Konzepte der LANCOM Management Cloud (LMC)

Ein gut funktionierendes Netzwerk ist das Herz eines jeden Unternehmens. Es aufzubauen und zu steuern ist jedoch eine hochkomplexe Angelegenheit. Zudem ist der Fachkräftemangel allgegenwärtig: qualifizierte Netzwerkexperten sind immer schwieriger zu finden. Gleichzeitig ist die traditionell manuelle Konfiguration zeitaufwändig, fehleranfällig und führt damit zu viel zu hohen Kosten.

Was wäre, wenn es eine intelligente, höhere Instanz gäbe, die das gesamte Netzwerk von zentraler Stelle aus automatisiert und steuert? Eine Art Intelligenz, die alle wichtigen Komponenten vernetzt, jederzeit dynamisch auf neue Anforderungen reagieren kann und dabei auch noch sicher ist.

Klingt wie ein Zukunftsszenario – ist es aber nicht. Mit der LANCOM Management Cloud (LMC) gibt es die vollständig integrierte Lösung. Beleuchten wir im Folgenden einige grundlegende Konzepte der LMC, wobei die beschriebenen Vorgehensweisen und Arbeitsschritte keine vollständige Anleitung zur initialen Konfiguration eines LMC-Projektes bieten. Hierzu wie auch zu anderen Themen empfiehlt sich der Besuch eines entsprechenden LANCOM Trainings.

Folgende Inhalte werden in diesem Techpaper behandelt:

1. Das Konzept – Design first, deploy hardware later
2. Die Organisationsebenen
   - Organisationen
   - Projekte
3. Die Netzwerkkonfiguration
   - Netze
   - Sicherheit
   - Standorte
   - Geräte
4. Rollen
5. Dashboards
6. Erweiterte Funktionen
7. Support

Das Konzept – Design first, deploy hardware later

Mit der LMC verändert sich der Workflow bei der Definition und Einrichtung eines Netzwerks. Bisher benötigen Sie Experten, die das Netzwerk definieren und anschließend jedes Gerät manuell konfigurieren. Häufig geschieht dies vor Ort, somit müssen die Experten zu jedem Standort eines Unternehmens reisen. Als Folge stehen die gut geschulten Experten nur mit einem Bruchteil ihrer realen Arbeitszeit für die Tätigkeiten zur Verfügung, für die Sie ihr Know-How erworben haben.

Mit der LMC designt ein Experte das komplette Netzwerk über eine benutzerfreundliche Weboberfläche und muss dafür nicht ein einziges Gerät real anfassen. Dabei nimmt die LMC einem viele Details ab, die sonst einzeln manuell für jedes Gerät konfiguriert werden. Sollen VPNs zwischen den Standorten eingerichtet werden, welche SSIDs werden wo verwendet, sollen VLANs verwendet werden? Die eigentliche Konfiguration auf allen Geräten übernimmt dann die LMC. Das ist nicht einfach ein zentrales Management, sondern der Blick auf die gesamte Infrastruktur eines Unternehmens.

Mit dem Rollout auf die Geräte erfolgt dann die komplette Konfiguration jedes Gerätes durch die LMC. Sobald nun ein Techniker an einem Standort die vom Experten vorher geplanten und im Projekt bekannt gemachten Geräte anschließt, melden diese sich bei der LMC und bekommen ihre Konfiguration von der LMC bzw. können nun vom Experten konkret innerhalb eines Projektes zugeteilt werden. Die Geräte am neuen Standort sind somit nach dem Anschluss innerhalb weniger Minuten betriebsbereit.

Betrachten wir nun die Elemente der LMC, die für diesen Workflow benötigt werden: Organisationen, Projekte, Netze, Sicherheit, Standorte und Geräte.

Die Organisationsebenen

Organisationen

Eine Organisation ist die höchste Ebene in der LMC-Architektur und den Projekten übergeordnet. Da die LMC sich an LANCOM Partner wendet, können nur diese als Organisation innerhalb der LMC angelegt werden. Der Partner kann dann für jeden seiner Kunden, den er über die LMC verwalten will, ein Projekt anlegen.

Falls ein Endkunde sein Netzwerk selbst verwalten will, ist dies möglich, aber er muss sich an einen LANCOM Partner wenden, der ihm wiederum ein Projekt innerhalb seiner Organisation anlegt.

Projekte

Projekte entsprechen den durch den Partner betreuten Kunden. Sprich: Für jeden Kunden kann man ein eigenes Projekt anlegen, in welchem alle Kundendaten abgelegt und globale, standortübergreifende Einstellungen vorgenommen werden. So hat man auf der Projektebene beispielsweise auch Einblick in den Lizenzpool für die in diesem Projekt verwalteten Geräte und über die Laufzeit der Gerätelizenzen.

Zum Thema Lizenzmanagement wie auch zu anderen Themen der LANCOM Management Cloud gibt es hilfreiche Tutorial-Videos.

Die Netzwerkkonfiguration

Netze

Auf der Ebene Netze werden globale Vorgaben für bestimmte Anwendungen innerhalb eines IP-Adressbereichs definiert. So lassen sich beispielsweise ein Entwicklungs- von einem Buchhaltungsnetz logisch voneinander trennen und innerhalb dieser Netze unterschiedliche Zugriffsberechtigungen zuweisen. Diese global definierten Netze können anschließend allen gewünschten Standorten zugewiesen werden, sodass z. B. ein Hotspot-Netz an allen Unternehmensstandorten in gleichen Design und den gleichen Zugangsdaten bereitgestellt werden kann.

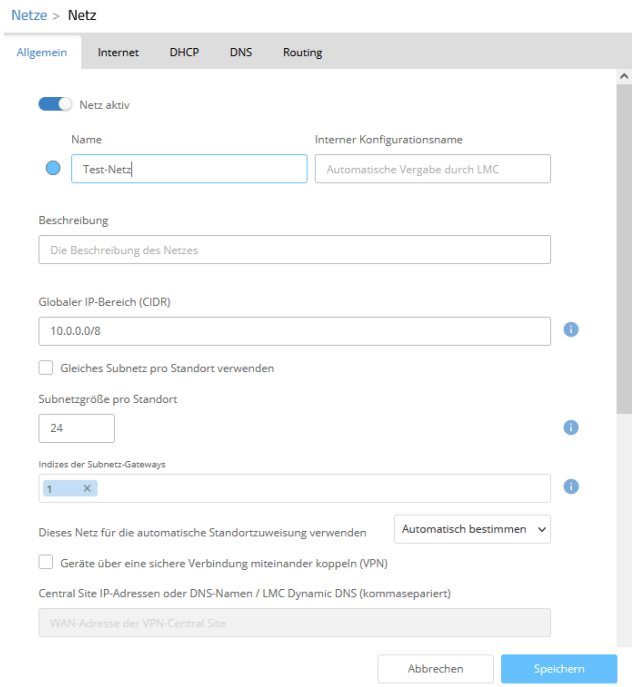

Abbildung 1:
Neues Netz erstellen

Ein Netz hat als erstes einen Namen, z. B. Gäste, Sales, LAN. Als nächstes einen IP-Adress-Bereich, z. B. ein Class-B-Netz 10.0.0.0/16. Zusammen mit der Definiton der Größe der lokalen Subnetze an einem Standort (z. B. /24 für Class-C-Netze) wird dann bei der Zuordnung des Netzes an einen Standort aus dem Bereich des Class-B-Netzes diesem Standort automatisch ein Class-C-Netz zugewiesen. Als nächstes legen Sie für ein Netz fest, ob die Standorte in diesem Netz über ein IPSec-VPN verbunden werden sollen. In diesem Fall werden dann bei Zuweisung dieses Netzes an mehrere Standorte automatisch VPN-Verbindungen zwischen diesen Standorten und der Zentrale erzeugt. Die LMC erzeugt somit immer ein sternförmiges VPN-Netz ausgehend von den Filialstandorten zu einer Zentrale.

Genauso können Sie einem Netz eine VLAN-ID zuweisen. Diese wird dann automatisch an alle Standorte ausgerollt, bei denen dieses Netz verwendet wird. Somit sind die Daten in diesem Netz automatisch mit dieser VLAN-ID getaggt. Dies dient der Trennung der Netze und ist u. a. notwendig, wenn mehr als ein Netz an einem Standort betrieben werden soll.

Über praktische Templates für jedes Switch-Modell (8-Port, 10-Port, 26-Port, etc.) lassen sich zudem die einzelnen Netze bestimmten Switch-Ports zuweisen. Somit ist die Portbelegung später an allen Standorten einheitlich vorgegeben und ein Techniker kann vor Ort die Verkabelung immer identisch vornehmen.

Alle diese Einstellungen für das Netz (VPN, VLAN, ...) nehmen Sie genau einmal vor und diese werden dann für alle Standorte automatisch angewendet.

Als letztes weisen Sie jedem Netz eine individuelle Farbe zu. Diese hilft z. B., die Zuordnung der vorhandenen Netze auf die Ports zu erkennen; gerade auch, wenn Sie eine Portbelegung individuell anpassen, um z. B. die Definition an ein bereits bestehendes Netz anzupassen.

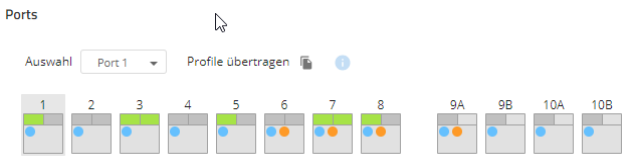

Abbildung 2: Ports

Auch eine WLAN-SSID mit einigen Optionen wie z. B. die Art der Verschlüsselung können Sie hinzufügen. Diese ist dann automatisch an den Standorten mit diesem Netz verfügbar, wenn dort ein Access Point angeschlossen wird.

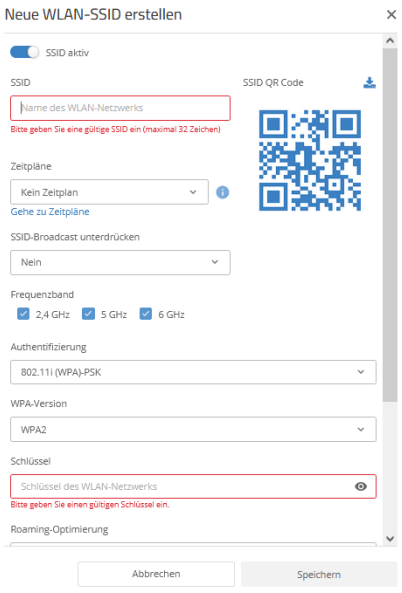

Abbildung 3: Neue WLAN-SSID erstellen

Weiterhin richten Sie mit wenigen Klicks ein Hotspot-Netz ein, welches dann an allen gewünschten Standorten verfügbar ist. Weiterführende Informationen erhalten Sie im Techpaper „Cloud-managed Hotspot“.

Stellen Sie zudem ein, über welchen Weg die jeweiligen Standorte ihren Weg ins Internet finden sollen. Sie haben die Wahl zwischen einem direkten lokalen Breakout, über die Zentrale oder aber über den Security-Dienstleister Zscaler.

Die Anbindung an Zscaler erfolgt über den Tab „Internet-Security“ im jeweiligen Standort. Beachten Sie, dass Zscaler separat bei der gleichnamigen Firma lizenziert und eingerichtet werden muss.

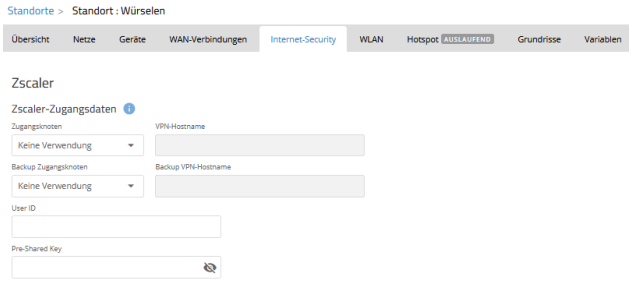

Abbildung 4:
Netz bearbeiten

Sicherheit

Mit dem Menüpunkt „Sicherheit“ behalten Sie Ihre Sicherheitseinstellungen an einem Ort im Blick. Für jedes Netz Ihres LMC-Projektes wird automatisch ein Sicherheitsprofil angelegt bzw. Ihre bereits bestehenden Einstellungen und Regeln dorthin migriert. Dort können Sie Regeln wie z. B. für Application Management, Content Filter und Paketfilter global für alle Netze anlegen und diese den entsprechenden Sicherheitsprofilen zuweisen. Unter Sicherheit > Profile erkennen Sie übersichtlich, welche Sicherheitsfunktionen im jeweiligen Netz greifen. Eine Schritt-für-Schritt-Anleitung entnehmen Sie gern unserem Techpaper „Cloud-managed Security“.

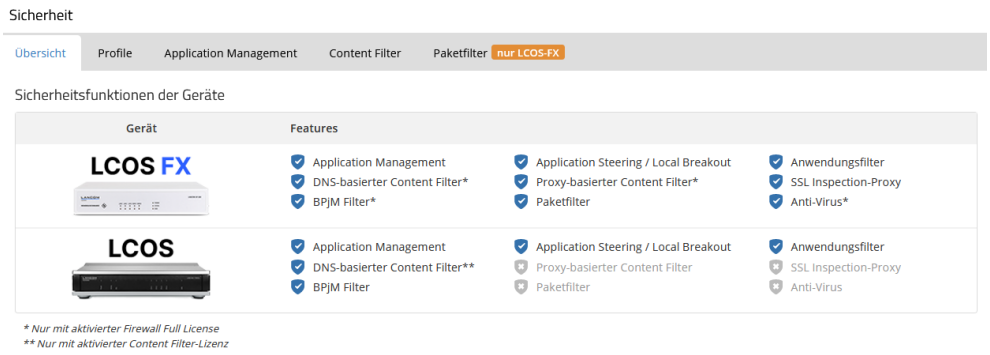

Abbildung 5:
Sicherheit

Standorte

Im nächsten Schritt legen Sie die Standorte an. Hier verknüpfen Sie die für das Netz getroffenen Vorgaben mit dem Standort. Gleichzeitig weisen Sie auch Geräte dem Standort zu. Dadurch erhalten diese Geräte die für diesen Standort getroffenen logischen Vorgaben.

Geben Sie die komplette Adresse des jeweiligen Standorts an, damit dieser korrekt auf der per Google Maps eingebundenen Karte angezeigt wird.

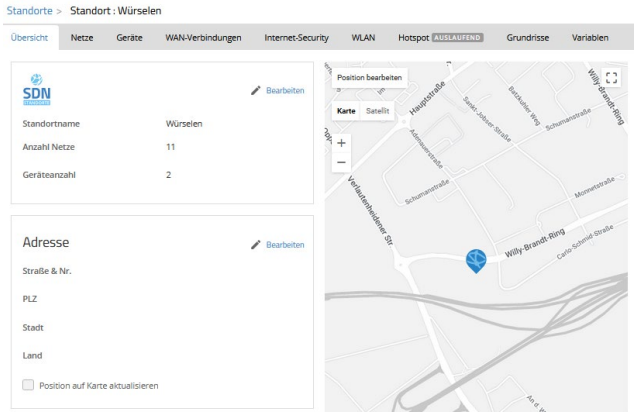

Abbildung 6: Standorte

Laden Sie optional Pläne der Gebäudestruktur des Standorts hoch. Auf diesen können Sie später die Geräte platzieren. Bei Access Points wird dann später im Dashboard die ungefähre Ausleuchtung des Funkfeldes angezeigt.

Dies kann natürlich keine Ausleuchtungsanalyse des Standorts ersetzen, da z. B. die Materialien der Wände nicht bekannt sind und daher auch nicht berücksichtigt werden können.

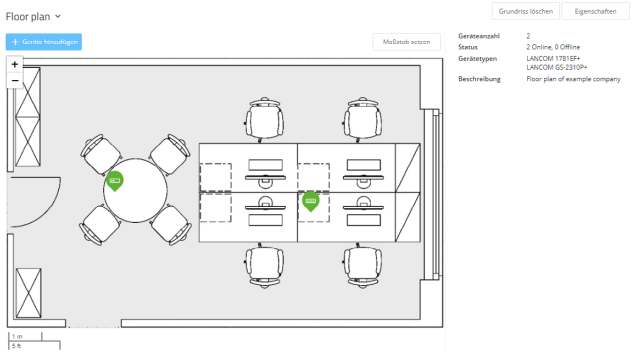

Abbildung 7: Gebäudeplan

Geräte

Die Basis jedes Netzes sind die Geräte, aus denen dieses gebildet wird: Gateways / Router, Switches, Access Points und Firewalls.

Jedes aktuelle LANCOM Gerät – auch virtuelle wie z. B. vRouter oder vFirewall – können Sie in der LMC über seine Seriennummer und die beigelegte Cloud-PIN innerhalb eines Projektes bekannt machen. Alternativ können Sie in der LMC einen Aktivierungscode anfordern. Über diesen Code übergeben Sie mittels LANconfig dann ein oder mehr Geräte an die LMC. Dieses Verfahren können Sie für jedes Gerät anwenden, welches Cloud-ready ist.

Ein Gerät ist damit allerdings nicht fest an dieses Projekt gebunden. Sie können es jederzeit an ein anderes ihrer Projekte übergeben oder wieder aus der LMC entfernen und stand-alone betreiben.

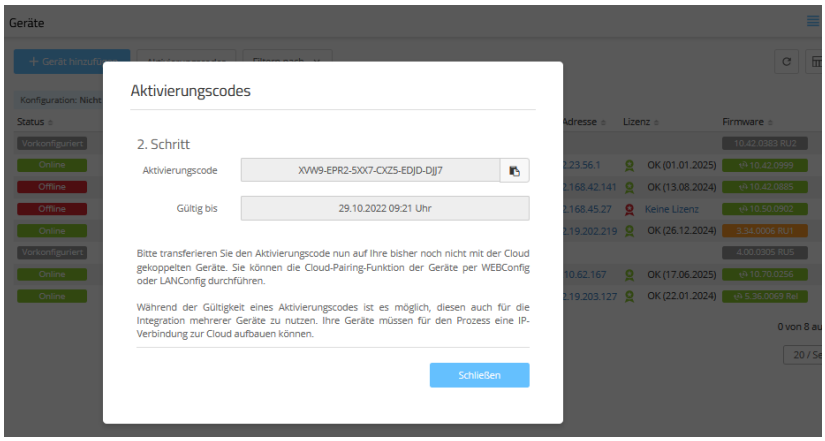

Abbildung 8:
Neues Gerät hinzufügen

Die registrierten LANCOM Geräte lassen sich nun den Standorten zuweisen. Dazu kann auch ein Foto und eine Beschreibung des Gerätestandorts (19“-Rack, abgehängte Decke, ...) hinterlegt werden, sodass ein remote agierender Administrator eine genaue Vorstellung hat und dies ggf. in der Kommunikation mit einem Techniker vor Ort nutzen kann.

Sobald diese Geräte dann am jeweiligen Standort angeschlossen werden, melden sie sich bei der LMC und werden unmittelbar mit einer passenden Konfiguration versorgt und ins 24/7-Monitoring übernommen.

Dazu müssen die Geräte Zugang zum Internet haben. Falls der Router einen dedizierten WAN-Ethernet-Port hat und einen DHCP-Server findet, dann kann er die LMC ebenfalls finden und bekommt sofort die korrekte Konfiguration, falls das Gerät bereits in der LMC bekannt gemacht wurde. Sonst muss für den Router des Standorts diese Grundkonfiguration über z. B. die

LANconfig Setup-Assistenten oder die WEBconfig Setup-Wizards durchgeführt werden. Hierbei kann dann auch die Zuordnung des Standortes erfolgen.

Dies bedeutet, dass die Access Points, Switches, Firewalls und ggf. sogar der Router vor Ort nicht speziell für die Konfiguration angefasst werden müssen – die Inbetriebnahme durch den Administrator erfolgt also im „Zero-touch"-Modus.

Die Daten (Seriennummer / PIN) für alle Geräte können Sie auch vorbereiten und dann alles auf einmal importieren (Bulk-Import). Weitere Informationen erhalten Sie im Techpaper „Rollout".

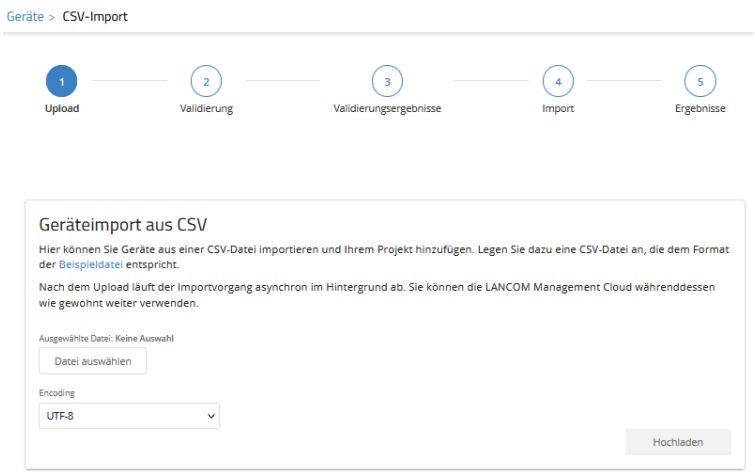

Abbildung 9:
CSV-Import

Rollen

Mit den Rollen für die Benutzer der LMC wird bestimmt, wer ein Projekt bearbeiten oder nur ansehen darf.

Es gibt die Rolle des **Organisations-Administrators**, der im Wesentlichen dem LANCOM Partner entspricht. Dieser darf Projekte und andere Benutzer anlegen. Er verfügt über alle Möglichkeiten innerhalb dieser Projekte, solange er in diesen Projekten auch als Projekt-Administrator eingetragen bleibt. Dieses Recht kann jederzeit entzogen werden. Der Organisations-Administrator hat somit nicht zwingend Zugriff auf die der Organisation zugeordneten Projekte.

Der **Projekt-Administrator** hat innerhalb des ihm zugeordneten Projektes alle Möglichkeiten, kann also insbesondere auch weitere Benutzer innerhalb dieses Projektes hinzufügen.

Der **technische Administrator** hat im Vergleich dazu keinen Zugriff auf die Benutzerverwaltung.

Dann gibt es **Projekt-Mitglieder**, die die Konfiguration der Geräte, Netze und Standorte bearbeiten können, aber z. B. keine weiteren Benutzer hinzufügen oder globale Projekt-informationen manipulieren dürfen.

Mitglieder der Rolle **Rollout-Assistant** sind (meist untechnische) Vor-Ort-Kollegen, die mithilfe der Webapplikation LMC Rollout Assistant Geräte dem Standort hinzufügen.

Auch die Rolle des **Hotspot-Betreibers** eignet sich für nichttechnische Mitarbeitende und dient zur Erstellung von Cloud-managed Hotspot Vouchers.

Zuletzt gibt es noch den **Projekt-Beobachter**, der sich die Daten eines Projektes nur ansehen kann. Über diese Rolle können Sie z. B. einem Kunden sehr leicht ein Monitoring seines Netzwerks ermöglichen.

Weiterführende Informationen zu den Rollen und Rechten erhalten Sie im Infopaper „User-Rollen und -Rechte“.

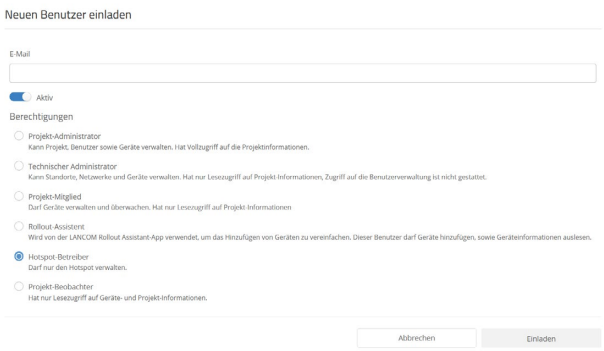

Abbildung 10:
Neuen Benutzer einladen

Dashboards

Mit den Dashboards visualisieren Sie alle Informationen eines Projektes oder einzelner Standorte, indem Sie jeweils den von Ihnen gewünschten Fokus auswählen. Im Folgenden betrachten wir einige ausgewählte Dashboards und besondere Informationen, die dort dargestellt werden.

WAN / VPN

Hier sehen Sie alle Standorte des Projektes auf einer Karte und können alle VPN-Tunnel zwischen den Standorten sowie deren aktuellen Status anhand der Signalfarben Grün und Rot sofort erkennen.

Mittels der historischen Daten zu WAN-Verbindungen haben Sie einen schnellen Überblick über den Durchsatz der Router und die jeweilige Anzahl der VPN-Verbindungen.

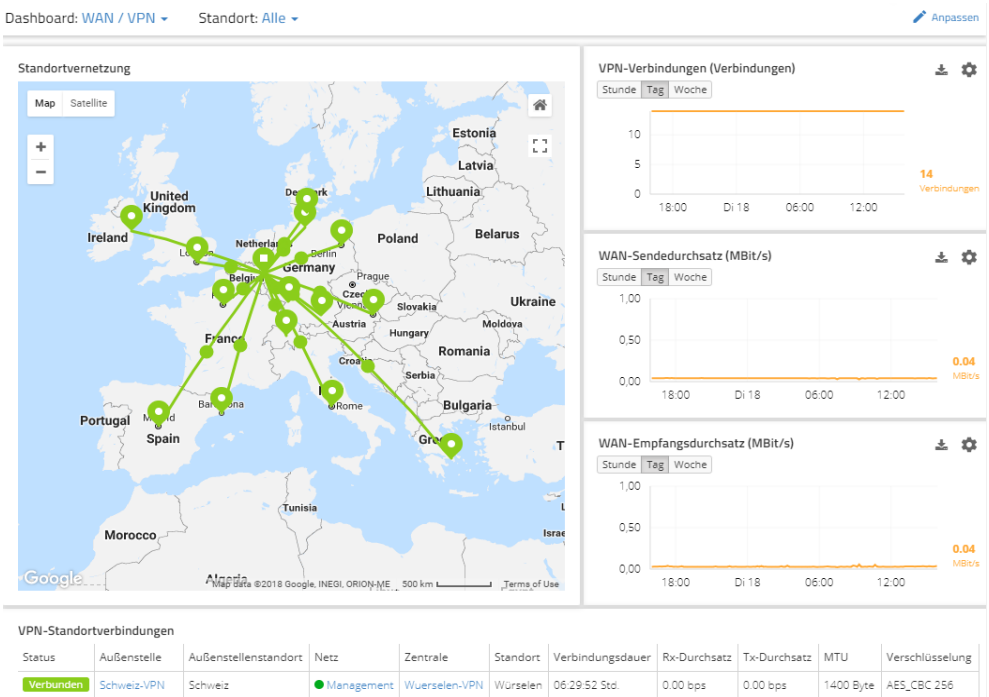

Abbildung 11:
Dashboard WAN / VPN

WLAN / LAN

Nachdem Sie Pläne Ihrer Gebäude hochgeladen haben, können Sie Ihre Access Points in diesen platzieren. Die Anzeige der Ausleuchtung kann natürlich nicht die Wände etc. berücksichtigen, aber sie bietet zumindest einen ersten Anhaltspunkt. Wesentlich an dieser Darstellung sind die aktuelle Auslastung jedes einzelnen Access Points, sodass Überlastungen zeitnah erkannt werden können.

Im Dashboard geben Ihnen die Statistiken einen Überblick über die eingesetzten Geräte, die Anzahl der Benutzer, die Auslastung, die Top-Anwendungen, etc. Sollten Sie z. B. einen Engpass erkennen, dann wechseln Sie aus dem Dashboard auf die jeweiligen Geräte des Standorts, um sich die Details näher anzusehen.

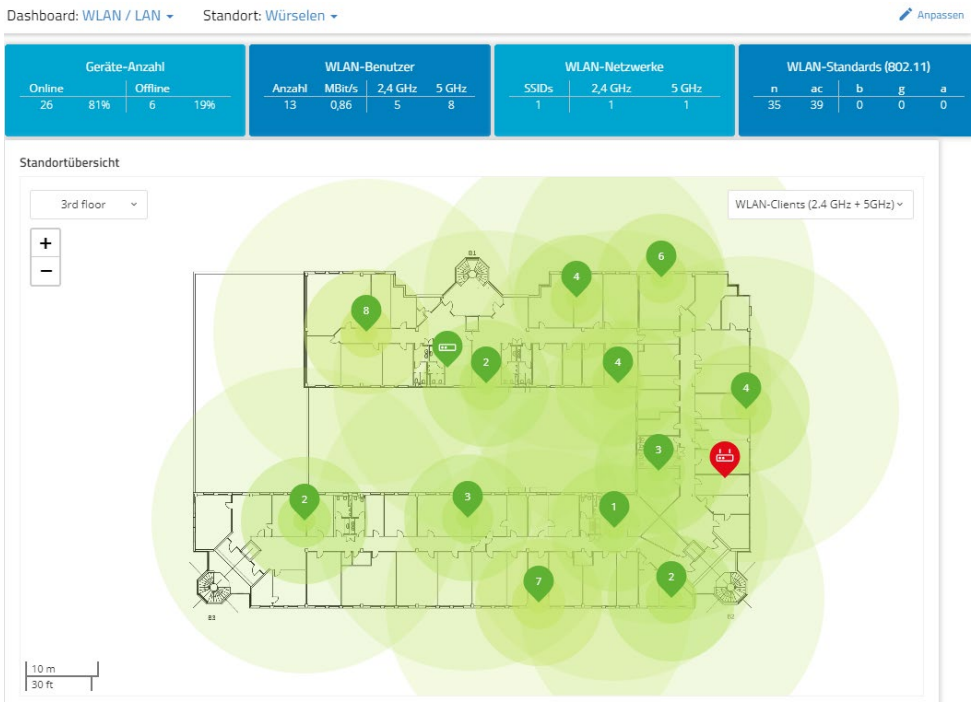

Abbildung 12:
Dashboard WLAN / LAN

Security / Compliance

Mittels der Widgets sehen Sie sofort, ob es Geräte ohne Passwort oder mit nicht aktueller Firmware gibt. Auch offene Ports werden mit entsprechender Warnung angezeigt.

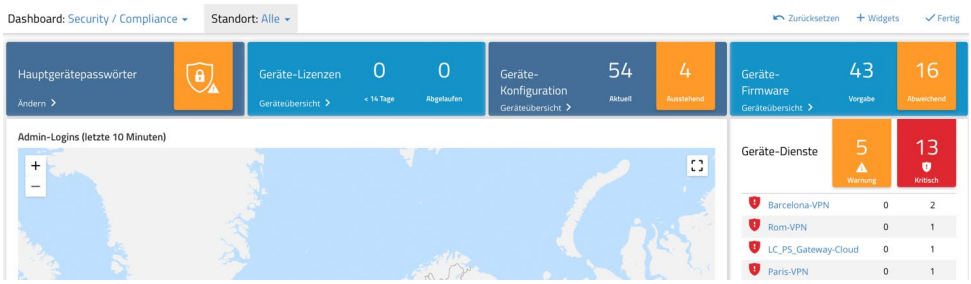

Abbildung 13:
Dashboard Sicherheit

Erweiterte Funktionen

Add-Ins / Scripting

Die für ein Projekt durch LANCOM Systems aktivierbaren Add-Ins erlauben für speziell geschulte AnwenderInnen individuelle Erweiterungen in der LMC. Mit diesen Erweiterungen können innerhalb einer Javascript-Sandbox Kommandozeilen-Skripte und Konfigurationserweiterungen basierend auf der OID-Struktur (LCOS bzw. LCOS SX) erzeugt werden. Dadurch können anschließend beliebige Konfigurationen auf den Geräten ausgerollt werden. Innerhalb der Skripte können Sie Variablen verwenden, die auf allen Ebenen der LMC (Netze, Sicherheit, Standorte, Geräte) belegt werden können und somit eine weitergehende individuelle Anpassung des Skripts erlauben. Eine Variable mit einem Auswahl-Typ könnte z. B. steuern, welcher Teil des Skriptes aktiv wird und damit die Definition für unterschiedliche SIP-Provider schreiben. Für weitere Informationen steht Ihnen das Add-In-Handbuch zur Verfügung.

Open Notification Interface

Um frühzeitig reagieren zu können, müssen Administratoren unmittelbar bei Eintreten eines Netzwerkereignisses benachrichtigt werden. Dank des Open Notification Interface können gesammelte Alarme über verschiedene Ereignisse an jeden Empfänger-Dienst wie z. B. Slack, Jira oder Splunk weitergeleitet werden, der eine Kommunikation mit der LMC auf Basis der Webhook-Technologie ermöglicht. Dadurch können Nutzer die Benachrichtigungen flexibel in ihre übliche Arbeitsumgebung integrieren und ebenfalls mit Alarmen von Fremdherstellersystemen zusammenführen. Weitere Informationen hierzu finden Sie im Techpaper „LMC Open Notification Interface“.

Application Programming Interface (API)

Jede Funktion innerhalb der Services in der LMC lässt sich ebenfalls über eine API programmatisch aufrufen. Die Dokumentation der REST-API der LMC-Services mit den http-Aufrufen finden Sie in den Systeminformationen der LMC. Näheres hierzu in der zugehörigen Dokumentation.

Support

Sollte eine Frage bezüglich der LMC auftauchen, dann steht der Support über den Live-Chat in der LMC in den Geschäftszeiten zur Verfügung, um die Frage sofort zu beantworten.

Alternativ bieten Ihnen sowohl das LMC-Hilfeportal als auch die LANCOM Knowledge Base Artikel zur LANCOM Management Cloud mit weiteren Informationen sowie hilfreichen Anleitungen. Ein Blick in die FAQs zur LMC liefert Ihnen Antworten auf häufige Fragen zu den Themenbereichen Sicherheit, Migration, Features, WLAN, Switches, Router / VPN, Betrieb und Lizenzierung.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen | Germany
info@lancom.de
www.lancom-systems.de