AIR ZEN

The AirZen System:

REMOTE MANAGEMENT & NETWORK RESILIENCE

For IT department decision-makers

Executive Summary

Network technology makes all digital operations in your business possible while protecting your organisation and your customers' data. Amid home offices, zero-day attacks, hacker culture, and the volatile needs of smart infrastructure, the bar of your system requirements keeps rising.

In this document, you will gain an insight into the functionality, structure, and processes of the AirZen system and its safety and user-friendliness aspirations. For us, Network as a Service means ongoing development, providing full sovereignty for users, and forward-looking security concepts.

TABLE OF CONTENT

NETWORK AS A SERVICE

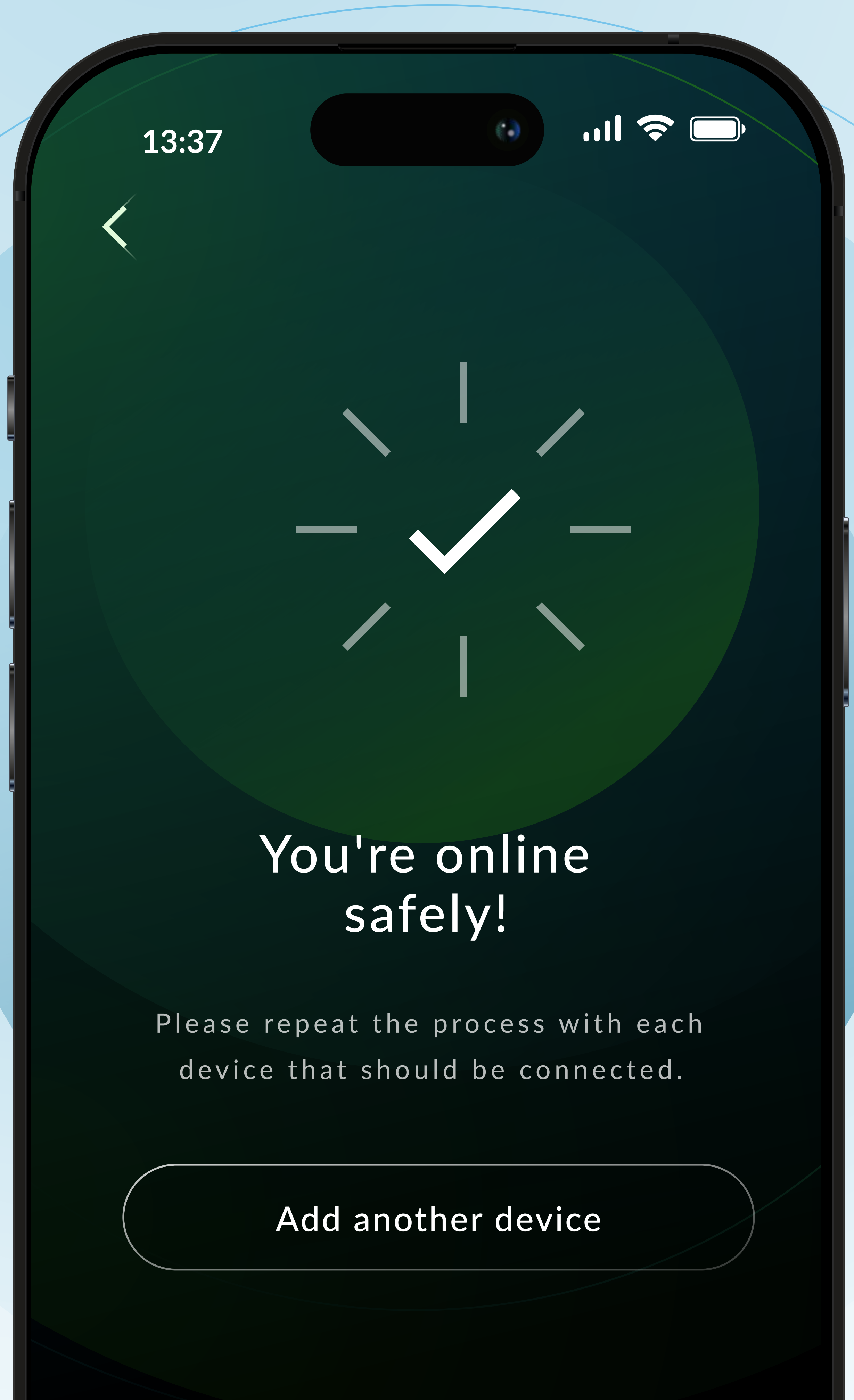
Our platform consists of our proprietary hardware and software written in-house. This practice makes us agnostic and enables a more holistic approach to safety and ease of use.

Homogeneous processes and progressive automation mean that our in-house software can offer enthusiastic home users almost the same level of service as complicated industrial applications or companies with numerous home offices. Our system securely and competently connects multiple sites with minimal setup time and dynamic expansion. No downtime.

Our hardware portfolio ranges from home applications to industrial requirements, powered by Dual-WiFi 6 or 5G (optional). We pre-test and optimise each setup according to your needs before shipping.

As of 2022, several well-known financial institutions are using our technology. We have thus overtaken competitors from the USA and China. As a result, industries, businesses, and government bodies alike have felt more and more pressure to adopt independent solutions. We are committed to meeting this demand and look forward to an ever-evolving network in the future.

Besides this white paper, other white papers are available covering our office, home office, and customer WLAN solutions.

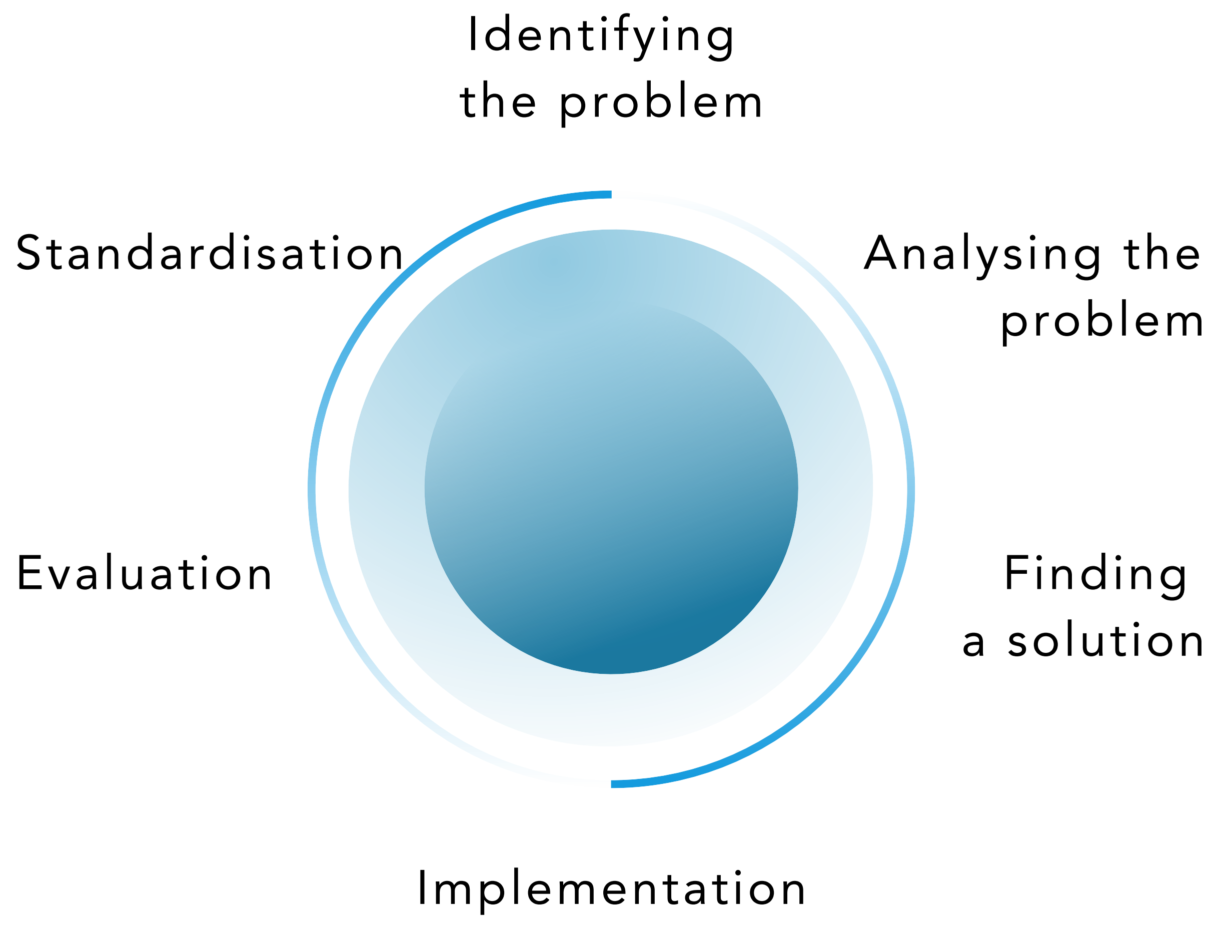


You're online safely!

Please repeat the process with each device that should be connected.

IT SECURITY: CORPORATE RISK AND SOLUTION

Latest by the year 2022, international conflicts have drastically increased the risk of cyberattacks on corporate organisations. The seriousness of this issue becomes apparent through recent governmental interventions in the form of revised laws and regulations at a national level up to the point of managerial liability. We continuously develop our services further and fulfil most requirements already before they become legally binding.



Identifying and analysing the problem

Not least because of international conflicts, IT technology is used more than ever as an espionage tool.

As infrastructure technologies contain a wide range of company information and represent gateways for employees, well-known manufacturers are becoming increasingly targeted by hackers.

Moreover, working from home has drastically increased the potential attack surface, requiring companies to protect not only their corporate network but also that of their employees at home.

Finding a solution

As the respective governments have already recognised, a solution can be found by looking at the origin of the technology.

Another critical step is the administration of all network locations, which includes the many individual users.

Considering the constantly growing number of attacks on the network infrastructure, sustainable security is only conceivable in a system that is always kept current through updates and additional security measures with functions such as those of the AirZen Protection Framework.

To take network security to a new level, we plan to release our technology under an open-source licence in the long term.

Implementing the solution

Our AirZen routers are installed remotely via managed service in line with a standardised rollout and security concept.

AirZen offers the remote administration of all network locations and their users as a managed service. For this, customers can choose a licence model that suits them.

The licensing model is the core of the AirZen system, as only regular software updates and the ability to directly defend against active threats provide security.

Consequently, AirZen's network technology can be understood as a European "network operating system" unique on the market.

AirZen technology is deployed and tested in home and enterprise networks and complex industrial network projects with strict security and compliance requirements.

Evaluation of requirements

During the development of the AirZen technology, the security requirements of the financial sector were evaluated, arguably the most challenging industry segment from an IT perspective, as data protection and GDPR compliance are secondary to the plethora of network security requirements.

The requirements related to security, modular networks and direct administration, employees and branch customers, as well as home offices, are exceptionally high in financial institutions and are, therefore, ideal for evaluating our products.

Standardisation

Missing updates, outdated devices or unsupervised communication with their company devices will inevitably become a security risk to your corporate network. Additionally, the potential attack surface increases enormously if your network is interfaced from many different routers on the employees' side due to remote working.

AirZen delivers a standardised product that fulfils all the IT security aspects mentioned above while offering time and cost savings through innovative remote commissioning, support and user management solutions.

AIRZEN SYSTEM
FUNCTION AND STRUCTURE

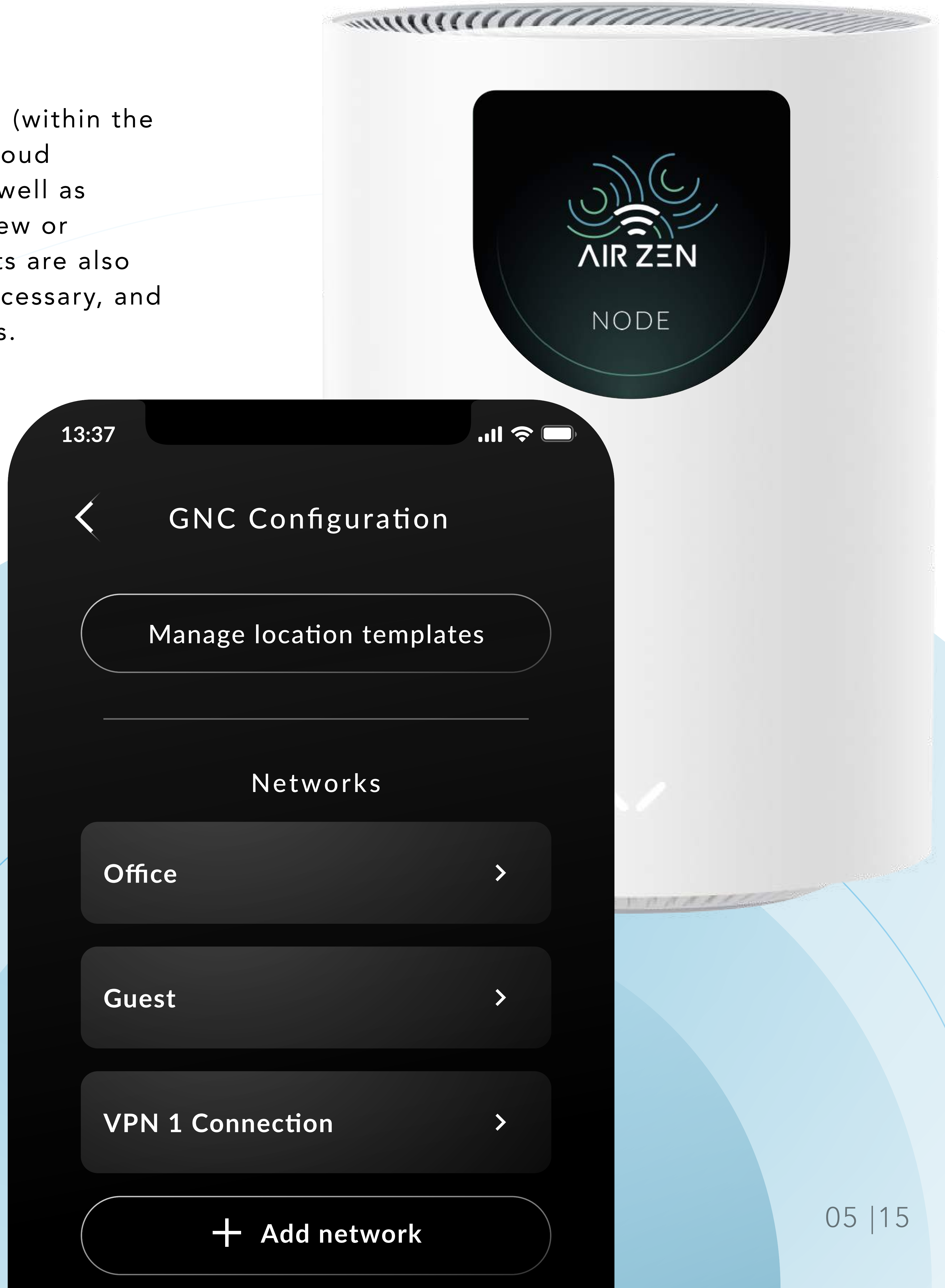
Our platform

The AirZen system is based on proprietary hardware and software with embedded "open source" elements and OEM modules. The AirZen software package is divided into server, client, and component functions. In addition, the AirZen hardware can be expanded with optional software modules.

The AirZen system actively supports only AirZen access points, routers (called "AirZen Nodes"), etc. These components are monitored, configured and administered by the system. Network components from other manufacturers (routers, switches, etc.) can be connected to and operated in the AirZen WLAN.

The AirZen platform is designed as a cloud WLAN system, whereby the AirZen Nodes can be regarded as a single unit across different locations, depending on the configuration.

All the applications operated by AirZen (within the described "cloud") are hosted with a cloud provider. The same applies to VPNs as well as development and test environments. New or improved software modules/components are also developed for local environments, if necessary, and then loaded into the respective systems.



13:37

GNC Configuration

Manage location templates

Networks

Office

Guest

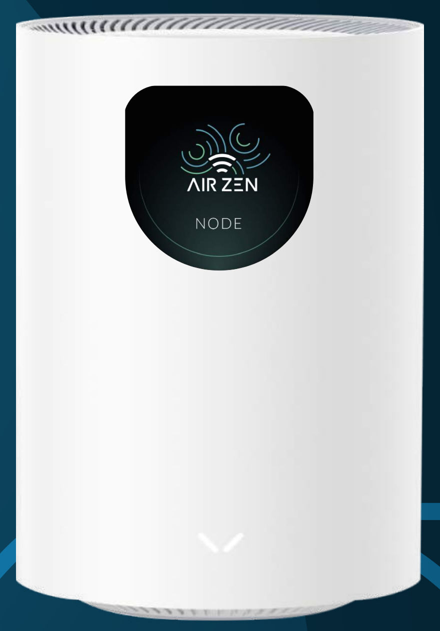
VPN 1 Connection

+ Add network

SOFTWARE DEFINED NETWORK TECHNOLOGY

over 40 microservices & digital infrastructure

HARDWARE



AirZen Nodes
Router, Access, Mesh & Security

TOUCHPOINTS

WiFi6
several virtually separated networks per node

Portal
comprehensive self-service

APP
full transparency

Command Line
full control

AirZen Team
Managed Service

SERVICES

Administration
smart automation, comprehensive analysis tools, autonomous updates

User networks
multiple locations in the same network or various subnets in one location

Guest network
safely separated and with a marketing function

Devices & Internet of Things
full connectivity with high-security standards

AirZen Protection Framework
VPN, malware filter, botnet blocker and many more

supported interfaces of various AirZen Node products:

Cable
Fibre & Ethernet

Bluetooth
up to 50 m

WiFi 6
up to 500 m, up to 10 km with accessories

AirZen IoT
Sensor data up to 10 km

4G & 5G
Mobile data reception at high speeds of up to 15 km

Starlink
Internet uplink for distances up to 550 km

GNSS/GPS
Location tracking up to 20,000 km

Iridium
Satellite connection, low bandwidth for sensor data

Modular system architecture

The most important architectural principles in the design and expression of our technical solutions are:

- a functional division of all services and processes
- Minimising dependencies
- clear regulation of access issues

The primary advantages of a modular system:

- Individual applications or components are easier to reset, re-install or replace in the event of a malfunction.
- The programme code is more manageable, less error-prone and easier to maintain.
- Straightforward revision or (partial) redesign of individual components, as minor or no adjustments are required to other components.
- A failed component (e.g., a single service) only directly affects dependent processes in their functioning.

Complex software stacks are avoided as far as possible during development. The tokens used to authorise interface users are defined in a precise and understandable way so that it is always clear which specific system resources the users have access to. For example, the network configuration may only be read by the routers; only the configuration API is granted write access.

An administrator only has access to specific systems (servers and databases), never to the entire system. However, the developers have access to the software components they are working on. In individual cases, e.g., for new developments or extensive testing measures, a development team may use a different host or separate dedicated servers.

Data of different categories are always stored separately (see "data categories"). In this way, for example, a high load on the database for WLAN sessions does not affect the system-critical database for the network configuration.

Separation from the home network

Many hacking attacks on companies occur through home offices. For example, employees of a company who can be identified via LinkedIn are more easily attacked by malware when they are on their home network. Even a VPN connection on just one end device is not adequate protection. On the contrary, the VPN tunnel can serve as a direct gateway into the company.

This is where the AirZen solution offers substantial protection in the employee's home office. Here, the private and corporate networks are separated, and additional active protection measures are carried out, such as blocking the IP addresses of command & control servers.

If malware (a virus) has penetrated the network, it needs commands from such malicious servers. Blocking their IP address prevents or hinders communication and renders the malware useless. The "block lists" of such command servers are updated daily by AirZen, while malware sites are blocked by DNS filters.

Dealing with incidents

Failed or disrupted applications are replaced, fixed, reconfigured, or reinitialised depending on the system expert's assessment and discretion. If an entire server is faulty, it can be set up again using the same IP. If this is not successful, the server must be fully replaced. In this case, the new server is not activated until the DNS records for the old server IPs have expired. The system architecture also allows backend parts to be operated in a separate data centre or hosted by another provider. In a DDoS attack, the attacked services can be outsourced to their own servers to protect neighbouring services, for example.

Service categories

AirZen services can be divided into the following categories:

- Operation and maintenance of the AirZen Cloud
- VPN gateway operation and management
- Operation and administration of routers, access points, etc.
- User interface operation and control
- Internet access configuration and monitoring

AirZen Cloud

The AirZen Cloud is the hub between the AirZen routers and the technicians carrying out the work. Here, any inputs are made via the command line or the AirZen app. The configuration is based on a software-defined network (SDN) principle. In this process, a configuration is created and stored in a database that the AirZen routers automatically retrieve across locations whenever a change is made. The AirZen Cloud only supports AirZen routers, no third-party hardware.

SD-Wan

SD-WAN facilitates using multiple internet sources so that if one connection fails, the system automatically switches to another. Fibre optics, 5G, and Gigabit Ethernet are available, allowing DSL, fibre and 5G connections to be covered with just two devices. This system features industrial 5G & 4G based on MiMo technology, which provides more bandwidth than standard LTE/5G routers.

The device can automatically activate the 5G fallback connection in case of an Internet failure of the cable network (DSL or similar). As a result, all employees at a location can continue working without interruption. AirZen can also access a site for support (e.g., a problem with the Internet uplink), even if the main Internet line is down.

SD-WAN example

One possible scenario with AirZen is replacing an MPLS/leased line at a company's premises or in a home office.

Uplink 1
One AirZen Node with two fibre ports is used; one is for the provider's fibre optic uplink, and the second is for the connection to the switch.

Uplink 2
In addition, or as a stand-alone device, a regular DSL connection (no fibre) is used at the AirZen Node. The external provider modem is connected to the Node and thus provides a second uplink.

Uplink 3
The AirZen Node establishes one of the fastest 5G connections using 4x4 MiMo.

AirZen Generic Network Controller (GNC)

The cloud-based AirZen Generic Network Controller is the foundation of the AirZen configuration. All configurations are stored in a central database. The individual AirZen Nodes (WLAN routers featuring an access point function) use the main configuration as default. A centrally updated configuration file is automatically transferred. Each configuration is assigned to a "location", and the corresponding AirZen Nodes are assigned to that location. Monitoring events such as logins are simultaneously transmitted from the AirZen Node to the cloud and recorded there. Any data collection on the AirZen Node itself is only temporary, if any. This makes AirZen Nodes easy to install and replace within a network. Each AirZen Node, therefore, only needs to be assigned to one specific location. When the AirZen Node is started for the first time, it obtains its assignment and initial configuration via the AirZen Cloud.

AirZen GNC is divided into several layers logically linked to each other. The following layers are available:

- Radio Config (hardware settings for WiFi, 5G, 4G, LoRa, etc.)
- Networks (VPN tunnel, UFPE, Private Uplink, Public Uplink)
- SSID
- Portal (Customer WiFi)

A logical link between the individual layers can be established by using these AirZen tools. The division into layers enables a wide variety of possible combinations. Here, the setup is mainly done via the command line.

Gateway server

The gateway servers do not collect connection logs from network users. During connection attempts, log information is recorded by AirZen Nodes in a standardised way and periodically deleted as part of the log rotation.

Logging

The AirZen Nodes regularly collect and transmit status information, which is stored in a volatile database for a limited period.

This status information includes the following:

- IP and MAC addresses of local gateways
- MAC addresses, signal strengths and transmission rates of WLAN clients

In the future, it is planned to store the following information:

- List of the current DHCP "Leases"
- 4G/5G connection information

Nodes only store information that is necessary for the actual routing function and the functionality of the device.

Portal functions

The portal only needs the configuration, sessions, and usage data to operate and access the databases. To activate a session, a client device communicates directly with the router. If the configuration database fails, the portal can still provide access to the network to other users/ clients for all configurations already loaded, as the portal configurations are persistently cached locally. No user entries are saved during a connection failure to the corresponding database.

Special operating features

Endpoints and VPN gateways, critical for router administration, are managed and administered in a particular way because, function-wise, they usually scale worse than other services, and individual servers cannot be reached from all locations with the same performance. Therefore, both are dynamically assigned to the respective router requests during operation. This way, VPN traffic can be divided among the gateways. The same applies to the routing endpoints. In case of problems, individual systems/services can be exchanged at any time through dynamically adjustable host names without waiting for DNS entries to expire.

OPERATING THE AIRZEN SYSTEM
EXEMPLARY ROLLOUT

Example company: Financial Institution
30 locations, including staff, equipment, customers, and 50 employees in HomeOffice.

Rollout completed

Week 1 *in cooperation*
Video meeting & project meeting, start of network planning

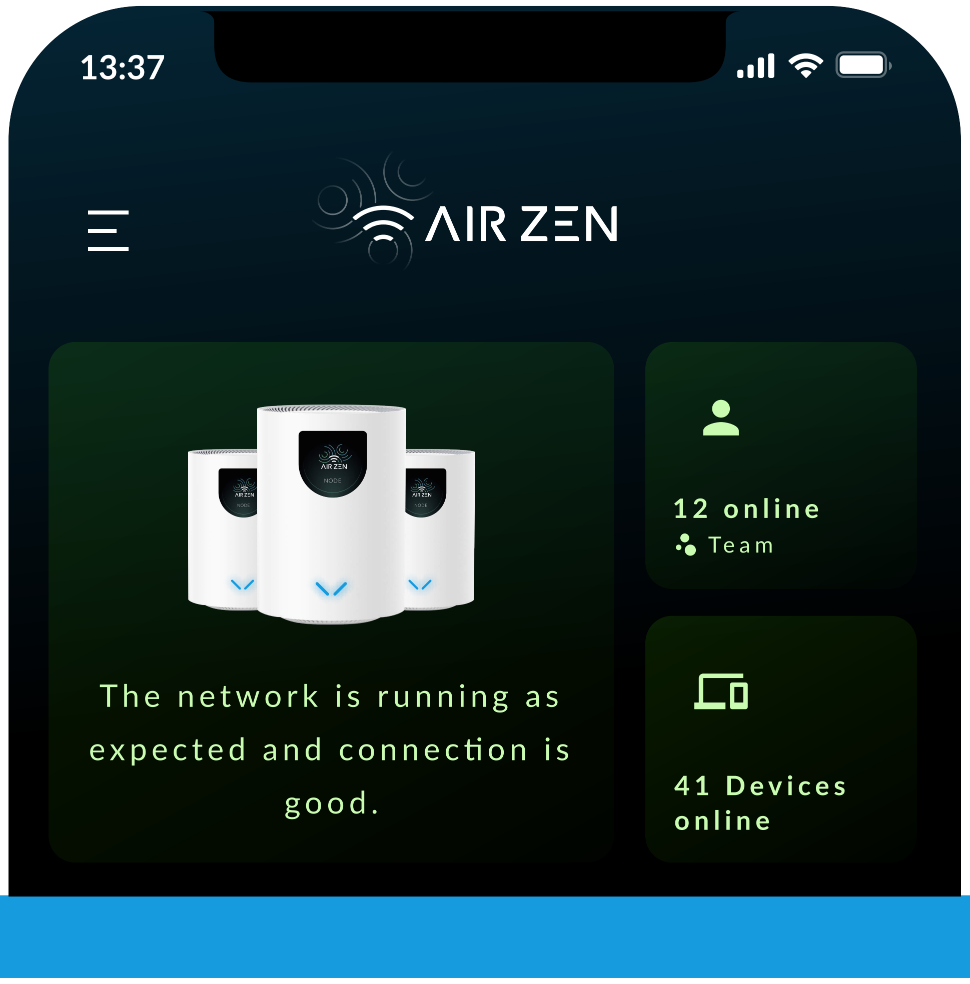
After the completion of our standard contract for corporate customers (which has already been reviewed by financial institutions, their legal departments, and data protection experts), the project commences with the delivery of hardware from stock to the D-A-CH regions.

Week 2 *via AirZen*
End of network planning, test unit with planned network configuration

The **AirZen Managed Service**, a core component of our solution, is carried out directly by AirZen or a certified partner. This service leads the project and serves as a replacement for an in-house expert on your side. Its primary focus lies in **network planning** and **IT security**. The Managed Service collaborates with you to design the network concept, asks the right questions, and turns your network requirements into reality.

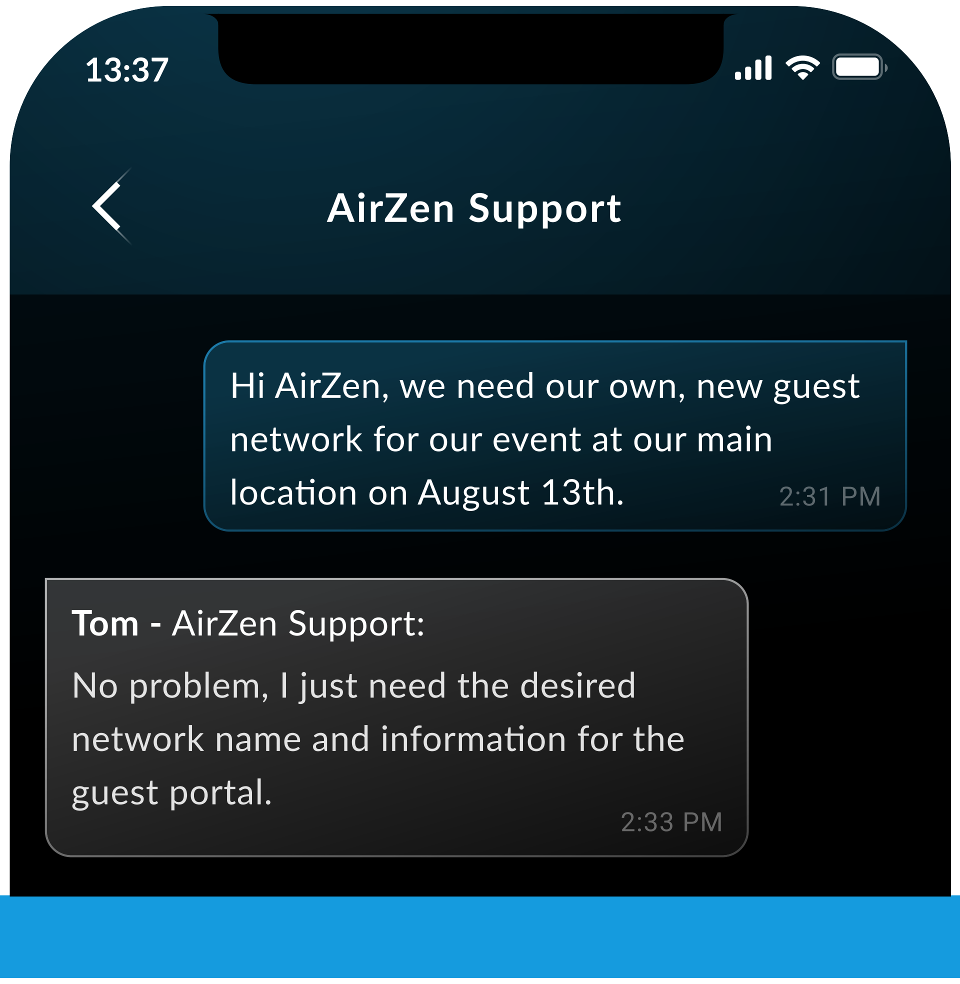
Week 3-5 *via AirZen*
Start of rollout, equipment shipment to customers. On-site installation via plug & play, the network is immediately available.

The installation of the nodes takes place at their respective locations via a plug-and-play process. Our Remote Managed Service assists the IT department with the installation, and together, all locations are activated.



The network is running as expected and connection is good.

Add or block users and devices, or specify user groups at the touch of a button.



Hi AirZen, we need our own, new guest network for our event at our main location on August 13th. 2:31 PM

Tom - AirZen Support:
No problem, I just need the desired network name and information for the guest portal. 2:33 PM

AirZen Managed Service via the AirZen App (Ticket system with integrated chat solution). If desired, staff can communicate directly with AirZen WiFi support, or the customer's IT team can be put as 1st level support.

Week 6-8

Conclusion and fine-tuning. Final details are set up and fine-tuned.

The productive operation is already underway, and first employees are being added via the self-service portal.

Summary

After completion of the plug-and-play installation, a comprehensive network is available through mesh technology. This not only enhances work quality but also improves IT security and enables smoother flexibility in work. Optionally, with AirZen routers, a direct VPN connection to the central hub can be established. The rollout of the AirZen Business Solution thus represents an overall significant relief for the respective IT department. Optional VPN solutions on end devices such as laptops are not affected by this.

- Installation with your own IT staff on site
- Nodes obtain a previously created, customised and tested network configuration via plug & play
- Customer-specific configuration via AirZen Managed Service
- Nodes synchronise automatically (no update of individual devices required)
- AirZen Nodes are permanently monitored for their functionality
- The system continuously measures WLAN quality and automatically communicates faults to AirZen Support

ZENPSK - AUTOMATED IT SECURITY IN THE ONBOARDING PROCESS

Vulnerability: WLAN password

Standard WLAN encryption used by most companies allows only one WLAN password to be assigned to each WLAN, meaning that the password is the same for all users of the WLAN. In this way, intentional or unintentional password disclosure can hardly be prevented and represents a significant security problem. Often, former employees still possess their old company password, which was not changed, opening a floodgate for attackers.

WLAN standards offer an alternative for this with the so-called WPA-EAP method. It is secure but cumbersome and, as a result, hardly used in everyday business - mainly for administrative reasons.

To use this technique, a dedicated "radius server" with additional certificates must be deployed. These certificates must be transferred to each and every end device, which restricts the applicability of the EAP procedure. Hence, this method is unsuitable for use cases with no direct access to the client devices (e.g., via Mobile Device Management MDM). Moreover, the administrative management of this technology is very time-consuming and requires extra infrastructure.

Multifactor authentication

IT security has a high priority in the financial sector. Thanks to its security features, AirZen has distinguished itself from international competitors as a European network provider. All staff members receive their personal WLAN password via a self-service portal. This drastically reduces the attack surface against the organisation.

AirZen's ZenPSK technology enables the use of several WLAN passwords (WPA2/3-PSK). Once the user has entered the password in the terminal, an encrypted connection is permanently active. The connection to the AirZen WLAN is automatically established at all assigned AirZen locations as soon as the company employees or customers enter the respective business premises.

Here, the underlying idea is "one password per device". AirZen Secure Access assigns a personal password to each client's MAC address to prevent users from sharing a password, intentionally or unintentionally.

The procedure is based on the fact that previously generated passwords are stored in the system. When entered for the first time, the AirZen system firmly assigns the PSK password entered to the specific MAC address. This vital security feature relieves the company's IT, ensuring a very high IT security level by proving the identity of the user and of each end device used in order to defend against external attacks.

Practical applications of ZenPSK

For employees
Within a company, a self-service portal is available via the AirZen App or a separate web URL. Employees can independently generate a password for their terminal device by choosing access options for this self-service portal.

To increase security further, access can, for example, be restricted to those employees who own a company email address. So, any access to the self-service portal would require entering the company email address. A one-time web link is then sent by email to activate the device. This process is straightforward and only takes a few moments. Employees may also add multiple devices to their accounts, depending on the corporate configuration of the AirZen network. This makes the network easy to manage, and the administrator can quickly deactivate staff members who leave the company. Apart from that, all devices no longer in use can be disabled automatically. For this purpose, the "idle time", usually six months, can be configured. So, the result is a "tidy" network in which all active users use their personal passwords.

This boosts IT security and enables better support. Besides password generation, direct support cases can also be reported via the self-service portal.

For customers, in a hotel
Customer WLAN is frequently provided via a "portal system". From a security standpoint, there is nothing wrong if access is limited to a few hours. However, this form of WLAN/Internet use is not practicable for more demanding hotel guests due to the intermittent connection.

Upon entering the hotel room, the guest can scan the AirZen QR code to open a website where the guest accepts the internet usage and data protection conditions before creating his or her personal password.

Apple devices, in particular, sometimes react stubbornly to WLANs with front-end portals. The AirZen network, on the other hand, makes the hotel guest feel "at home", providing an uninterrupted digital customer experience. There is an additional WLAN portal for guests to gain access without entering a password. If desired, this access can be limited in time.

AUTOMATED SOFTWARE UPDATES FOR WLAN ROUTERS AND CLOUD SYSTEMS

In today's digital world, most users are aware of the need to keep their laptops, mobile phones, etc., updated to protect their data. Yet, the WLAN router itself is often neglected.

Prevention is better than reaction: Regular, automated updates are paramount.

A WLAN router that does not receive periodic and automated software updates is a great security risk. Numerous WLAN routers come with outdated firmware ex-works and are thus no match for the current cyber threat situation. Such WLAN routers are all too often inadequately maintained. Hence, an additionally acquired security system will be of little use if the prime equipment connected directly to the Internet is the main problem.

At AirZen, a high update interval is maintained as a fundamental practice. The access points automatically check for new versions once daily, during the night. If an update is available, it is executed automatically, and normal operations are resumed within a few minutes. This facilitates the rapid deployment of time-critical security updates and feature enhancements. Updates can also be initiated manually, and there is the option to schedule updates based on a predefined time frame.

Critical Security Updates

On our servers, automatic installation of security updates for standard components takes place no later than four hours after their release. In the case of applications developed by AirZen, the structure is designed such that security-relevant components, such as connection encryption, are inherited from standard components that are regularly updated in this manner.

Regular Updates

Regularly updating software provides a dual benefit. Firstly, it allows for the closure of security vulnerabilities before they become publicly known. Secondly, it reduces the risk of interface changes in interim versions hindering the smooth installation of urgently needed updates. Since the majority of attacks are based on already-known security vulnerabilities, regular updates prove to be of utmost importance.

Feature Updates

The provided updates implement new product requirements. In cases where updates are released to adapt and expand functionality, they also include updates for the rest of the system whenever possible.

AIRZEN IDENTITY

AirZen is a manufacturer of European, innovative, high-quality and easy-to-use network solutions. Our pioneering Network-as-a-Service approach strengthens IT security and sustainably optimizes IT management to ensure maximum customer benefit.

Responsibility is the guiding principle for the development and deployment of AirZen products and solutions, with a focus on security, reliability, and performance.

As a manufacturer, we value direct collaboration with customers as well as partnerships with experienced IT partners. AirZen offers comprehensive solutions comprising proprietary hardware and software components.

For more information and contact details, please visit www.airzen.io.

AIR ZEN

AirZen Networks Lda.

Avenida Arriaga 30 / 1A
9000-064 Funchal
Madeira / Portugal

business@airzen.io

www. AirZen.io

AirZen reserves the right to make technical changes to the product specifications and features contained in this document, such as in the course of further product developments. Some information provided here may be outdated, inaccurate, incomplete, or misleading and is provided without warranty; errors are excepted.