



VPN Management mit neuer 2-Faktor-Authentisierung

NCP Secure Enterprise Management Server in Version 5.30

Nürnberg, 04. Februar 2020 – Der NCP Secure Enterprise Management Server (SEM) ist die zentrale Komponente der NCP Next Generation Network Access Technology und dient als „Single Point of Administration“. Mit ihm können Unternehmen ihr Remote Access-Netzwerk bequem von zentraler Stelle aus administrieren und müssen sich nicht mit einer Vielzahl an Insellösungen beschäftigen. In der neuen Version 5.30 profitieren Administratoren und Anwender von der neuen NCP Authenticator App zur Erzeugung eines Time-based One-time Password (TOTP), einem Web-Interface sowie einem Konfigurationstool unter Linux.

Die neue NCP Authenticator App steht im Apple Store sowie im Google Play Store für Smartphones und Tablets zum kostenlosen Download zur Verfügung. Mit dem NCP Secure Enterprise Management Server kann ein Time-based One-time Password (erzeugt mit NCP Authenticator App) alternativ zur NCP Advanced Authentication (SMS-Versand) als zweiter Faktor benutzt werden. Über den Time-based One-time Password Algorithmus wird ein temporäres Einmalpasswort generiert. Dieses Verfahren sorgt im Rahmen einer Zwei-Faktor-Authentisierung für ein erhöhtes Maß an IT-Sicherheit. Zur Erzeugung des Einmalpasswortes nach dem TOTP-Verfahren ist ein Software-Token wie beispielsweise der neue NCP Authenticator notwendig. Der NCP Authenticator generiert die Passcodes direkt auf dem Smartphone, ohne dass eine Internetverbindung erforderlich ist. Für zusätzliche Sicherheit können vom NCP Management generierte QR-Codes eine biometrische Authentifizierung (Fingerabdruck- oder Gesichtserkennung) zum Starten des NCP Authenticator erzwingen.

Im NCP Secure Enterprise Management Server 5.30 wird die 2-Faktor-Authentisierung durch ein Web-Interface zur Verfügung gestellt. Über dieses Web-Interface ist es Anwendern möglich, in ihrer NCP Authenticator App ein VPN-Konto für die 2-Faktor Authentisierung beim VPN-Tunnelaufbau anzulegen. Der Import der dazu notwendigen Information kann über einen QR-Code oder durch das Klicken auf einen Link im Webbrowser des iOS oder Android Smartphones erfolgen (letzteres sofern das Web-Interface direkt über das Smartphone aufgerufen wird).

Ab Version 5.30 gibt es unter Linux ein textbasiertes Konfigurationstool, welches die Inbetriebnahme des NCP Secure Enterprise Management Servers nach der Installation erleichtert. Es ermöglicht die Konfiguration der Datenbankverbindungen, das Starten und Stoppen von Diensten sowie das Konfigurieren der Betriebsart.



Außerdem wird der MariaDB-Connector mit ausgeliefert, um die Konfiguration der Datenbankanbindung des NCP Managements zu erleichtern.

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 und Linux als auch die NCP Secure Enterprise VPN Server. Der Rollout einer großen Anzahl von Usern oder ein Software-Update ist binnen kürzester Zeit realisierbar.

Über das Endpoint Security/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, Dienstinformationen, 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.

Keywords

NCP, Remote Access Management, VPN Management, Time-based One-time Password, NCP Authenticator App, Sicherheit, 2-Faktor-Authentisierung, Endpoint Security

Weitere Informationen

- NCP Secure Enterprise Management Server
<https://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/management.html>
- NCP Authenticator im App Store
<https://apps.apple.com/de/app/ncp-authenticator/id1483468626>
- NCP Authenticator im Google Play Store
<https://play.google.com/store/apps/details?id=de.ncp.authenticator.totp&hl=de>
- Wenn Sie mehr über NCP engineering erfahren möchten, dann besuchen Sie www.ncp-e.com
- Kontaktieren Sie NCP auch über unseren Blog [VPN Haus](#), über [Twitter](#), [Linkedin](#), [Facebook](#), [Xing](#) oder [YouTube](#)



Über NCP

Die NCP engineering GmbH mit Hauptsitz in Nürnberg vereinfacht den sicheren Zugriff auf zentrale Datennetze via Internet. NCP Produkte und Lösungen erfüllen alle Anforderungen hinsichtlich Benutzerfreundlichkeit, Sicherheit und Wirtschaftlichkeit.

Die Kernkompetenzen liegen auf den Gebieten IP-Routing, zentrales Management von remote Systemen sowie Verschlüsselungs-, VPN- und Firewall-Technologien.

Das Unternehmen entwickelt Software in den Bereichen Mobile Computing, Teleworking, Filialvernetzung, M2M sowie Industrie 4.0 (IIoT). Zum Portfolio gehören auch vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassene Lösungen. Die Technologie der NCP Produkte garantiert die Integration und Kompatibilität mit den Produkten anderer Hersteller. Für die nationale und internationale Vermarktung der Produkte und Lösungen setzt NCP sowohl auf die Zusammenarbeit mit Technologie- und OEM-Partnern als auch auf den Vertrieb über Distributoren und zertifizierte Systemhäuser. Zu den Kunden zählen Unternehmen, Behörden und Organisationen.

Pressekontakt:

NCP engineering GmbH

Oliver Bezold

Telefon: +49 911/99 68-124

Fax: +49 911/99 68-299

E-Mail: oliver.bezold@ncp-e.com

Twitter: [@NCP_engineering](https://twitter.com/NCP_engineering)