



NCP

Release Notes

NCP VS GovNet Connector (Windows)



Service-Release: 3.02 r29006
Datum: Oktober 2025

Voraussetzungen

Betriebssystem

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 25H2 auf x86-64 Prozessorarchitektur

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 Server: Version 7.13 oder neuer
- NCP Management Console: Version 7.10 oder neuer
- VS GovNet Connector Configuration Plug-in: Version 3.01 oder neuer
- License Plug-in: Version 14.00 oder neuer
- Firewall Plug-in (optional): Version 13.00 oder neuer
- PKI Enrollment Plug-in (optional): Version 7.10 oder neuer

Weitere Voraussetzungen

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 eingestufteten Informationen gelten die entsprechenden Vorgaben für das zugrunde liegende Betriebssystem sowie die Konfiguration des NCP VS GovNet Connectors.

Wichtiger Hinweis zum VS GovNet Connector 3.00:

Dieser sollte nicht mehr verwendet werden, da hier ein altes Signatur Zertifikat verwendet wird, mit dem der Betrieb des VS GovNet Connectors 3.00 ab dem 11.06.2025 verhindert wird.

1. Neue Leistungsmerkmale und Erweiterungen

Keine.



2. Verbesserungen / Fehlerbehebungen

Privilege Escalation im NCP MSI Installer (NCPVE-2025-0626)

Während bestimmter Aktionen wie Installation, Update oder Deinstallation werden temporär Kommandozeilenfenster (cmd.exe) mit den Rechten des SYSTEM-Kontos geöffnet. In älteren Windows-Versionen ist es möglich, in diesen interaktiven Eingabeaufforderungen beliebige Befehle oder Programme mit SYSTEM-Privilegien auszuführen. Dadurch kann ein Angreifer administrative Schutzmechanismen umgehen und uneingeschränkten Zugriff auf das System erlangen. Diese Sicherheitstücke wurde geschlossen.

Bluescreen mit Windows Update KB5065426

Nach der Installation des Windows Updates KB5065426 konnte es beim Einsatz des VS GovNet Connectors zu einem Bluescreen kommen. Dieses Problem wurde behoben.

Fehler nach Ziehen und Stecken der Smartcard im laufenden Betrieb

Wird die Smartcard im laufenden Betrieb abgezogen und anschließend wieder eingesteckt, konnten Verbindungsversuche fehlschlagen. Ursache war ein fehlerhafter Umgang mit bestehenden Smartcard-Sessions/Handles nach Hot-Unplug; dieses Verhalten wurde behoben — Verbindungen funktionieren nach erneutem Einstecken wieder zuverlässig.

Verbindungsabbruch durch erfolgloses Rekeying

In manchen Fällen wurde eine aufgebaute VPN-Verbindung nach einigen Minuten unerwartet getrennt. Grund dafür war ein fehlerhaftes, wiederholt gescheitertes Rekeying des Tunnels. Dieser Fehler wurde behoben, sodass die Verbindung nun stabil bestehen bleibt.

Anpassung im IKEv2 Mobility and Multihoming (MOBIKE) Protocol

Die Verarbeitung des Cookie2-Response-Headers wurde angepasst und entspricht nun vollständig der RFC-Spezifikation.

Problembhebung: Erweitertes Logging

Es wurde ein Problem behoben, bei dem die VPN-Dienste bei aktiviertem, erweitertem Logging unerwartet stoppten und der Client dadurch abstürzte. Ursache war eine fehlerhafte CRLDP-LDAP-URL.

3. Bekannte Einschränkungen

Kein Konfigurationsupdate bei Anmeldung mit dem Pre-Logon Access Provider (PLAP)

Bei Anmeldung mit dem PLAP wird ein möglicherweise vorhandenes Konfigurationsupdate nicht während der Anmeldung geladen. Das Update erfolgt erst nach der Anmeldung am Windows Desktop und zwar nach dem im Secure Enterprise Management eingestellten Intervall. Als Abhilfe wird empfohlen die Option „Benutzer informieren, wenn er eine neue Konfiguration erhalten hat“ einzustellen.

Fehler „RSA Signature with PKCS#1 V1.5 padding is not allowed by configuration“

Bei einem Verbindungsversuch kann der Fehler „RSA Signature with PKCS#1 V1.5 padding is not allowed by configuration“ auftreten. Dieser Fehler kann insbesondere nach einem Update von älteren Versionen auftreten. In diesem Fall muss über die Konfiguration die 'Padding Standardkonfiguration' geändert werden.

Expertenmodus / Erweiterte IPsec-Optionen

- Erlaube RSA-Authentisierung mit PKCS#1 V1.5 Padding → Deaktiviert
- Erlaube RSA-Authentisierung mit SHA-1 Hash → Deaktiviert

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.

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: 3.01 r28994
Datum: Juni 2025

Voraussetzungen

Betriebssystem

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 24H2 auf x86-64 Prozessorarchitektur

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 Server: Version 7.13 oder neuer
- NCP Management Console: Version 7.10 oder neuer
- VS GovNet Connector Configuration Plug-in: Version 3.01 oder neuer
- License Plug-in: Version 14.00 oder neuer
- Firewall Plug-in (optional): Version 13.00 oder neuer
- PKI Enrollment Plug-in (optional): Version 7.10 oder neuer

Weitere Voraussetzungen

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.

Wichtiger Hinweis zum VS GovNet Connector 3.00:

Dieser sollte nicht mehr verwendet werden, da hier ein altes Signatur Zertifikat verwendet wird, mit dem der Betrieb des VS GovNet Connectors 3.00 ab dem 11.06.2025 verhindert wird.

1. Neue Leistungsmerkmale und Erweiterungen

Keine



2. Verbesserungen / Fehlerbehebungen

Erneuerung des Signatur-Zertifikats

Das Signatur-Zertifikat wurde erneuert, mehr Informationen dazu finden Sie im Administrations-Handbuch unter Installation ==> Update ==> Neue Signatur-Zertifikate

Ausgangssituation: NCP VS GovNet Connector 3.00

Ziel: Einsatz des NCP VS GovNet Connectors in Version 3.01 Revision 28994

Voraussetzung für den Betrieb des NCP VS Connectors in Version 3.01 mit dem NCP Secure Enterprise Management (SEM): Um diese Client-Version zentral verwalten zu können bedarf es der folgenden Komponenten:

- NCP Secure Enterprise Management Server: Version 7.13 oder neuer
- NCP Management Console: Version 7.13 oder neuer
- VS GovNet Connector Configuration Plug-in: Version 3.01 oder neuer
- License Plug-in: Version 14.00 oder neuer
- Firewall Plug-in (optional): Version 13.00 oder neuer
- PKI Enrollment Plug-in (optional): Version 7.10 oder neuer

Schritt-für-Schritt-Anleitung:

- VS GovNet Connector Configuration Plug-in Version 3.01 Revision 31760 einspielen.
- Konfiguration mit dem neuen Plugin signieren.
- Konfiguration exportieren.
- NCP VS Connector in Version 3.00 deinstallieren.
- Neustart der Maschine.
- NCP VS GovNet Connector in Version 3.01 Revision 28994 inklusive neuer Konfiguration installieren.
- Neustart der Maschine.

3. Bekannte Einschränkungen

Kein Konfigurationsupdate bei Anmeldung mit dem Pre-Logon Access Provider (PLAP)

Bei Anmeldung mit dem PLAP wird ein möglicherweise vorhandenes Konfigurationsupdate nicht während der Anmeldung geladen. Das Update erfolgt erst nach der Anmeldung am Windows Desktop und zwar nach dem im Secure Enterprise Management eingestellten Intervall. Als Abhilfe wird empfohlen die Option „Benutzer informieren, wenn er eine neue Konfiguration erhalten hat“ einzustellen.

Fehler „RSA Signature with PKCS#1 V1.5 padding is not allowed by configuration“

Bei einem Verbindungsversuch kann der Fehler „RSA Signature with PKCS#1 V1.5 padding is not allowed by configuration“ auftreten. Dieser Fehler kann insbesondere nach einem Update von älteren Versionen auftreten. In diesem Fall muss über die Konfiguration die 'Padding Standardkonfiguration' geändert werden.

Expertenmodus / Erweiterte IPsec-Optionen

- Erlaube RSA-Authentisierung mit PKCS#1 V1.5 Padding → Deaktiviert
- Erlaube RSA-Authentisierung mit SHA-1 Hash → Deaktiviert

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.

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.

Major-Release: 3.00 r28988
Datum: Februar 2025

Voraussetzungen

Betriebssystem

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 24H2 auf x86-64 Prozessorarchitektur

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 Server: Version 7.13 oder neuer
- NCP Management Console: Version 7.10 oder neuer
- VS GovNet Connector Configuration Plug-in: Version 3.00 oder neuer
- License Plug-in: Version 14.00 oder neuer
- Firewall Plug-in (optional): Version 13.00 oder neuer
- PKI Enrollment Plug-in (optional): Version 7.10 oder neuer

Weitere Voraussetzungen

HotSpot-Anmeldung

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

Abgekündigte Funktionen

IEEE 802.1x-Authentisierung (EAP)

Die Funktion IEEE 802.1x-Authentisierung (EAP) unter dem Menüpunkt „Weitere Optionen/EAP“ steht nicht mehr zur Verfügung.

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.

1. Neue Leistungsmerkmale und Erweiterungen

NCP Pre-Logon

Die NCP Pre-Logon Funktionalität ermöglicht eine Anmeldung an Windows bzw.

Benutzerauthentisierung direkt an einem Active Directory, auch über das Internet. Hierfür wird nach



dem Start des Windows-Rechners, vor der Benutzeranmeldung, die Option zum Aufbau eines VPN-Tunnels zur Verfügung gestellt. Die Auswahl dieser Option geschieht über den NCP Pre-Logon Access Provider (PLAP).

Im Anschluss kann sich der Anwender mittels seines Benutzerzertifikates und der Eingabe der zugehörigen PIN für den VPN-Tunnelaufbau authentisieren. Ab diesem Zeitpunkt ist der Rechner des Anwenders mit dem zentralen Netzwerk verbunden und zentralseitig administrierbar. Die darauffolgende Anmeldung des Benutzers am Windows-System erfolgt zentral, über die Authentisierung an Active Directory.

2. Verbesserungen / Fehlerbehebungen

Registrierung der Client-Firewall in Windows-Sicherheit

Sofern die Firewall des NCP Secure Clients aktiviert ist, konnte dies in Windows-Sicherheit nicht eingesehen werden. Dieses Problem wurde behoben.

Verbindungsprobleme mit 5G-Modems

Bei einigen Endgeräten mit 5G-Modem konnte es zu Verbindungsproblemen mit Mobilfunk kommen, sobald der NCP VS GovNet Connector auf dem Gerät installiert wurde. Dabei wurden mit folgender Hardware Probleme festgestellt:

- Quectel RM520N – GL 5G M.2
- Snapdragon X62-5G (DW5932e)

Dieses Problem wurde behoben.

Wiederherstellung der 5G Konnektivität

Sofern bereits ein älterer NCP VS GovNet Connector mit Version < 3.0 auf einem Windows-Rechner mit integriertem 5G Mobilfunk-Modem installiert wurde, kann mit nachfolgender Vorgehensweise das 5G-Verbindungsproblem behoben werden:

1. Installation des NCP VS GovNet Connectors 3.0 bzw. Update auf 3.0 von einer Vorversion des NCP VS GovNet Connectors.
2. Aufruf des Geräte-Managers *devmgmt.msc* im Administratormodus.
3. Erweitern des Menüs *Netzwerkadapter* und Doppelklick auf das 5G-Modem.
4. In den Modem-Eigenschaften *Erweitert* auswählen.
5. In der Eigenschaftsliste alle nachfolgenden Einträge auf den Wert Rx & Tx Enabled setzen:
 - TCP Checksum Offload (IPv4) / TCP-Prüfsummen abladen (IPv4)
 - TCP Checksum Offload (IPv6) / TCP-Prüfsummen abladen (IPv6)
 - UDP Checksum Offload (IPv4) / UCP-Prüfsummen abladen (IPv4)
 - UDP Checksum Offload (IPv6) / UCP-Prüfsummen abladen (IPv6)
6. Bestätigen des Eigenschaftsdialogs mit *Ok* und Neustart des Rechners.

Meldungen zum Adapterstatus des integrierten WWAN-Moduls

Im Logbuch werden in sekundlichen Abständen Meldungen zum Adapterstatus eines integrierten

WWAN-Moduls angezeigt, wenn als Verbindungsmedium „automatische Medienerkennung“ konfiguriert ist. Dieses Problem wurde behoben.

Problembhebung Softwareupdate über Mobilfunk

Es werden Updates durchgeführt, obwohl Im Updateclient die Option Update über Mobilfunk auf inaktiv gesetzt ist. Das Problem wurde behoben.

Problembhebung: VPN-Dienst unerwartet beendet

Die Microsoft-Sicherheitsupdates für Windows 11 KB5055528 und KB5058411 verursachen eine Fehlersituation im NCP VS GovNet Connector, wodurch sich der „NCP Client VPN und Dialing Service“ unerwartet beendet bzw. die nachfolgende Fehlermeldung erscheint:

„Die Client Software hat ein Problem mit der Treiber-Schnittstelle festgestellt (Mif32init)“

Das Problem wurde behoben.

Fehlerhafte Logeinträge

Es werden fehlerhafte Logeinträge geschrieben, wenn der FND Server nicht verfügbar ist. Das Problem wurde behoben.

Neuer Treiber bzw. Netzwerkadapter

Der Treiber bzw. Netzwerkadapter des NCP VS GovNet Connectors wurde aufgrund eines möglichen Bluescreens angepasst. Dieser Bluescreen trat nach der Installation des NCP VS GovNet Connectors während des darauffolgenden Startvorganges auf. Betroffen waren nur vereinzelte Endgeräte mit der jeweils verwendeten Softwareumgebung.

Infolge dieser Anpassung wurde der Name des Netzwerkadapters geändert von vormals

„NCP Secure Client Virtual NDIS6.20 Adapter“ Version 12.1.2102.0

zu

„NCP Secure Client Virtual NDIS Adapter“ Version 13.1.2501.0

Routentabelle wurde nicht korrekt gesetzt

Waren beide nachfolgenden Bedingungen erfüllt, so wurde die Routing-Tabelle im VS GovNet Connector nicht richtig gesetzt:

- Der Verbindungsaufbau erfolgte über ein Profil mit dem Medientyp Mobilfunk.
- Die Konfiguration des Split Tunneling war nicht Teil der VS GovNet Connector Konfiguration, sondern der Connector bekam die entsprechende Konfiguration via IKEConfig Mode vom VPN-Gateway

Dieses Problem wurde behoben.

3. Bekannte Einschränkungen

Kein Konfigurationsupdate bei Anmeldung mit dem Pre-Logon Access Provider (PLAP)

Bei Anmeldung mit dem PLAP wird ein möglicherweise vorhandenes Konfigurationsupdate nicht während der Anmeldung geladen. Das Update erfolgt erst nach der Anmeldung am Windows Desktop und zwar nach dem im Secure Enterprise Management eingestellten Intervall. Als Abhilfe wird empfohlen die Option „Benutzer informieren, wenn er eine neue Konfiguration erhalten hat“ einzustellen.

Fehler „RSA Signature with PKCS#1 V1.5 padding is not allowed by configuration“

Bei einem Verbindungsversuch kann der Fehler „RSA Signature with PKCS#1 V1.5 padding is not allowed by configuration“ auftreten. Dieser Fehler kann insbesondere nach einem Update von älteren Versionen auftreten. In diesem Fall muss über die Konfiguration die 'Padding Standardkonfiguration' geändert werden.

Expertenmodus / Erweiterte IPsec-Optionen

- Erlaube RSA-Authentisierung mit PKCS#1 V1.5 Padding → Deaktiviert
- Erlaube RSA-Authentisierung mit SHA-1 Hash → Deaktiviert

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.

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.





NCP engineering GmbH
Dombühler Str. 2
90449 Nürnberg
Deutschland

+49 911 9968 0
info@ncp-e.com
www.ncp-e.com

NCP engineering, Inc.
19321 US Highway 19 N, Suite 401
Clearwater, FL 33764
USA

+1 650 316 6273
info@ncp-e.com
www.ncp-e.com