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.

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.

Decide How to Install AnyConnect

AnyConnect can be web deployed by ISE 2.0 (or later) and ASA headends or predeployed.
Web Deploy

- 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

- Using an Enterprise software management system (SMS), for example, Windows transforms.
- Manually distributing an AnyConnect file archive, with instructions for the user about how to install. File archive formats are ISO 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 Mac 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)

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 options are configured in the VPN client profile.
### Windows Logon Enforcement

<table>
<thead>
<tr>
<th>Preference Name</th>
<th>Values</th>
<th>Available in SBL Mode?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Preference Name</th>
<th>Values</th>
<th>Available in SBL Mode?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
</tbody>
</table>

• Allow Remote Users—Allows remote users to establish a VPN connection. However, if the configured VPN connection routing causes the remote user to become disconnected, the VPN connection terminates to allow the remote user to regain access to the client PC. Remote users must wait 90 seconds after VPN establishment if they want to disconnect their remote login session without causing the VPN connection to be terminated.

**Note**
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.

**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 7

**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.

<table>
<thead>
<tr>
<th>OS</th>
<th>AnyConnect Predeploy Package Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>anyconnect-win-version-pre-deploy-k9.iso</td>
</tr>
<tr>
<td>macOS</td>
<td>anyconnect-macosx-i386-version-k9.dmg</td>
</tr>
<tr>
<td>Linux (64-bit)</td>
<td>anyconnect-predeploy-linux-64-version-k9.tar.gz</td>
</tr>
</tbody>
</table>

*Note*  
Network Visibility 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 Web Security
• AnyConnect ISE Posture

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. See About the Profile Editor for more information about the Windows stand-alone editor.

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 Network Access Manager, ISE Posture, and Web Security clients to a Windows computer:

<table>
<thead>
<tr>
<th>Module</th>
<th>Web-Deploy Installer (Downloaded)</th>
<th>Predeploy Installer</th>
</tr>
</thead>
</table>

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>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>anyfilename.xml</code></td>
<td>AnyConnect profile. This file specifies the features and attribute values configured for a particular user type.</td>
</tr>
<tr>
<td><code>AnyConnectProfile.xsd</code></td>
<td>Defines the XML schema format. AnyConnect uses this file to validate the profile.</td>
</tr>
</tbody>
</table>
### Table 3: Profile Locations for all Operating Systems

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Module</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7 and 8.x</td>
<td>Core client with VPN</td>
<td>%ProgramData%\Cisco\Cisco AnyConnect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secure Mobility Client\Profile</td>
</tr>
<tr>
<td></td>
<td>Network Access Manager</td>
<td>%ProgramData%\Cisco\Cisco AnyConnect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secure Mobility Client\Network Access Manager</td>
</tr>
<tr>
<td></td>
<td>Web Security</td>
<td>%ProgramData%\Cisco\Cisco AnyConnect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secure Mobility Client\Web Security</td>
</tr>
<tr>
<td></td>
<td>Customer Experience</td>
<td>%ProgramData%\Cisco\Cisco AnyConnect</td>
</tr>
<tr>
<td></td>
<td>Feedback</td>
<td>Secure Mobility Client\CustomerExperienceFeedback</td>
</tr>
<tr>
<td></td>
<td>OPSWAT</td>
<td>%PROGRAMFILES%\Cisco\Cisco AnyConnect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secure Mobility Client\opswat</td>
</tr>
<tr>
<td></td>
<td>ISE Posture</td>
<td>%ProgramData%\Cisco\Cisco AnyConnect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secure Mobility Client\ISE Posture</td>
</tr>
<tr>
<td>macOS</td>
<td>All other modules</td>
<td>/opt/cisco/anyconnect/profile</td>
</tr>
<tr>
<td></td>
<td>Customer Experience</td>
<td>/opt/cisco/anyconnect/CustomerExperienceFeedback</td>
</tr>
<tr>
<td></td>
<td>Feedback</td>
<td></td>
</tr>
<tr>
<td>Binaries</td>
<td></td>
<td>/opt/cisco/anyconnect/bin</td>
</tr>
<tr>
<td>OPSWAT</td>
<td></td>
<td>/opt/cisco/anyconnect/opswat</td>
</tr>
</tbody>
</table>
Predeploying AnyConnect Modules as Stand-Alone Applications

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

The Network Access Manager, Web Security, and Umbrella Roaming Security modules can run as stand-alone 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-ver-pre-deploy-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 web security:

```
msiexec /package anyconnect-websecurity-win-<version>-pre-deploy-k9.msi /norestart /passive /lvx* c:\test.log
```

**Step 3** (Optional) Install DART.

```
misexec /package anynconnect-dart-win-<version>-k9.msi /norestart /passive /lvx* c:\test.log
```

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

**Step 5** Restart the Cisco AnyConnect Web Security Agent windows service.
Deploying AnyConnect Modules as Stand-Alone Applications

You can deploy the AnyConnect modules Network Access Manager and Web Security as stand-alone applications on a user computer. DART is supported with these applications.

You can deploy the AnyConnect Network Access Manager, Web Security, and Umbrella Roaming Security Modules as stand-alone 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 ISO 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 AnyConnect Web 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 Network Access Manager or Web Security 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 and/or the stand-alone Web 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.

Step 4

c) The Install Utility removes any existing VPN profiles and then installs VPNDisable_ServiceProfile.xml.

Step 4
d) The Install Utility invokes the Network Access Manager installer or the Web Security installer.

e) The Network Access Manager or Web Security Module is enabled without VPN service on the computer.
Pre-Deploying to Windows

Distributing AnyConnect Using the ISO

The ISO 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 ISO 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 choose which modules to load. So if you decide to distribute using an ISO, edit the ISO 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 PowerISO.

Pre-deployment ISO Modifications

- Update the ISO 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 ISO File

<table>
<thead>
<tr>
<th>File</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI.ico</td>
<td>AnyConnect icon image.</td>
</tr>
<tr>
<td>Setup.exe</td>
<td>Launches the Install Utility.</td>
</tr>
<tr>
<td>anyconnect-dart-win-version-k9.msi</td>
<td>MSI installer file for the DART module.</td>
</tr>
<tr>
<td>anyconnect-gina-win-version-pre-deploy-k9.msi</td>
<td>MSI installer file for the SBL module.</td>
</tr>
<tr>
<td>anyconnect-win-version-pre-deploy-k9.msi</td>
<td>MSI installer file for the AnyConnect core client.</td>
</tr>
<tr>
<td>autorun.inf</td>
<td>Information file for setup.exe.</td>
</tr>
<tr>
<td>eula.html</td>
<td>Acceptable Use Policy.</td>
</tr>
<tr>
<td>setup.hta</td>
<td>Install Utility HTML Application (HTA), which you can customize for your site.</td>
</tr>
</tbody>
</table>

Distributing AnyConnect Using an SMS

After extracting the installers (*.msi) for the modules you want to deploy from the ISO 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

<table>
<thead>
<tr>
<th>Module Installed</th>
<th>Command and Log File</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect core client No VPN capability. Use when installing stand-alone Network Access Manager or Web Security modules.</td>
<td><code>msiexec /package anyconnect-win-x.x.x-pre-deploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* anyconnect-win-x.x.x-pre-deploy-k9-install-datetimestamp.log</code></td>
</tr>
<tr>
<td>AnyConnect core client with VPN capability.</td>
<td><code>msiexec /package anyconnect-win-x.x.x-pre-deploy-k9.msi /norestart /passive /lvx* anyconnect-win-x.x.x-pre-deploy-k9-install-datetimestamp.log</code></td>
</tr>
<tr>
<td>Customer Experience Feedback</td>
<td><code>msiexec /package anyconnect-win-x.x.x-pre-deploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* anyconnect-win-x.x.x-pre-deploy-k9-install-datetimestamp.log</code></td>
</tr>
<tr>
<td>Diagnostic and Reporting Tool (DART)</td>
<td><code>msiexec /package anyconnect-dart-win-x.x.x-k9.msi /norestart /passive /lvx* anyconnect-dart-x.x.x-pre-deploy-k9-install-datetimestamp.log</code></td>
</tr>
<tr>
<td>SBL</td>
<td><code>msiexec /package anyconnect-gina-win-x.x.x-k9.msi /norestart /passive /lvx* anyconnect-gina-x.x.x-pre-deploy-k9-install-datetimestamp.log</code></td>
</tr>
</tbody>
</table>
## Module Installed | Command and Log File
---|---
Network Access Manager | msiexec /package anyconnect-nam-win-x.x.x-k9.msi /norestart /passive /lvx* anyconnect-nam-x.x.x-pre-deploy-k9-install-datetimestamp.log
Web Security | msiexec /package anyconnect-websecurity-win-x.x.x-pre-deploy-k9.msi /norestart/passive /lvx* anyconnect-websecurity-x.x.x-pre-deploy-k9-install-datetimestamp.log
VPN Posture (HostScan) | msiexec /package anyconnect-posture-win-x.x.x-pre-deploy-k9.msi /norestart/passive /lvx* anyconnect-posture-x.x.x-pre-deploy-k9-install-datetimestamp.log
ISE Posture | msiexec /package anyconnect-iseposture-win-x.x.x-pre-deploy-k9.msi /norestart/passive /lvx* anyconnect-iseposture-x.x.x-pre-deploy-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. In the Web Security module, you can use a service password to put the client in bypass mode. 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.

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 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.

We recommend that you use the sample transform 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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Install the AnyConnect modules in the following order:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a) Install the AnyConnect core client module, which installs the GUI and VPN capability (both SSL and IPsec).</td>
</tr>
<tr>
<td></td>
<td>b) Install the AnyConnect Diagnostic and Reporting Tool (DART) module, which provides useful diagnostic information about the AnyConnect core client installation.</td>
</tr>
<tr>
<td></td>
<td>c) Install the SBL, Network Access Manager, Web Security, Posture modules, or ISE compliance modules in any order.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Uninstall the AnyConnect modules in the following order:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a) Uninstall Network Access Manager, Web Security, Posture, ISE Compliance module, or SBL, in any order.</td>
</tr>
<tr>
<td></td>
<td>b) Uninstall the AnyConnect core client.</td>
</tr>
<tr>
<td></td>
<td>c) Uninstall DART last.</td>
</tr>
</tbody>
</table>

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. You can also modify the installer with ACTransforms.xml. You can customize the language and appearance and 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 Stand-Alone Application

The following procedure explains how to customize the modules by installing the stand-alone 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:

```
hdiskutil 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 WebSecurity_ServiceProfile.xml.

**Step 7** For these modules, the profile editor creates an additional obfuscated version of the profile, such as WebSecurity_ServiceProfile.wso for web security and saves it to the same location as you saved the file, such as WebSecurity_ServiceProfile.xml for web security. Follow these steps to complete the obfuscation:

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

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

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**

- 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](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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Install the AnyConnect core client module, which installs the GUI and VPN capability (both SSL and IPsec).</td>
</tr>
<tr>
<td>Step 2</td>
<td>Install the DART module, which provides useful diagnostic information about the AnyConnect core client installation.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Install the posture module or ISE compliance module.</td>
</tr>
</tbody>
</table>

**Uninstalling Modules for Linux**

The order that the user uninstalls AnyConnect is important.

DART information is valuable if the uninstall processes fails.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Uninstall the posture module or ISE compliance module.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Uninstall the AnyConnect core client.</td>
</tr>
</tbody>
</table>
Step 3  Uninstall DART.

Initializing Server Certificate Verification with Firefox

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 certificate 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 13.

This action is available for the VPN installer, Network Access Manager installer, and Web Security installer.

Manually Installing DART on a Linux Device


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.
Web Deployment with the ASA

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

User opens a browser and connects to the ASA’s clientless portal. The ASA establishes an initial SSL connection with the client, and opens a logon page. If the user satisfies logon and authentication, the clientless portal page displays the Start AnyConnect Client dialog. After the user selects an AnyConnect download, the ASA downloads the client that matches the computer’s operating system. After downloading, the client installs and configures itself and establishes an IPsec (IKEv2) or SSL connection to the ASA (web-launch). If web-launch cannot run because of problems with ActiveX or Java, then the user is able to download AnyConnect manually.

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.

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 tool 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

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 10 x86 (32-bit) and x64 (64-bit)</td>
<td>Internet Explorer 11</td>
</tr>
<tr>
<td></td>
<td>Firefox 3.51 and later</td>
</tr>
<tr>
<td>Windows 8.x x86 (32-bit) and x64 (64-bit)</td>
<td>Internet Explorer 11</td>
</tr>
<tr>
<td></td>
<td>Firefox 9.0.1 and later</td>
</tr>
<tr>
<td></td>
<td>Chrome 23.0.1271.95 m and later</td>
</tr>
<tr>
<td>Windows 7 x86 (32-bit) and x64 (64-bit)</td>
<td>Internet Explorer 11</td>
</tr>
<tr>
<td></td>
<td>Firefox 3 and later</td>
</tr>
<tr>
<td></td>
<td>Google Chrome 6 and later</td>
</tr>
<tr>
<td>Mac OS X 10.7, 10.8 (64-bit)</td>
<td>Safari 9.1</td>
</tr>
<tr>
<td>Mac OS X 10.9, 10.10, 10.11 (64-bit)</td>
<td>Google Chrome 6 and later</td>
</tr>
<tr>
<td>Linux64 (VPN install only)</td>
<td>(RHEL 6) Firefox 3 and later</td>
</tr>
<tr>
<td></td>
<td>(12.04) Firefox 10.0 and later</td>
</tr>
<tr>
<td></td>
<td>(14.04) Firefox 29.0 and later</td>
</tr>
</tbody>
</table>

Although versions other than those listed above may work, Cisco has not performed full testing on any version other than those listed.

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

AnyConnect 4.3 (and later) has moved to the Visual Studio (VS) 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 (and later), but the AnyConnect Secure Mobility Client must be upgraded first and running release 4.3 (and later).

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.

<table>
<thead>
<tr>
<th>OS</th>
<th>AnyConnect Web-Deploy Package Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>anyconnect-win-version-k9.pkg</td>
</tr>
<tr>
<td>macOS</td>
<td>anyconnect-macosx-i386-version-k9.pkg</td>
</tr>
<tr>
<td>Linux (64-bit)</td>
<td>anyconnect-linux-64-version-k9.pkg</td>
</tr>
</tbody>
</table>

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 downloder.

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 Machine
- Add AnyConnect Provisioning Resources from a Remote Site
- Deploy the AnyConnect client and resources

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
- 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.
- Combine customization and localization resources into a ZIP archive, which is called a bundle in ISE. A bundle can contain:
Configure ISE to Deploy AnyConnect

You must upload the AnyConnect package to ISE before you to 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. You must configure VPNDisable_ServiceProfile.xml to disable the VPN tile on AnyConnect GUI. VPNDisable_ServiceProfile.xml is on CCO with the other AnyConnect files.

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

<table>
<thead>
<tr>
<th>Prompt</th>
<th>ISE Resource Type and Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect Package</td>
<td>AnyConnectDesktopWindows</td>
</tr>
<tr>
<td></td>
<td>AnyConnectDesktopOSX</td>
</tr>
<tr>
<td></td>
<td>AnyConnectWebAgentWindows</td>
</tr>
<tr>
<td></td>
<td>AnyConnectWebAgentOSX</td>
</tr>
</tbody>
</table>
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.

### Configure 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, Mac, 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.

### Prompt | ISE Resource Type and Description
--- | ---
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
• 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.

• 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. If an update is available, the user connects to the Network Access Device (NAD), such as an ASA, wireless controller, or switch. Upon authorization, the NAD redirects the user to the ISE portal, and the AnyConnect downloader is installed on the client to manage the package extraction and installation.
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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In ASDM go to Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Group Policies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select a group policy and click <strong>Edit</strong> or <strong>Add</strong> a new group policy.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the navigation pane, choose <strong>Advanced</strong> &gt; AnyConnect Client &gt; Login Settings. Uncheck the Inherit check box, if necessary, and select a Post Login setting.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>OK</strong> and be sure to apply your changes to the group policy, then click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Custom Attribute</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeferredUpdateAllowed</td>
<td>true false</td>
<td>false</td>
<td>True enables deferred update. If deferred update is disabled (false), the settings below are ignored.</td>
</tr>
<tr>
<td>DeferredUpdateMinimumVersion</td>
<td>x.x.x</td>
<td>0.0.0</td>
<td>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.</td>
</tr>
</tbody>
</table>
**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 the VPN profile update, based on differentiation, should have occurred.

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

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

### Update Policy Guidelines

- Enable remote users to connect to a headend using its IP address by listing that server’s IP address in the authorized **Server Name** list. If the user attempts to connect using the IP address but the headend is listed as an FQDN, the attempt is treated as connecting to an unauthorized domain.

- Software updates include downloading customizations, localizations, scripts and transforms. When software updates are disallowed, these items will not be downloaded. Do not rely on scripts for policy enforcement if some clients will not be allowing script updates.

- Downloading a VPN profile with Always-On enabled deletes all other VPN profiles on the client. Consider this when deciding whether to allow or disallow VPN profiles updates from unauthorized, or non-corporate, headends.

- If no VPN profile is downloaded to the client due to your installation and update policy, the following features are unavailable:

  | Service Disable                  | Untrusted Network Policy |
  | Certificate Store Override       | Trusted DNS Domains      |
  | Show Pre-connect Message         | Trusted DNS Servers      |
  | Local LAN Access                 | Always-On                |
  | Start Before 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|

- 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:

  `%AllUsers%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Logs` directory.

### 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>true</AllowSoftwareUpdatesFromAnyServer>
    <AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer>
    <AllowServiceProfileUpdatesFromAnyServer>true</AllowServiceProfileUpdatesFromAnyServer>
    <AllowISEProfileUpdatesFromAnyServer>false</AllowISEProfileUpdatesFromAnyServer>
    <AllowComplianceModuleUpdatesFromAnyServer>true</AllowComplianceModuleUpdatesFromAnyServer>
    <AuthorizedServerList>
      <ServerName>seattle.example.com</ServerName>
      <ServerName>newyork.example.com</ServerName>
    </AuthorizedServerList>
  </UpdatePolicy>
</AnyConnectLocalPolicy>

With the following ASA headend configuration:

<table>
<thead>
<tr>
<th>ASA Headend</th>
<th>AnyConnect Package Loaded</th>
<th>Modules to Download</th>
</tr>
</thead>
<tbody>
<tr>
<td>seattle.example.com</td>
<td>Version 3.1.05182</td>
<td>VPN, Network Access Manager, Web Security</td>
</tr>
<tr>
<td>newyork.example.com</td>
<td>Version 3.1.06079</td>
<td>VPN, Network Access Manager</td>
</tr>
<tr>
<td>raleigh.example.com</td>
<td>Version 3.1.07021</td>
<td>VPN, Posture</td>
</tr>
</tbody>
</table>

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. The Web Security software module is downloaded and installed, as well as the Web Security profile, if available. 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, Network Access Manager, and Web Security modules are downloaded and installed. 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. Since software updates are allowed, the VPN, Network Access Manager, Web Security, and Posture modules are all upgraded. Because the VPN profile and service profile updates are not allowed, they are not downloaded. If the VPN profile could have been updated (based on it being different), the connection will terminate.
**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:

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

**Port Used by AnyConnect and the Legacy VPN Client**

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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Cisco AnyConnect Client Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS (SSL)</td>
<td>TCP 443</td>
</tr>
<tr>
<td>SSL Redirection</td>
<td>TCP 80 (optional)</td>
</tr>
<tr>
<td>DTLS</td>
<td>UDP 443 (optional, but highly recommended)</td>
</tr>
<tr>
<td>IPsec/IKEv2</td>
<td>UDP 500, UDP 4500</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Cisco VPN Client (IPsec) Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPsec/NATT</td>
<td>UDP 500, UDP 4500</td>
</tr>
<tr>
<td>IPsec/NATT</td>
<td>UDP 500, UDP 4500</td>
</tr>
<tr>
<td>IPsec/TCP</td>
<td>TCP (configurable)</td>
</tr>
<tr>
<td>Protocol</td>
<td>Cisco VPN Client (IPsec) Port</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>IPsec/UDP</td>
<td>UDP 500, UDP X (configurable)</td>
</tr>
</tbody>
</table>