The AnyConnect Profile Editor

About the Profile Editor

The AnyConnect Secure Mobility Client software package contains a profile editor for Windows. ASDM activates the profile editor when you load the AnyConnect image on the Secure Firewall ASA. You can upload a client profile from local or flash.

If you load multiple AnyConnect packages, ASDM activates the client profile editor from the newest AnyConnect package. This approach ensures that the editor displays the features for the newest AnyConnect loaded, as well as the older clients.

There is also a stand-alone profile editor which runs on Windows.

Add a New Profile from ASDM

Note You must first upload a client image before creating a client profile.

Profiles are deployed to administrator-defined end user requirements and authentication policies on endpoints as part of AnyConnect, and they make the preconfigured network profiles available to end users. Use the profile editor to create and configure one or more profiles. AnyConnect includes the profile editor as part of ASDM and as a stand-alone Windows program.

To add a new client profile to the Secure Firewall ASA from ASDM:

Step 1 Open ASDM and select **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**.

Step 2 Click **Add**.

Step 3 Enter a profile name.

Step 4 From the Profile Usage drop-down list, choose the module for which you are creating a profile.

Step 5 (Optional) In the Profile Location field, click **Browse Flash** and select a device file path for the XML file on the Secure Firewall ASA.

Step 6 (Optional) If you created a profile with the stand-alone editor, click **Upload** to use that profile definition.

Step 7 (Optional) Choose the AnyConnect group policy from the drop-down list.

Step 8 Click **OK**.

The AnyConnect VPN Profile

AnyConnect Secure Mobility Client features are enabled in the AnyConnect profiles. These profiles contain configuration settings for the core client VPN functionality and for the optional client modules (such as Network Access Manager, ISE posture, Umbrella, Network Visibility Module, AMP, and customer experience feedback). The Secure Firewall ASA deploys the profiles during AnyConnect installation and updates. Users cannot manage or modify profiles.

You can configure the Secure Firewall ASA or ISE to deploy profiles globally for all AnyConnect users or to users based on their group policy. Usually, a user has a single profile for each AnyConnect module installed. In some cases, you might want to provide more than one VPN profile for a user: for example, for someone who works from multiple locations.

Some profile settings are stored locally on the user's computer in a user preferences file or a global preferences file. The user file has information the AnyConnect needs to display user-controllable settings in the Preferences tab of the client GUI and information about the last connection, such as the user, the group, and the host.

We advise against having more than one Secure Client profile with the same <HostAddress>. If you do, the profile preferences are merged, and the more secure connection setting is chosen for the connection. With the merging, the endpoint may lose features and functionalities or may be denied a connection.

The global file has information about user-controllable settings so that you can apply those settings before login (since there is no user). For example, the client needs to know if Start Before Login and/or AutoConnect On Start are enabled before login.

AnyConnect Profile Editor, Preferences (Part 1)

- **Use Start Before Login**—(Windows Only) Enables Start Before Login for the client's use. With Start Before Login enabled, AnyConnect starts before the Windows login dialog box appears. The user connects to the enterprise infrastructure over a VPN connection, before logging on to Windows. After authenticating, the login dialog box appears, and the user logs in as usual.
- **Show Pre-connect Message**—Enables an administrator to have a one-time message displayed prior to a users' first connection attempt. For example, the message can remind users to insert their smart card into its reader. The message appears in the AnyConnect message catalog and is localized.
- **Client Certificate Store**—Controls which certificate store(s) AnyConnect uses for reading client certificates. The secure gateway must be configured accordingly and dictates to the client which one of the multiple certificate authentication combinations is acceptable for a particular VPN connection.

  Types of certificates that are acceptable to the secure gateway: either two user certificates or one machine and one user certificate.

To allow further filtering of the certificate stores accessible by AnyConnect, you can configure the certificate store from Windows, macOS, or Linux drop-down. The profile preferences support the values below:

- **Windows**
- All—[Default] Uses client certificates from both Windows machine and user certificate stores.
- Machine—Uses client certificates only from Windows certificate store.
- User—Uses client certificates only from Windows certificate store.
- **macOS**
- All—[Default] Uses client certificates from all available keychains and PEM file stores.
- System—Uses client certificates only from the System Keychain and system PEM file store.
- Login—Uses client certificates only from the user login and dynamic smartcard keychains, as well as the user PEM file store.
- **Linux**
- All—[Default] Uses client certificates from both system and user PEM file stores, as well as the user Firefox NSS store.
- Machine—Uses client certificates only from the system PEM file store.
- User—Uses client certificates only from the user PEM file store, as well as the user Firefox NSS store.

- **Windows Certificate Store Override**—Allows an administrator to direct AnyConnect to utilize certificates in the Windows machine (Local System) certificate store for client certificate authentication. Certificate Store Override only applies to SSL, where the connection is initiated, by default, by the UI process. When using IPSec/IKEv2, this feature in the AnyConnect Profile is not applicable.

Note You must have a predeployed profile with this option enabled in order to connect with Windows using a machine certificate. If this profile does not exist on a Windows device prior to connection, the certificate is not accessible in the machine store, and the connection fails.

  - **True**—AnyConnect searches for certificates in the Windows machine certificate store. Client Certificate Store (Windows) must set to *All* or *Machine*.
  - **False**—[Default] AnyConnect will not search for certificates in the Windows machine certificate store, when the user does not have administrative privileges.

- **AutomaticCertSelection**—When multiple certificate authentication is configured on the secure gateway, you must set this value to **true**.
- **Auto Connect on Start**—AnyConnect, when started, automatically establishes a VPN connection with the secure gateway specified by the AnyConnect profile, or to the last gateway to which the client connected.

- **Minimize On Connect**—After establishing a VPN connection, the AnyConnect GUI minimizes.
- **Local LAN Access**—Allows the user complete access to the local LAN connected to the remote computer during the VPN session to the Secure Firewall ASA.

Note Enabling local LAN access can potentially create a security weakness from the public network through the user computer into the corporate network. Alternatively, you can configure the security appliance (version 8.4(1) or later) to deploy an SSL client firewall that uses the AnyConnect Local Print firewall rule included in the default group policy. In order to enable this firewall rule, you also must enable Automatic VPN Policy, Always on, and Allow VPN Disconnect in this editor, Preferences (Part 2).

- **Disable Captive Portal Detection**—When AnyConnect receives a certificate with a common name that does not match the Secure Firewall ASA name, a captive portal is detected. This behavior prompts the user to authenticate. Some users using self signed certificates may want to enable connection to corporate resources behind an HTTP captive portal and should thus mark the **Disable Captive Portal Detection** checkbox. The administrator can also determine if they want the option to be user configurable and mark the checkbox accordingly. If user configurable is selected, the checkbox appears on the Preferences tab of the AnyConnect Secure Mobility Client UI.
- **Auto Reconnect**—AnyConnect attempts to reestablish a VPN connection if you lose connectivity. If you disable Auto Reconnect, it does not attempt to reconnect, regardless of the cause of the disconnection.

Note Use Auto Reconnect in scenarios where the user has control over the behavior of the client.

  - **Auto Reconnect Behavior**
    - DisconnectOnSuspend—AnyConnect releases the resources assigned to the VPN session upon a system suspend and does not attempt to reconnect after the system resumes.
    - ReconnectAfterResume (Default)—AnyConnect attempts to reestablish a VPN connection if you lose connectivity.

- **Suspend AnyConnect During Connected Standby**— (Windows Only) Available only for devices that support Connected Standby. During Connected Standby, the operating system throttles system process, which can impact how packets are processed. With this option, you can disable VPN traffic when the system enters Connected Standby mode. The feature is disabled by default.
- **Auto Update**—When checked, enables the automatic update of the client. If you check User Controllable, the user can override this setting in the client.
- **RSA Secure ID Integration** (Windows only)—Controls how the user interacts with RSA. By default, AnyConnect determines the correct method of RSA interaction (automatic setting: both software or hardware tokens accepted).
- **Windows Logon Enforcement**—Allows a VPN session to be established from a Remote Desktop Protocol (RDP) session. Split tunneling must be configured in the group policy. AnyConnect disconnects

the VPN connection when the user who established the VPN connection logs off. If the connection is established by a remote user, and that remote user logs off, the VPN connection terminates.

- Single Local Logon (Default)—(Local: 1, Remote: no limit) Allows only one local user to be logged on during the entire VPN connection. Also, a local user can establish a VPN connection while one or more remote users are logged on to the client PC. This setting has no effect on remote user logons from the enterprise network over the VPN connection.

Note If the VPN connection is configured for all-or-nothing tunneling, then the remote logon is disconnected because of the resulting modifications of the client PC routing table for the VPN connection. If the VPN connection is configured for split-tunneling, the remote logon might or might not be disconnected, depending on the routing configuration for the VPN connection.

- Single Logon—(Local + Remote: 1) Allows only one user to be logged on during the entire VPN connection. If more than one user is logged on, either locally or remotely, when the VPN connection is being established, the connection is not allowed. If a second user logs on, either locally or remotely, during the VPN connection, the VPN connection terminates. No additional logons are allowed during the VPN connection, so a remote logon over the VPN connection is not possible.

Note Multiple simultaneous logons are not supported.

- Single Logon No Remote—(Local: 1, Remote: 0) Allows only one local user to be logged on during the entire VPN connection. No remote users are allowed. If more than one local user or any remote user is logged on when the VPN connection is being established, the connection is not allowed. If a second local user or any remote user logs on during the VPN connection, the VPN connection terminates.

- **Windows VPN Establishment**—Determines the behavior of AnyConnect when a user who is remotely logged on to the client PC establishes a VPN connection. The possible values are:
  - Local Users Only (Default)—Prevents a remotely logged-on user from establishing a VPN connection. This is the same functionality as in prior versions of AnyConnect.
  - Allow Remote Users—Allows remote users to establish a VPN connection. However, if the configured VPN connection routing causes the remote user to become disconnected, the VPN connection terminates to allow the remote user to regain access to the client PC. Remote users must wait 90 seconds after VPN establishment if they want to disconnect their remote login session without causing the VPN connection to be terminated.

Note The preference works when Remote Desktop Protocol (RDP) is used to connect to the endpoint.

- **Linux Logon Enforcement**— Allows a VPN session to be established from an SSH session. You must configure split tunneling in the group policy. AnyConnect disconnects the VPN connection when the

user who established the VPN connection logs off. If the connection is established by a remote user, and that remote user logs off, the VPN connection terminates.

- Single Local Logon (Default)—(Local: 1, Remote: no limit) Allows only one local user to be logged on during the entire VPN connection. Also, a local user can establish a VPN connection while one or more remote users are logged on to the client PC. This setting has no effect on remote user logons from the enterprise network over the VPN connection.

Note If the VPN connection is configured for all-or-nothing tunneling, then the remote logon is disconnected because of the resulting modifications of the client PC routing table for the VPN connection. If the VPN connection is configured for split-tunneling, the remote logon might or might not be disconnected, depending on the routing configuration for the VPN connection.

- Single Logon—(Local + Remote: 1) Allows only one user to be logged on during the entire VPN connection. If more than one user is logged on, either locally or remotely, when the VPN connection is being established, the connection is not allowed. If a second user logs on, either locally or remotely, during the VPN connection, the VPN connection terminates. No additional logons are allowed during the VPN connection, so a remote logon over the VPN connection is not possible.

Note Multiple simultaneous logons are not supported.

- Single Logon No Remote—(Local: 1, Remote: 0) Allows only one local user to be logged on during the entire VPN connection. No remote users are allowed. If more than one local user or any remote user is logged on when the VPN connection is being established, the connection is not allowed. If a second local user or any remote user logs on during the VPN connection, the VPN connection terminates.

- **Linux VPN Establishment**— Determines the behavior of AnyConnect when a user who is logged on to the client PC using SSH establishes a VPN connection. The possible values are:
  - Local Users Only (Default)— Prevents a remotely logged-on user from establishing a VPN connection.
  - Allow Remote Users— Allows remote users to establish a VPN connection.
- **Clear SmartCard PIN** — Only certain smart cards support this function. It forces smart card users to re-enter their PIN during VPN authentication, even if has already been unlocked recently by another user who was using it without additional PIN prompts.
- **IP Protocol Supported**—For clients with both an IPv4 and IPv6 address attempting to connect to the Secure Firewall ASA using AnyConnect, AnyConnect needs to decide which IP protocol to use to initiate the connection. By default AnyConnect initially attempts to connect using IPv4. If that is not successful, AnyConnect attempts to initiate the connection using IPv6.

  This field configures the initial IP protocol and order of fallback.
  - IPv4—Only IPv4 connections can be made to the Secure Firewall ASA.
  - IPv6—Only IPv6 connections can be made to the Secure Firewall ASA.

- IPv4, IPv6—First, attempt to make an IPv4 connection to the Secure Firewall ASA. If the client cannot connect using IPv4, then try to make an IPv6 connection.
- IPv6, IPv4—First attempt to make an IPv6 connection to the Secure Firewall ASA. If the client cannot connect using IPv6 then try to make an IPv4 connection.

Note The IP protocol failover can also happen during the VPN session. Whether performed prior to or during the VPN session, the failover is maintained until the currently used secure gateway IP address is no longer reachable. The client fails over to the IP address matching the alternate IP protocol, if available, whenever the currently used IP address isn't reachable.

AnyConnect Profile Editor, Preferences (Part 2)

- **Disable Automatic Certificate Selection** (Windows only)—Disables automatic certificate selection by the client and prompts the user to select the authentication certificate.
- **Proxy Settings**—Specifies a policy in the AnyConnect profile to control client access to a proxy server. Use this when a proxy configuration prevents the user from establishing a tunnel from outside the corporate network.
  - Native—Causes the client to use both proxy settings previously configured by AnyConnect, and the proxy settings configured in the browser. The proxy settings configured in the global user preferences are pre-pended to the browser proxy settings.
  - IgnoreProxy—Ignores the browser proxy settings on the user's computer.
  - Override—Manually configures the address of the Public Proxy Server. Public proxy is the only type of proxy supported for Linux. Windows also supports public proxy. You can configure the public proxy address to be User Controllable.
- **Allow Local Proxy Connections**—By default, AnyConnect lets Windows users establish a VPN session through a transparent or non-transparent proxy service on the local PC. Uncheck this parameter if you want to disable support for local proxy connections. Some examples of elements that provide a transparent proxy service include acceleration software provided by some wireless data cards, and network components on some antivirus software.
- **Enable Optimal Gateway Selection** (OGS), (IPv4 clients only)—AnyConnect identifies and selects which secure gateway is best for connection or reconnection based on the round trip time (RTT), minimizing latency for Internet traffic without user intervention. OGS is not a security feature, and it performs no load balancing between secure gateway clusters or within clusters. You control the activation and deactivation of OGS and specify whether end users may control the feature themselves. Automatic Selection displays in the Connect To drop-down list on the Connection tab of the client GUI.
  - **Suspension Time Threshold** (hours)—Enter the minimum time (in hours) that the VPN must have been suspended before invoking a new gateway-selection calculation. By optimizing this value in combination with the next configurable parameter (Performance Improvement Threshold), you can find the correct balance between selecting the optimal gateway and reducing the number of times to force the re-entering of credentials.

- **Performance Improvement Threshold** (%)—The percentage of performance improvement that triggers the client to re-connect to another secure gateway following a system resume. Adjust these values for your particular network to find the correct balance between selecting the optimal gateway and reducing the number of times to force the re-entering of credentials. The default is 20%.

When OGS is enabled, we recommend that you also make the feature user-controllable.

OGS has the following limitations:

- It cannot operate with Always On
- It cannot operate with automatic proxy detection
- It cannot operate with proxy auto-configuration (PAC) files
- If AAA is used, users may have to re-enter their credentials when transitioning to a different secure gateway. Using certificates eliminates this problem.

- **Automatic VPN Policy** (Windows and macOS only)—Enables Trusted Network Detection allowing AnyConnect to automatically manage when to start or stop a VPN connection according to the Trusted Network Policy and Untrusted Network Policy. If disabled, VPN connections can only be started and stopped manually. Setting an Automatic VPN Policy does not prevent users from manually controlling a VPN connection.
  - **Trusted Network Policy**—Action AnyConnect automatically takes on the VPN connection when the user is inside the corporate network (the trusted network).
    - Disconnect (Default)—Disconnects the VPN connection upon the detection of the trusted network.
    - Connect—Initiates a VPN connection upon the detection of the trusted network.
    - Do Nothing—Takes no action in the untrusted network. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.
    - Pause—AnyConnect suspends the VPN session instead of disconnecting it if a user enters a network configured as trusted after establishing a VPN session outside the trusted network. When the user goes outside the trusted network again, AnyConnect resumes the session. This feature is for the user's convenience because it eliminates the need to establish a new VPN session after leaving a trusted network.

  - **Untrusted Network Policy**—AnyConnect starts the VPN connection when the user is outside the corporate network (the untrusted network). This feature encourages greater security awareness by initiating a VPN connection when the user is outside the trusted network.
    - Connect (Default)—Initiates the VPN connection upon the detection of an untrusted network.
    - Do Nothing—Takes no action in the trusted network. This option disables Always-On VPN. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.

      Bypass connect upon VPN session timeout—When a VPN session times out while either Trusted Network Policy or Untrusted Network Policy are set to connect, a connection retry begins automatically. If you want to disallow the connection retry, click **Bypass connect upon VPN session timeout**.

- **Trusted DNS Domains**—DNS suffixes (a string separated by commas) that a network interface may have when the client is in the trusted network. For example: *.cisco.com. Wildcards (*) are supported for DNS suffixes.

Note If you are using Network Visibility Module, Trusted DNS Domains and Servers are not supported because the the Network Visibility Module uses an administrator-defined trusted server and certificate hash to determine whether the user is on a trusted or untrusted network.

- **Trusted DNS Servers**—DNS server addresses (IP addresses separated by commas) that a network interface may have when the client is in the trusted network. For example: 192.168.1.2, 2001:DB8::1. Wildcards (*) are supported for IPv4 or IPv6 DNS server addresses.
- **Trusted Servers @ https://<server>[:<port>]**—The host URL that you want to add as trusted. After you click **Add**, the URL is added, and the certificate hash is pre-filled. If the hash is not found, an error message prompts the user to enter the certificate hash manually and click **Set**.

  You must have a secure web server that is accessible with a trusted certificate to be considered trusted. Secure TND attempts a connection to the first configured server in the list. If the server cannot be contacted or if the hash of the certificate doesn't match, secure TND attempts to contact the next server in the configured list. If the server can be contacted, and the hash is trusted, the "trusted" criteria is met.

  If a certificate is renewed or changed, the certificate hash does not get updated on the ASDM profile preference automatically. You must remove the server and re-add it into this field for the hash to update. Or, if you know the certificate hash or thumbprint numbers, you can update the hash value in the ASDM profile. Afterwards, you must manually reconfigure the secure TND server in the VPN profile. To ensure the expected server policy is applied, you must push the new profile to the endpoint, as the server certificate change is not automatically tracked or written to the VPN profile by ASDM or the Profile Editor.

Note You can configure this parameter only when at least one of the Trusted DNS Domains or Trusted DNS Servers is defined. If Trusted DNS Domains or Trusted DNS Servers are not defined, this field is disabled.

- **Always On**—Determines whether AnyConnect automatically connects to the VPN when the user logs in to a computer running one of the supported Windows or macOS operating systems. You can enforce corporate policies, protecting the computer from security threats by preventing access to Internet resources when it is not in a trusted network. You can set the Always-On VPN parameter in group policies and dynamic access policies to override this setting by specifying exceptions according to the matching criteria used to assign the policy. If the AnyConnect policy enables Always-On and a dynamic access policy or group policy disables it, the client retains the disable setting for the current and future VPN sessions, as long as its criteria match the dynamic access policy or group policy on the establishment of each new session. After enabling, you will be able to configure additional parameters.

Note AlwaysOn is used for scenarios where the connection establishment and redundancy run without user intervention; therefore, while using this feature, you need not configure or enable Auto Reconnect in Preferences, part 1.

- **Allow VPN Disconnect**—Determines whether AnyConnect displays a Disconnect button for Always-On VPN sessions. Users of Always-On VPN sessions may want to click Disconnect so they can choose an alternative secure gateway for reasons such as performance issues with the current VPN session or reconnection issues following the interruption of a VPN session.

  The Disconnect locks all interfaces to prevent data from leaking out and to protect the computer from internet access except for establishing a VPN session. For the reasons noted above, disabling the Disconnect button can at times hinder or prevent VPN access.

- **Allow Access to the Following Hosts With VPN Disconnected**—Allows endpoints to access the configured hosts while VPN is disconnected during Always On. Values are a comma-separated list of hosts which can be specified IP addresses, IP address ranges (CIDR format), or FQDNs. Access to all subdomains of the configured domains is also allowed. A maximum of 500 hosts are allowed, and wildcards are not supported.

  Caveat: Access to the specified FQDNs depends upon the name resolution performed in an untrusted network.

- **Connect Failure Policy**—Determines whether the computer can access the Internet if AnyConnect cannot establish a VPN session (for example, when a Secure Firewall ASA is unreachable). This parameter applies only if Always-On and Allow VPN Disconnect are enabled. If you choose Always-On, the fail-open policy permits network connectivity, and the fail-close policy disables network connectivity.

  - Closed—Restricts network access when the VPN is unreachable. The purpose of this setting is to help protect corporate assets from network threats when resources in the private network responsible for protecting the endpoint are unavailable.
  - Open—Permits network access when the VPN is unreachable.

Caution A connect failure closed policy prevents network access if AnyConnect fails to establish a VPN session. It is primarily for exceptionally secure organizations where security persistence is a greater concern than always-available network access. It prevents all network access except for local resources such as printers and tethered devices permitted by split tunneling and limited by ACLs. It can halt productivity if users require Internet access beyond the VPN if a secure gateway is unavailable. AnyConnect detects most captive portals. If it cannot detect a captive portal, a connect failure closed policy prevents all network connectivity.

If you deploy a closed connection policy, we highly recommend that you follow a phased approach. For example, first deploy Always-On VPN with a connect failure open policy and survey users for the frequency with which AnyConnect does not connect seamlessly. Then deploy a small pilot deployment of a connect failure closed policy among early-adopter users and solicit their feedback. Expand the pilot program gradually while continuing to solicit feedback before considering a full deployment. As you deploy a connect failure closed policy, be sure to educate the VPN users about the network access limitation as well as the advantages of a connect failure closed policy.

If Connect Failure Policy is Closed, then you can configure the following settings:

- **Allow Captive Portal Remediation**—Lets AnyConnect lift the network access restrictions imposed by the closed connect failure policy when the client detects a captive portal (hotspot). Hotels and airports typically use captive portals to require the user to open a browser and satisfy conditions required to permit Internet access. By default, this parameter is unchecked to provide the greatest security; however, you must enable it if you want the client to connect to the VPN if a captive portal is preventing it from doing so.
- **Remediation Timeout**—Number of minutes AnyConnect lifts the network access restrictions. This parameter applies if the Allow Captive Portal Remediation parameter is checked and the client detects a captive portal. Specify enough time to meet typical captive portal requirements (for example, 5 minutes).
- **Apply Last VPN Local Resource Rules**—If the VPN is unreachable, the client applies the last client firewall it received from the Secure Firewall ASA, which may include ACLs allowing access to resources on the local LAN.

- **Captive Portal Remediation Browser Failover**—Allows the end user to use an external browser (after closing the AnyConnect browser) for captive portal remediation.
- **Allow Manual Host Input**—Enables users to enter different VPN addresses than those listed in the drop-down box of the AnyConnect UI. If you uncheck this checkbox, the VPN connection choices are only those in the drop-down box, and users are restricted from entering a new VPN address.
- **PPP Exclusion**—For a VPN tunnel over a PPP connection, specifies whether and how to determine the exclusion route. The client can exclude traffic destined for the secure gateway from the tunneled traffic intended for destinations beyond the secure gateway. The exclusion route appears as a non-secured route in the Route Details display of the AnyConnect GUI. If you make this feature user controllable, users can read and change the PPP exclusion settings.

- Automatic—Enables PPP exclusion. AnyConnect automatically determines the IP address of the PPP server.
- Override—Enables PPP Exclusion using a predefined server IP address specified in the *PPP Exclusion Server IP* field. The *PPP Exclusion Server IP* field is only applicable to this Override method and should only be used when the Automatic options fails to detect the IP address of the PPP server.

  Checking **User Controllable** for the PPP Exclusion Server IP field allows the end user to manually update the IP address via the preferences.xml file.
- Disabled—PPP exclusion is not applied.

- **Enable Scripting**—Launches OnConnect and OnDisconnect scripts if present on the security appliance flash memory.
  - **Terminate Script On Next Event**—Terminates a running script process if a transition to another scriptable event occurs. For example, AnyConnect terminates a running OnConnect script if the VPN session ends, and terminates a running OnDisconnect script if the client starts a new VPN session. On Microsoft Windows, the client also terminates any scripts that the OnConnect or OnDisconnect script launched, and all their script descendents. On macOS and Linux, the client terminates only the OnConnect or OnDisconnect script; it does not terminate child scripts.
  - **Enable Post SBL On Connect Script**—Launches the OnConnect script if present, and SBL establishes the VPN session. (Only supported if VPN endpoint is running Microsoft Windows.)
- **Retain VPN On Logoff**—Determines whether to keep the VPN session when the user logs off a Windows or macOS.
  - **User Enforcement**—Specifies whether to end the VPN session if a different user logs on. This parameter applies only if "Retain VPN On Logoff" is checked, and the original user logged off Windows or macOS when the VPN session was up.
- **Authentication Timeout Values**—The number of seconds the client waits for an authentication response from the headend after successfully sending user credentials for the connection attempt. Enter the number of seconds in the range of 10 to 120.

Note If your client is structured to receive client certificates from the operating system, then the value in the profile is not considered.

AnyConnect Profile Editor, Backup Servers

You can configure a list of backup servers the client uses in case the user-selected server fails. If the user-selected server fails, the client attempts to connect to the optimal server's backup at the top of the list. If that fails, the client attempts each remaining server in the Optimal Gateway Selection list, ordered by its selection results.

Note Any backup servers that you configure here are **only** attempted when no backup servers are defined in AnyConnect Profile Editor, Add/Edit a Server List, on page 19. Those servers configured in the Server List take precedence, and backup servers listed here are overwritten.

Host Address—Specifies an IP address or a Fully-Qualified Domain Name (FQDN) to include in the backup server list.

- **Add**—Adds the host address to the backup server list.
- **Move Up**—Moves the selected backup server higher in the list. If the user-selected server fails, the client attempts to connect to the backup server at the top of the list first, and moves down the list, if necessary.
- **Move Down**—Moves the selected backup server down in the list.
- **Delete**—Removes the backup server from the server list.

AnyConnect Profile Editor, Certificate Matching

Enable the definition of various attributes that can be used to refine automatic client certificate selection on this pane.

If no certificate matching criteria is specified, AnyConnect applies the following certificate matching rules:

- Key Usage: Digital_Signature
- Extended Key Usage: Client Auth

If any criteria matching specifications are made in the profile, neither of these matching rules are applied unless they are specifically listed in the profile.

- **Key Usage**—Use the following Certificate Key attributes for choosing acceptable client certificates:
  - Decipher_Only—Deciphering data, and that no other bit (except Key_Agreement) is set.
  - Encipher_Only—Enciphering data, and any other bit (except Key_Agreement) is not set.
  - CRL_Sign—Verifying the CA signature on a CRL.
  - Key_Cert_Sign—Verifying the CA signature on a certificate.
  - Key_Agreement—Key agreement.
  - Data_Encipherment—Encrypting data other than Key_Encipherment.
  - Key_Encipherment—Encrypting keys.
  - Non_Repudiation—Verifying digital signatures protecting against falsely denying some action, other than Key_Cert_sign or CRL_Sign.
  - Digital_Signature—Verifying digital signatures other than Non_Repudiation, Key_Cert_Sign or CRL_Sign.
- **Extended Key Usage**—Use these Extended Key Usage settings. The OIDs are included in parenthesis:
  - ServerAuth (1.3.6.1.5.5.7.3.1)

- ClientAuth (1.3.6.1.5.5.7.3.2)
- CodeSign (1.3.6.1.5.5.7.3.3)
- EmailProtect (1.3.6.1.5.5.7.3.4)
- IPSecEndSystem (1.3.6.1.5.5.7.3.5)
- IPSecTunnel (1.3.6.1.5.5.7.3.6)
- IPSecUser (1.3.6.1.5.5.7.3.7)
- TimeStamp (1.3.6.1.5.5.7.3.8)
- OCSPSign (1.3.6.1.5.5.7.3.9)
- DVCS (1.3.6.1.5.5.7.3.10)
- IKE Intermediate

- **Custom Extended Match Key** (Max 10)—Specifies custom extended match keys, if any (maximum 10). A certificate must match all of the specified key(s) you enter. Enter the key in the OID format (for example, 1.3.6.1.5.5.7.3.11).

Note If a Custom Extended Match Key is created with the OID size greater than 30 characters, it is unaccepted when you click the OK button. The limit for the maximum characters for an OID is 30.

- **Match only certificates with Extended key usage**—Previous behavior was that if a certificate distinguished name (DN) match rule is set, the client would match certificates with the specific EKU OID and all certificates with no EKU. To keep consistency but provide more clarity, you can disallow the match to certificates with no EKU. The default is to keep the legacy behavior that customers have come to expect. You must click the check box to enable the new behavior and disallow the match.

- **Distinguished Name** (Max 10):—Specifies distinguished names (DNs) for exact match criteria in choosing acceptable client certificates.
  - **Name**—The distinguished name (DN) to use for matching:
    - CN—Subject Common Name
    - C—Subject Country
    - DC—Domain Component
    - DNQ—Subject Dn Qualifier
    - EA—Subject Email Address
    - GENQ—Subject Gen Qualifier
    - GN—Subject Given Name
    - I—Subject Initials
    - L—Subject City

- N—Subject Unstruct Name
- O—Subject Company
- OU—Subject Department
- SN—Subject Sur Name
- SP—Subject State
- ST—Subject State
- T—Subject Title
- ISSUER-CN—Issuer Common Name
- ISSUER-DC—Issuer Component
- ISSUER-SN—Issuer Sur Name
- ISSUER-GN—Issuer Given Name
- ISSUER-N—Issuer Unstruct Name
- ISSUER-I—Issuer Initials
- ISSUER-GENQ—Issuer Gen Qualifier
- ISSUER-DNQ—Issuer Dn Qualifier
- ISSUER-C—Issuer Country
- ISSUER-L—Issuer City
- ISSUER-SP—Issuer State
- ISSUER-ST—Issuer State
- ISSUER-O—Issuer Company
- ISSUER-OU—Issuer Department
- ISSUER-T—Issuer Title
- ISSUER-EA—Issuer Email Address

- **Pattern**—Specifies the string to match. The pattern to be matched should include only the portion of the string you want to match. There is no need to include pattern match or regular expression syntax. If entered, this syntax will be considered part of the string to search for.

  For example, if a sample string was abc.cisco.com and the intent is to match cisco.com, the pattern entered should be cisco.com.

- **Operator**—The operator to use when performing matches for this DN.
  - Equal—equivalent to ==
  - Not Equal—equivalent to !=

- **Wildcard**—Enabled includes wildcard pattern matching. With wildcard enabled, the pattern can be anywhere in the string.

- **Match Case**—Check to enable case-sensitive pattern matching.

Related Topics

Configure Certificate Matching

AnyConnect Profile Editor, Certificate Enrollment

Certificate Enrollment enables AnyConnect to use the Simple Certificate Enrollment Protocol (SCEP) to provision and renew a certificate for client authentication.

- **Certificate Expiration Threshold**—The number of days before the certificate expiration date that AnyConnect warns users their certificate is going to expire (not supported by RADIUS password-management). The default is zero (no warning displayed). The range of values is zero to 180 days.
- **Client Certificate Import Store**—Select to which certificate store to save enrollment certificates.
  - **Windows**
  - All—[Default] Import enrollment certificates to both Windows machine and user certificate stores.
  - Machine—Import enrollment certificates only to Windows machine certificate stores.
  - User—Import enrollment certificates only to Windows user certificate stores.
  - **Linux**
  - All—[Default] Import enrollment certificates to both user PEM file and user Firefox NSS certificate stores.
  - UserFirefoxNSS—Import enrollment certificates only to user Firefox NSS certificate store.
  - UserPEMFile—Import enrollment certificates only to user PEM file certificate store.
- **macOS**
- Enrollment certificates can only be imported to the user Login Keychain.
- **Mobile platforms**
- Enrollment certificates can only be imported to the app sandbox.
- **Certificate Contents**—Specifies certificate contents to include in the SCEP enrollment request:
  - Name (CN)—Common Name in the certificate.
  - Department (OU)—Department name specified in certificate.
  - Company (O)—Company name specified in certificate.
  - State (ST)—State identifier named in certificate.
  - State (SP)—Another state identifier.
  - Country (C)—Country identifier named in certificate.

- Email (EA)—Email address. In the following example, Email (EA) is %USER%@cisco.com. %USER% corresponds to the user's ASA username login credential.
- Domain (DC)—Domain component. In the following example, Domain (DC) is set to cisco.com.
- SurName (SN)—The family name or last name.
- GivenName (GN)—Generally, the first name.
- UnstructName (N)—Undefined name.
- Initials (I)—The initials of the user.
- Qualifier (GEN)—The generation qualifier of the user. For example, "Jr." or "III."
- Qualifier (DN)—A qualifier for the entire DN.
- City (L)—The city identifier.
- Title (T)—The person's title. For example, Ms., Mrs., Mr.
- CA Domain—Used for the SCEP enrollment and is generally the CA domain.
- Key size—The size of the RSA keys generated for the certificate to be enrolled.

- **Display Get Certificate Button**—Enables the AnyConnect GUI to display the Get Certificate button under the following conditions:
  - The certificate is set to expire within the period defined by the Certificate Expiration Threshold (not supported with RADIUS).
  - The certificate has expired.
  - No certificate is present.
  - The certificate fails to match.

Related Topics

Configure Certificate Enrollment

AnyConnect Profile Editor, Certificate Pin

Prerequisites

Use the VPN profile editor to enable the preference and configure global and per host certificate pins. You can only pin per host certificates in the server list section if the preference in the Global Pins section is enabled. After enabling the preference, you can configure a list of global pins that the client uses for certificate pin verification. Adding per host pins in the server list section is similar to adding global pins. You can pin any certificates in the certificate chain, and they get imported to the profile editor to calculate the information required for pinning.

Add Pin—Initiates the Certificate Pinning Wizard which guides you through importing certificates into the Profile Editor and pinning them.

The certificate details portion of the window allows you to visually verify the Subject and Issuer columns.

Certificate Pinning Wizard

You can import any certificate of the server certificate chain into the profile editor to specify the information required for pinning. The profile editor supports three certificate import options:

- Browse local file—Choose the certificate that is locally present on your computer.
- Download file from a URL—Download the certificate from any file hosting server.
- Paste information in PEM format—Insert information in PEM format including certificate begin and end headers.

Note You can only import certificates in DER, PEM, and PKCS7 data format.

AnyConnect Profile Editor, Mobile Policy

AnyConnect version 3.0 and later does not support Windows Mobile devices. See *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5*, for information related to Windows Mobile devices.

AnyConnect Profile Editor, Server List

You can configure a list of servers that appear in the client GUI. Users can select servers in the list to establish a VPN connection.

Server List Table Columns:

- Hostname—The alias used to refer to the host, IP address, or Full-Qualified Domain Name (FQDN).
- Host Address—IP address or FQDN of the server.
- User Group—Used in conjunction with Host Address to form a group-based URL.
- Automatic SCEP Host—The Simple Certificate Enrollment Protocol specified for provisioning and renewing a certificate used for client authentication.
- CA URL—The URL this server uses to connect to certificate authority (CA).
- Certificate Pins—Per host pins used by the client during pin verification. Refer to AnyConnect Profile Editor, Certificate Pin, on page 17.

Note Clients use global and the corresponding per host pins during pin verification. Per host pins are configured in a similar way that global pins are configured using the Certificate Pinning Wizard.

Add/Edit—Launches the Server List Entry dialog where you can specify the above server parameters.

Delete—Removes the server from the server list.

Details—Displays more details about backup servers or CA URLs for the server.

Related Topics

Configure VPN Connection Servers

AnyConnect Profile Editor, Add/Edit a Server List

- **Host Display Name**—Enter an alias used to refer to the host, IP address, or Full-Qualified Domain Name (FQDN).
- **FQDN or IP Address**— Specify an IP address or an FQDN for the server.
  - If you specify an IP address or FQDN in the Host Address Field, then the entry in the Host Name field becomes a label for the server in the connection drop-down list of the AnyConnect tray fly-out.
  - If you only specify an FQDN in the Hostname field, and no IP address in the Host Address field, then the FQDN in the Hostname field will be resolved by a DNS server.
  - If you enter an IP address, use the Public IPv4 or the Global IPv6 address of the secure gateway. Use of the link-local secure gateway address is not supported.
- **User Group**—Specify a user group.

  The user group is used in conjunction with Host Address to form a group-based URL. If you specify the Primary Protocol as IPsec, the User Group must be the exact name of the connection profile (tunnel group). For SSL, the user group is the group-url of the connection profile.

Note In IKEv2/IPsec connections, when the Primary Server is not reachable, **User Group** information entered for the Primary Server carries forward to Backup Servers. To have the same behavior for SSL, you must also supply user group information to the Backup Servers as a URL (for example, https://example.com/usergroup) and not just FQDN.

- **Additional mobile-only settings**—Select to configure Apple iOS and Android mobile devices.
- **Backup Server List**

  We recommend that you configure a list of backup servers the client uses in case the user-selected server fails. If the server fails, the client attempts to connect to the server at the top of the list first, and moves down the list, if necessary.

Note Conversely, the backup servers configured in AnyConnect Profile Editor, Backup Servers, on page 12 are global entries for all connection entries. Any entries put in Backup Servers of the Profile Editor are overwritten with what is entered here in Backup Server List for an individual server list entry. This setting takes precedence and is the recommended practice.

  - **Host Address**—Specifies an IP address or an FQDN to include in the backup server list. If the client cannot connect to the host, it attempts to connect to the backup server.
  - **Add**—Adds the host address to the backup server list.

- **Move Up**—Moves the selected backup server higher in the list. If the user-selected server fails, the client attempts to connect to the backup server at the top of the list first, and moves down the list, if necessary.
- **Move Down**—Moves the selected backup server down in the list.
- **Delete**—Removes the backup server from the server list.

- **Load Balancing Server List**

  If the host for this server list entry is a load balancing cluster of security appliances, and the Always-On feature is enabled, specify the backup devices of the cluster in this list. If you do not, Always-On blocks access to backup devices in the load balancing cluster.

  - **Host Address**—Specifies an IP address or an FQDN of a backup device in a load-balancing cluster.
  - **Add**—Adds the address to the load balancing backup server list.
  - **Delete**—Removes the load balancing backup server from the list.

- **Primary Protocol**—Specifies the protocol for connecting to this server, either SSL or IPsec with IKEv2. The default is SSL.
  - **Standard Authentication Only (IOS Gateways)**—When you select IPsec as the protocol, you are able to select this option to limit the authentication methods for connections to IOS servers.

Note If this server is a Secure Firewall ASA, then changing the authentication method from the proprietary AnyConnect EAP to a standards-based method disables the ability of the Secure Firewall ASA to configure session timeout, idle timeout, disconnected timeout, split tunneling, split DNS, MSIE proxy configuration, and other features.

  - **Auth Method During IKE Negotiation** Select one of the standard-based authentication methods.
    - **IKE Identity**—If you choose a standards-based EAP authentication method, you can enter a group or domain as the client identity in this field. The client sends the string as the ID_GROUP type IDi payload. By default, the string is *$AnyConnectClient$*.

- **CA URL**—Specify the URL of the SCEP CA server. Enter an FQDN or IP Address. For example, http://ca01.cisco.com.
- **Certificate Pins**—Per host pins used by the client during pin verification. See AnyConnect Profile Editor, Certificate Pin, on page 17.
- **Prompt For Challenge PW**—Enable to let the user make certificate requests manually. When the user clicks Get Certificate, the client prompts the user for a username and one-time password.
- **CA Thumbprint**—The certificate thumbprint of the CA. Use SHA1 or MD5 hashes.

Note Your CA server administrator can provide the CA URL and thumbprint. The thumprint should be retrieved directly from the server and not from a "fingerprint" or "thumbprint" attribute field in a certificate it issued.

Related Topics

Configure VPN Connection Servers

AnyConnect Profile Editor, Mobile Settings

Apple iOS / Android Settings

- **Certificate Authentication**—The Certificate Authentication policy attribute associated with a connection entry specifies how certificates are handled for this connection. Valid values are:
  - **Automatic**—AnyConnect automatically chooses the client certificate with which to authenticate when making a connection. In this case, AnyConnect views all the installed certificates, disregards those certificates that are out of date, applies the certificate matching criteria defined in VPN client profile, and then authenticates using the certificate that matches the criteria. This happens every time the device user attempts to establish a VPN connection.
  - **Manual**—AnyConnect searches for a certificate from the AnyConnect certificate store on the Android device when the profile is downloaded and does one of the following:
    - If AnyConnect finds a certificate based on the certificate matching criteria defined in the VPN client profile, it assigns that certificate to the connection entry and uses that certificate when establishing a connection.
    - If a matching certificate cannot be found, the Certificate Authentication policy is set to Automatic.
    - If the assigned certificate is removed from the AnyConnect certificate store for any reason, AnyConnect resets the Certificate Authentication policy to Automatic.
  - **Disabled**—A client certificate is not used for authentication.
- **Make this Server List Entry active when profile is imported**—Defines a server list entry as the default connection once the VPN profile has been downloaded to the device. Only one server list entry can have this designation. The default value is disabled.

Apple iOS Only Setting

- **Connect on Demand (requires certificate authorization)**—This field allows you to configure the Connect on Demand functionality provided by Apple iOS. You can create lists of rules that are checked whenever other applications start network connections that are resolved using the Domain Name System (DNS).

  Connect on Demand is an option only if the Certificate Authentication field is set to Manual or Automatic. If the Certificate Authentication field is set to Disabled, this checkbox is dimmed. The Connect on Demand rules, defined by the Match Domain or Host and the On Demand Action fields, can still be configured and saved when the checkbox is dimmed.

- **Match Domain or Host**—Enter the hostnames (host.example.com), domain names (.example.com), or partial domains (.internal.example.com) for which you want to create a Connect on Demand rule. Do not enter IP addresses (10.125.84.1) in this field.
- **On Demand Action**—Specify one of the following actions when a device user attempts to connect to the domain or host defined in the previous step:
  - **Never connect**—iOS will never start a VPN connection when rules in this list are matched. Rules in this list take precedence over all other lists.

Note When Connect On Demand is enabled, the application automatically adds the server address to this list. This prevents a VPN connection from being automatically established if you try accessing the server's clientless portal with a web browser. Remove this rule if you do not want this behavior.

  - **Connect if Needed**—iOS will start a VPN connection when rules in this list are matched only if the system could not resolve the address using DNS.
  - **Always Connect**—Always connect behaviour is release dependent:
    - On Apple iOS 6, iOS will always start a VPN connection when rules in this list are matched.
    - On iOS 7.x, Always Connect is not supported. When rules in this list are matched, they behave as Connect If Needed rules.
    - On later releases, Always Connect is not used. Configured rules are moved to the Connect If Needed list and behave as such.
- **Add or Delete**—Add the rule specified in the Match Domain or Host and On-Demand Action fields to the rules table, or delete a selected rule from the rules table.

Network Visibility Module Profile Editor

In the profile editor, configure the IP address or FQDN of the collection server. You can also customize the data collection policy choosing what type of data to send, and whether data is anonymized or not.

Network Visibility Module can establish connection with a single stack IPv4 with an IPv4 address, a single stack IPv6 with an IPv6 address, or a dual stack IPv4/IPv6 to the IP address as preferred by the OS.

The mobile Network Visibility Module can establish a connection using IPv4 only. IPv6 connectivity is not supported.

Note The Network Visibility Module sends flow information only when it is on the trusted network. By default, no data is collected. Data is collected only when configured as such in the profile, and the data continues to be collected when the endpoint is connected. If collection is done on an untrusted network, it is cached and sent when the endpoint is on a trusted network. If you are sending collection data to Stealthwatch 7.3.1 and prior releases (or something other than Splunk or similar SIEM tool), cache data is sent once on a trusted network but not processed. For Stealthwatch applications, refer to the Stealthwatch Enterprise Endpoint License and NVM Configuration Guide.

If TND is configured in the Network Visibility Module profile, then the trusted network detection is done by Network Visibility Module and does not depend on VPN to determine if the endpoint is in a trusted network. Also, if VPN is in a connected state, then the endpoint is considered to be on the trusted network, and the flow information is sent. The NVM-specific system logs show Trusted Network Detection use.

When configuring TND directly in the Network Visibility Module profile, an administrator-defined trusted server and certificate hash determine whether the user is on a trusted or untrusted network. Administrators configuring Trusted Network Detection for the core VPN profile would alternatively configure the Trusted DNS Domains and Trusted DNS Servers in the core VPN profile: AnyConnect Profile Editor, Preferences (Part 2), on page 7.

- **Desktop** or **Mobile**—Determines whether you are setting up Network Visibility Module on a desktop or mobile device. **Desktop** is the default.
- **Collector Configuration**
  - **IP Address/FQDN**—Specifies the IPv4 or IPv6 IP address/FQDN of the collector.
  - **Port**—Specifies at which port number the Collector is listening.
  - **Secure**—Determines if you want Network Visibility Module to securely send data to the collector over DTLS. When this checkbox is checked, Network Visibility Module uses DTLS for transport. The DTLS connection requires that the DTLS server (collector) certificate is trusted by the endpoint. Any untrusted certificates are silently rejected.

    The collector as part of the CESA Splunk App v3.1.0 is required for DTLS support, and DTLS 1.2 is the minimum supported version.
- **Cache Configuration**
  - **Max Size**—Specify the maximum size the database can reach. The cache size previously had a pre-set limit, but you can now configure it within the profile. The data in the cache is stored in an encrypted format, and only processes with root privileges are able to decrypt the data.

    Once a size limit is reached, the oldest data is dropped from the space for the most recent data.
  - **Max Duration**—Specify how many days of data you want to store. If you also set a max size, the limit which reaches first takes precedence.

    Once the day limit is reached, the oldest day's data is dropped from the space for the most recent day. If only Max Duration is configured, there is no size cap; if both are disabled, the size is capped at 50MB.
- **Periodic Template**—Specify the period interval at which templates are sent out from the endpoint. The default value is 1440 minutes.

- **Periodic Flow Reporting** (Optional, applies to desktop only)—Click to enable periodic flow reporting. By default, Network Visibility Module sends information about the flow at the end of connection (when this option is disabled). If you need periodic information on the flows even before they are closed, set an interval in seconds here. The value of 0 means the flow information is sent at the beginning and at the end of each flow. If the value is *n*, the flow information will be sent at the beginning, every *n* seconds, and at the end of each flow. Use this setting for tracking long-running connections, even before they are closed.
- **Aggregation Interval**—Specify at which interval the data flows should be exported from the endpoint. When the default value of 5 seconds is used, more than one data flow is captured in a single packet. If the interval value is 0 seconds, each packet has a single data flow. The valid range is 0 to 600 seconds.
- **Throttle Rate**—Throttling controls at what rate to send data from the cache to the collector so that the end user is minimally impacted. You can apply throttling on both real time and cached data, as long as there is cached data. Enter the throttle rate in Kbps. The default is 500 Kbps.

  The cached data is exported after this fixed period of time. Enter 0 to disable this feature.
- **Collection Mode**—Specify when data from the endpoint should be collected by choosing: collection mode is off, trusted network only, untrusted network only, or all networks.
- **Collection Criteria**— You can reduce unnecessary broadcasts during data collection so that you have only relevant data to analyze. Control collection of data with the following options:
  - **Broadcast packets** and **Multicast packets** (Applies to desktop only)—By default, and for efficiency, broadcast and multicast packet collection are turned off so that less time is spent on backend resources. Click the checkbox to enable collection for broadcast and multicast packets and to filter the data.
  - **KNOX only** (Optional and mobile specific)—When checked, data is collected from the KNOX workspace only. By default, this field is not checked, and data from inside and outside the workspace is collected.
- **Data Collection Policy**—You can add data collection policies and associate them with a network type or connectivity scenario. You can apply one policy to VPN and another to non-VPN traffic since multiple interfaces can be active at the same time.

  When you click Add, the Data Collection Policy window appears. Keep these guidelines in mind when creating policies:
  - By default, all fields are reported and collected if no policy is created or associated with a network type.
  - Each data collection policy must be associated with at least one network type, but you cannot have two policies for the same network type.
  - The policy with the more specific network type takes precedence. For example, since VPN is part of the trusted network, a policy containing VPN as a network type takes precedence over a policy which has trusted as the network specified.
  - You can only create a data collection policy for the network that applies based on the collection mode chosen. For example, if the **Collection Mode** is set to **Trusted Network Only**, you cannot create a **Data Collection Policy** for an **Untrusted Network Type**.
  - If a profile from an earlier AnyConnect release is opened in a later AnyConnect release profile editor, it automatically converts the profile to the newer release. Conversion adds a data collection policy for all networks that exclude the same fields as were anonymized previously.

- **Name**—Specify a name for the policy you are creating.
- **Network Type**—Determine the collection mode, or the network to which a data collection policy applies, by choosing VPN, trusted, or untrusted. If you choose trusted, the policy applies to the VPN case as well.
- **Flow Filter Rule**—Defines a set of conditions and an action that can be taken to either Collect or Ignore the flow when all conditions are satisfied. You can configure up to 25 rules, and each rule can define up to 25 conditions. Use the up and down buttons to the right of the Flow Filter Rules list to adjust the priority of rules and give them higher consideration over subsequent rules. Click **Add** to set up the component of a flow filter rule.
    - Name—The unique name of the flow filter rule.
    - Type—Each filter rule has a Collect or Ignore type. Determine the action (Collect or Ignore) to apply if the filter rule is satisfied. If collect, the flow is allowed when conditions are met. If ignore, the flow is dropped.
    - Conditions—Add an entry for each field that is to be matched and an operation to decide if the field value should be equal or unequal for a match. Each operation has a field identifier and a corresponding value for that field. The field matches are case sensitive unless you apply case-insensitive operations (EqualsIgnoreCase) to the rule set when you are setting up the filter engine rules. After it has been enabled, the input in the Value field set under the rule is case insensitive.
- **Include/Exclude**
    - **Type**—Determine which fields you want to **Include** or **Exclude** in the data collection policy. The default is **Exclude**. All fields not checked are collected. When no fields are checked, all fields are collected.
    - **Fields**—Determine what information to receive from the endpoint and which fields will be part of your data collection to meet policy requirements. Based on the network type and what fields are included or excluded, Network Visibility Module collects the appropriate data on the endpoint.

Note During an upgrade, the ProcessPath, ParentProcessPath, ProcessArgs, and ParentProcessArgs are excluded by default from being reported in the flow information, if one of these scenarios exist:

- If the profile in the older version of Network Visibility Module had no Data Collection Policy or had an include Data Collection Policy.
- If the profile in the older version of Network Visibility Module had an exclude Data Collection Policy, and the profile was opened and saved with a newer version profile editor. If the profile in the older version of Network Visibility Module had an exclude Data Collection Policy but the profile was *not* opened and saved with the newer 4.9 (or later) version profile editor, then these four fields are included.

If Network Visibility Module is unable to compute the parent process id, the value defaults to 4294967295.

FlowStartMsec and FlowStopMsec determine the Epoch timestamp of the flow in milliseconds.

You can choose Interface State and SSID, which specifies whether the network state of the interface is trusted or untrusted.

- **Optional Anonymization Fields**—If you want to correlate records from the same endpoint while still preserving privacy, choose the desired fields as anonymized. They are then sent as the hash of the value rather than actual values. A subset of the fields is available for anonymization.

  Fields marked for include or exclude are not available for anonymization; likewise, fields marked for anonymization are not available for include or exclude.

- **Data Collection Policy for Knox (Mobile Specific)**—Option to specify data collection policy when mobile profile is selected. To create Data Collection Policy for Knox Container, choose the **Knox-Only** checkbox under Scope. Data Collection policies applied under Device Scope apply for Knox Container traffic also, unless a separate Knox Container Data Collection policy is specified. To add or remove Data Collection Policies, see the Data Collection Policy description above. You can set a maximum of 6 different Data Collection Policies for mobile profile: 3 for Device, and 3 for Knox.
- **Export on Mobile Network (Optional and Mobile Specific)**—Specifies whether the exporting of Network Visibility Module flows is allowed when a device is using a mobile network. If enabled (the default value), an end user can override an administrator when an Acceptable User Policy window is displayed or later by enabling the **Settings** > **NVM-Settings** > **> Use mobile data for NVM** checkbox in the AnyConnect Android application. If you uncheck the **Export on Mobile Network** checkbox, Network Visibility Module flows are not exported when the device is using a mobile network, and an end user cannot change that.
- **Trusted Network Detection**—This feature detects if an endpoint is physically on the corporate network. The network state is used by the Network Visibility Module to determine when to export data and to apply the appropriate Data Collection Policy. Click **Configure** to set the configuration for Trusted Network Detection. An SSL probe is sent to the configured trusted headend, which responds with a certificate, if reachable. The thumbprint (SHA-256 hash) is then extracted and matched against the hash

set in the profile editor. A successful match signifies that the endpoint is in a trusted network; however, if the headend is unreachable, or if the certificate hash does not match, then the endpoint is considered to be in an untrusted network.

Note When operating from outside your internal network, Trusted Network Detection makes DNS requests and attempts to establish an SSL connection to the configured server. Cisco strongly recommends the use of an alias to ensure that the name and internal structure of your organization are not revealed through these requests by a machine being used outside your internal network.

1. **https://**—Enter the URL (IP address, FQDN, or port address) of each trusted server and click **Add**.

Note Trusted servers behind proxies are not supported.

2. **Certificate Hash (SHA-256)**—If the SSL connection to the trusted server is successful, this field is populated automatically. Otherwise, you can set it manually by entering the SHA-256 hash of the server certificate and clicking **Set**.
3. **List of Trusted Servers**—You can define multiple trusted servers with this process. (The maximum is 10.) Because the servers are attempted for trusted network detection in the order in which they are configured, you can use the **Move Up** and **Move |Down** buttons to adjust the order. If the endpoint fails to connect to the first server, it tries the second server and so on. After trying all of the servers in the list, the endpoint waits for ten seconds before making another final attempt. When a server authenticates, the endpoint is considered within a trusted network.

Save the profile as `NVM_ServiceProfile.xml`. You must save the profile with this exact name or Network Visibility Module fails to collect and send data.

The AnyConnect Local Policy

AnyConnectLocalPolicy.xml is an XML file that is installed automatically on the client with the AnyConnect VPN installer and contains some default security values. This file is not deployed by the Secure Firewall ASA. If you make changes to an existing local policy file on a user's system, you must reboot for the changes to take effect.

Local Policy Preferences

You can specify the following preferences in the VPN Local Policy Editor to be included in the `AnyConnectLocalPolicy.xml` file.

- **FIPS Mode**

  Enables FIPS mode for the client. This setting forces the client to only use algorithms and protocols approved by the FIPS standard.

- **Bypass Downloader**

When selected, disables the launch of the VPNDownloader.exe module, which is responsible for detecting the presence of and updating the local versions of dynamic content. The client does not check for dynamic content present on the Secure Firewall ASA, including translations, customizations, optional modules, and core software updates.

When Bypass Downloader is selected, one of two things happens upon client connection to the Secure Firewall ASA:

- If the VPN client profile on the Secure Firewall ASA is different than the one on the client, the client aborts the connection attempt.
- If there is no VPN client profile on the Secure Firewall ASA, the client makes the VPN connection, but it uses its hard-coded VPN client profile settings.

Note If you configure VPN client profiles on the Secure Firewall ASA, they must be installed on the client before the client connects to the Secure Firewall ASA with BypassDownloader set to true. Because the profile can contain an administrator defined policy, the BypassDownloader true setting is only recommended if you do not rely on the Secure Firewall ASA to centrally manage client profiles.

- **Enable CRL Check**

  This feature is only implemented for Windows desktop. For both SSL and IPsec VPN connections, you have the option to perform Certificate Revocation List (CRL) checking. When this setting is enabled, AnyConnect retrieves the updated CRL for all certificates in the chain. AnyConnect then verifies whether the certificate in question is among those revoked certificates which should no longer be trusted; and if found to be a certificate revoked by the Certificate Authority (CA), it does not connect.

  CRL checking is disabled by default. AnyConnect performs CRL checks only when Enable CRL Check is checked (or enabled), and as a result, the end user may observe the following:

  - If the certificate is revoked through CRL, the connection to the secure gateway fails unconditionally, even if Strict Certificate Trust is disabled in the AnyConnect Local Policy file.
  - If the CRL cannot be retrieved (such as due to an unreachable CRL distribution point), the connection to the secure gateway fails unconditionally, if Strict Certificate Trust is enabled in the AnyConnect Local Policy file. Otherwise, if Strict Certificate Trust is disabled, the user may be prompted to bypass the error.

Note AnyConnect cannot perform a CRL check when Always On is enabled. Also, if CRL distribution points are not publicly reachable, AnyConnect may encounter service disruption.

- **Enable OCSP Check**

  This feature is implemented only for Linux. It allows the client to query the status of individual certificates in realtime by making a request to the OSCP responder and parsing the OSCP response to get the certificate status. OCSP is used to verify the entire certificate chain and only works with PEM File Certificate Store (by setting Exclude Firefox NSS Cert Store to *True*). There is a five second timeout interval per certificate to access the OCSP responder.

OCSP checking is disabled by default. When enabled, the end user may observe the following:

- If the certificate is revoked through OCSP, the connection to the gateway fails unconditionally, even if Strict Certificate Trust is disabled in the AnyConnect Local Policy file.
- If the OCSP responder cannot be reached, the connection to the secure gateway fails unconditionally, if Strict Certificate Trust is enabled in the AnyConnect Local Policy file. Otherwise, if Strict Certificate Trust is disabled, the user may be prompted to bypass the error.

Note AnyConnect cannot perform an OCSP check when Always On is enabled. Also, if the OCSP responder is not publicly reachable, AnyConnect may encounter a service disruption.

- **Restrict Web Launch**

  Prevents users from using a non-FIPS-compliant browser to initiate WebLaunch. It does this by preventing the client from obtaining the security cookie that is used to initiate the AnyConnect tunnel. The client displays an informative message to the user.

- **Strict Certificate Trust**

  If selected, when authenticating remote security gateways, AnyConnect disallows any certificate that it cannot verify. Instead of prompting the user to accept these certificates, the client fails to connect to security gateways using self-signed certificates and displays `Local policy prohibits the acceptance of untrusted server certificates. A connection will not be established.`. If not selected, the client prompts the user to accept the certificate. This is the default behavior.

  We strongly recommend that you enable Strict Certificate Trust for the AnyConnect for the following reasons:

  - With the increase in targeted exploits, enabling Strict Certificate Trust in the local policy helps prevent “man in the middle” attacks when users are connecting from untrusted networks such as public-access networks.
  - Even if you use fully verifiable and trusted certificates, the AnyConnect, by default, allows end users to accept unverifiable certificates. If your end users are subjected to a man-in-the-middle attack, they may be prompted to accept a malicious certificate. To remove this decision from your end users, enable Strict Certificate Trust.

- **Restrict Server Cert Store** (Windows, macOS, and Linux)

  Prevents the client from using the user-based certificate store to verify server certificates. Only system-based certificate store will be used. Enabling this also enables <StrictCertificateTrust> and sets it to true.

- **Restrict Preference Caching**

  By design, AnyConnect does not cache sensitive information to disk. Enabling this parameter extends this policy to any type of user information stored in the AnyConnect preferences.

  - Credentials—The user name and second user name are not cached.
  - Thumbprints—The client and server certificate thumbprints are not cached.
  - CredentialsAndThumbprints—Certificate thumbprints and user names are not cached.

- All—No automatic preferences are cached.
- false—All preferences are written to disk (default).

- **Restrict Web-deploy Updates**—You can define the level of restriction for updates. In coordination with the Update Policy parameter below, you could restrict downloader distribution to only trusted Secure Firewall ASA sources by creating a list of trusted Secure Firewall ASAs and electing to download policies, help files, translations, and scripts from those trusted Secure Firewall ASAs. With the following settings, you can bypass certain downloader functions, while preserving VPN profile updates and software update capabilities. Or disable web deployment of scripts, localization files, help files, or UI customization from Secure Firewall ASAs, without impacting other functions of the AnyConnect downloader. If set for bypass, any necessary updates must be done with out-of-band software update mechanisms.
  - **Restrict Script Web-deploy Updates**—Prevents administrators from customizing on-connect script updates from the server.
  - **Restrict Resource Web-deploy Updates**—Prevents administrators from customizing user interface element updates from the server.
  - **Restrict Help Web-deploy Updates**—Prevents administrators from customizing help file updates from the server.
  - **Restrict Localization Web-deploy Updates**—Prevents administrators from customizing localization updates from the server.

- **Exclude Pem File Cert Store** (Linux and macOS)

  Prevents the client from using the PEM file certificate store to verify server certificates and search for client certificates.

  The store uses FIPS-capable OpenSSL and has information about where to obtain certificates for client certificate authentication. Permitting the PEM file certificate store ensures remote users are using a FIPS-compliant certificate store.

- **Exclude Firefox NSS Cert Store** (Linux)

  Prevents the client from using the Firefox NSS certificate store to verify server certificates and search for client certificates.

  The store has information about where to obtain certificates for client certificate authentication.

- **Update Policy**

  Controls which headends the client can get software or profile updates from. By default, allowing updates from any server is set to *TRUE*. To restrict downloader distribution to only trusted Secure Firewall ASA sources, add the server names in the Server Name field and uncheck those server updates that you do not want to allow. While *Allow Software Updates* used to encompass scripts, help files, resources, and localizations, we have changed it to four separate setting.
  - **Allow Software Updates From Any Server**
  - **Allow Compliance Module Updates From Any Server**
  - **Allow VPN Profile Updates From Any Server**
  - **Allow Management VPN Profile Updates From Any Server**
  - **Allow ISE Posture Profile Updates From Any Server**

- **Allow Service Profile Updates From Any Server**
- **Allow Script Updates From Any Server**
- **Allow Help Updates From Any Server**
- **Allow Resource Updates From Any Server**
- **Allow Localization Updates From Any Server**
- **Server Name**

  Specify authorized servers in this list. These headends are allowed full updates of all AnyConnect software and profiles upon VPN connectivity. ServerName can be an FQDN, IP address, domain name, or wildcard with domain name.

Related Topics: Set the Update Policy

- **Trusted ISE Certificate Fingerprints (SHA256)**—Allows you to establish ISE trust before fetching the posture policy. You can specify SHA256 fingerprints of the ISE certificates, an intermediate CA certificate, or the root CA certificate in the ISE certification chain. SHA256 fingerprints are case insensitive and can be added with or without colons. This setting is mandatory for Script Remediation.

Enable Local Policy Parameters in an MST File

See Local Policy Preferences for the descriptions and values that you can set.

Create an MST file to change local policy parameters. The MST parameter names correspond to the parameters in the AnyConnect Local Policy file (AnyConnectLocalPolicy.xml):

- LOCAL_POLICY_BYPASS_DOWNLOADER
- LOCAL_POLICY_FIPS_MODE
- LOCAL_POLICY_RESTRICT_PREFERENCE_CACHING
- LOCAL_POLICY_RESTRICT_TUNNEL_PROTOCOLS
- LOCAL_POLICY_RESTRICT_WEB_LAUNCH
- LOCAL_POLICY_STRICT_CERTIFICATE_TRUST

Note AnyConnect installation does not automatically overwrite an existing local policy file on the user computer. You must delete the existing policy file on user computers first, so the client installer can create a new policy file.

Note Any changes to the local policy file require the system to be rebooted.