



Release Notes for Cisco Secure Desktop, Release 3.4.2

Updated: May 6, 2010

Contents

Read the following sections carefully prior to installing, upgrading, and configuring Cisco® Secure Desktop 3.4.2:

- [Introduction, page 2](#)
- [Requirements, page 2](#)
- [Enhancements in CSD 3.4.1, page 4](#)
- [Administrator Guidelines, page 5](#)
- [End User Guidelines, page 5](#)
- [Caveats, page 9](#)



Note

This document identifies the latest enhancement and guidelines. After reading about them, use the [Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators, Version 3.4.1](#) for more information about the features; and for installation, upgrade, and configuration instructions.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

Cisco Secure Desktop (CSD) is a multifunctional component of the Cisco SSL VPN solution. The main features of CSD include:

- *Host Scan* checks for watermarks on a remote computer attempting to establish a Cisco AnyConnect client or browser-based (clientless) session. These watermarks can signify whether the computer is corporate-owned. The watermarks include registry entries, process names, and filenames. You can also use Host Scan to configure a check for antivirus and antispyware applications, associated definitions updates, and firewalls. CSD supports hundreds of versions of these applications. Host Scan reports results to the adaptive security appliance, which integrates them with the dynamic access policies (DAPs).
- *Secure Desktop (Vault)* encrypts the data and files associated with or downloaded during a remote session into a secure partition, and presents a graphical representation of a desktop that includes an image of a lock to signify a safe environment for the remote user to work in. When the remote session ends, a sanitation algorithm wipes the encrypted partition. Typically used during clientless SSL VPN sessions, Secure Desktop attempts to reduce the possibility that cookies, browser history, temporary files, and downloaded content remain after a remote user logs out, the session times out, or after an abrupt termination occurs.
- *Cache Cleaner*, an alternative to Secure Desktop, attempts to eliminate information in the browser cache at the end of a session. This information includes entered passwords, auto-completed text, files cached by the browser, and browser configuration changes.
- *Keystroke logger detection* and *host emulation detection* let you deny access based on the presence of a suspected keystroke logging application or a host emulator. You can use Secure Desktop Manager to specify the keystroke logging applications that are safe or let the remote user interactively approve the applications and host emulator the scan identifies. Both keystroke logger detection and host emulation detection are available with Cache Cleaner, Secure Desktop, and Host Scan.

No technology that interoperates with an operating system can ensure the total removal of all data, especially from an untrusted system with potentially malicious third party software installed. However, deployments of Cisco SSL VPN using CSD, when combined with other security controls and mechanisms within the context of an effective risk management strategy and policy, can help reduce risks associated with using such technologies.

Requirements

The following sections identify the adaptive security appliance platform and end-use interoperability that CSD requires or supports.

Cisco ASA 5500 Series

CSD 3.4.2 requires installation on a Cisco ASA 5500 Series running Release 8.0(4) or later and ASDM 6.1(3) or later.

OS and Browser Interoperability

The following sections name the CSD endpoint functions and list the endpoint OSs they support. The Cache Cleaner section also lists the supported browsers.

Host Scan



Note

Cisco does not officially support Windows 7 Beta; however, we have had encouraging results testing it with Host Scan.

Host Scan supports the following:

- 32- and 64-bit Microsoft Windows Vista, Vista SP1, and Vista SP2
- 32-bit Windows XP SP2 and SP3
- 64-bit Windows XP SP2
- 32-bit Windows 2000 SP4
- 32- and 64-bit Mac OS X 10.4 – 10.5
- 32- and 64-bit biarch (that is, 64-bit that can run 32-bit code) Linux with the following requirements: libxml2, libcurl (with openssl support), openssl, glibc 2.3.2 or later, and libz.
- [Antivirus, antispyware, and personal firewall applications](#).

We tested Host Scan on Redhat Enterprise Linux 3 and 4, and Fedora Core 4 and later, Ubuntu, and 32-bit and 64-bit FC9.

Although Host Scan might work on other OS's, we do not support them.

Secure Desktop (Vault), Keystroke Logger Detection, and Host Emulation Detection

Secure Desktop, Keystroke Logger Detection, and Host Emulation Detection run over the following OSs:

- 32-bit Windows Vista
[KB935855](#) or [Windows Vista SP1](#) (or later) must be installed.
- 32-bit Windows XP SP2 and SP3
- 32-bit Windows 2000 SP4

Although these features might work on other OS's, we do not support them.

Cache Cleaner



Note

Cisco does not officially support Windows 7 Beta; however, we have had encouraging results testing it with Cache Cleaner.

Cache Cleaner supports the following installations:

- 32- and 64-bit Windows Vista, Vista SP1, and Vista SP2
- 32-bit Windows XP SP3

- 32- and 64-bit Windows XP SP2
- 32-bit Windows 2000 SP4
- 32- and 64-bit Mac OS X 10.4.
WebLaunch requires Safari 1.0 or later, or Firefox 1.0 or later, on this OS.
- 32- and 64-bit Mac OS X 10.5.
WebLaunch requires Safari 1.0 or later, or Firefox 1.0 or later, on this OS.
- 32- or 64-bit biarch Linux with the following requirements: libxml2, libcurl (with openssl support), openssl, glibc 2.3.2 or later, and libz. WebLaunch requires Sun Java 1.5 or later and Firefox 1.0 or later.

We tested Cache Cleaner on Redhat Enterprise Linux 3 and 4, and Fedora Core 4 and later.

Although Cache Cleaner might work on other OS's, we do not support them.

Enhancements in CSD 3.4.2

CSD 3.4.2 is a fix release; however, we did add support for additional antivirus, antispware and personal firewall applications. [Cisco Secure Desktop, Release 3.4.2 List of Antivirus, Antispware, and Firewall Applications Supported by Host Scan](#) lists these applications.

Enhancements in CSD 3.4.1

CSD 3.4.1 includes the following enhancements:

- Support for additional antivirus, antispware and personal firewall applications.
The [Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators, Version 3.4.1](#), lists these applications.
- Customization of the Secure Desktop background (the vault with the lock icon) and its text color, and the dialog banners for the Desktop, Cache Cleaner, Keystroke Logger, and Close Secure Desktop windows.
Use this feature to replace the default images on the user desktop with those that are consistent with your branding policies or preferences. Choose **Secure Desktop Manager > Secure Desktop Customization** to access this feature.
Clicking the **Edit > Edit Using Local File Import** option in the Secure Desktop Customization panel in ASDM 6.1 and earlier to import an image displays a dialog box that instructs you to choose **Remote Access VPN > Clientless SSL VPN Access > Portal > Web Contents**. After doing so, click **Import** to transfer the file to the adaptive security appliance flash device. Then use the **Edit > Edit Using Device Web Contents** option in the Secure Desktop Customization panel to specify the application for the image. See the online help for details.
- Control over the severity (called logging level) of the hostscan.log file.
Secure Desktop Manager provides the option to record the CSD events to the hostscan.log file onto the user's computer. This log file is now the only CSD log file. The default logging level, off, does not generate this file, and removes any hostscan.log and csd.log files left from previous releases. Choose **Secure Desktop Manager > Logging Level** to access this feature. From that panel, you can access the online help for instructions.

Administrator Guidelines

Refer to the following sections for information you should know before installing and configuring CSD. These sections supplement the information provided in the [Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators, Version 3.4.1](#)

Reset All Button

The description of the **Reset All** button in the Secure Desktop Manager online help is incorrect. Clicking that button removes all unapplied changes from the current Secure Desktop Manager session.

Server Certificate Length Consideration

Many SSL connections using identity certificates with RSA key pairs that exceed 1024 bits can cause a high CPU usage on the adaptive security appliance and rejected clientless logins.

Application Compatibility Layer and User Account Protection

Windows Vista uses virtualization to provide application compatibility. CSD turns off user account control (UAC) from within Secure Desktop to avoid collisions with the CSD file system virtualization. Consequently, applications running over Secure Desktop do not always share the same resources, such as mapped drives, as non-secure desktop applications.

Downgrade Support

CSD supports upgrades and downgrades between 3.3 and 3.4.2 on the adaptive security appliance. Users can establish remote sessions with one or the other, but cannot connect to adaptive security appliances running CSD versions earlier than 3.2.1.

End User Guidelines

The following end user guidelines are the same in both 3.4.2 and 3.4.1. Be sure to communicate these guidelines to end users.

Responding to Java Warning Dialog Boxes

If a user who has not added the URL of the VPN as a trusted site initiates a Firefox connection to the adaptive security appliance, Firefox displays the following warning message in a dialog box: “The web site’s certificate cannot be verified. Do you want to continue?” Please instruct users to do the following:

Step 1 Click **Always trust content from this publisher**, then click **Yes**.

A second dialog box indicates “The application’s digital signature has been verified. Do you want to run the application?”

Step 2 Click **Always trust content from this publisher**, then click **Run**.

Following these two steps prevents the associated dialog boxes from appearing during subsequent connection attempts originating from that user profile on that computer.

User Interface Privilege Isolation

Because tasks such as Host Scan and idle mouse detection require monitoring of other processes, CSD cannot run at a low integrity level. This means that starting CSD sometimes requires privilege elevation. Users experience prompting for privilege elevation and have to consent to use CSD.

Internet Explorer (7 or later) on Vista runs at a low integrity level by default to avoid installation of software that monitors the system. This creates a conflict with CSD. Users who have limited privileges must add the URL of the adaptive security appliance to the trusted zone list before proceeding.

Home Directory Requirement

The home directory on the remote computer must not contain any folder or file named .cachedlg.zip.

Secure Desktop on Vista

Secure Desktop (the vault) cannot run over AnyConnect on Windows Vista.

If you want Secure Desktop to run on Windows 2000 and XP over an AnyConnect connection, you must configure CSD to identify Windows Vista and run Cache Cleaner on that O.S., as follows:

- Step 1** Use the Prelogin Policy option in the CSD menu to add an OS Check for Microsoft Windows. (If one is already present, continue with the next step.)
 - Step 2** Add a Registry Check node to the right of the Win 2K/XP/Vista line.
 - Step 3** Use the default value next to Key Path (that is, HKEY_LOCAL_MACHINE).
 - Step 4** Enter the following value into the adjacent text box:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\CurrentVersion
 - Step 5** Select **Matches** next to the String attribute.
 - Step 6** Enter 6.0 in the adjacent text box.
 - Step 7** Click **Update**.
 - Step 8** Click the end node to the right of the adjacent Success line and rename it “Windows Vista” to isolate computers that match this value.
 - Step 9** Click the end node to the right of the Failure line below, click Policy, and rename it “Windows 2K/XP” to specify a separate policy that, by default, configures Secure Desktop to run on these computers.
 - Step 10** Click the Windows Vista icon in the CSD menu.
 - Step 11** Check **Secure Desktop**.
 - Step 12** Click **Apply All**.
-

Windows Mail

CSD does not support Windows Mail, the e-mail client that comes with Windows Vista.

Internet Explorer, Microsoft Office, and Adobe Acrobat Interaction with Cisco Secure Desktop

CSD closes all instances of Internet Explorer, Microsoft Office applications, and Adobe Acrobat running on Windows operating systems before Secure Desktop installs or before users switch to the Secure Desktop.

If Desktop Switching is enabled, you cannot switch from a Secure Desktop session to the host desktop and then open Internet Explorer, Microsoft Office applications, or Adobe Acrobat. This Windows limitation might cause some applications running on the host desktop to fail.

Delays with Internet Explorer on Windows 2000

It can take about 45 seconds for Internet Explorer running on Windows 2000 to initiate the download of Secure Desktop if the user logs in using cached credentials (that is, if a user in an Active Directory domain logs in without a network connection to the domain controller). This scenario uses both DNS and NetBIOS to search for the domain controller, extending the connection time. To avoid this delay, instruct the user to log in using a non-domain (local) user account.

Microsoft Knowledge Base article no. [899875](#) provides the details that address this issue.

Cisco Security Agent with Secure Desktop and Cache Cleaner

Because Secure Desktop and Cache Cleaner connect tightly with the OS, the Cisco Security Agent often prompts the user to confirm that the CSD components can be trusted. It is important that the user confirms that they can be trusted when prompted by a dialog.

CSA Versions before V4.5 often prompt the user on the local desktop instead of Secure Desktop; for this reason we encourage that the user upgrade to CSA V4.5 or later, or contact the administrator to check the “Enable switching between Secure Desktop and Local Desktop” configuration option.

CSA Interoperability with the AnyConnect Client and CSD

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

To enable the AnyConnect VPN client and CSD, perform the following steps:

Step 1 Retrieve the CSA policies for the AnyConnect client and CSD. You can get the files from:

- The CD that shipped with the adaptive 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*.

ActiveX or Java Settings

CSD tries different methods to install itself on Microsoft Windows client computers until it finds a method that works. The installation is automatic and transparent to the user, however, one of the methods must be available on the remote computer and the user must have privileges to use that method. [Table 1](#) shows the installation methods and associated user requirements:

Table 1 CSD Installation Methods and Requirements

Installation Method	Remote User Requirement
ActiveX	Administrator privileges
Microsoft JavaVM	Power-user privileges
Sun JavaVM	Any user
Exe	Any user with execution permissions

The following Internet Explorer security 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

Do Not Change Cache Locations

Cache sessions may not get cleaned if a user changes cache locations during Secure Desktop and Cache Cleaner sessions.

CSD Installation through a Proxy

To specify CSD installation through a proxy server, regardless of the browser, go to the **Internet Options** control panel under Microsoft Windows, click the **Connections** tab, and click the **LAN Settings** button.

To use the ActiveX installation of CSD, go to the “Internet Options” control panel under Windows, click the **Advanced** tab, and enable the “Use HTTP 1.1” option.

To use the Java installation of CSD, go to the “Java” control panel under Windows, click the **General** tab, click the **Network Settings** button, and configure the proxy.

Starting Applications from within Folders Created inside Secure Desktop

Microsoft Windows treats folders created within Secure Desktop differently from other folders. An application cannot always determine the default folder location for files if you start it from within these folders. For example, if you create a folder within a Secure Desktop session, open the command prompt, change the directory to that folder without specifying the full path, and run FTP, it does not download files to that folder. We recommend that you specify the full path or explicitly change the working directory (for example, using the `lcd` command in the case of FTP) from within the applications. This problem occurs only for applications launched from within a shell. Otherwise, the problem does not occur.

History Not Erased With Multiple Explorer Windows

If multiple Windows Explorer windows are enabled using Windows 2000, Windows Explorer does not erase browser history because other Explorer windows could share it. Before users start Cache Cleaner, they should uncheck “Launch folder windows in a separate process” in the Windows Explorer **Tools > Folder Options > View > Launch** folder.

Caveats

For your convenience in locating caveats in the Cisco Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description.



Note

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

<http://www.cisco.com/support/bugtools>

To become a registered cisco.com user, go to the following website:

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

The following sections lists the caveats this release resolves and the open caveats.

Resolved Caveats

Table 2 lists the Severities 1–3 caveats that CSD 3.4.2 resolves.

Table 2 *Caveats Resolved by CSD 3.4.2*

Caveat ID	Description
CSCsx56105	CSD: Host Scan fails to recognize CSA 6.0 as a firewall
CSCsx98268	Corrupt libcurl.dll on Win XP not allowing AnyConnect Clients to connect
CSCsy17975	CSD unable to turn on Symantec Endpoint Protection AntiVirus
CSCsy61758	WebVPN login page blank intermittently after switching desktops
CSCsy62328	Norton Internet Security 2009 is not detected
CSCsz01382	AVG 8.5 free antivirus is not detected properly by Host Scan
CSCsz05166	CSD 3.4.1108 reports “internal error” for McAfee Personal Firewall 9.x
CSCsz10324	Keystroke Logger Detection crashes Cache Cleaner on 64-bit Vista
CSCsz39833	CSD truncates long host names

Open Caveats

Table 3 lists the Severities 1–3 caveats that are open in this release:

Table 3 *Open Caveats in CSD 3.4.2*

Caveat ID	Description
CSCsl10522	CSD: Cache Cleaner menu options do not apply to Mac OS and Linux
CSCsq73319	CSD: User can create files with existing names in Secure Desktop (Vault)
CSCsr99780	CSD: “Switching has been disabled” pop-up stays for approx. 40 secs.
CSCsu30996	CSD: Home page configured under group-policy does not open
CSCsu56816	CSD: Browser should display that Update is taking place
CSCsu56899	CSD: Prelogin Cert Check fails
CSCsv07813	CSD: Hostscan fails restarting logon page in Vault
CSCsv11862	CSD: Manual install unavailable via Firefox in Microsoft Windows
CSCsv20153	CSD: McAfee Antivirus does not get updated with Hostscan configured with AC SBL
CSCsv44098	CSD fails to bypass on mobile devices other than iPhone & Win Mobile
CSCsv61251	CSD: inst.exe downloaded on manual install on Linux
CSCsv68395	CSD ignores proxy configured via PAC file

Table 3 **Open Caveats in CSD 3.4.2**

Caveat ID	Description
CSCsv72868	CSD: Service pack detail not returned with 64 bit Vista with CC
CSCsv76223	CSD Linux: CC should clean the cache even if logged in as root.
CSCsx05118	CSD: Inspection has timed out or exited unexpectedly
CSCsx68071	CSD: Hostscan fails to recognize CSA 6.0.0.220 properly as an antivirus
CSCsy55560	Logging doesn't work with clientless and hostscan
CSCsy79634	Session Attribute logging information is missing with CSD logs
CSCsy81783	HostScan from csd 3.4 invoked UAC on Vista
CSCsy90640	Hostscan-advanced endpoint assessment dialog is too large
CSCsy98882	CSD Vault should allow AnyConnect Downloader from any temp folder
CSCsz70563	CSD: Intermittent cases when Host Scan does not load

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLynx, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco 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. (1002R)

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.

© 2010 Cisco Systems, Inc. All rights reserved.

