

## Operating Instructions Eaton VisionGuard

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



## Content

<b>1 Foreword and system requirements .....</b>	<b>4</b>	<b>6 Creating new users with user roles .....</b>	<b>28</b>
1.1 Foreword .....	4	6.1 User Account Control (UAC) information .....	28
1.2 Important information about VisionGuard cybersecurity in Ethernet networks.....	4		
1.3. System requirements – hardware/software requirements.....	9	<b>7 Adding DualGuard-S systems to VisionGuard .....</b>	<b>30</b>
1.4 Important information before installation .....	10	7.1 Configuring the HMI to connect to VisionGuard.....	30
1.4.1 Used Ports and Protocols.....	10	7.2 Adding and authorizing a DualGuard-S system in VisionGuard.....	32
1.4.2 Used Services and standard installation path.....	10	<b>8 Adding ZB-S systems to VisionGuard .....</b>	<b>34</b>
1.4.3 Prerequisite for a VisionGuard software installation	10	8.1 Configuring the CG-S Gateway.....	34
1.5. VisionGuard licenses .....	10	8.2 Adding and authorizing a ZB-S system in VisionGuard .....	35
1.5.1 Licensing models .....	10	8.2.1 Create new Groups and adding and authorizing ZB-S systems in VisionGuard .....	36
1.5.2 Licensing procedure.....	10		
<b>2 Installation instructions .....</b>	<b>11</b>	<b>9 Basic graphic layout and structure of VisionGuard .</b>	<b>38</b>
2.1 Installation of the VisionGuard software .....	11	9.1 Login screen .....	38
2.2 Installation of the CG-S Gateway software.....	14	9.2 Dashboard .....	38
2.3 Installation of the CG-S Interface driver package .....	17	9.2.1 System graphic and system status.....	39
2.4 Updating an already installed version of VisionGuard, CG-S Gateway and CG-S driver package .....	19	9.2.2 Server statistics .....	40
2.4.1 Update description of VisionGuard Software .....	19	9.2.3 Database and system services status indicators....	40
2.4.2 Performing an update of VisionGuard .....	19	9.2.4 Contacts .....	41
2.4.3 Update of a CG-S Gateway and the CG-S driver package .....	19	9.3 System overview .....	41
2.5 Deinstallation of VisionGuard software components.	20	9.4 Alarm list.....	41
<b>3 First launch of VisionGuard .....</b>	<b>20</b>	<b>10 DualGuard-S visualization .....</b>	<b>42</b>
3.1 Local access (VisionGuard server and client on a PC)	20	10.1 DualGuard-S detail view.....	42
3.2 Access to remote VisionGuard server (VisionGuard server and client on a different PC).....	21	10.2 ACU detail view .....	42
		10.3 BCM detail view.....	42
<b>4 License information.....</b>	<b>22</b>	10.4 BDM detail view .....	42
4.1 Activating a license .....	22	10.4.1 BBS detail view.....	43
		10.5 ATSD detail view (SKU).....	43
<b>5 Security certificate installation .....</b>	<b>24</b>	10.6 Luminaire detail view .....	43
5.1 Installing the security certificate via local access .....	24	10.7 Configuration of a DualGuard-S.....	44
5.2 Installation of the security certificate via remote access .....	27	10.7.1 System configuration.....	44
		10.7.2 ACU configuration .....	45
		10.7.3 SKU (ATSD) configuration .....	45
		10.7.4 IO, 3PM-IO, TLS configuration .....	45

<b>11 ZB-S Visualization .....</b>	<b>46</b>
11.1 ZB-S detail view.....	46
11.2 CU detail view .....	46
11.3 BCM detail view .....	47
11.4 SKU detail view .....	47
11.5 Luminaire detail view.....	47
 <b>12 E-Mail, printing and export function.....</b>	 <b>48</b>
12.1 E-mail function .....	48
12.1.1 Setting up an e-mail server.....	48
12.1.2 Creating e-mail recipients.....	49
12.1.3 Automatic status e-mail.....	50
12.2 Print function .....	50
12.3 Export function .....	51
 <b>13 Log book.....</b>	 <b>52</b>
 <b>14 History menu .....</b>	 <b>52</b>
 <b>15 Backup &amp; Restore Menu .....</b>	 <b>54</b>
15.1 Creation of automatic Backups.....	55
15.2 Creation of manual Backup.....	55
15.3 Creation of a manual restore .....	55
 <b>16 BACnet/IP Interface for DualGuard-S .....</b>	 <b>56</b>
 <b>17 Administration area .....</b>	 <b>59</b>
17.1 Services .....	59

# 1 Foreword and system requirements

## 1.1 Foreword

VisionGuard is a modern web-based monitoring, control and configuration software for the new DualGuard-S and monitoring and control software for ZB-S central battery systems. In next versions it will be expanded to include the configuration and CG-S bus-based emergency lighting systems AT-S+ and LP-STAR as well as the latest self contained battery system CGLine+.

### Features:

- Web-based client/server architecture for independent operation by multiple users
- For up to 500 emergency lighting systems (DualGuard-S or ZB-S)
- User Account Control (UAC) with 4 user roles for assigning different access rights (Supervisor, Administrator, Power User and User)
- Developed and verified for cybersecurity (EATON certified)
- Software license without hardware dongle key (Software download)
- Modern dashboard display as start page
- Responsive web design (automatic adjustment to different display sizes)
- Modern MQTT communication protocol (event-based communication)
- System overview of all systems in one screen
- Complete visualization and control
- Automatic function tests and service life tests for each device
- Extensive log book 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 protocol (only for DG-S)
- Occurring faults can be conveniently forwarded to external applications via an integrated export function
- 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 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.
- 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](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](http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf)

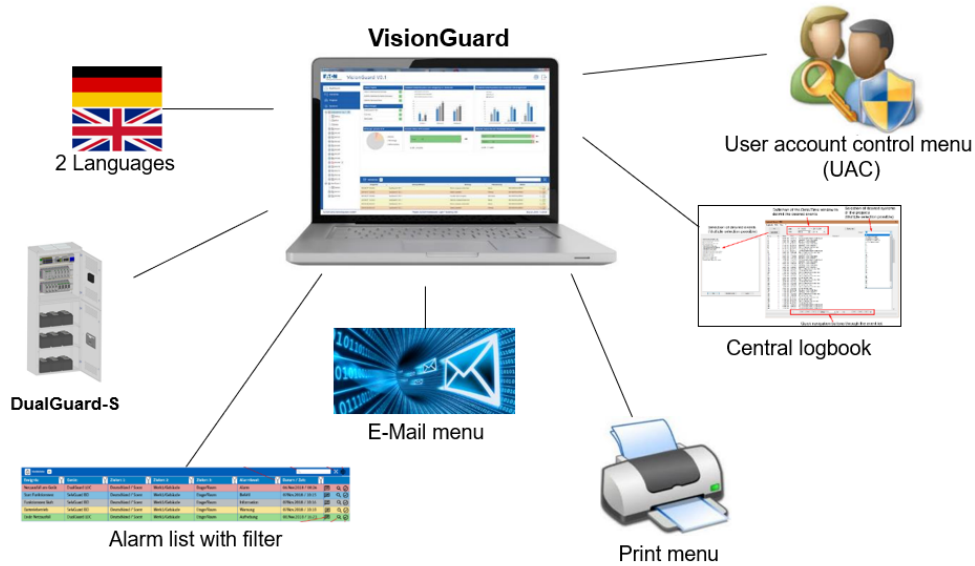
**[R2] Cybersecurity best practices checklist reminder (WP910003EN):** <https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf>

**[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](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)

## 1 Foreword and system requirements

Category	Description
<b>Intended Use &amp; Deployment Context</b>	<p>VisionGuard is a visualization software to monitor, control and configure DualGuard-S and monitor and control ZB-S Emergency Lighting Systems.</p> 
<b>Asset Management</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• (Software) Publisher, name, version, and version date.</li> </ul> <p>Please read the corresponding pages of the manual to get information how to find out these parameters.</p>
<b>Risk Assessment</b>	<p>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.</p>
<b>Physical Security</b>	<p>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.</p> <p>Following are some best practices that Eaton recommends to physically secure your system/device:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Restrict physical access to cabinets and/or enclosures containing VisionGuard and the associated system. Monitor and log the access at all times.</li> <li>• 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.</li> <li>• VisionGuard supports the following physical access ports. A network (RJ45) ports access should be restricted.</li> <li>• 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.</li> <li>• Before connecting any portable device through a USB port or SD card slot, scan the device for malware and viruses.</li> </ul>

<b>COTS platform security (Commercial off-the-shelf)</b>	<p>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.).</p> <ul style="list-style-type: none"> <li>• Eaton recommends that customers refer to the COTS vendor's documentation for guidance on how to harden these components.</li> <li>• Vendor-neutral guidance is made available by the Center for Internet Security <a href="https://www.cisecurity.org/">https://www.cisecurity.org/</a></li> </ul> <p>Irrespective of the platform, customers should consider the following best practices:</p> <ul style="list-style-type: none"> <li>• Install all security updates made available by the COTS manufacturer.</li> <li>• Change default credentials upon first login.</li> <li>• Disable or lock unused built-in accounts.</li> <li>• Limit use of privileged generic accounts (e.g., disable interactive login).</li> <li>• Change default SNMP community strings.</li> <li>• Restrict SNMP access using access control lists.</li> <li>• Disable unneeded ports &amp; services.</li> </ul>
<b>Account Management</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> <li>• Leverage the roles / access privileges (see manual, chapter 6) 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).</li> <li>• Perform periodic account maintenance (remove unused accounts).</li> <li>• 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).</li> <li>• Enforce session time-out after a period of inactivity.</li> </ul>
<b>Time synchronization</b>	<p>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).</p>
<b>Network security</b>	<p>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].</p> <p>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.</p> <p>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.</p>
<b>Remote Access</b>	<p>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.</p>

## 1 Foreword and system requirements

<b>Log and Event Management</b>	<ul style="list-style-type: none"><li>• Eaton recommends logging all relevant system and application events, including all administrative and maintenance activities.</li><li>• 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.).</li><li>• Ensure that logs are retained for a reasonable and appropriate length of time.</li><li>• 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.</li></ul>
<b>Vulnerability scanning</b>	<p>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.</p> <p>Vulnerability information for the VisionGuard can be obtained by signing up for updates at <a href="http://www.eaton.com/cybersecurity">www.eaton.com/cybersecurity</a> and by checking for vulnerabilities in the National Vulnerability Database (NVD), available at <a href="https://nvd.nist.gov/">https://nvd.nist.gov/</a>. and ICS CERT.</p> <p><i>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.</i></p>
<b>Malware Defenses</b>	Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.
<b>Secure maintenance</b>	<b>Best practices</b> Please check Eaton's cybersecurity website ( <a href="http://www.ceag.de">www.ceag.de</a> ) for information bulletins about available firmware and software updates.
<b>Business continuity/ cybersecurity disaster recovery</b>	<p>Plan for Business Continuity / Cybersecurity Disaster Recovery</p> <p>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:</p> <ul style="list-style-type: none"><li>• Updated software for VisionGuard. Make it a part of standard operating procedure to update the back-up copy as soon as the latest software is updated.</li><li>• Current configuration.</li><li>• Documentation of the current permissions / access controls, if not backed up as part of the configuration.</li></ul>
<b>Sensitive Information Disclosure</b>	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.

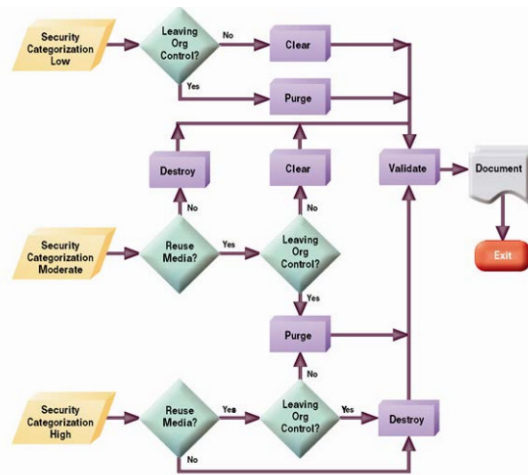


Figure 4-1: Sanitization and Disposition Decision Flow

#### • 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 licensed 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

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

**Operating system:** WIN 10 (64-bit), WIN server 2016, WIN server 2019

**Processor:** min. Intel Core i5 or AMD Ryzen 5

**Memory (RAM):** min. 8 GB, strongly recommended 16 GB DDR4 SDRAM

**HDD:** min. 256 GB SSD

### Client

**Hardware:** 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 24-inch FullHD

**Optimal resolution:** Full HD 1920x1080 or higher

**Peripheral devices:** Keyboard, mouse, printer

## 1.4 Important information before installation

### 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)
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\erl10.5	RabbitMQ Runtime
RabbitMQ	C:\Program Files\RabbitMQ Server	Messagebus
RabbitMQ Logs	C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\RabbitMQ	Logs of Messagebus
MSSQL 2019	C:\Program Files\Microsoft SQL Server	Database Server
VisionGuard	C:\Program Files\EATON\VisionGuard	Actual Software
VisionGuard Logs	C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\EATON\VisionGuard	Logs of the individual services

#### 1.4.3 Prerequisite for a VisionGuard software installation

- Care should be taken 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.

### 1.5. VisionGuard licenses

#### 1.5.1 Licensing models

VisionGuard is protected against unauthorized operation. A license is required to activate VisionGuard. The type of license depends on the DualGuard-S or ZB-S systems connected. A „device“ can be a Battery system or a substation with a Control unit (HMI or CU-S). Upgrading to a higher volume license is possible. The following volume licenses 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 (only for DG-S), for ZB-S in preparation

All VisionGuard version licenses 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

When a license 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 license purchased, this generates an activation key in the form of a license file in the file format ".v2c." (.Vendor to Customer) .

This license 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 Section 4 Licensing

## 2 Installation instructions

### Installation notes:

If only DualGuard-S (DG-S) systems are to be connected to the VisionGuard, it is sufficient to install only the VisionGuard software (see 2.1). If ZB-S emergency lighting systems 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 and 2.3)

### IMPORTANT NOTE

Depending on the system, an installation or an update procedure can take a longer time (up to 45 minutes) without any

## 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\_V3.1.0.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.“

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 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 5000. The standard ports 80 for unencrypted HTTP access and 443 for encrypted HTTPS access are set as web client ports.

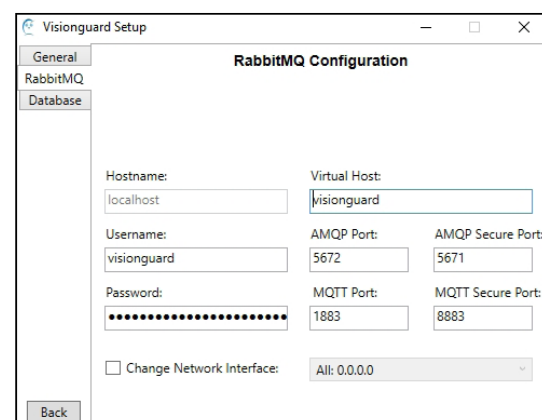
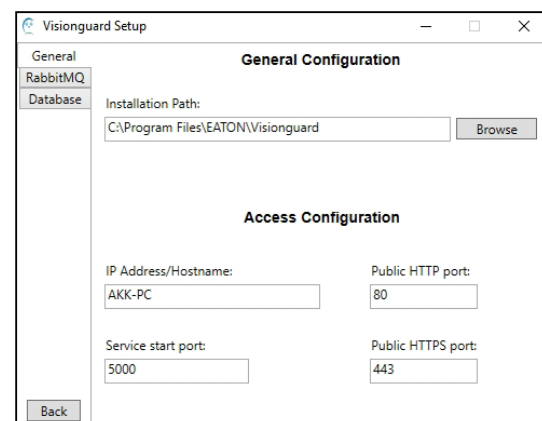
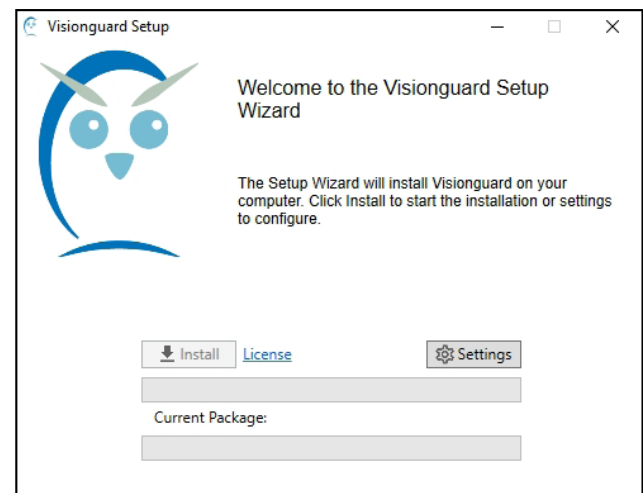
### Settings > RabbitMQ

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).

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 [www.eaton.com](http://www.eaton.com).**

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.

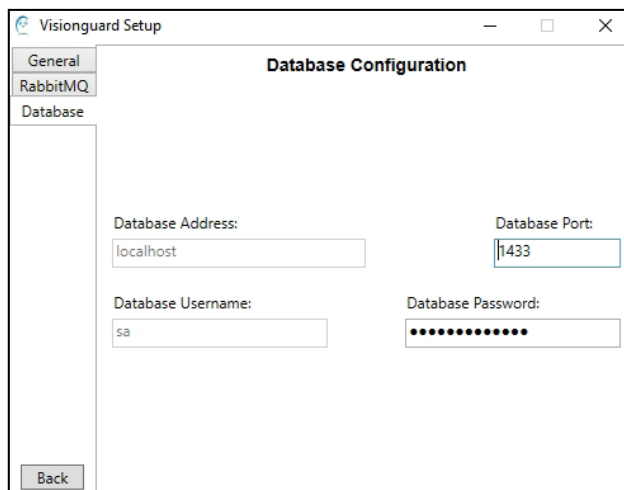


## 2 Installation instructions

### Settings > Database

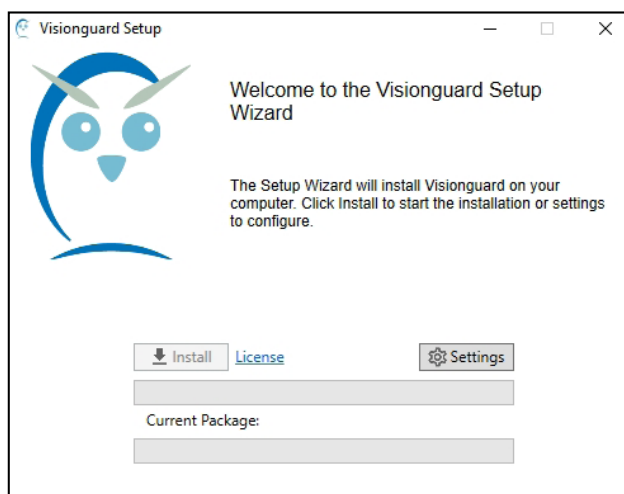
In this dialog box, the specifications of the MSSQL database can be changed.

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



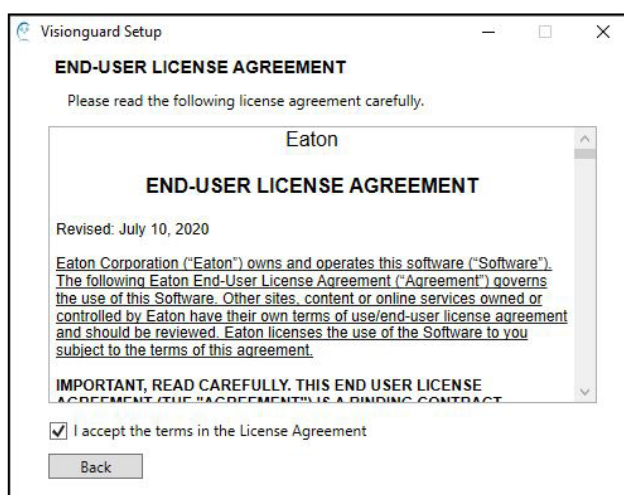
The screenshot shows the 'Database Configuration' window in the Visionguard Setup application. The window has a sidebar with 'General', 'RabbitMQ', and 'Database' tabs, with 'Database' selected. The main area contains four input fields: 'Database Address' (localhost), 'Database Port' (1433), 'Database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

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



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

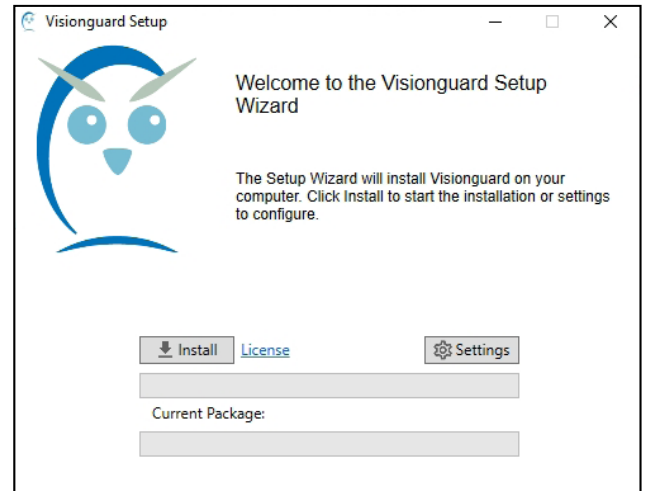
Please read the end-user license agreement (EULA) carefully and confirm the EULA by enabling "I accept the terms in the License Agreement."



The screenshot shows the 'END-USER LICENSE AGREEMENT' window. It displays the Eaton logo and the title 'END-USER LICENSE AGREEMENT'. The text states: 'Revised: July 10, 2020' and 'Eaton Corporation ("Eaton") owns and operates this software ("Software"). The following Eaton End-User License Agreement ("Agreement") governs the use of this Software. Other sites, content or online services owned or controlled by Eaton have their own terms of use/end-user license agreement and should be reviewed. Eaton licenses the use of the Software to you subject to the terms of this agreement.' Below this, it says 'IMPORTANT, READ CAREFULLY. THIS END USER LICENSE AGREEMENT (THE "AGREEMENT") IS A BINDING CONTRACT.' At the bottom, there is a checkbox labeled 'I accept the terms in the License Agreement' which is checked, and a 'Back' button.

Click "Back" to go back.

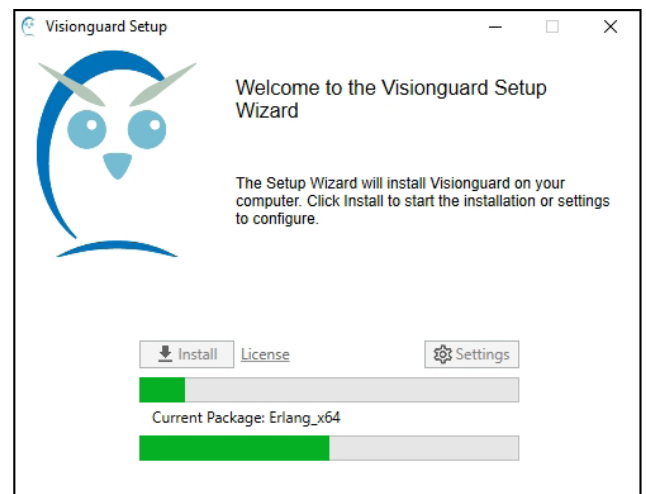
The installation can now be started by clicking "Install"



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.

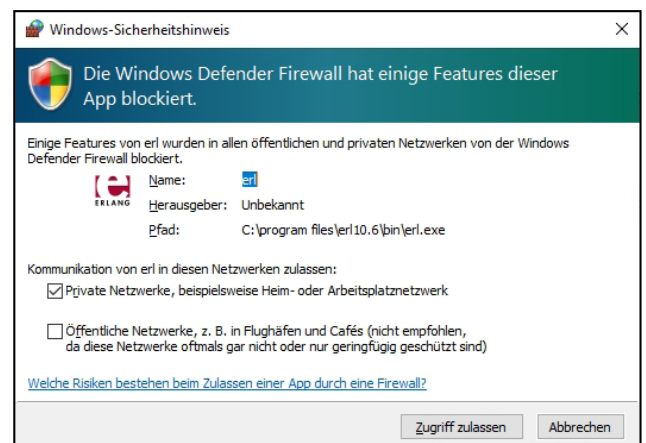
### NOTE

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:

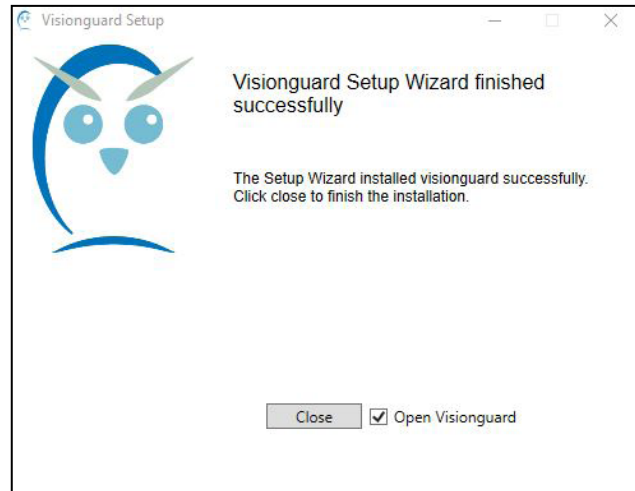
All accesses must be permitted, otherwise the HMIs of the DualGuard-S will not be able to establish a connection to VisionGuard!



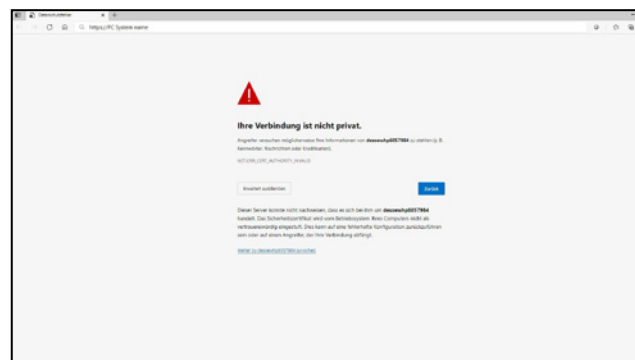
## 2.2 Installation of the CG-S Gateway software

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

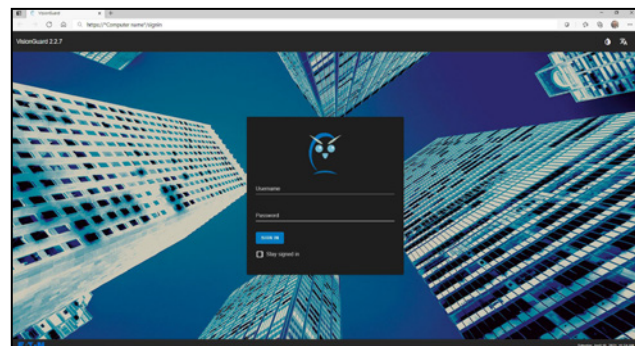
The installation of the VisionGuard software is now complete. It is recommended to activate „Open VisionGuard“. With Click on „Close“ the standard browser starts with the URL of the VisionGuard. If ZB-S emergency lighting systems are to be connected to the VisionGuard as mentioned above, gateway software and a CG-S interface driver package must also be installed. Please then perform the installations described in 2.2 and 2.3.



VisionGuard uses the Computer name for the local client access. 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“



Via „Advanced“ and „Continue to \*computer name\* (insecure)“, you get to the login page of the local VisionGuard. It is recommended to set a Book mark in the web browser now. To finish the installation it is strongly recommended to restart the PC.



## 2.2 Installation of the CG-S Gateway software

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



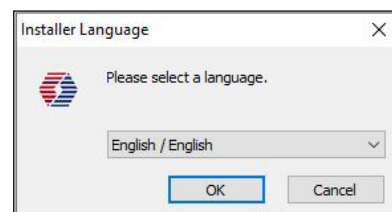
**CG-S-Gateway\_1.0.2.0\_Install.exe**

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.

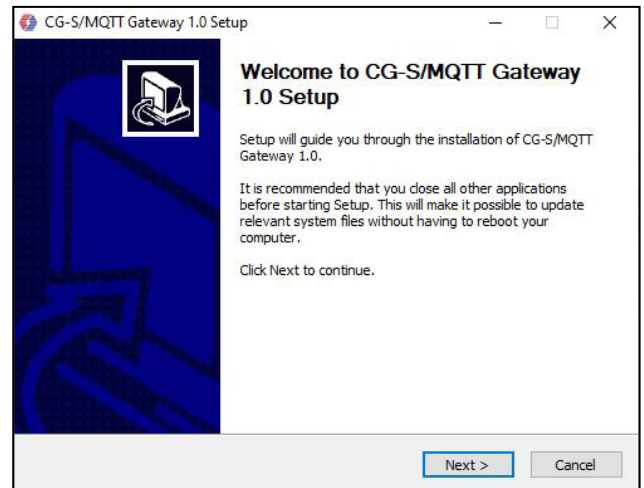
It is possible to choose between German or English. Select the desired language and click OK.



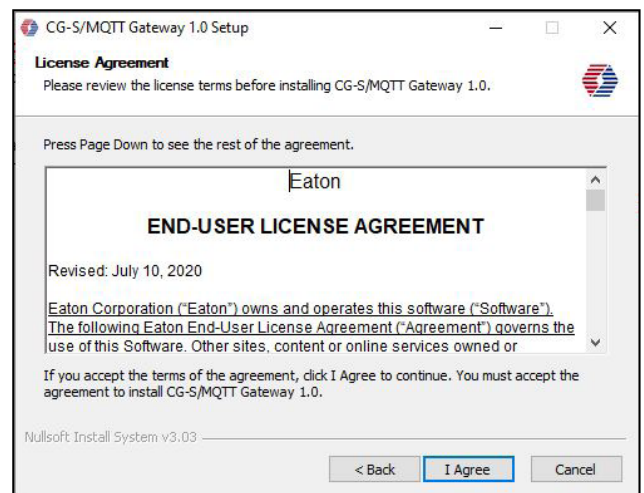


## 2.2 Installation of the CG-S Gateway software

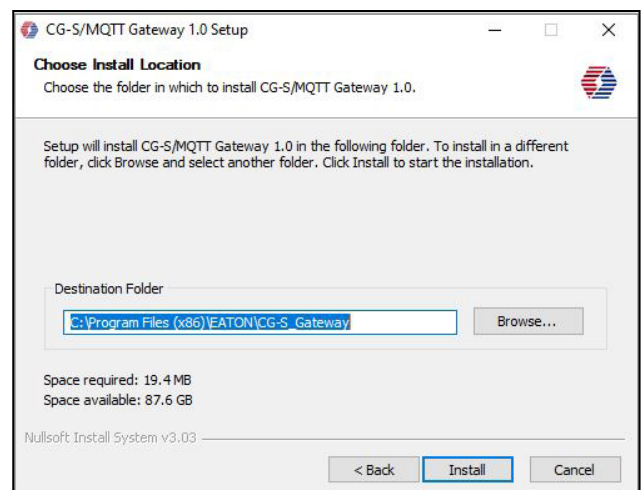
The Setup starts. Continue with "Next"



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

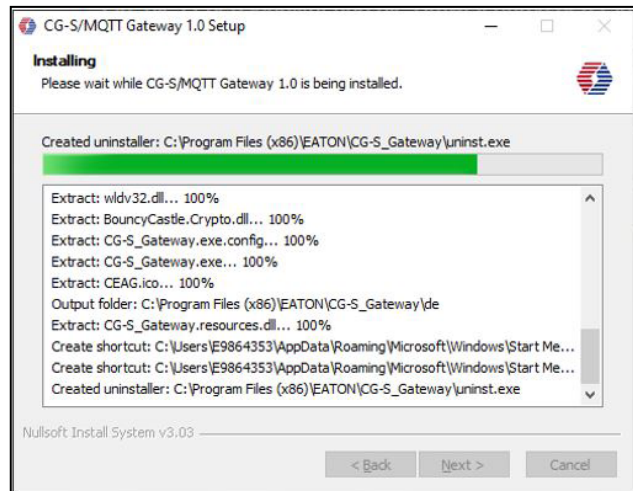


In the next window the destination directory can be selected. It is recommended to keep the settings. Continue with „Install“



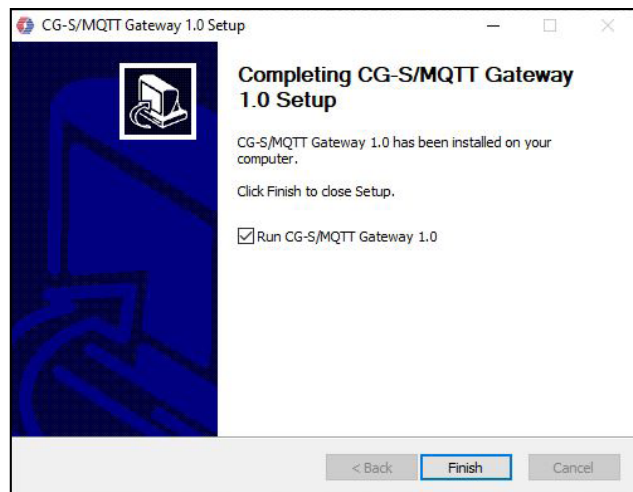
## 2.2 Installation of the CG-S Gateway software

The installation starts with a progress bar



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

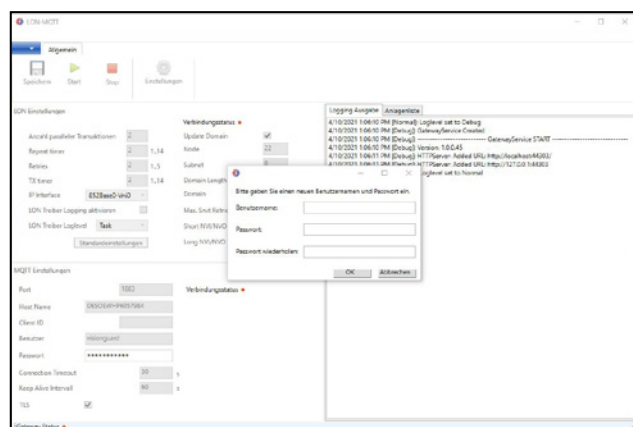
The installation is completed by clicking on „Finish“



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 NOTE

This visualization interface of the CG-S Gateway is only used for configuration. Please configure the gateway according to chapter „8.1 Configuring the CG-S Gateway“. After the configuration, the visualization interface can be closed. The CG-S Gateway starts automatically with Windows as a service in the background.

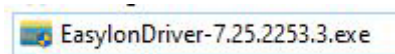




## 2.3 Installation of the CG-S Interface driver package

The CG-S Interface driver package allows a connection

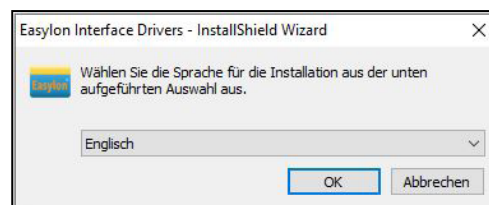
The installation must be started „as Administrator“. Right mouseclick on this .exe file



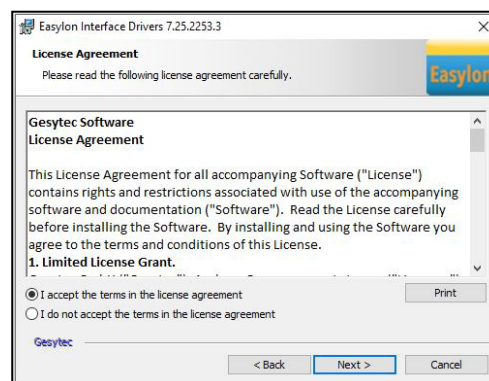
and click on „Run as administrator“.

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

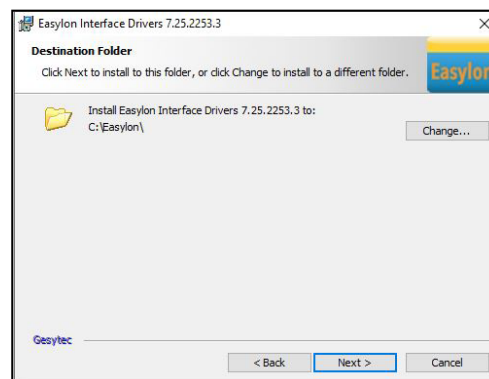
It is possible to choose between German or English. Select the desired language and click OK.



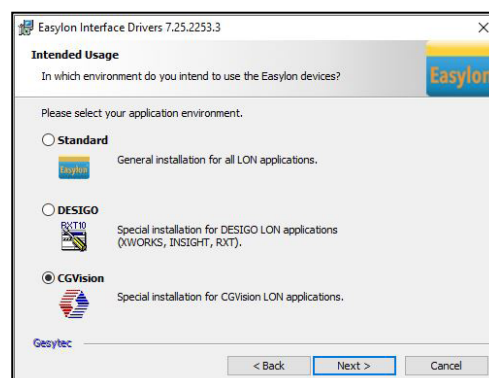
A License Agreement appears. Please read it carefully and confirm with "I accept the terms in the license Agreement", Continue with Next"



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

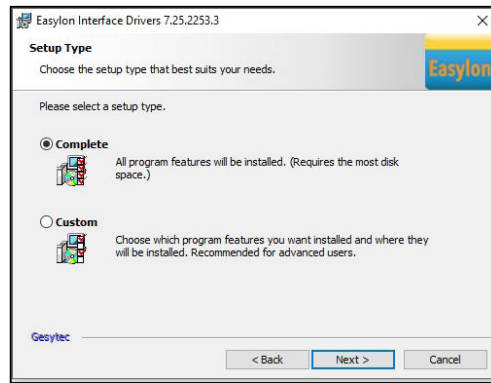


A selection for an application appears. Please select "CGVision" and continue with "Next"

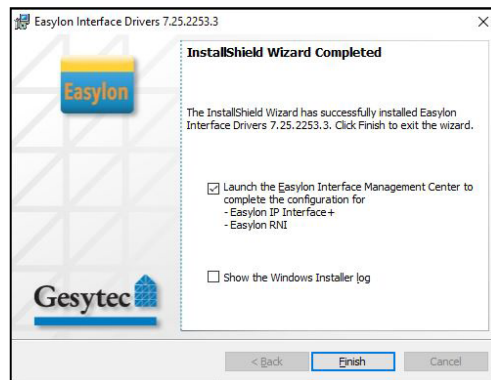


## 2.3 Installation of the CG-S Interface driver package

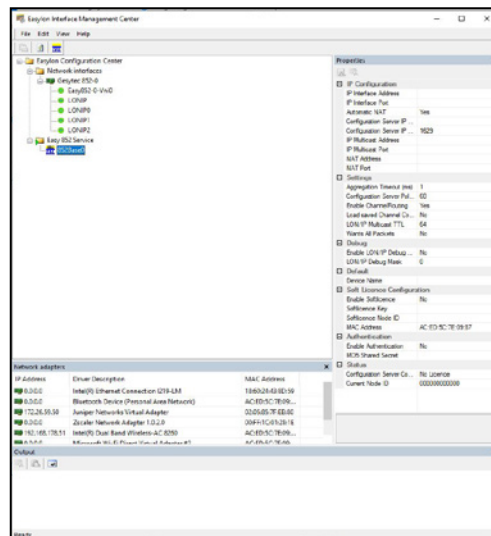
A Setup Type appears. Please select "Complete," and confirm with "Next".  
Please click in the next Window on "Install" to install the installation.  
It takes some minutes.  
A progress bar informs about the installation progress.



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".  
- Under "Configuration Server" the connection will be appears as licenced if the connection to the configuration 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 [www.eaton.com](http://www.eaton.com). 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.

Deinstallation of the previous 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, however, the current VisionGuard version must be stopped before the update installation is executed.

#### 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:

By clicking on "Uninstall," VisionGuard is first uninstalled and then the new installation is started, which takes about 5 minutes.

A progress bar indicates the current update progress. The following window appears at the end of the update.

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

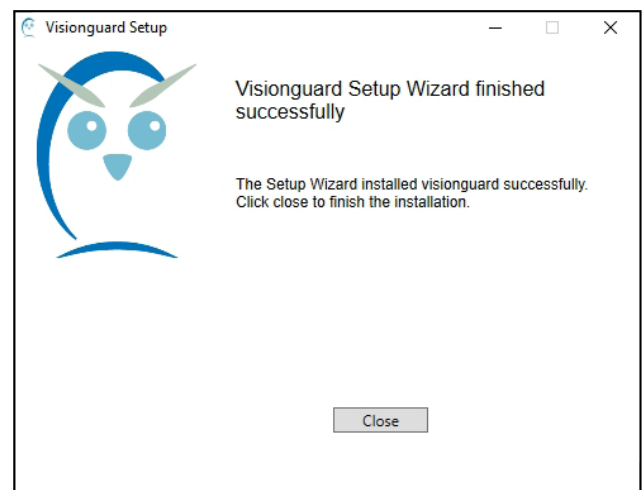
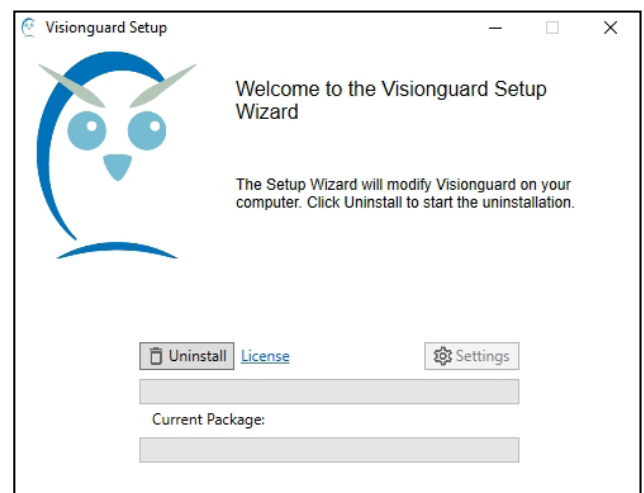
#### 2.4.3 Update of a CG-S Gateway and the CG-S driver package

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!

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 chapter „15 Backup & Restore Menu“.

#### 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 V3.0.1 or older to the current V3.1.0, the ODBC driver must be uninstalled manually via the Windows function „Apps & Features“! After the manual uninstallation, the PC must first be restarted. After the restart, the VisionGuard update can now be carried out. It is strongly recommended to make a backup (programme backup) before updating a V3.0.1. version. See section 15.



## 2.5 Deinstallation of VisionGuard software components

### 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:

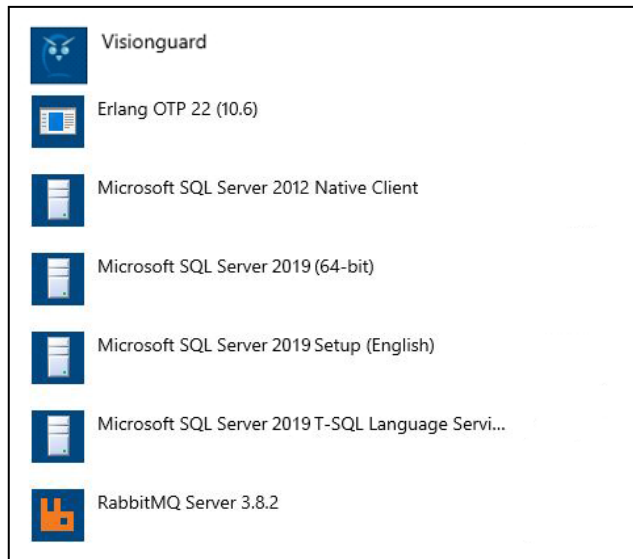
- VisionGuard
- Erlang
- Rabbit MQ
- Microsoft MSSQL 2019

#### IMPORTANT NOTE

Only the VisionGuard instances in Microsoft SQL Server may be uninstalled!

Otherwise, other programs that also use MSSQL may no longer work. To uninstall the CG-S Gateway, please go on „Start“; right mouse click on „LON\_MQTT“ and click deinstall. Same procedure for the CG-S driver package. Please click with right mouse click under the folder „Easyon“ the software „EIMC (CGVision)“ on deinstall.

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



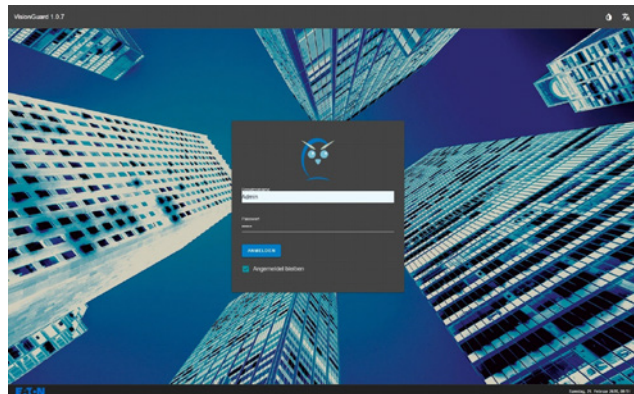
## 3 First launch of VisionGuard

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

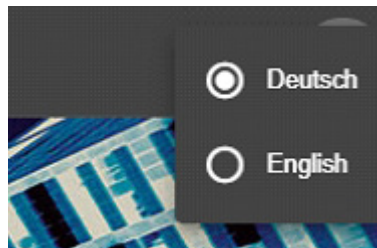
VisionGuard is accessed locally via a standard web browser, e.g. Microsoft Edge, via the URL:

*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:



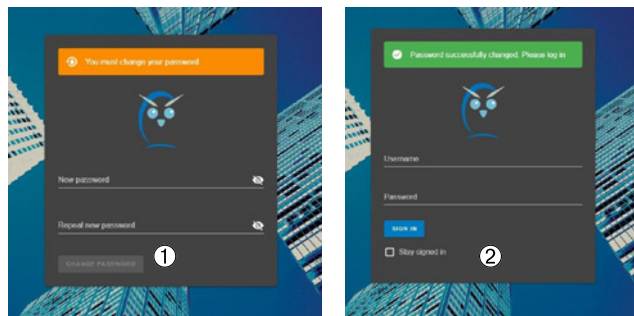
A default user with supervisor rights is preset in VisionGuard.

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



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

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:

#### IMPORTANT NOTE

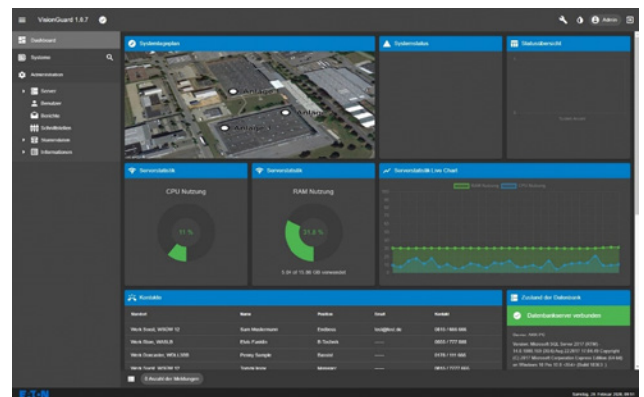
It is strongly recommended that you write down the new password and keep it safe.

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:

#### UAC – Password guidelines

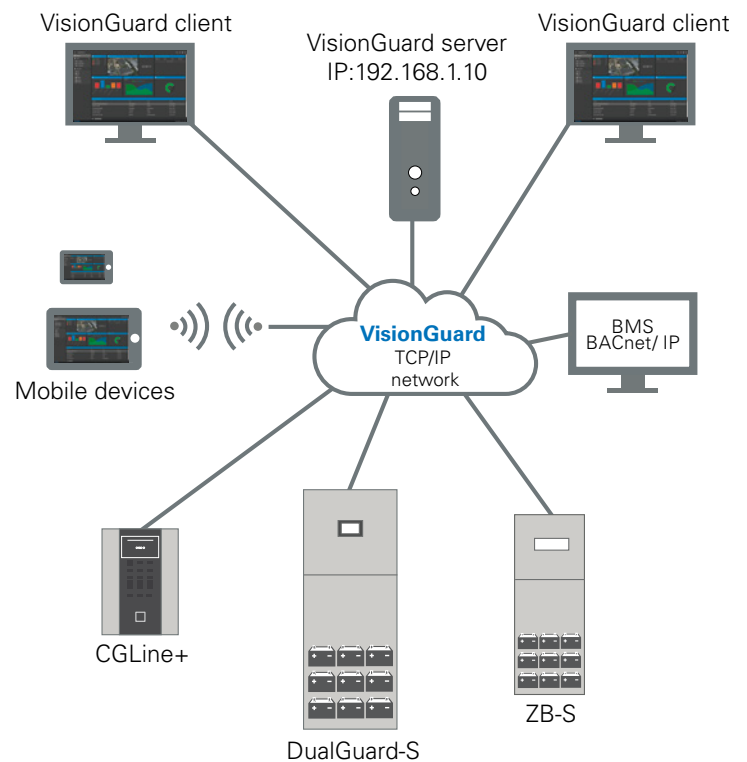
Directive	Value
Number	Yes
Special character	Yes
Small letters	Yes
Capital letters	Yes
Minimum password length	6

After logging in, the dashboard appears as the start screen, which is explained in more detail in Section 8.2:



### 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:



(Note: CGLine+ in preparation)

### 4 License information

#### 4.1 Activating a license

To use VisionGuard, a license must be purchased. Different licenses are available depending on how many DualGuard-S or ZB-S systems are to be connected to VisionGuard. You can find out which licenses are available in section 1.5 VisionGuard licenses. With the purchase of a VisionGuard license, the customer receives a product key in written form or optional on a USB-Stick, which is needed later.

#### IMPORTANT NOTE

Licensing may only be carried out by a user with supervisor rights.  
After logging into the newly installed VisionGuard, the message "not licensed" will appear: ①

In order to be able to complete the licensing step, a fingerprint must be requested in the Administration/Information/Licenses menu.

① "Get new fingerprint"

② 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 license server at

<https://ceagsystems.sentinelcloud.com/ems/customerLogin.html> (see Item 1).

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

xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxx

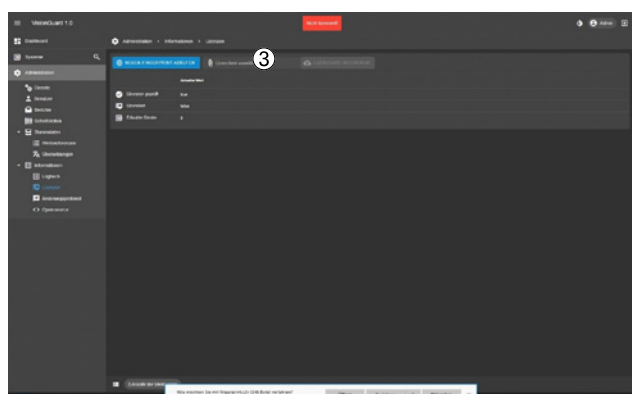
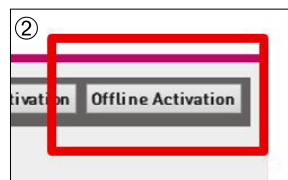
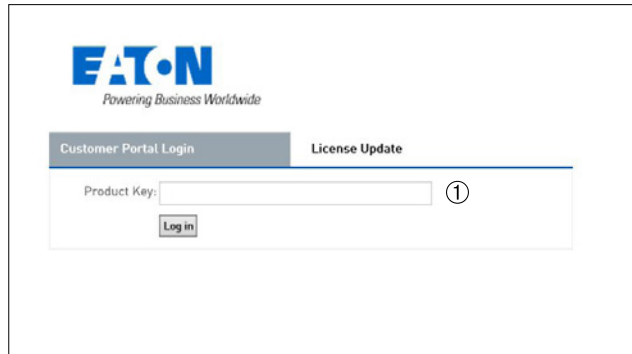
After logging in, enter your name and contact data in the activation register (optional).

Select "Offline Activation" in the upper right-hand corner. (Item 2)

Now upload the fingerprint created in VisionGuard in the "Upload C2V" field by searching for and selecting the source, e.g. USB stick via "...". (Item 3)

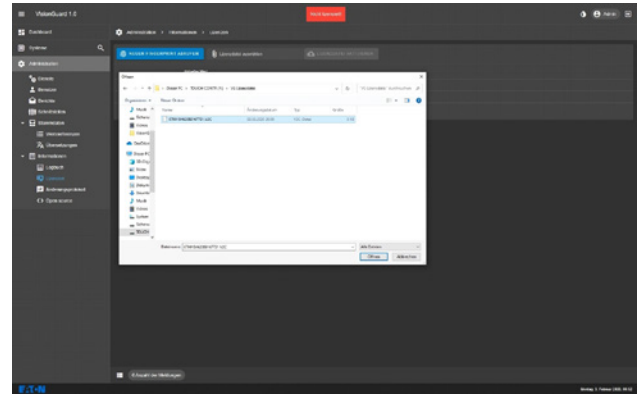
Click "Generate" for the license server to generate an activation key, which can be downloaded to the local data medium, e.g. C:\temp or an USB stick.

③ The activation key can be uploaded into VisionGuard by via "Select license file"

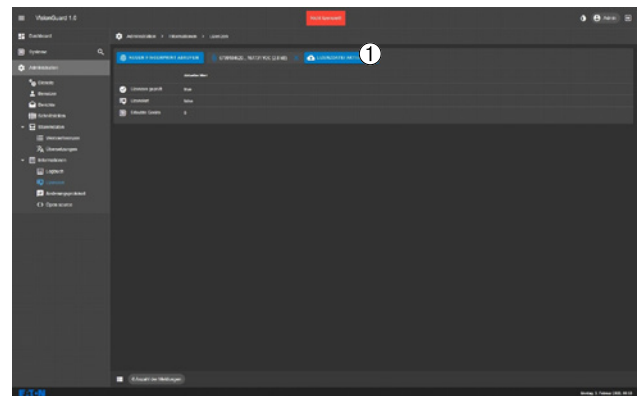




You can now specify the location of the activation key in the dialog box

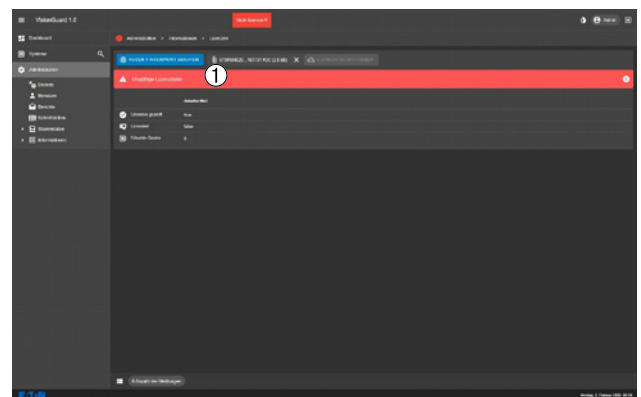


- ① The purchased license can be activated in VisionGuard by clicking "Activate license file"

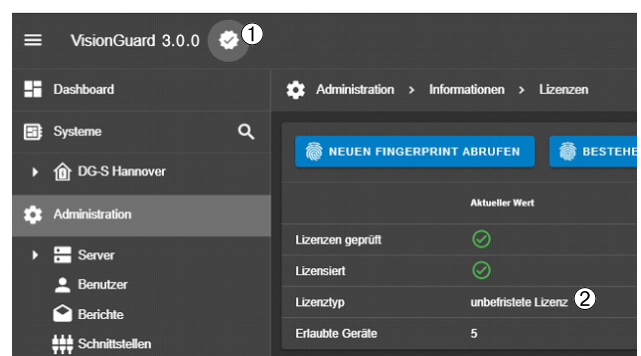


- ① The message "Invalid license file" then appears

The keyboard combination "Ctrl + 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 license type and volume license purchased are displayed here, which indicates how many emergency lighting systems can be connected to VisionGuard



### 5 Security certificate installation

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:

A distinction must be made here whether it is being accessed from a client PC on the network or locally on the same PC.

#### 5.1 Installing the security certificate via local access

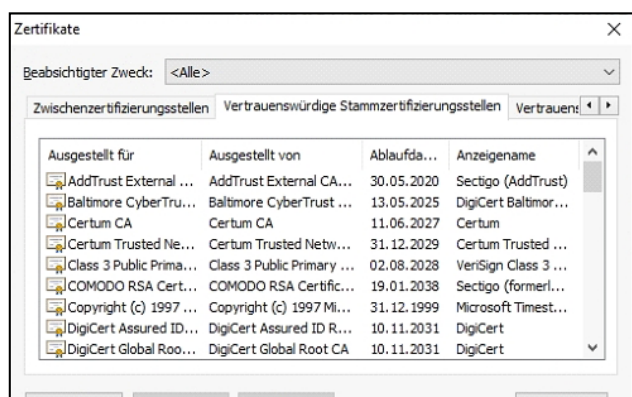
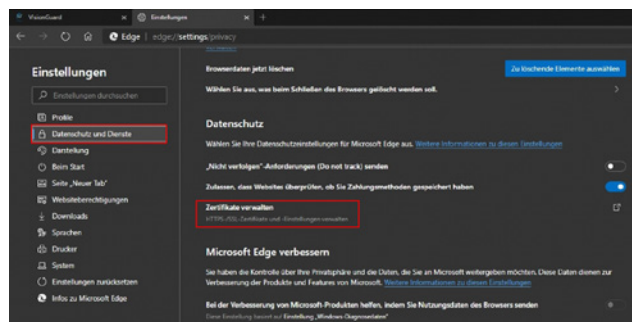
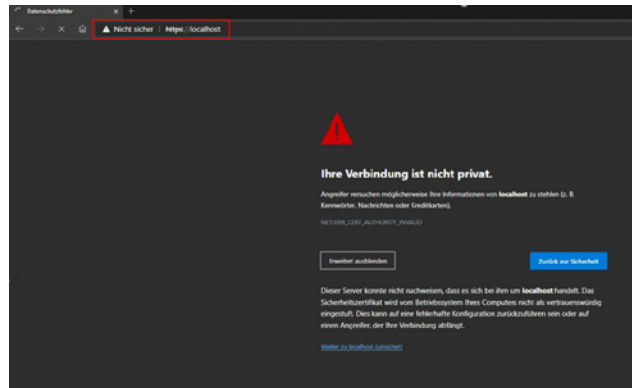
If accessing a locally installed version of VisionGuard from a browser, proceed as follows. The following instructions are based on Chrome. The procedure is similar for other browsers.

#### NOTE

For all internal HTTPS ports, a certificate with an automatically generated password is generated for installation. The certificate can be found under C:\Program Files\EATON\Visionguard\certs. cert\_api.crt

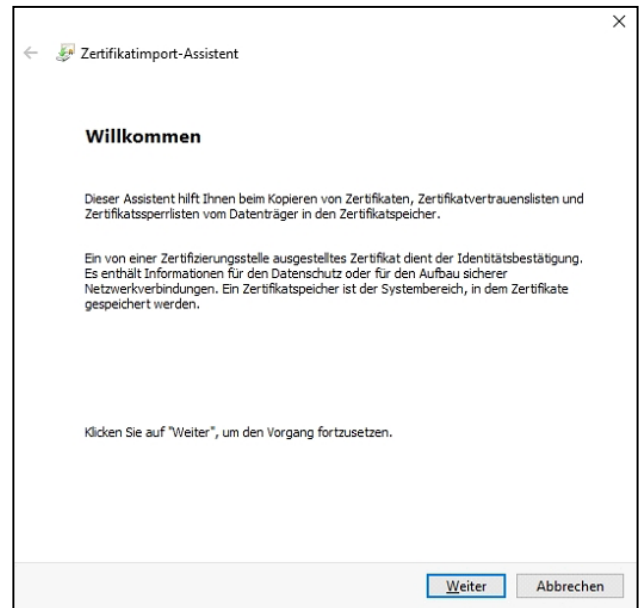
A certificate generated by Eaton is provided for external communication via the web server. This certificate can also be found under C:\Program Files\EATON\Visionguard\certs cert\_proxy.crt cert\_proxy.pem  
In the browser, go to Settings > Privacy and services > Manage certificates

"Manage certificates" opens the certificate management window, where you can import certificates

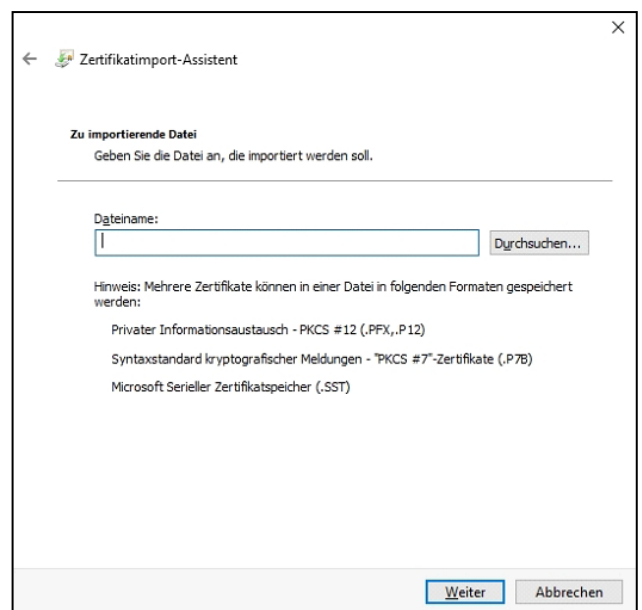




Click "Import" to start the certificate import wizard



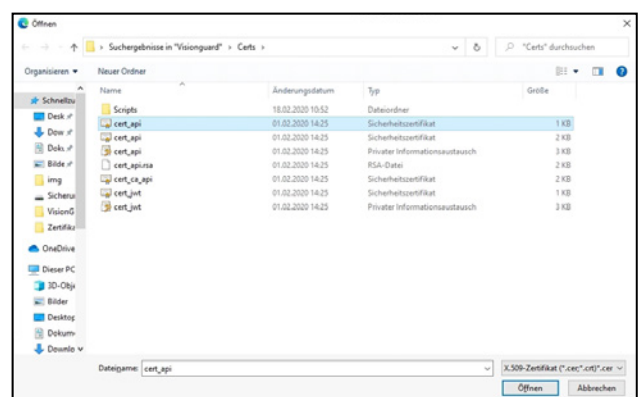
Click "Next" to search for the certificate in the next dialog box



Click "Browse" to select the certificate. For internal https Ports it is located in the folder  
*C:\ProgramFiles\EATON\Visionguard\certs*  
 The certificate is called  
 - cert\_api.crt

For external communication via the Web server the certificates are located in the folder  
*C:\ProgramFiles\EATON\Visionguard\certs*  
 The certificates are called  
 - cert\_proxy.crt  
 - cert\_proxy.pem

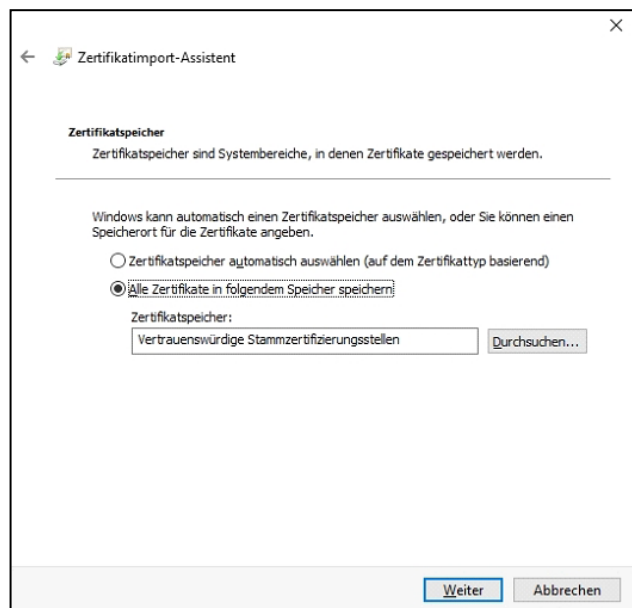
Once the certificate is selected, click "Open" to continue



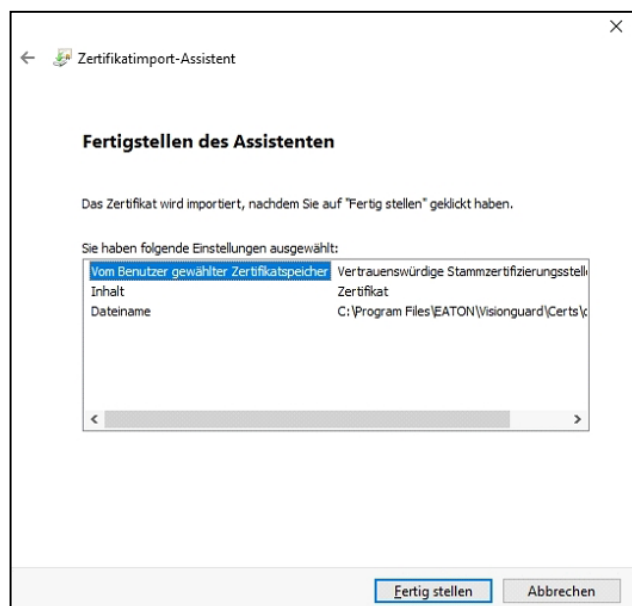
## 5 Security certificate installation

The certificate must be stored in the Trusted Root Certification Authorities store

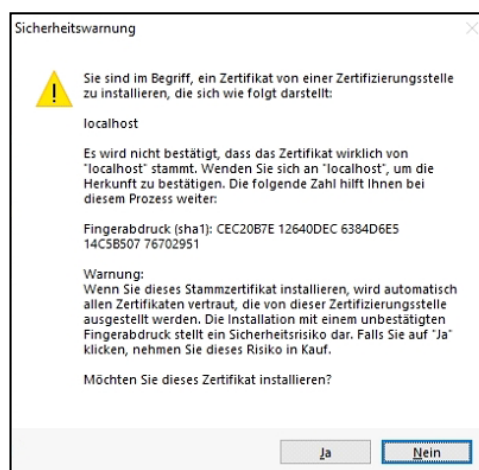
Continue with "Next"



Click "Finish" to exit



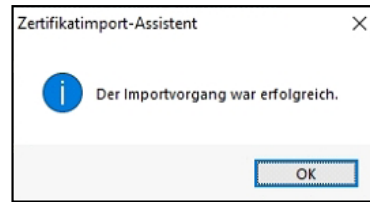
The certificate can now be installed in the security warning by clicking "Yes."



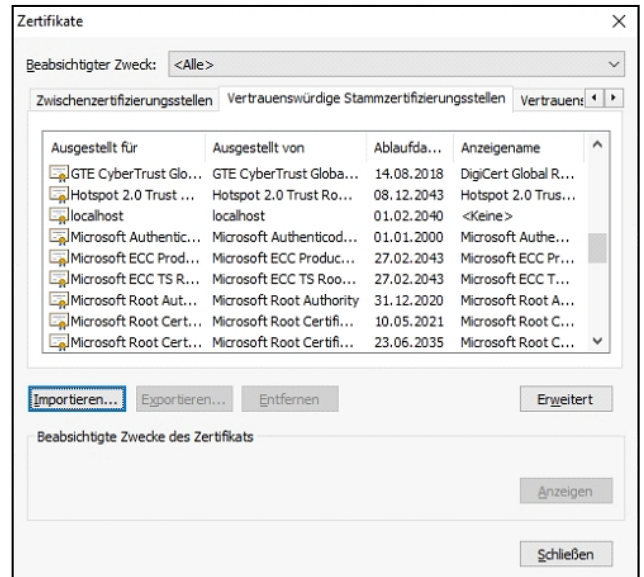
## 5.2 Installation of the security certificate via remote access

The following message should appear

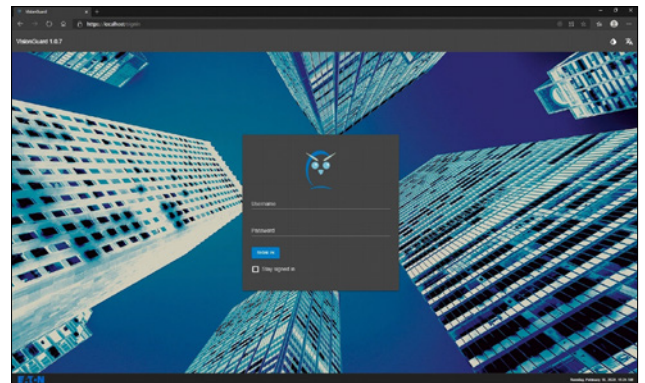
„The import process was successful“



The import process can be checked under certificate management. There, the certificate "localhost" with the expiration date 2099 should appear under "Trusted Root Certification Authorities"



Accessing VisionGuard should now be possible without the error message "Certificate error"



## 5.2 Installation of the security certificate via remote access

If the VisionGuard server is accessed from a remote web client in the network, the certificate must be downloaded from the VisionGuard folder to a data medium, e.g. a USB stick, as described above. Perform the installation on the client PC from which the VisionGuard is to be accessed in the same way as described in 5.1, only with the USB stick as the source for the certificate.

6 Creating new users with user roles

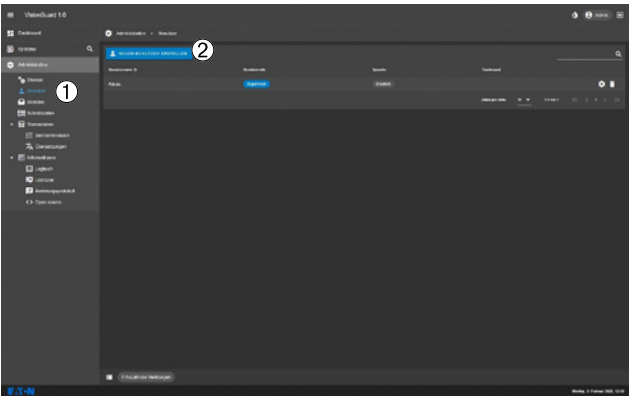
6.1 User Account Control (UAC) information

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

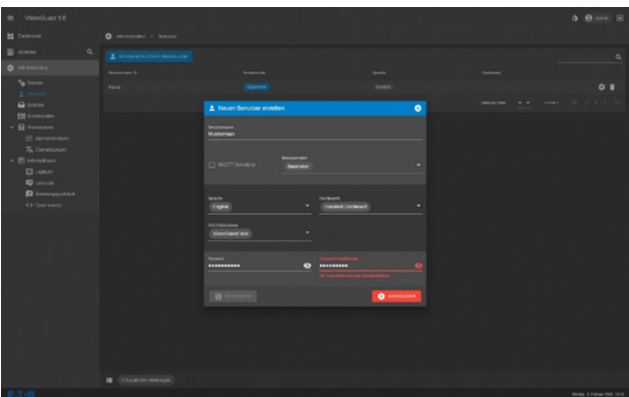
Role	Administrate UAC / Translations	Administrate VisionGuard Basics	DG-S configuration	DG-S / ZB-S control	DG-S / ZB-S status
Supervisor	X	X	X	X	X
Administrator		X	X	X	X
Power User				X	X
User					X

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

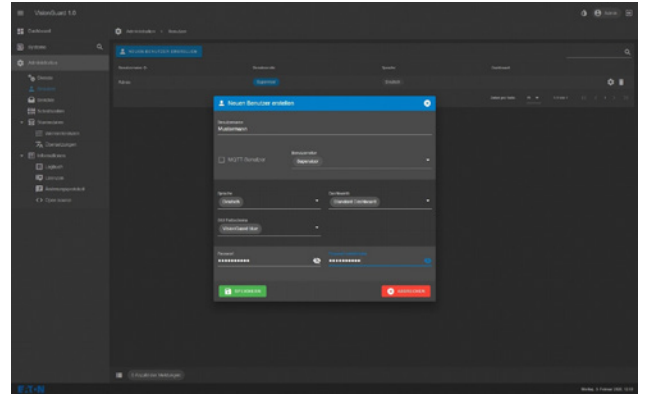


- ① Under User name, define the name of the new user. This is the name that is entered in the VisionGuard login screen when logging in.
- ② A role with different access permissions can be defined under User role (see table above)
- ③ Select the user language under Language. You can choose between German and English (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.



## 6 Creating new users with user roles

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



## 7 Adding DualGuard-S systems to VisionGuard

### 7 Adding DualGuard-S systems to VisionGuard

#### 7.1 Configuring the HMI to connect to VisionGuard

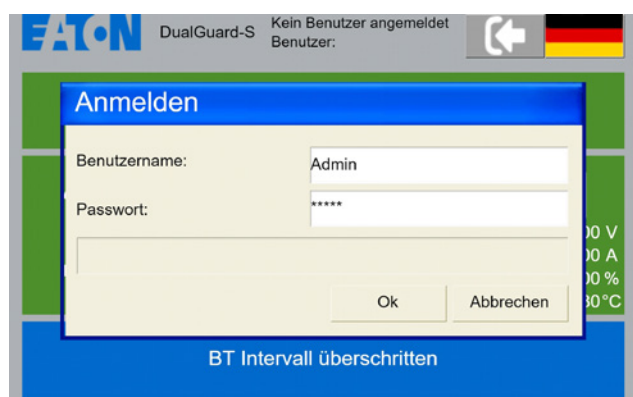
In order to add a Dualguard-S system on VisionGuard, connection settings must be made on the HMI.

Note: To be able to make the connection settings to VisionGuard in the HMI menu, you must be logged on as an "Expert."

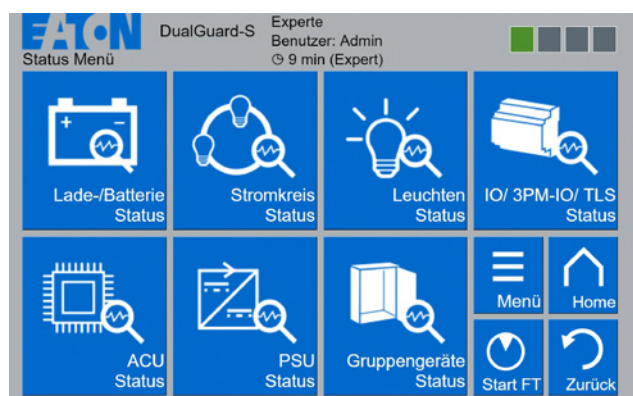
The connection settings can be made directly on the HMI or ideally via web access.

Log on to the HMI:

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



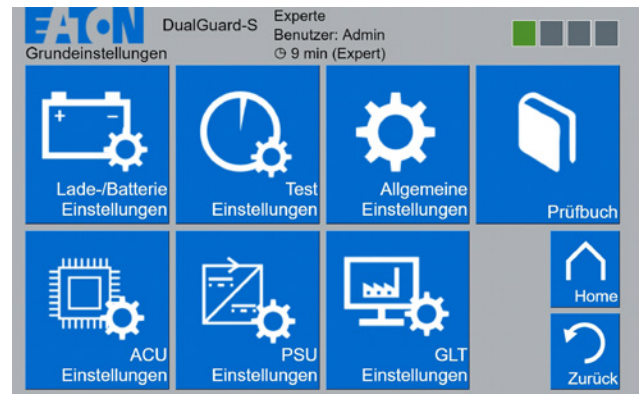
Click "Menu" to proceed



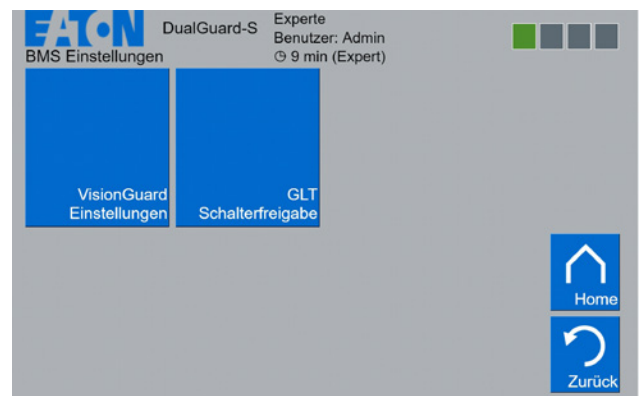
Then click "Basic settings"



Then click "BMS Settings"

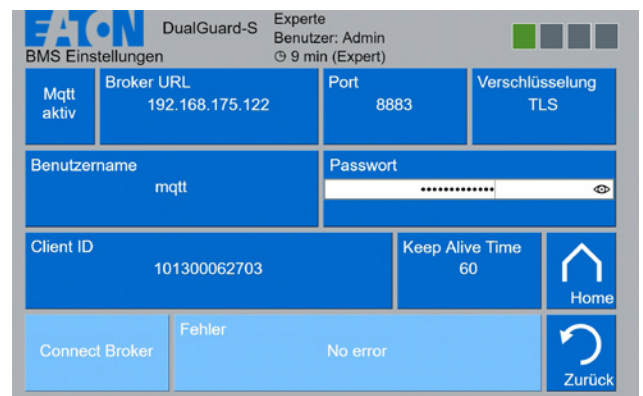


Then click "VisionGuard settings"



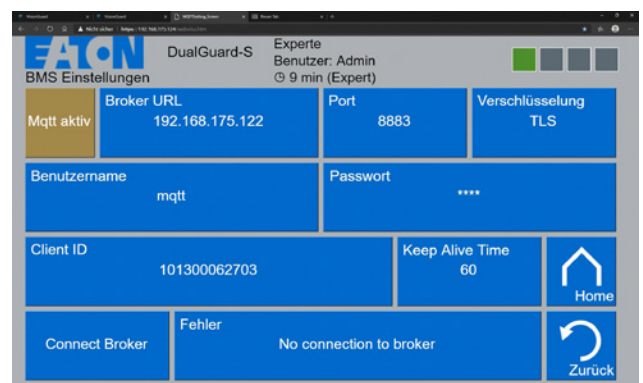
The following entries must be made in the "VisionGuard settings" menu:

- "Mqtt aktiv" must be inactive (blue display)
- The IP address of the VisionGuard 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 (see Figure 2 in 7.2)
- "Password" must be identical to the MQTT user password in VisionGuard (see Figure 3 in 7.2)



The MQTT interface can be activated after making the above settings. Click on „Connect Broker“. 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.



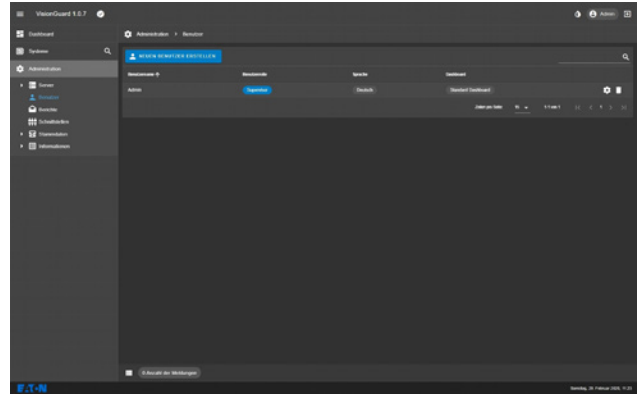


## 7.2 Adding and authorizing a DualGuard-S system in VisionGuard

### 7.2 Adding and authorizing a DualGuard-S system in VisionGuard

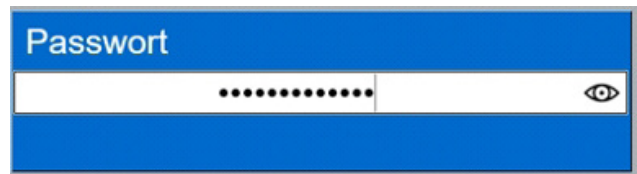
In order for DualGuard-S systems to be added in VisionGuard, an MQTT user must be created in VisionGuard.

- ① This is done in the Administration/User menu
- ② Create a new MQTT user by clicking "Create new user"

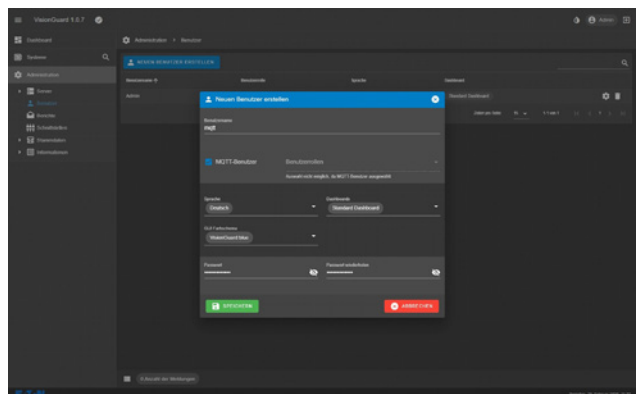


The following settings must be made in the next dialog box:

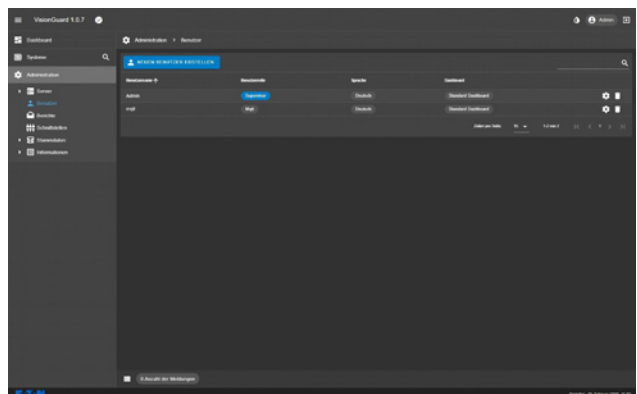
- ① The user name must be identical to the user name in the HMI. "Mqtt" is recommended for simplicity
- ② MQTT user must be checked
- ③ Choose the settings as desired
- ④ The password must be identical to the password in the HMI



- ⑤ Click "Save" to apply the settings



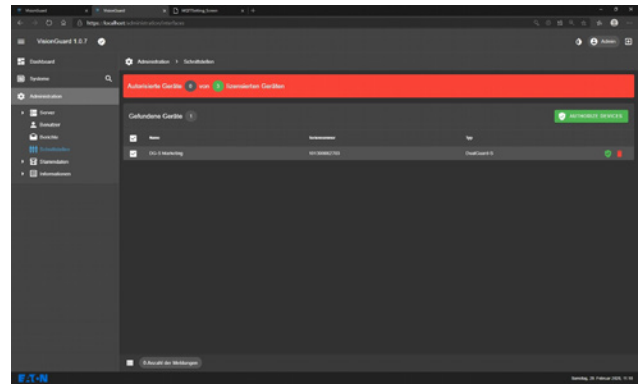
The user for the connection (here with the name mqtt) has now been created



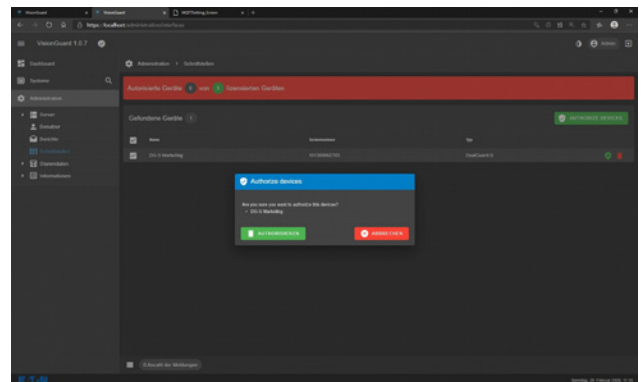


## 7.2 Adding and authorizing a DualGuard-S system in VisionGuard

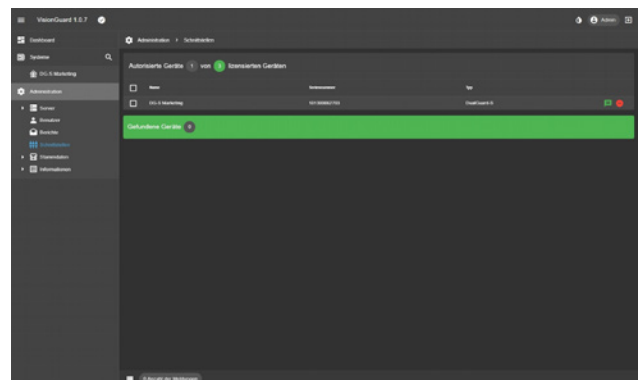
- ① If the settings in the HMI of the DualGuard-S match the settings of the mqtt user in VisionGuard, DualGuard is displayed in the Administration/Interfaces menu
- ② Click "Authorize device" to add the DualGuard-S to VisionGuard



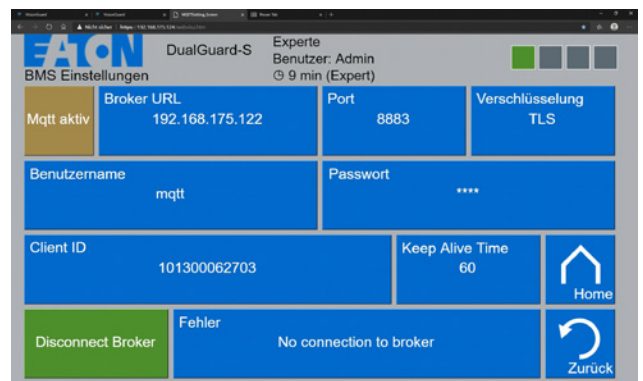
Confirm by clicking "Authorize"



The DualGuard-S has now been successfully registered in VisionGuard



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

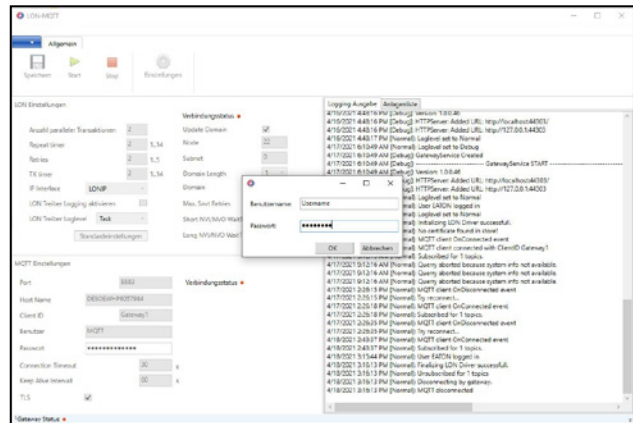
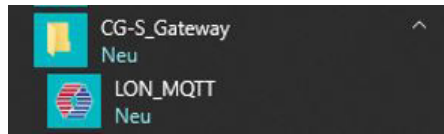


## 8 Adding ZB-S systems to VisionGuard

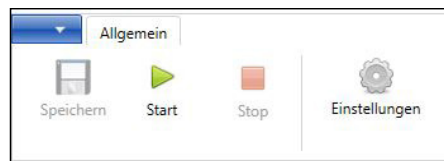
### 8.1 Configuring the CG-S Gateway

Start or open the CG-S Gateway software  
“LON MQTT” (perhaps it is needed to start as Administrator)

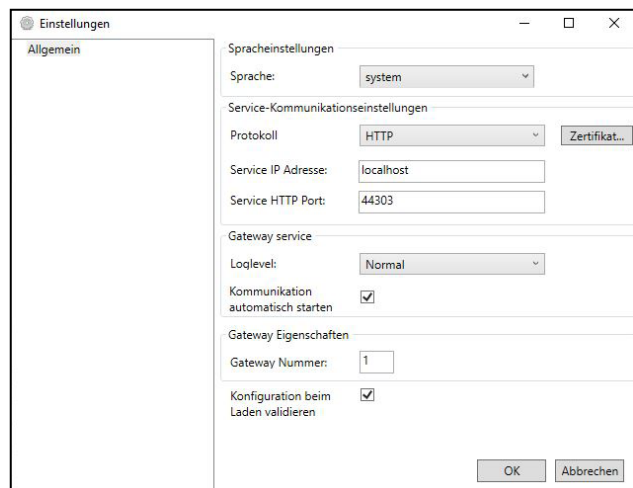
Please enter the user and password you assigned in chapter 2.2.



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



## 8.2 Adding and authorizing a ZB-S system in VisionGuard

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

For the CG-S/UIP-Interface the right setting is:

**LONIP**

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

**LONUSB**

---

### NOTE

---

Other settings not required. Please leave the default settings!

LON Einstellungen

Anzahl paralleler Transaktionen: 2

Repeat timer: 2 1.14

Retries: 2 1.5

TX timer: 2 1.14

IP Interface: LONIP

LON Treiber Logging aktivieren: ☐

LON Treiber LogLevel: Task

Verbindungsstatus: ●

Update Domain: ☒

Node: 22

Subnet: 0

Domain Length: 1

Domain: 1

Max. Snvt Retries: 4 1.20

Short NVI/NVO WaitTime: 100 50.10000

Long NVI/NVO WaitTime: 1000 400..20000

Standardeinstellungen

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 7.2)

Password/Passwort: Must be exactly the same password of the MQTT user of the VisionGuard (see section 7.2)

Connection Timeout: 30S

Keep aLive Intervall: 60s

TLS: Must be activated

MQTT Einstellungen

Port: 8883

Host Name: DESOEWHIP6057984

Client ID: LONMQTT

Benutzer: MQTT

Passwort: .....

Connection Timeout: 30 s

Keep Alive Intervall: 60 s

TLS: ☒

Verbindungsstatus: ●

Gateway Status: ●

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)

Allgemein

Speichern Start Stop Einstellungen

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

Verbindungsstatus: ●

## 8.2 Adding and authorizing a ZB-S system in VisionGuard

---

### PLEASE NOTE:

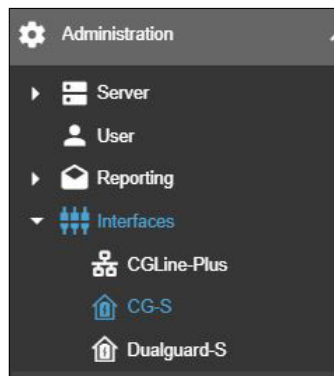
---

To add a ZB-S in the VisionGuard you must be logged in at least as Admin or Supervisor!

Preparation: To add a ZB-S system the Neuron ID and the device no. (1-32) from the ZB-S control unit CU-CG-S must be investigated. Please see the manual of the ZB-S.

## 8.2.1 Create new Groups and adding and authorizing ZB-S systems in VisionGuard

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



### 8.2.1 Create new Groups and adding and authorizing ZB-S systems in VisionGuard

Please note:

Any number of CG-S groups can be created, each with up to 32 ZB-S systems. This serves only a logical group assignment, which has no meaning in the later visualization representation in the VisionGuard.

To create a CG-S group please click on the blue button "NEW CG-S GROUP"



In the following window please enter:

Gateway ID:	1
Group ID:	Desired ID from 1 to 500
Types:	ZB-S
Name:	Desired group name with max. 100 characters

**Configure CG-S system**

Gateway ID	Group ID
1	1
Types	Name
zbs	Groupname max. 100 charac

**SAVE** **CANCEL**

## 8.2.1 Create new Groups and adding and authorizing ZB-S systems in VisionGuard

### IMPORTANT NOTE

Under types there are other CG-S Systems selectable. These are not supported in this VisionGuard Version 3!  
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 ZB-S systems to the created CG-S groups please proceed as follows.  
Click in this picture on the blue button  
"NEW CG-S SYSTEM"

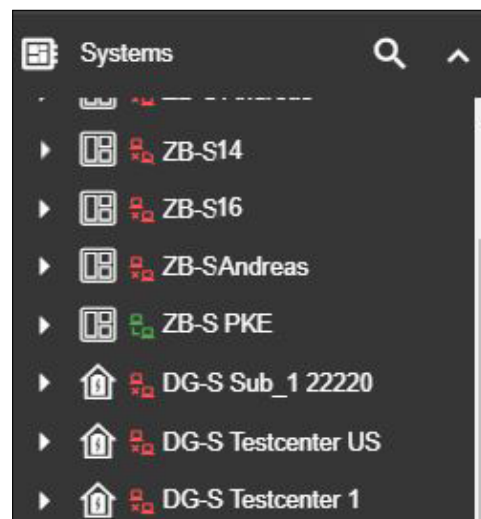
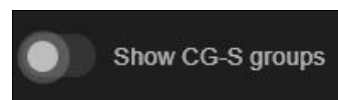
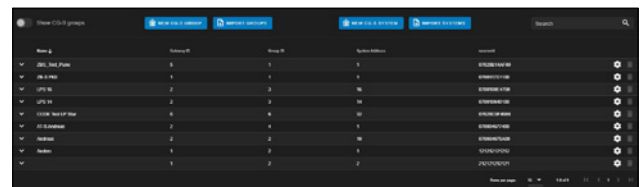
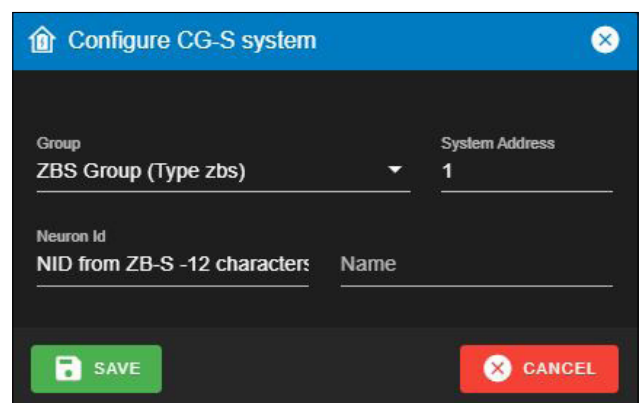
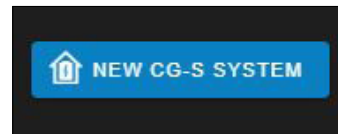
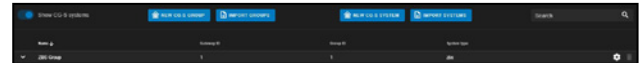
In the following window please enter:

Group: Select here one desired created CG-S group  
System Address: System Address from the ZB-S 1 to 32  
Neuron Id: Enter here the Neuron ID from the ZB-S control unit CU-CG-S with exact 12 characters  
Name: Will automatically filled in after authorization of the ZB-S in the VisionGuard

Click "Save" to add the ZB-S system in the VisionGuard  
Please proceed in the same way with all other ZB-S systems that you would like to integrate into the VisionGuard.  
All ZB-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 ZB-S systems are now visible and operable in the „Systems“ menu tree



## 9 Basic graphic layout and structure of VisionGuard

VisionGuard now automatically loads the complete DualGuard-S configuration

### IMPORTANT NOTE

Depending on the size of the system, it may take several minutes to load the configuration. Please let the configuration load fully before making any further settings changes in VisionGuard.

## 9 Basic graphic layout and structure of VisionGuard

### 9.1 Login screen

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

- ① Display of the current VisionGuard version (here e.g. V3.0.0)
- ② Light/dark mode setting
- ③ Login language setting German/English
- 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.

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 for the background image is: C:\Program Files\EATON\Visionguard\Proxy\html\img\app-signin-background.jpg

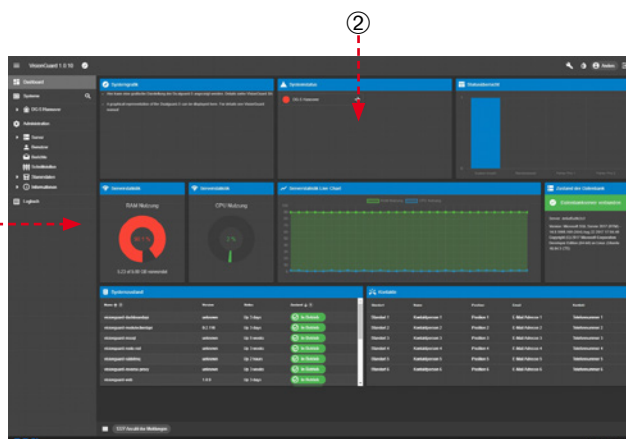
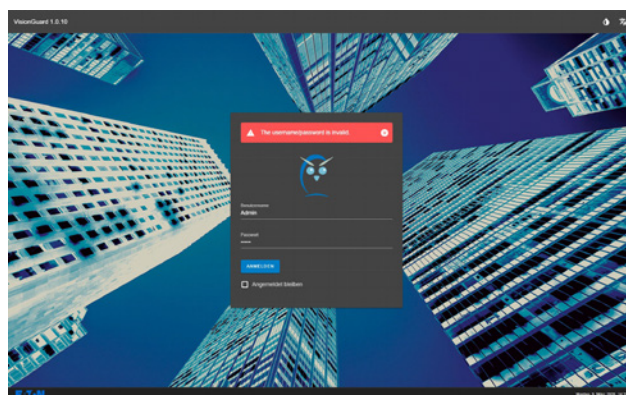
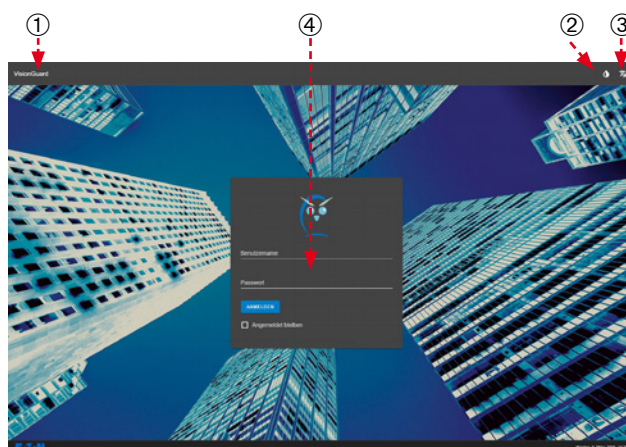
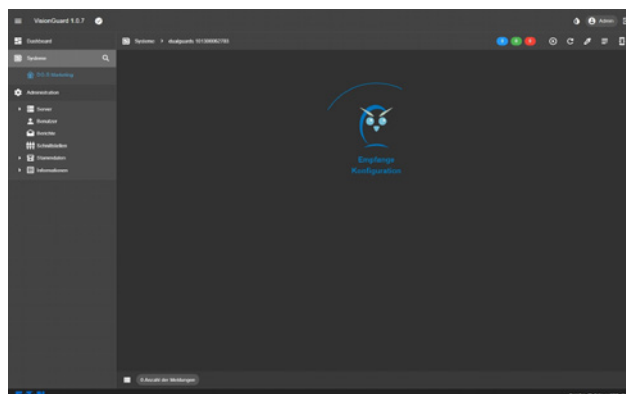
It can be replaced by a new .jpg with a size of 1920x1080 pixel.

It is recommended to rename the original image first.

### 9.2 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 eight defined widgets

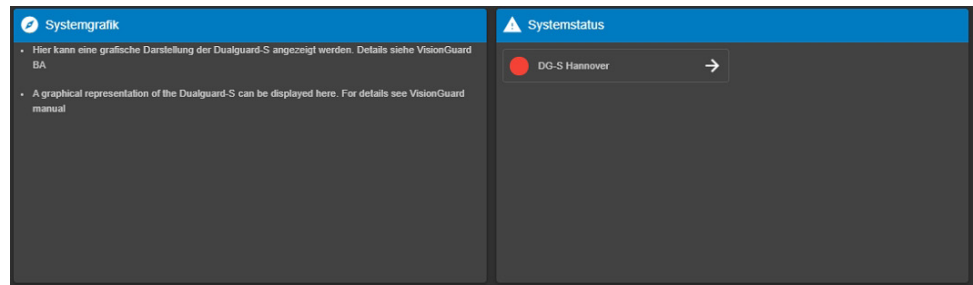




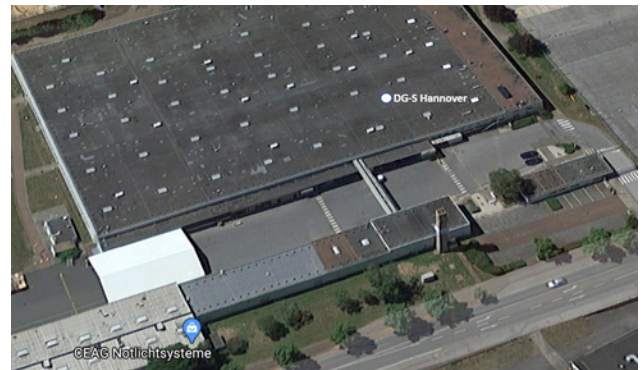
## 9.2.1 System graphic and system status

The system status widget clearly displays all connected and logged-on DualGuard-S systems in a single widget. For each DualGuard, the system name is displayed with a communication-color-coded status (green = Communication OK, red = Communication failure). The arrow to the right of the system name is used to navigate directly to the system overview.

In the system graphic widget, you can conveniently display the systems in an image, e.g. to indicate the location

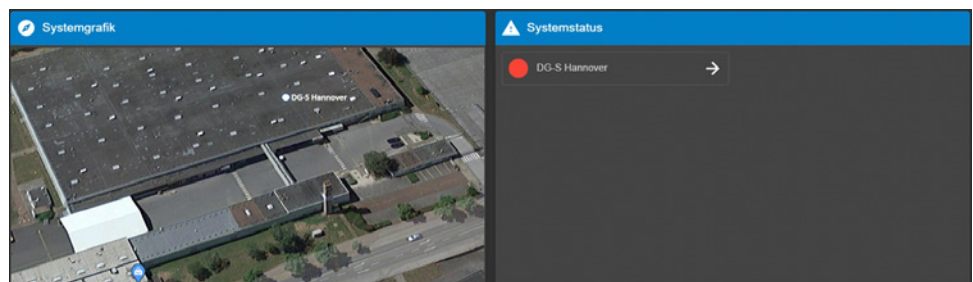


Example of a simple system graphic from Google Maps: You create a screenshot with the system location and add a text using a graphic tool, e.g. Paint:



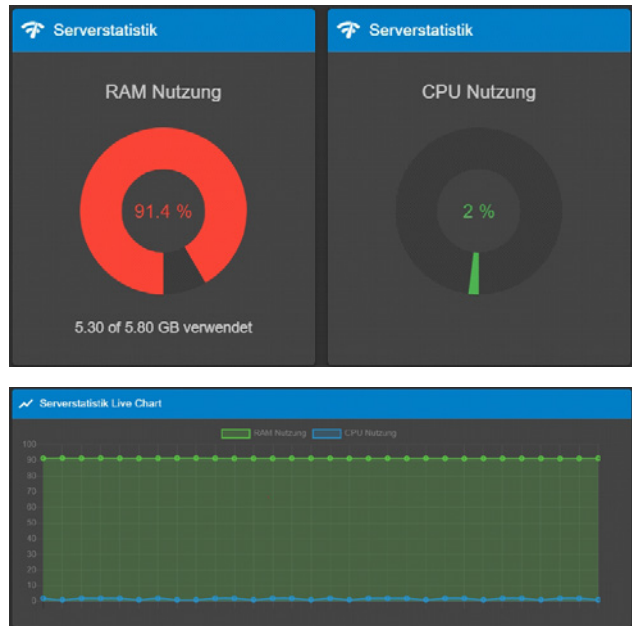
This image can now be copied as a .jpg with the name "widget-image-jpg-01.jpg" in the folder *C:\Program Files\EATON\Visionguard\Proxy\html\img\widgets*.

Ctrl + F5 refreshes the page and displays the system graphic in the widget:



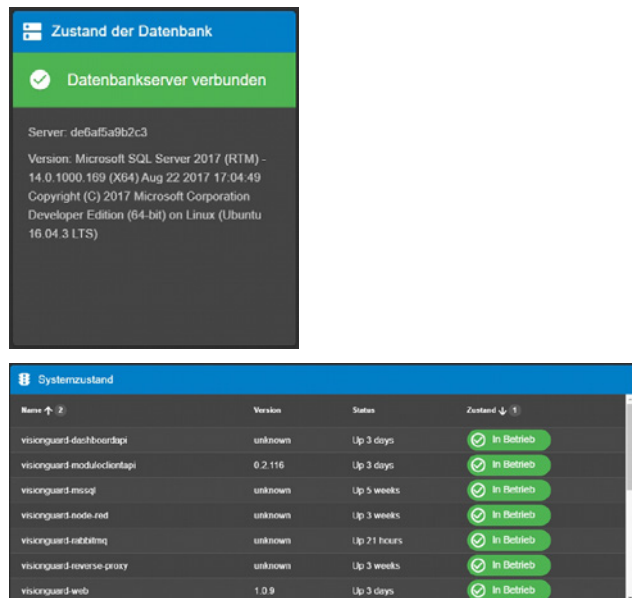
### 9.2.2 Server statistics

The server statistics 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.




### 9.2.3 Database and system services status indicators

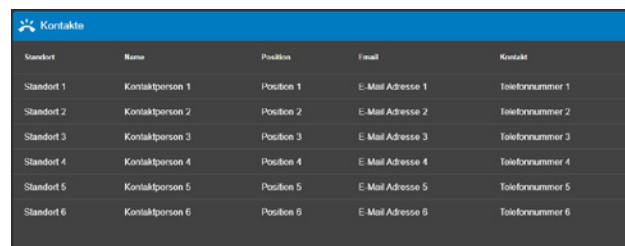
The database and system status widgets provide information about the functionality of VisionGuard. If the database server is working correctly, all data is exchanged correctly between the systems and VisionGuard. The system status widget can be used to check that all VisionGuard services are functioning 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 17.1).





## 9.2.4 Contacts

In the Contacts widget, contacts can be created with their contact details, e.g. to be informed about special events. The editing function can be activated by clicking on the wrench icon  in the upper right-hand corner to create or change contact data.

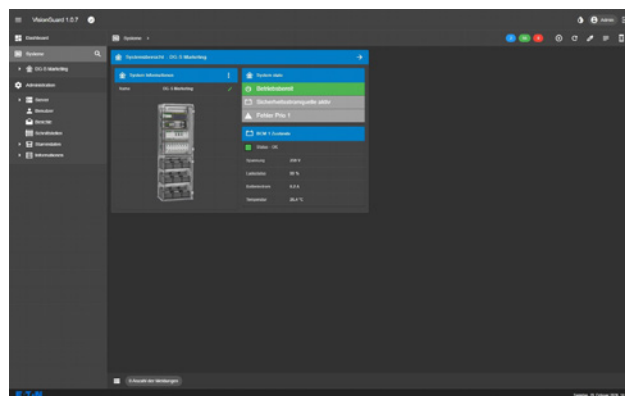


Standort	Name	Position	E-Mail	Kontakt
Standort 1	Kontaktperson 1	Position 1	E-Mail Adresse 1	Telefonnummer 1
Standort 2	Kontaktperson 2	Position 2	E-Mail Adresse 2	Telefonnummer 2
Standort 3	Kontaktperson 3	Position 3	E-Mail Adresse 3	Telefonnummer 3
Standort 4	Kontaktperson 4	Position 4	E-Mail Adresse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


## 9.3 System overview

The "Systems" menu displays a system overview with widgets of all installed DualGuard-S systems. The widgets show information such as the device name, battery values and the status of the DualGuard-S or ZB-S systems as they are displayed on the ACU directly on the device via LEDs, such as whether the device is pre-operational, whether the safety power source is active (battery operation) and whether there is a priority-1 sum failure (sum failure with light fault).

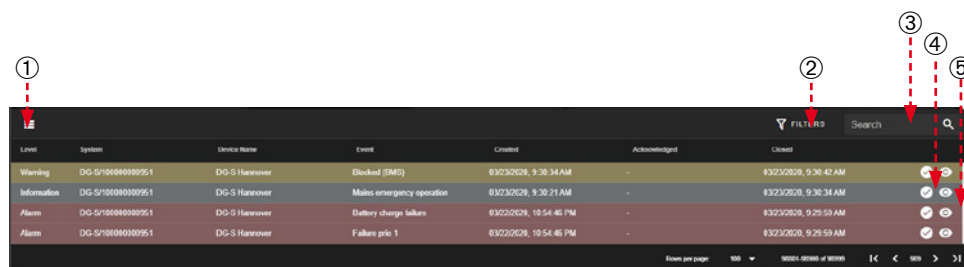
- ① The arrow takes you to the detailed view of the DualGuard (see separate Section)



## 9.4 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
- ② Filter 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" slide switch
- ⑤ The eye icon allows you to navigate directly to the event where it occurred

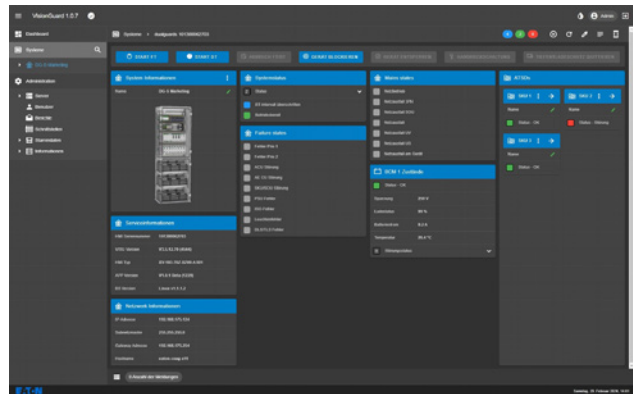


Level	System	Device Name	Event	Created	Acknowledged	Ended	
Warning	DG-S/10000000951	DG-S Hannover	Blocked (BMS)	8/23/2020, 9:30:34 AM	-	8/23/2020, 9:30:42 AM	⑤
Information	DG-S/10000000951	DG-S Hannover	Main emergency operation	8/23/2020, 9:30:21 AM	-	8/23/2020, 9:30:34 AM	⑤
Alarm	DG-S/10000000951	DG-S Hannover	Battery charge failure	8/23/2020, 10:54:46 PM	-	8/23/2020, 9:25:59 AM	⑤
Alarm	DG-S/10000000951	DG-S Hannover	Failure prio 1	8/23/2020, 10:54:46 PM	-	8/23/2020, 9:25:59 AM	⑤

## 10 DualGuard-S visualization

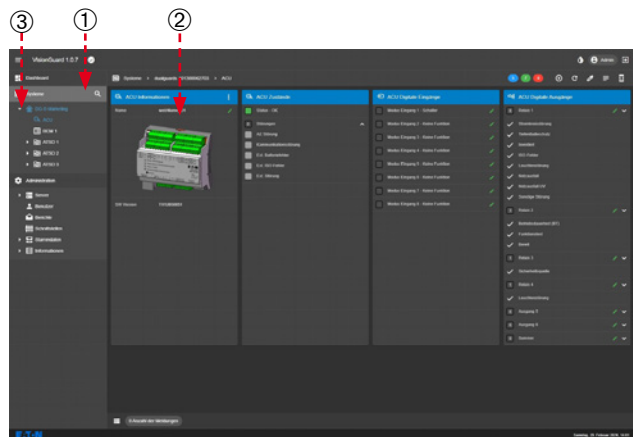
### 10.1 DualGuard-S detail view

Under the "Systems" menu, all Dualguard-S or ZB-S systems are listed with their device names in the explorer structure ①. Click on the name to see the detailed view of the DualGuard-S. 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. 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.



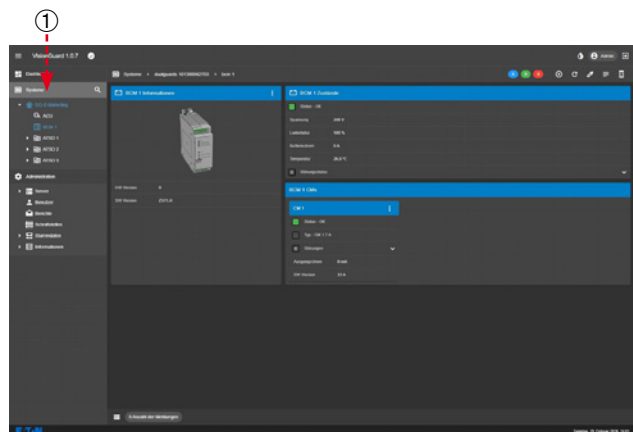
### 10.2 ACU detail view

- ① the ACU detail view shows the ACU status, the digital input configurations and relays. It is not possible to configure the digital inputs and relays in VisionGuard. These configurations must be carried out via the HMI.



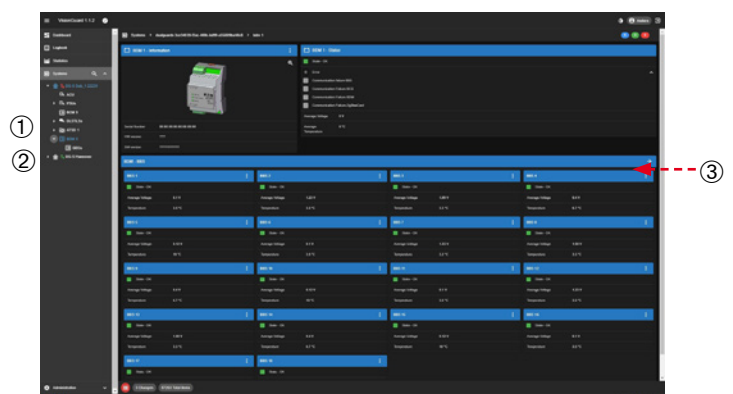
### 10.3 BCM detail view

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.



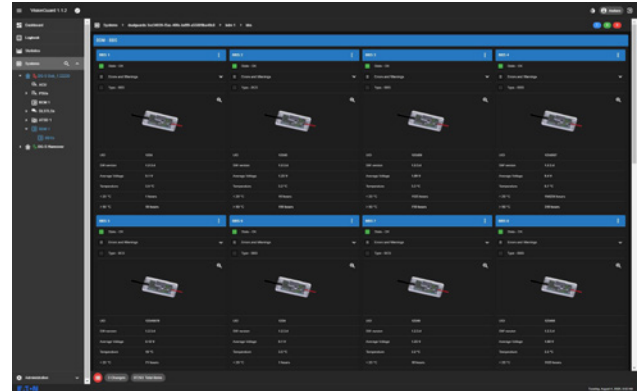
### 10.4 BDM detail view

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 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.



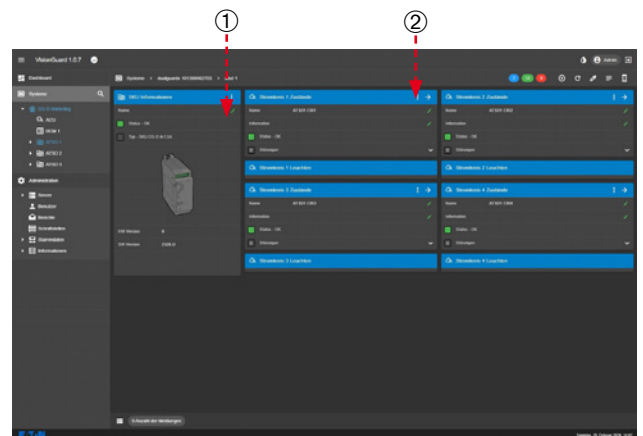
## 10.4.1 BBS detail view

With click on BBS in the system tree ② or the arrow ③, the BBS overview widget opens with the detail BBS status information



## 10.5 ATSD detail view (SKU)

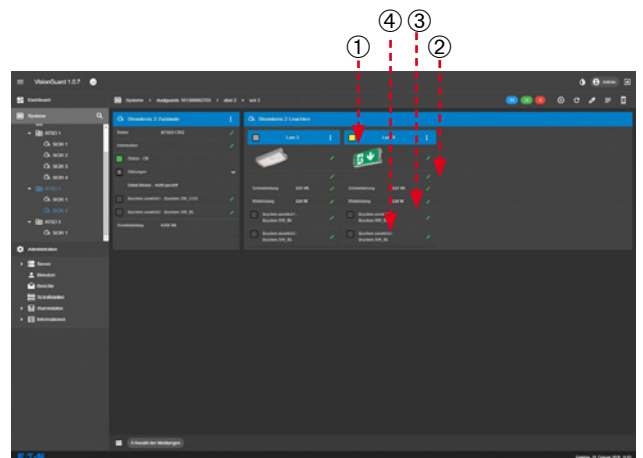
The ATSD detail view displays the SKU types and the names, additional information and total statuses of each circuit. The texts and the additional information can be edited by clicking on the green pen icon ①. In this case, it is advisable to enter target location designations in which the circuits with 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 ② to open the circuit's lights detail view.



## 10.6 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.

- ① The status of the light is displayed in the light widget header. Gray = off, yellow = on, red = fault/defect
- ② Under the heading text, the type of light can be defined using the green editing pen. The following types of lights are possible. Safety light, emergency sign light, left arrow rescue sign, right arrow rescue sign, down arrow rescue sign, up arrow rescue sign and red cross sign (GuideLed DX). IA and Matrix are currently not used.
- ③ In the information field "Apparent power" and "Real power", it is possible to enter the electrical data of the lights for informative purposes, in order to be able to more easily determine, for instance, the total load on the system.
- ④ Under switches 1 and switch 2 you can read out the assignment of the light to switches 1 + 2.



## 10.7 Configuration of a DualGuard-S

### 10.7 Configuration of a DualGuard-S

To configure a DualGuard-S system, the user must have Administrator or Supervisor rights!  
The configuration of the whole DualGuard-S system is only possible in the Administration area in menu "DualGuard-S", submenu „Interfaces“ and „DualGuard-S“:

Clicking on the gearwheel symbol (1) on the desired DualGuard-S opens the configuration menu

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

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

#### 10.7.1 System configuration

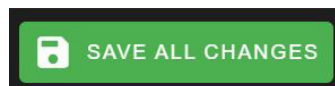
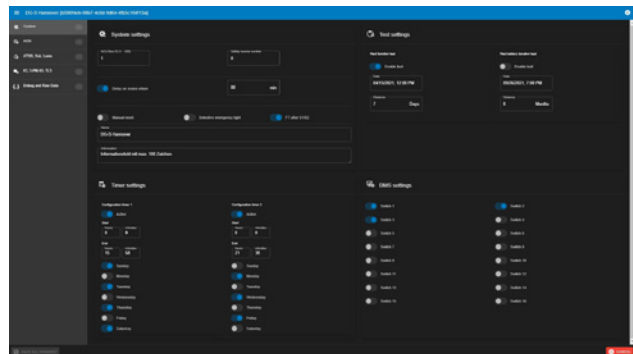
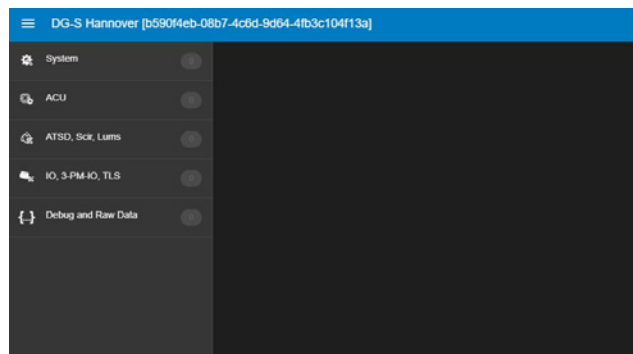
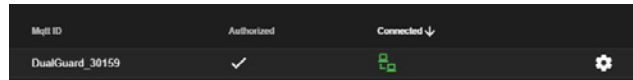
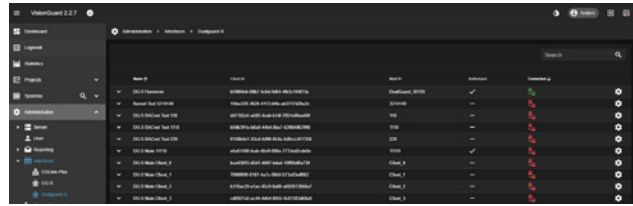
In the system configuration, all basic HMI settings can be made, such as:

- Name and Information text of the DG-S
- next automatic FT or DT
- Delay on mains return in min.
- Manual reset
- Selective emergency light etc.

For more details on the HMI basic settings, refer to the DG-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 HMI of the DG-S.



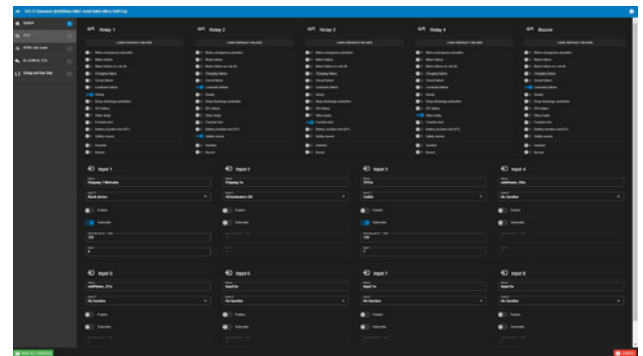
## 10.7.2 ACU configuration

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.

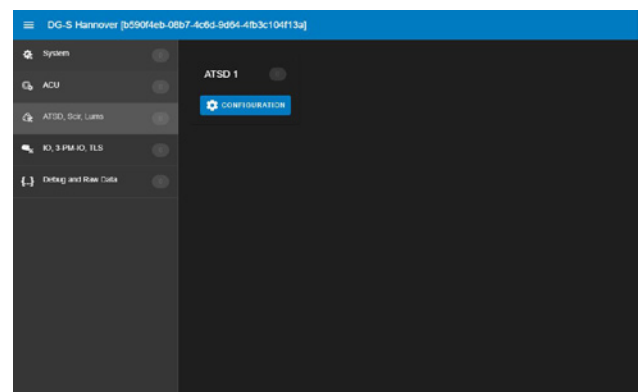
The digital Inputs of the ACU can be “Publish” and “Subscribed” to other ACUs of other DG-S, to enable a cross-plant function of several DualGuard-S systems. For more details on the ACU settings, refer to the DG-S manual.



## 10.7.3 SKU (ATSD) configuration

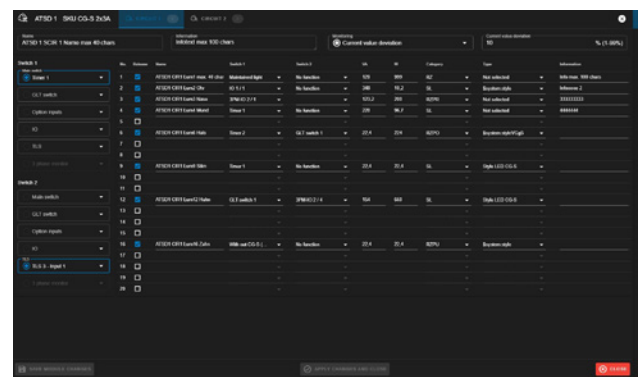
In the SKU configuration, all installed SKU (ATSD) are shown in an overview.

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



In the above part (1) the desired circuit can be selected. In this configuration menu, all desired settings up to the luminaire level can be made as usual, such as:

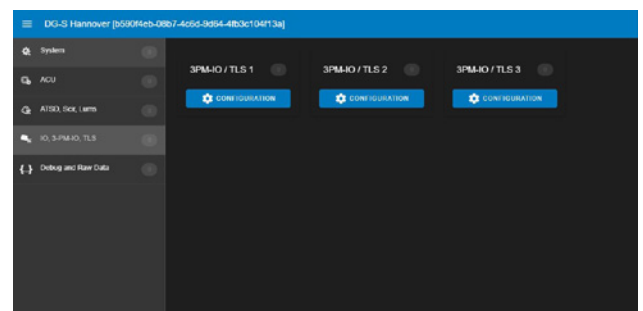
- Monitoring mode, e.g. CG Monitoring
- Information text of the circuits or luminaires
- Switch assignment of the circuit or luminaires
- Luminaire category
- Load of the luminaire in VA or W



## 10.7.4 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



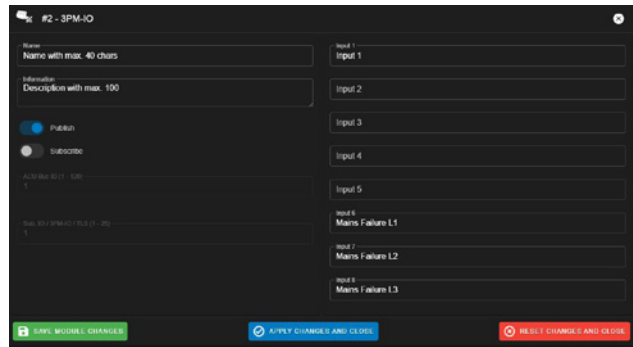
## 11 ZB-S Visualization

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
- Load of the luminaire in VA or W

The IO, 3PM-IO, TLS modules can be “Publish” and “Subscribed” to other IO, 3PM-IO, TLS modules of other DG-S, to enable a cross-plant function of several DualGuard-S systems.

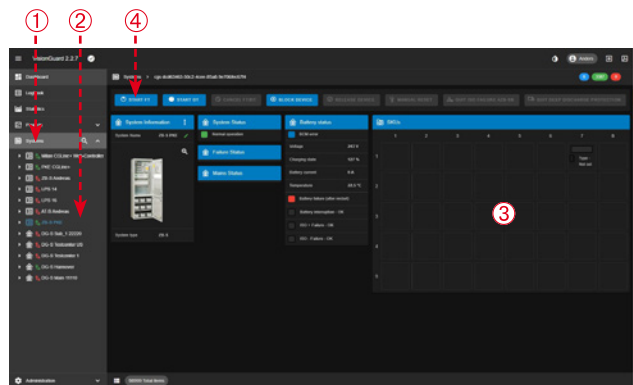
For more details on the IO, 3PM-IO, TLS modules settings, refer to the DG-S manual.



## 11 ZB-S Visualization

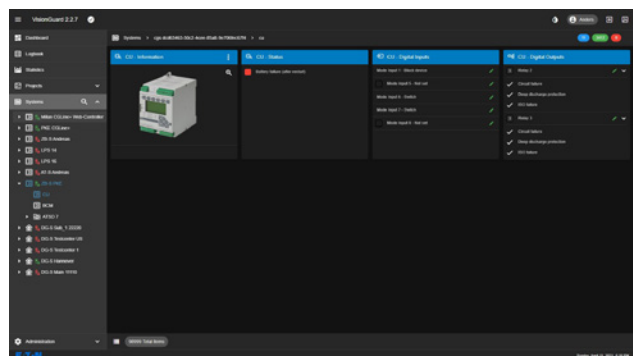
### 11.1 ZB-S detail view

Under the „Systems“ menu, all Dualguard-S/ZB-S systems are listed with their device names in the explorer structure (1). Click on the name (2) to see the detailed view of the ZB-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 SKUs (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 ZB-S, such as start a function test (Start FT) (4).



### 11.2 CU detail view

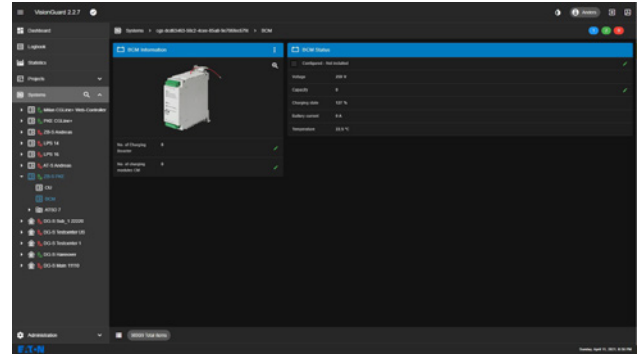
the CU detail view shows the CU status, the CU digital input configurations and the CU digital relay outputs. It is not possible to configure the digital inputs and relays in VisionGuard. These configurations must be carried out via the ZB-S PC-software.



## 11.3 BCM detail view

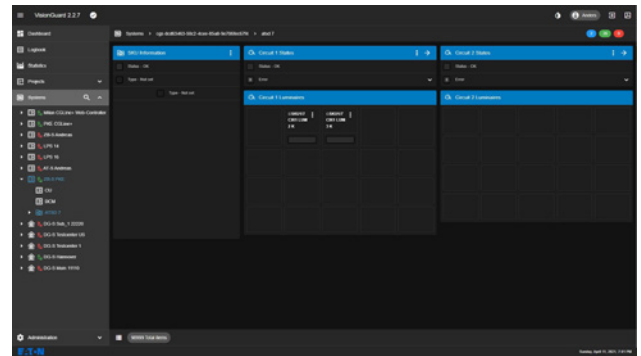
The BCM detail view shows the installed charging technology, consisting of BCM (battery control module) and CM (charger module) charging parts.

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.



## 11.4 SKU detail view

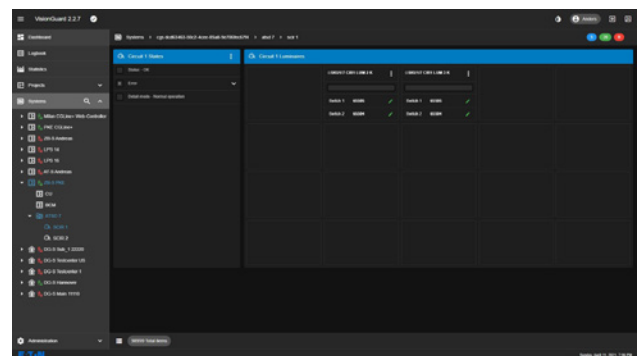
The SKU detail view displays the SKU types and the names, additional information and total statuses of each circuit according to the backplane assignment in the ZB-S cabinet. In the event of a circuit fault, the fault indicator will also pop up red here, which will then indicate the exact circuit fault. Click on the arrow in the blue Circuit head line to open the circuit's lights detail view.



## 11.5 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

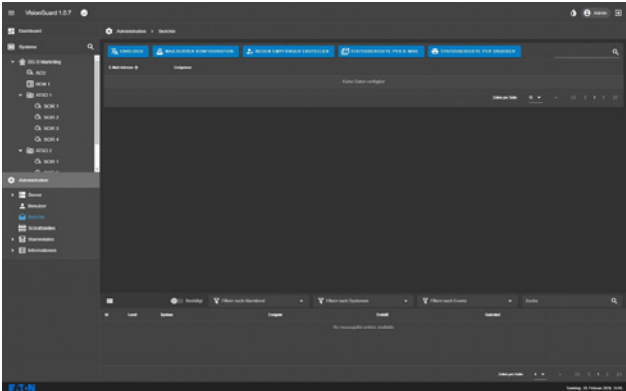




12 E-Mail, printing and export function

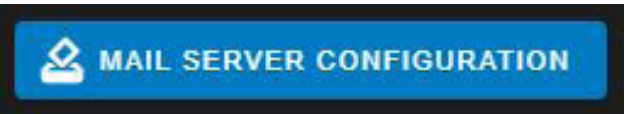
12 E-Mail, printing and export function

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



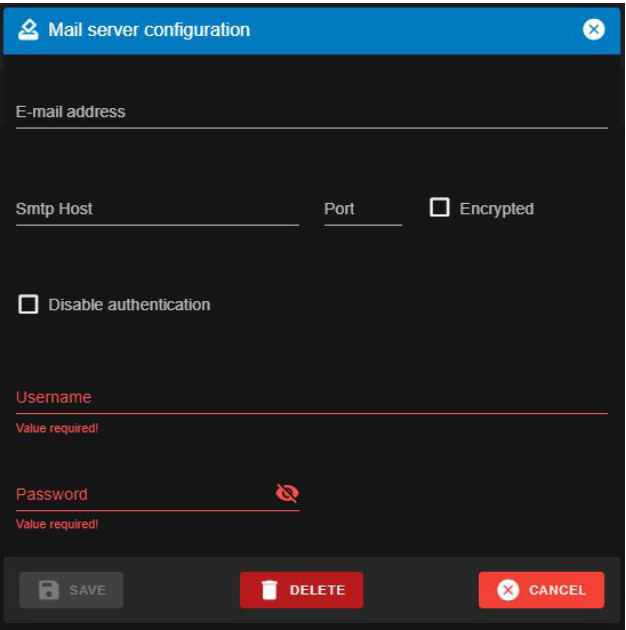
12.1 E-mail function

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.



12.1.1 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 "E-mail server configuration" button



A configuration window opens

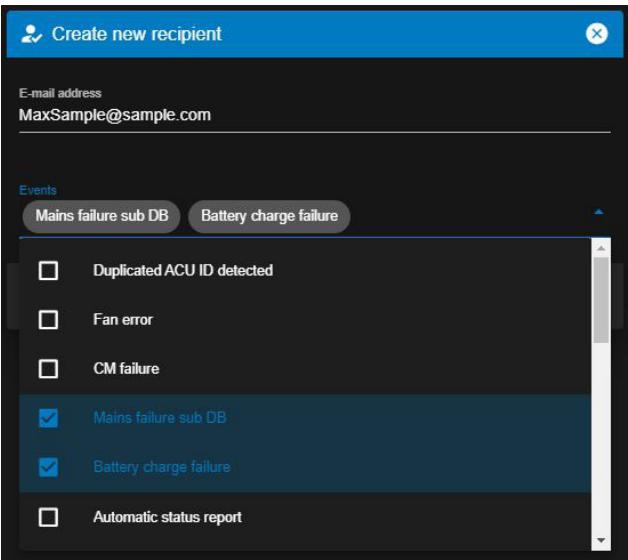
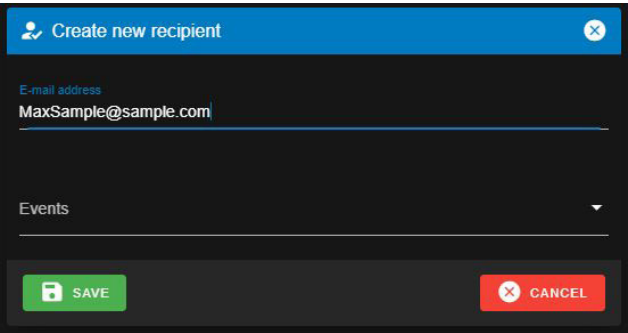
Contact your IT department for the correct e-mail server data.

### 12.1.2 Creating e-mail recipients

Click the "Create e-mail recipient" 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.



### 12.1.3 Automatic status e-mail

#### 12.1.3 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 DualGuard-S 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 DualGuard-S systems, the e-mail might be very long.

③ →

☐ Automatic status report

**STATUS REPORT BY E-MAIL**

**Status report by e-mail**

**Time settings**

☒ Monday  
☐ Tuesday  
☐ Wednesday  
☐ Thursday  
☒ Friday  
☐ Saturday  
☐ Sunday

Hour: 12 Minute: 15

☒ only errors

**Systems**

☐ DG-S/55554  
☒ DG-S/100000000951  
☐ DG-S/tst0  
☐ DG-S/12342  
☒ DG-S/client\_\_11110  
☒ DG-S/33330  
☒ DG-S/12341  
☐ DG-S/12340  
☐ DG-S/0  
☐ DG-S/55553

**SAVE** **CANCEL**

#### 12.2 Print function

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

In the following configuration window, the same settings can be made as for the "Status reports via e-mail" function

**STATUS REPORT VIA PRINTER**

**Status report by e-Print**

**Time settings**

☒ Monday  
☐ Tuesday  
☐ Wednesday  
☒ Thursday  
☐ Friday  
☐ Saturday  
☐ Sunday

Hour: 2 Minute: 0

☒ only errors

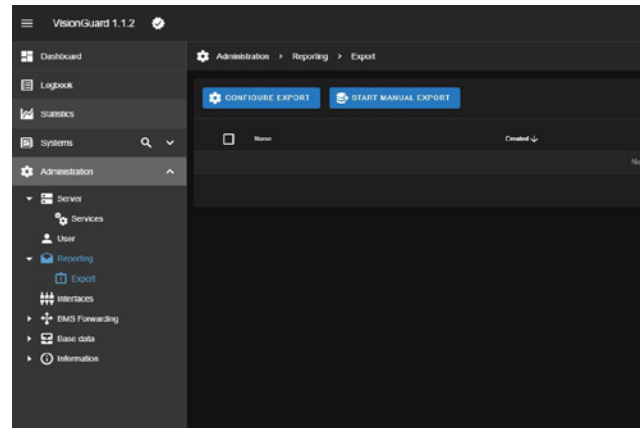
**Systems**

☐ DG-S/55554  
☒ DG-S/100000000951  
☐ DG-S/tst0  
☐ DG-S/12342  
☐ DG-S/client\_\_11110  
☐ DG-S/33330  
☐ DG-S/12341  
☐ DG-S/12340  
☐ DG-S/0

**SAVE** **CANCEL**

## 12.3 Export function

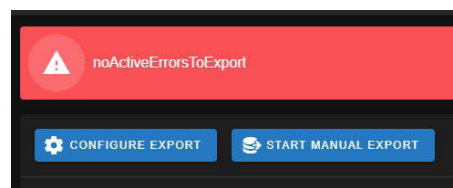
The “Export” function in the “Reporting” menu allows to export all occurred faults of the DualGuard-S systems in an Excel-based .csv file, e.g. for further processing by external applications.



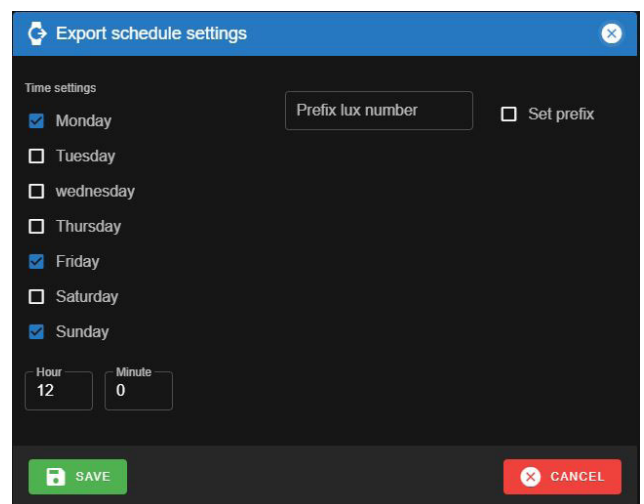
When the Export menu is selected, a black screen with two buttons appears “Configure Export” and “Start Manual Export”.

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 export 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 configured.

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:

```
LogId,EventId,System,SystemName,Name,Level,Device,Label,StateType,Created,PersonalComment
114570,57351,DG-S/101300062703,DG-S Marketing,avState1.moFl,Information,SYSTEM,System.moFl,Closed,04/06/2020 11:37:26,
114569,57351,DG-S/101300062703,DG-S Marketing,avState1.moFl,Information,SYSTEM,System.moFl,Opened,04/06/2020 11:37:46,
114568,57350,DG-S/101300062703,DG-S Marketing,uiDetailError.switchOfBatteryModeAccordingUnderVoltage,Information,ATSD/1/SCIR/1,System.switchOfBatteryModeAccordingUnderVoltage,Opened,04/06/2020 11:33:03,
114567,57349,DG-S/101300062703,DG-S Marketing,avState4.errMainsExtAtsd,Information,SYSTEM,System.errMainsExtAtsd,Opened,04/06/2020 11:33:03,
114566,57348,DG-S/101300062703,DG-S Marketing,avState4.btTestAllowed,Information,SYSTEM,System.btTestAllowed,Opened,04/06/2020 11:33:03,
114565,57347,DG-S/101300062703,DG-S Marketing,avState4.errSum,Information,SYSTEM,System.errSum,Opened,04/06/2020 11:33:03,
114564,57346,DG-S/101300062703,DG-S Marketing,avState4.errAe,Information,SYSTEM,System.errAe,Opened,04/06/2020 11:33:03,
114563,57345,DG-S/101300062703,DG-S Marketing,avState4.errDistis,Information,SYSTEM,System.errDistis,Opened,04/06/2020 11:33:03,
114562,57344,DG-S/101300062703,DG-S Marketing,avState4.errMainsSubstation,Information,SYSTEM,System.errMainsSubstation,Opened,04/06/2020 11:33:03,
114561,57343,DG-S/101300062703,DG-S Marketing,avState4.errFan,Information,SYSTEM,System.errFan,Opened,04/06/2020 11:33:03,
114560,57342,DG-S/101300062703,DG-S Marketing,avState3.errBcm,Information,SYSTEM,System.errBcm,Opened,04/06/2020 11:33:03,
114559,57341,DG-S/101300062703,DG-S Marketing,avState3.errCm,Information,SYSTEM,System.errCm,Opened,04/06/2020 11:33:03,
114558,57340,DG-S/101300062703,DG-S Marketing,avState3.errAcu,Information,SYSTEM,System.errAcu,Opened,04/06/2020 11:33:03,
114557,57339,DG-S/101300062703,DG-S Marketing,avState3.errLum,Information,SYSTEM,System.errLum,Opened,04/06/2020 11:33:03,
114556,57338,DG-S/101300062703,DG-S Marketing,avState3.errPss,Information,SYSTEM,System.errPss,Opened,04/06/2020 11:33:03,
114555,57337,DG-S/101300062703,DG-S Marketing,avState3.errBbs,Information,SYSTEM,System.errBbs,Opened,04/06/2020 11:33:03,
```

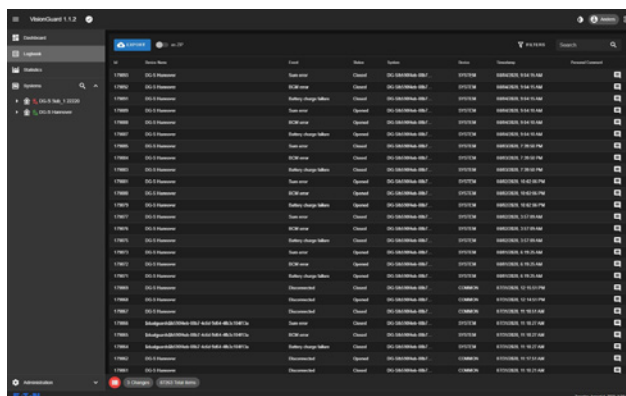
## 13 Log book

### 13 Log book

VisionGuard has a log book function to fulfill all requirements in accordance with DIN EN 50172/DIN VDE V 0108-100-1. The log book is in the lowermost position in the navigation bar.

Since the minimum period covered by the log book 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 log book has many filter functions as well as a search function.

In the default settings, the most recent log book entries are displayed at the top of the list.



- ① The log book can be downloaded in the Excel-readable format .csv by clicking "Export." In order to significantly reduce the download time if the log book contains many entries, it is advisable to download the file compressed as a ZIP file.
- ② You can narrow down the log book by date and time (time range)
- ③ Filter function allows filtering by system name and event (multiple selection is possible) and search function to find specific events
- ④ The eye icon can be used to navigate specifically to the screen where the event occurred

## 14 History menu

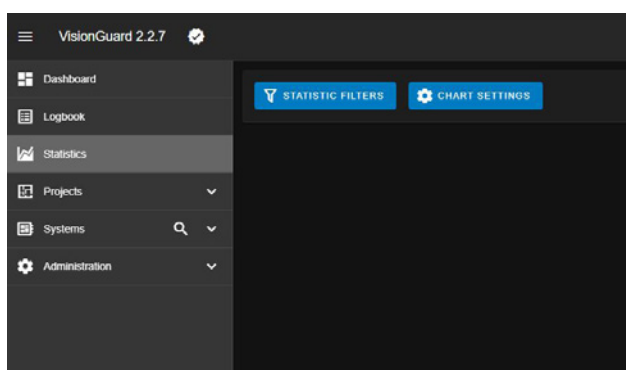
In the History menu, the four battery analog values such as battery voltage, battery current, battery room temperature and the state of charge of the battery can be displayed in a configurable graph over time. This function illustrates nicely e.g. the course of a battery duration test. This can help 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.

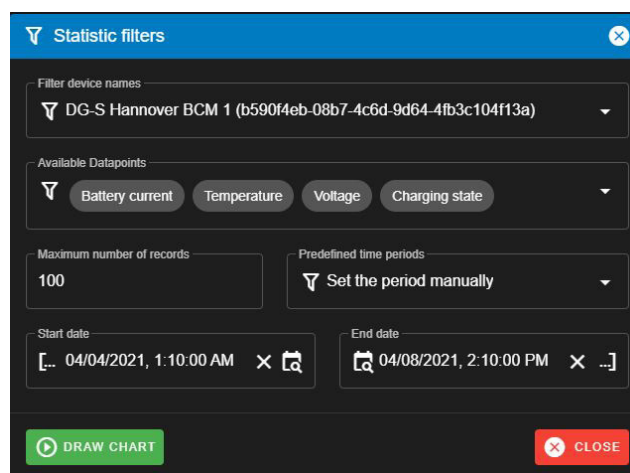
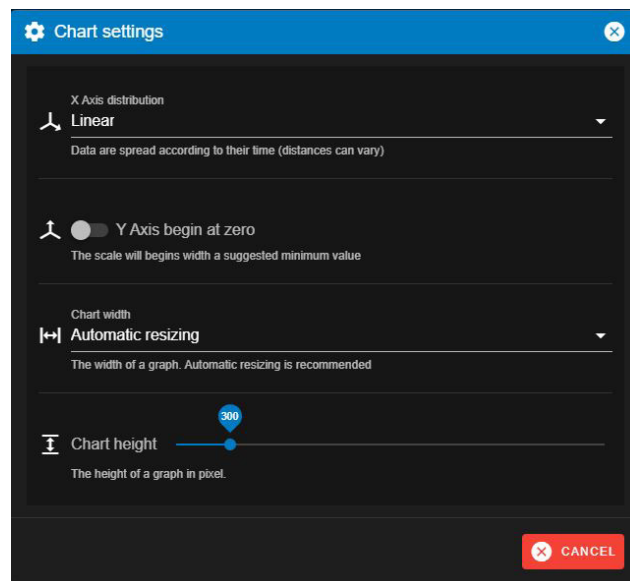
Presetting is 300 pixel.

After defining the graphic configurations, the graphics can be generated via „Draw chart“. A „Filter“ window will open:

Via „Filter device names“ the desired DualGuard-S or ZB-S system can be selected.

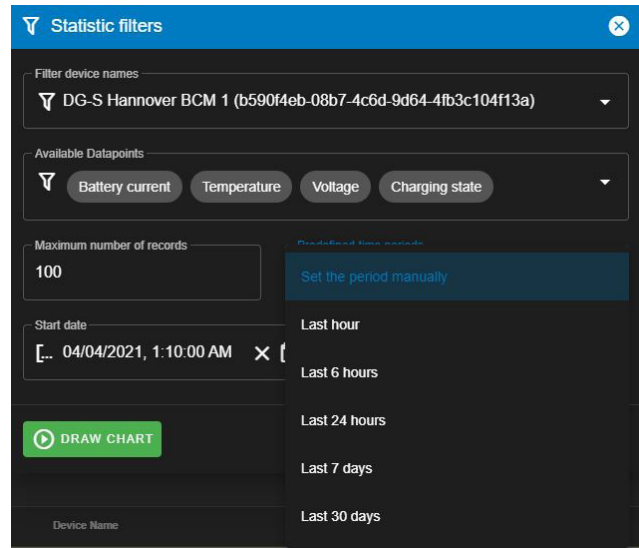
Via „Available datapoints“ the desired battery analogue values „Battery voltage“, „Battery current“, „Temperature“ and „Charging state“ can be selected. Example shows all available datapoints.

With Predefined time periods you can set the desired time period for the graphics. Either fixed time ranges can be set, or a start and end date/time can be set via „Set the period manually“. The example shows a period from 04th April 2021 01:10AM to 08th April 2021 02:10 PM



## 15 Backup & Restore Menu

Alternatively, a fixed time can be set much faster via „Pre-defined time period“, last hour, last 6 hours, last 7 days or last 30 days.

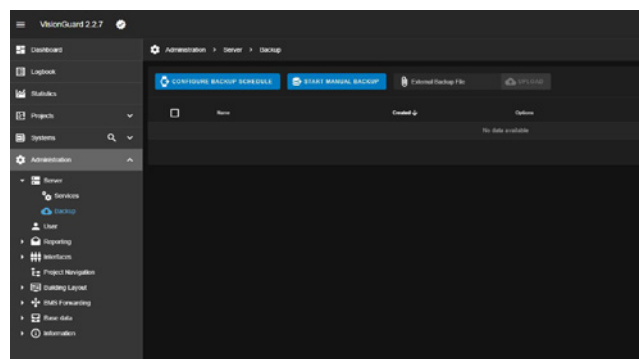


For example, it is quickly possible to look at the battery values directly after a battery duration test via “last hour”. In order to display the graphics clearly, the maximum number of recording points can be defined at the end. Presetting is 100 number of records. The graphics are generated automatically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



## 15 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. Please note: A manual Backup is only possible with local access to the VisionGuard, or with an access via a remote software!





### 15.1 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.  
Please activate all items for a full backup

### 15.2 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.  
Please activate all items for a full backup.  
With “Apply and Start” the download will be started,  
And create an entry in the Backup list

### 15.3 Creation of a manual restore

Via the button “Upload” it is possible to restore the VisionGuard with a created Backup file.  
Click on Upload, select the desired Backup file, and press OK.

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

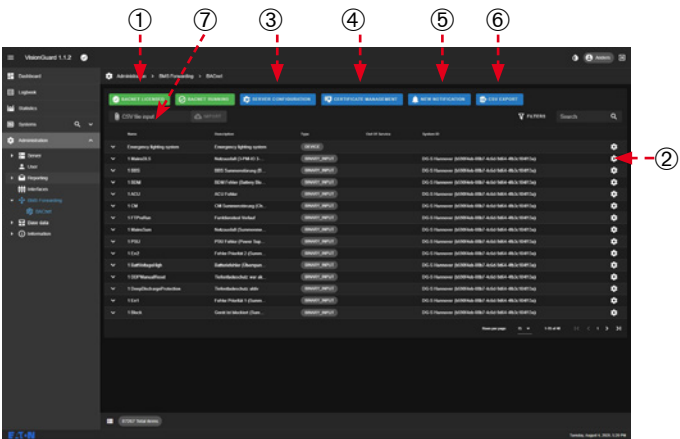
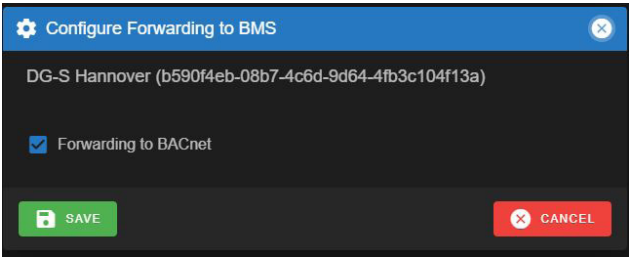
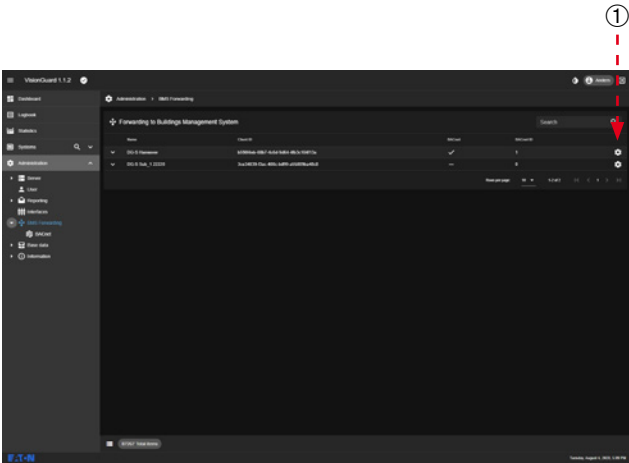
16 BACnet/IP Interface for DualGuard-S

If a BACnet/IP license 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 DualGuard-S.

This can be configured via the gear symbol ①. The following window opens. With a check mark „Forwarding to BACnet“ the BACnet interface can be activated for these Dualguard-S. With „Save“ the setting will be saved.

In the submenu „BACnet“ you can now check if the BACnet license and the BACnet server for connecting a BMS is activated in green. ①  
In addition, the BACnet data points (BACnet objects) can now be configured for the BMS via the gear wheel symbol ②.

Figure – BACnet Forwarding



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.

### BACnet Server Configuration

In this configuration menu the settings for the BACnet server can be done:

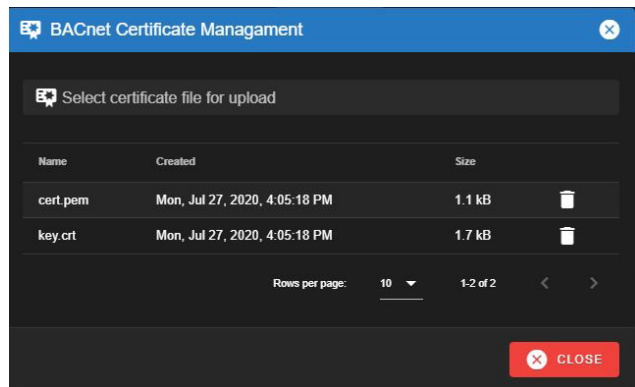
The “Instance number” is important for the unique identification of the Dualguard-S system on the BMS side.  
If BACnet Secure is required, it must be activated here

①. For further settings it is possible to configure BACnet secure settings under “CERTIFICATE MANAGEMENT”

## 16 BACnet/IP Interface for DualGuard-S

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

Certificates that are no longer needed can be deleted using the trashcan symbol.



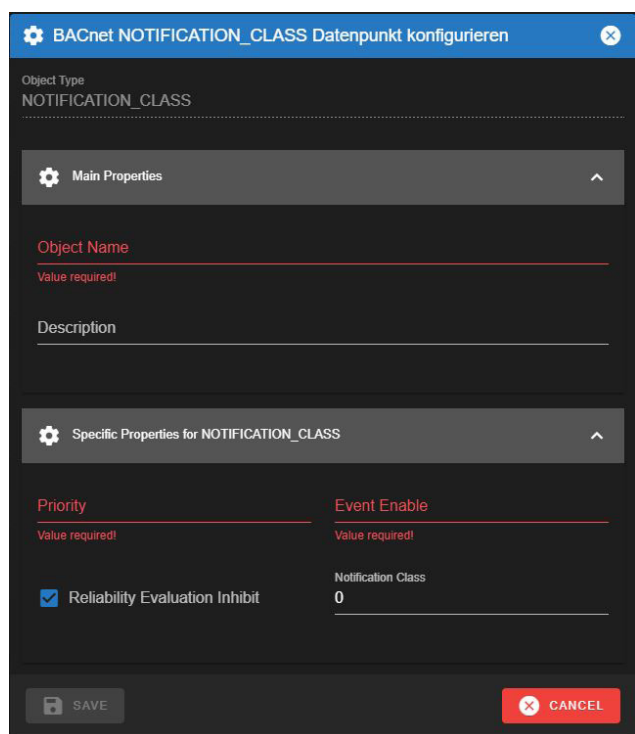
If required for the BMS notification classes, these can be configured in the „NEW NOTIFICATION“ menu.

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. After changing all data (important: everything must fit!) the csv. file can be loaded via the CSV file input „IMPORT“ function.



## 17 Administration area

In the CGVision administration area, you can restart services, manage users and licenses and information read about open source and changes in the different VisionGuard versions. Do not make any changes in the master data!

**Services** (see Section 17.1 Services)

**User** (see Section 6 – Creating new users with user roles)

**Reporting** (see Section 12 – E-mail and print function)

**Interfaces** (see Section 7 – Adding Dualguard-S systems to VisionGuard or Section 8- Adding ZB-S to VisionGuard)

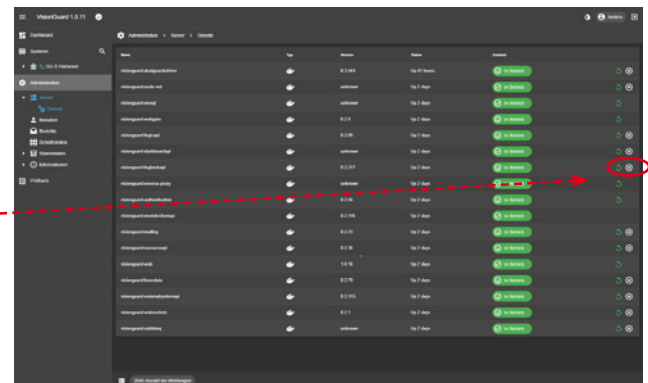
**BMS Forwarding** (See Section 16 BACnet/IP interface (optional) ) – Configuration of the optional available BACnet/IP interface

**Base data** – do not make any changes here!

**Information** – contains information on changes between different VisionGuard versions, licenses (see Section 4 Licensing) and open source with information about the open source software used

## 17.1 Services

The Services menu shows the functional state (operation) of all services used in VisionGuard. All services run independently, so VisionGuard is highly redundant by design. If a service fails, it is displayed in red. It can then be restarted by clicking on the symbol.



Eaton is dedicated to ensuring that reliable, efficient and safe power supply is available when it is needed most. With vast knowledge of power management across different industries, experts at Eaton deliver customized, integrated solutions for solving our customers' most critical challenges.

Our focus is on delivering the right solution for the application. But decision makers demand more than just innovative products. They turn to Eaton for an unwavering commitment to personal support that makes customer success a top priority. For more information, visit **[www.eaton.com](http://www.eaton.com)**.

**Eaton Industries Manufacturing GmbH**

Electrical Sector EMEA  
Route de la Longeraie 7  
1110 Morges, Switzerland  
[Eaton.eu](http://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](mailto:info-n@ceag.de)  
Website: [www.eaton.com](http://www.eaton.com)

© 2021 Eaton  
All rights reserved  
Printed in Germany  
Article no. 40071860371 (B)  
Publication number MN451070EN  
July 2021

Eaton is a registered trademark.

All other trademarks are the property of their respective owners.