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.

There is no mechanism that allows regular/limited privilege users to install AnyConnect.

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 AnyConnect weblaunch installation supported on 64-bit browsers (IE - Internet Explorer)?

A. AnyConnect installation via weblaunch is not supported on 64-bit IE browsers.

Q. Can AnyConnect co-exist with IPSec and or SSL VPN clients from other vendors on the same PC?

A. Yes. But the following general rules apply to all AnyConnect versions:

The AnyConnect client should work fine if the other vendor's products are ***disabled*** and ***don't*** do the following:

1. Install a Winsock LSP that remains active when the 3rd party software is not running.
2. Install a local http proxy that remains active when the 3rd party software is not running.
3. Installs any drivers that continue to intercept traffic when the 3rd party software is not running.

Additionally, any restrictions that are done to the MTU of the physical interface could result in performance degradation.

Q. After AnyConnect weblaunch why do we keep the browser open after AnyConnect session establishes?

A. A couple of reasons:

- A matter of convenience to allow the user continuing the use of the Clienltess portal even after the AnyConnect tunnel/session is operational.
- Current browsers implement tabbed windows, or mutiple windows from a single process, therefore the Anyconnect agent killing of the browser process causes the user to lose all tabs/windows in that process, not just the one for the Clientless portal.

Note:Currently there is no capability to allow the browser process to be killed when Anyconnect tunnel establishes. SSL VPN Client (SVC 1.x) did support this capability .

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

A. Not prior to AnyConnect version 2.3.0.185 .With version 2.3.0.185 and beyond there is a capability to not automatically upgrade the client. It's via a profile *Autoupdate* parameter. Please reference the Release notes for these preferences options.

http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect23/release/notes/anyconnect23rn.html#wp908334

Q. Can you use any version of AnyConnect (2.x and above) with any version of Adaptive Security Appliance (ASA) versions (8.x and above) ?

A. AnyConnect 2.x and 3.x versions are generally compatible with ASA version 8.x and vice versa.

Some features are only available in certain AnyConnect and ASA versions. Always consult the Supported VPN Platforms compatibility document for details/restrictions http://www.cisco.com/en/US/partner/products/ps6120/products_device_support_tables_list.html .

Q. What authentication methods does AnyConnect and Clientless SSL VPN support on the ASA?

A. Radius,LDAP,TACACS,Kerberos,NT Domain (NTLM), RSA/SDI, Local,and digital certificates, and a combination of AAA and certificates. See the AAA server support at http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/aaa.html#wp1059666

With ASA version 8.2, the SSL VPN remote access (Clientless and AnyConnect) supports secondary/double authentication. For example you can have RSA/OTP+LDAP authentication, or certificates+RSA/OTP+LDAP,etc.

Note: The AnyConnect Always-on feature requires the use of certificates. Refer to Always-on requirements chapter of the administration guide,

http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect25/administration/guide/ac03features.html#wp1230383

Q. Does AnyConnect and Clientless SSL VPN support re-authentication mechanisms?

A. AnyConnect client and Clientless SSL VPN do not currently support re-authentication triggered for such cases as posture-assessment and or rekeying scenarios.

Note:The VPN IPsec client (legacy IKev1) does support re-authentication on-rekey.

Q. Does Anyconnect support both user (personal store) and machine digital certificates?

A. Yes. With AnyConnect version 2.3 machine certificates authentication no longer requires administrative privileges.

Q. Is there a way for the standalone AnyConnect SSL VPN client to launch a browser and a URL after the session is established?

A. Yes. You can use the group-policy webvpn parameter **homepage** option to set a url page. For example,

homepage value https://myportal.company.com

Q. Where can I find documentation on AnyConnect?

A. Documentation is found here

http://www.cisco.com/en/US/products/ps8411/tsd_products_support_series_home.html .

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 to meet certain browser requirements.

See Supported VPN Platforms for details, http://www.cisco.com/en/US/partner/docs/security/asa/compatibility/asa-vpn-compatibility.html#wp157434 .

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, command:

-install "C:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnva.inf" VPNVA

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. Please collect the device log and system info (as the installer log may not reveal the problem).

Q. AnyConnect 2.4 client fails to connect to IOS headend with message 'A certificate problem has been encountered. A VPN connection will not be established'

A. The main cause for this is due to the below bug:
CSCtb73337 AnyConnect 2.4 does not work with IOS if cert not trusted/name mismatch
http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCtb73337

This can be verified if the Ancyonnect log in the event viewer shows the following message:
Description: error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed

This pertains only with Anyconnect 2.4 and IOS as headend.

Upgrade to a fixed verson of IOS or use workaround listed in the bug:

http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCtb73337

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. Does AnyConnect support MIPS platforms?

A. Not at this time.

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 heathly 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. Does AnyConnect support hunting for different VPN headends (Backup Servers) if one fails?

A. Yes. It's called BackupServerList option in profile (CSCsj88360). Update your AnyConnect profile with the following entries and push it down to the clients from the ASA group-policy.

```
<ServerList>
<HostEntry>
<HostName>Primary Server</HostName>
<HostAddress>x.x.x.x</HostAddress>
<BackupServerList>
<HostAddress>y.y.y.y</HostAddress>
</BackupServerList>
</HostEntry>
</ServerList>
```

Q. What is the requirements for AnyConnect and SSL versions (TLSv1, SSLV3)?

A. AnyConnect requires that the ASA be configured to accept TLSv1 traffic and that the browser settings be set for TLSV1.0. TLSv1.0 is a more secure and modern protocol then SSLv3.

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)

The ASA can suport a mix of TLSv1 for AnyConnect and SSLv3 for

Clientless , if the *ssl server-version* is set to Any.

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 (Internet Explorer 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 Cisco IOS® devices?

A. Yes. Only AnyConnect Premium. Essentials is not yet supportted on IOS.

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.
- AnyConnect Essentials is not currently supported by IOS

Q. Can the AnyConnect client work through an IPsec VPN remote access client tunnel (tunnel-over-tunnel) , or vice versa?

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 AnyConnect traffic at the IM layer.

Note:Clientless SSL VPN traffic can pass over a full-tunnel remote access client (AnyConnect or IPSec) and Site to Site IPSec.

Q. How does the AnyConnect client enforce/monitor the tunnel/split-tunnel policy?

A. AnyConnect enforces the tunnel policy in 2 ways:

1)Route monitoring and repair (e.g. if you change the route table), AnyConnect will restore it to what was provisioned.

2)Filtering (on platforms that support filter engines). Filtering ensures that even if you could perform some sort of route injection, the filters would block the packets.

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 initate 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 SSL VPN client , like a n IPSec full-tunnel client, 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/IOS 871 router/ASA 5505 which does PAT is not an issue with AnyConnect.

Q. Does AnyConnect have the ability to be able 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. The enhancement for this capability is tracked via CSCsk56537. As an immediate solution, the administrator can specify certificate match selection criteria in the AnyConnect Profile XML file. Refer to Configuring the Certificate Match Attribute.

Update: AnyConnect version 2.4 now provides the ability for the user to select a certificate from a list. Refer to 2.4 Administration Guide.

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 the other, 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. Java Runtime Environment version can 1.4.x and above is required. 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 administrative 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 enforced from DHCP.

Q. How is Idle Timeout handed for DTLS and TLS for the session?

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 AnyConnect installation log files stored?

A. The install log locations for all OS types are below:

Windows 2000 and XP:

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.

Vista:

Log is stored in <drive:>Users\<user>AppData-Local-Temp

Linux

Log is stored in **/opt/cisco/vpn**

MAC OS

Log is stored in **/opt/cisco/vpn**

Q. What are the locations for various AnyConnect files : Profiles, Preferences, Modules?

A. Please refer to the AnyConnect Administrator Guides for the particular version.

http://www.cisco.com/en/US/products/ps8411/prod_maintenance_guides_list.html

For example, the AnyConnect File location for version 3.0 is found at

http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/ac02asaconfig.html#wp1239181

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 abilty to run a logon script after connection.

Update: With AnyConnenct version 2.4 you can launch scripts before and after the VPN session establishes. Refer to Release Notes for details.

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 ASA 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 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 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. Does ASA SSL VPN (AnyConnect Client or Clientless) support QOS and policing bandwidth management capabilites?

A. No. ASA SSL VPN doesn't support these capabilities . You'll get an error if trying to configure this:

```
ASA(config)# tunnel-group a1 type webvpn

ASA(config)# tunnel-group a1 webvpn-attributes

ASA(config-tunnel-webvpn)# class-map c1

ASA(config-cmap)# match tunnel-group a1

ASA(config-cmap)# match flow ip destination-address

ASA(config-cmap)# policy-map p1

ASA(config-pmap)# class c1

ASA(config-pmap-c)# police output 100000

ERROR: tunnel with WEBVPN attributes doesn't support police!

ASA(config-pmap-c)#
```

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.

See more details in the AnyConnect Administrator Guide at http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect23/administration/23admin2.html#wp999826 .

Q. What is the AnyConnect Reconnect (Connection Persistense) Behavior?

A. AnyConnect will attempt to reconnect if the connection is disrupted. This is not configurable at the moment, but automatic (see CSCsl52873). As long as the session on the ASA is still valid, if AnyConnect can re-establish the physical connection, the session will be resumed. The amount if time the AnyConnect will try to reconnect is stored in the client in a parameter called "Disconnect Timeout" and is by default set to the lowest of either the group-policy's Idle Timeout or Maximum Connect Time. The enhancement request CSCsl52873, asks for the ASA platform to implement "Disconnect Timeout" as parameter in the Dynamic Access Policy and or group-policy.

For customers who do not want the reconnect feature, can set the the group-policy's Idle Timeout to a low value to prevent sleep or resume reconnects.

Note: If for example the endpoint has multiple interfaces (wired/wired and 3G) enabled and assigned with IP addresses , and if the AnyConnect session originally established with wireless drops, AnyConnect will reconnect and maintain the initial session with 3G.

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 as of AnyConnect version 2.2.

Q. Does AnyConnect 2.x support both x86 (32-bit) and x64 (64-bit) Vista , Windows 7 and MAC OSX 10.6.x?

A. Please see Supported VPN Platforms http://www.cisco.com/en/US/partner/docs/security/asa/compatibility/asa-vpn-compatibility.html#wp157434 .

Q. Is AnyConnect supported on mobile devices?

A. Yes. AnyConnect version 2.3 added mobile support. Please refer to the Release notes for the supported platforms. http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect23/release/notes/anyconnect23rn.html#wp878382

Q. Is AnyConnect supported on USB or VM on USB devices?

A. No. This configuration is not currently supported.

Q. How does the mobile license work/ordered?

A. The Mobile license is a fixed license on top of the existing # of licensed SSL users. It may be used either with a Premium SSL VPN license or an AnyConnect Essentials license. To order the license for an existing unit, the part number is: L-ASA-AC-M-55XX= (XX=05,10,20,40,50,80 depending on the model). This can also be added as an option for new device purchases (ASA-AC-M-55XX).

Q. Does the AnyConnect mobile license work with both AnyConnect Essentials and Premium clients?

A. Yes.

Q. On the ASA, can AnyConnect Essentials and Premium clients/license operate simultaneously?

A. No. It's either one or the other.

The AnyConnect Essentials license lets you use the AnyConnect client to connect to the adaptive security appliance, while supporting the platform limit for SSL VPN sessions. For example, you can use 25 sessions for the ASA 5505. Cisco Secure Desktop and clientless SSL VPN are not supported. The AnyConnect Essentials license is not compatible with the following licenses: AnyConnect Premium SSL VPN licenses (all types) and Advanced Endpoint Connection license. By default, the AnyConnect Essentials license is used instead of the above licenses, but you can disable the AnyConnect Essentials license in the configuration to restore use of the other licenses using the **no anyconnect-essentials** command.

Please refer to the Licenses guide for more details , http://www.cisco.com/en/US/partner/docs/security/asa/asa82/license/license82.html#wp179742 .

Q. Is AnyConnect Essentials supported on IOS (ISR, 7200,etc)?

A. Not at this time. Cisco is evaluating for future consideration.

Q. Does AnyConnect have the capability to display a message/warning to the end user when the client's digital certificate is about to expire in X future days?

A. The IPsec client has this capability, but the AnyConnect SSL VPN client currently doesn't support this (CSCsx65066 enhancement for future consideration).

Q. Once a user has logged into AnyConnect Start Before Login (SBL)using their AD credentials, can AnyConnect then pass these credentials transparently into windows so that it automatically logs them, without the need for secondary windows prompt?

A. This sort of SSO capability is not currently supported. Enhancement request (CSCsm08815-SBL credential pass to MS login)for possible future implementation.

Q. Can AnyConnect Start before Login (SBL) be prevented from executing if for example the ASA VPN server is not reachable or the endpoint PC is located in a specific IP subnet?

A. No . This control capability is not possible at this time.

Q. Does the AnyConnect API support Windows Mobile 5/6 devices?

A. The API does not support Windows Mobile at this time.

Q. Does the AnyConnect support the virtual keyboard feature?

A. No. This feature is only supported for Clientless (browser-mode) SSL VPN. If applicable, CSD Key-stroke-Logger can be enabled to identify potential password captures.

Q. Can you launch AnyConnect over an RDP session?

A. Yes. Feature introduced in AnyConnect version 2.3.254 .

Q. Does the AnyConnect have a capability to automatically start/terminate when an application (ie.Outlook) is launched/closed?

A. This capability is not supported at this time. AnyConnect 2.4 supports launching scripts before/after the AnyConnect starts/stops, perhaps this can be leveraged.

Q. Is AnyConnect Client available for Apple Iphone?

A.Yes. AnyConnect is available for Apple Iphone in the App Store.

Q. Does the AnyConnect Client and ASA5500 support TLS1.1 and 1.2 ?

A. As of ASA 8.4 and AnyConnect client 3.0, only TLS1.0 and DTLS 1.0 are supported. TLS versions 1.1 and 1.2 are not yet supported.

Troubleshooting

Q. How do I go about troubleshooting AnyConnect problems?

A. Please reference the following:

Using Diagnostic AnyConnect reporting Tool (DART) to Gather Troubleshooting Information

http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/ac12managemonitortbs.html#wp1058615

1) ASA 8.x: AnyConnect VPN Client Troubleshooting Tech Note

2) With AnyConnect 2.4 use the Diagnostic AnyConnect Reporting Tool (DART) on Windows to obtain the following information:

After the DART utility gathers the data, the bundle contains:
a) all event logs
b) The Client OS MSINFO file
c) Any minidump crash files
d) The setupapi and webinstall logs
e) The csd and hostscan logs (if using csd)

f)The relevant registry files

For more information on DART please refer to the AnyConnect Administration Guide-troubleshooting section .

3) Review the AnyConnect Release Notes for Latest Guidelines, Open Caveats, System Requirements,etc.

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

Related Information

- **Cisco AnyConnect VPN Client**
- **Managing License Features on the ASA 5500**
- **Cisco ASA 5500 Series Adaptive Security Appliances**
- **Technical Support & Documentation - Cisco Systems**

Document ID: 107391