



Introduction

Cisco SSL VPN solutions provide organizations with robust and flexible products for protecting the security and privacy of information, and can play an important part in an organization's compliance strategies. No single technology today addresses all security requirements under the proposed standards. In addition, given operating system limitations, 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 using Cisco Secure Desktop, when combined with other security controls and mechanisms within the context of an effective risk management strategy and policy, can help reduce risks associated with using such technologies.

The following sections describe the capabilities of Cisco Secure Desktop, introduce the Secure Desktop Manager interface, and describe how to save configuration changes:

- [Features](#)
- [Cisco Secure Desktop Workflow](#)
- [Management Interface](#)
- [Saving and Resetting the Running Configuration](#)

Features

Cisco Secure Desktop seeks to minimize the risks posed by the use of remote devices to establish a Cisco clientless SSL VPN or AnyConnect Client session. Cisco Secure Desktop provides a number of features that you can configure to work independently or together.

The following sections describe the Cisco Secure Desktop features:

- [Integration with Dynamic Access Policies](#)
- [Host Scan](#)
- [Prelogin Assessment](#)
- [Prelogin Policies](#)
- [Secure Session](#)
- [Cache Cleaner](#)
- [Keystroke Logger Detection](#)
- [Host Emulation Detection](#)

Integration with Dynamic Access Policies

The security appliance integrates the Cisco Secure Desktop features into dynamic access policies (DAPs). Depending on the configuration, the security appliance uses one or more endpoint attribute values in combination with optional, AAA attribute values as conditions for assigning a DAP. The Cisco Secure Desktop features supported by the endpoint attributes of DAPs include OS detection, prelogin policies, Basic Host Scan results, and Endpoint Assessment. (The sections that follow describe these features.)

As an administrator, you can specify a single attribute or combine attributes that together form the conditions required to assign a DAP to a session. The DAP provides network access at the level that is appropriate for the endpoint AAA attribute value. The security appliance applies a DAP when all of its configured endpoint criteria are satisfied.

Host Scan

Host Scan is a module that installs on the remote device after the user connects to the security appliance, before the user logs in. In Version 3.2.1, Host Scan runs on Microsoft Windows Vista, Windows XP, Windows 2000, Mac OS X 10.4, and Linux.

Host Scan consists of any combination of the following modules (Basic Host Scan, Endpoint Assessment, and advanced Endpoint Assessment), as configured by the Cisco Secure Desktop administrator.

Basic Host Scan

Basic Host Scan automatically identifies operating systems and service packs on connecting computers. It also lets you configure inspections for specific process names and filenames, and

keys on those running Microsoft Windows operating systems. Thus, you can use this feature to configure checks for watermarks on remote computers to determine whether they are corporate-owned. You can use the results to be returned by Basic Host Scan when configuring different DAPs to distinguish corporate computers, home computers, and public computers.

Basic Host Scan attempts to run on any remote device establishing a Cisco clientless SSL VPN or AnyConnect Client session, if Cisco Secure Desktop is enabled on the security appliance. The OS detection automatically qualifies or disqualifies the remote device from running Endpoint Assessment, Endpoint Assessment, Secure Session, and Cache Cleaner, whichever is configured to run. Process name, filename, and registry key checking to be performed by Basic Host Scan must be explicitly configured using Cisco Secure Desktop Manager. Basic Host Scan returns the name of the OS and service pack, and the results of any configured checks to the security appliance.

The security appliance evaluates the returned values against the endpoint criteria explicitly configured into the DAPs. Thus, you can assign DAPs to devices based on this data. For a list of the operating systems and service packs this module detects, see *Release Notes for Cisco Secure Desktop, Release 3.2.1*. To view this list, choose **Configuration > Network (Client) Access** or **Clientless SSL VPN Access > Dynamic Access Policies > Add** or **Edit**, **Add** or **Edit** next to the endpoint attributes table, select **Operating System** from the Endpoint Attribute Type drop-down list, check OS Version, and click the arrow to the right of the adjacent operator.

Basic Host Scan returns the following additional values for evaluation against configured DAP endpoint criteria:

- Microsoft Windows, Mac OS, and Linux builds

- Listening ports active on a connecting host running Microsoft Windows
- Cisco Secure Desktop components installed on the connecting host

To configure endpoint criteria to match this data, enter the appropriate free-form Lua text into the Advanced Logical Expressions text box. Be aware that doing so requires sophisticated knowledge of Lua. For more information, open the Add or Edit Dynamic Access Policies window, click **Advanced** at the bottom of the Selection Criteria area, and click the **Guide** button to the right of the Logical Expressions text box.

Endpoint Assessment

Endpoint Assessment, a Host Scan extension, examines the remote computer for a large collection of antivirus and antispymware applications, associated definitions updates, and firewalls. You can use this feature to combine endpoint criteria to satisfy your requirements before the security appliance assigns a specific DAP to the session.

Advanced Endpoint Assessment

Advanced Endpoint Assessment, another Host Scan extension, lets you configure an attempt to update noncompliant computers. For example, you can use this feature to attempt to force updates of a specific antivirus application version and its antivirus definitions file. This feature requires an Advanced Endpoint Assessment license.

Prelogin Assessment

The prelogin assessment module also installs itself after the user connects to the security appliance, but before the user logs in. This module can check the remote device for files, digital certificates, the OS version, IP address, and Microsoft Windows registry keys.

Secure Desktop Manager, the administrator interface to Cisco Secure Desktop, provides a graphical sequence editor to simplify the configuration of the prelogin assessment module.

When configuring the prelogin assessment module, the Cisco Secure Desktop administrator creates branches of nodes called *sequences*. Each sequence begins with the Start node, followed by an endpoint check. The result of the check determines whether to perform another endpoint check or to terminate the sequence with an end node.

The end node determines whether to display a Login Denied message, assign a prelogin policy to the device, or perform a secondary set of checks called a subsequence. A *subsequence* is a continuation of a sequence, typically consisting of more endpoint checks and an end node. This feature is useful to do the following:

- Reuse a sequence of checks in some cases but not others.
- Create a set of conditions that have an overall purpose that you want to document by using the subsequence name.
- Limit the horizontal space occupied by the graphical sequence editor.

Prelogin Policies

Prelogin policies let you determine how remote devices connect to your virtual private network, and protect them accordingly. Prelogin policies specify the remote user experience, rights, and restrictions. You create prelogin policies when you configure the prelogin assessment module. The results of the checks in the graphical sequence editor determine whether the prelogin assessment module assigns a particular prelogin policy.

As you create each policy, Secure Desktop Manager adds a menu named after the policy. Each of the prelogin policy menus let you assign unique settings for the policy. These settings determine whether the Secure Session module, Cache Cleaner module, or neither module installs on remote devices that match the prelogin criteria assigned to the policy. Administrators typically assign these modules to noncorporate computers to prevent access to corporate data and files after the session is over. The sections that follow provide more information about the Secure Session and Cache Cleaner modules.

You might choose to assign neither Secure Session nor Cache Cleaner to the prelogin policy if the remote device is a corporate computer. For example, computers connecting from within a workplace LAN on a 10.x.x.x network are an unlikely risk for exposing confidential information. For these computers, you might set up prelogin policy named Secure to match the IP addresses on the 10.x.x.x network, and disable Secure Session and Cache Cleaner on that policy.

In contrast, users' home computers might be considered more at risk to viruses because of their mixed use. For these computers, you might set up a prelogin policy named home for employees' home computers on which they have installed a corporate-supplied certificate. DAP criteria that includes this prelogin policy should also require the presence of antivirus and antispymware software to grant full access to the network.

Finally, for untrusted locations such as Internet cafes, you might set up a prelogin policy named "Public" that has either no matching criteria, thus making it the default policy for remote access devices that do not meet the requirements of more secure policies; or you might define criteria that are less stringent. This prelogin policy would require a Secure Session installation, and include a short timeout period to prevent access by unauthorized users.

Secure Session

Secure Session, also called Secure Desktop or Vault, encrypts the data and files associated with or downloaded during the remote session into a secure desktop 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. Upon session termination, it uses a U.S. Department of Defense (DoD) sanitation algorithm to remove the partition.

Typically used during clientless SSL VPN sessions, Secure Session attempts to reduce the possibility that cookies, browser history, temporary files, and downloaded content remain after a remote user logs out, the session times out, or after an abrupt termination occurs.

Secure Session runs over Microsoft Windows XP and Windows 2000. If a prelogin policy is configured to install Secure Session, but the operating system on the remote computer does not support Secure Session, Cache Cleaner attempts to install instead.

Secure Session does not encrypt or clean system memory information, including that which may be left on the disk by the operating system in the Microsoft Windows virtual memory file, commonly referred to as the paging file. Secure Desktop Manager provides an option that seeks to disable printing from within a user session. If local printing is permitted, there may be instances when data can remain in the local system print spool.

Cache Cleaner

Cache Cleaner, an alternative to Secure Desktop, is functionally more limited than Secure Session, but has the flexibility to support more operating systems. It attempts to eliminate the information from the browser cache at the end of a clientless SSL VPN or AnyConnect Client session. This information includes entered passwords, auto-completed text, files cached by the browser, and browser configuration changes made during the session.

Cache Cleaner runs on Microsoft Windows Vista, Windows XP, and Windows 2000; Apple Mac OS X 10.4 (PowerPC or Intel); and Linux.

Keystroke Logger Detection

You can configure each prelogin policy to scan for keystroke logging applications and deny access if a suspected keystroke logging application is present. You can use Secure Desktop Manager to enable or disable this feature, and specify the keystroke logging applications that are safe or let the remote user interactively approve the applications the scan identifies.

By default, keystroke logger detection is disabled for each prelogin policy. If you enable it, it downloads with Secure Desktop, Cache Cleaner, or Host Scan onto the remote computer. Following the download, keystroke logger runs first. The associated module runs only if the scan is clear, or only if you assign administrative control to the user and the user approves of the applications the scan identifies.

Keystroke logger detection supports Microsoft Windows Vista, Windows XP, and Windows 2000. It may be unable to detect every potentially malicious keystroke logger, including but not limited to hardware keystroke logging devices.

Host Emulation Detection

Host emulation detection, another feature of prelogin policies, determines whether a remote Microsoft Windows operating system is running over virtualization software. You can use Secure Desktop Manager to enable or disable this feature, and deny access if a host emulator is present or report the detection to the user and let the user decide whether to continue or terminate.

By default, host emulation detection is disabled for each prelogin policy. If you enable it, it downloads with Secure Desktop, Cache Cleaner, or Host Scan onto the remote computer. Following the download, host emulation detection runs first, along with keystroke logger detection if it is configured to do so. The associated module then runs if either of the following conditions are true:

- The host is not running over an emulator (or virtualization software).
- You did not configure it to always deny access, and the user approves of the detected host emulator.

Host emulation detection supports Microsoft Windows Vista, Windows XP, and Windows 2000.

Cisco Secure Desktop Workflow

When fully configured, Cisco Secure Desktop works with the security appliance to protect the corporate network as follows:

Step 1 The remote device attempts to establish a clientless SSL VPN or AnyConnect Client session with the security appliance.



Note Each of the “modules” identified in this section are features of Cisco Secure Desktop.

Step 2 A prelogin assessment module checks for the following on the remote device:

- OS.
- Presence or absence of any files you (the Cisco Secure Desktop administrator) specify.
- Presence or absence of any registry keys you specify. This check applies only if the computer is running Microsoft Windows.
- Presence of any digital certificates you specify. This check also applies only if the computer is running Microsoft Windows.
- IP address within a range you specify.

Step 3 One of the following events occurs, depending on the result of the previous step:

- The Login Denied message appears if the remote computer runs the prelogin assessment and traverses a sequence that ends with a Login Denied end node. In this case, interaction between the security appliance and the remote device stops.
- The prelogin assessment module assigns a prelogin policy name to the device and reports the name of the prelogin policy to the security appliance.

Step 4 Host Scan downloads and runs with Secure Session, Cache Cleaner, or neither, depending on whether one of these modules is enabled on the prelogin policy assigned to the remote device. If Secure Desktop (Secure Session) is enabled but it cannot run on the operating system detected, only Cache Cleaner runs.

Step 5 The user logs in.

Step 6 The security appliance typically uses the authentication data along with any configured endpoint attribute criteria, which can include such values as the prelogin policy and Host Scan results, to apply a DAP to the session.

Step 7 Following the termination of the user session, Host Scan terminates, and Cache Cleaner or Secure Desktop performs its cleanup functions.

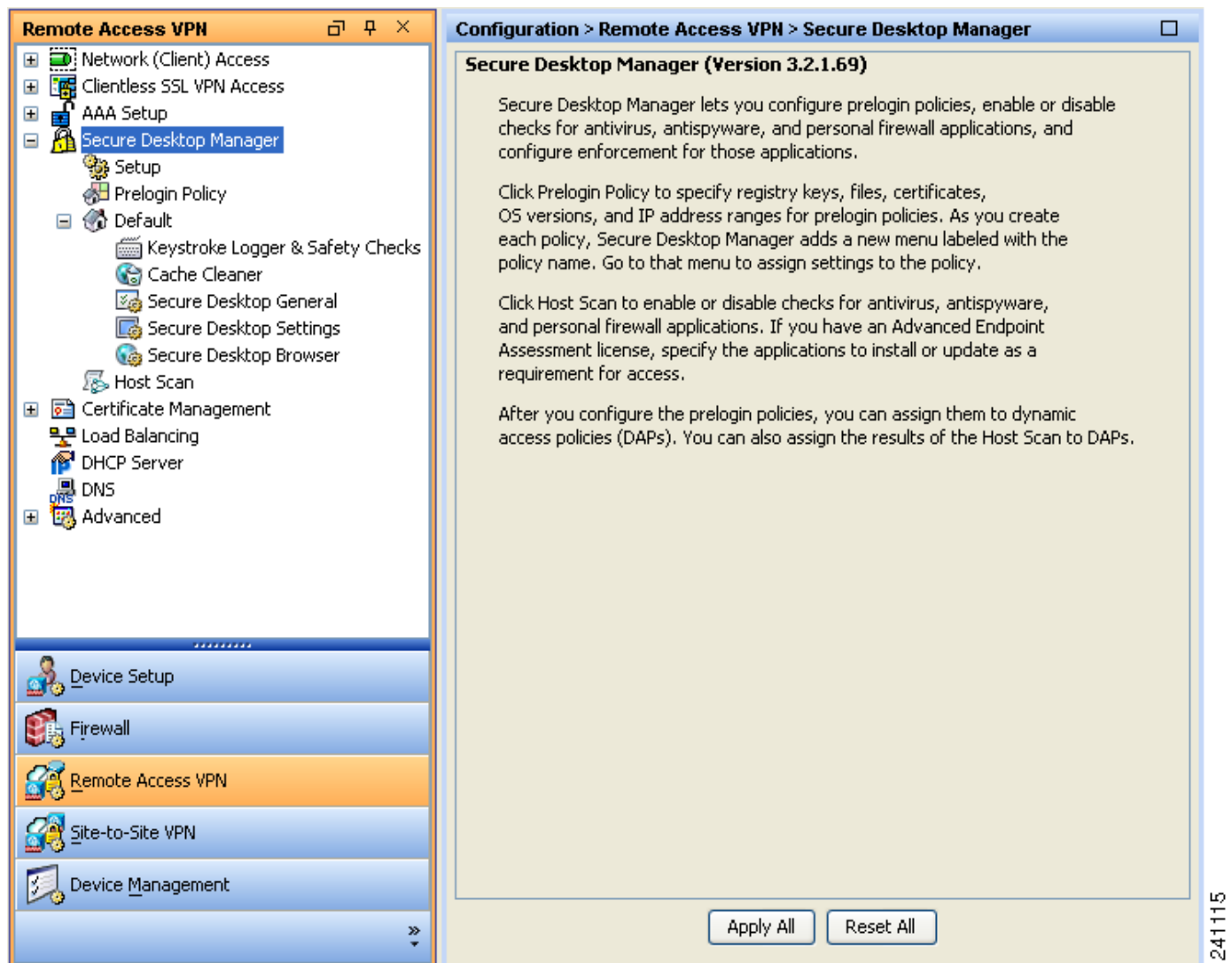
Management Interface

The management interface called *Secure Desktop Manager* lets you configure Cisco Secure Desktop on the security appliance. After installing and enabling Cisco Secure Desktop, choose **Configuration > Remote Access VPN > Secure Desktop Manager**.

The Secure Desktop Manager pane opens. When Cisco Secure Desktop is disabled, only the Setup menu option is present. This option lets you enable Cisco Secure Desktop.

Figure 1-1 shows the fully-expanded, default menu and the Secure Desktop Manager pane, which appears after you install and enable Secure Desktop, exit the ASDM connection, and establish a new ASDM connection.

Figure 1-1 Secure Desktop Manager (Initial)



The following options are present in the Secure Desktop Manager menu:

- **Setup**—Lets you retrieve a Cisco Secure Desktop image from your computer and install the image, replace and install the existing image with a newer or older one, uninstall the image, and enable or disable Cisco Secure Desktop.
- **Prelogin Policy** — Lets you view or configure the prelogin assessment of computers connecting to the security appliance, and add, view, rename, or remove prelogin policies to be applied to remote computers that pass prelogin assessment criteria.

Use the Prelogin Policy option to specify the conditions the remote computer must satisfy to qualify for a prelogin policy assignment. For example, you can assign a prelogin policy named “Secure” to remote computers with DHCP-assigned IP addresses within the corporate address range.

- **Default**—By default, the prelogin policy diagram displayed by the graphical sequence editor has only one prelogin policy. Its name is Default. Secure Desktop Manager adds a menu to the left for every prelogin policy named in the Prelogin Policy diagram. You can view and change the settings assigned to the prelogin policy by clicking its name in the menu or clicking its subordinate options. When you add a prelogin policy to the configuration, Secure Desktop Manager displays the name of the policy in the menu, along with the following options for configuring privileges and restrictions for that policy:
 - **Keystroke Logger & Safety Checks**—Enables and disables scans of the remote PC for keystroke logging applications and a host emulator.
 - **Cache Cleaner** — Click to refine the Cache Cleaner settings if Secure Desktop or Cache Cleaner on the parent menu is checked. This option now supports Microsoft Windows Vista, Windows XP, and Windows 2000; Apple Macintosh OS X 10.4 (PowerPC or Intel); and Linux.
 - **Secure Desktop General**—Lets you specify Secure Session settings if Secure Session is enabled.
 - **Secure Desktop Settings**—Lets you place restrictions on Secure Session if Secure Session is enabled.
 - **Secure Desktop Browser**—Lets you specify the default home page for the browser. This option also lets you specify folders and bookmarks (or “favorites”) to insert into the respective browser menu during the session.
- **Host Scan**—Click to specify files, processes, and Microsoft Windows registry keys to scan for after completing the prelogin assessment. The scan for these items is called a Basic Host Scan. You can also click Host Scan to enable Endpoint Assessment, a scan for antivirus, personal firewall, and antispyware applications and updates that are running on the remote computer. Finally, you can click Host Scan to configure an Advanced Endpoint Assessment, which updates the specified applications and updates on noncompliant computers. This latter feature requires you to have an Advanced Endpoint Assessment license.

Following the configuration of the prelogin policies and host scan options, you can configure a match of any one or any combination of the following Host Scan results to assign a dynamic access policy following the user login:

- operating system
- (prelogin) policy
- registry key (Microsoft Windows only)
- file
- process
- antivirus application
- personal firewall application
- antispyware application

Saving and Resetting the Running Configuration

Secure Desktop Manager saves all Cisco Secure Desktop configuration data to disk0:/sdesktop/data.xml.

**Note**

To copy the configuration settings from one security appliance to another, transfer a copy of the disk0:/sdesktop/data.xml file to the flash device of the target security appliance. Disable and reenable Cisco Secure Desktop to copy the disk0:/sdesktop/data.xml file into the running configuration.

The security appliance stores the settings displayed in the Secure Desktop Manager > Setup pane. Secure Desktop Manager stores the remaining settings in the disk0:/sdesktop/data.xml file. Secure Desktop Manager displays two buttons at the bottom of the panes beginning with Secure Desktop Manager > Prelogin Policy for interacting with that file. Use these buttons as follows:

- To save the running Cisco Secure Desktop configuration to the data.xml file, click **Apply All**.
- To overwrite all settings in the running Cisco Secure Desktop configuration with those stored in the data.xml file, click **Reset All**.

An “Unapplied Changes” dialog box prompts you to save the Cisco Secure Desktop configuration if you try to navigate away from it or exit without having saved the configuration. Clicking **Apply Changes** in that window is equivalent to clicking the **Apply All** button.

