Datenblatt

NCP Secure Enterprise Management

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

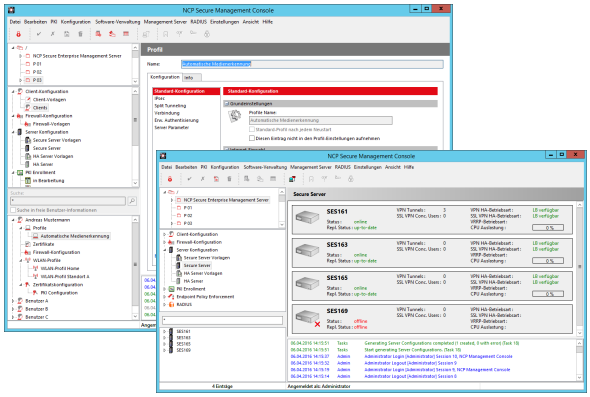
- Einfacher Rollout und Betrieb von Remote-Access-Infrastrukturen
- Zentrale Erstellung der Client-Konfigurationen
- Konfigurationsänderungen on-the-fly
- Minimaler Administrationsaufwand
- Reduzieren der Helpdesk-Calls
- Weniger Schulungs- und Dokumentationsaufwand
- Integration in vorhandene IT-Infrastruktur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

Überblick

Seit mehr als 30 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) angebunden werden und diese periodisch abfragen. Sobald ein neuer Mitarbeiter in der Datenbank erscheint oder ausgeschieden ist, wird das SEM aktiv und erstellt nach definierten Vorlagen die für diesen User individuellen Konfigurationen, trägt ihn im RADIUS-Server ein, weist ihm eine Providerkennung und ein Softzertifikat zu u.v.m. 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, iOS, Android, Linux und CE/Windows Mobile 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.

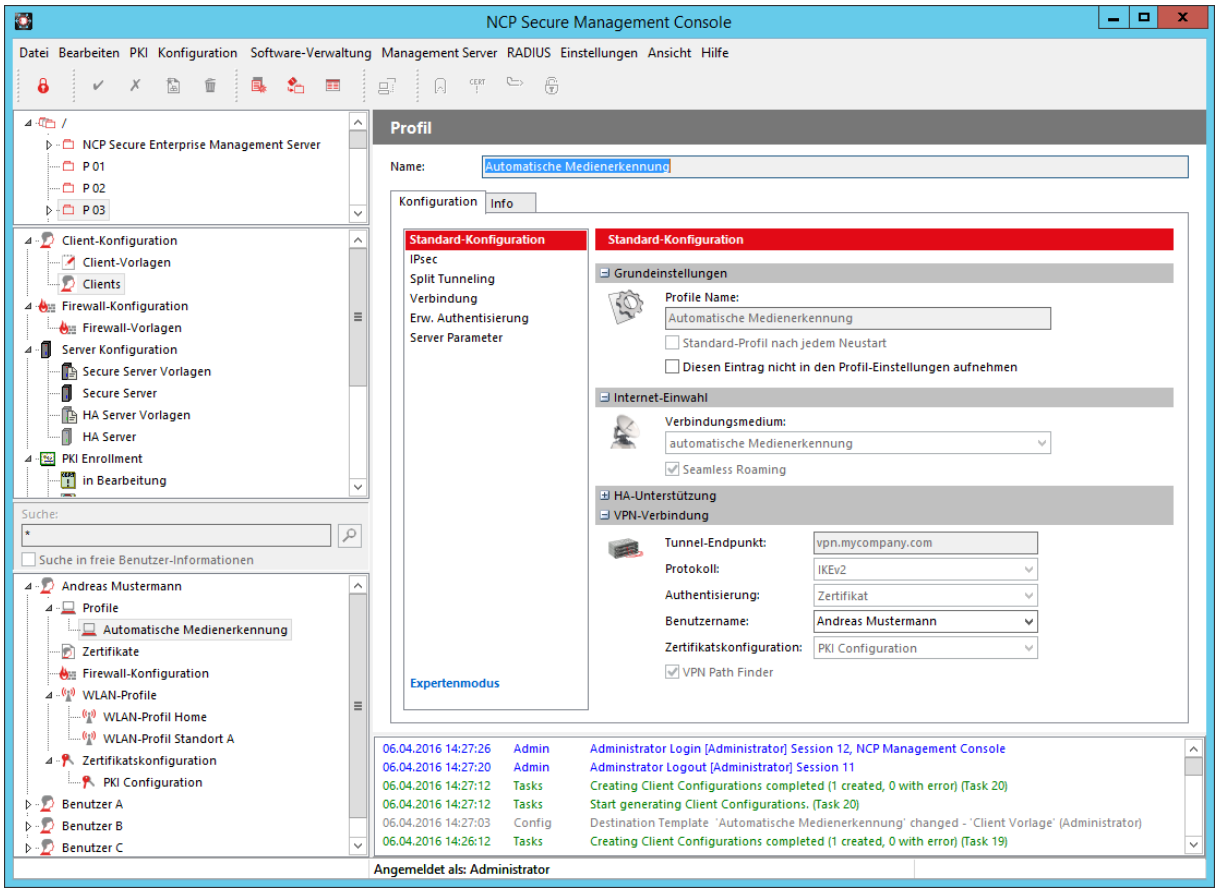
Management Server Plug-ins:

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

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 • V. 4.05
Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com

Datenblatt

NCP Secure Enterprise Management



NCP Client Konfiguration: Zu den Funktionen, die das leistungsstarke Secure Enterprise Management bereitstellt, zählt das zentrale konfigurieren und verwalten von VPN Clients

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 Netzwerk-verbindung zum Management Server.

Client Configuration Plug-in

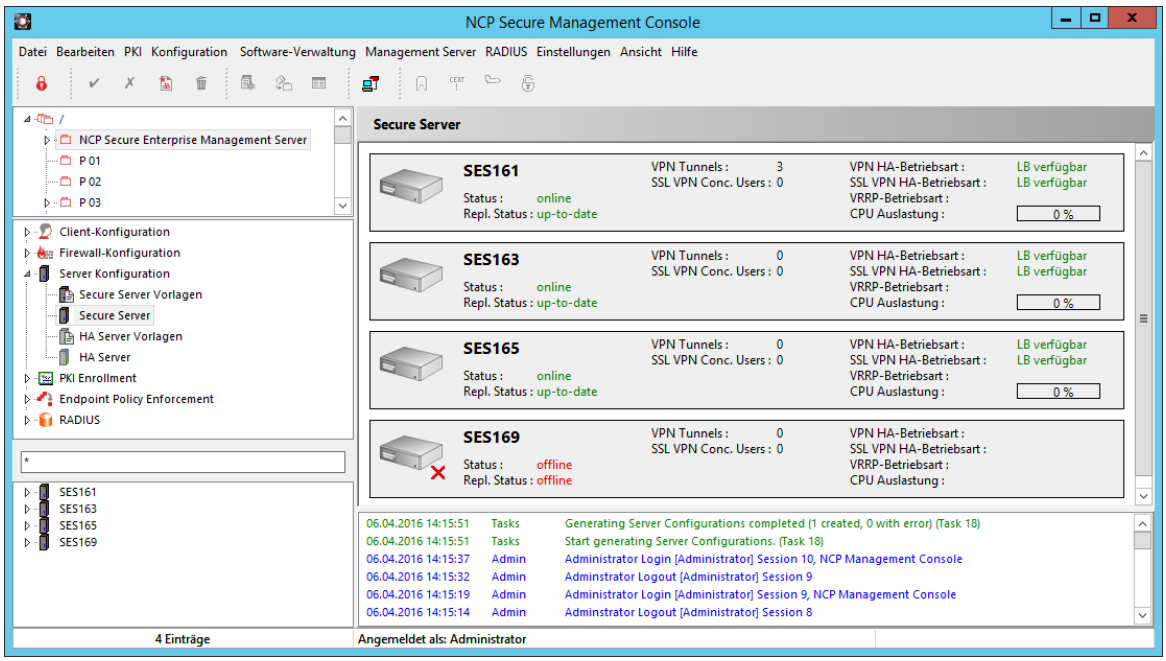
Dieses Plug-in ermöglicht die Konfiguration und Verwaltung von NCP Secure Enterprise Clients. Alle relevanten Parameter werden vordefiniert und in Vorlagen (Templates) abgelegt.

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 über-tragen. Das Update kann auch ohne VPN-

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 • V. 4.05

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com



NCP Secure Management Console: Unabdingbar ist unter dem Aspekt IT-Sicherheit das Monitoring aller wichtigen Ereignisse innerhalb einer VPN-Installation

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. (Siehe Kompatibilitätsliste unter www.ncp-e.com).
Auch ein Verteilungsmechanismus neuer Firmware für die NCP Secure VPN GovNet Box ist integriert.

Lizenzverwaltung (License Management 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.

System Monitor Plug-in

Dieses Plug-in dient der schnellen Information über alle wichtigen Ereignisse innerhalb einer VPN-Installation mittels graphischer Ausgabe als Balken- oder Linien-Diagramme. Der Administrator kann über den System Monitor je nach Bedarf aktuelle Status-Informationen in Echtzeit abrufen bzw. auf bereits gespeicherte Datenbestände der Remote Access-Umgebung zugreifen.

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 • V. 4.05
Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com

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 Firewallregeln pro mobilem Device.

Remote Server und Server Configuration Plug-ins

Mit dem Remote Server Configuration Plug-in werden entfernte Gateways, zum Beispiel in Filialen, als Managed Units lizenziert, konfiguriert und verwaltet. 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). Eine 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 Einstellungs-möglichkeiten 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.

Advanced Authentication Add-on

Durch das Add-on ist es möglich, ausgewählten Benutzern per SMS einen Passcode auf deren Mobiltelefon zu senden, der zusätzlich am Client zur Authentisierung eingeben werden muss (Zwei-Faktor-Authentifizierung). Dieser Passcode wird bei jedem Verbindungsaufbau zum Firmennetz am Secure Enterprise Management mit Zufallsgenerator neu erzeugt und an genau den Anwender per SMS versendet, der sich mittels Eingabe seiner VPN-Zugangsdaten in einem ersten Schritt gegenüber dem SEM authentisiert hat.

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 • V. 4.05
Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com

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.

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 • V. 4.05
Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com

Systemanforderungen

Betriebssysteme Management Server	64-Bit: Windows Server 2012 R2, 2012, 2008 R2 und 2016 Linux Kernel 2.6 ab Version 2.6.16 (Distributionen auf Anfrage)
Managed Units	Secure Enterprise Client ab V 10.0 Secure Android Client ab V 2.32 Secure Enterprise Server ab V 10.0
Plug-ins	Automatic Update, Client Firewall Configuration, Client Configuration, Endpoint Policy Enforcement, Lizenzmanagement, PKI, RADIUS, Remote Server Configuration, Server Configuration, Skript und System Monitor
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 vorgegebener Sicherheitslevels
Advanced Authentication	SEM 3.02 Advanced Authentication Add-on Client Plug-in 10.0 RADIUS Plug-in ab 2.06 Build 4
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	Oracle ab Version 9.0; MySQL; Maria DB, Microsoft SQL Server
Statistik und Logging	Detaillierte Statistik, Logging-Funktionalität, Versenden von SYSLOG-Meldungen
IF-MAP	Das Gesamtziel des ESUKOM Vorhabens ist die Konzeption und Entwicklung einer Echtzeit-Sicherheitslösung für Unternehmensnetze, die basierend auf der Konsolidierung von Metadaten arbeitet. Dabei soll insbesondere der durch mobile Endgeräte wie Smartphones erzeugten Bedrohungslage Rechnung getragen werden. ESUKOM setzt auf die Integration vorhandener Sicherheitslösungen (kommerziell und Open Source) basierend auf einem einheitlichen Metadatenformat gemäß der IF-MAP-Spezifikation der Trusted Computing Group (TCG). Derzeit kann der IF-MAP Server der Fachhochschule Hannover kostenfrei für Tests genutzt werden. Die URL lautet http://trust.f4.hs-hannover.de/

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 • V. 4.05
Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com

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 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)

Empfohlene VPN Clients / Kompatibilitäten

NCP Secure Enterprise Clients	Windows 32/64, macOS, iOS, Android, Windows Mobile/CE, Linux

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 • V. 4.05
Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com