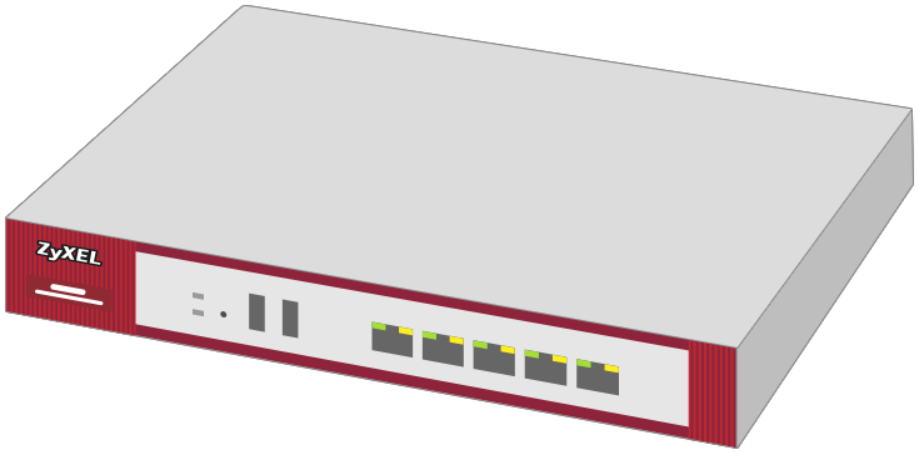
ZYXEL
Your Networking Ally



VPN 2FA mit SMS (eCall)

Zyxel Firewall-Serie

Knowledge Base KB-3825
Januar 2023

2FA MIT SMS ÜBER ECALL

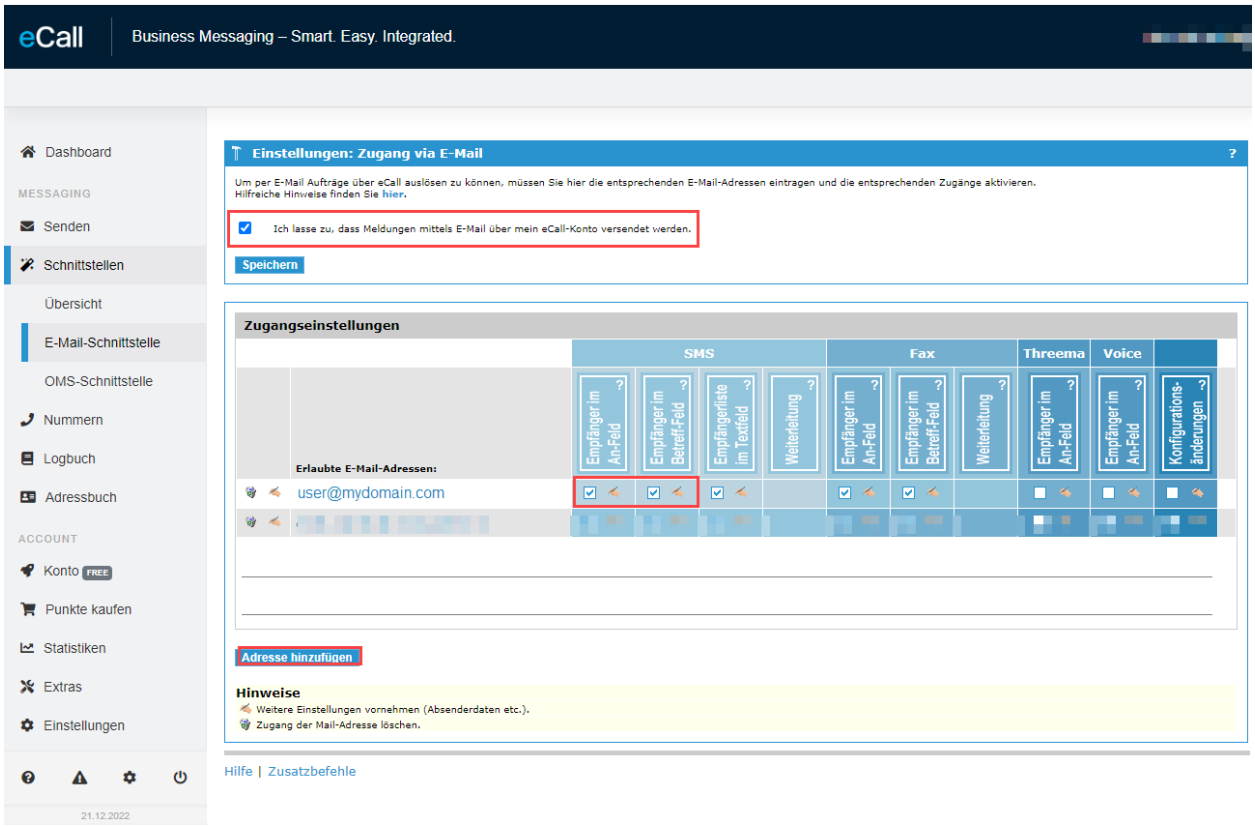
Die Zyxel Firewall-Serie bietet die Möglichkeit einer 2FA-Authentifizierung über SMS für VPN- und Admin-Zugriff. Es können lokale User der Firewall verwendet werden, aber auch AD oder Radius User.

ECALL PORTAL

Unter https://portal.ecall-messaging.com/ecall/ kann ein eCall Acount 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.

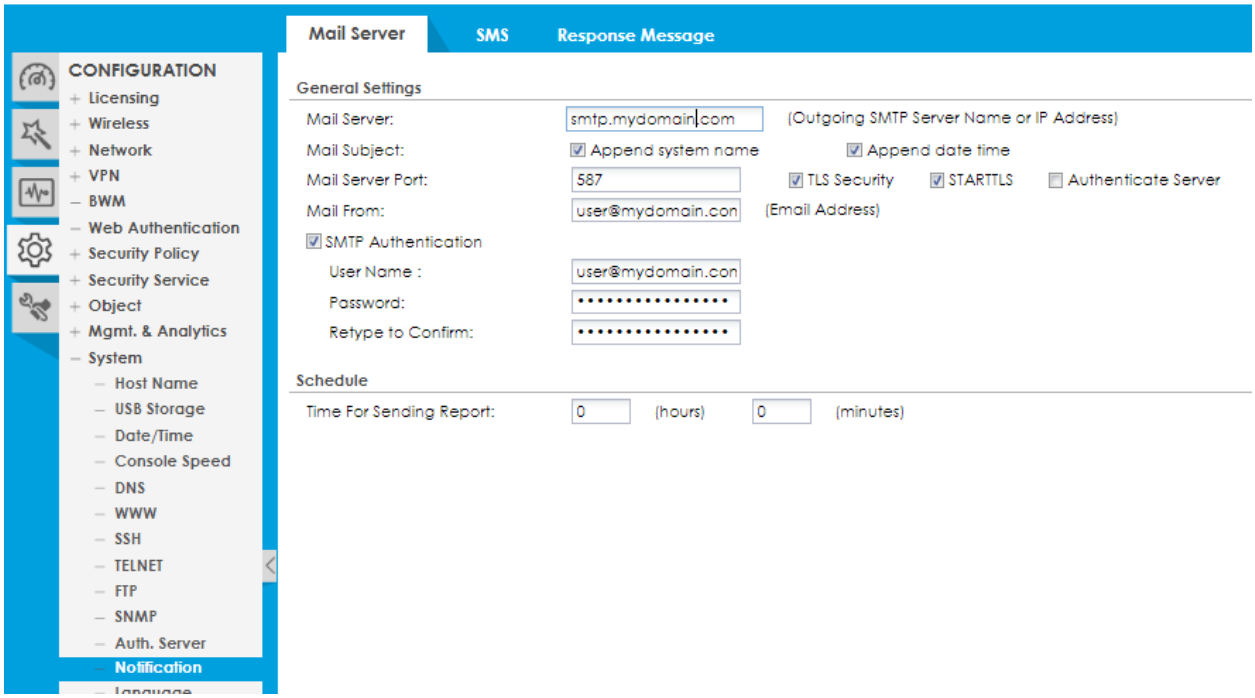
Es sind keine weiteren Einstellungen erforderlich.



NOTIFICATION SERVER

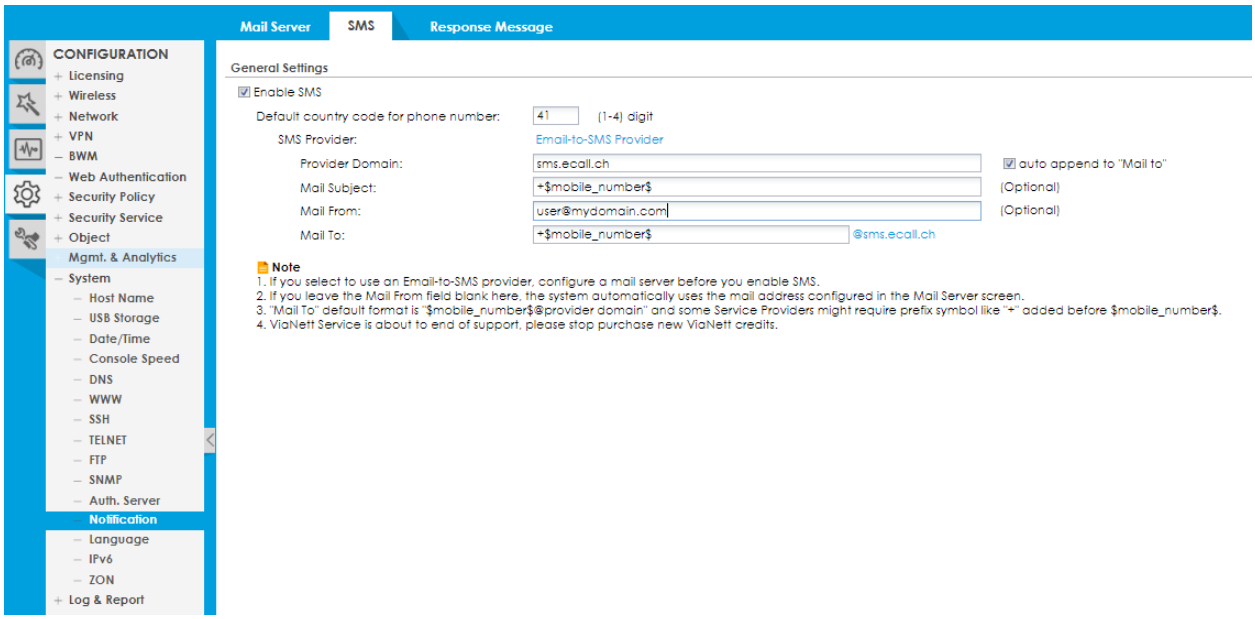
Configuration > System > Notification

Mail Server



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



Für eCall können folgende Einstellungen verwendet werden:

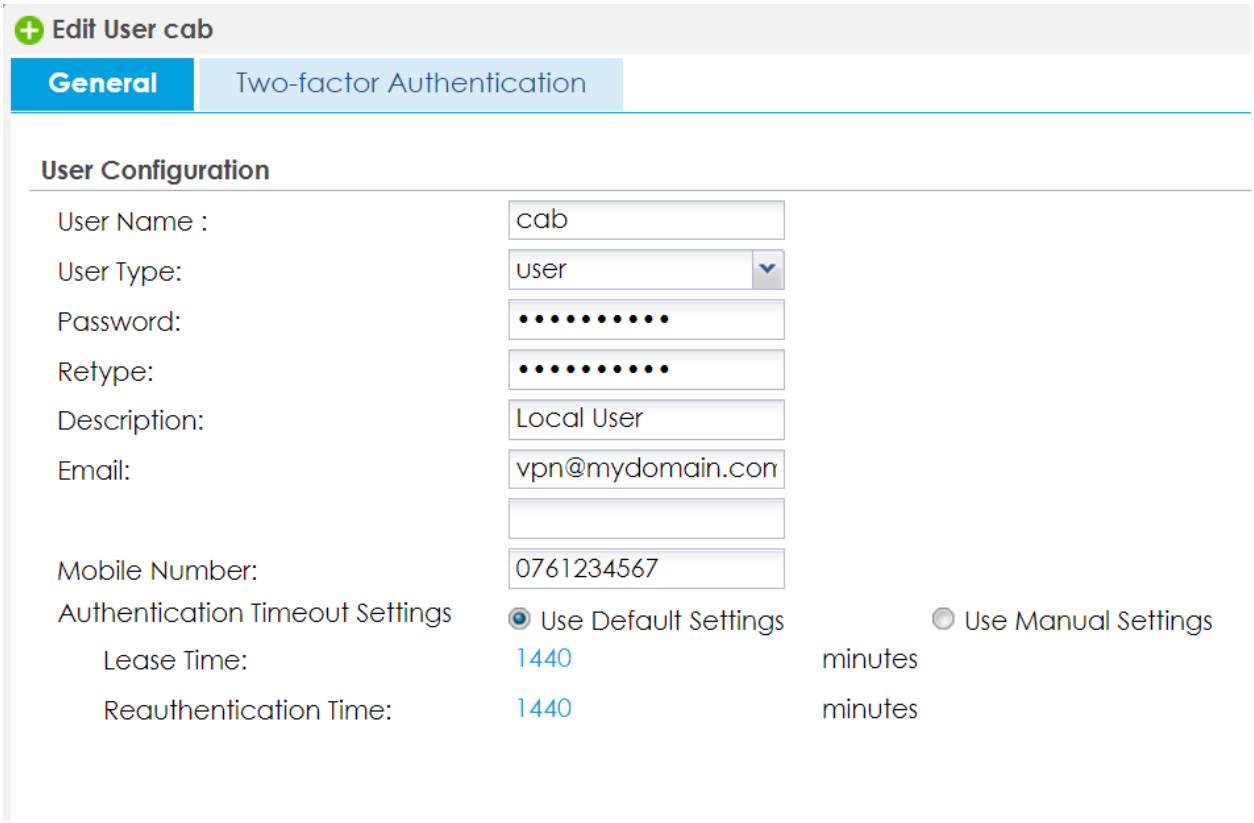
Enable SMS	aktivieren
Default contry code for phone number:	41 für Schweiz
Provider Domain:	sms.ecall.ch
Auto append to «mail to»	aktivieren
Mail Subject:	+$mobile_number$
Mail from:	E-Mail-Adresse, welche im eCall-Portal erfasst ist. idealerweise ist dieses identisch mit der E-Mail-Adresse in den Mail-Server-Einstellungen.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

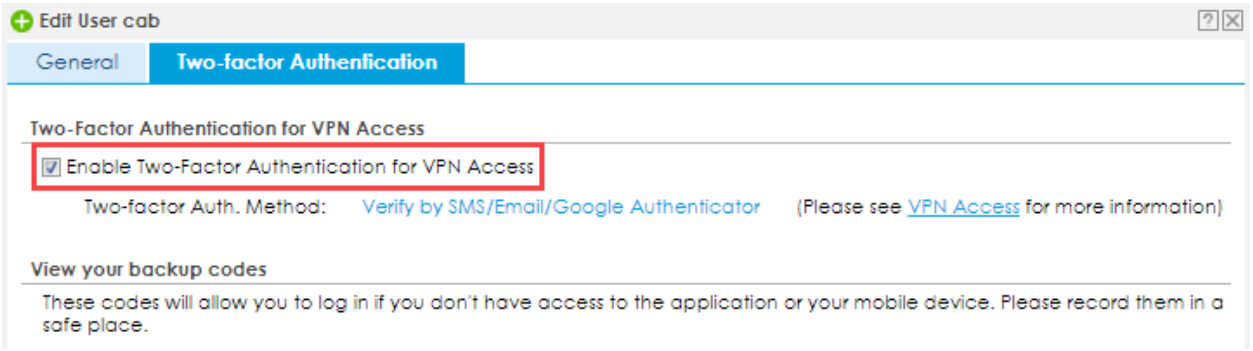
User Einstellungen

Configuration > Object > User/Group > User

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

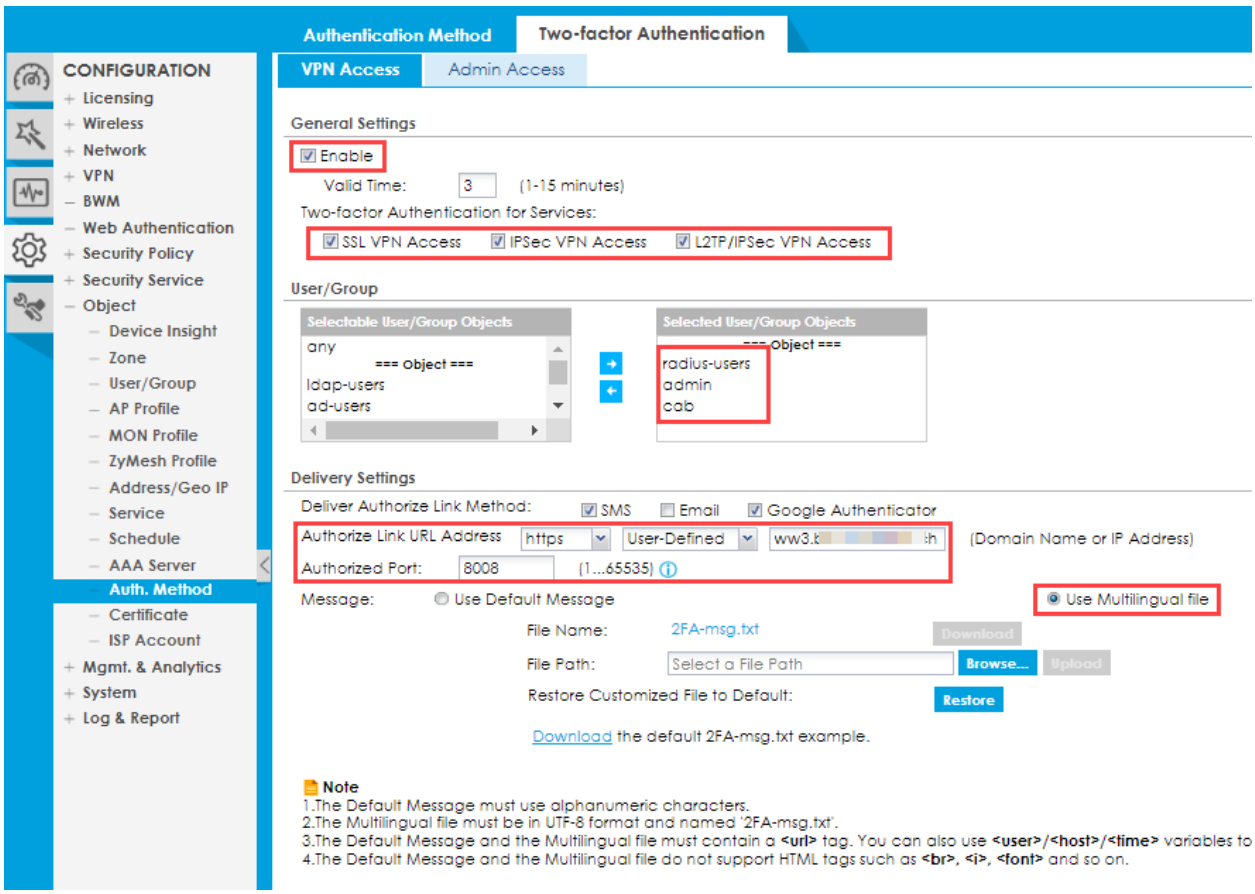


Zusätzlich wird 2FA aktiviert.



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

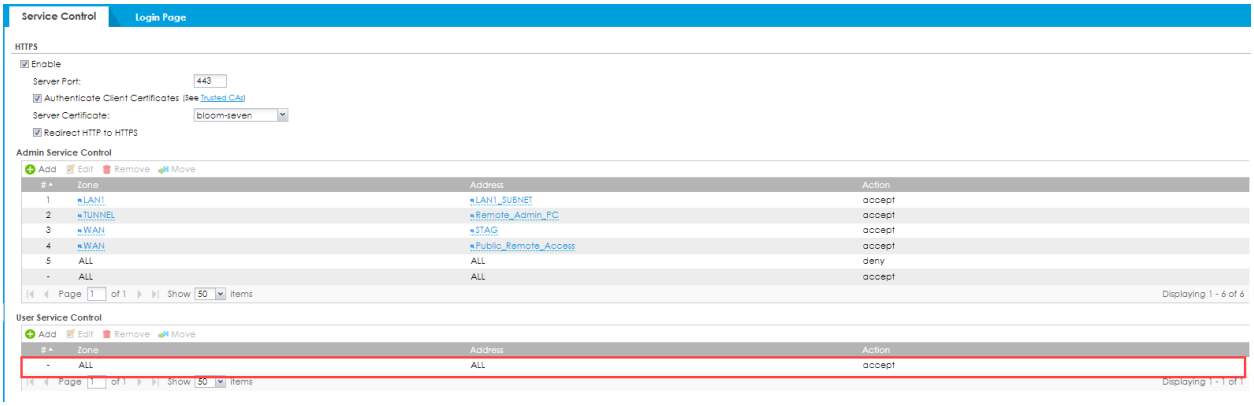
Für die Authentifizierung mittels 2FA muss eine Security Policy erstellt werden

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.



VPN GATEWAY

Configuration > VPN > IPSec VPN > VPN Gateway

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