NCP VS GovNet Connector
Release Notes

Service Release: **2.20 r28866**
Date: **November 2022**

Prerequisites

Microsoft Operating Systems:
The following Microsoft Windows operating systems are supported with this release:

- Windows 10 (64 Bit)
  (from version 1607 up to and including version 22H2 on x86-64 processor architecture)
- Windows 11 (64 Bit) up to version 22H2 on x86-64 processor architecture

HotSpot login
To use the HotSpot login, at least version 101.0.1210.39 of the Microsoft WebView2 runtime must be installed.

For the use of the NCP VS GovNet Connector within the scope of a BSI approval for the processing and transmission of information classified as VS – NUR FÜR DEN DIENSTGEBRAUCH, the corresponding requirements for the underlying operating system and the configuration of the NCP VS GovNet Connector apply.

Prerequisite for operation with NCP Secure Enterprise Management (SEM)

To centrally manage this client version, the following components are required:

- NCP Secure Enterprise Management: Version 6.10 or higher
- NCP Management Console: Version 6.10 or higher
- VS GovNet Connector Configuration Plug-in: Version 2.20 or higher
- License Plug-in: Version 12.30 or higher
- Firewall Plug-in: Version 12.30 or higher
- PKI Enrollment Plug-in: Version 4.05 or higher
- Endpoint Policy Plug-in: Version 4.00 or higher

The following features are no longer available as of Connector version 2.20:

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

Important note for updating from a VS GovNet Connector 2.1x or older:

For VS GovNet Connector 2.20, a new signing certificate is used to sign the VS GovNet Connector binaries. For this reason, before updating the software from version 2.1x or older to 2.20 or later, the following must be done in the order given:

1. update the VS GovNet Connector SEM plug-in to version 2.20 or higher.
2. recreate all required VS GovNet Connector configurations
3. distribute the new VS GovNet Connector configurations
4. update the software of the VS GovNet Connector

1. New Features and Enhancements

Use of SmartCard readers without integrated PIN pad.

With this version 2.20 of the VS GovNet Connector, the BSI approval has been extended to the use of SmartCard readers without an integrated PIN pad. Accordingly, this also applies to smart card readers integrated in the laptop.

Support for WPA3 encryption

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

2. Improvements / Problems Resolved

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

The directory and rights structure has been rebuilt so that no application in the user and system context writes to the same directory.

Misrepresentation in the firewall configuration

If the GUI of the Connector was started with administrator rights and the parameter lock was removed, there was a misrepresentation within the firewall configuration. This problem has been fixed.

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.

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].

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

Detection of smart card status.

When accessing the smart card reader via CSP and a selected CSP provider, the detection of a pulled or inserted smart card could fail. This issue has been fixed.

Hotspot login pages not visible

If the VS GovNet Connector GUI was started with the "Icon in system tray" setting, the HotSpot web page was not displayed. This problem has been fixed.

OpenSSL security patch

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

Software update

In rare cases, a termination occurred during the software update. This problem has been fixed.

Operating system display in Client Info Center

The Client Info Center incorrectly displayed Windows 10 when a Windows 11 operating system was present. This issue has been fixed.

Update dialog

With this version of the VS GovNet Connector, in case of sent log files and the notification setting "only with available updates " in the update list, no update dialog is displayed at the user. For the notification settings "always" and "never" in the software update list, the behavior has not changed.

Firewall: In the FND configuration for the VS GovNet Connector, the parameter "Check for friendly networks periodically" has been added

Firewall option "Continue to use firewall when client is stopped" as default value

This adjustment causes the client computer to be protected by the VS GovNet Connector firewall after its installation (without configuration) and the subsequent first reboot of the computer.

Update to OpenSSL version 1.0.2zf

The OpenSSL version used in the VS GovNet Connector has been raised to 1.0.2zf.

3. Known Issues

VPN connections with PSK

No user-specific settings can be made in the central management of the VS GovNet Connector. Therefore, the creation and use of an individual configuration with PSK is not possible.

VPN connections without certificate configuration

VPN connections without certificate configuration, such as IKEv2 with EAP authentication, cannot be executed by the VS GovNet Connector.

After a configuration update, the VPN connection is immediately disconnected

After the VS GovNet Connector has received a configuration update from NCP Secure Enterprise Management, the VPN connection was terminated. However, the update package or the new configuration is not loaded.

Proxy for Path Finder is not queried

In the configuration of the VS GovNet Connector, a proxy can be configured for the use of VPN Path Finder. In this version of VS GovNet Connector, this configuration is not implemented.

Error message when licensing the VS GovNet Connector

If the VS GovNet Connector receives its license key from the central management, the following error message appears three times in the connector log:

```
ERROR - MONITOR: NcpClCfgLicenseWriteParam failed -> ret= 0
```

These error messages can be ignored and have no influence on the functionality of the VS GovNet Connector or its licensing.

No differentiation between client and VS GovNet Connector plug-in in an administrator group.

In an administrator group, no distinction can be made between the plug-ins for the NCP Secure Enterprise Client and the VS GovNet Connector. Configured permissions apply to both "Client" and "Connector" in this case.

If the NCP Secure Enterprise Client and the VS GovNet Connector are used, it is recommended to create separate administrators in different administrator groups for the configuration of the respective plug-ins.

Service Release: **2.11 r28781**
Date: **February 2022**

Prerequisites

Microsoft Operating Systems:
The following Microsoft Windows operating systems are supported with this release.

- Windows 10 (64 Bit)
  (from version 1607 up to and including version 21H1 on x86-64 processor architecture)
- Windows 11 (64 Bit) up to version 21H2 on x86-64 processor architecture

For the use of the NCP VS GovNet Connector within the context of a BSI recommended use for the processing and transmission of information classified as VS - FOR OFFICIAL USE ONLY, the corresponding requirements for the underlying operating system and the configuration of the NCP VS GovNet Connector apply.

Prerequisite for operation with NCP Secure Enterprise Management (SEM)

To centrally manage this client version, the following components are required:

- NCP Secure Enterprise Management: Version 6.00 or higher
- NCP Management Console: Version 6.00 or higher
- VS GovNet Connector Configuration Plug-in: Version 2.10 or higher
- License Plug-in: Version 12.30 or higher
- Firewall Plug-in: Version 12.30 or higher
- PKI Enrollment Plug-in: Version 4.05 or higher
- Endpoint Policy Plug-in: Version 4.00 or higher

1. New Features and Enhancements

None.

2. Improvements / Problems Resolved

Incorrectly set proxy settings

When exiting the client GUI, the proxy settings of the operating system were set incorrectly, causing interference when sending and receiving application data. This problem has been fixed.

Firewall delayed to take effect after reboot

In certain cases, the firewall was not effective after a reboot during FND detection. This problem has been fixed.

3. Known Issues

Problem with configuration download and used NCP Secure Enterprise Management 6.0

When using version 6.0 of the NCP Secure Enterprise Management Server, the configuration download to the VS GovNet Connector is not possible with a certain setting in the VS GovNet Connector plug-in:
If the VS GovNet Connector version selection is configured to "2.10" in the VS GovNet Connector template under “Info / Profile settings”, no configuration download will occur. The configuration download only takes place by changing the VS GovNet Connector version to "always".

Error when using card readers

When updating to a higher version, in rare cases an error may occur with CSP card readers if the user is not logged in as admin on the PC.

VPN connections with PSK

No user-specific settings can be made in the central management of the VS GovNet Connector. Therefore, the creation and use of an individual configuration with PSK is not possible.

VPN connections without certificate configuration

VPN connections without certificate configuration, such as IKEv2 with EAP authentication, cannot be executed by the VS GovNet Connector.

Installation on Windows 10 (32 bit) or older Windows systems

The VS GovNet Connector can be installed on Windows 8 (64 bit) or Windows 10 (32 bit), but the correct function is blocked by the integration service. This behavior is correct because platforms prior to Windows 10 or in 32 bit architecture are not supported.

Subsequent installation of NCP Secure GovNet Box Suite delivers failures

The NCP Secure GovNet Box Suite and the VS GovNet Connector cannot be functionally installed on the same hardware at the same time. However, the subsequent installation of the NCP Secure GovNet Box Suite on a device with VS GovNet Connector already installed on it will not be blocked and will result in an error situation.

After a configuration update, the VPN connection is immediately disconnected

After the VS GovNet Connector has received a configuration update from NCP Secure Enterprise Management, the VPN connection was terminated. However, the update package or the new configuration is not loaded.

Proxy for Path Finder is not queried

In the configuration of the VS GovNet Connector, a proxy can be configured for the use of VPN Path Finder. In this version of VS GovNet Connector, this configuration is not implemented.

Service Release: **2.10 r28778**
Date: **October 2021**

Prerequisites

Microsoft Operating Systems:
The following Microsoft Windows operating systems are supported with this release.

- Windows 10 (64 Bit)
  (from version 1607 up to and including version 21H1 on x86-64 processor architecture)
- Windows 11 (64 Bit) up to version 21H2 on x86-64 processor architecture

For the use of the NCP VS GovNet Connector within the context of a BSI recommended use for the processing and transmission of information classified as VS - FOR OFFICIAL USE ONLY, the corresponding requirements for the underlying operating system and the configuration of the NCP VS GovNet Connector apply.

Prerequisite for operation with NCP Secure Enterprise Management (SEM)

To centrally manage this client version, the following components are required:

- NCP Secure Enterprise Management: Version 6.00 or higher
- NCP Management Console: Version 6.00 or higher
- VS GovNet Connector Configuration Plug-in: Version 2.10 or higher
- License Plug-in: Version 12.30 or higher
- Firewall Plug-in: Version 12.30 or higher
- PKI Enrollment Plug-in: Version 4.05 or higher
- Endpoint Policy Plug-in: Version 4.00 or higher

1. New Features and Enhancements

Revised hotspot login

From this version 2.10 of the VS GovNet Connector on, hotspot logon can be used within the approved operation specified by the "SECURITY OPERATING PROCEDURES AND OPERATIONAL COMSEC DOCTRINE" document. For this purpose, the Chrome-based Microsoft Edge web browser is invoked as the web browser through WebView2 runtime and used exclusively for the purpose of hotspot logon. 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

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

Friendly Net Detection

From this version 2.10 of the VS GovNet Connector, Friendly Net Detection can be used within the permitted operation specified by the deployment and operating conditions. The prerequisite for this is the use of the NCP Friendly Net Detection Server from version 4.0.

2. Improvements / Problems Resolved

Firewall option "Permit communication via GovNet Box" removed

In the VS GovNet Connector plug-in, the firewall option "Permit communication via GovNet Box" has been removed starting with version 2.10 of the VS GovNet Connector.

Uninstall routine modified

Up to the previous version 2.01 of the VS GovNet Connector, the `import.vscfg` file remained in the installation directory after uninstallation. This problem has been fixed.

Error with set option "profile filter groups" in VS GovNet Connector plug-in

With the "Profile filter groups" option set in the VS GovNet Connector plug-in, the created profile groups could not be selected correctly in the VS GovNet Connector. This problem has been fixed.

Error in `ncpclientcmd.exe`

If the client was shut down via `ncpclientcmd.exe/stop` and should be restarted afterwards, the start command had to be executed twice in a row for the client to work properly again. This problem has been fixed.

Troubleshooting for software update via NCP Management Server

When updating software via NCP Management Server, the old client version was still displayed in the management after the update process. Likewise, the number of downloaded update packages was not raised. This problem has been fixed.

3. Known Issues

Problem with configuration download and used NCP Secure Enterprise Management 6.0

When using version 6.0 of the NCP Secure Enterprise Management Server, the configuration download to the VS GovNet Connector is not possible with a certain setting in the VS GovNet Connector plug-in:
If the VS GovNet Connector version selection is configured to "2.10" in the VS GovNet Connector template under “Info / Profile settings”, no configuration download will occur. The configuration download only takes place by changing the VS GovNet Connector version to "always".

Error when using card readers

When updating to a higher version, in rare cases an error may occur with CSP card readers if the user is not logged in as admin on the PC.

VPN connections with PSK

No user-specific settings can be made in the central management of the VS GovNet Connector. Therefore, the creation and use of an individual configuration with PSK is not possible.

VPN connections without certificate configuration

VPN connections without certificate configuration, such as IKEv2 with EAP authentication, cannot be executed by the VS GovNet Connector.

Installation on Windows 10 (32 bit) or older Windows systems

The VS GovNet Connector can be installed on Windows 8 (64 bit) or Windows 10 (32 bit), but the correct function is blocked by the integration service. This behavior is correct because platforms prior to Windows 10 or in 32 bit architecture are not supported.

Subsequent installation of NCP Secure GovNet Box Suite delivers failures

The NCP Secure GovNet Box Suite and the VS GovNet Connector cannot be functionally installed on the same hardware at the same time. However, the subsequent installation of the NCP Secure GovNet Box Suite on a device with VS GovNet Connector already installed on it will not be blocked and will result in an error situation.

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

After a configuration update, the VPN connection is immediately disconnected

After the VS GovNet Connector has received a configuration update from NCP Secure Enterprise Management, the VPN connection was terminated. However, the update package or the new configuration is not loaded.

Proxy for Path Finder is not queried

In the configuration of the VS GovNet Connector, a proxy can be configured for the use of VPN Path Finder. In this version of VS GovNet Connector, this configuration is not implemented.

Service Release: **2.01 r28544**
Date: **August 2021**

Prerequisites

Microsoft Operating Systems:
The following Microsoft Windows operating systems are supported with this release.

- Windows 10 (64 Bit)
  (from version 1607 up to and including version 20H2 on x86-64 processor architecture)

For the use of the NCP VS GovNet Connector within the context of a BSI recommended use for the processing and transmission of information classified as VS - FOR OFFICIAL USE ONLY, the corresponding requirements for the underlying operating system and the configuration of the NCP VS GovNet Connector apply.

Prerequisite for operation with NCP Secure Enterprise Management (SEM)

To centrally manage this client version, the following central components are required:

- NCP Secure Enterprise Management: Version 6.00 or higher
- NCP Management Console: Version 6.00 or higher
- VS GovNet Connector Configuration Plug-in: Version 2.00 or higher
- License Plug-in: Version 12.30 or higher
- Firewall Plug-in: Version 12.11 or higher
- PKI Enrollment Plug-in: Version 4.05 or higher
- Endpoint Policy Plug-in: Version 4.00 or higher

1. New Features and Enhancements

Customization of the Software Update Package

From this version on, at least version 2.00 of the VS GovNet Connector is required for future updates via the NCP Management, as this requires an existing integrity service. An update of a version 1.x is therefore no longer possible.

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • 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

2. Improvements / Problems Resolved

Help in English language

In the previous version of the VS GovNet Connector the English help was not available. This has now been added.

Remove of FIPS in program options

If the installation routine was started for an already installed VS GovNet Connector, it incorrectly provided the option "FIPS Mode" under "Change program". This error has been fixed.

Problem with the connection after configuration download

When using a SmartCard for user authentication, after a configuration update by the central management it could occur that the wrong user ID was used to establish the connection and therefore no connection was established. This error has been fixed.

The default profile is displayed incorrect in the VS GovNet Connector

If the option "Default profile after each system restart" was set in the configuration, the display of the profiles in the VS GovNet Connector was inverted, i.e., all other VPN profiles were displayed as the default profile, but the profile configured for this purpose was not. When the computer was restarted, the correct default profile for the VS GovNet Connector was selected. This was therefore exclusively a display error. This error has been fixed.

Option for "Delete manually added WLAN profiles" was not implemented

If the option "Delete manually added WLAN profiles" was selected in the central management, it was not executed after a configuration update of the VS GovNet Connector. This error has been fixed.

Integrity service was not shut down during update

When updating to a higher version, an error occurred with `ncpclientcmd.exe/stop` when uninstalling the previous version, which prevented the integrity service from terminating. This error has been fixed.

Error after Windows function update

By installing a function update of Windows, in a few cases the NCP VS GovNet Connector could no longer be started, and a corresponding error message appeared. This error has been fixed.

Error with "Minimize after connection" setting

If the NCP VS GovNet Connector is installed and the selection "Minimize after connection" is chosen, the monitor does not minimize after the first startup. However, minimizing works in the following startups. This error has been fixed.

Window with ncpintegritycheckcli.exe is displayed for a very long time

After downloading the software update package from NCP SEM, in some cases a black program window was displayed for a very long time. This window overlapped other applications. This error has been fixed.

Improved FND compatibility with network switches

The libcurl library was raised to version 7.77.0

Crash of the ncprwsnt service

In rare cases, the ncprwsnt service crashed. This problem has been fixed.

GUI does not start after restarting the connector via CLI

If the VS GovNet Connector was stopped using CLI input `ncpclientcmdstop` and then restarted with `ncpclientcmd/start`, the GUI of the VS GovNet Connector did not start anymore. This problem has been fixed.

3. Known Issues

Error when using card readers

When updating to a higher version, in rare cases an error may occur with CSP card readers if the user is not logged in as admin on the PC.

VPN connections with PSK

No user-specific settings can be made in the central management of the VS GovNet Connector. Therefore, the creation and use of an individual configuration with PSK is not possible.

VPN connections without certificate configuration

VPN connections without certificate configuration, such as IKEv2 with EAP authentication, cannot be executed by the VS GovNet Connector.

Installation on Windows 10 (32 bit) or older Windows systems

The VS GovNet Connector can be installed on Windows 8 (64 bit) or Windows 10 (32 bit), but the correct function is blocked by the integration service. This behavior is correct because platforms prior to Windows 10 or in 32 bit architecture are not supported.

Subsequent installation of NCP Secure GovNet Box Suite delivers failures

The NCP Secure GovNet Box Suite and the VS GovNet Connector cannot be functionally installed on the same hardware at the same time. However, the subsequent installation of the NCP Secure GovNet Box Suite on a device with VS GovNet Connector already installed on it will not be blocked and will result in an error situation.

Software package download is not displayed in NCP Secure Enterprise Management

If an update of the VS GovNet Connector is distributed via NCP Secure Enterprise Management, the distributed update packages are not displayed correctly.

After a configuration update, the VPN connection is immediately disconnected

After the VS GovNet Connector has received a configuration update from NCP Secure Enterprise Management, the VPN connection was terminated. However, the update package or the new configuration is not loaded.

VPN profiles of a group cannot be opened

If the "Profile Filter Groups" option is activated on the central management and profiles have been created in a group, these profiles cannot be selected on the VS GovNet Connector.

Proxy for Path Finder is not queried

In the configuration of the VS GovNet Connector, a proxy can be configured for the use of VPN Path Finder. In this version of VS GovNet Connector, this configuration is not implemented.

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • 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

Initiales Release: **2.00 r28513**
Datum: **April 2021**

Prerequisites

Microsoft Operating Systems:
The following Microsoft Windows operating systems are supported with this release.

- Windows 10 (64 Bit)
  (from version 1607 up to and including version 20H2 on x86-64 processor architecture)

For the use of the NCP VS GovNet Connector within the context of a BSI recommended use for the processing and transmission of information classified as VS - FOR OFFICIAL USE ONLY, the corresponding requirements for the underlying operating system and the configuration of the NCP VS GovNet Connector apply.

Prerequisite for operation with NCP Secure Enterprise Management (SEM)

To centrally manage this client version, the following central components are required:

- NCP Secure Enterprise Management: Version 6.00 or higher
- NCP Management Console: Version 6.00 or higher
- VS GovNet Connector Configuration Plug-in: Version 2.00 or higher
- License Plug-in: Version 12.30 or higher
- Firewall Plug-in: Version 12.11 or higher
- PKI Enrollment Plug-in: Version 4.05 or higher
- Endpoint Policy Plug-in: Version 4.00 or higher

1. New Features and Enhancements

Self-Check by new integrity service

The integrity service included in the VS GovNet Connector performs continuous monitoring of correct functionality in the operating system. Any compromise of the VS GovNet Connector results in the transfer of the end device to a secure state, which prevents further communication of any kind. Furthermore, the integrity service is used to perform a secure remote update process of the VS GovNet Connector by the central management at any time.

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • 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

Audit-Log

The new audit log summarizes all security-relevant events of the VS GovNet Connector. It is periodically transmitted to the central management for evaluation.

VS GovNet Connector Plug-in

The VS GovNet Connector requires the VS GovNet Connector plug-in for configuration in central management. When creating a new template, the preset parameters correspond to the settings in the SecOPs document for BSI-approved operation. Each generated configuration contains a continuous epoch counter which is derived from the current UNIX timestamp. In addition, the configuration generated for the VS GovNet Connector is signed to protect against tampering and is verified by the VS GovNet Connector upon receipt.
Local configuration of the VS GovNet Connector is not possible. The configuration cannot be viewed by the user.

Tool for resetting the PC from the "safe error" state

The CLI tool `integrityStateReset.exe` is part of the VS GovNet Connector installation. It is needed to reset the workstation from the "safe error state". This state is invoked as soon as the integrity service detects a problem. The mentioned CLI tool can only be accessed by an administrator with appropriate rights.

2. Improvements / Problems Resolved

None.

3. Known Issues

VPN connections with PSK

No user-specific settings can be made in the central management of the VS GovNet Connector. It is therefore not possible to create and use an individual configuration with PSK.

VPN connections without certificate configuration

VPN connections without certificate configuration, such as IKEv2 with EAP authentication, cannot be executed by the VS GovNet Connector.

Installation on Windows 10 (32 bit) or older Windows systems

The VS GovNet Connector can be installed on Windows 8 (64 bit) or Windows 10 (32 bit), but the correct function is blocked by the integration service. This behavior is correct because operating systems prior to Windows 10 or in 32 bit architecture are not supported.

Subsequent installation of NCP Secure GovNet Box Suite delivers error situation

Die NCP Secure GovNet Box Suite and the VS GovNet Connector cannot be functionally installed on the same hardware at the same

time. However, the subsequent installation of NCP Secure GovNet Box Suite on a device with VS GovNet Connector already installed on it is not prevented and leads to an error.

Software package download is not displayed in NCP Secure Enterprise Management

If an update of the VS GovNet Connector is distributed via NCP Secure Enterprise Management, the distributed update packages are not displayed correctly.

After a configuration update, the VPN connection is immediately disconnected

After the VS GovNet Connector has received a configuration update from NCP Secure Enterprise Management, the VPN connection is terminated. However, the update package or the new configuration is not loaded.

VPN group profiles cannot be opened

If the "Profile Filter Groups" option is activated on the central management and profiles have been created in a group, these profiles cannot be selected on the VS GovNet Connector.

Proxy for Path Finder is not queried

In the configuration of the VS GovNet Connector, a proxy can be configured for the use of VPN Path Finder. In this version of VS GovNet Connector, this configuration is not considered.

Incorrect display in VS GovNet Connector for default profile

If the option "Default profile after each system restart" was set in the configuration, the display of the profiles in the VS GovNet Connector is inverted. All the other VPN profiles are displayed as the default profile, but the profile configured for this is not. When the computer is restarted, the correct default profile for the VS GovNet Connector is selected. This is only a display error.

Option for "Delete manually added WLAN profiles" is not implemented

If the option "Delete manually added WLAN profiles" is selected in the central management, it will not be executed after the VS GovNet Connector update.

English help in VS GovNet Connector is not available

4. Notes about the NCP VS GovNet Connector

For more information on the latest development status of NCP products, please visit the website:
https://www.ncp-e.com/en/service-resources/download-vpn-client/version-information/

For further support with questions about NCP VS GovNet Connector, please use the mail addresses on the following page:
https://www.ncp-e.com/en/company/contact/

5. Open source software components in use

The Software uses open source software components listed in the attached file *OpenSourceLicenseTerms-ncpgovnet.pdf* These open source software components are exclusively subject to the open source software license terms specified in the file *OpenSourceLicenseTerms-ncpgovnet.pdf*.

6. Features

Operating Systems [1]	Microsoft Windows 10 (64 bit) version 1607 or newer on x86-64 processor architecture Microsoft Windows 11 (64 Bit) on x86-64 processor architecture
Security Features	The VS GovNet Connector supports all IPsec standards in accordance with RFC
Personal Firewall Firewall Configuration	Stateful Packet Inspection; IP-NAT (Network Address Translation); differentiated filtering rules regarding: protocols, ports, applications and addresses, LAN adapter protection; IPv4 and IPv6 support; central administration; Friendly Net Detection (Automatic firewall termination rules when the connected network is detected based on an NCP FND server [4]); Secure Hotspot Login; Home Zone [2];
VPN Bypass [2]	The VPN bypass function allows you to specify applications that are allowed to communicate directly to the Internet outside the VPN configuration, despite split tunneling being deactivated. Alternatively, it is possible to specify domains or destination addresses to which data communication should bypass the VPN tunnel.
Virtual Private Networking [3]	IPsec (Layer 3 tunneling), RFC compliant; IKEv1/IKEv2; Event log; communication in tunnel only; MTU size fragmentation and reassembly; DPD; NAT Traversal (NAT-T); IPsec Tunnel Mode
Encryption [3]	Symmetric methods: AES 128, 192, 256 bits; Blowfish 128, 448 bits; Triple-DES 112, 168 bits; Dynamic key exchange methods: RSA up to 8192 bits; Seamless Rekeying (PFS); Hash algorithms: SHA-1, SHA-256, SHA-384, SHA-512, MD5, DH group 1, 2, 5, 14-21, 25-30.
Authentication Processes[3]	IKEv1 (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 to switches and access points (Layer 2); EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): extended authentication to switches and access points based on certificates (Layer 2); Support of certificates in a PKI: Soft certificates, smart cards, USB tokens and certificates with ECC technology; Multi Certificate Configurations; Pre-shared secrets, one-time passwords, and challenge response systems; RSA SecurID ready.
Strong Authentication[3]	X.509 v.3 Standard; biometric Authentication (Windows 8.1 or higher)

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • 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

	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 [2]	CMP (Certificate Management Protocol)
Network Access Control [5]	Endpoint Policy: Verification of virus scanner validity, existing hotfixes/service packs, started services, etc.
Networking Features	LAN emulation: Virtual Ethernet adapter, full WWAN support (Wireless Wide Area Network, Mobile Broadband)
Network protocols	IPv4 / IPv6 Dual Stack
Dialer [2]	NCP Internet Connector or Microsoft RAS Dialer (for ISP dial-in using dial-in script)
Seamless Roaming [2, 6]	Automatic switching of the VPN tunnel to another Internet transmission medium (LAN/WLAN/3G/4G) without IP address change so that applications communicating via the VPN tunnel are not affected or the application session is not disconnected.
VPN Path Finder [6]	NCP VPN Path Finder Technology, fallback IPsec /HTTPS (port 443) if port 500 or UDP encapsulation is not possible.
IP Address Allocation	DHCP (Dynamic Host Control Protocol); DNS 2: Dialing the central gateway with changing public IP address by querying the IP address via a DNS server.
Media	Internet, LAN, WLAN, GSM (incl. HSCSD), GPRS, UMTS, LTE, HSDPA, 5G
Line Management	DPD with configurable time interval; short hold mode; timeout (time and charge controlled); budget manager (management of connection time and/or volume for GPRS/UMTS and WLAN, for GPRS/UMTS separate management for roaming abroad) Connection modes: automatic, manual, alternating (connection setup depends on how disconnection was done before).
APN from SIM card	The APN (Access Point Name) defines the access point of a provider for a mobile data connection. The APN data is automatically transferred from the respective SIM card to the client configuration when the provider is changed.
Data compression	IPCOMP (lzs), Deflate (only for IKEv1)
Quality of Service	Prioritization of configured data streams within the VPN tunnel in the send direction.
Further features [3]	Automatic media type detection, UDP encapsulation, WISPr support (T-Mobile hotspots),

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • 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

	IPsec roaming or, WLAN roaming (prerequisite: NCP (Virtual) Secure Enterprise VPN Server or NCP Secure VPN GovNet Server).
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 (German, English); Client Info Center; Configuration, connection control and monitoring, connection statistics, log files (colored display, easy copy&paste function); Internet availability test; Trace tool for error diagnosis; Display of connection status; Integrated support of Mobile Connect Cards; Configuration and profile management with password protection, configuration parameter locking
Central management	The following software versions or newer are required for the operation and central management of the NCP VS GovNet Connector: • NCP Secure Enterprise Management Server — Version 6.00 or newer • NCP Management Console: — Version 6.00 or newer • VS GovNet Connector Configuration Plugin: — Version 2.00 or newer • License Plugin: — Version 12.30 or newer • Firewall Plug-in: — Version 12.11 or newer • PKI Enrollment Plug-in: — Version 4.05 or newer • Endpoint Policy Plug-in: — Version 4.00 or newer

[1] For approved operation according to VS-NfD, the specifications of the BSI regarding the operating system used must be observed.
[2] This functionality is not part of the VS-NfD approval.
[3] For approved operation according to VS-NfD, only the algorithms intended for this purpose and solutions approved by the BSI for strong authentication for VS-NfD may be used. This can be done, for example, by means of a smart card reader with integrated PIN pad, such as the REINER SCT cyberJack® RFID standard.
[4] The NCP Friendly Net Detection Server can be downloaded for free as an add-on here: https://www.ncp-e.com/en/service-resources/download-vpn-client/
[5] Prerequisite: NCP Secure Enterprise VPN Server, NCP Virtual Secure Enterprise VPN Server or NCP Secure VPN GovNet Server, NCP Secure Enterprise Management
[6] Prerequisite: NCP Secure Enterprise VPN Server, NCP Virtual Secure Enterprise VPN Server or NCP Secure VPN GovNet Server
[7] For the correct function the installation of a SmartCard API of the respective manufacturer is necessary (Telesec TCOS Read Only Cardmodul to Microsoft SmartCard BaseCSP with ECC support V1.1.0.0; Atos CardOS API V5.5)

The German Federal Office for Information Security (BSI) granted approval (BSI-VSA-10520) to the NCP VS GovNet Connector 2.0 on May 14, 2021.
You can request a free 30-day full version here: vertrieb@ncp-e.com

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • 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