Deploy AnyConnect

Before You Begin Deployment

If you are deploying the Umbrella Roaming Security module, any existing installation of the Umbrella Roaming Client will be detected and removed automatically to prevent conflicts. If the existing installation of the Umbrella Roaming Client is associated with an Umbrella service subscription, it will automatically be migrated to the Umbrella Roaming Security module *unless* an OrgInfo.json file is co-located with the AnyConnect installer, configured for web deployment or predeployed in the Umbrella module's directory. You may wish to manually uninstall the Umbrella Roaming Client prior to deploying the Umbrella Roaming Security module.

You must additionally complete the following prerequisites if using the Umbrella Roaming Security module:

- **Obtain Umbrella Roaming Account.** The Umbrella dashboard http://dashboard.umbrella.com is the login page where you obtain necessary information for the operation of the AnyConnect Umbrella Roaming Security Module. You also use this site to manage reporting for the roaming client activity.
- **Download the OrgInfo File from the Dashboard.** To prepare for deploying the AnyConnect Umbrella Roaming Security Module, obtain the OrgInfo.json file from the Umbrella dashboard. Click on **Roaming Computer** in the Identities menu structure and then click the + sign in the upper-left corner of the page. Scroll down to AnyConnect Umbrella Roaming Security Module and click **Module Profile**.

  The OrgInfo.json file contains specific information about your Umbrella service subscription that lets the Roaming Security module know where to report and which policies to enforce.

AnyConnect Deployment Overview

Deploying AnyConnect refers to installing, configuring, and upgrading the AnyConnect client and its related files.

The Cisco AnyConnect Secure Mobility 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).
- Web Deploy—The AnyConnect package is loaded on the headend, which is either an ASA or FTD firewall, or an ISE server. When the user connects to a firewall or to ISE, AnyConnect is deployed to the client.
  - For new installations, the user connects to a headend to download the AnyConnect client. The client is either installed manually or automatically (web-launch).
  - Updates are done by AnyConnect running on a system where AnyConnect is already installed, or by directing the user to the ASA clientless portal.
- Cloud Update—After the Umbrella Roaming Security module is deployed, you can update any AnyConnect modules using one of the above methods, as well as Cloud Update. With Cloud Update, the software upgrades are obtained automatically from the Umbrella cloud infrastructure, and the update track is dependent upon that and not any action of the administrator. By default, automatic updates from Cloud Update are disabled.

Note Consider the following regarding Cloud Update:

- Only the software modules that are currently installed are updated.
- Customizations, localizations, and any other deployment types are not supported.
- The updates occur only when logged in to a desktop and will not happen if a VPN is established.
- With updates disabled, the latest software features and updates will not be available.
- Disabling Cloud Update has no effect on other update mechanisms or settings (such as web deploy, deferred updates, and so on).
- Cloud Update ignores having newer, unreleased versions of AnyConnect (such as interim releases and patched versions).

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

Refer to the AnyConnect release notes for system, management, and endpoint requirements for 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 AnyConnect installation directory (C:\Program Files (x86)\Cisco for Windows or /opt/cisco for macOS) is trusted and/or in the allowed/exclusion/trusted lists for endpoint antivirus, antimalware, antispyware, data loss prevention, privilege manager, or group policy objects.

Decide How to Install AnyConnect

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

Web Deploy

To upgrade AnyConnect or install additional modules using web deploy (from ASA/ISE/Umbrella cloud with Downloader), you do not need administrative privileges.

- Web Deploying from an ASA or FTD device—User connects to the AnyConnect clientless portal on the headend device, and selects to download AnyConnect. The ASA downloads the AnyConnect Downloader. The AnyConnect 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 an ASA, wireless controller, or switch. The NAD authorizes the user, and redirects the user to the ISE portal. The AnyConnect Downloader is installed on the client to manage the package extraction and installation, but does not start a VPN connection.

Predeploy

To upgrade AnyConnect or install additional modules using predeploy (out of band deployment, either manually or using SCCM and so on), you need administrative privileges.

- Using an Enterprise software management system (SMS).
- Manually distributing an AnyConnect 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.

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

Note If you are using AnyConnect Posture (HostScan) to perform root privilege activities on a macOS or Linux platform, we recommend that you predeploy AnyConnect Posture.

Determine The Resources You Need to Install AnyConnect

Several types of files make up an AnyConnect deployment:

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

Preparing the Endpoint for AnyConnect

Using Mobile Broadband Cards with AnyConnect

Some 3G cards require configuration steps before using AnyConnect. 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 AnyConnect installation. When an AnyConnect interface is detected, the 3G manager drops the interface and allows the AnyConnect connection.

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

Add the ASA to the List of Internet Explorer Trusted Sites on Windows

An Active Directory administrator can use a group policy to add the ASA to the list of trusted sites in Internet Explorer. This procedure is different from the way a local user adds trusted sites in Internet Explorer.

Procedure

Step 1 On the Windows Domain server, log in as a member of the Domain Administrators group.

Step 2 Open the Active Directory Users and Computers MMC snap-in.

Step 3 Right-click the Domain or Organizational Unit where you want to create the Group Policy Object and click **Properties**.

Step 4 Select the **Group Policy** tab and click **New**.

Step 5 Type a name for the new Group Policy Object and press **Enter**.

Step 6 To prevent this new policy from being applied to some users or groups, click **Properties**. Select the **Security** tab. Add the user or group that you want to *prevent* from having this policy, and then clear the **Read** and the **Apply Group Policy** check boxes in the Allow column. Click **OK**.

Step 7 Click **Edit** and choose **User Configuration** > **Windows Settings** > **Internet Explorer Maintenance** > **Security**.

Step 8 Right-click **Security Zones and Content Ratings** in the right pane, and then click **Properties**.

Step 9 Select **Import the current security zones and privacy settings**. If prompted, click **Continue**.

Step 10 Click **Modify Settings**, select **Trusted Sites**, and click **Sites**.

Step 11 Type the URL for the Security Appliance that you want to add to the list of trusted sites and click **Add**. The format can contain a hostname (https://vpn.mycompany.com) or IP address (https://192.168.1.100). It can be an exact match (https://vpn.mycompany.com) or a wildcard (https://*.mycompany.com).

Step 12 Click **Close** and click **OK** continually until all dialog boxes close.

Step 13 Allow sufficient time for the policy to propagate throughout the domain or forest.

Step 14 Click **OK** in the Internet Options window.

Block Proxy Changes in Internet Explorer

Under certain conditions, AnyConnect 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 ASA configuration specifies Connections tab lockdown
- The ASA configuration specifies a private-side proxy
- A Windows group policy previously locked down the Connections tab (overriding the no lockdown ASA group policy setting)

For Windows 10 version 1703 (or later), in addition to hiding the Connections Tab in Internet Explorer, AnyConnect 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 AnyConnect session.
- **No** to disable proxy lockdown and expose the Internet Explorer Connections tab during the AnyConnect session.

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

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

Configure How AnyConnect Treats Windows RDP Sessions

You can configure AnyConnect 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 AnyConnect Secure Mobility 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)—Allows only one local user to be logged on during the entire VPN connection. Also, a local user can establish a VPN connection while one or more remote users are logged on to the client PC. This setting has no effect on remote user logons from the enterprise network over the VPN connection.

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

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

Note Multiple simultaneous logons are not supported.

Windows VPN Establishment—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.

See AnyConnect VPN Connectivity Options for additional VPN session connectivity options.

Configure How AnyConnect Treats Linux SSH Sessions

You can configure AnyConect 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 AnyConnect Secure Mobility 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 remotely logged-on user from establishing a VPN connection.
- Allow Remote Users—Allows remote users to establish a VPN connection.

See AnyConnect VPN Connectivity Options for additional VPN session connectivity options.

DES-Only SSL Encryption on Windows

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

Using NVM on Linux

Before using NVM on Linux, you must set up a kernel driver framework (KDF). You can choose to prebuild an AnyConnect 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 AnyConnect Kernel Module

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.
- 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 AnyConnect Linux Kernel Module

Before you begin

Complete the prerequisites in Prerequisites to Build the AnyConnect Kernel Module, on page 7.

Note NVM is not supported on devices with secure boot enabled.

The AnyConnect NVM can be packaged with a pre-built AnyConnect 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 AnyConnect Linux Kernel Module.

Procedure

Step 1 Extract the AnyConnect predeploy package: anyconnect-linux64-<*version*>-predeploy-k9.tar.gz.

Step 2 Navigate to the nvm directory.

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

After running the script, anyconnect-linux64-<*version*>**-ac_kdf_ko-k9.tar.gz** gets created, which includes the AnyConnect 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.

What to do next

When the target device's OS kernel is upgraded, you must re-deploy the AnyConnect NVM with the updated Linux Kernel Module.

Predeploying AnyConnect

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

When you create a file archive to install AnyConnect, 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 AnyConnect Profiles, on page 10

Before you begin

- If you manually deploy the VPN profile, you must also upload the profile to the headends. When the client system connects, AnyConnect 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 AnyConnect ISE Posture profile, you must also upload that file to ISE.

Procedure

Step 1 Download the AnyConnect Predeployment Package.

The AnyConnect files for predeployment are available on cisco.com.

OS	AnyConnect Predeploy Package Name
Windows	anyconnect-win-*version*-predeploy-k9.zip
macOS	anyconnect-macos-*version*-predeploy-k9.dmg
Linux (64-bit)	anyconnect-linux64-*version*-predeploy-k9.tar.gz

The Umbrella Roaming Security 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 a client profile:

- AnyConnect VPN
- AnyConnect Network Access Manager
- AnyConnect ISE Posture
- AnyConnect AMP Enabler
- Network Visibility Module
- Umbrella Roaming Security Module

The following modules do not require an AnyConnect client profile:

- AnyConnect VPN Start Before Logon
- AnyConnect Diagnostic and Reporting Tool
- AnyConnect Posture
- AnyConnect Customer Experience Feedback

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

Step 3 Optionally, Customize and Localize the AnyConnect Client and Installer.

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

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

AnyConnect Module Executables for Predeploy and Web Deploy

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

Table 1: Module Filenames for Web Deployment or Predeployment

Module	Web-Deploy Installer (Downloaded)	Predeploy Installer
Network Access Manager	anyconnect-win-*version*-nam-webdeploy-k9.msi	anyconnect-win-*version*-nam-predeploy-k9.msi
ISE Posture	anyconnect-win-*version*-iseposture-webdeploy-k9.msi	anyconnect-win-*version*-iseposture-predeploy-k9.msi
AMP Enabler	anyconnect-win-*version*-amp-webdeploy-k9.msi	anyconnect-win-*version*-amp-predeploy-k9.exe
Network Visibility Module	anyconnect-win-*version*-nvm-webdeploy-k9.exe	anyconnect-win-*version*-nvm-predeploy-k9.msi
Umbrella Roaming Security Module	anyconnect-win-*version*-umbrella-webdeploy-k9.exe	anyconnect-win-*version*-umbrella-predeploy-k9.msi

AnyConnect 4.3 (and later) has moved to the Visual Studio 2015 build environment and requires VS redistributable files for its Network Access Manager Module functionality. These files are installed as part of the install package. You can use the .msi files to upgrade the Network Access Manager Module to 4.3 (or later), but the AnyConnect Secure Mobility Client must be upgraded first and running release 4.3 (or later).

Note If you have a Windows server OS, you may experience installation errors when attempting to install AnyConnect 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 AnyConnect Profiles

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

Table 2: AnyConnect Core Files

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

Table 3: Profile Locations for all Operating Systems

Operating System	Module	Location
Windows	Core client with VPN	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
	Network Access Manager	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Network Access Manager\newConfigFiles
	Customer Experience Feedback	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\CustomerExperienceFeedback
	OPSWAT	%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\opswat
	ISE Posture	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture
	AMP Enabler	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\AMP Enabler
	Network Visibility Module	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM
	Umbrella Roaming Security Module	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility 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.

Operating System	Module	Location
macOS	All other modules	/opt/cisco/anyconnect/profile
	Customer Experience Feedback	/opt/cisco/anyconnect/CustomerExperienceFeedback
	Binaries	/opt/cisco/anyconnect/bin
	OPSWAT	/opt/cisco/anyconnect/lib/opswat
	Libraries	/opt/cisco/anyconnect/lib
	UI Resources	/Applications/Cisco/Cisco AnyConnect Secure Mobility Client.app/Contents/Resources/
	ISE Posture	/opt/cisco/anyconnect/iseposture/
	AMP Enabler	/opt/cisco/anyconnect/ampenabler/
	Network Visibility Module	/opt/cisco/anyconnect/NVM/
	Umbrella Roaming Security Module	/opt/cisco/anyconnect/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.
Linux	NVM	/opt/cisco/anyconnect/NVM
	All other modules	/opt/cisco/anyconnect/profile

Predeploying AnyConnect Modules as Standalone Applications

The Network Access Manager, Web Security, and Umbrella Roaming Security modules can run as standalone applications. The AnyConnect core client is installed, but the VPN and AnyConnect UI are not used.

Deploying Stand-Alone 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 anyconnect-win-version-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 anyconnect-win-version-umbrella-predeploy-k9.msi /norestart /passive /lvx*
c:\test.log
```

Step 3 (Optional) Install DART.

misexec /package annyconnect-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 AnyConnect service.

Deploying AnyConnect Modules as Standalone Applications

You can deploy the AnyConnect Network Access Manager or Umbrella Roaming Security Modules as standalone applications on a user computer. DART is supported with these applications.

Requirements

The VPNDisable_ServiceProfile.xml file must also be the only AnyConnect profile in the VPN client profile directory.

User Installation of Stand-Alone 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 stand-alone 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 AnyConnect Network Access Manager or Umbrella Roaming Security 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 or Umbrella Roaming Security Module as stand-alone 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 AnyConnect 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 stand-alone Network Access Manager or the Umbrella Roaming Security Module.
b) When the user clicks OK, the Install Utility invokes the AnyConnect core 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 or Umbrella Roaming Security installer.
e) The Network Access Manager or Umbrella Roaming Security Module is enabled without VPN service on the computer.

Predeploying to Windows

Distributing AnyConnect 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 AnyConnect 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 AnyConnect 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.

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 AnyConnect zip File

File	Purpose
GUI.ico	AnyConnect icon image.
Setup.exe	Launches the Install Utility.
anyconnect-win-*version*-dart-predeploy-k9.msi	MSI installer file for the DART module.
anyconnect-win-*version*-gina-predeploy-k9.msi	MSI installer file for the SBL module.
anyconnect-win-*version*-iseposture-predeploy-k9.msi	MSI installer for the ISE Posture module.
anyconnect-win-*version*-amp-predeploy-k9.exe	MSI installer file for the AMP Enabler.
anyconnect-win-*version*-nvm-predeploy-k9.msi	MSI installer file for the Network Visibility Module.
anyconnect-win-*version*-umbrella-predeploy-k9.msi	MSI installer file for the Umbrella Roaming Security Module.
anyconnect-win-*version*-nam-predeploy-k9.msi	MSI installer file for the Network Access Manager module.

File	Purpose
anyconnect-win-*version*-posture-predeploy-k9.msi	MSI installer file for the posture module.
anyconnect-win-*version*-core-vpn-predeploy-k9.msi	MSI installer file for the AnyConnect core client.
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 AnyConnect 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 AnyConnect onto Windows, you must disable either the AlwaysInstallElevated or the Windows User Account Control (UAC) group policy setting. If you do not, the AnyConnect 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 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.

Windows Predeployment MSI Examples

Module Installed	Command and Log File
AnyConnect core client No VPN capability. Use when installing stand-alone Network Access Manager modules.	msiexec /package anyconnect-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* anyconnect-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
AnyConnect core client with VPN capability.	msiexec /package anyconnect-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log

Module Installed	Command and Log File
Customer Experience Feedback	msiexec /package anyconnect-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* anyconnect-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
Diagnostic and Reporting Tool (DART)	msiexec /package anyconnect-win-*version*-dart-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-dart-predeploy-k9-install-datetimestamp.log
SBL	msiexec /package anyconnect-win-*version*-gina-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-gina-predeploy-k9-install-datetimestamp.log
Network Access Manager	msiexec /package anyconnect-win-*version*-nam-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-nam-predeploy-k9-install-datetimestamp.log
VPN Posture (HostScan)	msiexec /package anyconnect-win-*version*-posture-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-posture-predeploy-k9-install-datetimestamp.log
ISE Posture	msiexec /package anyconnect-win-*version*-iseposture-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-iseposture-predeploy-k9-install-datetimestamp.log
AMP Enabler	msiexec /package anyconnect-win-*version*-amp-predeploy-k9.msi / norestart/passive /lvx* anyconnect-win-*version*-amp-predeploy-k9-install-datetimestamp.log
Network Visibility Module	msiexec /package anyconnect-win-*version*-nvm-predeploy-k9.msi / norestart/passive /lvx* anyconnect-win-*version*-nvm-predeploy-k9-install-datetimestamp.log
Umbrella Roaming Security	msiexec /package anyconnect-win-*version*-umbrella-predeploy-k9.msi / norestart/passive /lvx* anyconnect-*version*-umbrella-predeploy-k9-install-datetimestamp.log

AnyConnect Sample Windows Transform

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

Windows Predeployment Security Options

Cisco recommends that end users are given limited rights on the device that hosts the Cisco AnyConnect Secure Mobility Client. If an end user warrants additional rights, installers can provide a lockdown capability that prevents users and local administrators from switching off or stopping those Windows services established as locked down on the endpoint. You can also prevent users from uninstalling AnyConnect.

Windows Lockdown Property

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

Hide AnyConnect from Add/Remove Programs List

You can hide the installed AnyConnect modules from users that view the Windows Add/Remove Programs list. If you launch any installer using ARPSYSTEMCOMPONENT=1, that module will not appear in the Windows Add/Remove Programs list.

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

AnyConnect 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.

Procedure

Step 1 Install the AnyConnect modules in the following order:

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

During this installation, a restricted user account (ciscoacvpnuser) is created for the management tunnel feature. This account is used by AnyConnect to enforce the principle of least privilege when initiating a management tunnel connection. This account does get removed during AnyConnect uninstallation.

b) Install the AnyConnect Diagnostic and Reporting Tool (DART) module, which provides useful diagnostic information about the AnyConnect core client installation.

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

Step 2 Uninstall the AnyConnect modules in the following order:

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

b) Uninstall the AnyConnect core client.

c) Uninstall DART last.

DART information is valuable should the uninstall processes fail.

Note By design, some XML files remain after uninstalling AnyConnect.

Predeploying to macOS

Install and Uninstall AnyConnect on macOS

AnyConnect for macOS is distributed in a DMG file, which includes all the AnyConnect modules. When users open the DMG file, and then run the AnyConnect.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.

To remove any of the AnyConnect modules from your distribution, use the Apple pkgutil tool, and sign the package after modifying it.staller with ACTransforms.xml. You can customize the language and appearance a You can also modify the innd change some other install actions, which is described in the Customization chapter: Customize Installer Behavior on macOS with ACTransforms.xml.

Installing AnyConnect Modules on macOS as a Standalone Application

You can install just the Network Visibility Module or Umbrella Roaming Security Module without the VPN. The VPN and AnyConnect UI are not used.

The following procedure explains how to customize the modules by installing the standalone Profile Editor, creating a profile, and adding that profile to the DMG package. It also sets the AnyConnect user interface to start automatically on boot-up, which enables AnyConnect to provide the necessary user and group information for the module.

Procedure

Step 1 Download the Cisco AnyConnect Secure Mobility Client DMG package from Cisco.com.

Step 2 Open the file to access the installer. Note that the downloaded image is a read-only file.

Step 3 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 4 Install the stand-alone Profile Editor on a computer running a Windows operating system. You must select the AnyConnect modules you want as part of a Custom installation or a Complete installation. They are not installed by default.

Step 5 Start the profile editor and create a profile.

Step 6 Save the profile appropriately as `OrgInfo.json` (that you get from the dashboard) in a secure location.

a) Copy the specified .wso file from the Windows device to the macOS installer package in the appropriate folder path, such as `AnyConnect x.x.x/Profiles/NVM`. Or, use the Terminal application, as shown below for NVM instance:

```
cp <path to the wso> \Volumes\"AnyConnect <VERSION>"\Profiles\nvm\
```

b) In the macOS installer, go to the `AnyConnect 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 AnyConnect 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 AnyConnect is signed application using an Apple certificate. If Gatekeeper is configured for Mac App Store (only), then you must either select the Anywhere setting or control-click to bypass the selected setting to install and run AnyConnect from a predeployed installation. For more information see: http://www.apple.com/macosx/mountain-lion/security.html.

Predeploying to Linux

Installing Modules for Linux

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

Procedure

Step 1 Install the AnyConnect core client module, which installs the GUI and VPN capability (both SSL and IPsec).

Step 2 Install the DART module, which provides useful diagnostic information about the AnyConnect core client installation.

Step 3 Install the posture module or ISE compliance module.

Step 4 Install the NVM.

Uninstalling Modules for Linux

The order that the user uninstalls AnyConnect is important.

DART information is valuable if the uninstall processes fails.

Procedure

Step 1 Uninstall the NVM.
Step 2 Uninstall the posture module or ISE compliance module.
Step 3 Uninstall the AnyConnect core client.
Step 4 Uninstall DART.

Manually Installing/Uninstalling NVM on a Linux Device

Procedure

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

You can uninstall NVM using /opt/cisco/anyconnect/bin/nvm_uninstall.sh.

Certificate Store for Server Certificate Verification

If you will be using server certificates with AnyConnect, you must make a certificate store available for AnyConnect to access and verify certificates as trusted. By default, AnyConnect uses the Firefox certificate store.

To Activate a Firefox Certificate Store

After you have AnyConnect installed on a Linux device, and before you attempt an AnyConnect connection for the first time, open up a Firefox browser. When you open Firefox, a profile is created, which includes a certficate store.

If You Do Not Use the Firefox Certificate Store

If you opt not to use Firefox, you must configure the local policy to exclude the Firefox certificate store, and must configure the PEM store.

Multiple Module Requirement

If you deploy the core client plus one or more optional modules, you must apply the lockdown property to each of the installers. Lockdown is described in the Windows Predeployment MSI Examples, on page 15.

This action is available for the VPN installer, Network Access Manager, Network Visibility Module, and Umbrella Roaming Security Module.

Note If you choose to activate lockdown to the VPN installer, you will consequently be locking down AMP Enabler as well.

Manually Installing DART on a Linux Device

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

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

Web Deploying AnyConnect

Web deployment refers to the AnyConnect Downloader on the client system getting AnyConnect software from a headend, or to using the portal on the headend to install or update AnyConnect. 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.

Web Deployment with the ASA

The Clientless Portal on the ASA web deploys AnyConnect. The process flow is:

Users open a browser and connect to the ASA's clientless portal. On the portal, the users click the **Start AnyConnect Client** button. They can then download the AnyConnect package manually. If they are running a browser that supports NPAPI (Netscape Plugin Application Programming Interface) plugins, they can also use the tab to launch the automatic web provisioning using weblaunch (ActiveX or Java).

ASA Web-Deployment Restrictions

- Loading multiple AnyConnect packages for the same O/S to the ASA is not supported.
- The OPSWAT definitions are not included in the VPN posture (HostScan) module when web deploying. You must either manually deploy the HostScan module or load it on the ASA in order to deliver the OPSWAT definitions to the client.
- If your ASA has only the default internal flash memory size, you could have problems storing and loading multiple AnyConnect client packages on the ASA. Even if you have enough space on flash to hold the package files, the ASA could run out of cache memory when it unzips and loads the client images. For more information about the ASA memory requirements when deploying AnyConnect, and possibly upgrading the ASA memory, see the latest release notes for your VPN Appliance.

- Users can connect to the ASA using the IP address or DNS, but the link-local secure gateway address is not supported.
- You must add the URL of the security appliance supporting web launch to the list of trusted sites in Internet Explorer. This can be done with a group policy, as described in Add the ASA to the List of Internet Explorer Trusted Sites on Windows.
- For Windows 7 SP1 users, we recommend that you install Microsoft .NET framework 4.0 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 Roaming Security module is not activated, and a message is displayed. To go and then install the .NET Framework, you must reboot to activate the Umbrella Roaming Security module.

Web Deployment with ISE

Policies on ISE determine when the AnyConnect client will be deployed. The user opens a browser and connects to a resource controlled by ISE and is redirected to the AnyConnect Client Portal. That ISE Portal helps the user download and install AnyConnect. In Internet Explorer, ActiveX controls guide the installation. For other browsers, the Portal downloads the Network Setup Assistant, and that tools helps the user install AnyConnect.

ISE Deployment Restrictions

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

Configuring Web Deployment on the ASA

Browser Restrictions for WebLaunch

Table 4: AnyConnect Browser Support for Weblaunch by Operating System

Operating System	Browser
Current Microsoft supported versions of Windows 10 x86 (32-bit) and x64 (64-bit)	Internet Explorer 11
Windows 8.x x86 (32-bit) and x64 (64-bit)	Internet Explorer 11
Windows 7 SP1 x86 (32-bit) and x64 (64-bit)	Internet Explorer 11
macOS 10.12, 10.13, and 10.14 (64-bit)	Safari 11

Note Because the EDGE browser does not support ActiveX, our provisioning page hides the Automatic Provisioning options.

Note Web launch works on all browsers that support NPAPI (Netscape Plugin Application Programming Interface) plugins.

Also, with the addition of the AnyConnect Umbrella Roaming Security Module, Microsoft .NET 4.0 is required.

Download the AnyConnect Package

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

OS	AnyConnect Web-Deploy Package Names
Windows	anyconnect-win-*version*-webdeploy-k9.pkg
macOS	anyconnect-macos-*version*-webdeploy-k9.pkg
Linux (64-bit)	anyconnect-linux64-*version*-webdeploy-k9.pkg

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

Load the AnyConnect Package on the ASA

Procedure

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

Step 2 To add an AnyConnect image, click **Add**.

- Click **Browse Flash** to select an AnyConnect image you have already uploaded to the ASA.
- Click **Upload** to browse to an AnyConnect image you have stored locally on your computer.

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

Step 4 Click **Apply**.

Enable Additional AnyConnect 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, AnyConnect must download those modules to the VPN endpoints.

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

Procedure

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

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

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

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

Create a Client Profile in ASDM

You must add an AnyConnect web-deployment package to the ASA before you can create a client profile on the 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 AnyConnect 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 AnyConnect core, ISE Posture module and OPSWAT (compliance module) to support posture for ISE. ISE can also deploy all the AnyConnect modules and resources that can be used when connecting to an ASA. When a user browses to a resource controlled by ISE:

- If ISE is behind an ASA, the user connects the ASA, downloads AnyConnect, and makes a VPN connection. If AnyConnect ISE Posture was not installed by the ASA, then the user is redirected to the AnyConnect Client Portal to install the ISE Posture.
- If ISE is not behind an ASA, the user connects to the AnyConnect Client Portal, which guides him to install the AnyConnect resources defined in the AnyConnect configuration on ISE. A common configuration is to redirect the browser to AnyConnect client provisioning portal if the ISE Posture status is unknown.

- When the user is directed to the AnyConnect Client Provisioning Portal in ISE:
  - If the browser is Internet Explorer, ISE downloads AnyConnect Downloader, and the Downloader loads AnyConnect.
  - 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 AnyConnect 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 AnyConnect Configuration profiles in ISE
- Add AnyConnect Resources to ISE from a local device
- Add AnyConnect Provisioning Resources from a Remote Site
- Deploy the AnyConnect client and resources

Note Because AnyConnect 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 AnyConnect resources:

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

Prepare AnyConnect Files for ISE Upload

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

Note With ASA, installation happens with the VPN downloader. With the download, the ISE posture profile is pushed via 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, 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 an AnyConnect 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:
  - AnyConnect UI resources
  - VPN Connection Scripts
  - Help file(s)
  - Installer Transforms

  An AnyConnect localization bundle can contain:
  - AnyConnect gettext translations, in binary format
  - Installer transforms

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

Configure ISE to Deploy AnyConnect

You must upload the AnyConnect package to ISE before you upload and create additional AnyConnect resources.

Note When configuring the AnyConnect Configuration object in ISE, unchecking the VPN module under AnyConnect 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 AnyConnect package file. Repeat adding agent resources from local disk for any other AnyConnect resources that you plan to deploy.

3. Select **Add** > **AnyConnect Configuration** > **.** This AnyConnect Configuration configures modules, profiles, customization/language packages, and the OPSWAT package, as described in the following table.

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

   Table 5: AnyConnect Resources in ISE

Prompt	ISE Resource Type and Description
AnyConnect Package	AnyConnectDesktopWindows AnyConnectDesktopOSX AnyConnectWebAgentWindows AnyConnectWebAgentOSX
Compliance Module	AnyConnectComplianceModuleWindows AnyConnectComplianceModuleOSX
AnyConnect Profiles	AnyConnectProfile ISE displays a checkbox for each profile provided by the uploaded AnyConnect package.
Customization Bundle	AnyConnectCustomizationBundle
Localization Bundle	AnyConnectLocalizationBundle

4. Create a Role or OS-based client provisioning policy. AnyConnect 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 AnyConnect agent or the legacy NAC/MAC agent. When configuring the AnyConnect agent, select one AnyConnect Configuration created in step 2.

Configuring Web Deployment on FTD

A Firepower Threat Defense (FTD) device is a Next Generation Firewall (NGFW) that provides secure gateway capabilities similar to the ASA. FTD devices support Remote Access VPN (RA VPN) using the AnyConnect Secure Mobility 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 an FTD device.

Windows, macOS, and Linux AnyConnect clients are configured on the FTD 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 FTD 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 AnyConnect client. The FTD headend downloads and installs the client that matches the operating system of the remote computer, and establishes a secure connection.

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

Currently, only the core AnyConnect VPN module and the AnyConnect VPN Profile can be configured on the FTD and distributed to endpoints. A Remote Access VPN Policy wizard in the Firepower Management Center (FMC) quickly and easily sets up these basic VPN capabilities.

Guidelines and Limitations for AnyConnect and FTD

- The only supported VPN client is the Cisco AnyConnect Secure Mobility 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 AnyConnect Client.
- Using AnyConnect with FTD requires version 4.0 or later of AnyConnect, and version 6.2.1 or later of the FMC.
- There is no inherent support for the AnyConnect Profile Editor in the FMC; you must configure the VPN profiles independently. The VPN Profile and AnyConnect VPN package are added as File Objects in the FMC, which become part of the RA VPN configuration.
- Secure Mobility, Network Access Management, and all the other AnyConnect modules and their profiles beyond the core VPN capabilities are not currently supported.
- VPN Load balancing is not supported.
- Browser Proxy is not supported.
- All posture variants (HostScan, Endpoint Posture Assessment, and ISE) and Dynamic Access Policies based on the client posture are not supported.
- The Firepower Threat Defense device does not configure or deploy the files necessary to customize or localize AnyConnect.
- Features requiring Custom Attributes on the AnyConnect Client are not supported on FTD such as: Deferred Upgrade on desktop clients and Per-App VPN on mobile clients.
- Authentication cannot be done on the FTD headend locally; therefore, configured users are not available for remote connections, and the FTD 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 AnyConnect on an FTD, 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 AnyConnect Software and Profiles

AnyConnect can be updated in several ways.

- AnyConnect Client—When AnyConnect connects to the ASA, the AnyConnect Downloader checks to see if any new software or profiles have been loaded on the ASA. It downloads those updates to the client, and the VPN tunnel is established.
- Cloud Update—The Umbrella Roaming Security Module can provide automatic updates for all installed AnyConnect modules from the Umbrella Cloud infrastructure. With Cloud Update, the software upgrades are obtained automatically from the Umbrella Cloud infrastructure, and the update track is dependent upon that and not any action of the administrator. By default, automatic updates from Cloud Update are disabled.
- ASA or FTD Portal—You instruct your users to connect to the ASA's Clientless Portal to get updates. FTD downloads the core VPN module only.
- ISE—When a user connects to ISE, ISE uses its AnyConnect 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 AnyConnect downloader is installed on the client to manage the package extraction and installation. We recommend that you upload the deploy package to the ASA headend and make sure that the versions of AnyConnect client match the 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 AnyConnect 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 AnyConnect update out of band
  - Configure the same version of AnyConnect on the 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 AnyConnect Client Provisioning portal on ISE, and that DACL has been pushed to the ASA.
- ISE is behind the ASA.

AnyConnect is Installed on the Client

1. User starts AnyConnect, provides credentials, and clicks Connect.
2. ASA opens SSL connection with client, passes authentication credentials to ISE, and ISE verifies the credentials.

3. AnyConnect launches the AnyConnect Downloader, which performs any upgrades, and initiates a VPN tunnel.

If ISE Posture was not installed by the ASA, then

1. A user browses to any site and is redirected to AnyConnect client provisioning portal on ISE by the DACL.
2. If the browser is Internet Explorer, ActiveX control launches AnyConnect Downloader. On other browsers, the user downloads and executes Network Setup Assistant (NSA), which downloads and starts the AnyConnect Downloader.
3. The AnyConnect Downloader performs any AnyConnect upgrades configured on ISE, which now includes the AnyConnect ISE Posture module.
4. The ISE Posture agent on the client starts posture.

AnyConnect is Not Installed

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

If ISE Posture was not installed by the ASA, then

1. User browses to a site again and is redirected to AnyConnect client provisioning portal on ISE.
2. On Internet Explorer, an ActiveX control launches AnyConnect Downloader. On other browsers, the user downloads and executes Network Setup Assistant, which downloads and launches the AnyConnect Downloader.
3. The AnyConnect Downloader performs any upgrades configured on ISE through the existing VPN tunnel, which includes adding the AnyConnect ISE Posture module.
4. ISE Posture agent starts posture assessment.

Disabling AnyConnect Auto Update

It is possible to disable or limit AnyConnect 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 AnyConnect 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 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 AnyConnect During WebLaunch

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

Prompting users to download AnyConnect 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 an AnyConnect update by disabling AutoUpdate, as described in Disabling AnyConnect Auto Update. AutoUpdate is on by default.

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

Configure Deferred Update on an ASA

On an 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 ASA configuration is dependent on the ASA/ASDM release you are running. See the *Cisco ASA Series VPN ASDM Configuration Guide* or the *Cisco ASA Series VPN CLI Configuration Guide* that corresponds to your ASA/ASDM deployed release for custom attribute configuration procedures.

The following attributes and values configure Deferred Update in ASDM:

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

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

* The custom attribute values are case-sensitive.

Configure Deferred Update in ISE

Procedure

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

Step 2 Upload any other AnyConnect resources you have created.

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

Deferred Update GUI

The following figure shows the UI that the user sees when an update is available, and Deferred Update is configured. The right part of the figure shows the UI when **DeferredUpdateDismissTimeout** is configured.

Set the Update Policy

Update Policy Overview

AnyConnect software and profile updates occur when they are available and allowed by the client upon connecting to a headend. Configuring the headend for AnyConnect 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 AnyConnect software and profiles by specifying them in the **Server Name** list.

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

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

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

- Allow or disallow ISE Posture Profile updates using the **Allow ISE Posture Profile Updates From Any Server** option.
- Allow or disallow Compliance Module updates using the **Allow Compliance Module Updates From Any Server** option.

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

Authorized Server Update Policy Behavior

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

- The version of the AnyConnect 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 AnyConnect package is older than the version on the client, no software updates occur.
  - If the version of the AnyConnect 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 AnyConnect 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 AnyConnect is updated as follows:

- **Allow Software Updates From Any Server:**
  - If this option is checked, software updates are allowed for this unauthorized 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 theVPN profile update, based on differentiation, should have occurred.

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

Update Policy Guidelines

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

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

- In Windows, the downloader creates a separate text log (UpdateHistory.log) that records the download history. This log includes the time of the updates, the 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 AnyConnect Secure Mobility Client\Logs` directory.

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

Update Policy Example

This example shows the client update behavior when the AnyConnect version on the client differs from various 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>
<AllowVPNProfileUpdatesFromAnyServer>false</AllowVPNProfileUpdatesFromAnyServer>
<AllowServiceProfileUpdatesFromAnyServer>false</AllowServiceProfileUpdatesFromAnyServer>
<AllowISEProfileUpdatesFromAnyServer>true</AllowISEProfileUpdatesFromAnyServer>
<AllowComplianceModuleUpdatesFromAnyServer>true</AllowComplianceModuleUpdatesFromAnyServer>
<AllowManagementVPNProfileUpdatesFromAnyServer>true</AllowManagementVPNProfileUpdatesFromAnyServer>
<AuthorizedServerList>
    <ServerName>seattle.example.com</ServerName>
    <ServerName>newyork.example.com</ServerName>
</AuthorizedServerList>
</UpdatePolicy>
</AnyConnectLocalPolicy>
```

With the following 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 AnyConnect VPN and Network Access Manager modules:

- The client connects to seattle.example.com, an authorized server configured with the same version of AnyConnect. 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 ASA configured with a newer version of AnyConnect. 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 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.

AnyConnect Reference Information

Locations of User Preferences Files on the Local Computer

AnyConnect stores some profile settings on the user computer in a user preferences file and a global preferences file. AnyConnect 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.

AnyConnect uses the global file for actions that occur before logon, for example, Start Before Logon and AutoConnect On Start.

The following table shows the filenames and installed paths for preferences files on the client computer:

Operating System	Type	File and Path
Windows	User	C:\Users\username\AppData\Local\Cisco\ Cisco AnyConnect VPN Client\preferences.xml
	Global	C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\ preferences_global.xml
macOS	User	/Users/username/.anyconnect
	Global	/opt/cisco/anyconnect/.anyconnect_global
Linux	User	/home/username/.anyconnect
	Global	/opt/cisco/anyconnect/.anyconnect_global

Port Used by AnyConnect

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

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