Robert Carpenter
github.com/robertmcarpenter
Sat Mar 1st 2025

Lab 10.7.6 Creating Guest Network for BYOD Devices on Ruckus Zone Director

From TestOut CompTIA Security+ Course

In this lab I will be setting up a separate Guest network away from the Corp's production network for users to connect to with their personal devices. (aka BYOD)

The scenario for this lab is as follows:

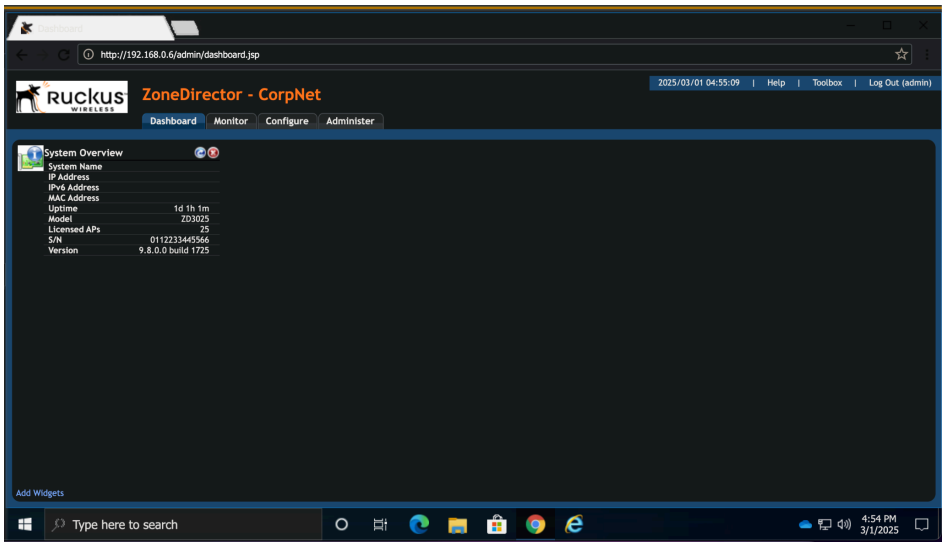
" You are a network technician for a small corporate network. You need to enable BYOD Guest Access Services on your network for guests and employees with mobile phones, tablets, and personal computers.
In this lab, your task is to perform the following:

- **Access the Wireless Controller console through Google Chrome at http://192.168.0.6.**
  - **Username: admin (case sensitive)**
  - **password: password**
- **Set up Guest Access Services using the following parameters:**
  - **Name: Guest_BYOD**
  - **Authentication: Use guest pass authentication**
  - **The guest should be presented with your terms of use statement and allowed to go to the URL they were trying to access.**
  - **Verify that 192.168.0.0/16 is on the list of restricted subnets.**
- **Create a guest WLAN using the following parameters:**
  - **Network name: Guest**
  - **ESSID: Guest_BYOD**
  - **Type: Guest Access**
  - **Authentication: Open**
  - **Encryption Method: None**
  - **Guest Access Service: Guest_BYOD**
  - **Isolate guest wireless clients from other clients on the access point.**
- **Open a new Google Chrome window and request a guest pass using the BYODAdmin user as follows:**
  - **URL: 192.168.0.6/guestpass**
  - **Username: BYODAdmin (case sensitive)**
  - **Password: P@ssw0rd (0 is a zero)**
  - **Use any *full name* in the Full Name field.**
  - **Make a note of or copy and paste the key in the Key field.**

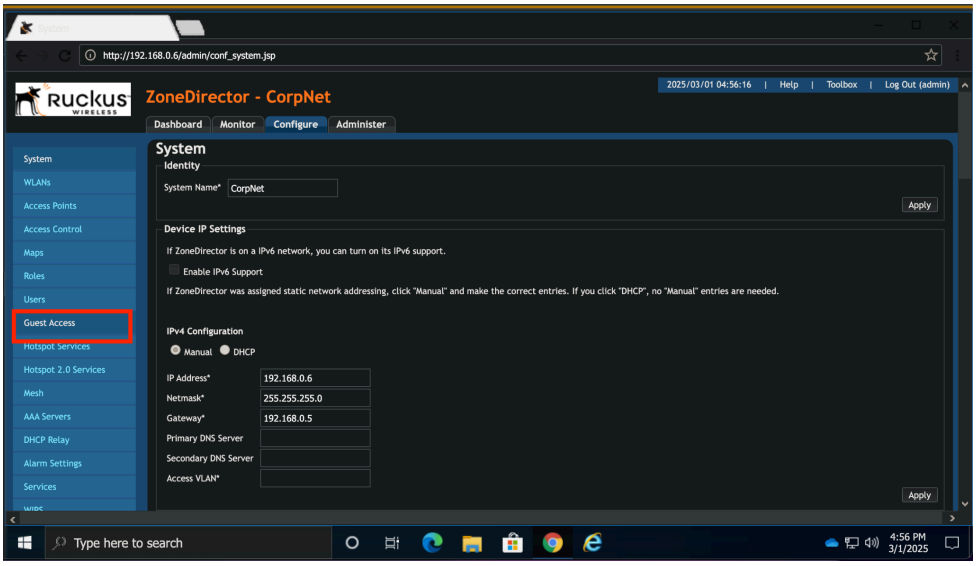
Robert Carpenter
github.com/robertmcarpenter
Sat Mar 1st 2025

- **Use the key from the guest pass request to authenticate to the wireless LAN Guest_BYOD from the Gst-Lap laptop computer in the Lobby."**

To start this lab I will navigate to the Management portal at **192.168.0.6**:80 using Google Chrome. Once there, I will login with the default credentials provided.



Once I am in the portal I will navigate to the top menu bar and select **Configure.** On the Configure sidebar menu I will select **Guest Access. (red rectangle)**



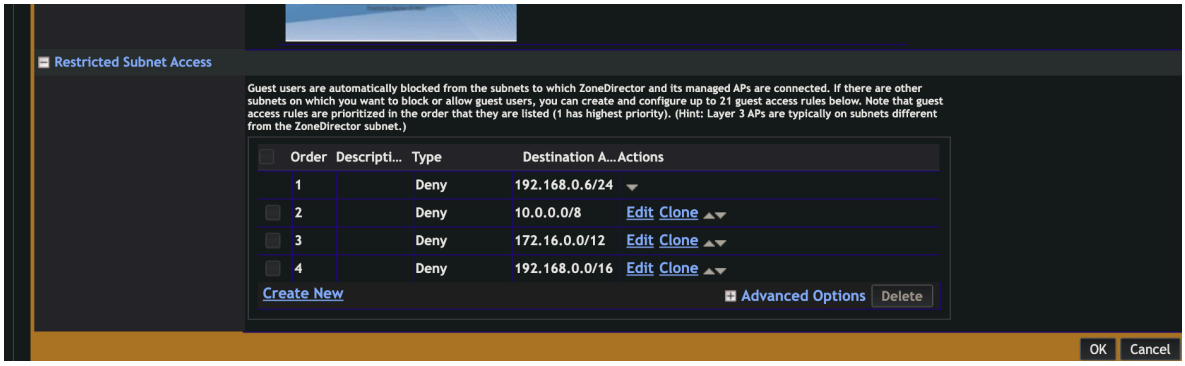
On the Guest Access menu I will then select **Create New.** A new area pops up asking me for the configuration options I would like to set.

Robert Carpenter
github.com/robertmcarpenter
Sat Mar 1st 2025

I'll need to set the following parameters:

- **Name: Guest_BYOD**
- **Authentication: Use guest pass authentication**
- **The guest should be presented with your terms of use statement and allowed to go to the URL they were trying to access.**
- **Verify that 192.168.0.0/16 is on the list of restricted subnets.**

I will set the above then expand the **Restricted Subnet** option to verify that the Guests cannot access the 192.168.0.0/16 (aka any 192.168.X.X) subnet.



Once everything looks correct I will go ahead and hit **OK.**

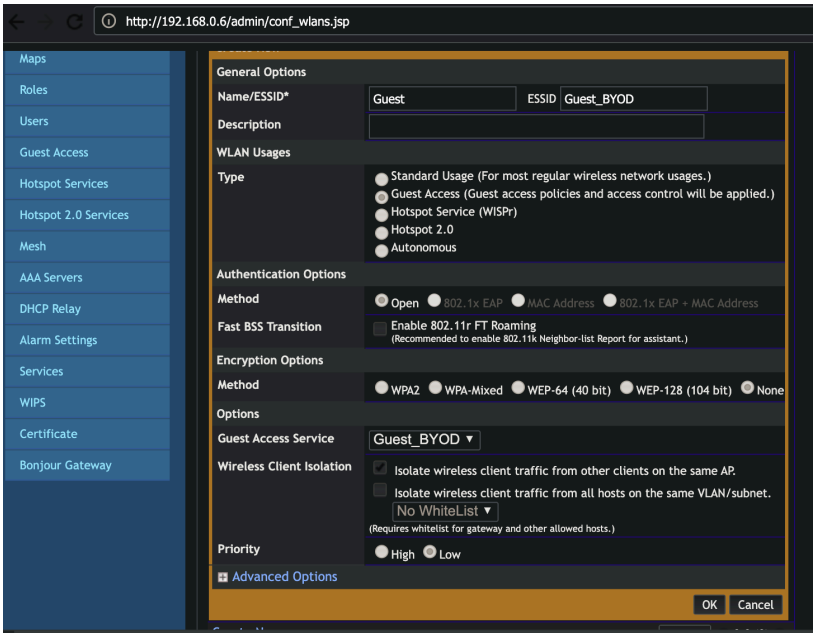
Now it's time to create a Guest WLAN. It's good practice to isolate all Guest connections to their own network so they cannot access any machine on the production network. It is important that we don't allow an attacker that easily connects to the Guest network to pivot inwards out of the DMZ and into the production environment where sensitive data is hosted.

From the left menu pane where I had previously selected **Guest Services** , I will scroll up and select **WLANs.**

I will configure this WLAN with these options:

- Network name: Guest
- ESSID: Guest_BYOD
- Type: Guest Access
- Authentication: Open

- Encryption Method: None
- Guest Access Service: Guest_BYOD
- Isolate guest wireless clients from other clients on the access point.

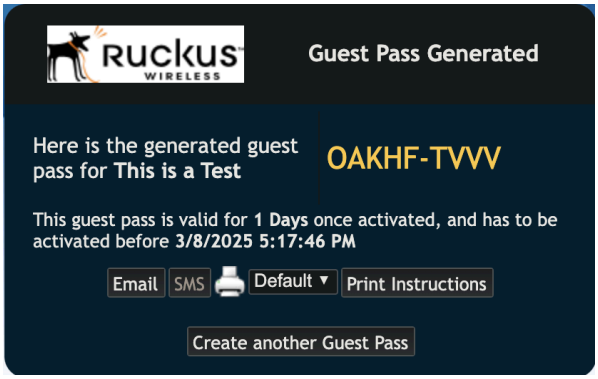


Once that has been set I will hit **OK.**

Now I will need to verify that the Guest service is working and that Guests can obtain a Guest Pass by doing the following:

- *Open a new Google Chrome window and request a guest pass using the BYODAdmin user as follows:*
  - *URL: 192.168.0.6/guestpass*
  - *Username: BYODAdmin (case sensitive)*
  - *Password: P@ssw0rd (0 is a zero)*
  - *Use any full name in the Full Name field.*
  - *Make a note of or copy and paste the key in the Key field.*

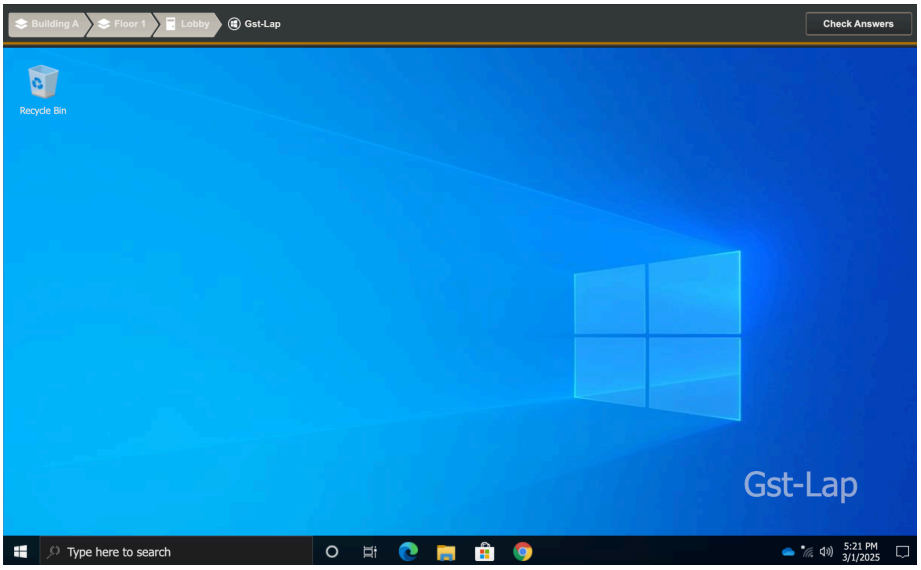
Robert Carpenter
github.com/robertmcarpenter
Sat Mar 1st 2025



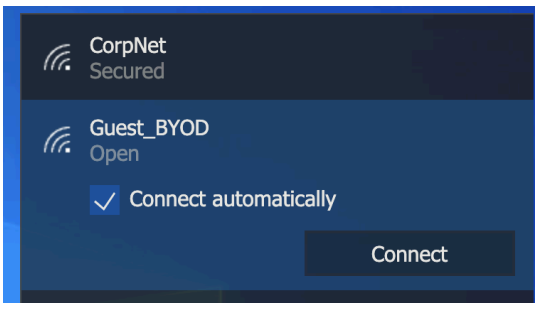
Now that I've obtained a Guest Pass I can go test this key allocated to me. To do that I will head over to a Guest device called **Gst-Lap** , which is a laptop on the 1st Floor of this Virtual Corporate environment. My goal is to see if I can authenticate to the Guest network and verify my configurations were a success.

Robert Carpenter
github.com/robertmcarpenter
Sat Mar 1st 2025

I am now logged into the Guest Laptop , **Gst-Lap:**

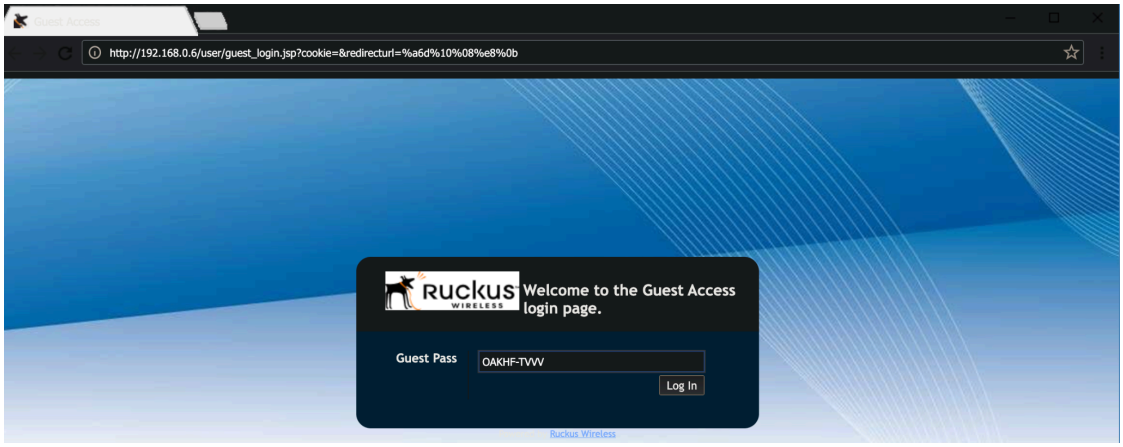


I'll navigate to the task bar and click on the WiFi icon in order to connect to the **Guest_BYOD** WLAN I created.

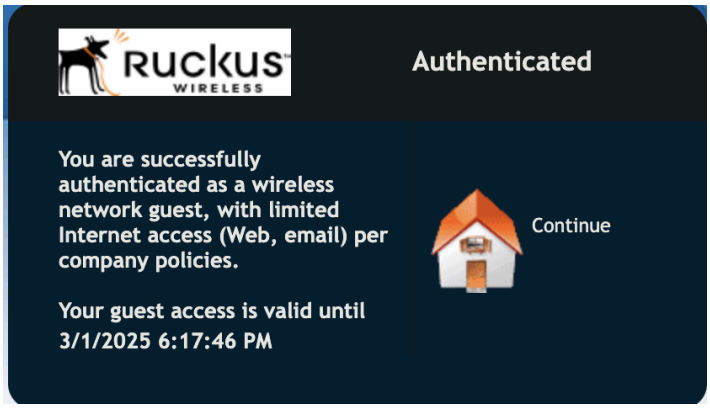


Robert Carpenter
github.com/robertmcarpenter
Sat Mar 1st 2025

Upon clicking **Connect** a web page is automatically opened. The Ruckus page now prompts me for my Guest Pass Code/Key. I will go ahead and paste in the key given to me from the Guest Pass.



After I hit the **Log in** button, a prompt shows up telling me I've been successfully authenticated!



This now concludes this lab on creating a Guest network for BYOD Devices within a Ruckus ZoneDirector Wireless LAN Controller.

Robert Carpenter
github.com/robertmcarpenter
Sat Mar 1st 2025