# **Upgrade from HostScan to Secure Firewall Posture on Windows**

# Contents

Introduction
<u>Prerequisites</u>
Requirements
Components Used
<u>Network Diagram</u>
Configurations
<u>Upgrade</u>
Method 1. Deploy on ASA Side
Step 1. Download Image File
Step 2. Transfer Image File to ASA Flash
Step 3. Specify Image File from ASA CLI
Step 4. Automatically Upgrade
Step 5. Confirm New Version
Method 2. Install on Client Side
Step 1. Download Installer
Step 2. Transfer Installer to Target Device
Step 3. Run Installer
Step 4. Confirm New Version
Frequently Asked Questions (FAQ)
Related Information

# Introduction

This document describes the procedure to upgrade from HostScan to Secure Firewall Posture (formerly HostScan) on Windows.

# Prerequisites

## Requirements

Cisco recommends that you have knowledge of this topic:

Configuration of Cisco Anyconnect and Hostscan

#### **Components Used**

The information in this document is based on these software and hardware versions:

- Cisco Adaptive Security Virtual Appliance 9.18 (4)
- Cisco Adaptive Security Device Manager 7.20 (1)
- Cisco AnyConnect Secure Mobility Client 4.10.07073

- AnyConnect HostScan 4.10.07073
- Cisco Secure Client 5.1.2.42
- Secure Firewall Posture 5.1.2.42

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## **Network Diagram**

This image shows the topology that is used for the example of this document.



Network Diagram

# **Configurations**

This is the minimal configuration in ASA CLI.

```
tunnel-group dap_test_tg type remote-access
tunnel-group dap_test_tg general-attributes
default-group-policy dap_test_gp
tunnel-group dap_test_tg webvpn-attributes
group-alias dap_test enable
group-policy dap_test_gp internal
group-policy dap_test_gp attributes
vpn-tunnel-protocol ssl-client
address-pools value ac_pool
webvpn
anyconnect keep-installer installed
always-on-vpn profile-setting
ip local pool ac_pool 172.16.1.11-172.16.1.20 mask 255.255.255.0
webvpn
enable outside
hostscan image disk0:/hostscan_4.10.07073-k9.pkg
hostscan enable
anyconnect image disk0:/anyconnect-win-4.10.07073-webdeploy-k9.pkg 1
anyconnect enable
```

ASAv

# Upgrade

This document provides an example of how to upgrade from AnyConnect HostScan version 4.10.07073 to Secure Firewall Posture version 5.1.2.42, in conjunction with the upgrade of Cisco Secure Client (Formerly Cisco AnyConnect Secure Mobility Client).



**Note**: Cisco recommend that you run the most recent version of Secure Firewall Posture (which is the same as the version of Cisco Secure Client).

#### Method 1. Deploy on ASA Side

#### Step 1. Download Image File

Download the image files for Cisco Secure Client and Secure Firewall Posture from the <u>Software</u> <u>Download</u>.

- Cisco Secure Client : cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg
- Secure Firewall Posture : secure-firewall-posture-5.1.2.42-k9.pkg

#### Step 2. Transfer Image File to ASA Flash

In this example, use ASA CLI to transfer the image files from an HTTP server to ASA flash.

```
copy http://l.x.x.x/cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg flash:/
copy http://l.x.x.x/secure-firewall-posture-5.1.2.42-k9.pkg flash:/
```

```
ciscoasa# show flash: | in secure
139 117011512 Mar 26 2024 08:08:56 cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg
140 92993311 Mar 26 2024 08:14:16 secure-firewall-posture-5.1.2.42-k9.pkg
```

#### Step 3. Specify Image File from ASA CLI

Specify the new image files used for Cisco Secure Client connection on ASA CLI.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# hostscan image disk0:/secure-firewall-posture-5.1.2.42-k9.pkg
ciscoasa(config-webvpn)# anyconnect image disk0:/cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg
```

#### Step 4. Automatically Upgrade

Both Cisco Secure Client and Secure Firewall Posture can be updated automatically the next time the client connects.

Secure Firewall Posture module is automatically upgraded as show in the image.

## Cisco Secure Client - Downloader



The Cisco Secure Client - Downloader is installing Cisco Secure Client - Secure Firewall Posture 5.1.2.42. Please wait...

```
Automatically Upgrade
```

**Step 5. Confirm New Version** 

Confirm that Cisco Secure Client and Secure Firewall Posture are successfully upgraded as show in the image.



New Version

#### Method 2. Install on Client Side

#### Step 1. Download Installer

Download the installer from Software Download.

• cisco-secure-client-win-5.1.2.42-predeploy-k9.zip

#### **Step 2. Transfer Installer to Target Device**

Transfer the downloaded installer to the target device using methods such as FTP (File Transfer Protocol), a USB drive, or other methods.

#### Step 3. Run Installer

On the target device, extract the compressed files and run Setup.exe.

Profiles	③ Cisco Secure Client Install Selector - □ ×
🚞 Setup	Select the Cisco Secure Client 5.1.2.42 modules you wish to install:
cisco-secure-client-win-1.182.3-thousandeyes-predeploy-k9.msi	S Core & AnyConnect VPN
cisco-secure-client-win-5.1.2.42-core-vpn-predeploy-k9.msi	Start Before Login
cisco-secure-client-win-5.1.2.42-dart-predeploy-k9.msi	Network Access Manager
cisco-secure-client-win-5.1.2.42-iseposture-predeploy-k9.msi	Secure Firewall Posture     Network Visibility Module
cisco-secure-client-win-5.1.2.42-nam-predeploy-k9.msi	🖬 Umbrella
cisco-secure-client-win-5.1.2.42-nvm-predeploy-k9.msi	ISE Posture
cisco-secure-client-win-5.1.2.42-posture-predeploy-k9.msi	■ ThousandEyes     ■
Cisco-secure-client-win-5.1.2.42-predeploy-k9.zip	Zero Trust Access
cisco-secure-client-win-5.1.2.42-sbl-predeploy-k9.msi	Select All
cisco-secure-client-win-5.1.2.42-umbrella-predeploy-k9.msi	Diagnostic And Reporting Tool
cisco-secure-client-win-5.1.2.5191-zta-predeploy-k9.msi	Lock Down Component Services
🕲 Setup.exe	Install Selected
setup.hta	

Run Installer

## Step 4. Confirm New Version

Confirm that Cisco Secure Client and Secure Firewall Posture are successfully upgraded as show in the image.

🕲 Cisco Secu	ire Client	- 🗆 X	O Cisco Secure Client		×
00:00:09	AnyConnect VP% Connected to 192.168.1.1. 192.168.1.1	V Disconnect JPv4	Copyright 2004 - 2023 Cisco Sys Copyright 2004 - 2023 Cisco Sys Terms of service Privacy statement Notices and disclaimers Third-party licenses and notices	lient tems, Inc. All Rights Reserved	
			Installed Modules: Name AnyConnect VPN Customer Experience Feedback Secure Firewall Posture Umbrella	Version 5.1.2.42 5.1.2.42 5.1.2.42 5.1.2.42	Close

# **Frequently Asked Questions (FAQ)**

# **Q** : If the version of Secure Firewall Posture (formerly HostScan) specified on the ASA side is older than the version installed on the terminal, does it still operate correctly ?

A: Yes. This is an example of operational verification after upgrading HostScan version 4.10.07073 to Secure Firewall Posture version 5.1.2.42 on a specific terminal, with DAP (<u>Scenario3. Multiple DAPs</u> (<u>Action : Continue</u>) are matched) configured in HostScan 4.10.07073.



**Caution**: The behavior can depend on the version of Secure Firewall Posture/Cisco Secure Client, so ensure to check the latest release notes for each version.

Image version configured on ASA side:

Image version on target device :

O Cisco Secure Client

# Secure Client

© Copyright 2004 - 2023 Cisco Systems, Inc. All Rights Reserved



#### Installed Modules:

Name	Version	^
AnyConnect VPN	5.1.2.42	
Customer Experience Feedback	5.1.2.42	
Secure Firewall Posture	5.1.2.42	
Umbrella	5.1.2.42	~

Close

Image Version on Device

Example of Cisco Secure Client connection :

 $\times$ 

Orisco Secure Client − □ ×	S Cisco Secure Client   192.168.1.1 X
AnyConnect VPI: Please enter your username and password. 192.168.1.1 V Connect	Please enter your username and password. Group: dap_test  v Username: cisco Password: *******
Cisco Secure Client X Security policies were applied to your session, access to some resources may be blocked. Your system administrator provided the following information to help you understand and remedy the security conditions: 01_dap_test 02_dap_test	OK Cancel  Cisco Secure Client  AnyConnect VPR Connected to 192.168.1.1.  192.168.1.1  Disconnect  00:00:30  Pv4
OK	

Cisco Secure Client Connection

#### **Q** : Does Cisco Secure Client 5.x work properly in combination with HostScan 4.x?

A : No. The combination of Cisco Secure Client 5.x and HostScan 4.x is not supported.

# **Q** : When upgrading from HostScan 4.x to Secure Firewall Posture 5.x, is it possible to upgrade only on certain devices ?

A : Yes. You can upgrade specific devices using the mentioned Method 2.

## **Related Information**

• Cisco Technical Support & Downloads