



AnyConnect HostScan

The AnyConnect Posture Module provides the AnyConnect Secure Mobility Client the ability to identify the operating system, anti-malware and firewall software installed on the host. The HostScan application gathers this information. Posture assessment requires HostScan to be installed on the host.

- [Prerequisites for HostScan, on page 1](#)
- [Licensing for HostScan, on page 1](#)
- [HostScan Packaging, on page 2](#)
- [Install or Upgrade HostScan, on page 2](#)
- [Enable or Disable HostScan, on page 3](#)
- [View the HostScan Version Enabled on the ASA, on page 3](#)
- [Uninstall HostScan, on page 4](#)
- [Assign AnyConnect Feature Modules to Group Policies, on page 5](#)
- [HostScan Related Documentation, on page 6](#)

Prerequisites for HostScan

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

Refer to [Supported VPN Platforms, Cisco ASA Series](#) for what operating systems are supported for posture module installation.

Licensing for HostScan

These are the AnyConnect licensing requirements for the HostScan:

- AnyConnect Apex

- AnyConnect VPN Only

HostScan Packaging

You can load the HostScan package on to the ASA as a standalone package: **hostscan-version.pkg**. This file contains the HostScan software as well as the HostScan library and support charts.

Install or Upgrade HostScan

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

Before you begin



Note

If you are attempting to upgrade to HostScan version 4.6.x or later from a 4.3.x version or earlier, you will receive an error message due to the fact that all existing AV/AS/FW DAP policies and LUA script(s) that you have previously established are incompatible with HostScan 4.6.x or greater.

There is a one time migration procedure that must be done to adapt your configuration. This procedure involves leaving this dialog box to migrate your configuration to be compatible with HostScan 4.4.x before saving this configuration. Abort this procedure and refer to the [AnyConnect HostScan 4.3.x to 4.6.x Migration Guide](#) for detailed instructions. Briefly, migration involves navigating to the ASDM DAP policy page to review and manually deleting the incompatible AV/AS/FW attributes, and then reviewing and rewriting LUA scripts.

- 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 to the ASA.

Procedure

Step 1 Enter webvpn configuration mode.

Example:

```
hostname(config)# webvpn
```

Step 2 Specify the path to the package you want to designate as the HostScan image. You can specify a standalone HostScan package or an AnyConnect Secure Mobility Client package as the HostScan package.

hostscan image path

Example:

```
ASAName(webvpn)#hostscan image disk0:/ hostscan_4.9.00086-k9.pkg
```

Step 3 Enable the HostScan image you designated in the previous step.

Example:

```
ASAName (webvpn) #hostscan enable
```

- Step 4** Save the running configuration to flash. After successfully saving the new configuration to flash memory, you receive the message [OK].

Example:

```
hostname (webvpn) # write memory
```

Step 5

Enable or Disable HostScan

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

Before you begin

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

Procedure

-
- Step 1** Enter webvpn configuration mode.

Example:

```
webvpn
```

- Step 2** Enable the standalone HostScan image if it has not been uninstalled from your ASA.

```
hostscan enable
```

- Step 3** Disable HostScan for all installed HostScan packages.

Note Before you uninstall the enabled HostScan image, you must first disable HostScan using this command.

```
no hostscan enable
```

View the HostScan Version Enabled on the ASA

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

Before you begin

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

Procedure

Show the version of HostScan enabled on the ASA.

```
show webvpn hostscan
```

Uninstall HostScan

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

Before you begin

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

Procedure

Step 1 Enter webvpn configuration mode.

```
webvpn
```

Step 2 Disable the HostScan image you want to uninstall.

```
no hostscanenable
```

Step 3 Specify the path to the HostScan image you want to uninstall. A standalone HostScan package may have been designated as the HostScan package.

```
no hostscan image path
```

Example:

```
hostname (webvpn) #no hostscan image disk0:/hostscan_4.9.00086-k9.pkg
```

Step 4 Save the running configuration to flash. After successfully saving the new configuration to flash memory, you receive the message [OK].

```
write memory
```

Assign 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.

Before you begin

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

Procedure

-
- Step 1** Adds an internal group policy for Network Client Access
- group-policy name internal**
- Example:**
- ```
hostname (config) # group-policy PostureModuleGroup internal
```
- Step 2** Edit the new group policy. After entering the command, you receive the prompt for group policy configuration mode, `hostname(config-group-policy)#`.
- group-policy name attributes**
- Example:**
- ```
hostname (config) # group-policy PostureModuleGroup attributes
```
- Step 3** Enter group policy webvpn configuration mode. After you enter the command, the ASA returns this prompt: `hostname(config-group-webvpn)#`
- webvpn**
- Step 4** Configure the group policy to download AnyConnect feature modules for all users in the group.
- anyconnect modules value AnyConnect Module Name**

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/Feature Name
dart	AnyConnect DART (Diagnostics and Reporting Tool)
vpngina	AnyConnect SBL (Start Before Logon)
websecurity	AnyConnect Web Security Module
telemetry	AnyConnect Telemetry Module
posture	AnyConnect Posture Module
nam	AnyConnect Network Access Manager

value	AnyConnect Module/Feature Name
none	Used by itself to remove all AnyConnect modules from the group policy.
profileMgmt	AnyConnect Management Tunnel VPN

Example:

```
hostname(config-group-webvpn)# anyconnect modules value websecurity,telemetry,posture
```

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 Save 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)#`

write memory

HostScan Related Documentation

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

These topics are covered in detail in these documents: [Cisco Adaptive Security Device Manager Configuration Guides](#). See also the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for more information about how HostScan works with AnyConnect clients.