

Bedienungsanleitung Eaton VisionGuard

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



Inhalt

1 Vorwort und Systemvoraussetzungen	4	8 Anlegen von ZB-S Systemen in VisionGuard	34
1.1 Vorwort	4	8.1 CG-S Gateway Konfiguration	34
1.2 Wichtige Hinweise zur Cyber Sicherheit der VisionGuard in Ethernet Netzwerken	4	8.2 Anlegen und autorisieren von ZB-S Systemen in VisionGuard	35
1.3. Systemvoraussetzungen – Hardware/Software Anforderungen	9	8.2.1 Erstellen neuer Gruppen und anlegen und autorisieren von ZB-S Systemen in VisionGuard	36
1.4 Wichtige Informationen vor der Installation	10		
1.4.1 Genutzte Ports und Protokolle	10	9 Grafischer Aufbau und Struktur der VisionGuard	38
1.4.2 Genutzte Dienste und der Standard-Installationspfad	10	9.1 Anmeldefenster	38
1.4.3 Vorbereitungen für eine VisionGuard Softwareinstallation	10	9.2 Dashboard	38
1.5. VisionGuard Lizenzen	10	9.2.1 Systemgrafik und Systemstatus	39
1.5.1 Lizenzmodelle	10	9.2.2 Serverstatistik	40
1.5.2 Lizenzierungsablauf	10	9.2.3 Zustandsanzeigen der Datenbank und Systemdienste	40
		9.2.4 Kontakte	40
2 Installationsanleitung	11	9.3 Systemübersicht	41
2.1 Installation der VisionGuard Software	11	9.4 Alarmliste	41
2.2 Installation der CG-S Gateway Software	14	10 DualGuard-S Visualisierung	41
2.3 Installation des CG-S Interface Treiberpakets ...	17	10.1 DualGuard-S Detailansicht	41
2.4 Update einer bestehenden VisionGuard Installation	19	10.2 ACU Detailansicht	42
2.4.1 Updatebeschreibung der VisionGuard Software	19	10.3 BCM Detailansicht	42
2.4.2 Durchführen eines Updates der VisionGuard Software	19	10.4 BDM Detailansicht	42
2.5 Deinstallation von VisionGuard Softwarekomponenten	20	10.4.1 BBS Detailansicht	42
3 Erster Start der VisionGuard	20	10.5 ATSD Detailansicht (SKU)	43
3.1 Lokaler Zugriff (VisionGuard Server und Client auf ein PC)	20	10.6 Leuchten Detailansicht	43
3.2 Zugriff auf entferntem VisionGuard Server (VisionGuard Server und Client auf unterschiedlichen PC)	21	10.7 Konfiguration einer DualGuard-S	44
4 Lizenzierung	22	10.7.1 Systemkonfiguration	44
4.1 Aktivierung einer Lizenzierung	22	10.7.2 ACU Konfiguration	45
5 Installation von Sicherheitszertifikaten	24	10.7.3 SKU (ATSD) Konfiguration	45
5.1 Installation des Sicherheitszertifikates bei lokalem Zugriff	24	10.7.4 I/O, 3-PM-IO, TLS Konfiguration	45
5.2 Installation des Sicherheitszertifikates bei Fernzugriff	27	11 ZB-S Visualisierung	46
6 Neue Benutzer mit Benutzerrollen anlegen	28	11.1 ZB-S Detailansicht	46
6.1 Information zur Benutzerkontensteuerung (UAC = User Account Control)	28	11.2 CU Detailansicht	46
7 Anlegen von Dualguard-S Systemen an die VisionGuard	30	11.3 BCM Detailansicht	47
7.1 HMI zur Anbindung an VisionGuard konfigurieren	30	11.4 SKU Detailansicht	47
7.2 Anlegen und autorisieren einer DualGuard-S in der VisionGuard	32	11.5 Leuchten Detailansicht	47
		12 E-Mail-, Druck- und Exportfunktion	48
		12.1 E-Mail Funktion	48
		12.1.1 E-Mail Server einrichten	49
		12.1.2 E-Mail Empfänger erstellen	49
		12.1.3 Automatische Status E-Mail	50
		12.2 Druckfunktion	50
		12.3 Exportfunktion	51
		13 Prüfbuch	52
		14 History menu	52
		15 Speichern und Wiederherstellen	54
		15 Erstellung automatischer Backups	55
		15.1 Erstellung automatischer Backups	55
		15.2 Erstellung manueller Backups	55
		15.3 Manuelle Wiederherstellung	55
		16 BACnet/IP Interface für DualGuard-S	56
		17 Administrationsbereich	59
		17.1 Dienste	59

1 Vorwort und Systemvoraussetzungen

1.1 Vorwort

VisionGuard ist eine moderne webbasierte Überwachungs-, Steuerungs- und Konfigurationssoftware für das neue DualGuard-S und Überwachungs- und Steuerungssoftware für ZB-S Zentralbatteriesysteme. In den nächsten Versionen wird sie um die Konfiguration der CG-S busbasierten Notlichtsysteme AT-S+ und LP-STAR sowie des neuesten Einzelbatteriesystems CGLine+ erweitert.

Features:

- Webbasierte Client-/Server Architektur für unabhängige Bedienung von mehreren Usern
- Für bis zu 500 Notlichtsysteme (DualGuard-S oder ZB-S)
- Benutzerkontenmenü (UAC) mit 4 Benutzerrollen für unterschiedliche Zugriffsberechtigungen (Supervisor, Administrator, Power User and User)
- Entwickelt und geprüft auf Cyber Sicherheit (EATON zertifiziert)
- Softwarelizenzierung ohne Hardwaredongle (Software Download)
- 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
- Grafische Darstellungen von Batterieanalogwerten im Statistikmenü bieten eine übersichtliche Darstellung in Form von Diagrammen über die Zeit
- Optionale BACnet/IP-Schnittstelle: Diese ermöglicht die einfache Anbindung an eine externe Gebäudeleittechnik (GLT) über das BACnet-Protokoll (nur für DG-S, BACnet/IP-Interface für ZB-S in Vorbereitung)
- Auftretende Störungen können über eine integrierte Exportfunktion bequem an externe Anwendungen weitergeleitet werden
- Batterieblocküberwachung: grafische Anzeige der optional erhältlichen Batterieblocküberwachung mit Blockspannung und-temperatur (nur DG-S)

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, Switches 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:

Überlegungen zur Cybersicherheit für elektrische Verteilungssysteme: (WP152002EN):

http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

Cybersecurity Best Practices Checklist Reminder (WP910003EN):

<https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf>

Referenzen

[R1] Überlegungen zur Cybersicherheit in der Informations- und Kommunikationstechnik

(WP152002EN): http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

[R2] Cybersecurity best practices checklist reminder

(WP910003EN): <https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf>

[R3] National Institute of Technology (NIST) interagency "Guidelines on firewalls and firewall policy, NIST special publication 800-41," Oktober 2009:

<https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final>

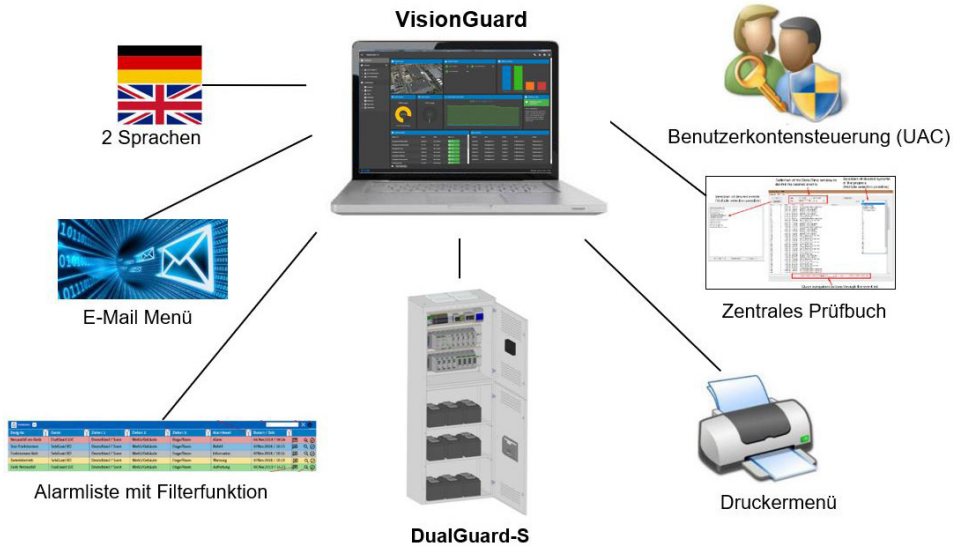
[R4] NIST SP 800-88, Guidelines for media sanitization, September 2006:

http://www.nist.gov/publication/get_pdf.cfm?pub_id=50819

[R5] A summary of cybersecurity best practices – Homeland Security

<https://www.hsdl.org/?view&did=806518> (.pdf als download)

1.2 Wichtige Hinweise zur Cyber Sicherheit der VisionGuard in Ethernet Netzwerken

Kategorie	Beschreibung
Vorgesehener Zweck und Einsatz der VisionGuard	Bei VisionGuard handelt es sich um eine Visualisierungssoftware zur Überwachung, Steuerung und Konfiguration von DualGuard-S und Überwachung und Steuerung von ZB-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 Netzkabeln sollte zum Schutz vor Abhör- oder Sabotageversuchen eingeschränkt werden. Es ist eine bewährte Vorgehensweise, Metallkanäle für die Netzkabelführung zwischen den Geräteschränken zu verwenden. • VisionGuard unterstützt die folgenden physischen Zugriffspoints: RJ45 Der Zugang zu RJ45diesem (LAN) Ports sollte möglichst ist einzugeschränkt 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.

1.2 Wichtige Hinweise zur Cyber Sicherheit der VisionGuard in Ethernet Netzwerken

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.

1.2 Wichtige Hinweise zur Cyber Sicherheit der VisionGuard in Ethernet Netzwerken

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.

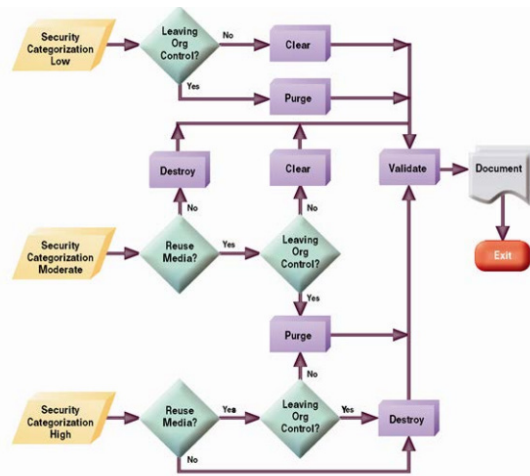


Figure 4-1: Sanitization and Disposition Decision Flow

* 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 Netzwerkkarten 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 VisionGuard 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 , dringend 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 Wichtige Informationen vor der Installation

1.4 Wichtige Informationen vor der Installation

1.4.1 Genutzte Ports und Protokolle

Die folgenden Ports und Protokolle werden von VisionGuard verwendet und müssen für eine korrekte Funktion im Netzwerk erlaubt sein.

Wenden Sie sich ggf. an Ihre IT-Abteilung, um die richtigen Netzwerkeinstellungen zu erhalten.

Protokoll	Port	Verschlüsselt	Verfügbar von Außen	Dienst	Beschreibung
AMQP	5672	-	-	RabbitMQ	Internal Service Communication
AMQP	5671	x	-	RabbitMQ	Internal Service Communication
MQTT	1883	-	x	RabbitMQ	HMI Communication
MQTT	8883	x	x	RabbitMQ	HMI Communication
HTTPS	15671	x	-	RabbitMQ	RabbitMQ Web Interface
TCP	1433	-	-	MSSQL	Service Database Communication
HTTP	80	-	x	VisionGuard	Client Access
HTTPS	443	-	x	VisionGuard	Client Access
HTTP/S	6000-6050	-/x	-	VisionGuard	Service Communication
TCP / UDP	1628/1629	-	-	-	Kommunikationsports für CG-S/IP-Router (ZB-S/AT-S+/LP-STAR)
BACnet/IP	47808	-	-	-	BACnet/IP Kommunikation

1.4.2 Genutzte Dienste und der Standard-Installationspfad

Name	Installationspfad	Beschreibung
.NET Core Runtime	C:\Program Files\dotnet	Runtime for Services
Erlang	C:\Program Files\erl10.5	RabbitMQ Runtime
RabbitMQ	C:\Program Files\RabbitMQ Server	Messagebus
RabbitMQ Logs	C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\RabbitMQ	Logs of Messagebus
MSSQL 2019	C:\Program Files\Microsoft SQL Server	Database Server
VisionGuard	C:\Program Files\EATON\VisionGuard	Actual Software
VisionGuard Logs	C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\EATON\VisionGuard	Logs of the individual services

1.4.3 Vorbereitungen für eine VisionGuard Softwareinstallation

- Es sollte beachtet werden, dass Virens Scanner die Installation beeinflussen können.
 - o Verlangsamung der Installation
 - o Blockieren von Teilen der Installation
 - o Erlaubnisabfragen, die vom Benutzer bestätigt werden müssen

- Es kann notwendig sein, einen Virens Scanner für die Dauer der Installation aus einem der oben genannten Gründe zu deaktivieren.
- Ein Ausschalten/Pausieren des PCs während der Installation ist zu unterlassen. Dazu gehört auch:
 - o Energiesparmodus
 - o Neustart
- Der Benutzer sollte auch während der Installation am PC bleiben, da Systemabfragen auftreten, die vom Benutzer bestätigt werden müssen. Bleiben diese Abfragen über einen längeren Zeitraum unbestätigt, wird die Installation abgebrochen.
- Während der Installation von VisionGuard sollten andere Installationen vermieden werden.
- Grundsätzlich sollten alle Formen des Energiesparmodus und das automatische Herunterfahren des Rechners deaktiviert werden, da das VisionGuard-System permanent verfügbar sein muss.

1.5. VisionGuard Lizenzen

1.5.1 Lizenzmodelle

Die VisionGuard ist vor unbefugtem Betrieb geschützt. Für eine Freischaltung zum Betrieb der VisionGuard ist eine Lizenz notwendig. Die Lizenz ist abhängig von den angeschlossenen DualGuard-S oder ZB-S Systemen. Ein „Gerät“ kann ein Batteriesystem oder eine Unterstation mit einer Steuereinheit (HMI oder CU-S) sein. 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 (nur für DG-S, ZB-S in Vorbereitung)

Alle VisionGuard-Versionen sind als Software-Key (Zertifikat mit Key) ohne Hardware, oder optional auf einem USB-Stick erhältlich. (VisionGuard software, CG-S Gateway, CG-S Treiberpaket, Dokumentation und Zugriffskey für die Aktivierung).

1.5.2 Lizenzierungsablauf

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

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

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

Der Lizenzierungsablauf ist detailliert im Kapitel 4 Lizenzierung beschrieben

2 Installationsanleitung

Hinweise zur Installation: Wenn nur DualGuard-S (DG-S)-Systeme an der VisionGuard angeschlossen werden sollen, ist es ausreichend, nur die VisionGuard-Software zu installieren (siehe 2.1). Sollen auch ZB-S Notlichtsysteme an der VisionGuard angeschlossen werden, muss zusätzlich eine CG-S Gateway Software und ein CG-S Interface Treiberpaket installiert werden. (siehe 2.2 und 2.3) Die neueste Version von VisionGuard, CG-S Gateway und dem CG-S Treiberpaket stehen auf der VisionGuard Produktseite unter www.eaton.com zum Download bereit.

2.1 Installation der VisionGuard Software

Die Installation wird gestartet über das ausführen des Visionguard Installers:

Visionguard_Installer_V3.1.0.exe

Die Installation muss „als Administrator“ gestartet werden. Ein rechter Mausklick auf diese .exe-Datei öffnet ein Menü. Klicken Sie auf „als Administrator ausführen“, um den VisionGuard-Setup-Assistenten zu starten. Es kann zunächst eine Meldung der Windows Benutzerkontensteuerung erscheinen. In diesem Fall bestätigen Sie bitte mit „JA“.

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.

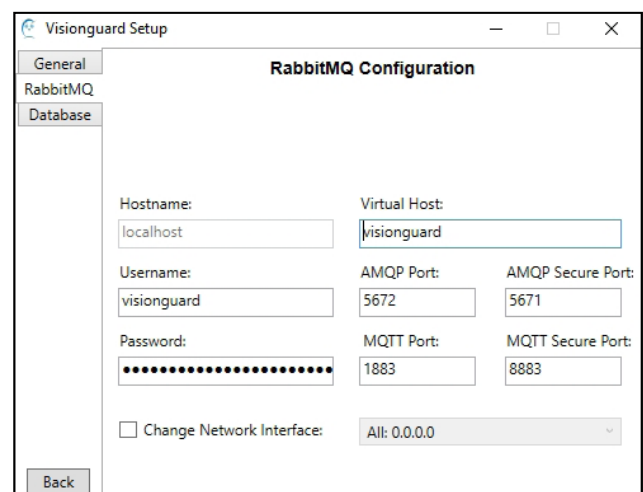
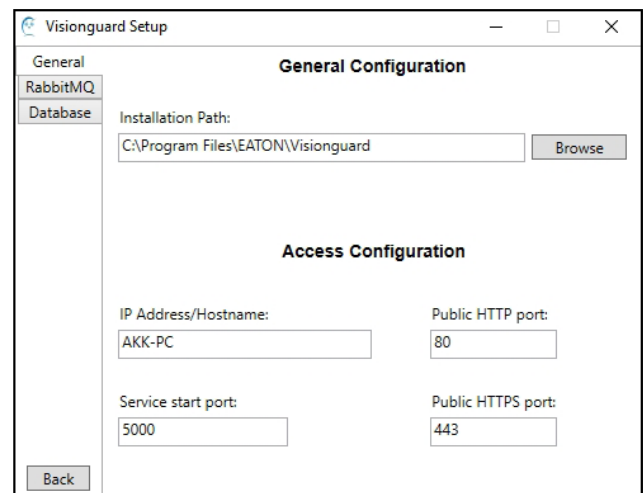
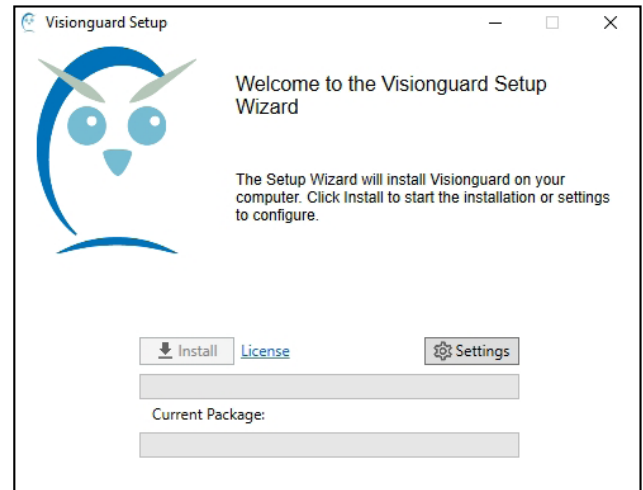
Settings > RabbitMQ

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).

WICHTIGER HINWEIS

Je nach System kann eine Installation oder ein Update-Vorgang längere Zeit dauern (bis zu 45 Minuten), ohne dass ein Installationsfortschritt sichtbar ist. Bitte unterbrechen Sie die Installation nicht.

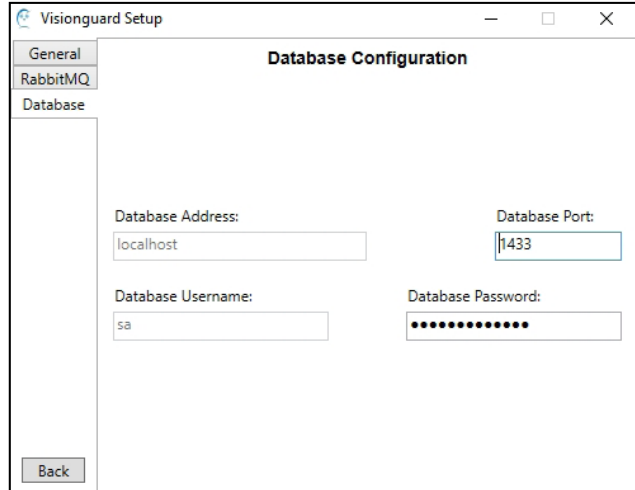
Es wird empfohlen, die Versionen vor der Installation in einen Ordner, z. B. C:/Temp, herunterzuladen. Wenn die Installationen auf einer anderen Windows-Umgebung durchgeführt werden sollen, empfiehlt es sich, die Software auf einen externen Datenträger, z. B. einen USB-Stick, herunterzuladen. Um die Installationszeit zu minimieren, wird empfohlen, von einer lokalen SSD oder Festplatte zu installieren, nicht von einem USB-Stick oder einem anderen externen Medium.



2.1 Installation der VisionGuard Software

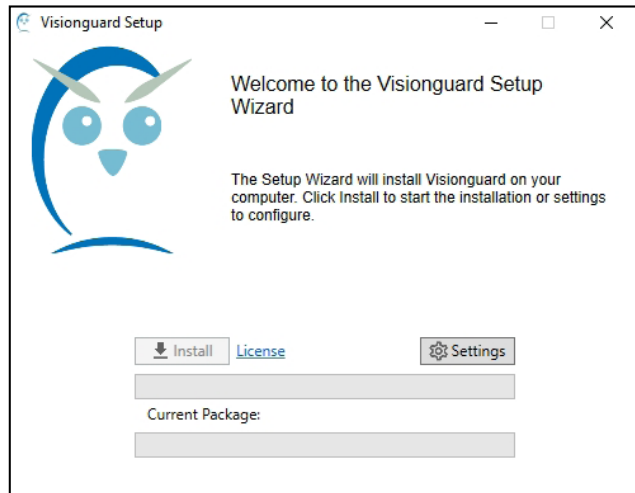
Settings > Database

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



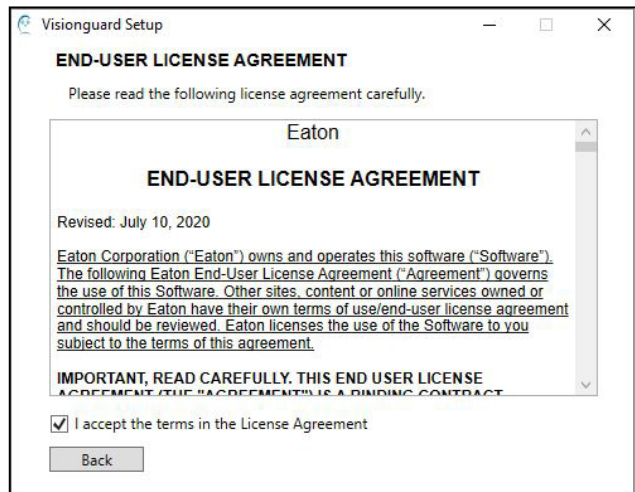
The screenshot shows the 'Database Configuration' window in the VisionGuard Setup application. It has a sidebar with 'General', 'RabbitMQ', and 'Database' tabs, with 'Database' selected. The main area contains four input fields: 'Database Address' (localhost), 'Database Port' (1433), 'Database Username' (sa), and 'Database Password' (masked with dots). A 'Back' button is at the bottom left.

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



The screenshot shows the 'Welcome to the Visionguard Setup Wizard' window. It features a blue owl logo on the left. The text says: 'Welcome to the Visionguard Setup Wizard' and 'The Setup Wizard will install Visionguard on your computer. Click Install to start the installation or settings to configure.' At the bottom, there are buttons for 'Install', 'License', and 'Settings'. Below these are two empty text boxes labeled 'Current Package:'.

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“

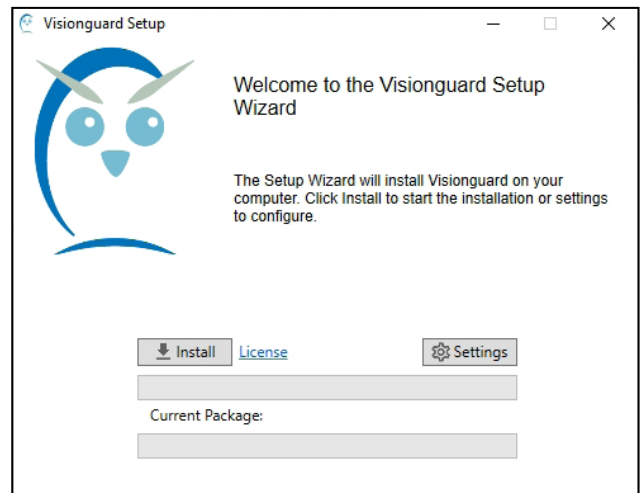


The screenshot shows the 'END-USER LICENSE AGREEMENT' window. It has a title bar 'Visionguard Setup' and a subtitle 'END-USER LICENSE AGREEMENT'. The text says: 'Please read the following license agreement carefully.' Below is a scrollable area containing the 'Eaton END-USER LICENSE AGREEMENT' document, which includes the date 'Revised: July 10, 2020' and a paragraph about the software's use. At the bottom, there is a checkbox labeled 'I accept the terms in the License Agreement' which is checked, and a 'Back' button.

Zurück mit „Back“.

2.1 Installation der VisionGuard Software

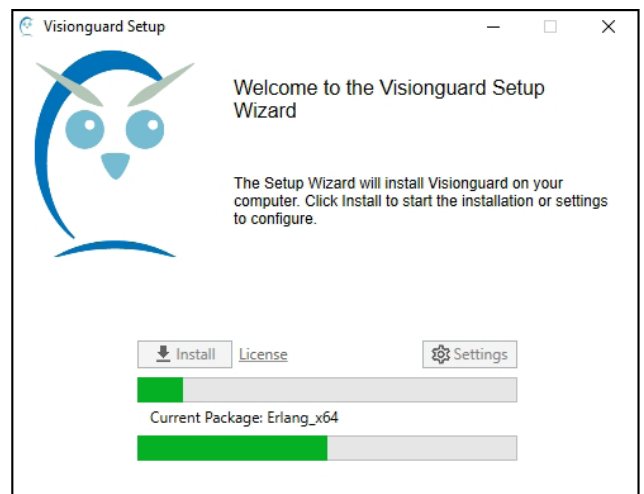
Die Installation kann nun über „Install“ gestartet werden



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 Installationsfortschritt wird über Fortschrittsbalken angezeigt.

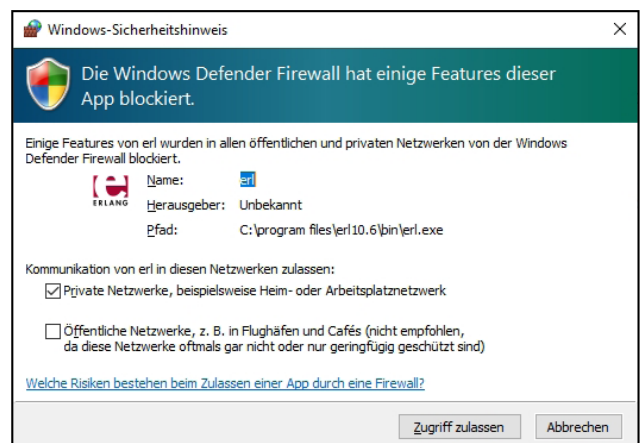
HINWEIS

In bestimmten Fällen kann die Installation ohne sichtbare Fortschrittsanzeige längere Zeit in Anspruch nehmen. Bitte unterbrechen Sie die Installation nicht.



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

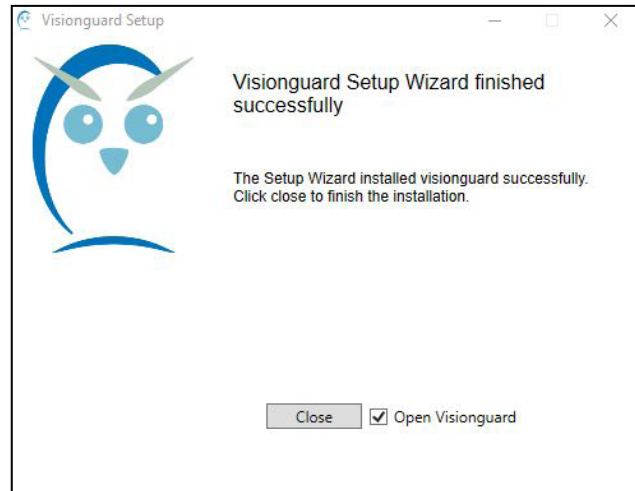
Es müssen unbedingt alle Zugriffe zugelassen werden, da ansonsten die HMIs der DualGuard-S keine Verbindung zur VisionGuard aufbauen können!



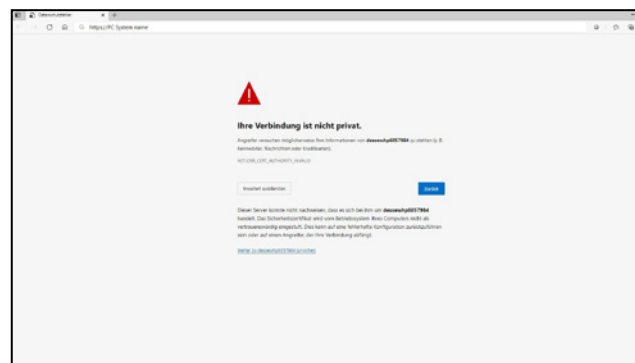
2.2 Installation der CG-S Gateway Software

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

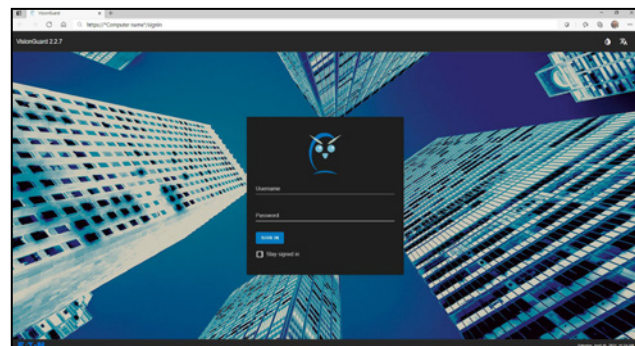
Die Installation der VisionGuard-Software ist nun abgeschlossen. Es wird empfohlen, „VisionGuard öffnen“ zu aktivieren. Mit Klick auf „Schließen“ startet der Standard-Browser mit der URL des VisionGuard. Sollen ZB-S Notlichtsysteme wie oben erwähnt an der VisionGuard angeschlossen werden, muss zusätzlich eine Gateway-Software und ein CG-S Interface Treiberpaket installiert werden. Bitte führen Sie dann die in 2.2 und 2.3 beschriebenen Installationen durch.



VisionGuard verwendet den Computernamen für den lokalen Client-Zugriff. Da noch kein Zertifikat installiert ist, erscheint eine Sicherheitsmeldung im Browser und verweigert den Zugriff. Um ein Zertifikat zu installieren, siehe Abschnitt 5 „Sicherheitszertifikat installieren“

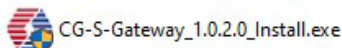


Über „Erweitert“ und „Weiter zu *Computername* (unsicher)“ gelangen Sie auf die Anmeldeseite des lokalen VisionGuards. Es wird empfohlen, jetzt ein Lesezeichen im Webbrowser zu setzen. Um die Installation abzuschließen, wird dringend empfohlen, den PC neu zu starten.



2.2 Installation der CG-S Gateway Software

Die Installation muss „als Administrator“ gestartet werden. Rechter Mausklick auf diese .exe-Datei

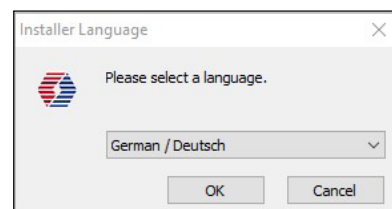


öffnet ein Menü. Klicken Sie auf „als Administrator ausführen“, um den VisionGuard-Einrichtungsassistenten zu starten. Es kann eine Meldung der Windows Benutzerkontensteuerung zuerst erscheinen

In diesem Fall, bitte mit „JA“ bestätigen.

Nach dem Start der Installations erscheint ein Fenster um die Sprache einzustellen.

Es kann zwischen Deutsch und Englisch gewählt werden. Wählen Sie Ihre bevorzugte Sprache und klicken Sie auf OK.

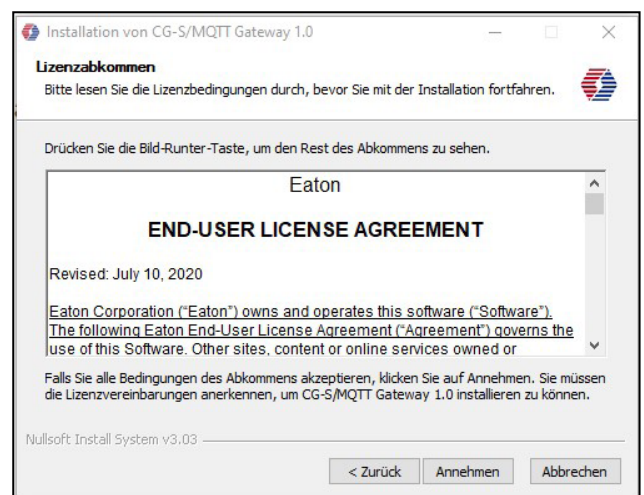


2.2 Installation der CG-S Gateway Software

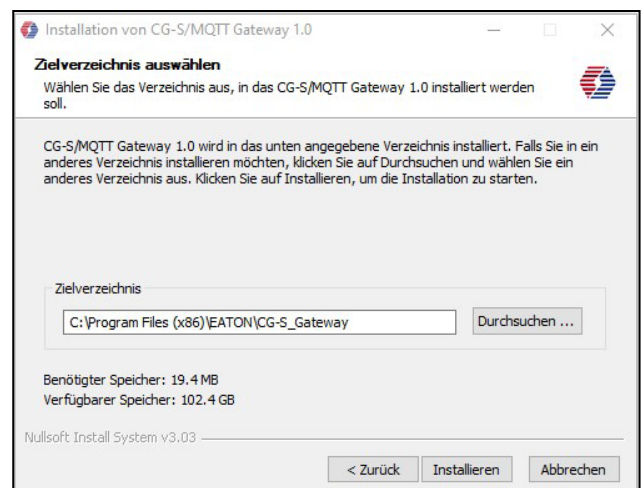
Die Installation startet. Weiter mit "Weiter"



Eine Lizenzvereinbarung erscheint. Bitte lesen Sie diese aufmerksam durch und bestätigen Sie durch „Annehmen“.

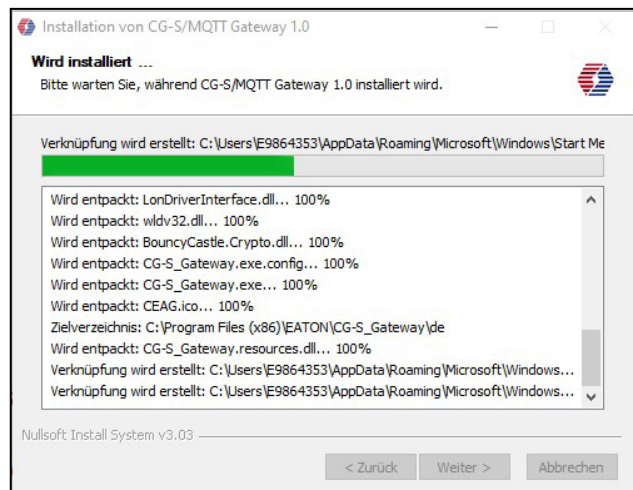


Im nächsten Fenster kann der gewünschte Installationspfad gewählt werden. Es wird empfohlen mit den Standardeinstellungen fortzufahren. Weiter mit "Installieren".



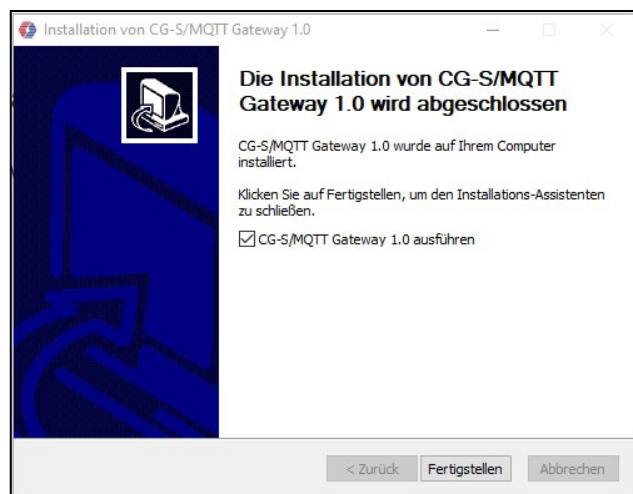
2.2 Installation der CG-S Gateway Software

Die Installation startet mit einer Fortschrittsanzeige.

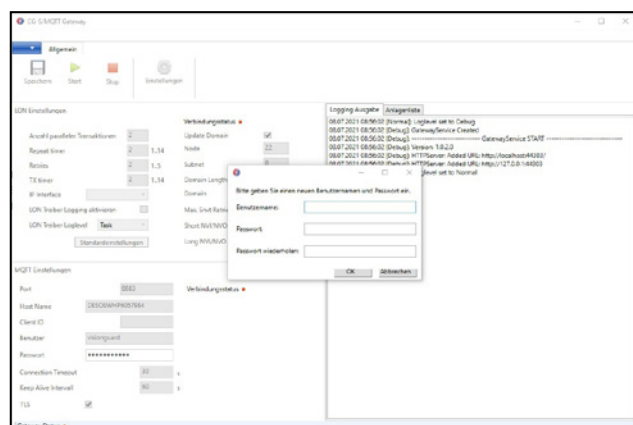


Nach der Installation aktivieren Sie bitte "Run CG-S/MQTT Gateway".

Die Installation wird durch einen Klick auf "Fertigstellen" abgeschlossen.



Die Gateway Software startet (CEAG Symbol in der Taskleiste). Es ist notwendig einen Nutzernamen zuzuweisen und ein sicheres Passwort zu setzen, um die Gateway Software zu betreiben.

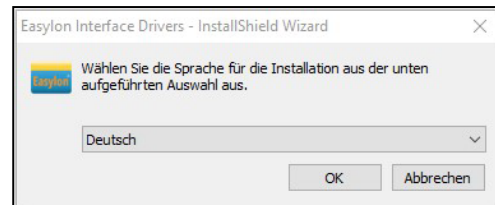


2.3 Installation des CG-S Interface Treiberpakets

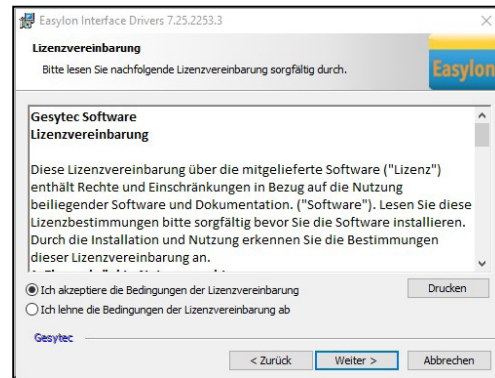
Das CG-S Interface Treiberpaket ermöglicht eine Verbindung. Die Installation muss "als Administrator" gestartet werden. Rechter Mausklick auf diese .exe-Datei:



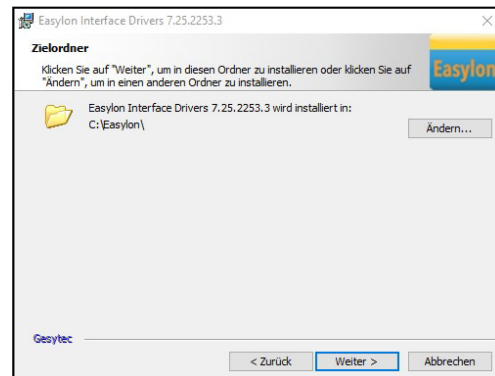
Nach Start der Installation erscheint ein Fenster zur Auswahl der Sprache. Es kann zwischen Deutsch und Englisch gewählt werden. Wählen Sie Ihre bevorzugte Sprache und klicken Sie auf „OK“.



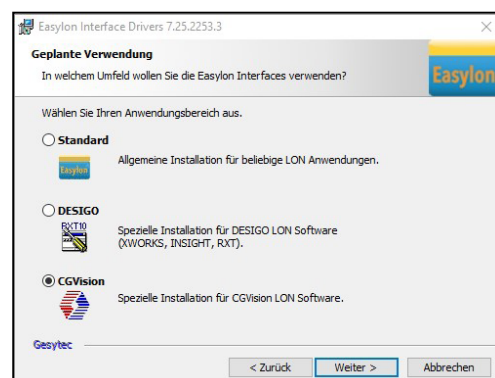
Eine Lizenzvereinbarung erscheint. Bitte lesen Sie sie aufmerksam und bestätigen Sie mit "I accept the terms in the license Agreement", dann weiter über „Weiter“



Im nächsten Fenster kann der Installationspfad gewählt werden. Es wird empfohlen die Standardeinstellungen beizubehalten. Fortsetzen über „Weiter“.



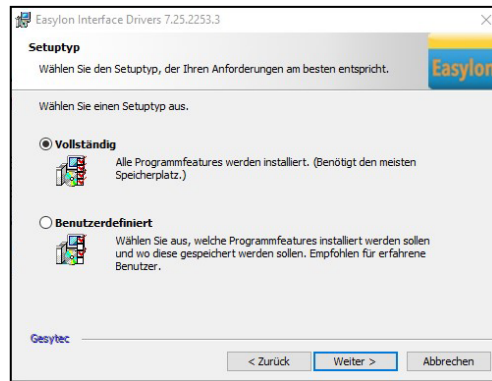
Eine Auswahl für die Anwendung erscheint. Bitte wählen Sie „CGVision“ und bestätigen Sie mit „Weiter“



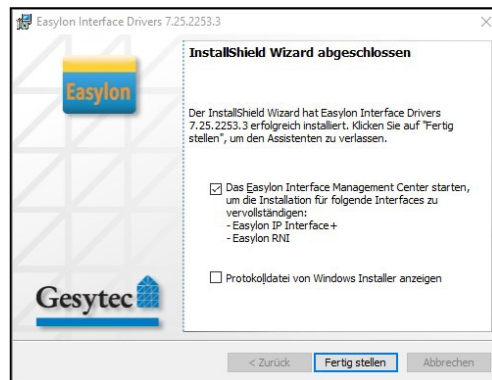
2.3 Installation des CG-S Interface Treiberpakets

Die Wahl des Installationstyps erscheint. Bitte wählen Sie "Vollständig" und bestätigen mit "Weiter".

Dies kann einige Minuten dauern.
Eine Fortschrittsanzeige hält Sie über den Status auf dem Laufenden.

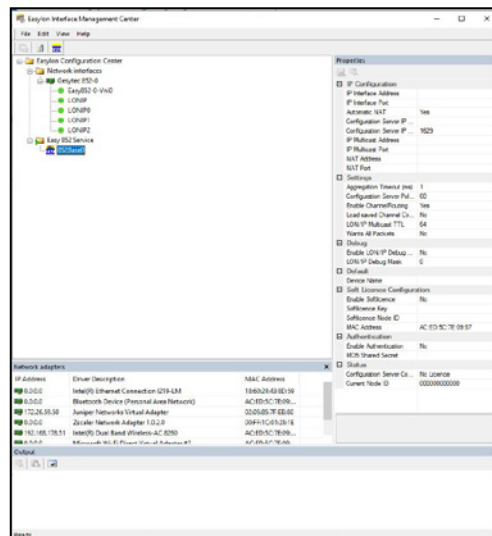


Um die Installation abzuschließen, aktivieren Sie "Launch of the Easyton Interface Management Center", um die richtigen Interface-Einstellungen zu konfigurieren und bestätigen Sie mit „Fertigstellen“.



Für die configuration, bitte wählen Sie

- das richtige CG-S-Interface
(852 CG-S/IP-Interface oder CG-S/USB-Interface).
- den richtigen "Network adapter" (IP-Adresse) des CG-S/IP-Interface, der als "IP-Interface Address" unter "IP-Configuration" erscheinen sollte.
- Unter "Configuration Server" erscheint die Verbindung als lizenziert wenn die Verbindung zum Konfigurations-Server erfolgreich aufgebaut ist.



2.4 Update einer bestehenden VisionGuard Installation

2.4.1 Updatebeschreibung der VisionGuard Software

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!

2.4.2 Durchführen eines Updates der VisionGuard Software

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

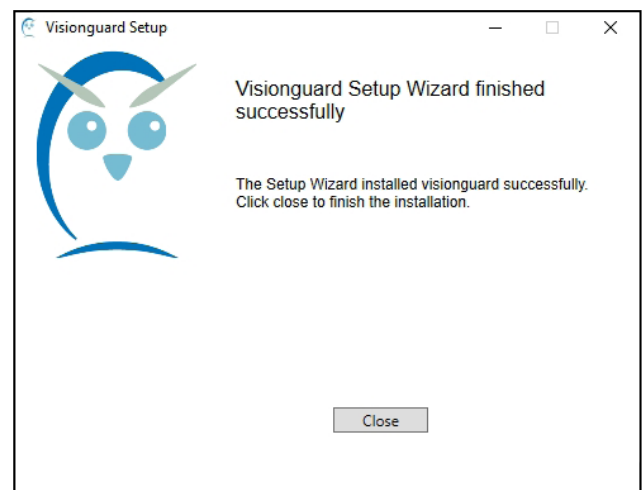
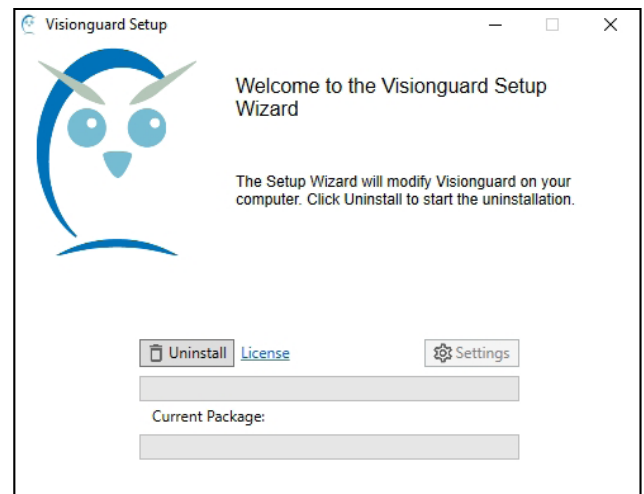
Mit Klick auf „Uninstall“ wird erst die VisionGuard deinstalliert, und die neue Installation gestartet was ca. 5 Minuten in Anspruch nimmt. Ein Fortschrittsbalken informiert über den aktuellen Updateverlauf. Zum Ende des Updates erscheint folgendes Fenster.

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

Bestehende Konfigurationen werden nicht überschrieben, aber es wird empfohlen, aus Sicherheitsgründen ein Backup der bestehenden VisionGuard-Version zu erstellen. Ein Backup kann über die integrierte Backup-Funktion in der VisionGuard durchgeführt werden. Siehe dazu Kapitel 15 „Speichern und Wiederherstellen“.

WICHTIGE HINWEISE

Je nach System kann ein Update-Vorgang längere Zeit dauern (bis zu 45 Minuten), ohne dass ein Installationsfortschritt sichtbar ist. Bitte unterbrechen Sie die Installation nicht. Bei einem Update von einer V3.0.1 oder älter, auf die aktuelle V3.1.0 muss unbedingt der ODBC-Treiber über die Windows Funktion „Apps & Features“ manuell deinstalliert werden! Nach der manuellen Deinstallation muss der PC erst neu gestartet werden. Nach dem Neustart kann nun das Update der VisionGuard durchgeführt werden. Es wird dringend empfohlen vor einem Update bei der V3.0.1 ein Backup (Programmsicherung) durchzuführen. Siehe Kapitel 15.



2.5 Deinstallation von VisionGuard Softwarekomponenten

2.5 Deinstallation von VisionGuard Softwarekomponenten

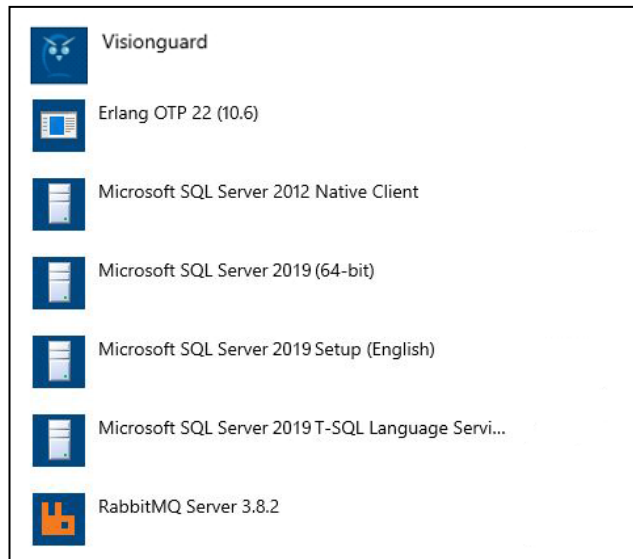
Für eine Deinstallation muss die VisionGuard vorher beendet werden! Eine komplette Deinstallation der VisionGuard kann über die Windowsfunktion „Apps & Features“ erfolgen. Folgende Dienste müssen deinstalliert werden:

- VisionGuard
- Erlang
- Rabbit MQ
- Microsoft MSSQL 2019

WICHTIGER HINWEIS:

Es dürfen nur die VisionGuard-Instanzen in Microsoft SQL Server deinstalliert werden! Andernfalls könnten andere Programme, die ebenfalls MSSQL verwenden, nicht mehr funktionieren.

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



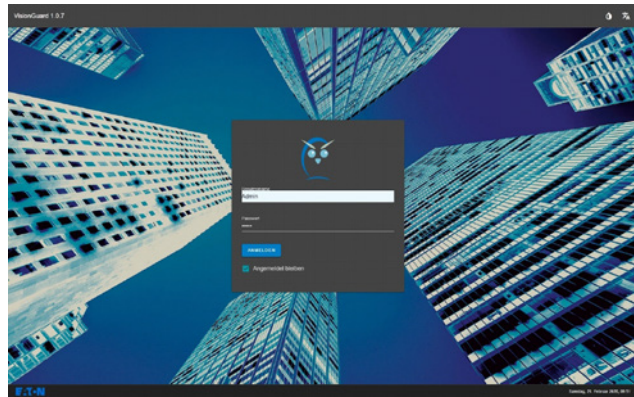
3 Erster Start der VisionGuard

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

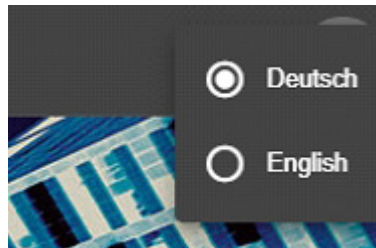
Die VisionGuard wird bei einem lokalen Zugriff über einen handelsüblichen Webbrowser, z.B. Microsoft Edge über die URL:

<https://localhost> (verschlüsselt) gestartet.

Es ist auch möglich, den Computernamen oder die aktive IP-Adresse für die Anmeldung an der VisionGuard zu verwenden. Es erscheint folgendes Anmeldefenster:



Im obigen rechten Bereich kann die Sprache voreingestellt werden:

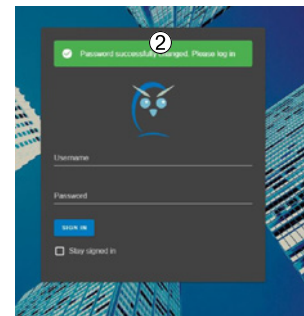
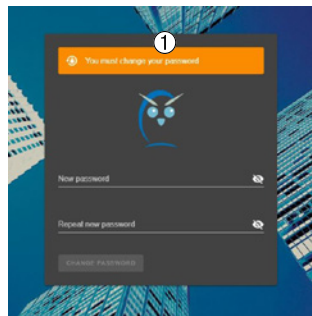


Es ist in der VisionGuard ein Standard-Benutzer mit Supervisor Rechten voreingestellt!

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



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

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

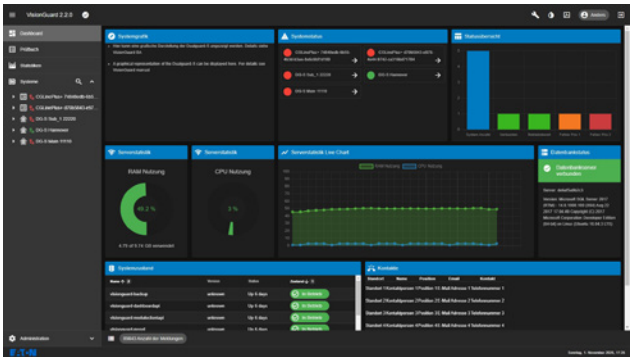
WICHTIGER HINWEIS

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

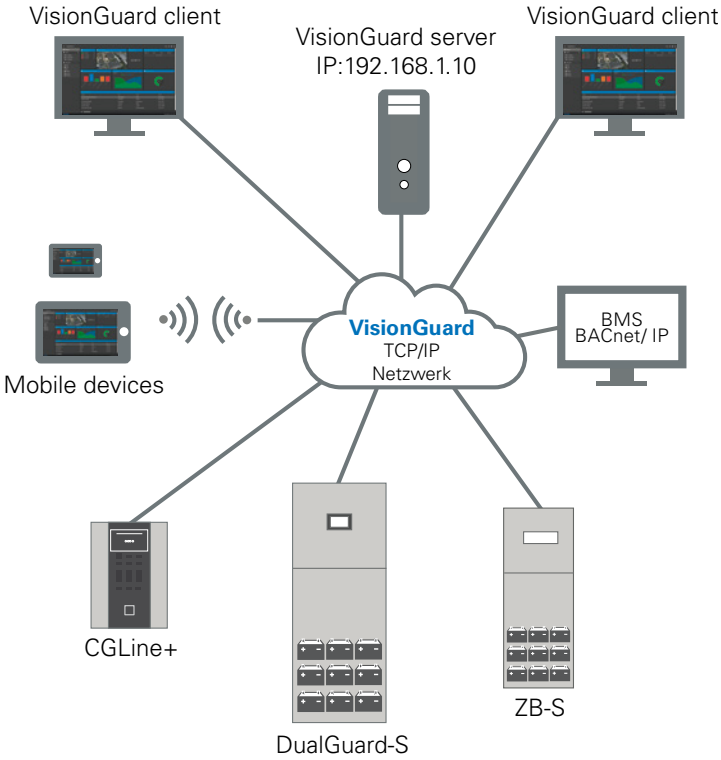
Richtlinie	Wert
Zahl	Ja
Sonderzeichen	Ja
Kleinbuchstaben	Ja
Großbuchstaben	Ja
Minimale Passwortlänge	6

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, oder über https://192.168.1.10 (verschlüsselt). Schema:



(Hinweis: CGLine+ in Vorbereitung)

4 Lizenzierung

4.1 Aktivierung einer Lizenzierung

Um die VisionGuard nutzen zu können, muss dafür eine Lizenz erworben werden. Es sind unterschiedliche Lizenzen erhältlich, je nachdem wie viele DualGuard-S oder ZB-S Systeme an die VisionGuard abgeschlossen werden sollen. Welche Lizenzen erhältlich sind, können Sie im Kapitel 1.5 VisionGuard Lizenzen nachlesen. Mit Erwerb einer VisionGuard Lizenz erhält der Kunde einen „Productkey“ in schriftlicher Form oder USB-Stick, der später benötigt wird.

WICHTIGER HINWEIS

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

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

① „Neuen Fingerprint abrufen“

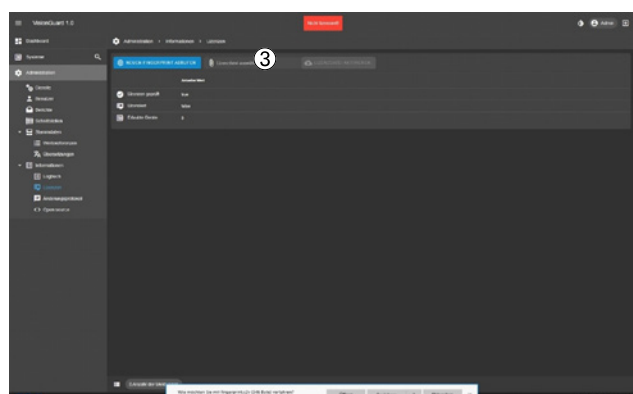
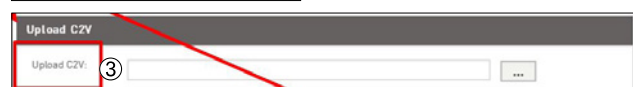
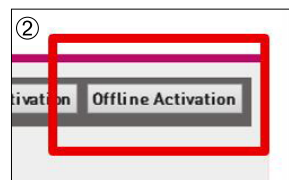
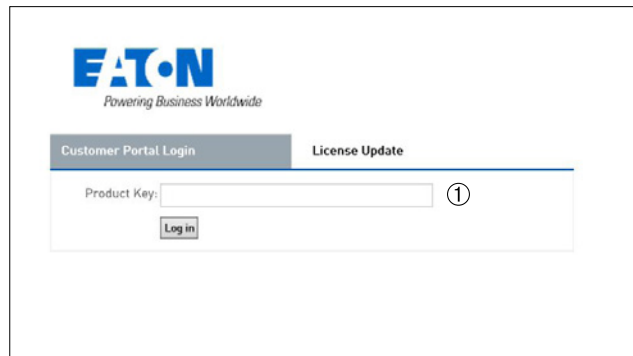
② Es wird eine Datei mit dem Namen „fingerprint.c2v“ erzeugt, die in einem Ordner, z.B. C:\temp oder auf einen externen Datenträger, z.B. USB-Stick gespeichert werden muss.

Diese Datei muss nun online im Lizenzserver unter <https://ceagsystems.sentinelcloud.com/ems/customerLogin.html> hochgeladen werden (siehe Pos. 1).

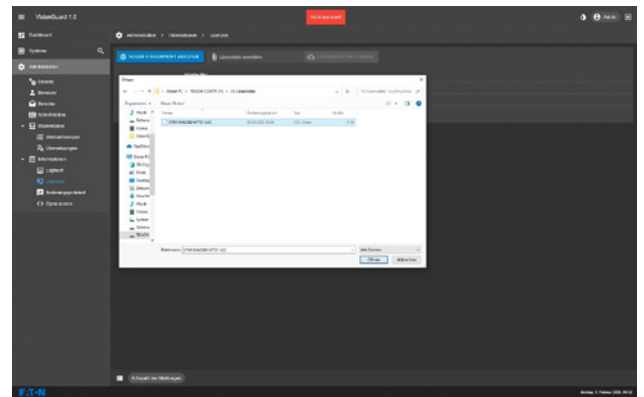
Für einen Login muss im Feld „Product Key“ der 32-stellige erworbene Produktkey eingegeben werden. Dieser hat das Format:
xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxx
Nach Login sollten im Aktivierungsregister Namen und Kontaktdaten eingegeben werden (freiwillig).
Wählen Sie oben rechts „Offline Activation“ (Pos.2)
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.

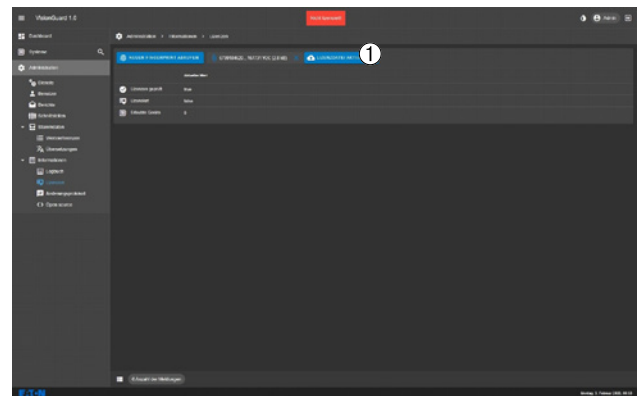
③ Über „Lizenzdatei auswählen“ kann der Aktivierungsschlüssel in die VisionGuard geladen werden



Im Dialogfenster kann nun der Speicherort des Aktivierungsschlüssels angegeben werden

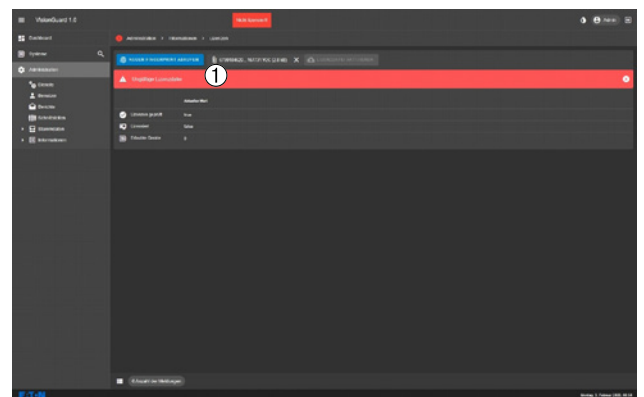


- ① Über „Lizenzdatei aktivieren“ kann die erworbene Lizenz in der VisionGuard aktiviert werden

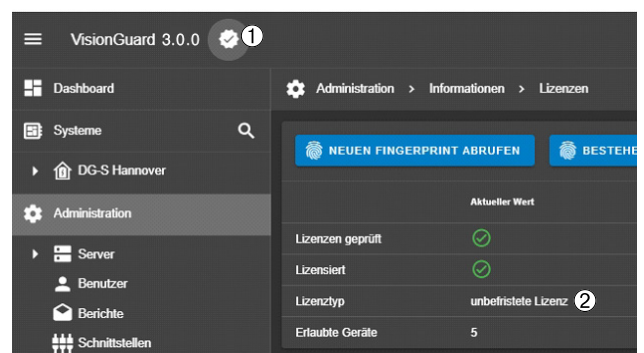


- ① Es erscheint noch die Meldung „ungültige Lizenzdatei“

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

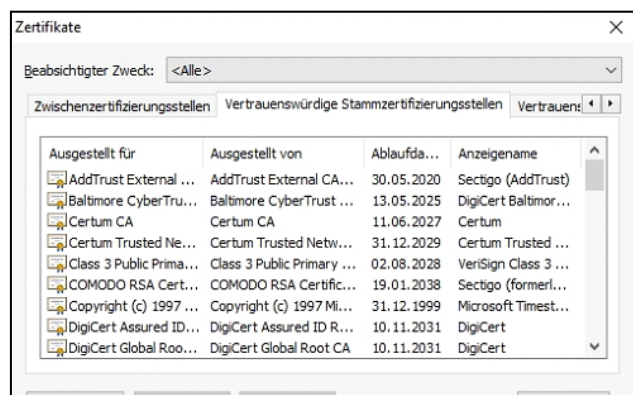
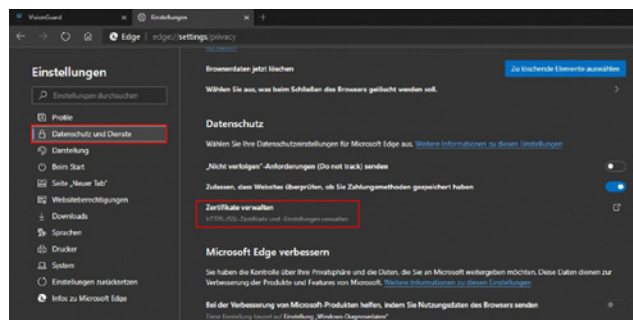
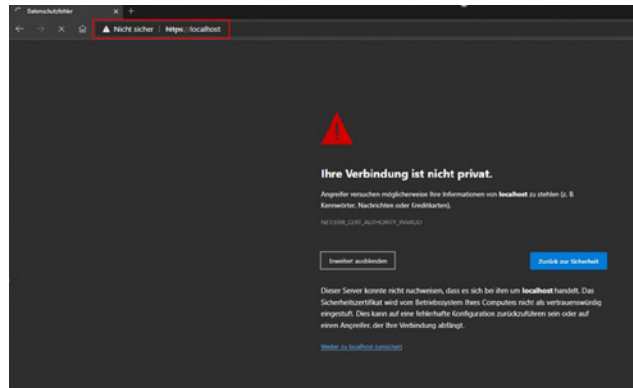
Erfolgt der Zugriff von einem Browser auf einen lokal installierten VisionGuard muss folgendermaßen vorgegangen werden. Die folgende Anleitung bezieht sich auf den Chrom-Browser. Bei anderen Browsern muss ähnlich vorgegangen werden.

HINWEIS

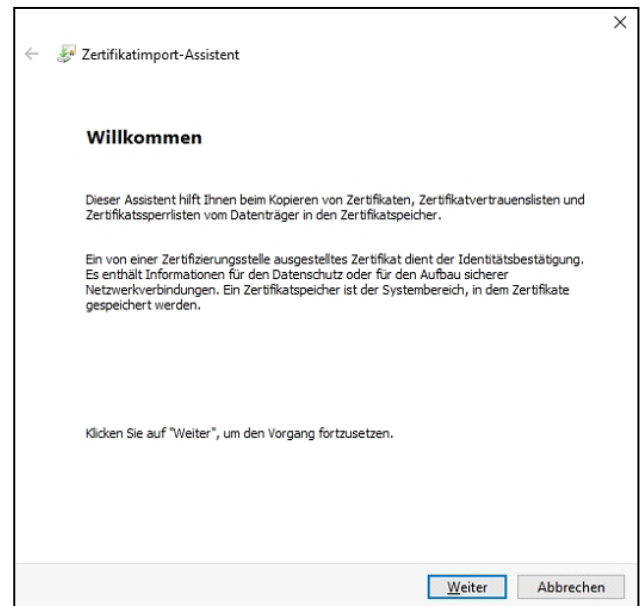
Für alle internen HTTPS-Ports wird bei der Installation ein Zertifikat mit einem automatisch generierten Passwort erzeugt. Das Zertifikat finden Sie unter C:\Program Files\EATON\Visionguard\certs\cert_api.crt

Für die externe Kommunikation über den Webserver wird ein von Eaton generiertes Zertifikat bereitgestellt. Dieses Zertifikat finden Sie ebenfalls unter C:\Program Files\EATON\Visionguard\certs\cert_proxy.crt
cert_proxy.pem
Öffnen sie im Browser das Menü Einstellungen > Datenschutz und Dienste > Zertifikate verwalten

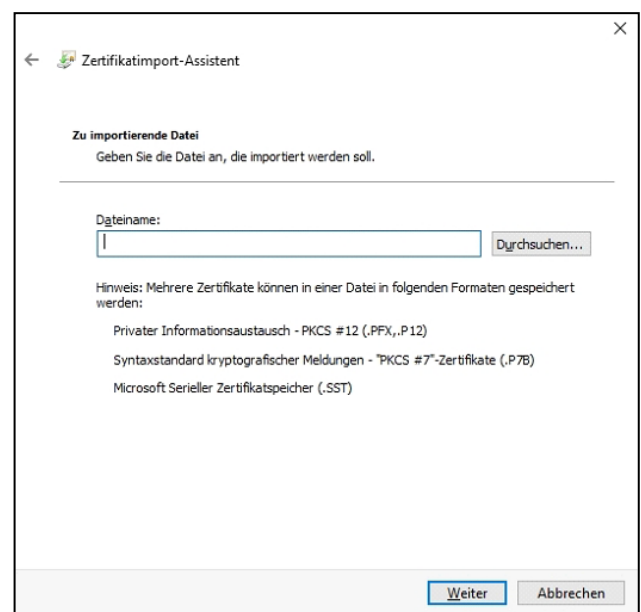
Über „Zertifikate verwalten“ öffnet sich die Zertifikatsverwaltung, in der man Zertifikate importieren kann



Über „Importieren“ startet man den Zertifikat-Import Assistenten



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



Über „Durchsuchen“ kann man das Zertifikat auswählen.
Für interne https-Ports befindet er sich im Ordner

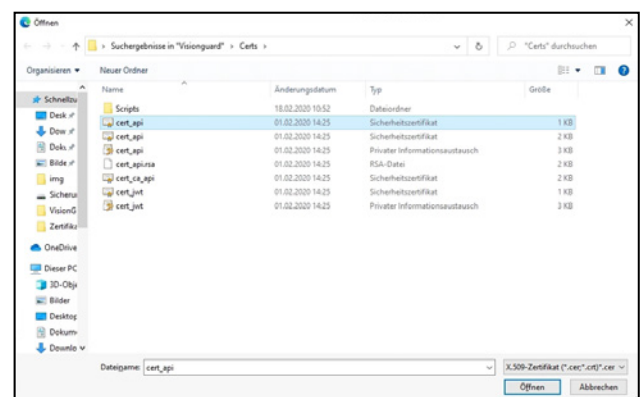
`C:\Program Files\EATON\Visionguard\cert`

Das Zertifikat hat den Namen: `cert_api.crt`

Für die externe Kommunikation über den Webserver befinden sich die Zertifikate im Ordner
`C:\Program Files\EATON\Visionguard\certs`

Die Zertifikate heißen
`cert_proxy.crt`
`cert_proxy.pem`

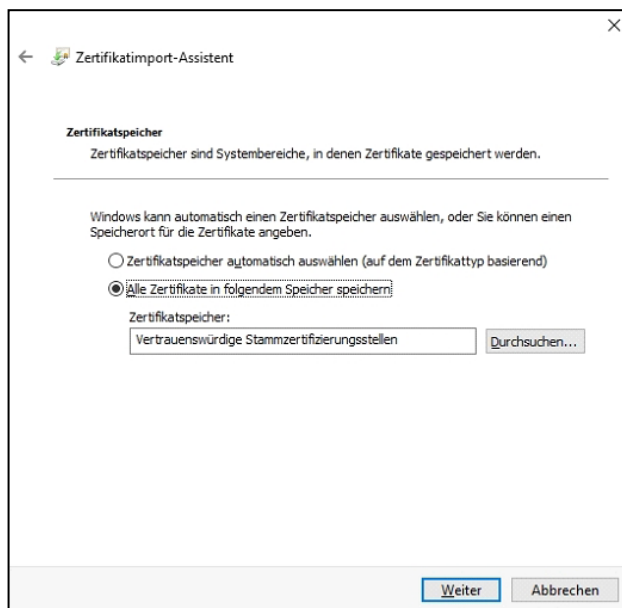
Nach Auswahl des Zertifikats wird fortgefahren mit „Öffnen“



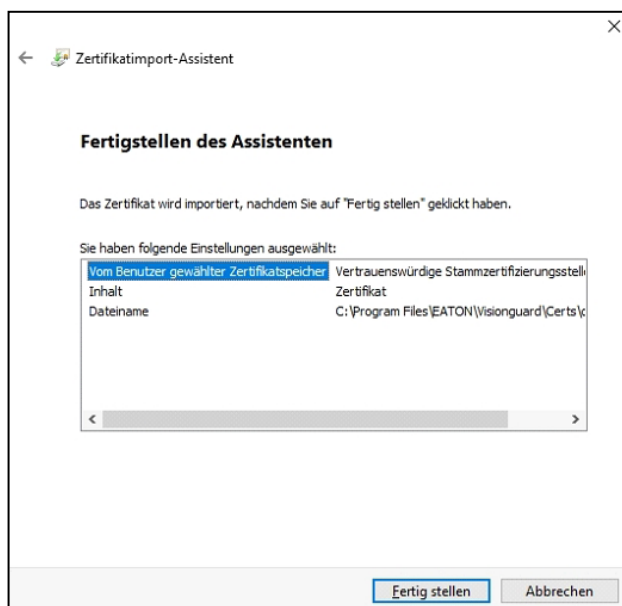
5 Installation von Sicherheitszertifikaten

Das Zertifikat muss im Zertifikatsspeicher „Vertrauenswürdige Stammzertifizierungsstellen“ gespeichert werden

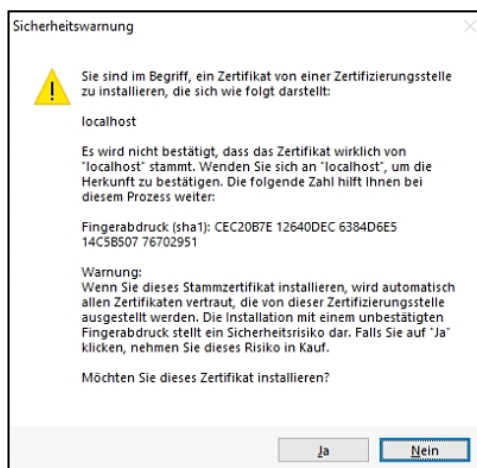
Fortfahren mit „Weiter“



Beenden mit „Fertig stellen“



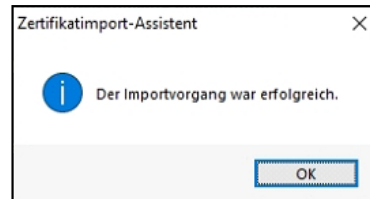
Das Zertifikat kann in der Sicherheitswarnung jetzt über „Ja“ installiert werden



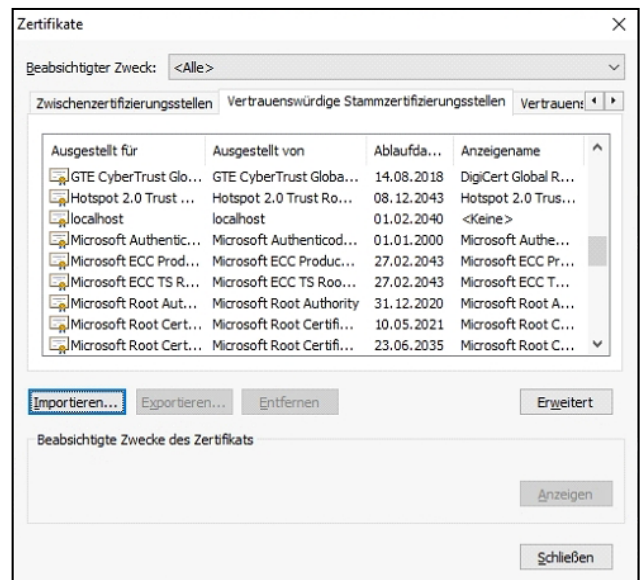
5.2 Installation des Sicherheitszertifikates bei Fernzugriff

Es muss folgende Meldung erscheinen

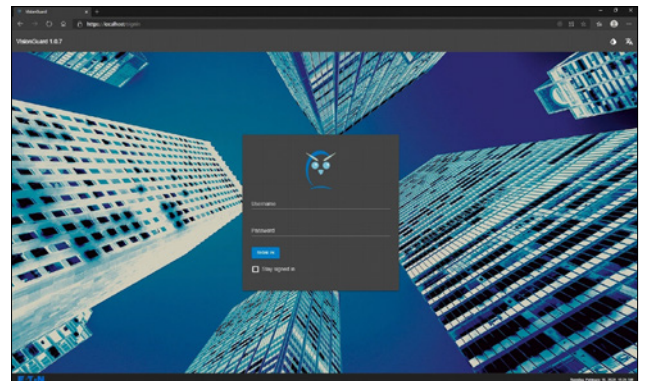
„Der Importvorgang war erfolgreich.“



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 Sicherheitszertifikates 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)

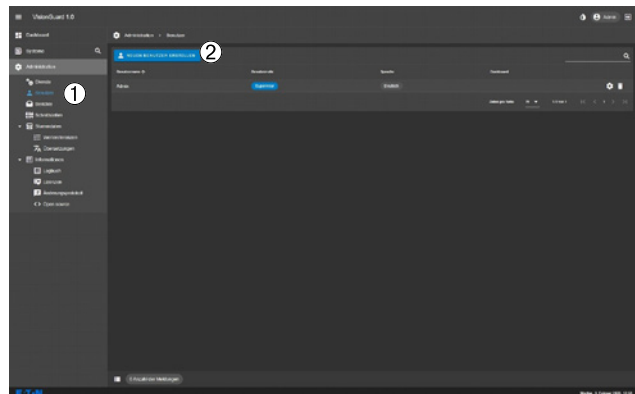
In der VisionGuard können beliebig viele Benutzer mit unterschiedlichen Benutzerrollen angelegt werden. Die unterschiedlichen Benutzerrollen definieren unterschiedliche Zugriffsberechtigungen:

Role	Administrative UAC / Translations	Administrative VisionGuard Basics	DG-S configuration	DG-S / ZB-S control	DG-S / ZB-S status
Supervisor	X	X	X	X	X
Administrator		X	X	X	X
Power User				X	X
User					X

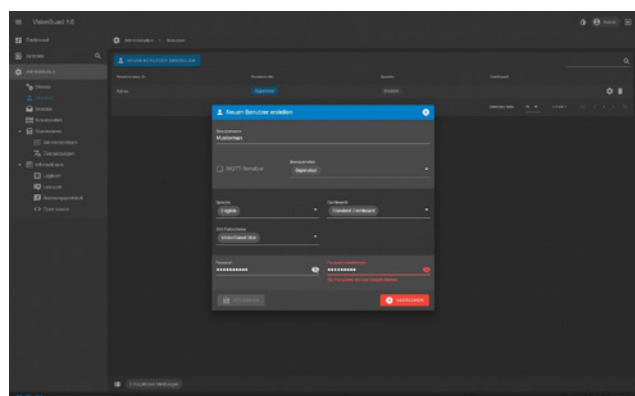
Der Supervisor hat gegenüber dem Administrator noch die Berechtigung Benutzerkonten zu erstellen und zu editieren sowie Übersetzungsdateien zu erstellen.

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

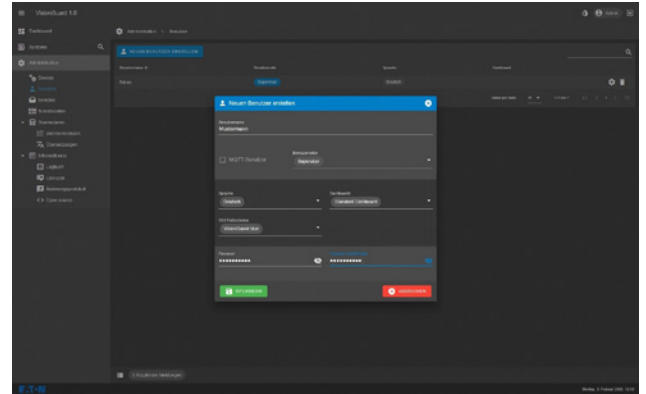


- ① Unter Benutzername kann der Name des neuen Benutzers der im Anmeldefenster der VisionGuard eingegeben werden muss, festgelegt werden
- ② Unter Benutzerrolle kann eine Rolle mit unterschiedlichen Zugriffsberechtigungen festgelegt werden (siehe Tabelle oben)
- ③ Unter Sprache kann die Benutzersprache 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.



6 Neue Benutzer mit Benutzerrollen anlegen

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



7 Anlegen von Dualguard-S Systemen in der VisionGuard

7.1 HMI zur Anbindung an VisionGuard konfigurieren

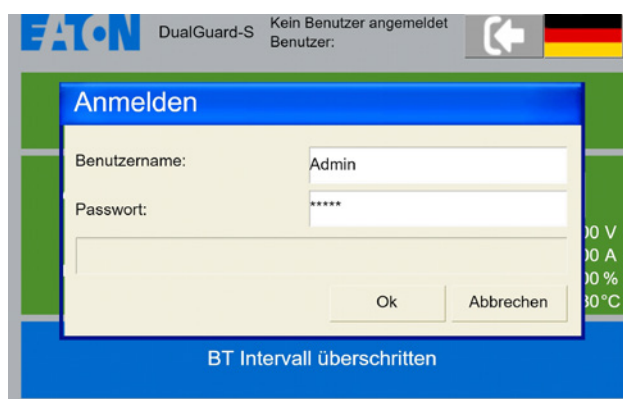
Um ein Dualguard-S System an der VisionGuard anzulegen, müssen am HMI Verbindungseinstellungen vorgenommen werden!

Hinweis: Um im HMI-Menü die Verbindungseinstellungen zur VisionGuard vornehmen zu können, muss man als „Experte“ angemeldet sein!

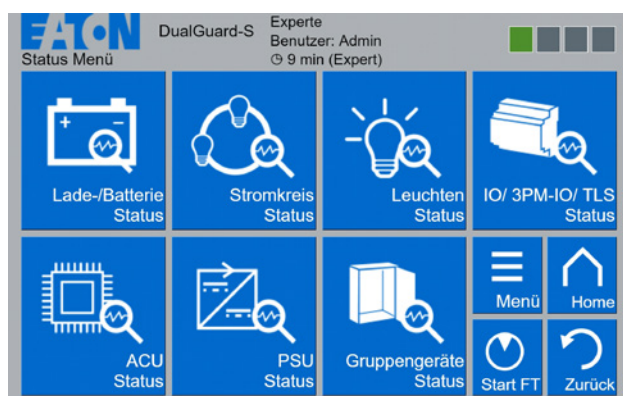
Die Verbindungseinstellungen können direkt am HMI oder idealerweise per Webzugriff vorgenommen werden.

Anmeldung im HMI:

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



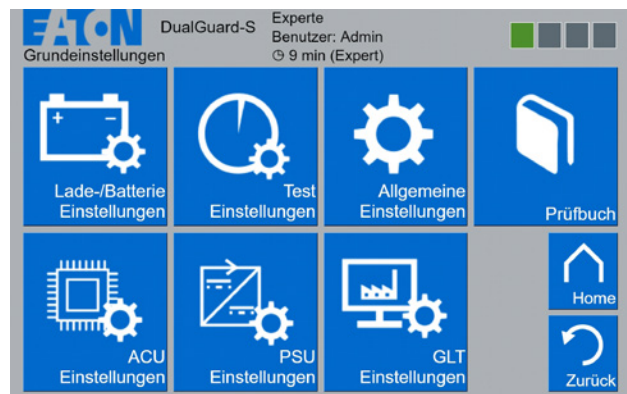
Weiter über „Menü“



Weiter über „Grundeinstellung“



Weiter über „GLT-Einstellungen“

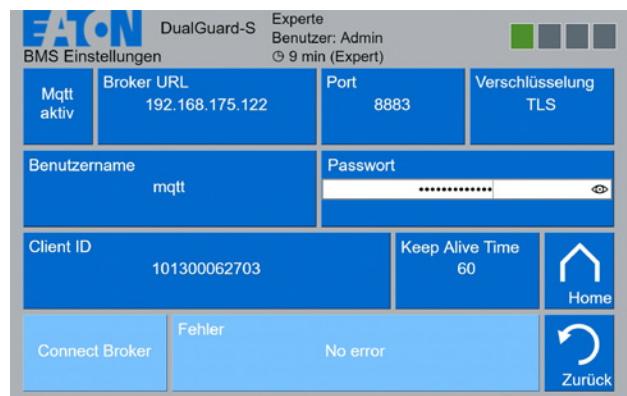


Weiter über „VisionGuard Einstellungen“



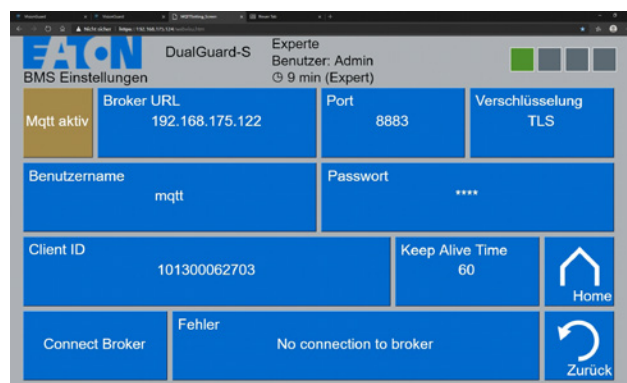
Im Menü „VisionGuard Einstellungen“ müssen folgende Eingaben gemacht werden:

- „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 dringend 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.

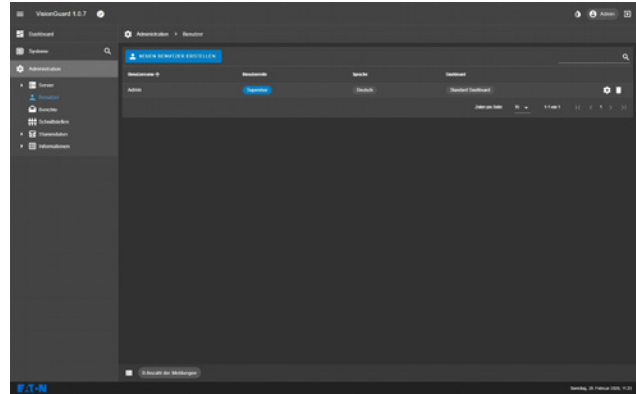


7.2 Anlegen und autorisieren einer DualGuard-S in der VisionGuard

7.2 Anlegen und autorisieren einer DualGuard-S in der VisionGuard

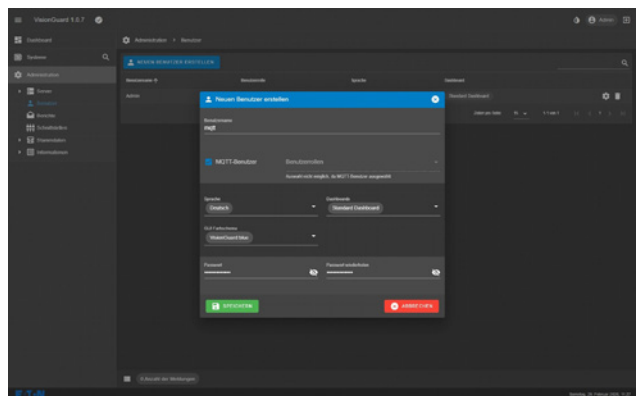
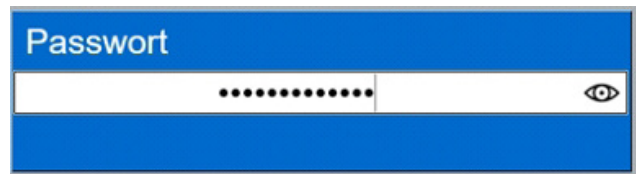
Damit Dualguard-S in der VisionGuard angelegt werden können, muss in VisionGuard ein MQTT-Benutzer angelegt werden.

- ① Dieses erfolgt im Menü Administration/Benutzer
- ② Über „Neuen Benutzer erstellen“ wird ein neuer MQTT-Benutzer angelegt

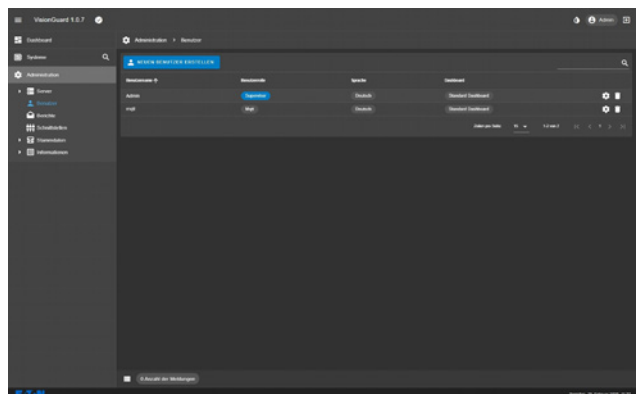


Im nächsten Dialogfenster müssen folgende Einstellungen vorgenommen werden:

- 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

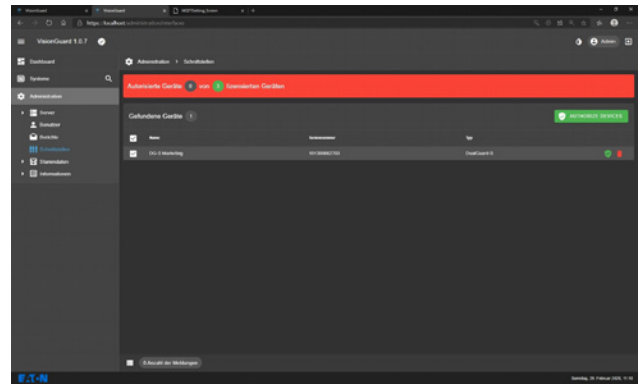


Der Benutzer für die Anbindung (hier mqtt) ist nun angelegt

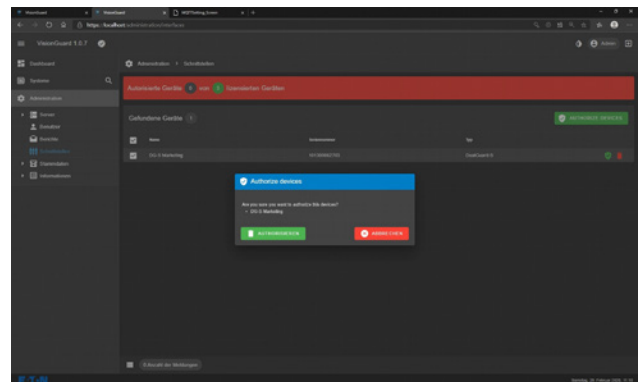


7.2 Anlegen und autorisieren einer DualGuard-S in der VisionGuard

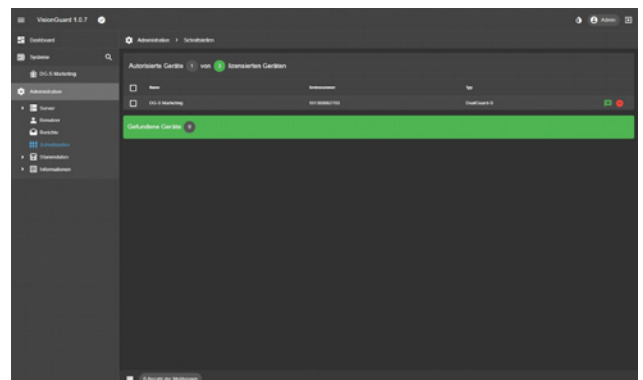
- ① Wenn die Einstellungen im HMI der Dualguard-S mit den Einstellungen des mqtt-Benutzers in der VisionGuard übereinstimmen, wird die DualGuard im Menü Administration/Schnittstellen angezeigt
- ② Über „Gerät autorisieren“ wird die Dualguard-S in der VisionGuard angelegt



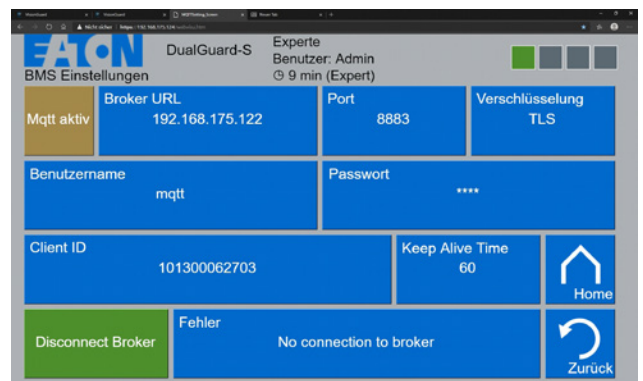
Bestätigen durch „Autorisieren“



Die DualGuard-S wurde nun in der VisionGuard erfolgreich angemeldet



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

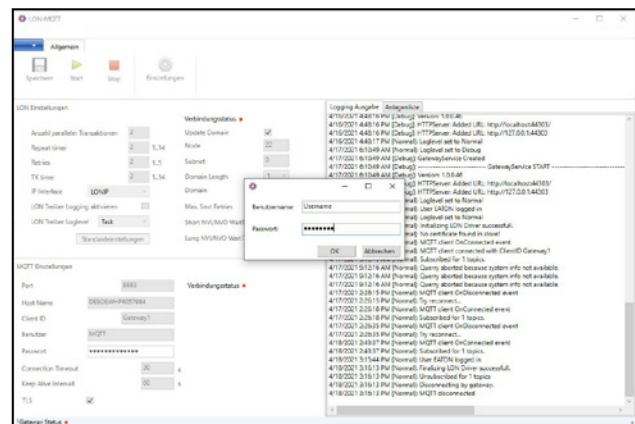
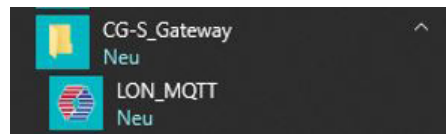


8 Anlegen von ZB-S Systemen in VisionGuard

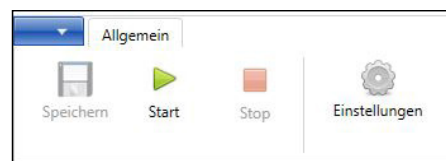
8.1 CG-S Gateway Konfiguration

Starten Sie die CG-S Gateway Software
"LON MQTT" (mgf. als Administrator ausführen)

Bitte geben Sie Nutzernamen und Passwort wie in Kapitel 2.2 erstellt ein.



Zuerst müssen die Einstellungen des Gateways überprüft oder konfiguriert werden.
Bitte "Einstellungen" öffnen.



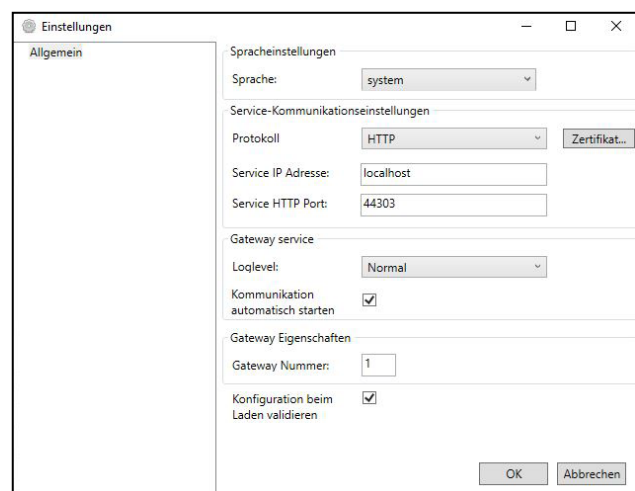
In den Einstellungen überprüfen Sie bitte die folgenden Punkte:

Sprache: Es kann zwischen "Betriebssystem", Deutsch oder Englisch gewählt werden
Protokoll: HTTP oder HTTPS

Bei HTTPS muss ein Zertifikat installiert werden.

Service IP Adresse: localhost oder die IP Adresse des VisionGuard Servers
Service HTTP port: 44303
Gateway service: Bitte aktivieren Sie "Kommunikation automatisch starten"
Gateway Nummer: 1

Dann auf OK klicken um die Einstellungen zu bestätigen.



Nun wählen Sie in den LON-Einstellungen das richtige IP-Interface. Unterstützt werden das CG-S/IP-Interface und das CG-S/USB-Interface.

Für das CG-S/IP-Interface ist die richtige Einstellung:

LONIP

Für das CG-S/USB-Interface ist die richtige Einstellung:

LONUSB

ACHTUNG!

Andere Einstellungen sind nicht erforderlich. Bitte auf Standard-Einstellungen belassen!

Unter MQTT Einstellungen müssen die folgenden Parameter gesetzt werden:

Port: 8883
 Host Name: Name des PCs oder der IP Adresse des VisionGuard Servers
 Client ID: LONMQTT (Standard)
 Benutzer: Muss exakt gleich dem MQTT Benutzer der VisionGuard sein (siehe Kapitel 7.2)
 Passwort: Muss exakt gleich dem MQTT Passwort der VisionGuard sein (siehe Kapitel 7.2)
 Connection Timeout: 30S
 Keep Alive Intervall: 60s
 TLS: Aktiviert

Nun müssen die Einstellungen über „Speichern“ gesichert werden.

Um die Funktion des Gateways zu testen, kann es nun über “Start” gestartet werden.

Der korrekte Betrieb des Gateways wird über die Verbindungsanzeige (Verbindungsstatus) in den LON- und MQTT-Einstellungen angezeigt. Die Anzeige muss in grüner Farbe erscheinen.

Eine rote Anzeige zeigt an, dass das Gateway nicht ordnungsgemäß funktioniert. Bitte überprüfen Sie die Einstellungen nochmals.

8.2 Anlegen und autorisieren von ZB-S Systemen in VisionGuard

BITTE BEACHTEN SIE:

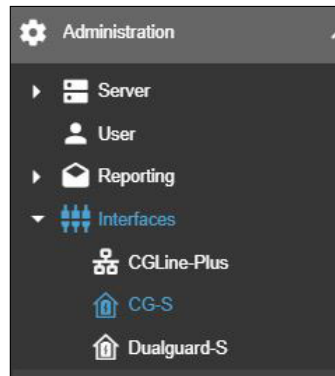
Um eine ZB-S in der VisionGuard hinzuzufügen, müssen Sie mindestens als Admin oder Supervisor eingeloggt sein!

Die Visionguard ist darauf ausgelegt, Strukturen und Daten einer bestehenden CGVision-Visualisierungssoftware zu übernehmen, die über eine Gruppen-/Systemstruktur verfügt, die bis zu 32 Notbeleuchtungsanlagen in bis zu 15 Gerätegruppen abgebildet hat.

Diese Gruppenstruktur für CG-S-Systeme ist in VisionGuard beibehalten worden, wird aber für die spätere Visualisierung in der Explorer-Struktur nicht sichtbar verwendet. Vorbereitung: Um ein ZB-S-System hinzuzufügen, müssen die Neuron-ID und die Geräte-Nr. (1-32) aus dem ZB-S-Steuergerät CU-CG-S ermittelt werden. Sehen Sie dazu in die Bedienungsanleitung der ZB-S.

8.2.1 Erstellen neuer Gruppen und anlegen und autorisieren von ZB-S Systemen in VisionGuard

Gehen Sie bitte im Menü „Administration“ in das Untermenü „Schnittstellen“ und „CG-S“.

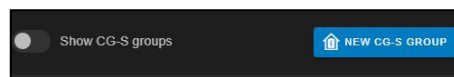


8.2.1 Erstellen neuer Gruppen und anlegen und autorisieren von ZB-S Systemen in VisionGuard

Bitte beachten Sie:

Es können beliebig viele CG-S-Gruppen mit jeweils bis zu 32 ZB-S-Systemen gebildet werden. Dies dient nur einer logischen Gruppenzuordnung, die in der späteren Visualisierungsdarstellung in der VisionGuard keine Bedeutung hat.

Um eine CG-S-Gruppe anzulegen, klicken Sie bitte auf die blaue Schaltfläche „NEUE CG-S GRUPPE“



Im nachfolgenden Fenster geben Sie bitte ein:

Gateway ID: 1
Gruppen ID: 1 bis 500, nach Wunsch
Typen: ZB-S
Name: Gewünschter Gruppenname mit max. 100 Zeichen

8.2.1 Erstellen neuer Gruppen und anlegen und autorisieren von ZB-S Systemen in VisionGuard

WICHTIGE ANMERKUNG!

Unter "Typen" sind weitere CG-S systeme wählbar. Diese sind in VisionGuard 3 noch nicht unterstützt! Klicken sie auf "Speichern" um die Einstellungen zu übernehmen.

Die neue CG-S Gruppe erscheint in der Liste.

Bitte wiederholen Sie die genannten Schritte um weitere CG-S Gruppen zu erstellen.

Um ZB-S Systeme zu einer Gruppe hinzuzufügen, führen Sie die folgenden Schritte aus.
Klicken Sie auf "NEUES CG-S SYSTEM"

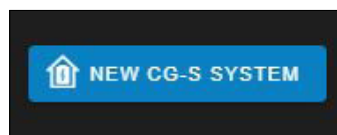
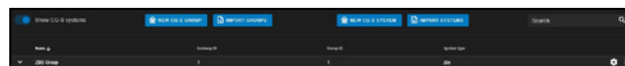
Im nachfolgenden Fenster geben Sie ein:

Gruppe: Wählen Sie die gewünschte CG-S Gruppe

Systemadresse: Systemadresse von ZB-S 1 bis 32

Neuron Id: Eingabe der Neuron ID aus dem ZB-S Steuergerät CU-CG-S mit 12 Zeichen

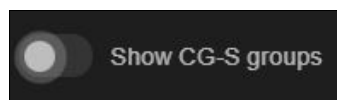
Name: Wird automatisch ausgefüllt, sobald die ZB-S in der VisionGuard autorisiert wird



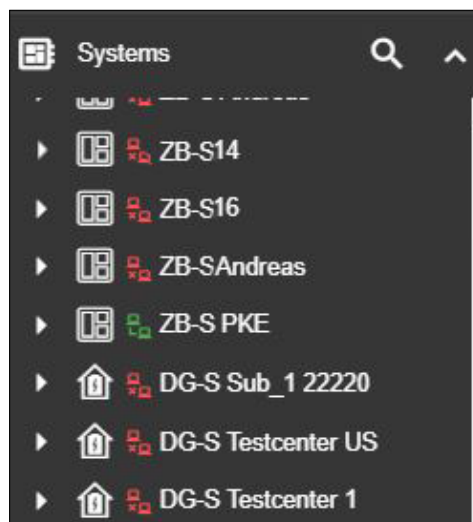
Klicken Sie auf "Speichern" um das ZB-S System in die VisionGuard zu übernehmen.

Bitte verfahren Sie genauso mit weiteren ZB-S Systemen die Sie in die VisionGuard integrieren möchten. Alle ZB-S Systeme erscheinen dann in einer Liste.

Über „Zeige CG-S Gruppen“ oder „Zeige CG-S Systeme“ kann die Listenansicht umgeschaltet werden.



Nach dem Prozess sind die ZB-S Systeme nun sichtbar und steuerbar im „System“ Menü-Baum.



9 Grafischer Aufbau und Struktur der VisionGuard

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!

9 Grafischer Aufbau und Struktur der VisionGuard

9.1 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

HINWEIS:

Es ist möglich, das Hintergrundbild durch ein eigenes Bild zu ersetzen.

Der Ordner für das Hintergrundbild ist: C:\Program Files\EATON\Visionguard\Proxy\html\img\app-signin-background.jpg

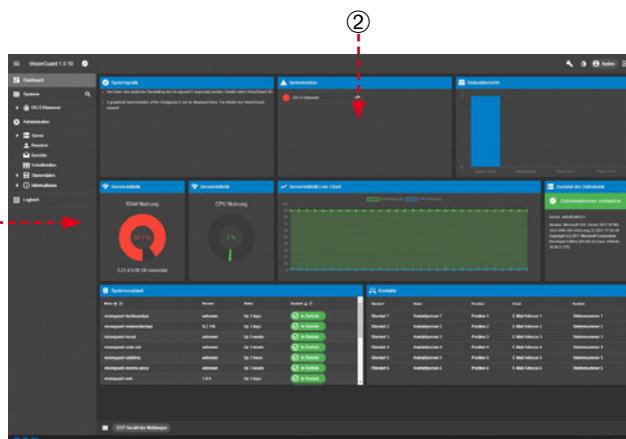
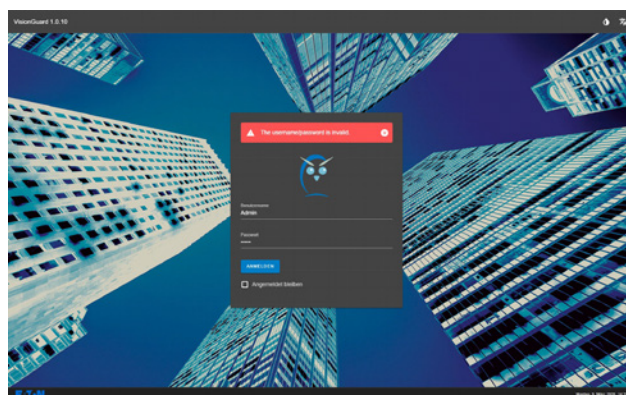
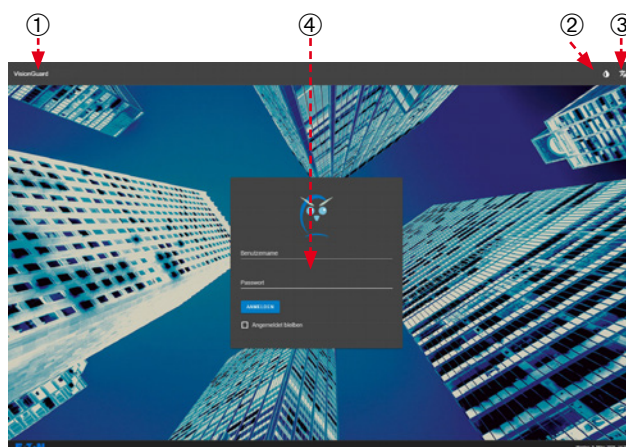
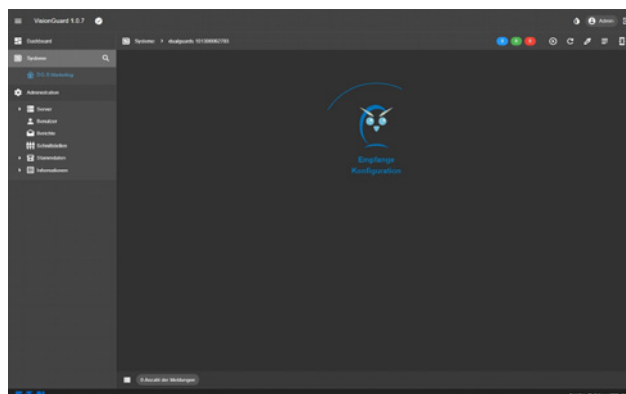
Es kann durch ein neues .jpg mit einer Größe von 1920x1080 Pixel ersetzt werden.

Es wird empfohlen, das Originalbild zuerst umzubenennen.

9.2 Dashboard

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

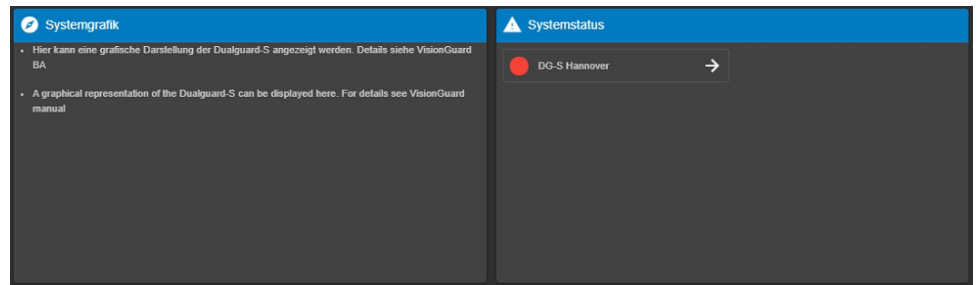
- ① Navigationsbereich zum direkten navigieren in die Untermenüs der VisionGuard
- ② Dashboard Widgets – Das Dashboard (Armaturenbrett) besteht aus acht festgelegten Widgets



9.2.1 Systemgrafik und Systemstatus

Das Widget Systemstatus zeigt alle angeschlossenen und angemeldeten DualGuard-S Systeme übersichtlich in einem Widget an. Je DualGuard wird der Anlagenname mit einem farbigen Status angezeigt (Grün= Kommunikation OK, Rot = Kommunikationsstörung). Über den Pfeil rechts vom Anlagenname navigiert man direkt in die Anlagenübersicht.

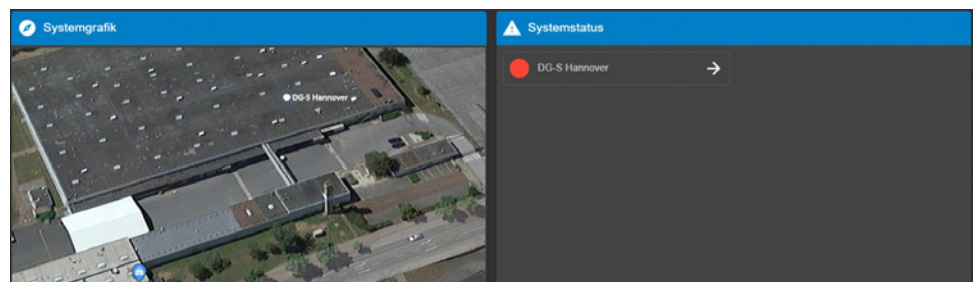
Im Widget Systemgrafik kann man auf einfache Weise die Anlagen in einer Grafik darstellen, um z.B. den Standort anzuzeigen



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:

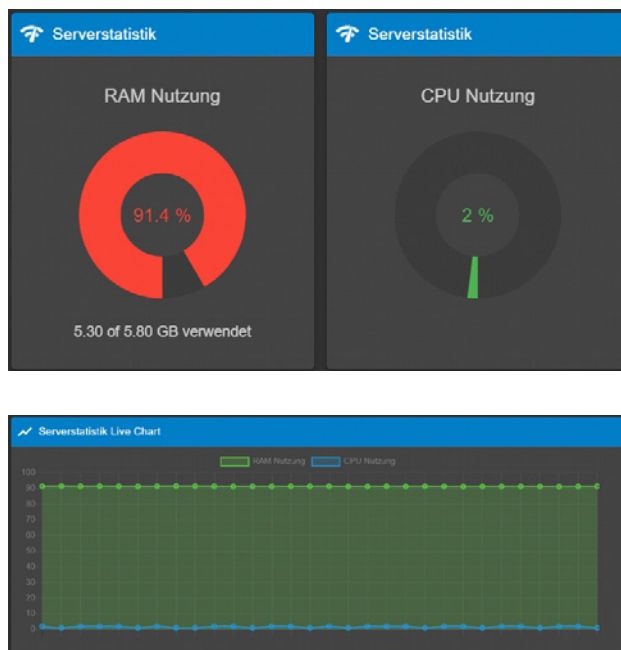


Dieses Bild kann nun als .jpg mit dem Namen „widget-image-jpg-01.jpg“ im Verzeichnis `C:\Program Files\EATON\Visionguard\Proxy\html\img\widgets` kopiert werden. Mit Strg+F5 wird die Seite neu geladen, und die Systemgrafik erscheint im Widget:



9.2.2 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.



9.2.3 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).

Zustand der Datenbank		Systemzustand			
Datenbankserver verbunden		Name ↑ 2	Version	Status	Zustand ↓ 1
Server: defa5a9b2c3		visionguard-dashboardapi	unknown	Up 3 days	In Betrieb
Version: Microsoft SQL Server 2017 (RTM) - 14.0.1000.169 (X64) Aug 22 2017 17:04:49 Copyright (C) 2017 Microsoft Corporation Developer Edition (64-bit) on Linux (Ubuntu 16.04.3 LTS)		visionguard-moduleclientapi	0.2.116	Up 3 days	In Betrieb
		visionguard-mssql	unknown	Up 5 weeks	In Betrieb
		visionguard-node-red	unknown	Up 3 weeks	In Betrieb
		visionguard-rabbitmq	unknown	Up 21 hours	In Betrieb
		visionguard-reverse-proxy	unknown	Up 3 weeks	In Betrieb
		visionguard-web	1.0.9	Up 3 days	In Betrieb

9.2.4 Kontakte

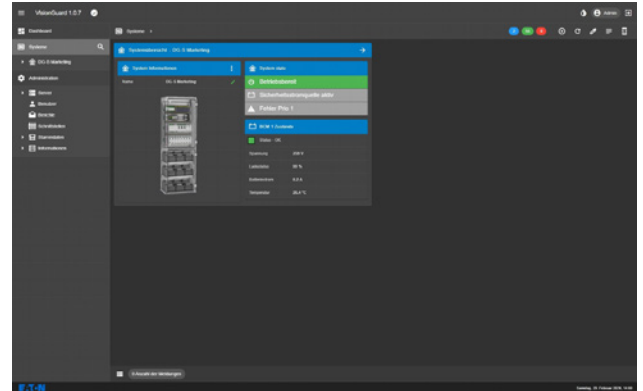
Im Widget Kontakte können Kontaktpersonen mit ihren Kontaktdaten angelegt werden, z.B. die bei speziellen Ereignissen zu informieren sind. Die Editierfunktion kann über das Schraubenschlüsselsymbol oben rechts aktiviert werden, um Kontaktdaten anzulegen oder zu ändern.

Standort	Name	Position	Email	Kontakt
Standort 1	Kontaktperson 1	Position 1	E-Mail Adresse 1	Telefonnummer 1
Standort 2	Kontaktperson 2	Position 2	E-Mail Adresse 2	Telefonnummer 2
Standort 3	Kontaktperson 3	Position 3	E-Mail Adresse 3	Telefonnummer 3
Standort 4	Kontaktperson 4	Position 4	E-Mail Adresse 4	Telefonnummer 4
Standort 5	Kontaktperson 5	Position 5	E-Mail Adresse 5	Telefonnummer 5
Standort 6	Kontaktperson 6	Position 6	E-Mail Adresse 6	Telefonnummer 6

9.3 Systemübersicht

Im Menü „Systeme“ erscheint eine Systemübersicht mit Widgets aller installierten DualGuard-S oder ZB-S Systeme. 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).

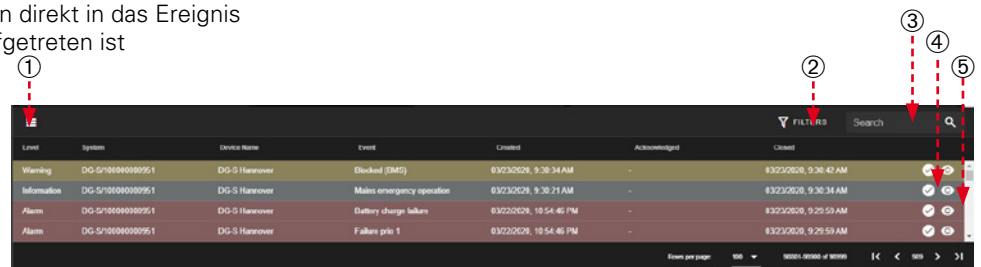
- ① Über den Pfeil gelangt man in die Detailansicht der DualGuard (siehe separates Kapitel)



9.4 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.

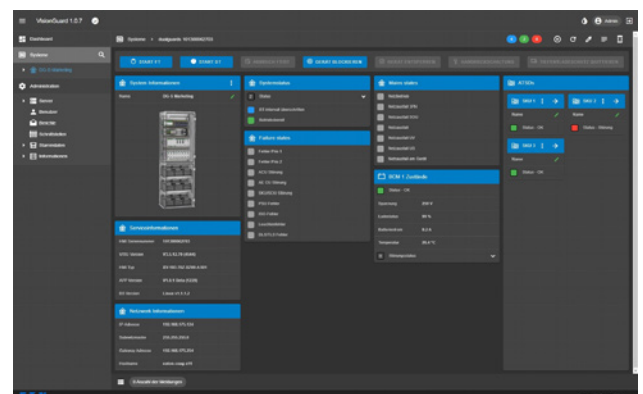
- ① Alarmliste EIN/AUS Anzeige
- ② Filter zum gezielten filtern nach Kategorien, Systemen oder Ereignissen
- ③ Suchfunktion zum gezielten suchen von Ereignissen
- ④ Hierüber kann das Ereignis bestätigt werden, so dass es aus der Alarmliste entfernt wird. Über den Schieberegler „bestätigt“ können die bestätigten Ereignisse eingeblendet werden
- ⑤ Über das Augensymbol kann direkt in das Ereignis navigiert werden, wo es aufgetreten ist



10 DualGuard-S Visualisierung

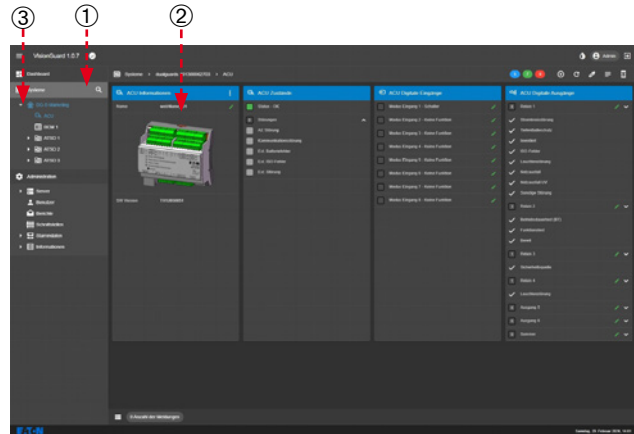
10.1 DualGuard-S Detailansicht

Unter dem Menü „Systeme“ werden alle DualGuard-S/ ZB-S Systeme mit ihren Gerätenamen in Explorerstruktur aufgelistet ①. Mit Klick auf den Namen erscheint die Detailansicht der Dualguard-S. Hier bekommt man detaillierte 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.



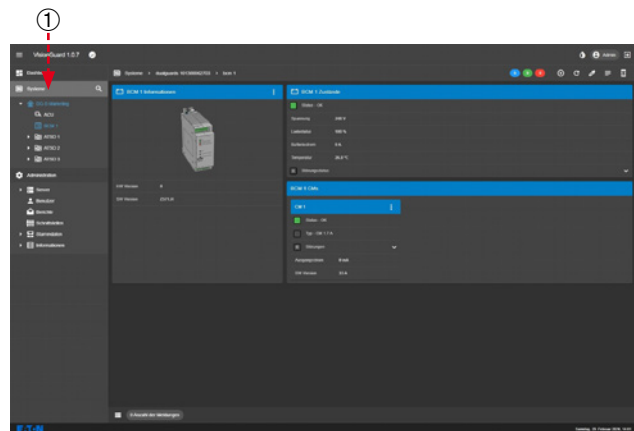
10.2 ACU Detailansicht

- 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.



10.3 BCM Detailansicht

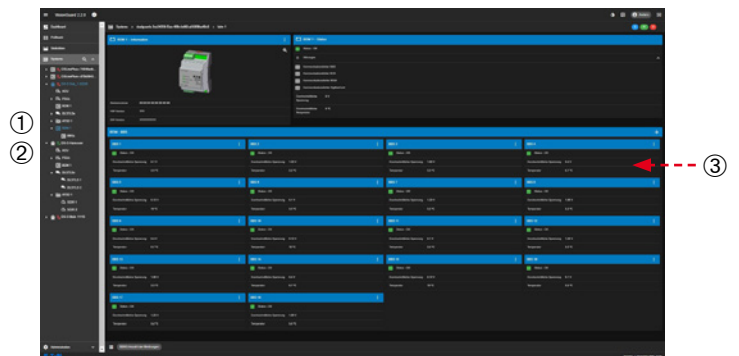
In der BCM Detailansicht wird die installierte Ladetechnik, bestehend aus BCM (Battery Control Module) und CM (Charger Module) Ladeteilen, angezeigt. Im BCM Widgets werden die Batteriewerte wie Spannung in Volt, Ladestatus in %, Lade-/Entladestrom in Ampere, und die Batterieraumtemperatur in C° angezeigt. 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.



10.4 BDM Detailansicht

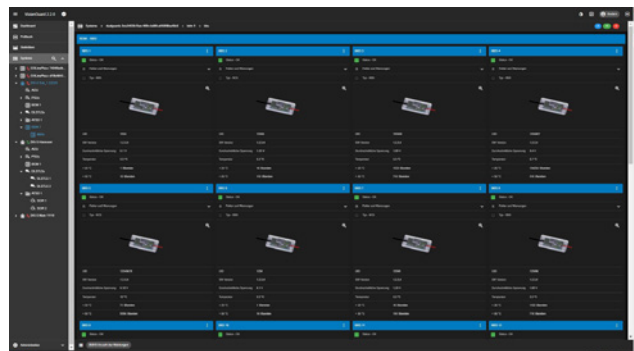
Wenn die optional erhältliche Batterieblocküberwachung installiert und am HMI angemeldet ist, erscheint im Systembaum automatisch der Menüpunkt „BDM“. ①

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.



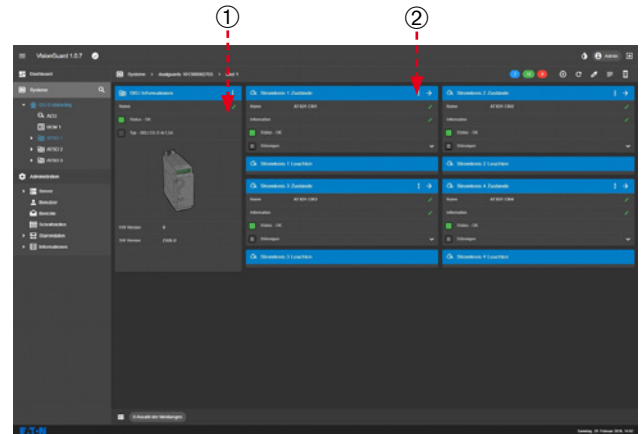
10.4.1 BBS Detailansicht

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



10.5 ATSD Detailansicht (SKU)

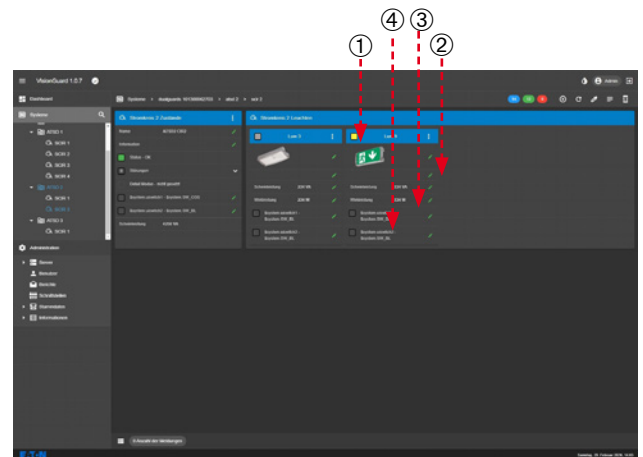
Die ATSD-Detailansicht zeigt die SKU-Typen und die Namen, zusätzliche Informationen und den Gesamtstatus jedes Stromkreises an. Die Texte und die Zusatzinformationen können durch Klicken auf das grüne Stift-Symbol ① bearbeitet werden. In diesem Fall empfiehlt es sich, Zielortbezeichnungen einzugeben, 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.



10.6 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 Kreuz (GuideLed DX). IA und Matrix werden z.Zt. nicht genutzt.
- ③ Im Infocfeld „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



10.7 Konfiguration einer DualGuard-S

10.7 Konfiguration einer DualGuard-S

Um ein DualGuard-S System zu konfigurieren muss der Benutzer Administrator oder Supervisor Rechte besitzen! Die gesamte Konfiguration des DualGuard-S Systems ist nur im Administrator-Bereich im Menü "DualGuard-S" möglich.

Ein Klick auf das Zahnrad Symbol (1) beim gewünschten DualGuard-S System öffnet das Konfigurationsmenü.

Im oberen linken Teil des Fensters können Sie nun das gewünschte Konfigurationslevel wählen:

- System
- ACU
- SKU (ATSD), Stromkreise and Leuchten

10.7.1 Systemkonfiguration

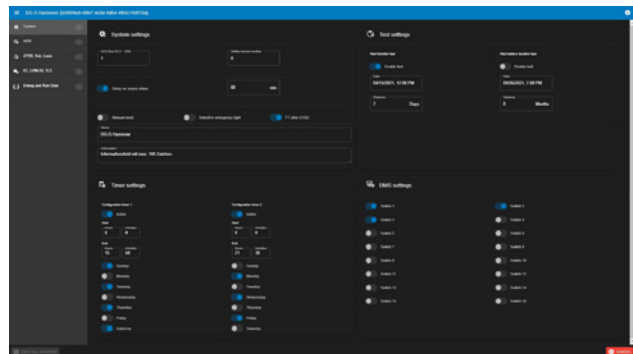
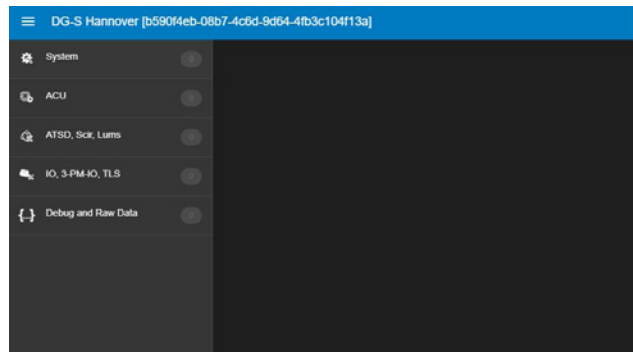
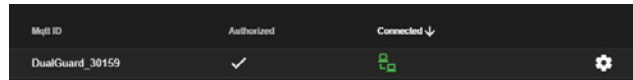
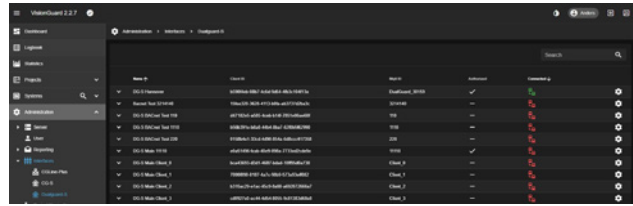
In der Systemkonfiguration können alle grundlegenden HMI-Einstellungen gemacht werden, wie:

- Name und Informationstext der DG-S
- nächster automatischer FT oder BT
- Verzug der Netzwiederkehr in Minuten
- Manueller Reset
- Selektives Notlicht, etc.

Für tiefergehende Details zu HMI-Grundeinstellungen schauen Sie in die DG-S Bedienungsanleitung.

Jede Änderung der Konfiguration wird durch einen Zähler aufgezeichnet, z.B. 6.

Wenn alle gewünschten Konfigurationen durchgeführt wurden, müssen Sie über „Alle Änderungen speichern“ gesichert werden. Die Änderungen werden nun zum HMI der DG-S übermittelt.



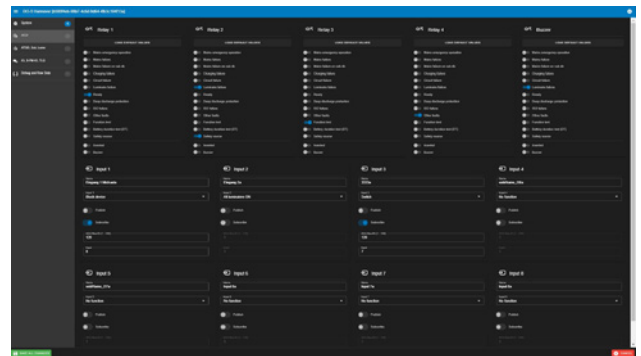
10.7.2 ACU Konfiguration

In der ACU Konfiguration können alle ACU Einstellungen durchgeführt werden, wie:

- Digitale Eingänge
- Relais-Ausgänge
- Summer

Mit "Standardwerte laden" können die Standardeinstellungen für die Relais gesetzt werden.

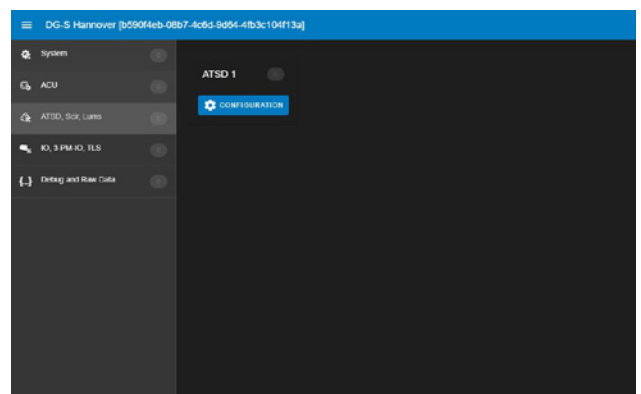
Die Digitaleingänge der ACU können zu anderen ACUs von anderen DG-S Systemen "published" und "abonniert" (subscribed) werden, um eine anlagenübergreifende Funktion zu anderen DualGuard-S Systemen zu gewährleisten. Für weitere Details zu den ACU Einstellungen schauen sie in die DG-S Bedienungsanleitung.



10.7.3 SKU (ATSD) Konfiguration

In der SKU Konfiguration werden alle installierten SKUs (ATSD) in einer Übersicht angezeigt.

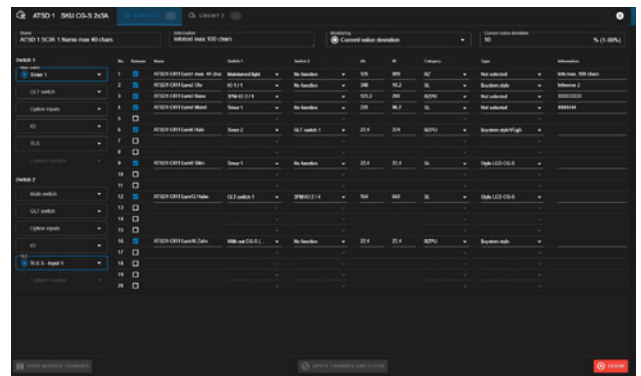
Über "Konfiguration" der gewünschten SKU (ATSD) 1 bis 40 werden die Stromkreiseinstellungen angezeigt.



Im oben gezeigten Teil (1) kann der gewünschte Stromkreis gewählt werden.

In diesem Konfigurationsmenü können wie gewohnt alle gewünschten Einstellungen bis zur Leuchtenebene vorgenommen werden, wie:

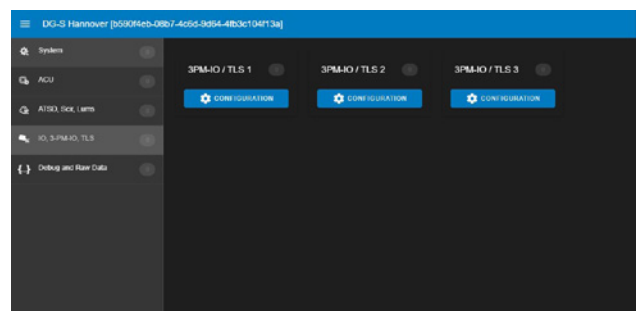
- Überwachungsmodus, z.B. CG Überwachung
- Informationstext der Stromkreise oder Leuchten
- Schalterbelegung der Stromkreise oder Leuchten
- Leuchtenkategorie
- Last der Leuchten in VA oder W



10.7.4 I/O, 3-PM-IO, TLS Konfiguration

In der I/O, 3-PM-IO, TLS Konfiguration werden alle installierten I/O, 3-PM-IO und TLS Module angezeigt.

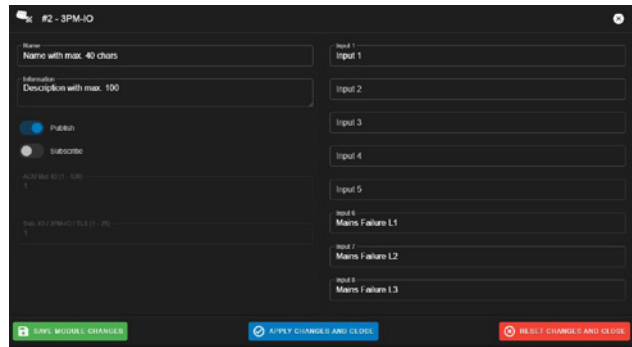
Über klicken auf "Konfiguration" beim gewünschten Modul 1 bis 25 erscheint das nächste Fenster der I/O, 3-PM-IO und TLS Konfiguration.



11 ZB-S Visualisierung

In diesem Konfigurationsmenü können alle gewünschten Einstellungen zu den I/O, 3-PM-IO und TLS Modulen vorgenommen werden, wie:

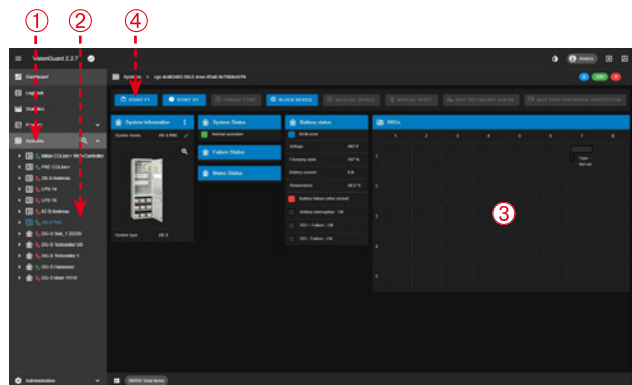
- Name und Informationstext des Moduls
- Name/Text jeden Eingangs
- Last der Leuchten in VA or W



11 ZB-S Visualisierung

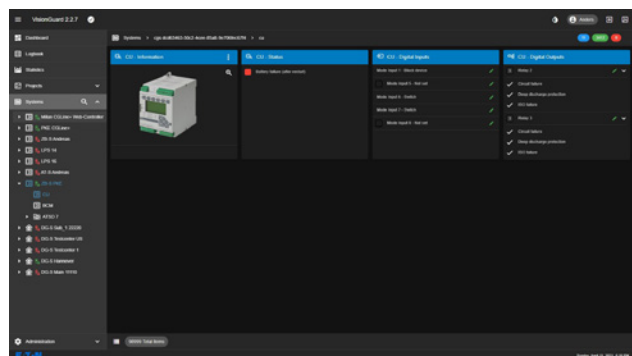
11.1 ZB-S Detailansicht

Unter dem Menü „Systeme“ sind alle Dualguard-S/ZB-S-Systeme mit ihren Gerätenamen in der Explorer-Struktur aufgelistet (1). Klicken Sie auf den Namen (2), um die Detailansicht der ZB-S zu sehen. Hier erhalten Sie detaillierte Statusinformationen über das System, Serviceinformationen wie z. B. eine Übersicht über die Systeminformation, System/Fehler und den Netzstatus. Es werden nur Datenpunkte mit Farben angezeigt, wenn diese aktiv sind. Dies ermöglicht eine übersichtliche Darstellung der Statusanzeigen. Ein Widget zeigt installierte SKUs (3) entsprechend der Montage auf den Backplanes im Schrankinneren mit dem Summenstatus an. Bei Klick auf eine SKU erscheint das SKU-Bild mit detaillierten Informationen zu den Stromkreisen. Zusätzlich können mit den blauen Steuertasten verschiedene Aktionen an der ZB-S aktiviert werden, wie z. B. das Starten eines Funktionstests (Start FT) (4).



11.2 CU Detailansicht

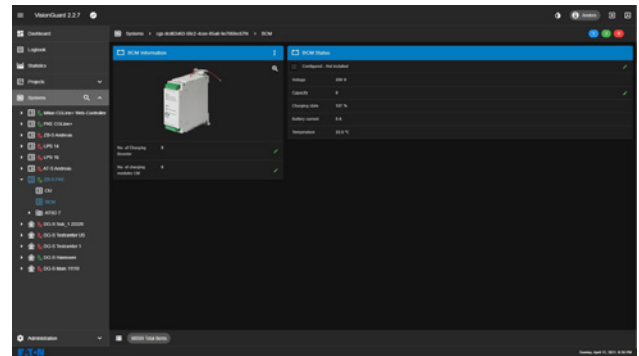
Die CU Detailansicht zeigt den CU-Status, die digitalen Eingangskonfigurationen der CU und die Relaisausgänge der CU. Es ist nicht möglich, die digitalen Eingänge und Relais in VisionGuard zu konfigurieren. Diese Konfigurationen müssen über die ZB-S PC-Software vorgenommen werden.



11.3 BCM Detailsicht

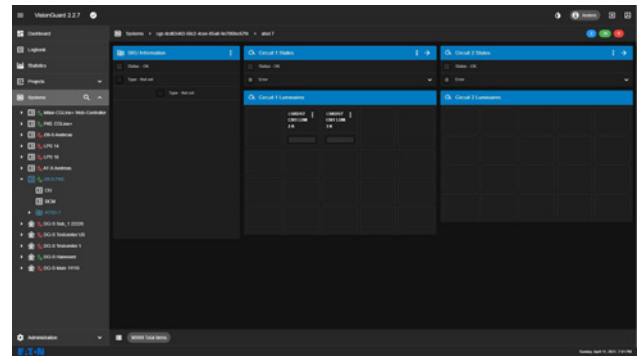
Die BCM-Detailsicht zeigt die installierte Ladetechnik, bestehend aus den Ladeteilen BCM (Batteriekontrollmodul) und CM (Lademodul).

Die BCM-Widgets zeigen die Batteriewerte wie Spannung in Volt, Ladezustand in %, Lade-/Entladestrom in Ampere und die Umgebungstemperatur der Batterie in °C an. Das CM-Widget zeigt den Gesamtstatus OK oder Fehler an, im Fehlerfall wird die Fehleranzeige erweitert, die dann den genauen Fehler anzeigt.



11.4 SKU Detailsicht

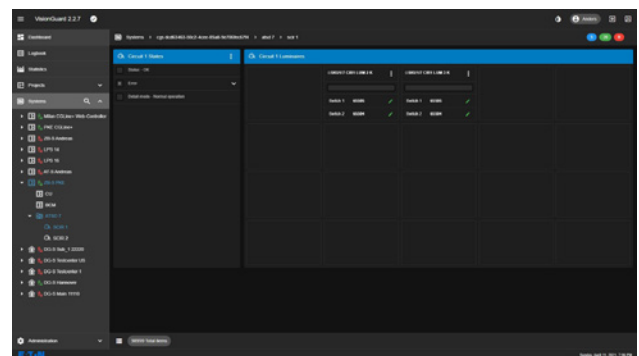
In der SKU Detailsicht werden die SKU-Typen sowie die Bezeichnungen, Zusatzinformationen und der Gesamtstatus jedes Stromkreises entsprechend der Backplane-Besetzung im ZB-S-Schrank angezeigt. Im Falle eines Stromkreisfehlers erscheint hier auch die Fehleranzeige rot, die dann den genauen Stromkreisfehler anzeigt. Klicken Sie auf den Pfeil in der blauen Kopfzeile des Stromkreises, um die Detailsicht der Leuchten des Stromkreises zu öffnen.



11.5 Leuchten Detailsicht

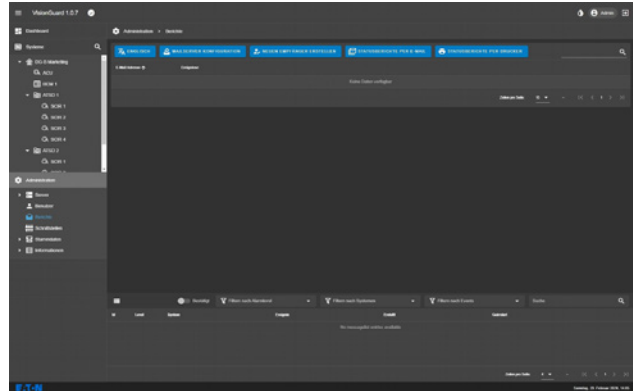
In der Leuchten Detailsicht werden die Status- und Informationstexte des Stromkreises angezeigt. Im Falle eines Stromkreisfehlers wird zusätzlich die Fehleranzeige geöffnet, die dann den genauen Stromkreisfehler anzeigt, z. B. AC-Sicherungsfehler.

Der Status der Leuchte wird in der Kopfzeile des Leuchten-Widgets angezeigt. Grau = aus, gelb = an, rot = Fehler/Defekt



12 E-Mail-, Druck- und Exportfunktion

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



12.1 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.



12.1.1 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.

Mailserver Konfiguration

E-Mail Adresse

Smtp Host Port ☐ Verschlüsselt

☐ Authentifizierung deaktivieren

Benutzername

Passwort

SPEICHERN **LÖSCHEN** **ABBRECHEN**

12.1.2 E-Mail Empfänger erstellen

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

Es öffnet sich folgendes Konfigurationsfenster



Neuen Empfänger erstellen

E-Mail Adresse
MaxMustermann@muster.de

Ereignisse

SPEICHERN **ABBRECHEN**

Oben muss eine gültige E-Mail-Adresse des Empfängers eingegeben 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 Häkchen aktiviert werden. Bei Auftreten des Ereignisses wird entsprechend eine Alarm E-Mail verschickt.

Neuen Empfänger erstellen

E-Mail Adresse
MaxMustermann@muster.de

Ereignisse

- ☐ ISO-Fehler
- ☐ DLS/TLS Fehler
- ☐ BCM Fehler
- ☒ Netzausfall am Gerät
- ☒ Statusbericht
- ☐ Batterieladefehler

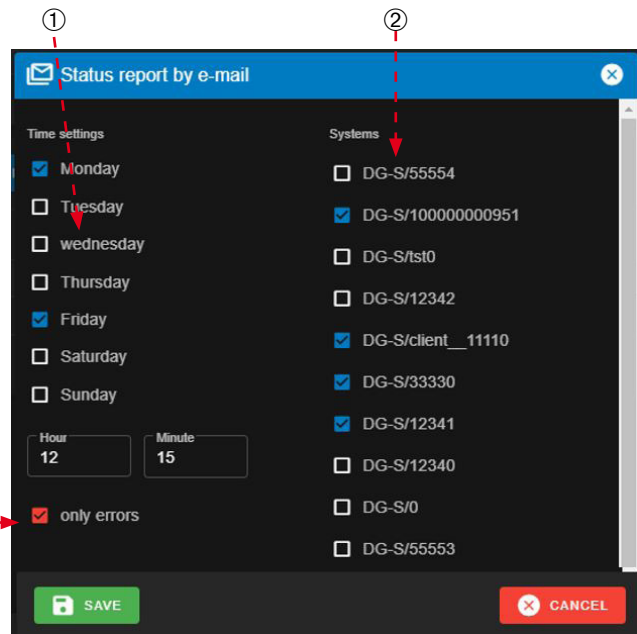
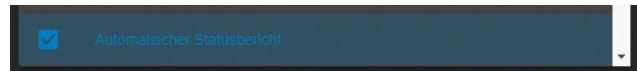
12.1.3 Automatische Status E-Mail

12.1.3 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

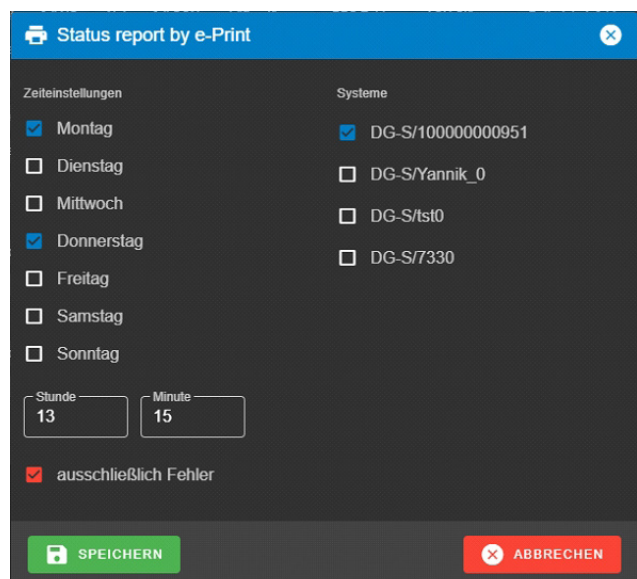
- ① Hier können die Wochentage und die Uhrzeit eingestellt werden, wann die Statusmail versendet werden soll.
- ② Hier können alle DualGuard-S Systeme ausgewählt werden, deren Status in der Mail angezeigt werden sollen
- ③ Wird „ausschließlich Fehler“ aktiviert, werden in der E-Mail nur Fehler angezeigt. 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!



12.2 Druckfunktion

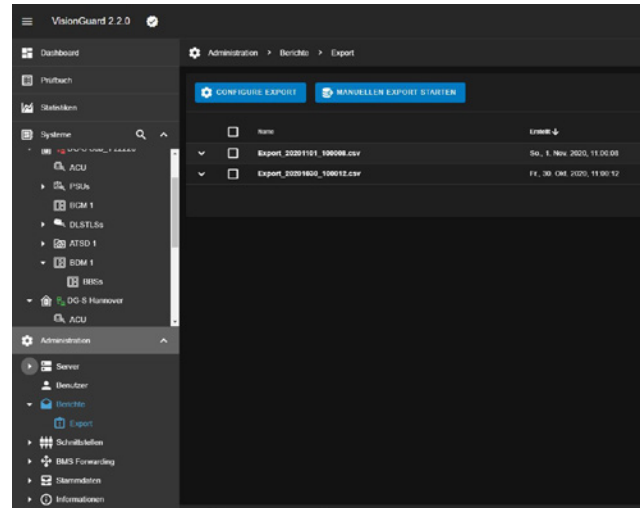
Die VisionGuard verfügt über eine automatische Druckfunktion die über die Schaltfläche „Statusberichte per Drucker“ aktiviert werden kann.

Im folgenden Konfigurationsfenster können wie bei den Statusberichten per Mail die gleichen Einstellungen vorgenommen werden.



12.3 Exportfunktion

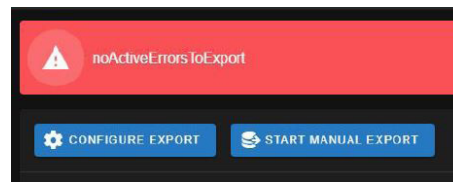
Die Funktion „Configure Export“ im Menü „Manuellen Export Starten“ ermöglicht es, alle aufgetretenen Störungen der DualGuard-S-Systeme in eine Excel-basierte .csv-Datei zu exportieren, z.B. zur Weiterverarbeitung durch externe Anwendungen.



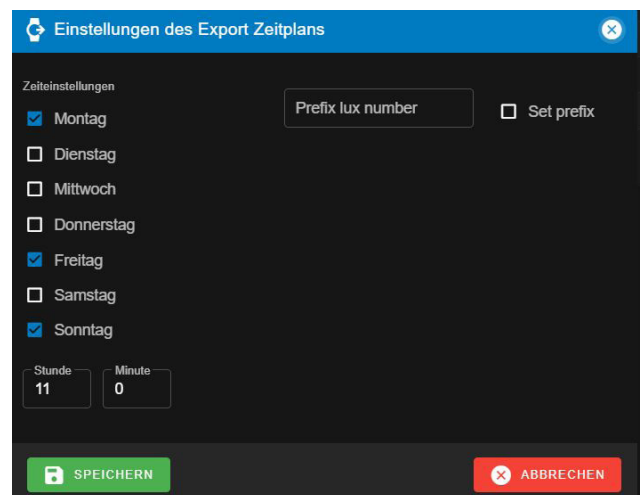
Wenn das Menü Export gewählt wird, erscheint ein schwarzer Bildschirm mit zwei Schaltflächen „Export konfigurieren“ und „Manuellen Export starten“.

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 Exportdatei 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:

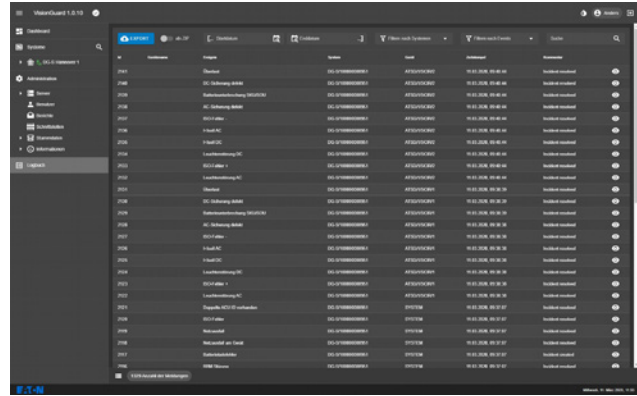
```
LogId,EventId,System,SystemName,Name,Level,Device,Label,StateType,Created,PersonalComment
114570,57351,DG-5/201300062703,DG-5 Marketing,avState1.mof,Information,SYSTEM,System.mof,Closed,04/06/2020 11:37:06,
114569,57352,DG-5/201300062703,DG-5 Marketing,avState1.mof,Information,SYSTEM,System.mof,Opened,04/06/2020 11:33:46,
114568,57350,DG-5/201300062703,DG-5 Marketing,avDetailError.switchOfBatteryModeAccordingUnderVoltage,Information,ATSD/1/SCIR/1,System.switchOfBatteryModeAccordingUnderVoltage,Opened,04/06/2020 11:33:04,
114567,57349,DG-5/201300062703,DG-5 Marketing,avState4.errMainExtAtsd,Information,SYSTEM,System.errMainExtAtsd,Opened,04/06/2020 11:33:03,
114566,57348,DG-5/201300062703,DG-5 Marketing,avState4.btTestAllowed,Information,SYSTEM,System.btTestAllowed,Opened,04/06/2020 11:33:03,
114565,57347,DG-5/201300062703,DG-5 Marketing,avState4.errSum,Information,SYSTEM,System.errSum,Opened,04/06/2020 11:33:03,
114564,57346,DG-5/201300062703,DG-5 Marketing,avState4.errAe,Information,SYSTEM,System.errAe,Opened,04/06/2020 11:33:03,
114563,57345,DG-5/201300062703,DG-5 Marketing,avState4.errDlts,Information,SYSTEM,System.errDlts,Opened,04/06/2020 11:33:03,
114562,57344,DG-5/201300062703,DG-5 Marketing,avState4.errMainSubstation,Information,SYSTEM,System.errMainSubstation,Opened,04/06/2020 11:33:03,
114561,57343,DG-5/201300062703,DG-5 Marketing,avState4.errFan,Information,SYSTEM,System.errFan,Opened,04/06/2020 11:33:03,
114560,57342,DG-5/201300062703,DG-5 Marketing,avState3.errBcm,Information,SYSTEM,System.errBcm,Opened,04/06/2020 11:33:03,
114559,57341,DG-5/201300062703,DG-5 Marketing,avState3.errCm,Information,SYSTEM,System.errCm,Opened,04/06/2020 11:33:03,
114558,57340,DG-5/201300062703,DG-5 Marketing,avState3.errAcu,Information,SYSTEM,System.errAcu,Opened,04/06/2020 11:33:03,
114557,57339,DG-5/201300062703,DG-5 Marketing,avState3.errSum,Information,SYSTEM,System.errSum,Opened,04/06/2020 11:33:03,
114556,57338,DG-5/201300062703,DG-5 Marketing,avState3.errPtu,Information,SYSTEM,System.errPtu,Opened,04/06/2020 11:33:03,
114555,57337,DG-5/201300062703,DG-5 Marketing,avState3.errBbs,Information,SYSTEM,System.errBbs,Opened,04/06/2020 11:33:03,
```


13 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

14 History menu

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 Temperaturschwankungen der Batterieumgebung zu erkennen.

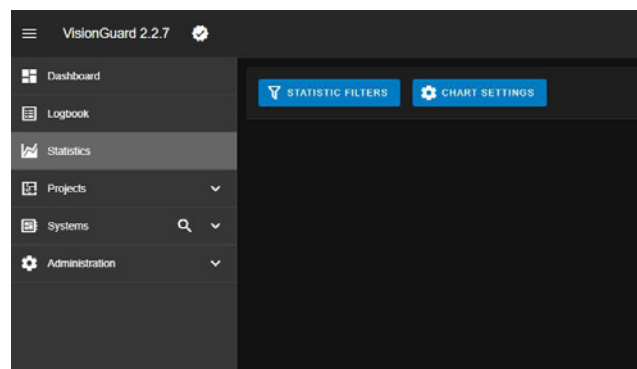
WICHTIGER HINWEIS:

Es wird empfohlen, nur sinnvolle Einstellungen zu verwenden.

Es ist möglich, Bereiche oder Zeiten einzustellen, die möglicherweise keine günstigen Verläufe über die Zeit darstellen. So ergibt es z. B. weniger Sinn, einen Test mit einer Dauer von einer Stunde über einen Zeitraum von einem Monat auszuwerten. Auch sehr kurze Intervalle, z. B. die Stromkurve über zehn Minuten, zeigen die hohe Taktung der Ladetechnik, die fehlinterpretiert werden könnte.

Wenn das Menü Statistik gewählt wird, erscheint ein schwarzer Bildschirm mit zwei Schaltflächen „Statistikfilter“ und „Diagramm 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%

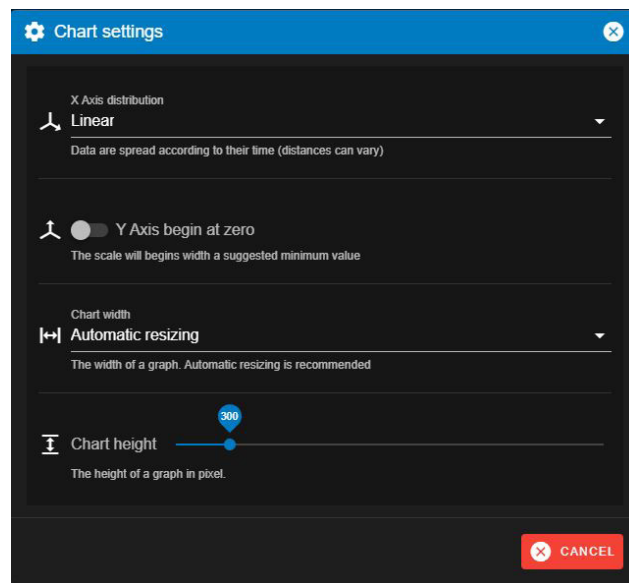
Mittel 50%

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 „Statistikfilter“ erzeugt werden. Es öffnet sich ein Fenster „Filter“:

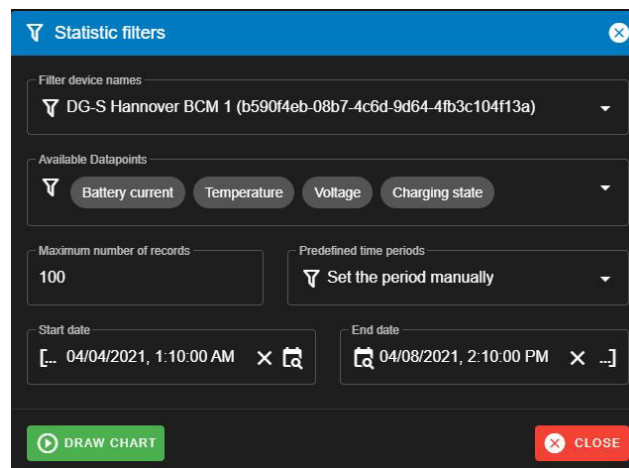
Über „Filter nach Gerätenamen“ kann das gewünschte DualGuard-S / ZB-S System ausgewählt werden.

Über „Verfügbare Datenpunkte“ können die gewünschten Batterie-Analogwerte „Spannung“, „Batteriestrom“, „Temperatur“ und „Ladestatus“ ausgewählt werden.

Über „vordefinierte Zeiträume“ kann der gewünschte Zeitraum für die Grafiken eingestellt werden.

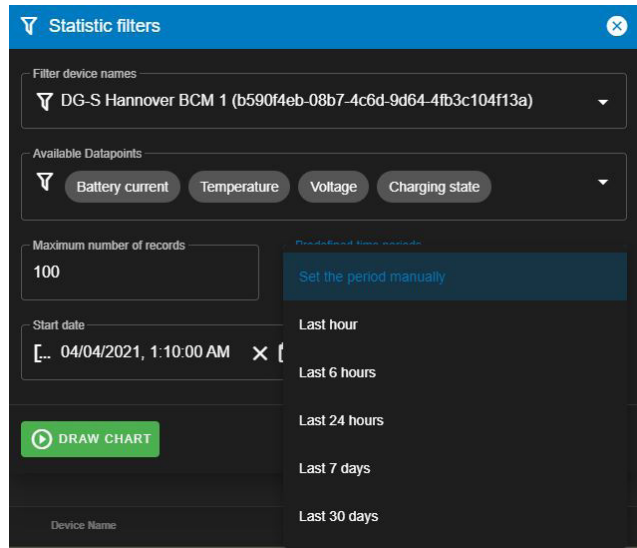
Es können entweder feste Zeitbereiche eingestellt werden, oder es kann über „Zeitraum manuell einstellen“ ein Start- und Enddatum/-zeitpunkt festgelegt werden.

Das Beispiel zeigt einen Zeitraum vom 04. April 2021, 01:10 Uhr bis zum 08. April 2021, 14:10 Uhr.



15 Speichern und Wiederherstellen

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:

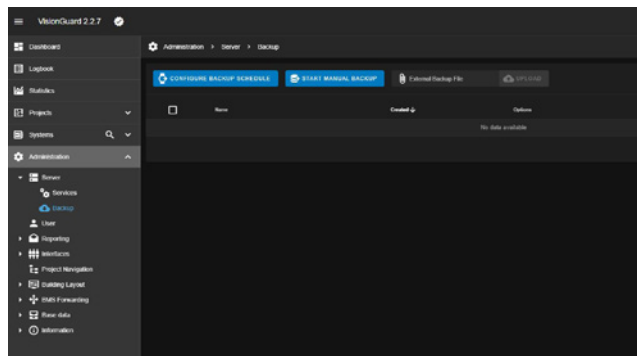


15 Speichern und Wiederherstellen

Die VisionGuard bietet ein Speicher- und Wiederherstellungsmenü an, unter Administration > Server > Backup. Es ermöglicht die einfache Erstellung eines Backups und die Wiederherstellung der gesamten Konfiguration, z. B. im Falle eines Systemabsturzes oder beim Umzug in eine neue PC-Umgebung.

Bitte beachten Sie:

Ein manuelles Backup ist nur mit lokalem Zugriff auf den VisionGuard möglich, oder mit einem Zugriff über eine Remote-Software!



15.1 Erstellung automatischer Backups

Über die Schaltfläche „Backup-Zeitplan konfigurieren“ ist es möglich automatische Backups zu erstellen. Unter Zeiteinstellungen können die Wochentage und die Uhrzeit ausgewählt werden. Unter Datenbanken kann der Dienst für das Backup ausgewählt werden. Bitte aktivieren Sie alle Punkte für ein vollständiges Backup.

15.2 Erstellung manueller Backups

Über die Schaltfläche „Manuelles Backup starten“ ist es möglich, sofort ein Backup zu erstellen. Bitte vergeben Sie einen Namen für das Backup und ggf. eine Beschreibung. Unter Datenbanken kann der Dienst für das Backup ausgewählt werden. Aktivieren Sie bitte alle Punkte für ein vollständiges Backup. Mit „Übernehmen und starten“ wird der Download gestartet und erzeugt einen Eintrag in der Backup-Liste.

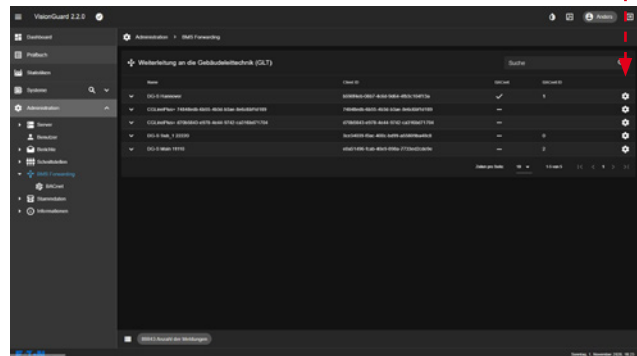
15.3 Manuelle Wiederherstellung

Über die Schaltfläche „Hochladen“ ist es möglich die VisionGuard mit einer zuvor erstellten Backup-Datei wiederherzustellen. Klicken Sie auf „Upload“, wählen Sie die gewünschte Backup-Datei aus und drücken Sie OK.

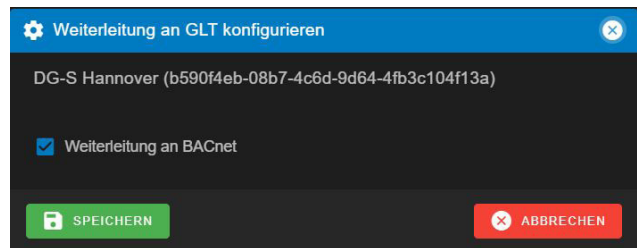
Nach einigen Minuten ist das System in der gewünschten Konfiguration wiederhergestellt.

16 BACnet/IP Interface für DualGuard-S

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

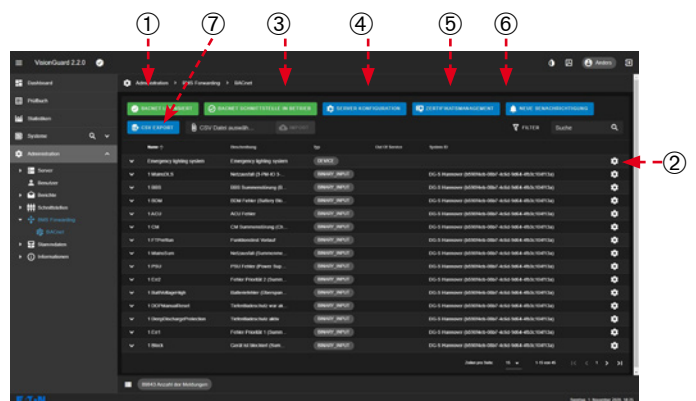


Dies kann über das Zahnradsymbol ① konfiguriert werden. Es öffnet sich das folgende Fenster. Mit einem Häkchen „Weiterleitung an BACnet“ kann die BACnet-Schnittstelle für diese DualGuard-S aktiviert werden. Mit „Speichern“ wird die Einstellung gespeichert.



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.

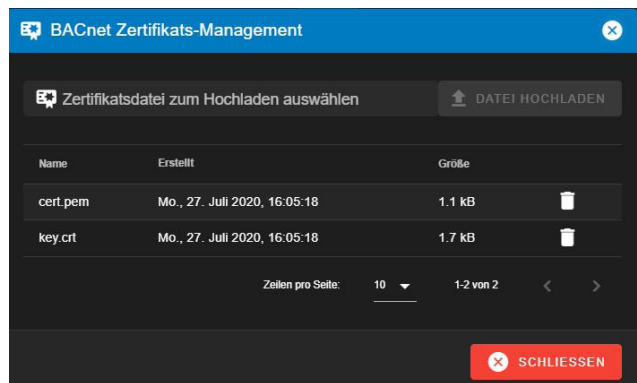
BACnet-Server-Konfiguration

Siehe Abbildung „BACnet-Weiterleitung“ (3).

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

16 BACnet/IP Interface für DualGuard-S

Die „Instanznummer“ ist wichtig für die eindeutige Identifizierung des DualGuard-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.

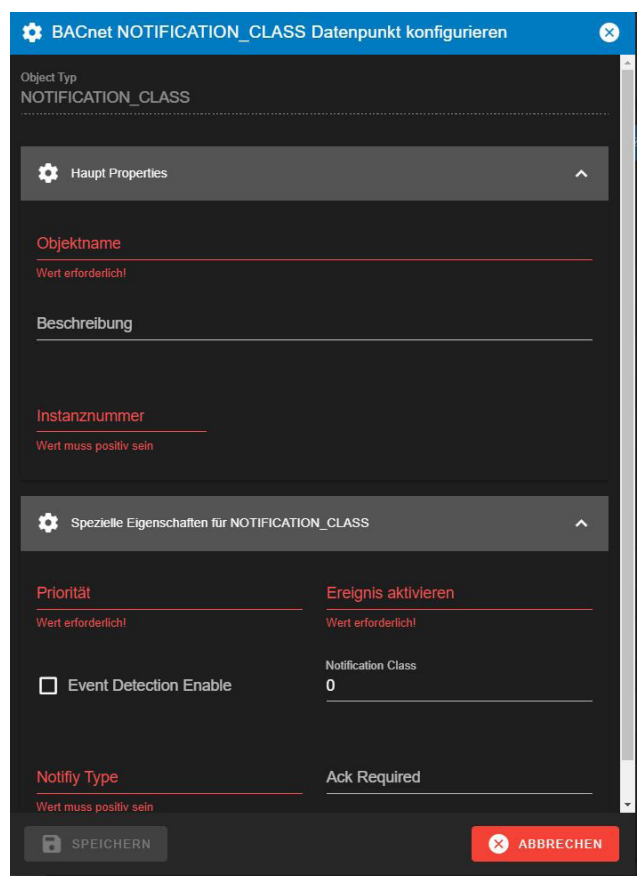


Falls für die BMS-Benachrichtigungsklassifizierung erforderlich, können diese im Menü „NEUE BENACHRICHTIGUNG“ konfiguriert werden. Siehe Abbildung BACnet-Weiterleitung (3). In diesem Konfigurationsmenü können die Einstellungen für den BACnet-Server vorgenommen werden:

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“.



17 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 17.1 Dienste)

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

Berichte (siehe Kapitel 12 – E-Mail- und Druckfunktion)

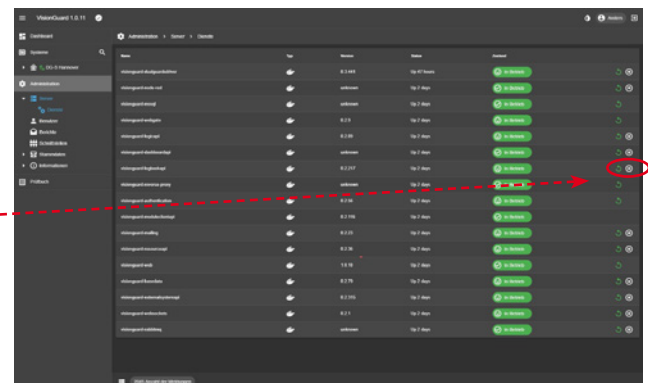
Schnittstellen (siehe Kapitel 7 – Anlegen von Dualguard-Systemen in der VisionGuard

Stammdaten – hier keine Änderungen vornehmen!

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

17.1 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.de/ceag**.

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.eaton.de/ceag Juli 2021

© 2021 Eaton
Alle Rechte vorbehalten
Printed in Germany
Bestell-Nr. 40071860370 (B)
Publikations-Nr. MN451069DE
Juli 2021

Eaton ist ein eingetragenes
Warenzeichen.

Alle anderen Warenzeichen sind
Eigentum Ihrer jeweiligen Inhaber.