NCP Secure Client – Juniper Edition
Release Notes

Service Release: **10.11 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 10.10

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".

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.

Product Icon *Status-Icons*

VPN disconnected	VPN connecting	preserve logical tunnel	VPN connected

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

None

3. Known Issues

None

Service Release: **10.10.03 r30578**
Date: **June 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 10.10

Software Updates and License Keys

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

A license update is required with the software update when updating the client software via SEM. 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 NCP 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 NCP 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 NCP 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 NCP Secure Client can be used again without any limitations.

4. New Features and Enhancements

None

5. Improvements / Problems Resolved

Problems Resolved with License File

In some cases, the license file may become corrupted or be deleted. The handling of the license file has been optimized to resolve this.

Update to Installation File Signature

The signature of the installation file is checked during online installation from Internet Explorer. This check failed because the certificate has expired. The certificate and the signature have been updated.

Connecting and Disconnecting the VPN Tunnel Manually

After clicking the Connect or Disconnect button in quick succession, the client may enter a state which does not allow a connection to be established. Previously this could only be remedied by changing the profile.

Update Behavior for Local Update or SEM Update

6. Known Issues

None

Major Release: **10.10 r29061**
Date: **April 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 10.10

Software Updates and License Keys

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

A license update is required with the software update when updating the client software via SEM. 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 NCP 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 NCP 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 NCP 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 NCP Secure Client can be used again without any limitations.

1. New Features and Enhancements

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.

3. Known Issues

None

4. Getting Help for the NCP Secure Client – Juniper Edition (Win32 / 64)

To ensure that you always have the latest information about NCP's products, always check the NCP website at:
http://www.ncp-e.com/en/downloads/software/version-information.html

For further assistance with the NCP Secure Enterprise Client (Win32/64), visit:
http://www.ncp-e.com/en/company/contact.html

E-Mail: support@ncp-e.com

5. Features

Operating Systems

See Prerequisites on page 1.

Support for Juniper Gateways with Junos and ScreenOS Operating Systems

Prerequisite

Juniper IPsec Gateway (support for ScreenOS)

Licensing

The NCP Secure Client – Juniper Edition supports three types of licensing/activation:

Offline Activation

In offline activation, a file must first be generated by entering a license key and serial number. This must then be sent to the NCP Activation Server which then returns an activation key. This key must then be used to activate the Secure Client.

Online Activation

In online activation the licensing data entered via a Wizard is validated, via the Internet, with the NCP Activation Server before being used to activate the Secure Client.

Licensing using an Initialization File

The Secure Client uses an Initialization File, distributed by an administrator, to authenticate itself with the Licensing Server, via the corporate VPN network. The Secure Client uses the actual license received for activation. (Prerequisite: NCP Volume License Server - previously named NCP Local License Server)

Security Features

Support of the Internet Society's Security Architecture for IPsec and all the associated RFCs.

Virtual Private Networking

- RFC conformant IPsec (Layer 3 Tunneling)
  - IPsec Tunnel Mode
  - IPsec proposals are negotiated via the IPsec gateway (IKE Phase 1, IPsec Phase 2)
  - Communikation only in the tunnel or Split Tunneling
  - Message Transfer Unit (MTU) size fragmentation and reassembly
  - Network Address Translation-Traversal (NAT-T)
  - Dead Peer Detection (DPD)
  - Anti-replay Protection

Authentication

- Internet Key Exchange (IKE):
  - Aggressive Mode, Main Mode, Quick Mode
  - Perfect Forward Secrecy (PFS)
  - IKE-Config-Mode for dynamic allocation of private (virtual) IP address from IP-Pool
  - Pre-shared Secrets or RSA signatures (and associated Public Key Infrastructure)
- Internet Key Exchange v2 (IKEv2):
  - Pre-shared secrets
  - RSA signatures (and associated Public Key Infrastructure)
  - Extended Authentication Protocol (EAP) – (username and password used to authenticates NCP Secure Enterprise Client with VPN gateway, PKI certificate used to authenticate VPN gateway with Client)
  - EAP supported: PAP, MD5, MS-CHAP v2, TLS (selected by responder)
  - IKEv2 Mobility and Multihoming protocol (MOBIKE)
  - Perfect Forward Secrecy (PFS)
  - IKE Config. Mode for dynamic allocation of private IP (virtual) address from address pool
- User authentication:
  - XAUTH (IKEv1) for extended user authentication
    - One-time passwords and challenge response systems
    - Authentication details from certificate (prerequisite PKI)
- Support for certificates in a PKI:
  - Soft certificates, Smart cards, and USB tokens: Multi Certificate Configurations
- Seamless Rekeying
- RSA SecurID Ready

Encryption and Encryption Algorithms

Symmetrical: AES-GCM 128, 256 bits (only IKEv2 & IPsec); AES-CTR 128, 256 bits (only IKEv2 and IPsec); AES (CBC) 128, 256 bits; Triple-DES 112,168 bits

Asymmetrical: RSA to 2048 bits, dynamic processes for key exchange

Hash / Message Authentisierungs-Algorithmen

- SHA-1, SHA-256, SHA-384, SHA-512, MD5.
- Diffie Hellman groups 1, 2, 5, 14, 18, 19 for asymmetric key exchange and PFS.

Public Key Infrastructure (PKI) – Strong Authentication

- X.509 v.3 Standard
- Support for certificates in a PKI
  - Smart cards and USB tokens

    - PKCS#11 interface for encryption tokens (smart cards and USB)
    - Smart card operating systems: TCOS 1.2, 2.0 und 3.0
  - Smart card reader systems
    - PC/SC, CT-API
  - Soft certificates
    - PKCS#12 interface for private keys in soft certificates
- PIN policy: administrative specification of PIN entry to any level of complexity
- Certificate Service Provider (CSP) for the use of user certificates in Windows certificate store
- Revocation:
  - End-entity Public-key Certificate Revocation List (EPRL formerly CRL)
  - Certification Authority Revocation List, (CARL formerly ARL)
  - Online Certificate Status Protocol (OCSP)

Networking Features

Secure Network Interface

- LAN Emulation
  - Ethernet adapter with NDIS interface

Network Protocol

- IPv4 protocol
  - IPv4 traffic inside and outside VPN tunnel can use IPv4 protocol;
- IPv6 protocol
  - IPv6 traffic used to establish and maintain the VPN tunnel can use IPv6 protocol (Client to VPN gateway and Client to NCP Secure Enterprise HA Server);
  - IP traffic inside any VPN tunnel MUST use IPv4 protocol;

Communications Media

- LAN

Line Management

- Dead Peer Detection with configurable time interval
- Connection Modes
  - manual
  - always
  - automatic (connection initiated by data transfer)
  - variable (Connect starts "automatic" mode)
  - variable (Connect starts "always" mode)
- Inactivity Timeout (send, receive or bi-directional)

IP Address Allocation

- Dynamic Host Control Protocol (DHCP)
- Domain Name Service (DNS) : gateway selection using public IP address allocated by querying DNS server

Data Compression

- IPsec Compression

Other Features

- Import of the file formats: *.ini, *.spd

Standards Conformance

Internet Society RFCs and 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

The Secure Client incorporates cryptographic algorithms conformant to the FIPS standard. The embedded cryptographic module incorporating these algorithms has been validated as conformant to FIPS 140-2 (certificate #1051).

FIPS conformance will always be maintained when any of the following algorithms are used for establishment and encryption of the IPsec connection:

- Diffie Hellman Group: Group 2 or higher (DH starting from a lenght of 1024 Bit)
- Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit
- Encryption Algorithms: AES with 128, 192, 256 Bit or Triple DES

Secure Client Monitor

Intuitive Graphical User Interface

- Language support (English, German)
  - Monitor & Setup: en, de
  - Online Help and License en, de
- Icon indicates connection status
- Client Info Center – overview of:
  - General information - version#, MAC address etc.

- Connection – current status
- Services/Applications – process(es) – status
- Certificate Configuration – PKI certificates in use etc.

- Configuration, connection statistics, Log-book (color coded, easy copy&paste function)
- Integrated support of Mobile Connect Cards
- Password protected configuration and profile management
- Trace tool for error diagnosis
- Internet Availability Tests
- VPN Tunnel Traffic Monitoring (Tunnel Availability Tests)

Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com
Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Fon +49 911 9968-0 · Fax +49 911 9968-299