Guest BYOD Wireless Access Configuration

Goal: Build a functional guest wireless environment using Ruckus ZoneDirector, including guest access services, a guest WLAN, a generated guest pass, and a successful client connection.

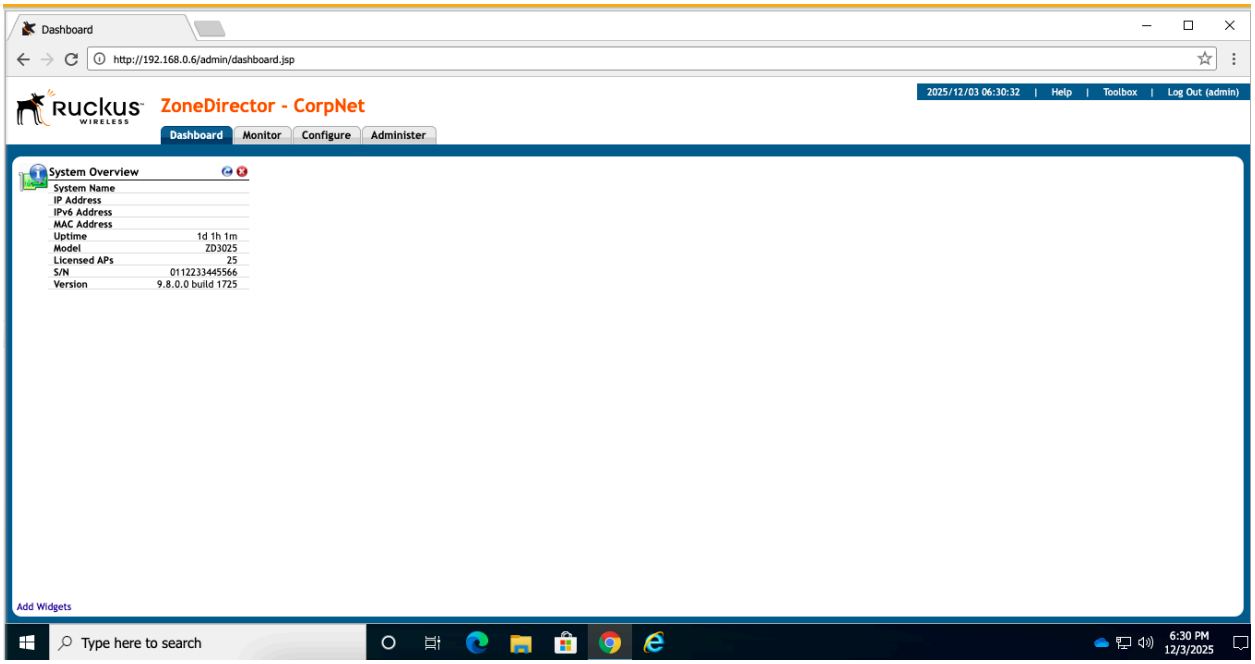
What This Lab Demonstrates

You're showing hiring managers that you understand how real guest networks operate in the enterprise: creating a controlled, isolated guest-access environment, building a WLAN backed by a guest access service, generating and managing temporary guest pass credentials, validating authentication through a captive portal, and following best practices for wireless client isolation.

Configuration Summary

1. ZoneDirector Access & Authentication

Connected to the Ruckus ZoneDirector management interface via browser using the controller's direct IP address.
Authenticated with admin credentials to access configuration menus.



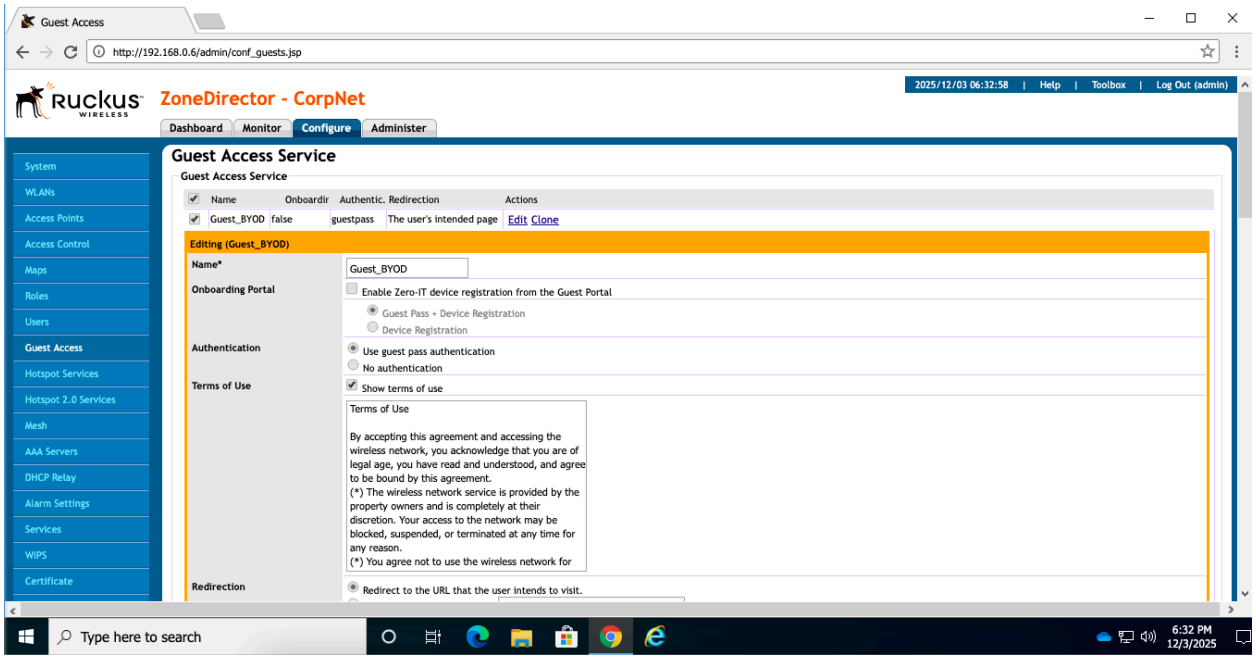
---

2. Guest Access Service Creation

Built a dedicated Guest Access Service used for managing temporary guest authentication.

Key actions:

- Named the service **Guest_BYOD**
- Enabled Terms of Use
- Confirmed restricted subnet access (192.168.0.0/16)
- Applied the configuration



---

3. Guest WLAN Setup

Created a wireless network that integrates directly with the Guest Access Service.

Configured:

- WLAN Name: **Guest**
- ESSID: **Guest_BYOD**
- Type: *Guest Access*
- Enabled wireless client isolation to prevent guest-to-guest communication

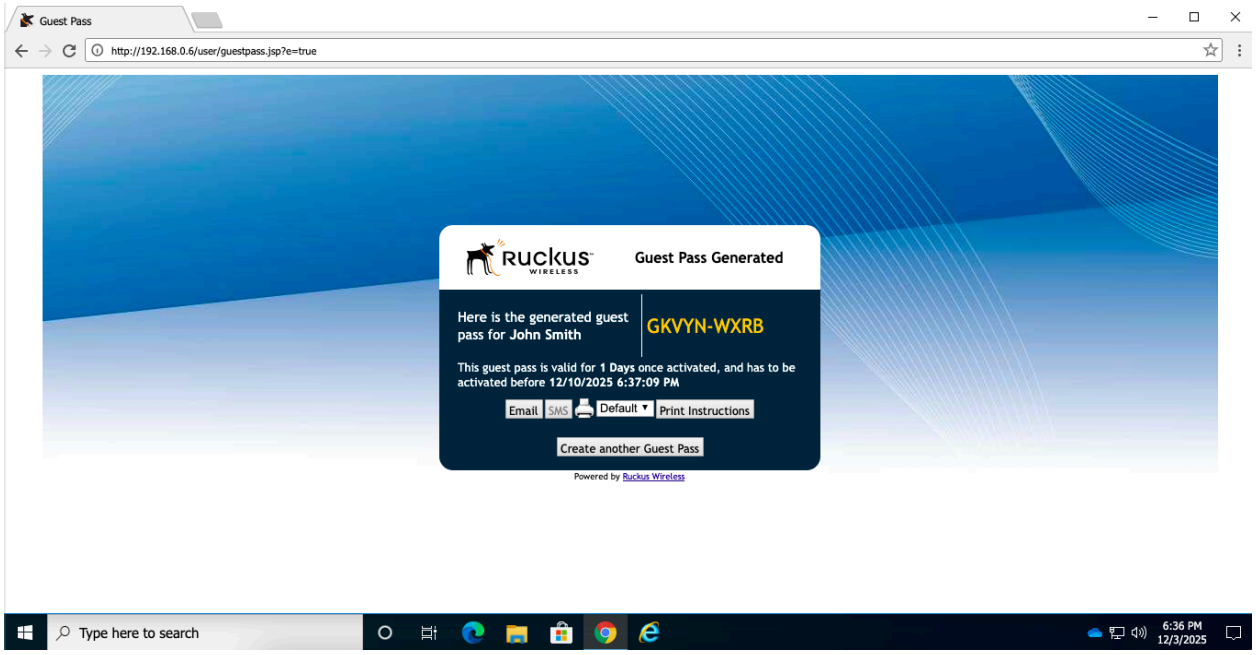
---

4. Guest Pass Generation

Accessed the ZoneDirector's guest pass portal and issued a single-use key for a visitor.
Included:

- Admin portal login

- Full name entry
- Guest pass key creation



---

5. Client Connection & Validation

Using the guest laptop (Gst-Lap), completed the full access flow:

- Selected the **Guest_BYOD** SSID
- Connected to the wireless network
- Encountered the captive portal automatically
- Entered the generated guest key
- Successfully authenticated and accessed the web

Security Value

This configuration provides secure guest Wi-Fi access while protecting internal systems through temporary credentials, client isolation, subnet restrictions, and proper traffic segregation.