NCP Secure Client – Juniper Edition

Major Release: **10.04 r38728**
Date: **March 2018**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 10 32/64 Bit Version 1709
- Windows 8.x (32 and 64 bit)
- Windows 7 (32 and 64 bit)
- Windows Vista (32 and 64 bit)

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.

Information on the operation of the Secure Client under Windows 10

It is necessary to have a product key for version 10.x to operate the Client.

Note when updating the operating system to Windows 10

When updating from Microsoft Windows 7, Windows 8 or Windows 8.1 to Microsoft Windows 10, it is vital that the NCP Secure Client be uninstalled before starting the update.

At the same time it is recommended that the configuration file, as well as the certificates used, is saved separately.

When the update to Windows 10 is complete, the latest version of the NCP Secure Client (10.02 or later) should then be installed.

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

Change to the NCP Network Driver Type under Windows 10

Changing the NCP network driver type from an "Ethernet Adapter" to "Virtual Adapter" under Windows 10 has resolved the issue that Wi-Fi adapters were deactivated by the operating system if the VPN was connected by Wi-Fi and Wi-Fi was not configured using the NCP Wi-Fi Manager.

NDIS Driver Optimization for Windows 10

The NDIS driver has been optimized for Windows 10 to correct problems during connection setup after leaving sleep mode.

Client Firewall Status in Windows

The firewall status is now shown in Windows (under "Security and Maintenance").

Instability after installation of Microsoft patches for Windows 7 64 Bit

The Microsoft patches KB4057400, KB4074598 or KB4075211 address the handling of SmartCards and certificates for user authentication. The PKI Support Service (ncpsec service) which is part of NCP Secure Client is also responsible for PKI features. It is started automatically when the operating system starts.

Under Windows 7 64 Bit, when the above patches are installed, the NCP Client PKI Support Service can no longer start correctly and that PKI features in the NCP Secure Client do not work properly. This issue has been resolved.

3. Known Issues

None

Major Release: **10.04 r31799**
Date: **August 2016**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

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

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.

Information on the operation of the Secure Client under Windows 10

It is necessary to have a product key for version 10.x to operate the Client.

Note when updating the operating system to Windows 10

When updating from Microsoft Windows 7, Windows 8 or Windows 8.1 to Microsoft Windows 10, it is vital that the NCP Secure Client be uninstalled before starting the update.

At the same time it is recommended that the configuration file, as well as the certificates used, is saved separately.

When the update to Windows 10 is complete, the latest version of the NCP Secure Client (10.02 or later) should then be installed.

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

License Deactivation

In some cases, the client license may have been deactivated after restarting the device. This issue has been resolved.

Unavailability of Network Connection

After an installation or update of the NCP Secure Client, the network connection was unavailable until restarting the device. From this maintenance release, the network connection is available immediately after the installation or update of the NCP Secure Client.

3. Known Issues

None

Major Release: **10.04 r31256**
Date: **August 2016**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

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

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.

Information on the operation of the Secure Client under Windows 10

It is necessary to have a product key for version 10.x to operate the Client.

Note when updating the operating system to Windows 10

When updating from Microsoft Windows 7, Windows 8 or Windows 8.1 to Microsoft Windows 10, it is vital that the NCP Secure Client be uninstalled before starting the update.

At the same time it is recommended that the configuration file, as well as the certificates used, is saved separately.

When the update to Windows 10 is complete, the latest version of the NCP Secure Client (10.02 or later) should then be installed.

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

Update Driver Signature (Anniversary Update Version 1607, Build 14393.10)

If the Anniversary Update for an older NCP Secure Client version is installed under Windows 10, the installation fails if "Secure Boot" is enabled in the BIOS /UEFI of the computer. The reason for this is that Windows 10 requires a driver signed by Microsoft after the Anniversary Update.

With this release of the NCP Secure Client (10.10 r31256), a signed driver is installed for all supported Windows versions.

Installing the Anniversary Update for a previously installed NCP Secure Client under Windows 10 does not affect the function of the client.

Correction in the Allocation of DNS Server IP Addresses

The IP address entries of the DNS servers did not always update correctly for VPN access by clients accessing different remote networks. This led to connection errors in some cases.

3. Known Issues

None

4. Getting Help for the NCP Secure Client – Juniper Edition

For further assistance with the NCP Secure Client – Juniper Edition, visit:
http://www.ncp-e.com/en/products/juniper-vpn-client.html

Mail: juniperhelpdesk@ncp-e.com

Major Release: **10.04 r26745**
Date: **November 2015**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

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

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.

Information on the operation of the Secure Client under Windows 10

It is necessary to have a product key for version 10.x to operate the Client.

Note when updating the operating system to Windows 10

When updating from Microsoft Windows 7, Windows 8 or Windows 8.1 to Microsoft Windows 10, it is vital that the NCP Secure Client be uninstalled before starting the update.

At the same time it is recommended that the configuration file, as well as the certificates used, is saved separately.

When the update to Windows 10 is complete, the latest version of the NCP Secure Client (10.02 or later) should then be installed.

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

Installation

Users experienced a rollback of the client installation during the filter driver setup. This version contains adjustments of the setup information correcting this behavior.

Split Tunneling

Error fixed in split tunneling when the remote network shared the same IP address range as the user's local network. This previously caused the local network route to be deleted if the VPN profile was changed.

Profile Import

The variable connection mode ConnMode=2 (automatic mode is started manually) was not imported during profile import. This error has been fixed.

3. Known Issues

None

4. Getting Help for the NCP Secure Client – Juniper Edition

For further assistance with the NCP Secure Client – Juniper Edition, visit:
http://www.ncp-e.com/en/products/juniper-vpn-client.html

Mail: juniperhelpdesk@ncp-e.com

Major Release: **10.00 build 21336**
Date: **January 2015**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

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

1. New Features and Enhancements

MSI Installer - Updating to NCP Secure Client - Juniper Edition Version 10.0

NCP Secure Client - Juniper Edition version 10.00 software is distributed in the Microsoft .msi format. The impact of this move is as follows:

- All NCP Secure Client - Juniper Edition software versions earlier than 10.00, must first be de-installed using the Microsoft "Programs and Features" functions. Then the new software can be installed from the .msi package; existing profiles can be preserved across the update. Subsequent updates can be applied, when available, using the MSI Update feature.

Enhanced Connection Modes

Connection Mode has been enhanced with two additional modes and the selections have been given more explanatory names as follows:

manual / (default Connection Mode)

When this mode is set, the user must manually establish the VPN connection by pressing "Connect". The connection will be disconnected dependent on timeout settings. If timeout is set to null (0) the connection must be disconnected manually.

automatic (connection initiated by data transfer)

When this mode is set, the Client software automatically establishes the connection as soon as data must be transferred across the connection. How the connection is disconnected is dependent on how the Client is configured, i. e. according to application requirements and profile settings.

always

When Connection Mode is set to "always", a VPN connection is always established automatically when the Client starts. Connection establishment is independent of the "Connect" button, of the onset of data transfer, or of how the monitor is set to be displayed

variable (Connect starts "automatic" mode)

When this mode is set, the first VPN connection is established manually (by pressing "Connect") The mode used to establish the next connection is dependent on how the previous connection was disconnected:

– if the connection was disconnected due to a timeout, then the next connection will be established whenever data transfer to a remote host is initiated by a Client application.

– If the connection was disconnected manually (by pressing "Disconnect")then the next connection must be established manually.

If timeout is set to zero (0), i.e. no timeout, then the connection must be disconnected manually.

Important: if connection mode is set to "manual" then activate a timeout (i.e. set timeout to non zero) in order to automate disconnection.

variable (Connect starts "always" mode)

When this mode is set, the first time "Connect" is pressed to establish a VPN connection, the connection mode is set to "always". This "always" mode stays set until the monitor is closed, when the mode is changed back to "variable (Connect starts "always" mode)".

Extended Log Settings

Under the monitor menu "Help/Extended Log Settings" the maximum log-entries retention period (in days) can be defined.

Execution of the RWSCMD and NcpClientCmd command-line tools, including the calling parameters, can be written to a log file. To do this the application must be activated in the "Extended Log Settings". Alternatively this can be done by adding the line "[RWSCMD]Logs=1" to the NCPMON.INI. The output is logged to "RwscmdLog.txt" in the log directory.

Enhancements to the Support Assistant

The support assistant has been enhanced to enable the Microsoft log file from the driver installation to be included.

The following files are included, if present:

WINDOWSDIR\inf\setupapi.dev.log

WINDOWSDIR\inf\setupapi.app.log

WINDOWSDIR\inf\setupapi.setup.log

IKEv2 Profile Configuration - GUI Improvements

IKEv2 based polices can be defined in the Client monitors' IPsec settings. IKEv2 key exchange is then handled according to these settings.

Further IKEv2 configuration settings are made in a profile's standard configuration, where the corresponding authentication can be selected - Certificate, Pre-shared Key or EAP.

The input fields for username and password or the IKE ID are blanked out, dependent on which authentication method is chosen,

In the profile settings under "IPsec" the required IKEv2 policy can be selected, unless automatic mode has been chosen.

The "Policy Editor" button can be used to switch directly from the IPsec profile settings to the IPsec policies configuration.

MSI Installer – NCP-specific Functions

Adding a .cnf file when installing

When installing a .msi package, a .cnf file can be included in the installation. In previous setup procedures the .cnf file had to be copied to the installation directory. Now the installer copies the .cnf autonomously

to the installation directory, providing the .cnf file is stored in the directory from which the .msi package, (or the installer as a .exe file) is to be executed. The return value from the copy is ignored. If errors occur, the installation is not aborted.

Adding files during the installation

Additional files, for example certificates or customer specific project logo files (CBO) which should be included in the setup can be installed.

Previously a directory ncple, was created under "Disk1" from where all files and directories were recursively copied to the installation directory.

This is now performed in a different way. If a directory IMPORTDIR is located in the directory from which the .msi package, (or the installer as a .exe file) is to be executed, this directory is copied recursively to the installation directory. The return value from the copy is ignored. If an error occurs, the installation is not aborted. As such files are not recognized by the installer, these are neither updated nor de-installed.

Another mechanism for adding files, icons, registry entries, etc. to an installation is the transform file. Using the admin tools from various software manufacturers (such as InstallShield, SuperOrca), the .msi package can be opened, any features, components, files etc., added, and a transform file created which can be passed as a parameter to the installation.

msiexec /i myproduct.msi TRANSFORM=mytransfom.mst

This is the officially supported method for extending an existing .msi package. The advantage is that the extensions are known to the installer and can be updated and de-installed by the installer.

Executing a batch file during the installation

If a batch file NcpInstall.bat is located in the directory from which the .msi package, (or the installer as a .exe file) is to be executed, this file is executed as the last process in the installation. The return value from the execution is ignored. If an error occurs during execution of the batch file, the installation is not aborted. The installer is unaware of the execution and therefore cannot manage it.

Starting a test version immediately

In many projects there is the wish to "Start the test version now" when starting the monitor but without the need to prompt the user. This can be achieved using the command line parameter "STARTTESTVERSION".

msiexec /i myproduct.msi STARTTESTVERSION=1

Silent Installation und De-installation

The previous "silent installation" has been replaced by a new form, handled by the installer. Its own "silent installation" is used, initiated by the display options.

e.g.: msiexec /i myproduct.msi /qn myproduct.exe /v"/qn"

The previous form of "silent installation" is replaced with one which is initiated via the display options.

e.g.: msiexec /x myproduct.msi /qn

Logging

Previously parts of the setup could be logged using the NCP specific SetupExt.ini. Now the Windows installer performs extensive logging. This can be configured using the logging options.

e.g.: msiexec /i myproduct.msi /log "c:\temp\myinstall.log" myproduct.exe /v"/log "c:\temp\myinstall.log""

Deleting all files during de-installation

Previously, during the last part of the de-installation, the user was asked whether personal files should deleted. Using "silent installation" the parameter -delall could be used for this purpose.

This has now changed and is dependent on the type of de-installation. If the Client is de-installed using the assistant, the user is prompted as previously. If it is de-installed directly (no dialog), the user is not prompted as no personal files are deleted. In this case the command line parameter DELETEALL=1 can be used, causing all files to be deleted.

e.g.: msiexec /x myproduct.msi DELETEALL=1

2. Improvements / Problems Resolved

OpenSSL Version 1.0.1j

OpenSSL 1.0.1j is used within the Client software. Security deficiencies associated with previous versions of the OpenSSL libraries are thereby resolved.

3. Known Issues

None

4. Getting Help for the NCP Secure Client – Juniper Edition

For further assistance with the NCP Secure Client – Juniper Edition, visit:
http://www.ncp-e.com/en/products/juniper-vpn-client.html

Mail: juniperhelpdesk@ncp-e.com

5. Features

Operating Systems

Microsoft Windows (32 and 64 bit): Windows 8.x, Windows 7 and Windows Vista

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

The NCP Secure Client – Juniper Edition supports the Internet Society's Security Architecture for the Internet Protocol (IPsec) and all the associated RFCs.

Virtual Private Networking

- IPsec (Layer 3 Tunneling)
- IPsec proposals are negotiated via the IPsec gateway (IKE Phase 1, IPsec Phase 2)
- Communication only in the tunnel
- Message Transfer Unit (MTU) size fragmentation and reassembly
- Dead Peer Detection (DPD), Event log
- Network Address Translation-Traversal (NAT-T)
- IPsec Tunnel Mode

Authentication

- Internet Key Exchange (IKE):
  - Aggressive Mode and Main Mode
  - Perfect Forward Secrecy (PFS)
  - IKE Config. Mode for dynamic allocation of private IP (virtual) address from address 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 Types 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 for extended user authentication
    - one-time passwords and challenge response systems
- Support for certificates in a PKI:
  - Soft certificates, Smart cards, and USB tokens: Multi Certificate Configurations
- Seamless rekeying (PFS)
- RSA SecurID ready

Encryption and Encryption Algorithms

Symmetrical:	AES-CTR 128, 192, 256 bits; AES 128, 192, 256 bits; Blowfish 128, 448 bits; Triple-DES 112, 168 bits
Asymmetrical:	RSA to 2048 bits, dynamic processes for key exchange

Hash / Message Authentication Algorithms

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

Public Key Infrastructure (PKI) - Strong Authentication

- X.509 v.3 Standard
- PKCS#11 interface for encryption tokens (USB and smartcards)
- Smart card operating systems:
  - TCOS 1.2, 2.0 and 3.0
- Smart card reader interfaces:
  - PC/SC, CT-API
- PKCS#12 interface for private keys in soft certificates
- Certificate Service Provider (CSP) for the use of user certificates in Windows certificate store
- PIN policy: administrative specification of PIN entry to any level of complexity
- 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

LAN Emulation

- Virtual Ethernet adapter with NDIS interface

Network Protocol

- IPv4 protocol
  - IP traffic inside and outside VPN tunnel can use IPv4 protocol
- IPv6 protocol
  - IP traffic used to establish and maintain the VPN tunnel can use IPv6 protocol (Client to VPN gateway),
  - IP traffic inside any VPN tunnel MUST use IPv4 protocol.

IP Address Allocation

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

Line Management

- Dead Peer Detection with configurable time interval

Additional 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 length of 1024 Bit)
- Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit
- Encryption Algorithms: AES with 128, 192 or 256 Bit or Triple DES

Client Monitor

Intuitive Graphical User Interface

- Bilingual (English, German)
- Traffic light icon indicates connection status
- Client Info Center – overview of
  - General information – version number, 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 and paste function)
- Trace tool for error diagnosis
- Internet Availability Tests