Release Notes for Cisco Secure Desktop, Release 3.2

Dec. 23, 2008 OL-14385-02

Contents

Read the following sections carefully prior to installing, upgrading, and configuring Cisco® Secure Desktop 3.2:

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 is a new feature that checks for watermarks on a remote computer. These watermarks can signify whether the computer is corporate-owned. The watermark options include a registry value, a filename and optional hash to validate the file, and a digital certificate. You can also use Host Scan to configure a check for the presence of required end system software, including antivirus, personal firewall, and antispyware applications and updates. With the introduction of Host Scan, Cisco Secure Desktop is enhanced in this release to support hundreds of versions of these applications, is available for Microsoft Windows Vista and XP and is integrated with the dynamic access policy (DAP) feature in Cisco ASA Software Version 8.0.

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 the desktop on the remote device to signify a safe environment for the remote user to work in. Upon session termination, it uses a U.S. Department of Defense (DoD) sanitation algorithm to remove 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 Microsoft Windows 2000.
- 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. As the administrator, you can use Cisco Secure Desktop Manager to specify the keystroke logging applications that are safe or let the remote user interactively approve of the applications the scan identifies. Both keystroke logger detection and host emulation detection are available with Cache Cleaner for Microsoft Windows or Secure Session.
- 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, XP, 2000, and 98; Apple Macintosh OS X 10.4 (PowerPC or Intel); and Linux.

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 to reduce risks associated with using such technologies.

For installation, upgrade, and configuration instructions, refer to the *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*, Version 3.2.

Requirements

The following sections identify the platforms, browsers, clients, and applications that the 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(2) or later.

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 shows which operating systems the Cisco Secure Desktop modules support.

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

Table 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.

Java must be installed, enabled, and working properly under the browser in use on the remote computer. Cisco Secure Desktop identifies the Java Virtual Machine (JavaVM), Microsoft or Sun, that is configured and uses it to install the Cisco Secure Desktop components. JavaVM 1.4 is required for Cisco Secure Desktop to install components on computers running Microsoft Windows, and JavaVM 1.5 is required for those running MacOS and Linux. On Linux, the browser must be configured to use JavaVM; just checking “Allow use Java” is not sufficient for Cisco Secure Desktop.

Clientless SSL VPN

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

Table 3 Clientless SSL VPN and Cisco Secure Desktop Interoperability

	Cisco Secure Desktop Remote Module			
Operating System[1]	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 4 shows the interoperability of the AnyConnect Client modes with Cisco Secure Desktop modules on remote computers.

Table 4 AnyConnect Client and Cisco Secure Desktop Interoperability

		Cisco Secure Desktop Remote Module			
AnyConnect Client Mode (SBL must not be enabled)[1]	Operating System[2]	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.

E-mail Applications

When using an e-mail application configured to use POP3 (a standard communication protocol between e-mail applications and e-mail servers), the client downloads e-mail messages to the local computer, after which, these messages exist only on the local computer. The Cisco Secure Desktop Manager “Allow email applications to work transparently” Secure Session parameter in the Secure Desktop Settings window lets the administrator choose whether to avoid deleting e-mail messages. If this parameter is checked, Secure Session does not remove files saved by e-mail applications, even when the application starts within Secure Session. However, e-mail applications cannot open files created by other applications launched from within Secure Session.

This feature applies to the following e-mail applications:

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

New Features and Enhancements

The following sections identify the new features and enhancements in Cisco Secure Desktop Release 3.2.

Host Scan

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, firewalls, operating systems, and associated updates. 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.

Integration with Dynamic Access Policies

The security appliance integrates the Cisco Secure Desktop features into dynamic access policies (DAPs). Depending on the configuration, the security appliance uses one or more endpoint attribute values in combination with optional, AAA attribute values as conditions for assigning a DAP. The Cisco Secure Desktop features supported by the endpoint attributes of DAPs include OS detection, prelogin policies, Basic Host Scan results, and Endpoint Assessment.

Simplified Prelogin Assessment Checks

Cisco Secure Desktop now simplifies the configuration of prelogin checks to perform on remote Microsoft Windows computers. Cisco Secure Desktop lets you add, modify, remove, and place conditions on endpoint checking criteria using a simplified, graphical view of the checks. As you use this graphical view to configure sequences of checks, link them to branches, deny logins, and assign endpoint profiles, Cisco Secure Desktop Manager records the changes to an XML file. Based on the checks the endpoint traverses, the assessment assigns a prelogin policy that determines whether Secure Session, Cache Cleaner, or neither are installed, and the settings that are assigned to Secure Session or Cache Cleaner.

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.

Release 3.1.1 User Connection following a Release 3.2 Connection

If a computer with ActiveX ends a Secure Session with a security appliance running Cisco Secure Desktop Release 3.1.1, and then attempts to establish a Secure Session with one running Cisco Secure Desktop Release 3.2, 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 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 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 5 shows the installation methods and associated user requirements:

Table 5 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

SSL VPN Client

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

File Checks on Windows Are Not Case-Sensitive

Secure Desktop Manager retains the case of the text you enter to check for a path to a file on the remote device. You can specify file paths in the following dialog boxes:

- File Check accessible from the Windows Location Settings [Prelogin Policy in 3.2.1] window.
- Add or Edit File Scan accessible from the Host Scan window.

The match results are case-sensitive only if the devices are running Linux or MacOS. The Windows file system is not case-sensitive.

Clientless SSL VPN Session Timeout Counting Continues after Secure Desktop Inactivity Timeout Expires

If the Idle Timeout value in the Configuration > Clientless SSL VPN Access > Group Policies > Add or Edit > General > More Options area exceeds the Security Desktop inactivity timeout and the latter reaches its threshold, the show vpn-session-db webvpn command shows the session is active until the former timeout value reaches its threshold.

The Clientless SSL VPN Access Inactivity Timeout overrides the Security Desktop inactivity timeout. We recommend that you set the former to exceed the latter so that the ASA database accurately represents the number of active clientless SSL VPN sessions.

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.

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 requires a lot of registry operations to do the filtering necessary to perform its tasks. It can therefore take three minutes or longer for the clientless SSL VPN login page to open in 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 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.

Location Settings: Do Not Use Quotes With Registry Key Names

Users must not type quotes in a Registry Key name that includes spaces.

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, for users with Administrator privileges. If users do not have those privileges, the 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.

If you use Secure Desktop Manager to configure keystroke logger detection and leave the "Force admin control on list of safe modules" attribute unchecked, and suspected keystroke loggers are found on the remote device, a window displays the path and name of each suspected module. The remote user must acknowledge that each module is safe or terminate the connection. To determine whether a given module is safe, the user can click the adjacent "Click for info" link to display Google search results.

Cisco Secure Desktop Installation through a Proxy

To specify Cisco Secure Desktop installation through a proxy server without regard to the browser, go to the "Internet Options" control panel under 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

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, and run FTP, FTP does not download files to that folder if you do not specify the full path. 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 essentially concerns applications launched from a shell. Otherwise, the problem does not occur.

History Not Erased With Multiple Explorer Windows

When multiple Windows 2000 Explorer windows are enabled (Windows Explorer > Tools > Folder Options > View > Launch folder windows in a separate process), Windows Explorer does not erase browser history because other Explorer windows could share it. Users need to uncheck this option before starting the Cache Cleaner.

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 issue, usually occurring with every five or six connection attempts.

  Workaround: Clear the cache and cookies, then reconnect.

- CSCsj00288 (Keystroke Logger check fails when HP Quick Launch app 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.

- 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.

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.