



Frequently Asked Questions

The Cisco Secure Desktop FAQs are as follows:

What happened to the VPN feature policies?

In Release 3.1.1, Secure Desktop Manager let you configure a VPN feature for each prelogin policy. The dynamic access policy (DAP) feature accessible on ASDM replaced and enhanced that feature.

What are the minimum rights for Secure Session, Cache Cleaner, Host Scan, and KeyStroke Logger Scanning?

Non-privileged, guest user accounts are sufficient to download and install Secure Session and host emulation detection, Cache Cleaner, and Host Scan. Keystroke Logger detection requires administrator privileges.

Must Secure Session install to check for malware?

Either Cisco Secure Desktop or NAC Framework must be configured to load Endpoint Assessment.

If the remote computer passes a prelogin assessment associated with a particular prelogin policy configured on the security appliance, a scan of the antivirus, antispymware, personal firewall, and other optional keylogger, file, registry, and process checks occurs. This scan can be turned on or off by the system administrator. Secure Session or Cache Cleaner installs only if the prelogin assessment associated with a particular prelogin policy passes, and only if the Secure Desktop or Cache Cleaner parameters are enabled for the matched prelogin policy. If both the prelogin assessment for a particular prelogin policy and the Host Scan checks pass, and the prelogin policy has both Secure Desktop and Cache Cleaner disabled (typically for a corporate computer login), only the DAP determines the user experience after authentication.

How does Host Scan work with dynamic access policies?

After you add scans for registry keys, files, and processes to the Basic Host Scan table in the Host Scan pane, choose **Configuration > Network (Client) Access** or **Clientless SSL VPN Access > Dynamic Access Policies > Add** or **Edit**. Choose Registry, File, or Process from the drop-down list next to the Endpoint Type attribute and enter the ID of the registry key, file, or process. Do this once for each entry in the Basic Host Scan table.

After you check Endpoint Assessment or Advanced Endpoint Assessment, choose **Configuration > Network (Client) Access** or **Clientless SSL VPN Access > Dynamic Access Policies > Add** or **Edit**. Choose Antispymware, Antivirus, or Personal Firewall from the drop-down list next to the Endpoint Type attribute and select the application you want to associate with a DAP. Do this once for each protective application you want to require as a condition for assigning a DAP.

What happened to Windows CE?

Previously, Cisco Secure Desktop let you configure a very simple VPN feature policy that enabled or restricted web browsing and file access for remote clients running Microsoft Windows CE.

The DAP feature accessible on ASDM replaces and expands on the Windows CE support provided by Cisco Secure Desktop Release 3.1.1. Configure a DAP for Pocket PC or Windows CE as follows:

-
- Step 1** Choose **Configuration > Clientless SSL VPN Access > Dynamic Access Policies > Add or Edit**.
- The Add or Edit Dynamic Policy window opens.
- Step 2** Move the mouse to the right of the Endpoint Attribute table and click **Add**.
- The Add or Edit Endpoint Attribute window opens.
- Step 3** Select **Operating System** from the drop-down list next to Endpoint Attribute Type, check **OS Version**, select **Pocket PC** from the adjacent drop-down list, and click **OK**.
- The Add or Edit Endpoint Attribute window closes, leaving the Add or Edit Dynamic Policy window open.
- Step 4** Use the Add or Edit Dynamic Policy window to name and prioritize the DAP entry, complete the configuration of any other selection criteria, and specify the access policy attributes, then click **OK**.
-

How does the timeout setting work on Secure Session?

The timeout setting is independent of the desktop on which the user is operating. If you set a timeout of 1 minute and the remote user switches to the Local Desktop and works there beyond the 1-minute setting, Secure Session closes at the end of the minute. Depending upon other settings, Secure Session saves the data or erases it from the disk. It also uninstalls itself if you configure it to do so.

Which antivirus, antispyware, and firewall applications does Host Scan support?

The list of supported applications and versions is very long and is updated frequently. To view the names of the applications, make sure Cisco Secure Desktop is enabled and that one of the Host Scan Extensions is checked in the Host Scan window, then choose **Configuration > Remote Access > Network (Client) Access or Clientless SSL VPN Access > Dynamic Access Policies > Add or Edit**, click **Add or Edit** on the far right side of the Add or Edit Dynamic Access Policy window, and select the Endpoint Attribute Type of interest. ASDM populates the Vendor ID and Product Description drop-down lists with the supported applications.

Does Secure Session completely eliminate the risk that data will be left behind on a system?

No. Secure Session diligently works to remove data from a remote system. However, Microsoft operating system limitations or installed malicious software may prevent it from completely removing all traces of a session from a remote system.

How does an end user use Secure Session after downloading it the first time?

Once you have downloaded and installed Secure Session, it appears as an entry in the Start menu. Users who want to reuse Secure Session can click **Start > Programs > Cisco Secure Desktop** and enter the password with which they protected the Secure Session.

Can I run multiple instances of Secure Session at the same time?

No, the current release does not support multiple instances of Secure Session on the same PC.

Can Cisco Secure Desktop detect all keystroke loggers?

Cisco Secure Desktop works diligently to detect keystroke loggers. There may be instances where Cisco Secure Desktop is unable to detect a particular keystroke logger, including but not limited to hardware keystroke logging devices.

What security settings do I need to set on user computers?

The following Internet Explorer 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

To launch Java using the Microsoft Virtual Machine:

- Scripting > Active scripting > Enable
- Scripting > Scripting of Java applets > Enable
- ActiveX controls and plug-ins > Download signed ActiveX controls > Enable
- Microsoft VM > Java permissions > High, medium or low safety

What kind of encryption do Secure Session and Cache Cleaner use?

Secure Session and Cache Cleaner encrypt data with 168-bit 3DES. Erasure of the cache meets U.S. Department of Defense standards.

Data Encryption Standard (DES) is an algorithm for protecting data using private encryption keys. DES-CBC is the Cipher Block Chaining (CBC) mode of DES, a stronger form of encryption; it applies an exclusive OR to each block of data with the previous block and then encrypts the data using the DES encryption key. 3DES or Triple DES, the strongest form of encryption, uses different keys to encrypt each data block three times.

How long can the password be for Secure Session reuse?

The password can be up to 127 characters, and can include any combination of upper and lower case letters, plus numbers and punctuation symbols, including spaces.

What happens when the cache is cleaned, either by Secure Session or Cache Cleaner?

Secure Session or Cache Cleaner sanitizes the system, disabling or erasing data that was downloaded, inserted, or created in the browser including file downloads, configuration changes, cached browser information, entered passwords, and auto-completed information.

Can I use fast user switching on Windows XP?

Secure Session does not support fast user switching because only one instance of Secure Session can run on the same computer.

Which Java Virtual Machine is used by Secure Session and Cache Cleaner?

Cisco Secure Desktop checks Internet Explorer to determine which Java Virtual Machine (JVM) has been configured for that particular machine, and uses JVM to install the Cisco Secure Desktop components.

When do modified settings apply to Cache Cleaner and Secure Session?

When you modify the settings in Secure Desktop Manager, you must deploy those settings by clicking the **Apply All** button. The settings take effect the next time that a user loads Secure Session or Cache Cleaner.

Does Secure Session support Japanese character encodings?

Secure Desktop Manager supports encoding such as the Shift_JIS, provided that you configure support for it using ASDM (**Configuration > Clientless SSL VPN Access > Advanced > Encoding**) or the remote user configures encoding using the browser (**View > Encoding** or **View > Character Encoding**).

What does transparent handling of e-mail applications mean?

The use of the term *transparent* means that the Secure Session handles e-mail the same way that the local desktop handles it.

Which applications does Secure Session handle transparently?

Secure Session supports transparent handling of Microsoft Outlook, Outlook Express, Eudora, and Lotus Notes.

Does Secure Session or Cache Cleaner detect a second network card for prelogin policy determination?

No, it detects only the IP address of the first network card.

I am using a personal firewall. What application must I allow to access the network?

You must allow the program main.exe to access the network.

Does the Host Scan check whether antivirus, antispysware, and firewall applications are present or running on the endpoint?

The Endpoint Assessment function of Host Scan, if enabled, returns for DAP evaluation the answer to whether the antivirus, antispysware, and firewall application selected as an endpoint attribute is *running*.