January 24, 2017

Eagle Eye Networks Implements Two Factor Authentication

This enhancement further protects the Eagle Eye Security Camera VMS from cyber threats.

Austin, TX – Eagle Eye Networks today announced implementation of Two Factor Authentication across the Eagle Eye Security Camera VMS including its iOS and Android mobile applications. Two Factor Authentication provides enhanced security for all Eagle Eye Users by establishing trusted devices and only allowing camera and video access from those trusted devices. Two Factor Authentication is utilized by most banks to protect online access to bank accounts and money transfers.

"Cyber security is of paramount concern at Eagle Eye Networks and implementation of Two Factor Authentication across our entire system ensures that our customer assets are even more secure." said Dean Drako, President and CEO of Eagle Eye Networks.

Eagle Eye Network's Two Factor Authentication has been deployed globally across its 7 data centers. All users of the Eagle Eye Security Camera VMS can employ this added layer of security.

"Our customers are highly concerned about their Cyber Security in addition to their physical security," said Vincent Scarpelli, Manager of Product Strategy in Video Solutions at Tyco Integrated Security. "Eagle Eye's Industry leading implementation of Two Factor Authentication ensures that our customers' video will not be compromised. We are pleased to offer this additional cyber security measure to our customers."

Two Factor Authentication is an extra layer of security for each Eagle Eye Account designed to ensure that only authorized users can access each Eagle Eye Account and cameras, even if someone obtains a password.

How It Works

With Two Factor Authentication, an Eagle Eye Account can only be accessed on devices that are trusted, like a mobile phone or a computer. When a user wants to utilize a new device for the first time, that user will need to provide two pieces of information— a password and a six-digit security code that must be obtained via a trusted phone number or a trusted email address.

Because a password alone is no longer enough to access an Eagle Eye Account, Two Factor Authentication dramatically improves the security of each Eagle Eye Account and access to corresponding cameras and video.

Once logged in, an Eagle Eye User won't be asked for a security code on that device again unless the user logs out completely, erases the device, or needs to change a password for security reasons. When an Eagle Eye User logs in

on the web, that user can choose to trust a browser so the user won't be asked for a security code the next time that user logs in from that same computer.

To learn more about Eagle Eye Networks, please visit www.EagleEyeNetworks.com.

Terms

Trusted Devices – A trusted device is a mobile device or a browser on a computer that has previously successfully logged in using Two Factor Authentication. It's a device that is known to be associated with that Eagle Eye User.

Trusted Phone Numbers and Emails – A trusted phone number is a number that can be used to receive a security code by text. A trusted email address is the email address for the Eagle Eye User on the Eagle Eye Account.

Security Code – A security code is a temporary code sent to a trusted device or phone number when the user logs in to a new device or browser.

About Eagle Eye Networks

Eagle Eye Networks delivers the fastest growing, on-demand cloud based security and operations video management system (VMS) providing both cloud and on premise recording. Eagle Eye also provides a cloud video API for integrations and application development. The Eagle Eye Platform offers secure, encrypted recording, camera management, mobile viewing and alerts – all 100% cloud managed. The API platform uses the Eagle Eye Big Data Video Framework™, with time based data structures used for indexing, search, retrieval and analysis of the live and archived video. Eagle Eye Networks sells through authorized reseller and installation partners.

###