InternetNow!

HORNETSECURITY

GUIDE ON ENFORCING MULTI-FACTOR AUTHENTICATION (MFA) FOR ADMINISTRATORS IN HORNETSECURITY

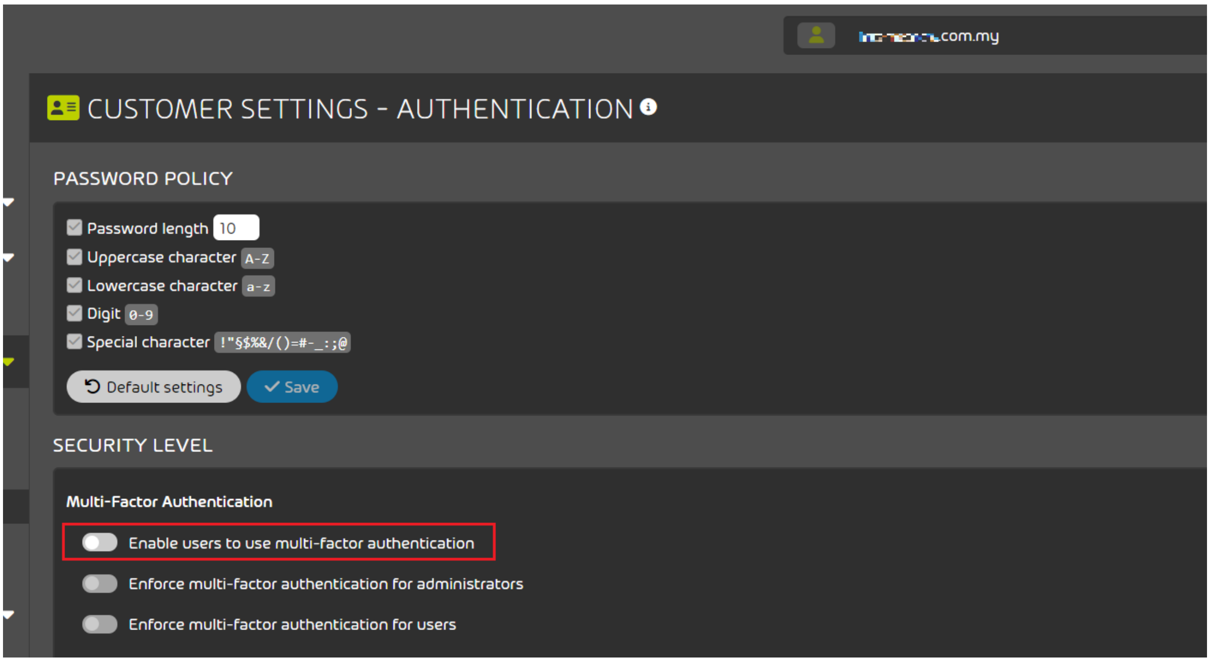
Multi-factor authentication increases security for the Control Panel login. We recommend in particular that administrators use multi-factor authentication.

Multi-factor authentication in the Control Panel uses the TOTP method. TOTP stands for **time-based one-time passwords**. In order to log in to the Control Panel using multi-factor authentication, you must enter a one-time-password from an authenticator app in addition to the Control Panel password.

IMPORTANT: Please **install a TOTP authenticator app (e.g., Microsoft Authenticator, Google Authenticator) on your mobile device** prior to following this guide.

ENABLING MULTI FACTOR AUTHENTICATION (MFA)

1. Log in to the Control Panel with your administrative credentials.
2. From the *scope selection*, select the domain for which you would like to enable multi-factor authentication.
3. Navigate to **Customer Settings** > **Authentication**.
4. Toggle the switch **Enable users to use multi-factor authentication** under **Multi-Factor Authentication.**



[redacted].com.my

CUSTOMER SETTINGS - AUTHENTICATION

PASSWORD POLICY

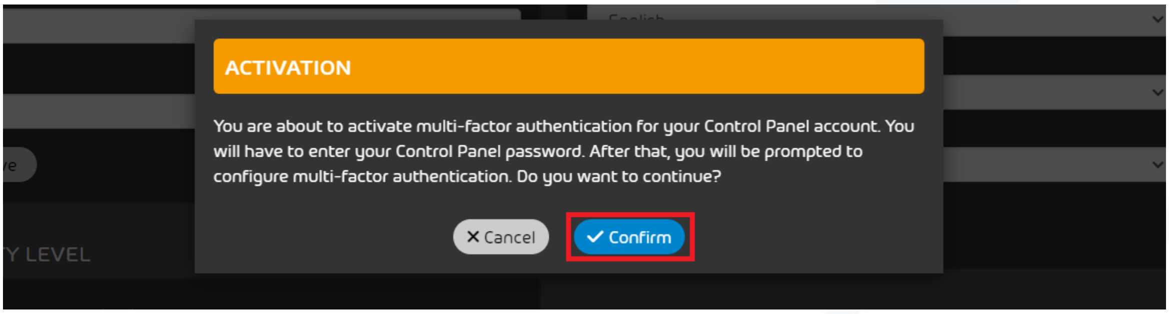
☑ Password length 10
☑ Uppercase character A-Z
☑ Lowercase character a-z
☑ Digit 0-9
☑ Special character !"§$%&/()=#-_:;@

SECURITY LEVEL

Multi-Factor Authentication

○ Enable users to use multi-factor authentication
○ Enforce multi-factor authentication for administrators
○ Enforce multi-factor authentication for users

The button turns green and a confirmation window opens.



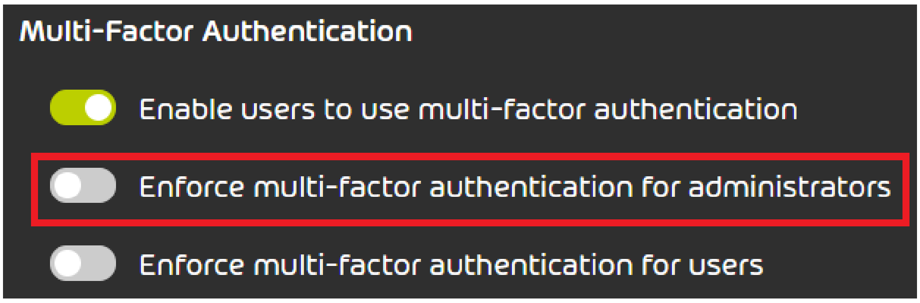
ACTIVATION

You are about to activate multi-factor authentication for your Control Panel account. You will have to enter your Control Panel password. After that, you will be prompted to configure multi-factor authentication. Do you want to continue?

5. Click on **Confirm.**

ENFORCING MULTI-FACTOR AUTHENTICATION FOR ADMINISTRATORS

1. Under Multi-Factor Authentication, toggle the switch **Enforce multi-factor authentication for administrators**.



Multi-Factor Authentication

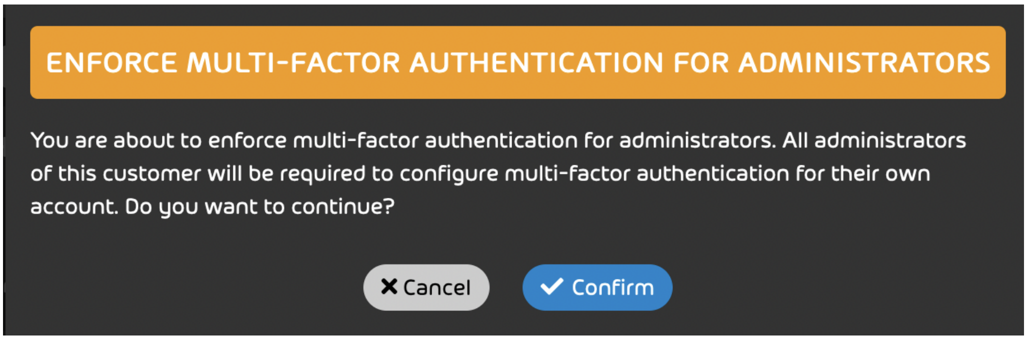
● Enable users to use multi-factor authentication

○ Enforce multi-factor authentication for administrators

○ Enforce multi-factor authentication for users

The switch is highlighted in green. A confirmation window opens.

2. Click on **Confirm**.



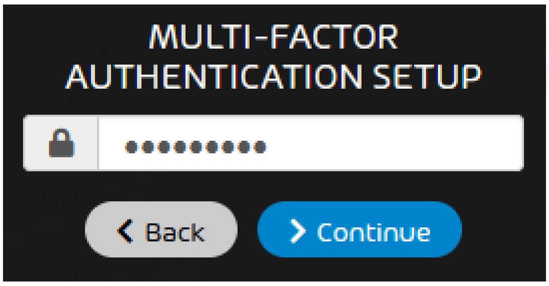
ENFORCE MULTI-FACTOR AUTHENTICATION FOR ADMINISTRATORS

You are about to enforce multi-factor authentication for administrators. All administrators of this customer will be required to configure multi-factor authentication for their own account. Do you want to continue?

Once the administrators log in to the Control Panel the next time, they must configure multi-factor authentication for their Control Panel account.

CONFIGURING MULTI-FACTOR AUTHENTICATION

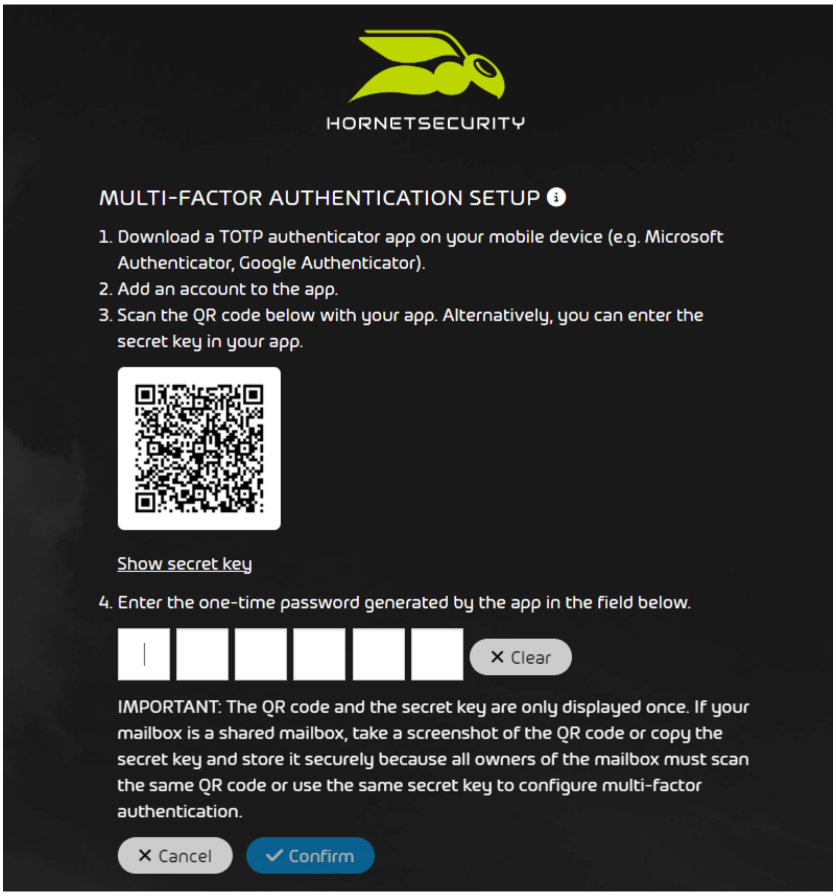
1. At the next control panel login, the page **Multi-factor authentication setup** is displayed.
2. Enter your Control Panel password in the input field.


MULTI-FACTOR AUTHENTICATION SETUP

●●●●●●●●●●

3. Click on **Continue**.

A page with instructions on how to configure multi-factor authentication is displayed.



MULTI-FACTOR AUTHENTICATION SETUP

1. Download a TOTP authenticator app on your mobile device (e.g. Microsoft Authenticator, Google Authenticator).
2. Add an account to the app.
3. Scan the QR code below with your app. Alternatively, you can enter the secret key in your app.

4. Enter the one-time password generated by the app in the field below.

IMPORTANT: The QR code and the secret key are only displayed once. If your mailbox is a shared mailbox, take a screenshot of the QR code or copy the secret key and store it securely because all owners of the mailbox must scan the same QR code or use the same secret key to configure multi-factor authentication.

4. Open your authenticator app on your mobile device.
5. Add a new account to the authenticator app.

   IMPORTANT: A QR code or secret key is required to configure multi-factor authentication.

6. Optional: If you would like to configure multi-factor authentication with the **QR code**, proceed as follows:

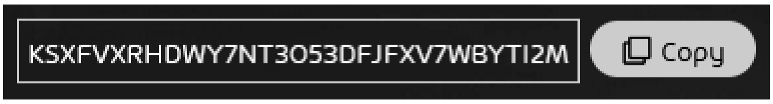
a. If your mailbox is a shared mailbox, create a screenshot of the QR code from the Control Panel and store it safely.
b. Scan the QR code from the Control Panel with the authenticator app.

Note: The authenticator app generates a new six-digit one-time password every 30 seconds.

7. Optional: If you would like to configure multi-factor authentication with the **secret key**, proceed as follows:

a. Click on **Show secret key**.

   The secret key is displayed.



KSXFVXRHDWY7NT3O53DFJFXV7WBYTI2M

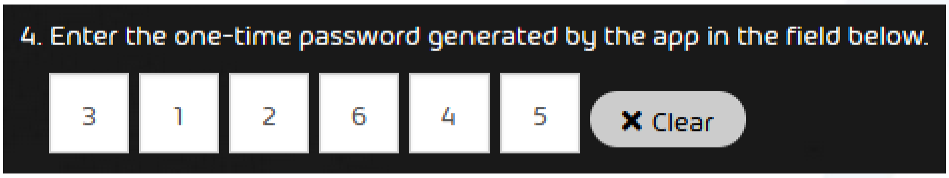
b. Click on **Copy** .

c. If your mailbox is a shared mailbox, save the secret key and store it safely.

d. Enter the secret key in the authenticator app.

Note: The authenticator app generates a new six-digit one-time password every 30 seconds.

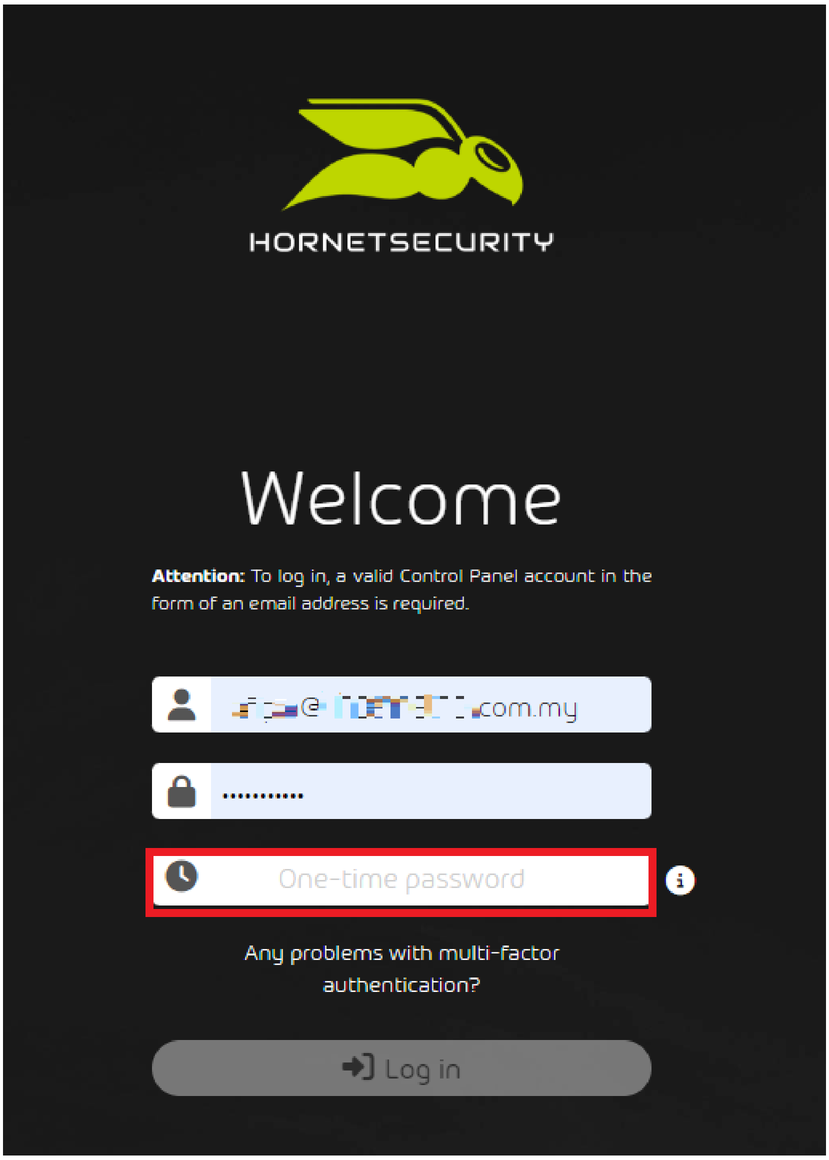
8. Enter the current one-time password from the authenticator app in the input mask in the Control Panel.



4. Enter the one-time password generated by the app in the field below.

9. Click on Confirm.

Multi-factor authentication is now configured. From now on, the Control Panel login for administrators will use multi-factor authentication.



Welcome

Attention: To log in, a valid Control Panel account in the form of an email address is required.

[redacted].com.my

....