



SecurITy
made
in
Germany
Trust Seal
www.teletrust.de/itsmig

NCP

Release Notes

NCP Secure Enterprise Client

für Linux



Minor-Release: 7.01 r31940
Datum: November 2025

Voraussetzungen

Linux-Betriebssysteme

Die folgenden Linux-Distributionen werden mit diesem Release unterstützt:

- Ubuntu Desktop 22.04 / 24.04, 64 Bit mit Gnome
- Fedora 42 / 43, 64 Bit mit KDE

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 7.10 oder neuer |
| • NCP Management Console: | Version 7.10 oder neuer |
| • Client Configuration Plug-in: | Version 14.00 oder neuer |
| • License Plug-in: | Version 14.01 oder neuer |
| • Firewall Plug-in: | Version 14.00 oder neuer |
| • Endpoint Policy Plug-in: | Version 6.20 oder neuer |

Installation des NCP Secure Enterprise Clients für Linux

Die Installation des NCP Secure Enterprise Clients 7.00 oder neuer unterstützt kein Update einer älteren Version. Sollte eine ältere Version bereits installiert sein, so ist diese vor der Installation des NCP Secure Enterprise Clients zu deinstallieren.

1. Neue Leistungsmerkmale und Erweiterungen

Keine.

2. Verbesserungen / Fehlerbehebungen

Privilege Escalation – NCPVE-2025-1015

Über eine OpenSSL-Konfigurationsdatei, welche mit normalen Benutzerrechten editierbar war, konnte ein kompromittierter Krypto-Provider geladen werden, welcher mit Systemrechten ausgeführt wurde. Ein Angreifer konnte sich dies zunutze machen und auf diesem Wege uneingeschränkten Zugriff auf das System erlangen. Diese Sicherheitslücke wurde geschlossen.

Angriffsszenario auf die Version 7.00 und Gegenmaßnahme (Mitigation)

Hierbei erstellt ein Standard-Benutzer bzw. Angreifer bei Kenntnis des Dateipfades für die OpenSSL-

Konfigurationsdatei, diesen Pfad mit einer manipulierten OpenSSL-Konfigurationsdatei am Zielsystem. Da Aufrufe innerhalb der OpenSSL-Konfigurationsdatei im Systemkontext stattfinden, kann ein Angreifer sich hierdurch systemweit administrative Rechte verschaffen. Voraussetzung für diesen Angriff ist der physische Zugriff auf die Konsole des Systems.

Unter Linux besteht diese Sicherheitslücke ausschließlich für den Fall, dass ein Benutzer namens „builduser“ existiert, der das Verzeichnis „builder“ unter /home/builduser/ anlegen kann. Die Sicherheitslücke kann durch die Vergabe ausschließlicher Leserechte auf dieses Verzeichnis beseitigt werden.

3. Bekannte Einschränkungen

Seamless Roaming wird in dieser Version des Clients nicht unterstützt

FND-Konfiguration mit neuem TLS-basierten Protokoll

In der Vorlagenauswahl des Firewall Plug-ins wird unter „Bekannte Netze“ nicht zwischen Windows- und Linux-Betriebssystem unterschieden. Es ist somit möglich eine Konfiguration mit dem neuen FND-Parameter „TLS-Protokoll“ an einen NCP Secure Enterprise Client für Windows zu verteilen. Der Enterprise Client für Windows unterstützt dieses Protokoll jedoch noch nicht. Konfigurationen mit diesem Parameter können vom Enterprise Client für Windows nicht verarbeitet werden und es kommt zu Fehlern beim Import.

Falscher FND-Status bei manueller Konfiguration

Für den Fall einer manuellen FND-Konfiguration, also basierend auf dem IP-Adressbereich des angeschlossenen Netzwerkes, ist die FND-Statusanzeige u.U. falsch.

Einschränkung bei Endpoint Security

Bedingt durch das OpenSSL Update auf die Version 3.5 wird für die korrekte Funktion der Endpoint Security ein bald verfügbarer NCP Secure Enterprise VPN Server der Version 13.52 oder neuer vorausgesetzt.

4. Hinweise zum NCP Secure Enterprise Client

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 Secure Enterprise Client finden Sie hier:

<https://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/management>

Weitere Unterstützung bei Fragen zum NCP Secure Enterprise Client für Linux, erhalten Sie über die Mail-Adressen auf folgender Seite:

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



Major-Release: 7.00 r31938
Datum: Juli 2025

Voraussetzungen

Linux-Betriebssysteme

Die folgenden Linux-Distributionen werden mit diesem Release unterstützt:

- Ubuntu Desktop 22.04 / 24.04, 64 Bit mit Gnome
- Fedora 41 / 42, 64 Bit mit KDE

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 7.10 oder neuer |
| • NCP Management Console: | Version 7.10 oder neuer |
| • Client Configuration Plug-in: | Version 14.00 oder neuer |
| • License Plug-in: | Version 14.01 oder neuer |
| • Firewall Plug-in: | Version 14.00 oder neuer |
| • PKI Plug-in: | Version 7.10 oder neuer |
| • Endpoint Policy Plug-in: | Version 6.20 oder neuer |

Installation des NCP Secure Enterprise Clients für Linux

Die Installation des NCP Secure Enterprise Clients 7.0 unterstützt kein Update einer älteren Version. Sollte eine ältere Version bereits installiert sein, so ist diese vor der Installation der Version 7.0 zu deinstallieren.

1. Neue Leistungsmerkmale und Erweiterungen

Bindung des NCP Secure Enterprise Clients an den SEM

Mit dem Ausrollen des NCP Secure Enterprise Clients wird im Normalfall auch eine Initialisierungskonfiguration mitgegeben. Diese ermöglicht bei der Inbetriebnahme eine Verbindung zum zentralen SEM und eine anschließende Provisionierung.

Ab diesem Zeitpunkt der Initialisierung ist die Client Software lizenziert und fest an den SEM gebunden.

Ein optionaler Testzeitraum von 30 Tagen kann nur ohne SEM-Bindung vor der Initialisierung genutzt werden. Mit der Lizenzierung wird der Enterprise Client immer genau an das Management-System gebunden, von dem er seine erste Konfiguration erhalten hat.

Die SEM-Bindung stellt ein zusätzliches Sicherheits-Feature dar, da der Enterprise Client nur von „seinem“ SEM eine neue Konfiguration erhalten kann. Nach einem Intervall von 16 Tagen nach dem

letzten Verbindungsaufbau des Clients in das Firmennetz, mithin zum SEM, wird dieser Client in einen Zustand geschaltet, der ihm nur eine Verbindung zum Management-System ins Firmennetz erlaubt, um seine Lizenz aufzufrischen. Dieser Vorgang spielt sich nach Start der VPN-Verbindung innerhalb kürzester Zeit ab, so dass der Client danach wieder in vollem Funktionsumfang genutzt werden kann.

Befindet sich der Client nach Ablauf des 16-Tage-Intervalls in einem nicht funktionsfähigen Zustand, so wird der VPN-Tunnel orange dargestellt. Ist die orangene Tunneldarstellung für den Benutzer sichtbar, so bedeutet dies, dass er statt des aktuell eingestellten Verbindungs-Profiles ein anderes selektieren muss, worüber das Firmennetz bzw. der SEM erreicht werden kann. Erst nach der Lizenzauffrischung wie in obigem Absatz beschrieben, kann der Client auch wieder Gateways erreichen, die sich nicht im Firmennetz befinden.

(In VPN-Umgebungen, in denen der Client den VPN-Tunnel immer ins Firmennetz aufbaut, erfolgt die Lizenzauffrischung in der Regel für den Benutzer unsichtbar.)

VPN-Bypass

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.

Diese Funktion kann unter anderem dazu genutzt werden, um regelmäßig notwendige, nicht sicherheitsrelevante Datenübertragung von der zentralen Infrastruktur fernzuhalten, um deren Performance nicht zu beeinträchtigen. Zum Beispiel könnten Updates des Betriebssystems oder des Virenschanners (mit bekannter Domäne) ohne Umweg über die VPN-Verbindung zugelassen werden oder bei bestimmten Cloud-Services der direkte Zugriff einer Anwendung über das Internet ermöglicht werden. Die Konfiguration erfolgt über die Client-GUI unter „Konfiguration / VPN-Bypass“ und in den Profileinstellungen unter „VPN-Bypass“.

Software Update über LAN

Ist der NCP Secure Enterprise Management Server vom Client über das lokale Netzwerk erreichbar, so kann der Client ein Update der Konfiguration oder der verwendeten Zertifikate erhalten.

Friendly Net Detection

Ab dieser Version 7.00 des NCP Secure Enterprise Clients für Linux wird ein neues, TLS-basiertes FND-Protokoll unterstützt. Dieses Protokoll soll langfristig das bisher bestehende FND-Protokoll ersetzen. Voraussetzung hierfür ist die Verwendung des NCP Friendly Net Detection Servers ab der Version 4.0.

2. Verbesserungen / Fehlerbehebungen

IPsec-Datenkompression wurde entfernt



Ausschließliche Unterstützung des Medientyps LAN

Die in den Vorversionen des Clients angebotene Medienunterstützung für Modem, ISDN und xDSL wurde entfernt. Entsprechend ist die Funktion „Automatische Medienauswahl“ nicht mehr vorhanden. Die Ansteuerung vorhandener WLAN- und Mobilfunkhardware übernimmt das Linux-Betriebssystem.

Update auf OpenSSL 3.5

Erweiterung der Diffie-Hellman Gruppen um 15-21, 25-30

Provisioning innerhalb der Installation

Die Installationsroutine wurde dahingehend erweitert eine Client-Konfiguration, CA- und Benutzerzertifikate mitzuinstallieren.

Die Unterstützung für FIPS inside wurde entfernt

Allgemeine Stabilitäts- und Leistungsverbesserungen

3. Bekannte Einschränkungen

Seamless Roaming wird in dieser Version des Clients nicht unterstützt

FND-Konfiguration mit neuem TLS-basierten Protokoll

In der Vorlagenauswahl des Firewall Plug-ins wird unter „Bekannte Netze“ nicht zwischen Windows- und Linux-Betriebssystem unterschieden. Es ist somit möglich eine Konfiguration mit dem neuen FND-Parameter „TLS-Protokoll“ an einen NCP Secure Enterprise Client für Windows zu verteilen. Der Enterprise Client für Windows unterstützt dieses Protokoll jedoch noch nicht. Konfigurationen mit diesem Parameter können vom Enterprise Client für Windows nicht verarbeitet werden und es kommt zu Fehlern beim Import.

Falscher FND-Status bei manueller Konfiguration

Für den Fall einer manuellen FND-Konfiguration, also basierend auf dem IP-Adressbereich des angeschlossenen Netzwerkes, ist die FND-Statusanzeige u.U. falsch.

Einschränkung bei Endpoint Security

Bedingt durch das OpenSSL Update auf die Version 3.5 wird für die korrekte Funktion der Endpoint Security ein bald verfügbarer NCP Secure Enterprise VPN Server der Version 13.52 oder neuer vorausgesetzt.

4. Hinweise zum NCP Secure Enterprise Client

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 Secure Enterprise Client finden Sie hier:

<https://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/management>

Weitere Unterstützung bei Fragen zum NCP Secure Enterprise Client für Linux, erhalten Sie über die Mail-Adressen auf folgender Seite:

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





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