

LANCOM Release Notes

Advanced VPN Client Windows

5.23 Rel / 4.16 Rel / 3.13 RU2

Copyright (c) 2002-2021 LANCOM Systems GmbH, Wuerselen (Germany)

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

Internet: <http://www.lancom-systems.com>

December 10th, 2021, CBuersch

Table of Contents

1. Preface	2
2. New features, changes, and history Advanced VPN Client Windows version 5.x	3
Advanced VPN Client Windows improvements in version 5.23 Rel Build 48767	3
Advanced VPN Client Windows improvements in version 5.20 Rel Build 48591	4
Advanced VPN Client Windows improvements in version 5.11 Rel Build 48297	5
Advanced VPN Client Windows improvements in version 5.00 Rel Build 45109	7
3. New features, changes, and history Advanced VPN Client Windows version 4.x	9
Advanced VPN Client Windows improvements in version 4.16 Rel Build 43395	9
Advanced VPN Client Windows improvements in version 4.14 Rel Build 42039	9
Advanced VPN Client Windows improvements in version 4.13 Rel Build 41436	10
Advanced VPN Client Windows improvements in version 4.10 Rel Build 39753	11
4. New features, changes, and history Advanced VPN Client Windows version 3.x	12
Advanced VPN Client Windows improvements in version 3.13 RU2 Build 40955	12
Advanced VPN Client Windows improvements in version 3.13 RU1 Build 38935	12
Advanced VPN Client Windows improvements in version 3.13 Rel Build 38189	13
Advanced VPN Client Windows improvements in version 3.11 Rel Build 32792	13
Advanced VPN Client Windows improvements in version 3.10 RU2 Build 31731	14
Advanced VPN Client Windows improvements in version 3.10 Rel Build 30578	14
Advanced VPN Client Windows improvements in version 3.10 Rel Build 29061	14
Advanced VPN Client Windows improvements in version 3.04 Rel Build 26745	15
Advanced VPN Client Windows improvements in version 3.02 RU1 Build 25056	15
Advanced VPN Client Windows improvements in version 3.02 Rel Build 24934	15
Advanced VPN Client Windows improvements in version 3.00 Rel Build 21499	16

1. Preface

The LANCOM Advanced VPN Client Windows provides mobile employees with encrypted access to the company network, whether they are at their home office, on the road, or even abroad.

This document describes the innovations within the Advanced VPN Client Windows software releases 5.23 Rel, 4.16 Rel, and 3.13 RU2, as well as the improvements since the previous versions.

The LANCOM Advanced VPN Client Windows supports Windows Vista, Windows 7, Windows 8, Windows 8.1, and Windows 10. The LANCOM Advanced VPN Client Windows 3.00 does no longer support Windows XP.

As from version 3.10, the client needs a license key of the same version for activation. Activation or update installation is no longer possible with an old license key. This applies from now on for every upcoming major version.

2. New features, changes, and history Advanced VPN Client Windows version 5.x

Advanced VPN Client Windows improvements in version 5.23 Rel Build 48767

Bugfixes / improvements

> Incomplete log files

Erroneous write accesses to the client log files could sporadically occur, resulting in the client log being incomplete.

> Revised installation routine

In rare cases, after the end of the installation process the network connection was completely disconnected before the computer restarted.

> Fixing CVE-2021-41793

Within the MSI installation process, the 'Repair program' functionality has been removed, thus eliminating CVE-2021-41793.

Advanced VPN Client Windows improvements in version 5.20 Rel Build 48591

New features

> DNS input for VPN bypass

This new configuration option ensures that for external VPN bypass targets, name resolution through the VPN tunnel is performed only by the two configured DNS servers. For this purpose, a primary and a secondary DNS, optionally as IPv4 or IPv6 address, can be entered in the VPN bypass configuration. In this release, the configured DNS servers are only effective for configured web domains. Configured applications within the VPN bypass functionality are currently not yet taken into account.

> Screen sharing via Wi-Fi

Screen sharing via Wi-Fi, e.g. for presentation via beamer via Miracast, is now possible.

Bugfixes / improvements

> Troubleshooting reverse DNS requests

Fixed a problem with reverse DNS requests (PTR requests) from the operating system.

> Update of the integrated OpenSSL version

The OpenSSL version used in the LANCOM Advanced VPN Client has been updated to the latest version.

> Problems in conjunction with multiple IPv6 addresses on the adapter

If multiple IPv6 addresses were assigned to the network adapter, the VPN connection establishment or data transfer through the VPN tunnel could be disrupted in certain cases.

> DNS troubleshooting

Under certain circumstances, DNS requests through the VPN tunnel were not resolved correctly or returned an error.

> Support Assistant

The output path for storing the ZIP file with the collected log files is now taken into account.

> No data throughput within the VPN tunnel

In rare cases, no data could be transported through the VPN tunnel after the media change when using seamless roaming.

> Troubleshooting in the VPN bypass functionality

> Various stability improvements

Known limitations

> Network connection remains disconnected after installation/update

After the installation/update process of the Advanced VPN Client, the network connection remains inactive and can only be used after restarting the computer.

> Dialog for silent installation under Windows 7

Since the change of the software signature from SHA-1 to SHA-256 within Windows 7, two Windows security dialogs are generally displayed to confirm the driver installation during the client installation.

Advanced VPN Client Windows improvements in version 5.11 Rel Build 48297

New features

> **Selecting the certificate for IEEE 802.1X authentication on the Wi-Fi network**

Within the wireless configuration of the LANCOM Advanced VPN Client, a Windows dialog for selecting a certificate from the certificate store can be called up under 'Profile/Encryption' by clicking on the 'Certificate selection' button. This certificate is then used for IEEE 802.1X authentication on a wireless LAN with configured SSID.

> **Support for the Cookie Challenge mechanism**

The Cookie Challenge mechanism is used to defend against DoS attacks on a VPN gateway. The function cannot be configured in the client.

> **Extension of the parameter lock for profile save / restore**

The parameter lock for profile backup has been replaced by two new parameter locks. A distinction is now made between backing up and restoring a profile.

Bugfixes / improvements

> **IPv6 prioritization with DNS resolution of the VPN tunnel endpoint**

If the VPN tunnel endpoint is configured as a domain name, a DNS server can return both an IPv6 and an IPv4 address. In this case the LANCOM Advanced VPN Client first selects the IPv6 address. If the connection setup fails, the IPv4 address is then attempted.

> **Input window for user name and password during connection establishment IKEv2/EAP**

If no user name or password is entered in the client configuration when using IKEv2/EAP, a separate input window now appears when the connection is established.

> **Read '%username%' for the ID of the local identity**

Similar to the entry of the environment variable '%username%' for the VPN user name, this entry can now also be made in the ID of the local identity. The first time the configuration is read by the client GUI, the corresponding value of '%username%' is permanently transferred to the configuration.

> **Display the available Wi-Fi SSIDs**

Available Wi-Fi SSIDs were not completely displayed in the Wi-Fi configuration of the LANCOM Advanced VPN Client

> **Optimizations of the client GUI in the 'extended log settings'**

> **Optimization of the 'OTP-Token' functionality**

> **Optimization of the functionality 'Logon options'**

If the LANCOM Advanced VPN Client was installed outside the 'C:\Programs' directory, the NCP Credential Provider was not displayed correctly during Windows logon.

> **Display of the connection information**

After disconnecting a VPN connection and re-establishing it, the IP addresses displayed were not updated. This problem has been fixed.

> **Omission of directory selection for firewall log files**

> **Improved compatibility with Gemplus USB Key SmartCard readers**

- > **Troubleshooting when processing certificates with contained certificate chains that are larger than 8 kByte**
- > **Fixed a bug in the search path of a PKCS#11 DLL on Windows 10**
- > **Improved compatibility to ReinerSCT cyberJack® card readers**
- > **Bug fixes in the Support Assistant**

When the Support Assistant was called to collect the log files, the PKI log files were missing. This problem has been fixed.
- > **Fixed a bug in the license handling**

In rare cases, the license file of the LANCOM Advanced VPN Client could be damaged. The following error message appeared: "License data could not be read". This problem has been solved.
- > **Adaptation of the error message if no VPN gateway is reached**
- > **Troubleshooting within the split tunneling configuration**

Known limitations

- > **Silent Installation under Windows 7**

Since the change of the software signature from SHA-1 to SHA-256 within Windows 7, two Windows security dialogs are generally displayed during the client installation to confirm the driver installation. This effect does not occur under Windows 8.x or Windows 10.
- > **Option 'Automatically open dialog for connection establishment'**

Under certain circumstances the logon option 'Automatically open dialog for connection establishment' does not work.

Advanced VPN Client Windows improvements in version 5.00 Rel Build 45109

New features

> Quality of Service

Outgoing client data can now be prioritized within the VPN tunnel. For this, the total bandwidth of the data channel in sending direction has to be configured in the QoS configuration. The configured total bandwidth is static. Due to this, the QoS functionality is currently only of limited suitability for mobile usage. Data which has to be prioritized can be specified, depending on its source, as .exe file (case sensitive) or directory (without subdirectories). These data sources can be grouped, and each group can be allocated a minimum bandwidth. Data which has to be sent and can not be allocated to any group is limited according to the remaining bandwidth. If a configured group is not in use, the remaining bandwidth is increased by the reserved throughput of this inactive group. The applying throughput rates of the configured groups in sending direction can be monitored under the menu item "Connection/Connection information/Quality of Service".

> IPv4 / IPv6 dual stack support

Within the VPN tunnel, the IPv4- as well as the IPv6 protocol is supported. The split tunneling functionality can be configured separately for IPv4 and IPv6.

> Temporary home zone

A new option "Set home zone only temporarily" has been added. Until now the Advanced VPN Client recognized a previously set home zone at a later time. Now, if this option is set, a configured home zone is forgotten after a restart, standby, or a change of the connection medium, and has to be re-set, if required.

> Expert mode

An expert configuration mode has been added to the client configuration.

> Extended connection management

The Advanced VPN Client connection management has been extended by two connection options: "Disable mobile radio with plugged LAN cable" and "Disable mobile radio with active Wi-Fi connection".

> Extended support wizard

As from this version, the support wizard collects all available log files for passing on to the support.

Bugfixes / improvements

> New directory structure

For reasons of operational reliability and Windows compatibility the directory structure of the Advanced VPN Client has been changed. Directories which had been previously created in the installation folder under “\Programs\LANCOM\Advanced VPN Client”, have now been moved to “\ProgramData\LANCOM\Advanced VPN Client”. You can find further information about the migration to the new directory structure in the file Readme.txt.

> Extended status window “Connection information”

In the status window “Connection information” the used algorithms within the IKE negotiation and the IPsec protocol for the current VPN connection are displayed.

> Removal of no longer relevant configuration parameters

The following configuration parameters have been removed from the configuration due to missing relevance:

Connection medium	ISDN
ISDN	Dynamic Link aggregation
ISDN	Threshold for link aggregation
IPSec address allocation	1. and 2. WINS server
Link firewall	only configurable in expert mode

> Support for the Gemalto IDPrime 830 SmartCard

The PIN handling of a Gemalto IDPrime 830 SmartCard which has been configured by Microsoft Smart Card Key Storage Provider (CSP) has been optimized.

> Optimized filter driver

The Advanced VPN filter driver has been optimized regarding data throughput.

> Optimized login via Time-based OTP (one-time passwords)

> GUI scaling bug fix

When using GUI scaling a faulty display within configuration dialogs could occur.

3. New features, changes, and history Advanced VPN Client Windows version 4.x

Advanced VPN Client Windows improvements in version 4.16 Rel Build 43395

Bugfixes / improvements

➤ **Credential provider without hotspot authentication**

The newly introduced credential provider hotspot authentication prior to the Windows user authentication had to be removed due to security reasons. The hotspot authentication is available as before without functional restriction after the Windows user authentication.

➤ **An issue has been solved with 802.1X authentication in the LAN**

➤ **An issue has been solved with VPN connection establishment in the Friendly Net**

➤ **Addition of a Wi-Fi profile name to the Wi-Fi profile**

The Wi-Fi profile name is now shown in the Wi-Fi configuration. By this, Wi-Fi profiles can now be distinguished and purposefully connected in case of identical SSIDs.

➤ **VPN tunnel disconnect when using a mobile radio connection**

A VPN tunnel which was established via mobile radio was disconnected after a short time due to Dead Peer Detection.

➤ **PKI error when using a smart card**

A PKI error occurred when using a smart card.

Advanced VPN Client Windows improvements in version 4.14 Rel Build 42039

Bugfixes / improvements

➤ **Check for Internet accessibility**

The continuous check of a connection medium for Internet accessibility by periodically sent pings to IP address 8.8.8.8 has been limited to four pings.

➤ **Optimizations for Hotspot authentication**

Miscellaneous optimizations have been made for Hotspot authentication, particularly with seamless roaming activated in the profile settings.

➤ **Credential Provider**

Using the NCP Credential Provider a user could gain access to the Windows explorer via the log window clicking its "Open file" button. Furthermore, it was possible to gain administrator rights within the Power Shell.

➤ **Deinstallation of the VPN Client**

In certain cases it could occur that the filter driver of the VPN client was not uninstalled properly.

➤ **IKEv1 / aggressive mode**

Issues could occur when using IKEv1 / aggressive mode with an automatic IKE policy.

➤ **Improved handling of available connection media after waking up from standby**

Advanced VPN Client Windows improvements in version 4.13 Rel Build 41436

Bugfixes / improvements

> Adjustments for Windows 10 version 1809

Due to Microsoft-internal changes it was not possible for previous clients to carry out a new installation on Windows 10 version 1809.

> Optimization of the client update process in case of a major update

The recognition of a major update within the installation process has been improved.

> VPN client display in the taskbar

If the client GUI is closed, the corresponding icon will no longer be displayed on the taskbar.

> Diagnostic data in the installation folder

In case of an activated trace function or a configured hotspot detection, diagnostic data was erroneously written to the client's installation folder.

> Firewall setting: Exception for VPN Path Finder

If the option "accept IPsec protocol (ESP, UDP 500) and VPN Path Finder (TCP 443)" was configured in the firewall, target stations were accessible through the VPN tunnel via HTTPS port 443, although this was not allowed by any additional firewall rule.

> PKCS#11 file name length

The length of the input field of the client's PKI configuration for the PKCS#11 module has been extended to 255 characters.

> Loading DLLs

Improvements in DLL file loading for increased protection against manipulated DLLs

> Update check improvements

The client's update check for availability of new versions has been improved for increased protection against manipulations.

> Optimized data transfer performance outside of the VPN tunnel

> Improved silent installation

> Improved compatibility to DHCP servers

> Improved compatibility to external gateways

Advanced VPN Client Windows improvements in version 4.10 Rel Build 39753

New features

- **Biometric authentication (e.g. fingerprint- or face recognition) before VPN connection establishment**

For protection against a VPN connection establishment by unauthorized third parties a biometric authentication has been added to the Advanced VPN Client Windows. Immediately after pressing the "Connect" button in the client GUI there is a prompt for user authentication. The VPN connection is only established after a positive authentication. The Windows Hello functionality is required for biometric authentication, which is available as from Windows 8.1 or later.
- **Modernized client GUI**

The client GUI and the tray popup window which is started from the taskbar have been adopted to the current Windows 10 design.
- **Complete 64 bit implementation of the Advanced VPN Client Windows**

As from this version, all components of the Advanced VPN Client Windows are included in 64-bit versions.
- **New GUI for the credential provider, including the Hotspot authentication functionality**

For establishing the VPN tunnel prior to the Windows user authentication, it is now possible to do a Hotspot authentication on a re-designed GUI.

Bugfixes / improvements

- **Configuration of the VPN tunnel endpoint**

Multiple VPN tunnel endpoints can now be configured using their domain names.
- Optimization of the DPD functionality
- **FIPS-Inside**

When installing from scratch or changing an existing configuration the FIPS mode can be enabled or disabled from within the installation routine.
- **Display of IPv6 connection information**

IPv6 addresses are now displayed on the connection information page, too.
- **Enhancements within the Client Info Center**

A new section with driver information has been added to the Client Info Center. For Windows 10 operating systems, driver version- and build number are now additionally displayed.
- **Improvements of the Hotspot functionality**

The compatibility to Hotspot authentication pages has been extended.

4. New features, changes, and history Advanced VPN Client Windows version 3.x

Advanced VPN Client Windows improvements in version 3.13 RU2 Build 40955

Bugfixes / improvements

> **Adjustments for Windows 10 version 1809**

Due to Microsoft-internal changes it was not possible for previous clients to do carry out a new installation on Windows 10 version 1809.

> **Diagnostic data in the installation folder**

In case of an activated trace function or a configured hotspot detection diagnostic data was erroneously written to the client's installation folder.

> **License after 30-day trial version**

A malfunction of the license management could occur after the expiration of the trial period.

> **Loading DLLs**

Improvements in DLL file loading for increased protection against manipulated DLLs

Advanced VPN Client Windows improvements in version 3.13 RU1 Build 38935

Bugfixes / improvements

> **Client firewall status feedback to the Windows operating system**

An activated Advanced VPN Client Windows firewall is now shown under "Security and maintenance" in the Windows operating system.

> **Network driver optimization**

The connection establishment behavior after a standby has been improved by optimizing the NDIS network driver.

> **Automatic network mask adjustment**

If an invalid network mask is specified for a dial-in profile, a class C network mask (255.255.255.0) is automatically used for this connection.

Advanced VPN Client Windows improvements in version 3.13 Rel Build 38189

Bugfixes / improvements

- › Full compatibility to Windows 10 Creators Update (1709)
- › IKEv2 connections remain operational after being reconnected.
- › The stability of the integrated firewall has been generally improved.
- › A display issue in the budget manager has been fixed.
- › Long domain names can be used again.
- › The hotspot functionality has been improved.
- › Extended status information in the client info center
- › Improved stability when using VPN bypass
- › Improved stability for certificate handling by clients
- › A malfunction regarding seamless roaming has been fixed.

Advanced VPN Client Windows improvements in version 3.11 Rel Build 32792

New features

- › Using VPN Bypass, internet communication is now possible despite disabled split-tunneling
- › Home Zone can now be enabled within the firewall to use local resources within the client without configuration
- › Selection of a user- or computer-certificate can be preset within the Windows CSP
- › New product- and status icons
- › Support for more than two FND servers
- › The Budget manager supports the function “no roaming allowed”
- › The VPN client can now connect to an IPv6 network

Bugfixes / improvements

- › Fixed an issue with hotspot authentication
- › IPv6 IKE packets are no longer blocked when activating the firewall function “allow IPsec protocol”
- › Selection of an alternative IPsec port works, even if the option “allow...IPsec protocol (ESP, UDP) and VPN path finder” is enabled within the firewall
- › Enabling/disabling the credential provider is only possible via monitoring menu (configuration -> logon options) and is no longer shown during installation

Advanced VPN Client Windows improvements in version 3.10 RU2 Build 31731

Bugfixes / improvements

- Modified driver signature to grant success for a VPN client reinstall after the Windows 10 Anniversary update was done and if secure boot is enabled in the computer's BIOS/UEFI
- After restart or waking from sleep mode the Wi-Fi will be reliably activated
- Fixed an issue within stateful inspection which lead to a failed hotspot authentication
- Fixed an issue which could cause a loss of client activation after a restart under certain circumstances

Advanced VPN Client Windows improvements in version 3.10 Rel Build 30578

Bugfixes / improvements

- The handling of the license file was optimized.
- The certificate and within its signature were refreshed.
- If the flight mode within a Windows 10 System is activated the client will recognize that and stop. Using 3G/4G-hardware won't be able to use in that situation.
- Clicking the Connect-/Disconnect button in quick succession it was possible that an undefined state could be reached. This issue is now solved.

Advanced VPN Client Windows improvements in version 3.10 Rel Build 29061

New features

- Revision of the hotspot login: After the user has been connected to a certain wireless network, a web browser integrated in the Advanced VPN Client Windows window hotspot logins opens automatically
- Surveillance of the filter operator: The AVC monitors Windows system drivers which are needed for the client's operation
- Windows Pre-Logon: The Windows Pre-Logon functionality (Credential Provider) is now also available for Windows 10
- Support for IKEv2 Redirect (RFC 5685)

Bugfixes / improvements

- If the client recognizes a filter driver malfunction, this will be fixed automatically, and the user is prompted to do a restart
- On a clean install, the client is installed to the programs directory by default

Advanced VPN Client Windows improvements in version 3.04 Rel Build 26745

New features

- › Compatibility improvements with various Windows operating systems when disabling the WLAN adapter with plugged LAN cable

Bugfixes / improvements

- › Bugfix for forwarding the manually entered username and password while authenticating to Windows via Credential Provider
- › Bugfix for firewall application detection
- › Bugfix for automatic media detection with PPPoE
- › The ConnMode=2 connection mode (alternating (manual start of automatic mode)) is imported correctly during a profile import
- › Bugfix for Split Tunneling when the remote network IP address range is the same as the local user network (the route to the local network was deleted after a VPN profile change)
- › Fixed a problem with Windows 10 Update 1511 which led to lost registry entries

Advanced VPN Client Windows improvements in version 3.02 RU1 Build 25056

Bugfixes / improvements

- › A problem was solved which led to a rollback of the client during the filter driver setup.

Advanced VPN Client Windows improvements in version 3.02 Rel Build 24934

New features

- › Extensions within the log reporting
- › Support for Windows 10
- › Improved scaling of the monitor for touch screen operation
- › Known networks can be checked periodically for connectivity.
- › The displayed dialog during a failed connection establishment can be deactivated.
- › When using a hardware certificate the VPN connection can be established at system startup, without logging on to Windows system.
- › The WLAN adapter can now be disabled if a LAN cable is plugged in.

Advanced VPN Client Windows improvements in version 3.00 Rel Build 21499

New features

- › Windows 8.x compatibility improvements
- › There is now a 32-bit and 64-bit version of the LANCOM Advanced VPN Client Windows.
- › MSI-Installer
- › The new option "Allow outbound traffic to reject acknowledge" was added to the Firewall.
- › **Two new connection modes for connection establishment**
 - Always (The client module will attempt to connect from system startup. If it does not exist it will try every 10 seconds.)
 - Changing (always-mode start manually)
- › Added a configurable ICMP polling for the VPN tunnel
- › An IPv6 address can be specified as endpoint for an IPv4 VPN tunnel.
- › The VPN network adapter can be hidden.

Bugfixes / improvements

- › Improved usage of a UMTS/GPRS connection
- › Under Windows 8, a replugged USB smartcard reader is recognized correctly by the LANCOM VPN Client Windows.