Release Notes for Cisco Secure Desktop, Release 3.3

23 December 2008

Contents

Read the following sections carefully prior to installing, upgrading, and configuring Cisco® Secure Desktop 3.3:

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 3.2.1 for more information about the features; and for installation, upgrade, and configuration instructions.

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

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

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).

- *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 U.S. Department of Defense (DoD) sanitation algorithm removes 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. Secure Desktop is available for computers running Microsoft Windows Vista, XP, and Windows 2000.
- *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. 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 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 security appliance platform and end-use interoperability that Cisco Secure Desktop requires or supports.

Platform– Cisco ASA 5500 Only

Cisco Secure Desktop 3.3.0.118 requires installation on a Cisco ASA 5500 Series running Version 8.03.1 or later and ASDM 6.0.3 or later.

End-use Interoperability

Note KB935855 or Windows Vista SP1 (or later) must be installed for Windows Vista support of Secure Desktop.

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 Feature Enhancement – Secure Desktop on Vista

Release 3.3 now lets you configure Secure Desktop to run on remote computers running Microsoft Windows Vista. Previously, Secure Desktop was limited to computers running Windows XP or 2000.

Note 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**.

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.

"Launch the following application after installation" Attribute

The "Launch the following application after installation" attribute on the Secure Desktop General panel lets you start an application automatically after Secure Desktop installs on the remote PC. Enter only the path to the application that follows the C:\Program Files\ portion. The application must be in the Program Files directory.

Application Compatibility Layer and User Account Protection

Windows Vista uses virtualization to provide application compatibility. Cisco Secure Desktop 3.3 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.

Persistence of Firewall Rules

The Host Scan extensions let you configure optional firewall rules. These rules apply at the beginning of each VPN session, and apply even after the VPN session closes. To return the firewall to its previous state, users must remove these rules manually. Therefore, we recommend that the administrator use firewall rules with discretion.

File Structure

Each securedesktop-asa-<*Cisco-Secure-Desktop-version*>.pkg on the Cisco Secure Desktop Downloads page contains the Cisco Secure Desktop image, including the Host Scan updates and Advanced Endpoint Assessment (AEA) remediation software. You must install and retain this image on the flash device of the ASA to enable Cisco Secure Desktop. To use the AEA, you must have an AEA license.

Cisco Secure Desktop automatically creates the /sdesktop/ directory on the flash device of the ASA and inserts the default data.xml file into the directory if they are not present when you enable Cisco Secure Desktop. The /sdesktop/data.xml file is the Cisco Secure Desktop configuration file. When you configure settings or upgrade Cisco Secure Desktop, it automatically writes the changed or new settings to the /sdesktop/data.xml file. Disabling Cisco Secure Desktop does not alter this file. You can delete this file, disable Cisco Secure Desktop, and re-enable it if you want to start again with default settings. Be sure to back up the file before deleting it and before upgrading the Cisco Secure Desktop image. You can also transfer a copy of the /sdesktop/data.xml file to the flash device of another ASA before enabling Cisco Secure Desktop on it if you want to duplicate the Cisco Secure Desktop configuration.

Encryption of Files on Network Folders

Cisco Secure Desktop no longer allows encryption of files on network folders. Because Cisco Secure Desktop does not clean up files written to mapped network drives, we strongly recommend that you check the "Disable access to network drives and network folders" check box in each Secure Desktop Settings window.

Windows Mail

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

Downgrade Support

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

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 Secure Desktop and Cisco AnyConnect VPN Client to run simultaneously on client PCs, except for those running Windows Vista. If you configure Cisco Secure Desktop to permit switching between the Secure Desktop and the local desktop for Windows 2000 and Windows XP, the AnyConnect session becomes available to both. To do so, click **Secure Desktop General** underneath the Windows 2K/XP node 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 Desktop does not wipe out the messages after the session ends, even if the application starts within Secure Desktop. This feature applies to the following e-mail applications:

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

Remote User Guidelines

Be sure to communicate the following guidelines to remote users.

User Interface Privilege Isolation

Because tasks such as Host Scan and console idle 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 will experience prompting for privilege elevation and have to consent to use Cisco Secure Desktop.

Internet Explorer (7 or later) on Vista runs with 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 security appliance to the trusted zone list before proceeding.

Limitations on Visibility of the File System

Only the Documents and Settings, WINDOWS and Program Files directory on Microsoft Windows are visible from the Secure Desktop (Vault).

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 Desktop to perform the read and write operations on the registry. Secure Desktop 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 Secure Desktop if the remote computer is slow or is cluttered.

Internet Explorer and Adobe Acrobat on Windows Vista

Cisco Secure Desktop closes all instances of Internet Explorer and Adobe Acrobat running on Microsoft Vista before Secure Desktop installs. If Desktop Switching is enabled, you cannot switch from a Secure Desktop session to the regular desktop and then open Internet Explorer or Acrobat. This Vista limitation might cause some applications running on the regular desktop to fail.

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 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

Because Secure Desktop 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 Desktop; 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 Desktop 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 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, 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 Desktop 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 Desktop. It 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 Desktop session. Printing from any other application works as expected.

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

- 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.

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.