NCP VS GovNet Connector
Release Notes

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

Voraussetzungen

Microsoft Windows Betriebssysteme:
Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows 10 (64 Bit) ab Version 1607 bis einschließlich Version 22H2 auf x86-64 Prozessorarchitektur
- Windows 11 (64 Bit) bis Version 22H2 auf x86-64 Prozessorarchitektur

HotSpot-Anmeldung
Für die Verwendung der HotSpot-Anmeldung muss mind. die Version 101.0.1210.39 der Microsoft WebView2-Runtime installiert sein.

Für die Nutzung des NCP VS GovNet Connectors im Rahmen einer BSI-Zulassung für die Verarbeitung und Übertragung von VS – NUR FÜR DEN DIENSTGEBRAUCH eingestuften Informationen gelten die entsprechenden Vorgaben für das zugrunde liegende Betriebssystem sowie die Konfiguration des NCP VS GovNet Connectors.

Voraussetzung für den Betrieb mit dem NCP Secure Enterprise Management (SEM)

Um diese Client-Version zentral verwalten zu können, bedarf es der folgenden Komponenten:

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

Die folgenden Funktionen sind ab der Connector-Version 2.20 nicht mehr verfügbar:

- SMS Center
- Verbindungsmedium: Modem, xDSL, ext. Dialer
- Credential Provider

Wichtiger Hinweis zum Update von einem VS GovNet Connector 2.1x oder älter:

Für den VS GovNet Connector 2.20 wird ein neues Signatur-Zertifikat genutzt, um die Binaries des VS GovNet Connectors zu signieren. Aus diesem Grund muss vor einem Softwareupdate von einer Version 2.1x oder älter auf 2.20 oder höher Folgendes in der angegebenen Reihenfolge getan werden:

1. Aktualisieren Sie das VS GovNet Connector SEM Plug-in auf die Version 2.20 oder höher
2. Erzeugen Sie alle erforderlichen VS GovNet Connector-Konfigurationen neu
3. Verteilen Sie die neuen VS GovNet Connector-Konfigurationen
4. Aktualisieren Sie die Software des VS GovNet Connectors

1. Neue Leistungsmerkmale und Erweiterungen

Nutzung von SmartCard-Lesern ohne integriertes PIN-Pad

Mit dieser Version 2.20 des VS GovNet Connectors ist die BSI-Zulassung auf die Nutzung von SmartCard-Lesern ohne integriertes PIN-Pad erweitert worden. Dies gilt dementsprechend auch für im Laptop integrierte SmartCard-Leser.

Unterstützung der WPA3-Verschlüsselung

Der im VS GovNet Connector integrierte WLAN-Manager kann nun auch mit WPA3 verschlüsselte WLANs verwalten.

2. Verbesserungen / Fehlerbehebungen

Neue Rechtestruktur innerhalb `C:\ProgramData\NCP\`

Die Verzeichnis- und Rechtestruktur wurde so umgebaut, dass keine Anwendung im User- und System-Kontext in das gleiche Verzeichnis schreibt.

Fehldarstellung in der Firewallkonfiguration

Wurde die GUI des Connectors mit Administratorrechten gestartet und die Parametersperre entfernt, so kam es zu einer Fehldarstellung innerhalb der Firewallkonfiguration. Dieses Problem wurde behoben.

Überarbeitetes Datei-Handling der ncp.db

In seltenen Fällen wurde die Datei `ncp.db` während des Betriebes unbrauchbar, wodurch der Client seine Lizenz verloren hatte. Dieses Problem wurde behoben.

Update auf zlib Version 1.2.12

Die im VPN-Client verwendete zlib-Version wurde auf 1.2.12 angehoben. Damit wurde die zlib-Sicherheitslücke [CVE-2018-25032] geschlossen.

Erkennung des Smartcard-Kartenstatus

Erfolgt der Zugriff auf den SmartCard-Leser via CSP und einen ausgewählten CSP-Provider, so kann die Erkennung einer gezogenen oder gesteckten SmartCard fehlschlagen. Dieses Problem wurde behoben.

Hotspot-Anmeldeseiten nicht sichtbar

Sofern die GUI des VS GovNet Connectors mit der Einstellung „Icon im System Tray“ gestartet wurde, wurde die Webseite des HotSpots nicht dargestellt. Dieses Problem wurde behoben.

OpenSSL Sicherheitspatch

Die Sicherheitslücken [CVE-2022-0778] und [CVE-2020-1971] wurden in OpenSSL behoben.

Software-Update

In seltenen Fällen kam es während des Software-Updates zu einem Abbruch. Dieses Problem wurde behoben.

Betriebssystemanzeige im Client Info Center

Im Client Info Center wurde bei einem vorhandenen Windows 11-Betriebssystem fälschlicherweise Windows 10 angezeigt. Dieses Problem wurde behoben.

Update-Dialog

Mit dieser Version des VS GovNet Connectors wird, im Falle gesendeter Log-Dateien und der Benachrichtigungs-Einstellung „nur bei vorhandenen Updates“ in der Update-Liste, kein Update-Dialog beim Anwender angezeigt. Für die Benachrichtigungs-Einstellungen „immer“ und „nie“ in der Software Update Liste hat sich das Verhalten nicht geändert.

Firewall: In der FND-Konfiguration für den VS GovNet Connector wurde der Parameter „Auf bekannte Netze periodisch prüfen“ hinzugefügt

Firewall-Option „Firewall bei gestopptem Client weiterhin verwenden“ als Standardwert

Diese Anpassung bewirkt den Schutz des Clientrechners durch die Firewall des VS GovNet Connectors nach dessen Installation (ohne Konfiguration) und dem darauffolgenden ersten Neustart des Rechners.

Update auf OpenSSL Version 1.0.2zf

Die im VS GovNet Connector verwendete OpenSSL-Version wurde auf 1.0.2zf angehoben.

3. Bekannte Einschränkungen

VPN-Verbindungen mit PSK

Im zentralen Management des VS GovNet Connectors können keine benutzerspezifischen Einstellungen vorgenommen werden. Die Erzeugung und Nutzung einer individuellen Konfiguration mit PSK ist daher nicht möglich.

VPN-Verbindungen ohne Zertifikatskonfiguration

VPN-Verbindungen ohne Zertifikatskonfiguration, wie beispielsweise IKEv2 mit EAP Authentisierung, können vom VS GovNet Connector nicht ausgeführt werden.

Nach einem Konfigurations-Update wird die VPN-Verbindung sofort getrennt

Nachdem der VS GovNet Connector ein Konfigurationsupdate vom NCP Secure Enterprise Management erhalten hat, wird die VPN-Verbindung beendet.

Proxy für Path Finder wird nicht abgefragt

In der Konfiguration des VS GovNet Connectors lässt sich ein Proxy für die Nutzung von VPN Path Finder konfigurieren. In dieser Version des VS GovNet Connectors wird diese Konfiguration nicht berücksichtigt.

Fehlermeldung bei der Lizensierung des VS GovNet Connectors

Erhält der VS GovNet Connector aus dem zentralen Management seinen Lizenzschlüssel, so erscheint im Connector-Log dreimal die folgende Fehlermeldung:

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

Diese Fehlermeldungen können ignoriert werden und haben keinen Einfluss auf die Funktionsweise des VS GovNet Connectors bzw. dessen Lizenzierung.

Keine Unterscheidung zwischen Client- und VS GovNet Connector-Plug-in in einer Administrator Gruppe

In einer Administrator-Gruppe kann zwischen den Plug-ins für den NCP Secure Enterprise Client und dem VS GovNet Connector nicht unterschieden werden. Konfigurierte Berechtigungen treffen in diesem Fall sowohl für „Client“ als auch „Connector“ zu.
Sofern der NCP Secure Enterprise Client und der VS GovNet Connector verwendet werden empfiehlt es sich zur Konfiguration der jeweiligen Plug-ins eigene Administratoren in unterschiedlichen Administrator-Gruppen anzulegen.

Service Release: **2.11 r28781**
Datum: **Februar 2022**

Voraussetzungen

Microsoft Windows Betriebssysteme:
Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt.

- Windows 10 (64 Bit) ab Version 1607 bis einschließlich Version 21H1 auf x86-64 Prozessorarchitektur
- Windows 11 (64 Bit) bis Version 21H2 auf x86-64 Prozessorarchitektur

Für die Nutzung des NCP VS GovNet Connectors im Rahmen einer BSI-Einsatzempfehlung für die Verarbeitung und Übertragung von VS – NUR FÜR DEN DIENSTGEBRAUCH eingestuften Informationen gelten die entsprechenden Vorgaben für das zugrunde liegende Betriebssystem sowie die Konfiguration des NCP VS GovNet Connectors.

Voraussetzung für den Betrieb mit dem NCP Secure Enterprise Management (SEM)

Um diese Client-Version zentral verwalten zu können, bedarf es der folgenden Komponenten:

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

1. Neue Leistungsmerkmale und Erweiterungen

Keine.

2. Verbesserungen / Fehlerbehebungen

Falsch gesetzte Proxy-Einstellungen

Beim Beenden der Client-GUI wurden die Proxy-Einstellungen des Betriebssystems falsch gesetzt, wodurch es beim Senden und Empfangen von Anwendungsdaten zu Störungen kam. Dieses Problem wurde behoben.

Firewall verspätet nach Neustart wirksam

In bestimmten Fällen war die Firewall nach einem Neustart während der FND-Erkennung nicht wirksam. Dieses Problem wurde behoben.

3. Bekannte Einschränkungen

Problem beim Konfigurationsdownload und verwendetem NCP Secure Enterprise Management 6.0

Bei der Verwendung der Version 6.0 des NCP Secure Enterprise Management Servers ist der Konfigurationsdownload auf den VS GovNet Connector bei einer bestimmten Einstellung im VS GovNet Connector Plug-in nicht möglich:
Ist in der VS GovNet Connector Vorlage unter „Info / Profil Einstellungen“ die Auswahl der VS GovNet Connector-Version auf „2.10“ konfiguriert, so erfolgt kein Konfigurationsdownload. Der Konfigurationsdownload erfolgt nur durch Umstellung der VS GovNet Connector-Version auf „immer“.

Fehler bei der Verwendung von Kartenlesegeräten

Bei Updates auf eine höhere Version kann es in seltenen Fällen zu einem Fehler mit CSP Kartenlesern kommen, wenn der User nicht als Admin auf dem PC angemeldet ist.

VPN-Verbindungen mit PSK

Im zentralen Management des VS GovNet Connectors können keine benutzerspezifischen Einstellungen vorgenommen werden. Die Erzeugung und Nutzung einer individuellen Konfiguration mit PSK ist daher nicht möglich.

VPN-Verbindungen ohne Zertifikatskonfiguration

VPN-Verbindungen ohne Zertifikatskonfiguration, wie beispielsweise IKEv2 mit EAP Authentisierung, können vom VS GovNet Connector nicht ausgeführt werden.

Installation auf Windows 10 (32 Bit) oder älteren Windows Systemen

Der VS GovNet Connector lässt sich zwar auf Windows 8 (64 Bit) oder Windows 10 (32 Bit) installieren, jedoch wird die korrekte Funktion durch den Integrationsdienst gesperrt. Dieses Verhalten ist insofern korrekt, da Plattformen vor Windows 10 oder in 32 Bit-Architektur nicht unterstützt werden.

Nachträgliche Installation der NCP Secure GovNet Box Suite liefert Fehlersituation

Die NCP Secure GovNet Box Suite und der VS GovNet Connector können nicht zeitgleich auf derselben Hardware funktionsfähig installiert sein. Die nachträgliche Installation der NCP Secure GovNet Box Suite auf ein Gerät mit bereits darauf installierten VS GovNet Connector wird jedoch nicht verhindert und führt zu einer Fehlersituation.

Nach einem Konfigurations-Update wird die VPN-Verbindung sofort getrennt

Nachdem der VS GovNet Connector ein Konfigurationsupdate vom NCP Secure Enterprise Management erhalten hat, wird die VPN-Verbindung beendet.

Proxy für Path Finder wird nicht abgefragt

In der Konfiguration des VS GovNet Connectors lässt sich ein Proxy für die Nutzung von VPN Path Finder konfigurieren. In dieser Version des VS GovNet Connectors wird diese Konfiguration nicht berücksichtigt.

Service Release: **2.10 r28778**
Datum: **Oktober 2021**

Voraussetzungen

Microsoft Windows Betriebssysteme:
Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt.

- Windows 10 (64 Bit) ab Version 1607 bis einschließlich Version 21H1 auf x86-64 Prozessorarchitektur
- Windows 11 (64 Bit) bis Version 21H2 auf x86-64 Prozessorarchitektur

Für die Nutzung des NCP VS GovNet Connectors im Rahmen einer BSI-Einsatzempfehlung für die Verarbeitung und Übertragung von VS – NUR FÜR DEN DIENSTGEBRAUCH eingestuften Informationen gelten die entsprechenden Vorgaben für das zugrunde liegende Betriebssystem sowie die Konfiguration des NCP VS GovNet Connectors.

Voraussetzung für den Betrieb mit dem NCP Secure Enterprise Management (SEM)

Um diese Client-Version zentral verwalten zu können, bedarf es der folgenden Komponenten:

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

1. Neue Leistungsmerkmale und Erweiterungen

Überarbeitete Hotspot-Anmeldung

Ab dieser Version 2.10 des VS GovNet Connectors kann die Hotspot-Anmeldung innerhalb des durch das Dokument „Einsatz- und Betriebsbedingungen“ vorgegebenen, zugelassenen Betriebes verwendet werden. Als Webbrowser wird dafür der Chrome-basierte Microsoft Edge-Webbrowser mittels WebView2-Runtime aufgerufen und ausschließlich für den Zweck der Anmeldung an einem Hotspot verwendet. Voraussetzung hierfür ist die installierte WebView2-Runtime (ab der Version 94.0.992.31 oder neuer) innerhalb des Betriebssystems. Die WebView2-Runtime kann hier heruntergeladen werden:
https://developer.microsoft.com/en-us/microsoft-edge/webview2/#download-section

Friendly Net Detection

Ab dieser Version 2.10 des VS GovNet Connectors kann die Friendly Net Detection innerhalb des durch die Einsatz- und Betriebsbedingungen vorgegebenen, zugelassenen Betriebes verwendet werden. Voraussetzung hierfür ist die Verwendung des NCP Friendly Net Detection Servers ab der Version 4.0.

2. Verbesserungen / Fehlerbehebungen

Firewall Option „Datenverkehr für GovNet Box zulassen“ entfernt

Im VS GovNet Connector Plug-in wurde die Firewalloption „Datenverkehr für GovNet Box zulassen“ ab der Version 2.10 des VS GovNet Connectors entfernt.

Deinstallationsroutine angepasst

Bis zur Vorversion 2.01 des VS GovNet Connectors verblieb die Datei `import.vscfg` noch im Installationsverzeichnis nach erfolgter Deinstallation. Dieses Problem wurde behoben.

Fehler bei gesetzter Option „Profil Filter Gruppen“ im VS GovNet Connector Plug-in

Bei gesetzter Option „Profil Filter Gruppen“ im VS GovNet Connector Plug-in konnten im VS GovNet Connector die erstellten Profilgruppen nicht korrekt ausgewählt werden. Dieses Problem wurde behoben.

Fehler in `ncpclientcmd.exe`

Wurde der Client über `ncpclientcmd.exe /stop` beendet und soll anschließend neu gestartet werden, musste der Start-Befehl zweimal hintereinander ausgeführt werden, damit der Client wieder ordnungsgemäß arbeitet. Dieses Problem wurde behoben.

Problembehebung beim Software-Update via NCP Management Server

Beim Software-Update via NCP Management Server wurde im Management nach dem Updatevorgang noch die alte Clientversion angezeigt. Ebenso wurde die Anzahl der heruntergeladenen Update-Pakete nicht erhöht. Dieses Problem wurde behoben.

3. Bekannte Einschränkungen

Problem beim Konfigurationsdownload und verwendetem NCP Secure Enterprise Management 6.0

Bei der Verwendung der Version 6.0 des NCP Secure Enterprise Management Servers ist der Konfigurationsdownload auf den VS GovNet Connector bei einer bestimmten Einstellung im VS GovNet Connector Plug-in nicht möglich:
Ist in der VS GovNet Connector Vorlage unter „Info / Profil Einstellungen“ die Auswahl der VS GovNet Connector-Version auf „2.10“ konfiguriert, so erfolgt kein Konfigurationsdownload. Der Konfigurationsdownload erfolgt nur durch Umstellung der VS GovNet Connector-Version auf „immer“.

Fehler bei der Verwendung von Kartenlesegeräten

Bei Updates auf eine höhere Version kann es in seltenen Fällen zu einem Fehler mit CSP Kartenlesern kommen, wenn der User nicht als Admin auf dem PC angemeldet ist.

VPN-Verbindungen mit PSK

Im zentralen Management des VS GovNet Connectors können keine benutzerspezifischen Einstellungen vorgenommen werden. Die Erzeugung und Nutzung einer individuellen Konfiguration mit PSK ist daher nicht möglich.

VPN-Verbindungen ohne Zertifikatskonfiguration

VPN-Verbindungen ohne Zertifikatskonfiguration, wie beispielsweise IKEv2 mit EAP Authentisierung, können vom VS GovNet Connector nicht ausgeführt werden.

Installation auf Windows 10 (32 Bit) oder älteren Windows Systemen

Der VS GovNet Connector lässt sich zwar auf Windows 8 (64 Bit) oder Windows 10 (32 Bit) installieren, jedoch wird die korrekte Funktion durch den Integrationsdienst gesperrt. Dieses Verhalten ist insofern korrekt, da Plattformen vor Windows 10 oder in 32 Bit-Architektur nicht unterstützt werden.

Nachträgliche Installation der NCP Secure GovNet Box Suite liefert Fehlersituation

Die NCP Secure GovNet Box Suite und der VS GovNet Connector können nicht zeitgleich auf derselben Hardware funktionsfähig installiert sein. Die nachträgliche Installation der NCP Secure GovNet Box Suite auf ein Gerät mit bereits darauf installierten VS GovNet Connector wird jedoch nicht verhindert und führt zu einer Fehlersituation.

Nach einem Konfigurations-Update wird die VPN-Verbindung sofort getrennt

Nachdem der VS GovNet Connector ein Konfigurationsupdate vom NCP Secure Enterprise Management erhalten hat, wird die VPN-Verbindung beendet.

Proxy für Path Finder wird nicht abgefragt

In der Konfiguration des VS GovNet Connectors lässt sich ein Proxy für die Nutzung von VPN Path Finder konfigurieren. In dieser Version des VS GovNet Connectors wird diese Konfiguration nicht berücksichtigt.

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

Voraussetzungen

Microsoft Windows Betriebssysteme:
Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt.

- Windows 10 (64 Bit)
  (ab Version 1607 bis einschließlich Version 21H1 auf x86-64 Prozessorarchitektur)

Für die Nutzung des NCP VS GovNet Connectors im Rahmen einer BSI-Einsatzempfehlung für die Verarbeitung und Übertragung von VS – NUR FÜR DEN DIENSTGEBRAUCH eingestuften Informationen gelten die entsprechenden Vorgaben für das zugrunde liegende Betriebssystem sowie die Konfiguration des NCP VS GovNet Connectors.

Voraussetzung für den Betrieb mit dem NCP Secure Enterprise Management (SEM)

Um diese Client-Version zentral verwalten zu können, bedarf es der folgenden zentralen Komponenten:

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

1. Neue Leistungsmerkmale und Erweiterungen

Anpassung des Software Update Packages

Ab dieser Version wird für den zukünftigen Updatevorgang via NCP Management mindestens die Version 2.00 des VS GovNet Connectors vorausgesetzt, da hierfür ein bereits vorhandener Integritätsdienst benötigt wird. Ein Update einer Version 1.x ist daher nicht mehr möglich.

2. Verbesserungen / Fehlerbehebungen

Englische Hilfe

In der Vorversion des VS GovNet Connectors ist die englische Hilfe nicht vorhanden. Diese wurde nun ergänzt.

Entfernen der FIPS-Option unter Programm ändern

Wurde bei einem bereits installierten VS GovNet Connector die Installationsroutine gestartet, so lieferte diese unter „Programm ändern“ fälschlicherweise die Option „FIPS Mode“. Dieser Fehler wurde behoben.

Problem mit dem Verbindungsaufbau nach Konfigurationsdownload

Bei der Verwendung einer SmartCard zur Benutzerauthentisierung konnte es nach einem Konfigurationsupdate durch das zentrale Management vorkommen, dass die falsche BenutzerID für den Verbindungsaufbau genutzt wurde und daher keine Verbindung zustande kam. Dieser Fehler wurde behoben.

Falsche Anzeige im VS GovNet Connector für Standard-Profil

Wurde in der Konfiguration die Option „Standard-Profil nach jedem Neustart des Systems“ gesetzt, erfolgte die Darstellung der Profile im VS GovNet Connector invertiert, d.h. alle anderen VPN-Profile wurden als Standard-Profil angezeigt, jedoch das dafür konfigurierte Profil nicht. Beim Neustart des Rechners wurde das korrekte Standard-Profil für den VS GovNet Connector ausgewählt. Es handelte sich daher ausschließlich um einen Darstellungsfehler. Dieser Fehler wurde behoben.

Option für „Manuell hinzugefügte WLAN-Profile löschen“ wird nicht umgesetzt

War im zentralen Management die Option „Manuell hinzugefügte WLAN-Profile löschen“ ausgewählt, so wurde diese nach einem Konfigurationsupdate des VS GovNet Connectors nicht ausgeführt. Dieser Fehler wurde behoben.

Integritätsdienst wurde beim Update nicht beendet

Beim Update auf eine höhere Version kam es beim Deinstallieren der Vorgängerversion zu einem Fehler mit `ncpclientcmd.exe /stop`, wodurch der Integritätsdienst nicht beendet werden konnte. Dieser Fehler wurde behoben.

Fehler nach Windows-Funktionsupdate

Durch die Installation eines Funktionsupdates von Windows konnte in wenigen Fällen der NCP VS GovNet Connector nicht mehr gestartet werden und es erschien eine entsprechende Fehlermeldung. Dieser Fehler wurde behoben.

Fehler mit Einstellung "Nach Verbindungsaufbau minimieren"

Wird der NCP VS GovNet Connector installiert und die Auswahl „Nach Verbindungsaufbau minimieren“ gewählt, minimiert sich der Monitor nach erstmaligem Starten nicht. In den folgenden Starts funktioniert jedoch das Minimieren. Dieser Fehler wurde behoben.

Fenster mit ncpintegritycheckcli.exe wird sehr lange angezeigt

Nach dem Herunterladen des Software Update Packages vom NCP SEM, wurde in einigen Fällen sehr lange ein schwarzes Programmfenster angezeigt. Dieses Fenster überlagerte andere Anwendungen. Dieser Fehler wurde behoben.

Verbesserung der FND-Kompatibilität zu Netzwerk-Switches

Die libcurl-Bibliothek wurde auf die Version 7.77.0 angehoben

Absturz des ncprwsnt-Dienstes

In seltenen Fällen kam es zum Absturz des ncprwsnt-Dienstes. Dieses Problem wurde behoben.

GUI startet nicht nach Neustart des Connectors via CLI

Wurde der VS GovNet Connector mittels CLI-Eingabe `ncpclientcmd /stop` beendet und anschließend mit `ncpclientcmd /start` wieder gestartet, so startete die GUI des VS GovNet Connectors nicht mehr. Dieses Problem wurde behoben.

3. Bekannte Einschränkungen

Fehler bei der Verwendung von Kartenlesegeräten

Bei Updates auf eine höhere Version kann es in seltenen Fällen zu einem Fehler mit CSP Kartenlesern kommen, wenn der User nicht als Admin auf dem PC angemeldet ist.

VPN-Verbindungen mit PSK

Im zentralen Management des VS GovNet Connectors können keine benutzerspezifischen Einstellungen vorgenommen werden. Die Erzeugung und Nutzung einer individuellen Konfiguration mit PSK ist daher nicht möglich.

VPN-Verbindungen ohne Zertifikatskonfiguration

VPN-Verbindungen ohne Zertifikatskonfiguration, wie beispielsweise IKEv2 mit EAP Authentisierung, können vom VS GovNet Connector nicht ausgeführt werden.

Installation auf Windows 10 (32 Bit) oder älteren Windows Systemen

Der VS GovNet Connector lässt sich zwar auf Windows 8 (64 Bit) oder Windows 10 (32 Bit) installieren, jedoch wird die korrekte Funktion durch den Integrationsdienst gesperrt. Dieses Verhalten ist insofern korrekt, da Plattformen vor Windows 10 oder in 32 Bit-Architektur nicht unterstützt werden.

Nachträgliche Installation der NCP Secure GovNet Box Suite liefert Fehlersituation

Die NCP Secure GovNet Box Suite und der VS GovNet Connector können nicht zeitgleich auf derselben Hardware funktionsfähig installiert sein. Die nachträgliche Installation der NCP Secure GovNet Box Suite auf ein Gerät mit bereits darauf installierten VS GovNet Connector wird jedoch nicht verhindert und führt zu einer Fehlersituation.

Software-Paket Download wird im NCP Secure Enterprise Management nicht angezeigt

Wird über das NCP Secure Enterprise Management ein Update des VS GovNet Connectors verteilt, so werden die verteilten Updatepakete nicht korrekt angezeigt.

Nach einem Konfigurations-Update wird die VPN-Verbindung sofort getrennt

Nachdem der VS GovNet Connector ein Konfigurationsupdate vom NCP Secure Enterprise Management erhalten hat, wird die VPN-Verbindung beendet.

VPN-Profile einer Gruppe können nicht geöffnet werden

Ist am zentralen Management die Option „Profil Filter Gruppen“ aktiviert und wurden Profile in einer Gruppe angelegt, so können diese Profile am VS GovNet Connector nicht ausgewählt werden.

Proxy für Path Finder wird nicht abgefragt

In der Konfiguration des VS GovNet Connectors lässt sich ein Proxy für die Nutzung von VPN Path Finder konfigurieren. In dieser Version des VS GovNet Connectors wird diese Konfiguration nicht berücksichtigt.

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

Voraussetzungen

Microsoft Windows Betriebssysteme:
Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt.

- Windows 10 (64 Bit)
  (ab Version 1607 bis einschließlich Version 20H2 auf x86-64 Prozessorarchitektur)

Für den Nutzung des NCP VS GovNet Connectors im Rahmen einer BSI-Einsatzempfehlung für die Verarbeitung und Übertragung von VS – NUR FÜR DEN DIENSTGEBRAUCH eingestuften Informationen gelten die entsprechenden Vorgaben für das zugrunde liegende Betriebssystem sowie die Konfiguration des NCP VS GovNet Connectors.

Voraussetzung für den Betrieb mit dem NCP Secure Enterprise Management (SEM)

Um diese Client-Version zentral verwalten zu können, bedarf es der folgenden zentralen Komponenten:

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

1. Neue Leistungsmerkmale und Erweiterungen

Self Check durch neuen Integritätsdienst

Der im VS GovNet Connector vorhandene Integritätsdienst führt eine kontinuierliche Überwachung der korrekten Funktionalität im Betriebssystem durch. Eine etwaige Kompromittierung des VS GovNet Connectors resultiert in der Überführung des Endgerätes in einen sicheren Zustand, der eine weitere Kommunikation jeglicher Art unterbindet.
Des Weiteren dient der Integritätsdienst der Durchführung eines, zu jedem Zeitpunkt, sicheren Remote-Updateprozesses des VS GovNet Connectors durch das zentrale Management.

Audit-Log

Das neue Audit-Log fasst alle sicherheitsrelevanten Ereignisse des VS GovNet Connectors zusammen. Es wird periodisch an das zentrale Management zur Auswertung übertragen.

VS GovNet Connector Plug-in

Der VS GovNet Connector benötigt zur Konfiguration im zentralen Management das VS GovNet Connector-Plug-in. Beim Erstellen einer neuen Vorlage entsprechen die voreingestellten Parameter den Einstellungen im SecOPs-Dokument für den BSI-zugelassenen Betrieb. Jede erzeugte Konfiguration enthält einen fortlaufenden Epochenzähler der sich aus dem aktuellen UNIX-Timestamp ergibt. Zudem ist die für den VS GovNet Connector erzeugte Konfiguration zum Schutz vor Manipulation signiert und wird vom VS GovNet Connector beim Erhalt überprüft.
Eine lokale Konfiguration des VS GovNet Connectors ist nicht möglich. Auch kann die Konfiguration vom Anwender nicht eingesehen werden.

Tool zum zurücksetzen des PCs aus dem "sicheren Fehlerzustand"

Das CLI-Tool `integrityStateReset.exe` ist Teil der Installation des VS GovNet Connectors. Es wird zum Zurücksetzen des Arbeitsplatzrechners aus dem „sicheren Fehlerzustand“ benötigt. Dieser Zustand wird aufgerufen sobald der Integritätsdienst ein Problem feststellt. Das genannte CLI-Tool kann nur von einem Administrator mit entsprechenden Rechten aufgerufen werden.

2. Verbesserungen / Fehlerbehebungen

Keine.

3. Bekannte Einschränkungen

VPN-Verbindungen mit PSK

Im zentralen Management des VS GovNet Connectors können keine benutzerspezifischen Einstellungen vorgenommen werden. Die Erzeugung und Nutzung einer individuellen Konfiguration mit PSK ist daher nicht möglich.

VPN-Verbindungen ohne Zertifikatskonfiguration

VPN-Verbindungen ohne Zertifikatskonfiguration, wie beispielsweise IKEv2 mit EAP Authentisierung, können vom VS GovNet Connector nicht ausgeführt werden.

Installation auf Windows 10 (32 Bit) oder älteren Windows Systemen

Der VS GovNet Connector lässt sich zwar auf Windows 8 (64 Bit) oder Windows 10 (32 Bit) installieren, jedoch wird die korrekte Funktion durch den Integrationsdienst gesperrt. Dieses Verhalten ist insofern korrekt, da Plattformen vor Windows 10 oder in 32 Bit-Architektur nicht unterstützt werden.

Nachträgliche Installation der NCP Secure GovNet Box Suite liefert Fehlersituation

Die NCP Secure GovNet Box Suite und der VS GovNet Connector können nicht zeitgleich auf derselben Hardware funktionsfähig installiert sein. Die nachträgliche Installation der NCP Secure GovNet Box Suite auf ein Gerät mit bereits darauf installierten VS GovNet Connector wird jedoch nicht verhindert und führt zu einer Fehlersituation.

Software-Paket Download wird im NCP Secure Enterprise Management nicht angezeigt

Wird über das NCP Secure Enterprise Management ein Update des VS GovNet Connectors verteilt, so werden die verteilten Updatepakete nicht korrekt angezeigt.

Nach einem Konfigurations-Update wird die VPN-Verbindung sofort getrennt

Nachdem der VS GovNet Connector ein Konfigurationsupdate vom NCP Secure Enterprise Management erhalten hat wird die VPN-Verbindung beendet. Jedoch wird das Updatepaket bzw. die neue Konfiguration nicht geladen.

VPN-Profile einer Gruppe können nicht geöffnet werden

Ist am zentralen Management die Option „Profil Filter Gruppen“ aktiviert und wurden Profile in einer Gruppe angelegt, so können diese Profile am VS GovNet Connector nicht ausgewählt werden.

Proxy für Path Finder wird nicht abgefragt

In der Konfiguration des VS GovNet Connectors lässt sich ein Proxy für die Nutzung von VPN Path Finder konfigurieren. In dieser Version des VS GovNet Connectors wird diese Konfiguration nicht berücksichtigt.

Falsche Anzeige im VS GovNet Connector für Standard-Profil

Wurde in der Konfiguration die Option „Standard-Profil nach jedem Neustart des Systems“ gesetzt, erfolgt die Darstellung der Profile im VS GovNet Connector invertiert, d.h. alle anderen VPN-Profile werden als Standard-Profil angezeigt, jedoch das dafür konfigurierte Profil nicht. Beim Neustart des Rechners wird das korrekte Standard-Profil für den VS GovNet Connector ausgewählt. Es handelt sich daher ausschließlich um einen Darstellungsfehler.

Option für „Manuell hinzugefügte WLAN-Profile löschen“ wird nicht umgesetzt

Ist im zentralen Management die Option „Manuell hinzugefügte WLAN-Profile löschen“ ausgewählt, so wird diese nach dem Update des VS GovNet Connectors nicht ausgeführt.

Im VS GovNet Connector ist die englische Hilfe nicht vorhanden

4. Hinweise zum NCP VS GovNet Connector

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:

https://www.ncp-e.com/de/service/download-vpn-client/versionsinformationen/

Weitere Informationen zum NCP VS GovNet Connector finden Sie hier:

https://www.ncp-e.com/de/produkte/vpn-fuer-vs-nfd/

Weitere Unterstützung bei Fragen zum NCP VS GovNet Connector, erhalten Sie über die Mail-Adressen auf folgender Seite:

https://www.ncp-e.com/de/unternehmen/kontakt/

5. Verwendete Open Source Software Komponenten

Die Software verwendet Open Source Software Komponenten, die in der beigefügten Datei *OpenSourceLicenseTerms-ncpgovnet.pdf* aufgeführt sind. Für diese Open Source Software Komponenten gelten ausschließlich die in der Datei *OpenSourceLicenseTerms-ncpgovnet.pdf* genannten Open Source Software Lizenzbedingungen.

6. Leistungsmerkmale

Betriebssysteme [1]	Microsoft Windows 10 (64 Bit) Version 1607 oder neuer auf x86-64 Prozessorarchitektur Microsoft Windows 11 (64 Bit) auf x86-64 Prozessorarchitektur
Security Features	Unterstützung aller IPsec Standards nach RFC
Personal Firewall Firewall Configuration	Stateful Packet Inspection; IP-NAT (Network Address Translation); differenzierte Filterregeln bezüglich: Protokolle, Ports, Applikationen und Adressen, Schutz des LAN-Adapters; IPv4- und IPv6-Unterstützung; zentrale Administration Friendly Net Detection (Automatische Umschaltung der Firewall-Regeln bei Erkennung des angeschlossenen Netzwerkes anhand eines NCP FND-Servers [4]); Secure Hotspot Login; Home Zone [2];
VPN Bypass [2]	Die VPN-Bypass-Funktion gestattet Anwendungen festzulegen, die trotz deaktiviertem Split Tunneling außerhalb der VPN-Konfiguration direkt ins Internet kommunizieren dürfen. Alternativ ist es möglich, Domänen bzw. Zieladressen zu bestimmen, zu denen die Datenkommunikation am VPN-Tunnel vorbei stattfinden soll.
Virtual Private Networking [3]	IPsec (Layer 3 Tunneling), RFC-konform; IKEv1/IKEv2; Event log; Kommunikation nur im Tunnel; MTU Size Fragmentation und Reassembly; DPD; NAT-Traversal (NAT-T); IPsec Tunnel Mode
Verschlüsselung (Encryption) [3]	Symmetrische Verfahren: AES 128, 192, 256 Bits; Blowfish 128, 448 Bits; Triple-DES 112, 168 Bits; Dynamische Verfahren für den Schlüsselaustausch: RSA bis 8192 Bits; Seamless Rekeying (PFS); Hash Algorithmen: SHA-1, SHA-256, SHA-384, SHA-512, MD5, DH Gruppe 1, 2, 5, 14-21, 25-30
Authentisierungsverfahren [3]	IKEv1 (Aggressive und Main Mode), Quick Mode; XAUTH für erweiterte User-Authentisierung; IKEv2 IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP); PFS; PAP, CHAP, MS CHAP V.2; IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): erweiterte Authentifikation gegenüber Switches und Access Points (Layer 2); EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): erweiterte Authentifikation gegenüber Switches und Access Points auf Basis von Zertifikaten (Layer 2); Unterstützung von Zertifikaten in einer PKI: Soft-Zertifikate, Smart Cards, USB Tokens und Zertifikate mit ECC-Technologie Multi-Zertifikatskonfiguration; One-Time Passwords und Challenge Response Systeme (u.a.RSA SecurID Ready)
Starke Authentisierung [3]	X.509 v.3 Standard; biometrische Authentisierung

	PKCS#11 Interface für Verschlüsselungs-Tokens (USB und Smart Cards); Smart Card Betriebssysteme: TeleSec TCOS 3.0 Signature Card Version 2.0 Release 1, Atos CardOS V5.3 QES, V1.0; Smart Card ReaderInterfaces: PC/SC, CT-API; Microsoft CSP; PKCS#12 Interface für Private Schlüssel in Soft Zertifikaten; CSP zur Verwendung von Benutzerzertifikaten im Windows-Zertifikatsspeicher; CSP zur Verwendung von SmartCards via API des Herstellers [7] PIN-Richtlinie; administrative Vorgabe für die Eingabe beliebig komplexer PINs; Revocation: EPRL (End-entity Public-key Certificate Revocation List, *vorm. CRL*), CARL (Certification Authority Revocation List, *vorm. ARL*), OCSP
PKI Enrollment [2]	CMP (Certificate Management Protocol)
Network Access Control [5]	Endpoint Policy: Überprüfung Aktualität des Virenscanners, vorhandene Hotfixes/Service Packs, gestartete Dienste, etc.
Networking Features	LAN Emulation: Virtual Ethernet-Adapter, vollständiger WWAN-Support (Wireless Wide Area Network, Mobile Broadband)
Netzwerkprotokolle	IPv4 / IPv6 Dual Stack
Dialer [2]	NCP Internet Connector oder Microsoft RAS Dialer (für ISP-Einwahl mittels Einwahl-Script)
Seamless Roaming [2, 6]	Automatische Umschaltung des VPN-Tunnels auf ein anderes Internet-Übertragungsmedium (LAN/WLAN/3G/4G) ohne IP-Adresswechsel, so dass über den VPN-Tunnel kommunizierende Anwendungen nicht beeinflusst werden, bzw. die Anwendungs-Session nicht getrennt wird
VPN Path Finder [6]	NCP VPN Path Finder Technology, Fallback IPsec /HTTPS (Port 443) wenn Port 500 bzw. UDP Encapsulation nicht möglich ist
IP Address Allocation	DHCP (Dynamic Host Control Protocol); DNS [2]: Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server
Übertragungsmedien	Internet, LAN, WLAN, GSM (inkl. HSCSD), GPRS, UMTS, LTE, HSDPA, 5G
Line Management	DPD mit konfigurierbarem Zeitintervall; Short Hold Mode; Timeout (zeit- und gebührengesteuert); Budget Manager (Verwaltung von Verbindungszeit und/oder -volumen für GPRS/UMTS und WLAN, bei GPRS/UMTS getrennte Verwaltung für Roaming im Ausland) Verbindungsmodi: automatisch, manuell, wechselnd (Der Verbindungsaufbau ist davon abhängig wie die Trennung zuvor stattgefunden hat)
APN von SIM-Karte	Der APN (Access Point Name) definiert den Zugangspunkt eines Providers für eine mobile Datenverbindung. Die APN-Daten werden bei einem Providerwechsel automatisiert aus der jeweiligen SIM-Karte in die Client-Konfiguration übernommen
Datenkompression	IPCOMP (lzs), Deflate (nur für IKEv1)
Quality of Service	Priorisierung konfigurierter Datenströme innerhalb des VPN-Tunnels in Senderichtung

Weitere Features [3]	Automatische Mediatyp-Erkennung, UDP-Encapsulation, IPsec-Roaming bzw., WLAN-Roaming (Voraussetzung: NCP (Virtual) Secure Enterprise VPN Server oder NCP Secure VPN GovNet Server)
Point-to-Point Protokolle	PPP over GSM, PPP over Ethernet, MLP, CCP, CHAP
Internet Society RFCs und 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, IKEv2-Authentisierung nach RFC 7427 (Padding-Verfahren)
Client Monitor Intuitive, grafische Benutzeroberfläche	Mehrsprachig (Deutsch, Englisch); Client Info Center; Konfiguration, Verbindungssteuerung und -überwachung, Verbindungsstatistik, Log-Files (farbige Darstellung, einfache Copy&Paste-Funktion); Test-Werkzeug für Internet-Verfügbarkeit; Trace-Werkzeug für Fehlerdiagnose; Anzeige des Verbindungsstatus; Integrierte Unterstützung von Mobile Connect Cards; Konfigurations- und Profil-Management mit Passwortschutz, Konfigurationsparametersperre
Zentrales Management	Voraussetzung für den Betrieb und das zentrale Management des NCP VS GovNet Connectors sind folgende Softwareversionen oder neuer: • NCP Secure Enterprise Management Server — Version 6.00 oder neuer • NCP Management Console: — Version 6.00 oder neuer • VS GovNet Connector Configuration Plugin: — Version 2.10 oder neuer • License Plugin: — Version 12.30 oder neuer • Firewall Plug-in: — Version 12.30 oder neuer • PKI Enrollment Plug-in: — Version 4.05 oder neuer • Endpoint Policy Plug-in: — Version 4.00 oder neuer

[1] Für den zugelassenen Betrieb gemäß VS-NfD sind die Vorgaben des BSI bzgl. des verwendeten Betriebssystems zu beachten.
[2] Diese Funktionalität ist nicht Bestandteil der VS-NfD-Zulassung.
[3] Für den zugelassenen Betrieb gemäß VS-NfD dürfen nur die dafür vorgesehenen Algorithmen und vom BSI zugelassenen Lösungen zur starken Authentisierung für VS-NfD verwendet werden. Dies kann beispielsweise mittels eines SmartCard-Lesers mit integriertem PIN-Pad, wie dem REINER SCT cyberJack® RFID standard, geschehen.
[4] Der NCP Friendly Net Detection Server kann kostenlos als Add-On hier heruntergeladen werden: https://www.ncp-e.com/de/service/download-vpn-client/
[5] Voraussetzung: NCP Secure Enterprise VPN Server, NCP Virtual Secure Enterprise VPN Server oder NCP Secure VPN GovNet Server, NCP Secure Enterprise Management
[6] Voraussetzung: NCP Secure Enterprise VPN Server, NCP Virtual Secure Enterprise VPN Server oder NCP Secure VPN GovNet Server
[7] Für die korrekte Funktion ist die Installation einer SmartCard API des jew. Herstellers notwendig (Telesec TCOS Read Only Cardmodul zum Microsoft SmartCard BaseCSP mit ECC-Unterstützung V1.1.0.0; Atos CardOS API V5.5)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat dem NCP VS GovNet Connector 2.0 am 14. Mai 2021 die Zulassung (BSI-VSA-10520) erteilt.
Eine kostenlose 30-Tage Vollversion können Sie hier anfordern: vertrieb@ncp-e.com

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