Data Sheet

NCP Exclusive Remote Access Management

Centrally Managed VPN – Fully Automatic Operation of a Remote Access VPN via a Single Console

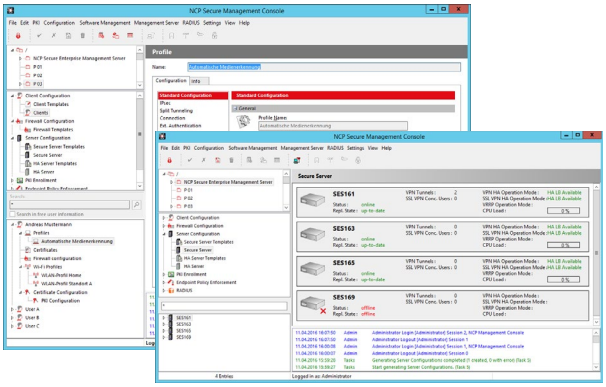
- Administration and license management system for NCP Exclusive Remote Access Clients
- Enables easy rollout and operation of secure remote access infrastructures
- Central creation of client configuration
- Configuration changes on the fly
- Minimal management effort
- Less help-desk calls
- Little training and documentation effort
- Integration into any existing IT infrastructure
- More than 30 years of remote access expertise
- Integrated RADIUS Server

Overview

NCP has been focusing on developing innovative software for more than 30 years. It aims to support companies and authorities with secure remote access which is easy to establish and operate. In this, NCP's Exclusive Remote Access Management is an important component, so to say, the heart of NCP's Next Generation Network Access Technology.

Fully Automatic Operation

NCP's Exclusive Remote Access Management can be connected with the company's existing user management (e.g. Microsoft Active Directory) and request regular updates. As soon as a new employee is listed in this data base the management creates an individual configuration for this user, according to defined templates, enters it at the RADIUS server and, among others, assigns a provider recognition and a software certificate. If a former employee has been removed from the data base, Exclusive Remote Access Management immediately blocks this VPN access.



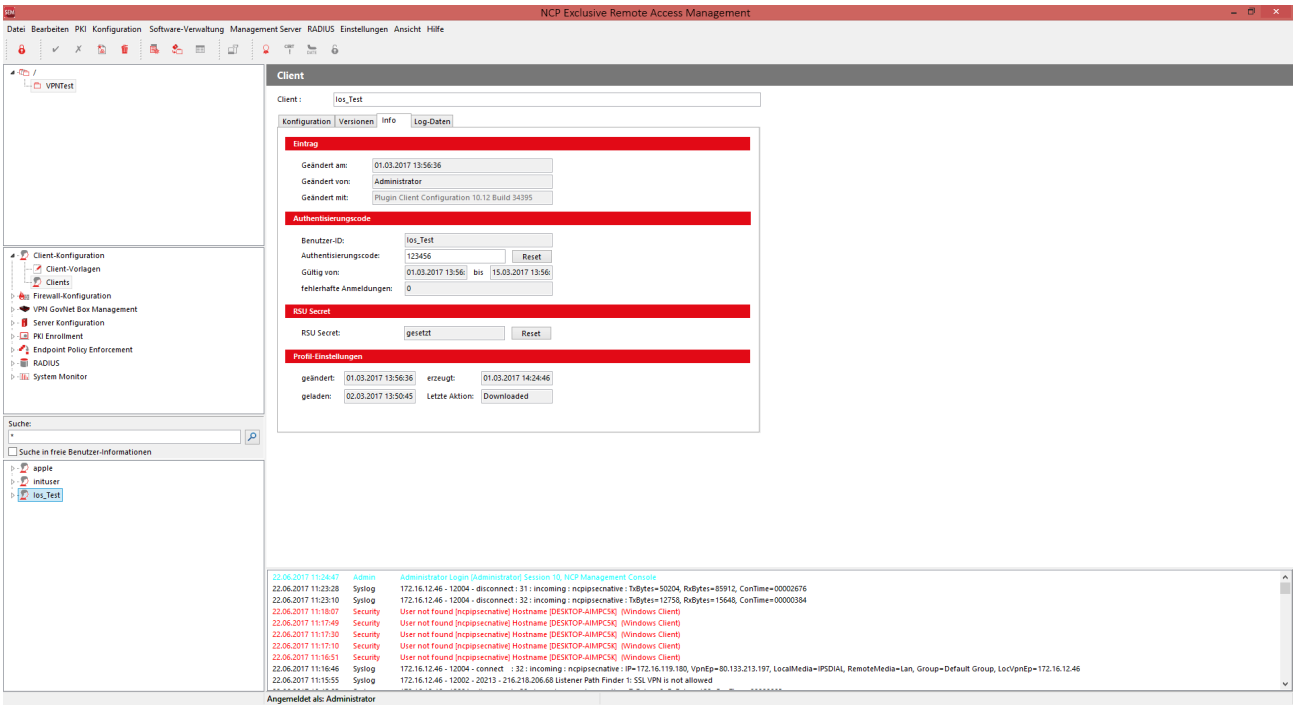
This eliminates the need to manually configure the computers of all mobile employees. Exclusive Remote Access Management also enables fast rollout of a large number of users or software updates.

Components

NCP Exclusive Remote Access Management consists of the Management Server and the Management Console with graphic user interface. The Management Server serves for configuration and management of all connected NCP components. This includes the NCP Exclusive Remote Access Clients. The Management Server is a database-based system and it corresponds with virtually any database via ODBC (e.g. Oracle, MySQL, MS SQL, MS Access, MaxDB). Optionally the Backup Management Server ensures high-availability of the Management Server, which always has the current data repository available through an integrated replication service.

Management Server Plug-ins:

- Client Configuration
- System Monitor
- Client Firewall Configuration
- PKI Enrollment, RADIUS



NCP Exclusive Management Console: Client Configuration

All configuration parameter are stored in the database and usually included into the backup process of the VPN operator. The Management Console can be installed at various administrator work stations, which require a network connection to the Management Server.

Client Configuration Plug-in

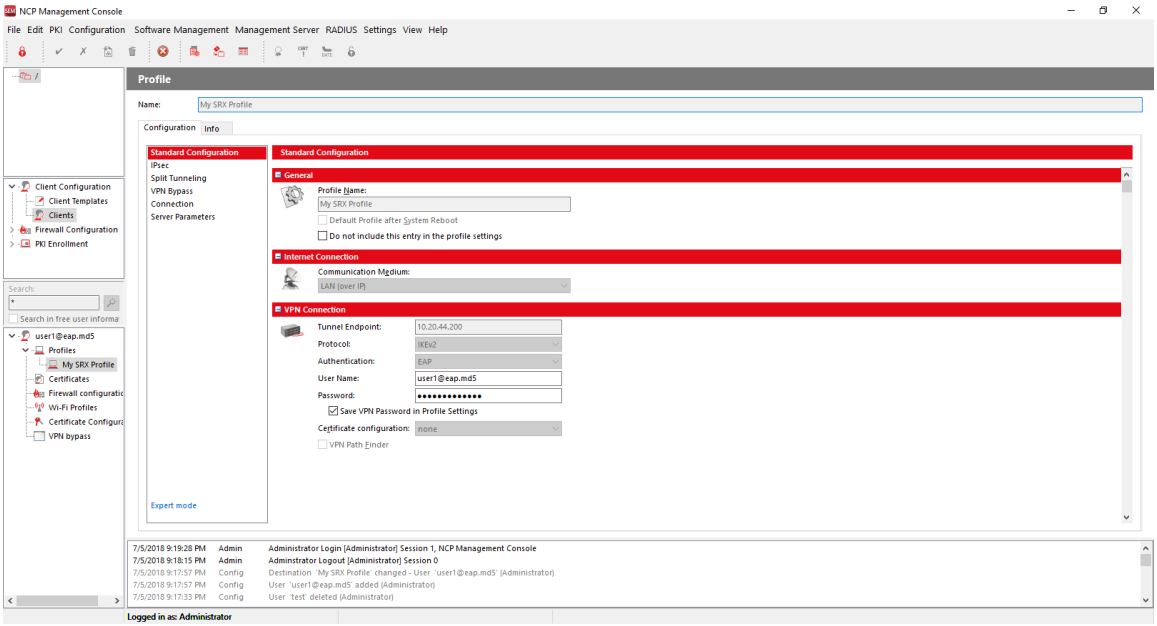
This plug-in enables configuration and administration of NCP Exclusive Remote Access Clients. All relevant parameters are predefined and stored in templates.

Automatic Update Process

The fully automatic update process allows the administrator to centrally provide all remote NCP Exclusive Remote Access Clients with configuration and certificate updates. As soon as the client logs in to the corporate network next, the system automatically installs them on the client.

If malfunctions occur during the transmission, then the previously existing configuration remains unaffected. The software is only updated after complete error-free transmission of all pre-defined files. An encrypted VPN Tunnel secures data transmission. As long as the end device is within the corporate network, the client can be updated without a VPN connection. If a NCP Exclusive Remote Access Client for Windows is used, the administrator can bind the client software update to the communication medium, e.g. only LAN and WLAN (because of smaller bandwidth on 3G/4G).

The NCP Management Console enables interactive input or transfer of all relevant data; alternatively this can be done in a script-driven process. For rollout, for



NCP Secure Management Console: SRX Profile

example, the administrator can automatically transfer user data, license keys, provider passwords, etc. to the Management Server for each remote system (= managed unit).

License Management Plug-in

The licenses of all connected components are centrally stored at the Exclusive Remote Access Management Server. The system transfers them into a license pool and automatically manages them according to specified guidelines. This license transfer might be used for: transfer into a configuration per remote client or Juniper gateway, returning the license to the license pool when an employee leaves a company, or triggering a prompt when no more licenses are available.

System Monitor Plug-in

This plug-in provides fast information in form of bar graphs or line diagrams about all important events within a VPN installation. The administrator can use the system monitor as needed to call up current status information in real time, or to access previously saved data repositories of the remote access environment.

Client Firewall Configuration Plug-in

The NCP Exclusive Remote Access Client software has a centrally managed, integrated Personal Firewall. The Client Firewall Configuration plug-in enables to granularly adjust the firewall rules for each teleworkstation.

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 soft certificate (PKCS#12) or on hardware, e.g. smart card or USB token (PKCS#11). The NCP Demo CA that

ships with the product can be used to simulate a PKI during the test phase, however, it is not intended for productive use. Conversion to an external CA is problem-free.

Parameter Lock

The parameter locks of the NCP Exclusive Remote Access Clients have two main functions: The first is to reduce the complexity of configuration possibilities. This function hides parameter folders for features which are not used, so that the user only sees the settings which are relevant for his working environment. The second function is that pre-settings can be made which the user cannot change. This avoids misconfigurations and undesired connection set ups.

RADIUS Plug-in

This plug-in is used to manage the integrated RADIUS server and to combine existing RADIUS Servers i.e. replace them in an economic way.

Advanced Authentication Add-On

Through this add-on selected users receive a pass code as SMS (text message) on their cell phone. Then they have to additionally enter this pass code during authentication at the client (two-factor authentication). A random generator of the Secure Enterprise Management creates this pass code at each connection setup to the company network. The system then sends the SMS (text message) to the user who, in a first step, has authenticated towards the SEM by entering his VPN access data.

Multi-Tenancy

Multi-company support makes NCP Exclusive Remote Access Management a natural choice for implementation at Managed Security Service Providers (MSSP), in cloud environments, or in remote access structures, where multiple companies jointly use one VPN platform (VPN sharing). This is done by forming groups and using a convenient method of assigning rights. Administrators are created in such a manner that each has exclusive access to his area, in other words to the units that he is responsible for managing. The possibility of encroaching on data of other clients in their protected areas is excluded.

System Requirements	Junos OS 15.1X49-D80 or higher is required
Operating Systems	Management Server: 64 bit: Windows Server 2016, Windows Server 2012 R2 CentOS 7.4, Ubuntu Server 16.04.4 LTS
Managed Units	NCP Exclusive Remote Access Clients
Plug-ins	Automatic Update, Client Firewall Configuration, Client Configuration, License Management, PKI, RADIUS, Script and System Monitor
Advanced Authentication	2-Factor-Authentication via SMS Provider: • NCP Advanced Authentication Connector (for smaller installations) • Sophos MCS (2FA) • Sophos MCS (SMS) • Mobilant • Multitech SMS Server • OpenIT
Multi Company Support	Group capability; Support of max. 256 domain groups (i.e. configuration of: authentication, forwarding, filter groups, IP pools, bandwidth limitation, etc.)
User Administration	LDAP, Novell NDS, MS Active Directory Services
Databases	Windows: • MySQL Server 5.x, Driver MySQL ODBC 5.x • MariaBD 10.2.10, Driver Maria DB ODBC 3.0.x • MS SQL Server 2016, Driver MS SQL Server 10.00.14393.00 • Oracle 11g Express, Driver ODBC InstantClient 12.01.00.02 • Oracle 12c Enterprise, Driver ODBC InstantClient 12.01.00.02 Linux: • MariaDB 5.5.56, Driver MySQL libmysqlclient.so18 Version 5.5.56-MariaDB • MySQL 5.7.22, Driver MySQL libmysqlclient.so18 Version 5.6.25-MySQL
Statistics and Logging	Detailed statistics, logging functionality, sending SYSLOG messages
IF-MAP	The overall aim of the ESUKOM Project is the design and development of a real time security solution for company networks which works on the basis of consolidating meta data. The special focus of the project is the threat resulting from mobile end devices, e.g. smartphones. ESUKOM focuses on the integration of existing security solutions (commercial and open source) which are based on a consistent meta data format according to IF-MAP specifications of the Trusted Computing Group (TCG).

	The IF-MAP server of the Hannover University of Applied Science and Arts can currently be used for free-of-charge testing. The URL is: http://trust.f4.hs-hannover.de/
Client/User Authentication Processes	OTP token, certificates (X.509 v.3): User and hardware certificates (IPsec), user name and password (XAUTH)

Certificates (X.509 v.3)

Revocation Lists	Revocation: EPRL (End-entity Public-key Certificate Revocation List, formerly CRL), CARL (Certification Authority Revocation List, formerly ARL)
Online Check	Automatic downloads of revocation lists from the CA at certain intervals; Online check: Checking certificates via OCSP or OCSP over http
Certification Authorities	Microsoft Certificate Services: as „stand alone CA": as of Windows 2008 R2 Server; As "integrated CA in the domain": as of Windows 2008 R2 (certificate templates cannot be adapted)
Supported RFCs and Drafts	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 2511Certificate 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)

Recommended VPN Clients / Compatibilities

NCP Exclusive Remote Access Clients	Windows, macOS, Android and iOS