# Release Notes

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

## Prerequisites

**Operating System Support**

The following Microsoft Operating Systems are supported with this release:

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

## New License Key from Version 3.10

*Software Updates and License Keys*

**From the current software version, every new major release will require a specific license key for the same version.**

If the software is updated without performing a license update, the client will receive a license for the remainder of the 30-day trial period.

*New Installation and License Keys*

For a new installation, the client software is installed under the Program Files directory (previously Program Files (x86)) and licensed as a trial version (for a maximum of 30 days) until a valid license is entered.

# 1. New Features and Enhancements

## VPN Bypass

The VPN Bypass function allows the administrator to define applications which can communicate over the Internet directly despite disabling split tunneling on the VPN connection. It is also possible to define which domains or target addresses can bypass the VPN tunnel.
This function can be used to separate regular and non-sensitive data traffic from central infrastructure, so as not to affect performance. For example, operating systems and virus scanner updates (with a known domain), can bypass the VPN connection easily, or certain cloud services can be permitted to access applications via the Internet directly. VPN Bypass is configured via “Configuration/VPN Bypass” in the client monitor and in the profile settings under "Split Tunneling / VPN bypass list".

## Home Zone

The Home Zone feature has been implemented as an option in the firewall to make the resources of a home network available without the administrator knowing the configuration of the employee's home office network.

The Home Zone can be activated under "Options" in the firewall settings and in the firewall default settings. The Home Zone can be set and deleted in the client monitor Connect menu by the user.

## Selecting a User or Computer Certificate in Windows CSP

In the client configuration menu under "Certificates" (Extended Key Usage), you can select the default certificate for a user or computer.

## Show Media Type Using ncpclientcmd.exe

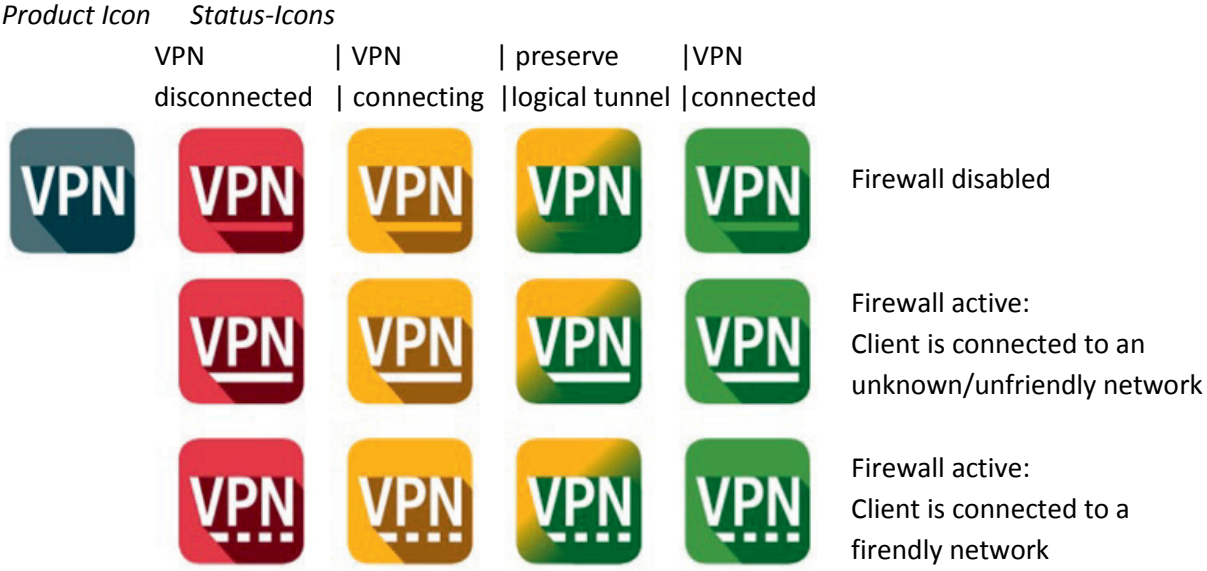
Entering the command "NcpClientCmd /getConnecionMedium" in the command prompt shows the connection media type.

## New Product and Status Icons

The product and status icons have been updated in this version.

The color of the status icons change from red to green during connection.

The line under the VPN icon shows whether the firewall is active and whether the device is connected to an unknown or friendly network.



### IKEv2 Signature Authentication (RFC 7427)

The client now supports certificate authentication according to RFC 7427 for IKEv2 RSASSA-PSS which also allows for modern padding (RSASSA-PSS).

## 2. Improvements / Problems Resolved

### Support for More than two FND Servers

The number of optional FND servers is restricted to 255 characters. Three addresses can be entered separated by a comma for example: fe80 :: E568: 8a83: 203c: 55c0,192.16.15.57, fnd2.ncp.de, 192.16.15.56

### Changes to Roaming Connection Options in Budget Manager

To prevent costs from being incurred by establishing a connection when roaming users can activate “No roaming” under “Connection Options” in the Budget Manager. In previous versions of the client, “Do not establish connection” was used. This connected to the network and disconnected if roaming was detected.

### Hotspot Logon

The client provides the installed version number of Internet Explorer during Hotspot Logon to avoid logon problems.

### Firewall Blocked IPv6 IKE Packets

Previously only a IPv4 VPN connection could be established if the option “Allow IPsec protocol (500, 4500, ESP, 443)” was enabled in the firewall. Both IPv4 and IPv6 connections are now supported.

### Alternative IPSec Port Fixed

VPN connection now works if the “Allow IPsec procol (ESP, UDP) and VPN Path Finder” firewall option is activated and an alternative IPsec port is configured.

### Enabling and Disabling the Credential Provider

Starting with this release, Windows PreLogon with the Credential Provider can no longer be selected during the software installation. The credential provider can now only be enabled and disabled under “Logon Options” in the client monitor “Configuration” menu.

## 3. Known Issues

None

Release Notes

# bintec elmeg IPSec Secure Client (Win32/64)

**Major Release:** **3.10**
**Date:** **April 2016**

## Prerequisites

### Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 10 (32 and 64 bit)
- Windows 8.x (32 and 64 bit)
- Windows 7 (32 and 64 bit)
- Windows Vista (32 and 64 bit)

## New License Key from Version 3.10

*Software Updates and License Keys*

**From the current software version, every new major release will require a specific license key for the same version.**

If the software is updated without performing a license update, the client will receive a license for the remainder of the 30-day trial period.

*New Installation and License Keys*

For a new installation, the client software is installed under the Program Files directory (previously Program Files (x86) and licensed as a trial version (for a maximum of 30 days) until a valid license is entered.

## Windows 10 Update 1511 (Threshold 2/Build 10586) causes problems with installed Bintec elmeg IPSec Secure Client

Microsoft's november update for Windows 10 is far more than merely a collection of patches and/or enhancements. In general it is essentially a new version of Windows. Some areas of the registry database are rewritten during the update and while doing so a few important entries of the bintec elmeg IPSec Secure Client are discarded.

To resolve this issue the lost registry keys and related values have to be written again. Therefore one has to perform an uninstall of the bintec elmeg IPSec Secure Client followed by a mandatory reboot prompted for within the uninstall procedure. After which one just has to reinstall the version of the client used before. (Please do **not** confirm the "Delete all files" option of the uninstall process).

The full configuration will be preserved; only the license information has to be re-entered after the installation. After having completed this procedure the bintec elmeg IPSec Secure Client can be used again without any limitations.

# 1. New Features and Enhancements

## New Hotspot Logon

Additional configuration is no longer required with the new Hotspot Logon feature. The client detects available hotspots and provides the user with an option to logon. When Hotspot Logon is started by the user, the NCP Wi-Fi Manager is displayed and the user can select the Wi-Fi network and log on to it. As soon as the Wi-Fi connection is established, the client checks access to the internet periodically. If internet access is not available, the client starts a restricted browser without the address bar. If the user has logged onto the hotspot operator's entry portal successfully, the VPN tunnel will be established automatically as soon as internet access is available.

### Improved Compatibility with Gateways Provided by Other Manufacturers

Secure Client supports IKEv2 redirect (RFC 5685). This means that load balancing functions provided by other manufacturers can be used.

### Monitoring the Filter Driver via the Secure Client

If the client detects a problem with the filter driver, it will attempt to resolve the error and prompt the user to restart the device.

### Using Half Routes and Default Gateways in Windows 10

The default client setting for the virtual network adapter is "half routes". This can be changed to "default gateways" by editing the registry. To do this, modify the following registry key:
Path:
`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ncprwsnt]`
Key:
`EnableDefGw = 1`
Type:
`REG_DWORD`
If the registry key EnableDefGw does not exist or is set to EnableDefGw=0, the client will use half routes.

## 2. Improvements / Problems Resolved

### Stability Improvements

The stability of the NCPRWSNT service and update clients has been improved.

### Enhancement of Log Messages

The log details for the PKI environment and ncpsec service have been enhanced.

### Functionality of Wi-Fi Module

In the event of a large number of Wi-Fi profiles (greater than 56), the Wi-Fi adapter did not function correctly and the adapter was no longer displayed under Wi-Fi Management. This issue has now been resolved.

### Windows Pre-Logon

Windows Pre-Logon (Credential Provider) has been adapted for Windows 10.

## 3. Known Issues

None