Trust Seal
www.teletrust.de/itsmig

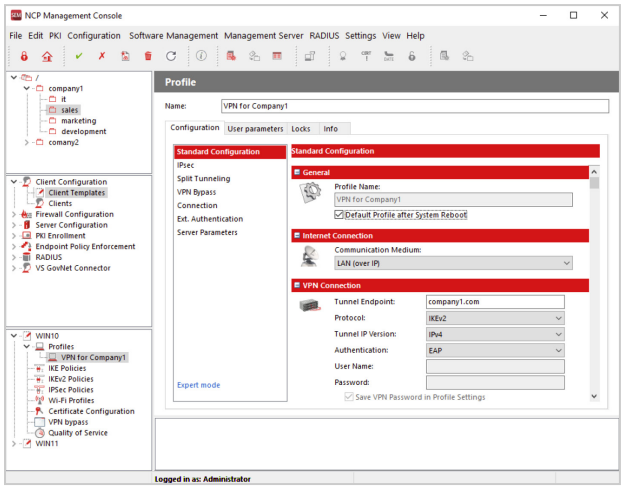
SecurITy made in Germany

Datenblatt

NCP Secure Enterprise Management

Remote Access VPN Management – Vollautomatischer Betrieb eines Remote Access VPN über eine Konsole

- Einfacher Rollout und Betrieb von Remote-Access-Infrastrukturen
- Zentrale Erstellung der Client-Konfigurationen
- Konfigurationsänderungen on-the-fly
- Minimaler Administrationsaufwand
- Reduzieren der Helpdesk-Calls
- Weniger Schulungs- und Dokumentationsaufwand
- Integration in vorhandene IT-Infrastruktur
- Integrierter RADIUS-Server
- Integrierte Zwei Faktor Authentifizierung



Überblick

Seit mehr als 35 Jahren fokussiert sich NCP auf die Entwicklung innovativer Software. Ziel ist es, Unternehmen und Behörden dabei zu unterstützen, auf einfache Weise sichere Remote Access-Umgebungen aufzubauen und zu betreiben. Ein wichtiger Baustein ist hierbei das NCP Secure Enterprise Management (SEM) – die zentrale Komponente der NCP Next Generation Network Access Technology.

Vollautomatisierter Betrieb

Das NCP Secure Enterprise Management kann an die bestehende Benutzerverwaltung im Unternehmen (z.B. Microsoft Active Directory, Microsoft Entra ID) angebunden werden und diese periodisch abfragen. Sobald ein neuer Mitarbeiter in der Datenbank erscheint oder ausgeschieden ist, wird das SEM aktiv. Nach definierten Vorlagen werden dann die individuellen Konfigurationen für diesen User vorgenommen – zum Beispiel die Eintragung in den RADIUS-Server, die Zuweisung einer Providerkennung oder eines Softzertifikats sowie weitere Einstellungen. Bei Ausscheiden des Users wird dessen VPN-Zugang sofort gesperrt. Die Rechner der mobilen Mitarbeiter müssen somit nicht individuell konfiguriert werden.

Der Rollout einer großen Anzahl von Usern oder ein Software-Update ist binnen kürzester Zeit realisierbar.

Komponenten

Das NCP Secure Enterprise Management besteht aus einem Management Server und einer Management Konsole mit grafischer Oberfläche. Der Management Server dient der Konfiguration und Administration aller daran angebundener NCP-Komponenten. Das betrifft sowohl die NCP Secure Enterprise Clients für Windows, macOS, Linux, iOS und Android als auch die NCP Secure Enterprise VPN Server. Es handelt sich um ein datenbankbasiertes System, das mit nahezu jeder Datenbank über ODBC korrespondiert. Für die Hochverfügbarkeit des Management Servers sorgt optional der Backup Management Server, der durch einen integrierten Replikationsdienst immer über den aktuellen Datenbestand verfügt.

Management Server Plug-ins:

- Client Configuration
- Client Firewall Configuration
- Server Configuration
- Network Access Control (NAC), PKI Enrollment, RADIUS

Alle Konfigurationsparameter werden in der Datenbank abgelegt und sind üblicherweise in den Backup-Prozess des VPN-Betreibers eingebunden. Die Installation der Management Konsole kann bei Bedarf an mehreren Administratorarbeitsplätzen erfolgen. Voraussetzung ist eine Netzwerkverbindung zum Management Server.

Client Configuration Plug-in

Dieses Plug-in ermöglicht die Konfiguration und Verwaltung von NCP Secure Enterprise Clients. Alle relevanten Parameter werden vordefiniert und in Vorlagen (Templates) abgelegt.

Automatisches Update-Verfahren

Das automatische Update-Verfahren ermöglicht dem Administrator für alle entfernten NCP Secure Enterprise Clients zentral Konfigurations- und Zertifikats-Updates bereitzustellen. Sobald eine Verbindung zwischen Client und Corporate Network besteht, werden diese Komponenten automatisch auf der Client-Seite eingespielt. Sollte es während der Übertragung zu Störungen kommen, bleibt die bereits vorhandene Konfiguration unberührt. Erst nach einem kompletten, fehlerfreien Transfer aller vordefinierten Daten findet das Update statt. Alle Daten werden verschlüsselt im VPN-Tunnel übertragen. Das Update kann auch ohne VPN-Verbindung durchgeführt werden, sofern sich der Client im heimischen Firmennetz befindet. Im Falle des NCP Secure Enterprise Clients für Windows kann auch ein Softwareupdate des Clients in Abhängigkeit vom aktuell verwendeten Verbindungsmedium durchgeführt werden, z.B. nur im LAN/WLAN (wegen geringer Bandbreiten bei 3G/4G). Die Eingabe und Übernahme aller relevanten Daten kann interaktiv über die NCP Management Konsole oder skriptgesteuert erfolgen. Benutzerdaten, Lizenzkeys, Providerkennungen etc. können beispielsweise bei einem Rollout, automatisiert je remote System (= Managed Unit) in den Management Server übernommen werden. Als VPN-Gateway kann der NCP Secure Enterprise VPN Server oder das VPN-Gateway eines beliebigen Herstellers eingesetzt werden.

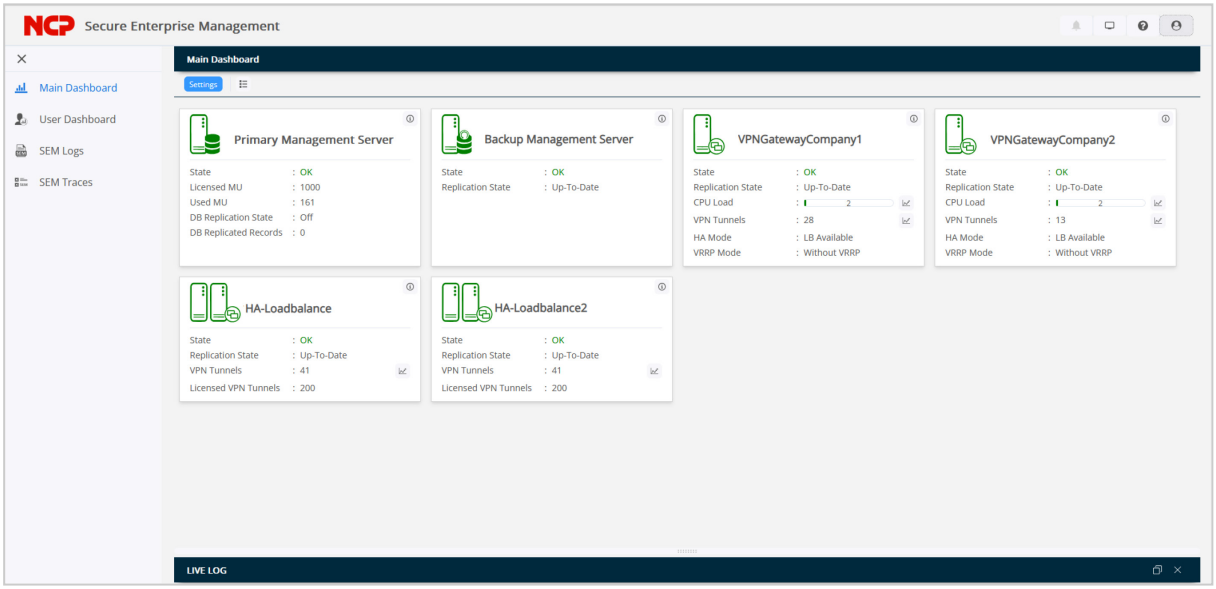
Auch ein Verteilungsmechanismus neuer Firmware für die NCP Secure VPN GovNet Box ist integriert.

Lizenzverwaltung (Plug-in)

Die Lizenzen aller beteiligten Komponenten werden zentral am NCP Secure Enterprise Management Server hinterlegt, in einem Pool übernommen und nach festgelegten Richtlinien automatisiert verwaltet. Funktionsbeispiele hierfür sind die Übernahme in eine Konfiguration pro remote Client bzw. Gateway, die Rücknahme bei Ausscheiden eines Mitarbeiters oder die Meldung für den Fall, dass keine Lizenzen mehr verfügbar sind.

Dashboard

Im Dashboard können via Webbrowser der Status sowie Logs der am SEM angebundenen Komponenten wie Backup SEM, SES und HA Server eingesehen werden.



Client Firewall Configuration Plug-in

Die NCP Secure Client Software verfügt über eine integrierte Personal Firewall, die zentral administrierbar ist. Das Client Firewall Configuration Plug-in ermöglicht eine granulare Einstellung von Firewall-Regeln pro mobilem Device.

Server Configuration Plug-in

Das Server Configuration Plug-in dient der Konfiguration und Verwaltung von Secure Servern (Secure Enterprise VPN Server und Secure High Availability Server) im zentralen Netz. An der Management Konsole werden die Zugriffsrechte für den jeweiligen Server verwaltet und die komplette Konfiguration des Servers erstellt. Zur Konfiguration einer Gruppe von Servern (Server Farm) können Vorlagen genutzt werden, ebenso wie für Client-Benutzergruppen.

PKI Enrollment Plug-in

Das PKI Enrollment Plug-in fungiert als Registration Authority (RA) und managed im Zusammenwirken mit unterschiedlichen Certification Authorities (CA) die Erstellung sowie Verwaltung von elektronischen Zertifikaten (X.509 v3). Ein erzeugtes Zertifikat kann wahlweise als Softzertifikat (PKCS#12) oder auf Hardware z.B. Smart Card oder USB-Token (PKCS#11) abgelegt werden. Die im Lieferumfang enthaltene NCP Demo-CA kann während der Testphase für die Abbildung einer PKI genutzt werden, ist jedoch nicht für den produktiven Einsatz vorgesehen. Die Umstellung auf eine externe CA ist problemlos möglich.

Network Access Control Plug-in (Endpoint Security)

Über das Endpoint Security - auch Network Access Control Plug-in werden alle sicherheitsrelevanten Parameter der Endgeräte vor einem Zugriff auf das Firmennetz überprüft. Dabei kann es sich beispielsweise um den Status von Virenscannern, Dienste-Informationen, Inhalte von Zertifikaten oder Softwarestand handeln. Die Einhaltung der Sicherheitsrichtlinien ist zwingend und vom Anwender nicht manipulierbar. Bei Abweichungen werden Anwender, sofern konfiguriert, in eine Quarantänezone geleitet.

Parametersperre

Die Parametersperre der NCP Secure Clients hat zwei wesentliche Funktionen. Zum einen kann damit die Komplexität der Konfigurations-möglichkeiten reduziert werden. Dabei werden Parameterfelder für nicht benötigte Funktionen ausgeblendet, sodass der Benutzer nur die in seiner Umgebung relevanten Einstellungsmöglichkeiten vorfindet. Zum anderen können Voreinstellungen vorgenommen werden, die für den Benutzer unveränderbar sind. Damit sind eine fehlerhafte Konfiguration durch den User und unerwünschte Verbindungsaufbauten ausgeschlossen.

RADIUS Plug-in

Dieses Plug-in dient der Verwaltung des integrierten RADIUS-Servers. Bereits vorhandene RADIUS-Server können zusammengefasst, d.h. auf wirtschaftliche Art und Weise abgelöst werden.

Mandantenfähigkeit

Der Multi-Company Support (Mandantenfähigkeit) prädestiniert das Secure Enterprise Management für den Einsatz bei Managed Security Service Providern (MSSP) bzw. in Cloud-Umgebungen oder in Remote Access-Strukturen, wo mehrere Firmen gemeinsam eine VPN-Plattform nutzen (VPN Sharing). Dies erfolgt durch Gruppenzuordnung und eine komfortable Rechtevergabe. Die Administratoren werden so angelegt, dass jeder ausschließlich Zugriff auf seinen Bereich, sprich seine zu verwaltenden Einheiten hat. Ein Übergriff auf Daten anderer Mandanten in deren geschützten Bereichen ist ausgeschlossen.

Systemanforderungen

Betriebssysteme Management Server	Windows Server 2025, Windows Server 2022 Red Hat Enterprise Linux 9.5, Debian GNU/Linux 11/12, SLES 15
Managed Units	Secure Enterprise Client ab V 13.00 Secure Android Client ab V 4.30 Secure Enterprise Server ab V 13.00
Plug-ins	Automatic Update, Client Firewall Configuration, Client Configuration, Endpoint Policy Enforcement, Lizenzmanagement, PKI, RADIUS, Server Configuration und Skript
Network Access Control (Endpoint Security)	Endpoint Policy Enforcement für kommende Datenverbindungen. Überprüfung vordefinierter, sicherheitsrelevanter Client-Parameter Maßnahmen bei Soll-/Ist-Abweichungen im IPsec VPN: ▪ Disconnect oder Verbleib in die Quarantänezone mit Handlungsanweisungen (Messagebox) oder Starten externer Anwendungen (z.B. Virenscanner-Update), Protokollierung in Logfiles. Maßnahmen bei Soll-/Ist-Abweichungen im SSL VPN: ▪ Granulare Abstufung der Zugriffsberechtigungen auf bestimmte Applikationen entsprechend vorgegebenen Sicherheitslevels
Mandantenfähigkeit	Gruppenfähigkeit; Unterstützung von max. 256 Domänen-Gruppen (d.h. Konfiguration von: Authentisierung, Weiterleitung, Filtergruppen, IP-Pools, Bandbreitenbegrenzung etc.)
Benutzerverwaltung	LDAP, Novell NDS, MS Active Directory Services
Datenbanken	Windows: • MariaBD 11.7.2, Treiber Maria DB ODBC 3.2.5 • MS SQL Server 2022, Treiber MS SQL Server 10.00.20348 • Oracle 23ai, Treiber ODBC InstantClient 23.05.00247 Linux: • MariaDB 10.5.15, Treiber Maria DB ODBC 3.1.17 • MariaDB 11.7.2, Treiber Maria DB ODBC 3.2.5
Statistik und Logging	Detaillierte Statistik, Logging-Funktionalität, Versenden von SYSLOG-Meldungen

Client/Benutzer Authentifizierungsverfahren	OTP-Token, Zertifikate (X.509 v.3): Benutzer- und Hardwarezertifikate (IPsec), Benutzername und Password (XAUTH)
Zertifikate (X.509 v.3)	
Zertifikate	Es können Zertifikate verwendet werden, die als PKCS#12 Container auf Clients und Server verteilt werden können
Revocation Lists	Revocation: EPRL (End-entity Public-key Certificate Revocation List, vorm. CRL), CARL (Certification Authority Revocation List, vorm. ARL)
Online Check	Automatische Downloads der Sperrlisten einer CA in bestimmten Zeitintervallen; Online-Check: Überprüfung der Zertifikate mittels OCSP oder OCSP over http
Certification Authorities	Microsoft Certificate Services: als „stand-alone CA"; Als "integrierte CA in der Domäne": Zertifikatsvorlagen können angepasst werden
Virenscanner	Unter Windows können alle Virenscanner abgefragt werden, die ihren Status über WMI (Windows Management Instrumentation) oder NAC (Network Admission Control) an das Security Center liefern
Unterstützte RFCs und 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 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)
Empfohlene VPN Clients / Kompatibilitäten	
NCP Secure Enterprise Clients	Windows, macOS, Linux, iOS, Android

NCP engineering GmbH
Dombühler Straße 2
90449 Nürnberg
Germany

+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