Release Notes

Advanced VPN Client Windows 6.14 Rel / 5.23 Rel

Table of contents

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 Windowssoftware releases 6.14 Rel and 5.23 Rel, as well as the improvements since the previous versions.

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. Requirements

Supported Microsoft Windows operating systems

You can see a list of supported operating systems / versions here:
https://support.lancom-systems.com/knowledge/pages/viewpage.action?pageId=37457174

HotSpot registration

For the correct function of the HotSpot login, at least version 101.0.1210.39 of the Microsoft WebView2 runtime must be installed.

New directory structure

For reasons of operational security and compatibility with Windows, the directory structure of the LANCOM Advanced VPN Client has been changed as of version 5.0. The following directories, which were located in the installation directory within **Programs\LANCOM\Advanced VPN Client** in older client versions, are now located in **ProgramData\LANCOM\Advanced VPN Client**:

- → arls
- → cacerts
- → certs
- → config
- → crls
- → CustomBrandingOption
- → data
- → hotspot
- → log
- → statistics

These are configuration files, certificates, or log files. Binaries or resources remain in the path **Programs\...**

During an update process, the new directory structure is automatically created and the client configuration is transferred accordingly. Thus, configuration paths within the certificate configuration that contain the variable **%InstallDir%** are rewritten to paths with **%CertDir%**. Here **%CertDir%** denotes the path **C:\ProgramData\LANCOM\Advanced VPN Client\certs**.

Note:
The configuration entry **%CertDir%\client1.p12** is equivalent to **client1.p12**.

3. History Advanced VPN Client Windows version 6.x

Advanced VPN Client Windows 6.14 Rel Build 29669

Bugfixes / improvements

→ **Adjustment of the PKCS#11 module configuration**
To increase the security of the LANCOM Advanced VPN Client, as of this client version only PKCS#11 files can be loaded from the following locations: WINDIR, PROGRAMFILES and PROGRAMFILES(x86).

→ **Enhancement: VPN bypass and mobile radio**
When using a profile with the connection medium 'Mobile' configured, the domain configured via VPN bypass can now be used reliably again.

→ **Improvement: Automatic media detection**
The 'automatic media detection' now reliably selects LAN as the connection medium again when the device is connected to the LAN.

→ **Improvement: Stateful boot option**

→ **Improvement: Status display (PIN symbol) in connection with smartcards**

→ **Customization of the IKEv2 configuration payload**
The length of the IKEv2 configuration payload attribute type INTERNAL_IP6_ADDRESS has been changed from 16 bytes to 17 bytes. Accordingly, the prefix is now also transmitted in addition to the IPv6 address.

→ **Support for RFC7383 (IKEv2 message fragmentation)**

→ **Update to OpenSSL version 1.0.2zg**

Known limitations

→ **Option: 'Automatically open dialog for connection setup'.**
Under certain circumstances, the logon option 'Automatically open dialog for connection establishment' does not work reliably.

→ **Application-based VPN bypass configuration**
Configuring a DNS within the VPN bypass configuration will invalidate an application-based rule contained within it.

→ **PIN menu entries**
When using hardware certificates, the PIN menu items 'Enter/Reset/Change PIN' / 'Enter/Reset/Change PIN' have no function, but can be selected incorrectly.

→ **Seamless roaming**

Under certain circumstances, the VPN tunnel status remains at ‘Keep tunnel logical’ when switching from Wi-Fi to LAN and a functional connection via LAN is not established. This must be done by manually disconnecting and connecting.

→ **Home Zone and IPv6**

If the predefined Home Zone rule is active in the firewall settings of the VPN client, outgoing IPv6 packets to the local network are dropped in the defined Home Zone network.

Advanced VPN Client Windows 6.11 Rel Build 29631

New features

→ **New option: Resolve DNS domains in the tunnel**
The Split DNS functionality can be configured using the new 'DNS domains to be resolved in the tunnel' option. In the case of configured Split tunneling, the DNS requests of the configured domains are sent into the VPN tunnel. All other DNS requests bypass the VPN tunnel.

→ **Distribution of Split Tunneling Configurations**
The VPN client now supports RFC 7296 for distributing Split Tunneling configurations on the part of the VPN gateway.

Bugfixes / improvements

→ **New rights structure within 'C:\ProgramData\NCP\'.**
The write permissions within the 'C:\ProgramData\NCP\' directory have been limited to a minimum. For example, a user can now no longer store CA certificates in the designated directory. Likewise, the directory and rights structure has been rebuilt so that no application in the user and system context writes to the same directory.

→ **Improvements in server-side configured split DNS**

→ **The automatic Windows login works again.**

→ **Seamless roaming now also works with IPv6 destination addresses.**

→ **Saved VPN usernames are displayed correctly again after an AVC update.**

→ **Improved compatibility with third-party gateways when addressing via IPv6**

→ **Compatibility with third-party gateways in connection with 2-factor authentication / token entry has been improved**

→ **Various GUI optimizations**

→ **Update to zlib version 1.2.12**

→ **CVE-2022-0778 and CVE-2020-1971 have been fixed in OpenSSL.**

→ **Migration to TLS 1.2 (TLS 1.0 and 1.1 are no longer supported)**

→ **Update to cURL library 7.84.0**

→ **Changes to the DNS entries in the VPN bypass configuration work properly again.**

→ **Improvement of the 'Connect before Windows login' function**

→ **The forwarding of the split DNS configuration by the gateway (RFC 8598) is now supported.**

→ **The network connection works properly again after a client installation.**

→ **General improvements in INI file import**

→ **Implementation of RFC8598 (https://datatracker.ietf.org/doc/html/**

rfc8598)

Known limitations

→ **Option: 'Open dialog for connection automatically'.**
Under certain circumstances the logon option 'Automatically open dialog for connection establishment' does not work.

→ **Application-based VPN bypass configuration**
Configuring a DNS within the VPN bypass configuration will invalidate an application-based rule contained within it.

→ **PIN menu entries**
When using hardware certificates, the PIN menu item 'Enter/reset/change PIN' has no function, but can be selected by mistake.

→ **Seamless Roaming**
Under certain circumstances, the VPN tunnel status remains at 'Keep tunnel logical' when switching from WLAN to LAN and a functional connection via LAN is not established. This must be done by manually disconnecting and connecting.

→ **Home Zone and IPv6**
If the predefined Home Zone rule is active in the firewall settings of the VPN client, outgoing IPv6 packets to the local network are dropped in the defined Home Zone network.

Advanced VPN Client Windows 6.04 Rel Build 29378

New features

→ **Revised hotspot login**

As of this version 6.0 of the LANCOM Advanced VPN Client, the Chrome-based Microsoft Edge web browser is invoked by means of WebView2 runtime and used exclusively for the purpose of logging into a hotspot. The prerequisite for this is the installed WebView2 runtime (from version 94.0.992.31 or newer) within the operating system. The WebView2 runtime can be downloaded here: https://developer.microsoft.com/en-us/microsoft-edge/webview2/#download-section

→ **INI file import for max. 250 split tunneling networks**

For both IPv4 and IPv6, up to 250 split tunneling configurations each can be imported into the client via INI file.

→ **INI file import: New split DNS parameter**

The specific redirection of DNS requests into the VPN tunnel can now be configured by setting the 'DomainInTunnel' parameter with a max. length of 1023 characters in the import file.

→ **Support for WPA3 encryption**

The Wi-Fi Manager integrated in the LANCOM Advanced VPN Client can now also manage Wi-Fi networks encrypted with WPA3.

→ **Support for RFC 7296**

RFC 7296 defines the passing of split tunneling remote networks through the VPN gateway to the VPN client. This feature is supported as from this client version.

→ **Extension of the VPN status in the Windows registry**

Until now, the connection status of the LANCOM Advanced VPN Client could be set in the registry under 'Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\NCP engineering GmbH\NCP RWS/GA\6.0' for the parameter 'SecClCsi' could be read out with the values

0 = not connected

and

1 = connected

As from this version, the client stores additional statuses under the following location in the Windows registry:

HKEY_LOCAL_MACHINE\SOFTWARE\NCP engineering GmbH\NCP Secure Client

respectively

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\NCP engineering GmbH\NCP Secure Client

The associated ConnectState parameter can take the following values:

0 = Connection is disconnected
1 = Connection is established
2 = Connection has been successfully established
3 = Internet connection is interrupted, VPN connection is held
4 = Connection has been established, but only communication with the NCP Management Server is possible (licensing)

Bugfixes / improvements

→ **Revised file handling of ncp.db**
In rare cases, the 'ncp.db' file became unusable during operation, causing the client to lose its license.

→ **'Network Location Awareness' not available with active firewall**
If the client firewall is activated, the 'Network Location Awareness' of the Windows operating system is not available. In the case of the exclusively desired 'Friendly Network Detection' functionality, the 'Network Location Awareness' of the Windows operating system can be used by configuring a client firewall rule 'Allow all network traffic bidirectionally' and setting a registry key. For this purpose, the parameter 'RegDw "WscIntegration"=0' must be configured in the registry within 'HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ncprwsnt'. The default value of this parameter is '1'.

→ **Automatic login via credential provider**
When using the logon option with configured user credentials, a locked Windows workstation could be unlocked by selecting the credential provider.

→ **Troubleshooting multiple certificates with the same issuer and subject in the Windows certificate storage**
If the Windows certificate storage contains certificates with identical issuer and subject, the wrong, expired certificate may have been used by the client and acknowledged with the message "unable to get issuer certificate".

→ **Changed default value in FND options**
The default value for the 'Check for known networks periodically' option has been changed from 0 sec to 3600 sec.

→ **Incomplete log files**
Under certain circumstances, incorrect write accesses to the client log files occurred, so that log entries were missing in the worst case.

→ **Revised installation routine**
In rare cases, the network connection was completely disconnected after the end of the installation process, before the computer restarted. Furthermore, the ‘Repair program’ functionality within the MSI installation process was removed.

→ **Standby status in connection with IPv6**
After the standby state of the PC, there were connection problems with IPv6.

→ **Installation with certmgr.exe**
During the installation of the LANCOM Advanced VPN Client, the file ‘certmgr.exe’ created by Microsoft was used to install the vendor certificate. This file was detected as unsigned. As of this version, the newer ‘certutil.exe’ is used instead of ‘certmgr.exe’.

→ **Dynamic certificate selection**
The certificate selection has been decisively improved, moreover, only valid certificates will be imported in the future.

→ **Bug fix in ESP header for IPv6**

→ **Revised parameter locks in the client GUI**
Measures have been taken in the client GUI to ensure that locked buttons cannot be activated by certain tools, thereby making locked functions available.

→ **Fixed a misbehavior when connecting with HTTPS encapsulation and IPv6.**

→ **Improved FND compatibility with network switches**

→ **Optimization of the establishment of an IKEv2 connection with EAP**
In certain situations, establishing the VPN tunnel with IKEv2 and EAP could take an unusually long time.

→ **Improvement of VPN bypass compatibility with MS Teams**

Known limitations

→ **Option ‘Automatically open dialog for connection establishment’**
Under certain circumstances the logon option ‘Automatically open dialog for connection establishment’ does not work.

4. History Advanced VPN Client Windows version 5.x

Advanced VPN Client Windows 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 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 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 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 functionallity 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 remining 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 functionallity 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.

5. Common advice

Disclaimer

LANCOM Systems GmbH does not take any guarantee and liability for software not developed, manufactured or distributed by LANCOM Systems GmbH, especially not for shareware and other extraneous software.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de
www.lancom-systems.com