

Release Notes

LMC Software Release 1.00.177.0

Table of contents

03	1. Preface
03	2. Important notes
04	3. New features, changes, and history
04	LANCOM Management Cloud 1.00.176.0 / 11.09.2024 → More efficiency for hybrid teams thanks to LTA Multi-Domain Access
05	LANCOM Management Cloud 1.00.176.0 / 11.09.2024 → More convenience and security for configuration comparison
07	LANCOM Management Cloud 1.00.175.0 / 20.08.2024 → Integration of external hotspot providers
09	LANCOM Management Cloud 1.00.174.0 / 06.08.2024 → Improved overview with color optimization of the device table
10	LANCOM Management Cloud 1.00.173.0 / 09.07.2024 → SIEM integration service for cloud-managed LANCOM R&S®Unified Firewalls
12	LANCOM Management Cloud 1.00.172.0 / 18.06.2024 → Full transparency before rollout thanks to configuration comparison
13	LANCOM Management Cloud 1.00.170.0 / 15.05.2024 → Trusted Internet Access: Mobile working as secure as in the office
14	LANCOM Management Cloud 1.00.169.0 / 16.04.2024 → Customized device overview using savable table views
15	LANCOM Management Cloud 1.00.168.0 / 26.03.2024 → More comfort with multi-language support for the cloud-managed hotspot
17	LANCOM Management Cloud 1.00.167.0 / 05.03.2024 → Precise troubleshooting with direct links to the source of the error



- 19 **LANCOM Management Cloud 1.00.166.0 / 13.02.2024**
→ Easy-to-view site assignment of a network
- 21 **LANCOM Management Cloud 1.00.165.0 / 23.01.2024**
→ Central administrator management at organization level
- 23 **LANCOM Management Cloud 1.00.164.0 / 02.01.2024**
→ A look back at 2023
- 24 **LANCOM Management Cloud 1.00.163.0 / 12.12.2023**
→ Your direct access to cloud-managed VPN
- 26 **LANCOM Management Cloud 1.00.162.0 / 22.11.2023**
→ LANCOM Trusted Access – Cloud-managed secure network access
- 28 **LANCOM Management Cloud 1.00.161.0 / 31.10.2023**
→ Refresh of the LANCOM Management Cloud user interface
- 30 **LANCOM Management Cloud 1.00.160.0 / 13.10.2023**
→ Simplified management and more overview for switch stacks
- 31 **LANCOM Management Cloud 1.00.158.0 / 29.08.2023**
→ Centralized port templates for optimized switch rollout
- 32 **LANCOM Management Cloud 1.00.157.0 / 09.08.2023**
→ Inspiration for your projects: Discover the new LMC website
- 33 **LANCOM Management Cloud 1.00.156.0 / 18.07.2023**
→ Network extension & device setups within minutes
- 34 **LANCOM Management Cloud 1.00.155.0 / 27.06.2023**
→ Efficient, automated workflows with webhooks
- 35 **LANCOM Management Cloud 1.00.154.0 / 07.06.2023**
- 36 **LANCOM Management Cloud 1.00.153.0 / 17.05.2023**
→ Two clicks to optimized Wi-Fi installations via the LMC
- 37 **LANCOM Management Cloud 1.00.152.0 / 25.04.2023**
→ Wi-Fi optimization with LANCOM Active Radio Control 2.0
- 39 **LANCOM Management Cloud 1.00.151.0 / 04.04.2023**
→ Maximum data, failure, and access protection with the LMC
- 40 **LANCOM Management Cloud 1.00.150.0 / 14.03.2023**
→ Secure WEBconfig access and CLI tunnel for GS-2000 switches
- 41 **LANCOM Management Cloud 1.00.149.0 / 21.02.2023**
→ Accelerated add-in extension with new developer mode
- 43 **LANCOM Management Cloud 1.00.148.0 / 31.01.2023**
→ Advanced security features in the LANCOM Management Cloud

- 45 **4. History of incompatible API changes**

- 46 **5. General advice**
→ Disclaimer

1. Preface

As an intelligent network management and monitoring system, the LANCOM Management Cloud automates and centralizes the entire network architecture in terms of its WAN, LAN, WLAN, and Security. Even complex networking scenarios with a large number of network components can be easily controlled, managed, and optimized with the LMC, saving valuable resources such as money and time.

The LMC Public Cloud is available at <https://cloud.lancom.de> and is regularly updated with new features and bug fixes.

This document describes the new features of the LMC Software Release 1.00.177.0, as well as the improvements since the previous version.

LANCOM Systems GmbH does not assume any warranty or liability for software not developed or produced by LANCOM Systems GmbH or distributed under the name of LANCOM Systems GmbH, in particular not for shareware and other third-party software.

2. Important notes

To ensure continued smooth operation with the LANCOM Management Cloud, LANCOM devices with an old firmware version must be updated to a newer version.

The following firmware versions are the minimum requirement:

- LCOS 10.12.0147 SU3
- LCOS FX 10.4
- LCOS LX 5.20 Rel
- LCOS SX 3.30.0417 RU3

To use all the functions of the LANCOM Management Cloud, we recommend using the latest release version.

A list of the URLs and ports via which LANCOM devices communicate with the LANCOM Management Cloud can be found in [this Knowledge Base document](#).

3. New features, changes, and history

LANCOM Management Cloud 1.00.176.0 / 11.09.2024

More efficiency for hybrid teams thanks to LTA Multi-Domain Access

LANCOM Trusted Access (LTA) with Multi-Domain Access provides hybrid, decentralized teams with secure and seamless access to internal network segments. This significantly facilitates collaboration with external employees. Through external login domains, they receive temporary, secure access to the necessary network areas to retrieve relevant information for their tasks. User accounts of additional domains must be enabled in the Identity Provider (IdP), allowing the LTA client to permit logins from additional external domain users. The logged-in users can be viewed via Dashboards > LANCOM Trusted Access.

Improvements

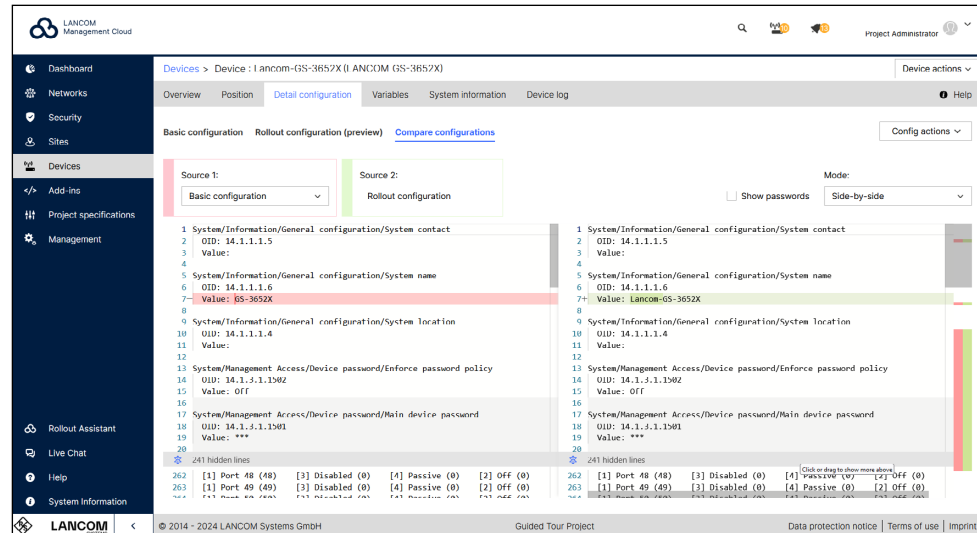
- Improvement on handling of not found (deep) links and URLs pointing to certain items
- Improved visual differentiation between official and custom authorities / roles
- Added an explicit confirmation on switching the central site role of a VPN network to a different site

Bug fixes

- A problem with the sorting in the firmware dialog is fixed
- A problem with the device status widget for new project was fixed
- Update of the logo and background for the hotspot

LANCOM Management Cloud 1.00.176.0 / 11.09.2024

More convenience and security for configuration comparison



Customize the configuration comparison to suit your preferences: Changes between two configurations are highlighted not only with row markers but also in content, making it easier to focus. Simultaneous horizontal scrolling of both configurations and the ability to hide irrelevant rows improve the overall overview. You control the appearance of your interface: Hidden sections can be fully revealed with a click or by dragging and dropping them back in row by row. Additionally, your preferred display format – side by side, stacked, or inline – is saved for future access. To protect against unauthorized access, changed passwords are no longer displayed by default. Discover the new features of the configuration comparison by clicking on a router, access point, or switch under “Detail configuration.”

Improvements

- Only Public LMC: Implementation of secure access to the LMC by LANCOM Support for customer support (ISM-240205)
- Uniform behavior in the device table when the mouse pointer is moved over an entry

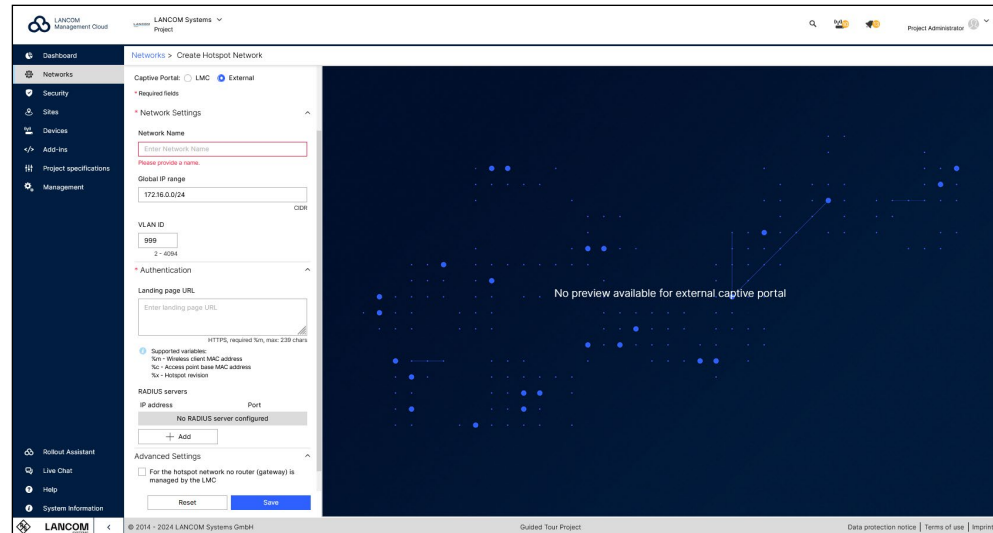
Bug fixes

- Corrected country selection for changing an address in the account management
- A problem with the website import when setting a standard DHCP gateway has been fixed.

- A problem with the display of new text content in the device overview has been fixed.
- Automatically created device passwords with a length of 15 characters sometimes did not match the password restrictions of the device. The algorithm now always creates valid passwords.
- The antenna gain is now set correctly in the SD-WLAN configuration for LCOS LX-based access points.
- The syslog is now correctly deactivated on switches of the SX series if this has been configured in the LMC.
- The network overview page now remembers the selected settings for the page length.
- The behavior after editing and deleting a variable has been corrected.
- The Polish translation of the hotspot has been revised.
- After clicking on an entry in the device compact view, the compact view is no longer exited.

LANCOM Management Cloud 1.00.175.0 / 20.08.2024

Integration of external hotspot providers



For more flexibility in hotspot provision via the LMC, you can now also integrate third-party hotspots that offer RADIUS interfaces for authentication and authorization. The centralized management via the LMC allows you to ensure uniform security policies for the entire network. To do this, create the hotspot under Networks > Add network > Hotspot network and select “External” for Captive Portal. In addition to the network name and IP range, enter the external URL and up to three RADIUS servers. Simply assign the new hotspot network to the desired locations. This way, hotspot users are forwarded directly to the portal of the external hotspot provider when they dial in.

Improvements

- The ‘Config Diff’ feature is leaving beta status.
- Add-in names can now be 64 characters long.
- Passwords for devices that are configured globally in the project settings can now be up to 30 characters long. New, random, individual passwords will use this length by default.

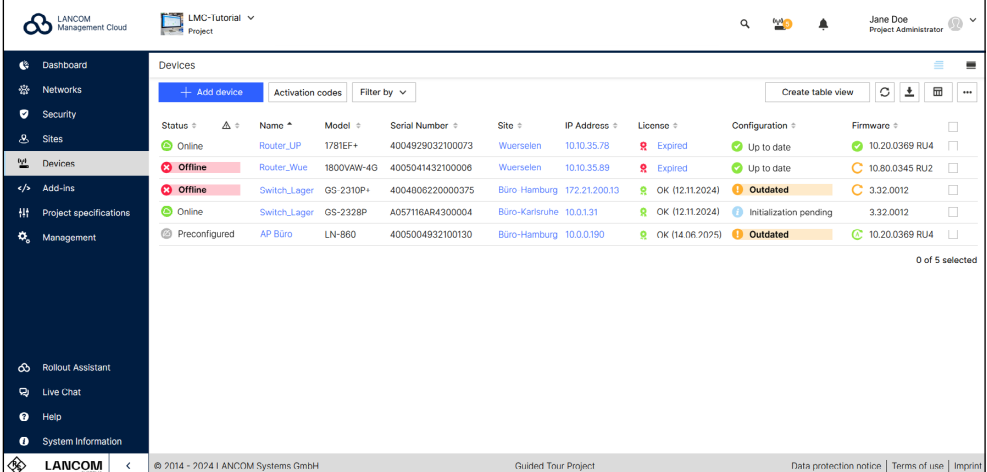
Existing passwords are not changed. If a device does not support the new length, the password is shortened and this is indicated with a log entry.

Bug fixes

- The exclamation mark in front of the beta label has been removed.
- The loading spinner has been restored in the device table while a configuration rollout is taking place.
- The licensing filter in SPLA projects has been removed from the device table.
- Fixed a problem in the device table where the configuration column could jump when the configuration status changed.

LANCOM Management Cloud 1.00.174.0 / 06.08.2024

Improved overview with color optimization of the device table



The screenshot shows the LANCOM Management Cloud interface. The left sidebar contains navigation options: Dashboard, Networks, Security, Sites, Devices (selected), Add-ins, Project specifications, Management, Rollout Assistant, Live Chat, Help, and System Information. The main content area displays a table of devices with the following columns: Status, Name, Model, Serial Number, Site, IP Address, License, Configuration, and Firmware. The table contains five rows of device data, each with a color-coded status indicator in the Status column.

Status	Name	Model	Serial Number	Site	IP Address	License	Configuration	Firmware
Online	Router_LUP	1781EF+	4004929032100073	Wuersefen	10.10.35.78	Expired	Up to date	10.20.0369 RU4
Offline	Router_Wue	1800VAW-4G	4005041432100006	Wuersefen	10.10.35.89	Expired	Up to date	10.80.0345 RU2
Offline	Switch_Lager	GS 2310P+	4004006220000375	Büro Hamburg	172.21.200.13	OK (12.11.2024)	Outdated	3.32.0012
Online	Switch_Lager	GS-2328P	A057116AR4300004	Büro-Karlsruhe	10.0.1.31	OK (12.11.2024)	Initialization pending	3.32.0012
Preconfigured	AP Büro	LN-860	4005004932100130	Büro-Hamburg	10.0.0.190	OK (14.06.2025)	Outdated	10.20.0369 RU4

Reduced in color, optimized in function: the new, subtle appearance of the device table provides an even more user-friendly LANCOM Management Cloud. Now, only those areas are highlighted that could currently require action on your part. These include warning and error messages for the device status ("offline") and configurations ("outdated"). All other harmless messages are displayed in reduced form. This means you are automatically less distracted, can recognize changes to all devices more easily, and can therefore concentrate on the essentials more quickly.

Bug fixes

- Problems with the new table design have been resolved.
- If the selectable values of a variable type based on a string selection are changed and the selected value is not available any more, a meaningful error message will be generated.
- An error in the generation bit field values was fixed in the add-in developer mode.
- A link directing to the non existing detail configuration of a Unified Firewall in the logs is removed.
- An error message that appeared when resetting the password of an unregistered user has been improved.
- Improvement to avoid creating unnecessary network objects on the Unified Firewall when using LTA in Split Tunnel mode
- Public LMC only: A problem with the usage data provided in the organization was solved. Please note that the data will be provided with a time delay of a few days in the coming months.

LANCOM Management Cloud 1.00.173.0 / 09.07.2024

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!**Improvements**

- Some optimizations regarding the BETA function 'Compare configurations'
- UX improvements when changing the role of administrators

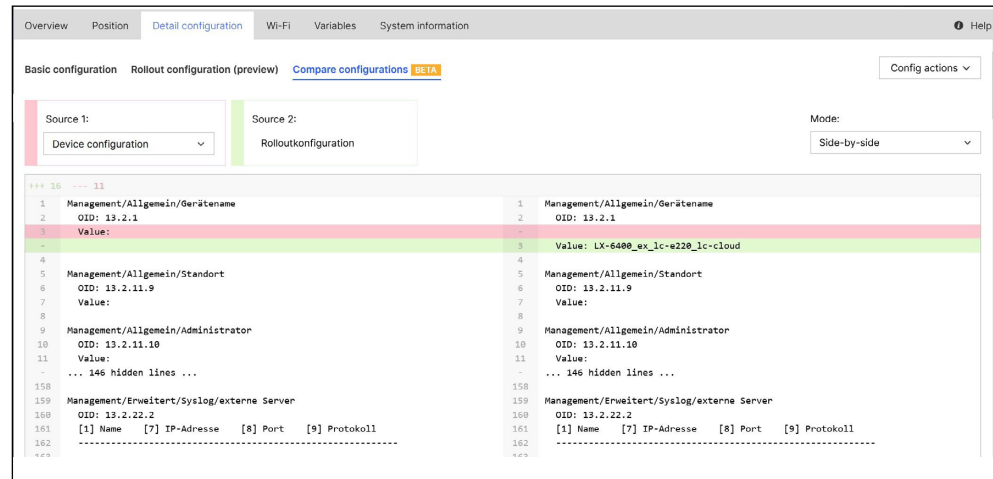
Bug fixes

- In some cases, there were discrepancies in the SPLA usage data for the month of May in the downloadable detailed report.
The data has been corrected.
- A problem with large tables on the Edge browser has been solved.
- For project viewers, the 'License' tab and the 'Initial Rollout Firmware' section were displayed, even if they were not accessible.
- Long project names in the membership table are now wrapped correctly.



LANCOM Management Cloud 1.00.172.0 / 18.06.2024

Full transparency before rollout thanks to configuration comparison



The practical configuration comparison gives you a detailed insight into the specific changes made by the rollout, particularly to the device configuration. This tool precisely shows you the sections in the device configuration that are overwritten by the LMC rollout configuration. The advantage: you get a clear overview of all changes in your device configuration before the rollout, minimizing risks from unforeseen results. Test this feature in the “Detail Configuration” tab of your routers, access points, or switches!

Improvements

→ Usage details on SPLA organizations can now be sent once a month.

Bug fixes

→ The DHCP settings at site level now check whether the configured default gateway belongs to the assigned network.

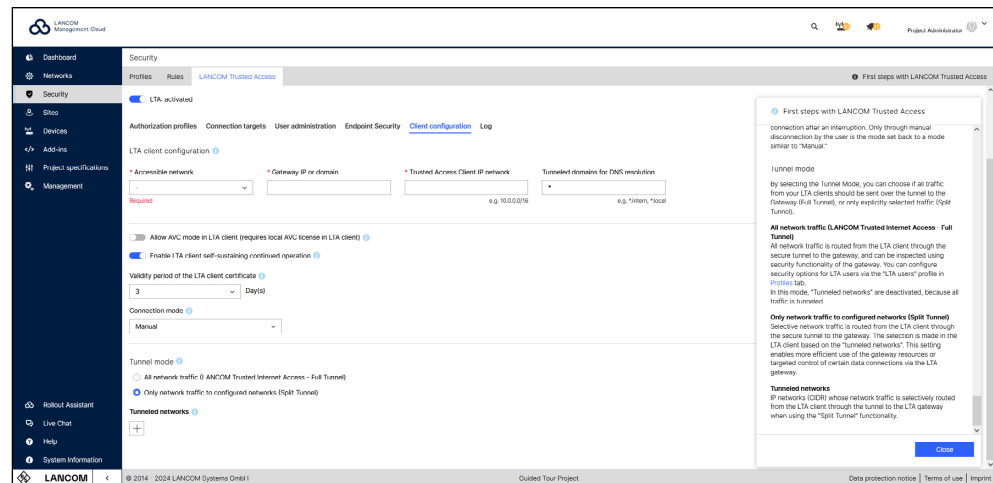
→ Project members can now browse through long add-ins.

→ A problem with the device and site tables on Edge browsers has been fixed.

LANCOM Management Cloud 1.00.170.0 / 15.05.2024

Trusted Internet Access: Mobile working as secure as in the office

LANCOM Trusted Access (LTA) now supports Full Tunnel operation (“Trusted Internet Access”), allowing all data traffic from connected LTA clients to be routed through the central LTA gateway. The advantage: activated security mechanisms on the gateway, such as Anti-Virus or Content Filter, are also applied to external web / cloud-based applications. Full Tunnel operation can be enabled under ‘Security > LANCOM Trusted Access > Client configuration’. Security settings for LTA users can be adjusted in the “LTA users” profile under ‘Security > Profiles’. Further information can be found in the [FAQs](#) or the [tech paper LTA system architecture](#).



Improvements

- The grouping of the firmware is now based on the model and the current firmware of the devices.
- In the firmware dialog, you can now choose to exclude selected devices/groups from the update.
- The rollout assistant can now be used as a project member.
- Extensions to the cloud hotspot
- Packet filter: AH_ESP can now be used in connection destinations.

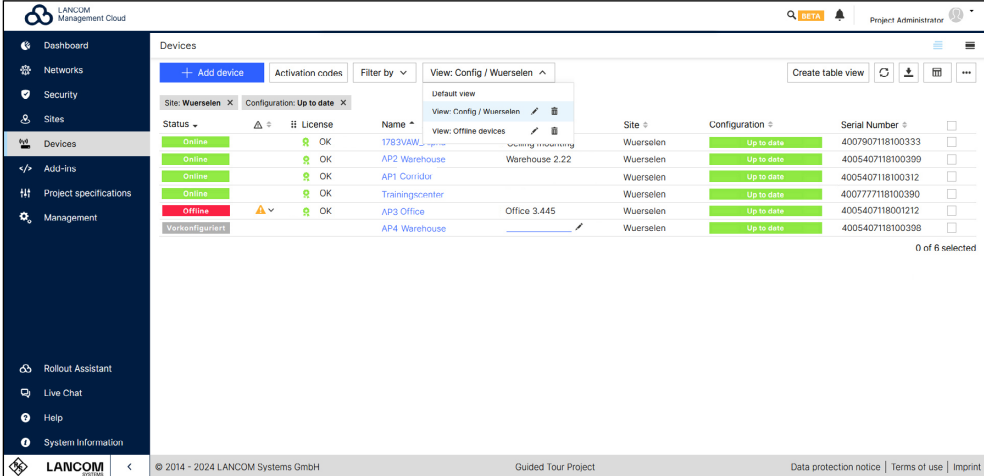
Bug fixes

- A problem with the middle mouse button to quickly open devices in the device list has been fixed.
- Spontaneous error “invalid destination” during LTA login fixed
- The number of LTA users could be wrong.
- Spontaneous exception in the site view
- When editing a membership, the ‘Technical administrator’ role could not be selected.
- When using 2FA, the terms of use could not be accepted.

LANCOM Management Cloud 1.00.169.0 / 16.04.2024

Customized device overview using savable table views

Focus more quickly on what you actually need: You can now customize your device view, including filter settings, to suit your needs using the “Create table view” button. The views you create are only visible to you and can be saved with an individual name so that you can access them again at any time. For example, move the table columns you are interested in using drag & drop, change the columns to be displayed under “Configure columns”, or filter the view using “Filter by” to make your daily workflows even more efficient.



Status	License	Name	Site	Configuration	Serial Number
Online	OK	1783VAW...	Wuerselen	Up to date	4007907118100333
Online	OK	AP2 Warehouse	Warehouse 2.22	Up to date	4005407118100399
Online	OK	AP1 Curiklar	Wuerselen	Up to date	4005407118100312
Online	OK	Trainingscenter	Wuerselen	Up to date	4007777118100390
Offline	OK	AP3 Office	Office 3.445	Up to date	4005407118001212
Unkonfiguriert		AP4 Warehouse	Wuerselen	Up to date	4005407118100398

Improvements

- The application templates for application management have been updated.
- The device tunnel service now provides an endpoint to check whether the device has correctly initiated a tunnel session.

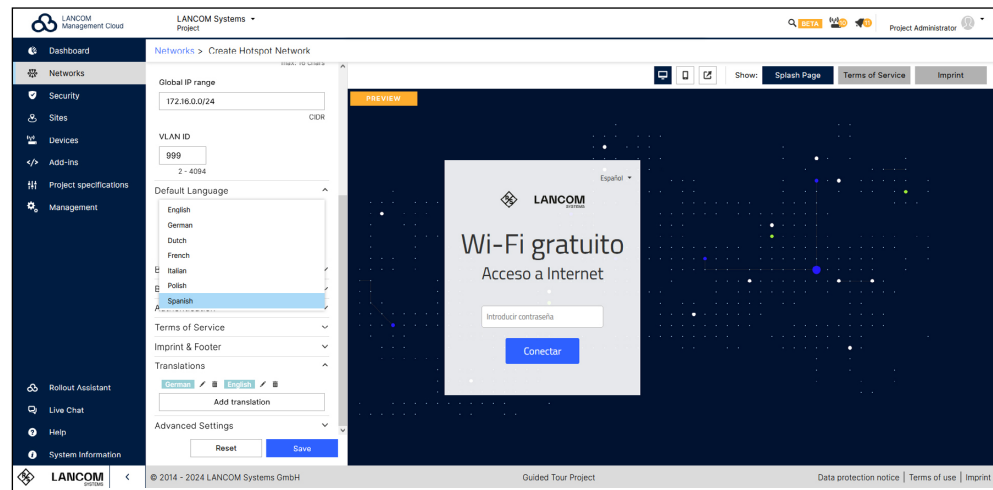
Bug fixes

- Pressing the Enter key in the editing dialog of variables now saves the content instead of discarding it.
- Spontaneous error messages during LTA login (invalid destination) have been fixed.
- In the ,Networks' area, the view of the ,Sites' tab now also works if a large number of sites have been assigned to a network.
- Updated the wording of the title in the log table regarding the LCOS restart in the event of a watchdog.

LANCOM Management Cloud 1.00.168.0 / 26.03.2024

More comfort with multi-language support for the cloud-managed hotspot

“Wifi en español? ¡Por supuesto!” – take full advantage of the language diversity when using the Wi-Fi hotspot via the LMC! Add translations of up to seven languages directly when creating a cloud-managed hotspot under Networks > Add Network > Hotspot Network > Translations. By selecting a default language, your hotspot users will see the preset language and the option to change the language. Simply assign the new hotspot network to the desired sites and your Wi-Fi hotspot will easily be available to visitors in different languages.



Improvements

- Uplink mode is now also available for LAG ports.
- The categories in the 'Application Management' section have been updated.
- All notifications can be closed at the same time.

Bug fixes

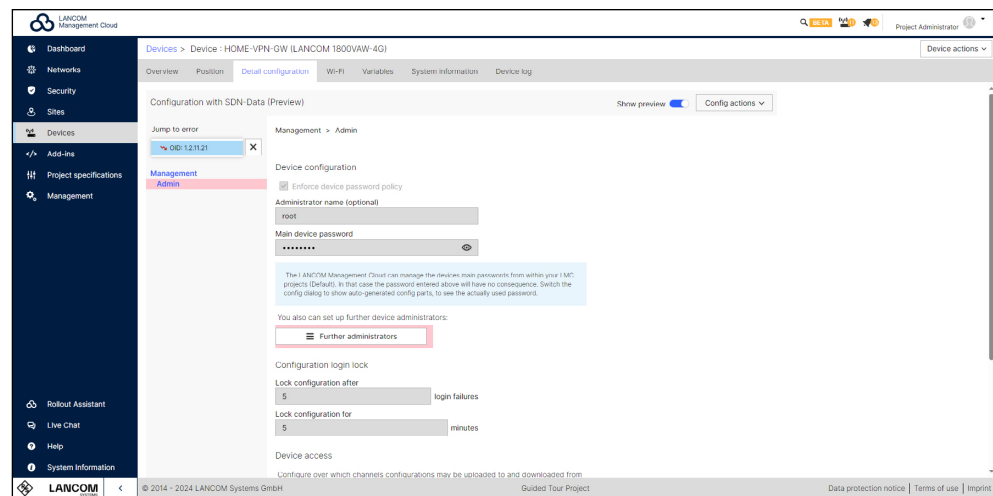
- When creating new WiFi networks, the key field is correctly available if WPA2/3 is selected.
- The actions configured in the action table are saved correctly in the detailed configuration.
- New projects with special characters can now be saved correctly.
- If a system variable UF_default_IF is set for a Unified Firewall, only the affected Unified Firewall is set to obsolete.
- More clarity in the log message when administrator roles are changed

- BPjM filter warnings on the security profile settings page are now always displayed correctly.
- The tooltip information about active packet filter rules in the ,Security / Profiles' table overview now shows the correct number of rules.
- The ,LMC Top Users' and ,Top Applications' data were labeled as gigabytes and terabytes respectively, although they are actually gigabits and terabits.
- Switching the monitoring from daily to hourly removed graphs on 5 unit stacks.
- The monitoring diagrams were sometimes empty.
- DPS Widget: Multiple networks with different central locations are not displayed.

LANCOM Management Cloud 1.00.167.0 / 05.03.2024

Precise troubleshooting with direct links to the source of the error

The time-consuming search is coming to an end: you can now benefit from optimized error notifications! For example, you can save yourself the laborious task of detecting errors in the event of invalid configuration parameters relating to object IDs (OIDs) in the device configuration. Clicking on the link displayed in the error report takes you directly to the corresponding point in the configuration preview in the detailed configuration of the device. This allows you to identify and localize the source of the error much faster!



Improvements

- Device tunnel log messages have been added to the device log if a dedicated tunnel could not technically be established after the tunnel was initialized.
- The device tunnel API layer now only allows to initialize a tunnel to a device if the device is online; if the device is offline, the request is rejected.
- Improved warning message that the network is still assigned to the location when the network is deleted
- When switching between full tunnel and split tunnel mode, the tunneled networks of the split tunneling were removed, now they are retained and deactivated by the system when switching to full tunnel.
- The configuration of static DHCP leases is now supported in the site-specific network settings.

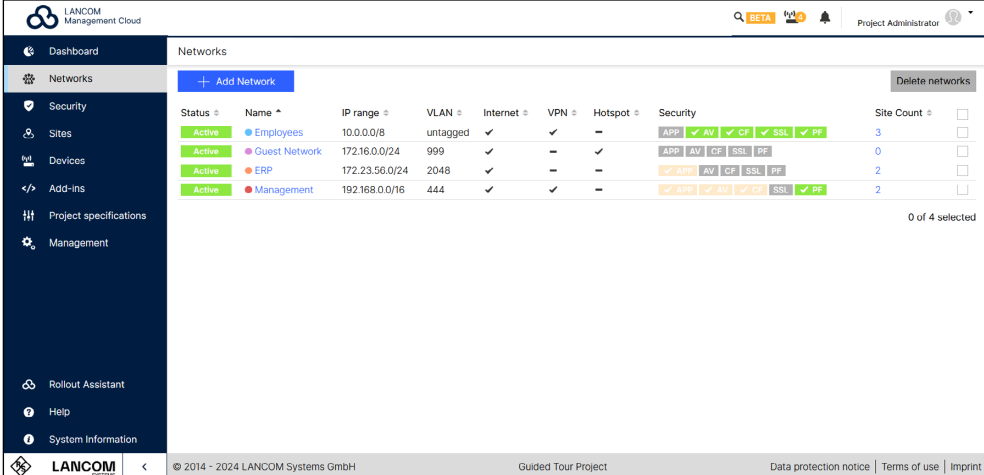
Bug fixes

- A problem with the location assignment in the device table has been fixed.
- A problem with the visibility of device list filters has been fixed.
- The network settings at site level were restricted if the network mode was set to “use the same network for each site”. It is now possible to configure settings for gateway IP addresses.
- The detail configuration now shows the correct values for the time base settings in the cron table.
- The ‘Description for networks’ field now also accepts spaces.
- The transmission power ranges have been corrected for 5 GHz WiFi settings.
- In the device overview for switches, the ‘Save’ button is only displayed if the configuration has actually been changed.
- The VLAN input field of the network configuration is now always active during the creation and editing of a network.
- If the gateway IP of a site-specific network is changed, the changes are correctly forwarded to the front end.

LANCOM Management Cloud 1.00.166.0 / 13.02.2024

Easy-to-view site assignment of a network

At which sites is a particular network used? How can networks be quickly removed from sites? Answers to these questions are now provided by the clear display in the „networks“ menu entry. Under „Site count“, you can see at a glance how many sites your networks are assigned to. Click on the number to go directly to the new detailed overview „Site“ of your selected network. Here you can remove the network assignment of one or more sites at the same time if required. In addition, a warning now appears when you delete a network, informing you if the network is still assigned to at least one site.



Status	Name	IP range	VLAN	Internet	VPN	Hotspot	Security	Site Count
Active	Employees	10.0.0.0/8	untagged	✓	✓	–	APP ✓ AV ✓ CF ✓ SSL ✓ PF ✓	3
Active	Guest Network	172.16.0.0/24	999	✓	–	✓	APP AV CF SSL PF	0
Active	ERP	172.23.56.0/24	2048	✓	–	–	APP AV CF SSL PF	2
Active	Management	192.168.0.0/16	444	✓	✓	–	APP AV CF SSL PF	2

Improvements

- Errors in the LMC logs that refer to OIDs in the device configuration now contain a direct link that points to the corresponding part of the configuration to localize the source of the error.
- There are now many smartphones that are equipped with more than one rear camera. Previously, the rollout assistant automatically selected a camera when scanning the serial number via barcode on a device, but this was not always the best one. Now it is possible to select the desired camera during the scan.
- According to a recommendation by the German Federal Office for Information Security (BSI), RSA-based certificates should have a key length of at least 3072 bits. Therefore, the pairing service will generate pairing CA keys with a length of 3072 bits instead of 2048 bits during the next automatic annual CA update.

If devices are re-paired from now on or are already paired and are automatically re-paired within a year, they will also generate RSA keys with a length of 3072 bits for the device-client certificate in relation to the LMC-TLS communication.

A technical impact is that the devices will need a little more time during the pairing process to generate the longer key length.

- Optimized display of error messages for invalid configuration parameters with a link to the configuration preview in the detailed configuration.
- A filter can now be used to quickly search for countries for addresses.
- The device CSV import no longer aborts when a device is imported again.
- The new LMC scripting manual has been linked.

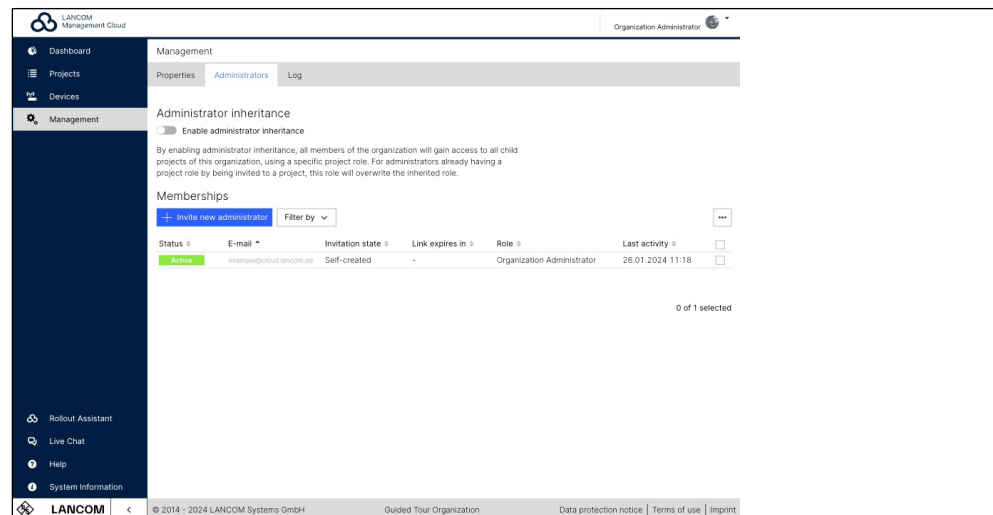
Bug fixes

- The function ‚enableBitByOidAtPos‘ of the LMC add-in now works correctly.
- The ‚*‘ character is now permitted in the configuration for RADIUS servers in the LMC.
- A display error in the detailed configuration in the tariff selection for Wi-Fi has been corrected.
- Sometimes the automatic selection for the DHCP start address selected an invalid network ID. This behavior has been corrected.
- If there was a change for the WAN connections at site level, too many devices were set to ‚Configuration obsolete‘. The selection of affected devices is now more precise.

LANCOM Management Cloud 1.00.165.0 / 23.01.2024

Central administrator management at organization level

Reduce time-consuming, manual activities when adding or deleting LMC administrators: Activating administrator inheritance gives members of an organization access to the subordinate projects. As the organization administrator, you control this access by selecting a role that is inherited to all subordinate projects in the organization. If you want to give administrators access to all projects but do not want them to have the administrative rights of an organization administrator, simply assign them the new „organization viewer“ user role under Management > Administrators. For projects in which administrator inheritance should not be activated, this can be excluded under Project specifications > Basic > Project access. All information on the LMC roles and rights can also be found in compact form in the Infopaper.



Improvements

- Project administrators can now export device data for the project from within the device table (e. g. for inventory purposes).
- Administrators can now assign devices to sites directly in the device table using an improved site filter.
- If devices without a position or address are added to a site, they are now automatically assigned.
- The ‚Device position‘ page has been redesigned and now allows larger images of the device installation to be uploaded.

- In the Wi-Fi profile, the ‚Minimum supported transmission rate‘ is renamed to ‚Base rate (beacons, multi- and broadcasts)‘ and applied to all corresponding LCOS LX settings.
- Support for additional languages in the hotspot menu
- New design for the rollout assistant web application

Bug fixes

- Sporadic LTA Idp synchronization errors have been fixed.
- Incorrect logging of the LTA Idp synchronization status has been fixed.
- The LTA main group was sporadically no longer displayed after synchronization.
- The workflow for resetting the password did not work if the form was used a second time.

LANCOM Management Cloud 1.00.164.0 / 02.01.2024

A look back at 2023



We would like to use the turn of the year to thank all administrators of the LANCOM Management Cloud. In 2023, many exciting projects with innovative solutions were realized with the LMC. At the same time, we continued to develop and drive forward the capabilities for the management of all network components. These key features are just a few examples:

→ **LANCOM Trusted Access – Cloud-managed Secure Network Access**

In addition to the central management of network components, the LMC also enables the secure connection of employees to the company network – from a single source! LANCOM Trusted Access (LTA) offers highly scalable remote access that protects hybrid working, whether as a cloud-managed VPN or based on the innovative Zero Trust principle. [Start your onboarding today!](#)

→ **Wi-Fi optimization with LANCOM Active Radio Control 2.0**

Best Wi-Fi at the touch of a button: LANCOM Active Radio Control 2.0 (ARC 2.0) predicts the optimization potential of the Wi-Fi network based on real usage data and automatically optimizes channels and channel widths.

[Discover the full power of ARC 2.0 on our topic page!](#)

→ **Efficient switch rollout thanks to centralized port templates**

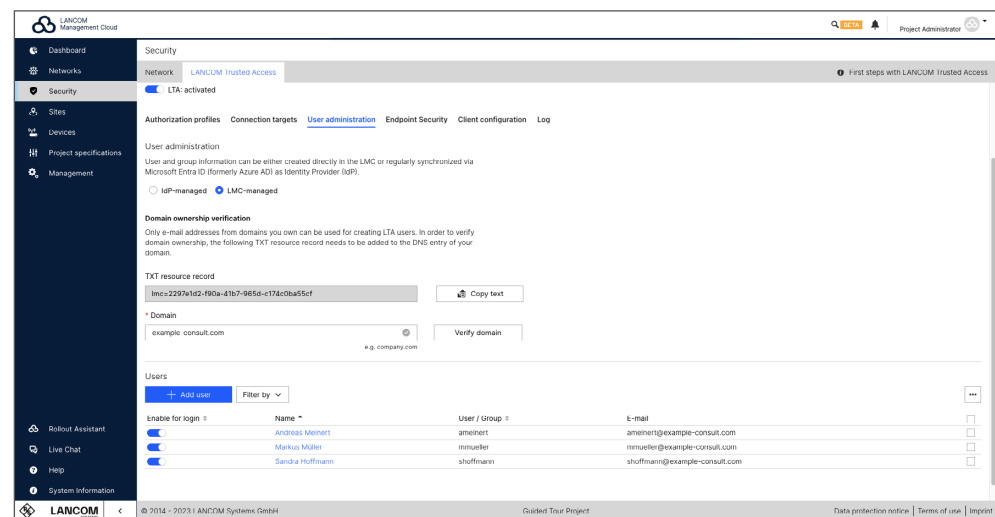
Network assignments to switch ports are simplified and assigned to the devices „zero-touch“. A major efficiency gain, especially with different port assignments at different locations.

We have also modernized the design of the user interface with a new look. You can already look forward to the further innovations that 2024 has in store for the LANCOM Management Cloud. Thank you for your continued support and trust!

LANCOM Management Cloud 1.00.163.0 / 12.12.2023

Your direct access to cloud-managed VPN

Centralized management of VPN users via the LANCOM Management Cloud (LMC) is also worthwhile for smaller installations. You do not need a user database (Active Directory), but can take immediate advantage of the remote access solution LANCOM Trusted Access: to do this, select the option „LMC-managed“ under Security > LANCOM Trusted Access > User management. Then copy the unique identifier (TXT resource record) from the LMC and paste it into the DNS configuration of your domain. After a brief check, the LMC verifies the domain and once you have entered your users' e-mail addresses, you can immediately enable them to use Trusted Access. Discover the LTA tutorials and trial versions today!



Improvements

- It is now possible to choose between 3 connection modes for the connection setup of the LTA client in the configuration of the LTA client profile: Manual, automatic or variable connection establishment (the behavior is identical to the current standalone AVC client).
- The add-in developer mode now supports values of the bitmask type.
- WWAN firmwares are displayed under ‚System information‘.

Bug fixes

- The stability of the tunneled WEBconfig access to LCOS FX firewall devices has been optimized. The optimization is only active in conjunction with the upcoming firmware release LCOS FX 10.13 RU3 (or higher).
- Error messages in the backend logs of the pairing service relating to cron jobs have been eliminated; however, the messages had no impact on functionality.

- Incorrect firewall rules were created for certain combinations of DPS with manually created applications and assigned DPS categories other than BE. The resulting firewall rules are now shortened so that they are acceptable for the device.
- A problem with the navigation on the page via the browser buttons has been fixed.
- Some linked materials that were still based on the old design have been updated.

LANCOM Management Cloud 1.00.162.0 / 22.11.2023

LANCOM Trusted Access – Cloud-managed secure network access

With the LANCOM Management Cloud (LMC), you now not only manage your network components, but also secure the connection of your employees to the corporate network centrally. With the highly scalable remote access solution LANCOM Trusted Access (LTA) and the new LANCOM Trusted Access Client, you can protect hybrid work – regardless of whether you want to use LTA as a cloud-managed VPN solution or on the basis of the future-proof Zero Trust principle with granular network control. Find out which LTA level of integration is right for you, start your LTA training, and test LTA for free for 30 days on the [LTA onboarding web pages](#).

The screenshot displays the LANCOM Management Cloud interface for a project named 'SDN-DEMO (LANCOM Visitor)'. The dashboard includes several key metrics: 1 Gateway, 120 Licenses, 110 Users, 32 Subscriptions, 1 Error, 4 Blocked Endpoints, and 6 Online Endpoints. The main content area is divided into three sections:

- LTA connections:** A table listing active connections with columns for Username, User Group, Hostname, IP Address, Security, and Connected at.

Username	User Group	Hostname	IP Address	Security	Connected at	Action
AlexanderFisher@company.com	Sales, IT, Marketing	Alexander_Laptop	192.168.43.72	Full	22.10.2023 00:43	...
ChristianMeyer@company.com	IT	Christian_LabJet	192.168.132.89	Full	22.10.2023 00:43	...
AnjaWagner@company.com	Marketing	Anja_Laptop	192.168.43.74	Full	22.10.2023 00:43	...
DanielSchneider@company.com	Development	Daniel_Laptop	192.168.43.75	Full	22.10.2023 00:43	...
- Event Logs:** A table showing system events with columns for Level, Created, Message, User, and Endpoint.

Level	Created	Message	User	Endpoint
Information	22.10.2023 00:43	LTA client has successfully established a secure tunnel to gateway.	SebastianWeber@company.com	Sebastian_Laptop
Information	22.10.2023 00:43	LTA client has disconnected the secure tunnel to the gateway.	AlexanderFisher@company.com	Alexander_LabJet
Error	22.10.2023 00:43	LTA client was spontaneously disconnected from the gateway after the secure tunnel was already established.	AnjaWagner@company.com	Anja_Laptop
Information	22.10.2023 00:43	LTA client has disconnected the secure tunnel to the gateway.	ChristianMeyer@company.com	Christian_LabJet
- Blocked endpoints:** A table listing blocked endpoints with columns for Hostname, Last logged in user, Permission, Last login attempt, Security, and Action.

Hostname	Last logged in user	Permission	Last login attempt	Security	Action
Daniel_Laptop	DanielSchneider@company.com	Blocked by admin	10.10.23 09:36	Full	Unblock
Sebastian_LabJet	SebastianWeber@company.com	Blocked by system	01.10.23 14:52	Full	Unblock
Thomas_Hotline	ThomasMuller@company.com	Blocked by system	24.01.23 17:08	Full	Unblock
Christian_LabJet	ChristianMeyer@company.com	Blocked by admin	09.09.23 07:32	Full	Unblock

Improvements

- In the switch device overview, the port labels and information about assigned networks can now be exported as a CSV file.
- If multiple ,0'-tagged default routes with different administrative distances are created in the underlying detailed configurations, these are adopted for automatically created SmartConfig default routes. This mechanism is only available if the WAN connections are not explicitly specified in the project or at the location.
- The displayed add-in console scripts from the configuration preview of the detailed configuration can now be copied without line numbers.

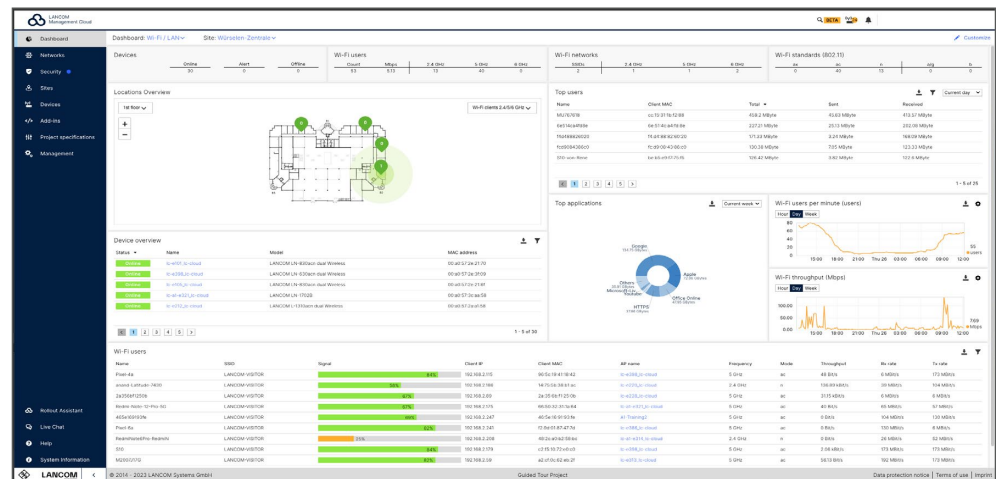
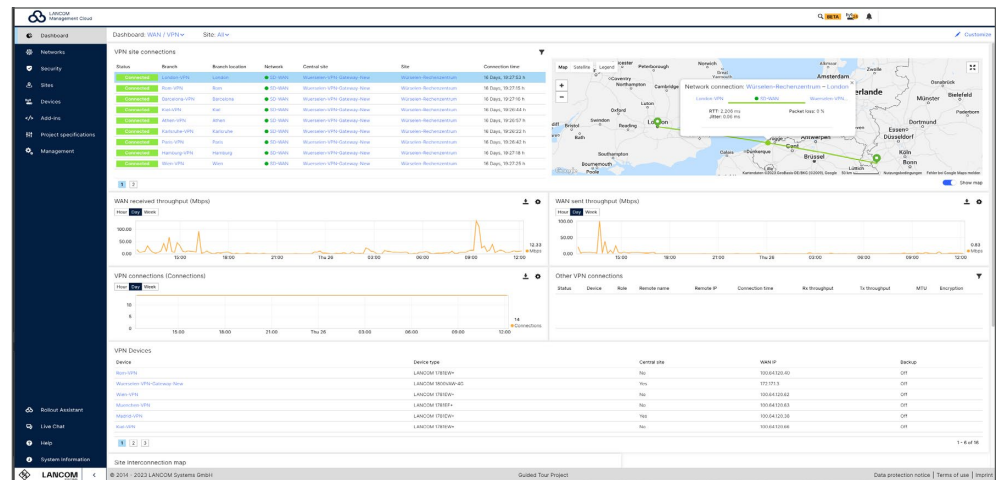
Bug fixes

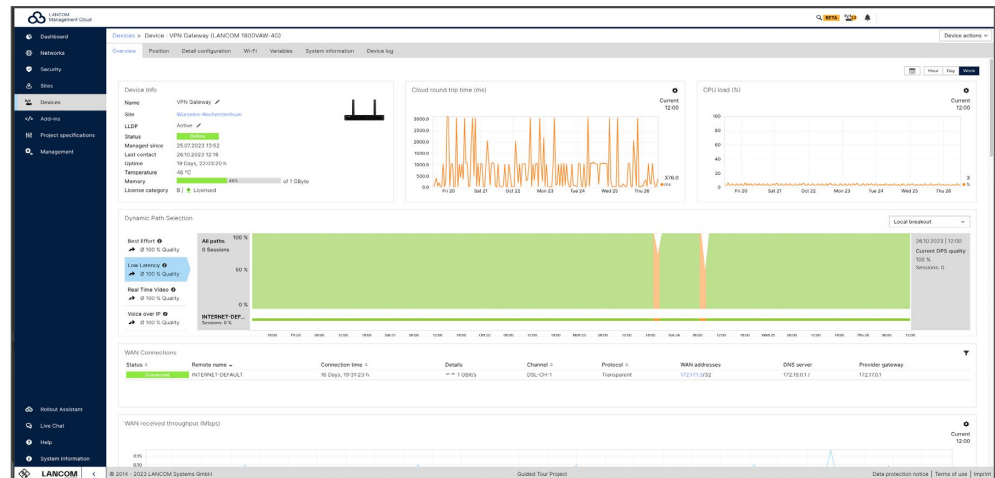
- If an add-in is assigned to a network, only the associated device classes are set to ,not current'.
- After use, the button for copying the device password is no longer blackened.
- Various visualization problems have been fixed.

LANCOM Management Cloud 1.00.161.0 / 31.10.2023

Refresh of the LANCOM Management Cloud user interface

Already noticed? The LANCOM Management Cloud now has a new LANCOM look. With a contemporary color palette and intuitively designed controls, the Cloud gets a breath of fresh air, while the features remain in the familiar place. Discover new colors and subtle design adjustments for an even better user experience. We welcome comments and feedback on the new Cloud design.





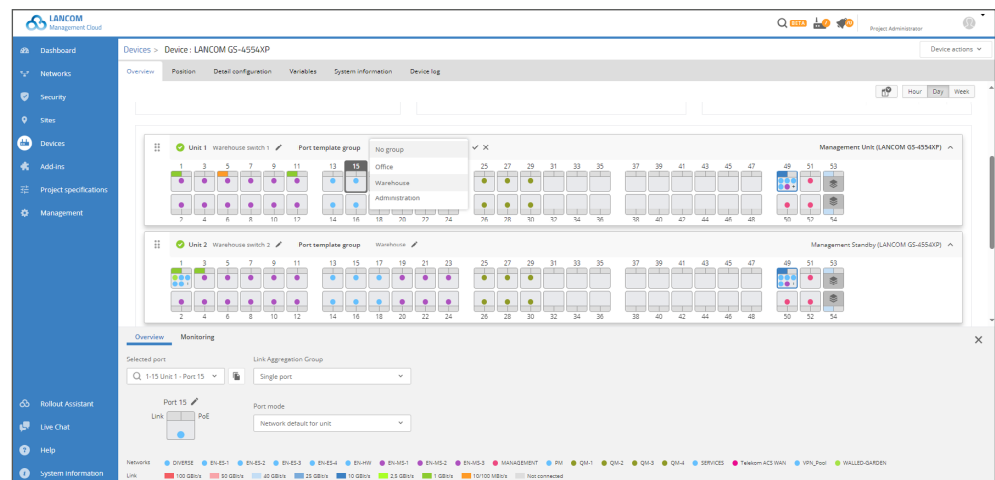
Improvements

- In the port template groups it is now possible to define, if a selected port should be operated in tagged mode or if an untagged operation is preferred.
- In the switch overview, a new port mode “uplink” can be assigned to individual ports. This operation mode causes every vlan of the site being assigned to the port either in hybrid or fully tagged way.
- Device list now optionally shows last contact time of offline devices.

LANCOM Management Cloud 1.00.160.0 / 13.10.2023

Simplified management and more overview for switch stacks

From now on, you can also benefit from convenient port management for switch stacks, so that individual and time-consuming port configurations of the stack units are a matter of the past. The central, cross-network port template groups are available for this purpose: Select one of your predefined port template groups for each unit of a stack to conveniently reuse your port configurations even for new stacks at different locations. The port template groups are assigned exclusively by your explicit selection in the unit overview of the stack and require the port mode „Network default for unit“. For even more overview, you can now additionally assign individual names to your stack units.



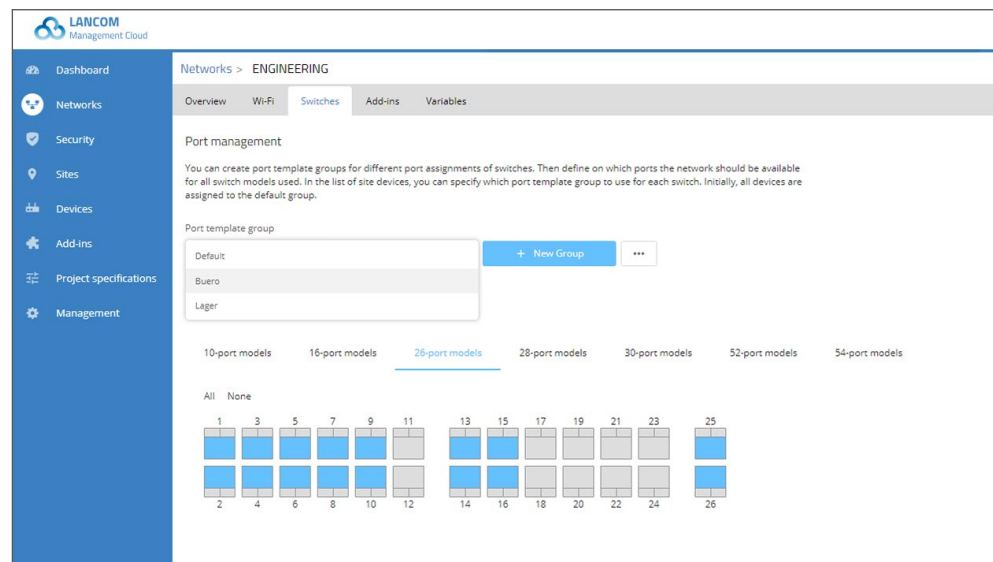
Bug fixes

→ The channels can be selected correctly again in the Wi-Fi settings.

LANCOM Management Cloud 1.00.158.0 / 29.08.2023

Centralized port templates for optimized switch rollout

Manual network assignments to switch ports could quickly become a challenge if you needed different port assignments for switches with the same number of ports at multiple locations. This is now remedied by extended, central templates, so-called port template groups. You can create, configure, and apply up to 50 different templates yourself for the networks and device models offered (e.g. 26-port model). Your previous port templates are initially assigned to the default group. You will find the port template groups under 'Networks > Selection of a network > Switches' and can easily map them to your devices on the site level for even more „zero-touch“.



Bug fixes

→ The channels can be selected correctly again in the Wi-Fi settings.

LANCOM Management Cloud 1.00.157.0 / 09.08.2023

Inspiration for your projects: Discover the new LMC website

We are pleased that you are using the LANCOM Management Cloud (LMC). With it, you benefit from:

- **Maximum productivity:** Configuration adjustments, firmware updates, monitoring & rollouts are automated and efficient – you save an average of 75% in time.
- **More performance and security:** VPNs, VLANs, ports, and UTM rules are defined and rolled out centrally. You can also securely connect remote workstations in the shortest possible time.
- **Immediate return on investment:** Make efficient use of valuable resources such as manpower, time and money. You can deploy new applications or optimize Wi-Fi infrastructures at the click of a mouse without expensive on-site visits.

We have summarized these and many other benefits and functions as well as customer references and awards on our relaunched [LMC website](#). We invite you to **use these benefits to win further projects** or to use the materials, customer references and use cases listed here as inspiration to further **develop your own network management concept**.

Bug fixes

- Schedules can be edited and created again.
- Variables with user-defined variable types can again be used correctly in the global add-in assignments.
- Change detection for add-in assignments works correctly again. The buttons for saving or discarding are only displayed when changes are made.
- The auto-correction of the input field for defining the IP network has been adjusted.
- Optimizations of the ARC 2.0 algorithm

LANCOM Management Cloud 1.00.156.0 / 18.07.2023

Network extension & device setups within minutes

Are you already benefiting from „zero-touch deployment“? Minimize your workload, especially when integrating many new access points, as this is where the LMC really shows its strengths: activate the project-wide location allocation based on the device IP address and define an initial firmware for new devices under Project specifications > Device startup. You can already register and configure your devices in advance via serial number and PIN independent of location – the LMC will then take care of everything else for you: if an Internet connection is established, your access points are automatically identified, assigned to a location, and immediately equipped with their pre-configuration. You can find more tips for a fast, automated rollout in the [techpaper LMC Rollout](#).

The screenshot displays the 'Preconfigure Device' form in the LANCOM Management Cloud interface. The form includes the following fields and options:

- Name:** Text input field containing 'LANCOM-LX-6400'. A note below states 'Will be used as device hostname'.
- Model:** Dropdown menu with 'LANCOM LX-6400' selected. A note below states 'Must match the physical device'.
- Target firmware:** Dropdown menu with '6.10.0106 Alpha (empfohlen)' selected. A note below states 'Bests for this configuration'.
- Software-Options:** Section with a checked checkbox for 'FCC standard conformance'.
- Site:** Dropdown menu with 'Würsteln' selected.

At the bottom of the form are 'Cancel' and 'Create' buttons. The footer of the page shows '© 2014 - 2023 LANCOM Systems GmbH' and 'Data protection notice | Terms of use | imprint'.

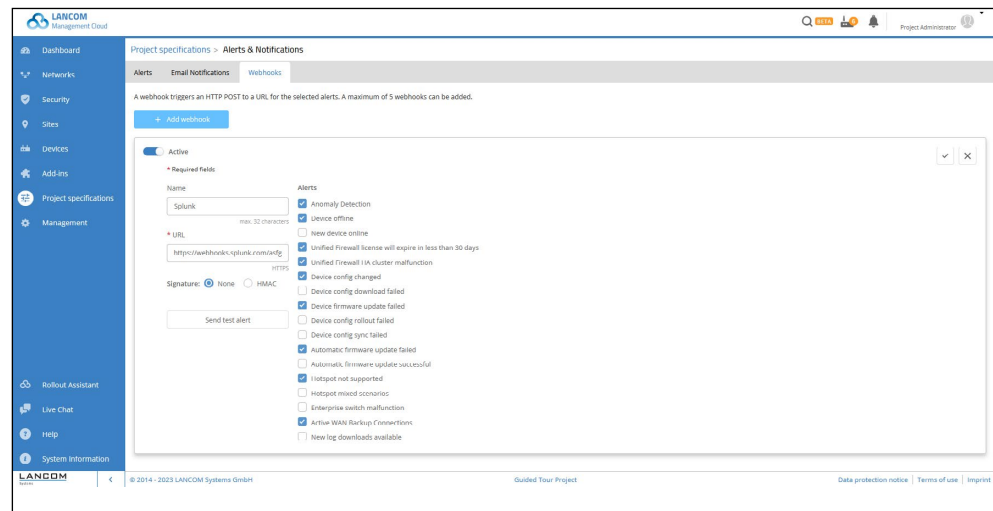
Bug fixes

- Fixed a problem with rolling out the configuration just before the license expires.
- CSV site and device imports were logged as system users.
- The hotspot password in the site-specific hotspot settings did not work.
- If the devices at a site have changed, the result of an ARC scan can continue to be used for the unchanged devices without a rescan.

LANCOM Management Cloud 1.00.155.0 / 27.06.2023

Efficient, automated workflows with webhooks

From monitoring and troubleshooting to deployment and upgrades: As an administrator, you rely on a holistic view of all network activities to respond quickly. Using webhooks in the LMC saves you valuable time by flexibly communicating alerts and notifications to messaging services and automation tools when an event occurs. Set up your webhooks for Slack or IFTTT, for example, under Project specifications > Alerts & Notifications > Webhooks and learn more in the [Webhooks techpaper](#).



Bug fixes

- In the device license assignment dialog the current license status was not shown.
- A display issue in the project specification dialog after saving the settings has been solved.
- An issue in the guided device replacement process has been solved.

LANCOM Management Cloud 1.00.154.0 / 07.06.2023**Improvements**

→ In add-ins, the variable contents of particular devices can now be accessed specifically via their serial number in order to use them for the configuration of other devices.

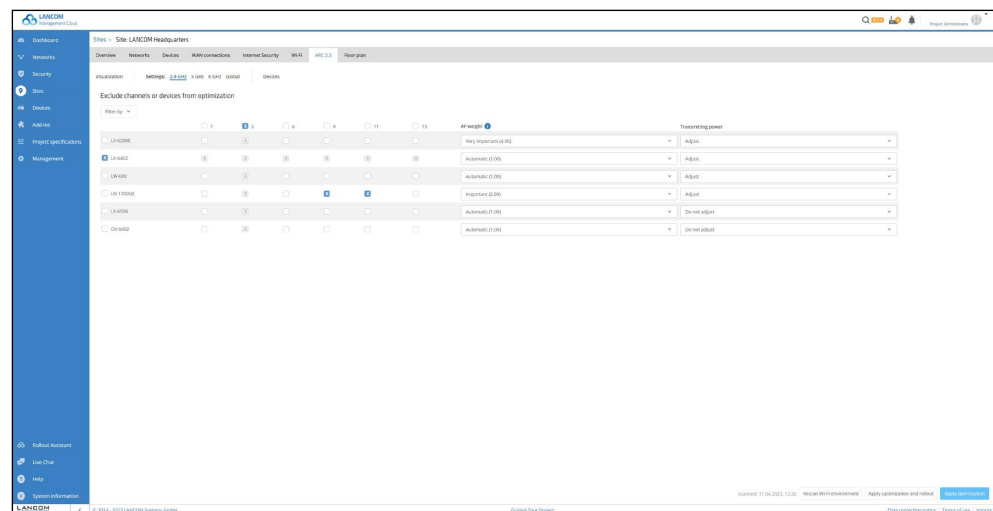
Bug fixes

→ The sender interfaces for communication with the LMC and the firmware update server are now also set correctly in scenarios with the cloud-managed hotspot.

LANCOM Management Cloud 1.00.153.0 / 17.05.2023

Two clicks to optimized Wi-Fi installations via the LMC

Scan, apply, and roll out – that is all it takes to make your Wi-Fi more efficient, even at sites with data-intensive applications, high user densities, or interfering third-party external networks. LANCOM Active Radio Control 2.0 (ARC 2.0) does exactly that job for you! After scanning the environment, the self-learning Wi-Fi optimization solution automatically takes into account the individual usage behavior of the Wi-Fi clients in your installation, predicts the expected Wi-Fi situation, and evaluates it using the ARC Index. Enhance your ARC Index and get the most out of your Wi-Fi installation! Find out your personal ARC Index potential now! Tips for custom settings are provided in the ARC 2.0 techpaper.



Further improvements

- To better distinguish the LMC administrative roles from the network users, the menu item 'Management → Users' has been renamed to 'Management → Administrators'.

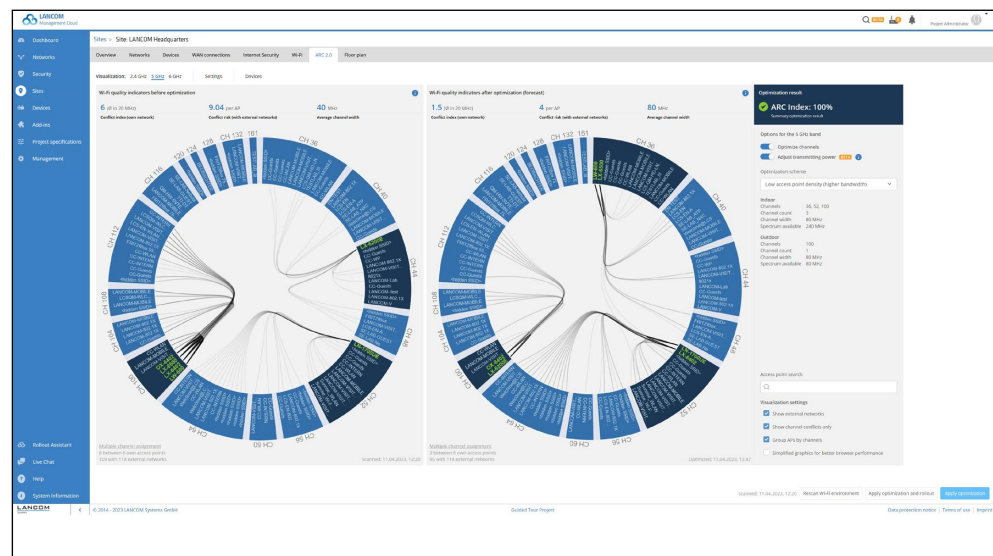
Bug fixes

- The encryption settings for WPA3 wireless networks have been corrected.
- The behavior of a rollout of linked Central Site devices when the VPN feature is disabled has been corrected.
- Optimizations of the calculation algorithm for ARC 2.0.
- Firmware updates and communication with the LMC could fail in certain scenarios due to incorrect settings of the source interfaces. The selection of source interfaces has been revised.

LANCOM Management Cloud 1.00.152.0 / 25.04.2023

Wi-Fi optimization with LANCOM Active Radio Control 2.0

Ensure optimal Wi-Fi for any network size at the push of a button – directly via the LMC! With the self-learning automation solution LANCOM Active Radio Control 2.0 (ARC 2.0), you can forecast the optimization potential of your Wi-Fi network based on learned usage behavior. For this purpose, ARC 2.0 analyzes existing multiple channel occupancies, taking into account external networks and access point densities. In this way, you receive a clear comparison of the actual radio field situation with a preview of the expected network status after adjustment. Clicking on „Apply optimization“ sets the most suitable channels and channel widths to automatically adjust transmitting powers and provide radio capacity where it is needed. Detailed ARC 2.0 settings such as prioritization, reservation, or exclusion of access points or channels can be made for access points as of LCOS LX 6.10 and other devices as of LCOS 10.72 under Sites > Site selection > ARC 2.0. Learn more about ARC 2.0 in this tech paper and try it out right away!



Further improvements

- The landing page UUID of the cloud-managed hotspot can be set in add-ins via a context variable (context.network.hotspotid).

Bug fixes

- The detail configuration now allows the simultaneous deletion of multiple table rows.
- Passwords can now be displayed again in the preview of the detailed configuration.
- ToolTip display errors in switch port information have been corrected.
- Devices are set to ,not up to date' when variables are changed even if they are not assigned to a site or network, but globally assigned add-ins are used.
- The commissioning process for devices with default configurations (manual or automatic assignment during commissioning) has been corrected.
- For globally assigned add-ins, switch variables with user-defined variable type can be used correctly again.
- Add-in developer mode outputs have been optimized for specific device types.
- If VPN is disabled for a network, no rollout of the connected Central Site devices is performed.

LANCOM Management Cloud 1.00.151.0 / 04.04.2023

Maximum data, failure, and access protection with the LMC

While you protect your network via the LANCOM Management Cloud (LMC), we take care of protecting the LMC itself in the background. With regular security audits, encrypted data backups, and geo-redundant, certified, and sustainably operated data centers in Germany, we minimize risks such as cyberattacks, data loss, and service outages. For you, this means data sovereignty at the highest level. To find out which data protection standards our LMC hosting meets in detail, visit our [Cloud security of the LMC website](#) or read the [LMC \(Public\) Data Protection and Data Security infopaper](#).



Bug fixes

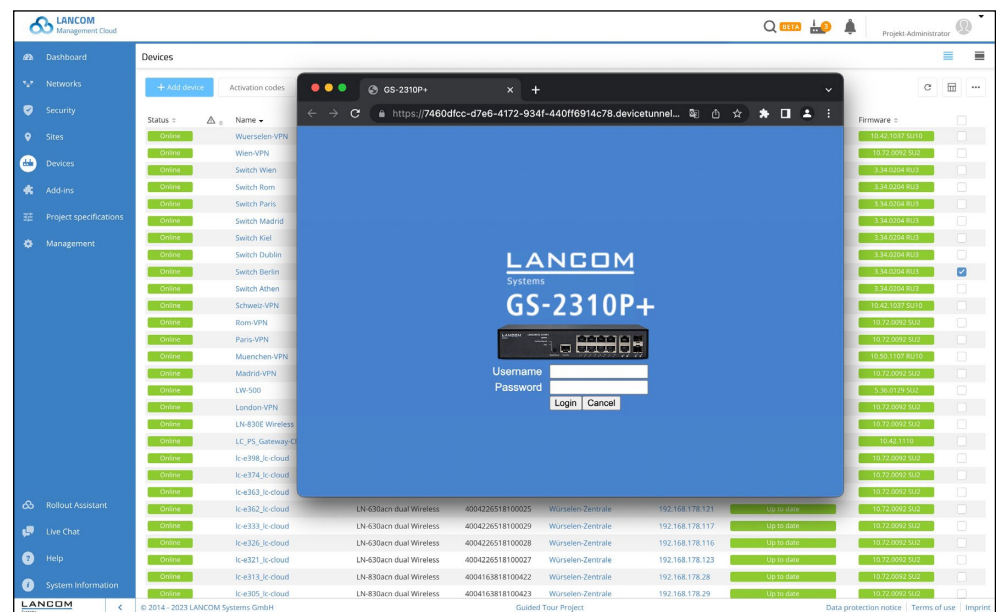
→ A display problem with the help chat has been fixed.

LANCOM Management Cloud 1.00.150.0 / 14.03.2023

Secure WEBconfig access and CLI tunnel for GS-2000 switches

We are continuously expanding the management options of the switches for you via the LANCOM Management Cloud (LMC): Direct remote access to a device's WEBconfig or command line interface (CLI) through the LMC saves system administrators valuable time and greatly simplifies device access. With the securely encrypted sessions tunneled through the LMC, you combine individual and global management for GS-2000 series switches in one application as well. To do this, select one or more switches (from firmware version LCOS SX 3.34 RU3) in the device overview and click 'Open terminal' or 'Open WEBconfig' in the selection menu.

Please note that local configuration changes can be overwritten by a configuration subsequently rolled out by the LANCOM Management Cloud.



Further improvements

- The structure of routing rules and tables rolled out to LCOS FX devices has been revised. This reduces the complexity of the routing configuration and the overall number of requests required to set up the device, thus increasing roll out speeds.

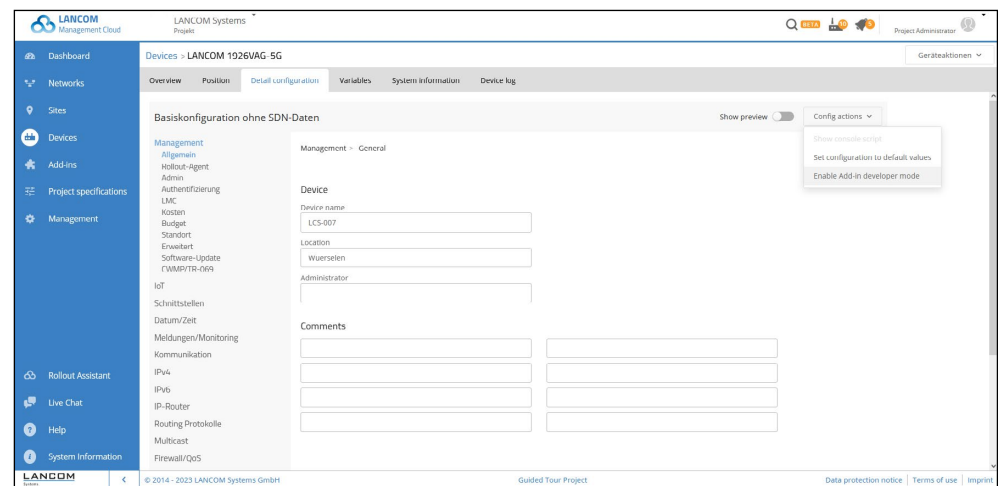
Bug fixes

- An issue with the user support chat has been solved.

LANCOM Management Cloud 1.00.149.0 / 21.02.2023

Accelerated add-in extension with new developer mode

Individually created add-in scripts are particularly useful for flexibly adapting your LMC configuration to customer-specific network scenarios. Accessing configuration data based on their object ID (OID) from the LMC is now even more convenient: make your adjustments, e.g. for a switch, in the detailed configuration and activate the new add-in developer mode under config actions. The LMC automatically converts your configuration changes into an add-in-compatible format that you can insert directly into your add-ins, saving you a lot of time. Learn more about add-ins in the [add-ins manual](#).



Further improvements

- When a device in a project goes online for the first time, a notification is displayed.
- The number of filtered locations is now displayed in the location overview.
- Anomaly detection notifications can now be closed.
- If a site's access point does not support the country assigned to the site, the device's configuration will not be written.

Bug fixes

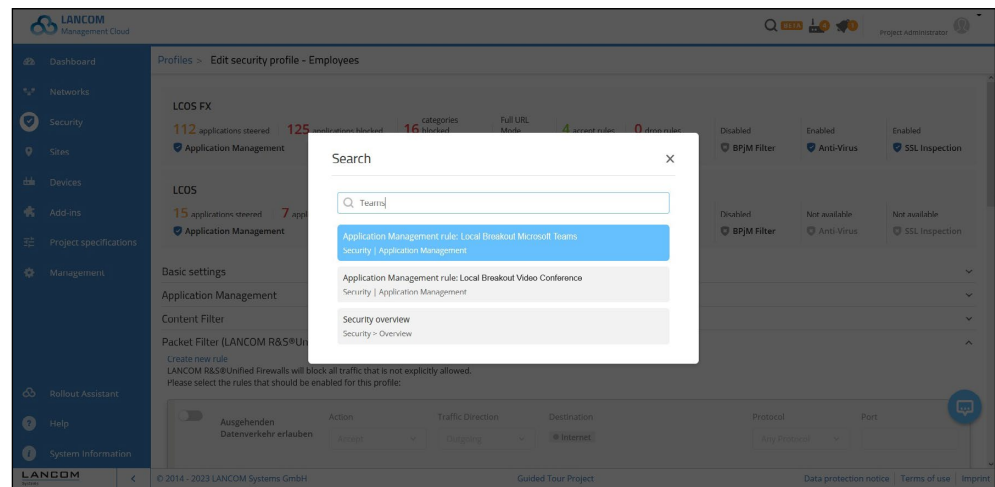
- Fixed an issue with a disappearing filter in the device overview.
- Fixed an issue with a delayed status display (online / offline) in the device detail view.
- Locations can be updated again via CSV import.
- The automatic assignment of locations based on IP addresses works again.
- The notation of MAC addresses in the detailed configuration has been corrected.

- The date selection in the detail configuration works again.
- The VLAN ID of a switch port that is part of an LAG is set correctly when the port is disabled in the individual port configuration.

LANCOM Management Cloud 1.00.148.0 / 31.01.2023

Advanced security features in the LANCOM Management Cloud

We are further expanding the "Security" menu for you: For improved usability and a more efficient workflow, you can now generate packet filter rules directly from a security profile. Especially if you have a large number of security profiles and rules, the project-wide search function helps you to locate the profile or rule you are looking for more quickly in the LMC. To do so, simply use the keyboard shortcut "ctrl + K" (Windows) oder "cmd + K" (macOS). An overview of the continuously developed security features can be found in our [tech paper](#).



Further improvements

- The design of the ‚Administration → Licenses‘ section has been revised.
- Improved overview within the security profiles
- The maximum number of floorplans has been increased to 25.

Bug fixes

- More robust error handling for the user's language setting
- Added support for 6 GHz in the ‚Wi-Fi Users‘ dashboard.
- The SD-WLAN configuration now enables 802.11ax on 2.4 GHz for the LANCOM routers of the 1800 series.
- The PoE status information for devices in a stack group has been corrected.
- The rollout of the device configuration via the action menu in the detailed configuration now also offers to roll out Central Site locations if required.
- Changes to variables now generate log messages.
- If the setting of the default networks of the Unified Firewalls is changed in the project settings for commissioning, only Unified Firewalls are now switched to ‚not up to date‘.

- If the device overview of a switch is called up several times, the order of the display of assigned networks remains unchanged.
- The DECT settings have been corrected in the detail configuration.

4. History of incompatible API changes

LANCOM Management Cloud 1.00.175.0 / 20.08.2024

- Deprecated POST /cloud-service-auth/actions (ACCOUNT_DELETE and USER_PROFILE_DELETE)
- **New:** POST /cloud-service-auth/user/self/delete
- **New:** POST /cloud-service-auth/accounts/{accountId}/delete

LANCOM Management Cloud 1.00.168.0 / 26.03.2024

- Deprecated GET /cloud-service-devices/meta/firmware?type=all
- New:** GET /cloud-service-devices/accounts/{accountId}/meta/firmware

LANCOM Management Cloud 1.00.160.0 / 11.10.2023

- Removed GET+PUT /cloud-service-logging/accounts/{accountId}/rules/configuration
- Existing alternative:**
GET+PUT /cloud-service-logging/accounts/{accountId}/alerts/settings/ruleconfig

LANCOM Management Cloud 1.00.157.0 / 08.08.2023

- Removed GET /cloud-service-devices/accounts/{accountId}/devices/licenses
- Existing alternative:**
GET /cloud-service-licenses/licenses
GET /cloud-service-licenses/licenses/ids

LANCOM Management Cloud 1.00.156.0 / 18.07.2023

- Removed GET /cloud-service-notification/accounts/{accountId}/notifications
- Existing alternative:** GET /cloud-service-notification/accounts/{accountId}/alerts

LANCOM Management Cloud 1.00.153.0 / 18.05.2023

The following APIs are deprecated and will be phased out in 3 months:

- Deprecated GET /cloud-service-devices/accounts/{accountId}/devices/licenses
- New:** GET /cloud-service-licenses/licenses/ids
- New:** GET /cloud-service-licenses/licenses



5. General advice

Disclaimer

LANCOM Systems GmbH does not take any guarantee and liability for software not developed, manufactured or distributed by LANCOM Systems GmbH, especially not for shareware and other extraneous software.

