



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

NCP

Release Notes

NCP Secure Enterprise Management

für Linux



Major-Release: 8.00 r31900
Datum: Juni 2025

Voraussetzungen

Betriebssystem

Die folgenden Linux Distributionen werden mit diesem Release unterstützt:

NCP Secure Enterprise Management Server 8.00

- SUSE Linux Enterprise Server 15
- Red Hat Enterprise Linux 9.5 (x86-64)
- Debian GNU/Linux 11/12 (x86-64)

NCP Management Konsole 8.00

- Windows Server 2025
- Windows Server 2022
- Windows 11

Datenbank

Folgende Betriebssystem/Datenbank-Kombinationen mit zugehörigem Treiber wurden getestet und freigegeben:

Betriebssystem	Datenbank	Treiber
Red Hat Enterprise Linux 9.5	MariaDB 10.5.27	ODBC MariaDB 3.2.5
SUSE Linux Enterprise Server 15 sp5	MariaDB 10.6.14	ODBC MariaDB 3.2.5
Debian GNU/Linux 12.9	MariaDB 11.7.2	ODBC MariaDB 3.2.5
Debian GNU/Linux 11	MariaDB 10.5.15	ODBC MariaDB 3.1.17

Voraussetzung für den Betrieb des NCP Secure Enterprise Management (SEM)

Um diese Management Version nutzen zu können bedarf es der folgenden Komponenten:

- NCP Management Console: Version 8.00 oder neuer
- VS GovNet Connector Configuration Plug-in: Version 2.20 oder neuer
- Client Configuration Plug-in: Version 13.10 oder neuer
- Firewall Plug-in: Version 13.00 oder neuer
- License Plug-in: Version 14.00 oder neuer
- Server Configuration Plug-in: Version 13.40 oder neuer
- Radius-Plug-in: Version 7.10 oder neuer
- PKI Enrollment Plug-in: Version 7.10 oder neuer
- Endpoint Policy Plug-in: Version 6.20 oder neuer
- Script Plug-in: Version 7.10 oder neuer

Voraussetzung für die Nutzung der NCP SEM API mit Python

- Python: Version 3.9 oder neuer

1. Neue Leistungsmerkmale und Erweiterungen

Speicherung der Administrator-Passwörter und OAUTH2 Secrets

Die Speicherung der Administrator-Passwörter und OAUTH2 Secrets ist ab dieser SEM-Version mittels Salted Hash-Verfahren in der Datenbank verfügbar. Die SEM-seitige Migration auf Salted Hash kann nur mit bereits verfügbaren SES und HA-Server Version 13.40 oder neuer erfolgen. Die Umstellung ist irreversibel.

Neue SEM WebUI

Das neue SEM WebUI bietet dem SEM Administrator eine webbasierte Konfigurationsoption. Diese wird sukzessive ausgebaut und bietet in dieser ersten Version die Konfiguration von Tasks und Erstellung von Skripten alternativ zur SEM Konsole. Der Einsatz im Produktivbetrieb wird derzeit noch nicht empfohlen.

Zertifikatsverteilung auf verwaltete SES

Innerhalb des PKI Plug-ins können neue Serverzertifikate zur weiteren Verteilung über das Server Plug-in importiert werden. Dieser Vorgang und die Verteilung an die einzelnen SES kann via REST-API automatisiert werden. Die Verteilung der Serverzertifikate setzt eine SES Version 14.0 oder neuer voraus.

Wartungsmodus

Der neu verfügbare Wartungsmodus dient dem einfachen Service einzelner NCP Secure Enterprise VPN Server im HA-Verbund. Hierfür kann ein einzelner oder mehrere SES in der HA Server-Statusanzeige der Management Konsole auf *inaktiv* geschaltet werden. Neue Verbindungen werden daraufhin von dem betreffenden SES nicht mehr angenommen und er/sie können zu einem beliebigen Zeitpunkt ein Update erhalten. Nach erfolgreichem Update können die SES wieder aktiv geschaltet werden und stehen dem HA-Verbund zur Verfügung. Der Wartungsmodus ist ebenso im SEM-Dashboard sichtbar. Die Skripting-Fähigkeit via REST-API wird in einem späteren SEM-Release nachgereicht.

Für den Wartungsmodus wird ein künftiger SES/HA-Server in der Version 14.0 oder neuer vorausgesetzt.

Lizenzreport via HTTPS versenden

Der Lizenzreport dient dazu die Berechnungsbasis für Lizenzmodelle zu liefern, die auf dem Nutzungsverhalten der NCP-Lösung basieren. Dementsprechend ist der Lizenzreport im SEM zu aktivieren.

Zur Abrechnung seitens NCP kann der Lizenzreport bisher wahlweise manuell oder automatisiert via E-



Mail und einem konfigurierten Mailserver beim Kunden an NCP übergeben werden. Mit dieser SEM-Version 8.0 kommt ein weiterer Weg hinzu: Die Übertragung via HTTPS an den NCP Lizenzserver.

SEM-Tasks in konfigurierbaren Intervallen ausführen

Das automatisierte Starten von SEM-Tasks ist nun flexibler konfigurierbar.

Neue Konfigurationsparameter – Erreichbarkeit externer RADIUS-Server

Das Verhalten im Falle eines nicht erreichbaren, externen RADIUS-Servers lässt sich mit neuen Konfigurationsparametern anpassen. Weitere Informationen hierzu befinden sich im Admin-Handbuch in der Liste der Server-Parameter.

2. Verbesserungen / Fehlerbehebungen

Performanceoptimierung bei Datenbankzugriffen

Zur Verbesserung der Performance bei Datenbankzugriffen wurden Indexe eingeführt.

Unterstützung von Vererbung in der REST-API

Durch die Unterstützung der GroupID wird in der REST-API nun Vererbung unterstützt. Ebenso wird die GroupID nun auch in RADIUS-Vorlagen und der RADIUS-Kommunikation unterstützt.

Problembehebung: Setzen der Parameter `MobileUsername` und `MobilePasswort` funktionierte nicht via REST-API

Problembehebung: `Error 0` beim Erzeugen einer VS GovNet Server-Konfiguration

Erstellung von Python-Skripten mit Umlauten

Bisher wurden Umlaute bei der Erstellung von Python-Skripten über die Konsole nicht unterstützt. Das Problem wurde behoben.

Anzeige des OAUTH Client Secrets

Mit der Aktivierung des Salted Hash-Verfahrens kann das OAUTH Client Secret nur bei dessen Erstellung einmalig angezeigt werden. Die Anzeige wurde um einen entsprechenden Hinweis ergänzt.

Absturz des SEM bei Abholung von Zertifikaten aus der CA

Sofern der SEM Zertifikate aus einer CA importierte und diese Zertifikate keinen Authority Key Identifier (AKID) oder Subject Key Identifier (SKID) enthielten, stürzte der SEM ab. Dieses Problem wurde behoben.

Unterstützung des Message-Authenticator Attributs

Im Falle einer Authentisierung via OTP oder MSCHAPv2 an einem externen RADIUS-Server wird das



Message-Authenticator Attribut gemäß RFC 2869 mit gesendet.

Die maximale Länge des Fallback-Passcodes wird auf 64 Zeichen begrenzt.

SEM-Absturz bei Datumswechsel

Werden beim Datumswechsel Tasks aus der Datenbank gelöscht und die Datenbankverbindung steht in diesem Augenblick nicht zur Verfügung, so konnte in bestimmten Situationen der SEM abstürzen. Dieses Problem wurde behoben.

Client mit REST-API in andere Vorlage schieben

Wurde einem Client via REST-API eine andere Vorlage mit aktivierter Lizenzverteilung zugewiesen, so erschien die Meldung „No license key available“. Dieses Problem wurde behoben.

Aufruf des Dashboards von einem Gruppenadministrator

Der Aufruf des Dashboards durch einen Gruppenadministrator schlug, trotz aller verfügbaren Berechtigungen, fehl. Das Problem wurde behoben.

Dashboard: „Entry already exists“

Wurde ein zweites Benutzer-Dashboard mit einem bereits vorhandenen Namen erzeugt, so wurde innerhalb derselben Session bei jedem Versuch ein Benutzer-Dashboard zu erzeugen die folgende Fehlermeldung ausgegeben: „Entry already exists“

Konsolenanmeldung mit Fehler „Login nicht möglich (SSL Fehler)“

Sofern das SEM-Zertifikat im Windows CSP abgelegt ist, kommt es bei der Konsolen-Anmeldung zu folgendem Fehler: „Login nicht möglich (SSL Fehler)“. Das Problem wurde behoben.

Anlegen eines Clients via REST-API

Wurde über die REST-API ein Client mit vererbter Firewall-Konfiguration angelegt, so erschien eine Fehlermeldung. Dieses Problem wurde behoben.

Allgemeine Stabilitäts- und Leistungsverbesserungen

3. Bekannte Einschränkungen

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.

Anzeige der Audit-Logs im VS GovNet Connector Plug-in aktuell nicht verfügbar

Dashboard: Page Not Found

Beim Wechseln der Ansicht innerhalb des Dashboards auf „Time-Based OTP Benutzer-Anmeldung“ erscheint die Fehlermeldung „Page Not Found“ sofern das Benutzer-Management ausgeschaltet ist.

Fehlerhafte Darstellung des Benutzer-Dashboards

Beim Update von einer NCP SEM Version 6.10 kann es zu einer fehlerhaften Darstellung des Benutzer-Dashboards kommen. Zur Behebung dieses Problems ist der „Content-Security-Policy“-Eintrag in der Datei `admmgm.conf` durch den entsprechenden Eintrag in der Datei `admmgm.sam` zu ersetzen. Beide Dateien befinden sich in folgendem Verzeichnis:

`/opt/ncp/sem/etc/nginx/`

Hier der zu kopierende Eintrag der Datei `admmgm.sam`:

```
add_header Content-Security-Policy "default-src 'self'; script-src 'self'
'unsafe-inline'; style-src 'self' 'unsafe-inline'; object-src 'none';
img-src 'self' www.w3.org/svg/ data: ";
```

Mögliche Privilege Escalation bei der Verwendung von Skripten

Werden NCP- bzw. Python-Skripte über den SEM gestartet, so werden sie mit den gleichen SEM-Berechtigungen ausgeführt. Es wird daher davon abgeraten Benutzer-Administratoren das Anlegen oder Modifizieren von Skripten zu gestatten. Zur Erhöhung der Sicherheit sind nach einem SEM-Update die Berechtigungen der Benutzer-Administratoren zu prüfen und das Anlegen und Modifizieren von Skripten nicht zu gestatten. Bereits vorhandene Skripte sollten überprüft werden.

4. Hinweise zum NCP Secure Enterprise Management Server

Weitere Informationen zum letzten Stand der Entwicklung des NCP Secure Enterprise Management Servers erhalten Sie auf der Website:

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





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