# Webhooks

**A modern IT infrastructure is a mosaic of multiple systems for different application areas. Cloud applications, such as the LANCOM Management Cloud, can be part of this by acting as control centers to manage the network components.**

**To reduce complexity, on the one hand a central monitoring and alerting system is often used as an aggregator, which allows the administrator to bundle notifications of events in these different systems in one interface. The advantage of such a system is that the administrator can receive and react to incident notifications even faster - regardless of the application area (network, mailing, telephony, etc.).**

**On the other hand, cross-system workflows ensure that processes run more leanly and thus more efficiently. The prerequisite for this is the connection of the systems involved "on the same language".**

**In these cases, webhooks are particularly practical. This techpaper explains how webhooks work and how they are implemented in the LANCOM Management Cloud (LMC).**

## Efficient communication between systems with webhooks

The term "webhook" is composed of the words web, i.e. HTTP-based communication, and hook. In programming, hook refers to an interface that can be used to intercept events.

Webhooks are often used in the development of web applications and APIs to simplify and speed up communication between two applications by automating real-time notification of events or triggering downstream processes. This involves sending a notification in the form of an HTTP post to the connected system when certain events predefined by the requestor occur.

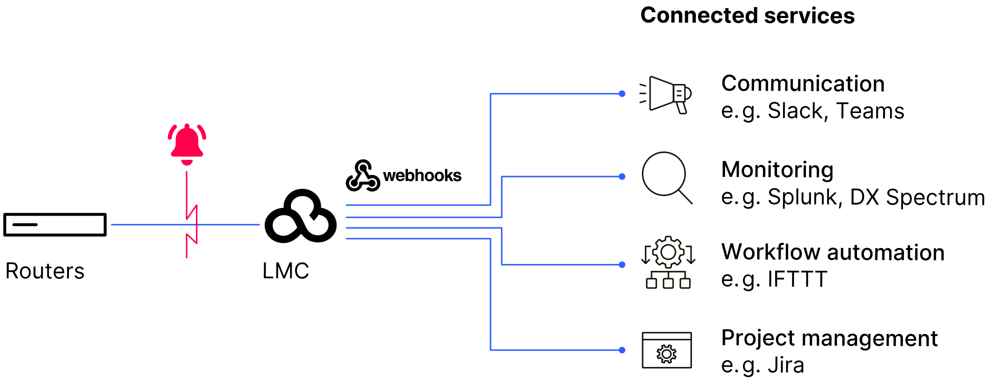


Figure 1:
Webhooks in the LMC with
exemplary connected services

The requestor / user defines himself which contents (body) the event notification should contain. Normally, the webhook body contains some information to identify the events, such as a unique ID, the project name, the actual notification as well as the event date etc..

**Example of a webhook body**

```
{
“alertId”: “UUID”,
“projectName”: “string”,
“accountId”: “UUID”,
“title”: “string”,
“text”: “string”,
“createdAt”: “date”,
“stateUpdatedAt”: “date”,
“state”: “string”,
}
```

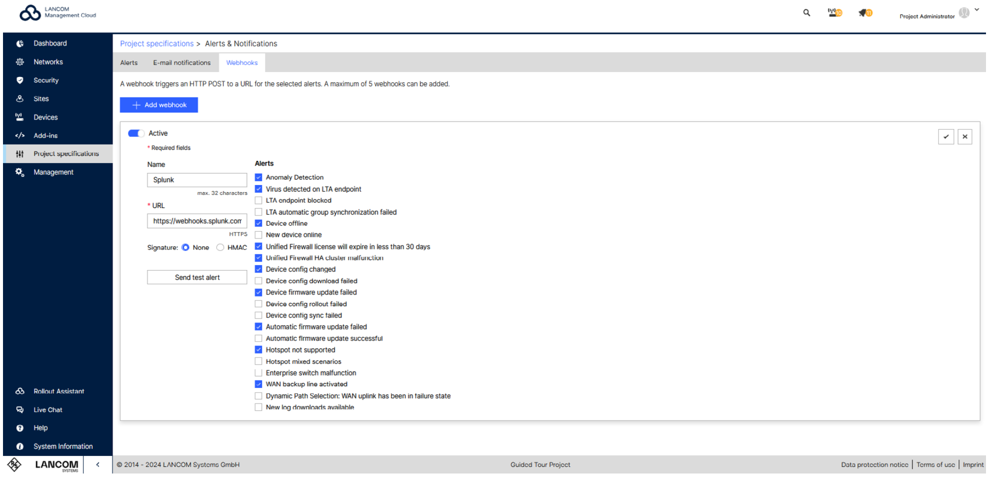
Since the webhook is based on HTTP, it is possible to secure the communication using standard technologies:

→ Source IP address filtering
→ HTTP basic authentication
→ HTTP request is signed using HMAC
→ Mutual TLS authentication

## Webhooks in the LANCOM Management Cloud

By using Webhook technology, the LANCOM Management Cloud (LMC) is able to communicate with a wide variety of applications and Web services. Some systems offer the option of mapping the content of the Webhook call to their internal data structure, making it possible to aggregate events. In the Splunk log, monitoring and reporting platform, for example, data from a wide variety of sources can be made available to users.

The LMC offers the possibility to set up to five external reception points for the webhook notifications. These reception points can be configured under ‘Project specifications > Alerts & Notifications > Webhooks’.



Project specifications > Alerts & Notifications

A webhook triggers an HTTP POST to a URL for the selected alerts. A maximum of 5 webhooks can be added.

Active

* Required fields

Name: Splunk (max. 32 characters)

* URL: https://webhooks.splunk.com (HTTPS)

Signature: ● None ○ HMAC

Alerts
- ☑ Anomaly Detection
- ☑ Virus detected on LTA endpoint
- □ LTA endpoint blocked
- □ LTA automatic group synchronization failed
- ☑ Device offline
- □ New device online
- ☑ Unified Firewall license will expire in less than 30 days
- ☑ Unified Firewall HA cluster malfunction
- ☑ Device config changed
- □ Device config download failed
- ☑ Device firmware update failed
- □ Device config rollout failed
- □ Device config sync failed
- ☑ Automatic firmware update failed
- □ Automatic firmware update successful
- ☑ Hotspot not supported
- □ Hotspot mixed scenarios
- □ Enterprise switch malfunction
- ☑ WAN backup line activated
- □ Dynamic Path Selection: WAN uplink has been in failure state
- □ New log downloads available

© 2014 - 2024 LANCOM Systems GmbH

Figure 2:
Adding and configuring webhooks in the LMC

For each webhook, it is possible to specify which notification should be delivered to the receiving service connected to it.

For example, if a device is detected as not connected to the LMC, the LMC generates a new notification alarm. Thereupon the LMC sends a message to each webhook with the above body.

The webhook calls follow the same pattern as sending email notifications:
→ a call is made when the event occurs (e.g. first device offline).
→ a call is made when the state of the system has deteriorated (e.g. further devices are offline)
→ a call is made when the alarm is resolved (e.g. all devices are back online)

The LMC offers the possibility to test the correct configuration of the webhook. It is even possible to trigger a test call directly on the configuration page.

## Secure end-to-end communication

To guarantee the authenticity of the webhook, the entire HTTP request can be signed with HMAC. The signature is then transmitted in the HTTP header. The sender and receiver know the secret key and thus verify the authenticity of the signature.

HMAC is a hash-based message authentication code that acts as a kind of checking authority to determine whether the notification has been tampered with in the communication path. In this way, man-in-the-middle (MITM) attacks can be avoided. For this purpose, the secret key can be specified in the LMC, which must be entered once to receive the webhooks in the target application.

## Conclusion

Thanks to the flexible deployment options for webhooks, it is possible to forward collected and automated notifications from the LANCOM Management Cloud to any system that offers communication via webhook. This means that all changes — be they malfunctions, required license and firmware updates, or changed device configurations — can be kept track of at all times, and processes can be triggered automatically without having to monitor processes themselves. Monitoring, troubleshooting and commissioning are possible individually and with little effort thanks to the flexible deployment options for webhooks.

LANCOM SYSTEMS

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