bintec Secure IPSec Client – Release Notes V. 6.04

1 Voraussetzungen

Microsoft Windows Betriebssysteme - Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows 11, 64 Bit (bis einschließlich Version 21H2)
- Windows 10, 64 Bit (bis einschließlich Version 21H2)

Beachten Sie, dass die Version 6 des Secure Client eine neue Lizenz erfordert, auch wenn Sie von einer früheren Version upgraden.

2 Nicht mehr verfügbare Funktionen

- Folgende Verbindungsmedien werden nicht mehr unterstützt: Modem, xDSL, externe Dialer.

3 Neue Leistungsmerkmale und Erweiterungen

- **Überarbeitete Hotspot-Anmeldung**
  Ab dieser Version 6.0 des bintec elmeg Secure Clients wird der Chrome-basierte Microsoft-Edge-Webbrowser mittels WebView2-Runtime aufgerufen und ausschließlich für den Zweck der Anmeldung an einem Hotspot verwendet. Voraussetzung hierfür ist die installierte WebView2-Runtime (ab der Version 94.0.992.31 oder neuer) innerhalb des Betriebssystems. Die WebView2-Runtime kann hier heruntergeladen werden: *https://developer.microsoft.com/en-us/microsoft-edge/webview2/#download-section*
- **INI-Datei-Import für max. 250 Split-Tunneling-Remote-Netzwerke**
  Sowohl für IPv4 als auch für IPv6 können jeweils bis zu 250 Split-Tunneling-Konfigurationen via INI-Datei in den Client importiert werden.
- **INI-Datei-Import: Neuer Split-DNS-Parameter**
  Die gezielte Umleitung von DNS-Requests in den VPN-Tunnel kann durch Setzen des Parameters **DomainInTunnel** in der INI-Import-Datei mit einer max. String-Länge von *1023* konfiguriert werden. Der String enthält, via Komma separiert, die aufzulösenden Domainnamen; z. B.:
  - *google.com* - alle Domains, die *google.com* enthalten, werden verwendet, z. B. *www.test-google.com*
  - *.google.com* –alle Domains, die *.google.com* enthalten, werden verwendet, z. B. news.google.com
  - *news.google.com* –alle Domains, die *news.google.com* enthalten, werden verwendet.
- **Unterstützung der WPA3-Verschlüsselung**
  Der im Secure Client integrierte WLAN-Manager kann nun auch mit WPA3 verschlüsselte WLANs verwalten.
- **Unterstützung von RFC 7296**
  In RFC 7296 ist die Weitergabe von Split-Tunneling-Remote-Netzwerken durch das VPN Gateway an den VPN Client definiert. Dieses RFC wird ab dieser Client-Version unterstützt.
- **Erweiterung des VPN-Status in der Windows-Registry**
  Bisher ließ sich der Verbindungsstatus des Secure Clients in der Registry unter **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\NCP engineering GmbH\NCP RWS/GA\6.0 -> SecClCsi** mit den Werten
  0 = nicht verbunden
  und
  1 = verbunden
  auslesen. Ab dieser Version speichert der Client weitere Zustände unter folgendem Ort in der Windows-Registry ab:

HKEY_LOCAL_MACHINE\SOFTWARE\NCP engineering GmbH\NCP Secure Client bzw. **HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\NCP engineering GmbH\NCP Secure Client**.
Der zugehörige Parameter **ConnectState** kann dabei die folgenden Werte annehmen:
0 = Verbindung ist getrennt
1 = Verbindung wird aufgebaut
2 = Verbindung ist erfolgreich aufgebaut
3 = Internetverbindung ist unterbrochen, VPN-Verbindung wird gehalten
4 = Verbindung hergestellt, aber nur Kommunikation mit dem NCP Management Server möglich (Lizenzierung)

4 Verbesserungen / Fehlerbehebungen

- **Überarbeitetes Datei-Handling der ncp.db**
  In seltenen Fällen wurde die Datei **ncp.db** während des Betriebes unbrauchbar, wodurch der Client seine Lizenz verloren hatte. Dieses Problem wurde behoben.
- **Network Location Awareness bei aktiver NCP-Firewall nicht verfügbar**
  Bei aktivierter Client-Firewall ist die Network Location Awareness des Windows-Betriebssystems nicht verfügbar. Für den Fall der ausschließlich gewünschten „Friendly Network Detection"-Funktionalität kann durch Konfigurieren einer Client-Firewall-Regel „jeden Netzwerkverkehr bidirektional zulassen" und Setzen eines Registry Keys die Network Location Awareness des Windows-Betriebssystems genutzt werden. Hierzu ist in der Registry innerhalb **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ncprwsnt** das DWord **WscIntegration** = *0* zu konfigurieren. Der Standardwert dieses Parameters ist *1*.
- **Option *WLAN bei gestecktem LAN-Kabel ausschalten* - Problem mit Hyper-V**
  Bei genutzter Hyper-V-Funktionalität wurde der WLAN-Adapter fälschlicherweise deaktiviert, wenn die Option **WLAN bei gestecktem LAN-Kabel ausschalten** aktiviert war. Dieses Problem wurde behoben.
- **Automatische Anmeldung via Credential Provider**
  Bei Verwendung der Logon-Option mit konfigurierten User Credentials konnte ein gesperrter Windows-Arbeitsplatz durch Auswahl des NCP Credential Providers entsperrt werden. Dieses Problem wurde behoben.
- **Problembehebung bei mehreren Zertifikaten mit gleichem *Issuer* und *Subject* im Windows-Zertifikatsspeicher**
  Sind im Windows-Zertifikatsspeicher Zertifikate mit identischem **Issuer** und **Subject** enthalten, wurde unter Umständen das falsche, abgelaufene Zertifikat vom Client verwendet und mit der Meldung „unable to get issuer certificate" quittiert. Dieses Problem wurde behoben.
- **Geänderter Standardwert in den FND-Optionen**
  Der Standardwert für die Option **Auf bekannte Netze periodisch prüfen** wurde von *0* Sek. auf *3600* Sek. geändert.
- **Unvollständige Log-Dateien**
  Unter bestimmten Umständen kam es zu fehlerhaften Schreibzugriffen auf die Client-Log-Dateien, so dass im schlechtesten Fall Log-Einträge fehlten. Dieses Problem wurde behoben.
- **Überarbeitete Installationsroutine**
  In seltenen Fällen wurde nach Ende des Installationsvorganges und vor dem Rechner-Neustart die Netzwerkverbindung komplett getrennt. Dieses Problem wurde behoben. Des Weiteren wurde innerhalb des MSI-Installationsvorganges die Option **Programm reparieren** entfernt.
- **Fehler nach dem Standby-Zustand in Verbindung mit IPv6 behoben**
  Nach dem Standby-Zustand des PCs kam es mit IPv6 zu Verbindungsproblemen. Dieser Fehler wurde behoben.
- **Problem bei der Installation mit certmgr.exe**
  Bei der Installation des Secure Clients wurde die von Microsoft erstellte Datei **certmgr.exe** zur Installation des NCP-Herstellerzertifikates verwendet. Diese Datei wurde als nicht signiert erkannt. Ab dieser Version wird anstatt **certmgr.exe** die neuere **certutil.exe** verwendet. Das Problem wurde dadurch behoben.
- **Dynamische Zertifikatsauswahl**
  Die Zertifikatsauswahl wurde entscheidend verbessert, zudem werden künftig nur gültige Zertifikate importiert.
- **Fehlerbehebung im ESP-Header für IPv6**

- **Überarbeitete Parametersperren in der Client-GUI**
  In der Client-GUI wurden dahingehend Maßnahmen getroffen, dass gesperrte Schaltflächen sich nicht durch bestimmte Tools aktivieren lassen und dadurch gesperrte Funktionen zur Verfügung gestellt werden.
- **Behebung eines Problems beim Verbindungsaufbau mit VPN Path Finder via IPv6**
- **Verbesserung der FND-Kompatibilität zu Netzwerk-Switches**
- **Optimierung des Aufbaus einer IKEv2-Verbindung mit EAP**
  In bestimmten Situationen konnte der Aufbau des VPN-Tunnels mit IKEv2 und EAP ungewöhnlich lang dauern. Dieses Problem wurde behoben.
- **Verbesserung der VPN-Bypass-Kompatibilität zu MS Teams**

5 Bekannte Einschränkungen

- **Option *Dialog für Verbindungsaufbau automatisch Öffnen***
  Unter bestimmten Umständen funktioniert die Logon-Option **Dialog für Verbindungsaufbau automatisch öffnen** nicht.