Secur|Ty
made in Germany
Trust Seal
www.teletrust.de/itsmig

NCP
SECURE COMMUNICATIONS

Product Information

Enterprise features that make a difference

Key Features in the NCP Enterprise VPN Solution

NCP has over 30 years of experience in developing highly secure remote access solutions. Classical VPN focuses on site-to-site networking and connecting up to several thousand end users to the company network – via various connection media and authentication methods.

When it comes to VPN, there are big differences between simple clients and professional business solutions with centralized management. Here are some of the most important features in NCP's solution:

- ✔ Integrated personal firewall (Friendly Net Detection, secure Hotspot Logon and Home Zone)
- ✔ Endpoint security
- ✔ System independence
- ✔ Seamless roaming
- ✔ NCP VPN Path Finder technology
- ✔ Quality of Service (QoS)
- ✔ Strong authentication (e.g. biometric features fingerprint or facial recognition)
- ✔ Windows Pre-Logon
- ✔ IPv4 / IPv6 dual stack support

Several features meet the requirements of zero-trust concepts. This allows companies to easily integrate NCP VPN solutions into their infrastructure according to zero-trust principles and benefit from features such as universal access management, extensive authentication options and centralized updates.

Integrated Personal Firewall

The integrated personal firewall in NCP Secure Enterprise Clients provides an additional layer of security, helping users to maintain secure communications from remote locations without the hassle of configuring software themselves. At the same time, this also avoids configuration problems caused by users and reduces the burden on IT support teams.

In contrast to third-party products, the NCP firewall can adapt to the client's network environment through Friendly Net Detection.
This technology adapts firewall rules automatically and connects or disconnects the VPN tunnel accordingly, depending on whether a device is connected to a public network or a trusted network.

+ Additional security
+ Reduces burden on IT support

Friendly Net Detection

Automatic adaptation of firewall rules in trusted networks or public networks

Hotspot Logon

When connecting to a public hotspot, users often have to register and log on through the hotspot provider's website, which bypasses the VPN tunnel and is usually not permitted in the business environment. Requiring the user to disable the firewall when connecting to a hotspot is an extremely poor solution.
The Hotspot Logon feature in the NCP Secure Client addresses this problem.

Users no longer have to connect to the hotspot provider over an unsecure connection, instead the NCP client launches a secure web browser for the hotspot logon process.

+ **Enhanced security**
+ **Easy to use**

Secure Hotspot Logon

Connect easily and securely to public hotspots without having to lower security settings.

Home Zone

As many organizations require all communications for remote workers to be routed through the VPN tunnel, users are often left without being able to access devices on their home network, e.g. printers.

The firewall in the NCP client can be configured to allow users to access local network devices such as printers in their home office.
At the same time, Internet access is transferred securely through the VPN tunnel.
In this configuration, the user's local network is assigned to the Home Zone which has a separate set of firewall rules.

+ **Easy to use**

Home Zone

Use local network devices such as printers or scanners in the home office with this user-friendly firewall feature.

Endpoint Security

Before accessing the company network, all security-relevant parameters are checked by the NCP Secure Client. This includes the status of virus scanners, services, certificates or software updates on the end device.

Compliance with the security policies is enforced and cannot be manipulated by the user.
If a problem is detected, access to the network will be denied or users will only have access to a quarantine zone to update their system.

+ Minimizes security risks

Endpoint Security

Security-relevant parameters (virus scanners, certificates, software updates) are automatically checked before the user can access the network.

Compatibility with Existing Infrastructure

The NCP solution can be integrated into any existing infrastructure and is compatible with all major firewall manufacturers (e.g. Cisco, Juniper, etc.).
This protects investments by ensuring compatibility with future changes to IT infrastructure and environments.

NCP clients are available for all common end devices such as notebooks, smartphones and tablets running Microsoft Windows, macOS, Linux, iOS and Android. An intuitive interface which is similar on all operating systems ensures a high level of user acceptance.

+ Safe investment

System independence

The universal NCP clients are available for all common notebooks, smartphones and tablets with Windows, macOS, Linux or Android.

Seamless Roaming

While users are working remotely, they often need to connect via Wi-Fi and 3G/4G/5G depending on network availability. Ensuring that users are not interrupted and can work seamlessly while the connection switches over is an important requirement for an effective VPN design that secures communications without restricting users.

The NCP VPN client changes the connection medium and redirects the VPN tunnel dynamically without interrupting the user's session. This feature requires a current version of the NCP Secure Enterprise VPN Server. Thanks to Seamless Roaming, the constant availability of applications is ensured for remote users.

+ Easy to use

Seamless Roaming

The VPN client automatically switches between Wi-Fi and 3G/4G as needed, guaranteeing uninterrupted work.

Patented NCP VPN Path Finder technology

Restrictions on the use of IPsec VPN services make it more and more difficult for business travelers to access their company network and work remotely.

VPN Path Finder technology enables secure external network access even in IPsec-hostile environments behind firewalls whose settings prevent IPsec-based traffic.

+ Enhanced security
+ Easy to use

Path Finder technology

VPN in IPsec hostile environments, even if connections are blocked by the firewall.

Strong Authentication

For maximum security, NCP clients support various authentication methods, including biometric features such as fingerprint or facial recognition. On Apple devices, Face ID and Touch ID are supported.

Multi-factor Authentication is also supported through the integrated Advanced Authentication, OTP token (One Time Password) and digital certificates in a public key infrastructure (PKI).

+ **Enhanced security**
+ **Easy to use**

Biometric Authentication

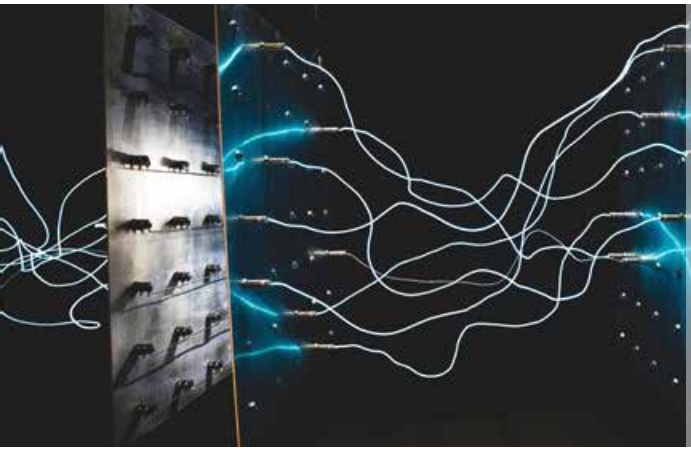
For strong authentication, the clients also support biometric authentication, for example by fingerprint recognition.

Quality of Service (QoS)

The Quality of Service (QoS) module in the NCP Secure Client for Microsoft Windows provides the ability to assign a guaranteed outgoing bandwidth to specific applications in the VPN tunnel. This can be especially useful in the home office with low upload bandwidth.

It prevents delays or interruptions, for example for improved voice quality in VoIP telephony or smooth streaming of audio and video data in applications and services such as Skype and YouTube.

+ **Enhanced security**
+ **Easy to use**



Quality of Service (QoS)

VoIP or Skype without interruptions due to guaranteed outgoing bandwidth in the VPN tunnel

Windows Pre-logon

Thanks to the Windows Pre-Logon features, users can connect to the company VPN before logging on to their local Windows system.

The user logs on through the VPN tunnel and is authenticated in the Windows domain or in the Active Directory.

+ **Enhanced security**
+ **Easy to use**

Windows Pre-logon

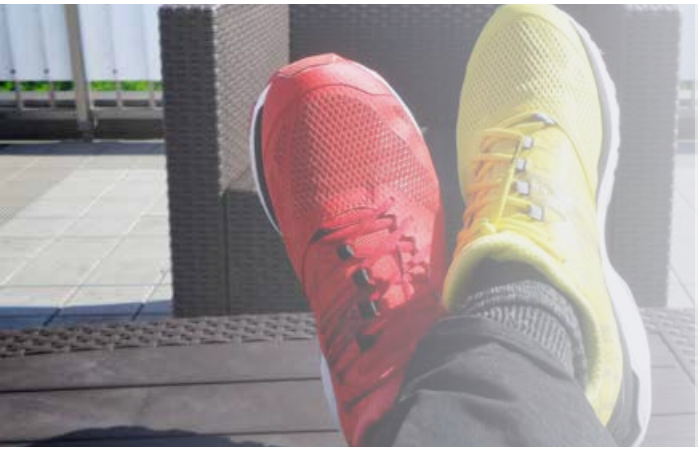
Secure login to the Windows domain through the VPN connection which has already been established to the company network.

IPv4 / IPv6 Dual Stack Support

All NCP products are fully IPv6-compatible, which is future-proof for later developments in network infrastructure. NCP VPN clients and servers are designed to support IPv4 or IPv6 communication and both protocols in dual-stack operation.

This supports scenarios when IPv6 addresses are used in the public network and IPv4 continues to be used in the internal company network or when the protocols are used simultaneously in both public and private networks.

+ **Enhanced security**
+ **Simplifies network administration**



IPv6 Dual Stack Support

NCP client and server software supports IPv4 and/or IPv6 communication and dual stack operation.

	Microsoft Windows	macOS*	iOS	Android	Linux
Personal Firewall	✔	✔			✔
Friendly Net Detection	✔	✔			✔
Hotspot Logon	✔				
Home Zone	✔				
Endpoint Security	✔	✔			✔
Seamless Roaming	✔				
Path Finder technology	✔	✔	✔	✔	✔
Biometric Authentication	✔	✔	✔	✔	
QoS	✔				
Windows Pre-logon	✔				
IPv4/IPv6 Dual Stack	✔	✔	✔	✔ *(planned)*	

**Personal Firewall and Friendly Net Detection are included in macOS clients from version 4.0 up to version 4.5*

NCP SECURE COMMUNICATIONS

Do you have any questions or would you like to make an appointment for a product demonstration? Please connect with us.

The Americas

NCP engineering, Inc.

19321 US Highway N, Suite 401
Clearwater, FL 33764
USA

+1 650 316-6273

sales@ncp-e.com
www.ncp-e.com

Europe, Asia and Pacific

NCP engineering GmbH

Dombuehler Str. 2
90449 Nuremberg
Germany

+49 911 9968-333

sales@ncp-e.com
www.ncp-e.com

We look forward to discussing how we can help you.