NCP Friendly Net Detection Server

for Windows

Release Notes

Major release: **3.00 r47008**
Date: **March 2020**

Prerequisites

Microsoft Operating Systems:

The following Microsoft Operating Systems are supported with this release:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

1. New Features and Enhancements

Certificate-Based Authentication of the Friendly Net Detection Server with TLS 1.2

The authentication of the FND server on the NCP Secure Client supports from this version both TLS 1.2 or TLS 1.0 if an older NCP Secure Client is used.

2. Improvements / Problems Resolved

Incompatibility with Microsoft Update KB4074598

After installing the Microsoft Update KB4074598, the NCP Friendly Net Detection Server did not function correctly. This issue has been resolved.

Password and PIN are now Encrypted in the Configuration File

When the NCP Friendly Net Detection Server is started, previously unencrypted user passwords contained in the configuration file and the certificate PIN are now encrypted.

The demo certificates have been updated

3. Known Issues

None.

4. Getting Help for the NCP Friendly Net Detection Server

To ensure that you always have the latest information about NCP's products, always check the NCP website at:
https://www.ncp-e.com/en/solutions/vpn/remote-access-vpn-technologies/friendly-net-detection/

You can find a list of open source components used in this product in the accompanying document (OpenSourceLicenseTerms.pdf).

5. Features of the NCP Friendly Net Detection Server

With the help of Friendly Net Detection (FND) technology, the NCP Secure Client is able to automatically detect a trustworthy, "friendly" network. As a result, the rules of the firewall of the NCP Secure Client can automatically adapt. For example, preconfigured access to the user's computer can be automatically activated in the "friendly" company network, whereas the computer is shielded from external access in unknown network environments.

Friendly Net Detection is a classic client / server application that can be centrally administered:

- The Friendly Net Detection server (FNDS) is a separate service that is installed independently of the VPN gateway on a permanently available computer in the "friendly" company network. This service must be available from the user's computing device or the NCP Secure Client from all parts of the network. In some cases, the router settings may need to be changed.
- The Friendly Net Detection Client (FNDC) contained in the NCP Secure Client is configured via the firewall settings of the NCP Secure Client. If the user computer is connected to a new network, the FNDC tries to establish a connection to the configured FNDS. In case of a successful authentication of the FNDS on the FNDC / NCP Secure Client, it is confirmed that the user computer is connected to a "Friendly Net". The firewall rules of the NCP Secure Client are automatically changed, according to the administrator's configuration.
- The administrator configures all firewall rules in the NCP Secure Client both for the "Friendly Net" and for unknown networks. The underlying firewall is part of the NCP Secure Entry and Enterprise Clients. Configuration locks prevent a user from automatically changing the firewall rules or deactivating the firewall. In centrally managed environments, this configuration can be carried out using NCP Secure Enterprise Management.

The Friendly Net Detection technology is based on established standards, a fact which ensures consistent system security while protecting system from errors which are frequent in proprietary solutions.

Operating Systems

See Prerequisites on page 1.

Security Features

Authentication
EAP, TLS or Certificate-based authentication of contact between NCP FND Server and NCP Secure Client

Support for certificates in a PKI:

- Soft certificates