

Captive Portal

**Guests get the internet.
Never a path to your network.**

Bring guest Wi-Fi under the same platform policy that governs everything else on your network.

Guest Wi-Fi is usually built and managed one controller at a time. Each site runs its own splash page, its own shared password, and its own rules with no identity behind the connection and no record of who was on the network once the session ends. That's not a minor inconsistency. It's an unmanaged, ungoverned edge, repeated at every location.

Portnox Captive Portal runs on the same cloud-native platform that governs employee, BYOD, and IoT access. Guests authenticate through a portal Portnox hosts and Portnox Cloud administers centrally, across multiple wireless vendors, with automatic expiration and a full audit trail — configured once and enforced everywhere.

Only authorized guests get access.

Four authentication types cover site operations: admin-issued credentials for tighter control, disclaimer-only for low-friction access, sponsor-based approval where any employee can vouch for a guest, and SMS self-registration by one-time code. Sessions expire automatically, with some controllers syncing expiration so guests can't re-enter on an old approval. The guest network stays separate from corporate resources, and a walled garden restricts unauthenticated devices to the captive portal, each with its own branding and disclaimer. Tenants get up to ten portal configurations to standardize globally or vary by site.

RETIRE THE PER-CONTROLLER GUEST PORTAL

- ⦿ **ACCESS**

Replace shared passwords with authorized, per-guest credentials
- ⦿ **ADMINISTRATION**

Consolidate per-site, per-vendor configuration into one platform policy, everywhere
- ⦿ **SECURITY**

Extend enforcement beyond a one-time splash page to session-length control and keep guests off the corporate network
- ⦿ **IT OVERHEAD**

Eliminate manual site-by-site builds and password administration with self-service, cloud-managed configuration
- ⦿ **VISIBILITY**

Replace fragmented, per-controller logs with one console, audit trail, and compliance-ready



Portnox secures our network by restricting personal device access to guest Wi-Fi, ensuring main Wi-Fi is exclusive to work devices, enhancing controlled access for improved security.

— Quan L., "A Game-Changer for Network Access Control", Verified G2 Review

Capabilities

Outcomes

Fast onboarding

- Four authentication flows: admin-issued, SMS, disclaimer only, sponsored
- Sponsor approval workflow supporting non-IT issued access

- Guests online in minutes, no help desk ticket, IT gets valuable time back
- Approved access only, to shared passwords to manage or leak

Standardized access

- Vendor-agnostic integration across major wireless providers
- One workflow applied consistently, even when NAS models or firmware differ
- One platform covering every site and vendor
- Replaces per-site splash pages, and shared passwords with a single configuration

- Extends the Wi-Fi infrastructure you already invested in
- Same guest experience at every site regardless of controller make and model
- Simplify control with one console to view, extend and revoke access
- IT defines the guest access workflow once, instead of rebuilding it per location

Accountability

- Dedicated guest SSID with walled-garden enforcement
- Identity captured for sponsored, SMS, and admin issued guests
- Dynamic session timeout, auto-synced to the controller where supported
- Branded disclaimer/acceptable-use acceptance captured at connection

- Guest traffic isolated from corporate systems by design
- Accountability for granted access, not blanket anonymity
- No stale guest accounts outliving their need for access
- Terms-of-use acceptance on record for every session

Portnox Captive Portal delivers secure, standardized guest Wi-Fi access across every wireless vendor — replacing fragmented, per-controller portals with a single platform that cuts onboarding friction, IT overhead, and the risk of shared passwords.

Learn more: portnox.com/portnox-cloud/captive-portal >>



Portnox is a cloud-native enterprise access control provider that helps organizations secure every identity — human and non-human — across networks (NAC), applications (ZTNA), and infrastructure (TACACS+). Its unified platform brings together passwordless authentication, access control, continuous policy enforcement, and automated response through a single policy engine.