

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 29
- Updating Cisco Secure Client Software and Profiles, on page 36

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.
- 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.

Due to a new Apple API change, when using webdeploy to upgrade from macOS Cisco Secure Client 5.0.x (or earlier) to 5.1.x (or later), you must have administrator privileges or manage the macOS devices via MDM to pre-approve the application extension. This restriction does not apply to Windows or Linux.

- 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: anyconnect-linux64-<*version*>-predeploy-k9.tgz.

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 12.

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 15.

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
Linux (64-bit)	(for RPM installer) cisco-secure-client-linux64-*version*-predeploy-rpm-k9.tgz (for DEB installer) cisco-secure-client-linux64-*version*-predeploy-deb-k9.tgz (for RPM ARM64) cisco-secure-client-linux-arm64-version-predeploy-rpm-k9.tgz for DEB ARM64) cisco-secure-client-linux-arm64-version-predeploy-deb-k9.tgz

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
- ThousandEyes
- Zero Trust Access
- Endpoint Data Loss Prevention

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 Secure Client and Installer.

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 Zero Trust Access Module, Umbrella Roaming Security Module, Network Access Manager, ISE Posture, Network Visibility Module, ThousandEyes Module or Secure Endpoint Data Loss Prevention 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 (on prem)	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
Endpoint Data Loss Prevention	n/a	cisco-secure-client-win-*version*-edlp-predeploy-k9.msi
Network Visibility Module (XDR)	n/a	Cloud Managed only
Endpoint Visibility Module	n/a	Cloud Managed only
Forensics	n/a	Cloud Managed only
Orbital	n/a	Cloud Managed only
Secure Access Root Certificate	n/a	Cloud Managed only

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
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

Module	Location
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.
Endpoint Data Loss Prevention	%ProgramData%\Cisco\Cisco Secure Client\EDLP\enrollments
macOS	
Zero Trust Access	(binaries) /opt/cisco/secureclient/zta/bin (config and other files) /opt/cisco/secureclient/zta
ISE Posture	/opt/cisco/secureclient/iseposture/
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.
AnyConnect VPN Profile	/opt/cisco/secureclient/vpn/profile
Linux	
Zero Trust Access	(binaries) /opt/cisco/secureclient/zta/bin (libraries) /opt/cisco/secureclient/zta/lib (config and other files) /opt/cisco/secureclient/zta (and subdirectories)
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

Linux Binaries and Libraries

- **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.

Deploying Network Visibility Module for Cloud

Follow these steps to set up and deploy the Network Visibility Module for cloud (XDR) use and run it as a standalone application without Secure Client VPN.

Procedure

Step 1 Create a custom deployment in XDR and opt only for the Cloud Management module.

Step 2 Download the installer generated from the XDR custom deployment and Cloud Management selection above and install it on the endpoints.

Step 3 Navigate within XDR to **Client Management** > **Profiles** and download the Network Visibility Module Cloud Default profile. Rename it to NVM_ServiceProfile.xml.

Step 4 Run the appropriate commands for your operating system.

For Windows:

a) Open cmd in admin mode.
b) Run `reg add HKLM\System\CurrentControlSet\Services\csc_nvmagent\ /v xdr /t REG_DWORD /d 1`
c) Install the Network Visibility Module standalone .msi.

For macOS:

a) Install the Network Visibility Module standalone .dmg.
b) Run `sudo touch /opt/cisco/secureclient/NVM/lib/.features`

Step 5 Create the NVM_BootstrapProfile.xml using the template xml file provided below. Replace the <*fqdn_of_server*> value in the template with the appropriate server address for your region:

For Asia Pacific—intake.prod.apjc.tmc.nvmc.csc.cisco.com

For Europe—intake.prod.eu.tmc.nvmc.csc.cisco.com

For North America—intake.prod.nam.tmc.nvmc.csc.cisco.com

```
<?xml version="1.0" encoding="UTF-8"?>
<NVMBootstrapProfile xsi:noNamespaceSchemaLocation="NVMBootstrapProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
<Cloud>
    <CloudServer><fqdn_of_server></CloudServer>
```

```
    <CloudPort>443</CloudPort>
</Cloud>
</NVMBootstrapProfile>
```

Step 6 Copy the *NVM_BootStrapProfile.xml* and *NVM_ServiceProfile.xml* to the following locations:

For Windows—%PROGRAMDATA%\Cisco\Cisco Secure Client\NVM

For macOS—/opt/cisco/secureclient/NVM

Step 7 Restart the Network Visibility Module service.

What to do next

You must do any upgrades of profile and Network Visibility Module standalone module out-of-band. Only cloud management upgrades are handled within XDR.

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.

File	Purpose
cisco-secure-client-win-<*version*>-zta-predeploy-k9.msi	MSI installer file for Zero Trust Access
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.
cisco-secure-client-win-v*version*-edlp-predeploy-k9.msi	MSI installer file for Endpoint Data Loss Prevention.
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

Module Installed	Command and Log File
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
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
Endpoint Data Loss Prevention	msiexec /package cisco-secure-client-win-*version*-edlp-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-*version*-edlp-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.

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, ISE compliance, or Zero Trust Access 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, SBL, or Zero Trust Access 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.

Uninstalling AnyConnect VPN will uninstall all modules with the exception of Duo Desktop and ThousandEyes. You can also uninstall Zero Trust Access separately.



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.

The Zero Trust Access Module is not part of the webdeploy package for macOS.

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.

Uninstalling AnyConnect VPN will remove Zero Trust Access. Additionally, you can run this shell script with sudo to remove just Zero Trust Access: /opt/cisco/secureclient/bin/zta_uninstall.sh

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

Additional Duo Desktop Requirements on macOS 11 (and later)

The Zero Trust Access Module includes Duo Desktop installation, which has its own additional setup requirements required when deploying Zero Trust Access through MDM on macOS 11 (and later).

Refer to the Guide to Duo Device Health App certificate deployment for macOS 11+ users for these additional Duo setup requirements.

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 .tgz file.

When VPN is installed, you cannot install vpn-cli.

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.

What to do next

Uninstalling AnyConnect VPN removes Zero Trust Access.

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 updates for RPM/DEB are now supported via the downloader starting with release 5.1.15, similar to how it worked for script-based installers before 5.1.15.
- 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. If you are updating from 5.1.x to 5.1.15 (or later) via the update process, no manual uninstallation is required.
- You cannot use a script installer out-of-band to update an existing RPM or DEB installation.

Using RPM or DEB Binaries for ACTransforms.xml

Prior to release 5.1.15, webdeploy downloaded a script (cisco-secure-client***.sh) to run manually. Now with release 5.1.15, webdeploy downloads a .DEB or .RPM that is installed using the same commands as predeployment (apt install, dnf install, zypp install).

Without a standard way to customize .pkg behavior in Linux, we created ACTransforms.xml. When this .xml file is positioned with the installer, it is read before running the installation. DEB/RPM binaries support the use of an ACTransforms.xml file, which can configure Secure Client settings (such as disabling VPN or customer experience feedback).

Before you begin

sqlite and lz4 are resolved from standard system paths and are not bundled with the installer. If either of these libraries are missing, the installation fails because of DEB/RPM package dependencies and requirements.

Procedure

Step 1 For predeploy, store the ACTransforms.xml in a Profiles folder located in the same directory as the package binary. The Profiles folder may also include AnyConnectLocalPolicy.xml (overriding the version included in the package) or VPN profile XML files (copied to the vpn/profile folder during installation).

OR

For web deploy, place ACTransforms.xml in the same directory as the downloaded package. Not the Profiles folder. AnyconnectLocalPolicy.xml and VPN profiles are not copied during web deployments.

Step 2 Because the installer packages cannot automatically detect the package path, set the environment variables ABSOLUTE_INSTALLER_FILE_PATH to the absolute path of the package:

For predeploy with ACTransforms.xml in Profiles/

```
ABSOLUTE_INSTALLER_FILE_PATH=/tmp apt install ./cisco-secure-client-*.deb
```

Example:

```
ABSOLUTE_INSTALLER_FILE_PATH=/home/user/downloads apt install
/home/user/downloads/cisco-secure-client-vpn.deb
```

For web deploy with ACTransforms.xml in the same directory as the package

```
ABSOLUTE_INSTALLER_FILE_PATH=/tmp IS_WEB_DEPLOY=1 apt install /tmp/cisco-secure-client-vpn.deb
```

Example:

```
ABSOLUTE_INSTALLER_FILE_PATH=/tmp IS_WEB_DEPLOY=1 apt install /tmp/cisco-secure-client-vpn.deb
```

Step 3 In order to disable VP, go to the Cisco Secure Client x.x.x/Profiles for Predeploy packages or Cisco Secure Client x.x.x for Webdeploy packages of the Linux installer and open the ACTransforms.xml in the text editor. Set the *DisableVPN* element to **true** to ensure that VPN functionality is not installed:`<ACTransforms><DisableVPN>true</DisableVPN> </ACTransforms>`

Example

Note DART is installed only using the DEB/RPM binary packages and is enhanced to capture log files from the respective manager on system (apt, dnf, yum, or SLES SUSE Linux Enterprise Server). You cannot use the dart_install.sh or dart_uninstall.sh scripts.

Installing and Uninstalling Linux Supported Versions of Secure Client

Note Zero Trust Access and SocketFilter modules both require administrator privileges to be installed.

Ubuntu

- Install—

```
apt install ./cisco-secure-client-*.deb
```

- Uninstall—

```
apt purge cisco-secure-client-*
```

RHEL

Note Before RHEL server installation, you must run the following command to include the PackageKit:

```
sudo apt install packagekit-tools # Ubuntu/Debian
```

OR

```
sudo dnf install packageKit # RHEL/Fedora
```

- Install—

```
dnf install ./cisco-secure-client-*.rpm
```

- Uninstall—

```
dnf remove cisco-secure-client-*
```

SUSE

Note Zero Trust Access and SocketFilter modules are only supported on Ubuntu and RHEL distributions.

- Install—

```
zypper install ./cisco-secure-client-*.rpm
```

- Uninstall—

```
zypper remove cisco-secure-client-*
```

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 ISE compliance module followed by the posture module.

Step 3 Uninstall the Secure Client ZTA module.

Step 4 Uninstall the Secure Client Socket Filter module.

Step 5 Uninstall the Cisco Secure Client core VPN module.

Step 6 Uninstall DART using the following commands:

a) Ubuntu: `apt purge`
b) RHEL: `dnf remove`
c) SLES: `zypp remove`

What to do next

Determine that all module dependencies are properly installed and available. If VPN is removed using the given uninstall commands (apt, dnf, or zypp), dependencies will be automatically removed.

Predeploying Secure Client ISE Posture on Linux

The order of installation to the endpoint must be 1) cisco-secure-client-vpn, 2) cisco-secure-client-iseposture, and 3) cisco-secure-client-isecompliance.

Enter the following command to predeploy ISE Posture or ISE compliance:

- RHEL/SUSE: sudo rpm -ivh *pkg_name*
- Ubuntu: sudo dpkg -i *pkg_name*

The *pkg_name* is available in the predeploy-*rpm/deb*-k9.tar.gz bundle that you download. Examples include the following for ISE Posture and ISE Compliance:

- cisco-secure-client-iseposture-*version*-**1.x86_64.rpm** for RHEL/SUSE endpoints
- cisco-secure-client-iseposture-*version*_**amd64.deb** for Ubuntu endpoints
- [CM] cisco-secure-client-isecompliance-*version*-**1.x86_64.rpm** for RHEL/SUSE endpoints
- [CM] cisco-secure-client-isecompliance-*version*_**amd64.deb** for Ubuntu endpoints

Note Cisco Secure Client version 5.1.15 (or later) will not work with shell-script based pre-deploy compliance module version 4.3.4392.0 (or earlier).

Cisco Secure Client version 5.1.14 (or earlier) will not work with RPM/DEB based pre-deploy compliance module.

Cisco will continue to release the shell-script based pre-deploy compliance module (cisco-secure-client-linux64-*version*-isecompliance-predeploy-k9.tar.gz) on Cisco.com for Cisco Secure Client version 5.1.14 (or earlier).

Uninstalling Secure Client ISE Posture on Linux

Follow these steps to uninstall Secure Client ISE Posture from RHEL/SUSE and Ubuntu.

Before you begin

The order of uninstallation to the endpoint must be 1) cisco-secure-client-isecompliance, 2) cisco-secure-client-iseposture, and 3) cisco-secure-client-vpn.

Procedure

Step 1 Enter one of the following:

RHEL/SUSE:

```
sudo rpm -e <pkg_name>
```

Ubuntu:

```
sudo dpkg -r <pkg_name>
```

Step 2 For a list of all Secure Client packages, enter the following:

For RHEL/SUSE endpoints:

```
rpm -qa | grep cisco-secure-client
```

For Ubuntu endpoints:

```
dpkg -l | grep cisco-secure-client
```

Manually Installing DART on a Linux Device

DART can still be manually installed, but now with the DEB and RPM packages.

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.

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

- Cisco Secure Client version 5.1.15 (or later) will not work with web-deploy compliance module version 4.3.4392.0 (or earlier). There is no impact on the upgrade and downgrade of compliance module package on Cisco Secure Client version 5.1.14 (or earlier).
- 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.

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.

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, ISE Posture, ThousandEyes, and Zero Trust Access
- 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

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.

If you are using the vpn-cli package, AutoUpdate is not supported.

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.
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.

Custom Attribute *	Valid Values	Default Value	Notes
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 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.
  - 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.

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
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

Operating System	Type	File and Path
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