

RELEASE NOTES

R&S®LMC SOFTWARE RELEASE 1.00.209.0

Table of contents

03	1. Preface
03	2. Important notes
04	3. New features, changes, and history
04	R&S®LANCOM Management Cloud 1.00.209.0 / 04.08.2026 Wireless Client Explorer
06	R&S®LANCOM Management Cloud 1.00.208.0 / 14.07.2026 We are Rohde & Schwarz Networks and Cybersecurity
07	R&S®LANCOM Management Cloud 1.00.207.0 / 24.06.2026 Global role management for multi-account environments
08	R&S®LANCOM Management Cloud 1.00.206.0 / 10.06.2026 Improved overview for organization administrators
10	R&S®LANCOM Management Cloud 1.00.205.0 / 12.05.2026 eSIM management with the R&S®LANCOM Management Cloud
12	R&S®LANCOM Management Cloud 1.00.204.0 / 21.04.2026 New licensing option for Docker support on R&S®LANCOM Unified Firewalls
13	R&S®LANCOM Management Cloud 1.00.203.0 / 31.03.2026 Monitoring and notifications for mobile connections
14	R&S®LANCOM Management Cloud 1.00.202.0 / 10.03.2026 Switch port templates for greater efficiency in dynamic networks
16	R&S®LANCOM Management Cloud 1.00.201.0 / 17.02.2026 Authorization of role assignment via an identity provider
18	R&S®LANCOM Management Cloud 1.00.200.0 / 27.01.2026 Cross-system monitoring via API for telemetry data
19	R&S®LANCOM Management Cloud 1.00.198/199.0 / 06.01.2026 Full transparency in lifecycle management
20	R&S®LANCOM Management Cloud 1.00.197.0 / 25.11.2025
21	R&S®LANCOM Management Cloud 1.00.196.0 / 04.11.2025 Device reboot in scheduled events
22	R&S®LANCOM Management Cloud 1.00.195.0 / 14.10.2025 Dashboard update for targeted monitoring
23	R&S®LANCOM Management Cloud 1.00.194.0 / 23.09.2025 Secure admin user management via an identity provider
24	R&S®LANCOM Management Cloud 1.00.193.0 / 02.09.2025 Convenient event planning for enterprise environments

25	R&S®LANCOM Management Cloud 1.00.192.0 / 12.08.2025
	Lifecycle at a glance: EOL status in the device table
26	R&S®LANCOM Management Cloud 1.00.191.0 / 22.07.2025
27	R&S®LANCOM Management Cloud 1.00.190.0 / 01.07.2025
	Device configuration backup
29	R&S®LANCOM Management Cloud 1.00.189.0 / 20.05.2025
	User-bound API keys for easy integration of third-party applications
30	R&S®LANCOM Management Cloud 1.00.188.0 / 20.05.2025
	Integration of R&S®LANCOM Unified Firewall licenses into your Service Provider License Agreement (SPLA)
31	R&S®LANCOM Management Cloud 1.00.187.0 / 29.04.2025
	More transparency for scheduled events
32	R&S®LANCOM Management Cloud 1.00.186.0 / 08.04.2025
	Update for Active Power Control: Smart power management for R&S®LANCOM devices
34	R&S®LANCOM Management Cloud 1.00.185.0 / 17.03.2025
	Increased efficiency through direct project navigation
35	R&S®LANCOM Management Cloud 1.00.184.0 / 24.02.2025
	My dashboards: A milestone for network monitoring and troubleshooting
37	R&S®LANCOM Management Cloud 1.00.183.0 / 04.02.2025
	Features for more overview and more convenience
39	R&S®LANCOM Management Cloud 1.00.182.0 / 13.01.2025
	Scheduled events in the R&S®LANCOM Management Cloud
41	4. History of incompatible API changes
42	5. General advice
	Disclaimer

1. Preface

As an intelligent network management and monitoring system, the R&S®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 R&S®LMC, saving valuable resources such as money and time.

The R&S®LMC Public 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 R&S®LMC Software Release 1.00.209.0, as well as the improvements since the previous version.

2. Important notes

To ensure continued smooth operation with the R&S®LANCOM Management Cloud, R&S®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

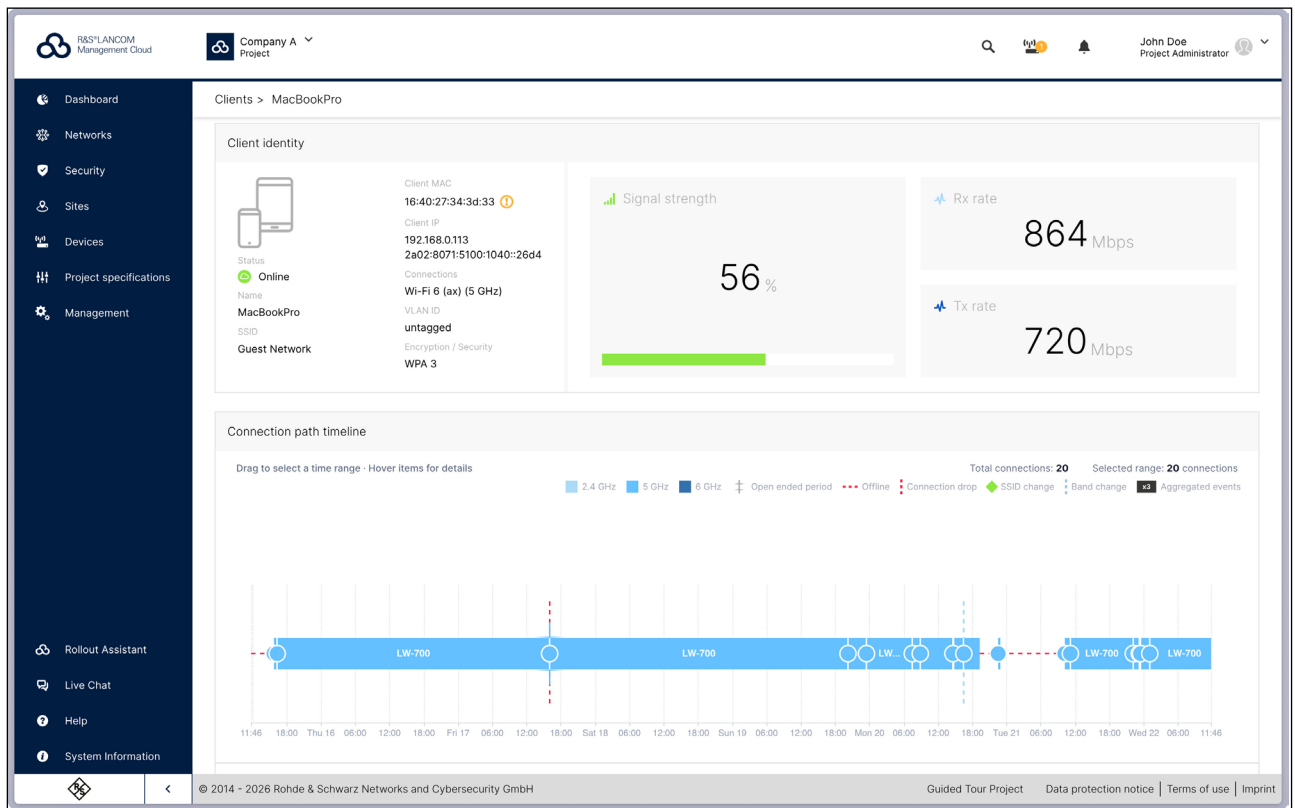
To use all the functions of the R&S®LANCOM Management Cloud, we recommend using the latest release version.

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

3. New features, changes, and history

R&S®LANCOM Management Cloud 1.00.209.0 / 04.08.2026

Wireless Client Explorer



Track the path of wireless clients through your network: The Wireless Client Explorer provides administrators with a centralized, client-focused view of the Wi-Fi clients connected to the network. Using the client profile, you can uniquely identify a client, including its location and the last access point it used. The new roaming timeline provides a 7-day history of all access points the client has connected to, offering a transparent and comprehensive view of its connection history. By eliminating the need for time-consuming manual reconstruction, it enables more efficient network administration and faster troubleshooting. You can access the Wireless Client Explorer via “Wi-Fi users” in the R&S®LMC dashboard “Wi-Fi & LAN”.

Stay tuned: Upcoming updates will expand the Wireless Client Explorer with client-specific metrics, a more flexible search function, and a dedicated client overview.

Improvements

- ▶ Selecting the device name in the floor plan overview table will now take you to the details page for that device.
- ▶ The thumbnails of the floor plans have been removed.
- ▶ Active alerts for devices are now displayed on the device details page in the floor plans and are linked to a full view in the global device table.
- ▶ The display of device details on the floor plan has been improved.
- ▶ Devices located at the same place on a floor plan now form a cluster.
- ▶ Devices can now be easily removed from floor plans.

Bug fixes

- ▶ The floor plan can now be deleted properly in full-screen mode.
- ▶ When uploading an incompatible image for a floor plan, a clear error message is now displayed.
- ▶ Warning messages in the toolbar are now visible even on small screens.
- ▶ Switching between a background image and a solid color now works on the hotspot network page.

We are Rohde & Schwarz Networks and Cybersecurity

Together, we are embarking on a new chapter. With the merger of LANCOM Systems and Rohde & Schwarz Cybersecurity to form Rohde & Schwarz Networks and Cybersecurity GmbH, two companies that have already been collaborating successfully for years are now joining forces. The merger unites the complementary range of solutions and expertise of both companies under a single umbrella.

As part of this development, we are also gradually rebranding the user interface of the R&S®LANCOM Management Cloud. These changes affect only the appearance and branding of the application. The functionality of the R&S®LMC remains unchanged. Likewise, no adjustments to existing device configurations are required—all systems can continue to be used as usual.

Improvements

- ▶ The Site network view now displays the subnet address (CIDR) for each network.
- ▶ The position and zoom level in floor plans can now be automatically adjusted so that the user can see the entire floor plan in a single view window.
- ▶ Different icons have been added to the floor plan widgets for various device types (access point, router, switch, firewall).
- ▶ To improve device management, a device list has been added to the floor plan overview.
- ▶ On the device overview page for access points, the Wi-Fi user table has been expanded to include MLO and VLAN IDs.

Bug fixes

- ▶ A problem has been fixed where selecting a device on a floor plan would be deselected by clicking on other areas or devices as long as there were unsaved changes.
- ▶ A problem has been fixed in which the floor plan remained in focus after the selected device's highlight was removed.
- ▶ A bug has been fixed that caused the old name to continue appearing in the drop-down menu for changing floor plans after a floor plan had been renamed.
- ▶ An issue has been resolved in which the number of devices and their statuses were displayed incorrectly on the 'Floor Plan Overview' tab after adding new devices.
- ▶ The email address is not automatically filled in the new login window when using the new password manager. This is in line with the latest technology and the user experience on other platforms.

Global role management for multi-account environments

External admin user management

Integrating an OIDC identity provider (IdP) simplifies admin user login through single sign-on (SSO), enhances security with centralized identity management, and increases convenience by reducing the need for multiple credentials.

In this section, you can manage your identity provider (IdP) configurations for admin user authentication and authorization within your LMC organization based on OpenID Connect (OIDC). Use the "Add IdP configuration" button to create a new entry, or select an existing entry to edit or delete it.

State	Share the IdP configuration to another account	Client ID	E-mail domains	Authorization	Role inheritance
Enabled	Share icon	https://login.microsoftonline.com/af3668f3-2e27-4abe-81a9-b825c72a847c/v2.0	azure2lancom.onmicrosoft.com	✓	✓
Enabled	Share icon	https://login.microsoftonline.com/af9768f3-6e27-4abc-8a09-c123c52e847c/v2.0	lancom.de	✓	✓
Disabled	Share icon	https://login.microsoftonline.com/af3998f3-7e27-4cbe-80a9-aa56c52e847c/v2.0	test.acme.org	✓	-

0 of 3 selected

Centralized authorization through the identity provider (IdP) is particularly beneficial for large multi-account environments. Roles and permissions can be managed centrally and deployed across multiple organizations. To enable this, an organization's base IdP configuration can be applied to other organizations, while administrators can be assigned organization-specific roles within each one. This reduces administrative overhead, minimizes maintenance efforts, and ensures consistent permission models across all accounts. At the same time, centralized administrator and role management enhances security and simplifies the onboarding and offboarding.

IdP configurations can be shared via the "Administration" menu in the "External admin user management" tab. When you hover over a configuration name, a share icon appears, allowing you to share the IdP configuration.

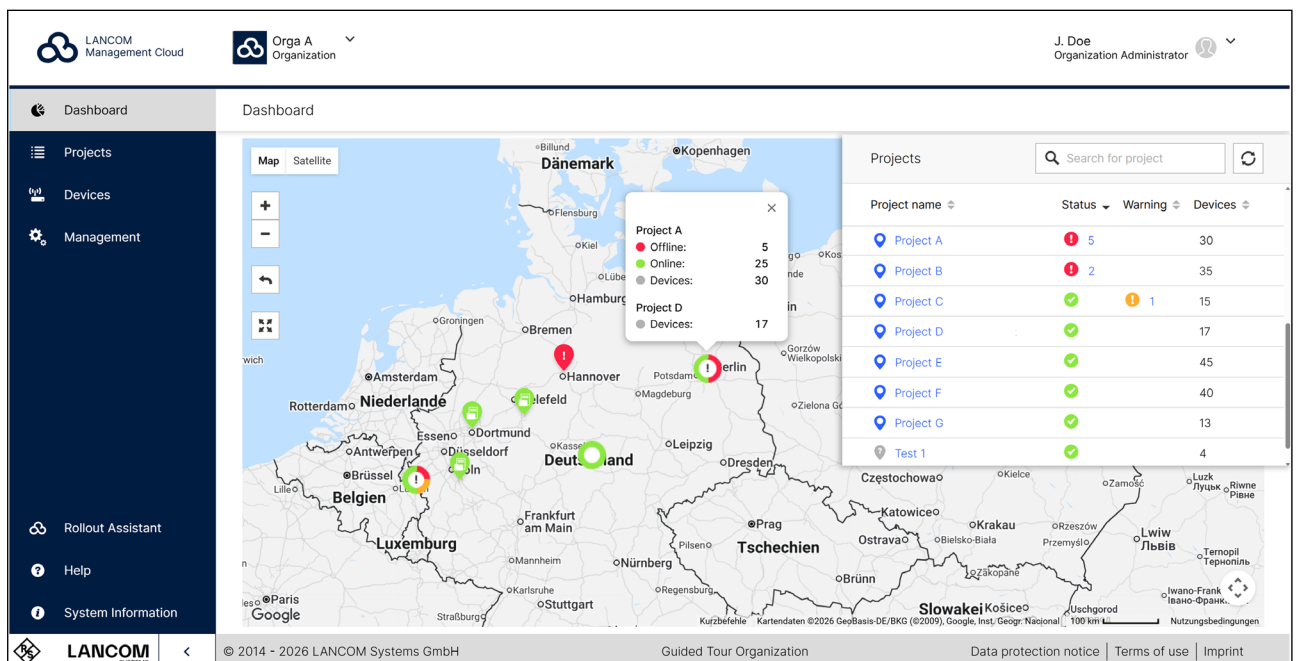
Improvements

- ▶ Display of the VLAN ID in the Wi-Fi user table on the R&S®LMC dashboards
- ▶ A CSV export feature has been added for the project table in the "Organization" view.
- ▶ Support for MLO features on compatible access points
- ▶ Improved use of floor plans

Bug fixes

- ▶ Several bug fixes have been made to the floor plans.
- ▶ The user is now redirected to the IdP, regardless of whether the domain portion of the entered email address is in uppercase or lowercase.
- ▶ An issue has been fixed where downloading the license usage summary temporarily returned a 404 error.

Improved overview for organization administrators



With the R&S® LANCOM Management Cloud's organization dashboard, organization administrators can now keep track of projects even more easily. The centralized map view provides a quick overview of project statuses and alerts, enabling prompt action. Affected projects can be accessed directly from the dashboard.

In addition, the project list has been expanded to include important business-relevant information, such as device lifecycle status and license expiration details. This enables organization administrators to identify risks early and manage customer projects even more efficiently.

Improvements

- The display of variables is now standardized throughout the R&S®LMC, with separate columns for 'Variable Name' and 'Display Name'.
- The organization section has been improved to provide a comprehensive overview of project status, licenses, and device lifecycles.
- If the maximum number of dashboards has been reached in 'My Dashboards', the 'Create' button will be disabled and a corresponding message will appear.

Bug fixes

- ▶ Large R&S®LMC backups no longer cause devices in the R&S®LMC to go offline.
- ▶ A bug has been fixed that allowed users to create an SSID profile with an 802.1X setting but without specifying a valid RADIUS server.
- ▶ Disabling administrator inheritance at the project level caused an error during IdP authorization.
- ▶ A bug has been fixed that prevented default values from being set in dynamic tables when the column was left blank.
- ▶ An issue has been resolved in which the sizes of the WWAN signal strength and temperature charts unexpectedly shrunk.
- ▶ An issue has been fixed where administrators were unable to filter by the 'MAC Address' field in the 'Wi-Fi users' widget.
- ▶ Organization Dashboards – An issue with inconsistent behavior of the 'Back' button has been resolved.

eSIM management with the R&S® LANCOM Management Cloud

The screenshot displays the R&S LANCOM Management Cloud interface. The top navigation bar includes the LANCOM logo, 'Company A Project', a search icon, and user information 'J. Doe Project Administrator'. The left sidebar contains a menu with options: Dashboard, Networks, Security, Sites, Devices (selected), Add-ins, Project specifications, Management, Rollout Assistant, Live Chat, Help, and System Information. The main content area is titled 'Devices > Device: LANCOM 1800VA-5G' and features a 'Device actions' dropdown. Below this, a tabbed interface shows 'Overview', 'Position', 'Detail configuration', 'Variables', 'eSIM' (active), 'System information', and 'Device log'. The 'eSIM' tab contains instructions on adding an eSIM profile, a 'Target eSIM' dropdown set to 'eSIM-1', and fields for 'eID' (12249032000001000000265227955711), 'IMEI' (867224070448074), 'Activation code' (LPA:1\$esim.lancom.com\$QR-G-5C-1TS-1W1Z2P7), 'Confirmation code / ePIN', and 'Alias'. A checkbox 'Activate the new eSIM profile after adding' is checked. At the bottom right of the form are 'Discard' and 'Add profile' buttons. The footer shows the LANCOM logo, copyright '© 2014 - 2026 LANCOM Systems GmbH', 'Guided Tour Project', and links for 'Data protection notice', 'Terms of use', and 'Imprint'.

The R&S® LANCOM Management Cloud now allows you to centrally configure and manage eSIM profiles on compatible SD-WAN gateways. This saves time and eliminates the need for costly on-site visits. At the same time, security is enhanced since no physical cards can be lost. It is ideal for branch networks, mobile workstations, or as a backup solution.

You can find these features in the device table under the new “eSIM” tab after selecting the corresponding SD-WAN gateway. An overview of supported devices is available [here](#).

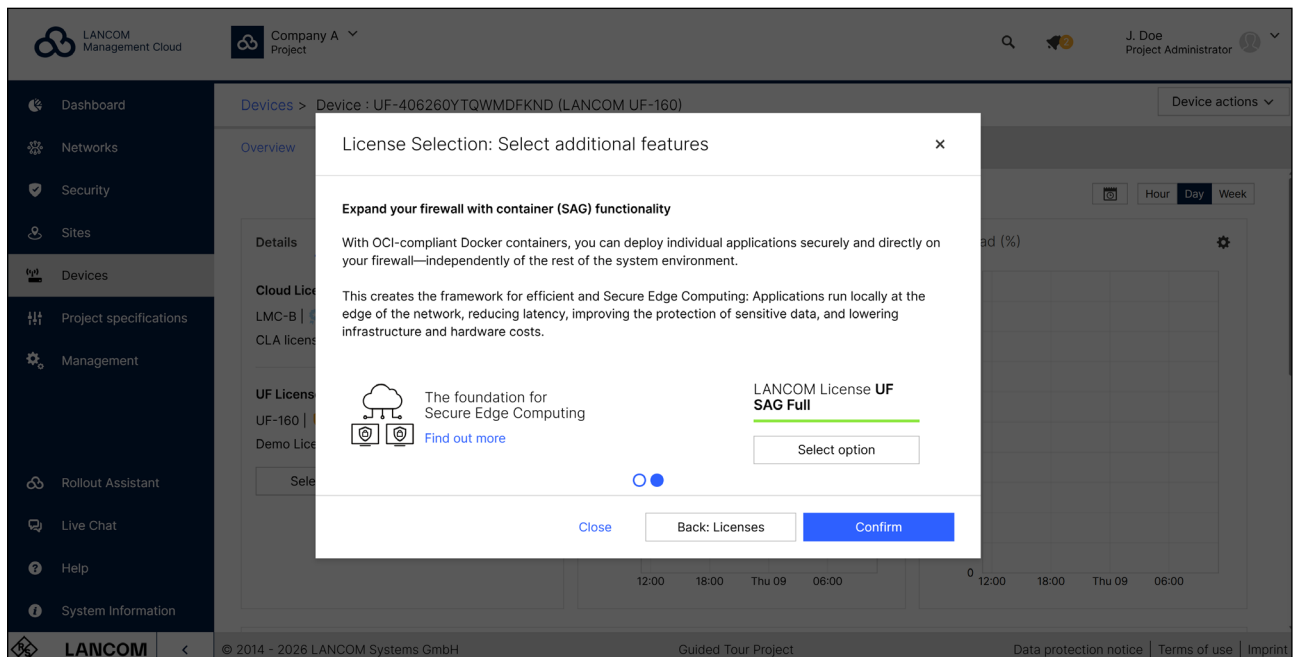
Improvements

- ▶ It is now possible to delete the last account administrator.
- ▶ The expanded monthly CSV export is available for download within the organization.
- ▶ Dashboards / Charts: No line interpolation for missing data points
- ▶ A procedure has been implemented to ensure that LTA certificates are properly renewed when necessary.
- ▶ The behavior of the R&S® LMC has been modified so that default values can be entered in the detailed configuration even if they fall outside the valid range for a particular option.
- ▶ Context-based areas can now be configured in the R&S® LMC user interface.
- ▶ Users can choose to automatically accept membership invitations.

Bug fixes

- ▶ A bug has been fixed that caused the 'Save' button to not work properly after copying an entry in the WAN tag table and changing the remote location.
- ▶ A bug has been fixed that prevented users from assigning JSON variables on devices or websites.
- ▶ Fixed an issue in the device overview for Edge routers that prevented mobile signal strength from displaying correctly.
- ▶ The metrics are now also visible when the connection is established via 5G.
- ▶ Dashboard Overview Page: An issue causing the thumbnails to appear on a black background in Firefox and Safari has been resolved.
- ▶ Correction to the rounding method for the 'VPN Connections' widget on the device overview page
- ▶ A bug that caused a DHCP warning to appear in certain cases even though no changes had been made has been fixed.

New licensing option for Docker support on R&S® LANCOM Unified Firewalls



With the latest update to the R&S® LANCOM Management Cloud (R&S® LMC), SPLA customers can now optionally enable support for Docker containers on R&S® LANCOM Unified Firewalls via the R&S® LMC and bill it on a monthly basis. Previously, this was already possible if a corresponding license had been installed directly on the device. Activation takes place in the device's License tab via R&S® LANCOM License UF SAG Basic or UF SAG Full. In addition, R&S® LMC objects can now also be adjusted locally on the device. For details, please refer to the [LCOS FX 11.2 Release Notes](#).

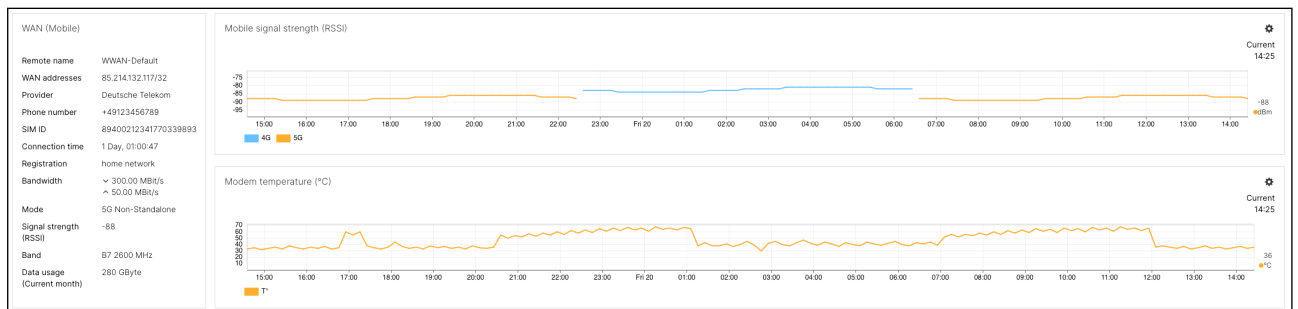
Improvements

- ▶ A new API endpoint returns all device identifiers for a project in a consistent order.
- ▶ Added a port copy function to the port settings in the switch port template.

Bug fixes

- ▶ Fixed a Bug that led to a 404 page error after deleting a switch port template.
- ▶ Fixed a bug in WAN connections and load balancing that prevented users from selecting all connections using the 'Select all' checkbox.
- ▶ Improved response on usage attempt for expired API key
- ▶ Under 'Management / Edit address', confirming without adding or changing address details no longer leaves the dialog open with a loading spinner that does not finish.
- ▶ When a port-description was set at device-level the switch-template configuration was not used for this port, because it was recognized as configured at device-level.
- ▶ In the cloud-managed hotspot preview, the accept or login link no longer opens an error page.
- ▶ For anomaly detection alerts, affected metrics are listed only once after refreshing the full notification list.

Monitoring and notifications for mobile connections



Keep a close eye on your mobile connection at all times. In the device overview of your 4G/5G SD-WAN gateways, you can now access detailed insights into key mobile data, such as your device's phone number, SIM information, and data usage. The signal mode (4G/5G) and signal strength can be easily tracked through a clear timeline. Additionally, for compatible device models, an extra widget visualizes the mobile modem temperature over time.

Advanced alerts and notification features also ensure maximum operational reliability. Simply enable these under "Project specifications" to receive real-time alerts instantly whenever anomalies occur or critical data limits are reached.

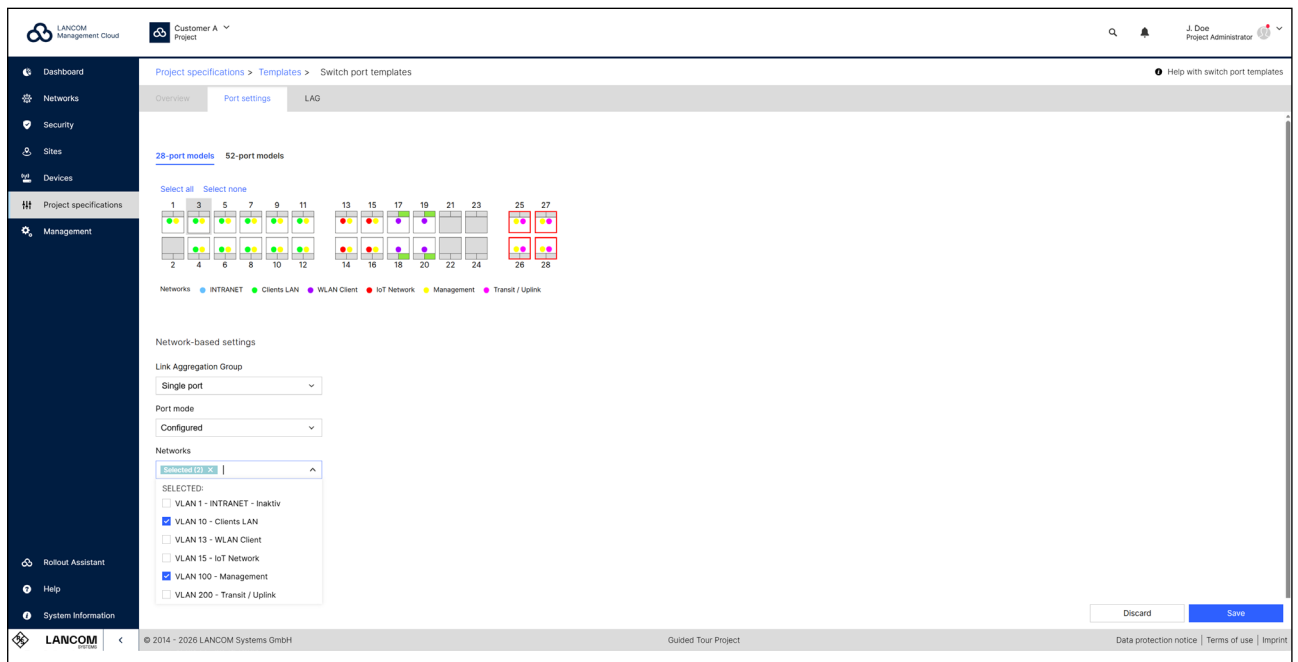
Improvements

- The workflow for creating vouchers can now be used with API keys.
- The CSV import now includes an optional column for device names. The names provided are validated during the import. If this column is missing, the import works as before, and empty entries are ignored. The sample import file has been updated to demonstrate the new feature.

Bug fixes

- Entries under "Support Access Granted" are now sorted by time within a specific day.

Switch port templates for greater efficiency in dynamic networks



The R&S®LMC Smart Configuration extension with switch port templates replaces individual add-ins with centralized templates and intelligent configuration mechanisms. Switch port settings are defined once and then consistently rolled out to all assigned devices. Subsequent extensions, such as adding VLANs, are just as quick and easy. The template-based approach reduces administrative effort, minimizes errors, and accelerates rollouts – especially in large, dynamically growing network environments.

You can access the 'Switch port templates' via the menu item 'Project specifications' > 'Templates'.

Improvements

- ▶ A device's lifecycle status is now displayed in the organization's project list.
- ▶ In the IdP configuration of the user domain, configuration details can be viewed on the 'Account details' tab.
- ▶ If a principal's domain is managed by IdP, the account containing this configuration is listed in the principal overview. Clicking on the link takes you to the corresponding search result in the account search.
- ▶ With the currently implemented UI-bound authentication code flow using PKCE, the validity of users cannot be guaranteed when using API keys. To avoid interrupting automations and causing security risks, it is possible to mix IdP and R&S®LMC-managed users within an account, allowing customers to invite R&S®LMC-managed users with different email domains as API key users to their accounts.

Since the administrator table provides additional transparency regarding the use of API keys, IdP user management should generally be used.

- ▶ The title and subtitle of a hotspot can now be up to 50 characters long.
- ▶ New line chart widget on the device overview page: modem temperature
- ▶ Wireless client VLAN available in the API
- ▶ AP ID accessible for ESL via API
- ▶ Help texts and function access for IdP authorization are included in the global R&S®LMC search results.

Bug fixes

- ▶ For devices with WAN interfaces, the WAN throughput (RX and TX) is displayed.
- ▶ The user profile area checks for invalid entries as you type.

Authorization of role assignment via an identity provider

External admin user management

Integrating an OIDC identity provider (IdP) simplifies admin user login through single sign-on (SSO), enhances security with centralized identity management, and increases convenience by reducing the need for multiple credentials.

In this section, you can manage your identity provider (IdP) configurations for admin user authentication and authorization within your LMC organization based on OpenID Connect (OIDC). Use the "Add IdP configuration" button to create a new entry, or select an existing entry to edit or delete it.

☐	Status	Name	Issuer URL	Client ID	E-mail domains	Authorization	Role inheritance
☐	Disabled	LCS	https://login.microsoftonline.com/a7f668f3-7e07-4zbe-81a9-b4923c527c7c/v2.0	b0uigf04-a9ac-482c-8126-f77263cd6f0d	lancom.de	-	-
☐	Enabled	Entra	https://login.microsoftonline.com/a72996f3-7e27-4abe-81a9-b779c52f247c/v2.0	b0azdf04-a9ad-482c-8127-f39552cd6f0d	azure2lancom.onmicrosoft.com	✓	✓

0 of 2 selected

In addition to direct login via your company's identity provider (IdP), role assignment in the R&S®LANCOM Management Cloud can now also be managed centrally via the IdP. This means that both authentication and authorization of access and usage rights are consolidated in a single central location. This increases security when onboarding and offboarding new administrators while significantly reducing administrative effort.

Improvements

- ▶ Wi-Fi 7 features can now be configured via the R&S®LMC Wi-Fi Smart Configuration.
- ▶ Signal strength and signal type have been added to the WWAN and hardware anomaly detection alerts.
- ▶ Additional Wi-Fi network configuration parameters have been added to the R&S®LMC Wi-Fi Smart Configuration. This reduces the need for additional add-ins to configure wireless networks. Furthermore, UI clarity has been improved by grouping related content into tabbed sections.
- ▶ The following additional parameter can now be configured in the R&S®LMC Wi-Fi Smart Configuration under 'Networks > Select network > Wi-Fi > Select Wi-Fi SSID > Client Management':
 - ▶ Maximum amount of clients
- ▶ The following additional parameters can now be configured in the R&S®LMC Wi-Fi Smart Configuration under 'Networks > Select network > Wi-Fi > Select Wi-Fi SSID > Transmission':
 - ▶ Block Multicast
 - ▶ Multicast to Unicast
 - ▶ ARP Handling
 - ▶ U-APSD
 - ▶ DTIM Period
 - ▶ RRM / 802.11k (Radio Resource Management)

- ▶ Default settings and new parameters have been added to the R&S®LMC Wi-Fi Smart Configuration to speed up the setup of the Wi-Fi network.

Common settings are automatically added to the default settings so that administrators do not have to configure each option manually. These default settings can be modified at any time.

The following presets are now available under

'Networks > Select network > Wi-Fi > Select SSID > Overview > Presets':

- ▶ Wi-Fi 7 (strict)
 - ▶ Wi-Fi 7 (802.1x)
 - ▶ Standard (WPA3)
 - ▶ Standard (802.1x)
 - ▶ Legacy (WPA2/3)
 - ▶ Open (unencrypted)
- ▶ The following additional parameters can now be configured in the R&S®LMC Wi-Fi Smart Configuration under 'Networks > Select network > Wi-Fi > Select Wi-Fi SSID > Security':
 - ▶ Encrypt Management Frames
 - ▶ Beacon Protection
 - ▶ Group Management Cipher
 - ▶ WPA2/3 Session Keytypes
 - ▶ New metrics available via monitoring API
 - ▶ Phone number
 - ▶ SIM ID
 - ▶ WWAN modem temperature
 - ▶ Data volume (requires enabled budget in LCOS)
 - ▶ Notifications for 'inherited' administrators in projects are suppressed (Telekom only).

Bug fixes

- ▶ Automatic merging of shadow configurations now works.
- ▶ (W)WAN monitoring issues have been resolved.
- ▶ The info window for external user management no longer remains on the screen.
- ▶ An incorrect time span when closing a notification has been fixed.

Cross-system monitoring via API for telemetry data

A new interface provides programmatic access to all telemetry data collected by the R&S®LANCOM Management Cloud. This enables you to flexibly integrate the desired values into external observability and monitoring systems, allowing for centralized monitoring across system boundaries. With targeted queries and access to up to 30 days of historical data, you can identify trends early, accelerate error analysis, and gain a transparent view of your network infrastructure's status.

This technology also serves as the foundation for upcoming native enhancements, such as expanded metrics in "My dashboards" and improved troubleshooting capabilities.

This [OpenAPI documentation](#) and [Knowledge Base document](#) help you integrate the interface quickly and easily.

Improvements

- ▶ Implementation of additional WWAN & hardware anomaly detection alerts

Bug fixes

- ▶ Any combination of upper and lower case letters is now permitted for LTA user names; a case sensitivity error has been fixed.
- ▶ Issues accessing 2FA projects after introducing the option to also allow IdP-managed users in 2FA-restricted accounts have been resolved.
- ▶ When switching between device configurations, the correct variable page is now reloaded.
- ▶ R&S®LMC WWAN monitoring only displays WWAN-related messages.
- ▶ Problems with processing 'wlan-neighbor/dhcp-lease processing' during direct insertions have been fixed.
- ▶ Batch processing of 'ControlActionResult' now also processes Kafka messages.
- ▶ Missing dashboard data has been corrected.
- ▶ The equality of the metric hub parameters has been corrected.
- ▶ The logging service now also works with large accounts.
- ▶ A problem with the device list user interface on mobile devices has been fixed.

Full transparency in lifecycle management

Dear administrator,

the lifecycle status of one or more models in a project has recently changed:

Project: LMC Project A ([SCP-PRJ-0004-266-18](#))

The following models in your project are affected:

- **LANCOM LN-630acn dual Wireless**
 - EOL date: 2026-04-01
 - Remaining lifetime: less than 3 months
 - Number of affected devices: 6

Please ensure timely planning for replacement or migration to supported models in order to maintain continuous support, security, and operational stability.

Further details can be found in the [Lifecycle Documentation](#). You may contact sales partner or sales@lancom.de directly for replacement devices.

Your LANCOM Team

Sehr geehrter Administrator,

der Lifecycle-Status eines oder mehrerer Modelle in Ihrem Projekt hat sich kürzlich geändert:

Projekt: LMC Project A ([SCP-PRJ-0004-266-18](#))

Die folgenden Modelle in Ihrem Projekt sind betroffen:

- **LANCOM LN-630acn dual Wireless**
 - EOL-Datum: 2026-04-01
 - Verbleibende Zeit: weniger als 3 Monate
 - Anzahl betroffener Geräte: 6

Bitte planen Sie rechtzeitig einen Austausch oder eine Migration auf unterstützte Modelle, um durchgehenden Support, Sicherheit und einen stabilen Betrieb sicherzustellen.

Weitere Informationen finden Sie in der [Lifecycle-Dokumentation](#). Sie können sich für Ersatzgeräte auch direkt an Ihren Vertriebspartner bzw. sales@lancom.de wenden.

Ihr LANCOM Team

Example R&S®LMC lifecycle notification

Enhancements to lifecycle management in the R&S®LANCOM Management Cloud now provide full transparency throughout the entire device lifecycle. Detect at an early stage when a device has reached, or is about to reach, its “End of Life” (EOL) status. Three months before expiration, the EOL status is clearly highlighted in the device list. An initial automated email notification is sent twelve months in advance, enabling reliable and timely planning for modernization.

In addition, lifecycle information is available as a new widget in the “Security & Compliance dashboard” and can also be flexibly integrated into “My dashboards”.

Improvements

- ▶ Project admins can allow IdP-managed users to enter 2FA restricted projects.
- ▶ Support for Unified Firewall containers with SPLA licenses
(requires firmware version LCOS FX 11.2 Rel)
- ▶ Improved lifecycle status display in the device list when hovering over the device name

Bug fixes

- ▶ Introduction of case-insensitive LTA user login, so that duplicates such as test@example.com and TEST@example.com are no longer permitted as two different users.

Improvements

- ▶ It is now visible when add-in instructions are skipped during configuration creation. When this happens a warning is created in the device log and the project log.

Bug fixes

- ▶ DPS graph refreshes every 10 minutes
- ▶ A scheduled firmware update does not offer the 'no update' option.
- ▶ LTA IdP automatic sync was not started every night.

Device reboot in scheduled events

The screenshot displays the R&S LANCOM Management Cloud interface. The left sidebar contains navigation options: Dashboard, Networks, Security, Sites, **Devices**, Add-ins, Project specifications, and Management. The main area shows the 'Devices' table with columns for Status, Name, Model, Serial Number, Site, IP Address, and Configuration. Several devices are listed, including Wuerselen-AP-E1.04, Hamburg-AP2, Wuerselen-GW, Hamburg-AP3, Wuerselen-AP-E2.01, Wuerselen-AP-E2.02, Vienna-AP1, Vienna-AP2, Sec-cld-fw01, Wuerselen-SW-Stack, Hamburg-AP1, Barcelona-AP1, Karlsruhe-AP1, Barcelona-GW, and Wuerselen-AP E2.03. The 'Configuration' column for all devices shows 'Up to date'. On the right, a sidebar menu is open, showing options like CONFIGURATION & FIRMWARE, Configuration roll out, Firmware update, Apply Add-in, Assign preconfiguration, Create device backup, Apply device backup, SITES, Assign to site, Remove from site, ALERTS, Mute, Unmute, OFFLINE ACKNOWLEDGEMENTS, Add, Remove, SCHEDULING, Schedule configuration rollout, Schedule firmware update, **Schedule device reboot**, MANAGEMENT, Open terminal, Open WEBconfig, Reboot, Transfer, Replace, and Remove. The bottom status bar shows '3 of 21 selected' and 'Guided Tour Project'.

In addition to configuration rollouts and firmware updates, you can now also schedule the reboot of selected devices in advance via the R&S®LMC – ideal, for example, if this is to take place outside of working hours. The process runs automatically, without any intervention from an administrator. To schedule a device reboot, select the desired components in the table within the “Devices” menu and choose the appropriate action from the three-dot menu in the “Scheduling” section. Under “Scheduled events” in the device table, you can keep track of all upcoming and completed processes, including their status.

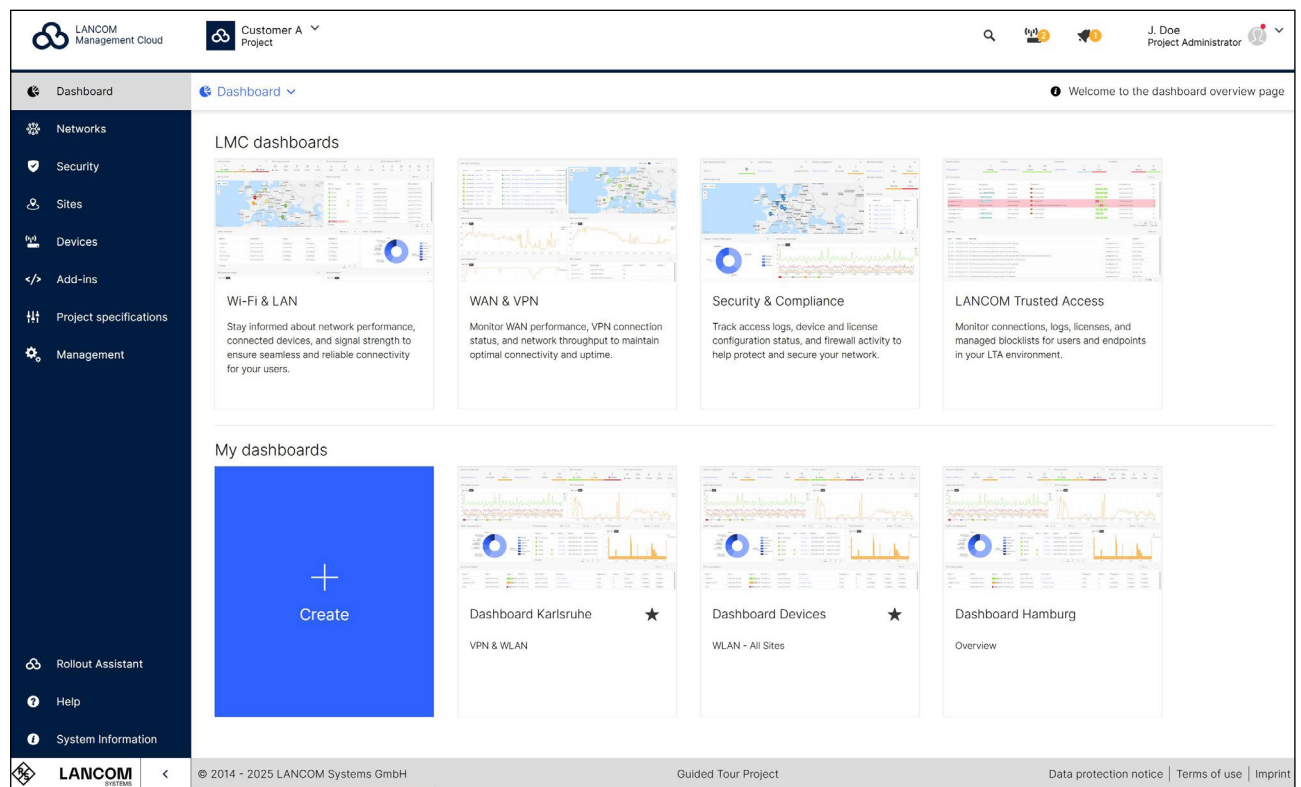
Improvements

- ▶ The lifecycle entry data for your devices is now displayed in the device table and in the device overview.
- ▶ Introduction of a new, filterable status ‘EOL approaching’, which is displayed 12 months before EOL, as well as a new lifecycle widget in ‘My Dashboards’.
- ▶ A new lifecycle icon will appear in the device table 3 months before EOL.

Bug fixes

- ▶ A problem with the full-screen floor plan view has been fixed.
- ▶ A problem with the visual representation of floor plans on small displays has been fixed.
- ▶ Bug fixes in the dynamic dashboard after launch
- ▶ R&S®LMC-wide persistence for sorting functions and table sizes
- ▶ Requesting multiple configuration rollouts in the R&S®LMC while a device is offline no longer results in multiple rollouts. Instead, only the last request is rolled out.
- ▶ When anomaly detection alerts are disabled, alerts are no longer displayed in the device overview.

Dashboard update for targeted monitoring



With the latest R&S®LMC update, your network monitoring is now even clearer and more flexible. The classic “R&S®LMC dashboards” and “My dashboards” are now based on the same framework and offer a unified set of tools for optimized monitoring. While “R&S®LMC dashboards” are customizable templates that help you get started quickly, “My dashboards” allow you to create personalized views and focus on the parameters that matter most to you. The enhanced overview page serves as your central hub: here, you can create, edit, and prioritize dashboards, mark favorites, and access everything with a single click. For more information, refer to the R&S®LMC help section and the [tech paper](#).

Improvements

- ▶ Improved navigation: Administrators can now switch move from the device overview to the floor plan and back.
- ▶ Config Journal - UI Integration

Bug fixes

- ▶ Fixed an issue with JSON variables during CSV site import.
- ▶ Fixed an issue that prevented alert details from opening in the device list.
- ▶ Fixed an issue where alerts in the device table displayed an endless spinner.

Secure admin user management via an identity provider

External user management

Integrating an OIDC Identity Provider (IdP) simplifies user login through single sign-on (SSO), enhances security with centralized identity management, and increases user convenience by reducing the need for multiple credentials.

In this section, you can manage your identity provider (IdP) configurations for OpenID Connect-based (OIDC) user authentication of your LMC organization. Use the 'Add IdP configuration' button to create a new entry, or select an existing one to edit or delete it.

[+ Add IdP configuration](#) [Delete](#)

☐	Status	Name	Issuer URL	Client ID	E-mail domains
☐	Enabled	Entra	https://login.microsoftonline.com/af3668f3-7*427-4abe-81722-3c52e847c/v2.0	b0550f04-a9af-1227-8126-f39552cd6f0d	✔ azure2lancom.onmicrosoft.com ⚠ acme.org

0 of 1 selected

R&S®LMC now supports direct login through your company's identity provider (IdP). After entering their e-mail address in R&S®LMC, admin users are automatically redirected to the IdP and authenticated there as part of the existing single sign-on process – without having to re-enter a password in the R&S®LMC. This enables all admin user accounts to be managed centrally within a unified identity management system. It also makes onboarding and offboarding new R&S®LMC administrators more secure while significantly reducing operational effort. At the same time, it strengthens your company's long-term security and ensures compliance with key access control regulations, such as required for meeting some of the NIS 2 regulations on network and information security.

The IdP can be configured in R&S®LMC via the "Management" menu under the "External admin user management" tab.

Improvements

- ▶ WeTransfer has been added to the R&S®LMC-based application list.
- ▶ Uplink auto and uplink trunk ports are now identified by different symbols.
- ▶ macOS 26 has been added to LTA endpoint security.

Bug fixes

- ▶ The automatic completion feature when manually creating new networks at a location has been corrected.
- ▶ The selection of device functions is no longer available for core switches.
- ▶ Improved platform security by updating a library used to create PDF files.

Convenient event planning for enterprise environments

The screenshot shows the LANCOM Management Cloud interface. The sidebar on the left contains navigation links: Dashboard, Networks, Security, Sites, Devices (highlighted), Add-ins, Project specifications, Management, Rollout Assistant, Live Chat, and Help. The main content area is titled 'Devices' and features a table with the following columns: Status, Name, Model, Serial Number, and License. A 'Select all' button is visible in the Status column. The table lists several devices, including 1800VAW-4G and 1926VAG-5G models. At the bottom of the table, it indicates '850 of 850 selected' and a pagination control set to '100 / page'.

Especially in large-scale installations with hundreds or even thousands of devices, you can now save valuable time and significantly reduce the administrative effort involved in event planning. Thanks to the new “All pages” selection option in the device table, you can select all devices across all pages with just one click. Then, using the three-dot menu under “Schedules,” you can easily carry out planned configuration rollouts or firmware updates for your entire device inventory.

Improvements

- ▶ The start date for licenses in the SPLA license CSV report has been changed to the date of initial licensing (available in the October report).
- ▶ The name of a device can now be specified in the ‘Claiming’ dialog box.
- ▶ Improved user feedback for validation errors when changing device names
- ▶ New wireless WAN widget in the device overview
- ▶ Audit log privacy mode only for inherited administrators
- ▶ The device transfer dialog is now searchable.
- ▶ User interface improvements for scroll bars on small devices (mobile phones)

Bug fixes

- ▶ Several minor issues in the ‘Floor Plans’ section of the website have been fixed.
- ▶ Irish postal codes for project addresses are now permitted.

Lifecycle at a glance: EOL status in the device table

Devices

+ Add device

Activation codes

Filter by ▾

 Scheduled events

Type: Switch ✕

☐	Status ▾	 ▾	Name ▲	Model ▾	Serial Number ▾	License	Site ▾
☐	 Online		GS-4554XP	 2 GS-4530XP	4006168920000019		Würselen-Switch-Stacking
☐	 Preconfigured		SW01	GS-3652XUP			
☐	 Online		Switch Athen	 GS-2310P	4003708420000207		Athen
☐	 Online		Switch Berlin	 GS-2310P	4003376020000083		Berlin
☐	 Online		Switch Dublin	 GS-2310P	4004058420000222		Dublin

Five years after official discontinuation, a device reaches EOL (end of life) status and, among other things, the entitlement to further firmware updates or support services ends. You can now see at a glance whether an EOL device and thus a potential security risk is in use in your R&S®LMC project: In the device table, a red icon appears next to the model name of EOL devices in the “Model” column. In addition, the lifecycle status (“Available”, “End of Sale”, or “End of Life”) is displayed in the device detail view.

Improvements

- ▶ Security improvements for API usage
 - ▶ To reduce potential security risks, especially with regard to accessing or storing log data, the authentication token is now forced to be included in the authorization header as a bearer token instead of being sent as a query parameter.
 - ▶ API keys with comprehensive rights are now given a validity date of no more than one year.
- ▶ Optimization of the input focus behavior in forms.

Bug fixes

- ▶ The behavior of the scrollbar in administrator tables has been corrected.
- ▶ Elimination of inconsistencies between warnings and device table.
- ▶ WiFi4EU: The appearance on small displays has been corrected.

Improvements

- ▶ If a device is at the end of its lifecycle status, this is displayed in the device overview.
- ▶ API keys can now be created at organization level (supports inheritance).
- ▶ The option for unlimited API keys for cross-account keys has been removed for security reasons (these API keys are now valid for a maximum of 1 year).

Bug fixes

- ▶ A problem with licensing of Unified Firewalls in SPLA has been solved.
- ▶ A problem with licensing LTA users has been solved.
- ▶ A problem with the configuration of Internet access when using LTA Full Tunnel has been solved.

Device configuration backup

The screenshot displays the 'Apply device backup' interface in the LANCOM Management Cloud. The top navigation bar shows 'Customer A' and 'Project'. The left sidebar contains various management tools. The main content area features a table of device backups. A dropdown menu is open for 'Group selection for all devices', showing options like 'No device backup', 'Manually created device backup', 'Latest device backup', and 'Latest device backup until'. The table lists three backup entries for SiteB and one for GW-SiteA, all with a status of 'Ok'.

Site	Firmware	Device backup	Status	Download
SiteB	10.92.0018	07.03.2025 11:37 - FW: 10.92.0018	Ok	Download
SiteB	10.92.0018	07.03.2025 11:37 - FW: 10.92.0018	Ok	Download
GW-SiteA	4005057132100011	07.03.2025 11:37 - FW: 10.92.0018	Ok	Download

At the bottom of the interface, there are buttons for 'Discard' and 'Apply 3 device backup(s)'. The footer contains copyright information and links to data protection notice, terms of use, and imprint.

Despite careful planning and technical support, configuration errors can never be completely ruled out and may lead to network disruptions. To quickly respond to such errors, the R&S®LMC now offers a backup and restore function for device configurations. This allows users to swiftly reset to a stable state, gaining valuable time for root cause analysis. By making precise comparisons between configuration versions, errors can be efficiently identified and corrected before rolling out the revised configuration to the device again.

Further details and instructions for use can be found in this [tech paper](#).

Authentication Notice: Removal of Basic Auth from API Documentation

As part of our ongoing efforts to enhance security and maintain high quality standards, the Basic Authentication method has been removed from our API documentation.

Please note: Technical support for Basic Auth will remain available until June 30, 2026, to allow for a smooth transition of existing integrations.

We strongly recommend switching to the officially supported, user-bound API keys, which offer a more secure and flexible way to authenticate.

If you have any questions regarding the use of API keys, please read our [Knowledge Base article](#).

Improvements

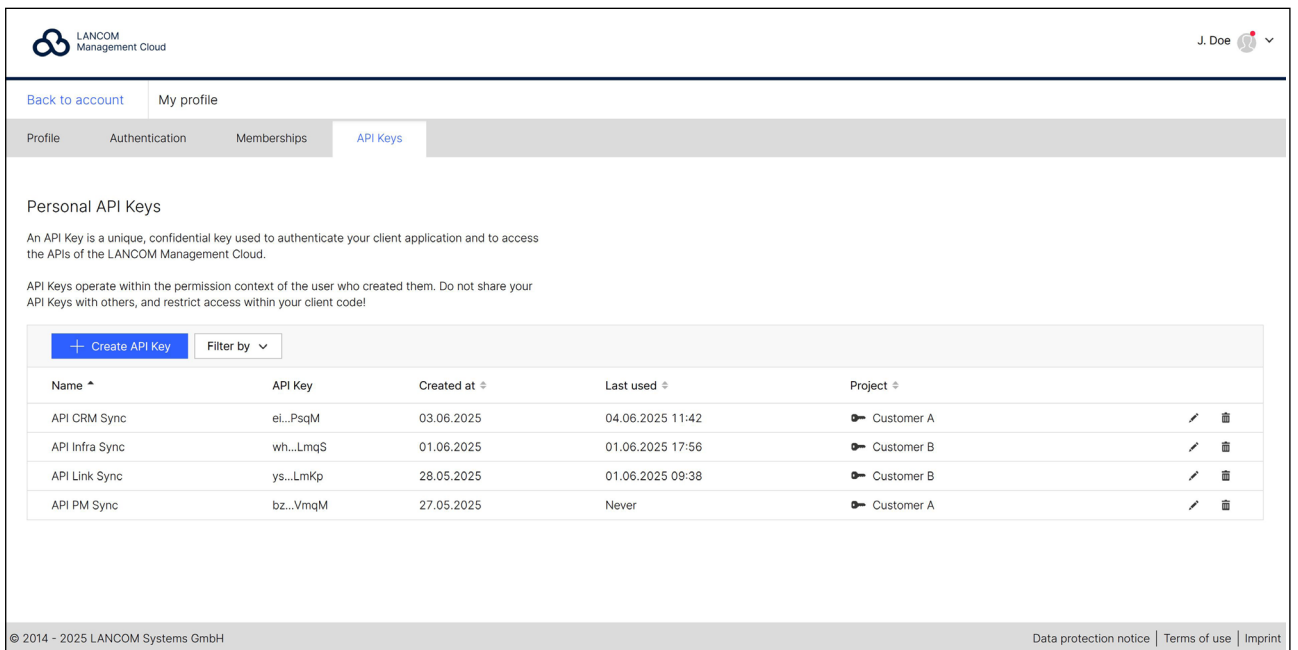
- ▶ The scrolling behavior of the location and administrator tables has been improved
- ▶ API keys can now optionally be given an expiration date

Please note: All keys already created have been assigned an initial expiration date of one year from the date of creation.

Bug fixes

- ▶ L7 app detection is now being activated on LAN and Wi-Fi interfaces of Wi-Fi routers, if the app detection shall take place on the router
- ▶ Switch templates on network level are now available for 12-port switch types
- ▶ JSON variables used in Add-ins now also support to access data through numeric indices

User-bound API keys for easy integration of third-party applications



The screenshot shows the LANCOM Management Cloud interface. At the top, the user is logged in as 'J. Doe'. The navigation bar includes 'Back to account' and 'My profile'. Under 'My profile', there are tabs for 'Profile', 'Authentication', 'Memberships', and 'API Keys'. The 'API Keys' tab is active, displaying 'Personal API Keys'. A text block explains that an API Key is a unique, confidential key used for authentication and access to the LANCOM Management Cloud APIs. It also states that API Keys operate within the user's permission context and should not be shared. Below this, there is a '+ Create API Key' button and a 'Filter by' dropdown. A table lists four API keys:

Name ^	API Key	Created at ^	Last used ^	Project ^	
API CRM Sync	ei...PsqM	03.06.2025	04.06.2025 11:42	Customer A	✎ 🗑
API Infra Sync	wh...LmqS	01.06.2025	01.06.2025 17:56	Customer B	✎ 🗑
API Link Sync	ys...LmKp	28.05.2025	01.06.2025 09:38	Customer B	✎ 🗑
API PM Sync	bz...VmQm	27.05.2025	Never	Customer A	✎ 🗑

At the bottom of the page, there is a footer with '© 2014 - 2025 LANCOM Systems GmbH' and links for 'Data protection notice', 'Terms of use', and 'Imprint'.

You can now create user-specific API keys directly under “My profile > API Keys”. These enable secure and flexible integration of third-party applications – without complex authentication procedures or additional configuration. The API keys operate within the access rights context of your user account, allowing all accesses and actions to be distinctly attributed to you. You decide whether access is project-related or cross-project. You gain more security and control through clear management of recent usage and transparent visibility in project and device logs.

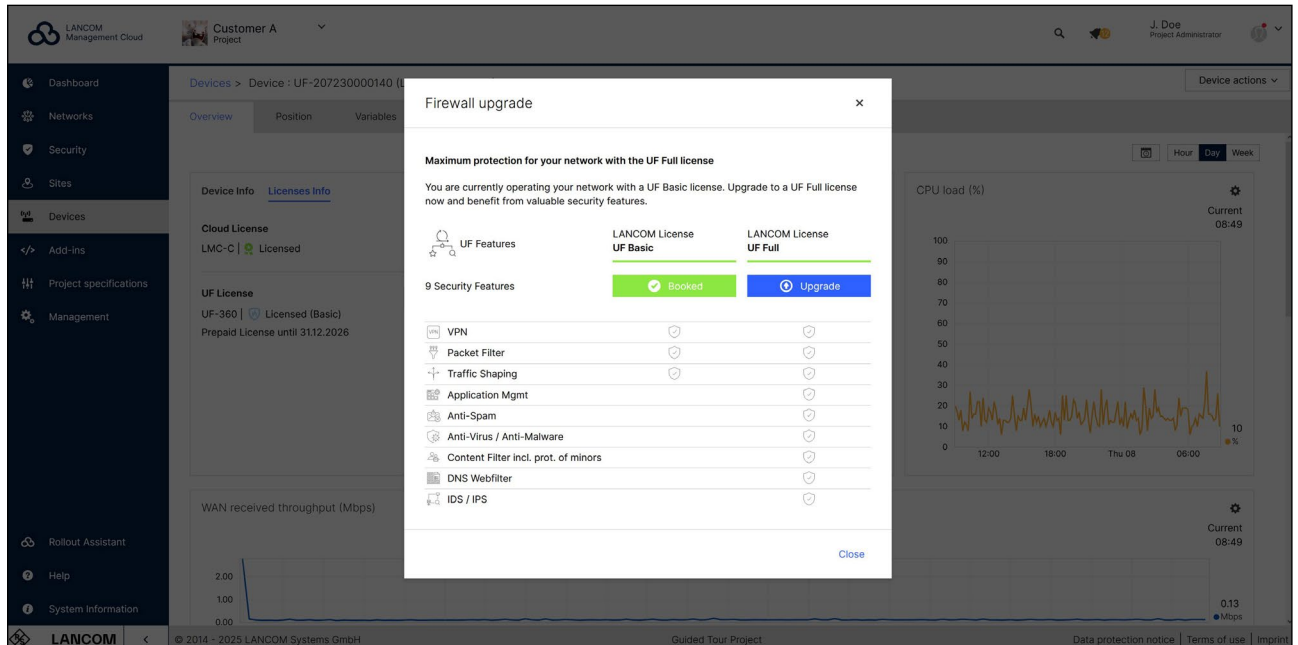
Improvements

- ▶ Support for LCOS 10.92 including the transition of filter categories from the R&S®LANCOM Content Filter Option to the R&S®LANCOM Security Essentials Option. An overview of the updated categories can be found [here](#).
- ▶ The individual port settings in the switches’ device overview now support the configuration of the PoE operation mode.

Bug fixes

- ▶ The Organization Administrator can change an inherited role of a project member to ‘Project Administrator’.
- ▶ DNS domains created from SmartConfig information no longer contain ‘_’.

Integration of R&S® LANCOM Unified Firewall licenses into your Service Provider License Agreement (SPLA)



Effective immediately, R&S® LANCOM Unified Firewall licenses can be billed monthly under your SPLA agreement, in addition to R&S® LMC licenses. This offers a simple and flexible way to manage licensing and costs – ideal for larger installations or tailored customer projects.

Activation takes place directly in the R&S® LANCOM Management Cloud, under the “License Info” tab of the respective device. There, the functionality of the Unified Firewall can be flexibly adjusted at any time by switching between license types (Basic or Full License). You can now also change the vFirewall variant as required (from S to XL).

Note: The monthly billing model requires a current SPLA contract with Rohde & Schwarz Networks and Cybersecurity.

Please contact your Rohde & Schwarz Networks and Cybersecurity sales team for further information.

Improvements

- ▶ Unused connection targets are not rolled out to Unified Firewalls as ‘Desktop Objects’ anymore.
- ▶ Header and footer of the device table are now permanently displayed when scrolling.

Bug fixes

- ▶ A problem with the automatic email delivery of the details report has been solved.

More transparency for scheduled events

Status	Time window	Type	Devices
Scheduled	18.04.2025 14:14 - 18.04.2025 14:29	Firmware update	16
Completed	14.04.2025 14:06 - 15.04.2025 14:06	Firmware update	14
Completed	09.04.2025 14:39 - 09.04.2025 14:54	Firmware update	35
Completed	09.04.2025 14:38 - 09.04.2025 14:53	Config rollout	10
Failed (Device does not respond)	08.04.2025 17:49 - 08.04.2025 18:04	Firmware update	1 (1 failed)
Completed	08.04.2025 17:43 - 08.04.2025 17:58	Firmware update	18
Failed (Time window expired)	01.04.2025 11:36 - 01.04.2025 12:51	Config rollout	22 (2 failed)
Completed	27.03.2025 15:30 - 27.03.2025 15:45	Config rollout	18
Completed	27.03.2025 15:14 - 27.03.2025 15:29	Config rollout	24
Completed	26.03.2025 11:08 - 26.03.2025 11:23	Firmware update	10
Completed	21.03.2025 10:55 - 21.03.2025 11:10	Config rollout	75
Completed	20.03.2025 09:50 - 20.03.2025 10:05	Config rollout	82
Failed (Event error)	19.03.2025 14:10 - 19.03.2025 14:25	Config rollout	2 (1 failed)
Completed	19.03.2025 08:07 - 19.03.2025 08:22	Config rollout	12

The new update makes your scheduled events even more transparent: planned configuration rollouts and firmware updates can now be filtered, managed, and optimized more precisely. An enhanced overview with additional details, along with a new, detailed results page for your planned events, gives you a comprehensive view of the status of each individual process and also simplifies error analysis and troubleshooting.

You can also learn more about the detailed “scheduled events” process in our [tech paper](#).

Improvements

- ▶ Added Irish/Gaeilge language for hotspot networks
- ▶ The configuration of the automatic firmware updater is now available for switches with LCOS SX 4.30.
- ▶ Variables for Add-ins can now be defined with type JSON to provide complex data into the JavaScript of the Add-ins.

Bug fixes

- ▶ The WAN anomaly icon did not correctly disappear after the alert was closed.
- ▶ Corrected the deletion process of variables.
- ▶ Changes in Add-ins assigned to networks will not affect devices which are not assigned to the same network.

Update for Active Power Control: Smart power management for R&S® LANCOM devices

LANCOM

Management Cloud

APC-ActivePowerControl

Project

Search

fyti

J. Doe
Project Administrator

Dashboard

Networks

Security

Sites

Devices

Add-ins

Project specifications

Management

Rollout Assistant

Help

System Information

Project specifications > Active Power Control

About Active Power Control

Active Power Control (APC) manages and optimizes power consumption of LANCOM network equipments and offers insights into project energy usage by site, and device type. Key features include the LANCOM Sustainability Mode, which reduces power consumption of access points during low activity periods, without impact on user experience. APC also delivers comprehensive energy consumption reports and retains data for 18 months, ensuring accurate insights for sustainable energy management.

☒ LANCOM Sustainability Mode: Reduction of Access Points capabilities in case of inactive clients

Devices

81

321.07 kWh

1,605.35Wh

Total devices in project

Project energy consumption (current month)

Project energy consumption (current year)

Energy consumption per device type (current month)

Device type	Energy consumption (kWh)	LANCOM network devices included	LANCOM network devices not included
Access Point	202.33	63	0
Switch	74.57	9	0
Router	27.38	5	0
Firewall	16.79	5	0
Unknown	0	0	1

Energy consumption per site (current month)

Filter by

Site name	Energy consumption (kWh)	LANCOM network devices included	LANCOM network devices not included
Berlin	121.41	32	0
Munich	81.49	22	0
Hamburg	33.37	8	0
Cologne	57.92	14	1
Frankfurt	26.88	6	0

Energy consumption report

Generate report for current month

Month	Reports
February 2025	Download report
January 2025	Download report
December 2024	Download report
November 2024	Download report

Active Power Control (APC) is an intelligent solution for sustainable network management. It offers a transparent view of the power consumption of R&S® LANCOM devices – broken down by project, location, or device type – and reveals energy-saving potential through the already integrated “R&S® LANCOM Sustainability Mode”. The latest update expands the reporting capabilities and now provides new monthly and annual views of key energy consumption metrics, as well as detailed consumption reports in Excel format. Based on consumption data, device analyses, and clear visuals, APC helps you identify trends and uncover optimization potential.

A full overview of APC features is available in the corresponding [tech paper](#) or directly in the R&S® LMC information area under > Project specifications > Active Power Control.

32

Rohde & Schwarz Networks and Cybersecurity | Release Notes - R&S® LMC Software Release 1.00.209.0

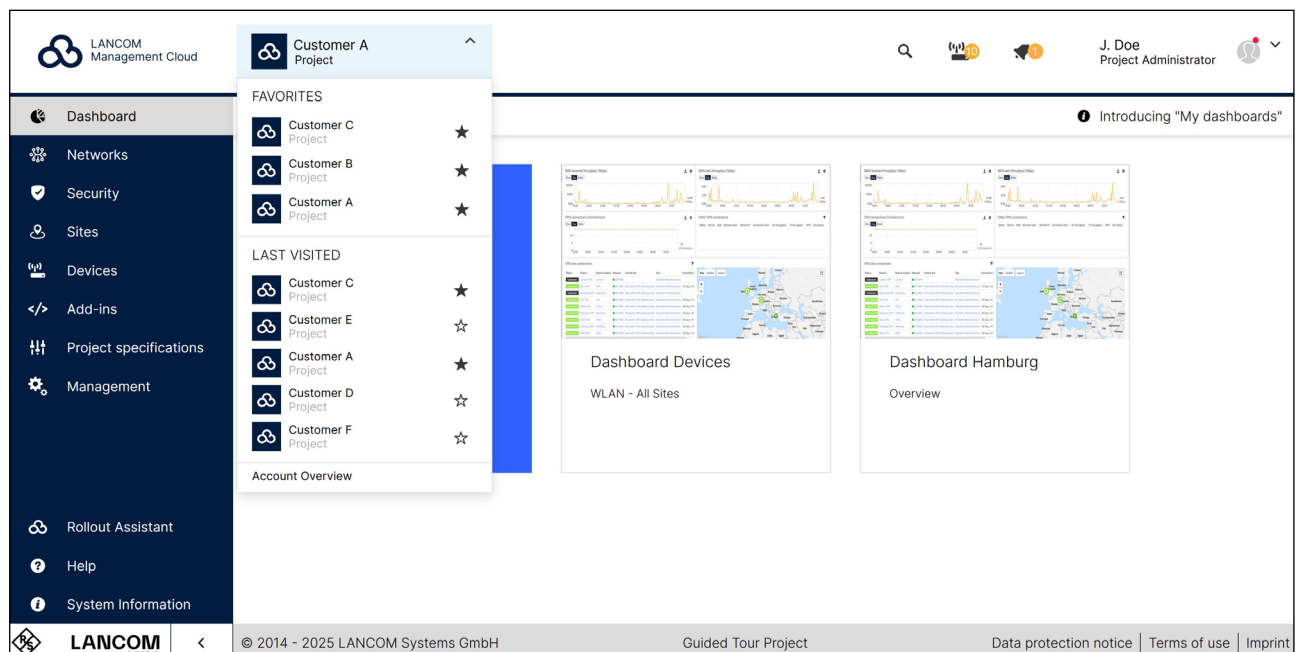
Improvements

- ▶ The display of the status of the Unified Firewall stack during synchronization has been optimized.
- ▶ Improved views and help texts

Bug fixes

- ▶ The R&S®LMC now deactivates the 6 GHz band for access points that are operated in outdoor mode.
- ▶ Reduced log messages when a configuration with LAGs is carried out for a switch.
- ▶ Custom applications based on the DPS protocol do not create configuration objects that are not accepted by an LCOS device.
- ▶ A problem with the display of project favorites after a name change has been fixed.

Increased efficiency through direct project navigation



Administrators managing multiple projects within their organization can now benefit from direct and seamless access to up to five favorite projects. These projects can be easily marked as favorites in the “account overview” or the account selection menu and remain accessible from there. The optimized navigation enables quick project switching, making daily workflows even more efficient.

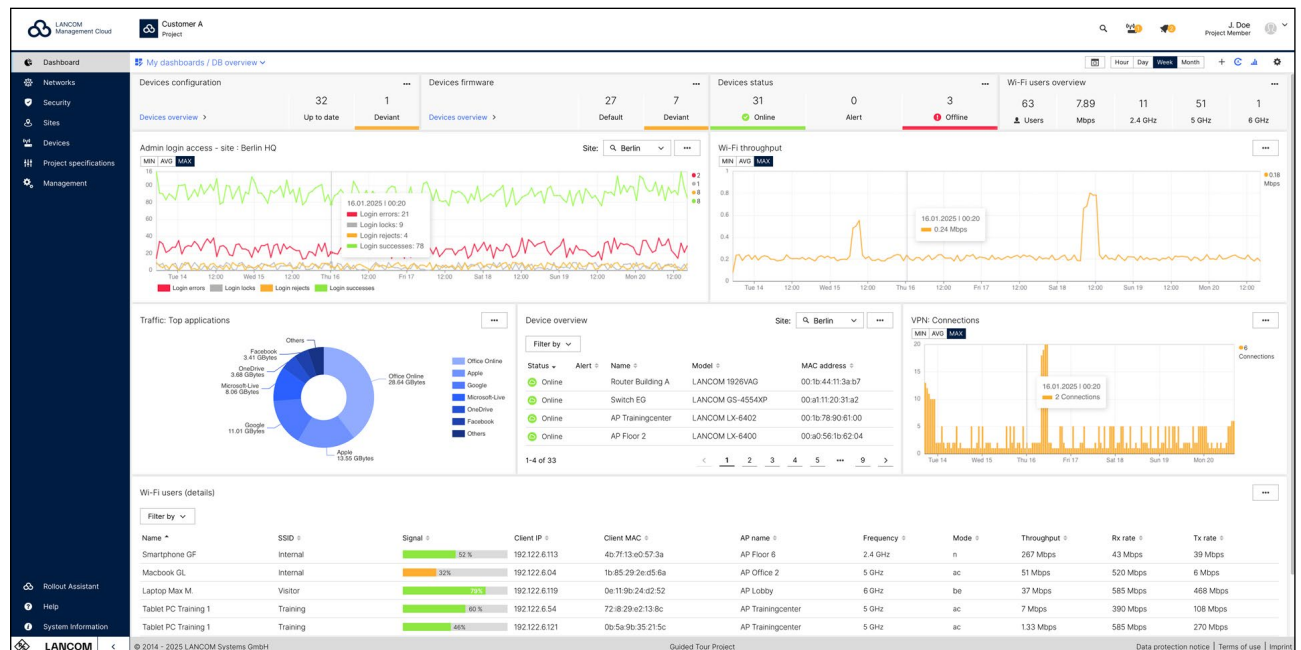
Improvements

- ▶ Improved error and status messages and a better overview on the ‘scheduled events’ page
- ▶ Support for reduced animations on the main page of the user interface
- ▶ It is now possible to use DynDNS domains with LTA.

Bug fixes

- ▶ If activated, 2-factor authentication is now also used for account deletion.
- ▶ Existing masquerading settings are used in the routing table.
- ▶ Several problems with the ‘Site overview’ widget have been fixed.

My dashboards: A milestone for network monitoring and troubleshooting



With “My dashboards”, you can design your monitoring according to your personal requirements. Customizable dashboards and practical monitoring tools allow you to keep an eye on network events, identify errors faster, and optimize workflows – for maximum productivity.

Individual dashboards: Create up to 11 custom dashboards per project, with flexible layouts, widgets, and filters for a personalized monitoring.

Efficient troubleshooting: The improved filter system enables you to perform targeted analyses at device or location level and hides information that is not required. New, time-synchronized diagram tooltips allow you to correlate events at a glance.

In-depth analysis: Quickly selectable data values (minimum, average, maximum), customizable time intervals, and extended data storage (up to one month) help you make precise and well-founded decisions.

Optimized visualization: Add widgets and customize metrics, visualization types, filters, sizes, and positions according to your needs. Alternative chart types and dynamic layout adjustments enhance clarity, making complex data easier to interpret.

Risk-free testing: “My dashboards” are only visible to you. Take advantage of the opportunity to try out new configurations without affecting your colleagues’ workflows.

Of course, the regular dashboards remain available and can still be used as usual.

You can find a detailed overview of your options and instructions for creating your personal dashboards directly in the R&S® LMC, in the dashboard’s information area, as well as in this [techpaper](#).

Improvements

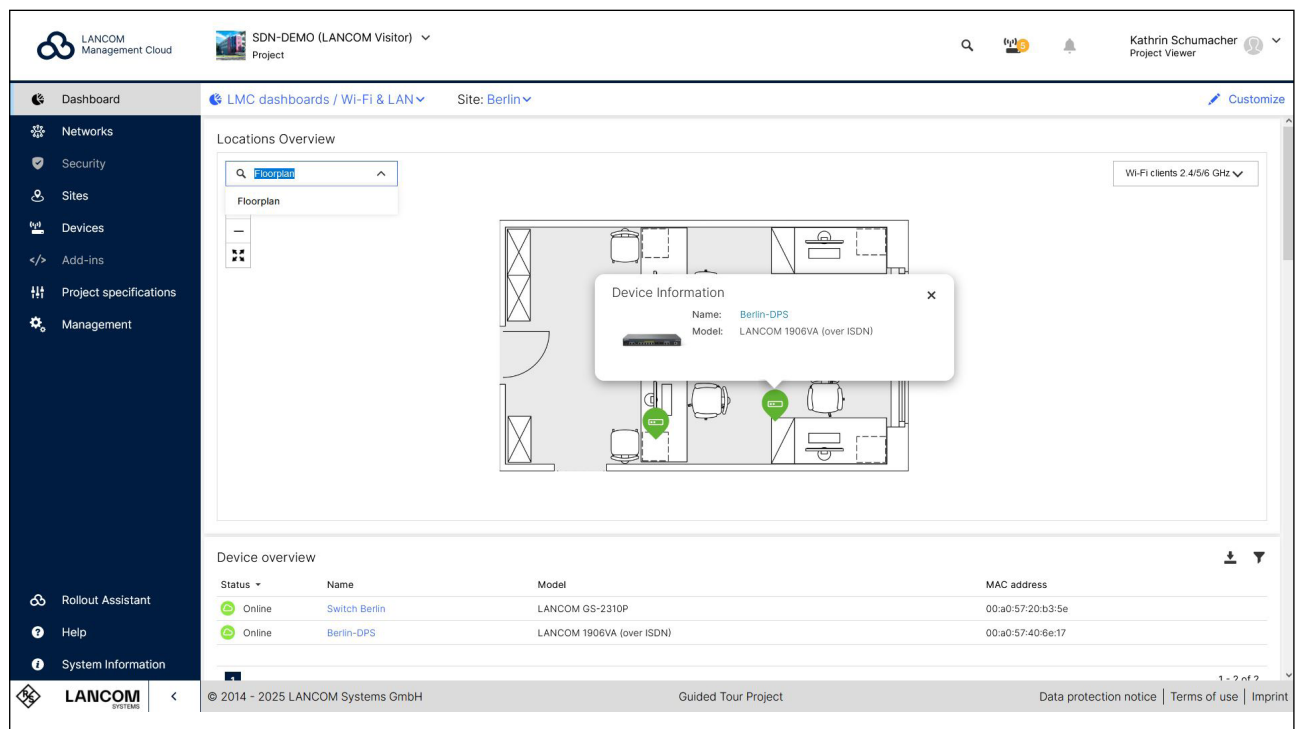
- Support for reduced animations in the help slider depending on the OS setting.
- Administrators can now use the system variable ROLLOUT_ENABLED to temporarily disable the rollout for specific

devices or locations.

Bug fixes

- ▶ The handling of fields with hashed passwords in the detailed configuration of switches has been corrected.
- ▶ BPjM content filter rules are now supported for devices with LCOS FX-I.
- ▶ A problem with switching sites in the 'Site overview' widget has been fixed.
- ▶ Fixed an issue where the drop-down menu for swapping floor plans did not respond when maximized.

Features for more overview and more convenience



In addition to developing new features, we continuously work on optimizing user-friendliness to make workflows more efficient and intuitive. Two recently implemented improvements are:

► Optimized use of floor plans:

In the “Location Overview” dashboard widget as well as under “Locations” → “Floor plans”, you can now use full-text search to quickly find the desired floor plan for a selected location. The new full-screen view option gives you an improved overview—especially for highly detailed floor plans. The devices marked on the floor plan are now linked, so you can see the device details in the device view with just one click.

► Improvements in browser history and tab management:

The new, descriptive tab names improve clarity and also make it easier to navigate your browser history. Furthermore, individual locations and projects can now be opened in separate tabs (e.g., via the “Locations” menu: right-click on the desired location → “Open in new tab”). Ideal if you want to keep an eye on multiple networks at the same time.

Do you have any further suggestions for improving the user-friendliness of the R&S® LANCOM Management Cloud?

[Feel free to let us know!](#)

Improvements

- ▶ When filling in form fields, error messages regarding unfulfilled input requirements are no longer displayed immediately.

Bug fixes

- ▶ Fixed a display error in the organization dashboard when more than 20 projects were listed.
- ▶ The member list is now loaded correctly regardless of the number of users.
- ▶ After starting and ending an ACR 2.0 scan, the ARC 2.0 device page now displays the correct text for an offline device.
- ▶ The error message “Not accepted” after updating a R&S®LANCOM GS-3510XP from LCOS 4.30 RU3 to LCOS 4.30RU4 and subsequent reboot has been fixed.
- ▶ The WPA3 Enterprise configuration is now also possible for a R&S®LANCOM LN-630acn dual Wireless.
- ▶ If many VLANs are stored for a switch, these are no longer cut off in the switch port configuration.

Scheduled events in the R&S® LANCOM Management Cloud

Schedule configuration rollout

Scheduling allows you to perform configuration rollouts within a defined time window. Rollouts will be performed sequentially as determined by position of device model groups within the table below, with each rollout group starting only when the previous group is finished. By default, the order is given by the type of each device model groups - access points are at the top, followed by switches, routers, and firewalls. You can change the order by dragging rows inside the table to a new position.

Order	Count	Model	Device type
#1	15	LX-6402	Access Point
#2	2	GS-4530XP	Switch
#3	1	1803VA	Router
#4	1	UF-260	Firewall

Expert settings

By default, a scheduled configuration rollout event will be stopped if any configuration rollout fails. By selecting the option "ignore failed devices", you can allow the rollout process to continue even if a configuration rollout fails.

- ☐ Automatically roll out potentially dependent Central Site devices
- ☒ Start configuration in test mode after roll out (recommended!)
- ☐ Ignore failed devices

Time window

The valid time window length is minimum 15 minutes and maximum 24 hours. Please note that executing scheduled updates may exceed the defined time window by up to 30 minutes. Please adjust your time window accordingly.

Start: 25.01.2025 10:30 End: 25.01.2025 12:30 Time window: 2 hours 0 minutes

Discard Create

© 2014 - 2025 LANCOM Systems GmbH | Guided Tour Project | Data protection notice | Terms of use | Imprint

Configuration rollouts and firmware updates can now be planned in advance and executed automatically, eliminating the need for active administrator involvement. All that is required is to define the time window and select the respective devices beforehand.

By default, the R&S® LANCOM Management Cloud organizes the selected devices by model type and updates them one after the other to ensure smooth operation—from access points and switches to firewalls and routers.

Scheduling new events is simple: In the “Devices” menu, select the desired components in the table, choose the desired action (configuration rollout or firmware update) via the three-dot menu under “Scheduling”, and customize additional details and options for smooth operation.

For a clear overview, the “Scheduled events” button in the device table view provides a complete list of all upcoming and previous updates at a glance.

If you need detailed information on “scheduled events”, please take a look at our [techpaper](#).

You can also look forward to continuous improvements and even more new features in this area. We will keep you updated.

Improvements

- Users can now open projects and sites in new tabs by right-clicking.
- Floor plans can now be displayed in full screen mode in the widget ‘Site overview’.
- The list of floor plans in the ‘Site overview’ widget can now be filtered.
- Improved table of floor plans in the site management section.

Bug fixes

- ▶ A problem with the site list in the dashboard when switching between projects has been fixed.
- ▶ A problem with the display of an offline secondary device in an HA cluster in the cluster view has been fixed.
- ▶ Improved consistency of SSID / Wi-Fi network names containing a space in the add-ins.
- ▶ Protocol-based applications for DPS can be created and edited correctly again.
- ▶ In the detail configuration, when switching between basic and rollout configuration, the row selection is reset.
- ▶ SNMPv3 users can be set correctly in the detail configuration of the GS-3xxx switches.
- ▶ DHCPv6 reservations are handled correctly in the LCOS detail configuration.
- ▶ The weighting of an access point for ARC 2.0 is taken into account again.

4. History of incompatible API changes

R&S®LANCOM Management Cloud 1.00.207.0 / 24.06.2026

The field 'WarrantyEndDate' will be removed from multiple APIs after 06.10.2026, including

- ▶ GET /cloud-service-devices/accounts/{accountId}/device/{deviceId}
- ▶ GET /cloud-service-devices/accounts/{accountId}/devices

R&S®LANCOM Management Cloud 1.00.205.0 / 12.05.2026

- ▶ Deprecated GET /cloud-service-auth/users/self/invitations
New/ replace with: GET /cloud-service-auth/users/self/memberships
- ▶ Deprecated GET /cloud-service-auth/users/self/invitations/{invitationId}
New/ replace with: GET /cloud-service-auth/users/self/memberships/{membershipId}
- ▶ Deprecated POST /cloud-service-auth/users/self/invitations/{invitationId}
New/ replace with: POST /cloud-service-auth/users/self/memberships/{membershipId}
- ▶ Removed GET /cloud-service-auth/auto-logout-setting
New/ replace with: GET /cloud-service-auth/settings/auto-logout
- ▶ Removed GET /cloud-service-auth/dpa/unaccepted
New/ replace with: GET /cloud-service-auth/dpa/{accountId}/unaccepted

R&S®LANCOM Management Cloud 1.00.198/199.0 / 16.12.2025

- ▶ Removed 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
See release notes for sprint 175 for deprecation note

R&S®LANCOM Management Cloud 1.00.178.0 / 29.10.2024

- ▶ Removed endpoints (deprecated note June 2022)
GET/POST /cloud-service-auth/accounts/{accountId}/custom-fields
GET/POST/DELETE /cloud-service-auth/accounts/{accountId}/custom-fields/{fieldId}
GET /cloud-service-auth/custom-field-targets
GET /cloud-service-auth/custom-field-targets/{targetId}

R&S®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

R&S®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

5. General advice

Disclaimer

Rohde & Schwarz Networks and Cybersecurity does not take any guarantee and liability for software not developed, manufactured or distributed by Rohde & Schwarz Networks and Cybersecurity, especially not for shareware and other extraneous software.

Rohde & Schwarz Networks and Cybersecurity GmbH
Adenauerstr. 20/B2
52146 Wuersele | Germany
info.rs-nc@rohde-schwarz.com | www.rohde-schwarz.com/networks-and-cybersecurity

R&S and Rohde & Schwarz are trademarks of Rohde & Schwarz GmbH & Co. KG, registered or used, among others, in Germany, the EU, the USA, China, and other countries. Other names or designations used may be registered trademarks of different companies or owners. This document contains forward-looking statements regarding products and product features. The publisher reserves the right to change these at any time without stating reasons. No liability is accepted for technical inaccuracies or omissions.

ROHDE & SCHWARZ
Make ideas real

