LANCOM Info paper

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.

Using SIEM with LANCOM R&S®Unified Firewalls in the LMC (OneLog)

In the following we describe, how a SIEM system can be used with LANCOM R&S®Unified Firewalls in the LMC.

Requirements

- → Your LANCOM Unified Firewall must be managed by the LMC
- → The Unified Firewall must be assigned to a site
- → The Unified Firewall must be assigned the role Gateway
- → Access to the LMC to update and roll out the configuration of the Unified Unified Firewall
- → LCOS FX as of version 10.13 Rel (download latest version)
- → Configured and functional SIEM system

The SIEM implementation in the LMC has been successfully tested with the following SIEM systems:

- → Microsoft Sentinel
- → Splunk
- → Enginsight
- → Wazuh
- → Logpoint

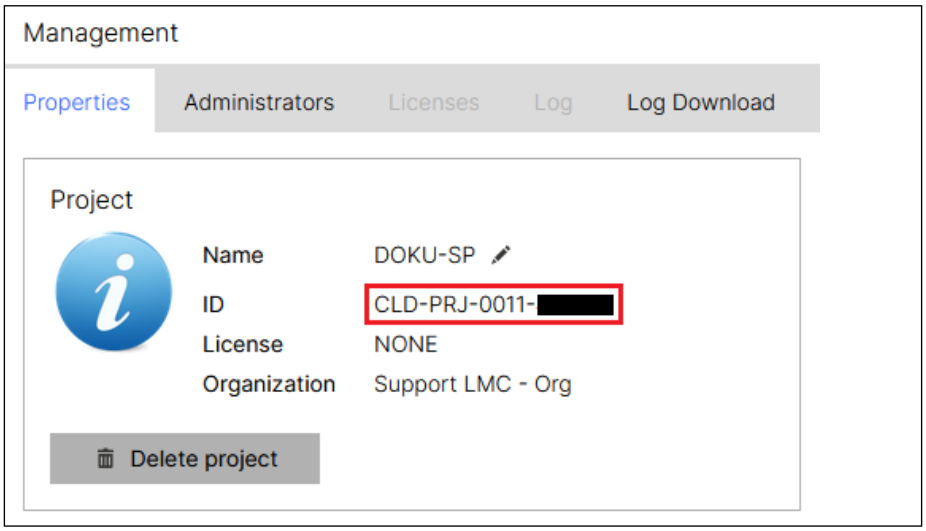
Procedure

1. Activate SIEM support within the LMC

SIEM support is activated in your LMC project by LANCOM Systems at your request.

Send an activation request for SIEM support to LANCOM Support and enclose your Project ID.

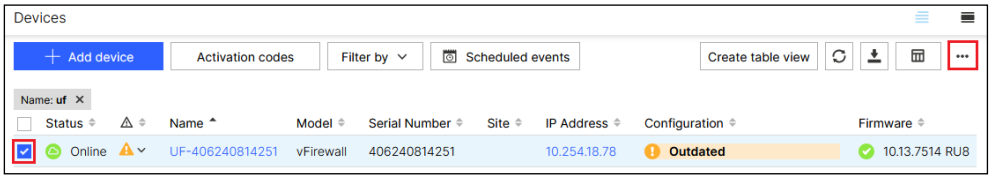
You can find the Project ID in the LMC menu ‚Management → Properties‘.

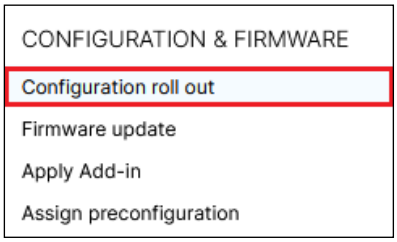


2. Provide IDPS messages from the Unified Firewall for the SIEM system

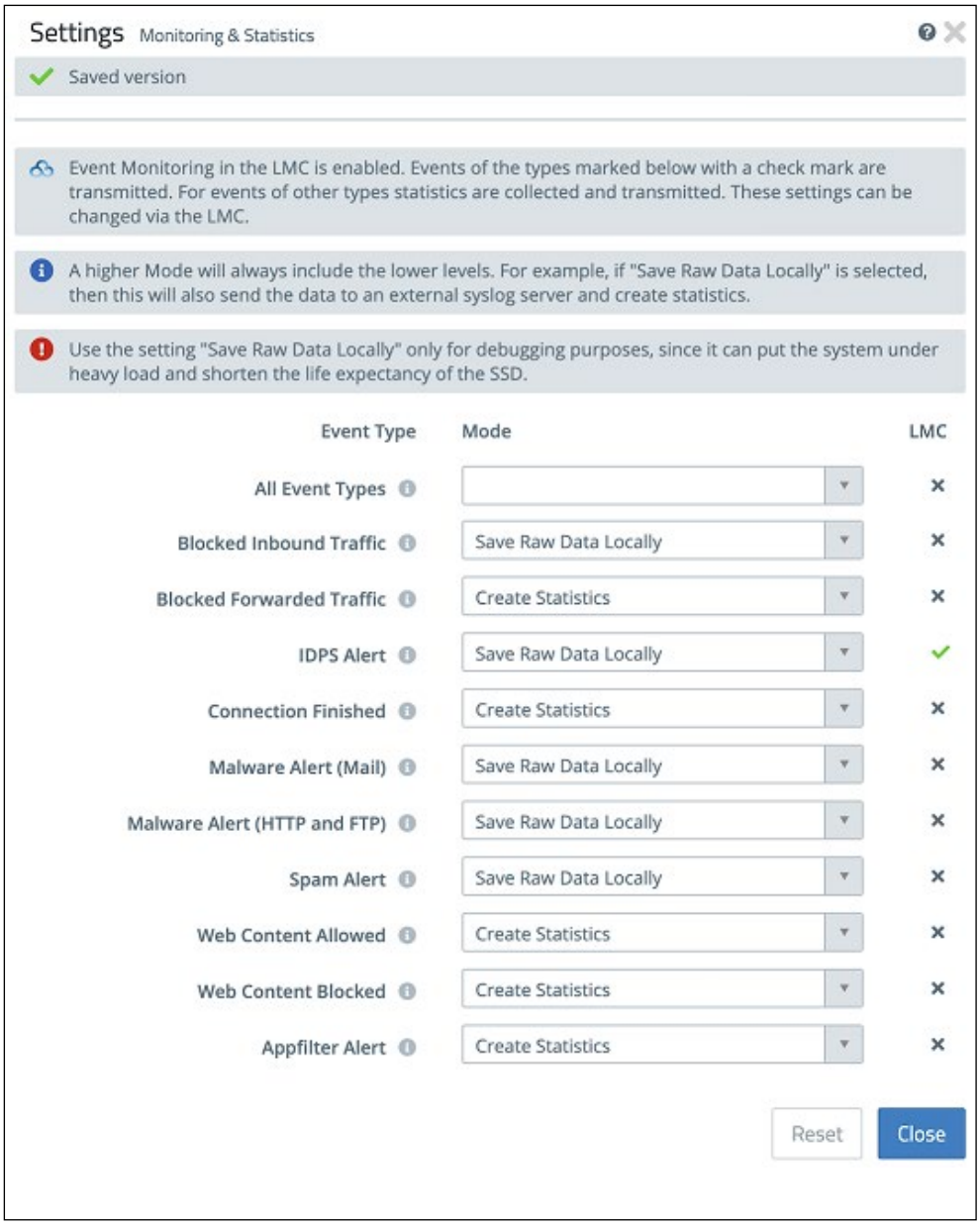
After activating SIEM support the Unified Firewall changes to the state Outdated. Roll out the configuration to the Unified Firewall, so that the IDPS alerts are provided.

As of December 2024 only IDPS alerts are provided. Support for additional logs will be added in future LMC and LCOS FX versions.



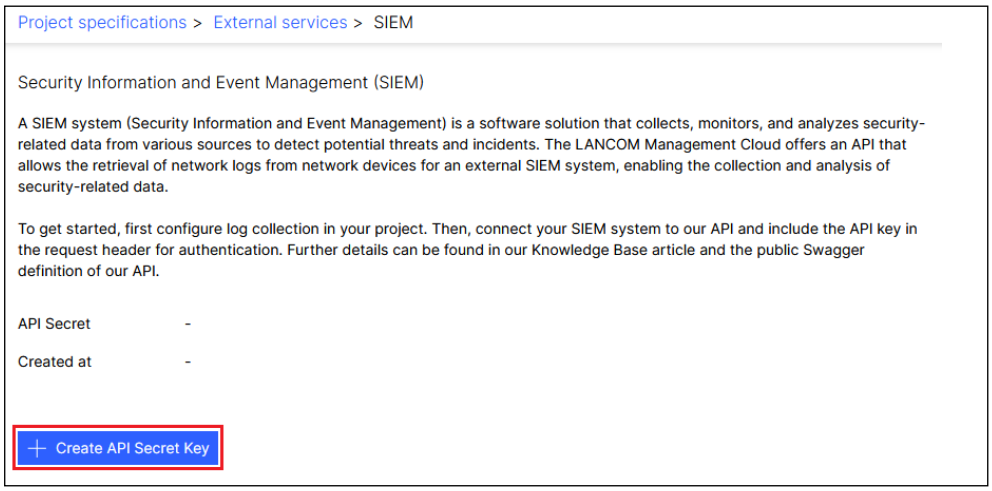


Connect to the Unified Firewall via the WEBconfig tunnel in the LMC and check in the menu ‚Monitoring & Statistics → Settings', if the additional column LMC was rolled out and if the option is active for IDPS Alert.

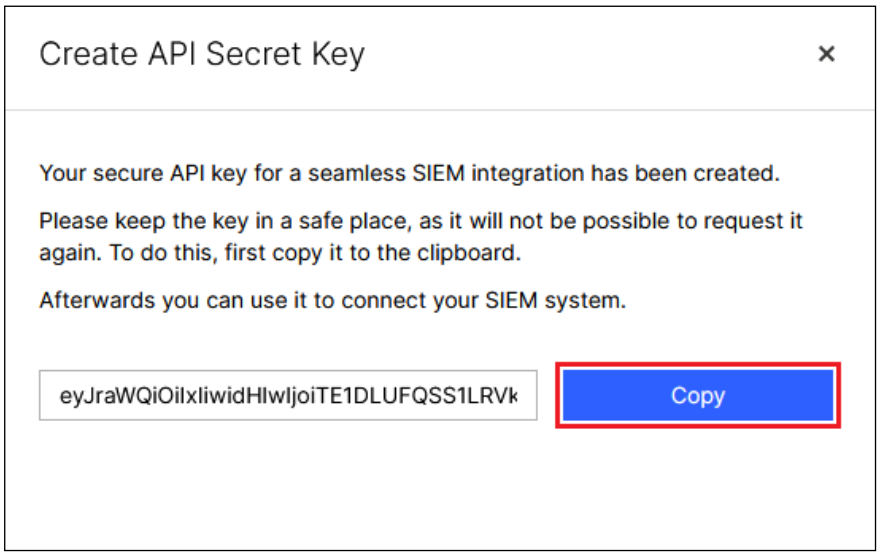


3. Generate a SIEM API Secret in the LMC

In the LMC go to the menu ‚Project specifications → External services → SIEM' and click on ‚Create API Secret Key'.



Copy the Secret Key and save it in a secure location. Enter the Secret Key in your SIEM system afterwards.

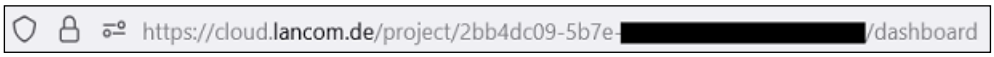


4. Example commands in the SIEM API

You can find the SIEM API documentation (swagger) under the following link: https://cloud.lancom.de/cloud-service-siem/api-docs/

In order to be able to use the SIEM API, you need the UUID of your LMC project as well as the API Secret Key (see step 3).

When you are logged in to your LMC project, you can find the UUID in the adress bar of the browser after project/.



DeviceLogs

With the endpoint DeviceLogs you can read out the device logs for the specified account.

The command must be entered in the following format:

GET /cloud-service-siem/accounts/<UUID of your LMC project>/logs HTTP/1.1
Host: cloud.lancom.de
Authorization: LMC-API-KEY <API Secret Key (see step 3)>

Example test query (without valid account data or Secret Key)

curl --request GET \
--url https://cloud.lancom.de/cloud-service-siem/accounts/ea96d5d0-01f6-498a-b9ec-629be24eae9e/logs \
--header ‚Authorization: LMC-API-KEY eyJraWQiOiIxIiwidHlwIjoiTE1DLUFQSS1LRVkiLCJhbGciOiJIUzI1NiJ9.3zezFHKzCYJICgh-3V1KN0yEe8ITUQEE75DXc-Vv2Dc._93wf35NVk8Q6yt7omWzyohTgW58424tQzRFIPgr111‘ \

Successful result message

{
“startOffset”: 10,
“endOffset”: 109,
“nextOffset”: 110,
“count”: 100,
“deviceLogs”: [
{
“deviceId”: “ea96d5d0-01f6-498a-b9ec-629be24eae9e”,
“accountId”: “ea96d5d0-01f6-498a-b9ec-629be24eae9e”,

“siteId”: “ea96d5d0-01f6-498a-b9ec-629be24eae9e”,
“messageId”: “8bb136e3-0c4e-459e-8cd7-85b8209e2e3b”,
“createdAt”: “2022-12-21T13:17:40.78731Z”,
“receivedAt”: “2022-12-21T13:17:40.78731Z”,
“rawMessage”: “IDPS: Malicious message detected [Classification:] [Severity: 3] [Signature Id: 5000000] [Action: allowed] [Source: 10.10.10.20:0] [Destination: 8.8.76.5:0]”,
“severity”: “3”,
“additionalProperties”: {
“category”: “IDPS”,
“idps_event_type”: “alert”,
“signature”: “5000000”,
“idps_category”: “”,
“source_ip”: “10.10.10.20”,
“source_port”: “0”,
“destination_ip”: “8.8.76.5”,
“destination_port”: “0”,
“action”: “allowed”
}
}
],
“_links”: {
“self”: “https://cloud.lancom.de/cloud-service-siem/accounts/ea96d5d0-01f6-498a-b9ec-629be24eae9e/logs?offset=1&limit=100”,
“next”: “https://cloud.lancom.de/cloud-service-siem/accounts/ea96d5d0-01f6-498a-b9ec-629be24eae9e/logs?offset=101&limit=100”
}
}

Offsets

With the endpoint Offsets you can read out the number of the first logfile and the next unread logfile as well as the offset limit for the specified account.

The command must be entered in the following format:
GET /cloud-service-siem/accounts/<UUID Ihres LMC-Projekts>/offsets HTTP/1.1
Host: cloud.lancom.de
Authorization: LMC-API-KEY <API Secret Key (see step 3)>

Example test query (without valid account data or Secret Key)

```
curl --request GET \
--url https://cloud.lancom.de/cloud-service-siem/accounts/30995a43-3705-439a-9c2c-da1331bb5106/offsets \
--header 'Authorization: LMC-API-KEY eyJraWQiOiIxIiwidHlwIjoiTE1DLUFQSS1LRVkiLCJhbGciOiJIUzI1NiJ9.3zezFHKzCYJICgh-3V1KN0yEe8ITUQEE75DXc-Vv2Dc._93wf35NVk8Q6yt7omWzyohTgW58424tQzRFIP11111' \
```

Successful result message

```
{
  "startMinOffset": 0,
  "nextUnreadOffset": 99,
  "endMaxOffset": 100
}
```

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