# NCP Secure Enterprise Management

for Linux

Release Notes

**Service Release:** **5.01 r40724**
**Date:** **August 2018**

## Prerequisites

The following distributions and databases with the associated Connector/C drivers are supported with this release:

| Linux distribution | Database | Driver |
|---|---|---|
| CentOS 7.4 64 Bit | MariaDB 5.5.56 | MySQL libmysqlclient.so.18 Version: 5.5.56-MariaDB |
| Ubuntu Server 16.04.4 LTS 64 Bit | MySQL 5.7.22 | MySQL libmysqlclient.so.18 Version: 5.6.25-MySQL |

The NCP Secure Enterprise Management (hereinafter “SEM”) is only available as 64-bit software. NCP recommends using the tested Connector/C drivers.

For database communication via ODBC the MariaDB ODBC driver 3.0.3 or newer is recommended. In conjunction with a MySQL database the communication with the database cannot use SOCKET mode.

NCP Management Console 5.0 for configuration purposes.

# 1. New Features and Enhancements

None.

# 2. Improvements / Problems Resolved

## Issue with Importing Licenses

Licenses with less than 100 managed units could not be correctly imported into the management interface. Update licenses with the same serial number could also be imported in different groups. These issues have been resolved.

## Backup Management

If plug-ins were deleted in the primary management, e.g. after installing a more recent version of the plug-in, backup management could not be started without errors. This issue has been resolved.

## Problems Entering a License and Using a Backup Management Server

If the backup management server was shutdown, installing new licenses on the primary management server could stop the backup server from functioning. This issue has been resolved.

## Management Service Hangs

If several scripts created or deleted entries in the same table at the same time, this could block communication of the ncprsumain process. This issue has been resolved.

## Incorrect Console Login

When using the native database connection (C-Connector) of MySQL/MariaDB, the error "Incorrect logon" could occur during console logon. The subsequent login was correct. This issue has been resolved.

## Error when Creating Templates with the ISDN Connection Medium

The generation of a template profile with the ISDN Connection Medium generates an error message. This issue has been resolved.

## Unexpected Termination of the RADIUS Service

If the external authentication server (MS Active Directory) cannot be reached during the user logon (e.g. via MC CHAPv2), the RADIUS service was terminated. This issue has been resolved.

## Error when Assigning a MAC Address to the NCP Secure Enterprise VPN Server (SES)

The management application could not assign a MAC address to the SES with certain database code page settings. The error message was: “Eintrag konnte nicht geändert werden" (en: "Entry cannot be modified"). This issue has been resolved.

## Deleting Static Routes Does Not Work

When using MariaDB with the MariaDB C-Connector 3.0.5 static routes could not be deleted in SES. This issue has been resolved.

## No Error Message if DB is Not Connected

If the database is not accessible when the management application is started, the console's connection attempt was rejected but the corresponding error message was not displayed. This issue has been resolved

### RADIUS MSCHAPv2: The Error Message "Password expired" was not Forwarded.

If the external authentication server (MS Active Directory) outputs the error message "Password expired" during the logon phase of a user, this message was not forwarded to the client. This issue has been resolved.

### Incorrect Management Notification "Certificate expired"

The management notification "Certificate expired" was still displayed, although the expired certificate was already deleted.

### Error when using "rsurestore" function

Under certain conditions the “rsurestore” function wasn’t executed correctly at the primary SEM. This issue has been resolved.

## 3. Known Issues

To ensure stable operation, the MariaDB/MySQL database connection should be made via a Connector/C driver. ODBC connections only currently work stably with the MariaDB ODBC driver version 3.0.3 . Using other ODBC driver versions can lead to instabilities.

**Major Release:** **5.00 r39572**
**Date:** **May 2018**

### Prerequisites

The following distributions and databases with the associated Connector/C drivers are supported with this release:

| Linux distribution | Database | Driver |
|---|---|---|
| CentOS 7.4 64 Bit | MariaDB 5.5.56 | MySQL libmysqlclient.so.18 Version: 5.5.56-MariaDB |
| Ubuntu Server 16.04.4 LTS 64 Bit | MySQL 5.7.22 | MySQL libmysqlclient.so.18 Version: 5.6.25-MySQL |

NCP recommends using the tested Connector/C drivers.

For database communication via ODBC the MariaDB ODBC driver 3.0.3 or newer is recommended. In conjunction with a MySQL database the communication with the database cannot use SOCKET mode.

NCP Management Console 5.0 for configuration purposes.

## 4. New Features and Enhancements

### Internal Redesign of the Database Interface

As of SEM 5.0, it is possible to use several database sessions simultaneously. The maximum number can be specified in the configuration file ncprsu.conf. The default value is 10 sessions.
Furthermore, the MySQL or MariaDB database can now also be controlled natively via Connector/C in addition to ODBC. An ODBC driver is not required in this case.

### Optimization of the Integrated RADIUS Server

A thread pool has been implemented in the integrated RADIUS server. If a RADIUS message is received via one of the RADIUS ports, it is buffered in the queue of the thread pool. A free thread then processes the RADIUS message and sends the response to the RADIUS client. The number of threads in the pool can be changed using a configuration parameter. The default value is 8 threads.

**RADIUS Secret for External Authentication**
For external authentication via RADIUS/OTP, a separate RADIUS secret can now be configured. If this secret is empty, the secret of the RADIUS client is used. This functionality requires a RADIUS plug-in version 5.0 or newer.

**EAP**
The type of EAP negotiation to be used is always determined by the server. In this case by the RADIUS server in SEM. For this purpose, the desired EAP protocol options can be enabled in the RADIUS client and in the RADIUS group settings. If several EAP protocols are activated simultaneously in both the RADIUS client and the RADIUS group settings, the EAP type is determined by the following sequence.

- EAP-TLS
- EAP-MSCHAPv2
- EAP-OTP (NCP)
- EAP-MD5

**EAP-OTP (NCP)**
Username and password (in plain text) are transferred between the Secure Enterprise VPN Server and SEM according to a NCP proprietary protocol. However, the EAP type "OTP" is used. It is planned to encrypt credentials with EAP-PEAP or EAP-TTLS in the future. External authentication is possible with all protocols (OTP/RADIUS, LDAP, Kerberos). NCP Advanced Authentication can also be used.

**EAP-MSCHAPv2**
The EAP-MSCHAPv2 implementation is RFC-compliant. External authentication or NCP Advanced Authentication cannot be used.

**Optimized EAP-TLS Communication**

## Plug-in Installation During SEM Installation

If plug-ins have not been installed in SEM yet, the installation of the SEM plug-ins is offered after logging in with the SEM console.

### Notifications

Event notifications for example errors, warnings or information, are displayed via an icon in the console menu. Click on this icon for more details. The color of the icon indicates which the event category

- Red: Error
- Yellow: Warning
- Blue: Info
- Black: No current notifications

### Entering the License Key

As of SEM 5.0, the license key is entered via the console under "Management Server" → "License". Although SEM can now be run without a valid license, the following functions are disabled:

- Software download of the update clients
- RADIUS Server (does not respond)
- SES and HA server administration (connection to SEM is no longer allowed)

The above menu item is only displayed if an admin with the user name "Administrator" is logged into the root group. After entering the license data, SEM no longer needs to be restarted.

### Administrative Access only from Defined IP Networks

Administrators can only log on to SEM from defined IP networks.

## 5. Improvements / Problems Resolved

### SEM Console and SEM Console Plug-in

NCP Secure Enterprise Management 5.0 (SEM) requires NCP Secure Enterprise Management Console 5.0 for configuration. This console can connect to SEM version 5.x or 4.05. Older SEM versions – before 4.05 – require older consoles. The SEM Console plug-in is no longer available as of version 5.0.

### General Logging Improvements

The scopes of the individual logging agents can be changed at runtime via the Management Console 5.0. Menu: "Management Konsole" →"Scopes".

### SEM Certificate Validation

As of version 5.0, the console checks the SEM certificate. If the certificate check returns an error, the administrator is notified and can allow or stop the connection establishment if necessary.

### Start Information

As of SEM 5.0 and console 5.0, the status is displayed in the console during the SEM startup process.

### Scripting with Passwords

Passwords can be stored encrypted in the file ncprsu.conf with the prefix "crypt:". The encrypted passwords can be generated in NCP's Script IDE under Edit / Crypt Password. They can be used in a script accordingly with the prefix "crypt:".

### SEM Settings Dialog – Search for Parameters

A search function has been added to the SEM Settings dialog (menu "Management Server" →"Settings").

### Display ODBC / MySQL Driver Version

In the Info dialog (menu "Management Server" → "Info"), the version of the ODBC/MySQL driver is displayed under Details.

### Changing the Warning Display in the System Monitor Plug-in

The threshold value for displaying a warning regarding the management units used can be set within the Management Server settings in the SystemMonitor group with the parameter MaxMUsWarnValue (value range: 0–100).

### New Button to view the Start Page.

By clicking on this button, the administrator can access the start page as it appears immediately after logging on to the console.

## 6. Known Issues

To ensure stable operation, the MariaDB/MySQL database connection should be made via a Connector/C driver. ODBC connections only currently work stably with the MariaDB ODBC driver version 3.0.3 . Using other ODBC driver versions can lead to instabilities.

# 7. 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/support/

Mail: helpdesk@ncp-e.com

# 8. 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

**64 bit operating systems / Linux distributions / Database / ODBC**

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. The same applies for the Management Console, which may also be installed as a plug-in.

**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)

## 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.



Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Fon +49 911 9968-0 · Fax +49 911 9968-299

**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. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Fon +49 911 9968-0 · Fax +49 911 9968-299