NCP Exclusive Remote Access Management

for Linux

Release Notes

Service Release: **5.30 r46836**
Date: **February 2020**

Prerequisites

The NCP Exclusive Remote Access Management 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 Server 8.1 (x64)	MariaDB 10.3.17	libmysqlclient.so.3 Version 10.4.0
Debian GNU/Linux 9.9 64 Bit	MariaDB 10.3.17	libmysqlclient.so.3 Version 10.4.0

As we do not suggest using the ODBC driver, we recommend using the Connector/C driver in general.

Prerequisites for NCP Exclusive Remote Access Management

The following components are required to use this Exclusive Remote Access Management version:

- NCP Management Console: Version 5.30
- Client Configuration Plug-in: Version 12.01 or newer (if required)
- License Plug-in: Version 12.01 or newer (if required)
- Radius-Plug-in: Version 5.30 or newer

1. New Features and Enhancements

New Two-Factor Authentication according to Time-based One-time Password Procedures

Integration of time-based one-time password authentication for two-factor authentication of the VPN client. A software token such as NCP Authenticator is required to generate the one-time password using the TOTP procedure.
Prerequisite: Client Configuration Plug-in 11.21 or later

Using a web interface provided by NCP Exclusive Remote Access Management, users can create a VPN account in their smartphone app for 2-factor authentication when establishing a VPN tunnel.
The necessary information can be imported via a QR code or by clicking on a link in the smartphone's web browser (the latter if the web interface is accessed directly from the smartphone).
NCP recommends using the NCP Authenticator which is available from the Apple App Store and the Google Play Store:

Erhältlich im App Store

JETZT BEI Google play

After the QR code has been imported successfully and the account has been added to the NCP Authenticator app, the app can be used to generate passcodes in accordance with RFC 6238. In comparison to other authentication apps, NCP authenticator can be configured via NCP management to require authentication on the smartphone via fingerprint or face recognition.
Within the NCP management user configuration end users can access the web interface via a username and password. Access via VPN client, on the other hand is managed by entering the passcode and checking the machine certificate if necessary.

New Configuration Tool for Commissioning

After the installation of the NCP Exclusive Remote Access Management, further steps for commissioning must be performed, such as the connecting to a database or the configuring the operating mode, etc. To simplify this configuration work, the text-based tool sem-config was added to the scope of delivery. The operation of this tool is described in the Linux administration manual, which is also included in the delivery.

Configuration of Password Complexity for Exclusive Remote Access Management Login

In Exclusive Remote Access Management, it is now possible to set the password complexity via the NCP Management Console.

2. Improvements / Problems Resolved

Database Connector for MariaDB Included

The `MariaDB-C connector` is included in the scope of delivery from this version onwards. Potential incompatibilities within the database connection due to problems with connectors are thus avoided.

Extending the Search in the Management Console

In the Management Console search, you can now search for license serial numbers depending on their status (free/reserved/used serial number). An issue in the license detail view which occurred if more than 1000 licenses were issued has now been resolved.

Internal IP Ports can no Longer be Changed in the Console

From with version 5.30, internally used ports can no longer be changed within the Management Console, they are now read only. Changing ports requires restarting the management service.
If it is necessary to change a port, this must be configured in the file `ncprsu.conf` in the `[General]` section.

Issue Resolved in NCP Scripting

The NCP script function `UpdateDest` deleted previous OTP secrets. This issue has been resolved.

Troubleshooting OTP

An issue has been resolved where a user was not deactivated/locked despite exceeding the maximum allowed login attempts. An issue with 2-factor authentication and SMS was also fixed. The RADIUS server did not report a reject if the SMS could not be sent.

Troubleshooting Scheduled Execution of NCP Scripts

An error in the executable file `ncpscriptexe.exe` was fixed, which caused the scheduled execution of an NCP script to stop after a certain time.

Troubleshooting External Authentication with Kerberos

An issue was resolved with external authentication using Kerberos and UPN suffixes.

Error uploading Upload Packages with Subdirectories

If a package uploaded to the Exclusive Remote Access Management contained subdirectories, the upload was terminated with an error message. This issue has been resolved.

Maximum Runtime of Scripts

The maximum runtime of a script depends on the length of the run interval. If the script is set to run on

an hourly interval, the maximum runtime of the script is one hour. For longer run intervals, a script may have a maximum runtime of 23 hours and 59 minutes.

Maximum Number of Incorrect RADIUS Login Attempts

The maximum number of incorrect RADIUS login attempts entered in the RADIUS group settings was ignored. Regardless of the number entered, user accounts were blocked after five incorrect login attempts. This issue has been resolved.

`localhost` does not work for a MySQL configuration

When configuring the database connection, the local host name or the local IP address `127.0.0.1` had to be configured. `localhost` was not resolved correctly. This issue has been resolved.

Replication Service had to be Restarted After Changes to the Backup Server Configuration

When creating or changing the backup server configuration, the replication service had to be restarted. This issue has been resolved. The configuration changes are now applied immediately.

Incorrect CA Certificate Expiry Date Warning

The warning message concerning CA certificate expiry not display the correct date. This issue has been resolved.

Invalid incoming attribute error on RADIUS login

If a RADIUS group configuration was changed with a script, this may have caused an "Invalid incoming attribute" error during RADIUS login. This issue has been resolved.

Error During External RADIUS Authentication

When authenticating via an external RADIUS server, the suffix of the user name was not always removed correctly if the user entered different upper/lower case letters for the suffix. This issue has been resolved.

Troubleshooting Administrator Login

If a new Exclusive Remote Access Management administrator was created within the Active Directory in an OU with umlauts, this administrator could not log in correctly to Exclusive Remote Access Management. This issue has been resolved.

In the Exclusive Remote Access Management settings dialog, the parameters can now be sorted according to the column names.

The default port in the NCP Management Script IDE has now been changed to 12504

Many Log Messages After Incorrect RADIUS Login

If the login to the RADIUS server of the backup Management was made with an incorrect password, a large number of log messages were generated. This issue has been resolved.

RADIUS Service Crashes

Under certain circumstances, the RADIUS service could crash. This issue has been resolved.

Umlauts Display Incorrectly after Management Server Update

When using Connector/C, umlauts were displayed incorrectly in the management console. This problem was solved by configuring the code page in the *ncprsu.conf* file for the "DB" group or "DB-MgmBackup" with "CharSet=...".

SQL Error when Using Oracle database

If the backup Management Server used an Oracle database, an SQL error occurred when the backup management server was started. This issue has been resolved.

Client Session Service Crash

When extending or sending a renewed hardware certificate to the client, the client session service crashed. This issue has been resolved.

Reset Administrator Password

The command `ncprsud -clearadminpw` to reset the administrator password had no effect if the management server was started at the same time. This issue has been resolved.

Management Console Crash

If a large number of users were connected via VPN with RADIUS authentication, the management console crashed when the corresponding link profiles were accessed under statistics. This issue has been resolved.

3. Known Issues

None.

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 Exclusive Remote Access Management (hereinafter "Management") 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

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.

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 Management. This issue has been resolved.

3. Known Issues

None.

4. Getting Help for the NCP Exclusive Remote Access 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 Exclusive Remote Access Management, visit:
https://www.ncp-e.com/en/support/

Mail: helpdesk@ncp-e.com

5. Features

Central Management

NCP Exclusive Remote Access Management (Management) 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 the Exclusive Remote Access Management, configurations, certificates and software updates are created and updated centrally, stored or distributed and rolled-out.

Components of the Exclusive Remote Access Management

The NCP Exclusive Remote Access Management (Management) 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
- License Management Plug-in
- PKI Management 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 Exclusive Remote Access 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.

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 Exclusive Remote Access 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 (Exclusive Remote Access Management 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. 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, Exclusive Remote Access Management 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 Exclusive Remote Access Management 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.

PKI Enrollment Plug-in

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

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.

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.