Release Notes for Cisco Secure Desktop, Release 3.2.1

24 Dec 2008, OL-15306-03

Contents

Read the following sections carefully prior to installing, upgrading, and configuring Cisco® Secure Desktop 3.2.1:

Introduction to Cisco Secure Desktop

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 on Microsoft Windows Vista, Windows XP, and Windows 2000, Apple Mac OS X 10.4, and Linux. Host Scan reports results to the security appliance, which integrates them with the dynamic access policies (DAPs).

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

- *Secure Session*, also called Secure Desktop or 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 U.S. Department of Defense (DoD) sanitation algorithm removes the encrypted partition. Typically used during clientless SSL VPN sessions, Secure Session 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. This feature is available on Microsoft Windows XP and Windows 2000.
- *Cache Cleaner*, an alternative to Secure Session, 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. Cache Cleaner runs on Microsoft Windows Vista, Windows XP, Windows 2000, Apple Mac OS X 10.4 (PowerPC or Intel), and Linux.
- *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 Session, 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.

For more information about these features; and installation, upgrade, and configuration instructions; refer to the *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*, Version 3.2.1.

Requirements

The following sections identify the security appliance platform and end-use interoperability that Cisco Secure Desktop requires or supports.

Platform– Cisco ASA 5500 Only

This release of Cisco Secure Desktop requires installation on a Cisco ASA 5500 Series running Version 8.0(3) or later.

End-use Interoperability

For the latest results of connectivity tests with OS's, browsers, clients, clientless, and e-mail applications, see the *Cisco ASA 5500 Series VPN Compatibility Reference*.

OS and Browser Interoperability

For the latest OS and browser test results with Cisco Secure Desktop, the AnyConnect Client, Clientless SSL VPN, see the *Cisco ASA 5500 Series VPN Compatibility Reference*.

New Features and Enhancements

The following sections identify the new features and enhancements in Cisco Secure Desktop Release 3.2.1.

Integration with AnyConnect Client Start Before Logon

Release 3.2.1 supports Release 2.1 of the Cisco AnyConnect Client, with the Start Before Logon (SBL) feature of AnyConnect Client enabled or disabled.

The Cisco Secure Desktop modules are not interoperable with AnyConnect Client Release 2.0 if SBL is enabled.

Host Scan Support for Mac OS and Linux

As a condition for the completion of a Cisco AnyConnect or clientless SSL VPN connection, the remote computer installs the Cisco Secure Desktop Host Scan module, which scans for a greatly expanded collection of antivirus and antispyware applications, associated definitions updates, and firewalls. It also scans for any registry entries, filenames, and process names that you specify. It sends the scan results to the security appliance. The security appliance uses both the user login credentials and the computer scan results to assign a Dynamic Access Policy (DAP).

With an Advanced Endpoint Assessment License, you can enhance Host Scan by configuring an attempt to update noncompliant computers to meet version requirements so that they meet conditions required for assignment of prelogin policies.

Release 3.2 introduced Host Scan support for remote computers running Microsoft Windows Vista, Windows XP, and Windows 2000. Release 3.2.1 adds Host Scan support for remote computers running Mac OS X 10.4 and Linux. The Host Scan extensions let you configure separate enforcement settings for Microsoft Windows, Mac OS, and Linux.

Remediation of Multiple Applications

Advanced Endpoint Assessment now lets you configure remediation of more than one application for each type supported (antivirus, antispyware, and firewall). If you specify more than one application of a given type, Host Scan attempts to remediate the one that is present on the connecting computer.

Policy and Cache Cleaner Support for Mac OS and Linux

The prelogin assessment includes checks for Mac OS X 10.4 and Linux, as well as Microsoft Windows Vista, Windows XP, and Windows 2000. The Cache Cleaner settings assigned to each Cisco Secure Desktop policy now supports all five of these operating systems, so the Mac & Linux Cache Cleaner option is no longer present on the Secure Desktop Manager menu.

Keystroke Logger and Host Emulation Detection on Vista

The detection of keystroke loggers and host emulators as part of each Cisco Secure Desktop policy now works for Microsoft Windows Vista, as well as Windows XP and Windows 2000.

Secure Desktop List of Allowed Applications

Secure Desktop Manager lets you specify the applications that can run on a Secure Desktop session, in addition to that of the originating browser. To do so, choose **Secure Desktop Settings** under the policy name in the Secure Desktop Manager menu, check **Restrict application usage to the web browser only**; and enter the names of the executable files into the list box that opens or click **Add** and select the options from a preconfigured list. You can also specify a hash to help ensure the executable file specified is authentic; however, if you do this, you should add an entry for each version of the application you want to allow.

Secure Desktop Session Disconnection Timer

Secure Session displays a countdown when nine seconds are left for the "Enable Secure Desktop inactivity timeout," accompanied by an optional audible timer that beeps each second. The user can restart the timer by moving the mouse.

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 server certificate keys that exceed 1024 bits can cause a high CPU usage and rejected clientless log-ins.

User Connection to Release 3.1.1 following a Connection to a Later Version

If a computer with ActiveX ends a Secure Session with a security appliance running Cisco Secure Desktop Release 3.2 or 3.2.1, and then attempts to establish a Secure Session with one running Release 3.1.1, the message "The installer has had to abort the process..." appears on the remote computer and the connection attempt fails (CSCsi05637).

If this occurs, the remote user must choose **Internet Options > Settings > View Objects** and delete the "InstallerWeb Control" object before attempting to reconnect again.

Cache File System

The default size of the cache file system (20 Mb) is not enough to support all four versions of the AnyConnect packages (Windows, Linux, Mac OS X arch386, Mac OS X ppc) and Cisco Secure Desktop. If you want to install all five client packages on the security appliance, you should first increase the maximum size of cache file system entering the **(config-webvpn)# cache-fs limit** command. The recommended size of the cache file system is 22 Mb.

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 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 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*.

Remote Privilege Requirements

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

Cisco AnyConnect VPN Client

You can configure both the Secure Session component of Cisco Secure Desktop and Cisco AnyConnect VPN Client to run simultaneously on client PCs. If you configure Cisco Secure Desktop to permit switching between the Secure Desktop and the local desktop, the AnyConnect session becomes available to both. To do so, click **Secure Desktop General** and check "Enable switching between Secure Desktop and Local Desktop for each location."

Windows Cache Cleaner Profile Under Netscape and Mozilla

To create a temporary Mozilla profile, Cache Cleaner uses the default profile as a template. If no default profile is present, Cache Cleaner looks for a profile with the same name as the logged in user. If none is present, Cache Cleaner creates a new profile.

E-mail Messages

When using an e-mail application configured to use POP3, the client downloads e-mail messages to the local computer, after which they remain only on the local computer. If you check "Allow email applications to work transparently" in the Secure Desktop Settings window, Secure Session does not wipe out the messages after the session ends, even if the application starts within Secure Session. This feature applies to the following e-mail applications:

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

Client Guidelines

Be sure to communicate the following guidelines to remote users.

Home Directory Requirement

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

Delays on Cluttered Systems

Browser plug-ins, shell extensions, and a cluttered registry can greatly extend the time needed for Secure Session to perform the read and write operations on the registry. Secure Session performs registry operations to do the filtering necessary to perform its tasks. It can therefore take a longer period of time than one would expect for the clientless SSL VPN login page to open a Secure Session if the remote computer is slow or is cluttered.

Delays with Internet Explorer on Windows 2000

It can take about 45 seconds for Internet Explorer running on Microsoft Windows 2000 to initiate the download of Secure Session 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

Because Secure Session and Cache Cleaner connect tightly with the Operating System, 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 Session; for this reason we encourage that the user upgrade to CSA V4.5 or contact the administrator to check the "Enable switching between Secure Desktop and Local Desktop" configuration option.

Do Not Change Cache Locations

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

Keystroke Logger Detection Limitations

Cisco Secure Desktop only detects keystroke loggers, if configured, if the user has administrator privileges. If the user does not, keystroke logger detection does not run.

It may not be possible for Cisco Secure Desktop to detect all keystroke loggers present, including but not limited to hardware keystroke logging devices.

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 Session

Microsoft Windows treats folders created within Secure Session 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 Session, open the command prompt, change the directory to that folder without specifying the full path, and run FTP, FTP 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 Microsoft 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.

Secure Session Only Supports Applications Installed in the Default Location

For optimum security, only applications installed under the Windows and Program Files directories are accessible under Secure Session. Secure Session does not support or allow access to applications not found in these default installation locations.

Open Caveats

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

- CSCsi87951 (CSD fails to print through Citrix application)

  Symptom: Printing to a spool fails with a Citrix application over a Secure Session. Printing from any other application works as expected.

  Workaround: Use a local printer, not a print spool.

- CSCsi91653 (Stuck at Processing, Please wait... message)

  Symptom: When Internet Explorer 7.0 opens in Secure Desktop, it gets stuck after displaying the message, "Processing, please wait..."

  Conditions: This issue is intermittent, usually occurring with every five or six connection attempts.

  Workaround: Clear the cache and cookies, then reconnect.

- CSCsj35242 (Prelogin certificate check needs to validate the certificate)

  Symptom: The prelogin assessment certificate check tests for the presence of a certificate, but does not determine whether the certificate is valid.

- CSCsj78392 (CSD: Hostscan.exe lingers if you log out too quickly)

  Symptom: hostscan.exe process lingers if you log out too quickly.

  Conditions: If a user logs into the portal, then immediately logs out (without waiting about 15 seconds), the hostscan.exe process may linger.

  Workaround: Ask users to wait 30 seconds after logging in before logging off.

Resolved Caveat

This release of Cisco Secure Desktop resolves the following caveat:

- CSCsj00288 (Keystroke Logger check fails when HP Quick Launch application is running)

  Symptom: Cisco Secure Desktop displays the user message “Inspection has timed out or exited unexpectedly.”

  Conditions: All of the following must be true:

  - “Check for Keystroke Loggers” must be enabled on the security appliance.
  - A keystroke logger is present on the remote computer.
  - The HP Quick Launch Buttons application (qlbctrl.exe) is running on the remote computer.