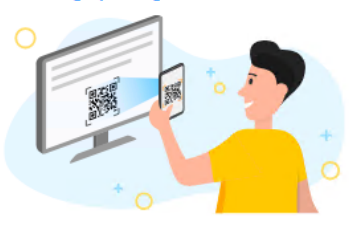


Zyxel IPSec VPN 2FA konfigurieren

Unter
Configuration
→ Objects →
User/Group
einen neuen
Benutzer
erfassen

General	Two-factor Authentication
User Configuration	
User Name :	vor.nachname
User Type:	user
Password:	
Retype:	
Description:	Local User
Email:	
Mobile Number:	
Authentication Timeout Settings	☒ Use Default Settings
Lease Time:	1440
Reauthentication Time:	1440

Im Reiter
«Two-factor
Authentication»
2FA aktivieren
und
konfigurieren

General	Two-factor Authentication
Two-factor Authentication for VPN Access	
☒ Enable Two-Factor Authentication for VPN Access	
Two-factor Auth. Method: Verify by SMS/Email/Google Authenticator (Please see VPN Access for more information)	
Two-Factor Authentication for Network Access	
Finish Setting up Google Authenticator to enable 2FA  Set up Google Authenticator	

Der angezeigte QR-Code funktioniert auch mit anderen 2FA Apps als Google Authenticator. Den QR-Code mit der App scannen und den generierten Code im dritten Feld eingeben	Two-Factor Authentication for Network Access Set up Google Authenticator Step 1 Download & install Google Authenticator on your mobile device.  Google Authenticator   Step 2 Add your account to Google Authenticator After clicking the "+" icon in Google Authenticator, use the camera to scan the QR code on the screen.  Can not scan the QR code? Step 3 Verify your device Enter code Verify code and finish
---	--

Unter
Konfiguration
→ VPN → IPsec
VPN unter
«VPN-
Gateway»
Ein neues
Gateway
hinzufügen

Einstellungen
gemäss
Screenshot
konfigurieren

Edit VPN Gateway GW_Dyn_2FA

Hide Advanced Settings Create New Object

General Settings

☒ Enable

VPN Gateway Name: GW_Dyn_2FA

IKE Version

☐ IKE

☒ IKEv2

Gateway Settings

My Address

☒ Interface

wan

Static -- 213.180.189.10/255.255.255.252

☐ Domain Name / IPv4

Peer Gateway Address

☐ Static Address

Primary 0.0.0.0Secondary 0.0.0.0

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: 300 (60-86400 seconds)

☒ Dynamic Address

Authentication

☐ Pre-Shared Key

unmasked

☒ Certificate

default

(See [My Certificates](#))

☒ Advance

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Advance

Proposal

+ Add Edit Remove

#	Encryption	Authentication
1	AES256	SHA512

Key Group: DH5

Extended Authentication Protocol

☒ Enable Extended Authentication Protocol

Allowed Auth Method: mschapv2

☒ Server Mode

AAA Method: default

Allowed User: vpn_user

☐ Client Mode

User Name :
Password:
Retype to Confirm:

☒ Enable Two-factor Authentication (See [VPN Access](#))

OK

Cancel

Danach im
Reiter «VPN-
Connection»
eine neue
Verbindung
hinzufügen

Einstellungen
gemäss
Screenshot
konfigurieren

Edit VPN Connection VPN_Dyn_2FA [?] [X]

☐ Hide Advanced Settings ☐ Create New Object

General Settings

☒ Enable

Connection Name:

Advanced

☐ Natted-Up

☐ Enable Replay Detection

☐ Enable NetBIOS broadcast over IPSec

MSS Adjustment

☐ Custom Size (200 - 1460 Bytes)

☒ Auto

☒ Narrowed

VPN Gateway

Application Scenario

☐ Site-to-site

☐ Site-to-site with Dynamic Peer

☒ Remote Access (Server Role)

☐ Remote Access (Client Role)

☐ VPN Tunnel Interface

VPN Gateway: wan 0.0.0.0, 0.0.0.0

Policy

Local Policy: INTERFACE SUBNET, 10.0.0.0/23

Advanced

☐ Enable GRE over IPSec ⓘ

Configuration Payload

☒ Enable Configuration Payload

IP Address Pool: SUBNET, 10.10.0.0/24 ⓘ

First DNS Server (Optional):

Second DNS Server (Optional):

First WINS Server (Optional):

Second WINS Server (Optional):

☒ Allow Traffic Through WAN Zone

Phase 2 Setting

SA Life Time: (180 - 3000000 Seconds)

Advanced

Active Protocol:

Encapsulation:

Proposal

#	Encryption	Authentication
1	AES256	SHA512

Perfect Forward Secrecy (PFS): ⓘ

Related Settings

Zone: ⓘ

Advanced

Inbound/Outbound traffic NAT

Outbound Traffic

☐ Source NAT

Source:

Destination:

SNAT:

Inbound Traffic

☐ Source NAT

Source:

Destination:

SNAT:

☐ Destination NAT

#	Original IP	Mapped IP	Protocol	Original Port ...	Original Port ...	Mapped Por...	Mapped Por...
No data to display							

Page 0 of 0 Show 50 items

OK Cancel

Im Reiter
«Configuration
Provisioning»
die Funktion
aktivieren und
die soeben
erstellte VPN-
Konfiguration
freigeben

VPN Connection
VPN Gateway
Concentrator
Configuration Provisioning

General Settings

☒ Enable Configuration Provisioning
VPN Provisioning Port:
(1...65535)

Authentication

Client Authentication Method:

Configuration

Note:
Upload Bandwidth Limit only applies to subscription-based SecuExtender IPSec VPN client versions: 5.6.80.007 or higher (for Windows), 1.2.0.7 or higher (for macOS).

Add
Edit
Remove
Activate
Inactivate
Move

#	Status	Priority	VPN Connection	Upload Bandwidth Limit (1-1048576 Kbps)	Allowed User
1	🔔	1	VPN_Dyn_2FA		vpn_user

⏪

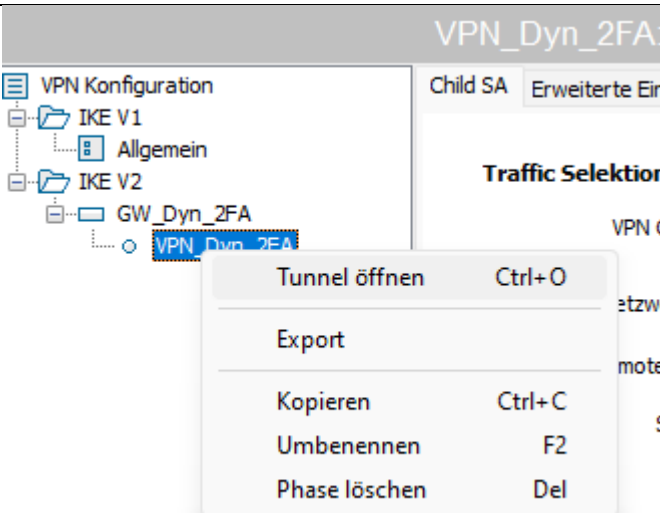
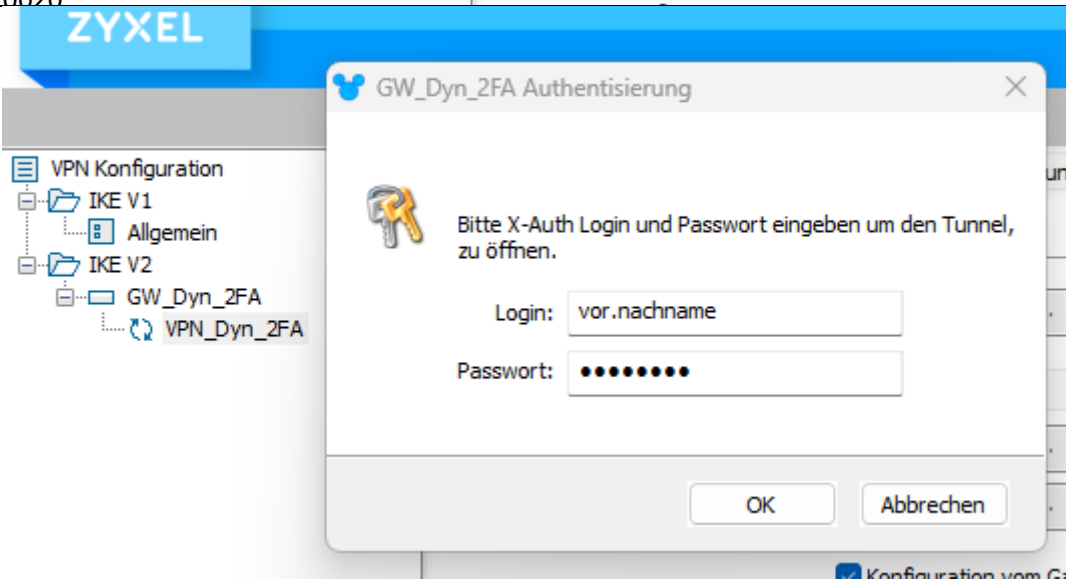
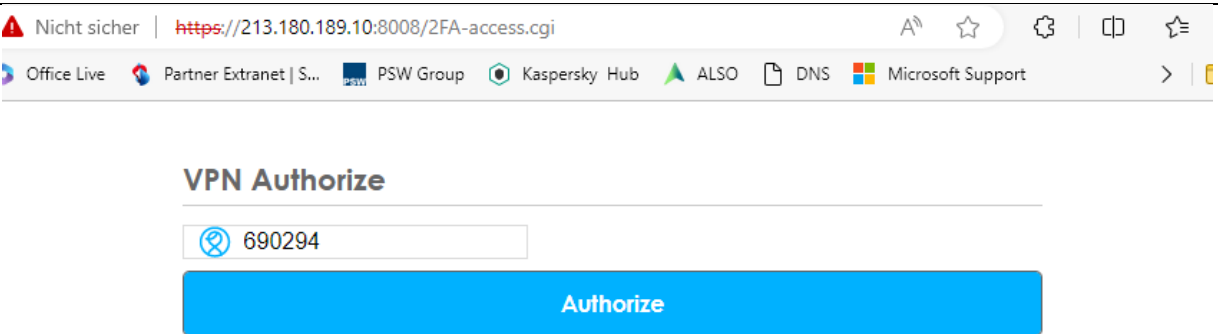
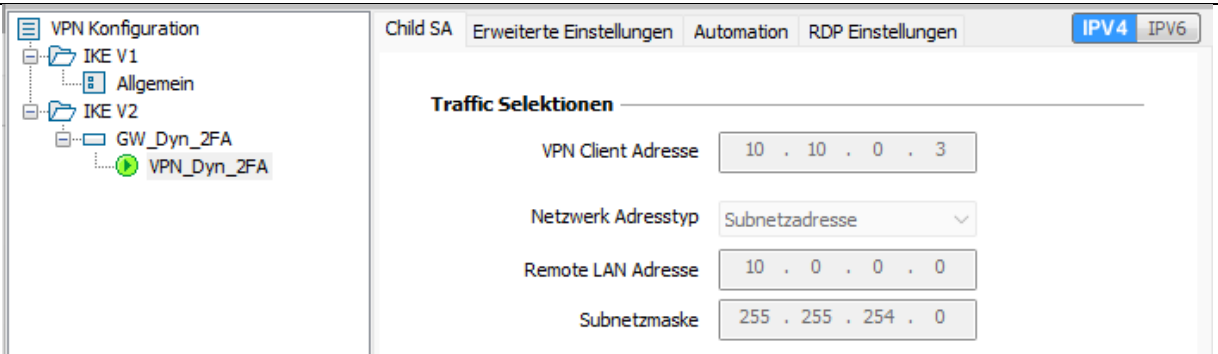
Page 1 of 1

⏩

Show 50 items

Auf dem VPN Client

ZyWALL IPSec VPN Client auf dem PC installieren Nach erfolgreicher Installation über Konfiguration -> Beziehen von Server	ZyWALL IPSec VPN Client KonfigurationTools? SpeichernCtrl+S Importieren Exportieren Beziehen von Server VPN Konfigurationsdatei auf USB verschieben Konfigurationsassistent Beenden
--	---

Jetzt sollte die Konfiguration ersichtlich sein Verbindung herstellen	
Mit Benutzernamen und Passwort anmelden	
Es sollte der Browser mit folgenden Login Fenster aufgehen Mit 2FA Code autorisieren	
Jetzt sollte die Verbindung stehen	

Weitere Hilfestellung:

<https://support.zyxel.eu/hc/de/articles/5738704012050-VPN-IKEv2-mit-Zertifikat-konfigurieren-On-Premise-Firewall-mit-2FA->