Release Notes
bintec Secure IPSec Client
Version 4.13

Content

Prerequisites

Operating System Support:

The following Microsoft Operating Systems are supported with this release:

- Windows 10 32/64 Bit (up to and including versio1809)
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit

1 New Features and Enhancements

1.1 Update for Windows 10 Version 1809 – Driver Installation

Due to Microsoft updates, it was not possible to install previous clients on Windows 10 version 1809. This problem has been resolved.

2 Improvements / Problems Resolved

2.1 Friendly Net Detection Server

In networks with network access control when the IP segment changes after successful authentication, the detection of the Friendly Net Detection Server has been improved.

2.2 Performance Optimization of Data Transfer Outside the VPN

Optimization of the Client Update Process for Major Updates

Detection of major updates within the MSI installation process has now been improved. An issue with the `NcpClntInstallPath` environment variable, which may have been deleted after the client update, was also fixed.

2.3 Display of the VPN Client in the Task Bar

If the client GUI is closed, the icon is no longer displayed in the task bar. This corresponds to the behavior of client versions before 11.0.

2.4 Diagnostic Data in the Installation Directory

If the full trace function was enabled or a HotSpot detection configured, diagnostic files were incorrectly written to the installation directory of the client. This issue has been resolved.

2.5 Improvement to Silent Installation

Under certain circumstances, the REBOOT property could be overwritten during the installation of the client. This issue has now been resolved.

2.6 Improved Compatibility to DHCP Servers

For a DHCP request, specifying the host name is optional, but not all DHCP servers support omitting the host name. For this reason, the host name is always sent as of this release.

2.7 Improved Compatibility to Third-party Gateways

IKE negotiation has been updated to improve compatibility to external gateways.

2.8 Firewall Setting: Exception for VPN Path Finder

If the "Allow IPsec protocol (ESP, UDP 500) and VPN Path Finder (TCP 443)" option was configured in the firewall settings, destinations were accessible through the VPN connection via HTTPS port 443 although this was not allowed by any other firewall rule. This issue has been resolved.

2.9 Length of the PKCS#11 File Name

The length of the input field in the PKI configuration of the client for the PKCS#11 module has been increased to 255 characters.

2.10 Reloading DLLs

The DLL loading process has been enhanced for increased security against manipulated DLLs.

2.11 Enhanced Security During Update Check

Security has been improved to avoid manipulation when the client checks for new versions.

3 Known Issues

3.1 Demo User Certificates

The **demo user certificates** installed with previous client versions will expire on October 9, 2018. This means that existing test profiles such as for the NCP demo server "vpntest.ncp-e.com" will no longer work. From this client version on, new installations will no longer automatically configure these test profiles using this certificate. Only test profiles with the VPN configuration "Pre-shared key" can be created.

New certificates with extended validity are located in the certs subdirectory after installation. Previously, these certificates were located directly in the installation directory.