Bedienungsanleitung CEAG VisionGuard

Zielgruppe Teil 1: Elektrofachkraft gem. EN 50110-1 und
elektrisch unterwiesende Personen

Powering Business Worldwide

Inhalt

1 Vorwort und Systemvoraussetzungen

1.1 Vorwort

Die VisionGuard ist eine moderne webbasierte Überwachungs- Steuerungs- und Konfigurationssoftware für die neuen Zentralbatteriesysteme DualGuard-S und wird mit der nächsten Version ab Q4 / 2020 um die aktuellen CG-S-Bus basierten Notlichtsysteme ZB-S, AT-S+, LP-STAR, sowie das aktuelle Einzelbatteriesystem CGLine+ erweitert.

Features:

- Webbasierte Client-/Server Architektur für unabhängige Bedienung von mehreren Usern
- Für bis zu 500 Notlichtsysteme (DualGuard)
- Benutzerkontenmenü (UAC) mit 4 Benutzerrollen für unterschiedliche Zugriffsberechtigungen
- Entwickelt und geprüft auf Cyber Sicherheit (EATON zertifiziert)
- Softwarelizensierung ohne Hardwaredongle
- Moderne Dashboard Darstellung als Startseite
- Responsive Webdesign (automatische Anpassung auf unterschiedliche Displaygrössen)
- Modernes MQTT Kommunikationsprotokoll (ereignisorientierte Kommunikation)
- Systemübersicht aller Anlagen in einem Bild
- Volle Visualisierung und Steuerung
- Automatische Funktionstests und Betriebsdauertest je Gerät
- Umfangreiches Prüfbuch mit vielen Filter-Funktionen
- Integrierte E-Mailfunktion frei konfigurierbar
- Komfortable und umfangreiche Druckfunktionen

Generelle Hinweise zu den Anzeigen:

Die Statusanzeigen in der VisionGuard werden farblich dargestellt.

Grün = OK, es liegt kein Fehler vor

Blau = Information, z.B. FT Intervall überschritten

Grau = Stromkreis oder Leuchte ausgeschaltet

Gelb = Batteriebetrieb, Funktionstest (FT) aktiv oder Batteriedauertest (BT) aktiv, Stromkreis oder Leuchte eingeschaltet

Orange = Störung Prio.1 oder Netzausfall am 3-Phasenwächter (3PM-IO)

Rot = Störung, es liegt ein Fehler bzw. Störung an.

Namen können generell 40 Zeichen und Informationen 100 Zeichen lang sein. Alle Sonderzeichen sind erlaubt.

1.2 Wichtige Hinweise zur Cyber Sicherheit der VisionGuard in Ethernet Netzwerken

Wird die VisionGuard in einem Ethernet basiertem Kommunikationsnetzwerk betrieben, sollte besonderer Wert darauf gelegt werden, einen unbefugten Zugriff, z.B. durch Hackerangriffe vorzubeugen. Die Sicherheit der VisionGuard ist letztendlich aber stark abhängig von der betreiberseitigen Einrichtung, z.B. hohe Passwortqualität, und der Netzwerkumgebung, in der die VisionGuard betrieben wird. Eine unsichere Netzwerkumgebung erleichtert einen ungewünschten Zugriff durch fremde Personen. Um eine Hilfestellung zu geben, möchten wir hiermit auf wichtige Punkte hinweisen, um die VisionGuard Software so sicher wie möglich gegen Fremdzugriff zu schützen.

Einstellungen in der VisionGuard

Die VisionGuard verfügt über einen integrierten Passwortschutz, der über eine Sicherheitsstufe folgendermaßen vordefiniert ist:

- Es muss mindestens sechs Zeichen lang sein (je länger desto besser). Es muss aus mindestens jeweils einem Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern (?!%+…) bestehen.

Der Passwortschutz ist sehr wichtig gegen unerlaubten bzw. unerwünschten Zugriff durch Fremde! Deswegen sollten bei Vergabe eines Passwortes noch einige Regeln beachtet werden:

- Vermeiden sie Namen von Familienmitgliedern, eines Haustieres, des besten Freundes, des Lieblingsstars oder deren Geburtsdaten oder ähnliche Konstellationen.
- Wenn möglich sollten Passwörter nicht in Wörterbüchern vorkommen.
- Es soll nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern bestehen, also nicht qwertz oder abcd1234 und so weiter.
- Einfache Ziffern am Ende des Passwortes anzuhängen oder eines der üblichen Sonderzeichen $! ? #, am Anfang oder Ende eines ansonsten simplen Passwortes zu ergänzen ist auch nicht empfehlenswert.

Einsatz in einem Netzwerk, z.B. Intranet

Allgemeine Hinweise zu gemanagter Netzwerk Hardware, z.B. Router, Switche etc.

- Halten Sie die Firmware aktuell!
- Ändern Sie das Standard Passwort der Geräte!
- Richten Sie eine Firewall mit MAC-Adressen Filter ein!
- DDoS Abwehr aktivieren (Distributed Denial of Service)
- Sperren Sie nicht benötigte Ports und Protokolle
- Deaktivieren Sie nicht benötigte Funktionen ihres Routers!
- Deaktivieren Sie den Fernzugang ihres Routers!

Weitere Empfehlungen und Richtlinien von EATON sind im folgendem beschrieben:

Richtlinien für die sichere Konfiguration von Eaton Produkten

Dokumentation zur sicheren Installation und Konfiguration von Eaton Produkten

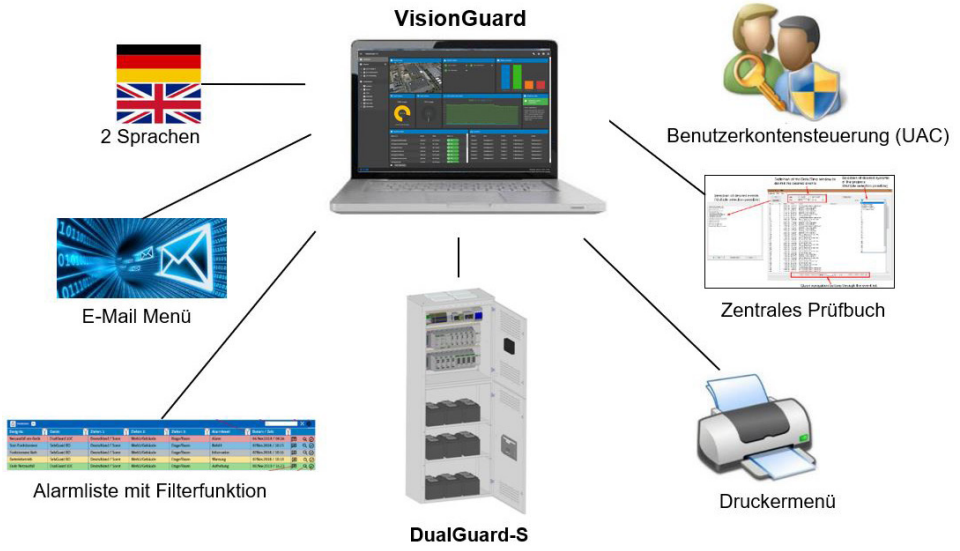
Die VisionGuard wurde so konzipiert, dass Cybersicherheit eine wesentliche Anforderung ist. Deswegen bietet dieses Produkt Funktionen, um Cybersicherheitsrisiken zu beseitigen. Diese Cybersicherheitsempfehlungen liefern Informationen, die den Benutzern helfen, das Produkt so einzusetzen und zu warten, dass Cybersicherheitsrisiken minimiert werden. Mit diesen Cybersicherheitsempfehlungen soll kein umfassender Leitfaden zur Cybersicherheit bereitgestellt werden, sondern die bestehenden Cybersicherheitsprogramme der Kunden ergänzt werden.

Eaton ist bestrebt, das Cybersicherheitsrisiko in seinen Produkten zu minimieren und Best Practices für die Cybersicherheit in seinen Produkten und Lösungen einzusetzen, um sie für die Kunden sicherer, zuverlässiger und wettbewerbsfähiger zu machen.

Die folgenden Whitepaper bieten weitere Informationen zu allgemeinen Best Practices und Richtlinien für die Cybersicherheit:

Cybersicherheitsbetrachtungen für die Informations- und Kommunikationstechnik (WP152002EN):
http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

Cybersecurity Best Practices Checklist Reminder (WP910003EN):
http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf

Kategorie	Beschreibung
Vorgesehener Zweck und Einsatz der VisionGuard	Bei VisionGuard handelt es sich um eine Visualisierungssoftware zur Überwachung, Steuerung und Konfiguration von DualGuard-S Notlichtsystemen.  Weitere Informationen dazu sind im Handbuch enthalten.
Softwareverwaltung	Die Verwaltung von Soft- und Hardware-Ressourcen in Ihrer Umgebung ist eine Grundvoraussetzung für ein effektives Cybersicherheitsmanagement. Eaton empfiehlt Ihnen, eine Anlageninventur durchzuführen, die jede wichtige Komponente eindeutig identifiziert. VisionGuard verfügt über folgende Daten zur Identifizierung: • Software-Herausgeber, Name, Version und Versionsdatum. Genaue Hinweise zu den Daten finden Sie in der Anleitung der VisionGuard Software.
Risikobewertung	Eaton empfiehlt die Durchführung einer Risikobewertung, um hinreichend vorhersehbare interne und externe Risiken für die Vertraulichkeit, Verfügbarkeit und Integrität des Systems, des Geräts und seiner Umgebung zu identifizieren und zu bewerten. Diese Aufgabe sollte in Übereinstimmung mit den geltenden technischen und regulatorischen Rahmenbedingungen wie IEC 62443 durchgeführt werden. Die Risikobewertung sollte regelmäßig wiederholt werden.
Physische Sicherheit	Ein Angreifer mit unbefugtem physischem Zugriff kann schwerwiegende Störungen der Funktionalität des Systems oder des Geräts verursachen. Darüber hinaus bieten die Industriesteuerungsprotokolle keinen kryptographischen Schutz, was die ICS- und SCADA-Kommunikation besonders anfällig für Gefahren für Ihre Datensicherheit macht. Die physische Sicherheit ist in solchen Fällen eine wichtige Schutzebene. VisionGuard ist für den Einsatz und Betrieb an einem physisch sicheren Ort konzipiert. Im Folgenden finden Sie einige bewährte Verfahren, die Eaton empfiehlt, um Ihr System oder Gerät physisch zu sichern: • Sichern Sie die Räumlichkeiten und Geräte mit Zugangskontrollmechanismen wie Schlössern, Zutrittskartenlesern, Wachpersonal, Personenschleusen, Videoüberwachung usw., falls erforderlich. • Beschränken Sie den physischen Zugang zu Schränken und/oder Gehäusen, die VisionGuard und das zugehörige System enthalten. Überwachen und protokollieren Sie den Zugriff jederzeit. • Der physische Zugang zu den Telekommunikationsleitungen und den Netzwerkkabeln sollte zum Schutz vor Abhör- oder Sabotageversuchen eingeschränkt werden. Es ist eine bewährte Vorgehensweise, Metallkanäle für die Netzwerkkabelführung zwischen den Geräteschränken zu verwenden. • VisionGuard unterstützt die folgenden physischen Zugriffsports: RJ45 Der Zugang zu RJ45diesem (LAN) Ports sollte möglichst ist einzusgeschränkt werden. • Schließen Sie keine Wechselmedien (z.B. USB-Geräte, SD-Karten usw.) für irgendwelche Vorgänge (z.B. Firmware-Upgrade, Konfigurationsänderungen oder Änderungen an der Boot-Applikation) an, es sei denn, der Ursprung der Medien ist bekannt und vertrauenswürdig. • Bevor Sie ein tragbares Gerät über einen USB-Anschluss anschließen, scannen Sie das Gerät auf Schadsoftware und Viren.

COTS Platform Security (Commercial-off-the-shelf)	Eaton empfiehlt seinen Kunden, kommerzielle Standard-Betriebssysteme oder Plattformen von Drittanbietern (z.B. Hardware von Drittanbietern, Betriebssysteme und Hypervisor, wie sie von Dell, Microsoft, VMware, Cisco usw. zur Verfügung gestellt werden) einzusetzen. • Eaton empfiehlt seinen Kunden, sich in der Dokumentation des COTS-Anbieters über die Vorgehensweise bei der Härtung dieser Komponenten zu informieren. • Herstellerneutrale Anleitungen werden vom Zentrum für Internetsicherheit zur Verfügung gestellt https://www.cisecurity.org/ Unabhängig von der Plattform sollten Kunden die folgenden Best Practices in Betracht ziehen: • Installieren Sie alle Sicherheitsupdates, die vom COTS-Hersteller zur Verfügung gestellt werden. • Ändern Sie die Standard-Anmeldeinformationen bei der ersten Anmeldung. • Deaktivieren oder sperren Sie nicht verwendete eingebaute Konten. • Beschränken Sie die Verwendung von privilegierten allgemeinen Konten (z.B. interaktive Anmeldung deaktivieren). • Ändern Sie die Standard-SNMP-Community-Strings. • Schränken Sie den SNMP-Zugriff mit Hilfe von Zugriffskontrolllisten ein. • Deaktivieren Sie nicht benötigte Ports und Dienste.
Konto Management (Account Management)	Der logische Zugriff auf das System sollte auf legitime Benutzer beschränkt sein, denen nur die Privilegien zugewiesen werden sollten, die für die Erfüllung ihrer Aufgabenrollen/Funktionen erforderlich sind. Einige der folgenden Best Practices müssen möglicherweise durch die Einbindung in die internen Richtlinien des Unternehmens umgesetzt werden: • Stellen Sie sicher, dass die Standard-Anmeldeinformationen bei der Erstanmeldung geändert werden. Die VisionGuard Software sollte nicht in Umgebungen mit Standard-Anmeldeinformationen eingesetzt werden, da Standard-Anmeldeinformationen veröffentlicht werden. • Keine Kontenfreigabe- Jedem Benutzer sollte ein eindeutiges Konto zugewiesen werden, anstatt Konten und Passwörter zu teilen. Die Sicherheitsüberwachungs- und Protokollierungsfunktionen des Produkts werden basierend auf jedem Benutzer mit einem individuellen Konto eingerichtet. Wenn Benutzer Anmeldeinformationen gemeinsam nutzen können, wird die Sicherheit beeinträchtigt. • Administrative Zugriffsrechte einschränken- Angreifer versuchen, die Kontrolle über zulässige Anmeldeinformationen zu erlangen, insbesondere über solche für besonders privilegierte Konten. Administrative Zugriffsrechte sollten nur für Konten vergeben werden, die speziell für Verwaltungsaufgaben bestimmt sind, und nicht für die regelmäßige Nutzung. • Nutzen Sie die Rollen / Zugriffsrechte, um den Benutzern einen abgestuften Zugriff entsprechend den geschäftlichen / betrieblichen Anforderungen zu ermöglichen (s. Handbuch). Versuchen Sie prinzipiell nur wenige Zugriffsrechte zu vergeben (Vergabe der minimalen Berechtigungsstufe und Zugriff auf die für die Rolle erforderlichen Systemressourcen). • Führen Sie eine regelmäßige Kontenpflege durch (entfernen Sie unbenutzte Konten). • Stellen Sie sicher, dass die Länge, Komplexität und Ablaufzeiten der Passwörter angemessen eingestellt sind, insbesondere für alle Verwaltungskonten (z.B. mindestens Zeichen, Mischung aus Groß- und Kleinbuchstaben und Sonderzeichen,). • Erzwingen Sie eine Sitzungsauszeit nach einer Inaktivitätsphase.
Zeitsynchronisation	Viele Vorgänge in Stromnetzen und IT-Netzen sind stark von präzisen Zeitinformationen abhängig. Stellen Sie sicher, dass die Systemuhr mit einer autoritativen Zeitquelle synchronisiert ist (mit manueller Konfiguration, NTP, SNTP oder IEEE 1588).
Netzwerksicherheit	Die VisionGuard unterstützt die Netzwerkkommunikation mit anderen Geräten in nativer Form über Ethernet. Diese Funktion kann Risiken bergen, wenn sie nicht sicher konfiguriert wurde. Im Folgenden werden von Eaton empfohlene Best Practices zur Sicherung des Netzwerks aufgeführt. Weitere Informationen zu den verschiedenen Netzschutzstrategien finden Sie in Eaton Cybersicherheitsüberlegungen für elektrische Verteilersysteme[R1]. Eaton empfiehlt die Segmentierung von Netzwerken in logische Enklaven, wodurch der Datenverkehr zwischen den Segmenten mit Ausnahme desjenigen, der ausdrücklich erlaubt ist, verweigert wird, und die Kommunikation auf host-to-host-Pfade beschränkt wird (z.B. durch Verwendung von Router-ACLs und Firewall-Regeln). Dies trägt zum Schutz sensibler Informationen und kritischer Dienste bei und schafft zusätzliche Barrieren im Falle einer Netzwerkperimeterverletzung. Ein Netzwerk von industriellen Steuerungssystemen für Versorgungsunternehmen sollte mindestens in eine dreistufige Architektur (wie von NIST SP 800-82[R3] empfohlen) unterteilt werden, um die Sicherheitskontrolle zu verbessern. Eaton empfiehlt, nur die Ports freizugeben, die für den Betrieb erforderlich sind, und die Netzwerkkommunikation mit Netzwerkschutzsystemen wie Firewalls und Zugangskontrollsystemen / Intrusion Prevention Systemen zu schützen. Verwenden Sie die folgenden Informationen, um Ihre Firewallkonfiguration so anzupassen, dass der für den reibungslosen Betrieb von VisionGuard erforderliche Zugriff möglich ist.

Fernzugriff	Der Fernzugriff auf Geräte/Systeme schafft einen weiteren Einstiegspunkt in das Netzwerk. Eine strenge Verwaltung und Validierung der Beendigung eines solchen Zugriffs ist unerlässlich, um die Kontrolle über die gesamte IKS-Sicherheit (interne Kontroll Systeme) zu behalten. Das Produkt unterstützt den interaktiven Fernzugriff nicht automatisch.
Protokoll- und Eventmanagement	• Eaton empfiehlt, alle relevanten System- und Anwendungsereignisse zu protokollieren, einschließlich aller Verwaltungs- und Wartungsaktivitäten. • Protokolle sollten vor Manipulationen und anderen Risiken für ihre Integrität geschützt werden (z.B. durch Einschränkung der Zugriffs- und Änderungsrechte, Übertragung von Protokollen an ein Sicherheitsinformations- und Ereignisverwaltungssystem usw.). • Stellen Sie sicher, dass die Protokolle für eine angemessene und ausreichende Zeit aufbewahrt werden. • Überprüfen Sie die Protokolle regelmäßig. Die Häufigkeit der Überprüfung sollte angemessen sein, wenn man die Empfindlichkeit und Kritikalität des Systems und aller Daten, die es verarbeitet, berücksichtigt.
Schwachstellen-Scanning	Es ist nicht möglich, Software von Drittanbietern zu installieren und zu nutzen. Alle bekannten kritischen oder schwerwiegenden Schwachstellen auf Komponenten/Bibliotheken von Drittanbietern, die zur Ausführung von Software/Anwendungen verwendet werden, sollten behoben werden, bevor das Gerät /-System in Betrieb genommen wird. Informationen über Schwachstellen für den VisionGuard erhalten Sie, wenn Sie sich unter *www.eaton.com/cybersecurity* für Updates anmelden, oder Sie können auch in der National Vulnerability Database (NVD) unter *https://nvd.nist.gov/* nach Schwachstellen suchen. **Hinweis:** Viele Compliance-Frameworks und Sicherheits-Best-Practices erfordern eine monatliche Überprüfung der Schwachstellen. Für viele Nicht-COTS-Produkte (Commercial-off-the-shelf) werden Schwachstellen direkt über die Herstellerseite kommuniziert.
Schutz vor Malware	Eaton empfiehlt den Einsatz geeigneter Malware-Abwehrmaßnahmen zum Schutz des Produkts oder der Plattformen, auf denen das Eaton-Produkt betrieben wird.
Sichere Wartung	**Best Practices** Auf der Website zur Cybersicherheit von Eaton (www.ceag.de) finden Sie Informationen über verfügbare Firmware und Software-Updates.
Geschäftskontinuität / Cybersicherheit Notfallwiederherstellung	Plan für die Geschäftskontinuität / Cybersicherheit Notfallwiederherstellung Eaton empfiehlt, in die Geschäftskontinuitäts- und Notfallmodelle des Unternehmens aufzunehmen. Unternehmen sollten einen Geschäftskontinuitätsplan und einen Notfallplan erstellen und diese Pläne regelmäßig überprüfen und, wenn möglich, anwenden. Als Teil des Plans sollten wichtige System-/Gerätedaten gesichert und sicher gespeichert werden, einschließlich: • Aktualisierte Software für VisionGuard. Machen Sie es zum Bestandteil der Standardprozedur, die Sicherungskopie zu aktualisieren, sobald die neueste Software aktualisiert wird. • Aktuelle Konfiguration • Dokumentation der aktuellen Berechtigungen / Zugriffskontrollen, falls nicht im Rahmen der Konfiguration gesichert;
Offenlegung vertraulicher Informationen	Eaton empfiehlt, dass vertrauliche Informationen (z.B. Konnektivität, Protokolldaten, persönliche Daten), die von der VisionGuard gespeichert werden können, durch den Einsatz von organisatorischen Sicherheitsverfahren angemessen geschützt werden.

Außerbetriebnahme oder Nullstellung	Es ist eine bewährte Vorgehensweise, Daten zu bereinigen, bevor Sie ein Gerät mit Daten entsorgen. Richtlinien für die Stilllegung sind in NIST SP 800-88 enthalten. Eaton empfiehlt, dass Produkte mit eingebettetem Flash-Speicher sicher zerstört werden, um sicherzustellen, dass Daten nicht wiederhergestellt werden können.

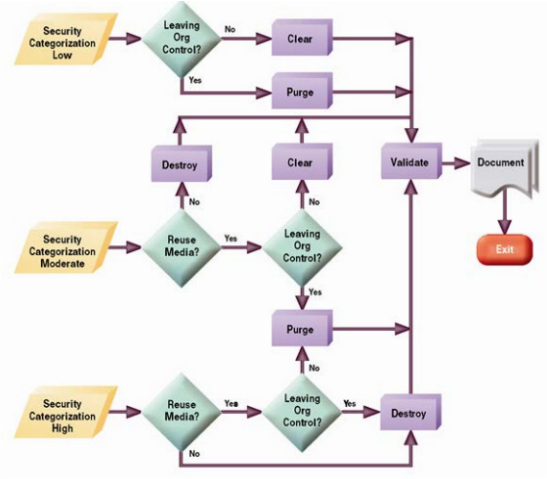


Figure 4-1: Sanitization and Disposition Decision Flow

* Abbildung und Daten aus NIST SP800-88

- Integrierter Flash-Speicher in Platinen und Geräten
- Eaton empfiehlt die folgenden Verfahren zur Entsorgung von Motherboards, Peripheriekarten wie Netzwerkadaptern oder anderen Adaptern mit nichtflüchtigem Flash-Speicher.
- **Löschen:** Wenn vom Gerät unterstützt, setzen Sie den Zustand auf die ursprünglichen Werkseinstellungen zurück.
- **Bereinigen:** Wenn der Flash-Speicher leicht identifiziert und von der Karte entfernt werden kann, kann der Flash-Speicher unabhängig von der Karte, die den Flash-Speicher enthielt, zerstört werden. Andernfalls sollte die gesamte Platine zerstört werden.
- **Vernichten:** Es wird empfohlen zur Entsorgung von Speichern diese sicher zu vernichten, z.B. durch schreddern.

1.3. Systemvoraussetzungen – Hardware/ Software Anforderungen

Folgende Hardware wird für einen einwandfreien Betrieb der VisonGuard empfohlen. Die VisionGuard Server Software ist nicht lauffähig auf Linux oder Mac OS Betriebssystemen! Der VisionGuard Client kann dagegen ein beliebiger Web-Browser sein, d.h. unabhängig vom Betriebssystem.

VisionGuard Server

Hardware: Standard PC (Tower, Rack), Virtuelle Maschine (VMWare/Hyper-V)

Betriebssystem: WIN 10 (64 Bit), WIN Server 2016, WIN Server 2019

Prozessor: min. Intel Core i5 oder AMD Ryzen 5

Speicher (RAM): min. 8 GB , empfohlen 16GB DDR4 SDRAM

HDD: min. 256 GB SSD

Client

Hardware: Standard PC Arbeitsplatz, AiO-PC

Grafik: DirectX 12

Software: Standard Webbrowser z.B. Edge, Chrome, Firefox, Safari

Monitor: min. 19 Zoll, empfohlen 24 Zoll FullHD

optimale Auflösung: FullHD 1920x1080 oder höher

Peripherie: Tastatur, Maus, Drucker

1.4. VisionGuard Lizenzen

1.4.1 Lizenzmodelle

Die VisionGuard ist vor unbefugten Betrieb geschützt. Für eine Freischaltung zum Betrieb der VisionGuard ist eine Lizenz notwendig. Die Lizenz ist abhängig von den angeschlossenen DualGuard-S Systemen. Ein Upgrade auf eine höhere Volumenlizenz ist problemlos möglich. Es sind folgende Volumen Lizenzen erhältlich:

- Basis Version für 3 Geräte
- Basis Version für 10 Geräte
- Basis Version für 25 Geräte
- Basis Version für 50 Geräte
- Basis Version für 100 Geräte
- Basis Version für 500 Geräte
- Optional: VisionGuard BACnet/IP Schnittstelle

1.4.2 Lizensierungsablauf

Bei Erwerb einer Lizenz wird diese online auf einem Lizensierungsserver hinterlegt. Nach Installation der VisionGuard muss in einem Lizensierungmenü ein Fingerprint erzeugt werden. Hierbei wird ein Schlüssel basierend der verbauten Hardwarekomponenten erstellt. Der Fingerprint hat das Dateiformat fingerprint.c2v.

Dieser muss online im Lizensierungsserver eingeben werden. Dieser erzeugt aufgrund der erworbenen Volumenlizenz einen Aktivierungsschlüssel in Form einer Lizenzdatei im Dateiformat „.v2c".

Diese Lizenzdatei muss wiederum im Lizensierungsmenü der VisionGuard eingelesen werden, um die VisionGuard für die Anzahl der erworbenen Systeme freizuschalten.

Der Lizensierungsablauf ist detailliert im Kapitel 4 Lizensierung beschrieben

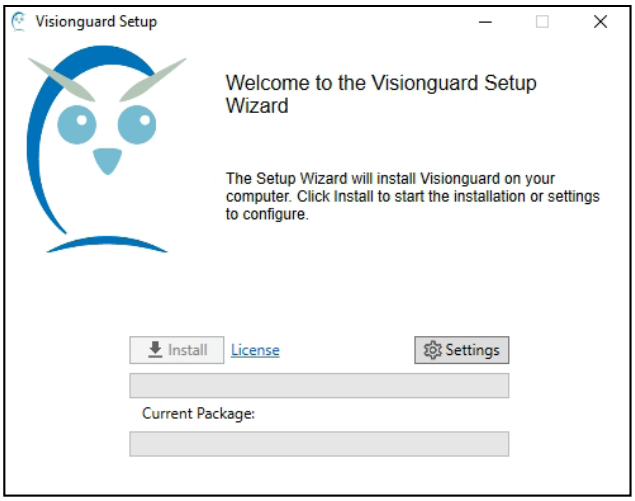
2 Installationsanleitung

2.1 Installation

Die aktuellste VisionGuard Version ist als Download auf der Produktseite von VisionGuard auf www.eaton.com verfügbar. Es wird empfohlen sich diese Version vor Installation auf ein Verzeichnis z.B. C:/Temp herunterzuladen. Soll die Installation auf einer anderen Windows-Umgebung erfolgen, wird empfohlen die VisionGuard auf einen externen Datenträger, z.B. USB-Stick herunterzuladen. Um die Installationszeit möglichst gering zu halten, wird empfohlen, die Installation von einem lokalen SSD-Laufwerk oder Festplatte durchzuführen, nicht von einem USB-Stick oder anderen externen Datenträger!

Die Installation wird gestartet über das ausführen des Visionguard Installers:

Visionguard_Installer_2.0.0.exe

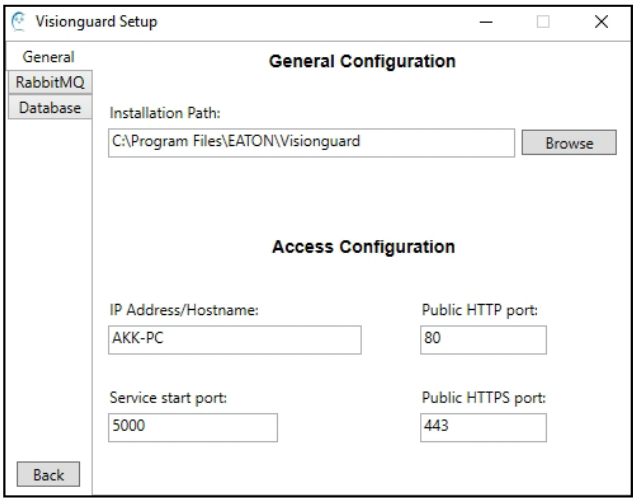


Nach Doppelklick auf die Datei startet der VisionGuard Setup Wizard. Eventuell erscheint erst eine Meldung der Windows Benutzerkontensteuerung. In dem Fall bitte mit „JA" bestätigen.

Über „Settings" können weitere Installationseinstellungen vorgenommen werden. Es wird aber empfohlen, die voreingestellten Werte zu übernehmen. Änderungen sollten nur durch IT-Administratoren vorgenommen werden!

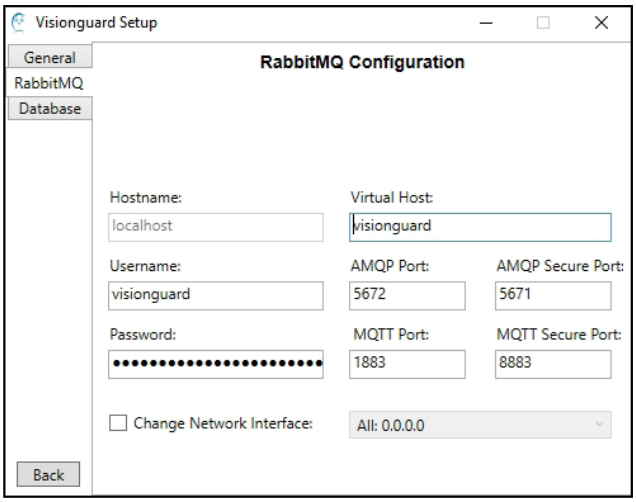
Settings > General

Hier kann der Installationspfad und der Hostname des PC`s bestimmt werden. Dieser wird zur Anbindung der HMI der DualGuard-S an die VisionGuard benötigt. Alternativ kann zur Anbindung aber auch die IP-Adresse des PC`s genutzt werden. Weiterhin können ein Portbereich und die Webclient Ports für die Webzugriffe festgelegt werden. Es muss ein Startportbereich definiert werden, was dann min. 30 Ports für die VisionGuard reserviert. Defaultmässig ist der Start-Port 5000 vorgegeben. Als Webclient Ports sind die Standardports 80 für unverschlüsselten http-Zugriff und der Port 443 für verschlüsselten https-Zugriff vorgegeben.

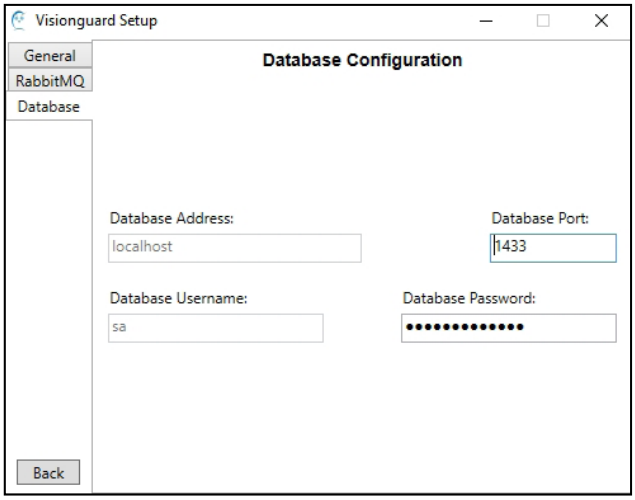


Settings > RabittMQ

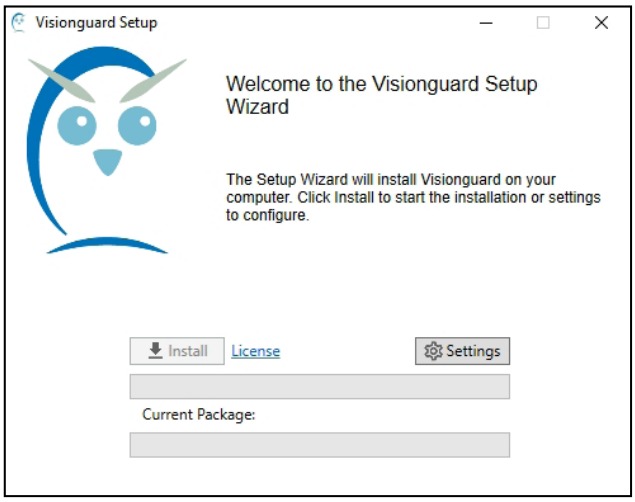
Dieses Dialogfenster dient zur Konfiguration der Kommunikationsschnittstelle der VisionGuard. Über den Hostnamen kann später die VisionGuard lokal auf dem PC per Webbrowser aufgerufen werden. Defaulteinstellung ist „localhost", d.h. der lokale Aufruf der VisionGuard erfolgt nach der Installation über http://localhost (unverschlüsselt) oder über https://localhost (verschlüsselt).



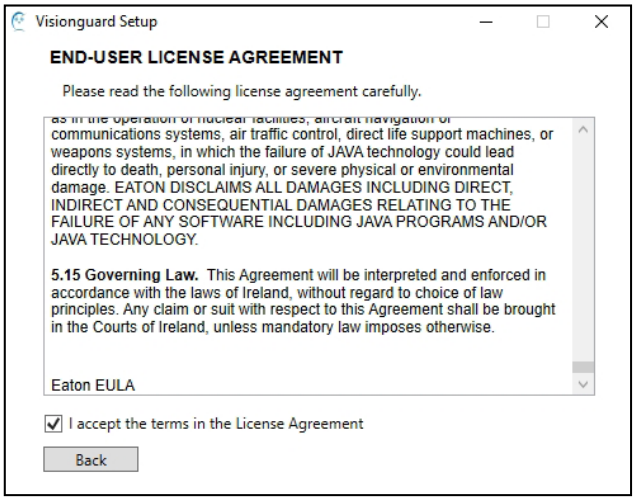
Settings > Database
In diesem Dialogfenster können die Vorgaben der MSSQL Datenbank verändert werden.
Auch hier wird unbedingt empfohlen die vorgegebenen Einstellungen beizubehalten.



Zurück mit „Back“. Um die Installation starten zu können muss erst die EULA (End-User License Agreement) gelesen und bestätigt werden. Die EULA wird über den Link „License“ geöffnet

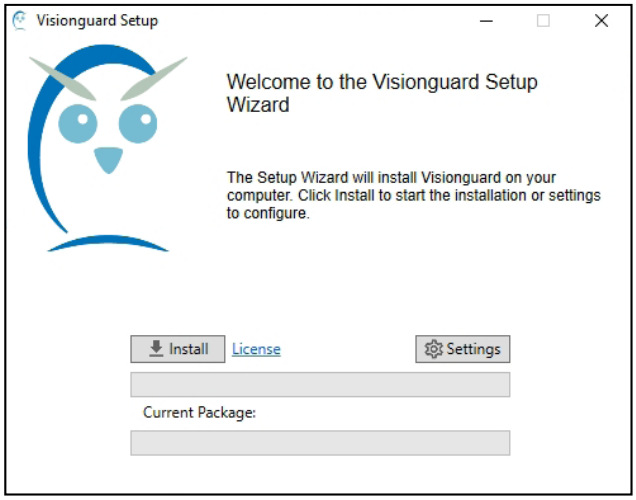


Bitte lesen Sie die EULA (End-User License Agreement) aufmerksam durch, und bestätigen die EULA durch aktivieren „I accept the terms in the License Agreement“.

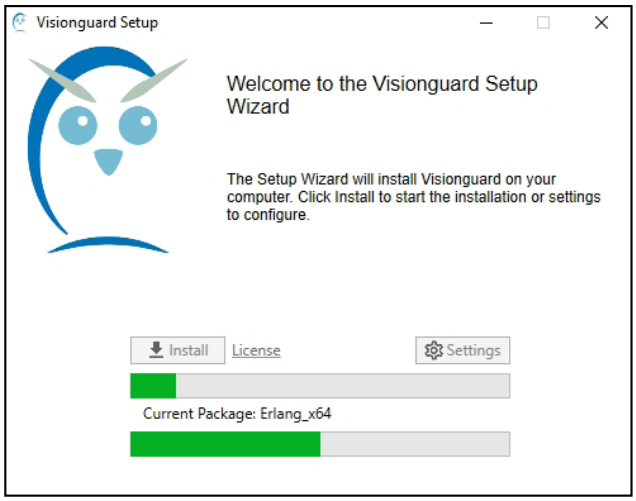


Zurück mit „Back“.

Die Installation kann nun über „Install“ gestartet werden

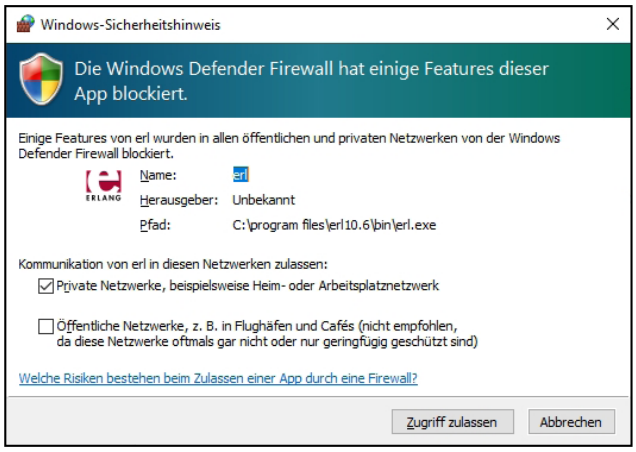


Es folgen eventuell bis zu drei Sicherheitsabfragen der Windows Benutzerkontensteuerung (UAC). Diese bitte mit „Ja“ bestätigen. Die Installation kann einige Minuten in Anspruch nehmen! Bitte starten Sie keine anderen Anwendungen während der Installation. Der Installations-fortschritt wird über Fortschrittsbalken angezeigt.



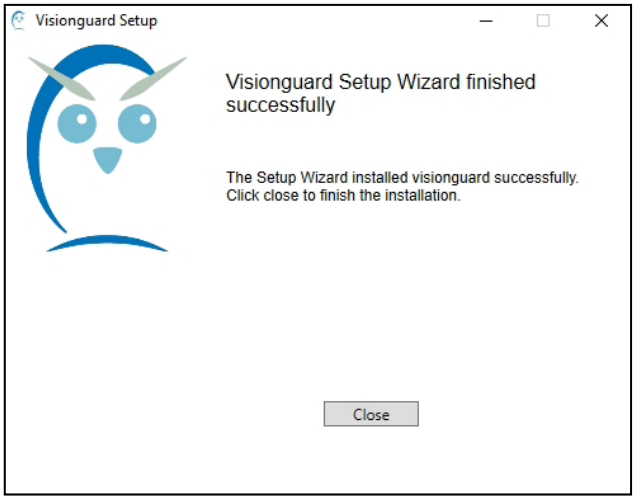
Falls eine Firewall aktiv ist, können Meldungen erscheinen, die die Funktionen einiger Apps blockieren.
z.B. beim Windows Defender kann folgende Meldung erscheinen:

Es müssen unbedingt alle Zugriffe zugelassen werden, da ansonsten die HMIs der DualGuard-S keine Verbindung zur VisionGuard aufbauen können!



Nach Beendigung der Installation kann der Installationsassistent im nächsten Fenster über „Close“ beendet werden.

Die Installation ist jetzt abgeschlossen. Es wird unbedingt empfohlen einen Neustart des PC`s durchzuführen!



2.2 Update einer bestehenden VisionGuard Installation

2.2.1 Updatebeschreibung

Ein Update kann notwendig sein, wenn neue Funktionen verfügbar sind, oder Fehler durch Bugfixes behoben wurden! Es wird empfohlen die Software auf neuestem Stand zu halten.

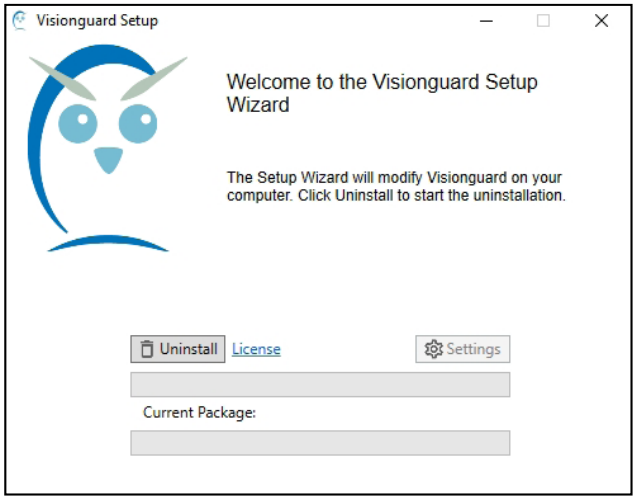
Die aktuellste VisionGuard Version ist auf der Produktseite von VisionGuard auf unserer Webseite www.eaton.com zum Download verfügbar. Es wird empfohlen in regelmässigen Abständen, z.B. 3-6 Monaten die Webseite auf Updates zu überprüfen, und die VisionGuard Update Software für eine Installation entweder direkt auf den PC oder auf einen USB-Stick zu laden.

Bei einem Update ist keine Deinstallation der bisherigen Version notwendig, d.h. ein Update kann einfach über eine bestehende VisionGuard installiert werden. Hierzu muss jedoch die aktuelle VisionGuard beendet werden, bevor die Updateinstallation ausgeführt wird!

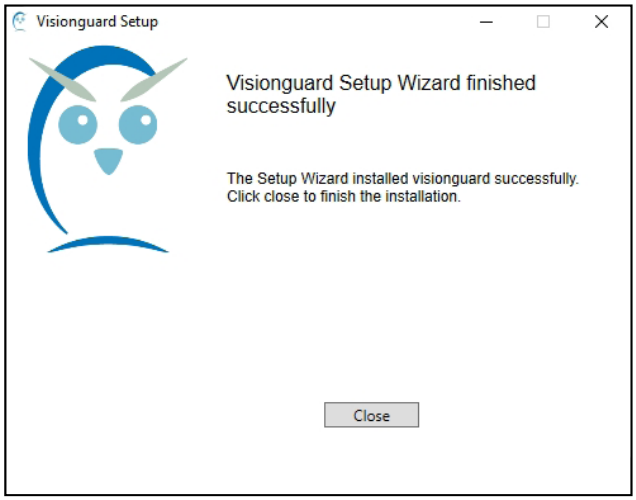
Bestehende Konfigurationen werden nicht überschrieben, es wird aber aus Sicherheitsgründen empfohlen, eine Sicherung der bestehenden VisionGuard durchzuführen. Eine Back-Up Funktion in der VisionGuard ist erst für Version 2 geplant. Eine Sicherung sollte bis dahin mit einem externen Back-Up Programm, oder über die im Windows verfügbare Dateiversionsverlauf-Sicherung durchgeführt werden.

2.2.2 Durchführen eines Updates

Für ein Update der VisionGuard wird einfach wie in 2.1 Installationsanleitung beschrieben, der Installer ausgeführt. Es erscheint folgendes Dialogfenster:



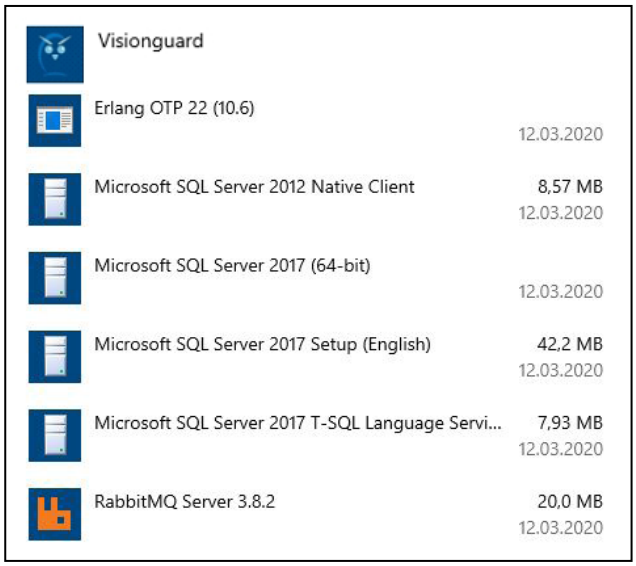
Mit Klick auf „Uninstall", wird erst die VisionGuard deinstalliert, und die neue Installation gestartet was ca. 5 Minuten in Anspruch nimmt.
Ein Fortschrittsbalken informiert über den aktuellen Updateverlauf. Zum Ende des Updates erscheint folgendes Fenster.



Nach Installation des Updates muss der PC unbedingt neu gestartet werden!

2.3 Deinstallation

Für eine Deinstallation muss die VisionGuard vorher beendet werden!
Eine komplette Deinstallation der VisionGuard kann über die Windowsfunktion „Apps & Features" erfolgen.
Folgende Dienste müssen deinstalliert werden:

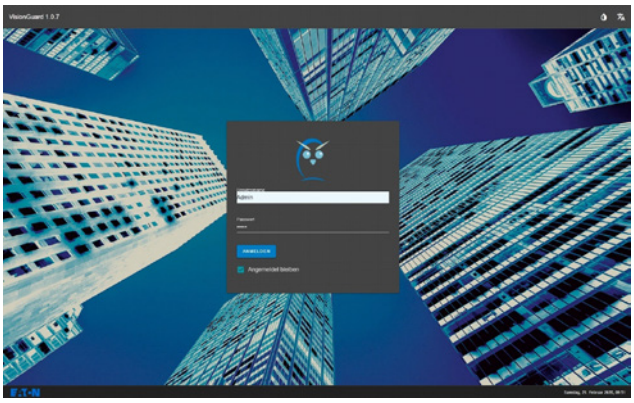


Nach der Deinstallation aller rechts stehenden Anwendungen muss der PC neu gestartet werden!

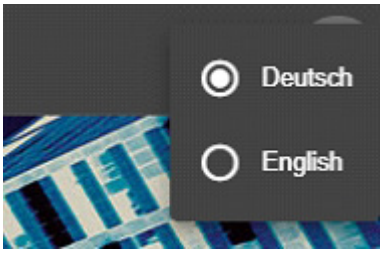
3 Erster Start der VisionGuard

3.1 Lokaler Zugriff (VisionGuard Server und Client auf ein PC)

Die VisionGuard wird bei einem lokalen Zugriff über über einen handelsüblichen Webbrowser, z.B. Microsoft Edge über die URL:
http://localhost (unverschlüsselt),
oder über
https://localhost (verschlüsselt) gestartet.
Es erscheint folgendes Anmeldefenster:

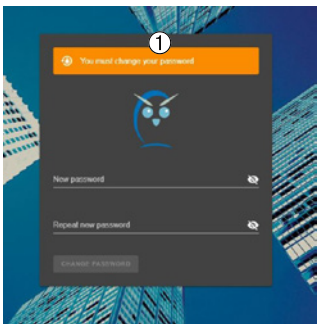


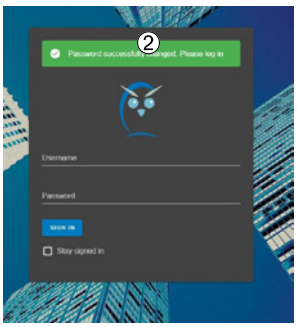
Im obigen rechten Bereich kann die Sprache voreingestellt werden:



Es ist in der VisionGuard ein Standard-Benutzer mit Supervisor Rechten voreingestellt!
Der Benutzername und das Passwort für die erste Anmeldung des Standard-Benutzers ist:
Benutzername: Admin
Passwort: EATON

Die Aufforderung kommt, ein neues Passwort zu vergeben! ①





Voreingestellt ist eine Passwortsicherheit von min. 6 Zeichen, die jeweils mindestens einen Großbuchstaben, Kleinbuchstaben, Zahl und ein Sonderzeichen enthalten muss:

WICHTIGER HINWEIS

Es wird dringend empfohlen, sich das neue Passwort zu notieren und sicher aufzubewahren!
Wurde das Passwort erfolgreich geändert, wird dieses im Anmeldefenster grün angezeigt ②. Jetzt muss der Login nochmal mit dem neuen Passwort durchgeführt werden:

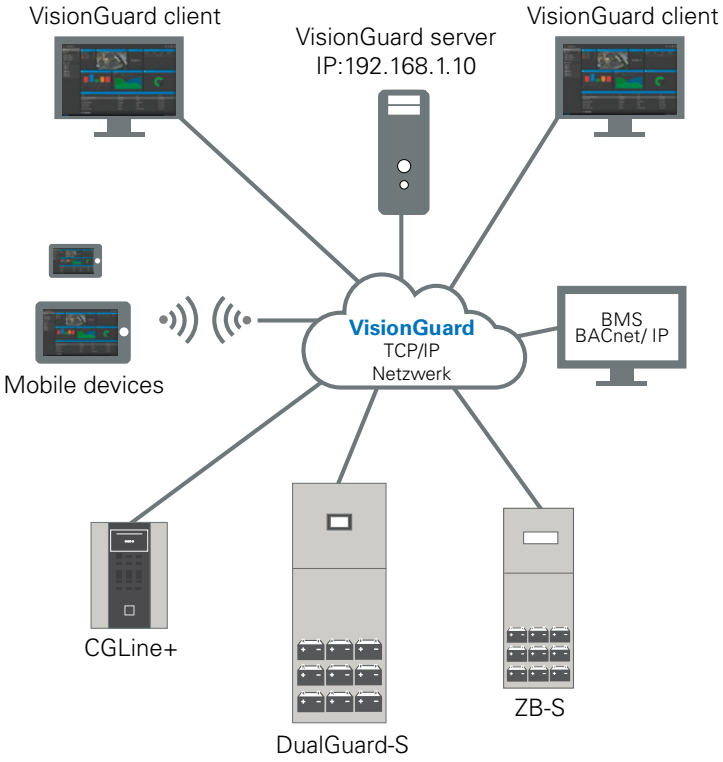
UAC – Passwort Richtlinien

Richtlinie	Wert
Zahl	Ja
Sonderzeichen	Ja
Kleinbuchstaben	Ja
Großbuchstaben	Ja
Minimale Passwortlänge	6

Nach der Anmeldung erscheint als Startbildschirm das Dashboard, was im Kapitel 8.2 näher erklärt wird:

3.2 Zugriff auf entferntem VisionGuard Server (VisionGuard Server und Client auf unterschiedlichen PC)

Soll der Zugriff auf die VisionGuard von einem anderen Client-PC über das Ethernet Netzwerk erfolgen, z.B. die VisionGuard auf einer virtuellen Umgebung installiert wurde, erfolgt der Zugriff über einen handelsüblichen Webbrowser, z.B. Microsoft Edge über die IP-Adresse des Server PCs, z.B. : http://192.168.1.10 (unverschlüsselt), oder über https://192.168.1.10 (verschlüsselt).
Schema:



(Hinweis: CGLine+ und ZB-S in Vorbereitung)

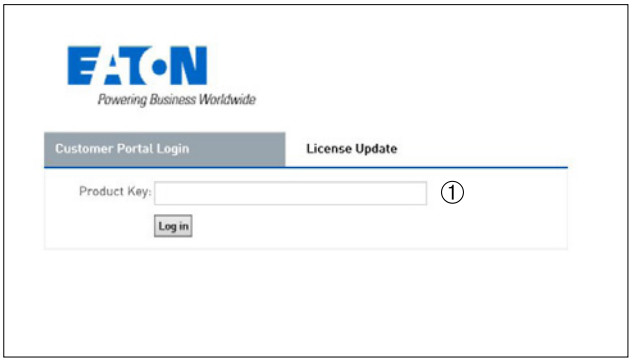
4 Lizensierung

4.1 Aktivierung einer Lizensierung

Um die VisionGuard nutzen zu können, muss dafür eine Lizenz erworben werden. Es sind unterschiedliche Lizenzen erhältlich, je nachdem wie viele DualGuard-S Systeme an die VisionGuard abgeschlossen werden sollen. Welche Lizenzen erhältlich sind, können Sie im Kapitel 1.4 VisionGuard Lizenzen nachlesen. Mit Erwerb einer VisionGuard Lizenz erhält der Kunde einen „Productkey“ in schriftlicher Form, der später benötigt wird.

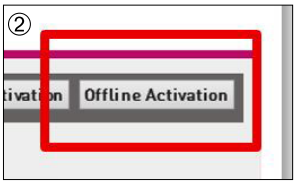
WICHTIGER HINWEIS

Eine Lizensierung darf nur von einem Benutzer mit Supervisor Berechtigungen durchgeführt werden!
Nach Login in die neuinstallierte VisionGuard erscheint folgende Meldung „nicht lizensiert“: ①



Um eine Lizensierung durchführen zu können, muss im Menü: Administration/Information/Licenzen ein Fingerprint abgerufen werden.

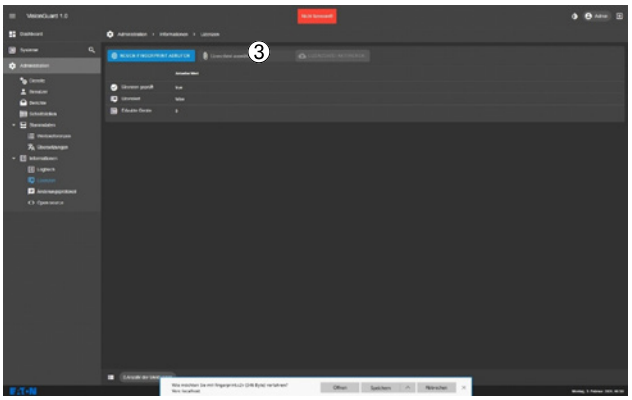
① „Neuen Fingerprint abrufen“



② Es wird eine Datei mit dem Namen „fingerprint.c2v“ erzeugt, die in einem Ordner, z.B. C:\temp oder auf einen externen Datenträger, z.B. USB-Stick gespeichert werden muss.
Diese Datei muss nun online im Lizenzserver unter *https://ceagsystems.sentinelcloud.com/ems/customerLogin.html* hochgeladen werden (siehe Pos. 1).

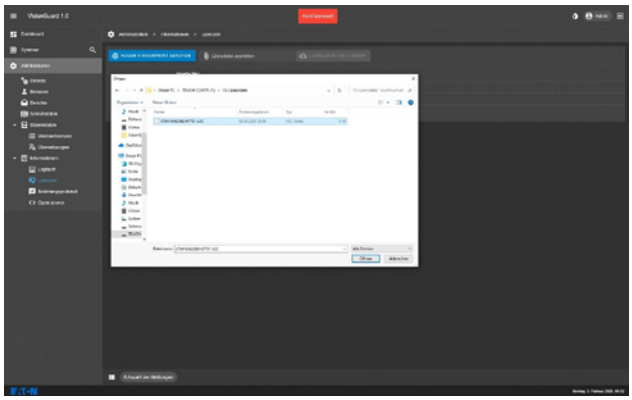
Für einen Login muss im Feld „Product Key“ der 32-stellige erworbene Produktkey eingegeben werden. Dieser hat das Format:
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Nach Login sollten im Aktivierungsregister Namen und Kontaktdaten eingegeben werden (freiwillig).
Wählen Sie oben rechts „Offline Activation“. (Pos.2)
Laden Sie jetzt den in der VisionGuard erzeugten Fingerprint im Feld „Upload C2V“ rein, indem Sie die Quelle, z.B. USB-Stick über „...“ suchen und selektieren. (Pos.3)

Der Lizenzserver erzeugt über „Generate“ ein Aktivierungsschlüssel der auf dem lokalen Datenträger z.B. C:\temp oder auf einen USB-Stick runtergeladen werden kann.

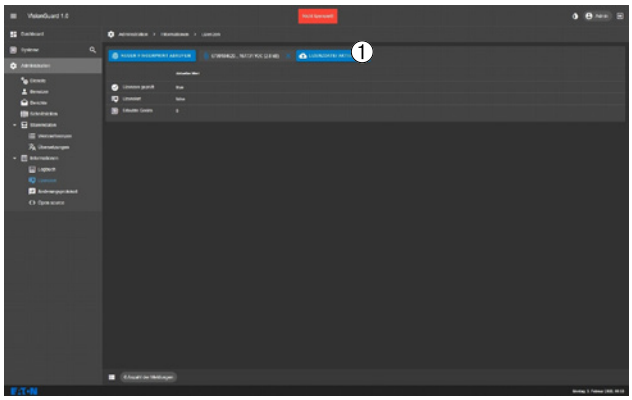


③ Über „Lizenzdatei auswählen“ kann der Aktivierungsschlüssel in die VisionGuard geladen werden

Im Dialogfenster kann nun der Speicherort des Aktivierungsschlüssel angegeben werden

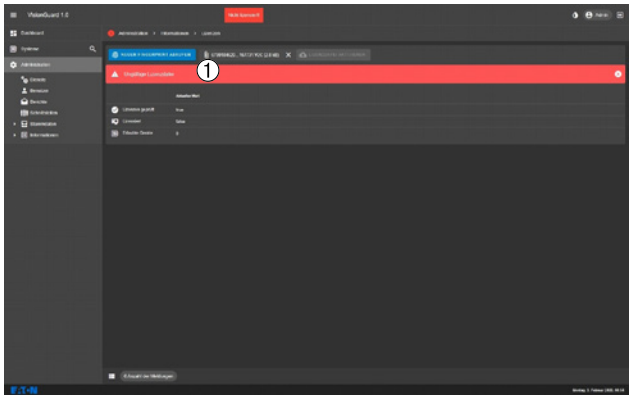


① Über „Lizenzdatei aktivieren“ kann die erworbene Lizenz in der VisionGuard aktiviert werden



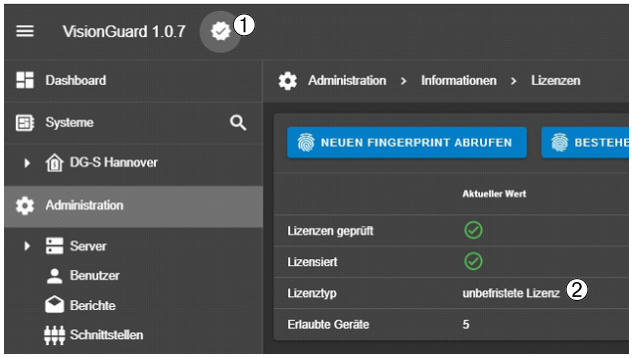
① Es erscheint noch die Meldung „ungültige Lizenzdatei“

Über die Tastaturkombination „Strg“ und „F5“ wird der Cache des Webbrowsers gelöscht und die Webseite neu geladen



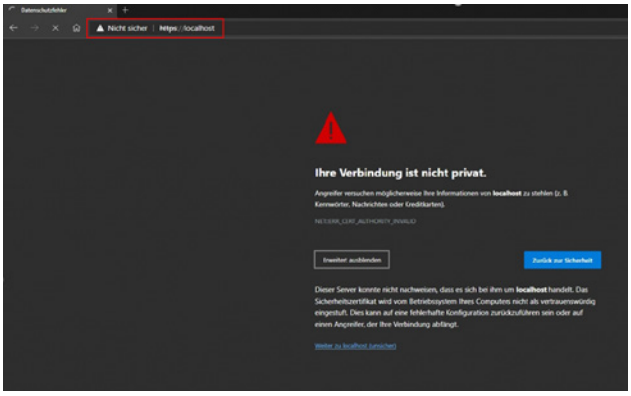
① Die Aktivierung ist nach laden der neuen Webseite nun aktiv! Dieses wird über das weiße Siegel angezeigt

② Hier wird der Lizenztyp und die erworbene Volumenlizenz angezeigt, die angibt wie viele Notlichtsysteme an die VisionGuard angeschlossen werden dürfen



5 Installation von Sicherheitszertifikaten

Erfolgt der Zugriff auf die VisionGuard über das verschlüsselte HTTPS-Protokoll müssen im Webbrowser Sicherheitszertifikate installiert werden, damit der Webbrowser den Zugriff nicht als unsicher einstuft und einen Zertifikatsfehler anzeigt:



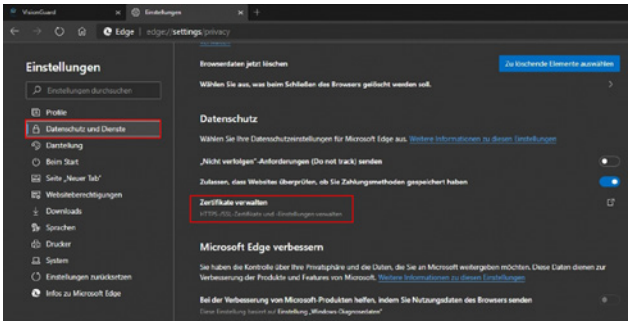
Hier muss unterschieden werden, ob der Zugriff von einem Client-PC aus dem Netzwerk heraus erfolgt, oder lokal auf demselben PC.

5.1 Installation des Sicherheitszertifikates bei lokalem Zugriff

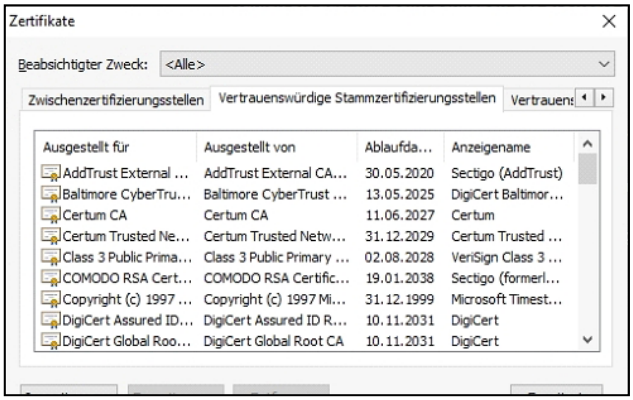
Erfolgt der Zugriff von einem Browser auf einen lokal installierten VisionGuard muss folgendermaßen vorgegangen werden. Die folgende Anleitung bezieht sich auf den Chrom-Browser. Bei anderen Browsern muss ähnlich vorgegangen werden.

HINWEIS

Diese Zertifikatsinstallation ist bei jedem Client-PC einmalig notwendig!
Öffnen sie im Browser das Menü Einstellungen > Datenschutz und Dienste > Zertifikate verwalten

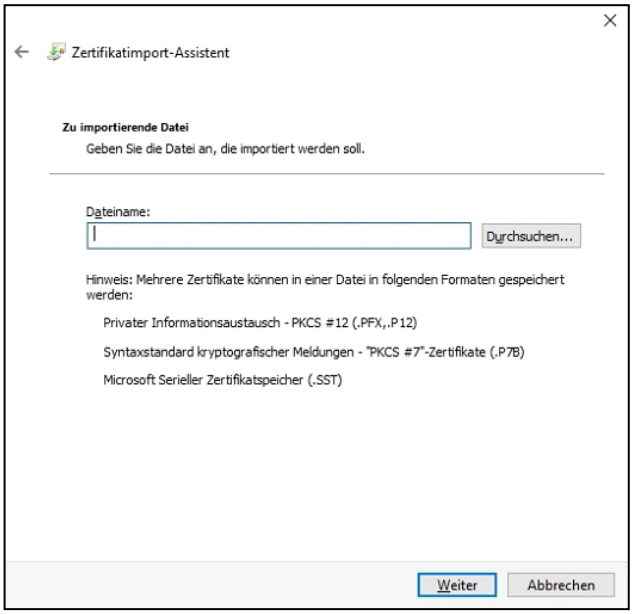


Über „Zertifikate verwalten“ öffnet sich die Zertifkatsverwaltung, in der man Zertifikate importieren kann



Über „Importieren“ startet man den Zertifikat-Import Assitenten

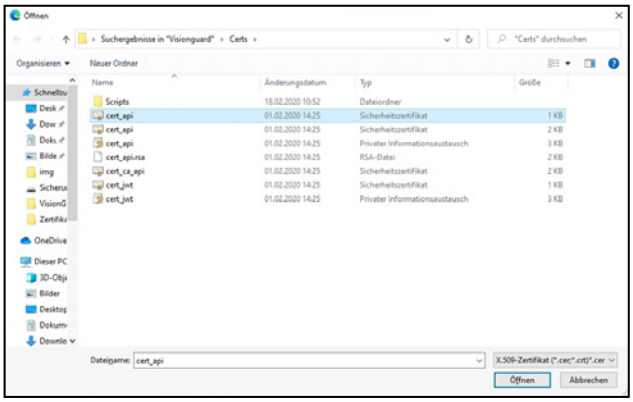
Über „Weiter“ kann man im nächsten Dialogfenster nach dem Zertifikat suchen



Über „Durchsuchen“ kann man das Zertifikat auswählen. Es befindet sich im Ordner:

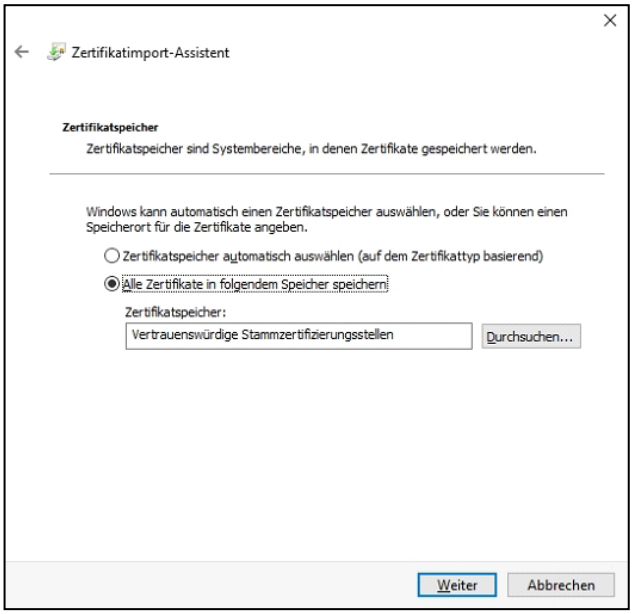
C:\Programme\EATON\Visionguard\Certs

Das Zertifikat hat den Namen: cert.api



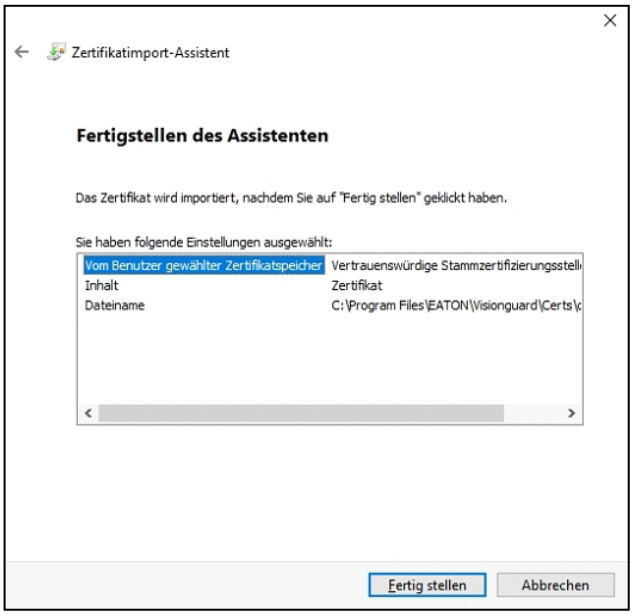
Nach Auswahl des Zertifikats wird fortgefahren mit „Öffnen“

Das Zertifikat muss im Zertifikatsspeicher „Vertrauenswürdige Stammzertifizierungsstellen“ gespeichert werden

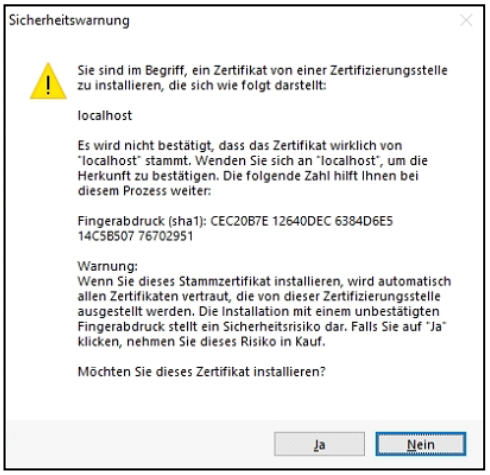


Fortfahren mit „Weiter“

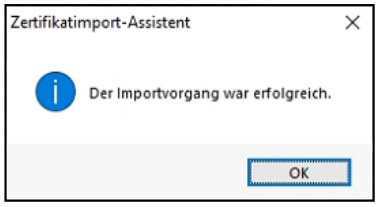
Beenden mit „Fertig stellen“



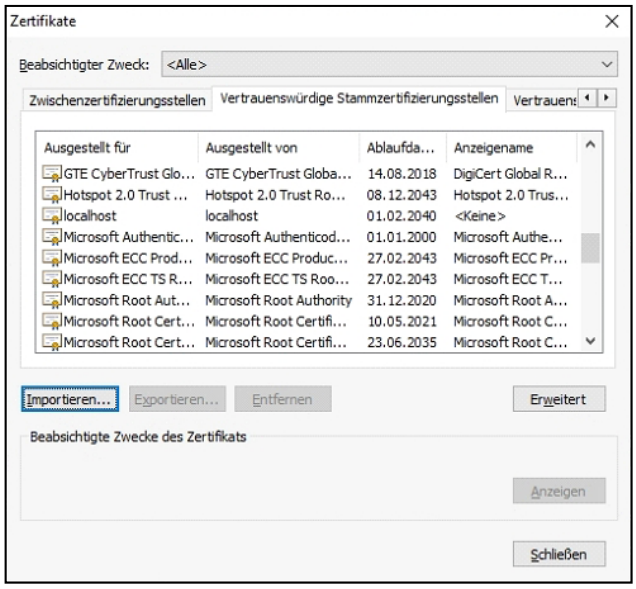
Das Zertifikat kann in der Sicherheitswarnung jetzt über „Ja“ installiert werden



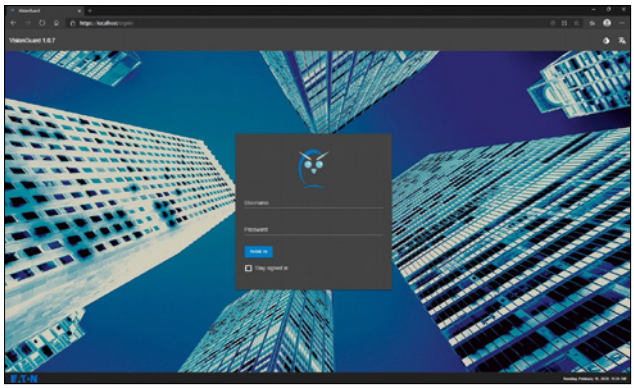
Es muss folgende Meldung erscheinen



Geprüft werden kann der Importvorgang in der Zertifikatsverwaltung. Dort muss unter „Vertrauenswürdige Stammzertifizierungsstellen“ das Zertifikat „localhost“ mit dem Ablaufdatum 2099 erscheinen



Die nächsten Zugriffe auf die VisionGuard erfolgen nun ohne Fehlermeldung „Zertifikatsfehler“



5.2 Installation des Sicherheitszertifkates bei Fernzugriff

Erfolgt der Zugriff auf den VisionGuard Server von einem entfernten Web-Client im Netzwerk, dann muss das Zertifikat wie oben beschrieben vom VisionGuard Ordner auf einen Datenträger, z.B. USB-Stick geladen werden. Die Installation erfolgt dann genauso wie in 5.1 beschrieben, auf dem Client-PC, von wo auf die VisionGuard zugegriffen werden soll, nur mit dem USB-Stick als Quelle für das Zertifikat.

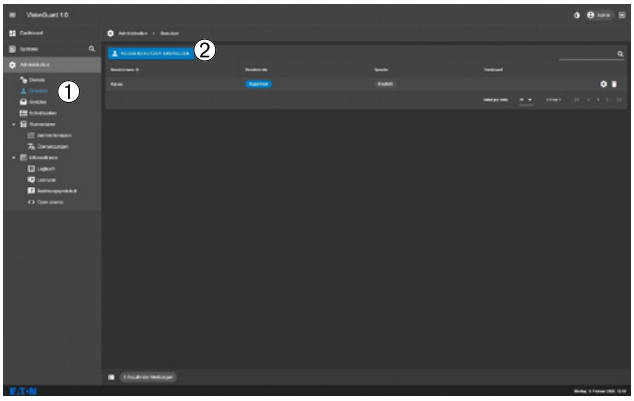
6 Neue Benutzer mit Benutzerrollen anlegen

6.1 Information zur Benutzerkontensteuerung (UAC = User Account Control)

In der VisionGuard können beliebig viele Benutzer mit unterschiedlichen Benutzerrollen angelegt werden. Die unterschiedlichen Benutzerrollen definieren unterschiedliche Zugriffsberechtigungen:

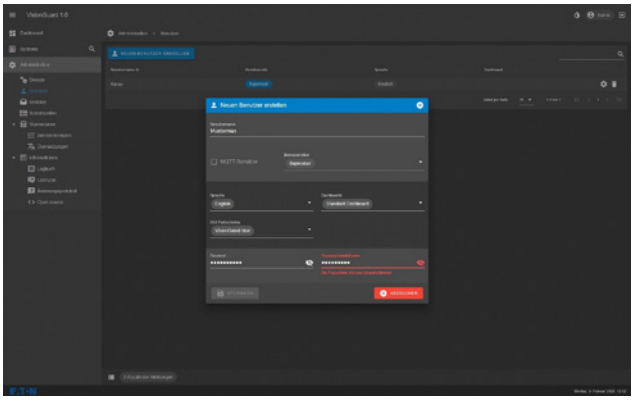
Rolle	VisionGuard administrieren	HMI konfigurieren	HMI steuern	HMI lesen
Supervisor	x	x	x	x
Administrator	x	x	x	x
Power User			x	x
User				x

Der Supervisor hat gegenüber dem Administrator noch die Berechtigung Benutzerkonten zu erstellen und zu editieren.
Es wird empfohlen nur einen Benutzer mit Supervisorberechtigung anzulegen, der die anderen Benutzerkonten verwaltet, um ungewünschte Änderungen durch zu viele Personen zu vermeiden.



① Das anlegen, editieren und löschen von Benutzern erfolgt im Menü Administration/Benutzer

② Über „Neuen Benutzer erstellen“ kann nun ein neuer Benutzer angelegt werden



① Unter Benutzername kann der Name des neuen Benutzers der im Anmeldefenster der VisionGuard eingegeben werden muss, festgelegt werden

② Unter Benutzerrolle kann eine Rolle mit unterschiedlichen Zugriffsberechtigungen festgelegt werden (siehe Tabelle oben)

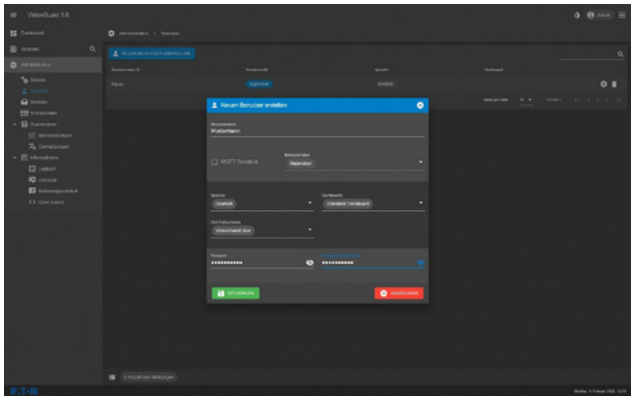
③ Unter Sprache kann die Benutzersprache fest voreingestellt werden. Es ist zwischen deutsch und englisch wählbar (weitere Sprachen sind in Vorbereitung)

④ Das Standard Dashboard ist fest voreingestellt, und kann nicht verändert werden

⑤ Hier kann das Farbschema für den Benutzer fest voreingestellt werden zwischen den Modi „Dunkel“ „Hell“ und „Blau“ (Dunkel mit blauen Kopfzeilen)

⑥ Hier wird das Passwort des neuen Benutzers festgelegt, und muss zur Sicherheit wiederholt werden.

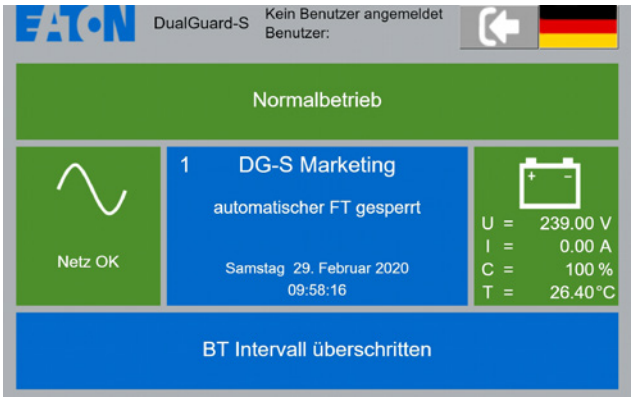
① Beide Passwörter müssen übereinstimmen, damit das Profil des neuen Benutzers gespeichert werden kann!



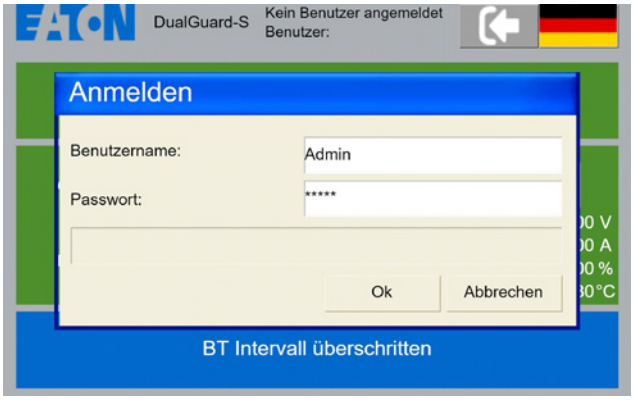
7 Anlegen von Dualguard-S Systemen an die VisionGuard

7.1 HMI zur Anbindung an VisionGuard konfigurieren

Um ein Dualguard-S System an der VisionGuard anzulegen, müssen am HMI Verbindungseinstellungen vorgenommen werden!
Hinweis: Um im HMI-Menü die Verbindungseinstellungen zur VisionGuard vornehmen zu können, muss man als „Experte“ angemeldet sein!
Die Verbindungseinstellungen können direkt am HMI oder idealweise per Webzugriff vorgenommen werden.
Anmeldung im HMI:

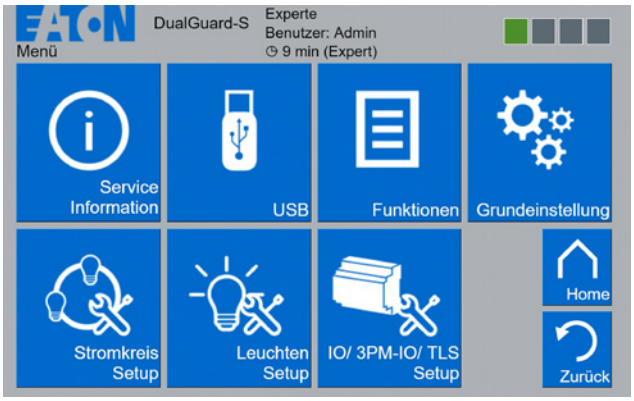


Eingabe von Benutzername und Passwort (Benutzer muss als „Experte“ angemeldet werden).

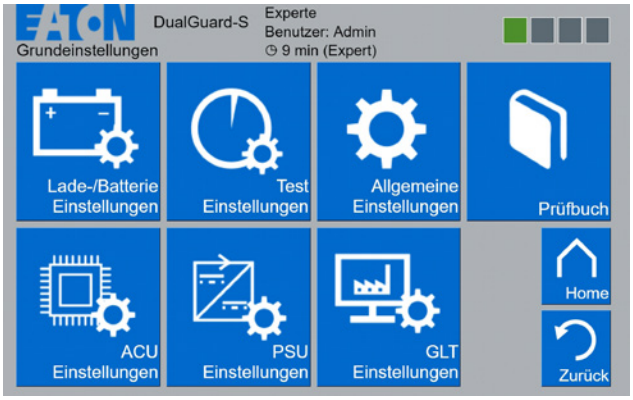


Weiter über „Menü“

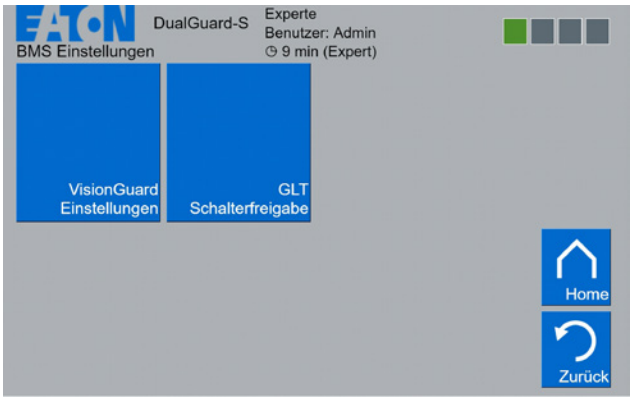
Weiter über „Grundeinstellung“



Weiter über „GLT-Einstellungen“

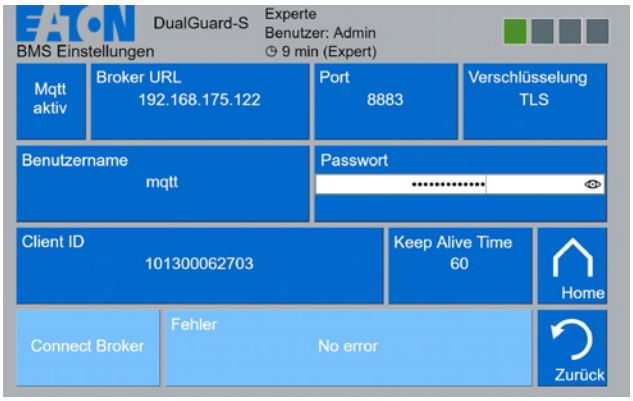


Weiter über „VisionGuard Einstellungen“



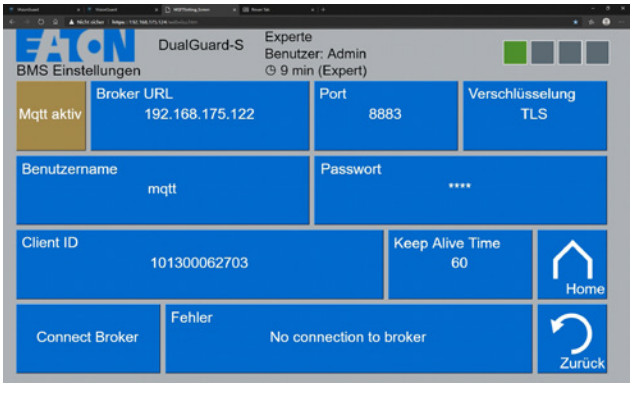
Im Menü „VisionGuard Einstellungen“ müssen folgende Eingaben gemacht werden:

- „Mqtt aktiv“ muss inaktiv sein (blaue Darstellung)
- In „Broker URL“ muss die IP-Adresse des VisionGuard PCs eingetragen werden
- „Port“ kann 1883 (unverschlüsselt) oder 8883 (verschlüsselt) sein. Es wird verschlüsselt empfohlen
- „Verschlüsselung“ muss bei Port 8883 auf TLS stehen
- „Benutzername“ muss identisch mit dem MQTT Benutzer in der VisionGuard sein (siehe Bild 7.2 2.)
- „Passwort“ muss identisch mit dem MQTT Benutzer Passwort in der VisionGuard sein (siehe Bild 3 in 7.2)



Nach obigen Einstellungen kann die MQTT-Schnittstelle aktiviert werden. Das HMI versucht nun eine Verbindung zur VisionGuard herzustellen. Hierzu muss nun in der VisionGuard das HMI autorisiert werden.

Siehe nächstes Kapitel 7.2.

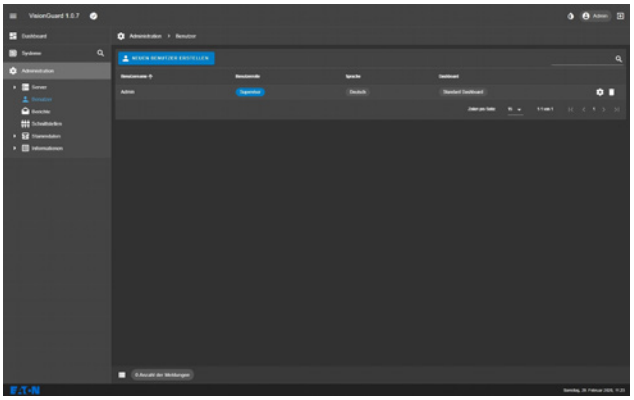


7.2 Anlegen und autorisieren einer DualGuard-S in der VisionGuard

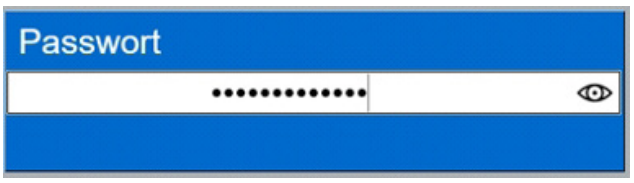
Damit Dualguard-S in der VisionGuard angelegt werden können, muss in VisionGuard ein MQTT-Benutzer angelegt werden.

① Dieses erfolgt im Menü Administration/Benutzer

② Über „Neuen Benutzer erstellen“ wird ein neuer MQTT-Benutzer angelegt



Im nächsten Dialogfenster müssen folgende Einstellungen vorgenommen werden:



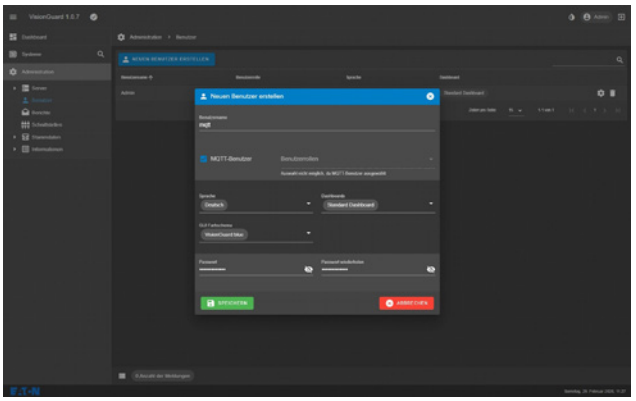
① Benutzername muss identisch dem Benutzernamen im HMI sein. Empfohlen wird der Einfachheit halber „mqtt“

② MQTT-Benutzer muss angehakt sein

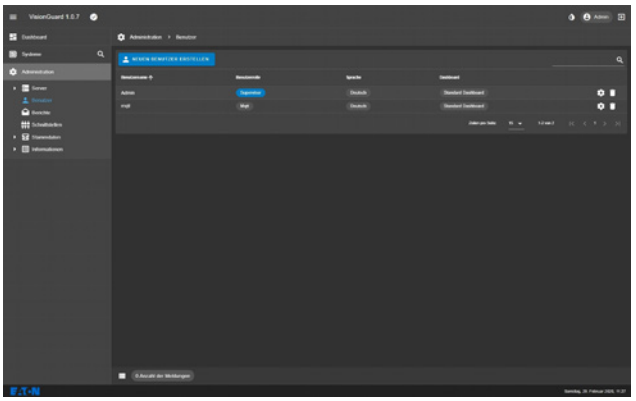
③ Die Einstellungen können beliebig erfolgen

④ Das Passwort muss identisch mit dem Passwort im HMI sein

⑤ Mit „Speichern“ werden die Einstellungen übernommen

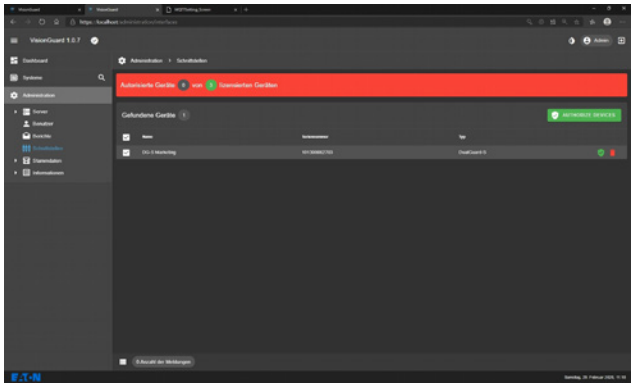


Der Benutzer für die Anbindung (hier mqtt) ist nun angelegt

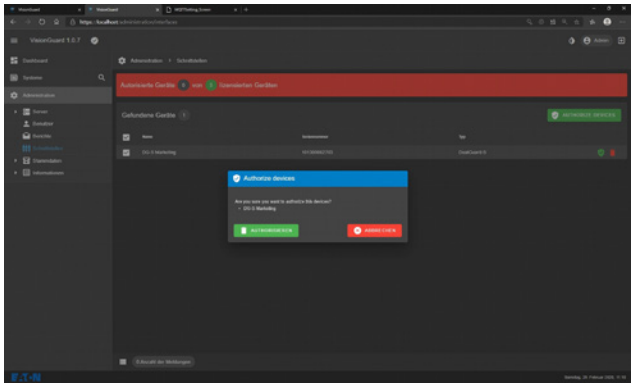


① Wenn die Einstellungen im HMI der Dualguard-S mit den Einstellungen des mqtt-Benutzers in der VisionGuard übereinstimmen, wird die DualGuard im Menü Administration/Schnittstellen angezeigt

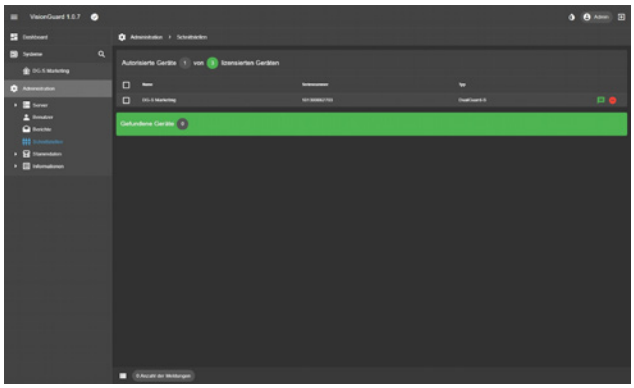
② Über „Gerät autorisieren“ wird die Dualguard-S in der VisionGuard angelegt



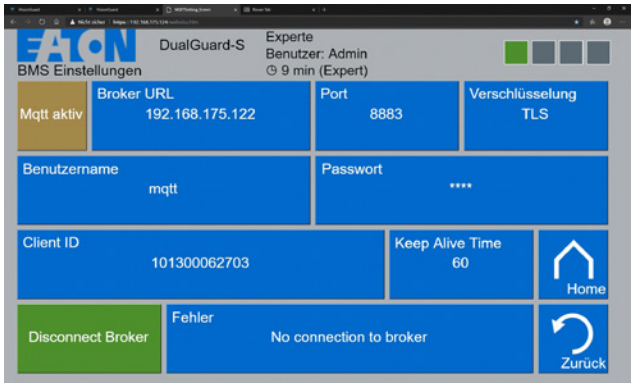
Bestätigen durch „Autorisieren“



Die DualGuard-S wurde nun in der VisionGuard erfolgreich angemeldet



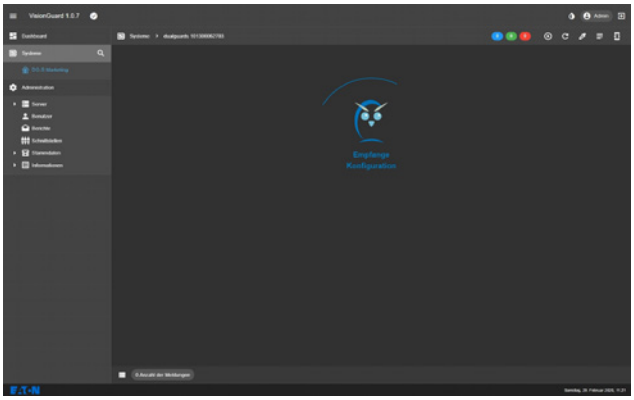
① Die korrekte Verbindung zwischen HMI und VisionGuard wird nun im HMI (grün) angezeigt



Die VisionGuard lädt jetzt automatisch die komplette Konfiguration der DualGuard-S

WICHTIGER HINWEIS

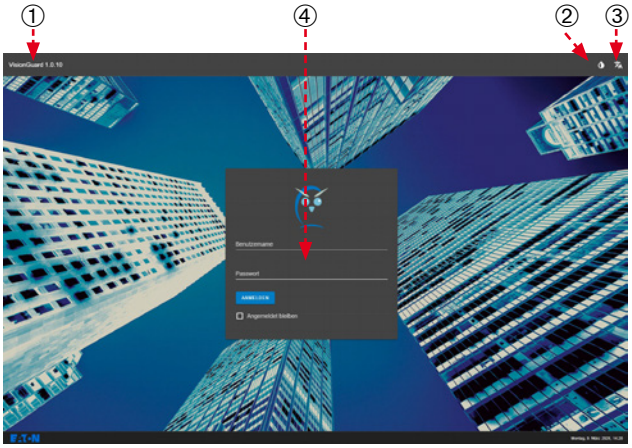
Das laden der Konfiguration kann je nach Anlagengröße mehrere Minuten in Anspruch nehmen! Bitte lassen Sie die Konfiguration vollständig laden, bevor weitere Einstellungen an der VisionGuard vorgenommen werden!



8 Grafischer Aufbau und Struktur der VisionGuard

8.1 Anmeldefenster

Nach Aufruf der VisionGuard über einen Webbrowser erscheint das Anmeldefenster



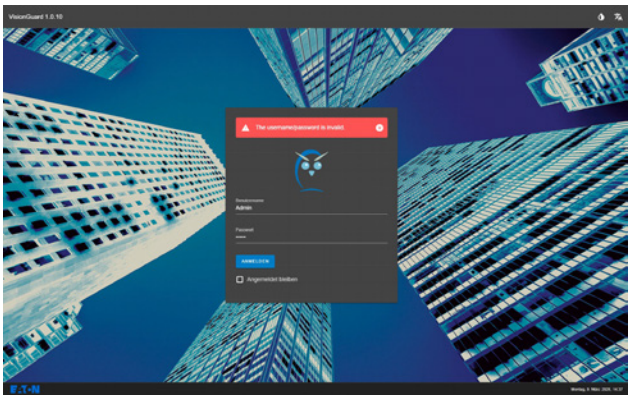
① Anzeige der aktuellen VisionGuard Version (hier z.B. V1.0.10)

② Umschaltung Hell-/Dunkelmodus

③ Umschaltung Login Sprache deutsch/englisch

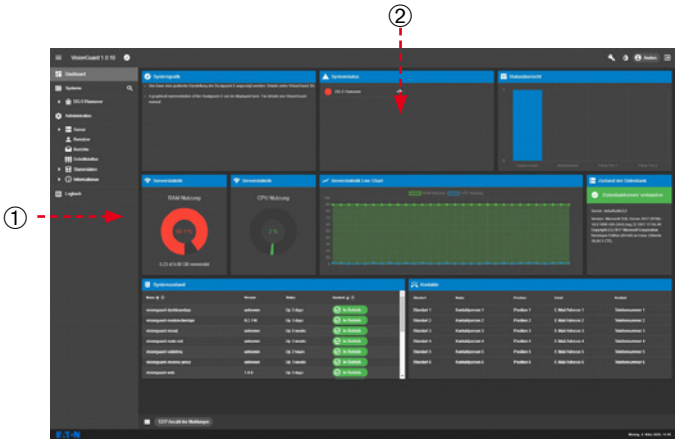
④ Eingabe von Benutzername und Passwort. Über „Angemeldet bleiben" kann man über eine Zeit von 8 Stunden ohne erneute Eingabe des Benutzernamens/ Passwort die VisionGuard öffnen, wenn **ohne** Abmeldung der Tab im Browser geschlossen wurde.

Wird der Benutzer oder das Passwort falsch eingegeben, erscheint eine Fehlermeldung



Sind die Anmeldedaten korrekt, öffnet sich als Startbildschirm das Dashboard der VisionGuard

8.2 Dashboard



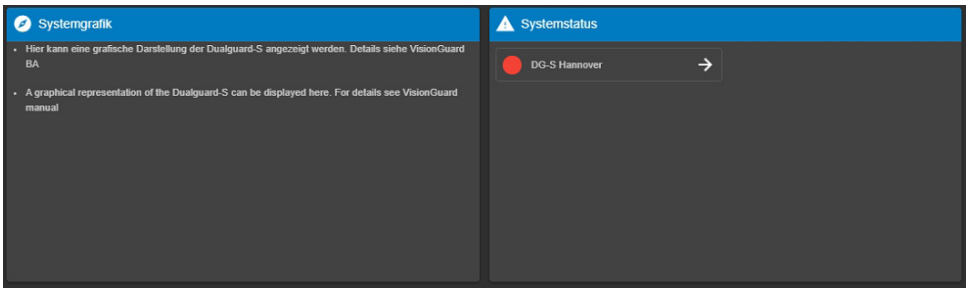
Das Dashboard (Armaturenbrett) dient dazu Informationen zur VisionGuard und den angeschlossenen Notlichtsystemem übersichtlich in einer Grafik darzustellen.

① Navigationsbereich zum direkten navigieren in die Untermenüs der VisionGuard

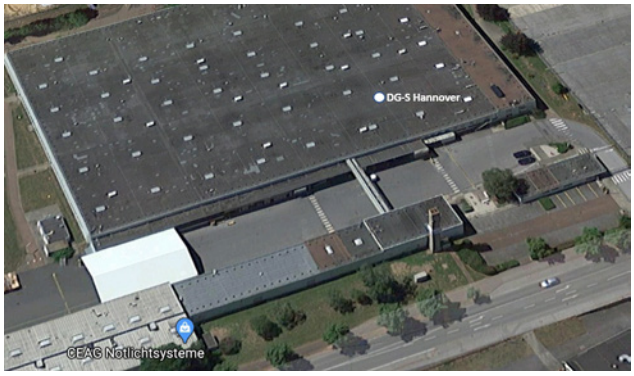
② Dashboard Widgets – Das Dashboard (Armaturenbrett) besteht aus 9 festgelegten Widgets

8.2.1 Systemgrafik und Systemstatus

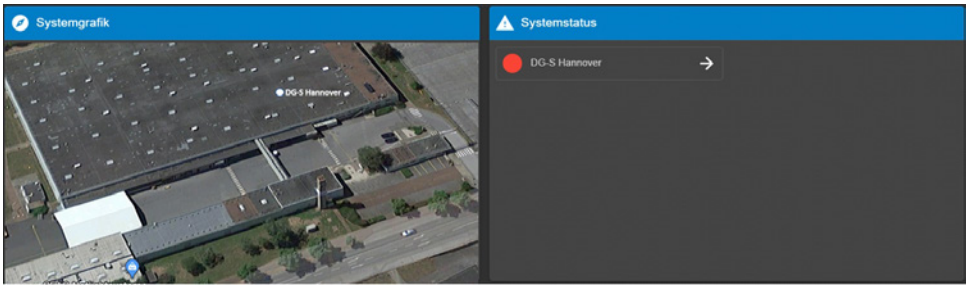
Das Widget Systemstatus zeigt alle angeschlossenen und angemeldeten DualGuard-S Systeme übersichtlich in einem Widget an. Je DualGuard wird der Anlagename mit einem farbigen Status angezeigt (Grün= OK, Rot = Störung). Über den Pfeil rechts vom Anlagenname navigiert man direkt in die Analgenübersicht.
Im Widget Systemgrafik kann man auf einfache Weise die Anlagen in einer Grafik darstellen, um z.B. den Standort anzuzeigen



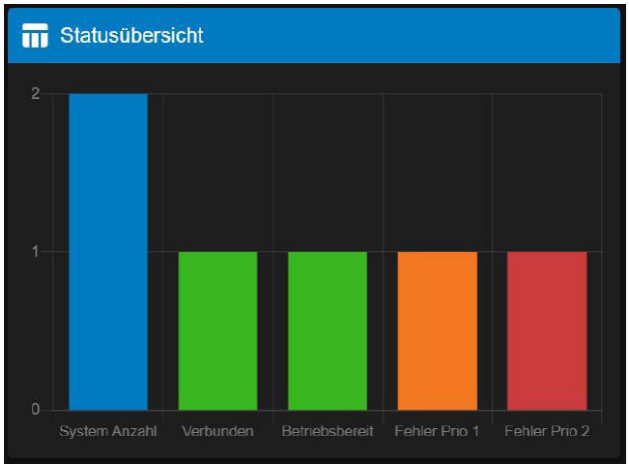
Beispiel einer einfachen Systemgrafik aus Google Maps: Man erzeugt ein Screenshot mit dem Anlagenstandort, und fügt mit Hilfe eines Grafiktools, z.B. Paint einen Text hinzu:



Dieses Bild kann nun als .jpg mit dem Namen „widget-image-jpg-01.jpg“ im Verzeichnis *C:\Programme\EATON\Visionguard\Proxy\html\img\widgets*
kopiert werden. Mit Strg+F5 wird die Seite neu geladen, und die Systemgrafik erscheint im Widget:



8.2.2 Statusübersicht



Das Widget Statusübersicht zeigt auf übersichtliche Weise mit einem Balkendiagramm den Status aller angeschlossenen Systeme an.

Blauer Balken = Anzahl aller angeschlossenen Systeme

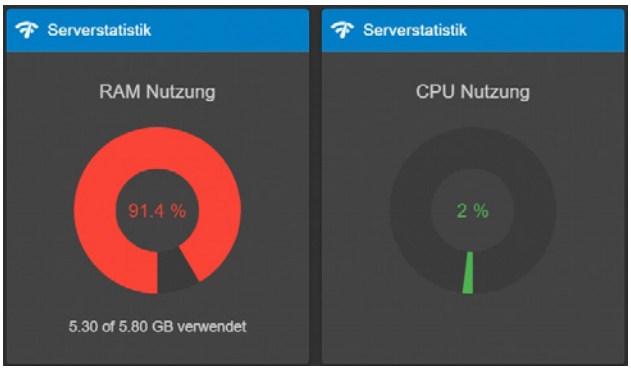
Grüner Balken 1 = Betriebsbereite Systeme

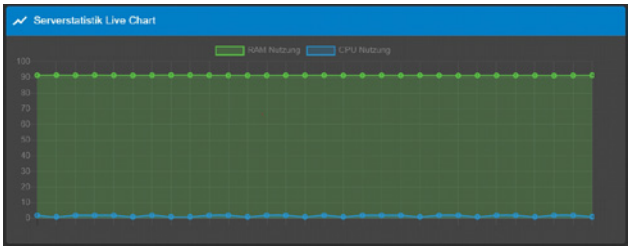
Grüner Balken 2 = Anzahl der Systeme ohne Kommunikationsstörung

Oranger Balken = Systeme mit Summenstörung Prio.1, d.h. inklusive Leuchtenfehler

Roter Balken = Systeme mit Summenstörung Prio.2 d.h. ohne Leuchtenfehler, z.B. bei Batteriestörung

8.2.3 Serverstatistik

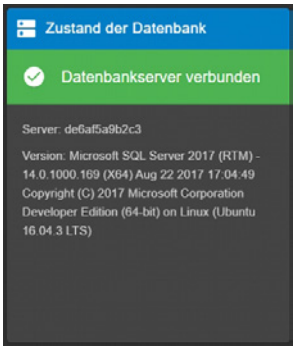


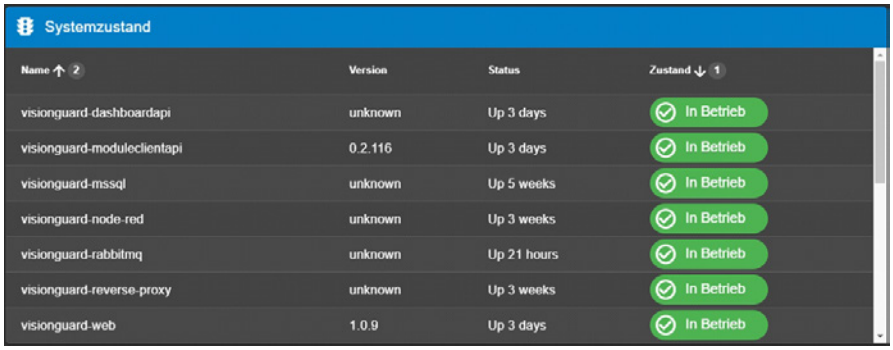


Die Widgets Serverstatistiken geben Auskunft über die aktuelle Prozessor- und Arbeitsspeicherauslastung, je in einem Tortendiagramm und gemeinsam über den Zeitverlauf in einem Liniendiagramm. Diese Informationen sind wichtig um eine Aussage über die aktuelle System-Performance für die VisionGuard zu bekommen. Dies kann eine gute Hilfe sein, um z.B. bei virtuellen Maschinen besser die Zuweisung von Prozessorkernen und Arbeitsspeicher bestimmen zu können. Befinden sich die Auslastungen längere Zeit im Bereich um 100%, wird dringend empfohlen die Performance zu erhöhen, z.B. Prozessorkerne zuzuweisen oder Arbeitsspeicher nachzurüsten.

8.2.4 Zustandsanzeigen der Datenbank und Systemdienste

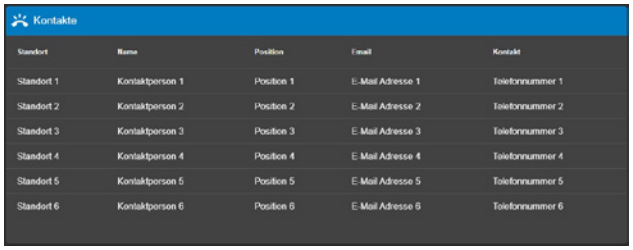
Die Widgets Zustand der Datenbank und Systemzustand geben Auskunft über die Funktionsfähigkeit der VisionGuard. Arbeitet der Datenbankserver korrekt, werden alle Daten zwischen den Systemen und der VisionGuard korrekt ausgetauscht. Im Widget Systemzustand kann die korrekte Funktion aller Dienste der VisionGuard überprüft werden, z.B. Mailclient. Die VisionGuard ist redundant aufgebaut, was bedeutet, wenn z.B. die Mailfunktion gestört ist, laufen alle anderen Dienste problemlos weiter. Im Widget wird auch angezeigt, wie lange schon ein Dienst ausgeführt wird, oder wie lange ein Dienst nicht mehr funktioniert hat. Ist ein Dienst ausgefallen, kann er problemlos im Menü Dienste neu gestartet werden (siehe Kapitel 11.1).





8.2.5 Kontakte

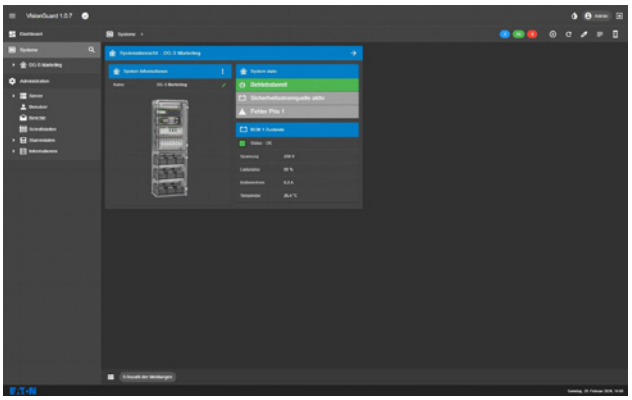
Im Widget Kontakte können Kontaktpersonen mit ihren Kontaktdaten angelegt werden, z.B. die bei speziellen Ereignissen zu informieren sind. Die Editierfunktion kann über das Schraubenschlüsselsymbol oben rechts aktiviert werden, um Kontaktdaten anzulegen oder zu ändern.



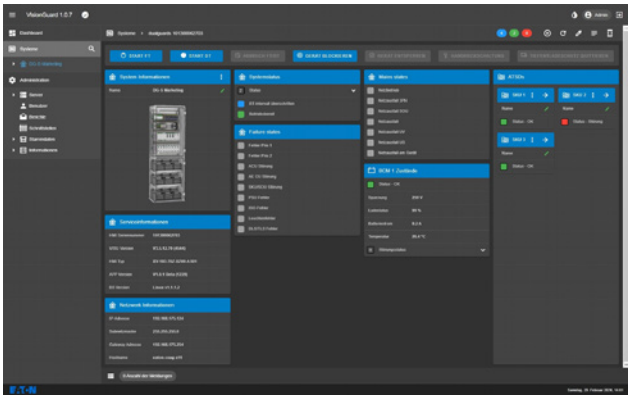
8.3 Systemübersicht

Im Menü „Systeme“ erscheint eine Systemübersicht mit Widgets aller instllierten DualGuard-S Systemen. Die Widgets zeigen Informationen wie den Gerätenamen, Batteriewerte und den Status der DualGuard-S wie sie auf dem ACU direkt am Gerät über LEDs angezeigt werden, wie Gerät ist betriebsbereit, die Sicherheitsstromquelle ist aktiv (Batteriebetrieb) und einen Summenfehler Prio.1 (Summenfehler inkl. Leuchtenfehler).

① Über den Pfeil gelangt man in die Detailansicht der DualGuard (siehe nächstes Kapitel 8.4)

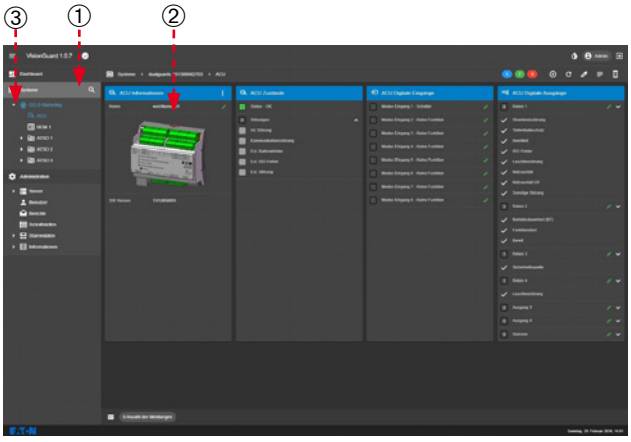


8.4 DualGuard-S Detailansicht



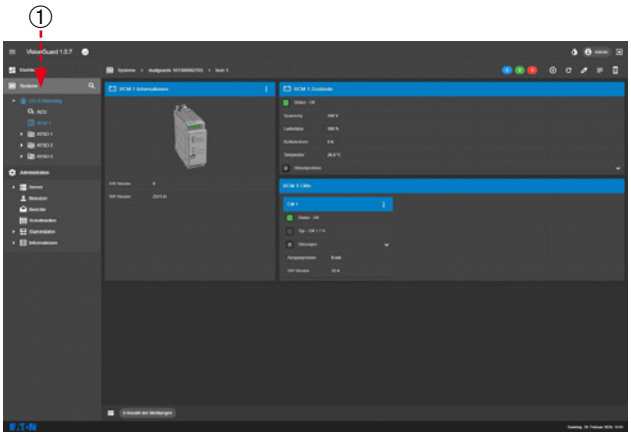
Unter dem Menü „Systeme“ werden alle Dualguard-S Systeme mit ihren Gerätenamen in Explorerstruktur aufgelistet ①. Mit Klick auf den Namen erscheint die Detailansicht der Dualguard-S. Hier bekommt man detailierte Statusinformationen zum System, Serviceinformationen wie z.B. Netzwerkeinstellungen, und eine Übersicht der installierten SKU.1 (Stromkreisumschaltungen) mit Statusanzeige. Darüberhinaus können über die blauen Steuerschaltflächen diverse Aktionen am Gerät ausgelöst werden, wie z.B. Funktionstest starten (Start FT) ②. ③ Über den Pfeil links neben dem Gerätenamen können die installierten Komponenten in Explorerstruktur angezeigt werden, was in den nächsten Unterkapiteln beschrieben wird.

8.4.1 ACU Detailansicht



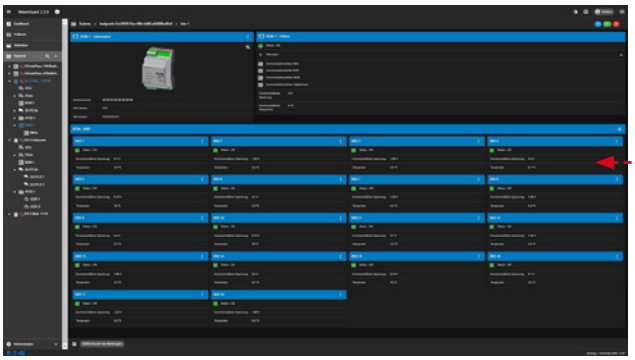
① In der Detailansicht der ACU wird der Status der ACU, die Konfigurationen der digitalen Eingänge und der Relais angezeigt. Eine Konfiguration der digitalen Eingänge und der Relais ist von der VisionGuard nicht möglich. Die Konfigurationen müssen über das HMI durchgeführt werden.

8.4.2 BCM Detailansicht



In der BCM Detailansicht wird die installierte Ladetechnik, bestehend aus BCM (Battery Control Module) und CM (Charger Module) Ladeteilen, angezeigt.
Im BCM Widgets werden die Batteriewerte wie Spannung in Volt, Ladestatus in %, Lade-/Entladestrom in Ampere, und die Batterieraumtemperatur in C° angezeigt. In den CM Widget wird der Gesamtstatus OK oder Störung angezeigt, und im Falle einer Störung, wird die Störungsanzeige aufgeklappt, die dann den genauen Fehler anzeigt.

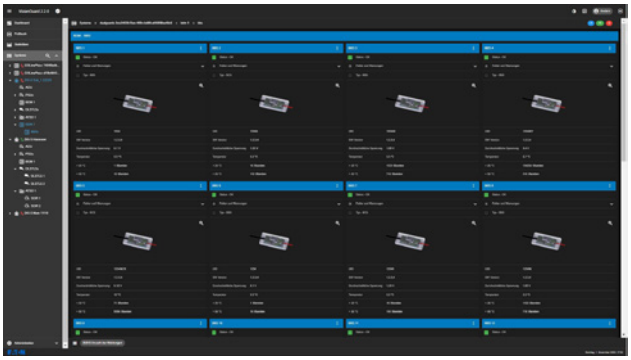
8.4.3 BDM Detailansicht



Wenn die optional erhältliche Batterieblocküberwachung installiert und am HMI angemeldet ist, erscheint im Systembaum automatisch der Menüpunkt „BDM“. ①

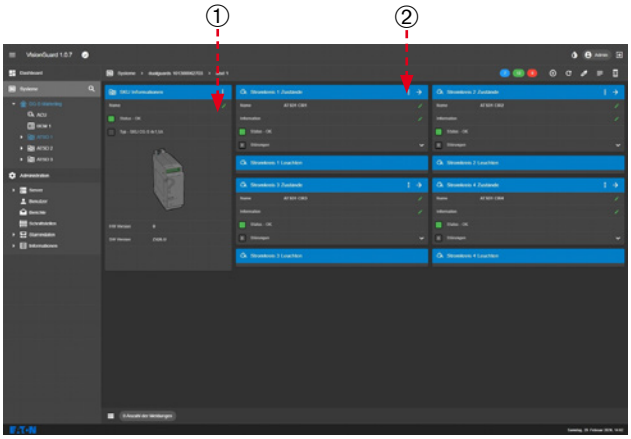
In der BDM-Ansicht wird das BDM (Battery Data Module) mit einem zusätzlichen Status-Widget angezeigt und alle angeschlossenen BBS (Battery Block Sensors) werden in einem Übersichts-Widget unterhalb des BDM mit der einzelnen Batterieblockspannung und der Batterieblocktemperatur angezeigt.

8.4.3.1 BBS Detailansicht



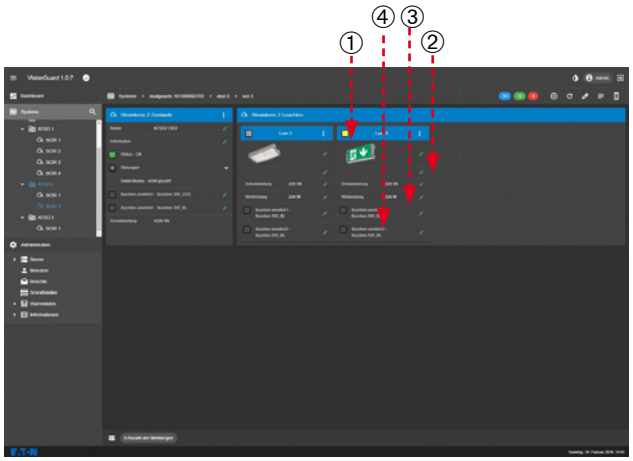
Mit einem Klick auf BBS im Systembaum ② oder auf den Pfeil ③ öffnet sich das BBS-Übersichts-Widget mit den detaillierten BBS-Statusinformationen.

8.4.4 ATSD Detailansicht (SKU)



Die ATSD-Detailansicht zeigt die SKU-Typen und die Namen, zusätzliche Informationen und den Gesamtstatus jedes Stromkreises an. Die Texte und die Zusatzinformationen können durch Klicken auf das grüne Stift-Symbol ① bearbeitet werden. In diesem Fall empfiehlt es sich, Zielortbezeichnungen einzugeben, in denen die Stromkreise mit den Lichtern geführt werden, z.B. Stromkreis 1 Hauptgebäude Halle 1. Im Falle eines Stromkreisfehlers erscheint hier auch die Fehleranzeige, die dann den genauen Stromkreisfehler anzeigt. Klicken Sie auf den Pfeil ②, um die Detailansicht des Stromkreises mit den Leuchten zu öffnen.

8.4.4 Leuchten Detailansicht



In der Leuchten Detailansicht wird der Status und Informationstexte des Stromkreises angezeigt. Auch hier wird im Falle einer Stromkreisstörung die Störungsanzeige aufgeklappt, die dann den genauen Stromkreisfehler anzeigt, z.B. Sicherungsfehler AC.

① In den Leuchtenwidgets wird im Kopf der Status der Leuchte angezeigt. Grau = ausgeschaltet, Gelb = eingeschaltet, Rot = gestört/defekt

② Unter dem Kopftext kann der Typ der Leuchte über den grünen Editierstift definiert werden. Möglich sind folgende Leuchtentypen. Sicherheitsleuchte, Rettungszeichenleuchte, Rettungszeichen Pfeil links, Rettungszeichen Pfeil rechts, Rettungszeichen Pfeil unten, Rettungszeichen Pfeil oben und Rotes Keuz (GuideLed DX). IA und Matrix werden z.Zt. nicht genutzt.

③ Im Infofeld „Scheinleistung“ und „Wirkleistung“ hat man die Möglichkeit für informative Zwecke die elektrischen Daten der Leuchten einzutragen, um z.B. die Gesamtlast an der Anlage leichter ermitteln zu können.

④ Unter Schalter 1 und Schalter 2 kann man die Zuordnung der Leuchte zu den Schaltern 1 + 2 auslesen

8.4.5 Alarmliste

Im linken Fußbereich der VisionGuard kann jederzeit eine Alarmliste über das Symbol ☰ ein- und ausgeklappt werden. Die Alarmliste zeigt mit Datum- und Zeitstempel alle Ereignisse an, die aufgetreten sind und wann sie wieder beendet wurden. Die Ereignisse werden nach Kategorie farblich angezeigt. Blau = Befehl, Grau = Information, Gelb = Warnung, Rot = Alarm.

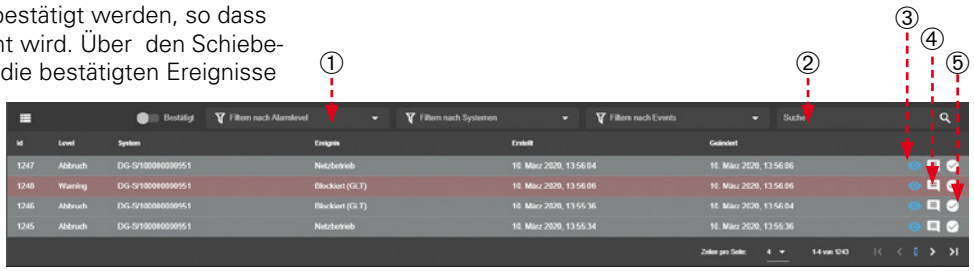
① Filter zum gezielten filtern nach Kategorien, Systemen oder Ereignissen

② Suchfunktion zum gezielten suchen von Ereignissen

③ Über das Augensymbol kann direkt in das Ereignis navigiert werden, wo es aufgetreten ist

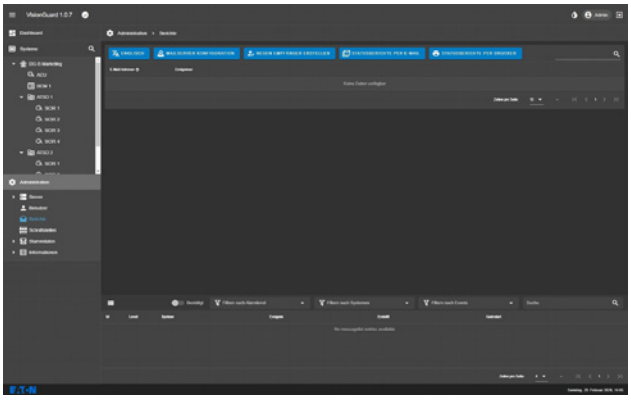
④ Über das Komentarsymbol kann man dem Ereignis ein Kommentar hinzufügen, z.B. wenn spezielle Aktionen zum Ereignis gestartet wurden

⑤ Hierüber kann das Ereignis bestätigt werden, so dass es aus der Alarmliste entfernt wird. Über den Schiebeschalter „bestätigt" können die bestätigten Ereignisse eingeblendet werden



9 E-Mail- und Druckfunktion

Im Menü „Berichte" kann man eine E-Mail und Druckfunktion aktivieren und einrichten.

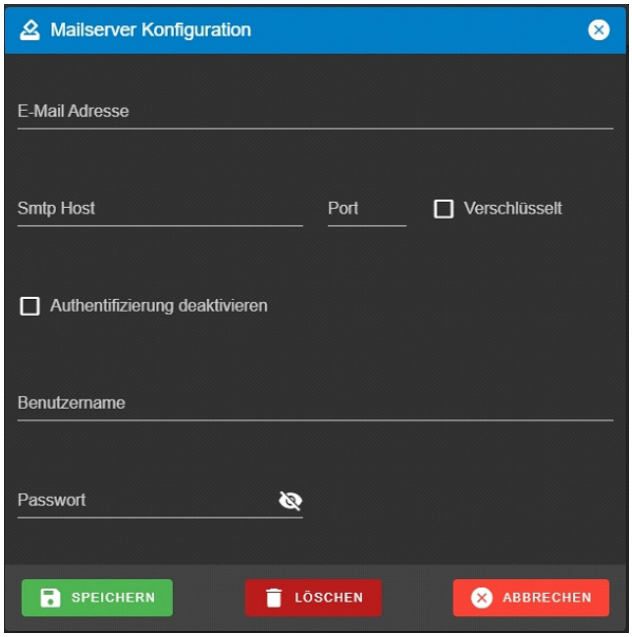


9.1 E-Mail Funktion

Die VisionGuard verfügt über einen E-Mail Client der an beliebige E-Mail Empfänger ereignisorientierte Alarm E-Mails, und einen automatischen Statusbericht mit aktuellen Fehlern versenden kann.

9.1.1 E-Mail Server einrichten

Um E-Mails von der VisionGuard versenden zu können muss zuerst ein Mailserver eingerichtet werden. Dieses erfolgt über die Schaltfläche „Mailserver Konfiguration“



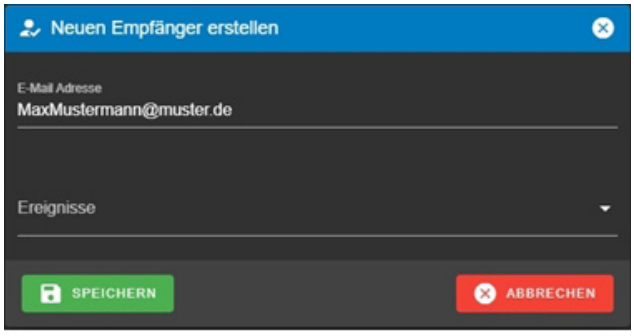
Es öffnet sich ein Konfigurationsfenster

Die richtigen Daten zum Mailserver erhalten Sie von der zuständigen IT-Abteilung.

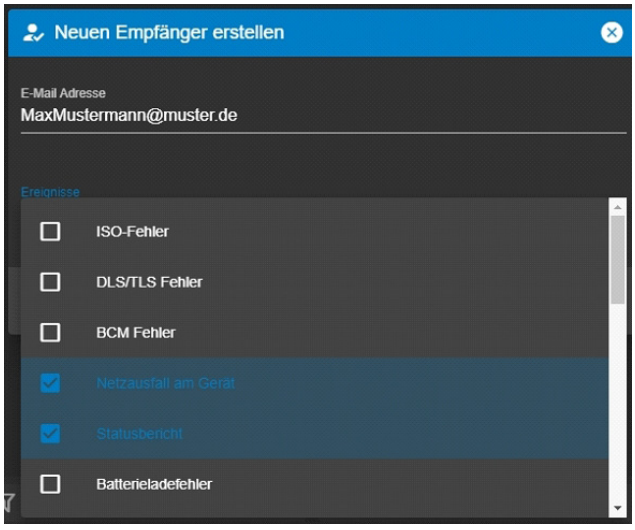
9.1.2 E-Mail Empfänger erstellen

Ein E-Mail Empfänger wird über die Schaltfläche „E-Mail Empfänger erstellen“ Schaltfläche angelegt.

Es öffnet sich folgendes Konfigurationsfenster



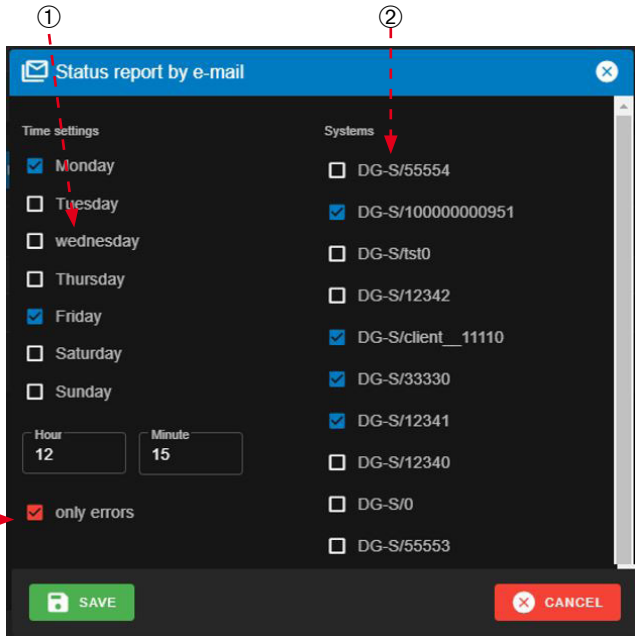
Oben muss eine gültige E-Mail-Adresse des Empfängers eingeben werden. Bei Klick auf Ereignisse öffnet sich eine Auswahl mit Ereignissen. Soll eine E-Mail bei auftreten eines gewünschten Ereignisses geschickt werden, muss dieses per Häckchen aktiviert werden. Bei Auftreten des Ereignisses wird ensprechend eine Alarm E-Mail verschickt.



9.1.3 automatische Status E-Mail

Wird im obigen Auswahlfeld „Automatischer Statusbericht“ ausgewählt, müssen noch die Parameter zum Versand der automatischen E-Mail eingestellt werden. Dieses erfolgt über die Schaltfläche „Statusberichte per E-Mail“

Es erscheint folgendes Konfigurationsfenster



① Hier können die Wochentage und die Uhrzeit eingestellt werden, wann die Statusmail versendet werden soll.

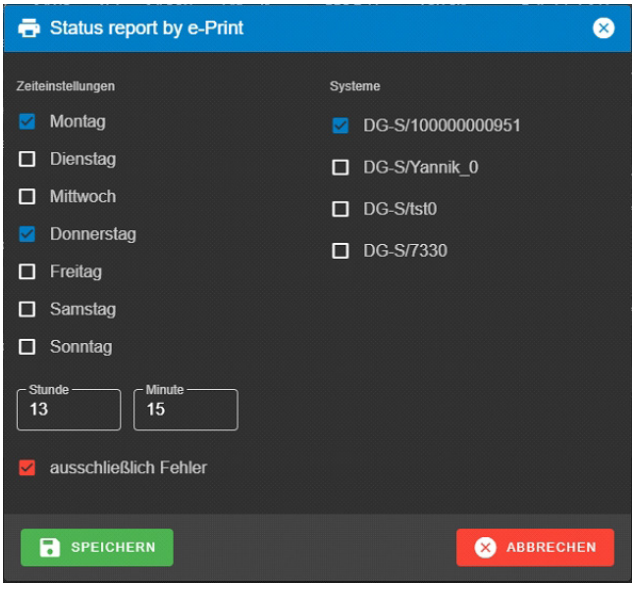
② Hier können alle DualGuard-S Systeme angewählt werden, deren Status in der Mail angezeigt werden sollen

③ Wird „ausschließlich Fehler“ aktiviert, werden in der E-Mail nur Fehler angezeigt. Wird das Feld deaktiviert werden alle Komponenten mit Status in der E-Mail aufgeführt. Die Mail kann je nach Umfang der DualGuard-S Systeme sehr umfangreich werden!

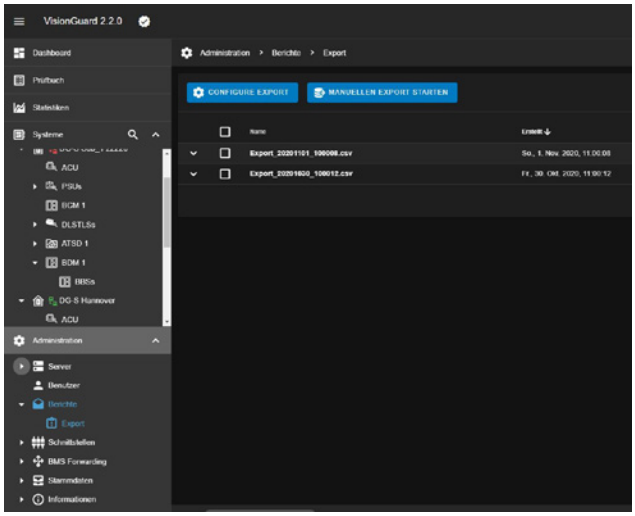
9.2 Druck Funktion

Die VisionGuard verfügt über eine automatische Druckfunktion die über die Schaltfläche „Statusberichte per Drucker“ aktiviert werden kann.

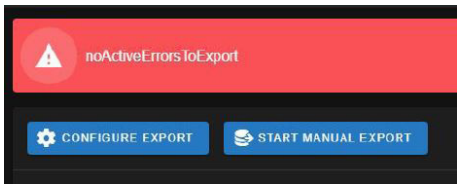
Im folgenden Konfgurationsfenster können wie bei den Statusberichten per Mail die gleichen Einstellungen vorgnommen werden.



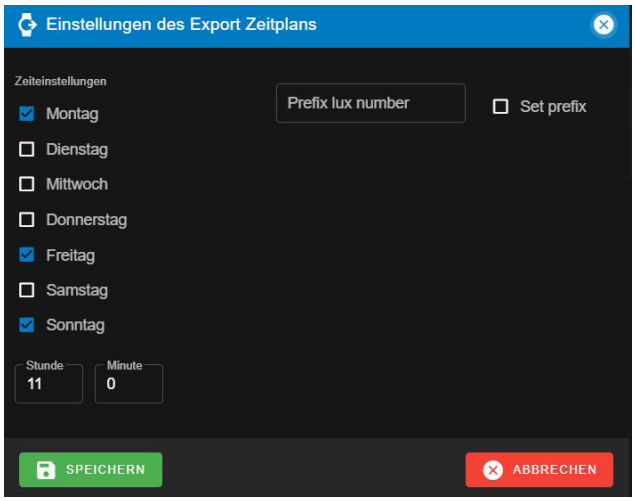
9.3 Exportfunktion



Die Funktion „Configure Export“ im Menü „Manuellen Export Starten“ ermöglicht es, alle aufgetretenen Störungen der DualGuard-S-Systeme in eine Excel-basierte .csv-Datei zu exportieren, z.B. zur Weiterverarbeitung durch externe Anwendungen.



Wenn das Menü Export gewählt wird, erscheint ein schwarzer Bildschirm mit zwei Schaltflächen „Export konfigurieren“ und „Manuellen Export starten“.
Mit der Funktion „Manueller Export starten“ wird direkt eine .csv-Datei mit allen Fehlern erzeugt, die in einen beliebigen Ordner, z.B. ein Netzlaufwerk, exportiert werden kann.
Falls keine Expertendatei erzeugt werden kann, z.B. wenn keine Fehler vorhanden sind, erscheint folgende Meldung.



Mit „Konfiguration Export“ kann ein automatischer Export der .csv-Datei konfiguriert werden. Das folgende Konfigurationsfenster erscheint

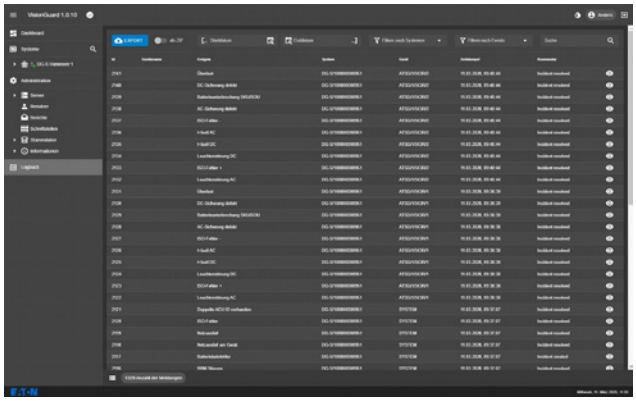
Über die Zeiteinstellungen können bestimmte Wochentage und der Zeitpunkt des automatischen Exports konkretisiert werden. Über Präfix setzen kann vor dem Export ein gewünschtes Präfix definiert werden.

Der Inhalt der .csv-Datei hat folgende Struktur mit Komma als Trennzeichen:
LogId,EventId,System,SystemName,Name,Level,Gerät,
Label,StateType,Erstellt,PersonalComment

Auszug aus der .csv:

```
LogId,EventId,System,SystemName,Name,Level,Device,Label,StateType,Created,PersonalComment
114570,57351,DG-S/101300062703,DG-S Marketing,awState1.moFt,Information,SYSTEM,$system.moFt,Closed,04/06/2020 11:37:26,
114569,57351,DG-S/101300062703,DG-S Marketing,awState1.moFt,Information,SYSTEM,$system.moFt,Opened,04/06/2020 11:33:46,
114568,57350,DG-S/101300062703,DG-S Marketing,uiDetailError.switchOfBatteryModeAccordingUnderVoltage,Information,ATSD/1/SCIR/1,$system.switchOfBatteryModeAccordingUnderVoltage,Opened,04/06/2020 11:33:04,
114567,57349,DG-S/101300062703,DG-S Marketing,awState4.errMainsExtAtsd,Information,SYSTEM,$system.errMainsExtAtsd,Opened,04/06/2020 11:33:03,
114566,57348,DG-S/101300062703,DG-S Marketing,awState4.btTestAllowed,Information,SYSTEM,$system.btTestAllowed,Opened,04/06/2020 11:33:03,
114565,57347,DG-S/101300062703,DG-S Marketing,awState4.errSum,Information,SYSTEM,$system.errSum,Opened,04/06/2020 11:33:03,
114564,57346,DG-S/101300062703,DG-S Marketing,awState4.errAe,Information,SYSTEM,$system.errAe,Opened,04/06/2020 11:33:03,
114563,57345,DG-S/101300062703,DG-S Marketing,awState4.errDistls,Information,SYSTEM,$system.errDistls,Opened,04/06/2020 11:33:03,
114562,57344,DG-S/101300062703,DG-S Marketing,awState4.errMainsSubstation,Information,SYSTEM,$system.errMainsSubstation,Opened,04/06/2020 11:33:03,
114561,57343,DG-S/101300062703,DG-S Marketing,awState4.errFan,Information,SYSTEM,$system.errFan,Opened,04/06/2020 11:33:03,
114560,57342,DG-S/101300062703,DG-S Marketing,awState3.errBcm,Information,SYSTEM,$system.errBcm,Opened,04/06/2020 11:33:03,
114559,57341,DG-S/101300062703,DG-S Marketing,awState3.errCm,Information,SYSTEM,$system.errCm,Opened,04/06/2020 11:33:03,
114558,57340,DG-S/101300062703,DG-S Marketing,awState3.errAcu,Information,SYSTEM,$system.errAcu,Opened,04/06/2020 11:33:03,
114557,57339,DG-S/101300062703,DG-S Marketing,awState3.errLum,Information,SYSTEM,$system.errLum,Opened,04/06/2020 11:33:03,
114556,57338,DG-S/101300062703,DG-S Marketing,awState3.errPsu,Information,SYSTEM,$system.errPsu,Opened,04/06/2020 11:33:03,
114555,57337,DG-S/101300062703,DG-S Marketing,awState3.errBbs,Information,SYSTEM,$system.errBbs,Opened,04/06/2020 11:33:03,
```

10 Prüfbuch



Die VisionGuard verfügt über eine Prüfbuchfunktion um alle Anforderungen gemäss der DIN EN 50172 / DIN VDE V 0108-100-1 zu erfüllen. Das Prüfbuch befindet sich in der Navigationsleiste an der untersten Position.
Da der Zeitraum des Prüfbuches mindestens die letzten 4 Jahre beträgt, können sehr viele Prüfbucheinträge vorhanden sein. Um diese übersichtlich darzustellen, oder gewünschte Einträge schnell ermitteln zu können, verfügt das Prüfbuch über viele Filterfunktionen und eine Suchfunktion.
In der Standeinstellung werden die neuesten Prüfbucheinträge oben in der Liste angezeigt.

① Über „Export" lässt sich das Prüfbuch im Excel lesbaren Format .csv runterladen. Um die Downloadzeit deutlich zu verkürzen, empfiehlt sich die Datei bei einem Prüfbuch mit vielen Einträgen „als ZIP" gepackt runter zu laden.

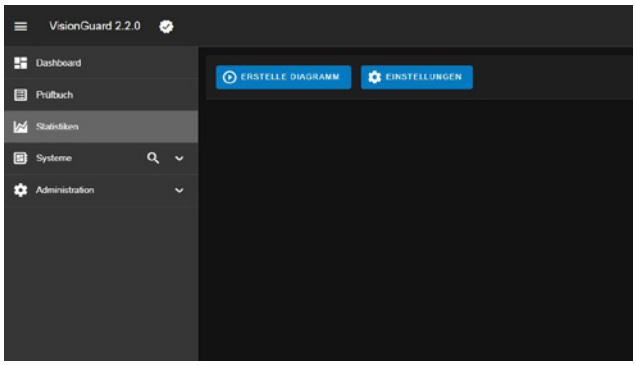
② Eingrenzen des Prüfbuches nach Datum und Uhrzeit (Zeitbereich)

③ Filter nach Systemnamen und Ereignissen (Mehrfachselektion ist möglich) sowie Suchfunktion nach bestimmten Ereignissen

④ Über das Augensymbol kann gezielt in das Bild navigiert werden, wo das Ereignis aufgetreten ist

11 Statistiken

Im Menü Statistiken können die vier Batterie-Analogwerte wie Batteriespannung, Batteriestrom, Batterieraumtemperatur und der Ladezustand der Batterie in einer konfigurierbaren Grafik über die Zeit angezeigt werden. Diese Funktion veranschaulicht z.B. den Verlauf eines Batteriedauertests sehr schön.
Dies kann helfen, die Qualität der Batterie zu bestimmen oder Temperaturausreißer der Batterieumgebung zu erkennen.



Wenn das Menü Statistik gewählt wird, erscheint ein schwarzer Bildschirm mit zwei Schaltflächen „Erstelle Diagramm" und „Einstellungen".

Die Grafiken können im Menü „Einstellungen" vorkonfiguriert werden:

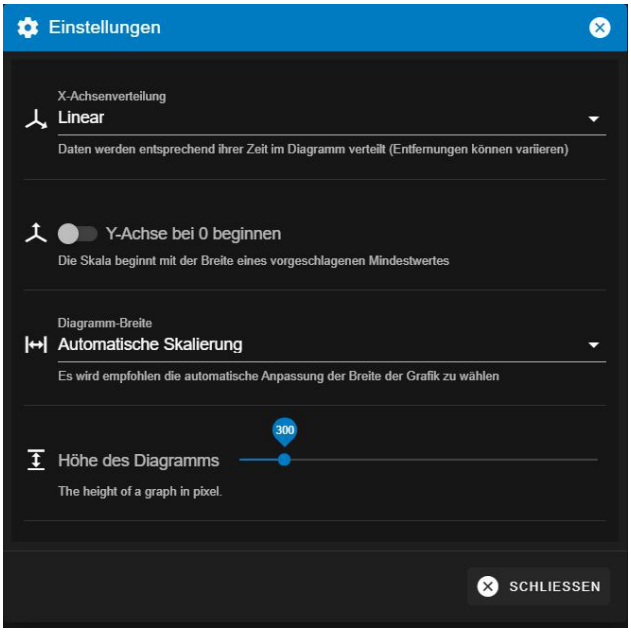
Folgende Konfigurationen können für die Grafiken vorgenommen werden

X-Achsen-Verteilung:
Linear = Daten werden entsprechend ihrer Zeit verteilt (Entfernungen können variieren- empfohlene Einstellungen)
Serie = Daten werden mit gleichem Abstand voneinander verteilt

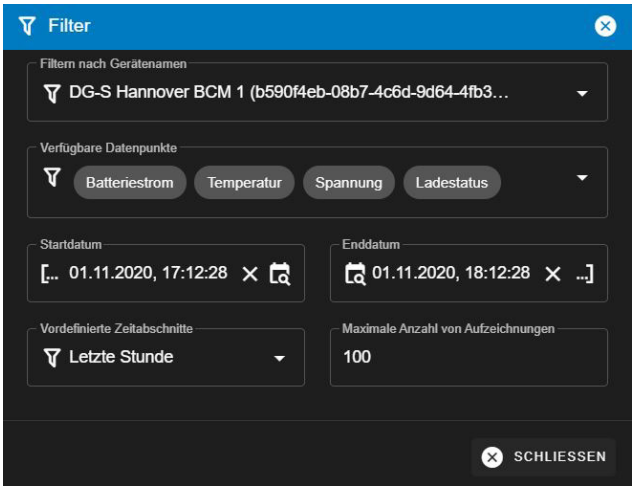
Die Y-Achse beginnt bei Null:
Deaktiviert = Daten werden auf der Y-Achse im Datenbereich angezeigt
Aktiviert = Daten werden auf der Y-Achse von 0

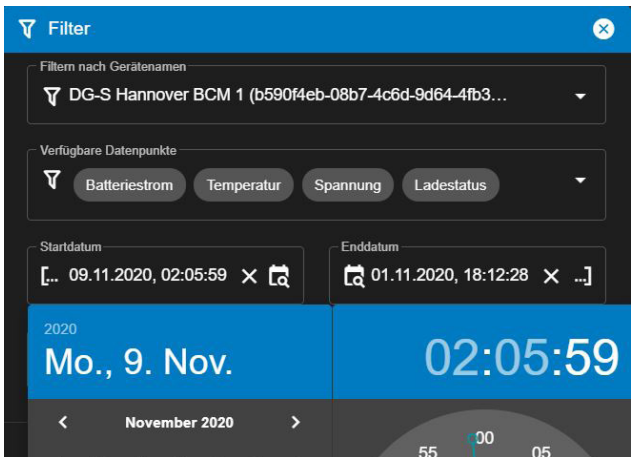
Breite des Diagramms:
Ermöglicht die Anpassung der Größe der Diagrammbreite.
Automatische Größenanpassung (empfohlene Einstellung)
Groß 100%
Mittel 50%
Kleine 25%

Höhe des Diagramms:
Ermöglicht die Anpassung der Größe der Diagrammhöhe von 200 bis 1000 Pixel.
Die Voreinstellung beträgt 300 Pixel.

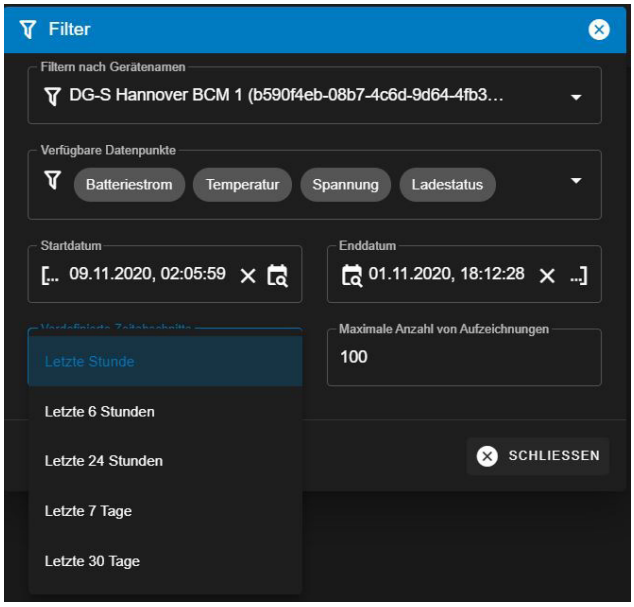


Nach der Einstellung der grafischen Konfigurationen können die Grafiken über „Erstelle Diagramm“ erzeugt werden. Es öffnet sich ein Fenster „Filter“:
Über „Filter nach Gerätenamen“ kann das gewünschte DualGuard-S System ausgewählt werden.
Über „Verfügbare Datenpunkte“ können die gewünschten Batterie-Analogwerte „Spannung“, „Batteriestrom“, „Temperatur“ und „Ladestatus“ ausgewählt werden.
Über „Startdatum“ und „Enddatum“ kann der gewünschte Zeitraum für die Grafiken eingestellt werden. Das Beispiel zeigt einen Zeitraum vom 30. Juli 2020, 13:10 Uhr bis zum 2. August 2020, 18:30 Uhr:





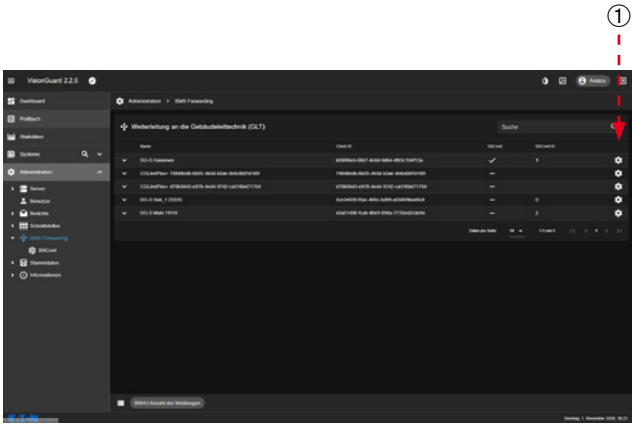
Alternativ kann eine feste Zeit viel schneller über „Vordefinierte Zeitspanne“eingestellt werden. Beispielsweise über die letzte Stunde, letzten sechs Stunden, letzten sieben Tage oder letzten 30 Tage.



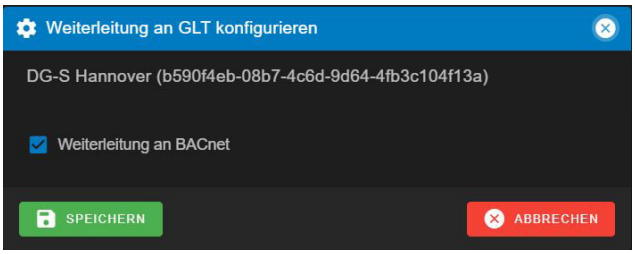
So ist es beispielsweise schnell möglich, die Batteriewerte direkt nach einem Batteriedauertest über „letzte Stunde“ einzusehen.
Um die Grafiken übersichtlich darzustellen, kann am Ende die maximale Anzahl der Aufnahmepunkte definiert werden. Voreingestellt ist die Anzahl von 100 Datensätzen.
Die Grafiken werden nach Eingabe aller Parameter automatisch generiert, z.B.
Grafik der letzten 30 Tage über den Batteriestrom und die Batterieraumtemperatur:

12 BACnet/IP Interface

Sobald die BACnet/IP-Lizenz erworben und aktiviert wurde, erscheint im Administrationsbereich der Menüpunkt „BMS Weiterleitung“ mit dem Untermenü „BACnet“. Im Menü „BACnet-Weiterletiung“ besteht die Möglichkeit, die BACnet/IP-Schnittstelle für jede einzelne DualGuard-S zu aktivieren.

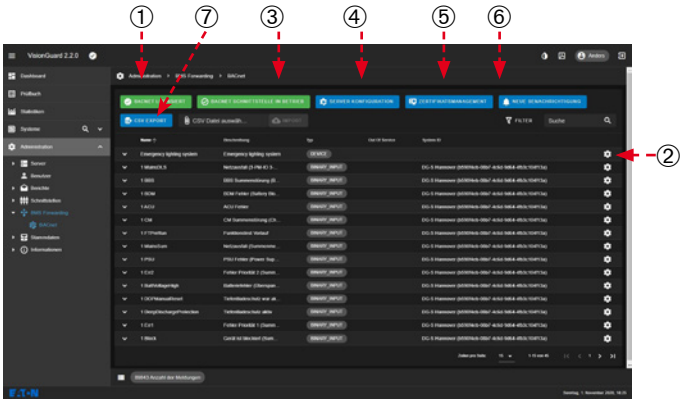


Dies kann über das Zahnradsymbol ① konfiguriert werden. Es öffnet sich das folgende Fenster. Mit einem Häkchen „Weiterleitung an BACnet“ kann die BACnet-Schnittstelle für diese DualGuard-S aktiviert werden. Mit „Speichern“ wird die Einstellung gespeichert.

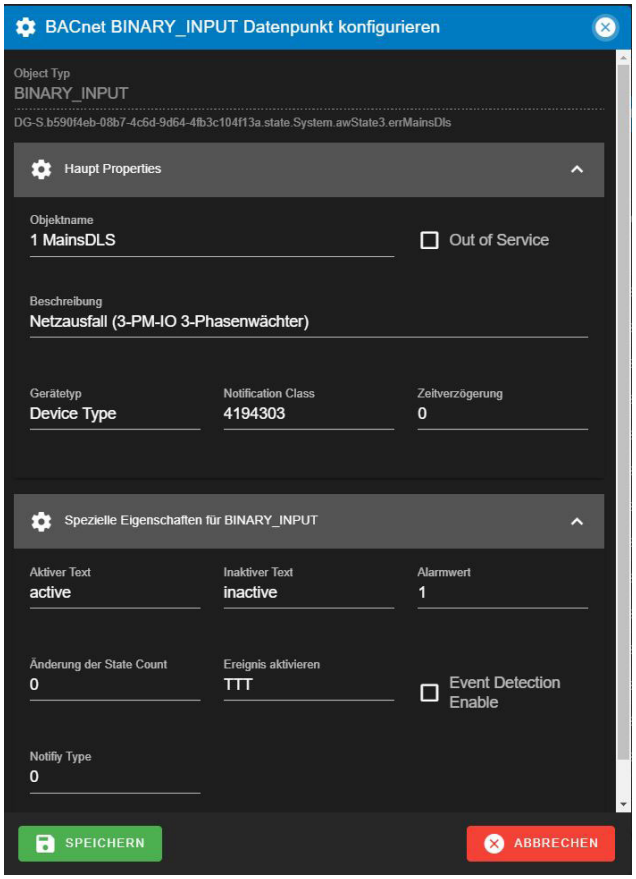


Im Untermenü „BACnet“ können Sie nun überprüfen, ob die BACnet-Lizenz und der BACnet-Server zur Anbindung einer BMS grün aktiviert ist. ①
Darüber hinaus können die BACnet-Datenpunkte (BACnet-Objekte) nun über das Zahnradsymbol für die BMS konfiguriert werden. ②

Abbildung- BACnet-Weiterleitung



Beispiel:
„Netzausfall 3-Phasenwächter“. Das folgende Konfigurationsfenster für das BACnet-Objekt wird geöffnet:

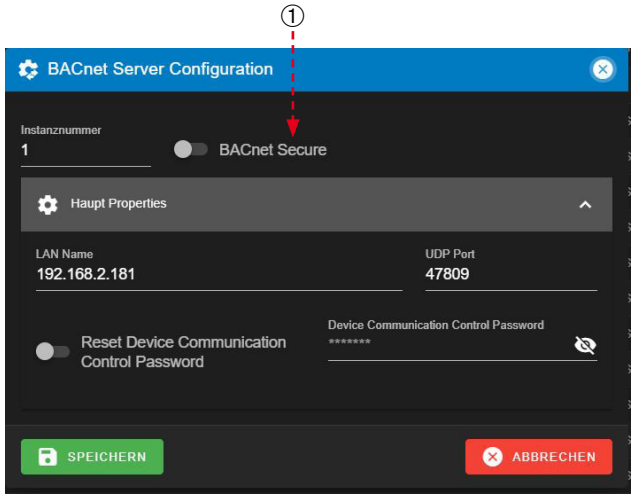


Der Objekttyp gibt den BACnet-Objekttyp an, z.B. BINARY_INPUT. Dies ist ein fester Wert.
Die Haupteigenschaften und die Spezifischen Eigenschaften für den BACnet-Objekttyp „BINARY_INPUT“ können nun entsprechend der BACnet-Spezifikation für die GLT-Verbindung konfiguriert werden, z.B. zeigt die Beschreibung die Bedeutung des BACnet-Objekts, in diesem Fall „Netzausfall 3-PM-IO 3 Phasenwächter“.
Dieser Informationstext zum BMS kann bei Bedarf geändert werden.

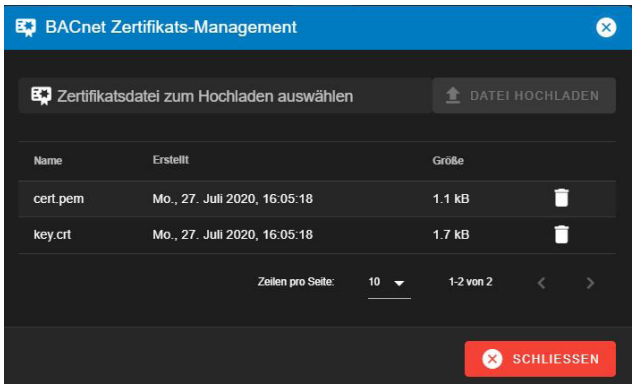
BACnet-Server-Konfiguration

Siehe Abbildung „BACnet-Weiterleitung“ (3).

In diesem Konfigurationsmenü können die Einstellungen für den BACnet-Server vorgenommen werden:

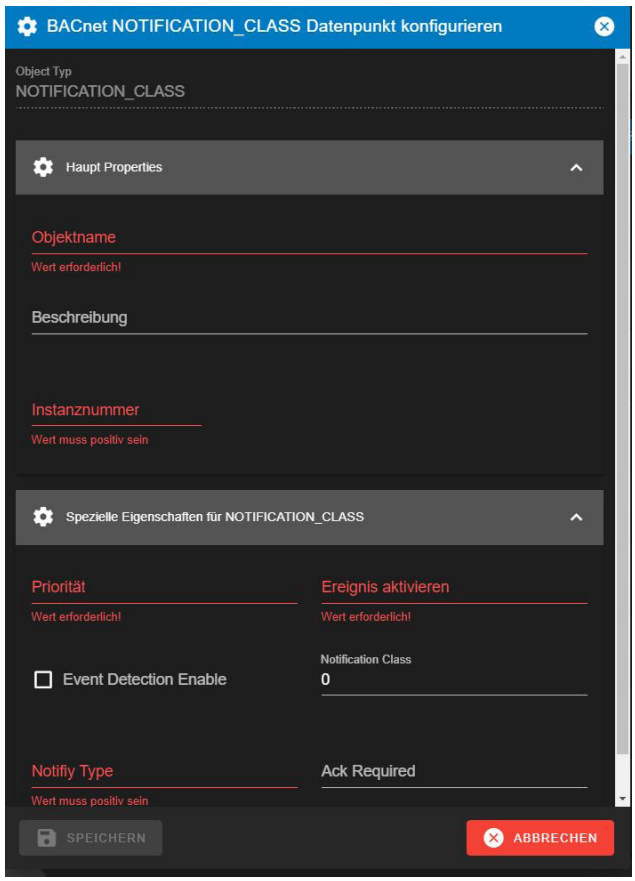


Die „Instanznummer“ ist wichtig für die eindeutige Identifizierung des Dualguad-S-Systems auf der BMS-Seite.
Falls BACnet Secure benötigt wird, muss es hier aktiviert werden. Für weitere Einstellungen ist es möglich, unter „Zertifikats-Management“ BACnet Secure Einstellungen zu konfigurieren. Siehe Abbildung BACnet-Weiterleitung.
Im folgenden Dialogfenster kann nun ein gültiges BACnet-Zertifikat geladen werden.
Nicht mehr benötigte Zertifikate können über das Papierkorb-Symbol gelöscht werden.



Falls für die BMS-Benachrichtigungsklassifizierung erforderlich, können diese im Menü „NEUE BENACHRICHTIGUNG“ konfiguriert werden.
Siehe Abbildung BACnet-Weiterleitung (3). In diesem Konfigurationsmenü können die Einstellungen für den BACnet-Server vorgenommen werden:

Hier können die entsprechenden Objektnamen ausgewählt und unter „Spezielle Eigenschaften für NOTIFICATION_CLASS“ die Priorität und „Ereignis aktivieren“ eingestellt werden. Für die Benachrichtigungsklasse 3 sind Zahlen zwischen 0 und 255 erlaubt. (Vorgabe vom BMS-Integrator)
Für das „Ereignis aktivieren“ sind nur 3 Buchstaben erlaubt, mit T oder F, die für T=„True“ oder F=„False“ stehen.



CSV-EXPORT

Siehe Abbildung BACnet-Weiterleitung.
Mit dem CSV-Export ist es auch möglich, die Bacnet-Konfiguration über eine csv.-Tabelle z.B. über Excel vorzunehmen. Nach Änderung aller Daten (wichtig: die Eingaben müssen korrekt sein!) kann die csv.-Datei über die CSV-Datei-Eingabefunktion „IMPORT“ geladen werden.
Siehe Abbildung „BACnet-Weiterleitung“.

13 Administrationsbereich

Im Administrationsbereich der CGVision können Dienste neu gestartet, Benutzer und Lizenzen verwaltet, sowie Informationen zu Open Source und Änderungen in den verschiedenen VisionGuard Versionen nachgelesen werden. Eine Änderung in den Stammdaten darf nicht durchgeführt werden!

Dienste (siehe Kapitel 11.1 Dienste)

Benutzer (siehe Kapitel 6 – Neue Benutzer mit Benutzerrollen anlegen)

Berichte (siehe Kapitel 9 – E-Mail- und Druckfunktion)

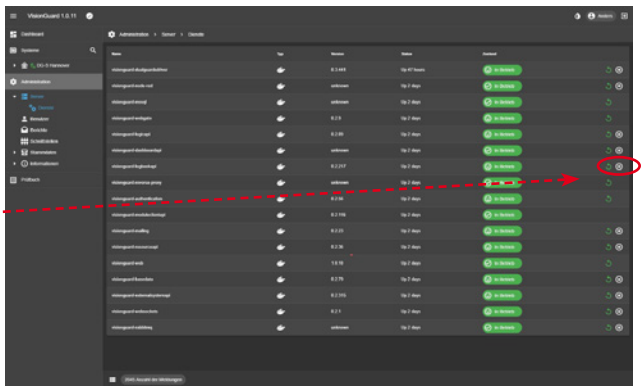
Schnittstellen (siehe Kapitel 7 – Anlegen von Dualguard-S Systemen an die VisionGuard

Stammdaten – hier keine Änderungen vornehmen!

Informationen – enthält Änderungsinformationen zu den unterschiedlichen VisionGuard Versionen, Lizenzen (siehe Kapitel 4 Lizensierung) und Open Source mit Informationen zu genutzer Open Source Software

13.1 Dienste

Im Menü Dienste wird der Funktionszustand (Betrieb) aller in der VisionGuard genutzten Dienste dargestellt. Alle Dienste laufen unabhängig, so dass die VisionGuard sehr redundant aufgebaut ist. Fällt ein Dienst aus, wird dieses rot angezeigt. Dieser kann über das Symbol neu gestartet werden.



Eatons Ziel ist es, zuverlässige, effiziente und sichere Stromversorgung dann zu bieten, wenn sie am meisten benötigt wird. Die Experten von Eaton verfügen über ein umfassendes Fachwissen im Bereich Energiemanagement in verschiedensten Branchen und sorgen so für kundenspezifische, integrierte Lösungen, um anspruchsvollste Anforderungen der Kunden zu erfüllen.

Wir sind darauf fokussiert, stets die richtige Lösung für jede Anwendung zu finden. Dabei erwarten Entscheidungsträger mehr als lediglich innovative Produkte. Unternehmen wenden sich an Eaton, weil individuelle Unterstützung und der Erfolg unserer Kunden stets an erster Stelle stehen. Für mehr Informationen besuchen Sie **www.eaton.eu**.

Ihre Ansprechpartner finden Sie unter **www.ceag.de**.

Eaton Industries Manufacturing GmbH
Electrical Sector EMEA
Route de la Longeraie 7
1110 Morges, Switzerland
Eaton.eu

CEAG Notlichtsysteme GmbH
Senator-Schwartz-Ring 26
59494 Soest, Germany
Tel.: +49 (0) 2921 69-870
Fax: +49 (0) 2921 69-617
E-Mail: info-n@ceag.de
Web: www.ceag.de

Printed in Germany
Bestell-Nr. 40071860370 (A)
Publikations-Nr. MN451069DE
November 2020

Powering Business Worldwide