

HERHSIANG

NGS 系列新世代防火牆

2022

企業系統第一防線，支援雙因子認證 2FA



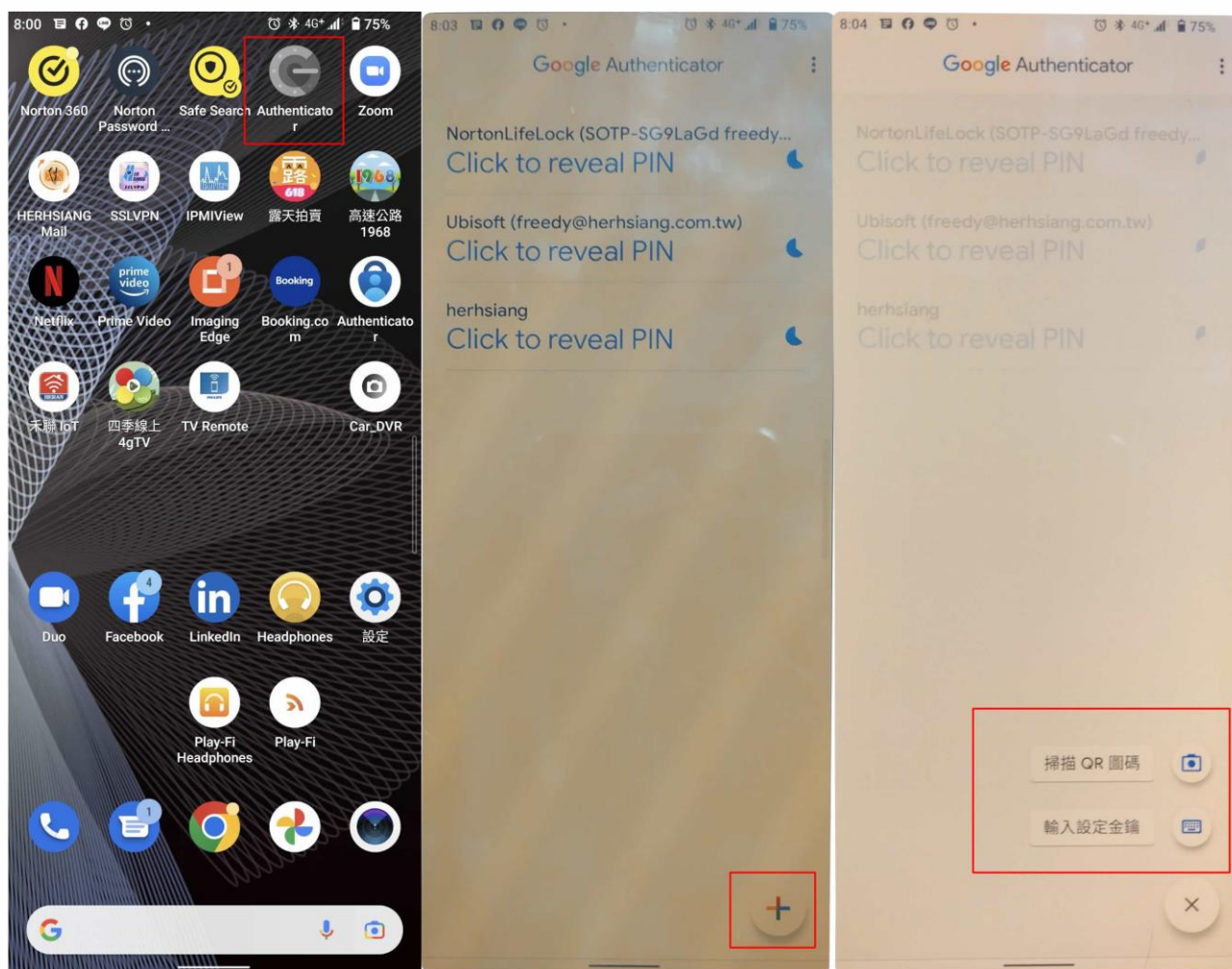


不同於以往許多網路服務預設使用單因素之密碼認證，

雙因子認證(Two-Factor Authentication, 2FA)，結合兩種不同身分驗證方式，使用者需通過兩種以上的認證機制後，才能得到授權存取服務方所提供的系統資源。而驗證的方式很多種，如 PIN 碼、指紋、掃描 QR code、或一次性代碼等輔助驗證，而目的都是為帳戶提供更高的安全性。

禾翔資訊 NGS 新世代防火牆設備使用者可透過韌體版本更新至 v9.0.2.2.以上(依型號不同，支援版本不同)，此雙因子驗證功能結合 **Google Authenticator**，透過使用者所擁有的手機作為第二個驗證因素，來達到輔助驗證。功能預設關閉，啟用此功能後，系統會提示您輸入密碼與和一次性代碼，方可存取您的帳戶。禾翔 NGS 防火牆有三個部分，支援兩步驟驗證：帳號管理、上網認證、SSL VPN，依序介紹如下。

手機 Google 或 IOS 商店街下載

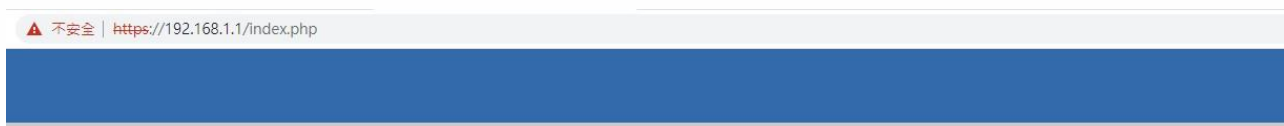


帳號管理

步驟 1. 請至系統設定>基本設定>管理介面存取設定，新增管理者帳號兩步驟驗證進行設定。(管理者可選擇每次登入都要做兩步驟驗證，或是驗證成功後，多久時間內可以不用再做二次驗證。)



範例 1:每次登入都要做兩步驟驗證,使用 Google Authenticator App 掃描 QR Code 或產生驗證碼，輸入驗證碼。(啟用驗證沒啟用金鑰)



兩步驟驗證

請使用 Google Authenticator App

掃描QR Code

或輸入金鑰

顯示金鑰

帳號 herhsiang

驗證碼

確定



HERHSIANG NGS

帳號

密碼

勿忘密碼

☐ ☐ ☐ ☐ ☐

☒ 記住登入帳號

繁體中文 ▼

系統登入

Copyright © 2010 HERHSIANG Information Co., LTD. All rights reserved.

範例 2: 驗證成功後，多久時間內可以不用再做二次驗證。

HERHSIANG NGS

帳號

密碼

☐ 記住登入帳號

繁體中文 ▼

系統登入

Copyright © 2010 HERHSIANG Information Co., LTD. All rights reserved.

上網認證

步驟 1. 請至管理目標>上網認證>本機使用者& POP3, IMAP 伺服器列表，啟用二步驟驗證後，使用者輸入帳與密後，需要再輸入 Google Authenticator 所產生的驗證碼，驗證全部完成後，才算登入成功。

範例 1: 使用 POP3 通訊協定

HERHSIANG INFORMATION

管理目標 > 上網認證

POP3, IMAP 伺服器設定

網域名稱: herhsiang.com.tw

伺服器: mail.herhsiang.com.tw ex: 74.125.53.109 或 pop.gmail.com

登入帳號附加網域: ☒

通訊協定: ☒ POP3 ☐ IMAP

安全性: ☐ 一般 ☐ TLS ☒ SSL

通訊埠: 995

連線: ☒ 勾選

連接測試

啟用

啟用	使用者帳號	金鑰資訊
☒	herhsiang	未啟用 產生金鑰

全部啟用 全部關閉 1/1 列表 1 頁數 每頁 16 條

儲存

範例 2: 使用 IMAP 通訊協定

HERHSIANG INFORMATION

管理目標 > 上網認證

POP3, IMAP 伺服器設定

網域名稱: herhsiang.com.tw

伺服器: mail.herhsiang.com.tw ex: 74.125.53.109 或 pop.gmail.com

登入帳號附加網域: ☒

通訊協定: ☐ POP3 ☒ IMAP

安全性: ☐ 一般 ☐ TLS ☒ SSL

通訊埠: 993

連線: ☒ 勾選

連接測試

啟用

啟用	使用者帳號	金鑰資訊
☒	herhsiang	2022-06-22 19:12:39 已啟用 顯示金鑰 移除金鑰

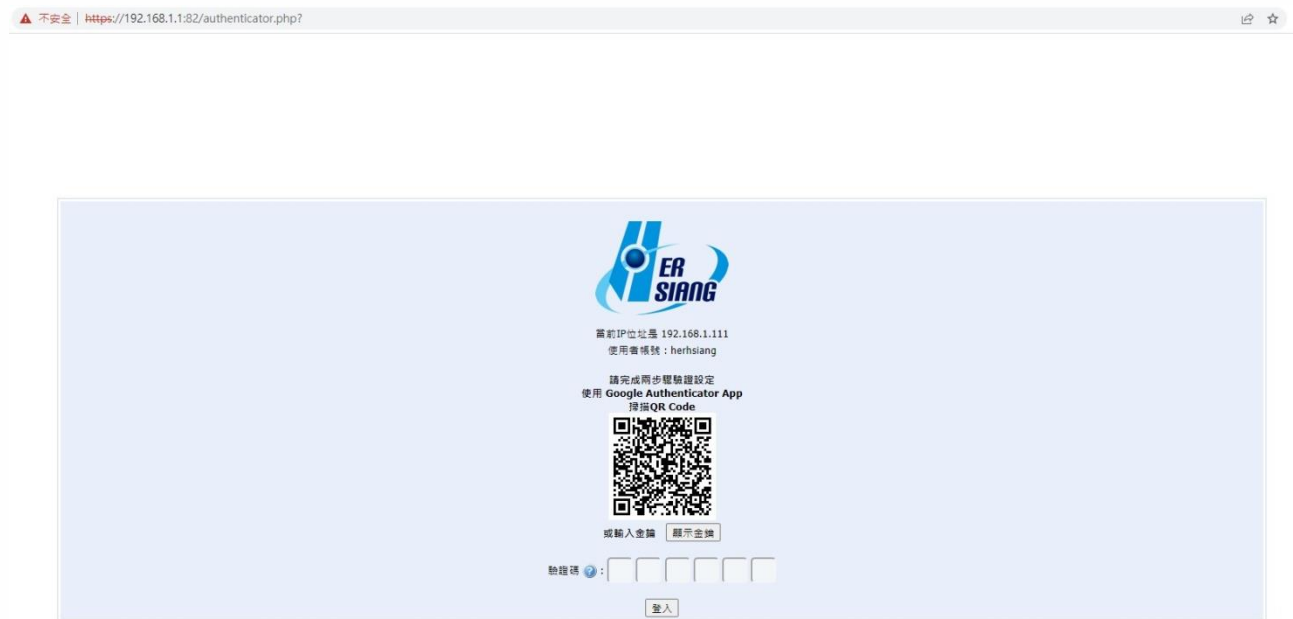
全部啟用 全部關閉 1/1 列表 1 頁數 每頁 16 條

儲存



步驟 2.

-當首次啟用兩步驟驗證(尚未產生金鑰時)或更換金鑰後：驗證畫面將會自動建立金鑰給使用者設定。



-當金鑰已產生時：驗證頁面不會顯示金鑰資訊。



請注意：驗證碼可容許時間差為 1 分鐘。

SSL VPN

步驟 1. 請至 VPN > SSL VPN Server- sslvpn.php 登入帳號與密碼，增加輸入驗證碼之後才能進入下載頁面（請參考前段的驗證圖示）。



步驟 2. 當啟用兩步驟驗證時，SSL VPN 連線軟體密碼欄位需輸入**密碼+驗證碼**，使用者可以參考 **SSL VPN Client 軟體兩步驟驗證說明連結**來開啟說明文件。

