Release Notes

Service Release: **3.11 r32792**
Datum: **November 2016**

Voraussetzungen

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

- Windows 10 32/64 Bit
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit
- Windows Vista, 32/64 Bit

Neue Lizenzschlüssel ab Version 3.10

Software Update und Lizenzschlüssel
Ab der aktuellen Software-Version benötigt jedes zukünftige Major Release der Software einen neuen Lizenzschlüssel gleicher Version.
Erfolgt das Software Update ohne nachfolgendes Lizenz Update so kann der Client nur für die Restlaufzeit der 30-Tage-Testversion bis zum Erhalt der neuen Lizenz für die neue Version betrieben werden.
Neue Installation und Lizenzschlüssel
Bei Neu-Installationen wird die Client Software standardmäßig im Verzeichnis „Programme“ (vorher „Programme (x86)“) installiert und als Testversion (max. 30 Tage) bis zur Eingabe der passenden Lizenz für die neue Version betrieben.

1. Neue Leistungsmerkmale und Erweiterungen

VPN-Bypass

Die VPN-Bypass-Funktion gestattet Anwendungen festzulegen, die trotz deaktiviertem Split Tunneling außerhalb der VPN-Konfiguration direkt ins Internet kommunizieren dürfen. Alternativ ist es möglich, Domänen bzw. Zieladressen zu bestimmen, zu denen die Datenkommunikation am VPN-Tunnel vorbei stattfinden soll.
Diese Funktion kann unter anderem dazu genutzt werden, um regelmäßig notwendige, nicht sicherheitsrelevante Datenübertragung von der zentralen Infrastruktur fernzuhalten, um deren Performance nicht zu beeinträchtigen. Zum Beispiel könnten Updates des Betriebssystems oder des Virenscanners (mit bekannter Domäne) ohne Umweg über die VPN-Verbindung zugelassen werden, oder bei bestimmten Cloud-Services der direkte Zugriff einer Anwendungen über das Internet ermöglicht werden.
Die Konfiguration erfolgt über den Client-Monitor über „Konfiguration / VPN-Bypass“ und in den Profileinstellungen unter „Split Tunneling / VPN-Bypassliste“.

Home Zone

Die Funktionalität der Home Zone wurde als Option in der Firewall implementiert, um auch die Ressourcen eines Heimnetzwerks zur Verfügung stellen zu können, ohne dass die Administration jedes einzelne IP-Netz im Home-Office seiner Mitarbeiter kennen muss.
Die Aktivierung erfolgt in den Firewall-Einstellungen unter „Optionen“ und in den Firewall-Grundeinstellungen. Gesetzt und gelöscht wird die Home Zone im Verbinden-Menü des Client-Monitors durch den Anwender.

Auswahl eines Benutzer- oder Computer-Zertifikats im Windows-CSP

Im Konfigurationsmenü des Clients unter „Zertifikate“ kann anhand der Erweiterten Schlüsselverwendung (Extended Key Usage) die Auswahl eines bestimmten Benutzer- oder Computer-Zertifikats voreingestellt werden.

Ausgabe des MediaType mit dem Tool ncpclientcmd.exe

Das Kommandozeilen-Tool „ncpclientcmd.exe“ zeigt bei Eingabe des Kommandos „NcpClientCmd /getConnecionMedium“ das Verbindungsmedium bzw. den MediaType an.

Neues Produkt- und Status-Icon

Mit dieser Version wurden die Icons modernisiert.
Die Farben des Status-Icons wechseln beim Verbindungsaufbau von rot nach grün.
Die Darstellung der Firewall als Linie unter „VPN“ zeigt, ob die Firewall aktiv ist und ob sich der Client in einem bekannten oder fremden Netz befindet.

Projekt-Icon	*Status-Icons* ohne VPN-Tunnel	Tunnel-aufbau	logischen Tunnel halten	Tunnel aufgebaut	
					Firewall aus
					aktive Firewall erkennt: Client befindet sich in einem fremden/unfreundlichen Netz
					aktive Firewall erkennt: Client befindet sich in einem bekannten/freundlichen Netz

IKEv2 Signature Authentication nach RFC 7427

Die Client Software unterstützt für den IKEv2 die zertifikatsbasierte Authentisierung nach RFC 7427, womit auch modernes Padding-Verfahren (RSASSA-PSS) möglich ist.

2. Verbesserungen / Fehlerbehebungen

Unterstützung von mehr als zwei FND-Servern

Die Begrenzung der Anzahl von optionalen FND-Servern erfolgt ausschließlich durch die maximale Anzahl der Zeichen im Eingabefeld der GUI, die auf 255 Zeichen beschränkt ist. Folgende Eingabe von drei durch Komma getrennten Adressen wird unterstützt:
fe80::e568:8a83:203c:55c0,192.16.15.57,fnd2.ncp.de,192.16.15.56

Fehlerkorrektur bei Hotspot-Anmeldung

Der Client gibt beim Aufruf die aktuelle Versionsnummer des installierten Internet Explorers für die Überprüfung am Hotspot mit, sodass die Anmeldung unmittelbar fehlerfrei erfolgt.

Firewall blockierte IPv6 IKE Pakete

Bisher wurde in der Firewall-Oberfläche mit der Aktivierung der Funktion „IPsec Protokoll zulassen (500, 4500, ESP, 443)“ nur der VPN-Aufbau mit IPv4 unterstützt. Jetzt kann mit dem Schalter sowohl der Tunnelaufbau mit IPv4 als auch der mit IPv6 erfolgen.

Fehlerbehebung bei alternativem IPsec Port

Der VPN-Verbindungsaufbau funktioniert mit der Firewall-Option „IPsec-Protokoll (ESP, UDP) und VPN Path Finder…zulassen“ nun auch, wenn ein alternativer IPsec Port konfiguriert wurde.

Ein- und Ausschalten des Credential Providers

Ab dieser Version kann das Feature des Windows Prelogon mit dem Credential Provider nicht mehr während der Software-Installation ausgewählt werden. Das Ein- und Ausschalten des Credential Providers ist nur noch über das Monitormenü „Konfiguration“ unter „Logon-Optionen“ möglich.

3. Bekannte Einschränkungen

Keine

Release Notes

bintec elmeg IPSec Secure Client (Win32/64)

Major Release: **3.10**
Datum: **April 2016**

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme sind mit diesem Release unterstützt:

- Windows 10 32/64 Bit
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit
- Windows Vista, 32/64 Bit

Neue Lizenzschlüssel ab Version 3.10

Software Update und Lizenzschlüssel

Ab der aktuellen Software-Version benötigt jedes zukünftige Major Release der Software einen neuen Lizenzschlüssel gleicher Version.

Erfolgt das Software Update ohne nachfolgendes Lizenz Update so kann der Client nur für die Restlaufzeit der 30-Tage-Testversion bis zum Erhalt der neuen Lizenz für die neue Version betrieben werden.

Neue Installation und Lizenzschlüssel

Bei Neu-Installationen wird die Client Software standardmäßig im Verzeichnis „Programme" (vorher „Programme (x86)") installiert und als Testversion (max. 30 Tage) bis zur Eingabe der passenden Lizenz für die neue Version betrieben.

Windows 10 Update 1511 (Threshold 2/Build 10586) führt zu Problemen mit installiertem NCP Secure Client

Das November-Update von Microsoft für Windows 10 ist weit mehr als nur die Sammlung einiger Patches oder Erweiterungen sondern prinzipiell eine runderneuerte Version von Windows 10. Im Zuge des Updates werden Bereiche der Registrierungsdatenbank umgeschrieben und einige für den bintec elmeg IPSec Secure Client wichtige Einträge gehen während dieses Vorgangs verloren.

Um dieses Problem zu beheben und die nicht übernommenen Schlüssel und zugehörigen Werte neu zu schreiben, ist eine Deinstallation und nach einem anschließenden obligatorischen Neustart des Systems erneute Installation des bintec elmeg IPSec Secure Client notwendig. (Bestätigen Sie bei der Deinstallation **nicht** die Option „Alle Dateien löschen").

Dabei bleibt die Konfiguration komplett erhalten, jedoch müssen die Lizenzinformationen erneut eingegeben werden. Nach diesem Vorgang ist der bintec elmeg IPSec Secure Client wieder ohne Einschränkungen einsatzbereit.

1. Neue Leistungsmerkmale und Erweiterungen

Neue Hotspot-Anmeldung

Innerhalb der neuen Hotspot-Anmeldung entfällt die zugehörige Konfiguration. Der Client erkennt potenziell verfügbare Hotspots und bietet dem Anwender in der Client GUI die Anmeldung daran an. Startet der Anwender die Hotspot-Anmeldung, so erscheint der bintec elmeg IPSec Secure Client WLAN-Manager, womit der Anwender das gewünschte WLAN-Netz auswählen und die Anmeldung daran starten kann. Sobald die WLAN-Verbindung aufgebaut ist prüft der Client periodisch diese Verbindung auf Zugriff ins Internet. Ist kein Internetzugang verfügbar, startet der Client einen funktionsreduzierten Webbrowser ohne Adressleiste. Hat sich der Anwender erfolgreich am

Eingangsportal des Hotspot-Betreibers angemeldet, wird der Aufbau des VPN-Tunnels automatisch gestartet, sobald der Zugang ins Internet möglich ist.

Erhöhung der Kompatibilität zu Gateways anderer Hersteller

Der Secure Client unterstützt IKEv2 Redirect (RFC 5685). Damit können Load Balancing-Funktionen anderer Hersteller genutzt werden.

Überwachung des Filtertreibers durch den Secure Client

Erkennt der Client eine Fehlfunktion des Filtertreibers, so wird diese selbsttätig behoben und der Anwender aufgefordert einen Neustart durchzuführen.

Verwendung von Half-Routes und Default Gateways unter Windows 10

Die Client Software verwendet in der Standardeinstellung für den virtuellen Netzwerkadapter „Half-Routes". Durch einen Registry-Eintrag kann auf die Verwendung von „Default Gateways" umgestellt werden. Der Registry Key hierfür lautet:
Pfad:
`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ncprwsnt]`
Schlüssel:
`EnableDefGw = 1`
Type:
`REG_DWORD`

Ist der Registry-Eintrag `EnableDefGw` nicht vorhanden oder `EnableDefGw=0` gesetzt, werden Half-Routes verwendet.

2. Verbesserungen / Fehlerbehebungen

Stabilitätsverbesserungen

Die Stabilität des NCPRWSNT-Dienstes und des Update-Clients wurde verbessert.

Erweiterungen der Log-Meldungen

Die Log-Ausgaben für das PKI-Umfeld und den ncpsec-Dienst wurden erweitert.

Funktionsfähigkeit des WLAN-Moduls

Bei einer großen Anzahl von WLAN-Profilen (über 56) war die Funktion des WLAN-Adapters beeinträchtigt und der Adapter wurde im WLAN-Management nicht mehr angezeigt. Dieser Fehler ist behoben.

Windows Pre-Logon

Die Windows Pre-Logon-Funktionalität (Credential Provider) wurde für Windows 10 angepasst.

3. Bekannte Einschränkungen

Keine