

Corporate WiFi Access

Secure, managed connectivity for employees and guests. Full control over identity, permissions and audit, with seamless integration into your IT stack.

Benefits of Corporate WiFi

Turn intuition into action plan: where to optimize, when to intervene, and what truly moves the needle.

Simplify access management

Manage employee and guest connections with temporary credentials from a central platform.

Seamless integration

Use APIs to automate provisioning and integrate with existing IT or visitor systems.

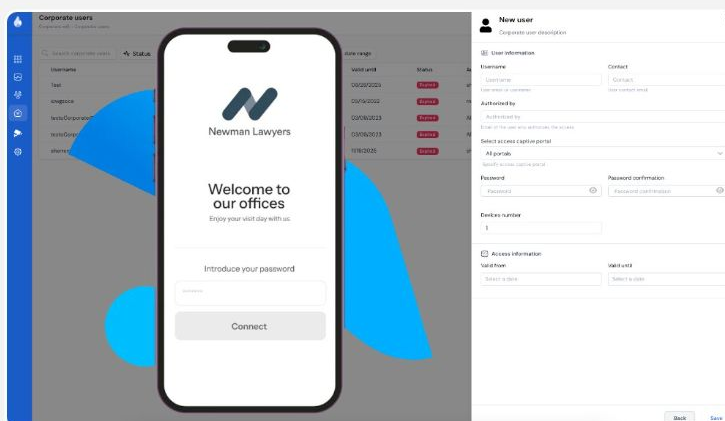
Improve security and compliance

Only authorized users connect — full privacy, traceability and enterprise-grade security.

Improve visitor experience

Visitors request access via form or host approval — fast, simple and branded.

THE PLATFORM Secure access, simple management



Flame Corporate WiFi gives organizations full control over connectivity. Manage credentials, assign time-based permissions and automate user access via APIs.

Provide secure WiFi access for guests and employees, all from a unified platform.

Credentials management

Time-based permissions

API automation

Unified access

The metrics that change decisions

Cross visitors with operations and sales to discover actionable patterns.

01

Active users

Connected employees and guests in real time.

02

Employees vs. guests

Distribution of total network connections.

03

Traffic by area

Connectivity per location: which offices are most used.

04

Load per access point

Detect saturated APs and plan infrastructure.

05

Auditable logs

Full compliance traceability.

06

Security alerts

Notifications for unusual access patterns.

— HOW IT WORKS

How Flame Connect works

- 1

Runs on your existing network

Flame integrates with your existing controller (Cisco, Aruba, Meraki, Ruckus, Ubiquiti) via RADIUS, WPA2/3 Enterprise or HTTPS redirect, with no network rearchitecting. Pricing is per access point, not per user.
- 2

SSO for staff, codes for visitors

Native SSO with Microsoft Entra ID, Google Workspace, Okta or any SAML 2.0 provider, or local credentials with MFA renewed with the employee lifecycle. Visitors either fill a self-service form on arrival or get host-approved access from the app or email.
- 3

Traceability and compliance

Full log of connections, attempts, devices, durations and locations, exportable to SIEM systems via syslog or API. Credentials can be limited by duration, zone, bandwidth or time slot.

KEY FACTS	
Authentication	SSO, MFA and temporary codes
Networks	RADIUS, WPA2/3 Ent., redirect
Deployment	1-2 weeks
Compliance	GDPR and NIS2

Enterprise WiFi access with full control.

Deployed in 1-2 weeks on the WiFi network you already have, priced per access point and not per user.