Release Notes

NCP Secure Enterprise Management

for Linux

Major release: 8.10 r31908
Date: October 2025

Prerequisites

Operating System

The following Linux distributions are supported with this release:

NCP Secure Enterprise Management Server 8.10

- SUSE Linux Enterprise Server 15 sp7
- Red Hat Enterprise Linux 9.6/10 (x86-64)
- Debian GNU/Linux 12/13 (x86-64)

NCP Management Console 8.00

- Windows Server 2025
- Windows Server 2022
- Windows 11

Database

The following operating system/database combinations with associated driver have been tested and approved:

Linux distribution	Database	Driver
Red Hat Enterprise Linux 9.6/10	MariaDB 10.11.11	ODBC MariaDB 3.2.6
SUSE Linux Enterprise Server 15 sp7	MariaDB 11.8.2	ODBC MariaDB 3.2.6
Debian GNU/Linux 12/13	MariaDB 11.7.2	ODBC MariaDB 3.2.6

Prerequisites for NCP Secure Enterprise Management (SEM)

The following components are required to use this SEM version:

- NCP Management Console: Version 8.00 or newer
- VS GovNet Connector Configuration Plug-in: Version 2.21 or newer
- Client Configuration Plug-in: Version 13.10 or newer
- Firewall Plug-in: Version 13.00 or newer
- License Plug-in: Version 14.00 or newer
- Server Configuration Plug-in: Version 13.40 or newer
- Radius-Plug-in: Version 7.10 or newer
- PKI Enrollment Plug-in: Version 7.10 or newer
- Endpoint Policy Plug-in: Version 6.20 or newer
- Script Plug-in: Version 7.10 or newer

Prerequisite for using the NCP SEM API with Python

- Python: Version 3.9 or newer

1. New features and enhancements

Compatibility with Ivanti Connect Secure (ICS)

RADIUS communication has been adapted to the ICS gateway with regard to message attribute 80.

2. Improvements / Problems Resolved

Privilege escalation – NCPVE-2025-1015

An OpenSSL configuration file that could be edited with normal user rights could be used to load a compromised crypto provider that was executed with system rights. An attacker could exploit this to gain unrestricted access to the system. This security vulnerability has been closed.

Error when generating configuration for future HA server versions

The generation of a configuration for a future HA server version 14 or GovNet HA server version 3 failed. The error “Wrong license key ...” appeared. This problem has been fixed.

Crash of the SEM

If a parameter list sent from the console to the SEM could not be saved correctly there, a subsequent console login by the same user or another parameter list sent would cause a crash. This problem has been fixed.

3. Known Issues

No differentiation between client plug-in 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.

Dashboard: Page Not Found

When switching the view within the dashboard to "Time-Based OTP User Login", the error message "Page Not Found" appears if user management is disabled.

Incorrect display of the user dashboard

When updating from an NCP SEM version 6.10, an incorrect display of the user dashboard can occur. To fix this problem, replace the "Content-Security-Policy" entry in the `admmgm.conf` file with the corresponding entry in the `admmgm.sam` file. Both files are located in the following directory:

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

Here is the entry of the `admmgm.sam` file to be copied:

```
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: ";
```

Possible privilege escalation when using scripts

If NCP or Python scripts are started via the SEM, they are executed with the same SEM privileges. It is therefore not recommended to allow user administrators to create or modify scripts. To increase security, the permissions of user administrators should be checked after an SEM update and the creation and modification of scripts should not be allowed. Existing scripts should be reviewed.

Major release: 8.00 r31900
Date: June 2025

Prerequisites

Operating System

The following Linux distributions are supported with this release:

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 Console 8.00

- Windows Server 2025
- Windows Server 2022
- Windows 11

Database

The following operating system/database combinations with associated driver have been tested and approved:

Linux distribution	Database	Driver
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

Prerequisites for NCP Secure Enterprise Management (SEM)

The following components are required to use this SEM version:

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

Prerequisite for using the NCP SEM API with Python

- Python: Version 3.9 or newer

1. New features and enhancements

Storage of administrator passwords and OAUTH2 secrets

Starting with this SEM version, administrator passwords and OAUTH2 secrets are stored in the database using a salted hash procedure. Migration to salted hash on the SEM side can only be performed with SES and HA Server version 13.40 or newer. The change is irreversible.

New SEM WebUI

The new SEM WebUI offers the SEM administrator a web-based configuration option. This will be expanded gradually and, in this first version, offers the configuration of tasks and creation of scripts as an alternative to the SEM console. Use in production is not yet recommended.

Certificate distribution to managed SES

Within the PKI plug-in, new server certificates can be imported for further distribution via the server plug-in. This process and distribution to the individual SES can be automated via REST API. Distribution of server certificates requires SES version 14.0 or newer.

Maintenance mode

The newly available maintenance mode is used for easy servicing of individual NCP Secure Enterprise VPN Servers in an HA cluster. To do this, one or more SESs can be set to inactive in the HA server status display of the management console. New connections will then no longer be accepted by the relevant SES and it can be updated at any time. After a successful update, the SES can be switched back to active and are available to the HA cluster. Maintenance mode is also visible in the SEM dashboard. Scripting capability via REST API will be added in a later SEM release.

Maintenance mode requires a future SES/HA server in version 14.0 or later.

Send license report via HTTPS

The license report is used to provide the calculation basis for license models based on the usage behavior of the NCP solution. Accordingly, the license report must be activated in SEM.

For billing by NCP, the license report can currently be transferred to NCP either manually or automatically via email and a configured mail server at the customer's site. With this SEM version 8.0, another option is available: transmission via HTTPS to the NCP license server.

Execute SEM tasks at configurable intervals

The automated start of SEM tasks can now be configured more flexibly.

New configuration parameters – availability of external RADIUS servers

The behavior in the event of an unavailable external RADIUS server can be customized with new configuration parameters. For more information, refer to the list of server parameters in the admin manual.

2. Improvements / Problems Resolved

Performance optimization for database access

Indexes have been introduced to improve performance for database access.

Support for inheritance in the REST API

With support for GroupID, inheritance is now supported in the REST API. GroupID is now also supported in RADIUS templates and RADIUS communication.

Bug fix: Setting the `MobileUsername` and `MobilePassword` parameters did not work via the REST API

Bug fix: `Error 0` when creating a VS GovNet Server configuration

Creation of Python scripts with umlauts

Previously, umlauts were not supported when creating Python scripts via the console. The problem has been fixed.

Display of the OAUTH client secret

With the salted hash method enabled, the OAUTH client secret can only be displayed once when it is created. A corresponding note has been added to the display.

SEM crash when retrieving certificates from the CA

If the SEM imported certificates from a CA and these certificates did not contain an Authority Key Identifier (AKID) or Subject Key Identifier (SKID), the SEM crashed. This problem has been fixed.

Support for the Message Authenticator attribute

In the case of authentication via OTP or MSCHAPv2 on an external RADIUS server, the Message Authenticator attribute is also sent in accordance with RFC 2869.

The maximum length of the fallback passcode is limited to 64 characters.

SEM crash when changing dates

If tasks were deleted from the database when changing dates and the database connection was not

available at that moment, SEM could crash in certain situations. This problem has been fixed.

Move client with REST API to another template

If a client was assigned a different template with license distribution enabled via REST API, the message **"No license key available"** appeared. This issue has been fixed.

Calling the dashboard from a group administrator

Calling the dashboard by a group administrator failed despite all permissions being available. The issue has been fixed.

Dashboard: "Entry already exists"

If a second user dashboard was created with an existing name, the following error message was displayed within the same session each time an attempt was made to create a user dashboard: **"Entry already exists."**

Console login with error "Login not possible (SSL error)"

If the SEM certificate is stored in Windows CSP, the following error occurs when logging in to the console: "Login not possible (SSL error)". The problem has been fixed.

Creating a client via REST API

If a client with inherited firewall configuration was created via the REST API, an error message appeared. This problem has been fixed.

General stability and performance improvements

3. Known Issues

No differentiation between client plug-in 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.

The VS GovNet Connector Plug-in is currently not able to display the VS GovNet Connector's audit logs

Dashboard: Page Not Found

When switching the view within the dashboard to "Time-Based OTP User Login", the error message

"Page Not Found" appears if user management is disabled.

Incorrect display of the user dashboard

When updating from an NCP SEM version 6.10, an incorrect display of the user dashboard can occur. To fix this problem, replace the "Content-Security-Policy" entry in the `admmgm.conf` file with the corresponding entry in the `admmgm.sam` file. Both files are located in the following directory:

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

Here is the entry of the `admmgm.sam` file to be copied:

```
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: ";
```

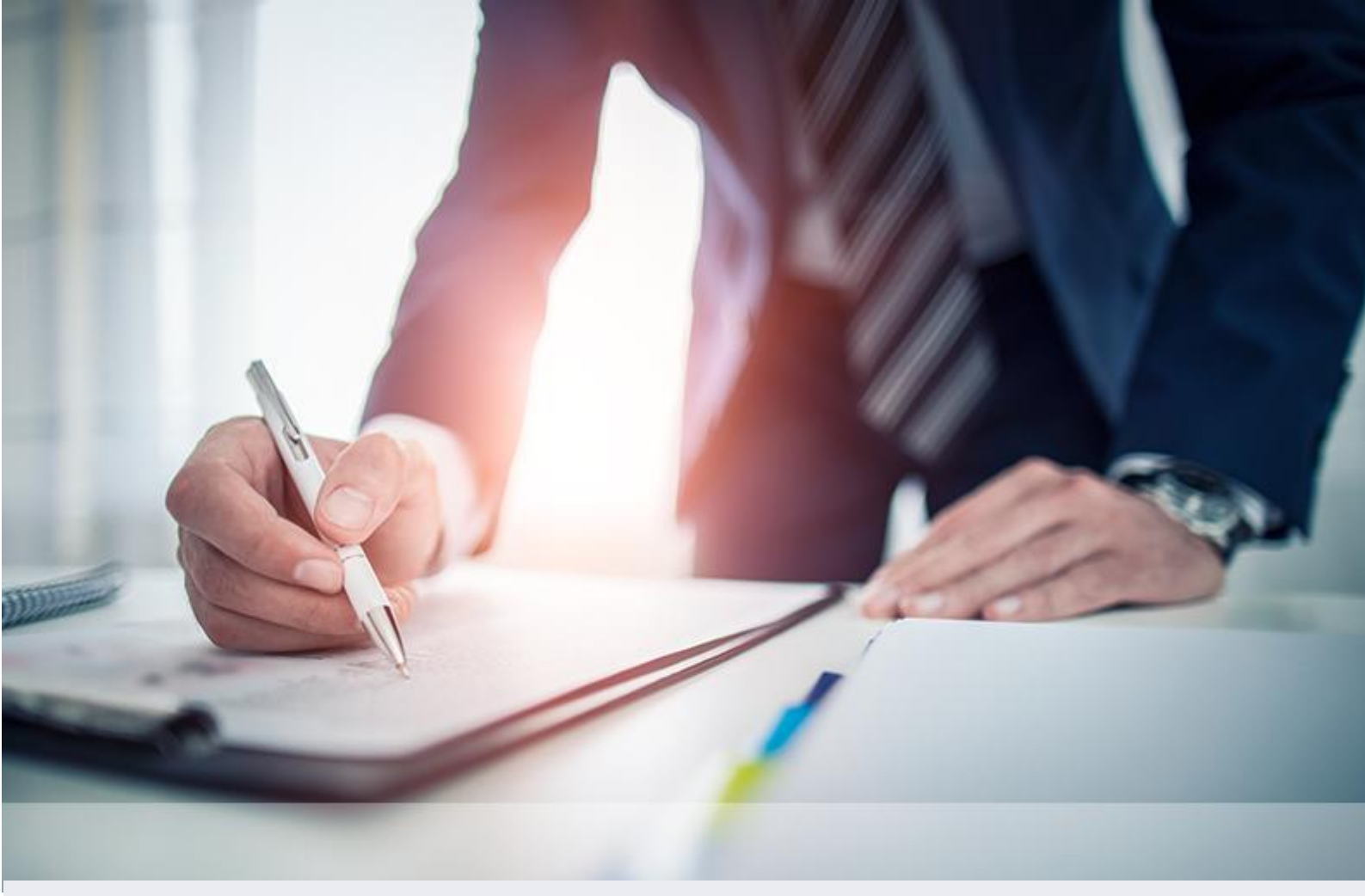
Possible privilege escalation when using scripts

If NCP or Python scripts are started via the SEM, they are executed with the same SEM privileges. It is therefore not recommended to allow user administrators to create or modify scripts. To increase security, the permissions of user administrators should be checked after an SEM update and the creation and modification of scripts should not be allowed. Existing scripts should be reviewed.

4. Getting Help for the NCP Secure Enterprise Management Server

To ensure that you always have the latest information about the NCP Secure Enterprise Management Server, always check the NCP website at:

https://www.ncp-e.com/en/products/centrally-managed-vpn-solution/management/



NCP engineering GmbH
Dombuehler Str. 2
90449 Nuremberg
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