

SIEM integration service for cloud-managed LANCOM R&S®Unified Firewalls



Robust security management is essential, especially for larger organizations and managed service providers (MSPs). A centralized Security Information and Event Management (SIEM) system helps organizations detect, analyze, and respond to security threats quickly, preventing damage to business operations.

We invite you to enhance your SIEM with our integration service for cloud-managed LANCOM R&S®Unified Firewalls, ensuring comprehensive detection of attacks on your network infrastructure.

Compliance with market-leading SIEM systems

Our solution drastically simplifies integration with popular SIEM systems like Microsoft Azure Sentinel, Splunk, Enginsight, Wazuh, and Logpoint. The LANCOM Management Cloud (LMC) collects event logs from all managed Unified Firewalls in a network, providing a single endpoint for SIEM systems to retrieve all logs in standard JSON format. This setup ensures quick visibility of network infrastructure attacks, enabling rapid response to threats such as viruses, malware, and DDoS attacks.

Easy setup with the LANCOM SIEM integration service

Our experienced support team will assist you with an uncomplicated integration process:

- 1. Create a ticket with the LANCOM support team:** Open a support ticket and submit the request for the SIEM integration service.
- 2. LANCOM support contacts you:** Our team prepares the necessary configurations for the Unified Firewalls and the LANCOM Management Cloud.
- 3. Receive a security token:** After setup, you will receive a security token for secure communication between the LMC and your SIEM system.
- 4. Rollout of the configuration:** At a time of your choice, you roll out the configuration of your Unified Firewalls via the LMC and update their firmware if needed.
- 5. Configure the interface in your SIEM: If required, we** provide all the necessary information to retrieve and analyze the logs.

Technical prerequisites

- Your LANCOM R&S®Unified Firewalls (all models) are managed in the LANCOM Management Cloud (LMC).
- Minimum firmware version:
 - LCOS FX 10.13.6566 (REL) or higher
 - LCOS FX-I 1.0 or higher
- The firewalls are assigned to a location and configured as a gateway
- You have your Cloud ID or UUID at hand
- You have access to the LMC to update the firewalls and roll out the configurations.

By integrating cloud-managed Unified Firewalls into your SIEM, you can optimize your security processes and safeguard your IT infrastructure. Our integration service ensures a smooth rollout.

Get in touch with us today!

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de | lancom-systems.com

LANCOM, LANCOM Systems, LCOS, LANcommunity and Hyper Integration are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and / or omissions. 07/2024