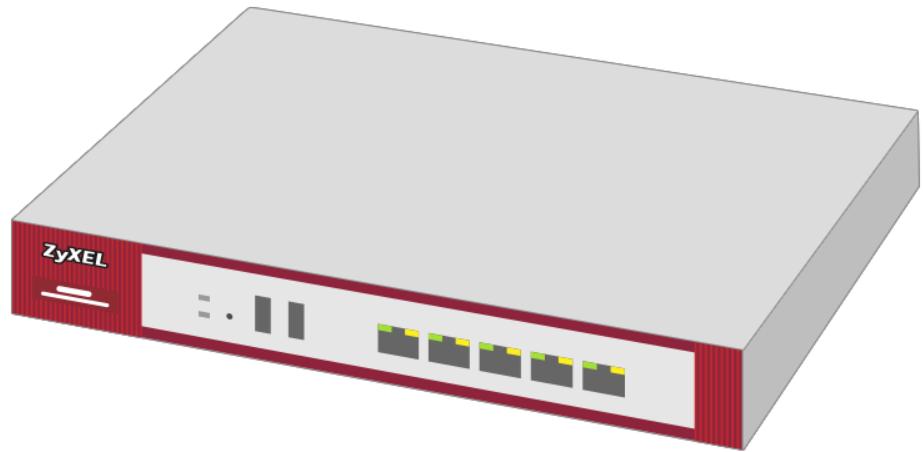


ZYXEL

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.

The screenshot shows the eCall Portal interface. The left sidebar includes links for Dashboard, Messaging (Senden), Schnittstellen (Overview, E-Mail-Schnittstelle, OMS-Schnittstelle), Nummern, Logbuch, Adressbuch, Account (Konto FREE, Punkte kaufen, Statistiken, Extras, Einstellungen), and general help links. The main content area has a header "Einstellungen: Zugang via E-Mail". It contains a note about entering email addresses and activating logins. A checkbox "Ich lasse zu, dass Meldungen mittels E-Mail über mein eCall-Konto versendet werden." is checked and highlighted with a red border. Below this is a "Speichern" button. The "Zugangseinstellungen" section shows a table for "Erlaubte E-Mail-Adressen" with one entry: "user@mydomain.com". This entry has checkboxes for "Empfänger im An-Feld" and "Empfänger im Betreff-Feld" both checked and highlighted with a red border. The table also includes columns for SMS, Fax, Threema, Voice, and Konfigurationsänderungen. At the bottom, there's a "Hinweise" section with links for "Weitere Einstellungen vornehmen (Absenderdaten etc.)" and "Zugang der Mail-Adresse löschen". A footer at the bottom of the page shows "21.12.2022".

NOTIFICATION SERVER

Configuration > System > Notification

Mail Server

General Settings

- Mail Server: smtp.mydomain.com (Outgoing SMTP Server Name or IP Address)
- Mail Subject: Append system name Append date time
- Mail Server Port: 587 TLS Security STARTTLS Authenticate Server
- Mail From: user@mydomain.com (Email Address)

SMTP Authentication

- User Name : user@mydomain.com
- Password: *****
- Retype to Confirm: *****

Schedule

Time For Sending Report: 0 (hours) 0 (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

The screenshot shows the Zyxel device's configuration interface with the following details:

- Left Sidebar:** Shows the navigation tree with sections like Configuration, System, and Notification.
- Top Bar:** Shows tabs for Mail Server, SMS, and Response Message. The SMS tab is active.
- General Settings:**
 - Enable SMS:** Checked.
 - Default country code for phone number:** Set to 41 (1-4 digit).
 - SMS Provider:** Set to Email-to-SMS Provider.
 - Provider Domain:** sms.ecall.ch
 - Mail Subject:** +\$mobile_number\$
 - Mail From:** user@mydomain.com
 - Mail To:** +\$mobile_number\$ @sms.ecall.ch
 - Auto append to "Mail to":** Checked.
- Note:**
 - If you select to use an Email-to-SMS provider, configure a mail server before you enable SMS.
 - If you leave the Mail From field blank here, the system automatically uses the mail address configured in the Mail Server screen.
 - Mail To default format is '\$mobile_number\$@provider domain' and some Service Providers might require prefix symbol like '+' added before \$mobile_number\$.
 - 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 country 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 country 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

Lease Time:	1440	minutes
Reauthentication Time:	1440	minutes

Use Default Settings Use Manual Settings

Zusätzlich wird 2FA aktiviert.

Edit User cab

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

The screenshot shows the Zyxel Firewall's configuration interface under the 'Object' section. The 'Auth. Method' tab is selected. The 'Two-factor Authentication' tab is active. The 'VPN Access' sub-tab is selected. In the 'General Settings' section, the 'Enable' checkbox is checked. The 'Valid Time' is set to 3 minutes. Under 'Two-factor Authentication for Services', all three options are checked: 'SSL VPN Access', 'IPSec VPN Access', and 'L2TP/IPSec VPN Access'. In the 'User/Group' section, 'radius-users' and 'admin' are selected. Under 'Delivery Settings', the 'Authorized Port' is set to 8008. A note at the bottom provides instructions for using placeholders in messages.

Note:

- 1.The Default Message must use alphanumeric characters.
- 2.The Multilingual file must be in UTF-8 format and named '2FA-msg.txt'.
- 3.The Default Message and the Multilingual file must contain a <url> tag. You can also use <user>/<host>/<time> variables to
- 4.The Default Message and the Multilingual file do not support HTML tags such as
, <i>, and so on.

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

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.

The screenshot shows the ZyWALL web interface with the following sections visible:

- Service Control**: Shows the "Login Page" tab selected. Under "HTTPS", the "Enable" checkbox is checked, "Server Port" is set to 443, and "Authenticate Client Certificates" is unchecked. "Server Certificate" is set to "bloom-reven". "Redirect HTTP to HTTPS" is checked. The "Admin Service Control" table lists zones and their actions:

#	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

 The "User Service Control" table shows a single entry for "ALL" with an "accept" action.

VPN GATEWAY

Configuration > VPN > IPSec VPN > VPN Gateway

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

