ZF Net Remote 3
FAQ (EN)

Version 1.00.3

10.05.2021

Lenkungsinformationen / Control Information

Title:		Title:	ZF Net Remote 3 FAQ

Erstellt/ Prepared by:		Geprüft/ Checked by:		Freigegeben/ Approved by:	
Datum/ Date:	2019-11-20	Datum/ Date:	(YYYY-MM-DD)	Datum/ Date:	(YYYY-MM-DD)
Name:		Name:		Name:	

Datum Date (YYYY-MM-DD)	Version Version	Inhalt / Änderung Content / Change	Ersteller Author
2019-11-20	1.00.1	Document established	
2020-06-22	1.00.2	Determine VPN typ	
2021-05-10	1.00.3	Router fixed IP	

Table of Contents

1   Summary

Here, you will find answers to frequently asked questions relating to ZF Net Remote.
Target group:
ZF Net Remote users
Validity:
Status of the information stated below: 11/2019
Changes may be implemented at any time.

2   What do I need in order to start?

You need a valid ZF Net Remote account which can be obtained on request from User Management. If you do not have authorization, your responsible applicant must make the request for authorization.

Authorized applicant

ZF-internal   : E.g. direct superior, cost center manager, group manager, etc. by AnGeBer process.

ZF-external   : ZF contact person, ZF contact, … by AnGeBer process and Network rights (Firewall-rights) via Ticket.

3   What does ZF Net Remote do?

ZF Net Remote enables secure (encrypted) access to the ZF network via the Internet. An Internet connection is required if you are working exclusively with the VPN client (Pulse Secure).

4   Restrictions in the local network

- The secure tunnel "has no doors" and prevents the computer from accessing any other systems in the local network. When the tunnel is set up you can only access systems on the Internet via the ZF network and when you have Internet authorization.
- Blocking caused by a firewall in the local network can hinder access to the ZF network, even if "normal" surfing on the Internet is still possible. Contact the operator or administrator of the network to have the block removed.

5   When should I use the ZF-EMEA, ZF-AMERICA, ZF-APA and ZF-CHINA connections?

You use these three gateways (dial-in nodes) when you are connected to the Internet and want to access the ZF network. Three dial-in nodes (gateways) were set up worldwide for this purpose:

- ZF-EMEA   = **E**urope **M**iddle **E**ast **A**frica
- ZF-AMERICA   = North and South **America**
- ZF-APA   = **A**sia and **P**acific **A**rea
- ZF-CHINA   = China

Recommendation (only for ZF-User): Use the gateway closest to your location to minimize any delays (latency periods). You can however also use one of the other gateways if necessary.

Comment: One exception is the group of external users - they can only use the home gateway.

6   Problems in the home office, what can I do?

ZF Net Remote presumes the Internet connection (unknown number of connection segments) between the local network and the ZF Gateway is stable.
Connection problems are usually caused by interferences in the local network, in addition to interferences on the Internet.

Influencing factors:

- The user and ZF Friedrichshafen AG do not have any influence on the sub-sections of the Internet connection, but have some influence on the start and end segments.
- The user can use a convenient wi-fi connection or decide to use a more stable LAN connection.
- The operator is responsible for the stability of the local network (LAN).

Even if the user can surf the Internet, this fact is no guarantee for a stable ZF Net Remote connection. The reason for this is that secure connections have greater requirements regarding the stability of the connection and security.

6.1   Define the problem (various options)

6.1.1   Connect the notebook directly to the router

If errors occur, connect your notebook initially via a LAN cable directly to your router. Use a suitable LAN cable for this purpose. Switch wi-fi off on the notebook while carrying out the test. Remember, even a LAN cable can be defective - if the error occurs again, try using a different LAN cable.
If the problem is no longer present when connected via the LAN cable, proceed as described in 6.1.2.

6.1.2   Use the notebook in the direct vicinity of the wi-fi access point

Place your notebook close to the wi-fi access point which is usually integrated in the router. Test the dial-up connection and increase the distance from the router until the first error occurs. Move one step closer to the access point. The remaining distance to the access point marks the greatest distance that you can reach at this location.
If it is not possible to work like that, we recommend only working in this local network with a LAN cable.

6.1.3 Check local IPv4 adress

The router's network address (IPv4 address) is usually assigned automatically. If the IPv4 is changed while you are connected to Pulse Secure, there may be a short interruption. After the event of short interruption the VPN connection to the ZF is automatically restored. Programs like SAP, Skype, etc. can dedect the recovery time as a problem and respond with an error message.
Remedy: Assign a fixed IPv4 address to your computer in the router. If you are using LAN and / or WLAN, you must perform the fixed IP assignment for both connection types.

6.1.4 Connect the notebook to a different DSL connection

Connect the notebook to a different DSL connection for testing purposes. For example, ask the neighbor, family or friends if you can use their DSL connection. Ideally, the DSL connection should be from a different connection provider.

6.1.5 Test the ZF notebook in the ZF network

If the notebook is a ZF notebook, you can also test the function in the ZF LAN, ZF Office Network and even in the Guest Net. In the latter case, you will need temporary access with a username and password.

6.2 Router settings

The router configuration can also be responsible for problems. Even if you have not made any changes, the "default settings" may be the cause. Quick tips for experienced users:

- Energy options   → Switch off the energy-saving mode for LAN Ports
- IPv6 configuration   → Switch off
- Bandwidths were limited   → Increase for test purposes
- Child-safety   → Switch off or check
- Firewall   → E.g. SSL Port (443) blocked > Enable
- Current use of IP telephony   → Switch off or limit
- Current use of TV or VOD   → Switch off or limit
- Bandwidth Up/Down link too low   → Increase if possible
- IPv4 address automatically   → Assign fixed IP to ZFNR computer (LAN / WiFi)

6.3 Wi-fi level display

The signal strength display is often misunderstood - this means the number of the relative level display = vertical "bars". These do not say anything about the quality of the connection or speed. We recommend carrying out Points 6.1 - 6.2 even when full signal strength, i.e. all bars, is displayed.

6.4 Power LAN (PLC)

Power LAN is also popular, e.g. means one less cable. Some of these "socket adapters" can cause problems. If the adapter becomes hotter than usual, this can for example be a sign of a forthcoming outage. Initial "glitches" can occur during this time and may be the cause for a poor connection. As in the case of wi-fi, we recommend following Points 6.1 - 6.2.

6.5 DECT (cordless phone)

Private phones are nowadays usually radiotelephones - specifically DECT phones. A part of the DECT telefone is the base station, unless they are coupled with the router. Is the phone, or the base station, positioned too close to the notebook (< 1m), interferences can disturb the wireless connection of the notebook. Here it helps to keep a greater distance. Example: place

Problems in the home office, what can I do?

the base station on the shelf, not on the desktop or place the radio handset far from the notebook.

Problems in the home office, what can I do?

7   Time and time zone, what is important?

Valid for: PingID user with PingApp, external User with smartphone

Please proceed as follows:
1. Change time zone
2. Check the date, time and time zone again
3. Restart smartphone.

Additional information:
Change time zone without restarting the Smartphone usually the result is that the login is no longer possible. **The incorrect code leads to lock access** after several unsuccessful attempts. If locked, the hotline (IT helpdesk) is required to unlock the access.

Why that all?
- The correct time is important, as this included in the calculation of the codes.

8 Determine VPN type (speed relevant). How to do this?

The VPN type shows which connection type is currently used. An existing connection is therefore a prerequisite.
The VPN-type takes affects the connection speed.

Line of action:
- Establish a connection to one of the ZF gateways.
- Wait a minute. The precise automatic negotiation of the VPN type takes time.
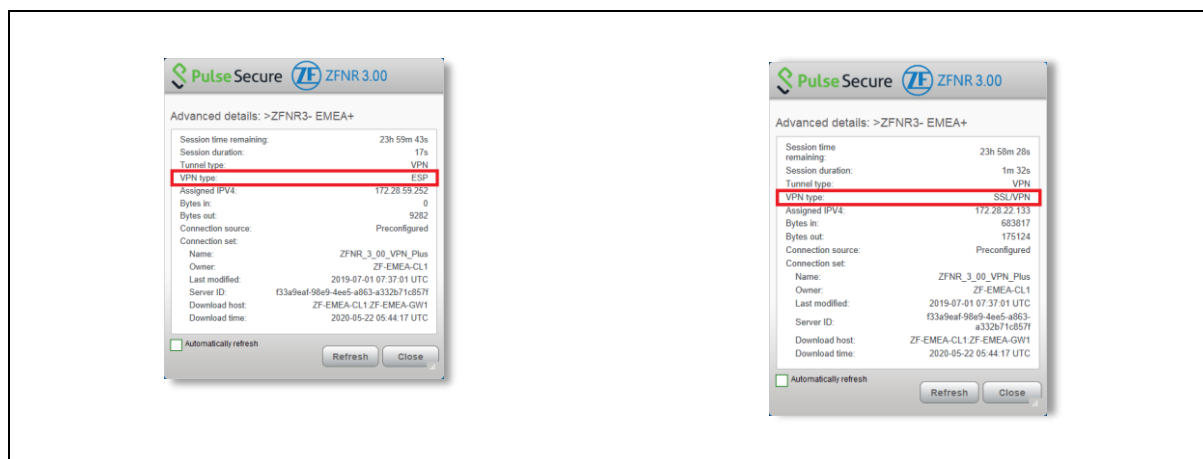- Click the current connection. The connection will be marked (highlighted blue).
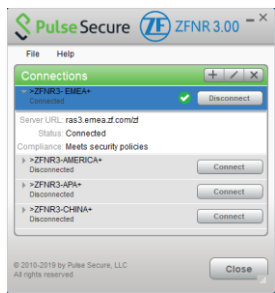
- Click on „File" → „Connections" → „Advanced Connection Details…".
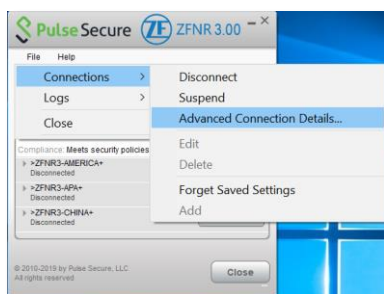
The connection details are now displayed in a new window.
Your current VPN type can be found in the line "VPN type:". There are two possibilities. Either "ESP" or "SSL/VPN".
- The "ESP" type is more powerful.
- The "SSL/VPN" type is usually slower, but more robust.

9   IT HelpDesk (IT-Hotline)

ZF EMEA IT HelpDesk (**E**urope, **M**iddle **E**ast **A**sia) Mo.-Fr. 05:00 - 22:00 (UTC+1 summer time, UTC+2 winter time) Tel: +49 7541 77 3600	**ZF APA IT HelpDesk** (**A**sia, **P**acific **A**rea) Mo.-Fr. 08:00 - 18:00 (UTC+8) Tel: +86 21 3761 3600
ZF AMERICA - North IT HelpDesk Mo.-Fr. 07:00 - 17:00 EST (USA) (UTC-7) Tel: +1 734 582 8330 Mo.-Fr. 08:00 - 17:30 CST (Mexico) (UTC-6) Tel.: + 52 33 32080000 ext 1911 (Mexico)	**ZF AMERICA - South IT HelpDesk** 7/24 Tel: +55 15 4009 3600