NCP Secure Entry Client (Win32/64)

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

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

Improvements when using a GPRS / 3G connection

Support for the Mobile Broadband Adapter has been optimized. In addition GPRS/3G authentication with PAP or CHAP has been improved.

USB SmartCard Problem Resolved

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

Hotspot Login and Proxy Settings Deactivation

If Hotspot Login was pressed a second time and before expiry of the timer to reset the proxy settings, the proxy settings were permanently deactivated

This problem has been resolved.

3. Known Issues

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 this Service Release

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.

Manual definition of a GPRS data connection (MS Windows XP and MS Windows Vista only) (Force Edge/GPRS in order to prevent continual switchover to 3G)

3G hardware automatically switches between the two alternative wireless networks, GPRS (2G) and UMTS (3G), dependent on the received signal strength. If this automatic changeover is not desired, MS Windows XP and MS Windows Vista can be set for manual activation of the GPRS wireless network.

Hotspot login optimizations associated with failed Wi-Fi connections

If an attempt is made to logon to a hotspot without a Wi-Fi connection having first been established, the user is prompted with a warning message at the start of the logon process. The actual message displayed is dependent on whether or not the Wi-Fi adapter is being managed by the NCP Secure Client software:

If the Wi-Fi adapter IS NOT being managed by the NCP Secure Client software, the following message is displayed:

Cannot logon to the hotspot.

Please establish a network connection, via Wi-Fi or another communication medium, to the hotspot and repeat the "Hotspot Logon"

After pressing "OK" to continue, the user should then establish a suitable connection to the hotspot access point and then select "Hotspot Logon" from the "Connection" main menu.

If the Wi-Fi adapter IS being managed by the NCP Secure Client software, the following message is displayed:

Cannot logon to the hotspot.

Please first ensure there is a connection to the hotspot

Wi-Fi network, then logon to the hotspot again.

If you want to open the Wi-Fi configuration, press "Yes"

If you want to logon via another medium, first establish a network connection and then press "No"

If the user presses "Yes", the "Wi-Fi Settings" window is displayed where a suitable Wi-Fi profile can be created.

If the user wants to logon via another medium, he/she must first create a suitable connection profile to the hotspot using another communication medium and then return to this dialog and press "No".

When a suitable profile has been created, the user should then repeat the "Hotspot Logon".

UDP-Prefiltering - new default value

The default value for UDP prefiltering ("Configuration" menu, "Firewall / Options / General") is now OFF. In addition, this function is now coupled with the Firewall, i.e. it is only effective when the Firewall has been activated.

If the Firewall is not activated, the OFF value is passed to the Firewall module, regardless of which value is set. The configured value is stored under a new ID. When the profile settings (.cfg and .cnf) file is read, the parameter is checked, inserted and the existing value changed as necessary.

The feature is implemented in such a way that the Monitor is backwards compatible and can continue to be configured with the existing Client plugin.

Firewall dialog does not block other Client Monitor dialogs

The firewall dialog has been modified to allow other Monitor dialogs to be used in parallel with the firewall dialog.

Automatic configuration of a wireless network connection (evaluating the ProviderID to enable a Provider List to be selected)

When creating a 3G profile for GPRS / 3G (in Configuration menu under "Profile Settings") it is no longer necessary to specify a manual configuration. With the default setting "APN from SIM-card", the corresponding configuration settings (APN, phone number, username and password) are read from the APN.INI file using the ProviderID taken from the SIM card. Prerequisite is the correct installation of the 3G hardware.

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

Optimizations in Seamless Roaming

"Seamless Roaming" functionality has been optimized to make a more intelligent selection of the connection media available. For example, when a LAN connection is active, a "less optimal" medium such as Wi-Fi is mostly ignored, ensuring that the physical LAN connection is not broken.

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

Permit all Ports with Hotspot Logon

In order to be able to login to the corporate network from any hotspot in the world, it may be necessary to use any TCP port, rather than just 80 (http) or 443 (https), as some hotspots perform dynamic port selection.

In the "Hotspot Configuration" folder (Monitor Menu / Configuration / Hotspot):

a) an individual port or a range of ports can be entered in the "Additional Ports" field, or

b) if the switch "Permit all ports for hotspot logon" is selected, the input field is grayed out, making it non-editable, and ports 1-65535 are automatically entered in the "Additional Ports" field and.

Prompt for Access Credentials after Hibernation/Standby when in Automatic Connection Mode

If security requirements demand that, when in automatic connection mode, the cached VPN access credentials (username and password) must be deleted from memory after hibernation or standby, the option "Prompt for username and password after hibernation/standby", located under "Configuration / Logon Options / Logoff", can be activated. This ensures that the user is prompted to enter username and password after a restart from hibernation or standby.

APN from SIM Card

The APN (Access Point Name) defines the access point via which a mobile Internet connection can be established over 2G/3G/4G. Each mobile wireless service provider has their own unique APN profile and the APN details configured in the Secure Client software must match those of the corresponding mobile network.

Until now, the APN settings were manually configurable and, in order to simplify the user's task, were centrally pre-configured. However, if a SIM card from another mobile wireless service provider were to be used, the user had to manually change the APN settings locally.

This configuration task has been obviated by this new version; configuration of the correct APN is now handled automatically. APN.ini has been extended with the NetIDs of all service providers. When using the Profile Wizard to create a new GPRS/3G profile and the Configuration Mode "APN from SIM card" is selected (the default selection from this version onwards), all fields from the current provider configuration are deleted. The Secure Client then uses the NetID from the SIM card to search the APN.ini file for the associated APN details.

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 of information 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

Optimization of 3G Connection Establishment

If a 3G connection is to be established in an area where there is poor reception, the Secure Client will autonomously make three attempts to successfully establish a connection. This internal process is only logged in the log-file, and its occurrence is only signaled there.

Seamless Roaming Related Optimizations

Further optimizations in connection with Seamless Roaming have been incorporated, particularly in connection with the recognition and handling of mobile wireless and Wi-Fi connections.

LOG Output Related Optimizations

A change from one communication medium to another is logged in the log book, for example: "MONITOR: Communication Medium change LAN=-> WLAN"

In the logbook, scrolling sometimes could not be stopped when a line had been highlighted. This happened when there were more than 400 entries in ListView.

Highlighting has been added to aid recognition of problems.

Booting, Full Version, Firewall Not Displayed

Under certain circumstances, after being booted, and only with a full version, the firewall was not displayed.

Compatibility Problems Associated with Symantec Security Center.

Problem resolved

Batch File Without Path Details was Not Being Started

Applications (batch files and programs) located in the NCP program directory and configured, for automatic, connection dependent start, in "Configuration / Logon Options / Ext Applications" without a path entry being specified were not being started. This was also the case for firewall configurations under "Friendly Networks / Actions" and for configuration of the connection options under "Configuration / Link Options / Ext. Applications". This problem has been 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 }

Friendly Net, Statically Configured Network Adapters and System Boot

If a network adapter configured with a static IP address is not connected to a network while the system is rebooting, Friendly Net status will not be detected after the adapter has been connected to a network that corresponds to a Friendly Net. This problem has been resolved.

Friendly Net, Statically Configured IP Address and No Standard Gateway

A Friendly Net detection problem, relating to the combination of network adapter configured with a static IP address but without a standard gateway, has been resolved.

Friendly Net and RWSCMD

If the firewall was switched off with RWSCMD (rwscmd /firewalloff), Friendly Net status was not displayed correctly and the full functionality of the firewall was not switched off correctly. This problem has been resolved.

By default, changes to firewall settings made during the Firewall-Off phase are not actioned.

Using Special Characters for Wi-Fi/WPA Keys or for Mobile Broadband Username/Password

It is now possible to use special characters for Wi-Fi/WPA keys as well as for Mobile Broadband access information (username and password).

Other problems resolved

- In "automatic" Connection Mode, user login was incorrectly requested under certain circumstances. Problem resolved.
- An error in the NAT module in connection with incoming sessions has been corrected.
- An error relating to IKEv2 and UDP encapsulation via port 4500 has been corrected.
- An error message was incorrectly displayed on the firewall when the system was being closed down. Problem resolved.
- A problem, associated with changing the SIM PIN in connection with Mobile Broadband, has been resolved.
- If, in the Profile Settings of a GPRS/3G profile the 3G password was set to "<pwreq>" and username left blank, the username/password dialog was displayed with username "<dummy>". Now, the username is displayed as a string of spaces.

3. Known Issues in Service Release 9.30 Build 186

Repeated Entry of Wrong GPRS / UMTS / 3G PIN

After the wrong PIN (GPRS / UMTS / 3G) has been entered repeatedly the PUK will be requested. This can only be entered correctly when:

- the Monitor has been started with Administrator rights
- the User Account Control (UAC) settings have been set to the correct low level

(Vista and Windows 7)

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

1. New Features and Enhancements in Service Release 9.30 Build 146

Seamless Roaming under IKEv2

Seamless Roaming can now be used for IPsec connections that are established using IKEv2-based IKE policies. (Profile Settings / IPsec General Settings / Exch. Mode / IKEv2)

Prerequisite: NCP Secure Enterprise VPN Server from version 8.10 onwards.

Language Support: Spanish

Monitor menus and help files are now available in Spanish. (Monitor menu / View / Language)

Diffie Hellman Groups 15-18 – for IPsec Policies (PFS)

DH Groups 15-18 were introduced in release 9.30 build 70 for use in IKE policies exclusively. From this release 9.30 build 146 onwards, they can now be used in IPsec Policies – Perfect Forward Secrecy (PFS).

New Feature: Anti-replay Protection

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

The following message shows that packages are recognized and dropped:
`"Esp: Warning - AntiReplay error on sequence number=xxxx"`

Enhancement to the Certificate Configuration

If a hardware certificate is stored in the "Computer Certificate Store" 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.

In contrast to a user specific certificate in the "CSP User Certificate Store", which can only be used after the Windows user has first logged on, hardware certificates from the "Computer Certificate Store" can be used while the machine is booting (for example for domain registration).

If a hardware certificate is used in addition to a user certificate, this will ensure that the associated user always connects to the VPN gateway from the same computer.

Future Support for Platforms Based on Microsoft Windows 8

The NCP Secure Entry 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 Entry Client on any version of Windows 8. Important: there could be errors or faulty operation on such an installation of the Secure Client.

Optimizations in Seamless Roaming

2. Improvements / Problems Resolved in Service Release 9.30 Build 146

Symantec Network Threat Protection

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

GPRS/3G Configuration mode: Provider List: Germany / T-Mobile D (Germany)

The APN for this provider has been corrected to "internet.telekom"

3. Known Issues in Service Release 9.30 Build 146

Additional Ports in Hotspot Configuration

The functionality that uses the definition of additional ports within the hotspot configuration will fail under certain circumstances.
This error only occurs when the hotspot login must initially be established via a specific port – such as 8080. In the case of conventional, public hotspots this error does not occur as here a default web browser request to port 80 or 443 on the server is redirected to the hotspot login page. In this case, the additionally configured ports can be used.

Service Release: **9.30 Build 102**
Date: **February 2012**

1. New Features and Enhancements in Service 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.

The default behavior is to preserve the logical tunnel connection when the physical connection is broken. This default behavior can be changed by enabling the function "Disconnect the logical VPN tunnel when the connection is broken" in the Profile / Line Management menu.

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.

Enhancement of the 3G Panel

The GPRS / 3G panel, displayed in the Client Monitor when a profile is used that makes use of these connection media or LTE, has been enhanced to include LTE, in line with the new LTE standard. The name of the network type displayed, together with its field strength, will be dependent on the provider's wireless network currently being used. This also applies for the NCP GINA 3G panel.

External Applications

The facility to start external applications (Logon options / Ext. applications) has been enhanced to enable scripts with the extension *.vbs to also be started.

Importing Configuration Locks

Extensions have been made to the files import-de.txt and import-en.txt for importing configuration locks. The following options are now available:

- profiles can be exported
- profiles can be imported.

Wi-Fi Configuration Assistant

The Wi-Fi Configuration assistant now only lists an open, unprotected Wi-Fi access point as a hotspot logon if this access point is a known SSID of a hotspot provider.

2. Improvements / Problems Resolved in Service 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 as password and pre-shared key were not transferred in such a case.

3. Known Issues in Service Release 9.30 Build 102

None

Major Release: **9.30 Build 70**
Date: **October 2011**

1. New Features and Enhancements in Major Release 9.30 Build 70

Seamless Roaming

Seamless Roaming supports the automatic switchover of the existing VPN tunnel to another Internet communication medium. If a laptop, for example, is set into a docking station, the switchover is from the previously used Wi-Fi or GPRS/3G connection to the LAN connection. In doing so, the VPN tunnel IP address is preserved, ensuring that any application(s) communicating over the VPN tunnel are not disrupted during operation.

If, due to poor signal reception for example, the Internet connection is temporarily interrupted, the VPN tunnel is logically preserved. Again, in such a case, an application communicating via the VPN tunnel is unaffected by the disruption.

Prerequisite is an NCP Secure Enterprise VPN Server version 8.05. Seamless Roaming is only supported under IKEv1 based connections.

International Expansion of the 3G Provider List

Support of Profile settings for 3G and GPRS connections has been expanded with an International Provider List. When in configuration mode, selection of a country will display the most important providers and selection of a provider will automatically configure the parameters associated with that provider. The Provider List is editable and stored as APN.ini in the installation directory. (Configuration settings are stored in the Profile Settings under GPRS / 3G.)

Windows 7 - Mobile Broadband Support

The higher transfer rates supported by LTE would have meant that the earlier implementation based on MS Windows virtual COM ports would have been a bottleneck. Communication via the MS Windows Mobile Broadband interface removes this bottleneck.

IKEv2 Support

The implementation of Internet Key Exchange Protocol Version 2 (IKEv2), including the Mobility Extensions (MOBIKE), in the Secure Client's base, makes the Secure Client compatible with the latest versions of IPsec gateways such as Microsoft Windows Server 2008 R2.
Selection of the alternatives, IKEv1 or IKEv2, is configured in the Secure Client's profile settings under the "IPsec Settings / Exchange Mode" rubric.

Wi-Fi Configuration Wizard Enhancement

If a new Wi-Fi profile is created using the Wi-Fi configuration wizard, on completion a new connection is immediately established using the new profile.

Disable Proxy System Settings

Any proxy server settings defined for the system can be disabled with a switch in the hotspot configuration settings. The proxy server will be automatically re-activated immediately after expiry of the timeout (see below) or successful establishment of a VPN connection.

Note that these settings only work with browsers that make use of the system settings, such as Safari, Google Chrome, Internet Explorer, Firefox.

Project Logo has been Renamed Custom Branding Option

"Project Logo" option has been renamed in this and further versions to "Custom Branding Option" in all languages.

Testing for Internet Availability

Network Tests are an option 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.
The tests are particularly useful for testing firewall rules for DNS requests and outgoing connections to the Internet.

Diffie Hellman Groups 15-18

The Diffie Hellman Group enhancements are exclusively for IKE Policies.

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".

Disconnect Wi-Fi when VPN Tunnel Disconnects

Security in a hotspot environment is increased by setting the option "Disconnect Wi-Fi when VPN tunnel disconnects". This parameter has been introduced into the Wi-Fi Profile configuration under "General".

New Firewall Configuration GUI

The Firewall GUI has been reworked enabling firewall rules to be activated and deactivated directly with a mouse click. New rules can be created more easily and there is a better overview of the rules. A DENY rule is always placed at the head of the rules. The "Open Basic Setting" has been removed.

Firewall – New parameter "Start FND Dependent Action"

As soon as the Secure Client detects a change from unknown to friendly networks (or the reverse), a dependent action can be started. This enables, for example, an external program to alter proxy system settings of a Windows system.

Firewall IPv6 Capability

The firewall is now capable of handling IPv6 traffic.

Command Line Tool "NcpClientCmd"

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

Hiding Blocked Menu Items

Those menu items in the Secure Client Monitor's pull down menus that have been locked from use by the administrator are completely suppressed, and the pull down menus contracted accordingly, and not just grayed out as in the previous versions. Locking is configured using the Configuration Locks in the Secure Entry Client "Configuration" pull down menu.

2. Improvements / Problems Resolved in Major Release 9.30 Build 70

Changes in the WLAN Assistant

Previously, if, using the Wi-Fi configuration wizard, an unprotected Wi-Fi connection was configured, the dialog for Hotspot logon was displayed. This often led to confusion as only a limited list of hotspots was displayed.

Now, if an unprotected Wi-Fi connection is configured, the Hotspot dialog is only displayed when the SSID is from a known hotspot provider. In such a case the Hotspot List will contain the associated SSID.

3. Known Issues in Major Release 9.30 Build 70

None

4. Getting Help for the NCP Secure Entry Client (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 Entry Client (Win32/64), visit:
http://www.ncp-e.com/en/about-us/contact.html

Mail: helpdesk@ncp-e.com

5. Features

Operating Systems

Microsoft Windows (32 & 64 bit): Windows 8, Windows 7, Windows Vista, Windows XP

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)
  - Communication only in the tunnel
  - Message Transfer Unit (MTU) size fragmentation and reassembly
  - Network Address Translation-Traversal (NAT-T)
  - Dead Peer Detection (DPD)

Authentication

- Internet Key Exchange (IKE):
  - Aggressive Mode and Main Mode, Quick Mode
  - IKEv2 incl. Mobility and Multihoming Protocol (MOBIKE)
  - 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:
  - User Authentication via GINA/Credential Management
    - Windows Logon over VPN connection
  - XAUTH 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
- PAP, CHAP, MS-CHAP v2
- Pre-Authentication (Authentication before VPN establishment)
- IEEE 802.1x:
  - Extensible Authentication Protocol – Message Digest 5 (EAP-MD5): Extended authentication relative to switches and access points (layer 2)
  - Extensible Authentication Protocol – Transport Layer Security (EAP-TLS): Extended authentication relative to switches and access points on the basis of certificates (layer 2)
  - Extensible Authentication Protocol – Transport Layer Security (MS-CHAP v2): Extended authentication relative to switches and access points on the basis of certificates using IKEv2 (layer 2)
- Secure hotspot logon using HTTP or EAP
- 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

- SHA1, SHA-256, SHA-384, SHA-512, MD5
- Diffie Hellman groups 1, 2, 5, 14, 15-18 used for asymmetric key exchange and PFS

Public Key Infrastructure (PKI) - Strong Authentication

- X.509 v.3 Standard
- Entrust ready
- 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 and 3.0
    - Smart card reader systems
      - PC/SC, CT-API
    - Soft certificates
      - 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)
  - Certificate Management Protocol (CMP)[i]

Personal Firewall

- Stateful Packet Inspection
- IP-NAT (Network Address Translation)
- Friendly Net Detection (FND)
  - Firewall rules adapted automatically if connected network recognized based on its IP subnet address or an NCP FND Server[i]
  - FND dependent actions
- Supports secure hotspot logon feature
- Start application before or after VPN establishment
- Differentiated filter rules relative to:
  - Protocols, ports or IP addresses
  - LAN adapter protection,
- Protect VMware Guest systems
- IPv4 and IPv6 support

Networking Features

Secure Network Interface

- LAN Emulation
  - NCP Virtual Ethernet adapter with NDIS interface
- Wireless Local Area Network (WLAN) support
- Wireless Wide Area Network (WWAN) support

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.

Communications Media

- LAN
- Wi-Fi
- GPRS / 3G (UMTS, HSDPA), GSM (incl. HSCSD)
  - Windows 7 and 8 – Mobile Broadband Support
- xDSL (PPPoE)
- xDSL (PPP over CAPI, AVM)
- PSTN
- ISDN
- Automatic Media Detection (AMD)
- External Dialer
- Seamless Roaming (LAN / Wi-Fi / GPRS / 3G)

Dialers

- NCP Secure Dialer
- Microsoft RAS Dialer (for ISP dial-up using dial-up script)

Line Management

- Dead Peer Detection with configurable time interval
- Short Hold Mode
- Inactivity Timeout (send, receive or bi-directional)
- Channel Bundling (dynamic in ISDN) with freely configurable threshold value
- Wi-Fi Roaming (handover)
- Budget Manager
  - Separate management of Wi-Fi, GPRS/3G, xDSL, PPTP, ISDN and modem connections
  - Duration or volume based budgets
  - Management of GPRS/3G roaming costs
  - Separate management of multiple Wi-Fi access points

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

VPN Path Finder
- NCP Path Finder Technology
  - Fallback to HTTPS (port 443) from IPsec if neither port 500 nor UDP encapsulation are available [ii]

Data Compression
- IPsec Compression: lzs, deflate

Link Firewall
- Stateful Packet Inspection

Additional Features
- VoIP prioritization
- UDP encapsulation
- IPsec roaming [ii]
- Wi-Fi roaming [ii]
- WISPr support (T-Mobile hotspots)

Point-to-Point Protocols
- PPP over Ethernet
- PPP over GSM,
- PPP over ISDN,
- PPP over PSTN,
  - LCP, IPCP, MLP, CCP, PAP, CHAP, ECP

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)
- Internet Key Exchange Protocol v2 (IKEv2) (RFC 4306, 5996)
  - IKEv2 Mobility and Multihoming Protocol (MOBIKE) (RFC 4555)
- UDP encapsulation of IPsec Packets (RFC 3948),
- Additional Extended Key Usages:
  - id-kp-ipsecIKE (1.3.6.1.5.5.7.3.17) in accordance with RFC 4945
  - anyExtendedKeyUsage (2.5.29.37.0) in accordance with RFC 4945
  - IKEIntermediate (1.3.6.1.5.5.8.2.2) in accordance with draft-ietf-IPsec-pki-req-03

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

Usability Features

APN from SIM Card

The APN (Access Point Name) defines the access point of a mobile data connection at a provider. This option makes it easy to change to a less expensive provider when roaming, especially when abroad. The system automatically takes APN data from the new SIM card and uses it to configure the corresponding profile.

Secure Client Monitor

Intuitive Graphical User Interface

- Language support (English, German, French, Spanish)
  - Monitor & Setup: en, de, fr, es
  - Online Help and License en, de, es
- 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 (PCMCIA, embedded)
- Password protected configuration and profile management
- Trace tool for error diagnosis
- Monitor can be tailored to include company name or support information
- Tip of the Day
- Hotkey connection establishment and disconnection
- Custom Branding Option
- Internet Availability Tests
- VPN Tunnel Traffic Monitoring (Tunnel Availability Tests)

Notes

[i] If you wish to download NCP's FND Server as an add-on, please click here:
http://www.ncp-e.com/en/downloads/software.html

[ii] Prerequisite: NCP Secure Enterprise VPN Server V 8.0 and later

More information on the NCP Secure Entry Client (Win32/64) is available on the Internet at:
http://www.ncp-e.com/en/products/universal-vpn-client-suite.html

Test it for free: download a free, 30-day full version of the NCP Secure Entry Client (Win32/64) from NCP's website:
http://www.ncp-e.com/en/downloads/software.html