Configure Posture

The AnyConnect Secure Mobility Client offers a VPN Posture/HostScan Module and an ISE Posture Module. Both provide the AnyConnect with the ability to assess an endpoint's compliance for things like antivirus, antispyware, and firewall software installed on the host. You can then restrict network access until the endpoint is in compliance or can elevate local user privileges so they can establish remediation practices.

VPN Posture is bundled with hostscan_version.pkg, which is the application that gathers what operating system, antivirus, antispyware, and software is installed on the host. ISE Posture deploys one client when accessing ISE-controlled networks, rather than deploying both AnyConnect and the NAC Agent. ISE Posture is a module you can choose to install as an additional security component into the AnyConnect product.

ISE Posture performs a client-side evaluation. The client receives the posture requirement policy from the headend, performs the posture data collection, compares the results against the policy, and sends the assessment results back to the headend. Even though ISE actually determines whether or not the endpoint is compliant, it relies on the endpoint's own evaluation of the policy.

In contrast, HostScan performs server-side evaluation where the Secure Firewall ASA asks only for a list of endpoint attributes (such as operating system, IP address, registry entries, local certificates, and filenames), and they are returned by HostScan. Based on the result of the policy's evaluation, you can control which hosts are allowed to create a remote access connection to the security appliance.

Note The combined use of HostScan and ISE posture agent is not supported. Unexpected results occur when two different posture agents are running.

The following posture checks are supported in HostScan but not ISE Posture: Hostname, IP address, MAC address, port numbers, OPSWAT version, BIOS serial number, and certificate field attributes.

- What ISE Posture Module Provides, on page 2
- Operations That Interrupt AnyConnect ISE Flow, on page 9
- Status of ISE Posture, on page 10
- Script Remediation Messaging, on page 12
- Posture Condition Script, on page 13
- Posture and Multi Homing, on page 13
- Simultaneous Users on an Endpoint, on page 13
- Logging for Posture Modules, on page 13
- Posture Modules' Log Files and Locations, on page 14
- ISE Posture Profile Editor, on page 14

• Advanced Panel , on page 17
• What VPN Posture Module Provides, on page 17
• OPSWAT Support, on page 20

What ISE Posture Module Provides

Posture Checks

The ISE Posture module uses the OPSWAT v3 or v4 library to perform posture checks. With an initial posture check, any endpoint that fails to satisfy all mandatory requirements is deemed non-compliant. The other endpoint authorization states are posture unknown or compliant (meeting mandatory requirements).

Note With the macOS 64-bit migration, AnyConnect ISE posture module is not compatible with older OPSWAT v3 compliance modules.

If an error occurs during the posture checking phase and AnyConnect is able to continue, the user is notified, but posture checking continues, if possible. If the error occurs during a mandatory posture check, the check is marked as failed. Network access is granted if all mandatory requirements are satisfied. If not, the user can restart the posture process.

Any Necessary Remediation

The remediation window runs in the background so that the updates on network activity don't pop up and interfere or cause disruption. You can click **Details** in the ISE Posture tile portion of the AnyConnect UI to see what has been detected and what updates are needed before you can join the network. If a required manual remediation is necessary, the remediation window opens, displaying the items that require action. This System Scan window shows the progress of the updates, the time left of the allotted update time, the status of any requirements, and the system compliance state.

Note Applications which require elevated privileges use automatic remediation only with non-administrator user accounts. Administrator accounts must perform remediation manually.

Note Posture checks and remediations that require elevated privileges will only be executed if the server is trusted.

When only optional updates are left, you can choose to **Skip** to the next one or **Skip All** to disregard all remaining remediations. You can skip the optional remediations in the interest of time and still maintain network access.

After remediation (or after requirement checks when no remediation was needed), you may get an Acceptable Use Policy notification. It requires you to accept the policy for network access and limits access if you reject it. During this part of remediation, the Posture tile portion of the AnyConnect UI displays "System Scan: Network Acceptable Use Policy."

When remediation is complete, all of the checks listed as required updates appear with a Done status and a green checkbox. After remediation, the agent sends the posture result to ISE.

Patch Management Checks and Remediation

AnyConnect with a Patch Management agent provides patch management checks and patch management remediation. It checks the state of patches missing on the endpoint. If no patches are missing on the endpoint, the patch management check passes. You can use the Patch Management agent to install the missing patches, if configured. The ISE server must be trusted for these advanced check and remediation operations.

When a client installs a patch whose installation occurs before a reboot, the client reports the installation status (installed or not installed) of the patch when the machine reboots. However, when a client installs a patch whose installation starts *after* a reboot, the client doesn't report the status of the patch immediately.

The AnyConnect compliance module can't force the client to provide any status at this point. The amount of time that a posture module client takes to complete native API requests is a function of different dynamic OS parameters (such as CPU load, number of pending patches, no restarts after patch installation, and so on) and network factors (such as connectivity and latency between posture module client and server). You may have to wait for the client to respond, but some lab results with known patches have been about ten minutes.

A similar behavior is also observed with Windows Server Update Services (WSUS) search APIs taking more time to respond, sometimes 20 to 30 minutes. Windows Update checks for missing patches of all Microsoft products (such as Microsoft Office), not only for Windows OS. The APIs used for condition and remediation are unreliable, and you could see unexpected behavior. We recommend that you use a Patch Management condition and remediation instead, for the validation of patches on Windows platforms.

Refer to Policy Conditions to learn how to set up policy conditions on ISE or Patch Management Remediation for further information on patch management remediation.

Reassessment of Endpoint Compliance

After the endpoint is deemed compliant and is granted network access, the endpoint can optionally be periodically reassessed based on what controls the administrator configured. The passive reassessment posture checks differ from the initial posture checks. If any fail, the user is given the option to remediate, if the administrator had the setting configured as such. The configuration settings control whether or not the user maintains trusted network access, even when one or more mandatory requirements have not been met. With initial posture assessment, failing to satisfy all mandatory requirements deems the endpoint non-compliant. This feature is set to disabled by default, and if enabled for a user role, it reassesses the posture every 1 to 24 hours.

The administrator can set the outcome to Continue, Logoff, or Remediate and can configure other options such as enforcement and grace time.

You can use the ISE UI to create more informative messages that are displayed in VPN Posture profiles. The button text and links are also customizable.

Grace Period for Noncompliant Devices

You can set up a grace period in the Cisco ISE UI. With this configured, an endpoint that becomes non-compliant, but was compliant in a previous posture status, can be granted access to the network. Cisco ISE looks for the previously known good state in its cache and provides grace time for the device. When the grace period expires, AnyConnect performs the posture check again, this time with no remediation, and determines the endpoint state as compliant or non-compliant based on the results of the check.

Note The following happens when a device is in grace period but is updated in the posture policy:

- *(If the grace period is extended),* the new grace period is applied when the earlier grace period elapses or the device is deleted from ISE.
- *(If the grace period is reduced),* the new grace period is applied to the device only if the device goes through the posture flow process again.

Grace period is not applicable for the temporal agent, hardware inventory, and application monitoring.

Periodic reassessment (PRA) is not applicable when a user is in a grace period.

When a device matches multiple posture policies (with each policy having a different grace period), the device gets the maximum grace period configured among the different policies.

The Acceptable Use Policy (AUP) is not displayed when the device is moved to the grace period.

The grace period is set under the VPN Posture profile on the ISE UI in **Policy > Posture or Work Centers > Posture > Posture Policy.** Valid values are specified in days, hours, or minutes. By default, this setting is disabled.

Flexible Notification

You can use the Delay Notification option to delay the display of the custom notification window until a specific percentage of grace period has elapsed. For example, if the Delay Notification field on the ISE UI is set to 50% and the configured grace period is 10 minutes, ISE Posture rescans the endpoint after 5 minutes and displays the notification window if the endpoint is found to be noncompliant. The notification window is not displayed if the endpoint status is compliant. If the notification delay period is set to 0%, the user is prompted immediately at the beginning of the grace period to remediate the problem. The endpoint is granted access until the grace period expires.

The AnyConnect UI pops up a caution when an endpoint is noncompliant only when the custom notifications are configured on the ISE UI. A notification also indicates the start of grace period and any endpoints that are non-compliant after the grace period start. The AnyConnect System Scan tile highlights all of the posture failures, and you can hit the **Scan Again** button to maintain full network access by forcing a rerun of the posture policies.

Note For the Scan Again option to appear, the Enable Rescan Button option must be set to Enabled.

In a remediation flow, you are basically blocked from access until you fix the issue. No temporary access is available. In a grace period flow, you can get deferred access, providing you a grace period to fix the issue. If you click the **Launch Browser** option in the flexible notification flow, you can launch a browser, if the server is trusted. The browser option allows you to get additional details about complying with posture policies.

Cisco Temporal Agent

The Cisco Temporal Agent is designed for Windows or macOS environments to share compliance status when a user accesses a trusted network. The configuration for the Cisco Temporal Agent is done on the ISE UI. The Cisco Temporal Agent extractable .exe (for Windows) or dmg (for macOS) is downloaded to the endpoint

whenever it attempts to access the internet. The users must run the downloaded executable or dmg for the compliance check: no administrator privileges are required.

The UI is then automatically launched and starts the check to determine if the endpoint is compliant or not. After completing the compliance checks, based on how the policies are configured on the ISE UI, ISE can take any necessary action.

In Windows, the executable is self extractable and all of the necessary dll and other files for compliance check are put into the temporary folder with this extraction. All of the extracted files and executables are deleted after the completion of the compliance check. For complete removal of the files and executables, the user must quit the UI.

Refer to Cisco Temporal Agent Workflows in the *Cisco Identity Services Engine Administrator Guide* for detailed configuration steps on the ISE UI.

Limitations of Cisco Temporal Agent

- A VLAN-controlled posture environment for temporal agent is not supported in macOS because the refresh adapter (DHCP renewal) process cannot occur without root privileges. The temporal agent can run as a user process only. An ACL-controlled posture environment is supported because it does not require refreshing the IP of the endpoint.
- If a network interface happens during remediation, the user must quit the current UI and redo the whole procedure.
- In macOS, the dmg file will not be deleted.
- After launching the temporal agent installer, it may hide behind the browser when running on the endpoint. To proceed with collecting health on the temporal agent application, the end user should minimize the browser. Mostly Windows 10 users have this issue because UAC mode is set to high on those clients, to accept the third-party application that is running with high security conditions.
- You cannot use temporal agent when stealth mode is enabled on the endpoint.
- The following conditions are unsupported by the Cisco Temporal Agent:
    - Service Condition-macOS—System Daemon check
    - Service Condition-macOS—Daemon or User Agent check
    - PM—Up to Date check
    - PM—Enabled check
    - DE—Encryption Location based check

Posture Policy Enhancements for Optional Mode

You can perform remediation for failed requirement checks in Optional Mode, regardless of whether mandatory checks passed or failed. A message about remediation is presented on the AnyConnect ISE Posture UI, and you can see what failed and what requires remediation action.

- Manual Remediation of Optional Mode—The System Scan Summary screen shows any Optional Mode status that may require remediation if a condition failed. You can manually click Start to remediate or click Skip. Even if the remediation fails, the endpoint would still be compliant since these are only optional requirements. The System Scan Summary shows if they are skipped, failed, or successful.

- Automatic Remediation of Optional Mode—You can monitor the System Scan tile as it notes when it is applying optional updates. You will not be asked to start remediation because it happens automatically. If any automatic remediation fails, you get a message that remediation could not be attempted. Further, you have a choice to skip the remediation action, if desired.

Visibility into Hardware Inventory

An Endpoints > Hardware tab has been added under Context Visibility on the ISE UI. It helps you collect, analyze, and report endpoint hardware information within a short time. You can gather information such as finding endpoints with low memory capacity or finding the BIOS model/version in an endpoint. Based on the findings, you can increase the memory capacity, upgrade the BIOS version, or assess the requirements before you plan the purchase of an asset. The Manufacturers Utilization dashlet displays hardware inventory details for endpoints with Windows or macOS, and the Endpoint Utilizations dashlet displays the CPU, Memory, and Disk utilization for endpoints. Refer to The Hardware Tab of the *Cisco Identity Services Engine Administrator Guide* for detailed information.

Stealth Mode

An administrator can configure ISE Posture while the AnyConnect UI tile is hidden from the end user client. No popups are shown, and any scenarios which require user intervention will take the default action. This feature is available on Windows and macOS operating systems.

Refer to the *Configure Posture Policies* section in the Cisco Identity Services Engine Administrator Guide where you specify stealth mode in the clientless state as disabled or enabled.

On the ISE UI, you can set stealth mode to have notifications enabled so that end users still see error notifications.

After you map the profile in the ISE Posture Profile Editor, on page 14 and then map AnyConnect configuration to the Client Provisioning page in ISE, AnyConnect can read the posture profile, set it to the intended mode, and send information related to the selected mode to ISE during initial posture request. Based on the mode and other factors, such as identity group, OS, and compliance module, Cisco ISE matches to the right policy.

Refer to the stealth mode deployment and its impact in the Cisco Identity Services Engine Administrator Guide.

ISE Posture does not allow you to set the following functions in stealth mode:

- Any manual remediation
- Link remediation
- File remediation
- WSUS show UI remediation
- Activate GUI remediation
- AUP policy

Posture Policy Enforcement

To improve the overall visibility of the software installed on your endpoints, we have provided these posture enhancements:

- You can check the state of an endpoint firewall product to see if it is running. If desired, you can enable the firewall and enforce policies during initial posture and periodic reassessment (PRA). To set, see the *Firewall Condition Settings* section in the Cisco Identity Services Engine Configuration Guide.
- Similarly, you can run a query of applications that are installed on an endpoint. If an unwanted application is running or installed, you can stop the application or uninstall the unwanted application. To set, see the *Application Remediation* section in the Cisco Identity Services Engine Configuration Guide section in the ISE UI.

UDID Integration

When AnyConnect is installed on a device, it will have its own unique identifier (UDID) shared among all modules in AnyConnect. This UDID is an identifier for the endpoint and is saved as an endpoint attribute, which ensures posture control on a specific endpoint rather than on a MAC address. You can then query endpoints based on the UDID, which is a constant that won't change regardless of how the endpoint connects, or upon upgrade or uninstallation. The Context Visibility page on the ISE UI **(Context Visibility > Endpoints > Compliance)** can then display one entry instead of multiple entries for endpoints with multiple NICs.

Application Monitoring

The posture client can continuously monitor different endpoint attributes so that dynamic changes are observed and reported back to the policy server. Depending on how the posture policy is configured, you can monitor different attributes such as what applications are installed and running for antispyware, antivirus, antimalware, firewall, and so on. Refer to the *Continuous Endpoint Attribute Monitoring* section in the Cisco Identity Services Engine Administrator Guide for details about the application condition settings.

USB Storage Device Detection

When a USB mass storage device is attached to a Windows endpoint, a posture client is able to detect it and either block or allow the device depending on the posture policy block. With the USB detection, the agent continuously monitors the endpoint as long as it remains in the same ISE-controlled network. If a USB device matching the criteria is connected within this time period, the specified remediation action is performed. The incident is also reported to the policy server.

USB storage detection relies on the OPSWAT v4 compliance module. You must configure the USB check in the periodic reassessment policy (PRA) on the ISE UI at **Work Centers > Posture > Policy Elements > USB**.

Note The checks and remediation are performed sequentially, so setting the PRA grace time to a minimal number for other checks prevents delays in handling USB checks. The grace time is set on the ISE UI in **Work Centers > Posture > Settings > Reassessment Config**.

Refer to USB Mass Storage Check Workflow for steps on configuring the detection of USB storage on the ISE UI.

Automatic Compliance

With posture lease, the ISE server can skip posture completely and simply put the system into compliant state. With this functionality, users do not experience delays switching between networks when their system has recently been postured. The ISE Posture agent simply sends a status message to the UI shortly after the ISE server is discovered, indicating whether the system is compliant. In the ISE UI (in Settings > Posture > General Settings), you can specify an amount of time when an endpoint is considered posture compliant after an initial compliance check. The compliance status is expected to be preserved even when users switch from one communicating interface to another.

In a Posture lease-enabled environment, users will have permit access when connecting during the lease period. Because of the absence of the redirect ACL, redirect probes such as DiscoveryHost and DefaultGateway will not function during the discovery phase. If the Posture profile setting *Enable extra probes so non-redirection flow can work* is disabled, the Posture agent will only rely on the previously connected PSN for discovery. In these scenarios, you must enable non-redirection-based discovery for the posture discovery to use the call home list and previously connected PSNs.

Note With a posture lease, if the session is valid on ISE, the endpoint is expected to go from posture unknown state to compliant state.

VLAN Monitoring and Transitioning

Some sites use different VLANs or subnets to partition their network for corporate groups and levels of access. A change of authorization (CoA) from ISE specifies a VLAN change. Changes can also happen due to administrator actions, such as session termination. To support VLAN changes during wired connections, configure the following settings in the ISE Posture profile:

- VLAN Detection Interval— Determines the frequency with which the agent detects a VLAN transition and whether monitoring is disabled. VLAN monitoring is enabled when this interval is set to something besides 0. Set this value to at least 5 for macOS.

  VLAN monitoring is implemented on both Windows and macOS, although it is only necessary on macOS for the detection of unexpected VLAN changes. If a VPN is connected or an acise (the main AnyConnect ISE process) is not running, it disables automatically. The valid range is 0 to 900 seconds.

- Enable Agent IP Refresh—When unchecked, ISE sends the Network Transition Delay value to the agent. When checked, ISE sends DHCP release and renew values to the agent, and the agent does an IP refresh to retrieve the latest IP address.

- DHCP Release Delay and DHCP Renew Delay— Used in correlation with an IP refresh and the Enable Agent IP Refresh setting. When you check the Enable Agent IP Refresh checkbox and this value is not 0, the agent waits for the release delay number of seconds, refreshes the IP addresses, and waits for the renew delay number of seconds. If a VPN is connected, IP refresh is automatically disabled. If 4 consecutive probes are dropped, it triggers a DHCP refresh.
- Network Transition Delay— Used when VLAN monitoring is disabled or enabled by the agent (in the Enable Agent IP Refresh checkbox). This delay adds a buffer when a VLAN is not used, giving the agent an appropriate amount of time to wait for an accurate status from the server. ISE sends this value to the

agent. If you also have the Network Transition Delay value set in the global settings on the ISE UI, the value in the ISE Posture Profile Editor overwrites it.

Note The Secure Firewall ASA does not support VLAN changes, so these settings do not apply when the client is connected to ISE through a Secure Firewall ASA.

Troubleshooting

If the endpoint device cannot access the network after posture is complete, check the following:

- Is the VLAN change configured on the ISE UI?
  - If yes, is DHCP release delay and renew delay set in the profile?
  - If both settings are 0, is Network Transition Delay set in the profile?

Operations That Interrupt AnyConnect ISE Flow

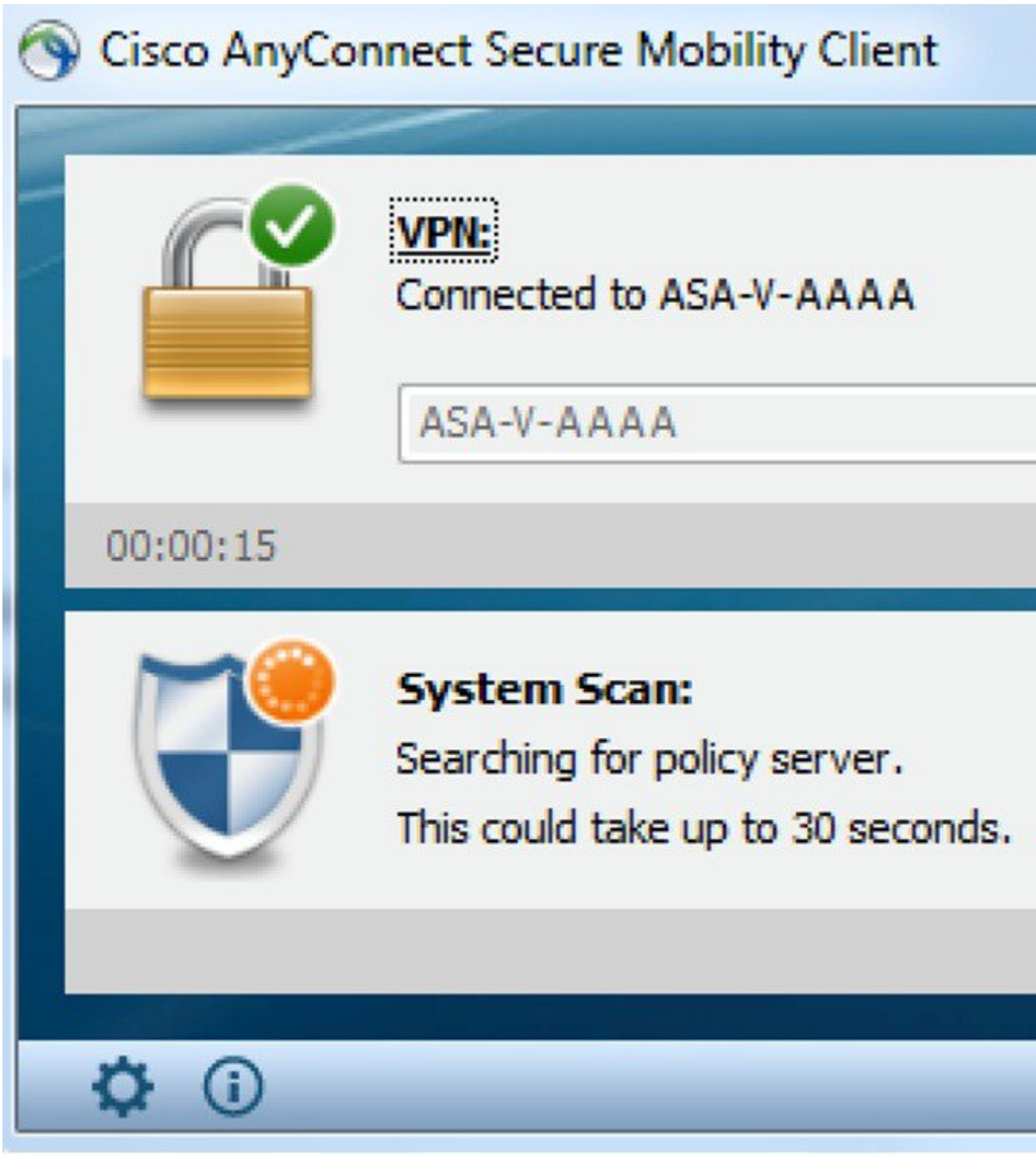
For various reasons, AnyConnect ISE Posture flow can be interrupted during either initial posture reassessment or passive reassessment.

- User Cancels AnyConnect ISE—During the period of posture checking and remediation, the user can cancel AnyConnect ISE. The UI immediately notifies a user that a cancellation is in progress, but it should occur only during a time that avoids putting the endpoint into a questionable state. Some cancellations may require a reboot if third-party software was used. The ISE Posture tile portion of the AnyConnect UI shows the compliance state after the cancellation.
- Remediation Timer Expires—The administrator-controlled time to satisfy posture requirements has expired. An assessment report is sent to the headend. During passive reassessment, the user retains network access, and with posture assessment, network access is granted when all mandatory requirements are satisfied.
- Error During Posture Checking—If an error occurs during the posture checking phase and AnyConnect is able to continue, the user is notified, but posture checking continues, if possible. If the error occurs during a mandatory posture check, the check is marked as failed. Network access is granted if all mandatory requirements are satisfied. If not, the user can restart the posture process.
- Error During Remediation—If an error occurs during the remediation phase and AnyConnect ISE Posture can continue, the user is notified. AnyConnect ISE Posture stops the remediation process if the failed remediation step is associated with a mandatory posture requirement. If the failed remediation step is associated with an optional posture requirement, it attempts to continue with the next step and finish the ISE Posture operation. Network access is granted if all mandatory requirements are satisfied. If not, the user can restart the posture process.
- Default Gateway Change—A user might lose trusted network access because of a change to the default gateway, causing the ISE Posture to attempt a rediscovery of ISE. The ISE Posture tile portion on the AnyConnect UI displays the status of ISE Posture when it goes into rediscovery mode.
- Loss of Connectivity Between AnyConnect and ISE—After the endpoint is deemed compliant and granted network access, various network scenarios can occur: the endpoint can experience complete loss of network connectivity, ISE could go down, the ISE posture could fail (because of a session timeout, manual restart, or the like), or ISE behind a Secure Firewall ASA may lose the VPN tunnel.

- You cannot have multiple console users logged in on a macOS endpoint when using ISE posture.
- Delays in Initalization and Posture Assessment Flow (macOS only)—Apple advises you to allow their subnet in the pre-posture phase so that failures with signature verification of Compliance Module libraries won't occur.

Status of ISE Posture

When AnyConnect ISE Posture is working and blocking network access as expected, you see "System Scan: Searching for policy server" in the ISE Posture tile of the AnyConnect UI. In the Windows Task Manager or macOS system log, you can see that the process is running. If the service is not running, you see "System Scan: Service is unavailable" in the ISE Posture tile of the System Scan UI.



A network change starts the discovery phase. With AnyConnect ISE Posture, if the default route of the primary interface is changed, it brings the agent back to the discovery process. For example, when Wi-Fi and the primary LAN are connected, the agent restarts discovery. Likewise, if Wi-Fi and the primary LAN are connected but then Wi-Fi becomes disconnected, the agent will not restart discovery.

You may also see the following status messages after "System Scan" in the ISE Posture tile of the AnyConnect UI:

- Limited or no connectivity—No discovery is occurring because you have no connection. The AnyConnect ISE Posture agent may be performing discovery on the wrong endpoint on the network.
- System scan not required on current Wi-Fi—No discovery is occurring because an unsecured Wi-Fi was detected. The AnyConnect ISE Posture agent only starts discovery on the LAN, on the wireless if 802.1X authentication is used, and on the VPN. The Wi-Fi may be unsecured, or you disabled the feature by setting *OperateOnNonDot1XWireless* to 1 in the agent profile.
- Unauthorized policy server—The host does not match the server name rule of the ISE network so there is limited or no network access.
- The AnyConnect Downloader is performing update...—The downloader is invoked and compares the package versions, downloads the AnyConnect configuration, and performs the necessary upgrades.
- Scanning System...—Scanning for antivirus and antispyware security products has started. If the network is changed during this process, the agent recycles the process of generating the log file, and the status goes back to "No policy server detected."
- Bypassing AnyConnect scan—Your network is configured to use the Cisco NAC agent.
- Untrusted Policy Server Cancelled by the user—When you unblock the connection to untrusted servers in the AnyConnect UI with the System Scan Preferences tab, you receive the AnyConnect Downloader's Security Warning in a popup window. When you click **Cancel Connection** on this warning page, the ISE Posture tile changes to this status.
- Network Acceptable Use Policy—The access to the network requires that you view and accept the Acceptable Use Policy. Declining the policy may result in limited network access.
- Updating Network Settings—In the ISE UI in Settings > Posture > General Settings, you can specify how many seconds of delay should occur between network transitions.
- Not Compliant. Update time expired.—The time set for remediation has expired.
- Compliant. Network access allowed.—The remediation is complete. The AnyConnect > Scan Summary also shows the status as complete.
- No policy server detected—The ISE network is not found. After 30 seconds, the agent slows down probing. The default network access takes effect.

Script Remediation Messaging

You may see remediation or user notification popups during the course of script remediation, unless you are running in Linux, which has limited UI. For script remediation to be successful, the fingerprints must be present in AnyConnectLocalPolicy.xml. If you add a fingerprint, it is validated even in a normal posture flow, irrespective of whether script condition or remediation is configured on ISE. You may encounter the following messaging regarding script remediation:

- **Remediation cannot be attempted because the script has an invalid hash**—Appears in the System Scan Details when there is a hash mismatch of the downloaded script or if the policy sign verification failed.
- **The script you are trying to run exits with an error**—Appears in the System Scan Details when the script exists with a non-zero exit code. On Windows, it might also be that the execution policy that was configurd does not allow for script execution.

- **Remediation was unsuccessful because the script timed out**—Appears in the System Scan Details when the script takes longer than the remediation timer to exit. If the script doesn't exit within the remaining remediation timer, AnyConnect stops the script and marks the remediation as failed.
- **Remediation cannot be done because you are connected to an untrusted server**—Appears in the AnyConnect Details when the endpoint is connected to an untrusted ISE server. Either the server certificate is not marked as trusted in the certificate store or you have no fingerprints configured in AnyConnectLocalPolicy.xml. The fingerprints in the certificate presented by ISE must match the ones configured in AnyConnectLocalPolicy.xml.

Posture Condition Script

You can create and upload a posture condition script for posture checks on an endpoint. The following platforms and script types are supported. The configuration details of adding a script condition are in the *Cisco Identity Services Engine Administrator Guide*.

- Windows: PowerShell script (.ps1)
- macOS: Shell script (.sh)
- Linux: Shell script (.sh)

Remediation scripts configured to run as *administrator/root* on macOS and Linux are launched in a separate root environment. User session environmental variables like $HOME and the user-specific $PATH are not inherited; therefore, they should not be used in the script.

Posture and Multi Homing

AnyConnect ISE Posture module does not support multi homing because its behavior for such scenarios is undefined. For example, when media changes from wired to wireless and them back to wired, the user may see a posture status of compliant from the ISE posture module even though the endpoint is actually in redirect on the wired connection.

Simultaneous Users on an Endpoint

AnyConnect ISE Posture does not support separate posture assessment when multiple users are logged onto an endpoint simultaneously sharing a network connection. When the first user to run AnyConnect ISE Posture is successfully postured, and the endpoint is granted trusted network access, all other users on the endpoint inherit the network access. To prevent this, the administrator can disable features that allow simultaneous users on the endpoint.

Logging for Posture Modules

For ISE Posture, events are written to the native operating system event logs (Windows Event Log Viewer or macOS system log).

For VPN Posture, any errors and warnings go to syslogs (for non-Windows) and to the event viewer (for Windows). All available messages go to the log files.

The VPN Posture module components provide log outputs based on your operating system, privilege level, and launching mechanism:

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

Posture Modules' Log Files and Locations

For ISE Posture, events are contained in their own subfolder of the installed AnyConnect version, making them easy to isolate from the rest of the AnyConnect events. Each viewer allows the searching of keywords and filtering. The Web Agent events write to the standard application log.

For troubleshooting purposes, the ISE Posture requirement policy and assessment reports are logged, but to a separate, obfuscated file on the endpoint rather than to the event logs. Some log file sizes, such as aciseposture, can be configured by the administrator in the profile; however, the UI log size is predefined.

Whenever a process terminates abnormally, a mini dump file is generated, just as other AnyConnect modules provide.

For VPN Posture, the files are located in the users' home folder in the following directory:

- (Non-Windows)—.cisco/hostscan/log
- (Windows)— C:\Users\<user_name>\AppData\Local\Cisco HostScan\log\cscan.log

ISE Posture Profile Editor

An administrator can choose to use the standalone editor to create the posture profile and then upload it to ISE. Otherwise, the embedded posture profile editor is configured in the ISE UI under Policy Elements. When the AnyConnect configuration editor is launched in ISE, it creates the AnyConnect configuration complete with AnyConnect software and its associated modules, profiles, OPSWAT, and any customization. The standalone profile editor for ISE Posture contains the following parameters:

- **Agent Behavior**
  - **Enable signature check**—If checked, enables signature checking of executables before the agent runs them.
  - **Log file size**—The maximum Compliance Module logs file size. The valid values are 5 to 200 Mb.
  - **Remediation timer**—The time the user has for remediation before being tagged as non-compliant. The valid values are 1 to 300 minutes.
  - **Automated DART Count**—Determine how many automated DART bundles to collect during failure scenarios.

- **Enable agent log trace**—Enables the debug log on the agent.
- **Operate on non-802.1X wireless networks**—If checked, enables the agent to operate on non-802.1X wireless networks.
- **Enable posture non-redirection flow**—If unchecked, posture non-redirection flow is disabled. Make sure that all the NADs support redirection before you disable.
- **Enable Stealth Mode**—Choose whether to enable Stealth Mode which allows posture to run as a service without user intervention.
- **Enable Stealth With Notification**—If stealth mode notifications are set to enabled, the end user still gets notification messages when AnyConnect stealth mode is in noncompliant state, has limited network access, has an unreachable server, and so on.
- **Enable Rescan Button**—If you want to restart posture (or discovery) after a failure, after manual remediation, or when posture gets stuck (and so on), enable this button so that a **Scan Again** selection appears in the System Scan tile. You can show or hide the option in the ISE posture profile. When you click **Scan Again**, the discovery starts, and the entire posture flow is initiated.

Note Scan Again is only visible on the tile when the EnableRescan tag is set to 1 in the posture profile. If set to 0, the Scan Again button appears only in the conditions when it used to appear (prior to this option).

Note If profile changes occur on the ISE side, the AnyConnect tile reflects the change the next time discovery starts.

- **Disable UAC Popup**—Decide whether the Windows User Account Control (UAC) popup appears during policy validation. With the default value (unchecked), the end user continues to be prompted for administrator privileges when connecting. If you enable, end users will not see a Windows User Account Control (UAC) prompt during policy validation. By turning off the UAC prompt, VPN Posture uses a system process for privilege escalation instead of "Run as administrator." Validate your posture policies on the device where users have local admin rights before disabling the UAC prompt.
- **Backoff Timer Limit**—Enter the time up to which AnyConnect sends probes for ISE discovery. Because the probes add more traffic, you should choose a value that is not disruptive to your network.
- **Periodic Probe Interval**—Specify a discovery probing interval after the Backoff Timer Limit is crossed. AnyConnect sends the periodic probes with the given interval continuously until a valid ISE server is found. The default is 30 minutes, and after initial rounds of probing, probes are sent in continuous 30 minute intervals. Setting the value to 0 disables periodic probing.

- **IP Address Change**

  For the optimal user experience, set the values below to our recommendations.

  - **VLAN detection interval**—Interval at which the agent checks for VLAN changes before refreshing the client IP address. The valid range is 0 to 900 seconds, and the recommended value is 5 seconds. If set to 0, the VLAN detection feature is disabled. When set from 1 to 900, the agent sends an

Internet Control Message Protocol (ICMP) or Address Resolution Protocol (ARP) query every x seconds.

- **Ping or ARP**—The method for detecting IP address changes. The choices are Ping (0) to poll using ICMP, Arp (1) to poll using ARP, and Ping then Arp (2) to poll using ICMP first, then ARP if ICMP fails. The recommended setting is to poll using ARP because the default gateway might be configured to block ICMP packets.
- **Maximum timeout for ping**—The ping timeout from 1 to 10 seconds.
- **Enable agent IP refresh**—Check to enable VLAN change detection.
- **DHCP renew delay**—The number of seconds the agent waits after an IP refresh. Configure this value when you have Enable Agent IP Refresh enabled. If this value is not 0, the agent will do an IP refresh during this expected transition. If a VPN is detected during the refresh, the refresh will be disabled. The valid values are 0 to 60 seconds, and the recommended value is 5 seconds. Set this parameter to 0 to disable the feature.
- **DHCP release delay**— The number of seconds the agent delays doing an IP refresh. Configure this value when you have Enable Agent IP Refresh enabled. If this value is not 0, the agent will do an IP refresh during this expected transition. If a VPN is detected during the refresh, the refresh will be disabled. The valid values are 0 to 60 seconds, and the recommended value is 5 seconds. Set this parameter to 0 to disable this feature.
- **Network transition delay**—The timeframe (in seconds) for which the agent suspends network monitoring so that it can wait for a planned IP change. The recommended value is 5 seconds.

- **Posture Protocol**
  - **Discovery host**—Used for Policy Service Node discovery in redirection-based networks. Uses IP or FQDN to determine which server the Network Access Device can perform the redirection to. For standalone profile editors, enter a single host only.
  - **Server name rules**—A list of wild-carded, comma-separated names that defines the servers to which the agent can connect (such as example1.cisco.com or *.cisco.com).
  - **Call Home List**—Enter IPs or FQDNs that you want to use for load balancing, monitoring and troubleshooting lookup, or for DNS mapped to the default Policy Service Node (PSN) in that node (if in a multiple scenario). When this is configured, the first probe for monitoring and troubleshooting lookup is sent to call home. You must configure this while migrating from a redirection to a non-redirection network.
  - **PRA retransmission time**—When a passive reassessment communication failure occurs, this agent retry period is specified. The valid range is 60 to 3600 seconds.
  - **Retransmission Delay**—Specify the time in seconds to wait before retrying, after a failure occurs performing an HTTP task (GET or POST). The valid range is from 5 to 300 seconds, and the default is 60, accepting only integer values.
  - **Retransmission Limit**—Specify the number of retries allowed for a message, after a failure occurs performing an HTTP task (GET or POST). The valid range is from 0 to 10, and the default value is 4, accepting only integer values.

Advanced Panel

The Advanced Panel of the AnyConnect Secure Mobility Client UI is an area for each component to display statistics, user preferences, and any extra information specific to the component. If you click the **Advanced Window for all components** icon on the AnyConnect system tray, the new System Scan section contains the following tabs:

Note These statistics, user preferences, message history, and such are displayed under the Statistics window on macOS. Preferences are in the Preferences window and not in a tab orientation as in Windows.

- **Preferences**—Allows you to block connections to untrusted servers so that during the downloader process, you receive an "Untrusted Server Blocked" message for any ISE server that has untrusted certification and is unverified. If you disable the blocking, AnyConnect will not block connections to potentially malicious network devices.
- **Statistics**—Provides current ISE Posture status (compliant or not), OPSWAT version information, the status of the Acceptable Use Policy, the last running time stamp for posture, any missing requirements, and any other statistics deemed important enough to display for troubleshooting purposes.
- **Security Products**—Accesses the list of antimalware products installed on your system.
- **Scan Summary**—Allows the users to see whatever posture items the administrator configured for them to see. For example, when configured, they could see all of the items that have been postured on their system or only the ones that failed the posture check and required remediation.
- **Message History**—Provides a history of every status message sent to the system tray for a component. This history is useful for troubleshooting.

What VPN Posture Module Provides

HostScan

HostScan is a package that installs on the remote device after the user connects to the Secure Firewall ASA and before the user logs in. HostScan consists of any combination of the basic module, the endpoint assessment module, and the advanced endpoint assessment module. HostScan is not supported with mobile devices (Android, iOS, Chrome, or UWP).

Basic Functionality

HostScan automatically identifies operating systems and service packs on any remote device establishing a AnyConnect VPN client session.

You can also configure HostScan to inspect the endpoint for specific processes, files, and registry keys. It performs all of these inspections before full tunnel establishment and sends this information to the Secure Firewall ASA to distinguish between corporate-owned, personal, and public computers. The information can also be used in assessments.

Note Pre-login assessment and returning certificate information is not available. HostScan is not an authentication method; it simply checks to verify what exists on the device attempting to connect.

HostScan also automatically returns the following additional values for evaluation against configured DAP endpoint criteria:

- Microsoft Windows, macOS, and Linux operating systems
- Microsoft Knowledge Base numbers (Kbs)
- Device endpoint attributes types such as host name, MAC address, BIOS serial number, port numbers (legacy attribute), TCP/UDP port number, privacy protection, and version of endpoint assessment (OPSWAT)

Note HostScan gathers service release (GDR) information about Microsoft software updates on a Windows client system. A service release contains multiple hotfixes. The service release endpoint attribute is used in DAP rules, not hotfixes.

Endpoint Assessment

Endpoint Assessment is a HostScan extension that examines the remote computer for a large collection of antivirus and antispyware applications, associated definitions updates, and firewalls. You can use this feature to combine endpoint criteria to satisfy your requirements before the Secure Firewall ASA assigns a specific dynamic access policy (DAP) to the session.

See the *Dynamic Access Policies* section in the appropriate version of the Cisco ASA Series VPN CLI or ASDM Configuration Guide for details.

Advanced Endpoint Assessment: AntiMalware and Firewall Remediation

On Windows, macOS, and Linux desktops, Advanced Endpoint Assessment can attempt to begin remediation of various aspects of antimalware and personal firewall protection if that software allows a separate application to begin remediation.

Antimalware—Advanced Endpoint Assessment can attempt to remediate these components of antimalware software:

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

Personal Firewall—The Advanced Endpoint Assessment module can enable or disable the firewall.

HostScan does not support the blocking or allowing of an application and port using personal firewall.

Note Not all personal firewalls support this Force Enable/Force Disable feature.

Configure Antimalware Applications for HostScan

Before installing the VPN Posture module, configure your antimalware software to make security exceptions for these applications below. Antimalware applications can misinterpret the behavior of these applications as malicious:

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

Integration with Dynamic Access Policies

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

You can specify a single attribute or combine attributes that form the conditions required to assign a DAP to a session. The DAP provides network access at the level that is appropriate for the endpoint AAA attribute value. The ASA applies a DAP when all of its configured endpoint criteria are satisfied.

See the *Configure Dynamic Access Policies* section in the Cisco ASA Series VPN CLI or ASDM Configuration Guide.

BIOS Serial Number in a DAP

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

Specify the BIOS as a DAP Endpoint Attribute

Procedure

Step 1 Log on to ASDM.

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

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

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

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

Step 6 Check the **BIOS Serial Number** checkbox, select **=** (equals) or **!=** (not equals), and enter the BIOS number in the BIOS Serial Number field. Click **OK** to save changes in the Endpoint Attribute dialog box.

Step 7 Click **OK** to save your changes to the Edit Dynamic Access Policy.

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

Step 9 Click **Save**.

How to Obtain BIOS Serial Numbers

- Windows—http://support.microsoft.com/kb/558124
- macOS—http://support.apple.com/kb/ht1529
- Linux—Use this command:

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

Determine the HostScan Image Enabled on the Secure Firewall ASA

Open ASDM and choose **Configuration > Remote Access VPN >Secure Desktop Manager > HostScan Image**.

Disk Encryption

You can enable the reporting of what disk encryption products are installed on the endpoint. Then on the csc_cscan log, you can find the version details and the encryption state of disks.

In the Advanced Endpoint Assessment screen on ASDM, an *Identify Encrypted Disks on Endpoint* checkbox activates disk encryption. The navigation for this screen in ASDM is Configuration > Remote Access VPN > Posture (for Secure Firewall) > Posture Settings > Configure.

Upgrade HostScan

If you are upgrading AnyConnect and HostScan manually (using msiexec), make sure that you first upgrade AnyConnect and then HostScan.

OPSWAT Support

VPN Posture, formerly HostScan, and ISE Posture modules both use the OPSWAT framework to secure endpoints.

This framework, that involves both the client and the headend, assists in the assessment of third-party applications on the endpoint. Support charts are provided for each posture method, as recognized by the OPSWAT version used. They contain product and version information for the list of applications.

When there is a mismatch in the version number between the headend (Secure Firewall ASA or ISE) and the endpoint (VPN Posture or ISE posture), the OPSWAT compliance module gets upgraded or downgraded to match the version on the headend. These upgrades/downgrades are mandatory and happen automatically without end user intervention, as soon as a connection to the headend is established.

VPN Posture OPSWAT Support

The HostScan Support Charts correspond to the HostScan package version and provide what works with a Secure Firewall ASA headend.

HostScan is versioned to coordinate with AnyConnect major and maintenance releases. You specify the version when you configure the HostScan package in ASDM at **Configuration > Remote Access VPN > Secure Desktop Manager > HostScan Image**.

VPN Posture guidelines:

- The version of OPSWAT used in the client and the headend must match.
- All versions of HostScan up through and including 4.3.x use OPSWAT v2. HostScan 4.6x and later use OPSWAT v4. OPSWAT v3 is not supported in any version of HostScan.

ISE Posture OPSWAT Support

AnyConnect Agent Compliance Modules are for the ISE Posture Module.

ISE Agent Compliance Modules version reflects the base OPSWAT version. In ISE posture, the OPSWAT binaries are packaged into a separate installer. You can manually load the OPSWAT library to the ISE headend from the local file system, or configure ISE to obtain it directly using the ISE Update Feed URL.

When using AnyConnect with ISE 2.1 (or later), you can choose to use either OPSWAT v3 or v4 for the ISE Compliance Module. The configuration for antimalware is on the ISE UI at **Work Centers > Posture > Posture Elements > Conditions > Antimalware**.