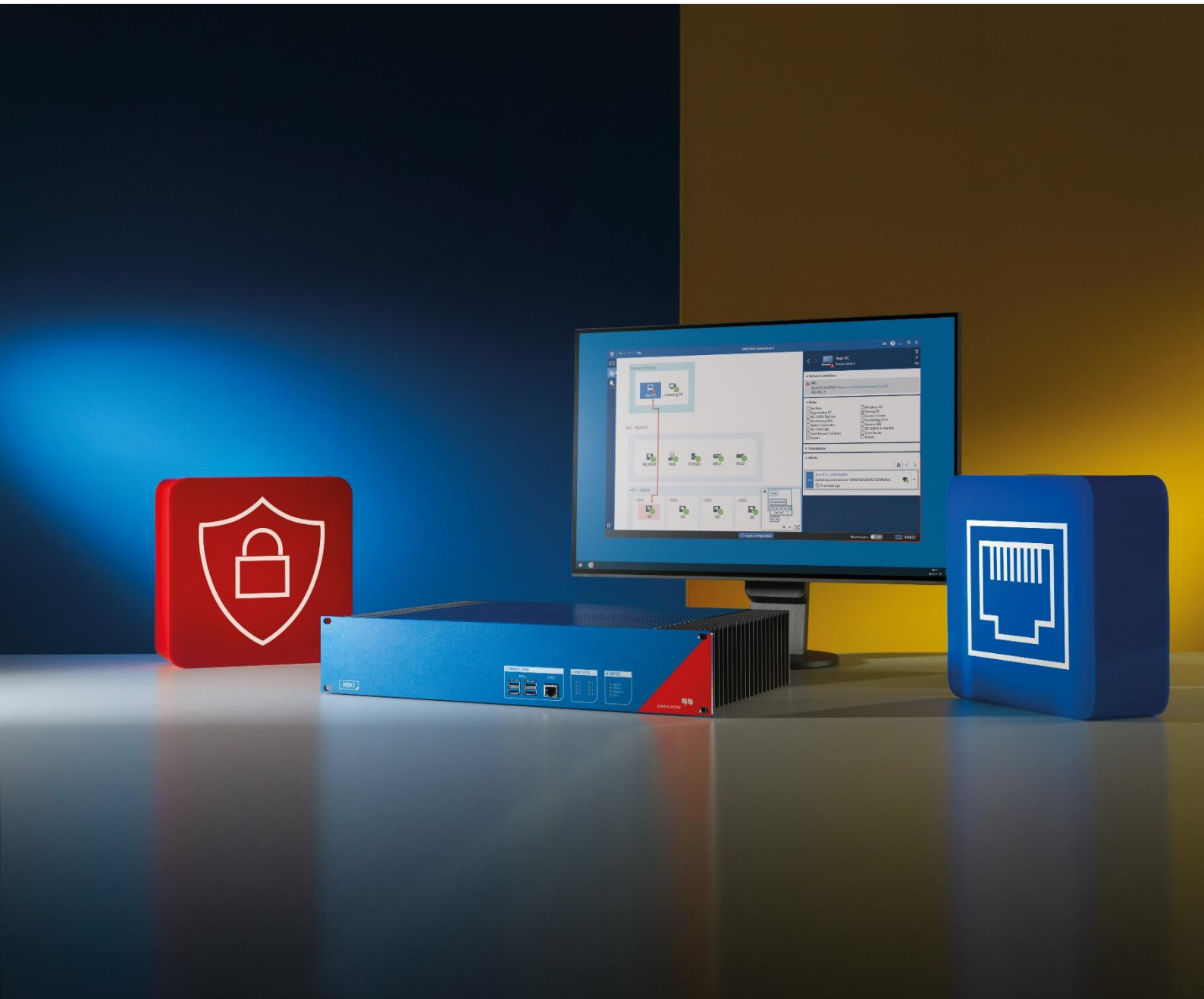
StationGuard and FortiSIEM

Integration Note



Content

1 General Information

1.1 Description

This document describes the configuration process of automatically importing OMICRON StationGuard events into FortiSIEM via inbound integration. FortiSIEM receives all syslogs via TCP and UDP (each via the same ports).

1.2 Rules

There are specific **Rules** provided by StationGuard. Regular updates will increase the number of these rules.
Additionally, custom or general rules that refer **to Event Type Groups** that are also used by StationGuard event types can trigger reactions. Examples of these are successful or unsuccessful brute force attacks on authentication. These rules are also triggered by StationGuard.

1.3 Reports

StationGuard will not issue specific automatic **Reports**. However, such reports can provide results if they match the **Event Type Groups** associated with StationGuard events.

2 Step-by-Step Guide

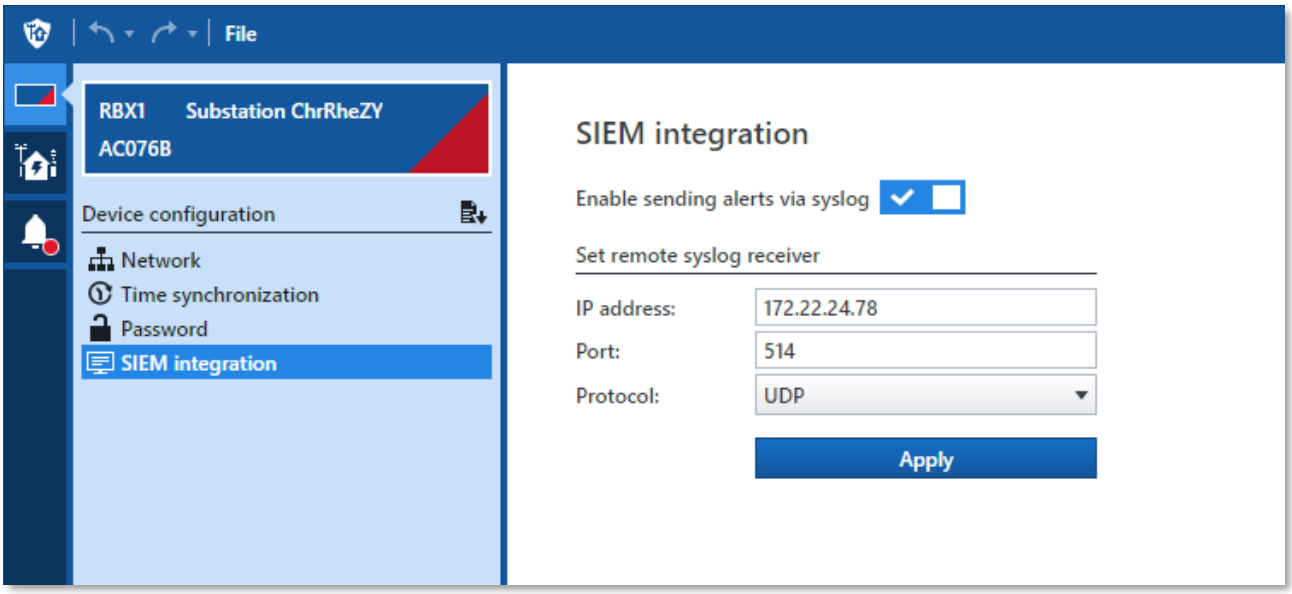
2.1 Configuration of FortiSIEM

Whether a configuration in FortiSIEM is necessary depends on the installed FortiSIEM version:

- For version 6.00 and higher, you do not need any additional steps (fabric-ready).
- If you are still using version 5.00 or lower, please email us: puc.support@omicronenergy.com. We will provide you with all relevant imports.

2.2 Integration of StationGuard in FortiSIEM

1. Access your *Device configuration* in the upper left corner.
2. Click the tab *SIEM integration*.
3. Move the switch *Enable sending alerts via syslog* to on.
4. Type in your IP address and Port number as well as your protocol type.
   - **4a.** If you are using TCP, set port number to 1470
   - **4b.** If you are using UDP, set port number to 514.
5. Press *Apply*.



OMICRON is an international company that works passionately on ideas for making electric power systems safe and reliable. Our pioneering solutions are designed to meet our industry's current and future challenges. We always go the extra mile to empower our customers: we react to their needs, provide extraordinary local support, and share our expertise.

Within the OMICRON group, we research and develop innovative technologies for all fields in electric power systems. When it comes to electrical testing for medium- and high-voltage equipment, protection testing, digital substation testing solutions, and cybersecurity solutions, customers all over the world trust in the accuracy, speed, and quality of our user-friendly solutions.

Founded in 1984, OMICRON draws on their decades of profound expertise in the field of electric power engineering. A dedicated team of more than 900 employees provides solutions with 24/7 support at 25 locations worldwide and serves customers in more than 160 countries.

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

www.omicronenergy.com