AnyConnect VPN Client FAQ

Document ID: 107391

Questions

Introduction
Installation
Software Upgrade
Licensing
Supported Devices
Supported Software
Log Messages
Datagram Transport Layer Security (DTLS)
Supported features
Error Messages
Related Information

Introduction

This document provides answers to the most frequently asked questions (FAQs) related to the Cisco AnyConnect VPN Client.

The Cisco AnyConnect VPN Client provides remote users with secure VPN connections to the Cisco ASA 5500 Series Adaptive Security Appliance using the Secure Socket Layer (SSL) protocol and the Datagram TLS (DTLS) protocol. AnyConnect provides remote end users with the benefits of a Cisco SSL VPN client, and supports applications and functions unavailable to a clientless, browser−based SSL VPN connection.

Note: The target audience for this document is a network administrator who understands CLI commands and features and has experience with the configuration of AnyConnect VPN Client.

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Installation

Q. What level of rights is required for the AnyConnect VPN Client?

A. For the first installation, you need administrative privileges. However, subsequent upgrades do not require the admin level privilege.

Q. Is a reboot required after AnyConnect is installed or upgraded ?

A. No. Unlike the IPSec VPN Client, a reboot is not required after an AnyConnect installation or upgrade.

Note: This applies to the VPN module only.

Software Upgrade

Q. Is it possible to turn off the automatic AnyConnect upgrade via ASA?

A. Yes. Use one of these methods in order to turn off the automatic AnyConnect upgrade via the ASA:

- Adjust the profile on the ASA to disable updates.

```
<AutoUpdate UserControllable="false">false</AutoUpdate>
```

- Use a local policy to disable the AnyConnect downloader.

```
BypassDownloader
 true
 The client does not check for any dynamic content present on the ASA,
     including profile updates, translations, customization, optional
     modules, and core software updates.
```

<BypassDownloader>true</BypassDownloader>

Refer to AnyConnect Local Policy File Parameters and Values for more information.

Q. How can I download the AnyConnect VPN Client software?

A. The Cisco AnyConnect VPN Client software can be downloaded from the Software Downloads location.

Licensing

Q. How can I receive the AnyConnect Mobile license for the ASA?

A. The Mobile license is a fixed license on top of the existing number of licensed Secure Socket Layer (SSL) users. It can be used either with a Premium SSL VPN license or an AnyConnect Essentials license. To order the AnyConnect Mobile license for an existing unit with an SSL license, the part number is L−ASA−AC−M−55XX= (XX=05,10,20,40,50,80 depending on the model). This Mobile license can also be added as an option for new device purchases (ASA−AC−M−55XX). To order the AnyConnect Mobile license for an existing unit, contact your Cisco reseller. For an evaluation license for devices that have Essentials or Premium licenses, refer to Product License Registration for AnyConnect Mobile (registered customers only) . If you have specific questions on Mobile license requirements, send an e−mail to ac−mobile−license−request@cisco.com.

Supported Devices

Q. Is AnyConnect supported on the Cisco VPN 3000 Concentrator?

A. No.

Q. Is AnyConnect VPN Client supported on PIX Security Appliances?

A. No. AnyConnect VPN Client is not supported on PIX.

Q. Is AnyConnect supported on Cisco IOS® devices?

A. Yes.

As of Cisco IOS Software Release 12.4(15)T in browser−initiated mode only as per the Release 12.4T New Security Features Notes.

As of Cisco IOS Software Release 12.4(20)T, standalone mode is also supported.

For more information, refer to SSL VPN Remote User Guide.

Notes:

- Support for DTLS is introduced from Cisco IOS version 15.1(2)T. Refer to the **svc dtls** command for more information.
- Client keepalives are not supported on Cisco IOS devices until the 12.4(20)T release.
- Updates to the hardware crypto that can cause disconnects have been resolved with 12.4(T2) for 87x platforms.
- Start Before Logon is currently not supported by Cisco IOS.

Q. Is AnyConnect VPN Client supported on the Apple iPad or iPhone?

A. Yes. The Anyconnect VPN Client supports Apple iOS from version 2.4. Currently, iPhone 3G, iPhone 3GS, iPhone 4, and iPod Touch (second generation and later) are the supported devices. Support for iPad is expected to be available with the release of Apple iOS 4.2. For more information, refer to the Release notes of Cisco Anyconnect 2.4 for Apple iOS. For configuration related information, please refer to User guide of Cisco Anyconnect 2.4 for Apple iOS.

Q. Is it possible to connect the iPad, iPod, or iPhone AnyConnect VPN Client to a Cisco IOS router?

A. No. It is not possible to connect the iPad, iPod, or iPhone AnyConnect VPN Client to a Cisco IOS router. AnyConnect on iPad/iPhone can connect only to an ASA that runs version 8.0(3).1 or later. Cisco IOS is not supported by the AnyConnect VPN Client for Apple iOS. For more information, refer to the Security Appliances and Software Supported section of the *Release Notes for Cisco AnyConnect Secure Mobility Client 2.4, Apple iOS 4.2 and 4.3*.

Q. VPN session failover (SSL) is possible with dual Internet Service Providers (ISPs) without breaking the session. For example, if a customer is communicating through SSL VPN through ISP 1 and if ISP 1 goes down, will this take over the connection through ISP 2 without losing any packet (VPN session)? Is this possible with any Cisco device?

A. If you mean dual−ISP on the head end, this is not possible. However, if you are talking about something like dual ISP at a remote location, SSL VPN will be able to resume a lost connection. AnyConnect will attempt to reconnect if the connection is disrupted. This is not configurable, but automatic. As long as the session on the ASA is still valid, if AnyConnect can re−establish the physical connection, the session will be resumed.

Supported Software

Q. What are the supported MAC OS versions?

A. Cisco AnyConnect VPN Client releases from 2.0 to 3.0 support Mac OS X versions 10.4 and later.

Cisco AnyConnect VPN Client Release 3.0 supports these versions of Mac OS:

- Mac OS 10.5 (Intel CPU only)
- Mac OS 10.6.x (32−bit and 64−bit)
- Mac OS X 10.7 (Lion)

For support information for other AnyConnect clients, refer to the Release Notes for Cisco AnyConnect Secure Mobility Client.

Note: In the *Requirements* section of the release notes, you can verify the minimum system requirements to run AnyConnect client on each of these platforms.

Q. Does AnyConnect require Java and permissions?

A. The AnyConnect VPN Client requires either ActiveX or Java to use the web−based connection/install. For ActiveX, the user needs to have permission to install into their web browser (or it can be pre−installed). If ActiveX is not supported or used, Java is attempted. The version can be 1.4.x or 1.5. The Java implementation is an applet and is browser−based (no download).

On the first connection, the ActiveX/Java is used to install the AnyConnect VPN Client software. This initial connection requires admin rights. Subsequent connections do not require admin rights (even for client upgrades). The client has a standalone installer for cases where admin privileges are not granted to the user.

Q. What are the supported Windows OS versions?

A. The AnyConnect client provides support for remote end users that run Microsoft Vista, Windows 7, Windows XP, and Windows 2000.

Cisco AnyConnect VPN Client release 3.0 supports these versions of the Windows operating system:

- Windows 7 x86 (32−bit) and x64 (64−bit)
- Windows Vista SP2 x86 (32−bit) and x64 (64−bit)
- Windows XP SP3 x86 (32−bit)

For support information for other AnyConnect clients, refer to the Release Notes for Cisco AnyConnect Secure Mobility Client.

Note: In the *Requirements* section of the release notes, you can verify the minimum system requirements to run AnyConnect client on each of these platforms.

Q. What are the supported Linux OS versions ?

A. Cisco AnyConnect VPN client supports a wide variety of Linux distributions, such as Red Hat Enterprise Linux, Fedora Core, OpenSuse, Slackware and Ubuntu.

Cisco AnyConnect VPN Client release 3.0 supports these versions of the Linux operating system:

- Red Hat Enterprise Linux 5 Desktop
- Red Hat Enterprise Linux 6 Desktop
- Ubuntu 9.x and 10.x

For support information for other AnyConnect clients, refer to the Release Notes for Cisco AnyConnect Secure Mobility Client.

Q. Does AnyConnect support Windows Mobile devices? What are the supported versions?

A. AnyConnect is compatible with Windows Mobile 5.0, 6.0 and 6.1. Support has been introduced from version 2.3 up to version 2.5. The latest AnyConnect client 3.0 does not offer support for Windows Mobile devices.

Refer to the Windows Mobile section of the *Release Notes for Cisco AnyConnect Secure Mobility Client, Release 2.5* for a complete list all supported Windows mobile devices by the AnyConnect Client Version 2.5.

For complete details on the installation procedure, refer to Installing AnyConnect on a Windows Mobile Device.

Q. Does AnyConnect support the new Symbian software?

A. Yes. A separate AnyConnect client for Symbian is launched with version 2.4.5. For information on how to install the client, refer to the Symbian User Guide for Cisco AnyConnect Secure Mobility Client, Release 2.4.5. For support information, refer to the Release Notes for Cisco AnyConnect Secure Mobility Client 2.4 for Symbian.

Q. Is AnyConnect VPN Client supported on the Google Chrome browser?

A. Yes. It is supported in AnyConnect version 3.0. Refer to AnyConnect 3.0 Computer OSs Supported for complete details.

Q. Does Anyconnect VPN Client support the Android operating system?

A. Yes. Cisco AnyConnect Secure Mobility Client 2.4 for Android supports Android devices. Refer to these documents for more information:

- Release Notes for Cisco AnyConnect Secure Mobility Client 2.4 for Android
- User Guide for Cisco AnyConnect Secure Mobility Client, Release 2.4 for Android

Q. What are the compatibility details for the different versions of AnyConnect and ASA ?

A. Refer to ASA, ASDM, Cisco Secure Desktop, and AnyConnect Compatibility for information on compatibility.

Q. Is there a compatibility matrix that shows all the supported AnyConnect features with regard to different operating systems?

A. Yes. Refer to AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 2.5 for more information. This document also describes the feature support in regards to the different available licenses.

Q. Has Secure Socket Layer (SSL) VPN (AnyConnect/Clientless) been validated on Novell Linux Desktop Thin Client Edition?

A. Cisco does not test with this edition of Linux. The best bet is to make sure you meet the prerequisites defined in the release notes. Then, give it a try, assuming you are asking about AnyConnect. This would not be officially qualified, but if the system meets the prerequisites it might work fine. Asking about Clientless SSL VPN should work fine, because you generally just need the browser.

Log Messages

Q. Where are the AnyConnect installation logs stored on Linux operating systems?

A. On the Linux operating system, these logs are stored in **/opt/cisco/vpn**.

Q. Where are the Windows AnyConnect installation logs stored on Windows operating systems?

A. There are two possible locations for the installation logs on Windows operating systems:

- If it is a fresh install, the installation logs will be in the user's Temp directory. In order to locate this directory, complete these steps based on your operating system:
  - Windows XP and Windows 2000: Go to **Start > Run**, enter **%TEMP%**, and click **OK**.
  - Windows Vista: Enter **%TEMP%** in the search window, and press **Enter.**
- If it is an upgrade, the installation logs will be located in the system's temp directory which is typically *%SYSTEMDRIVE%\temp* or *%SYSTEMROOT%\temp*; however, the logs might be located elsewhere.

  The file name uses a convention similar to *WinSetup−Release−2.0install−21333219012007.log*.

Datagram Transport Layer Security (DTLS)

Q. What is the difference between the SSL−Tunnel and DTLS−Tunnel? What type of traffic goes through each?

A. The SSL−Tunnel is the TCP tunnel that is first created to the ASA. When it is fully established, the client will then try to negotiate a UDP DTLS−Tunnel. While the DTLS−Tunnel is being established, data can pass over the SSL−Tunnel. When the DTLS−Tunnel is fully established, all data now moves to the DTLS−tunnel and the

SSL−tunnel is only used for occasional control channel traffic. If something should happen to UDP, the DTLS−Tunnel will be torn down and all data will pass through the SSL−Tunnel again.

The decision of how to send the data is very dynamic. As each network bound data packet is processed there is a point in the code where the decision is made to use either the SSL connection or the DTLS connection. If the DTLS connection is healthy at that moment, the packet is sent via the DTLS connection. Otherwise it is sent via the SSL connection.

The SSL connection is established first and data is passed over this connection while attempting to establish a DTLS connection. Once the DTLS connection has been established, the decision point in the code described above just starts sending the packets via the DTLS connection instead of the SSL connection. Control packets, on the other hand, always go over the SSL connection.

The key point is if the connection is considered healthy. If DTLS, an unreliable protocol, is in use and the DTLS connection has gone bad for whatever reason, the client does not know this until Dead Peer Detection (DPD) occurs. Therefore, data will be lost over the DTLS connection during that short period of time because the connection is still considered healthy. Once DPD occurs, data will immediately be set via the SSL connection and a DTLS reconnect will happen.

The ASA will send data over the last connection it received data on. Therefore, if the client has determined that the DTLS connection is not healthy, and starts sending data over the SSL connection, the ASA will reply on the SSL connection. The ASA will resume use of the DTLS connection when data is received on the DTLS connection.

Q. On what platforms is Datagram Transport Layer Security (DTLS) supported?

A. DTLS is supported on Windows 2000, Windows XP, Windows Vista, Mac OS, and Linux operating systems.

Q. Does DTLS support both 32−bit and 64−bit platforms?

A. Yes.

Q. Do both tunnels (SSL and DTLS), have to Idle Timeout for the session to be disconnected?

A. When a DTLS−Tunnel is active, that is the only tunnel where idle timeout matters. Because very little control channel traffic passes over the SSL−Tunnel, it is almost always idle so it is exempt while there is an active DTLS−Tunnel. If something happened to UDP and the DTLS−Tunnel was torn down, then idle timeout would apply to the SSL−Tunnel.

Unfortunately with most Windows computers, they are never truly "idle" so many people think idle timeout is not working. There has been discussion about making a "data threshold" value for idle timeout, but even that could be tricky. In order to make a Windows computer truly idle, you have to remove Microsoft Networking and File and Print Sharing from the Network Config for the computer's physical interface.

Q. AnyConnect connects through a proxy server and DTLS is not used. Why?

A. The AnyConnect SSL VPN Client can use a configured proxy server in your browser (Internet Explorer only). However, when it connects, it does not negotiate a Datagram Transport Layer Security (DTLS) User Datagram Protocol (UDP) tunnel. Only TLS TCP is used when you connect this way because the proxy server configuration is not configurable to proxy UDP packets used by DTLS.

Q. When I use Datagram Transport Layer Security (DTLS) on AnyConnect VPN tunnel, I cannot download large files and have connectivity issues. How can I resolve this issue?

A. Make sure that the UDP port is not blocked as this port is used by DTLS. Also, check if DTLS is not blocked or dropped by ISP. Enable DTLS on the interface that you are connecting to from the AnyConnect. For more information on enabling DTLS, refer to Enabling Datagram Transport Layer Security (DTLS) with AnyConnect (SSL) Connections.

Supported features

Q. Is it possible to save the password credentials on AnyConnect so that it will not request authentication from the user (password storage feature)?

A. No, it is not possible to save the password credentials on AnyConnect.

Q. Is the launching a dialer feature available on the AnyConnect VPN Client?

A. No. Dialer and third−party application launchers are not supported for AnyConnect Start Before Logon (SBL).

Q. What are the requirements for AnyConnect and SSL versions?

A. AnyConnect requires that the ASA be configured to accept TLSv1 traffic and that the browser settings be set for TLSV1.0.

The AnyConnect VPN Client cannot establish a connection with these ASA settings for SSL server−version:

- SSL server−version sslv3
- SSL server−version sslv3−only (CSCsh76698)

Q. Is there a method by which we can automatically map the network drives when the users connect via VPN and disconnect them once the user disconnects VPN?

A. Yes. You must write a script in order to achieve this. Refer to Writing and Deploying Scripts for more information.

Q. Can the AnyConnect VPN Client work through an IPSec VPN Client tunnel?

A. This is not officially supported. The reason it cannot work is because both the IPSec VPN Client and the AnyConnect VPN Client are trying to route traffic to their virtual adapters. The IPSec VPN Client is intercepting AnyConnect traffic at the instant messaging (IM) layer.

However, it has been retested and appears that it might work with some caveats.

Q. Can AnyConnect (or Clientless SSL VPN) users initiate password−management changes from the AnyConnect VPN Client itself?

A. No. AnyConnect does not have any option inside of it to trigger or initiate a password change.

Password changes are only triggered from the head−end when required as part of MSCHAPv2 RADIUS with expiry or Lightweight Directory Access Protocol (LDAP) password expiration. Customers can change their Active Directory (AD) password using the same Ctrl−Alt−Delete mechanism assuming they are logging in to the network (Start Before Login).

Q. Does AnyConnect support a pool with a single address? If you want the ASA to do Port Address Translation (PAT), such that all the remote clients appear on the inside network as a single address, differentiated by source TCP port number?

A. AnyConnect requires a unique IP address for each client. Thus, the PAT pool does not apply with AnyConnect in this context. Certainly, going through a device which does PAT (such as home) is not an issue with AnyConnect.

Q. Is there a way to allow for a user to select the authentication certificate?

A. Yes. You must set the `<AutomaticCertSelection>` element to *false* in the client profile.

Here is an example:

```
<AnyConnectProfile>
        <ClientInitialization>
                <AutomaticCertSelection>false</AutomaticCertSelection>
        </ClientInitialization>
</AnyConnectProfile>
```

For more information, refer to Automatic Certificate Selection.

Q. Does SSL VPN have the facility where the user can create two tunnels at the same time and then after accessing the network, if one tunnel goes down the VPN Client can automatically shift the user to the second tunnel?

A. SSL VPN cannot have multiple tunnels at the same time and shift from one to one if one goes down.

Q. Can a DHCP server assign DNS and WINS servers to an AnyConnect VPN Client?

A. DHCP assignment only assigns the IP address to the client. Parameters such as DNS and WINS are assigned from the group−policy settings and not ascertained from DHCP.

Q. I would like to be able to process a logon script only when I connect to the corporate network. Can I run a logon script after AnyConnect establishes a VPN connection rather than running Start Before Logon (SBL), which must be run every time I start the computer (whether or not I want to VPN)?

A. AnyConnect has introduced the OnConnect script feature in version 2.4 and later. Refer to Scripting section of the *Release Notes for Cisco AnyConnect VPN Client, Release 2.4*. For complete information on scripting, refer to the Scripting section of the *Cisco AnyConnect VPN Client Administrator Guide, Release 2.4*.

Q. Will AnyConnect Start Before Logon (SBL) function with whole−disk encryption software such as Encryption Anywhere, PointSec, and PGP?

A. Yes, this is supported in version 2.2 of AnyConnect.

Q. Is there a way to support SOCKS type proxy?

A. AnyConnect is not supported with SOCKS type proxy. SOCKS is not a HTTPS proxy, so Cisco does not support SOCKS proxies.

AnyConnect will work in SSL mode via "HTTPS" proxies (specifically HTTPS 1.1). Additionally, authenticating proxies that use Basic or NTLM for authorization can also be used.

You must enable **use https 1.1 for proxies** in the advanced Internet Explorer settings.

Q. How do I prompt remote users to download the client?

A. You can enable the security appliance to prompt remote SSL VPN Client users to download the client with the **svc ask** command from group policy webvpn or username webvpn configuration modes:

```
svc ask {none | enable [default {webvpn | svc} timeout value]}
```

The **svc ask enable** command prompts the remote user to download the client or go to the portal page for a clientless connection and waits indefinitely for user response.

- **svc ask enable default svc** Immediately downloads the client.
- **svc ask enable default webvpn** Immediately goes to the portal page.
- **svc ask enable default svc timeout value** Prompts the remote user to download the client or go to the portal page and waits the duration of value before taking the default

action downloading the client.

- **svc ask enable default webvpn timeout value** Prompts the remote user to download the client or go to the portal page, and waits the duration of value before taking the default action displaying the portal page.

Q. What is the AnyConnect reconnect behavior?

A. AnyConnect will attempt to reconnect if the connection is disrupted. This behavior is automatic and not configurable. As long as the session on the ASA is still valid, the session will be resumed if AnyConnect can re−establish the physical connection.

Version 2.2 includes a roaming feature that allows AnyConnect to reconnect after a PC sleep. The client will continue trying indefinitely until the head−end tells it that it cannot reconnect and the client will not immediately tear down the tunnel when the system goes in to hibernate/standby. For customers who do not want this feature, set the session timeout to a low value to prevent sleep or resume reconnects.

Q. When a reconnect occurs, does the AnyConnect Virtual Adapter (VA) flap or does the routing table change at all?

A. A low level reconnect will not do either. This is a reconnect on just SSL or DTLS. These go about 30 seconds before giving up. If DTLS fails it is just dropped. If SSL fails it causes a high level reconnect. A high level reconnect will completely redo the routing. If the client address assigned on the reconnect (or any other configuration parameters impacting the VA), are not changed, then the VA is not disabled

Q. Does AnyConnect VPN Client support two−factor authentication?

A. AnyConnect VPN Client supports two−factor authentication beginning with ASA Version 8.2(x). It is not supported in versions prior to 8.2.(x).

Q. Does AnyConnect VPN Client support other VPN clients from other vendors installed simultaneously on the same PC?

A. AnyConnect 2.5 installations can coexist with other VPN clients, including IPsec clients, on all supported endpoints; however, Cisco does not support running AnyConnect while other VPN clients are running.

Q. Does AnyConnect support Internet Connection Sharing (ICS)?

A. Internet Connection Sharing (ICS) is not compatible with AnyConnect. You must disable ICS for proper AnyConnect functionality.

When you try to launch AnyConnect on a PC on which ICS is already running, AnyConnect returns this error message:

```
The vpn client agent was unable to create the interprocess
communication depot.
```

In order to resolve this issue, disable the ICS and launch again AnyConnect.

Q. Does ASA support CSD pre−login assessment for iOS devices while connecting to AnyConnect?

A. Currently, it is not supported on ASA. Refer to enhancement request CSCtr63396 (registered customers only) for more details.

Q. How do I check if AnyConnect is connected or not from the DOS prompt on a Windows machine?

A. Complete these steps:

1. On the Windows machine, click **Start** > **Run**, type **cmd**, and click **Enter** in order to open the Command Prompt window.
2. Issue this command on the CLI:

```
C:\Program Files\Cisco\Cisco AnyConnect VPN Client> vpncli.exe state

Cisco AnyConnect VPN Client (version 2.5.0193) beta.

Copyright (c) 2004 − 2010 Cisco Systems, Inc. All Rights Reserved.

 >> state: Connected
 >> state: Connected
 >> registered with local VPN subsystem.
 >> state: Connected
 >> state: Connected
```

Q. Can the IP address assigned to the AnyConnect client be the same as the client PC's original IP address?

A. No. The ASA (by design) assigns internal IP addresses to all users. If you were to route traffic back to an end user without an assigned IP address, the ASA would need to be the default gateway for everything on the network. This would not be realistic from a network design perspective.

Q. Is AnyConnect a FIPS complaint client?

A. Yes. Starting with AnyConnect version 2.4, it is a FIPS complaint client. It requires you to purchase a FIPS license in order to go on the ASA. The license (per ASA) gives you access to the required information in order to have a FIPS compliant version of AnyConnect. Refer to FIPS and Additional Security in the New AnyConnect Local Policy for more details.

Q. Does the AnyConnect VPN Client support the split DNS functionality?

A. Yes. Starting with release 3.0.4235, AnyConnect supports true split DNS functionality for both Windows and Mac machines. Refer to Split DNS Functionality Enhancement for more details.

Q. What ports need to be opened both ways on a client in order for AnyConnect to function properly?

A. For AnyConnect 3.0, these ports need to be allowed:

```
TLS (SSL)            TCP 443
SSL Redirection      TCP 80   (optional)
DTLS                 UDP 443  (optional but HIGHLY recommended)
IPsec/IKEv2          UDP 500, UDP 4500  (and the client services port used for SSL)
Legacy IPsec IKEv1 −  ESP mode   UDP 500, Protocol 50
IPsec/NAT−T    UDP 500, UDP 4500
IPsec/TCP    TCP XXX            (admin definable)
IPsec/UDP     UDP 500, UDP XXX  (admin definable)
```

For more information, refer to Port Information for AnyConnect VPN Client.

Q. What attributes are reported by DAP when an AnyConnect client connects without CSD support and CSD is enabled on ASA?

A. When CSD is not available for an AnyConnect platform, but CSD is enabled on the ASA, AnyConnect performs a "CSD Bypass". When CSD Bypass is performed, AnyConnect reports these DAP attributes:

```
endpoint.os.version = "MacOS" | "Palm WebOS" | "Linux" | "Pocket PC" |
   "Apple Plugin" | "Unknown"
endpoint.feature = "failure"
```

The "Apple Plugin" attribute is reported for both the iPad and the iPhone. "Palm WebOS" is reported for devices running WebOS, such as the Palm Pre. "Linux" is reported for Linux desktops and embedded Linux derived clients (such as the consumer TelePresence client). "Pocket PC" is reported for Windows Mobile devices. "MacOS" is reported for Apple Mac devices. "Unknown" is reported for all other devices.

For example, a DAP trace on an iPhone client will display this information:

```
DAP_TRACE: dap_add_to_lua_tree:endpoint["application"]
   ["clienttype"]="AnyConnect"
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.feature="failure"
DAP_TRACE: dap_add_csd_data_to_lua:endpoint.os.version="Apple Plugin"
```

The DAP attribute for iOS devices may be broken in some ASA versions. As a result, if its not working, make sure that you are not running into the issue in Cisco bug ID CSCtj46900 (registered customers only) .

Q. Which of the four protection classes (Class A, B, C, or D) is used to store the AnyConnect data (such as user credentials, VPN sessions, etc) that is stored locally on Apple iOS devices?

A. The AnyConnect Client on iPhone does not store user credentials. The Digital certificates are stored in Apple s cert store and protected via Apple, not Cisco.

AnyConnect directly stores the data which is non−sensitive − Current theme, URI handler settings, and Localization Data. AnyConnect does not set any special encryption properties for this data. The other content (profiles, connect attributes, etc) are all handled via Apple VPN specific APIs. As per Apple, the configuration is stored in a .plist without any added protection (that is, Class D).

Q. Does AnyConnect on Android support the VPN load balancing feature?

A. Yes. This feature is supported from AnyConnect for Android release 2.4. For more details, refer to this Table.

Error Messages

Q. AnyConnect VPN Client installation fails with this error message: `Error 1722. There is a problem with this Windows Installer package`. How can I resolve this issue?

A. AnyConnect installation fails with this error:

```
MSI (s) (D8:70) [14:59:10:750]: Product: Cisco AnyConnect VPN Client
-- Error 1722. There is a problem with this Windows Installer package

A program run as part of the setup did not finish as expected. Contact
 your support personnel or package vendor. Action VACon_Install,
        location: C:\Program Files\Cisco\Cisco AnyConnect VPN Client\VACon.exe, comm
        -install "C:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnva.inf" VPN\
```

The 1722 error is an generic code for an MSI action failure. In this case, as revealed in the MSI log, the Virtual Adapter installer has failed. Therefore, you need to check whether this registry key is present or not: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`.

In addition, you can try one of these actions in order to resolve the issue:

- Execute this command in order to perform a quiet installation of AnyConnect:

  ```
  msiexec /quiet /norestart /i anyconnect.msi
  ```
- Scan your registry for AnyConnect related bogus keys and remove them.

Q. Users behind a Microsoft Proxy receive this error when they connect to the VPN Concentrator via the SSL VPN Client: `None of the authentication protocols offered by the proxy server are supported.` How can I resolve this issue?

A. This error message usually means that the proxy server is configured to use an authentication mechanism that is not supported by the SSL VPN Client.

AnyConnect will work in SSL mode via HTTPS proxies (specifically HTTPS 1.1). Additionally, authenticating proxies that use Basic or NT LAN Manager (NTLM) for authorization can also be used. It is recommended to use NTLM when you use the proxy server.

Internet Explorer Proxy With the AnyConnect VPN Client

If you have Internet Explorer configured with a proxy, you must activate the *Use HTTP 1.1 through proxy connections* setting to use the AnyConnect VPN Client. If this option is not set, the AnyConnect VPN Client connection does not come up.

In Internet Explorer, choose **Internet Options** from the Tools menu. Click the **Advanced** tab, and under the HTTP 1.1 Settings, check **Use HTTP 1.1 through proxy connections**.

How does this Internet Explorer setting affect AnyConnect?

AnyConnect, like SVC, uses Windows Internet (WinINet) for the pre−tunnel connection. This is the connection that is used to perform the initial authentication and downloading of updates. WinINet is the programmatic interface that Internet Explorer also uses under the covers. WinINet exposes configuration via the options menu in Internet Explorer. One of the items in this menu is to use http:1.1 over proxies.

Therefore, when the VPNDownloader connects to the headend to perform validation, it does so via WinINet APIs. This is part of the pre−tunnel operation that occurs.

The actual tunnel of data occurs over a separate channel that does not use WinINet, and it is this separate channel that only knows about *ProxyIP:ProxyTCPPort*.

In short, think of the AnyConnect GUI/VPNDownloader and the browser launch as extensions of Internet Explorer for the purposes of negotiating the tunnel connection. However, all tunnel data is done via a separate channel that does not use WinINet.

Q. When I attempt to install AnyConnect VPN Client on Windows machine, I receive this error message: `Administrator privileges are required to install the VPN client`. How can I resolve this issue?

A. Try one of these workarounds in order to resolve this issue:

- Disable the client firewall, any antivirus software, and any third−party softwares running on the client machine.
- Verify the compatibility of the operating system on the client machine. Refer to the Cisco AnyConnect Secure Mobility Client Release Notes for more information.
- Verify if language customization is configured and, if it is, disable it.

  use ASDM to check the path: *Configuration > Remote Access VPN > Language Localization > Client MST Language Transforms*.
- Ensure that the `RunOnce` registry key (`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`) exists as documented in the Cisco bug ID CSCsr54507 (registered customers only) .
- Add the IP address or name of the ASA to the Trusted Site list on the web browser. For more information, refer to Cisco bug ID CSCsu54601 (registered customers only) .

Q. AnyConnect VPN Client downloads the older profiles when a new profile of the same file name is uploaded to the ASA flash. How can I resolve this issue?

A. Issue the **svc profile** command again to reload the cache (preferred). Or you can manually copy the profile from **disk0: to cache:/stc/profiles**.

Alternatively, uploading a different file name for the new profile (such as profile1.xml, profile2.xml, etc.) and mapping this new file name to the group will update AnyConnect with the new profile information on its next connection.

Q. AnyConnect VPN Client software crashes with this error message: `Cisco Anyconnect vpn client downloader has encountered a problem and needs to close`. How can I resolve this issue?

A. The error occurs due to the *biolsp.dll* driver. This is a known problem with this driver. The error is resolved by updating the driver.

Q. When I attempt to connect with AnyConnect VPN Client version 2.4, I receive this error message: `A certificate problem has been encountered. A VPN connection will not be established`. How can I resolve this issue?

A. This error occurs due to an issue documented in Cisco bug ID CSCtb73337 (registered customers only) . AnyConnect Client version 2.4 does not work with Cisco IOS headend when a certificate is used that is not trusted or there is mismatch in the host name entered in the URL to that to the CN (common name) or SAN (subject alternative name) in the Cisco IOS router certificate.

AnyConnect 2.4 fails to connect with Cisco IOS headend due to certificate verify fail error.

This issue can be resolved through one of these workarounds:

- Make sure that the router certificate is trusted (import into certificate store) and then match the CN/SAN on the certificate to that of the URL. If there is no DNS entry, then you can use a local DNS entry by updating the host file for the host name in certificate.
- Downgrade AnyConnect to a previous version: 2.3.

Q. When I connect to ASA with AnyConnect version 2.5 on my Linux machine, I receive this error: `The AnyConnect package on the secure gateway could not be located`. How can I resolve this issue?

A. Verify that you uploaded the correct AnyConnect package (for Linux) on to the ASA and specified this image in the WebVPN configuration. Use these commands to perform these tasks:

- Copy the anyconnect−linux−2.X.XXXX−k9.pkg image file:

```
hostname#copy tftp flash
```

- Specify the priority of the image to use for AnyConnect:

```
hostname(config−webvpn)#svc image anyconnect−linux−2.X.XXXX−k9.pkg 1
```

Q. I cannot connect with AnyConnect and I receive this error: `ANYConnect is not enabled on the VPN Server`. How can I resolve this issue?

A. The `ANYConnect is not enabled on the VPN Server` error message might occur due to these reasons:

- You have not loaded the package file on the ASA.
- The version of the package file on the ASA is different from the version of the MSI (AnyConnect VPN Client) used on the PC.

  For example, you might have the package for version 2.1 of AnyConnect VPN Client installed on ASA and have 2.3 MSI installed on the PC. The same versions should be used on both the ASA and the PC to avoid this issue.

Q. When I attempt to connect with AnyConnect VPN Client using Internet Explorer 7, I receive this error message: `Revocation information for the security certificate for this site is not available. Do you want to proceed?` I click the Yes radio button three times before the window goes away. Why does this error occur and how is it resolved?

A. The `Revocation information for the security certificate for this site is not available` error message is usually due to a problem with the certificate you are using, as well as the browser trying the connection. It usually means that in your certificate you have either an HTTP or LDAP CRL distribution point configured and that your browser is configured to check this, but cannot reach it.

In order to resolve this issue, verify that the *Check for server certificate revocation* option (located under **Tools > Internet Options > Advanced Tab > Check for server certificate revocation (requires restart the browser)**) is unchecked. If the option is checked, uncheck the option, and save the settings in order to resolve this issue.

Q. I am unable to connect with AnyConnect VPN Client on Windows Vista after the sleep and resume feature has been used. I receive this error message on the AnyConnect GUI: `The VPN client driver has encountered an error.` Why does this error occur and how is it resolved?

A. This issue is documented in Cisco bug ID CSCsm60339 (registered customers only) .

In order to resolve this issue, reboot the PC, and try to reconnect the tunnel. The workaround is to apply the HotFix described in KB−952876 .

Q. I received this error message: `The server certificate received or its chain does not comply with FIPS.` How can I resolve this issue?

A. You might receive the error message during a failed attempt to log in to the AnyConnect Client. Refer to Anyconnect 'The server certificate received or its chain does not comply with FIPS' for information on how to resolve this issue.

Related Information

- **Cisco AnyConnect VPN Client**
- **Cisco AnyConnect Secure Mobility Client Release Notes**
- **PIX/ASA Security Appliance FAQ**

- **Cisco Secure Desktop (CSD) FAQ**
- **Cisco ASA 5500 Series Adaptive Security Appliances**
- **Technical Support & Documentation − CiscoSystems**

Updated: Jul 26, 2011 Document ID: 107391
