Release Notes for Cisco Secure Desktop, Release 3.1.1

October 2006

Contents

These release notes describe the new features in Cisco® Secure Desktop 3.1.1, enhancements, changes to existing features, limitations and restrictions (“caveats”), and fixes. Read these release notes carefully prior to installing, upgrading, and configuring CSD.

These release notes include the following sections:

- Introduction, page 1
- Requirements, page 2
- New Features and Enhancements, page 4
- Administrator Guidelines, page 5
- Client Guidelines, page 7
- Caveats, page 8

Introduction

Cisco Secure Desktop (CSD) is an optional software package you can install on the security appliance to validate the security of client computers requesting access to your SSL VPN, help ensure they remain secure while they are connected, and attempt to remove traces of the session after they disconnect.

After a remote PC running Microsoft Windows connects to the security appliance, CSD installs itself and uses the IP address and presence of specific files, registry keys, and certificates to identify the type of location from which the PC is connecting. Following user authentication, CSD uses optional criteria as conditions for granting access rights. These criteria include the operating system, antivirus software, antispyware, and personal firewall running on the PC.

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

To help ensure security while a PC is connected to your network, the Secure Desktop, a CSD application that runs on Microsoft Windows XP and Windows 2000 clients, limits the operations available to the user during the session. For remote users with administrator privileges, Secure Desktop uses the 168-bit Triple Data Encryption Standard (3DES) to encrypt the data and files associated with or downloaded during an SSL VPN session. For remote users with lesser privileges, it uses the Rivest Cipher 4 (RC4) encryption algorithm. When the session closes, Secure Desktop attempts to overwrite and remove data from the remote PC using the U.S. Department of Defense (DoD) security standard for securely deleting files. These actions will reduce the risk of cookies, browser history, temporary files, and downloaded content remaining after a remote user logs out or an SSL VPN session times out. CSD also can attempt to uninstall itself from the client PC. Given limitations of the Microsoft operating system, no technology that interoperates with the 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 to reduce risks associated with using such technologies.

Cache Cleaner, which attempts to wipe out the client cache when the session ends, supports Windows XP, Windows 2000, Windows 9x, Linux, and Apple Macintosh OS X clients.

For installation, upgrade, and configuration instructions, refer to the guide that names your security appliance:

- *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*
- *Cisco Secure Desktop Configuration Guide for VPN 3000 Concentrator Series and Catalyst 6500 Series WebVPN Services Module Administrators*

Requirements

The following sections identify the platforms, browsers, clients, and applications that the CSD requires or supports.

Platforms

This release of CSD requires interoperability with a platform running one of the following releases:

- Cisco ASA 5500 Series running Version 7.1(1) or later
- Cisco VPN 3000 Series Concentrator, Release 4.7.1 or later
- Cisco WebVPN Services Module, Release 1.2 or later, installed in a Cisco Catalyst® 6500 Series switch.

Supported Browsers

CSD supports the following browsers on the client:

- Internet Explorer 6.0 – 7 (Beta)
- Netscape 7.x – 8

  If you use Netscape 8 to install Windows Cache Cleaner, it starts Internet Explorer and cleans only the Internet Explorer cache.
- Mozilla 1.7.x

- Mozilla Firefox 1.0.x – 1.5

  If you use Firefox to install Windows Cache Cleaner, it starts Internet Explorer and cleans only the Internet Explorer cache.

To administer CSD, you need one of the following browsers:

- Internet Explorer 6.0 SP2 – 7 (Beta)
- Netscape 7.x – 8
- Mozilla 1.7.x
- Mozilla Firefox 1.0.x – 1.5

Mac & Linux Cache Cleaner Client Requirements

The Cache Cleaner for Macintosh & Linux requires that Java be installed, enabled, and working properly under the browser in use on the client. The Mac & Linux Cache Cleaner cleans only the default location of Netscape, Mozilla, or Safari.

Note The home directory must not contain any folder or file named .cachedlg.zip.

Cisco Security Agent (CSA) Compatibility

The Cisco Security Agent (CSA) V4.5 is compatible with both the Cisco Secure Desktop (CSD) and the Cisco SSL VPN Client (SVC) on Windows Operating Systems. Versions of CSA preceding V4.5 are not compatible with CSD/SVC.

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. To avoid deleting e-mail messages, CSD, at the administrator's discretion, does not remove files saved by e-mail applications, even when the application starts within the secure desktop. However, e-mail applications cannot open files created by other applications launched from within a secure desktop.

This feature applies to the following e-mail applications:

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

New Features and Enhancements

This section identifies the new features and enhancements.

Cisco Secure Desktop Manager

You can now install CSD 3.1.1 on the Cisco ASA 5500 Series running Version 7.1(1). Cisco Secure Desktop Manager (CSDM) is the Java-based Internet browser interface you use to configure CSD on the ASA 5500.

The ASDM Configuration > VPN > WebVPN > CSD Setup menu path provides the facility to install, upgrade, enable, and disable the CSD software on the ASA 5500 Series.

First, use ASDM to install and enable CSD. Once you enable CSD, choose Configuration > CSD Manager to access CSDM.

Refer to *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators* for detailed installation and configuration instructions.

Note Context-sensitive online help documentation is also available from the CSDM windows.

Support for the Japanese Operating System

CSD supports the Japanese operating system in the English language.

System Detection Support for Protection Software Upgrades

In CSD Version 3.1.1.27 and later versions, System Detection supports the following protection software upgrades, in addition to the ones listed in the *Cisco Secure Desktop Configuration Guide* for the security appliance you are using:

- Norton Personal Firewall 2006
- McAfee Personal Firewall Plus 2006 Version 7.0
- ZoneAlarm Pro 6.0
- AVG 7.1
- Trend Micro OfficeScan 7.0

Support for Internet Browser Upgrades

Secure Desktop supports the following Internet browser upgrades:

- Netscape 8
- Firefox 1.5
- Internet Explorer 7 (Beta)

If you use Netscape 8 or Firefox to install Windows Cache Cleaner, it starts Internet Explorer and cleans only the Internet Explorer cache.

Multiple Certificate Store Search Criteria

In addition to using the personal certificate store for location matching, CSD also supports the following certificate search criteria:

- CA—Certification authority certificates.
- MY—Certificate store that holds certificates with associated private keys.
- ROOT—Root certificates.
- SPC—Software Publisher Certificate.

Cache History Preservation in Internet Explorer

In previous versions, Cache Cleaner attempted to remove browser history, including the history of recently typed addresses, from remote PCs. Now Cache Cleaner attempts to remove both the current session cache and history from remote PCs only if you choose Windows Location Settings > Cache Cleaner and check **Clean the whole cache in addition to the current session cache (IE only)**.

Administrator Guidelines

Refer to the following sections for information you should know before installing and configuring CSD.

Remote Client Installation Privilege Requirements

The 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 client and the user must have privileges to use that method. The installation methods and associated user requirements are as follows:

Table 1 CSD Installation Methods and Requirements

CSD Installation Method	Client User Requirement
ActiveX	Administrator privileges
Microsoft JVM	Power-user privileges
Sun JVM	Any user
Exe	Any user with execution permissions

SSL VPN Client

You can configure both the Secure Desktop component of CSD and Cisco SSL VPN Client (SVC) to run simultaneously on client PCs. If you configure CSD 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.

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 exists, Cache Cleaner creates a new profile.

Administrator Guidelines for the VPN 3000 Series Concentrator Only

The following guidelines apply only if CSD is running on a VPN 3000 Series Concentrator.

Downgrading a VPN 3000 Series Concentrator

Note the following before downgrading a VPN 3000 Series Concentrator equipped with CSD:

- VPN 3000 Concentrator Releases 4.7.1 and later require CSD 3.0.2.278 and above.
- We do not support CSD releases earlier than 3.0.2.278.
- If you downgrade the VPN 3000 Concentrator to a release earlier than 4.7.1, be sure to uninstall CSD before downgrading, and do not reinstall CSD.

Downgrade a VPN 3000 Concentrator as follows:

Step 1 Uninstall CSD first.

Caution VPN 3000 Concentrator versions earlier than 4.7 do not provide a provision to uninstall CSD. A failure to uninstall before downgrading leaves you without an interface to uninstall CSD, and the operating system perceives a loss of flash memory storage.

Step 2 Downgrade the VPN 3000 Concentrator to the version you require.

Step 3 Install CSD 3.0.2.278 or later if you downgraded to Release 4.7.1 or later.

Chunked Transfer-Encoding Required for Proxy Server On VPN 3000 Concentrator Series

If you use a proxy server with WebVPN on the VPN 3000 Concentrator, the proxy server must support the Transfer-Encoding HTTP header value “chunked”. One effect of not supporting this value is that mail text entries displayed by Microsoft Outlook Web Access remain in a “Loading” state instead of showing the e-mail content.

Save after Changing the Hostname on a VPN 3000 Concentrator

Secure Desktop installation (.EXE version) requires that the hostname be configured on the VPN 3000 Concentrator. Either place the Fully Qualified Domain Name (FQDN) in the “System Name” field under [Configuration > System > General > Identification], or place the host name in the “System Name” field and configure the domain name under [Configuration > System > Servers > DNS]. The host name and domain name are combined to form the FQDN (for example, systemname.domain.com).

When you change the Hostname, you must click **Save** under the Secure Desktop Manager to update the client installer with the new Hostname.

Client Guidelines

Be sure to communicate the following guidelines to CSD users.

Cisco Security Agent

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

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

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 Desktop and Cache Cleaner sessions.

Keystroke Logger Detection Limitations

CSD only detects keystroke loggers, if configured, for users with Administrator privileges.

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

Cisco Secure Desktop Installation through a Proxy

To specify CSD 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 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

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, open the command prompt, change the directory to that folder, and run FTP, FTP does not download files (whose full paths are not provided) to that folder. We recommend that you specify the full path or explicitly change the working directory (for example by 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.

Delay with Internet Explorer on Windows 2000

It can take about 45 seconds for Internet Explorer running on Windows 2000 to initiate the download of CSD 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).

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 Desktop Only Supports Applications Installed in the Default Location

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

Caveats

The following sections list both the open and closed caveats.

Open Caveats - Release 3.1.1

CSD had no known caveats at the time of publication of this document. For the latest up-to-date list, use the Bug Navigator available on
http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Resolved Caveats - Release 3.1.1

Release 3.1.1 resolves the following issues:

- CSCsc12461

  Symptom: Secure Desktop did not start on some PCs (for example, some laptops and tablet PCs). The main.exe program consumed all of the CPU for a few minutes, then it terminated.

  Condition: This problem originated from a compatibility issue with the Data Execution Protection (DEP) feature implemented in the hardware of some PCs, and in the software in Windows XP SP2.

- CSCsc57907

  Symptom: Clients ran out of virtual memory when using CSD.

- CSCsc58518

  Symptom: The ASDM search feature could not search any CSD nodes.

  Conditions: All

- CSCsc73672

  Symptom: The word “impossibility” in an error message was awkward.

- CSCse24947

  Symptom: Cache Cleaner failed to install on MacOS X.

  Condition: Loading the installation module from Safari running on the user's Macintosh was exceptionally slow.

- CSCse48309

  Symptom: After switching to Secure Desktop on a Windows PC, it took a long time for the login prompt to appear in Internet Explorer.

  Conditions: Java 1.5 was installed.

Resolved Caveats - Release 3.1

Release 3.1 resolves the following issues:

- CSCef20063

  Symptom: CSD did not delete history files.

  Conditions: Internet Explorer 6.0 over Windows 2000

- CSCef87806

  Symptom: Adding a picture from the Secure Desktop Space affected the guest machine.

- CSCeg02025

  Symptom: Jasc Paint Shop Pro started in Secure Desktop displayed the following message:

  ```
  The folder listed below is used to saved your user files. It is not currently
  accessible. C:\Documents and settings\Administrator\My Documents\My PSP8 Files\
  ```

  Conditions: Starting Jasc Paint Shop Pro in Secure Desktop yielded this message.

- CSCeg16993

  Symptom: Secure Desktop did not use some Netscape, Mozilla, or Firefox settings.

- CSCeg22298

  Symptom: Secure Desktop would not preserve the position of the Recycle Bin shortcut between sessions.

  Conditions: Secure Desktop configured with Vault Reuse enabled.

- CSCeh03155

  Symptom: Keystroke Logger displayed a dialog box that was not resizable.

- CSCeh13403

  Symptoms: Key stroke logger detection would hang.

  Condition: When deleting ActMon logger on XP SP1.

- CSCeh26663

  Symptom: CSD did not delete some cached files.

  Conditions: When closing a browser, a popup window opened.

- CSCeh31095

  Symptom: CSD prompted the user connecting with Netscape, Mozilla, or Firefox to choose a profile.

  Condition: This occurred when the local PC clock was adjusted outside of the certificate's valid period.

- CSCeh35107

  Symptom: Cisco SSL VPN Client could not be installed within Secure Desktop using ActiveX.

  Condition: Java was not enabled and the system was running a non-NTFS file system.

- CSCeh40405

  Symptom: Command line ftp left files on the guest desktop.

  Condition: This occurred when the user used command line ftp to "get" files.

- CSCeh44497

  Symptom: A file downloaded using the command line ftp did not appear in the current directory.

  Condition: The user did not use the lcd command (or full path) to explicitly tell ftp where to store the file.

- CSCeh72313

  Symptom: A security module did not recognize Mozilla browser on the Secure Desktop.

  Condition: The security module was installed on a per-profile basis, and users used a brand new Mozilla profile in the Secure Desktop.

- CSCeh72572

  Symptoms: The installation of SSL VPN Client did not succeed. The user was prompted on whether to install the client.

  Condition: Within the Secure Desktop (on some machines only).

- CSCei32208

  Symptom: “The requested resource is in use” error message appeared when the user tried to switch to Secure Desktop.

  Condition: When the local machine had a Panicware popup blocker installed.

- CSCei34985

  Symptom: SVC V1.0.1.116 was unable to execute within the SD space when CSD V3.0.2.275 ran on Release 4.7.1 of the VPN 3000 Concentrator.

  Condition: When configured to use SVC within the SD space, CSD prompted the user as follows:

  ```
  Secure Desktop suspect that a software installation will occur which is not
  recommended.
  Do you want to proceed (unrecommended)
  Selecting Yes at this point fails to allow the SVC to install
  ```

- CSCei44217

  Symptoms: Failure to switch to secure desktop. A message appeared and then disappeared.

  Condition: The vault was not created properly. The “!” directory was not created within the Secure Desktop directory. This was likely because the storage service wasn't started in time.

- CSCei63284

  Symptom: Proxy settings were not pushed to IE when running over SSL VPN Client inside Secure Desktop.

  Conditions: CSD: 3.1.0.9, Client: XP SP2 IE 6.0

- CSCsb44829

  Symptom: Upon uninstallation of CSD from the client PC, the Internet Explorer Favorites failed to restore to the previous list.

- CSCsb56610

  Symptom: Popup blocker settings not carried over to secure desktop

  Condition: When Mozilla like browsers were used

- CSCsb71127

  Symptoms: CSD would not start.

  Condition: When CSD did not properly uninstalled during the upgrade.

- CSCsb82907

  Symptom: Some Explorer windows did not close when the cache cleaner exited.

  Conditions: Java scripts were running that prevented the Explorer windows from closing.

- CSCsb90101

  Symptom: The installation of Secure Desktop on Japanese Windows XP would hang if a certificate was not installed. Specifically, after one clicked “Yes” in response to a Security Alert dialog box to confirm installation without a certificate, Windows would hang after displaying the message, “Please wait while the configuration is checked...”

Conditions:

- VPN 3005 4.7.2A
- Secure Desktop 3.0.2.278
- Windows XP without SP, with SP1, or with SP2 (all Japanese versions)

- CSCsb93871

  Symptom: SSL VPN Client failed to install from within Secure Desktop.

  Conditions: TEMP or TMP environment variables set to non-default values.

- CSCsc41851

  Symptom: Corrupted hosts file.

  Conditions: Opening and closing the Applet window twice while using Application Access within a Secure Desktop.