bintec Secure IPSec Client – Release Notes V. 6.04

1 Requirements

Microsoft Windows Operating Systems - The following Microsoft Windows operating systems are supported with this release:

- Windows 11, 64 bit (up to and including version 21H2)
- Windows 10, 64 bit (up to and including version 21H2)

Note that version 6 of the Secure Client requires a new license, also when upgrading from a previous version.

2 Removed functions

- The following connection media are no longer supported: Modem, xDSL, external dialer.

3 New features and enhancements

- **Revised hotspot login**
  Starting with this version 6.0 of the bintec elmeg Secure Client, the Chrome-based Microsoft Edge web browser is invoked by means of WebView2 runtime and used exclusively for the purpose of logging on to a hotspot. This requires that the WebView2 runtime (from version 94.0.992.31 or newer) is installed 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 remote 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.**
  A specific redirection of DNS requests into the VPN tunnel can be configured by setting the **DomainInTunnel** parameter in the INI import file with a max. string length of *1023*. The string contains a comma separated list of domain names to be resolved, e.g. :
  - *google.com* - all domains containing *google.com* are used, e.g. *www.test-google.com*
  - *. google.com* -all domains containing *.google.com* are used, e.g. news.google.com
  - *news.google.com* -all domains containing *news.google.com* are used.
- **Support for WPA3 encryption**
  The Wi-Fi Manager integrated in the Secure 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 RFC is supported as of this client version.
- **Extension of the VPN status in the Windows registry**
  Up to now the connection status of the Secure Client could be read out from the registry with **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\NCP engineering GmbH\NCP RWS/GA\6.0 -> SecClCsi** taking either of these values:
  0 = not connected
  1 = connected.
  As of this version, the client stores additional states under the following location in the Windows registry:
  HKEY_LOCAL_MACHINE\SOFTWARE\NCP engineering GmbH\NCP Secure Client or **HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\NCP engineering GmbH\NCP Secure Client**.
  The corresponding parameter **ConnectState** can have the following values:
  0 = Disconnected
  1 = Connection is being established
  2 = Connection has been established successfully

3 = Internet connection is interrupted, VPN connection is held
4 = Connection established, but only communication with the NCP Management Server is possible (licensing).

4 Improvements / bug fixes

- **Revised file handling of ncp.db**
  In rare cases, the **ncp.db** file became unusable during operation, causing the client to lose its license. This problem has been fixed.
- **Network Location Awareness not** available **with active NCP firewall**
  Network Location Awareness of the Windows operating system is not available when the client firewall is active. In the case of "Friendly Network Detection" is desired, 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 DWord **WscIntegration** = *0 must be* configured in the registry within **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ncprwsnt.** The default value of this parameter is *1*.
- ***Switch off Wi-Fi* option *when LAN cable is plugged in* - problem with Hyper-V**
  When Hyper-V functionality was in use, the Wi-Fi adapter was incorrectly disabled if the option **Turn off WLAN when LAN cable is plugged** was enabled. This problem has been fixed.
- **Automatic logon via credential provider**
  When using the logon option with configured user credentials, a locked Windows workstation could be unlocked by selecting the NCP Credential Provider. This problem has been fixed.
- **Troubleshooting multiple certificates with the same *issuer* and *subject* in the Windows certificate store**
  If the Windows certificate store contained certificates with identical **issuer** and **subject**, the wrong, expired certificate was sometimes used by the client and the message "unable to get issuer certificate" was issued. This problem has been fixed.
- **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, potentially resulting in missing log entries. This problem has been fixed.
- **Revised installation routine**
  In rare cases, the network connection was completely disconnected after the end of the installation process and before the computer restart. This problem has been fixed. Additionally, the **Repair program** option within the MSI installation process has been removed.
- **Error after standby state in connection with IPv6 fixed**
  After waking from a standby, there were connection problems with IPv6. This error has been fixed.
- **Problem during installation with certmgr.exe**
  During the installation of the Secure Client the file certmgr**.exe** created by Microsoft was used to install the NCP manufacturer certificate. This file was recognized as not signed. Starting from this version the newer **certutil.exe** is used instead of **certmgr.exe.** This has fixed the problem.
- **Dynamic certificate selection**
  The certificate selection has been significantly improved. In addition, 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 to make locked functions available.
- **Fixing a problem when connecting to VPN Path Finder via IPv6**
- **Improve FND compatibility with network switches**
- **Optimizing the establishment of an IKEv2 connection with EAP**
  In certain situations, establishing the VPN tunnel with IKEv2 and EAP could take unusually long. This problem has been fixed.
- **Improvement of VPN bypass compatibility with MS Teams**

5 Known limitations

- **Option *Automatically open dialog for connection establishment***
  Under certain circumstances, the logon option **Automatically open dialog for connection establishment** does not work.