

Cisco Secure Desktop (CSD) FAQ

Document ID: 107461

Questions

Introduction

What components comprise Cisco Secure Desktop?

Where can I find a compability matrix of OSES, Browsers, ASA versions, SSL VPN components supported by CSD?

Where is the CSD configuration stored?

Does CSD interoperate with the IPsec VPN Client?

Are the CSD PreLogin certificates checks applicable to both machine and user certificates?

If the Secure vault is used, how does interaction occur between it and the real desktop?

For example, can files be moved between the two or is it only into the vault?

Is there a limit to the number of CSD locations that can be defined?

Can files that are created within the CSD vault be saved onto the guest PC?

Can files be saved onto an external media such as a USB fob, a CD, or disk?

Can files be saved on shared network folders?

When a file is created or amended within the Secure Desktop space, can it be saved to a Network Neighborhood if a network connection through SSL VPN or IPsec exists ?

How are the locations matched to the client?

Even if ActiveX and Java are disabled, can I execute the CSD installation through the browser?

Are there restrictions of Sun JVM ?

Does the Cisco Security Agent (CSA) V4.5 inter-operate with CSD and SVC?

How big of a partition on the hard drive does CSD create?

How does CSD decide what applications to support? Is it just all the applications that are available on the normal desktop? Can this be controlled ?

Can the use of `print screen` be prevented in CSD?

Does the Secure Desktop run on DEP (MS KB 875352) enabled PCs and Tablet PCs ?

Is there any way to pre-install CSD on a PC?

What browsers support Cache Cleaner on Windows platforms and MAC OS?

What happens if a remote client is connected to secure desktop over WebVPN and they terminate the session like unplugging the network cable from the computer. Will the secure desktop still remove traces of the file? I believe a similar scenario would be if the machine is powered off in the middle of the session, is the file accessible then?

Are the new versions of CSD 3.2.x , which shipped with ASA version 8.0.2.x, backwards-compatible with ASA version 7.1.x/7.2.x?

Does CSD v3.2 support Secure Desktop/Vault and Cache Cleaner?

Can CSD 3.2.x Advanced Endpoint Assessment remediate multiple versions of AV, AS, FW?

Is CSD 3.2 able to control control CD-R media?

How susceptible is the CSD secure vault to threats from the host operating system while running CSD? Is it a case of the vault in effect that keeps all bad things at bay, or is the use of the normal desktop on the host just as vulnerable? The posture check is relied upon in order to mitigate against some of these issues.

How do I position CCA NAC appliance versus CSD + Adv Endpoint Assessment in ASA 8.0? It seems like the posture check functionality is similar. Does CCA offer any significant advantages over 8.0 for VPN users?

Can CSD be enabled on a per-group-policy, post authentication?

How is CSD uninstalled from the client PC?
How do I find a list of what products are supported by Cisco Secure Desktop (CSD) Host Scan?
How do I find the subset of products that are supported with Advanced Endpoint Assessment?
What CSD operations require Administrative privileges?
Are any of the CSD features such as Host Scan, Cache Cleaner, and Vault supported on 64-bit platforms?
Can CSD PreLogin Checks (Location policy) be configured if CSD is not enabled?
What are the supported CSD Prelogin checks?
Can you delete all the PreLogin Policies in one shot instead of individually?
Are the CSD Prelogin certificate checks PKI-validated or does it only check for the presence of the certificates on the endpoint host?
Registry and Certificate Prelogin checks apply to which OSes?
Can CSD settings be pushed from Radius/LDAP?
Can CSD detect TCP listening ports on the endpoint PC?
What are the the CSD and DAP endpoint attributes that can be enforced on an SSL VPN policy?
What is this CSD token seen within the DAP debugs (DAP_TRACE: DAP_add_CSD: csd_token = [71F16BEE51C8B569360F9BF0]) ?
What CSD capability is available with AnyConnect in Start Before Login (SBL) mode?
What is the recommended way to update the CSD file without the deletion of the PreLogin policy (Locations) configuration?
I face issues when I access Citrix ICA client using Java versions 1.6.10,1.6.11,and 1.6.12. Why does the connection fail as soon as the client connects to the Citrix remote desktop while using CSD?
NetPro Discussion Forums – Featured Conversations
Related Information

Introduction

This document provides information on the most frequently asked questions (FAQ) related to the Cisco Secure Desktop (CSD).

Cisco Secure Desktop seeks to minimize the risks posed by the use of remote devices in order to establish a Cisco clientless SSL VPN or AnyConnect Client session.

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Q. What components comprise Cisco Secure Desktop?

A. CSD comprises several components:

- ◆ PreLogin Assessment/Policies
- ◆ Host Scan (Basic and Advanced with remediation capabilities)
- ◆ Cache Cleaner
- ◆ Secure Vault
- ◆ Keystroke Logger
- ◆ Host emulation detection

Refer to CSD Configuration Guide for more information.

Q. Where can I find a compability matrix of OSeS, Browsers, ASA versions, SSL VPN components supported by CSD?

A. Refer to Cisco ASA 5500 Series VPN Compatibility Reference for more information.

Q. Where is the CSD configuration stored?

A. The CSD configuration is stored on the flash under sdesktop/data.xml file.

Q. Does CSD interoperate with the IPsec VPN Client?

A. No. CSD only interoperates with Clientless SSL VPN and Anyconnect 2.x.

Q. Are the CSD PreLogin certificates checks applicable to both machine and user certificates?

A. Yes. PreLogin checks for Machine Certificates was implemented in CSD 3.2.1 (CSCsj35249).

Q. If the Secure vault is used, how does interaction occur between it and the real desktop? For example, can files be moved between the two or is it only into the vault?

A. The file system is virtualized. Inside the vault you can see essential local files such as program files and windows, but files within the vault cannot be moved outside.

Q. Is there a limit to the number of CSD locations that can be defined?

A. No.

Q. Can files that are created within the CSD vault be saved onto the guest PC?

A. No.

Note: One exception to this is the use of certain email applications such as Outlook, Outlook Express, Eudora and Lotus Notes that operate as they do on the client PC. These applications are not generally found in the public domain.

Q. Can files be saved onto an external media such as a USB fob, a CD, or disk?

A. Yes, but the data is encrypted and is removed once the vault is uninstalled and is not visible if the key is removed.

Q. Can files be saved on shared network folders?

A. Yes. If the shared network folders exist as part of the Network Neighborhood on the client PC, then they also appear on the Secure Desktop Network Neighborhood.

Q. When a file is created or amended within the Secure Desktop space, can it be saved to a Network Neighborhood if a network connection through SSL VPN or IPsec exists ?

A. Yes.

Q. How are the locations matched to the client?

A. As outlined in the documentation, locations are identified when the criteria of the different locations are checked with the use of the priority of top to bottom as displayed in the windows location pane. The first location that meets the criteria is used as the connection location. Cisco suggests the use of a location with no criteria as the last location so that it becomes the default if no other locations with criteria are matched.

Q. Even if ActiveX and Java are disabled, can I execute the CSD installation through the browser?

A. Yes, You can still install CSD even if both Active X and Java are not detected on the client PC.

Q. Are there restrictions of Sun JVM ?

A. No, there are not any restrictions for Cisco Secure Desktop or the SSL VPN Client.

Q. Does the Cisco Security Agent (CSA) V4.5 inter-operate with CSD and SVC?

A. Yes. CSA V4.5 now supports and is fully compatible with both CSD and SVC.

Q. How big of a partition on the hard drive does CSD create?

A. When a Secure Desktop environment is created, an encrypted file space (the vault) is generated , which starts as a small file space and grows to a max of 2 GB, which depends on what applications are loaded from their default locations whilst operating within the vault.

Q. How does CSD decide what applications to support? Is it just all the applications that are available on the normal desktop? Can this be controlled ?

A. This is detailed in the release notes and cannot be controlled. It does not allow applications to be installed whilst in the SD Vault/space, but uses the default applications under Program Files that are already installed on the client PC. 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.

Q. Can the use of print screen be prevented in CSD?

A. This is a configuration option within the Secure desktop management configuration. The copy/paste buffer (clipboard) is cleared once you switch back to the client PC, if enabled in the configuration.

Restrict Printing on Secure Desktop Check to prevent the user from printing while the Secure Desktop space is used. For maximum security of sensitive data, check this option.

Q. Does the Secure Desktop run on DEP (MS KB 875352) enabled PCs and Tablet PCs ?

A. This was not supported in earlier versions (earlier than 3.1.0.29) and detailed in CSCsc12461. The workaround at that time was to disable DEP in the BIOS as mentioned in the DDTS. As of version 3.1.0.29, this has now been resolved.

Q. Is there any way to pre-install CSD on a PC?

A. No, because the CSD component that you want to install depends on result of prelogin policy.

Q. What browsers support Cache Cleaner on Windows platforms and MAC OS?

A. CSD v3.3 does support CSD-Vault (sandbox) feature on 32-bit Vista platforms.

See VPN_Compatibility for more details.

Q. What happens if a remote client is connected to secure desktop over WebVPN and they terminate the session like unplugging the network cable from the computer. Will the secure desktop still remove traces of the file? I believe a similar scenario would be if the machine is powered off in the middle of the session, is the file accessible then?

A. The data remains encrypted/inaccessible and then is erased the next time Cisco Secure Desktop is launched. If you use a cache cleaner, the data is wiped out the next time you logon.

Q. Are the new versions of CSD 3.2.x , which shipped with ASA version 8.0.2.x, backwards-compatible with ASA version 7.1.x/7.2.x?

A. The new version of Cisco Secure Desktop 3.2.x is not backwards compatible with older ASA 7.1.x/7.2.x.

Q. Does CSD v3.2 support Secure Desktop/Vault and Cache Cleaner?

A. CSD 3.2 for ASA 8.0.2.x supports ONLY Cache Cleaner on Vista , 32-bit machines. Secure Vault support on Vista is for future consideration (CSD v3.3) .

Update CSD v3.3 does support CSD-Vault (sandbox) feature on 32-bit Vista platforms.

Q. Can CSD 3.2.x Advanced Endpoint Assessment remediate multiple versions of AV, AS, FW?

A. CSD 3.2 Advanced Endpoint Assessment does not allow the checking of multiple versions of an Antivirus, Personal Firewall or AntiSpyware program. CSD 3.2.1 does have the ability to check for multiple Antivirus, Personal Firewall or AntiSpyware programs with the use of the Dynamic Access Policy with the Endpoint Assessment feature.

Note: CSD 3.2.1, ASDM6.0.3/ASA 8.0.3, which FCSed in November 2007 , includes this capability (CSCsk71239) .

Q. Is CSD 3.2 able to control control CD–R media?

A. The current design does not allow for CSD to control CD drives.

Q. How susceptible is the CSD secure vault to threats from the host operating system while running CSD? Is it a case of the vault in effect that keeps all bad things at bay, or is the use of the normal desktop on the host just as vulnerable? The posture check is relied upon in order to mitigate against some of these issues.

A. CSD concept is to not leave anything behind. The CSD vault is for storage of session data such as cached web pages created during the vpn session. The vault is encrypted for protection. It is not supposed to be a type of virus protection device.

Q. How do I position CCA NAC appliance versus CSD + Adv Endpoint Assessment in ASA 8.0? It seems like the posture check functionality is similar. Does CCA offer any significant advantages over 8.0 for VPN users?

A. CSD provides posture check and limited remediation, while CCA can actually support a more sophisticated and complete remediation process. This is key if the VPN user is a full–time telecommuter, for instance, that is not that tech savvy and requires instruction on the next steps that are necessary without bogging down the internal support department. That can also lead to a reduction in support costs and increased productivity if you want to extrapolate the possibilities.

Q. Can CSD be enabled on a per–group–policy, post authentication?

A. Not currently as of v8.0.3. CSD is globally enabled on the ASA for all group–policies before Authentication/Authorization takes place. The main reason why Cisco Secure Desktop was loaded pre–login is to offer protection over the login process itself, especially when static credentials are in use.

Q. How is CSD uninstalled from the client PC?

A. When Secure Desktop is installed, it can be uninstalled manually or automatically when a session is closed. An option is available in the **CSD Manager > Secure Desktop General** in order to do this automatically.

Q. How do I find a list of what products are supported by Cisco Secure Desktop (CSD) Host Scan?

A. The latest information is always visible inside of ASDM. You can also extract secinsp_<VERSION>_av.xml, secinsp_<VERSION>_as.xml and secinsp_<VERSION>_fw.xml from the current CSD package (as a ZIP) and search for Product_ID attribute.

These checks are updated with every release and as such, it is impossible for the documentation to keep up with the list.

Q. How do I find the subset of products that are supported with Advanced Endpoint Assessment?

A. Search for Allow_port and Block_port attribute value for each product.

```
v= implemented
x= not implemented
```

Q. What CSD operations require Administrative privileges?

A. The CSD installation with Java already installed and most basic host scanning operations do not require administrative privileges. Operations such as enabling a FW process, do not work without administrative privilege, of course. Do not expect it to be scanned for files that it does not have privilege for which to scan; for example, if you are limited user, you cannot detect /users/administrator/mydocuments/file.txt. Key stroke logger requires administrative privileges.

Q. Are any of the CSD features such as Host Scan, Cache Cleaner, and Vault supported on 64-bit platforms?

A. No. CSD only supports 32-bit platforms.

Q. Can CSD PreLogin Checks (Location policy) be configured if CSD is not enabled?

A. No. Prelogin policy checks rely on CSD being enabled.

Q. What are the supported CSD Prelogin checks?

A. The checks are IP Address (Source IP range), Certificate, Registry, File and OS.

Q. Can you delete all the PreLogin Policies in one shot instead of individually?

A. In ASDM there is currently no button/knob to delete *all* Prelogin policies. You can only delete them individually. There is an enhancement request CSCsq91629 in order to be able to do this.

On the ASA CLI, you can complete these steps in order to clear all Prelogin policies and set CSD configuration to default.

1. #delete sdesktop/data.xml
2. Then you must Exit and restart ASDM for the change to take affect.

Q. Are the CSD Prelogin certificate checks PKI–validated or does it only check for the *presence* of the certificates on the endpoint host?

A. The certificate checks verifies only that the certificate is present on the endpoint host, and not whether the certificate is PKI–validated.

Q. Registry and Certificate Prelogin checks apply to which OSES?

A. Only Windows.

Q. Can CSD settings be pushed from Radius/LDAP?

A. No. CSD specific policies cannot be set through Radius/LDAP .

Q. Can CSD detect TCP listening ports on the endpoint PC?

A. CSD 3.2.1 now supports Port Scanning on the endpoint PC (Windows, MAC, Linux) and was implemented in CSCsj44999. Dynamic Access Policies (DAP) can enforce the endpoint.device.port attribute in policy.

Q. What are the the CSD and DAP endpoint attributes that can be enforced on an SSL VPN policy?

A. Here is a a list of DAP Endpoint Selection attribute categories as of 8.0.3.x:

- ◆ Anti–Spyware
- ◆ Anti–Virus
- ◆ Application
- ◆ File
- ◆ NAC
- ◆ Operating System
- ◆ Personal Firewall
- ◆ Policy (Location)
- ◆ Process
- ◆ Registry
- ◆ Device such as Hostname, Mac Address, Port Number, and Privacy Protection

Q. What is this CSD token seen within the DAP debugs (DAP_TRACE: DAP_add_CSD: csd_token = [71F16BEE51C8B569360F9BF0]) ?

A. ASA creates unique random numbers and assigns them to HostScans so it can distinguish one HostScan from another. HostScan happens before the login when no SSL VPN session exists. HostScan does not send CSD token in the scan file. The token is used to attach the scan data to the ASA SSL VPN session.

Q. What CSD capability is available with AnyConnect in Start Before Login (SBL) mode?

A. When Anyconnect is launched in SBL mode, only hostscan is performed by CSD regardless of what prelogin policy dictates, unless there is no location match, in which case CSD launch fails.

Q. What is the recommended way to update the CSD file without the deletion of the PreLogin policy (Locations) configuration?

A. Upgrade a new CSD image, which keeps all settings intact, except upgrades from CSD 3.1.1 to 3.2 or later.

Q. I face issues when I access Citrix ICA client using Java versions 1.6.10, 1.6.11, and 1.6.12. Why does the connection fail as soon as the client connects to the Citrix remote desktop while using CSD?

A. In JRE6 Update 10 and later, Java starts differently from standard practice. Refer to Introducing Java SE 6 update 10 for more information on Java update 10.

The Secure Desktop Vault browser freezes if you open a website that contains a Java applet, and JRE Update 10 or later is installed on the computer. This problem occurs only if you have checked the **Restrict application usage to the web browser only** option present in **Secure Desktop Manager > <policy_name> > Secure Desktop Settings**. The default setting is unchecked. You can do one of these options in order to make Java applets functional on Secure Desktop:

1. Add these lines to the text box under the checked attribute **Restrict application usage to the web browser only**:

```
◇ c:\program\java.exe  
◇ c:\program\jp2launcher.exe
```

2. Uncheck **Restrict application usage to the web browser only** checkbox. This resolves the issue.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- Cisco ASA 5500 Series Security Appliances
- Cisco ASA 5500 Series VPN Compatibility Reference
- Cisco Secure Desktop

- **Configuring Cisco Secure Desktop**
 - **Technical Support & Documentation – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jul 29, 2008

Document ID: 107461
