Release Notes for Cisco Secure Client (including AnyConnect), Release 5 for Universal Windows Platform

Cisco Secure Client for Universal Windows Platform

Cisco Secure Client (including AnyConnect) for Universal Windows Platform provides remote Windows users with secure VPN connections to the Cisco Secure Firewall ASA and other Cisco-supported headend devices. It provides seamless and secure remote access to enterprise networks, allowing installed applications to communicate as though connected directly to the enterprise network. Cisco Secure Client supports connections to IPv4 and IPv6 resources over an IPv4 or IPv6 tunnel.

This document, written for system administrators of the Cisco Secure Client and the Cisco Secure Firewall ASA, provides release specific information for Secure Client running on Universal Windows Platform.

The Cisco Secure Client app is available on the Windows Store only. You cannot deploy the mobile app from the Secure Firewall ASA. You can deploy other releases of Cisco Secure Client for desktop devices from the ASA while supporting this mobile release.

Cisco Secure Client Mobile Support Policy

Cisco supports the Cisco Secure Client version that is currently available in the app store; however, fixes and enhancements are provided only in the most recently released version.

Cisco Secure Client Licensing

To connect to the Secure Firewall ASA headend, an Advantage or Premier license is required. Trial licenses are available: Cisco Secure Client Ordering Guide.

For the latest end-user license agreement, see Cisco End User License Agreement, Cisco Secure Client.

For our open source licensing acknowledgments, see Open Source Software Used in Cisco Secure Client for Mobile.

Cisco Secure Client Mobile Related Documentation

For more information refer to the following documentation:

- Cisco Secure Client Release Notes
- Cisco Secure Client Administrator Guides
- Cisco Secure Firewall ASA Documentation Landing Page

Universal Windows Platform Supported Devices

Windows Support

Cisco Secure Client for Universal Windows Platform is supported on devices that run Microsoft Windows 10 RS4 (1803) or higher.

Universal Windows Platform Cisco Secure Client Feature Matrix

The following remote access features are supported by Cisco Secure Client on Universal Windows Platform:

Category: Feature	Universal Windows Platform
Deployment and Configuration:	
Install or upgrade from Application Store	Yes
Cisco VPN Profile support (manual import)	No
Cisco VPN Profile support (import on connect)	No
MDM configured connection entries	Yes
User-configured connection entries	Yes
Tunneling:	
TLS	Yes
Datagram TLS (DTLS)	Yes
IPsec IKEv2 NAT-T	No
IKEv2 - raw ESP	No
Suite B (IPsec only)	No
TLS compression	No
Dead peer detection	No
Tunnel keepalive	No
Multiple active network interfaces	No
Per-App Tunneling (requires Advantage or Premier license and ASA 9.4.2 or later)	No
Full tunnel (OS may make exceptions on some traffic, such as traffic to the app store)	Yes
Split tunnel (split include)	Yes
Local LAN (split exclude)	No
Split-DNS	Yes

Category: Feature	Universal Windows Platform
Auto Reconnect / Network Roaming	Yes, if user remains on the same network and the network connection has not terminated.
VPN on-demand (triggered by destination)	Yes
VPN on-demand (triggered by application)	No
Rekey	No
IPv4 public transport	Yes
IPv6 public transport	Yes
IPv4 over IPv4 tunnel	Yes
IPv6 over IPv4 tunnel	Yes
Default domain	Yes
DNS server configuration	Yes
Private-side proxy support	Yes
Proxy Exceptions	No
Public-side proxy support	No
Pre-login banner	Yes
Post-login banner	Yes
DSCP Preservation	No
Connecting and Disconnecting:	
VPN load balancing	Yes
Backup server list	No
Optimal Gateway Selection	No
Authentication:	
SAML 2.0	No
Client Certificate Authentication	Yes
Online Certificate Status Protocol (OCSP)	No
Manual user certificate management	Yes
Manual server certificate management	Yes
SCEP legacy enrollment Please confirm for your platform.	No
SCEP proxy enrollment Please confirm for your platform.	No
Automatic certificate selection	Yes
Manual certificate selection	No
Smart card support	Yes

Category: Feature	Universal Windows Platform
Username and password	Yes
Tokens/challenge	Yes
Double authentication	Yes
Group URL (specified in server address)	Yes
Group selection (drop-down selection)	Yes
Credential prefill from user certificate	Yes
Save password	No
User interface:	
Standalone GUI	Yes, limited functions.
Native OS GUI	Yes
API / URI Handler (see below)	No
UI customization	No
UI localization	No
User preferences	Partial
Home screen widgets for one-click VPN access	No
AnyConnect specific status icon	No
Mobile Posture: (AnyConnect Identity Extensions, ACIDex)	
Serial number or unique ID check	No
OS and Cisco Secure Client version shared with headend	Yes
URI Handling:	
Add connection entry	No
Connect to a VPN	No
Credential pre-fill on connect	No
Disconnect VPN	No
Import certificate	No
Import localization data	No
Import XML client profile	No
External (user) control of URI commands	No
Reporting and Troubleshooting:	
Statistics	No
Logging / Diagnostic Information (DART)	Yes, obtain the logs via the Windows 10 directory 'C:\Users\[username]\AppData\Local\Packages\CiscoSystems.AnyConnect_cdgkw48xf\LocalState\Logs'

Category: Feature	Universal Windows Platform
Certifications:	
FIPS 140-2 Level 1	No

New Features in Cisco Secure Client 5.0.00907 for Universal Windows Platform

This 5.0.00907 version introduces the new Cisco Secure Client (including AnyConnect) for Universal Windows Platform and includes the following new feature and known limitation.

—Support for DTLS. This new feature has the following caveats:

- Tunnel rekey is not supported.
- If DTLS is blocked, a 3 second delay occurs.
- TLS MTU is used for the DTLS tunnel.
- The tunnel will disconnect on Sleep and Network Transition because of a framework limitation.
- DTLS tunnel compression is not supported.
- Dead Peer Detection (DPD) is not supported.

Known Limitation for UWP on ARM64 devices—When a certificate threshold warning is triggered, it always reports 0 days left (CSCwd60132).

Cisco Secure Firewall ASA Requirements

Cisco Secure Firewall ASA Release 8.0(3) and Adaptive Security Device Manager (ASDM) 6.1(3) are the minimum releases that support Cisco Secure Client for mobile devices. A minimum release of the Cisco Secure Firewall ASA is required to use the following features:

Note Refer to the feature matrix for your platform to verify the availability of these features in the current Cisco Secure Client mobile release.

- SAML authentication —Secure Firewall ASA 9.7.1.24, 9.8.2.28, 9.9.2.1 or later. Make sure that both the client and server versions are up-to-date.
- TLS 1.2—Secure Firewall ASA 9.3.2 or later.
- IPsec IKEv2 VPN, Suite B cryptography, SCEP Proxy, or Mobile Posture—Secure Firewall ASA 9.0.