The AnyConnect Profile Editor

About the Profile Editor

The Cisco AnyConnect Secure Mobility Client software package contains a profile editor for all operating systems. ASDM activates the profile editor when you load the AnyConnect client image on the 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 ASA from ASDM:

Procedure

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 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 an AnyConnect group policy from the drop-down list.

Step 8 Click **OK**.

Stand-Alone Profile Editor

In addition to the profile editors in ASDM, you can use stand-alone versions of the profile editors for Windows. When predeploying the client, you use the stand-alone profile editors to create profiles for the VPN service and other modules that you deploy to computers using your software management system.

You can modify the stand-alone Cisco AnyConnect Profile Editor installation or uninstall the VPN or other profile editors using Add or Remove Programs.

Requirements

- Java—A minimum of JRE 1.6 is a prerequisite for the profile editor, but administrators must deploy it on their own.

> **Note** JRE 1.6 is not uninstalled automatically when uninstalling the stand-alone profile editor. You must uninstall it separately.

- Supported Operating Systems—This application has been tested on Windows 7. The MSI only runs on Windows.

- Supported Browsers—The help files in this application are supported by Firefox and Internet Explorer. They have not been tested in other browsers.

- Required Hard Drive Space—The Cisco AnyConnect Profile Editor application requires less than five megabytes of hard drive space. JRE 1.6 requires less than 100 megabytes of hard drive space.

- You must include the ASA in the VPN profile's server list in order for the client GUI to display all user controllable settings on the first connection. If you do not add the ASA address or FQDN as a host entry in the profile, then filters do not apply for the session. For example, if you create a certificate match and the certificate properly matches the criteria, but you do not add the ASA as a host entry in that profile, the certificate match is ignored.

Install the Stand-Alone AnyConnect Profile Editor

The stand-alone AnyConnect profile editor is distributed as a Windows executable msi file, separately from the AnyConnect ISO and .pkg files, and has this file naming convention: `anyconnect-profileeditor-win-<version>-k9.msi`.

Procedure

Step 1 Download the `anyconnect-profileeditor-win-<version>-k9.msi` from https://software.cisco.com/download/release.html?mdfid=286281283&flowid=72322&softwareid=282364313&release=4.0.00061&relind=AVAILABLE&rellifecycle=&reltype=latest.

Step 2 Double-click `anyconnect-profileeditor-win-<version>-k9.msi` to launch the installation wizard.

Step 3 At the Welcome screen, click **Next**.

Step 4 At the Choose Setup Type window, click one of the following buttons and click **Next**:

- **Typical**—Installs only the Network Access Manager profile editor automatically.

- **Custom**—Allows you to choose any of the profile editors to install.

- **Complete**—Automatically installs all of the profile editors.

Step 5 If you clicked **Typical** or **Complete** in the previous step, skip to the next step. If you clicked Custom in the previous step, click the icon for the stand-alone profile editor you want to install and select Will be installed on local hard drive or click Entire Feature will be unavailable to prevent the stand-alone profile editor from being installed. Click **Next**.

Step 6 At the Ready to Install screen, click **Install**.

Step 7 Click **Finish**.

- The stand-alone AnyConnect profile editor is installed in the `C:\Program Files\Cisco\Cisco AnyConnect` Profile Editor directory.

- You can launch the profile editors by selecting **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** and then clicking the stand-alone profile editor you want from the submenu or by clicking the appropriate profile editor shortcut icon installed on the desktop.

Edit a Client Profile Using the Stand-Alone Profile Editor

For reasons of security, you cannot manually edit the client profile XML files outside of the stand-alone profile editor. Any profile XML file that is edited outside the stand-alone profile editor will not be accepted by the ASA.

Procedure

Step 1 Launch the desired profile editor by double-clicking the shortcut icon on the desktop or by navigating to **Start** > **All Programs** > **Cisco** > **Cisco AnyConnect Profile Editor** and selecting the desired profile editor from the submenu.

Step 2 Select **File** > **Open** and navigate to the client profile XML file that you want to edit.

If you mistakenly try to open a client profile of one kind of feature, such as Web Security, using the profile editor of another feature, such as VPN, you receive a **Schema Validation failed** message and you will not be able to edit the profile.

If you inadvertently try to edit the same client profile in two instances of the same kind of profile editor, the last edits made to the client profile are saved.

Step 3 Make your changes to the profile and select **File** > **Save** to save your changes.

The AnyConnect VPN Profile

Cisco 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 Network Access Manager, ISE posture, customer experience feedback, and Web Security. The ASA deploys the profiles during AnyConnect installation and updates. Users cannot manage or modify profiles.

You can configure the 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 file for each AnyConnect module installed. In some cases, you might want to provide more than one VPN profile for a user. Someone who works from multiple locations might need more than one VPN profile.

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 client 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.

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 Logon and/or AutoConnect On Start are enabled before login.

AnyConnect Profile Editor, Preferences (Part 1)

- **Use Start Before Logon**—(Windows Only) Forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting AnyConnect before the Windows login dialog box appears. 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.

- **Certificate Store**—Controls which certificate store(s) AnyConnect uses for storing and reading certificates. The default setting (All) is appropriate for most cases. Do not change this setting unless you have a specific reason or scenario requirement to do so.

    ◦ All—(Default) Directs the AnyConnect client to use all certificate stores for locating certificates.

    ◦ Machine—Directs the AnyConnect client to restrict certificate lookup to the Windows local machine certificate store.

    ◦ User—Directs the AnyConnect client to restrict certificate lookup to the local user certificate stores.

- **Certificate Store Override**—Allows an administrator to direct AnyConnect to search for certificates in the Windows machine certificate store when the users do not have administrator privileges on their device.

    ✎

    Note   You must have a pre-deployed 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.

- **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 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 Client 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).

-

- **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. This feature is not supported with AlwaysOn.

    ◦ **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.

- **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)—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—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.

- **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.

- **Clear SmartCard PIN**

- **IP Protocol Supported**—For clients with both an IPv4 and IPv6 address attempting to connect to the 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 ASA.

  - IPv6—Only IPv6 connections can be made to the ASA.

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

    > **Note** The IPv4 to IPv6 and IPv6 to IPv4 protocol failover can also happen during the VPN session. If the primary IP protocol is lost, the VPN session will be re-established via the secondary IP protocol, if possible.

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.

  Related Topics: Configure Certificate Selection

- **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 component 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.

◦ **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 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.

You can configure this parameter only when at least one of the Trusted DNS Domains or Trusted DNS Servers is defined. The Network Visibility Module sends flow information only when this feature is enabled so that data is sent over a secure TND connection. 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 an 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.

Related Topics: Require VPN Connections Using Always On

◦ **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.

◦ **Connect Failure Policy**—Determines whether the computer can access the Internet if AnyConnect cannot establish a VPN session (for example, when an 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.

Related Topics: About Captive Portals

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 ASA, which may include ACLs allowing access to resources on the local LAN.

Related Topics: Configure a Connect Failure Policy

- **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 uses the IP address of the PPP server. Instruct users to change the value only if automatic detection fails to get the IP address.

    ◦ Disabled—PPP exclusion is not applied.

    ◦ Override—Also enables PPP exclusion. Choose if automatic detection fails to get the IP address of the PPP server, and you configured PPP exclusion as user controllable.

    If PPP Exclusion is enabled also set:

    ◦ **PPP Exclusion Server IP**—The IP address of the security gateway used for PPP exclusion.

    Related Topics: Instruct Users to Override PPP Exclusion

- **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 OS.

    ◦ **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 when the VPN session was up.

- **Authentication Timeout Values**—By default, AnyConnect waits up to 12 seconds for an authentication from the secure gateway before terminating the connection attempt. AnyConnect then displays a message indicating the authentication timed out. Enter a number of seconds in the range of 0 to 120.

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 17. 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.

- **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.

- **Certificate Import Store**—Select which Windows certificate store to save enrollment certificates to.

- **Automatic SCEP Host**—For Legacy SECP, specifies the host name and connection profile (tunnel group) of the ASA that has SCEP certificate retrieval configured. Enter a Fully Qualified Domain Name (FQDN) or a connection profile name of the ASA. For example, the hostname asa.cisco.com and the connection profile name scep_eng.

- **CA URL**—For Legacy SCEP, identifies the SCEP CA server. Enter an FQDN or IP Address of the CA server. For example, http://ca01.cisco.com.

  ◦ **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.

  ◦ **Thumbprint**—The certificate thumbprint of the CA. Use SHA1 or MD5 hashes.

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

- **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, 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).

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 Client 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 or group-alias of the connection profile.

• **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 11 are global entries for all connection entries. Any entries put in the Backup Servers location are overwritten with what is entered here 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 an ASA, then changing the authentication method from the proprietary AnyConnect EAP to a standards-based method disables the ability of the 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 *$AnyConnectClient$*.

- **Automatic SCEP Host**—This host is used for legacy SCEP.

- **CA URL**—Specify the URL of the SCEP CA server. Enter an FQDN or IP Address. For example, http://ca01.cisco.com.

- **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

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

- **Reconnect when roaming between 3G/Wifi networks**—When enabled (default), AnyConnect does not limit the time that it takes to try to reconnect after losing a connection, after the device wakes up, or after changes occur in the connection type (such as EDGE(2G), 1xRTT(2G), 3G, or Wi-Fi). This feature provides seamless mobility with a secure connection that persists across networks. It is useful for applications that require a connection to the enterprise, but consumes more battery life.

    If Network Roaming is disabled and AnyConnect loses a connection, it tries to re-establish a connection for up to 20 seconds if necessary. If it cannot, the device user or application must start a new VPN connection if one is necessary.

    Note   Network Roaming does not affect data roaming or the use of multiple mobile service providers.

- **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 check box 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 check box 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.

The AnyConnect Local Policy

AnyConnectLocalPolicy.xml is an XML file on the client containing security settings. This file is not deployed by the ASA. You must install it manually or deploy it to a user computer using an enterprise software deployment system. If you make changes to an existing local policy file on a user's system, that system should be rebooted.

Local Policy Parameters and Values

The following parameters are elements in the VPN Local Policy Editor and in the `AnyConnectLocalPolicy.xml` file. XML elements are shown in angle brackets.

> **Note** If you manually edit the file and omit a policy parameter, that feature resorts to default behavior.

- <acversion>

  Specifies the minimum version of the AnyConnect client capable of interpreting all of the parameters in this file. If a client running a version of AnyConnect that is older than this version reads the file, it issues an event log warning.

  The format is acversion="<version number>".

- **FIPS Mode** <FipsMode>

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

- **Bypass Downloader** <BypassDownloader>

  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 ASA, including translations, customizations, optional modules, and core software updates.

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

  - If the VPN client profile on the ASA is different than the one on the client, the client aborts the connection attempt.

  - If there is no VPN client profile on the 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 ASA, they must be installed on the client before the client connects to an 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 ASA to centrally manage client profiles.

- **Enable CRL Check** <EnableCRLCheck>

  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.

- **Restrict Web Launch** <RestrictWebLaunch>

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 an AnyConnect tunnel. The client displays an informative message to the user.

- **Strict Certificate Trust** <StrictCertificateTrust>

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 client 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 client, 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 Preference Caching** <RestrictPreferenceCaching>

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).

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

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 Mac Native Cert Store** (macOS only) <ExcludeMacNativeCertStore>

Prevents the client from using the Mac native (keychain) certificate store to verify server certificates and search for client certificates.

- **Exclude Firefox NSS Cert Store** (Linux and macOS) <ExcludeFirefoxNSSCertStore>

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** <UpdatePolicy>

Controls which headends the client can get software or profile updates from.

- **Allow Software Updates From AnyServer** <AllowSoftwareUpdatesFromAnyServer>

Allow or disallow software updates of the VPN core module and other optional modules from unauthorized servers (ones not listed in the Server Name list).

- **Allow VPN Profile Updates From AnyServer** <AllowVPNProfileUpdatesFromAnyServer>

Allow or disallow VPN Profile updates from unauthorized servers (ones not listed in the Server Name list).

- **Allow Service Profile Updates From AnyServer** <AllowServiceProfileUpdatesFromAnyServer>

Allow or disallow other service module profile updates from unauthorized servers (ones not listed in the Server Name list).

- **Allow ISE Posture Profile Updates From Any Server**<AllowISEProfileUpdatesFromAnyServer>

Allow or disallow ISE Posture Profile updates from unauthorized servers (ones not listed in the Server Name list).

- **Allow Compliance Module Updates From Any Server**<AllowComplianceModuleUpdatesFromAnyServer>

Allow or disallow Compliance Module updates from unauthorized servers (ones not listed in the Server Name list).

- **Server Name** <ServerName>

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.

Change Local Policy Parameters Manually

Procedure

Step 1 Retrieve a copy of the AnyConnect Local Policy file (AnyConnectLocalPolicy.xml) from a client installation.

Table 1: Operating System and AnyConnect Local Policy File Installation Path

Operating System	Installation Path
Windows	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client
Linux	/opt/cisco/anyconnect
macOS	/opt/cisco/anyconnect

Step 2 Edit the parameter settings. You can either edit the AnyConnectLocalPolicy file manually, or use the VPN Local Policy editor, which is distributed with the AnyConnect Profile Editor installer.

Step 3 Save the file as `AnyConnectLocalPolicy.xml` and deploy the file to remote computers using a corporate software deployment system.

Step 4 Reboot the remote computers so that the changes to the local policy file take effect.

Enable Local Policy Parameters in an MST File

See Local Policy Parameters and Values 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 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.

Enable Local Policy Parameters with the Enable FIPS Tool

For all operating systems, you can use Cisco's Enable FIPS tool to create an AnyConnect Local Policy file with FIPS enabled. The Enable FIPS tools is a command line tool that runs on Windows using administrator privileges or as a root user for Linux and macOS.

For information about where you can download the Enable FIPS tool, see the licensing information you received for the FIPS client.

You run the Enable FIPS tool by entering the command EnableFIPS <arguments> from the command line of the computer. The following usage notes apply to the Enable FIPS tool:

- If you do not supply any arguments, the tool enables FIPS and restarts the vpnagent service (Windows) or the vpnagent daemon (macOS and Linux).

- Separate multiple arguments with spaces.

The following example shows the Enable FIPS tool command, run on a Windows computer:

```
EnableFIPS rwl=false sct=true bd=true fm=false
```
The next example shows the command, run on a Linux or macOS computer:

```
./EnableFIPS rwl=false sct=true bd=true fm=false
```
The next table shows the policy settings you can configure with the Enable FIPS tool. The arguments match the parameters in the AnyConnect local policy file.

Policy Setting	Argument and Syntax
FIPS mode	fm=[true | false]
Bypass downloader	bd=[true | false]
Restrict weblaunch	rwl=[true | false]
Strict certificate trust	sct=[true | false]
Restrict preferences caching	rpc=[Credentials | Thumbprints | CredentialsAndThumbprints | All | false]
Exclude FireFox NSS certificate store (Linux and macOS)	efn=[true | false]
Exclude PEM file certificate store (Linux and macOS)	epf=[true | false]
Exclude Mac native certificate store (macOS only)	emn=[true | false]