Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.10

First Published: 2023-05-04

Last Modified: 2024-02-26

Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.10

These release notes provide information for AnyConnect Secure Mobility Client on Windows, macOS, and Linux. An always-on intelligent VPN helps AnyConnect devices to automatically select the optimal network access point and adapt its tunneling protocol to the most efficient method.

Download the Latest Version of AnyConnect

Before you begin

To download the latest version of AnyConnect, you must be a registered user of Cisco.com.

Procedure

Step 1 Follow this link to the AnyConnect Secure Mobility Client product support page:

http://www.cisco.com/en/US/products/ps10884/tsd_products_support_series_home.html.

Step 2 Log in to Cisco.com.

Step 3 Click **Download Software**.

Step 4 Expand the **Latest Releases** folder and click the latest release, if it is not already selected.

Step 5 Download AnyConnect Packages using one of these methods:

- To download a single package, find the package you want to download and click **Download**.
- To download multiple packages, click **Add to cart** in the package row and then click **Download Cart** at the top of the Download Software page.

Step 6 Read and accept the Cisco license agreement when prompted.

Step 7 Select a local directory in which to save the downloads and click **Save**.

Step 8 See the AnyConnect Secure Mobility Client Administrator Guide, Release 4.x.

AnyConnect Secure Mobility Client Package Filenames for Web Deployment

OS	AnyConnect Web-Deploy Package Names
Windows	anyconnect-win-*version*-webdeploy-k9.pkg
macOS	anyconnect-macos-*version*-webdeploy-k9.pkg
Linux (64-bit)*	anyconnect-linux64-*version*-webdeploy-k9.pkg

* Web deployment for RPM&DEB installation is not currently supported.

AnyConnect Package Filenames for Predeployment

OS	AnyConnect Predeploy Package Name
Windows	anyconnect-win-*version*-predeploy-k9.zip
macOS	anyconnect-macos-*version*-predeploy-k9.dmg
Linux (64-bit)	(for script installer) anyconnect-linux64-*version*-predeploy-k9.tar.gz (for RPM installer*) anyconnect-linux64-*version*-predeploy-rpm-k9.tar.gz (for DEB installer*) anyconnect-linux64-*version*-predeploy-deb-k9.tar.gz

*Modules provided with RPM and DEB installers: VPN, DART

Other files, which help you add additional features to AnyConnect, can also be downloaded.

AnyConnect 4.10.08029 New Features

This is a maintenance release that includes the following new features and support updates, and that resolves the defects described in AnyConnect 4.10.08029, on page 39:

- Windows 10 ARM64 is no longer supported.
- Dynamic Split Exclusions are supported for macOS AnyConnect based on CNAME DNS responses

Known Issues:

- CSCwj04530— Captive portal does not load in embedded browser on macOS12 in a specific scenario
- CSCwi99127— NVM: No support for Multihoming

AnyConnect 4.10.08025 New Features

This is a maintenance release that includes the following new features and support updates, and that resolves the defects described in AnyConnect 4.10.08025, on page 40:

- CSCur83728—When you have an EAP-FAST network and are authenticated by a certificate, choose *Disconnect from Network* for the *Smart Card Removal Policy*, so that the smartcard is removed when the network is disconnected.
- We have implemented a Network Access Manager addition to disable the setting of PMF IGTK until a Windows fix becomes available. Microsoft estimates that fixes for Windows 10 22H2 and Windows 11 21H2 (and later) should be available in the first half of calendar year 2024, which will allow you to set the IGTK from the Network Access Manager. Until then, you can disable the setting of PMF IGTK and allow a connection to a network configured to provide Protection of Management Frames (PMF). If the Windows fix is not yet available, and you can't avoid connecting to a network with PMF enabled, you need to modify the Windows registry editor by adding the following registry key as a DWORD and setting it as described to disable the use of IGTK by the Network Access Manager:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Network Access Manager\DisableIGTK
  set to 1
  ```

Note We strongly discourage against disabling the PMF IGTK unless necessary as it provides protection of wireless management frames.

- **Known Issues:**
  - CSCwh23924—After install of SBL/Network Access Manager, popup is not coming up asking for reboot
  - CSCwi53240—With 4.10 MR8 build, Network Visibility Module installation is failing on Ubuntu with latest kernel

AnyConnect 4.10.07073 New Features

This is a maintenance release that includes the following updates to the Umbrella Roaming Security Module and that resolves the defects described in AnyConnect 4.10.07073, on page 43:

- Improved reliability of DNS protection on some dual-stack IPv6 networks
- Fixed an issue where DNS security module would periodically lose protection or connectivity

AnyConnect 4.10.07062 New Features

This is an AnyConnect maintenance release that resolves a defect found in Windows (Intel) only. Refer to AnyConnect 4.10.07062, on page 43 for details on the resolved caveat.

AnyConnect 4.10.07061 New Features

This is a maintenance release that includes the following new features and support updates, and that resolves the defects described in AnyConnect 4.10.07061, on page 43 :

- WPA3 Enhanced Open (OWE) and WPA3 Personal (SAE) support added to Network Access Manager.

- 802.1x-SHA256 support added to the wireless Authentication Key Management suite for Network Access Manager (CSCwe38560).
- **Disable EDR Internet Check**—An ISE Posture Profile Editor option to skip the real-time transfer protocol check, and the definition check of the endpoint and detection response (EDR). If you have EDR products installed, you can use this option during system scan to perform an internet check.
- **Bypass Connect Upon VPN Session Timeout**—Allows you to bypass the connection retry that automatically occurs if a VPN session times out, while either Trusted Network Policy or Untrusted Network Policy are set to connect. This checkbox is added to the VPN Profile Editor (Preferences Part 2).

Known Issues:

(CSCwf21453)— Even when the client profile setting for **Retain VPN on Logoff** is *Enabled*, and **User Enforcement** is set to *Any User*, an established VPN connection is not being retained when the user signs out, and a different user logs in. The VPN connection is terminated with an error that "The VPN client agent has configured private-side proxy settings and is unable to restore public proxy settings during user logon."

AnyConnect 4.10.06090 New Features

This is a maintenance release that resolves the defects described in AnyConnect 4.10.06090, on page 47.

AnyConnect 4.10.06079 New Features

This is a maintenance release that includes the following new features and support updates, and that resolves the defects described in AnyConnect 4.10.06079, on page 48:

- Support for Captive Portal Detection in Network Access Manager.
- Adjusted the handling of the Authentication Timeout Values in the profile editor setting (CSCvx35970). Refer to *AnyConnect Profile Editor, Preferences (Part 2)* in the Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.10 for additional information.
- AnyConnect does not support DNS load balancing with external browser SAML authentication.

AnyConnect 4.10.05111 New Features

This is a maintenance release that resolves the defects described in AnyConnect 4.10.05111, on page 50.

AnyConnect 4.10.05095 New Features

This is a maintenance release that includes the following enhancements, and that resolves the defects described in AnyConnect 4.10.05095, on page 51.

- On Windows, the AnyConnect embedded browser now defaults to WebView2, as long as the WebView2 runtime is installed. If you need to revert back to the legacy embedded browser control, add **DWORD** registry value UseLegacyEmbeddedBrowser set to 1 to one of the following registry keys:

- (64-bit machine) Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cisco\Cisco AnyConnect Secure Mobility Client
- (32-bit machine) Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility Client
- (32-bit or 64-bit machine) Computer\HKEY_CURRENT_USER\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility Client

- An Umbrella issue that could cause a total Domain Name System failure on macOS 11 and later versions, requiring a reboot or removal of AnyConnect to resolve, has been fixed.
- Ability to create and upload a posture condition script for posture checks on an endpoint
  - Windows: PowerShell script (.ps1)
  - macOS: Shell script (.sh)
  - Linux: Shell script (.sh)

AnyConnect 4.10.05085 New Features

This is a maintenance release that includes the following support updates, and that resolves the defects described in AnyConnect 4.10.05085, on page 51:

- Added AnyConnect VPN interoperability for Apple AirDrop on Big Sur (macOS 11.x) and later versions. Such interoperability requires the enabling of IPv6 Local LAN split exclude tunneling in the VPN policy. (CSCwa59261)
- A UDID collision issue that occurred in the Network Visibility Module for Linux platforms has been fixed and is remedied after an upgrade to AnyConnect 4.10.05081.

AnyConnect 4.10.04071 New Features

This is a maintenance release that resolves the defects described in AnyConnect 4.10.04071, on page 53.

AnyConnect 4.10.04065 New Features

This is a maintenance release that includes the following features and support updates, and that resolves the defects described in AnyConnect 4.10.04065, on page 53:

- Support for an AnyConnect VPN SAML External Browser —As an optional add-on, you can choose the external browser package (external-sso-4.10.04065-webdeploy-k9.pkg) for AnyConnect VPN SAML External Browser use. When you use SAML as the primary authentication method for the AnyConnect VPN connection profile, you can choose for the AnyConnect client to use a local browser, instead of the AnyConnect embedded browser, when performing web authentication. With this feature, AnyConnect supports WebAuthN and any other SAML-based web authentication options, such as Single Sign On (SSO), biometric authentication, or other enhanced methods that are unavailable with embedded browser. For SAML external browser use, you must perform configuration using ASA release 9.17.1 (CLI), ASDM 7.17.1, or FDM 7.1 and later.

Refer to the following related documentation to set up this feature:

ASA Command Reference

anyconnect external-browser-pkg

external-browser

show webvpn anyconnect external-browser-pkg

Cisco ASA Series VPN ASDM Configuration Guide, 7.17.1

AnyConnect Connection Profile, Basic Attributes

AnyConnect VPN External Browser SAML Package

Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Release 7.1

Configure AAA for a Connection Profile

Cisco Firepower Management Center Device Configuration Guide, 7.1

Configure AAA Settings for Remote Access VPN

- (CSCvv92919) Support for Always-On VPN with external SAML identity provider—You must configure Always On as described in Use Always-On VPN with External SAML Identity Provider to allow the interoperability.
- (CSCvt99770) Support for DNS load balancing using SAML authentication on Windows.
- Updates to the Network Visibility Module collections: flow direction and additional logged-in users list
- (CSCvz99382) A fix to successfully upgrade Network Access Manager module using SCCM on Windows when ADVERTISE indicated that a lower version was present.
- (CSCvz77002) Linux support for RPM/DEB installers. See Limitations When Using RPM/DEB Installer, on page 22.

Known Issues

CSCwa22837—Intermittent acumbrellaagent crash is observed after AnyConnect upgrade (via ASA or Umbrella cloud)

CSCvz74755—Windows 11: Umbrella dashboard incorrectly displays OS version of Windows 11 client as 'Windows 10"

CSCvz17505—Windows: Umbrella agent crash due to .NET/CLR exception in acumbrella plugin library

AnyConnect 4.10.03104 New Features

This is a maintenance release that includes the following features and support updates, and that resolves the defects described in AnyConnect 4.10.03104, on page 55:

- OCSP Check (Linux only)—Allows the client to query the status of individual certificates in realtime, by making a request to the Online Certificate Status Protocol (OCSP) responder and parsing the OSCP response. This feature works only with PEM File Certificate Store. Refer to Root CA Conflict With Firefox NSS Store (Linux Only), on page 23.
- Before AnyConnect release 4.10.03104, Windows ADVERTISE installer action was not supported (CSCvw79615). With release 4.10.03104 and later, we provided a fix to successfully upgrade with

Windows ADVERTISE for those with a lower version of AnyConnect. Consider however that future upgrades could still fail if AnyConnect version 4.10.02086 or earlier (as opposed to 4.10.03104 or later) is advertised.

Known Issues

CSCvy92621—posture-asa: AC Windows version incorrectly shows Windows 10 instead of Windows 11 with HS 10.02067

CSCvy92676—Posture-ISE: Windows 11 OS is showing as Windows 10 professional instead of Windows 11

CSCvz74755—Windows 11: Umbrella dashboard incorrectly displays OS version of Windows 11 client as 'Windows 10"

CSCvz74132—macOS 12; acumbrellaagent crash seen after OS update to beta7

CSCvz17505—Windows: Umbrella agent crash due to .NET/CLR exception in acumbrella plugin library

AnyConnect 4.10.02086 New Features

This is a maintenance release that includes the following features and support updates, and that resolves the defects described in AnyConnect 4.10.02086, on page 56:

- Linux enhancements to include client certificate store (in AnyConnect Profile Editor, Preferences: Part 1 and AnyConnect Profile Editor, Certificate Enrollment), related AnyConnect Local Policy profile additions, and options for configuring VPN access with multiple or basic certificate authentication.
- Removal of Web Security module: https://www.cisco.com/c/en/us/products/security/cloud-web-security/eos-eol-notice-listing.html
- AnyConnect VPN interoperability with VMware Fusion on macOS Big Sur (CSCvy10495)—VMware Fusion virtual machine connectivity with an AnyConnect VPN tunnel running on a macOS Big Sur host is possible, provided that at least restricted local LAN split exclude tunneling is enabled on the VPN headend. Refer to Connectivity Issues with VM-based Subsystems in the troubleshooting chapter of the *AnyConnect Secure Mobility Client Administration Guide, Release 4.10* for further information. If a Fusion VM happens to be active during the AnyConnect installation (or an upgrade from version 4.10.01075 or earlier), either a reboot or Fusion restart is required after the AnyConnect installation, to restore the Fusion VM network connectivity. Subsequent AnyConnect upgrades do not require a reboot or restart.
- Limited extended support for Windows 7 will be provided for customers who have active Windows 7 extended support contracts with Microsoft. Although Cisco no longer performs substantial quality assurance testing on Windows 7, issues will be resolved whenever possible. Cisco highly recommends upgrading to the latest version of AnyConnect and Windows to take advantage of security enhancements.
- Native macOS arm64 Support—A single macOS installer supports both x86_64 and Apple Silicon (M1 chip) natively (without Rosetta). With this, all binaries moving forward will be Universal Binaries, including OPSWAT compliance modules. Therefore, OPSWAT compliance modules for macOS released prior to 4.3.1858.0 do not support Apple Silicon (M1 chip), where OPSWAT compliance modules 4.3.1858.0 and later support both Intel (x86_64) and Apple Silicon (M1 chip) devices. Due to this dynamic adoption in supporting Apple Silicon (M1 chip), macOS endpoints, using AnyConnect 4.10.02086 or later (and either ISE Posture or HostScan), must also upgrade their Posture Compliance Modules accordingly. The following chart outlines the minimum requirements:

AnyConnect Version	ISE Posture Compliance Library Minimum Version Supported/Required	HostScan Engine (.pkg) Minimum Version Supported/Required
• 4.10.01075 or earlier	macOS - all versions posted on CCO are supported. Most recently posted version is always suggested.	All versions posted on CCO are supported. Most recent HostScan .pkg that is posted is always suggested.
4.10.02086 or later	macOS - 4.3.1935.4353 or later is required	4.10.02086 or later is required. Most recent HostScan .pkg that is posted is always suggested.

Note The above arm64 support is unrelated to the ISE 3.1 release.

- Linux support for ISE Posture module.
- Expansion of trust verification for ISE within the AnyConnect Local Policy Preferences setting. For script remediation, it is mandatory that you configure SHA256 fingerprints of any certificate in the ISE certification chain to establish ISE trust. Refer to Local Policy Preferences in the administration guide.
- Script remediation messages were added to the ISE Posture Details and Cisco Secure Client Details.

Known Issues

CSCvz17505—Windows: Umbrella agent crash due to .NET/CLR exception in acumbrella plugin library

AnyConnect 4.10.01075 New Features

This is a maintenance release that includes the following features and support updates, and that resolves the defects described in AnyConnect 4.10.01075, on page 59:

- Added split DNS for split exclude tunneling (CSCuq89328)—When split DNS for split exclude tunneling is configured, specific DNS queries are sent outside the VPN tunnel, to a public DNS server. All othe DNS queries are tunneled to a VPN DNS server.
- Added support for interoperability with VM-based subsystems (CSCvw81982)—Windows Subsystem for Linux 2 (WSL2) had connectivity issues with AnyConnect VPN active on a Windows 10 host. We addressed this issue by enhancing support for Local LAN wildcard split exclude tunneling, specifically by allowing the limiting of the Local LAN split exclude to virtual adapter subnets. Refer to Connectivity Issues With VM-Based Subsystems in the troubleshooting chapter of the *AnyConnect Secure Mobility Client Administrator Guide, Release 4.10* for further information.

AnyConnect 4.10.00093 New Features

This is a major release that includes the following features and support updates, and that resolves the defects described in AnyConnect 4.10.00093, on page 62:

- Enhanced captive portal remediation now supported in macOS.

- Architecture improvement of downloader to address local platform security concerns.
- Ability to individually allow/disallow scripts, help, resources, or localization updates in Local Policy, while previously they were part of Allow Software Updates.
- CiscoSSL changes: enable EMS for only TLS, and disable EMS for DTLS.
- Operating system support has changed to eliminate older versions. Refer to AnyConnect Supported Operating Systems, on page 16.
- Revision to Linux requirements (due to Linux build toolchain/GTK migration). Refer to AnyConnect Support for Linux, on page 19.
- CSCvx78941—(Windows only) The product code signing certificate has been updated with a new certificate issued by DigiCert, instead of VeriSign. For code signatures to be verified and trusted by the OS, you must have the root certificate installed in the operating system's list of trusted root certificates. If Windows trusted root certificate updates are disabled, an AnyConnect install or upgrade may fail. If necessary, download and install the *CN = DigiCert Assured ID Root CA* root certificate from DigiCert into the Windows trusted root store (https://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt.pem).

AnyConnect HostScan Engine Update 4.10.08029 New Features

AnyConnect HostScan 4.10.08029 includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defects listed in HostScan 4.10.08029, on page 64.

AnyConnect HostScan Engine Update 4.10.08025 New Features

AnyConnect HostScan 4.10.08025 includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defects listed in HostScan 4.10.08025, on page 64.

AnyConnect HostScan Engine Update 4.10.07073 New Features

AnyConnect HostScan 4.10.07073 includes updates to the OPSWAT engine versions for Windows, macOS, and Linux.

AnyConnect HostScan Engine Update 4.10.07061 New Features

HostScan 4.10.07061 includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defects listed in HostScan 4.10.07061, on page 65.

AnyConnect HostScan Engine Update 4.10.06090 New Features

HostScan 4.10.06090 includes updates to the OPSWAT engine versions for Windows, macOS, and Linux.

AnyConnect HostScan Engine Update 4.10.06083 New Features

AnyConnect HostScan 4.10.06083 includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defects listed in HostScan 4.10.06083, on page 66.

AnyConnect HostScan Engine Update 4.10.06081 New Features

AnyConnect HostScan 4.10.06081 includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defects listed in HostScan 4.10.06081, on page 67.

AnyConnect HostScan Engine Update 4.10.05111 New Features

AnyConnect HostScan 4.10.05111 provides updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the bug listed in HostScan 4.10.05111, on page 68.

AnyConnect HostScan Engine Update 4.10.05095 New Features

AnyConnect HostScan 4.10.05095 provides updates to the OPSWAT engine versions for Windows, macOS, and Linux.

AnyConnect HostScan Engine Update 4.10.05085 New Features

AnyConnect HostScan 4.10.05085 includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defects listed in HostScan 4.10.05085, on page 68.

AnyConnect HostScan Engine Update 4.10.04071 New Features

AnyConnect HostScan 4.10.04071 includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defects listed in HostScan 4.10.04071, on page 68.

AnyConnect HostScan Engine Update 4.10.04065 New Features

AnyConnect HostScan 4.10.04065 includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defects listed in HostScan 4.10.04065, on page 69.

AnyConnect HostScan Engine Update 4.10.03104 New Features

AnyConnect HostScan 4.10.03104 includes updates to the OPSWAT engine versions for Windows, macOS, and Linux and resolves the defects listed in HostScan 4.10.03104, on page 69.

AnyConnect HostScan Engine Update 4.10.02089 New Features

AnyConnect HostScan 4.10.02089 includes updates to the OPSWAT engine versions for Windows, macOS, and Linux, and resolves the defect listed in HostScan 4.10.02089, on page 70. This release is only for the HostScan module.

AnyConnect HostScan Engine Update 4.10.02086 New Features

AnyConnect HostScan 4.10.02086 resolves the defects listed in HostScan 4.10.02086, on page 70.

AnyConnect HostScan Engine Update 4.10.01094 New Features

AnyConnect HostScan 4.10.01094 includes updates to the OPSWAT engine versions for Windows, macOS, and Linux, and resolves the defect listed in HostScan 4.10.01094, on page 70. This release is only for the HostScan module.

AnyConnect HostScan Engine Update 4.10.01075 New Features

AnyConnect HostScan 4.10.01075 includes updates to the HostScan module and resolves the defects listed in HostScan 4.10.01075, on page 71.

AnyConnect HostScan Engine Update 4.10.00093 New Features

AnyConnect HostScan 4.10.00093 includes updates to the HostScan module and resolves the defects listed in HostScan 4.10.00093, on page 71.

Refer to AnyConnect 4.10.00093 New Features, on page 8 for an important change to the code signing certificate that could impact VPN installation or upgrade.

System Requirements

This section identifies the management and endpoint requirements for this release. For endpoint OS support and license requirements for each feature, see AnyConnect Features, Licenses, and OSs.

Cisco cannot guarantee compatibility with other VPN third-party clients.

Changes to the AnyConnect Profile Editor

You must install Java, version 8 or higher, before launching the profile editor. AnyConnect Profile Editor supports OpenJDK and also Oracle Java. For certain OpenJDK builds, Profile Editor may fail to launch when the JRE path cannot be determined. Navigate to the installed JRE path where you will be prompted to properly launch the Profile Editor.

SAML Requirements

Follow the guidelines below when using SAML:

- For AnyConnect VPN SAML embedded browser

  Safari update 14.1.2 (or later) is required: contains an updated Webkit version, which resolves various behaviors

- For AnyConnect VPN SAML external browser

  AnyConnect release 4.10.04065 (or later)

  ASA 9.17.1/ASDM 7/7/1 (or later)

  FDM 7.1 (or later)

ISE Requirements for AnyConnect

- **Warning!**

  Incompatibility Warning: If you are an Identity Services Engine (ISE) customer running 2.0 (or later), you must read this before proceeding!

  The ISE RADIUS has supported TLS 1.2 since release 2.0; however, there is a defect in the ISE implementation of EAP-FAST using TLS 1.2, tracked by CSCvm03681. The defect has been fixed in the 2.4p5 release of ISE. The fix will be made available in future hot patches for supported releases of ISE.

  If Network Access Manager 4.7 (and later) is used to authenticate using EAP-FAST with any ISE releases that support TLS 1.2 prior to the above releases, the authentication will fail, and the endpoint will not have access to the network.

- ISE 2.6 (and later) with AnyConnect 4.7MR1 (and later) supports IPv6 non-redirection flows (using stage 2 discovery) on wired and VPN flows.
- AnyConnect temporal agent flows are working on IPv6 networks based on network topology. ISE supports multiple ways of IPv6 configuration on a network interface (for example, eth0/eth1).
- IPv6 networks with regards to ISE posture flows have the following limitations: [IPv6] ISE posture discovery is in infinite loop due to specific type of network adapters (for example, Microsoft Teredo virtual adapter) (CSCvo36890).
- ISE 2.0 is the minimum release capable of deploying AnyConnect software to an endpoint and posturing that endpoint using the new ISE Posture module in AnyConnect 4.0 and later.
- ISE 2.0 can only deploy AnyConnect release 4.0 and later. Older releases of AnyConnect must be web deployed from an ASA, predeployed with an SMS, or manually deployed.
- If you are installing or updating the AnyConnect ISE Posture module, the package and modules configured on ASA must be the same as the ones configured on ISE. VPN is always upgraded when other modules are upgraded, and a VPN module upgrade is not allowed from ISE when the tunnel is active.

ISE Licensing Requirements

To deploy AnyConnect from an ISE headend and use the ISE Posture module, a Cisco ISE Premier License is required on the ISE Administration node. For detailed ISE license information, see the *Cisco ISE Licenses* chapter of the Cisco Identity Services Engine Admin Guide.

Secure Firewall ASA Requirements for AnyConnect

Minimum ASA/ASDM Release Requirements for Specified Features

- You must upgrade to Secure Firewall ASA 9.10.1 (or later) and ASDM 7.10.1 (or later) to use DTLSv1.2.

Note DTLSv1.2 is supported on all Secure Firewall ASA models except the 5506-X, 5508-X, and 5516-X and applies when the ASA is acting as a server only, not a client. DTLS 1.2 supports additional ciphers, as well as all current TLS/DTLS ciphers and a larger cookie size.

- You must upgrade to ASDM 7.10.1 to use management VPN tunnel.
- You must upgrade to ASDM 7.5.1 to use Network Visibility Module.
- You must upgrade to ASDM 7.4.2 to use AMP Enabler.
- You must upgrade to Secure Firewall ASA 9.3(2) to use TLS 1.2.
- You must upgrade to Secure Firewall ASA 9.2(1) if you want to use the following features:
  - ISE Posture over VPN
  - ISE Deployment of AnyConnect
  - Change of Authorization (CoA) on ASA is supported from this version onwards
- You must upgrade to Secure Firewall ASA 9.0 if you want to use the following features:
  - IPv6 support
  - Cisco Next Generation Encryption “Suite-B” security
  - Dynamic Split Tunneling(Custom Attributes)
  - AnyConnect deferred upgrades
  - Management VPN Tunnel (Custom Attributes)
- You must use Secure Firewall ASA 8.4(1) or later if you want to do the following:
  - Use IKEv2.
  - Use the ASDM to edit non-VPN client profiles (such as Network Access Manager).
  - Deploy firewall rules. If you deploy always-on VPN, you might want to enable split tunneling and configure firewall rules to restrict network access to local printing and tethered mobile devices.
  - Configure dynamic access policies or group policies to exempt qualified VPN users from an always-on VPN deployment.

- Configure dynamic access policies to display a message on the AnyConnect GUI when an AnyConnect session is in quarantine.

- To perform the HostScan migration from 4.3x to 4.6.x, ASDM 7.9.2 or later is required.

Secure Firewall ASA Memory Requirements

Caution The minimum flash memory recommended for all Secure Firewall ASA models using AnyConnect is 512MB. This will allow hosting of multiple endpoint operating systems, and logging and debugging to be enabled on the ASA.

Due to flash size limitations on the Secure Firewall ASA (maximum of 128 MB), not all permutations of the AnyConnect package will be able to be loaded onto this model. To successfully load AnyConnect, you will need to reduce the size of your packages (such as fewer OSs, no HostScan, and so on) until they fit on the available flash.

Check for the available space before proceeding with the AnyConnect install or upgrade. You can use one of the following methods to do so:

- CLI—Enter the **show memory** command.

```
asa3# show memory
Free memory:        304701712 bytes (57%)
Used memory:        232169200 bytes (43%)
-------------      ----------------
Total memory:       536870912 bytes (100%)
```

- ASDM—Choose Tools > File Management. The File Management window displays flash space.

If your Secure Firewall ASA has only the default internal flash memory size or the default DRAM size (for cache memory), you could have problems storing and loading multiple AnyConnect packages on the ASA. Even if you have enough space on the flash to hold the package files, the Secure Firewall ASA could run out of cache memory when it unzips and loads the client images. For additional information about the ASA memory requirements and upgrading ASA memory, see the latest release notes for the Cisco ASA.

HostScan

AnyConnect 4.10.x clients **must** use Secure Firewall Posture 5.0 (or later) or HostScan 4.10.x.

Note AnyConnect 4.10.x will not establish a VPN connection when used with an incompatible version of HostScan. Therefore, if you are using a HostScan version prior to 4.10.x, you must upgrade to Secure Firewall Posture 5.0.x (or later) or HostScan 4.10.x. We always recommend that you upgrade to the latest version available for download on CCO.

If you are currently using **HostScan 4.3.x or earlier**, a one-time HostScan migration **must** be performed prior to upgrading to any newer version of HostScan. Refer to the AnyConnect HostScan Migration 4.3.x to 4.6.x and Later documentation for the specifics of how to do this migration.

Also, Cisco does not recommend the combined use of HostScan and ISE posture. Unexpected results occur when the two different posture agents are run.

The HostScan Module provides AnyConnect the ability to identify the operating system, antimalware, and firewall software installed on the host to the Secure Firewall ASA.

When using Start Before Login (SBL) and HostScan, you must install the AnyConnect predeploy module on the endpoints to achieve full HostScan functionality, since SBL is pre-login.

With HostScan, macOS Big Sur (version 11.x) is officially supported. Therefore, if you are using macOS Big Sur beta or the official macOS Big Sur (version 11.x) release with HostScan, the HostScan Module (if previously installed) on the endpoint and the HostScan package on the Secure Firewall ASA must be upgraded to 4.9.04045 or later.

Due to this dynamic adoption in supporting Apple Silicon (M1 chip), macOS endpoints using AnyConnect 4.10.02086 or later must also upgrade the HostScan package version to 4.10.02086 or later. The following chart outlines the minimum requirements:

AnyConnect Version	HostScan Engine (.pkg) Minimum Version Supported/Required
4.10.01075 or earlier	All versions posted on CCO are supported. The most recent HostScan.pkg that is posted is always suggested.
4.10.02086 or later	4.10.02086 or later is required. The most recent HostScan .pkg that is posted is always suggested.

When using Start Before Login (SBL) and Secure Firewall Posture, you must install the Cisco Secure Client predeploy module on the endpoints to achieve full Secure Firewall Posture functionality, since SBL is pre-login.

The HostScan Antimalware and Firewall Support Charts are available on cisco.com.

Notice of End Date for HostScan 4.3.x

End of Support (EOS) for HostScan 4.3.x was announced December 31, 2018. If you are currently using **HostScan 4.3.x or earlier**, a one-time HostScan migration **must** be performed prior to upgrading to any newer version of HostScan. Refer to the AnyConnect HostScan Migration 4.3.x to 4.6.x and Later documentation for the specifics of how to do this migration.

ISE Posture Compliance Module

(CSCvy53730-Windows only) As of AnyConnect 4.9.06037, the Compliance Modules from ISE cannot be updated. Due to this change, Compliance Module version 4.3.1634.6145 or later are required for AnyConnect 4.9.06037 (and above) and Cisco Secure Client 5 (up to 5.0.01242).

The ISE Posture compliance module contains the list of supported antimalware and firewall for ISE posture. While the HostScan list is organized by vendor, the ISE posture list organizes by product type. When the version number on the headend (ISE or Secure Firewall ASA) is greater than the version on the endpoint, the OPSWAT gets updated. These upgrades are mandatory and happen automatically without end user intervention.

The individual files within the library (a zip file) are digitally signed by OPSWAT, Inc., and the library itself is packaged as a single, self-extracting executable which is code signed by a Cisco certificate. Refer to the ISE compliance modules for details.

IOS Support of AnyConnect

Cisco supports AnyConnect VPN access to IOS Release 15.1(2)T functioning as the secure gateway; however, IOS Release 15.1(2)T does not currently support the following AnyConnect features:

- Post Log-in Always-on VPN
- Connect Failure Policy
- Client Firewall providing Local Printer and Tethered Device access
- Optimal Gateway Selection
- Quarantine
- AnyConnect Profile Editor
- DTLSv1.2

For additional limitations of IOS support for AnyConnect VPN, please see Features Not Supported on the Cisco IOS SSL VPN.

Refer to http://www.cisco.com/go/fn for additional IOS feature support information.

AnyConnect Supported Operating Systems

The following tables list the minimum versions supported. When specific versions are noted, as opposed to something such as *8.x*, it is because only particular versions are supported. For example, ISE Posture is not supported on Red Hat 8.0, but it is supported on Red Hat 8.1 and later, and noted as such.

Table 1: Windows

Windows Versions	VPN	Network Access Manager	Secure Firewall Posture	ISE Posture	DART	Customer Experience Feedback	Network Visibility Module	AMP Enabler	Umbrella Roaming Security
Windows 11 (64-bit) and current Microsoft supported versions of Windows 10 x86 (32-bit) and x64 (64-bit)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
	Yes	No	Yes	No	Yes	Yes	No	No	No
Microsoft-supported versions of Windows 11 for ARM64-based PCs	Yes	No	Yes	No	Yes	Yes	No	No	No

Table 2: macOS

macOS Versions	VPN	Network Access Manager	Secure Firewall Posture	ISE Posture	DART	Customer Experience Feedback	Network Visibility Module	AMP Enabler	Umbrella Roaming Security
macOS 14 Sonoma, macOS 13 Ventura, and macOS 12 Monterey, and macOS 11 Big Sur (all 64-bit)	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 3: Linux

Linux Versions	VPN	Secure Firewall Posture	Network Visibility Module	ISE Posture	DART	Customer Experience Feedback
Red Hat	9.x and 8.x	9.x and 8.x	9.x and 8.x	9.x and 8.1 (and later)	Yes	Yes
Ubuntu	22.04 and 20.04	22.04 and 20.04	22.04 and 20.04	22.04 and 20.04	Yes	Yes
SUSE (SLES)	Limited support. Used only to install ISE Posture	not supported	not supported	12.3 (and later) and 15.0 (and later)	Yes	Yes

AnyConnect Support for Microsoft Windows

Windows Requirements

- Pentium class processor or greater.
- 100 MB hard disk space.
- Microsoft Installer, version 3.1.
- Upgrading to Windows 8.1 from any previous Windows release requires you to uninstall AnyConnect, and reinstall it after your Windows upgrade is complete.
- Upgrading from Windows XP to any later Windows release requires a clean install since the AnyConnect Virtual Adapter is not preserved during the upgrade. Manually uninstall AnyConnect, upgrade Windows, then reinstall AnyConnect manually or via WebLaunch.
- To start AnyConnect with WebLaunch, you must use the 32-bit version of Firefox 3.0+ and enable ActiveX or install Sun JRE 1.4+.
- ASDM version 7.02 or higher is required when using Windows 8 or 8.1.

Windows Limitations

- Before AnyConnect release 4.10.03104, Windows ADVERTISE installer action was not supported (CSCvw79615). With release 4.10.03104 and later, we provided a fix to successfully upgrade with Windows ADVERTISE for those with a lower version of AnyConnect. Consider however that future upgrades could still fail if AnyConnect version 4.10.02086 or earlier (as opposed to 4.10.03104 or later) is advertised.
- AnyConnect is not supported on Windows RT. There are no APIs provided in the operating system to implement this functionality. Cisco has an open request with Microsoft on this topic. Those who want this functionality should contact Microsoft to express their interest.

- Other third-party product's incompatibility with Windows 8 prevent AnyConnect from establishing a VPN connection over wireless networks. Here are two examples of this problem:
  - WinPcap service "Remote Packet Capture Protocol v.0 (experimental)" distributed with Wireshark does not support Windows 8.

    To work around this problem, uninstall Wireshark or disable the WinPcap service, reboot your Windows 8 computer, and attempt the AnyConnect connection again.
  - Outdated wireless cards or wireless card drivers that do not support Windows 8 prevent AnyConnect from establishing a VPN connection.

    To work around this problem, make sure you have the latest wireless network cards or drivers that support Windows 8 installed on your Windows 8 computer.
- AnyConnect is not integrated with the new UI framework, known as the Metro design language, that is deployed on Windows 8; however, AnyConnect does run on Windows 8 in desktop mode.
- HP Protect tools do not work with AnyConnect on Windows 8.x.
- If you are using Network Access Manager on a system that supports standby, Cisco recommends that the default Windows 8.x association timer value (5 seconds) is used. If you find the Scanlist in Windows appears shorter than expected, increase the association timer so that the driver can complete a network scan and populate the scanlist.

Windows Guidelines

- Verify that the driver on the client system is supported by your Windows version. Drivers that are not supported may have intermittent connection problems.
- For Network Access Manager, machine authentication using machine password will not work on Windows 8 or 10 / Server 2012 unless a registry fix described in Microsoft KB 2743127 is applied to the client desktop. This fix includes adding a DWORD value LsaAllowReturningUnencryptedSecrets to the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa registry key and setting this value to 1.

  Machine authentication using machine certificate (rather than machine password) does not require a change and is the more secure option. Because machine password was accessible in an unencrypted format, Microsoft changed the OS so that a special key was required. Network Access Manager cannot know the password established between the operating system and active directory server and can only obtain it by setting the key above. This change permits Local Security Authority (LSA) to provide clients like Cisco Network Access Manager with the machine password.

Note Machine authentication allows a client desktop to be authenticated to the network before the user logs in. During this time the administrator can perform scheduled administrative tasks for this client machine. Machine authentication is also required for the EAP Chaining feature where a RADIUS server can authenticate both the User and Machine for a particular client. This will result in identifying company assets and applying appropriate access policies. For example, if this is a personal asset (PC/laptop/tablet), and corporate credentials are used, the endpoint will fail Machine authentication, but succeed User authentication, and the proper network access restrictions are applied to the user's network connection.

- On Windows 8, the Export Stats button on the Preferences > VPN > Statistics tab saves the file on the desktop. In other versions of Windows, the user is asked where to save the file.
- AnyConnect VPN is compatible with 3G/4G/5G data cards which interface with Windows via a WWAN adapter.

AnyConnect Support for Linux

Linux Requirements

- Using VPN CLI without GUI sessions (for example SSH) is not supported
- The Snap version of Firefox is not supported by AnyConnect on Linux
- Administrator privileges are required for installation
- x86 instruction set
- 64-bit processor
- 100 MB hard disk space
- tun support in Linux Kernel
- libstdc++ 6.0.19 (GLIBCXX_3.4.19) or later
- iptables 1.4.21 or later
- NetworkManager 1.0.6 or later
- zlib - to support SSL deflate compression
- glib 2.36 and later
- polkit 0.105 or later
- gtk 3.8 or later
- systemd
- webkitgtk+ 2.10 or later, required only if you are using the AnyConnect embedded browser app
- libnm (libnm.so or libnm-glib.so), required only if you are using Network Visibility Module

AnyConnect Support for macOS

macOS Requirements

- AnyConnect requires 50MB of hard disk space.
- To operate correctly with macOS, AnyConnect requires a minimum display resolution of 1024 by 640 pixels.

macOS Guidelines

- AnyConnect 4.8 (and later) for macOS has been notarized, and installer disk images (dmg) have been stapled.
- Because of the introduction of access control in macOS 10.15, you may see additional popups when Secure Firewall Posture (formerly HostScan) or ISE posture are performing a scan on the endpoint. You are required to accept which files and folders can be accessed and scanned.

AnyConnect Licensing

For the latest end-user license agreement, see Cisco End User License Agreement, AnyConnect Secure Mobility Client.

For our open source licensing acknowledgments, see Open Source Software Used in AnyConnect Secure Mobility Client.

To deploy AnyConnect from an ISE headend and use the ISE Posture module, a Cisco ISE Premier License is required on the ISE Administration node. For detailed ISE license information, see the *Cisco ISE Licenses* chapter of the Cisco Identity Services Engine.

To deploy AnyConnect from a Secure Firewall ASA headend and use the VPN and HostScan modules, an Advantage or Premier license is required. Trial licenses are available. See the AnyConnect Ordering Guide.

For an overview of the Advantage and Premier licenses and a description of which license the features use, see AnyConnect Secure Mobility Client Features, Licenses, and OSs.

AnyConnect Installation Overview

Deploying AnyConnect refers to installing, configuring, and upgrading the AnyConnect and its related files. The AnyConnect can be deployed to remote users by the following methods:

- Predeploy—New installations and upgrades are done either by the end user, or by using an enterprise software management system (SMS).
- Web Deploy—The AnyConnect package is loaded on the headend, which is either a Secure Firewall ASA or ISE server. When the user connects to a Secure Firewall ASA or to ISE, AnyConnect is deployed to the client.
  - For new installations, the user connects to a headend to download AnyConnect. The client is either installed manually, or automatically (web-launch).
  - Updates are done by AnyConnect running on a system where AnyConnect is already installed, or by directing the user to the Secure Firewall ASA clientless portal.
- Cloud Update—After the Umbrella Roaming Security module is deployed, you can update any AnyConnect modules using one of the above methods, as well as Cloud Update. With Cloud Update, the software upgrades are obtained automatically from the Umbrella cloud infrastructure, and the update track is dependent upon that and not any action of the administrator. By default, automatic updates from Cloud Update are disabled.

When you deploy AnyConnect, you can include the optional modules that enable extra features, and client profiles that configure the VPN and other features. Keep in mind the following:

- All AnyConnect modules and profiles can be predeployed. When predeploying, you must pay special attention to the module installation sequence and other details.
- The Customer Experience Feedback module and the HostScan package, used by the VPN Posture module, cannot be web deployed from the ISE.
- The Compliance Module, used by the ISE Posture module, cannot be web deployed from the Secure Firewall ASA.

Note Make sure to update the localization MST files with the latest release from CCO whenever you upgrade to a new AnyConnect package.

Web-based Installation May Fail on 64-bit Windows

This issue applies to Internet Explorer versions 10 and 11, on Windows 8.

When the Windows registry entry HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\TabProcGrowth is set to 0, Active X has problems during AnyConnect web deployment.

See http://support.microsoft.com/kb/2716529 for more information.

The solution to is to:

- Run a 32-bit version of Internet Explorer.
- Edit the registry entry to a non-zero value, or remove that value from the registry.

Note On Windows 8, starting Internet Explorer from the Windows start screen runs the 64-bit version. Starting from the desktop runs the 32-bit version.

AnyConnect Support Policy

Cisco only provides fixes and enhancements based on the most recent Version 4.10 release. TAC support is available to any customer with an active AnyConnect Version 4.10 term/contract running a released version of AnyConnect Version 4.10. If you experience a problem with an out-of-date software version, you may be asked to validate whether the current maintenance release resolves your issue.

Software Center access is limited to AnyConnect Version 4.10 versions with current fixes. We recommend that you download all images for your deployment, as we cannot guarantee that the version you are looking to deploy will still be available for download at a future date.

Guidelines and Limitations

VPN Headend DNS Load Balancing Not Supported

AnyConnect supports DNS load balancing using SAML authentication for an embedded browser. Using Secure Firewall ASA, Secure Firewall Threat Defense, or other headends and an external/native browser, VPN headend DNS load balancing is not supported due to operating system limitations, which restrict the ability for Cisco Secure Client to control the necessary underlying conditions.

macOS 13 Known Issue

Continuity Camera in macOS 13 is currently not functioning during an active VPN connection.

Simultaneous VPN Sessions Not Supported

AnyConnect VPN cannot be active at the same time as any other client VPN, either Cisco software like the AnyConnect Secure Mobility Client for Universal Windows Platform or third-party VPNs.

DNS (Name Resolution) on macOS 12.x May Fail

Those running AnyConnect on macOS 12.x may experience a loss of DNS (name resolution), requiring a reboot for restoration. The cause has been identified as a macOS bug, which has been addressed in macOS 12.3 (FB9803355).

Windows Local Group Policy DNS Settings Ignored

Global DNS settings Searchlist and UseDomainNameDevolution are used by AnyConnect to build the DNS suffix search list for a VPN connection. Any overrides configured via local group policy will be ignored.

Encrypted DNS Impact and Mitigation

Encrypted Domain Name System (DNS) resolution impacts AnyConnect Secure Mobility Client functionality, namely network flows targeting FQDNs resolved via encrypted DNS either circumvent or are not properly handled by the following AnyConnect Secure Mobility Client features: Umbrella DNS protection, Umbrella web protection (when name-based redirect rules are used), VPN (dynamic split tunneling and Always On with name-based exceptions), Network Visibility (reporting of peer FQDN). To mitigate this impact, you should disable encrypted DNS in browser settings pertaining to AnyConnect Secure Mobility Client users.

As an additional mitigation, AnyConnect Secure Mobility Client prohibits DNS over HTTPS (DoH) name resolution for the Windows DNS client via local policy setting **Configure DNS over HTTP (DoH) name resolution** (under Computer Configuration > Administrative Templates > Network > DNS Client). This change is applicable to Windows 11 and later versions and is enforced while any of the following modules is active: VPN, Umbrella Roaming Security, or Network Visibility. AnyConnect Secure Mobility Client does not alter this policy setting if a conflicting setting of higher precedence (for example, domain GPO setting) is detected.

Limitations When Using RPM/DEB Installer

When using an RPM/DEB installer to upgrade from the version installed by the script, the following limitations exist:

- Automatic client update from headend is not supported. You must do updates out-of-band with a system package manager.
- The only AnyConnect modules supported with RPM and DEB installers are VPN and DART.
- You must uninstall current existing AnyConnect (including all modules) before switching to use RPM or DEB installer. See CSCwa16755 for the workaround to a known issue.
- You cannot use a script installer to update an existing RPM or DEB installation.

Root CA Conflict With Firefox NSS Store (Linux Only)

When a root certificate authority (CA) is public trusted, it is already in the File Certificate Store. However, if the Firefox NSS store is left enabled at the same time, the OCSP check might be bypassed, as we only support OCSP check with File Cert Store. To prevent this bypass, disable Firefox NSS store by setting ExcludeFirefoxNSSCertStore to *true* in the local policy file.

Initiating an Automatic VPN Connection With TND (CSCvz02896)

When using Trusted Network Detection, the automatic VPN connection may not be initiated according to the TND policy, if the system route table does not contain a default route.

AnyConnect 4.10 Upgrade Failure on Linux (Only AnyConnect Versions Prior to 4.9.01095)

If you are using web deploy to upgrade to AnyConnect or HostScan 4.10 from a version prior to 4.9.01095, an error could result. Since AnyConnect versions prior to 4.9.01095 did not have the capacity to parse the system CA store, the result is an upgrade failure, because the correct NSS certificate store path could not be determined in the user's profile directory. If you are upgrading to AnyConnect 4.10 from a release prior to 4.9.01095, copy the root certificate (DigiCertAssuredIDRootCA.pem) to /opt/.cisco/certificates/ca prior to upgrading AnyConnect on the endpoint.

NVM Installation Fails With Ubuntu 20

If you are using Ubuntu 20.04 (which has kernel version 5.4), you must use AnyConnect 4.8 (or later), or Network Visibility Module installation fails.

Local and Network Proxy Incompatibilities

Local and/or network proxies (such as software/security applications like Fiddler, Charles Proxy, or Third-party Antimalware/Security software that includes Web HTTP/HTTPS inspection and/or decryption capabilities) are not compatible with AnyConnect.

Web Deployment Workflow Limitations on Linux

Consider these two limitations when doing a web deployment on Linux:

- The Ubuntu NetworkManager Connectivity Checking functionality allows periodic testing, whether the internet can be accessed or not. Because Connectivity Checking has its own prompt, you can receive a network logon window if a network without internet connectivity is detected. To avoid such network prompts, that aren’t tied to a browser window and don't have download capability, you should disable Connectivity Checking in Ubuntu 17 and beyond. By disabling, the user will be able to download a file from the ISE portal using a browser for ISE-based AnyConnect web deployment.

- Before doing a web deploy onto a Linux endpoint, you must disable access control with the xhost+ command. Xhost controls the access of a remote host running a terminal on the endpoint, which is restricted by default. Without disabling access control, AnyConnect web deployment fails.

Client First Auto-Reconnect Unsuccessful After Upgrading to AnyConnect 4.9.01xxx (Linux Only)

With the fix of CSCvu65566 and its device ID computation change, certain deployments of Linux (particularly those that use LVM) experience a one-time connection attempt error immediately after updating from a headend to 4.9.01xxx or later. Linux users running AnyConnect 4.8 (and later) and connecting to a headend to perform an auto update (web-deploy) may receive this error: "The secure gateway has rejected the connection attempt. A new connection attempt to the same or another secure gateway is needed, which requires re-authentication." To successfully connect, you can manually initiate another VPN connection after AnyConnect upgrade. After an initial upgrade to 4.9.01xxx or later, you will no longer hit this issue.

Potential Issues Connecting to a Wireless Network After An Upgrade from AnyConnect 4.7MR4

The Network Access Manager made a revision to write wireless LAN profiles to disk rather than just using temporary profiles in memory. Microsoft requested this change to address an OS bug, but it resulted in a crash of the Wireless LAN Data Usage window and eventual intermittent wireless connectivity issues. To prevent these issues, we reverted the Network Access Manager to using the original temporary WLAN profiles in memory. The Network Access Manager removes most of the wireless LAN profiles on disk when upgrading to version 4.8MR2 or later. Some hard profiles cannot be removed by the OS WLAN service when directed, but any remaining interfere with the ability for the Network Access Manager to connect to wireless networks. Follow these steps if you experience problems connecting to a wireless network after an upgrade from 4.7MR4 to 4.8MR2:

1. Stop the AnyConnect Network Access Manager service.
2. From the administrator command prompt, enter

```
netsh wlan delete profile name=*(AC)
```

This removes leftover profiles from previous versions (AnyConnect 4.7MR4 to 4.8MR2). Alternatively, you can look for profiles with **AC** appended to the name and delete them from the native supplicant.

Nslookup Command Needs macOS Fix To Work As Expected

macOS 11 fixed an issue seen in AnyConnect version 4.8.03036 (and later) related to the nslookup command, namely nslookup not sending DNS queries through the VPN tunnel with split-include tunneling configuration. The issue initiated in AnyConnect 4.8.03036 when that version included a fix for defect CSCvo18938. The Apple-suggested changes for that defect ended up revealing another OS issue, causing the nslookup problematic behavior.

As a workaround for macOS 10.x, you can pass the VPN DNS server as a parameter to nslookup: **`nslookup [name] [ip_dnsServer_vpn]`**.

Server Certificate Validation Error

(CSCvu71024) AnyConnect authentication may fail if the Secure Firewall ASA headend or SAML provider uses certificates signed by the AddTrust root (or one of the intermediaries), because they expired in May 2020.

The expired certificate causes AnyConnect to fail and presents as a server certificate validation error, until operating systems make the required updates to accommodate the May 2020 expiration.

Windows DNS Client Optimizations Caveat

Windows DNS Client optimizations present in Windows 8 and above may result in failure to resolve certain domain names when split DNS is enabled. The workaround is to disable such optimizations by updating the following registry keys:

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters

Value:DisableParallelAandAAAA

Data: 1

Key: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\DNSClient

Value: DisableSmartNameResolution

Data: 1
```

Preparation for macOS 10.15 Users

The macOS 10.15 operating system does not support 32-bit binaries. Additionally, Apple verifies that all software installed on 10.15 has been cryptographically notarized via digital signature. From AnyConnect 4.8 and later, operation on macOS 10.15 is supported with no 32-bit code.

Make note of these limitations:

- AnyConnect versions prior to 4.7.03052 may require an active internet connection to upgrade.
- HostScan versions prior to 4.8.x will not function on macOS 10.15.
- HostScan and System Scan users on macOS 10.15 will experience permission popups during initial launch.

HostScan Will Not Function With macOS 10.15 Without Upgrade (CSCvq11813)

HostScan packages earlier than 4.8.x will not function with macOS Catalina (10.15). End users who attempt to connect from macOS Catalina to Secure Firewall ASA headends running HostScan packages earlier than 4.8.x will not be able to successfully complete VPN connections, receiving a posture assessment failed message.

AnyConnect 4.10.x clients on macOS Big Sur (11.x) must use HostScan 4.9.04045 or later.

To enable successful VPN connections for HostScan users, all DAP and HostScan policies must be HostScan 4.8.00175 (or later) compatible. Refer to AnyConnect HostScan Migration 4.3.x to 4.6.x and Later for additional information related to policy migration from HostScan 4.3.x to 4.8.x.

As a workaround to restore VPN connectivity, administrators of systems with HostScan packages on their Secure Firewall ASA headends may disable HostScan. If disabled, allHostScan posture functionality, and DAP policies that depend on endpoint information, will be unavailable.

The associated field notice can be found here: https://www.cisco.com/c/en/us/support/docs/field-notices/704/fn70445.html.

Permission Popups During Initial HostScan or System Scan Launch (CSCvq64942)

macOS 10.15 (and later) requires that applications obtain user permissions for access to Desktop, Documents, Downloads, and Network Volume folders. To grant this access, you may see popups during an initial launch

of HostScan, System Scan (when ISE posture is enabled on the network), or DART (when ISE posture or AnyConnect is installed). ISE posture and HostScan use OPSWAT for posture assessment on endpoints, and the posture checks access these folders based on the product and policies configured.

At these popups, you must click **OK** to have access to these folders and to continue with the posture flow. If you click **Don't Allow**, the endpoint may not remain compliant, and the posture assessment and remediation may fail without access to these folders.

To Remedy a *Don't Allow* Selection

To see these popups again and grant access to the folders, edit cached settings:

1. Open **System Preferences**.
2. Navigate to **Security & Privacy** > **Privacy > Files and Folders** > **.**
3. Delete folder access related cache details in the AnyConnect Secure Mobility Client folder.

The permission popups will reappear with a subsequent start of posture, and the user can click **OK** to grant access.

GUI Customization on macOS Not Supported

GUI resource customization on macOS is currently not supported.

Incompatibility with SentinelOne

AnyConnect Umbrella module is incompatible with SentinelOne endpoint security software.

macOS Management Tunnel Disconnect After Upgrade to 4.8

If you encounter any of the following scenarios, it is related to security improvements to comply with Apple notarizations:

- You had management tunnel connectivity with AnyConnect 4.7, but the AnyConnect 4.8 version fails in the same environment.
- The VPN statistic window displays "Disconnect (Connect Failed)" as the management tunnel state.
- Console logs indicate "Certificate Validation Failure," signifying a management tunnel disconnect.

If configured to allow access (without prompting) to the AnyConnect app or executables, ACLs must be reconfigured after upgrading to AnyConnect 4.8 (or later), by re-adding the app or executable. You must change the private key access in the system store of the keychain access to include the vpnagentd process:

1. Navigate to **System Keychain** > **System** > **My Certificates** > **Private key**.
2. Remove the vpnagentd process from the access control tab.
3. Add the current vpnagentd into the /opt/cisco/anyconnect/bin folder.
4. Enter the password when prompted.
5. Quit Keychain Access and stop the VPN service.
6. Restart.

No Detection of Default Patch Management in ISE Posture (CSCvq64901)

ISE posture failed to detect the default Patch Management while using macOS 10.15. An OPSWAT fix is required to remedy this situation.

PMK-Based Roaming Not Supported With Network Access Manager

You cannot use PMK-based roaming with Network Access Manager on Windows.

DART Requires Admin Privileges

Due to system security restrictions, DART now requires administrator privileges on macOS, Ubuntu, and Red Hat to collect logs.

Restored IPsec Connections in FIPS Mode (CSCvm87884)

AnyConnect releases 4.6.2 and 4.6.3 had IPsec connection issues. With the restoration of the IPsec connection (CSCvm87884) in AnyConnect release 4.7 (and later), Diffie-Hellman groups 2 and 5 in FIPS mode are no longer supported. Therefore, AnyConnect in FIPS mode can no longer connect to Secure Firewall ASA prior to release 9.6 and with configuration dictating DH groups 2 or 5.

Changes with Certificate Store Database (NSS Library Updates) on Firefox58

(Only Impacting users using Firefox prior to 58) Due to the NSS certificate store DB format change starting with Firefox 58, AnyConnect also made the change to use new certificate DB. If using Firefox version prior to 58, set NSS_DEFAULT_DB_TYPE="sql" environment variable to 58 to ensure Firefox and AnyConnect are accessing the same DB files.

Conflict with Network Access Manager and Group Policy

If your wired or wireless network settings or specific SSIDs are pushed from a Windows group policy, they can conflict with the proper operation of the Network Access Manager. With the Network Access Manager installed, a group policy for wireless settings is not supported.

No Hidden Network Scanlist on Network Access Manager with Windows 10 Version 1703 (CSCvg04014)

Windows 10 version 1703 changed their WLAN behavior, which caused disruptions when the Network Access Manager scans for wireless network SSIDs. Because of a bug with the Windows code that Microsoft is investigating, the Network Access Manager's attempt to access hidden networks is impacted. To provide the best user experience, we have disabled Microsoft's new functionality by setting two registry keys during Network Access Manager installation and removing them during an uninstall.

AnyConnect macOS 10.13 (High Sierra) Compatibility

AnyConnect 4.5.02XXX and later has additional functionality and warnings to guide users through the steps needed to leverage complete capabilities, by enabling the Secure Client, formerly AnyConnect, software extension in their macOS Preferences -> Security & Privacy pane. The requirement to manually enable the software extension is a new operating system requirement in macOS 10.13 (High Sierra). Additionally, if AnyConnect is upgraded before a user’s system is upgraded to macOS 10.13 and later, the user will automatically have the AnyConnect software extension enabled.

Users running macOS 10.13 (and later) with a version earlier than 4.5.02XXX must enable the Secure Client, formerly AnyConnect, software extension in their macOS Preferences -> Security & Privacy pane. You may need to manually reboot after enabling the extension.

As described in https://support.apple.com/en-gb/HT208019, macOS system administrators potentially have additional capabilities to disable User Approved Kernel Extension Loading, which would be effective with any currently supported version of AnyConnect.

Impact on Posture When a Power Event or Network Interruption Occurs

If a network change or power event occurs, a posture process that is interrupted will not complete successfully. The network or power change results in the AnyConnect downloader error that must be acknowledged by the user before continuing the process.

Network Access Manager Does Not Automatically Fallback to WWAN/3G/4G/5G

All connections to WWAN/3G/4G/5G must be manually triggered by the user. The Network Access Manager does NOT automatically connect to these networks if no wired or wireless connection is available.

Web Deploy of NAM, DART, ISE Posture, and/or Posture Fails with Signature/File Integrity Verification Error

A "timestamp signature and/or certificate could not be verified or is malformed" error only occurs on Windows during web deploy of AnyConnect 4.4MR2 (or later) from Secure Firewall ASA or ISE. Only the Network Access Manager, DART, ISE Posture, and Posture modules that are deployed as MSI files are affected. Because of the use of SHA-2 timestamping certificate service, the most up-to-date trusted root certificates are required to properly validate the timestamp certificate chain. You will not have this issue with predeploy or an out-of-the-box Windows system configured to automatically update root certificates. However, if the automatic root certificate update setting has been disabled (not the default), refer to https://technet.microsoft.com/en-us/library/dn265983(v=ws.11).aspx or manually install the timestamping root certificates that we use. You can also use the signtool to verify if the issue is outside of AnyConnect by running the

```
signtool.exe verify /v /all/debug/pa<file to verify>
```

command from a Microsoft provided Windows SDK.

macOS Keychain Prompts During Authentication

On macOS, a keychain authentication prompt may appear after the VPN connection is initiated. The prompt only occurs when access to a client certificate private key is necessary, after a client certificate request from the secure gateway. Even if the tunnel group is not configured with certificate authentication, certificate mapping may be configured on the Secure Firewall ASA, causing the keychain prompts when the access control setting for the client certificate private key is configured as *Confirm Before Allowing Access*.

Configure the AnyConnect profile to restrict AnyConnect access strictly to clients certificates from the login keychain (in the ASDM profile editor, choose Login under Preferences (Part 1) - Certificate Store - macOS). You can stop the keychain authentication prompts with one of the following actions:

- Configure the certificate matching criteria in the client profile to exclude well-known system keychain certificates.
- Configure the access control setting for the client certificate private keys in the system keychain to allow access to AnyConnect.

Umbrella Roaming Security Module Changes

The dashboard to retrieve the `OrgInfo.json` file is https://dashboard.umbrella.com. From there you navigate to **Identities** > **Roaming Computers**, click the **+** (Add icon) in the upper left, and click **Module Profile** from the AnyConnect Umbrella Roaming Security Module section.

Microsoft Inadvertently Blocks Updates to Windows 10 When Network Access Manager is Installed

Microsoft intended to block updates to earlier versions of Windows when the Network Access Manager is installed, but Windows 10 and Creators Edition (RS2) were inadvertently blocked as well. Because of the error (Microsoft Sysdev 11911272), you must first uninstall the Network Access Manager module before you can upgrade to the Creators Editor (RS2). You can then reinstall the module after the upgrade. Microsoft's fix for this error is planned for June 2017.

Windows 10 Defender False Positive—Cisco AnyConnect Adapter Issue

When upgrading to Windows 10 Creator Update (April 2017), you may encounter a Windows Defender message that the AnyConnect adapter has an issue. Windows Defender instructs you to enable the adapter under the Device Performance and Health section. In actuality, the adapter should be disabled when not in use, and no manual action should be taken. This false positive error has been reported to Microsoft under Sysdev # 11295710.

AnyConnect 4.4MR1 (or later) and 4.3MR5 are compatible with Windows 10 Creators Edition (RS2).

AnyConnect Compatibility with Microsoft Windows 10

For best results, we recommend a clean install of AnyConnect on a Windows 10 system and not an upgrade from Windows 7/8/8.1. If you are planning to perform an upgrade from Windows 7/8/8.1 with AnyConnect pre-installed, make sure that you first upgrade AnyConnect prior to uprading the operating system. The Network Access Manager Module **must** be uninstalled prior to upgrading to Windows 10. After the system upgrade is complete, you can re-install Network Access Manager on the system. You may also choose to fully uninstall AnyConnect and re-install one of the supported versions after upgrading to Windows 10.

New Split Include Tunnel Behavior (CSCum90946)

Formerly, if a split-include network was a Supernet of a Local Subnet, the local subnet traffic was *not* tunneled unless a split-include network that exactly matches the Local Subnet was configured. With the resolution of CSCum90946, when a split-include network is a Supernet of a Local Subnet, the Local Subnet traffic is tunneled, unless a split-exclude (deny 0.0.0.0/32 or ::/128) is also configured in the access-list (ACE/ACL).

The following configuration is required when a Supernet is configured in the split-include *and* the desired behavior is to allow LocalLan access:

- access-list (ACE/ACL) must include *both* a permit action for the Supernet and a deny action for 0.0.0.0/32 or ::/128.
- Enable Local LAN Access in the AnyConnect profile (in the Preferences Part 1 menu) of the profile editor. (You also have the option to make it user controllable.)

Microsoft Phasing out SHA-1 Support

A secure gateway with a SHA-1 certificate or a certificate with SHA-1 intermediate certificates may no longer be considered valid by a Windows Internet Explorer 11 / Edge browser or a Windows AnyConnect endpoint after February 14, 2017. After February 14, 2017, Windows endpoints may no longer consider a secure gateway with a SHA-1 certificate or intermediate certificate as trusted. We highly recommend that your secure gateway does not have a SHA-1 identity certificate and that any intermediate certificates are not SHA-1.

Microsoft has made modifications to their original plan of record and timing. They have published details for how to test whether your environment will be impacted by their February 2017 changes. Cisco is not able to make any guarantees of correct AnyConnect operation for customers with SHA-1 secure gateway or intermediate certificates or running old versions of AnyConnect.

Cisco highly recommends that customers stay up to date with the current maintenance release of AnyConnect in order to ensure that they have all available fixes in place. The most up-to-date version of AnyConnect 4.x and beyond are available Cisco.com Software Center for customers with active AnyConnect Plus, Apex, and VPN Only terms/contracts. AnyConnect Version 3.x is no longer actively maintained and should no longer be used for any deployments.

Note Cisco has validated that AnyConnect 4.3 and 4.4 (and beyond) releases will continue to operate correctly as Microsoft further phases out SHA-1. Long term, Microsoft intends to distrust SHA-1 throughout Windows in all contexts, but their current advisory does not provide any specifics or timing on this. Depending on the exact date of that deprecation, many earlier versions of AnyConnect may no longer operate at any time. Refer to Microsoft's advisory for further information.

Authentication Failure When Using a SHA512 Certificate for Authentication

(For Windows 7, 8, and 8.1 users running an AnyConnect version prior to 4.9.03047) When the client uses a SHA512 certificate for authentication, authentication fails, even though the client logs show that the certificate is being used. The ASA logs correctly show that no certificate was sent by AnyConnect. These versions of Windows require that you enable support for SHA512 certificates in TLS 1.2, which is not supported by default. Refer to https://support.microsoft.com/en-us/kb/2973337 for information on enabling support for these SHA512 certificates. 4.9.03049

OpenSSL Cipher Suites Changes

Because the OpenSSL standards development team marked some cipher suites as compromised, we no long support them beyond AnyConnect 3.1.05187. The unsupported cipher suites include the following: DES-CBC-SHA, RC4-SHA, and RC4-MD5.

Likewise, our crypto toolkit has discontinued support for RC4 ciphers; therefore, our support for them will be dropped with releases 3.1.13011 and 4.2.01035 and beyond.

Using Log Trace in ISE Posture

After a fresh installation, you see ISE posture log trace messages as expected. However, if you go into the ISE Posture Profile Editor and change the Enable Agent Log Trace file to 0 (disable), a service restart of AnyConnect is required to get expected results.

Interoperability With ISE Posture on macOS

If you are using macOS 10.9 or later and want to use ISE posture, you may need to do the following to avoid issues:

- Turn off certificate validation to avoid a "failed to contact policy server" error during posture assessment.
- Disable the captive portal application; otherwise, discovery probes are blocked, and the application remains in pre-posture ACL state.

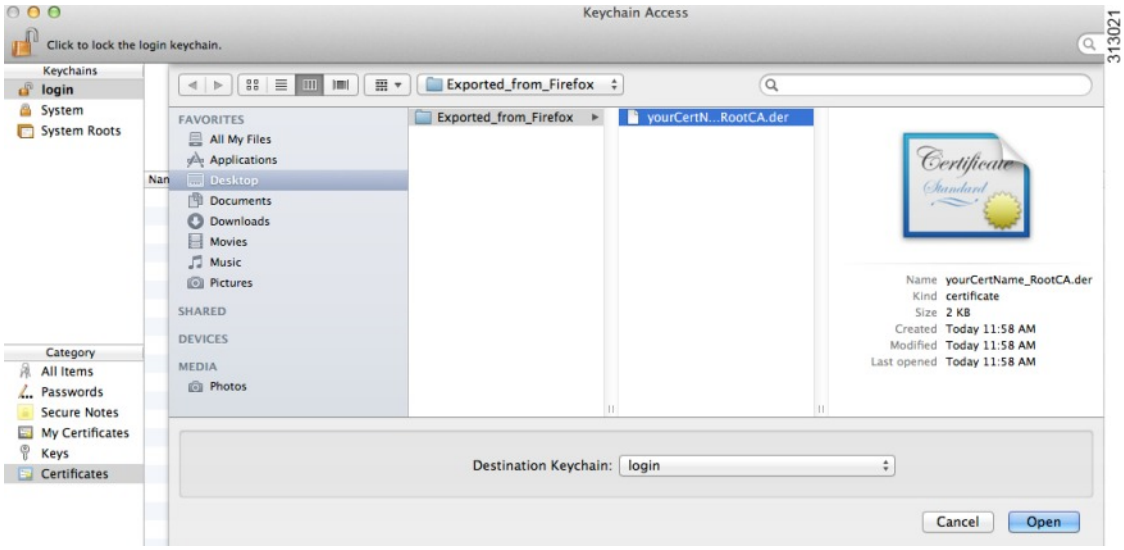
Firefox Certificate Store on macOS is Not Supported

The Firefox certificate store on macOS is stored with permissions that allow any user to alter the contents of the store, which allows unauthorized users or processes to add an illegitimate CA into the trusted root store. AnyConnect no longer utilizes the Firefox store for either server validation or client certificates.

If necessary, instruct your users how to export your AnyConnect certificates from their Firefox certificate stores, and how to import them into the macOS keychain. The following steps are an example of what you may want to tell your AnyConnect users.

1. Navigate to **Firefox > Preferences > Privacy & Security > Advanced**, Certificates tab, click **View Certificates**.
2. Select the Certificate used for AnyConnect, and click **Export**.

   Your AnyConnect Certificate(s) will most likely be located under the Authorities category. Verify with your Certificate Administrator, as they may be located under a different category (Your Certificates or Servers).
3. Select a location to save the Certificate(s), for example, a folder on your desktop.
4. In the Format pull down menu, select **X.509 Certificate (DER)**. Add the .der extension to the certificate name, if required.

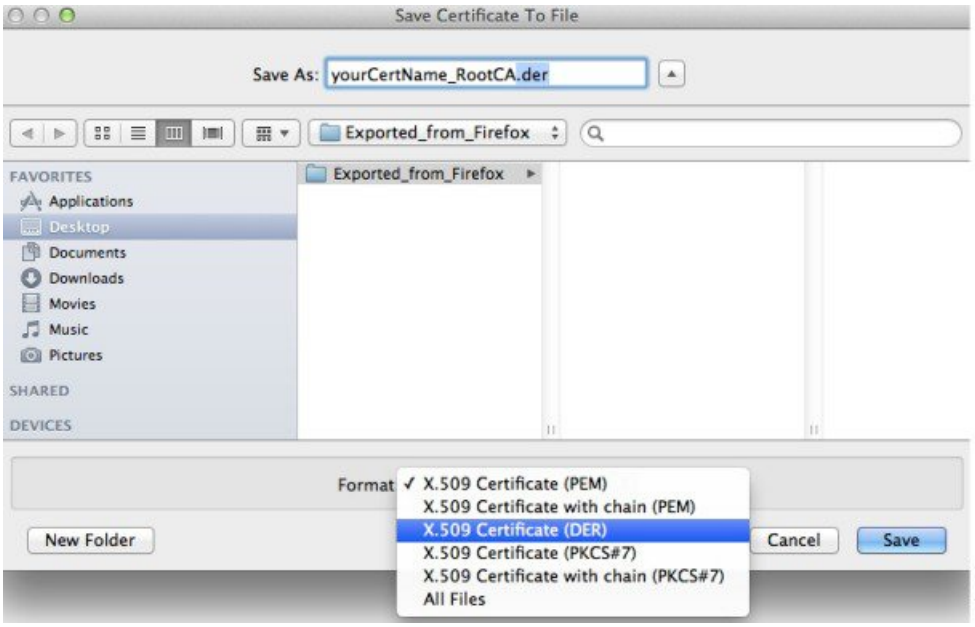


Note If more than one AnyConnect Certificate and/or a Private Key is used/required, repeat the above process for each Certificate).

5. Launch KeyChain. Navigate to File, Import Items…, and select the Certificate that you exported from Firefox.

   In the Destination Keychain:, select the desired Keychain. The login Keychain that is used for this example may not be the one used at your company. Ask your Certificate Administrator to which Keychain your certificate(s) should be imported.

6. In the Destination Keychain:, select the desired Keychain. The login Keychain that is used for this example may not be the one used at your company. Ask your Certificate Administrator to which keychain your certificate(s) should be imported.



7. Repeat the preceding steps for additional Certificates that are used or required for AnyConnect.

SSLv3 Prevents HostScan From Working

(CSCue04930) HostScan does not function when the SSLv3 options SSLv3 only or Negotiate SSL V3 are chosen in ASDM (Configuration > Remote Access VPN > Advanced > SSL Settings > The SSL version for the security appliance to negotiate as a server). A warning message displays in ASDM to alert the administrator.

WebLaunch Issues With Safari

There is an issue with Weblaunch with Safari. The default security settings in the version of Safari that comes with OS X 10.9 (Mavericks) prevents AnyConnect Weblaunch from working. To configure Safari to allow Weblaunch, edit the URL of the ASA to Unsafe Mode, as described below.

Safari 9 (and earlier)

1. Open Safari **Preferences**.
2. Choose **Security** preference.
3. Click **Manage Website Settings...** button.
4. Choose **Java** from the options listed on the left side.
5. Change the option from **Block** to **Allow Always** for the website "Hostname_or_IP_address" that you are trying to connect to.
6. Click **Done**.

Safari 10 (and later)

1. Open Safari **Preferences**.
2. Choose **Security** preference.
3. Check the **Internet plug-ins:** option to **allow plug-ins.**
4. Choose **Plug-in Settings** button.
5. Choose **Java** from the options listed on the left side.
6. Highlight the "Hostname_or_IP_address" that you are trying to connect to.
7. Hold **Alt** (or **Option**) and click the drop-down menu. Make sure that **On** is checked, and **Run in Safe Mode** is unchecked.
8. Click **Done**.

Active X Upgrade Can Disable Weblaunch

Automatic upgrades of AnyConnect software via WebLaunch will work with limited user accounts as long as there are no changes required for the ActiveX control.

Occasionally, the control will change due to either a security fix or the addition of new functionality.

Should the control require an upgrade when invoked from a limited user account, the administrator must deploy the control using the AnyConnect pre-installer, SMS, GPO or other administrative deployment methodology.

Java 7 Issues

Java 7 can cause problems with AnyConnect and HostScan. A description of the issues and workarounds is provided in the Troubleshooting Technote Java 7 Issues with AnyConnect, CSD/HostScan, and WebVPN - Troubleshooting Guide, which is in Cisco documentation under Security > CiscoHostScan.

Implicit DHCP filter applied when Tunnel All Networks Configured

To allow local DHCP traffic to flow in the clear when Tunnel All Networks is configured, AnyConnect adds a specific route to the local DHCP server when AnyConnect connects. To prevent data leakage on this route,

AnyConnect also applies an implicit filter on the LAN adapter of the host machine, blocking all traffic for that route except DHCP traffic.

AnyConnect over Tethered Devices

Network connectivity provided by Bluetooth or USB tethered mobile phones or mobile data devices are not specifically qualified by Cisco and should be verified with AnyConnect before deployment.

AnyConnect Smart Card Support

AnyConnect supports Smartcard provided credentials in the following environments:

- Microsoft CAPI 1.0 and CAPI 2.0 on Windows7, Windows 8, and Windows 10.
- Keychain on macOS, and CryptoTokenKit on macOS 10.12 and higher.

Note AnyConnect does not support Smart cards on Linux or PKCS #11 devices.

AnyConnect Virtual Testing Environment

Cisco performs a portion of AnyConnect testing using these virtual machine environments:

- VM Fusion 7.5.x, 10.x, 11.5.x
- ESXi Hypervisor 6.0.0, 6.5.0, and 6.7.x
- VMware Workstation 15.x

We do not support running AnyConnect in virtual environments; however, we expect AnyConnect to function properly in the VMWare environments we test in.

If you encounter any issues with AnyConnect in your virtual environment, report them. We will make our best effort to resolve them.

UTF-8 Character Support for AnyConnect Passwords

AnyConnect 3.0 or later used with Secure Firewall ASA 8.4(1) or later supports UTF-8 characters in passwords sent using RADIUS/MSCHAP and LDAP protocols.

Disabling Auto Update May Prevent Connectivity Due to a Version Conflict

When Auto Update is disabled for a client running AnyConnect, the Secure Firewall ASA must have the same version of AnyConnect or earlier installed, or the client will fail to connect to the VPN.

To avoid this problem, configure the same version or earlier AnyConnect package on the Secure Firewall ASA, or upgrade the client to the new version by enabling Auto Update.

Interoperability between Network Access Manager and other Connection Managers

When the Network Access Manager operates, it takes exclusive control over the network adapters and blocks attempts by other software connection managers (including the Windows native connection manager) to

establish connections. Therefore, if you want AnyConnect users to use other connection managers on their endpoint computers (such as iPassConnect Mobility Manager), they must disable Network Access Manager either through the Disable Client option in the Network Access Manager GUI, or by stopping the Network Access Manager service.

Network Interface Card Drivers Incompatible with Network Access Manager

The Intel wireless network interface card driver, version 12.4.4.5, is incompatible with Network Access Manager. If this driver is installed on the same endpoint as the Network Access Manager, it can cause inconsistent network connectivity and an abrupt shutdown of the Windows operating system.

Configuring Antivirus Applications for AnyConnect

Applications like antivirus, antimalware, and Intrusion Prevention System (IPS) can misinterpret the behavior of AnyConnect Secure Mobility Client applications as malicious. You can configure exceptions to avoid such misinterpretation. After installing the AnyConnect modules or packages, configure your antivirus software to allow the AnyConnect Installation folder or make security exceptions for the AnyConnect applications.

The common directories to exclude are listed below, although the list may not be complete:

- C:\Users\<user>\AppData\Local\Cisco
- C:\ProgramData\Cisco
- C:\Program Files x86)\Cisco

Configuring Antivirus Applications for HostScan

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

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

Public Proxy Not Supported by IKEv2

IKEv2 does not support the public-side proxy. If you need support for that feature, use SSL. Private-side proxies are supported by both IKEv2 and SSL as dictated by the configuration sent from the secure gateway. IKEv2 applies the proxy configuration sent from the gateway, and subsequent HTTP traffic is subject to that proxy configuration.

MTU Adjustment on Group Policy May Be Required for IKEv2

AnyConnect sometimes receives and drops packet fragments with some routers, resulting in a failure of some web traffic to pass.

To avoid this, lower the value of the MTU. We recommend 1200. The following example shows how to do this using CLI:

```
hostname# config t
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect mtu 1200
```

To set the MTU using ASDM, go to **Configuration** > **Network (Client) Access** > **Group Policies** > **Add** or **Edit** > **Advanced** > **AnyConnect Client**.

MTU Automatically Adjusted When Using DTLS

If Dead Peer Detection (DPD) is enabled for DTLS, the client automatically determines the path MTU. If you previously reduced the MTU using the Secure Firewall ASA, you should restore the setting to the default (1406). During tunnel establishment, the client auto-tunes the MTU using special DPD packets. If you still have a problem, use the MTU configuration on the Secure Firewall ASA to restrict the MTU as before.

Network Access Manager and Group Policy

Windows Active Directory Wireless Group Policies manage the wireless settings and any wireless networks that are deployed to PCs in a specific Active Directory Domain. When installing the Network Access Manager, administrators must be aware that certain wireless Group Policy Objects (GPOs) can affect the behavior of the Network Access Manager. Administrators should test the GPO policy settings with the Network Access Manager before doing full GPO deployment. GPOs pertaining to wireless networks are not supported.

FreeRADIUS Configuration to Work With Network Access Manager

To use Network Access Manager, you may need to adjust the FreeRADIUS configuration. Any ECDH related ciphers are disabled by default to prevent vulnerability. In /etc/raddb/eap.conf, change the cipher_list value.

Full Authentication Required if Roaming between Access Points

A mobile endpoint running Windows 7 or later must do a full EAP authentication instead of leveraging the quicker PMKID reassociation when the client roams between access points on the same network. Consequently, in some cases, AnyConnect prompts the user to enter credentials for every full authentication if the active profile requires it.

User Guideline for Cisco Cloud Web Security Behavior with IPv6 Web Traffic

Unless an exception for an IPv6 address, domain name, address range, or wild card is specified, IPv6 web traffic is sent to the scanning proxy where it performs a DNS lookup to see if there is an IPv4 address for the URL the user is trying to reach. If the scanning proxy finds an IPv4 address, it uses that for the connection. If it does not find an IPv4 address, the connection is dropped.

If you want all IPv6 traffic to bypass the scanning proxies, you can add this static exception for all IPv6 traffic ::/0. Doing this makes all IPv6 traffic bypass all scanning proxies. This means that IPv6 traffic is not protected by Cisco Cloud Web Security.

Preventing Other Devices in a LAN from Displaying Hostnames

After one uses AnyConnect to establish a VPN session with Windows 7 or later on a remote LAN, the network browsers on the other devices in the user's LAN display the names of hosts on the protected remote network. However, the other devices cannot access these hosts.

To ensure the AnyConnect host prevents the hostname leak between subnets, including the name of the AnyConnect endpoint host, configure that endpoint to never become the primary or backup browser.

1. Enter **regedit** in the Search Programs and Files text box.
2. Navigate to **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Browser\Parameters**
3. Double-click **MaintainServerList**.

The Edit String window opens.

1. Enter **No**.
2. Click **OK**.
3. Close the Registry Editor window.

Revocation Message

The AnyConnect certificate revocation warning popup window opens after authentication if AnyConnect attempts to verify a server certificate that specifies the distribution point of an LDAP certificate revocation list (CRL), if the distribution point is only internally accessible.

If you want to avoid the display of this popup window, do one of the following:

- Obtain a certificate without any private CRL requirements.
- Disable server certificate revocation checking in Internet Explorer.

Caution Disabling server certificate revocation checking in Internet Explorer can have severe security ramifications for other uses of the OS.

Messages in the Localization File Can Span More than One Line

If you try to search for messages in the localization file, they can span more than one line, as shown in the example below:

```
msgid ""
"The service provider in your current location is restricting access to the "
"Secure Gateway. "
```

AnyConnect for macOS Performance when Behind Certain Routers

When AnyConnect for macOS attempts to create an SSL connection to a gateway running IOS, or when AnyConnect attempts to create an IPsec connection to a Secure Firewall ASA from behind certain types of routers (such as the Cisco Virtual Office (CVO) router), some web traffic may pass through the connection while other traffic drops. AnyConnect may calculate the MTU incorrectly.

To work around this problem, manually set the MTU for the AnyConnect adaptor to a lower value using the following command from the macOS command line:

```
sudo ifconfig utun0 mtu 1200
```

Preventing Windows Users from Circumventing Always-on

On Windows computers, users with limited or standard privileges may sometimes have write access to their program data folders. These privileges could allow them to delete the AnyConnect profile and thereby circumvent the Always-On feature. To prevent this, configure the computer to restrict access to the `C:\ProgramData` folder, or at least the Cisco sub-folder.

Avoid Wireless-Hosted-Network

Using the Windows 7 or later, the Wireless Hosted Network feature can make AnyConnect unstable. When using AnyConnect, we do not recommend enabling this feature or running front-end applications that enable it (such as Connectify or Virtual Router).

AnyConnect Requires That the Secure Firewall ASA Not Be Configured to Require SSLv3 Traffic

AnyConnect requires the Secure Firewall ASA to accept TLSv1 or TLSv1.2 traffic, but not SSLv3 traffic. The SSLv3 key derivation algorithm uses MD5 and SHA-1 in a way that can weaken the key derivation. TLSv1, the successor to SSLv3, resolves this and other security issues present in SSLv3.

AnyConnect cannot establish a connection with the following Secure Firewall ASA settings for “ssl server-version”:

ssl server-version sslv3

ssl server-version sslv3-only

Trend Micro Conflicts with Install

If you have Trend Micro on your device, the Network Access Manager will not install because of a driver conflict. You can uninstall the Trend Micro or uncheck **trend micro common firewall driver** to bypass the issue.

What HostScan Reports

None of the supported antimalware and firewall products report the last scan time information. HostScan reports the following:

- For antimalware
  - Product description
  - Product version
  - File system protection status (active scan)
  - Data file time (last update and timestamp)
- For firewall
  - Product description
  - Product version
  - Is firewall enabled

Long Reconnects (CSCtx35606)

You may experience long reconnects on Windows if IPv6 is enabled and auto-discovery of proxy setting is either enabled in Internet Explorer or not supported by the current network environment. As a workaround, you can disconnect any physical network adapters not used for VPN connection or disable proxy auto-discovery in IE, if proxy auto-discovery is not supported by the current network environment.

No Pro-Active Key Caching (PKC) or CCKM Support

Network Access Manager does not support PKC or CCKM caching. Fast roaming is unavailable on all Windows platforms.

Application Programming Interface for the AnyConnect Secure Mobility Client

AnyConnect Secure Mobility Client includes an Application Programming Interface (API) for those who want to write their own client programs.

The API package contains documentation, source files, and library files to support a C++ interface for the AnyConnect. You can use the libraries and example programs for building on Windows, Linux and MAC platforms. The Makefiles (or project files) for the Windows platform are also included. For other platforms, it includes platform specific scripts showing how to compile the example code. Network administrators can link their application (GUI, CLI, or embedded application) with these files and libraries.

You can download the APIs from Cisco.com.

For support issues regarding the AnyConnect API, send e-mail to the following address: anyconnect-api-support@cisco.com.

AnyConnect 4.10.08029

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCwh73937	core	ENH: macOS AnyConnect to support Dynamic Split Exclusions based on CNAME DNS responses
CSCwi69374	core	macOS: Captive portal remediation not possible via AnyConnect browser with PAC file proxy settings
CSCwi69388	core	macOS: AnyConnect browser used only intermittently for captive portal remediation

Identifier	Component	Headline
CSCwd21905	posture-ise	AutoDART generates bundles when no value is set

AnyConnect 4.10.08025

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCwc58452	core	Cisco AnyConnect Secure Mobility Client for Windows Information Disclosure Vulnerability
CSCwe67896	core	Vulnerabilities in openssl CVE-2023-0215 and others
CSCwe92223	core	Windows arm64: SplitDNSV6 tests showing stray DNS queries in pcap outside tunnel
CSCwf32105	core	AC agent is crashing after upgrading AnyConnect from version 4.10.06079 to 4.10.06090
CSCwf67833	core	(Windows only) - Error: The VPN client is unable to configure private-side proxy settings
CSCwh57935	core	AnyConnect launches the Client Downloader pop-up outside of core update
CSCwi07144	core	Vulnerabilities in zlib - multiple versions
CSCwf58968	download_install	macOS 14-VPN notification app failed to launch; KDF deactivation skipped during uninstall
CSCur83728	nam	AnyConnect NAM doesn't send an EAPol logoff when CAC card is removed
CSCvq05530	nam	ENH: NAM - add support for Management Frame Protection (PMF)

Identifier	Component	Headline
CSCwb94282	nam	NAM can't connect to WPA2+WPA3/Enterprise SSID
CSCwd26172	nam	AnyConnect NAM fails to display/connect SSID in Unicode characters
CSCwf08769	nam	NAM: Disable Windows RnR on Windows 10 and Windows 11 21H2
CSCwh45972	nam	PE - Unable to save NAM profile when SSID is having space in between words
CSCwi27062	nam	NAM unable to connect to Eero mesh APs
CSCwi27137	nam	NAM does not recognize default PMF IGTK cipher
CSCwb30765	opswat-ise	ENH: Include Cyber Eye Security Agent from Trend Micro to Posture Conditions
CSCwb91318	opswat-ise	Sophos Endpoint Agent and Sophos Cloud Agent 2.20.13 fails definition check with CM 4.3.2815
CSCwc10117	opswat-ise	AnyConnect is not detecting the definition of Check Point Endpoint Security 86.25
CSCwc22358	opswat-ise	ENH: Windows: More error codes for Patch Management up to date condition failure
CSCwd43799	opswat-ise	macOS 12.6 - Xprotect AM install version value detected incorrectly
CSCwe11874	opswat-ise	ENH: ISE posture does not support Kaspersky Endpoint Security 12.x
CSCwe33823	opswat-ise	ISE Compliance Module is failing to detect McAfee endpoint Disk Encryption version 7.4.x version
CSCwh70413	posture-ise	ENH: ISE Posture | Apple XProtect support for versions 2171 & 2172

Identifier	Component	Headline
CSCwi03257	posture-ise	ISE Posture IPC on macOS breaks when Symantec WSS is connected, leading to posture failure
CSCwd81612	profile-editor	Unable to save NAM profile when SSID is UNICODE character in PE
CSCwf17017	swg	Timeouts observed while probing to MSFT URL
CSCwf22189	swg	SWG is not getting into protected state occasionally
CSCwf37767	swg	Enable SWG max debug log based on the presence of a custom flag file
CSCwd68113	vpn	AAA auth failing even when correct password is being entered
CSCwe45817	vpn	Unencoded embedded URL in HTTP redirect prevents captive portal detection
CSCwe49687	vpn	macOS 12&13: Delay before CP remediation possible, AnyConnect browser not used
CSCwe83519	vpn	DTLS MTU DPDs are set too early and may be dropped by headend
CSCwf21381	vpn	Cisco Secure Client Denial of Service Vulnerability
CSCwf33688	vpn	Always On filtering is applied with a slight delay on newly enabled network interface
CSCwf92553	vpn	Cisco Secure Client Denial of Service Vulnerability
CSCwh51369	vpn	SBL not able to restore proxy settings during reconnect
CSCwh75976	vpn	Captive portal is not loading in WebView2 based embedded browser after upgrade to v117.x
CSCwf94247	web	QR code may not be properly displayed in External Browser for SAML

AnyConnect 4.10.07073

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCwh02451	core	Client certificate authentication from smartcard fails
CSCwh06886	nam	NAM unable to connect to SSIDs containing curly apostrophes
CSCwd21905	posture-ise	AutoDART generates bundles when no value is set

AnyConnect 4.10.07062

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCwf24327	nam	Network Access Manager fails to connect to mixed WPA2/WPA3 Personal network when NAM policy does not allow WPA3

AnyConnect 4.10.07061

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCwc92975	cli	VPN CLI stuck on disconnecting state
CSCvu77796	core	CIAM: libxml 2.9.10

Identifier	Component	Headline
CSCwb77035	core	Windows Security 'Credential Required' popup not in focus
CSCwc55221	core	AnyConnect does not clear SmartCard pin
CSCwd73497	core	AC is detecting Trusted Network and UI is quitting when there is no network connectivity during SBL
CSCwd74058	core	Vulnerabilities in libxml2 2.9.10
CSCwe00252	core	Cisco AnyConnect Secure Mobility Client and Secure Client for Windows Privilege Esc Vuln
CSCwe43455	core	macOS 13: DNS-related features not working properly with DDR-enabled resolvers
CSCwd06986	dart	AnyConnect DART bundle on Windows 11 in summary reads 'Windows 10' instead of 'Windows 11'
CSCwc64861	gui	AnyConnect GUI message update after successful SAML authentication
CSCwb45685	nam	Add support for empty PIN when accessing smart card certificates
CSCwc78325	nam	Support for Certificate Matching Rule Field Certificate Template information
CSCwd79171	nam	libxml2 code may point to a dangling pointer which can result in an invalid memory access
CSCwd90898	nam	Add support for WPA3 OWE and SAE networks
CSCwe06686	nam	NAM authentication fails after out-of-band password change and reauth
CSCwe33650	nam	NAM acnamcontrol utility requires network GUID to be all caps for restartAdapter

Identifier	Component	Headline
CSCwe38560	nam	NAM unable to connect to networks using AKM 802.1X EAP SHA256
CSCwe40749	nam	File and product version mismatch for acnamihv.dll
CSCvw43299	opswat-ise	ISE posture module is not detecting SEP 14.3 build 82 installation check for macOS
CSCvx19454	opswat-ise	[ENH] Add support for Sophos Home 10.x
CSCvz20268	opswat-ise	ENH: ISE Posture does not support Google Chrome version 89
CSCvz20270	opswat-ise	ENH: ISE Posture does not support Mozilla Firefox version 87
CSCwa81027	opswat-ise	ISE Posture Patch Management Condition - add BMC Client Management Agent 20.x
CSCwb20579	opswat-ise	ISE Posture support docker desktop application for uninstall remediation
CSCwc76493	opswat-ise	Windows 11: Patch Management Check Failure
CSCwd11788	opswat-ise	OPSWAT unable to detect the FireEye after upgrade to CM version 4.3.2998.6145
CSCwd56796	opswat-ise	Wrong Windows Update Agent version is returned on Windows 11 22H2
CSCwe11588	opswat-ise	Windows Update GUI does not open when activate patch management GUI remediation is configured in ISE
CSCwe70047	posture-ise	macOS: ISE Posture not accurately detecting FileValue 'state' (On/Off)
CSCwd84695	swg	Clear the OS DNS cache when SWG becomes active

Identifier	Component	Headline
CSCwe22036	swg	Backoff SWG protection only in noNetwork, Trusted Network and VPN cases
CSCwe70156	swg	AnyConnect SWG: DNS Lookup thread exhaustion adding delay in connection establishment
CSCwe86049	swg	Handle non-success HTTP code as connection failure and enhance CP detection logic on slow CP network
CSCwe07816	umbrella	Umbrella agent crash with high rate of socket errors reported by Umbrella plugin
CSCvf70372	vpn	AnyConnect and 'AutoConnectOnStart' feature with Umbrella modules causes 'AutoConnectOnStart' to fail
CSCwd23719	vpn	VPN connection failure due to Session ID caching in cURL
CSCvy09941	vpn	vpn-session-timeout doesn't work with Untrusted Network Policy and certificate based authentication
CSCvy99392	vpn	VPN connection via local proxy does not work and fails with "Cannot connect to this gateway"
CSCwc50423	vpn	AnyConnect client is not able to restore proxy settings when the machine is powered off
CSCwc79898	vpn	AnyConnect Ubuntu 22.04 - SAML External browser does not launch
CSCwc81098	vpn	Update AnyConnect LaunchDaemon plist header syntax
CSCwc85871	vpn	ENH: Add Original Address payload for IKEv2 IPv4/IPv6 dual-stack support with public NAT on IOS-XE
CSCwd09989	vpn	AnyConnect - proxy settings are not restored correctly after machine resumes from connected standby

Identifier	Component	Headline
CSCwd15773	vpn	Sidecar and Continuity Camera video feed not working on macOS 13 with VPN connection active
CSCwd16706	vpn	Proxy settings are not being restored properly at all places (intermittently)
CSCwd17651	vpn	Management Tunnel goes down after 4-7 days and then Disconnected
CSCwd40263	vpn	Proxy settings are not being applied everywhere
CSCwd82040	vpn	Linux/Mac/iOS: TLS1.2 client connecting to TLS1.3 headend with cert auth could fail negotiation

AnyConnect 4.10.06090

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCwd34655	opswat-ise	Windows: Definition check failure with Cortex XDR
CSCwd62517	opswat-ise	Adding new "CrowdStrike Windows Sensor" application on AnyConnect Posture ISE
CSCwe05151	posture-ise	Skipping internet check while getting definition info and RTP state for EDR product
CSCwd83114	umbrella	dcp2 crash fix
CSCwe07816	umbrella	Umbrella agent crash with high rate of socket errors reported by Umbrella plugin
CSCwd82040	vpn	Linux/macOS: TLS 1.2 client connecting to TLS 1.3 headend with cert auth could fail negotiation

AnyConnect 4.10.06079

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvz84164	api	RestrictPreferenceCaching credentials still displays username when group-policy has no XMLprofile
CSCwb41421	core	CiscoSSL CVE-2022-0778
CSCvw31155	core	Multiple Certificate Validation Failure pops up when using Always On
CSCvx35970	core	AC 4.9MR5 is ignoring AuthenticationTimeout VPN profile settings
CSCwa94606	core	AnyConnect should handle null mac address in ACIDEX
CSCwb48021	core	AnyConnect: Linux/KVM - traffic destined to VM dropped by IPtables
CSCvz68411	dart	DART missing the Umbrella whitelist file
CSCwb78515	dart	DART does not collect VPN Management Tunnel mini dump crash file
CSCvz87690	download_install	AnyConnect CSD Posture assessment failed due to proxy environment variables
CSCwb74542	download_install	AnyConnect installation failed when changing date format in PC
CSCvz70357	fireamp	AMP Enabler to verify connector binary code
CSCwc13889	fireamp	Uninstallation fails with error code ValidateCodeSign failed with 4.

Identifier	Component	Headline
CSCvz53637	gui	AnyConnect: users can change preferences while UserControllable is set to False
CSCvo07690	nam	ENH: Add NAM support for automatic launch of web browser when captive portal detected
CSCvx54528	nam	AnyConnect NAM enables "Allow Connection Before Logon" automatically when upgrading to version 4.9
CSCwb14670	posture-ise	ISE does not support Windows OS Chinese edition
CSCwb64132	posture-ise	[ENH] AnyConnect shows cosmetic error message "Reassessment failed" on clients for session change
CSCwa69058	profile-editor	Standalone VPN Profile Editor for Windows only with Oracle Java
CSCwc41729	swg	Reverse DNS lookup in KDF by SWG also accommodate flow targeting IPv4-mapped IPv6 address
CSCwc53340	swg	macOS: SWG domain bypass fails intermittently for web flows targeting FQDNs with trailing dot
CSCwc61270	swg	Web Protection State not getting updated appropriately on Trusted Network
CSCwa91811	umbrella	UAC client is unable to resolve very long domain names
CSCvj04741	vpn	AC TND does not check next TrustedHttpsServer if first server hash doesn't match, moves to untrusted
CSCvx62066	vpn	ACIDEX attributes are not being retrieved by AnyConnect if device-type contains (&) character
CSCwb25527	vpn	macOS: Traffic via pre-VPN TCP connection blocked during VPN despite matching split exclude

Identifier	Component	Headline
CSCwb85473	vpn	Windows: RSAT slow when only virtual subnets are excluded from tunnel (for WSL2 interoperability)
CSCwc15262	vpn	AC 4.10 MR4 or 4.9 MR4 Cannot connect VPN using Smartcard Cert auth
CSCwc46323	vpn	Windows Integrated Authentication failure through SAML flow
CSCwc50423	vpn	AnyConnect client is not able to restore proxy settings when the machine is powered off
CSCwc64425	vpn	Zenmu Virtual Desktop and AnyConnect SAML External Browser Compatibility
CSCwd14401	vpn	Windows Always on: VPN can't connect (DNS error) after VPN disconnect and expected connect failure
CSCwa44949	web	AnyConnect: Embedded browser error for SAML authentication post upgrade to 4.10.03104
CSCwb22799	web	Embedded Browser incorrect windows size

AnyConnect 4.10.05111

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCwc03545	core	macOS 12.4: DNS outage occurs after switching to iPhone hotspot or if DNS server has IPv6 link-local
CSCwb89172	posture-ise	macOS: ISE Posture does not accurately detect FileVault 'state' (On/Off)

Identifier	Component	Headline
CSCwb67733	vpn	AnyConnect increases timeout to 120 seconds for cURL certificate signing operations
CSCwb91574	vpn	Change default setting for AllowSingleSignOnUsingOSPrimaryAccount in WebView 2

AnyConnect 4.10.05095

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCwb39828	swg	Captive portal page didn't open when SWG is enabled for both fail open/fail close.
CSCvy78997	web	Logging entry "New window not yet supported" needs to be removed from AnyConnect logs

AnyConnect 4.10.05085

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCwa59261	core	AirDrop on Big Sur (macOS 11) does not work with Split Exclude Tunnel type
CSCwa77222	core	Split-tunneling interoperability with Zentera security software
CSCvz50397	nam	Network Access Manager-authentication failed after enabling FIPS mode on NAM profile

Identifier	Component	Headline
CSCvz69614	nam	Unable to edit script for user defined network
CSCwa85342	nvm	Network Visibility Module crash observed when TND resolutions happen over TLS 1.3
CSCvy88561	opswat-ise	Fireeye security agent version 33.x is missing in latest ISE posture updates
CSCvz75848	opswat-ise	ISE compliance module v4.3.1981.4353 support for macOS version of AVG Antivirus 20.x
CSCvz75853	opswat-ise	ISE compliance module 4.3.1981.4353 support for macOS version of Avast Mac Security 15.x
CSCvz97883	opswat-ise	Windows: Cisco AMP installation check failure
CSCwa06784	opswat-ise	Windows: Patch Management check failure
CSCwa07578	opswat-ise	macOS: Compliance Module 4.3.2009.4353: Symantec Endpoint Protection: Incorrect Version
CSCwa23013	opswat-ise	Checkpoint Endpoint Security 85.x not listed in AV/AM conditions
CSCwa64826	opswat-ise	Check Point Endpoint Security 85.x and 86.x not yet supported
CSCvz74132	umbrella	macOS: acumbrellaagent.crash seen after OS update to 12 beta7
CSCvy79511	vpn	AnyConnect 4.10 still updates even if AutoUpdate is set to "false" in the profile
CSCvz51167	vpn	Chrome browser crashes after external browser authentication on macOS
CSCvz71309	vpn	BSOD (DPC_WATCHDOG_VIOLATION) during VPN session with dynamic split tunneling enabled

Identifier	Component	Headline
CSCwa62414	vpn	Windows 10: Active Directory browsing very slow with split tunneling and tunnel-all-DNS enabled
CSCwa92301	vpn	Defer upgrade prompt not shown when connecting through SBL
CSCwb06945	vpn	VPN Agent crashes when secure TND probes negotiate Poly1305 ciphers

AnyConnect 4.10.04071

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvz90541	nam	AnyConnect NAM 4.9.x/4.10.x fails authentication w/ ISE 3.1, but is successful with previous ISE versions
CSCvz17505	umbrella	Windows: Umbrella agent crash due to .NET/CLR exception in acumbrella plugin library

AnyConnect 4.10.04065

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvt36114	core	ENH: return of EXTERNAL browser support for SAML [Single-Sign-On]

Identifier	Component	Headline
CSCvt99770	core	ENH: Support for DNS load balancing/round robin with AnyConnect using SAML authentication on Windows Vulnerability
CSCvw60190	core	ENH: Management tunnel HostName entry shows in AnyConnect UI when using SBL
CSCvy23801	core	macOS 11: VPN agent crashes unexpectedly
CSCvz25236	core	Dual-stack Windows DNS resolution fails with Split-DNS or tunnel-all-DNS enabled
CSCvz67203	core	Cisco AnyConnect Secure Mobility Client for Windows Privilege Escalation
CSCvz67532	download_install	AnyConnect 4.10 downloader fails if SG name cannot be resolved and must connect via a proxy
CSCvz99382	download_install	NAM installer ADVERTISE fix does not work when deployed using SCCM
CSCvz55627	opswat-ise	Selecting ANY in Cybereason AM condition detects version 21.x when it's not listed in ISE
CSCvy92443	posture-ise	AM definition version and date info is not shown under Security Products
CSCvz79420	posture-ise	No posture discovery on machine exiting connected standby event
CSCvz37687	swg	Unable to connect to hotspots via captive portal with AnyConnect SWG Module enabled
CSCvz74132	umbrella	macOS: acumbrellaagent.crash seen after OS update to 12 beta7
CSCvm51303	vpn	ENH: Scroll bar in preferences window for AnyConnect client

Identifier	Component	Headline
CSCvp09954	vpn	Always On should limit access to headed IP address to only critical processes
CSCvv92919	vpn	ENH: SAML Auth (external IdP) with Always on Fail Close Enabled
CSCvz75859	vpn	VPN connection fails if the gateway FQDN is added as Always On host exception

AnyConnect 4.10.03104

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvy99682	api	ENH: MCA must send certificates from machine, PIV stores in order during SBL
CSCvw43009	certificate	Server certificate validation fails for IKEv2 sessions on AnyConnect 4.9 after upgrade of client
CSCvz22856	certificate	ENH: AnyConnect should set SHA-256, SHA-1 to cURL if no supported sig are provided by crypto provider
CSCvw51951	core	macOSAnyConnect crash - Exception type: EXC_CRASH (SIGABRT)
CSCvw52376	core	macOS: vpnagentd using 100% CPU during IPsec tunnel termination, excessive error logging
CSCvx36273	core	ENH: Implement exception domain validation for both Enhanced DSI/DSE
CSCvw79615	download_install	ENH: Improve AnyConnect uninstall of unsupported MSI ADVERTISE option on Windows

Identifier	Component	Headline
CSCvz27629	download_install	Issue with AnyConnect Downloader IPC
CSCvz67532	download_install	4.10 downloader fails if SG name cannot be resolved and must connect via a proxy
CSCvw50627	nam	NAM is binding to the AnyConnect virtual adapter
CSCvx65595	nvm	NVM should not rely on www.gstatic.com as a DNS connectivity test
CSCvz08505	opswat-ise	ENH: Bitdefender 9.X Antivirus for macOS
CSCvz11091	umbrella	macOS 12: acumbrellaagent crash seen intermittently on IPv4 network
CSCvy69858	vpn	Name resolution does not failback to public interface DNS servers when using split-exclude tunnel
CSCvz01007	vpn	macOS: vpndownloader crash during ASA upgrade if user hits cancel downloader log
CSCvz16781	vpn	Linux: AnyConnect is located in "Other" folder instead of "Internet"
CSCvz37517	vpn	VPN tunnel optimizations being incorrectly disabled when no customer attributes are pushed to the client
CSCvz46724	vpn	Secure TND: untrusted network incorrectly detected upon transitioning between trusted networks
CSCvz55373	vpn	VPN connection attempt fails randomly with "SSL engine encountered an error"

AnyConnect 4.10.02086

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvy60749	api	ENH: AnyConnect support for MCA during SBL using certs from machine store and smartcard
CSCvu42428	core	Multiple vulnerabilities in sqlite3 3.28.0
CSCvx65653	core	AnyConnect Profile Editor - Certificate Enrollment - Qualifier GEN and DN - Schema Validation failed
CSCvx89290	core	CIAM: sqlite 3.29.0
CSCvy23333	core	macOS 11: CPU hogged and DNS failing with link-local resolver address
CSCvy99119	core	macOS 12: VPN connection fails without IPv4 connectivity
CSCvy99325	core	macOS 12: VPN agent incorrectly reporting "no DNS connectivity" despite hosts file entry
CSCvn07053	nam	NAM fails to connect to SSID when random MAC address is enabled on Windows
CSCvy59155	nam	NAM DART file shows errors for acnamim driver
CSCvy10479	nvm	nvzFlowLoggedInUser showing "none" for system processes
CSCvu06648	opswat-ise	OPSWAT module can't read actual database release date KES 11.3
CSCvv34965	opswat-ise	Kasper Sky security center 12 support
CSCvv96231	opswat-ise	Support for Trend Micro Apex One Security Agent 16.x (Windows platform)
CSCvw81617	opswat-ise	ENH: Include support for ESET Endpoint Antivirus version 8 in ISE posture

Identifier	Component	Headline
CSCvw99789	opswat-ise	source_time and last_update returning 0 for MalwareBytes Definition check
CSCvx48049	opswat-ise	JAMF install condition is failing for users using compliance module version 4.3.1466.4353
CSCvx76435	opswat-ise	ISE posture Bitlocker condition not detecting version
CSCvx75464	opswat-ise	Definition check failing for Trend Micro Apex One (macOS) 3.x
CSCvy14274	opswat-ise	GetDefinitionState for FireEye Endpoint Agent is stuck - CM 4.3.1614.6145 on Windows
CSCvy18948	opswat-ise	Windows: Delay in definition check for CrowdStrike Falcon
CSCvy30728	opswat-ise	Opswat support for KES 21.3.10.394
CSCvy37094	opswat-ise	ESET AM active scan protection issue on HostScan
CSCvy37121	opswat-ise	HostScan 4.9.06046 returning current date/time as Definition date for Cybereason ActiveProbe
CSCvy51930	opswat-ise	CM to support Manage Engine Manager Plus to manage Windows Updated for posture
CSCvw60979	posture-ise	ENH: Message change request "Your network is configured to use Cisco NAC Agent"
CSCvy42987	posture-ise	Mandate CM version to be downloaded for macOS endpoints
CSCvy44614	posture-ise	Move sensitive logs to encrypted logs in aciseagent
CSCvy38455	profile-editor-wer	AnyConnect Local Policy Editor 4.10 not showing "Restrict Server Cert Store" parameter
CSCvz11091	umbrella	macOS12: acumbrellaagent crash seen intermittently on IPv4 network with IPv6 custom resolver

Identifier	Component	Headline
CSCvv74971	vpn	AnyConnect Mobility Client can be used to add entries to the windows host file
CSCvx92746	vpn	No failover to secondary SG address once reachable if promoted primary SG address is unreachable
CSCvy10495	vpn	macOS 11: VMware Fusion guest loses network connectivity with VPN running on host
CSCvy24725	vpn	AnyConnect client is stuck in 'Optimizing connection...' or 'Disconnecting' state
CSCvy32808	vpn	AnyConnect notification popup appears in wrong location on 6K monitor
CSCvy34972	vpn	New virtual if. subnet route removed by AnyConnect route correction despite LocalLAN split exclude
CSCvy60649	vpn	WinINet proxy options must be set from user space
CSCvy86968	vpn	macOS 12 beta: VPN connection fails with IPv4 LocalLAN split exclude
CSCvt10982	web	ENH: (Windows Platform) AnyConnect embedded browser support for multiple windows "pop-up"

AnyConnect 4.10.01075

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvw81982	core	ENH: Windows 10 VPN tunnel should capture WSL (Windows Subsystem for Linux 2) traffic
CSCvx31341	core	macOS 11: After upgrade, VPN connection to DST-enabled headend fails with "DNS component" error
CSCvx58220	core	Windows update issue when AnyConnect Management VPN tunnel is in use
CSCvx89289	core	AnyConnect openssl 1.1.1k update
CSCvy07747	core	macOS: VPN connction fails with 2 default routes on public interface after incorrect router restore
CSCvw22016	down_install-wer	macOS privilege escalation exploitable through Cisco AnyConnect Secure Mobility Client
CSCvy04232	download_install	AnyConnect VPN installer prevents install on Windows 10 ARM64 insiders with x64 emulation
CSCvw94933	nam	Implement additional translations for strings related to NAM prompts
CSCvw30775	nvm	NVM does TND check when connected to VPN right after NVM service restart
CSCvx57786	nvm	NVM trusted server retry interval
CSCvx77722	nvm	Linux: Not working after kernel update
CSCvu06648	opswat-ise	OPSWAT module can't read database release date KES 11.3
CSCvw81049	opswat-ise	OPSWAT fails to detect actual version of KES 11.5.0.590 instead it detects incorrect version 21.2.x
CSCvo36890	posture-ise	[IPv6] ISE Posture discovery is in infinite loop due to specific IPv6 networks [MS Teredo]

Identifier	Component	Headline
CSCvx56591	posture-ise	Cisco AnyConnect posture bypass vulnerability
CSCvx57152	posture-ise	Retrieve AM definition info only if AM definition condition is configured
CSCvx58922	posture-ise	ENH: Retaining iseposture folder files after ISE posture module version upgrade
CSCvx70102	posture-ise	Missing signature verification for one dll
CSCuq89328	vpn	ENH: Enhance split DNS so that you can exclude domain names vs include
CSCvt21946	vpn	ENH: Reduce time taken for the AnyConnect MTU discovery process
CSCvt21979	vpn	ENH: Do not show "Connected" in AnyConnect until the MTU discovery process completes
CSCvv93458	vpn	ENH: AnyConnect restarts VPN tunnel when temporary IPv6 addresses are created/modified
CSCvv95822	vpn	AnyConnect does not send tunnel-group attribute while connecting to backup server from XML profile
CSCvw96507	vpn	macOS ENH: Ensure VPN tunnel DNS configuration remains valid after network interface changes
CSCvx32879	vpn	ENH: Increase the password entropy for ciscoacvpnuser to match the BitLocker recovery key entropy
CSCvx42883	vpn	Internet Explorer (IE) proxy settings are not being restored for remote logins
CSCvx81669	vpn	ENH: Detect VPN adapter address assignment as per Microsoft recommendation

Identifier	Component	Headline
CSCvx85975	vpn	macOS: DST domain resolutions time out after 50+ awd10 addr. refreshes (high DST exclusion rate)
CSCvx87886	vpn	Tunnel disconnects automatically due to Downloader crash on 4.10 FCS
CSCvx92871	vpn	macOS 11: AnyConnect extension crashes upon unexpected disabling

AnyConnect 4.10.00093

The Cisco Bug Seach Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvx63335	certificate	Windows: AnyConnect randomly throws 'Certificate has expired' error
CSCvx78941	certificate	AnyConnect's code signing certificate needs to be updated due to Symantec Root CAs distrust
CSCvs75542	core	ENH: Support for Enhanced Captive Portal Remediation on macOS
CSCvu14938	core	Cisco AnyConnect Secure Mobility Client for Windows Profile folder modification vulnerability
CSCvu78363	core	AnyConnect Start Before Logon (SBL) displays incorrect name when Native VPN client is configured
CSCvv30103	core	Cisco AnyConnect Secure Mobility Client Arbitrary Code Execution Vulnerability
CSCvw16391	core	UI loses IPC/TCP channel with Agent after keepidle timer is blocked by third-party firewall(s)

Identifier	Component	Headline
CSCvw16601	core	AnyConnect does not fallback to IPv6 when using IPSec/IKEv2
CSCvw29572	core	Cisco AnyConnect Secure Mobility Client Denial of Service Vulnerability
CSCvx04208	core	macOS: WebEx app call interruptions with high rate and/or count of dynamic tunnel inclusions
CSCvx55399	core	When HostScan enable + tunnel-group-list disable, default tunnel group was selected
CSCvw21825	down_install-wer	Cisco AnyConnect Secure Mobility file overwrite vulnerability
CSCvx23656	download_install	Failed to launch downloader due to proxy environment variables
CSCvr54037	nam	Network Access Manager PE not saving user defined EKU for Cert Matching Rule-Machine EAP-TLS
CSCvw63452	nam	NAM bind control DLL deleted during upgrade of Network Access Manager from versions that used DIFxAPI
CSCvx25251	nvm	NVM installation fails with latest kernel version of Ubuntu 20
CSCvw08005	opswat-ise	ISE posture module is not detecting SEP version 14.3.1148.0100
CSCvt26597	posture-ise	ENH: ISE Posture Module support in Linux OS
CSCvu23579	vpn	ENH: Permit 20,000 characters in Dynamic Split Tunnel list
CSCvv61677	vpn	device-mac/device-public-mac ACIDEX attributes are not sent from AnyConnect when using Bluetooth NIC
CSCvw92182	vpn	AnyConnect on macOS connected to the ASA tls-only is reconnecting ~ 20s after connected

Identifier	Component	Headline
CSCvw96331	vpn	Linux: Update Policy, Software and Profile lock feature is broken
CSCvx04190	vpn	anyconnect_global file corrupt after connecting with vpncli on Linux when using OGS
CSCvx20136	vpn	DNS queries are failing for some FQDNs after waking from sleep on macOS Big Sur with AnyConnect 4.9
CSCvx27372	vpn	macOS: Connectivity lost after connected for a while to DST-enabled headend (low TTL DST domains)
CSCvx65570	vpn	AnyConnect UI shows blank "Connect To:" on Linux when no profile is used

HostScan 4.10.08029

Caveats describe unexpected behavior or defects in Cisco software releases.

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvz19204	opswat-asa	ENH: Need to add support of "Sophos Endpoint" Antimalware 10.1.x for macOS on HostScan
CSCwh68527	opwat-asa	This is an ENH to add support for Sophos Endpoint Agent 2023.1.3.5 on AnyConnect and CSC

HostScan 4.10.08025

Caveats describe unexpected behavior or defects in Cisco software releases.

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvz19204	opswat-asa	ENH: Need to add support of "Sophos Endpoint" Antimalware 10.1.x for macOS on HostScan
CSCwb54510	opswat-asa	HostScan fails to detect ESET AM active scan after upgrade to Windows 10 despite fix for CSCvy37094
CSCwd39477	opswat-asa	Sophos Endpoint Agent 2022.2.1.9 fails definition check with Secure FW Posture (HostScan) 5.0.00529
CSCwf09464	opswat-asa	ENH: Support for McAfee LiveSafe - Internet Security version 16.0 R51
CSCwf52023	opswat-asa	HostScan 4.10.x firewall state and active scan check cause unexpected delays with Crowdstrike Falcon
CSCwf70012	opswat-asa	HostScan getting stuck in definition check for TrendMicro Apex One
CSCwh25309	opswat-asa	ENH: HostScan to add support for Sophos Endpoint Agent 2023.1.2.3 on AnyConnect 4.10
CSCwc62461	posture-asa	When logging into ASDM pop up for HostScan - image doesn't include important security fixes
CSCwf35884	posture-asa	ASDM UI to Skip internet check for EDR products
CSCwh71692	posture-asa	HostScan: Periodic polling adding extra header on every 60 second assessment

HostScan 4.10.07073

HostScan 4.10.07073 includes updated OPSWAT engine versions for Windows, macOS, and Linux. Refer to the HostScan Support Charts under Release and Compatibility for additional information.

HostScan 4.10.07061

Caveats describe unexpected behavior or defects in Cisco software releases.

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCwc37015	opswat-asa	ENH: HostScan support for Cybereason ActiveProbe Antimalware 21.2.270+ on macOS
CSCwd05214	opwat-asa	ENH: Add support for firewalld 1.1.x & 1.2.x
CSCwd94368	opswat-asa	ENH: HostScan support for Cisco Secure Endpoint 7.5.5.21061
CSCwe21646	opswat-asa	AnyConnect - Microsoft blocks access due to cscan polling URL for Internet Access test
CSCwe34677	opswat-asa	Latest HostScan versions do not support 13.2 Gatekeeper version on macOS
CSCwe51207	opswat-asa	ENH: HostScan 4.10 should support latest version of CrowdStrike for Linux
CSCwf98852	opswat-asa	Trellix Security Agent incorrectly identified as outdated product McAfee Security Agent
CSCwe25243	posture-asa	Skip OPSWAT internet connectivity check after vpn-user is logged in

HostScan 4.10.06090

HostScan 4.10.06090 includes updates to the OPSWAT engine versions for Windows, macOS, and Linux. Refer to the HostScan Support Charts under Release and Compatibility for additional information.

HostScan 4.10.06083

Caveats describe unexpected behavior or defects in Cisco software releases.

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCwd44206	opswat-asa	HostScan: firewalld prompts for system credentials after upgrade to HostScan version 4.10.05111

HostScan 4.10.06081

Caveats describe unexpected behavior or defects in Cisco software releases.

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvy87936	opswat-asa	Mac 12 support for the OPSWAT ISE and HS
CSCvz70815	opswat-asa	Need to add support for Cisco Secure Endpoint (antimalware) on HostScan for Windows and macOS
CSCwa32346	opswat-asa	ENH: HostScan support for Microsoft Defender Threat Protection (ATP) for macOS endpoints
CSCwc37015	opswat-asa	ENH: HostScan support for Cybereason ActiveProbe Antimalware 21.2.270+ on macOS
CSCwc62378	opwat-asa	Libwalocal.dll crash causes HostScan to hang and token validation to fail
CSCvy30093	posture-asa	HostScan unable to retrieve Certification information from Linux endpoints
CSCwb38379	posture-asa	On macOS clients, VPN is getting timeout with cscan crash observed on console logs
CSCwc68714	posture-asa	ENH: HostScan image to support Sophos Endpoint Agent version 2022.2.1.9

HostScan 4.10.05111

Caveats describe unexpected behavior or defects in Cisco software releases.

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCwb45946	opswat-asa	Windows: HostScan authentication timeout when preventing access to command prompt

Refer to the HostScan Support Charts under Release and Compatibility for additional information.

HostScan 4.10.05095

HostScan 4.10.05095 includes updated OPSWAT engine versions for Windows, macOS, and Linux. Refer to the HostScan Support Charts under Release and Compatibility for additional information.

HostScan 4.10.05085

Caveats describe unexpected behavior or defects in Cisco software releases.

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvz73177	opswat-asa	Windows: Compliance Module libraries initialization issue

HostScan 4.10.04071

Caveats describe unexpected behavior or defects in Cisco software releases.

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvz69382	opswat-asa	ENH: Support for detecting Bitdefender Endpoint Security version 7.2.2.90 via HostScan

HostScan 4.10.04065

Caveats describe unexpected behavior or defects in Cisco software releases.

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvy53770	opswat-asa	HostScan 4.10.x versions returning last update="2" for Crowdstrike Falcon on macOS
CSCvz63025	posture-asa	Running HostScan on Linux will launch Pacman game if it is installed

HostScan 4.10.03104

Caveats describe unexpected behavior or defects in Cisco software releases.

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvx38469	opswat-asa	AnyConnect should use '-n' while checking iptables
CSCvx75497	posture-asa	HostScan process check fails to detect running process with long name on macOS
CSCvy52914	posture-asa	Enhancement to support multi-string value type for registry

Identifier	Component	Headline
CSCvz38526	posture-asa	Multiple download retries
CSCvz38540	posture-asa	Log curl operations on demand

HostScan 4.10.02089

Caveats describe unexpected behavior or defects in Cisco software releases.

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvx38469	opswat-asa	AnyConnect should use 'n' while checking iptables
CSCvy52914	posture-asa	Enhancement to support multi-string value type for registry

HostScan 4.10.02086

Caveats describe unexpected behavior or defects in Cisco software releases.

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvx65190	posture-asa	"HostScan is waiting for the next scan" message is misleading
CSCvy54697	posture-asa	Wildcard support for registry check
CSCvy54733	posture-asa	Environment variable expansion for file check on Windows

HostScan 4.10.01094

Caveats describe unexpected behavior or defects in Cisco software releases.

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvx41020	opswat-asa	Windows delay in OPSWAT with Cybereason ActiveProbe
CSCvy21260	opswat-asa	Windows: 30 second delay in version check for Windows Defender
CSCvy37121	opswat-asa	HostScan 4.9.06046 returning current date/time as Definition date for Cybereason ActiveProbe

HostScan 4.10.01075

Caveats describe unexpected behavior or defects in Cisco software releases.

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvu75511	opswat-asa	ENH: HostScan support for Microsoft Defender Advanced Threat Protection (ATP) for Linux endpoints
CSCvx38993	posture-asa	HostScan unable to retrieve the serial number of macOS Big Sur with Apple MR1 chip inserted
CSCvx82055	posture-asa	AnyConnect 4.9.06037 with HostScan 4.9.06046 stuck in "HostScan state idle" on Oracle Linux 7.9

HostScan 4.10.00093

Caveats describe unexpected behavior or defects in Cisco software releases.

The Cisco Bug Search Tool has detailed information about the following open and resolved caveats in this release. A Cisco account is required to access the Bug Search Tool. If you do not have one, register at https://Cisco.com.

Resolved

Identifier	Component	Headline
CSCvx38993	posture-asa	HostScan unable to retrieve the serial number of macOS Big Sur with Apple M1 chip inserted
CSCvx82055	posture-asa	AnyConnect 4.9.06037 with HostScan 4.9.06046 stuck in "HostScan state idle" on Oracle Linux 7.9

Related Documentation

Other AnyConnect Documents

- Cisco AnyConnect Secure Mobility Client Administrator Guide
- Cisco AnyConnect Secure Mobility Client Features, Licenses, and OSs
- Open Source Software Used in AnyConnect Secure Mobility Client
- Cisco General Terms, AnyConnect Secure Mobility Client, Release 4.x

ASA Related Documents

- Release Notes for the Cisco ASA Series
- Navigating the Cisco ASA Series Documentation
- Cisco ASA 5500-X Series Next-Generation Firewalls, Configuration Guides
- Supported VPN Platforms, Cisco ASA 5500 Series
- HostScan Support Charts

ISE Related Documents

- Release Notes for Cisco Identity Service Engine