Configuring AnyConnect Host Scan

Configuration > Remote Access VPN > Host Scan Image

The AnyConnect Posture Module provides the AnyConnect Secure Mobility Client the ability to identify the operating system, anti-virus, anti-spyware, and firewall software installed on the host. The Host Scan application gathers this information.

Using the secure desktop manager tool in the Adaptive Security Device Manager (ASDM), you can create a prelogin policy which evaluates the operating system, anti-virus, anti-spyware, and firewall software Host Scan identifies. 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.

The Host Scan support chart contains the product name and version information for the anti-virus, anti-spyware, and firewall applications you use in your prelogin policies. We deliver Host Scan and the Host Scan support chart, as well as other components, in the Host Scan package.

Starting with AnyConnect Secure Mobility Client, release 3.0, Host Scan is available separately from CSD. This means you can deploy Host Scan functionality without having to install CSD and you will be able to update your Host Scan support charts by upgrading the latest Host Scan package.

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

This chapter contains the following sections:

Host Scan Dependencies and System Requirements

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.

- SCEP authentication
- AnyConnect Telemetry Module

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)
- Windows Mobile

Licensing

These are the AnyConnect licensing requirements for the posture module:

- AnyConnect Premium for basic Host Scan.
- Advanced Endpoint Assessment license is required for
  - Remediation
  - Mobile Device Management

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

File	Description
hostscan-*version*.pkg	This file contains the Host Scan software as well as the Host Scan library and support charts.
anyconnect-NGC-win-*version*-k9.pkg	This package contains all the Cisco AnyConnect Secure Mobility Client features including the hostscan-*version*.pkg file.
csd_*version*-k9.pkg	This file contains all Cisco Secure Desktop features including Host Scan software as well as the Host Scan library and support charts. This method requires a separate license for Cisco Secure Desktop.

Installing and Enabling Host Scan on the ASA

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

- Installing or Upgrading Host Scan
- Enabling or Disabling a Host Scan
- Viewing the Host Scan Version Enabled on the ASA
- Uninstalling Host Scan
- Assigning AnyConnect Feature Modules to Group Policies

Installing or Upgrading Host Scan

Use this procedure to install or upgrade the Host Scan package and enable it using the command line interface for the ASA.

Prerequisites

- Log on to the ASA and enter global configuration mode. In global configuration mode, the ASA displays this prompt: hostname(config)#
- Upload the hostscan_version-k9.pkg file or anyconnect-NGC-win-version-k9.pkg file to the ASA.

Detailed Steps

	Command	Purpose
Step 1	**webvpn** **Example:** `ciscoasa(config)# webvpn`	Enter webvpn configuration mode.

Step 2	**csd hostscan image** path
	
	Example:
	`ASAName(webvpn)#csd hostscan image disk0:/hostscan-3.6.0-k9.pkg`
	`ASAName(webvpn)#csd hostscan image disk0:/anyconnect-NGC-win-3.0.0327-k9.pkg`
		Specify the path to the package you want to designate as the Host Scan image. You can specify a standalone Host Scan package or an AnyConnect Secure Mobility Client package as the Host Scan package.
		Note For all operating systems, Windows, Linux, and Mac OS X, customers need to upload the anyconnect-NGC-win-*version*-k9.pkg file in order for the endpoints to install Host Scan.

Step 3	**csd enable** **Example:** `ASAName(webvpn)#csd enable`	Enables the Host Scan image you designated in the previous step.

Step 4	`write memory`
	
	Example:
	`hostname(webvpn)# write memory`
		Saves the running configuration to flash.
		After successfully saving the new configuration to flash memory, you receive the message [OK].

Enabling or Disabling a Host Scan

These commands enable or disable an installed Host Scan image using the command line interface of the ASA.

Prerequisites

Log on to the ASA and enter global configuration mode. In global configuration mode, the ASA displays this prompt: hostname(config)#

Detailed Steps for Enabling Host Scan

	Command	Purpose
Step 1	**webvpn** **Example:** `ciscoasa(config)# webvpn`	Enter webvpn configuration mode.
Step 2	**csd enable** **Example:** ciscoasa(config)# **csd enable**	Enables the standalone Host Scan image or the Host Scan image in the AnyConnect Secure Mobility Client package if they have not been uninstalled from your ASA. If neither of those types of packages is installed and a CSD package is installed, this enables the Host Scan function in the CSD package.

Detailed Steps for Disabling Host Scan

	Command	Purpose
Step 1	**webvpn** **Example:** `ciscoasa(config)# webvpn`	Enter webvpn configuration mode.
Step 2	**no csd enable** **Example:** ciscoasa(config)# **no csd enable**	Disables Host Scan for all installed Host Scan packages. **Note** Before you uninstall the enabled Host Scan image, you must first disable Host Scan using this command.

Viewing the Host Scan Version Enabled on the ASA

Use this procedure to determine the enabled Host Scan version using ASA's command line interface.

Prerequisites

Log on to the ASA and enter privileged exec mode. In privileged exec mode, the ASA displays this prompt: **hostname#**

Command	Purpose

`show webvpn csd hostscan`
 	
Example:
`ciscoasa# show webvpn csd hostscan`
	Show the version of Host Scan enabled on the ASA.

Uninstalling Host Scan

Uninstalling 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.

Prerequisites

Log on to the ASA and enter global configuration mode. In global configuration mode, the ASA displays this prompt: **hostname(config)#.**

Detailed Steps

	Command	Purpose
Step 1	**`webvpn`** **Example:** `ciscoasa(config)# webvpn`	Enter webvpn configuration mode.
Step 2	**`no csd enable`** **Example:** `ASAName(webvpn)#no csd enable`	Disables the Host Scan image you want to uninstall.
Step 3	**`no csd hostscan image`** `path` **Example:** hostname(webvpn)#no csd hostscan image disk0:/hostscan-3.6.0-k9.pkg `hostname(webvpn)#no csd hostscan image disk0:/anyconnect-NGC-win-3.0.0327-k9.pkg`	Specifies the path to the Host Scan image you want to uninstall. A standalone Host Scan package or an AnyConnect Secure Mobility Client package may have been designated as the Host Scan package.

Step 4	`write memory`
	
	Example:
	`hostname(webvpn)# write memory`
		Saves the running configuration to flash.
		After successfully saving the new configuration to flash memory, you receive the message [OK].

Assigning AnyConnect Feature Modules to Group Policies

This procedure associates AnyConnect feature modules with a group policy. When VPN users connect to the ASA, the ASA downloads and installs these AnyConnect feature modules to their endpoint computer.

Prerequisites

Log on to the ASA and enter global configuration mode. In global configuration mode, the ASA displays this prompt: **hostname(config)#**

Detailed Steps

	Command	Purpose
Step 1	**group-policy** *name* **internal** **Example:** `hostname(config)# group-policy PostureModuleGroup internal`	Adds an internal group policy for Network Client Access
Step 2	**group-policy** *name* **attributes** **Example:** `hostname(config)# group-policy PostureModuleGroup attributes`	Edits the new group policy. After entering the command, you receive the prompt for group policy configuration mode, **hostname(config-group-policy)#**.

Step 3	`webvpn`
	
	Example:
	`hostname(config-group-policy)# webvpn`
		Enters group policy webvpn configuration mode. After you enter the command, the ASA returns this prompt:
		
		hostname(config-group-webvpn)#

	Command	Purpose
Step 4	`hostname(config-group-webvpn)# anyconnect modules value` AnyConnect Module *Name* **Example:** `hostname(config-group-webvpn)# anyconnect modules value websecurity,telemetry,posture`	Configures the group policy to download AnyConnect feature modules for all users in the group. The value of the anyconnect module command can contain one or more of the following values. When specifying more than one module, separate the values with a comma. **value** — **AnyConnect Module Name** **dart** — AnyConnect DART (Diagnostics and Reporting Tool) **nam** — AnyConnect Network Access Manager **vpngina** — AnyConnect SBL (Start Before Logon) **websecurity** — AnyConnect Web Security Module **telemetry** — AnyConnect Telemetry Module **posture** — AnyConnect Posture Module **none** — Used by itself to remove all AnyConnect modules from the group policy. To remove one of the modules, re-send the command specifying only the module values you want to keep. For example, this command **removes** the websecurity module: `hostname(config-group-webvpn)# anyconnect modules value telemetry,posture`

Step 5	`write memory`
	
	Example:
	`hostname(config-group-webvpn)# write memory`
		Saves the running configuration to flash.
		
		After successfully saving the new configuration to flash memory, you receive the message [OK] and the ASA returns you to this prompt:
		
		hostname(config-group-webvpn)#

Other Important Documentation Addressing Host Scan

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

See also the Cisco *AnyConnect Secure Mobility Client Administrator Guide, Release 3.0* for more information about how Host Scan works with AnyConnect clients.