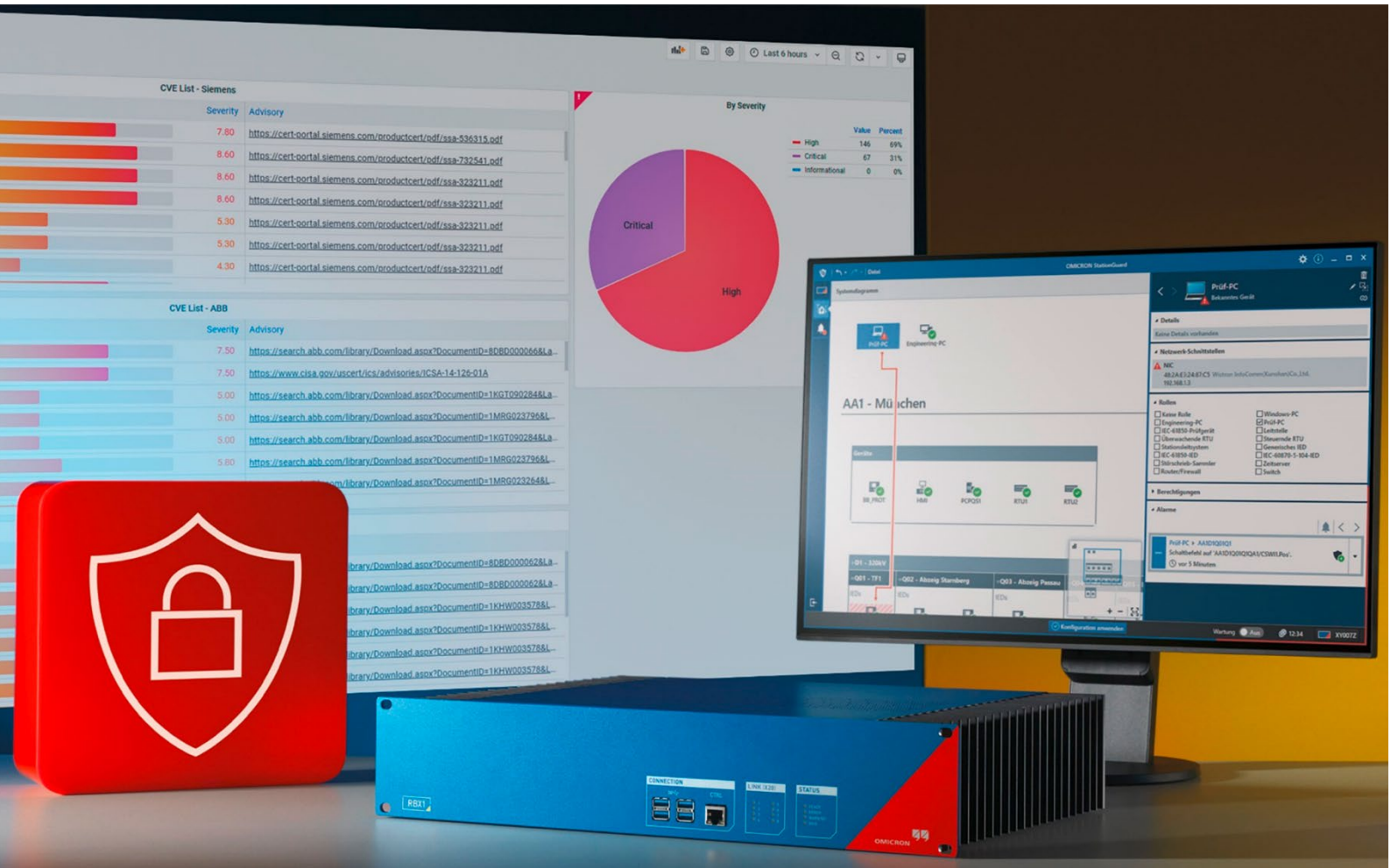
OMICRON

StationGuard Sensor

What’s New in Version 3.00



Version 3.00

Highlights

- Create new devices via CSV import
- Visualize the entire network communication
- Device role template library (DRTL)
- Replay PCAP
- Start and stop maintenance mode via binary inputs

1 Create new devices via CSV import

You can add previously known devices to StationGuard by importing an asset inventory CSV file. The CSV can include details such as device name, description, nameplate data, MAC address, and IP address. Device roles can also be assigned directly within the file.

This feature enables a full configuration of StationGuard including all network devices to be prepared in advance, allowing setup to be completed in the office before deployment on-site.

These are the new options available for implementing the StationGuard Sensor:

- Create missing network interfaces when importing assets.
- Create missing devices with network interfaces when importing assets.
- Have a separate section in the ZeroLine for imported assets.

2 Visualize the entire network communication

The *Network Diagram View* feature introduces a new visualization panel that complements the system diagram by depicting network communication and its participants. This panel has detailed statistics and insights into active services, protocols, and node activities. You can quickly identify nodes, analyze communication patterns, and gain a comprehensive understanding of network context.

These are the new options available for visualizing your network communication:

- Show a graph visualization of the network communication.
- Combine nodes within the network diagram based on devices defined in the system definition.
- Select nodes in the network diagram to show the overview of the respective device in the system model.
- Show available information for network diagram nodes unknown to the system model.
- Refresh the network diagram.
- Track the network protocols/applications used by selected device.

3 User interface and documentation in more languages

The StationGuard user interface and documentation is available in English, German, and French.

4 Start and stop maintenance mode via binary input

Maintenance mode can be activated in two ways: Either via the user interface of the StationGuard Sensor, or – thanks to the new feature – externally via binary input contacts on the RBX1. This allows third-party systems to trigger maintenance mode without accessing the UI. This is especially useful for teams such as

OT engineers, SCADA specialists, or remote operators in the control center who need to activate maintenance mode before performing work in the plant.

5 Replay PCAP

You can replay recorded network traffic (PCAP files) to analyze system behavior and event detection. Traffic is replayed in real-time not in bursts to ensure accurate analysis by the detection engine. Each packet is processed and compared against the established communication baseline and rules. Any deviations are flagged as alerts and labeled with *PCAP* for traceability.

6 Visibility of routed IP addresses

Routed IP addresses are displayed under the corresponding network interface of the router devices. With this feature, you can quickly identify routed devices and their associated IP addresses across the network. Routed IPs are only visible when the StationGuard sensor monitors both the inbound and outbound sides of the routed traffic.

7 Analyze alarms of selected devices in ZeroLine diagram

Simply hide all alerts in the ZeroLine diagram to focus exclusively on alerts from the selected device, simplifying analysis and emphasizing specific nodes.

8 Device Role Template Library (DRTL)

Our Device Role Template Library (DRTL) now contains profiles for many power utility automation and SCADA devices (SIPROTEC, REL, SPRECON, A8000 …), each with preset permissions.

9 License mechanism for VBX

The license file on the StationGuard VBX is time-limited, meaning the sensor will operate only until the end of the defined license period. After expiration, detection will stop. A 3-month grace period is provided, so you can still update the license if it was overlooked.

Licenses can be activated either online or offline via the license server.

10 Detection engine improvements

- Classification of OPC classic protocol is available.
- Classification of S7CommPlus protocol is available.
- StationGuard sensor detects usage of unrecommended cipher suites over encrypted traffics.
- Ensure core detection functionality under different load conditions.

11 Bug fixes and other improvements

- Additional icons for imported roles are available.
- "Roles & Permissions" files created in StationGuard version 3.00 or later are not compatible with StationGuard versions 2.40 and earlier. This incompatibility is due to changes in the detection engine, including the removal of certain protocols and the renaming of "IEC 61850 MMS" to "MMS."
- Multiple bugs and issues were fixed.

12 Product lifecycle and support notice

The update from StationGuard 2.40 to version 3.00 is free of charge for all installations. Please note that StationGuard version 3.00 replaces version 2.40 as service baseline. We strongly recommend updating all your devices to version 3.00.

At OMICRON, we take any type of vulnerability affecting our products very seriously, and we appreciate and welcome any report that helps us improve their security. Consequently, we have established a systematic approach for receiving, handling, and disclosing such vulnerabilities.

Please visit https://www.omicronenergy.com/en/support/product-security for further information.

Previous Releases

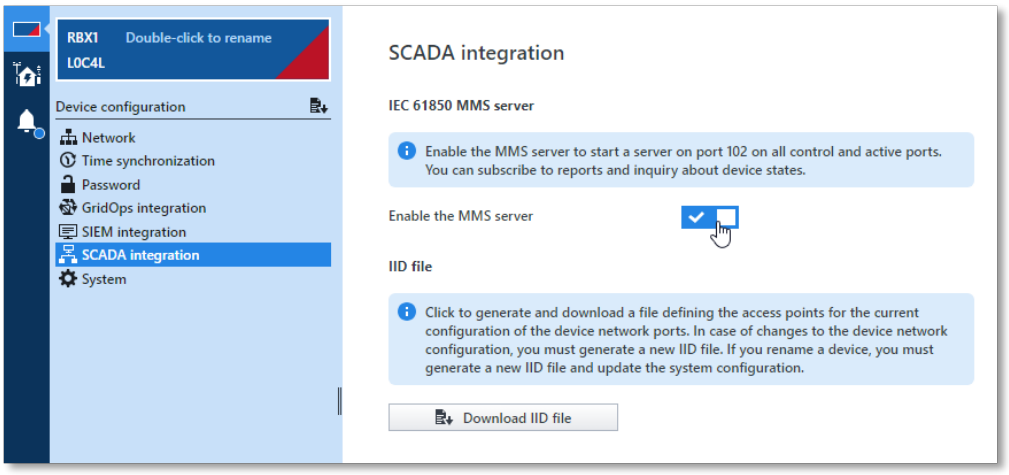
	Focus	Released in
Version 2.40	Reduced Configuration Effort	May 2024
Version 2.31	Installer Update	December 2023
Version 2.30	Roles, Permissions & Categorization	October 2023
Version 2.21	Critical Security Release	March 2023
Version 2.20	GridOps Support	January 2023
Version 2.10	Usability Improvements	June 2022
Version 2.00	Deep Packet Inspection	May 2021
Version 1.10	Asset Inventory Improvements	November 2020

Version 2.40

1 Usability upgrade with MMS server availability

StationGuard now includes an MMS server that provides access to the data model with current alarm states and maintenance mode status. You can download the data model as an .iid file and report it to MMS clients for SCADA integration. You will receive notifications of sensor events and maintenance mode changes in StationGuard.

In addition, StationGuard nameplate information, such as vendor, model, and hardware and software version, is accessible within the data model, allowing active asset inventory tools to query and use this data.



2 Enhanced Router support: Distinguish between devices

In StationGuard, devices communicating behind a router are associated with the router's MAC address. This previously resulted in multiple IP addresses being grouped under the same MAC address, causing potential confusion.

With the latest update, StationGuard can now distinguish individual devices communicating behind a router. This enhancement lets you create separate device entries for each IP address behind the router. You can then assign specific roles and permissions to these individual IP addresses which improves network visibility and security management.

3 Merge and split device interfaces

Often, discovered devices have more than one interface with different purposes. StationGuard can merge these interfaces and visualize them under one asset. The *Split* function allows you to split the network interfaces and IP addresses and add individual permissions and roles, which is especially useful for multi-function devices such as HMIs and RTUs.

4 Suppress warnings for MMS and IEC 104 events

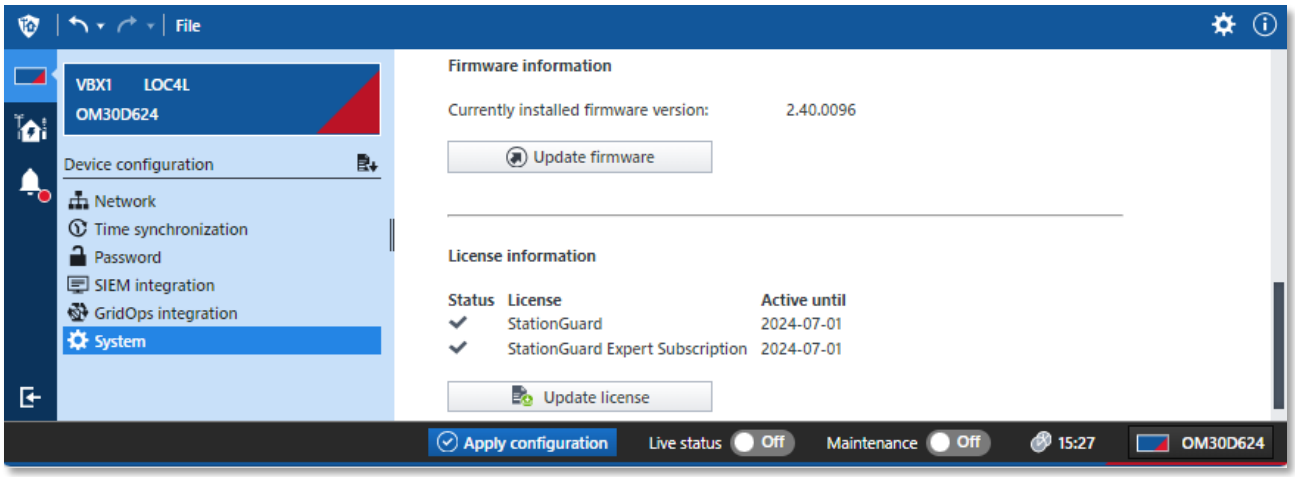
Failed control commands can generate excessive warnings, which you can now suppress in the same way as *info* events.

5 Custom certificates for StationGuard web interface

You can use custom certificates to securely access the StationGuard web interface.

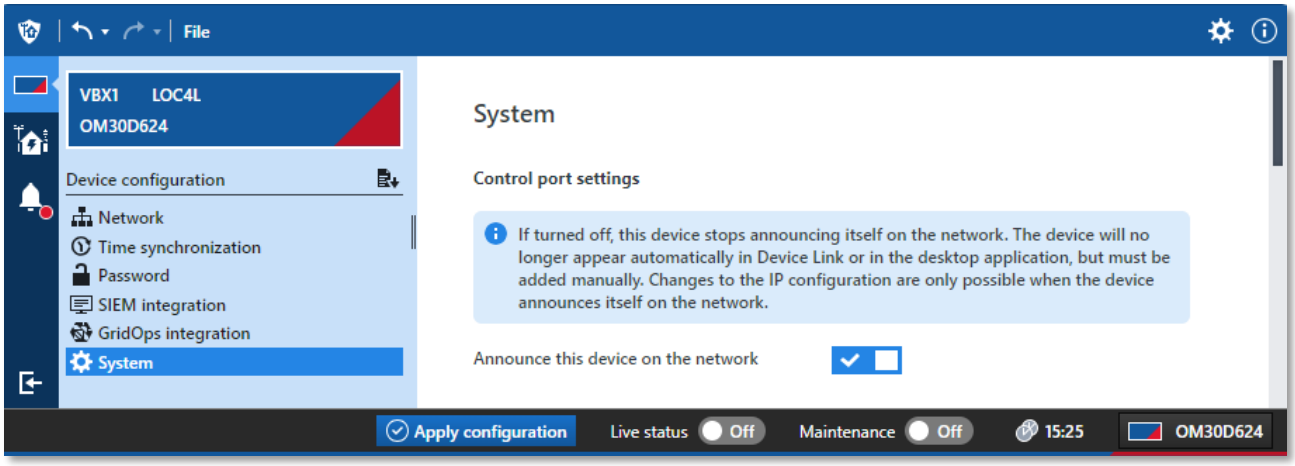
6 Update firmware and license of RBX/MBX/VBX via web interface

Conveniently update the firmware and license of your RBX, MBX, or VBX directly from the StationGuard web browser. Previously, firmware and license updates could only be performed through the StationGuard client software.



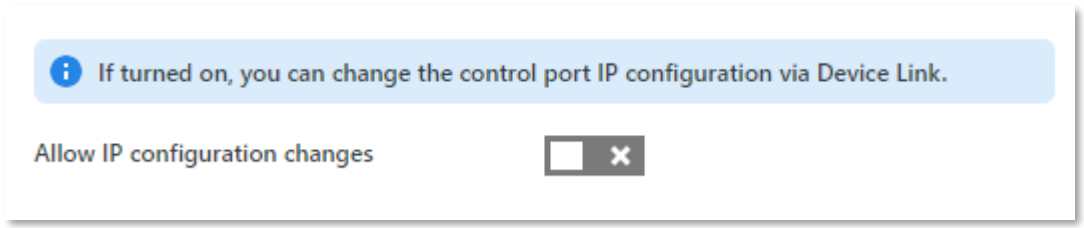
7 Disable device announcements

StationGuard announces itself via the Device Link control port and the StationGuard client software. You can now disable this announcement if the user does not want this traffic on the network.



8 Disable control port IP changes

To prevent unwanted IP address assignments, you can disable IP address changes from the sensor.



9 Connect the active port to more than one subnet

It is now possible to connect to different subnets using one active StationGuard port. This feature allows you to add multiple IP addresses to an active port and communicate with different subnets and networks.

10 Bug fixes and other improvements

> Bug fixes have been implemented to resolve the prioritization issue between multiple NTP servers for StationGuard.

Version 2.31

1 Update for StationGuard installer

The StationGuard installer includes the latest Device Link version, 3.00 SR1, to support older Windows 10 versions such as 1809 and newer.

2 Bug fixes

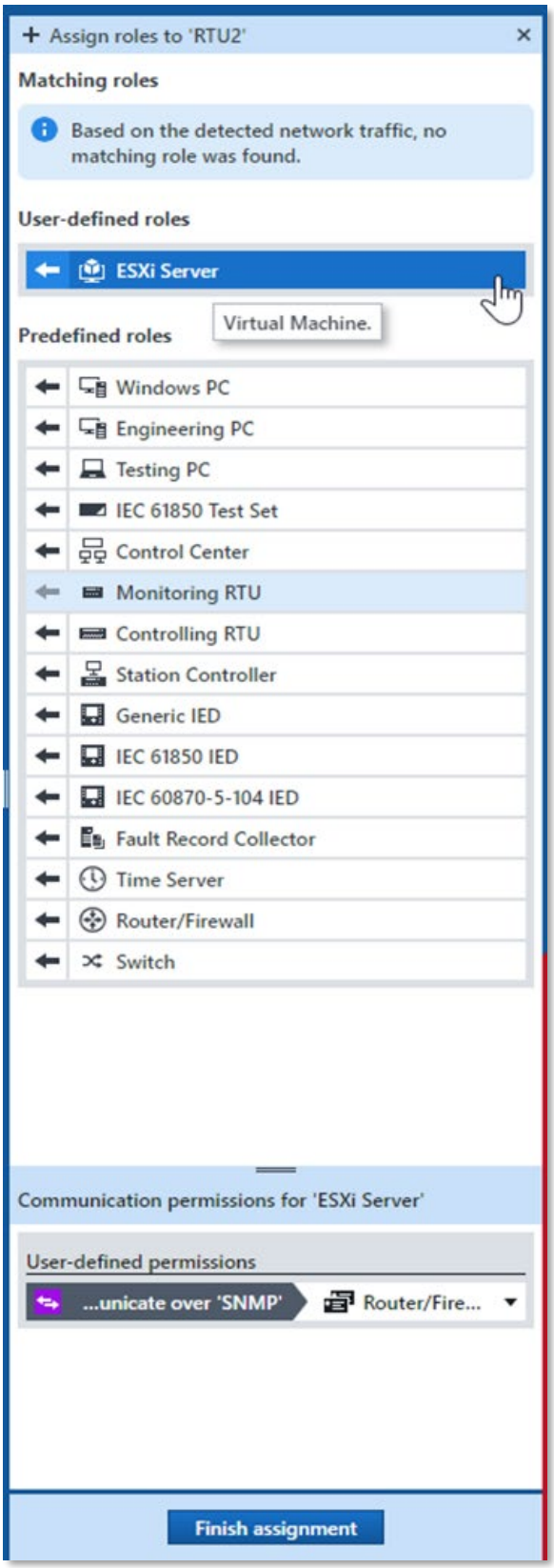
Numerous smaller bug fixes have been implemented.

Version 2.30

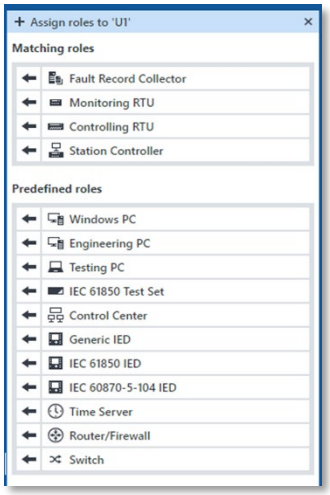
1 Custom roles & permissions for all sites

Stop waiting for alerts – take the initiative and define permissions proactively! Now, you can create custom roles and permissions tailored to your devices and network. This advanced feature gives you the freedom to optimize security according to your specific requirements, even if some traffic has not yet occurred during the learning phase.

It also eliminates the need to relearn all permissions and roles at each site. Simply import and export your own unique list of permissions and custom roles seamlessly across multiple sensors and sites using our well-defined JSON format.



2 Role matching & automatic device categorization



Get a smoother experience without the hassle of manual categorization and clueless role assignment. This efficient feature helps you quickly distinguish between different types of devices on your network, saving you valuable time.

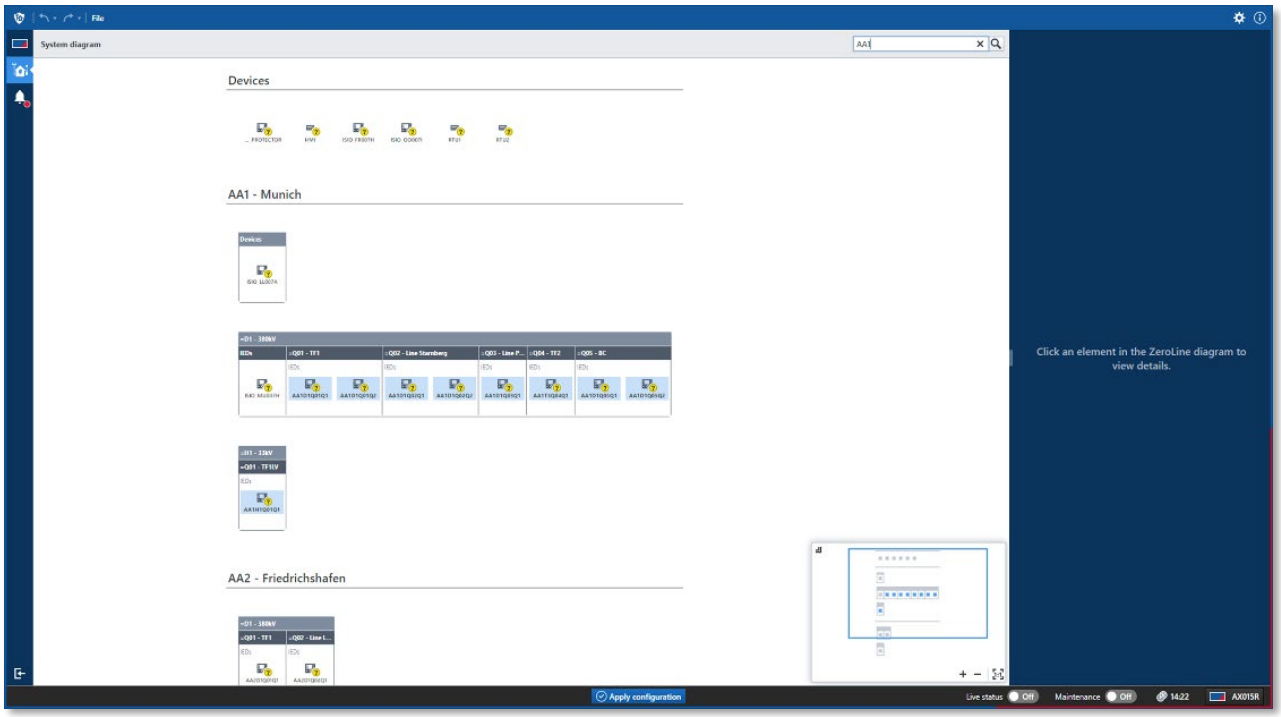
In addition, StationGuard's intelligent traffic comparison makes role assignment effortless. The system automatically detects and suggests the most appropriate roles at the top of the list (e.g., ACME-Protec-400-Relay, Protection Testing Laptop B), making it easier for you to assign them with confidence.

Enjoy enhanced visualization by creating graphical groups for devices such as PCs, IEDs, or network devices and use this easy-to-use feature to streamline your operations and improve your workflow.

3 Find devices in ZeroLine

Tired of wasting time searching, reading, and clicking through countless IEDs? Use the convenient search bar to easily locate and tag devices using various parameters, such as name, type, description, manufacturer, firmware version, hardware version, MAC address, and IP address. All devices matching your search criteria are highlighted in the ZeroLine diagram with a light blue background color.

The search function can also used to group matching devices together to better distinguish between areas, zones, and security levels during monitoring and analysis for a clearer and more comprehensive view.



4 Device-specific certificates for encrypted communication

Enjoy peace of mind as communication to the device is now even more secure. As of version 2.30, our MBX1 and RBX1 platforms now generate individual certificates for all encrypted communication, further enhancing

security. Previously, a common certificate was used for all devices, but this update ensures a unique certificate for each device.

Please note that you will need to identify and confirm the device once before connecting to it, as the certificates cannot be validated automatically.

5 VBX1: Run StationGuard, StationScout, and IEDScout on existing hardware

After successfully completing an extensive beta phase, the VBX1 has been rigorously tested in a variety of environments to ensure robust stability and reliability.

Along with our proven hardware offerings, the platforms RBX1 and MBX1, our innovative software solutions are now optimized for the VBX1 platform. This ready-to-deploy virtual machine runs effortlessly on VMware systems and delivers uncompromised software performance directly on your current virtualization infrastructure.

To ensure the optimal setup for your network, we invite you to consult with our experts who can help you choose the most suitable solution.

6 Security fixes

For more information about this issue, see our Security Advisories OSA-7.

7 Bug fixes and other improvements

- Info events for allowed communication can now be turned off for each permission individually.
- Fixed a bug where StationGuard would not show the NTP time as synchronized, even though the necessary accuracy was reached.
- The use of IEC 60870-5-104 ASDU types in the range 128-255 no longer triggers an encoding alert. his is now a separate alert and communication using ASDU types from this range can be allowed.

Version 2.21

1 Critical security release

This release contains important security fixes. We strongly recommend that you update all your sites immediately. For more details, see Security Advisories OSA-5 and OSA-6 at https://www.omicronenergy.com/en/support/product-security.

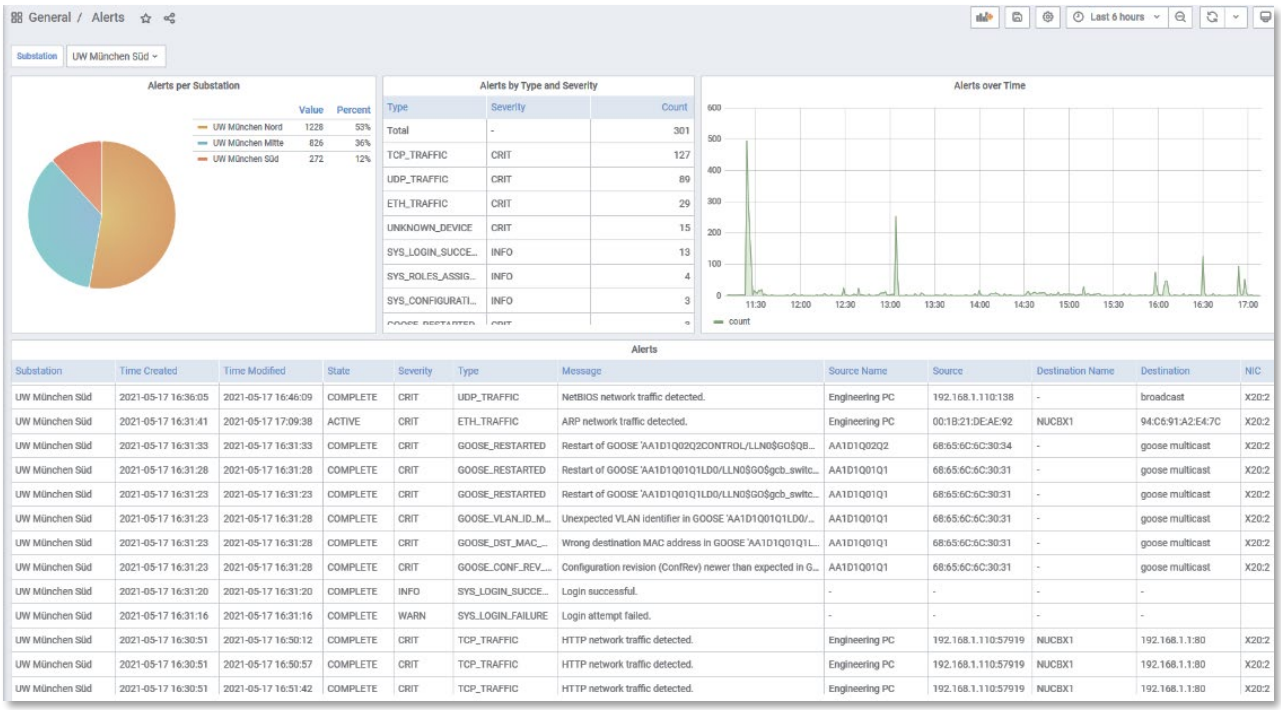
Version 2.20

1 Introduction

StationGuard 2.20 includes several improvements and new sensor-level features and supports the new central management system GridOps. Adding the new central management system GridOps to your StationGuard setup is optional, and the StationGuard sensors can still be used stand-alone.
GridOps provides multiple dashboards with different perspectives, which can be used as a visual representation of the security performance of the operational technology (OT) networks across the grid.

1.1 GridOps assets and events synchronization

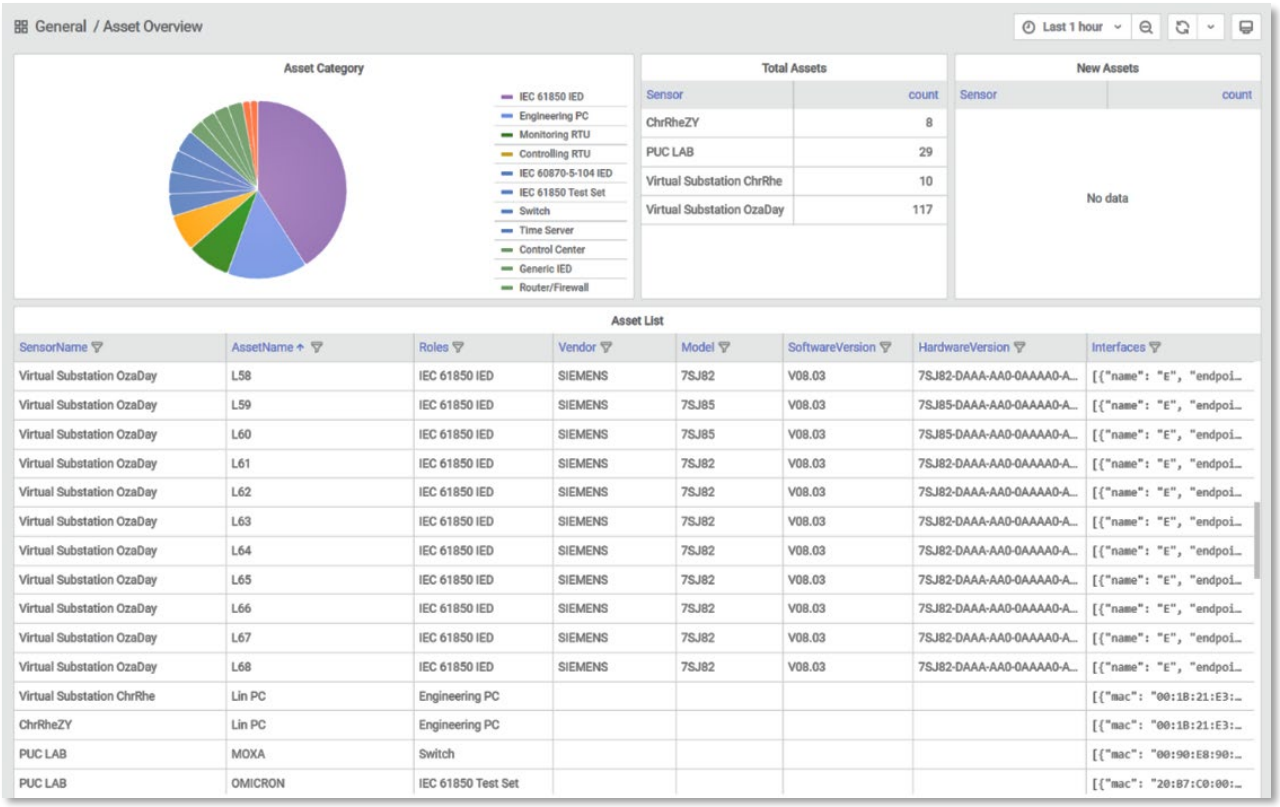
StationGuard 2.20 synchronizes all events with a central GridOps instance. If the connection between GridOps and a StationGuard sensor is interrupted, GridOps will re-synchronize all events as soon as the sensor is reachable again. GridOps thus serves as a backup and historical database for the alerts created by the StationGuard sensors.
GridOps offers different dashboards that can be used to view and analyze current and historical alerts. By using these dashboards, you will have a real-time understanding of the alert status across all your sites, and if there are any critical alerts, you will be notified immediately.
The GridOps platform has also been designed so that it keeps track of all alert activity from all sensor locations in its database. This makes it possible for you to quickly browse and search through all previous events from all sensor locations across time.
In addition to the alert statistics, pie charts and time-series graphs allow you to distinctly see how the various alert types were distributed across your sites. The information on how they relate to specific asset types and how the alert frequency changes over time allows you to analyze their relationship. You can use these statistics to analyze trends for specific events and detect general patterns and suspicious activities occurring over time.
You can also perform a number of additional analyses for all operational events (also known as functional events) that StationGuard logs, such as successful and unsuccessful switching operations, disruption record downloads, etc.



1.2 Global asset inventory

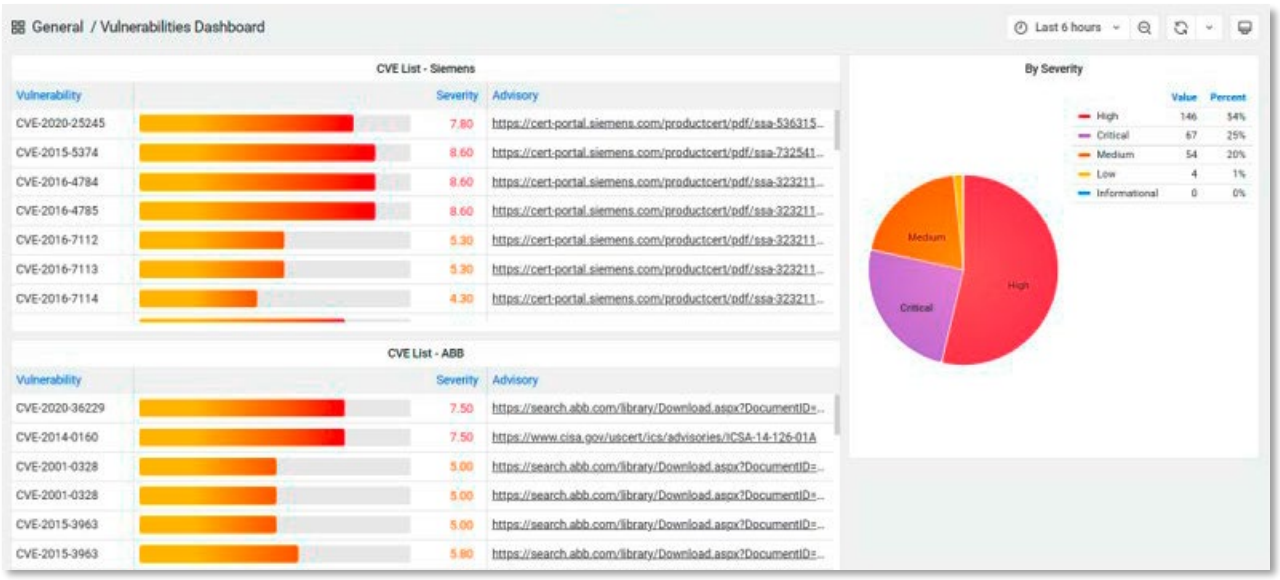
StationGuard synchronizes all assets to the central GridOps instance, which then creates a global asset inventory that is searchable and may be organized by asset type. This inventory contains all devices identified

by all StationGuard sensors located across the grid. GridOps also keeps a history of different asset inventory states over time. The application keeps the inventory up to date with asset information retrieved by all sensors connected to the system and displays asset properties in a table format in real-time so they can be easily viewed. Using the filter functions, you can search for specific asset types for vulnerability management. When combined with StationGuard's unprecedented ability to retrieve the most exact details about each asset, GridOps and StationGuard's capabilities work together to create a powerful asset inventory management solution. For instance, you can import SCL files or plant documentation spreadsheets containing asset data. Without a doubt, having comprehensive and rich data per asset is crucial for successful vulnerability and risk management, as you can prioritize the assets more successfully if you perform a more accurate vulnerability analysis thanks to your in-depth knowledge of each asset.
In addition to the automatic asset inventory, this feature is also available for sensors that are only active temporarily, like those found in the mobile version of StationGuard on the MBX1 platform.



1.3 Vulnerability management

It can be extremely difficult to match vulnerabilities discovered in protection and automation devices to actual hardware installed on-site. You must look at the issue from several perspectives and consider a number of variables to reach the most appropriate conclusion. To determine the applicable vulnerabilities, the exact device type, firmware version and module configuration must be known. It is critical to note that by conducting a risk assessment, you will be able to determine whether or not your devices may be vulnerable to being compromised in the future.
A further concern is the fact that security advisories may occasionally not be as accurate as they should be, which adds to the complexity of the situation.
GridOps' vulnerability management is designed to analyze the impact of various common vulnerability exposures (CVEs) and identify which IEDs are at risk based on the particular CVE or security advisory. The asset vulnerability dashboard offers insight into the extent of your vulnerability exposure as well as the criticality of those vulnerabilities and the patch capabilities of your assets in relation to them.

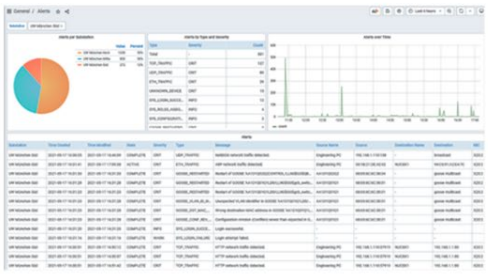


1.4 Reporting

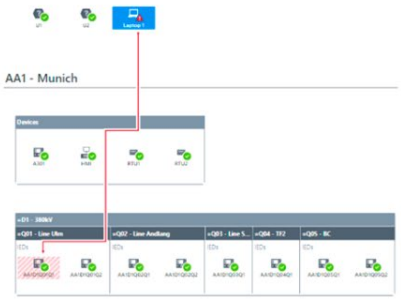
In addition to creating reports, GridOps also caters to your asset inventory and its vulnerabilities so that you have early insight into cybersecurity trends and statistics. By analyzing these reports, you can determine the level of security posture your organization has at any given time. Furthermore, it is also in the highest interest of management, vendors, and regulators that comprehensive information and reports are generated to identify and mitigate risks in a timely manner.

1.5 Grid to station level incident analysis

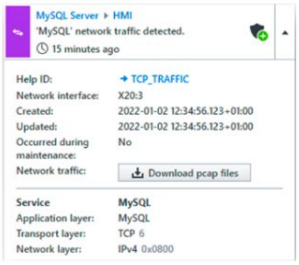
A key feature of StationGuard is its unique way of visualizing power grid networks by displaying the entire network and all devices in a graphical view that is familiar to both OT experts and IT officers at the same time. To effectively respond to emerging threats, GridOps provides a comprehensive analysis and investigation approach. It is now possible to view all the alerts using the familiar StationGuard ZeroLine diagram visualization and navigating from a grid-level overview to a specific control center, power plant, or substation network view. In most cases, the ZeroLine diagram is derived from the engineering documentation. Then, it is manually revised to be as similar as possible to the official plant network documentation.



Grid level
Multiple dashboards to provide overview on the status of all your networks



Plant level
Intuitive network visualization



Communication
Visualize assets and their communication

1.6 Active Directory integration and role-based access control

GridOps can be integrated into an Active Directory environment using LDAP as part of the integration process. With the purpose of limiting which sets of functions are available to which users, StationGuard assigns different roles to different users to control access to the various functions available for viewing and configuring StationGuard instances. Additionally, StationGuard IDS sensors may be accessed using the StationGuard local client user interface if a network is down for some reason. In this way, you are still able to access the sensors separately as a backup option if you desire.

1.7 Active asset identification using live nameplate reading

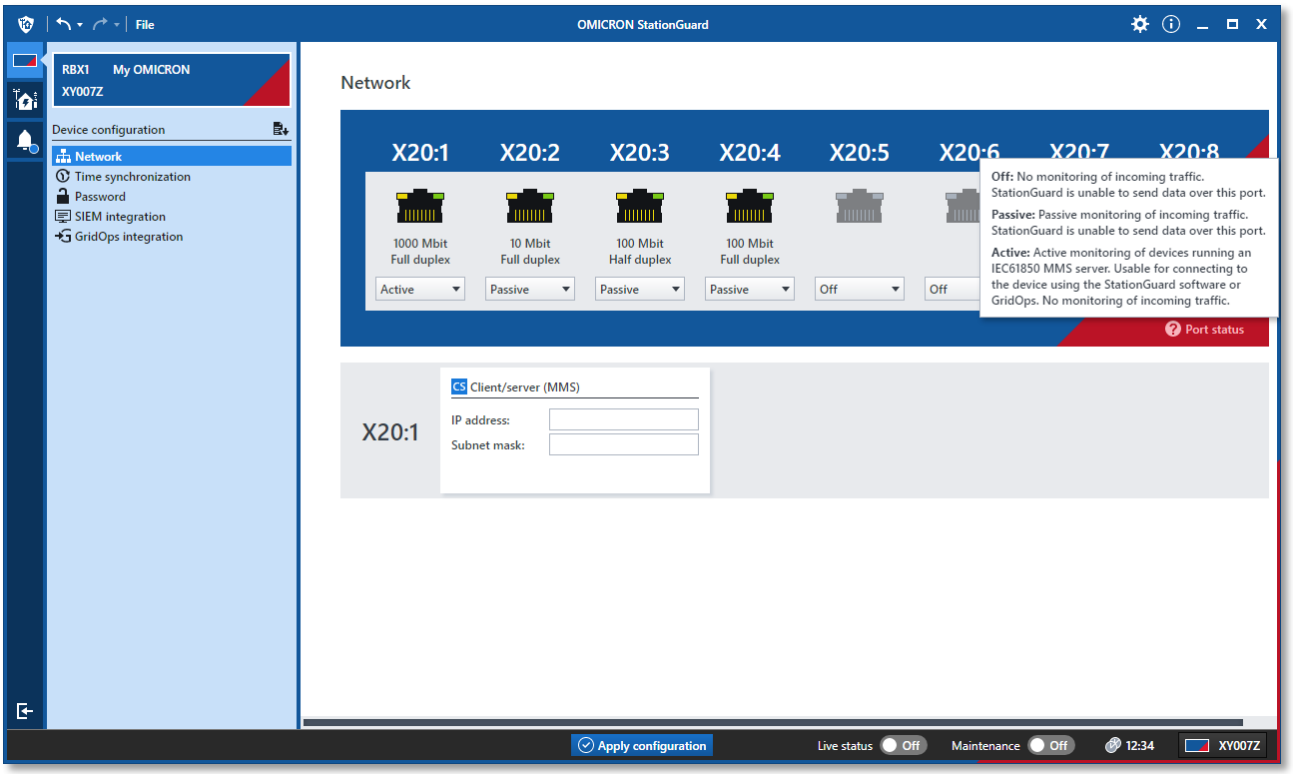
By reading nameplate information, StationGuard 2.20 can actively recognize the devices and their properties. This is an optional feature which needs to be enabled first.
To respond to cyber threats effectively the first step you should take is to thoroughly understand the environment, and the key to a successful OT cybersecurity program is real-time, automated software that can be used to track and identify all assets in real-time.

With active asset discovery, you will be able to use a reliable method to query devices for particular configuration parameters, firmware versions, and other information. Active asset discovery provides a much broader picture of the OT environment and a lot more information about it than passive network monitoring alone.

The IEC 61850 MMS protocol is currently used for live nameplate reading. Unlike SNMP and Web interfaces, MMS is most commonly used in substation automation systems, and the IEC 61850 MMS protocol is without a doubt the most reliable way to obtain nameplate data at substations.
As part of future releases, other protocols will be supported for active identification of devices in the network.

1.7.1 How active asset identification works

You can only use active asset identification by changing the status of a network interface from **Passive** to **Active** and assigning an IP address to the port. Consequently, this port is no longer used for monitoring and only ports in **Passive** status are used to receive traffic from the IDS.



1.7.2 Safety

We have demonstrated that OMICRON's active discovery of IEC 61850 MMS has proven to be safe and effective in hundreds of substations around the world. This can be attributed to the fact that for over a decade the same technology has been used in both StationScout and IEDScout, and the certification of IEDs according to IEC 61850 by some accredited labs is even carried out by using our IEC-61850-MMS stack.
Nameplate data is read only once when the connection to the device is established. There is no subsequent polling so StationGuard's active asset identification places almost no additional load on the network and IEDs. The active connection between StationGuard and the IED will be re-established whenever an IED is restarted, triggering StationGuard to read the nameplate data again. A second read of the device is performed after a firmware update to confirm that the updated asset information is accurately reflected. This is because the firmware update forces the device to reboot as a result of the configuration change made in the update.

1.8 Using the STATION ports to manage StationGuard

In earlier versions of StationGuard, the management interface, NTP, and Syslog connections were only available on the CONTROL port (on the front of the RBX1 platform). With StationGuard 2.20 it is possible to use STATION ports as an additional interface for managing StationGuard and connecting to NTP and Syslog servers, provided that the STATION ports are in **Active** status and have an IP address assigned. Note however that when resetting the StationGuard configuration this IP setting will be reset too and StationGuard will then only be reachable on the CONTROL port.

1.9 Web interface access

You can now also manage a StationGuard sensor via a browser without the need to install the application. The StationGuard web interface offers the same functionality as the installed desktop application.

1.10 Bug fixes and other improvements

NTP time configuration offers more feedback about the synchronization state and possible synchronization problems.

Version 2.10

1 Custom system diagrams

There are new possibilities to visualize your network. StationGuard allows you to create custom system diagrams by adding and renaming sections or moving sections and devices. In addition to the substation structure, you can also visualize your control center or power plant networks according to the Purdue model. Furthermore, a complete visual redesign should help you get a better overview and find the elements you are looking for.

2 Packet captures for alerts

When StationGuard raises an alert, you can download and inspect the network traffic causing it. StationGuard allows you to download network packet captures in PCAP format containing the traffic before, during, and after the alert was detected. The packet captures are stored in the StationGuard (sensor) device independent from the central connection.

3 Suggestions for merging devices

StationGuard allows you to merge multiple devices and supports you by suggesting devices with the same MAC vendor and a similar MAC address. This will help to quickly merge network switches and IEDs which have multiple ports. StationGuard will give you a quick overview of the permissions and alerts of the device to merge.

4 Asset inventory import

StationGuard allows you to import asset inventory information from CSV files which use the defined StationGuard format. This functionality supports adding additional asset details like HW configuration, serial numbers, or firmware versions from external sources and it is also useful to set multiple device names to their correct names according to the plant documentation e.g. the SCADA signal list. StationGuard uses the same format for exporting and importing to keep the device information synchronized with your asset inventory.
You can also import asset details discovered through the companion tool StationScout.

5 Deep packet inspection (DPI) support for additional protocols

We continuously improve our detection engine. Amongst other improvements in detection accuracy, we have now added deep packet inspection support for three additional OT protocols: Profinet, EtherCAT, and CIP (Common Industrial Protocol).

6 Time zone support

In StationGuard, all times are shown in your local time zone by default to allow easier comparison with event lists and log files. It is possible to change to UTC if your other systems are running on UTC.

7 Customer Experience Improvement Program

To help us with our goal to constantly improve the user experience of StationGuard, we have added the possibility to collect usage data anonymously. You can turn off data collection in the privacy dialog shown at startup, where you will also find more details about our Customer Experience Improvement Program (CEIP) and the measures we take to protect your data.

8 Bug fixes and other improvements

- Added a link to the alert details to open a help item showing the alert description.
- In addition to alerts with severity level "Warning" and "Critical", alerts with severity level "Info" are now also forwarded over syslog to be able to see system notifications in central systems like SIEMs.
- Alerts are now also detected if the specified length of a logical link control (LLC) network packet is greater than the actual payload size. Thanks to Matthias Z. from TransnetBW for reporting this issue.
- GOOSE “Not Found” messages are easier to associate with the device that was supposed to send the message.
- The TCP traffic direction is now detected more reliably.
- The assignment of static or dynamic ports is now independent of the detected TCP traffic direction.

Version 2.00

1 New features

1.1 Deep Packet Inspection for more than 300 OT and IT protocols

The unprecedented level of detail for inspecting IEC 61850 protocols has been extended to support Deep Packet Inspection (DPI) on over 300 additional IT and OT protocols. Using DPI, StationGuard not only detects encoding violations, but also, for example, if port numbers of remote connections are hijacked by attackers (port spoofing).

Not just the port numbers, but also the detected applications using these ports, are now part of the StationGuard allow list. When you allow a connection in StationGuard 2.0, the detected application running on that connection will be added to the allow list. If the application using that connection changes, an alert will be raised.

StationGuard can currently detect over 1400 different applications.

1.1.1 Supported OT Protocols

IEC 61850 protocols
IEC 62439-3 PRP and HSR
IEC 60870-5-104, IEC 60870-5-101 and -103 over TCP/IP
DNP3
Modbus TCP and Modbus RTU over TCP
IEC 62056 (DLMS/COSEM)
IEEE C37.118 (Synchrophasor protocol)
IEEE 1703-2012 / ANSI C12.22 (AMI protocol)
IEC 60870-6 (ICCP/TASE.2 - UCA 2.0)
EtherNet/IP
S7 Communication

1.1.2 Most important IT Protocols supported

FTP
HTTP
SSH, HTTPS (application detection, without decryption)
RDP
NTP
SNMP
Netbios (Windows file sharing)
ARP, DHCP
MySQL, MSSQL, PostgreSQL
telnet
ICMP, ICMPv6
RIPv2
SSDP
MDNS
... and many more

1.2 Fine-grained permissions for IEC 60870-5-104

For IEC 60870-5-104, you can set permissions, defining which devices can perform which operations, for example switchgear and other control operations, write, read, and more. The predefined roles for devices have been updated with a useful set of 104 permissions.

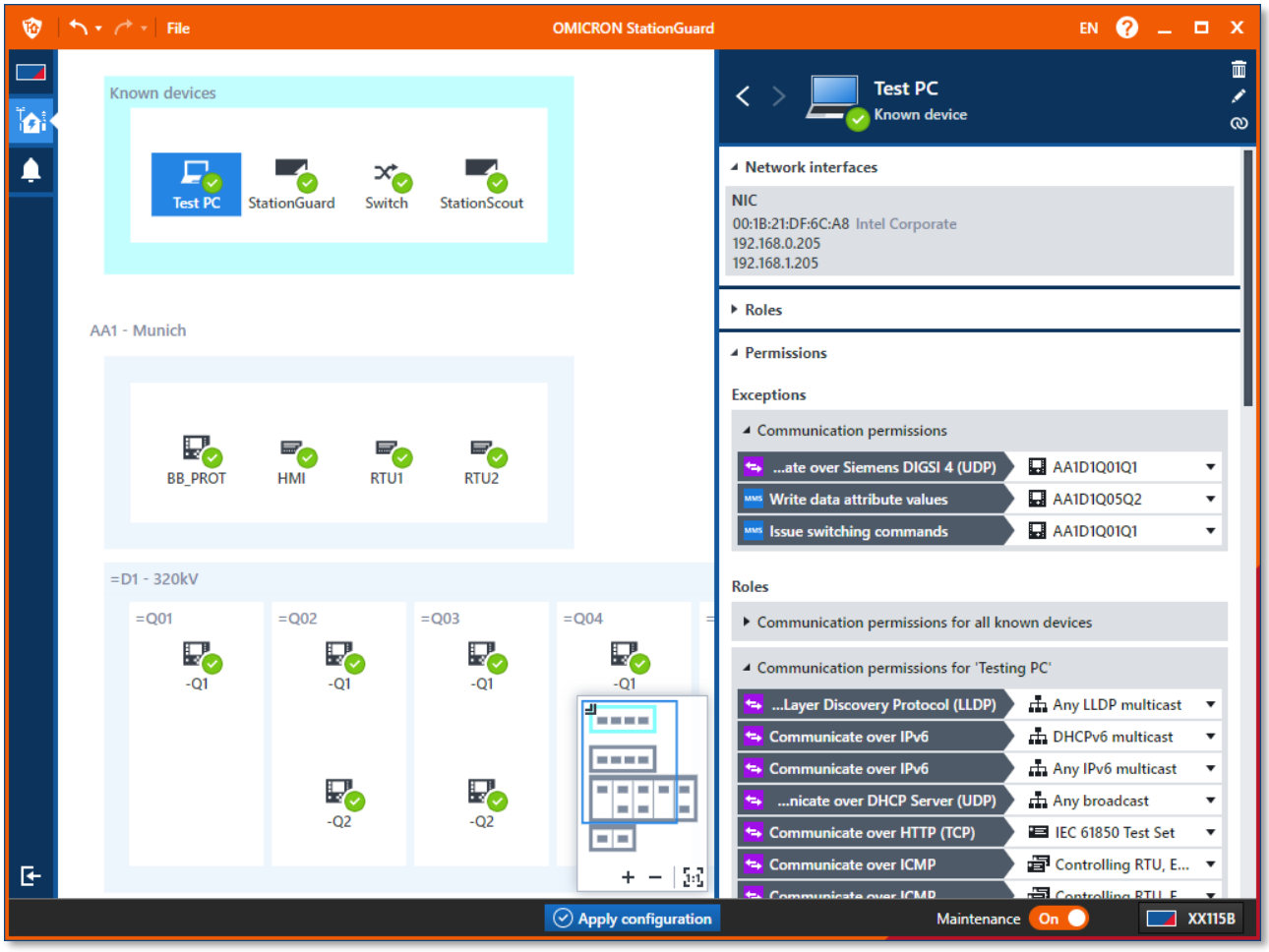
Additional roles for Control Centers, 104 IEDs and Generic IEDs allow common traffic to be covered quickly with predefined permissions.

1.3 Support for commissioning and maintenance

Engineering protocols and IED web interfaces have many known vulnerabilities and new ones are being released all the time. However, these interfaces are needed in the commissioning phase and during routine maintenance. To protect your substations against attacks on these ports, you should generally prohibit engineering activity and only allow it when needed. For this purpose, you can turn on Maintenance in StationGuard. It greatly enhances safety by prohibiting engineering activities during normal operation, while providing a low number of false alarms during maintenance phases.

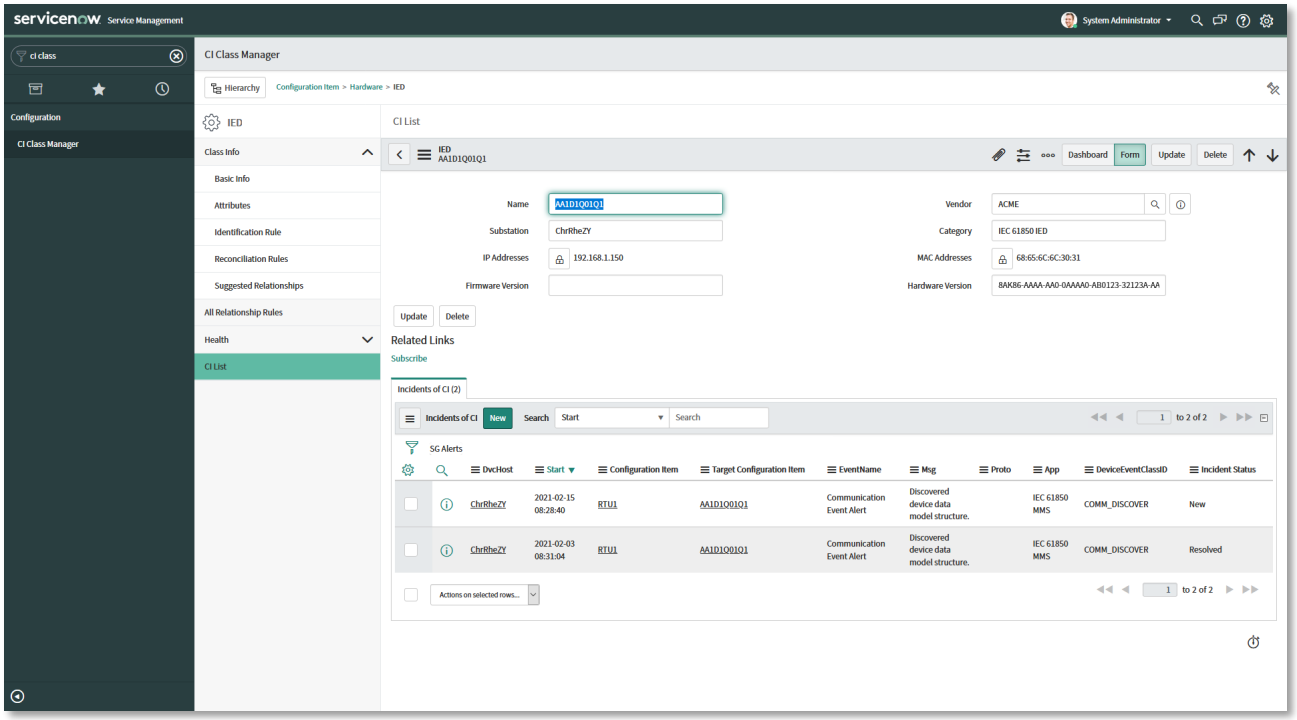
For example, the Engineering PC in the substation must not be active for the majority of time and may, for example, only use a certain engineering protocol or access the web interface of switches while Maintenance is active on StationGuard. If the Engineering PC shows potentially dangerous or suspicious activity, this will always trigger an alert. In contrast to baseline or learning-based IDS, StationGuard supports the different phases in the lifecycle of a substation with high selectivity in the alerts.

Maintenance can be turned on in the StationGuard client software. In future it will also be possible to activate it through binary input contact, for example, wired to a hardware key switch on a panel. The predefined roles for Engineering PCs and Testing PCs already provide a safe set of permissions covering what should only be allowed during maintenance. While Maintenance is on, the StationGuard client application is framed in orange as a warning. All alerts which occurred during maintenance are marked as such to aid assessment.



1.4 ServiceNow integration

The integration of StationGuard alerts into the ServiceNow Service Management platform allows for efficient Incident Management. The StationGuard asset inventory can be imported into the ServiceNow CMDB and the engineers responsible for particular assets or substations can be associated there. This allows for an automatic assignment of ServiceNow tickets to the responsible engineers.



StationGuard also integrates into your Security Information and Event Management Systems (SIEM). Many different SIEM systems are supported by StationGuard, including FortiSIEM©, ArcSight©, IBM QRadar, Splunk.
For Splunk users, a dedicated Splunk App for StationGuard is available.

2 Other improvements

2.1 New alerts and details on protocol encoding issues

StationGuard now provides additional details about protocol parsing issues to determine which parts of the packet are malformed or even manipulated.
In addition, there are new alerts if an outdated SSL/TLS version is in use and if a new IP address is detected for an existing device with a known MAC address.

2.2 Global permissions for GOOSE VLAN alerts

If, due to configuration issues or other restraints, StationGuard does not see VLAN tags in GOOSE messages or if VLAN information is modified by a switch, all GOOSE on the network show the same VLAN issue. If needed, you can now create global permissions to cover VLAN issues in all GOOSE messages on the network.

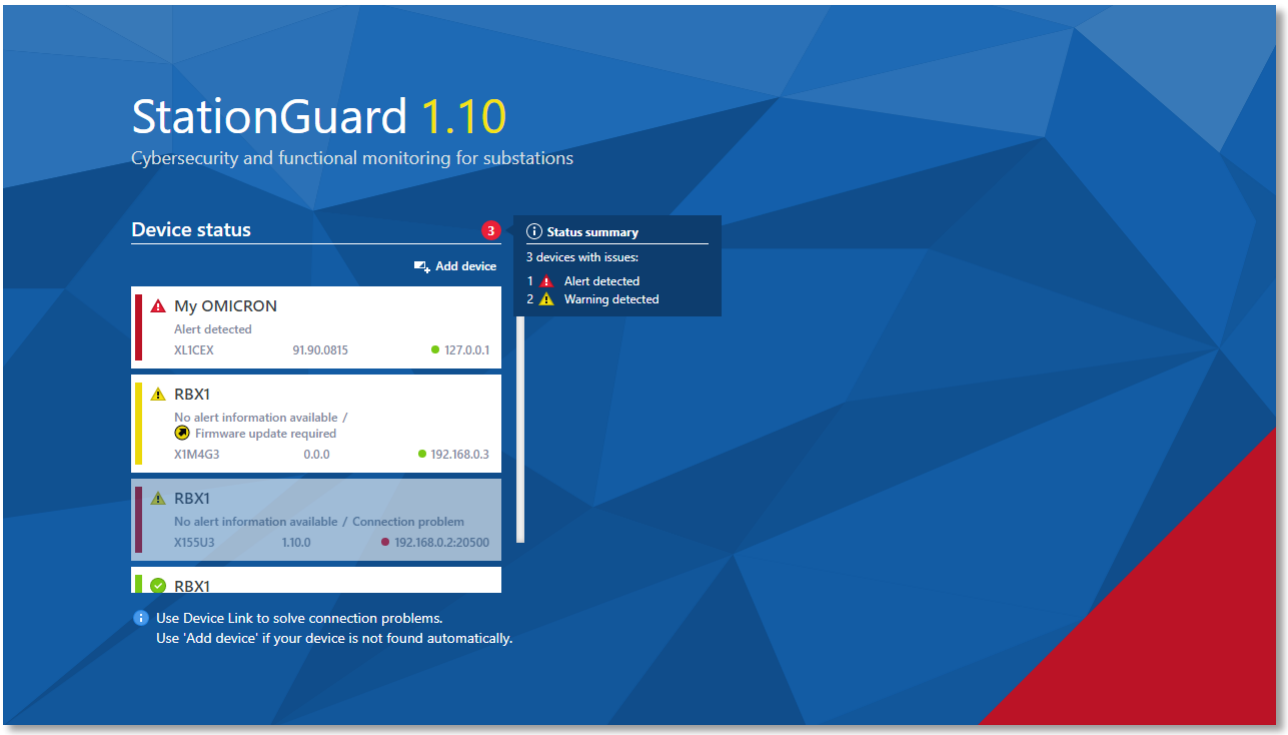
2.3 Stability and performance

StationGuard now creates a backup of the configuration whenever you successfully applied a configuration. If something goes wrong, StationGuard automatically rolls back to the last working configuration.
In addition to the features and improvements listed above, our dedicated team is constantly working on optimizing StationGuard's user experience, performance, and stability.

Version 1.10

1 Central dashboard displaying alert statuses in all substations

A central dashboard is now available, displaying the alert status of all StationGuard devices in all substations. The status of each device is shown in green/yellow/red color based on their alert and connection status. A summary icon shows at a glance how many devices indicate an alert/warning.



2 Export of asset inventory as CSV file

You can now export information about all devices detected by StationGuard into a CSV file and thus document all devices active in the network. This can be useful for security auditing or during the commissioning of a substation.

The asset information exported for each device is a combination of information passively sniffed on the network (MAC, IP addresses) and information from the SCD file, such as IED name, description, hardware version (product ordering code for some vendors), vendor, model, serial number, and firmware version.

The substation automation visualization and testing tool StationScout 1.30 also provides this asset inventory export feature. StationScout uses active interrogation of IEC 61850 devices to read all their nameplate and firmware version information.

StationScout and StationGuard combined thus provide a powerful asset inventory solution.

	A	B	C	D	E	F	G	H	I	J	K
1	Name	Description	Hardware version	Model	Serial	Softwa	Vendor	IP addresses	Origin	MAC addresses	Roles
2	AA1D1Q01Q1	Transformer infeed bay Q01	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.150	system_scd_v3.2	68:65:6C:6C:30:31	IEC 61850 IED
3	AA1D1Q02Q1	Bay control unit Q02 - Starnberg	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.152	system_scd_v3.3	68:65:6C:6C:30:33	IEC 61850 IED
4	AA1D1Q02Q2	Disconnector control unit Q02 - S	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.153	system_scd_v3.3	68:65:6C:6C:30:34	IEC 61850 IED
5	AA1D1Q03Q1	Bay control unit Q03 - Passau	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.154	system_scd_v3.3	68:65:6C:6C:30:35	IEC 61850 IED
6	AA1D1Q03Q2	Disconnector control unit Q03 - P	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.151	system_scd_v3.3	68:65:6C:6C:30:36	IEC 61850 IED
7	AA1D1Q04Q1	Transformer bay Q04	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.155	system_scd_v3.3	68:65:6C:6C:30:37	IEC 61850 IED
8	AA1D1Q05Q2	320kV measuring bay - Merging U		MU 300			ACME	192.168.1.157	system_scd_v3.3	68:65:6C:6C:30:39	IEC 61850 IED
9	AA1H1Q01Q1	Transformer 33kV bay Q01	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.160	system_scd_v3.3	68:65:6C:6C:30:32	IEC 61850 IED
10	AA1H1Q02Q1	Transformer 33kV bay Q02	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.161	system_scd_v3.3	68:65:6C:6C:31:30	IEC 61850 IED
11	BB_PROT	Busbar Protection	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.173	system_scd_v3.3	68:65:6C:6C:30:30	IEC 61850 IED
12	HMI	IHMI		HMI 300			ACME	192.168.1.200	system_scd_v3.3	68:65:6C:6C:31:31	Monitoring RTU
13	PCPQS1	Disturbance data collector		COLLEC 400			ACME	192.168.1.190	system_scd_v3.3		Monitoring RTU
14	RTU1	RTU for transformer bays		RTU 600			ACME	192.168.1.201	system_scd_v3.3	68:65:6C:6C:31:32	Monitoring RTU
15	RTU2	RTU for feeder bays		RTU 600			ACME	192.168.1.202	system_scd_v3.3	68:65:6C:6C:31:33	Monitoring RTU

3 Alert output on binary contacts

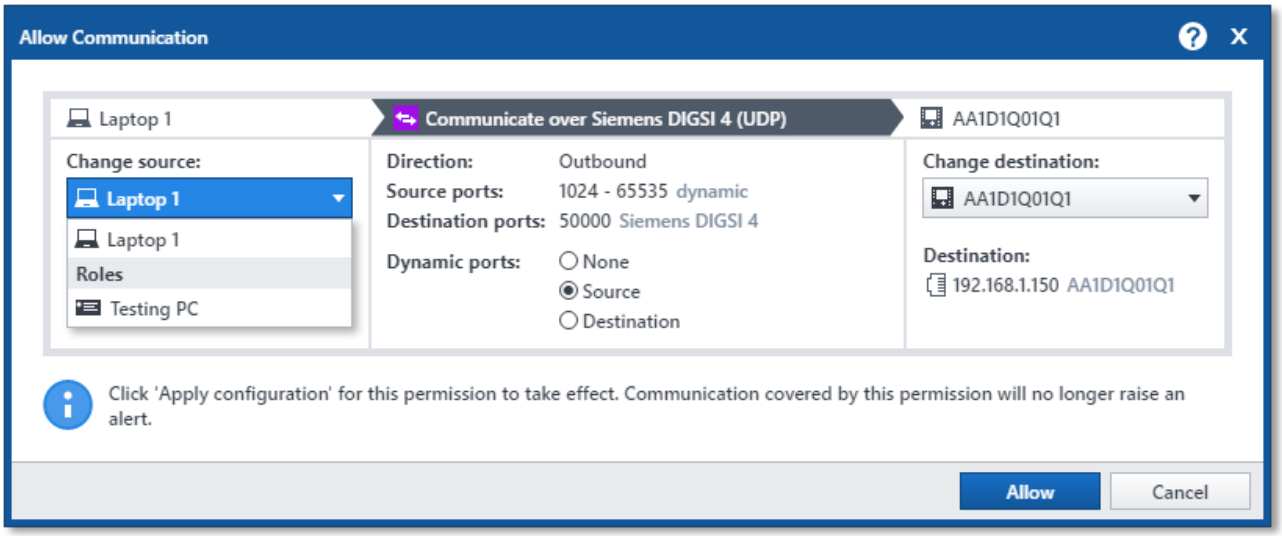
The StationGuard RBX1 hardware platform provides 8 binary output contacts. They are now operated if there are unverified StationGuard alerts or warnings. This facilitates integrating StationGuard alerts into SCADA signal lists by wiring the alert and warning contacts to an RTU.

The status of the binary output contacts is also indicated by the front LEDs of the RBX1 platform.
Alert information can also be sent out by each StationGuard unit over syslog TCP or UDP, where StationGuard is compatible to SIEMs of all major vendors.

4 Other improvements

4.1 Extend predefined roles by adding new permissions to a role

You can now modify the permissions of predefined roles such as “Engineering PC” and “IEC 61850 IED” by adding new permissions. StationGuard shows a dialog box where you can choose if you want to allow certain communication just between two devices or for all devices with these roles.

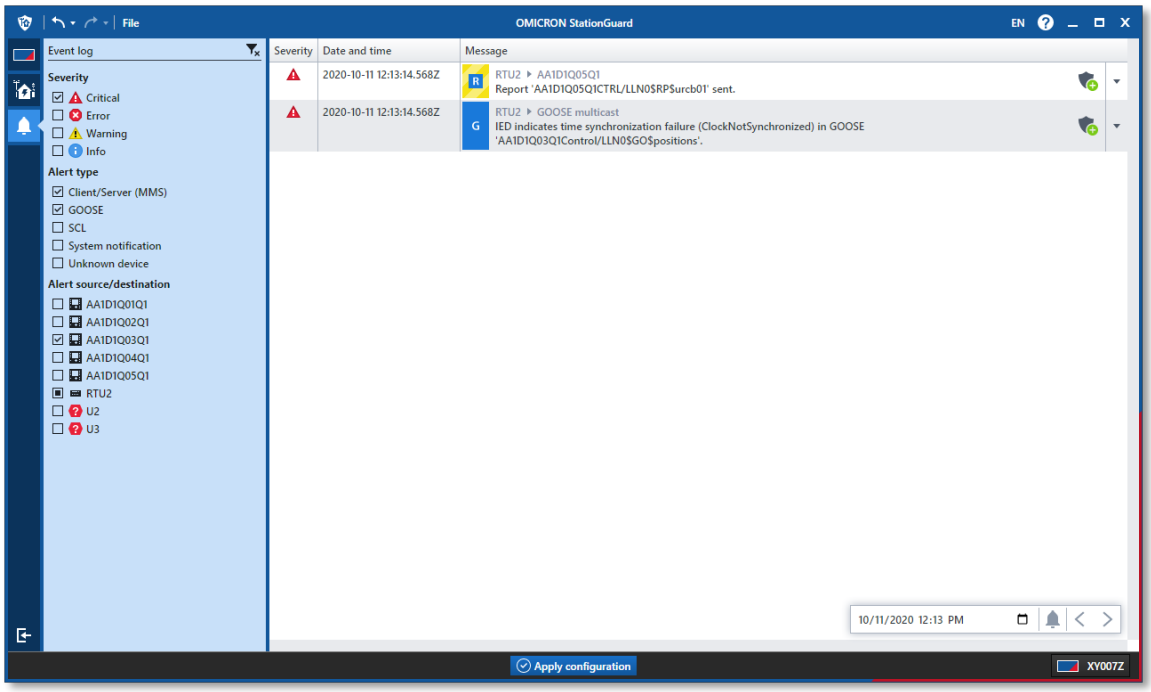


4.2 Indication of device status in the ZeroLine diagram

The device icons in the ZeroLine diagram are now displayed with overlay icons indicating alerts, issues, or their current status.

4.3 View the full event history of a device

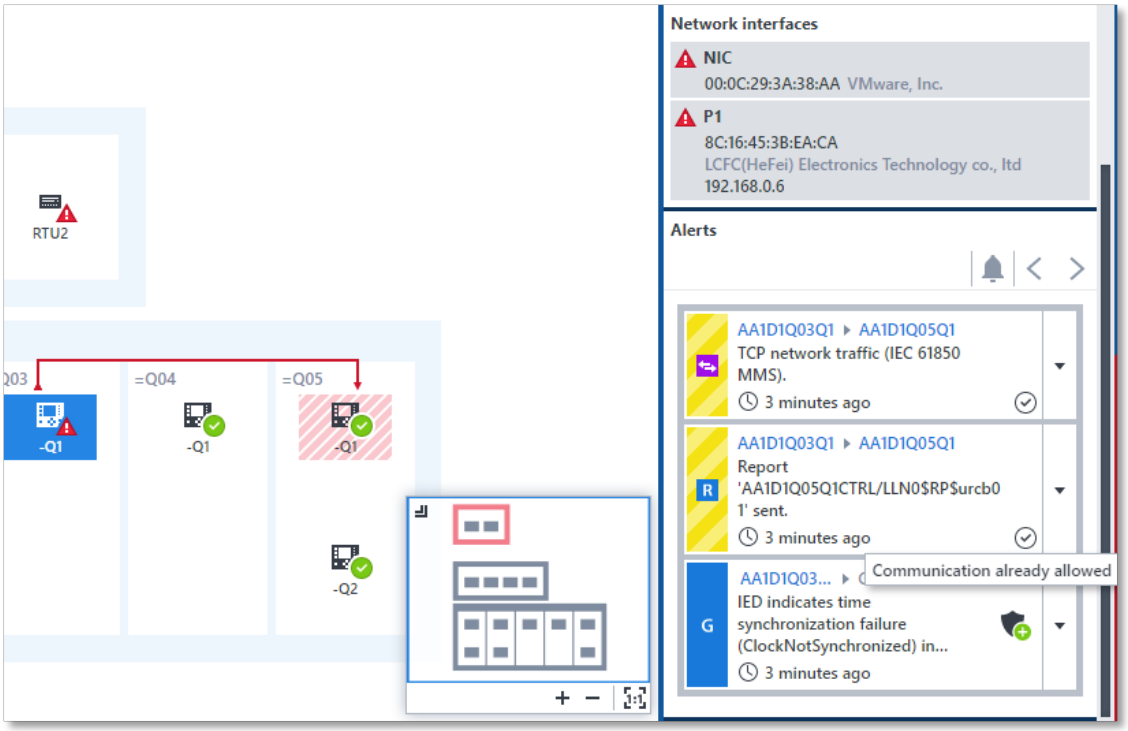
You can now filter the event log by devices to only display alerts and issues linked to this device – either as a source of the alert or as a destination of the communication causing the alert.



4.4 See if alerts are already covered by permissions

When you add a permission or when you add a new role for a device, the effect on all displayed alerts will be shown. If an alert would no longer appear with the current permission/role settings, a checkmark icon is displayed next to the alert.

This also works for alerts listed in the event log.



4.5 Export the event log along with the configuration backup

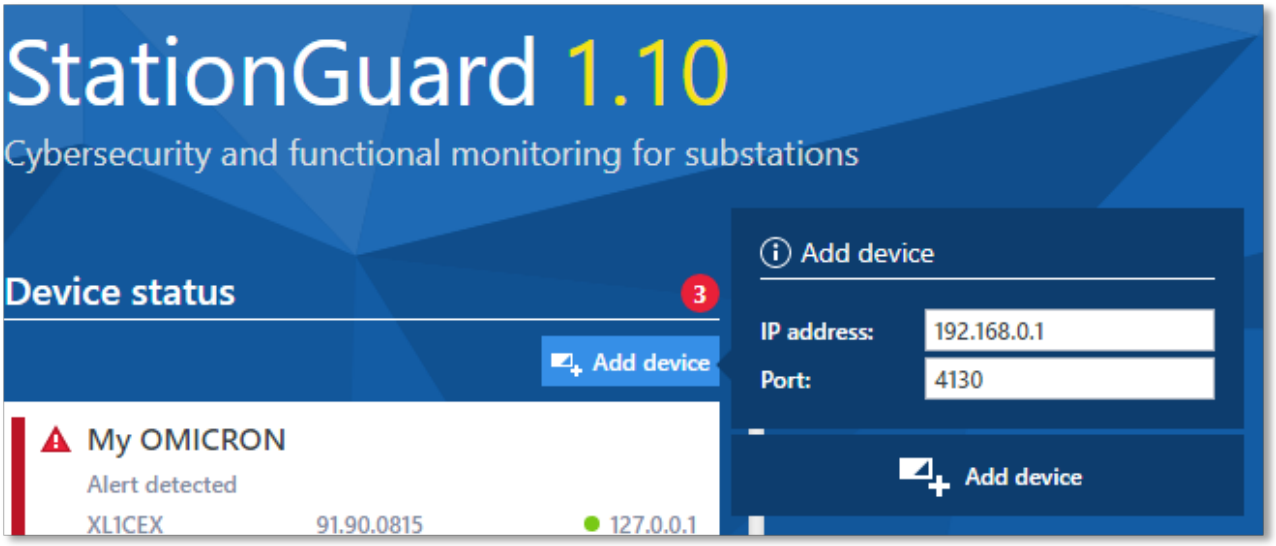
It is now possible to export the event log in the configuration backup. When importing a backed-up configuration you can choose if you want to import only the configuration, or the event log as well.

By importing the event log to a different RBX1 or MBX1 StationGuard device, you can analyze it at a later point, in your office.

4.6 Usage of StationGuard behind Network Address Translations (NAT) and fewer network ports required

Now only one port (TCP 20499) has to be opened in the substation firewall to allow connection using the StationGuard client software – no further settings are necessary. Refer to the StationGuard help for further information about network ports and security.

You can now also connect to devices behind NAT routers.



OMICRON

For more information, additional literature, and detailed contact information of our worldwide offices, please visit our website.

www.omicronenergy.com and www.omicroncybersecurity.com