Release Notes for Cisco AnyConnect Secure Mobility Client 2.4 for Symbian

Updated: May 31, 2011

Content

This document includes the following sections:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

This document provides only Symbian information for the Cisco Secure Mobility client. This document supplements the *Cisco AnyConnect VPN Client Administrator Guide.* You can use the same Cisco adaptive security appliances (ASAs) to support or deploy later releases of AnyConnect for other devices simultaneously.

This release of AnyConnect provides remote users with secure VPN connections to the Cisco ASA 5500 Series using the Secure Socket Layer (SSL) protocol and the Datagram TLS (DTLS) protocol.

Seamless and secure remote access to enterprise networks is provided. If the AnyConnect VPN access point is used for traffic, the client provides a full or split include/exclude tunneling experience that allows any installed application to communicate as though connected directly to the enterprise network. If the user explicitly uses a different access point (besides the AnyConnect VPN access point), traffic is not encrypted, and packets are not visible to AnyConnect.

Devices Supported

This AnyConnect release supports the Nokia E6 and any other Nokia device that runs a "New Symbian OS." The device must be a touchscreen phone.

Note "New Symbian OS" is the name for the latest Symbian operating system, previously referred to as Symbian^3.

Security Appliances and Software Supported

Only ASA models support the Cisco AnyConnect Secure Mobility client for Symbian. See the *Adaptive Security Appliance VPN Compatibility Reference*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html for a complete list of compatibility requirements.

Table 1 shows the minimum Cisco ASA 5500 software images that support AnyConnect.

Table 1 Software Images that Support AnyConnect, Release 2.4

Image Type	Version
ASA Boot Image	8.0(4) or later
Adaptive Security Device Manager (ASDM)	6.1(3) or later

Note Routers running Cisco IOS do not currently support AnyConnect for Symbian.

AnyConnect Licensing

An AnyConnect Mobile license is required for VPN connections when using AnyConnect for Symbian.

This license is mutually exclusive per ASA, but you can configure a mixed network. The AnyConnect Mobile license is nominally priced to cover Cisco support. We offer the following trial options:

- If you have an AnyConnect Essentials or Premium license and you would like to obtain a three-month trial Mobile AnyConnect license, go to the following website: https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?FormId=717
- If you would like to obtain both an AnyConnect Essentials or Premium license and an AnyConnect Mobile license, or you have questions about licensing, email us a request with the **show version** output from your ASA to ac-mobile-license-request@cisco.com.

For brief descriptions and example product numbers (SKUs) of the AnyConnect user license options, see Cisco Secure Remote Access: VPN Licensing Overview.

For the latest details about the AnyConnect user license options, see Managing Feature Licenses in the *Cisco ASA 5500 Series Configuration Guide using the CLI, 8.3*.

Other Supported Features

Cisco supports the following AnyConnect features:

- Tunnel Protocols
  - Cisco SSL Tunneling Protocol (CSTP)
  - Cisco DTLS Tunneling Protocol (CDTP)
- SSL Cipher Suites
  - AES256-SHA
  - AES128-SHA
  - DES-CBC3-SHA
  - RC4-SHA
  - RC4-MD5
  - DES-CBC-SHA
- DTLS Cipher Suites
  - AES256-SHA
  - AES128-SHA
  - DES-CBC3-SHA
  - DES-CBC-SHA
- Authentication
  - Client certification authentication
  - Username/password
  - Double authentication
  - Group selection
  - RADIUS and LDAP server-based authentication

- Simultaneous full-tunnel and clientless connections
- Rekey
- TLS Compression
- Cisco Profile Support
- Profile Update
- Post-Login Banner
- Dead Peer Detection

Note If the update interval is set to a minimum value, it has an adverse effect on device battery life.

- Tunnel Keep-Alive
- Backup Server List
- Default Domain
- Cluster Support
- DNS Server Configuration (only 2 on the VPN session)
- Network Change Monitoring, limited

Note When a new, higher priority WiFi network becomes available, AnyConnect does not switch over to it immediately. To conserve battery life, Symbian does not do real-time scanning for wireless networks. A timeout, configurable in the WiFi settings on the phone, determines the timeframe for AnyConnect to discover a new WiFI network and migrate to it, even if the phone is in the range of a known high-priority WiFi access point.

- Statistics
- Graphical User Interface
- Pre-login Banner
- Certificate Import
- Automatic upgrades from secure gateway

Limitations of the AnyConnect Secure Mobility Client for Symbian

This release of AnyConnect for Symbian supports only the features that are strictly related to remote access. It supports the following types of VPN configurations:

- Manually generated
- AnyConnect profile imported

This release supports the Tunnel Keep-Alive feature; however, it can reduce the battery life of the device. Increasing the update interval can mitigate the issue.

Note AnyConnect 2.4 for Symbian does not support features introduced in later AnyConnect releases, such as AnyConnect 2.5 or 3.0.

Open Bugs in AnyConnect for Symbian

Release 2.4 has the following known bugs for Symbian:

CSCto43931: Symbian Web Browser converts to *Ask when needed* mode when an AnyConnect VPN access point is selected as the connection.

Symbian's built-in Web Browser (like most other apps) allows the user to select the connection option as one of the following:

- Ask when needed
- Select a specific destination (recommended)
- Select a specific access point

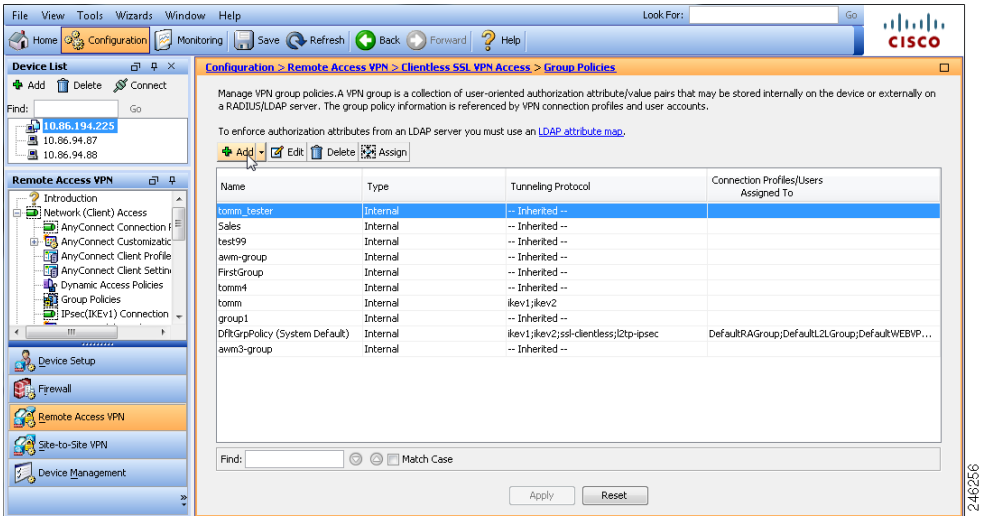
Workaround: With the *Select a specific access point* option, you can specify an access point (AnyConnect VPN). We recommend that you choose the intranet destination as the connection type. This selection allows the browser to use the intranet WiFi access points when available and automatically switches to VPN (AnyConnect VPN) when no other higher priority intranet access point is available.

Setting Up Automatic Download of SiS Installer

The Cisco AnyConnect Secure Mobility client for a Symbian device is installed with the standard Software Installation Script (SiS) standalone installer. The .sis file is contained within the .pkg file, and neither requires manipulation as long as you use a group URL for the connection profile, as described below. Follow these steps to set up the automatic download of the SiS installer for the user:

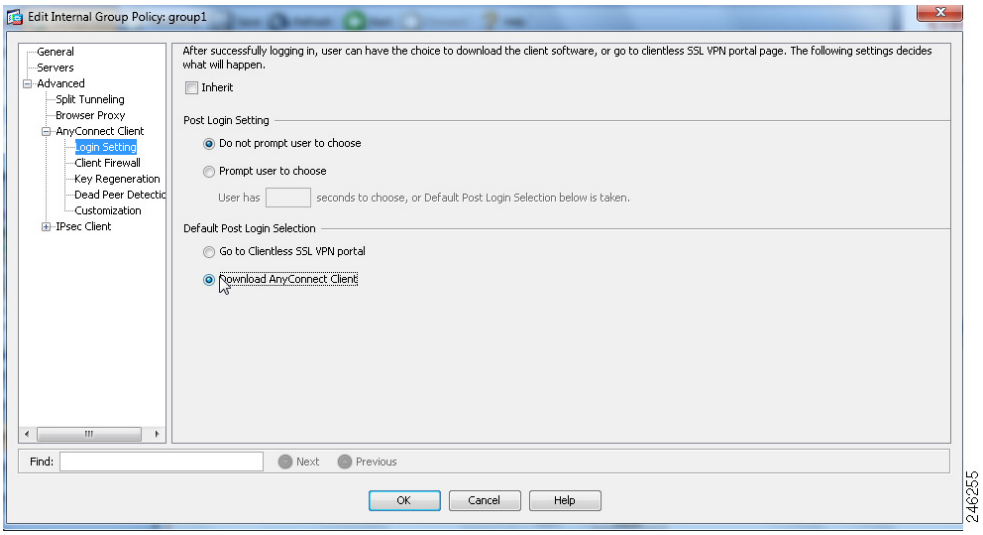
Step 1 Create a new group policy (see Figure 1) using all default content (at Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add).

Figure 1 Creating Group Policy



Step 2 In the created group policy, change the Default Post Login Selection to **Download AnyConnect Client** (at Edit Internal Group Policy > Advanced > AnyConnect Client > Login Setting).

Figure 2 Choosing Download AnyConnect Client



Step 3 Create a new connection profile (at Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile > Add). Use the **Group Policy** drop-down menu to choose the group policy created in Step 2.

Step 4 In the profile creation window go to **Advanced > SSL VPN**. Under Group URLs, click **Add** to add a new group URL for this connection profile.

Step 5 Enter **https://exampleasa.com/getinstaller** (where *exampleasa.com* is the hostname of your ASA and *getinstaller* is the group URL identifier) in the group URL. Also in the group URL section, check the **Do not run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above** check box.

Step 6 Click **OK** to save the connection profile.

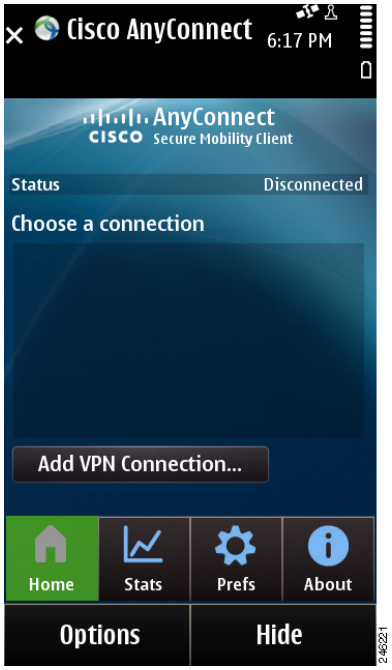
Step 7 Provide your users with the group URL configured in Step 5 (such as https://exampleasa.com/getinstaller) and the necessary credentials to access ASA.

Users can visit the given URL with their browser, authenticate using the provided credentials, and then download the AnyConnect installer.

Client User Interface

Choose the AnyConnect icon on the Nokia desktop to display the Home screen. Figure 3 shows the Home screen.

Figure 3 Nokia AnyConnect Home Screen



The Home screen lists the names of the VPN connection entries stored on the device and lets you add new VPN connection entries.

The icon bar at the bottom of the display provides navigation icons for the Home, Statistics, Preferences, and About screens.

Configuration and Deployment Overview

At minimum, AnyConnect requires the user to create a connection entry that requires the following:

- Description—Uniquely identifies one VPN connection from another.
- Server address—Fully qualified domain name or IP address of the destination, including the URL path if the ASA VPN configuration specifies the group URL.

AnyConnect Profiles

An AnyConnect client user profile is an XML file that enables you to identify a list of secure gateways (security appliances) that you want to make accessible. In addition, a profile conveys additional connection attributes and constraints on a user.

You can use the AnyConnect Profile editor to configure the client features within a profile; then configure the security appliance to upload this file when a Symbian device establishes a VPN connection.

Typically, a user has a single profile file. This profile contains all the hosts needed by a user, and additional settings as needed. The client downloads the profile from the head-end and creates VPN connections based on the host entries in the profile.

Note AnyConnect retains only one profile on the Symbian device at a time. However, a profile can consist of multiple connection entries.

If you choose the **Prefs** button, you can set preferences for some items. The items and values are populated based on the user controller preferences from the profile. Some of the items and values include the following:

- Minimize on Connect—Controls the AnyConnect GUI behavior when a VPN session is established. By default, the GUI does not minimize when the VPN session is established. If set to true, AnyConnect is sent to the background immediately after the VPN is connected.
- Debug Level—Specify which level you want recorded in the log file.
  - Trace—Logs debug messages, warnings, and error messages (used for troubleshooting purposes)
  - Errors—Logs only error messages (the default configuration)
  - Warnings—Logs errors and warning messages
- AutoReconnect—Allows an administrator to control how a client behaves when the VPN session is interrupted. If set to true, the VPN automatically tries to reconnect when interrupted.
- AutoUpdate—Allows an administrator to turn off the dynamic update functionality of AnyConnect.

Connection Persistence

AnyConnect for Symbian supports a full suite of authentication capabilities similar to AnyConnect for Windows, Mac OS X, and Linux.

To achieve the most transparent end user experience, use certificate-only authentication. When a digital certificate is issued, AnyConnect supports the Symbian on-demand VPN feature which enables a VPN connection to be established without user interaction. The user may also manually establish a connection.

Symbian On-Demand VPN

The Symbian On-Demand VPN feature lets an application initiate a VPN connection when a VPN access point is chosen to open a network connection. The user must choose the correct access point or destination and then, outside of AnyConnect, it is determined whether the VPN is used. For example, if your official email client is configured to use the intranet destination, the AnyConnect VPN access point

automatically connects when no other connection is available through the intranet destination. No special configuration (such as hostname or DNS) is required, but Cisco provides an implementation so that users can get a connection either with or without being prompted for credentials, depending on the current default server.

Note Cisco recommends that a group URL be configured for the VPN connection. On demand operates as expected if no group URL is established, but the user will be prompted during authentication.

AnyConnect supports different kinds of authentication, either password based or certificate based. You are not required to have only certificate-based authentication during on-demand VPN.

Recommended ASA Configurations

For the best user experience, Cisco recommends using multiple connection profiles (tunnel groups) for mobile devices, depending on the authentication configuration. You will have to decide how best to balance user experience with security.

- For certificate-based authentication connection profiles for mobile devices that have on-demand VPN configured, use an idle timeout (vpn-idle-timeout) for the connection profile that is very short (such as 180 seconds). You may want to set the idle timeout if your VPN session is not critical for an application and does not need to be connected all the time. This allows the Symbian device to close the VPN connection when it is no longer needed, for example when the device goes into sleep mode. The default time-out for an idle connection profile is 30 minutes.
- For AAA-based authentication connection profiles for mobile devices, use a very long idle-timeout for the connection profile, such as 24 hours, to let the client remain in a reconnecting state without requiring the user to re-authenticate.

Troubleshooting

This section describes solutions to common problems related to AnyConnect for Symbian. If problems still persist after trying these solutions, contact your organization's IT support department.

- **Connection time-outs and unresolved hosts.**

  Internet connectivity issues, a low cell signal level, or a congested network resource can often cause time-outs and unresolved host errors. If a LAN is within reach, try using your device Settings app to establish a connection with the LAN first. Retrying multiple times in response to time-outs often results in success.

- **VPN client driver encountered an error**

  After the session initiation starts, the connection times out if the session is not established within the stipulated timeframe (currently defaulted to five minutes). If a timeout occurs and this error appears, invoke a retry.

- **Certificate-based authentication does not work.**

  Check the validity and expiration of the certificate if you succeeded with it before. Check with your system administrator to make sure you are using the appropriate certificate for the connection.

- **AnyConnect failed to establish a connection but no error message was displayed.**

Messages can be displayed only when the AnyConnect application is open.

- **A profile called Cisco AnyConnect exists that cannot be deleted.**

  Try restarting the application.

- **When I remove the AnyConnect application, VPN configurations still appear in the Symbian network settings.**

  Manually delete the VPN configuration or Internet Access Point (IAP) from the intranet destination using Menu > Settings > Connectivity > Settings > Destinations > Intranet.

- **AnyConnect VPN Connection does not migrate to the new Internet WiFi network.**

  To conserve battery life, Symbian does not do real-time scanning for wireless access points. WiFi scanning might be delayed as much as 10 minutes (default). The timeout is configurable in the WiFi settings on the phone. Based on this timeout value, it might take time for AnyConnect to discover a new WiFi network and migrate to it, even if the phone is in the range of a known high-priority WiFi access point.

Preventing Symbian Devices from Establishing SSL VPN Connections

An adaptive security appliance (ASA) must be activated with an AnyConnect Mobile license to support Symbian SSL VPN connections. If an ASA is not activated with an AnyConnect Mobile license, it automatically denies these connection attempts.

By default, an ASA activated with an AnyConnect Mobile license lets any user who can authenticate log in from a Symbian device running AnyConnect. You can configure an ASA to prevent these connections; however, at this time, doing so requires both of the following:

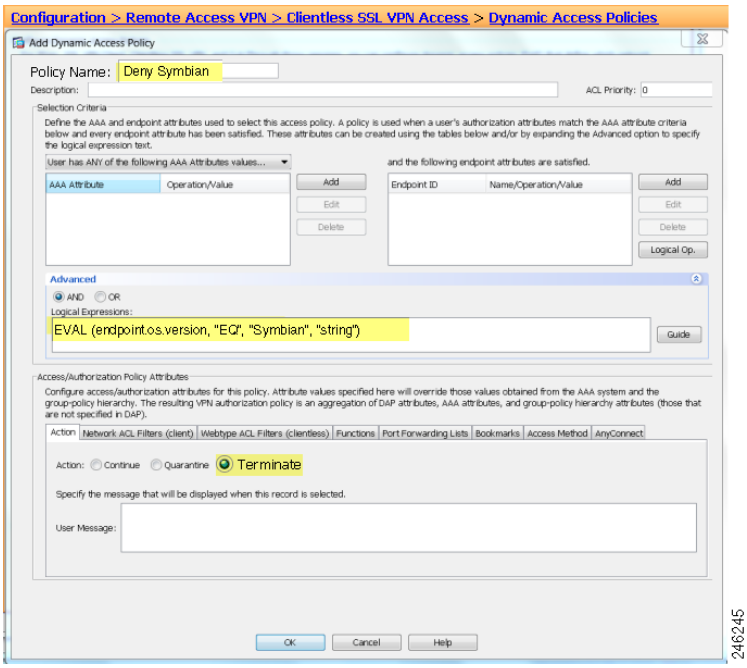
- The ASA must be activated with an AnyConnect Premium license. This is a technical requirement. We are considering an enhancement request to eliminate it.
- CSD must be enabled.

To configure an ASA to prevent SSL VPN connections from Symbian, add a dynamic access policy, as follows:

Step 1 Establish an ASDM session with the ASA.

Step 2 Choose **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add**.

Figure 4 DAP to Prevent SSL VPN Connections from Symbian Devices



Step 3 Name the policy (for example, `Deny Symbian`).

Step 4 Click **Advanced**.

Step 5 Enter the following into the Logical Expressions text box:

```
EVAL(endpoint.os.version, "EQ", "Symbian", "string")
```

Step 6 Click **Terminate** under the Action tab.

Step 7 Click **OK** and **Apply**.

AnyConnect Support Policy

Cisco supports all AnyConnect software versions downloaded for the Nokia devices; however, fixes and enhancements are provided only in the most recently released version.

End-User License Agreement

For the end-user license agreement, go to:
http://www.cisco.com/univercd/cc/td/doc/es_inpck/eu1jen__.pdf

OpenSSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

For Open Source License information for this product, please see the following link: http://www.cisco.com/en/US/docs/security/asa/asa83/license/opensrce.html#wp50053.

Related Documentation

For more information, refer to the following documentation:

- *Release Notes for Cisco AnyConnect VPN Client Release 2.4:*

  http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect24/release/notes/anyconnect24rn.html

- *Cisco AnyConnect VPN Client, Administrator Guide*

  http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect24/administration/guide/anyconnectadmin24.html

- *Navigating the Cisco ASA 5500 Series Documentation*:

  http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html