EASTWIND

Eastwind Multi-Factor Setup Guide

The Challenge:

Enterprises today fight a complicated battle: there is a global army of hackers who never sleep and who are looking for new and creative ways to break into networks, whether hosted or on-premise. Eastwind arms security teams with comprehensive visibility.

The Solution:

EASTWIND
Multi-Factor Auth

The Benefits:

- Complete cyber security and visibility of your SaaS solutions.
- Enhance your Breach Analytics with Eastwind for SaaS telemetry.
- Streamline your procurement; No POs required; Be up and running in minutes.

Overview

In order to provide better safeguards to our customers information Eastwind has implemented Multi-Factor Authentication (MFA) to the Eastwind portal. The simple process to enable MFA and then access the Eastwind portal are outlined in this document.

Install Multi-Factor Authentication App

In order to use MFA you will need to install either a desktop or mobile application. Eastwind recommends either Google Authenticator, FreeOTP or similar.

Enable Multi-Factor Authentication

Once installed, logon to the Eastwind portal, navigate to Management -> Profile and click on the Turn On button. This will generate a secret key and a QR Code. Either scan the QR Code or manually enter the secret key into the application, this will create time based One Time Passwords for use when logging on to the Eastwind portal.

Note: Manually entering the secret key is the only option for a desktop app as you cannot scan the QR Code.

Accessing the Eastwind Portal after MFA is Enabled

After you enable Multi-Factor Authentication, you enter your username and password as usual then be prompted to enter a code from the MFA app installed earlier. The codes will expire every 30 seconds so you will need to promptly enter the code or obtain a new value.

EASTWIND

For more information on Eastwind for Multi-Factor,
please see eastwindnetworks.com