

## NCP Secure Client – Juniper Edition

**Release: 10.04 r38728**

**Datum: März 2018**

### Voraussetzungen

#### Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme sind mit diesem Release unterstützt:

- Windows 10 32/64 Bit Version 1709
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit
- Windows Vista, 32/64 Bit

### 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 NCP 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 NCP Secure Clients 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 NCP Secure Client wieder ohne Einschränkungen einsatzbereit.

### Hinweis zum Betrieb des Secure Clients unter Windows 10

Zum Betrieb des Clients ist ein Produktschlüssel der Version 10.x nötig.

### Hinweis zu einem Betriebssystem-Update auf Windows 10

Bei einem Update des Betriebssystems Windows 7, Windows 8 oder Windows 8.1 auf die Version Windows 10 ist darauf zu achten, dass der NCP Secure Client unbedingt vor dem Windows-Update deinstalliert wird.

Dabei wird empfohlen die Konfigurationsdatei sowie verwendete Zertifikate separat zu sichern.

Erst nachdem das Update auf Windows 10 abgeschlossen wurde, sollte die neueste Version der NCP Secure Clients (10.02 oder höher) installiert werden.

## 1. Neue Leistungsmerkmale und Erweiterungen

Keine

## 2. Verbesserungen / Fehlerbehebungen

### Änderung des NCP Netzwerktreibertyps für Windows 10

Durch Änderung des NCP Netzwerktreibertyps von „Ethernet Adapter“ zu „Virtual Adapter“ unter Windows 10 konnte das Problem gelöst werden, dass bei aufgebauter VPN-Verbindung über WLAN die WLAN-Adapter vom Betriebssystem ausgeschaltet wurden, wenn diese nicht über den NCP WLAN-Manager verwaltet wurden.

### Optimierung des NDIS-Treibers für Windows 10

Durch die Optimierung des NDIS-Treibers kann bei Verwendung von Windows 10 ein fehlerhaftes Verhalten beim Verbindungsaufbau nach dem Erwachen aus dem Sleep-Modus ausgeschlossen werden.

### Client-Firewall Statusrückmeldung an das Windows-Betriebssystem

Eine aktive Client-Firewall wird im Windows-Betriebssystem an entsprechender Stelle (z.B. „Sicherheit und Wartung“) angezeigt.

### Instabilität nach Microsoft Patches für Windows 7 64 Bit

Die Microsoft Patches KB4057400, KB4074598 oder KB4075211 adressieren das Handling von SmartCards bzw. der darauf befindlichen Zertifikate zur Benutzer-Authentisierung. Der im NCP Secure Client enthaltene NCP Client PKI Support-Dienst (ncpsec-Dienst) zeichnet sich ebenso für PKI-Funktionalitäten verantwortlich. Er wird mit dem Betriebssystemstart automatisch gestartet.

Unter Windows 7 64 Bit bewirkt das Einspielen der Microsoft Patches jedoch, dass der NCP Client PKI Support-Dienst nicht mehr korrekt starten kann und damit PKI-Funktionalitäten im NCP Secure Client nicht fehlerfrei arbeiten. Dieses Problem ist nun behoben.

## 3. Bekannte Einschränkungen

Keine

**Release:** 10.04 r31799  
**Datum:** August 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

## 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 NCP 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 NCP Secure Clients 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 NCP Secure Client wieder ohne Einschränkungen einsatzbereit.

## Hinweis zum Betrieb des Secure Clients unter Windows 10

Zum Betrieb des Clients ist ein Produktschlüssel der Version 10.x nötig.

## Hinweis zu einem Betriebssystem-Update auf Windows 10

Bei einem Update des Betriebssystems Windows 7, Windows 8 oder Windows 8.1 auf die Version Windows 10 ist darauf zu achten, dass der NCP Secure Client unbedingt vor dem Windows-Update deinstalliert wird.

Dabei wird empfohlen die Konfigurationsdatei sowie verwendete Zertifikate separat zu sichern.

Erst nachdem das Update auf Windows 10 abgeschlossen wurde, sollte die neueste Version der NCP Secure Clients (10.02 oder höher) installiert werden.

## 1. Neue Leistungsmerkmale und Erweiterungen

Keine

## 2. Verbesserungen / Fehlerbehebungen

### Lizenzverlust

Unter bestimmten Voraussetzungen konnte die Aktivierung des Clients verloren gehen, nachdem ein Neustart durchgeführt wurde. Diese Einschränkung wurde behoben.

### Einschränkung der Netzwerkverbindung

Nach einer Installation oder einem Update des NCP Secure Clients war die Netzwerkverbindung bis zu

einem anschließenden Neustart nicht verfügbar. Ab diesem Wartungsrelease ist die Netzwerkverbindung nach der Installation oder dem Update des NCP Secure Clients weiterhin vorhanden.

### 3. Bekannte Einschränkungen

Keine

**Release:** 10.04 r31256  
**Datum:** August 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

## 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 NCP 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 NCP Secure Clients 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 NCP Secure Client wieder ohne Einschränkungen einsatzbereit.

## Hinweis zum Betrieb des Secure Clients unter Windows 10

Zum Betrieb des Clients ist ein Produktschlüssel der Version 10.x nötig.

## Hinweis zu einem Betriebssystem-Update auf Windows 10

Bei einem Update des Betriebssystems Windows 7, Windows 8 oder Windows 8.1 auf die Version Windows 10 ist darauf zu achten, dass der NCP Secure Client unbedingt vor dem Windows-Update deinstalliert wird.

Dabei wird empfohlen die Konfigurationsdatei sowie verwendete Zertifikate separat zu sichern.

Erst nachdem das Update auf Windows 10 abgeschlossen wurde, sollte die neueste Version der NCP Secure Clients (10.02 oder höher) installiert werden.

## 1. Neue Leistungsmerkmale und Erweiterungen

Keine

## 2. Verbesserungen / Fehlerbehebungen

### Angepasste Treibersignatur (zu Anniversary Update Version 1607, Build 14393.10)

Wurde das Anniversary Update von Windows 10 durchgeführt, schlug eine Neuinstallation älterer NCP Secure Clients fehl, wenn im BIOS/UEFI des Rechners „Secure Boot“ aktiviert ist. Der Grund hierfür besteht darin, dass Windows 10 nach dem Anniversary Update einen durch Microsoft signierten Treiber zwingend voraussetzt.

Mit diesem Release des NCP Secure Clients (10.10 r31256) wird bei allen unterstützten Windows-Systemen während der Installation der Treiber mit der passenden Signatur aufgespielt.

Die Aktualisierung von Windows 10 auf das Anniversary Update bei bereits installiertem NCP Secure Client hat keine Auswirkungen auf die Funktion des Clients.

### **Korrektur bei der Zuweisung von IP-Adressen der DNS-Server**

Die IP-Adress-Einträge der DNS-Server wurden bei VPN-Zugriffen von Clients auf verschiedene Gegenstellen nicht immer korrekt aktualisiert. In besonderen Fällen traten deshalb Verbindungsfehler auf.

## **3. Bekannte Einschränkungen**

Keine

## **4. Hinweise zum NCP Secure Client – Juniper Edition**

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:

<http://www.ncp-e.com/de/produkte/juniper-vpn-client.html>

E-Mail: [juniperhelpdesk@ncp-e.com](mailto:juniperhelpdesk@ncp-e.com)

**Release: 10.04 Build 26745**  
**Datum: November 2015**

## 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

## 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 NCP 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 NCP Secure Clients 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 NCP Secure Client wieder ohne Einschränkungen einsatzbereit.

## Hinweis zum Betrieb des Secure Clients unter Windows 10

Zum Betrieb des Clients ist ein Produktschlüssel der Version 10.x nötig.

## Hinweis zu einem Betriebssystem-Update auf Windows 10

Bei einem Update des Betriebssystems Windows 7, Windows 8 oder Windows 8.1 auf die Version Windows 10 ist darauf zu achten, dass der NCP Secure Client unbedingt vor dem Windows-Update deinstalliert wird.

Dabei wird empfohlen die Konfigurationsdatei sowie verwendete Zertifikate separat zu sichern.

Erst nachdem das Update auf Windows 10 abgeschlossen wurde, sollte die neueste Version der NCP Secure Clients (10.02 oder höher) installiert werden.

## 1. Neue Leistungsmerkmale und Erweiterungen

Keine

## 2. Verbesserungen / Fehlerbehebungen

### Korrekturen zur Installation

Es konnte bei der Installation des Clients zu einem Rollback während der Einrichtung des Filtertreibers kommen. Dies wurde durch Anpassung der Setup-Informationen korrigiert.

### Split Tunneling

Fehlerbehebung im Bereich Split Tunneling sofern das Remote Netzwerk denselben IP-Adressbereich hatte wie das lokale Netzwerk des Anwenders. So wurde nach einem VPN-Profilwechsel die Route in das lokale Netzwerk gelöscht.



## Profilimport

Der Verbindungsmodus ConnMode=2, der den Verbindungsmodus „wechselnd“ (automatischen Modus manuell starten) bezeichnet, wurde beim Profilimport nicht importiert. Dieser Fehler ist behoben.

### 3. Bekannte Einschränkungen

Keine

### 4. Hinweise zum NCP Secure Client – Juniper Edition

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:

<http://www.ncp-e.com/de/produkte/juniper-vpn-client.html>

E-Mail: [juniperhelpdesk@ncp-e.com](mailto:juniperhelpdesk@ncp-e.com)



**Release: 10.00 Build 21336**  
**Datum: Januar 2015**

## Voraussetzungen

### Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme sind mit diesem Release unterstützt:

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

## 1. Neue Leistungsmerkmale und Erweiterungen

### MSI-Installer – Update auf die NCP Secure Entry Client Version 10.0

Der NCP Secure Client – Juniper Edition wird ab Version 10.00 im Microsoft-Format MSI ausgeliefert. Die Einführung des neuen Formats erfordert folgendes Vorgehen:

- Clients einer früheren Version als 10.x müssen deinstalliert werden. Anschließend kann die Neu-Installation mit dem MSI-Paket auf dem Endgerät erfolgen. Im Weiteren können neue Versionen via MSI-Update-Funktionalität eingespielt werden.

### Modi des Verbindungsaufbaus

Die Auswahl für die Voreinstellungen des VPN-Verbindungsaufbaus wurde um zwei Modi erweitert. Zusätzlich wurden die Auswahlmöglichkeiten detaillierter benannt. Folgende Optionen für den Verbindungsaufbau stehen nun zur Verfügung:

#### manuell / (Standardeinstellung des Verbindungsmodus)

Unter dieser Einstellung muss die VPN-Verbindung vom Anwender über den Schalter in der Benutzeroberfläche manuell hergestellt werden. Ein Trennen der Verbindung erfolgt je nach eingestelltem Wert für den Timeout. Ist der Timeout auf Null (0) gesetzt, d. h. kein Timeout eingestellt, muss die Verbindung manuell getrennt werden.

#### automatisch (Datenverkehr initiiert VPN-Verbindung)

Dies bedeutet, dass die Client Software die Verbindung zum Zielsystem automatisch herstellt sobald ein Datentransfer ansteht. Das Trennen der Verbindung erfolgt je nach Protokoll Ihres Systems, entsprechend den Anforderungen der Anwendung und den Einstellungen des Profils.

#### immer

Mit dieser Einstellung wird unmittelbar nach dem Start des Clients ständig der VPN-Verbindungsaufbau angeregt. Dies erfolgt unabhängig vom Betätigen des Verbinden-Buttons, unabhängig von anstehendem Datenverkehr und unabhängig von der Darstellung des Monitors, die unter Autostart eingestellt werden kann.

#### wechselnd (automatischen Modus manuell starten)

Wird dieser Modus gewählt, muss zunächst die Verbindung "manuell" aufgebaut werden. Danach wechselt der Modus je nach Art des Verbindungsabbaus:

- Wird die Verbindung mit Timeout also automatisch beendet, so wird die Verbindung für den nächsten Datentransfer wieder automatisch hergestellt;
- wird die Verbindung manuell abgebaut, muss sie auch wieder manuell aufgebaut werden.

Ist der Timeout auf Null (0) gesetzt, d. h. kein Timeout eingestellt, müssen Sie in jedem Fall die Verbindung manuell trennen.

Wichtig: Sollten Sie den Verbindungsaufbau auf "manuell" umschalten, so sollten Sie den Timeout aktivieren und auf einen anderen Wert als null (0) setzen, um den Verbindungsabbau zu automatisieren.

## wechselnd (Immer-Modus manuell starten)

Ist dieser Modus eingestellt, wird mit dem einmaligen Betätigen des Verbinden-Buttons der beständige Verbindungsaufbau "immer" angeregt. Dies erfolgt für die gesamte Betriebszeit des Monitors bis zu dessen Beenden.

## Erweiterte Log-Einstellungen

In den erweiterten Log-Einstellungen, unter „Hilfe / Erweiterte Log-Einstellungen“ im Monitormenü, kann der Zyklus bzw. die maximale Anzahl der gespeicherten Log-Dateien verändert werden.

Die Aufrufe der Kommandozeilen-Tools RWSCMD und NcpClientCmd inklusive der eingesetzten Parameter können in eine Logdatei geschrieben werden. Dazu müssen diese Anwendungen in den erweiterten Log-Einstellungen aktiviert werden. Alternativ kann dies auch über die NCPMON.INI mit der Zeile "[RWSCMD]Logs=1" angeregt werden. Die Logausgabe erfolgt als "RwscmdLog.txt" in das Log-Verzeichnis.

## Erweiterung des Support-Assistenten

Der Support-Assistent wurde erweitert, damit jetzt auch die Log-Dateien von Microsoft für die Treiber-Installation hinzugefügt werden können.

Folgende Dateien werden dann hinzugefügt falls sie vorhanden sind:

WINDOWSDIR\inf\setupapi.dev.log

WINDOWSDIR\inf\setupapi.app.log

WINDOWSDIR\inf\setupapi.setup.log

## Optimierte IKEv2-Konfiguration

Der Client-Monitor bietet in den IPsec-Einstellungen (unter „Konfiguration“) die Möglichkeit für IKEv2 eigene Richtlinien anzulegen. Nach diesen Richtlinien erfolgt der IKEv2-Schlüsselaustausch.

Die weitere IKEv2-Konfiguration befindet sich in der Standard-Profilkonfiguration. Hier kann die zugehörige Authentisierung – Zertifikat, Pre-shared Key oder EAP – konfiguriert werden.

Entsprechend der gewählten Authentisierungsmethode werden Eingabefelder für VPN-Benutzername und Passwort bzw. die IKE-ID ein- oder ausgeblendet.

In den Profil-Einstellungen unter „IPsec“ wird die gewünschte IKEv2-Richtlinie selektiert, sofern nicht der automatische Modus gewählt wird.

Über den Editor-Button kann von der IPsec-Konfiguration der Profil-Einstellungen direkt zur Konfiguration der Richtlinien gewechselt werden.

## MSI-Installer – NCP spezifische Funktionen

### Beim Installieren eine CNF-Datei hinzufügen

Bei der Installation des MSI-Pakets kann weiterhin eine CNF-Datei mit installiert werden. Musste beim früheren Setup die CNF-Datei in das Disk1-Verzeichnis kopiert werden, kopiert der Installer die CNF-Datei nun selbständig in das Installationsverzeichnis, sobald er sie in dem Verzeichnis findet, in dem auch das MSI-Paket oder der Installer als EXE-Datei liegt. Der Rückgabewert beim Kopieren wird nicht berücksichtigt. Bei einem Fehler bricht die Installation nicht ab.

### Beim Installieren zusätzliche Dateien hinzufügen

Zusätzliche Dateien können zum Beispiel eigene Zertifikate oder Dateien für ein kundenspezifisches Projekt-Logo (CBO) sein, welche mit dem Setup installiert werden sollen.

Früher wurde im Disk1-Verzeichnis ein Unterverzeichnis **ncple** angelegt, woraus alle Dateien inklusive Unterverzeichnisse entnommen und in das Installationsverzeichnis mit installiert wurden.

Dies erfolgt jetzt anders. Findet der Installer im Verzeichnis in dem sich auch das MSI-Paket oder der Installer als EXE-Datei befindet das Verzeichnis **IMPORTDIR**, werden aus diesem Verzeichnis alle Dateien rekursiv, inklusive aller Unterverzeichnisse, ins Installationsverzeichnis mit installiert. Der

Rückgabewert beim Kopieren wird nicht berücksichtigt. Bei einem Fehler bricht die Installation nicht ab. Da diese Dateien der Installer nicht kennt werden diese weder aktualisiert noch deinstalliert.

Eine weitere Möglichkeit Dateien, Icons, Registry-Einträge, usw. einer Installation hinzufügen ist der Weg über eine Transform-Datei. Hierfür kann über Admin-Tools diverser Hersteller (z.B. InstallShield, SuperOrca) das MSI-Paket geöffnet werden, beliebige Features, Komponenten, Dateien usw. hinzugefügt werden und eine Transform-Datei erstellt wird, welche bei der Installation übergeben wird.

```
msiexec /i myproduct.msi TRANSFORM=mytransform.mst
```

Dies ist der offizielle Weg, ein bestehendes MSI-Paket zu ergänzen. Vorteil ist, dass diese Ergänzungen dem Installer bekannt sind und er diese aktualisieren und deinstallieren kann.

## Beim Installieren eine Batch-Datei ausführen

Findet der Installer im Verzeichnis in dem sich auch das MSI-Paket oder der Installer als EXE-Datei befindet die Datei **NcpInstall.bat**, wird diese vom Installer am Ende der Installation ausgeführt. Der Rückgabewert wird nicht berücksichtigt. Tritt bei der Ausführung der Batch-Datei ein Fehler auf, so bricht die Installation nicht ab. Die Ausführungen sind dem Installer nicht bekannt und er kann diese auch nicht verwalten.

## Testversion sofort starten

In manchen Projekten besteht der Wunsch, dass beim ersten Start des Monitors die Testversion ohne Abfrage „Testversion jetzt starten?“ sofort gestartet wird. Dies wird jetzt über den Kommandozeilenparameter „STARTTESTVERSION=1“ ermöglicht:

```
msiexec /i myproduct.msi STARTTESTVERSION=1
```

## Silent Installation und Deinstallation

Die frühere Silent Installation wird durch eine neue Form ersetzt, wobei der Windows Installer eingesetzt wird. Er unterstützt eine eigene Silent Installation, welche über die Anzeigeeoptionen angegeben werden kann. Z.B.: `msiexec /i myproduct.msi /qn myproduct.exe /v"/qn"`

Die frühere Form der Silent Deinstallation wird abgelöst über eine, welche über die Anzeigeeoptionen durchgeführt wird. Z.B.: `msiexec /x myproduct.msi /qn`

## Protokollierung

Früher konnte über die NCP-spezifische SetupExt.ini ein Teil des Setups protokolliert werden. Jetzt gestattet der Windows Installer eine eigene sehr umfangreiche Protokollierung. Über die Protokollierungsoptionen kann diese konfiguriert werden.

Z.B.: `msiexec /i myproduct.msi /log "c:\temp\myinstall.log"`  
`myproduct.exe /v"/log "c:\temp\myinstall.log"`

## MSI-Datei extrahieren

Die MSI-Datei ist in der bereitgestellten EXE-Datei enthalten. Sie kann durch folgende Eingabe aus der EXE-Datei extrahiert werden:

```
setup.exe /b"C:\FolderInWhichMSIWillBeExtracted"
```

Das gestartete Installations-Setup kann nun abgebrochen werden und die MSI-Datei aus dem angegebenen Verzeichnis verwendet werden. Für die Softwareverteilung darf die MSI-Datei nicht umbenannt werden, da es im Update-Fall hier zu Fehlersituationen kommen kann. Aus diesem Grund stellt NCP ausschließlich die ausführbare EXE-Datei zur Verfügung, die im Dateinamen auch die aktuelle Version enthält. Die aktuelle Version ist im Namen der MSI-Datei nicht enthalten.

## Bei Deinstallation alle Dateien löschen

Früher wurde bei der Deinstallation über die GUI im letzten Dialog abgefragt, ob die persönlichen Daten gelöscht werden sollen, bevor sie entfernt wurden. Bei der Silent-Deinstallation konnte das Attribut `-delall` angegeben werden.

Dies ändert sich jetzt mit der Art der Deinstallation. Wird der Client mit dem Assistenten deinstalliert, erfolgt die Abfrage, ob alle Dateien entfernt werden sollen, bevor dies erfolgt. Wird er direkt deinstalliert (kleiner Dialog), erfolgt keine Abfrage und die persönlichen Daten bleiben erhalten. In diesem Fall kann über die Kommandozeile die Eigenschaft DELETEALL=1 gesetzt werden, damit alle Dateien entfernt werden. Z.B.: `msiexec /x myproduct.msi DELETEALL=1`

## 2. Verbesserungen / Fehlerbehebungen

### OpenSSL Version 1.0.1j

In der Client Software wird OpenSSL 1.0.1j eingesetzt. Sicherheitsdefizite in Verbindung mit früheren Versionen der OpenSSL Libraries sind damit behoben.

## 3. Bekannte Einschränkungen

keine

## 4. Hinweise zum NCP Secure Client – Juniper Edition

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:

<http://www.ncp-e.com/de/produkte/juniper-vpn-client.html>

E-Mail: [juniperhelpdesk@ncp-e.com](mailto:juniperhelpdesk@ncp-e.com)

## 5. Leistungsmerkmale

### Betriebssysteme

Microsoft Windows (32 und 64 Bit): Windows 8, Windows 7, Windows Vista, Windows XP

### Unterstützung von Juniper Gateways mit Junos- und ScreenOS-Betriebssystemen

### Voraussetzung

Juniper IPsec Gateway (support for ScreenOS)

### Lizenzierung

Der NCP Secure Client – Juniper Edition unterstützt wahlweise drei Arten der Lizenzierung:

#### Offline

- In der Offline-Variante muss eine Datei, die nach Eingabe von Lizenzschlüssel und Seriennummer erzeugt wird, an den Web Server geschickt werden und der daraufhin auf der Website angezeigte Aktivierungsschlüssel notiert werden.

#### Online

- In der Online-Variante werden die Lizenzierungsdaten über einen Assistenten unmittelbar nach Eingabe an den Web Server weitergegeben und die Software damit unverzüglich freigeschaltet.

#### Lizenzierung über Initialisierungs-Datei

- Der Client authentisiert sich am Lizenzserver im Firmennetz mit einer durch den Administrator verteilten Initialisierungsdatei. Der Client erhält daraufhin seine eigentliche Lizenz und ist freigeschaltet. (Voraussetzung: NCP Volume License Server - vorherigen Namen NCP Local License Server)

### Security Features

Der NCP Secure Client – Juniper Edition unterstützt alle IPsec-Standards der Internet Society's Security Architecture für das Internet-Protokoll (IPsec) sowie alle zugehörigen RFCs.

#### Virtual Private Networking

- IPsec (Layer 3 Tunneling)
- IPsec-Proposals können determiniert werden durch das IPsec -Gateway (IKE, IPsec Phase 2)
- Kommunikation nur im Tunnel, Message Transfer Unit (MTU) Size Fragmentation und Re-assembly
- Dead Peer Detection (DPD)
- Network Address Translation-Traversal (NAT-T)
- IPsec Tunnel Mode

#### Authentication

- Internet Key Exchange (IKE):
  - Aggressive Mode, Main Mode, Quick Mode
  - IKEv2 einschl. Mobility and Multihoming Protocol (MOBIKE)
  - Perfect Forward Secrecy (PFS)
  - IKE-Config-Mode für dynamische Zuteilung einer privaten (virtuellen) Adresse aus IP-Pool
  - Pre-shared Secrets oder RSA-Signaturen (mit entsprechender Public Key Infrastructure)
- Internet Key Exchange v2 (IKEv2):
  - Pre-shared secrets
  - RSA Signatures (and associated Public Key Infrastructure)
  - Extended Authentication Protocol (EAP) – (Benutzername und Passwort für Client-Authentisierung gegenüber Gateway; Zertifikat zur Server-Authentisierung gegenüber Client)  
EAP unterstützt: PAP, MD5, MS-CHAP v2, TLS (ausgewählt durch Responder/Gateway)
  - IKEv2 Mobility und Multihoming Protokoll (MOBIKE)

- Perfect Forward Secrecy (PFS)
- IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP)
- Benutzer-Authentisierung:
  - XAUTH für erweiterte Benutzer-Authentisierung
    - One-Time-Passwörter und Challenge Response Systeme
- Unterstützung von Zertifikaten in einer PKI:
  - Soft-Zertifikate, Smart Cards, USB Token: Multi-Zertifikats-Konfiguration
- Seamless rekeying (PFS)
- RSA SecurID Ready

## Verschlüsselung (Encryption)

Symmetrisch: AES-CTR 128, 192, 256 bits; AES 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits

Asymmetrisch: RSA bis 2048 bits für dynamischen Schlüsselaustausch

## Hash / Message Authentisierungs-Algorithmen

- SHA-256, SHA-384, SHA-512, MD5
- Diffie Hellman-Gruppen 1, 2, 5 und 14 für asymmetrischen Schlüsselaustausch und PFS

## Public Key Infrastructure (PKI) – Starke Authentisierung

- X.509 v.3 Standard
- PKCS#11-Schnittstelle für Verschlüsselungs-Tokens (USB und Smart Cards)
- Smart Card-Betriebssysteme
  - TCOS 1.2, 2.0 und 3.0
- Smart Card Reader-Schnittstellen
  - PC/SC, CT-API
- PKCS#12-Schnittstelle für private Schlüssel in Soft-Zertifikaten
- Certificate Status Protocol (CSP) zur Verwendung von Benutzerzertifikaten im Windows-Zertifikatsspeicher
- Administrative Vorgabe für die Eingabe beliebig komplexer PINs
- Revocation:
  - End-entity Public-key Certificate Revocation List (EPRL vormalis CRL)
  - Certification Authority Revocation List, (CARL vormalis ARL)
  - Online Certificate Status Protocol (OCSP)

## Networking Features

### LAN Emulation

- Virtueller Ethernet-Adapter mit NDIS-Schnittstelle

### Netzwerk Protokoll

- IPv4-Protokoll
  - IPv4 für Tunnelaufbau und Datenverkehr innerhalb des VPN-Tunnels;
- IPv6-Protokoll
  - IPv6 für Tunnelaufbau von Client zu NCP Server-Komponenten (Secure Enterprise VPN Server);
  - zur Datenübertragung innerhalb des VPN-Tunnels wird IPv4 genutzt

### IP Address Allocation

- Dynamic Host Control Protocol (DHCP)
- DNS: Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Serve

### Line Management

- Dead Peer Detection mit konfigurierbarem Zeitintervall

## Weitere Leistungsmerkmale

- Import der Dateiformate \*.ini und \*.spd

## Unterstützte Standards

### Internet Society RFCs und Drafts

Security Architecture for the Internet Protocol and assoc. RFCs (RFC2401 - 2409),

- Internet Key Exchange Protocol v1 (IKE) (includes IKMP/Oakley) (RFC 2406),
  - IKE Extended Authentication (XAUTH), IKE configure (IKECFG) and Dead Peer Detection (DPD)
  - Negotiation of NAT-Traversal in the IKE (RFC 3947)
- UDP encapsulation of IPsec Packets (RFC 3948),

### FIPS Inside

Der Secure Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 zertifiziert (Zertifikat #1051).

Die FIPS-Kompatibilität ist immer gegeben, wenn einer der folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden:

- Diffie Hellman Gruppe: Gruppe 2 oder höher (DH ab eine Länge von 1024 Bit)
- Hash Algorithmen: SHA1, SHA 256, SHA 384, oder SHA 512 Bit
- Verschlüsselungsalgorithmen: AES mit 128, 192 oder 256 Bit oder Triple DES

## Client Monitor

### Intuitive graphische Benutzeroberfläche

- Mehrsprachigkeit (Englisch und Deutsch)
- Icon, das den Verbindungsstatus anzeigt
- Client Info Center – Übersicht über:
  - Allgemeine Informationen - Version#, MAC-Adresse etc.
  - Verbindung – aktueller Status
  - Services/Applications – Prozess-Status
  - Zertifikats-Konfiguration – eingesetzte Zertifikate etc.
- Konfiguration, Verbindungsstatus, Logbuch (mit Farbmarkierungen und Copy&Paste-Funktion)
- Trace Tool zur Fehlerdiagnose
- Tests zur Internet-Verfügbarkeit