NCP Secure Enterprise Client
Release Notes

Minor release: **13.14 r29669**
Date: **March 2023**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 11, 64 bit (from version 21H2 up to and including version 22H2)
- Windows 10, 64 bit (from version 20H2 up to and including version 22H2, as well as Windows 10 Enterprise LTSC 2019 version 1809)

HotSpot login

For the correct function of the HotSpot login, at least version 101.0.1210.39 of the Microsoft WebView2 Runtime must be installed.

Prerequisites for the central management via Secure Enterprise Management (SEM)

To manage the client software centrally via SEM the following plugins are required:

- NCP Secure Enterprise Management: Version 6.10 or newer
- NCP Management Console: Version 6.10 or newer
- Client Configuration Plugin: Version 13.10 or newer
- License Plugin: Version 13.00 or newer
- Firewall Plug-in: Version 13.00 or newer
- Endpoint Policy Plug-in Version 6.20 or newer

The following features are no longer available as of this client version:

- SMS Center
- Connection medium: modem, xDSL, ext. dialer

Before updating to version 13, we recommend checking the client version already installed on the user computer in the case of a rollout via SEM. If the version number is version 11.14 or above, the update to version 13 can be carried out without further measures. If the client version is older, it is strongly recommended to first distribute the update client version 6.01 up to max. 7.01 via SEM. This will place it first in the software update list.
When updating from a version lower than 12.0, the notes in "New Directory Structure" must be observed.

New Directory Structure

For security reasons and compatibility with Windows, the directory structure of the NCP Secure Client has been changed as of version 12.0. The following directories that were previously in the installation directory under `Programs\NCP\SecureClient\` have been migrated to `ProgramData\NCP\SecureClient\`:
`arls, cacerts, certs, config, crls, CustomBrandingOption, data, hotspot, log, statistics`
These are configuration files, certificates or log files. Binaries or resources remain in `Programs\...`.
During the update process, the new directory structure is created automatically and the configuration is transferred accordingly. Configuration paths within the certificate configuration that contain the variable `%InstallDir%` are converted to paths with `%CertDir%`. `%CertDir%` refers to the path `C:\ProgramData\NCP\SecureClient\certs`.
Note: The configuration entry `%CertDir%\client1.p12` is equivalent to `client1.p12`.
Please note when using the NCP Secure Enterprise Management:
The NCP Secure Enterprise Clients can be upgraded to version 13.x as before. The local configuration is automatically converted during the update process. When using NCP Secure Enterprise Management to assign new configurations, the paths in the configurations or templates to be assigned must be modified before distribution. Likewise, for different client versions, a distinction must be made between configurations from version 12.x and older versions. The use of absolute paths is not recommended by NCP.

1. New Features and Enhancements

None.

2. Improvements / Problems Resolved

Troubleshooting: IKEv2 rekeying did not work with Juniper SRX gateways

Adjustment of PKCS#11 module configuration

The configuration of a PKCS#11 module has been adapted to increase the security in the NCP Secure Client. For this reason with this client version only PKCS#11 files can be loaded from the following locations: `WINDIR, PROGRAMFILES and PROGRAMFILES(x86).`
Alternatively, the following path for the PKCS#11 module can be configured in the registry with existing admin rights:
`"HKLM\\Software\NCP engineering GmbH\NCP Secure Client\\P11DllPath".`
In the client configuration, the PKCS#11 DLL including the complete path must always be specified.

Troubleshooting: VPN Bypass and mobile communication

When using a profile with configured connection medium "mobile network", a domain configured via VPN Bypass was not accessible. This problem has been fixed.

Troubleshooting: Split DNS with Cisco ASA Gateway

If split DNS was configured on the gateway side on a CISCO ASA hardware, only the first DNS name is used for split DNS. This problem has been fixed.

Troubleshooting: Stateful Boot Option

Provided that all of the following conditions are met,

- basically only communication through the VPN tunnel or within a Friendly Net is allowed
- Windows manages the connection media itself (the media change is not triggered by the NCP Secure Client)
- immediately after a Windows system start, mobile network is selected as the connection medium by the Windows system
- the stateful boot option is configured in the client's firewall settings

a connection to the Internet - without a VPN tunnel - could be established from the user's computer. This problem has been fixed.

Troubleshooting: Automatic media detection

In rare cases the "automatic media detection" configured in the NCP Secure Client incorrectly switched to WiFi although the device was still connected to LAN. This problem has been fixed.

Rework of SAML authentication

A vulnerability was fixed in the communication between the NCP Secure Client and the Authentication Provider that allowed an attacker to take over a user's session using a phishing attack. This problem has been fixed.

Note: SAML authentication is not supported during the Windows Pre-Login phase.

Adjustment of the IKEv2 Configuration Payload

The length of the IKEv2 Configuration Payload attribute type `INTERNAL_IP6_ADDRESS` has been changed from 16 bytes to 17 bytes. Accordingly, the prefix is now also transmitted in addition to the IPv6 address.

Support of RFC7383 (IKEv2 Message Fragmentation)

With RFC7383 support, compatibility with third-party gateways has been improved.

Troubleshooting: Endpoint Policy check gets stuck

Under certain circumstances, the Endpoint Policy check could fail to complete during VPN connection establishment. In this case, no data could be transported through the VPN tunnel. This problem has been fixed.

Troubleshooting: PIN icon turns green despite PIN not entered

If the user's computer was started with an inserted SmartCard, the status display for PIN entry was incorrectly displayed in green in the NCP Secure Client – corresponds to PIN entry already done. This problem has been fixed.

Improvement of the compatibility to the Juniper SRX within the rekeying phase

If rekeying was initialized by the client against a Juniper SRX, an error situation occurred. This problem has been fixed.

Audit log

Sending of the audit log to the central management has been completely disabled with this client version. Audit logs generated by the NCP Secure Client on the user's computer that are older than one day are also deleted.

Update to OpenSSL version 1.0.2zg

The OpenSSL version used in the NCP Secure Client has been upgraded to 1.0.2zg.

Americas: NCP engineering, Inc. • 19321 US Highway 19 N, Suite 401 • Clearwater, FL 33764 • Phone: +1 (650) 316-6273 • www.ncp-e.com
Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299

3. Known Issues

Application-based VPN bypass configuration

Configuring a DNS within the VPN Bypass configuration will invalidate an application-based rule contained within it.

Compatibility of the Update Client

The Update Client 8.0x included in the NCP Secure Client is not compatible with older versions of the NCP Secure Client and accordingly cannot be distributed for these versions via SEM update.

PIN menu entries

When using hardware certificates, the PIN menu entries “Enter/Reset/Change PIN” without function can be selected incorrectly.

Seamless roaming

Under certain circumstances, the VPN tunnel status remains at "Keep tunnel logical" when switching from WLAN to LAN and a functional connection via LAN is not established. This must be done by manually disconnecting and connecting.

Home Zone and IPv6

If the predefined Home Zone rule is active in the firewall settings of the VPN client, outgoing IPv6 packets to the local network are dropped in the defined Home Zone network.

Minor release: **13.13 r29638**
Date: **November 2022**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 11, 64 bit (up to and including version 22H2)
- Windows 10, 64 bit (up to and including version 22H2)

HotSpot login

For the correct function of the HotSpot login, at least version 101.0.1210.39 of the Microsoft WebView2 Runtime must be installed.

Prerequisites for the central management via Secure Enterprise Management (SEM)

To manage the client software centrally via SEM the following plugins are required:

- NCP Secure Enterprise Management: Version 5.30 or newer
- NCP Management Console: Version 5.30 or newer
- Client Configuration Plugin: Version 13.10 or newer
- License Plugin: Version 13.00 or newer
- Firewall Plug-in: Version 13.00 or newer
- Endpoint Policy Plug-in Version 6.20 or newer

The following features are no longer available as of this client version:

- SMS Center
- Connection medium: modem, xDSL, ext. dialer

Before updating to version 13, we recommend checking the client version already installed on the user computer in the case of a rollout via SEM. If the version number is version 11.14 or above, the update to version 13 can be carried out without further measures. If the client version is older, it is strongly recommended to first distribute the update client version 6.01 up to max. 7.01 via SEM. This will place it first in the software update list.
When updating from a version lower than 12.0, the notes in "New Directory Structure" must be observed.

New Directory Structure

For security reasons and compatibility with Windows, the directory structure of the NCP Secure Client has been changed as of version 12.0. The following directories that were previously in the installation directory under `Programs\NCP\SecureClient\` have been migrated to `ProgramData\NCP\SecureClient\`:
`arls, cacerts, certs, config, crls, CustomBrandingOption, data, hotspot, log, statistics`
These are configuration files, certificates or log files. Binaries or resources remain in `Programs\...`.
During the update process, the new directory structure is created automatically and the configuration is transferred accordingly. Configuration paths within the certificate configuration that contain the variable `%InstallDir%` are converted to paths with `%CertDir%`. `%CertDir%` refers to the path `C:\ProgramData\NCP\SecureClient\certs`.
Note: The configuration entry `%CertDir%\client1.p12` is equivalent to `client1.p12`.
Please note when using the NCP Secure Enterprise Management:
The NCP Secure Enterprise Clients can be upgraded to version 13.x as before. The local configuration is automatically converted during the update process. When using NCP Secure Enterprise Management to assign new configurations, the paths in the configurations or templates to be assigned must be modified before distribution. Likewise, for different client versions, a distinction must be made between configurations from version 12.x and older versions. The use of absolute paths is not recommended by NCP.

1. New Features and Enhancements

Extended support of the NCP Authentication Provider

In the context of user authentication via SAML protocol, the use of the NCP Authentication Provider is necessary. With this version of the NCP Secure Enterprise Client, the redirect/load balancing functionality of the NCP Authentication Provider is supported.

2. Improvements / Problems Resolved

Update Dialog

The Update Client included in the NCP Secure Enterprise Client is responsible for exchanging data with the central management. This includes sending the log files and the results of the endpoint policy audit as well as receiving any client software updates.
With the introduction of the audit log, the update dialog was displayed to the user at least once a day

because of the log transfer.
With the introduction of version 8.01 of the Update Client in this NCP Secure Enterprise Client, no update dialog is displayed to the user in the case of sent log files and the notification setting "only with available updates " in the update list. For the notification settings "always" and "never" the behavior of the update client has not changed.
The Update Client 8.01 is provided separately to the subsequent update of the NCP Secure Enterprise Client 13.04/13.10/13.11 by the NCP Secure Enterprise Management.

3. Known Issues

Application-based VPN bypass configuration

Configuring a DNS within the VPN Bypass configuration will invalidate an application-based rule contained within it.

Compatibility of the Update Client

The Update Client 8.0x included in the NCP Secure Client is not compatible with older versions of the NCP Secure Client and accordingly cannot be distributed for these versions via SEM update.

PIN menu entries

When using hardware certificates, the PIN menu entries “Enter/Reset/Change PIN” without function can be selected incorrectly.

Seamless roaming

Under certain circumstances, the VPN tunnel status remains at "Keep tunnel logical" when switching from WLAN to LAN and a functional connection via LAN is not established. This must be done by manually disconnecting and connecting.

Home Zone and IPv6

If the predefined Home Zone rule is active in the firewall settings of the VPN client, outgoing IPv6 packets to the local network are dropped in the defined Home Zone network.

Minor release: **13.11 r29631**
Date: **September 2022**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 11, 64 bit (up to and including version 22H2)
- Windows 10, 64 bit (up to and including version 22H2)

HotSpot login

For the correct function of the HotSpot login, at least version 101.0.1210.39 of the Microsoft WebView2 Runtime must be installed.

Prerequisites for the central management via Secure Enterprise Management (SEM)

To manage the client software centrally via SEM the following plugins are required:

- NCP Secure Enterprise Management: Version 5.30 or newer
- NCP Management Console: Version 5.30 or newer
- Client Configuration Plugin: Version 13.10 or newer
- License Plugin: Version 13.00 or newer
- Firewall Plug-in: Version 13.00 or newer
- Endpoint Policy Plug-in Version 6.20 or newer

The following features are no longer available as of this client version:

- SMS Center
- Connection medium: modem, xDSL, ext. dialer

Before updating to version 13, we recommend checking the client version already installed on the user computer in the case of a rollout via SEM. If the version number is version 11.14 or above, the update to version 13 can be carried out without further measures. If the client version is older, it is strongly recommended to first distribute the update client version 6.01 up to max. 7.01 via SEM. This will place it first in the software update list.
When updating from a version lower than 12.0, the notes in "New Directory Structure" must be observed.

New Directory Structure

For security reasons and compatibility with Windows, the directory structure of the NCP Secure Client has been changed as of version 12.0. The following directories that were previously in the installation directory under `Programs\NCP\SecureClient\` have been migrated to `ProgramData\NCP\SecureClient\`:
`arls, cacerts, certs, config, crls, CustomBrandingOption, data, hotspot, log, statistics`
These are configuration files, certificates or log files. Binaries or resources remain in `Programs\...`.
During the update process, the new directory structure is created automatically and the configuration is transferred accordingly. Configuration paths within the certificate configuration that contain the variable `%InstallDir%` are converted to paths with `%CertDir%`. `%CertDir%` refers to the path `C:\ProgramData\NCP\SecureClient\certs`.
Note: The configuration entry `%CertDir%\client1.p12` is equivalent to `client1.p12`.
Please note when using the NCP Secure Enterprise Management:
The NCP Secure Enterprise Clients can be upgraded to version 13.x as before. The local configuration is automatically converted during the update process. When using NCP Secure Enterprise Management to assign new configurations, the paths in the configurations or templates to be assigned must be modified before distribution. Likewise, for different client versions, a distinction must be made between configurations from version 12.x and older versions. The use of absolute paths is not recommended by NCP.

1. New Features and Enhancements

None.

2. Improvements / Problems Resolved

Improve compatibility with Juniper SRX gateways in case of ReKeying phase.

Support for RFC 8598

RFC 8598 defines how the VPN gateway passes the split DNS configuration to the VPN client. This RFC is supported as of this client version.

Program maintenance / Change program

If the VPN client is made to perform program maintenance via the classic control panel "Change program", a rollback of the installation is performed with the driver update. After the "Finish" of the action, the message "Serious error during installation" appears. This problem has been fixed.

Improved compatibility with third-party gateways regarding IP address assignment.

If the VPN client was assigned an IP address ending with `.255` during connection establishment, routing through the VPN tunnel was not possible. This problem has been fixed.

3. Known Issues

Application-based VPN bypass configuration

Configuring a DNS within the VPN Bypass configuration will invalidate an application-based rule contained within it.

Compatibility of the Update Client

The Update Client 8.0 included in the NCP Secure Client is not compatible with older versions of the NCP Secure Client and accordingly cannot be distributed for these versions via SEM update.

Display of the software update list

The software update list is displayed more often, although it is set in the Secure Enterprise Management Server that the user is informed "only when updates are available". This is due to the introduction of the audit log in the VPN client, which is transmitted to the central management at least once a day.

PIN menu entries

When using hardware certificates, the PIN menu entries “Enter/Reset/Change PIN” without function can be selected incorrectly.

Seamless roaming

Under certain circumstances, the VPN tunnel status remains at "Keep tunnel logical" when switching from WLAN to LAN and a functional connection via LAN is not established. This must be done by manually disconnecting and connecting.

Home Zone and IPv6

If the predefined Home Zone rule is active in the firewall settings of the VPN client, outgoing IPv6 packets to the local network are dropped in the defined Home Zone network.

Minor release: **13.10 r29617**
Date: **August 2022**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 11, 64 bit (up to and including version 22H2)
- Windows 10, 64 bit (up to and including version 22H2)

HotSpot login

For the correct function of the HotSpot login, at least version 101.0.1210.39 of the Microsoft WebView2 Runtime must be installed.

Prerequisites for the central management via Secure Enterprise Management (SEM)

To manage the client software centrally via SEM the following plugins are required:

- NCP Secure Enterprise Management: Version 5.30 or newer
- NCP Management Console: Version 5.30 or newer
- Client Configuration Plugin: Version 13.10 or newer
- License Plugin: Version 13.00 or newer
- Firewall Plug-in: Version 13.00 or newer
- Endpoint Policy Plug-in Version 6.20 or newer

The following features are no longer available as of this client version:

- SMS Center
- Connection medium: modem, xDSL, ext. dialer

Before updating to version 13, we recommend checking the client version already installed on the user computer in the case of a rollout via SEM. If the version number is version 11.14 or above, the update to version 13 can be carried out without further measures. If the client version is older, it is strongly recommended to first distribute the update client version 6.01 up to max. 7.01 via SEM. This will place it first in the software update list.
When updating from a version lower than 12.0, the notes in "New Directory Structure" must be observed.

New Directory Structure

For security reasons and compatibility with Windows, the directory structure of the NCP Secure Client has been changed as of version 12.0. The following directories that were previously in the installation directory under `Programs\NCP\SecureClient\` have been migrated to `ProgramData\NCP\SecureClient\`:
`arls, cacerts, certs, config, crls, CustomBrandingOption, data, hotspot, log, statistics`
These are configuration files, certificates or log files. Binaries or resources remain in `Programs\...`.
During the update process, the new directory structure is created automatically and the configuration is transferred accordingly. Configuration paths within the certificate configuration that contain the variable `%InstallDir%` are converted to paths with `%CertDir%`. `%CertDir%` refers to the path `C:\ProgramData\NCP\SecureClient\certs`.
Note: The configuration entry `%CertDir%\client1.p12` is equivalent to `client1.p12`.
Please note when using the NCP Secure Enterprise Management:
The NCP Secure Enterprise Clients can be upgraded to version 13.x as before. The local configuration is automatically converted during the update process. When using NCP Secure Enterprise Management to assign new configurations, the paths in the configurations or templates to be assigned must be modified before distribution. Likewise, for different client versions, a distinction must be made between configurations from version 12.x and older versions. The use of absolute paths is not recommended by NCP.

1. New Features and Enhancements

Preparation for the new user authentication via SAML protocol

The NCP solution will gradually introduce a new user authentication via SAML protocol. The login for this is done with the standard web browser available on the user's computer. Authentication takes place at an identity service such as Microsoft Azure AD or Okta. The Authentication Server, which is still under development, represents the interface to the NCP solution, NCP Secure Enterprise Management.

New option: "DNS domains to be resolved in the tunnel".

The split DNS functionality can be configured using the new option "DNS domains to be resolved in the tunnel". In the case of configured split tunneling, the DNS requests of the configured domains are sent into the VPN tunnel. All other DNS requests bypass the VPN tunnel.

RFC 7296 support

The VPN client now supports RFC 7296 for distributing split tunneling configurations from the VPN gateway.

New parameter "DNS_HOSTNAME" within Endpoint Policy check

In contrast to the "COMPUTERNAME" parameter, the "DNS_HOSTNAME" parameter also supports names longer than 15 characters as well as upper/lower case.

2. Improvements / Problems Resolved

Software update via mobile radio

The locking of software updates of the client via mobile radio did not work. This problem has been fixed.

New rights structure within `C:\ProgramData\NCP\`

A user had write permissions within the directory `C:\ProgramData\NCP\`. These were limited to a minimum. For example, a user can now no longer store CA certificates in the designated directory. Likewise, the directory and permissions structure has been rebuilt so that no application in the user and system context writes to the same directory. This problem has been fixed.

Improvements in server-side configured Split DNS

Automatic Windows logon

If the option "Automatic Windows logon with configured credentials" was selected within the logon options, the Windows logon did not work. Likewise, there was a problem in connection with 2-factor authentication via TOTP. This problem has been fixed.

Fix for Seamleass Roaming and IPv6 destination addresses

VPN username from cache

After updating a previous version, the cached VPN username was sometimes not displayed correctly in the login dialog. This problem has been fixed.

Wrong status display after profile change

After a profile change from a certificate-based profile with successful PIN entry to a profile with pre-shared key, the entered PIN was not deleted and the PIN icon was not removed from the client GUI. This issue has been fixed.

PKI error when switching profiles

When switching profiles from a certificate-based profile with *.p12 file to a profile with SmartCard reader, a PKI error was displayed. This problem has been fixed.

Update to zlib version 1.2.12

The zlib version used in the VPN client was raised to 1.2.12. This closed the zlib security vulnerability [CVE-2018-25032].

OpenSSL security patch

The vulnerabilities [CVE-2022-0778] and [CVE-2020-1971] have been fixed in OpenSSL.

Migration to TLS 1.2

TLS versions 1.0 and 1.1 are no longer supported with this client release.

Update to cURL library 7.84.0

The cURL version used in the VPN client has been upgraded to 7.84.0. This closed the cURL vulnerabilities [CVE-2022-27776], [CVE-2022-27775], [CVE-2022-27774], [CVE-2022-22576], [CVE-2022-32205], [CVE-2022-32206], [CVE-2022-32207], and [CVE-2022-32208].

Improved compatibility with third-party gateways in conjunction with 2-factor authentication / token entry.

Incorrect status display: smart card

Under certain circumstances, a profile with 2-factor authentication incorrectly displayed a smart card icon. When switching to a profile with a smart card, an error message was displayed stating that the smart card was not initialized correctly. This problem has been fixed.

Problem solved after changing DNS entries in VPN Bypass configuration.

Problem solved in rollout process with INITUser and certificate distribution

Problem solved within the Client API

Problem solved when calling HotSpot login

The HotSpot login was not called correctly if the autostart option "Icon in system tray" was selected. This problem has been fixed.

Troubleshooting an incorrectly displayed PIN request

When using the CSP user certificate store, a PIN was sometimes incorrectly prompted. This problem has been fixed. Likewise, the PIN query option in the case of the CSP user certificate store has been removed in the client plug-in.

`WINDOWSDISPLAYVERSION` added to the Endpoint Policy

The `WINDOWSDISPLAYVERSION` parameter has been implemented for the Endpoint Policy check to determine the correct Windows 10 version.

Support for Windows 11 in the Endpoint Policy check

Improved compatibility with third-party gateways when addressing via IPv6

PAP/CHAP error during connection setup

Under certain circumstances, the VPN client displays a PAP/CHAP error when establishing an IKEv2 connection. This can be resolved by the user by opening the VPN profile and confirming with "Ok". This problem has been fixed.

3. Known Issues

Application-based VPN bypass configuration

Configuring a DNS within the VPN Bypass configuration will invalidate an application-based rule contained within it.

Compatibility of the Update Client

The Update Client 8.0 included in the NCP Secure Client is not compatible with older versions of the NCP Secure Client and accordingly cannot be distributed for these versions via SEM update.

Display of the software update list

The software update list is displayed more often, although it is set in the Secure Enterprise Management Server that the user is informed "only when updates are available". This is due to the introduction of the audit log in the VPN client, which is transmitted to the central management at least once a day.

PIN menu entries

When using hardware certificates, the PIN menu entries “Enter/Reset/Change PIN” without function can be selected incorrectly.

Seamless roaming

Under certain circumstances, the VPN tunnel status remains at "Keep tunnel logical" when switching from WLAN to LAN and a functional connection via LAN is not established. This must be done by manually disconnecting and connecting.

Home Zone and IPv6

If the predefined Home Zone rule is active in the firewall settings of the VPN client, outgoing IPv6 packets to the local network are dropped in the defined Home Zone network.

Program maintenance / Change program

If the VPN client is made to perform program maintenance via the classic control panel "Change program", a rollback of the installation is performed with the driver update. After the "Finish" of the action, the message "Serious error during installation" appears. The VPN client is fully functional again after closing all dialogs.

Minor release: **13.05 r29388**
Date: **May 2022**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 11, 64 bit (up to and including version 21H2)
- Windows 10, 64 bit (up to and including version 21H2)

Prerequisites for the central management via Secure Enterprise Management (SEM)

To manage the client software centrally via SEM the following plugins are required:

- NCP Secure Enterprise Management: Version 5.30 or newer
- NCP Management Console: Version 5.30 or newer
- Client Configuration Plugin: Version 13.00 or newer
- License Plugin: Version 13.00 or newer
- Firewall Plug-in: Version 13.00 or newer

The following features are no longer available as of this client version:

- SMS Center
- Connection medium: modem, xDSL, ext. dialer

Before updating to version 13, we recommend checking the client version already installed on the user computer in the case of a rollout via SEM. If the version number is version 11.14 or above, the update to version 13 can be carried out without further measures. If the client version is older, it is strongly recommended to first distribute the update client version 6.01 up to max. 7.01 via SEM. This will place it first in the software update list.
When updating from a version lower than 12.0, the notes in "New Directory Structure" must be observed.

New Directory Structure

For security reasons and compatibility with Windows, the directory structure of the NCP Secure Client has been changed as of version 12.0. The following directories that were previously in the installation directory under `Programs\NCP\SecureClient\` have been migrated to `ProgramData\NCP\SecureClient\`:
`arls, cacerts, certs, config, crls, CustomBrandingOption, data, hotspot, log, statistics`
These are configuration files, certificates or log files. Binaries or resources remain in `Programs\...`.
During the update process, the new directory structure is created automatically and the configuration is transferred accordingly. Configuration paths within the certificate configuration that contain the variable `%InstallDir%` are converted to paths with `%CertDir%`. `%CertDir%` refers to the path `C:\ProgramData\NCP\SecureClient\certs`.
Note: The configuration entry `%CertDir%\client1.p12` is equivalent to `client1.p12`.
Please note when using the NCP Secure Enterprise Management:
The NCP Secure Enterprise Clients can be upgraded to version 13.x as before. The local configuration is automatically converted during the update process. When using NCP Secure Enterprise Management to assign new configurations, the paths in the configurations or templates to be assigned must be modified before distribution. Likewise, for different client versions, a distinction must be made between configurations from version 12.x and older versions. The use of absolute paths is not recommended by NCP.

1. New Features and Enhancements

None.

2. Improvements / Problems Resolved

The NCPRWSNT service stops responding

In rare cases, primarily on new hardware, sporadic crashes of the NCPRWSNT service occurred. This problem, which occurred on an "HP ZBook Firefly 14 G8 Mobile Workstation", has been fixed.

Smartcard via CSP: Problems with PIN entry

When using a SmartCard reader controlled via CSP, the PIN entry dialog was not automatically displayed when accessing the SmartCard. In this situation, the user had to call the PIN entry manually. This problem has been fixed.

Logon options: Problem with Windows automatic logon and TOTP.

Within the logon options, the client can be configured to pass the VPN user ID and password to the Windows logon. This did not previously work for the case of 2-factor authentication with the entry of an additional passcode. This problem has been fixed.

Update to OpenSSL version 1.0.2u-12

The OpenSSL version used in the NCP Secure Client has been upgraded to 1.0.2u-12. This closed the OpenSSL security vulnerability CVE-2022-0778.

After pulling and inserting a smart card, it is no longer recognized in the client

When using a smart card reader and controlling it via CSP – Microsoft Smart Card Key Storage Provider – the smart card was no longer recognized after repeated pulling and inserting. This problem has been fixed.

Wrong display of PIN icon

When using the Credential Provider (Windows Pre-Logon), the PIN status was set incorrectly when the "Enter PIN on every connection" option was enabled. This problem has been fixed.

3. Known Issues

PIN and SmartCard reader status display

If both VPN profiles with and without certificate configuration are present in the NCP Secure Client, the status of the PIN icon or SmartCard reader may be displayed incorrectly in the client GUI under certain circumstances. The use of a profile without certificate configuration may only be possible after restarting the PKI service.

Application-based VPN bypass configuration

Configuring a DNS within the VPN Bypass configuration will invalidate an application-based rule contained within it.

Compatibility of the Update Client

The Update Client 8.0 included in the NCP Secure Client is not compatible with older versions of the NCP Secure Client and accordingly cannot be distributed for these versions via SEM Update.

Option: "Automatically Open Connection Setup Dialog“

Under certain circumstances, the Logon option "Automatically Open Connection Dialog" does not work.

Major release: **13.04 r29374**
Date: **March 2022**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 11, 64 bit (up to and including version 21H2)
- Windows 10, 64 bit (up to and including version 21H2)

Prerequisites for the central management via Secure Enterprise Management (SEM)

To manage the client software centrally via SEM the following plugins are required:

- NCP Secure Enterprise Management: Version 5.30 or newer
- NCP Management Console: Version 5.30 or newer
- Client Configuration Plugin: Version 13.00 or newer
- License Plugin: Version 13.00 or newer
- Firewall Plug-in: Version 13.00 or newer

The following features are no longer available as of this client version:

- SMS Center
- Connection medium: modem, xDSL, ext. dialer

Before updating to version 13, we recommend checking the client version already installed on the user computer in the case of a rollout via SEM. If the version number is version 11.14 or above, the update to version 13 can be carried out without further measures. If the client version is older, it is strongly recommended to first distribute the update client version 6.01 up to max. 7.01 via SEM. This will place it first in the software update list.
When updating from a version lower than 12.0, the notes in "New Directory Structure" must be observed.

New Directory Structure

For security reasons and compatibility with Windows, the directory structure of the NCP Secure Client has been changed as of version 12.0. The following directories that were previously in the installation directory under `Programs\NCP\SecureClient\` have been migrated to `ProgramData\NCP\SecureClient\`:
`arls, cacerts, certs, config, crls, CustomBrandingOption, data, hotspot, log, statistics`
These are configuration files, certificates or log files. Binaries or resources remain in `Programs\...`.
During the update process, the new directory structure is created automatically and the configuration is transferred accordingly. Configuration paths within the certificate configuration that contain the variable `%InstallDir%` are converted to paths with `%CertDir%`. `%CertDir%` refers to the path `C:\ProgramData\NCP\SecureClient\certs`.
Note: The configuration entry `%CertDir%\client1.p12` is equivalent to `client1.p12`.
Please note when using the NCP Secure Enterprise Management:
The NCP Secure Enterprise Clients can be upgraded to version 13.x as before. The local configuration is automatically converted during the update process. When using NCP Secure Enterprise Management to assign new configurations, the paths in the configurations or templates to be assigned must be modified before distribution. Likewise, for different client versions, a distinction must be made between configurations from version 12.x and older versions. The use of absolute paths is not recommended by NCP.

1. New Features and Enhancements

Revised hotspot login

Starting with this version 13.0 of the NCP Secure Client, the Chrome-based Microsoft Edge web browser is invoked via WebView2 runtime and used exclusively for the purpose of logging into a hotspot. The prerequisite for this is the installed WebView2 runtime (from version 94.0.992.31 or newer) within the operating system. The WebView2 runtime can be downloaded here:
https://developer.microsoft.com/en-us/microsoft-edge/webview2/#download-section

Support for max. 250 split tunneling remote networks

For both IPv4 and IPv6, up to 250 split tunneling configurations can be communicated from the NCP Secure Enterprise VPN Server to the client via IKEConfigMode. The prerequisite for this is an NCP Secure Enterprise VPN Server version 13.0 or higher.

Support for WPA3 encryption

The Wi-Fi Manager integrated in the NCP Secure Client can now also manage Wi-Fis encrypted with WPA3.

Support of RFC 7296

RFC 7296 defines the forwarding of split tunneling remote networks by the VPN gateway to the VPN client. This RFC is supported as of this client version.

Enhanced of the VPN status in the Windows registry

Previously, the connection status of the NCP client could be found in the registry under "`Computer \ HKEY_LOCAL_MACHINE \ SOFTWARE \ WOW6432Node \ NCP engineering GmbH \ NCP RWS / GA \ 6.0`" for the `SecClCsi` parameter with the values

0 = not connected

and

1 = connected

read out. As of this version, the client saves additional states in the Windows registry in the following location:

`HKEY_LOCAL_MACHINE \ SOFTWARE \ NCP engineering GmbH \ NCP Secure Client`

or

`HKEY_LOCAL_MACHINE \ SOFTWARE \ WOW6432Node \ NCP engineering GmbH \ NCP Secure Client`

The associated parameter `ConnectState` can have the following values:

0 = connection is disconnected

1 = connection is being established

2 = connection has been successfully established

3 = Internet connection is interrupted, VPN connection is on hold

4 = connection established but only communication with the NCP management server possible (licensing)

Reading out Windows environment variables in the certificate configuration

In the "CSP user certificate store" certificate configuration, the client supports the entry of Windows environment variables, e.g. `%userdnsdomain%`, `%userdomain%` or `%computername%`. These are queried when reading the cnf configuration in the underlying operating system and their return values are statically adopted in the configuration. A combination with additional characters is possible, for example: "`%computername%.%userdnsdomain%`".

2. Improvements / Problems Resolved

Revised file handling of ncp.db

In rare cases, the `ncp.db` file became unusable during operation, causing the client to lose its license. This problem has been fixed.

„Network Location Awareness“ not available with NCP firewall active

If the client firewall is activated, the "Network Location Awareness" of the Windows operating system is not available. In the case of the exclusively desired Friendly Network Detection functionality, the "Network Location Awareness" of the Windows operating system can be used by configuring a client firewall rule "Allow all network traffic bidirectionally" and setting a registry key. For this purpose the parameter `RegDw "WscIntegration"=0` has to be configured in the registry within `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ncprwsnt`. The default value of this parameter is `1`.

Option "Disable Wi-Fi when LAN cable is connected": Problem with Hyper-V

When using Hyper-V functionality, the Wi-Fi adapter was incorrectly deactivated when the "Disable Wi-Fi when LAN cable is connected" option was set. This problem has been fixed.

Automatic login via credential provider

When using the logon option with configured user credentials, a locked Windows workstation could be unlocked by selecting the NCP credential provider. This problem has been fixed.

Troubleshooting for multiple certificates with the same issuer and subject in the Windows certificate store

If the Windows certificate store contained certificates with identical issuer and subject, the wrong expired certificate was sometimes used by the client and acknowledged with the message "unable to get issuer certificate". This problem has been fixed.

Support for NCP Secure VPN GovNet Box removed

Removed the internal firewall rules required to run the NCP Secure VPN GovNet Box.

Changed default value in FND options

The default value for the "Check for friendly networks periodically" option has been changed from 0 sec to 3600 sec.

Incomplete log files

Under certain circumstances, incorrect write accesses to the client log files occurred, so that log entries

were missing in the worst case. This problem has been fixed.

Revised installation routine

In rare cases, after the end of the installation process, before the computer restart, the network connection was completely disconnected. This problem has been fixed. Furthermore, the "Repair program" functionality within the MSI installation process has been removed.

Error after standby state in connection with IPv6 fixed

After the standby state of the PC there were connection problems with IPv6. This error has been fixed.

Newly imported certificates in Computer CSP were not taken over

In rare cases, connection errors occurred when using NCP Secure Client 12.20 when a new certificate was distributed by Entrust. This error has been fixed.

Problem during installation with `certmgr.exe`

During the installation of the NCP Secure Client, the `certmgr.exe` file created by Microsoft was used to install the NCP manufacturer certificate. This file was recognized as not signed. Starting from this version, the newer `certutil.exe` is used instead of `certmgr.exe`. This has fixed the problem.

Dynamic certificate selection

The certificate selection has been significantly improved. In addition, only valid certificates will be imported in the future.

Import of a `ncpphone.cnf` via `ncpclientcmd.exe` before user login

Starting with version 12.x of the NCP Secure Client, the CLI tools `rwscmd.exe` and `ncpclientcmd.exe` could not read in a cnf configuration before user login. This problem has been fixed.

Bugfix in ESP header for IPv6

Revised parameter locks in the client GUI

In the client GUI, measures have been taken to ensure that blocked buttons cannot be activated by certain tools and that blocked functions are made available as a result.

Fixed a problem when establishing a connection with VPN Path Finder via IPv6

Improvement of the FND compatibility with network switches

Optimization of the establishment of an IKEv2 connection with EAP

In certain situations, the establishment of the VPN tunnel with IKEv2 and EAP could take an unusually long time. This problem has been resolved.

Improvement of the VPN bypass compatibility with MS Teams

3. Known Issues

Compatibility of the Update Client

The Update Client 8.0 included in the NCP Secure Client is not compatible with older versions of the NCP Secure Client and accordingly cannot be distributed for these versions via SEM Update.

Option: "Automatically Open Connection Setup Dialog“

Under certain circumstances, the Logon option "Automatically Open Connection Dialog" does not work.

4. Getting Help for the NCP Secure Enterprise Client

To ensure that you always have the latest information about NCP’s products, always check the NCP website at:

https://www.ncp-e.com/en/service-resources/download-vpn-client/version-information/

For further information about the Enterprise Client, visit:

https://www.ncp-e.com/en/products/centrally-managed-vpn-solution/

For further assistance with the NCP Secure Enterprise Client (Win32/64), visit:

https://www.ncp-e.com/en/company/contact/

5. Features

Operating Systems	Microsoft Windows (64 bit): Windows 11, Windows 10 x86-64 platform
Security Features	The Enterprise Client supports all major IPsec standards in accordance with RFC
Personal Firewall Firewall Configuration*	Stateful Packet Inspection; IP-NAT (Network Address Translation); Friendly Net Detection (Firewall rules adapted automatically if the connected network is recognized based on its IP subnet address, the DHCP server's MAC address or an NCP FND Server*); Start FND dependent action; Secure hotspot logon; Home Zone; Differentiated filter rules relative to: protocols, ports, applications and addresses, LAN adapter protection, IPv4 and IPv6 support, Central administration*
VPN Bypass	The VPN Bypass function allows the administrator to define applications which can communicate over the Internet directly despite disabling split tunneling on the VPN connection. It is also possible to define which domains or target addresses can bypass the VPN tunnel.
Virtual Private Networking	IPsec (Layer 3 Tunneling), RFC-conformant; IPsec proposals can be determined through the IPsec gateway (IKEv1/IKEv2, IPsec Phase 2); Event log; communication only in the tunnel; MTU size fragmentation and reassembly, DPD, NAT-Traversal (NAT-T); IPsec tunnel mode
Encryption	Symmetric processes: AES 128, 192, 256 bits; Blowfish 128, 448 bits; Triple-DES 112, 168 bits; Dynamic processes for key exchange: RSA to 2048 bits; seamless rekeying (PFS); Hash algorithms: SHA-1, SHA-256, SHA384, SHA-512, MD5, DH group 1, 2, 5, 14-21, 25-30
FIPS Inside	The IPsec Client incorporates cryptographic algorithms conformant with the FIPS standard. The embedded cryptographic module incorporating these algorithms has been validated as conformant to FIPS 140-2 (certificate #1747). FIPS conformance will always be maintained when any of the following algorithms are used for establishment and encryption of the IPsec connection: ▪ DH 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

Authentication Processes	IKE (Aggressive Mode and Main Mode, Quick Mode); XAUTH for extended user authentication; IKEv2; IKE config. mode for dynamic assignment of a virtual address from the internal address pool (private IP); PFS; PAP, CHAP, MS CHAP V.2; IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): Extended authentication relative to switches and access points (Layer 2); EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): Extended authentication relative to switches and access points on the basis of certificates (Layer 2); Support of certificates in a PKI: Soft certificates, smart cards, and USB tokens; Multi Certificate Configurations; Pre-shared secrets, one-time passwords, and challenge response systems; RSA SecurID ready
Strong Authentication	X.509 v.3 Standard; biometric Authentication (Windows 8.1 or higher) PKCS#11 interface for encryption tokens (USB and smart cards); smart card operating systems: TCOS 1.2, 2.0 and 3.0 Signature Card Version 2.0 Release 1, Atos CardOS V5.3 QES, V1.0; Smart card reader interfaces: PC/SC, CT-API, Microsoft CSP; PKCS#12 interface for private keys in soft certificates; CSP for the use of user certificates in the windows certificate store CSP for the use of smart cards via vendor API PIN policy; administrative specification for PIN entry in any level of complexity; revocation: EPRL (End-entity Public-key Certificate Revocation List, formerly CRL), CARL (Certification Authority Revocation List, formerly ARL), OCSP
PKI Enrollment*	CMP* (Certificate Management Protocol)
Network Access Control	Endpoint Policy Enforcement**
Networking Features	LAN emulation: Ethernet adapter with NDIS interface, full Wi Fi (Wireless Local Area Network) and WWAN (Wireless Wide Area Network, Mobile Broadband) support
Network Protocol	IPv4 / IPv6 Dual Stack
Dialers	NCP Internet Connector or Microsoft RAS Dialer (for ISP dial-in via dial-in script)
Seamless Roaming**	If a communications medium error occurs, automatic switchover of VPN tunnel to another Internet communication medium (LAN/WWAN/mobile data connection) without altering IP address ensures that applications communicating over VPN tunnel are not disturbed and application session is not disconnected. (prerequisite: NCP (Virtual) Secure Enterprise VPN Server)

VPN Path Finder**	NCP Path Finder Technology: Fallback IPsec/ HTTPS (port 443) if port 500 respectively UDP encapsulation is not possible (prerequisite: NCP VPN Path Finder Technology on VPN gateway)
IP Address Allocation	DHCP (Dynamic Host Control Protocol), DNS: Dial-in to the central gateway with changing public IP addresses through IP address query via DNS server
Communication Media	Internet, LAN, Wi-Fi, GSM, GPRS, LTE, 5G, PSTN.
Line Management	DPD with configurable time interval; Short Hold Mode; Wi-Fi roaming (handover); Timeout (controlled by time and charges); Budget manager (administration of connection time and/or –volume for mobile data connection and Wi-Fi, in case of mobile data connection separated administration of roaming abroad) Connection Modes: automatic, manual, variable (reconnection dependent on how previous disconnect invoked)
APN from SIM Card	APN (Access Point Name) defines access point of a mobile data connection at a provider. If user changes provider, system automatically uses APN data from SIM card to configure Secure Client
Data Compression	IPCOMP (lzs), deflate (only for IKEv1)
Quality of Service	Prioritization of configured outgoing bandwidth in VPN tunnel.
Additional Features	Automatic media detection; UDP encapsulation, WISPr-support, IPsec-Roaming, Wi-Fi roaming, Split Tunneling
Point-to-Point Protocols	PPP over GSM, PPP over Ethernet; MLP, CCP, CHAP
Internet Society RFCs and Drafts	RFC 2401 –2409 (IPsec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IP security architecture, ESP, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation, IPCOMP; RFC 7427: IKEv2-Authentication (Padding-method)
Client Monitor Intuitive, Graphical User Interface	Multilingual (English, Spanish, French, German); Client Info Center; Configuration, Connection Management and Monitoring, Connection Statistics, Log-files, Internet availability test, Trace Tool for error diagnosis; Display of connection status; Integrated support of Mobile Connect Cards; Client Monitor can be tailored to include company name or support information; Password protected configuration management and profile management, configuration parameter lock

Update with SEM	To update the client software the SEM version 5.30 and the following plugins are required: • License Plugin: Version 13.00 • Client Configuration Plugin: Version 13.00 • Firewall Plug-in: Version 13.00 • Update Client: Version 8.00

*) If you wish to download NCP's FND server as an add-on, please click here:
https://www.ncp-e.com/en/service-resources/download-vpn-client/
**) Prerequisite: NCP (Virtual) Secure Enterprise VPN Server

More information on NCP Secure Enterprise Client is available on the Internet at:
https://www.ncp-e.com/en/products/centrally-managed-vpn-solution/

FIPS 140-2 Inside