KONNECT ACCESS+

# Konnect Access Technical Documentation

A technical overview of the KONNECT+ managed Wi-Fi platform — architecture, guest authentication, PMS integration, security and requirements.

www.konnect-plus.com

Technical overview · prepared for the client

# Contents

**1.** Introduction & scope

**2.** System overview

**3.** Solution architecture

**4.** Guest authentication methods

**5.** Captive portal & session lifecycle

**6.** Bandwidth, quota & policy

**7.** Fair-use & abuse prevention

**8.** PMS integration

**9.** Management console

**10.** Monetisation

**11.** Interfaces & standards

**12.** Multi-site & scalability

**13.** High availability & continuity

**14.** Security & data privacy

**15.** Installation & deployment

**16.** Sizing & specifications

**17.** Requirements & prerequisites

**18.** Support & reporting

# 1. Introduction & scope

Konnect Access (KONNECT+) is a managed Wi-Fi platform for hotels, office buildings and industrial sites. It provides secure, scalable and monetisable guest internet: a branded captive portal, carrier-grade authentication and accounting, bandwidth and quota policy, network segmentation, and a web console for operators.

This document provides a technical overview of the platform for the client's IT and network teams: how the solution is structured, how guests authenticate, what it integrates with, how it is secured, and what the site must provide. It complements the *Konnect Access Administrator User Manual* which explains the console screen-by-screen. Proprietary implementation details are intentionally omitted.

**Audience**
Site IT and network stakeholders evaluating or operating the platform. Assumes general familiarity with Wi-Fi networks, captive portals and hotel PMS.

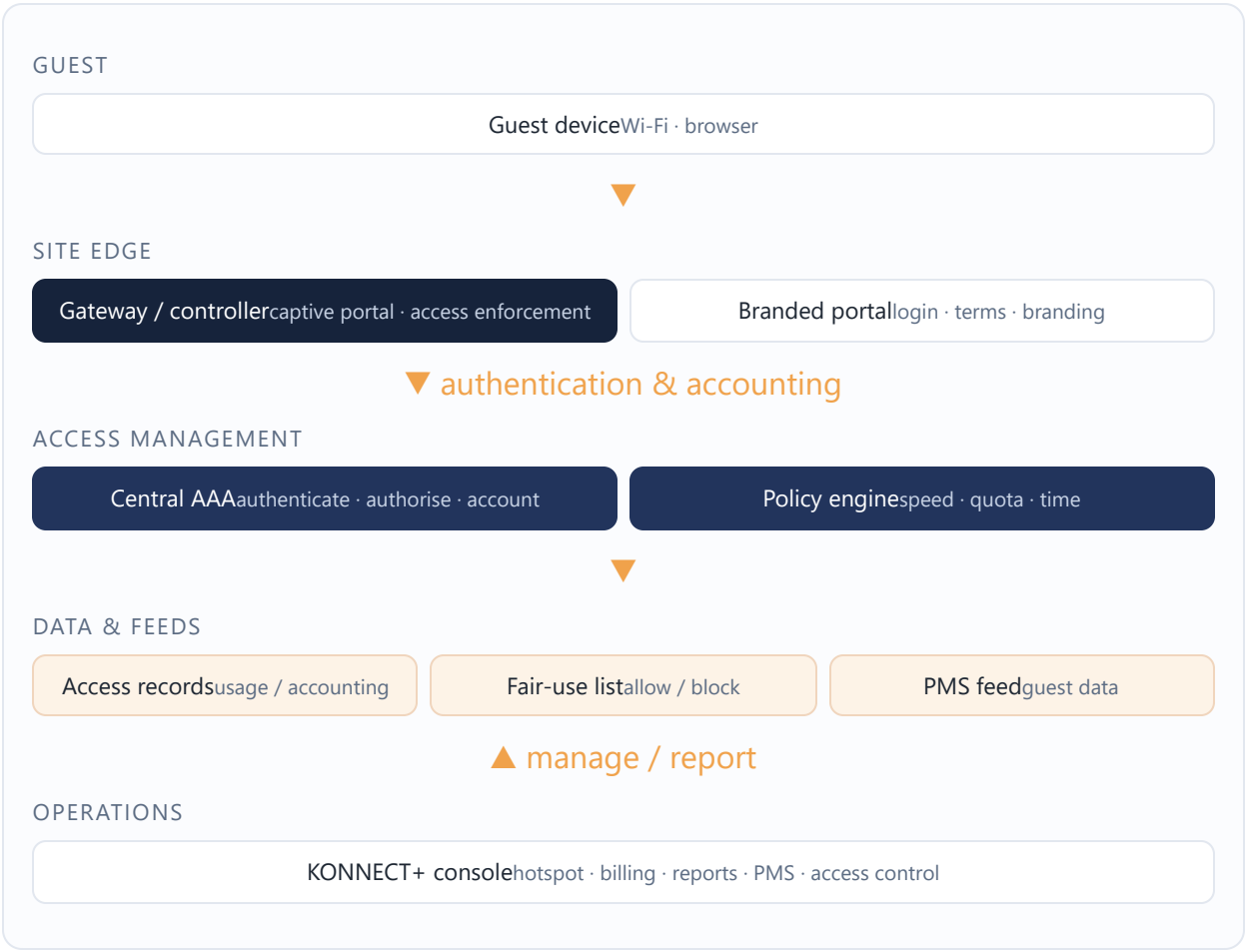
# 2. System overview

At each site a gateway/controller (network access server) manages guest traffic and presents the captive portal. Guest credentials are verified centrally, sessions are metered, and policy (speed, quota, time) is applied per guest. Guest identity can be sourced from the property PMS, and operators manage and report on everything from the KONNECT+ console.

| Concern | Handled by |
|---|---|
| Traffic capture & redirect | Site gateway / controller (captive portal) |
| Portal UI & guest login | Branded captive-portal experience |
| Authentication & accounting | Central carrier-grade AAA |
| Guest identity | Property PMS (where integrated) |
| Policy (speed / quota / VLAN) | Per-guest access profiles |
| Operations & reporting | KONNECT+ management console |

## 3. Solution architecture

Guest devices connect through the site gateway, which presents the captive portal and enforces access. Authentication and accounting are handled centrally against guest data that can be fed from the property PMS. Operators use the KONNECT+ console to configure and report.




**Deployment model**
The platform can serve a single site or many sites centrally. Each site's gateway integrates with the central access-management layer; guest data stays scoped to its own site.

## 4. Guest authentication methods

The portal supports several login methods; a site can enable one or more:

| Method | Description |
| --- | --- |
| Room + guest name | Guests sign in with their room number and name (validated against PMS data). |
| E-mail | Guests sign in with an e-mail address (with fair-use controls). |
| Voucher / access code | Prepaid codes issued at reception or by the operator. |
| Social / free login | Optional lightweight login where permitted. |

**Flexibility**
The accepted login format is configurable per site and can be changed without replacing the portal or gateway.

## 5. Captive portal & session lifecycle

1. Guest connects to Wi-Fi; the gateway redirects unauthenticated traffic to the branded portal.
2. The portal presents the site's branding and the enabled login method(s).
3. Credentials are verified centrally; on success the session is opened.
4. The guest's access profile (speed, quota, time) is applied.
5. Usage is metered throughout the session; quotas or time limits end it automatically.

## 6. Bandwidth, quota & policy

- Per-guest **speed** limits (download/upload) by plan.
- **Data quota** and **time** limits per plan or voucher.
- **Network segmentation** (VLANs) keeps guests, staff and IoT separated.
- Policies are expressed as reusable access profiles applied at login.

## 7. Fair-use & abuse prevention

For sites that allow e-mail or open login, KONNECT+ enforces fair-use controls to prevent shared-account abuse:

- Per-room device limits.
- An allow/block list operators can manage from the console.
- Automatic flagging of an identity used across an unusually large number of rooms.

## 8. PMS integration

Where a property runs a PMS (e.g. Oracle Opera), KONNECT+ can use guest data to enable room/name or e-mail login and to keep the guest list current. The console also governs the maximum number of devices per room and shows the in-house guest list. The integration is read-oriented and arranged with the property's PMS administrator during onboarding.

## 9. Management console

Operators manage and report on the service from one web console:

| Area | Function |
|---|---|
| Dashboard | Live connected / authenticated / registered users, service health, sessions. |
| Hotspot | Overview, auto-login, history, and voucher generation/printing. |
| Management | Users & roles, batches, hotspots, user-groups, IP pools. |
| Reports & accounting | Online users, logs, service status, usage accounting. |
| Billing | Point of sale, plans, rates, transactions, invoices, payments. |
| Access control | Device (MAC) control, e-mail fair-use filter, e-mail campaigns, login-page editor. |
| PMS | PMS properties, integration, guest history and data. |
| Configuration | General settings, operators, backup, external authentication. |

**Localisation**

The guest-facing portal supports a large multi-language set (with a configurable default language) so guests see the portal in their own language.

## 10. Monetisation

- **Plans & rates:** speed/quota/time bundles that can be free or paid.
- **Vouchers:** prepaid access codes generated and printed from the console and redeemed at the portal.
- **Billing:** usage-based invoices, payments and point-of-sale, driven by accounting records.

## 11. Interfaces & standards

| Area | Standard / approach |
|---|---|
| Authentication & accounting | Industry-standard carrier-grade AAA (RADIUS). |
| Gateways / controllers | Standards-based captive-portal appliances/controllers. |
| Guest ↔ portal | Encrypted web protocols (HTTPS). |
| PMS | Oracle Opera integration (where present). |

## 12. Multi-site & scalability

- A single central platform can manage many sites, each with its own branding, plans and guest data.
- A site can present multiple access points/controllers under one profile.
- Capacity scales with the number of access points, rooms and concurrent guests.

## 13. High availability & continuity

- Central services are designed for resilience; a site remains serviceable independently of others.
- Configuration and accounting data are backed up on a regular schedule.
- Recovery procedures allow rapid restoration in a disaster scenario.

## 14. Security & data privacy

- **Network segmentation:** guests, staff and IoT are separated by VLANs; guest traffic is isolated from management.
- **Secure access management:** unique credentials per site gateway; central, auditable authentication.
- **Encrypted portal:** the guest portal and console are served over encrypted web protocols.
- **Role-based operations:** console access is controlled by operator roles.
- **Fair-use & abuse controls:** per-room device caps and allow/block lists guard against credential sharing.
- **Privacy:** guest personal data (e.g. room, name, e-mail) is treated as confidential, kept scoped to its own site, and handled in line with data-protection obligations.

## 15. Installation & deployment

KONNECT+ is delivered as a self-contained installation image (ISO) that bundles the operating system and the complete platform — there is no separate software to install. Deployment is straightforward:

1. Download the latest KONNECT+ installation image (ISO) from the Konnect Plus portal at **https://www.konnect-plus.com**.
2. Provision a physical server or a virtual machine that meets the recommended specification for the expected number of users (see §16).
3. Boot the server / VM from the ISO and follow the guided installer; it installs the operating system and the full KONNECT+ platform automatically.
4. Complete the first-boot setup wizard: network settings, site details and the operator account.
5. Register the site gateway/controller(s) and apply the license.
6. Configure portal branding, plans and PMS integration from the console.

**Deployment options**
The image installs on bare-metal servers or on virtual machines (VMware, Hyper-V, Proxmox/KVM), on-premises or in a private/public cloud, and can serve one site or many centrally. Updates are delivered as managed updates / refreshed images from the same portal.

## 16. Sizing & specifications

Recommended server specification scales with the number of **concurrent online users**. The figures below are a starting-point guideline for a single-node deployment; final sizing is confirmed at onboarding based on peak concurrency, number of sites and reporting retention.

| Tier | Concurrent users | CPU | RAM | Storage | Notes |
|---|---|---|---|---|---|
| Small | up to 500 | 2 vCPU | 4 GB | 100 GB SSD | Single site / node. |
| Medium | up to 2,000 | 4 vCPU | 8 GB | 200 GB SSD | Single node. |
| Large | up to 10,000 | 8 vCPU | 16–32 GB | 500 GB SSD | Multi-site capable. |
| Enterprise | 10,000+ / many sites | 16+ vCPU | 64 GB | 1 TB SSD (NVMe) | High-availability pair. |

| Factor | Guidance |
| --- | --- |
| Accounting / reporting | Usage records grow with sessions and retention period — size storage to the reporting window required. |
| Sites & gateways | Each additional site/controller adds light overhead; large estates benefit from more RAM. |
| Network | Reliable connectivity between site gateways and the platform; adequate internet uplink per site. |
| Virtualisation | Allocate the CPU/RAM above as dedicated (reserved) resources on shared hosts. |

**Note**
These are recommended minimums for smooth operation. Exact specification and any high-availability configuration are agreed during onboarding.

## 17. Requirements & prerequisites

| Area | Requirement |
|---|---|
| Gateway / controller | A supported captive-portal gateway or controller at each site. |
| Network | A managed LAN/WLAN with VLAN separation for guest, staff and IoT; adequate internet bandwidth. |
| Access points | Wi-Fi coverage appropriate to the property. |
| PMS access | A read interface to the property PMS (for room/e-mail login and guest sync), where used. |
| Hosting | Central platform hosting (managed) as agreed at onboarding. |

## 18. Support & reporting

- **Reporting:** live and historical usage, sessions and service status from the console.
- **Monitoring:** service health is monitored with operational alerting.
- **Backups & updates:** regular backups and managed platform updates.
- **Support:** handled through the agreed support channel and SLA.

**Document status**
This client-facing overview describes the platform's capabilities and technical approach and deliberately omits proprietary implementation details. For onboarding specifics (gateways, connectivity, PMS interface) refer to the project's deployment plan.