text box, enter the issuer of the certificate into the Issuer text field, and click **Update**.

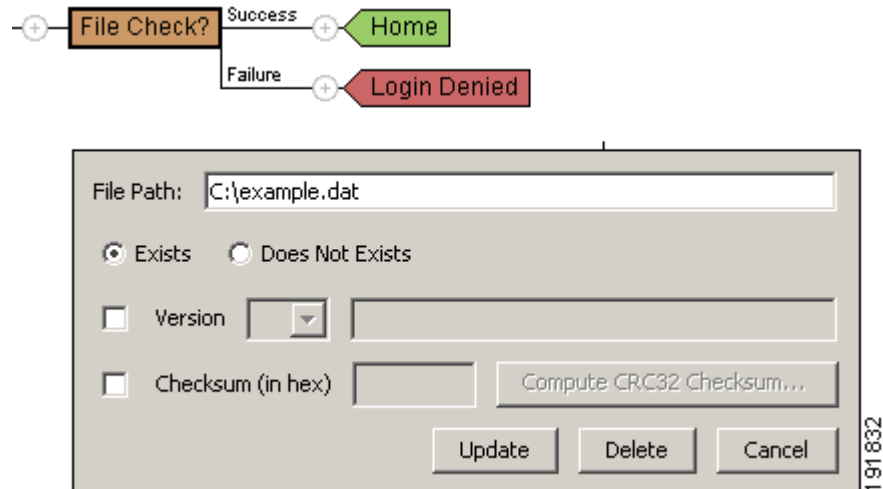
For each additional field of a single certificate that you want to match, create another prelogin check that specifies that field and value.

Step 9 Click the plus sign to the left of the end node labeled Home.

Step 10 Select **File Check** and click **Add**.

Secure Desktop Manager inserts the File Check node and opens the File check window below the diagram (Figure A-9).

Figure A-9 File Check



Step 11 Enter a path to the file in the drop-down box, select a radio button such as **Exists**, and click **Update**.

Step 12 Repeat Steps 9–10 to insert an additional file check.

This step completes the instructions for creating checks for the example Secure node. Continue with the next section to create the checks for the example Home node.

Configuring an Endpoint Profile and Prelogin Assessment for a Public Computer

Use the following instructions to create an example endpoint profile named “Public” and assign a prelogin assessment to qualify Windows computers for a Cache Cleaner installation.

These instructions say to add several prelogin file checks to qualify a Windows computer for Cache Cleaner, however, you can use any prelogin checks, or replace any Login Denied end node with a “Public” end node if you do not want to require a match.



Note

These instructions assume you have followed the instructions in the previous sections.

Step 1 Choose **Windows Location Settings**.

Step 2 Click the Login Denied end node that follows the Win 9x branch.

Step 3 Click the Subsequence radio button, replace the text in the box with the name Public Check, and click **Update**.

Step 4 Change the Login Denied end nodes that follow the IP Address Check, Certificate Check, and File check boxes to a subsequence end node, also named Public Check.

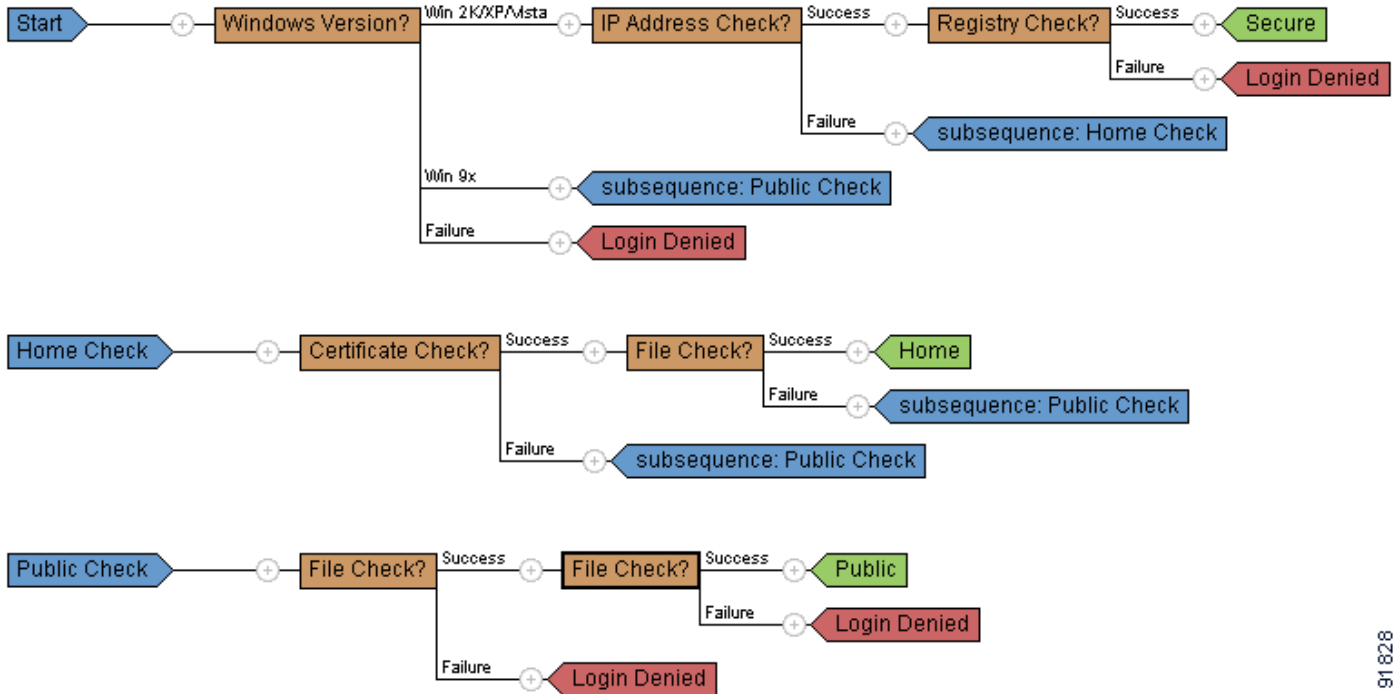
Step 5 Scroll to the Public Check node on the left side of the diagram and click the Login Denied end node to its right.

Step 6 Click the **Location** radio button and replace the text in the box with the word Public.

Step 7 Insert two File Checks to the left of the Public end node.

This step completes the configuration of the example prelogin assessment. The diagram of your prelogin assessment should look like the one shown in [Figure A-10](#).

Figure A-10 Example Prelogin Configuration



191828

Continue with the next section to assign the Secure Session and Cache Cleaner settings appropriate for each endpoint profile.

Assigning Secure Session and Cache Cleaner Settings for Each Endpoint Profile

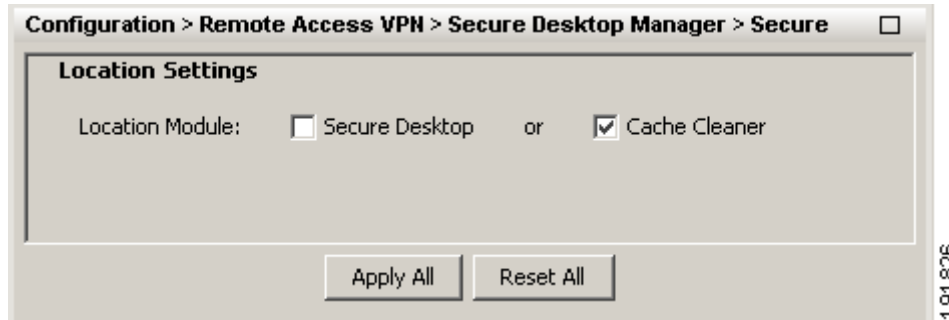
The following sections describe how to enable or disable Secure Desktop (Secure Session) and Cache Cleaner for each endpoint profile and how to configure scanning for keystroke loggers:

- [Enabling or Disabling Secure Session and Cache Cleaner](#)
- [Configuring Keystroke Logger Scanning](#)

Enabling or Disabling Secure Session and Cache Cleaner

For each endpoint profile, click the name of the endpoint profile in the Secure Desktop menu. The Location Settings pane opens. [Figure A-11](#) shows the default settings for each endpoint profile.

Figure A-11 Location Settings



This window lets you specify whether to install Secure Session or Cache Cleaner on the remote desktops of computers that match the criteria associated with the selected profile.



Note Secure Desktop Manager lets you uncheck both options, or check one or the other. If you check Secure Desktop and the operating system is Windows 98 or Vista, Cache Cleaner loads instead, even if the prelogin assessment for that endpoint profile does not contain a Windows version check. Therefore, even if you check Secure Desktop, it is important to make sure the Cache Cleaner settings are appropriate for the endpoint profile, as described later in this tutorial.

See [Table A-1](#) to check or uncheck Secure Desktop or Cache Cleaner.

Table A-1 Location Settings—Sample Values

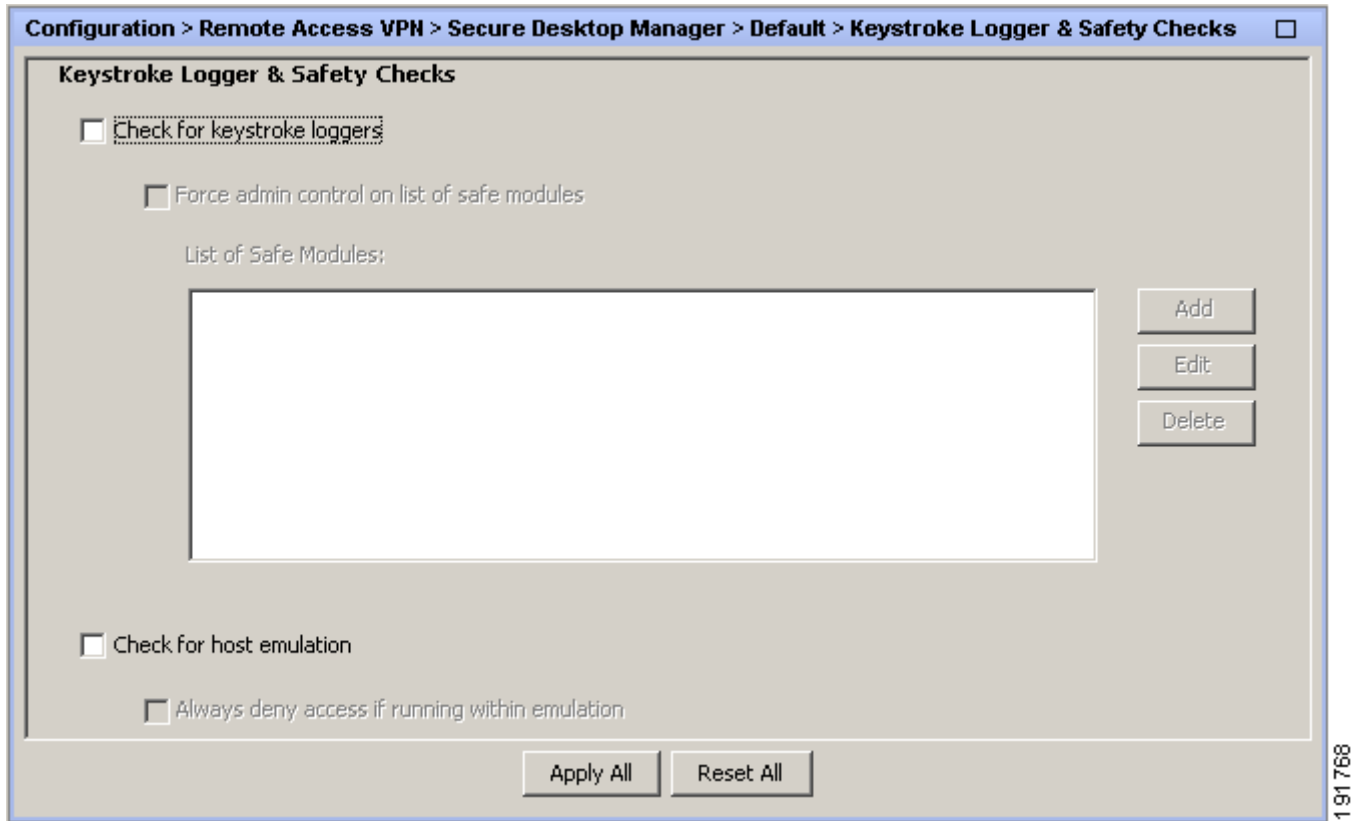
Action and Attribute	Endpoint Profile		
	Secure	Home	Public
Check Secure Desktop?	No	Yes	—
Check Cache Cleaner?	No	—	Yes

Configuring Keystroke Logger Scanning

By default, keystroke logger scanning is disabled. Keep it disabled for the Secure endpoint profile. Configure scanning for keystroke loggers once for the Home endpoint profile and once for the Public profile, as follows:

- Step 1** Click **Keystroke Logger** under the name of the endpoint profile you are configuring in the menu on the left.
- The Keystroke Logger window opens ([Figure A-12](#)).

Figure A-12 Keystroke Logger Window



See [Table A-2](#) to check the attributes in this window.

Table A-2 Keystroke Logger & Safety Checks—Sample Values

Action and Attribute	Endpoint Profile		
	Secure	Home	Public
Check for keystroke loggers	No	Yes	Yes
Check Force Admin control on list of safe module?	—	No	Yes
Populate List of Save Modules?	—	—	Yes
Check for host emulation?	No	Yes	Yes
Check Always deny access if running within emulation?	—	—	Yes

Step 2 Check **Check for keystroke loggers** to scan for a keystroke logging application on the remote PC and make sure one is not running, before creating the Secure Session 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, the Cisco Secure Desktop installer lists the keystroke loggers discovered on the client computer. To access Secure Session, 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.

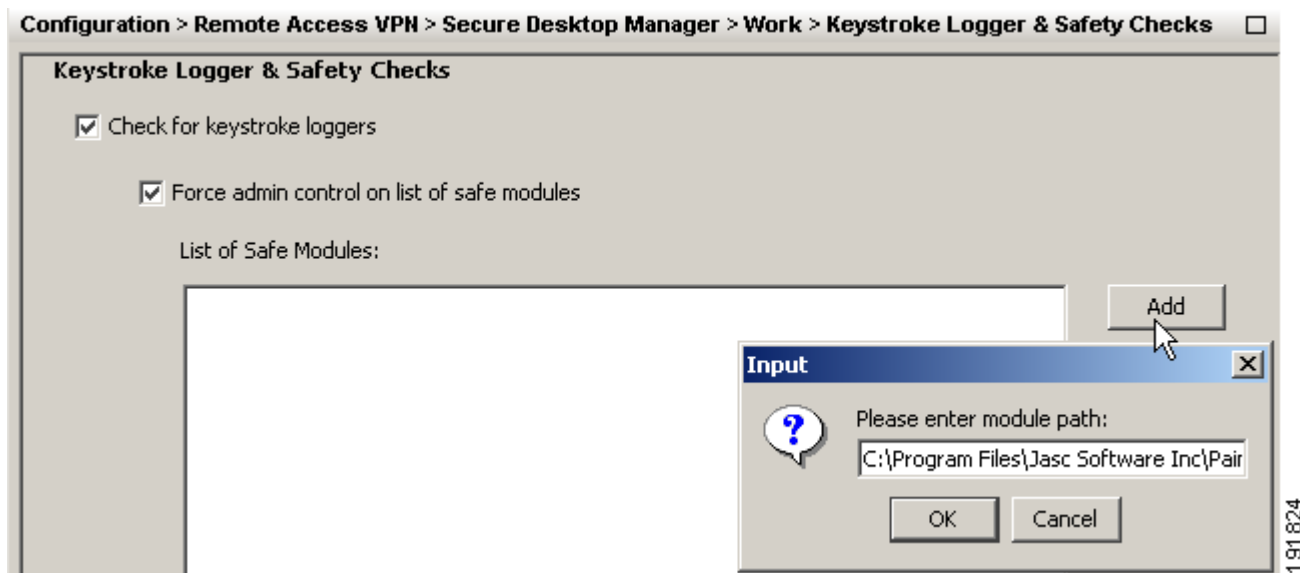


Note Unchecking this attribute deactivates but does not delete the contents of the “List of Safe Modules” window.

- 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.

Cisco Secure Desktop Manager opens the Input dialog box (Figure A-13).

Figure A-13 Input (for Keystroke Logger)



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

Cisco Secure Desktop Manager 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**.

Configuring Cache Cleaner Support for Mac OS X and Linux

Cisco Secure Desktop handles Mac OS X and Linux systems differently from Windows. Cisco Secure Desktop applies the same settings to all Mac OS X and Linux hosts connecting from both secure and insecure locations. Configure the Mac OS X 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**.

See the option descriptions in “[Configuring Cache Cleaner for Mac OS X and Linux Computers](#)” for more information about the settings in this window.

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

Assigning a DAP for Each Endpoint Profile



Note These instructions assume you have followed the instructions in the previous sections of this tutorial.

Configure a dynamic access policy (DAP) to support an endpoint profile as follows:

Step 1 Choose **Configuration > Network (Client) Access** or **Clientless SSL VPN Access > Dynamic Access Policies > Add** or **Edit**.

The Add or Edit Dynamic Policy window opens ([Figure A-14](#)).

Figure A-14 Add Dynamic Access Policy

Policy Name:

Description: Priority:

Selection Criteria

Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ANY of the following AAA Attributes values... and the following endpoint attributes are satisfied.

AAA Attribute	Operation/Value	Add	Endpoint ID	Name/Operation/Value	Add
		Edit			Edit
		Delete			Delete

Advanced

Access Policy Attributes

Configure access policy attributes for this policy. Attributes values specified here will override those values obtained from the AAA system.

Action

Action: Continue Terminate

Specify the message that will be displayed when this record is selected.

User Message:

OK Cancel Help

191821

- Step 2** Move the mouse to the right of the Endpoint Attribute table and click **Add**.
The Add Endpoint Attribute window opens (Figure A-15).

Figure A-15 Add Endpoint Attribute

Step 3 Select **Policy** from the drop-down list next to the **Endpoint Attribute Type**.

Step 4 Enter the name of an endpoint profile in the Location field.

The Location field is case-sensitive.

Step 5 Click **OK**.

The Add or Edit Endpoint Attribute window closes, leaving the Add or Edit Dynamic Policy window open.

Step 6 For each entry in the basic host scan table, click **Add** to the right of the Endpoint Attribute table. Select the type (Registry, File, or Process) next to the Endpoint Attribute Type attribute, enter the unique ID of the entry in the Endpoint ID box, and click **OK**.

Step 7 For each antispyware, antivirus, and personal firewall application you would like to require as part of the DAP, click **Add** to the right of the Endpoint Attribute table. Select the type (Antispyware, Antivirus, or Personal Firewall) next to the Endpoint Attribute Type attribute, select the company and application, and click **OK**.

Step 8 Use the Add or Edit Dynamic Policy window to name and prioritize the DAP entry, complete the configuration of any other selection criteria, and specify the access policy attributes, then click **OK**.



Frequently Asked Questions

The following sections address the Cisco Secure Desktop FAQs:

- [New Questions for Cisco Secure Desktop Release 3.2](#)
- [Timeout Questions](#)
- [Secure Session and Cache Cleaner Questions](#)
- [Networking and Firewall Questions](#)

New Questions for Cisco Secure Desktop Release 3.2

The following questions are new for this release.

What happened to the VPN feature policies?

Previously, Secure Desktop Manager let you configure a VPN feature for each endpoint profile. The dynamic access policy (DAP) feature accessible on ASDM replaces and expands on this feature.

What are the minimum rights for Secure Session, Cache Cleaner, Host Scan, and KeyStroke Logger Scanning?

Non-privileged, guest user accounts are sufficient to download and install Secure Session, Cache Cleaner, and Host Scan. Keystroke Logger scanning requires administrator privileges.

What is the sequence of events when a remote computer connects?

One or more of the following occurs when a remote computer attempts to establish a VPN connection to a security appliance configured with Cisco Secure Desktop:

- Cache Cleaner loads if both of the following are true:
 - Cache Cleaner for Mac OS X and Linux is enabled in the Cisco Secure Desktop configuration.
 - The remote computer is running Mac OS X or Linux
- The Login Denied message appears if the remote computer is running Windows and the result of the prelogin assessment does not match an endpoint profile.

- Host Scan loads if all of the following are true:
 - The Cisco Secure Desktop configuration contains basic Host Scan entries or the Host Scan extensions are enabled.
 - The remote computer is running Windows Vista, XP, 2000, or 98.
 - The prelogin assessment results match an endpoint profile.
- Secure Session loads if it is enabled on the matched endpoint profile, and the remote operating system is Windows XP or 2000. If Host Scan also loads, it loads with Secure Session after the prelogin assessment.
- Cache Cleaner loads if either Secure Session or Cache Cleaner for Windows is enabled on the matched endpoint profile, and the remote operating system is Windows Vista or 98. If Host Scan also loads, it loads with Cache Cleaner after the prelogin assessment.
- The security appliance uses configured endpoint attribute criteria such as Host Scan results and an endpoint profile match to apply a DAP, after the user logs in.

Must Secure Session install to check for malware?

Either Cisco Secure Desktop or NAC Framework must be configured to load the endpoint assessment.

If the remote computer passes a prelogin assessment associated with a particular endpoint profile configured on the security appliance, a scan of the antivirus, antispymware, personal firewall, and other optional keylogger, file, registry, and process checks occurs. This scan can be turned on or off by the system administrator. Secure Session or Cache Cleaner installs only if the prelogin assessment associated with a particular endpoint profile passes, and only if the Secure Desktop or Cache Cleaner parameters are enabled for the matched endpoint profile. If both the prelogin assessment for a particular endpoint profile and the Host Scan checks pass, and the endpoint profile has both Secure Desktop and Cache Cleaner disabled (typically for a corporate computer login), only the association of the matched endpoint profile in combination with other attributes with a particular DAP determines the user experience after authentication.

How does Host Scan work with dynamic access policies?

After you add scans for registry keys, files, and processes to the Basic Host Scan table in the Host Scan pane, choose **Configuration > Network (Client) Access** or **Clientless SSL VPN Access > Dynamic Access Policies > Add** or **Edit**. Choose Registry, File, or Process from the drop-down list next to the Endpoint Type attribute and enter the ID of the registry key, file, or process. Do this once for each entry in the Basic Host Scan table.

After you check Endpoint Assessment or Advanced Endpoint Assessment, choose **Configuration > Network (Client) Access** or **Clientless SSL VPN Access > Dynamic Access Policies > Add** or **Edit**. Choose Antispymware, Antivirus, or Personal Firewall from the drop-down list next to the Endpoint Type attribute and select the application you want to associate with a DAP. Do this once for each protective application you want to require to assign a DAP.

What happened to Windows CE?

Previously, Cisco Secure Desktop let you configure a very simple VPN feature policy that enabled or restricted web browsing and file access for remote clients running Microsoft Windows CE.

The DAP feature accessible on ASDM replaces and expands on the Windows CE support previously provided by Cisco Secure Desktop. Configure a DAP for Pocket PC or Windows CE as follows:

-
- Step 1** Choose **Configuration > Clientless SSL VPN Access > Dynamic Access Policies > Add or Edit**.
The Add or Edit Dynamic Policy window opens.
 - Step 2** Move the mouse to the right of the Endpoint Attribute table and click **Add**.
The Add or Edit Endpoint Attribute window opens.
 - Step 3** Select **Operating System** from the drop-down list next to Endpoint Attribute Type, check **OS Version**, select **Pocket PC** from the adjacent drop-down list, and click **OK**.
The Add or Edit Endpoint Attribute window closes, leaving the Add or Edit Dynamic Policy window open.
 - Step 4** Use the Add or Edit Dynamic Policy window to name and prioritize the DAP entry, complete the configuration of any other selection criteria, and specify the access policy attributes, then click **OK**.
-

Timeout Questions

The following questions address timeout settings with Secure Session and the Cache Cleaner.

How does the timeout setting work on Secure Session?

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, Secure Session closes at the end of the minute. Depending upon other settings, Secure Session saves the data or erases it from the disk. It also uninstalls itself if you configure it to do so.

Do Mac OS X and Linux have a timeout setting?

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

Which antivirus, antispyware, and firewall applications does Host Scan support?

The list of supported applications and versions is very long and is updated frequently. To view the names of the applications, make sure Cisco Secure Desktop is enabled and that one of the Host Scan Extensions is checked in the Host Scan window, then choose Configuration > Remote Access > Network (Client) Access or Clientless SSL VPN Access > Dynamic Access Policies > Add or Edit, click Add or Edit on

the far right side of the Add or Edit Dynamic Access Policy window, and select the Endpoint Attribute Type of interest. ASDM populates the Vendor ID and Product Description drop-down lists with the supported applications.

Secure Session and Cache Cleaner Questions

The following questions address the use of the Secure Session and Cache Cleaner features.

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

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

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

When you enable Secure Session 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 Secure Session after downloading it the first time?

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

Can I run multiple instances of Secure Session at the same time?

The current release does not support multiple instances of Secure Session on the same endpoint.

Can Cisco Secure Desktop detect all keystroke loggers?

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

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

The following Internet Explorer settings are required. 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 Secure Session and Cache Cleaner use?

Secure Session and Cache Cleaner encrypt 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 Secure Session 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 Secure Session or Cache Cleaner?

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

Can I use fast user switching on Windows XP?

Secure Session does not support fast user switching because only one instance of Secure Session can run on the same computer.

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

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

When do modified settings apply to Cache Cleaner and Secure Session?

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

Does Secure Session support Japanese character encodings?

Secure Desktop Manager supports encoding such as the Shift_JIS, provided that you configure support for it using ASDM (**Configuration > Clientless SSL VPN Access > Advanced > 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 Session 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 Session handle transparently?

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

Networking and Firewall Questions

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

Does the Secure Session or Cache Cleaner detect a second network card for endpoint profile determination?

No, it detects 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

Numerics

3DES [B-5](#)

A

ActiveX [B-5](#)

Allow e-mail applications to work transparently, attribute [3-22](#)

B

basic host scan [1-1, 3-25](#)

bit conversion [3-20](#)

bookmarks [3-23](#)

browser

 home page and favorites [3-23](#)

 restrict [3-21](#)

C

Cache Cleaner

 description [B-5](#)

 Mac OS X and Linux [4-1](#)

 Secure Session, when settings apply [B-6](#)

 Use Module, attribute [3-13](#)

 Windows [1-6, 3-17, 3-17 to 3-18](#)

character encoding [B-6](#)

Check for keystroke loggers, attribute [3-15, A-11](#)

Checksum, attribute [3-8](#)

Cipher Block Chaining (CBC) [B-5](#)

Clean the whole cache in addition to the current session cache, attribute [3-18](#)

command prompt, disable [3-22](#)

configuration settings, transfer to another security appliance [1-6](#)

Customize bookmarks, pane [3-23](#)

Customize bookmarks, window [3-23](#)

D

data.xml [1-6](#)

Data Encryption Standard (DES) [B-5](#)

delete *See* Secure Delete

deleting files [3-22](#)

DES-CBC [B-5](#)

desktop switching [3-19](#)

Disable access to network drives and network folders, attribute [3-21](#)

Disable access to removable drives and removable folders, attribute [3-22](#)

Disable command prompt access [3-22](#)

Disable printing, attribute [3-22](#)

Disable registry modification, attribute [3-22](#)

DoD delete *See* Secure Delete

Does not exist, criterion for a registry key or file [3-6](#)

Do not encrypt files on network drives, attribute [3-21](#)

Do not encrypt files on removable drives, attribute [3-22](#)

drive access [3-21, 3-22](#)

Dword [3-5, 3-6](#)

E

e-mail [3-22](#)

Enable Cache Cleaner for Mac and Linux, attribute [4-2](#)

Enable cancellation of cleaning, attribute [4-2](#)

Enable Secure Desktop inactivity timeout, attribute [3-20](#)

Enable switching between Secure Desktop and local desktop, attribute [3-19](#)

Enable Vault Reuse, attribute [3-20](#)

encryption [3-20, 3-21, 3-22, B-5](#)

endpoint profile

criteria [3-14](#)

definition [1-2, 1-5](#)

example configuration [A-1 to A-13](#)

Exists, criterion for a file [3-7](#)

Exists, criterion for a registry key or file [3-5](#)

F

FAQs [B-1 to B-7](#)

fast user switching [B-5](#)

favorites [3-23](#)

file criteria [3-2](#)

firewall [B-7](#)

folders in favorites or bookmarks [3-23](#)

Force admin control on list of safe modules, attribute [3-15, A-12](#)

Force application uninstall upon Secure Desktop closing, attribute [3-20](#)

frequently asked questions [B-1 to B-7](#)

G

GUI menu, figure [1-5](#)

H

Hidden URL, attribute [3-17](#)

hives [3-5, 3-26](#)

HKEY_CLASSES_ROOT [3-5, 3-26](#)

HKEY_CURRENT_USER [3-5, 3-26](#)

HKEY_LOCAL_MACHINE [3-5, 3-6, 3-26](#)

HKEY_USERS [3-5, 3-26](#)

home endpoint profile, example configuration [1-2, A-1](#)

Home Page, attribute [3-23](#)

host integrity *See* O.S Detection

I

inactivity timer [3-18, 3-20](#)

installing Cisco Secure Desktop [2-1 to 2-3](#)

Internet Explorer settings on remote access device [B-4](#)

IP address [3-12](#)

J

Japanese character encodings [B-6](#)

Java [B-5](#)

Java Virtual Machine [B-6](#)

K

Keystroke Logger [3-14 to 3-16, A-10 to A-12](#)

Keystroke Logger & Safety Checks [1-6](#)

L

Launch cleanup upon closing of all browser instances, attribute [3-18](#)

Launch cleanup upon exiting of browser, attribute [4-2](#)

Launch cleanup upon global timeout attribute [4-2](#)

Launch cleanup upon timeout based on inactivity, attribute [3-18](#)

Launch hidden URL after installation, attribute [3-17](#)

Let user reset timeout, attribute [4-2](#)

List of Safe Modules, pane [3-15](#)

local desktop, switch [3-19](#)

M

Mac & Linux Cache Cleaner, menu option [4-1](#)

main.exe [B-7](#)

menu, figure [1-5](#)

Microsoft Virtual Machine [B-5](#)

Microsoft Windows operating systems and service packs [1-7](#)

N

navigation [1-3](#)
 network card [B-6](#)
 network drive access [3-21](#)

O

Open following web page after Secure Desktop closes, attribute [3-20](#)

P

password, Secure Session [B-5](#)
 personal firewall [B-7](#)
 printing [3-22](#)
 public endpoint profile, example configuration [1-2, A-2](#)

R

registry
 criteria [3-2](#)
 disable modification [3-22](#)
 removable drive access [3-22](#)
 Restrict application usage to the web browser only, attribute [3-21](#)
 restricted mode [3-21](#)
 reusing CSD settings [1-6](#)

S

safe modules [3-15, A-12](#)
 secure, example configuration [1-2, 3-12, A-1](#)
 Secure Delete
 Mac OS X and Windows Cache Cleaner [4-2](#)
 Secure Session [3-20](#)

Windows Cache Cleaner [3-18](#)

See also encryption

Secure Desktop

Browser [1-6, 3-23](#)
 configuring [3-1](#)
 encryption type [B-5](#)
 FAQs [B-4](#)
 force uninstall [3-20](#)
 General [1-6, 3-19 to 3-20](#)
 inactivity timeout [3-20](#)
 local desktop switch [3-19](#)
 Manager
 establishing a session [1-3](#)
 menu, figure [1-5](#)
 multiple [B-4](#)
 open web page when closing [3-20](#)
 prompt to uninstall [3-20](#)
 Settings window [1-6, 3-21 to 3-22](#)
 Use Module, attribute [3-13](#)

Secure Session

Cache Cleaner, when settings apply [B-6](#)
 description [B-5](#)
 Suggest application uninstall, attribute [3-20](#)
 Vault Reuse, attribute [3-20](#)

security settings [B-4](#)

service packs [1-7](#)

Shift_JIS [B-6](#)

Show success message at the end of successful installation, attribute [3-18](#)

SSL VPN Client [3-19](#)

String value, attribute of a registry key as an endpoint criterion [3-6](#)

subnet mask [3-12](#)

Suggest application uninstall upon Secure Desktop closing, attribute [3-20](#)

Sygate Personal Firewall [B-6](#)

Sygate Security Agent [B-6](#)

T

timeout [B-3](#)

 Linux [B-3](#)

 Mac OS X [B-3](#)

Timeout after, attribute [3-18, 3-20, 4-2](#)

transparent e-mail [3-22](#)

Triple DES [B-5](#)

U

URLs on home page and favorites [3-23](#)

W

Windows Location Settings, menu option [1-3](#)

Windows operating systems and service packs [1-7](#)

X

xml [1-6](#)