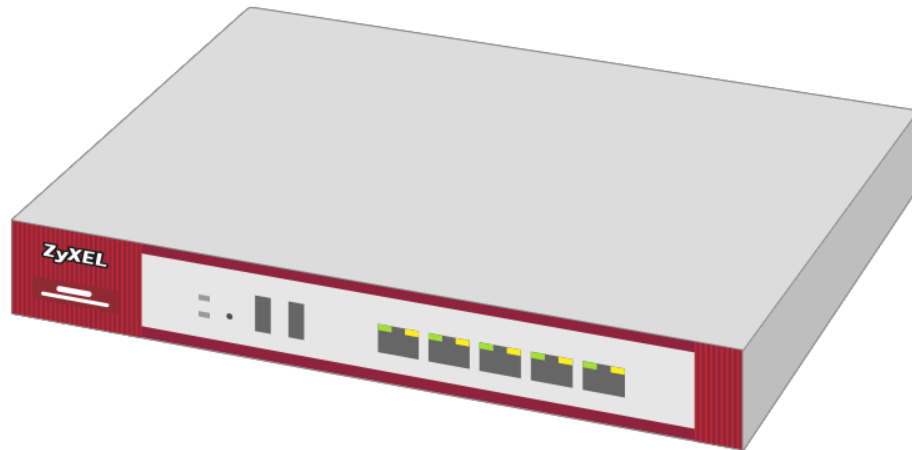


ZYXEL

Your Networking Ally



VPN 2FA mit SMS (eCall)

Zyxel Firewall-Serie

Knowledge Base KB-3825

Januar 2023

© Zyxel Corporation

2FA MIT SMS ÜBER ECALL

Die Zyxel Firewall-Serie bietet die Möglichkeit einer 2FA-Authentifizierung über SMS für VPN- und Admin-Zugriff. Es können lokale User der Firewall verwendet werden, aber auch AD oder Radius User.

ECALL PORTAL

Unter <https://portal.ecall-messaging.com/ecall/> kann ein eCall Account eröffnet werden. Die Eröffnung des Kontos ist in sehr kurzer Zeit vollzogen.

Ist der Account eröffnet, kann unter Schnittstellen > E-Mail-Schnittstelle über die Schaltfläche «Adresse hinzufügen» die Absender-Adresse der Firewall erfasst werden. Zusätzlich muss die Option „Ich lasse zu, dass Meldungen mittels E-Mail über mein eCall-Konto versendet werden.“ aktiviert sein.

Es sind keine weiteren Einstellungen erforderlich.

eCall Business Messaging – Smart. Easy. Integrated.

Einstellungen: Zugang via E-Mail

Um per E-Mail Aufträge über eCall auslösen zu können, müssen Sie hier die entsprechenden E-Mail-Adressen eintragen und die entsprechenden Zugänge aktivieren. Hilfreiche Hinweise finden Sie [hier](#).

Ich lasse zu, dass Meldungen mittels E-Mail über mein eCall-Konto versendet werden.

Speichern

Zugangseinstellungen

	SMS				Fax			Threema	Voice	
	Empfänger im An-Feld ?	Empfänger im Betreff-Feld ?	Empfängerliste im Textfeld ?	Weiterleitung ?	Empfänger im An-Feld ?	Empfänger im Betreff-Feld ?	Weiterleitung ?	Empfänger im An-Feld ?	Empfänger im An-Feld ?	Konfigurations-änderungen ?
Erlaubte E-Mail-Adressen:										
user@mydomain.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Adresse hinzufügen

Hinweise

- Weitere Einstellungen vornehmen (Absenderdaten etc.).
- Zugang der Mail-Adresse löschen.

Hilfe | Zusatzbefehle

21.12.2022

NOTIFICATION SERVER

[Configuration](#) > [System](#) > [Notification](#)

Mail Server

Mail Server SMS Response Message

CONFIGURATION

- + Licensing
- + Wireless
- + Network
- + VPN
- BWM
- Web Authentication
- + Security Policy
- + Security Service
- + Object
- + Mgmt. & Analytics
- System
 - Host Name
 - USB Storage
 - Date/Time
 - Console Speed
 - DNS
 - WWW
 - SSH
 - TELNET
 - FTP
 - SNMP
 - Auth. Server
 - Notification**
 - Language

General Settings

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Subject: Append system name Append date time

Mail Server Port: TLS Security STARTTLS Authenticate Server

Mail From: (Email Address)

SMTP Authentication

User Name :

Password:

Retype to Confirm:

Schedule

Time For Sending Report: (hours) (minutes)

Richten Sie zuerst einen E-Mail-Server für den Mail Versand ein. In der Regel wird Port 587 für den Versand verwendet sowie TLS Security und allenfalls STARTLS.

Ob der Mail Server korrekt eingerichtet ist, kann z.B. durch den Versand eines Daily Report überprüft werden.

SMS

Mail Server | **SMS** | Response Message

CONFIGURATION

- + Licensing
- + Wireless
- + Network
- + VPN
- BWM
- Web Authentication
- + Security Policy
- + Security Service
- + Object
- Mgmt. & Analytics
- System
 - Host Name
 - USB Storage
 - Date/Time
 - Console Speed
 - DNS
 - WWW
 - SSH
 - TELNET
 - FTP
 - SNMP
 - Auth. Server
- Notification
 - Language
 - IPv6
 - ZON
- + Log & Report

General Settings

Enable SMS

Default country code for phone number: (1-4) digit

SMS Provider: [Email-to-SMS Provider](#)

Provider Domain: auto append to "Mail to" (Optional)

Mail Subject: (Optional)

Mail From: (Optional)

Mail To:

Note

1. If you select to use an Email-to-SMS provider, configure a mail server before you enable SMS.
2. If you leave the Mail From field blank here, the system automatically uses the mail address configured in the Mail Server screen.
3. "Mail To" default format is "\$mobile_number\$@provider domain" and some Service Providers might require prefix symbol like "+" added before \$mobile_number\$.
4. ViaNett Service is about to end of support, please stop purchase new ViaNett credits.

Für eCall können folgende Einstellungen verwendet werden:

Enable SMS	aktivieren
Default contry code for phone number:	41 für Schweiz
Provider Domain:	sms.ecall.ch
Auto append to «mail to»	aktivieren
Mail Subject:	+\$mobile_number\$
Mail from:	E-Mail-Adresse, welche im eCall-Portal erfasst ist. idealerweise ist dieses identisch mit der E-Mail-Adresse in den Mail-Server-Einstellungen.
Mail To:	+\$mobile_number\$

Als «Default contry code for phone number» kann auch «0» eingesetzt werden.

Die Telefonnummer des Users muss dann jedoch mit der Vorwahl («+xx») definiert werden, z.B. +41761234567.

User Einstellungen

[Configuration](#) > [Object](#) > [User/Group](#) > [User](#)

Auf dem User wird eine Mobile-Nummer im Format 0761234567 hinzugefügt.

+ Edit User cab

General

Two-factor Authentication

User Configuration

User Name :	cab
User Type:	user ▼
Password:	••••••••
Retype:	••••••••
Description:	Local User
Email:	vpn@mydomain.com
Mobile Number:	0761234567
Authentication Timeout Settings	<input checked="" type="radio"/> Use Default Settings <input type="radio"/> Use Manual Settings
Lease Time:	1440 minutes
Reauthentication Time:	1440 minutes

Zusätzlich wird 2FA aktiviert.

+ Edit User cab ? X

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)

View your backup codes

These codes will allow you to log in if you don't have access to the application or your mobile device. Please record them in a safe place.

TWO-FACTOR AUTHENTICATION

Configuration > Object > Auth. Method > Two-factor Authentication > VPN Access

Die Funktion muss grundlegend eingeschaltet sein.

Anschliessend wird bestimmt, für wen und welche Verbindung 2FA aktiv sein soll.

«Authorized Link URL» ist die Adresse, welche in der SMS-Nachricht definiert ist.

Ein Zugriff von extern muss über den angegebenen Port von extern möglich sein.

Für eCall muss die Option «Use Multilingual file» verwendet werden.

Das Vorlage-File kann über den Download Link bezogen und angepasst werden.

Anschliessend kann das File wieder auf die Firewall geladen werden.

Das File muss den Platzhalter **<url>** zwingend beinhalten.

Folgende Platzhalter können verwendet werden:

<url> Authoriz Link URL Address

<user> User, welcher sich für 2FA angemeldet hat

<host> Name der Firewall ([Configuration > System > Host Name](#))

<Time> Valid Time > Zeit, in der sich der Client authentifizieren kann.

SECURITY POLICY

[Configuration](#) > [Security Policy](#) > [Policy Control](#)

Für die Authentifizierung mittels 2FA muss eine Security Policy erstellt werden

10	🔍	_2FA	WAN	ZyWALL	Schweiz	any	Wiz_2FA	any	cob	none	allow
----	---	------	-----	--------	---------	-----	---------	-----	-----	------	-------

From: wan
 To: ZyWALL
 Source: kann allenfalls eingeschränkt werden, z.B. auf Schweiz
 Service: Wiz_2FA (Port passt sich dynamisch an, wenn dieser im 2FA Menu geändert wird)
 Action: allow

HTTPS EINSTELLUNGEN

[Configuration](#) > [System](#) > [WWW](#) > [HTTPS](#) > [User Service Control](#)

Der Zugriff muss für das «User Service Control» aus der Zone «WAN» oder «ALL» zugelassen sein.

Service Control Login Page

HTTPS

Enable

Server Port:

Authenticate Client Certificates (See [Installed CAs](#))

Server Certificate:

Redirect HTTP to HTTPS

Admin Service Control

[Add](#) [Edit](#) [Remove](#) [Move](#)

#	Zone	Address	Action
1	LAN1	LAN1_SUBNET	accept
2	TUNNEL	Remote_Admin_PC	accept
3	WAN	STAG	accept
4	WAN	Public_Remote_Access	accept
5	ALL	ALL	deny
-	ALL	ALL	accept

Page 1 of 1 | Show 50 Items | Displaying 1 - 6 of 6

User Service Control

[Add](#) [Edit](#) [Remove](#) [Move](#)

#	Zone	Address	Action
-	ALL	ALL	accept

Page 1 of 1 | Show 50 Items | Displaying 1 - 1 of 1

VPN GATEWAY

[Configuration](#) > [VPN](#) > [IPSec VPN](#) > [VPN Gateway](#)

Für IPSec VPN (L2TP/IKEv1/IKEv2) muss 2FA im VPN Gateway aktiviert sein.

