

Anleitung

**Digta**»

# Digta W/LAN-Adapter VPN-Konfiguration

Ab Firmware V2.3

Stand: März 2021



Der Digita W/LAN-Adapter implementiert VPN auf Basis des Open Source OpenVPN 2.4 Dämons. Daher kann der Systemadministrator im Allgemeinen alle dokumentierten OpenVPN-Optionen für die OVPN-Konfigurationsdatei verwenden:

<https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/>

Es gibt einige Ausnahmen und Einschränkungen, die im Folgenden beschrieben werden.

## 1 OVPN-Konfigurationsdatei herunterladen

Sie können die von Ihrem VPN-Server bereitgestellte \*.ovpn-Konfigurationsdatei verwenden (möglicherweise mit einigen zusätzlichen \*.pem- und \*.p12-Dateien).

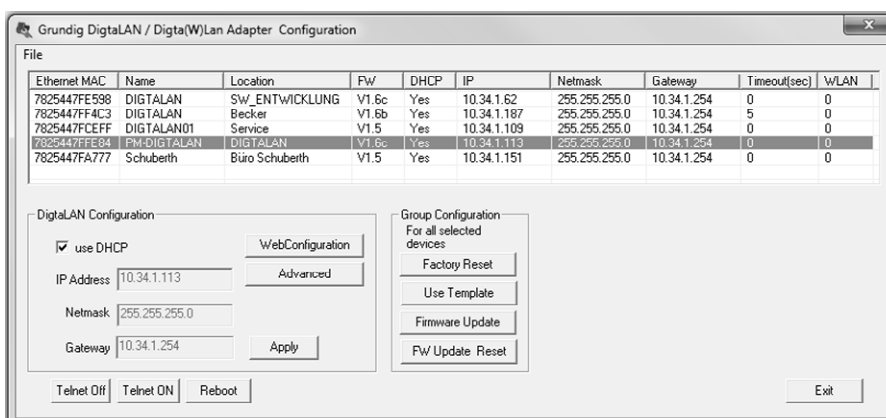
Die OVPN -Konfigurationsdatei selbst von Grund auf zu erstellen ist nicht ganz einfach. Die VPN-Einstellungen sind für verschiedene Server sehr unterschiedlich und daher gibt es kein allgemeines Rezept wie man die OVPN-Datei von Hand erstellt. Lesen Sie dazu das obige Referenzhandbuch und kontaktieren Sie den Systemadministrator des Ziel-VPN-Servers.

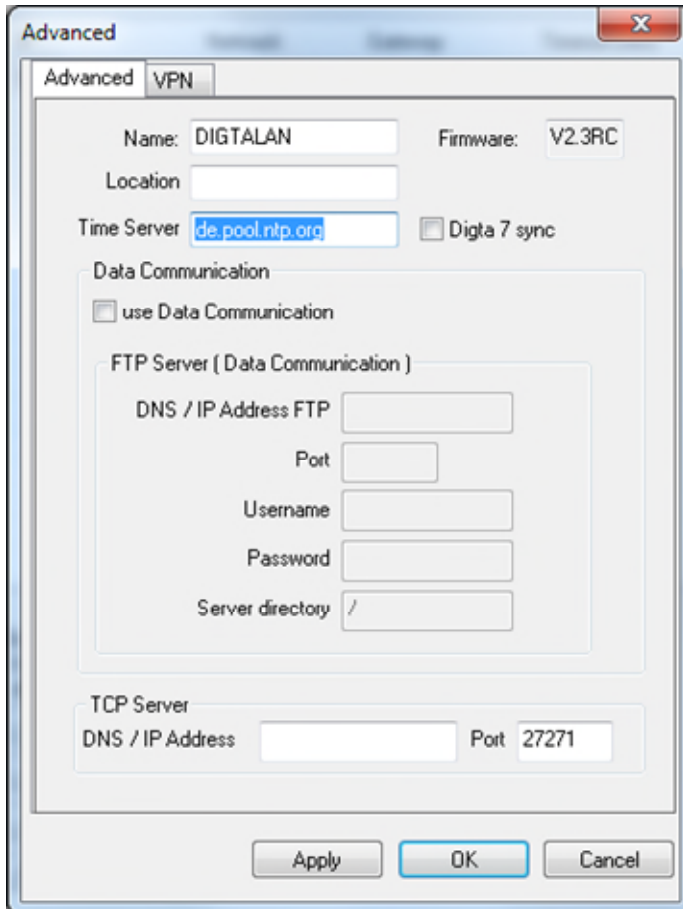
## 2 Synchronisation der Uhr am Adapter einrichten

Für eine gute Verbindung mit dem VPN-Server müssen Sie die Uhr des Adapters mit einem nahegelegenen NTP-Server synchronisieren. Wenn es in Ihrem lokalem Netzwerk keinen solchen Server gibt, dann können Sie einen der Server von dieser Seite verwenden:

<https://www.ntppool.org>

Starten Sie das Konfigurationstool „DigitaLANConfig.exe“ und klicken Sie auf die Schaltfläche „Advanced“.



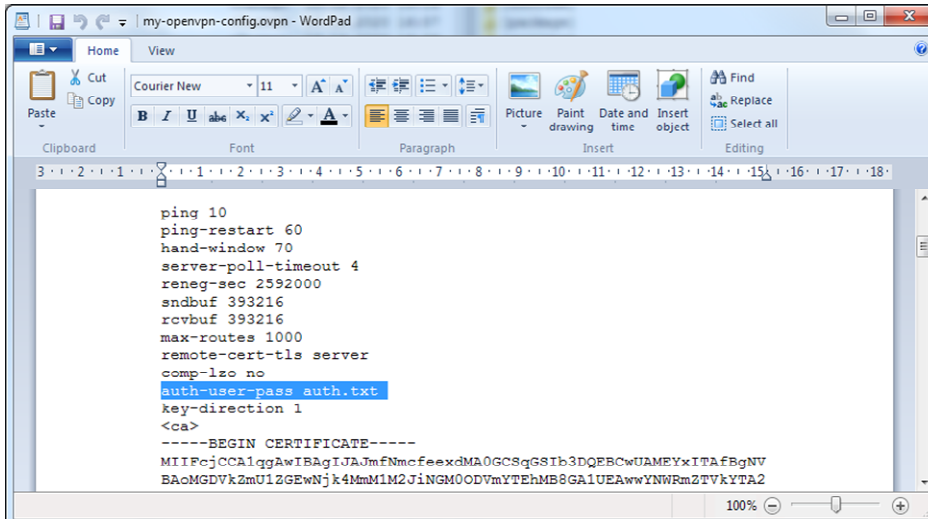


Nachdem Sie auf der Registerkarte "Advanced" die Schaltfläche "OK" gedrückt haben, starten Sie bitte den Adapter neu, um die neuen NTP-Server-Einstellungen zu übernehmen. Sie können das synchronisierte Datum und die Uhrzeit im UTC-Format auf der Hauptseite des Web-Interface des Adapters überprüfen (siehe Schaltfläche "WebConfiguration"). Warten Sie nach dem Neustart 1-2 Minuten, um die Uhrensynchronisation abzuschließen.

### 3 OVPN-Konfigurationsdatei mit eingetragenen Zertifikaten

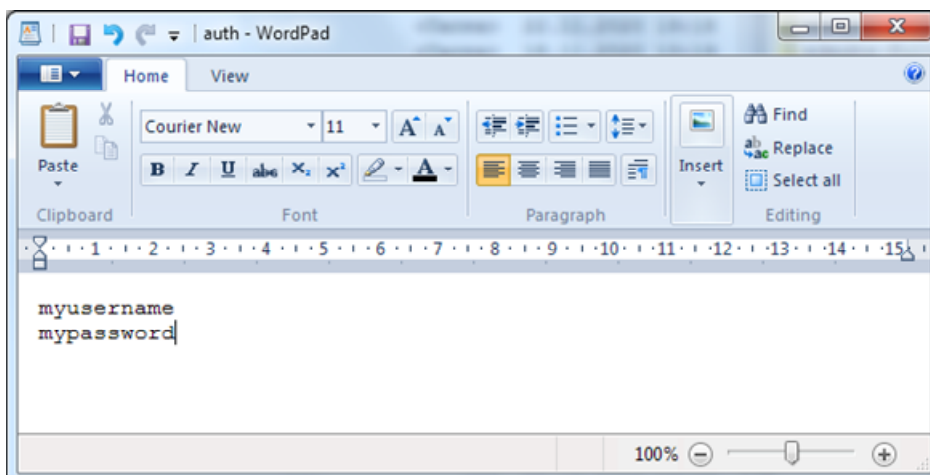
Wenn Sie eine "All-in-One"-OVPN-Datei mit eingefügten Zertifikaten und Schlüsseln haben, ist die Einrichtung am einfachsten. Sie können die \*.ovpn-Datei in einem beliebigen Texteditor öffnen, der EOLs im Unix-Stil (LF) unterstützt, und nach <ca>-, <cert>- und <key>-Tags und Base64-kodiertem Text dazwischen suchen. Wenn Tags vorhanden sind, können Sie diese Datei einfach in den Adapter hochladen.

Falls Ihr Server eine Benutzer/Passwort-Authentifizierung erfordert, müssen Sie die Option auth-user-pass zur OVPN-Konfigurationsdatei hinzufügen. Verwenden Sie keinen absoluten oder relativen Pfad für diese Option und geben Sie nur den Dateinamen ohne Verzeichnisse an.



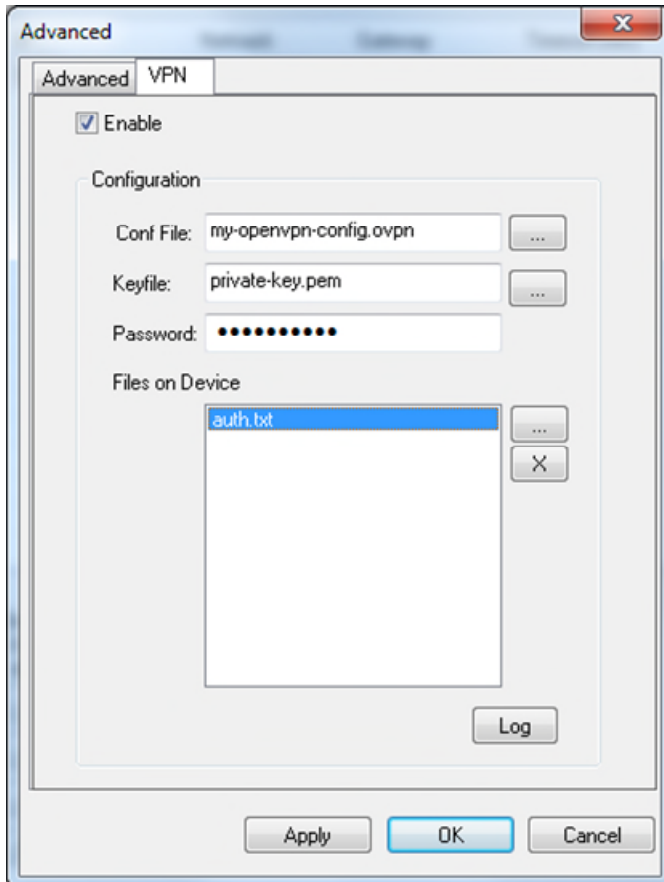
```
ping 10
ping-restart 60
hand-window 70
server-poll-timeout 4
reneg-sec 2592000
sndbuf 393216
rcvbuf 393216
max-routes 1000
remote-cert-tls server
comp-lzo no
auth-user-pass auth.txt
key-direction 1
<ca>
-----BEGIN CERTIFICATE-----
MIIFCjCCA1ggAwIBAgIJAJmfNmcfeexDMA0GCSqGSIb3DQEBCwUAMEYxITAFBgNV
BAoMGDVkZmU1ZGEwNjk4MmM1M2JiNGM0ODVmYTEhMB8GA1UEAwwYNWRm2TVkYTA2
```

Speichern Sie Ihren Benutzernamen und Ihr Passwort in einer separaten auth.txt-Datei. In die erste Zeile setzen Sie den Benutzernamen und in die zweite Zeile das Passwort.

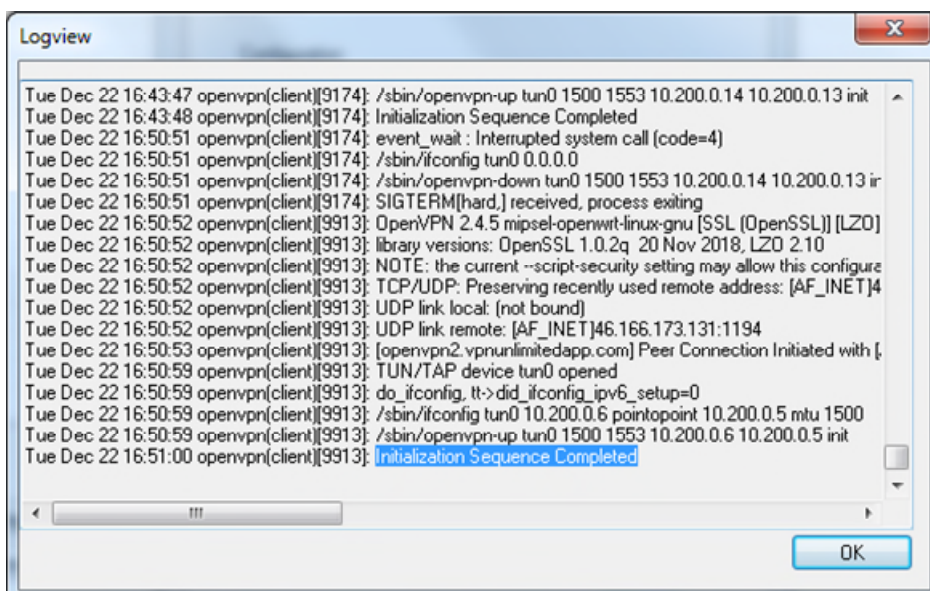


```
myusername
mypassword
```

Jetzt können Sie VPN aktivieren und die \*.ovpn-Datei (und optional auth.txt) auf den Adapter hochladen.



Lassen Sie die Felder "Keyfile" und "Password" für die OVPN-Konfiguration mit eingefügten Dateien leer. Nach dem Drücken der Schaltfläche "Apply" können Sie das OpenVPN-Log überprüfen (siehe Schaltfläche "Log"). Warten Sie einige Minuten bis die Verbindung zum VPN-Server hergestellt und der VPN-Tunnel aufgebaut ist. Wenn VPN erfolgreich war, sehen Sie im Fenster "Logview" am Ende die Meldung „Initialization Sequence Completed“. Öffnen Sie dieses Fenster erneut, um die Log-Datei zu aktualisieren.



**Hinweis:**

Die VPN-Einstellungen bleiben beim Neustart des Adapters erhalten und der OpenVPN-Dämon baut den VPN-Tunnel nach dem Neustart in wenigen Minuten wieder auf. Daher müssen Sie das Kontrollkästchen „Enable“ explizit deaktivieren, um die Verwendung des VPN-Tunnels für alle Verbindungen zu unterbinden.

Sie können die neue externe VPN-IP-Adresse auch auf der Hauptseite der Web-Oberfläche des Adapters überprüfen (Schaltfläche "WebConfiguration").



The screenshot shows the Grundig Business Systems web interface. The top header includes the text "turn voice into" followed by a voice icon and the word "action", and the Grundig Business Systems logo. On the left side, there is a navigation menu with links for Setup, LAN, WLAN, Transfer, SMTP, FTP, Log, and License. The main content area is titled "Digta»" and contains several configuration sections:

- Info:** A table showing system information: Version (Digta W/Lan Adapter V2.3RC2), Ethernet MAC (7825447E8F41), WLAN MAC (7825447E8F41), UTC (2020-12-22 15:53:44), and VPN ([AF\_INET]46.166.173.131 1194).
- Language:** A dropdown menu set to "English" with an "Apply" button.
- Digta W/LAN:** A section for device configuration with a "Device name" field containing "DIGTALAN".
- Access password:** Fields for "Name" (edm), "Password" (masked with dots), and "Confirm password" (masked with dots), with "Apply" and "Cancel" buttons.
- Configuration:** An "Erase" button.

## 4 OVPN-Konfigurationsdatei mit Verweise auf externe Dateien

Wenn Sie Zertifikate oder Schlüssel als separate Dateien haben, müssen Sie diese in der Haupt-OVPN-Konfigurationsdatei referenzieren und alle diese Dateien auch auf den Adapter hochladen. Schreiben Sie jede Option mit dem Dateinamen in eine extra Zeile.

```
ca my-ca-file-name.pem
cert my-cert-file-name.pem
extra-certs my-extra-certs-file-name.pem
dh my-dh-file-name.pem
key my-key-file-name.pem
pkcs12 my-pkcs12-file-name.p12
```

Verwenden Sie für diese Optionen keinen absoluten oder relativen Pfad. Geben Sie nur den Dateinamen ohne Verzeichnisse an. Alle diese Dateien müssen im PEM-Format sein (außer pkcs12). Es ist nicht notwendig, dass Sie alle diese Optionen/Dateien verwenden (normalerweise nur ca, cert und key oder pkcs12-Bündel). Sie können auch eine gemischte OVPN-Konfiguration verwenden, wenn ein Teil der Dateien eingetragen ist (wie <ca> und <cert> Tags) und ein anderer Teil separat hochgeladen wird (wie die Schlüsseloption). Bitte sprechen Sie mit dem Systemadministrator Ihres VPN-Servers darüber, welche Dateien Sie wirklich benötigen.

Sie müssen alle diese \*.pem- und \*.p12-Dateien über das Listenfeld "Files on Device" hochladen mit Ausnahme der Schlüsseldatei.

Wenn Ihre private Schlüsseldatei mit einem Passwort geschützt ist, müssen Sie sie in das Feld "Keyfile" eintragen und auch das Feld "Password" ausfüllen. In diesem Fall brauchen Sie die Schlüsseldatei nicht in der Haupt-OVPN-Konfigurationsdatei zu referenzieren. Außerdem hat die Schlüsseldatei, die über das Feld "Keyfile" hochgeladen wird, immer eine höhere Priorität als die Schlüsseldatei, die in der OVPN-Konfigurationsdatei referenziert und über das Listenfeld "Files on Device" hochgeladen wird.

**Hinweis:**

Um eine hochgeladene Datei vom Adapter zu löschen, entfernen Sie sie aus dem Listenfeld "Files on Device" und drücken Sie die Schaltfläche "Apply" oder "OK". Um die über das Feld "Keyfile" hochgeladene Schlüsseldatei zu löschen, entfernen Sie den Dateinamen aus diesem Feld und drücken Sie die Schaltfläche "Apply" oder "OK".

**Hinweis:**

Laden Sie keine Dateien mit der Erweiterung \*.conf über das Listenfeld "Files on Device" hoch. Denn der OpenVPN-Dämon würde versuchen, diese Dateien zu parsen und irgendwelche zufälligen Wörter als VPN-Optionen zu interpretieren. Es ist besser, immer nur Dateien mit den Erweiterungen \*.ovpn, \*.pem, \*.p12 und \*.txt hochzuladen.

## 5 Standard DNS für VPN

Bei bestehender VPN-Verbindung versucht der Adapter immer, DNS-Server zu verwenden, die vom VPN-Server gepusht wurden (aber nicht vom lokalen Netzwerk). Wenn der VPN-Server keine DNS-Server bereitstellt, verwendet der Adapter Google Public DNS.

<https://developers.google.com/speed/public-dns>

Zurzeit gibt es keine Möglichkeit, andere Standard-DNS-Server während der VPN-Verbindung einzurichten.

Copyright © 2021 Grundig Business Systems GmbH  
Alle Angaben können sich ohne Vorankündigung ändern.  
Irrtümer vorbehalten.

**Grundig Business Systems GmbH**

Weierstraße 10

95448 Bayreuth

Germany

[www.grundig-gbs.com](http://www.grundig-gbs.com)