

Eagle Eye Application Note – AN031

Implementing Two-Factor Authentication

2022-07-22 Revision 01.2

Target Audience

This Application Note is intended for end users of the Eagle Eye Cloud VMS. Specifically, admin users who will be responsible for adding users and determining if they require Two-Factor Authentication.

Overview

Two-Factor Authentication provides enhanced security for all Eagle Eye Cloud VMS users by establishing trusted devices and allowing only camera and video access from those trusted devices. It is an extra layer of security designed to ensure that only authorized users can access the account and cameras, even if someone has obtained a user's password. Two-Factor Authentication is commonly found and utilized by many businesses to protect online access to sensitive and/or personal information.

Theory of Operation

With Two-Factor Authentication, an Eagle Eye Cloud VMS 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 four-digit security code that must be obtained via a trusted phone number or a trusted email address.

Functionality

Eagle Eye Cloud VMS administrators have the option to enforce Two-Factor Authentication across sub-accounts/customer accounts or by specific users. See the example below that illustrates "Customer 1" user login with a sub-account.

The screenshot shows a user interface with a dark header bar. On the left, a user profile dropdown menu is open, showing options: "My Profile" (highlighted in blue), "Account Settings", and "Log Out". The header bar also displays "Customer 1", a notification icon, and the time "12:38:33". On the right, a login form is visible with the following fields and options:

- Navigation tabs: Login, Notifications, Time, Layouts, Previews, Trusted Devices
- Login (email): xxxxxxdemo@gmail.com
- Name: Customer, 1
- Language: English
- Password: Change Password
- Alternate email: Alternate email (for alerts)
- Two Factor Authentication:
- SMS Phone: SG, xxxxxxxx (for authentication)

Login using "Customer 1" credentials and click on "dropdown" in the top right corner to select "My Profile."

Enable "Two Factor Authentication" and enter a mobile phone as an additional trusted device that will receive the security code. Save changes when finished.

The screenshot shows a modal dialog box with the following content:

- Header: Please enter your password to update your two factor authentication preference
- Input field: A text box containing seven dots (password mask).
- Buttons: "Cancel" (orange) and "Send Security Code" (green).

To proceed, enter "Customer 1" credentials and click "Send Security Code". This will send a security code to the email assigned to "Customer 1."

The screenshot shows a modal dialog box with the following content:

- Header: Verify your Security Code
- Text: A Security Code has been sent to your email. Please, enter it below.
- Input field: An empty text box for entering the security code.
- Buttons: "Cancel" (orange) and "Verify Code" (green).

Enter the security code received from the "Customer 1" email to save this configuration. The next time "Customer 1" logs into the system, Two-Factor Authentication will be enforced.

In the illustration below, a sub-account is enforced with Two-Factor Authentication. All users created are mandated to use Two-Factor Authentication in this scenario.

Login to the Master account to manage sub-accounts. Click "Settings" to modify changes to this sub-account.

Proceed to the "Access" tab and enable "Two Factor Authentication". Save changes when finished.

New users logging in for the first time to this sub-account will have to go through the Two-Factor Authentication process. If users would like to receive a security code via their mobile phones, they can be added as a trusted device in their profile settings.

Application

The first time a user enters credentials to sign into an Eagle Eye Cloud VMS account after Two-Factor Authentication is enabled, a security code can be sent to their email or mobile phone (if a mobile phone is assigned as a trusted device).




Email Address

We need to verify your account with a Security Code.
How would you like to receive it?

*****emo@gmail.com (Email)
 +** **** *408 (Phone)

When the Security Code has been verified, the user is successfully signed in. After the first successful login, the mobile phone becomes a trusted device and the verification step won't be required the next time they attempt to login. After 180 days, the user will need to repeat this process.



Email Address

Please check your phone for the code and enter it below.

Note that if an Eagle Eye Cloud VMS user removes a trusted device in the “My Profile” settings or needs to change a password for security reasons, the user will have to go through the process of entering a Two-Factor Authentication security code again.

The screenshot shows the 'My Profile' settings page with the 'Trusted Devices' tab selected. The page displays a list of five trusted devices, each with a trash icon for removal. Below the list is a 'Remove All' button, and at the bottom right are 'Cancel' and 'Save changes' buttons.

Device Type	Info	IP Address	Last Login
PC	PC / Windows 10 / Chrome 95.0.4638	42.60.50.50	Thu Oct 21 2021 15:28:15 GMT+0800 (Singapore Standard Time)
Mobile	Samsung SM-G998B / Android 11 / Samsung Internet 15.0	111.65.32.172	Tue Oct 19 2021 20:58:25 GMT+0800 (Singapore Standard Time)
PC	PC / Windows 10 / Edge 94.0.992	172.87.156.190	Mon Oct 04 2021 14:39:27 GMT+0800 (Singapore Standard Time)
Mobile	Samsung SM-G998B / Android 11 / Chrome Mobile 94.0.4606	111.65.32.172	Tue Oct 19 2021 20:57:08 GMT+0800 (Singapore Standard Time)
Other	Other / Other / okhttp 4.9.2	42.60.51.90	Wed Oct 13 2021 11:14:12 GMT+0800 (Singapore Standard Time)

Notes and Other Helpful Details

Trusted devices: A trusted device is a mobile device or a browser on a particular computer or tablet that has successfully signed in to Eagle Eye Cloud VMS using Two-Factor Authentication within the last 180 days. It is a device that is known to be associated with that Eagle Eye Cloud VMS user.

Trusted phone numbers and emails: A trusted phone number is a number that can be used to receive a security code by text and is linked to a user from within their “My Profile.” A trusted email address is the email address for the Eagle Eye Cloud VMS user on the Eagle Eye Networks Account.

Security code: A security code is a temporary code that gets sent to a trusted phone number or email address when a user attempts to sign in to a new device or browser.

Credentials: The email address and password of an Eagle Eye Networks' user account.

Example of security codes obtained from an email/mobile device are shown below:

