Release Notes for Cisco Secure Desktop 3.6

Last Updated: May 8, 2013

This document contains release information for Cisco Secure Desktop version 3.6.x. Read the following sections carefully prior to installing, upgrading, and configuring Cisco Secure Desktop.

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

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

Introduction

Cisco Secure Desktop (CSD) is a multifunctional component of the Cisco SSL VPN solution. The main features of CSD include:

- *HostScan* checks for certain attributes on a remote endpoint device attempting to establish a Cisco AnyConnect client or browser-based (clientless) session. These attributes can signify whether the computer is corporate-owned. These attributes include registry entries, process names, and filenames. You can also use HostScan to configure a check for antivirus and antispyware applications, associated definitions updates, and firewalls. CSD supports hundreds of versions of these applications. HostScan reports results to the ASA, which integrates them with the dynamic access policies (DAPs).
- *Secure Desktop (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 sanitization 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.

  If you want to run Secure Desktop (the “Vault”) on Windows XP over an AnyConnect connection, you must configure CSD to identify Windows Vista and Windows 7 operating systems in the prelogin policy and then run Cache Cleaner for those operating systems instead of Secure Desktop.

  Note We do not support running AnyConnect from within the Secure Desktop on Windows Vista or Windows 7.

- *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 is only relevant to users making clientless SSL VPN connections. If your users are creating a VPN connection using the AnyConnect Secure Mobility Client, they will not need Cache Cleaner.

- *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 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 HostScan.

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 and AnyConnect using CSD, 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.

Deprecation of Features: Secure Desktop (Vault), Cache Cleaner, Keystroke Logger Detection, and Host Emulation Detection

Cisco stopped developing the Secure Desktop (Vault), Cache Cleaner, Keystroke Logger Detection (KSL), and Host Emulation Detection features on November 20, 2012.

Deprecated features, the screens used to configure these features in the Adaptive Security Device Manager (ASDM), and the commands used to configure these features in the Adaptive Security Appliance (ASA) command line interface will not be removed from the packages in which they are delivered until the end of engineering support to address severity 1 and severity 2 defects.

After the features have been deprecated, they will continue to provide the functionality for which they were built but will eventually be incompatible with future releases of the ASA, ASDM, AnyConnect, or the operating system on which the endpoint runs.

For more information, see the deprecation field notice "Secure Desktop (Vault), Cache Cleaner, Keystroke Logger Detection, and Host Emulation Detection Features Are Deprecated."

Downloading the Latest Version of CSD

To download the latest version of CSD you must be a registered user of Cisco.com.

Step 1 Follow this link to the CSD Product/Technology Support page:

http://www.cisco.com/en/US/products/ps6742/tsd_products_support_series_home.html

Step 2 Click **Download Software.**

Step 3 Log on to Cisco.com if you are not already.

Step 4 Expand the **All Releases > 3** directory and click the link for CSD **3.6.6249.**

Step 5 There are different CSD packages for Windows, Mac OS X, and Linux. Download CSD Packages using one of these methods:

- To download a single package, find the package you want to download and click **Download**.

- To download multiple packages, click **Add to cart** in the package row and then click **Download Cart** at the top of the Download Software page.

Step 6 Read and accept the **End User License Agreement**.

Step 7 Select a local directory in which to save the downloads and click **Save**.

Upgrading from CSD 3.5.x to CSD 3.6.x

Before upgrading from CSD 3.5.x to CSD 3.6.x, read Before Upgrading or Downgrading Between CSD 3.5.x and 3.6.x, page 15.

Important AnyConnect, CSD, and HostScan Interoperability Information

AnyConnect 3.0.10055 and AnyConnect 3.1.03104 are compatible with HostScan 3.0.08057 or later versions and CSD 3.6.6020 or later versions.

⚠ **Caution** AnyConnect will not establish a VPN connection when used with an incompatible version of HostScan or CSD.

⚠ **Caution** If you can't upgrade AnyConnect and HostScan or AnyConnect and CSD at the same time, upgrade HostScan or CSD fist, then upgrade AnyConnect.

Table 1 AnyConnect and Cisco Secure Desktop Compatibility

AnyConnect Client Version	Cisco Secure Desktop Version	Are these versions compatible?
3.0.08057 or later	3.6.6020 or later	yes
3.0.08057 or later	3.6.5005 or earlier	no
2.5.6005 or later	3.6.6020 or later	yes
2.5.6005 or later	3.6.5005 or earlier	no
2.5.3055 or earlier	Any version of CSD	no

Table 2 AnyConnect and HostScan Compatibility

AnyConnect Client Version	HostScan Version	Are these versions compatible?
3.0.08057 or later	3.0.08057 or later	yes
3.0.07059 or earlier	3.0.08057 or later	yes
2.5.6005 or later	3.0.08057 or later	yes

Table 2 AnyConnect and HostScan Compatibility

AnyConnect Client Version	HostScan Version	Are these versions compatible?
2.5.6005 or later	3.0.07059 or earlier	no
2.5.3005 and earlier	Any version of HostScan	no

Changes in CSD 3.6.6249

CSD 3.6.6249 is a maintenance release that resolves the defects described in Caveats Resolved by CSD Release 3.6.6249 and incorporates HostScan Engine Update, 3.1.03104.

Changes in CSD 3.6.6234

CSD 3.6.6234 is a maintenance release that resolves the defects described in Caveats Resolved by CSD Release 3.6.6234, page 25.

Changes in CSD 3.6.6228

CSD 3.6.6228 is a maintenance release that resolves the defects described in Caveats Resolved by CSD Release 3.6.6234 and incorporates HostScan Engine Update, 3.1.02016.

Some Features in CSD 3.6.6228 are Deprecated

Secure Desktop (Vault), Cache Cleaner, Keystroke Logger Detection, and Host Emulation Detection features were deprecated on November 20, 2012. This release and subsequent releases of CSD are subject to the deprecation notice described in Deprecation of Features: Secure Desktop (Vault), Cache Cleaner, Keystroke Logger Detection, and Host Emulation Detection, page 3.

Changes in CSD 3.6.6215

CSD 3.6.6215 is a maintenance release that resolves the defects described in Caveats Resolved by CSD Release 3.6.6215 and incorporates HostScan Engine Update 3.1.01065.

Some Features in CSD 3.6.6215 are Deprecated

Secure Desktop (Vault), Cache Cleaner, Keystroke Logger Detection, and Host Emulation Detection features were deprecated on November 20, 2012. This release and subsequent releases of CSD are subject to the deprecation notice described in Deprecation of Features: Secure Desktop (Vault), Cache Cleaner, Keystroke Logger Detection, and Host Emulation Detection, page 3.

Changes in CSD 3.6.6210

CSD 3.6.6210 is a maintenance release that resolves the defects described in Caveats Resolved by CSD Release 3.6.6210 and incorporates HostScan Engine Update 3.0.10055. This release does not introduce any new features.

Troubleshooting HostScan and CSD Support for Windows 8

Users on Windows 8 and Windows XP fail to connect to an ASA after an upgrade to CSD 3.6.6104 or HostScan 3.0.08066.

Symptom:

Users on Windows 8 and Windows XP fail to connect to an ASA after an upgrade to CSD 3.6.6104 or HostScan 3.0.08066. After users fail to connect they receive one of these messages:

“Posture assessment failed: Hostscan Initialize error..”

“HostScan Processing Failed”

Conditions:

Client running Windows 8 or Windows XP.

Workaround:

Upgrade the CSD on the ASA to CSD 3.6.6210, or upgrade the HostScan image on the ASA to HostScan 3.0.10057, or HostScan 3.1.01065.

Changes in CSD 3.6.6203

Support for Mac OS X v10.8

CSD 3.6.6203 is the first CSD release to support supports Mac OS X v10.8. This is the complete list of supported Mac OS X operating systems:

- Mac OS X v10.8 (x86 32-bit and x64 64-bit)
- Mac OS X v10.7 (x86 32-bit and x64 64-bit)
- Mac OS X v10.6 (x86 32-bit and x64 64-bit)
- Mac OS X v10.5 (x86 32-bit)

Updated HostScan Engine

An updated HostScan engine, **hostscan_3.0.08066-k9.pkg,** has been incorporated in CSD 3.6.6203.

Changes in CSD 3.6.6104

CSD 3.6.6104 is a maintenance release that incorporates the HostScan Engine Update 3.0.08062. This release does not introduce any new features.

Changes in CSD 3.6.6020

CSD 3.6.6020 specifies new compatibility requirements between AnyConnect, HostScan, and CSD as described in Important AnyConnect, CSD, and HostScan Interoperability Information on page page 4 and resolves the list of caveats in Table 5.

Changes in CSD 3.6.5005

CSD 3.6.5005 is a maintenance release that incorporates HostScan Engine Update, 3.0.7042.

Changes in CSD 3.6.4021

CSD 3.6.4021 is a maintenance release that incorporates the HostScan Engine Update, 3.0.5077. This release does not introduce any new features.

Changes in CSD 3.6.3002

CSD 3.6.3002 is a maintenance release that incorporates the HostScan Engine Update, 3.0.5009. This release does not introduce any new features.

Changes in CSD 3.6.2002

CSD 3.6.1001 is a maintenance release. It incorporates the HostScan Engine Update,3.0.5009. This release does not introduce any new features.

Changes in CSD 3.6.1001

CSD 3.6.1001 is a maintenance release. It incorporates the HostScan Engine Update, 3.0.4216. This release does not introduce any new features.

Changes in CSD 3.6.185

CSD 3.6.185 is a maintenance release that resolves the caveats in Table 6 and incorporates the HostScan Engine Update, 3.0.4016. This release does not introduce any new features.

New Features Introduced in CSD 3.6.181

- Independent HostScan Upgrades, page 8
- Keystroke Logger Detection and Host Emulation Detection Delivered with HostScan Package, page 9
- HostScan Keystroke Logger Detection and Host Emulation Detection User Interface, page 9
- Pre-login Keystroke Logger Detection Available in HostScan Package, page 9
- Secure Desktop (Vault) Support for Windows 7, page 9
- HostScan Support for Antivirus, Antispyware, and Personal Firewall Software, page 10

Independent HostScan Upgrades

Starting with CSD 3.6, the HostScan package becomes a shared component of CSD and the AnyConnect Secure Mobility Client. Previously, the HostScan package was one of several components available only by installing CSD.

The purpose of providing a HostScan package separate from CSD is to allow you to update HostScan support charts more frequently than it was possible when they were delivered solely as part of CSD. The HostScan support charts contain the product name and version information of the antivirus, antispyware, and firewall applications you use in your prelogin policies. We deliver the HostScan application and the HostScan support charts, as well as other components, in the HostScan package.

The HostScan package can now be delivered in one of these ways: as a standalone package, with CSD, with the AnyConnect Posture Module, or with the full AnyConnect client image.

In addition to identifying operating system, antivirus, antispyware, and firewall software installed on the endpoint, the HostScan package delivers the components to perform a prelogin assessment, identify keystroke loggers, and detect host emulation and virtual machines running on the endpoint. Keystroke logger detection, host emulation and virtual machine detection were also features of CSD that are now included in the HostScan package.

Still, the HostScan package is not a replacement for CSD. Customers that want cache cleaning or Secure Desktop (Vault) need to install and enable CSD in addition to the HostScan package. See http://www.cisco.com/en/US/products/ps6742/products_installation_and_configuration_guides_list.html to learn about the Secure Desktop (Vault) feature in the CSD Configuration Guides.

You can install, uninstall, enable, and disable a HostScan package using the ASA's Adaptive Security Device Manager (ASDM) or its command line interface. You can configure prelogin policies using the Secure Desktop Manager tool on the ASDM.

Which HostScan Image Gets Enabled When There is More than One Loaded on the ASA?

The HostScan image is delivered with the HostScan package. It can be deployed to the endpoint from the standalone HostScan package, the full AnyConnect Secure Mobility Client package, and Cisco Secure Desktop. Depending on what licenses you have installed on your ASA, you may have all of these packages loaded on your ASA. In that case, the ASA enables the image that you specified as the HostScan image first and if you haven't specified one, the ASA enables the HostScan functionality from Cisco Secure Desktop.

If you uninstall the HostScan package, the ASA cannot enable its HostScan image.

These scenarios describe which HostScan package the ASA distributes when it has more than one loaded.

- If you have installed a standalone HostScan package on the ASA and have designated it as the HostScan image, and you enable CSD/hostscan, ASA distributes the standalone HostScan package.
- If you have installed a standalone HostScan package on the ASA, and have designated it as the HostScan image, and you have installed a CSD image on the ASA, and you enable CSD/hostscan, ASA distributes the standalone HostScan image.
- If you have installed an AnyConnect Secure Mobility Client package on the ASA and have designated it as the HostScan image, the ASA will distribute the HostScan image from that package.
- If you install an AnyConnect Secure Mobility Client package file on the ASA but do not specify it as the HostScan image, the ASA will not distribute the HostScan package associated with that AnyConnect package. The ASA will distribute an installed HostScan package or CSD package, provided CSD is enabled.

Keystroke Logger Detection and Host Emulation Detection Delivered with HostScan Package

In order to help customers transition to the AnyConnect Secure Mobility Client, keystroke logger detection (KSL) and host emulation detection are now delivered with the standalone HostScan package.

KSL and host emulation detection functions delivered with the standalone HostScan package are identical to those delivered with CSD 3.5 but they also provide support for additional operating systems. HostScan host emulation detection provides support for all windows desktop operating systems including x64 (64-bit) VMWare, VirtualBox, and Virtual PC. Support for these additional operating systems is not available in the host emulation detection functionality delivered with CSD 3.6 Secure Desktop (Vault) feature.

Both HostScan and Vault are included in CSD 3.6. If CSD 3.6 is installed on the ASA, and Vault is enabled, the KSL and host emulation detection functionality provided by Vault takes precedence over the KSL and host emulation detection functionality provided in the standalone HostScan package.

HostScan Keystroke Logger Detection and Host Emulation Detection User Interface

The user interface provided by HostScan keystroke logger (KSL) and host emulation functions is simpler than that provided by the Cisco Secure Desktop KSL and host emulation detection functions.

There are no longer user notifications indicating the starting of keystroke logger detection. HostScan KSL only notifies users that a keystroke logger has been found when the keystroke logger is not listed among the **List of Safe Modules** specified in the **Keystroke Logger & Safety Checks** panel in ASDM.

There is only one translation template (pot file) for both CSD and HostScan and there is only one translated file (po files), per language, for both CSD and HostScan.

Pre-login Keystroke Logger Detection Available in HostScan Package

The keystroke logger detection feature is now available with the HostScan package. Like it does when deployed with Secure Desktop (Vault), KSL can detect the presence of keystroke loggers before the user logs in. You do not need to enable Secure Desktop (Vault) in order to enable the keystroke logger detection delivered with the HostScan package.

Secure Desktop (Vault) Support for Windows 7

The Vault included in CSD 3.6 now provides support for x86 (32-bit) Windows 7. Other than support for this additional operating system, there are no new Vault features in CSD 3.6.

Note If you want to run Secure Desktop (the “Vault”) on Windows XP over an AnyConnect connection, you must configure CSD to identify Windows Vista and Windows 7 operating systems in the prelogin policy and then run Cache Cleaner for those operating systems instead of Secure Desktop.

We do not support running AnyConnect from within the Secure Desktop on Windows Vista or Windows 7

HostScan Support for Antivirus, Antispyware, and Personal Firewall Software

With an Advanced Endpoint Assessment license, on Windows desktops, Cisco Secure Desktop 3.6 updates the list of antivirus, antispyware, and personal firewall applications it supports. The Cisco Secure Desktop Compatibility site lists the antivirus, antispyware, and firewall applications that HostScan checks for on the endpoint.

System and Environment Requirements

The following sections identify the ASA platform and end-user interoperability that CSD requires or supports.

ASA Requirements

In order to take advantage of all the HostScan engine updates in CSD 3.6, you need to install CSD 3.6 with these versions of ASA and ASDM:

- Cisco ASA 5500 series security appliance with total memory of 512 MB.
- ASA release 8.4(1) or later
- ASDM 6.4(0)104 or later

For all other features, CSD 3.6 works with these minimum versions of ASA and ASDM:

- Cisco ASA 5500 series security appliance with total memory of 512 MB.
- ASA 5500 series security appliance running ASA release 8.0(4) or later
- ASDM 6.1(3) or later

Operating System Requirements

The following section lists the CSD endpoint functions and identifies the endpoint OSs they support.

Note For information on endpoint devices and operating systems that CSD no longer supports, see Administrator Guidelines, page 17.

HostScan

HostScan supports the following operating systems:

Windows

- x86 (32-bit) and x64 (64-bit) Windows 8
- x86 (32-bit) and x64 (64-bit) Windows 7
- x86 (32-bit) and x64 (64-bit) Windows Vista, Vista SP1, Vista SP2
- x64 (64-bit) Windows XP SP2
- x86 (32-bit) Windows XP SP2 and SP3

Note After April 8, 2014, Microsoft will no longer provide new security updates, non-security hotfixes, free or paid assisted support options, or online technical content updates for Windows XP (http://www.microsoft.com/en-us/windows/endofsupport.aspx). On the same date, Cisco will stop providing customer support for AnyConnect releases running on Windows XP, and we will not offer Windows XP as a supported operation system for future AnyConnect releases.

- Windows Mobile versions 6.0, 6.1, 6.1.4, and 6.5 for touch screen devices only (Windows Mobile Professional).

Mac OS X

- 32-bit and 64-bit Mac OS X v10.8 (starting in release 3.6.6203)
- 32-bit and 64-bit Mac OS X v10.7
- 32-bit and 64-bit Mac OS X v10.6
- 32-bit and 64-bit Mac OS X v10.5

Linux

- 32-bit Redhat Enterprise Linux 5
- 32-bit Redhat Enterprise Linux 4
- 32-bit Redhat Enterprise Linux 3
- 32-bit Fedora Core 4 and later
- Ubuntu

Note HostScan is a 32-bit application and does not operate on 64-bit Linux platforms.

Cache Cleaner

Cache Cleaner supports the following operating systems for 32-bit browsers only:

Windows

- x86 (32-bit) and x64 (64-bit) Windows 7
- x86 (32-bit) and x64 (64-bit) Windows Vista, Vista SP1, Vista SP2
- x64 (64-bit) Windows XP SP2
- x86 (32-bit) Windows XP SP2 and SP3

Mac OS X

- 32-bit and 64-bit Mac OS X v10.8 (starting in release 3.6.6203)
- 32-bit and 64-bit Mac OS X v10.7
- 32-bit and 64-bit Mac OS X v10.6
- 32-bit and 64-bit Mac OS X v10.5

Linux

- 32-bit Redhat Enterprise Linux 3
- 32-bit Redhat Enterprise Linux 4
- 32-bit Redhat Enterprise Linux 5

- 32-bit Fedora Core 4 and later
- Ubuntu

  Note Cache Cleaner does not operate on 64-bit Linux platforms.

Note Cache Cleaner does not support the standalone startup of AnyConnect Client from any computer.

Secure Desktop (Vault)

Secure Desktop (Vault) is delivered only with CSD 3.6; the Vault runs on the following operating systems:

- x86 (32-bit) Windows 7
- x86 (32-bit) Windows Vista, SP1, and SP2

  KB935855 must be installed on systems running Windows Vista without SP1 or SP2.
- x86 (32-bit) Windows XP SP2 and SP3

Keystroke Logger Detection and Host Emulation Detection Delivered with CSD 3.6 Package

The KSL and host emulation detection functions included with CSD 3.6 support the following operating systems:

- x86 (32-bit) Windows 7
- x86 (32-bit) Windows Vista, SP1, and SP2

  KB935855 must be installed on systems running Windows Vista without SP1 or SP2.
- x86 (32-bit) Windows XP SP2 and SP3

Keystroke Logger Detection and Host Emulation Detection Delivered with HostScan Package

The KSL and host emulation detection functions included with the standalone HostScan package support the following operating systems:

- x86 (32-bit) Windows 7
- x86 (32-bit) Windows Vista SP2
- x86 (32-bit) Windows XP SP3

HostScan, CSD, and AnyConnect Secure Mobility Client Interoperability

Caution A HostScan package deployed along with AnyConnect Secure Mobility Client version 3.0.x, must have the same or a later version number than the AnyConnect Secure Mobility Client.

- If you have Cisco Secure Desktop (CSD) version 3.5, or earlier, enabled on the ASA and you do not upgrade the HostScan package in accordance with Important AnyConnect, CSD, and HostScan Interoperability Information, page 4 to match or exceed the version of AnyConnect Secure Mobility

Client 3.0.x you are deploying, prelogin assessments will fail and users will not be able to establish a VPN session. This will happen even if the AnyConnect 3.0.x posture module is pre-deployed to the endpoint because the ASA will automatically downgrade the HostScan package on the endpoint to match the HostScan package enabled on the ASA.

- Cisco Secure Desktop versions 3.6 and later are not compatible with AnyConnect version 2.4 and earlier.

Tip See "Chapter 5, Configuring HostScan" in the *AnyConnect Secure Mobility Client Administrator's Guide, Release 3.0* for instructions on installing and enabling the HostScan image.

Browser Interoperability

These are the minimum versions of browsers HostScan, Cache Cleaner, Secure Desktop (Vault), and Web Launch support:

- Internet Explorer 6.0
- Safari 3.2.1
- Firefox 3.0.x

HostScan, Cache Cleaner, Secure Desktop (Vault), and Web Launch also require Java 1.4 or later. You must install CSD 3.6.6020 or later to use Java 1.7. These browsers must also have JavaScript capabilities enabled and the browsers must support XML parsing operations.

HostScan and Cache Cleaner do not support 64-bit versions of Internet Explorer. Please instruct users of x64 (64-bit) Windows OSs to use the 32-bit version of Internet Explorer or Firefox to avoid VPN connection issues. (At this time, Firefox is available only in a 32-bit version.) If you use a 64-bit version of Internet Explorer to try to establish a VPN session with a security appliance configured to install HostScan or Cache Cleaner on the endpoint, a "Platform Detection" message states, "Web-based launch of Cisco Secure Desktop is not supported with 64-bit versions of IE. Please retry with the 32-bit version of IE."

Internet Explorer 8 Settings on Windows 7

CSD has been tested on, and supports, Windows 7 using Internet Explorer 8 running in Browser Mode **Internet Explorer 8** and Document Mode **Internet Explorer 8 Standards (Page Default)**. CSD does not support IE8 running in IE7 modes.

License Types

Cisco Secure Desktop requires an **AnyConnect Premium SSL VPN Edition (single device)** or **AnyConnect Premium SSL VPN Edition shared license (main device and participant device)** license. Some features require the purchase of an Advanced Endpoint Assessment license.

Advanced Endpoint Assessment License

With the purchase of an Advanced Endpoint Assessment license installed on the ASA, you can use these advanced features of CSD:

- **Remediation** - On Windows, Mac OS X, and Linux desktops, Advanced Endpoint Assessment can attempt to initiate remediation of various aspects of antivirus, antispyware and personal firewall protection if that software allows a separate application to initiate remediation.
- **Windows Mobile Device Lua Expressions** - For Windows Mobile Devices, administrators will be able to write Lua expressions in Dynamic Access Policies (DAPs) to perform posture checks on those attributes unique to mobile devices. See Specifying Windows 7 in a Dynamic Access Policy, page 18 for an example of a Lua expression.

HostScan Engine Update, 3.1.03104

Caution See Important AnyConnect, CSD, and HostScan Interoperability Information, page 4 for important Host Scan and AnyConnect compatibility information.

Tip It is a "best practice" to always upgrade to the latest HostScan engine.

The HostScan engine, which is among the components delivered by AnyConnect Secure Mobility Client, identifies endpoint posture attributes of the host. The updated HostScan package, **hostscan_3.1.03104-k9.pkg**, is available for use with CSD 3.6.6020 and later.

The AnyConnect Host Scan Engine 3.1.03104: List of supported Antivirus, Antispyware, and Firewall Applications support chart provides a list of what antivirus, antispyware, and firewall application this version of HostScan detect. The support chart is now available on cisco.com.

Tip The support chart opens most easily using a Firefox browser. If you are using Internet Explorer, download the file to your computer and change the file extension from .zip to .xlsm. You can open the file in Microsoft Excel, Microsoft Excel viewer, or Open Office.

System Requirements

See the "Important AnyConnect, CSD, and HostScan Interoperability Information" section on page 4" for important Host Scan and AnyConnect compatibility information. This HostScan update can be installed on ASA version 8.4 or higher.

Downloading the HostScan Engine Update

HostScan engines 3.1.03104 is available as a separate download on cisco.com. To download HostScan engine 3.1.03104, you must be a registered user of Cisco.com.

Step 1 Click this link to reach the software download area for VPN Client Tools and Utilities-Engine Updates:

http://www.cisco.com/cisco/software/release.html?mdfid=284384091&flowid=33102&softwareid=283929405&release=3.1.03104&relind=AVAILABLE&rellifecycle=&reltype=latest

Step 2 In the product tree, expand **Latest Releases**.

Step 3 In the **Release Engine Update** table, find **hostscan_3.1.03104-k9.pkg** and click **Download.**

Step 4 Enter your cisco.com credentials and click **Login**.

Step 5 Click **Proceed with Download.**

Step 6 Read the End User License Agreement and click **Agree**.

Step 7 Select a download manager option and click the **download** link to proceed with the download.

Step 8 See "Installing, Enabling, and Uninstalling HostScan on the ASA" in the *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators, Release 3.6* or instructions on installing and enabling the HostScan image.

Before Upgrading or Downgrading Between CSD 3.5.x and 3.6.x

Caution Read these two procedures before upgrading and downgrading between CSD 3.5.x and CSD 3.6.x.

- Backing up and Restoring the Data.xml File During Upgrade or Downgrade, page 15
- Reconfigure Prelogin Operating System Checks in the Data.xml File, page 16

Backing up and Restoring the Data.xml File During Upgrade or Downgrade

When upgrading from CSD version 3.5.x or earlier to CSD 3.6.x, or downgrading from CSD 3.6.x to CSD version 3.5.x or earlier, the Adaptive Security Device Manager (ASDM) overwrites the data.xml file with the default CSD settings without notifying the administrator. The data.xml file is the CSD configuration file and must be preserved or all previous configurations will be lost upon upgrade. We maintain a record of this problem in our Bug Toolkit and use the number CSCto11223 to identify it.

This problem affects the following configurations:

- CSD Global Settings
- Prelogin policies
- Keystroke Logger & Safety checks
- Cache cleaner customization
- Secure Desktop (Vault) configurations
- Secure Desktop Customization
- HostScan entries manually configured for registry scan, file scan, and process scan
- Endpoint Assessment licenses

Tip To work around this problem, backup the data.xml file before you upgrade or downgrade.

To backup your data.xml file before you upgrade or downgrade and reinstate it afterwards, follow this procedure:

Step 1 Open ASDM, click the **Tools** menu and select **Backup Configurations**.

Step 2 Click **File Transfer** and select **Between Local PC and Flash**.

Step 3 Expand the directory tree for **disk0:/sdesktop** and transfer the **data.xml file** to your local PC.

Step 4 Close the File Transfer window.

Step 5 Close the File Management window.

Step 6 (Optional) If you are **upgrading** and you have configured a prelogin policy that uses an operating system check, read Reconfigure Prelogin Operating System Checks in the Data.xml File, page 16 and edit the your local copy of the data.xml file as described in steps 4 - 6 of that procedure.

Step 7 (Optional) If you are **downgrading** and you have configured a prelogin policy that uses an operating system check, read Reconfigure Prelogin Operating System Checks in the Data.xml File, page 16 and edit the your local copy of the data.xml file as described in steps 4, 7 and 8 of that procedure.

Step 8 Upgrade or downgrade the CSD image using the procedures in the Installing and Enabling CSD chapter of Cisco Secure Desktop Configuration Guide.

Step 9 Click the **Tools** menu in the ASDM menu bar and select **File Management**.

Step 10 Click **File Transfer** and select **Between Local PC and Flash**.

Step 11 Transfer the **data.xml** file from your local PC to the **disk0:/sdesktop** directory.

Step 12 Click **Save**.

Step 13 Restart **ASDM**.

Step 14 (Optional) If you had the Advanced Endpoint Assessment or the Endpoint Assessment license activated before the upgrade, you will need to re-enable them manually:

a. In ASDM, navigate **Configuration > Remote Access VPN > Secure Desktop Manager > HostScan**.

b. Check either or both the **Advanced Endpoint Assessment** or **Endpoint Assessment** in HostScan Extensions.

c. Click **Apply All**.

d. Click **Save**.

e. Restart **ASDM.**

Reconfigure Prelogin Operating System Checks in the Data.xml File

Upgrading from CSD version 3.5.x or earlier to CSD 3.6.x, or downgrading from CSD 3.6.x to CSD 3.5.x or earlier introduces a labeling mismatch in the data.xml file that results in your prelogin policies being hidden from view in the Prelogin Policy window. We maintain a record of this problem in our Bug Toolkit and use the number CSCtq02168 to identify it.

Tip To work around this problem, edit the data.xml file directly to fix the label.

Follow this procedure to perform this workaround:

Step 1 Open ASDM, click the **Tools** menu and select **File Management**.

Step 2 Click **File Transfer** and select **Between Local PC and Flash**.

Step 3 Expand the directory tree for **disk0:/sdesktop** and transfer the **data.xml** file to your local PC.

Step 4 Open the data.xml file on your local PC in a plain text or XML editor.

Step 5 (Optional) If you are **upgrading your version of CSD**, look for an entry similar to this:

```
<choose type="os_check">
          <when label="Win 2K/XP" test="os_check" arg1="win2k">
```

Step 6 Change this string `"Win 2K/XP"` to this string `"Win 2K/XP/Vista/Win7"` and save your local copy.

Step 7 (Optional) If you are **downgrading your version of CSD**, look for an entry similar to this:

```
<choose type="os_check">
          <when label="Win 2K/XP/Vista/Win7" test="os_check" arg1="win2k">
```

Step 8 Change this string `“Win 2K/XP/Vista/Win7” to this string “Win 2K/XP”` and save your local copy.

Step 9 On the ASDM, click **File Transfer** and select **Between Local PC and Flash**.

Step 10 Transfer the data.xml file from your local PC to the **disk0:/sdesktop** directory.

Step 11 Click **Yes** to overwrite the existing data.xml file.

Step 12 **Close** the File Transfer window.

Step 13 **Close** the File Management window.

Step 14 Click **Save**.

Step 15 Restart **ASDM**.

Step 16 After logging back in to ASDM, select **Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy** and then you will see your prelogin policy.

Administrator Guidelines

Refer to the following sections for information you should know before installing, upgrading, and configuring CSD. These sections supplement the information provided in the *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators, Release 3.6.*

Endpoints and Operating Systems no Longer Supported by CSD

This section lists hardware and software which were previously supported by CSD but are no longer. We do not maintain a list of hardware and software that CSD has never supported.

See System and Environment Requirements, page 10 for a list of hardware and software CSD 3.6 does support.

Endpoint Devices No Longer Supported

Starting with release 3.6.181, CSD **stopped supporting** MAC PowerPCs.

Operating Systems No Longer Supported

Starting with release 3.5.841, CSD **stopped supporting** Windows 2000 and Mac OS X v10.4.

Browsers No Longer Supported

Starting with release 3.5.841, Cache Cleaner **stopped supporting** Internet Explorer 5.0.

Enabling the Taskbar to Display the Yellow Lock Icon when Cache Cleaner is Running

By default, the taskbar no longer displays the yellow lock icon while Cache Cleaner is running. Releases of Cisco Secure Desktop earlier than 3.5 displayed this icon with Cache Cleaner. To display the icon, enable keystroke logger detection, host emulation detection, or both.

⚠ **Caution** Enabling keystroke logger detection, host emulation detection, or both turns on the Cisco Secure Desktop 3.4.2048 behavior of Cache Cleaner. It also replaces the Cisco Secure Desktop 3.5 version of HostScan with that provided in Cisco Secure Desktop 3.4.2048 for both Cache Cleaner and AnyConnect sessions.

CSD Loads Slowly or Appears to Stop

If CSD is taking too long to load, it may be that the SSL client (your browser) cannot access the certificate revocation list (CRL) server. In this case, your browser will attempt to reconnect. Eventually, the connection will time-out. These extra attempts delay CSD from launching.

Ensure that your CRL server is properly configured so that your browser can reach it and access the certificate revocation list. This will help CSD launch more quickly.

Here is an example of when the SSL server and SSL client attempt to reach the certificate revocation list:

During the initial SSL handshake between the ASA and the client, the ASA (the SSL server) sends down a certificate, that has its name on it, to the SSL client (your browser). Your browser then attempts to validate the certificate. For example, it could check that the certificate's name corresponds to the host and domain name the browser is pointing to. After that, the client may also contact the certificate revocation list server to determine if the certificate has been revoked.

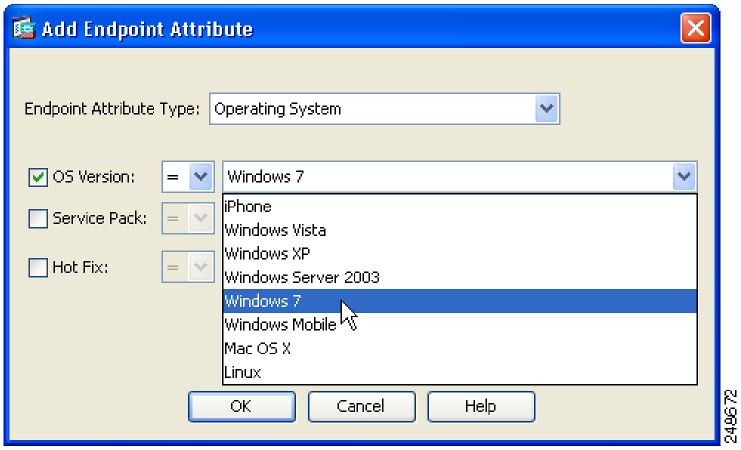
The ASA may also request a certificate from the client, in which case, the client, if it has one, submits its client certificate. The ASA will then attempt to validate the certificate similarly to the way the client did.

Specifying Windows 7 in a Dynamic Access Policy

Specifying Windows 7 as an Endpoint Attribute in the ASDM GUI

You will be able to specify Windows 7 as an endpoint attribute, using the ASDM GUI, if you are using ASDM version 6.2.(5) on an ASA running version 8.2.2 or earlier. See Figure 1 for an example.

Figure 1 Windows 7 Specified as an Endpoint Attribute Using ASDM GUI



Endpoint Attribute Type: Operating System

☑ OS Version: = Windows 7

□ Service Pack: =

□ Hot Fix: =

Specifying Windows 7 as an Operating System Attribute Using a Lua Expression

If you are running a version of ASDM, which is earlier that 6.2(5), on your ASA, you can still use a DAP to check for the Windows 7 OS but you will need to do this using a Lua expression.

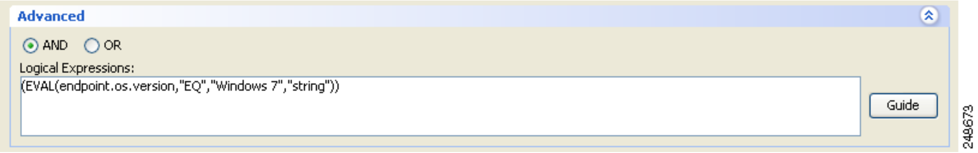
To learn more about Lua expressions in Dynamic Access Policies, see the section on "Configuring Dynamic Access Policies" in Cisco Security Appliance Configuration Guide Using ASDM.

This Lua expression is true if the operating system on the endpoint is Windows 7:

```
(EVAL(endpoint.os.version,"EQ","Windows 7","string"))
```

See Figure 2 for an example of the previous Lua expression displayed in the ASDM interface.

Figure 2 Windows 7 Specified in a Lua Expression



● AND ○ OR

Logical Expressions:

```
(EVAL(endpoint.os.version,"EQ","Windows 7","string"))
```

HostScan and GPS Interaction

HostScan does not wait for the GPS device to activate in order to retrieve location information. It reports the latest GPS location if the GPS device is active and has a GPS fix.

If the GPS hardware is off, hostscan does not switch it on. It uses the cached location information at the timestamp noted. If the mobile device has erased or invalidated latitude and longitude information, it will not be reported to hostscan.

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 ASA and rejected VPN log-ins.

Application Compatibility Layer and User Account Control

Windows Vista uses virtualization to provide application compatibility. CSD turns off user account control (UAC) from within Secure Desktop to avoid collisions with the CSD file system virtualization. Consequently, applications running over Secure Desktop (Vault) do not always share the same resources, such as mapped drives, as non-secure desktop applications.

Downgrade Support

CSD supports upgrades and downgrades between versions 3.6.185 and 3.4.2 on the ASA. Users can establish remote sessions with one or the other, but cannot connect to ASAs running CSD versions earlier than 3.2.1.

With the use of the procedures Before Upgrading or Downgrading Between CSD 3.5.x and 3.6.x, page 15, CSD supports upgrades and downgrades between versions 3.6.181 and 3.4.2 on the ASA. Users can establish remote sessions with one or the other, but cannot connect to ASAs running CSD versions earlier than 3.2.1.

Tip Avoid downgrade issues from 3.6.181 to other versions of CSD by upgrading to CSD 3.6.185.

End User Guidelines

Be sure to communicate these 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 ASA, 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.

ActiveX or Java Settings

CSD 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 3 shows the installation methods and associated user requirements.

Note Starting in this release, CSD no longer supports Microsoft Java VM.

Table 3 CSD Installation Methods and Requirements

Installation Method	Remote User Requirement
ActiveX	Administrator privileges
Sun JavaVM	Any user
Exe	Any user with execution permissions **Note** When User Account Control (UAC) is enabled on Windows Vista, users need to be able to provide the administrator password in order to install CSD.

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

User Interface Privilege Isolation

Because tasks such as HostScan and idle mouse detection require monitoring of other processes, CSD cannot run at a low integrity level. This means that starting CSD sometimes requires privilege elevation. Users experience prompting for privilege elevation and have to consent to use CSD.

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 CSD. Users who have limited privileges must add the URL of the ASA to the trusted zone list before proceeding.

Windows Mail

CSD 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.

Configuring Antivirus Applications for CSD

Antivirus applications can misinterpret the behavior of some of the applications included in Cisco Secure Desktop as malicious. Before installing CSD, configure your antivirus software to “white-list” or make security exceptions for these applications:

- cscan.exe
- ciscod.exe
- cstub.exe

Home Directory Requirement

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

User Guidelines Related to Cache Cleaner

Do Not Change Cache Locations

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

History Not Erased With Multiple Explorer Windows

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.

Cache Cleaner Installation Behavior

Cisco Secure Desktop's Cache Cleaner has a configurable option in the Cache Cleaner panel of Secure Desktop Manager called, **Show success message at the end of successful installation. (Windows only)**. When this option was selected in CSD 3.4 and earlier releases, a message informed users when Cache Cleaner was successfully installed. Cache Cleaner no longer displays this message.

Cache Cleaner Interface Change

In CSD 3.4 and earlier releases, when Cache Cleaner was running, a yellow lock icon displayed in the system tray as a visual reminder to the user. Cache Cleaner no longer displays this icon.

Cache Cleaner Delay

When an SSL VPN s0ession ends, Cache Cleaner may take about a minute to clean the cache and close the browser. Differences in endpoints and the size of the cache can affect the length of the delay.

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 CSD 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 administrators to check the "Enable switching between Secure Desktop and Local Desktop" configuration option.

Installation Guidelines

CSD Installation through a Proxy

To specify CSD 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 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.

New Certificate Required

Cisco Secure Desktop 3.6 is signed with the new certificate **VeriSign Class 3 Public Primary Certification Authority - G5**. Upon installation, Windows XP, Windows Vista, Mac OS X, and Linux users might see a downloader error message, such as the following:

```
An internal certificate chaining error has occurred.
```

This event can occur if one or all of the following are true:

- One has intentionally pruned root certificates.
- Update Root Certificates is disabled.
- The internet is not reachable when an upgrade occurs (e.g. you have your ASA in a private network without Internet access).

CSD installations and upgrades might require endpoint users to install the root CA before upgrading or installing CSD. To do so, enable Update Root Certificates and verify that the Internet is reachable before the CSD installation. By default, Update Root Certificates is enabled. Users can also update the root CA manually, as instructed on the VeriSign website.

For more information, see:

- http://technet.microsoft.com/en-us/library/bb457160.aspx
- http://technet.microsoft.com/en-us/library/cc749331%28WS.10%29.aspx

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.

CSD 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 sections lists the caveats this release resolves and the open caveats.

Resolved CSD Caveats

Caveats Resolved by CSD Release 3.6.6249

Component	Identifier	Headline
hostscan	CSCug65893	IE with Java 7 crashes on HostScan Weblaunch
hostscan	CSCug65985	Posture module not working on 64bit linux
hostscan	CSCug65994	Hostscan on Mac not returning definition date for Trend Micro Sec
hostscan	CSCug66011	POSTURE-ASA: [DetectDLL!GetResult+36] cscan.exe: c0000005 (NULL_POINTER_
hostscan	CSCug66014	Posture - Potential issue with locks

Component	Identifier	Headline
hostscan	CSCug66017	Hostscan: Enable support for Ubuntu 12.04
hostscan	CSCug66019	CSD: "Critical failure. Prelogin failed!." with IE9 ActiveX
hostscan	CSCug66025	POSTURE-ASA: [msvcrt!strcmp+10] cscan.exe: c0000005 (INVALID_POINTER_REA
hostscan	CSCug66028	HostScan fails to install on 32bit Ubuntu with native libcurl
hostscan	CSCug66039	HostScan Weblaunch fails on upgrade when using ActiveX
hostscan	CSCug66046	Cache Cleaner removes Firefox profiles.ini file on Ubuntu
hostscan	CSCug66049	Linux-64: Java applet should verify cstub before launching it.
hostscan	CSCug66056	Linux-64: HostScan should verify executables before linking/launching
hostscan	CSCug66064	Host Scan: cscan process crashes when detecting KSL on WinXP
hostscan	CSCug66070	Cisco Host Scan Heap Overflow Vulnerability
hostscan	CSCug66081	Cisco Host Scan Elevation of Privileges Vulnerability
hostscan	CSCug66088	CSD: Hostscan doesn't report MAC address of WiFi Adapter to ASA
hostscan	CSCug66094	Hostscan CSD Prelogin Error with TLSv1 on OSX and Linux Systems
hostscan	CSCug66095	Hostscan Pre-login assessment fails when computer uses proxy server
hostscan	CSCug66102	Unknown hostscan process running on Win w/MR11,MR2 and hotfix build
hostscan	CSCug66108	Linux64: cstub signature verification fails with weblaunch
hostscan	CSCug66113	Non-admin users may not have access to Posture ActiveX control
hostscan	CSCug66116	Hostscan Proxy Detection takes about 20 seconds on Windows 7
hostscan	CSCug66119	AnyConnect error messages are written to the Win Application log
hostscan	CSCug66398	csdm does not have IPV6 prelogin option
hostscan	CSCug66399	CSDM: Include deprecation notice for Vault, KSL & HE Detection, CC
hostscan	CSCug66401	Enh:CSD should support SEP 12.1 FW
hostscan	CSCug66403	Enable crash dump utility by default

Caveats Resolved by CSD Release 3.6.6234

Component	Identifier	Headline
hostscan	CSCue60895	Signature verification fails on linux with error-certificate has expired

Caveats Resolved by CSD Release 3.6.6228

Component	Identifier	Headline
hostscan	CSCuc55801	HostScan does not detect “lastupdate” of Kaspersky AV 8.x on Mac OS X
hostscan	CSCuc55823	HostScan reports a negative “lastupdate” value for Kaspersky 12.x

Component	Identifier	Headline
hostscan	CSCuc55842	HostScan must renew ASA token every 10 mins until reporting is complete
hostscan	CSCud05624	IE with Java 7 crashes on HostScan Weblaunch
hostscan	CSCud15249	HostScan does not detect Microsoft Forefront Endpoint Protection 2010
hostscan	CSCud15256	HostScan reports Sophos AV Virus Def Last Update incorrectly on MacOSX
hostscan	CSCud50945	CSD malfunction with Vault: Failed to load InspectorExtension.dll

Caveats Resolved by CSD Release 3.6.6215

Component	Identifier	Headline
hostscan	CSCuc03839	Improve the HostScan logging: Label non-warning messages as debug
hostscan	CSCuc04266	HostScan is consuming large amounts of CPU time
hostscan	CSCuc04353	CSD Prelogin failed. Denied access.
hostscan	CSCuc04395	HostScan does not detect Free Avast AV 7.x software on MAC OS
hostscan	CSCuc04406	Hostscan Engine 3.0.08062 support chart incorrectly list 'Eset Software'
hostscan	CSCuc04635	Hostscan reports “elevationrequired” with Eset AV
hostscan	CSCuc04661	HostScan doesn't report “lastupdate” value for Kaspersky 11.x
hostscan	CSCuc55815	CSD/HS not detecting Norton AV 10.2.3
hostscan	CSCuc55831	HostScan does not support Virus Security Zero v12
hostscan	CSCuc55842	HostScan must renew ASA token every 10 mins until reporting is complete
hostscan	CSCuc96846	CSD: Hostscan does not detect Malwarebytes Anti-Malware software
hostscan	CSCud29504	MAC needs to support cert verification
hostscan	CSCud29560	cscan.exe error after applying Firefox update
hostscan	CSCud29794	Re-instate signing for Mac
hostscan	CSCud29969	CSD Critical Failure, Prelogin Falied randomly prevents the web vpn
posture-asa	CSCud46431	The amount of memory used by csan.exe increases continually over time.

Caveats Resolved by CSD Release 3.6.6210

Table 4 Caveats Resolved by CSD Release 3.6.6210

Component	Identifier	Headline
hostscan	CSCuc04387	Posture module within AC 3.0.5080 causes HostScan failure
hostscan	CSCuc04417	Weblaunch for Hostscan/CSD does not work against windows 8

Table 4 Caveats Resolved by CSD Release 3.6.6210

Component	Identifier	Headline
hostscan	CSCuc04469	Support (posture) for MC OSX 10.8
hostscan	CSCuc04647	Hostscan Initialize error causing connect failure
hostscan	CSCuc04677	memory leaks in ciscod under certain Hostscan settings
hostscan	CSCuc04711	Hostscan weblaunch is not successful when using Java 6
hostscan	CSCuc04720	HostScan weblaunch fails from Internet Explorer with Java 7
posture-asa	CSCub19055	Host Scan initialization error causes a failure on Windows 8 and Windows XP

Caveats Resolved by CSD Release 3.6.6020

Table 5 Caveats Resolved by CSD Release 3.6.6020

Component	Identifier	Headline
posture-asa	CSCtx74235	CSD: Downloaders/ActiveX to fix validation of downloaded code
securevault	CSCti97720	Remote Code Execution Vulnerability in Cisco Secure Desktop

Caveats Resolved by CSD Release 3.6.185

Table 6 lists the caveats that have been resolved by CSD Release 3.6.185.

Table 6 Caveats Resolved by 3.6.185

Caveat ID	Headline
CSCsw17514	CSD:deny access if emulation message box has blank button
CSCtd26933	CSD: Hostscan returns protection=”vault” with XP 64,should return “secur
CSCtl17920	CSD only logs the last connection attempt
CSCtn87540	CSD Add support for Avast
CSCtn93301	CSD 3.5 fails to validate Sophos AV 7.x on MacOSX
CSCto11223	Upgrade csd from 3.5.x to 3.6.x sets the data.xml file to defaults
CSCto45087	We need a way to roll over logs like AnyConnect VPN RollingLogger
CSCto65864	Improper return value for the Kaspersky Antivirus
CSCto91503	CSD: PreLogin Device Protection is reported incorrectly
CSCto96682	AnyConnect Hostscan module noisy log warnings
CSCtq00045	Vault login denied when Host Scan incorrectly reports main.exe not running
CSCtq02168	Errors in CSD 3.6 prelogin policy panel if reusing data.xml from CSD 3.5
CSCtq08733	cscan.exe consuming 195MB of memory and climbing
CSCtq18019	CSD weblaunch with ActiveX fails (Java OK) - Fingerprints do not match
CSCtq34383	Privacy protection value not working

Table 6 Caveats Resolved by 3.6.185

Caveat ID	Headline
CSCtq48037	DOC: Need to remove wrong doc on csd Prelogin Cert check for MAC
CSCtq61788	Expired cert with CSD's Java file....
CSCtq68002	CSD: Error 1920 when installing CSD 3.6.181 MSI on French Windows 7
CSCtq81064	DOC: CSD does not support Symantec Endpoint Protection 12.x anti-spyware
CSCtq92552	CSD: HostScan fails to check LastUpdate for Microsoft Forefront AV
CSCto11223	Upgrade csd from 3.5.x to 3.6.x sets the data.xml file to defaults

Caveats Resolved by CSD Release 3.6.181

This table lists the caveats that have been resolved by CSD Release 3.6.181.

Table 7 Caveats resolved by CSD 3.6.181

Caveat ID	Description
CSCsr68962	CSD: KeyStroke Logger should require no initial interaction
CSCsx05118	CSD displays “Inspection has timed out or exited unexpectedly”
CSCtc05747	Prelogin OS list should include Windows 7
CSCtd23098	An instance of IE is not closed by Cache Cleaner on disconnect
CSCte49200	CSD: Add support for Norton AV 2010 and Internet Sec 2010
CSCtf31080	CSD: Host Scan Displays unlisted OID numbers as “O”
CSCtf33588	CSD 3.5 & anyconnect SBL w/ keystroke logger fails with hostscan error
CSCtf34055	CSD: AV not recognized by HS when KSL-MachineCert are enabled
CSCtf36376	CSD: Machine Cert detection fails when all Locations have KSL enabled.
CSCtf39471	CSD 3.5 Explain new Cache Cleaner behavior in docs
CSCtf46292	Heap leak in libcsd.dll causing vpnui.exe to crash
CSCtf78998	CSD: Linux Hostscan generates large number of /tmp/OPSWAT_* files
CSCtf93020	HostScan invokes UAC for Admin Users on Vista in any case
CSCtf94771	CSD secure Vault ignores proxy configured via PAC file
CSCtf98980	CSD: Hostscan fails to return AV info->unable to download required library
CSCtf99181	CSD should fall back to non-predeploy if ciscod can't be contacted
CSCth08882	CSD: Hostscan doesn't update 'lastupdate' for AV after forced AV update
CSCth42819	CSD: Prelogin Check cannot find certificate in Trusted Root CA folder
CSCth43939	CSD 3.5: Add DLLexceptions for Apps operation in Vault with ASA 8.3
CSCth53868	CSD:Vault does not allow smart tunnel access to CWA (VistaSP1+IE8)
CSCth58570	CSD not detecting hotfix
CSCth76255	CSD fails to read and evaluate top level registry keys
CSCti35153	OPSWAT causes memory leak
CSCti62349	UI is crashing in csdlib with CSD/hostscan enabled

Table 7 Caveats resolved by CSD 3.6.181

Caveat ID	Description
CSCtj03005	Remote Code Execution Vulnerability in Cisco Secure Desktop. (Active X)
CSCtj07374	CSD - documentation of endpoint.device.hostname is missing
CSCtj59457	Libcsd.dll Causes GUI Crash
CSCtj61980	Implement logic to automatically restart the ciscod service if it fails
CSCtj62430	CSD fails to download and launch the stub when pre-deployed on Win7
CSCtj69426	Hostscan fails to report the path during process check on win7-32
CSCtj86557	CSD: Hostscan not reporting AV in Vault
CSCtj86833	AV.activescan value returned is “Ok” for disabled SymantecEndpoint
CSCtj99800	Vault not launching on Win 7.
CSCtk36156	CSD Vault/Hostscan is not launching with pre-deployment kit
CSCtk47345	failure while adding rule to firewall in win 7
CSCtl12989	Anyconnect credential page appears outside Vault with AC 2.5
CSCtl42142	CSD ver 3.6.152 has wrong Preinstaller (.msi) Package
CSCtn39379	Block port via firewall not working in Linux
CSCtn59240	Cannot configure certain file versions for pre-login file check
CSCtn71355	Release Notes link for CSD 3.5.2008 points to CSC 3.5.1077
CSCtn99517	FileScan is not working when some applications open target file
CSCto08218	Active-x & java not working_179 build

Open CSD Caveats

The following table lists the severity 1–3 caveats that are open in this release of CSD:

Component	Identifier	Headline
csdm	CSCud30407	IPv6 : no option to configure ipv6 prelogin policy
hostscan	CSCtb47343	CSDM: AEA lists 13 AVG vendors - only 2 are supported
hostscan	CSCuc86278	CSD: "Critical failure. Prelogin failed!." with IE9 ActiveX
hostscan	CSCuc86284	Posture - Potential issue with locks
java	CSCtt40292	Error in saving the modified settings in CSD
posture-asa	CSCti24021	Posture localization PO file needs updated translation
posture-asa	CSCtk05829	Hostscan does not work when using Google Chrome on a MAC
posture-asa	CSCtr39580	JPN CSD: Host Scan Registry MBCS Registry name is not working
posture-asa	CSCtr39606	JPN CSD: Host Scan File MBCS File name is not working
posture-asa	CSCtr39613	JPN CSD: Host Scan MBCS Folder name is not working
posture-asa	CSCtr39630	JPN CSD: Host Scan Process MBCS name is not working

Component	Identifier	Headline
posture-asa	CSCts00066	Hostscan:Posture assessment and connection fails w/IKEv2 to Load Bal ASA
posture-asa	CSCtz67975	CSD: Ability to prevent a user from opening data.xml in a browser
posture-asa	CSCtz73641	UDP ports not detected on Linux and OSX
posture-asa	CSCua68938	HostScan fails to pick the AV defined as a DAP rule
posture-asa	CSCub32322	cstub should validate server certificates for a ssl connection
posture-asa	CSCuc42358	HostScan fails to install on 32bit Ubuntu with native libcurl
posture-asa	CSCuc56437	Cache Cleaner removes Firefox profiles.ini file on Ubuntu
posture-asa	CSCuc92128	Posture pre-deploy msi does not install the ActiveX control
posture-asa	CSCud14153	Cisco Host Scan Elevation of Privileges Vulnerability
posture-asa	CSCud26605	CSD: Hostscan doesn't report MAC address of WiFi Adapter to ASA
posture-asa	CSCud39455	Hostscan Pre-login assessment fails when computer uses proxy server
posture-asa	CSCud47132	HS: Computer Associates etrust AV not detected
posture-asa	CSCud54452	ASDM: upgrading hostscan deletes endpoint config
posture-asa	CSCue44500	Hostscan - warnings and errors are not sent to event viewer through AC
posture-asa	CSCue49663	Signature verification fails on linux with error-certificate has expired
posture-asa	CSCue56046	HostScan fails to evaluate user/client certificates on Ubuntu 12
posture-asa	CSCue57439	CSD/Hostscan does not detect hotfix KB2761226
posture-asa	CSCue70557	CSD/Hostscan detects hotfix even though this hotfix was uninstalled
securevault	CSCtr25566	ALL-LANG CSD: file was shared between Local and Secure Desktop

Related Documentation

- Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators, Release 3.6
- List of Antivirus, Antispyware, and Firewall Applications Supported by HostScan.
- Open Source Used In Cisco Secure Desktop, Release 3.6
- AnyConnect Secure Mobility Client Release Notes
- AnyConnect Secure Mobility Client Administrator Guide
- Cisco ASA 5500 Series Release Notes
- Cisco ASDM Release Notes

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

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.