Introduction to the AnyConnect Secure Mobility Client

The Cisco AnyConnect Secure Mobility client is the next-generation VPN client, providing remote users with secure IPsec (IKEv2) or SSL VPN connections to the Cisco 5500 Series Adaptive Security Appliance (ASA). AnyConnect provides end users with a connectivity experience that is intelligent, seamless and always-on, with secure mobility across today's proliferating managed and unmanaged mobile devices.

Deployable from the ASA or from Enterprise Software Deployment Systems

AnyConnect can be deployed to remote users from the ASA or using enterprise software deployment systems. When deployed from the ASA, remote users make an initial SSL connection to the ASA by entering the IP address or DNS name in their browser of an ASA configured to accept clientless SSL VPN connections. The ASA presents a login screen in the browser window, and if the user satisfies the login and authentication, downloads the client that matches the computer operating system. After downloading, the client installs and configures itself and establishes an IPsec (IKEv2) or SSL connection to the ASA.

Customizable and Translatable

You can customize the AnyConnect to display your own corporate image to remote users. You can rebrand AnyConnect by replacing our default GUI components, deploy a transform you create for more extensive rebranding, or deploy your own client GUI that uses the AnyConnect API. You can also translate messages displayed by AnyConnect or the installer program in the language preferred by the remote user.

Easily Configured

Using ASDM, you can easily configure AnyConnect features in the client profile—an XML file that provides basic information about connection setup, as well as advanced features such as Start Before Logon (SBL). For some features, you also need to configure the ASA. The ASA deploys the profile during AnyConnect installation and updates.

Additional Supported Modules

The Cisco AnyConnect Secure Mobility client, Version 3.1, integrates these modules into the AnyConnect client package:

- AnyConnect Network Access Manager—(Formerly called the Cisco Secure Services Client) This module provides the detection and selection of the optimal Layer 2 access network and performs device authentication for access to both wired and wireless networks.
- AnyConnect Posture Assessment—Provides the AnyConnect Secure Mobility Client the ability to identify the operating system, antivirus, antispyware, and firewall software installed on the host prior to creating a remote access connection to the ASA. Based on this prelogin evaluation, you can control which hosts are allowed to create a remote access connection to the security appliance. The Host Scan application is delivered with the posture module and is the application that gathers this information.
- AnyConnect Telemetry—Sends information about the origin of malicious content detected by the antivirus software to the web filtering infrastructure of the Cisco IronPort Web Security Appliance (WSA), which uses this data to provide better URL filtering rules.
- AnyConnect Web Security—Routes HTTP traffic to the ScanSafe Web Security scanning proxy server for content analysis, detection of malware, and administration of acceptable use policies.
- AnyConnect Diagnostic and Reporting Tool (DART)—Captures a snapshot of system logs and other diagnostic information and creates a .zip file on your desktop so you can conveniently send troubleshooting information to Cisco TAC.
- AnyConnect Start Before Logon (SBL)—Starts AnyConnect before the Window dialog box appears and forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting AnyConnect before the Windows login dialog box appears.
- AnyConnect Customer Experience Feedback—This feature provides Cisco with client information that gives us insight into the user experience statistics, the basis of crash incidents, and so on, so that software quality and user experience are further improved.

This chapter includes the following sections:

AnyConnect License Options

Overview

The AnyConnect Secure Mobility client requires license activation to support VPN sessions and web security. The license(s) required depend on the AnyConnect VPN Client and Secure Mobility features that will be used, and the number of sessions you want to support. One or more of the following AnyConnect licenses may be required for your deployment:

License	Description	Applied to:
AnyConnect Essentials	Supports basic AnyConnect features for SSL and IPSec VPN connections. This license specifies the maximum number of remote access sessions supported at a time.	Cisco ASA 8.0(x) or later.
AnyConnect Premium	Supports all basic AnyConnect Essentials features plus Premium AnyConnect client features such as browser-based VPN access, and Cisco Secure Desktop, and Host Scan/Posture module functions. This license specifies the maximum number of remote access sessions supported at a time, this license type can also be shared.	Cisco ASA 8.0(x) or later.
AnyConnect Mobile	Supports AnyConnect mobile access to the security appliance. It is available as an addition to, and requires, either an AnyConnect Essentials or an AnyConnect Premium license.	Cisco ASA 8.0(x) or later.
AnyConnect Flex	A flex license provides business continuity support for all licensed features.	Cisco ASA 8.0(x) or later
Advanced Endpoint Assessment	Enables advanced endpoint assessment capabilities such as auto-remediation. Requires an activated AnyConnect Premium license.	Cisco ASA
Cisco Secure Mobility for AnyConnect	Supports web security features provided by the Cisco IronPort Web Security Appliance (WSA). The license name depends on the AnyConnect license activated on the ASA, Essentials or Premium. A Cisco IronPort Web Security Appliance license is also required.	Cisco WSA 7.0 or later.
Cisco Secure Mobility for Cisco Cloud Web Security	Supports security features provided with the AnyConnect Web Security module allowing roaming users to be protected by Cisco Cloud Web Security (ScanSafe). This license is required in addition to Cisco Cloud Web Security Web Filtering and/or Cisco Cloud Web Security Malware Scanning license.	

AnyConnect Essentials and Premium Licenses

- You can activate either an AnyConnect Essentials license or an AnyConnect Premium license on a Cisco ASA 8.0(x) or later, but you cannot activate both licenses together. Some features require later versions of the ASA, as indicated in the Features Table. Choose the license you will activate based on the AnyConnect Secure Mobility features you will use.
- In addition to AnyConnect connectivity, an AnyConnect Essentials activated on the ASA supports sessions established using Cisco's legacy VPN Client, and full tunneling access to enterprise applications. Clientless VPN access and Cisco Secure Desktop are not available with an AnyConnect Essentials license.
- An ASA activated with an AnyConnect Premium license supports all access allowed by the AnyConnect Essentials license plus the following AnyConnect premium features:
  - Clientless VPN access: Allows a remote user to use a browser to establish a VPN session, and lets specific applications use the browser to access that session.
  - Cisco Secure Desktop: For both browser-based and AnyConnect sessions.
  - Post Log-in Always-on VPN: Always-on establishes a VPN session automatically after the user logs in to a computer. For more information, see Always-on VPN. This feature also includes a Connect Failure policy and Captive Portal Hotspot Detection and Remediation.

Note Always-on can also be enabled by activating a Cisco Secure Mobility for AnyConnect license on the WSA with an AnyConnect Essentials license on the ASA.

  - Endpoint assessment: Ensures that your choice of antivirus software versions, antispyware versions, associated update definitions, firewall software versions, and corporate property verification checks comply with policies to qualify a session to be granted access to the VPN.

    Endpoint remediation requires an Advanced Endpoint Assessment License in addition to the AnyConnect Premium License as described below.

  - Quarantine: Using Dynamic Access Policies to quarantine non-compliant AnyConnect users. User can be notified with a custom message.

- Neither the AnyConnect Essentials or Premium license is required for:
  - The Network Access Manager module. It is licensed without charge for use with Cisco wireless access points, wireless LAN controllers, switches, and RADIUS servers. A current SmartNet contract is required on the related Cisco equipment.
  - The DART module and Customer Feedback function.

AnyConnect Mobile License

The activation of an AnyConnect Mobile license on the ASA supports mobile access but does not provide support for AnyConnect features. It is available as an option with either an AnyConnect Essentials or an AnyConnect Premium license.

AnyConnect 3.1 does not currently support mobile devices, this license will need to be activated on the ASA if you expect connectivity from Android or Apple iOS devices running older versions of AnyConnect.

AnyConnect Flex License

An AnyConnect Flex license provides business continuity support for licensed features only. Business continuity increases the number of licensed remote access VPN sessions to prepare for temporary spikes in usage during cataclysmic events such as pandemics. Each Flex license is ASA-specific and provides support for sixty days. The count can consist of both contiguous and noncontiguous days.

Advanced Endpoint Assessment License

An Advanced Endpoint Assessment license must be activated in conjunction with an AnyConnect Premium license. It allows the initiation of endpoint remediation.

Endpoint remediation is initiated when a connection has been disallowed by Dynamic Access Policies (DAPs) on the ASA. Endpoint remediation attempts to remediate various aspects of antivirus, antispyware and personal firewall protection on the endpoint, only if that software allows a separate application to initiate remediation. If the endpoint remediation is successful, DAP will allow a subsequent connection.

Cisco Secure Mobility for AnyConnect License

A Cisco Secure Mobility for AnyConnect license activated on the WSA provides services for browser-based SSL sessions and AnyConnect VPN sessions such as:

- Malware defense.
- Acceptable use policy enforcement.
- Data leakage prevention for the web.
- Protecting endpoints from websites found to be unsafe by granting or denying all HTTP and HTTPS requests.
- Providing administrator access to Internet usage reports for all VPN sessions.

The Cisco Secure Mobility for AnyConnect license must be activated as follows:

- A Cisco Secure Mobility for AnyConnect Premium license activation on the WSA requires activation of either an AnyConnect Premium or an AnyConnect Essentials license on the ASA.
- A Cisco Secure Mobility for AnyConnect Essentials license activation on the WSA requires activation of an AnyConnect Essentials license on the ASA. You cannot use a Cisco Secure Mobility for AnyConnect Essentials license activated on a WSA in combination with an AnyConnect Premium license activated on an ASA.

  Note Post Log-in Always-on VPN, a Premium feature, can be enabled by activating a Cisco Secure Mobility for AnyConnect license on the WSA with an AnyConnect Essentials license on the ASA.

- The Cisco Secure Mobility for AnyConnect license activated on the WSA must match or exceed the number of VPN sessions supported by the AnyConnect license activated on the ASA.

This Cisco Secure Mobility license for AnyConnect, Premium or Essentials, is in addition to the activated Cisco IronPort Web Security Appliance license.

For more information, see the *Cisco IronPort Web Security Appliances Introduction*.

Combining AnyConnect Licenses

Sessions License	License Option	Basic Access	Mobile Access	Client-less Access	Post Log-in Always-on VPN	Malware Defense, Acceptable Use Policy Enforcement, and Data Leakage Prevention on the Web	Endpoint Assess-ment	Endpoint Reme-diation
AnyConnect Essentials	(base license)	✓						
+	AnyConnect Mobile	✓	✓					
+	Cisco Secure Mobility for AnyConnect Essentials	✓	✓		✓	✓		
+	AnyConnect Flex[1]	✓	✓		✓	✓		
AnyConnect Premium SSL VPN Edition	(base license)	✓		✓	✓		✓	
+	AnyConnect Mobile	✓	✓	✓	✓		✓	
+	Cisco Secure Mobility for AnyConnect Premium	✓	✓	✓	✓	✓	✓	
+	Advanced Endpoint Assessment	✓	✓	✓	✓	✓	✓	✓
+	AnyConnect Flex[1]	✓	✓	✓	✓	✓	✓	✓

[1] A flex license provides business continuity support for mobile access, malware defense, acceptable use policy enforcement, data leakage prevention on the web, and endpoint remediation features only if those features are licensed.

Standalone and WebLaunch Options

The user can use AnyConnect in the following modes:

- Standalone mode—Lets the user establish an AnyConnect connection without using a web browser. If you have permanently installed AnyConnect on the user's PC, the user can run in standalone mode. In standalone mode, a user opens AnyConnect just like any other application and enters the username and password credentials into the fields of the AnyConnect GUI. Depending on how you configure the system, the user might also be required to select a group. When the connection is established, the ASA checks the version of AnyConnect on the user's PC and, if necessary, the client downloads the latest version.

- WebLaunch mode—Lets the user enter the URL of the ASA in the Address or Location field of a browser using the HTTPS protocol. The user then enters the username and password information on a Logon screen, selects the group, and clicks **Submit**. If you have specified a banner, that information appears, and the user acknowledges the banner by clicking **Continue**.

  The portal window appears. To start AnyConnect, the user clicks **Start AnyConnect** on the main pane. A series of documentary windows appears. When the Connection Established dialog box appears, the connection is working, and the user can proceed with online activities.

If you configure the ASA to deploy the AnyConnect package, you ensure that the ASA is the single point of enforcement as to which versions of AnyConnect can establish a session, even if you deploy AnyConnect with an enterprise software deployment system. When you load an AnyConnect package on the ASA, you enforce a policy to which only versions as new as the one loaded on the ASA can connect. AnyConnect upgrades itself when it connects to the ASA. Alternatively, you can deploy a local policy file that specifies whether the client bypasses the client downloader, eliminating the requirement for the client package file on the ASA. However, other features such as weblaunch and automatic updates are disabled.

Configuration and Deployment Overview

Use the AnyConnect Profile editor to configure the AnyConnect features in the profile file; then configure the ASA to download this file along with AnyConnect client automatically when users make a VPN connection to the ASA with a browser. The profile file drives the display in the user interface and defines the names and addresses of host computers. By creating and assigning different profiles to group policies configured on the ASA, you can differentiate access to these features. Following assignment to the respective group policies, the ASA automatically pushes the profile assigned to the user upon connection setup.

Profiles provide basic information about connection setup, and users cannot manage or modify them. The profile is an XML file that lets you identify the secure gateway (ASA) hosts that you want to make accessible. In addition, the profile conveys additional connection attributes and constraints on a user. For some features, you can specify some settings in the profile as user controllable. The AnyConnect GUI displays controls for these settings to the end user.

If a user has a single profile file, this profile contains all the hosts needed by a user, and additional settings as needed. In some cases, you might want to provide more than one profile for a given user. For example, someone who works from multiple locations might need more than one profile. Be aware, however, that some of the profile settings, such as Start Before Login, control the connection experience at a global level. Other settings, such as those unique to a particular host, depend on the host selected.

Alternatively, you can use an enterprise software deployment system to install the profile file and client as an application on computers for later access.

AnyConnect Secure Mobility Feature Configuration Guidelines

AnyConnect Secure Mobility is a set of features you can configure to optimize the security of the VPN endpoints. To configure all of the AnyConnect secure mobility client options, refer to the following sections:

Step 1 Go to the section “Configuring WSA Support of the AnyConnect Secure Mobility Solution” on page 17 of the Cisco AnyConnect Secure Mobility Solution Guide as a guide to configuring a WSA to support AnyConnect.

Step 2 Use the AnyConnect Profile Editor to configure the following features:

- Trusted Network Detection, page 3-22
- Always-on VPN, page 3-24
- Disconnect Button for Always-on VPN, page 3-29
- Connect Failure Policy for Always-on VPN, page 3-31
- Captive Portal Hotspot Detection and Remediation, page 3-33
- Configuring Certificate Enrollment using SCEP, page 3-42

API

Use the Application Programming Interface (API) if you want to automate a VPN connection with AnyConnect from another application, including the following:

- Preferences
- Set tunnel-group method

The API package contains documentation, source files, and library files to support a C++ interface for AnyConnect. You can use libraries and example programs for building AnyConnect on Windows, Linux, and Mac OS X. The API package includes project files (Makefiles) for the Windows platform. For other platforms, a platform-specific script shows how to compile the example code. You can link your application (GUI, CLI, or embedded application) with these files and libraries.

The API supports only the VPN functionality of the client. It does not support the optional AnyConnect modules, such as the Network Access Manager, Web Security, and telemetry.

AnyConnect Accessibility

AnyConnect provides functionality for users that allows them to access buttons on the window without using a mouse.

The following navigation shortcuts assist visually impaired or blind attendants to use the application.

Keystroke	Action
Alt	Moves focus to the browser menu bar.
Enter	Chooses the item with focus.
Alt+arrow keys	Moves between browser menus.
Alt+underlined letter	Takes you to the menu.
Spacebar	Toggles control; for example, checks and unchecks a check box.
Tab	Moves focus to the next item in the tab order or to next control group.
Shift+Tab	Moves focus to the previous item or group in the tab order.

Keystroke	Action
Arrow keys	Moves among controls within a group.
Home	Moves to the top of the window if more than one screenful of information exists. Moves to the beginning of a line of user-entered text.
End	Moves to the end of a line of user-entered text. Moves to the bottom of the window if more than one screenful of information exists.
Page Up	Scrolls up one screen.
Page Down	Scrolls down one screen.