NCP Secure Client – Juniper Edition

Service Release: **9.32 Build 218**
Date: **March 2014**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 8.1 (32 and 64 bit)
- Windows 8.1 (32 and 64 bit)
- Windows 7 (32 and 64 bit)
- Windows Vista (32 and 64 bit)
- Windows XP (32 and 64 bit)

1. New Features and Enhancements

Logbook Display of VPN Tunnel Connections and Transfer Volumes

The Logbook has been enhanced to display information about successful and unsuccessful VPN tunnel connection establishments and disconnects, together with detailed data volume information about 3G and Wi-Fi connections.

The following are logged in the logbook and highlighted in blue:

After a successful VPN tunnel establishment:

03.02.2014 15:59:35 INFO - MONITOR: Connected -> Test Connection IPsec Native

03.02.2014 15:59:35 INFO - MONITOR: Media=GPRS / UMTS, Tx=1176 Byte, Rx=0 Byte

in addition, for each 3G media connection:

03.02.2014 15:59:35 INFO - MONITOR: Provider=T-Mobile D, Media=UMTS

in addition, for each Wi-Fi media connection:

03.02.2014 15:59:35 INFO - MONITOR: SSID=MyHomeWlan

After a successful VPN tunnel disconnection:

03.02.2014 16:00:10 INFO - MONITOR: Disconnected

03.02.2014 16:00:10 INFO - MONITOR: Media=GPRS / UMTS, Tx=15509 Byte, Rx=0 Byte

After an unsuccessful VPN tunnel establishment attempt:

Unsuccessful connection attempts are logged in red as follows:

03.02.2014 16:25:35 ERROR - error message

See Error_Codes_(en/de).txt (located in the installation directory) for text of specific errors.

2. Improvements / Problems Resolved

Windows 8 or Windows 8.1 and UMTS/3G Handling

Problems resolved

PathFinder

Problems resolved

Forcing NAT-T in IKEv2

Problems resolved

3. Known Issues

None

Service Release: **9.32 Build 160**
Date: **November 2013**

1. New Features and Enhancements in Service Release 9.32 Build 160

Windows 8.1 Support

The Secure Entry Client is supported on the Microsoft Windows 8.1 operating system.

Checking that Data is Passing Through the Tunnel

In locations with poor mobile wireless reception, there is a chance that, despite a VPN tunnel being established and marked green, data is not actually transferred across the tunnel. In order to give the correct feedback to the user in such a situation, "Tunnel Traffic Monitoring" can be enabled in the Client connection profile under the "Line Management" folder; this causes a configurable, target address in the remote network to be automatically pinged periodically. The VPN tunnel status is modified in line with the response from the ping.

IPv6 support

This release introduces support for the IPv6 protocol for communications between NCP Secure Entry Client and an NCP Secure Enterprise VPN Server, or third party VPN gateway.

NOTE: regardless of whether IPv4 or IPv6 is used to establish the VPN tunnel, traffic within the tunnel MUST use the IPv4 protocol.

Prerequisites:

NCP Secure Enterprise VPN Server (WIN):	Version 8.11 build 168
NCP Secure Enterprise VPN Server (Linux):	Version 8.11 from rev 5620

Additional Information in the System Tray

When the Client is controlled externally via the API or RWSCMD, balloon tips are displayed above the system tray. These balloon tips display status of commands, e.g. whether a connection was successfully established or configuration errors in the case that a connection is not successfully established.

System tray balloon tips also convey information about the use of SmartCards in connection with the Entry Client.

Hiding the NCP Network Adapter in the System

From Windows 7 onwards, the NCP Secure Entry Client's network adapter is visible when installed in the system; this is done in order to improve compatibility with 3rd party applications. If this is not desired the adapter can be hidden from view by, before installing the NCP Secure Client software, setting the parameter NoHideAdapter, located in setupext.ini, to "0".

In the case of an already installed Secure Client, the adapter can subsequently be changed from visible to hidden by altering a setting in the Windows registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\ncprwsnt
NoHideAdapter (DWORD): 0

2. Improvements / Problems Resolved in Service Release 9.32 Build 160

USB SmartCard Problem Resolved

Plugging and un-plugging a USB SmartCard reader under Windows 8 is now recognized correctly by the Client.

3. Known Issues in Service Release 9.32 Build 160

Caution when Updating from Windows 8 to Windows 8.1

After an update from Windows 8 to Windows 8.1, the previously installed and licensed NCP Secure Entry Client is no longer functional. Before the update to Windows 8.1, de-install the NCP software keeping the current configuration settings, and then install version 9.32 build 160 of the NCP Secure Entry Client software.

Service Release: **9.31 Build 104**
Date: **January 2013**

1. New Features and Enhancements in Service Release 9.31 Build 104

Support of NCP Secure Client software on MS Windows 8

This release 9.31 build 100 is the first version of the NCP Secure Client software that is fully supported when running on Microsoft Windows 8, either Professional or Enterprise. There are no restrictions when installing this version of the NCP Secure Client on MS Windows 8.

Upgrading a system with MS Windows 7 / NCP Secure Client software to MS Windows 8

On a system which already has NCP Secure Client software installed and running on MS Windows 7, under certain conditions the upgrade from MS Windows 7 to MS Windows 8 could cause corruptions to the Windows registry entries belonging to the NCP Secure Client software. To ensure that such corruptions do not lead to problems, it is advisable to adopt the following Windows 7 to 8 upgrade procedure on systems which already have NCP Secure Client software installed and running:

- Connection Profiles: backup the Secure Client profiles settings ("Configuration / Profile Settings Backup / Create") - the files "NCPPHONE.SAV" is saved in the NCP installation directory.
- Certificates: ensure backup copies of any PKCS#12 based certificate files are available.
  In the case of certificates that are stored in the Microsoft CSP User Certificate Store, either follow Microsoft instructions for backing up the CSP store or ensure the original certificates used to populate the CSP store are available.
- Copy all backed up files to a backup medium.
- Upgrade the OS software to Windows 8
- Install the latest version of NCP Secure Client software by running the "setup" program on the Secure Client software media. The "setup" program automatically recognizes that the software is already installed, and only upgrades those files necessary and preserves all existing profile settings.

The files backed up in step 3 will only be needed in the unlikely event that the NCP Secure Client profile settings or certificates become corrupted during step 4.

Changes to the Menu structure

The "Log Book" sub-menu is now located under the "Help" menu.

Secure Client Monitor compatibility with "High Contrast" display mode

The "High Contrast" display mode is an operating system option designed to reduce eye-strain and make the screen easier to read. The option can be switched on and off using SHIFT + ALT (left) + PRINT SCREEN.

Profile Groups in Context Menus and Profile Selection in Tray Icon

Profile Groups have always provided the ability to group similar profiles together in order to provide a better overview of the Connection Profiles available. Until now, once a group had been selected in the profile configuration menu, only a profile within that group could be selected for use as a Connection Profile, selection being either via a context menu displayed by clicking with the left mouse on the world map area of the Monitor or via the Secure Client's Tray Icon.

With this enhancement, the context menus mentioned above now enable a specific group to be selected, and then the required profile. Alternatively a profile from the complete list of profiles could be selected, i.e. the same function as in previous versions.

Deactivate Entry Client

In order to be able to use a licensed version of the Client software, without restrictions, on another machine, the license details (serial number and license key) bound to the current hardware and operating system must be released at the NCP Activation Server.

The user informs the Activation Server that the license will temporarily not be used by selecting "Deactivate Client" in the Help menu. In the input screen displayed, the user enters his/her name, optionally the name of the company and a valid e-mail address. When send is pressed, these details together with the serial number, license key and the language ID are sent to the Activation Server.

The Client is now deactivated; this is recognizable by the text "Software not Activated" displayed in a banner in the Client Monitor.

Subsequently the user will receive a mail with a URL link. When the URL link is opened in a web browser window, the license is reset at the Activation Server, i.e. the license details can then be used for activating the Client software installed on another machine.

Support for importing UTF8 formatted profile data from.ini files

Client profiles containing umlauts or other special characters encoded in ANSI or UTF8 format, and stored in .ini files are now correctly imported by the Client software.

2. Improvements / Problems Resolved in Service Release 9.31 Build 104

None

3. Known Issues in Service Release 9.31 Build 104

None

Service Release: **9.30 Build 186**
Date: **July 2012**

1. New Features and Enhancements in Service Release 9.30 Build 186

Configurable Service Wait-Time when Starting Monitor

In very rare cases the preconfigured delay after the start of the NCP Monitor is insufficient to allow the NCP services to start and an error message is displayed. The cause of the exceptionally long delay is due to system settings in the computer. With this release onwards, the delay can be reconfigured.

Description: when the NCP Monitor starts, it waits, for a maximum of 60 seconds, until the NcpClCfg service has started and next, for a maximum of 120 seconds, until the NcpRwsnt service has started. If these delays are insufficient and an error message is displayed, the delay can be reconfigured in the "GENERAL" section of NCPMON.ini, located in the Secure Client installation directory:

…

[GENERAL]

WaitForConfigService = 60 (NcpClCfg service, default 60 seconds)

WaitForDriverService = 120 (NcpRwsnt service, default 120 seconds)

…

The error messages displayed when such delays are encountered are:

- *Service "NCPCLCFG" is not running*
  In this case, increase the WaitForConfigService setting until the problem is circumvented
- *The Client Software has experienced a problem with the driver interface and is not working correctly (Mif32Init). Please reboot, and if the problem persists, please contact support.*
  In this case, increase the WaitForDriverService setting until the problem is circumvented.

The causes of such start-up delays are totally dependent on configuration settings in the Secure Client computer. These should be investigated and corrected with the help of support. Increasing the "WaitFor" times is only an interim solution.

Support Assistant und Extended Log Settings

Two additional help menu items have been introduced:

- "Support Assistant": an assistant with a selectable list to define which information is to be forwarded to the manufacturer via e-mail
- "Extended Log Settings": activate extended logging and tracing when requested by support.

Important: when updating from Windows 7 to Windows 8

When updating from Microsoft Windows 7 to Microsoft Windows 8, it is vital that the NCP Secure Client be de-installed before starting the update. It is also recommended that backup copies be made of any configuration files and certificates used. When the update to Windows 8 is complete, the latest version of the NCP Secure Client should then be downloaded from the NCP website and installed. Failure to de-install the NCP Secure Client before updating to Windows 8 could subsequently lead to having to carry out a new install of Windows 8.

2. Improvements / Problems Resolved in Service Release 9.30 Build 186

Compatibility problems associated with Symantec Security Center.

Problem resolved

Changes to Pre-shared Key/XAUTH Proposals

The following pre-shared key/XAUTH proposals used in Aggressive Mode have been deleted from the automatic mode policy proposals:

{ AES_CBC , HASH_SHA , XAUTH_INIT_PSK , ALT_MODP_1536 , SECONDS , (28800 * 3) , 0 , 192 },
{ AES_CBC , HASH_MD5 , XAUTH_INIT_PSK , ALT_MODP_1536 , SECONDS , (28800 * 3) , 0 , 192 },
{ AES_CBC , HASH_SHA , PRE_SHARED_KEY , ALT_MODP_1536 , SECONDS , (28800 * 3) , 0 , 192 },
{ AES_CBC , HASH_MD5 , PRE_SHARED_KEY , ALT_MODP_1536 , SECONDS , (28800 * 3) , 0 , 192 }

3. Known Issues in Service Release 9.30 Build 186

None

Service Release: **9.30 Build 146**
Date: **April 2012**

1. New Features and Enhancements in Release 9.30 Build 146

The following describes the new feature introduced in this release:

New feature: Anti-replay Protection

The delayed arrival of IP packets could imply that these are corrupt; if this feature (based on RFC 2406) is enabled, such packets are discarded. (Profile Settings / Advanced IPsec Options / Anti-replay Protection)

The following message shows that packages have been recognized and dropped:

```
"Esp: Warning - AntiReplay error on sequence number=xxxx"
```

2. Improvements / Problems Resolved in Release 9.30 Build 146

Symantec Network Threat Protection

A compatibility problem in connection with a Symantec Network Threat Protection has been resolved.

3. Known Issues in Release 9.30 Build 146

None

Service Release: 9.30 Build 133
Date: April 2012

1. New Features and Enhancements in Release 9.30 Build 133

Enhancement to the Certificate Configuration

If a hardware certificate is stored in the local computer certificate store (and accessed using the Certificate Status Protocol), i.e. the certificate is imported into the Windows certificate store, this certificate can be used for authenticating the Secure Client. If a number of certificates have been imported into the certificate store, the certificate required can be selected via the configuration GUI, by entering the Subject and Issuer Common Names.

Future Support for Platforms based on Microsoft Windows 8

This build of NCP Secure Client can be installed on beta versions of Microsoft Windows 8. Availability on that operating system is currently only intended for test purposes, and NCP gives no warranty for the correct functioning of this release and build of the NCP Secure Client on any version of Windows 8. Important: there could be errors or faulty operation on such an installation of the Secure Client.

Disconnect the Logical VPN Tunnel when the Connection is Broken

The default setting of the Secure Client ensures that the existing VPN tunnel remains established, for an unspecified length of time when a break occurs in the physical communication medium. Thus the tunnel remains logically active while the new physical connection is being established.

During the period the physical connection is broken, the normally solid green bar displayed in the Secure Client Monitor changes to a dashed green bar and the icon in the system tray flashes yellow and green. These indicators remain until the physical connection is re-established, when they return to solid green.

The monitor does not show the dashed green bar if the Secure Client's default behavior is switched off (Profile Settings / Line Management).

2. Improvements / Problems Resolved in Release 9.30 Build 133

None

3. Known Issues in Release 9.30 Build 133

None

Service Release: 9.30 Build 102
Date: February 2012

1. New Features and Enhancements in Release 9.30 Build 102

Visual Feedback about Status of Tunnel

When the physical communication medium connection, used to establish a VPN tunnel, breaks, the existing VPN tunnel remains established, i.e. the tunnel remains logically active, for an unspecified length of time. Use of the logical tunnel by pre-existing connections can resume when the physical connection has been re-established.

During the period the physical connection is broken, the normally solid green line displayed in the Secure Client Monitor changes to a dashed green line and the icon in the system tray flashes yellow and green. These indicators remain until the physical connection is re-established, when they return to solid green.

If the Secure Client loses the Internet connection and the tunnel remains logically connected, this status is displayed in a balloon over the tray icon. In this way the user has feedback about the status, even when the monitor is minimized.

Enhancements to Online Help and Tips

The help text has been adapted to the current version of the Secure Client. The dialog for profile groups has been enhanced with a help button. All help text is available, as usual, via a help button or, context sensitive, with the F1 key. The tips have been adapted to the current version of the Secure Client.

2. Improvements / Problems Resolved in Release 9.30 Build 102

Blocked Monitor

When displaying a PKI error message via the callback function, if the monitor was minimized during startup before the monitor image was fully displayed, the error message could not be displayed and the monitor was blocked.

Routing Tables Updated Incorrectly

The Secure Client monitors DHCP requests on every network adapter, in order to keep IP related information for each adapter. Some situations require that the Secure Client triggers a DHCP exchange with a RENEW command. If a RENEW command was issued for an adapter without an IP address or with link status "down", the subsequent route table alterations could not be performed for some minutes.

Error when Setting Routes in Split-Tunneling

In some cases routes were incorrectly set when using split-tunneling.

Error in Export File on Network Drive

Until now, a Secure Client's profile settings were not directly exported to a file on a network drive.

3. Known Issues in Release 9.30 Build 102

None

Service Release: **9.30 Build 75**
Date: **November 2011**

1. New Features and Enhancements in Release 9.30 Build 075

Testing for Internet Availability

Network Tests are an option in the Secure Client Monitor's Help Menu and these can be used to test Internet availability. They support both PING to an IP Address in the Internet as well as resolution of an Internet Domain Name to an IP address. Domain names should be of the form "ncp-e.com".
Enter the address and press the corresponding Test button.
The test results are displayed via a symbol (success: green tick, failure: red cross). More details are displayed in a clear text log.

Animation of Connection Establishment

The user gets an optical feedback immediately after the Connect button has been pressed, in the form of a rotating symbol. This symbol, signaling the process of connection establishment, is displayed for the duration of this process. If the connection cannot be established, the rotating symbol disappears and an error message is displayed in the Secure Client Monitor's graphics field instead of the normal green connection bar.

Automated Search for New Software Update

If the menu item "Search for Updates" is called, a new dialog is displayed via which the search cycle (never, daily, weekly, monthly) can be configured. In addition there is a new button "Search now".

Command Line Tool "NcpClientCmd"

Alternative command line program to "rwscmd", which does not make use of graphical output.

2. Improvements / Problems Resolved in Release 9.30 Build 075

None

3. Known Issues in Release 9.30 Build 075

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, Windows 7, Windows Vista, Windows XP

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, Quick 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)

- 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 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
- VPN Tunnel Traffic Monitoring (Tunnel Availability Tests)