

**Contact:**

Caroline Smith  
Springboard Public Relations  
732-863-1900  
[caroline.smith@springboardpr.com](mailto:caroline.smith@springboardpr.com)

**For Immediate Release:****NCP engineering Releases Secure Enterprise Management Server 5.20**

*New VPN Management System Provides Enhanced Security with Time-Based One-Time Password Authentication*

**Sunnyvale, CA (June xx, 2019)** – [NCP engineering](#) today released the Secure Enterprise Management Server 5.20, enabling companies to easily administer their remote access network from a central location. New features include a time-based one-time password (TOTP) for two-factor authentication, configuration of password complexity, and subscription support for the new NCP Virtual Secure Enterprise VPN Server. For greater economic flexibility, the pay-per-use licensing model is also supported.

In Version 5.20 of the NCP Secure Enterprise Management Server, a time-based one-time password can be used as an alternative to the NCP Advanced Authentication (SMS sending) as the second factor. The time-based one-time password algorithm generates a one-time password valid for 30 seconds to ensure a high degree of IT security. To generate the one-time password according to the TOTP method, a software token such as Google Authenticator is necessary. A proprietary software token is currently being developed by NCP.

"The introduction of a time-based one-time password within the new NCP Secure Enterprise Management Server provides companies of all sizes with enhanced security and protection against cyberattacks," said Patrick Oliver Graf, CEO of NCP engineering.

In addition to the time-based one-time password, an administrator also has the option to configure password complexity for local logon via the NCP Management Console.

The NCP Secure Enterprise Management Server now supports the new NCP Virtual Secure Enterprise VPN Server and its subscription licensing. The NCP Virtual Secure Enterprise VPN Server can be integrated into existing enterprise installations with multiple NCP VPN gateways in the load balancing network.

With the pay-per-use licensing model, available for NCP Secure Enterprise Clients and the Secure Enterprise VPN Server, customers only pay for the service they use.

## Resources

- To learn more about the NCP Secure Enterprise Management Server, please see the corresponding product page: <https://www.ncp-e.com/en/products/centrally-managed-vpn-solution/management/>
- To learn more about the NCP Virtual Secure Enterprise VPN Server, please see the corresponding product page: <https://www.ncp-e.com/en/products/centrally-managed-vpn-solution/gateway/>
- Reach NCP engineering on its blog, [VPN Haus](#), or [LinkedIn](#), [Twitter](#), [Facebook](#), [Google+](#) or [YouTube](#).

## About NCP engineering

Since its inception in 1986, NCP engineering has delivered innovative software that allows enterprises to rethink their remote access, and overcome the complexities of creating, managing and maintaining secure network access for staff.

NCP's award-winning product line spans the spectrum of remote access, from IPsec/SSL VPNs to endpoint firewalls and network access control (NAC) functions. The company's products support organizations with complex remote user needs, and that want to leverage the latest end-devices to increase staff productivity, reduce network administration and adapt policy changes on-the-fly. Each solution is interoperable with existing third-party software or hardware.

With global headquarters in Nuremberg, Germany and North American headquarters in the San Francisco Bay Area, the company serves 35,000-plus customers worldwide throughout the healthcare, financial, education and government markets, as well as many Fortune 500 companies. NCP has established a network of national and regional technology, channel and OEM partners to serve its customers. For more information, visit [www.ncp-e.com](http://www.ncp-e.com).

###