Operating Instructions Eaton VisionGuard

Target Audience Part 1: Qualified electricians in accordance with
EN 50110-1 and electrically instructed persons

Powering Business Worldwide

Table of Contents

1.Foreword and system requirements

1.1 Foreword

VisionGuard is a modern web-based monitoring, control and configuration software for the new DualGuard-S (DG-S) / LoadStar-S (LS-S), ZB-S, LP-STAR emergency lighting systems and CGLine+ self-contained systems and monitoring and control software for AT-S+ emergency lighting systems

Important note for the use of CG-S bus-based emergency lighting systems ZB-S, AT-S+ and LP-STAR:

To connect these systems to VisionGuard, the CG-S Gateway software must be installed. For the operation of the gateway with the emergency lighting systems, a CG-S interface is required (as with the predecessor software CGVision). This can be a CG-S/USB interface for connection via a USB port (40071347137), or can be preferably a CG-S/IP interface as USB dongle (40071361027) for communication of the systems via TCP/IP with CG-S/IP router on the system side. For operating the VisionGuard on a virtual machine, the CG-S/IP interface is as a pure software licence (40071362852) also available. For this software licence, the MAC address of the VisionGuard environment is required upfront.

Features:

- Web-based client/server architecture for independent operation by multiple users
- Up to 500 emergency lighting systems (DualGuard-S / LoadStar-S, ZB-S, LP-STAR, AT-S+ and CGLine+) can be connected
- Clear and concise status display via system tree, system overview or in a project overview
- User Account Control (UAC) with 4 user roles for assigning different access rights (Supervisor, Administrator, Power User and User)
- Developed and verified for cybersecurity (tested by EATON)
- Software licence without hardware dongle key (Software download) *
- Multi-language: Support of English, German, French, Polish and Norwegian
- Adjustable landing page after log-in (dashboard, log book, project navigation or system overview).
- Available in multiple languages. Language settings can be assigned to each user.
- Responsive web design (automatic adjustment to different display sizes)
- Modern MQTT communication protocol (event-based communication)
- System overview of all systems in one image (Smart view) with easy switching to detailed view. With filter function by system or status
- Complete visualisation, control and configuration of all emergency lighting systems (except from AT-S+)
- Modern project navigation enables a clear arrangement of all connected emergency lighting systems in a navigation tree with freely configurable levels
- A Building Layout Programming (optional) allows a comfortable representation of System status information and Luminaire status in a site plan or floor plan
- Automatic function tests and service life tests for each device
- Extensive Logbook with many filter functions
- Integrated, freely configurable e-mail function
- Graphical representations of battery analog values in the statistic menu offer a clear representation in the form of diagrams over time
- Convenient, comprehensive printing functions
- Optional BACnet/IP interface: This allows easy connection to an external building management system (BMS) via the BACnet protocoll for DG-S, ZB-S, AT-S+, LP-STAR and CGLine+
- Battery block monitoring: graphic display of the optionally available individual battery block monitoring with single battery block voltage and single battery block temperature (only for DG-S or LS-S available)

General information about the displays:

The status indicators in the VisionGuard are color coded.

Green = OK, there is no error

Blue = Notification, e.g. FT interval exceeded

Grey = Circuit or light is turned off

Yellow = Battery operation, function test (FT) active or battery life test (BT) active, circuit or light is turned on

Orange = Priority-1 fault or power failure on the 3-phase monitoring relay (3PM-IO)

Red = Fault, there is an error or fault present.

In general, names can be 40 characters long and information text can be 100 characters long. All special characters are permissible.

1.2 Important information about VisionGuard cybersecurity in Ethernet networks

If VisionGuard is operated in an Ethernet-based communication network, special attention should be paid to preventing unauthorized access, e.g. through hacker attacks. However, the security of VisionGuard is ultimately highly dependent on the operator's setup, e.g. high password quality and the network environment in which VisionGuard is operated. An insecure network environment facilitates unwanted access by others. In order to provide assistance, we would like to draw attention to important points in order to protect the VisionGuard software as securely as possible against unauthorized access.

Settings in VisionGuard

VisionGuard has integrated password protection, which is preset with a security level as follows:

- It must be at least six characters long (the longer the better). It must contain at least one uppercase and lowercase letter as well as special characters and numbers (?!%, etc.)

Password protection is very important for protection against unauthorized or unwanted access by third parties. For this reason, a few rules should be observed when assigning a password:

- Avoid names of family members, pets, best friends, favorite stars, or their birth dates or similar arrangements.

* Note: For an operation of CG-S systems (ZB-S, LP-STAR and AT-S+) an additional CG-S soft license is required!

- If possible, passwords should not appear in dictionaries.
- It should not consist of common variants and repeat or keyboard patterns, i.e. not qwerty or abcd1234 and so on.
- Appending simple numbers to the end of the password or placing one of the usual special characters $! ? # at the beginning or end of an otherwise simple password is likewise inadvisable.

Operation in a network, e.g. intranet

General information about managed network hardware, e.g. routers, switches etc.

- Keep firmware up to date.
- Change the default password of all devices.
- Set up a firewall with MAC address filtering.
- Enable distributed denial of service (DDoS) protection.
- Disable unused ports and protocols.
- Disable unnecessary features of your router.
- Disable remote access to your router.

Further EATON recommendations and guidelines are described in the following:

Guidelines for the secure configuration of Eaton products

Documentation for the secure installation and configuration of Eaton products

The VisionGuard has been designed with cybersecurity as an important consideration. A number of features are offered in the product to address cybersecurity risks. These Cybersecurity Recommendations provide information to help users to deploy and maintain the product in a manner that minimizes the cybersecurity risks. These Cybersecurity Recommendations are not intended to provide a comprehensive guide to cybersecurity, but rather to complement customers' existing cybersecurity programs.

Eaton is committed to minimizing the cybersecurity risk in its products and deploying cybersecurity best practices in its products and solutions, making them more secure, reliable and competitive for customers.

The following whitepapers are available for more information on general cybersecurity best practices and guidelines:

Cybersecurity Considerations for Electrical Distribution Systems (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

References

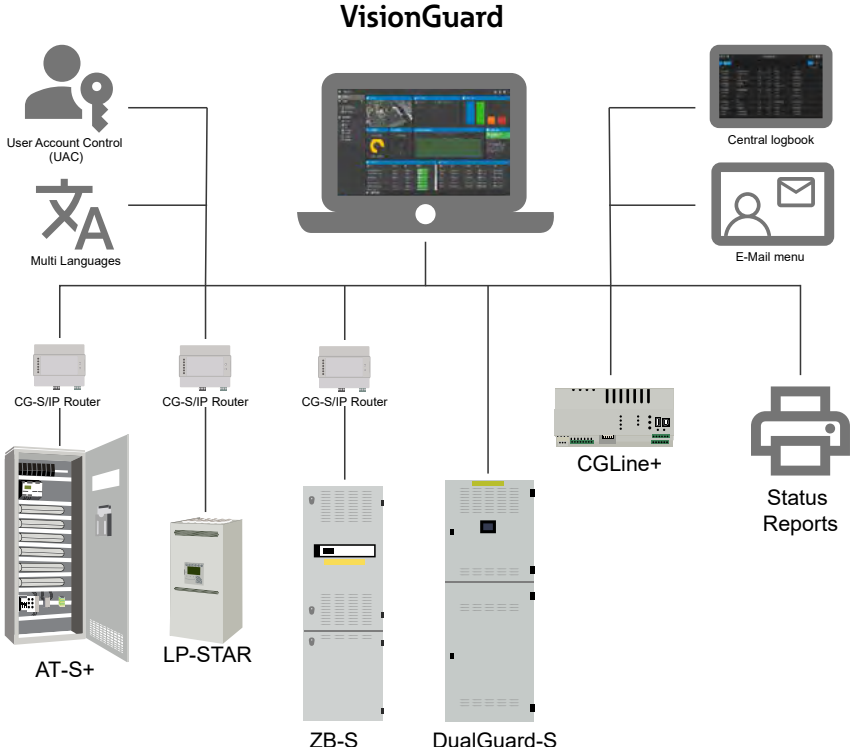
[R1] Cybersecurity considerations for information and communication technology (WP152002EN): http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

[R2] Cybersecurity best practices checklist reminder (WP910003EN): https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf

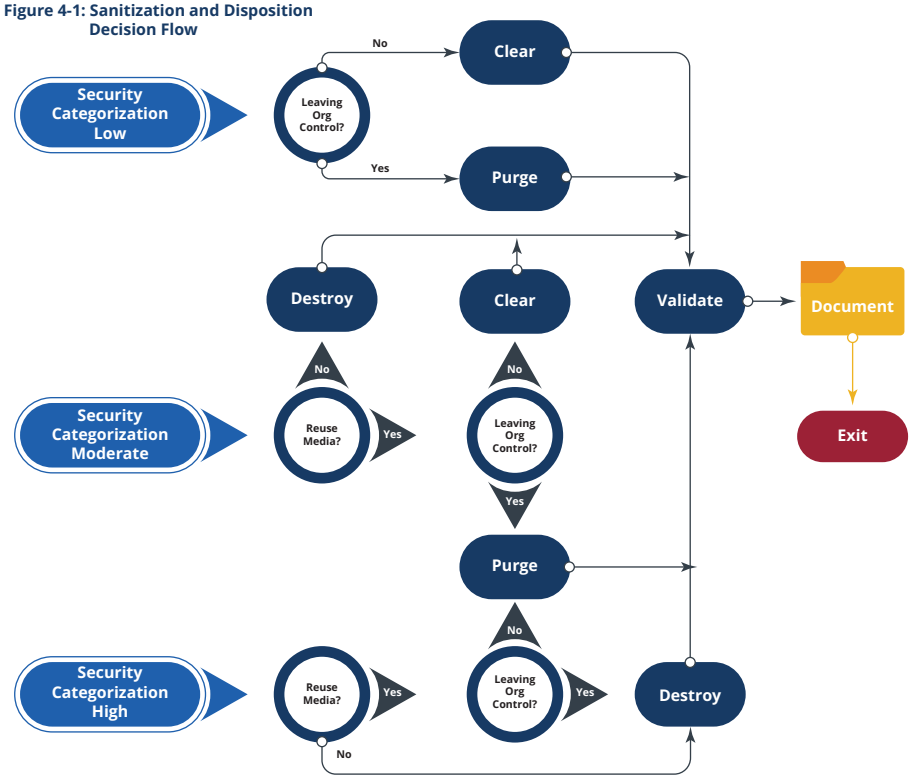
[R3] National Institute of Technology (NIST) interagency "Guidelines on firewalls and firewall policy, NIST special publication 800-41," October 2009: https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final

[R4] NIST SP 800-88, Guidelines for media sanitization, September 2006: http://ws680.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 file as download)

Category	Description
Intended Use & Deployment Context	VisionGuard is a visualisation software to monitor, control and configure DG-S / LS-S, ZB-S, LP-STAR and monitor and control AT-S+ and CGLine+ Web-Controller Emergency Lighting Systems. 
Asset Management	Keeping track of software and hardware assets in your environment is a pre-requisite for effectively managing cybersecurity. Eaton recommends that you maintain an asset inventory that uniquely identifies each important component. To facilitate this, VisionGuard supports the following identifying information: • (Software) Publisher, name, version, and version date. • Please read the corresponding pages of the manual to get information how to find out these parameters.
Risk Assessment	Eaton recommends conducting a risk assessment to identify and assess reasonably foreseeable internal and external risks to the confidentiality, availability and integrity of the system | device and its environment. This exercise should be conducted in accordance with applicable technical and regulatory frameworks such as IEC 62443. The risk assessment should be repeated periodically.
Physical Security	An attacker with unauthorized physical access can cause serious disruption to system/device functionality. Additionally, Industrial Control Protocols don't offer cryptographic protections, making ICS and SCADA communications especially vulnerable to threats to their confidentiality. Physical security is an important layer of defense in such cases. VisionGuard is designed to be deployed and operated in a physically secure location. Following are some best practices that Eaton recommends to physically secure your system/ device: • Secure the facility and equipment rooms or closets with access control mechanisms such as locks, entry card readers, guards, man traps, CCTV, etc. as appropriate. • Restrict physical access to cabinets and/or enclosures containing VisionGuard and the associated system. Monitor and log the access at all times. • Physical access to the telecommunication lines and network cabling should be restricted to protect against attempts to intercept or sabotage communications. It's a best practice to use metal conduits for the network cabling running between equipment cabinets. • VisionGuard supports the following physical access ports. A network (RJ45) ports access should be restricted. • Do not connect removable media (e.g., USB devices, SD cards, etc.) for any operation (e.g., firmware upgrade, configuration change, or boot application change) unless the origin of the media is known and trusted. • Before connecting any portable device through a USB port or SD card slot, scan the device for malware and viruses.

COTS platform security (Commercial off-the-shelf)	Eaton recommends that customers harden third-party commercial off-the-shelf (COTS) operating systems or platforms that are used to run Eaton applications / products (e.g., third party hardware, operating systems and hypervisors, such as those made available by Dell, Microsoft, VMware, Cisco, etc.). • Eaton recommends that customers refer to the COTS vendor's documentation for guidance on how to harden these components. • Vendor-neutral guidance is made available by the Center for Internet Security **https://www.cisecurity.org/** Irrespective of the platform, customers should consider the following best practices: • Install all security updates made available by the COTS manufacturer. • Change default credentials upon first login. • Disable or lock unused built-in accounts. • Limit use of privileged generic accounts (e.g., disable interactive login). • Change default SNMP community strings. • Restrict SNMP access using access control lists. • Disable unneeded ports & services.
Account Management	Logical access to the system | device should be restricted to legitimate users, who should be assigned only the privileges necessary to complete their job roles/functions. Some of the following best practices may need to be implemented by incorporating them into the organization's written policies: • Ensure default credentials are changed upon first login VisionGuard should not be deployed in production environments with default credentials, as default credentials are publicly known. • No account sharing – Each user should be provisioned a unique account instead of sharing accounts and passwords. Security monitoring/logging features in the product are designed based on each user having a unique account. Allowing users to share credentials weakens security. • Restrict administrative privileges - Attackers seek to gain control of legitimate credentials, especially those for highly privileged accounts. Administrative privileges should be assigned only to accounts specifically designated for administrative duties and not for regular use. • Leverage the roles / access privileges (**see „6. Creating new users with user roles" on Page 30** to provide tiered access to the users as per the business /operational need. Follow the principle of least privilege (allocate the minimum authority level and access to system resources required for the role). • Perform periodic account maintenance (remove unused accounts). • Ensure password length, complexity and expiration requirements are appropriately set, particularly for all administrative accounts (e.g., minimum 10 characters, mix of upper- and lower-case and special characters, and expire every 90 days, or otherwise in accordance with your organization's policies). • Enforce session time-out after a period of inactivity.
Time synchronization	Many operations in power grids and IT networks heavily depend on precise timing information. Ensure the system clock is synchronized with an authoritative time source (using manual configuration, NTP, SNTP, or IEEE 1588).
Network security	VisionGuard supports network communication with other devices natively over Ethernet communication. This capability can present risks if it's not configured securely. Following are Eaton recommended best practices to help secure the network. Additional information about various network protection strategies is available in Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1]. Eaton recommends segmentation of networks into logical enclaves, denying traffic between segments except that which is specifically allowed, and restricting communication to host-to-host paths (for example, using router ACLs and firewall rules). This helps to protect sensitive information and critical services and creates additional barriers in the event of a network perimeter breach. At a minimum, a utility Industrial Control Systems network should be segmented into a three-tiered architecture (as recommended by NIST SP 800-82[R3]) for better security control. Eaton recommends opening only those ports that are required for operations and protect the network communication using network protection systems like firewalls and intrusion detection systems / intrusion prevention systems. Use the information below to configure your firewall rules to allow access needed for the VisionGuard to operate smoothly.
Remote Access	Remote access to devices/systems creates another entry point into the network. Strict management and validation of termination of such access is vital for maintaining control over overall ICS security. Interactive remote access to the product is not supported natively.
Log and Event Management	• Eaton recommends logging all relevant system and application events, including all administrative and maintenance activities. • Logs should be protected from tampering and other risks to their integrity (for example, by restricting permissions to access and modify logs, transmitting logs to a security information and event management system, etc.). • Ensure that logs are retained for a reasonable and appropriate length of time. • Review the logs regularly. The frequency of review should be reasonable, taking into account the sensitivity and criticality of the system | device and any data it processes.
Vulnerability scanning	It is not possible to install and use third-party software with VisionGuard. Any known critical or high severity vulnerabilities on third party component/libraries used to run software /applications should be remediated before putting the device | system into production. Vulnerability information for the VisionGuard can be obtained by signing up for updates at **www.eaton.com/cybersecurity** and by checking for vulnerabilities in the National Vulnerability Database (NVD), available at **https://nvd.nist.gov/**. and ICS CERT. Note: Many compliance frameworks and security best practices require a monthly vulnerability review. For many non-COTS products vulnerabilities will be communicated directly through the vendor site.

Malware Defenses	Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.
Secure maintenance	**Best practices** Please check Eaton's cybersecurity website (**https://www.eaton.com/us/en-us/company/news-insights/cybersecurity.html**) for information bulletins about available firmware and software updates.
Business continuity/ cybersecurity disaster recovery	Plan for Business Continuity / Cybersecurity Disaster Recovery Eaton recommends incorporating VisionGuard into the organization's business continuity and disaster recovery plans. Organizations should establish a Business Continuity Plan and a Disaster Recovery Plan and should periodically review and, where possible, exercise these plans. As part of the plan, important system | device data should be backed up and securely stored, including: • Updated software for VisionGuard. Make it a part of standard operating procedure to update the backup copy as soon as the latest software is updated. • Current configuration. • Documentation of the current permissions / access controls, if not backed up as part of the configuration.
Sensitive Information Disclosure	Eaton recommends that sensitive information (i.e. connectivity, log data, personal information) that may be stored by VisionGuard be adequately protected through the deployment of organizational security practices.
Decommissioning or zeroing	It is a best practice to purge data before disposing of any device containing data. Guidelines for decommissioning are provided in NIST SP 800-88. Eaton recommends that products containing embedded flash memory be securely destroyed to ensure data is unrecoverable. **Figure 4-1: Sanitization and Disposition Decision Flow**  **• Embedded Flash Memory on Boards and Devices** • Eaton recommends the following methods for disposing of motherboards, peripheral cards such as network adapters, or any other adapter containing non-volatile flash memory. • **Clear:** If supported by the device, reset the state to original factory settings. • **Purge:** If the flash memory can be easily identified and removed from the board, the flash memory may be destroyed independently of the board that contained the flash memory. Otherwise, the whole board should be destroyed. • **Destroy:** Shred, disintegrate, pulverize, or Incinerate by burning the device in a licenced incinerator.

1.3 System requirements – hardware/software requirements

The following hardware is recommended for proper operation of VisionGuard. VisionGuard server software does not run on Linux or Mac OS operating systems! The VisionGuard client, on the other hand, can be any web browser, i.e. independent of the operating system.

VisionGuard server

PC System: Standard PC (tower, rack), virtual machine (VMware/Hyper-V)

Operating system: Windows® 10 Pro/Enterprise (64 Bit), Windows® 11 Pro/Enterprise, Windows ® Server 2016, Windows® Server 2019, Windows® Server 2022

Processor: min. Intel Core i5 or AMD Ryzen 5

Memory (RAM):

Versions VisionGuard V4.0.1and older:

min. 16 GB for VisionGuard Basic Version 3 / 10 / 25
min. 32 GB for VisionGuard Basic Version 50 / 100 / 500 (64 GB recommended)

VisionGuard V4.2.1:

min. 32 GB (64 GB recommended)

HDD: min. 1 TB SSD (min. 300GB free space)

A CG-S interface is required to connect CG-S systems:

possible options

CG-S/USB-Interface (40071347137)

CG-S/IP-Interface (40071361027)

CG-S/IP interface soft licence (40071362852) (MAC address of the VisionGuard Server PC must be included in the order!)

Client

PC System: Standard PC workstation, AiO PC, Tablet PC or Smartphone with actual web browser

Graphics card: DirectX 12

Software: Standard web browser, e.g. Edge, Chrome, Firefox, Safari

Monitor: min. 19-inch, recommended 27-inch FullHD or higher

Optimal resolution: Full HD 1920x1080 or higher

Peripheral devices: Keyboard, mouse, printer

1.4 Important information before installation

1.4.1 Used Ports and Protocols

The following ports and protocols are used by the VisionGuard and must be allowed in the network for a proper function.

If necessary, please contact your IT department for the right network settings.

Protocol	Port	Encrypted	Accessible from outside	Service	Description
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	-	-	-	Communication ports of CG-S/IP router (ZB-S/AT-S+/LP-STAR)
TCP	5000 / 5050	-	-	-	CGline+
BACnet/IP	47808	-	-	-	BACnet/IP communication

1.4.2 Used Services and standard installation path

Name	Installation Path	Description
.NET Core Runtime	**C:\Program** Files\dotnet	Runtime for Services
Erlang	**C:\Program** Files\ er-24.2.1	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 Prerequisite for a VisionGuard software installation

IMPORTANT NOTE

Before install the VisionGuard software on a Windows Server 2016 or Windows Server 2019 OS, the Windows .NET framework 4.7.2 or higher must be enabled/installed!

When installing/updating the VisionGuard, the HOMEDRIVE must always be C:!

- Please ensure that the emergency lighting systems have minimum following software releases to ensure a proper operation on VisionGuard:

ZB-S CU CG-S: Software Z410X_B

CGline+ Web-Controller: Software Z1000.T

CGLine+ Compact-Controller 160/400: Software Z1030.D

- Take care that virus scanners can affect the installation:
  - Slowing down the installation
  - Blocking parts of the installation
  - Permission prompts to be acknowledged by the user
- It may be necessary to disable a virus scanner for the duration of the installation for one of the above reasons.
- Any switching off/pausing of the PC during the installation should be refrained from. This also includes:
  - Energy saving mode
  - Restarts
- The user should also remain on the PC during the installation, as system queries occur which must be confirmed by the user. If these queries remain unconfirmed for a longer period of time, the installation will be aborted.
- During the Visionguard installation other installations should be avoided.
- Basically, all forms of energy saving mode and automatic shutdown of the computer should be deactivated, as the VisionGuard system must be permanently available.

• After an installation or update of a VisionGuard, a reboot of the PC is strictly recommended!

1.5 VisionGuard licences

1.5.1 Licensing models

VisionGuard is protected against unauthorized operation. A licence is required to activate VisionGuard. The type of licence depends on the number of the connected devices. A „device“ can be a Battery system or a substation with a Control unit (HMI or CU-S and/or a CGLine+ Web Controller). Upgrading to a higher volume licence is possible. The following volume licences are available:

- Basic version for 3 devices
- Basic version for 10 devices
- Basic version for 25 devices
- Basic version for 50 devices
- Basic version for 100 devices
- Basic version for 500 devices

Options:

- VisionGuard BACnet/IP Interface for DG-S/LS-S, ZB-S, AT-S+, LP-STAR and CGLine+
- Building Layout Programming

All VisionGuard version licences are available as Software key (certificate with access key) without hardware, or optional on an USB-Stick (VisionGuard software, CG-S Gateway, CG-S driver package, documentation and access key).

1.5.2 Licensing procedure

IMPORTANT NOTE

The BACnet/IP-Interface and Building layout options are separate single licences! For each licence the same licensing procedure is required.

When a licence is purchased, it is stored online on a licensing server. After installing VisionGuard, a fingerprint must be generated in a licensing menu. A key is created based on the hardware components installed. The fingerprint has the file format fingerprint.c2v (.Customer to Vendor).

This must be entered online in the licensing server. To access the online licensing process, you will need the access key that was supplied to you. Based on the volume licence purchased, this generates an activation key in the form of a licence file in the file format ".v2c." (.Vendor to Customer).

This licence file must again be read in the VisionGuard licensing menu in order to activate VisionGuard for the number of systems purchased.

The licensing procedure is described in detail in **„4. Licence information“ on Page 23.**

2. Installation instructions

Installation notes:

If only DualGuard-S (DG-S) or LoadStar-S (LS-S) systems are to be connected to the VisionGuard, it is sufficient to install only the VisionGuard software (see **„2.1 Installation of the VisionGuard software“ on Page 11**). If CG-S emergency lighting systems (ZB-S, LP-STAR or AT-S+) are also to be connected to the VisionGuard, a CG-S Gateway software and a CG-S interface driver package must also be installed. (see **„2.2 Installation of the CG-S Gateway software“ on Page 14** and **„2.3 Installation of the CG-S Interface driver package“ on Page 16**

IMPORTANT NOTE

Depending on the system, an installation or an update procedure can take a longer time (up to 45 minutes) without any installation progress being visible. Please do not interrupt the installation.

The latest version of the VisionGuard, CG-S Gateway and the CG-S Driver package are available for download from the VisionGuard product page at : **https://www.eaton.com/de/en-gb/catalog/emergency-lighting/visionguard.resources.html#tab-3.**

The downlaod .zip file contains the VisionGuard Installer.exe and a SHA 256 file to check the correct download.

Here between the text insert the image "Download.zip.jpg"

Please unzip both files into the same folder.

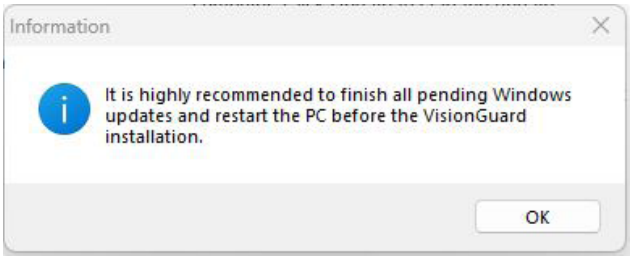
It is recommended that you download the versions to a folder, e.g. C:/Temp, before installing it. If the installations are to be carried out on another Windows environment, it is recommended to download the software to an external data medium, e.g. a USB stick. To minimize installation time, it is recommended that you install from a local SSD or hard drive, not from a USB stick or other external media.

This hash file is a checksum that ensures that the VisionGuard installation file has been downloaded correctly, given its size of around 1.6GB. More information about the hash file is explained in chapter 2.1.

2.1 Installation of the VisionGuard software

Please also be sure to observe the installation instructions under 1.4.3. The installation is started by running the VisionGuard installer: **VisionGuard-Installer-V4.2.1.exe**

The installation must be started „as Administrator“. Right mouseclick on this .exe file opens a menu. Click on „run as Administrator“ to start the VisionGuard setup wizard. A Windows User Account Control message may appear first. In this case, please confirm with „**YES**.“
An information box appears:

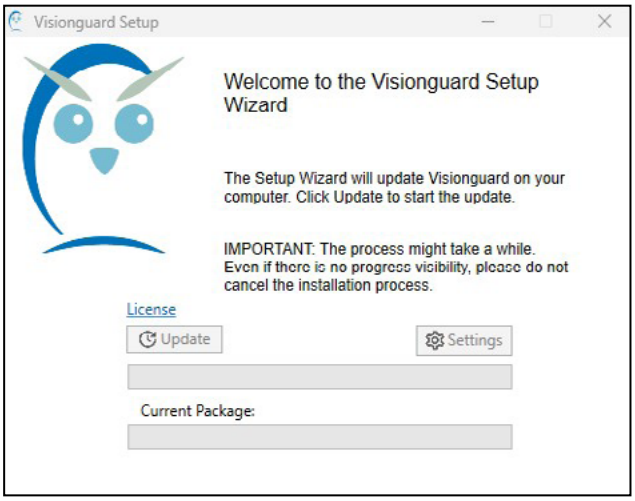


Please ensure that all windows updates are done, and restart the PC!

After confirming this information with "OK", the installation dialog box "Welcome to the VisionGuard Setup Wizard" appears. To ensure the right downloaded installer, please compare the HASH of the installer:

The SHA256 appears on the bottom line of the dialog box.

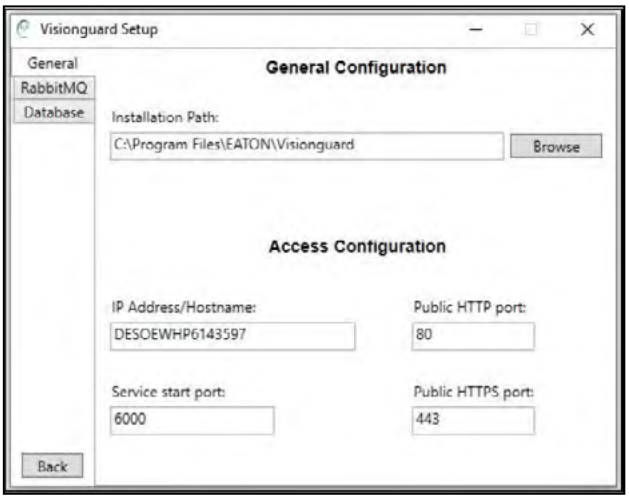
In this case an OK next to the HASH will appear, which indicate that the installer is right downloaded:



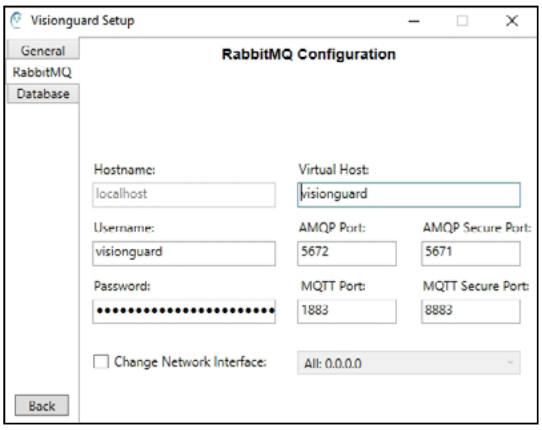
Additional installation settings can be made by clicking on „Settings“. However, it is strongly recommended to accept the default values. Changes should only be made by IT administrators.

Settings > General

Set the installation path and the host name of the PC here. This is required to connect the HMI of the DualGuard-S or LoadStar–S to VisionGuard. Alternatively, the IP address of the PC can be used for the connection. You can also specify a port range and the web client ports for web access. A start port range must be defined, which then reserves at least 30 ports for VisionGuard. The default start port is 6000. The standard ports 80 for unencrypted HTTP access and 443 for encrypted HTTPS access are set as web client ports.



Settings > RabittMQ
Use this dialog box to configure the VisionGuard communication interface. The host name can later be used to access VisionGuard locally on the PC via a web browser. The default setting is "localhost," i.e. local access to VisionGuard is made after installation via http://localhost (unencrypted) or via https://localhost (encrypted).

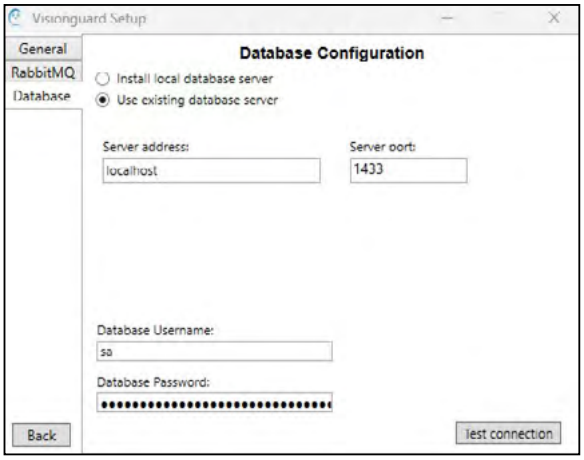


Settings > Database
In this dialog box, the specifications of the MSSQL database can be changed.

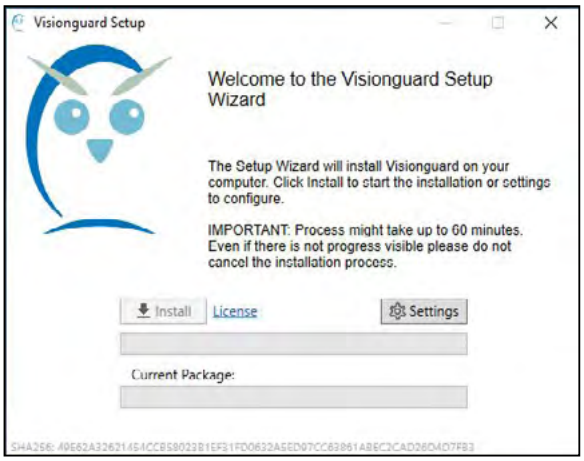
Again, it is strongly recommended to keep the default settings.

IMPORTANT NOTE

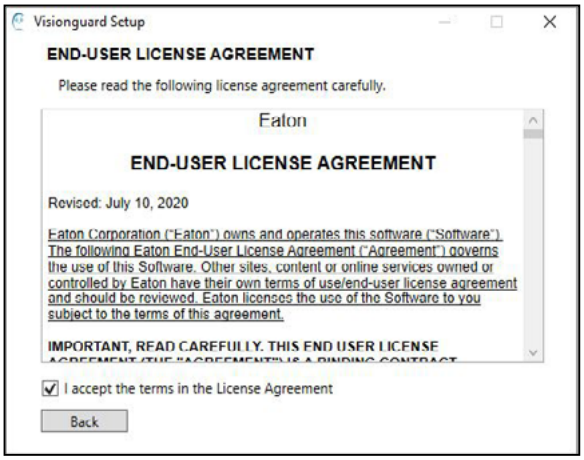
A support of a local MS SQL database is currently not supported. This function is planned for the next VisionGuard version!



Click "***Back***" to go back. In order to start the installation, the EULA (end-user licence agreement) must first be read and confirmed. Open the EULA via the "***Licence***" link

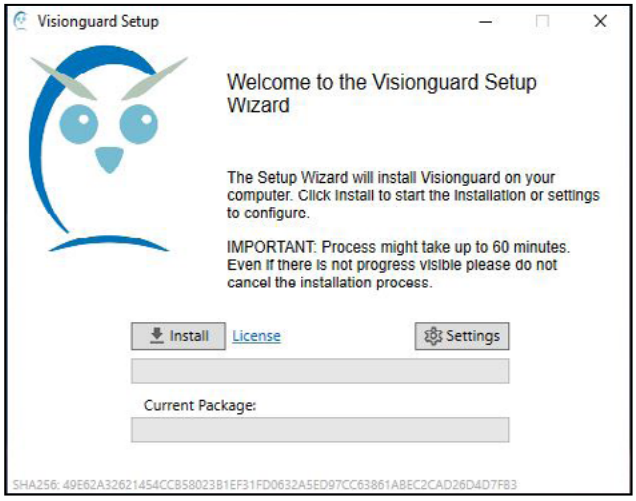


Please read the end-user licence agreement (EULA) carefully and confirm the EULA by enabling "***I accept the terms in the Licence Agreement.***"

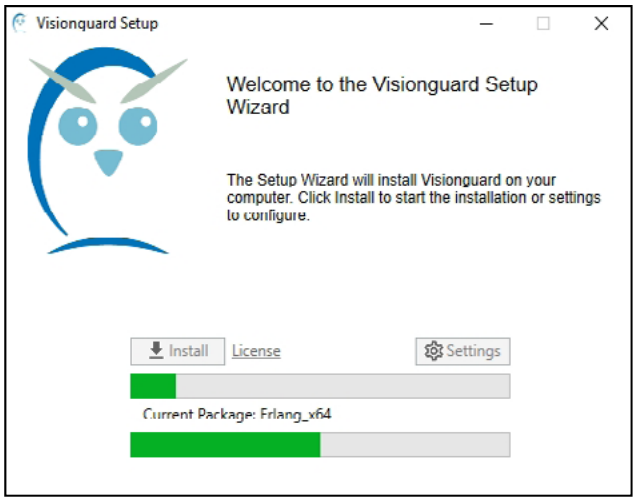


Click "Back" to go back.

The installation can now be started by clicking "***Install***"



Up to three Windows User Account Control (UAC) confirmation prompts may follow. Please confirm these with "***Yes***." The installation may take a few minutes. Please do not start any other applications during installation. The installation progress is indicated by progress bars.

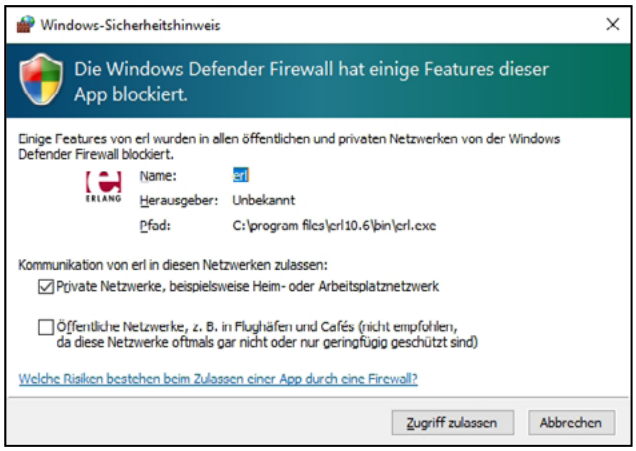


NOTE

In certain cases, the installation may take a longer time without a visible progress indicator. Please do not interrupt the installation.

If a firewall has been enabled, messages may appear that block the functions of some apps.
For example, Windows Defender might display the following message:

All accesses must be permitted, otherwise the HMIs of the DualGuard-S or LoadStar–S will not be able to establish a connection to VisionGuard!

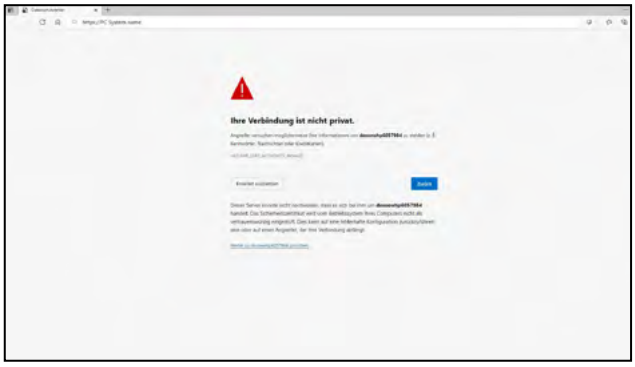


When the installation is complete, the installation wizard can be closed in the next window by clicking "***Close***."

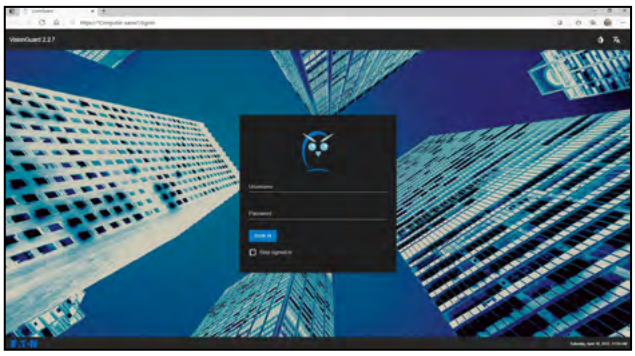
The installation of the VisionGuard software is now complete. If ZB-S, LP-STAR or AT-S+ emergency lighting systems are to be connected to the VisionGuard as mentioned above, gateway software and a CG-S interface driver package must also be installed. Please then perform the installations described in 2.2 and 2.3.

A message appears stating that the computer needs to be restarted. Confirm with "Yes". The computer will restart automatically.

After the restart VisionGuard is ready for operation. Start a web browser, e.g. Edge. Enter the IP address of the PC, PC name or localhost in the input line of the web browser and click "***Enter***".



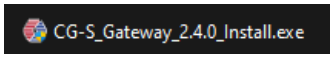
Since no certificate has been installed yet, a security message appears in the browser and denies access. To install a certificate, see section **„5. Security certificate installation" on Page 25**.



Via „***Advanced***" and „***Continue to *computer name* (insecure)***", you get to the login page of the local VisionGuard. It is recommended to set a bookmark in the web browser now. For more information on the operation of the VisionGuard see **„3.First launch of VisionGuard" on Page 21**.

2.2 Installation of the CG-S Gateway software

The installation must be started „as Administrator". Right mouseclick on this .exe file



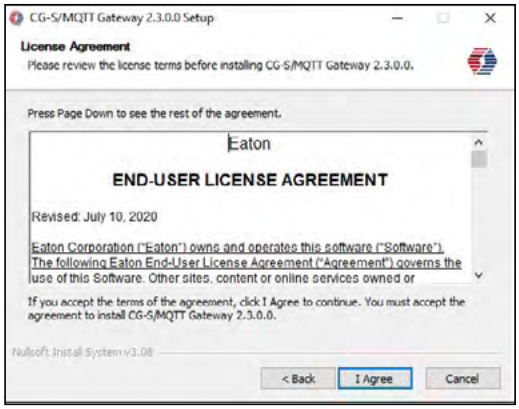
opens a menu. Click on „***Run as Administrator***" to start the VisionGuard setup wizard. A Windows User Account Control message may appear first. In this case, please confirm with „***YES***."

After start of the installation a window appear, to select the language.

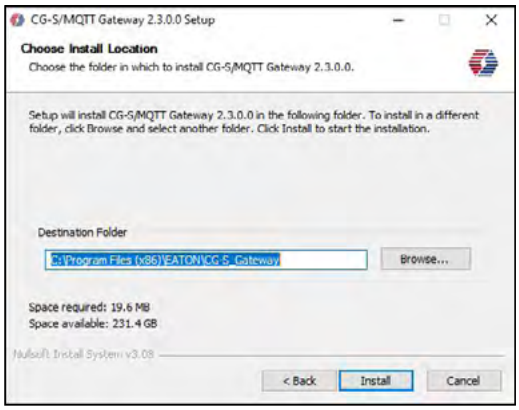
It is possible to choose between German or English. Select the desired language and click ***OK***.

The Setup starts. Continue with "***Next***"

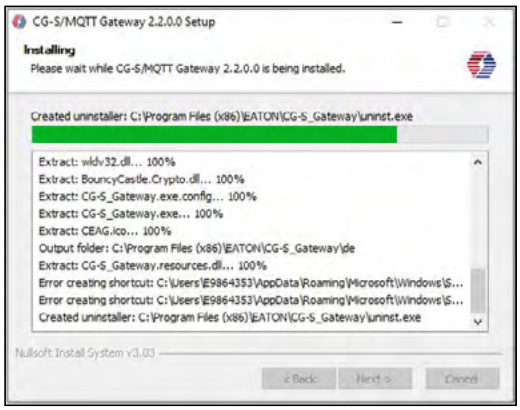
A Licence Agreement appears. Please read it carefully and confirm with "***I Agree***"



In the next window the destination directory can be selected. It is recommended to keep the settings. Continue with „***Install***".

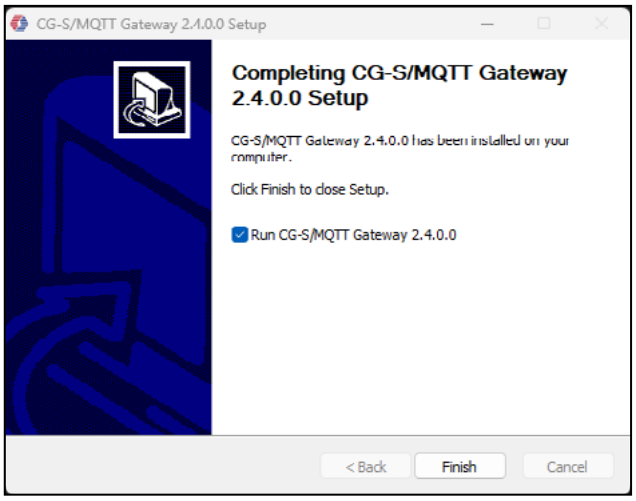


The installation starts with a progress bar



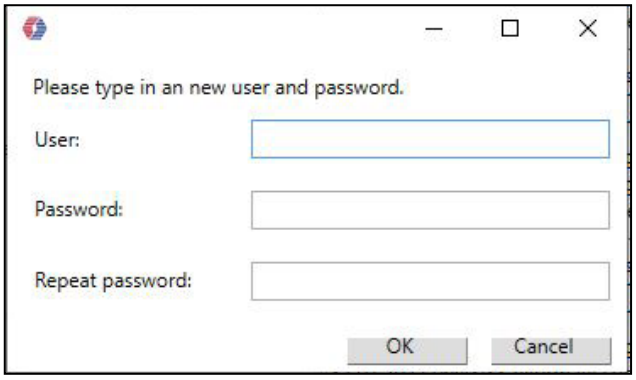
After the installation please activate "***Run CG-S/MQTT Gateway***".

The installation is completed by clicking on „***Finish***".



The Gateway Software starts (CEAG Icon on the task bar). It is necessary to assign a user name and a secure password to operate the gateway.

Please make a note of the password and keep it safe for future changes!



IMPORTANT NOTE

This visualisation interface of the CG-S Gateway is only used for configuration. Please configure the gateway according to chapter „***Configuring the CG-S Gateway***". After the configuration, the visualisation interface can be closed. The CG-S Gateway starts automatically with Windows as a service in the background.

2.3 Installation of the CG-S Interface driver package

The CG-S Interface driver package allows a connection between the CG-S Gateway and the CG-S Bus based emergency lighting systems ZB-S, AT-S+ or LP-STAR. A CG-S interface is absolutely required for operation! This can be a CG-S/USB interface for connection via a USB port (40071347137), or preferably a CG-S/IP interface as USB dongle (40071361027) for communication of the systems via TCP/IP with CG-S/IP router on the system side.

For operating the VisionGuard on a virtual machine, the CG-S/IP interface is also available as a pure software licence (40071362852). For this software licence, the MAC address of the VisionGuard environment is required.

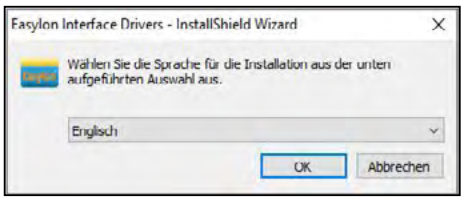
The installation must be started „as Administrator".

Right mouseclick on this .exe file

and click on „***Run as administrator***".

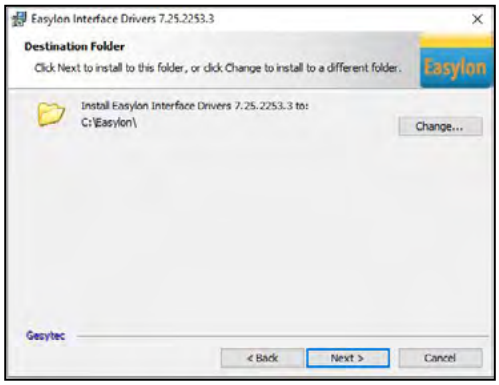
After start of the installation a window appear, to select the language.

It is possible to choose between German or English. Select the desired language and click "***OK"***.

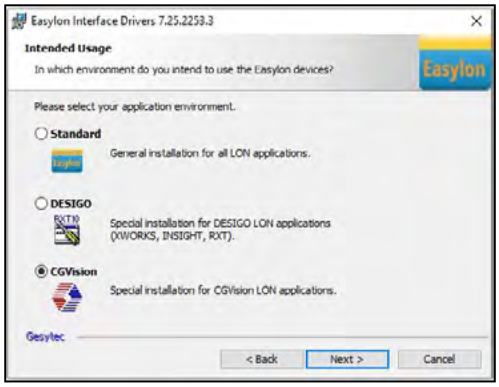


A Licence Agreement appears. Please read it carefully and confirm with "***I accept the terms in the licence Agreement***", Continue with "***Next***"

In the next window the destination directory can be selected. It is recommended to keep the settings. Continue with „***Next***".



A selection for an appllication appears. Please select "***CGVision***" and continue with "***Next***"



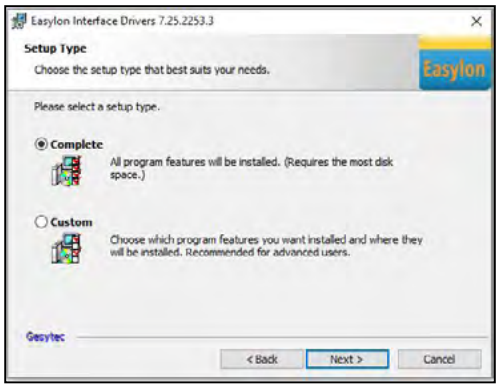
A Setup Type appears. Please select "Complete",

and confirm with "***Next***".

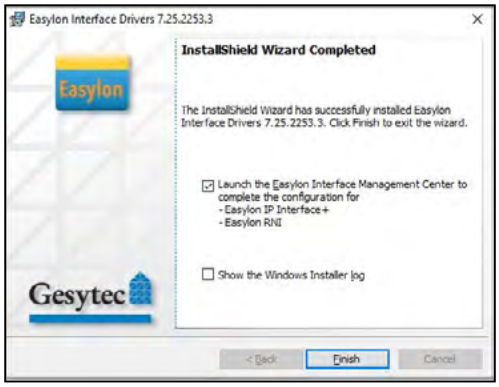
Please click in the next Window on "Install" to install the installation.

It takes some minutes.

A progress bar informs about the installation progress.

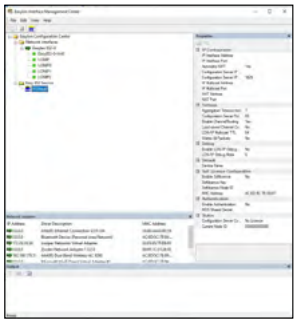


To the end of the installation, please activate the Launch of the Easylon Interface Management Center, to configure the right interface settings, and continue with "Finish".



For the configuration, please select

- the right CG-S-Interface (852 CG-S/IP-Interface or CG-S/USB-Interface).
- Select the right "Network adapter" (IP-Address) of the CG-S/IP-Interface, which must be appear as "IP-Interface Address" under "IP-Configuration". Save the settings using the save icon above (right).
- Under "Configuration Server" the connection will be appears as licenced if the connection to the configuartion server is OK.



2.4 Updating an already installed version of VisionGuard, CG-S Gateway and CG-S driver package

2.4.1 Update description of VisionGuard Software

An update may be necessary if new features are available or bugs have been fixed by bug fixes. It is recommended to keep the software up-to-date.

The latest VisionGuard version is available for download on the VisionGuard product page on our website

https://www.eaton.com/de/en-gb/catalog/emergency-lighting/visionguard.resources.html#tab-3.

It is recommended to check the website for updates at regular intervals, e.g. every 3–6 months, and to download the VisionGuard update software directly to the PC or to a USB stick for installation.

If the existing VisionGuard version is older than V3.0.1, a deinstallation is required. See important notes below.

If a version >V3.0.1 to <V3.2.0 is installed, the VisionGuard must first be updated to V3.2.0, as a database migration must be performed, which takes some time.

After installing V3.2.0, please wait approx. 30 minutes, the VisionGuard carries out a database migration. After this it is essential to restart the PC before installing V4.2.1.

If a VisionGuard V3.2.0 is installed, a deinstallation of this version is not necessary for an update, i.e. an update can be installed simply over the top of an existing VisionGuard version. To do this the current VisionGuard version must be stopped before the update installation is executed.

Existing configurations are not overwritten, but it is recommended to back up the existing VisionGuard version for security reasons. A backup can be performed via the integrated backup function in the VisionGuard. For this, see **„19.Backup & Restore Menu“ on Page 81** .

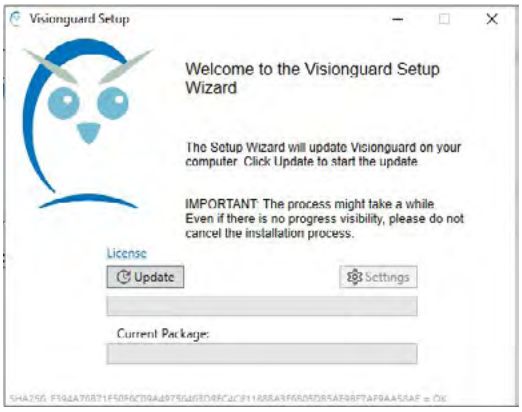
IMPORTANT NOTES

Depending on the system, an update procedure can take a longer time (up to 45 minutes) without any installation progress being visible. Please do not interrupt the installation.
When updating from an older version than V3.0.1, an uninstallation of the VisionGuard is required. Please create a Back Up, and uninstall the ODBC driver manually via the Windows function "Apps & Features". Please restart the PC and uninstall the VisionGuard components according to section 2.5. Please restart the PC again, an install the new VisionGuard V4.2.1 according to section 2.

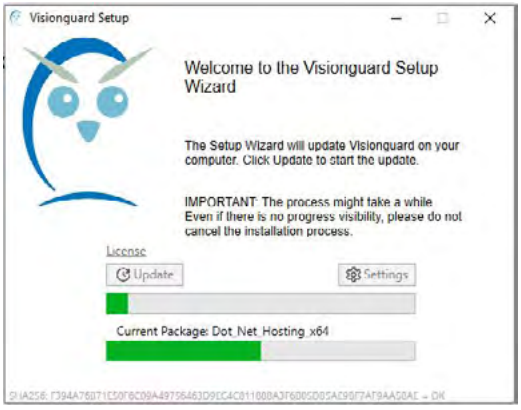
2.4.2 Performing an update of VisionGuard

To update VisionGuard, simply run the installer as described in 2.1 Installation instructions. The following dialog box appears.

Please click on "Licence" and read carefully the End-User Licence Agreement. Agree with setting a hook at "***I accept the terms in the licence Agreement***", and click on "***Back***".

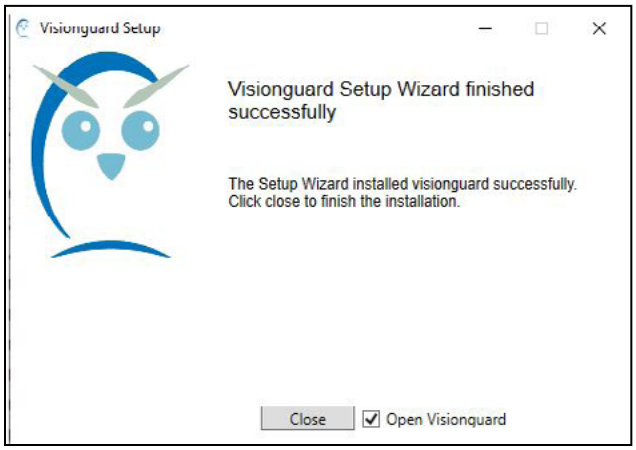


Now you can click on "***Update***".



A progress bar indicates the current update progress, including a process text, for example "Stopping services...". Please note that the update can take up to 60 minutes.The following window appears at the end of the update.

After installing the update, it is essential to restart the PC.

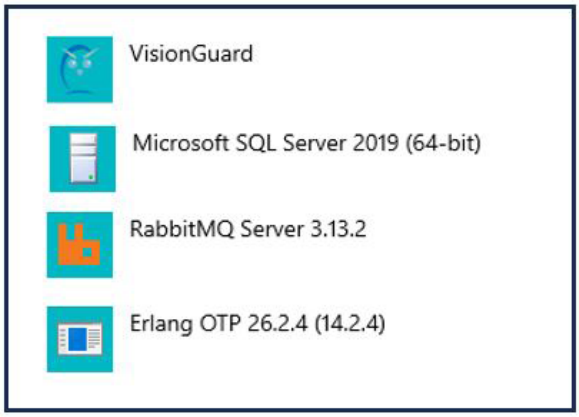


2.4.3 Update of a CG-S Gateway and the CG-S driver package

If you download the newest CG-S Gateway or CG-S driver package, you can easily install over the existing CG-S Gateway/drivers with click on the new setups. Please ensure to run the newer software/drivers as Administrator!

2.5 Deinstallation of VisionGuard software components

VisionGuard must be exited before deinstallation.
VisionGuard can be completely uninstalled via the Windows "***Apps & Features***" function.

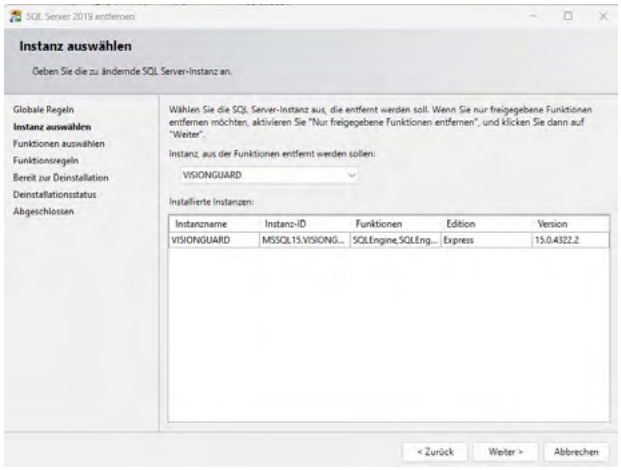


The following services must be uninstalled in the given order:

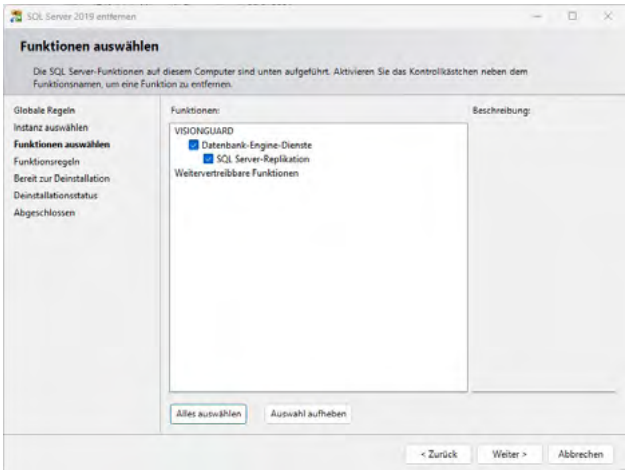
1. VisionGuard
2. Microsoft SQL Server 2019 (64-bit)
3. RabbitMQ Server
4. Erlang OTP

IMPORTANT NOTE

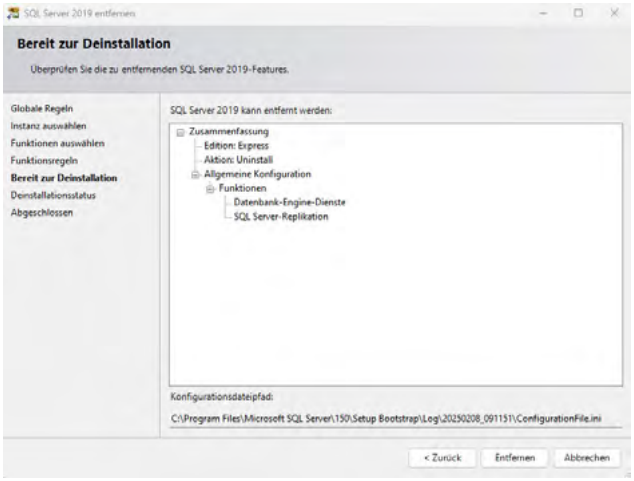
Only the VisionGuard instances in Microsoft SQL Server may be uninstalled!
Otherwise, other programs that also use MSSQL may no longer work.



Deinstallation of Microsoft SQL Server (64-bit):
Please deinstall only the VisionGuard instances of the Microsoft SQL Server!
Click on the next dialog box of the deinstallation process Instancename "VISIONGUARD" and click continue (***Weiter***)

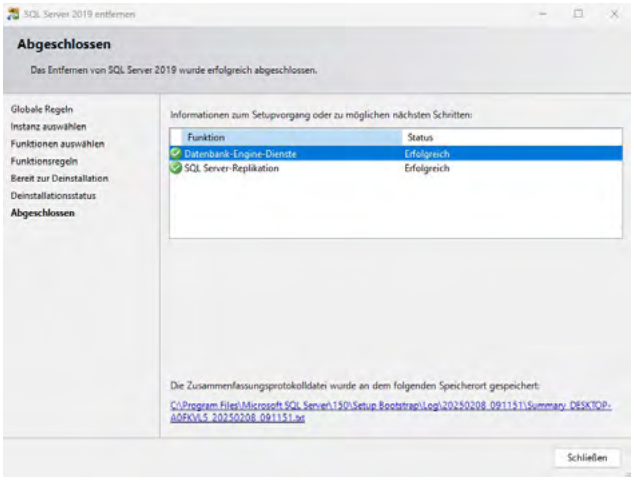


In the next dialog box plaese click on "Database-engine-services" (Datenbank-Engine-Dienste) and "SQL Server-Replikation". Click on continue (***Weiter***)



A summary of the files to deinstall appears. Continue with delete (Entfernen)

A final dialog appears with the message of a succesful deinstallation of the files.



To uninstall the CG-S Gateway, please go on „Start“, right mouse click on "CG-S Gateway" and click deinstall. Same procedure for the CG-S driver package. Please click with right mouse click under the folder „Easylon“ the software „EIMC (CGVision)“ on deinstall.

After uninstalling all applications on the right, **the PC must be restarted.**

3.First launch of VisionGuard

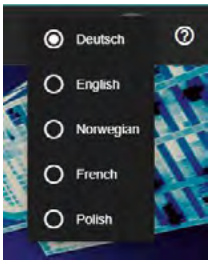
3.1 Local access (VisionGuard server and client on a PC)

VisionGuard is accessed locally via a standard web browser, e.g. Microsoft Edge, via the URL:
https://localhost (encrypted).

It is possible to use the computer name or the active IP address as well, for login into the VisionGuard.

The following login window screen appears:

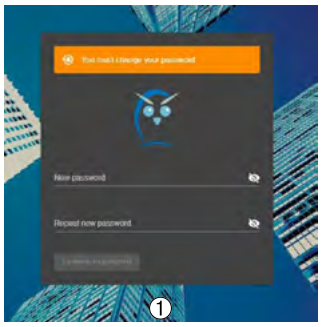
The language can be set in the top right-hand corner:



A default user with supervisor rights is preset in VisionGuard.

The user name and password for the default user's first login is:

User name: Admin
Password: EATON



A request appears to assign a new password. ①

Please type in a new password, and repeat it.

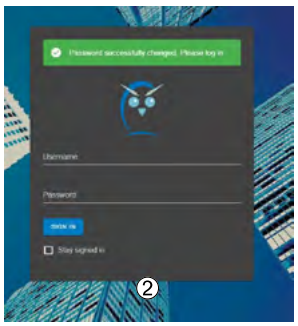
Make sure that the default password security is min. 6 characters, containing at least one of each of the following: uppercase letter, lowercase letter, number, and special character:

UAC – Password guidelines

Directive	Value
Number	Yes
Special character	Yes
Small letters	Yes
Capital letters	Yes
Minimum password length	6

IMPORTANT NOTE

It is strongly recommended that you write down the new password and keep it safe.



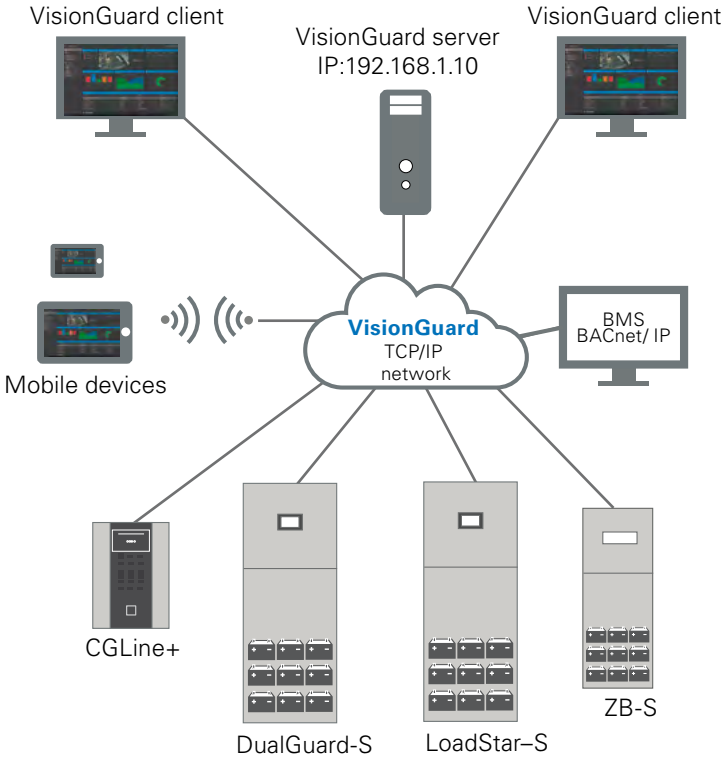
If the password has been successfully changed, the password is displayed in green in the login screen ②.

Now log in again with the new password:

After logging in, the dashboard appears as the start screen, which is explained in more detail in Section ***„Dashboard“.***

3.2 Access to remote VisionGuard server (VisionGuard server and client on a different PC)

To access VisionGuard from another client PC via the Ethernet network, e.g. VisionGuard was installed in a virtual environment, it is accessed via a standard web browser, e.g. Microsoft Edge, via the IP address of the server PC, e.g. **https://192.168.1.10** (encrypted).
Schematic:



4. Licence information

4.1 Activating a licence

To use VisionGuard, a licence must be purchased. Different licences are available depending on how many DG-S/LS-S, ZB-S, LP-STAR, AT-S+ or CGLine+ Web-Controller systems are to be connected to VisionGuard. You can find out which licences are available in section VisionGuard licences. Optional licenses for the BACnet/IP interface (DG-S, ZB-S, LP-STAR, AT-S+ and CGLine+) and the Building Layout Programming option are also available. In addition to the VisionGuard basic license, these must be purchased individually and activated in VisionGuard. With the purchase of a VisionGuard licence, the customer receives a product key in written form or optional on a USB-Stick, which is needed to activate the licence.

IMPORTANT NOTE

Licensing may only be carried out by a user with supervisor rights.

After logging into the newly installed VisionGuard, the message "not licenced" will appear: ①
In order to be able to complete the licensing step, a fingerprint must be requested in the Administration/ Information/Licences menu.

② "Get new fingerprint"

③ A file with the name "fingerprint.c2v" is created, which must be saved in a folder, e.g. **C:\temp**, or on an external data medium, e.g. a USB stick.
This file must now be uploaded online in the licence server at **https://ceagsystems.sentinelcloud.com/ems/customerLogin.html**
or click on the button "***Licensing Customer Portal***":

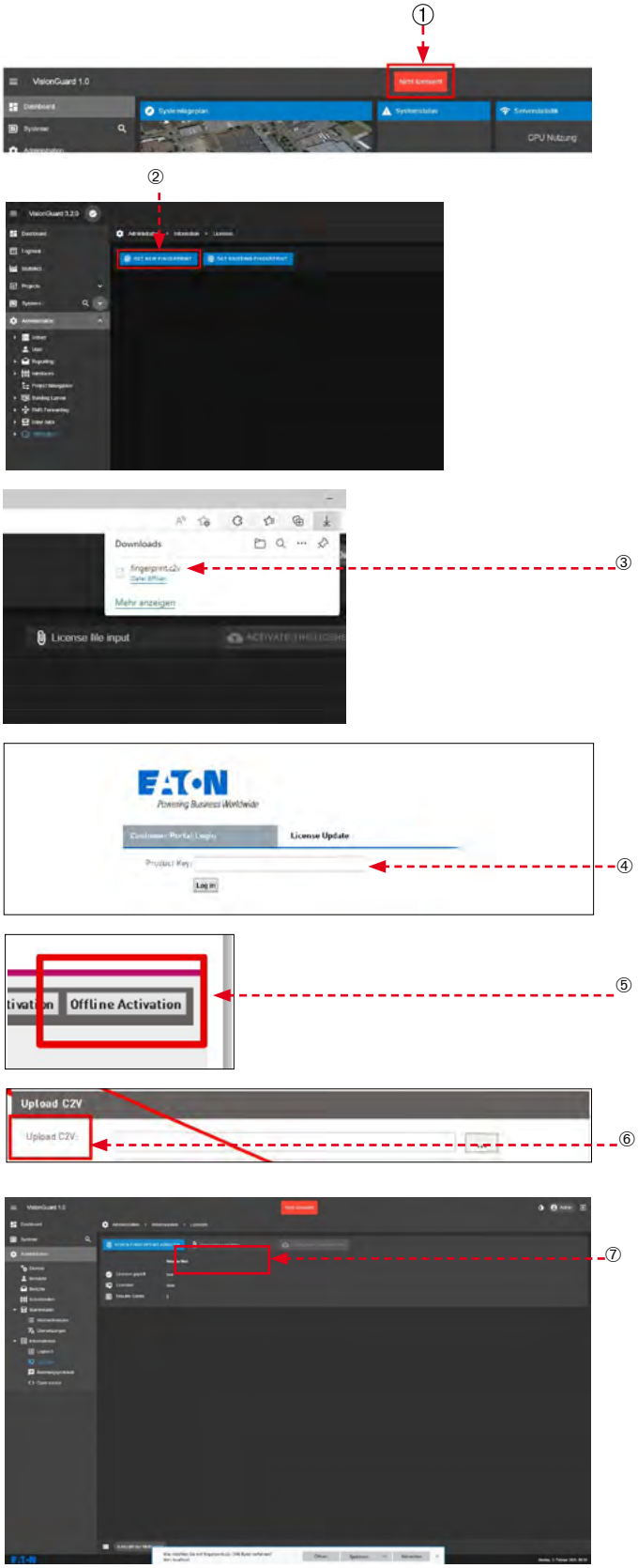
Note: An internet connection is required!

④ To log in, enter the 32-digit product key you purchased in the "Product Key" field. This is in the format: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

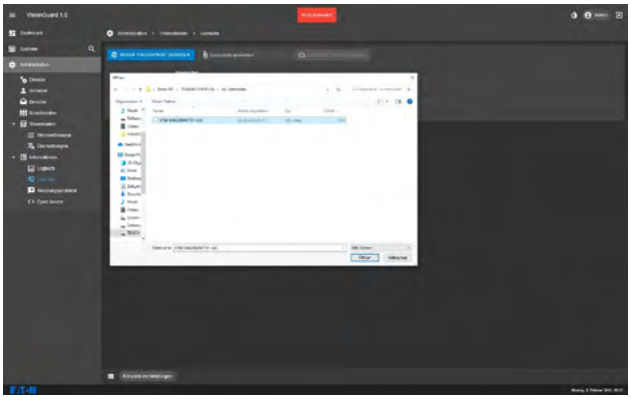
⑤ After logging in, enter your name and contact data in the activation register (optional).
Select "Offline Activation" in the upper right-hand corner.

⑥ Now upload the fingerprint created in VisionGuard in the "Upload C2V" field by searching for and selecting the source, e.g. USB stick via "...".

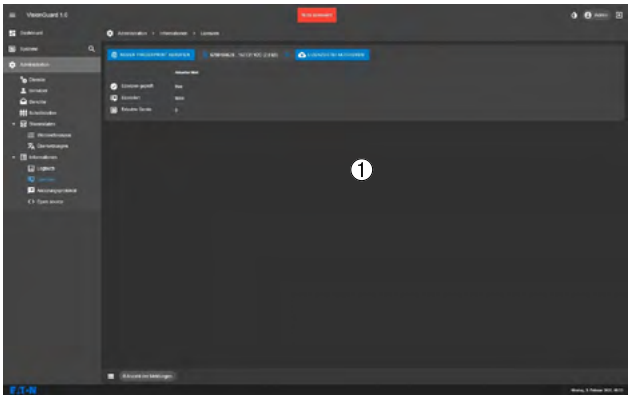
Click "Generate" for the licence server to generate an activation key, which can be downloaded to the local data medium, e.g. **C:\temp** or an USB stick.
⑦ The activation key can be uploaded into VisionGuard by via "Select licence file"



You can now specify the location of the activation key in the dialog box

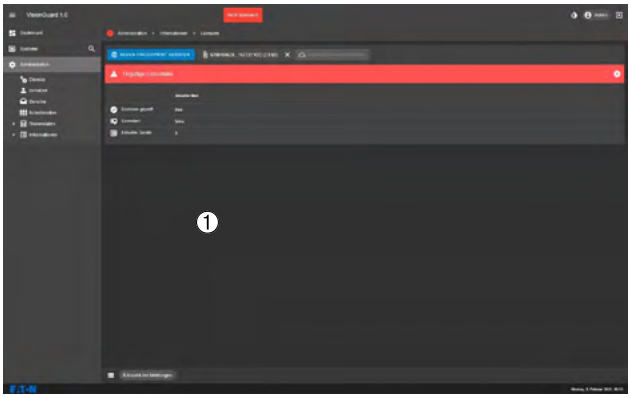


① The purchased licence can be activated in VisionGuard by clicking "Activate licence file"



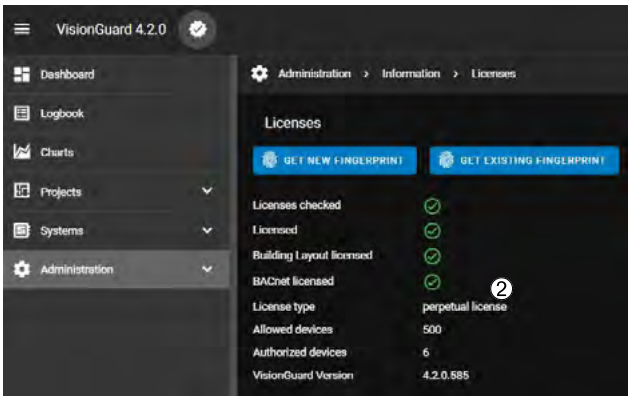
① The message "Invalid licence file" then appears

The keyboard combination "Ctrl" and "F5" clears the web browser cache and refreshes the web page



① Once the web page has reloaded, activation is now complete! This is indicated by the white seal
② The licence type and volume licence purchased are displayed here, which indicates how many emergency lighting systems can be connected to VisionGuard

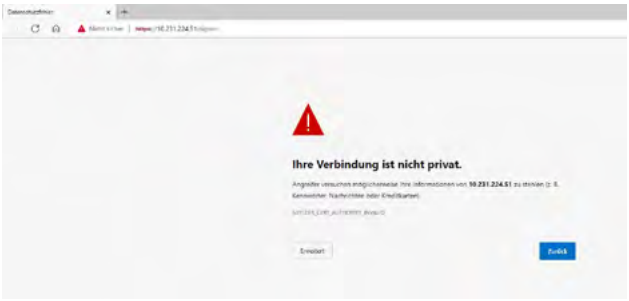
The picture shows activated licences for
- VisionGuard 500
- Building Layout Programming
- BACnet/IP-Interface (DG-S/CGLine+)



5. Security certificate installation

Foreword

If you access VisionGuard using the encrypted HTTPS protocol, security certificates must be installed in the web browser to prevent the web browser from classing the access as insecure and displaying a certificate error:



This section describes the certificate installation on the VisionGuard Server! (local access). For a certificate installation on a client PC, please contact your IT department for support.

Important:

After changing the certificate, the "Visionguard Proxy" service must be restarted!

Administrator rights are required to exchange the certificates and restart the proxy service.

5.1 Terms

Certificate
Record for authentication.

Server certificate
Certificate that confirms the authenticity of a device.

Self-signed certificate
Certificate issued without a root certificate or by a private certification authority.

Certification authority
Organization that can issue certificates. There are official ones, which are automatically accepted by browsers, and private ones, which have to be added to the browser manually.

Root certificate
Certificate of a certification authority with which a certificate can be issued.

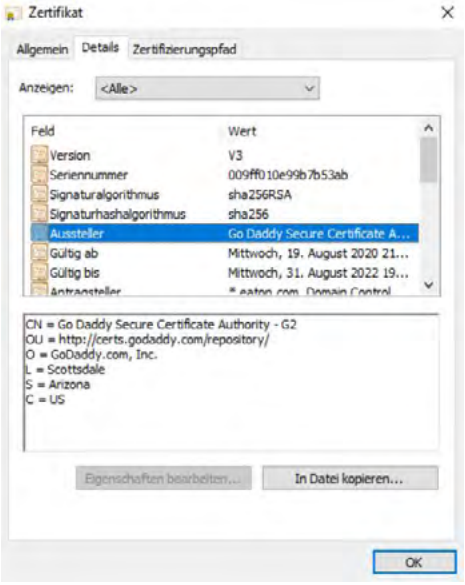
Key
Randomly generated numerical code that is included in the certificate and used for communication.

5.2 Checking the validity of a certificate

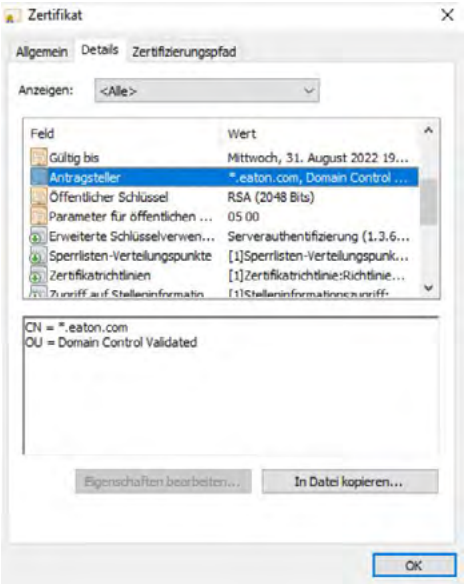
The web browser checks the validity of the certificate when VisionGuard is called up.

For the browser to recognize the new certificate as valid, the following criteria must be met, among others:

- The certificate must be issued to at least the host name or URL of the computer.
- If the VisionGuard is accessed via IP address, the IP address must also be included in the certificate.
- In addition, the entry "localhost" can be useful for local access
- The certificate must have been created with a root certificate
- This can be a root certificate created by yourself or optimally from a trusted certificate authority
- A self-created root certificate must be added to the certificate store of the client PCs.
- The certificates must not be expired



For a public site such as **www.eaton.com**, the server certificate is created by a trusted certificate authority. Which one this is and what the complete certification path is can be queried in the browser.



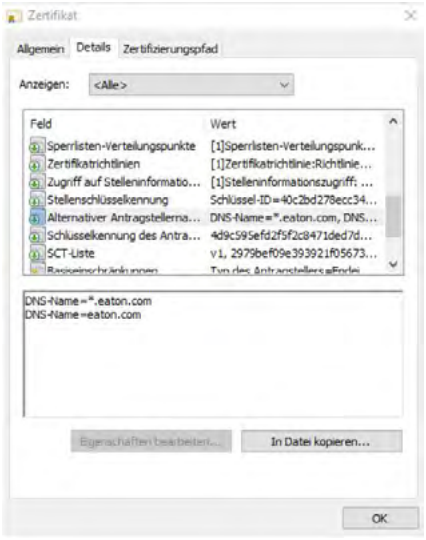
The current browsers have all already imported the root certificates from the trusted certificate authorities.

Therefore, if a server certificate issued by such a certificate authority is used for VisionGuard, the website is automatically recognized as secure by all browsers.

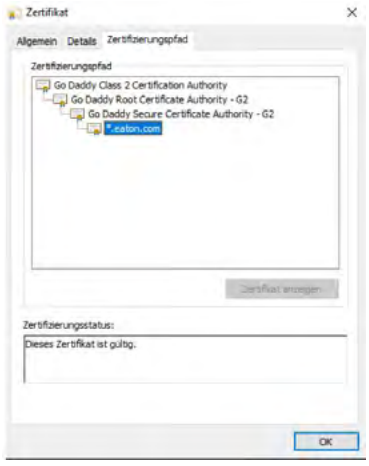
If a self-created root certificate is used for the server certificate, this must be installed on every computer/browser with which the VisionGuard is called up.

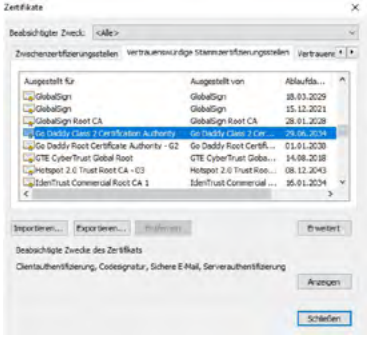
If necessary, this can be done automatically by the IT department within the company.

For the installation of the root certificate, see “Installing the root certificate”.



1. The approximate procedure when a browser calls up the VisionGuard:





1.

2.

3. For e.g. URL https://www.eaton.com/visionguard (subdirectory on **eatom.com**)

4. or also https://visionguard.eaton.com (subdomain of **eaton.com**)

5. An encrypted TLS connection is established.

6. The server certificate is retrieved.

7. Valid from, Valid to, Purpose, ... are checked.

8. The called URL is compared with the DNS entry in the server certificate.

9. Here the wildcard allows also the subdomains of **eaton.com**. This can also be different.

10. The certification path is checked if the main issuer is known and valid.

11. If all conditions are fulfilled, the web page is recognized as valid by the browser.

5.3 Use pre-installed server certificate

The VisionGuard has a pre-installed server certificate which is used by default.

The pre-installed certificate is only issued to the local server with our root certificate EatonCA.
The root certificate is located under
C:/program files/EATON/Visionguard/Certs/cert_proxy.crt.

The certificate is only valid when accessing the VisionGuard via **https://localhost**

For the installation of the root certificate, please follow the steps according to chapter **„5.5 Install root certificate“ on Page 29**

Your own certificate can be copied to the VisionGuard and used. See **„5.4 Use own server certificate“ on Page 28**".

5.4 Use own server certificate

A separate server certificate can also be used for the VisionGuard.

There are two options for this:

1. **Replace the pre-installed certificates with your own.**
The server certificates for the VisionGuard web server are located in the VisionGuard installation directory:
Server certificate: Cert\cert_proxy.crt
Server key: Cert\cert_proxy.pem

2. **Changing the web server configuration.**
Configuration file:
Proxy\conf\nginx.conf

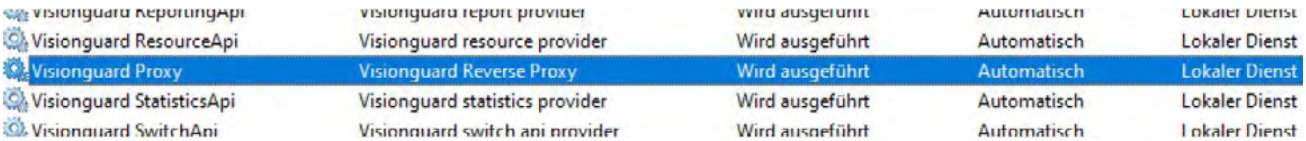
Here change the two lines to the path of your own certificates:

ssl_certificate "C:/Program Files/EATON/Visionguard/Certs/cert_proxy.crt";

ssl_certificate_key "C:/Program Files/EATON/Visionguard/Certs/cert_proxy.pem";

To change the nginx.conf file, an editor, for example Notepad, must be started as administrator and then the file opened. For this, the file filter may still have to be changed to all files.

The VisionGuard proxy service must then be restarted. (via Windows Task-Manager)



A custom server certificate can be created, for example, with the CreateCustomServerCert.bat sample batch file.

The host name, IP address and URL are queried and then the certificate is created, which can then be copied to the VisionGuard.

In addition, an organization and organizational unit must be entered. These are required purely for identification in the browser and can be of any type.

The root certificate and the corresponding key in the RootCert directory are required for this.

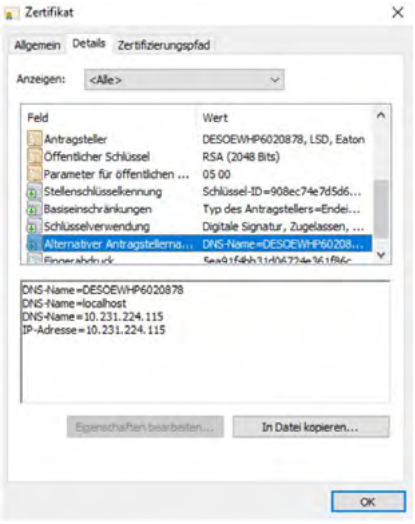
These can be your own or created beforehand with the batch file CreateCustomRootCert.bat.

Here also an organization, organization unit and additionally an issuer must be entered.

The batch call CreateCustomServerCert.bat, apart from some queries like the organization and IP address, only executes the following OpenSSL commands:

- Create 2048 bit RSA key
  - openssl req -new -key ...
  - The key strength is taken from the file openssl.cfg
- Generate server certificate
  - openssl x509 -req ...
  - Issued by the root certificate from the RootCert\ folder
  - Issued to the entered organization, IP address and domain
  - Valid for 30 years
  - The batch call CreateCustomRootCert.bat creates a new root certificate and key if it does not exist.
- Create 2048 bit RSA key
  - Only if the file RootCert\ca-key.pem does not exist
  - openssl genrsa -out ca-key.pem 2048
- Generate root certificate
  - openssl req -x509 -new ...
  - Issued to the entered organization
  - Valid for 50 years
  - The certificate and key will be stored under RootCert\.
  - The batch calls each use the OpenSSL **www.openssl.org** program.
  - The certificate and key is stored under two file names under Certs\

The certificate could then look like this:



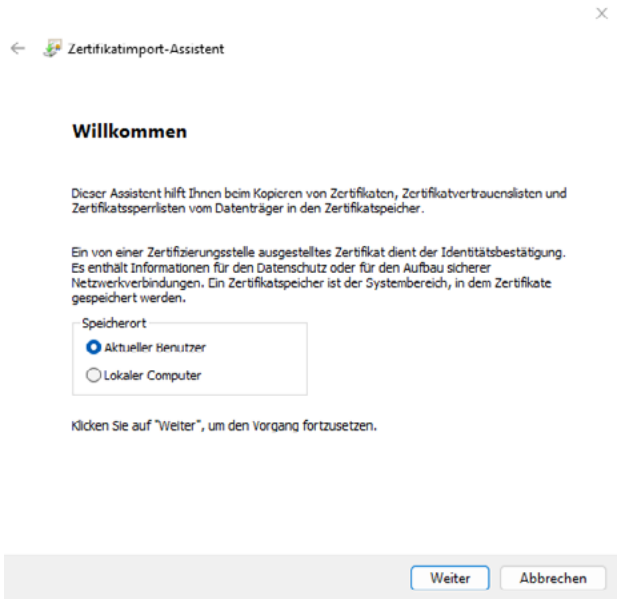
5.5 Install root certificate

In Explorer, go to the VisionGuard certificate folder ***C:/ Programs/EATON/Visionguard/Certs***. Start the certificate installation by right-clicking and “Install certificate” or by double-clicking on the certificate file “cert_proxy.crt”. The following dialog window appears:

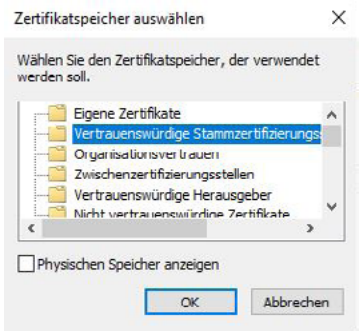
Click on "***Certifikate installation"***.

During the installation you can decide whether the certificate should be installed for the current user or all users of this PC. It is recommended to chose "***Lokaler Computer***" (all users of the current PC).

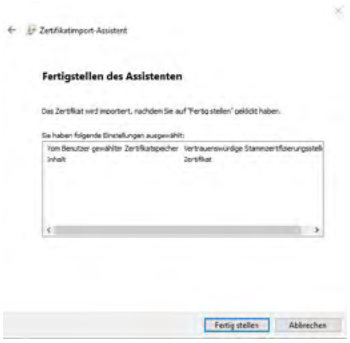
Click on "***Continue***".



In the next window click on "***Save all certificates to the following store***". Then go to browse and select "***Trusted Root Certification Authorities***"



The "***Complete the Wizard***" dialog box appears. Click "***Finish***" to import the certificate.
A message appears that the import process was successful.



The browser must then be restarted. If necessary, the "VisionGuard Proxy" service must be restarted in the task manager. To start VisionGuard without data protection errors, please enter "https://Localhost" as the address.

6.Creating new users with user roles

6.1 User Account Control (UAC) information

Any number of users with different user roles can be created in VisionGuard. Different user roles define different access rights:

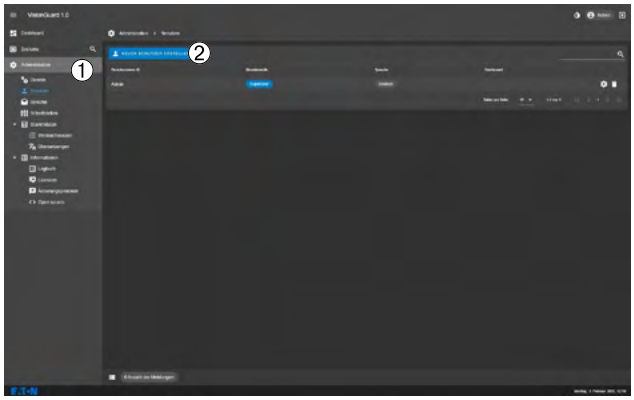
Role	Administrate UAC / Translations 1*	Administrate VisionGuard Special menus **	DG-S / LS-S, ZB-S Configuration	DG-S / LS-S, ZB-S, LP-STAR. AT-S+, CGLine+ Control	DG-S / LS-S, ZB-S, LP-STAR, AT-S+, CGLine+ Status view
Supervisior	X	X	X	X	X
Administrator		X	X	X	X
Power User				X	X
User					X

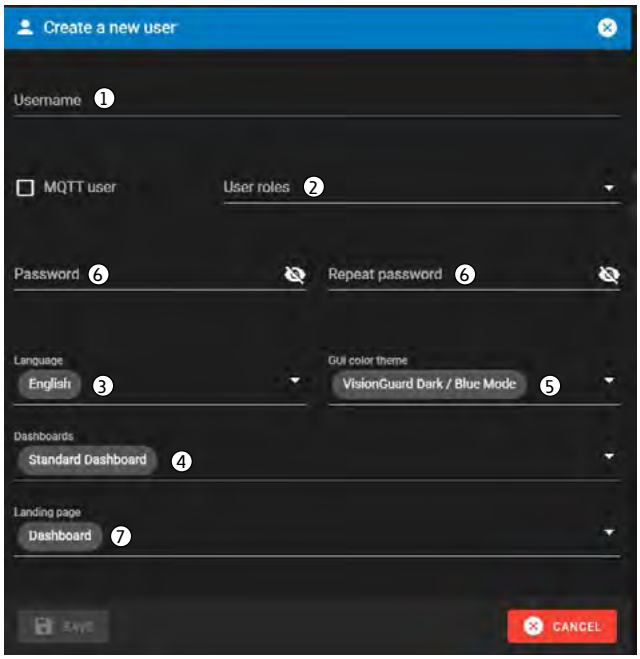
* UAC/Translations: Access to the User Account control and Translation folder to add/modify translation texts
** Special menus: Access to the Administration area with E-Mail setup

As opposed to the administrator, the supervisor also has authorization to create and edit user accounts and translations files.

It is recommended that you create only one user with supervisor rights who manages the other user accounts to avoid unwanted changes by too many people.

① You can create, edit and delete users in the Administration/ User menu
② Click "Create new user" to create a new user

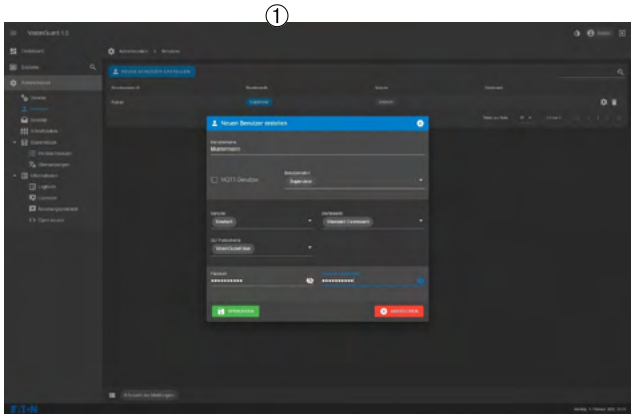




① Under User name, define the name of the new user. This is the name that is entered in the VisionGuard login screen when logging in.
② A role with different access permissions can be defined under User role (see table above)
③ Select the user language under Language. You can choose between German, English, Norwegian, French or Polish (further languages are being prepared)
④ The default dashboard is fixed and cannot be changed
⑤ Here, the color scheme can be preset for the user between the modes "dark," "light" and "blue" (dark with blue headers)
⑥ This is where the new user's password is set and must be repeated for security purposes.
⑦ With landing page, the start page can be set after logging in. This can be the Dashboard, Projects, Logbook or Systems.

① Both passwords must match in order to be able to save the new user's profile.

When the new user logs in for the first time, VisionGuard requires the entry of a new secure password in accordance with cyber security guidelines!



7. Adding DualGuard-S or LoadStar-S systems to VisionGuard

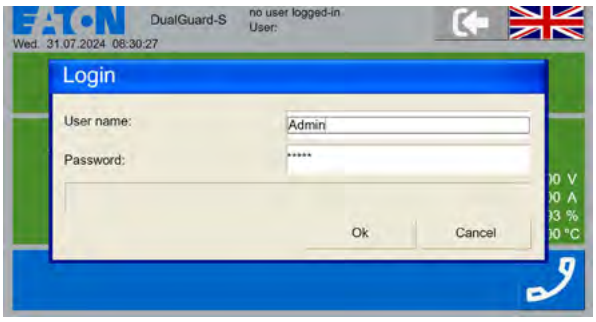
7.1 Configuring the HMI to connect to VisionGuard

In order to add a Dualguard-S system or LoadStar-S on VisionGuard, connection settings must be made on the HMI.

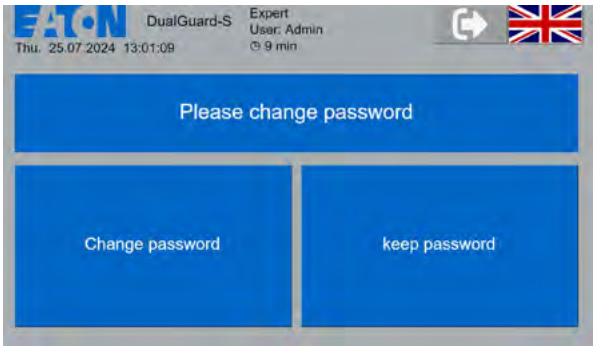
IMPORTANT NOTE

To be able to make the connection settings to VisionGuard in the HMI menu, you must be logged on as an "Expert."
The connection settings can be made directly on the HMI or ideally via web access.
Log on to the HMI:
https://"IP-address of the HMI"/webvisu.htm

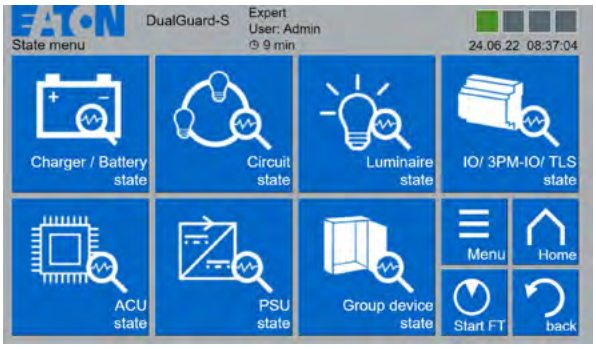
Enter your user name and password (user must be logged in as "***Expert***").



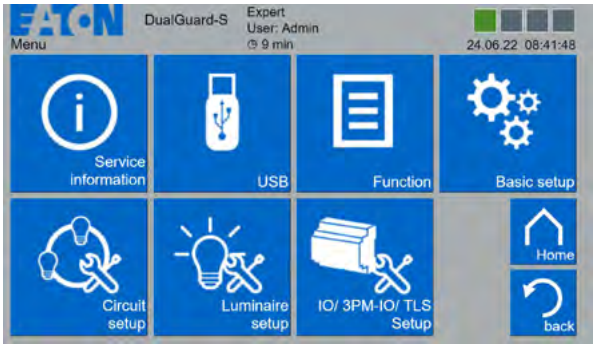
A message screen appears to change the password to a new save password.
Click on "***Change password***" to change the passoword according to password rules.
To keep the password, click "***keep password***" to enter the menu.



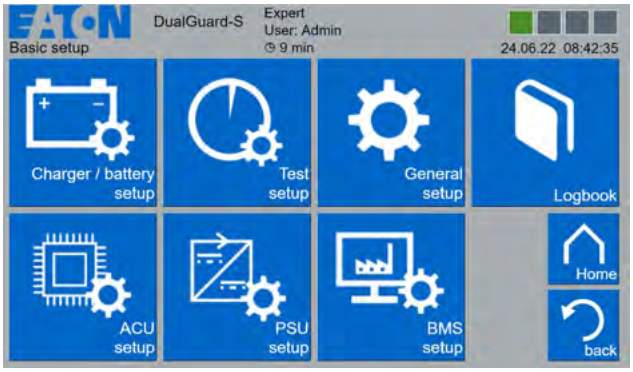
Click "***Menu***" to proceed



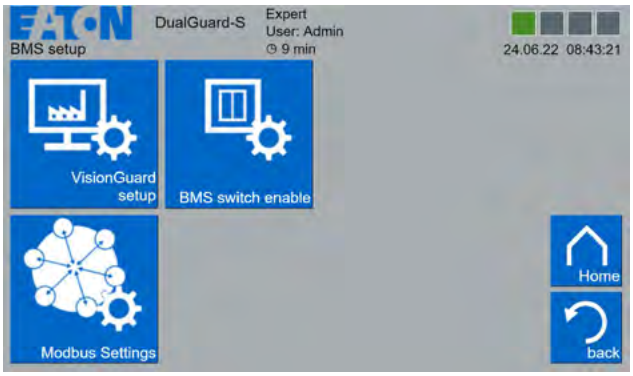
Then click "***Basic setup***"



Then click "BMS setup"

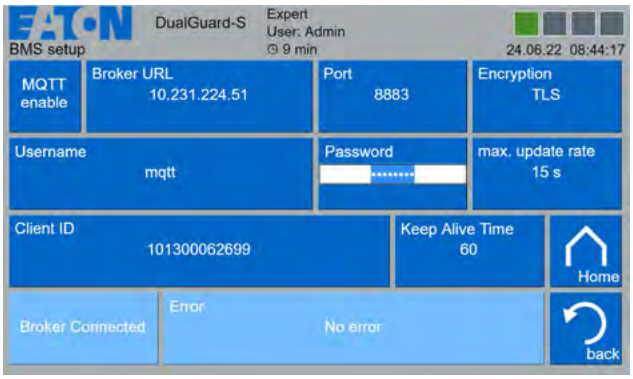


Then click "***VisionGuard setup***"



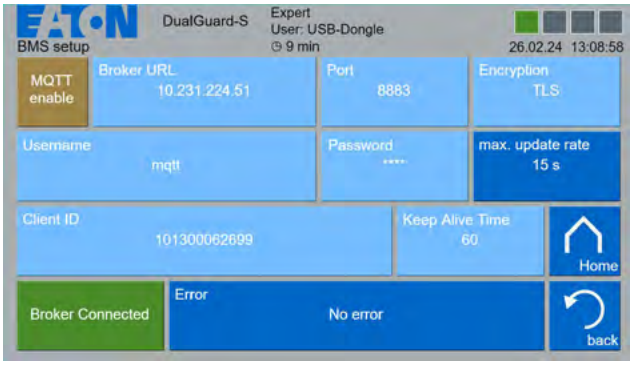
The following entries must be made in the "VisionGuard settings" menu:

- "***MQTT enable***" must be inactive (blue display)
- The IP address of the VisionGuard Server PC must be entered in "Broker URL"
- "***Port***" can be 1883 (unencrypted) or 8883 (encrypted). Encrypted is strongly recommended
- "***Encryption***" must be on TLS on port 8883
- "***User name***" must be identical to the MQTT user in VisionGuard
- "***Password***" must be identical to the MQTT user password in VisionGuard see more in: **„7.2 Adding and authorizing a DualGuard-S or LoadStar-S system in VisionGuard“ on Page 34**



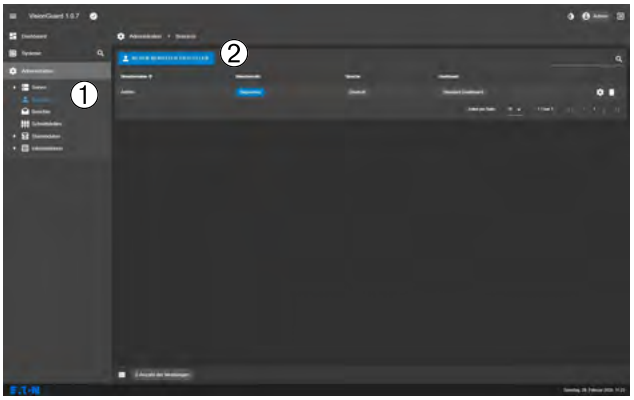
The MQTT interface can be activated after making the above settings. Click on „***MQTT enable***“. The HMI now attempts to establish a connection to VisionGuard. To do so, the HMI must now be authorized in VisionGuard.

See Section **„7.2 Adding and authorizing a DualGuard-S or LoadStar-S system in VisionGuard“ on Page 34„.**



7.2 Adding and authorizing a DualGuard-S or LoadStar-S system in VisionGuard

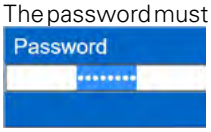
In order for DualGuard-S or LoadStar-S systems to be added in VisionGuard, an MQTT user must be created in VisionGuard.
① This is done in the Administration/User menu
② Create a new MQTT user by clicking "Create new user"



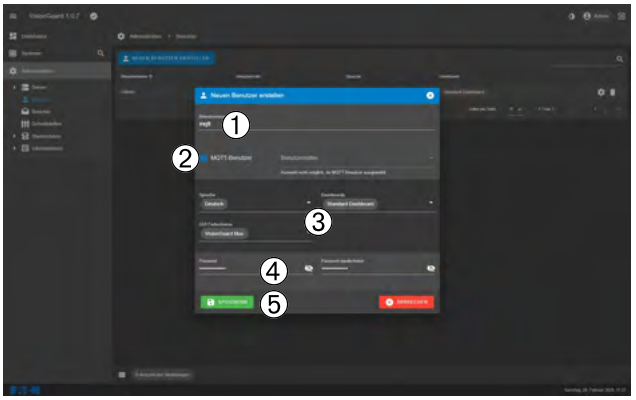
The following settings must be made in the next dialog box:

① The user name must be identical to the user name in the HMI. "mqtt" is recommended for simplicity

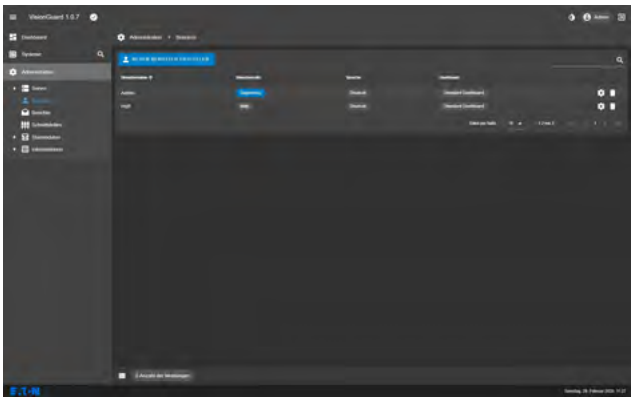
② MQTT user must be checked
③ Any settings here are not required
④ The password must be identical to the password in the HMI



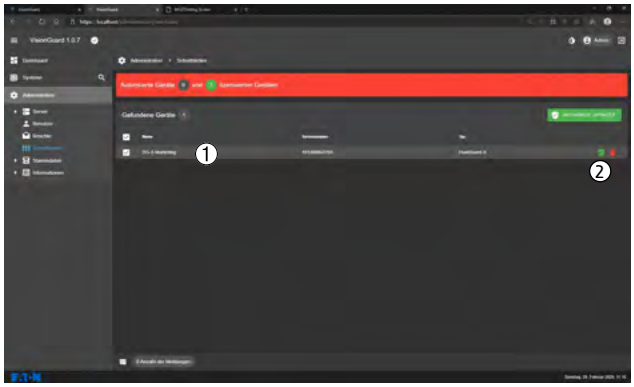
⑤ Click "Save" to apply the settings



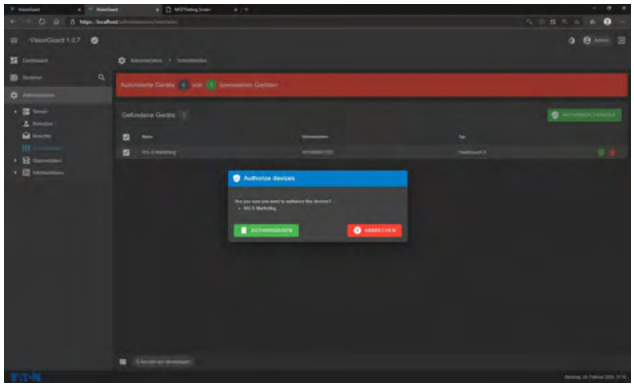
The user for the connection (here with the name mqtt) has now been created



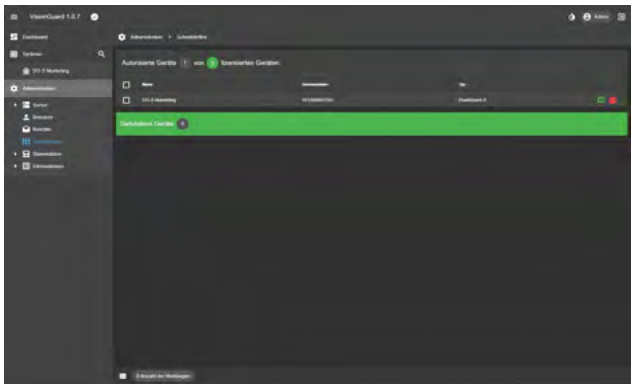
① If the settings in the HMI of the DualGuard-S or LoadStar-S match the settings of the mqtt user in VisionGuard, DualGuard-S or LoadStar-S is displayed in the Administration/Interfaces menu
② Click "Authorize device" to add the DualGuard-S or LoadStar-S to VisionGuard



Confirm by clicking "Authorize"



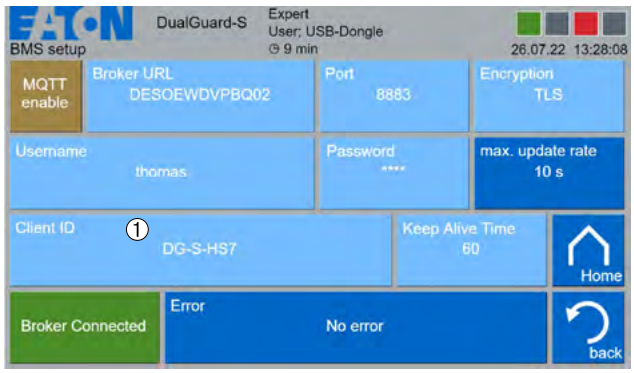
The DualGuard-S or LoadStar-S has now been successfully registered in VisionGuard



IMPORTANT NOTE

After registering a DualGuard-S or LoadStar-S, the configurations are loaded. This process can take up to 15 minutes! It is recommended not to carry out any other operations in the VisionGuard after creating systems until the configurations have been completely loaded!
This can be checked in the system overview. All installed components must be visible, e.g. PSU, ATSD (SKU), luminaires etc.

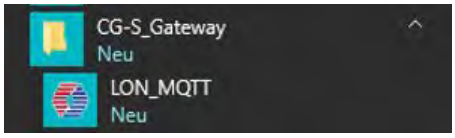
① The correct connection between the HMI and VisionGuard is now displayed in the HMI (green)



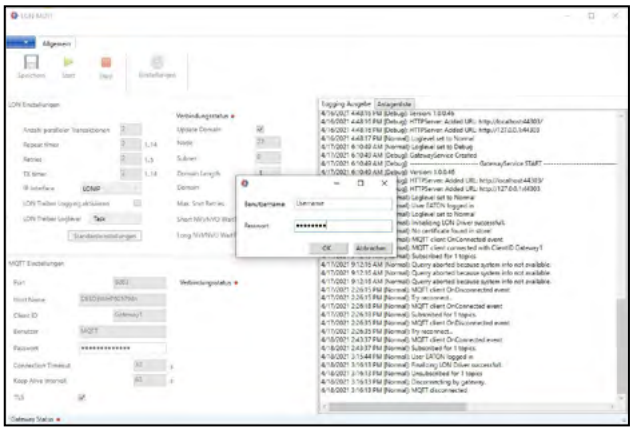
8. Adding CG-S (ZB-S, LP-Star, AT-S+) systems to VisionGuard

8.1 Configuring the CG-S Gateway

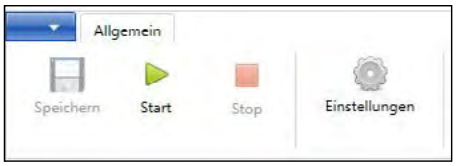
Start or open the CG-S Gateway software
"***LON MQTT***" (must be started as Administrator)



Please enter the user and password you assigned in chapter 2.2.

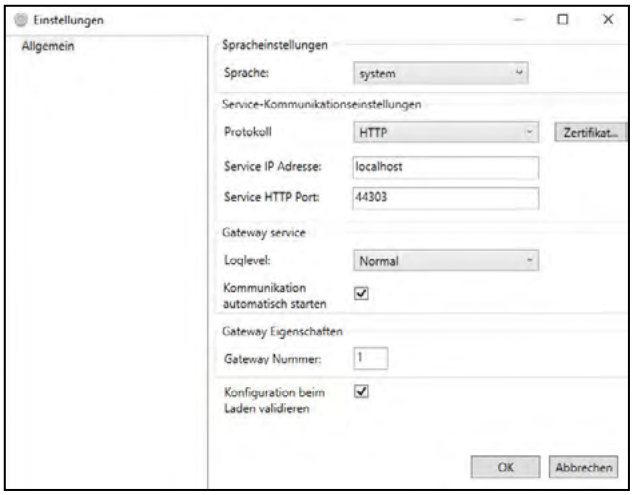


First it is important to setup or check the settings (***Einstellungen***) of the Gateway.
Please open Settings (***Einstellungen***)



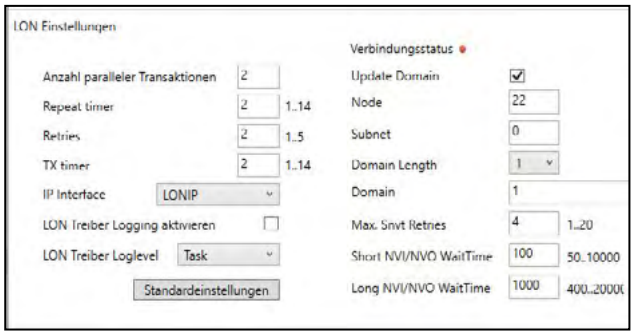
In the settings please check following settings:

Language (Sprache): You can use Win System or between German and English language
Protokoll: HTTP or HTTPS, If you choose HTTPS, you have to install a certificat (Zertifikat)
Service IP address: localhost or the IP address of the VisionGuard server network address
Service HTTP port: 44303
Gateway service: Please activate "Start Communication Automatic" (Kommunikation automatisch starten)
Gateway Number: 1
And click OK to confirm the settings



Then select in the part of LON-settings (LON Einstellungen), the right IP Interface must be selected. Supported are the CG-S/IP-Interface (USB Dongle or Soft licence) and the CG-S/USB-Interface.

For the CG-S/IP-Interface the right setting is:
LONIP
For the CG-S/USB-Interface the right setting is:
LONUSB

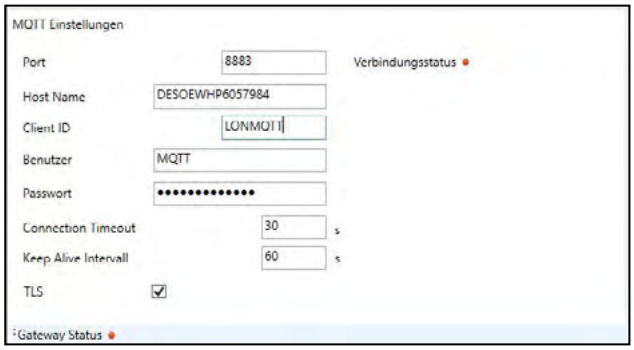


IMPORTANT NOTE

Other settings not required.
Please leave the default settings!

Under MQTT Settings following settings must be selected correct:

Port: 8883
Hostname: Name of the PC or the IP address of the VisionGuard Server
Client ID: LONMQTT (default)
User/Benutzer: Must be exactly the same MQTT user of the VisionGuard (see section "**Adding and authorizing a DualGuard-S or LoadStar-S system in VisionGuard“)**
Password/Passwort: Must be exactly the same password of the MQTT user of the VisionGuard (see section **„Adding and authorizing a DualGuard-S or LoadStar-S system in VisionGuard“)**



Connection Timeout: 30S
Keep aAlive Intervall: 60s
TLS: Must be activated

Now settings must be saved via the save button (Speichern). To test the correct working of the gateway, it can be started via the Start button (Start)

The correct operation of the gateway will be displayed via the connection display (Verbindungsstatus) in the LON and MQTT settings. The flag must appear in green.
A red flag indicates a not correct working Gateway. Please check the right settings again

8.2 Adding and authorizing a CG-S system (ZB-S, LP-Star, AT-S+) in VisionGuard

PLEASE NOTE:

To add a CG-S system in the VisionGuard, you must be logged in at least as Admin or Supervisor!
VisionGuard is designed to take over structures and data from an existing CGVision visualisation software, which has a group/system structure that has mapped up to 32 emergency lighting systems in up to 15 device groups.

This group structure for CG-S systems has been retained in VisionGuard, but is not visibly used for subsequent visualisation in the Explorer structure.
Preparation: To add a CG-S system, the Neuron ID and the device number (1-32) must be determined from the CG-S control unit CU-CG-S. Please refer to the operating instructions for the ZB-S, AT-S+ or LP-STAR.

Please go in the "***Administration***" menu to the sub menu "***Interfaces***" and "CG-S"

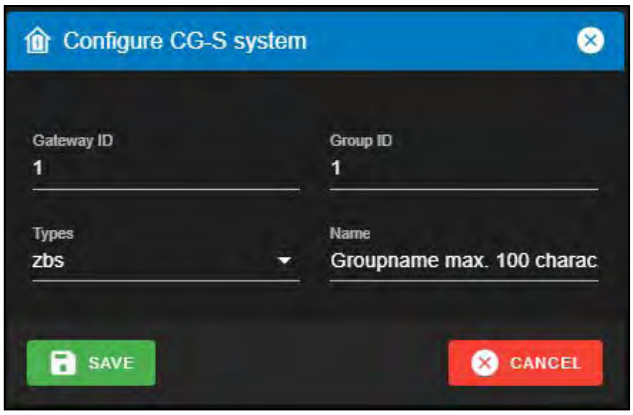
8.2.1 Creating new CG-S groups and adding and authorizing CG-S (ZB-S, LP-Star, AT-S+) systems in VisionGuard

PLEASE NOTE:

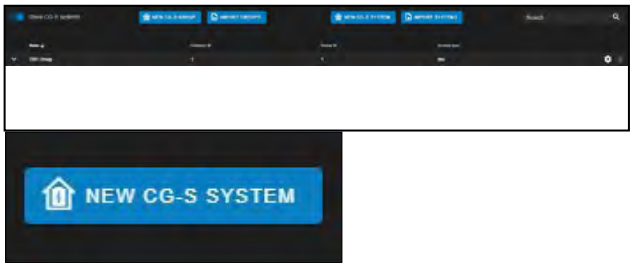
Any number of CG-S groups can be created, each with up to 32 ZB-S, AT-S+ or LP-STAR systems can be formed. The device types cannot be mixed. This only serves the purpose of logical group assignment, which is later visualisation display in the VisionGuard visualisation display. To create a CG-S group, please click on the blue button blue "NEW CG-S GROUP" button

In the Configure CG-S system window please enter:

Gateway ID:	1
Group ID:	Desired ID from 1-16
Types:	ZB-S, LP-Star or AT-S+ (AT-S+ Dual System, AT-S+ Generator or AT-S+ Loadstar)
Name:	Desired group name with max. 100 characters



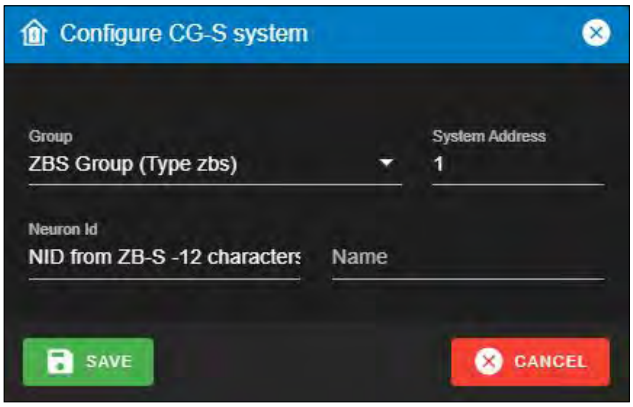
Click “Save” to overtake the settings.
The new CG-S group appears in the list
Please repeat above steps to create additional CG-S groups



To add CG-S (ZB-S/AT-S+/LP-STAR) systems to the created CG-S groups please proceed as follows.
Click in this picture on the blue button
“NEW CG-S SYSTEM”

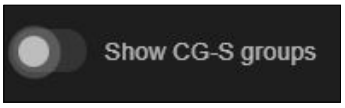
In the following window please enter:

Group: Select here one desired created CG-S group, e.g. ZB-S
System Address: System Address from the ZB-S 1 to 32
Neuron ID: Enter here the Neuron ID from the CG-S control module with exact 12 characters
Name: The name with the ZB-S with up to 20 characters is automatically uploaded from the ZB-S to the VisionGuard when the configuration is loaded.

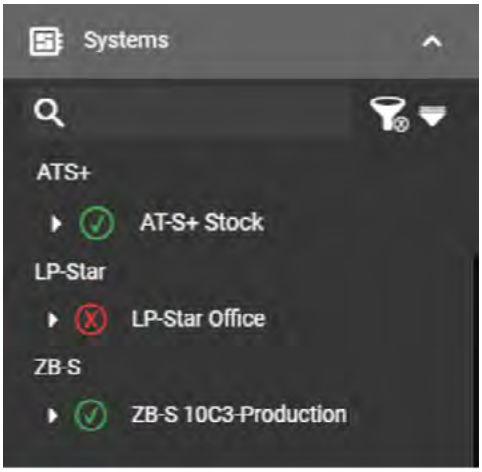


Click “***Save”*** to add the CG-S (ZB-S, LP-Star, AT-S+) system in the VisionGuard.
Please proceed in the same way with all other CG-S systems that you would like to integrate into the VisionGuard. All CG-S systems appear in a list.

Via „***Show CG-S groups***“ or „Show CG-S systems“ you can switch the list view accordingly.



After the whole procedure, the added CG-S system are now visible and operable in the „***Systems***“ menu tree



IMPORTANT NOTE

Depending on the size of the system, loading the configuration may take several minutes! Please allow load the configuration completely before making any further setting changes on VisionGuard!

8.3 CGVision import of CG-S systems (ZB-S, AT-S+ and LP-STAR) into VisionGuard

VisionGuard V4.2.1 has a CGVision import function for CG-S systems.
The import function makes it possible to transfer a backup from an existing CGVision visualisation to VisionGuard. This import function is described in a separate manual, which is available on request.

9. Adding CGLine+ Web-Controller / CGLine+ Compact-Controller 160 or 400 to VisionGuard

9.1 Adding and authorizing a CGLine+ Web-Controller / Compact-Controller 160 or 400 in VisionGuard

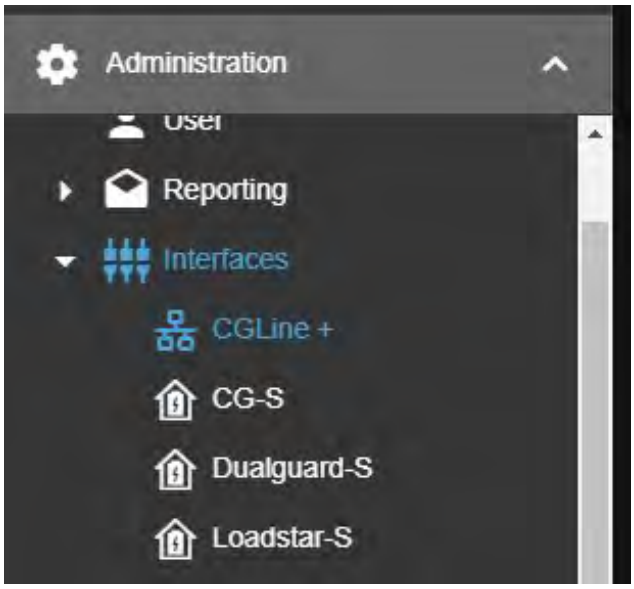
IMPORTANT NOTE

To add a CGLine+ Web-Controller / Compact-Controller 160 or 400 in the VisionGuard you must be logged in as Administrator or Supervisor!

Preparation: To add a CGLine+ Web-Controller the IP address must be known and the communication port must be right adjusted. Please see the manual of the **CGLine+ Web-Controller**.

This chapter describes how to add and authorize a CGLine+ Compact controller. Please proceed in the same way with the CGLine+ Compact Controller 160 or 400.

Go to "***Administration***" menu, "I***nterfaces***" and select "***CGLine-Plus***" sub menu from the dropdown list.

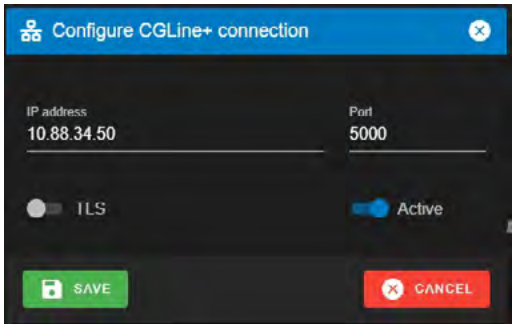


To add a CGLine+ Web-Controller click on "NEW CGLINE+ DEVICE".

Please enter in the next window:

- IP address (IPV4)
- Port
- TLS encryption Active/Not active
  Unencrypted Standard port is 5000
  TLS Encrypted Standard Port is 5050
- Active (Must be enabled!)

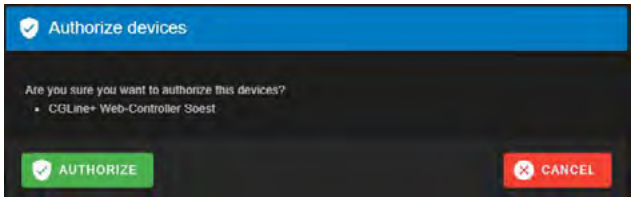
Click on “Save” to overtake the settings



Now the CGLine+ is listed under New CGLine+ device.
A green connection status shows the correct communication.

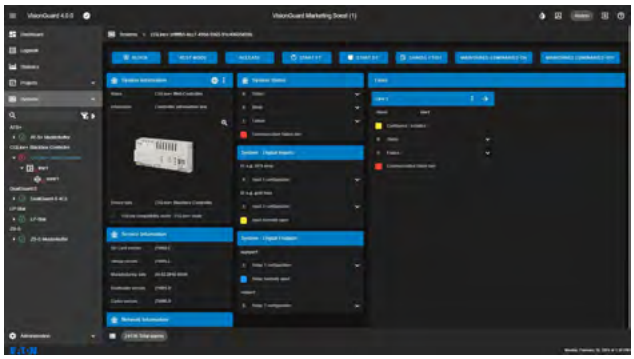
To authorize the CGLine+ Web-Controller please click in menu “Interfaces” on the green flag of the Controller ① .

Click on “Authorize”.



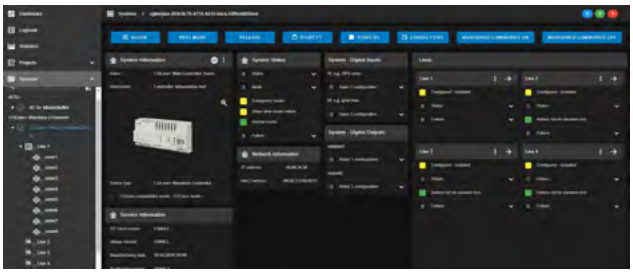
The CGLine+ Web-Controller appears now under “Authorized devices” with green connection status.

The CGLine+ Web-Controller is now listed under the Systems menu. The VisionGuard starts now a download of the Controller configuration. This can take some minutes. Please don`t do further activities during the download of the configuration.



The configuration is successfully downloaded, if the configured lines and zones are visible under the CGLine+ Web-Controller ① .

The CGline+ Web-Controller is now ready to use. For more information see **„13. CGLine+ Web-/Compact 160/400-Controller“ on Page 62**.



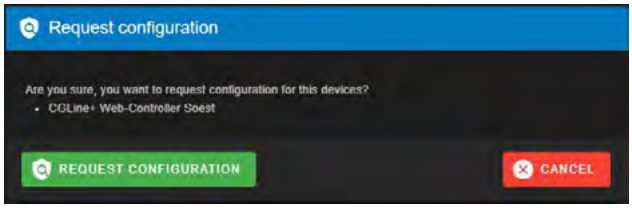
Please proceed in the same way with all other Web-Controller / Compact-Controller 160 or 400 that you would like to integrate into the VisionGuard.

9.2 Manual loading of the CGLine+ Web-Controller / Compact-Controller 160 or 400 configuration

In case of changing the CGLine+ Web-Controller / Compact-Controller 160 or 400 configuration via the CGLine+ PC-software, it is necessary to download the new configuration manually.

For this please navigate to the menu “***Interfaces***” in the ***Administration*** menu.

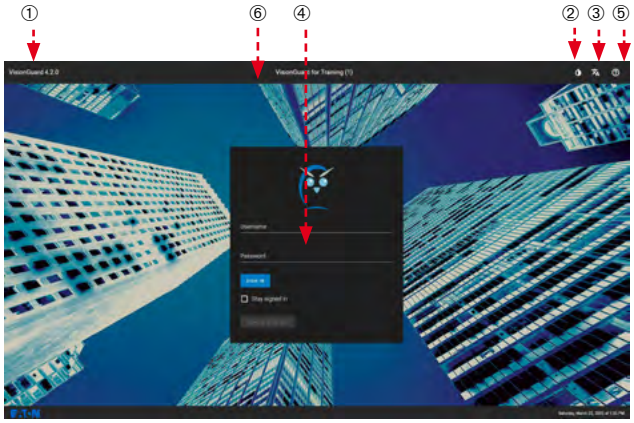
To load the configuration, please click on the green flag of the CGline+ Web-Controller / Compact-Controller 160 or 400



Please proceed in the same way with all other CGLine+ Web-Controller / Compact-Controller 160 or 400 that you would like to integrate into the VisionGuard.

10. Basic graphic layout and structure of VisionGuard

10.1 Login screen



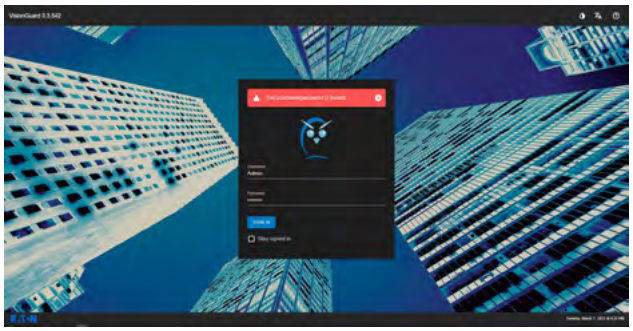
When you open VisionGuard via a web browser, the login screen appears

① Display of the current VisionGuard version (here e.g. V4.2.1)
② Light/dark mode setting
③ Login language setting German/English/Norwegian/ French/Polish
④ User name and password fields. By clicking "Stay logged in," you can open VisionGuard any time within a period of 8 hours without reentering the user name/password, provided the tab in the browser was closed **without** logging off.
⑤ ***?*** Symbol is a Hyperlink to the VisionGuard www. download page with the possibility to check the latest VisionGuard version, CG-S Gateway and CG-S driver package.

Note: Internet connection is required.

⑥ VisionGuard name of max. 100 Characters

If the user name or password is entered incorrectly, an error message appears



If the login data is correct, the VisionGuard dashboard opens as the start screen

NOTE

It is possible to exchange the background image for your own image one.

The folder on the VisionGuard server PC installation for the background image is: **C:\Program** Files\EATON\Visionguard\ Proxy\html\img\app-signin-background.jpg

It can be replaced by a new .jpg with a size of 1920x1080 pixel.

The name of the image must be a .jpg with the name "app-signin-background.jpg"

It is recommended to rename the original image first.

10.2 Dashboard

The dashboard is used to clearly display information about VisionGuard and any connected emergency lighting systems in various charts.

① Navigation area for navigating directly to the VisionGuard submenus

② Dashboard widgets – the dashboard consists of seven defined widgets

10.2.1 Device statistics summary (device status overview)

The "Device statistics summary" widget clearly shows the status of all connected devices in a graphic:

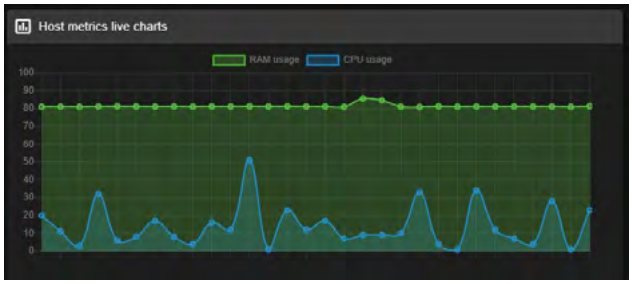
System count = number of connected systems
Connected = number of devices where communication between VisionGuard and device is OK
Ready for operation = number of devices that are ready for operation
Failure = Number of devices with a fault without a luminaire fault
Luminaire failure = Number of devices with a luminaire fault
Revision mode = Number of devices which are in Revision mode (Construction Site)

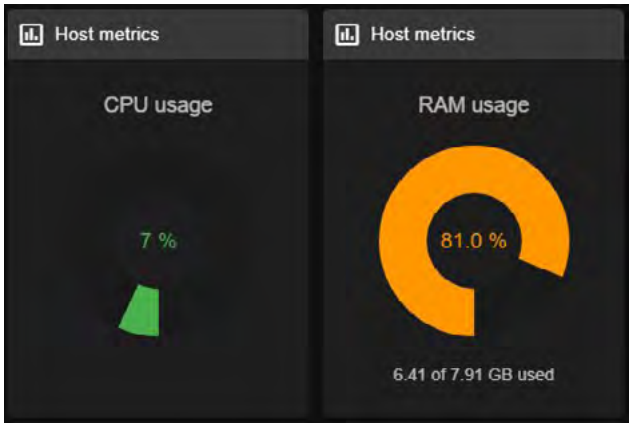
10.2.2 Communication status

The Communication status widget shows which device's communication with the VisionGuard is OK (green) or faulty (red). Click on the arrow to open the system overview of the device.

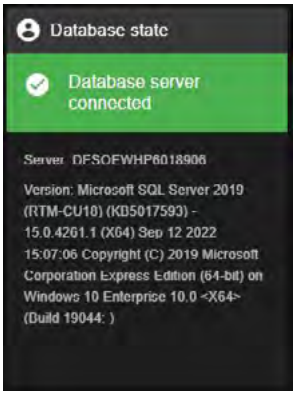
10.2.3 Server statistics

The Host metrics widgets provide information about the current processor and memory usage, each individually in a pie chart and together over time in a line chart. This information is important to get an overview of the current system performance for VisionGuard. This can be a good help to better determine the allocation of processor cores and memory for virtual machines, for instance. If utilization is close to 100% for an extended period of time, it is strongly recommended to increase the performance, e.g. allocate processor cores or upgrade memory.





10.2.4 Database and system services status indicators



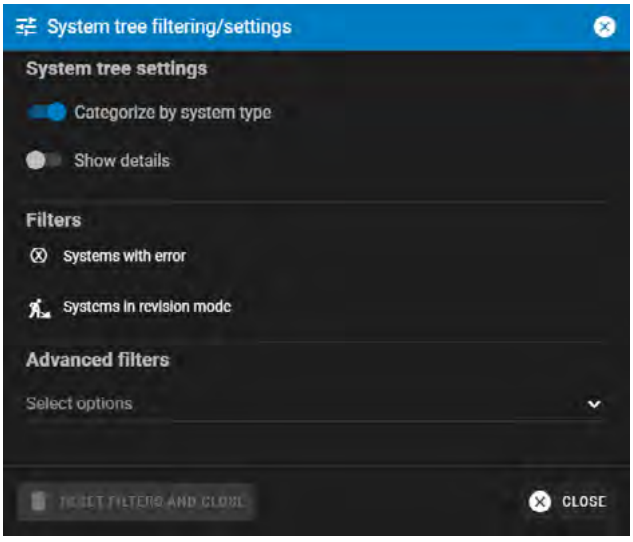
The database and system status widgets provide information about the functionality of VisionGuard. If the database server is working correctly, all data is exchanged correctly between the systems and VisionGuard. The system status widget can be used to check that all VisionGuard services are functioning correctly, e.g. the e-mail client. VisionGuard has a redundant structure, which means that if, for instance, the e-mail function is faulty, all other services will continue to run without any problems.
The widget also shows how long a service has been running or how long a service has stopped working. If a service has failed, it can be restarted easily in the Services menu (see Section **"Services"**).

10.3 System overview

In the "***Systems***" menu, all connected emergency lighting systems are clearly displayed according to device types with status. Click on the device to open the detailed view. On the left side of the menu tree, the systems are displayed in Explorer structure. With the arrow on the left, you can display the installed components, e.g. ACU with status. Clicking on a component opens its detailed view with detailed status information.

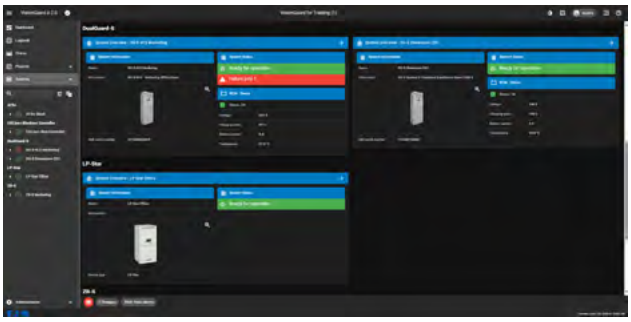
Numerous adjustments can be made via the filter menu at the top right of the system overview or in the system tree.

- Categorize by system type
- Show Details
- Systems with error
- Systems in revision mode
- Advanced filters – Select options



If "Categorize by system type" is deactivated via the slide switch, the systems are grouped according to their status, e.g. all devices with luminaire errors.

If "Show Details" is activated, each system is displayed in its own widget with details such as names, battery values, sum status, etc.

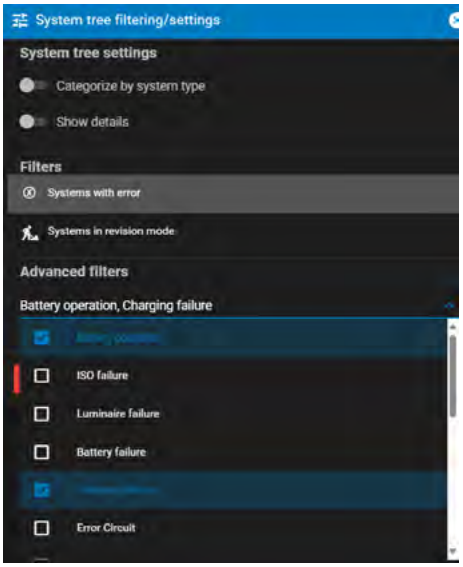


With the filter "Systems with error", only those systems that have a fault are displayed in the system overview and in the system tree, with the indication of which fault exists.

If the "Systems in revision mode" filter is activated, only the attachments that are in revision mode are displayed. You can find more information about revision mode in the separate chapter on this topic.

Via "Advanced filters", individual desired status messages such as various errors, e.g. charging fault or states, e.g. battery operation, can be selected via "Select options". Multiple selection is possible.

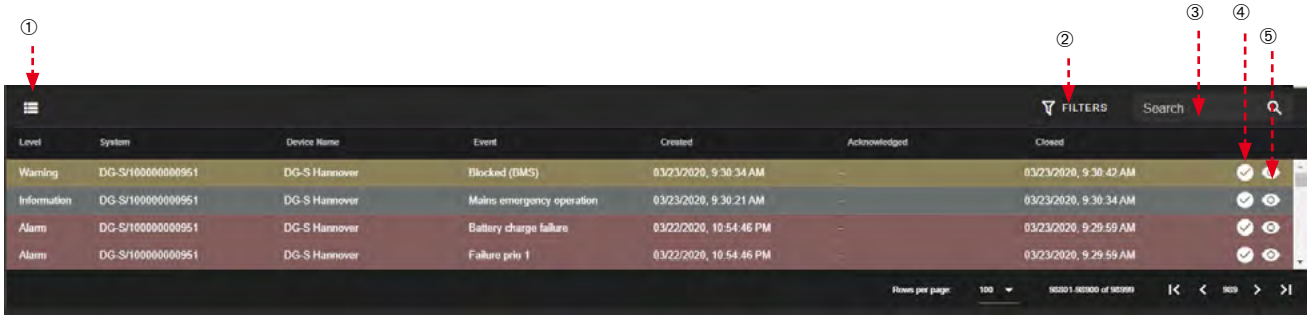
The filters can be easily reset by clicking on the red "Reset filters and close" button.



10.4 Alarm list

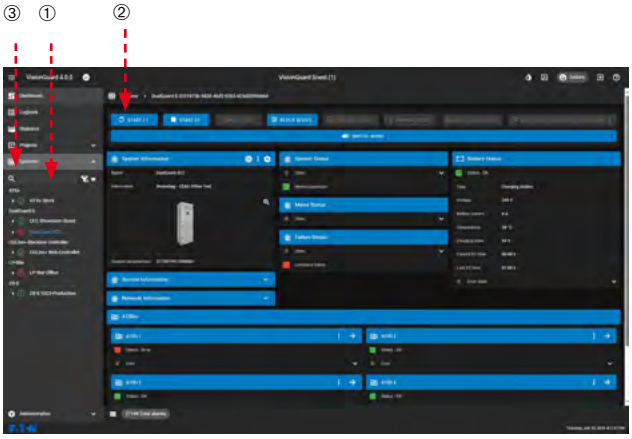
In the bottom left-hand corner of the VisionGuard display, you can show or hide an alarm list at any time by clicking on this symbol . The alarm list shows all events that occurred and when they ended, including a date and time stamp. The events are color coded by category.
Blue = command,
Grey = information,
Yellow = warning,
Red = alarm.

① Alarm bar ON/OFF display
②Filter function for filtering results by category, system or event
③ Search function for targeted search of events
④ Click here to acknowledge the event so that it is removed from the alarm list. The acknowledged events can be displayed by clicking on the "Acknowledged" slideing switch
⑤ The eye icon allows you to navigate directly to the event where it occurred



11. DualGuard-S / LoadStar-S visualisation

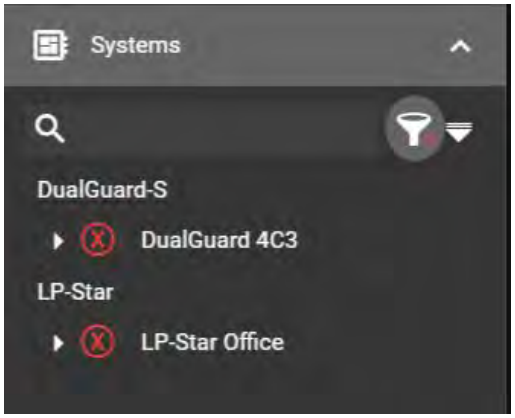
11.1 DualGuard-S / LoadStar-S detail view



Under the "Systems" menu, all DualGuard-S / LoadStar-S or CG-S systems (ZB-S, LP-Star, AT-S+) or CGLine+ Web-Controller / CGLine+ Compact-Controller 160/400 are listed with their device names in the explorer structure ①. Click on the name to see the detailed view of the device. Here you get detailed status information about the system, service information such as network settings and an overview of the installed ATSDs (SKU) with status display. In addition, the blue control buttons can be used to activate various actions on the device, such as start a function test (Start FT) ②.
Following commandos are possible:
Start FT = Start of a Function Test
Start DT = Start of a Battery Duration Test
Cancel FT/DT = Abort of a Function or Duration Test
Block Device = Block the emergency function of the DG-S
Release Device = Releases again the emergency function of the DG-S
Manual Reset = Manual reset of the emergency lighting functionaftermainspowerrecovery(ManualReset function must be configured)
Reset ISO-Failure = resets an insulation fault
Reset Deep Discharge Protection = Acknowledges the message after a terminated deep discharge protection
Switch menu = See **„11.9 Switch Menu“ on Page 55**
③ Click the arrow to the left of the device name to display the installed components in the explorer structure, which is described in the next subsections.

Icons in the menu tree show the status of the system and the installed components at any time.

A search window with real time display allows you to quickly find specific systems by name.



With the funnel icon it is possible to show only systems with failures.

Detailed description of the Icons:
- (4) System is ready for operation, no errors
- (5) Any error in the system
- (6) Function test pre run (AC mode)
- (7) Function test active (Battery mode)
- (8) Duration test pre run (AC mode)
- (9) Duration test active (Battery mode)
- (10) Communication error to the system

Description of the Widgets:

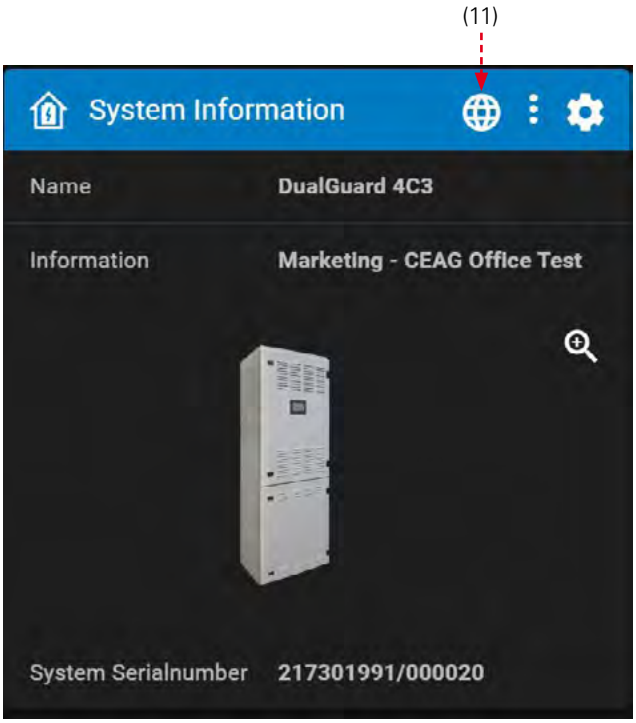
System information
Shows the name (max. 40 Character) and Information (max. 100 Character) of the DG-S /LS-S System

Via the earth icon (11) a link (new tab) to the Web visualisation to the DG-S / LS-S HMI appears

Via the gear symbol the configuration section appears

User with Administrator rights or Supervisor rights can configure the whole DG.S system

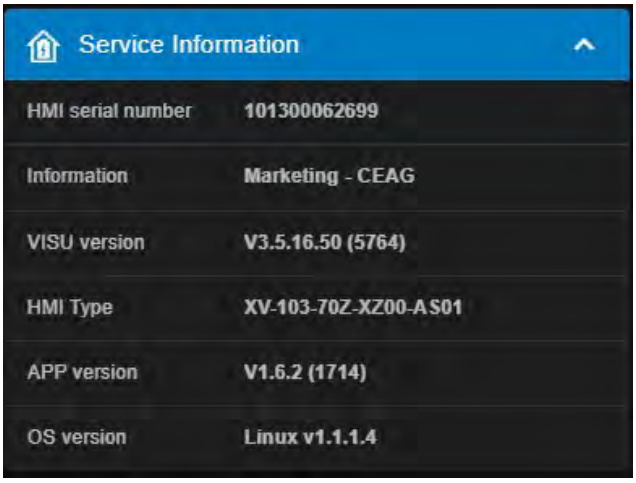
User with User rights or Power user rights can only see the configuration. Any changes of the configuration are not possible!



Service information

(Folded widget can be opened via the arrow on the right in the header)

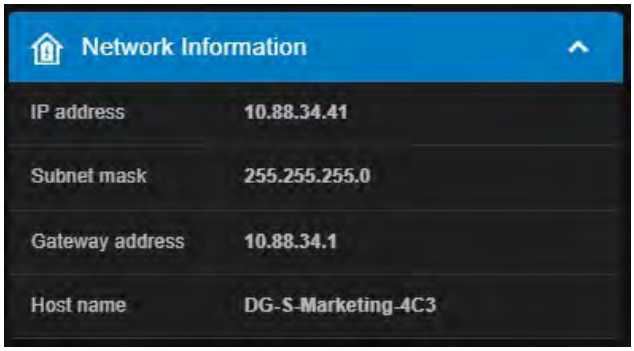
Shows all information about the software/firmware of the DG-S / LS-S



Network information

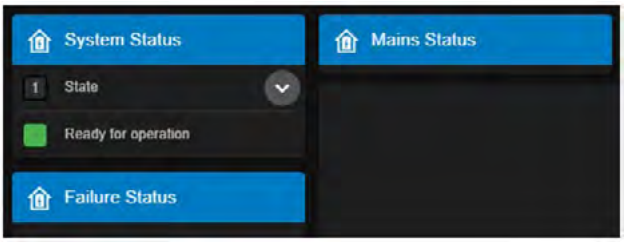
(Folded widget can be opened via the arrow on the right in the header)

Shows all information about the DG-S / LS-S network settings, such as IP-address.



System Status / Main Status / Failure Status

These Widgets shows detailed information about the system status of the DG-S / LS-S such as failure information

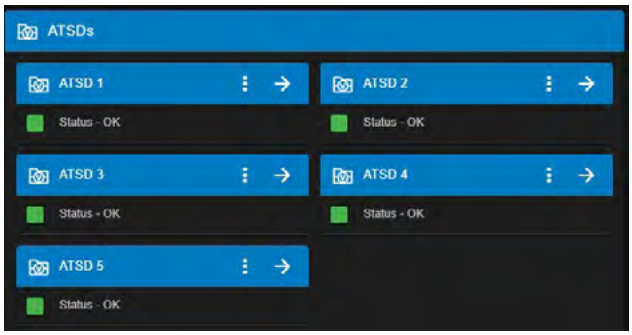


Battery Status

Shows detailed information about the analogue battery values such as Battery voltage, Charge-/Discharge current…and the current Duration test time (if the DT is active) and the last reached Duration test time

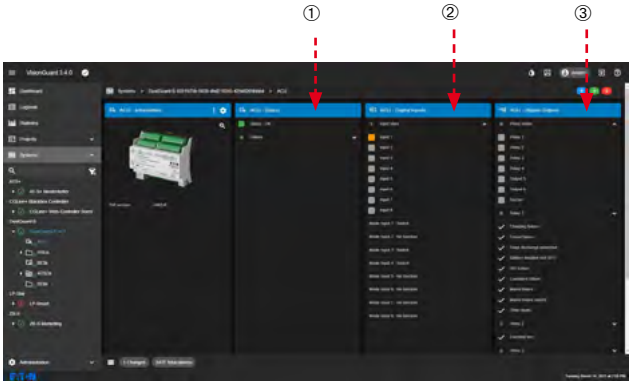
ATSDs (SKUs)

This widget shows all installed SKUs (ATSD) with a sum status. With click on the arrow right in the widget head, the SKU overview will appear.
The three dots opens a generic display with additional information to the SKU (ATSD).



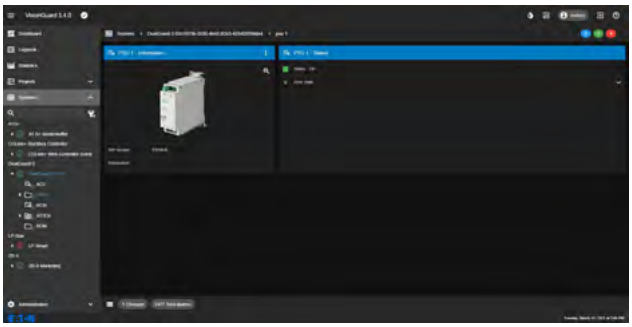
11.2 ACU detail view

The ACU detail view shows the ACU status ①, the digital input configurations ② and relay outputs ③. The configuration of the digital inputs and relays can be done with click on the gear symbol above the ACU picture or in the Administration menu "***Configuration***".



11.3 PCU detail view

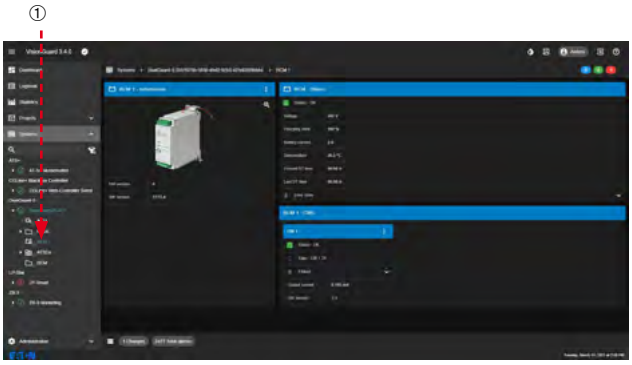
The PSU detail view shows the status of the Power Supply Unit (PSU). In case of Failures it will be displayed in the PSU Status widget.



11.4 BCM detail view

① The BCM detail view shows the installed charging technology, consisting of BCM (battery control module) and CM (charger module) charging parts.

The BCM widgets display the battery values such as voltage in volts, charge status in %, charge/discharge current in amps and the battery ambient temperature in °C. The CM widget displays the overall status OK or fault, and in the event of a fault, the fault display is expanded, which then shows the exact fault.

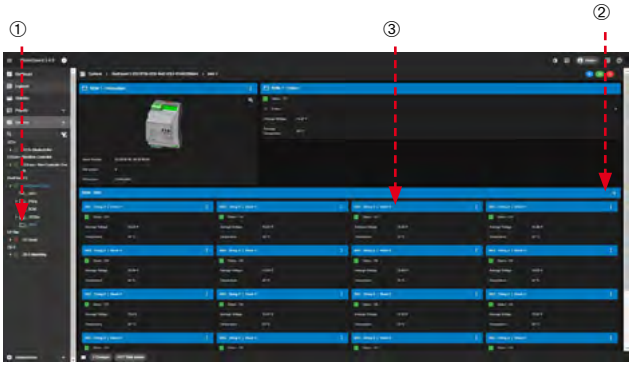


11.5 BDM detail view

If the optional available Battery Block Monitoring is installed and logged on to the HMI, the menu item „BDM“ automatically appears in the system tree. ①

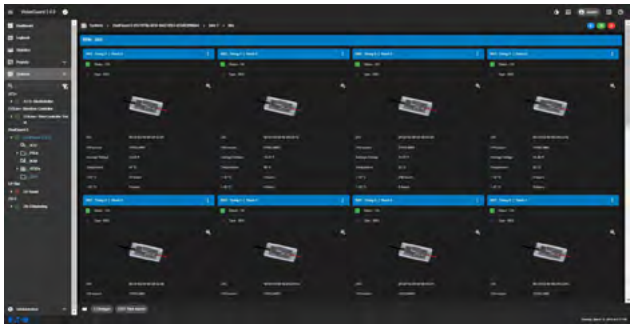
In the BDM view, the BDM (Battery Data Module) is displayed with an extra status widget ② and all connected BBS (Battery Block Sensors) are displayed in an overview widget below of the BDM with the single battery block voltage and the single battery block temperature.

③ With click on the arrow, the BBS detail view appears



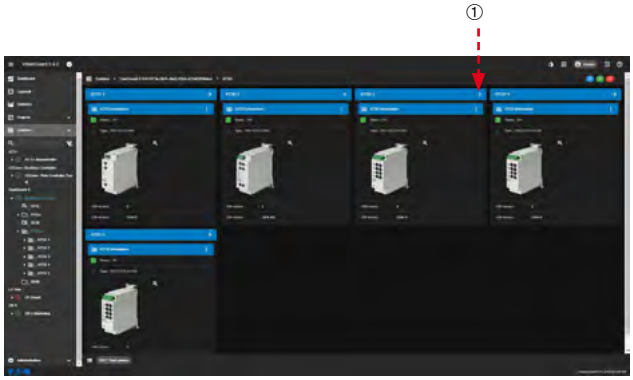
11.5.1 BBS detail view

The BBS detail view show the voltage and temperature of each single battery block. Furthermore it shows the UID (unified ID number), the software version of the sensor, and the time of the average temperature



11.6 ATSD (SKU) detail view

The ATSD detail view displays the SKU types and the names, additional information and total statuses of each circuit. In this case, it is recommended to enter target location designations in which the circuits with the lights are routed, e.g. Circuit 1 Head building Hall 1. In the event of a circuit fault, the fault indicator will also pop up here, which will then indicate the exact circuit fault. Click on the arrow ① to open the circuit's lights detail view.



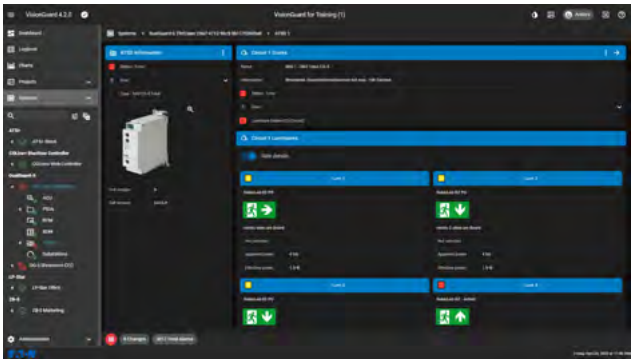
11.7 Luminaire detail view

In the luminaire detail view, luminaires 1 to 20 are clearly displayed along with their status:

- ***Black*** = not installed
- ***Gray*** = OFF
- ***Yellow*** = ON
- ***Red*** = fault

The "Show details" slider opens the detail view with a widget for each installed luminaire, containing the following information:

- Luminaire number and status in the header (as described above)
- Luminaire name (max. 40 characters)
- Luminaire category, e.g., emergency exit sign arrow right (if selected in the luminaire configuration)
- Additional information text (max. 100 characters)
- Apparent power in VA (if manually entered in the luminaire configuration)
- Effective power in watts (if manually entered in the luminaire configuration)

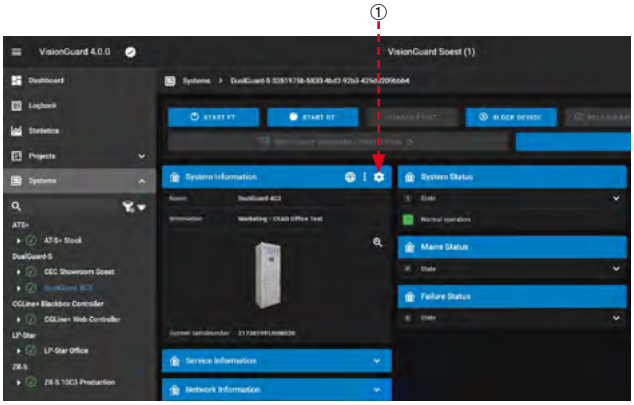


11.8 Configuration of a DualGuard-S / LoadStar-S

To configure a DualGuard-S / LoadStar-S system, the user must have Administrator or Supervisor rights!
The configuration menu is reachable via the gear symbol ① on the widget "***System information***". A new window appears.

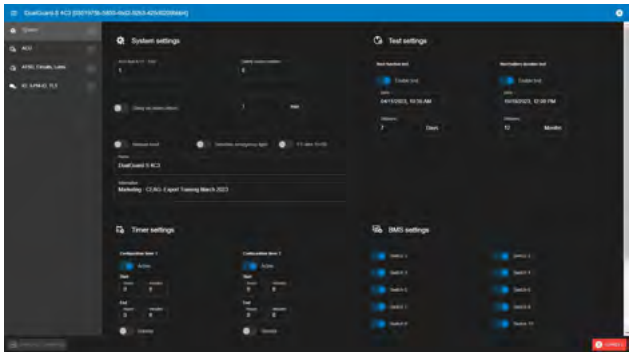
NOTE

Clicking on the globe in the header bar opens the DG-S HMI web server in a new tab.

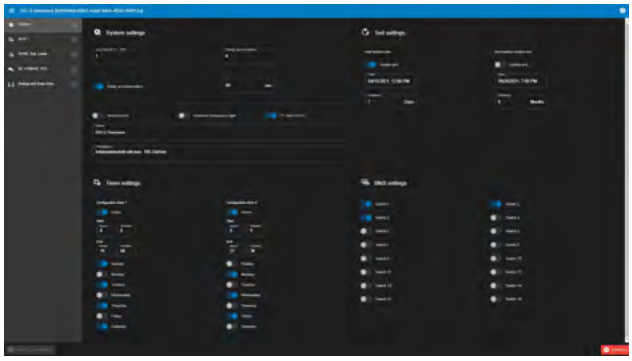


In the upper left part of the window you can now select the desired configuration levels:

- System
- ACU
- SKU (ATSD), Circuits and luminaires
- IO, 3-PM-IO, TLS
- Revision mode



11.8.1 System configuration



In the system configuration, all basic HMI settings can be made, such as:

System settings

- ACU Bus ID (value may be 1 - 120)
- Number of the safety source (within the ACU bus ID)
- Delay on mains return (1-99 min.)
- Activation of manual reset
- Activation of selective emergency lighting
- Activation of an FT after blocking via S1/S2
- Name of the DG-S (max. 40 characters)
- Additional information field (max. 100 characters)

Test settings

- Activation of automatic FT
- FT date and time
- Interval in days
- Activation of automatic BT
- Date and time BT
- Interval in months

Timer settings

- Activation of timer 1 / timer 2
- Start (time)
- End (time)
- Sundays No/Yes

BMS settings

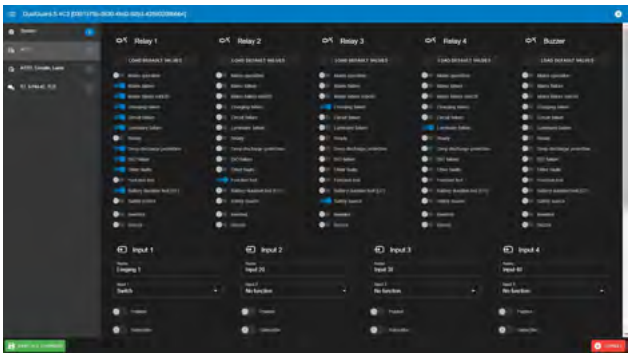
Activation of 1 to 16 virtual switches for the switch menu or external BMS connection via BACnet/IP

Note: The virtual switches are activated/deactivated via this menu, not switched!

Each change of a configuration is recorded in a counter, e.g. 6

When all desired configurations have been carried out, they must be saved via „***Save all changes***". The changes are then sent to the HMI of the DG-S / LS-S.

11.8.2 ACU configuration



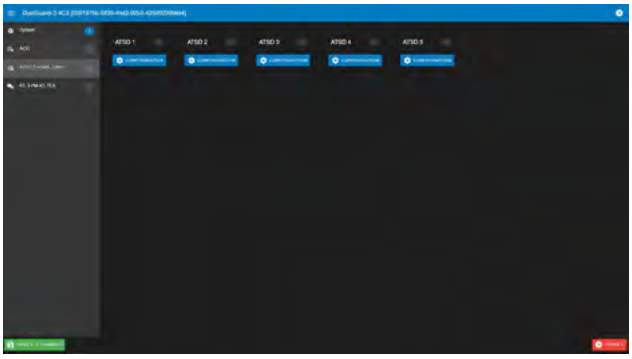
In the ACU configuration, all ACU settings can be made, such

- Digital inputs
- Relay outputs
- Buzzer

With "***Load Default Values***", all settings of the relay can set to the default setting.

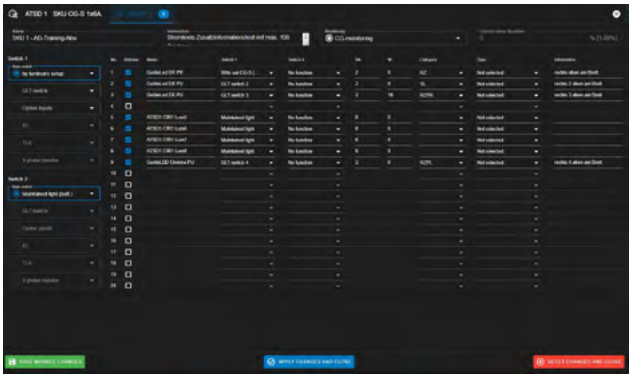
The digital Inputs of the ACU can be "***Publish***" and "***Subscribed***" to other ACUs of other DG-S / LS-S, to enable a cross-plant function of several DualGuard-S / LoadStar-S systems. For more details on the ACU settings, refer to the DG-S / LS-S manual.

11.8.3 ATSD (=SKU), Circuits, Lums configuration



In the SKU configuration, all installed SKU (ATSD) are shown in an overview.

Via the "***configuration***" button of the desired SKU (ATSD) 1 to 40, the next configuration of the circuits appears



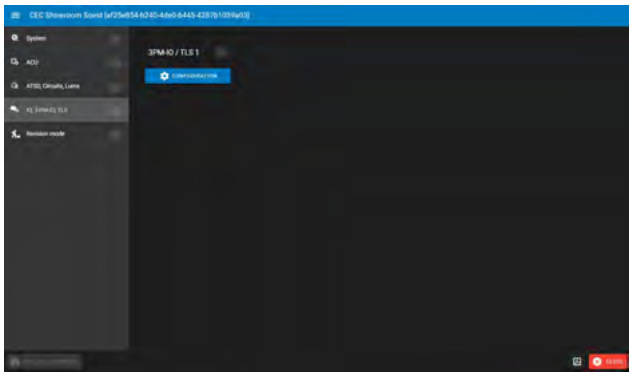
In this configuration menu, all desired settings up to the luminaire level can be made as usual, such as:

- Monitoring mode, e.g. CG Monitoring
- Information text of the circuits or luminaires
- Switch assignment of the circuit or luminiares
- Luminaire category
  SL = Safety Luminaire (picture)
  RZ = Exit Sign (picture)
  RZPL = Exit Sign Arrow Left
  RZPR = Exit Sign Arrow Right
  RZPU = Exit Sign Arrow Down
  RZPO = Exit Sign Arrow Up
- Load of the luminaire in VA or W

To overtake change settings, please click on the green button "***Save module changes***", to abort the changes please click the red button "***Reset changes and close***"

11.8.4 IO, 3PM-IO, TLS configuration

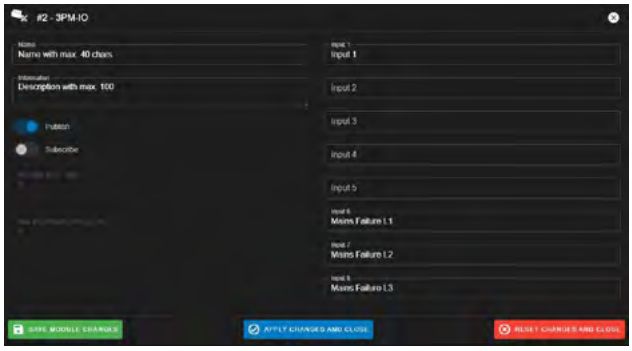
In the IO, 3PM-IO, TLS configuration, all installed IO, 3PM-IO, TLS modules are shown in an overview. Via the "***configuration***" button of the desired module 1 to 25, the next configuration of the IO, 3PM-IO, TLS modules appears



In this configuration menu, all desired settings of the IO, 3PM-IO, TLS modules can be made, such as:

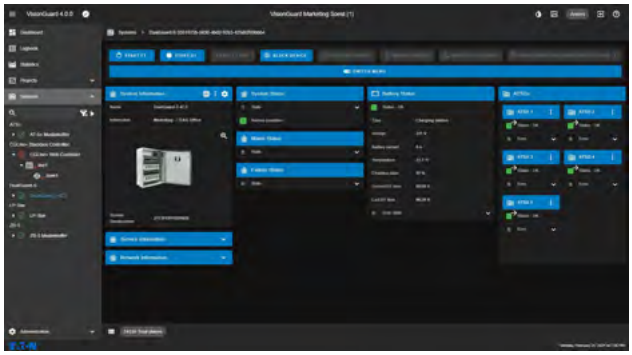
- Name and Information text of the module
- Name text of each input

The the IO, 3PM-IO, TLS modules can be "***Publish***" and "***Subscribed***" to other IO, 3PM-IO, TLS modules of other DG-S / LS-S, to enable a cross-plant function of several DualGuard-S / LoadStar-S systems.
For more details on the IO, 3PM-IO, TLS modules settings, refer to the DG-S / LS-S manual.



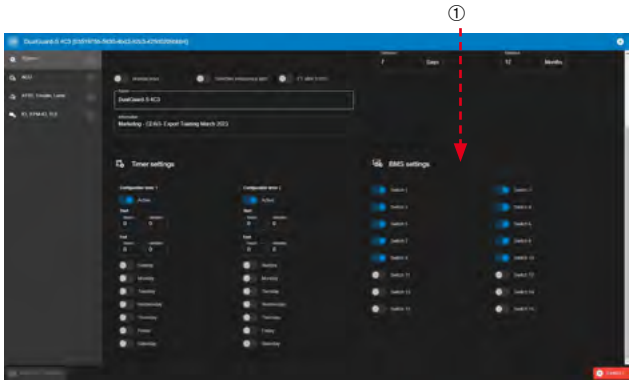
11.9 Switch Menu

The Switch menu for DG-S under the control buttons allows switching of luminaires or circuits via up to 16 virtual switches in the DualGuard-S.
The virtual switches must be activated for this in the DG-S, and the luminaires or circuits must be configured accordingly to the virtual switches, which will be explained in the next subchapters



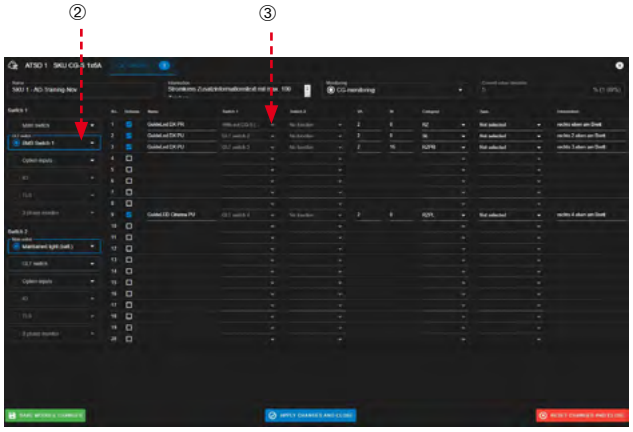
11.9.1 Activation of the virtual switches

The virtual switches 1-16 can be activated individually in the HMI configuration under "***System***" in the area "***BMS Switch"*** via the slide switches (1).
The example shows an activation of Virtual Switch 1-10.
Switch 11-16 are not active.
Only activated switches can be used to switch circuits or lights via the switch menu or via BACnet/IP.



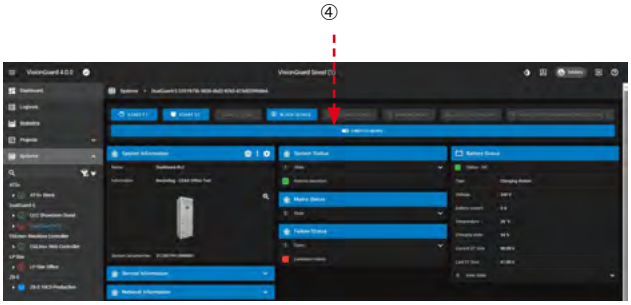
11.9.2 Configuration of circuits or luminaires to the virtual switches

After activation of the virtual switches a circuit can configured to the switches via Switch 1 and Switch 2 setting via “GLT switch” (2).
To configure luminaires to the virtual switches, the Main switch of the circuit must be configured to “by luminaire setup” (2). Now the Switch 1 and Switch 2 of the luminaires can be configured to the virtual switches “GLT switch 1 to 16” (3).

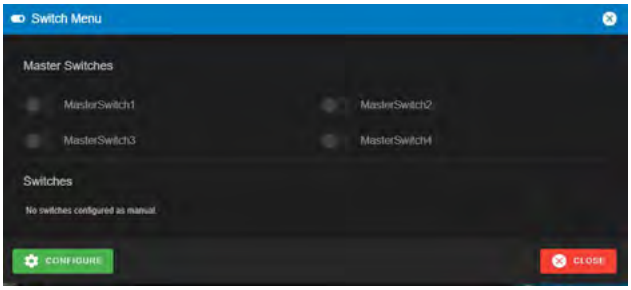


11.9.3 Configuration of the virtual switches in the Switch Menu

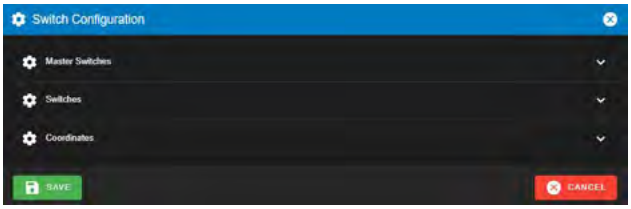
The virtual switches can now be configured with special features in the Switch Menu (4).



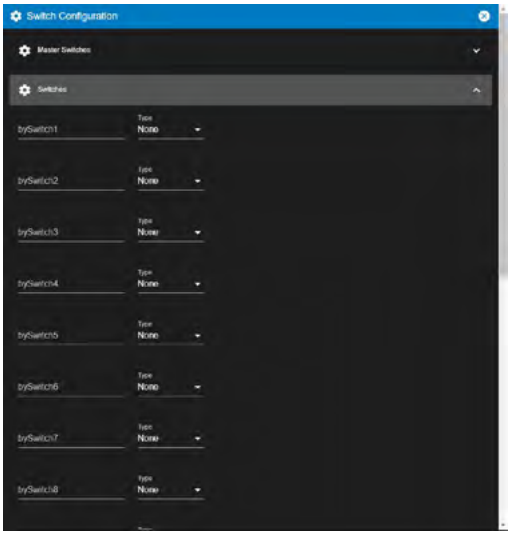
The Switch menu contains a widget with slide switches to switch the circuits or luminaires



The Switch configuration contains three submenus:
1. Master Switches
Allows to combine Static switches to a group
2. Switches
Configuration of the switch functionality
3. Coordinates
Sets the GPS country coordinates of the software to determine for sunrise and sunset to use the switches as Astro timer

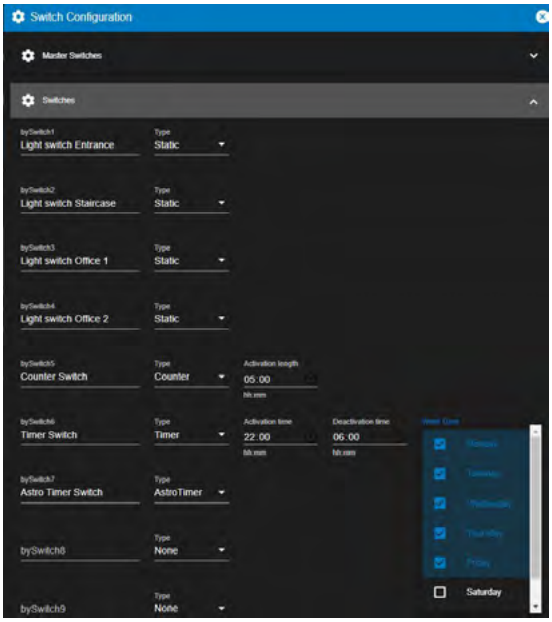


To configure the virtual switches open the “***Switches***” drop down menu with all 16 virtual switches.
Now the name and the switch type can be configured of each single switch.



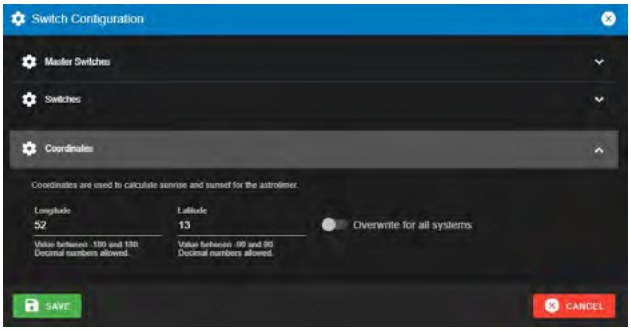
The virtual switches can be configured as follows:
- **Static Switch** (Slide function)
- **Counter** (hh:mm, max. 23:59 h:min)
- **Timer** (hh:mm, week days)
- **Astro Timer** (Sun rise = OFF / Sun set = ON)

Example shows:
Switch 1 to 4 = Static Switch
Switch 5 = Counter 5h = ON
Switch 6 = Timer 10:00 PM to 06:00 AM
Working Days = ON
Switch 7 = Astro Timer



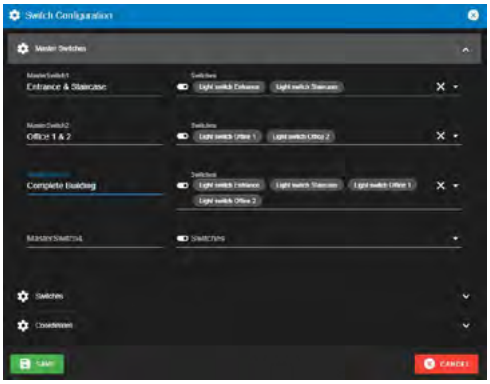
Astro Timer (Coordinates)

Coordinates for Astro Timer can be configured in the submenu "***Coordinates***".
You can find out the Longitude and Latitude values of a location in www.
Berlin has for example Longitude 52 and Latidude 13 to have the right sun rise and sun set times.



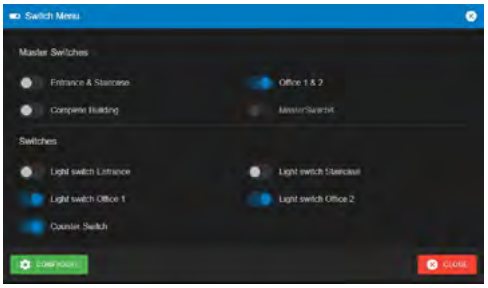
Master Switches

In the menu Master Switches groups of Static Switches can be configured, e.g. to switch separate areas together, for example for a cleaning team or security patrol.
The example shows a configuration of:
MasterSwitch 1 = Entrance & Staircase
MasterSwitch 2 = Office 1 & Office 2
MasterSwitch 3 = All Rooms



11.9.4 Use of the Switch Menu

The virtual switches can now be used in the widget of the Switch menu. The Switches are in design of slide switches. The example shows Master Switch 2 is ON, so Lights of Office 1 and Office 2 is ON.
Counter Switch with 5 hours counting time is active



12. CG-S (ZB-S,LP-STAR,AT-S+) Visualisation

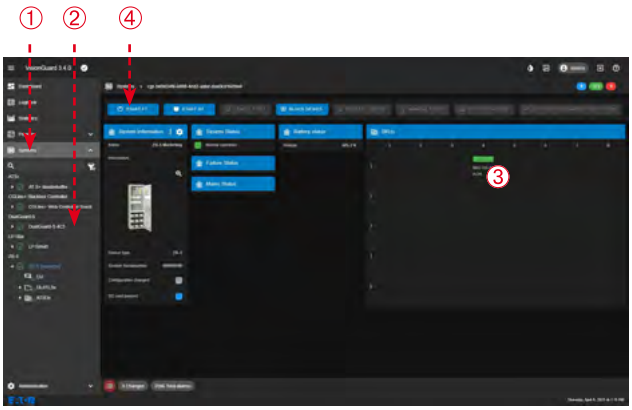
12.1 CG-S system detail view

Under the „***Systems***" menu, all devices (DG-S/LS-S, ZB-S, LP-Star, AT-S+, CGLine+ Web Controller) are listed with their device names in the explorer structure (1).

Click on the name of a CG-S system (2) to see the detailed view of the ZB-S, LP-Star or AT-S+. Here you get detailed status information about the system, service information such as an overview of the System Information, System/Failure and Mains Status. Only data points with colors are displayed when they are active. This provides a clear overview of the status displays.

A Widget shows installed SKU/SOU or SCIR (=Circuits,only LP-Star) (3) according to the mounting on the backplanes inside of the cabinet with the sum status. With click on a SKU the SKU picture with detailed information of the circuits appears. In addition, the blue control buttons can be used to activate various actions on the CG-S system, such as start a function test (Start FT) (4).

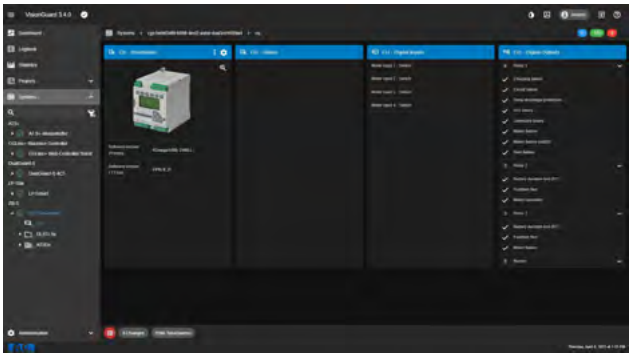
For explanation of the other control buttons, **see section 12.1**.



12.2 CU detail view

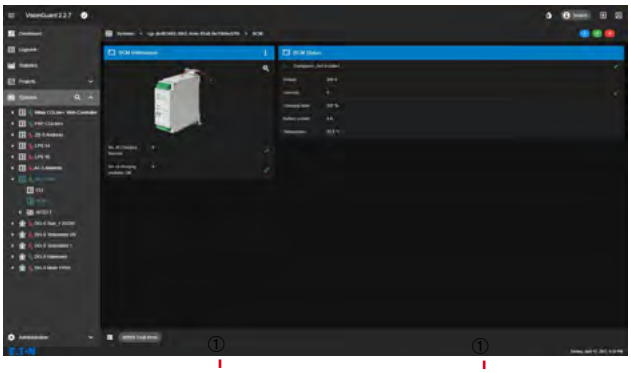
The CU detail view shows the CU status, the CU digital input configurations and the CU digital relay outputs of the CG-S device. It is not possible to configure the digital inputs and relays in VisionGuard. These configurations must be carried out via the ZB-S, AT-S+, LP-STAR PC-Software.

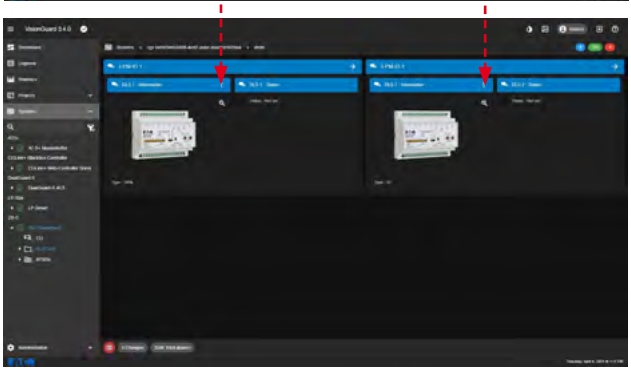
The gear symbol takes you to the control unit configuration.



12.3 BCM detail view (for ZB-S only)

The BCM detail view shows the installed charging technology of a ZB-S system consisting of BCM (battery control module) and CM (charger module) charging parts.
The BCM widgets display the battery values such as voltage in volts, charge status in %, charge/discharge current in amps and the battery ambient temperature in °C.
The CM widget displays the overall status OK or fault, and in the event of a fault, the fault display is expanded, which then shows the exact fault.





12.4 3-PM-IO (DLS) / TLS detail view (only ZB-S/AT-S+)

The 3-PM-IO/TLS detail view display the status of all connected IO, 3-PM-IO and TLS modules. The DLS/TLS Status widget show the sum status of the 3-PM-IO (DLS) / TLS module:

Green = OK, no failure
Red = Failure (with text, e.g. Mains failure subDB).
The ... (1) show the status of each input in a new widget.

Use the arrow on the right in the blue header to open a new widget with detailed information on the digital inputs.
Grey = not active
Yellow = active

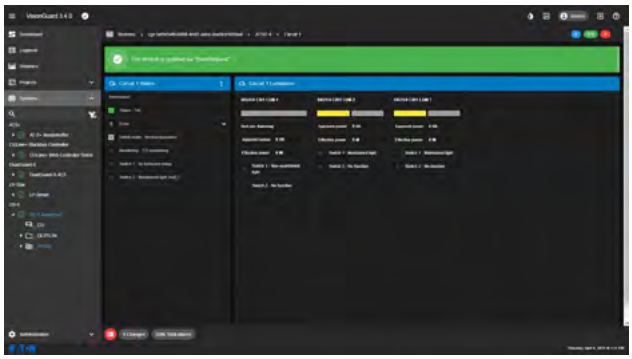
If the modules are configured as phase monitors, inputs 6 to 8 are
Yellow = phase OK
Red = phase power failure

12.5 SKU (ZB-S,AT-S+) / Circuit (LP-Star) detail view

The ATSD (=SKU) detail view displays the SKU types and the names, additional information and total status of each circuit according to the backplane assignement in the ZB-S/AT-S+ cabinet. LP-STAR has fixed 4 circuits, which provide same information of SKU circuits. In the event of a circuit fault, the fault indicator will also pop up red here, which will then indicate the exact circuit fault. Click on the arrow in the blue Circuit head line to open the circuit's lights detail view.

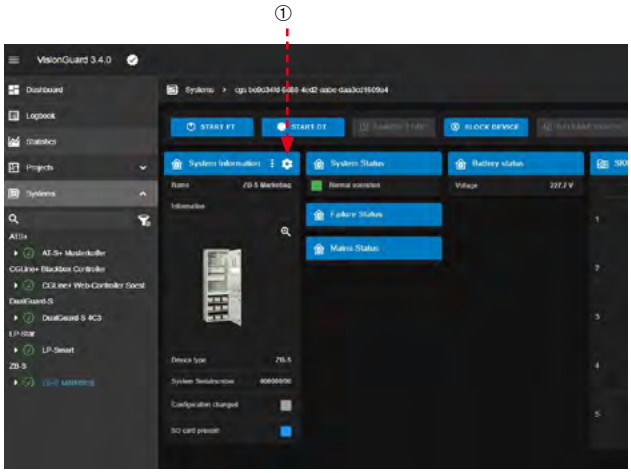
12.6 Luminaire detail view

The status and information texts of the circuit are displayed in the luminaire detail view. In the event of a circuit fault, the fault display is also opened, which then indicates the exact circuit fault, e.g. AC fuse fault.
The status of the light is displayed in the light widget header. **Gray** = off, **yellow** = on, **red** = fault/defect



12.7 Configuration of a ZB-S / LP-STAR

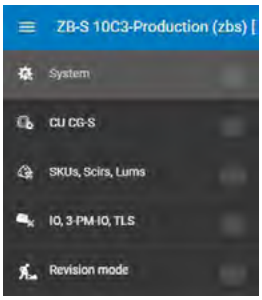
To configure a ZB-S / LP-STAR system, the user must have Administrator or Supervisor rights!
The configuration menu is reachable via the gear symbol ① on the widget "System information". A new window appears.
The configuration of ZB-S and LP-STAR is similar. The procedure that are the same for both systems are described here using ZB-S.

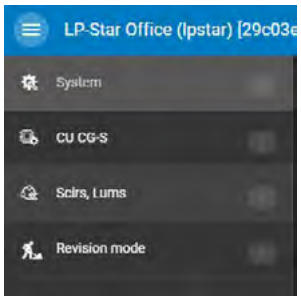


The same procedure applies for LP-STAR.
Click on the gearwheel symbol ① to open the desired ZB-S configuration menu.

In the upper left part of the window, you can now select the desired configuration levels:

- System
- CU CG-S (Control unit)
- SKUs, Circuits and luminaires
- IO (only ZB-S)
- 3PM-IO (only ZB-S)
- TLS (only ZB-S)
- Revision mode



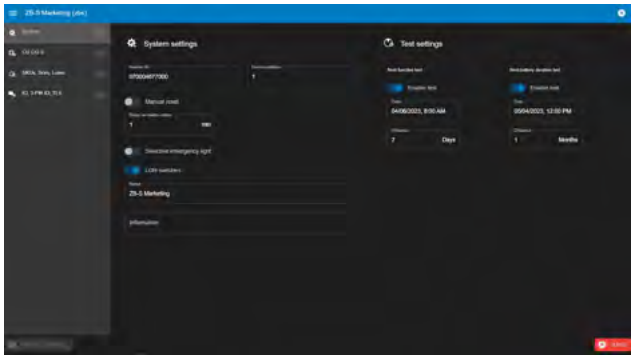


12.7.1 System configuration

In the system configuration, all basic settings can be made, such as:

- Name and Information text of the ZB-S / LP-STAR
- Next automatic FT or DT
- Manual reset
- Delay on mains return in minutes (0-99 Min.)
- Selective emergency light (only ZB-S)
- Activation of the virtual LON switches (16 pcs.)

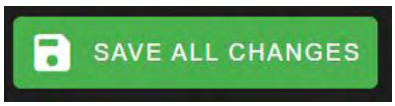
Note: It is not possible to change the Neuron ID and the device address.



For more details on the basic settings, refer to the ZB-S manual.

Each change of a configuration is recorded in a counter, e.g., 6

When all desired configurations have been carried out, they must be saved via „***Save all changes***“. The changes are then sent to the ZB-S / LP-STAR.

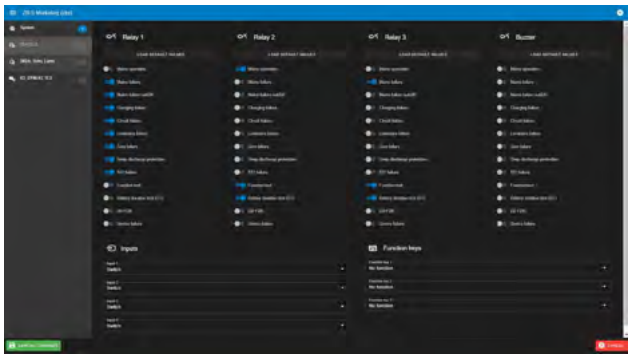


12.7.2 CU CG-S configuration

In the CU CG-S configuration, following settings are possible:

- Relay outputs and Buzzer
- Digital Inputs (1 to 3 for ZB-S, 1 to 8 for LP-STAR) with text assignment
- Function keys with text assignment

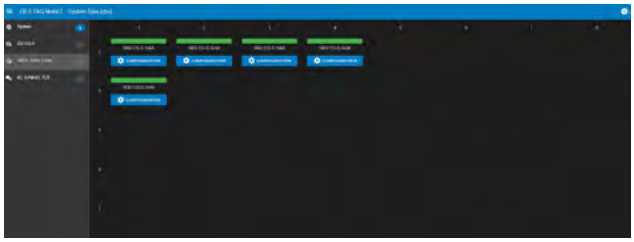
With “***Load Default Values***”, all settings of the relay can set to the default setting



12.7.3 SKU (ZB-S) / Circuits (LP-STAR) configuration

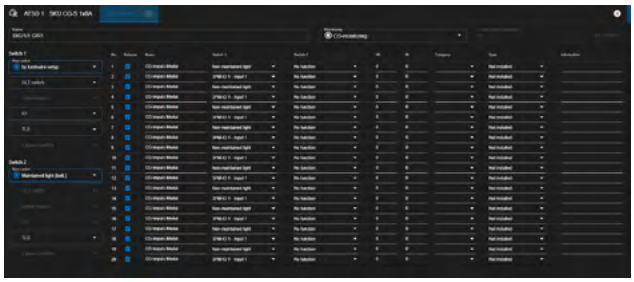
In the SKU / Circuit configuration, all installed SKU are shown in an overview. The picture shows the SKU arrangement as installed in the ZB-S cabinet. LP-STAR has 4 fixed circuits.

Via the "***configuration***" button of the desired SKU 1 to 40 (ZB-S) or Circuit 1 to 4 (LP-STAR), the next configuration of the circuits appears.



In this configuration menu, all desired settings up to the luminaire level can be made as usual, such as:

- Add / Delete luminaires
- Monitoring mode, e.g. CG Monitoring
- Information text of the circuits or luminaires
- Switch assignment of the circuit or luminaires
- Luminaire category
- Load of the luminaire in VA (Apparent Power) or W (Effective Power)



12.7.4 IO, 3PM-IO, TLS configuration (only ZB-S)

In the IO, 3PM-IO, TLS configuration, all installed IO, 3PM-IO, TLS modules are shown in an overview.

Via "***configuration***" text assignment of the modules can be entered

- Name with max. 20 characters
- Information text with max. 100 characters

12.7.5 Revision mode (Construction Site)

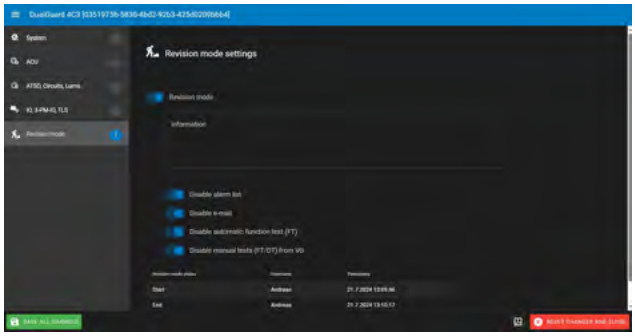
The Revision mode (Construction site mode) allows a deactivation of notification, in case the DualGuard-S (Revision mode is available for all systems) is in maintenance. This is useful to avoid any notification, e.g. an E-mail during the maintenance of a system.

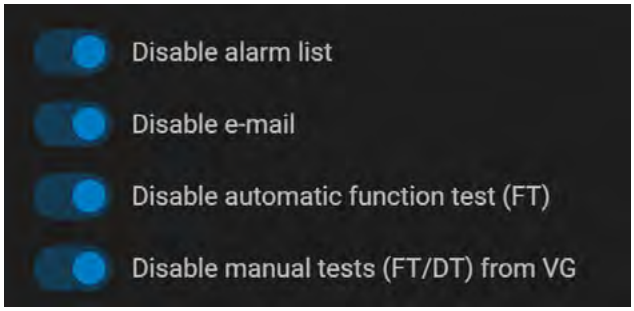
The Revision mode can be activated via the slider "Revision mode".
It is mandatory to enter a text in the information box, e.g. to explain the reason for the activation of the Revision mode, the duration etc

As standard all notification will be deactivated

- Disable alarm list : The Alarm list will not report any events anymore.
- Disable e-mail : VisionGuard will not send an E-Mail for this system anymore.
- Disable automatic function test (FT) : All automatic function tests are no longer performed.
- Disable manual test (FT/DT) from VG : All manual tests (Function Test / Duration Test) from VisionGuard will be disabled, to avoid manual actions during the maintenance.

All events can be activated individually using the sliders.
In the lower area, a time stamp is used to log which user has activated and deactivated the revision mode.



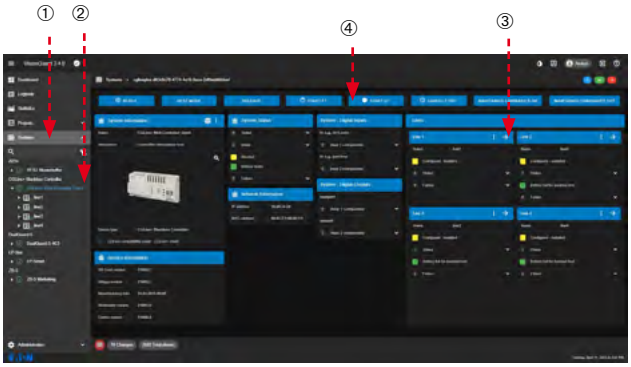


13. CGLine+ Web-/Compact 160/400-Controller

NOTE

It is possible to connect CGLine+ Web-Controller and CGLine+ Compact Controller 160 / 400. Please see Chapter 1.4.3 for minimum Firmware requirements. This chapter describes the functions of the CGLine+ Web-Controller. The functions of the Compact Controller 160/400 are almost the same, only with limited scope.

13.1 CGLine+ Web-Controller detail view



Under the "***Systems***" menu, all systems are listed with their device names in the explorer structure ① .
Click on the name ② of a CGLine+ Web-Controller to see the detailed view. Here you get detailed status information about the system, service information such as an overview of the System Information, System Status with failures, Settings of the digital In-/Outputs and Line Status with summary status information of the luminaires. Only data points with colors are displayed when they are active. This provides a clear overview of the status displays.
With click on the **->** of a line ③ , detailed information of the zones and luminaires appears.
The blue control buttons ④ can be used to activate various actions on the CGLine+ Web-Controller, see next section **„Control buttons".**

13.2 Control buttons

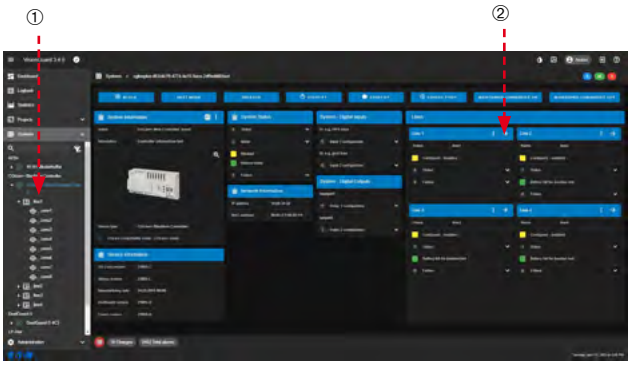
The Control buttons are available on the Controller view, Line view and Zone view.
This means that commands can be started down to the zone level.
You can control all connected luminaires with the control buttons. Following commands are possible:
BLOCK = Block all luminaires
REST MODE = Activation of the Rest Mode
RELEASE = Unblock all luminaires
START FT = Start of a Function Test
START DT = Start of a battery Duration Test
CANCEL FT/DT = Stop a running Function- or Duration Test
MAINTAINED LUMINAIRES ON = Switch ON all luminaires
MAINTAINED LUMINAIRES OFF = Switch OFF all luminaires

Note: To switch luminaires ON and OFF the L` in the luminaire must be connected! (See manual of the luminaire)

IA START = Activate IA - Blink in case of an emergency evacuation (only Controller and Line)
IA STOP = Deactivate Increased Affordance (only Controller and Line)

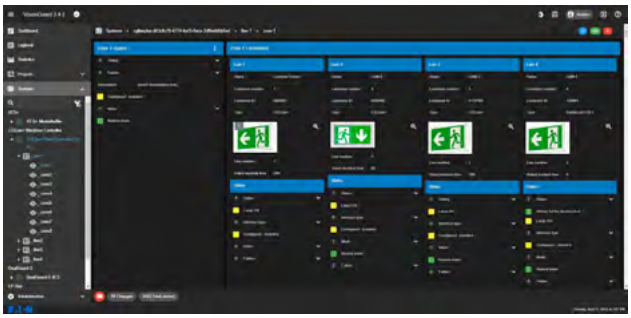
13.3 Line detail view

To navigate to the Line detail view it is possible to click the Line number under the CGLine+ Web-Controller in the System overview ① , or on the arrow in the Line widget ② .



The Line overview with assigned Zones and connect with assigned Zones and connected luminaires appears.

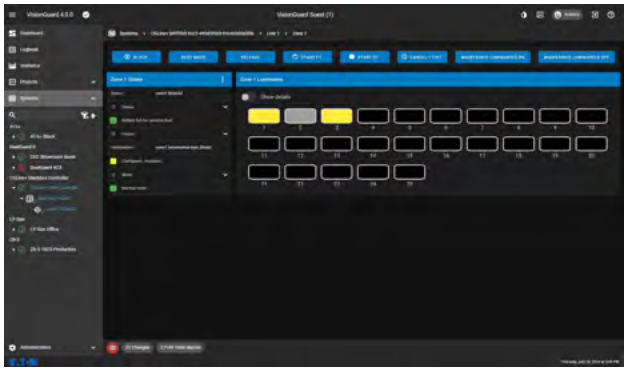
In the headline of each Zone a summary status of all luminaires is displayed. In the Zone x Luminaires widget, all luminaires with their detailed status in an own widget are displayed.



13.4 Zone detail view

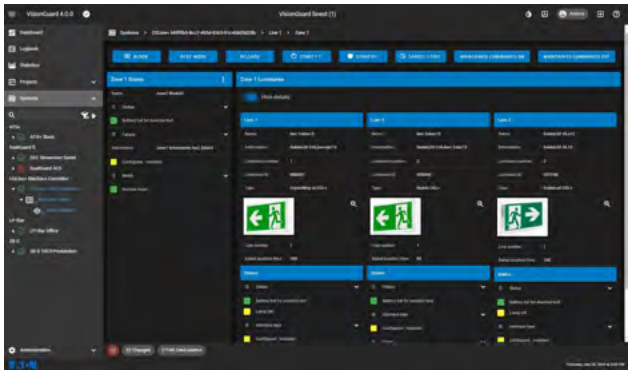
To navigate to the Zone detail view it is possible to click the Zone number under the CGLine+ Web-Controller in the System overview.

In the zone overview, all lights are clearly displayed with their total status in colour in a matrix:
Black = not installed
Grey = switched off
Yellow = switched on
Red = faulty



The blue control buttons above can be used to start the actions described above for the zone for all luminaires in this zone

The Zone overview shows all luminaires with their detailed status of that zone.



14.Project Navigation

14.1 Description

The Project navigation enables large or complex projects to be displayed in a very clearly structure. The project is divided into a project tree or navigation tree similar to an Explorer structure. The project can be divided into several levels, e.g. locations - buildings - floors - rooms.

Each level can in turn be subdivided or expanded into sublevels, e.g. location 1 - location 2 - location 3 etc. with all the sublevels described above. In each level, all connected emergency lighting systems, e.g. DG-S, can be placed as desired. This gives a very good overview of the installation location or the emergency lighting supply area of the emergency lighting system.

This can be structured and expanded as desired, so that even complex projects can be clearly displayed.

Furthermore the project navigation is connected with the optional Building Layout Programming.

(Must be purchased as seperate licence)

The Building Layout Programming allows a convenient view

of system status and luminaires as graphical coloured data points in a building layout. The colours of the data points enable immediate recognition of the status. Tooltips (pop-up windows) display further information (e.g. luminaire name) on the data points. For more information please see **„15. Building Layout Programming“ on Page 68**.

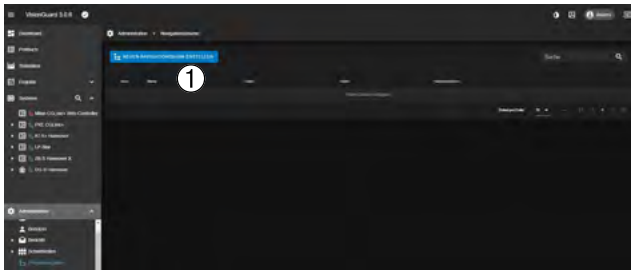
Example:

Project name: Sample project

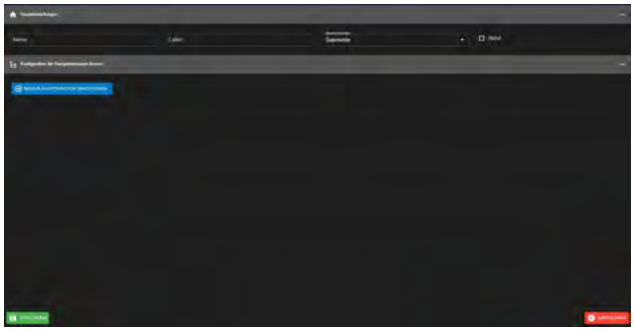
- Location 1
  - Building 1
  - DG-S Emergency lighting for Building1
    - Floor 1
    - ZB-S 2C3 for technical rooms floor 1
      - Room 1
        - DG-S 4C3
      - Room 2
        - US-S 38
      - Room 3
        - DG-S2C3
    - Floor 2
      - Room 1
        - DG-S 2C3
  - Building 2
    - Floor 1
      - Room 1
      - Room 2
- Location 2
  - Building 1
    - Floor 1
      - Room 1
      - Room 2
      - Room 3
    - Floor 2
      - Room 1
      - Room 2
      - Room 3
      - Room 4
  - Building 2
    - Floor 1
      - Room 1
      - Room 2
    - Floor 2
      - Room 1
      - Room 2

14.2 Creating a project tree

Remarks:
It is highly recommended to plan a meaningful project tree on paper first, and then to transfer or create the project tree step by step in VisionGuard! This makes the process easier and clearer. Several project navigation trees can also be created. The desired project tree can be activated at any time with a mouse click. In this way, planned extensions, changes, etc. can be taken into account in advance.
The project tree can only be created by an administrator or supervisor in the administration level in the menu "***Project navigation***":



Click on "***Create new navigation tree***" ① to start the configuration menu. A new window opens with the configuration menu, consisting of the two submenus "***Main properties***" and "***Navigation tree nodes configuration***".



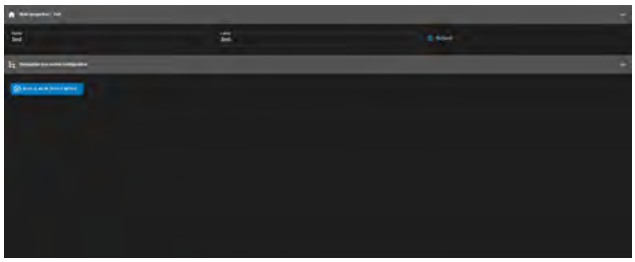
Click on these menus to show or hide them.

14.2.1 Main properties

In the Main properties field, names and a Label name can be assigned to the navigation tree and the navigation tree can be set to active or inactive if several navigation trees have been created as mentioned above.
In the field "***Name***" and "***Label***" you can assign a name and an additional label to the navigation tree. Furthermore, the corresponding user role can be selected that is to have access to the project navigation.

Example:
Sample project with 2 locations + additional information text

You can now configure the navigation tree directly.



14.2.2 Navigation tree nodes configuration

To configure the navigation tree, click on "***Add new main node***". You can then create a name for the node in the "***Node label***" field. This name then appears on the left-hand side of the navigation tree under the "***Projects***" menu. In the "Url route label" field, the name is taken from the Label node. However, this can be changed as required. This name then appears in the project overview. A sub-node can now be created using the + sign. This can be done as often as required. Nodes can be deleted again using the dustbin symbol. Further new nodes can be created using the "Add new main node" button. This is shown in the following example.

Example: Sample project with 2 locations
As already mentioned, it makes sense to plan a meaningful project tree on paper first. As an example, the following simple project tree should be created:
Main nodes = Location 1 and Location 2
First sub-nodes = Building 1 and Building 2 (in both main nodes)
Second sub-nodes = Floor 1 and Floor 2
Third sub-node of floor 1 = Room 1 and Room 2
and so on...

Example:

Project name: Sample project with two locations

- Location 1
  - Building 1
    - Floor 1
      - Room 1
      - Room 2
    - Floor 2
  - Building 2
    - Floor 1
      - Room 1
      - Room 2
- Location 2
  - Building 1
  - Building 2

The emergency lighting systems can be placed immediately during configuration. In this example, the emergency lighting systems are placed after configuration of the navigation tree for the sake of clarity.

Any changes and extensions can be made later at any time with a few mouse clicks.

Start by clicking on "***ADD NEW ROOT NODE***":

A widget with a node is created with the following editing options:

1) Select visualisation view.

This function is only supported from VisionGuard V4.0.0! In future, a graphic, e.g. terrain plan with buildings or a floor plan visualisation, e.g. of a building, floor, etc. can be stored here.

2) Select direct system link (emergency lighting system)

Here you can select a desired emergency lighting system, which is then created accordingly in the project tree. In this example, this is explained after configuring the navigation tree.

3) Account icon

Here, if required, you have the option of displaying an ICON in front of the node in the project navigation (selection from Material Design), e.g. for a location, building, floor, level, etc.

ICON examples:

4) Node label

Here you can assign a name to the node for the project tree. In the case of the example, the first main node is called: "***Site 1***".

The settings described above can be changed individually for each node created.

5) URL route label

The name of the node label is automatically adopted, but as already described above, you can give the label its own name, which is then displayed differently in the project overview than in the project tree. For the sake of simplicity, it is recommended to keep both names the same.

14.2.3 Creating the main nodes and subnodes

To create the navigation tree described above as an example, proceed as follows.

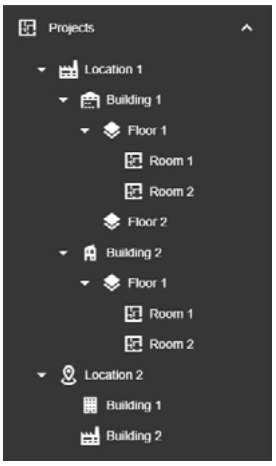
It is recommended to first create all main nodes via "***ADD NEW ROOT NODE***". In our example, these are the two main nodes "***Location 1***" and "***Location 2***":

The **+** symbol at the top right of each main node, the desired sub-nodes can now be added accordingly
Using the ***dustbin symbol***, main nodes or sub-nodes can be deleted again at any time.

This is how the prior example looks for location 1:

Once all main nodes and subnodes have been created, the navigation tree must be saved using "***Save***" (bottom left). The navigation tree will then be displayed accordingly in the "***Project***" navigation menu.

In the administration area, all settings can be edited again with a few mouse clicks.



14.2.4 Creating and placing emergency lighting systems in the navigation tree

After creating the navigation tree, the emergency lighting systems can now be placed anywhere in the navigation tree. To do this, open the navigation tree again in the administration area. Using the selection menu "***Select direct system link***", you can now select and place an emergency lighting system in each main node or sub-node.

In the tree, the assigned plant names are then displayed by the HMI! It is recommended to use sensible destination names for the plant names.

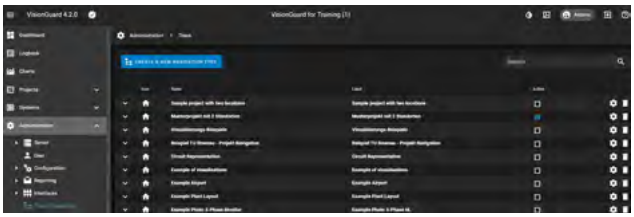
Example:

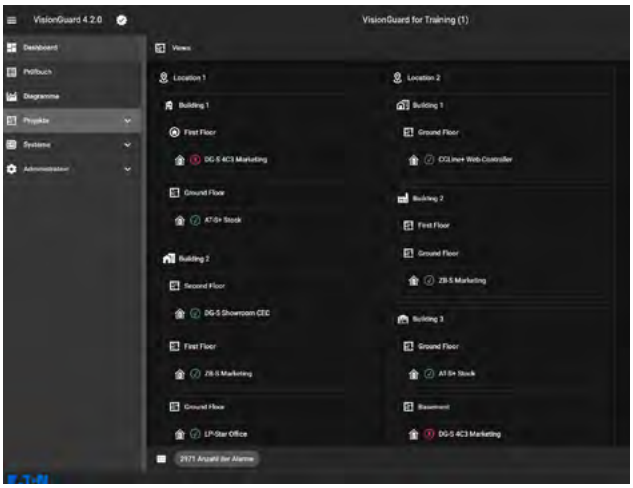
Project name: Sample project with two locations

- Location 1
  - Building 1
    - **DualGuard-S 20C6**
    - Floor 1
      - Room 1
        - **DualGuard-S 12C6**
      - Room 2
        - **DualGuard-S 12C4**
    - Floor 2
      - **DualGuard-S US-S 15**
  - Building 2
    - Floor 1
      - Room 1
        - **DualGuard-S 12C6**
      - Room 2
        - **DualGuard-S US-S 7**
- Location 2
  - Building 1
    - **DualGuard-S 4C3**
  - Building 2
    - **DualGuard-S 12C4**

14.3 Activating Created Project Navigators

The created project navigation must now be activated in the list. If multiple project navigations have been created, they can be quickly and easily activated here, or you can switch between them.





The activated project navigation is then immediately visible in the "***Projects***" menu.

15. Building Layout Programming

The building floor plan programming allows convenient display of the emergency lighting systems and emergency luminaires with coloured status display (***green*** = ok, ***red*** = fault) in any graphics such as site plans or building floor plans. In addition, other data points can also be visualised in the graphics, such as analogue battery values, 3-phase monitoring of general lighting distributors and much more.

The building floor plan programming is linked to the project navigation, i.e. any number of project levels can be created, in which maps, site plans or building floor plans can then be integrated. For example, you can create maps for locations, then site plans with buildings for the locations, and then floor plans of the buildings with any number of levels or storeys.

Flexible linking between the plans makes it easy to navigate through the graphics.

Graphic formats such as .dwg (AutoCAD up to 2017), .dxf, .png, .jpg, .bmp and .svg with a maximum size of 100 MB are supported.

15.1 Preliminary consideration

Before creating a Building Layout project in VisionGuard, it is recommended that you first draw it on paper in order to have a sensible structure before creating it in the VisionGuard. In the first step, this guide explains how to upload graphics in a library from the client PC to the VisionGuard Server and how to create graphics with data points. The second step explains how to integrate the finished graphics into a project navigation and how to link the graphics to each other for easy navigation.

15.2 Licensing of Building Layout Programming

The optional Building Layout Programming for VisionGuard is available in two versions:

Order number: 40071362830

VisionGuard Building Layout Programming

Certificate with download link and licence key

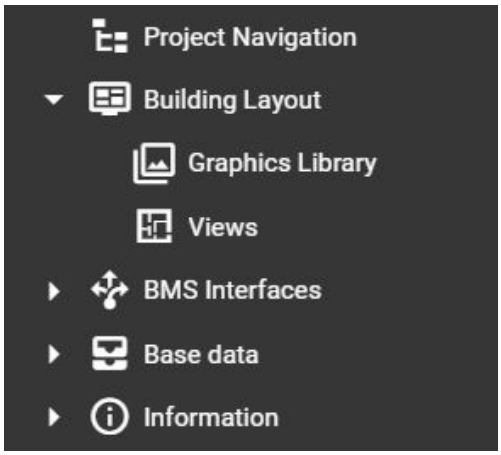
Order number: 40071362831

VisionGuard Building Layout Programming / USB

VisionGuard Software on USB-Stick with Building Layout licence key file

Licensing is carried out in the same way as licensing a Visio basic version. The licensing process is explained in the operating instructions in chapter 4 Licencing.

After successful licensing, the '***Building Layout***' menu appears under Administration with the '***Graphics Library***' and '***Views***' submenus.



15.3 Graphics Library (Upload of graphics)

After creating a sensible concept for the project structure with the integration of graphics such as maps, site plans or building floor plans, the graphics can be uploaded from the client PC to the VisionGuard server.

Please ensure that the floor plans are clean, i.e. without drawing elements that could interfere with the view of the emergency lighting data points, such as grids, notes, furniture, etc. Furthermore, it is recommended not to use any colors in order to achieve a good contrast for the status messages of the data points.

Please use meaningful and simple names for the graphics in order to have a good orientation when creating them.

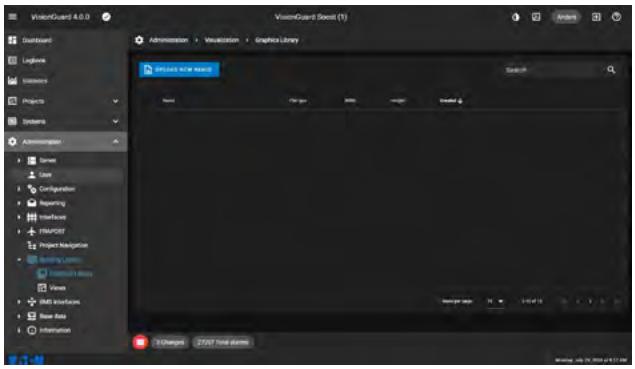
The upload of the graphics can be done in the menu "***Graphics Library***".

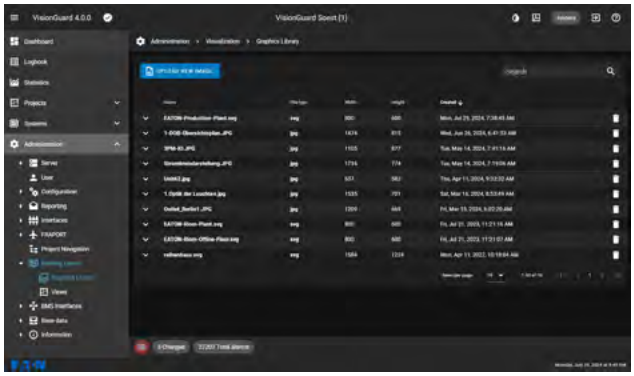
Via the button "***Upload new image***" the desired image can be selected from any Client PC drive.

With "***Upload***", the graphic will be uploaded to the VisionGuard Server

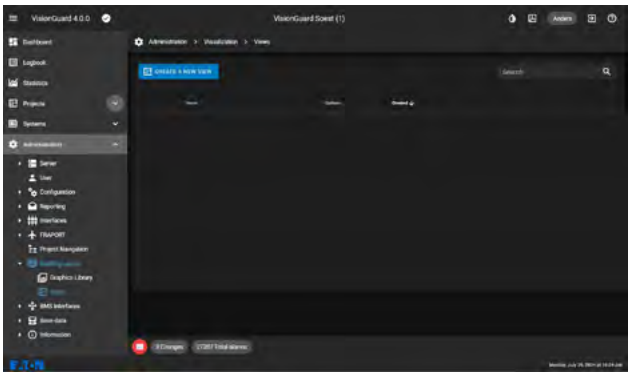
After upload of all graphics, they will appear in the graphics library as list in uploaded order with the name, file type, size of the graphic in dpi and time stamp of creation.

Via the bin symbol icon, it is possible to delete a graphic from the library again.





15.4 Views (Create a Building Layout)



Once all the graphics have been uploaded to the VisionGuard Server graphics library, the graphics can now be created with the desired data points. This description explains two options in two sub-chapters:

15.4.1. creation of a site plan with status display of the installed emergency lighting systems

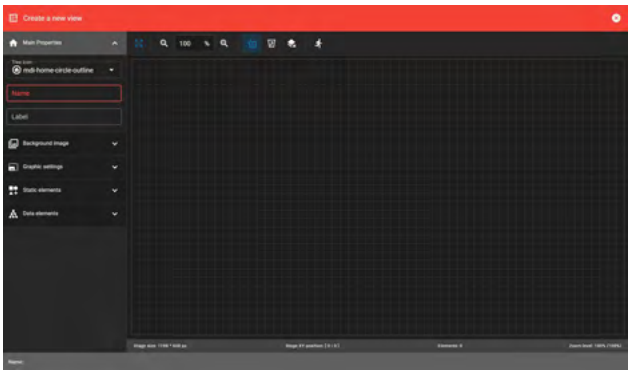
15.4.2. creation of a building floor plan with status display of the installed emergency luminaires

A graphic can be created in menu "***Views***"

Via the button "***Create a new View***" a graphic can be created via uploaded image.

The graphic editor opens with following menus:

Main properties

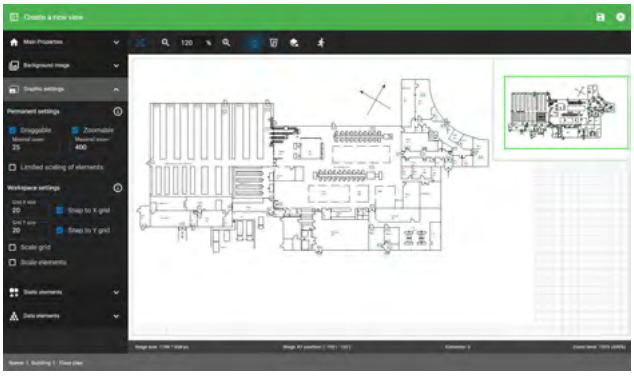


Tree icon:
Here you can select a desired Icon of the graphic, which will appear in the project navigation for orientation.

Name:
Please enter a clearly understandable and simple name here in order to have an easy assignment in the project navigation. Numbering can also be helpful.

Label:
Name of the label in the Breadcrumb navigation.
It is recommended to use the "***Name***".

Background image



Select background image:
Here you can select one of the uploaded images (graphics) in the Library. The graphic will appear in the white center of the editor.

Width and Height at 100%:

Information of the size in pixel (px)

Lock aspect ratio:
if selected, the ratio of Width and Height is locked.

Fit image size to page:
If the Zoom is changed, it will place the new size to the top left corner. It is recommended to set this as last step before saving this programming.

Image transparency:
Transparent view. It is recommended to unselect, so the image background shows in white.

White background:
If selected, the Background displays as white whichis the recommended setting.

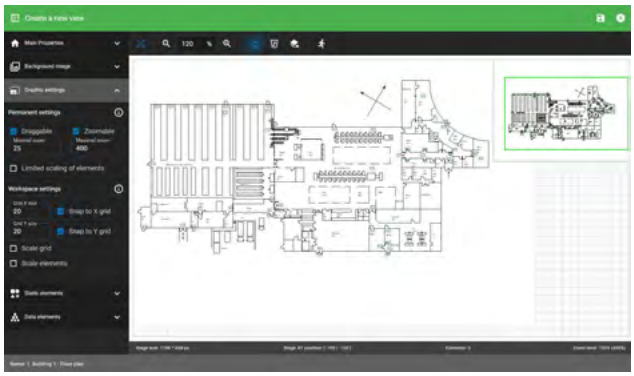
Graphic settings

Draggable:

Activation or deactivation of the panning function

If the image has a big size, e.g. a site plan or a big building, it is recommended to activate the panning function.

Zoomable (with Minimal and Maximal Zoom):



Activation of the zooming function. For big plans or buildings, it is recommended to activate the Zoom function. With minimal and maximal zoom, it is possible to select the best zoom sizes in minimal and maximal view. The correct values must be determined by trial. The small overview image in the top right-hand corner shows the position in a zoomed display with a green frame for good orientation.

Tip: To get the best possible resolution, a high zoom setting is recommended

Workspace settings:

With Workspace settings it is possible to activate X and Y grids, which can support the positioning of the data elements. It is possible to define the size of the grids, and with Snap to Grid the data elements are automatically aligned to the grids. If you want to place the data elements in a precise position, it is advisable to deactivate the Snap to Grid function.

Static elements

Static elements are freely configurable text fields that can be used to add designations to the graphic (e.g. location designations, customized circuit or luminaire names, etc.)

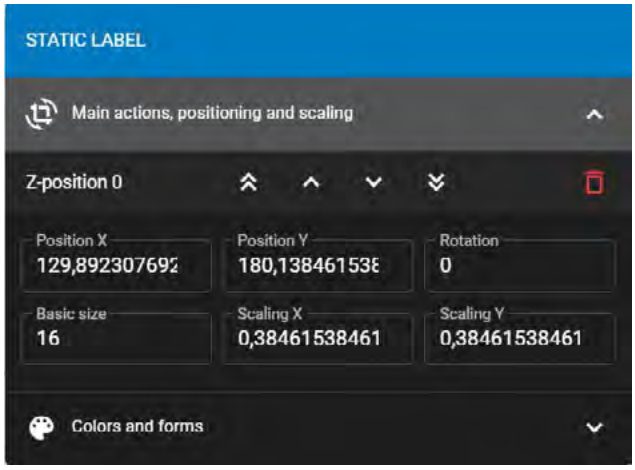
Static Label :

A Static Label is a standard text field

Via right-click to open a menu where you can freely edit the size, rotation, color, border, corners and text

Main action :

Here the size (Basic size) and the rotation 0-360° (Rotation) can be set



Color and forms :

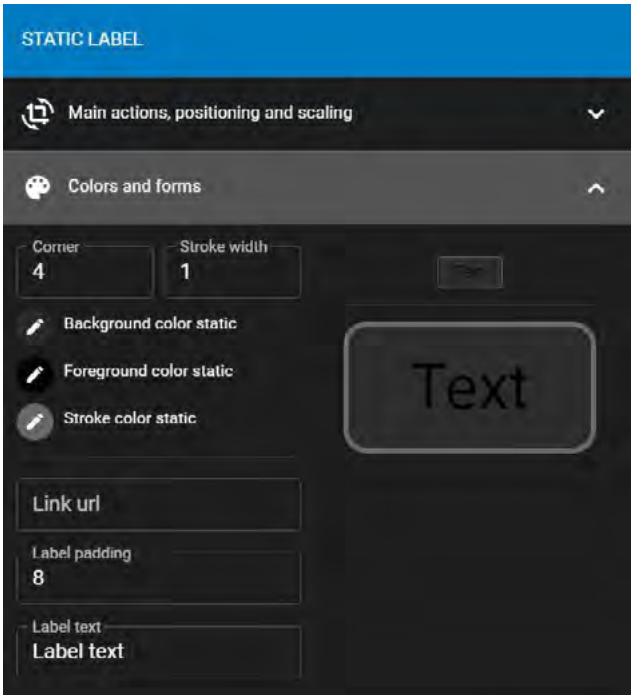
The Corner (scare to round) and Stroke width (Text field margin) can be set via arrow up and arrow up setting boxes.

The colors of the Background, Foreground (Text Colour) and the Stroke (Text field margin) can be freely configured.

A preview window shows the subsequent result.

Finally, the text of the label can be entered in the "***Label text***" field

To close the edit menu it is only required to click outsite of the box

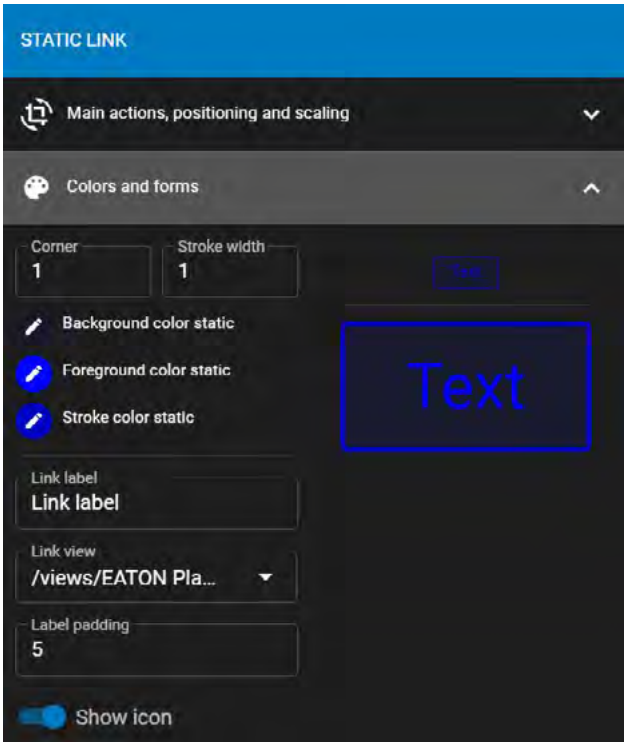


Static Link :

A Static Link is a text field with the possibility to link to any other graphic in a complex structured building layout programming

The settings for size, colours etc. are made in the same way as described above. In addition, you can select the link to another floor plan image via 'Link View'. All floor plan images that have been created so far are displayed. It is therefore advisable to link to other images at the very end.

With Show icon it is possible to deactivate the link symbol left of the text.



Rectangle:

This field/tag is in preparation for a next version of the Building Layout Programming with links to URL.

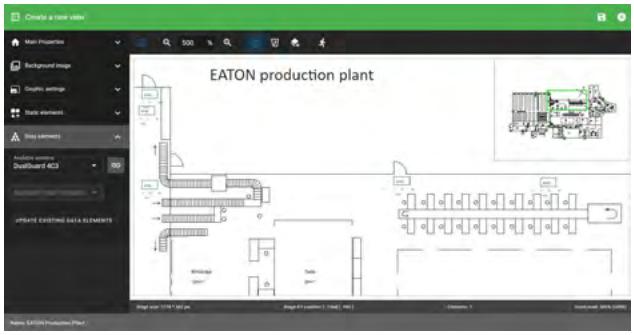
Static Text:

This text tag is a pure text field without Background. Size, Rotation and Color see above description.

Text

Data elements

Via Data elements, it is possible to place any number of status datapoints of all on VisionGuard connected emergency lighting systems

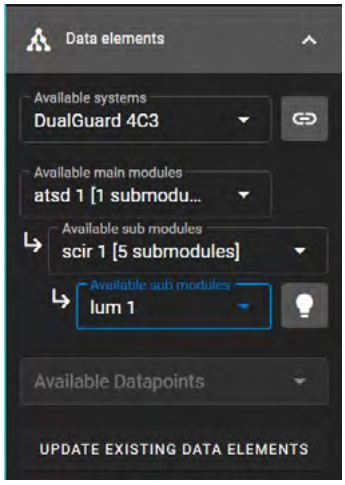


Available systems :

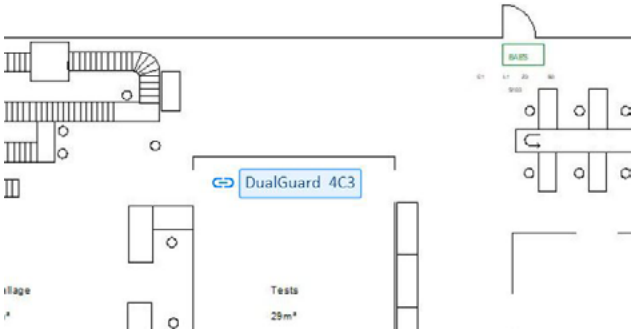
Selection of the desired emergency lighting system via the name of the system.

Available main modules :

Selection of installed submodules, e.g. ATSD (SKUs), Circuits, Luminaires



Via the link symbol  next to "***Available systems***" it is possible to create a system link with the name on the layout.
Size, Rotation and Color see above description.
In later operation, clicking on the symbol opens the system overview with detailed information.



15.4.1 Creation of a status display of the installed emergency lighting system in a layout

To create a status display of a system, please select desired system, e.g. DualGuard-S.

On the selection box "***Available main modules"*** please select "***System***". Right next to the selection box a link

Icon appears:

With left mouse click and hold, move the datapoint to the desired place in the layout where the system is installed.

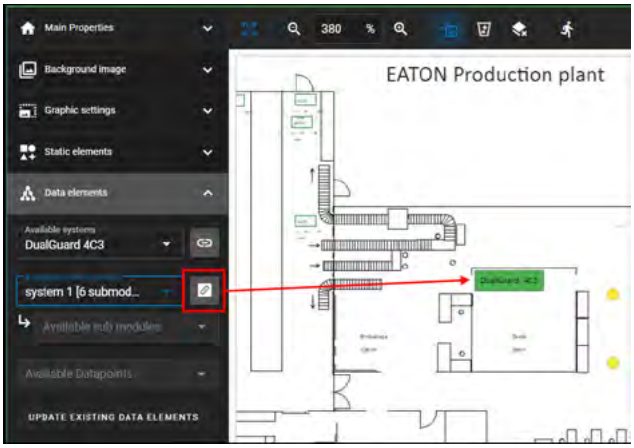
In operation the datapoint shows the name and the status of the system in the layout with color:

Green = System OK

Red = Sum Failure (any Failure on the system)

With click on the datapoint the System overview opens with detailed information.

This procedure is valid for all other systems, such as ZB-S, LP-STAR, AT-S+ and CGLine+ Web-Controller.



15.4.2 Creation of a status display of the installed emergency lighting luminaire in a layout

To create the status display of the installed luminaires of the EML systems, please select desired system, e.g. CGLine+ Web-Controller.

On the selection box "***Available main modules***" please select desired line, e.g. "Line 1". (For DG-S / CG-S select desired ATSD (SKU)).

Under "***Available sub module***s" please select desired zone, e.g. "zone1". (For DG-S / CG-S select desired Circuit (scir)).

In the next box all installed luminaires of that zone will appear. Cick on desired luminaire, e.g. lum1. Right next to the selection box a link

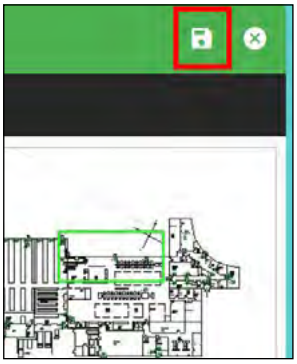
and this icon appears:

With left mouse click and hold, move the datapoint to the desired place in the layout where the system is installed.

To finish a building Layout project (One View) click on

"***Save View***"

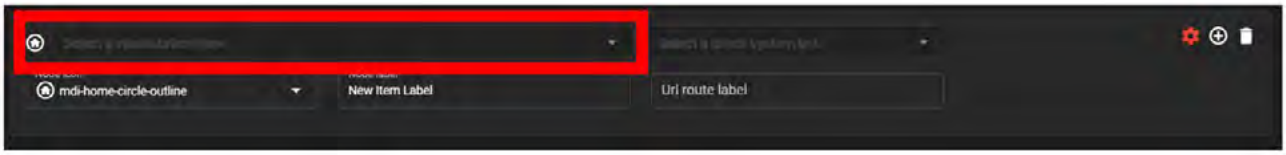
With right mouse click, the look and feel of the luminaire ca be changed, e.g. Size, Shape etc.



15.5 Creation of Building Layouts in the Project Navigation

To use all created graphics you must start a Project navigation, **see Chapter „14.Project Navigation“ on Page 64**

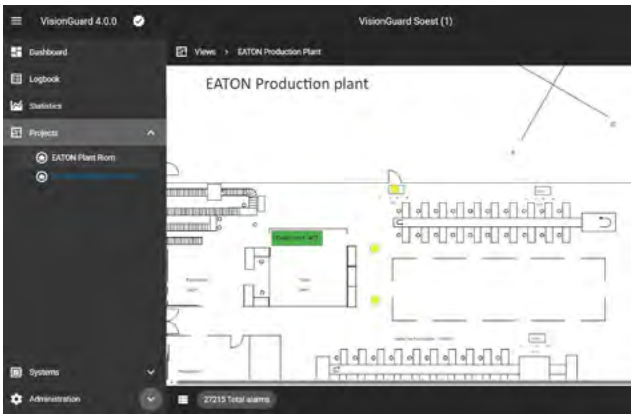
The graphics can be selected in every project level via "***Select a visualisation view***:



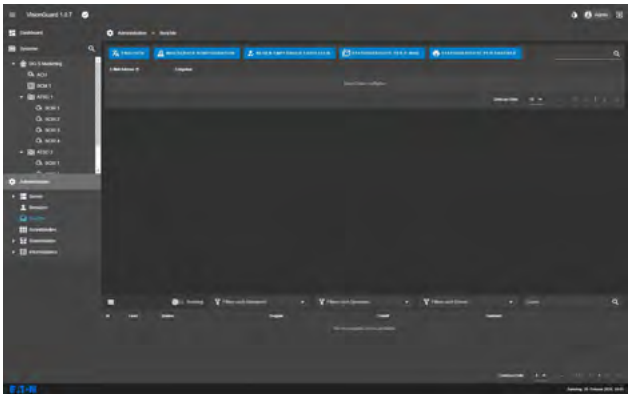
15.6 View of the created building layout images via the project navigation

After creation of all desired building layout graphics in the project navigation, the project navigation must be saved and active according to chapter 14.

There is no limit to the numbers of floor plans and data points used for all systems. Please note that very elaborate and complex project structures require system performance.



16. E-Mail, printing and export function



In the "***Reporting***" menu, you can activate and set up an e-mail, print and export function.

IMPORTANT NOTE

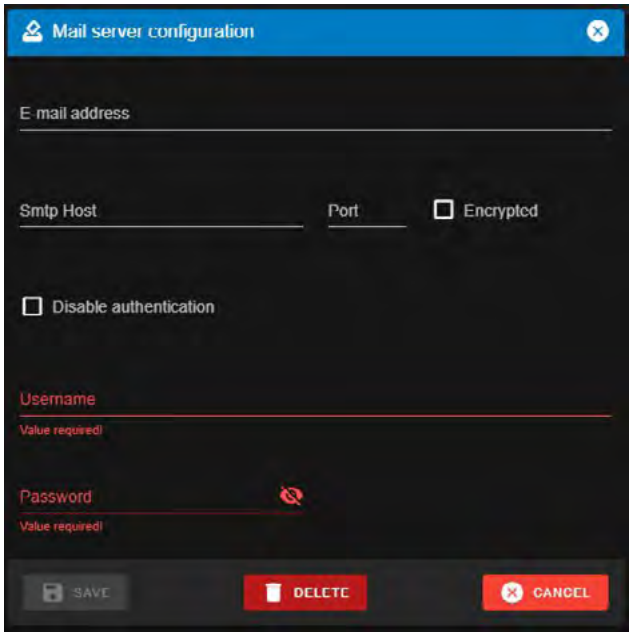
For the access to the Reporting menu, you must be logged in as Administrator or Supervisor.

The reporting language can be set in this menu using the blue button. Please note that the default setting is "***English***".

16.1 E-mail function

VisionGuard has an e-mail client that can send event-based alarm e-mails and an automatic status report with current errors to any e-mail recipient.

16.1.1 Setting up an e-mail server



In order to be able to send e-mails from VisionGuard, an e-mail server must first be set up. This is done via the "***Mail Server Configuration***" button

A configuration window opens

The following data must be entered here:

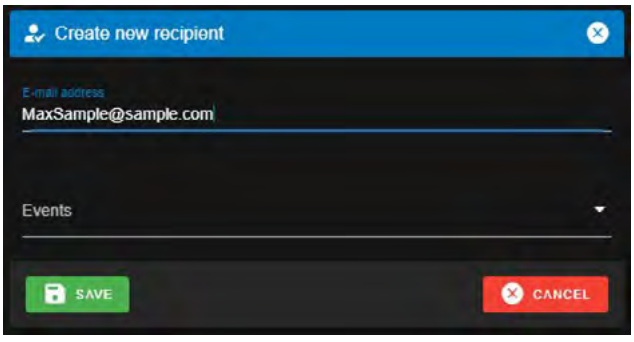
- E-mail address of VisionGuard
  (this will then appear as the sender in the mail)
- Address of the mail server
- SMTP port for sending the mail
- Activation of encryption
- Deactivate authentication
- User name and password
  (not necessary if authentication is deactivated)

Contact your IT department for the correct e-mail server data.

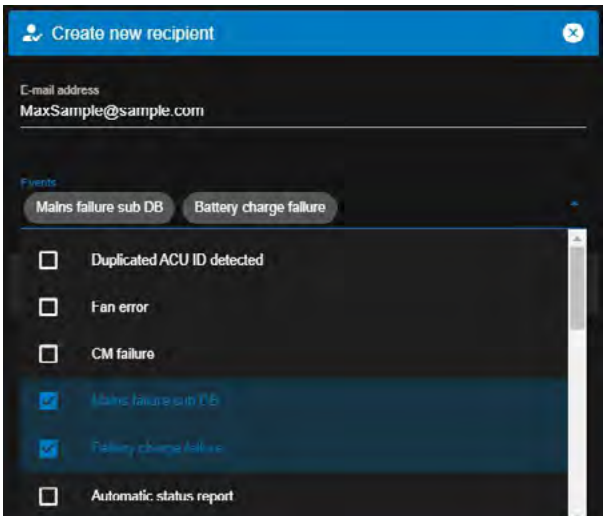
16.1.2 Creating e-mail recipients

Click the "***Create e-mail recipien***t" button to create an e-mail recipient.

The following configuration window opens

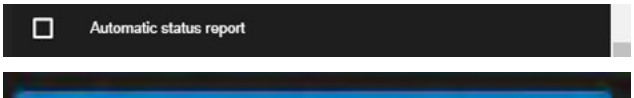


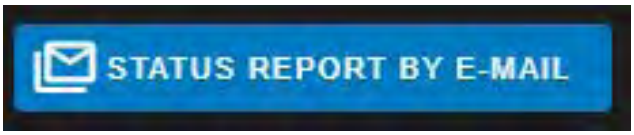
A valid recipient e-mail address must be entered at the top. Clicking on ***Events*** opens a selection of events. If an e-mail is to be sent when a desired event occurs, this must be activated by checking the box. If the event occurs, an alarm e-mail is sent accordingly.



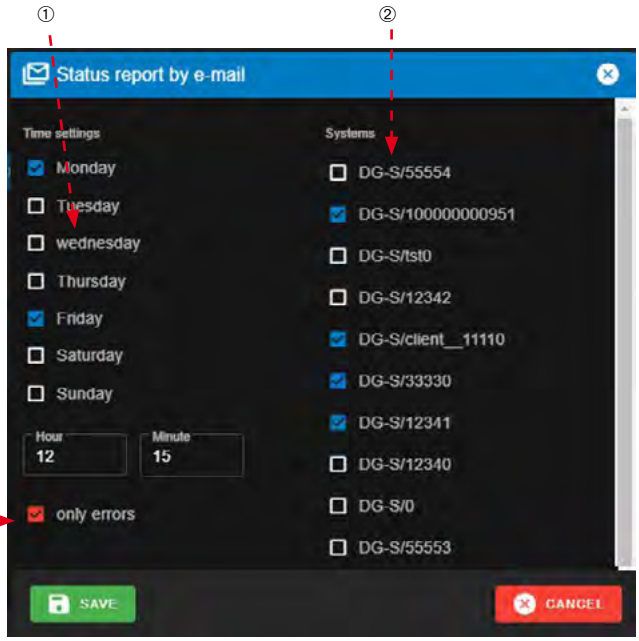
16.1.3 Automatic status e-mail

If "***Automatic status report***" is selected in the above selection field, the parameters for sending the automatic e-mail must then be set. To do so, click on the "Status reports via e-mail" button





The following configuration window appears

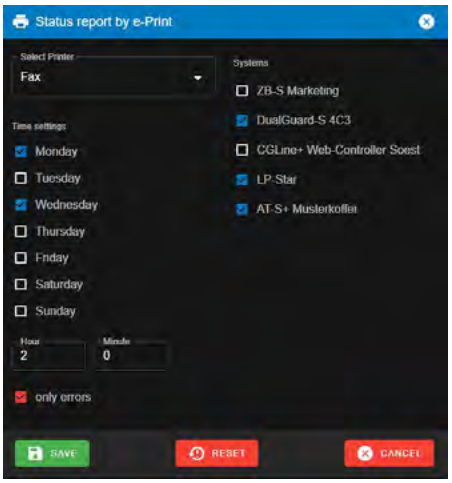


① Here you can set the days of the weekday and the time when the status e-mail is to be sent.
② All emergency lighting systems whose status is to be displayed in the e-mail can be selected here.
③ If "Faults only" is enabled, only faults will be displayed in the e-mail. If this field is disabled, all components with statuses are listed in the e-mail. Depending on the scope of the emergency lighting systems, the e-mail might be very long.

The example shows the content of a status report by e-mail with:
- Header text with information
- Device name with additional text
- System status in the event of a fault Lines with detailed information:
- Fault status
- Status of the affected module

16.2 Print function

VisionGuard has an automatic print function that can be activated by click on the "***Status reports via printer***" button

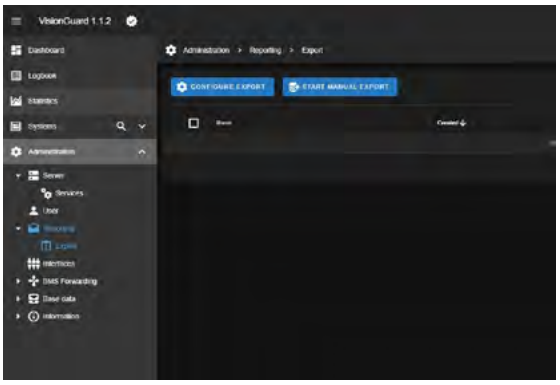


IMPORTANT NOTE

An automatic printout is only possible on the VisionGuard server, where a standard printer is preinstalled.

In the following configuration window, the printer can be selected in the drop down menu "***Select printer***".

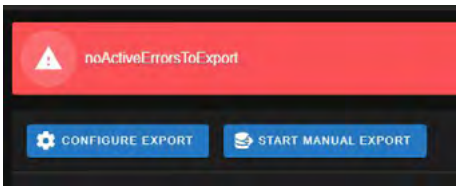
In the below selection menu the day, time and the systems can be selected.
With activation of "***only errors"*** only the failure status of effected systems will be printed.



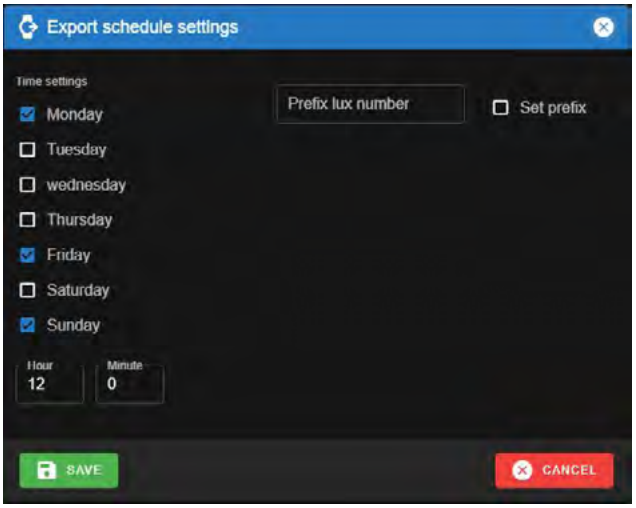
16.3 Export function

The "***Export***" function in the "***Reporting***" menu allows to export all occurred faults of the EL systems in an Excel-based .csv file, e.g. for further processing by external applications.

When the Export menu is selected, a black screen with two buttons appears "***Configure Export***" and "***Start Manual Export***".
Using the function "***Start Manual Export***", a .csv file with all faults is directly generated, which can be exported to any folder, e.g. a network drive.
In case no expert file can be generated, e.g. if there are no faults, the following message appears

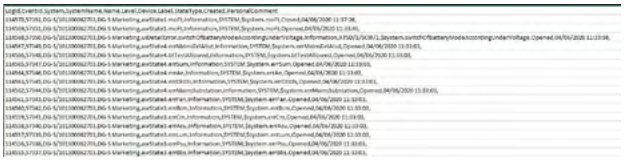


With „***Configure Export***" an automatic export of the .csv file can be configured. The following configuration window appears



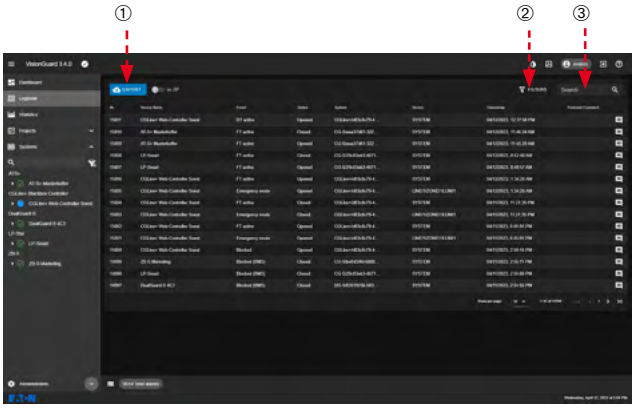
Via „Time settings" certain weekdays and the time of the automatic export can be configurated.
Via „Set prefix" a desired prefix can be defined before the export

The content of the .csv file has following structure with commas separation:
LogId,EventId,System,SystemName,Name,Level,Device, Label,StateType,Created,PersonalComment
Extract from the .csv:

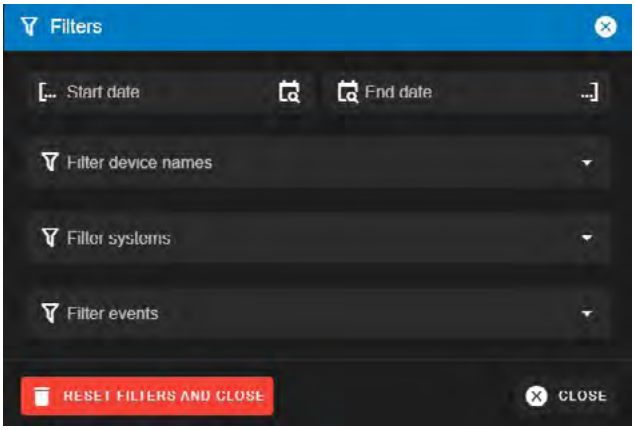


17. Logbook

VisionGuard has a Logbook function to fulfill all requirements in accordance with DIN EN 50172/DIN VDE V 0108-100-1. The Logbook is in the second position in the navigation bar. Since the minimum period covered by the Logbook is the last 4 years, there may be a large number of log entries. In order to display these clearly, or to be able to quickly find the desired entries, the Logbook has many filter functions as well as a search function.
In the default settings, the most recent Logbook entries are displayed at the top of the list.

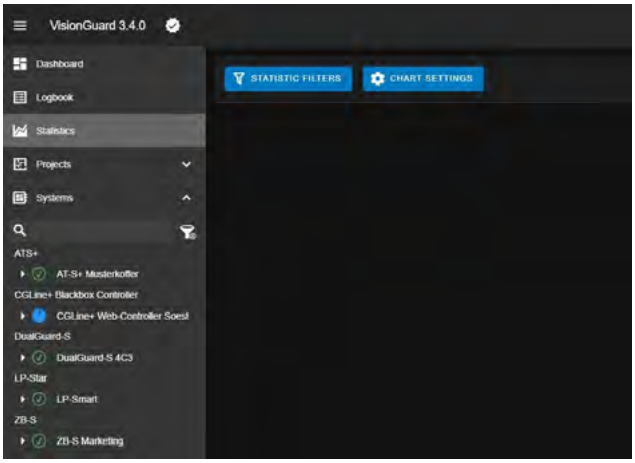


① The Logbook can be downloaded in the Excel-readable format .csv by clicking "***Export***." In order to significantly reduce the download time if the Logbook contains many entries, it is advisable to download the file compressed as a ZIP file.
② With click on "***Filters***" a new windows appears. Here you can narrow down the Logbook by date and time (time range). Furthermore the filters allows filtering by device name and event (multiple selection is possible)
③ With the search bar, it is possible to search for an event according to the event name



18. History menu (only for DG-S/LS-S and CG-S systems)

In the History menu (Statistics), the four battery analog values such as battery voltage, battery current, battery room temperature and the state of charge of the battery can be displayed in a configurable graph over time. This function illustrates nicely e.g. the course of a battery duration test.
This can help to determine the quality of the battery or detect temperature outliers of the battery environment.



IMPORTANT NOTICE

It is recommended to use reasonable settings.
It is possible to set ranges or times that may not represent favorable progressions over time. For example, it makes little sense to evaluate a 1-hour duration test over a period of 1 month. Also very short intervals, e.g. the current curve over 10 minutes shows the high clocking of the charging technology, which may be misinterpreted.

When the History (Statistics) menu is selected, a black screen with two buttons appears "***Statistic Filters***" and "***Chart Settings***".

The graphics can be preconfigured in the ***Settings menu***:

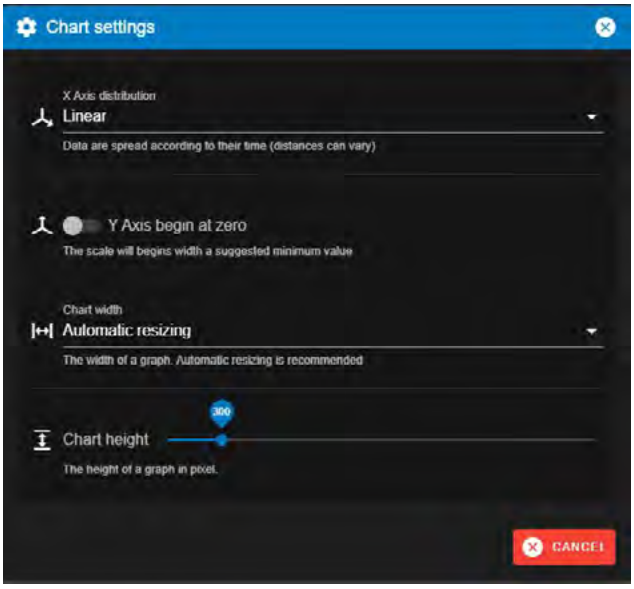
Following configurations can be made for the graphics

X Axis distribution:
Linear = Data are spread according to their time (distances can vary - Recommended settings)
Series = Data are spread at the same distance from each other

Y Axis begins at zero:
Disabled = Data is displayed on the Y-axis in the data area
Enabled = Data is displayed on the Y-axis from 0

Chart width:
Allows to adjust the size of the chart width.
Automatic resizing (recommended setting)
Large 100%
Medium 50%
Small 25%

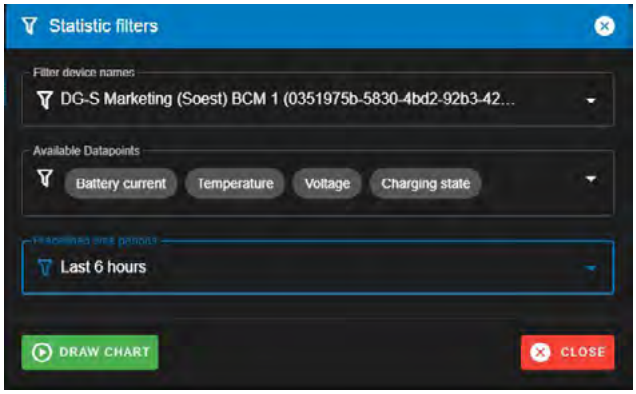
Chart height:
Allows to adjust the size of the chart height from 200 to 1000 pixel.
Presetting is 300 pixel.



With click on "***Statistic filters***" a new window appears.

Via „***Filter device names***" the desired DG-S / LS-S or CG-S system can be selected.
Via "***Available datapoints***" the desired battery analogue values "***Battery voltage***", "***Battery current***", "***Temperature***" and "***Charging state***" can be selected. Example shows all available datapoints.

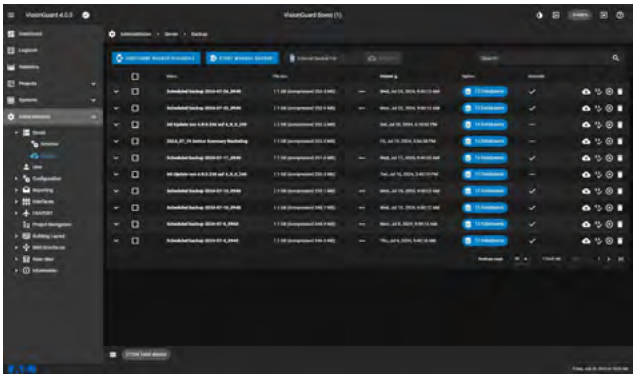
With "***Predefined time periods***" you can choose between different times for the drawings, e.g. Last 6 hours to see the discharge behavior of a battery duration test.



For example, it is quickly possible to look at the battery values directly after a battery duration test via "last hour".
In order to display the graphics clearly, the maximum number of recording points can be defined at the end. Presetting is 100 number of records.
The graphics are generated automatically after entering all parameters, e.g.
Graphic of the last 30 days about the battery current and the battery room temperature:

19.Backup & Restore Menu

The VisionGuard provides a Backup & Restore menu under Administration > Server > Backup.
It allows to easily create a backup and restore the entire configuration, e.g. in case of a system crash, or for moving to a new PC environment.

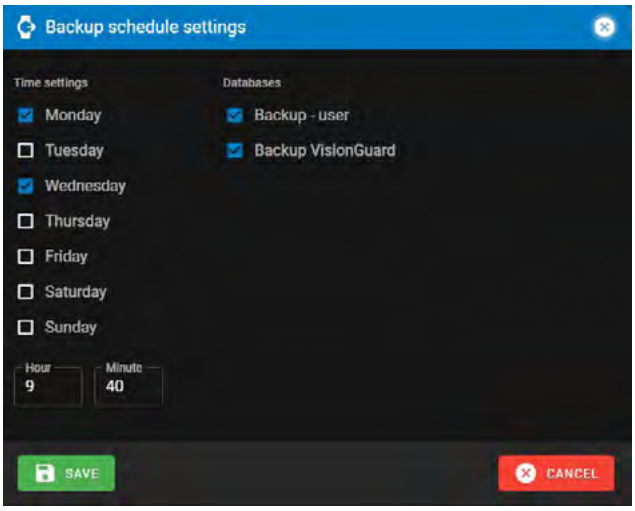


19.1 Creation of automatic Backups

Via the button "Configure Backup Schedule" it is possible to create automatic Backups.
Under time settings the weekdays and the time can be selected.
Under databases, the service for the Backup can be selected.
1. Backup - user
Create a Backup of the UAC

2. Backup VisionGuard
Create a Backup of all other settings and configurations

Please activate both items for a full backup



IMPORTANT NOTE

Please consider that backups requires a lot of drive space! Please provide enough memory or delete older backups.

19.2 Creation of manual Backup

Via the button "Start manual Backup" it is possible to create a Backup immediately.

Please create a name for the Backup and a description if required.

Under databases, the service for the Backup can be selected.
1. Backup - user

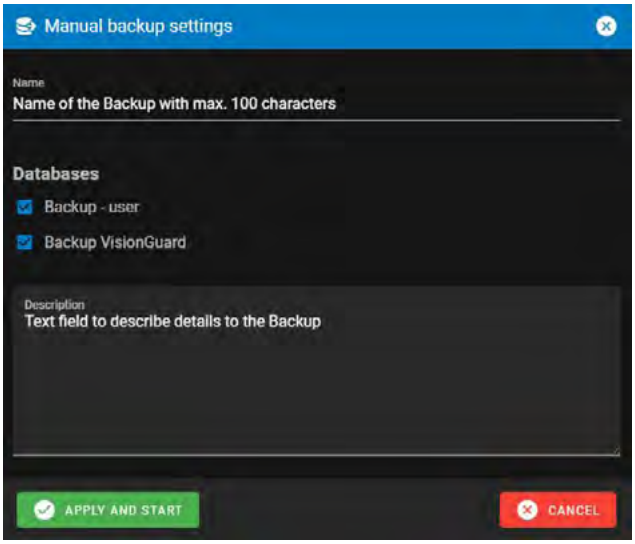
Create a Backup of the UAC

2. Backup VisionGuard

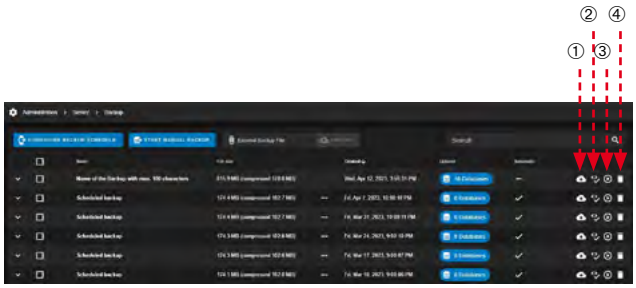
Create a Backup of all other settings and configurations

Please activate both items for a full backup.

With "Apply and Start" the download will be started, and create an entry in the Backup list.



After creation of the manual backup, it will be listed with name and the size. On the right side following actions are possible:
(1) Download of the backup to the client PC
(2) Check the Backup compatibilty to this VisionGuard
(3) Restore the VisionGuard with this Backup
(4) Delete the Backup

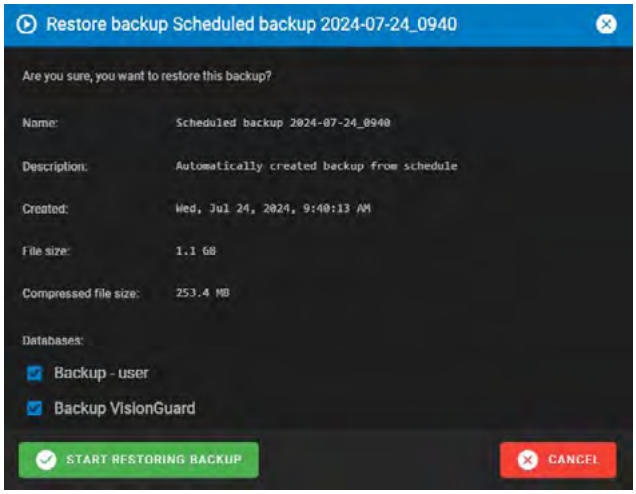


19.3 Creation of a manual restore

Via the button (3) it is possible
to restore the VisionGuard with a created Backup file.

Select which databases should be restored. It is recommended to select both. With click on "Start Restoring Backup", the VisionGuard will be restored with the desired Backup.

After some Minutes the System is restored to the desired configuration.



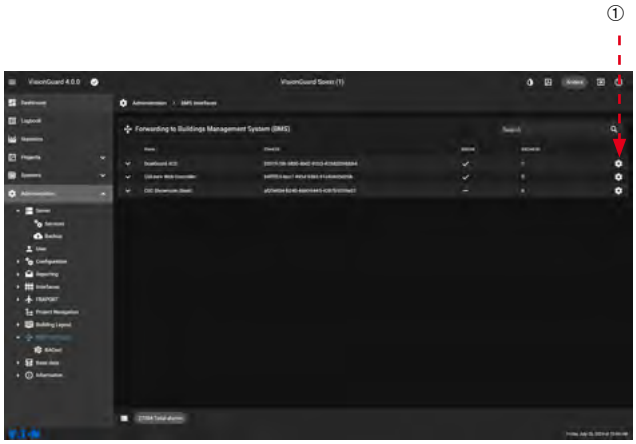
20. BACnet/IP Interface for DG-S/LS-S, ZB-S, AT-S+, LP-STAR and CGLine

For each emergency lighting system following number of BACnet objects on System level are available:

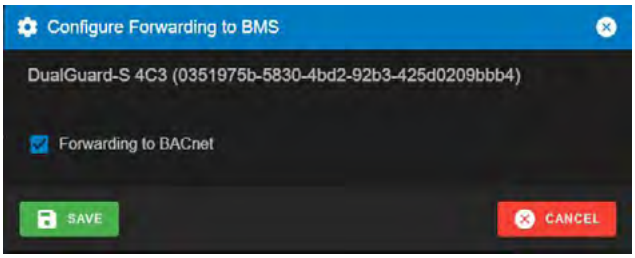
DG-S/LS-S:	64 objects
ZB-S:	59 objects
AT-S+:	48 objects
LP-STAR:	55 objects
CGLine+:	54 objects

The BACnet/IP interface descritions for all Emergency Lighting Systems with detailed information are available as separate documents on demand.

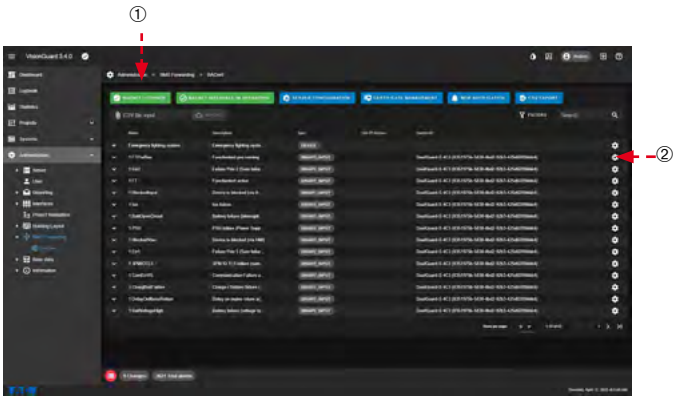
If a BACnet/IP licence has been purchased and activated, the menu item „***BMS Forwarding***" with the submenu „***BACnet***" appears in the administration area. In the menu "***BACnet forwarding***" it is possible to activate the BACnet/IP interface for each individual emergency lighting system. This can be configured via the gear symbol ① (e.g. DG-S).



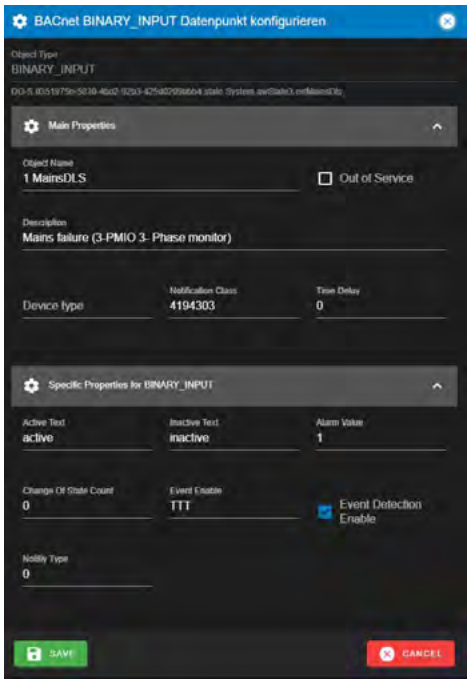
The following window opens. With a check mark „Forwarding to BACnet“ the BACnet interface can be activated for these DualGuard-S / LoadStar-S. With „Save“ the setting will be saved.



In the submenu „BACnet“ you can now check if the BACnet licence and the BACnet server for connecting a BMS is activated in green. ①
The list shows all active BACnet objects. The BACnet data points (BACnet objects) can now be configured for the BMS via the gear wheel symbol ②.



Example „Mains failure 3-Phase monitor“. The following configuration window for the BACnet object opens:

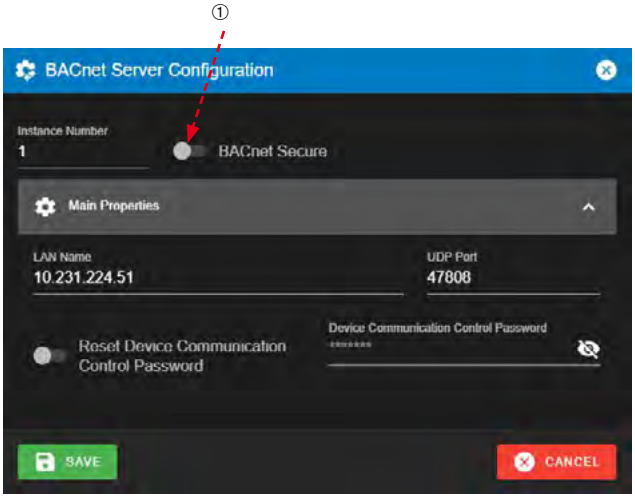


The Object type specifies the BACnet object type, e.g. BINARY_INPUT. This is a fixed value.
The “Main properties” and the “Specific properties” for the BACnet Object type „BINARY_INPUT“ can now be configured according to the BACnet specification for the BMS connection, e.g. the “Description” describes the meaning of the BACnet Object, in this case „Mains Failure 3-PM-IO 3 Phase monitor”.
This information text on the BMS can be changed as required.
The other settings should be specified by the BACnet BMS Integrator.

Explanation of the menus:

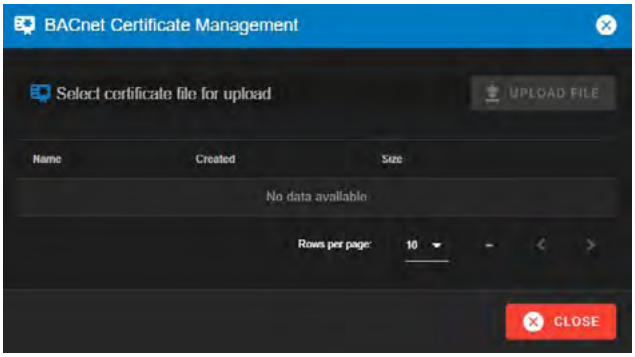
BACnet Server configuration

In this configuration menu the settings for the BACnet server can be done:
The “Instance number” is important for the unique identification of the DualGuard-S / LoadStar-S system on the BMS side.
If BACnet Secure is required, it must be activated here ①. For further settings it is possible to configure BACnet secure settings under “CERTIFICATE MANAGEMENT”.



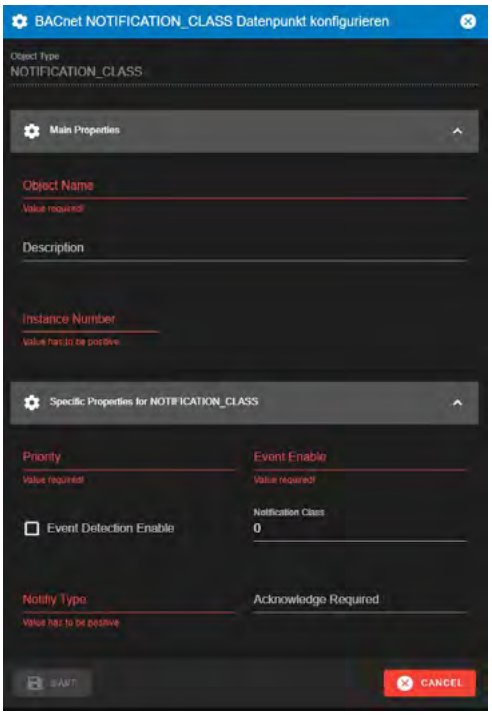
Certificate Management

A valid BACnet certificate can be loaded in the following dialog window.



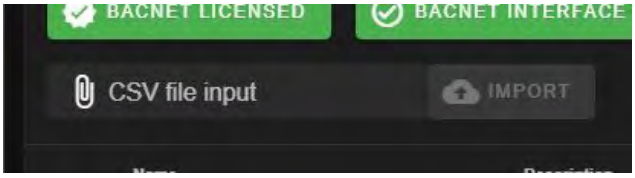
New Notification (Notification Classes)

If required for the BMS notification classes, these can be configured in the „NEW NOTIFICATION“ menu.
Here the corresponding object names can be selected and under „Specific Properties for NOTIFICATION_CLASS“ the priority and „Event Enable“ can be set. For the notification class 3 numbers are allowed between 0 and 255. (Specification from the BMS integrator)
Only 3 letters are allowed for the „Event Enable“, with T or F, which stand for T=“True” or F=“False”.



CSV EXPORT

With CSV Export it is also possible to make the Bacnet configuration via a csv. table e.g. via Excel. The .csv file will be available as download of the web browser. After changing all data (important: everything must fit!) the csv. file can be loaded via the CSV file input „IMPORT“ function.

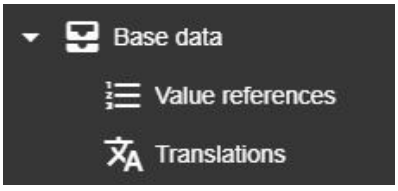


21.21 Administration area

IMPORTANT NOTE

The administration area is only accessible for administrators and supervisors!

In the VisionGuard administration area, you can restart services, manage users and licences and information read about open source and changes in the different VisionGuard versions. **Do not make any changes in the Base data folder "Value references" and "Translations"!**
This may cause a mailfunction of the software!



22.Notes

Eaton is an intelligent power management company dedicated to protecting the environment and improving the quality of life for people everywhere. We make products for the data center, utility, industrial, commercial, machine building, residential, aerospace and mobility markets. We are guided by our commitment to do business right, to operate sustainably and to help our customers manage power – today and well into the future. By capitalizing on the global growth trends of electrification and digitalization, we're accelerating the planet's transition to renewable energy sources, helping to solve the world's most urgent power management challenges, and building a more sustainable society for people today and generations to come.

Eaton was founded in 1911 and has been listed on the New York Stock Exchange for more than a century. We reported revenues of $23.2 billion in 2023 and serve customers in more than 160 countries. For more information, visit **www.eaton.com**. Follow us on LinkedIn.

Eaton
EMEA Headquarters
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
Email: **info-n@ceag.de**
Website: **www.eaton.com**

© 2024 Eaton
All rights reserved
Printed in Germany
Article no. 40071860371 (J)
Publication number MN451070EN
June 2025

Eaton is a registered trademark.

All other trademarks are the property of their respective owners.

Powering Business Worldwide

www.eaton.com/recycling