Release Notes for Cisco AnyConnect Secure Mobility Client 2.4.x for Android Mobile Devices

Updated: September 15, 2011

Content

This document includes the following sections:

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

Introduction

Written for system administrators of Cisco ASA 5500 Series adaptive security appliances, this document provides only Android-specific information for the Cisco AnyConnect Secure Mobility client, version 2.4.x. This document supplements the Cisco AnyConnect Administrator Guides. You can deploy later releases of AnyConnect for other devices simultaneously with this release.

AnyConnect 2.4.x 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. It also provides seamless and secure remote access to enterprise networks. The AnyConnect client provides a full tunneling experience that allows any installed application to communicate as though connected directly to the enterprise network.

The Cisco AnyConnect for Samsung, Cisco AnyConnect for Lenovo, and Cisco AnyConnect for Rooted Android releases are available on the Android Market. The Android Market provides all AnyConnect for Android distributions and updates.

Requirements

The following sections list the secure gateway release requirements, and license and configuration options.

Note For device requirements, installation instructions, and user information, see the *User Guide for Cisco AnyConnect Secure Mobility Client, Release 2.4 for Android*.

Secure Gateway Requirements

Adaptive Security Appliances (ASA)

ASA models support the Cisco AnyConnect Secure Mobility client for Android. See the *Adaptive Security Appliance VPN Compatibility Reference* 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 for Android

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

Cisco Routers

Any Cisco router running Cisco IOS version 15.1(1)T or later support the Cisco AnyConnect Secure Mobility client for Android.

License Options

AnyConnect for Android connections require the following licenses on the ASA:

- One of the following AnyConnect core license options:
  - Cisco AnyConnect Essentials license (L-ASA-AC-E-55XX=), sufficient for ASA Release 8.2 or later.
  - Cisco AnyConnect Premium Clientless SSL VPN Edition license (L-ASA-AC-SSL-YYYY=), required for ASA Releases 8.0(3) or later.
- AnyConnect Mobile license (L-ASA-AC-M-55XX=).

The XX in the license code represents the last two digits of your ASA model number. The YYYY represents the number of simultaneous users.

These licenses are mutually exclusive per ASA, but you can configure a mixed network. The AnyConnect Essentials and AnyConnect Mobile licenses are nominally priced. 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, please 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, please 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 latest Cisco ASA 5500 Series Configuration Guide.

ASA Configuration Options

ASAs running Release 8.2(5+) and 8.4(2) feature AnyConnect Identification Extensions (ACIDEx) for mobile device detection. ACIDEx lets you accept or restrict mobile connections without Cisco Secure Desktop, so you can use it to grant access to mobile users without activating an AnyConnect Premium license. Earlier releases require both Cisco Secure Desktop and an AnyConnect Premium license (Table 2).

Table 2 AnyConnect Requirements for ASA Releases

Requirements	ASA Release 8.2(5+)and 8.4(2) and later[1]	ASA Releases 8.0(4) – 8.2(4), and 8.4(1)
Cisco Secure Desktop enabled?	Not required	Yes
Licenses required	AnyConnect Essentials or AnyConnect Premium AnyConnect Mobile	AnyConnect Premium AnyConnect Mobile
Dynamic access policy (DAP) endpoint configuration	Open ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies** > **Add** or **Edit** > **Add** to the right of the Endpoint Attributes table, change the Endpoint Attribute Type to **AnyConnect**, and change the Platform to **Android**. ASDM displays a drop-down list next to Device Type that shows the supported Samsung families; however, the drop-down options are not supported. Enter the Samsung model name into the Device Type field. Add one endpoint attribute to a DAP for each Samsung device to assign a policy to it. Use the tabs in the Access/Authorization Policy Attributes section of the Add or Edit Dynamic Access Policy window to continue, terminate, or impose restrictions on Android connections.	Open ASDM and choose **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies** > **Add** or **Edit**, click **Advanced**, and enter the following line into the Logical Expressions box to grant, restrict, or deny access to Android connections: `EVAL(endpoint.os.version, "EQ", "Android", "string")` Use the tabs in the Access/Authorization Policy Attributes section of the Add or Edit Dynamic Access Policy window to continue, terminate, or impose restrictions on Android connections. **Note**: The Android user sees the message entered in the message box on the Action tab of the ASDM Add or Edit Dynamic Access Policy window only if the regular expression fails to match.

[1] If you already have AnyConnect Premium and Cisco Secure Desktop, and the ASA is running 8.0(4) or later, you have the option to add the logical expression shown in the third column.

AnyConnect for Android Feature Matrix

Table 3 lists the AnyConnect features and whether Android supports them.

Table 3 AnyConnect Features

AnyConnect Feature	Sub Feature	Android	Introduced for Android in AnyConnect version
Tunneling	TLS/DTLS	Yes	2.4.7030
	IKEv2 - NAT-T	No	
	IKEv2 - raw ESP	No	
	Suite B support	No	
	TLS compression	Yes	2.4.7030
	Dead peer detection	Yes	2.4.7030
	Tunnel keepalive	Yes	2.4.7030
Tunnel Establishment	Auto headend selection	No	
	VPN load balancing	Yes	2.4.7030
	Backup server list	Yes	2.4.7030

Table 3 AnyConnect Features

AnyConnect Feature	Sub Feature	Android	Introduced for Android in AnyConnect version
Tunnel Policy	All/full tunnel	Yes	2.4.7030
	Split tunnel (split include)	Yes	2.4.7030
	Local LAN (split exclude)	Yes	2.4.7030
	Always-on enforcement	No	
	Auto-reconnect	Yes	
	VPN on-demand (triggered by destination)	No	
	VPN on-demand (triggered by application)	No	
	Trusted network detection	No	
	Rekey	Yes	2.4.7030
	ASA group profile support	Yes, limited	2.4.7030
	IPv4 public transport	Yes	2.4.7030
	IPv6 public transport	No	
	IPv4 over IPv4 tunnel	Yes	
	IPv6 over IPv4 tunnel	Yes	2.4.7070
	Default Domain	Yes	2.4.7030
	DNS server configuration	Yes	2.4.7030
	Private-side proxy support	No	
	Pre-login banner	Yes	2.4.7030
	Post-login banner	Yes	2.4.7030
	Scripting	No	
Tunnel Security	Network change monitoring	Yes, limited	2.4.7030
	Shim intercept/filtering	No	
	Embedded firewall rules	No	

Table 3 AnyConnect Features

AnyConnect Feature	Sub Feature	Android	Introduced for Android in AnyConnect version
Authentication	Manual certificate import (get certificate)	Yes	2.4.7030
	URI handler support for importing a certificate	Yes, imports the entire certificate chain (unlike AnyConnect for Apple iOS).	2.4.7030
	SCEP enrollment		2.4.7030
	Automatic certificate selection	Yes	2.4.7030
	Non-exportable certificate	N/A	
	Smart card support	No	
	Username and password	Yes	2.4.7030
	Tokens/challenge	Yes	2.4.7030
	Double authentication	Yes	2.4.7030
	Group selection	Yes	2.4.7030
	Certificate Prefill	Yes	2.4.7030
	Save password	No	2.4.7030
User interface	Standalone GUI	Yes	2.4.7030
	Native OS GUI	No	
	CLI	No	
	API	Yes, Java not C++	2.4.7030
	User preferences	No	
	UI customization	Yes (themes)	2.4.7030
	UI Localization	No	
Deployment	WebLaunch (browser-initiated)	No	
	Web redirect to application store	No	
	Standalone installer	No	
	Preinstalled by OEM	No	
	Install or Upgrade from the ASA	No	
	Install or upgrade from Android Market	Yes	2.4.7030

Table 3 AnyConnect Features

AnyConnect Feature	Sub Feature	Android	Introduced for Android in AnyConnect version
Posture Assessment	Device check (pin lock, encryption, etc)	No	
	Running or installed apps	No	
	Serial number or unique ID check	No	
	ACIDEx	Yes, with the DAP attribute endpoint.anyconnect.deviceuniqueid	2.4.7030
Troubleshooting	Statistics	Yes	2.4.7030
	Logging	Yes, email logs supported	2.4.7030
	DART	No, but diagnostics available	
Certifications	FIPS 140-2 Level 1	No	
	Common criteria	No	

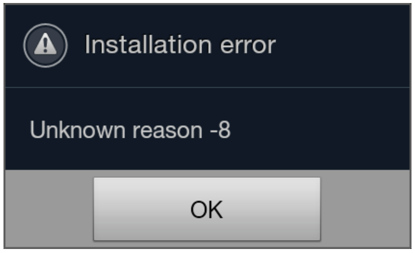
Known Issues and Bugs

The following sections describe the known limitations and caveats in the AnyConnect 2.4.7x releases.

Known Issues and Bugs in AnyConnect 2.4.7073

- If users attempt to install AnyConnect on devices that are not supported, they receive a pop-up message saying, “Installation Error: Unknown reason -8”. This message is generated by the Android OS. Figure 1 shows the installation error message.

Figure 1 Android Installation Error



Installation error

Unknown reason -8

- When the user has an AnyConnect widget on their home screen, the AnyConnect services will be automatically started (but not connected) regardless of the “Launch at startup” preference.

Fixed Issues and Bugs in AnyConnect 2.4.7073

This issue, present in AnyConnect 2.4.7030, was resolved:

> If a VPN connection is established over Wi-Fi and DHCP renews the IP address of the device, its media connection to the LAN breaks, but the control connection does not. To recover, disable and re-enable WiFi.

Known Issues and Bugs in AnyConnect 2.4.7030

- AnyConnect for Android requires UTF-8 character encoding for extended ASCII characters when using pre-fill from client certificates. The client certificate must be in UTF-8 if you want to use prefill, per the instructions in KB-890772 and KB-888180.
- AnyConnect blocks voice calls if it is sending or receiving VPN traffic over an EDGE connection per the inherent nature of EDGE and other early radio technology.
- If a VPN connection is established over Wi-Fi and DHCP renews the IP address of the device, its media connection to the LAN breaks, but the control connection does not. To recover, disable and re-enable WiFi.
- Some known file compression utilities do not successfully decompress log bundles packaged with the use of the AnyConnect Send Log button. As a workaround, use the native utilities on Windows and Mac OS X to decompress AnyConnect log files.
- The following message is shown on Samsung devices upon the initial installation of AnyConnect:

  ```
  An active VPN connection may block phone services like Visual Vociemail and Multimedia
  Message Service (MMS) from functioning properly.
  ```

Limitations of the AnyConnect Secure Mobility Client for Android

This release of AnyConnect for Android supports only the features that are strictly related to remote access. It supports connection entries that the user adds and connection entries populated by an AnyConnect profile pushed by an ASA. The Android device supports no more than one AnyConnect profile. However, a profile can consist of multiple connection entries.

AnyConnect retains only the connection entries the user added and those populated by the most recent AnyConnect profile pushed by an ASA. For example, if a user goes to vpn.example1.com and then goes to vpn.example2.com, the configuration profile imported from vpn.example2.com replaces the one imported from vpn.example1.com.

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

The ASA does not provide distributions and updates for AnyConnect for Android. They are available only on Android Market.

This release does not support the ability to hide the AnyConnect icon displayed in the status bar while AnyConnect is disconnected.

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.

Alternatively, you can use the URI handler feature to embed the connection entry into a link in an email to be sent to the user or on a website to be accessed to the user.

AnyConnect Client Profiles

An AnyConnect client user profile is an XML file that lets you identify a list of ASAs that you want to make accessible. In addition, a profile conveys additional connection attributes and constraints on a user. Users cannot modify the description and service address of an AnyConnect connection entry obtained from a profile. They cannot delete individual connection entries obtained from a profile; however, they can delete all AnyConnect data, including the profile. They can modify and delete connection entries added with a URI handler **create** or **connect** action.

You can use the AnyConnect Profile editor to configure the client features within the profile; then configure the ASA to push this file when Android establishes a VPN connection.

By default, AnyConnect sends all network traffic over the VPN connection. You can enable a split tunneling policy to control traffic flow, directing traffic appropriate for the tunnel (called split include) or traffic appropriate for the data network (called split exclude). For instructions, refer to the Cisco ASA Configuration Guide associated with the version running on the ASA.

Recommended ASA Configurations

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

For AAA-based authentication tunnel groups for mobile devices, the tunnel group should have a very long idle-timeout, such as 24 hours, to let the client remain in a reconnecting state without requiring the user to re-authenticate.

Using the URI Handler to Automate AnyConnect Actions

The URI handler lets applications pass action requests in the form of Universal Resource Identifiers (URIs) to AnyConnect. You can use URIs to generate VPN connection entries, import a certificate chain, establish a connection to a VPN, or disconnect.

To simplify the AnyConnect user setup process, you can embed the URIs as links on webpages or email messages and give users instructions to access them.

Note You must use URL encoding when entering URI handler parameter values. Use a tool such as the one in this link to encode an action request.

Note You cannot insert these URIs into your Android's Web browser because Android does not allow you to. You either need to access these URIs from a remote web server or, depending on your email client, you may be able to click on it as a link in email.

As a security measure, AnyConnect prompts the user whenever an application uses the URI handler to pass an action it supports. Please inform users how to respond to the prompts if you set up URI handling. The actions and associated prompts are as follows:

- Create—`Another application has requested that AnyConnect create a new connection to` *`host`*`. Do you want to allow this? [Yes | No]`
- Import—`Another application has requested that AnyConnect import a certificate bundle to the AnyConnect certificate store. Do you want to allow this? [Yes | No]`
- Connect—`Another application has requested that AnyConnect connect to` *`host`*`. Do you want to allow this? [Yes | No]`
- Disconnect—`Another application has requested that AnyConnect disconnect the current connection. Do you want to allow this? [Yes | No]`

The following sections show the syntax, examples, and parameter descriptions of the supported actions.

Using the URI Handler to Generate a VPN Connection Entry

Use the AnyConnect URI handler **create** action to simplify the generation of an AnyConnect connection entry for users.

Insert a separate link for each connection entry you want to add to the device. We do not support multiple create actions in a single link.

Use the following syntax to insert the create action to add an AnyConnect connection entry to the endpoint configuration:

```
anyconnect:[//]create[/]?name=Description&host=ServerAddress[&Parameter1=Value&Parameter2=
Value...]
```

Examples:

```
anyconnect:create?name=SimpleExample&host=vpn.example.com

anyconnect:create?name=Example with
certificate&host=vpn.example.com&usecert=true&certcommonname=example-ID
```

The slashes before and after **create** are optional. The create action requires that you specify the `name` or `host`. All parameters are also optional.

Note You must use URL encoding when entering URI handler parameter values. Use a tool such as the one in this link to encode an action request.

Enter the parameter values, as follows:

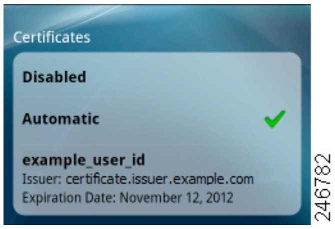
- **name**—Specifies a unique name for the connection entry to appear in the connection list of the AnyConnect home window and the Description field of the AnyConnect connection entry. AnyConnect responds only if the name is unique. The letters are case-sensitive.

- **host**—Identifies the domain name, IP address, or Group URL of the ASA with which to connect. AnyConnect inserts the value of this parameter into the Server Address field of the AnyConnect connection entry. For example,

  ```
  vpn.example.com
  ```

- **usecert** (optional)—Determines whether to use a digital certificate preinstalled on the device when establishing a VPN connection to the `host`. The valid values are:
  - true (default setting)—Enables automatic certificate selection when establishing a VPN connection with the `host`. Turning **usecert** to true without specifying a **certcommonname** value sets the Certificates field to Automatic.
  - false (default)—Disables automatic certificate selection.
- **certcommonname** (optional, but valid only if **usecert** is set to its default value, true)—Matches the Common Name of a valid certificate pre-installed on the device. To view this value on a certificate installed on the device, long-press the VPN connection entry, tap **Edit connection**, then tap **Certificate**. AnyConnect displays the value in bold in the first line of the certificate associated with the issuer. The common name in the following example is `example_user_id`.

Figure 2 Select Certificate Window



Certificates

Disabled

Automatic ✓

example_user_id
Issuer: certificate.issuer.example.com
Expiration Date: November 12, 2012

You might need to scroll to view the certificate required by the `host`.

Using the URI Handler to Import Certificates

Use the following syntax to import a certificate chain into AnyConnect, and add the import action to an email or a webpage to be displayed to the user:

anyconnect:[**//**]**import**[**/**]**?type=pkcs12&uri=**[**file**|**http**|**https**|**ftp**]**:**[**//**]**=***address*

The slashes before and after **import** are optional.

Note You must use URL encoding when entering URI handler parameter values. Use a tool such as the one in this link to encode an action request.

Examples:

In the following example, 10.0.0.10 is the FTP server:

`ftp:user:password@10.0.0.10/certificate.p12`:

In the following example, the URI translates to **file:///sdcard/certificate.p12**:

`File:anyconnect:import?type=pkcs12&uri=file%3A%2F%2F%2Fsdcard%2Fcertificate.p12`

address is the source address of the certificate or certificate chain. It is case-sensitive.

Using the URI Handler to Establish a VPN Connection

Use either syntax expression to insert the connect action into an email or webpage to be displayed to the user:

```
anyconnect:[//]connect[/]?[name=Description|host=ServerAddress]
anyconnect:[//]connect[/]?name=Description&host=ServerAddress
```

Examples:

```
anyconnect:connect?host=hr.example.com
anyconnect:connect?name=Example&host=hr.example.com
```

The slashes before and after **connect** are optional.

Note You must use URL encoding when entering URI handler parameter values. Use a tool such as the one in this link to encode an action request.

All parameters are optional. AnyConnect applies both the **create** and **connect** actions if you specify the `name` and `host`. AnyConnect attempts to establish a VPN connection to the host named at the top of the AnyConnect home window if the **connect** action does not specify the `name` or `host`.

Enter the parameter values, as follows:

- **name**—Name of the connection entry as it appears in the connection list of the AnyConnect home window. AnyConnect evaluates this value against the Description field of the AnyConnect connection entries, also called `name` if you used the previous instructions to generate the connection entry on the Android device. The letters are case-sensitive.
- **host**—Enter the domain name, IP address, or Group URL of the ASA to match the Server Address field of an AnyConnect connection entry.

Using the URI Handler to Disconnect from a VPN

Use the following syntax to insert the disconnect action:

```
anyconnect:[//]disconnect[/]
```

Example:

```
anyconnect:disconnect
```

The slashes are optional. The disconnect action takes no parameters.

Disabling or Minimizing the Impact of Keepalive Messages

We recommend increasing the keepalive update interval or disabling keepalive messages to conserve the battery life of mobile devices. To access the Keepalive Messages parameter, use ASDM to go to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies** > **Add** or **Edit** > **Advanced** > **AnyConnect Client**.

We also recommend that you enable client-side dead-peer detection to let AnyConnect determine when the quality of the transmission media is too low or unavailable to continue sending traffic over the VPN connection.

Troubleshooting

Please follow the user troubleshooting instructions in the latest Cisco AnyConnect Administrator Guide. If following those instructions does not resolve the issue, try the following suggestions:

- Ensure the AnyConnect Mobile license is installed on the ASAs. See License Options on page 3 for more information.
- Determine whether the same problem occurs with the desktop client.
- Determine whether the same problem occurs with another supported mobile OS.
- If the VPN connection is not restored after the device wakes up, ensure that Auto-Reconnect is enabled in the profile.
- If certificate authentication fails, ensure the correct certificate has been selected. Ensure that the client certificate on the device has Client Authentication as an Extended Key Usage. Ensure the certificate matching rules in the AnyConnect profile are not filtering out the user's selected certificate. Even if a user selected a certificate, it will not be used for authentication if it does not match the filtering rules in the profile. If your authentication mechanism uses any associated accounting policy to an ASA, verify that the user can successfully authenticate. If problems persist, enable logging on the client and enable debug logging on the ASA.
- If you see an authentication screen when you are expecting to use certificate-only authentication, configure the connection to use a group URL and ensure that secondary authentication is not configured for the tunnel group. For details, refer to the Cisco ASA Configuration Guide associated with the version running on the ASA.

AnyConnect Support Policy

Cisco supports all AnyConnect software versions downloaded from the Android Market; however, fixes and enhancements are provided only in the most recently released version.

Licensing

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

For our open source licensing acknowledgements, see *Open Source Used in Cisco AnyConnect Secure Mobility Client, Release 2.4 for Android*.

For the end-user license agreement, see *End User License Agreement*.

Related Documentation

For more information, refer to the following documentation:

- Cisco AnyConnect Administrator Guides
- *User Guide for Cisco AnyConnect Secure Mobility Client, Release 2.4 for Android*
- *Cisco AnyConnect Secure Mobility Client Release Notes*
- *Release Notes for Cisco AnyConnect VPN Client Release 2.4*
- *Navigating the Cisco ASA 5500 Series Documentation*

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.