ZF Net Remote 3.01 Operating Instructions – External User

For Partners / Externals

Doc.Version

3.01.05

29.07.2023

Lenkungsinformationen / Control Information

Titel:		Titel:	ZF Net Remote 3.01 Operating Instructions – External User

Erstellt/ Prepared by:		Geprüft/ Checked by:		Freigegeben/ Approved by:	
Datum/ Date:	2021-05-20	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
2021-05-20	3.01.01	Origin for ZFNR 3.01	FIII52
2021-06-09	3.01.02	Update and reorganization chapter 3 & 4	FIII52
2021-07-16	3.01.03	Inserted new chapter 5.1	FIII52
2021-08-23	3.01.04	Inserted new chapter 5.4 VM dropping connection	FIII52
2023-07-28	3.01.05	Update pictures, added MFA section	FIII53 (GK)

Table of contents

1. Introduction 4
1.1. Prerequisites of using ZFNR3.01 with success 4
1.2. Minimum requirements for the operating system and its environment 4
2. Authentication 5
2.1 Azure Multi Factor Authentication (MFA) 5
2.1.1 Important requirements 5
2.1.2 Multifactor authentication setup 5
2.1.3 Install MS Authenticator app on your mobile phone 7
2.2 PingID (not for new users) 9
2.2.1 Important requirements 9
2.2.2 Install PingID app on your mobile phone 9
2.2.3 Register your ZF account 9
2.2.4 Additional information 10
3 Establish a VPN connection 11
3.2 Open Pulse Secure connection 11
3.3 Authentication 12
3.4 ZFNR F/W Login Portal authentication 13
3.5 Disconnect the VPN connection 13
4 Internet connect during VPN session 14
4.2 Proxy settings 14
5 Troubleshooting and Assistance 15
5.2 Problem: Connection did not open 15
5.3 Problem: Connection is not well working 15
5.4 Problem: WLAN connection is not working 15
5.5 Problem: Connection drops under using a VM 15
5.6 VPN Connections via Firewall Systems 16
6 IT Global Service Desk (IT Global Service Desk) 17

Important information:

- **Before using the software for the first time**
  - **Make sure to have Internet access without restrictions**
  - **Installed ZFNR 3.xx Software**
  - **MFA Registration (or old PingID)**
  - **Privileges to use ZFNR 3.xx**
- **Please close all programs that are processing any data from ZF or another network when you establish or terminate a connection with ZF Net Remote. Warning: Data may otherwise be lost.**
- **If a VPN connection is established, no devices in your local network are usable.**

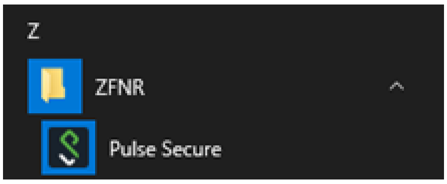
1. Introduction

ZF Net Remote 3.01 is used to connect your mobile computer to the ZF company network (ZF Net).

1.1. Prerequisites of using ZFNR3.01 with success

- Internet access without restrictions
- ZF domain user (mandatory) to use Azure MFA or PingID
- Azure MFA or PingID- Registration (2nd factor)
- Installed ZFNR 3.01 Software
- Privileges to use ZFNR 3.01

VPN connection to ZF network the necessary VPN software Pulse Secure is located at Start→ All Programs → ZFNR



1.2. Minimum requirements for the operating system and its environment

The host is automatically checked during the login process. The local machine must fulfill all the following requirements.

- Windows 10, Windows 11 - not EOL (end of life).
- OS up to date (last Update / Patch not older than 2 month), Patches with severity "Critical" , Category "Security Update", "Critical Update"
- Anti Virus software is active and up to date (signature not older than 2 days).
- A local firewall is activated (any supported product/solution).

2. Authentication

For security reasons, connections to the ZF network must be secured with an independent second factor.
Net Remote 3.0x is used to connect a non ZF computer, with Windows operation system, to the ZF Company Network (ZF Net). The solution is based on Pulse Secure software as basic software and PingID as second factor authentication.
Until end of this year all external users will be migrated to Azure MFA solution. PingID will be retired until end of the year.
Both solution require adjust your mobile phone. You have to download and install additional software via the well-known App Stores.

2.1 Azure Multi Factor Authentication (MFA)

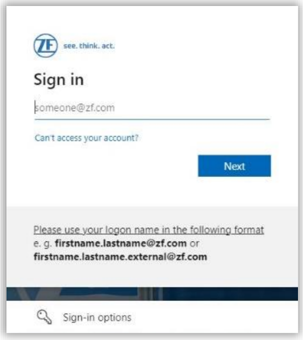
Azure Multifactor Authentication (MFA) is becoming the standard at ZF.
All external users/partners are required to implement this solution. New users should only use this solution as an authenticator for VPN connections.

2.1.1 Important requirements

- **The mobile phone used by you for the MFA authentication must not be rooted! (you have gained superuser privileges on your device)**
- External ZF users are allowed to use a private device.
- Installed the MS Authenticator mobile application on the device from the common App Stores (Apple/ Google Play Store).
- The mobile device requires and internet connection to complete the device pairing process.
- Your mobile phone must have a screen lock – by number, fingerprint, or other possibilities.
- Allowing the PingID app to access the device camera will allow you to scan a QR code required in the device pairing process. If you do not want this, you can manually enter the device pairing key.
- The PingID app requires iOS Version 11.x or Android Version 6.0 and higher.
- Microsoft Windows Phones are not supported.

2.1.2 Multifactor authentication setup

Open https://aka.ms/mfasetup in your browser



see. think. act.

Sign in

someone@zf.com

Can't access your account?

Next

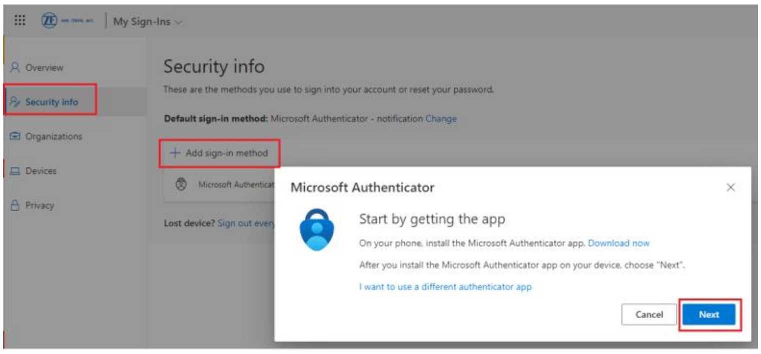
Please use your logon name in the following format
e. g. **firstname.lastname@zf.com** or
firstname.lastname.external@zf.com

Sign-in options

By default the Azure Multi-Factor Authentication is asking you to setup Microsoft Authenticator as your primary authentication method.

Hint: If you cannot install the app on your phone / tablet please select “I want to set up a different method” and choose “Phone” from drop-down menu and “Confirm”. Otherwise proceed with the setup of the Microsoft Authenticator App.
If you are not already registered, the following registration page will be shown to set up Microsoft Authenticator App.

In case you already registered with Azure MFA the Security Info Page loads, and you click on "+ Add Method" to register a new authentication method.



Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Microsoft Authenticator - notification Change

Lost device? Sign out every

Microsoft Authenticator

Start by getting the app

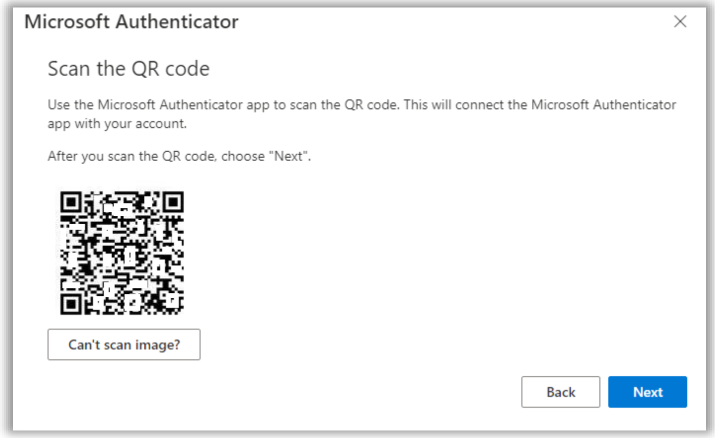
On your phone, install the Microsoft Authenticator app. Download now

After you install the Microsoft Authenticator app on your device, choose "Next".

I want to use a different authenticator app

Then accept next screen concerning set up your account and enter **“Next “** button.

You will get the QR code to use in next step .



Microsoft Authenticator

Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose "Next".

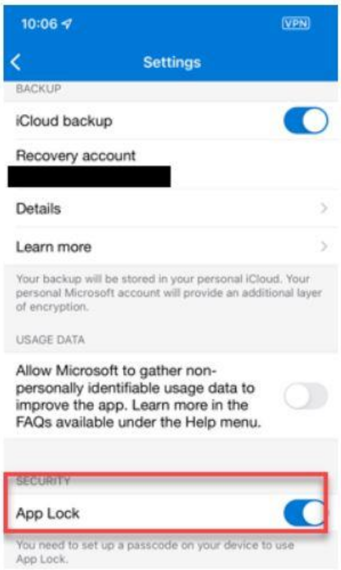
3

Keep this window open and follow the instructions.

2.1.3 Install MS Authenticator app on your mobile phone

To use MFA please open Google Play Store for android device or App store for IOS device. Install the **Microsoft Authenticator** app on your mobile device .

Enable the "App Lock" in the Microsoft Authenticator App settings.



10:06
Settings

BACKUP

iCloud backup

Recovery account
[redacted]

Details

Learn more

Your backup will be stored in your personal iCloud. Your personal Microsoft account will provide an additional layer of encryption.

USAGE DATA

Allow Microsoft to gather non-personally identifiable usage data to improve the app. Learn more in the FAQs available under the Help menu.

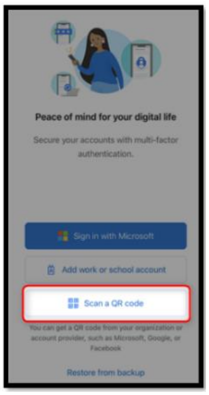
SECURITY

App Lock

You need to set up a passcode on your device to use App Lock.

This will further protect your second-factor credentials from unauthorized access.

If you see this screen tap Scan a QR code.



Peace of mind for your digital life

Secure your accounts with multi-factor authentication.

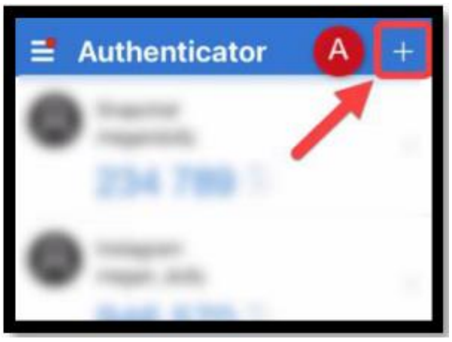
You can get a QR code from your organization or account provider, such as Microsoft, Google, or Facebook

Your phone camera will activate.

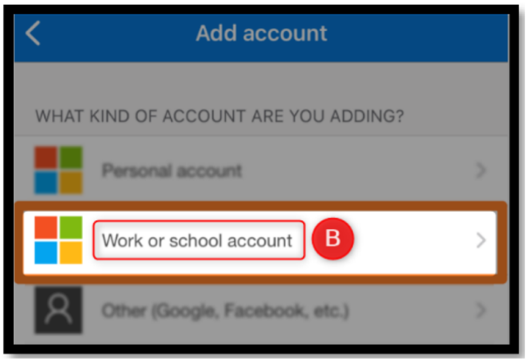
NOTE: if prompted, grant all permissions to Microsoft Authenticator to use your phone’s camera, send notifications, use FaceID(iPhone) or Fingerprint (Android), or App Lock.

If you are already signed into Authenticator…

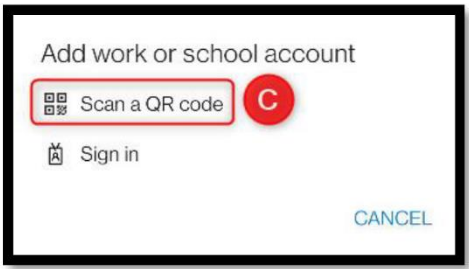
A) Tap on the **“+”**



B) Tap on **Work or School account**


Add account
WHAT KIND OF ACCOUNT ARE YOU ADDING?
Personal account
Work or school account
B
Other (Google, Facebook, etc.)

C) Tap **Scan a QR code**



Your phone camera will activate.

D) Tap **Scan a QR code**
Point your mobile device camera (within the Microsoft Authenticator app) to your PC screen to scan the QR code.

Note:
If you are requested to enter a pin code, enter the same one used to unlock your screen.

E) A code will appear on the Authenticator app on your smartphone
F) Insert in this field the code generated by your Authenticator app.
G) Click sign In

2.2 PingID (not for new users)

Until end of this year all external users will be migrated to Azure MFA solution. PingID will be retired until end of the year.

2.2.1 Important requirements

- **The mobile phone used by you for the 2nd-factor authentication must not be rooted! (you have gained superuser privileges on your device)**
- External ZF users are allowed to use a private device.
- Installed the PingID mobile application on the device from the common App Stores (Apple/ Google Play Store).
- The mobile device requires and internet connection to complete the device pairing process.
- Your mobile phone must have a screen lock – by number, fingerprint, or other possibilities.
- Allowing the PingID app to access the device camera will allow you to scan a QR code required in the device pairing process. If you do not want this, you can manually enter the device pairing key.
- The PingID app requires iOS Version 11.x or Android Version 6.0 and higher.
- Microsoft Windows Phones are not supported.

2.2.2 Install PingID app on your mobile phone

ZF owners can find detailed information on PingID in the ZF network on the intranet site: PingID .

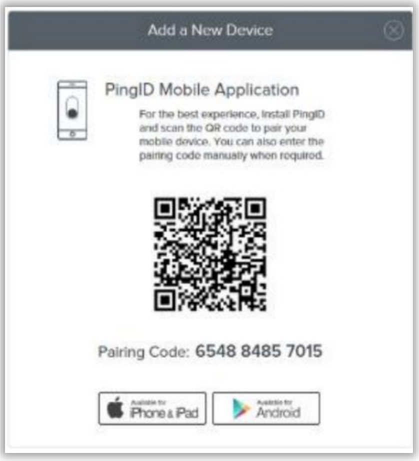
Open your App Store, depending on your mobile phone. Install "PingID".

External users cannot enter intranet sites without VPN!

Install "PingID" App on your phone

2.2.3 Register your ZF account

You will receive a mail with username, temporary password and QR code to registration in ZF. This QR code is valid 48 hours and is sent by identitymanagement@zf.com.
After expiration of QR validity user has to request a pairing code for the mobile device from IT Global Service Desk.
Please proceed with the following steps:
iD Open PingID by clicking on your home screen.
PingID will immediately start searching for a QR code.
Please place your device in front of the QR code you received in the e-mail from the IT Global Service Desk.



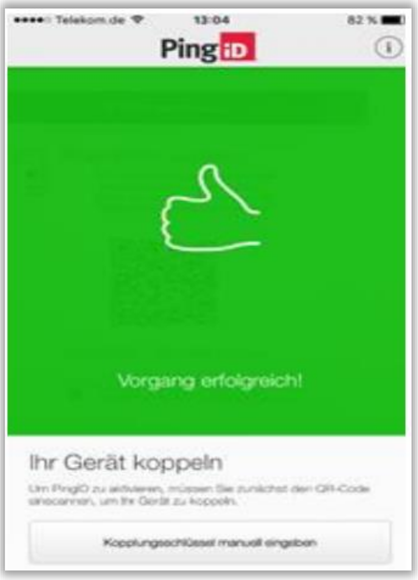
Add a New Device

PingID Mobile Application

For the best experience, install PingID and scan the QR code to pair your mobile device. You can also enter the pairing code manually when required.

Pairing Code: 6548 8485 7015

Registration is performed in the background.
You are informed when the registration was completed successfully.



Vorgang erfolgreich!

Ihr Gerät koppeln

Um PingID zu aktivieren, müssen Sie zunächst den QR-Code einscannen, um Ihr Gerät zu koppeln.

Kopplungsschlüssel manuell eingeben

PingID application will confirm correct pairing the mobile phone and youd ZF account.
Please enter a profile name- feel free to choose the name that you like.
External users can register only 1 mobile device!

If you have any problems, please contact the IT Global Service Desk (section 6) and inform the Desk IT Global Service Desk about KBA00001763.

2.2.4 Additional information

If the user has a valid password then the user can use it, otherwise should go in touch with the ZF contact.

3 Establish a VPN connection

To establish a connection to the ZF network it is necessary to perform **always** three steps:

1. Open Pulse Secure connection
2. Azure MFA or PingID authentication
3. ZFNR F/W Login Portal authentication

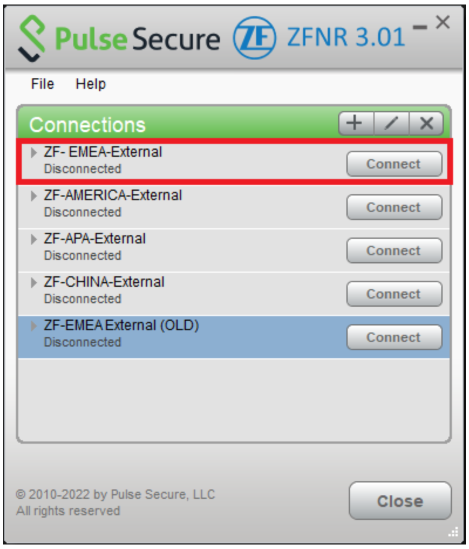
Only if you have successfully carried out all three steps will you have access to all services and servers in the ZF network enabled for you.

3.2 Open Pulse Secure connection

To establish a VPN connection to one of the four gateways please click on the correspondent link buttons. Please be informed you can establish only one connection at the same time.

Note:
Please close ALL programs (Outlook, Skype, SAP, etc.) before connecting. After the connection is successfully established, start the software you need.

An Internet network connection is a requirement for this. You can then establish a connection to the ZF network. Click on the "Connect" button belonging to the connection of your nearest ZF gateway.

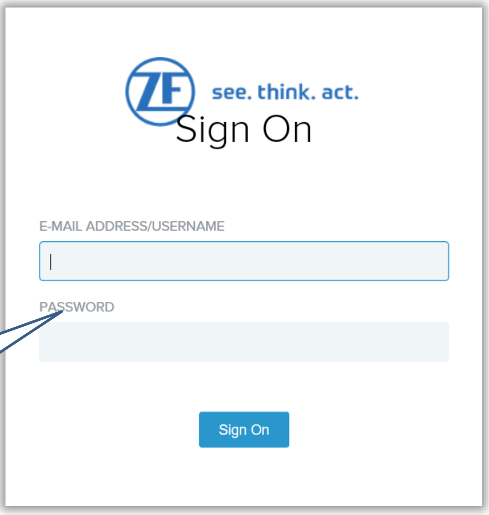


ZF- EMEA-External
Disconnected
ZF-AMERICA-External
Disconnected
ZF-APA-External
Disconnected
ZF-CHINA-External
Disconnected
ZF-EMEA External (OLD)
Disconnected

© 2010-2022 by Pulse Secure, LLC
All rights reserved

Browser with Login page.
Use the data from your **current windows login** on the computer.

After Pulse Secure log in the PingID authentication starts automatically.
Confirm the connection in the MS Authenticator application.

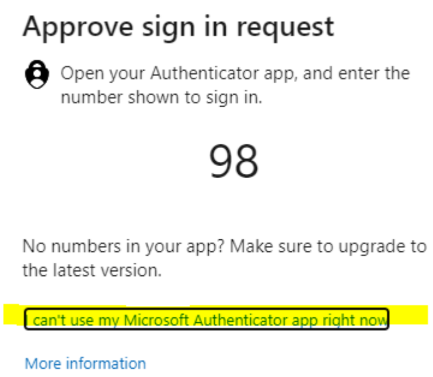


Use your current Windows login data

3.3 Authentication

After Pulse Secure log in the Azure MFA or PingID authentication starts automatically.

Please confir connection in the mobile App.



Approve sign in request

Open your Authenticator app, and enter the number shown to sign in.

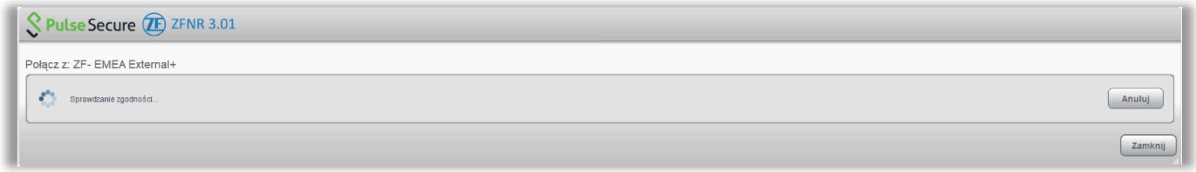
98

No numbers in your app? Make sure to upgrade to the latest version.

I can't use my Microsoft Authenticator app right now

More information

After confirm the connection Host hecker will start check the computer state .

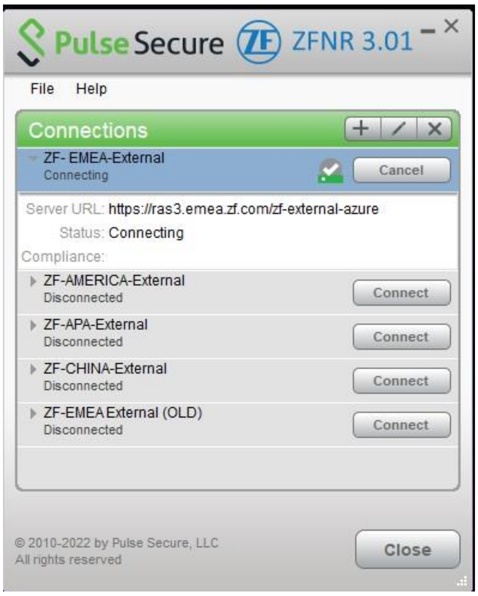


Połącz z: ZF- EMEA External+

Sprawdzanie zgodności...

The popup window disappears after a while (maybe some minutes) automatically.

Once you have finished the work requiring ZF network access, you can disconnect from the ZF network.



ZF- EMEA-External
Connecting

Server URL: https://ras3.emea.zf.com/zf-external-azure
Status: Connecting
Compliance:

ZF-AMERICA-External
Disconnected

ZF-APA-External
Disconnected

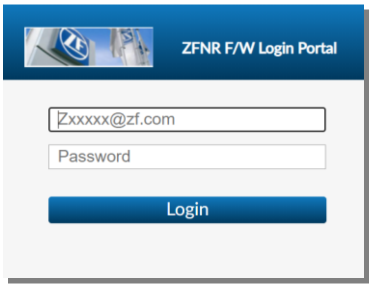
ZF-CHINA-External
Disconnected

ZF-EMEA External (OLD)
Disconnected

© 2010-2022 by Pulse Secure, LLC
All rights reserved

3.4 ZFNR F/W Login Portal authentication

After a successful connection to ZFNR3.0, a user is required to authenticate on the ZFNR Firewall Login Portal in order to be given access to ZF.
For authentication, open one of the following links and put in your credentials. Please use this format only.



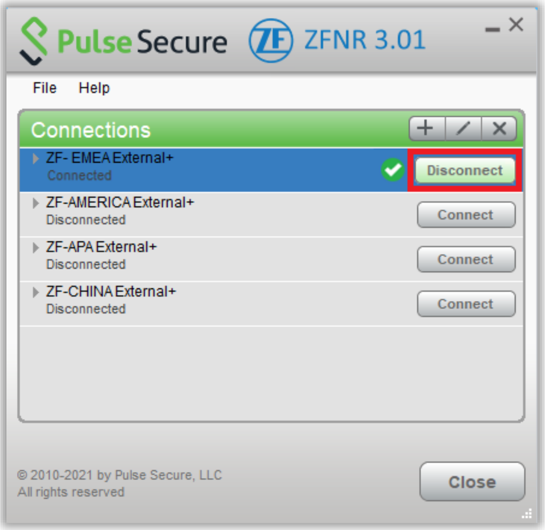
https://fw-auth-zfnr
https://fw-auth-zfnr.emea.zf-world.com
https://fw-auth-zfnr.america.zf-world.com
https://fw-auth-zfnr.apa.zf-world.com

Attention: A successful authentication to the firewall portal is only valid for the next 12 hours or you perform log out.

In case of problems contact the IT Global Service Desk, see section 6.

3.5 Disconnect the VPN connection

If you do not require the connection, it can be closed once again via the "Disconnect" button.



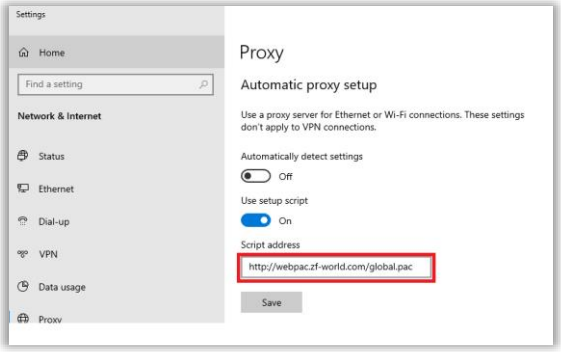
4 Internet connect during VPN session

Access to the Internet is not set by default for the external users. If you need this option please manually change your Proxy settings.

4.2 Proxy settings

To access the Internet, users should manually select the following *.pac file in their system or browser.
Script address: http://webpac.zf-world.com/global.pac

Go to Settings → Network and Internet → Proxy
and enter the correct link in the "Script address" field:



Proxy

Automatic proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Automatically detect settings
Off

Use setup script
On

Script address
http://webpac.zf-world.com/global.pac

After reopening the browser, Internet access should be granted.

5 Troubleshooting and Assistance

These are examples of the most common problems, for more refer to the FAQ chapter 6.

5.2 Problem: Connection did not open

The connection is not established. There are various error messages. Usually already at the first test. This is often due to local security software.

Please do the following:

1. Turn off the local security software. Just for this test. Not permanent.
2. Test opening connection with Pulse Secure again.
3. Turn on local security again.

If the test was successful with the local security software switched off, this must be configured. You may need to consult your local IT department for this.

Software known to us that had to be configured:

- zscaler

5.3 Problem: Connection is not well working

A local proxy in your network can cause applications to fail to start or not working during an existing connection (e.g., ZF_EMEA ...).

A possible workaround is:
Establish the connection. After the connection is established → disable the use of the local proxy.
If the connection is no longer needed → disconnect and enable the use of a local proxy.
For more or additional information please ask your IT.

5.4 Problem: WLAN connection is not working

The WLAN appears in the list of available Wi-Fi networks, but a connection attempt is aborted with an error message.

Cause:
If the laptop is connected to a LAN with a network cable, technical reasons prevent a simultaneous connection to WLAN.

Solution:
Disconnect the network cable from the laptop to enable the WLAN connection. You may have to switch the WLAN switch off and then on again. In other cases, it may be necessary to double-click on the WLAN connection.

5.5 Problem: Connection drops under using a VM

When using a VM, the connection often drops after about 5 to 10 minutes. Use with a VM has not been tested, but is widely used. Feedback from users has shown that changing the VM network configuration from NAT to bridge mode can help with this problem.

5.6 VPN Connections via Firewall Systems

To be able to connect to the ZF network, some ports and/or IP addresses must be enabled. For more information’s ask the IT Global Service Desk- refer to section 6.

6 IT Global Service Desk (IT Global Service Desk)

To contact ZF IT Global Service Desk call 3600 (from outside: site number + extension 3600)

The IT Global Service Desk is available in multiple language via phone.

English	24 hours a day, 7 days a week
German	Mon – Fri, 7am to 7pm CET
Spanish	Mon – Fri, 7am to 7pm CDT
GSD Chat (English only)	24 hours a day, 7 days a week