

Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5

First Published: 2023-07-31

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

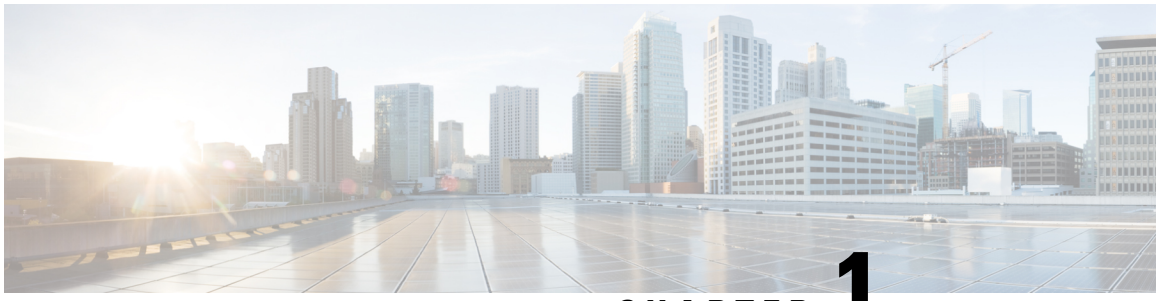
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

Deploy Cisco Secure Client

- Before You Begin, on page 1
- Cisco Secure Client Deployment Overview, on page 2
- Preparing the Endpoint for Cisco Secure Client, on page 4
- Using Network Visibility Module on Linux, on page 7
- Predeploying Cisco Secure Client, on page 8
- Web Deploying Cisco Secure Client, on page 25
- Updating Cisco Secure Client Software and Profiles, on page 32

Before You Begin

The following bulleted list highlights key support, naming, and functionality changes that are different from the AnyConnect Secure Mobility Client 4.x release. For release 5, AnyConnect Secure Mobility Client has been renamed to Cisco Secure Client.

- Although Network Access Manager is part of Cisco Secure Client 5.0, the Network Access Manager Profile Editor within Cisco Secure Client Cloud Management will not be available for release 5.
- AMP Enabler is for macOS only in Cisco Secure Client 5, as Cisco Secure Client for Windows offers full integration with Cisco Secure Endpoint, formerly AMP for Endpoints.
- Some AnyConnect modules also have new names in the Cisco Secure Client 5 release. HostScan (VPN Posture) will be changed to Secure Firewall Posture. In the ASDM UI, you will see it referenced as Posture (for Secure Firewall) in the Remote Access VPN windows. Similarly, the hostscan.pkg download from Cisco.com will be renamed as secure-firewall-posture-*version*-k9.pkg.
- You will notice references in the documentation and in the ASDM UI to AnyConnect. We currently do not intend to change those references to the new Cisco Secure Client name, although ASDM is fully supported to configure Cisco Secure Client 5 profiles. Secure Firewall ASA will be the new ASA name for version 9.18 and later.
- The ability of the Umbrella Roaming Security module to provide automatic updates for all installed AnyConnect modules with the Umbrella Cloud infrastructure has been removed for release 5.
- The Apex and Plus licenses for AnyConnect have been changed to Premier and Advantage licenses for Cisco Secure Client.

Cisco Secure Client Deployment Overview

Deploying Cisco Secure Client refers to installing, configuring, and upgrading Cisco Secure Client and its related files.

The Cisco Secure Client can be deployed to remote users by the following methods:

- **Predeploy**—New installations and upgrades are done either by the end user, or by using an enterprise software management system (SMS). This deployment option offers no cloud management.
- **Web Deploy**—The Cisco Secure Client package is loaded on the headend, which is either a Secure Firewall ASA, Secure Firewall Threat Defense, or an ISE server. When the user connects to a firewall or to ISE, Cisco Secure Client is deployed to the client. This deployment option offers no cloud management.
  - For new installations, the user connects to a headend to download Cisco Secure Client. The client is either installed manually or automatically (web-launch).
  - Updates are done by Cisco Secure Client running on a system where Cisco Secure Client is already installed, or by directing the user to the Secure Firewall ASA clientless portal.
- **Cisco Secure Client Cloud Management Deployment**—Once you have chosen which Cisco Secure Client options you want to enable (such as Start Before Login, Diagnostics and Reporting Tool, Secure Firewall Posture, Network Visibility Module, Secure Umbrella, ISE Posture, and Network Access Manager, and so on), click the ellipsis icon for the desired operating system. Choose **Network Installer** or **Full Installer** on the Deployment Management page of the Secure Client Cloud Management UI. This action downloads the csc-deployment.exe file, which then can be executed in a command prompt to install the Cloud Management service and your configured modules onto the endpoints. After you have the XDR Default Deployment installed on your endpoints, you can view the Network Visibility Module data in Secure Cloud Analytics (now part of Cisco XDR). Cisco Secure Client can be used with or without cloud management.

  Within XDR, you can navigate to Client Management > Deployments to see a list of all Secure Client deployments in your Cisco XDR organization. Refer to XDR documentation for further details.

When you deploy AnyConnect VPN, you can include optional Cisco Secure Client modules that enable extra features, and client profiles that configure the AnyConnect VPN and optional Cisco Secure Client features.

Refer to the Cisco Secure Client release notes for system, management, and endpoint requirements for Secure Firewall ASA, IOS, Microsoft Windows, Linux, and macOS.

Note Some third-party applications and operating systems may restrict the ISE posture agent and other processes from necessary file access and privilege elevation. Make sure the Cisco Secure Client installation directory is trusted and/or in the allowed/exclusion/trusted lists for endpoint antivirus, antimalware, antispyware, data loss prevention, privilege manager, or group policy objects. The following are the paths to be included:

- Windows
  - C:\Program Files (x86)\Cisco\
  - C:\ProgramData\Cisco\
  - C:\Users\%username%\AppData\Local\Cisco\
- macOS and Linux
  - /opt/cisco/
  - ~/.cisco/
  - ~/.vpn/

Additionally, third-party security applications (AV/AS/AM/DLP) could result in failure with a Compliance Module upgrade, because the interaction leads to missing libraries on the endpoint. To avoid these issues, upgrade the Compliance Module version and set these to exclude (in your third-party security application), before upgrading the Compliance Module:

```
-cisco-secure-client-win-4.3.xxxx.xxxx-isecompliance-webdeploy-k0.pkg
-cisco-secure-client-win-4.3.xxxx.xxxx-isecompliance-webdeploy-k9.exe
-cisco-secure-client-win-4.3.xxxx.xxxx-isecompliance-webdeploy-k9.msi
-opswat.msi
```

Compliance Module is not part of Secure Client Cloud Management deployments.

Decide How to Install Cisco Secure Client

Cisco Secure Client can be web deployed by ISE 2.0 (or later) and Secure Firewall ASA headends or predeployed. To install Cisco Secure Client initially requires administrative privileges.

Web Deploy

To upgrade Cisco Secure Client or install additional modules using web deploy (from ASA/ISE/Secure Firewall Threat Defense with Downloader), you do not need administrative privileges.

- Web Deploying from a Secure Firewall ASA or Secure Firewall Threat Defense—User connects to the Cisco Secure Client clientless portal on the headend device, and selects to download Cisco Secure Client. The Secure Firewall ASA downloads the Cisco Secure Client Downloader. The Cisco Secure Client Downloader downloads the client, installs the client, and starts a VPN connection.
- Web Deploying from ISE—User connects to the Network Access Device (NAD), such as a Secure Firewall ASA, wireless controller, or switch. The NAD authorizes the user, and redirects the user to the ISE portal. The Cisco Secure Client Downloader is installed on the client to manage the package extraction and installation, but does not start a VPN connection.

Predeploy

To upgrade Cisco Secure Client or install additional modules using predeploy (out-of-band deployment, either manually or using SCCM and so on), you need administrative privileges whether:

- Using an Enterprise software management system (SMS).
- Manually distributing the Cisco Secure Client file archive, with instructions for the user about how to install. File archive formats are zip for Windows, DMG for macOS, and gzip for Linux.

When utilizing out-of-band deployment methods, whether manually or through SCCM, you should initiate pre-deploy installers for software upgrades. It is important to note that you should not remove any Cisco Secure Client (AnyConnect) registry entries within SCCM or other deployment scripts during the upgrade process. For upgrade-related issues, consult Cisco.

For system requirements and licensing dependencies, refer to the Cisco Secure Client Features, License, and OS Guide.

Note If you are using Secure Firewall Posture to perform root privilege activities on a macOS or Linux platform, we recommend that you predeploy Secure Firewall Posture.

Determine The Resources You Need to Install Cisco Secure Client

Several types of files make up the Cisco Secure Client deployment:

- AnyConnect VPN, which is included in the Cisco Secure Client package.
- Modules that support extra features, which are included in the Cisco Secure Client package.
- Client profiles that configure Cisco Secure Client and the extra features, which you create.
- Language files, images, scripts, and help files, if you wish to customize or localize your deployment.
- ISE posture and the compliance module (OPSWAT).

Preparing the Endpoint for Cisco Secure Client

Using Mobile Broadband Cards with Cisco Secure Client

Some 3G cards require configuration steps before using Cisco Secure Client. For example, the VZAccess Manager has three settings:

- modem manually connects
- modem auto connect except when roaming
- LAN adapter auto connect

If you choose **LAN adapter auto connect**, set the preference to NDIS mode. NDIS is an always on connection where you can stay connected even when the VZAccess Manager is closed. The VZAccess Manager shows an autoconnect LAN adapter as the device connection preference when it is ready for Cisco Secure Client

installation. When the Cisco Secure Client interface is detected, the 3G manager drops the interface and allows the Cisco Secure Client connection.

When you move to a higher priority connection—wired networks are the highest priority, followed by WiFi, and then mobile broadband—Cisco Secure Client makes the new connection before breaking the old one.

Block Proxy Changes in Internet Explorer

Under certain conditions, Cisco Secure Client hides (locks down) the Internet Explorer Tools > Internet Options > Connections tab. When exposed, this tab lets the user set proxy information. Hiding this tab prevents the user from intentionally or unintentionally circumventing the tunnel. The tab lockdown setting is reversed upon disconnect. Tab lockdown is overridden by any administrator-defined policies applied to that tab. The lockdown is applied when:

- The Secure Firewall ASA configuration specifies Connections tab lockdown
- The Secure Firewall ASA configuration specifies a private-side proxy
- A Windows group policy previously locked down the Connections tab (overriding the no lockdown Secure Firewall ASA group policy setting)

For Windows 10 version 1703 (or later), in addition to hiding the Connections Tab in Internet Explorer, Cisco Secure Client hides (locks down) the system proxy tab in the Settings app to prevent the user from intentionally or unintentionally circumventing the tunnel. This lockdown is reversed upon disconnect.

Procedure

Step 1 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.

Step 2 Select a group policy and click **Edit** or **Add** a new group policy.

Step 3 In the navigation pane, go to **Advanced** > **Browser Proxy**. The Proxy Server Policy pane displays.

Step 4 Click **Proxy Lockdown** to display more proxy settings.

Step 5 Uncheck **Inherit** and select either:

- **Yes** to enable proxy lockdown and hide the Internet Explorer Connections tab during the Cisco Secure Client session.
- **No** to disable proxy lockdown and expose the Internet Explorer Connections tab during the Cisco Secure Client session.

Step 6 Click **OK** to save the Proxy Server Policy changes.

Step 7 Click **Apply** to save the Group Policy changes.

Configure How Cisco Secure Client Treats Windows RDP Sessions

You can configure Cisco Secure Client to allow VPN connections from Windows RDP sessions. By default, users connected to a computer by RDP are not able to start a VPN connection with the Cisco Secure Client. The following table shows the logon and logout options for a VPN connection from an RDP session. These preferences are configured in the VPN client profile:

Windows Logon Enforcement—Available in SBL mode

- 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—Not Available in SBL Mode

- 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.

Configure How Cisco Secure Client Treats Linux SSH Sessions

You can configure Cisco Secure Client to allow VPN connections from Linux SSH sessions. By default, users connected to a computer by SSH are not able to start a VPN connection with the Cisco Secure Client. The following table shows the logon and logout options for a VPN connection from an SSH session. These options are configured in the VPN client profile.

Linux Login Enforcement— 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.

Linux VPN Establishment—

- Local Users Only (Default)—Prevents a user, who is logged in remotely, from establishing a VPN connection.
- Allow Remote Users—Allows remote users to establish a VPN connection.

DES-Only SSL Encryption on Windows

By default, Windows does not support DES SSL encryption. If you configure DES-only on the Secure Firewall ASA, the Cisco Secure Client connection fails. Because configuring these operating systems for DES is difficult, we do not recommend that you configure the Secure Firewall ASA for DES-only SSL encryption.

Using Network Visibility Module on Linux

Before using Network Visibility Module on Linux, you must set up a kernel driver framework (KDF). You can choose to prebuild the Cisco Secure Client Kernel Module or build the driver on target. If you choose to build on target, no action is required; the build is handled automatically during deployment or during reboot.

Prerequisites to Build the Cisco Secure Client Kernel Module

If you are using eBPF, this process is not required. Prepare the target device:

- Make sure that the GNU Make Utility is installed.
- Install the kernel header package:
  - For RHEL, install the package **kernel-devel-$(uname -r)**, such as kernel-devel-2.6.32-642.13.1.el6.x86_64.
  - For Ubuntu, install the package **linux-headers-$(uname -r)**, such as linux-headers-4.2.0-27-generic.
  - For Linux, install the required libelf devel packages.
- Make sure that the GCC compiler is installed. The *major.minor* version of the installed GCC compiler should match the GCC version with which the kernel was built. You can verify this in the /proc/version file.

Package NVM with Prebuilt Cisco Secure Client Linux Kernel Module

Before you begin

Complete the prerequisites in Prerequisites to Build the Cisco Secure Client Kernel Module, on page 7.

The Cisco Secure Client Network Visibility Module can be packaged with a pre-built Cisco Secure Client Linux Kernel Module so that you do not need to build it on every target device, especially when the target devices have the same OS kernel version. If you decide to not use the pre-built option, you can use on target, which happens automatically during deployment or reboot without administrator input. Alternatively, if your deployment doesn't have the kernel prerequisites on all endpoints, you could use the pre-built option.



Note Web deployment is not supported with the pre-built Cisco Secure Client Linux Kernel Module.

Procedure

Step 1 Extract the Cisco Secure Client predeploy package: cisco-secure-client-linux64-<*version*>-predeploy-k9.tar.gz.

Step 2 Navigate to the nvm directory.

Step 3 Invoke the script **$sudo ./build_and_package_ac_ko.sh.**

What to do next

After running the script, cisco-secure-client-linux64-<*version*>-**ac_kdf_ko-k9.tar.gz** gets created, which includes the Cisco Secure Client Linux Kernel Module build. On Secure Boot enabled systems, sign the module with a private key allowed by Secure Boot. This file can only be used for predeploy.

When the target device's OS kernel is upgraded, you must re-deploy the Cisco Secure Client Network Visibility Module with the updated Linux Kernel Module.

Predeploying Cisco Secure Client

Cisco Secure Client can be predeployed by using an SMS, manually by distributing files for end users to install, or making your Cisco Secure Client file archive available for users to connect to.

When you create a file archive to install Cisco Secure Client, the directory structure of the archive must match the directory structure of the files installed on the client, as described in Locations to Predeploy the Cisco Secure Client Profiles, on page 11.

Before you begin

- Ensure that the following requirements are followed when creating or deploying a profile in Secure Client Cloud Management. Refer to the Secure Client Cloud Management documentation for additional information.
    - The profile name (for VPN or any of the Cisco Secure module profiles) must exactly match the name of the profile(s) as created and configured on the ASA/FTD headends and/or in ISE.

- To make sure the profile(s) remain synchronized across all endpoints and deployments, the profile(s) created in Secure Client Cloud Management must also then be imported into the ASA/FTD headends and/or in ISE.

  If the above requirements are not followed, profile(s) will not remain synchronized across all environments and could potentially disable certain features currently configured in existing deployments. For example, if you want remote desktop capabilities when using VPN, you must 1) have remote desktop capabilities enabled in theVPN profile on Secure Client Cloud Management, and 2) have the feature enabled in the profile(s) which are configured on the ASA/FTD and/or ISE environments.

  If you want to distribute a profile out-of-band (using SCCM, MDM, Secure Client Cloud Management, or the like) without configuring a Cisco Secure Client Profile (previously known as an AnyConnect profile) on the Secure Firewall ASA, you can use the *UseLocalProfileAsAlternative* custom attribute. When you configure this custom attribute, the client uses the local (on disk) Cisco Secure Client profile for its settings and preferences (rather than the usual defaults). Establishing the session using the local profile only occurs when 1) *UseLocalProfileAsAlternative* is set to enabled, and 2) if an ASA group policy profile is not configured. If you configure this custom attribute and do not undo or remove the Cisco Secure Client profile from the Group Policy configuaration on the ASA, the Cisco Secure Client Profile configured on the Group Policy will be maintained and used for each connection, where the custom attribute setting will be ignored. Refer to Configure Secure Client Custom Attributes in an Internal Group Policy in the *Cisco Secure Firewall ASA Series VPN ASDM Configuration Guide* for additional information.

- If you manually deploy the VPN profile, you must also upload the profile to the headends. When the client system connects, Cisco Secure Client verifies that the profile on the client matches the profile on the headend. If you have disabled profile updates, and the profile on the headend is different from the client, then the manually deployed profile will not work.
- If you manually deploy the Cisco Secure Client ISE Posture profile, you must also upload that file to ISE.
- If you are using a cloned VM, refer to Guidelines for Cloning VMs With Cisco Secure Client (Windows Only), on page 14.

Procedure

Step 1 Download the Cisco Secure Client Predeployment Package.

The Cisco Secure Client files for predeployment are available on cisco.com.

OS	Cisco Secure Client Predeploy Package Name
Windows	cisco-secure-client-win-*version*-predeploy-k9.zip (for ARM 64) cisco-secure-client-win-arm64-*version*-predeploy-k9.zip
macOS	cisco-secure-client-macos-*version*-predeploy-k9.dmg

OS	Cisco Secure Client Predeploy Package Name
Linux (64-bit)	(for script installer) cisco-secure-client-linux64-*version*-predeploy-k9.tar.gz (for RPM installer) cisco-secure-client-linux64-*version*-predeploy-rpm-k9.tar.gz (for DEB installer) cisco-secure-client-linux64-*version*-predeploy-deb-k9.tar.gz

The Secure Umbrella module is not available in the Linux operating system.

Step 2 Create client profiles: some modules and features require a client profile.

The following modules require Cisco Secure Client profiles to be created:

- AnyConnect VPN
- Network Access Manager
- ISE Posture
- Cisco Secure Endpoint
- Network Visibility Module
- Umbrella Roaming Secure Module

The following modules do not require Cisco Secure Client profiles to be created:

- Start Before Login
- Diagnostic and Reporting Tool
- Secure Firewall Posture
- Customer Experience Feedback

You can create client profiles in ASDM, and copy those files to your PC. Or, you can use the standalone profile editor on a Windows PC.

Step 3 Optionally, Customize and Localize Cisco Secure Client and Installer, on page 41.

Step 4 Prepare the files for distribution. The directory structure of the files is described in Locations to Pre-Deploy the AnyConnect Profiles.

Step 5 After you have created all the files for Cisco Secure Client installation, you can distribute them in an archive file, or copy the files to the client. Make sure that the same Cisco Secure Client files are also on the headends you plan to connect to: Secure Firewall ASA, ISE, and so on.

Cisco Secure Client Module Executables for Predeploy and Web Deploy

The following table shows the filenames on the endpoint computer when you predeploy or web deploy the Umbrella Roaming Security Module, Network Access Manager, ISE Posture, Network Visibility Module, and Thousand Eyes Module clients to a Windows computer.

Table 1: Module Filenames for Web Deployment or Predeployment

Module	Web-Deploy Installer (Downloaded)	Predeploy Installer
Zero Trust Access	cisco-secure-client-win-<*version*>-zta-webdeploy-k9.msi	cisco-secure-client-win-<*version*>-zta-predeploy-k9.msi
Network Access Manager	cisco-secure-client-win-*version*-nam-webdeploy-k9.msi	cisco-secure-client-win-*version*-nam-predeploy-k9.msi
ISE Posture	cisco-secure-client-win-*version*-iseposture-webdeploy-k9.msi	cisco-secure-client-win-*version*-iseposture-predeploy-k9.msi
Network Visibility Module	cisco-secure-client-win-*version*-nvm-webdeploy-k9.msi	cisco-secure-client-win-*version*-nvm-predeploy-k9.msi
Umbrella Roaming Security Module	cisco-secure-client-win-*version*-umbrella-webdeploy-k9.msi	cisco-secure-client-win-*version*-umbrella-predeploy-k9.msi
ThousandEyes Endpoint Agent Module	n/a	cisco-secure-client-win-*version*-thousandeyes-predeploy-k9.msi

Note If you have a Windows server OS, you may experience installation errors when attempting to install the Network Access Manager. The WLAN service is not installed by default on the server operating system, so you must install it and reboot the PC. The WLANAutoconfig service is a requirement for the Network Access Manager to function on any Windows operating system.

Locations to Predeploy the Cisco Secure Client Profiles

If you are copying the files to the client system, the following tables show where you must place the files.

Table 2: Cisco Secure Client Core Files

File	Description
anyfilename.xml	Cisco Secure Client profile. This file specifies the features and attribute values configured for a particular user type.
AnyConnectProfile.xsd	Defines the XML schema format. Cisco Secure Client uses this file to validate the profile.

Table 3: Profile Locations for all Operating Systems

Module	Location
Windows	
AnyConnect VPN Profile	%ProgramData%\Cisco\Cisco Secure Client\VPN\Profile

Module	Location
Zero Trust Access	(binaries) C:\Program Files (x86)\Cisco\Cisco Secure Client\ZTA (config and other files) C:\ProgramData\Cisco\Cisco Secure Client\ZTA
Network Access Manager	%ProgramData%\Cisco\ Cisco Secure Client\Network Access Manager\newConfigFiles
Customer Experience Feedback	%ProgramData%\Cisco\ Cisco Secure Client\CustomerExperienceFeedback
ISE Posture	%ProgramData%\Cisco\Cisco Secure Client\ISE Posture
Cisco Secure Endpoint	%ProgramData%\Cisco\AMP
Network Visibility Module	%ProgramData%\Cisco\Cisco Secure Client\NVM
ThousandEyes Endpoint Agent Module	(Windows Only) %ProgramData%\Cisco\Cisco Secure Client\ThousandEyes Endpoint Agent\ThousandEyes Endpoint Agent Configuration.json
Umbrella Roaming Security Module	%ProgramData%\Cisco\Cisco Secure Client\Umbrella **Note** In order to enable the Umbrella Roaming Security module, you must copy the OrgInfo.json file from the Umbrella dashboard and place it into this target directory without any renaming. You can alternatively co-locate the OrgInfo.json file with the Umbrella Roaming Security module installer, placing the file in \Profiles\umbrella before installation.
macOS	
Zero Trust Access	(binaries) /opt/cisco/secureclient/zta/bin (config and other files) /opt/cisco/secureclient/zta
ISE Posture	/opt/cisco/secureclient/iseposture/
AMP Enabler	/opt/cisco/secureclient/AMPEnabler/
Network Visibility Module	/opt/cisco/secureclient/NVM/
Umbrella Roaming Security Module	/opt/cisco/secureclient/umbrella **Note** In order to enable the Umbrella Roaming Security module, you must copy the OrgInfo.json file from the Umbrella dashboard and place it into this target directory without any renaming. You can alternatively co-locate the OrgInfo.json file with the Umbrella Roaming Security module installer, placing the file in \Profiles\umbrella before installation.

Module	Location
AnyConnect VPN Profile	/opt/cisco/secureclient/vpn/profile
Linux	
Network Visibility Module	/opt/cisco/secureclient/NVM
AnyConnect VPN Profile	/opt/cisco/secureclient/vpn/profile

Other Cisco Secure Client File Locations

Customization and Localization - Windows

- **L10N**
  - %ALLUSERSPROFILE%\Cisco\Cisco Secure Client\l10n
- **Resources**
  - %PROGRAMFILES%\Cisco\Cisco Secure Client\UI\res

Customization and Localization - macOS and Linux

- **L10N**
  - /opt/cisco/secureclient/l10n
- **Resources**
  - /opt/cisco/secureclient/resources

macOS Binaries, Libraries, and UI Resources

- **UI Resources**
  - /Applications/Cisco/Cisco Secure Client.app/Contents/Resources/
- **Binaries**
  - /opt/cisco/secureclient/bin
- **Libraries**
  - /opt/cisco/secureclient/lib

Help

- **Windows**
  - %ALLUSERSPROFILE%\Cisco\Cisco Secure Client\Help

- **macOS & Linux**
  - /opt/cisco/secureclient/help

OPSWAT Libraries

Used by both ISE Posture and Secure Firewall Posture

- **Windows**
  - %PROGRAMFILES%\Cisco\Cisco Secure Client\OPSWAT
- **macOS**

  /opt/cisco/secureclient/lib/opswat

Guidelines for Cloning VMs With Cisco Secure Client (Windows Only)

Cisco Secure Client endpoints are uniquely identified by a Universal Device Identifier (UDID), which all modules of Cisco Secure Client use. When a Windows VM is cloned, the UDID remains the same for all the clones from a source. To avoid any potential issues with cloned VMs, follow this action before using Cisco Secure Client:

1. Navigate to **%ProgramFiles(x86)%\Cisco\Cisco Secure Client\DART** and run dartcli.exe with administrator privileges as:

   ```
   dartcli.exe -nu
   ```

   or

   ```
   dartcli.exe -newudid
   ```

2. Print the UDID prior to and after this command to ensure that the UDID has changed with this command:

   ```
   dartcli.exe -u
   ```

   or

   ```
   dartcli.exe -udid
   ```

Predeploying Cisco Secure Client Modules as Standalone Applications

Some modules such as the Network Access Manager, Umbrella Roaming Security module, or ThousandEyes Endpoint Agent Module can run as standalone applications. The Cisco Secure Client is installed, but the VPN and Cisco Secure Client UI are not used.

Deploying StandAlone Modules with an SMS on Windows

Procedure

Step 1 Disable VPN functionality by configuring your software management system (SMS) to set the MSI property PRE_DEPLOY_DISABLE_VPN=1. For example:

```
msiexec /package cisco-secure-client-win-version-core-vpn-predeploy-k9.msi /norestart /passive
PRE_DEPLOY_DISABLE_VPN=1 /lvx* <log_file_name>
```

The MSI copies the VPNDisable_ServiceProfile.xml file embedded in the MSI to the directory specified for profiles for VPN functionality.

Step 2 Install the module. For example, the following CLI command installs Umbrella:

```
msiexec /package cisco-secure-client-win-version-umbrella-predeploy-k9.msi /norestart /passive /lvx*
c:\test.log
```

Step 3 (Optional) Install DART.

```
misexec /package cisco-secure-client-win-version-dart-predeploy-k9.msi /norestart /passive /lvx*
c:\test.log
```

Step 4 Save a copy of the obfuscated client profile to the proper Windows folder.

Step 5 Restart the Cisco Cisco Secure Client service.

Deploying Cisco Secure Client Modules as Standalone Applications

Requirements

The VPNDisable_ServiceProfile.xml file must also be the only Cisco Secure Client profile in the VPN client profile directory.

User Installation of StandAlone Modules

You can break out the individual installers and distribute them manually.

If you decide to make the zip image available to your users, and then ask to install it, be sure to instruct them to install only the standalone modules.

Note If a previous installation of Network Access Manager did not exist on the computer, the user must reboot the computer to complete the Network Access Manager installation. Also, if the installation is an upgrade that required upgrading some of the system files, the user must reboot.

Procedure

Step 1 Instruct users to check the Secure Client Network Access Manager, Secure Umbrella Module, or ThousandEyes Endpoint Agent Module.

Step 2 Instruct users to uncheck **Cisco AnyConnect VPN Module**.

Doing so disables the VPN functionality of the core client, and the Install Utility installs the Network Access Manager, Secure Umbrella Module, or ThousandEyes Endpoint Agent Module as standalone applications with no VPN functionality.

Step 3 (Optional) Check the **Lock Down Component Services** check box. The lockdown component service prevents users from switching off or stopping the Windows service.

Step 4 Instruct users to run the installers for the optional modules, which can use the Cisco Secure Client GUI without the VPN service. When the user clicks the Install Selected button, the following happens:

a) A pop-up dialog box confirms the selection of the standalone Network Access Manager, the Umbrella Roaming Security Module, or the ThousandEyes Endpoint Agent Module.
b) When the user clicks OK, the Install Utility invokes the Cisco Secure Client installer with a setting of PRE_DEPLOY_DISABLE_VPN=1.
c) The Install Utility removes any existing VPN profiles and then installs VPNDisable_ServiceProfile.xml.
d) The Install Utility invokes the Network Access Manager, Secure Umbrella, or ThousandEyes Endpoint Agent Module installer.
e) The Network Access Manager, Secure Umbrella Module, or ThousandEyes Endpoint Agent is enabled without VPN service on the computer.

Predeploying to Windows

Distributing Cisco Secure Client Using the zip File

The zip package file contains the Install Utility, a selector menu program to launch the individual component installers, and the MSIs for the core and optional Cisco Secure Client modules. When you make the zip package file available to users, they run the setup program (setup.exe). The program displays the Install Utility menu, from which users choose which Cisco Secure Client modules to install. You probably do not want your users to chose which modules to load. So if you decide to distribute using a zip file, edit the zip to remove the modules you do not want to use, and edit the HTA file.



Note If you are running Windows ARM64, there is no setup.exe option. For predeploying when running Windows ARM64, choose the appropriate .msi file.

One way to distribute an ISO is by using virtual CD mount software, such as SlySoft or PowerIS.

Predeployment zip Modifications

- Update the zip file with any profiles that you created when you bundled the files, and to remove any installers for modules that you do not want to distribute.
- Edit the HTA file to personalize the installation menu, and to remove links to any module installers that you do not want to distribute.

Contents of the Cisco Secure Client zip File

File	Purpose
GUI.ico	Cisco Secure Client icon image.
Setup.exe	Launches the Install Utility.
cisco-secure-client-win-*version*-dart-predeploy-k9.msi	MSI installer file for the DART Module.
cisco-secure-client-win-<*version*>-zta-predeploy-k9.msi	MSI installer file for Zero Trust Access

File	Purpose
cisco-secure-client-win-*version*-SBL-predeploy-k9.msi	MSI installer file for the SBL Module.
cisco-secure-client-win-*version*-iseposture-predeploy-k9.msi	MSI installer for the ISE Posture Module.
cisco-secure-client-win-*version*-nvm-predeploy-k9.msi	MSI installer file for the Network Visibility Module.
cisco-secure-client-win-*version*-umbrella-predeploy-k9.msi	MSI installer file for the Umbrella Roaming Security Module.
cisco-secure-client-win-*version*-nam-predeploy-k9.msi	MSI installer file for the Network Access Manager Module.
cisco-secure-client-win-*version*-posture-predeploy-k9.msi	MSI installer file for the Posture Module.
cisco-secure-client-win-*version*-thousandeyes-predeploy-k9.msi	MSI installer file for the ThousandEyes Endpoint Agent Module.
cisco-secure-client-win-*version*-core-predeploy-k9.msi	MSI installer file for the AnyConnect VPN Module.
autorun.inf	Information file for setup.exe.
eula.html	Acceptable Use Policy.
setup.hta	Install Utility HTML Application (HTA), which you can customize for your site.

Distributing Cisco Secure Client Using an SMS

After extracting the installers (*.msi) for the modules you want to deploy from the zip image, you can distribute them manually.

Requirements

- When installing Cisco Secure Client onto Windows, you must disable either the AlwaysInstallElevated or the Windows User Account Control (UAC) group policy setting. If you do not, the Cisco Secure Client installers may not be able to access some directories required for installation.
- Microsoft Internet Explorer (MSIE) users should add the headend to the list of trusted sites or install Java. Adding to the list of trusted sites enables the ActiveX control to install with minimal interaction from the user.

Profile Deployment Process

- If you are using the MSI installer, the MSI picks any profile that has been placed in the Profiles folder and places it in the appropriate folder during installation. The proper folder paths are available in the predeployment MSI file available on CCO.
- If you are predeploying the profile manually after the installation, copy the profile manually or use an SMS, such as Altiris, to deploy the profile to the appropriate folder.
- Make sure you put the same client profile on the headend that you predeploy to the client. This profile must also be tied to the group policy being used on the Secure Firewall ASA. If the client profile does not match the one on the headend or if it is not tied to the group policy, you can get inconsistent behavior, including denied access.
- The table below provides recommendations for log file names. By following the recommendations, you will have predictable locations, making it easier to find desired logs within the DART collection. Likewise,

some example commands provided may provide a function that is not desired by you. For example, the customer experience feedback command disables the feedback, which is enabled by default.

Windows Predeployment MSI Examples

Module Installed	Command and Log File
Cisco Secure core client: No VPN capability. (Use when installing standalone modules.)	msiexec /package cisco-secure-client-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* cisco-secure-client-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
Cisco secure core client with VPN capability. (Use for all cases except when installing standalone modules.)	msiexec /package cisco-secure-client-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
Zero Trust Access	msiexec /package cisco-secure-client-win-*version*-zta-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-<*version*>-zta-predeploy-k9-install-datetimestamp.log
Customer Experience Feedback	msiexec /package cisco-secure-client-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* cisco-secure-client-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
Diagnostic and Reporting Tool (DART)	msiexec /package cisco-secure-client-win-*version*-dart-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-*version*-dart-predeploy-k9-install-datetimestamp.log
SBL	msiexec /package cisco-secure-client-win-*version*-SBL-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-*version*-SBL-predeploy-k9-install-datetimestamp.log
Network Access Manager	msiexec /package cisco-secure-client-win-*version*-nam-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-*version*-nam-predeploy-k9-install-datetimestamp.log
Secure Firewall Posture	msiexec /package cisco-secure-client-win-*version*-posture-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-*version*-posture-predeploy-k9-install-datetimestamp.log
ISE Posture	msiexec /package cisco-secure-client-win-*version*-iseposture-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-*version*-iseposture-predeploy-k9-install-datetimestamp.log
Network Visibility Module	msiexec /package cisco-secure-client-win-*version*-nvm-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-*version*-nvm-predeploy-k9-install-datetimestamp.log

Module Installed	Command and Log File
Umbrella Roaming Security	msiexec /package cisco-secure-client-win-*version*-umbrella-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-*version*-umbrella-predeploy-k9-install-datetimestamp.log
ThousandEyes Endpoint Agent Module	msiexec /package cisco-secure-client-win-*version*-thousandeyes-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-*version*-thousandeyes-predeploy-k9-install-datetimestamp.log

Cisco Secure Client Sample Windows Transform

Cisco provides example Windows transforms, along with documents that describe how to use the transforms. A transform that starts with an underscore character (_) is a general Windows transform which allows you to apply only certain transforms to certain module installers. Transforms that start with an alphabetic character are VPN transforms. Each transform has a document that explains how to use it. The transform download is sampleTransforms-*x.x.x*.zip.

Windows Predeployment Security Options

Cisco recommends that end users are given limited rights on the device that hosts the Cisco Secure Client. If an end user warrants additional rights, installers can provide a lockdown capability that prevents users and local administrators from switching off or stopping those Windows services established as locked down on the endpoint. With the lockdown service option enabled, you can also uninstall all Cisco Secure Client Modules if you have administrator privileges.

Windows Lockdown Property

Each MSI installer supports a common property (LOCKDOWN) which, when set to a non-zero value, prevents the Windows service(s) associated with that installer from being controlled by users or local administrators on the endpoint device. We recommend that you use the sample transform (tools-cisco-secure-client-win-X.X.xxxx-transforms.zip) provided at the time of install to set this property and apply the transform to each MSI installer that you want to have locked down. The lockdown option is also a check box within the ISO Install Utility.

Hide Cisco Secure Client from Add/Remove Programs List

You can hide the installed Cisco Secure Client modules from users that view the Windows Add/Remove Programs list. You cannot start or stop Cisco Secure Client services. If you launch any installer using ARPSYSTEMCOMPONENT=1, that module will not appear in the Windows Add/Remove Programs list.

We recommend that you use the sample transform (tools-cisco-secure-client-win-X.X.xxxxx-transforms.zip) that we provide to set this property. Apply the transform to each MSI installer for each module that you want to hide.

Cisco Secure Client Module Installation and Removal Order on Windows

The module installers verify that they are the same version as the core client before starting to install. If the versions do not match, the module does not install, and the installer notifies the user of the mismatch. If you use the Install Utility, the modules in the package are built and packaged together, and the versions always match.

Because DART information is valuable should an uninstall process fail, you should follow the uninstall order in Step 2 below. You can just remove certain modules and leave the AnyConnect core module and DART. You can also uninstall everything in one step by uninstalling AnyConnect core if you use Add/Remove Programs.

Procedure

Step 1 Install the Cisco Secure Client modules in the following order:

a) Install the Cisco Secure Client core client module, which installs the GUI and VPN capability (both SSL and IPsec).

In Windows and macOS, a restricted user account (ciscoacvpnuser) is created to enforce the principle of least privilege only when the management tunnel feature is detected as enabled. This account gets removed during Cisco Secure Client uninstallation or during an installation upgrade.

b) Install the Cisco Secure Client Diagnostic and Reporting Tool (DART) module, which provides useful diagnostic information about the Cisco Secure Client installation.

c) Install the Umbrella Roaming Security, Network Visibility Module, SBL, Network Access Manager, Posture modules, or ISE compliance modules in any order.

Step 2 Uninstall the Cisco Secure Client modules in the following order:

a) Uninstall Umbrella Roaming Security, Network Visibility Module, Network Access Manager, Posture, ISE Compliance module, or SBL, in any order.

b) Uninstall the Cisco Secure Client core client module, and all modules are also removed.

c) Uninstall DART last.

The ThousandEyes Endpoint Agent Module is not uninstalled when Secure Client is uninstalled. It requires its own uninstall.



Note By design, some XML files remain after uninstalling Cisco Secure Client.

Predeploying to macOS

Install and Uninstall Cisco Secure Client on macOS

Cisco Secure Client for macOS is distributed in a DMG file, which includes all the Cisco Secure Client modules. When users open the DMG file, and then run the cisco-secure-client.pkg file, an installation dialog starts, which guides the user through installation. On the Installation Type screen, the user is able to select which packages (modules) to install.

Cisco Secure Client 5 supports all Apple supported versions of macOS 11 (and later).

To remove any of the Cisco Secure Client modules from your distribution, run the Cisco Secure Client uninstaller in Finder, navigate to Applications>Cisco, and double click **Uninstall**. Or run the VPN vpn_uninstall.sh script in /opt/cisco/secure client/bin.

Deploying Secure Client on macOS via MDM/EMM Without Client Management

On Windows, the predeploy package is the right choice for MDM/EMM. It contains the MSI files that MDM platforms deploy natively. However, on macOS, the predeploy package is designed for local interactive installation and cannot be deployed via MDM without an error. The solution is to use the web deploy package, which is historically used for headend-assisted deployments (Cisco ASA, FTD, ISE) as the source for extracting deployable module packages.

Do not attempt to deploy the Secure Client module .dmg files directly to your MDM. These DMG files are not structured for direct MDM deployments and will fail silently.

Before you begin

If you instead want to distribute Secure Client via MDM/EMM using Client Management, refer to Deploying Cisco XDR Client Management on macOS via MDM.

Procedure

Step 1 Download the Secure Client webdeploy package: cisco-secure-client-macos-version-webdeploy-k9.

Step 2 Rename it to cisco-secure-client-macos-version-webdeploy.zip and unzip it.

Step 3 Go into the Binaries/ directory and find the individual .dmg files for the various modules (VPN, NVM, ISE Posture, etc.) that you want to push to the endpoint.

Step 4 Mount each module DMG and extract the .pkg file inside.

Step 5 Upload each .pkg to your MDM and create a deployment policy.

Step 6 Deploy Core VPN first, as all other modules depend on it.

What to do next

A complete step-by-step procedure including package verification, MDM policy configuration, and system extension preapproval is outside of the scope of this documentation. Refer to Deploying Cisco Secure Client on macOS via MDM/EMM for additional details.

Get Write Permissions to Place Profiles for macOS Predeployment

The following procedure explains how to customize a module, create a profile, and add that profile to the DMG package. You must establish write permissions for the installer image before copying any files to the embedded profiles folder. It also sets the Cisco Secure Client user interface to start automatically on boot-up, which enables Cisco Secure Client to provide the necessary user and group information for the module.

Procedure

Step 1 Download the Cisco Secure Client DMG package (such as cisco-secure-client-macos-<*version*>-*nvm*-standalone.dmg for the Network Visibility Module) from Cisco.com.

Step 2 During the installation process, approve the system extensions popup that appears.

When the installation is complete, the standalone application is installed on the endpoint, and the supporting files are placed under the /opt/cisco/secureclient directory of the appropriate module. For example, for Network Visibility Module, the files are placed in /opt/cisco/secureclient/nvm.

Step 3 Open the file to access the installer. Note that the downloaded image is a read-only file.

Step 4 Make the installer image writable by either running the Disk Utility or using the Terminal application, as follows: `hdiutil convert <source dmg> -format UDRW -o <output dmg>`

Step 5 Install the stand-alone Profile Editor on a computer running a Windows operating system. You must choose the Cisco Secure Client modules you want as part of a custom installation or perform a complete installation. They are not installed by default.

Step 6 Start the profile editor and create a profile with the required configuration.

Step 7 Using Network Visibility Module as an example, the steps below explain how to appropriately save the profile. Following these steps, the profile editor creates an additional obfuscated version of the profile (such as NVM_ServiceProfile.wso for Network Visibility Module) and saves it to the same location as you saved the file (such as NVM_ServiceProfile.xml).

a) Copy the specified .wso file from the Windows device to the macOS installer package in the appropriate folder path, such as Cisco Secure Client x.x.x/Profiles/NVM. Or, use the Terminal application, as shown below for Network Visibility Module instance:`cp <path to the wso> \Volumes\"Cisco Secure Client <VERSION>"\Profiles\nvm\`

b) In the macOS installer, go to the Cisco Secure Client x.x.x/Profiles directory and open the ACTransforms.xml file in TextEdit for editing. Set the <DisableVPN> element to **true** to ensure that VPN functionality is not installed:`<ACTransforms><DisableVPN>true</DisableVPN></ACTransforms>`

c) The Cisco Secure Client DMG package is now ready to distribute to your users.

Restrict Applications on macOS

Gatekeeper restricts which applications are allowed to run on the system. You can choose to permit applications downloaded from:

- Mac App Store
- Mac App Store and identified developers
- Anywhere

The default setting is Mac App Store and identified developers (signed applications).

The current version of Cisco Secure Client is signed using an Apple-issued certificate and is notarized by Apple. If Gatekeeper is configured for Mac App Store (only), then you must either select the **App Store and identified developers** setting or control-click to bypass the selected setting to install and run Cisco Secure Client from a predeployed installation. For more information see: Safely open apps on your Mac

Predeploying to Linux

Installing Modules for Linux

You can break out the individual installers for Linux and distribute them manually. Each installer in the predeploy package can run individually. Use a compressed file utility to view and extract the files in the tar.gz file.

Before you begin

You must install the GNU Privacy Guard (GPG) key on the endpoint before installing Secure Client. It provides the necessary open-source crytography software.

Procedure

Step 1 Install the Cisco Secure Client core VPN module, which installs the GUI and VPN capability (both SSL and IPsec).

Step 2 Install the DART module, which provides diagnostic information about the Cisco Secure Client core VPN and other installed modules.

Step 3 If you are installing multiple modules at once using DEB and RPM packages, run the install commands uing && between each command for the modules you wish to install or upgrade. The order is critical for both install and upgrade. You must always install VPN first, and if you are installing Zero Trust Access, ensure that the Socket Filter module is included before the Zero Trust Access install command. For example `sudo apt install -y ./cisco-secure-client-<module1>_amd64.deb && \sudo apt install -y ./cisco-secure-client-<nodule2>_amd64.deb && \`

Step 4 Install the posture module or ISE compliance module.

Step 5 Install the Network Visibility Module.

Using RPM or DEB Installer for Upgrade

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

- Automatic client update from headend is not supported. You must do updates out-of-band with a system package manager.
- The only Cisco Secure Client modules supported with RPM and DEB installers are VPN and DART.
- You must uninstall the existing Cisco Secure Client (including all modules) installed by the script installers before switching to use the RPM or DEB installer.
- You cannot use a script installer out-of-band to update an existing RPM or DEB installation.

Uninstalling Modules for Linux

The order that the user uninstalls Cisco Secure Client is important.

DART information is valuable if the uninstall processes fails.

Procedure

Step 1 Uninstall the Network Visibility Module.

Step 2 Uninstall the posture module or ISE compliance module.

Step 3 Uninstall the Cisco Secure Client core VPN module.

Step 4 Uninstall DART using the following commands:

a) Ubuntu: `apt purge`

b) RHEL: `dnf remove`
c) SLES: `zypp remove`

Manually Installing/Uninstalling NVM on a Linux Device

Procedure

Step 1 Extract the Cisco Secure Client predeploy package.
Step 2 Navigate to the nvm directory.
Step 3 Invoke the script **$sudo ./nvm_install.sh**.

You can uninstall Network Visibility Module using /opt/cisco/secureclient/bin/nvm_uninstall.sh.

Manually Installing DART on a Linux Device

Procedure

Step 1 Store the predeploy package locally (such as cisco-secure-client-linux-arm64-100.0.0.143-predeploy-deb-k9.tgz), using the same naming conventions as above.
Step 2 Store ciscosecureclient-dart-linux-(ver)-k9.tar.gz locally.
Step 3 Install using: **Ubuntu**`apt install ./cisco-secure-client-dart*.deb`**RHEL**`dnf install ./cisco-secure-client-dart*.rpm`**SLES**`zypp install ./cisco-secure-client-dart*.rpm`
Step 4 Accept the installation.

Manually Installing DART on a Linux Device

1. Store ciscosecureclient-dart-linux-(ver)-k9.tar.gz locally.
2. From a terminal, extract the tar.gz file using the **tar -zxvf** <*path to tar.gz file including the file name* command.
3. From a terminal, navigate to the extracted folder and run dart_install.sh using the **sudo ./dart_install.sh** command.
4. Accept the license agreement and wait for the installation to finish.

Note You can only uninstall DART using **/opt/cisco/ciscosecureclient/dart/dart_uninstall.sh**.

Web Deploying Cisco Secure Client

Web deployment refers to the Cisco Secure Client Downloader on the client system getting Cisco Secure Client software from a headend, or to using the portal on the headend to install or update Cisco Secure Client. As an alternative to our traditional web launch which relied too heavily on browser support (and Java and ActiveX requirements), we improved the flow of auto web deploy, which is presented at initial download and upon launch from a clientless page. Automatic provisioning (Weblaunch) works on Windows operating systems with Internet Explorer browsers only. Additionally, if you are using a Microsoft-supported version of Windows 11 for ARM64-based devices, you must use a Chrome or Edge browser for web launch.

Web Deployment with the Secure Firewall ASA

The Clientless Portal on the Secure Firewall ASA web deploys Cisco Secure Client.

Users open a browser and connect to the Secure Firewall ASA clientless portal. On the portal, the users click the **Start AnyConnect Client** button. They can then download the Cisco Secure Client package manually.

You are not required to configure the Cisco Secure Client web-deploy package on the Secure Firewall ASA if you are using a different method for software updates or if you don't need profile editor integration with ASDM.

Secure Firewall ASA Web-Deployment Restrictions

- Loading multiple Cisco Secure Client packages for the same operating system to the Secure Firewall ASA is not supported.
- The OPSWAT definitions are not included in the Secure Firewall Posture module when web deploying. You must either manually deploy the Secure Firewall Posture module or load it on the ASA in order to deliver the OPSWAT definitions to the client.
- If your Secure Firewall ASA has only the default internal flash memory size, you could have problems storing and loading multiple Cisco Secure Client packages on the ASA. Even if you have enough space on flash to hold the package files, the Secure Firewall ASA could run out of cache memory when it unzips and loads the client images. For more information about the Secure Firewall ASA memory requirements when deploying Cisco Secure Client, and possibly upgrading the ASA memory, see the latest release notes for your VPN Appliance.
- Users can connect to the Secure Firewall ASA using the IP address or DNS, but the link-local secure gateway address is not supported.
- For Windows users, we recommend that you install Microsoft .NET framework 4.6.2 (and later) before installation or initial use. At startup, the Umbrella service checks if .NET framework 4.0 (or newer) is installed. If it is not detected, the Umbrella module is not activated, and a message is displayed. To go and then install the .NET Framework, you must reboot to activate the Umbrella module.

Web Deployment with ISE

Policies on ISE determine when the Cisco Secure Client will be deployed. The user opens a browser and connects to a resource controlled by ISE and is redirected to the Cisco Secure Client portal. That ISE Portal helps the user download and install Cisco Secure Client. The Portal downloads the Network Setup Assistant, and that tool helps the user install Cisco Secure Client.

ISE Deployment Restrictions

- If both ISE and Secure Firewall ASA are web deploying Cisco Secure Client, the configurations must match on both headends.
- The ISE server can only be discovered by the Cisco Secure Client ISE Posture agent if that agent is configured in the ISE Client Provisioning Policy. The ISE administrator configures either the NAC Agent or the Cisco Secure Client ISE Posture module under Agent Configuration > Policy > Client Provisioning.

Configuring Web Deployment on the ASA

Download the Cisco Secure Client Package

Download the latest Cisco Secure Client package from the Cisco Software Download webpage.

OS	AnyConnect Web-Deploy Package Names
Windows	cisco-secure-client-win-*version*-webdeploy-k9.pkg (for ARM64) cisco-secure-client-win-arm64-*version*-webdeploy-k9.pkg
macOS	cisco-secure-client-macos-*version*-webdeploy-k9.pkg
Linux (64-bit)	cisco-secure-client-linux64-*version*-webdeploy-k9.pkg (for ARM64) cisco-secure-client-linux-arm64-*version*-webdeploy-k9.pkg

Note You should not have different versions for the same operating system on the Secure Firewall ASA.

Load the Cisco Secure Client Package on the Secure Firewall ASA

Procedure

Step 1 Navigate to **Configuration** > **Remote Access** > **VPN** > **Network (Client) Access** > **AnyConnect Client Software**. The Cisco Secure Client panel displays the Cisco Secure Client images currently loaded on the Secure Firewall ASA. The order in which the images appear is the order the Secure Firewall ASA downloads them to remote computers.

Step 2 To add the Cisco Secure Client image, click **Add** and choose one of the following:

- Click **Browse Flash** to select the Cisco Secure Client image you have already uploaded to the Secure Firewall ASA.
- Click **Upload** to browse to the Cisco Secure Client image you have stored locally on your computer.

Step 3 Click **OK** or **Upload**.

Step 4 Click **Apply**.

Enable Additional Cisco Secure Client Modules

To enable additional features, specify the new module names in the group-policy or Local Users configuration. Be aware that enabling additional modules impacts download time. When you enable features, Cisco Secure Client must download those modules to the VPN endpoints.

Note If you choose Start Before Login, you must also enable this feature in the AnyConnect VPN profile.

Procedure

Step 1 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.

Step 2 Select a group policy and click **Edit** or **Add** a new group policy.

Step 3 In the navigation pane, select **VPN Policy** > **AnyConnect Client**. At **Client Modules to Download,** click **Add** and choose each module you want to add to this group policy. The modules that are available are the ones you added or uploaded to the Secure Firewall ASA.

Step 4 Click **Apply** and save your changes to the group policy.

Create a Client Profile in ASDM

You must add the Cisco Secure Client web-deployment package to the Secure Firewall ASA before you can create a client profile on the Secure Firewall ASA.

Procedure

Step 1 Navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile.**

Step 2 Select the client profile you want to associate with a group and click **Change Group Policy**.

Step 3 In the Change Policy for Profile policy name window, choose a group policy from the Available Group Policies field and click the right arrow to move it to the Policies field.

Step 4 Click **OK**.

Step 5 In the Cisco Secure Client profile page, click **Apply**.

Step 6 Click **Save**.

Step 7 When you have finished with the configuration, click **OK**.

Configuring Web Deployment on ISE

ISE can configure and deploy the Cisco Secure Client core VPN module, ISE Posture module, and OPSWAT (compliance module) to support posture for ISE. ISE can also deploy all the Cisco Secure Client modules and resources that can be used when connecting to the Secure Firewall ASA. When a user browses to a resource controlled by ISE:

- If ISE is behind a Secure Firewall ASA, the user connects the ASA, downloads Cisco Secure Client, and makes a VPN connection. If Cisco Secure Client ISE Posture was not installed by the Secure Firewall ASA, then the user is redirected to the Cisco Secure Client portal to install the ISE Posture.
- If ISE is not behind a Secure Firewall ASA, users connect to the Cisco Secure Client portal, which guides them to install the Cisco Secure Client resources defined in the Cisco Secure Client configuration on ISE. A common configuration is to redirect the browser to Cisco Secure Client provisioning portal if the ISE Posture status is unknown.
- When the user is directed to the Cisco Secure Client provisioning portal in ISE:
  - If the browser is Internet Explorer, ISE downloads Cisco Secure Client Downloader, and the Downloader loads the Cisco Secure Client.
  - For all other browsers, ISE opens the client provisioning redirection portal, which displays a link to download the Network Setup Assistant (NSA) tool. The user runs the NSA, which finds the ISE server, and downloads the Cisco Secure Client downloader.

    When the NSA is done running in Windows, it deletes itself. When it is done running on macOS, it must be manually deleted.

The ISE documentation describes how to:

- Create Cisco Secure Client configuration profiles in ISE
- Add Cisco Secure Client resources to ISE from a local device
- Add Cisco Secure Client provisioning resources from a remote site
- Deploy the Cisco Secure Client and resources



Note Because Cisco Secure Client ISE posture module does not support web proxy based redirection in discovery, Cisco recommends that you use non-redirection based discovery. You can find further information in the Client Provisioning Without URL Redirection for Different Networks section of the Cisco Identity Services Engine Administrator Guide.

ISE can configure and deploy the following Cisco Secure Client resources:

- Cisco Secure Client core VPN and other modules, including the ISE Posture module
- Profiles: Network Visibility Module,Cisco Secure Endpoint, VPN, Network Access Manager, Customer Feedback and ISE Posture
- Files for customization
  - UI Resources
  - Binaries, connection scripts and help files
- Localization files
  - Cisco Secure Client gettext translations for message localizations
  - Windows Installer Transforms

Prepare Cisco Secure Client Files for ISE Upload

- Download the Cisco Secure Client packages for your operating systems, and other Cisco Secure Client resources that you want to deploy to your local PC.

Note With Secure Firewall ASA, installation happens with the VPN downloader. With the download, the ISE posture profile is pushed via Secure Firewall ASA, and the discovery host needed for later provisioning the profile is available before the ISE posture module contacts ISE. Whereas with ISE, the ISE posture module will get the profile only after ISE is discovered, which could result in errors. Therefore, Secure Firewall ASA is recommended to push the ISE posture module when connected to a VPN.

- Create profiles for the modules you plan to deploy. At a minimum, create the Cisco Secure Client ISE Posture profile (ISEPostureCFG.xml).

Note An ISE posture profile with a Call Home List is mandatory for predeploying the ISE posture module, if non-redirection based discovery is used.

- Combine customization and localization resources into a ZIP archive, which is called a bundle in ISE. A bundle can contain:
  - Cisco Secure Client UI resources
  - VPN Connection Scripts
  - Help file(s)
  - Installer Transforms

  The Cisco Secure Client localization bundle can contain:
  - Cisco Secure Client gettext translations, in binary format
  - Installer transforms

Creating ISE bundles is described in Prepare AnyConnect Customizations and Localizations for ISE Deployment .

Configure ISE to Deploy Cisco Secure Client

You must upload the Cisco Secure Client package to ISE before you upload and create additional Cisco Secure Client resources.

Note When configuring the Cisco Secure Client configuration object in ISE, unchecking the VPN module under Cisco Secure Client module selection does not disable the VPN on the deployed/provisioned client.

1. In ISE, select **Policy** > **Policy Elements** > **results** > **.** Expand **Client Provisioning** to show **Resources**, and select **Resources**.
2. Select **Add** > **Agent resources from local disk**, and upload the Cisco Secure Client package file. Repeat adding agent resources from local disk for any other Cisco Secure Client resources that you plan to deploy.
3. Select **Add** > **AnyConnect Configuration** > **.** This Cisco Secure Client configuration configures modules, profiles, customization/language packages, and the OPSWAT package, as described in the following table.

   The Cisco Secure Client ISE Posture profile can be created and edited in ISE, on the Secure Firewall ASA, or in the Windows Cisco Secure Client Profile Editor. The following table describes the name of each Cisco Secure Client resource, and the name of the resource type in ISE.

   Table 4: Cisco Secure Client Resources in ISE

Prompt	ISE Resource Type and Description
Cisco Secure Client Package	CiscoSecureClientDesktopWindows CiscoSecureClientDesktopOSX CiscoSecureClientDesktopLinux CiscoTemporalAgentWindows CiscoTemporalAgentOSX
Compliance Module	CiscoSecureClientComplianceModuleWindows CiscoSecureClientComplianceModuleOSX CiscoSecureClientComplianceModuleLinux
Cisco Secure Client Profiles	AgentProfile ISE displays a checkbox for each profile provided by the uploaded Cisco Secure Client package.
Customization Bundle	AgentCustomizationBundle
Localization Bundle	AgentLocalizationBundle

4. Create a Role or OS-based client provisioning policy. Cisco Secure Client and the ISE legacy NAC/MAC agent can be selected for Client provisioning posture agents. Each CP policy can only provision one agent, either the Cisco Secure Client agent or the legacy NAC/MAC agent. When configuring the Cisco Secure Client agent, select one Cisco Secure Client configuration created in step 2.

Configuring Web Deployment on Secure Firewall Threat Defense

A Secure Firewall Threat Defense device is a Next Generation Firewall (NGFW) that provides secure gateway capabilities similar to the Secure Firewall ASA. Secure Firewall Threat Defense devices support Remote Access VPN (RA VPN) using the Cisco Secure Client only, no other clients, or clientless VPN access is supported. Tunnel establishment and connectivity are done with IPsec IKEv2 or SSL. IKEv1 is not supported when connecting to a Secure Firewall Threat Defense device.

Windows, macOS, and Linux Cisco Secure Client is configured on the Secure Firewall Threat Defense headend and deployed upon connectivity, giving remote users the benefits of an SSL or IKEv2 IPsec VPN client without the need for client software installation and configuration. In the case of a previously installed client, when the user authenticates, the Secure Firewall Threat Defense headend examines the revision of the client, and upgrades the client as necessary.

Without a previously installed client, remote users enter the IP address of an interface configured to download and install the Cisco Secure Client. The Secure Firewall Threat Defense headend downloads and installs the client that matches the operating system of the remote computer, and establishes a secure connection.

The Cisco Secure Client apps for Apple iOS and Android devices are installed from the platform app store. They require a minimum configuration to establish connectivity to the Secure Firewall Threat Defense headend. As with other headend devices and environments, alternative deployment methods, as described in this chapter, can also be used to distribute the Cisco Secure Client software.

Currently, only the Cisco Secure Client core VPN and the Cisco Secure Client VPN Profile can be configured on the Secure Firewall Threat Defense and distributed to endpoints. A Remote Access VPN Policy wizard in the Secure Firewall Management Center quickly and easily sets up these basic VPN capabilities.

Guidelines and Limitations for Cisco Secure Client and Secure Firewall Threat Defense

- The only supported VPN client is the Cisco Secure Client. No other clients or native VPNs are supported. Clientless VPN is not supported as its own entity; it is only used to deploy the Cisco Secure Client.
- Using Cisco Secure Client with Secure Firewall Threat Defense requires version 4.0 or later of Cisco Secure Client, and version 6.2.1 or later of the Secure Firewall Management Center.
- There is no inherent support for the Cisco Secure Client Profile Editor in the Secure Firewall Management Center; you must configure the VPN profiles independently. The VPN Profile and Cisco Secure Client VPN package are added as File Objects in the Secure Firewall Management Center, which become part of the RA VPN configuration.
- Browser Proxy is not supported.
- Authentication cannot be done on the Secure Firewall Threat Defense headend locally; therefore, configured users are not available for remote connections, and the Secure Firewall Threat Defense cannot act as a Certificate Authority. Also, the following authentication features are not supported:
  - Secondary or double authentication
  - Single Sign-on using SAML 2.0
  - TACACS, Kerberos (KCD Authentication) and RSA SDI
  - LDAP Authorization (LDAP Attribute Map)
  - RADIUS CoA

For details on configuring and deploying Cisco Secure Client on a Secure Firewall Threat Defense, see the *Firepower Threat Defense Remote Access VPN* chapter in the appropriate release of the Firepower Management Center Configuration Guide, Release 6.2.1 or later.

Updating Cisco Secure Client Software and Profiles

Cisco Secure Client can be updated in several ways. Upgrades to Cisco Secure Client from AnyConnect 4.x use the same process as upgrades from older versions of Secure Client 5 to the most recent versions of Secure Client 5.

- Cisco Secure Client—When Cisco Secure Client connects to the Secure Firewall ASA, the Cisco Secure Client Downloader checks to see if any new software or profiles have been loaded on the Secure Firewall ASA. It downloads those updates to the client, and the VPN tunnel is established.
- ASA or FTD Portal—You instruct your users to connect to the Secure Firewall ASA Clientless Portal to get updates. FTD downloads the core VPN module only.
- ISE—When a user connects to ISE, ISE uses its Cisco Secure Client configuration to decide if there are updated components or new posture requirements. Upon authorization, the Network Access Device (NAD) redirects the users to the ISE portal, and the Cisco Secure Client downloader is installed on the client to manage the package extraction and installation. You must upload the deploy package to the Secure Firewall ASA headend and make sure that the versions of Cisco Secure Client match the Secure Firewall ASA and ISE deployment package versions.

  Receiving a message that "automatic software updates are required but cannot be performed while the VPN tunnel is established" indicates that the configured ISE policy requires updates. When the Cisco Secure Client version on the local device is older than what's configured on ISE, you have the following options, because client updates are not allowed while the VPN is active:

  - Deploy Cisco Secure Client update out of band
  - Configure the same version of Cisco Secure Client on the Secure Firewall ASA and ISE

You can allow the end user to delay updates, and you can also prevent clients from updating even if you do load updates to the headend.

Upgrade Example Flows

Prerequisites

The following examples assume that:

- You have created a Dynamic Authorization Control List (DACL) in ISE that uses the posture status of the client to determine when to redirect the client to the Cisco Secure Client Client Provisioning portal on ISE, and that DACL has been pushed to the Secure Firewall ASA.
- ISE is behind the Secure Firewall ASA.

Cisco Secure Client is Installed on the Client

1. User starts Cisco Secure Client, provides credentials, and clicks Connect.
2. Secure Firewall ASA opens SSL connection with client, passes authentication credentials to ISE, and ISE verifies the credentials.
3. Cisco Secure Client launches the Cisco Secure Client Downloader, which performs any upgrades, and initiates a VPN tunnel.

If ISE Posture was not installed by the Secure Firewall ASA, then

1. A user browses to any site and is redirected to Cisco Secure Client provisioning portal on ISE by the DACL.
2. With the browser, the user downloads and executes Network Setup Assistant (NSA), which downloads and starts the Cisco Secure Client Downloader.
3. The Cisco Secure Client Downloader performs any Cisco Secure Client upgrades configured on ISE, which now includes the Cisco Secure Client ISE Posture module.
4. The ISE Posture agent on the client starts posture.

Cisco Secure Client is Not Installed

1. The user browses to a site, which starts a connection to the Secure Firewall ASA Portal.
2. The user provides authentication credentials, which are passed to ISE, and verified.
3. Cisco Secure Client Downloader is launched by ActiveX control on Internet Explorer and by Java applet on other browsers.
4. Cisco Secure Client Downloader performs upgrades configured on Secure Firewall ASA and then initiates VPN tunnel. Downloader finishes.

If ISE Posture was not installed by the Secure Firewall ASA, then

1. User browses to a site again and is redirected to Cisco Secure Client client provisioning portal on ISE.
2. The Cisco Secure Client Downloader performs any upgrades configured on ISE through the existing VPN tunnel, which includes adding the Cisco Secure Client ISE Posture module.
3. ISE Posture agent starts posture assessment.

Disabling Cisco Secure Client Auto Update

It is possible to disable or limit Cisco Secure Client automatic updates by configuring and distributing client profiles.

- In the VPN Client Profile:
  - Auto Update disables automatic updates. You can include this profile with the Cisco Secure Client web-deployment installation or add to an existing client installation. You can also allow the user to toggle this setting.
- In the VPN Local Policy Profile:
  - Bypass Downloader prevents any updated content on the Secure Firewall ASA from being downloaded to the client.
  - Update Policy offers granular control over software and profiles updates when connecting to different headends.

Prompting Users to Download Cisco Secure Client During WebLaunch

You can configure the Secure Firewall ASA to prompt remote users to start web deployment, and configure a time period within which they can choose to download Cisco Secure Client or go to the clientless portal page.

Prompting users to download Cisco Secure Client is configured on a group policy or user account. The following steps show how to enable this feature on a group policy.

Procedure

Step 1 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.

Step 2 Select a group policy and click **Edit** or **Add** a new group policy.

Step 3 In the navigation pane, choose **Advanced** > **AnyConnect Client** > **Login Settings**. Uncheck the **Inherit** check box, if necessary, and select a Post Login setting.

If you choose to prompt users, specify a timeout period and select a default action to take when that period expires in the Default Post Login Selection area.

Step 4 **Click** OK and be sure to apply your changes to the group policy, then click **Save**.

Allowing Users to Defer Upgrade

You can force users to accept the Cisco Secure Client update by disabling AutoUpdate, as described in Disabling AnyConnect Auto Update. AutoUpdate is on by default.

You can also allow users to defer client update until later by setting Deferred Update. If Deferred Update is configured, then when a client update is available, Cisco Secure Client opens a dialog asking the user if they would like to update, or to defer. Deferred Upgrade is supported by all Windows, Linux and macOS.

Configure Deferred Update on Secure Firewall ASA

On the Secure Firewall ASA, Deferred Update is enabled by adding custom attributes and then referencing and configuring those attributes in the group policies. You must create and configure **all** custom attributes to use Deferred Upgrade.

The procedure to add custom attributes to your Secure Firewall ASA configuration is dependent on the ASA/ASDM release you are running. See the Cisco ASA Series VPN CLI or ASDM Configuration Guide that corresponds to your ASA/ASDM deployed release for custom attribute configuration procedures.

The following attributes and values configure Deferred Update in ASDM:

Custom Attribute *	Valid Values	Default Value	Notes
DeferredUpdateAllowed	true false	false	True enables deferred update. If deferred update is disabled (false), the settings below are ignored.

Custom Attribute *	Valid Values	Default Value	Notes
DeferredUpdateMinimumVersion	*x.x.x*	0.0.0	Minimum version of Cisco Secure Client that must be installed for updates to be deferrable. The minimum version check applies to all modules enabled on the headend. If any enabled module (including VPN) is not installed or does not meet the minimum version, then the connection is not eligible for deferred update. If this attribute is not specified, then a deferral prompt is displayed (or auto-dismissed) regardless of the version installed on the endpoint.
DeferredUpdateDismissTimeout	0-300 (seconds)	150 seconds	Number of seconds that the deferred upgrade prompt is displayed before being dismissed automatically. This attribute only applies when a deferred update prompt is to be displayed (the minimum version attribute is evaluated first). If this attribute is missing, then the auto-dismiss feature is disabled, and a dialog is displayed (if required) until the user responds. Setting this attribute to zero allows automatic deferral or upgrade to be forced based on: • The installed version and the value of DeferredUpdateMinimumVersion. • The value of DeferredUpdateDismissResponse.
DeferredUpdateDismissResponse	defer update	update	Action to take when DeferredUpdateDismissTimeout occurs.

* The custom attribute values are case-sensitive.

Configure Deferred Update in ISE

Procedure

Step 1 Follow this navigation:
a) Choose **Policy** > **Results** .
b) Expand **Client Provisioning**.
c) Select **Resources**, and click **Add** > **Agent Resources from Local Disk**.
d) Upload the Cisco Secure Client pkg file, and choose **Submit**.

Step 2 Upload any other Cisco Secure Client resources you have created.

Step 3 On **Resources**, add an **AnyConnect Configuration** using the Cisco Secure Client package that you uploaded. The Cisco Secure Client configuration has fields to configure Deferred Update.

Set the Update Policy

Update Policy Overview

Cisco Secure Client software and profile updates occur when they are available and allowed by the client upon connecting to a headend. Configuring the headend for Cisco Secure Client updates makes them available. The Update Policy settings in the VPN Local Policy file determine if they are allowed.

Update policy is sometimes referred to as software locks. When multiple headends are configured, the update policy is also referred to as the multiple domain policy.

By default, the Update Policy settings allow software and profile updates from any headend. Set the Update Policy parameters to restrict this as follows:

- Allow, or authorize, specific headends to update all Cisco Secure Client software and profiles by specifying them in the **Server Name** list.

  The headend server name can be an FQDN or an IP Address. They can also be wild cards, for example: *.example.com.

  See Authorized Server Update Policy Behavior below for a full description of how the update occurs.

- For all other unspecified, or unauthorized headends:
  - Allow or disallow software updates of the VPN core module and other optional modules using the **Allow Software Updates From Any Server** option.
  - Allow or disallow VPN Profile updates using the **Allow VPN Profile Updates From Any Server** option.
  - Allow or disallow other service module profile updates using the **Allow Service Profile Updates From Any Server** option.
  - Allow or disallow ISE Posture Profile updates using the **Allow ISE Posture Profile Updates From Any Server** option.
  - Allow or disallow Compliance Module updates using the **Allow Compliance Module Updates From Any Server** option.

    See Unauthorized Server Update Policy Behavior below for a full description of how the update occurs.

Authorized Server Update Policy Behavior

When connecting to an authorized headend identified in the **Server Name** list, the other Update Policy parameters do not apply and the following occurs:

- The version of the Cisco Secure Client package on the headend is compared to the version on the client to determine if the software should be updated.
  - If the version of the Cisco Secure Client package is older than the version on the client, no software updates occur.
  - If the version of the Cisco Secure Client package is the same as the version on the client, only software modules that are configured for download on the headend and not present on the client are downloaded and installed.

- If the version of the Cisco Secure Client package is newer than the version on the client, software modules configured for download on the headend, as well as software modules already installed on the client, are downloaded and installed.

- The VPN profile, ISE Posture profile, and each service profile on the headend is compared to that profile on the client to determine if it should be updated:
  - If the profile on the headend is the same as the profile on the client, it is not updated.
  - If the profile on the headend is different than the profile on the client, it is downloaded.

Unauthorized Server Update Policy Behavior

When connecting to an unauthorized headend, the **Allow ... Updates From Any Server** options are used to determine how Cisco Secure Client is updated as follows:

- **Allow Software Updates From Any Server:**
  - If this option is checked, software updates are allowed for this unauthorized Secure Firewall ASA. Updates are based on version comparisons as described above for authorized headends.
  - If this option is not checked, software updates do not occur. In addition, VPN connection attempts will terminate if updates, based on version comparisons, should have occurred.

- **Allow VPN Profile Updates From Any Server:**
  - If this option is checked, the VPN profile is updated if the VPN profile on the headend is different than the one on the client.
  - If this option is not checked, the VPN profile is not updated. In addition, VPN connection attempts will terminate if the VPN profile update, based on differentiation, should have occurred.

- **Allow Service Profile Updates From Any Server:**
  - If this option is checked, each service profile is updated if the profile on the headend is different than the one on the client.
  - If this option is not checked, the service profiles are not updated.

- **Allow ISE Posture Profile Updates From Any Server:**
  - If this option is checked, the ISE Posture profile is updated when the ISE Posture profile on the headend is different than the one on the client.
  - If this option is not checked, the ISE Posture profile is not updated. ISE Posture profile is required for the ISE Posture agent to work.

- **Allow Compliance Module Updates From Any Server:**
  - If this option is checked, the Compliance Module is updated when the Compliance Module on the headend is different than the one on the client.
  - If this option is not checked, the Compliance Module is not updated. The Compliance Module is required for the ISE Posture agent to work.

Update Policy Guidelines

- Enable remote users to connect to a headend using its IP address by listing that server's IP address in the authorized **Server Name** list. If the user attempts to connect using the IP address but the headend is listed as an FQDN, the attempt is treated as connecting to an unauthorized domain.
- Software updates include downloading customizations, localizations, scripts and transforms. When software updates are disallowed, these items will not be downloaded. Do not rely on scripts for policy enforcement if some clients will not be allowing script updates.
- Downloading a VPN profile with Always-On enabled deletes all other VPN profiles on the client. Consider this when deciding whether to allow or disallow VPN profiles updates from unauthorized, or non-corporate, headends.
- If no VPN profile is downloaded to the client due to your installation and update policy, the following features are unavailable:

Service Disable	Untrusted Network Policy
Certificate Store Override	Trusted DNS Domains
Show Pre-connect Message	Trusted DNS Servers
Local LAN Access	Always-On
Start Before Login	Captive Portal Remediation
Local proxy connections	Scripting
PPP Exclusion	Retain VPN on Logoff
Automatic VPN Policy	Device Lock Required
Trusted Network Policy	Automatic Server Selection

- In Windows, the downloader creates a separate text log (UpdateHistory.log) that records the download history. This log includes the time of the updates, the Secure Firewall ASA that updated the client, the modules updated, and what version was installed before and after the upgrade. This log file is stored here:

  `%ALLUSERESPROFILE%\Cisco\Cisco Secure Client\Logs` directory.

- You must restart the Cisco Secure Client service to pick up any changes in the Local Policy file.

Update Policy Example

This example shows the client update behavior when the Cisco Secure Client version on the client differs from various Secure Firewall ASA headends.

Given the following Update Policy in the VPN Local Policy XML file:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
xmlns=http://schemas.xmlsoap.org/encoding/
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
<FipsMode>false</FipsMode>
<BypassDownloader>false</BypassDownloader><RestrictWebLaunch>false</RestrictWebLaunch>
<StrictCertificateTrust>false</StrictCertificateTrust>
```

```
<RestrictPreferenceCaching>false</RestrictPreferenceCaching>
<RestrictTunnelProtocols>false</RestrictTunnelProtocols>
<UpdatePolicy>
<AllowSoftwareUpdatesFromAnyServer>false</AllowSoftwareUpdatesFromAnyServer>
<AllowComplianceModuleUpdatesFromAnyServer>true</AllowComplianceModuleUpdatesFromAnyServer>
<AllowManagementVPNProfileUpdatesFromAnyServer>true</AllowManagementVPNProfileUpdatesFromAnyServer>
<AllowISEProfileUpdatesFromAnyServer>true</AllowISEProfileUpdatesFromAnyServer>
<AllowServiceProfileUpdatesFromAnyServer>false</AllowServiceProfileUpdatesFromAnyServer>
<AllowScriptUpdatesFromAnyServer>true</AllowScriptUpdatesFromAnyServer>
<AllowHelpUpdatesFromAnyServer>true</AllowHelpUpdatesFromAnyServer>
<AllowResourceUpdatesFromAnyServer>true</AllowResourceUpdatesFromAnyServer>
<AllowLocalizationUpdatesFromAnyServer>true</AllowLocalizationUpdatesFromAnyServer>
<AuthorizedServerList>
<ServerName>seattle.example.com</ServerName>
<ServerName>newyork.example.com</ServerName>
</AuthorizedServerList>
</UpdatePolicy>
</AnyConnectLocalPolicy>
```

With the following Secure Firewall ASA headend configuration:

ASA Headend	AnyConnect Package Loaded	Modules to Download
seattle.example.com	Version 4.7.01076	VPN, Network Access Manager
newyork.example.com	Version 4.7.03052	VPN, Network Access Manager
raleigh.example.com	Version 4.7.04056	VPN, Posture

The following update sequence is possible when the client is currently running Cisco Secure Client VPN core and Network Access Manager modules:

- The client connects to seattle.example.com, an authorized server configured with the same version of Cisco Secure Client. If the VPN and Network Access Manager profiles are available for download and different than the ones on the client, they will also be downloaded.
- The client then connects to newyork.example.com, an authorized Secure Firewall ASA configured with a newer version of Cisco Secure Client. The VPN and Network Access Manager modules are upgraded. Profiles that are available for download and different than the ones on the client are also downloaded.
- The client then connects to raleigh.example.com, an unauthorized Secure Firewall ASA. Even though a software update is necessary and a software update is available, the update is not allowed due to the policy determining version upgrades are not allowed. The connection terminates.

Locations of User Preferences Files on the Local Computer

Cisco Secure Client stores some profile settings on the user computer in a user preferences file and a global preferences file. Cisco Secure Client uses the local file to configure user-controllable settings in the Preferences tab of the client GUI and to display information about the last connection, such as the user, the group, and the host.

Cisco Secure Client uses the global file for actions that occur before logon, for example, AutoConnect On Start.

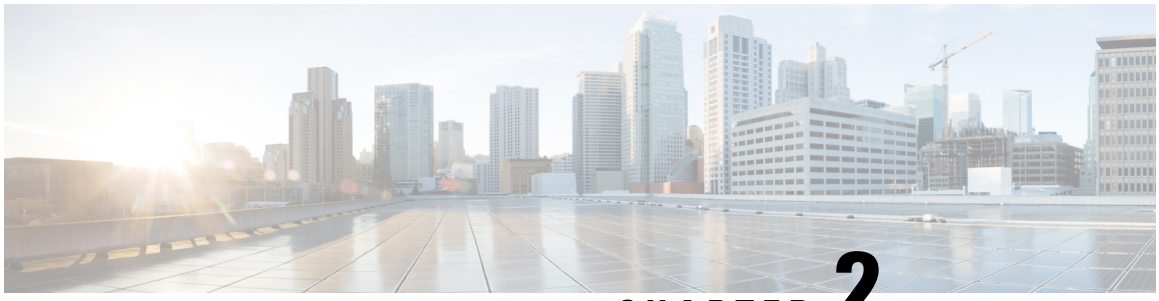
The following table shows the filenames and installed paths for preferences files that are placed under VPN sub directory for Cisco Secure Client:

Operating System	Type	File and Path
Windows	User	%LOCALAPPDATA%\Cisco\Cisco Secure Client\VPN\preferences.xml
	Global	%ALLUSERSPROFILE%\Cisco\Cisco Secure Client\VPN\preferences_global.xml
macOS	User	$HOME/.vpn/.anyconnect
	Global	/opt/cisco/secureclient/vpn/.anyconnect_global
Linux	User	$HOME/.vpn/.anyconnect
	Global	/opt/cisco/secureclient/.vpn/.anyconnect_global

Port Used by Cisco Secure Client

The following tables list the ports used by the Cisco Secure Client for each protocol.

Protocol	Cisco Secure Client Port
TLS (SSL)	TCP 443
SSL Redirection	TCP 80 (optional)
DTLS	UDP 443 (optional, but highly recommended)
IPsec/IKEv2	UDP 500, UDP 4500



CHAPTER 2

Customize and Localize Cisco Secure Client and Installer

- Modify Cisco Secure Client Installation Behavior, on page 41
- Enable DSCP Preservation, on page 48
- Set Public DHCP Server Route, on page 49
- Customize the Cisco Secure Client GUI Text and Messages, on page 49
- Create Custom Icons and Logos for the Cisco Secure Client GUI, on page 57
- Create and Upload the Cisco Secure Client Help File, on page 63
- Write and Deploy Scripts, on page 64
- Write and Deploy Custom Applications with the Cisco Secure Client API, on page 68
- Use the Cisco Secure Client CLI Commands, on page 68
- Prepare Cisco Secure Client Customizations and Localizations for ISE Deployment, on page 72

Modify Cisco Secure Client Installation Behavior

Disable Customer Experience Feedback

The Customer Experience Feedback module is enabled by default. This module provides Cisco with anonymous information about what features and modules customers have enabled and are using. This information gives us insight into the user experience so that Cisco can continue to improve quality, reliability, performance, and user experience.

To manually disable the Customer Experience Feedback module, create a CustomerExperience_Feedback.xml file using the standalone profile editor. You must stop the Cisco Secure Client service, name the file CustomerExperience_Feedback.xml, and put it in the C:\ProgramData\Cisco\Cisco Secure Client\CustomerExperienceFeedback\ directory. When the file is created with the disable flag set, you can manually deploy this to Cisco Secure Client. To check the results, open the Cisco Secure Client About menu and verify that the Customer Experience Feedback module is not listed in the Installed Module section.

You can disable the Customer Experience Feedback module using:

- A Customer Feedback Experience module client profile—Uncheck Enable Customer Experience Feedback Service, and distribute the profile.
- An MST file—Extract secureclient-win-disable-customer-experience-feedback.mst from secureclient-vpn-transforms-X.X.xxxxx.zip.

Modify Installation Behavior, Windows

Use the following Windows installer properties to modify Cisco Secure Client installation behavior. In the ISO image, the installer program setup.hta is HTML and can be edited.

Note Cisco Secure Client does not support Windows Installer ADVERTISE mode.

- Command-Line Parameters—One or more properties are passed as parameters on the command-line installer, msiexec. This method is for predeployment; it is not supported by web deployment.
- Installer Transform—You can modify the installer property table with a transform. Several tools are available to create transforms; one common tool is Microsoft Orca. The Orca tool is part of the Microsoft Windows Installer Software Development Kit (SDK), which is included in the Microsoft Windows SDK. To get the Windows SDK, browse to http://msdn.microsoft.com, and search for the SDK for your version of Windows.

  Transforms can be used for predeploy only. (Only Cisco signed transforms will work for web deploy when the downloader invokes the installer.) You can apply your own transforms through the out-of-band methods, but the details are outside the scope of this guide.

Limitations

The Cisco Secure Client uninstall prompt is not customizable.

Windows Installer Properties That Customize Client Installations

The following Windows installer properties customize Cisco Secure Client installations. Bear in mind that there are many other Windows installer properties supported by Microsoft that you can use.

- Resetting the System MTU—When the VPN installer property (RESET_ADAPTER_MTU) is set to 1, the installer resets all Windows network adapter MTU settings to their default value. The system must be rebooted for the changes to take effect.
- Setting Windows Lockdown—Cisco recommends that end users be given limited rights to the Cisco Secure Client on their device. If an end user warrants additional rights, installers can provide a lockdown capability that prevents users and local administrators from switching off or stopping the Cisco Secure Client services. You can also stop the services from the command prompt with the service password.

  The MSI installers for VPN, Network Access Manager, Network Visibility Module, and Umbrella Roaming Security Module support a common property (LOCKDOWN). When LOCKDOWN is set to a non-zero value, Windows service(s) associated with that installer cannot be controlled by users or local administrators on the endpoint device. We recommend using the sample transform that we provide to set this property, and apply the transform to each MSI installer that you want to have locked down. You can download the sample transforms from the Cisco Secure Client software download page.

  If you deploy the core client plus one or more optional modules, you must apply the LOCKDOWN property to each of the installers. This operation is one way only and cannot be removed unless you re-install the product.
- Hiding Cisco Secure Client from the Add/Remove Program List—You can hide the installed Cisco Secure Client modules from a user's Add/Remove Programs list in the Windows Control Panel. Passing

ARPSYSTEMCOMPONENT=1 to the installer prevents that module from appearing in the list of installed programs.

We recommend that you use the sample transform we provide to set this property, applying the transform to each MSI installer for each module that you want to hide. You can download the sample transforms from the Cisco Secure Client software download page.

Import a Customized Installer Transform to the Secure Firewall Adaptive Security Appliance

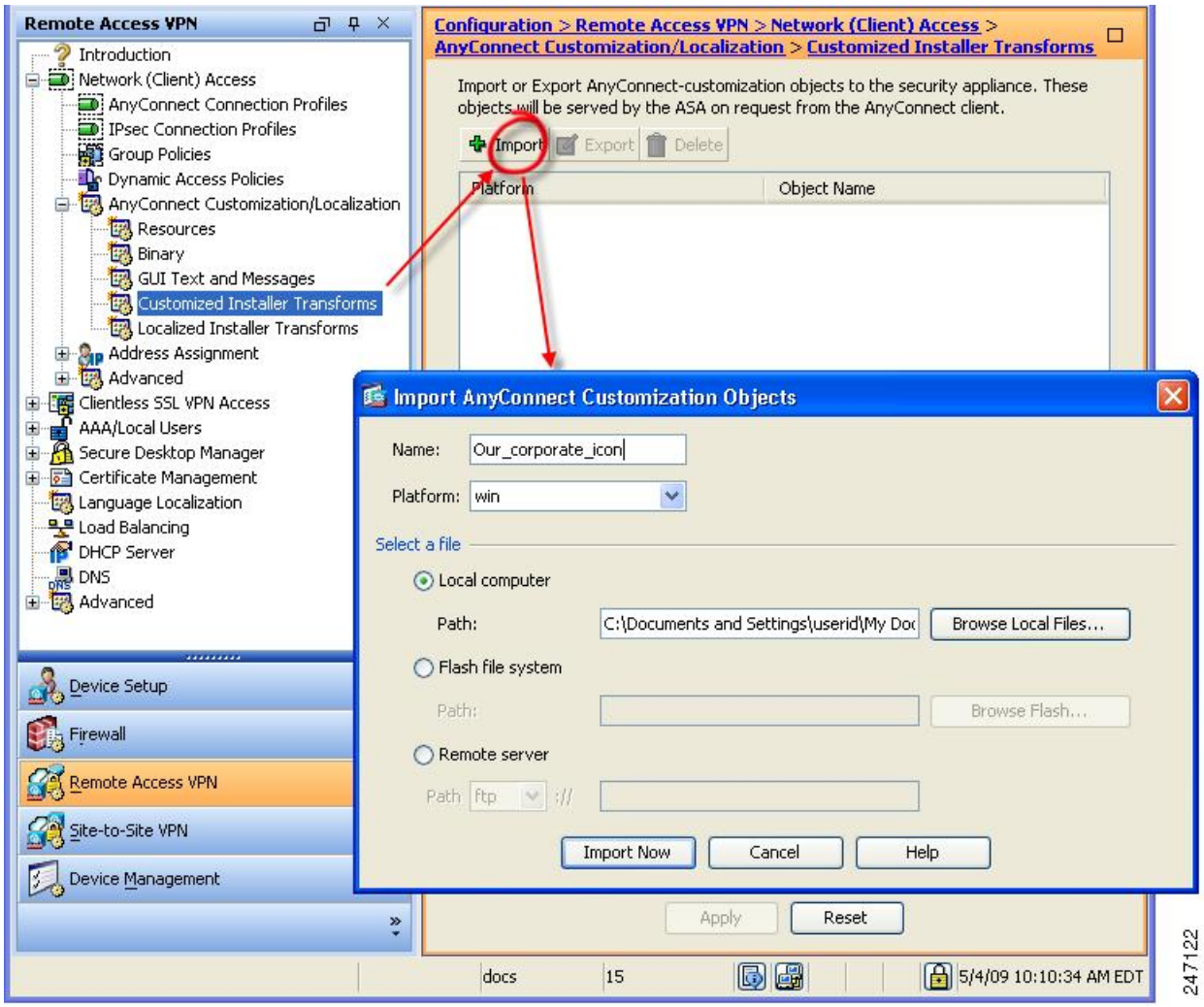
Importing a Cisco provided Windows transform to the Secure Firewall ASA allows you to use it for web deployment.

Procedure

Step 1 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Customization/Localization** > **Customized Installer Transforms**.

Step 2 Click **Import**.

The Import AnyConnect Customization Objects windows displays:



Step 3 Enter the name of the file to import. The name of the transform file determines to which module the installer transform file applies. You can apply transforms globally or per module with the following syntax:

a) *_name*.mst: applied to all installers

b) <moduleid>*_name*.mst: applied to a single module installer

c) *name*.mst: applied to the VPN installer only

Step 4 Select a platform and specify the file to import. Click **Import Now**. The file now appears in the table of installer transforms.

What to do next

If the transform file is incorrect, the installation/upgrade process for remote Windows users may fail with a *Failed to install Cisco Secure Client* error. This error represents itself in the DART file as DOWNLOADER_ERROR_INTEGRITY_CHECK_FAILED.

Localize the Cisco Secure Client Installer Screens

You can translate the messages displayed by the Cisco Secure Client installer. The Secure Firewall ASA uses a transform to translate the messages displayed by the installer. The transform alters the installation but leaves the original security-signed MSI intact. These transforms only translate the installer screens and do not translate the client GUI screens.



Note Every release of Cisco Secure Client includes a localized transform that administrators can upload to the Secure Firewall ASA whenever they upload Cisco Secure Client packages with new software. If you are using our localization transform, make sure to update them with the latest release from cisco.com whenever you upload a new Cisco Secure Client package.

We currently offer transforms for 30 languages. These transforms are available in the following .zip file on the Cisco Secure Client software download page at cisco.com:

`secureclient-win-<VERSION>-webdeploy-k9-lang.zip`

In this file, <VERSION> is the version of Cisco Secure Client release.

The archive contains the transforms (.mst files) for the available translations. If you need to provide a language to remote users that is not one of the 30 languages we provide, you can create your own transform and import it to the Secure Firewall ASA as a new language. With Orca, the database editor from Microsoft, you can modify existing installations and new files. Orca is part of the Microsoft Windows Installer Software Development Kit (SDK) which is included in the Microsoft Windows SDK.

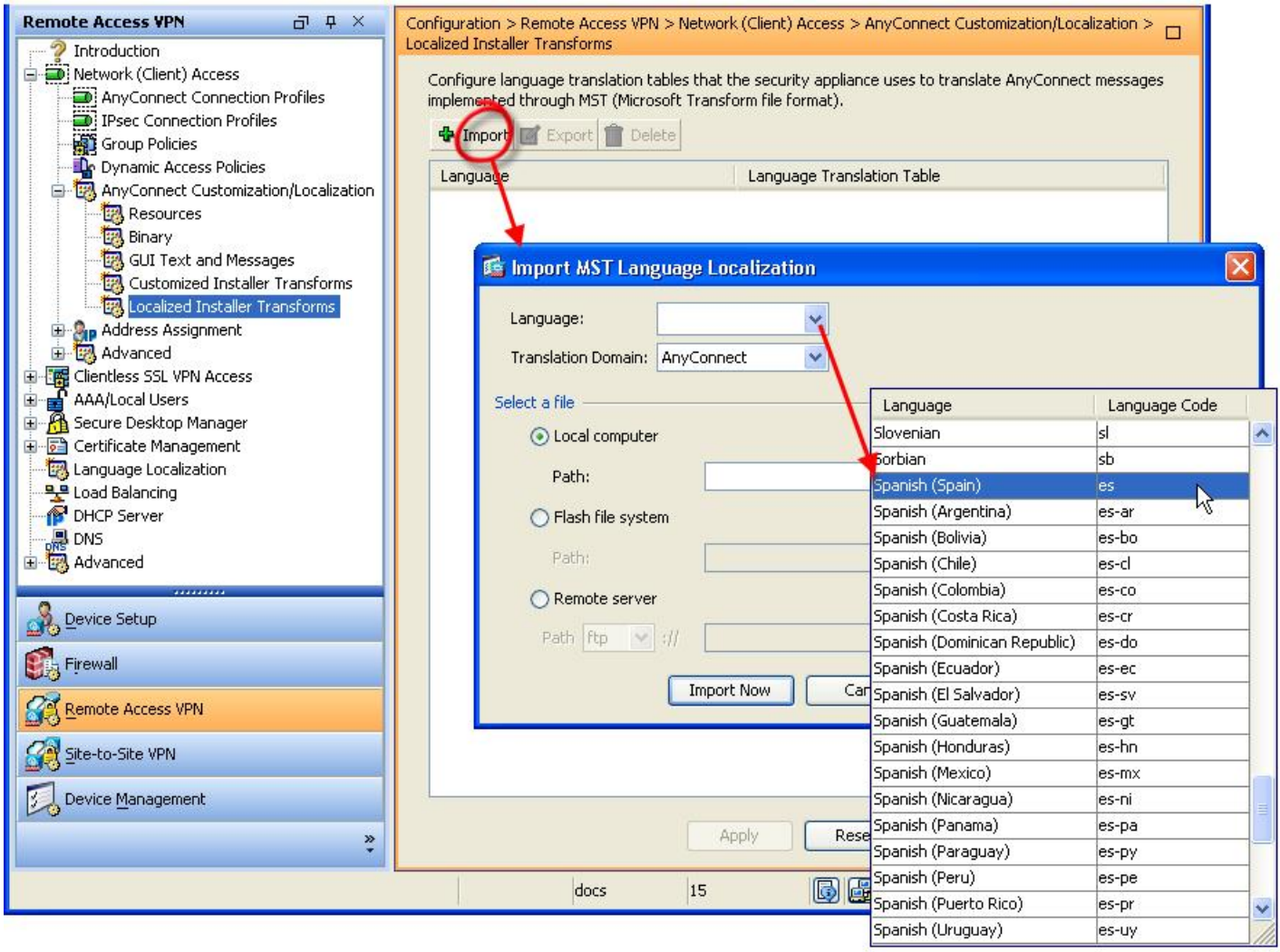
Import a Localized Installer Transform to the Secure Firewall ASA

The following procedure shows how to import a transform to the Secure Firewall ASA using ASDM.

Procedure

Step 1 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Customization/Localization** > **Localized Installer Transforms**.

Step 2 Click **Import**. The Import MST Language Localization window opens:



Step 3 Click the **Language** drop-down list to choose a language (and the industry-recognized abbreviation) for this transform. If you enter the abbreviation manually, be sure to use an abbreviation recognized by browsers and operating systems.

Step 4 Click **Import Now**.
A message displays saying you successfully imported the table.

Step 5 Click **Apply** to save your changes.

In this procedure we specified the language as Spanish (es). The following illustration shows the new transform for Spanish in the list of Languages for Cisco Secure Client.



Modify Installation Behavior, macOS

The Cisco Secure Client installer cannot be localized. The strings used by the installer come from the macOS installer application, not the Cisco Secure Client installer.

Note You cannot manipulate the optional module selection that is seen by the user in the installer UI. Changing the default optional module selection in the installer UI requires editing of the installer, which would then invalidate the signature.

Customize Installer Behavior on macOS with ACTransforms.xml

No standard way to customize .pkg behavior is provided for macOS, so we created ACTransforms.xml. When this XML file is positioned with the installer, the installer reads this file before running the installation. You must place the file in a specific location relative to the installer. The installer searches in this order to see if a modification is found:

1. In a “Profile” directory in the same directory as the .pkg installer file.
2. In a “Profile” directory in the root of a mounted disk image volume.
3. In a “Profile” directory in the root of a mounted disk image volume.

The XML file has this format:

```
<ACTransforms>
<PropertyName1>Value</PropertyName1>
<PropertyName2>Value</PropertyName2>
</ACTransforms>
```

For example, the macOS ACTransforms.xml property is DisableVPN to create a “stand-alone” deployment of Network Visibility Module. ACTransforms.xml is in the Profiles directory in the DMG file.

Disable the Customer Experience Feedback Module

The Customer Experience Feedback module is enabled by default. To switch this feature off on macOS:

Procedure

Step 1 Convert the dmg package from read-only to read-write using Disk Utility or hdiutil. For example:

```
hdiutil convert cisco-secure-client-macosx-version-predeploy-k9.dmg -format UDRW -o
cisco-secure-client-macosx-version-predeploy-k9-rw.dmg
```

Step 2 Edit ACTransforms.xml, and set or add the following value, if it is not already set.

```
<DisableCustomerExperienceFeedback>false</DisableCustomerExperienceFeedback>
```

Modify Installation Behavior, Linux

Customizing Installer Behavior on Linux with ACTransform.xml

No standard way to customize .pkg behavior is provided for Linux, so we created ACTransforms.xml. When this XML file is positioned with the installer, the installer reads this file before running the installation. You must place the file in a specific location relative to the installer. The installer searches in this order to see if a modification is found:

- In a “Profile” directory in the same directory as the .rpm/.deb installer file
- In a “Profile” directory in the root of a mounted disk image volume
- In a “Profile” directory in the same directory as the .dmg file

The XML file, ACTransforms.xml, in the Profiles directory in the predeployment package has this format:

```
<ACTransforms>

<PropertyName1>Value</PropertyName1>

<PropertyName2>Value</PropertyName2>

</ACTransforms>
```

Enable DSCP Preservation

You can set a custom attribute to control Differentiated Services Code Point (DSCP) on Windows or macOS platforms for DTLS connection only. DSCP preservation allows devices to prioritize latency sensitive traffic; the router takes into account whether this is set and marks prioritized traffic to improve outbound connection quality.

The custom attribute type is DSCPPreservationAllowed, and the valid values are True or False.

Note By default Cisco Secure Client performs DSCP preservation (True). To disable it, set the custom attribute value to false on the headend and reinitiate the connection.

This feature is configured in ASDM at **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > Advanced > AnyConnect Client > Custom Attributes**. Refer to the *Enable DSCP Preservation* section in the appropriate release of the Cisco ASA Series VPN ASDM Configuration Guide for the configuration process.

Set Public DHCP Server Route

To allow local DHCP traffic to flow in the clear when Tunnel All Network is configured, Cisco Secure Client adds a specific route to the local DHCP server when the client connects. To prevent data leakage on this route, Cisco Secure Client also applies an implicit filter on the LAN adapter of the host device, blocking all traffic for that route except DHCP traffic. If you are connecting to the external interface and using a local DHCP server once a connection is established, a specific route to that server is created, pointing to the NIC and not the virtual adapter. If other services are running on the same server (such as WINS or DNS), this route breaks these services after the VPN session is established.

On Windows, by setting a group policy custom attribute, you can control the creation of the public DHCP server route. The no-dhcp-server-route custom attribute must be present and set to true to avoid creating the public DHCP server route upon tunnel establishment.

This feature is configured in ASDM at **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > Advanced > AnyConnect Client > Custom Attributes**. Refer to the appropriate release of the Cisco ASA Series VPN ASDM Configuration Guide for the configuration process.

Customize the Cisco Secure Client GUI Text and Messages

The Secure Firewall ASA uses translation tables to translate user messages displayed by Cisco Secure Client. The translation tables are text files with strings of translated message text. You can edit existing messages or add additional languages using ASDM or using transforms (for Windows).

The following Windows sample transforms for localization are available on www.cisco.com:

- Language localization transform files for predeploy package for Windows platforms
- Language localization transform files for web-deploy package for Windows platforms

The Cisco Secure Client package file for Windows contains a default English language template for Cisco Secure Client messages. The Cisco Secure Firewall ASA automatically imports this file when you load the Cisco Secure Client package on the ASA. This template contains the latest changes to message strings in the Cisco Secure Client software. You can use it to create new translation tables for other languages, or you can import one of the following translation tables available on www.cisco.com (see Import Translation Tables to the Secure Firewall ASA, on page 53):

- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Dutch
- French
- French (Canadian)
- German
- Hungarian
- Italian

- Japanese
- Korean
- Polish
- Portuguese (Brazil)
- Russian
- Spanish (Latin American)

In Cisco Secure Client release 5.0, default localization files for various languages are included with installation. Refer to Localization on Desktop Devices, on page 51.

The following sections contain procedures for translating GUI text and messages if the desired languages are not available or if you wish to further customize imported translation tables:

- Add or Edit the AnyConnect Text and Messages. You can make changes to the message file by adding or editing the file to change message text for one or more message IDs in one of the following ways:
  - Typing your changes into the text in the open dialog.
  - Copying the text in the open dialog to a text editor, making your changes, and pasting the text back into the dialog.
- Import Translation Tables to the Secure Firewall ASA, on page 53. You can export the message file by clicking Save to File, editing the file, and importing it back into the ASDM.

After you update the translation table on the Secure Firewall ASA, the updated messages are not applied until the client is restarted and makes another successful connection.



Note If you are not deploying the client from the Secure Firewall ASA and are using a corporate software deployment system such as Altiris Agent, you can manually convert the Cisco Secure Client translation table (anyconnect.po) to a .mo file using a catalog utility such as Gettext and install the .mo file to the proper folder on the client computer. See "Create Message Catalogs for Enterprise Deployment" section on page 3-22 for more information.

Guidelines and Limitations

Cisco Secure Client is not fully compliant with all internationalization requirements, exceptions include:

- Date/Time formats do not always follow locale requirements.
- Right to left languages are not supported.
- Some strings are truncated in the UI due to hardcoded field lengths.
- A few hardcoded English strings remain such as:
  - Status messages, when updating.
  - Untrusted server messages.
  - Deferred update messages.

Localization on Desktop Devices

With Cisco Secure Client installation, default localization files for various languages are included. The Secure Client will use string localization from ASDM if available. If that language file is not available, the Secure Client uses the default embedded language matching the provided system locale language. If no match is found, English is used.

When Cisco Secure Client gets the translations from ASA, it will try to fill in any translation gaps using the default translations. For example, if administrators have strings that they didn't provide, Cisco Secure Client will still translate, if the string is part of the default translations. Localization data is provided for these languages by default:

- Canadian French (Canada) — (fr-CA)
- Chinese (China) — (zh-CN)
- Chinese (Simplified) — (zh-HANS)
- Chinese (Taiwan) — (zh-TW)
- Chinese (Traditional) — (zh-HANT)
- Czech (Czech Republic) — (cs-CZ)
- Dutch (Netherlands) — (nl-nNL)
- French (France) — (fr-FR)
- German (Germany) — (de-DE)
- Hungarian (Hungary) — (hu-HU)
- Italian (Italy) — (it-IT)
- Japanese (Japan) — (ja-JP)
- Korean (Korea) — (ko-KR)
- Polish (Poland) — (pl-PL)
- Portuguese (Brazil) — (pt-BR)
- Russian (Russia) — (ru-RU)
- Spanish (Spain) — (es-ES)

Add or Edit the Cisco Secure Client Text and Messages

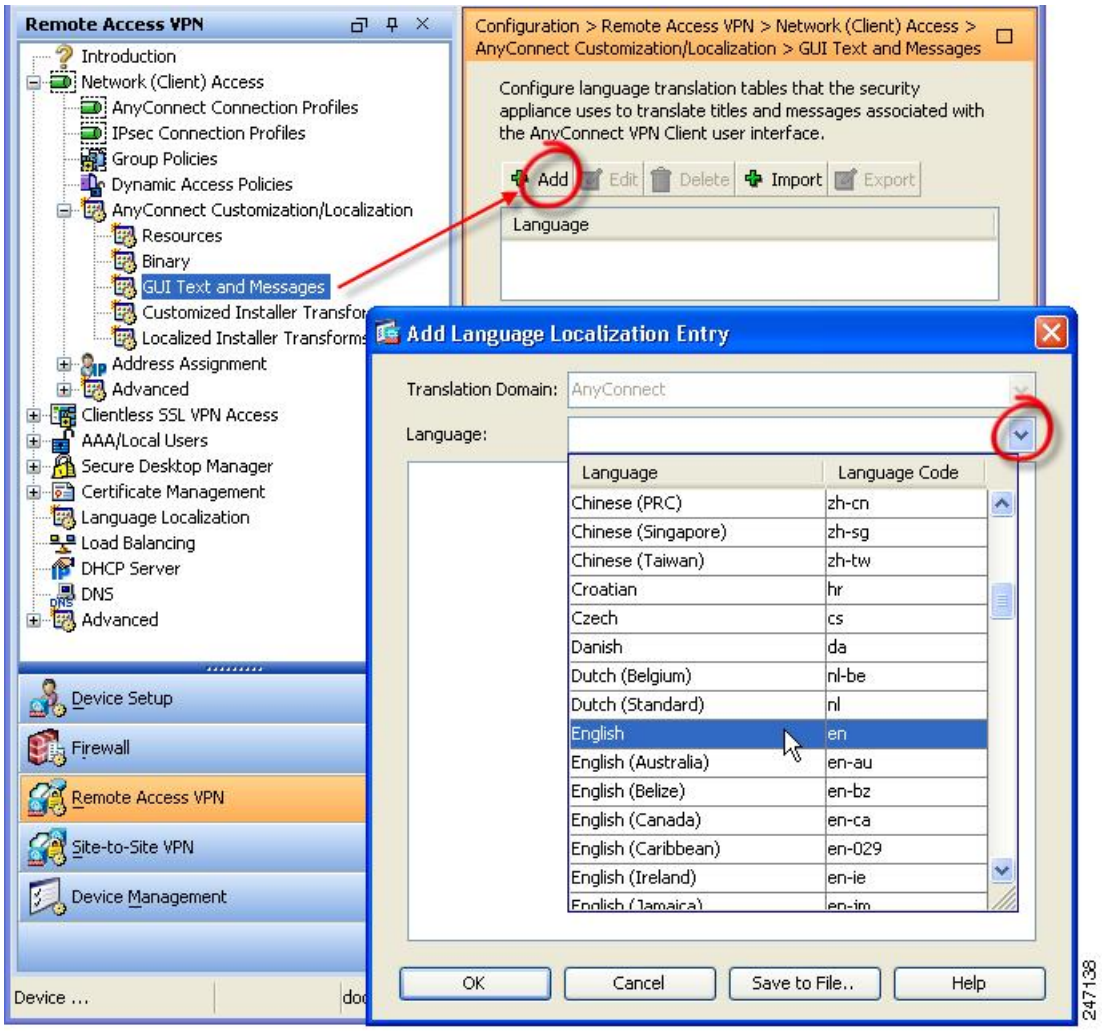
You can make changes to the English messages displayed on the Cisco Secure Client GUI by adding or editing the English translation table and changing message text for one or more message IDs. After you open the message file, you can edit it by:

- Typing your changes into the text in the open dialog.
- Copying the text in the open dialog to a text editor, making your changes, and pasting the text back into the dialog.
- Exporting the message file by clicking Save to File, editing the file, and importing it into the ASDM.

Procedure

Step 1 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Customization/Localization** > **GUI Text and Messages**.

Step 2 Click **Add**. The Add Language Localization Entry window displays.

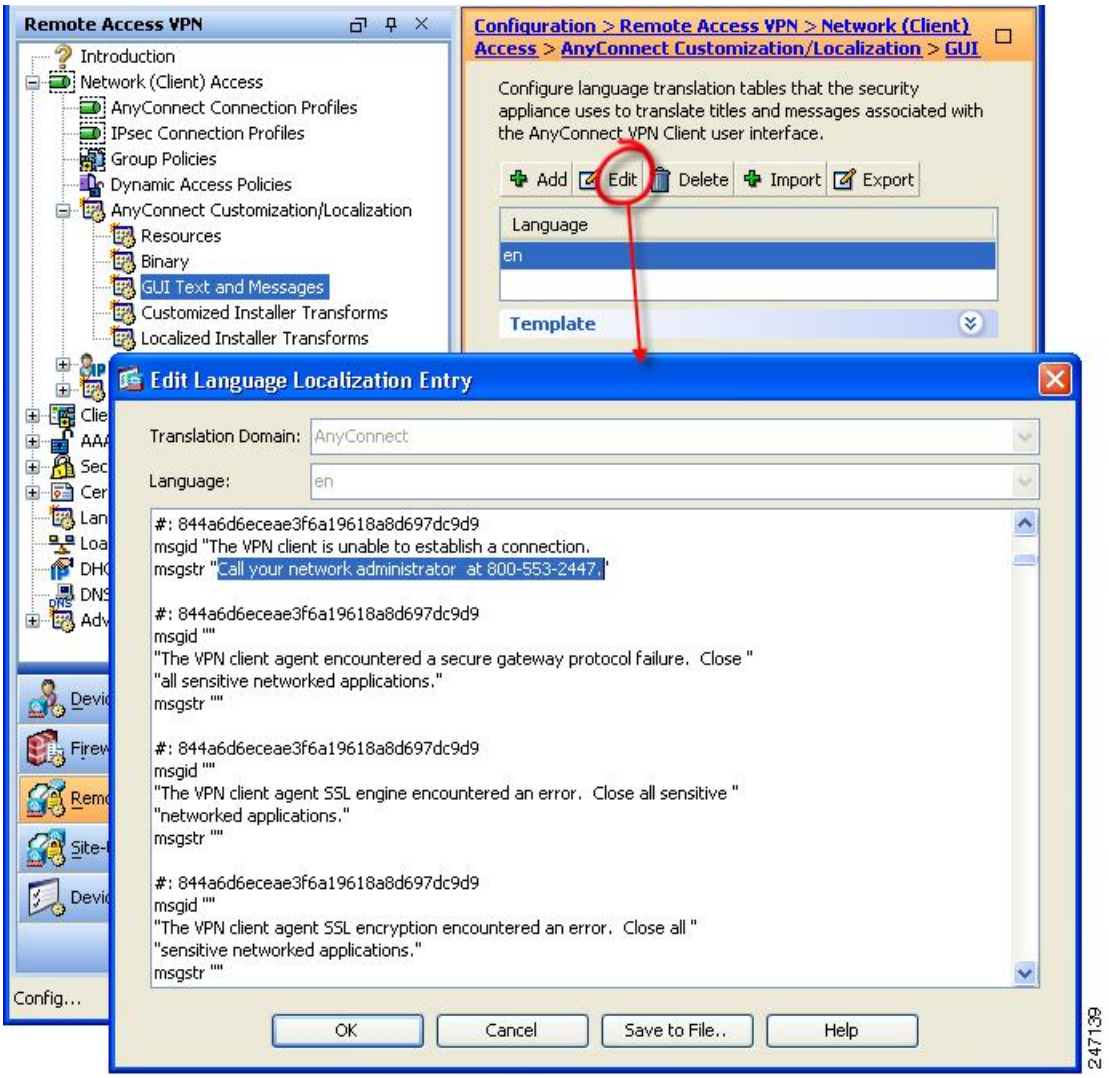


Step 3 Click the Language drop-list and specify the language as English (en). The translation table for English displays in the list of languages in the pane.

Step 4 Click **Edit** to begin editing the messages.

The Edit Language Localization Entry window displays. The text between the quotes of msgid is the default English text displayed by the client and must not be changed. The msgstr string contains text that the client uses to replace the default text in msgid. Insert your own text between the quotes of the msgstr.

In the example below, we insert “Call your network administrator at 800-553-2447.”



Step 5 Click **OK** and then **Apply** to save your changes.

Import Translation Tables to the Secure Firewall ASA

Procedure

Step 1 Download the desired translation table from www.cisco.com.

Step 2 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Customization/Localization** > **GUI Text and Messages**.

Step 3 Click **Import**. The Import Language Localization Entry window displays.

Step 4 Choose the appropriate Language from the drop-down list.

Step 5 Specify where the translation table will be imported from.

Step 6 Click **Import Now**. This translation table will be deployed to Cisco Secure Client clients with this preferred language. Localization will be applied after Cisco Secure Client restarts and connects.

Create Message Catalogs for Enterprise Deployment

If you are not deploying the client with the Secure Firewall ASA, and are using an enterprise software deployment system such as Altiris Agent, you can manually convert the Cisco Secure Client translation table to a message catalog using a utility such as Gettext. After converting the table from a .po file to a .mo file, you then place the file in the proper folder on the client computer.



Note GetText and PoeEdit are third-party software applications. The recommended method for Cisco Secure Client GUI customization is to take the default .mo file from the Secure Firewall ASA and edit it as necessary for any deployments to the client. Using the default .mo avoids potential conversion issues resulting from third-party applications such as GetText and PoeEdit.

Gettext is a utility from The GNU Project and runs in the command window. See the GNU website at gnu.org for more information. You can also use a GUI-based utility that uses Gettext, such as Poedit. This software is available at poedit.net. This procedure creates a message catalog using Gettext:

Cisco Secure Client Message Template Directories

Cisco Secure Client message templates are located in the folders listed below for each operating system:



Note The `\l10n` directory is part of each directory path listed below. The directory name is spelled: lower case l ("el"), one, zero, lower case n.

- For Windows— `<DriveLetter>:\ProgramData\Cisco\Cisco Secure Client\l10n\<LANGUAGE-CODE>\LC_MESSAGES`
- For macOS and Linux— `/opt/cisco/secureclient/l10n/<LANGUAGE-CODE>/LC_MESSAGES`

Procedure

Step 1 Download the Gettext utilities from http://www.gnu.org/software/gettext/ and install Gettext on a computer that you use for administration (not a remote user computer).

Step 2 Retrieve a copy of the Cisco Secure Client message template AnyConnect.po on a computer with Cisco Secure Client installed.

Step 3 Edit the AnyConnect.po file (use notepad.exe or any plain text editor) to change strings as desired.

Step 4 Run the Gettext message file compiler to create the .mo file from the .po file:

msgfmt -o AnyConnect.mo AnyConnect.po

Step 5 Place a copy of the .mo file in the correct message template directory on the user's computer.

Merge New Messages into a Customized Translation Table on the Secure Firewall ASA

New user messages are added to some releases of Cisco Secure Client. To enable translation of these new messages, new message strings are added to the translation template that is packaged with the latest client image. If you have created translation tables based on the template included with the previous client, the new messages are not automatically displayed to remote users. You must merge the latest template with your translation table to ensure your translation table has these new messages.

There are free third-party tools to perform the merge. Gettext utilities from The GNU Project is available for Windows and runs in the command window. See the GNU website at gnu.org for more information. You can also use a GUI-based utility that uses Gettext, such as Poedit. This software is available at poedit.net. Both methods are covered in the procedure below.



Note This procedure assumes that you have already loaded the latest Cisco Secure Client image package to the Secure Firewall ASA. The template is not available for export until you do.

Procedure

Step 1 Export the latest Cisco Secure Client Translation Template from **Remote Access VPN** > **Language Localization** > **Templates**. Export the template with the filename as `AnyConnect.pot`. This filename ensures that the msgmerge.exe program recognizes the file as a message catalog template.

Step 2 Merge the Cisco Secure Client Template and Translation Table.

If you are using the Gettext utilities for Windows, open a command prompt window and run the following command. The command merges the Cisco Secure Client translation table (.po) and the template (.pot), creating the new `AnyConnect_merged.po` file:

```
msgmerge -o AnyConnect_merged.po AnyConnect.po AnyConnect.pot
```

The following example shows the results of the command:

```
C:\Program Files\GnuWin32\bin> msgmerge -o AnyConnect_merged.po AnyConnect.po AnyConnect.pot
..................................... done.
```

If you are using Poedit, first open the AnyConnect.po file; go to **File > Open > <AnyConnect.po>**. Then merge it with the template; go to **Catalog > Update** from POT file <AnyConnect.pot>. Poedit displays an Update Summary window with both new and obsolete strings. Save the file, which you will import in the next step.

Step 3 Import the merged translation table to **Remote Access VPN** > **Language Localization**. Click **Import**, specify a language, and select **AnyConnect** as the Translation Domain. Specify the file to import as `AnyConnect_merged.po`.

Determining the Language on the Client

When the remote user connects to the Secure Firewall ASA and downloads the client, Cisco Secure Client determines the preferred language of the device and applies the appropriate translation table, by detecting the specified system locale. If no localization is established from ASA, it attempts one of the 17 default translations that come with Secure Client. If none of those translations are a match,English is used.

If you want to bypass the default localization files embedded within the client (stored in the Program Files), refer to the Bypass Default Localization preference in Local Policy. When this preference in the Local Policy is changed to *true*, it skips the usage of translations that come with Secure Client and instead uses English.

View/Change the Specified System Locale in Windows

Procedure

Step 1 Navigate to the **Control Panel** > **Region > Administrative > Change system locale** > **.**

Step 2 Choose the desired language from the **Current system locale** drop down.

When the system locale is changed, Windows requires a restart for the changes to take effect. Refer to the documentation associated with your specific operating system for additional details.

View/Change the Specified System Locale in macOS

Procedure

Step 1 Navigate to the **System Settings** > **General > Language & Region > Region** > **.**

Step 2 Change to the desired region.

Step 3 Add Cisco Secure Client as an application in the Language & region and set the desired language.

When the system locale is changed, macOS requires a restart for the changes to take effect. Refer to the documentation associated with your specific operating system for additional details.

View/Change the Specified System Locale in Linux

Procedure

Step 1 Navigate to the **Settings** > **Region > Language** > **.**

Step 2 Change to the desired language.

Step 3 Change to the desired region.

When the system locale is changed, Linux requires a restart for the changes to take effect. Refer to the documentation associated with your specific operating system for additional details.

Create Custom Icons and Logos for the Cisco Secure Client GUI

The tables in this section list the Cisco Secure Client files that you can replace for each operating system. The images in the tables are used by the Cisco Secure Client core VPN and Network Access Manager module.

Restrictions

- The filenames of your custom components must match the filenames used by the Cisco Secure Client GUI, which are different for each operating system and are case sensitive for macOS and Linux. For example, if you want to replace the corporate logo for Windows clients, you must import your corporate logo as company_logo.png. If you import it as a different filename, the Cisco Secure Client installer does not change the component. However, if you deploy your own executable to customize the GUI, the executable can call resource files using any filename.
- If you import an image as a resource file (such as company_logo.bmp), the image that you import customizes Cisco Secure Client until you reimport another image using the same filename. For example, if you replace company_logo.bmp with a custom image and then delete the image, the client continues to display your image until you import a new image (or the original Cisco logo image) using the same filename.

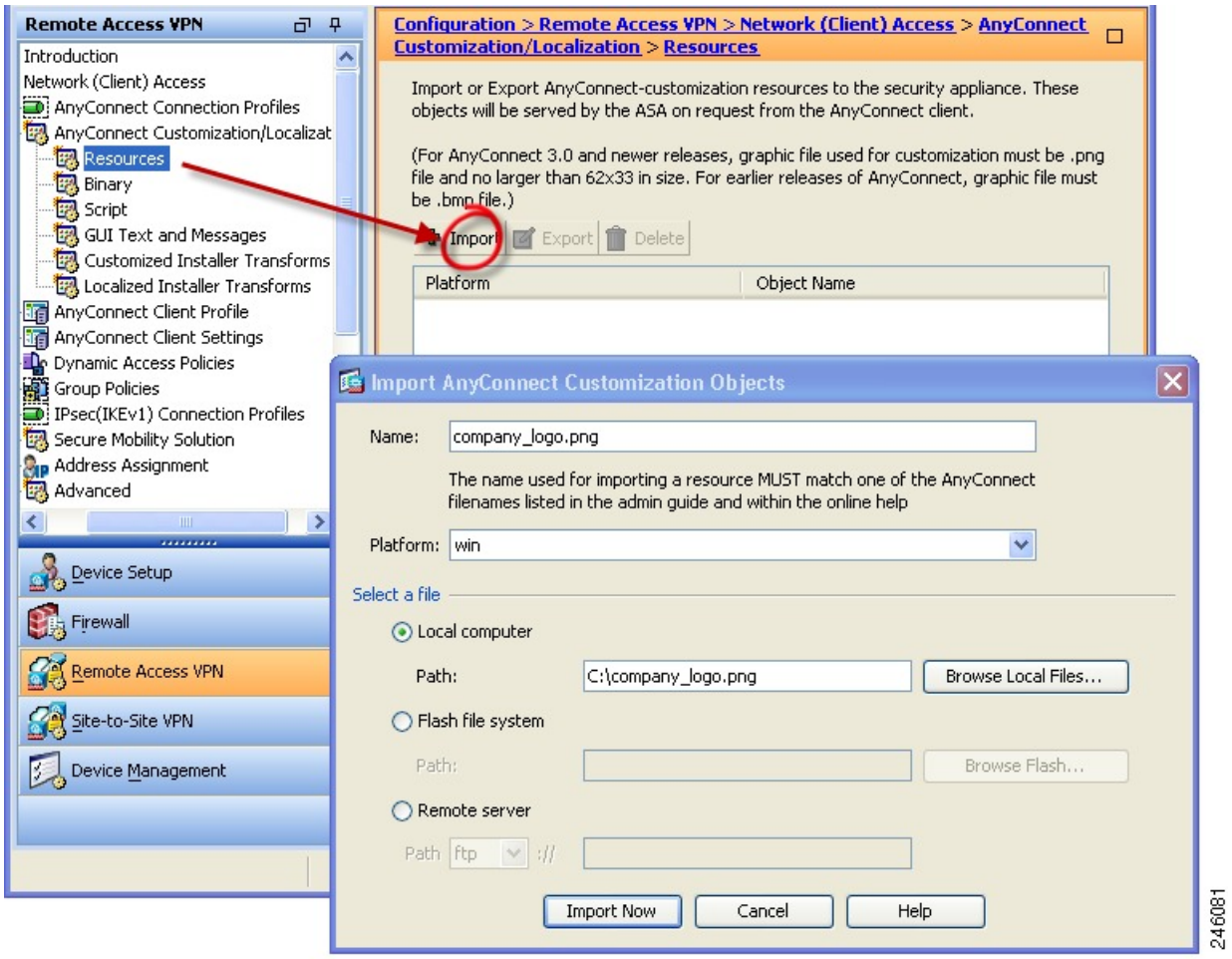
Replace Cisco Secure Client GUI Components

You can customize Cisco Secure Client by importing your own custom files to the security appliance, which deploys the new files with the client.

Procedure

Step 1 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Customization/Localization** > **Resources**.

Step 2 Click **Import**. The **Import AnyConnect Customization Objects** window displays.



Step 3 Enter the name of the file to import.

Step 4 Select a platform and specify the file to import. Click **Import Now**. The file now appears in the list of objects.

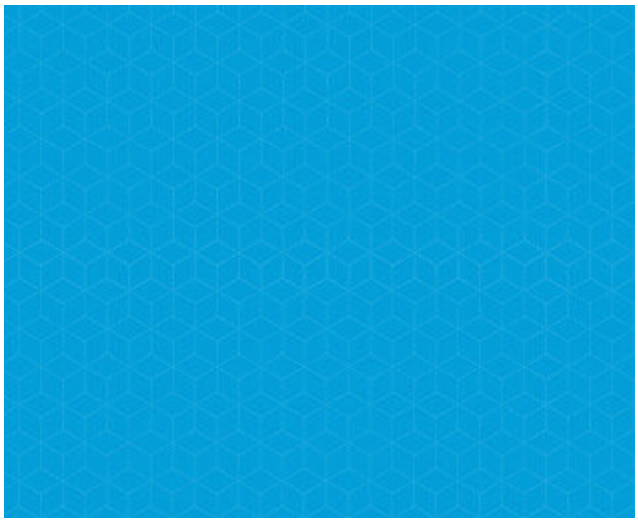
Cisco Secure Client Icons and Logos for Windows

All files for Windows are located in:

`%PROGRAMFILES%\Cisco\Cisco Secure Client\res\`

Note %PROGRAMFILES% refers to the environment variable by the same name. In most Windows installations, this is `C:\Program Files`.

Filename and Description in Windows Installation	Image Size (Pixels, L x H) and Type
about.png The About button in the upper-right corner of the Advanced dialog. The size is not adjustable. 	24 x 24 PNG
about_hover.png The About button in the upper-right corner of the Advanced dialog. The size is not adjustable. 	24 x 24 PNG
app_logo.png 128 x 128 is the maximum size. If your custom file is not that size, it is resized to 128 x 128 in the application. If it is not in the same ratio, it is stretched. 	128 x 128 PNG
attention.ico System tray icon alerting the user to a condition requiring attention or interaction. For example, a dialog about the user credentials. The size is not adjustable. 	16 x 16 ICO
company_logo.png The company logo displayed in the top-left corner of the tray flyout and Advanced dialog. 97 x 58 is the maximum size. If your custom file is not that size, it is resized to 97 x 58 in the application. If it is not in the same ratio, it is stretched. 	97 x 58 (maximum) PNG

Filename and Description in Windows Installation	Image Size (Pixels, L x H) and Type
company_logo_alt.png The company logo displayed in the bottom-right corner of the About dialog. 97 x 58 is the maximum size. If your custom file is not that size, it is resized to 97 x 58 in the application. If it is not in the same ratio, it is stretched. 	97 Xx58 PNG
cues_bg.jpg The background image for the tray flyout, Advanced window, and About dialog. Because images are not stretched, using a replacement image that is too small results in black space. 	1260 x 1024 JPEG
error.ico System tray icon alerting the user that something is critically wrong with one or more components. The size is not adjustable. 	16 x 16 ICO
neutral.ico System tray icon indicating that client components are operating correctly. The size is not adjustable. 	16 x 16 ICO

Filename and Description in Windows Installation	Image Size (Pixels, L x H) and Type
transition_1.ico System tray icon that displays along with transition_2.ico and transition_3.ico indicating that one or more client components are in transition between states (for example, when the VPN is connecting or when Network Access Manager is connecting). The three icon files display in succession, appearing to be a single icon bouncing from left to right. The size is not adjustable. 	16 x 16 ICO
transition_2.ico System tray icon that displays along with transition_1.ico and transition_3.ico indicating that one or more client components are in transition between states (for example, when the VPN is connecting or when Network Access Manager is connecting). The three icon files display in succession, appearing to be a single icon bouncing from left to right. The size is not adjustable. 	16 x 16 ICO
transition_3.ico System tray icon that displays along with transition_1.ico and transition_2.ico indicating that one or more client components are in transition between states (for example, when the VPN is connecting or when the Network Access Manager is connecting). The three icon files display in succession, appearing to be a single icon bouncing from left to right. The size is not adjustable. 	16 x 16 ICO
vpn_connected.ico System tray icon indicating that the VPN is connected. The size is not adjustable. 	16 x 16 ICO

Cisco Secure Client Icons and Logos for Linux

All files for Linux are located in:

```
/opt/cisco/secure client/pixmaps
```

The following table lists the files that you can replace and the client GUI area that is affected.

Filename and Description in Linux Installation	Image Size (Pixels, L x H) and Type
company-logo.png Corporate logo that appears on each tab of the user interface. Use PNG images no bigger than 62x33 pixels. 	142 x 92 PNG
cvc-about.png Icon that appears on the About tab. 	16 x 16 PNG
cvc-connect.png Icon that appears next to the Connect button, and on the Connection tab. 	16 x 16 PNG
cvc-disconnect.png Icon that appears next to the Disconnect button. 	16 x 16 PNG
cvc-info.png Icon that appears on the Statistics tab. 	16 x 16 PNG
systray_connected.png Tray icon that displays when the client is connected. 	16 x 16 PNG
systray_notconnected.png Tray icon that displays when the client is not connected. 	16 x 16 PNG

Filename and Description in Linux Installation	Image Size (Pixels, L x H) and Type
systray_disconnecting.png Tray icon that displays when the client is disconnecting. 	16 x 16 PNG
systray_quarantined.png Tray icon that displays when the client is quarantined. 	16x16 PNG
systray_reconnecting.png Tray icon that displays when the client is reconnecting. 	16 x 16 PNG
vpnui48.png Main program icon. 	48 x 48 PNG

Cisco Secure Client Icons and Logos for macOS

Cisco Secure Client icons and logos for macOS GUI resource customization on macOS are currently not supported.

Create and Upload the Cisco Secure Client Help File

To provide Cisco Secure Client users with help, create a help file with instructions about your site and load it on the Secure Firewall ASA. When users connect with Cisco Secure Client, the help file is downloaded, and the help icon displays on the Cisco Secure Client user interface. When the user clicks the help icon, the browser opens the help file. PDF and HTML files are supported.

Procedure

Step 1 Create an HTML file named `help_AnyConnect.html`.

Step 2 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Customization/Localization** > **Binary**.

Step 3 Import the **help_AnyConnect.xxx** file. The supported formats are: PDF, HTML, HTM, and MHT.

Step 4 On your device, bring up Cisco Secure Client and connect to your Secure Firewall ASA. The help file will be downloaded to the client device.
You should see that the help icon is added to the UI automatically.

Step 5 Click the help icon to open the help file in the browser.

If the help icon does not appear, check the help directory to see if the Cisco Secure Client downloader was able to retrieve the help file.

The "help_" part of the filename is removed by the downloader, so you should see AnyConnect.html in one of the following directories, depending on the operating system:

- Windows—`C:\ProgramData\Cisco\Cisco Secure Client\Help`
- macOS—`/opt/cisco/secureclient/help`

Write and Deploy Scripts

Cisco Secure Client lets you download and run scripts when the following events occur:

- Upon the establishment of a new client VPN session with the security appliance. We refer to a script triggered by this event as an *OnConnect* script because it requires this filename prefix.
- Upon the tear-down of a client VPN session with the security appliance. We refer to a script triggered by this event as an *OnDisconnect* script because it requires this filename prefix.

The establishment of a new client VPN session initiated by Trusted Network Detection triggers the OnConnect script (assuming the requirements are satisfied to run the script), but the reconnection of a persistent VPN session after a network disruption does not trigger the OnConnect script.

Some examples that show how you might want to use this feature include:

- Refreshing the group policy upon VPN connection.
- Mapping a network drive upon VPN connection, and un-mapping it after disconnection.
- Logging on to a service upon VPN connection, and logging off after disconnection.

Cisco Secure Client supports script launching during WebLaunch and stand-alone launches.

These instructions assume you know how to write scripts and run them from the command line of the targeted endpoint to test them.

Note The Cisco Secure Client software download site provides some example scripts; if you examine them, remember that they are only examples. They may not satisfy the local computer requirements for running them and are unlikely to be usable without customizing them for your network and user needs. Cisco does not support example scripts or customer-written scripts.

Scripting Requirements and Limitations

Be aware of the following requirements and limitations for scripts:

- Number of Scripts Supported—Cisco Secure Client runs only one OnConnect and one OnDisconnect script; however, these scripts may launch other scripts.
- File Formats—Cisco Secure Client identifies the OnConnect and onDisconnect script by the filename. It looks for a file whose name begins with OnConnect or OnDisconnect regardless of file extension. The first script encountered with the matching prefix is executed. It recognizes an interpreted script (such as VBS, Perl, or Bash) or an executable.
- Script Language—The client does not require the script to be written in a specific language but does require an application that can run the script to be installed on the client computer. Thus, for the client to launch the script, the script must be capable of running from the command line.
- Restrictions on Scripts by the Windows Security Environment—On Microsoft Windows, Cisco Secure Client can only launch scripts after the user logs onto Windows and establishes a VPN session. Thus, the restrictions imposed by the user's security environment apply to these scripts; scripts can only execute functions that the user has rights to invoke. Cisco Secure Client hides the cmd window during the execution of a script on Windows, so executing a script to display a message in a .bat file for testing purposes does not work.
- Enabling the Script—By default, the client does not launch scripts. Use the Cisco Secure Client profile EnableScripting parameter to enable scripts. The client does not require the presence of scripts if you do so.



Note Although there is no requirement for XML profiles beyond setting this *EnableScripting* parameter, it is expected by the vpnagent that the profile be pushed from the headend. Because the *EnableScripting* setting is enforced after the VPN session is established, the setting remains at the default (EnableScripting set to *false*) if no VPN profile was pushed from the headend via the Group-Policy attributes. Even though the XML profile is loaded prior to the VPN establishment, features like certificate store override, SBL, certificate store, and such require the OnConnect/OnDisconnect script to operate based on the VPN headend Group-Policy attributes.

- Client GUI Termination—Client GUI termination does not necessarily terminate the VPN session; the OnDisconnect script runs after session termination.
- Running Scripts on 64-bit Windows—The Cisco Secure Client is a 32-bit application. When running on a 64-bit Windows version, it uses the 32-bit version of cmd.exe.

  Because the 32-bit cmd.exe lacks some commands that the 64-bit cmd.exe supports, some scripts could stop executing when attempting to run an unsupported command, or run partially and stop. For example, the msg command, supported by the 64-bit cmd.exe, may not be understood by the 32-bit version of Windows 7 (found in %WINDIR%\SysWOW64).

  Therefore, when you create a script, use commands supported by the 32-bit cmd.exe.

Write, Test, and Deploy Scripts

Write and test your scripts on the targeted operating system. If a script cannot run properly from the command line on the native operating system, then Cisco Secure Client cannot run it properly.

Procedure

Step 1 Write and test your scripts.

Step 2 Choose how to deploy the scripts:

- Use ASDM to import the script as a binary file to the Secure Firewall ASA.

  Go to **Network (Client) Access** > **AnyConnect Customization/Localization** > **Script**.

  If you use ASDM version 6.3 or later, the Secure Firewall ASA adds the prefix scripts_ and the prefix OnConnect or OnDisconnect to your filename to identify the file as a script. When the client connects, the security appliance downloads the script to the proper target directory on the remote computer, removes the scripts_ prefix and leaves the OnConnect or OnDisconnect prefix. For example, if you import the script myscript.bat, the script appears on the security appliance as scripts_OnConnect_myscript.bat. On the remote computer, the script appears as OnConnect_myscript.bat.

  If you use an ASDM version earlier than 6.3, you must import the scripts with the following prefixes:

  - scripts_OnConnect
  - scripts_OnDisconnect

    To ensure the scripts run reliably, configure all Secure Firewall ASAs to deploy the same scripts. If you modify or replace a script, use the same name as the previous version and assign the replacement script to all of the Secure Firewall ASAs that the users might connect to. When the user connects, the new script overwrites the one with the same name.

- Use an enterprise software deployment system to deploy scripts manually to the VPN endpoints.

  If you use this method, use the script filename prefixes below:

  - OnConnect
  - OnDisconnect

    Install the scripts in the following directory:

Table 5: Required Script Locations

OS	Directory
Microsoft Windows	%ALLUSERSPROFILE%\Cisco\Cisco Secure Client\VPN\Script
Linux (On Linux, assign execute permissions to the file for User, Group and Other.)	/opt/cisco/secureclient/vpn/script

OS	Directory
macOS	/opt/cisco/secureclient/vpn/script

Configure the Cisco Secure Client Profile for Scripting

Procedure

Step 1 Open the VPN Profile Editor and choose **Preferences (Part 2)** from the navigation pane.

Step 2 Check **Enable Scripting**. The client launches scripts on connecting or disconnecting the VPN connection.

Step 3 Check **User Controllable** to let users enable or disable the running of On Connect and OnDisconnect scripts.

Step 4 Check **Terminate Script On Next Event** to enable the client to terminate a running script process if a transition to another scriptable event occurs. For example, the client terminates a running On Connect script if the VPN session ends and terminates a running OnDisconnect script if Cisco Secure Client starts a new VPN session. On Microsoft Windows, the client also terminates any scripts that the On Connect or OnDisconnect script launched, and all their script descendents. On macOS and Linux, the client terminates only the On Connect or OnDisconnect script; it does not terminate child scripts.

Step 5 Check **Enable Post SBL On Connect Script** (enabled by default) to let the client launch the On Connect script (if present) if SBL establishes the VPN session.

Note Be sure to add the client profile to the Secure Firewall ASA group policy to download it to the VPN endpoint.

Troubleshoot Scripts

If a script fails to run, try resolving the problem as follows:

Procedure

Step 1 Make sure that the script has an `OnConnect` or `OnDisconnect` prefix name. Write, Test and Deploy Scripts shows the required scripts directory for each operating system.

Step 2 Try running the script from the command line. The client cannot run the script if it cannot run from the command line. If the script fails to run on the command line, make sure the application that runs the script is installed, and try rewriting the script on that operating system.

Step 3 Verify that there is only one OnConnect script and only one OnDisconnect script in the scripts directory on the VPN endpoint. If the client downloads an OnConnect script from the Secure Firewall ASA, then downloads a second OnConnect script with a different filename suffix for another Secure Firewall ASA, then the client might not run the script you intended to run. If the script path contains more than one OnConnect or OnDisconnect script, and you are using the Secure

Firewall ASA to deploy scripts, then remove the contents of the scripts directory and re-establish a VPN session. If the script path contains more than one OnConnect or OnDisconnect script, and you are using the manual deployment method, then remove the unwanted scripts and re-establish a VPN session.

Step 4 If the operating system is Linux, make sure that the script file permissions are set to execute.

Step 5 Make sure that the client profile has scripting enabled.

Write and Deploy Custom Applications with the Cisco Secure Client API

For Windows, Linux, and macOS computers, you can develop your own executable User Interface (UI) with the Cisco Secure Client API. Deploy your UI by replacing the Cisco Secure Client binary files.

The following table lists the filenames of the client executable files for the different operating systems.

Client OS	Client GUI File	Client CLI File
Windows	vpnui.exe	vpncli.exe
Linux	vpnui	vpn
macOS	Not supported by the Secure Firewall ASA deployment. However, you can deploy an executable for the macOS that replaces the client GUI using other means, such as Altiris Agent.	vpn

Your executable can call any resource files that you import to the Secure Firewall ASA, such as logo images. When you deploy your own executable, you can use any filenames for your resource files.

Restrictions

- You cannot deploy updated Cisco Secure Client software from the Secure Firewall ASA. If you place an updated version of the Cisco Secure Client package on the Secure Firewall ASA, the Cisco Secure Client downloads the update, which replaces your custom UI. You must manage distribution of your custom client and related Cisco Secure Client software. Even though ASDM allows you to upload binaries to replace Cisco Secure Client, this deployment function is not supported when using custom applications.
- If you deploy the Network Access Manager, use the Cisco Secure Client GUI.
- Start Before Login is not supported.

Use the Cisco Secure Client CLI Commands

The Cisco Secure Client provides a command line interface (CLI) for users who prefer to enter client commands instead of using the graphical user interface. The following sections describe how to launch the CLI command prompt and the commands available through the CLI:

• Launch the Client CLI Prompt, on page 69
• Use the Client CLI Commands, on page 69
• Prevent a Windows Popup Message When Secure Firewall ASA Terminates a Session, on page 71

Note In Windows and macOS, the same downloader is used for profile updates in both VPN UI or CLI connections. In Linux, the downloader for the VPN UI can display warnings and popups, such as the Untrusted Certificate warning we often see when connecting or when downloading a profile or other component. However, a second Linux downloader for the VPN CLI is not capable of displaying such popups and warnings, and you receive a connection failure message as expected behavior.

Launch the Client CLI Prompt

To launch the CLI command prompt:

- (Windows) Locate the file *vpncli.exe* in the Windows folder C:\Program Files (x86)\Cisco\Cisco Secure Client. Double click vpncli.exe.
- (Linux and macOS) Locate the file *vpn* in the folder /opt/cisco/secureclient/bin/. Execute the file *vpn*.

Use the Client CLI Commands

If you run the CLI in interactive mode, it provides its own prompt. You can also use the command line.

- connect *IP address or alias*—Client establishes a connection to a specific Secure Firewall ASA
- disconnect—Client closes a previously established connection
- stats—Displays statistics about an established connection
- quit—Exits the CLI interactive mode
- exit—Exits the CLI interactive mode

The following examples show the user establishing and terminating a connection from the command line:

Windows

```
connect 209.165.200.224
```

Establishes a connection to a security appliance with the address 209.165.200.224. After contacting the requested host, Cisco Secure Client displays the group to which the user belongs and asks for the user's username and password. If you have specified that an optional banner be displayed, the user must respond to the banner. The default response is n, which terminates the connection attempt. For example:

```
VPN > connect 209.165.200.224
>>contacting host (209.165.200.224) for login information...
>>Please enter your username and password.
Group: testgroup
Username: testuser
Password: ********
>>notice: Please respond to banner.
```

```
VPN>
STOP! Please read. Scheduled system maintenance will occur tonight from 1:00-2:00 AM for
one hour.
The system will not be available during that time.

accept? [y/n] y
>> notice: Authentication succeeded. Checking for updates...
>> state: Connecting
>> notice: Establishing connection to 209.165.200.224.
>> State: Connected
>> notice: VPN session established.
VPN>
```

stats

Displays statistics for the current connection; for example:

```
VPN > stats
[Tunnel information]

Time Connected: 01:17:33
Client Address: 192.168.23.45
Server Address: 209.165.200.224

[Tunnel Details]

Tunneling Mode: All traffic
Protocol: DTLS
Protocol Cipher: RSA_AES_256_SHA1
Protocol Compression: None

[Data Transfer]

Bytes (sent/received): 1950410/23861719
Packets (sent/received): 18346/28851
Bypassed (outbound/inbound): 0/0
Discarded (outbound/inbound): 0/0

[Secure Routes]

Network Subnet
0.0.0.0 0.0.0.0
VPN>
```

disconnect

Closes a previously established connection; for example:

```
VPN > disconnect
>> state: Disconnecting
>> state: Disconnected
>> notice: VPN session ended.
VPN>
```

quit or exit

Either command exits the CLI interactive mode; for example:

```
quit
goodbye
>>state: Disconnected
```

Linux or macOS

```
/opt/cisco/secureclient/bin/vpn connect 1.2.3.4
```

Establishes a connection to the Secure Firewall ASA with the address 1.2.3.4

```
/opt/cisco/secureclient/bin/vpn connect some_asa_alias
```

Establishes a connection to the Secure Firewall ASA by reading the profile and looking up the alias *some_asa_alias* in order to find its address

```
/opt/cisco/secureclient/bin/vpn stats
```

Displays statistics about the vpn connection

```
/opt/cisco/secureclient/bin/vpn disconnect
```

Disconnect the vpn session if it exists.

Prevent a Windows Popup Message When Secure Firewall ASA Terminates a Session

If you terminate the Cisco Secure Client session by issuing a session reset from the Secure Firewall ASA, the following Windows popup message displays to the end user:

```
The secure gateway has terminated the vpn connection. The following message was received
for the gateway: Administrator Reset
```

You may not want this message to appear (for example, when the VPN tunnel is initiated using the CLI command). You can prevent the message from appearing by restarting the client CLI after the client connects. The following example shows the CLI output when you do this:

```
C:\Program Files(x86)\Cisco\Cisco Secure Client>vpncli
Cisco Secure Client (version 5.x).
Copyright (c) 2022 Cisco Systems, Inc.
All Rights Reserved.
>> state: Connected
>> state: Connected
>> notice: Connected to asa.cisco.com.
>> notice: Connected to asa.cisco.com.
>> registered with local VPN subsystem.
>> state: Connected
>> notice: Connected to asa.cisco.com.
>> state: Disconnecting
>> notice: Disconnect in progress, please wait...
>> state: Disconnected
>> notice: On a trusted network.
>> error: The secure gateway has terminated the VPN connection.
The following message was received from the secure gateway: Administrator Reset
VPN>
```

Alternatively, in the Windows registry, you can create a 32-bit double value with the name SuppressModalDialogs on the endpoint device in the following locations. The client checks for the name but ignores its value:

- 64-bit Windows:

  HKEY_LOCAL_MACHINE/SOFTWARE\Wow6432Node\Cisco\ Cisco Secure Client

- 32-bit Windows:

  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco Secure Client

Prepare Cisco Secure Client Customizations and Localizations for ISE Deployment

Prepare Cisco Secure Client Localization Bundle

The Cisco Secure Client Localization Bundle is a zip file containing translation table files and installer transform files used to localize Cisco Secure Client. This zip file is part of an ISE Cisco Secure Client resource that is used to deploy Cisco Secure Client from your ISE to your users. The contents of this zip file are defined by the languages you support in your Cisco Secure Client deployment as described in this procedure.

Before you begin

The ISE requires compiled, binary translation tables in its Cisco Secure Client localization bundle. In gettext there are two file formats: a text .po format used for editing and a compiled, binary .mo format used at runtime. Compiling is done with the gettext tool msgfmt. Download the Gettext utilities from http://www.gnu.org/software/gettext/ and install Gettext on a local computer you use for administration (not a remote user computer).

Procedure

Step 1 Obtain and prepare the translation table files used by your Cisco Secure Client deployment.

a) From the Cisco Secure Client Software Download page on www.cisco.com, download and open the `AnyConnect-translations-`*`(date)`*`.zip` file.

This zip file contains *.po files for all language translations provided by Cisco.

b) (Optional) Locate any other translation table files (*.po files) that you have customized or created for your own environment.

c) Run the gettext message file compiler to create a *.mo file from each *.po file you are using:

```
msgfmt -o AnyConnect.mo AnyConnect.po
```

Step 2 Assemble the translation table files used by your Cisco Secure Client deployment.

a) Create a directory named `l10n` in a working area on your local computer.

b) Create a directory under `l10n` for each language you want to include whose name is the language code.

For example `fr-ch` for French (Canadian).

c) Put each compiled translation table file that you want to include into the appropriately named directory.

Do NOT put any *.po files in the compiled translation table. Only *.mo files should go into this file.

Your directory structure will be similar to the following which includes translation tables for French (Canadian), Hebrew, and Japanese:

```
l10n\fr-ch\AnyConnect.mo
    \he\AnyConnect.mo
    \ja\AnyConnect.mo
```

Step 3 (Windows only) Obtain and prepare the language localization transform files used by your Cisco Secure Client deployment.

a) From the Cisco Secure Client Software Download page on www.cisco.com, download and open the zip file containing the language localization transform files, which apply translations to the installer screens.

The zip file is named `secureclient-win-(version)-webdeploy-k9-lang.zip`.

Note
The version of the language localization files must match the version of Cisco Secure Client used in your environment. When upgrading to a new version of Cisco Secure Client, you must also upgrade the language localization files used in the localization bundle to the same version.

b) Locate any language localization transform files that you have customized or created for your own environment.

Step 4 (Windows only) Assemble the language localization files used by your Cisco Secure Client deployment.

a) Create a directory named `mst` in the same working area on your local computer.
b) Create a directory under `mst` for each language you want to include whose name is the language code.

For example `fr-ch` for French (Canadian).

c) Put each language localization file that you want to include into the appropriately named directory.

Your directory structure will now be similar to the following:

```
l10n\fr-ch\AnyConnect.mo
    \he\AnyConnect.mo
    \ja\AnyConnect.mo
mst\fr-ch\AnyConnect_fr-ca.mst
   \he\AnyConnect_he.mst
   \ja\AnyConnect_ja.mst
```

Step 5 Zip up this directory structure using a standard compression utility into an appropriately named file, such as `SecureClient-Localization-Bundle-(release).zip`, to create your Cisco Secure Client Localization Bundle.

What to do next

Upload the Cisco Secure Client Localization Bundle onto ISE. This ISE resource is used to deploy Cisco Secure Client to your users.

Prepare Your Cisco Secure Client Customization Bundle

The Cisco Secure Client Customization Bundle is a zip file containing custom Cisco Secure Client GUI resources, a custom help file, VPN scripts, and installer transforms. This zip file is part of an ISE Cisco Secure Client resource that is used to deploy Cisco Secure Client from your ISE to your users. It has the following directory structure:

```
win\resource\
   \binary
   \transform
mac-intel\resource
         \binary
         \transform
```

Customized Cisco Secure Client components are included in the `resource`, `binary` and `transform` sub-directories for Windows and macOS platforms as follows:

- Each `resource` sub-directory contains all the custom Cisco Secure Client GUI components for that platform.

To create these resources see Create Custom Icons and Logos for the Cisco Secure Client GUI, on page 57.

- Each `binary` sub-directory contains the custom help file and VPN scripts for that platform.
  - To create the Cisco Secure Client help file, see Create and Upload the Cisco Secure Client Help File, on page 63.
  - To create VPN scripts, see Write and Deploy Scripts, on page 64.
- Each `transform` sub-directory contains the installer transforms for that platform.
  - To create Windows Customized Installer Transforms, see Modify Installation Behavior, Windows, on page 42.
  - To create macOS Installer Transforms, see Customize Installer Behavior on macOS with ACTransforms.xml, on page 47 .

Before you begin

Create all the necessary custom components before preparing the Cisco Secure Client Customization Bundle.

Procedure

Step 1 Create the described directory structure in a working area of your local computer.

Step 2 Populate the `resources` directories with your custom Cisco Secure Client GUI files for each platform. Verify files are all named appropriately and icons and logos are sized appropriately.

Step 3 Populate the `binary` directories with your custom `help_AnyConnect.html` file.

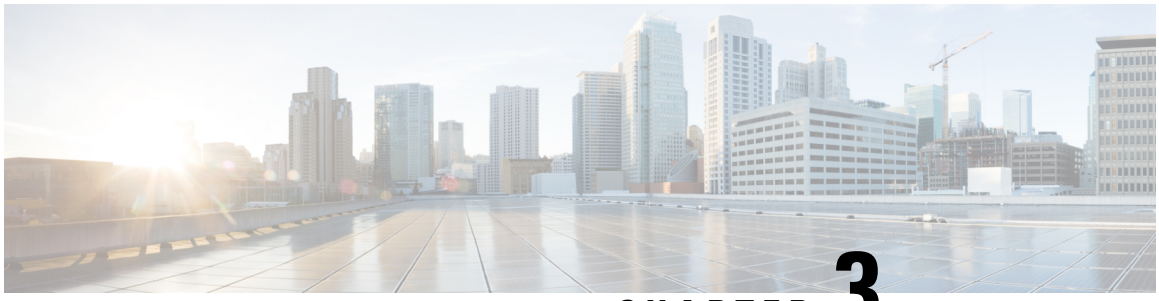
Step 4 Populate the `binary` directories with your VPN `OnConnect` and `OnDisconnect` scripts, and any additional scripts they call.

Step 5 Populate the `transform` directories with your platform specific installer transforms.

Step 6 Zip up this directory structure using a standard compression utility into an appropriately named file, such as cisco-secure-client-*version*-core-vpn-lang-webdeploy-k9.zip , to create your Cisco Secure Client Customization Bundle.

What to do next

Upload the Cisco Secure Client Customization Bundle onto ISE. This ISE resource is used to deploy Cisco Secure Client to your users.



CHAPTER 3

The Cisco Secure Client Profile Editor

- About the Profile Editor, on page 75
- The Cisco Secure Client VPN Profile, on page 76
- The Cisco Secure Client Local Policy, on page 99

About the Profile Editor

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

If you load multiple Cisco Secure Client packages, ASDM activates the client profile editor from the newest Cisco Secure Client package. This approach ensures that the editor displays the features for the newest Cisco Secure Client 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 Cisco Secure Client, and they make the preconfigured network profiles available to end users. Use the profile editor to create and configure one or more profiles. Cisco Secure Client 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:

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 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 Cisco Secure Client group policy from the drop-down list.

Step 8 Click **OK**.

The Cisco Secure Client VPN Profile

Cisco Secure Client features are enabled in the Cisco Secure Client 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, Cisco Secure Endpoint, and customer experience feedback). The Secure Firewall ASA deploys the profiles during Cisco Secure Client installation and updates. Users cannot manage or modify profiles.

You can configure the Secure Firewall ASA or ISE to deploy profiles globally for all Cisco Secure Client users or to users based on their group policy. Usually, a user has a single profile for each Cisco Secure Client 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 Cisco Secure 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.

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 AutoConnect On Start is enabled before login.

Cisco Secure Client 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, Cisco Secure Client 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 Cisco Secure Client message catalog and is localized.
- **Client Certificate Store**—Controls which certificate store(s) Cisco Secure Client 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 Cisco Secure Client, you can configure the certificate store from Windows, macOS, or Linux drop-down. The profile preferences support the values below:

- **Windows**



Note Enumeration of client certificates may take longer if certificate revocation checks cannot be performed from the network where the VPN connection is initiated.

  - 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 Cisco Secure Client 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 Cisco Secure Client 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**—Cisco Secure Client searches for certificates in the Windows machine certificate store. Client Certificate Store (Windows) must set to *All* or *Machine*.
  - **False**—[Default] Cisco Secure Client 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**—Cisco Secure Client, when started, automatically establishes a VPN connection with the secure gateway specified by the Cisco Secure Client profile, or to the last gateway to which the client connected.
- **Minimize On Connect**—After establishing a VPN connection, the Cisco Secure Client 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 Cisco Secure 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).

- **Disable Captive Portal Detection**—When Cisco Secure Client 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 Cisco Secure Client UI.
- **Auto Reconnect**—Cisco Secure Client 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—Cisco Secure Client releases the resources assigned to the VPN session upon a system suspend and does not attempt to reconnect after the system resumes.
    - ReconnectAfterResume (Default)—Cisco Secure Client 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, Cisco Secure Client 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. Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client.
  - 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. Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client, Cisco Secure Client needs to decide which IP protocol to use to initiate the connection. By default Cisco Secure Client initially attempts to connect using IPv4. If that is not successful, Cisco Secure Client 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.

Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client, 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, Cisco Secure Client 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)—Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client 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—Cisco Secure Client 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, Cisco Secure Client 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**—Cisco Secure Client 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.

- **Always On**—Determines whether Cisco Secure Client 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 Cisco Secure Client 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.

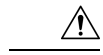
  - **Allow VPN Disconnect**—Determines whether Cisco Secure Client displays a Disconnect button for Always-On VPN sessions. Users of Always-On VPN sessions may want to click Disconnect so they can choose an alternative secure gateway for reasons such as performance issues with the current VPN session 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 Cisco Secure Client 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 Cisco Secure Client 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. Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client GUI. If you make this feature user controllable, users can read and change the PPP exclusion settings.

- Automatic—Enables PPP exclusion. Cisco Secure Client 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, Cisco Secure Client 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.

Cisco Secure Client 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 Cisco Secure Client Profile Editor, Add/Edit a Server List, on page 91. 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.

Cisco Secure Client 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, Cisco Secure Client 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. When you add multiple Distinguished Names, each certificate is checked against all entries, and all of them must match.
  - **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.

Cisco Secure Client Profile Editor, Certificate Enrollment

Certificate Enrollment enables Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client 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.

Cisco Secure Client 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.

Cisco Secure Client 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 Cisco Secure Client Profile Editor, Certificate Pin, on page 90.



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.

Cisco Secure Client 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 Cisco Secure 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 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 Cisco Secure Client Profile Editor, Backup Servers, on page 85 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 Cisco Secure Client 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 Cisco Secure Client Profile Editor, Certificate Pin, on page 90.
- **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.

Cisco Secure Client 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**—Cisco Secure Client automatically chooses the client certificate with which to authenticate when making a connection. In this case, Cisco Secure Client 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**—Cisco Secure Client searches for a certificate from the Cisco Secure Client certificate store on the Android device when the profile is downloaded and does one of the following:
  - If Cisco Secure Client 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 Cisco Secure Client certificate store for any reason, Cisco Secure Client 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 Cisco Secure Cloud Analytics 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 Cisco Secure Cloud Analytics applications, refer to the Cisco Secure Cloud Analytics 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: Cisco Secure Client Profile Editor, Preferences (Part 2), on page 81.

- **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.

- **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 Cisco Secure Client release is opened in a later Cisco Secure Client 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.
- **Acceptable Use Policy** (Optional and mobile specific)—Click **Edit** to define an Acceptable Use Policy for mobile devices in the dialog box. Once complete, click **OK**. A maximum of 4000 characters is allowed.

  This message is shown to the user once after Network Visibility Module is configured. The remote user does not have a choice to decline Network Visibility Module activities. The network administrator controls Network Visibility Module using MDM facilities.
- **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 Cisco Secure Client 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 Cisco Secure Client Local Policy

AnyConnectLocalPolicy.xml is a file that is installed automatically on the client with the AnyConnect VPN installer and contains some default security values. The local policy file is loaded as a result of multiple Secure Client processes (such as csc_ui.exe after installation, vpnagent.exe upon installation completion, vpncli.exe upon manual start, or vpndownloader.exe when a VPN is established). This file is not deployed by the Secure Firewall ASA. From Secure Client Cloud Management, you can deploy this AnyConnectLocalPolicy.xml file when Cisco Secure Client is installed from that UI. 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, Cisco Secure Client retrieves the updated CRL for all certificates in the chain. Cisco Secure Client 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. Cisco Secure Client 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 Cisco Secure Client cannot perform a CRL check when Always On is enabled. Also, if CRL distribution points are not publicly reachable, Cisco Secure Client 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 Cisco Secure Client cannot perform an OCSP check when Always On is enabled. Also, if the OCSP responder is not publicly reachable, Cisco Secure Client may encounter a service disruption.

- **Strict Certificate Trust**

  If selected, when authenticating remote security gateways, Cisco Secure Client 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 Cisco Secure 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 Cisco Secure 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 Server Cert Store** (Windows 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, Cisco Secure Client does not cache sensitive information to disk. Enabling this parameter extends this policy to any type of user information stored in the Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client software and profiles upon VPN connectivity. ServerName can be an FQDN, IP address, domain name, or wildcard with domain name.

- **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

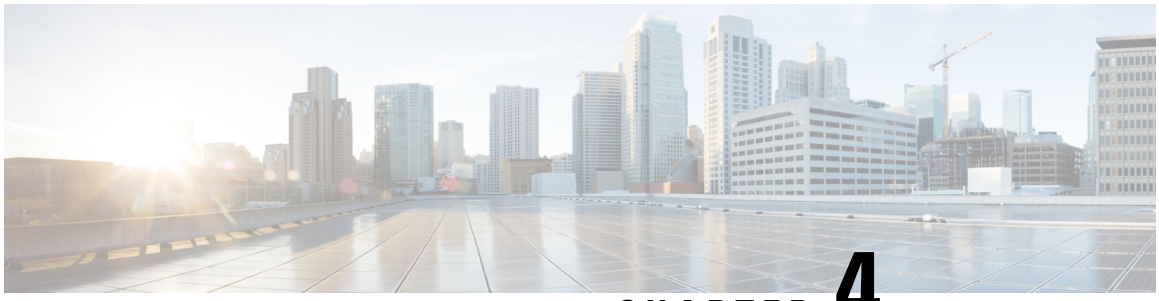
See Local Policy Parameters and Values for the descriptions and values that you can set.

Create an MST file to change local policy parameters. The MST parameter names correspond to the parameters in 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 Cisco Secure Client 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.



CHAPTER 4

Connect and Disconnect to a VPN

- AnyConnect VPN Connectivity Options, on page 105
- Configure VPN Connection Servers, on page 107
- Start Windows VPN Connections Before Login, on page 108
- Automatically Start VPN Connections When Cisco Secure Client Starts, on page 112
- Configure Start Before Login (PLAP) on Windows Systems, on page 112
- Use Trusted Network Detection to Connect and Disconnect, on page 113
- Require VPN Connections Using Always-On, on page 116
- Use Captive Portal Hotspot Detection and Remediation, on page 122
- Configure Cisco Secure Client over L2TP or PPTP, on page 125
- Use Management VPN Tunnel, on page 126
- Configure Cisco Secure Client Proxy Connections, on page 132
- Select and Exclude VPN Traffic, on page 137
- Manage VPN Authentication, on page 147

AnyConnect VPN Connectivity Options

Cisco Secure Client provides many options for automatically connecting, reconnecting, or disconnecting VPN sessions. These options provide a convenient way for your users to connect to your VPN, and they also support your network security requirements.

Starting and Restarting AnyConnect Connections

Configure VPN Connection Servers to provide the names and addresses of the secure gateways your users will manually connect to.

Choose from the following Cisco Secure Client capabilities to provide convenient, automatic VPN connectivity:

- Automatically Start Windows VPN Connections Before Login
- Automatically Start VPN Connections when AnyConnect Starts
- Automatically Restart VPN Connections

Also, consider using the following Automatic VPN Policy options to enforce greater network security or restrict network access to the VPN only:

- Use Trusted Network Detection to Connect and Disconnect

- Require VPN Connections Using Always On
- Use Captive Portal Hotspot Detection and Remediation

Renegotiating and Maintaining the Cisco Secure Client Connection

You can limit how long the Secure Firewall ASA keeps an AnyConnect VPN connection available to the user even with no activity. If a VPN session goes idle, you can terminate the connection or re-negotiate the connection.

- Keepalive—The Secure Firewall ASA sends keepalive messages at regular intervals. These messages are ignored by the Secure Firewall ASA, but are useful in maintaining connections with devices between the client and the Secure Firewall ASA.

  For instructions to configure Keepalive with the ASDM or CLI, see the *Enable Keepalive* section in the Cisco ASA Series VPN Configuration Guide.

- Dead Peer Detection—The Secure Firewall ASA and Cisco Secure Client send "R-U-There" messages. These messages are sent less frequently than IPsec's keepalive messages. You can enable both the Secure Firewall ASA (gateway) and Cisco Secure Client to send DPD messages, and configure a timeout interval.
  - If the client does not respond to the Secure Firewall ASA's DPD messages, the ASA tries once more before putting the session into "Waiting to Resume" mode. This mode allows the user to roam networks, or enter sleep mode and later recover the connection. If the user does not reconnect before the idle timeout occurs, the Secure Firewall ASA will terminate the tunnel. The recommended gateway DPD interval is 300 seconds.
  - If the Secure Firewall ASA does not respond to the client's DPD messages, the client tries again before terminating the tunnel. The recommended client DPD interval is 30 seconds.

    For instructions to configure DPD within the ASDM, refer to *Configure Dead Peer Detection* in the appropriate release of the Cisco ASA Series VPN ASDM Configuration Guide.

- Best Practices:
  - Set Client DPD to 30 seconds (Group Policy > Advanced > AnyConnect Client > Dead Peer Detection).
  - Set Server DPD to 300 seconds (Group Policy > Advanced > AnyConnect Client > Dead Peer Detection).
  - Set Rekey, for both SSL and IPsec to 1 hour (Group Policy > Advanced > AnyConnect Client > Key Regeneration).

Terminating an AnyConnect VPN Connection

Terminating an AnyConnect VPN connection requires users to re-authenticate their endpoint to the secure gateway and create a new VPN connection.

The following connection parameters terminate the VPN session based on timeouts:

- Maximum Connect Time—Sets the maximum user connection time in minutes. At the end of this time, the system terminates the connection. You can also allow unlimited connection time(default).
- VPN Idle Timeout—Terminates any user's session when the session is inactive for the specified time. If the VPN idle timeout is not configured, then the default idle timeout is used.

- Default Idle Timeout—Terminates any user's session when the session is inactive for the specified time. The default value is 30 minutes (or 1800 seconds).

See the *Specify a VPN Session Idle Timeout for a Group Policy* section in the appropriate release of the Cisco ASA Series VPN ASDM Configuration Guide to set these parameters.

Configure VPN Connection Servers

The Cisco Secure Client VPN server list consists of host name and host address pairs identifying the secure gateways that your VPN users will connect to. The host name can be an alias, an FQDN, or an IP address.

The hosts added to the server list display in the Connect to drop-down list in the Cisco Secure Client GUI. The user can then select from the drop-down list to initiate a VPN connection. The host at the top of the list is the default server, and appears first in the GUI drop-down list. If the user selects an alternate server from the list, the selected server becomes the new default server.

Once you add a server to the server list, you can view its details and edit or delete the server entry. To add a server to the server list, follow this procedure.

Procedure

Step 1 Open the VPN Profile Editor and choose **Server List** from the navigation pane.

Step 2 Click **Add**.

Step 3 Configure the server's host name and address:

a) Enter a **Host Display Name**, an alias used to refer to the host, an FQDN, or an IP address. Do not use "&" or "<" characters in the name. If you enter an FQDN or an IP address, you do not need to enter the **FQDN** or **IP Address** in the next step.

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.

b) (Optional) Enter the host's **FQDN** or **IP Address** if not entered in the Host Display Name.

c) (Optional) Specify a **User Group**.

Cisco Secure Client uses the FQDN or IP Address in conjunction with User Group to form the Group URL.

Step 4 Enter the server to fall back to as the backup server in the **Backup Server List**. Do not use "&" or "<" characters in the name.

Note
Conversely, the Backup Server tab on the Server menu is a global entry for all connection entries. Any entries put in that Backup Server location are overwritten with what is entered here for an individual server list entry. This setting takes precedence and is the recommended practice.

Step 5 (Optional) Add load balancing servers to the **Load Balancing Server List.** Do not use "&" or "<" characters in the name.

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

Step 6 Specify the **Primary Protocol** for the client to use for this Secure Firewall ASA:

a) Choose SSL (default) or IPsec.

If you specify 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.

b) If you specify IPsec, select **Standard Authentication Only** to disable the default authentication method (proprietary AnyConnect EAP), and choose a method from the drop-down list.

Note
Changing the authentication method from the proprietary Cisco Secure Client 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.

Step 7 (Optional) Configure SCEP for this server:

a) Specify the URL of the SCEP CA server. Enter an FQDN or IP Address. For example, http://ca01.cisco.com.
b) Check **Prompt For Challenge PW** to enable the user to make certificate requests manually. When the user clicks **Get Certificate**, the client prompts the user for a username and one-time password.
c) Enter the certificate thumbprint of the CA. Use SHA1 or MD5 hashes. 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 a certificate it issued.

Step 8 Click **OK**.

Start Windows VPN Connections Before Login

About Start Before Login

This feature called Start Before Login (SBL) allows users to establish their VPN connection to the enterprise infrastructure before logging onto Windows.



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

After SBL is installed and enabled, the Network Connection button launches Cisco Secure Client core VPN and Network Access Manager UI.

SBL also includes the Network Access Manager tile and allows connections using user configured home network profiles. Network profiles allowed in SBL mode include all media types employing non-802.1X authentication modes, such as open WEP, WPA/WPA2 Personal, and static key (WEP) networks.

SBL is available on Windows systems only, and is implemented using different mechanisms depending on the version of Windows:

- On Windows, the Pre-Login Access Provider (PLAP) is used to implement Cisco Secure Client SBL.

With PLAP, the Ctrl+Alt+Del key combination opens a window where the user can choose either to log in to the system or activate Network Connections (PLAP components) using the Network Connect button in the lower-right corner of the window.

PLAP supports 32-bit and 64-bit versions of the Windows.

Reasons you might consider enabling SBL for your users include:

- The user's computer is joined to an Active Directory infrastructure.
- A user has network-mapped drives that require authentication with the Microsoft Active Directory infrastructure.
- The user cannot have cached credentials on the computer (the group policy disallows cached credentials). In this scenario, users must be able to communicate with a domain controller on the corporate network for their credentials to be validated before gaining access to the computer.
- The user must run logon scripts that execute from a network resource or need access to a network resource. With SBL enabled, the user has access to the local infrastructure and logon scripts that would normally run when a user is in the office. This includes domain logon scripts, group policy objects and other Active Directory functionality that normally occurs when users log on to their system.
- Networking components (such as MS NAP/CS NAC) exist that might require connection to the infrastructure.

Limitations of Start Before Login

- Cisco Secure Client is not compatible with fast user switching.
- You cannot use Start Before Login with Captive Portal Detection.
- Cisco Secure Client cannot be started by third-party Start Before Login applications.
- In release 5.1.13.xxx, the Start Before Login preference in the profile editor was removed. If you have existing profiles that use this preference, they will still be treated as valid profiles. If you used this preference in a profile to disable Start Before Logon prior to 5.1.13.xxx, this change will impact you.

Install the Cisco Secure Client Start Before Login Module

The Cisco Secure Client installer detects the underlying operating system and places the appropriate Cisco Secure Client DLL from the Cisco Secure Client SBL module in the system directory. On Windows devices, the installer determines whether the 32-bit or 64-bit version of the operating system is in use and installs the appropriate PLAP component, vpnplap.dll or vpnplap64.dll.



Note If you uninstall Cisco Secure Client while leaving the SBL module installed, the SBL module is disabled and not visible to the remote user.

You can predeploy the SBL module or configure the ASA to download it. When predeploying Cisco Secure Client, the Start Before Login module requires that the core client software is installed first. If predeploying AnyConnect VPN and Start Before Login components using MSI files, the order must be correct.

Procedure

Step 1 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.
Step 2 Select a group policy and click **Edit** or **Add** a new group policy.
Step 3 Select **Advanced** > **AnyConnect Client** in the left navigation pane.
Step 4 Uncheck **Inherit** for the Optional Client Module for Download setting.
Step 5 Select the **AnyConnect SBL** module in the drop-down list.

Configure Start Before Login

Procedure

Step 1 Install the AnyConnect Start Before Logon Module.
Step 2 Enable SBL in the AnyConnect Profile.

Install the Cisco Secure Client Start Before Login Module

The Cisco Secure Client installer detects the underlying operating system and places the appropriate Cisco Secure Client DLL from the Cisco Secure Client SBL module in the system directory. On Windows devices, the installer determines whether the 32-bit or 64-bit version of the operating system is in use and installs the appropriate PLAP component, vpnplap.dll or vpnplap64.dll.



Note If you uninstall Cisco Secure Client while leaving the SBL module installed, the SBL module is disabled and not visible to the remote user.

You can predeploy the SBL module or configure the ASA to download it. When predeploying Cisco Secure Client, the Start Before Login module requires that the core client software is installed first. If predeploying AnyConnect VPN and Start Before Login components using MSI files, the order must be correct.

Procedure

Step 1 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.
Step 2 Select a group policy and click **Edit** or **Add** a new group policy.
Step 3 Select **Advanced** > **AnyConnect Client** in the left navigation pane.
Step 4 Uncheck **Inherit** for the Optional Client Module for Download setting.
Step 5 Select the **AnyConnect SBL** module in the drop-down list.

Enable SBL in the Cisco Secure Client VPN Profile

Before you begin

- SBL requires a network connection to be present at the time it is invoked. In some cases, this might not be possible, because a wireless connection might depend on credentials of the user to connect to the wireless infrastructure. Since SBL mode precedes the credential phase of a logon, a connection would not be available in this scenario. In this case, the wireless connection needs to be configured to cache the credentials across logon, or another wireless authentication needs to be configured, for SBL to work.
- If the Network Access Manager is installed, you must deploy device connection to ensure that an appropriate connection is available.

Procedure

Step 1 Open the VPN Profile Editor and choose **Preferences (Part 1)** from the navigation pane.

Step 2 Select **Use Start Before Login**.

Step 3 (Optional) To give the remote user control over SBL, select **User Controllable**.

Note
The user must reboot the remote computer before SBL takes effect.

Troubleshoot Start Before Login

Procedure

Step 1 Ensure that the Cisco Secure Client VPN profile is loaded on the Secure Firewall ASA, ready to be deployed.

Step 2 Delete prior profiles. The profile locations are provided in this table.

Step 3 Using Windows Add/Remove Programs, reinstall the SBL Components. Reboot the computer and retest.

Step 4 Clear the user's Cisco Secure Client log in the Event Viewer and retest.

Step 5 Browse back to the security appliance to install Cisco Secure Client again.

Step 6 Reboot once. On the next reboot, you should be prompted with the Start Before Login prompt.

Step 7 Collect a DART bundle and send it to your Cisco Secure Client administrator.

Step 8 If you see the following error, delete the user's Cisco Secure Client VPN profile:

```
Description: Unable to parse the profile C:\Documents and Settings\All Users\Application Data
\Cisco\Cisco Secure Client\Profile\VABaseProfile.xml. Host data not available.
```

Step 9 Go back to the .tmpl file, save a copy as an.xml file, and use that XML file as the default profile.

Automatically Start VPN Connections When Cisco Secure Client Starts

This feature called Auto Connect On Start, automatically establishes a VPN connection with the secure gateway specified by the VPN client profile when Cisco Secure Client starts.

Auto Connect On Start is disabled by default, requiring the user to specify or select a secure gateway.

Procedure

Step 1 Open the VPN Profile Editor and choose **Preferences (Part 2)** from the navigation pane.

Step 2 Select **Auto Connect On Start**.

Step 3 (Optional) To give the user control over Auto Connect on Start, select **User Controllable**.

Configure Start Before Login (PLAP) on Windows Systems

The Start Before Login (SBL) feature starts a VPN connection before the user logs in to Windows. This ensures that users connect to their corporate infrastructure before logging on to their computers. Windows only supports one PLAP being installed at the a time.

The SBL Cisco Secure Client feature is known as the Pre-Login Access Provider (PLAP), which is a connectable credential provider. This feature lets programmatic network administrators perform specific tasks, such as collecting credentials or connecting to network resources before logon. PLAP provides SBL functions on all of the supported Windows operating systems. PLAP supports 32-bit and 64-bit versions of the operating system with vpnplap.dll and vpnplap64.dll, respectively. The PLAP functions supports x86 and x64.

Automatically Restart VPN Connections

When Auto Reconnect is enabled (default), Cisco Secure Client recovers from VPN session disruptions and reestablishes a session, regardless of the media used for the initial connection. For example, it can reestablish a session on wired, wireless, or 3G/4G/5G. When Auto Reconnect is enabled, you also specify the reconnect behavior upon system suspend or system resume. A system suspend is a low-power standby, such as Windows “hibernation” or macOS or Linux “sleep.” A system resume is a recovery following a system suspend.

If you disable Auto Reconnect, the client does not attempt to reconnect regardless of the cause of the disconnection. Cisco highly recommends using the default setting (enabled) for this feature. Disabling this setting can cause interruptions in VPN connectivity over unstable connections.

Procedure

Step 1 Open the VPN Profile Editor and choose **Preferences (Part 2)** from the navigation pane.

Step 2 Select **Auto Reconnect**.

Step 3 Choose the Auto Reconnect Behavior:

- Disconnect On Suspend—(Default) Cisco Secure Client releases the resources assigned to the VPN session upon a system suspend and does not attempt to reconnect after the system resume.
- Reconnect After Resume—The client retains resources assigned to the VPN session during a system suspend and attempts to reconnect after the system resume.

Use Trusted Network Detection to Connect and Disconnect

About Trusted Network Detection

Trusted Network Detection (TND) gives you the ability to have Cisco Secure Client automatically disconnect a VPN connection when the user is inside the corporate network (the trusted network) and start the VPN connection when the user is outside the corporate network (the untrusted network).

TND does not interfere with the ability of the user to manually establish a VPN connection. It does not disconnect a VPN connection that the user starts manually in the trusted network. TND only disconnects the VPN session if the user first connects in an untrusted network and moves into a trusted network. For example, TND disconnects the VPN session if the user makes a VPN connection at home and then moves into the corporate office.

Note To configure the TND feature for the Network Visibility Module, see the Network Visibility Module Profile Editor, on page 95 in the *Network Visibility Module* chapter.

You configure TND in the Cisco Secure ClientVPN profile. No changes are required to the Secure Firewall ASA configuration. You need to specify the action or policy Cisco Secure Client takes when recognizing it is transitioning between trusted and untrusted networks, and identify your trusted networks and servers.

Note Whenever the TND policy evaluation occurs with the VPN tunnel connected and the policy specifies name-based trusted servers, that name resolution is performed over the VPN tunnel using the DNS servers pushed by the VPN headend.

Guidelines for Trusted Network Detection

- Because the TND feature controls the Cisco Secure Client GUI and automatically starts connections, the GUI should run at all times. If the user exits the GUI, TND does not automatically start the VPN connection.
- If Cisco Secure Client - AnyConnect VPN is also running Start Before Login (SBL), and the user moves into the trusted network, the SBL window displayed on the computer automatically closes.

- Trusted Network Detection with or without Always-On configured is supported on IPv6 and IPv4 VPN connections to the Secure Firewall ASA over IPv4 and IPv6 networks.
- TND policies take into effect only on a pre-existing VPN tunnel state. TND will not be triggered when a network or interface change occurs during an ongoing Cisco Secure Client connection/reconnection attempt (for example, in a dual-home scenario where an interface change occurs while Cisco Secure Client is already attempting a connection/reconnection). If there are multiple interfaces (one trusted and other untrusted), it depends upon the operating system as to which interface is chosen for the network activity for Cisco Secure Client.
- Multiple profiles on a user computer may present problems if the TND configuration is different. In a dual-home scenario, you should have at least one interface which satisfies all the TND conditions to deem the endpoint as trusted.

  If the user has received a TND-enabled profile in the past, upon system restart, Cisco Secure Client attempts to connect to the security appliance it was last connected to, which may not be the behavior you desire. To connect to a different security appliance, they must manually disconnect and re-connect to that headend. The following workarounds will help you prevent this problem:

  - Enable TND in the client profiles loaded on all the Secure Firewall ASAs on your corporate network.
  - Create one profile listing all the Secure Firewall ASAs in the host entry section, and load that profile on all your Secure Firewall ASAs.
  - If users do not need to have multiple, different profiles, use the same profile name for the profiles on all the Secure Firewall ASAs. Each Secure Firewall ASA overrides the existing profile.

- To use TND on Linux, you must have the Network Manager installed and running properly on the target (RHEL/Ubuntu) device, and the network manager must be maintaining the network interfaces.
- The function between each main criteria such as DNS domains and DNS servers would be an *AND* function. However, the function within the criteria would be an *OR* function. When DNS domains and DNS servers are specified, the client device needs to match one criteria from each section. However, if more than 10 DNS servers are specified, the client only needs to have one of those on the client's interface, and cannot contain any that do not match the 10.
  - DNS Servers—The client device must not have a DNS server that does not match the ones listed, but the client device does not need ALL servers listed here.
  - DNS Domains—The client device must not have a DNS domain that does not match the ones listed, but the client device does not need ALL domains listed here.
  - Trusted Servers—At least one server specified needs to be reachable and have a trusted hash.

Configure Trusted Network Detection

Procedure

Step 1 Open the VPN profile editor and choose **Preferences (Part 2)** from the navigation pane.

Step 2 Select **Automatic VPN Policy**.

Step 3 Choose a **Trusted Network Policy.**

This is the action the client takes when the user is inside the corporate network (the trusted network). The options are:

- Disconnect—(Default) The client terminates the VPN connection in the trusted network.
- Connect—The client starts a VPN connection in the trusted network.
- Do Nothing—The client takes no action in the trusted network. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection (TND).
- Pause—Cisco Secure Client suspends its AnyConnect 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 VPN 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.

Step 4 Choose an **Untrusted Network Policy**.

This is the action the client takes when the user is outside the corporate network. The options are:

- Connect—The client starts a VPN connection upon the detection of an untrusted network.
- Do Nothing—The client takes no action upon detection of an untrusted network. This option disablesAlways-On VPN. Setting both the Trusted Network Policy and Untrusted Network Policy to **Do Nothing** disables Trusted Network Detection.

Step 5 Specify **Trusted DNS Domains**.

Specify the DNS suffixes (comma-separated strings) that a network interface may have when the client is in the trusted network. Wildcarded entries are supported, as follows:

To Match This DNS Suffix:	Use This Value for TrustedDNSDomains:
example.com (only)	*example.com
example.com AND vpn.example.com	*.example.com OR example.com, vpn.example.com
asa.example.com AND vpn.example.com	*.example.com OR asa.example.com, vpn.example.com

Step 6 Specify **Trusted DNS Servers**.

All DNS server addresses (a string separated by commas) that a network interface may have when the client is in the trusted network. For example: 203.0.113.1,2001:DB8::1. Wildcards (*) are supported for IPv4 and IPv6 DNS server addresses.

Note
You can configure either TrustedDNSDomains, TrustedDNSServers, or both. If you configure TrustedDNSServers, be sure to enter all your DNS servers, so your site(s) will all be part of the Trusted Network.

An active interface will be considered as an In-Trusted-Network if it matches *all* the rules in the VPN profile.

Step 7 Specify a host URL that you want to add as trusted. You must have a secure web server that is accessible with a trusted certificate to be considered 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**.

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.

Require VPN Connections Using Always-On

About Always-On VPN

Always-On operation prevents access to Internet resources when the computer is not on a trusted network, unless a VPN session is active. Enforcing the VPN to always be on in this situation protects the computer from security threats.

When Always-On is enabled, it establishes a VPN session automatically after the user logs in and upon detection of an untrusted network. The VPN session remains open until the user logs out of the computer, or the session timer or idle session timer (specified in the Secure Firewall ASA group policy) expires. Cisco Secure Client continually attempts to reestablish the connection to reactivate the session if it is still open; otherwise, it continually attempts to establish a new VPN session.

When Always-On is enabled in the VPN Profile, Cisco Secure Client protects the endpoint by deleting all the other downloaded Cisco Secure Client profiles and ignores any public proxies configured to connect to the Secure Firewall ASA.

The following Cisco Secure Client options also need to be considered when enabling Always-On:

Limitations of Always-On VPN

- Always On is available only on Windows and macOS
- If Always-On is enabled, but the user does not log on, AnyConnect VPN does not establish the VPN connection. AnyConnect VPN starts the VPN connection only post-login.
- Always-On VPN does not support connecting though a proxy.

Guidelines for Always-On VPN

To enhance protection against threats, we recommend the following additional protective measures if you configure Always-On VPN:

- We strongly recommend purchasing a digital certificate from a certificate authority (CA) and enrolling it on the secure gateways. The ASDM provides an **Enroll ASA SSL VPN with Entrust** button on the **Configuration > Remote Access VPN > Certificate Management > Identity Certificates** panel to facilitate enrollment of a public certificate.
- Predeploy a profile configured with Always-On to the endpoints to limit connectivity to the pre-defined Secure Firewall ASAs. Predeployment prevents contact with a rogue server.
- Restrict administrator rights so that users cannot terminate processes. A PC user with admin rights can bypass an Always-On policy by stopping the agent. If you want to ensure fully-secure Always-On, you must deny local admin rights to users.

- Restrict access to the Cisco sub-folders on Windows computers, typically `C:\ProgramData`.
- Users with limited or standard privileges may sometimes have write access to their program data folders. They could use this access to delete the Cisco Secure Client profile and thereby circumvent the Always-On feature.
- Predeploy a group policy object (GPO) for Windows users to prevent users with limited rights from terminating the GUI. Predeploy equivalent measures for macOS users.

Configure Always-On VPN

Procedure

Step 1 Configure Always-On in the VPN Profile, on page 117.

Step 2 (Optional) Add Load-Balancing Backup Cluster Members to the Server List.

Step 3 (Optional) Exempt Users from Always-On VPN.

Configure Always-On in the VPN Profile

Before you begin

Always-On VPN requires that a valid, trusted server certificate be configured on the Secure Firewall ASA; otherwise, it fails and logs an event indicating the certificate is invalid. In addition, ensuring that the server certificate can pass Strict Certificate Trust mode prevents the download of an Always-On VPN profile that locks a VPN connection to a rogue server.

Procedure

Step 1 Open the VPN Profile Editor and choose **Preferences (Part 2)** from the navigation pane.

Step 2 Select **Automatic VPN Policy**.

Step 3 Configure Trusted Network Detection, on page 114.

Step 4 Select **Always On**.

Step 5 (Optional) Select or un-select **Allow VPN Disconnect**.

Step 6 (Optional) Define the hosts that endpoints can access while VPN is disconnected during Always On. If SAML authentication is used, refer to Use Always-On VPN With External SAML Identity Provider, on page 117.

Step 7 (Optional) Configure a Connect Failure Policy.

Step 8 (Optional) Configure Captive Portal Remediation.

Use Always-On VPN With External SAML Identity Provider

To support SAML authentication with Always On enabled, follow these steps, which impact the *Allow Access to the Following Hosts With VPN Disconnected* parameter configuration.

Procedure

Step 1 Disable the Always On parameter in the Cisco Secure Client Profile Editor, Preferences (Part 2), on page 81.

Step 2 After the resulting profile is deployed, perform SAML authentication while capturing all DNS flows, as well as all TCP flows generated by the browser (either embedded or the default), used by Cisco Secure Client during SAML authentication.

Windows

- Use the Microsoft tool ProcMon to capture the browser TCP flows.
- Before starting the ProcMon trace, if the Cisco Secure Client browser is used, add process name filter acwebhelper.exe. If the default browser is used, add the process name filter matching the default browser's executable.
- Capture DNS traffic and TCP flow traffic with Wireshark using display filter **udp.port==53 || (tcp.flags.syn == 1 && tcp.flags.ack ==0)**.

macOS

- Use the native tool tcpmon to capture relevant network traffic with process name metadata: **sudo tcpdump -n -k NP > /tmp/capture.txt**
- For packets originating from the Cisco Secure Client embedded browser, the process name field shows up as *(proc com .apple.WebKit:PID1, eproc Cisco AnyConnect:PID2)*.

Step 3 Identify all TCP connections originating from the browser that are used by Cisco Secure Client for SAML authentication, as well as the DNS response packets preceding such TCP connections and containing the TCP connection's destination IP address.

Step 4 Extract FQDNs from the query name field of the previously identified DNS response packets and add them to the Always On **Allow Access to the Following Hosts With VPN Disconnected** parameter in the Cisco Secure Client Profile Editor, Preferences (Part 2).

Step 5 Also, to the same Always On preference parameter, add all IP addresses corresponding to browser connections that aren't preceded by corresponding DNS traffic (such as, connections by IP address).

Step 6 Re-enable the Always On profile preference.

Add Load-Balancing Backup Cluster Members to the Server List

Always-On VPN affects the load balancing of AnyConnect VPN sessions. With Always-On VPN disabled, when the client connects to a primary device within a load balancing cluster, the client complies with a redirection from the primary device to any of the backup cluster members. With Always-On enabled, the client does not comply with a redirection from the primary device unless the address of the backup cluster member is specified in the server list of the client profile. Therefore, be sure to add any backup cluster members to the server list.

To specify the addresses of backup cluster members in the client profile, use ASDM to add a load-balancing backup server list by following these steps:

Procedure

Step 1 Open the VPN Profile Editor and choose **Server List** from the navigation pane.

Step 2 Choose a server that is a primary device of a load-balancing cluster and click **Edit**.

Step 3 Enter an FQDN or IP address of any load-balancing cluster member.

Exempt Users from Always-On VPN

You can configure exemptions to override an Always-On policy. For example, you might want to let certain individuals establish VPN sessions with other companies or exempt the Always-On policy for noncorporate assets.

Exemptions set in group policies and dynamic access policies on the Secure Firewall ASA override the Always-On policy. You specify exceptions according to the matching criteria used to assign the policy. If the Cisco Secure Client VPN 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.

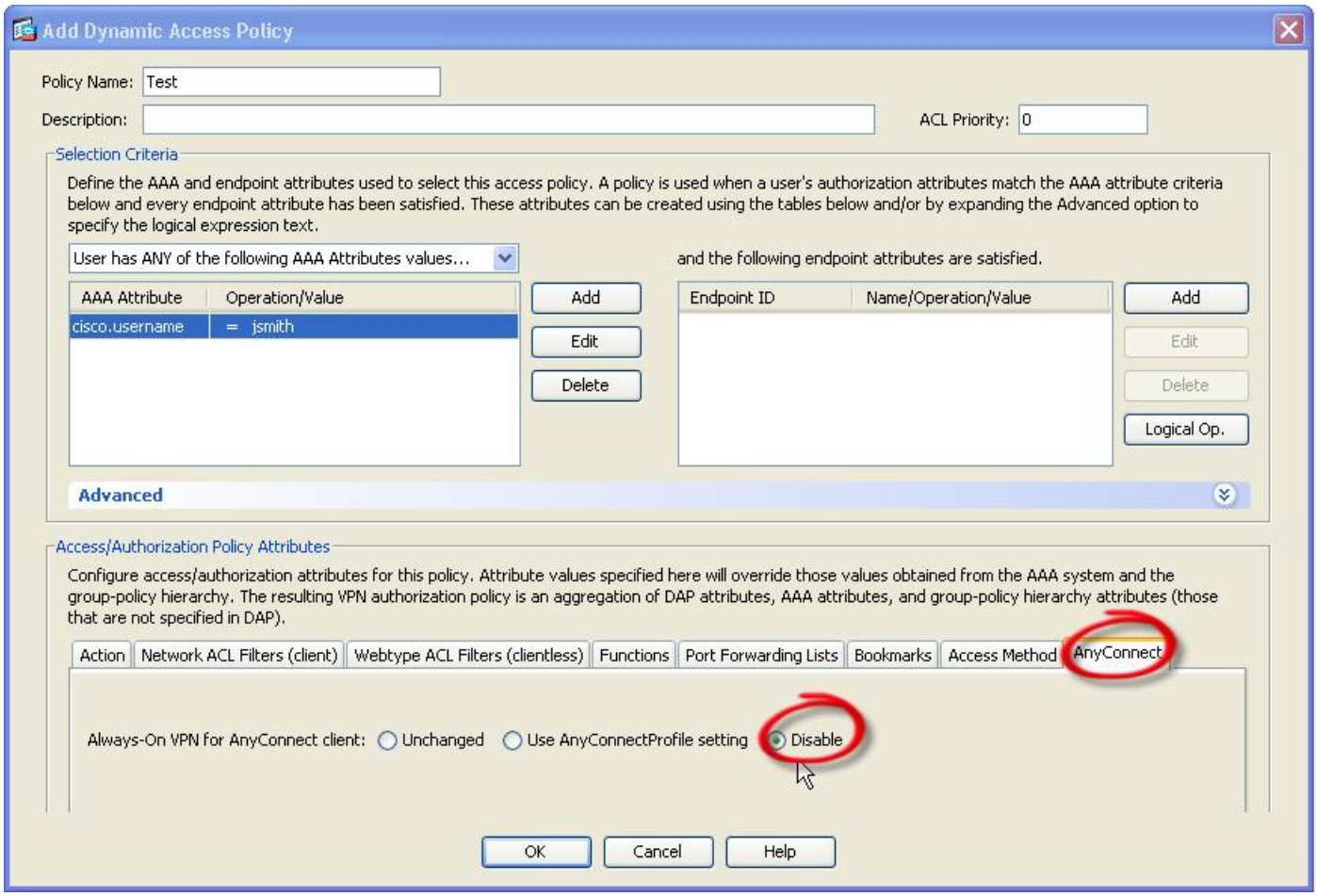
This procedure configures a dynamic access policy that uses AAA endpoint criteria to match sessions to noncorporate assets.

Procedure

Step 1 Choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies** > **Add** or **Edit**.

Step 2 Configure criteria to exempt users from Always-On VPN. For example, use the Selection Criteria area to specify AAA attributes to match user logon IDs.

Step 3 Click the **AnyConnect** tab on the bottom half of the Add or Edit Dynamic Access Policy window.



Step 4 Click **Disable** next to “Always-On VPN for AnyConnect client."

Set a Connect Failure Policy for Always-On

About the Connect Failure Policy

The connect failure policy determines whether the computer can access the internet if Always-On VPN is enabled and Cisco Secure Client cannot establish a VPN session. This can occur when a secure gateway is unreachable, or when Cisco Secure Client fails to detect the presence of a captive portal hotspot.

An open policy permits full network access, letting users continue to perform tasks where access to the Internet or other local network resources is needed.

A closed policy disables all network connectivity until the VPN session is established. Cisco Secure Client does this by enabling packet filters that block all traffic from the endpoint that is not bound for a secure gateway to which the computer is allowed to connect.

Regardless of the connect failure policy, Cisco Secure Client continues to try to establish the VPN connection.

Guidelines for Setting the Connect Failure Policy

Consider the following when using an open policy which permits full network access:

- Security and protection are not available until the VPN session is established; therefore, the endpoint device may get infected with web-based malware or sensitive data may leak.
- An open connect failure policy does not apply if you enable the Disconnect button and the user clicks **Disconnect**.

Consider the following when using a closed policy which disables all network connectivity until the VPN session is established:

- A closed policy can halt productivity if users require Internet access outside the VPN.
- The purpose of closed is to help protect corporate assets from network threats when resources in the private network that protect the endpoint are not available.The endpoint is protected from web-based malware and sensitive data leakage at all times because all network access is prevented except for local resources such as printers and tethered devices permitted by split tunneling.
- This option is primarily for organizations where security persistence is a greater concern than always-available network access.
- A closed policy prevents captive portal remediation unless you specifically enable it.
- You can allow the application of the local resource rules imposed by the most recent VPN session if **Apply Last VPN Local Resources** is enabled in the client profile. For example, these rules could determine access to active sync and local printing.
- The network is unblocked and open during the Cisco Secure Client software upgrade when Always-On is enabled regardless of a closed policy.
- If you deploy a closed connection policy, we highly recommend that you follow a phased approach. For example, first deploy Always-On with a connect failure open policy and survey users for the frequency with which Cisco Secure Client 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.



Caution A connect failure closed policy prevents network access if Cisco Secure Client fails to establish a VPN session. Use extreme caution when implementing a connect failure closed policy.

Configure a Connect Failure Policy

You configure a Connect Failure Policy only when the Always-On feature is enabled. By default, the connect failure policy is closed, preventing Internet access if the VPN is unreachable. To allow Internet access in this situation, the connect failure policy must be set to open.

Procedure

Step 1 Open the VPN Profile Editor and choose **Preferences (Part 2)** from the navigation pane.

Step 2 Set the **Connect Failure Policy** parameter to one of the following settings:

- Closed—(Default) Restricts network access when the secure gateway is unreachable.
- Open—Permits network access by browsers and other applications when the client cannot connect to the secure gateway.

Step 3 If you specified a closed policy:

a) Configure Captive Portal Remediation.

b) Select **Apply Last VPN Local Resources** if you would like to retain the last VPN session's local device rules while network access is disabled.

Use Captive Portal Hotspot Detection and Remediation

About Captive Portals

Many facilities that offer Wi-Fi and wired access, such as airports, coffee shops, and hotels, require the user to pay before obtaining access, to agree to abide by an acceptable use policy, or both. These facilities use a technique called captive portal to prevent applications from connecting until the user opens a browser and accepts the conditions for access. Captive portal detection is the recognition of this restriction, and captive portal remediation is the process of satisfying the requirements of a captive portal hotspot in order to obtain network access.

Captive portals are detected automatically by Cisco Secure Client when initiating a VPN connection requiring no additional configuration. Also, Cisco Secure Client does not modify any browser configuration settings during captive portal detection and does not automatically remediate the captive portal. It relies on the end user to perform the remediation. Cisco Secure Client reacts to the detection of a captive portal depending on the current configuration:

- If Always-On is disabled, or if Always-On is enabled and the Connect Failure Policy is open, the following message is displayed on each connection attempt:

  ```
  The service provider in your current location is restricting access to the Internet.
  You need to log on with the service provider before you can establish a VPN session.
  You can try this by visiting any website with your browser.
  ```

  The end user must perform captive portal remediation by meeting the requirements of the provider of the hotspot. These requirements could be paying a fee to access the network, signing an acceptable use policy, both, or some other requirement defined by the provider.

- If Always-On is enabled and the connect failure policy is closed, captive portal remediation needs to be explicitly enabled. If enabled, the end user can perform remediation as described above. If disabled, the following message is displayed upon each connection attempt, and the VPN cannot be connected.

```
The service provider in your current location is restricting access to the Internet.
The Cisco
        Secure Client protection settings must be lowered for you to log on with the
service provider. Your current enterprise security policy does not allow this.
```

Configure Captive Portal Remediation

You configure captive portal remediation only when the Always-On feature is enabled and the Connect Failure Policy is set to closed. In this situation, configuring captive portal remediation allows Cisco Secure Client to connect to the VPN when a captive portal is preventing it from doing so.



Note Configuration of captive portal remediation is not applicable to Linux, since Always On is not supported on this platform. Therefore, regardless of the *Allow Captive Portal Remediation Always On* setting in the profile editor, the Linux user can remediate a captive portal.

If the Connect Failure Policy is set to open or Always-On is not enabled, your users are not restricted from network access and are capable of remediating a captive portal without any specific configuration in the Cisco Secure Client VPN profile.

By default, captive portal remediation is disabled on platforms supporting Always on to provide the greatest security. Cisco Secure Client does not provide data leakage protection capabilities during the captive portal remediation phase. If data loss protection is desired, you should employ a relevant endpoint security product.

Procedure

Step 1 Open the VPN Profile Editor and choose **Preferences (Part 2)** from the navigation pane.

Step 2 Select **Allow Captive Portal Remediation.**

This setting lifts the network access restrictions imposed by the closed connect failure policy.

Step 3 Specify the Remediation Timeout.

Enter the number of minutes for which Cisco Secure Client lifts the network access restrictions. The user needs enough time to satisfy the captive portal requirements.

Enhanced Captive Portal Remediation (Windows and macOS)

With enhanced captive portal remediation, the Cisco Secure Client embedded browser is used for remediation whenever captive portal is detected with network access restricted by Cisco Secure Client (for example, due to Always On). Other applications remain with network access blocked while captive portal remediation with the Cisco Secure Client browser is pending. The user can close the Cisco Secure Client browser and fail over to an external browser (when enabled in the profile), causing Cisco Secure Client to revert to the regular captive portal remediation behavior. In doing so, the following message is shown:

```
Please retry logging on with the service provider to retain access to the Internet, by
visiting any website with your browser.
```

When captive portal is detected but network access is restricted by Cisco Secure Client, the Cisco Secure Client browser is automatically launched, with the following message displayed to prompt the user to remediate:

```
The service provider in your current location is restricting access to the internet. You
need to log on with the service provider before you establish a VPN session, using the Cisco
 Secure Client browser.
```

Configure Captive Portal Remediation Browser Failover

You may want to set browser failover to apply whenever the Cisco Secure Client browser is launched for captive portal remediation. By setting the browser failover, users can remediate the captive portal via an external browser, after closing the Cisco Secure Client browser.

The Cisco Secure Client browser launched for captive portal remediation has tighter security settings with regard to server security certificates. Untrusted server certificates are not accepted during the captive portal remediation. If an untrusted server certificate is encountered, the corresponding HTTPS URL is not loaded by the Cisco Secure Client browser, potentially blocking the remediation process. If untrusted server certificates are acceptable during captive portal remediation, you should enable captive portal remediation browser failover in order to allow the user to remediate the captive portal. After enabling, the user can close the Cisco Secure Client browser and continue remediation with an external browser (as Cisco Secure Client reverts to the regular captive portal remediation behavior).

Before you begin

Supported on Windows and macOS.

Procedure

Step 1 Open the VPN Profile Editor and choose **Preferences (Part 2)** from the navigation pane.

Step 2 Check **Captive Portal Remediation Browser Failover** if you want the end user to use an external browser (after closing the Cisco Secure Client browser) for captive portal remediation. The default is for the end user to only remediate a captive portal with the Cisco Secure Client browser; that is, the user is unable to disable the enhanced captive portal remediation.

Troubleshoot Captive Portal Detection and Remediation

Cisco Secure Client can falsely assume that it is in a captive portal in the following situations.

- If attempts to contact an Secure Firewall ASA with a certificate containing an incorrect server name (CN), then Cisco Secure Client will think it is in a “captive portal” environment.

  To prevent this, make sure the Secure Firewall ASA certificate is properly configured. The CN value in the certificate must match the name of the Secure Firewall ASA server in the VPN client profile.

- If there is another device on the network before the Secure Firewall ASA, and that device responds to the client's attempt to contact the Secure Firewall ASA by blocking HTTPS access to the ASA, then Cisco Secure Client will think it is in a “captive portal” environment. This situation can occur when a user is on an internal network, and connects through a firewall to connect to the Secure Firewall ASA.

  If you need to restrict access to the Secure Firewall ASA from inside the corporation, configure your firewall such that HTTP and HTTPS traffic to the ASA’s address does not return an HTTP status.

HTTP/HTTPS access to the Secure Firewall ASA should either be allowed or completely blocked to ensure that HTTP/HTTPS requests sent to the ASA will not return an unexpected response.

If users cannot access a captive portal remediation page, ask them to try the following:

- Terminate any applications that use HTTP, such as instant messaging programs, e-mail clients, IP phone clients, and all but one browser to perform the remediation.

  The captive portal may be actively inhibiting DoS attacks by ignoring repetitive attempts to connect, causing them to time out on the client end. The attempt by many applications to make HTTP connections exacerbates this problem.

- Disable and re-enable the network interface. This action triggers a captive portal detection retry.
- Restart the computer.

Configure Cisco Secure Client over L2TP or PPTP

ISPs in some countries require support of the Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP).

To send traffic destined for the secure gateway over a Point-to-Point Protocol (PPP) connection, Cisco Secure Client uses the point-to-point adapter generated by the external tunnel. When establishing a VPN tunnel over a PPP connection, the client must exclude traffic destined for the Secure Firewall ASA from the tunneled traffic intended for destinations beyond the Secure Firewall ASA. To specify whether and how to determine the exclusion route, use the PPP Exclusion setting in the Cisco Secure Client profile. The exclusion route appears as a non-secured route in the Route Details display of the Cisco Secure Client GUI.

Procedure

Step 1 Open the VPN Profile Editor and choose **Preferences (Part 2)** from the navigation pane.

Step 2 Choose a **PPP Exclusion** method. Also, check **User Controllable** for this field to let users view and change this setting:

- Automatic—Enables PPP exclusion. Cisco Secure Client 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. Refer to the Instruct Users to Override PPP Exclusion, on page 125 section.

- Disabled—PPP exclusion is not applied.

Instruct Users to Override PPP Exclusion

If automatic detection does not work and you configured the PPP Exclusion fields as user controllable, the user can override the setting by editing the Cisco Secure Client preferences file on the local computer.

Procedure

Step 1 Use an editor such as Notepad to open the preferences XML file.

This file is at one of the following paths on the user's computer:

- Windows: %LOCALAPPDATA%\Cisco\Cisco Secure Client\VPN\preferences.xml. For example,
- macOS: /Users/username/.vpn/.anyconnect
- Linux: /home/username/.vpn/.anyconnect

Step 2 Insert the PPPExclusion details under `<ControllablePreferences>`, while specifying the Override value and the IP address of the PPP server. The address must be a well-formed IPv4 address. For example:

```
<AnyConnectPreferences>
<ControllablePreferences>
<PPPExclusion>Override
<PPPExclusionServerIP>192.168.22.44</PPPExclusionServerIP></PPPExclusion>
</ControllablePreferences>
</AnyConnectPreferences>
```

Step 3 Save the file.

Step 4 Exit and restart Cisco Secure Client.

Use Management VPN Tunnel

About the Management VPN Tunnel

A management VPN tunnel ensures connectivity to the corporate network whenever the client system is powered up, not just when a VPN connection is established by the end user. You can perform patch management on out-of-the-office endpoints, especially devices that are infrequently connected by the user, via VPN, to the office network. Endpoint OS login scripts which require corporate network connectivity will also benefit from this feature.

The management VPN tunnel is meant to be transparent to the end user; therefore, network traffic initiated by user applications is not impacted, by default, but instead directed outside the management VPN tunnel.

When a management tunnel feature is detected as enabled, a restricted user account (ciscoacvpnuser) is created to enforce the principle of least privilege. This account gets removed during Cisco Secure Client uninstallation or during an installation upgrade.

If a user complains of slow logins, it may be an indication that the management tunnel was not configured appropriately. Configure the Management VPN Tunnel, on page 129 describes the configuration steps that are required to enable the feature. If symptoms suggest lack of connectivity to the corporate network despite following this configuration, refer to Troubleshooting Management VPN Tunnel Connectivity Issues.

Compatibilities and Requirements of Management VPN Tunnel

- Requires ASA 9.0.1 (or later) and ASDM 7.10.1 (or later)

- Connects whenever the user initiated VPN tunnel is disconnected, before or after user login.

Note The management VPN tunnel is not established when a trusted network is detected by the Trusted Network Detection (TND) feature or when Cisco Secure Client software update is in progress.

- Disconnects whenever the user initiates a VPN tunnel, before or after user login.
- Uses only machine store certificate authentication.
- Requires split include tunneling configuration, by default, to avoid impacting user initiated network communication (since the management VPN tunnel is meant to be transparent to the end user). To override this behavior, see Configure a Custom Attribute to Support Tunnel-All Configuration , on page 130.
- Performs strict certificate checking on server certificate. The server certificate's root CA certificate must reside in the machine certificate store (computer certificate store on Windows, or system keychain or system file certificate store on macOS).
- Works with backup server list.
- Currently available only on Windows and macOS. Linux support will be added in subsequent releases.

Incompatibilities and Limitations of Management VPN Tunnel

- The management VPN profile does not support the value *Native* for proxy settings. This restriction applies only to Windows client, since the management VPN tunnel can be initiated without any user logged in; therefore, it cannot rely on user-specific browser proxy settings.
- The management VPN profile does not support private proxy settings that are pushed from the VPN server. Since the management VPN tunnel is meant to be transparent to the end user, user-specific or system proxy settings are not altered.
- Not compatible with the Always On feature, since the management VPN tunnel is established whenever the user VPN tunnel is inactive. However, you can configure the group policy for the management tunnel connection to tunnel all traffic, ensuring that no traffic is leaked by physical interfaces while the user VPN tunnel is inactive. Refer to Configure a Custom Attribute to Support Tunnel-All Configuration , on page 130.
- Captive portal remediation is only performed when the Cisco Secure Client UI is running and while the user is logged in, as if the management VPN tunnel feature was not enabled.
- The management VPN profile settings are only enforced by Cisco Secure Client while the management VPN tunnel is active. When the management VPN tunnel is disconnected, only user VPN tunnel profile settings are enforced. Therefore, the management VPN tunnel is initiated according to the Trusted Network Detection (TND) settings in the user VPN tunnel profile, namely when TND is disabled or when it detects "untrusted network," regardless of the configured Untrusted Network Policy. Additionally, the TND Connect action in the management VPN profile (enforced only when the management VPN tunnel is active), always applies to the user VPN tunnel, to ensure that the management VPN tunnel is transparent to the end user. For a consistent user experience, you must use identical TND settings in both user and management VPN tunnel profiles.

Mandatory Preferences Enforced by Management VPN Profile

Certain profile preferences are mandatory while the management VPN tunnel is active. To assist you in configuring a valid profile, mandatory preferences are enforced by the Cisco Secure Client Management VPN Profile Editor, by disabling the corresponding UI controls. During a management tunnel connection, the following preference values are overridden, mostly to eliminate user interaction and to minimize tunnel interruptions:

- *AllowManualHostInput: false*—Not relevant to the management tunnel (headless client).
- *AlwaysOn: false*—Not relevant, since user tunnel profile preferences are enforced whenever the management tunnel is disconnected.
- *AutoConnectOnStart: false*—Relevant only to a UI client, for automatic connection on start-up to the previously connected host.
- *AutomaticCertSelection: true*—To avoid certificate selection popups.
- *AutoReconnect: true*—To avoid management tunnel termination on network changes.
- *AutoReconnectBehavior: ReconnectAfterResume*—To avoid management tunnel termination on network changes.
- *AutoUpdate: false*—No software updates are performed during a management tunnel connection.
- *BlockUntrustedServers: true*—To avoid untrusted server certificate prompts.
- *CertificateStore: MachineStore*—Management tunnel authentication should also succeed without a logged in user.
- *CertificateStoreOverride: true*—Required for machine certificate authentication on Windows.
- *EnableAutomaticServerSelection: false*—Only one host entry is expected in the management VPN profile.
- *EnableScripting: false*—Cisco Secure Client customization scripts (invoked at connect and/or disconnect time) are not executed during a management tunnel connection.
- *MinimizeOnConnect:false*—Not relevant to the management tunnel (headless client).
- *RetainVPNOnLogoff:true*—The management tunnel should remain active on user logoff.
- *ShowPreConnect Message*—Not relevant to the management tunnel (headless client).
- *UserEnforcement: AnyUser*—To ensure that the management tunnel is not potentially disconnected when a certain user logs in.
- *UseStartBeforeLogon:False*—Only applicable to user tunnel.
- *WindowsVPNEstablishment: AllowRemote Users*—To ensure that the management tunnel is not impacted by any type of user (local/remote) logging in.
- *LinuxVPNEstablishment: Allow Remote Users*— To ensure that the management tunnel is not impacted by any type of user (local/remote)

Also, Cisco Secure Client does not enforce the following profile preferences during a management tunnel connection: WindowsLogonEnforcement and SCEP related preferences.

Configure the Management VPN Tunnel

Because the management tunnel connection may occur without any user logged in, only machine store certificate authentication is supported. Consequently, at least one relevant client certificate needs to be available in the client host's machine certificate store.

Configure the Tunnel Group for the Management VPN Tunnel

You must configure the authentication method of the tunnel group as "certificate only" by navigating to **Configuration** > **Remote Access > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit** in ASDM and choosing it from the Method drop-down menu under Authentication. Then configure the group URL in Advanced > Group Alias/Group URL, which is then specified in the management VPN profile (as described in Create a Profile for Management VPN Tunnel, on page 129).

The group policy for this tunnel group must have split include tunneling configured for all IP protocols with client address assignment configured in the the tunnel group: choose **Tunnel Network List Below** from ASDM **Remote Access VPN** > **Network (Client) Access > Group Policies > Edit > Advanced > Split Tunneling** > **.** Configure a Custom Attribute to Support Tunnel-All Configuration , on page 130 describes how to enable support for other split tunneling configurations. If a client address assignment is not configured in the tunnel group for both IP protocols, you must enable *Client Bypass Protocol* in the group policy, so that traffic matching the IP protocol without client address assignment is not disrupted by the management VPN tunnel.

Create a Profile for Management VPN Tunnel

You can deploy only one management VPN profile to a given client device. The management VPN profile is stored in a dedicated directory (%ProgramData%\Cisco\Cisco Secure Client\VPN\Profile\MgmtTun in Windows, /opt/cisco/secureclient/VPN/profile/mgmttun in macOS) with a fixed name (VpnMgmtTunProfile.xml). A management VPN profile can have zero or one host entry that points to a tunnel group configured as per section Configure the Tunnel Group for the Management VPN Tunnel, on page 129. To automatically disable the feature (upon profile update during tunnel establishment), you should configure zero host entries in the management VPN profile.

Before you begin

Complete Configure the Tunnel Group for the Management VPN Tunnel, on page 129.

Procedure

Step 1 Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

Step 2 Click **Add**. The Add AnyConnect Client Profiles window appears.

Step 3 Choose **AnyConnect Management VPN Profile** as the profile usage. Refer to the *Configure AnyConnect Client Profiles* section in the Cisco ASA Series VPN ASDM Configuration Guide for further description of how to populate the fields on the Add AnyConnect Client Profile screen.

Step 4 Choose the group policy created in Configure the Tunnel Group for the Management VPN Tunnel, on page 129. Click **OK** to create the Management VPN Profile, then **Edit** to configure it, as well as for subsequent updates.

(Optional) Upload an Already Configured Management VPN Profile

You may need to upload to Secure Firewall ASA an already configured management VPN profile that was edited or created using the standalone Cisco Secure Client Management VPN Profile Editor, copied from Cisco Secure Client, or exported from another Secure Firewall ASA.

Procedure

Step 1 From the AnyConnect Client Profile window in ASDM, click **Add** and then **Upload...**.
When choosing a destination location for the upload file, ensure that you choose a profile with a *vpnm* extension.

Step 2 Provide a profile name and choose **AnyConnect Management VPN Profile** from the Profile Usage drop-down menu.

Step 3 Choose the group policy created in Configure the Tunnel Group for the Management VPN Tunnel, on page 129. Click **OK** to create the Management VPN Profile.

Associate the Management VPN Profile to Group Policies

You must add the management VPN profile to the group policy associated with the tunnel group used for the management tunnel connection.

Note Similarly, you may also add the management VPN profile to the group policy mapped to the regular tunnel group, used for the user tunnel connection. When the user connects, the management VPN profile is downloaded, along with the user VPN profile already mapped to the group policy, enabling the management VPN tunnel feature.

Alternatively, you can deploy the management VPN profile out of band: ensure it is named VpnMgmtTunProfile.xml, copy it to the above mentioned management VPN profile directory, and restart the Cisco Secure Client Agent service (or reboot).

Before you begin

Complete Configure the Tunnel Group for the Management VPN Tunnel, on page 129 and Create a Profile for Management VPN Tunnel, on page 129.

Procedure

Step 1 Navigate to **Group Policy** > **Advanced** > **AnyConnect Client** in ASDM.

Step 2 In Client Profiles to Download, click **Add** and choose the management VPN profile created or updated in the Create a Profile for Management VPN Tunnel, on page 129 section.

Configure a Custom Attribute to Support Tunnel-All Configuration

Management VPN tunnel requires split include tunneling configuration, by default, to avoid impacting user initiated network communication (since management VPN tunnel is meant to be transparent to the end user). You can override this behavior by configuring the following custom attribute in the group policy used by the

management tunnel connection (in the Create Custom Attribute ASDM window: **Configuration** > **Remote Access VPN > Network (Client) Access > Group Policies > Edit > Advanced > AnyConnect Client > Custom Attributes > Add**).

If you set a new custom attribute type to **ManagementTunnelAllAllowed** and set the corresponding custom attributes to *true,* Cisco Secure Client proceeds with the management tunnel connection, if the configuration is one of tunnel-all, split-exclude, split-include, or bypass for both IP protocols.

Restrict Management VPN Profile Updates

You can restrict management VPN profile updates to a certain trusted server list with a new AnyConnect local policy file (AnyConnectLocalPolicy.xml) setting, and still allow user VPN profile updates from any server. Edit this setting through the AnyConnect VPN Local Policy Editor by checking the **Allow Management VPN Profile Updates From Any Server** checkbox.

For example, if management VPN profile updates are allowed only from the VPN server TrustedServer, the checkbox would be unchecked, and TrustedServer would be added to the trusted server list. (Replace TrustedServer with the FQDN or IP address present in the corresponding VPN profile server entry.)

Troubleshoot Management VPN Tunnel Connectivity Issues

If the client host is not reachable remotely, various scenarios may have occurred causing the management VPN tunnel to disconnect or not be established. In these scenarios, the Cisco Secure Client GUI and CLI reflect the Management Connection State as a statistics entry:

- Disconnected (disabled)—The feature is disabled.
- Disconnected (trusted network)—TND detected a trusted network so the management tunnel is not established.
- Disconnected (user tunnel active)—A user tunnel is currently pending (thus disconnecting the management tunnel).
- Disconnected (process launch failed)—A process launch failure was encountered upon attempting the management tunnel connection.
- Disconnected (connect failed)—A connection failure was encountered upon establishing the management tunnel.
- Disconnected (invalid VPN configuration)—An invalid split tunneling configuration was encountered upon management tunnel establishment. Refer to Configure a Custom Attribute to Support Tunnel-All Configuration , on page 130 for additional information.
- Diconnected (software update pending)—Cisco Secure Client software update is currently pending (thus disconnecting the management tunnel).
- Disconnected—The management tunnel is about to be established or could not be established for some other reason.

To troubleshoot the lack of connectivity over the management VPN tunnel (expected to be established on the client host), verify the following:

- Check the state of the management VPN connection on the Cisco Secure Client UI Statistics tab, in the Export Stats output, or the Connection Information/Management Connection State in the CLI. If the

management connection state is unexpectedly listed as "disconnected" and the provided explanation is insufficient, capture the Cisco Secure Client logs with the DART tool for further troubleshooting.

- If you see *Management Connection State: Disconnected (disabled)* in the UI stats line, ensure that the management VPN profile is configured with a single host entry, pointing to a tunnel group set up with certificate authentication. The associated group policy must have a single profile configured: the management VPN profile.



Note The associated group policy should have no banner enabled. User interaction is not supported during a management tunnel connection.

- If you see *Management Connection State: Disconnected (disabled)* in the UI stats line, ensure that the management VPN profile is configured within the group policy that is associated with the tunnel group used for regular user tunnel connections. When the user connects with that tunnel group, the management VPN profile is downloaded, and the feature is enabled.



Note Alternatively, you can deploy the management VPN profile out of band.

- If you see *Management Connection State: Disconnected (connect failed)* in the UI stats line, note that the management tunnel connection fails whenever user interaction is needed, as follows:
  - if the server certificate is not trusted. The server certificate's root CA certificate must reside in the machine certificate store.
  - if a private key (pertaining to a machine store certificate) is password protected, the corresponding client certificate is not usable by the management tunnel connection. The client certificate is not usable because the user cannot be prompted for the private key password.
  - if a macOS system keychain private key is not configured to allow access without prompting to the Cisco Secure Client agent executable (vpnagentd); the corresponding client certificate is unusable by the management tunnel connection, since the user cannot be prompted for credentials to access the private key.
  - if group policy was configured with a banner.

Configure Cisco Secure Client Proxy Connections

About Cisco Secure Client Proxy Connections

Cisco Secure Client supports VPN sessions through Local, Public, and Private proxies:

- Local Proxy Connections:

  A local proxy runs on the same PC as Cisco Secure Client, and is sometimes used as a transparent proxy. Some examples of a transparent proxy service include acceleration software provided by some wireless data cards, or a network component on some antivirus software, such as Kaspersky.

The use of a local proxy is enabled or disabled in the Cisco Secure Client profile, see Allow a Local Proxy Connection.

- Public Proxy Connections:

  Public proxies are usually used to anonymize web traffic. When Windows is configured to use a public proxy, Cisco Secure Client uses that connection. Public proxy is supported on macOS and Linux for both native and override.

  Configuring a public proxy is described in Public Proxy, on page 134 .

- Private Proxy Connections:

  Private proxy servers are used on a corporate network to prevent corporate users from accessing certain Web sites based on corporate usage policies, for example, pornography, gambling, or gaming sites.

  You configure a group policy to download private proxy settings to the browser after the tunnel is established. The settings return to their original state after the VPN session ends. See Configure a Private Proxy Connection, on page 135.



Note Cisco Secure Client SBL connections through a proxy server are dependent on the Windows operating system version and system (machine) configuration or other third-party proxy software capabilities; therefore, refer to system wide proxy settings as provided by Microsoft or whatever third-party proxy application you use.

Control Client Proxy with VPN Client Profile

The VPN Client profile can block or redirect the client system's proxy connection. For Windows and Linux, you can configure, or you can allow the user to configure, the address of a public proxy server.

For more information about configuring the proxy settings in the VPN client profile, see Cisco Secure Client Profile Editor, Preferences (Part 2), on page 81.

Proxy Auto-Configuration File Generation for Clientless Support

Some versions of the Secure Firewall ASA require Cisco Secure Client configuration to support clientless portal access through a proxy server after establishing the Cisco Secure Client session. Cisco Secure Client uses a proxy auto-configuration (PAC) file to modify the client-side proxy settings to let this occur. Cisco Secure Client generates this file only if the Secure Firewall ASA does not specify private-side proxy settings.

Requirements for Cisco Secure Client Proxy Connections

OS support of proxy connections varies as shown:

Proxy Connection Type	Windows	macOS	Linux
Local Proxy	Yes	Yes (Override& Native)	Yes

Proxy Connection Type	Windows	macOS	Linux
Private Proxy	Yes (on Internet Explorer)	Yes (set as system proxy settings)	No
Public Proxy	Yes (IE and Override)	Yes (Override & Native	Yes (Override& Native)

Limitations on Proxy Connections

- Connecting through a proxy is not supported with the Always-On feature enabled.
- A VPN client profile is required to allow access to a local proxy.

Allow a Local Proxy Connection

Procedure

Step 1 Open the VPN Profile Editor and choose **Preferences (Part 2)** from the navigation pane.

Step 2 Select (default) or unselect **Allow Local Proxy Connections**. Local proxy is disabled by default.

Public Proxy

Public proxies are supported on Windows and Linux platforms. Proxy servers are chosen based on preferences set in the client profile. In case of proxy override, Cisco Secure Client extracts proxy servers from the profile. With release 4.1 (and later) we added proxy support on macOS along with Native-proxy configuration on Linux and macOS.

On Linux, native-proxy settings are exported before Cisco Secure Client runs. If you change the settings, a restart must happen.

Authenticating Proxy Servers requires a username and password. Cisco Secure Client supports Basic and NTLM authentication when the proxy server is configured to require authentication. Cisco Secure Client dialogs manage the authentication process. After successfully authenticating to the proxy server, Cisco Secure Client prompts for the Secure Firewall ASA username and password.

Configure a Public Proxy Connection, Windows

Follow these steps to configure a public proxy connection on Windows.

Procedure

Step 1 Open **Internet Options** from Internet Explorer or the Control Panel.

Step 2 Select the **Connections** Tab, and click the **LAN Settings** button.

Step 3 Configure the LAN to use a proxy server, and enter the IP address of the proxy server.

Configure a Public Proxy Connection, macOS

Procedure

Step 1 Go to system preferences and choose the appropriate interface on which you are connected.

Step 2 Click **Advanced**.

Step 3 Choose **Proxies** tab from the new window.

Step 4 Enable HTTPS proxy.

Step 5 Enter the proxy server address in the Secure Proxy Server field on the right panel.

Configure a Public Proxy Connection, Linux

To configure a public proxy connection in Linux, you must set an environment variable.

Configure a Private Proxy Connection

Procedure

Step 1 Configure the private proxy information in the Secure Firewall ASA group policy. See the Configuring a Browser Proxy for an Internal Group Policy section in the Cisco ASA Series VPN CLI or ASDM Configuration Guide.

Note
In a macOS environment, the proxy information that is pushed down from the Secure Firewall ASA (upon a VPN connection) is not viewed in the browser until you open up a terminal and issue a `scutil --proxy`.

Step 2 (Optional) Configure the Client to Ignore Browser Proxy Settings.

Step 3 (Optional) Lockdown the Internet Explorer Connections Tab.

What to do next



Note When a VPN session initiated via proxy is active, network access via proxy is restricted only to Cisco Secure Client related processes. Therefore, to accommodate third-party applications communicating over HTTP/HTTPS, you must set the private proxy settings in the VPN policy to something other than *Do not modify client proxy settings*, such as *Do not use proxy*. Alternatively, you can configure the VPN profile Proxy Settings so that system proxy settings are ignored upon initiating a VPN connection.

Proxy hardening enforcement remains enabled if the private proxy matches the public proxy settings.

Configure the Client to Ignore Browser Proxy Settings

You can specify a policy in the Cisco Secure Client profile to bypass the Microsoft Internet Explorer or Safari proxy configuration settings on the user's PC. This prevents the user from establishing a tunnel from outside the corporate network, and prevents Cisco Secure Client from connecting through an undesirable or illegitimate proxy server.

Procedure

Step 1 Open the VPN Profile Editor and choose **Preferences (Part 2)** from the navigation pane.

Step 2 In the Proxy Settings drop-down list, choose **IgnoreProxy**. Ignore Proxy causes the client to ignore all proxy settings. No action is taken against proxies that are downloaded from the Secure Firewall ASA.

Lock Down the Internet Explorer Connections Tab

Under certain conditions, Cisco Secure Client hides the Internet Explorer Tools > Internet Options > Connections tab. When exposed, this tab lets the user set proxy information. Hiding this tab prevents the user from intentionally or unintentionally circumventing the tunnel. The tab lockdown is reversed on disconnect, and it is superseded by any administrator-defined policies applied to that tab. The conditions under which this lock down occurs are the following:

- The Secure Firewall ASA configuration specifies Connections tab lockdown.
- The Secure Firewall ASA configuration specifies a private-side proxy.
- A Windows group policy previously locked down the Connections tab (overriding the no lockdown Secure Firewall ASA group policy setting).

You can configure the Secure Firewall ASA to allow or not allow proxy lockdown, in the group policy. To do this using ASDM, follow this procedure:

Procedure

Step 1 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.

Step 2 Select a group policy and click **Edit** or **Add** a new group policy.

Step 3 In the navigation pane, go to **Advanced** > **Browser Proxy**. The Proxy Server Policy pane displays.

Step 4 Click **Proxy Lockdown** to display more proxy settings.

Step 5 Uncheck **Inherit** and select **Yes** to enable proxy lockdown and hide the Internet Explorer Connections tab for the duration of the Cisco Secure Client session or; select **No** to disable proxy lockdown and expose the Internet Explorer Connections tab for the duration of the Cisco Secure Client session.

Step 6 Click **OK** to save the Proxy Server Policy changes.

Step 7 Click **Apply** to save the Group Policy changes.

Verify the Proxy Settings

- For Windows: Find the user and system proxy settings in the registry under:

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
```

- For macOS: Open a terminal window, and type:

```
scutil --proxy
```

Select and Exclude VPN Traffic

Configure IPv4 or IPv6 Traffic to Bypass the VPN

You can configure how Cisco Secure Client manages IPv4 traffic when the Secure Firewall ASA is expecting only IPv6 traffic or how Cisco Secure Client manages IPv6 traffic when the ASA is only expecting IPv4 traffic using the Client Bypass Protocol setting.

When Cisco Secure Client makes a VPN connection to the Secure Firewall ASA, the ASA can assign the client an IPv4, IPv6, or both an IPv4 and IPv6 address.

If Client Bypass Protocol is enabled for an IP protocol and an address pool is not configured for that protocol (in other words, no IP address for that protocol was assigned to client by the Secure Firewall ASA), any IP traffic using that protocol will not be sent through the VPN tunnel. It will be sent outside the tunnel.

If Client Bypass Protocol is disabled, and an address pool is not configured for that protocol, the client drops all traffic for that IP protocol once the VPN tunnel is established.

For example, assume that the Secure Firewall ASA assigns only an IPv4 address to the Cisco Secure Client connection, and the endpoint is dual stacked. When the endpoint attempts to reach an IPv6 address, if Client Bypass Protocol is disabled, the IPv6 traffic is dropped. If Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear.

If establishing an IPsec tunnel (as opposed to an SSL connection), the Secure Firewall ASA is not notified whether or not IPv6 is enabled on the client, so Secure Firewall ASA always pushes down the client bypass protocol setting.

You configure the Client Bypass Protocol on the Secure Firewall ASA in the group policies.

Procedure

Step 1 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**.

Step 2 Select a group policy and click **Edit** or **Add** a new group policy.

Step 3 Select **Advanced** > **AnyConnect**.

Step 4 Next to **Client Bypass Protocol**, uncheck **Inherit** if this is a group policy other than the default group policy.

Step 5 Choose one of these options:

- Click **Disable** to drop IP traffic for which the Secure Firewall ASA did not assign an address.
- Click **Enable** to send that IP traffic in the clear.

Step 6 Click **OK**.

Step 7 Click **Apply**.

Configure a Client Firewall with Local Printer and Tethered Device Support

Usage Notes About Firewall Behavior

The following notes clarify how the Secure Client uses the firewall:

The source IP is not used for firewall rules. The client ignores the source IP information in the firewall rules sent from the ASA. The client determines the source IP depending on whether the rules are public or private. Public rules are applied to all interfaces on the client. Private rules are applied to the Virtual Adapter.

The ASA supports many protocols for ACL rules. However, the Secure Client firewall feature supports only TCP, UDP, ICMP, and IP. If the client receives a rule with a different protocol, it treats it as an invalid firewall rule, and then disables split tunneling and uses full tunneling for security reasons.

Be aware of the following differences in behavior for each operating system:

- For Windows devices, deny rules take precedence over allow rules in Windows Firewall. If the ASA pushes down an allow rule to the Secure Client, but the user has created a custom deny rule, the Secure Client rule is not enforced.
- Windows users whose firewall service must be started by the Secure Client (not started automatically by the system) may experience a noticeable increase in the time it takes to establish a VPN connection.
- On macOS devices, the Secure Client applies rules sequentially in the same order the ASA applies them. Global rules should always be last.
- For third-party firewalls, traffic is passed only if both the Secure Client firewall and the third-party firewall allow that traffic type. If the third-party firewall blocks a specific traffic type that the Secure Client allows, the client blocks the traffic.

Limitations and Restrictions of the Client Firewall

When using the client firewall to restrict local LAN access, Secure Firewall Posture and some third-party firewalls can interfere with the firewall.

The following table clarifies what direction of traffic is affected by the source and destination port settings:

Source Port	Destination Port	Traffic Direction Affected
Specific port number	Specific port number	Inbound and outbound
A range or 'All' (value of 0)	A range or 'All' (value of 0)	Inbound and outbound
Specific port number	A range or 'All' (value of 0)	Inbound only
A range or 'All' (value of 0)	Specific port number	Outbound only

See the *Client Firewall with Local Printer and Tethered Device Support* section in the Cisco ASA Series VPN CLI or ASDM Configuration Guide for additional information.

Configure Split Tunneling

Split tunneling is configured in a Network (Client) Access group policy. See the *Configure Split Tunneling for AnyConnect Traffic* section in the Cisco ASA Series VPN CLI or ASDM Configuration Guide.

After making changes to the group policy in ASDM, be sure the group policy is associated with a Connection Profile in **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Group Policy**.

Routing Network Traffic on Linux

To enable Linux users to route network traffic on a VM instance/docker container, you must create a new custom attribute and enable it. Create a **tunnel-from-any-source** custom attribute and when set to *true*, Cisco Secure Client permits packets with any source addresses in split-include or split-exclude tunnel mode, allowing network access inside the VM instance or Docker container.

Note The network used by the VM instance or Docker container must be excluded from the tunnel initially.

Omitted Traffic

Regardless of whether your VPN tunnel type (Full, Split Include, or Split Exclude), DHCPv4, DHCPv6, and Stateless Address Autoconfiguration packets are allowed. Their traffic on the public network helps the operating system to negotiate an IP address and ensure baseline IP connectivity.

About Dynamic Split Tunneling

Dynamic split tunneling was designed to enhance the static split tunneling options, which are configured with the "Exclude Network List Below" or "Tunnel Network List Below" option in ASDM group policy configuration. Beyond the static inclusions or exclusions typically used to define split tunneling, the dynamic split tunneling inclusions or exclusions address scenarios when traffic pertaining to a certain service needs to be excluded from or included into the VPN tunnel. Additionally, we provide an enhanced dynamic split tunneling, where both dynamic exclude and dynamic include domains are specified.

The limits also vary from static split tunneling to dynamic split tunneling. For static split tunneling, the limit is 2500 networks/ACEs per IP protocol. With dynamic split tunneling, Cisco Secure Client takes into account only dynamic split tunneling domains with the first 20,000 characters of the domain list pushed by the headend,

and is only enforced via truncation on the client. Wildcards are not supported. For both dynamic split exclude and dynamic split include, besides the configured domains, all of their subdomains are also excluded from (or included into for dynamic split include) the tunnel.

Dynamic Split Exclude Tunneling—Multiple cloud-based services may be hosted on the same IP pool and may resolve to different IP addresses based on the location of the user or the load of cloud-hosted compute resources. Administrators who only want to exclude a single such service from the VPN tunnel would have a difficult time defining such a policy using static exclusions, especially when ISP NAT, 6to4, 4to6, and other network translation schemes are also considered. With dynamic split exclude tunneling, you can dynamically provision split exclude tunneling after tunnel establishment, based on the host DNS domain name. For example, a VPN administrator could configure example.com to be excluded from the VPN tunnel at runtime. When the VPN tunnel is up and an application attempts to connect to mail.example.com, the VPN client automatically changes the system routing table and filters to allow the connection outside of the tunnel.

Enhanced Dynamic Split Exclude Tunneling—When dynamic split exclude tunneling is configured with both dynamic split exclude and dynamic split include domains, traffic dynamically excluded from the VPN tunnel much match at least one dynamic split exclude domain, but no dynamic split include domains. For example, if a VPN administrator configured a dynamic split exclude domain example.com and a dynamic split include domain of mail.example.com, all example.com traffic other than mail.example.com is excluded from tunneling.

Dynamic Split Include Tunneling—With dynamic split include tunneling, you can dynamically provision split include tunneling after tunnel establishment, based on the host DNS domain name. For example, a VPN administrator could configure domain.com to be included into the VPN tunnel at runtime. When the VPN tunnel is up and an application attempts to connect to www.domain.com, the VPN client automatically changes the system routing table and filters to allow the connection inside the VPN tunnel.

Enhanced Dynamic Split Include Tunneling—When dynamic split include tunneling is configured with both dynamic split include and dynamic split exclude domains, traffic dynamically included into the VPN tunnel must match at least one dynamic split include domain, but no dynamic split exclude domains. For example, if a VPN administrator configured domain.com as a split include domain and www.domain.com as a split exclude domain, all domain.com traffic other than www.domain.com is tunneled.



Note Dynamic split tunneling is not supported on Linux or any mobile platforms.

Interoperability Between Static Split Tunneling and Dynamic Split Tunneling

Both static and dynamic exclusions can coexist. While static split tunneling is applied when the tunnel is established, dynamic split tunneling is applied when the traffic to the domain occurs, while the tunnel is already connected.

Dynamic Split Exclude Tunneling

Dynamic split exclude tunneling applies to "tunnel all," "split include," and "split exclude" tunneling:

- Tunnel All Networks—All exclusions from the VPN tunnel are dynamic.
- Exclude Specific Networks—Dynamic exclusions are added to preconfigured static ones.
- Include Specific Networks—Dynamic exclusions are only relevant if at least one IP address of the excluded host names overlaps with a split include network. Otherwise, the traffic is already excluded from the VPN tunnel, and no dynamic exclusion is performed.

Enhanced dynamic split exclude tunneling applies to "tunnel all" and "split exclude" tunneling. If both dynamic split exclude and dynamic split include domains, as well as split include tunneling, are configured, the resulting configuration is enhanced dynamic split include tunneling.

Dynamic Split Include Tunneling

Dynamic split include tunneling applies only to split include configuration.

Enhanced dynamic split include tunneling applies only to split include configuration.



Note Umbrella Roaming Security protection is active when either static or dynamic split tunneling is enabled. You may have to statically include or exclude the Umbrella cloud resolvers from the VPN tunnel, unless they are reachable and can be probed over the VPN tunnel.

Outcome of Overlapping Scenarios with Split Tunneling Configuration

Dynamic inclusion or exclusion covers only IP addresses not already included or excluded. When both static and some form of dynamic tunneling is applied and a new inclusion or exclusion needs to be enforced, a collision with an already applied inclusion or exclusion may occur. When a dynamic exclusion is enforced (which contains all IP addresses that are part of a DNS response matching an excluded domain name), only those addresses not already excluded are considered for exclusion. Likewise, when a dynamic inclusion is enforced (which contains all IP addresses that are part of a DNS response matching an included domain name), only those addresses not already included are considered for inclusion.

Static public routes (such as split-exclude and critical routes such as the secure gateway route) take precedence over dynamic split include routes. For that reason, if at least one IP address of the dynamic inclusion matches a static public route, the dynamic inclusion is not enforced.

Similarly, static split-include routes take precedence over dynamic split exclude routes. For that reason, if at least one IP address of the dynamic exclusion matches a static split-include route, the dynamic exclusion is not enforced.

Notifications of Dynamic Split Tunneling Usage

While the VPN tunnel is connected, you can see what is set for dynamic split tunneling in several ways:

- Statistics tab—Displays Dynamic Tunnel Exclusions and Dynamic Tunnel Inclusions, containing the domain names excluded from or included into the VPN tunnel, as configured in the Secure Firewall ASA group policy.
- Export Stats—Produces a file that contains the domain names excluded from or included into the VPN tunneling, along with the tunnel modes for both IPv4 and IPv6. Dynamic routes are also included in the exported statistics.
- Route Details tab—Shows the IPv4 and IPv6 dynamic split exclude and include routes with the host names that correspond to each excluded or included IP address.



Note The Cisco Secure Client UI only displays up to 200 per IP protocol of the secured or non-secured routes enforced by AnyConnect VPN. In excess of 200 routes, truncation occurs, and you can run either **`route print`** on Windows or **`netstat -rn`** on Linux or macOS to view all routes.

- VPN configuration log message—Shows the number of domains excluded from or included into the VPN tunnel.

Configure Dynamic Split Exclude Tunneling

Before you begin

Refer to About Dynamic Split Tunneling, on page 139.

With dynamic split tunneling, you can dynamically provision split exclude tunneling after tunnel establishment based on the host DNS domain name. Dynamic split tunneling is configured by creating a custom attribute and adding it to a group policy on Secure Firewall ASA. Refer to *Configure Dynamic Split Tunneling* in the Cisco ASA Series VPN ASDM Configuration Guide for GUI steps.

Procedure

Step 1 Define the custom attribute type in the WebVPN context with the following command:

```
anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude domains
```

Step 2 Define the custom attribute names for each cloud/web service that needs access by the client outside the VPN tunnel. For example, add Google_domains to represent a list of DNS domain names pertaining to Google web services. The attribute value contains the list of domain names to exclude from the VPN tunnel and must be in comma-separated-values (CSV) format using the following as an example:

```
anyconnect-custom-data dynamic-split-exclude-domains example_service_domains example1.com, example2.com
```

Step 3 Attach the previously defined custom attribute to a certain policy group with the following command, executed in the group-policy attributes context:

```
anyconnect-custom dynamic-split-exclude-domains value example_service_domains
```

Configure Enhanced Dynamic Split Exclude Tunneling

Before you begin

Refer to About Dynamic Split Tunneling, on page 139.

Enhanced domain name matching is supported when dynamic split exclude tunneling is configured with both dynamic split exclude and dynamic split include domains. Enhanced dynamic split exclude tunneling is configured by creating two custom attribute and adding it to a group policy on Secure Firewall ASA. Refer to *Configure Dynamic Split Tunneling* in the Cisco ASA Series VPN ASDM Configuration Guide for GUI steps.

Procedure

Step 1 Define the custom attribute type in the WebVPN context with the following command:

```
anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude domains
```

Step 2 Define the custom attribute names for each cloud/web service that needs access by the client outside the VPN tunnel. For example, when example.com is the dynamic split exclude domain while www.example.com is the dynamic split include domain, all traffic to examples.com is excluded except www.example.com. The attribute value contains the list of domain names to exclude (or not) from the VPN tunnel and must be in comma-separated-values (CSV) format using the following as an example:

```
anyconnect-custom-data dynamic-split-exclude-domains example_service_domains example1.com, example2.com
```

```
anyconnect-custom-data dynamic-split-include-domains example_service_domains_tunneled www.example1.com,
 www.example2.com
```

Step 3 Attach the previously defined custom attributes to a certain policy group with the following command, executed in the group-policy attributes context:

```
anyconnect-custom dynamic-split-exclude-domains value
```

```
example_service_domains
```

```
anyconnect-custom dynamic-split-include-domains value
```

```
example_service_domains_tunneled
```

Configure Dynamic Split Include Tunneling

Before you begin

Refer to About Dynamic Split Tunneling, on page 139.

With dynamic split tunneling, you can dynamically provision split include tunneling after tunnel establishment based on the host DNS domain name. Dynamic split tunneling is configured by creating a custom attribute and adding it to a group policy on Secure Firewall ASA. Refer to *Configure Dynamic Split Tunneling* in the Cisco ASA Series VPN ASDM Configuration Guide for GUI steps.

Procedure

Step 1 Define the custom attribute type in the WebVPN context with the following command:

```
anyconnect-custom-attr dynamic-split-include-domains description dynamic split include domains
```

Step 2 Define the custom attribute names for each cloud/web service that needs client access by the VPN tunnel. The attribute value contains the list of domain names to include into the VPN tunnel and must be in comma-separated-values (CSV) format using the following as an example:

```
anyconnect-custom-data dynamic-split-include-domains corporate_service_domains domain1.com, domain2.com
```

Note
A custom attribute cannot exceed 421 characters. A list of dynamically included domains (in CSV format) may need to be partitioned into smaller values if exceeding the limit.

Step 3 Attach the previously defined custom attribute to a certain policy group with the following command, executed in the group-policy attributes context:

```
anyconnect-custom dynamic-split-include-domains value
```

```
corporate_service_domains
```

Configure Enhanced Dynamic Split Include Tunneling

Before you begin

Refer to About Dynamic Split Tunneling, on page 139.

Enhanced domain name matching is supported when dynamic split include tunneling is configured with both dynamic split include and dynamic split exclude domains. Enhanced dynamic split include tunneling is configured by creating two custom attribute and adding it to a group policy on Secure Firewall ASA. Refer to *Configure Dynamic Split Tunneling* in the Cisco ASA Series VPN ASDM Configuration Guide for GUI steps.

Procedure

Step 1 Define the custom attribute type in the WebVPN context with the following command:

```
anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude domains
```

Step 2 Define the custom attribute names for each cloud/web service that needs client access from the VPN tunnel. For example, when domain.com is the dynamic split include domain while www.domain.com is the dynamic split exclude domain, all traffic to domain.com is included except www.domain.com.The attribute value contains the list of domain names to include (or not) into the VPN tunnel and must be in comma-separated-values (CSV) format using the following as an example:

```
anyconnect-custom-data dynamic-split-include-domains corporate_service_domains domain1.com, domain2.com
```

```
anyconnect-custom-data dynamic-split-include-domains corporate_service_domains_excluded www.domain1.com,
 www.domain2.com
```

Step 3 Attach the previously defined custom attributes to a certain policy group with the following command, executed in the group-policy attributes context:

```
anyconnect-custom dynamic-split-include-domains value
```

```
corporate_service_domains
```

```
anyconnect-custom dynamic-split-exclude-domains value
```

```
corporate_service_domains_excluded
```

Split DNS

Split DNS is supported for both split include and split exclude tunneling configurations.

When split DNS for split include tunneling is configured in the Network (Client) Access group policy, Cisco Secure Client tunnels specific DNS queries to a VPN DNS server (also configured in the group policy). All other DNS queries are directed outside the VPN tunnel, to a public DNS server.

When split DNS for split exclude tunneling is configured, specific DNS queries are sent outside the VPN tunnel, to a public DNS server. All othe DNS queries are tunneled to a VPN DNS server.

If split DNS is not enabled with a split tunneling configuration, DNS queries are routed over the tunnel only if "Send All DNS lookups through tunnel" is configured in the group policy. Otherwise, they could be also routed outside the tunnel.

Requirements for Split DNS

Split DNS is supported on Windows and macOS platforms.

- Limited support is available on Linux, namely only tunneled DNS requests are subject to the split DNS policy. Consequently, some DNS requests sent outside the tunnel may not comply with the split DNS policy.

For macOS, Cisco Secure Client can use true split-DNS for a certain IP protocol only if one of the following conditions is met:

- Split-DNS is configured for one IP protocol (such as IPv4), and Client Bypass Protocol is configured for the other IP protocol (such as IPv6) in the group policy (with no address pool configured for the latter IP protocol).
- Split-DNS is configured for both IP protocols.

If split DNS for split include is configured for one IP protocol and split DNS for split exclude is configured for the other protocol, split DNS for split include takes precedence, resulting in Cisco Secure Client ignoring the split DNS for split exclude settings.

Split DNS is relevant only to typical applications relying on the native/OS DNS client for name resolution, such as browsers, mail applications, and such. Unsupported applications include tools using a custom resolver, such as dig and nslookup.

You can assign multiple DNS suffixes if you add them to the split-dns list and specify a default domain on the Secure Firewall ASA.

Cisco Secure Client builds the DNS suffix list in the following order:

- The domain passed by the head end.
- The split-DNS suffix list passed by the head end.
- The public interface's DNS suffixes, if configured. If not, the primary and connection-specific suffixes, along with the parent suffixes of the primary DNS suffix (if the corresponding box is checked in the Advanced TCP/IP Settings).

Configure Split DNS for Split Include Tunneling

To configure split DNS for split include tunneling in the group policy, do the following:

Procedure

Step 1 Configure at least one DNS server.

See the *Configure Server Attributes for an Internal Group Policy* section in the Cisco ASA Series VPN CLI or ASDM Configuration Guide.

Ensure the private DNS servers specified do not overlap with the DNS servers configured for the client platform. If they do, name resolution may not function properly.

Step 2 Configure split-include tunneling:

On the **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Advanced > Split Tunneling** pane, choose the **Tunnel Network List Below** policy, and specify a **Network List** of addresses to be tunneled.

Step 3 On the **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Advanced > Split Tunneling** pane, uncheck **Send All DNS lookups through tunnel**, and specify the names of the domains whose queries will be tunneled in **DNS Names**.

What to do next

After making changes to the group policy in ASDM, be sure the group policy is associated with a Connection Profile in **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Group Policy**.

Configure Split DNS for Split Exclude Tunneling

To configure split DNS for split exclude tunneling in the group policy, do the following:

Procedure

Step 1 In ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes** to configure a new custom attribute type. Choose **Add** and set the following in the Create Custom Attribute pane:

a) Enter **split-dns-exclude-domains** as the new type.
b) Optionally, enter a description.

Step 2 To configure a new custom attribute name for the created type, choose **Add** and set the following in the Create Custom Attribute Name pane:

a) Choose **split-dns-exclude-domains** for the type.
b) Enter a name.
c) For the value, enter a comma-separated list of domain names whose queries should not be tunneled. The client accepts up to 300 such domains. Wildcards are not supported.

Step 3 Choose **Add** and set the following in the Create Custom Attribute pane:

a) Choose the *type* created in step 1 for the Attribute Type field.
b) Choose the *name* created in step 2 for the Value field.

Step 4 Configure at least one VPN DNS server.

See the *Configure Server Attributes for an Internal Group Policy* section in the Cisco ASA Series VPN CLI or ASDM Configuration Guide.

Ensure the private DNS servers specified do not overlap with the DNS servers configured for the client platform. If they do, name resolution may not function properly.

Step 5 Configure split exclude or dynamic split exclude tunneling.

On the **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Advanced > Split Tunneling** pane, choose the **Exclude Network List Below** policy, and specify a Network List of addresses to be excluded.

See Configure Dynamic Split Exclude Tunneling, on page 142 for additional information. Dynamic split exclude configurations with split include tunneling are not supported.

Step 6 On the **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Advanced > Split Tunneling** pane, uncheck **Send All DNS lookups through tunnel**.

What to do next

After making changes to the group policy in ASDM, be sure the group policy is associated with a Connection Profile in **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Group Policy**.

Verify Split DNS Using Cisco Secure Client Logs

To verify if split-DNS is enabled, search the Cisco Secure Client logs for an entry containing "Received VPN Session Configuration Settings." There are separate log entries for IPv4 and IPv6 split DNS.

- For split DNS exclude:
  - IPv4 split DNS: 5 excluded domains
  - IPv6 split DNS: 5 excluded domains
- For split DNS include:
  - IPv4 split DNS: 5 included domains
  - IPv6 split DNS: 5 included domains

Manage VPN Authentication

Important Security Considerations

We do not recommend using a self-signed certificate on your secure gateway

- because of the possibility that a user could inadvertently configure a browser to trust a certificate on a rogue server, and
- because of the inconvenience to users of having to respond to a security warning when connecting to your secure gateway.

We strongly recommend that you enable Strict Certificate Trust for the Cisco Secure Client client. To configure **Strict Certificate Trust**, see the *Local Policy Parameters and Values* section: Local Policy Preferences, on page 100.

Supported Security Types

Cisco Secure Client supports RSA and ECDSA certificates for both server certificate verification and for client certificate authentication.

- **RSA Certificates**

  Cisco Secure Client supports RSA certificates with the following properties:

  - Key length of 2048, 4096, or 8192 bits
  - Hash algorithms MD5*, SHA1, SHA256, SHA384, or SHA512

    * RSA certificates that use the MD5 hash are not supported when Cisco Secure Client is operating in FIPS mode.

- **ECDSA Certificates**

  Cisco Secure Client supports ECDSA certificates with the following properties:

  - Key lengths of 256, 384, or 521 bits. These correspond to the NIST P-256, P-384, and P-521 elliptic curves respectively.

- **EdDSA Certificates**

  Cisco Secure Client relies on the Windows and macOS operating systems to establish trust and perform signing operations using digital certificates. Since these operating systems do not yet support EdDSA certificates, Cisco Secure Client also cannot support them.

Configure Server Certificate Handling

Server Certificate Verification

- The certificate must meet the minimum key size noted above and be one of the support types (RSA or ECDSA).
- (Windows only) For both SSL and IPsec VPN connections, you have the option to perform Certificate Revocation List (CRL) checking. When enabled in the profile editor, Cisco Secure Client retrieves the updated CRL for all certificates in the chain. It 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, it does not connect. Refer to Local Policy Preferences, on page 100 for further information.
- When a user connects to a Secure Firewall ASA that is configured with a server certificate, the checkbox to trust and import that certificate will still display, even if there is a problem with the trust chain (Root, Intermediate, etc.) If there are any other certificate problems, that checkbox will not display.
- SSL connections being performed via FQDN do not make a secondary server certificate verification with the FQDN's resolved IP address for name verification if the initial verification using the FQDN fails.
- The date and time (as reported by the operating system) at which verification is being performed must be after the certificate's Valid From date and before the Valid To date.
- Although not recommended, server certificates do not require a Key Usage (KU) or an Extended Key Usage (EKU) to be accepted. However, if the fields are present (which is most common), the following conditions apply:

For SSL and IPsec (both RSA and ECDSA certificates), any KU field must contain DigitalSignature. For RSA certificates, the KU must also contain KeyEncipherment or KeyAgreement.

For IPsec VPN, any EKU field must contain ServerAuth or IkeIntermediate.

- IPsec and SSL connections perform name verification on server certificates. The following rules are applied for the purposes of IPsec and SSL name verification:
  - If a Subject Alternative Name extension is present with relevant attributes, name verification is performed solely against the Subject Alternative Name. Relevant attributes include DNS Name attributes for all certificates, and additionally include IP address attributes if the connection is being performed to an IP address.
  - If a Subject Alternative Name extension is not present, or is present but contains no relevant attributes, name verification is performed against any Common Name attributes found in the Subject of the certificate.
  - If a certificate uses a wildcard for the purposes of name verification, the wildcard must be in the first (left-most) subdomain only, and additionally must be the last (right-most) character in the subdomain. Any wildcard entry not in compliance is ignored for the purposes of name verification.
- For macOS, expired certificates are displayed only when Keychain Access is configured to "Show Expired Certificates." Expired certificates are hidden by default, which may confuse users.

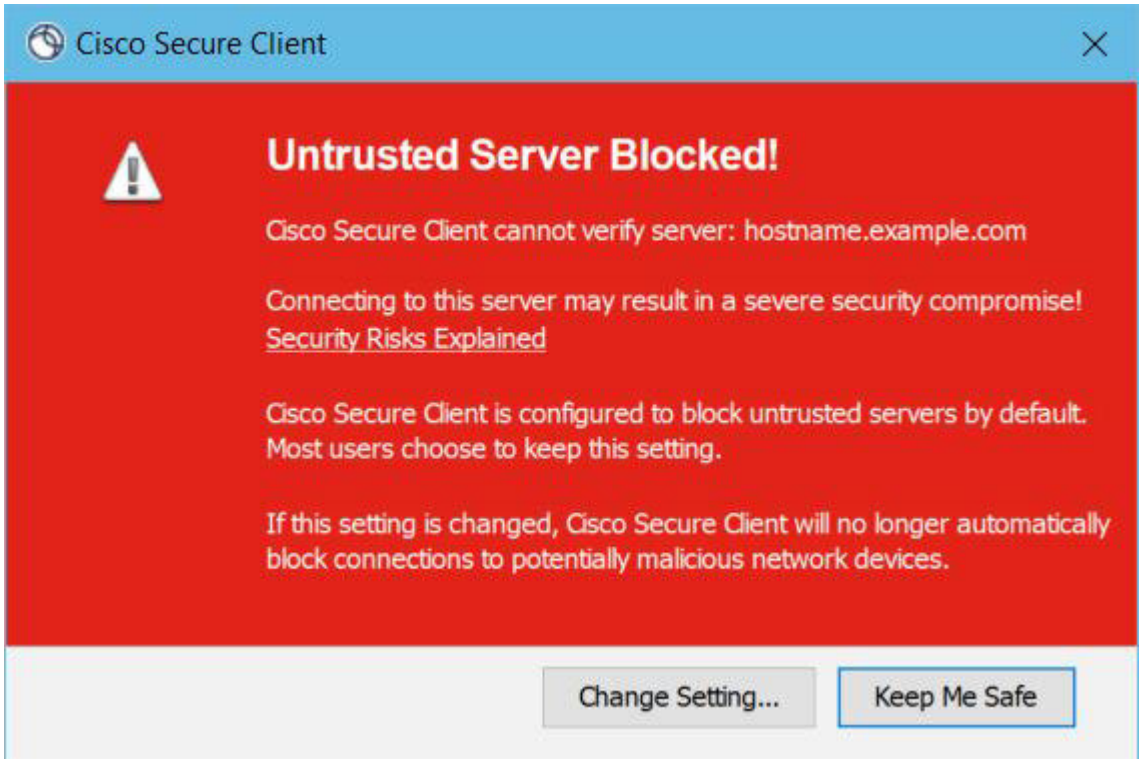
Invalid Server Certificate Handling

In response to the increase of targeted attacks against mobile users on untrusted networks, we have improved the security protections in the client to help prevent serious security breaches. The default client behavior has been changed to provide an extra layer of defense against Man-in-the-middle attacks.

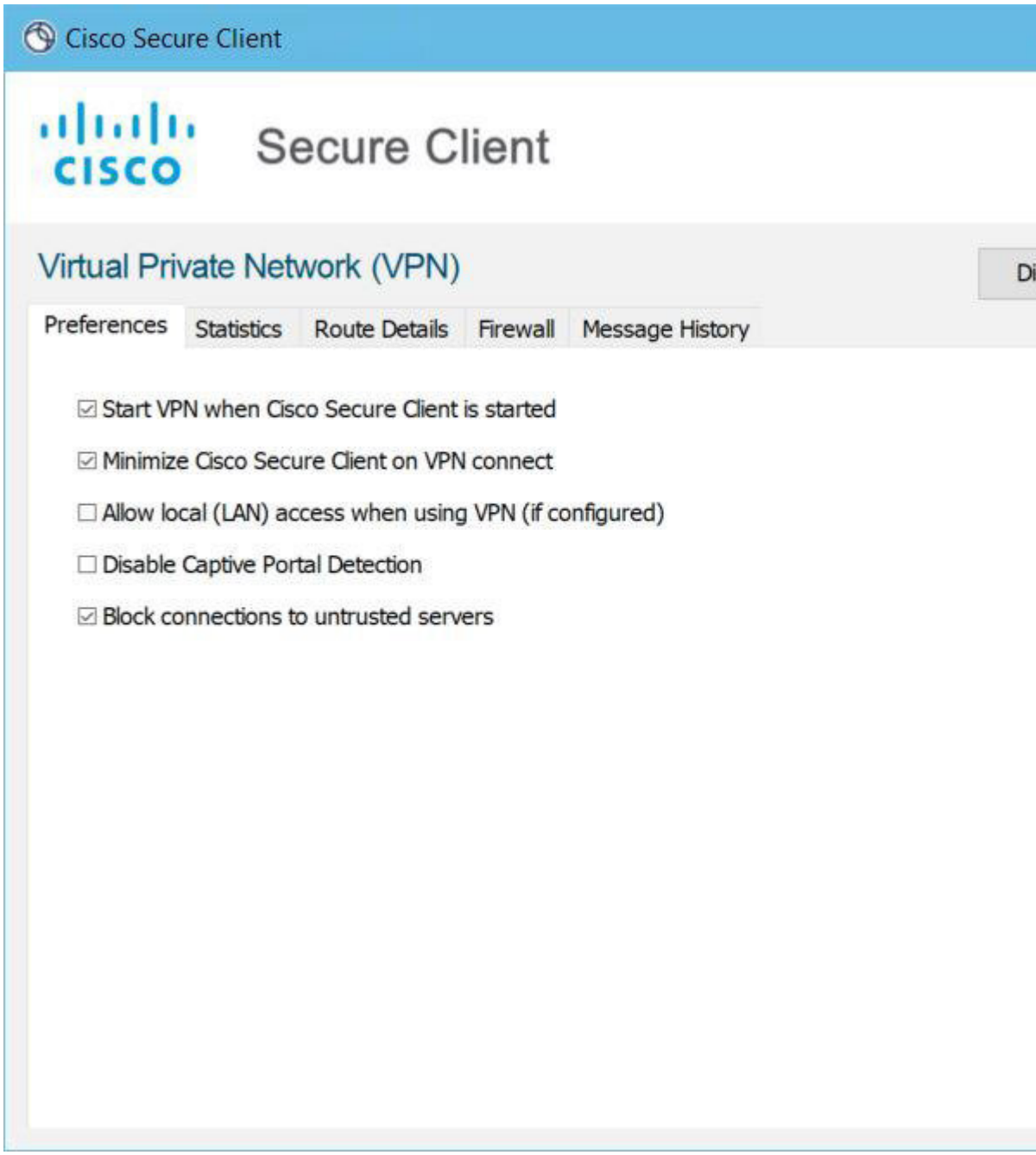
User Interaction

When the user tries to connect to a secure gateway, and there is a certificate error (due to expired, invalid date, wrong key usage, or CN mismatch), the user sees a red-colored dialog with Change Settings and Keep Me Safe buttons.

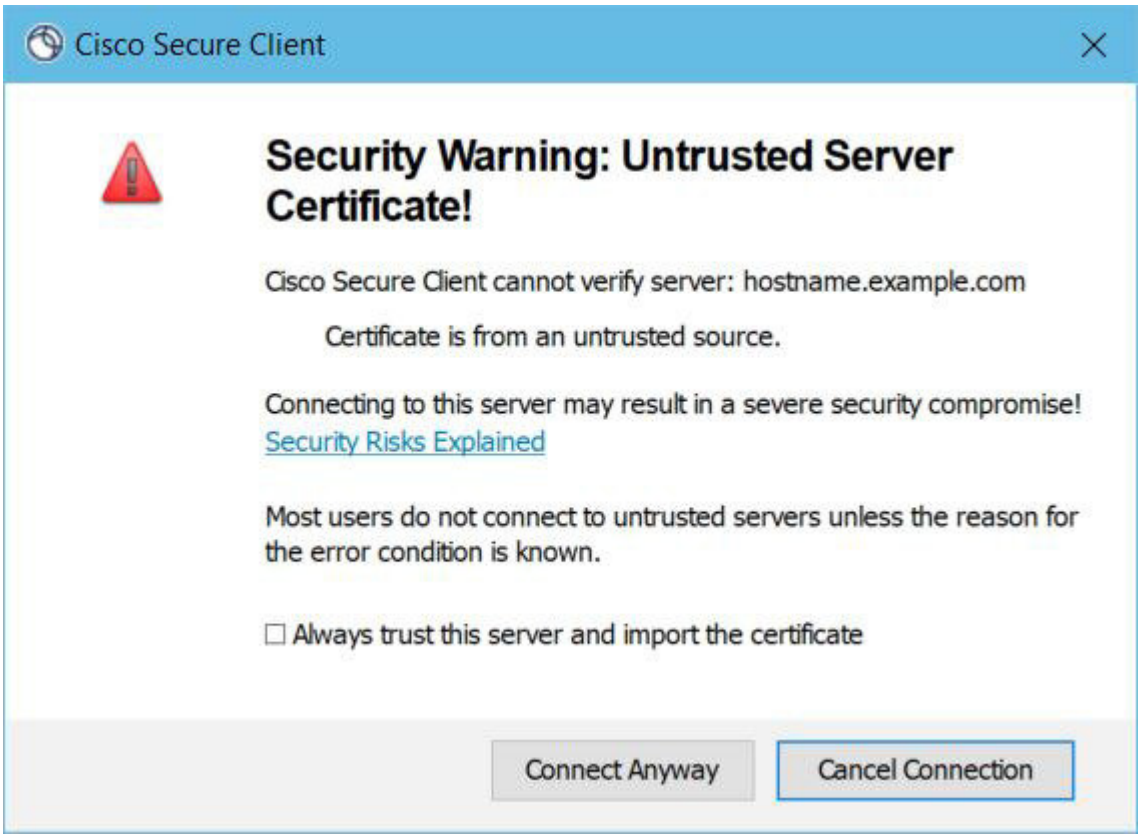
Note The dialogs for Linux may look different from the ones shown in this document.



- Clicking **Keep Me Safe** cancels the connection.
- Clicking **Change Settings** opens the Cisco Secure Client Advanced > VPN >Preferences dialog, where the user can enable connections to untrusted servers. The current connection attempt is canceled.



If the user un-checks **Block connections to untrusted servers**, and the only issue with the certificate is that the CA is untrusted, then the next time the user attempts to connect to this secure gateway, the user will not see the Certificate Blocked Error Dialog dialog.



If the user checks **Always trust this VPN server and import the certificate**, then future connections to this secure gateway will not prompt the user to continue.

Note If the user checks **Block connections to untrusted servers** in **Cisco Secure Client Advanced > VPN > Preferences**, or if the user's configuration meets one of the conditions in the list of the modes described under the guidelines and limitations section, then Cisco Secure Client rejects invalid server certificates and connections to untrusted servers, regardless of whether the Strict Certificate Trust option in the Profile Editor is enabled.

Improved Security Behavior

When the client accepts an invalid server certificate, that certificate is saved in the client's certificate store. Previously, only the thumbprint of the certificate was saved. Note that invalid certificates are saved only when the user has elected to always trust and import invalid server certificates.

There is no administrative override to make the end user less secure automatically. To completely remove the preceding security decisions from your end users, enable **Strict Certificate Trust** in the user's local policy file. When Strict Certificate Trust is enabled, the user sees an error message, and the connection fails; there is no user prompt.

For information about enabling Strict Certificate Trust in the local policy file, see the Local Policy Preferences, on page 100.

Guidelines and Limitations

Invalid server certificates are rejected when:

- Always On is enabled in the Cisco Secure Client profile and is not turned off by an applied group policy or DAP.
- The client has a Local Policy with Strict Certificate Trust enabled.
- Cisco Secure Client Start Before Login is configured.
- A client certificate from the machine certificate store is used for authentication.

Configure Certificate-Only Authentication

You can specify whether you want users to authenticate using Secure Firewall ASA with a username and password or using a digital certificate (or both). When you configure certificate-only authentication, users can connect with a digital certificate and are not required to provide a user ID and password.

To support certificate-only authentication in an environment where multiple groups are used, you may provision more than one group-url. Each group-url would contain a different client profile with some piece of customized data that would allow for a group-specific certificate map to be created. For example, the Department_OU value of Engineering could be provisioned on the Secure Firewall ASA to place the user in this group when the certificate from this process is presented to the Secure Firewall ASA.



Note The certificate used to authenticate the client to the secure gateway must be valid and trusted (signed by a CA). A self-signed client certificate will not be accepted.

Procedure

Step 1 Go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Connection Profiles**. Select a connection profile and click Edit. The Edit AnyConnect Connection Profile window opens.

Step 2 If it is not already, click the **Basic** node of the navigation tree on the left pane of the window. In the right pane of the window, in the **Authentication** area, enable the method **Certificate**.

Step 3 Click **OK** and apply your changes.

Configure Certificate Enrollment

The Cisco Secure Client uses the Simple Certificate Enrollment Protocol (SCEP) to provision and renew a certificate as part of client authentication. Certificate enrollment using SCEP is supported by Cisco Secure Client IPsec and SSL VPN connections to the Secure Firewall ASA in the following ways:

- SCEP Proxy: The Secure Firewall ASA acts as a proxy for SCEP requests and responses between the client and the Certificate Authority (CA).
  - The CA must be accessible to the Secure Firewall ASA, not Cisco Secure Client, since the client does not access the CA directly.

- Enrollment is always initiated automatically by the client. No user involvement is necessary.

SCEP Proxy Enrollment and Operation

The following steps describe how a certificate is obtained and a certificate-based connection is made when Cisco Secure Client and the Secure Firewall ASA are configured for SCEP Proxy.

1. The user connects to the Secure Firewall ASA headend using a connection profile configured for both certificate and AAA authentication. The Secure Firewall ASA requests a certificate and AAA credentials for authentication from the client.
2. The user enters his/her AAA credentials, but a valid certificate is not available. This situation triggers the client to send an automatic SCEP enrollment request after the tunnel has been established using the entered AAA credentials.
3. The Secure Firewall ASA forwards the enrollment request to the CA and returns the CA's response to the client.
4. If SCEP enrollment is successful, the client presents a (configurable) message to the user and disconnects the current session. The user can now connect using certificate authentication to the Secure Firewall ASA tunnel group.

   If SCEP enrollment fails, the client displays a (configurable) message to the user and disconnects the current session. The user should contact his/her administrator.

Other SCEP Proxy operational considerations:

- If configured to do so, the client automatically renews the certificate before it expires, without user intervention.
- SCEP Proxy enollment uses SSL for both SSL and IPsec tunnel certificate authentication.

Certificate Authority Requirements

- All SCEP-compliant CAs, including IOS CS, Windows Server 2003 CA, and Windows Server 2008 CA, are supported.
- The CA must be in auto-grant mode; polling for certificates is not supported.
- You can configure some CAs to email users an enrollment password for an additional layer of security. The CA password is the challenge password or token that is sent to the certificate authority to identify the user. The password can then be configured in the Cisco Secure Client profile, which becomes part of SCEP request that the CA verifies before granting the certificate.

Guidelines for Certificate Enrollment

- Secure Firewall ASA load balancing is supported with SCEP enrollment.
- The Secure Firewall ASA does not indicate why an enrollment failed, although it does log the requests received from the client. Connection problems must be debugged on the CA or the client.
- Certificate-Only Authentication and Certificate Mapping on the Secure Firewall ASA:

  To support certificate-only authentication in an environment where multiple groups are used, you may provision more than one group-url. Each group-url would contain a different client profile with some

piece of customized data that would allow for a group-specific certificate map to be created. For example, the Department_OU value of Engineering could be provisioned on the Secure Firewall ASA to place the user in this tunnel group when the certificate from this process is presented to the Secure Firewall ASA.

- Identifying Enrollment Connections to Apply Policies:

  On the Secure Firewall ASA, the aaa.cisco.sceprequired attribute can be used to catch the enrollment connections and apply the appropriate policies in the selected DAP record.

- Windows Certificate Warning:

  When Windows clients first attempt to retrieve a certificate from a certificate authority they may see a warning. When prompted, users must click Yes. This allows them to import the root certificate. It does not affect their ability to connect with the client certificate.

Configure SCEP Proxy Certificate Enrollment

Configure a VPN Client Profile for SCEP Proxy Enrollment

Procedure

Step 1 Open the VPN Profile Editor and choose **Certificate Enrollment** from the navigation pane.

Step 2 Select **Certificate Enrollment**.

Step 3 Configure the **Certificate Contents** to be requested in the enrollment certificate. For definitions of the certificate fields, see AnyConnect Profile Editor, Certificate Enrollment .

Note

- If you use %machineid%, then Secure Firewall Posture must be loaded for the desktop client.
- For mobile clients, at least one certificate field must be specified.

Configure the Secure Firewall ASA to Support SCEP Proxy Enrollment

For SCEP Proxy, a single Secure Firewall ASA connection profile supports certificate enrollment and the certificate authorized VPN connection.

Procedure

Step 1 Create a group policy, for example, cert_group. Set the following fields:

- On General, enter the URL to the CA in **SCEP Forwarding URL**.
- On the Advanced > Cisco Secure Client pane, uncheck **Inherit** for Client Profiles to Download and specify the client profile configured for SCEP Proxy. For example, specify the ac_vpn_scep_proxy client profile.

Step 2 Create a connection profile for certificate enrollment and certificate authorized connection, for example, cert_tunnel.

- Authentication: Both (AAA and Certificate).

- Default Group Policy: cert_group.
- On Advanced > General, check **Enable SCEP Enrollment for this Connction Profile**.
- On Advanced > GroupAlias/Group URL, create a Group URL containing the group (cert_group) for this connection profile.

Set Up a Windows 2012 Server Certificate Authority for SCEP

If your Certificate Authority software is running on a Windows 2012 server, you may need to make one of the following configuration changes to the server to support SCEP with Cisco Secure Client.

Disable the SCEP Password on the Certificate Authority

The following steps describe how to disable the SCEP challenge password, so that clients will not need to provide an out-of-band password before SCEP enrollment.

Procedure

Step 1 On the Certificate Authority server, launch the Registry Editor. You can do this by selecting **Start** > **Run**, typing **regedit**, and clicking **OK**.

Step 2 Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword.

If the EnforcePassword key does not exist, create it as a new Key.

Step 3 Edit EnforcePassword, and set it to '0'. If it does not exist, create it as a REG-DWORD.

Step 4 Exit regedit, and reboot the certificate authority server.

Setting the SCEP Template on the Certificate Authority

The following steps describe how to create a certificate template, and assign it as the default SCEP template.

Procedure

Step 1 Launch the Server Manager. You can do this by selecting Start > Admin Tools > Server Manager.

Step 2 Expand Roles > Certificate Services (or AD Certificate Services).

Step 3 Navigate to CA Name > Certificate Templates.

Step 4 Right-click **Certificate Templates > Manage**.

Step 5 From the Cert Templates Console, right-click User template and choose **Duplicate**

Step 6 Choose **Windows Server 2012 version** for new template, and click **OK**.

Step 7 Change the template display name to something descriptive, such as NDES-IPSec-SSL.

Step 8 Adjust the Validity Period for your site. Most sites choose three or more years to avoid expired certificates.

Step 9 On the Cryptography tab, set the minimum key size for your deployment.

Step 10 On the Subject Name tab, select **Supply in Request**.

Step 11 On the Extensions tab, set the Application Policies to include at least:

- Client Authentication
- IP security end system
- IP security IKE intermediate
- IP security tunnel termination
- IP security user

These values are valid for SSL or IPsec.

Step 12 On the Security tab, ensure to grant enrollment permissions to only desired user group(s).

Step 13 Click **Apply**, then **OK** to save new template.

Step 14 From Server manager > Certificate Services-CA Name, right-click Certificate Templates. Select New > Certificate Template to Issue, select the new template you created (in this example, NDES-IPSec-SSL), and click **OK**.

Step 15 Edit the registry. You can do this by selecting Start > Run, regedit, and clicking **OK**.

Step 16 Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP.

Step 17 Set the value of the following three keys to **NDES-IPSec-SSL**.

- EncryptionTemplate
- GeneralPurposeTemplate
- SignatureTemplate

Step 18 Click **Save**, and reboot the certificate authority server.

Configure a Certificate Expiration Notice

Configure Cisco Secure Client to warn users that their authentication certificate is about to expire. The **Certificate Expiration Threshold** setting specifies the number of days before the certificate's expiration date. Cisco Secure Client uses the threshold to determine when to warn users that their certificate is expiring. Cisco Secure Client warns the user upon each connect until the certificate has actually expired or a new certificate has been acquired.

Note The Certificate Expiration Threshold feature cannot be used with RADIUS.

Procedure

Step 1 Open the Cisco Secure Client Profile Editor - VPN and choose **Certificate Enrollment** from the navigation pane.

Step 2 Select **Certificate Enrollment.**

Step 3 Specify a **Certificate Expiration Threshold**.

This threshold is the number of days before the certificate's expiration date. Cisco Secure Client uses the threshold to determine when to warn users that their certificate is expiring.

The default is 0 (no warning displayed). The range is 0 to 180 days.

Step 4 Click **OK**.

Configure Certificate Selection

The following steps show all the places in the Cisco Secure Client profiles where you configure how certificates are searched for and how they are selected on the client system. None of the steps are required, and if you do not specify any criteria, Cisco Secure Client uses default key matching.

Cisco Secure Client reads the browser certificate stores on Windows. For Linux, you must create a Privacy Enhanced Mail (PEM) formatted file store. For macOS, you may use a Privacy Enhanced Mail (PEM) formatted file store or the Keychain.

Procedure

Step 1 Windows and macOS:Configure Which Certificate Stores to Use, on page 158

Specify which certificate stores are used by Cisco Secure Client in the VPN client profile.

Step 2 Windows Only: Prompt Windows Users to Select Authentication Certificate, on page 160

Configure Cisco Secure Client to present a list of valid certificates to users and let them choose the certificate to authenticate the session.

Step 3 For macOS and Linux environments: Create a PEM Certificate Store for macOS and Linux, on page 161

Step 4 For macOS and Linux environments: Select which certificate stores to exclude in the VPN Local Policy profile.

Step 5 Configure Certificate Matching, on page 162

Configure keys that Cisco Secure Client tries to match, when searching for a certificate in the store. You can specify keys, extended keys, and add custom extended keys. You can also specify a pattern for the value of an operator in a distinguished name for Cisco Secure Client to match.

Configure Which Certificate Stores to Use

For Windows, macOS, and Linux, separate certificate stores are provided for Cisco Secure Client to use in the VPN client profile. You can have single or multiple certificate authentication combinations and can configure the secure gateway to dictate to the client which one of the multiple certificate authentication choices is acceptable for a particular VPN connection. For example, on macOS, if you set ExcludePemFileCertStore to *true* in the local policy file (to force Cisco Secure Client to use only native Keychain certificate stores) and also set the profile-based certificate store to Login (to force Cisco Secure Client to use only certificate stores such as User Login and dynamic smartcard Keychains, plus the user PEM file store), the combined filtering results in Cisco Secure Client using strictly the User Login Keychain certificate store.

For Windows, users with administrative privileges on the computer have access to both certificate stores. Users without administrative privileges only have access to the user certificate store. Usually, Windows users

do not have administrative privileges. Choosing **Windows Certificate Store Override** allows Cisco Secure Client to access the machine store, even when the user does not have administrative privileges.



Note Access-control for the machine store can vary depending on the Windows version and security settings. Because of this, the user may be unable to use certificates in the machine store even though they have administrative privileges. In this case, select **Certificate Store Override** to allow machine store access.

The following table describes how Cisco Secure Client searches for certificates on a client based on what **Certificate Store** is searched, and whether **Windows Certificate Store Override** is checked.

Certificate Store Setting	Certificate Store Override Setting	Cisco Secure Client Search Strategy
All (for Windows)	false	Cisco Secure Client searches all certificate stores. Cisco Secure Client is not allowed to access the machine store when the user does not have administrative privileges. This setting is the default. This setting is appropriate for most cases. Do not change this setting unless you have a specific reason or scenario requirement to do so.
All (for Windows)	true	Cisco Secure Client searches all certificate stores. Cisco Secure Client is allowed to access the machine store when the user does not have administrative privileges.
Machine (for Windows)	true	Cisco Secure Client searches in machine certificate store only. Cisco Secure Client is allowed to access the machine store when the user does not have administrative privileges.
User (for Windows)	does not apply	Cisco Secure Client searches in the user certificate store only. The certificate store override is not applicable because users without administrative rights can have access to this certificate store.
All (for macOS)	does not apply	Cisco Secure Client uses certificates from all available macOS keychains and file stores.
System (for macOS)	does not apply	Cisco Secure Client uses certificates only from the macOS system keychain and system file/PEM store.
Login (for macOS)	does not apply	Cisco Secure Client uses certificates only from the macOS login and dynamic smartcard keychains, as well as the user file/PEM store.
All (for Linux)	does not apply	Cisco Secure Client uses client certificates from both system and user PEM file stores, as well as the user Firefox NSS store.
Machine (for Linux)	does not apply	Cisco Secure Client uses client certificate stores only from the system PEM file store.
User (for Linux)	does not apply	Cisco Secure Client uses client certificates only from the user PEM file store, as well as the user Firefox NSS store.

With Multiple Certificate Authentication

Before you begin

- Only supported on desktop platforms (Windows, macOS, and Linux).
- You must have *AutomaticCertSelection* enabled in the VPN profile.
- The certificate matching configuration you set in the VPN profile limits the certificates available for multiple certificate authentication.



Note SCEP is not supported.

Procedure

Step 1 Set **Certificate Store**:

- For one machine and one user certificate, set to **All** in the VPN profile and enable *CertficateStoreOverride* as described in Step 2 for Windows platform.
- For two user certificates, set to either **All** or **User/Login** in the VPN profile but keep *CertificateStoreOverride* as described in Step 2 for Windows platform.

Step 2 Choose **Windows Certificate Store Override** if you want to allow Cisco Secure Client to search the machine certificate store when users do not have administrative privileges.

With Basic Certificate Authentication

Procedure

Step 1 Set **Certificate Store**.

- All—(Default) Directs Cisco Secure Client to use all certificate stores for locating certificates.
- Machine/System—Directs Cisco Secure Client to restrict certificate lookup to the local machine/system level certificate store.
- User/Login—Directs Cisco Secure Client to restrict certificate lookup to the local user certificate stores.

Step 2 Choose **Windows Certificate Store Override** if you want to allow Cisco Secure Client to search the machine certificate store when users do not have administrative privileges.

Prompt Windows Users to Select Authentication Certificate

You can configure Cisco Secure Client to present a list of valid certificates to users and let them choose the certificate to authenticate the session. An expired certificate is not necessarily considered invalid. For example,

if you are using SCEP, the server might issue a new certificate to the client. Eliminating expired certificates might keep a client from connecting at all; thus requiring manual intervention and out-of-band certificate distribution. Cisco Secure Client only restricts the client certificate based on security-related properties, such as key usage, key type and strength, and so on, based on configured certificate matching rules. This configuration is available only for Windows. By default, user certificate selection is disabled.

Procedure

Step 1 Open the Cisco Secure Client Profile Editor - VPN **Preferences (Part 2)** from the navigation pane.

Step 2 To enable certificate selection, uncheck **Disable Certificate Selection**.

Step 3 Uncheck **User Controllable**, unless you want users to be able to turn automatic certificate selection on and off in the **Advanced** > **VPN** > **Preferences** pane.

Create a PEM Certificate Store for macOS and Linux

Cisco Secure Client supports certificate retrieval from a Privacy Enhanced Mail (PEM) formatted file store. Cisco Secure Client reads PEM-formatted certificate files from the file system on the remote computer, verifies, and signs them.

Before you begin

In order for the client to acquire the appropriate certificates under all circumstances, ensure that your files meet the following requirements:

- All certificate files must end with the extension .pem or .crt.
- All private key files must end with the extension .key.
- A client certificate and its corresponding private key must have the same filename. For example: client.pem and client.key.

Tip Instead of keeping copies of the PEM files, you can use soft links to PEM files.

To create the PEM file certificate store, create the paths and folders listed below. Place the appropriate certificates in these folders:

PEM File Certificate Store Folders	Type of Certificates Stored
~/.cisco/certificates/ca **Note** .cisco/ is located in the home directory.	Trusted CA and root certificates
~/.cisco/certificates/client	Client certificates
~/.cisco/certificates/client/private	Private keys

Machine certificates are the same as PEM file certificates, except for the root directory. For machine certificates, substitute /opt/.cisco for ~/.cisco. Otherwise, the paths, folders, and types of certificates listed apply. Cisco Secure Client also uses system CA certificate location (/etc/ssl/certs) to verify server certificates.

Certificate Store for Server Certificate Verification

By default, Cisco Secure Client uses the PEM File certificate store, including system CA certificate location (/etc/ssl/certs) to verify server certificates. NSS certificate store could also be used for Cisco Secure Client to verify server certificates.

To Activate NSS Certificate Store

You can follow one of these options:

- Create folder: ~/.cisco/certificates/nssdb. Cisco Secure Client uses this path to store the NSS certificate database. You can create this folder with OnConnect script.
- Let Cisco Secure Client search and use the NSS certificate database inside Firefox default profile for the current user. Firefox installed via Snap or Flatpak is not supported.

If you have never launched the installed Firefox browser, you must first launch it in order to let Firefox generate the default profile.

If You Do Not Use the NSS Certificate Store

You must configure the local policy to exclude the Firefox NSS certificate store and must keep the PEM File certificate store enabled.

Multiple Module Requirement

If you deploy the core client plus one or more optional modules, you must apply the lockdown property to each of the installers.

This action is available for the VPN installer, Network Access Manager, Network Visibility Module, and Umbrella Roaming Security Module.



Note If you choose to activate lockdown to the VPN installer, you will consequently be locking down Cisco Secure Endpoint as well.

Configure Certificate Matching

Cisco Secure Client can limit its search of certificates to those certificates that match a specific set of keys. Certificate matchings are global criteria that are set in an Cisco Secure Client VPN profile, in the **Certificate Matching** pane. The criteria are:

- Key Usage
- Extended Key Usage
- Distinguished Name

Configure Key Usage

Selecting the **Key Usage** keys limits the certificates that Cisco Secure Client can use to those certificates that have at least one of the selected keys. The supported set is listed in the **Key Usage** list on the VPN client profile, and it includes:

- DECIPHER_ONLY
- ENCIPHER_ONLY
- CRL_SIGN
- KEY_CERT_SIGN
- KEY_AGREEMENT
- DATA_ENCIPHERMENT
- KEY_ENCIPHERMENT
- NON_REPUDIATION
- DIGITAL_SIGNATURE

If one or more criteria are specified, a certificate must match at least one to be considered a matching certificate.

Configure Extended Key Usage

Selecting the **Extended Key Usage** keys limits the certificates that Cisco Secure Client can use to the certificates that have these keys. The following table lists the well-known set of constraints with their corresponding object identifiers (OIDs).

Constraint	OID
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	1.3.6.1.5.5.8.2.2

Configure Custom Extended Match Key

All other OIDs (such as 1.3.6.1.5.5.7.3.11, used in some examples in this document) are considered "custom." As an administrator, you can add your own OIDs if the OID that you want is not in the well-known set.

Configure Certificate Distinguished Name

The **Distinguished Name** table contains certificate identifiers that limit the certificates that the client can use to the certificates that match the specified criteria and criteria match conditions. Click the **Add** button to add criteria to the list and to set a value or wildcard to match the contents of the added criteria.

Identifier	Description
CN	SubjectCommonName
SN	SubjectSurName
GN	SubjectGivenName
N	SubjectUnstructName
I	SubjectInitials
GENQ	SubjectGenQualifier
DNQ	SubjectDnQualifier
C	SubjectCountry
L	SubjectCity
SP	SubjectState
ST	SubjectState
O	SubjectCompany
OU	SubjectDept
T	SubjectTitle
EA	SubjectEmailAddr
DC	DomainComponent
ISSUER-CN	IssuerCommonName
ISSUER-SN	IssuerSurName
ISSUER-GN	IssuerGivenName
ISSUER-N	IssuerUnstructName
ISSUER-I	IssuerInitials
ISSUER-GENQ	IssuerGenQualifier

Identifier	Description
ISSUER-DNQ	IssuerDnQualifier
ISSUER-C	IssuerCountry
ISSUER-L	IssuerCity
ISSUER-SP	IssuerState
ISSUER-ST	IssuerState
ISSUER-O	IssuerCompany
ISSUER-OU	IssuerDept
ISSUER-T	IssuerTitle
ISSUER-EA	IssuerEmailAddr
ISSUER-DC	IssuerDomainComponent

Distinguished Name can contain zero or more matching criteria. A certificate must match all specified criteria to be considered a matching certificate. **Distinguished Name** matching specifies that a certificate must or must not have the specified string, and whether wild carding for the string is allowed.

VPN Authentication Using SAML

You can use SAML 2.0 integrated with Secure Firewall ASA release 9.7.1 (and later) for initial session authentication. An enhanced version of SAML integration was later introduced which replaces the native (external) browser integration with an embedded browser. When connecting to a tunnel group configured for SAML authentication, Cisco Secure Client opens an embedded browser window to complete the authentication process. Every SAML attempt uses a new browser session, and the browser session is specific to Cisco Secure Client (the session state is not shared with any other browsers). Although each SAML authentication attempt starts with no session state, permanent cookies persist between attempts.

Secure Firewall ASA release 9.17.1 (and later) /ASDM release 7.17.1 (and later) introduced support for VPN SAML external browser with Cisco Secure Client. When you use SAML as the primary authentication method for the Cisco Secure Client VPN connection profile, you can choose for Cisco Secure Client to use a local browser, instead of the embedded browser, when performing web authentication. With this feature, Cisco Secure Client supports WebAuthN and any other SAML-based web authentication options, such asSingleSign On, biometric authentication, or other enhanced methods that are unavailable with the embedded browser. For SAML external browser use, you must perform the configuration described in the *Configure Default OS Browser for SAML Authentication* section of the Cisco ASA Series VPN CLI Configuration Guide, 9.17.

Platform Specific Requirements

You must meet the following system requirements in order to use SAML with an embedded browser:

- Windows—Windows 7 (and later), Internet Explorer 11 (and later)
- macOS—macOS 10.10 (or later) (Cisco Secure Client officially supports macOS 10.11 or later)
- Linux—WebKitGTK+ 2.1x (or later), official packages for Red Hat 7.4 (or later) and Ubuntu 16.04 (or later)

Upgrade Process

Cisco Secure Client SAML 2.0 with a native (external) browser is available with Secure Firewall ASA release 9.7.x, 9.8.x, and 9.9.1. The enhanced Cisco Secure Client version with embedded browser is available with Secure Firewall ASA 9.7.1.24 (or later), 9.8.2.28 (or later), or 9.9.2.1 (or later).

When upgrading or deploying the headend or client devices with the embedded browser SAML integration, take note of these scenarios:

- *If you deploy Cisco Secure Client first*, both the native (external) browser and the embedded browser SAML integration function as expected without further action. An existing or an updated Secure Firewall ASA version is supported, even when you deploy Cisco Secure Client first.
- *If you deploy the updated Secure Firewall ASA version (with the embedded browser SAML integration) first*, you must in turn upgrade Cisco Secure Client. By default, the updated Secure Firewall ASA releases are not backward compatible with the native (external) browser SAML integration in previous releases. The upgrade for any existing Cisco Secure Client clients occurs after authentication and requires you to enable the **saml external-browser** command in tunnel group configuration.

Follow these guidelines when using SAML:

- If Always-On VPN is enabled, refer to Use Always-On VPN With External SAML Identity Provider, on page 117.
- Untrusted server certificates are not allowed in the embedded browser.
- The embedded browser SAML integration is not supported in CLI or SBL modes.
- (Mobile only) Single logout is not supported.
- SAML authentication established in a web browser is not shared with Cisco Secure Client and vice versa.
- Depending on the configuration, various methods are used when connecting to the headend with the embedded browser. For example, while Cisco Secure Client might prefer an IPv4 connection over an IPv6 connection, the embedded browser might prefer IPv6, or vice versa. Similarly, Cisco Secure Client may fall back to no proxy after trying proxy and getting a failure, while the embedded browser may stop navigation after trying proxy and getting a failure.
- You must synchronize Network Time Protocol (NTP) server on the Secure Firewall ASA with the IdP NTP server in order to use the SAML feature.
- The SAML IdP *NameID* attribute determines the user's username and is used for authorization, accounting, and VPN session database.
- You should set Auto Reconnect to *ReconnectAfterResume* in the Cisco Secure Client Profile Editor, Preferences (Part 1), on page 76 if you want users to re-authenticate with the Identity Provider (IdP) every time they establish a VPN session via SAML.
- Since Cisco Secure Client with the embedded browser uses a new browser session on every VPN attempt, users must re-authenticate every time, if the IdP uses HTTP session cookies to track logon state. In this case, the *Force Re-Authentication* setting in **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers** > has no effect on Cisco Secure Client initiated SAML authentication.

Refer to the latest release (9.7 or later) of the Cisco ASA Series VPN CLI or ASDM Configuration Guide for additional SAML configuration details.

VPN Authentication Using SDI Token (SoftID) Integration

Cisco Secure Client integrates support for RSA SecurID client software versions 1.1 and later running on Windows x86 (32-bit) and x64 (64-bit).

RSA SecurID software authenticators reduce the number of items a user has to manage for safe and secure access to corporate assets. RSA SecurID Software Tokens residing on a remote device generate a random one-time-use passcode that changes every 60 seconds. The term SDI stands for Security Dynamics, Inc. technology, which refers to this one-time password generation technology that uses hardware and software tokens.

Typically, users make the Cisco Secure Client connection by clicking the Cisco Secure Client icon in the tools tray, selecting the connection profile with which they wish to connect, and then entering the appropriate credentials in the authentication dialog box. The login (challenge) dialog box matches the type of authentication configured for the tunnel group to which the user belongs. The input fields of the login dialog box clearly indicate what kind of input is required for authentication.

For SDI authentication, the remote user enters a PIN (Personal Identification Number) into the Cisco Secure Client software interface and receives an RSA SecurID passcode. After the user enters the passcode into the secured application, the RSA Authentication Manager validates the passcode and allows the user to gain access.

Users who use RSA SecurID hardware or software tokens see input fields indicating whether the user should enter a passcode or a PIN, a PIN, or a passcode and the status line at the bottom of the dialog box provides further information about the requirements. The user enters a software token PIN or passcode directly into the Cisco Secure Client user interface.

The appearance of the initial login dialog box depends on the secure gateway settings: the user can access the secure gateway either through the main login page, the main index URL, a tunnel-group login page, or a tunnel group URL (URL/tunnel-group). To access the secure gateway via the main login page, the “Allow user to select connection” checkbox must be set in the Network (Client) Access AnyConnect Connection Profiles page. In either case, the secure gateway sends the client a login page. The main login page contains a drop-down list in which the user selects a tunnel group; the tunnel-group login page does not, since the tunnel-group is specified in the URL.

In the case of a main login page (with a drop-down list of connection profiles or tunnel groups), the authentication type of the default tunnel group determines the initial setting for the password input field label. For example, if the default tunnel group uses SDI authentication, the field label is “Passcode;” but if the default tunnel group uses NTLM authentication, the field label is “Password.” In Release 2.1 and later, the field label is not dynamically updated with the user selection of a different tunnel group. For a tunnel-group login page, the field label matches the tunnel-group requirements.

The client supports input of RSA SecurID Software Token PINs in the password input field. If the RSA SecurID Software Token software is installed and the tunnel-group authentication type is SDI, the field label is “Passcode” and the status bar states “Enter a username and passcode or software token PIN.” If a PIN is used, subsequent consecutive logins for the same tunnel group and username have the field label “PIN.” The client retrieves the passcode from the RSA SecurID Software Token DLL using the entered PIN. With each successful authentication, the client saves the tunnel group, the username, and authentication type, and the saved tunnel group becomes the new default tunnel group.

Cisco Secure Client accepts passcodes for any SDI authentication. Even when the password input label is “PIN,” the user may still enter a passcode as instructed by the status bar. The client sends the passcode to the secure gateway as is. If a passcode is used, subsequent consecutive logins for the same tunnel group and username have the field label “Passcode.”

The RSASecureIDIntegration profile setting has three possible values:

- Automatic—The client first attempts one method, and if it fails, the other method is tried. The default is to treat the user input as a token passcode (HardwareToken), and if that fails, treat it as a software token pin (SoftwareToken). When authentication is successful, the successful method is set as the new SDI Token Type and cached in the user preferences file. For the next authentication attempt, the SDI Token Type defines which method is attempted first. Generally, the token used for the current authentication attempt is the same token used in the last successful authentication attempt. However, when the username or group selection is changed, it reverts to attempting the default method first, as shown in the input field label.

Note The SDI Token Type only has meaning for the automatic setting. You can ignore logs of the SKI Token Type when the authentication mode is not automatic. HardwareToken as the default avoids triggering next token mode.

- SoftwareToken—The client always interprets the user input as a software token PIN, and the input field label is “PIN:.”
- HardwareToken—The client always interprets the user input as a token passcode, and the input field label is “Passcode:.”

Note Cisco Secure Client does not support token selection from multiple tokens imported into the RSA Software Token client software. Instead, the client uses the default selected via the RSA SecurID Software Token GUI.

Categories of SDI Authentication Exchanges

All SDI authentication exchanges fall into one of the following categories:

- Normal SDI Authentication Login
- New User mode
- New PIN mode
- Clear PIN mode
- Next Token Code mode

Normal SDI Authentication Login

A normal login challenge is always the first challenge. The SDI authentication user must provide a user name and token passcode (or PIN, in the case of a software token) in the username and passcode or PIN fields, respectively. The client returns the information to the secure gateway (central-site device), and the secure gateway verifies the authentication with the authentication server (SDI or SDI via RADIUS proxy).

If the authentication server accepts the authentication request, the secure gateway sends a success page back to the client, and the authentication exchange is complete.

If the passcode is not accepted, the authentication fails, and the secure gateway sends a new login challenge page, along with an error message. If the passcode failure threshold on the SDI server has been reached, then the SDI server places the token into next token code mode.

New User, Clear PIN, and New PIN Modes

The PIN can be cleared only on the SDI server and only by the network administrator.

In the New User, Clear PIN, and New PIN modes, Cisco Secure Client caches the user-created PIN or system-assigned PIN for later use in the “next passcode” login challenge.

Clear PIN mode and New User mode are identical from the point of view of the remote user and are both treated the same by the secure gateway. In both cases, the remote user either must enter a new PIN or be assigned a new PIN by the SDI server. The only difference is in the user response to the initial challenge.

For New PIN mode, the existing PIN is used to generate the passcode, as it would be in any normal challenge. For Clear PIN mode, no PIN is used at all for hardware tokens, with the user entering just a token code. A PIN of eight consecutive zeros (00000000) is used to generate a passcode for RSA software tokens. In either case, the SDI server administrator must inform the user of what, if any, PIN value to use.

Adding a new user to an SDI server has the same result as clearing the PIN of an existing user. In both cases, the user must either provide a new PIN or be assigned a new PIN by the SDI server. In these modes, for hardware tokens, the user enters just a token code from the RSA device. In either case, the SDI server administrator must inform the user of what, if any, PIN value to use.

Creating a New PIN

If there is no current PIN, the SDI server requires that one of the following conditions be met, depending on how the system is configured:

- The system must assign a new PIN to the user (Default)
- The user must create a new PIN
- The user can choose whether to create a PIN or have the system assign it

If the SDI server is configured to allow the remote user to choose whether to create a PIN or have the system assign a PIN, the login screen presents a drop-down list showing the options. The status line provides a prompt message.

For a system-assigned PIN, if the SDI server accepts the passcode that the user enters on the login page, then the secure gateway sends the client the system-assigned PIN. The client sends a response back to the secure gateway, indicating that the user has seen the new PIN, and the system continues with a “next passcode’ challenge.

If the user chooses to create a new PIN, Cisco Secure Client presents a dialog box on which to enter that PIN. The PIN must be a number from 4 to 8 digits long. Because the PIN is a type of password, anything the user enters into these input fields is displayed as asterisks.

With RADIUS proxy, the PIN confirmation is a separate challenge, subsequent to the original dialog box. The client sends the new PIN to the secure gateway, and the secure gateway continues with a “next passcode” challenge.

“Next Passcode” and “Next Token Code” Challenges

For a “next passcode” challenge, the client uses the PIN value cached during the creation or assignment of a new PIN to retrieve the next passcode from the RSA SecurID Software Token DLL and return it to the secure gateway without prompting the user. Similarly, in the case of a “next Token Code” challenge for a software token, the client retrieves the next Token Code from the RSA SecurID Software Token DLL.

Compare Native SDI with RADIUS SDI

The network administrator can configure the secure gateway to allow SDI authentication in either of the following modes:

- Native SDI refers to the native ability in the secure gateway to communicate directly with the SDI server for handling SDI authentication.
- RADIUS SDI refers to the process of the secure gateway performing SDI authentication using a RADIUS SDI proxy, which communicates with the SDI server.

Native SDI and RADIUS SDI appear identical to the remote user. Because the SDI messages are configurable on the SDI server, the message text on the Secure Firewall ASA must match the message text on the SDI server. Otherwise, the prompts displayed to the remote client user might not be appropriate for the action required during authentication. Cisco Secure Client might fail to respond, and authentication might fail.

RADIUS SDI challenges, with minor exceptions, essentially mirror native SDI exchanges. Since both ultimately communicate with the SDI server, the information needed from the client and the order in which that information is requested is the same.

During authentication, the RADIUS server presents access challenge messages to the Secure Firewall ASA. Within these challenge messages are reply messages containing text from the SDI server. The message text is different when the Secure Firewall ASA is communicating directly with an SDI server from when communicating through the RADIUS proxy. Therefore, in order to appear as a native SDI server to Cisco Secure Client, the Secure Firewall ASA must interpret the messages from the RADIUS server.

Also, because the SDI messages are configurable on the SDI server, the message text on the Secure Firewall ASA must match (in whole or in part) the message text on the SDI server. Otherwise, the prompts displayed to the remote client user may not be appropriate for the action required during authentication. Cisco Secure Client might fail to respond and authentication might fail.

Configure the Secure Firewall ASA to Support RADIUS/SDI Messages

To configure the Secure Firewall ASA to interpret SDI-specific RADIUS reply messages and prompt the Cisco Secure Client user for the appropriate action, you must configure a connection profile (tunnel group) to forward RADIUS reply messages in a manner that simulates direct communication with an SDI server. Users authenticating to the SDI server must connect over this connection profile.

Procedure

Step 1 Go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Connection Profiles**.

Step 2 Select the connection profile you want to configure to interpret SDI-specific RADIUS reply messages and click **Edit**.

Step 3 In the **Edit AnyConnect Connection Profile** window, expand the Advanced node in the navigation pane on the left and select **Group Alias / Group URL.**

Step 4 Check **Enable the display of SecurID messages on the login screen**.

Step 5 Click **OK**.

Step 6 Choose **Configuration** > **Remote Access VPN** > **AAA/Local Users** > **AAA Server Groups**.

Step 7 Click **Add** to Add a AAA Server group.

Step 8 Configure the AAA server group in the Edit AAA Server Group dialog and click **OK**.

Step 9 In the **AAA Server Groups** area, select the AAA server group you just created and then click **Add** in the **Servers in the Selected Group** area.

Step 10 In the SDI Messages area, expand the **Message Table** area. Double-click a message text field to edit the message. Configure the RADIUS reply message text on the Secure Firewall ASA to match (in whole or in part) the message text sent by the RADIUS server.

The following table shows the message code, the default RADIUS reply message text, and the function of each message:

Note
The default message text used by the Secure Firewall ASA is the default message text used by Cisco Secure Access Control Server (ACS). If you are using Cisco Secure ACS, and it is using the default message text, you do not need to configure the message text on the Secure Firewall ASA.

Because the security appliance searches for strings in the order in which they appear in the table, you must ensure that the string you use for the message text is not a subset of another string. For example, “new PIN” is a subset of the default message text for both new-pin-sup and next-ccode-and-reauth. If you configure new-pin-sup as “new PIN,” when the security appliance receives “new PIN with the next card code” from the RADIUS server, it will match the text to the new-pin-sup code instead of the next-ccode-and-reauth code.

Message Code	Default RADIUS Reply Message Text	Function
next-code	Enter Next PASSCODE	Indicates the user must enter the NEXT tokencode without the PIN.
new-pin-sup	Please remember your new PIN	Indicates the new system PIN has been supplied and displays that PIN for the user.
new-pin-meth	Do you want to enter your own pin	Requests from the user which new PIN method to use to create a new PIN.
new-pin-req	Enter your new Alpha-Numerical PIN	Indicates a user-generated PIN and requests that the user enter the PIN.
new-pin-reenter	Reenter PIN:	Used internally by the Secure Firewall ASA for user-supplied PIN confirmation. The client confirms the PIN without prompting the user.
new-pin-sys-ok	New PIN Accepted	Indicates the user-supplied PIN was accepted.
next-ccode-and-reauth	new PIN with the next card code	Follows a PIN operation and indicates the user must wait for the next tokencode and to enter both the new PIN and next tokencode to authenticate.
ready-for-sys- pin	ACCEPT A SYSTEM GENERATED PIN	Used internally by the Secure Firewall ASA to indicate the user is ready for the system-generated PIN.

Step 11 Click **OK**, then **Apply**, then **Save**.

About Certificate Pinning

Cisco Secure Client certificate pinning helps to detect if a server certificate chain actually came from the connecting server. This feature is guided by VPN profile settings and is an addition to the Cisco Secure Client server certificate verification policies. The strict certificate trust settings in the Cisco Secure Client local policy file have no influence on Certificate Pinning check. You can configure pins globally or by per host basis in the VPN profile. Those pins configured for primary host are also valid for back up hosts in the server list. The preference to perform certificate pinning checks is not user controllable. A pin verification failure results in the termination of the VPN connection.

Note Cisco Secure Client performs pin verification only when the preference is enabled and the connecting server has pins in the VPN profile.

In the VPN profile editor Cisco Secure Client Profile Editor, Certificate Pin, on page 90, you can enable the preference and configure the global and per host certificate pins.

You must be cautious when configuring and maintaining certificate pinning. Consider these recommendations when setting preferences:

- Pin root and/or intermediate certificates since they are well maintained by CA vendors in the operating system
- Pin multiple root and/or intermediate certificates from a different CA to serve as a backup when any CA is compromised
- Pin multiple root and/or intermediate certificates for ease of CA transitions
- Use the same Certificate Signing Request if a leaf certificate is pinned, to retain the public key upon certificate renewal
- Pin all connection hosts in the server list

Global and Per Host Pins

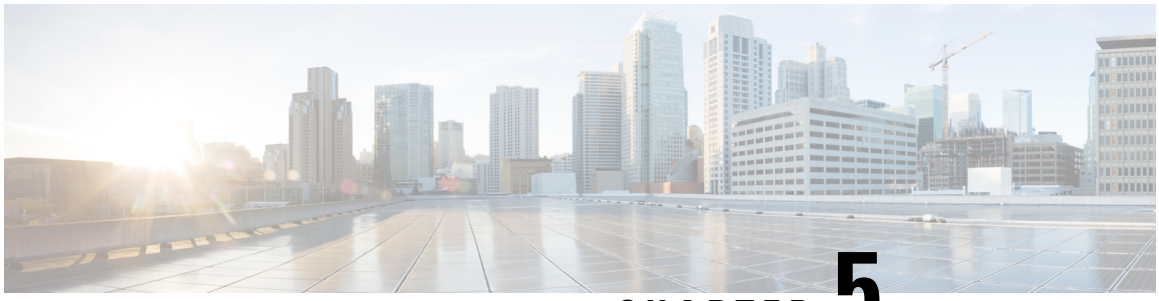
You can configure certificate pins on a global or by per host basis. Pins which are valid for most of the connection hosts are configured as global pins. We recommend that you configure root, intermediate certificate authorities, and wild card leaf certificates under global pins in the VPN profile. Pins that are valid only for a connection host are considered as per host pins. We recommend that you configure leaf, self-signed certificates under per host pins in the VPN profile.

Note Cisco Secure Client checks global pins and per host pins for the corresponding connection server during pin verification.

Note Global pins across multiple VPN profiles are not merged. Pins are strictly considered from the file connection server for VPN connection.



Note You can only pin per host certificates when certificate pinning preference is enabled in the global pins section.



CHAPTER 5

Configure Network Access Manager

This chapter provides an overview of the Network Access Manager configuration and provides instructions for adding and configuring user policies and network profiles.

- About Network Access Manager, on page 175
- Network Access Manager Deployment, on page 178
- Disable DHCP Requests by Network Access Manager During Connectivity Testing, on page 179
- Network Access Manager Profile, on page 179

About Network Access Manager

Network Access Manager is client software that provides a secure Layer 2 network in accordance with its policies. It detects and selects the optimal Layer 2 access network and performs device authentication for access to both wired and wireless networks. Network Access Manager manages user and device identity and the network access protocols required for secure access. It works intelligently to prevent end users from making connections that are in violation of administrator-defined policies.

The Network Access Manager is designed to be single homed, allowing only one network connection at a time. Also, wired connections have higher priority than wireless so that if you are plugged into the network with a wired connection, the wireless adapter becomes disabled with no IP address.

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

Note Network Access Manager is not supported on macOS or Linux.

Note If you are using ISE posture on a Windows OS, Network Access Manager must be installed prior to starting Cisco Secure Client ISE Posture.

The Network Access Manager component of the Cisco Secure Client supports the following main features:

- Captive Portal Detection. Refer to Captive Portal Detection Requirements with Network Access Manager, on page 182. Captive Portal Detection is not supported on Windows 7.

- Transport Layer Security (TLS) Protocol Version 1.2.
- Wired (IEEE 802.3) and wireless (IEEE 802.11) network adapters.
- Some Mobile Broadband (3G) network adapters with Windows 7 or later. (Requires a WAN adapter that supports Microsoft Mobile Broadband APIs.)
- Pre-login authentication using Windows machine credentials.
- Single sign-on user authentication using Windows logon credentials.
- Simplified IEEE 802.1X configuration.
- IEEE MACsec wired encryption and enterprise policy control.
- EAP methods:
  - EAP-FAST, PEAP, EAP-TTLS, EAP-TLS, and LEAP (EAP-MD5, EAP-GTC, and EAP-MSCHAPv2 for IEEE 802.3 wired only).
- Inner EAP methods:
  - PEAP—EAP-GTC, EAP-MSCHAPv2, and EAP-TLS.
  - EAP-TTLS—EAP-MD5 and EAP-MSCHAPv2 and legacy methods (PAP, CHAP, MSCHAP, and MSCHAPv2).
  - EAP-FAST—GTC, EAP-MSCHAPv2, and EAP-TLS.
- Encryption modes—Static WEP (Open or Shared), dynamic WEP, TKIP, and AES.
- Key establishment protocols—WPA, WPA2/802.11i.
- Cisco Secure Client supports smartcard-provided credentials in the following environments:
  - Microsoft CAPI 1.0 and CAPI 2.0 (CNG) on Windows.
  - Windows logon does not support ECDSA certificates; therefore, the Network Access Manager Single Sign-On (SSO) does not support ECDSA client certificates.



Note WPA3 Enhanced Open (OWE) and WPA3 Personal (SAE) support added to Network Access Manager with Cisco Secure Client Release 5.0.02075.

Suite B and FIPS

The following features are FIPS-certified on Windows 7 or later, and any exceptions are listed:

- ACS and ISE do not support Suite B, but FreeRADIUS 2.x with OpenSSL 1.x does. Microsoft NPS 2008 supports Suite B in part (the NPS certificate still has to be RSA).
- 802.1X/EAP supports the transitional Suite B profile only (as defined in RFC 5430).
- MACsec is FIPS-compliant.
- Elliptic Curve Diffie-Hellman (ECDH) key exchange is supported.

- ECDSA client certificates are supported.
- ECDSA CA certificates in the OS store are supported.
- ECDSA CA certificates in the network profile (PEM encoded) are supported.
- Server’s ECDSA certificate chain verification is supported.

Single Sign On "Single User" Enforcement

Microsoft Windows allows multiple users to be logged on concurrently, but Cisco Secure Client Network Access Manager restricts network authentication to a single user. Cisco Secure Client Network Access Manager can be active for one user per desktop or server, regardless of how many users are logged on. Single user login enforcement implies that only one user can be logged in to the system at any one time and that administrators cannot force the currently logged-in user to log off.

When the Network Access Manager client module is installed on Windows desktops, the default behavior is to enforce single user logon. When installed on servers, the default behavior is to relax the single user login enforcement. In either case, you can modify or add a registry to change the default behavior.

Restrictions

- Windows administrators are restricted from forcing currently logged-on users to log off.
- RDP to a connected workstation is supported for the same user.
- To be considered the same user, credentials must be in the same format. For example, user/example is not the same as user@example.com.
- Smart-card users must also have the same PIN to be considered the same user.

Configure Single Sign-On Single User Enforcement

To change how a Windows workstation or server handles multiple users, change the value of EnforceSingleLogon in the registry.

On Windows, the registry key is **EnforceSingleLogon** and is in the same registry location as the OverlayIcon key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential
Providers\{B12744B8-5BB7-463a-B85E-BB7627E73002}
```

To configure single or multiple user logon, add a DWORD named EnforceSingleLogon, and give it a value of 1 or 0.

For Windows:

- 1 restricts logon to a single user.
- 0 allows multiple users to be logged on.

Network Access Manager Deployment

Network Access Manager is deployed as part of Cisco Secure Client. For information about how to install Cisco Secure Client, along with the Network Access Manager and other modules, see the AnyConnect Deployment Overview.

Guidelines

- Confusion about the Windows network status task tray icon—Network Access Manager overrides Windows network management. Therefore, after installing the Network Access Manager, you cannot use the network status icon to connect to networks.

  Recommended Action—Remove the Windows network icon from the task tray by setting **Remove the networking icon** in a Windows group policy. This setting affects only the tray icon. The user can still create native wireless networks using the Control Panel.

- Hidden networks and network selection for Windows 7 or later—Network Access Manager tries to connect to only the networks that are configured in the Network Access Manager network scan list.

  On Windows 7 or later, the Network Access Manager probes for hidden SSIDs. When the first hidden SSID is found, it stops looking. When multiple hidden networks are configured, the Network Access Manager selects the SSID as follows:

  - The first administrator-defined hidden corporate network.
  - The administrator-defined hidden network.
  - The first user-defined hidden network. Cisco recommends having only one hidden corporate network at your site, since the Network Access Manager can probe only one non-broadcasting SSID at a time.

- Momentary loss of network connectivity or longer connection times—If you defined networks in Windows before the Network Access Manager was installed, the Windows connection manager may occasionally try to make a connection to that network.

  Recommended Action—When the network is in range, switch off **Connect Automatically** for all Windows-defined networks or delete all the Windows-defined networks.

- The Network Access Manager module can be configured to convert some existing Windows 7 or later wireless profiles to the Network Access Manager profile format when the module is installed on the client system for the first time. Infrastructure networks that match the following criteria can be converted:

  - Open
  - Static WEP
  - WPA/WPA2 Personal
  - Only non-GPO native Wi-Fi user network profiles are converted.
  - WLAN services must be running on the system during profile conversion.
  - Conversion will not be done if a Network Access Manager XML configuration file already exists (userConfiguration.xml).

To enable network profile conversion, create an MSI transform that sets the PROFILE_CONVERSION property value to 1, and apply it to the MSI package. Or change the PROFILE_CONVERSION property to 1 in the command line, and install the MSI package. For example, **msiexec /i cisco-secure-client-win-<version>-nam-predeploy-k9.msi PROFILE_CONVERSION=1**.

- You must install the Network Access Manager before ISE Posture starts. ISE Posture uses the Network Access Manager plugin to detect the network change events and 802.1x Wi-Fi.

Disable DHCP Requests by Network Access Manager During Connectivity Testing

When a network is configured to use dynamic IP addresses, the Windows OS service tries to establish connectivity using DHCP. However, the operating system process can take up to two minutes before it notifies the Network Access Manager that it has completed a DHCP transaction. The Network Access Manager triggers DHCP transactions, in addition to the OS DHCP transactions, to avoid long delays in establishing connectivity through the OS and to verify network connectivity.

When you want to disable the use of DHCP transactions by Network Access Manager for connectivity testing, add the following registry key as a DWORD and set the value as indicated:

- 64-bit Windows—HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\Cisco Secure Client Network Access Manager\DisableDHCP set to 1
- 32-bit Windows—HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco Secure Client Network Access Manager\DisableDHCP set to 1

Note We strongly discourage disabling the Network Access Manager DHCP connectivity test because it often results in a longer connectivity time.

Network Access Manager Profile

Network Access Manager profiles are configured in the Network Access Manager profile editor, which is available in the ASDM and also as a stand-alone Windows application.

Client Policy Window

The **Client Policy** window enables you to configure the client policy options. The following sections are included:

Connection Settings

Enables you to define whether a network connection is attempted before or after the user logs on.

- **Default Connection Timeout**—The number of seconds to use as the connection timeout for user-created networks. The default value is 40 seconds.

- **Before User Logon**—Connect to the network before the user logs on. The user-logon types that are supported include user account (Kerberos) authentication, loading of user GPOs, and GPO-based logon script execution. If you choose Before User Logon, you can also set *Time to Wait Before Allowing a User to Logon*.
- **Time to wait before allowing user to Logon**—Specifies the maximum (worst-case) number of seconds to wait for the Network Access Manager to make a complete network connection. If a network connection cannot be established within this time, the Windows logon process continues with user logon. The default is five seconds.

Note If the Network Access Manager is configured to manage wireless connections, you must set **Time to wait before allowing user to logon** to 30 seconds or more because of the additional time that it may take to establish a wireless connection. You should also account for the time required to obtain an IP address via DHCP. If two or more network profiles are configured, you should increase the value to cover two or more connection attempts.

- **After User Logon**—Connect to the network after the user logs on to Windows.

Media

Specifies which types of media are controlled by the Network Access Manager client.

- **Manage Wi-Fi (wireless) Media**—Enables management of Wi-Fi media and, optionally, validation of a WPA/WPA2 handshake.

  The IEEE 802.11i Wireless Networking standard specifies that the supplicant (in this case, the Network Access Manager) must validate the access point's RSN IE (Robust Secure Network Information Exchange). The IE is sent in the IEEE 801.X protocol packet's EAPOL key data during key derivation, and it should match the access point's RSN IE found in the beacon/probe response frame.

- **Enable validation of WPA/WPA2 handshake**—Validates a WPA/WPA2 handshake. If unchecked, this optional validation step is skipped.

Note Some adapters do not consistently provide the access point's RSN IE, so the authentication attempt fails, and the client will not connect.

- **Enable Randomized MAC Address**—(Windows 10 and later only) Enables randomization for hardware or drivers that support it. When enabled, each unique wireless network SSID utilizes a new randomized address and uses that private address for the network. You can also change the randomized address every 24 hours, if desired. If a connection is forgotten and then reconnected, a new MAC address is assigned. Refer to Enable MAC Address Randomization, on page 189.
- **Default Association Timeout** (sec)—If you enable the WPA/WPA2 handshake, you must specify the default association timeout.
- **Manage Wired (IEEE 802.3) Media**—Enables management of wired connections.
- **Manage Mobile Broadband Media**—Enables management of Windows Mobile Broadband Adapters. This feature is disabled by default.

Note This feature is in a beta release state. Cisco TAC does not provide support for beta releases.

- **Enable Data Roaming**—Determines whether to allow data roaming.

End-user Control

Enables you to configure the following control for users:

- **Disable Client**—Allows users to disable and enable the Network Access Manager's management of wired and wireless media using the Cisco Secure Client UI.
- **Display user groups**—Makes user-created groups (created from CSSC 5.x) visible and capable of a connection, even though they do not correspond to administrator-defined groups.
- **Specify a script or application to run when connected**—Allows users to specify a script or application to run when the network connects.

Note The scripting settings are specific to one user-configured network and allow the user to specify a local file (.exe, .bat, or .cmd) to run when that network gets to a connected state. To avoid conflicts, the scripting feature permits users to configure a script or application for only user-defined networks and not for administrator-defined networks. The feature does not allow users to alter administrator networks regarding the running of scripts; therefore, the interface for administrator networks is not available to the user. Also, if you do not allow users to configure a running script, the feature is not seen in the Network Access Manager GUI.

- **Auto-connect**—Connects automatically to a network without a user choosing it. The default is automatic connection.
- **Select Machine Connection Type**—Enables an *Allow Connection Before Logon* choice for end users, when adding a user-defined network. The end user choice determines whether networks can connect prior to user login. Subsequently, they can choose a personal, shared WEP, or open security.

  Enable by Default—Automatically enables Allow Connection Before Logon for the end user when adding a user-defined network.

Note If you upgrade AnyConnect from an earlier version to 4.9.01095 (or later), you must open the configuration.xml file with the proper profile editor and save the file in order to get an updated xml with the new features.

Administrative Status

- **Service Operation**—If you switch off the service, clients who use this profile will not be able to connect to establish Layer 2 connections.

- **FIPS Mode**—If you enable FIPS mode, the Network Access Manager performs cryptographic operations in a way that meets the government requirements.

  Federal Information Processing Standard (FIPS 140-2 Level 1) is a U.S. government standard that specifies security requirements for cryptography modules. FIPS is supported by the Network Access Manager for MACsec or Wi-Fi, depending on the type of software and hardware.

  Table 6: FIPS Support by the Network Access Manager

Media/Operating System	Windows 7 or later
Wired with MACsec	FIPS compliant when an Intel HW MACsec capable NIC or any non-hardware MACsec is used
Wi-Fi	Not FIPS compliant

- **Captive Portal Detection**—You can choose to enable or disable the automatic launch of a default web browser upon captive portal detection. With captive portal detection enabled, the user is prompted to enter credentials or to acknowledge the portal page, permitting network access on the browser that is launched. When the default web browser is launched, the Network UI tile displays "Action needed, no internet. Open browser and connect." This UI tile changes to "Captive Portal Detected" and "Connected" upon authentication. If no configuration for captive portal detection exists, Network Access Manager sets the option to disabled.

Captive Portal Detection Requirements with Network Access Manager

- Within the configurable End-User Controls for Network Access Manager, captive portal remediation will not be an option.
- Captive Portal Detection is not supported on Windows 7.
- To prevent the potential for conflict, Network Access Manager Captive Portal Detection, when enabled, disables the Windows Network Location Awareness Service captive portal detection. Thw Windows service is restored only if Network Access Manager is set to disabled or uninstalled.
- The Network Access Manager probes for a connection every 10 seconds, and when it detects the completion of web authentication, it provides internet connectivity. It does not monitor when a user logs out.

Authentication Policy Window

The Authentication Policy window enables you to create association and authentication network filters, which apply to all network connections. If you do not check any of the association or authentication modes, the user cannot connect to an authenticating Wi-Fi network. If you choose a subset of the modes, the user can connect to networks for those types only. Select each required association or authentication mode, or choose **Select All**.

The inner methods can also be restricted to only specific authentication protocols. The inner methods are shown indented under the outer methods (tunneling) in the Allowed Authentication Modes pane.

The mechanism for choosing the authentication protocol is integrated with the current client authentication database. A secure wireless LAN deployment does not require the creation of a new authentication system for users.

The EAP methods available for inner tunneling are based on the inner method credential type and the outer tunneling method. In the following list, each outer tunnel method lists the types of inner methods that are supported for each credential type.

- PEAP
  - Password credentials: EAP-MSCHAPv2 or EAP-GTC
  - Token credentials: EAP-GTC
  - Certificate credentials: EAP-TLS
- EAP-FAST
  - Password credentials: EAP-MSCHAPv2 or EAP-GTC
  - Token credentials: EAP-GTC
  - Certificate credentials: EAP-TLS
- EAP-TTLS
  - Password credentials: EAP-MSCHAPv2, EAP-MD5, PAP (L), CHAP (L), MSCHAP (L), MSCHAP-v2 (Legacy)
  - Token credentials: PAP (Legacy). The default token option that Network Access Manager supports is PAP, since challenge/response methods are not well suited for token-based authentication.
  - Certificate credentials: N/A

Networks Window

The Networks window enables you to configure predefined networks for your enterprise user. You can either configure networks that are available to all groups or create groups with specific networks. The Networks window displays a wizard that may add panes to the existing window, and enables you to advance to more configuration options by clicking **Next**.

A group, fundamentally, is a collection of configured connections (networks). Every configured connection must belong to a group or be a member of all groups.



Note For backward compatibility, administrator-created networks deployed with the Cisco Secure Services Client are treated as hidden networks, which do not broadcast SSIDs. However, user networks are treated as networks that broadcast SSIDs.

Only administrators can create a new group. If no groups are defined in the configuration, the profile editor creates an auto-generated group. The auto-generated group contains networks that are not assigned to any administrator-defined group. The client attempts to make a network connection using the connections defined in the active group. Depending on the setting of the **Create Networks** option in the Network Groups window, end users can add user networks to the active group or delete user networks from the active group.

Networks that are defined are available to all groups at the top of the list. Because you control what networks are in the global networks, you can specify the enterprise networks that an end user can connect to, even in the presence of user-defined networks. An end user cannot modify or remove administrator-configured networks.

Note End users may add networks to groups, except for networks in the globalNetworks section, because these networks exist in all groups, and they can only be created using the profile editor.

A typical end user of an enterprise network does not need knowledge of groups to use this client. The active group is the first group in the configuration, but if only one is available, the client is unaware and does not display the active group. However, if more than one group exists, the UI displays a list of groups indicating that the active group is selected. Users can then choose from the active group, and the setting persists across reboots. Depending on the setting of the **Create Networks** option in the Network Groups window, end users can add or delete their own networks without using groups.

Note A group selection is maintained across reboots and network repairs (done while right-clicking the tray icon and choosing **Network Repair**). When the Network Access Manager is repaired or restarted, it starts using the previously active group.

Networks, Media Type Page

The Networks window Media Type page enables you to create or edit a wired or a wireless network. The settings vary depending on your choice.

The following sections are included in the first dialog:

- Name—Enter the name that is displayed for this network.
- Group Membership—Select to which network group or groups this profile should be available.
- Network Media—Select Wired or Wi-Fi (wireless). If you choose Wi-Fi, you can also configure the following parameters:
  - SSID—Enter the SSID (Service Set Identifier) of your wireless network.
  - Hidden Network—Allow a connection to a network even if it is not broadcasting its SSID.
  - Corporate Network—Forces a connection to a network configured as Corporate first, if one is in proximity. When a corporate network uses a non-broadcasting (hidden) SSID, and is configured as hidden, the Network Access Manager actively probes for hidden SSIDs and establishes the connection when a corporate SSID is in range.
  - Association Timeout—Enter the length of time that the Network Access Manager waits for association with a particular wireless network before it re-evaluates the available networks. The default association timeout is five seconds.
- Common Settings
  - Script or application—Enter the path and filename of the file to run on the local system, or browse to a folder and select one. The following rules apply to scripts and applications:

- You cannot run scripts when in Start Before Login mode.
- Files with .exe, .bat, or .cmd extensions are accepted.
- Users may not alter the script or application defined in an administrator-created network.
- You may specify only the path and script or application filename using the profile editor. If the script or application does not exist on a user's machine, an error message appears. Users are informed that the script or application does not exist on their machine and that they need to contact their system administrator.
- You must specify the full path of the application that you want to run, unless the application exists in the user's path. If the application exists in the user's path, you can specify only the application or script name.
- Connection Timeout—Enter the number of seconds that the Network Access Manager waits for a network connection to be established before it tries to connect to another network (when the connection mode is automatic) or uses another adapter.



Note Some smartcard authentication systems require almost 60 seconds to complete an authentication. When using a smartcard, you should increase the Connection Timeout value, especially if the smartcard may have to try several networks before making a successful connection.



Note To mitigate issues found with certain smart card middleware, the Cisco Secure Client Network Access Manager verifies smartcard PINs by performing a signing operation on test data and verifying that signature. This test signing is done for each certificate located on a smartcard, and dependent on the number of certificates, can add significant delays to smartcard authentication. If you want to disable the test signing operation, you can add **DisableSmartcardPinVerifyBySigning** as a DWORD set to 1 in the registry entry at HKEY_LOCAL_MACHINE/SOFTWARE/Cisco/ Cisco Secure Client Network Access Manager. Any change to enabling this key should be fully tested with all smartcards and related hardware to ensure proper operation.

Networks, Security Level Page

In the Security Level page of the Networks wizard, choose Open Network, Authentication Network, or (displayed for wireless network media only) Shared Key Network. The configuration flow for each of those network types is different and is described in the following sections.

- Configure an Authenticating Network—Recommended for a secure enterprise.
- Configure an Open Network—Not recommended, but can be used to provide guest access through captive portal environment. Network Access Manager does not support the automatic launch of a browser when in the captive portal state.

- Configure a Shared Key Network—Recommended for wireless networks such as small offices or home offices.

Additionally, within an open, shared, or authenticating network, you can Enable MAC Address Randomization, on page 189.

Configure an Authenticating Network

If you chose Authenticating Network in the Security Level section, additional panes appear, which are described below. When you are done configuring settings on these panes, click the **Next** button or select the **Connection Type** tab to open the Network Connection Type dialog.

802.1X Settings Pane

Adjust the IEEE 802.1X settings according to your network configuration:

Note When Cisco Secure Client ISE Posture is installed with the Network Access Manager, ISE posture uses the Network Access Manager plugin to detect the network change events and 802.1X WiFi.

- authPeriod (sec)—When authentication begins, this setting determines how long the supplicant waits in between authentication messages before it times out and requires the authenticator to initiate authentication again.
- heldPeriod (sec)—When authentication fails, this setting defines how long the supplicant waits before another authentication attempt can be made.
- startPeriod (sec)—The interval, in seconds, between the retransmission of EAPOL-Start messages if no response to any EAPOL-Start messages is received from the authenticator.
- maxStart—The number of times the supplicant initiates authentication with the authenticator by sending an IEEE 801.X protocol packet, EAPOL key data, or EAPoL-Start before the supplicant assumes that there is no authenticator present. When this happens, the supplicant allows data traffic.

Tip You can configure a single authenticating wired connection to work with both open and authenticating networks by carefully setting the startPeriod and maxStart such that the total time spent trying to initiate authentication is less than the network connection timer (startPeriod x maxStart < network connection timer).

Note that in this scenario, you should increase the network connection timer by (startPeriod x maxStart) seconds to give the client enough time to acquire a DHCP address and finish the network connection.

Conversely, to allow data traffic only after authentication succeeds, you should make sure that the startPeriod and maxStart is such that the total time spent trying to initiate authentication is greater than the network connection timer (start Period x maxStart > Network Connection Timer).

Security Pane

Appears only for wired networks.

In the Security pane, select values for the following parameters:

- Key Management—Determine which key management protocol to use with the MACsec-enabled wired network.
  - None—No key management protocols are used, and no wired encryption is performed.
  - MKA—The supplicant attempts to negotiate MACsec key agreement protocol policies and encryption keys. MACsec is MAC-Layer Security, which provides MAC-layer encryption over wired networks. The MACsec protocol represents a means to secure MAC-level frames with encryption and relies on the MACsec Key Agreement (MKA) Entity to negotiate and distribute the encryption keys.
- Encryption
  - None—Data traffic is integrity-checked but not encrypted.
  - MACsec: AES-GCM-128—This option is available only if you chose MKA for key management. It causes data traffic to be encrypted using AES-GCM-128.
  - MACsec: AES-GCM-256—This option is supported on select IOS versions with the enterprise edge (eEdge) integration and is available only if you choose MKA for key management. It must match the setting on the switch side. By enabling the MACsec 256 encryption standard, 802.1 AE encryption with MACsec Key Agreement (MKA) is supported on downlink ports for encryption between a MACsec-capable device and host devices.

See Identity-Based Networking Services: MAC Security for more information.

Port Authentication Exception Policy Pane

This pane appears only for wired networks.

The Port Authentication Exception Policy pane enables you to tailor the IEEE 802.1X supplicant's behavior during the authentication process. If port exceptions are not enabled, the supplicant continues its existing behavior and opens the port only upon successfully completing the full configuration (or as described earlier in this section, after the maxStarts number of authentications are initiated without a response from the authenticator). Choose from one of the following options:

- Allow data traffic before authentication—Allows data traffic prior to an authentication attempt.
- Allow data traffic after authentication even if:
  - EAP fails—When selected, the supplicant attempts authentication. If authentication fails, the supplicant allows data traffic despite the authentication failure.
  - EAP succeeds but key management fails—When selected, the supplicant attempts to negotiate keys with the key server but allows data traffic if the key negotiation fails for any reason. This setting is valid only when key management is configured. If key management is set to none, the check box is dimmed out.



Restriction MACsec requires ACS version 5.1 or later and a MACsec capable switch. Refer to the *Catalyst 3750-X and 3560-X Switch Software Configuration Guide* for ACS or switch configuration.

Association Mode

The pane appears only for wireless networks.

Choose the association mode:

- WEP
- WAP Enterprise (TKIP)
- WPA Enterprise (AES)
- WPA2 Enterprise (TKIP)
- WPA2 Enterprise (AES)
- CCKM (TKIP)—(requires Cisco CB21AG Wireless NIC)
- CCKM (AES)—(requires Cisco CB21AG Wireless NIC)

Configure an Open Network

An open network uses no authentication or encryption. Follow these steps if you want to create an open (non-secure) network.

Procedure

Step 1 Choose **Open Network** from the Security Level page. This choice provides the least secure network and is recommended for guest access wireless networks.

Step 2 Click **Next**.

Step 3 Determine a connection type.

In the Wi-Fi (wireless) Settings pane, you can choose the WPA3 Open (also known as OWE) checkbox.

Configure a Shared Key Network

Wi-Fi networks may use a shared key to derive an encryption key for use when encrypting data between endpoints and network access points. Using a shared key with WPA, WPA2 Personal, or WPA3 Personal provides a medium-level security class that is suitable for small or home offices.

Note Shared key security is not recommended for enterprise wireless networks.

Follow these steps if you want shared key network as your security level.

Procedure

Step 1 Choose **Shared Key Network**.

Step 2 Click **Next** on the Security Level window.

Step 3 Specify **User Connection** or **Machine Connection**.

Step 4 Click **Next**.

Step 5 Shared Key Type—Specify the shared key association mode, which determines the shared key type. The choices are as follows:

- WEP—Legacy IEEE 802.11 open-system association with static WEP encryption.
- Shared—Legacy IEEE 802.11 shared-key association with static WEP encryption.
- WPA/WPA2 Personal—A Wi-Fi security protocol that derives encryption keys from a passphrase pre-shared key (PSK).
- WPA3 Personal (also known as SAE)

Step 6 If you chose legacy IEEE 802.11 WEP or shared key, choose 40 bit, 64 bit, 104 bit, or 128 bit. A 40- or 64-bit WEP key must be 5 ASCII characters or 10 hexadecimal digits. A 104- or 128-bit WEP key must be 13 ASCII characters or 26 hex digits.

Step 7 If you chose WPA or WPA2 Personal, choose the type of encryption to use (TKIP/AES) and then enter a shared key. The key must be entered as 8 to 63 ASCII characters or exactly 64 hexadecimal digits. Choose **ASCII** if your shared key consists of ASCII characters. Choose **Hexadecimal** if your shared key includes 64 hexadecimal digits.

Step 8 Click **Done**. Then Click **OK**.

Enable MAC Address Randomization

On Windows 10 and later only, you can enable MAC address randomization for hardware or drivers that support it. Windows uses random addresses for probe requests or for connection to a network. A per-network address is calculated to ensure that the client always uses the same address when connecting to a particular network. If a connection is forgotten and then reconnected, a new MAC address is assigned.

1. If client policy allows, check the **Enable MAC Address Randomization** checkbox on the Networks, Security Level Page, on page 185. By enabling, each wireless network utilizes a random MAC address which is retained as long as the network is not deleted from the user configuration.
2. With any security level, you can check **Change Random MAC Address Daily**, if steps 1 and 2 are completed. This option allows each wireless network to utilize a random MAC address, which is retained for 24 hours. A new random MAC address is generated upon a new connection after 24 hours have passed.

Networks, Network Connection Type Pane

This section describes the network connection type pane of the Networks window, which follows Security Level in the Network Access Manager profile editor. Choose one of the following connection types:

- Machine Connection—The device's name, as stored in the Windows Active Directory, is used for authorization. Machine connection is typically used when user credentials are not required for a connection. Choose this option if the end station should log on to the network even when a user is logged off and user credentials are unavailable. This option is typically used for connecting to domains and to get GPOs and other updates from the network before the user has access.

Note Cisco Secure Client Start Before Login (SBL) fails if no known network is available. Network profiles allowed in SBL mode include all media types employing non-802.1X authentication modes, such as open WEP, WPA/WPA2 Personal, and static key (WEP) networks. If you configure the Network Access Manager for Before User Logon and machine connection authorization, the Network Access Manager asks the user for network information, and the VPN SBL succeeds.

- User Connection—User credentials are used for authorization.

  If Before User Logon was selected in the Client Policy pane, the Network Access Manager gathers the user's credentials after the user enters logon credentials on the Windows start screen. Network Access Manager establishes the network connection while Windows is starting the user's windows session.

  If After User Logon was selected in the Client Policy pane, the Network Access Manager starts the connection, after the user logs on to Windows.

  When the user logs off, the current user network connection is terminated. If machine network profiles are available, NAM reconnects to a machine network.

- Machine and User Connection—Only available when configuring an authenticating network, as selected in the Security Level pane. Machine ID and user credentials are both used, however, the machine part is valid only when a user is not logged on to the device. The configuration is the same for the two parts, but the authentication type and credentials for machine connection can be different from the authentication type and credentials for the user connection.

  Choose this option to keep the PC connected to the network at all times using the machine connection when a user is not logged in and using the user connection when a user has logged in.

  When EAP-FAST is configured as the EAP method (in the next pane), EAP chaining is supported. That means that the Network Access Manager verifies that the machine and the user are known entities, and are managed by the corporation.

  When you choose the network connection type, additional tabs are displayed in the Networks dialog, which allow you to set EAP methods and credentials for the chosen network connection type.

Networks, User or Machine Authentication Page

After selecting the network connection type, choose the authentication method(s) for those connection types. After you select an authentication method, the display is updated to the method that you chose, and you are required to provide additional information.

Note If you have enabled MACsec, ensure that you select an EAP method that supports MSK key derivation, such as PEAP, EAP-TLS, or EAP-FAST. Also, even if MACsec is not enabled, using the Network Access Manager reduces MTU from 1500 to 1468 to account for MACsec.

EAP Overview

EAP is an IETF RFC that addresses the requirements for an authentication protocol to be decoupled from the transport protocol carrying it. This decoupling allows the transport protocols (such as IEEE 802.1X, UDP, or RADIUS) to carry the EAP protocol without changes to the authentication protocol.

The basic EAP protocol is made up of four packet types:

- EAP request—The authenticator sends the request packet to the supplicant. Each request has a type field that indicates what is being requested, such as the supplicant identity and EAP type to use. A sequence number allows the authenticator and the peer to match an EAP response to each EAP request.
- EAP response—The supplicant sends the response packet to the authenticator and uses a sequence number to match the initiating EAP request. The type of the EAP response generally matches the EAP request, unless the response is a negative (NAK).
- EAP success—The authenticator sends a success packet to the supplicant upon successful authentication.
- EAP failure—The authenticator sends a failure packet to the supplicant if authentication failed.

When EAP is in use in an IEEE 802.11X system, the access point operates in an EAP pass-through mode. In this mode, the access point checks the code, identifier, and length fields and then forwards the EAP packets received from the supplicant to the AAA server. Packets received from the AAA server authenticator are forwarded to the supplicant.

EAP-GTC

EAP-GTC is an EAP authentication method based on simple username and password authentication. Without using the challenge-response method, both username and password are passed in clear text. This method is recommended for either inside a tunneling EAP method (see tunneling EAP methods below) or with a One Time Password (OTP).

EAP-GTC does not provide mutual authentication. It only authenticates clients, so a rogue server may potentially obtain users' credentials. If mutual authentication is required, EAP-GTC is used inside tunneling EAP methods, which provides server authentication.

No keying material is provided by EAP-GTC; therefore, you cannot use this method for MACsec. If keying material for further traffic encryption is required, EAP-GTC is used inside tunneling EAP methods, which provides the keying material (and inner and outer EAP methods crytobinding, if necessary).

You have two password source options:

- Authenticate using a password—Suitable only for well-protected wired environments
- Authenticate using a token—More secure because of the short lifetime (usually about 10 seconds) of a token code or OTP



Note Neither the Network Access Manager, the authenticator, nor the EAP-GTC protocol can distinguish between password and token code. These options impact only the credential's lifetime within the Network Access Manager. While a password can be remembered until logout or longer, the token code cannot (because the user is prompted for the token code with every authentication).

If a password is used for authentication, you can use this protocol for authentication against the database with hashed passwords since it is passed to the authenticator in clear text. We recommend this method if a possibility of a database leak exists.

EAP-TLS

EAP-Transport Layer Security (EAP-TLS) is an IEEE 802.1X EAP authentication algorithm based on the TLS protocol (RFC 2246). TLS uses mutual authentication based on X.509 digital certificates. The EAP-TLS message exchange provides mutual authentication, cipher suite negotiation, key exchange, verification between the client and the authenticating server, and keying material that can be used for traffic encryption.

The list below provides the main reasons why EAP-TLS client certificates can provide strong authentication for wired and wireless connections:

- Authentication occurs automatically, usually with no intervention by the user.
- No dependency on a user password exists.
- Digital certificates provide strong authentication protection.
- Message exchange is protected with public key encryption.
- The certificates are not susceptible to dictionary attacks.
- The authentication process results in a mutually determined key for data encryption and signing.

EAP-TLS contains two options:

- Validate Server Certificate—Enables server certificate validation.
- Enable Fast Reconnect—Enables TLS session resumption, which allows for much faster reauthentication by using an abbreviated TLS handshake as long as TLS session data is preserved on both the client and the server.



Note The Disable When Using a Smart Card option is not available for machine connection authentication.

EAP-TTLS

EAP-Tunneled Transport Layer Security (EAP-TTLS) is a two-phase protocol that expands the EAP-TLS functionality. Phase 1 conducts a complete TLS session and derives the session keys used in Phase 2 to securely tunnel attributes between the server and the client. You can use the attributes tunneled during Phase 2 to perform additional authentications using a number of different mechanisms.

Network Access Manager does not support the cryptobinding of the inner and outer methods used during EAP-TTLS authentication. If cryptobinding is required, you must use EAP-FAST. Cryptobinding provides protection from a special class of man-in-the-middle attacks where an attacker hijacks the user's connection without knowing the credentials.

The authentication mechanisms that can be used during Phase 2 include these protocols:

- PAP (Password Authentication Protocol)—Uses a two-way handshake to provide a simple method for the peer to prove its identity. An ID/Password pair is repeatedly sent by the peer to the authenticator until authentication is acknowledged or fails. If mutual authentication is required, you must configure EAP-TTLS to validate the server's certificate at Phase 1.

  Because a password is passed to the authenticator, you can use this protocol for authentication against a database with hashed passwords. We recommend this method when a possibility of a database leak exists.



Note You can use EAP-TTLS PAP for token and OTP-based authentications.

- CHAP (Challenge Handshake Authentication Protocol)—Uses a three-way handshake to verify the identity of the peer. If mutual authentication is required, you should configure EAP-TTLS to validate the server's certificate at Phase 1. Using this challenge-response method, you are required to store clear text passwords in the authenticator's database.
- MS-CHAP (Microsoft CHAP)—Uses a three-way handshake to verify the identity of the peer. If mutual authentication is required, you should configure EAP-TTLS to validate the server's certificate at Phase 1. Using this challenge-response method based on the NT-hash of the password, you are required to store either the clear text password or at least the NT-hash of the password in the authenticator's database.
- MS-CHAPv2—Provides mutual authentication between peers by including a peer challenge in the response packet and an authenticator response in the success packet. The client is authenticated before the server. If the server needs to be authenticated before the client (to prevent dictionary attacks), you should configure EAP-TTLS to validate the server's certificate at Phase 1. Using this challenge-response method based on the NT-hash of the password, you are required to store either the clear text password or at least the NT-hash of the password in the authenticator's database.

Configure EAP-TTLS

- EAP—Allows use of the following EAP methods:
  - EAP-MD5 (EAP Message Digest 5)—Uses a three-way handshake to verify the peer's identity (similar to CHAP). Using this challenge-response method, you are required to store the clear text password in the authenticator's database.
  - EAP-MSCHAPv2—Uses a three-way handshake to verify the identity of the peer. The client is authenticated before the server. If the server needs to be authenticated before the client (such as for the prevention of a dictionary attack), you should configure EAP-TTLS to validate the server's certificate at Phase 1. Using this challenge-response method on the NT-hash of the password, you are required to store either the clear text password or at least the NT-hash of the password in the authenticator's database.
- EAP-TTLS Settings
  - Validate Server Identity—Enables server certificate validation.

Note If you enable this, make sure that the server certificate installed on your RADIUS server contains the Extended Key Usage (EKU) of *Server Authentication*. When the RADIUS server sends its configured certificate to the client during authentication, it must have this Server Authentication setting for network access and authentication.

- Enable Fast Reconnect—Enables outer TLS session resumption only, regardless of whether the inner authentication is skipped or is controlled by the authenticator.

Note *Disable When Using a Smart Card* is not available on machine connection authentication.

- Inner Methods—Specifies the inner methods used after the TLS tunnel is created. Available only for Wi-Fi Media Type.

PEAP Options

Protected EAP (PEAP) is a tunneling TLS-based EAP method. It uses TLS for server authentication before the client authentication for the encrypting of inner authentication methods. The inner authentication occurs inside a trusted cryptographically protected tunnel and supports a variety of different inner authentication methods, including certificates, tokens, and passwords. Network Access Manager does not support the cryptobinding of the inner and outer methods used during PEAP authentication. If cryptobinding is required, you must use EAP-FAST. Cryptobinding provides protection from a special class of man-in-the-middle attacks where an attacker hijacks the user's connection without knowing the credentials.

PEAP protects the EAP methods by providing these services:

- TLS tunnel creation for the EAP packets
- Message authentication
- Message encryption
- Authentication of server to client

You can use these authentication methods:

- Authenticate using a password
  - EAP-MSCHAPv2—Uses a three-way handshake to verify the identity of the peer. The client is authenticated before the server. If the server needs to be authenticated before the client (such as for the prevention of a dictionary attack), you must configure PEAP to validate the server's certificate. Using the challenge-response method based on the NT-hash of the password, you are required to store either the clear text password or at least the NT-hash of the password in the authenticator's database.
  - EAP-GTC (EAP Generic Token Card)—Defines an EAP envelope to carry the username and password. If mutual authentication is required, you must configure PEAP to validate the server's certificate. Because the password is passed to the authenticator in clear text, you can use this protocol

for authentication against the database with hashed passwords. We recommend this method if a possibility of a database leak exists.

- EAP-TLS, using a certificate
  - EAP-TLS—Defines an EAP envelope to carry the user certificate. In order to avoid a man-in-the-middle attack (the hijacking of a valid user's connection), we recommend that you do not mix PEAP (EAP-TLS) and EAP-TLS profiles meant for authentication against the same authenticator. You should configure the authenticator accordingly (not enabling both plain and tunneled EAP-TLS).

Configure PEAP

- PEAP-EAP settings
  - Validate Server Identity—Enables server certificate validation.



Note If you enable this, make sure that the server certificate installed on your RADIUS server contains the Extended Key Usage (EKU) of *Server Authentication*. When the RADIUS server sends its configured certificate to the client during authentication, it must have this Server Authentication setting for network access and authentication.

  - Enable Fast Reconnect—Enables outer TLS session resumption only. The authenticator controls whether or not the inner authentication is skipped.
  - Disable when using a smart card—Do not use Fast Reconnect when using a smart card for authentication. Smart cards apply only to user connections.
  - Authenticate using a token and EAP GTC—Not available for machine authentication.
- Inner methods based on Credentials Source
  - Authenticate using a password for EAP-MSCHAPv2 and/or EAP-GTC.
  - EAP-TLS, authenticate using a certificate.
  - Authenticate using a token and EAP-GTC—Not available for machine authentication.



Note Before user logon, smart card support is not available on Windows.

EAP-FAST Settings

EAP-FAST is an IEEE 802.1X authentication type that offers flexible, easy deployment and management. It supports a variety of user and password database types, server-initiated password expiration and change, and a digital certificate (optional).

EAP-FAST was developed for customers who want to deploy an IEEE 802.1X EAP type that does not use certificates and provides protection from dictionary attacks.

EAP chaining is supported when both machine and user connections are configured. That means that the Network Access Manager verifies that the machine and the user are known entities and are managed by the corporation, which is useful for controlling user-owned assets that are connected to the corporate network. For more information about EAP chaining, see RFC 3748.

EAP-FAST encapsulates TLS messages within EAP and consists of three protocol phases:

1. A provisioning phase that uses Authenticated Diffie-Hellman Protocol (ADHP) to provision the client with a shared secret credential called a Protected Access Credential (PAC).
2. A tunnel establishment phase in which the PAC is used to establish the tunnel.
3. An authentication phase in which the authentication server authenticates the user's credentials (token, username/password, or digital certificate).

Unlike the other tunneling EAP methods, EAP-FAST provides cryptobinding between inner and outer methods, preventing the special class of man-in-the-middle attacks where an attacker hijacks a valid user's connection.

Configure EAP-FAST

- EAP-FAST Settings
  - Validate Server Identity—Enables server certificate validation. Enabling this introduces two extra dialogs in the management utility and adds additional Certificate panes in to the Network Access Manager Profile Editor task list.



Note If you enable this, make sure that the server certificate installed on your RADIUS server contains the Extended Key Usage (EKU) of *Server Authentication*. When the RADIUS server sends its configured certificate to the client during authentication, it must have this Server Authentication setting for network access and authentication.

  - Enable Fast Reconnect—Enables session resumption. The two mechanisms to resume the authentication sessions in EAP-FAST are user authorization PAC, which substitutes for the inner authentication, and TLS session resumption, which allows for an abbreviated outer TLS handshake. This Enable Fast Reconnect parameter enables or disables both mechanisms. The authenticator decides which one to use.



Note The machine PAC provides an abbreviated TLS handshake and eliminates inner authentication. This control is handled by the enable/disable PAC parameter.



Note The Disable When Using a Smart Card option is available only for user connection authorization.

- Inner methods based on Credentials Source—Enables you to authenticate using a password or certificate.
  - Authenticate using a password for EAP-MSCHAPv2 or EAP-GTC. EAP-MSCHAPv2 provides mutual authentication, but it authenticates the client before authenticating the server. If you want

mutual authentication with the server being authenticated first, configure EAP-FAST for authenticated provisioning only, and verify the server's certificate. Using the challenge-response method based on the NT-hash of the password, EAP-MSCHAPv2 requires you to store either the clear text password or at least the NT-hash of the password in the authenticator's database. Since the password is passed to the authenticator in clear text within EAP-GTC, you can use this protocol for authentication against the database.

- Authenticate using a certificate—Decide the following criteria for authenticating using a certificate: when requested, send the client certificate in the clear, only send client certificates inside the tunnel, or send the client certificate using EAP-TLS in the tunnel.
- Authenticate using a token and EAP-GTC.

- Use PACs—You can specify the use of PAC for EAP-FAST authentication. PACs are credentials that are distributed to clients for optimized network authentication.

Note Typically, you use the PAC option because most authentication servers use PACs for EAP-FAST. Before removing this option, verify that your authentication server does not use PACs for EAP-FAST; otherwise, the client's authentication attempts are unsuccessful.

LEAP Settings

LEAP (Lightweight EAP) supports wireless networks. It is based on the Extensible Authentication Protocol (EAP) framework and was developed by Cisco to create a protocol that was more secure than WEP.

Note LEAP is subject to dictionary attacks unless you enforce strong passwords and periodically expire passwords. Cisco recommends that you use EAP-FAST, PEAP, or EAP-TLS, whose authentication methods are not susceptible to dictionary attacks.

LEAP settings, which are available only for user authentication:

- Extend user connection beyond log off—Keeps the connection open when the user logs off. If the same user logs back on, the network connection is still active.

See Dictionary Attack on Cisco LEAP Vulnerability for more information.

Define Networks Credentials

On the Networks > Credentials pane, you specify whether to use user and/or machine credentials, and you configure trusted server validation rules.

Configure User Credentials

An EAP conversation may involve more than one EAP authentication method, and the identities claimed for each of these authentications may be different (such as machine authentication followed by user authentication). For example, a peer may initially claim the identity of nouser@cisco.com to route the authentication request to the cisco.com EAP server. However, once the TLS session has been negotiated, the peer may claim the

identity of johndoe@cisco.com. Thus, even if protection is provided by the user's identity, the destination realm may not necessarily match, unless the conversation terminates at the local authentication server.

For user connections, when the [username] and [domain] placeholder patterns are used, the following conditions apply:

- If a client certificate is used for authentication—Obtain the placeholder values for [username] and [password] from various X509 certificate properties. The properties are analyzed in the order described below, according to the first match. For example, if the identity is userA@example.com (where username=userA and domain=example.com) for user authentication and hostA.example.com (where username=hostA and domain=example.com) for machine authentication, the following properties are analyzed:
- If user certificate based authentication:
  - SubjectAlternativeName: UPN = userA@example.com
  - Subject = .../CN=userA@example.com/...
  - Subject = userA@eample.com
  - Subject = .../CN=userA/DC=example/DC=com/...
  - Subject = userA (no domain)
- If machine certificate based authentication:
  - SubjectAlternativeName: DNS = hostA.example.com
  - Subject = .../DC=hostA.example.com/...
  - Subject = .../CN=hostA.example.com/...
  - Subject = hostA.example.com
- If the credential source is the end user—Obtain the placeholder's value from the information that the user enters.
- If the credentials are obtained from the operating system—Obtain the placeholder's value from the logon information.
- If the credentials are static—Use no placeholders.

On the Credentials pane, you can specify the desired credentials to use for authenticating the associated network.

Procedure

Step 1 Define a user identity for the Protected Identity Pattern. Network Access Manager supports the following identity placeholder patterns:

- [username]—Specifies the username. If a user enters username@domain or domain\username, the domain portion is stripped off.
- [raw]—Specifies the username, exactly as entered by the user.

- [domain]—Specifies the domain of the user's device.

Step 2 Specify typical unprotected identity patterns.

Sessions that have yet to be negotiated experience identity request and response in the clear without integrity protection or authentication. These sessions are subject to snooping and packet modification.

- anonymous@[domain]—Often used in tunneled methods to hide the user identity when the value is sent in clear text. The real user identity is provided in the inner method as the protected identity.
- [username]@[domain]—For non-tunneled methods.

Note
Unprotected identity information is sent in clear text. If the initial clear text identity request or response is tampered with, the server may discover that it cannot verify the identity once the TLS session is established. For example, the user ID may be invalid or not within the realm handled by the EAP server.

Step 3 Specify the protect identities patterns.

To protect the user ID from snooping, the clear text identity may provide only enough information to enable routing of the authentication request to the correct realm.

- [username]@[domain]
- The actual string to use as the user's identity (no placeholders)

Step 4 Provide further user credential information:

- Use Single Sign On Credentials—Obtains the credentials from the operating system's logon information. If logon credentials fail, the Network Access Manager temporarily (until next logon) switches and prompts the user for credentials with the GUI.

  Note
  You cannot use Windows login credentials automatically with Network Access Manager and SSO. Using SSO with Network Access Manager requires that logon credentials are intercepted; therefore, you are prompted for a reboot after an installation or a log off.

- Use Static Credentials—Obtains the user credentials from the network profiles that this profile editor provides. If static credentials fail, the Network Access Manager does not use the credentials again until a new configuration is loaded.

  Note
  An ampersand is an invalid character in this field.

- Prompt for Credentials—Obtains the credentials from the end user with the Cisco Secure Client GUI as specified here:
  - Remember Forever—The credentials are remembered forever. If remembered credentials fail, the user is prompted for the credentials again. Credentials are preserved in the file and encrypted using a local machine password.
  - Remember While User Is Logged On—The credentials are remembered until the user logs off. If remembered credentials fail, the user is prompted for credentials again.
  - Never Remember—The credentials are never remembered. Network Access Manager prompts the user each time it needs credential information for authentication.

Step 5 Determine which certificate source to use for authentication when certificates are required:

- Smart card or OS certificates—Network Access Manager uses certificates found in the OS Certificate Stores or on a smart card.
- Smart Card certificates only— Network Access Manager uses only certificates found on a smart card.

Step 6 At the Remember Smart Card Pin parameter, determine how long Network Access Manager remembers the PIN used to retrieve the certificate from a smart card. Refer to Step 2 for the available options.

Note
The PIN is never preserved longer than a certificate itself.

Some smart cards may take longer than others to connect, depending on the smart card chip and driver, also known as the cryptographic service provider (CSP) and the key storage provider (KSP). Increasing the connection timeout may give the network enough time to perform the smart-card-based authentication.

Configure Machine Credentials

An EAP conversation may involve more than one EAP authentication method, and the identities claimed for each of these authentications may be different (such as machine authentication followed by user authentication). For example, a peer may initially claim the identity of nouser@example.com to route the authentication request to the cisco.com EAP server. However, once the TLS session has been negotiated, the peer may claim the identity of johndoe@example.com. Thus, even if protection is provided by the user's identity, the destination realm may not necessarily match, unless the conversation terminates at the local authentication server.

For machine connections, whenever the [username] and [domain] placeholders are used, these conditions apply:

- If a client certificate is used for authentication—Obtain the placeholder values for [username] and [password] from various X509 certificate properties. The properties are analyzed in the order described below, according to the first match. For example, if the identity is userA@cisco.com (where username=userA and domain=cisco.com) for user authentication and hostA.cisco.com (where username=hostA and domain=cisco.com) for machine authentication, the following properties are analyzed:
- If user certificate based authentication:
  - SubjectAlternativeName: UPN = userA@example.com
  - Subject = .../CN=userA@example.com/...
  - Subject = userA@example.com
  - Subject = .../CN=userA/DC=example.com/...
  - Subject = userA (no domain)
- If machine certificate based authentication:
  - SubjectAlternativeName: DNS = hostA.example.com
  - Subject = .../DC=hostA.example.com/...
  - Subject = .../CN=hostA.example.com/...

- Subject = hostA.example.com

- If a client certificate is not used for authentication—Obtain the credentials from the operating system, and the [username] placeholder represents the assigned machine name.

With the Credentials panel you can specify the desired machine credentials.

Procedure

Step 1 Define a machine identity for the Protected Identity Pattern. Network Access Manager supports the following identity placeholder patterns:

- [username]—Specifies the username. If a user enters username@domain or domain\username, the domain portion is removed.
- [raw]—Specifies the username, exactly as entered by the user.
- [domain]—Specifies the domain of the user's PC.

Step 2 Define typical unprotected machine identity patterns.

Sessions that have yet to be negotiated experience identity request and response in the clear without integrity protection or authentication. These sessions are subject to snooping and packet modification.

- host/anonymous@[domain]
- The actual string to send as the machine's identity (no placeholders)

Step 3 Define the protected machine identity patterns.

To protect the user ID from snooping, the clear text identity may provide only enough information to enable routing of the authentication request to the correct realm. Typical protected machine identity patterns are as follows:

- host/[username]@[domain]
- The actual string to use as the machine's identity (no placeholders)

Step 4 Provide further machine credential information:

- Use Machine Credentials—Obtains the credentials from the operating system.
- Use Static Credentials—Specifies an actual static password to send in the deployment file. Static credentials do not apply for certificate-based authentication.

Set up Network Access Manager to Choose Correct Certificate

When there are two certificates during client authentication, the Network Access Manager automatically chooses the best certificate based on certificate attributes. Because the criteria of what is the preferred certificate varies from customer to customer, you must configure the following fields to determine certificate selection and provide any desired rules to override certificate selection.

If multiple certificates match the same rule or none matches the rule, the ACE engine runs through an algorithm to prioritize certificates and selects one based on certain criteria (such as whether it has a private key, whether it is from the machine store, and so on). If multiple certificates are of the same priority, the ACE engine chooses the first certificate it finds within that priority.

Procedure

Step 1 From the Cisco Secure Client Profile Editor, choose the **Networks** tab.

Step 2 Choose which network to edit.

Step 3 Choose the **Machine Credentials** tab.

Step 4 At the bottom of the page, choose **Use Certificate Matching Rule**.

Step 5 From the Certificate Field drop-down menu, choose what you want to use for search criteria.

Step 6 From the Match drop-down menu, determine if the search includes an exact match on the field (Equals) or a part of the field to match (Includes).

Step 7 In the Value field, enter the certificate search criteria.

Configure Trusted Server Validation Rules

When the Validate Server Identity option is configured for the EAP method, the Certificate panel is enabled to allow you to configure validation rules for certificate server or authority. The outcome of the validation determines whether the certificate server or the authority is trusted.

To define certificate server validation rules, follow these steps:

Procedure

Step 1 When the optional settings appear for the **Certificate Field** and the **Match** columns, click the drop-down arrows and select the desired settings.

Step 2 Enter a value in the Value field.

Step 3 Under Rule, click **Add**.

Step 4 In the Certificate Trusted Authority pane, choose one of the following options:

- Trust Any Root Certificate Authority (CA) Installed on the OS—If chosen, only the local machine or certificate stores are considered for the server's certificate chain validation.
- Include Root Certificate Authority (CA) Certificates.

Note
If you choose Include Root Certificate Authority (CA) Certificates, you must click **Add** to import the CA certificate into the configuration. If the certificate being used is being exported from the Windows certificate store, use the "Base 64 encoded X.509 (.cer)" option.

Network Groups Window

In the Network Groups window, you assign network connections to particular groups. Classifying connections into groups provides multiple benefits:

- Improved user experience when attempting to make a connection. When multiple hidden networks are configured, the client walks through the list of hidden networks in the order that they are defined until a successful connection is made. In such instances, groups are used to greatly reduce the amount of time needed to make a connection.
- Easier management of configured connections. Enables you to separate administrator networks from user networks if you want and allows users who have multiple roles in a company (or who often visit the same area) to tailor the networks in a group to make the list of selectable networks more manageable.

Networks defined as part of the distribution package are locked, preventing the user from editing the configuration settings or removing the network profiles.

You can define a network as global. When doing so, it appears in the Global Networks section. This section is split between the wired and wireless network types. You can perform only sort order edits on this type of network.

All non-global networks must exist in a group. One group is created by default, and the user can delete that group if all networks are global.

Procedure

Step 1 Choose a group by selecting it from the drop-down list.

Step 2 Choose **Create networks** to allow the end user to create networks in this group. When deployed, if you uncheck this, Network Access Manager deletes any user-created networks from this group, which may force the user to re-enter network configuration in another group.

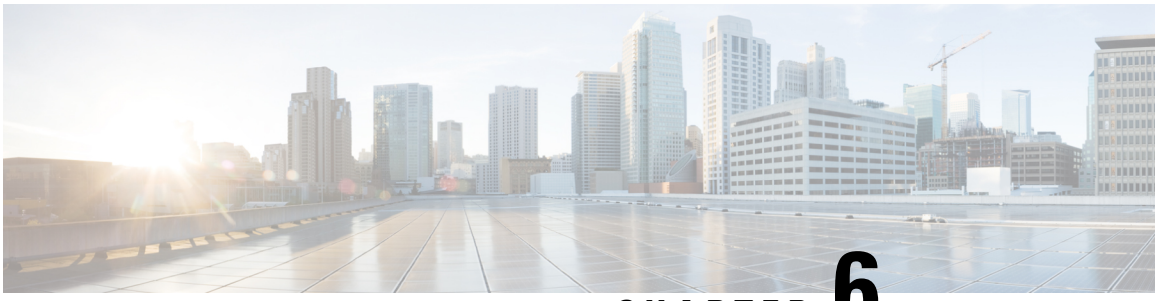
Step 3 Choose **See scan list** to allow end users to view the scan list when the group is selected as the active group using the Cisco Secure Client GUI. Alternatively, clear the check box to restrict users from viewing the scan list. For instance, if you want to prevent users from accidentally connecting to nearby devices, you should restrict scan list access.

Note
Those settings are applied on a per-group basis.

Step 4 Use the right and left arrows to insert and remove a network from the group selected in the Group drop-down list. If a network is moved out of the current group, it is placed into the default group. When the default group is being edited, you cannot move a network from it (using the > button).

Note
Within a given network, the display name of each network must be unique; therefore, any one group cannot contain two or more networks with the same display name.

Step 5 Use the up and down arrows to change the priority order of the networks within a group.



CHAPTER 6

Configure Posture

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

Secure Firewall Posture is bundled with secure-firewall-posture-<*version*>-k9.pkg, which is the application that gathers what operating system, antivirus, antispyware, and software is installed on the host. ISE Posture deploys one client when accessing ISE-controlled networks, rather than deploying both Cisco Secure Client and the NAC Agent. ISE Posture is a module you can choose to install as an additional security component into the Cisco Secure Client product.

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

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

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

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

- What ISE Posture Module Provides, on page 206
- Operations That Interrupt Cisco Secure Client ISE Flow, on page 214
- Status of ISE Posture, on page 215
- Script Remediation Messaging, on page 217
- Posture Condition Script, on page 217
- Posture and Multi Homing, on page 217
- Simultaneous Users on an Endpoint, on page 218
- Logging for Posture Modules, on page 218
- Posture Modules' Log Files and Locations, on page 218

• ISE Posture Profile Editor, on page 218
• Advanced Panel , on page 221
• What Secure Firewall Posture Module Provides, on page 222
• OPSWAT Support, on page 225

What ISE Posture Module Provides

Posture Checks

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

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

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

Any Necessary Remediation

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

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

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

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

After remediation (or after requirement checks when no remediation was needed), you may get an Acceptable Use Policy notification. It requires you to accept the policy for network access and limits access if you reject

it. During this part of remediation, the Posture tile portion of the Cisco Secure Client UI displays "ISE Posture: Network Acceptable Use Policy."

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

Patch Management Checks and Remediation

Cisco Secure Client with a Patch Management agent provides patch management checks and patch management remediation. It checks the state of patches missing on the endpoint. If no patches are missing on the endpoint, the patch management check passes. You can use the Patch Management agent to install the missing patches, if configured. The ISE server must be trusted for these advanced check and remediation operations. Windows Update Services connectivity is required during the pre-posture phase to validate the Patch Management checks. The same server access is also needed during the quarantine phase for Patch Management remediation.

When the patch management check for Windows is configured on ISE, you should verify that all required patches defined by configured conditions have been installed on the endpoints, and then update the Posture Feed.

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

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

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

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

Reassessment of Endpoint Compliance

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

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

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

Grace Period for Noncompliant Devices

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



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

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

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

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

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

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

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

Flexible Notification

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

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



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

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

Posture CLI for Multiple Connections and Automation Purposes

ISE Posture CLI is installed and available on Windows only when the ISE Posture module is chosen for predeploy or web deploy as part of Cisco Secure Client. Refer to Cisco Secure Client Module Executables for Predeploy and Web Deploy, on page 10 for additional installer deployment details for ISE Posture. With posture CLI, you can have multiple clients connecting to the posture subsystem, and data can be sent to those connected client processes, instead of just one client and one server communicating, which was all the UI process can support.

To run the posture CLI, navigate to where the Cisco Security Client is installed and run **posturecli.exe**. By default the path is C:\Program Files(x86)\Cisco\Cisco Secure Client\. The available commands and their results are provided below. When the commands are executed, the ISE Posture tile of the Secure Client GUI also changes to indicate the various statuses. Refer to Status of ISE Posture, on page 215 for those additional ISE Posture tile updates.

Initiate the Posture Scan

At the ISEPosture> prompt, enter **rescan**. The posture scan will begin.

Verify the State of the Policy Server

At the ISEPosture> prompt, enter **state**. The state of the policy server is provided.

Retrieve ISE Posture Module Statistics

At the ISEPosture> prompt, enter **stats**. The following statistics are returned:

- Current Status—Defines the client device as compliant or non-compliant based on whether the endpoint complies with the ISE headend policies.
- Policy Server—Provides the IP address or name of the policy server.
- Scan Start Time—Provides the latest scan start time.
- Compliance Module Version—Provides the compliance module version.

See What Security Products Are Present

At the ISEPosture> prompt, enter **showproducts**. This command reveals what security products are present for the client.

Get Scan Summary Findings

At the ISEPosture> prompt, enter **showreport**. This command provides the findings of the posture scan summary.

Get the Compliance Module Version

At the ISEPosture> prompt, enter **showcmversion**. This command provides the Compliance Module version.

Disconnect CLI Interface

At the ISEPosture> prompt, enter **exit**. This command disconnects the CLI interface. Any existing posture sessions remain active.

Get Help with ISE Posture CLI Commands

At the ISEPosture> prompt, enter **help** for assistance with CLI commands. For help with a specific command, enter **help <command>**.

Cisco Temporal Agent

The Cisco Temporal Agent is designed for Windows or macOS environments to share compliance status when a user accesses a trusted network. The configuration for the Cisco Temporal Agent is done on the ISE UI. The Cisco Temporal Agent extractable .exe (for Windows) or dmg (for macOS) is downloaded to the endpoint whenever it attempts to access the internet. The users must run the downloaded executable or dmg for the compliance check: no administrator privileges are required.

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

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

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

Limitations of Cisco Temporal Agent

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

- DE—Encryption Location based check

Posture Policy Enhancements for Optional Mode

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

- Manual Remediation of Optional Mode—The ISE Posture Summary screen shows any Optional Mode status that may require remediation if a condition failed. You can manually click Start to remediate or click Skip. Even if the remediation fails, the endpoint would still be compliant since these are only optional requirements. The ISE Posture Summary shows if they are skipped, failed, or successful.
- Automatic Remediation of Optional Mode—You can monitor the ISE Posture tile as it notes when it is applying optional updates. You will not be asked to start remediation because it happens automatically. If any automatic remediation fails, you get a message that remediation could not be attempted. Further, you have a choice to skip the remediation action, if desired.

Visibility into Hardware Inventory

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

Stealth Mode

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

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

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

After you map the profile in the ISE Posture Profile Editor, on page 218 and then map Cisco Secure Client configuration to the Client Provisioning page in ISE, Cisco Secure Client can read the posture profile, set it to the intended mode, and send information related to the selected mode to ISE during initial posture request. Based on the mode and other factors, such as identity group, OS, and compliance module, Cisco ISE matches to the right policy.

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

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

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

Posture Policy Enforcement

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

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

UDID Integration

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

Application Monitoring

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

USB Storage Device Detection

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

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

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

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

Automatic Compliance

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

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

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

VLAN Monitoring and Transitioning

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

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

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

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



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

Troubleshooting

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

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

Operations That Interrupt Cisco Secure Client ISE Flow

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

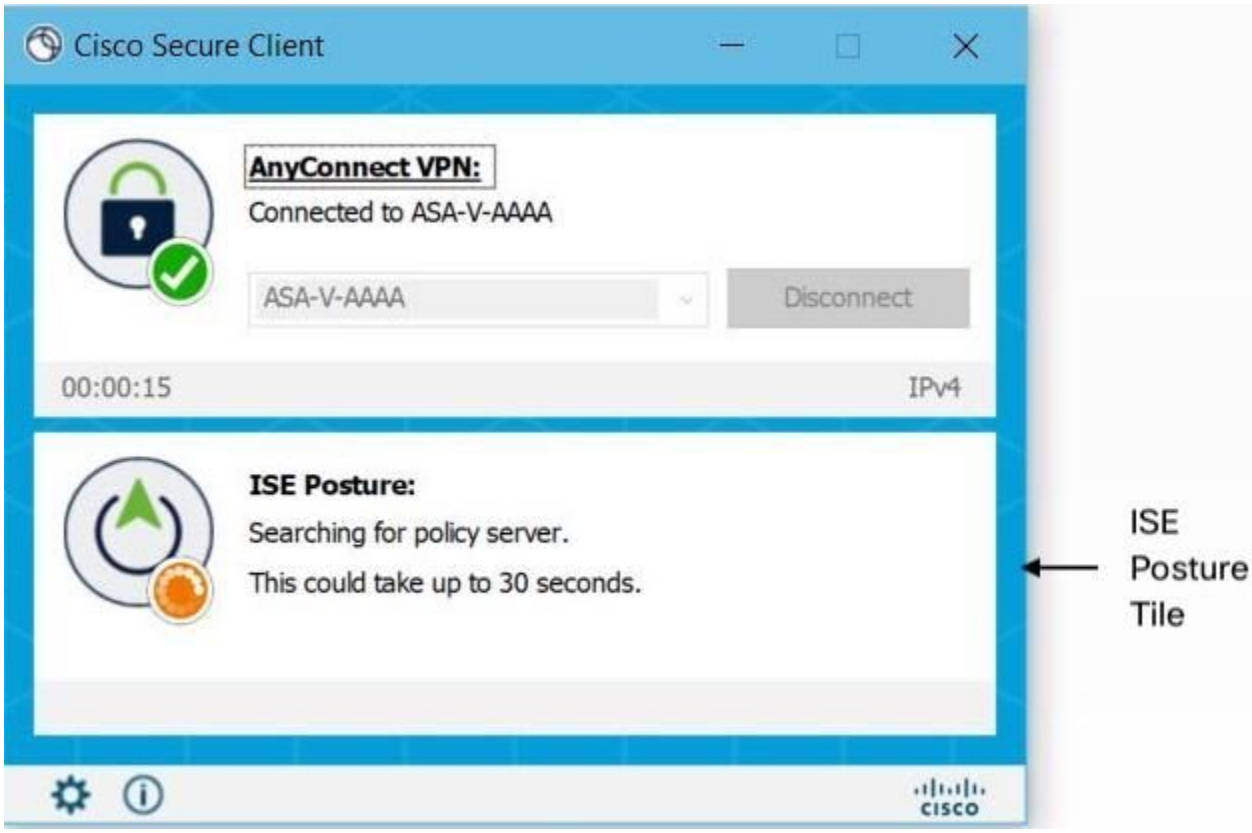
- User Cancels Cisco Secure Client ISE—During the period of posture checking and remediation, the user can cancel Cisco Secure Client ISE. The UI immediately notifies a user that a cancellation is in progress, but it should occur only during a time that avoids putting the endpoint into a questionable state. Some cancellations may require a reboot if third-party software was used. The ISE Posture tile portion of the Cisco Secure Client UI shows the compliance state after the cancellation.
- Remediation Timer Expires—The administrator-controlled time to satisfy posture requirements has expired. An assessment report is sent to the headend. During passive reassessment, the user retains network access, and with posture assessment, network access is granted when all mandatory requirements are satisfied.
- Error During Posture Checking—If an error occurs during the posture checking phase and Cisco Secure Client is able to continue, the user is notified, but posture checking continues, if possible. If the error occurs during a mandatory posture check, the check is marked as failed. Network access is granted if all mandatory requirements are satisfied. If not, the user can restart the posture process.
- Error During Remediation—If an error occurs during the remediation phase and Cisco Secure Client ISE Posture can continue, the user is notified. Cisco Secure Client ISE Posture stops the remediation process

if the failed remediation step is associated with a mandatory posture requirement. If the failed remediation step is associated with an optional posture requirement, it attempts to continue with the next step and finish the ISE Posture operation. Network access is granted if all mandatory requirements are satisfied. If not, the user can restart the posture process.

- Default Gateway Change—A user might lose trusted network access because of a change to the default gateway, causing the ISE Posture to attempt a rediscovery of ISE. The ISE Posture tile portion on the Cisco Secure Client UI displays the status of ISE Posture when it goes into rediscovery mode.
- Loss of Connectivity Between Cisco Secure Client and ISE—After the endpoint is deemed compliant and granted network access, various network scenarios can occur: the endpoint can experience complete loss of network connectivity, ISE could go down, the ISE posture could fail (because of a session timeout, manual restart, or the like), or ISE behind a Secure Firewall ASA may lose the VPN tunnel.
- You cannot have multiple console users logged in on a macOS endpoint when using ISE posture.
- Delays in Initalization and Posture Assessment Flow (macOS only)—Apple advises you to allow their subnet in the pre-posture phase so that failures with signature verification of Compliance Module libraries won't occur.

Status of ISE Posture

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



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

You may also see the following status messages after "ISE Posture" in the ISE Posture tile of the Cisco Secure Client UI:

- Failed to load compliance module—Returned upon entering *state* at the ISEPosture> CLI prompt without the compliance module being loaded.
- Limited or no connectivity—No discovery is occurring because you have no connection. The Cisco Secure Client ISE Posture agent may be performing discovery on the wrong endpoint on the network.
- System scan not required on current Wi-Fi—No discovery is occurring because an unsecured Wi-Fi was detected. The Cisco Secure Client ISE Posture agent only starts discovery on the LAN, on the wireless if 802.1X authentication is used, and on the VPN. The Wi-Fi may be unsecured, or you disabled the feature by setting *OperateOnNonDot1XWireless* to 1 in the agent profile.
- Unauthorized policy server—The host does not match the server name rule of the ISE network so there is limited or no network access.
- The Cisco Secure Client Downloader is performing update...—The downloader is invoked and compares the package versions, downloads the Cisco Secure Client configuration, and performs the necessary upgrades.
- Scanning System...—Scanning for antivirus and antispyware security products has started. If the network is changed during this process, the agent recycles the process of generating the log file, and the status goes back to "No policy server detected."
- Bypassing Cisco Secure Client scan—Your network is configured to use the Cisco NAC agent.
- Untrusted Policy Server Cancelled by the user—When you unblock the connection to untrusted servers in the Cisco Secure Client UI with the ISE Posture Preferences tab, you receive the Cisco Secure Client Downloader's Security Warning in a popup window. When you click **Cancel Connection** on this warning page, the ISE Posture tile changes to this status.

  This message can also occur upon entering *state* at the ISEPosture> CLI prompt, and determining the policy server is untrusted.
- Network Acceptable Use Policy—The access to the network requires that you view and accept the Acceptable Use Policy. Declining the policy may result in limited network access.
- Updating Network Settings—In the ISE UI in Settings > Posture > General Settings, you can specify how many seconds of delay should occur between network transitions.
- Not Compliant. Update time expired.—The time set for remediation has expired.
- Compliant. Network access allowed.—The remediation is complete. The Cisco Secure Client > Scan Summary also shows the status as complete.

  This message can also occur upon entering *state* at the ISEPosture> CLI prompt, and determining the policy server is trusted.
- No policy server detected—The ISE network is not found. After 30 seconds, the agent slows down probing. The default network access takes effect.

Script Remediation Messaging

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

- **Remediation cannot be attempted because the script has an invalid hash**—Appears in the ISE Posture Details when there is a hash mismatch of the downloaded script or if the policy sign verification failed.
- **The script you are trying to run exits with an error**—Appears in the ISE Posture Details when the script exists with a non-zero exit code. On Windows, it might also be that the execution policy that was configurd does not allow for script execution.
- **Remediation was unsuccessful because the script timed out**—Appears in the ISE Posture Details when the script takes longer than the remediation timer to exit. If the script doesn't exit within the remaining remediation timer, Cisco Secure Client stops the script and marks the remediation as failed.
- **Remediation cannot be done because you are connected to an untrusted server**—Appears in the Cisco Secure Client Details when the endpoint is connected to an untrusted ISE server. Either the server certificate is not marked as trusted in the certificate store or you have no fingerprints configured in AnyConnectLocalPolicy.xml. The fingerprints in the certificate presented by ISE must match the ones configured in AnyConnectLocalPolicy.xml.

Posture Condition Script

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

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

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

Posture and Multi Homing

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

Simultaneous Users on an Endpoint

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

Logging for Posture Modules

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

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

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

- libcsd.log—Created by the Cisco Secure Client thread that uses the Secure Firewall Posture API. Debugging entries are made in this log depending on the logging level configuration.
- cscan.log—Created by the scanning executable (cscan.exe) and is the main log for Secure Firewall Posture. Debugging entries are made in this log depending on the logging level configuration.

Posture Modules' Log Files and Locations

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

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

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

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

- (Non-Windows)—.cisco/posture/log
- (Windows)— C:\Users\<user_name>\AppData\Local\Cisco Secure Firewall Posture\log\cscan.log

ISE Posture Profile Editor

An administrator can choose to use the standalone editor to create the posture profile and then upload it to ISE. Otherwise, the embedded posture profile editor is configured in the ISE UI under Policy Elements. When

the Cisco Secure Client configuration editor is launched in ISE, it creates the Cisco Secure Client configuration complete with Cisco Secure Client software and its associated modules, profiles, OPSWAT, and any customization. The standalone profile editor for ISE Posture contains the following parameters:

- **Agent Behavior**
  - **Enable signature check**—If checked, enables signature checking of executables before the agent runs them.
  - **Log file size**—The maximum Compliance Module logs file size. The valid values are 5 to 200 Mb.
  - **Remediation timer**—The time the user has for remediation before being tagged as non-compliant. The valid values are 1 to 300 minutes.
  - **Automated DART Count**—Determine how many automated DART bundles to collect during failure scenarios.
  - **Enable agent log trace**—Enables the debug log on the agent.
  - **Operate on non-802.1X wireless networks**—If checked, enables the agent to operate on non-802.1X wireless networks.
  - **Enable posture non-redirection flow**—If unchecked, posture non-redirection flow is disabled. Make sure that all the NADs support redirection before you disable.
  - **Enable Stealth Mode**—Choose whether to enable Stealth Mode which allows posture to run as a service without user intervention.
  - **Enable Stealth With Notification**—If stealth mode notifications are set to enabled, the end user still gets notification messages when Cisco Secure Client stealth mode is in noncompliant state, has limited network access, has an unreachable server, and so on.
  - **Disable EDR Internet Check**—Definition check failure is observed when the endpoint has a configured proxy. When the endpoint has a configured proxy, it causes any EDR product such as Cortex XDR to fail in reaching the internet. To bypass the internet check and skip the real-time transfer protocol check and the definition check of the endpoint and detection response product (EDR), click this checkbox to set it to Yes.
  - **Enable Rescan Button**—If you want to restart posture (or discovery) after a failure, after manual remediation, or when posture gets stuck (and so on), enable this button so that a **Scan Again** selection appears in the ISE Posture tile. You can show or hide the option in the ISE posture profile. When you click **Scan Again**, the discovery starts, and the entire posture flow is initiated.



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



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

  - **Disable UAC Popup**—Decide whether the Windows User Account Control (UAC) popup appears during policy validation. With the default value (unchecked), the end user continues to be prompted

for administrator privileges when connecting. If you enable, end users will not see a Windows User Account Control (UAC) prompt during policy validation. By turning off the UAC prompt, Secure Firewall Posture uses a system process for privilege escalation instead of "Run as administrator." Validate your posture policies on the device where users have local admin rights before disabling the UAC prompt.

- **Backoff Timer Limit**—Enter the time up to which Cisco Secure Client sends probes for ISE discovery. Because the probes add more traffic, you should choose a value that is not disruptive to your network.
- **Periodic Probe Interval**—Specify a discovery probing interval after the Backoff Timer Limit is crossed. Cisco Secure Client sends the periodic probes with the given interval continuously until a valid ISE server is found. The default is 30 minutes, and after initial rounds of probing, probes are sent in continuous 30 minute intervals. Setting the value to 0 disables periodic probing.
- **Posture State Synchronization Interval**—Enter 0 to disable periodic probing. Valid range is 0 to 300 seconds. You must enable Periodic Reassessment (PRA) in ISE for the Posture State Synchronization interval to function as expected when posture lease is enabled.
- **Posture State Synchronization Probe List**—During discovery phase, the agent sends probes to the backup list to find an ISE server. The default is no value. It uses all packet switch networks as backup servers.
- **Maximum time for CWA/BYOD probing**—If a central web authentication (CWA) or bring-your-own-device (BYOD) flow is configured, the agent will probe the packet switch network up to this number of seconds to determine if the end user has completed the flow. If completed, the agent starts posture flow.
- **Interval of CWA/BYOD probing**—If central web authentication (CWA) or bring-your-own-device (BYOD) flow is configured, the agent will probe the packet switch network in this interval of seconds, until CWA/BYOD flow completes or the maximum time is reached.

- **IP Address Change**

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

  - **VLAN detection interval**—Interval at which the agent checks for VLAN changes before refreshing the client IP address. The valid range is 0 to 900 seconds, and the recommended value is 5 seconds. If set to 0, the VLAN detection feature is disabled. When set from 1 to 900, the agent sends an Internet Control Message Protocol (ICMP) or Address Resolution Protocol (ARP) query every x seconds.
  - **Ping or ARP**—The method for detecting IP address changes. The choices are Ping (0) to poll using ICMP, Arp (1) to poll using ARP, and Ping then Arp (2) to poll using ICMP first, then ARP if ICMP fails. The recommended setting is to poll using ARP because the default gateway might be configured to block ICMP packets.
  - **Maximum timeout for ping**—The ping timeout from 1 to 10 seconds.
  - **Enable agent IP refresh**—Check to enable VLAN change detection.
  - **DHCP renew delay**—The number of seconds the agent waits after an IP refresh. Configure this value when you have Enable Agent IP Refresh enabled. If this value is not 0, the agent will do an IP refresh during this expected transition. If a VPN is detected during the refresh, the refresh will be disabled. The valid values are 0 to 60 seconds, and the recommended value is 5 seconds. Set this parameter to 0 to disable the feature.

- **DHCP release delay**— The number of seconds the agent delays doing an IP refresh. Configure this value when you have Enable Agent IP Refresh enabled. If this value is not 0, the agent will do an IP refresh during this expected transition. If a VPN is detected during the refresh, the refresh will be disabled. The valid values are 0 to 60 seconds, and the recommended value is 5 seconds. Set this parameter to 0 to disable this feature.
- **Network transition delay**—The timeframe (in seconds) for which the agent suspends network monitoring so that it can wait for a planned IP change. The recommended value is 5 seconds.

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

Advanced Panel

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



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

- **Preferences**—Allows you to block connections to untrusted servers so that during the downloader process, you receive an "Untrusted Server Blocked" message for any ISE server that has untrusted certification and is unverified. If you disable the blocking, Cisco Secure Client will not block connections to potentially malicious network devices.

- **Statistics**—Provides current ISE Posture status (compliant or not), OPSWAT version information, the status of the Acceptable Use Policy, the last running time stamp for posture, any missing requirements, and any other statistics deemed important enough to display for troubleshooting purposes.
- **Security Products**—Accesses the list of antimalware products installed on your system.
- **Scan Summary**—Allows the users to see whatever posture items the administrator configured for them to see. For example, when configured, they could see all of the items that have been postured on their system or only the ones that failed the posture check and required remediation.
- **Message History**—Provides a history of every status message sent to the system tray for a component. This history is useful for troubleshooting.

What Secure Firewall Posture Module Provides

Secure Firewall Posture

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

Basic Functionality

Secure Firewall Posture automatically identifies operating systems and service packs on any remote device establishing a Cisco Secure Client VPN client session.

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

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

Secure Firewall Posture also automatically returns the following additional values for evaluation against configured DAP endpoint criteria:

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

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

Endpoint Assessment

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

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

Advanced Endpoint Assessment: AntiMalware and Firewall Remediation

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

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

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

Note If you plan to use the ActiveScan or Last Update check (and have the ActiveScan or Last Update check enabled within the Dynamic Access Policy configuration of the ASDM or FMC headend manager), you must install the Secure Firewall Posture Module. For example, for macOS with predeploy, install cisco-secure-client-macos-*version*-predeploy-k9.dmg or for macOS webdeploy, install cisco-secure-client-macos-*version*-webdeploy-k9.pkg. Installing Secure Firewall Posture modules provides administrator rights to the posture scan, which allows ActiveScan to complete. If you only have the Secure Firewall Posture executables from the ASA or FTD, ActiveScan for antimalware detection using Crowdstrike or Symantec or the like will fail.

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

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

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

Configure Antimalware Applications for Secure Firewall Posture

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

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

Integration with Dynamic Access Policies

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

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

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

BIOS Serial Number in a DAP

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

Specify the BIOS as a DAP Endpoint Attribute

Procedure

Step 1 Log on to ASDM.

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

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

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

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

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

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

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

Step 9 Click **Save**.

How to Obtain BIOS Serial Numbers

- Windows—http://support.microsoft.com/kb/558124

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

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

Determine the Secure Firewall Posture Image Enabled on the Secure Firewall ASA

Open ASDM and choose **Configuration > Remote Access VPN > Posture (for Secure Firewall) > Posture Image**.

Disk Encryption

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

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

Upgrade Secure Firewall Posture

If you are upgrading Cisco Secure Client and Secure Firewall Posture manually (using msiexec), make sure that you first upgrade Cisco Secure Client and then Secure Firewall Posture.

OPSWAT Support

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

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

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

Secure Firewall Posture OPSWAT Support

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

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



Note With an upcoming ASDM release, this menu path will be **Configuration > Remote Access VPN > Posture (for Secure Firewall > Posture Image**, as HostScan has been renamed.

Secure Firewall Posture guidelines:

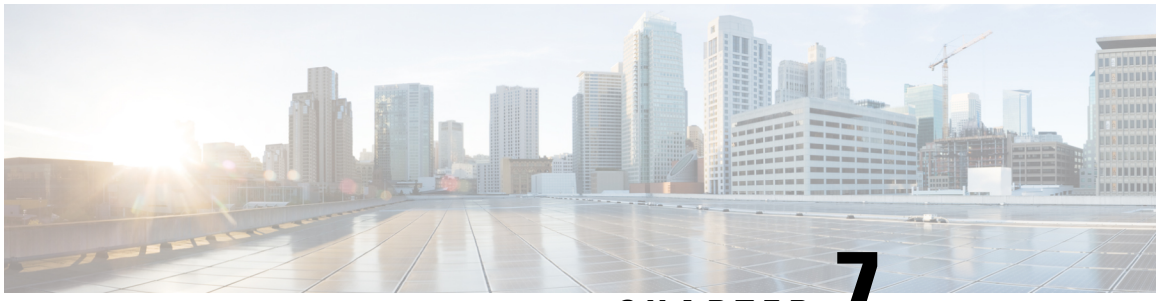
- The version of OPSWAT used in the client and the headend must match.
- All versions of HostScan up through and including 4.3.x use OPSWAT v2. HostScan 4.6x and later use OPSWAT v4. OPSWAT v3 is not supported in any version of HostScan.

ISE Posture OPSWAT Support

Cisco Secure Client Agent Compliance Modules are for the ISE Posture Module.

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

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



CHAPTER 7

Cisco Secure Endpoint Integration

- About Cisco Secure Endpoint, on page 227
- AMP Enabler Deployment, on page 227
- AMP Enabler Profile Editor, on page 227
- Status of AMP Enabler, on page 228

About Cisco Secure Endpoint

AMP Enabler Deployment

Note You can find documentation here for Cisco Secure Endpoint, formerly AMP. Currently Cisco Secure Endpoint integration is available only on Windows. When Cisco Secure Endpoint integration becomes available on macOS with a later 5.x version of Cisco Secure Client, AMP Enabler will no longer be a feature.

With macOS, you can install AMP Enabler without needing system administrator privileges. You will create and configure a policy, create a group, assign the policy to it, and then choose that group when you download the installer.

After you have created policies and assigned them to groups, you can begin deploying the connectors to devices in your organization. AMP Enabler is a macOS-only feature, which is a plugin that lets the connector talk to the cloud when Cisco Secure Client is running.

AMP Enabler Profile Editor

An administrator can choose to use the standalone editor to create the AMP profile and then upload it to Secure Firewall ASA. Otherwise, the embedded profile editor is configured in the ISE UI under Policy Elements or in ASDM. For the trusted local web server to work with the AMP Profile Editor, you must use the key tool command to import the root CA certificate into the JAVA certificate store:

For macOS—sudo keytool-import-keystore [JAVA-HOME]/lib/security/cacerts -storepass changeit -trustcacerts -alias root -file [PATH_TO_THE_CERTIFICATE]/certnew.cer

- Name

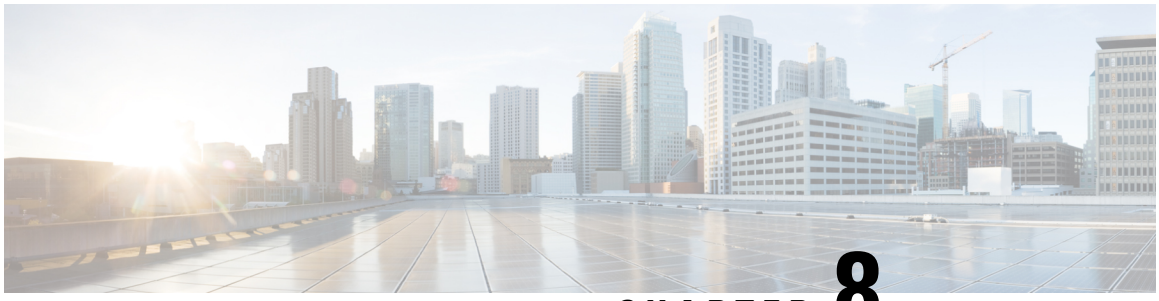
- Description
- Install AMP—Choose if you want to configure this profile to install AMP.
- Uninstall AMP—Choose if you want to configure this profile to uninstall AMP. No input is expected in other fields if uninstall is chosen.
- Mac Installer—Enter the local hosting server address or URL where the .pkg file is located.
- Check—Click to run a check on the URL to ensure it is valid. A valid URL is one that is reachable and contains a certificate that is trusted. If the server is reachable and a connection is established at this URL, you can save the profile.
- Add to Start Menu —Creates Start menu shortcuts.
- Add to Desktop — Creates a desktop icon.
- Add to Context Menu —If you choose this option, you can right click from any file or folder and choose **Scan Now** to activate the scan.

Status of AMP Enabler

Any messages related to the actual download of AMP and the installation appear as a partial tile of the Cisco Secure Client UI. Users see messages when antimalware protection is installing or uninstalling and are given any indications of failure or necessary reboots. After installation, all AMP-related messages are in the AMP UI and not the Cisco Secure Client UI.



Note AMP Enabler is available for Cisco Secure Client on macOS only, as Cisco Secure Client 5.0 for Windows includes a full Cisco Secure Endpoint module, formerly AMP for Endpoints, with a full Secure Client Cloud Management integration. Cisco Secure Client Cloud Management integrates security portofolios and delivers unified visibility (with shared context and metrics), built-in integrations, accelerated threat investigations, and remediation across your security ecosystem. Refer to Secure Client Cloud Management to link your Secure Endpoint account.



CHAPTER 8

Network Visibility Module

- About Network Visibility Module, on page 229
- How to Use Network Visibility Module, on page 232
- Collection Parameters for Network Visibility Module, on page 232
- Network Visibility Module Profile Editor, on page 236
- About Flow Filters, on page 241
- Customer Feedback Module Gives NVM Status, on page 242

About Network Visibility Module

Because users are increasingly operating on unmanaged devices, enterprise administrators have less visibility into what is going on inside and outside of the network. The Network Visibility Module (NVM) collects rich flow context from an endpoint on or off premise and provides visibility into network connected devices and user behaviors when coupled with a Cisco solution such as Cisco Secure Cloud Analytics, Splunk, or a third-party solution. The enterprise administrator can then do capacity and service planning, auditing, compliance, and security analytics. Network Visibility Module provides the following services:

- Monitors application use to enable better informed improvements (expanded IPFIX collector elements in nvzFlow protocol specification: https://developer.cisco.com/site/network-visibility-module/) in network design.
- Classifies logical groups of applications, users, or endpoints.
- Finds potential anomalies to help track enterprise assets and plan migration activities.

This feature allows you to choose whether you want the telemetry targeted as opposed to whole infrastructure deployment. The Network Visibility Module collects the endpoint telemetry for better visibility into the following:

- The device—the endpoint, irrespective of its location
- The user—the one logged into the endpoint
- The application—what generates the traffic
- The location—the network location the traffic was generated on
- The destination—the actual FQDN to which this traffic was intended

When on a trusted network, Cisco Secure Client Network Visibility Module exports the flow records to a collector such as Cisco Secure Cloud Analytics, Splunk, or a third-party vendor, which performs the file analysis and provides a UI interface and reports. The flow records provide information about the capabilities of the user, and the values are exported with ids (such as LoggedInUserAccountType as 12361, ProcessUserAccountType as 12362, and ParentProcessUserAccountType as 12363). For more information about Cisco Endpoint Security Analytics (CESA) built on Splunk, refer to http://www.cisco.com/go/cesa. Since most enterprise IT administrators want to build their own visualization templates with the data, we provide some sample base templates through a Splunk app plugin.

NVM on Desktop Cisco Secure Client

Historically, a flow collector provided the ability to collect IP network traffic as it enters or exits an interface of a switch or a router. It could determine the source of congestion in the network, the path of flow, but not much else. With Network Visibility Module on the endpoint, the flow is augmented by rich endpoint context such as type of device, the user, the application, and so on. This makes the flow records more actionable depending on the capabilities of the collection platform. The exported data provided with Network Visibility Module which is sent via IPFIX is compatible with Cisco NetFlow collectors and Splunk, as well as other 3rd party flow collection platforms. See platform-specific integration documentation for additional information, For example, Splunk integration is available via https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/200600-Install-and-Configure-Cisco-Network-Visi.html.

When using Network Visibility Module Collector in releases 4.9 or later, you must use Splunk app 3.x to view the additional parameters.

The Cisco Secure Client profile for Network Visibility Module gets pushed from the ISE or Secure Firewall ASA headend if this feature is enabled. On the ISE headend, you can use the standalone profile editor, generate the Network Visibility Module service profile XML, upload it to ISE, and map it against the new Network Visibility Module module, just as you do with Network Access Manager. On the Secure Firewall ASA headend, you can use either the standalone or ASDM profile editor.

Network Visibility Module gets notified when the VPN state changes to connected and when the endpoint is in a trusted network.

Note If you are using Network Visibility Module with Linux, make sure that you have completed the preliminary steps in Using Network Visibility Module on Linux, on page 7.

Standalone NVM

For those who do not have Cisco Secure Client deployment or are using another VPN solution, you can install the Network Visibility Module standalone package for your Network Visibility Module needs. This package works independently but provides the same level of flow collection from an an endpoint as the existing Cisco Secure Client Network Visibility Module solution. If you install the standalone Network Visibility Module, the active processes (such as the Activity Monitor on macOS) indicate the use.

Standalone Network Visibility Module is configured with the Network Visibility Module Profile Editor, on page 95, and Trusted Network Detection (TND) configuration is mandatory. Using the TND configuration, Network Visibility Module determines if the endpoint is on the corporate network and then applies the appropriate policies.

Troubleshooting and logging is still done by Cisco Secure Client DART, which can be installed from the Cisco Secure Client package.

Deployment Modes

You can deploy Network Visibility Module 1) with the Cisco Secure Client package or 2) with the Standalone Network Visibility Module package (on Cisco Secure Client desktop only). Refer to the *Deploy Cisco Secure Client* chapter for steps to deploy as part of the Cisco Secure Client package. Otherwise, you can initially install the Standalone Network Visibility Module without the complete Cisco Secure Client package by downloading the following packages:

- cisco-secure-client-win-[version]-nvm-standalone-k9.msi (for Windows)
- cisco-secure-client-macos-[version]-nvm-standalone.dmg (for macOS)
- cisco-secure-client-linux64-[version]-nvm-standalone.tar.gz (for Linux)

Additionally Network Visibility Module is a core part of Cisco XDR. You can send telemetry directly to Cisco XDR without needing an on-premise collector by installing the XDR Default Deployment on your endpoints. Cisco XDR uses this data to create new detections, correlate multiple events into a single incident, and fill invisibility gaps in your network. Within XDR, you can navigate to Client Management > Deployments to see a list of all Secure Client deployments in your Cisco XDR organization and allows users to define a list of all packages and related profiles that must be installed on all computers in a specific deployment within an organization. Refer to XDR documentation for further details.

The Standalone Network Visibility Module does not depend on VPN for its functionining; therefore, you can deploy it on the endpoint without having to install VPN.

If standalone Network Visibility Module is already installed, you can seamlessly migrate to a full Cisco Secure Client installation of the same or higher version, and all Network Visibility Module data files and profiles will be retained.

To upgrade to a Network Visibility Module standalone configuration, you must use an out-of-band method (such as SMS) with an Network Visibility Module profile. If you need both VPN and Network Visibility Module functionality on the endpoint, we recommend that you deploy the Cisco Secure Client package to install both VPN and Network Visibility Module, as a separate installation is not recommended. Installation fails in the following scenarios:

- downgrading standalone Network Visibility Module
- installing an older version of Cisco Secure Client Network Visibility Module where a newer version of standalone Network Visibility Module already existed. This scenario would result in uninstallation of standalone Network Visibility Module.
- installing any version of standalone Network Visibility Module where Cisco Secure Client Network Visibility Module already existed

NVM on Mobile Cisco Secure Client

The Network Visibility Module (NVM) is included in the latest version of the Cisco Secure Client for Android available in the Google Play Store. Network Visibility Module is supported on Samsung devices running Samsung Knox version 2.8 or later. No other mobile devices are currently supported.

Network Visibility Module on Android is part of the service profile configurations. To configure Network Visibility Module on Android, the Cisco Secure Client Network Visibility Module profile is generated by the

Cisco Secure Client Network Visibility Module Profile Editor, and then pushed to the Samsung mobile device using Mobile Device Management (MDM).

Guidelines

- Network Visibility Module is supported on Samsung devices running Samsung Knox version 3.0 or later. No other mobile devices are currently supported.
- On mobile devices, connectivity to the Network Visibility Module Collector is supported over IPv4 or IPv6.
- Data collection traffic on Java based apps is supported.

How to Use Network Visibility Module

You can use Network Visibility Module for the following scenarios:

- To audit a user's network history for potential exfiltration after a security incident occurred.
- To see how system or adminstrative rights impact what network connected processes are running on a user's machine.
- To get a list of all devices running a legacy OS.
- To determine what application in your network is running the highest network bandwidth.
- To determine how many versions of Firefox are being used in your network.
- To determine what percentage of Chrome.exe connections are IPv6 in your network.

Collection Parameters for Network Visibility Module

Of the three syslog data sources: per flow, endpoint identity, and interface info, the Unique Identifier (UDID) field is used as a way to correlate records between these sources. You can use the InterfaceInfoUDID field to correlate a per flow record with an interface info record for collecting details on that specific interface. The following parameters are collected at the endpoint and exported to the collector:

Table 7: Endpoint Identity

Parameter	Description / Notes
Virtual Station Name	Device name configured on the endpoint (for example, Boris-Macbook) Domain joined machines will be in the form <machinename>.<domainname>.<com> (for example, CESA-WIN10-1.mydomain.com) Empty for Android; not provided by Samsung.

Parameter	Description / Notes
UDID	Universally Unique Identifier. Uniquely identifies the endpoint corresponding to each flow. This UDID value is also reported by Secure Firewall Posture in Desktop, and ACIDex in Mobile.
OS Name	Name of the operating system on the endpoint (for example, WinNT)
OS Version	Version of the operating system on the endpoint (for example, 6.1.7601)
OS Edition	The OS edition, such as Windows 8.1 Enterprise Edition
SystemManufacturer	Endpoint manufacturer (for example, Lenovo, Apple, and so on)
System Type	Set to `arm` for Android. `x86` or `x64` for other platforms.
Agent Version	Version of Network Visibility Module client software running on the endpoint. Typically of the form major_v.minor_v.build_no
Timestamp	Absolute timestamp of the endpoint data in milliseconds.
AMP GUID	Unique endpoint ID of Secure Endpoint (AMP)

Table 8: Interface Information

Parameter	Description / Notes
Endpoint UDID	Same as UDID.
InterfaceInfoUID	Unique ID for an interface metadata. Used to look up the interface metadata from the InterfaceInfo records.
Interface Index	The index of the network interface as reported by the OS.
Interface Type	Interface type, such as wired, wireless, cellular, VPN, and so on.
Interface Name	Network interface/adapter name as reported by the OS.
Interface Details List	State and SSID, attributes of InterfaceDetailsList. Indicate the network state of the interface (trusted or untrusted), and the SSID of the connection.
Interface MAC address	MAC address of the interface. Desktop only. Empty for Android (not supported).
Timestamp	Absolute of the interface record in milliseconds.

Table 9: Flow Information

Parameter	Description / Notes
Source IPv4 Address	IPv4 address of the interface from where the flow was generated on the endpoint.
Destination IPv4 Address	IPv4 address of the destination to where the flow was generated from the endpoint.
Source Transport Port	Source port number from where the flow was generated on the endpoint.
Destination Transport Port	Destination port number to where the flow was generated from the endpoint.
Flow Direction	The direction of the flow observed at the endpoint. it is a mandatory parameter collected from the endpoint. The two values are 0:ingress flow or 1:egress flow.
Source IPv6 Address	IPv6 address of the interface from where the flow was generated on the endpoint. Empty for Android (not supported).
Destination IPv6 Address	IPv6 address of the destination to where the flow was generated from the endpoint. Empty for Android (not supported).
Start Sec End Sec	The absolute timestamp of the start or end of the flow in seconds.
Start Msec End Msec	The absolute timestamp of the start or end of the flow in milliseconds.
Flow UDID	Same as UDID.
Logged In User	The logged in username on the physical device, in the form Authority\Principal Empty for Android (not supported).
Logged In User Account Type	Account type of the logged in user. Empty for Android (not supported).
Process ID	Process ID of the process that intitiated the network flow.
Process Name	Name of the executable generating the network flow on the endpoint.
Process Hash	Unique SHA256 hash for the executable generating the network flow on the endpoint.

Parameter	Description / Notes
Process Account	The fully qualified account, in the form Authority\Principle, under whose context the application generating the network flow on the endpoint was executed. Empty for Android (not supported).
Process Account Type	Account type of the process account. Empty for Android (not supported).
Process Path	Filesystem path of the process that intiated the network flow Empty for Android (not supported).
Process args	Command line arguments of the process that intiated the network flow, excluding the process path. Empty for Android (not supported).
Parent Process ID	Process ID of the parent of the process that initated the network flow.
Parent Process Name	Name of the parent process of the application generating the network flow on the endpoint.
Parent Process Hash	Unique SHA256 hash for the executable of the parent process of the application generating the network flow on the endpoint. Set to 0 for Android.
Parent Process Account	The fully qualified account, in the form Authority\Principle, under whose context the parent process of the application generating the network flow on the endpoint was executed. Empty for Android (not supported).
Parent Process Account Type	Account type of the parent process account. Empty for Android (not supported).
Parent Process Path	Filesystem path of the parent of the process that initiated the network flow. Empty for Android (not supported).
Parent Process Args	Command line arguments of the parent of the process that intiated the network flow, excluding the parent process path. Empty for Android (not supported).
DNS Suffix	Configured on the interface associated with the flow on the endpoint.
L4ByteCountIn	The total number of bytes downloaded during a given flow on the endpoint at layer 4, not including L4 headers.

Parameter	Description / Notes
L4ByteCountOut	The total number of bytes uploaded during a given flow on the endpoint at layer 4, not including L4 headers.
Destination Hostname	Actual FQDN that resolved to the destination IP on the endpoint
Interface UID	Same as interface UID in interface information table. Used to identify the interface information for this flow from the interface records sent along with UDID.
Module Name List	List of 0 or more names of the modules hosted by the process that generated the flow. This can include the main DLLs in common containers, such as dllhost, svchost, rundll32, and so on. It can also contain other hosted components, such as the name of the jar file in a JVM. Empty for Android (not supported).
Module Hash List	List of 0 or more SHA256 hashes of the modules associated with the Module Name List. Empty for Android (not supported).
Additional Logged In Users List	(Windows Only) The list of logged in users on the device (other than nzFlowLoggedInUser), each in the form SessionType:AccountType:Authority\Principal. For example, rdp:8001:ACME\JSmith console:0002:<machine>\Administrator During upgrades, by default, this parameter is excluded from being reported: 1) if the profile in the older version of NVM had no Data Collection Policy or an include Data Collection Policy 2) if the profile in the older version of NVM had an exclude Data Collection Policy, and the profile was opened and saved with the 4.10 profile editor. **Note** For non-system processes, this field is empty.
Process Integrity Level	Integrity level defines the trust between process and another object (files, processes, or threads)
Parent Process Integrity Level	Integrity level defines the trust between parent process and another object (files, processes, or threads)
Flow Report Stage	Stage of the flow record. 0: End flow record, 1: Start flow record, and 2: Periodic/Intermediate flow record.

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 Cisco Secure Cloud Analytics 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 Cisco Secure Cloud Analytics applications, refer to the Cisco Secure Cloud Analytics 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: Cisco Secure Client Profile Editor, Preferences (Part 2), on page 81.

- **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.
- **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 Cisco Secure Client release is opened in a later Cisco Secure Client 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.
- **Acceptable Use Policy** (Optional and mobile specific)—Click **Edit** to define an Acceptable Use Policy for mobile devices in the dialog box. Once complete, click **OK**. A maximum of 4000 characters is allowed.

  This message is shown to the user once after Network Visibility Module is configured. The remote user does not have a choice to decline Network Visibility Module activities. The network administrator controls Network Visibility Module using MDM facilities.
- **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 Cisco Secure Client 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.

About Flow Filters

The addition of flow filters extends the current data collection policy from being just field centric, where the action is configured for a given field in each flow. With flow filter, you can create and apply rules to collect or ignore entire flows (as opposed to only particular fields), thus monitoring only the traffic of interest and potentially reducing storage requirements.

Rule Conditions

- A rule is a match only if *all* of the conditions specified in the rule are satisfied when matched against the flow data.
- The first rule that is satisfied is applied on the flow.
- The rest of the data collection policy (include/exclude fields, anonymized fields) is also applied on the flow if it is allowed by the filter policy.
- With instances of multiple rules,
  - No action is taken on the flow if no rule matches the flow data. The default behavior is followed, which is to collect the flow.
  - If a rule matches the flow data, the action specified in that rule of the flow is applied. Subsequent rules are not checked. The order of rules, as designated in the Network Visibility Module Profile Editor, on page 95 Flow Filter Rule parameter, indicates the priority if multiple matches could occur.

Use of Wildcard, CIDR, and Escape Sequence Support

When entering rule conditions, you can define a wider range of field values using wildcard characters or CIDR notations, in the case of IP addresses. Also, you can use certain escape sequences in the field value. For IP fields, the CIDR/slash notation can specify the IP address that the rule should match. For example, "192.30.250.00/16" would match all addresses that have the routing prefix "192.30.0.0" derived by applying

the subnet mask of "255.255.0.0." For text fields, you can use wildcards (* and ?) and escape sequences (*, \?, and \\) to catch a wider range of inputs. For example, logged in user "Jane*" would match all user names that start with "Jane."

Sample Configurations to Achieve Flow Filtering Scenarios

To drop all UDP traffic on a particular port (such as port 53), configure a flow filter rule with type *Ignore* and two conditions:

- Condition 1: Specify that the Flow Protocol *Equals* UDP.
- Condition 2: Specify that the port number *Equals* 53.

To only collect traffic originating from only one particular process (such as Tor Browser), configure a filter rule with type *Ignore* to drop all other flows by adding one condition:

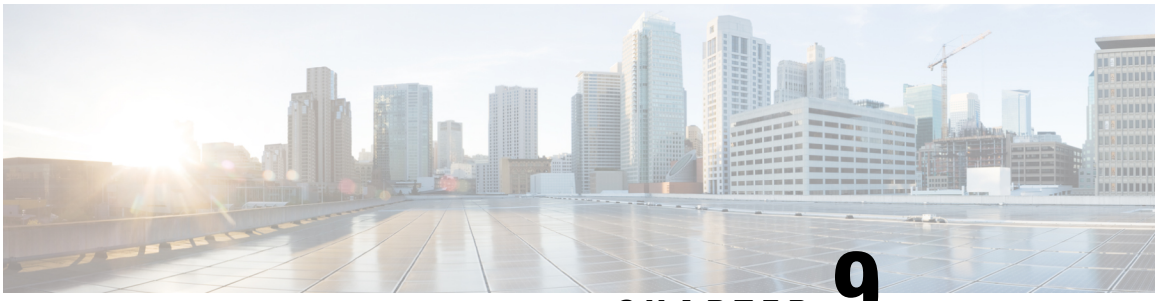
- Condition 1: Specify that the process name *Not Equals* Tor Browser.

To only collect traffic originating from only one particular IP in a subnet, configure two rules:

- Rule 1: Set a rule of type *Collect* with the condition that the IPv4 source address *Equals* 192.168.30.14.
- Rule 2: Set a second rule of type *Ignore* with the condition that the IPv4 source *Equals* 192.168.30.0/24.

Customer Feedback Module Gives NVM Status

Part of the Customer Feedback Module collection provides data about whether Network Visibility Module is installed or not, the number of flows per day, and the DB size.



CHAPTER 9

Umbrella Roaming Security

The Umbrella Roaming Security module requires a subscription to a Umbrella Roaming Security service with either the DNS Security Essentials, DNS Security Advantage, SIG Essentials, or SIG Advantage. Umbrella Roaming Security provides DNS-layer security when no VPN is active, and a Cisco Umbrella subscription adds Intelligent Proxy. Additionally, Cisco Umbrella subscriptions provide content filtering, multiple policies, robust reporting, active directory integration, and much more. The same Umbrella Roaming Security module is used regardless of the subscription.

The Umbrella Roaming Security module profile (OrgInfo.json) associates each deployment with the corresponding service, and the corresponding protection features are enabled automatically.

The Umbrella Dashboard provides real-time visibility into all of the Internet activity originating from the Umbrella Roaming Security module. The level of granularity in policies and reports depends on the Umbrella subscription.

Refer to https://umbrella.cisco.com/products/packages for a detailed comparison of which features are included in which service level subscriptions.

- Umbrella Module for Cisco Secure Client (for Android OS), on page 243
- Umbrella Module for Cisco Secure Client (for Windows or macOS), on page 244

Umbrella Module for Cisco Secure Client (for Android OS)

The Umbrella Module for Cisco Secure Client for Android OS is a roaming client for managed Android devices that provides DNS-layer protection, and this protection extends to both apps and browsing covered by the Android work profile.

A mobile device management system (MDM) is required to deploy this client to Android devices and to push the Umbrella configuration to the Android devices. For a list of supported MDMs and other prerequisites, see Prerequisites for Deploying the Umbrella Module for AnyConnect on Android OS.

Some Cisco Secure Client features may have limitations in functionality with Umbrella on Android:

- Per-app VPN does not work with the Umbrella Module because of an OS restrictions. If remote access VPN is active, Umbrella protection will only apply to DNS traffic that is intercepted by the VPN tunneled. If remote access is configured for per-app VPN, Umbrella protection only applies to DNS traffic for the tunneled applications.
- You should not use always-on VPN with the lockdown (Fail Close) option. It stops the internet access when the VPN server is not reachable. Refer to your MDM guide to turn off the lockdown setting when always-on VPN is set to On.

For an explanation of the complete Umbrella feature set, refer to the Umbrella Module for AnyConnect (Android OS) documentation.

Prerequisites for Deploying the Umbrella Module for Cisco Secure Client on Android OS



Note Cisco Secure Client monitors traffic generated from apps and browsers within the work profile created in an MDM and blocks or allows browsing accordingly. Any traffic generated outside the work profile by apps and/or browsers is not monitored.

- Mobile device management system (MDMs) for deploying the software and pushing the Umbrella configuration to the mobile devices. Current tested versions are Mobile Iron, Meraki, VMWare workspace 1 (Airwatch), or Microsoft Intune.
- Android (Samsung/Google Pixel) mobile devices with Android OS version 6.0.1 and above.
- Umbrella license to configure DNS policies, manage registered Android devices, and for reporting.
- Umbrella organization ID for enabling the feature.
- For Trusted Network Detection (TND):
  - If the Umbrella module detects a virtual appliance (VA) with HTTPS enabled, it deactivates itself; however, if the VA does not support HTTPS, the Umbrella module continues.
  - All VA FQDN in umbrella_va_fqdns must be enabled.

Umbrella Module for Cisco Secure Client (for Windows or macOS)

Obtain Cisco Umbrella Account

The Umbrella dashboard (http://dashboard.umbrella.com/) is the login page where you can obtain the profile (OrgInfo.json) for the Umbrella Roaming Security module to include in your deployment. From there you can also manage policy and reporting for the activity of the roaming client.

Download the OrgInfo File From Dashboard

The OrgInfo.json file is specific information about your Umbrella dashboard instance that lets the Umbrella Roaming Security module know where to report and which policies to enforce.

You must obtain the OrgInfo.json file from the Umbrella dashboard (https://dashboard.umbrella.com) .

Click on **Roaming Computers** in the Identities menu structure and then click the + sign in the upper-left corner of the page. Scroll down to Umbrella Roaming Security Module and click **Module Profile**. Refer to

the Cisco Secure Client Deployment Overview, on page 2 for specific installation/deployment steps and package and file specifics.

Note When you deploy the OrgInfo.json file for the first time, it is copied to the data subdirectory (/umbrella/data), where several other registration files are also created. Therefore, if you need to deploy a replacement OrgInfo.json file, the data subdirectory must be deleted. Alternatively, you can uninstall the Umbrella Roaming Security module (which deletes the data subdirectory) and reinstall with the new OrgInfo.json file.

Get Umbrella Roaming Security Up and Running

When you deploy Cisco Secure Client, the Umbrella Roaming Security module is one of the optional modules that you can include to enable extra features.

To interpret the status and conditions of the Umbrella Roaming Security Module, refer to The AnyConnect Plugin: Umbrella Roaming Security Client Administrator Guide.

Configure the OrgInfo.json File

The OrgInfo.json file contains specific information about your Umbrella service subscription that lets the Umbrella Roaming Security module know where to report and which policies to enforce. You can deploy the OrgInfo.json file and enable the Umbrella Roaming Security module from the Secure Firewall ASA or ISE using CLI or GUI. The steps below describe how to enable from the Secure Firewall ASA first and then how to enable from ISE:

Secure Firewall ASA CLI

1. Upload the OrgInfo.json that you obtained from the Umbrella dashboard (https://dashboard.umbrella.com) to the Secure Firewall ASA file system.
2. Issue the following commands, adjusting the group-policy name as appropriate for your configuration.

```
webvpn
 anyconnect profiles OrgInfo disk0:/OrgInfo.json

group-policy DfltGrpPolicy attribute
 webvpn
  anyconnect profiles value OrgInfo type umbrella
```

ASDM GUI

1. Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
2. Choose **Add**.
3. Give the profile a name.
4. Choose the Umbrella Security Roaming Client type from the Profile Usage drop-down menu. The OrgInfo.json file populates in the Profile Location field.
5. Click **Upload** and browse to the location of the OrgInfo.json file that you downloaded from the dashboard.
6. Associate it with the DfltGrpPolicy at the Group Policy drop-down menu. Refer to Enable Additional Cisco Secure Client Modules, on page 27 to specify the new module name in the group-policy.

ISE

Follow these steps to enable from ISE:

1. Upload the OrgInfo.json from the Umbrella dashboard https://dashboard.umbrella.com.
2. Rename the file OrgInfo.xml.
3. Follow steps in Configure ISE to Deploy Cisco Secure Client, on page 29.

Configure Security Policies and Review the Reports

You must have a Cisco Umbrella account to receive protection, see reporting information, and configure policies. For in-depth explanations, visit https://docs.umbrella.com/product/umbrella/ or https://support.umbrella.com for additional information.

After installation, the Roaming Computer is visible in your Umbrella Dashboard within 90 minutes to 2 hours. Navigating and authenticating to https://dashboard.umbrella.com and then going to **Identities > Roaming Computers** shows a list of Roaming Clients (both active and inactive), as well as details about each installed client.

Initially, a default policy with a base level of security filtering is applied to your Roaming Computers. This Default Policy is found in the Policies section of the dashboard (or Configuration > Policy for Cisco Umbrella accounts).

Reporting for the Roaming Clients is found under the Reports section. Check the Activity Search report to see DNS traffic from computers with the Umbrella Roaming Security module installed and the VPN turned off.

Interpret Diagnostics

You should run a DART report to diagnose any Umbrella Roaming Security module issues. Refer here for instructions on how to run. Refer to Cisco Umbrella Troubleshooting for Umbrella concerns and troubleshooting details.

SWG Debug Logging

By copying an SWGConfigOverride.json file into the SWG folder, you can enable debug logging. If there is a value present for SWGConfig.json, the configuration value in SWGConfigOverride.json will override its log level {"logLevel":"1"} and autotuning {"authtuning:"1"} configurations. The locations of the SWG folder are as follows:

- Windows (Secure Client)— C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG
- macOS (Secure Client)— /opt/cisco/secureclient/umbrella/swg

You will need to restart the SWG service (or Umbrella service) after the override file is copied.

After you have copied the SWGConfigOverride.json file to the appropriate SWG folder, do the following to enable debug logging:

- For macOS—Refer to https://support.umbrella.com/hc/en-us/articles/230561067#Roaming-Client-for-OS-X5 for steps to stop and start the Secure Client agent.

- For Windows—Restart, or stop and start, the Secure Web Gateway (acswgagent in 4.10.x builds /csc_swgagent in 5.x builds) service via the Services MMC snap-in (Start > Run > Services.msc).

Umbrella Roaming Security Module

While the Umbrella Roaming Security module provides DNS layer security, the Cisco Secure Client Umbrella Secure Web Gateway (SWG) Agent module provides a level of security on the endpoint that increases flexibility and potential for more deployment scenarios. Umbrella Secure Web Gateway allows you to authenticate and redirect web traffic securely in both off prem and on prem scenarios. This implementation requires a SIG Essentials or SIG add-on subscription from Umbrella.

The Secure Web Gateway client inserts encrypted headers into HTTP requests, and the headend extracts the header, decrypts it, and uses its user data for identity and policy determination and enforcement. Similarly, for HTTPS traffic, the Secure Web Gateway client initiates HTTP connect requests with the SWG headend, and the connect request carries encrypted headers, which are extracted, decrypted, and used for the identity/ policies determination and enforcement.

By default, Secure Web Gateway intercepts HTTP or HTTPS traffic on ports 80 and 443. You can add non-standard ports (beyond 80 and 443) with Umbrella Cloud configuration. When it is configured, Secure Web Gateway listens for HTTP/HTTPS traffic on these additional ports in addition to the default standard ports.

With Trusted Network Detection, users can choose to inactivate Secure Web Gateway when on a trusted network. When this setting is configured in the Umbrella Cloud, the Secure Web Gateway functionality is disabled if on a trusted network when an AnyConnect VPN tunnel state is active. The Web Protection Status shown in the UI Statistics window reflects any change in the state.



Note Configuring this setting also inactivates Secure Web Gateway in the case of certain errors (such as when the Umbrella Resolvers are unreachable), which are determined by Umbrella's DNS protection state.

Any domain or IP address that should not be proxied can be defined in the Umbrella dashboard under Deployments > Domain Management. Wildcards are not supported, but Umbrella will match any subdomain belonging to a parent domain; for example, if example.com is entered into the domain management list, then www.example.com will also match and be bypassed. You enter IP addresses in the Classless Inter-Domain Routing (CIDR) notation.

If Cisco Secure Client cannot open a connection to an Umbrella proxy, Cisco Secure Client fails open by default, allowing direct access to the user. You cannot configure this hard-coded behavior.

Refer to the Cisco Umbrella SIG User Guide for additional information on all of these Umbrella UI configurations.

Limitations of Secure Web Gateway

- In scenarios where the local host with Cisco Secure Client installed is also configured with a proxy auto-configuration (PAC) file, the PAC file takes priority over Cisco Secure Client.
- Only IPv4 is currently supported.
- Local proxies are not supported.

- After installation, it may take up to 50 minutes for the Umbrella Secure Web Gateway Agent to synchronize with the Umbrella cloud and receive its configuration. However, the default web policy should apply until the synchronization occurs.

Installation and Upgrade for Umbrella SWG

The Cisco Secure Client Umbrella Secure Web Gateway module is available for Windows or macOS only. You have the option to disable VPN functionality and hide the VPN tile on Secure Client's UI. If the AnyConnect VPN is installed with the Cisco Secure Client Umbrella Secure Web Gateway Agent, you must enable the *AllowLocalProxyConnections* setting in the VPN profile.

Both predeploy and web deploy over Secure Firewall ASA or ISE are supported.

Umbrella SWG Log Files and Messages

Umbrella sends the configuration information to the Cisco Secure Client SWG module in the form of a SWGConfig.json file. The config file SWGConfig.json is stored in the following locations:

- Windows—C:\ProgramData (x86)\Cisco\Cisco Secure Client\Umbrella\SWG
- macOS—/opt/cisco/secureclient/umbrella/swg/

Status in Umbrella Roaming Security Tile

You can verify the state of Secure Web Gateway in the Advanced Statistics window. In the Umbrella Roaming Security tile of that window, the Web Protection Status indicates one of the following:

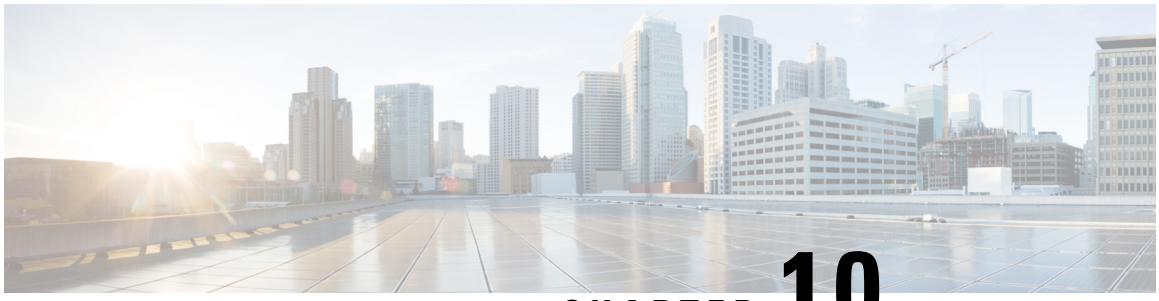
- Disabled—the Umbrella service is down
- Protected—cscswgagent is running
- Unprotected—cscswgagent is not running
- Config Error—incorrect value in SWGConfig.json
- Cloud Service Unavailable—Umbrella proxy not reachable

For detailed statistics on the Umbrella Secure Web Gateway Agent, open the Cisco Secure Client UI and navigate to the Umbrella Roaming Security branch to see the number of HTTP requests redirected to the umbrella proxy, the number of HTTPS requests redirected to the umbrella proxy, the number of requests that we were unable to redirect to proxy, and the Umbrella proxy Cisco Secure Client connected to. Errors and informative messages are logged in the message history.

Troubleshooting Umbrella Secure Web Gateway

When you run a DART bundle, it will include the SWGConfig.json and SWG-related logs if you have Cisco Secure Client Umbrella Roaming Secure Module checked on the Log File Selection window. Go to http://httpbin.org/ip to check if traffic is getting to an Umbrella proxy. If you encounter a connection reset, send an HTTP request to see the response code:

- If the HTTP response code is 452, check if the client's clock is synchronized or if the timestamp is incorrect. A malicious user could be trying to replay the headers.
- If the HTTP response code is 401, the keys are not current. Check the last synchronization time for the device on the Umbrella dashboard.



CHAPTER 10

Cisco Secure Client ThousandEyes Endpoint Agent Module

- About Cisco Secure Client ThousandEyes Endpoint Agent Module, on page 249
- ThousandEyes Endpoint Agent Module Deployment, on page 250

About Cisco Secure Client ThousandEyes Endpoint Agent Module

The Endpoint Agent is an application that collects network- and application-layer performance data when users access specific websites from within monitored networks. It enhances a customers' ability to get a complete picture of their application health, allowing them to make better-informed decisions and to resolve issues quicker. With the installation of ThousandEyes in Secure Client, its version is displayed in the Secure Client About box upon its detection.

Once an Endpoint Agent is installed, it attempts to register with the ThousandEyes service using a secret key and a unique machine ID. Upon successful registration, the Endpoint Agent downloads the latest configuration. When the configuration is up-to-date, the data collection begins with browser-based data and periodic local network probes. The endpoint agent can then measure application performance with scheduled tests, automated session tests, browser sessions, or network access. All of the collected data and metrics are displayed in one expansive view.

Older ThousandEyes versions without the Secure Client presentation plugin cannot be detected.The installer will detect if an Enterprise version of ThousandEyes is installed and will not allow installation while that is present.

The ThousandEyes Endpoint Agent Module is available in Secure Client for Windows 10 and 11 and macOS 10.10 (or later). We do not support ARM64 devices. The current Endpoint Agent version supported is 1.168.2 (or later).

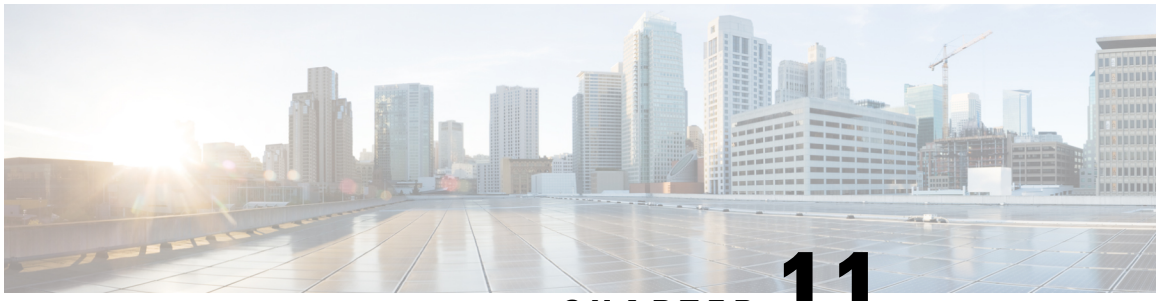
Refer to the Cisco Secure Client ThousandEyes Endpoint Agent Module Integration Guide for additional information.

ThousandEyes Endpoint Agent Module Deployment

As part of the Secure Client zip file contents, a ThousandEyes Module is available with a Windows installer (cisco-secure-client-win-version-thousandeyes-predeploy-k9.msi) or a macOS installer (Cisco Secure Client - ThousandEyes Endpoint Agent-x64-<vers>.pkg). For Windows, you can either extract the installer from the predeploy package or run with the predeploy setup.exe utility. For macOS, refer to Install and Uninstall Cisco Secure Client on macOS.

(Windows only) You can deploy the ThousandEyes json profile (C:\ProgramData\Cisco\Cisco Secure Client\ThousandEyes Endpoint Agent\ThousandEyes Endpoint Agent Configuration.json) with Downloader from VPN or ISE headends.

Installation of AnyConnect VPN is not required for the ThousandEyes Module with Secure Client. Refer to the Deploy Cisco Secure Client chapter and Cisco Secure Client ThousandEyes Endpoint Agent Modulefor additional deployment details.



CHAPTER 11

Enable FIPS in the Local Policy

- About FIPS, NGE, and Cisco Secure Client, on page 251
- Configure FIPS for AnyConnect VPN, on page 254
- Configure FIPS for the Network Access Manager, on page 255

About FIPS, NGE, and Cisco Secure Client

Cisco Secure Client incorporates the Cisco Common Cryptographic Module (C3M). This Cisco SSL implementation includes Federal Information Processing Standard (FIPS) 140-2 compliant cryptography modules and National Security Agency (NSA) Suite B cryptography as part of its Next Generation Encryption (NGE) algorithms.

Next Generation Encryption introduces new encryption, authentication, digital signatures, and key exchange algorithms for escalating security and performance requirements. RFC 6379 defines the Suite B cryptography algorithms that must conform to meet U.S. FIPS 140-2 standards.

Cisco Secure Client components negotiate and use FIPS standard cryptography based on the configuration of the headend, the Secure Firewall ASA or the IOS router. The following Cisco Secure Client client modules support FIPS:

- AnyConnect VPN—FIPS compliance for the VPN client is enabled using a FIPS-mode parameter in the local policy file on the user computer. Suite B cryptography is available for TLS/DTLS and IKEv2/IPsec VPN connections. See Configure FIPS for the AnyConnect Core VPN Client for details and procedures.

  The AnyConnect local policy file, AnyConnectLocalPolicy.xml, contains additional security settings beyond FIPS-mode that apply to the local client. It is not deployed by the Secure Firewall ASA and must be installed manually, or deployed using an enterprise software deployment system. You also have the option to deploy this AnyConnectLocalPolicy.xml file from Secure Client Cloud Management. See The AnyConnect Local Policy for details on using this profile.

- Cisco Secure Client Network Access Manager—FIPS compliance for the Network Access Manager is enabled using the FIPS-mode parameter in the configuration.xml file (located in C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\System directory) and the FIPS-mode parameter in the Network Access Manager profile. FIPS for the Network Access Manager is supported on Windows. See Configure FIPS for the Network Access Manager for details and procedures.

FIPS Features in Cisco Secure Client

Feature	Core VPN Module	Network Access Manager Module
AES-GCM support for symmetric encryption and integrity.	128-, 192-, and 256-bit keys for IKEv2 payload encryption and authentication. ESP packet encryption and authentication.	128-bit and 256-bit keys for 802.1AE (MACsec) for wired traffic encryption in software (Windows).
AES-CBC encryption	128-, 192-, and 256-bit key sizes	128-, 192-, and 256-bit key sizes
SHA-2 support for hashing, SHA with 256/384/512 bits.	IKEv2 payload authentication and ESP packet authentication. (Windows 7 or later and macOS 10.7 or later).	Ability to use certificates with SHA-2 in TLS-based EAP methods.
SHA-1	IKEv2 PRF and integrity/authentication as well as PFS. IPsec/ESP integrity/authentication.	n/a
ECDH support for key exchange.	Groups 19, 20, and 21 IKEv2 key exchange and IKEv2 PFS.	Ability to use ECDH in TLS-based EAP methods (Windows).
MODP for key exchange (in addition to the ECDH support listed above)	Groups 15 and 16	Groups 15 and 16
ECDSA support for digital signature, asymmetric encryption, and authentication, 256-, 384-, 521-bit elliptic curves.	IKEv2 user authentication and server certificate verification.	Ability to use certificates with ECDSA in TLS-based EAP methods.
Pseudo Random Functions	SHA1, SHA256, SHA384, and SHA512	SHA1, SHA256, SHA384, and SHA512
Integrity algorithms	SHA1, SHA256, SHA384, and SHA512	SHA1, SHA256, SHA384, and SHA512
Diffie Hellman	Groups 15, 16, 19, 20, 21 (15 and 16 are the older Modular Exponential (MODP) DH groups, while 19, 20, and 21 are elliptical curve DH groups)	Groups 15, 16, 19, 20, 21 (15 and 16 are the older Modular Exponential (MODP) DH groups, while 19, 20, and 21 are elliptical curve DH groups)
Additional support:	All required crypto algorithms for IPsecV3 except for NULL encryption. RSA certificates with 4096 bit keys for TLS/DTLS and IKEv2.	n/a

[1] On Linux, only the Cisco Secure Client file store is supported for ECDSA. To add certificates to a file store, see .
[2] IPsecV3 also specifies that Extended Sequence Numbers (ESN) must be supported, but Cisco Secure Client does not support ESN.

Cisco Secure Client FIPS Requirements

- Suite B cryptography is available for TLS/DTLS and IKEv2/IPsec VPN connections.
- FIPS and/or Suite B support is required on the secure gateway. Cisco provides Suite B capability on the Secure Firewall ASA version 9.0 and later, and FIPS capability on the Secure Firewall ASA version 8.4.1 and later.
- ECDSA certificate requirements:
  - Must have a Digest strength equal or greater than the Curve strength. For example, an EC-384 key must use SHA2-384 or greater.
  - Support on Windows 7 or later, macOS 10.7 or later, Red Hat Enterprise Linux 6.x or 6.4 (64-bit) or later, and Ubuntu 12.4 and 12.10 (64-bit) or later. ECDSA smart cards are supported only on Windows 7 (and later).

Limitations of Cisco Secure Client FIPS

No EAP methods support SHA-2 except in TLS-based EAP when validating certificates signed using SHA-2.

Guidelines for Cisco Secure Client FIPS

- The Cisco Secure Client Statistics panel (under the Transport Information heading) shows the name of the cipher being used.
- Because AES-GCM is computationally intensive algorithms, you may experience a lower overall data rate when using these algorithms. Some processors contain special instructions specifically introduced to improve the performance of AES-GCM. Cisco Secure Client automatically detects whether the processor on which it is running supports these new instructions. If so, Cisco Secure Client uses the new instructions to significantly improve VPN data rates as compared to those processors that do not have the special instructions. Contact your CPU manufacturer to determine which models of their CPUs support AES-GCM optimization.
- Combined-mode encryption algorithms, where both encryption and integrity verifications are performed in one operation, are supported only on SMP ASA gateways with hardware crypto acceleration (such as 5585 and 5515-X). AES-GCM is the combined-mode encryption algorithm that Cisco supports.

Note An IKEv2 policy can include either a normal- or a combined-mode encryption algorithm, but not both types. When a combined-mode algorithm is configured in the IKEv2 policy, all normal-mode algorithms are disabled, so the only valid integrity algorithm is NULL.

The IKEv2 IPsec proposals use a different model and can specify both normal- and combined-mode encryption algorithms in the same proposal. With this usage, you are required to configure integrity algorithms for both, which leaves a non-NULL integrity algorithm configured with AES-GCM encryption.

- When the Secure Firewall ASA is configured with a different server certificate for SSL and IPsec, use trusted certificates. A Posture Assessment or Downloader failure can occur if using Suite B (ECDSA) untrusted certificates having different IPsec and SSL certificates.

Avoiding Endpoint Problems from Cisco Secure Client FIPS Registry Changes

Enabling FIPS for the AnyConnect VPN changes Windows registry settings on the endpoint. Other components of the endpoint may detect that AnyConnect VPN has enabled FIPS. For example, the Microsoft Terminal Services client Remote Desktop Protocol (RDP) will not work, because RDP requires that servers use FIPS compliant cryptography.

To avoid these problems, you can temporarily disable FIPS encryption in the Windows Local System Cryptography settings by changing the parameter *Use FIPs compliant algorithms for encryption, hashing, and signing* to Disabled. Be aware that rebooting the endpoint device changes this setting back to enabled.

AnyConnect VPN sets the FIPSAlgorithmPolicy value to 1 in the Windows registry key HKLM\System\CurrentControlSet\ Control\Lsa. Note that disabling FIPS mode in the AnyConnect local policy file does not cause AnyConnect VPN to alter the FIPSAlgorithmPolicy value.

Configure FIPS for AnyConnect VPN

Enable FIPS for AnyConnect VPN

Procedure

Step 1 Open or create a VPN Local Policy profile in the Cisco Secure Client Profile Editor - VPN Local Policy.

Step 2 Select **FIPS Mode**.

Step 3 Save the VPN Local Policy profile.

We recommend that you name the profile to indicate that FIPS is enabled.

Enable FIPS During Windows Installation

For Windows installations, you can apply a Cisco MST file to the standard MSI installation file to enable FIPS in the AnyConnect Local Policy. For information about where you can download this MST file, see the licensing information you received for FIPS. The installation generates an AnyConnect Local Policy file with FIPS enabled. Update the user's system after running this utility.



Note This MST only enables FIPS. It does not change other parameters. To change other local policy settings during Windows installation, see Enable Local Policy Parameters in an MST File.

Configure FIPS for the Network Access Manager

The Network Access Manager can be configured to connect to both FIPS and non-FIPS networks simultaneously, or to FIPS networks only.

Procedure

Step 1 Enable FIPS for the Network Access Manager, page 9-5.

Enabling FIPS allows the Network Access Manager to connect to both FIPS and non-FIPS networks.

Step 2 If desired, Enforce FIPS Mode for the Network Access Manager, page 9-6.

Enforcing FIPS mode restricts the Network Access Manager connections to FIPS networks only.

Enable FIPS for the Network Access Manager

Enable FIPs mode in the Cisco Secure Client Network Access Manager client profile. For Windows 10 and 11, you must enable FIPS on your operating system to be FIPS compliant, besides just enabling FIPS for the Network Access Manager.

Procedure

Step 1 Open or create a Network Access Manager profile in the Cisco Secure Client Profile Editor.

Step 2 Select the **Client Policy** configuration window.

Step 3 Under the **Administrative Status** section select **Enable** for **FIPS Mode**.

Step 4 Save the Network Access Manager profile as configuration.xml.

Enforce FIPS Mode for the Network Access Manager

Force enterprise employees to only connect to FIPS-compliant networks by restricting the allowed association and encryption modes, and the authentication methods in the Network Access Manager profile.

You must first Enable FIPS for the Network Access Manager to enforce FIPS mode.

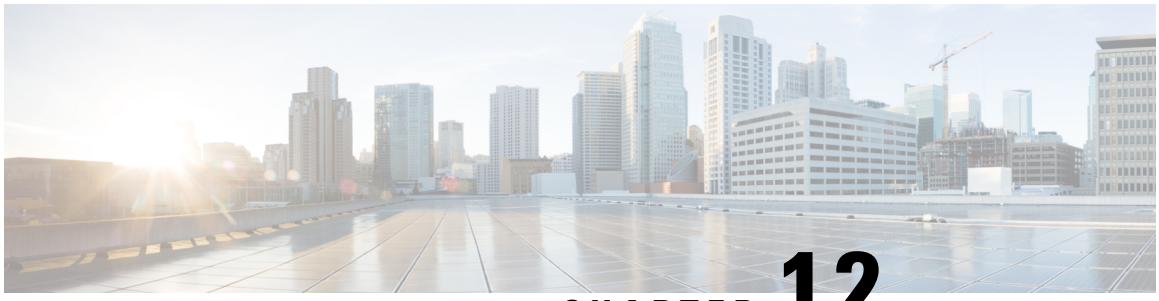
Procedure

Step 1 Open your Network Access Manager profile in the Cisco Secure Client Profile Editor.

Step 2 Network Access Manager FIPS compliance requires FIPS-approved AES encryption modes including WPA2 Personal (WPA2-PSK) and WPA2 Enterprise (802.1X).

Step 3 The Network Access Manager FIPS support includes EAP methods EAP-TLS, EAP-TTLS, PEAP, EAP-FAST and LEAP.

Step 4 Save the Network Access Manager profile as configuration.xml.



CHAPTER 12

Cisco Secure Client on Mobile Devices

Cisco Secure Client on mobile devices is similar to Cisco Secure Client on Windows, macOS, and Linux platforms. This chapter provides device information, configuration information, support information, as well as other administrative tasks specific to Cisco Secure Client for mobile devices.

- Cisco Secure Client Operation and Options on Mobile Devices, on page 257
- Cisco Secure Client on Android Devices, on page 264
- Cisco Secure Client on Apple iOS Devices, on page 274
- Cisco Secure Client on Chrome OS Devices, on page 279
- Cisco Secure Client on Universal Windows Platform, on page 280
- Configure Mobile Device VPN Connectivity on the Secure Firewall ASA Gateway, on page 280
- Configure Per-App VPN, on page 282
- Configure Mobile Device Connections in the Cisco Secure Client VPN Profile, on page 287
- Automate Cisco Secure Client Actions Using the URI Handler, on page 289
- Troubleshoot Cisco Secure Client on Mobile Devices, on page 296

Cisco Secure Client Operation and Options on Mobile Devices

About Cisco Secure Client Mobile VPN Connections

This release of the Cisco Secure Client is available on the following mobile platforms:

- Android
- Apple iOS
- Chromebook
- Windows Phone

Cisco Secure Client is provided on the app store for each supported platform. It is not available on www.cisco.com or distributed from a secure gateway.

Cisco Secure Client mobile apps contain the core VPN client only. They do not include other Cisco Secure Client modules such as the Network Access Manager or Posture (Secure Firewall Posture or ISE Posture). Posture information, referred to as Mobile Posture, is provided to the headend using AnyConnect Identifier Extensions (ACIDex) when the VPN is connecting.

Cisco Secure Client VPN connection can be established in one of the following ways:

- Manually by a user.
- Manually by the user when they click an automated connect action provided by the administrator (Android and Apple iOS only).
- Automatically by the Connect On-Demand feature (Apple iOS only).

Cisco Secure Client VPN Connection Entries on Mobile Devices

A connection entry identifies the address of the secure gateway by its fully qualified domain name or IP address, including the tunnel group URL if required. It can also include other connection attributes.

Cisco Secure Client supports multiple connection entries on a mobile device addressing different secure gateways and/or VPN tunnel groups. If multiple connection entries are configured, it is important that the user knows which one to use to initiate the VPN connection. Connection entries are configured in one of the following ways:

- Manually configured by the user. See the appropriate platform user guide for procedures to configure a connection entry on a mobile device.
- Added after the user clicks a link provided by the administrator to configure connection entries.

  See Generate a VPN Connection Entry, on page 289 to provide this kind of connection entry configuration to your users.
- Defined by the Cisco Secure Client VPN Client Profile.

  The Cisco Secure Client VPN Client Profile specifies client behavior and defines VPN connection entries. For details refer to Configure Mobile Device Connections in the Cisco Secure Client VPN Profile, on page 287.

Tunneling Modes

Cisco Secure Client can operate in a managed or an unmanaged BYOD environment. VPN tunneling in these environments operates exclusively in one of the following modes:

- System-tunneling mode—The VPN connections are used to tunnel all data (full-tunneling), or only data flowing to and from particular domains or addresses (split-tunneling). This mode is available on all mobile platforms.
- Per-App VPN mode—The VPN connection is used for a specific set of apps on the mobile device (Android and Apple iOS only).

  Cisco Secure Client allows the set of apps defined by the administrator on the headend. This list is defined using the Secure Firewall ASA Custom Attributes mechanism. This list is sent to Cisco Secure Client and enforced on the device. For all other apps, data is sent outside of the tunnel or in the clear.

  On Apple iOS, a managed environment is required to run in this mode. On Android, both managed and unmanaged environments are supported. On both platforms, in a managed environment, the Mobile Device Manager must also configure the device to tunnel the same list of apps that Cisco Secure Client is configured to tunnel.
- Multi-tunnel—Cisco Secure Client on iOS supports multiple tunnels with the following patterns:

- One regular (without Per-App) VPN tunnel and one or more Per-App tunnels connected at a time
- Multiple Per-App VPN tunnels connected at a time

Refer to Multiple Tunnel for iOS, on page 259 for additional information.

Cisco Secure Client operates in the mode determined by the configuration information received from the Secure Firewall ASA headend: specifically, the presence or absence of a Per-App VPN list in the Group Policy or Dynamic Access Policy (DAP) associated with the connection. If the Per-App VPN list is present, Cisco Secure Client operates in Per-App VPN mode; if it is absent, Cisco Secure Client operates in system-tunneling mode.

Multiple Tunnel for iOS

A user can only manually start a VPN connection for one tunnel (either without per-app VPN or with per-app VPN). Because per-app VPN automatically starts with the associated application, you must add a **MultiTunnel** key and set it as **true** in VendorConfig of the MDM VPN profile to use multi-tunnel.

In the iOS Cisco Secure Client home screen, you will see a table showing the selected tunnel, regardless of whether it is connected or not. A second table is dynamic and only appears when per-app VPN is connected. This second table only shows the connection status of per-app tunnels, until the user clicks **Status** to see Detailed Statistics of the connection with bytes received and sent.

You can refer to Diagnostics for a log of the currently selected regular VPN. When a user decides to share logs, the log package includes all VPN debug log files for the connected VPN configurations.

Secure Gateway Authentication on Mobile Devices

Block Untrusted Servers

When establishing a VPN connection, Cisco Secure Client uses the digital certificate received from the secure gateway to verify the server's identify. If the server certificate is invalid (there is a certificate error due to an expired or invalid date, wrong key usage, or a name mismatch), or if it is untrusted (the certificate cannot be verified by a Certificate Authority), or both, the connection is blocked. A blocking message displays, and the user must choose how to proceed.

The **Block Untrusted Servers** application setting determines how Cisco Secure Client reacts if it cannot identify the secure gateway. This protection is ON by default; it can be turned OFF by the user, but this is not recommended.

When **Block Untrusted Servers** is ON, a blocking **Untrusted VPN Server** notification alerts the user to this security threat. The user can choose:

- **Keep Me Safe** to terminate this connection and remain safe.
- **Change Settings** to turn the Block Untrusted Servers application preference OFF, but this is not recommended. After the user disables this security protection, they must reinitiate the VPN connection.

When **Block Untrusted Servers** is OFF, a non-blocking **Untrusted VPN Server** notification alerts the user to this security threat. The user can choose to:

- **Cancel** the connection and remain safe.
- **Continue** the connection, but this is not recommended.

- **View Details** of the certificate to visually determine acceptability.

  If the certificate that the user is viewing is valid but untrusted, the user can:

  - Import the server certificate into the Cisco Secure Client certificate store for future use and continue the connection by selecting **Import and Continue**.

    Once this certificate is imported into the Cisco Secure Client store, subsequent connections made to the server using this digital certificate are automatically accepted.

  - Go back to the previous screen and choose **Cancel** or **Continue**.

  If the certificate is invalid, for any reason, the user can only return to the previous screen and choose **Cancel** or **Continue**.

Leaving the Block Untrusted Servers setting ON (default setting), having a valid and trusted server certificate configured on your secure gateway, and instructing your mobile users to always choose **Keep Me Safe** is the safest configuration for VPN connectivity to your network.



Note **Strict Certificate Trust** overrides this setting, see description below.

OCSP Revocation

Cisco Secure Client supports OCSP (Online Certificate Status Protocol). This allows the client to query the status of individual certificates in real time by making a request to the OCSP responder and parsing the OCSP response to get the certificate status. OCSP is used to verify the entire certificate chain. There is a five second timeout interval per certificate to access the OCSP responder.

The user can enable or disable OCSP verification in the Cisco Secure Client settings activity. We have also added new APIs in our framework which can be used by MDM administrators to control this feature remotely. Currently we support Samsung and Google MDM.

Strict Certificate Trust

If enabled by the user, when authenticating remote security gateways, Cisco Secure Client disallows any certificate that it cannot verify. Instead of prompting the user to accept these certificates, the client fails to connect to security gateways.



Note This setting overrides **Block Untrusted Server**.

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 with Cisco Secure 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, Cisco Secure 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.

Client Authentication on Mobile Devices

To complete a VPN connection, the user must authenticate by providing credentials in the form of a username and password, a digital certificate, or both. The administrator defines the authentication method on the tunnel group. For the best user experience on mobile devices, Cisco recommends using multiple Cisco Secure Client connection profiles depending on the authentication configuration. You will have to decide how best to balance user experience with security. We recommend the following:

- For AAA-based authentication tunnel groups for mobile devices, the group policy should have a very long idle timeout, such as 24 hours, to let the client remain in a reconnecting state without requiring the user to re-authenticate.
- To achieve the most transparent end user experience, use certificate-only authentication. When a digital certificate is used, a VPN connection is established without user interaction.

In order to authenticate the mobile device to the secure gateway using a certificate, end users must import a certificate onto their device. This certificate is then available for automatic certificate selection, or it can be associated with a particular connection entry manually. Certificates are imported using the following methods:

- Imported manually by the user. See the appropriate user guide for procedures to import certificates to your mobile device.
- Using SCEP. See Configure Certificate Enrollment, on page 153 for additional details.
- Added after the user clicks a link provided by the administrator to import a certificate.

  See Import Certificates, on page 295 to provide this kind of certificate deployment to your users.

Localization on Mobile Devices

Cisco Secure Client for Android and Apple iOS supports localization, adapting the Cisco Secure Client user interface and messages to the user's locale.

Prepackaged Localization

The following language translations are included in the Cisco Secure Client Android and Apple iOS apps:

- Canadian French (fr-ca)
- Chinese (Taiwan) (zh-tw)
- Czech (cs-cz)
- Dutch (nl-nl)
- French (fr-fr)
- German (de-de)
- Hungarian (hu-hu)
- Italian (it-it)

- Japanese (ja-jp)
- Korean (ko-kr)
- Latin American Spanish (es-co)
- Polish (pl-pl)
- Portuguese (Brazil) (pt-br)
- Russian (ru-ru)
- Simplified Chinese (zh-cn)
- Spanish (es-es)

Localization data for these languages is installed on the mobile device when Cisco Secure Client is installed. The locale specified on your mobile device determines the displayed language. Cisco Secure Client uses the language specification, then the region specification, to determine the best match. For example, after installation, a French-Switzerland (fr-ch) locale setting results in a French-Canadian (fr-ca) display. Cisco Secure Client UIs and messages are translated when Cisco Secure Client starts.

Downloaded Localization

For languages not in the Cisco Secure Client package, administrators add localization data to the Secure Firewall ASA to be downloaded to the device upon AnyConnect VPN connectivity.

Cisco provides the anyconnect.po file, including all localizable Cisco Secure Client strings, on the product download center of Cisco.com. Cisco Secure Client administrators download the anyconnect.po file, provide translations for the available strings, and then upload the file to the Secure Firewall ASA. Cisco Secure Client administrators that already have an anyconnect.po file installed on the Secure Firewall ASA will download this updated version.

Initially, the Cisco Secure Client user interface and messages are presented to the user in the installed language. When the device user establishes the first connection to the Secure Firewall ASA, Cisco Secure Client compares the device's preferred language to the available localization languages on the Secure Firewall ASA. If Cisco Secure Client finds a matching localization file, it downloads the localized file. Once the download is complete, Cisco Secure Client presents the user interface and user messages using the translated strings added to anyconnect.po file. If a string was not translated, Cisco Secure Client presents the default English strings.

See Import Translation Tables to the Secure Firewall ASA, on page 53 for instructions on configuring localization on an Secure Firewall ASA. If the Secure Firewall ASA does not contain localization data for the device's locale, the preloaded localization data from the Cisco Secure Client application package continues to be used.

More Ways to Provide Localization on Mobile Devices

Localize the Cisco Secure Client UI and Messages, on page 296 by providing a URI link to the user.

Ask your mobile device users to manage localization data on their own device. See the appropriate User Guide for procedures to perform the following localization activities:

- Import localization data from a specified server. The user chooses to import localization data and specifies the address of the secure gateway and the locale. The locale is specified per ISO 639-1, with the country code added if applicable (for example, en-US, fr-CA, ar-IQ, and so on). This localization data is used in place of the prepackaged, installed localization data.

- Restore default localization data. The use of the preloaded localization data is restored from the Cisco Secure Client package and all imported localization data is deleted.

VPN Authentication Using SAML

SAML 2.0 support was added to mobile devices in the following releases. When SAML authentication is used, it applies to the Cisco Secure Client session only. It does not apply to web sites, browser-initiated SAML logins, or installed applications. To provide a seamless reconnect without disruption, Cisco Secure Client intentionally skips the repeating of the SAML authentication process. Additionally, if the user logs out of the IdP using a browser, the Cisco Secure Client session remains intact.

- iOS—version 4.6; SAML plus client certificate in version 4.8
- Android—version 4.6; SAML plus client certificate in version 4.8
- Android app on ChromeOS
- ChromeOS Flex 135

Follow these guidelines when using SAML:

- If you are using always-on VPN in failover mode, external SAML IdP is not supported (however, with internal SAML IdP, the Secure Firewall ASA proxies all traffic to IdP and is supported)
- Untrusted server certificates are not allowed in the embedded browser.
- The embedded browser SAML integration is not supported in CLI or SBL modes.
- (Mobile only) Single logout is not supported.
- SAML authentication established in a web browser is not shared with Cisco Secure Client and vice versa.
- Depending on the configuration, various methods are used when connecting to the headend with the embedded browser. For example, while Cisco Secure Client might prefer an IPv4 connection over an IPv6 connection, the embedded browser might prefer IPv6, or vice versa. Similarly, Cisco Secure Client may fall back to no proxy after trying proxy and getting a failure, while the embedded browser may stop navigation after trying proxy and getting a failure.
- You must synchronize the Network Time Protocol (NTP) server on the Secure Firewall ASA with your IdP NTP server in order to use the SAML feature.
- The VPN Wizard on ASDM does not currently support SAML configurations.
- The SAML IdP *NameID* attribute determines the user's username and is used for authorization, accounting, and VPN session database.
- You should set Auto Reconnect to *ReconnectAfterResume* in the Cisco Secure Client Profile Editor, Preferences (Part 1), on page 76 if you want users to re-authenticate with the Identity Provider (IdP) every time they establish a VPN session via SAML.
- Since Cisco Secure Client with the embedded browser uses a new browser session on every VPN attempt, users must re-authenticate every time, if the IdP uses HTTP session cookies to track logon state. In this case, the *Force Re-Authentication* setting in **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers** > has no effect on Cisco Secure Client initiated SAML authentication.

Refer to the *SAML 2.0* section in the appropriate release, 9.7 or later, of the Cisco ASA Series VPN CLI or ASDM Configuration Guide for additional configuration details.

Import Translation Tables to the Secure Firewall ASA

Procedure

Step 1 Download the desired translation table from www.cisco.com.

Step 2 In ASDM go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Customization/Localization** > **GUI Text and Messages**.

Step 3 Click **Import**. The Import Language Localization Entry window displays.

Step 4 Choose the appropriate Language from the drop-down list.

Step 5 Specify where the translation table will be imported from.

Step 6 Click **Import Now**. This translation table will be deployed to Cisco Secure Client clients with this preferred language. Localization will be applied after Cisco Secure Client restarts and connects.

FIPS and Suite B Cryptography on Mobile Devices

Cisco Secure Client for mobile devices incorporates Cisco Common Cryptographic Module (C3M), the Cisco SSL implementation which includes FIPS 140-2 compliant cryptography modules and NSA Suite B cryptography as part of its Next Generation Encryption (NGE) algorithms. Suite B cryptography is available for IPsec VPNs only; FIPS-compliant cryptography is available for both IPsec and SSL VPNs.

Use of cryptography algorithms is negotiated with the headend while connecting. Negotiation is dependent on the capabilities of both ends of the VPN connection. Therefore, the secure gateway must also support FIPS-compliant and Suite B cryptography.

The user configures Cisco Secure Client to accept only NGE algorithms during negotiation by enabling **FIPS Mode** in the Cisco Secure Client app settings. When FIPS Mode is disabled, Cisco Secure Client also accepts non-FIPS cryptography algorithms for VPN connections.

Additional Mobile Guidelines and Limitations

- Apple iOS 5.0 or later is required for Suite B cryptography; this is the minimum Apple iOS version that supports ECDSA certificates used in Suite B.
- Android 4.4 (KitKat) or later is required for Suite B cryptography; this is the minimum Android version that supports ECDSA certificates used in Suite B.
- A device that is running in FIPS mode is not compatible with using SCEP to provide mobile users with digital certificates by proxy method or legacy method. Plan your deployment accordingly.

Cisco Secure Client on Android Devices

Refer to Release Notes for Cisco Secure Client, for Android for features and updates by release.

Refer to the Cisco Secure Client Mobile Platforms and Feature Guide for features and devices supported by this release.

Guidelines and Limitations for Cisco Secure Client on Android

- The Secure Firewall ASA does not provide distributions and updates for Cisco Secure Client for Android. They are available on Google Play. The APK (package) file for the latest version is also posted on Cisco.com.
- Cisco Secure Client for Android supports only the Network Visibility Module and Umbrella; it does not support any other Secure Client modules.
- The Android device supports no more than one Cisco Secure Client profile, which is the last one received from a headend. However, a profile can consist of multiple connection entries.
- If users attempt to install Cisco Secure Client on devices that are not supported, they receive the pop-up message `Installation Error: Unknown reason -8`. This message is generated by the Android OS.
- With users who have Cisco Secure Client in a widget on their home screen, the Cisco Secure Client services are automatically started (but not connected) regardless of the "Launch at startup" preference.
- Cisco Secure Client for Android requires UTF-8 character encoding for extended ASCII characters when using pre-fill from client certificates. The client certificate must be in UTF-8 if you want to use prefill, per the instructions in KB-890772 and KB-888180.
- Cisco Secure Client blocks voice calls if it is sending or receiving VPN traffic over an EDGE connection per the inherent nature of EDGE and other early radio technology.
- Some known file compression utilities do not successfully decompress log bundles packaged with the use of the Cisco Secure Client Send Log button. As a workaround, use the native utilities on Windows and macOS to decompress Cisco Secure Client log files.
- DHE Incompatibility—With the introduction of DHE cipher support in Cisco Secure Client, incompatibility issues result in Cisco Secure Firewall ASA versions before ASA 9.2. If you are using DHE ciphers with Secure Firewall ASA releases earlier than 9.2, you must disable DHE ciphers on those Secure Firewall ASA versions.
- Because Cisco Secure Client is a networking VPN application, it requires background operation to function; therefore, you should never add Cisco Secure Client to the deep sleep list.

Android Specific Considerations

Android Mobile Posture Device ID Generation

Upon a fresh installation, or after the user clears the application data, Cisco Secure Client now generates a unique 256-byte device ID, which is based on the Android ID. This ID replaces the legacy 40-byte device ID based on the IMEI and MAC address generated in earlier releases.

If an earlier version of Cisco Secure Client is installed, a legacy ID has already been generated. After upgrading to this version of Cisco Secure Client, this legacy ID continues to be reported as the Device Unique ID until the user clears the application data or uninstalls Cisco Secure Client.

Generated device IDs can be viewed after the initial application launch from the Cisco Secure Client **Diagnostics** > **Logging and System Information** > **System** > **Device Identifiers** screen, or inside the Cisco Secure Client log in the `device_identifiers.txt` file, or on the **About** Screen.



Note DAP policies on the secure gateway will need to be updated to use the new device IDs.

The `Device-ID` is determined as follows:

```
Device-ID = bytesToHexString(SHA256(Android-ID))
```

Where the `Android-ID` and `bytesToHexString` are defined as follows:

```
Android-ID = Secure.getString(context.getContentResolver(), Secure.ANDROID_ID)
```

```
String bytesToHexString(byte[] sha256rawbytes){
String hashHex = null;
if (sha256rawbytes != null){
  StringBuffer sb = new StringBuffer(sha256rawbytes.length * 2);
    for (int i = 0; i < sha256rawbytes.length; i++){
    String s = Integer.toHexString(0xFF & sha256rawbytes[i]).toUpperCase();
    if (s.length() < 2) {sb.append("0");}
    sb.append(s);
    }
  hashHex = sb.toString();
  }
return hashHex; }
```

Android Device Permissions

The following permissions are declared in the Android manifest file for Cisco Secure Client operation:

Manifest Permission	Description
uses-permission: android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks.
uses-permission: android.permission.ACCESS_WIFI_STATE	Allows applications to access information about Wi-Fi networks.
uses-permission: android.permission.BROADCAST_STICKY	Allows an application to broadcast sticky intents. These are broadcasts whose data is held by the system after being finished, so that clients can quickly retrieve that data without having to wait for the next broadcast.
uses-permission: android.permission.INTERNET	Allows applications to open network sockets.
uses-permission: android.permission.READ_EXTERNAL_STORAGE	Allows an application to read from external storage.
uses-permission: android.permission.READ_LOGS	Allows an application to read the low-level system log files.
uses-permission: android.permission.READ_PHONE_STATE	Allows read only access to phone state, including the phone number of the device, current cellular network information, the status of any ongoing calls, and a list of any PhoneAccounts registered on the device.

Manifest Permission	Description
uses-permission: android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the broadcast after the system finishes booting.

Configure Cisco Secure Client for Android on Chromebooks

Google recently announced a deprecation of all native Chromebook applications. These steps migrate you from the native Chromebook applications and help you with configuring Cisco Secure Client for Android on Chromebooks.

You can access this Google documentation for additional information.

Procedure

Step 1 Sign in to your Google administrator console using an administrator account.

Step 2 From the Google Admin console Home page, go to **Devices** > **Chrome**.

Step 3 Click **Apps & extensions** > **Users & browsers**.

Step 4 Leave the top organizational unit selected if you want to apply the setting to everyone. Otherwise, apply a child organizational unit.

Step 5 Click **Add** > **Add from Google Play**.

Step 6 Choose Cisco Secure Client as the application you'd like to manage.

Step 7 The only managed configuration is the JSON file, which you can paste in or upload by clicking the upload icon.

What to do next

Keys are defined in the .apk package file for Android. The only required field is vpn_connection_host, but if you are pushing your Cisco Secure Client XML profile, the JSON key is vpn_connection_profile. Cisco Secure Client supports all of the managed configuration keys listed in the next section.

Managed Configuration Keys Supported by Cisco Secure Client

Managed Restrictions (Root)

vpn_connection_name

- Title—Connection name
- Type—String
- Description—User friendly name (for display only). If not set, defaults to the host.

vpn_connection_host

- Title—Host
- Type—string
- Description—URL to the headend. This field is required.

vpn_connection_profile

- Title—protocol
- Type—choice
- Possible Values—SSL | IPsec
- Description—VPN tunnel protocol (SSL or IPsec). Defaults to SSL

vpn_connection_ipsec_auth_mode

- Title—IPsec Authentication Mode
- Type—choice
- Description—(Optional) Authentication mode to use if tunnel protocol is IPsec. Defaults to EAP-AnyConnect

vpn_connection_ipsec_ike_identity

- Title—IKE identity
- Type—string
- Description—(Optional) Only applicable if IPsec authentication mode is EAP_GTC, EAP-Md5, or EAP-MSCHAPv2

vpn_connection_ipsec_ike_identity

- Title—IKE identity
- Type—string
- Description—(Optional) Only applicable if IPsec authentication mode is EAP_GTC, EAP-MD5, or EAP-MSCHAPv2.

vpn_connection_keychain_cert_alias

- Title—Keychain Certificate Alias
- Type—string
- Description—(Optional) Keychain alias of the client certificate to use for this VPN configuration

vpn_connection_allowed_apps

- Title—Per-App VPN Allowed Apps
- Type—string
- Description—(Optional) Specifies which apps (comma separated list of Android app package names) should be tunneled, thus enabling per-app VPN. All other apps are NOT tunneled. This setting requires a per-app VPN to be enabled on the headend.

vpn_connection_disallowed_apps

- Title—Per App VPN Disallowed Apps
- Type—string

- Description—(Optional) Specifies which apps (comma separated list of Android app package names) should NOT be tunneled, thus enabling per app VPN. All other apps are tunneled. This setting requires a per app VPN to be enabled on the headend.

vpn_connection_allow_bypass

- Title—Allow Apps to Bypass VPN Tunnel
- Type—boolean
- Description—(Optional) Allow apps to bypass this VPN connection. By default, this is disabled.

vpn_setting_replace_existing_profile

- Title—Replace Existing Profile
- Type—bool
- Description—(Optional) Only applicable if vpn_connection_profile is set. Specifies whether the managed configuration profile should replace any already installed profile on the client. Disabling this may be desirable to avoid conflicts with Secure Firewall ASA pushed profiles. By default, this is enabled.

vpn_setting_apply_perapp_to_profile

- Title—Apply Per App Rules to Profile Imported Configurations
- Type—bool
- Description—(Optional) Specifies whether to apply managed configuration per-app VPN rules (if they exist) to configurations imported from Cisco Secure Client profile XML. By default, this is disabled.

vpn_connection_set_active

- Title—Set Active
- Type—bool
- Default value—true
- Description—(Optional) Sets this as the last selected VPN configuration if there was none.

vpn_setting_fips_mode

- Title—Fips mode
- Type—bool
- Description—(Optional) Whether to enable FIPS mode for Cisco Secure Client.

vpn_setting_uri_external_control

- Title—URI External Control
- Type—string
- Description—(Optional) Configure URI Handling (External Control). Valid options are prompted, enabled, and disabled.

vpn_setting_strict_mode

- Title—Strict Mode
- Type—bool
- Description—(Optional) Whether to enable Strict Certificate Trust mode for Cisco Secure Client.

vpn_setting_certificate_revocation

- Title—Certificate Revocation
- Type—bool
- Description—(Optional) Whether to enable OCSP server certificate checking Cisco Secure Client.

vpn_connection_profile

- Title—Cisco Secure Client profile
- Type—string
- Description—(Optional) Cisco Secure Client Profile (XML format or Base64 encoding of XML) to import

vpn_connection_device_id

- Title—Device Identifier
- Type—string
- Description—(Optional) Identifier of the device report to the headend. If not set, Cisco Secure Client will generate a random persistent device identifier.

vpn_connection_report_hardware_id

- Title—Report Hardware Identifiers (MAC address and IMEI) for VPN authentication
- Type—bool
- Description—(Optional) Whether Cisco Secure Client should attempt to report hardware identifiers to the headend. By default, Cisco Secure Client tries to report hardware identifiers if they are accessible.

vpn_setting_allowed_saved_credentials

- Title—Allow users to save credentials
- Type—bool
- Default value—false
- Description—(Optional) Whether to allow user to save credentials (requires a screen lock). By default, user is not allowed to save credentials.

vpn_configuration_list

- Title—VPN Connection List
- Type—bundle_array
- Description—(Optional) Use this to configure more than one connection entries. Each entry is a vpn_configuration bundle.

umbrella_org_id

- Title—Umbrella Organization Id
- Type—string
- Description—The organization id to which customer belongs and it is as seen in the configuration file downloaded from Cisco Umbrella dashboard.

umbrella_reg_token

- Title—Umbrella Registration Token
- Type—string
- Description—The unique regToken issued to an organization, and the value is as seen in the configuration file downloaded from Cisco Umbrella dashboard.

umbrella_va_fqdns

- Title—Umbrella VA FQDNs list
- Type—string
- Description—This is the FQDN list of the VAs present in the connected network.

admin_email

- Title—Administrator Email Address
- Type—string
- Description—(Optional) Set a default administrator email address for sending logs.

vpn_always_on_umbrella_only

- Title—Enable Always On VPN Mode for Umbrella Protection Only
- Type—bool
- Default value—false
- Description—(Only applicable if using Umbrella) If set to true, always-on VPN will only apply Umbrella protection. If set to false, always-on VPN will apply to both Umbrella and remote access.

block_user_create_vpn_connection

- Title—Block users from creating new VPN connections
- Type—boolean
- Possible Values—true/false
- Description—To block Cisco Secure Client users from creating new VPN connections, set the **block_user_create_vpn_connection** key to *true*. The default is false, which allows VPN connection creation.

vpn_setting_block_untrusted_servers

- Title—Block Untrusted Servers

- Type—boolean
- Possible Values—true/false
- Description—To set the Block Untrusted Server option for managed devices, set the **vpn_setting_block_untrusted_servers** key to *true*. With this setting, users will not be able to connect to servers with untrusted server certificates. The default is false.

accept_seula_for_user

- Title—Accept SEULA for Users
- Type—boolean
- Possible Values—true/false
- Description—To hide the end user license agreement (EULA) on managed devices and ease new user onboarding, set the **accept_seula_for_user** key to *true*. With this setting, users get access without having to complate the default Cisco EULA requirements for the first time the app is launched. The default is false.

vpn_connection_yubikey_cert_slot

- Title—Yubikey Certificate Slot
- Type—string
- Possible Values—9a, 9c, 9d, or 9e
- Description— (Optional) Specifies which Yubikey slot (9a, 9c, 9d, or 9e) to use for certificate authentication.

Managed Restrictions for vpn_configuration Bundle

vpn_name

- Title—Display Name
- Type—string
- Description—User friendly name (for display only). If not set, defaults to the host.

vpn_host

- Title—Host
- Type—string
- Description—URL to the headend. This field is required.

vpn_protocol

- Title—Protocol
- Type—choice
- Possible values—SSL | IPsec
- Description—VPN tunnel protocol (SSL or IPsec). Defaults to SSL.

vpn_ipsec_auth_mode

- Title—IPsec Authentication Mode
- Type—choice
- Possible Values—EAP-AnyConnect | EAP-GTC | EAP-MD5 | EAP-MSCHAPv2 | IKE RSA
- Description—(Optional) Authentication mode to use if tunnel protocol is IPsec. Defaults to EAP-Connect.

vpn_ipsec_ike_identity

- Title—IKE identity
- Type—string
- Description—(Optional) Only applicable if IPsec authentication mode is EAP_GTC, EAP-MD5, or EAP-MSCHAPv2.

vpn_keychain_cert_alias

- Title—Keychain Certificate Alias
- Type—string
- Description—(Optional) Keychain alias of the client certificate to use for this VPN configuration.

vpn_allowed_apps

- Key—vpn_allowed_apps
- Title—Per-App VPN Allowed Apps
- Type—string
- Description—(Optional) Specifies which apps (comma separated list of Android app package names) should be tunneled, thus enabling per-app VPN. All other apps are NOT tunneled. This setting requires a per-app VPN to be enabled on the headend.

vpn_disallowed_apps

- Title—Per-App VPN Disallowed Apps
- Type—string
- Description—(Optional) Specifies which apps (comma separated list of Android app package names) should NOT be tunneled, thus enabling per-app VPN. All other apps are tunneled. This setting requires a per-app VPN to be enabled on the headend.

vpn_allow_bypass

- Title—Allow Apps to Bypass VPN Tunnel
- Type—bool
- Description—(Optional) Allow apps to bypass this VPN connection. By default, this is disabled.

vpn_set_active

- Title—Set Active:

- Type—bool
- Default value—false
- Description—(Optional) Sets this as the last selected VPN configuration if there was none.

vpn_yubikey_cert_slot

- Title—YubiKey Certificate Slot
- Type—string
- Possible Values—9a, 9c, 9d, or 9e
- Description—(Optional) Specifies which Yubikey slot (9a, 9c, 9d, or 9e) to use for certificate authentication

Cisco Secure Client on Apple iOS Devices

Refer to the Release Notes for Cisco Secure Client, for Apple iOS for features and devices supported by this release.

Guidelines and Limitations for Cisco Secure Client on Apple iOS

Cisco Secure Client for Apple iOS supports only features that are related to remote VPN access such as:

- Cisco Secure Client can be configured by the user (manually), by the Cisco Secure Client VPN Client Profile, generated by the Apple Configurator Utility (http://www.apple.com/support/iphone/enterprise/), or using an Enterprise Mobile Device Manager.
- The Apple iOS device supports no more than one Cisco Secure Client VPN client profile. The contents of the generated configuration always match the most recent profile. For example, you connect to vpn.example1.com and then to vpn.example2.com. The Cisco Secure Client VPN client profile imported from vpn.example2.com replaces the one imported from vpn.example1.com.
- This release supports the tunnel keepalive feature; however, it reduces battery life of the device. Increasing the update interval value mitigates this issue.

Apple iOS Connect On-Demand Considerations:

- VPN sessions, which are automatically connected as a result of iOS On-Demand logic and have Disconnect on Suspend configured, are disconnected when the device sleeps. After the device wakes up, On-Demand logic will reconnect the VPN session when it is necessary again.
- Cisco Secure Client collects device information when the UI is launched and a VPN connection is initiated. Therefore, there are circumstances in which Cisco Secure Client can misreport mobile posture information if the user relies on iOS Connect On-Demand feature to make a connection initially, or after device information, such as the OS version has changed.

Apple iOS Specific Considerations

When supporting Cisco Secure Client on Apple iOS devices, consider:

- The SCEP references in this document apply exclusively to Cisco Secure Client SCEP, not Apple iOS SCEP.
- Push email notifications do not work over VPN because of Apple iOS constraints. However, Cisco Secure Client works in parallel with externally accessible ActiveSync connections, when the tunnel policy excludes these from the session.
- Cisco Secure Client on iOS can be controlled via iOS Accessibility features such as Siri, Shortcuts, and Keyboard Shortcuts. The operations of connecting and disconnecting donate "Intents" to the OS are managed using Cisco Secure Client with the Shortcuts app and with Siri (and/or other automation mechanisms) enabled. For example, within the Shortcuts app, you can create a new shortcut, search for Cisco Secure Client, and choose "Start VPN." Then when you press **Play**, the shortcut runs, and a default prompt is displayed. You can create a similar shortcut for "Stop VPN," and they can be edited to change color, glyph, or reorder. You can also disable the prompt by expanding the entry and unchecking "Show When Run."

  Cisco Secure Client on iOS is a sandboxed application and does not have direct access to user keystrokes outside of the application. However, after connecting and disconnecting from a server, Cisco Secure Client can be controlled via Siri, Shortcuts, and Keyboard Shortcuts. Refer to iOS Accessibility features for instructions on the use of iOS Shortcuts and Keyboard Shortcuts.

The Apple Configurator Utility

The iPhone Configurator Utility (IPCU), available from Apple for Windows or macOS, is used to create and deploy configurations to an Apple iOS device. This can be done in place of configuring the Cisco Secure Client profile on the secure gateway.

The existing IPCU GUI, controlled by Apple, does not know of the Cisco Secure Client IPsec capabilities. Configure IPsec VPN connections within the existing Cisco Secure Client GUI in IPCU. Use the following URI syntax, as defined in RFC 2996 in the Server field. This Server field syntax is backward compatible with the documented usage for configuring SSL VPN connections.

[**ipsec**://][<**AUTHENTICATION**>[“:”<**IKE-IDENTITY**>“@”]]
<**HOST**>[“:”<**PORT**>][“/”<**GROUP-URL**>]

Parameter	Description
ipsec	Indicates that this is an IPsec connection. If omitted, SSL is assumed.
AUTHENTICATION	Specifies the authentication method for an IPsec connection. If omitted, EAP-AnyConnect is assumed. Valid values are: • EAP-AnyConnect • EAP-GTC • EAP-MD5 • EAP-MSCHAPv2 • IKE-RSA
IKE-IDENTITY	Specifies the IKE identify when AUTHENTICATION is set to EAP-GTC, EAP-MD5, or EAP-MSCHAPv2. This parameter is invalid when used for other authentication settings.

Parameter	Description
HOST	Specifies the server address. The hostname or IP address to be used.
PORT	Currently ignored, included for consistency with the HTTP URI scheme.
GROUP=URL	Tunnel group name appended to the server name.

Examples:

```
ipsec://EAP-AnyConnect@asa-gateway.example.com
ipsec://asa-gateway.example.com
```

To connect to a standards-compliant Cisco IOS router only, use the following:

```
ipsec://eap-md5:<identity>@ios-gateway.example.com
```

Connect-on-Demand Usage Guidelines

The Apple iOS Connect-on-Demand feature lets other applications, such as Safari, start a VPN connection. Apple iOS evaluates the domain requested by the application against the rules configured for the device's active connection entry. Apple iOS establishes a VPN connection on behalf of an application only if all of the following are true:

- A VPN connection is not already established.
- An application compatible with the Apple iOS Connect-on-Demand framework requests a domain.
- The connection entry is configured to use a valid certificate.
- Connect On Demand is enabled in the connection entry.
- Apple iOS fails to match a string in the Never Connect list to the domain request.
- Either of the following is true: Apple iOS matches a string in the Always Connect list to the domain request (on Apple iOS 6 only). Or a DNS lookup failed, and Apple iOS matches a string in the Connect if Needed list to the domain request.

Keep in mind the following when using the Connect-on-Demand feature:

- After a VPN connection is initiated using iOS's Connect on Demand, iOS disconnects the tunnel if the tunnel is inactive for a particular time interval. See Apple’s VPN Connect-on-Demand documentation for more information.
- We recommend using the Connect if Needed option if you configure rules. A Connect if Needed rule starts a VPN connection if the DNS lookup to an internal host fails. It requires a correct DNS configuration so that hostnames within the enterprise are resolved using internal DNS servers only.
- For mobile devices that have Connect on Demand configured, certificate-based authentication tunnel groups have a short (60 second) idle timeout (vpn-idle-timeout). Set a short idle timeout if your VPN session is not critical for an application and does not always need to be connected. The Apple device closes the VPN connection when it is no longer needed, for example, when the device goes into sleep mode. The default idle timeout for a tunnel group is 60 minutes.
- Always connect behavior is release dependent:
    - On Apple iOS 6, iOS always starts 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.

- Apple has introduced a Trusted Network Detection (TND) enhancement to the Connect-on-Demand feature. This enhancement:
  - Extends the Connect-on-Demand functionality by determining whether the device user is on a trusted network.
  - Applies to Wi-Fi connectivity only. When operating over other types of network connections, Connect on Demand does not use TND to determine whether to connect a VPN.
  - Is not a separate feature and cannot be configured or used outside the Connect-on-Demand capabilities.

  Contact Apple for more information about Connect-on-Demand Trusted Network Detection in iOS 6.
- The integrated Apple iOS IPsec client and Cisco Secure Client both use the same Apple iOS VPN Connect-on-Demand framework.

Split DNS Resolution Behavior with Split Tunnel

The Secure Firewall ASA split tunneling feature lets you specify which traffic goes over the VPN tunnel and which traffic goes in the clear. An associated feature called split DNS lets you specify which DNS traffic is eligible for DNS resolution over the VPN tunnel and which DNS traffic the endpoint DNS resolver handles (in the clear). Split DNS works differently on Apple iOS devices than on other devices if you also configure split tunneling. Cisco Secure Client for Apple iOS responds to this command as follows:

- Encrypts only DNS queries for domains in the split-dns list.

  Cisco Secure Client tunnels only the DNS queries for the domains specified in the command. It sends all other DNS queries to the local DNS resolver for resolution in-the-clear. For example, Cisco Secure Client tunnels only the DNS queries for example1.com and example2.com in response to the following command:

  ```
  hostname(config-group-policy)# split-dns value example1.com example2.com
  ```
- Encrypts only DNS queries for the domain in the default-domain command.

  If the **split-dns none** command is present and the **default-domain** command specifies a domain, Cisco Secure Client tunnels only DNS queries for that domain and sends all other DNS queries to the local DNS resolver for resolution in-the-clear. For example, Cisco Secure Client tunnels only the DNS queries for example1.com in response to the following commands:

  ```
  hostname(config-group-policy)# split-dns none
  hostname(config-group-policy)# default-domain value example1.com
  ```
- Sends all DNS queries in-the-clear. If the **split-dns none** and **default-domain none** commands are present in the group policy, or if these commands are absent from the group policy but present in the default group policy, Cisco Secure Client sends all DNS queries to the local DNS resolver for resolution in-the-clear.



Note If split-dns is not specified, the group policy inherits the spit tunneling domain lists that are present in the default group policy. To prevent inheriting a split tunneling domain list, use the split-dns none command.

YubiKey Certificate Authentication for iOS

You can use YubiKey as an external certificate for VPN certificate authentication. To enable the Yubikey feature, add the following into VendorConfig of the MDM VPN profile:

YubiKeyCertSlot with valid slot values of 9a, 9c, 9d, or 9e.

The Yubikey is not the same as and is not supported the same as other SmartCard/token devices. For example, the **SmartCard removal disconnect** command, which is configured in the Secure Firewall ASA Default Group Policy, has no affect on Yubikey with mobile devices.

MDM Configurable Settings for Cisco Secure Client on iOS

Import VPN xml Profile Via Vendor Data

You can import VPN xml profiles via vendor data into VPN profile. Use MDM with the following key/value pairs to change the default values and add to custom data. You can then go to system settings to install the profile and push it from the MDM server to user devices.

Using the first key/value pair passes the VPN xml profile. The second key/value pair indicates whether to replace the existing profile if one is present.

Key	Values
VpnConnectionProfile	[string of xml profile]
VpnReplaceExistingProfile	true/false

Define Cisco Secure Client Local Secure Settings

To define Cisco Secure Client local secure settings on managed Apple iOS devices, use MDM with the following key/value pairs to change the default values. When these key or value pairs are configured by MDM, they are pushed to the end user's device. These values, set with MDM configuration, disable the Cisco Secure Client end user from changing these settings in the Cisco Secure Client UI.

Key	Value	Type
UriExternalControl	Disabled/Prompt/Enabled	string
BlockUntrustedServers	true/false	Boolean
EnableFipsMode	true/false	Boolean
CheckCert Revocation	true/false	Boolean
StrictCertTrust	true/false	Boolean

.plist File

You can upload the following .plist file to MDM:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>BlockUserCreateVPNConnection</key>
    <true/>
    <key>StrictCertTrust</key>
    <true/>
    <key>CheckCertRevocation</key>
    <true/>
    <key>EnableFipsMode</key>
    <false/>
    <key>BlockUntrustedServers</key>
    <true/>
    <key>UriExternalControl</key>
    <string>Prompt</string>
</dict>
</plist>
```

Block End Users from Adding VPN Connections

To block Cisco Secure Client end users from adding VPN connections on managed Apple iOS devices, use MDM with the BlockUserCreateVPNConnection key set to a *true* value. These values, set with MDM configuration, prevent the Cisco Secure Client end user from adding VPN connection or importing a profile. Also, the URI handling will be disabled for creating VPN connection or importing profiles. If this key or value pair is not set with MDM, the end user will be able to add VPN connections (the default).

Cisco Secure Client on Chrome OS Devices

Refer to the Release Notes for Cisco Secure Client, for Google Chrome OS for features and devices supported by this release.

Guidelines and Limitations for Cisco Secure Client on Chrome OS

- We are not planning any future Chrome OS app releases. Because all current ChromeBooks support Android Apps, we advise you to use the Cisco Secure Client Android App instead.
- When the Chromebook device is managed (enrolled in an Enterprise Chrome Management service), then Cisco Secure Client cannot access client certificates: client certificate authentication does not work.
- There is limited VPN performance on low-end Chromebooks (chromium issue #514341).
- Auto reconnect, reconnecting the VPN session when the network interface goes down and up, is supported when using Cisco Secure Client release 4.0.10113 (or later) with Chrome OS 51 (or later). Prior to Chrome 51, if you lost WiFi, or put your device to sleep, Cisco Secure Client would not be able to reconnect on its own.
- Unless you are using Chrome OS 45 (or later), all server certificates, even fully trusted and valid ones, received from the secure gateway are seen as untrusted.

- After installing or upgrading Cisco Secure Client on Chrome OS, wait until initializing is complete to configure Cisco Secure Client. "Initializing, please wait..." is displayed in the Cisco Secure Client app. This process may take a few minutes.

Cisco Secure Client on Universal Windows Platform

Refer to the Release Notes for Cisco Secure Client, for Universal Windows Platform for features and devices supported by this release.

Guidelines and Limitations for Cisco Secure Client on Universal Windows Platform

- Performance is limited due to non-support of DTLS and IPsec/IKEv2.
- VPN roaming (transitioning between Wi-Fi and 3G/4G/5G networks) is not supported.
- A user initiated disconnect does not cleanly disconnect from the headend. Cisco recommends you connect to Secure Firewall ASA VPN groups with a small idle timeout to clear orphaned sessions on the Secure Firewall ASA.
- When the mobile device user is connecting to the Secure Firewall ASA that does not have a valid mobile license, the user will get into a login loop, where after entering credentials the authentication will restart and eventually (after 5 attempts) send the user a generic error message: `The VPN connection has failed with error code 602`. Please contact your administrator and ensure that a valid mobile license is installed on the secure gateway

Configure Mobile Device VPN Connectivity on the Secure Firewall ASA Gateway

Procedure

Step 1 Refer to the appropriate release of the Cisco ASA Series VPN CLI or ASDM Configuration Guides for configuration procedures that are common to desktop and mobile endpoints. Consider the following for mobile devices:

Attribute	ASDM Location	Exception
Home page URL	**Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add / Edit > Advanced > AnyConnect Client > Customization**	Cisco Secure Client Mobile ignores the home page URL setting. You cannot redirect mobile clients after successful authentication.

Attribute	ASDM Location	Exception
Name and Aliases of the Cisco Secure Client Connection Profile	**Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add / Edit**	Do not use special characters in the Name or Aliases fields of tunnel groups (connection profiles) that are used for Cisco Secure Client mobile client connectivity. Use of special characters may cause Cisco Secure Client to display the error message: `Connect attempt has failed` after logging that it is `Unable to process response from Gateway`.
Dead Peer Detection	**Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add / Edit > Advanced > AnyConnect Client**	Switch off server-side dead peer detection because it prevents the device from sleeping. However, client-side dead peer detection should remain switched on because it enables the client to determine when the tunnel is terminated due to a lack of network connectivity.
SSL Keepalive Messages	**Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add / Edit > Advanced > AnyConnect Client**	We recommend disabling these keepalive messages to conserve the battery life of mobile devices, especially if client-side dead peer detection is enabled.
IPsec over NAT-T Keepalive Messages	**Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Parameters**	**Enable IPsec over NAT-T** must be selected for Cisco Secure Client IPsec to work. When enabled, NAT Keepalive messages are sent every 20 seconds by default, causing excessive battery drainage on mobile devices. To minimally effect battery usage on mobile devices, we recommend you Set the NAT-T Keepalives to the maximum value of 3600 because these messages cannot be disabled. Use the `crypto isakmp nat-traversal 3600` command to specify this in the Secure Firewall ASA CLI.

Step 2 Configure Mobile Posture (also called AnyConnect Identifier Extensions, ACIDex) to accept, deny, or restrict mobile connections as desired.

See the *Configuring Endpoint Attributes Used in DAPs* procedure, in the appropriate release of the Cisco ASA Series VPN CLI or ASDM Configuration Guides .

Example:

The following attributes are sent by Cisco Secure Client on Apple iOS to the headend when establishing a connection:

```
endpoint.anyconnect.clientversion="4.0.03004";
endpoint.anyconnect.platform="apple-ios";
endpoint.anyconnect.devicetype="iPhone7,2";
endpoint.anyconnect.platformversion="9.0";
endpoint.anyconnect.deviceuniqueid="11025f84e99351e807f3583343bfec96351cb416";
```

Step 3 (Optional) Configure Per-App VPN tunneling mode.

See Configure Per-App VPN, on page 282.

If Per-App VPN tunneling mode is not configured, the Cisco Secure Client app operates in system-tunneling mode.

Configure Per-App VPN

Before you begin

Cisco Secure Client Per-App VPN tunneling requires:

- ASA 9.3.1 (or later) to configure Per-App VPN tunneling.
- Cisco Secure Client Advantage or Premier license.

Cisco Secure Client Per-App VPN supports the following mobile platforms:

- Android devices running Android 5.0 (Lollipop) or later.
- Apple iOS devices running Apple iOS 8.3 or later configured to use Per-App VPN in a Mobile Device Management (MDM) solution.

Procedure

Step 1 Install the Cisco Secure Client Enterprise Application Selector Tool, on page 282.

Step 2 Determine Which Apps Should Be Allowed in the Tunnel, on page 283.

Step 3 Determine Which Apps Should Bypass Tunnel, on page 284.

Step 4 Determine the Application IDs for Mobile Apps, on page 284.

Step 5 Configure Per-App VPN, on page 282.

Step 6 Use the Application Selector tool to specify Cisco Secure ClientPer-App VPN policy for your platform:

- Define a Per-App VPN Policy for Android Devices, on page 285
- Define a Per-App VPN Policy for Apple iOS Devices, on page 286

Step 7 Create Per-App Custom Attributes, on page 286 on the Secure Firewall ASA.

Step 8 Assign a Custom Attribute to a Policy on the Secure Firewall ASA, on page 287.

Install the Cisco Secure Client Enterprise Application Selector Tool

The Application Selector Tool is a standalone application that supports policy generation for both Android and Apple iOS devices.

Before you begin

The Cisco Secure Client Enterprise Application Selector requires Java 7 or later.

Procedure

Step 1 Download the Cisco Secure Client Enterprise Application Selector tool from the Cisco.com Cisco Secure Client Software Center.

Step 2 If you are using Android apps in your policy, you must have the Android SDK and the Android SDK Build-tools installed on your system. If you do not, install them as follows.

a) Install the latest version of the Android SDK Tools for the platform on which the Application Selector Tool is running.

Install the recommended **SDK Tools Only** package for your platform using the default paths and settings; including Install for All Users, so access to package entities is as described.

b) Using the Android SDK Manager, install the latest version of the **Android SDK Build-tools**.

What to do next



Note If prompted in the application selector tool, configure access to the Android Asset Packaging Tool, **aapt**, by specifying its installed location, *Android SDK installation directory*\build-tools*build-tools version number*\.

Determine Which Apps Should Be Allowed in the Tunnel

When you support mobile devices, such as phones running Android or iOS, you can use Mobile Device Manager (MDM) applications to fine-tune VPN access so that only supported applications are allowed to use the VPN tunnel. By restricting the remote access VPN to approved applications, you can reduce the load on the VPN headend and also protect the corporate network from malicious applications installed on these mobile devices.

To use a per-app remote access VPN, you must install and configure a third-party MDM application. It is in the MDM that you define the list of approved applications that can be used over the VPN tunnel. Explaining how to configure and use the third-party MDM that you select is outside the scope of this document.

When you use Cisco Secure Client to establish a VPN connection from a mobile device, all the traffic including the traffic from personal applications is routed through the VPN. If you instead want to route corporate applications only through the VPN, so that non-corporate traffic is excluded from the VPN, you can use per-app VPN to select which applications should be tunneled through the VPN.

Configure per-app VPN has the following main benefits:

- Performance—It limits traffic in the VPN to the traffic that needs to go to the corporate network. Thus, you free up resources at the headend of the remote access VPN.
- Protection—Because only traffic from approved applications is allowed, it protects the corporate tunnel from unapproved malicious applications that a user might unwittingly install on the mobile device. Because these applications are not included in the tunnel, traffic from them is never sent to the headend.

The Mobile Device Manager (MDM) running on the mobile endpoint enforces the Per-app VPN policy on the applications.

Determine Which Apps Should Bypass Tunnel

As an alternative configuration, Android also supports the use of MDM to specify what applications can bypass the tunnel while all other unspecified applications use the tunnel. This option works like split exclude on other platforms, except on an application basis instead of a routes basis.

You must install and configure a third-party MDM application. Within MDM, you define the list of applications that you want to bypass the VPN tunnel. Explaining how to configure and use third-party MDM is outside the scope of this documentation, but the MDM running on the mobile endpoint enforces which application exclusions to enforce based on the per-app VPN policy. Within MDM, set the Android configuration framework key value pairs and define which keys to support. With MDM Android managed configuration, just as you can choose **vpn_connection_allowed_apps** for any applications that you want to pass through the tunnel, choose **vpn_connection_disallowed_apps** for any applications that you want to bypass the tunnel. Then provide a comma-separated list of application IDs that you want to exclude or include.

Both settings require a per-app VPN to be enabled on the headend. For example:

- `string name="vpn_connection_allowed_apps"`

  Specifies which apps should be tunneled, thus enabling per-app VPN. All other apps are not tunneled.

- `string name="vpn_connection_disallowed_apps"`

  Specifies which apps should bypass the tunnel, thus enabling per-app VPN. These apps are available for public interface, and all other apps are tunneled.

Determine the Application IDs for Mobile Apps

We strongly recommend that you configure the per-app policy in your selected Mobile Device Manager (MDM) that provides the service on the user's mobile device. This greatly simplifies the headend configuration.

If you instead decide that you also want to configure the list of allowed apps on the headend or the list of blocked apps, you need to determine the application IDs for each application on each type of endpoint.

The application ID, called the bundle ID in iOS, is a reverse DNS name. You can use an asterisk as a wildcard. For example, *.* indicates all applications: com.cisco.* indicates all Cisco applications.

- Android—Go to Google play in a web browser and choose the Apps category. Click on (or hover over) an application that you want to allow (or not allow), then look at the URL. The app id is in the URL, on the **id=** parameter. For example, the following URL is for Facebook Messenger, so the app id is com.facebook.orca:

  `https://play.google.com/store/apps/details?id=com.facebook.orca`

For applications that are not available through Google Play, such as your own applications, download a package name viewer application to extract the app ID. Cisco does not endorse any of the available applications, but one of them should provide what you need.

- iOS—One means to find the bundle ID:

  1. Use a desktop browser such as Chrome to search for the application name.
  2. In the search results, look for the link to download the app from the Apple App Store. For example, Facebook messenger would be similar to https://apps.apple.com/us/app/messenger/id454638411.
  3. Copy the number after the **id** string. In this example, **454638411.**

4. Open a new browser window, and add the number to the end of the following URL:

   `https://itunes.apple.com/lookup?id=`

   For this example, https://itunes.apple.com/lookup?id=454638411

5. You will be prompted to download a text file, usually named 1.txt. Download the file.

6. Open the file in a text editor such as WordPad and search for bundleId. For example: "bundleId":"com.facebook.Messenger". In this example, the bundle ID is com.facebook.Messenger. Use this as the app ID.

Once you have your list of application IDs, you can configure the policy.

Define a Per-App VPN Policy for Android Devices

Your Per-app VPN policy consists of a set of rules, where each rule identifies an app whose data flows over the tunnel. Specify the rule options to more stringently identify the allowable app and its use in your mobile device environment. You are required to configure some Per-App Policy (custom attribute) on the Secure Firewall ASA in order for Per App to work, even if MDM has been configured for Per App. The Application Selector tool uses information from the app's package file, `*.apk`, to set rule options. See http://developer.android.com/guide/topics/manifest/manifest-element.html for Android package manifest information.

Before you begin

The Cisco Secure Client Enterprise Application Selector requires Java 7 or later.

Procedure

Step 1 Start the application selector and choose the **Android** mobile device platform.

Step 2 Set the required **App ID** field.

- Choose **Import from Disk** to obtain app-specific package information from an app stored on your local system.

  The App ID field (a string in reverse-DNS format) is automatically filled in. For example, if choosing the Chrome app for an Apple iOS policy, the App ID field is set to **`com.google.chrome.ios`**. For Chrome on Android, it would be set to **`com.android.chrome`**.

- Alternatively, you may enter this app-specific information directly.

- Specify reverse-DNS format using a wildcard, for example, specify com.cisco.* to tunnel all Cisco apps, instead of listing each one in its own rule. The wildcard must be the last character in the APP ID entry.

  When configuring Per-app VPN in a managed environment, verify that the Secure Firewall ASA policy allows the same apps to tunnel as the MDM policy. We recommend specifying *.* as the App ID to allow tunneling of ALL apps and to ensure that the MDM policy is the only arbiter of tunneled apps. Non *.* policies are not supported.

Step 3 (Optional) Select a listed app and configure more parameters if desired.

- Minimum Version—The minimum version of the chosen app as specified in the package's manifest attribute *android: versionCode*.

- Match Certificate ID—A digest of the application signing certificate.
- Allow Shared UID—Default value is true. If set to false, applications with an *android: sharedUserId* attribute specified in the package manifest will not match this rule and are prevented from accessing the tunnel.

Step 4 Click **File > Save** to save this Per-app VPN policy.

Step 5 Select **Policy > View Policy** to view the representation of the defined policy.

Copy this string. This string becomes the value of a *perapp* custom attribute on the Secure Firewall ASA.

Define a Per-App VPN Policy for Apple iOS Devices

The policy for Per-App VPN on Apple iOS devices is entirely controlled by the MDM facilities. Therefore, Cisco Secure Client must allow ALL apps, and MDM must configure Per-App policies to specify the particular apps that can be tunneled.

Before you begin

The Cisco Secure Client Enterprise Application Selector requires Java 7 or later.

Procedure

Step 1 Start the application selector and choose the **Apple iOS** mobile device platform.

Step 2 Set the required **App ID** field to ***.***.

This setting allows ALL apps to tunnel through Cisco Secure Client and ensures that the MDM per app policy is the only arbiter of tunneled apps.

Step 3 Click **File > Save** to save this Per-App VPN policy.

Step 4 Select **Policy > View Policy** to view the representation of the defined policy.

Copy this string. This string becomes the value of a *perapp* custom attribute on the Secure Firewall ASA.

Create Per-App Custom Attributes

Procedure

Step 1 In ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes** to configure a custom attribute type.

Step 2 Choose **Add** or **Edit** and set the following in the **Create / Edit Custom Attribute Type** pane:

a) Enter *perapp* as the type.

The type must be *perapp* because it is the only type of attribute understood by Cisco Secure Client for Per-App VPN. Adding this attribute to remote access VPN group profile automatically limits the tunnel to the explicitly identified platforms. Traffic from all other application is automatically excluded from the tunnel.

b) Enter a description of your choosing.

Step 3 Click **OK** to close this pane.

Step 4 Navigate to **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names** to configure a custom attribute.

Step 5 Choose **Add** or **Edit** and set the following in the **Create / Edit Custom Attribute Name** pane:

a) Choose the *perapp* attribute **Type**.

b) Enter a **Name**. This name is used to assign this attribute to a policy.

c) **Add** one or more values by copying the BASE64 format from the policy tool and pasting it here.

Each value cannot exceed 420 characters. If your value exceeds this length, add multiple values for the additional value content. The configured values are concatenated before being sent to Cisco Secure Client.

Assign a Custom Attribute to a Policy on the Secure Firewall ASA

The perapp custom attribute can be assigned to a Group Policy or a Dynamic Access Policy.

Procedure

Step 1 Open the policy on the Secure Firewall ASA:

- For a Group Policy, navigate to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add / Edit > Advanced > AnyConnect Client > Custom Attributes**.
- For a Dynamic Access Policy, navigate to **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies Add / Edit** . In the **Access/Authorization Policy Attributes** section select the **AnyConnect Custom Attributes** tab.

Step 2 Click **Add** or **Edit** an existing attribute to open the **Create / Edit Custom Attribute** pane.

Step 3 Select the predefined *perapp* attribute type from the drop-down list.

Step 4 Choose **Select Value** and select a predefined value from the drop-down list

Step 5 Click **OK** to close the open configuration panes.

Configure Mobile Device Connections in the Cisco Secure Client VPN Profile

The Cisco Secure Client VPN Profile is an XML file that specifies client behavior and defines VPN connection entries. Each connection entry specifies a secure gateway that is accessible to the endpoint device and other connection attributes, policies, and constraints. Use the Cisco Secure Client Profile Editor to create a VPN client profile that includes host connection entries for mobile devices.

Connection entries defined in the VPN profile and delivered to mobile devices from the Secure Firewall ASA cannot be modified or deleted by the user. Users can modify and delete only the connection entries that they create manually.

Cisco Secure Client retains only one current VPN Profile on the mobile device at a time. Upon startup of an automatic or manual VPN connection, the new VPN profile entirely replaces the current profile. If the user manually deletes the current profile, the profile is removed, and all connection entries defined in this profile are deleted.

Procedure

Step 1 Configure basic VPN access.

Some procedures are common to desktop and mobile endpoints, considering the following exceptions:

Profile Attribute	Exception
Auto Reconnect	For all platforms except Apple iOS, regardless of your Auto Reconnect specification, Cisco Secure Client Mobile always attempts to ReconnectAfterResume. For Apple iOS only, Disconnect On Suspend is supported. When Disconnect On Suspend is chosen, Cisco Secure Client disconnects and then releases the resources assigned to the VPN session. It will only reconnect in response to a user's manual connection or an On Demand connection (if configured).
Local LAN Access	(iOS only)Cisco Secure Client Mobile ignores the Local LAN Access setting, always allowing Local LAN Access regardless of the setting in the client profile.

Step 2 Configure Mobile Specific Attributes:

a) In the VPN Profile, select **Server List** in the navigation pane.
b) Select **Add** to add a new server entry to the list, or select a server entry from the list and press **Edit** to open the Server List Entry dialog box.
c) Configure mobile specific parameters.
d) Click **OK**.

Step 3 Distribute the VPN profile in one of the following ways:

- Configure the Secure Firewall ASA to upload a client profile onto the mobile device upon VPN connectivity.

  See The Cisco Secure Client Profile Editor, on page 75 chapter for instructions on how to import the VPN profile to the Secure Firewall ASA and associate it with a group policy.

- Provide the user with the Cisco Secure Client URI link to import a client profile. (Android and Apple iOS only)

  See Import a VPN Profile, on page 296 to provide this kind of deployment procedure to your users.

- Have users import their Cisco Secure Client profile using **Profile Management** on the mobile device. (Android and Apple iOS only)

Automate Cisco Secure Client Actions Using the URI Handler

The URI handler in Cisco Secure Client lets other applications pass action requests in the form of Universal Resource Identifiers (URIs) to Cisco Secure Client. To simplify the Cisco Secure Client user setup process, embed URIs as links on web pages or e-mail messages, and give users instructions to access them.

Before you begin

- The URI handler in Cisco Secure Client lets other applications pass action requests in the form of Universal Resource Identifiers (URIs) to Cisco Secure Client.

  In managed environment:

  When enabled, external control allows all URI commands without user interaction. When set for prompting, the user is notified of URI activity and allows or disallows it at request time. You should inform your users how to respond to prompts associated with URI handling if you are using them. The key and values for configuring the settings on MDM are:

  Key - *UriExternalControl*

  Values - *Enabled*, *Prompt*, or *Disabled*



Note Once the configuration setting has been done in MDM and pushed down to the user device, the user is not allowed to make changes to this setting.

  In unmanaged environment:

  URI handling in the Cisco Secure Client application is disabled by default. Mobile device users allow this functionality by setting the **External Control** app setting to Enable or Prompt. When enabled, external control allows all URI commands without user interaction. When set for prompting, the user is notified of URI activity and allows or disallows it at request time.

- You must use URL encoding when entering URI handler parameter values. Use a tool such as the one in this link to encode an action request. Also, refer to provided examples below.
- In the URI, `%20` represents a space, `%3A` represents a colon (:), `%2F` represents a forward slash (/), and `%40` represents an ampersand (@).
- Slashes in the URI are optional.

Provide your users with any of the following actions.

Generate a VPN Connection Entry

Use this Cisco Secure Client URI handler to simplify the generation of the Cisco Secure Client connection entry for users.

anyconnect:[*//*]**create**[*/*]**?name**=*Description*&**host**=*ServerAddress*[**&Parameter1**=*Value*&**Parameter2**=*Value* ...]

Guidelines

- The *host* parameter is required. All other parameters are optional. When the action runs on the device, Cisco Secure Client saves all the parameter values that you enter to the connection entry associated with that *name* and *host*.
- Use a separate link for each connection entry that you want to add to the device. Specifying multiple create connection entry actions in a single link is not supported.

Parameters

- **name**—Unique name for the connection entry to appear in the connection list of the Cisco Secure Client home screen and the Description field of the Cisco Secure Client connection entry. Cisco Secure Client responds only if the name is unique. We recommend using a maximum of 24 characters to ensure that they fit in the connection list. Use letters, numbers, or symbols on the keyboard displayed on the device when you enter text into a field. The letters are case-sensitive.
- **host**—Enter the domain name, IP address, or Group URL of the Secure Firewall ASA with which to connect. Cisco Secure Client inserts the value of this parameter into the Server Address field of the Cisco Secure Client connection entry.

```
anyconnect://create/?name=SimpleExample&host=vpn.example.com
anyconnect:create?name=SimpleExample&host=vpn.example.com
```

- **protocol** (optional, defaults to SSL if unspecified)—The VPN protocol used for this connection. The valid values are:
  - SSL
  - IPsec

```
anyconnect:create?name=ExampleIPsec&host=vpn.company.com&protocol=IPsec
```

- **authentication** (optional, applies when protocol specifies IPsec only, defaults to EAP-AnyConnect)—The authentication method used for an IPsec VPN connection. The valid values are:
  - EAP-AnyConnect
  - EAP-GTC
  - EAP-MD5
  - EAP-MSCHAPv2
  - IKE-RSA
- **ike-identity** (required if authentication is set to EAP-GTC, EAP-MD5, or EAP-MSCAPv2)—The IKE identify when AUTHENTICATION is set to EAP-GTC, EAP-MD5, or EAP-MSCHAPv2. This parameter is invalid when used for other authentication settings.

```
anyconnect:create?name=Description&host=vpn.company.com&protocol=IPsec
&authentication=eap-md5&ike-identity=012A4F8B29A9BCD
```

- **netroam** (optional, applies to Apple iOS only)—Determines whether to limit the time that it takes to reconnect after the device wakes up or after a change to the connection type (such as EDGE, 3G, or WiFi).This parameter does not affect data roaming or the use of multiple mobile service providers. The valid values are:

- true—(Default) This option optimizes VPN access. Cisco Secure Client inserts the value ON into the Network Roaming field of the Cisco Secure Client connection entry. If Cisco Secure Client loses a connection, it tries to establish a new one until it succeeds. This setting lets applications rely on a sustained connection to the VPN. Cisco Secure Client does not impose a limit on the time that it takes to reconnect.
- false—This option optimizes battery life. Cisco Secure Client associates this value with the OFF value in the Network Roaming field of the Cisco Secure Client connection entry. If Cisco Secure Client loses a connection, it tries to establish a a new one for 20 seconds and then stops trying. The user or application must start a new VPN connection if one is necessary.

```
anyconnect:create?name=Example%201&host=vpn.example.com&netroam=true
```

- **keychainalias** (optional)—Imports a certificate from the System Certificate Store to the Cisco Secure Client Certificate Store. This option is for the Android mobile platform only.

  If the named certificate is not already in the system store, the user will be prompted to choose and install it before being prompted to allow or deny it being copied into the Cisco Secure Client store. External Control must be enabled on the mobile device.

  The following example creates a new connection entry named *SimpleExample* whose IP address is set to *vpn.example.com* with the certificate named *client* assigned to it for authentication.

  ```
  anyconnect://create/?name=SimpleExample&host=vpn.example.com&keychainalias=client
  ```

- **usecert** (optional)—Determines whether to use a digital certificate installed on the device when establishing a VPN connection to the host. The valid values are:
  - true (default setting)—Enables automatic certificate selection when establishing a VPN connection with the host. Turning usecert to *true* without specifying a certcommonname value sets the Certificates field to *Automatic*, selecting a certificate from the Cisco Secure Client certificate store at connection time.
  - false—Disables automatic certificate selection.

  ```
  anyconnect:create?name=Example%201&host=vpn.example.com&usecert=true
  ```

- **certcommonname** (optional, but requires the *isecert* parameter)—Matches the Common Name of a valid certificate pre-installed on the device. Cisco Secure Client inserts the value into the Certificate field of the Cisco Secure Client connection entry.

  To view this certificate installed on the device, tap **Diagnostics** > **Certificates**. You might need to scroll to view the certificate required by the host. Tap the detail disclosure button to view the Common Name parameter read from the certificate, as well as the other values.

- **useondemand** (optional, applies to Apple iOS only and requires the *usercert*, *certcommonname* parameters, and *domain* specifications below)—Determines whether applications, such as Safari, can start VPN connections. Valid values are:
  - false (Default)—Prevents applications from starting a VPN connection. Using this option is the only way to prevent an application that makes a DNS request from potentially triggering a VPN connection. Cisco Secure Client associates this option with the OFF value in the Connect-on-Demand field of the Cisco Secure Client connection entry.
  - true—Lets an application use Apple iOS to start a VPN connection. If you set the useondemand parameter to *true*, Cisco Secure Client inserts the value ON into the Connect on Demand field of the Cisco Secure Client connection entry. (domainlistalways or domainlistifneeded parameter required if useondemand=true)

```
anyconnect:create?name=Example%20with%20certificate&host=vpn.example.com
&netroam=true&usecert=true&certcommonname=example-ID&useondemand=true
&domainlistalways=email.example.com,pay.examplecloud.com
&domainlistnever=www.example.com&domainlistifneeded=intranet.example.com
```

- **domainlistnever** (optional, requires useondemand=true)—Lists the domains to evaluate for a match to disqualify the use of the Connect-on-Demand feature. This list is the first one Cisco Secure Client uses to evaluate domain requests for a match. If a domain request matches, Cisco Secure Client ignores the domain request. Cisco Secure Client inserts this list into the Never Connect field of the Cisco Secure Client connection entry. This list lets you exclude certain resources. For example, you might not want an automatic VPN connection over a public-facing web server. An example value is `www.example.com`.
- **domainlistalways**(domainlistalways or domainlistifneeded parameter required if useondemand=true)—Lists the domains to evaluate for a match for the Connect-on-Demand feature. This list is the second one Cisco Secure Client uses to evaluate domain requests for a match. If an application requests access to one of the domains specified by this parameter and a VPN connection is not already in progress, Apple iOS attempts to establish a VPN connection. Cisco Secure Client inserts this list into the Always Connect field of the Cisco Secure Client connection entry. An example value list is `email.example.com,pay.examplecloud.com`.
- **domainlistifneeded** (domainlistalways or domainlistifneeded parameter required if useondemand=true)—Cisco Secure Client evaluates a domain request for a match against this list if a DNS error occurred. If a string in this list matches the domain, Apple iOS attempts to establish a VPN connection. Cisco Secure Client inserts this list into the Connect if Needed field of the Cisco Secure Client connection entry. The most common use case for this list is to obtain brief access to an internal resource that is not accessible in a LAN within the corporate network. An example value is `intranet.example.com`.

Use a comma-delimited list to specify multiple domains. The Connect-on-Demand rules support only domain names, not IP addresses. However, Cisco Secure Client is flexible about the domain name format of each list entry, as follows:

Match	Instruction	Example Entry	Example Matches	Example Match Failures
Exact prefix and domain name only.	Enter the prefix, dot, and domain name.	email.example.com	email.example.com	www.example.com email.1example.com email.example1.com email.example.org
Any prefix with the exact domain name. The leading dot prevents connections to hosts ending with *example.com, such as notexample.com.	Enter a dot followed by the domain name to be matched.	.example.org	anytext.example.org	anytext.example.com anytext.1example.org anytext.example1.org
Any domain name ending with the text you specify.	Enter the end of the domain name to be matched.	example.net anytext	anytext-example.net anytext.example.net	anytext.example1.net anytext.example.com

Establish a VPN Connection

Use this Cisco Secure Client URI handler to connect to a VPN allowing users to easily establish VPN connections. You can also embed additional information in the URI to perform the following tasks:

- Prefill a Username and Password
- Prefill Usernames and Passwords for Double Authentication
- Prefill a Username and Password, and Specify a Connection Profile Alias

This action requires either the name or the host parameters, but allows both using one of the following syntaxes:

anyconnect:[//]**connect**[/]**?**[**name=***Description*|**host=***ServerAddress*]
[**&Parameter1**=*Value***&Parameter2**=*Value* ..]

or

anyconnect:[//]**connect**[/]**?name=***Description***&host=***ServerAddress*
[**&Parameter1**=*Value***&Parameter2**=*Value* ..]

Guidelines

- If all the parameter values in the statement match those of the Cisco Secure Client connection entry on the device, Cisco Secure Client uses the remaining parameters to establish the connection.
- If Cisco Secure Client does not match all parameters in the statement to those in a connection entry and the name parameter is unique, it generates a new connection entry and then attempts the VPN connection.
- Specifying a password when establishing a VPN connection using a URI should be used only in conjunction with a One Time Password (OTP) infrastructure.

Parameters

- **name**—Name of the connection entry as it appears in the connection list of the Cisco Secure Client home window. Cisco Secure Client evaluates this value against the Description field of the Cisco Secure Client connection entries, also called name if you used the previous instructions to create the connection entry on the device. This value is case-sensitive.
- **host**—Enter the domain name, IP address, or Group URL of the Secure Firewall ASA to match the Server Address field of the Cisco Secure Client connection entry, also called the host if you used the previous instructions to generate the connection entry on the device.

  The Group URL is configured in ASDM by selecting **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Advanced > Group Alias/Group URL > Group-URL**.
- **onsuccess**—Execute this action if the connection is successful. Platform specific behavior:
  - For Apple iOS devices, specify the URL to be opened when this connection transitions into the connected state, or use the anyconnect:close command to close the Cisco Secure Client GUI.
  - For Android devices, specify the URL to open when this connection transitions into or is already in the connected state. Multiple onsuccess actions can be specified. Cisco Secure Client always closes the GUI after a successful connection on Android devices.
- **onerror**—Execute this action if the connection fails. Platform specific behavior:

- For Apple iOS devices, specify the URL to be opened when this connection fails, or use the anyconnect:close command to close the Cisco Secure Client GUI.
- For Android devices, specify the URL to be opened when this connection fails. Multiple onerror actions can be specified. Cisco Secure Client always closes the GUI after a failed connection on Android devices.

- **prefill_username**—Provides the username in the connect URI and prefills it in connection prompts.
- **prefill_password**—Provides the password in the connect URI and pre-fills it in connection prompts. This field should only be used with connection profiles configured for one-time passwords.
- **prefill_secondary_username**—In environments that are configured to require double authentication, this parameter provides the secondary username in the connect URI and prefills it in the connection prompts.
- **prefill_secondary_password**—In environments that are configured to require double authentication, this parameter provides the password for the secondary username in the connect URI and pre-fills it in the connection prompts.
- **prefill_group_list**—The connection alias defined in ASDM by selecting **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Advanced > Group Alias/Group URL > Connection Aliases**.

Examples

- Provide the Connection Name and Hostname or Group URL in a URI:

```
anyconnect://connect/?name=Example
```

```
anyconnect:connect?host=hr.example.com
```

```
anyconnect:connect?name=Example&host=hr.example.com
```

```
anyconnect://connect/?name=Example&host=hr.example.com/group-url
&prefill_username=user1&prefill_password=password1
```

- Provide Actions For Success or Failure

  Use the onsuccess or onerror parameters to initiate the opening of a specified URL based on the results of the connect action:

```
anyconnect://connect?host=vpn.company.com
&onsuccess=http%3A%2F%2Fwww.cisco.com
```

```
anyconnect://connect?host=vpn.company.com
&onerror=http%3A%2F%2Fwww.cisco.com%2Ffailure.html
&onsuccess=http%3A%2F%2Fwww.cisco.com
```

  On Android you can specify multiple onsuccess actions:

```
anyconnect://connect?host=vpn.company.com
&onerror=http%3A%2F%2Fwww.cisco.com%2Ffailure.html
&onsuccess=http%3A%2F%2Fwww.cisco.com
&onsuccess=tel:9781111111
```

  On Apple iOS devices, the anyconnect://close command can be used in the onsuccess or onerror parameter to close the Cisco Secure Client GUI:

```
anyconnect://connect?host=vpn.company.com
&onsuccess=anyconnect%3A%2F%2Fclose
```

- Provide Connection Information and Prefill a Username and Password in a URI:

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
```

```
anyconnect:connect?name=Example&host=hr.example.com/group-url
&prefill_username=user1&prefill_password=password1
```

- Provide Connection Information and Prefill Usernames and Passwords for Double Authentication:

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
&prefill_secondary_username=user2&prefill_secondary_password=password2
```

- Provide Connection Information, Prefill a Username and Password, and Specify a Connection Profile Alias:

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
&prefill_group_list=10.%20Single%20Authentication
```

Disconnect from a VPN

Use this Cisco Secure Client URI handler to disconnect the user from a VPN.

anyconnect:[//]**disconnect**[/]**&onsuccess=**URL

Parameters

The onsuccess parameter applies to Android devices only. Specify the URL to open when this connection disconnects or if it is already in the disconnected state.

Example

```
anyconnect:disconnect
```

Import Certificates

Use this URI handler command to import a PKCS12 encoded certificate bundle to the endpoint. Cisco Secure Client authenticates itself to the Secure Firewall ASA using a PKCS12 encoded certificate that has been installed on the endpoint. Only pkcs12 certificate type is supported.

anyconnect:[//]**import**[/]**?type=pkcs12&uri=***http%3A%2F%2Fexample.com%2Fcertificatename.p12*

Parameters

- **type**—Only pkcs12 certificate type is supported.
- **uri**—URL encoded identifier where the certificate is found.

Examples

```
anyconnect:import?type=pkcs12&uri=http%3A%2F%2Fexample.com%2FCertName.p12
```

Import a VPN Profile

Use this URI handler method to distribute client profiles to Cisco Secure Client.

anyconnect:[//]**import**[/]**?type=profile&uri**=*filename.xml*

Example

```
anyconnect:import?type=profile&uri=file%3A%2F%2Fsdcard%2Fprofile.xml
```

Localize the Cisco Secure Client UI and Messages

Use this URI handler method to localize Cisco Secure Client.

anyconnect:[//]**import**[/]**?type=localization&lang=***LanguageCode***&host=***ServerAddress*

Parameters

The import action requires all parameters.

- **type**—The import type, in this case localization.
- **lang**—The two- or four-character language tag representing the language provided in the anyconnect.po file. For example, the language tag may simply be fr for “French” or fr-ca for “Canadian French.”
- **host**—Enter the domain name or IP address of the Secure Firewall ASA to match the Server Address field of the Cisco Secure Client connection entry.

Example

```
anyconnect:import?type=localization&lang=fr&host=asa.example.com
```

Troubleshoot Cisco Secure Client on Mobile Devices

Before you begin

Enable logging on the mobile device.

Procedure

Step 1 Determine whether the same problem occurs with the desktop client or another mobile OS.

Step 2 Ensure that the proper licenses are installed on the Secure Firewall ASAs.

Step 3 If certificate authentication is failing, check the following:

a) Ensure that the correct certificate is being selected.
b) Ensure that the client certificate on the device has Client Authentication as an Extended Key Usage.
c) Ensure that the certificate matching rules in the Cisco Secure Client profile are not filtering out the user’s selected certificate.

Even if a user selected the certificate, it is not used for authentication if it does not match the filtering rules in the profile.

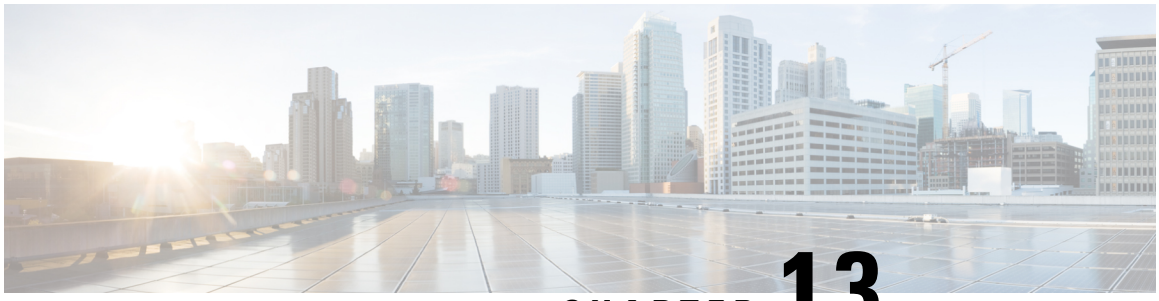
d) If your authentication mechanism uses any associated accounting policy to a Secure Firewall ASA, verify that the user can successfully authenticate.
e) If you see an authentication screen when you are expecting to use certificate-only authentication, configure the connection to use a group URL and ensure that secondary authentication is not configured for the tunnel group.

Step 4 On Apple iOS devices, check the following.

a) If the VPN connection is not restored after the device wakes up, ensure that Network Roaming is enabled.
b) If using Connect on Demand, verify certificate-only authentication and a Group URL are configured.

What to do next

If problems persist, enable logging on the client and enable debug logging on the Secure Firewall ASA. For details, refer to the release-appropriate Cisco ASA Series VPN CLI or ASDM Configuration Guide.



CHAPTER 13

Cisco Secure Client Customer Experience Feedback Module

Note BY DEFAULT YOUR PRIVATE AND CORPORATE DATA IS COLLECTED.

The customer experience feedback (CEF) module provides us with information about which features and modules customers use and have enabled. This information gives us insight into the user experience so that Cisco can continue to improve the quality, reliability, performance, and user experience of Cisco Secure Client.

For details about the collection and use of information, refer to the Cisco Online Privacy Statement Highlights page where you can access the Cisco Secure Client Supplement. All data is collected anonymously and does not contain personally identifiable data. The data is also securely sent.

Cisco collects the following types of data:

- Usability data—See the privacy policy for details. This data is collected and sent once every month.
- Web threat data—Sent whenever a threat is reported.
- Crash reports—Crash dump files generated by Cisco Secure Client are checked every 24 hours, collected, and sent to the customer experience feedback server.

The major components in the customer experience feedback modules are as follows:

- Feedback Module—Cisco Secure Client software component that collects the information and periodically sends it to the server.
- Cisco Feedback Server—Cisco-owned cloud infrastructure that collects the customer experience feedback data and stores it in temporary storage as raw format.

- Configure Customer Experience Feedback, on page 299

Configure Customer Experience Feedback

The Cisco Secure Client Customer Experience Feedback module is deployed with Cisco Secure Client, and enabled by default. You can modify what feedback is sent by creating a Customer Experience Feedback

profile, including opting out of experience feedback entirely. This method is the preferred method to disable the feedback module, but you can also remove it altogether during Cisco Secure Client deployment.

Before you begin

The customer experience feedback module is enabled automatically.

Procedure

Step 1 Open the standalone Customer Experience Feedback Profile Editor or in ASDM, navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**.

Step 2 Create your Cisco Secure Client profile with Profile Usage of **Feedback Service Profile**.

Step 3 If you do not want to provide feedback, uncheck **Enable customer Experience Feedback Service**.

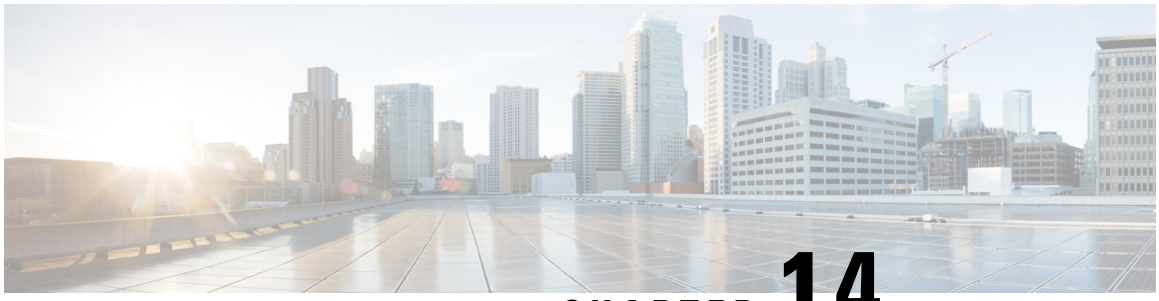
You can disable feedback any time after installation.

Step 4 If you do not want to send crash reports generated by Cisco Secure Client, uncheck **Include Crash Report**.

The default is to include a crash report.

Step 5 Enter a customer key or ID of your choice.

This ID allows Cisco to identify information from your organization.



CHAPTER 14

Troubleshoot Cisco Secure Client

- Gather Information for Troubleshooting, on page 301
- Cisco Secure Client Connection or Disconnection Issues, on page 305
- VPN Service Failures, on page 309
- Driver Crashes, on page 310
- Other Crashes, on page 311
- Security Alerts, on page 312
- Dropped Connections, on page 313
- Installation Failures, on page 315
- Incompatability Issues, on page 315
- Known Third-Party Application Conflicts, on page 317

Gather Information for Troubleshooting

View Statistical Details

An administrator or end user can view statistical information for a current Cisco Secure Client session.

Procedure

Step 1 On Windows, choose the gear icon on the left of the UI and then navigate to **Advanced Window** > **Statistics** > **AnyConnect VPN drawer**. On macOS, choose the **Statistics** icon next to the gear. On Linux, click the **Details** button on the user GUI.

Step 2 Choose from the following options, depending upon the packages that are loaded on the client computer.

- **Export Stats**—Saves the connection statistics to a text file for later analysis and debugging.
- **Reset**—Resets the connection information to zero so Cisco Secure Client begins collecting new data.
- **Diagnostics**—Launches the Cisco Secure Client Diagnostics and Reporting Tool (DART) wizard which bundles specified log files and diagnostic information for analyzing and debugging the client connection. On macOS, you must choose **Generate Diagnostic Report** from the Cisco Secure Client application menu to start the DART.

Run DART to Gather Data for Troubleshooting

DART is the Cisco Secure Client Diagnostics and Reporting Tool that you can use to collect data for troubleshooting Cisco Secure Client installation and connection problems. DART assembles the logs, status, and diagnostic information for Cisco Technical Assistance Center (TAC) analysis. Note that by default, data collection is based on U.S. region format (MM/DD/YY).

The DART wizard runs on the device that runs Cisco Secure Client. You can launch DART from Cisco Secure Client, or by itself without Cisco Secure Client.

Note DART requires administrator privileges on macOS, Ubuntu 18.04, and Red Hat 7 to collect logs.

Also, for ISE posture only, you can automatically collect DART, if configured, as soon as an ISE posture crash occurs or when an endpoint goes to non-compliant. To enable Auto-DART, set the DARTCount to any non-zero value. When set to 0, the feature is disabled. Enabling Auto-DART prevents data loss due to time lapse. Gather the auto-collected DARTS at the following locations:

- **Windows:** %LocalAppData%\Cisco\Cisco Secure Client
- **macOS:** ~/.cisco/iseposture/log

The following operating systems are supported:

- Windows
- macOS
- Linux

Procedure

Step 1 Launch DART:

- For a Windows device, launch the Cisco Secure Client.
- For a Linux device, choose **Applications** > **Internet** > **Cisco DART**

  or /opt/cisco/anyconnect/dart/dartui.
- For a macOS device, choose **Applications** > **Cisco** > **Cisco DART**

Step 2 Click the gear icon and then **Diagnostics**.

Step 3 Choose **Default** or **Custom** bundle creation.

- Default—Includes the typical log files and diagnostic information, such as the Cisco Secure Client log files, general information about the computer, and a summary of what DART did and did not do. The default name for the bundle is `DARTBundle.zip`, and it is saved to the local desktop.
- Custom—Allows you to specify what files you want to include in the bundle (or the default files) and where to store the bundle.

Successful route and filtering changes for Linux and macOS will be kept out of the log so that you can better notice important events. Otherwise, with syslog event rate limiting, important events might drop off and be overlooked. Also, capture filtering settings enable you to see the system configuration file for macOS as well as the Cisco Secure Client filtering configuration files. For Linux, iptables and ip6tables outputs are visible in DART even though access to most of these configuration is restricted unless the DART tool is run via sudo.

Note
Default is the only option for macOS. You cannot customize which files to include in the bundle.

Note
If you select **Custom**, you can configure which files to include in the bundle, and specify a different storage location for the file.

Step 4 If DART seems to be taking a long time to gather the default list of files, click **Cancel**, re-run DART, and choose **Custom**, selecting fewer files.

Step 5 If you chose **Default**, DART starts creating the bundle. If you chose **Custom**, continue following the wizard prompts to specify logs, preference files, diagnostic information, and any other customizations.

Expose UDID in DART

Within the DART CLI, you can display the client's unique device identifier (UDID). For example, with Windows, go to the folder containing dartcli.exe (C:\Program Files\Cisco\Cisco Secure Client) and enter **dartcli.exe -u** or **dartclie.exe -udid**.

Collect Logs to Gather Data for Install or Uninstall Issues (for Windows)

If you have an install or uninstall failure with Cisco Secure Client, you need to collect logs, because the DART collection does not have diagnostics for this.

Run the msiexec command in the same directory where you unzipped Cisco Secure Client files:

- For install failures, enter

```
C:\Windows\temp>msiexec /i cisco-secure-client-win-version-predeploy-k9.msi /lvx
ac-install.log
```

where *ac-install.log* can be a filename of your choice.

- For uninstall failures, enter

```
C:\Windows\temp>msiexec /x cisco-secure-client-win-version-predeploy-k9.msi /lvx
ac-uninstall.log
```

where *ac-uninstall.log* can be a filename of your choice.

Note For uninstall failures, you should use the MSI specific to the version currently installed.

You can alter the same commands above to capture information about any module on Windows which is not installing or uninstalling correctly.

Get Computer System Info

For Windows type **msinfo32 /nfo c:\msinfo.nfo**.

Get Systeminfo File Dump

For Windows use the **systeminfo** command to gather info and store it in the txt file `systeminfo > c:\temp\sysinfo.txt` .

Check Registry File

An entry in the SetupAPI log file as below indicates a file cannot be found:

```
E122 Device install failed. Error 2: The system cannot find the file specified.
E154 Class installer failed. Error 2: The system cannot fine the file specified.
```

Make sure the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce registry key exists. Without this registry key, all INF install packages are forbidden.

Location of Cisco Secure Client Log Files

The logs are retained in the following files:

- Windows—`\Windows\Inf\setupapi.app.log or \Windows\Inf\setupapi.dev.log`



Note In Windows, you must make the hidden files visible.

  Because the deployment is manual, you can choose to download the installer file on the web portal and assign your own log filename.

  If an upgrade was pushed from the gateway, the log file is in the following location:

  `%WINDIR%\TEMP\cisco-secure-client-win-<version>-core-vpn-webdeploy-k9-install-yyyyyyyyyyyyy.log`.

  Obtain the most recent file for the version of the client you want to install. The *xxx* varies depending on the version, and the *yyyyyyyyyyyyy* specifies the date and time of the install.

- macOS (10.12 and later)—the logging database; use Console app or log command to query logs for VPN, DART, or Umbrella
- macOS (legacy file based log)—`/var/log/system.log` for all other modules
- Linux Ubuntu—`/var/log/syslog`
- Linux Red Hat—`/var/log/messages`

Run DART to Clear Troubleshooting Data

In Windows, you can use the DART wizard to clear the generated logs.

Procedure

Step 1 Launch DART with administrator privileges.

Step 2 Click **Clear All Logs** to start the clearing of the logs.

Cisco Secure Client Connection or Disconnection Issues

Cisco Secure Client Not Establishing Initial Connection or Not Disconnecting

Problem: Cisco Secure Client will not establish initial connection, or you get unexpected results when you click **Disconnect** on the Cisco Secure Client window.

Solution: Check the following:

- You can experience intermittent connectivity issues because the network or WiFi adapter drivers are ooutdated. Upgrade those drivers and retry.
- If you are using Citrix Advanced Gateway Client Version 2.2.1, remove the Citrix Advanced Gateway Client until the CtxLsp.dll issue is resolved by Citrix.
- If you are using AT&T Communication Manager Version 6.2 or 6.7 with an AT&T Sierra Wireless 875 card, follow these steps to correct the problem:
  1. Disable acceleration on the Aircard.
  2. Launch **AT&T communication manager > Tools > Settings > Acceleration > Startup**.
  3. Type **manual**.
  4. Click **Stop**.
- Obtain the config file from the Secure Firewall ASA to look for signs of a connection failure:
  - From the Secure Firewall ASA console, type **write net x.x.x.x:ASA-Config.txt**, where *x.x.x.x* is the IP address of the TFTP server on the network.
  - From the Secure Firewall ASA console, type **show running-config**. Cut and paste the config into a text editor and save.
- View the Secure Firewall ASA event logs:
  1. At the Secure Firewall ASA console, add the following lines to look at the ssl, webvpn, anyconnect, and auth events:

```
config terminal
logging enable
logging timestamp
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging
logging class anyconnect console debugging
```

2. Attempt connection to Cisco Secure Client, and when the connect error occurs, cut and paste the log information from the console into a text editor and save.
3. Type **no logging enable** to disable logging.

- Obtain the Cisco Secure Client log from the client computer using the Windows Event Viewer.
  1. Choose **Start** > **Run** and type **eventvwr.msc /s**.
  2. Locate the Cisco Secure Client in the Applications and Services Logs (of Windows 7) and choose **Save Log File As..**.
  3. Assign a filename, for example, `CiscoSecureClientLog.evt`. You must use the `.evt` file format.
- Modify the Windows Diagnostic Debug Utility.
  1. Attach the vpnagent.exe process as shown in the WinDbg documentation.
  2. Determine if there is a conflict with the IPv6/IPv4 IP address assignments. Look in the event logs for any idenfied conflicts.
  3. If a conflict was identified, add additional routing debugs to the registry of the client computer being used. These conflicts may appear in the Cisco Secure Client event logs as follows:

```
Function: CRouteMgr:modifyRoutingTable Return code: 0xFE06000E File: .\VpnMgr.cpp
Line:1122
Description: ROUTEMGR_ERROR_ROUTE_TABLE_VERIFICATION_FAILED.
Termination reason code 27: Unable to successfully verify all routing table
modifications are correct.

Function: CChangeRouteTable::VerifyRouteTable Return code: 0xFE070007
File: .\RouteMgr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
gr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
```

  4. Enable route debugging on a one-time basis for a connection by adding a specific registry entry (Windows) or file (Linux and macOS).
     - On 32-bit Windows, the DWORD registry value must be `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco Secure Client\DebugRoutesEnabled`
     - On 64-bit Windows, the DWORD registry value must be `HKEY_LOCAL_MACHINE\Software\WOW6432node\Cisco\Cisco Secure Client\DebugRoutesEnabled`
     - On Linux or macOS, create a file in the following path using the sudo touch command: `/opt/cisco/secureclient/vpn/debugroutes`

Note The key or file is deleted when the tunnel connection is started. The value of the key or content of the file is not important as the existence of the key or file is sufficient to enable debugging.

Start a VPN connection. When this key or file is found, two route debug text files are created in the system temp directory (usually C:\Windows\Temp on Windows and /opt/cisco/secureclient/vpn on macOS or Linux). The two files (debug_routechangesv4.txt4 and debug_routechangesv6.txt) are overwritten if they already exist.

Cisco Secure Client Not Passing Traffic

Problem: Cisco Secure Client cannot send data to the private network once connected.

Solution: Check the following:

- If you are using AT&T Communication Manager Version 6.2 or 6.7 with an AT&T Sierra Wireless 875 card, follow these steps to correct the problem:
  1. Disable acceleration on the Aircard.
  2. Launch AT&T communication manager > Tools > Settings > Acceleration > Startup.
  3. Type **manual**.
  4. Click **Stop**.
- Obtain the output of the **show vpn-sessiondb detail anyconnect filter name <username>** command. If the output specifies Filter Name: XXXXX, get the output for the show access-list XXXXX command as well. Verify that the ACL is not blocking the intended traffic flow.
- Obtain the DART file or the output from Cisco Secure Client > Statistics > Details > Export (AnyConnect-ExportedStats.txt). Observe the statistics, interfaces, and routing table.
- Check the Secure Firewall ASA config file for NAT statements. If NAT is enabled, you must exempt data returning to the client from network address translation. For example, to NAT exempt the IP addresses from the Cisco Secure Client pool, the following code would be used:

  ```
  access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
  ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
  nat (inside) 0 access-list in_nat0_out
  ```

- Verify whether the tunneled default gateway is enabled for the setup. The traditional default gateway is the gateway of last resort for non-decrypted traffic:

  ```
  route outside 0.0.209.165.200.225
  route inside 0 0 10.0.4.2 tunneled
  ```

  If a VPN client needs to access a resource that is not in the routing table of the VPN gateway, packets are routed by the standard default gateway. The VPN gateway does not need to have the whole internal routing table. If you use a tunneled keyword, the route handles decrypted traffic coming from IPsec/SSL VPN connection. Standard traffic routes to 209.165.200.225 as a last resort, while traffic coming from the VPN routes to 10.0.4.2 and is decrypted.
- Collect a text dump of ipconfig /all and a route print output before and after establishing a tunnel with Cisco Secure Client.
- Perform a network packet capture on the client or enable a capture on the Secure Firewall ASA.



Note If some applications (such as Microsoft Outlook) do not operate with the tunnel, ping a known device in the network with a scaling set of pings to see what size gets accepted (for example, ping -| 500, ping -| 1000, ping -| 1500, and ping -| 2000). The ping results provide clues to the fragmentation issues in the network. Then you can configure a special group for users who might experience fragmentation and set the anyconnect mtu for this group to 1200. You can also copy the Set MTU.exe utility from the old IPsec client and force the physical adapter MTU to 1300. Upon reboot, see if you notice a difference.

Connectivity Issues with VM-based Subsystems

If you experience connectivity issues with Windows Subsystem for Linux (WSL2) or VMware Fusion VM when the AnyConnect VPN is active on the host (Windows 10 or macOS 11 (and later), follow these steps to configure Local LAN split exclude tunneling restricted to only virtual adapter subnets.

Procedure

Step 1 In ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes** to configure a new custom attribute type.

Step 2 Choose **Add** and set the following in the Create Custom Attribute pane:

a) Enter **BypassVirtualSubnetsOnlyV4** for IPv4 or **BypassVirtualSubnetsOnlyV6** for IPv6 as the new type.

b) Optionally, enter a description.

c) Set the name and value to *true* in **AnyConnect Custom Attributes Names**.

If the local LAN wildcard split exclude is already configured in the group policy for a certain IP protocol, it is restricted by the client to only virtual subnets, provided that the custom attribute is enabled for the same IP protocol. If the local LAN wildcard split exclude is not configured in the group policy, it is added by the client for the IP protocol(s) with the custom attribute enabled, resulting in restricted local LAN split exclude being enforced accordingly. With no other split-exclude networks configured, all physical adapter traffic is tunneled, similar to the tunnel-all configuration.

Step 3 Attach the previously created custom attribute type and name to a group policy via **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Edit >Advanced > AnyConnect Client > Custom Attributes**.

What to do next

To verify if the attribute value was set correctly, check the Cisco Secure Client logs for a message starting with "Received VPN Session Configuration." It should say that local LAN Wildcard is limited to virtual subnets.

ZTA Enrollment URL Timeout (Linux)

On Linux, the embedded browser used during enrollment relies on the WebKitGTK framework. This framework supports proxying network traffic when configured. If the proxy settings are misconfigured, URL timeouts may occur during enrollment and appear in the logs. Use the following command to check the user-specific proxy configuration:

```
gsettings get org.gnome.system.proxy mode
```

You can update the configuration using the following per-user settings command:

```
gsettings set org.gnome.system.proxy mode 'none'
```

- 'none'—No proxy is used
- 'manual'—Proxy settings are manually configured (per protocol like HTTP, HTTPS, and so on)
- 'auto'—Proxy settings are automatically configured, typically via a PAC (Proxy Auto-Config) URL

VPN Service Failures

VPN Service Connection Fails

Problem: You receive an "Unable to Proceed, Cannot Connect to the VPN Service" message. The VPN service for Cisco Secure Client is not running.

Solution: Determine if another application conflicted with the service. See Determine What Conflicted With Service, page 11-7.

Determine What Conflicted With Service

The following procedure determines if the conflict is with the initialization of the server at boot-up or with another running service, for example, because the service failed to start.

Procedure

Step 1 Check the services under the Windows Administration Tools to ensure that the Cisco Secure Client VPN Agent is *not* running. If it is running and the error message still appears, another VPN application on the workstation may need disabled or even uninstalled. After taking that action, reboot, and repeat this step.

Step 2 Try to start the Cisco Secure Client VPN Agent.

Step 3 Check the Cisco Secure Client logs in the Event Viewer for any messages stating that the service was unable to start. Notice the timestamps of the manual restart from Step 2, as well as when the workstation was booted up.

Step 4 Check the System and Application logs in the Event Viewer for the same general time stamps of any messages of conflict.

Step 5 If the logs indicate a failure starting the service, look for other information messages around the same time stamp which indicate one of the following:

- a missing file—reinstall Cisco Secure Client from a standalone MSI installation to rule out a missing file.
- a delay in another dependent service—disable startup activities to speed up the workstation's boot time.
- a conflict with another application or service—determine whether another service is listening on the same port as the port the vpnagent is using or if some HIDS software is blocking our software from listening on a port.

Step 6 If the logs do not point directly to a cause, use the trial and error method to identify the conflict. When the most likely candidates are identified, disable those services (such as VPN products, HIDS software, spybot cleaners, sniffers, antivirus software, and so on) from the Services panel.

Step 7 Reboot. If the VPN Agent service still fails to start, start turning off services that were not installed by a default installation of the operating system.

VPN Client Driver Encounters Error (after a Microsoft Windows Update)

Problem: If you recently updated the Microsoft certclass.inf file, the following message is encountered when trying to establish a VPN connection:

```
The VPN client driver has encountered an error.
```

If you check the C:\WINDOWS\setupapi.log, you can see the following error:

```
#W239 The driver signing class list "C:\WINDOWS\INF\certclass.inf" was missing or invalid.
 Error 0xfffffbf8: Unknown Error. Assuming all device classes are subject to driver signing
 policy.
```

Solution: Check which updates have recently been installed by entering **C:\>systeminfo** at the command prompt or checking the C:\WINDOWS\WindowsUpdate.log. Follow the instructions to repair the VPN driver.

Repair VPN Client Driver Error

Even though the steps taken above may indicate that the catalog is not corrupt, the key file(s) may still have been overwritten with an unsigned one. If the failure still occurs, open a case with Microsoft to determine why the driver signing database is being corrupted.

Procedure

Step 1 Open a command prompt as an admin.

Step 2 Enter **net stop CryptSvc**.

Step 3 Analyze the database to verify its validity by entering **esentutl /g %systemroot%\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb** or rename the following directory: %/WINDIR%\system32\catroot2 to catroot2_old.

Step 4 When prompted, choose **OK** to attempt the repair. Exit the command prompt and reboot.

Driver Crashes

Fix Driver Crashes in VPNVA.sys

Problem: VPNVA.sys driver crashes.

Solution: Find any intermediate drivers that are bound to the Cisco Secure Client Virtual Adapter and uncheck them.

Fix Driver Crashes in vpnagent.exe

Procedure

Step 1 Create a directory called c:\vpnagent.

Step 2 Look at the Process tab in the Task Manager and determine the PID of the process in vpnagent.exe.

Step 3 Open a command prompt and change to the directory where you installed the debugging tools. By default, the debugging tools for Windows are located in `C:\Program Files\Debugging Tools`.

Step 4 Type **cscript vpnagent4.vbs -crash -p PID -o c:\vpnagent -nodumponfirst**, where *PID* is the PID of **vpnagent.exe**.

Step 5 Let the open window run in minimized state. You cannot log off of the system while you are monitoring.

Step 6 When the crash occurs, collect the contents of c:\vpnagent in a zip file.

Step 7 Use **!analyze -v** to further diagnose the crashdmp file.

Link/Driver Issues with Network Access Manager

If the Network Access Manager fails to recognize your wired adapter, try unplugging your network cable and reinserting it. If this does not work, you may have a link issue. The Network Access Manager may not be able to determine the correct link state of your adapter. Check the Connection Properties of your NIC driver. You may have a "Wait for Link" option in the Advanced Panel. When the setting is On, the wired NIC driver initialization code waits for auto negotiation to complete and then determines if a link is present.



Note Certain older Intel NIC do not support WPA3. If you attempt to create a WPA3 network using one of these cards (Intel 72xx and 82xx), Network Access Manager will not be able to complete the connection.

Other Crashes

Cisco Secure Client Crashes

Problem: You received a “the system has recovered from a serious error” message after a reboot.

Solution: Gather the .log and .dmp generated files from the %temp% directory (such as C:\DOCUME~1\jsmith\LOCALS~1\Temp). Copy the files or back them up. See How to Back Up .log or .dmp Files, page 11-9.

How to Back Up .log or .dmp Files

Procedure

Step 1 Run the Microsoft utility called Dr. Watson (Drwtsn32.exe) from the Start > Run menu.

Step 2 Configure the following and click **OK**:

```
Number of Instructions     : 25
Number of Errors to Save : 25
Crash Dump Type   : Mini
Dump Symbol Table : Checked
Dump All Thread Contexts : Checked
Append to Existing Log File : Checked
Visual Notification : Checked
Create Crash Dump File : Checked
```

Step 3 On the client device, get the Cisco Secure Client VPN client log from the Windows Event Viewer by entering **eventvwr.msc /s** at the Start > Run menu.

Step 4 Locate the Cisco Secure Client in the Applications and Services Logs (of Windows) and choose **Save Log File As..**. Assign a filename such as CiscoSecureClientLog.evt in the .evt file format.

Cisco Secure Client Crashes in vpndownloader (Layered Service Provider (LSP) Modules and NOD32 AV)

Problem: When Cisco Secure Client attempts to establish a connection, it authenticates successfully and builds the ssl session, but then it crashes in the vpndownloader if using LSP or NOD32 AV.

Solution: Remove the Internet Monitor component in version 2.7 and upgrade to version 3.0 of ESET NOD32 AV.

Blue Screen (AT & T Dialer)

Problem: If you are using an AT&T Dialer, the client operating system sometimes experiences a blue screen, which causes the creation of a mini dump file.

Solution: Upgrade to the latest 7.6.2 AT&T Global Network Client.

Security Alerts

Microsoft Internet Explorer Security Alert

Problem: A security alert window appears in Microsoft Internet Explorer with the following text:

```
Information you exchange with this site cannot be viewed or changed by others. However,
there is a problem with the site's security certificate. The security certificate was issued
 by a company you have not chosen to trust. View the certificate to determine whether you
want to trust the certifying authority.
```

Solution: This alert may appear when connecting to a Secure Firewall ASA that is is not recognized as a trusted site. To prevent this alert, install a trusted root certificate on a client. See Install Trusted Root Certificates on a Client, page 11-10.

"Certified by an Unknown Authority" Alert

Problem: A “Web Site Certified by an Unknown Authority” alert window may appear in the browser. The upper half of the Security Alert window shows the following text:

```
Unable to verify the identity of <Hostname_or_IP_address> as a trusted site.
```

Solution: This security alert may appear when connecting to a Secure Firewall ASA that is not recognized as a trusted site. To prevent this alert, install a trusted root certificate on a client. See Install Trusted Root Certificates on a Client, page 11-10.

Install Trusted Root Certificates on a Client

Before you begin

Generate or obtain the certificate to be used as the trusted root certificate.

Note You can avoid security certificate warnings in the short term by installing a self-signed certificate as a trusted root certificate on the client. However, we do not recommend this because of the possibility that a user could inadvertently configure a browser to trust a certificate on a rogue server and because of the inconvenience to users of having to respond to a security warning when connecting to your secure gateway.

Procedure

Step 1 Click **View Certificate** in the Security Alert window.
Step 2 Click **Install Certificate**.
Step 3 Click **Next**.
Step 4 Select **Place all certificates in the following store**.
Step 5 Click **Browse**.
Step 6 In the drop-down list, choose **Trusted Root Certification Authorities**.
Step 7 Continue following the Certificate Import wizard prompts.

Dropped Connections

Wireless Connection Drops When Wired Connection is Introduced (Juniper Odyssey Client)

Problem: When wireless suppression is enabled on an Odyssey client, the wireless connection drops if a wired connection is introduced. With wireless suppression disabled, the wireless operates as expected.

Solution: Configure the Odyssey Client, page 11-11.

Configure the Odyssey Client

Procedure

Step 1 In Network Connections, copy the name of the adapter as it appears in its connection properties. If you edit the registry, perform a backup before making any changes and use caution as serious problems can occur if modified incorrectly.
Step 2 Open the registry and go to HKEY_LOCAL_MACHINE\SOFTWARE\Funk Software, Inc.\odyssey\client\configuration\options\adapterType\virtual.

Step 3 Create a new string value under virtual. Copy the name of the adapter from Network properties into the registry portion. The additional registry settings, once saved, are ported over when a customer MSI is created and is pushed down to other clients.

Connections to the Secure Firewall ASA Fail (Kaspersky AV Workstation 6.x)

Problem: When Kaspersky 6.0.3 is installed (even if disabled), Cisco Secure Client connections to the Secure Firewall ASA fail right after CSTP state = CONNECTED. The following message appears:

```
SVC message: t/s=3/16: Failed to fully establish a connection to the secure gateway (proxy
 authentication, handshake, bad cert, etc.).
```

Solution: Uninstall Kaspersky and refer to their forums for additional updates.

No UDP DTLS Connection (McAfee Firewall 5)

Problem: When using McAfee Firewall 5, a UDP DTLS connection cannot be established.

Solution: In the McAfee Firewall central console, choose **Advanced Tasks > Advanced options and Logging** and uncheck the **Block incoming fragments automatically** checkbox in McAfee Firewall.

Connection to the Host Device Fails (Microsoft Routing and Remote Access Server)

Problem: If you are using RRAS, the following termination error is returned to the event log when Cisco Secure Client attempts to establish a connection to the host device:

```
Termination reason code 29 [Routing and Remote Access service is running]
The Windows service “Routing and Remote Access” is incompatible with the Cisco Secure Client.
```

Solution: Disable the RRAS service.

Failed Connection/Lack of Credentials (Load Balancers)

Problem: The connection fails due to lack of credentials.

Solution: The third-party load balancer has no insight into the load on the Secure Firewall ASA devices. Because the load balance functionality in the ASA is intelligent enough to evenly distribute the VPN load across the devices, we recommend using the internal Secure Firewall ASA load balancing instead.

Installation Failures

Do Not Edit Windows Registry Without Root Cause

If you are receiving a failure while installing, uninstalling, or upgrading Cisco Secure Client, we do not recommend modifying the Windows Installer registry keys directly, because it can lead to undesired consequences. Microsoft-provided tools can troubleshoot installer issues after proper root cause is determined.

Cisco Secure Client Fails to Download (Wave EMBASSY Trust Suite)

Problem: Cisco Secure Client fails to download and produces the following error message:

```
"Cisco AnyConnect VPN Client Downloader has encountered a problem and needs to close."
```

Solution: Upload the patch update to version 1.2.1.38 to resolve all dll issues.

Incompatability Issues

Failure to Update the Routing Table (Bonjour Printing Service)

Problem: If you are using Bonjour Printing Services, the Cisco Secure Client event logs indicate a failure to identify the IP forwarding table.

Solution: Disable the BonJour Printing Service by typing **net stop "bonjour service"** at the command prompt. A new version of mDNSResponder (1.0.5.11) has been produced by Apple. To resolve this issue, a new version of Bonjour is bundled with iTunes and made available as a separate download from the Apple web site.

Version of TUN is Incompatible (OpenVPN Client)

Problem: An error indicates that the version of TUN is already installed on this system and is incompatible with the Cisco Secure Client.

Solution: Uninstall the Viscosity OpenVPN Client.

Winsock Catalog Conflict (LSP Symptom 2 Conflict)

Problem: If an LSP module is present on the client, a Winsock catalog conflict may occur.

Solution: Uninstall the LSP module.

Slow Data Throughput (LSP Symptom 3 Conflict)

Problem: Slow data throughput may occur with the use of NOD32 Antivirus V4.0.468 x64 using Windows.

Solution: Disable SSL protocol scanning. See Disable SSL Protocol Scanning.

Disable SSL Protocol Scanning

Procedure

Step 1 Go to **Protocol Filtering** > **SSL** in the Advanced Setup and enable SSL protocol scanning.

Step 2 Go to **Web access protection** > **HTTP, HTTPS** and check **Do not use HTTPS protocol checking**.

Step 3 Go back to **Protocol filtering** > **SSL** and disable **SSL protocol scanning.**

DPD Failure (EVDO Wireless Cards and Venturi Driver)

Problem: If you are using a EVDO wireless card and Venturi driver while a client disconnect occurred, the event log reports the following:

```
%ASA-5-722037: Group <Group-Name> User <User-Name> IP <IP-Address> SVC closing connection:
 DPD failure.
```

Solution:

- Check the Application, System, and Cisco Secure Client event logs for a relating disconnect event and determine if a NIC card reset was applied at the same time.
- Ensure that the Venturi driver is up to date. Disable **Use Rules Engine** in the 6.7 version of the AT&T Communications Manager.

DTLS Traffic Failing (DSL Router)

Problem: If you are connecting with a DSL router, DTLS traffic may fail even if successfully negotiated.

Solution: Connect to a Linksys router with factory settings. This setting allows a stable DTLS session and no interruption in pings. Add a rule to allow DTLS return traffic.

NETINTERFACE_ERROR (CheckPoint and other Third-Party Software such as Kaspersky)

Problem: When attempting to retrieve operating system information on the computer's network used to make the SSL connection, the Cisco Secure Client log may indicate a failure to fully establish a connection to the secure gateway.

Solution:

- If you are uninstalling the Integrity Agent and then installing Cisco Secure Client, enable TCP/IP.
- Ensure that if you disable SmartDefense on Integrity agent installation, TCP/IP is checked.
- If third-party software is intercepting or otherwise blocking the operating system API calls while retrieving network interface information, check for any suspect AV, FW, AS, and such.

- Confirm that only one instance of the Cisco Secure Client adapter appears in the Device Manager. If there is only one instance, authenticate with Cisco Secure Client, and after 5 seconds, manually enable the adapter from the Device Manager.
- If any suspect drivers have been enabled within the Cisco Secure Client adapter, disable them by unchecking them in the Connection window of Cisco Secure Client.

Performance Issues (Virtual Machine Network Service Drivers)

Problem: When using Cisco Secure Client on some Virtual Machine Network Service devices, performance issues have resulted.

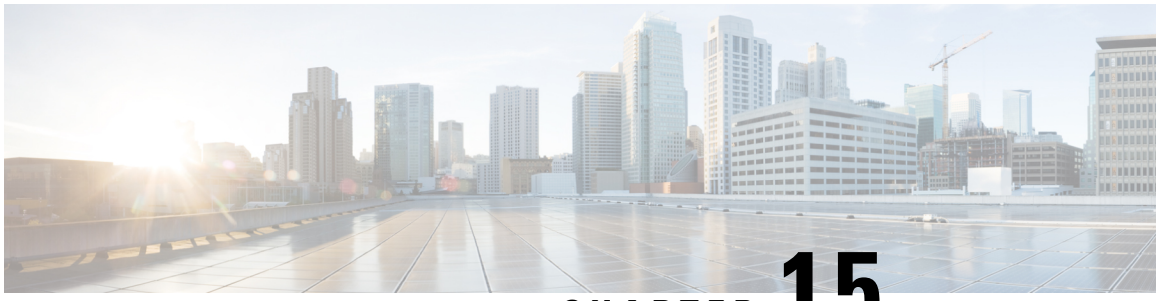
Solution: Uncheck the binding for all IM devices within the Cisco Secure Client virtual adapter. The application dsagent.exe resides in C:\Windows\System\dgagent. Although it does not appear in the process list, you can see it by opening sockets with TCPview (sysinternals). When you terminate this process, normal operation of Cisco Secure Client returns.

Known Third-Party Application Conflicts

The following third-party applications have known complications with Cisco Secure Client:

- Adobe and Apple—Bonjour Printing Service
  - Adobe Creative Suite 3
  - BonJour Printing Service
  - iTunes
- AT&T Communications Manager Versions 6.2 and 6.7
  - AT&T Sierra Wireless 875 card
- AT&T Global Dialer
- CheckPoint and other Third-Party Software such as Kaspersky
- Cisco Secure Client for Apple iOS on Apple M1 devices running the same time as Cisco Secure Client on macOS
- Cisco Secure Client on Universal Windows Platform
- Citrix Advanced Gateway Client Version 2.2.1
- DSL routers
- EVDO Wireless Cards and Venturi Driver
- Firewall Conflicts
  - Third-party firewalls can interfere with the firewall function configured on the Secure Firewall ASA group policy.
- Juniper Odyssey Client

- Kaspersky AV Workstation 6.x
- Layered Service Provider (LSP) Modules and NOD32 AV
- Load balancers
- McAfee Firewall 5
- Microsoft Internet Explorer 8
- Microsoft Routing and Remote Access Server
- Microsoft VPN
- OpenVPN client
- Pulse Secure
- Virtual Machine Network Service Drivers
- Wave EMBASSY Trust Suite



CHAPTER 15

Cisco Secure Client Changes Related to macOS 11 (And Later)

On macOS 11 and later, Cisco Secure Client leverages the macOS System Extension framework, while it formerly used the now-deprecated Kernel Extension Framework. An administrator must approve the Cisco Secure Client system extension as described in the sections below. Also, if a critical system extension (or related OS framework) issue is encountered, you can follow the steps for failing over to the Cisco Secure Client kernel extension, as a last resort workaround, but it is installed solely for this purpose and is no longer used by default.

- About the Cisco Secure Client System Extension, on page 319
- Approving the Cisco Secure Client System Extension, on page 320
- Deactivate the Cisco Secure Client System Extension, on page 321
- Failover to Kernel Extension, on page 322
- Sample MDM Configuration Profile for Cisco Secure Client System Extension Approval , on page 323
- Sample MDM Configuration Profile for Cisco Secure Client Managed Login Items, on page 326

About the Cisco Secure Client System Extension

Cisco Secure Client uses a network system extension on macOS 11 (and later), bundled into an application named Cisco Secure Client - Socket Filter. The app controls the extension activation and deactivation and is installed under /Applications/Cisco.

The Cisco Secure Client extension has the following three components that are visible in the macOS System Preferences-Network UI window:

- DNS proxy
- App/transparent proxy
- Content filter

Cisco Secure Client requires its system extension and all its components to be active for proper operation, which implies that the mentioned components are all present and show as green (running) in the left pane of the macOS Network UI.

If a third-party product is employing a system extension with DNS proxy capabilities, either Cisco Secure Client or the third-party product (or both), may not function properly. macOS only supports one active DNS proxy extension at a time.

Approving the Cisco Secure Client System Extension

The Cisco Secure Client system extension activation requires either approval by an end user with administrator rights or MDM approval:

- Approve the System Extension Loading/Activation, on page 320
- Approve the System Extension Using MDM, on page 320

Approve the System Extension Loading/Activation

Approve the Cisco Secure Client system extension and its content filter component by following the OS prompts or the more explicit Cisco Secure Client - Notification application's instructions.

Procedure

Step 1 When you receive the "System Extension Blocked" message from macOS, perform this operation:

- For macOS 15 (and later), click the **Open System Settings** button in the Cisco Secure Client - Notification app and then choose **Network Extensions** in System Settings > General > Login Items & Extensions section.
- For macOS 13 and 14, click the **Open Preferences** button in the Cisco Secure Client - Notification app, or the **Open Security Preferences** button. You can also navigate to the System Preferences application and go to the Security&Privacy window.

Step 2 Click the bottom-left lock and provide the requested credentials to unlock.

Step 3 For macOS 15, click to allow the Cisco Secure Client Socket Filter. For macOS 13 or 14, click **Allow** on the Security & Privacy window to accept the Cisco Secure Client - Socket Filter extension.

You will receive a "System Extension Enabled" message.

Approve the System Extension Using MDM

Approve the Cisco Secure Client system extension without end user interaction using a management profile's SystemExtensions payload with the following settings:

Property	Value
Team Identifier	DE8Y96K9QP
Bundle Identifier	com.cisco.anyconnect.macos.acsockext
System Extension Type	NetworkExtension

Approve the extension's content filter component with the following WebContentFilter payload settings:

Property	Value
AutoFilterEnabled	false
FilterBrowsers	false
FilterSockets	true
FilterPackets	false
FilterGrade	firewall
FilterDataProviderBundleIdentifier	com.cisco.anyconnect.macos.acsockext
FilterDataProviderDesignatedRequirement	anchor apple generic and identifier "com.cisco.anyconnect.macos.acsockext" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = DE8Y96K9QP)
PluginBundleID	com.cisco.anyconnect.macos.acsock
VendorConfig	
UserDefinedName	Cisco AnyConnect Content Filter

Confirm Activation of Cisco Secure Client System Extension

To confirm that the Cisco Secure Client system extension has been approved and activated, run the **systemextensionsctl list** command:

```
% systemextensionsctl list
1 extension(s)
--- com.apple.system_extension.network_extension
enabled active teamID bundleID (version) name [state]
* * DE8Y96K9QP com.cisco.anyconnect.macos.acsockext
(5.0.00xxx/5.0..00xxx) Cisco Secure Client - Socket Filter Extension
[activated enabled]
```

You can also check the System Preferences network UI to confirm that all three Cisco Secure Client extension components are active.

Deactivate the Cisco Secure Client System Extension

During Cisco Secure Client uninstallation, the user is prompted for administrator credentials to approve the system extension deactivation. On macOS 12 and later, the Cisco Secure Client system extension can be silently removed after deploying a management profile with the RemovableSystemExtensions property added to the SystemExtensions payload. This property must contain the bundle identifier of the Cisco Secure Client system extension (com.cisco.anyconnect.macos.acsockext).

Note You should only use this management profile configuration when the administrator wants to automate the Cisco Secure Client uninstallation, as it grants any user or process with root privileges the ability to remove the Cisco Secure Client system extension, without prompting the user for a password.

Failover to Kernel Extension

Cisco Secure Client still installs its kernel extension on macOS 11 (and later versions); however, you should use it only as a fallback in the event of a critical system extension (or related OS framework) issue or with instruction by Cisco Technical Assistance Center (TAC). Kernel extensions require approval via MDM before loading on macOS 11 (and later). End user approval is no longer an option.

Before you begin

Use these steps only as a last-resort workaround.

Procedure

Step 1 Approve the Cisco Secure Client kernel extension using a management profile's *SystemPolicyKernelExtensions* payload with the following settings:

Property	Value
Team Identifier	DE8Y96K9QP
Bundle Identifier	com.cisco.kext.acsock

The MDM configuration profile is installed.

Step 2 Run the following command that causes Cisco Secure Client to deactivate the system extensions and start using the kernel extension instead. You will be prompted for administrator credentials.

- If running a version higher than 5.0.00556, enter **% sudo launchctl unload /Library/LaunchDaemons/com.cisco.secureclient.vpnagentd.plist && /Applications/Cisco/Cisco\ Secure\ Client\ -\ Socket\ Filter.app/Contents/MacOS/Cisco\ Secure\ Client\ -\ Socket\ Filter -deactivateExt && echo kext=1 | sudo tee /opt/cisco/secureclient/kdf/acsock.cfg && sudo launchctl load /Library/LaunchDaemons/com.cisco.secureclient.csc_vpnagentd.plist**
- If running version 5.0.00556, enter **% sudo launchctl unload /Library/LaunchDaemons/com.cisco.secureclient.csc_vpnagentd.plist && /Applications/Cisco/Cisco\ Secure\ Client\ -\ Socket\ Filter.app/Contents/MacOS/Cisco\ Secure\ Client\ -\ Socket\ Filter -deactivateExt && echo kext=1 | sudo tee /opt/cisco/secureclient/kdf/acsock.cfg && sudo launchctl load /Library/LaunchDaemons/com.cisco.secureclient.csc_vpnagentd.plist**

Step 3 Run the following command to verify that the kernel extension was loaded: **% kextstat | grep com.cisco.kext.acsock**

If Cisco Secure Client failed to load its kernel extension, perform a reboot.

Revert Back to System Extension

If Cisco TAC confirms a fix to the system extension issue (and eliminates the needs for the failover to kernel extension), run the following command, which instructs Cisco Secure Client to switch back to the system extension. The command depends on the version of Cisco Secure Client you are running.

If a version higher than 5.0.00556, run this:

```
% sudo launchctl unload /Library/LaunchDaemons/com.cisco.secureclient.vpnagentd.plist &&
sudo kextunload -b com.cisco.kext.acsock && sudo rm /opt/cisco/secureclient/kdf/acsock.cfg
 && sudo launchctl load /Library/LaunchDaemons/com.cisco.secureclient.csc_vpnagentd.plist
```

If running version 5.0.00556, run this:

```
% sudo launchctl unload /Library/LaunchDaemons/com.cisco.secureclient.csc_vpnagentd.plist
&& sudo kextunload -b com.cisco.kext.acsock && sudo rm /opt/cisco/secureclient/kdf/acsock.cfg
 && sudo launchctl load /Library/LaunchDaemons/com.cisco.secureclient.csc_vpnagentd.plist
```

```
% osascript -e 'quit app "Cisco Secure Client - AnyConnect VPN Service.app"' && open -W -a
"/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app" --args
uninstall && sudo /opt/cisco/secureclient/kdf/bin/acsocktool -kfr && open -a
"/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app"% sudo launchctl
unload /Library/LaunchDaemons/com.cisco.secureclient.vpnagentd.plist && sudo
/opt/cisco/secureclient/kdf/bin/acsocktool -kfr && sudo launchctl load
/Library/LaunchDaemons/com.cisco.secureclient.vpnagentd.plist
```

Sample MDM Configuration Profile for Cisco Secure Client System Extension Approval

Use the following MDM configuration profile to load both the Cisco Secure Client system and the kernel extensions, including the system extension's content filter component.

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0">

      <dict>

      <key>PayloadContent</key>

      <array>

      <dict>

                  <key>AllowUserOverrides</key>

                  <true/>

                  <key>AllowedSystemExtensions</key>

                  <dict>

                        <key>DE8Y96K9QP</key>

                        <array>
```

```
                        <string>com.cisco.anyconnect.macos.acsockext</string>
                        </array>
                </dict>
                <key>PayloadDescription</key>
                <string></string>
                <key>PayloadDisplayName</key>
                <string>Cisco
Secure Client System Extension</string>
                <key>PayloadEnabled</key>
                <true/>
                <key>PayloadIdentifier</key>
                <string>A8364220-5D8D-40A9-Af66-1Fbfef94E116</string>
                <key>PayloadOrganization</key>
                <string>Cisco Systems, Inc.</string>
                <key>PayloadType</key>
                <string>com.apple.system-extension-policy</string>
                <key>PayloadUUID</key>
                <string>A8364220-5D8D-40A9-Af66-1Fbfef94E116</string>
                <key>PayloadVersion</key>
                <integer>1</integer>
            </dict>
            <dict>
                <key>Enabled</key>
                <true/>
                <key>AutoFilterEnabled</key>
                <false/>
                <key>FilterBrowsers</key>
                <false/>
                <key>FilterSockets</key>
                <true/>
                <key>FilterPackets</key>
                <false/>
                <key>FilterType</key>
```

```
                    <string>Plugin</string>

                    <key>FilterGrade</key>

                    <string>firewall</string>

                    <key>PayloadDescription</key>

                    <string></string>

                    <key>PayloadDisplayName</key>

                    <string>Cisco
          Secure Client Content Filter</string>

                    <key>PayloadIdentifier</key>


<string>com.apple.webcontent-filter.339Ec532-9Ada-480A-Bf3D-A535F0F0B665</string>

                    <key>PayloadType</key>

                    <string>com.apple.webcontent-filter</string>

                    <key>PayloadUUID</key>

                    <string>339Ec532-9Ada-480A-Bf3D-A535F0F0B665</string>

                    <key>PayloadVersion</key>

                    <integer>1</integer>

                    <key>FilterDataProviderBundleIdentifier</key>

                    <string>com.cisco.anyconnect.macos.acsockext</string>

                    <key>FilterDataProviderDesignatedRequirement</key>

                    <string>anchor apple generic and identifier
"com.cisco.anyconnect.macos.acsockext" and (certificate leaf[field.1.2.840.113635.100.6.1.9]
 /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
 leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
DE8Y96K9QP)</string>

                    <key>PluginBundleID</key>

                    <string>com.cisco.anyconnect.macos.acsock</string>

                    <key>UserDefinedName</key>

                    <string>Cisco AnyConnect Content Filter</string>

               </dict>

          </array>

          <key>PayloadDescription</key>

          <string></string>

          <key>PayloadDisplayName</key>

          <string>Approved Cisco
```

```
      Secure Client System and Kernel Extensions</string>

    <key>PayloadEnabled</key>

    <true/>

    <key>PayloadIdentifier</key>

    <string>A401Bdc2-4Ab1-4406-A143-11F077Baf52B</string>

    <key>PayloadOrganization</key>

    <string>Cisco Systems, Inc.</string>

    <key>PayloadRemovalDisallowed</key>

    <true/>

    <key>PayloadScope</key>

    <string>System</string>

    <key>PayloadType</key>

    <string>Configuration</string>

    <key>PayloadUUID</key>

    <string>A401Bdc2-4Ab1-4406-A143-11F077Baf52B</string>

    <key>PayloadVersion</key>

    <integer>1</integer>

</dict>

</plist>
```

Sample MDM Configuration Profile for Cisco Secure Client Managed Login Items

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <array>
        <dict>
            <key>PayloadIdentifier</key>
            <string>com.example.myservicemanagementpayload</string>
            <key>PayloadUUID</key>
            <string>0d4e2ece-dfa7-4103-97ff-e91a9f842a1d</string>
            <key>PayloadType</key>
            <string>com.apple.servicemanagement</string>
            <key>Rules</key>
            <array>
                <dict>
                    <key>RuleType</key>
                    <string>BundleIdentifierPrefix</string>
```

```
                    <key>RuleValue</key>
                    <string>com.cisco.secureclient</string>
                    <key>Comment</key>
                    <string>All apps from CSC</string>
                </dict>
            </array>
        </dict>
    </array>
    <key>PayloadDisplayName</key>
    <string>Service Management</string>
    <key>PayloadIdentifier</key>
    <string>com.example.myprofile</string>
    <key>PayloadUUID</key>
    <string>03cca12c-a610-44c2-96f9-fdabe3acd47d</string>
    <key>PayloadType</key>
    <string>Configuration</string>
    <key>PayloadScope</key>
    <string>System</string>
</dict>
</plist>
```