Release Notes for Cisco Secure Desktop, Release 3.4

Updated: May 6, 2010

Contents

Read the following sections carefully prior to installing, upgrading, and configuring Cisco® Secure Desktop 3.4:

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 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 is a multifunctional component of the Cisco SSL VPN solution. The main features of Cisco Secure Desktop 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. Cisco Secure Desktop 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* 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 Cisco 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 Cisco Secure Desktop, 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 Cisco Secure Desktop requires or supports.

Cisco ASA 5500 Series

Cisco Secure Desktop 3.4 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 Cisco Secure Desktop endpoint functions and list the endpoint OS's they support. The Cache Cleaner section also lists the supported browsers.

Host Scan

Host Scan supports the following OS's.

- 32- and 64-bit Microsoft Windows Vista
- 32- and 64-bit Windows Vista SP1
- 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
- 32- and 64-bit Mac OS X 10.5
- 32- and 64-bit (that is, 64-bit that can run 32-bit code) biarch Linux with the following requirements: libxml2, libcurl (with openssl support), openssl, glibc 2.3.2 or later, and libz.

  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 OS's:

- 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

Cache Cleaner supports the following installations:

- 32- and 64-bit Windows Vista
- 32- and 64-bit Windows Vista SP1
- 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.

Quality Enhancements

Cisco Secure Desktop 3.4 includes the following quality enhancements:

- Support for additional antivirus, antispyware and personal firewall applications.
- Improved Host Scan interoperability with AnyConnect

  The recommended AnyConnect version for use with CSD 3.4 is AnyConnect 2.3.xxxx or later.

- Improved Host Scan performance
- Improved Host Scan trouble-shooting

  Cisco Secure Desktop logs errors and warnings to the application log on Windows, and the syslog on Mac OS and Linux. Messages of all levels go to a hostscan.log and csd.log in the user's home folder. The location is dependent on the OS and VPN method, as follows:

  - Microsoft with AnyConnect Client start before logon (SBL): WINDOWS\system32\config\systemprofile\Application Data\Cisco
  - Microsoft without SBL: %APPDATA%\Cisco\Cisco HostScan
  - Apple Mac OS and Linux: ~/.cisco/hostscan (also accessed through $HOME/.cisco/hostscan). Both paths are case-specific.

Administrator Guidelines

Refer to the following sections for information you should know before installing and configuring Cisco Secure Desktop.

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. Cisco Secure Desktop turns off user account control (UAC) from within Secure Desktop to avoid collisions with the Cisco Secure Desktop 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

Cisco Secure Desktop supports upgrades and downgrades between 3.3 and 3.4 on the adaptive security appliance. Users can establish remote sessions with one or the other, but cannot connect to adaptive security appliances running Cisco Secure Desktop versions earlier than 3.2.1.

End User Guidelines

Be sure to communicate the following 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, Cisco Secure Desktop cannot run at a low integrity level. This means that starting Cisco Secure Desktop sometimes requires privilege elevation. Users experience prompting for privilege elevation and have to consent to use Cisco Secure Desktop.

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 Cisco Secure Desktop. 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) running on Windows Vista cannot run over AnyConnect.

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

Step 1 Use the Prelogin Policy option in the Cisco Secure Desktop 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 Cisco Secure Desktop menu.

Step 11 Check **Secure Desktop**.

Step 12 Click **Apply All**.

Windows Mail

Cisco Secure Desktop 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 (http://support.microsoft.com/default.aspx?scid=kb;en-us;899875).

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 Cisco Secure Desktop 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 Cisco Secure Desktop

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 Cisco Secure Desktop to interoperate with the adaptive security appliance.

To enable the AnyConnect VPN client and Cisco Secure Desktop, perform the following steps:

Step 1 Retrieve the CSA policies for the AnyConnect client and Cisco Secure Desktop. 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

Cisco Secure Desktop 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 Cisco Secure Desktop 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.

Cisco Secure Desktop Installation through a Proxy

To specify Cisco Secure Desktop 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 Cisco Secure Desktop, 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 Cisco Secure Desktop, 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.

Open 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 Severities 1–3 caveats are open in this release of Cisco Secure Desktop:

Table 1 Open Caveats in CSD 3.4

Caveat ID	Description
CSCsq73319	CSD: User can create files with existing names in Secure Desktop (Vault)
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

Table 1 Open Caveats in CSD 3.4

Caveat ID	Description
CSCsv61251	CSD: inst.exe downloaded on manual install on Linux
CSCsv64389	CSD folder not deleted when the Vault closes
CSCsl10522	CSD: Cache Cleaner menu options do not apply to Mac OS and Linux
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
CSCsr51160	CSD: CAC authentication causes error on Microsoft Windows Vista
CSCsv44098	CSD fails to bypass on mobile devices other than iPhone & Win Mobile
CSCsv63073	CSD: Error initializing main application on XP 64 bit
CSCsv68008	CSD: Host Scan adds a new rule after each enforcement cycle on Vista
CSCsv72868	CSD: Service pack detail not returned with 64 bit Vista with CC
CSCsv68395	CSD ignores proxy configured via PAC file