

AnyConnect VPN Client FAQ

Document ID: 107391

Questions

Introduction

What level of rights is required for the AnyConnect client?

Is a reboot required after AnyConnect is installed/updated?

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

Is there a way to prevent the Adaptive Security Appliance (ASA) from automatically upgrading to a new AnyConnect version?

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

AnyConnect client will not install (Error 1722). Why?

Is "launching a dialer" missing on the AnyConnect client?

What platforms is Datagram Transport Layer Security (DTLS) supported on?

Does DTLS support both 32-bit and 64-bit platforms?

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

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

Is there a way to support SOCKS type proxy?

What are the requirements for AnyConnect and SSL versions?

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?

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

Is AnyConnect supported on the Cisco VPN 3000 Concentrator?

Is AnyConnect supported on Cisco IOS® devices?

Can the AnyConnect client work through an IPsec VPN client tunnel?

Does AnyConnect VPN Client support Mac OS?

Can AnyConnect (or Clientless SSL VPN) users "initiate"

password-management/changes from the AnyConnect client itself?

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?

Does AnyConnect have the ability to present a popup with the list of certificates, such as what is available for SSL VPN Clientless?

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, 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?

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?

Does AnyConnect require any Java and Permissions?

Does AnyConnect standalone mode require the system to have Internet Explorer (IE) installed?

Can a DHCP server assign DNS and WINS servers to an AnyConnect client?

Do both tunnels have to Idle Timeout for the session to be disconnected?

Where are the Windows AnyConnect installation logs stored?

Where are the Linux AnyConnect installation logs stored?

Can you 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), I would like to be able to process a logon script only when connecting to the corporate network.

Users behind a Microsoft Proxy receive the "None of the authentication protocols offered by the proxy server are supported." error when they connect to the VPN Concentrator via the SSL VPN Client. Why?

How do I prompt the Remote Users to download the client?

What is the AnyConnect Reconnect Behavior?

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

Will AnyConnect SBL function with whole-disk encryption software such as Encryption Anywhere, PointSec and PGP?

Does AnyConnect 2.x support both x86 (32-bit) and x64 (64-bit) Vista?

I am trying to install AnyConnect VPN client on Windows 2003 server. During installation I receive the Administrator privileges are required to install the VPN client error. Why?

AnyConnect VPN client software crashes with the "Cisco Anyconnect vpn client downloader has encountered a problem and needs to close" error message. Why?

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

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

AnyConnect client downloads the older profiles when a new profile of the same exact filename is uploaded to the ASA flash. How is this resolved?

I cannot connect with AnyConnect and I receive this error: ANYConnect is not enabled on the VPN Server. How is this resolved?

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

Related Information

Introduction

The document addresses the most frequently asked questions (FAQs) related to Cisco AnyConnect VPN Client.

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

Q. What level of rights is required for the AnyConnect 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/upgraded?

A. No. Unlike the IPsec VPN Client, a reboot is not required after the AnyConnect installation/upgrade.

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, this is not possible.

Q. Is there a way to prevent the Adaptive Security Appliance (ASA) from automatically upgrading to a new AnyConnect version?

A. No. Currently there is no way to disable automatic AnyConnect upgrades.

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 pre-requisites 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 pre-requisites it might work fine. Asking about Clientless SSL VPN should work fine, because you generally just need the browser.

Q. AnyConnect client will not install (Error 1722). Why?

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.
```

Q. Is "launching a dialer" missing on the AnyConnect client?

A. Dialer and third party application launchers are not supported for AnyConnect Start Before Logon (SBL).

Q. What platforms is Datagram Transport Layer Security (DTLS) supported on?

A. DTLS is supported on WIN2K/XP/Vista/Mac OS and Linux.

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

A. Yes.

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

A. Yes. From the ASA, configure either of these commands in order to turn off the automatic upgrade:

- ◆ `no svc ask enable`
- ◆ `svc ask enable`

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. 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 IE settings.

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 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. No. There is no automatic way for the client to perform this.

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 (IE only). However, when it connects, it does not negotiate a DTLS (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. Is AnyConnect supported on the Cisco VPN 3000 Concentrator?

A. No.

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.

Note:

- ◆ The low latency DTLS protocol is not supported by IOS at this time, so it is an SSL only TLS connection (like SVC).
- ◆ Client keepalives are not supported on 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 IOS.

Q. Can the AnyConnect client work through an IPsec VPN client tunnel?

A. This is not officially supported. The reason it cannot work is because both the IPsec client and the AnyConnect client are trying to route traffic to their virtual adapters. The IPsec client is intercepting AC traffic at the IM layer.

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

Q. Does AnyConnect VPN Client support Mac OS?

A. Yes. Cisco AnyConnect VPN Client Releases 2.0 to 2.3 support Mac OS X Versions 10.4 and later.

Cisco AnyConnect VPN Client Release 2.4 supports these versions of Mac OS:

- ◆ Mac OS X 10.5
- ◆ Mac OS X 10.6 and 10.6.1 (both 32-bit and 64-bit)

Q. Can AnyConnect (or Clientless SSL VPN) users "initiate" password-management/changes from the AnyConnect 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-del 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 linksys which does PAT (such as home) is not an issue with AnyConnect.

Q. Does AnyConnect have the ability to present a popup with the list of certificates, such as what is available for SSL VPN Clientless?

A. There is no popup asking the user for certificate selection. As an immediate solution, the administrator can specify certificate match selection criteria in the AnyConnect Profile XML file.

```
<CertificateMatch>  
<KeyUsage>  
<MatchKey>Non_Repudiation</MatchKey>  
<MatchKey>Digital_Signature</MatchKey>
```

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, 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.

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. Does AnyConnect require any Java and Permissions?

A. The AnyConnect client requires either ActiveX or Java to use the web-based connection/install. For ActiveX, the user will need 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 would be used to install the AnyConnect client software. This 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. Does AnyConnect standalone mode require the system to have Internet Explorer (IE) installed?

A. In brief testing, AnyConnect standalone mode appears to operate properly even after IE is removed from the system.

Q. Can a DHCP server assign DNS and WINS servers to an AnyConnect 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. Do both tunnels 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 PCs, 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 PC truly idle, you have to remove Microsoft Networking and File and Print Sharing from the Network Config for the PC's physical interface.

Q. Where are the Windows AnyConnect installation logs stored?

A. There are two possible locations for the install logs on Windows:

- ◆ If this is a fresh install, then it will be in the USER's temp directory. This directory can be found by entering **%TEMP%** from the Start->run menu in Windows XP or 2K (and the search window on Vista) and then clicking **ok / <enter>**.
- ◆ If this is an upgrade, then this file will be located in the SYSTEM's temp directory which is typically **%SYSTEMDRIVE%\temp** or **%SYSTEMROOT%\temp**, but might be located elsewhere.

The file has a format of WinSetup–Release–2.0install–21333219012007.log, for example.

Q. Where are the Linux AnyConnect installation logs stored?

A. These logs are stored in **/opt/cisco/vpn**.

Q. Can you 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), I would like to be able to process a logon script only when connecting to the corporate network.

A. Aside from using SBL for this, AnyConnect does not have the ability to run a logon script after connection.

Q. Users behind a Microsoft Proxy receive the "None of the authentication protocols offered by the proxy server are supported." error when they connect to the VPN Concentrator via the SSL VPN Client. Why?

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 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 client. If this option is not set, the AnyConnect 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 IE setting affect AnyConnect?

AnyConnect, like SVC, uses WinInet for the pretunnel 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 IE. 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 IE for the purposes of negotiating the tunnel connection. However, all tunnel data is done via a separate channel that does not use WinInet.

Q. How do I prompt the 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:

```
no] 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 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.

In version 2.2, there is a roaming feature that allows AnyConnect to reconnect after a PC sleep. The client will continue trying infinitely 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 happens, 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. Will AnyConnect 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. In earlier releases, there was a bug that has been resolved.

Q. Does AnyConnect 2.x support both x86 (32-bit) and x64 (64-bit) Vista?

A. Yes.

Q. I am trying to install AnyConnect VPN client on Windows 2003 server. During installation I receive the Administrator privileges are required to install the VPN client error. Why?

A. AnyConnect VPN client is not designed for Windows 2003 server. Refer to Release Notes for Cisco AnyConnect VPN Client, Release 2.2 for more information.

Q. AnyConnect VPN client software crashes with the "Cisco Anyconnect vpn client downloader has encountered a problem and needs to close" error message. Why?

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. 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 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 a 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 licensing@cisco.com.

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

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](#).

Q. AnyConnect client downloads the older profiles when a new profile of the same exact filename is uploaded to the ASA flash. How is this resolved?

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 filename for the new profile (such as profile1.xml, profile2.xml, etc.) and mapping this new filename to the group will update AnyConnect on their next connection with the new profile information.

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

A. This error message might occur due to these reasons:

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

For example, you might have the package for version 2.1 of AnyConnect Client installed on ASA and have 2.3 MSI 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 Client using Internet Explorer 7, I receive the Revocation information for the security certificate for this site is not available. Do you want to proceed? error . I click on the Yes radio button three times before the window goes away. Why does this error occur and how is this resolved?

A. This is usually a problem with the certificate you are using and 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 check if the **Check for server certificate revocation** option present 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. This resolves the issue.

Related Information

- [Cisco AnyConnect VPN Client](#)
 - [PIX/ASA : Security Appliance FAQ](#)
 - [Cisco Secure Desktop \(CSD\) FAQ](#)
 - [Cisco ASA 5500 Series Adaptive Security Appliances](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jun 11, 2008

Document ID: 107391
