CHAPTER 5

Configuring Host Scan

The AnyConnect Posture Module provides the AnyConnect Secure Mobility Client the ability to identify the operating system, antivirus, antispyware, and firewall software installed on the host. The Host Scan application, which is among the components delivered by the posture module, is the application that gathers this information.

In the adaptive security appliance (ASA), you can create a prelogin policy that evaluates endpoint attributes such as operating system, IP address, registry entries, local certificates, and filenames. Based on the result of the prelogin policy's evaluation, you can control which hosts are allowed to create a remote access connection to the security appliance.

Starting with AnyConnect 3.0, the Host Scan package becomes a shared component of the AnyConnect Secure Mobility client and Cisco Secure Desktop (CSD). Previously, the Host Scan package was one of several components available only by installing CSD.

The purpose of separating the Host Scan package from CSD is to allow you to update Host Scan support charts more frequently than it was possible when they were delivered as part of CSD. The Host Scan support charts contain the product name and version information of the antivirus, antispyware, and firewall applications used to assign Dynamic Access Policies (DAPs). We deliver the Host Scan application and the Host Scan support charts, as well as other components, in the Host Scan package.

The standalone Host Scan package and the Host Scan package delivered with the posture module provide the same functionality. We provide a separate Host Scan package so that you can update the Host Scan support charts easily.

The Host Scan package can now be delivered in one of three ways: with the AnyConnect Posture Module, with CSD, or as a standalone package. There are two types of AnyConnect posture modules: one version is pushed down by the ASA along with the AnyConnect installation and the other is configured as a pre-deployment module. The pre-deployment module can be installed on endpoints before they make their initial connection to the ASA.

In addition to identifying operating system, antivirus, antispyware, and firewall software installed on the endpoint, the host scan 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 Host Scan package.

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

The AnyConnect client cannot be launched from within Secure Desktop. Users can make AnyConnect connections by first establishing a clientless SSL VPN connection to the ASA and then launching AnyConnect from the portal page.

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

Posture assessment and the AnyConnect telemetry module require Host Scan to be installed on the host.

This chapter contains the following sections:

- Host Scan Workflow, page 5-2
- Features Enabled with the AnyConnect Posture Module, page 5-3
- AnyConnect Posture Module Dependencies and System Requirements, page 5-10
- Host Scan Packaging, page 5-12
- Installing and Enabling Host Scan on the ASA, page 5-14
- Deploying the AnyConnect Posture Module and Host Scan, page 5-13
- Host Scan and CSD Upgrades and Downgrades, page 5-17
- Determining the Host Scan Image Enabled on the ASA, page 5-17
- Uninstalling Host Scan, page 5-17
- Host Scan Logging, page 5-18
- Using a BIOS Serial Number in a Lua Expression, page 5-20
- Other Important Documentation, page 5-21

Host Scan Workflow

Host Scan works with the ASA to protect the corporate network as described in the workflow that follows:

1. The remote device attempts to establish a clientless SSL VPN or AnyConnect Client session with the security appliance.
2. The ASA downloads Host Scan to the client ensuring that the ASA and the client are using the same version of Host Scan.
3. A prelogin assessment checks for the following on the remote computer:
   - Operating system
   - Presence or absence of any files you 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.
4. At the same time the client is undergoing the prelogin assessment, host scan is performing it's endpoint assessment and gathering up the antivirus, firewall, and antispyware version information; as well as scanning for registry keys, files, and processes that you have specified in dynamic access policies.
5. One of the following events occurs, depending on the result of the prelogin assessment:

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

6. Host Scan checks for keystroke loggers and host emulation on the remote computer, based on the configuration of the prelogin policy the remote computer was assigned after the prelogin assessment.
7. Antivirus, firewall, or antispyware remediation occurs if it is warranted and you have a license for Advanced Endpoint Assessment.
8. The user logs in.
9. The ASA typically uses the authentication data gathered in 3. along with any configured endpoint attribute criteria gathered in 4., which can include such values as the prelogin policy and Host Scan results, to apply a dynamic access policy to the session.
10. Following the termination of the user session, Host Scan terminates, and Cache Cleaner performs its cleanup functions.

Features Enabled with the AnyConnect Posture Module

- Prelogin Assessment
- Prelogin Policies
- Keystroke Logger Detection
- Host Emulation Detection
- Cache Cleaner
- Host Scan
- Integration with Dynamic Access Policies

Prelogin Assessment

The prelogin assessment runs after the user connects to the ASA, but before the user logs in. This assessment can check the remote device for files, digital certificates, the OS, IP address, and Microsoft Windows registry keys.

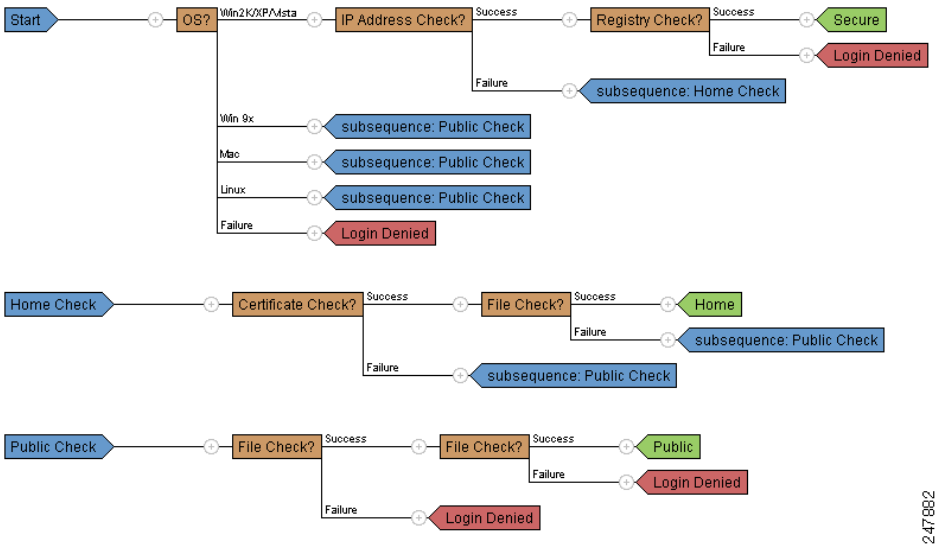
Secure Desktop Manager, the administrator interface to Host Scan, provides a graphical sequence editor to simplify the configuration of the prelogin assessment module.

When configuring the prelogin assessment module, the Host Scan 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.

Figure 5-1 Example of a Completed Prelogin Assessment

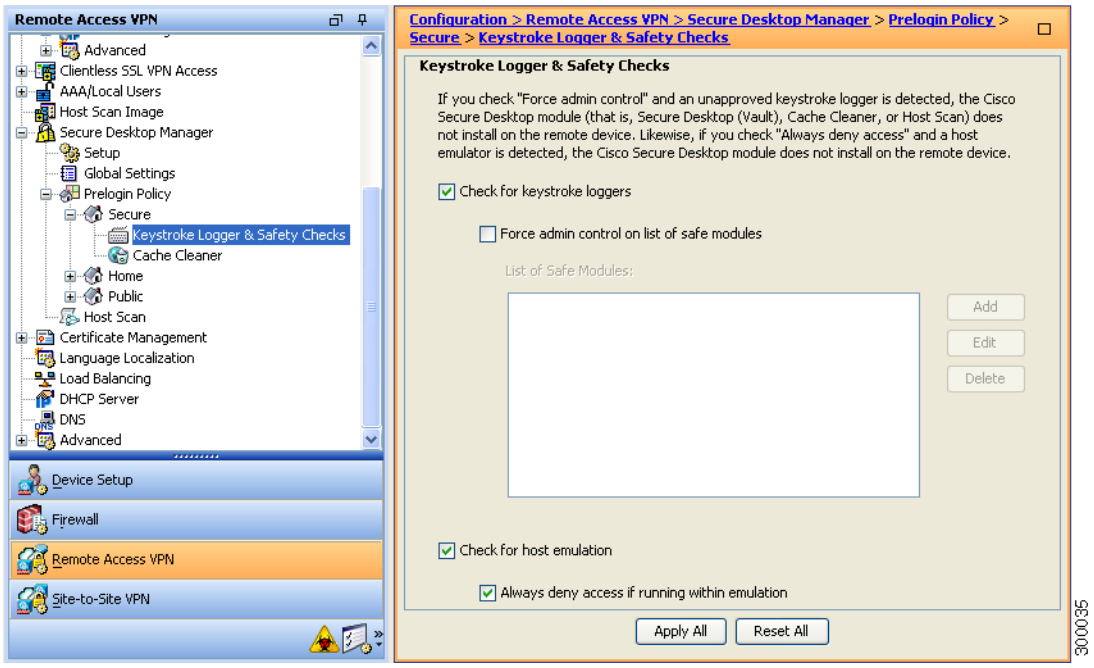


Prelogin Policies

The results of the checks of the prelogin assessment configured in the graphical sequence editor, Figure 5-1, determine whether the prelogin assessment results in the assignment of a particular prelogin policy or a denied remote access connection.

As you create each policy, Secure Desktop Manager adds a menu named after the policy. Each of the policy menus let you assign unique settings to the policy. These settings determine whether Keystroke Logger Detection, Host Emulation Detection, or Cache Cleaner installs on remote devices that match the prelogin criteria assigned to the policy. Administrators typically assign these modules to non-corporate computers to prevent access to corporate data and files after the session is over.

Figure 5-2 Prelogin Policies



Keystroke Logger Detection

You can configure selected prelogin policies to scan for processes or modules that record keystrokes entered by the user, and deny VPN access if a suspected keystroke logging application is present.

By default, keystroke logger detection is disabled for each prelogin policy. You can use Secure Desktop Manager to enable or disable keystroke logger detection. You can specify the keystroke loggers that are safe or let the remote user interactively approve the ones that the scan identifies as a condition for running Cache Cleaner or Host Scan on the remote computer.

If you enable it, keystroke logger detection downloads with Cache Cleaner or Host Scan onto the remote computer. Following the download, keystroke logger detection runs only if the OS is Windows and the user login has administrator privileges.

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.

Note Keystroke logger detection applies to both user mode and kernel mode loggers as long as the end-user is logged in with administrator privileges.

Keystroke logger detection runs only on 32-bit Microsoft Windows OS's. See the "Keystroke Logger Detection and Host Emulation Detection Supported Operating Systems" section on page 5-6.

Keystroke logger detection may be unable to detect every potentially malicious keystroke logger. It does not detect 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.

See the "Keystroke Logger Detection and Host Emulation Detection Supported Operating Systems" section on page 5-6.

Keystroke Logger Detection and Host Emulation Detection Supported Operating Systems

Keystroke Logger Detection and Host Emulation Detection run on the following operating systems:

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

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

Note Secure Desktop, Keystroke Logger Detection and Host Emulation Detection are not supported on Windows 7.

Cache Cleaner

Cache Cleaner, an alternative to Secure Desktop, is functionally more limited, 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, browser configuration changes made during the session, and cookies.

Cache Cleaner runs on Microsoft Windows, Apple Mac OS, and Linux. For detailed system requirements, see the Cisco Secure Desktop Release Notes.

This is a typical sequence of events when Cache Cleaner has been deployed and the endpoint attempts to create a clientless SSL VPN connection or attempts to launch AnyConnect using web launch:

Step 1 The endpoint connects to the ASA when the user enters its URL in a browser.

Step 2 Hostscan performs the prelogin assessment.

Step 3 Assuming that the endpoint passes the prelogin assessment, AnyConnect authentication begins. The user may enter a password or use a certificate to authenticate.

Step 4 For users running Internet Explorer without **Clean the whole cache in addition to the current session cache (IE only)** enabled, or for users running Safari or Firefox, the Cache Cleaner takes a snapshot of the browser's cache approximately one minute after the user authenticates.

Step 5 As the user works, the browser caches information.

Step 6 When users logout of the VPN session:

- For users running Internet Explorer with **Clean the whole cache in addition to the current session cache (IE only)** enabled, Cache Cleaner attempts to delete the browser's entire cache.
- For users running Internet Explorer without **Clean the whole cache in addition to the current session cache (IE only)** enabled, or running Safari or Firefox, Cache Cleaner attempts to delete all of the browser's cache and then Cache Cleaner restores the snapshot it took of the cache.

  To prevent any sensitive information from being restored on the computer, we recommend that you manually clean the browser's cache, after your session and then close the browser.

Note We recommend that Cache Cleaner be configured with the **Clean the whole cache in addition to the current session cache (IE only)** option enabled.

Host Scan

Host Scan is a package that installs on the remote device after the user connects to the ASA and before the user logs in. Host Scan consists of any combination of the Basic Host Scan module, Endpoint Assessment module, and Advanced Endpoint Assessment module; as configured by the CSD administrator. Host Scan runs on Microsoft Windows, Apple Mac OS X, and Linux. For detailed requirements, see System Requirements, page 5-11.

The Host Scan package is delivered bundled with CSD, as a standalone module, and as part of the Posture Module of the AnyConnect 3.0 client.

Basic Host Scan Functionality

Host Scan automatically identifies operating systems and service packs on any remote device establishing a Cisco clientless SSL VPN or AnyConnect client session and when CSD or Host Scan/CSD is enabled on the ASA.

You can also configure Host Scan to inspect the endpoint, for specific processes, files, registry keys, digital certificates, and IP addresses using the Secure Desktop manager. Secure Desktop manager is integrated with Adaptive Security Device Manager (ASDM) on the ASA.

Host Scan performs all of these inspections before users log on to their computers.

After Host Scan gathers from the endpoint the operating system and service pack information along with the processes, files, registry keys, digital certificates, and IP addresses you configured it to gather, it sends this information to the ASA where it can be used to distinguish between corporate-owned, personal, and public computers. The information can also be used in prelogin assessments. See Prelogin Assessment, page 5-3 for more information.

Host Scan also automatically 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
- CSD components installed on the connecting host
- Microsoft Knowledge Base numbers (KBs)

For more information about DAP and Lua expressions see Integration with Dynamic Access Policies, page 5-9 and Chapter 7, "Using Match Criteria to Configure Dynamic Access Policies" in *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*.

Endpoint Assessment

Endpoint Assessment is a Host Scan extension that examines the remote computer for a large collection of antivirus and antispyware applications, associated definitions updates, and firewalls. You can use this feature to combine endpoint criteria to satisfy your requirements before the ASA assigns a specific dynamic access policy (DAP) to the session. See Chapter 7, "Using Match Criteria to Configure Dynamic Access Policies" in *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators* for more information on DAPs.

Advanced Endpoint Assessment - Antivirus, Antispyware, and Firewall Remediation

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

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.

Antivirus —Advanced Endpoint Assessment can attempt to remediate these components of antivirus software:

- Force File System Protection — If the antivirus software is disabled, Advanced Endpoint Assessment can enable it.
- Force Virus Definitions Update — If the antivirus definitions have not been updated in the number of days defined by the Advanced Endpoint Assessment configuration, Advanced Endpoint Assessment can attempt to initiate an update of virus definitions.

Antispyware — If the antispyware definitions have not been updated in the number of days defined by the Advanced Endpoint Assessment configuration, Advanced Endpoint Assessment can attempt to initiate an update of antispyware definitions.

Personal Firewall — The Advanced Endpoint Assessment module can attempt to reconfigure firewall settings and rules if they do not meet the requirements defined in the Advanced Endpoint Assessment configuration.

- The firewall can be enabled or disabled.
- Applications can be prevented from running or allowed to run.
- Ports can be blocked or opened.

Note Not all personal firewalls support this feature.

If the end-user disables antivirus or personal firewall, after successfully establishing the VPN connection, our Advanced Endpoint Assessment feature will attempt to re-enable that application within approximately 60 seconds.

Host Scan Support Charts

The Host Scan support charts contain the product name and version information for the antivirus, antispyware, and firewall applications you use in your prelogin policies. We deliver Host Scan and the Host Scan support chart in the Host Scan package.

In this release of the AnyConnect Secure Mobility Client, the Host Scan package can be uploaded separately from Cisco Secure Desktop (CSD). This means you can deploy Host Scan functionality without having to install CSD, and you are able to update your Host Scan support charts by upgrading to the latest Host Scan package.

You can download the Host Scan support charts from cisco.com, here:
http://www.cisco.com/en/US/products/ps10884/products_device_support_tables_list.html

These support charts can be viewed using Microsoft Excel, Microsoft Excel Viewer, or OpenOffice. Browsers such as Firefox, Chrome, and Safari provide the best download experience.

Configuring Antivirus Applications for Host Scan

Antivirus applications can misinterpret the behavior of some of the applications included in the posture module and the Host Scan package as malicious. Before installing the posture module or Host Scan package, configure your antivirus software to "white-list" or make security exceptions for these Host Scan applications:

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

Integration with Dynamic Access Policies

The ASA integrates the Host Scan features into dynamic access policies (DAPs). Depending on the configuration, the ASA uses one or more endpoint attribute values in combination with optional AAA attribute values as conditions for assigning a DAP. The Host Scan features supported by the endpoint attributes of DAPs include OS detection, prelogin policies, basic Host Scan results, and endpoint assessment.

Note In order to enable Host Scan features, you must have an AnyConnect Premium license installed on the ASA.

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 ASA applies a DAP when all of its configured endpoint criteria are satisfied.

Difference Between the Posture Module and the Standalone Host Scan Package

The AnyConnect Posture Module can be deployed by the ASA to the endpoint, or it can be installed on the endpoint using a pre-deployment kit before the endpoint makes its initial connection to the ASA.

The posture module contains the Host Scan package, prelogin assessment, keystroke logger detection, host emulation detection, and cache cleaner, as well as a few other modules that the Host Scan application requires. Deploying the posture module allows Host Scan to run privileged operations even when the user on the endpoint is not an administrator, and it allows other AnyConnect modules to start using Host Scan.

The standalone Host Scan package delivers the Host Scan engine, prelogin assessment module, keystroke logger detection and host emulation detection.

AnyConnect Posture Module Dependencies and System Requirements

The AnyConnect posture module contains the Host Scan package and other components.

Dependencies

The AnyConnect Secure Mobility Client with the posture module requires these minimum ASA components:

- ASA 8.4
- ASDM 6.4

These AnyConnect features require that you install the posture module.

- Host Scan
- SCEP authentication
- AnyConnect Telemetry Module

Host Scan, CSD, and AnyConnect Secure Mobility Client Interoperability

Caution If you deploy Host Scan with the AnyConnect Secure Mobility Client, version 3.0.x, the AnyConnect Secure Mobility Client requires Host Scan to have the same version number, or a later version number, than itself.

If you have Cisco Secure Desktop (CSD) version 3.5, or earlier, enabled on the ASA and you do not upgrade the Host Scan package to match or exceed the version of AnyConnect Secure Mobility Client 3.0.x you are deploying, prelogin assessments will fail, and users will be unable 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 Host Scan package on the endpoint to match the Host Scan package enabled on the ASA.

AnyConnect 2.5.3005 and earlier is not compatible with any version of Host Scan.

System Requirements

The posture module can be installed on any of these platforms:

- Windows XP (x86 and x86 running on x64)
- Windows Vista (x86 and x86 running on x64)
- Windows 7 (x86 and x86 running on x64)
- Mac OS X 10.5,10.6 (32-bit and 32-bit running on 64-bit)
- Linux (32-bit and 32-bit running on 64-bit)

Note Host Scan is a 32-bit application and requires the core 32-bit libraries to be installed on 64-bit Linux operating systems. Host Scan does not provide these 32-bit libraries at the time it is installed. Customers need to install the 32-bit libraries on the endpoints themselves, if they are not already provisioned.

Licensing

These are the AnyConnect licensing requirements for the posture module:

- An AnyConnect Premium license is required for all features delivered with Host Scan including basic Host Scan, endpoint assessment, and advanced endpoint assessment.
- The Advanced Endpoint Assessment license is an additional license required for
  - Remediation
  - Mobile Device Management

Entering an Activation Key to Support Advanced Endpoint Assessment

Advanced Endpoint Assessment includes all of the Endpoint Assessment features and lets you configure an attempt to update noncompliant computers to meet version requirements. You can use ASDM to activate a key to support Advanced Endpoint Assessment after acquiring it from Cisco, as follows:

Step 1 Choose **Configuration > Device Management > Licensing > Activation Key**.

Step 2 Enter the key in the **New Activation Key** field.

Step 3 Click **Update Activation Key**.

Step 4 Choose **File > Save Running Configuration to Flash**.

An Advanced Endpoint Assessment entry appears and the Configure button becomes active in the Host Scan Extensions area of the **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan** pane, which is accessible only if CSD is enabled.

Host Scan Packaging

You can load the Host Scan package on to the ASA in one of these ways:

- You can upload it as a standalone package: **hostscan-*version*-k9.pkg**
- You can upload it by uploading an AnyConnect Secure Mobility package: **anyconnect-win-*version*-k9.pkg**
- You can upload it by uploading a Cisco Secure Desktop package: **csd_version-k9.pkg**

Table 5-1 Host Scan Packages You Load to the ASA

File	Description
hostscan-*version*-k9.pkg	This file contains the Host Scan image, Host Scan support charts, prelogin assessment module, cache cleaner, keystroke logger detection and host emulation detection.
anyconnect-win-*version*-k9.pkg	This package contains all the Cisco AnyConnect Secure Mobility Client features including the hostscan-*version*-k9.pkg file.
csd_*version*-k9.pkg	This file contains all Cisco Secure Desktop features including Host Scan software as well as the Host Scan support charts, secure desktop (Vault), cache cleaner, key stroke logger detection, and host emulation detection.

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

The Host Scan image is delivered with the Host Scan package. It can be deployed to the endpoint from the standalone Host Scan 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 Host Scan image first and if you have not specified one, the ASA enables the Host Scan functionality from Cisco Secure Desktop. See the "Installing or Upgrading Host Scan" section on page 5-15.

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

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

- If you have installed a standalone Host Scan package on the ASA and have designated it as the Host Scan image, and you enable CSD/hostscan, ASA distributes the standalone Host Scan package.
- If you have installed a standalone Host Scan package on the ASA and have designated it as the Host Scan image and you have installed a CSD image on the ASA, and you enable CSD/hostscan, ASA will distribute the standalone Host Scan image.
- If you have installed a Host Scan image on the ASA, but you have not enabled it, and you have installed a CSD image on the ASA and you have enabled CSD/hostscan, the ASA will distribute the standalone Host Scan image because it was not uninstalled.
- If you have installed an AnyConnect Secure Mobility Client package on the ASA and have designated it as the Host Scan image, the ASA will distribute the Host Scan image from that package.

- If you install an AnyConnect Secure Mobility Client package file on the ASA but do not specify it as the Host Scan image, the ASA will not distribute the Host Scan package associated with that AnyConnect package. The ASA will distribute an installed Host Scan package or CSD package, provided CSD is enabled.

Deploying the AnyConnect Posture Module and Host Scan

There are two different deployment scenarios for the posture module and Host Scan.

Pre-deployment. Using the pre-deployment method, you install the AnyConnect client and posture module before the endpoint attempts to make a connection to the ASA. The pre-deployment posture module package contains every component, library, and support chart that could be used to gather posture attributes as well as the applications that provide you with the features described in the "Features Enabled with the AnyConnect Posture Module" section on page 5-3. If you pre-deploy to the endpoint the same version of the AnyConnect client and posture module installed on the ASA, no additional posture module files are pushed down from the ASA when the endpoint connects to the ASA.

Web-deployment. Using the web-deployment method, when the endpoint connects to the ASA, the ASA pushes the AnyConnect client and posture module down to the endpoint. To make the download as fast and efficient as possible, the ASA only downloads the essential posture module files.

When the endpoint connects again, the essential posture module files determine what other libraries or files it needs to perform an endpoint assessment and retrieves those files from the ASA. For example, the posture module may retrieve a Host Scan support chart of all Norton anti-virus software because a version of Norton anti-virus is running on the endpoint. After the posture module retrieves the additional files it needs, it performs the endpoint assessment and forwards the attributes to the ASA. Assuming the endpoint attributes are sufficient to satisfy a dynamic access policy (DAP) rule, the ASA allows the endpoint to connect. As a result of satisfying the DAP, the ASA could be configured to push the remainder of the posture module to the endpoint or not.

If you do not want the entire posture module web-deployed to the endpoint, you can perform a limited web-deployment where only one posture file is downloaded to the endpoint, and it requests only the Host Scan libraries it needs to perform endpoint assessment. In this scenario, you will have very short downloads times from the ASA to the endpoint, but you will lose the ability to perform Advanced Endpoint Assessment and perform such tasks as antivirus, antispyware, or firewall remediation tasks.

Pre-Deploying the AnyConnect Posture Module

When you pre-deploy the posture module, you install it on the endpoint before the AnyConnect client makes its initial connection to the ASA.

You need to install the AnyConnect Secure Mobility Client on the endpoint before you install the posture module. See Chapter 2, "Deploying the AnyConnect Secure Mobility Client" for instructions on installing the AnyConnect Secure Mobility Client and the posture module using web-deployment and pre-deployment methods.

Table 5-2 lists the posture module pre-deployment kits:

Table 5-2 Posture Module Pre-Deployment Kits

File	Description
Windows	anyconnect-posture-win-*version*-pre-deploy-k9.msi

Table 5-2 Posture Module Pre-Deployment Kits

File	Description
Linux	anyconnect-linux-*version*-posture-k9.tar.gz
Mac OS X	anyconnect-macosx-posture-i386-*version*-i386-k9.dmg

Installing and Enabling Host Scan on the ASA

These tasks describe installing and enabling Host Scan on the ASA:

- Downloading the Latest Host Scan Engine Update
- Installing or Upgrading Host Scan
- Enabling or Disabling Host Scan on the ASA
- Uninstalling Host Scan
- Assigning AnyConnect Posture Module to a Group Policy

Downloading the Latest Host Scan Engine Update

To download the latest Cisco Host Scan Engine Updates, you must be a registered user of Cisco.com.

Step 1 Click this link to reach the software download area for Cisco VPN Client Tools:

http://www.cisco.com/cisco/software/release.html?mdfid=282414594&flowid=4470&softwareid=282364364&release=Engine%20Updates&relind=AVAILABLE&rellifecycle=&reltype=latest

Step 2 Expand **Latest Releases** in the product directory tree.

Step 3 Click **Engine Updates.**

Step 4 In the column on the right, find the latest version of **hostscan_3.0.xxxx-k9.pkg** and click **Download Now.**

Step 5 Enter your cisco.com credentials and click **Login**.

Step 6 Click **Proceed with Download.**

Step 7 Read the End User License Agreement and click **Agree**.

Step 8 Select a download manager option and click the **download** link to proceed with the download.

Installing or Upgrading Host Scan

Use this procedure to upload, or upgrade, and enable a new Host Scan image on the ASA. Use the image to enable Host Scan functionality for AnyConnect or upgrade the Host Scan support charts for an existing deployment of Cisco Secure Desktop (CSD).

You can specify a standalone Host Scan package or an AnyConnect Secure Mobility Client version 3.0 or later package in the field.

If you previously uploaded a CSD image to the ASA, the Host Scan image you specify will upgrade or downgrade the existing Host Scan files that were delivered with that CSD package.

You do not need to restart the security appliance after you install or upgrade Host Scan; however, you must exit and restart Adaptive Security Device Manager (ASDM) to access the Secure Desktop Manager tool in ASDM.

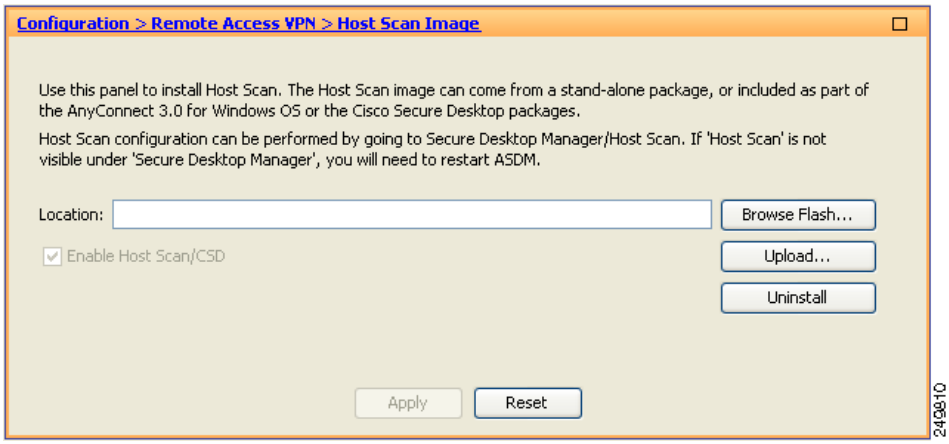
Note Host Scan requires an AnyConnect Secure Mobility Client premium license.

Step 1 Download the latest version of the Host Scan package using Downloading the Latest Host Scan Engine Update, page 5-14.

Note You will need to have an account on Cisco.com and be logged in to download the software.

Step 2 Open ASDM and choose **Configuration > Remote Access VPN > Host Scan Image.** ASDM opens the Host Scan Image panel (Figure 5-3).

Figure 5-3 Host Scan Image Panel



Step 3 Click **Upload** to prepare to transfer a copy of the Host Scan package from your computer to a drive on the ASA.

Step 4 In the Upload Image dialog box, click **Browse Local Files** to search for the Host Scan package on your local computer.

Step 5 Select the **hostscan_*version*.pkg** file or **anyconnect-win-*version*-k9.pkg** file you downloaded in Step 1 and click **Select**. The path to the file you selected is in the Local File Path field and the Flash File System Path field reflects the destination path of the Host Scan package. If your ASA has more than one flash drive, you can edit the Flash File System Path to indicate another flash drive.

Step 6 Click **Upload File**. ASDM transfers a copy of the file to the flash card. An Information dialog box displays the following message:

```
File has been uploaded to flash successfully.
```

Step 7 Click **OK**.

Step 8 In the Use Uploaded Image dialog, click **OK** to use the Host Scan package file you just uploaded as the current image.

Step 9 Check **Enable Host Scan/CSD** if it is not already checked.

Step 10 Click **Apply**.

Note If AnyConnect Essentials is enabled on the ASA, you receive a message that Host Scan and CSD will not work with it. You have the choice to **Disable** or **Keep** AnyConnect Essentials.

Step 11 Click **Save**.

Enabling or Disabling Host Scan on the ASA

When you first upload or upgrade a Host Scan image using ASDM, you enable the image as part of that procedure. See the "Installing and Enabling Host Scan on the ASA" section on page 5-14.

Otherwise, to enable or disable a Host Scan image using ASDM, follow this procedure:

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Host Scan Image.** ASDM opens the Host Scan Image panel (Figure 5-3).

Step 2 Check **Enable Host Scan/CSD** to enable Host Scan or uncheck **Enable Host Scan/CSD** to disable Host Scan.

Step 3 Click **Apply**.

Step 4 Click **Save**.

Enabling or Disabling CSD on the ASA

Enabling Cisco Secure Desktop (CSD) loads the CSD configuration file and data.xml from the flash device to the running configuration. Disabling CSD does not alter the CSD configuration.

Use ASDM to enable or disable CSD as follows:

Step 1 Choose **Configuration > Remote Access VPN > Secure Desktop Manager > Setup**.

ASDM opens the Setup pane (Figure 5-3).

Note The Secure Desktop Image field displays the image (and version) that is currently installed. The Enable Secure Desktop check box indicates whether CSD is enabled.

Step 2 Check **Enable Secure Desktop** to enable CSD or uncheck **Enable Secure Desktop** to disable CSD.

Step 3 Close ASDM. A window displays the following message:

```
The configuration has been modified. Do you want to save the running configuration to
flash memory?
```

Step 4 Click **Save**. ASDM saves the configuration and closes.

Host Scan and CSD Upgrades and Downgrades

The ASA automatically distributes the enabled Host Scan package to the endpoint whether that package is the standalone Host Scan package, the package included with AnyConnect Secure Mobility Client, or the package included with Cisco Secure Desktop. If the endpoint has an older version of the Host Scan package installed, the package on the endpoint gets upgraded; if the endpoint has a newer version of the Host Scan package, the endpoint package gets downgraded.

Determining the Host Scan Image Enabled on the ASA

Open ASDM and select **Configuration > Remote Access VPN > Host Scan Image**.

If there is a Host Scan image designated in the Host Scan Image location field, and the Enable HostScan/CSD box is checked, the version of that image is the Host Scan version being used by the ASA.

If the Host Scan Image filed is empty, and the Enable HostScan/CSD box is checked, select **Configuration > Remote Access VPN > Secure Desktop Manager**. The version of CSD in the Secure Desktop Image Location field is the Host Scan version being used by the ASA.

Uninstalling Host Scan

Uninstalling the Host Scan Package

Uninstalling the Host Scan package removes it from view on the ASDM interface and prevents the ASA from deploying it even if Host Scan or CSD is enabled. Uninstalling Host Scan does not delete the Host Scan package from the flash drive.

Use this procedure to uninstall Host Scan on the security appliance:

Step 1 Open ASDM and select **Configuration > Remote Access VPN > Host Scan Image**.

Step 2 In the Host Scan Image pane, click **Uninstall**. ASDM removes the text from the Location text box.

Step 3 Click **Save**.

Uninstalling CSD from the ASA

Uninstalling Cisco Secure Desktop (CSD) **removes the CSD configuration file, data.xml, from the desktop directory on the flash card**. If you want to retain the file, copy it using an alternative name or download it to your workstation before you uninstall CSD.

Use this procedure to uninstall CSD on the security appliance:

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Secure Desktop Manager > Setup**.

ASDM opens the Setup pane (Figure 5-3).

Step 2 Click **Uninstall**.

A confirmation window displays the following message:

```
Do you want to delete disk0:/csd_<n>.<n>.*.pkg and all CSD data files?
```

Step 3 Click **Yes**.

ASDM removes the text from the Location text box and removes the Secure Desktop Manager menu options below Setup.

Step 4 Close ASDM. A window displays the following message:

```
The configuration has been modified. Do you want to save the running configuration to
flash memory?
```

Step 5 Click **Save**. ASDM saves the configuration and closes.

Assigning AnyConnect Posture Module to a Group Policy

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies.**

Step 2 In the Group Policies panel, click **Add** to create a new group policy or select the group policy to which you want to assign the Host Scan package and click **Edit**.

Step 3 In the Edit Internal Group Policy panel, expand the **Advanced** navigation tree on the left side of the panel and select **AnyConnect Client**.

Step 4 Uncheck the Optional Client Modules to Download **Inherit** checkbox.

Step 5 In the Optional Client Modules to Download drop down menu, check the AnyConnect Posture Module and click **OK**.

Step 6 Click **OK**.

Host Scan Logging

Host Scan logs to the Event Viewer on Windows platforms, and syslog on non-windows platforms. In the Event Viewer all logs will be in their own “Cisco AnyConnect Secure Mobility Client Posture” folder.

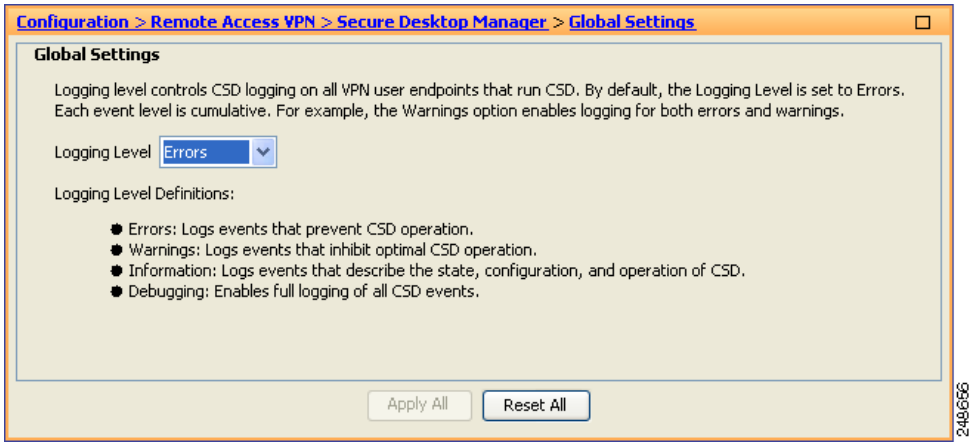
Configuring the Logging Level for All Posture Module Components

By default, components in the posture module log "Error" severity level events. Use these instructions to change the logging severity level for all components of the posture module.

The posture module installs the cscan.log file in the user's home folder. The cscan.log file shows only the entries from the last VPN session. Each time the user connects to the ASA, Host Scan overwrites the entries in this file with new logging data.

To view or change the posture logging level:

Step 1 From the ASDM interface select **Configuration > Remote Access VPN > Secure Desktop Manager > Global Settings**. The Global Settings panel opens.



Step 2 Set the **Logging Level** using the Logging Level Definitions in the panel as a guide.

Step 3 Click **Apply All** to save the changes to the running configuration.

Note If Host Scan is disabled for a particular connection profile, Host Scan logging does not occur for users of that connection profile.

Posture Module Log Files and Locations

Posture module components output up to three logs based on your operating system, privilege level, and launching mechanism (Web Launch or AnyConnect):

- cstub.log - Captures logging when AnyConnect web launch is used.
- libcsd.log - Created by the AnyConnect thread that uses the Host Scan API. Debugging entries would be made in this log depending on the logging level configuration.
- cscan.log - Created by the scanning executable (cscan.exe) and is the main log for posture and Host Scan. Debugging entries would be made in this log depending on the logging level configuration.

The posture module puts these log files in the user's home folder. The location is dependent on the operating system and VPN method.

Cisco Technical Assistant Center (TAC) uses these log files to debug problems if the need arises. You will not need to review these files. Should Cisco TAC need them, you will be asked to provide them with a DART Bundle. The DART utility will collect all the necessary AnyConnect configuration and log files and store them in a compressed file which you will then send to TAC. See the "Using DART to Gather Troubleshooting Information" section on page 12-3 for more information about DART.

Using a BIOS Serial Number in a Lua Expression

Host Scan can retrieve the BIOS serial number of a host. You can use a Dynamic Access Policy (DAP) to allow or prevent a VPN connection to the ASA based on that BIOS serial number.

Expressing the BIOS in a Lua Expression

This is the Lua logical expression you can use in the **Advanced** field of the **Edit Dynamic Access Policy** screen of ASDM:

endpoint.device.id=***BIOSSerialNumber***

Where ***BIOSSerialNumber*** represents the BIOS serial number of the hardware device attempting to connect to the ASA. This string is a variable length string and is, generally, OS-specific.

Specifying the BIOS as a DAP Endpoint Attribute

Step 1 Log on to ASDM.

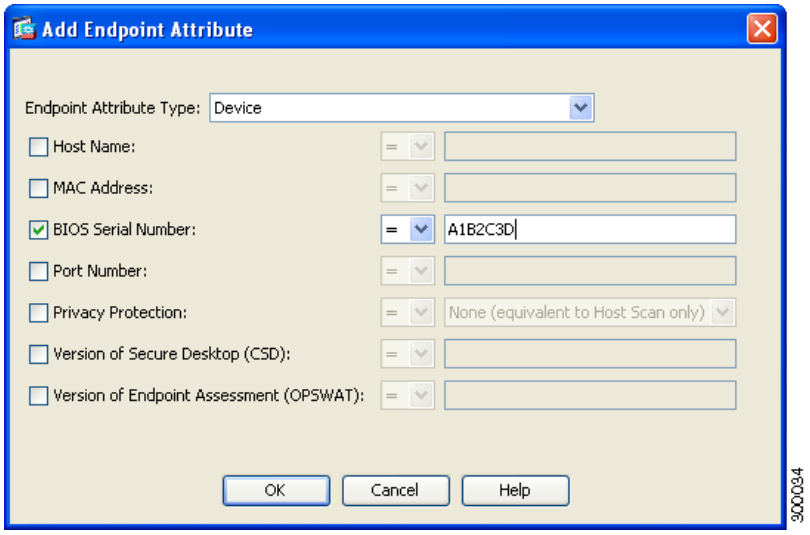
Step 2 Select **Configuration > Remote Access VPN > Network (Client) Access** or **Clientless SSL VPN Access > Dynamic Access Policies**.

Step 3 In the Configure Dynamic Access Policies panel, click **Add** or **Edit** to configure BIOS as a DAP Endpoint Attribute.

Step 4 To the right of the Endpoint ID table, click **Add**.

Step 5 In the Endpoint Attribute Type field, select **Device**.

Step 6 Check the **BIOS Serial Number** checkbox, select **=** (equals) or **!=** (not equals), and enter the BIOS number in the BIOS Serial Number field.



Step 7 Click **OK** to save changes in the Endpoint Attribute dialog box.

Step 8 Click **OK** to save your changes to the Edit Dynamic Access Policy.

Step 9 Click **Apply** to save your changes to the Dynamic Access Policy.

Step 10 Click **Save**.

How to Obtain BIOS Serial Numbers

These resources explain how to obtain the BIOS Serial number on various endpoints.

- Windows: http://support.microsoft.com/kb/558124
- Mac OS X: http://support.apple.com/kb/ht1529
- Linux: Use this command:

```
/usr/bin/hal-get-property --udi /org/freedesktop/Hal/devices/computer --key
system.hardware.serial
```

Other Important Documentation

Once Host Scan gathers the posture credentials from the endpoint computer, you will need to understand subjects like, configuring prelogin policies, configuring dynamic access policies, and using Lua expressions to make use of the information.

These topics are covered in detail in these documents:

- Cisco Secure Desktop Configuration Guides
- Cisco Adaptive Security Device Manager Configuration Guides
- List of Antivirus, Antispyware, and Firewall Applications supported by Host Scan