NCP Secure Enterprise Management

for Linux

Release Notes

Major Release: **6.10 r29390**
Date: **March 2022**

Prerequisites

The NCP Secure Enterprise Management (hereinafter “SEM”) is only available as 64 bit software.
The following distributions and databases with the associated Connector/C drivers have been tested with this release:

Linux distribution	Database	Driver
Red Hat Enterprise Linux 8.5	MariaDB 10.4.24	ODBC MariaDB 3.1.6
Debian GNU/Linux 11	MariaDB 10.5.11	ODBC MariaDB 3.1.6
Debian GNU/Linux 10.9	MariaDB 10.3	ODBC MariaDB 3.1.6

Prerequisites for NCP Secure Enterprise Management (SEM)

The following components are required to use this SEM version:

- NCP Management Console: Version 6.10
- VS GovNet Connector Configuration Plug-in: Version 2.10 or newer
- Client Configuration Plug-in: Version 13.00 or newer
- Firewall Plug-in: Version 13.00 or newer
- License Plug-in: Version 13.00 or newer
- Server Configuration Plug-in: Version 12.13 or newer
- Radius-Plug-in: Version 5.30 or newer
- PKI Enrollment Plug-in: Version 4.05 or newer
- Endpoint Policy Plug-in: Version 4.00 or newer
- Script Plug-in: Version 6.10 or newer

Note for the migration from NCP Exclusive Remote Access Management to NCP Secure Enterprise Management Server 6.10

Attention: To ensure an uninterrupted operation, please make sure to have a valid license key for the NCP Secure Enterprise Management Server 6.10 available.

The migration from NCP Exclusive Remote Access Management to NCP Secure Enterprise Management Server 6.10 is supported by the update process. Already installed licenses can still be used after the update/migration. After the update process is complete, make sure to import a valid license for the NCP Secure Enterprise Management Server 6.10 in the management console.

Note for the use of NCP 2-factor authentication

Attention: The use of the NCP 2-factor authentication via TOTP soft token or SMS (Advanced Authentication) is a chargeable option starting with this SEM version for which a separate license key is required.

Note for the automated execution of scripts

The automated execution of scripts, e.g. by actions like "delete user" or "renew certificate", is deprecated as of this SEM version and will not be included in version 6.20.

1. New Features and Enhancements

REST API

The new REST API introduced as of this release enables even better integration of the NCP Secure Enterprise Management Server into the user's IT infrastructure. The following areas can be addressed via REST-API:

- Basic SEM settings
- Client Management
- PKI Management
- RADIUS Management
- Firewall Configuration
- License Management

In principle, the SEM can be addressed via REST by any programming language. To further simplify the use for administrators, NCP offers an NCP Python API for the Python scripting language. This can be installed from pypi.org (Python Package Index) using the command line `pip install NcpSemApi`.

New menu item "Configuration license report

The license report necessary for PayPerUse licensing can be configured by calling the new menu item

"Configuration License Report" and the corresponding mail dispatch can be tested.

Support of the NCP VS GovNet Connector 2.0

From this version of the NCP Secure Enterprise Management Server, the NCP VS GovNet Connector 2.0 is supported in conjunction with the associated plug-in.

Dedicated license for NCP 2-factor authentication according to TOTP or SMS procedure

The use of NCP 2-factor authentication according to TOTP or SMS procedure is chargeable from this version of the NCP Secure Enterprise Management Server and therefore requires its own license.

Support of the audit log in the NCP VS GovNet Connector 2.0

Using the CLI call `rsulog -t auditlog` … the audit log of the NCP VS GovNet Connector can be called up on the NCP Secure Enterprise Management Server.

Enhancement of the NCP script by a login period for RADIUS users

This enhancement of NCP script enables the access of existing RADIUS users to be restricted to defined time windows.

2. Improvements / Problems Resolved

Using TLS 1.2

All TLS communication of the SEM is done with TLS 1.2 from this version on. If the use of TLS 1.0 or 1.1 is necessary for backward compatibility reasons, this can be configured in the configuration file `ncprsu.conf` in the section `[General]` by entering the following parameters:

- `MgmMinTLSVersion` (for console, script, plug-in upload tool, software packages).
- `RsuMinTLSVersion` (update clients)
- `SrvCfgMinTLSVersion` ((v)SES, (v)HAS, Backup Server)

Possible values for these parameters are "1.0", "1.1", "1.2". If these values are not set, TLS version 1.2 applies. The following software versions do not require an adjustment of the TLS version for SEM upload:

- Client SoftwareUpdatePackage as of 11.10
- Client Plug-in as of 11.10 (exception 11.21 r44244)
- Firewall Plug-in as of 12.00
- License plug-in as of 11.10
- RADIUS Plug-in as of 5.10
- Server Plug-in as of 12.10

In general, the plug-in import via .plugin file is not critical with regard to the TLS version. Current servers, HA servers, Windows clients of version 12.x and macOS clients of version 4.x are also uncritical.

New parameters in the account log

The following RADIUS attributes sent from the NCP Secure Enterprise VPN Server (SES) to the SEM are stored in the account log:

- NAS ID (32)
- NAS Port Type (61)
- Client Tunnel Endpoint (67)
- Server Tunnel Endpoint (66)
- Framed IP Address (8)
- Framed Protocol (7)
- Client DNS Name (190)

Extension of the administrator AD Authentication Configuration

Within the administrator group configuration, the search attribute for the authentication of the console administrator in LDAP can now be configured under "AD Authentication". By default "sAMAccountName" is set here for Microsoft Active Directory.

Recursive creation of client configurations

Changed client configurations can now be recursively generated for the clients located in the subgroups by setting the "Including all subgroups" option.

New default values in RADIUS dictionary on new installation

In case of a new installation of the SEM, the parameter names in the RADIUS dictionary are set to NCP default values. In case of an update the parameter names remain unchanged.

Error message "Package not compatible

If a client version for a macOS, Linux, Android client or VS GovNet Connector was set in the client template on the SEM, the "Package not compatible" message was returned. This issue has been fixed.

High CPU load

When a new user was created in SEM, the CPU load increased significantly. This problem has been fixed.

External authentication via Kerberos

External authentication via Kerberos is case insensitive by default, i.e. VPN user names are checked with the Active Directory via Kerberos, regardless of upper or lower case. Using the new RADIUS setting `KrbSendEncTimeStamp=1` introduced in SEM, the check can be switched to case sensitive.

CA certificate import - "Entry could not be inserted"

CA certificates whose Authority Key Identifier (AKID) has a length of 70 bytes could not be imported in

Americas: NCP engineering, Inc. • 601 Cleveland Street, Suite 501-25 • Clearwater, FL 33755 • Phone: +1 (650) 316-6273

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 • www.ncp-e.com

SEM and the error message "Entry could not be inserted" was displayed. This problem has been fixed.

Problem solving when creating a detailed license report

Duplicate RADIUS user

Under certain circumstances a RADIUS user could be created twice. This problem has been fixed.

Replication error or failure of backup SEM

When transferring a large number of users with State=0, a timeout occurred at the Primary SEM. This problem has been fixed.

Missing task ID in output files

The output files `task.out` and `task.err` associated with a created task did not contain a task ID. This problem was fixed.

Display of used iOS client licenses

When deleting an iOS client, the associated device ID was not released, which caused an incorrect display of free iOS client licenses. This issue has been fixed.

Log output "Usage error: tried to wait on non-existent child"

The script-driven sending of the license report generated the log output "Usage error: tried to wait on non-existent child". This problem has been fixed.

Bug fixes when using subscription licensing

When using subscription licensing, problems occurred in connection with a proxy server or displaying the subscription status in the HA server. These issues have been resolved.

Missing group name in log output

When a license was assigned or removed from a user, the associated log output did not include the group name. This problem has been fixed.

Problem solving with usernames and umlauts contained therein

User names containing umlauts and external RADIUS authentication via MS-CHAPv2 could not be authenticated. This problem has been fixed.

Fixed a problem with renaming a VPN bypass list in the plug-in

Problem solved when entering new server and HA server licenses of newer version

Enhancement of the written logs by the name of the management server used

Americas: NCP engineering, Inc. • 601 Cleveland Street, Suite 501-25 • Clearwater, FL 33755 • Phone: +1 (650) 316-6273
Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 • www.ncp-e.com

In order to be able to distinguish in the log entries which management server (primary or backup) created the entries, the name of the management server is added to these entries.

Creation of RADIUS users without a configured password

With this version of the NCP Secure Enterprise Management Server, RADIUS users can be created in the event of external authentication without a password. Until now, a random dummy password was always generated for this. This change is intended to prevent the RADIUS user in question from being able to log in with the dummy password if the external authentication is inadvertently switched off. Users without a configured password are blocked in the event of missing external authentication.

Troubleshooting with certificates whose common name is 63 characters or longer

Error message `... tpb.zip "does not exist! Errno = 2`

In the case of an update of the NCP Secure Enterprise Management Server, an error message with the content `... tpb.zip "does not exist! Errno = 2` could appear. This problem has been fixed.

NCP script `user.createConfig` always provides a positive return value

The NCP script method `createConfig` of the `CUser` class always returned the return value 1, even if the method fails. This problem has been fixed.

Display error in the notification "SEM server certificate will be invalid soon"

Under certain conditions, the notification “SEM Server certificate will be invalid soon” was missing the expiry date of the certificate. This problem has been fixed.

Troubleshooting when saving a Secure Server template

Uninstall the NCP Secure Enterprise Management Server

After uninstalling the NCP Secure Enterprise Management Server, not all log files were removed. This problem has been fixed.

Configuration of the NCP Virtual Secure Enterprise VPN Server

Changes in the configuration of an NCP Virtual Secure Enterprise VPN Server are sent to the gateway but not displayed. This problem has been fixed.

Package and download of the International Phonebook removed

The package and download of the International Phonebook for using an external dialer (iPass) on the client has been removed.

Troubleshooting for RADIUS users with german umlauts in their names

Option "License / used VPN gateways in HA LB mode" in the server plug-in

The option “License / used VPN gateways in HA LB mode” cannot be enabled in the server plug-in. This problem has been fixed.

Advanced authentication with Sophos MCS

The SMS service provider Sophos MCS has been removed from the configuration of the Advanced Authentication because it has discontinued its service.

Troubleshooting within the recovery of the primary management server configuration from failsafe replication using `rsurestore`

New configuration option for the synchronization of subscription licenses via a proxy in the settings of the NCP Secure Enterprise Management Server

Troubleshooting with certificate templates whose name is 63 characters or longer

Troubleshooting with `sem-config` after operating system update

License plug-in only imports license versions that are known to it

Previously, the license plug-in could also be used to import newer license versions than are known to him. However, this led to problems in other areas under certain circumstances. Therefore, from this version onwards, only known license versions can be imported via the license plug-in.

Security update of the OpenLDAP library used to version 2.4.57

The security update to the OpenLDAP library 2.4.57 closes the following security issues in OpenLDAP: CVE-2020-36221 CVE-2020-36222 CVE-2020-36223 CVE-2020-36224 CVE-2020-36225 CVE-2020-36226 CVE-2020-36227 CVE-2020-36228 CVE-2020-36229 CVE-2020-36230

Removing of old logs loaded into the management after creating a new client

After uninstalling and then reinstalling a client, its logs were still available on the central management. This problem has been fixed.

Fixed a XAUTH issue after a RADIUS user has not logged in for more than 8 hours

Optimization of the switchover of the primary management server to a secondary management server

3. Known Issues

The NCP VS GovNet Connector 1.10 is no longer supported

The administration of the NCP VS GovNet Connector 1.10 is no longer supported from this version of the NCP Secure Enterprise Management Server.

It is not possible to differentiate between NCP Secure Enterprise Client and VS GovNet Connector in an administrator group

If an administrator group is created, the entry "Client configuration" is displayed for the client plug-in and the connector plug-in. An individual configuration of these two client entries is not possible.

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

4. Getting Help for the NCP Secure Enterprise Management

To ensure that you always have the latest information about NCP's products, always check the NCP website at:
https://www.ncp-e.com/en/service/
For further assistance with the NCP Secure Enterprise Server, visit:
https://www.ncp-e.com/en/service-resources/support/

Mail: helpdesk@ncp-e.com

5. Features

Central Management

NCP Secure Enterprise Management (SEM) is the central component of the NCP Next Generation Network Access technology. As the Single Point of Administration it provides the transparency required to enable network administrators to centrally manage mobile and stationary workstations, as well as remote VPN gateways (such as those in branch office networks). The NCP software tool provides all functionalities and automation mechanisms that are required for commissioning and operating a remote access infrastructure.

Using SEM, configurations, certificates and software updates are created and updated centrally, stored or distributed and rolled-out.

The Policies for Endpoint Security (Network Access Control) are created centrally at SEM and, dependent on their conformance to the resultant rules, Enterprise Clients are allowed or denied access to the corporate network.

Licensing the Managed Units

The total number of Managed Units to be licensed in a Secure Management Server system is the sum of the number of Client entries. The units forming the central server serving the Configuration Plug-ins (Secure Server and HA Server) do not count towards determining the number of Managed Units to be licensed.

Components of the Secure Enterprise Management

The NCP Secure Enterprise Management (SEM) consists of the Management Server and the Management Console. Database system software is not included the package.

Server Prerequisites

Operating Systems

See Prerequisites on page 1

Computer

CPU min. Pentium III-800 MHz (depending on the number of managed units)

With RADIUS Plug-in: Pentium IV-1,5 GHz

Hard disk: min. 50 MB free disk capacity plus disk capacity for log files and app. 20 MB per software package

Databases Supported

See Prerequisites on page 1

All system relevant information is stored in the database and is usually integrated in the VPN operator's backup process; i.e. user profiles (configurations of the managed units), license keys and authentication data, certificates, provider passwords, etc.

Backup System

A backup option includes the integrated replication services needed by main and backup Management Servers to ensure the continuous availability of management services.

Supported Certification Authorities

Microsoft Certificate Services as integrated or stand-alone CA.

Console Prerequisites

The Management Console is used to centrally manage the VPN user data.

Operating Systems

Windows Desktop operating systems 32 bit or 64 bit

Management Server-Module

The Management Server modules are provided as plug-ins and can be installed as from any Windows computer within the local network by simply entering the IP address of the Management Server using the Management Console. (The database system is not included in the product scope).

Available Plug-ins

- Client Configuration Plug-in
- Firewall Plug-in
- Server Configuration Plug-in (HA Server and Secure Server)
- License Management Plug-in
- PKI Management Plug-in
- Endpoint Policy Plug-in
- Script Plug-in
- RADIUS Plug-in
- System Monitor Plug-in (experimental)
- VS GovNet Connector Configuration Plug-in

RFCs and Drafts supported

- RFC 2138 Remote Authentication Dial In User Service (RADIUS)
- RFC 2139 RADIUS Accounting
- RFC 2433 Microsoft CHAP
- RFC 2759 Microsoft CHAP V2
- RFC 2548 Microsoft Vendor-specific RADIUS Attributes
- RFC 3579 RADIUS Support for Extensible Authentication Protocol (EAP)
- RFC 2716 PPP EAP TLS Authentication Protocol
- RFC 2246 The TLS Protocol
- RFC 2284 PPP Extensible Authentication Protocol (EAP)
- RFC 2716 Certificate Management Protocol
- RFC 2511 Certificate Request Message Format
- Draft-ietf-pkix-cmp-transport-protocols-04.txt, Transport Protocols for CMP
- Draft-ietf-pkix-rfc2511bis-05.txt, Certificate Request Message Format (CRMF)

Core Functionality

Management of Administrators and Multi-Company Support

The Secure Enterprise Management system's multi-company support makes it a natural choice for implementation at Managed Security Service Providers (MSSP) with their "managed VPNs", or in remote access structures, where multiple companies jointly use one VPN platform (VPN sharing).

Using centralized administrator management, access rights can be defined for the administrators of the respective stand-alone companies and their associated VPN users.

Administrator groups mean that the rights of the administrators can be assigned in such a manner that each has exclusive access to only his/her specific company (Organization Group); the chances of infringing on any other organization's data are precluded.

The Secure Enterprise Server, or a server supplied by any manufacturer (see the compatibility list at www.ncp-e.com) can be implemented as VPN gateway. Secure Enterprise Management can thus be integrated within any existing IT infrastructure and it enables operation even in complex VPN environments.00

License Management (License Management Plug-in)

Using License Management, all the managed units are made available to the Management Server. The Managed Units can be either user licenses or remote server licenses. All licenses are managed according to predefined policies:

- Licensing can be handled either automatically or manually

- When no longer required licenses can be returned to the pool
- A warning is given when the license pool is empty

Creating Configurations for the Managed Units

Using the Management Console, user data can be called down or configurations and certificates stored. All relevant information is stored in the database and is normally integrated into the backup process of the VPN operator.

All relevant data can be input either interactively via the Management Console or scripted via the Script Plug-in.

Automatic Update (via LAN or VPN)

The Secure Enterprise Management Update Service enables all software components relevant for a remote access environment to be held centrally. As soon as a connection is established between a Client and the corporate network, these components are copied to the Client. Even if the connection is interrupted during the transfer, the pre-existing software status and configurations are preserved unchanged. Only after a complete, error-free transfer of all pre-defined data does the actual update take place.

- Control of the Update Package
  Software components are distributed according to an Update List, collected together by an administrator and based on certain pre-defined needs. In this way it is possible to differentiate, per component, between communications media, frequency that an update is refused and type of update.
- Update Components
  The following software components can be prepared for automatic update:
  - Configurations (Enterprise Client Profiles and Monitor settings)
  - User Certificates (Soft certificates, p12 format)
  - Issue Certificates (Soft certificates, .cer and .pem format)
  - Update Client
  - Software versions (Software Updates/Upgrades can only be performed on Clients under Windows desktop operating systems)

- Communications Media
  All communications media supported by the remote device can be used for update components. This ensures, for instance, that a fast communications media can be used to transfer large amounts of data.

- Update Process
  As an alternative to updates via VPN, updates can also be performed via LAN. (An NCP Dynamic Personal Firewall can only be updated via LAN). During updates via VPN all data is transferred encrypted through the tunnel. During updates via LAN, when the Client machine is located in a home corporate network, data is transferred using an SSL VPN connection.

Description of the Plug-ins

System Monitor Plug-in (as test software)
This plug-in provides information about all important events within a VPN installation, in bar graphs or line diagrams. The administrator can use the system monitor to call up current status information in real time, or to access previously saved data repositories of the remote access environment. Each graph can be paged backwards or forwards on the time axis. The views of the diagrams can be freely selected.

Client Configuration Plug-in
Using this plug-in, Secure Enterprise Clients profiles can be created, configured and administered, using such facilities as:

- automatic generation of all group specific and connectivity parameters, based on predefined templates
- only personalized data need be entered manually (authentication data for the first connection during the rollout)
- definition of those parameters that will not be alterable by the remote user
- automatic configuration of central component data (RADIUS, LDAP, SNMP) that is referenced in user profiles
- extensive logging (versions, time stamps for configuration changes, automatic upload of client log files)
- creation of a generalized init-user for rollout, and
- automatic creation and provision of configuration updates.

Firewall Plug-in
The Firewall Plug-in is used for configuring the personal firewall of the Secure Enterprise Clients and also for configuring the Dynamic Personal Firewall of the Client Suite. Configuration options include:

- definition of application and connection dependent filter rules
- filter rules can be based on protocols, ports and addresses
- definition of specifications for detection of “friendly networks“ (IP address, network, network mask, IP address of the DHCP server, MAC address)
- definition of logging settings
- FND server configuration (Friendly Net Detection), and

- alterations to firewall settings that will not be alterable by the remote user.

Server Configuration Plug-in

The Server Configuration Plug-in is used for configuring and managing the NCP Secure Servers (Secure Enterprise Server and Secure High Availability Server) in the corporate network. Licensing of the Server components is handled decentralized at the respective machine, via its web interface.
Access rights for those servers and their entire configuration is created and managed at the Management Console.
The Servers' configuration and statistics components of the web interface are replicated one-to-one at the Management Console. When necessary, server configuration via a server's web interface can be temporarily enabled, using controls at the Management Console; however, conflicting configuration changes are inhibited.
Templates can be used to predefine parameters for servers (Server Farm) and for Client user groups.

PKI Enrollment Plug-in

The PKI Enrollment Plug-in functions as Registration Authority (RA) and manages the creation as well as the administration of electronic certificates (X.509 v3) in conjunction with different certification authorities (CA). A generated certificate can optionally be stored as a soft certificate (PKCS#12) or on hardware, e.g. smart card or USB token (PKCS#12). The NCP Demo CA that ships with the product can be used to simulate a PKI during the test phase, however it is not recommended for production operations. Conversion to an external CA is problem-free. The most important functionalities include:

- creation of user and hardware certificates (also bulk mode)
- renewing of certificate validations (PKCS#7)
- revocation of certificates
- distribution of the certificates (also multi client certificates)
- creation of the user configuration via LDAP in the directory service
- creation of a PAC letter (Personal Authentication Code) for initial connection and licensing, and
- generation and distribution of server certificates.

Endpoint Policy Plug-in

Use this plug-in to define all security relevant parameters that must be checked prior to allowing access to the corporate network. Compliance with the specified security policies is mandatory and cannot be bypassed or manipulated by the user. The system can check for the following client parameters:

- Secure Enterprise Client software version
- operating system information, e.g. version or hot fix

- operating system services information
- file information
- state of a virus scanner
- contents of registry values, and
- contents of user and hardware certificates.

Deviations from the pre-defined policies are logged and can trigger different messages or actions, such as:

- display a message at the Client
- output a message to the Client's logbook
- send a message to the Management Server
- send a message to a Syslog server
- release of the relevant firewall rules
- transfer Client to a quarantine zone, and
- disconnect the VPN connection.

RADIUS Plug-in

The RADIUS interface is optionally available for configuration of managed units (users) in the central VPN gateway. This plug-in is used to manage the integrated RADIUS server and it is responsible for the following functions:

- automatic creation of RADIUS accounts via the client and remote server configuration plug-ins
- support of PAP/CHAP requests
- capture of accounting data
- blocking users when repeating incorrect logon attempts
- management of multiple RADIUS configurations of various gateways, and
- RSA authentication manager proxy functionality

Redundancy through backup RADIUS servers is optionally. Existing RADIUS servers can be combined, i.e. they can be replaced in an economical manner.

Americas: NCP engineering, Inc. • 601 Cleveland Street, Suite 501-25 • Clearwater, FL 33755 • Phone: +1 (650) 316-6273

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 • www.ncp-e.com