

What's New

high security remote access

NCP Secure Entry Client (Windows 32/64 Bit)

New Features version 9.23 to 9.0

Disclaimer

Considerable care has been taken in the preparation and publication of this document, errors in content, typographical or otherwise may occur. NCP makes no representations or warranties with respect to the contents or use of this manual, and explicitly disclaims all expressed or implied warranties of merchantability or use for any particular purpose. Furthermore NCP reserves the right to revise this publication and to make amendments to the content, at any time, without obligation to notify any person or entity of such revisions and changes.

Trademarks

All trademarks or registered trademarks appearing in this manual belong to their respective owners.

Overview

New features in version 9.23 to version 9.21.....	2
New features in version 9.21 to version 9.10.....	7
New features of version 9.1 relative to version 9.0	10
New features of version 9.1 relative to 9.04.....	10
New features of version 9.04 relative to 9.03.....	10
New features of version 9.03 relative to 9.01.....	11
New features of version 9.01 relative to 9.0.....	12

Please note:

- Features marked with a "p" have to be purchased, i.e. in order to use them a new license key has to be purchased.
- Of course, features of older versions, which were assigned to certain operating systems, were transferred to the latest 32 / 64 Bit platforms.
- Customers with older versions please contact marketing@ncp-e.com.

New features in version 9.23 to version 9.21

FIPS inside

The Secure Client integrates cryptographic algorithms according to the FIPS standard. The embedded cryptographic module, containing the corresponding algorithms, is certified according to FIPS 140-2 (Certificate #1051).

If you use one of the following algorithms for set-up and encryption of an IPsec connection, FIPS compatibility is always given.

- 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 and 256 Bit or Triple DES

Configuration expansion for hotspot logon (starting from V. 9.21 B. 62)

Now you can enter a further, additional, application in the configuration field for hotspot logon. This second application is responsible for communication since it is able to set up outgoing connections. An internal application-bound firewall rule monitors this application.

If both applications (hotspot logon and communication) are identical, you may refrain from entering anything in the parameter field "application for automatic firewall rule".

Carry out hotspot configuration via the monitor menu "configuration / hotspot". Set up the firewall rule via "configuration / firewall".

NCP's VPN Path-Finder Technology icon

If you set up a connection via port 443 with the VPN Path Finder, the monitor displays this via an icon in its state display (below the HQ / gateway to the right). The monitor interface displays the

icon after VPN dial up. It also appears in the interface of Windows Logon, via NCP GINA or NCP credential provider.

Language Selection

Selecting "Language" in the "View" menu of the monitor, you can choose the language of the monitor's interface. English, German and French are available to you, while Polish and Dutch have been removed. The setup languages are: English, German and French.

State Display of the Messaging Centre

You can activate the text message service of the messaging centre if the driver of a mobile connect card for GPRS / 3G has been installed on the machine. In order to use this service, the mobile connect card has to support text messages. (The monitor has to display the menu item "Mobile Connect Card" within the connection setup menu).

The client monitor features a letter symbol, after activation of this feature. In future you can open the messaging centre by simply clicking this symbol.

The meaning of the symbol's colors:

If the letter is colored in red, the messaging centre has been activated via the connection menu of the monitor but no suitable modem is available. If the letter is colored in yellow, the computer is either searching for a GPRS or 3G network, the card is faulty, the SIM PIN is missing, etc. this, of course, will be accompanied with the respective message in the quick tip. If the letter is colored in gray, the text messages can be received. If the letter is colored in green, a text message has been received. The number of unread messages can be read in the quick tip.

Use of the VPN access data for Windows logon.

You can also use "VPN user ID as user ID" for windows logon if you have specified this in the profile settings under "VPN parameter". The same is true for the "VPN password as password" feature (Gina / Credential).

If the VPN access data (VPN user ID and VPN password) are to be read from a field of the certificate used, this setting is automatically used for Windows log on, too.

Alternatively you can also define access data for Windows log on, only.

Suffix for VPN user ID

You can enter a "VPN suffix" in the profile settings as a new "Tunnel Parameter".

The "VPN Suffix" facilitates the creation of groups through the Secure Enterprise Management (SEM). Alternatively the administrator may configure an environmental variable for the "VPN suffix" or the "VPN user ID", e.g. %userdomain% or %username%, respectively. This variable is then read at the client and automatically used as a "VPN suffix".

Then the user ID is made up of "VPN user ID" plus "VPN suffix". In order to set up a VPN connection, however, the user only has to enter the personal "VPN user ID". The gateway recognizes the user group by its suffix.

Environmental variable USERNAME:

The computer uses the environmental variable USERNAME as a VPN suffix, if %username% has been entered in the field "VPN suffix". If the environmental variable is not available within the settings of the client PC, the entry %username% is used as it is.

Initialization of NCP's Secure Enterprise Client or NCP's Dynamic Personal Firewall, respectively

Initialization has been expanded with Windows environmental variables as alternative use. This means, the administrator is now in a position to configure environment variables for the user and the authentication code, in order to authenticate the client at the central management. The user does not have to interact in this process. This feature facilitates rollout of the NCP dynamic personal firewall, which runs in the background at the client machine.

Recognition of fully operative 3G cards

If the messaging center (SMS) has been activated, or a GPRS / 3G profile has been selected, the client notifies the user if the 3G card has been removed and closes the GPRS / 3G panel. If a fully operative 3G card is inserted, the GPRS / 3G panel is opened again and the network is being scanned again.

The search sequence for available GPRS / 3G hardware has been adapted, so that the computer searches for removable hardware, first, and then for integrated hardware.

Additional support of further GPRS / 3G hardware

Data of the Info Center

The NCP secure enterprise client's info center displays all relevant data of the current client version, VPN connection, state of the related services, certificates used and the modem COM ports. You can export them into a text file by using the respective button in the client's GUI. You can also export the information independent of the monitor's operation state if you enter the RWSCMD command: `rwscmd/writeClientInfoCenterData [OutFileName]`.

Expansion of attribute types for certificate check

Certificate issuer and user can create different entries in their certificates. Then these entries can be read in the respective field of the certificate displayed. The secure client can use these entries for checking incoming certificates.

Open the configuration field "certificate check" in the particular profile settings and enter the attribute, which you received from the server. This ensures that the client can only set up a connection to the server whose certificate contains the particular attribute in its certificate's user or issuer field.

The serial number of the user and the issuer (sn) of the incoming certificate have been added to the list of available attributes. (This is not the certificate serial number.)

Protect VMware Guest System

If the firewall is activated, a VMware guest system can be protected by a client installed in the main system. This means the firewall of the client has to be active in the "locked basic settings" or at least one firewall rule has to be active in the "open basic settings". The guest system cannot receive incoming connections.

VMware offers different modes for the guest system: Bridged, NAT and host only. (Independent of the firewall, the computer always uses a bidirectional communication with the main system, if you use the host only mode.)

Bridged Mode:

The guest system is completely sealed off if it is in the bridged mode and the option "Protect VM-

ware Guest System" has been selected. In this mode, there is no possibility of setting up a connection to or from the internet. Even DHCP requests are blocked.

NAT Mode:

In the NAT mode, with the option "Protect VMware Guest System" being selected, the configurable firewall rules apply to the outgoing connections. It is not possible, however, to set-up an inbound connection.

Bidirectional communication between guest system and main system remains possible.

You can activate the option "Protect VMware Guest Systems" in the firewall settings of the client and via the configuration menu of the monitor under options.

View NCP Firewall State in Windows Center

If the NCP secure enterprise client's firewall is active, its state is reported to the Windows Vista Security Center or the Windows 7 Maintenance Center respectively, and can be viewed there. (If you use Windows Vista, Service Pack 1 has to be installed, at the minimum.)

Dynamic selection of filter rules in case of negative Endpoint Security Check

According to your endpoint security policy, only devices, which comply with these policies, are allowed access to the company network. During connection setup to the gateway, the device is checked for policy compliance for the first time. If it does not comply, the client is kept in quarantine, which the Secure Enterprise Server provides (according to its configuration). There, the user has the opportunity to update the device (according to the policy configuration). If the device complies with the endpoint security policies after the updates, the client is allowed access to the company network. The Secure Server dynamically selects a different firewall rule and opens the quarantine zone.

While the VPN connection is active, further endpoint security checks are carried out in set intervals. If the policy is not met in one of those checks, e.g. the virus scanner has been deactivated, the filter rules are adapted, in a way that the VPN connection is restricted to the quarantine zone.

Prerequisite for dynamical use of the quarantine zone during a VPN connection is a NCP Secure Enterprise Server (starting with version 8.05) as well as a NCP Secure Client (starting with version 9.23).

Forced password prompt at 3G connection setup

Usually, no distinct user ID or password is required when setting up an Internet connection via 3G. If the 3G connection requires the user to enter a user ID or password, because the company's internet access has an APN (Access Point Name) or provider of its own, for example, user identification prompt can be automatically displayed in a new window.

In order to use the forced password prompt, enter <pwreq> (including angle brackets) in the password configuration field in the "GPRS / 3G" configuration of the secure clients' profile settings for the GPRS / 3G connection.

L2Sec - Certificate Configuration

If the client is used in the VPN mode "L2Sec" and encryption is configured as "SSL with certificate", connection setup to the gateway can only be carried out only with a corresponding certificate at the gateway.

Troubleshooting

Data exchange via VPN tunnel using a 3G connection and the Windows 7 interface

This only applies to 3G connections whose 3G hardware driver accesses the new Windows 7 mobile broadband interface. As a result, on computers using the operating system Windows 7, it was impossible to exchange data via the VPN tunnel if the internet connection had been established via 3G / mobile broadband and not via the client software. This error has been removed.

No VPN tunnel in friendly network

The firewall configuration of friendly networks allows you to select the option to block VPN connection setup in a friendly network. If you select this option, you can neither set up a VPN connection via the connection menu nor via the connect button in the client monitor. Connection setup has remained possible though, through the command bar of RWSCMD.EXE.

This bug has been removed, and now it is impossible to set up a connection via RWSCMD in a friendly network, provided, of course, the particular setting has been selected in the firewall configuration.

Scripts adapted for Vodafone Web Sessions

If you wish to use your mobile internet access for Vodafone Web Sessions, only the Vodafone Web Session SIM card for the 3G card has to be installed and a profile with the connection type GPRS / 3G has to be set up. Please note that the messaging center is not available during the use of Vodafone Web Sessions.

In the profile settings in "GPRS / 3G" the user defined APN has to be "event.vodafone.de" and the dial-up number "*99#". For "HTTP Logon" select the HTTP authentication script, which corresponds to your planned internet use (30 minutes = vodafoneweb-session30m.nhs, 1 hour = vodafoneweb-session01h.nhs, 24 hours = vodafoneweb-session24h.nhs).

After connection setup and entry of your access data you have direct internet access.

Readability of stored log output

The client's stored log output now features blanks to improve readability. The output "20.08.2010 15:19:55 IPsec: Start building connection", for example, has been changed to "20.08.2010 15:19:55 IPsec: Start building connection".

Additionally, notation of numbers has been localized. In English, numbers are now written "235,000.15 kByte", while they are written "235.000,15 kByte" in German.

Faulty analysis of certificates without specification of time zone

Certificates with faulty time designation (i.e. without specification of time zone) are recognized as valid, after they have expired.

Weakness in NCP's Secure Client

NCP's Secure Client had been vulnerable against an attack, known as DLL Hijacking. This attack exploits a weakness in the Windows DLL loading process.

This weakness has been patched. Further information and download under:

http://www.ncp-e.com/fileadmin/pdf/service_support/NCP_Client_Vulnerability_Statement.pdf

New features in version 9.21 to version 9.10

Windows 7 Support (p)

Full support is provided for the new Microsoft desktop operating system Windows 7 from version 9.2 onwards. The following Windows operating systems are supported: Windows XP (32/64 Bit), Windows Vista (32/64 Bit), and Windows 7 (32/64 Bit) *(Please note: The support for Windows 2000 has been discontinued, starting with NCP Secure Entry Client Version 9.2. In case of an update from Windows Vista to Windows 7, only the monitor of a Client version 9.1 can be started in order to enter a Client version 9.2 key.)*

Benefit

All current Windows desktop operating systems are supported.

NCP VPN Path Finder incl. proxy support (p)

If default IPsec via port 500 or UDP Encapsulation via a freely configurable port is not possible, the VPN Path Finder automatically switches to an alternative connection protocol - TCP encapsulation with SSL header via port 443. Prerequisite: NCP Secure Server 8.0

Benefit

The user has the possibility to connect to the corporate headquarters via VPN, even with restricted internet access (to HTTPS port 443).

Wi-Fi roaming

If the laptop is moved within the range of several access points with the same SSID, the system automatically switches to an access point with higher field strength in the case of low Wi-Fi reception. Applications via this VPN tunnel are not affected by this change.

Benefit

The NCP Client can automatically switch to different access points within corporate networks (e.g. change of location with a laptop). Applications communicating via this VPN tunnel are not affected by this.

Improved data throughput on 64 bit Windows platforms

For the use of the RWSNT service, data throughput has been augmented by about 20%.

Support for new Intel Wi-Fi driver versions 12.4.0.21 or above.

The new drivers are seen as Wi-Fi drivers instead of ethernet drivers. Due to this fact it is necessary first to uninstall the NCP Entry Client, reboot and then install the new client.

Mobile broadband support in Windows 7.

Revised 3G configuration, provider list configurable via INI file (APN.ini)

A new parameter folder GPRS / 3G has been introduced in the profile settings and with that the former 3G configuration has been revised. There are three modes now:

- a) Provider list (default setting): By selecting the provider, the APN and the dial-up number is being suggested.
- b) APN from SIM card: The APN is not handed over to the SIM card. This only works is an APN is configured on the SIM card.
- c) User-defined: The user is free to configure all dial-up parameters manually.

Benefit

The use of GPRS/3G configuration has been facilitated.

Modularization of the NCP Secure Enterprise Client

For a trial period, the NCP Secure Enterprise client may either be installed as NCP Dynamic Personal Firewall or NCP Secure Enterprise Client. After choosing either option, the full software is installed on the destination system. The NCP Dynamic Personal Firewall comprises all features of the software, except for the VPN feature; this means a centrally administrable firewall is available to the user. The product key defines, which of the two types, NCP Dynamic Personal Firewall or NCP Secure Enterprise Client, is used.

Users, who want to benefit from the advantages of a centrally administrable firewall including friendly net detection but do not need the VPN feature, are now able to purchase and license the respective solution.

At a later point in time, an upgrade to the full Enterprise Client is still possible with the respective license key.

Use of the CSP User Certificate Store

Via the certificate configuration (in the monitor menu under configuration/certificates/user certificate) a certificate from the Windows certificate store may be used as user certificate. If you select the "CSP user certificate store" from the listbox, the certificate from the CSP user certificate store is used for extended authentication. Please enter the certificates "Subject CN" and "Issuer CN" in the respective fields.

Since this function is only available after the user's logon to the windows system, it cannot be used for domain logon via VPN.

Messaging Center (SMS)

The messaging center (monitor menu under Connection / Messaging Center (SMS)) offers a comfortable way to send and receive text messages. This, for instance, offers comfortable authentication at hotspots by the means of one-time passwords.

The messaging center can be used independent of an internet or VPN connection. This means, in order to send or receive text messages, the messaging center may remain open in addition to an internet or VPN connection.

The Secure Enterprise Management Software starting with version 2.03 offers the possibility to lock the use of the messaging center by graying out the menu item.

Revised Wi-Fi GUI in regard to field strength measurement and tray icon

If "Wi-Fi" has been activated, the affiliated tray icon appears in the taskbar. This icon shows the current connection state, the field strength and the mode of encryption. Clicking on the tray icon, all available Wi-Fi networks are displayed. Selecting one of the Wi-Fi networks either starts connection set up or the Wi-Fi profile wizard. The Wi-Fi profile wizard facilitates connection set up to a new Wi-Fi network. Apart from that the encryption mode (WEP, WPA, WPA2) is now automatically detected.

Benefit

Wi-Fi handling has been facilitated for the user.

Status display for scanning Wi-Fi networks and connection set up (animated icon)

If "Wi-Fi" is activated, a periodical scan for Wi-Fi networks is run. During scanning the respective icon is animated. Connection set up to an access point is displayed with a blinking yellow ball next to the selected SSID of the Wi-Fi network. A green ball indicates the established connection to a Wi-Fi

access point. If several Wi-Fi access points use the same SSID, a small red triangle is displayed next to the SSID.

Benefit

Wi-Fi handling has been facilitated for the user.

Profile export

This feature exports the selected profile. Then it can be imported to another Entry Client. Certificates, however, have to be imported separately.

Benefit

The user can easily transfer a VPN profile to another computer.

Budget manager history for the previous twelve months

The budget manager history records and also displays the data volume of the previous twelve months.

Vodafone web sessions support

After setting up a VPN tunnel by clicking on "connect" the user can log on to Vodafone web sessions.

New option in the client's configuration wizard to create new profiles

The configuration wizard now directly allows for new profiles to be assigned to a profile filter group.

Rearranged display:

- New display for the NCP Secure Enterprise Client
- Connect/ Disconnect Switch – modern GUI
- World map depending on time zone;
Depending on the time zone configured on the PC the corresponding section of the world map is displayed. Maps exist for Europe, America and Asia / Australia.

Improved log handling

When highlighting a line in the monitor's log, the log stops scrolling which allows for better log viewing.

The client connection is faster

Improved behavior of the disconnected client with DHCP and manual Connection mode enabled

Enhancement of encryption and hash options.

Diffie-Hellmann-Group 14, SHA-256, SHA-384 and SHA-512

Other changes:

- "VPN IP Networks" renamed to "Split-Tunneling"
- Optimized display of scanned WiFi networks
- French and Polish language have been added to the setup routine
- Number of configurable remote VPN networks raised to 250
- IPsec Optimization: Improved compatibility
- Improved processing of application related rules within the client's personal firewall
- Improved handling of language selection in the client's GUI
- Troubleshooting within the Diffie-Hellman computation regarding Padding and Montgomery reduction

New features of version 9.1 relative to version 9.0

New features of version 9.1 relative to 9.04

Budget Manager (p)

The **Budget-Manager** serves to monitor the costs of all available connection types, focusing on UMTS, GPRS as well as WLAN connections. For this purpose, the administrators or users configure volume or time limits according to the basic provider rates. Should the user exceed his set limit, depending on the settings either a warning notice appears or further connection attempts are hindered. The Budget Manager also allows the restriction or disabling of roaming. Nasty surprises in the monthly provider invoice are avoided in this manner.

Extended Certificate Configuration (p)

A number of individual certificate settings may be saved as multi certificate configurations in the client configuration. Per profile, one certificate configuration can be chosen from the selection. The different certificates enable authentication against different VPN remote stations e.g. to VPN gateway 1 with soft certificate and to gateway 2 with a certificate saved to smartcard.

Profile Filter (p)

The configured profiles can be combined into groups, which can then be easily selected via the context menu of the client monitor. This can increase the clarity of existing

Client Info Center

Log and error messages were revised and their informative values were increased to optimize user help desk support. An overview with the following information is available:

- Client version (incl. build number)
- Current connection status (connected, broken, broken with error)
- Client service status
- Current certificate configuration (incl. validity)
- VPN user ID
- User for management server connection

New features of version 9.04 relative to 9.03

Importing PCF Data

Via the Entry Client monitor menu "Configuration / Import Profile", configuration data for the profile can be read in with the help of a wizard. These profile settings can be created from the prevailing destination system as differential data types. If individual configurations are not present in these profile settings (e.g. password), these are called by wizard upon import. The NCP Entry Client supports the following data types: *.ini, *.pcf, *.wgx and *.spd.

Software Update over LAN (p)

Software Update over LAN without VPN connection.

Roaming with IPSec Connections

If a new IP address is assigned to the client during a session with wireless LAN or LAN connection via DHCP, the client assumes the new IP address and sends an IKE notify report (NCP-specific) to the gateway in order to inform the address change. Meanwhile, the IPSec connection is not interrupted and need not be reestablished. Prerequisite: NCP Secure Server >= 7.02 Build 25.

WISPR for comfortable Login on T-Mobile Hostspots

The NCP Secure Entry Client 9.04 Build 60 supports the new logon technology via WISPr protocol (Wireless Internet Service Provider roaming). This ensures compatibility to T-Mobile hotspots in Germany, Austria, Netherlands, Czechia and Great Britain, and also in some Lufthansa lounges of international airports. The configuration can be made by entering the access data into a script of a WLAN profile.

Improved UMTS card handling

Store SIM PIN in the Configuration

The option "Store SIM PIN in Configuration" has been added in the dialog for entry of the SIM PIN for GPRS/UMTS cards. If this function is used, the formerly registered SIM PIN is employed for each destination system with the connection medium GPRS/UMTS, and need no longer be entered specially.

This function is not visible in the Entry Client default setting. It becomes visible and configurable for the user when the privilege is granted to him in the configuration locks under "GPRS/UMTS", i.e. "Allow user to save the SIM PIN in the configuration" has been activated.

[New features of version 9.03 relative to 9.01](#)

64-Bit operating system (p)

The new client supports Microsoft Windows XP for 64 bit.

License Key for Windows Operating Systems

To use the client software on Windows XP 64 bits and Vista 64 bits and Vista 32 bits a version 9.0 license key is required.

Driver Signature for Windows XP

The intermediate driver for the Windows operating systems XP 32 bits and XP 64 bits is now signed. The security detection therefore will no longer prompt the user about installing an unsigned driver. Problems with third party firewalls should no longer occur due to the adaptation of the signed intermediate driver.

2-factor authentication OTP Mobile

OTP Mobile by T-Systems and T-Mobile uses the existing mobile phone for 2-factor authentication. It calculates at the press of a button – completely without mobile radio connection – a one-time password, that the user enters in the login mask of the application.

Support for certificates with a key length of 4096 bit

Certificates with a key length of 4096 bit can be deployed on the server and client side for user authentication.

New features of version 9.01 relative to 9.0

64-Bit Operation System

The current version of the client software supports the 64-Bit operation system of Microsoft Windows Vista.

1. Windows Vista support

With version 9.0 of the NCP Secure Enterprise Client, in addition to the operating systems Windows 2000 and Windows XP, Windows Vista in the 32-bit und 64-bit variants is also supported.

NCP no longer supports the Windows operating systems, Windows NT, Windows 98, and Windows ME; this means that NCP assumes no warranty for full functionality of the Client software under these operating systems.

Note: The Client software, version 9.0, requires a license key 9.0 under Windows Vista. Utilization with an older license key (<9.0) is not possible.

2. New user interface (Monitor)

The Client interface has been visually adapted to the Windows Vista operating system. The functional flow of connection setup, connection disconnect, and authentication, which is indicated by icons, is clear and understandable in its design.

Comment texts (tooltips) explain the specific icons and facilitate troubleshooting if there is a malfunction. The status of the integrated Personal Firewall is indicated in the icon within the toolbar.

3. Firewall settings

The setting possibilities of the firewall, under "Firewall Settings" in the Monitor menu, have been extended relative to known networks. For "known networks" the headers "Manual" and "Automatic" have been introduced. The manual definition of a known network by the administrator and the automatic detection of a known network via Friendly Net Detection can be used concurrently and they can be configured via the "Manual" and "Automatic" tabs. Under the Options header you can specify that additional VPN tunnel set up is no longer possible if the Client is already in a known network. If the option "VPN connection not allowed in known network" is switched on then the button for connection set up (or the menu item) in the Client Monitor is deactivated. However an existing VPN connection that may have been established by a different application can be disconnected.

If the Client is already in a known network the logon options for domain logon can be hidden. To do this the function "Hide logon options in the known network" must be activated. The timeframe for automatic Friendly Net Detection can be entered independently of the timeout value. The value for the network search time must be at least 30 seconds. (The default is 60 seconds). (These settings can be pre-configured via the Management Console of the Secure Enterprise Management system as of v. 1.04 build 24.)

The basic modes of the firewall are displayed as quick-info for a tool tip on the system tray icon so that you can quickly tell whether the firewall (FW) or the Link Firewall (LFW) is active or inactive, and whether the Client is in a known network or an unknown network.

In addition on the tray icon and on the application icon an active firewall is indicated in red, with Friendly Net is indicated in green.

4. WLAN panel

The display of the WLAN panel can be configured in such a manner that it permanently shows current WLAN status, regardless of the transmission medium used. Thus it is possible for the teleworker to constantly check the field strength (and thus the status) of his WLAN connection, and to change the connection medium if necessary.

5. Automatic detection of the connected PC/SC smart card reader

If use of a certificate is configured on the Client for the PKI environment, then the Client automatically detects the connected PC/SC card reader. This simplifies creation of phonebooks with the Management Console of the Enterprise Management system.

In the central certificate configuration, it is no longer necessary to configure a user-specific smart card reader. The users can have different PC/SC readers on their teleworkstations, as needed.

Note: This feature can only be used in conjunction with smart cards that can be directly addressed without interface software. (e.g. TCOS, Netkey from Telesec, and TC Trust).

6. Extended configuration possibilities for the Client with the Management Console of the Secure Enterprise Management as of v. 1.04

- block that the user can no longer close the monitor.
- Parameter block extensions: License information can no longer be read by the user.

7. Endpoint policy - message box for the user

Automatic display of message texts in one message box. Message texts are specified centrally. For example: "The virus scanner has old signatures and will be automatically updated. Please restart your PC".

8. Disabling the ad-hoc mode for WLAN profiles

Ad-hoc queries are a flexible procedure in order to quickly access data on an external computer. In other words this mode is also supported standard in WLAN environments by Microsoft operating systems. For mobile teleworkstations such PC - PC connections should always be suppressed for technical security reasons. Within the WLAN profile the NCP Client can be set in such a manner that a PC - PC connection is not possible via WLAN.

9. Simplified entry of user ID and password dialogs

To further increase user-friendliness, entry of user IDs and passwords has been combined in one dialog, if user ID and password have not been stored in the configuration.

10. Integrated support of additional multifunction cards (Mobile Connect Cards)

If a multifunction card is inserted that is detected by the Client then the menu item "Multifunction Card" is shown in the "Connection" Monitor menu. The following multifunction cards* have been added to the list of already supported cards:

- Integrated card of the Lenovo notebook (Sierra chipset) - Vodaphone USB adapter for UMTS/GPRS.

The following functions are available under the "Multifunction card" menu item:

- Network search
- Activate UMTS or GPRS
- Enter or change SIM PIN

The functions "Network Search" and "Activate UMTS or GPRS" can also be triggered via the field for graphic display of signal strength. This field is always open when a profile has been selected with the connection type "UMTS/GPRS" from the profile settings. The PIN dialog for entering the SIM PIN is always displayed if the media type "UMTS/GPRS" has been configured in a profile and a multifunction card has been inserted that the Client detects.

*) See the compatibility list at: <http://www.ncp-e.com/en/support/compatibility/umts-3g-hardware.html>

11. Extended protection of the teleworkstation via UDP filter

In the Monitor menu firewall settings a UDP filter can be set that prevents UDP packets from being filtered out when the Client has started, independently of the Firewall. This prevents a UDP connection from the outside on the teleworkstation.