Release Notes

NCP Secure Enterprise Client (Win32/64)

Service Release: 9.32 Build 142
Date: October 2013

1. New Features and Enhancements

**IKEv2 Profile Configuration GUI Improvements on Update to Version 10.0 License**

After applying a version 10.0 license a new configuration window is available in the Profile Configuration. For license update via the Secure Enterprise Management the Client Plug-in version 10.0 build 002 or later is required.

The new window in the "Extended Configuration" mode provides the options, in the first configuration field of the "Standard Configuration", to configure IKEv1 or IKEv2 (as well as L2TP) as the "Protocol" for the "VPN Connection"; this corresponds to "Exchange Mode" under "Advanced IPsec Options" in previous versions of the Secure Client. In addition the type of "Authentication" can be configured here for IKEv1 (XAUTH or none) or for IKEv2 (Certificate, Pre-shared Key or EAP).

Dependent on the IKE version selected, a second step enables all other configuration fields for "IKEv1" or "IKEv2" and "IPSec" relevant settings, together with the respective policies, to be selected or configured here.

**IPv6 support**

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

a) to establish and carry traffic across the link to the VPN tunnel endpoint at the VPN gateway

b) to communicate with any NCP Secure Enterprise HA Servers used to provide HA services for an NCP Secure Enterprise VPN Server.

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 HA Server (WIN): Version 3.04 build 020
NCP Secure Enterprise VPN Server (Linux): Version 8.11 from rev 5620
NCP Secure Enterprise HA Server (Linux): Version 3.04 from rev 3933
Release Notes

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 Enterprise Client.

2. Improvements / Problems Resolved

Notification of Connection Refusal/Disconnect due to User Prioritization

If a connection is refused or disconnected due to user prioritization, notification is via an infobox. In addition, a disconnect is sent to the driver, ensuring no further attempts to establish a connection are made.

A connection disconnection due to user prioritization does not affect the behavior of automatic media detection nor Seamless Roaming, nor does it have any effect on the "Connection Mode" configured.

Improvement 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.

PIN request for IKEv2 Authentication

When using IKEv2, the PIN for a certificate was requested, even though the profile was configured to use a Pre-shared Key. This problem has been resolved.

Other Problems Resolved

- On performing a configuration update of the NCP Dynamic Net Guard firewall of the Secure Enterprise Client, the profile configurations are now correctly imported, and, in particular, the state of the "Path Finder" parameter remains unaltered.
- The Wi-Fi profile in which only locked parameters should modified can now be updated at the Secure Enterprise Management ("Only update locked parameters").
- Plugging and un-plugging a USB SmartCard reader under Windows 8 is now recognized correctly by the Client.
- The Client monitor can be minimized and maximized at any time.
- Compatibility problems with Cisco gateways have been resolved.
- IPsec over L2TP works correctly, also when packets are being fragmented.
- The PPPoE Provider password remains correct.
- Trace functionality has been corrected and optimized
- If, during a LAN update, a configuration with a version 10.0 license key was received when the monitor had not yet been started, the license key was not recognized, and the error message "The installed software version is older than the license key!" was displayed. License handling now works correctly.
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 Enterprise Client is no longer functional. After the Windows update, de-install the NCP software, keeping the current configuration settings and then install the NCP Secure Enterprise Client version 9.32 144 software.

No Support for IPsec over L2TP

When a version 10.0 license key is entered, support for IPsec over L2TP is canceled.
Release Notes

Service Release: 9.32 Build 124
Date: August 2013

1. New Features and Enhancements
None

2. Improvements / Problems Resolved

Problems resolved in the GUI of the Expert Mode of the Profile Settings
Revision of the FIPS Mode

3. Known Issues
If a version 10 license key is used to activate the software, support for IPsec over L2TP is canceled.
1. New Features and Enhancements

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

Client Prioritization by an HA Server
The VPN access by Clients (from this version onwards) to a VPN gateway (from version 8.11 build 137 onwards) can be managed by an HA Server (from version 3.04 build 9 onwards) or through an NCP Secure Enterprise Management (using Server Plug-in version 8.11 build 40) according to a priority scheme.

The prioritization of Clients’ access to VPN connections to a gateway in an HA environment is important when capacity is at a maximum, i.e. when there are not enough free VPN tunnels available for all Clients

User priority (Clients or Domain Groups) can be predefined at the HA server or via Enterprise Management, ensuring that Clients with a sufficiently high priority always get VPN access to the gateway in the HA environment. Connections from lower priority Clients will be disconnected in such circumstances, and disconnections and rejections of VPN connection establishment attempts are logged with a corresponding message at the Client (from version 9.32 build 73 onwards).

The following features require a version 10 product key:

Optimized IKEv2 Configuration
The Client Monitor now supports creation of an IKEv2 policy in the "Configuration" / "IPsec Settings" folder. IKEv2 key exchange is then handled in accordance with this policy.

Other IKEv2 configuration parameters are located in the "Standard Configuration" connection profile folder. The corresponding authentication – certificate, pre-shared key or EAP - can be configured here.

Input fields for VPN username and password or IKE-ID are unlocked or grayed out, dependent on the authentication method chosen.

The IKEv2 policy required can be selected in the connection profile settings under "IPsec", providing Automatic Mode has not been selected. In addition, Diffie-Hellman and PFS-Groups can be selected to be used for IKEv2 key exchange with Elliptical Curve Cryptography (ECP with DH Groups: 19, 20, 21, 25, 26).

The policy configuration editor can be called directly from the profile settings IPsec configuration folder, in order to configure policies.

Support for Elliptic Curves in Certificates and Key Exchange Processes (ECC, Elliptic Curve Cryptography)
Various storage media and locations can be accessed when using certificates that employ Elliptical Curve Cryptography. Such certificates can be read from PKCS#12 files or from PKCS#11 or PC/SC interfaces via a SmartCard reader, or they can be accessed via the Windows CSP or CNG.

Verification of signatures using ECC is only supported under IKEv2. Therefore newer SmartCards such as TCOS 3.0 V2, which only employ Elliptical Curve Cryptography, can only be used in connection with IKEv2 connections.
Release Notes

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 "Connection" / "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.

2. Improvements / Problems Resolved

None

3. Known Issues

If a version 10 license key is used to activate the software, support for IPsec over L2TP is cancelled.
Release Notes

Service Release: 9.31 Build 116
Date: February 2013

1. New Features and Enhancements

Support of NCP Secure Client software on MS Windows 8

This release is the first version of the NCP Secure Client software that is fully supported when running on Microsoft Windows 8, either Professional or Enterprise. Previous versions of the Secure Client software are not supported when running on Windows 8. 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
- Perform an upgrade install of this version of the 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, 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.

Hiding the NCP Network Adapter in the System

From Windows 7 onwards, the NCP Secure Enterprise 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
**Release Notes**

**Hotspot login enhancements 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 logon via the Wi-Fi network, press “Yes”.

  If you want to logon via another communication medium, press "No".

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

  If "No" is pressed then the user must create a suitable connection profile to the hotspot using another communication medium.

  When a suitable profile is profile, the user should establish a connection via it to the hotspot access point and repeat the "Hotspot Logon".

**UDP Prefiltering - new default value**

The default value for UDP prefiltering is now OFF. In addition, this function is 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.

UDP Prefiltering can be configured under the "Firewall / Options / General" Monitor menu item.

**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.

**Automatic configuration of a wireless network connection**

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 NetID taken from the SIM card. Prerequisite is the correct installation of the 3G hardware.
Release Notes

GUI / Monitor Optimizations

The "Log Book" sub-menu is now located under the "Help" menu. The "Extended Log Settings" and "Support Assistant" sub-menus have also been introduced here.

The "Connect" / "Disconnect" button has been moved to the RH side of the Monitor and the (optional) Company Logo is displayed on the LH side.

The status icons displayed under the graphical frame of the Monitor are linked to the statistics setting (in the "Display Statistics" View menu) and are only displayed when the statistics are being displayed.

The edit "Profile Settings" screen includes an option, only available in Expert mode, to display the help text of the item currently pointed to by the cursor.

The NCP Secure Client has been optimized in connection with "Barrier Free" operation and makes use of the "High Contrast" display mode, 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.

Support Assistant and Extended Log Settings

Two additional menu items have been introduced under the top level "Help" menu:

- Use the "Extended Log Settings" to activate extended logging and tracing of individual services of the NCP Secure Client software. Logging and tracing is designed to be used to assist support personnel in diagnosing problems. The "Restart" buttons associated with the corresponding log settings are only for restarting the individual services, and not the computer.
- The "Support Assistant" displays a list of information from which individual sets of information can be selected for forwarding via e-mail to the NCP support desk.

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.

2. Improvements / Problems Resolved

None

3. Known Issues

None
Release Notes

Service Release: 9.30 Build 186
Date: October 2012

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

The following features and enhancements are introduced with this release:

**Hide Username when Prompted for Credentials**

During the re-establishment of a VPN connection with manual input of the access credentials (after the previous VPN connection was disconnected), the user can be forced to re-enter the username in order to successfully establish the new VPN connection. To force this behavior, enable the parameter "Hide username when prompted for credentials", located under "Profile Settings / Expert Mode / Line Management". The parameter is effective on the VPN connection-establishment credentials dialog as well as during Windows pre-logon.

**Security Check after Hibernation/Standby**

In order to prevent unauthorized use of a VPN connection which is being re-established automatically after the system resumes from hibernation or standby, the user can be forced to re-enter username and password. This feature, "Prompt for username and password after hibernation/standby", can be activated under "Configuration / Logon Options / Logoff".

**APN from SIM Card**

APN.ini has been extended with the NetIDs of all the service providers in all countries with a GPRS/3G wireless network. When using the Profile Wizard to create a new GPRS/3G profile and the Configuration Mode "APN from SIM card" is selected, all fields from the current provider configuration are deleted. The driver 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**

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. Occasionally, these delays are insufficient and an error message is displayed, usually generating a support case etc. In such a case, the wait time can be reconfigured in 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.
Release Notes

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.

Identical Source and Destination Ports in IKE

This parameter is located in "Profile Settings / Expert Mode / Advanced IPsec Options". When enabled, the IKE message payloads are handled in strict compliance with the IKE RFC, in particular the same numerical value is used for both the source and destination ports in use. Port numbers are 500 when using standard IPsec or 4500 (default, can be altered) when using UDP encapsulation.

Always Use IKE Fragmentation

This parameter is located in "Profile Settings / Expert Mode / Advanced IPsec Options". If enabled, IKE packets are always fragmented to the smallest negotiated MTU (Message Transfer Unit) size before being encapsulated, ensuring that all packets will successfully transit all subnets between Secure Client and VPN gateway. This fragmentation is carried out regardless of the result of the IKE Fragmentation negotiation, which is still carried out.

If the parameter is disabled, the behavior is fully compatible with previous Secure Client versions; the IKE Fragmentation negotiation is carried out to determine whether fragmentation is required. If so then IKE packets are fragmented before being handed to the transport layer.

This feature is intended for use in those situations where the destination VPN gateway does not fully comply with the IKE Fragmentation protocol, especially the negotiation phase.

Feature Support in NCP Secure Enterprise Management Client Configuration Plug-in

In order to manage all the above features from an NCP Secure Enterprise Management Server / Console, the Management Plug-in – Client Configuration version 9.30 later than build 066 is required.

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

Seamless Roaming Related Optimization

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. This problem has been resolved. Highlighting has been added as an additional eye-catcher.
Release Notes

Entrust-PKI and Tunnel State
A problem with Entrust PKI and the default status "Maintain logical VPN tunnel" has been resolved.

After Configuration Update from SEM, Old Wi-Fi Profile from SEM was Not Being Deleted
After a configuration update from SEM, the old Wi-Fi profile from SEM was not being deleted. This problem has been 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 / Logon" without a path entry were not being started. This was also the case for firewall configurations under "Friendly Networks / Actions" and for configuration of the connection options under "External Applications". This problem has been resolved.

Menu Item "Change PIN" Not Displayed
The menu item "Change PIN" was not being displayed if the parameter "User may change certificate configuration" was not set. The incorrect linkage has been corrected.

Globalsign Certificate Re-introduced
The Globalsign certificate has been re-introduced, as otherwise the Update Client would have needed to carry out a Software Update when an old software package that used this certificate was contained in the Update List.

Changes to Pre-shared Key/XAUTH Automatic Mode 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 IP Address 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.
Release Notes

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.


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 Secure Client Monitor has been started with Administrator rights
- the User Account Control (UAC) settings have been set to the correct low level
- (Microsoft Vista and Windows 7)
Release Notes

Service Release 9.30 Build 162
Date: May 2012

1. New Features and Enhancements in Service Release 9.30 Build 162

Enhancement of the 3G Panel
The GPRS / 3G panel, displayed in the Secure 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.

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.

Permit All Ports with Hotspot Logon
In the "Hotspot Configuration" folder (Configuration / Hotspot):
 a) a range of ports or an individual port can be entered in the "Additional Ports" field, or
 b) if the switch "Permit all ports for hotspot logon" is selected, ports 1-65535 are entered in the "Additional Ports" field and the input field is grayed out (making it non-editable).
Prerequisite: if the hotspot is to be configured using SEM, Client Plug-in 9.30 Build 054 is required.

Seamless Roaming under IKEv2
Seamless Roaming can 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).
Release Notes

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 gateway from the same computer.

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.

Future Support for Platforms based on Microsoft Windows 8

The NCP Secure Enterprise 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 Enterprise 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 162

DPD, "variable" Connection Mode and Tunnel Re-establishment

If the "Profile Settings / Line Management / Connection Mode" is set to "variable" and a VPN tunnel disconnection is triggered by Dead Peer Detection timeout, the VPN tunnel will be automatically re-established when the peer comes back online.

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"

None
Release Notes

Service Release: 9.30 Build 102
Date: January 2012

1. New Features and Enhancements in Service Release 9.30 Build 102

None

2. Improvements / Problems Resolved in Service Release 9.30 Build 102

**Error when Setting Routes in Split-Tunneling**
In some cases routes were incorrectly set when using split-tunneling.

**Error when Updating from 9.0 to 9.3**
The corresponding update package has been modified.


**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.
Release Notes

Service Release 9.30 Build 100
Date: January 2012

1. New Features and Enhancements in Service Release 9.30 Build 100

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 dashed green, 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 Secure Client’s default behavior (Maintain logical VPN tunnel) can be switched off using the Secure Client’s Expert configuration mode to enable the function "Disconnect the logical VPN tunnel when the connection is broken".

2. Improvements / Problems Resolved in Service Release 9.30 Build 100

Wrong VPN Tunnel over LAN

When the computer was connected to the Internet via a LAN cable and an attempt made to establish VPN connection via Windows interface Mobile Broadband media, the Mobile Broadband to Internet connection was established but the VPN tunnel, however, used the existing LAN cable connection.

Incorrect Carryover of Pre-shared Keys when Updating

Updating an old Secure Client failed, if that Client incorporated a VPN profile that used a pre-shared key. The VPN profile had to be modified manually, as it was not carried over correctly.

Update Error when Using iPass Client

If an iPass Client accessed the NCP Secure Enterprise Client via the API, the Secure Client update via NCP Secure Enterprise Management failed. From this release onwards, the iPass service is stopped; for this reason it is recommended that the computer is re-booted after the Secure Client update.

Correction to Ping in Roaming Mode

In Windows XP, the NCP Secure Client pings used in roaming mode were not working correctly.

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.
Wrong Message when SIM Not Inserted
The NCP 3G monitor incorrectly reported "Modem not found" even though the 3G hardware was present but a SIM was not inserted.

IPsec Loop at NCP VPN Server
During an ongoing VPN connection over LAN, Dead Peer Detection messages sent from the Secure Client (outside the tunnel) were appearing with a source address assigned to the VPN adapter and not to the LAN interface. This caused an IPsec loop on NCP VPN Server.

Optimizations when calling the NCP Secure Client
Various problems associated with calling the NCP Secure Client, via the API, from the iPass Client have been resolved.

3. Known Issues in Service Release 9.30 Build 100
None
Release Notes

Service Release 9.30 Build 092
Date: November 2011

1. New Features and Enhancements in Service Release 9.30 Build 092

Dynamic Net Guard
The NCP Secure Enterprise Client Suite includes the Dynamic Net Guard (re-named from Enterprise Dynamic Firewall), a firewall product that when installed, does not include the VPN Client functionality. Dynamic Net Guard functionality is as described in the appropriate firewall sections of the NCP Secure Enterprise Client release 9.30 build 086 Release Notes – also listed below in this document.

Automatically Setting the VPN User ID
The administrator can centrally pre-configure the VPN User ID (in "Expert mode" under "VPN Tunneling") via an environment variable, either %USERNAME% or %NCPUSERNAME%. This variable is then read from the Secure Client PC's Windows environment settings and used automatically to instantiate the VPN User ID.

If the string %USERNAME% is entered, the USERNAME Windows environment variable is read once (and used to instantiate the VPN User ID) when the Secure Client is first started, and remains unchanged over all subsequent restarts.

If %NCPUSERNAME% is entered, the USERNAME Windows environment variable is read anew each time the Secure Client is started. In this way different users can logon to Windows and each user's specific USERNAME will then be passed to the Secure Client software to instantiate the VPN User ID.

This variable and the associated functionality cannot be used if Windows logon is performed via the NCP GINA.

2. Improvements / Problems Resolved in Service Release 9.30 Build 092
None

None
Release Notes

Major Release: 9.30 Build 086
Date: November 2011

1. New Features and Enhancements in
   Major Release 9.30 Build 086

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.

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.
Release Notes

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, and Firefox.

Simplified Profile Configuration with Optimized Profile Overview

The importance of parameters and the frequency with which they must be configured is reflected in three new configuration modes now available in the profile settings: Standard, Extended and Expert. Automatic Media Detection and definition of the Default Profile are duplicated and can be altered in the list of "Profiles Available", meaning that the profile settings no longer have to be opened.

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.

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 to enable 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.
Release Notes

Firewall – New Parameter "Start FND Dependent Action"
As soon as the Secure Client detects a change from unknown to friendly network (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.

New Client Plug-in for Secure Enterprise Management
The new features described above can be reproduced and configured on the Secure Enterprise Management by using the Management Plug-in – Client Configuration, version 9.30 build 005 onwards.
In addition the menu item "Load Last Configuration" (on the Client Monitor under "Configuration") can be blocked.

2. Improvements / Problems Resolved in Service Release 9.30 Build 086

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.
The following configuration option has been removed

FND Configuration via MAC address
The capability to configure or define a friendly network by use of the MAC address has been removed.

None
4. Getting Help for the NCP Secure Enterprise Client (Win32 / 64)

To ensure that you always have the latest information about NCP’s products, always check the NCP website at:
For further information about the Enterprise Client, visit:
For further assistance with the NCP Secure Enterprise Client (Win32/64), visit:
http://www.ncp-e.com/en/company/contact.html
5. Features

Central Management

As the **Single Point of Management**, NCP’s Secure Enterprise Management (SEM) provides functionality and automation for the rollout, commissioning and efficient use of Secure Enterprise Clients. The Secure Enterprise Management (SEM) makes use of a VPN connection or the LAN (when on the company network), to automatically provide NCP Secure Enterprise Clients with:

- configuration updates,
- certificate updates, and
- updates to the Update Client.

Network Access Control / Endpoint Security

The policies for Endpoint Security (Endpoint Policy Enforcement) are created centrally at the Secure Enterprise Management (SEM) and each NCP Secure Enterprise Client is only permitted access to the company network in accordance with the corresponding rules.

High Availability Services

The NCP Secure Enterprise Client supports the NCP HA Services. These services are client / server based and can be used in two different operating modes: load balancing or failsafe mode. Regardless of the load on the server or whether a server has failed, the VPN connection to the corporate network is established and maintained reliably, in the background and without any delay for the user of the NCP Secure Enterprise Client.

Operating Systems


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)
  - Anti-replay Protection
Release Notes

Authentication

- Internet Key Exchange version 1 (IKE):
  - Aggressive Mode and Main Mode, Quick Mode
  - Pre-shared secrets
  - RSA Signatures (and associated Public Key Infrastructure)
  - Perfect Forward Secrecy (PFS)
  - IKE Config. Mode for dynamic allocation of private IP (virtual) address from address pool
- 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:
  - User Authentication via GINA/Credential Management
    - Windows Logon over VPN connection
  - XAUTH (with IKEv1) for extended user authentication
    - One-time passwords and challenge response systems
    - Authentication details from certificate (prerequisite PKI)
- Support for certificates in a PKI:
  - Soft certificates, Smart cards, and USB tokens: Multi Certificate Configurations
- Seamless rekeying
- 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)
- Secure hotspot logon using HTTP or EAP
- RSA SecurID ready

Encryption and Encryption Algorithms

Symmetrical: A-ES-CTR 128, 192, 256 bits (for IKEv2); AES 128,192,256 bits;
Blowfish 128,448 bits; Triple-DES 112,168 bits
Asymmetrical: RSA to 2048 bits, dynamic processes for key exchange
Release Notes

Hash / Message Authentication Algorithms

- SHA1, SHA-256, SHA-384, SHA-512, MD5
- Diffie Hellman groups 1, 2, 5, 14, 15 - 18, 19 - 21, 25-26 used for asymmetric key exchange and PFS
- Diffie Hellman groups 19, 20, 21, 25,26 employ Elliptical Curve Cryptography algorithm (only under IKEv2).

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
- PIN policy: administrative specification of PIN entry to any level of complexity
- Certificate Service Provider (CSP) for the use of user certificates in Windows certificate store
- Revocation:
  - End-entity Public-key Certificate Revocation List (EPRL formerly CRL)
  - Certification Authority Revocation List, (CARL formerly ARL)
  - Online Certificate Status Protocol (OCSP)
  - Certificate Management Protocol (CMP)

Personal Firewall

- Stateful Packet Inspection
- IP-NAT (Network Address Translation)
- Friendly Net Detection (Firewall rules adapted automatically if connected network recognized based on its IP subnet address, the DHCP server’s MAC address or an NCP FND Server)
- 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,
- Central administration (optional)
- Protect VMware Guest systems
- IPv4 and IPv6 support

Endpoint Security

- Endpoint Policy Enforcement
Networking Features

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

**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 and Client to NCP Secure Enterprise HA Server),
  - IP traffic inside any VPN tunnel MUST use IPv4 protocol.

**Communications Media**
- LAN
- Wi-Fi
- GPRS / 3G (UMTS, HSDPA), GSM (incl. HSCSD)
  - Windows 7 – Mobile Broadband support
  - Messaging Center (send & receive SMSs)
- 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
Release Notes

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

Data Compression
- IPsec Compression: lzs, deflate

Link Firewall
- Stateful Packet Inspection

Additional Features
- VoIP prioritization
- UDP encapsulation
- IPsec roaming
- Wi-Fi roaming

Additional Features (cont.)
- 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 associated RFCs (RFC 2401 – 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. If the user changes provider, the system automatically takes APN data from the corresponding SIM card and uses it in client configuration. This makes it easy to use inexpensive, local providers abroad.
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
- 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
- Custom Branding Option
- Internet Availability Tests
- VPN Tunnel Availability Tests

Notes
i If you wish to download NCP’s FND Server as an add-on, please click here:
ii Prerequisite: NCP Secure Enterprise Management
iii Prerequisite: NCP Secure Enterprise VPN Server V 8.0 and later