ZF Net Remote 3.1.x Operating Instructions – External User

For Partners / Externals

Doc.Version

3.1.00

01.09.2024

Lenkungsinformationen / Control Information

Titel:		Titel:	ZF Net Remote 3.1.00 Operating Instructions – External User

Erstellt/ Prepared by:		Geprüft/ Checked by:		Freigegeben/ Approved by:	
Datum/ Date:	2024.09.01	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
2024-09-01	3.1.00	New instruction for Ivanti client	FIII53 (GK)

Table of contents

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**
  - **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 3.1.x is used to connect your mobile computer to the ZF company network (ZF Net).

1.1. Prerequisites of using ZFNR3.1.x with success

- Internet access without restrictions
- ZF domain user (mandatory)
- MS Entra ID registration (MFA)
- Installed ZFNR 3.1.x Software
- Privileges to use ZFNR 3.1.x

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).

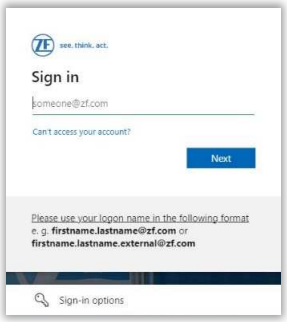
2. Authentication

For security reasons, connections to the ZF network must be secured with an independent second factor.
Net Remote 3.1.x is used to connect a non ZF computer, with Windows operation system, to the ZF Company Network (ZF Net). The solution is based on Ivanti software as basic software and MS Authenticator as second factor authentication.

Important :
As login use ZF account communication mail eg. name.surname.external@zf.com

2.1. Multi Factor Authentication (MFA)

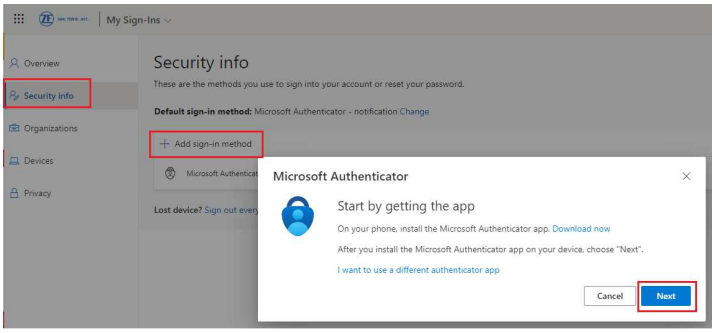
All External users should use MS Authenticator App (MS EntraID) as an authenticator for VPN connections.
All external users/partners are required to implement this solution.
To register new factor authentication open https://aka.ms/mfasetup in your browser



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

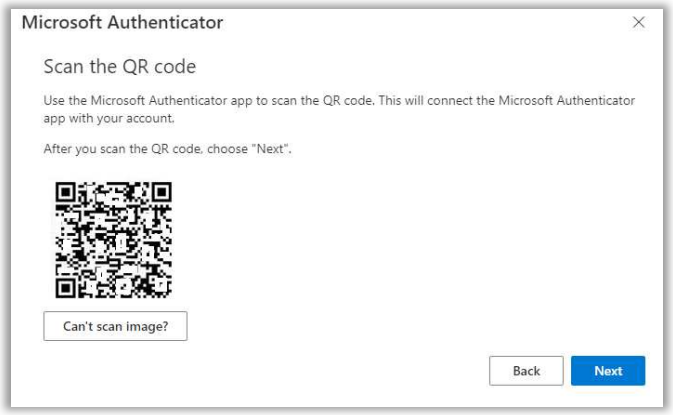
Hint: If you cannot install the app on your phone / tablet please select “I want to set up a different method” and choose “Phone” from drop-down menu and “Confirm”. Otherwise proceed with the setup of the Microsoft Authenticator App.
If you are not already registered, the following registration page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



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

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



Keep this window open and follow the instructions.

2.2. 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.

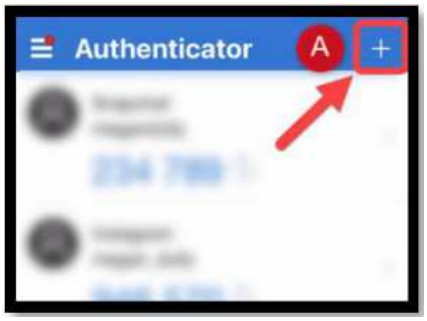
Enable the "App Lock" in the Microsoft Authenticator App settings. This will further protect your second-factor credentials from unauthorized access.

If you see screen tap Scan a QR code, 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.

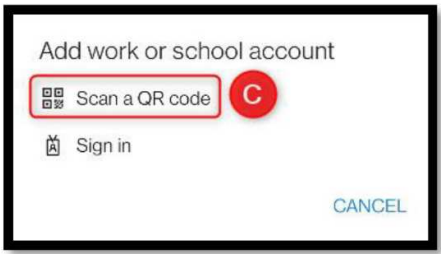
If you are already signed into Authenticator…

A) Tap on the **"+"**



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

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

3 Establish a VPN connection

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

1. Open Ivanti connection
2. Confirm connection in MS EntraID (MS Authenticator app , browser etc.)
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.

3.1 Open Ivanti 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, MS Teams, 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.

Browser with login page.
Use the data from your **ZF e-mail address** on the computer.

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

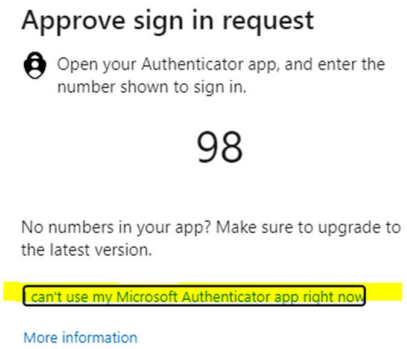
Please use your current ZF email address eg.
firstname.lastname.external@zf.com
Sign-in with Z-ID is not possible

Attention: A successful authentication to the MFA system assign to the connection the token, valid for the next 1 hour. Reconnections durring this time will not need MS Authenticator confirmation.

3.2 Authentication

After Ivanti log in the MS Entra ID (MFA) authentication starts automatically.

Please confir connection in the mobile App.



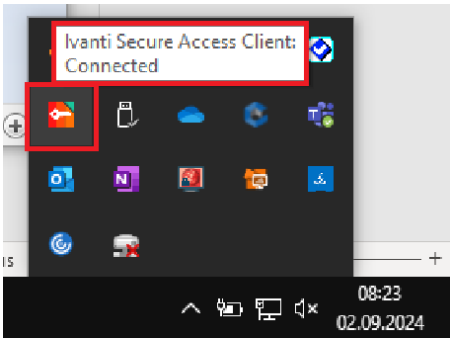
After confirm the connection Host checker will start check the computer state and securing connecting.

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

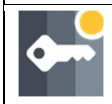
Once you have finished the work requiring ZF network access, you can disconnect from the ZF network.

3.3 Connection status

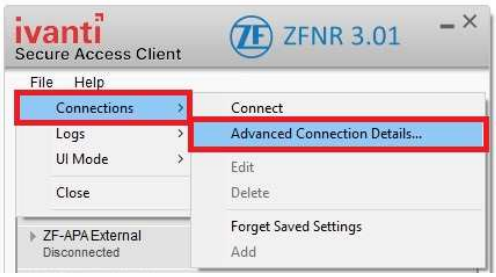
The Ivanti Secure Access Client tray icon indicates the current state of your network connection.



When any active connection has an issue, the system tray icon changes its state. The following icons indicate connection status.

Tray Icon	Description
	No connection.
	Connecting. A connection stays in this state until it fails or succeeds.
	Suspended.
	Connected with issues.
	Connection failed.
	Connected.
	Connected to the local network but no Internet access available.

To check more information about selected connection you can click Advanced Connection Details from the local “File” menu.



3.4 ZFNR F/W Login Portal authentication

After a successful connection to ZFNR3.1, 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.

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

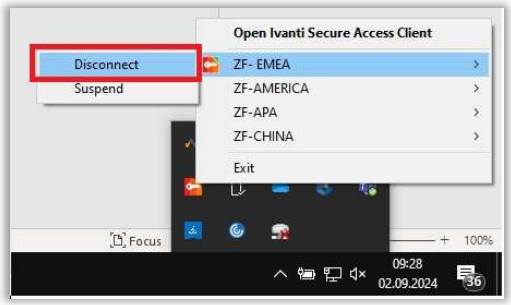
Please use this format only Zxxxxx@zf.com

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

On this page you can also request a ZIM password reset using the link at the bottom of the login page.

3.5 Disconnect the VPN connection

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

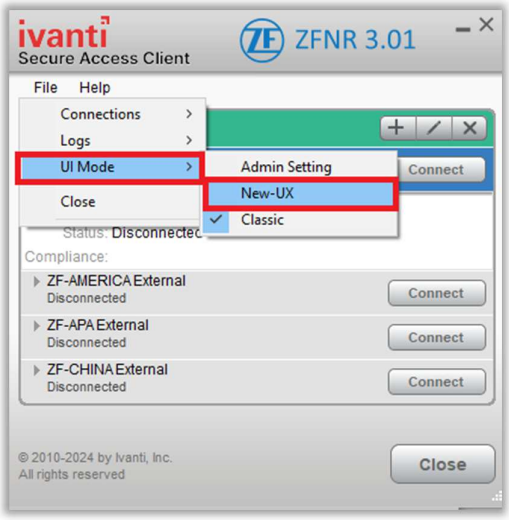


Second way is use “Disconnect” button on the try menu bar.

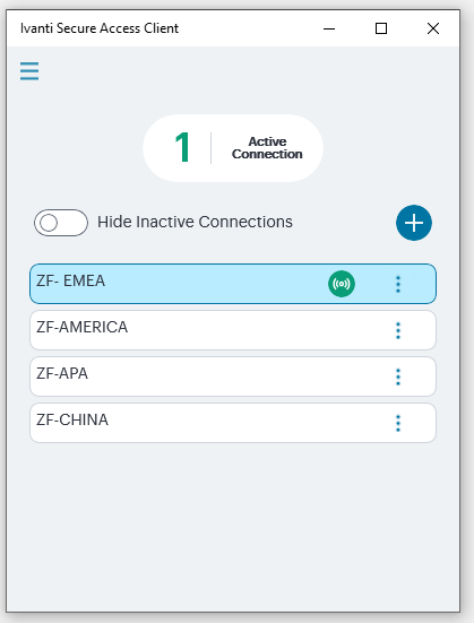
3.6 Switching UI modes

The Ivanti Secure Access Client allows to navigate from the New-UX to Classic UI and vice versa.

On Classic UI, click **File > UI Mode** to switch between the modes.



After switching and confirming the whole process, you can use the new UI mode:



Technically, it doesn't matter which UI mode is used.
The user can switch modes at any time, but some details are different from the classic mode.

Please use ISA Client Help from top menu to find more details concerning new interface.

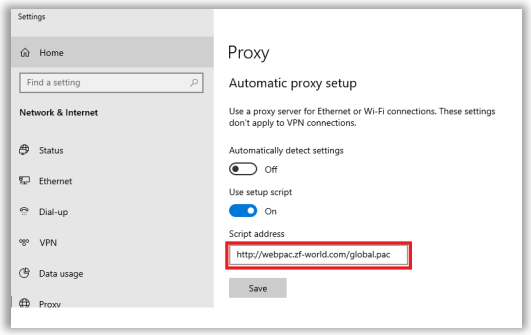
4 Internet connect during VPN session

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

4.1 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:



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.

5.1 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 Ivanti 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

5.2 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.

5.3 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.

5.4 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.

5.5 VPN Connections via Firewall Systems

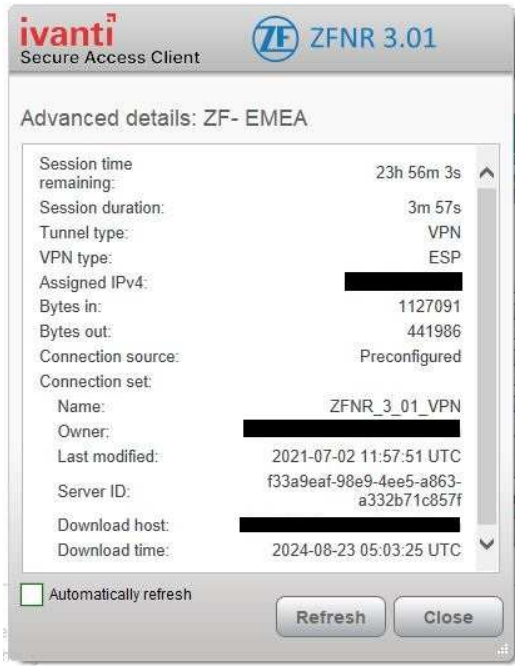
To be able to connect to the ZF network, some ports and/or IP addresses must be enabled. The router configuration can also be responsible for problems. Even if you have not made any changes, the "default settings" may be the cause. Quick tips for experienced users:

- 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)

For more information's ask the IT Global Service Desk- refer to FAQ section 6.

5.6 VPN Connection details

To check more information about selected connection you can click Advanced Connection Details from the local "File-> Connections-> Advanced Connection Details … " menu.

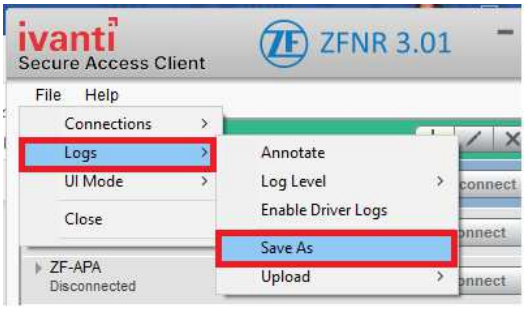


In case of service issue requested to the ZF please send / attach this data / screenshot to analyzing.

5.7 Save log file

In case of service issue requested to the ZF please send / attach log file to analyzing.

Go to the Pulse Secure app.
- First he should enable detailed logs:
  Pulse Secure-> File -> Log Level -> detailed
- Then set an annotation:
  File -> Logs -> Annotate
  The text should be "username or Z-number ".
- Try log in to EMEA .
- Disconnect
- Save the log , send to ZF Help Desk and attach directly to the service case.



6 IT Global Service Desk (IT Global Service Desk)

To contact ZF IT Global Service Desk call 3600 (or site number + extension 3600*)

The IT Global Service Desk is available in multiple languages via phone. Always contact us by phone for URGENT issues relating to outages! (alternatively: +49 7541 77 3600)

English	24 hours a day, 7 days a week
German	Mon - Fri, 7am to 7pm CET
Spanish	Mon - Fri, 7am CET to 7pm CDT
Polish	Mon - Fri, 7am to 7pm CET
Romanian	Mon - Fri, 7am to 7pm CET
GSD Chat via IT HelpBot (English only)	24 hours a day, 7 days a week