

NCP Friendly Net Detection Server

für Windows

Release Notes



Service Release: 3.01 r47324
Datum: April 2020

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

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

1. Neue Leistungsmerkmale und Erweiterungen

Keine.

2. Verbesserungen / Fehlerbehebungen

Abwärtskompatibilität zu NCP Secure Clients mit Version bis einschließlich 11.x

Die TLS 1.0 Verhandlung zu älteren NCP Secure Clients bis einschließlich Version 11.x schlug fehl.
Dieser Fehler wurde behoben.

3. Bekannte Einschränkungen

Keine.

NCP Friendly Net Detection Server

für Windows

Release Notes



Major Release: 3.00 r47008
Datum: März 2020

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

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

1. Neue Leistungsmerkmale und Erweiterungen

Zertifikatsbasierte Authentisierung des Friendly Net Detection Servers mit TLS 1.2

Die Authentisierung des FND Servers am NCP Secure Client unterstützt ab dieser Version sowohl TLS 1.2 als auch TLS 1.0 sofern ein älterer NCP Secure Client verwendet wird.

2. Verbesserungen / Fehlerbehebungen

Inkompatibilität mit Microsoft Update KB4074598

Nach dem Einspielen des Microsoft Updates KB4074598 verweigerte der NCP Friendly Net Detection Server die korrekte Funktion. Dieser Fehler wurde behoben.

Passwort und PIN werden verschlüsselt in der Konfigurationsdatei abgelegt

Beim Start des NCP Friendly Net Detection Servers werden in der Konfigurationsdatei enthaltene, unverschlüsselte Benutzer-Passwörter und die Zertifikats-PIN ab dieser Version verschlüsselt in die Konfigurationsdatei zurückgeschrieben.

Die mitgelieferten Demo-Zertifikate wurden aktualisiert

3. Bekannte Einschränkungen

Keine.

NCP Friendly Net Detection Server

für Windows

Release Notes



4. Hinweise zum NCP Friendly Net Detection Server

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:

<https://www.ncp-e.com/de/loesungen/vpn/remote-access-vpn-technologien/friendly-net-detection/>

Eine Auflistung der im Produkt verwendeten Open Source Komponenten finden Sie im beigelegten Dokument „OpenSourceLicenseTerms.pdf“.

5. Leistungsmerkmale des NCP Friendly Net Detection Servers

Mit Hilfe der Friendly Net Detection (FND)-Technologie, ist der NCP Secure Client in der Lage ein vertrauenswürdiges, „freundliches“ Netzwerk automatisch zu erkennen. Daraus resultierend kann sich das Regelwerk der Firewall des NCP Secure Clients automatisch anpassen. So können beispielsweise vorkonfigurierte Zugriffe auf den Rechner des Anwenders automatisch im „befreundeten“ Firmennetzwerk aktiviert werden, wogegen der Rechner in unbekannten Netzwerk-Umgebungen vor externen Zugriffen abgeschirmt wird.

- Der Friendly Net Detection Server (FNDS) ist ein separater Dienst, der unabhängig vom VPN-Gateway auf einem permanent verfügbaren Computer im „Friendly Net“ bzw. „bekannten Firmennetzwerk“ installiert wird. Dieser Dienst muss vom Anwender-Rechner bzw. dem NCP Secure Client aus allen Teilen des Netzwerks verfügbar sein. Dazu müssen in einigen Fällen ggf. die Router-Einstellungen geändert werden.
- Der im NCP Secure Client enthaltene Friendly Net Detection-Client (FNDC) wird über die Firewall-Einstellungen des NCP Secure Clients konfiguriert. Wird der Anwender-Rechner mit einem neuen Netzwerk verbunden, versucht der FNDC, eine Verbindung zum konfigurierten FNDS herzustellen. Im Falle einer erfolgreichen Authentisierung des FNDS am NCP Secure Client wird bestätigt, dass sich der Anwender Rechner in einem „Friendly Net“ befindet. Die Firewall-Regeln des NCP Secure Clients werden automatisch, entsprechend den Vorgaben durch den Administrator, geändert.
- Der Administrator konfiguriert alle Firewallregeln im NCP Secure Client sowohl für das „Friendly Net“ als auch für unbekannte Netzwerke. Die zugrundeliegende Firewall ist Teil der NCP Secure Entry und Enterprise Clients. Konfigurationssperren verhindern, dass ein Anwender selbsttätig die Firewallregeln ändert oder die Firewall deaktiviert. In zentral verwalteten Umgebungen kann diese Konfiguration mit Hilfe des NCP Secure Enterprise Managements durchgeführt werden.

Die Friendly Net Detection-Technologie basiert auf etablierten Standards, die eine konsistente Systemsicherheit gewährleisten und das System vor Fehlern schützen, die bei proprietären Lösungen häufig auftreten.

NCP Friendly Net Detection Server

für Windows

Release Notes



Betriebssysteme

Siehe Voraussetzungen auf Seite 1.

Sicherheitsfunktionen

Authentisierung

EAP, TLS oder Zertifikats-basierte Authentisierung zwischen dem NCP Friendly Net Detection Server und dem NCP Secure Client.

Unterstützung von Zertifikaten innerhalb einer PKI:

- Soft Zertifikate