



Präambel:

Wir entwickeln EmergencyEye® fortlaufend weiter, um Sie bestmöglich zu unterstützen und informieren Sie hiermit über die anstehende Einführung neuer Funktionen und Änderungen. Wir haben mit Ihnen und Ihren KollegInnen zahlreiche Neuerungen erarbeitet und dürfen Ihnen diese nun im Release 5.4.0 zur Verfügung stellen.

- I. Der Release 5.4.0 wird für die Instanzen **Videosupport.emeye-t.ch**, sowie alle **WhiteLabels** am **07.11.2023** um **12 Uhr** erfolgen.
- II. **EmergencyEye® COMMAND**, und die **EmergencyEye®** Instanzen der Notruf und Gefahrenabwehreinrichtungen werden am **14.11.2023** um **12 Uhr** auf 5.4.0 umgestellt.

Die Downtime wird wie immer unter einer Minute liegen. Sollten Sie Störungen registrieren, so bitten wir Sie um eine Benachrichtigung über unser Ticketsystem unter: <https://support.emergencyeye.de> oder per mail unter support@emergencyeye.de .

-
1. Mit dem neuen **“Passwortmanager“** können Sie nun neue Nutzer per automatisierter Mail zur eigenen Passwortvergabe auf die Plattform einladen. Nutzer können eine **“Passwort Vergessen“** Funktion nutzen.
Ebenfalls ist es nun möglich, dass Sie für Ihr Zentrum eine Passwort-Policy festlegen.
 2. Des Weiteren bieten wir Ihnen das **“Fileshare“** an, um Dateien zwischen Anrufenden und Agenten beidseits zu teilen.
Dies werden wir erst nach Rücksprache mit Ihnen live schalten.
 3. Mittels der **“Autodownload“** Funktion können Sie nun entscheiden, ob Sie Fotos weiterhin direkt und automatisch herunterladen möchten, oder nur situativ durch aktives Anklicken.
 4. Anpassungen zur besseren Übersicht in der Admin Oberfläche:
 - a. Die bereits bekannten Funktionen **“IP-Restriktion“** und **“API-Token“** wurden unter der Rubrik **“Authentifizierung“** zusammengefasst.
 - b. Die Rubrik **“Medien“** wurde geschaffen und die neue Funktion **“Autodownload“** und das bereits bekannte **“Aufzeichnen“** dort einsortiert.

Wir nehmen mit Ihnen zur Abstimmung in Kürze Kontakt auf und freuen uns auf Ihr Feedback.

Wie gewohnt erhalten Sie die Beschreibungen der neuen Funktionen als Video-Tutorials für die Industrieeinrichtungen oder Notrufleitstellen und die Gefahrenabwehr unter:

- <https://helpdesk.emergencyeye.de/tutorials-fuer-die-industrie/>
oder
- <https://helpdesk.emergencyeye.de/tutorials-fuer-notrufleitstellen-und-gefahrenabwehr/>



1) Passwortmanager:

Der "Passwortmanager" ermöglicht Ihnen, Ihre Mitarbeiter als Benutzer anzulegen und für die EmergencyEye-Technologie einzuladen. Diese können sich dann selbst ein Passwort vergeben. Alternativ kann wie gewohnt ein Passwort gesetzt und dem neuen Benutzer mitgeteilt werden.

Außerdem können Mitarbeiter die "Passwort Vergessen" Funktion nutzen, wenn sie ihr Passwort vergessen haben.

Zentren die keine persönliche Passwortvergabe haben oder einen statischen Nutzer mit festem Passwort nutzen, ist darauf zu achten, dass bei der Passwortvergabe beim Nutzer die Auswahl auf "Passwort festlegen" gesetzt ist und im Feld darunter das Häkchen für "Benutzer darf Passwort ändern" herausgenommen wurde.

- a) Administratoren **müssen** auf der Admin Oberfläche die Passwort Policy festlegen, s.a. folgende Abbildung.

Dispatch Center bearbeiten corevas

Allgemein Authentifizierung Adressbuch Teilen Session-Report Disclaimer Medien Funktionen

Passwort Policy

Legen Sie hier fest, welche Anforderungen Passwörter erfüllen müssen und wie lange sie gültig sind.

Passwortanforderungen

- Mindestlänge
- Gemischte Groß- und Kleinschreibung
- Sonderzeichen
- Ziffern
- Darf nicht identisch sein mit dem zuletzt verwendeten Passwort

Passwort Gültigkeitsdauer

Monate

Geben Sie einen numerischen Wert zwischen 1 und 99 ein oder 0 für keine Passwortablaufzeit ein.

Passwortrichtlinie speichern

Generiere ein API Token

Dieses Token ermöglicht den Zugriff auf die EmergencyEye® X API. Ein neues Token kann jederzeit erzeugt werden. Es wird außerdem automatisch ein User erzeugt, über den der Zugriff verwaltet werden kann.

Token generieren

generiertes Token

IP-Restriktionen

z.B. 123.456.789.*; 123.654.*:123

max. 255 ZeichenDie IP kann als Regullärer Express eingegeben werden. Um Regulläre Ausdruck zu prüfen nutzen Sie bitte die Website regex101.com

IP-Restriktionen speichern

Nach dem Speichern ist diese für die eingestellte Gültigkeitsdauer bindend. Bestehende Accounts behalten jedoch ihre Gültigkeit für die Dauer der Gültigkeitsdauer. Nach einer festgelegten Passwort Gültigkeitsdauer werden die Nutzer der Accounts aufgefordert, ihre Passwörter zu erneuern. Hierzu erhalten die Nutzer eine Woche vor Ablauf der festgelegten Passwort Gültigkeitsdauer eine Erinnerung bei LogIn.



- b) Administratoren müssen für jeden Nutzer individuell entscheiden, ob der jeweilige Benutzer die "Passwort Vergessen" Funktion nutzen darf. Die Auswahl erfolgt bei den Einstellungen des Benutzers ("Neuen Benutzer anlegen", oder "Benutzer ändern") über eine Checkbox (Haken in dem blauen Kästchen bei "Benutzer darf Passwort ändern").

Neuen Benutzer anlegen

Name
 max. 255 Zeichen

E-Mail
 max. 255 Zeichen

Passwortvergabe
Passwort festlegen
 Benutzer darf Passwort ändern

Passwort max. 255 Zeichen **Passwort wiederholen** max. 255 Zeichen

Dispatch Center
Bitte wählen

Rolle
Nutzer

IP-Restriktionen

max. 255 Zeichen
Die IP kann als Regulärer Express eingegeben werden. Um Reguläre Ausdruck zu prüfen nutzen Sie bitte die Website regex101.com
Eine Vorlage kann beim Dispatch Center gepflegt werden.

In Zentren, in denen keine persönlichen Passworte genutzt werden oder eine SSO Funktion im Einsatz ist, sollte kein Haken in dem blauen Kästchen bei "Benutzer darf Passwort ändern" gesetzt sein. Andernfalls würde eine evtl. Anforderung eines neuen Passwortes durch Anwender in die Leere laufen, da dem Account sicher keine aktive Mailadresse hinterlegt ist.

Bei Nutzern, die ein persönliches Passwort nutzen, ist dringend darauf zu achten, dass eine funktionierende Mailadresse angelegt wurde, da über die angelegte Account-Mailadresse die bei den Funktionen Passwort-Vergessen und Passwortvergabe eingeladen wird.



- c) Nutzer der EmergencyEye®-Technologie können auf der Oberfläche nach dem Release eine "Passwort Vergessen" Funktion nutzen, s.a. folgende Abbildung.

Account E-Mail-Adresse

Password

Passwort vergessen?

Login

Passwort zurücksetzen

Bitte geben Sie die E-Mail-Adresse ein, die zur Registrierung Ihres Kontos verwendet wurde. Wir senden Ihnen Anweisungen zur Zurücksetzung Ihres Passworts.

E-Mail-Adresse

Passwort zurücksetzen

🔒?
🔒?
🔒?
🔒?

Anfrage gesendet

Eine E-Mail zum Zurücksetzen Ihres Passworts wurde an die angegebene E-Mail-Adresse gesendet. Bitte öffnen Sie die E-Mail und folgen Sie den Anweisungen. Überprüfen Sie auch Ihren Spam-Ordner. Wenn Sie keine E-Mail erhalten haben, wiederholen Sie den Vorgang oder kontaktieren Sie uns.

support@emergencyeye.de

🔒?
🔒?
🔒?
🔒?

Die Nutzer erhalten anschließend folgende Mail:

Handlung erforderlich

N No-Reply <corevas@emergencyeye.de>
An: guenterhuhle@corevas.de

Guten Tag,
Es wurde eine Anforderung zur Zurücksetzung Ihres Passworts gestartet. Sie können jetzt das Zurücksetzen Ihres Passworts über folgenden Link initiieren:
https://emeyex-alpha.mdeg.io/auth/oauth2/setpassword?t=3d849816-098c-4b7b-bbc6-b7e286ab26a5&client_id=auth1159736
Falls Sie diese Anfrage nicht gestellt haben, ignorieren Sie diese E-Mail bitte.
Vielen Dank,
Ihr Team

Wenn die Nutzer den Link für das Zurücksetzen des Passwortes nutzen, können Sie durch folgende Schritte ihr Passwort zurücksetzen und sehen währenddessen, ob sie die Passwort Policy berücksichtigen (im folgenden Beispiel nur die Mindestlänge 8).

Neues Passwort

✔ Mindestlänge: 8

Neues Passwort bestätigen

Passwort ändern

🔒?
🔒?
🔒?
🔒?

Passwort erfolgreich geändert

Ihr Passwort wurde erfolgreich geändert. Sie können sich jetzt mit Ihrem neuen Passwort anmelden.

Login

🔒?
🔒?
🔒?
🔒?

Account E-Mail-Adresse

Password

Passwort vergessen?

Login

Anschließend können die Nutzer die EmergencyEye®-Technologie einsetzen.

Wurde für den Benutzer festgelegt, dass er sein Passwort nicht ändern darf kann der Button "Passwort vergessen" dennoch verwendet und eine E-Mail-Adresse angegeben werden. Ist die E-Mail-Adresse als Benutzer hinterlegt, erhält der Benutzer eine Hinweis-E-Mail, dass er nicht berechtigt ist sein Passwort zu ändern.

Handlung erforderlich

N No-Reply <corevas@emergencyeye.de>
An: guenterhuhle@corevas.de

Guten Tag,
Sie sind nicht berechtigt ihr Passwort zu ändern. Bitte wenden Sie sich für weitere Informationen an Ihren Administrator.
Vielen Dank,
Ihr Team



2. Fileshare:

Im Einzelfall kann es wünschenswert sein, Dokumente, Bilder oder andere Files mit den Anrufern zu teilen, oder von diesen zu erhalten. Dafür haben wir die Funktion "Fileshare" entwickelt.

Die zu teilenden Dateien werden während der Session auf einem extra dafür eingerichteten File-Server einer DSGVO-, HDS- und HIPAA-konformen Instanz bei dem bereits in den Auftragsdatenverarbeitungsvereinbarungen verankerten Partner APIZEE, vorgehalten und nach der von den Admins vorgegebenen Zeit gelöscht. Sollten Sie die "Fileshare" Funktion nutzen wollen, so werden wir mit Ihnen die bestehende Auftragsdatenverarbeitungsvereinbarung entsprechend erweitern.

Funktionsbeschreibung:

Vorausgesetzt Sie haben die "Fileshare" Funktion für Ihr Zentrum aktivieren lassen, wird bei einer aktiven Session der Funktionsbereich um diese Funktion erweitert.

a. Fileshare für die Administratoren

Die Administratoren können auf der Admin-Oberfläche die Länge der Speicherdauer auf einer DSGVO-, HDS- und HIPAA-konformen Serverinstanz bei dem bereits in den Auftragsdatenverarbeitungsvereinbarungen verankerten Partner APIZEE vorgeben. Hierzu nutzen die Admins unter Medien in der Sektion Datenfreigabe und Aufzeichnungen die Auswahl Tage/Monate und können hier die maximale Vorhaltdauer festlegen, s.a. folgende Abbildung.

Dispatch Center bearbeiten Corevas

Allgemein	Authentifizierung	Adressbuch	Teilen	Session-Report	Disclaimer	Medien	Funktionen
-----------	-------------------	------------	--------	----------------	------------	--------	------------

Medien-Einstellungen

Fotoeinstellungen

Sie können hier die Einstellung für den automatischen Download von Fotos festlegen.

Auto-Download

Dateifreigabe und Aufzeichnung

Hier können Sie die Aufbewahrungsfrist für Aufzeichnungen und Dateifreigabe-Uploads festlegen.

Tage max. 30

Die Speicherdauer beträgt maximal 180 Tage und kann später wieder geändert werden. Bereits abgelegte Daten werden nach der vorher festgelegten Speicherdauer verwaltet.

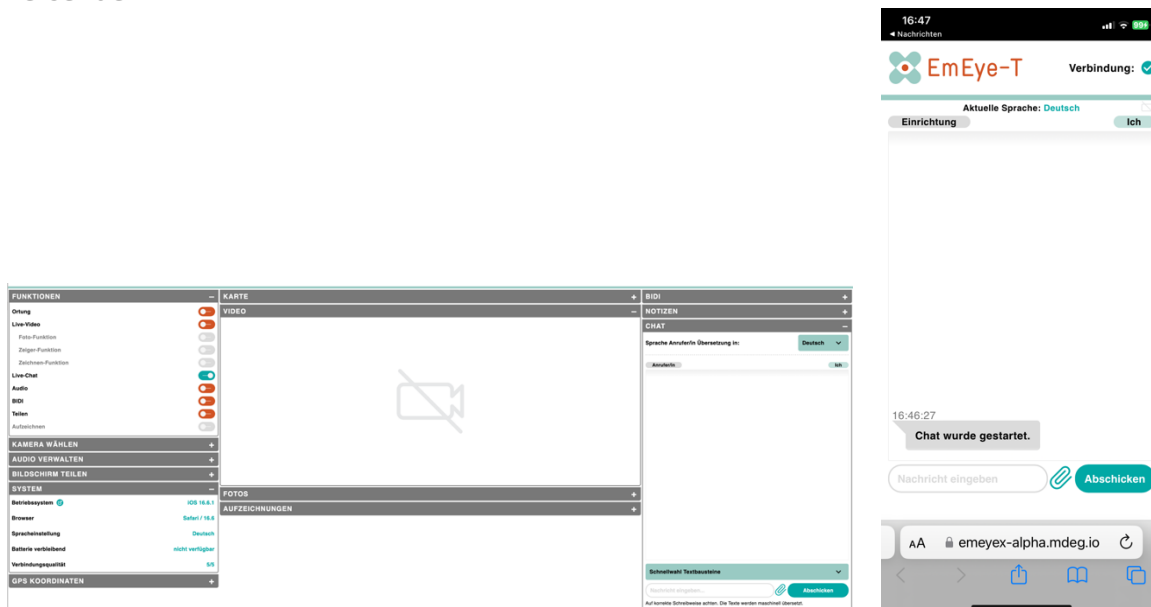


b. Fileshare seitens Dispatcher/Agent und Anrufenden

Die Funktion Fileshare kann sowohl vom Dispatcher/Agenten, als auch vom Anrufenden genutzt werden.

Über die Büroklammer neben dem Texteingabefeld, können Dokumente angehängt werden.

Zusätzlich können Dispatcher per "Drag 'n Drop" Dateien direkt in den Chat ziehen und so versenden.



Anschließend können Dateien ausgewählt und übermittelt werden.

Die Empfänger müssen dann nur noch entscheiden, ob sie die Dateien auch beziehen wollen. Nach aktivem Download können diese von den Empfängern eingesehen werden.

Sollten die Anrufenden während einer laufenden Session die Dateien einsehen, so wird die Browser-Verbindung pausiert und kann in gewohnter Weise anschließend wieder aufgenommen werden.

Es werden folgende Informationen im Sessionreport und über die API dokumentiert:

- File-Share aktiviert
- File gesendet (inkl. File-Name, -Größe)
- File ausgeliefert (inkl. URL zum Download)
- File downloaded, falls erfolgt.

Hinweis:

Heruntergeladene Dateien / Dokumente über die Funktion Fileshare sind auch nach Beendigung der EmergencyEye-Sitzung auf der Seite der Empfänger noch vorhanden (z.B. im Downloadspeicher).



3. "Autodownload"

Des Weiteren dürfen wir Ihnen die "Autodownload" Funktion für Fotos vorstellen. Diese ermöglicht Ihnen für Ihr Zentrum festzulegen, ob Sie auch in Zukunft die Standard- und/oder HD- Fotos weiterhin direkt und automatisch herunterladen möchten, oder nur situativ durch aktives Herunterladen. Manchen Anwender war durch den direkten und automatischen Download zu viele Bilder in den Downloadordnern gelandet und somit Speicherkapazität unnötig belegt.

Dispatch Center bearbeiten Corevas

Allgemein Authentifizierung Adressbuch Teilen Session-Report Disclaimer Medien Funktionen

Medien-Einstellungen

Fotoeinstellungen

Sie können hier die Einstellung für den automatischen Download von Fotos festlegen.

Auto-Download



Autodownload angeschaltet:

Bilder werden direkt nach dem Betätigen des Standardfoto oder Erhalt von HD-Fotos in den vom Dispatcher/Agenten im Browser festgelegten Download-Ordner des Browsers heruntergeladen.

Autodownload ausgeschaltet:

Bilder werden nicht mehr direkt nach dem Betätigen des Standardfoto oder Erhalt von HD-Fotos in den Download-Ordner des Browsers heruntergeladen, sondern müssen manuell heruntergeladen werden durch Betätigen des Downloadbuttons.

Unabhängig, ob der Autodownload an- oder ausgeschaltet ist, werden erhaltene Fotos im Session-Report und über die API bereitgestellt, als rechtsichere Dokumentation.



4. Anpassungen zur besseren Übersicht in der Admin Oberfläche:

- a. Die bereits bekannten Funktionen "IP-Restriktion" und "API-Token" wurden unter der Rubrik "Authentifizierung" zusammengefasst. Dort wurde auch die "Passwort Policy" eingefügt, s.a. folgende Abbildung:

Dispatch Center bearbeiten Corevas

Allgemein **Authentifizierung** Adressbuch Teilen Session-Report Disclaimer Medien Funktionen

Passwort Policy

Legen Sie hier fest, welche Anforderungen Passwörter erfüllen müssen und wie lange sie gültig sind.

Passwortanforderungen

Mindestlänge

Gemischte Groß- und Kleinschreibung

Sonderzeichen

Ziffern

Darf nicht identisch sein mit dem zuletzt verwendeten Passwort

Passwort Gültigkeitsdauer

Monate

Geben Sie einen numerischen Wert zwischen 1 und 99 ein oder 0 für keine Passwortlaufzeit ein.

[Passwortrichtlinie speichern](#)

Generiere ein API Token

Dieses Token ermöglicht den Zugriff auf die EmergencyEye® X API. Ein neues Token kann jederzeit erzeugt werden. Es wird außerdem automatisch ein User erzeugt, über den der Zugriff verwaltet werden kann.

[Token generieren](#)

generiertes Token

IP-Restriktionen

max. 255 ZeichenDie IP kann als Regulärer Express eingegeben werden. Um Reguläre Ausdruck zu prüfen nutzen Sie bitte die Website regex101.com

[IP-Restriktionen speichern](#)

- b. Die Rubrik "Medien" wurde geschaffen und die neue Funktion "Autodownload" und das bereits bekannte "Aufzeichnen" dort einsortiert. Im Bereich "Datenfreigabe und Aufzeichnung" können Zentren, die diese aktiviert haben, die Speicherdauer sowohl für die Video-/Audio-Aufzeichnung als auch für den Fileshare festlegen.

Dispatch Center bearbeiten Corevas

Allgemein Authentifizierung Adressbuch Teilen Session-Report Disclaimer **Medien** Funktionen

Medien-Einstellungen

Fotoeinstellungen

Sie können hier die Einstellung für den automatischen Download von Fotos festlegen.

Auto-Download

Dateifreigabe und Aufzeichnung

Hier können Sie die Aufbewahrungsfrist für Aufzeichnungen und Dateifreigabe-Uploads festlegen.

Tage max. 30

[Speichern](#)



Wir möchten Sie und Ihre Firewall- und Proxy-Verantwortlichen sensibilisieren, dass für den reibungslosen Einsatz aller Funktionen folgende Freigaben erforderlich sind:

(IP-Adressen werden sich ändern. Wir empfehlen daher die Freigabe auf Basis des FQDN)

Name	Funktion	DNS	Port/Protokoll
ApiZee	WebRTC Media Proxy, Media Library und Call Control Server	*.apizee.com	TCP: 443, UDP: 443, 49152-65535
Blazing CDN	Blur für BIDI-Funktion	cdn28477102.blazingcdn.net2	TCP:443
EmergencyEye- Technologie, auch WhiteLabel	Dispatcher-Zugang	Dispatcher URL z.B. ee02.emergencyeye.de	TCP: 443
	Admin-Zugang	Admin URL z.B. admin.ee02.emergencyeye.de	TCP: 443
Geoapify	Map Tiles	*.geoapify.com	TCP: 443
Corevas	Helpdesk	helpdesk.emergencyeye.de	TCP: 443
	Support	support.emergencyeye.de	TCP: 443

¹ Wir empfehlen die Nutzung von Wildcards *.-----, um Weiterentwicklungen und Redundanzsystem vollumfänglich nutzen zu können. Sollten Sie dennoch auf Einzelfreigaben bestehen, dann melden Sie sich gerne bei uns. In diesen Fällen kann jedoch eine kurzfristige Änderung seitens Dienstleister eine Inkompatibilität erwirken, da Ihre Proxy- und Firewall-Einstellung einen Datenaustausch unterbinden.

² Für unsere Funktion BIDI benötigen Sie die oben genannte Freigabe. Sollten Sie die Funktion BIDI in ihrem DispatchCenter nicht nutzen, so kann diese Freigabe entfallen.

Die Videoverbindung ist verschlüsselt. Die Deep-Package Inspection erlaubt keinen verschlüsselten Datenverkehr und **muss daher deaktiviert bleiben bzw. werden.**

Die EmergencyEye®-Plattform ist keine Progressive Web App (PWA) und eine Einschränkung auf PWA kann zu Funktionseinschränkungen führen und empfehlen wir zu vermeiden.

Vielen Dank für Ihre Vorschläge, die wir auch in diesem Release wieder umsetzen.
Sollten Sie eine ungewünschte Fehlfunktion bemerken, so bitten wir um eine kurze Nachricht.
Bzgl. Anregungen und Störungen per Ticket-System <https://support.emergencyeye.de>
oder per E-Mail support@emergencyeye.de

Wir danken Ihnen für Ihr Vertrauen

Das EmergencyEye Team, Sie erreichen uns hier:

emergencyeye@corevas.de

3001-03-EmergencyEye_ReleaseNotes
_Extern_5.4.0_D

Erstellt durch:
GHU

Geprüft durch:
JAH

Freigegeben durch:
GHU