

Lab 8.6.6: Hardening a Ruckus AP Wireless LAN Controller

From TestOut CompTIA Security+ Course

In this lab I will be configuring security settings for a Ruckus WLC (Wireless/WiFi LAN Controller) in order to harden (i.e. increase security) it from attacks from unauthorized devices as well as restricting content for end-users.

The scenario for this lab is as follows:

“You are a network technician for a small corporate network. You need to increase the security of your wireless network. Your new wireless controller provides several security features that you want to implement.

Access the Wireless Controller console through Chrome on <http://192.168.0.6> with the username admin and the password password. The username and password are case-sensitive.

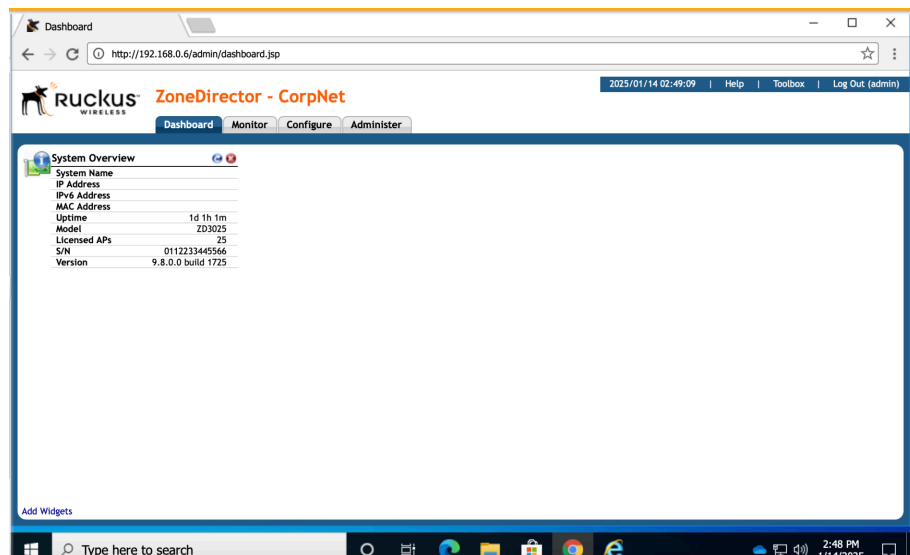
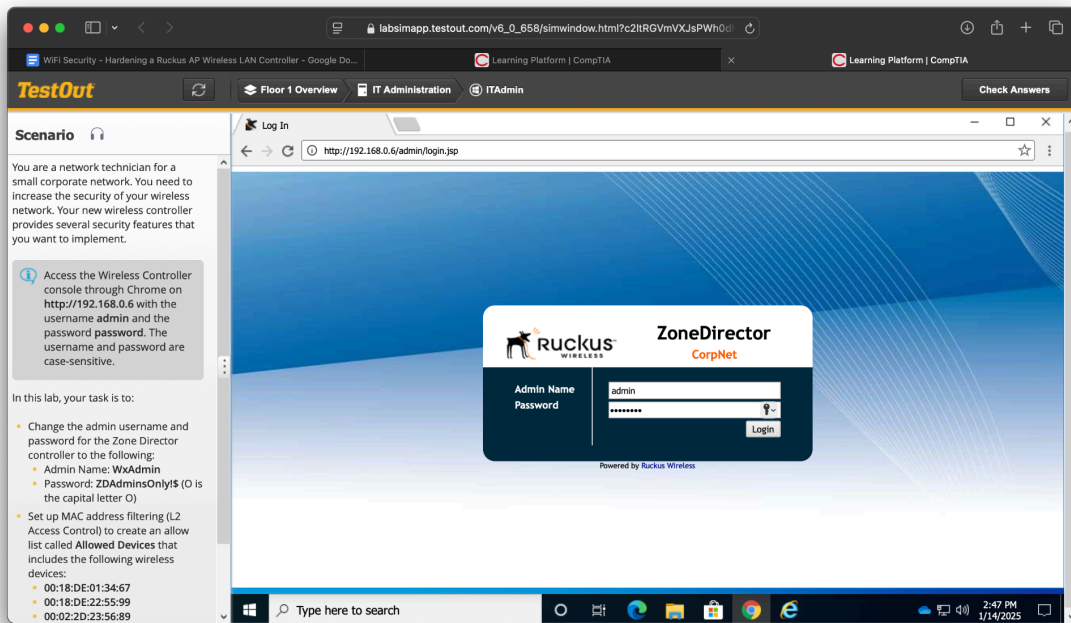
In this lab, your task is to:

- **Change the admin username and password for the Zone Director controller to the following:**
 - **Admin Name: WxAdmin**
 - **Password: ZDAdminsOnly!\$ (O is the capital letter O)**
- **Set up MAC address filtering (L2 Access Control) to create an allow list called Allowed Devices that includes the following wireless devices:**
 - **00:18:DE:01:34:67**
 - **00:18:DE:22:55:99**
 - **00:02:2D:23:56:89**
 - **00:02:2D:44:66:88**
- **Implement a device access policy called NoGames that blocks gaming consoles from the wireless network.”**

To start this I'll need to log in to the Ruckus Controller. Note that the lab says that the controller is using the default credentials. The good thing is that our first task is to change these credentials , which is something that would be done in the first

Robert Carpenter
github.com/robertmcarpenter
Tues January 14th 2025

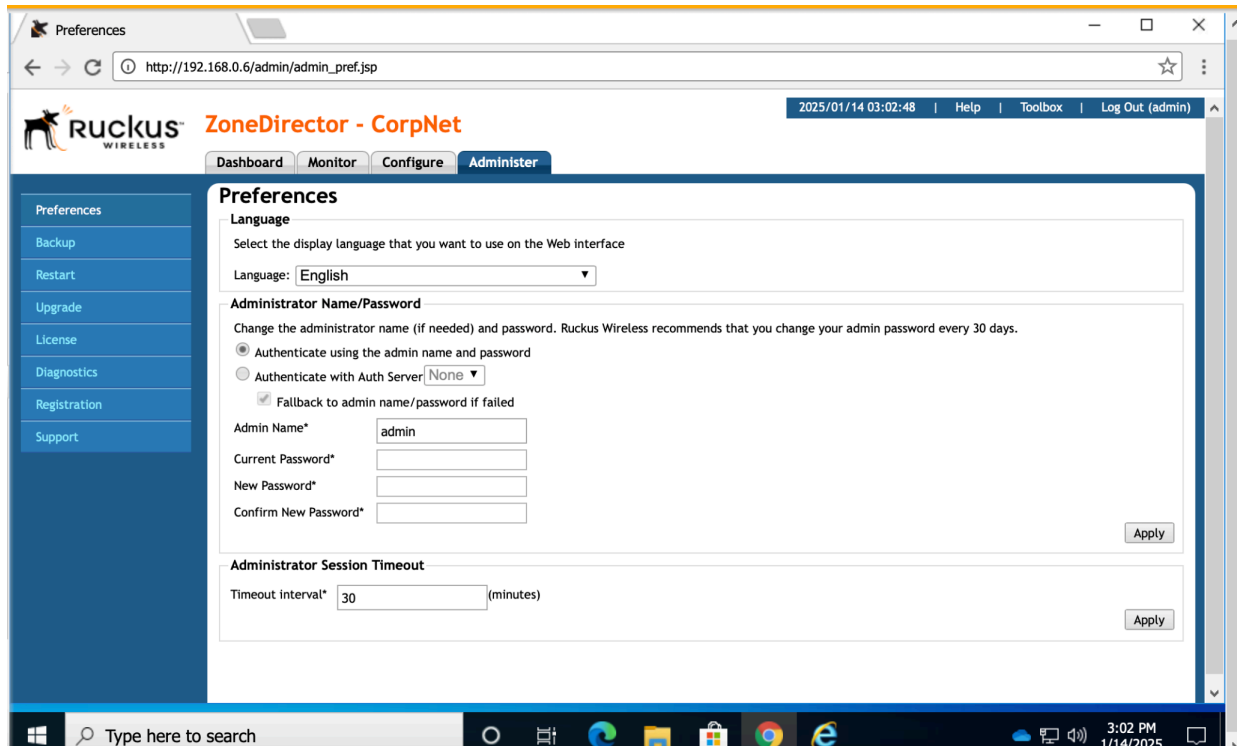
place before it's even deployed to a corporate network (good thing this is a hypothetical lab!).



Now that I'm logged in, my first task as stated above is to change the credentials for this Ruckus WLAN Controller. To do that I will head to the **Administer** tab at the top menu bar next to **Dashboard** (where I'm currently at).

Robert Carpenter
github.com/robertmcarpenter
Tues January 14th 2025

Clicking **Administer** brings up the following page:



The screenshot shows a web browser window displaying the Ruckus ZoneDirector - CorpNet Administer page. The page has a navigation bar with tabs for Dashboard, Monitor, Configure, and Administer. The Administer tab is active. On the left, there is a sidebar with links for Preferences, Backup, Restart, Upgrade, License, Diagnostics, Registration, and Support. The main content area is titled 'Preferences' and contains two sections: 'Language' and 'Administrator Name/Password'. The 'Language' section has a dropdown menu set to 'English'. The 'Administrator Name/Password' section has a note about changing the administrator name and password every 30 days. It includes two radio buttons: 'Authenticate using the admin name and password' (selected) and 'Authenticate with Auth Server' (set to 'None'). There is a checkbox for 'Fallback to admin name/password if failed' which is checked. Below these are input fields for 'Admin Name*' (containing 'admin'), 'Current Password*', 'New Password*', and 'Confirm New Password*'. There is an 'Apply' button at the bottom right of this section. Below the 'Administrator Name/Password' section is the 'Administrator Session Timeout' section, which has a 'Timeout interval*' input field set to '30' minutes, with an 'Apply' button at the bottom right. The browser's address bar shows 'http://192.168.0.6/admin/admin_pref.jsp'. The Windows taskbar at the bottom shows the search bar and several application icons.

This is the page I can enter the new login credentials. The Lab wants me to change it to:

- **Admin Name: WxAdmin**
- **Password: ZDAdminsOnly!\$ (O is the capital letter O)**

I'll do that now:

Robert Carpenter

github.com/robertmcarpenter

Tues January 14th 2025

Preferences

Language

Select the display language that you want to use on the Web interface

Language:

Administrator Name/Password

Change the administrator name (if needed) and password. Ruckus Wireless recommends that you change your admin password every 30 days.

☒ Authenticate using the admin name and password

☐ Authenticate with Auth Server

☒ Fallback to admin name/password if failed

Admin Name*

Current Password*

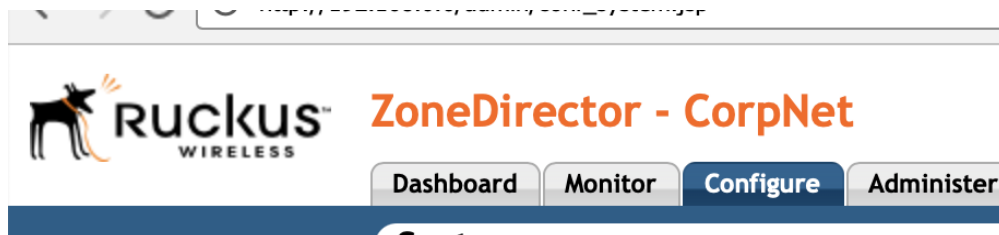
New Password*

Confirm New Password* 

After clicking **Apply** I see that the changes were successfully applied. Now that I have changed the credentials I'll move on to the next part of the lab.

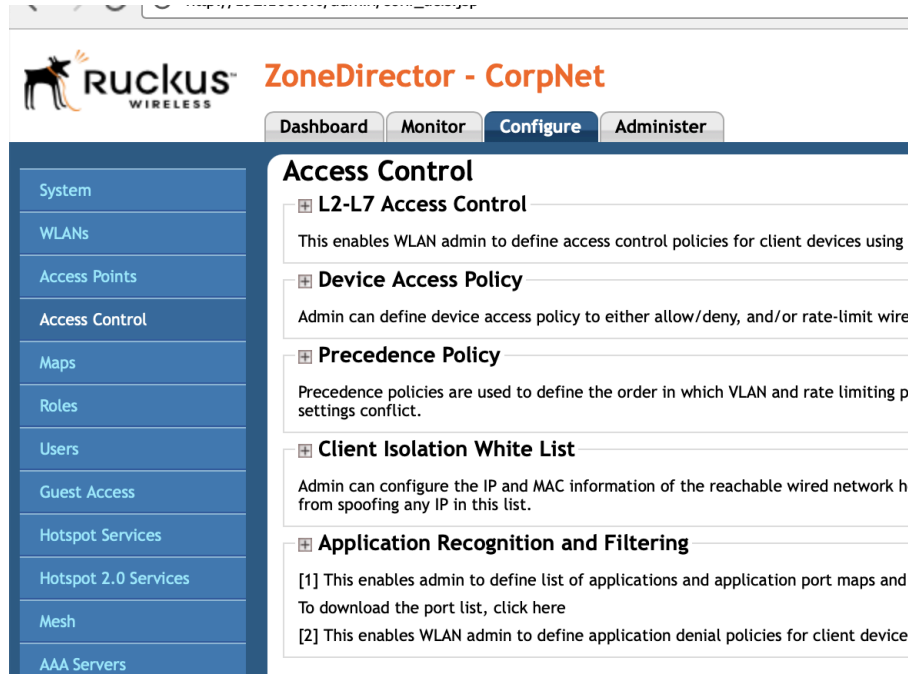
The next part of this lab is for me to setup MAC Address Filtering (aka Layer 2 Filtering) so that we only allow certain devices access to the WLAN.

On this Ruckus Controller I will need to go to the **Configure** tab at the same top menu where I accessed this **Administer** tab to change the credentials.

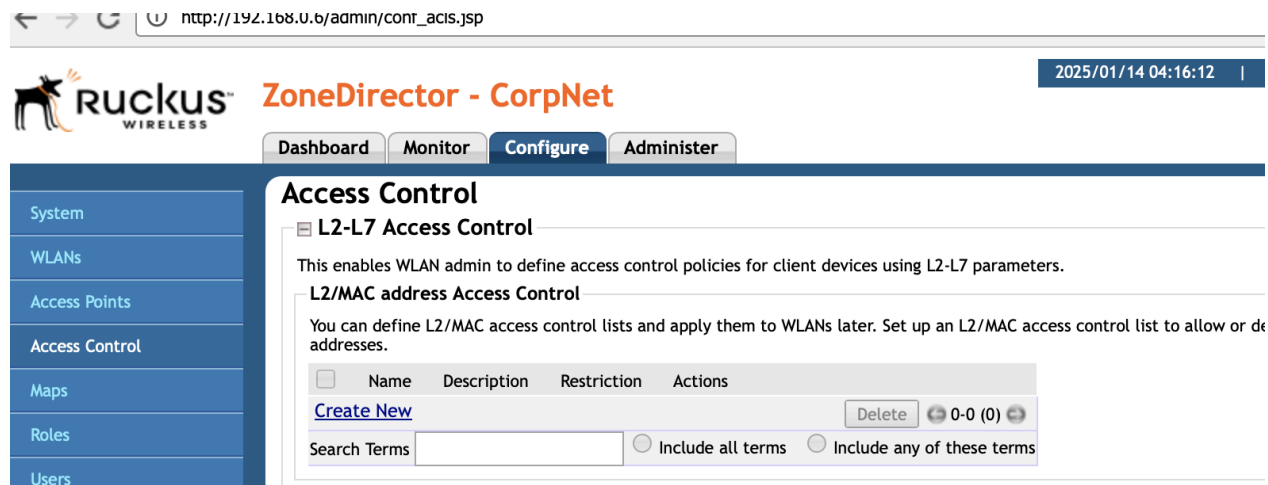


Now that I'm on the **Configure** page, I'll head to the left menu pane and select **Access Control**:

Robert Carpenter
github.com/robertmcarpenter
Tues January 14th 2025



Once here, I'll click the Plus button to expand the **L2-L7 Access Control** menu.



To create a new list I will hit the **Create New** button. On the menu that pops up it prompts me to enter a new name for this Access Control list. The Lab has asked us to name this list **Allowed Devices**. Once I enter the name I will go ahead and begin entering the 4 MAC Addresses of the allowed devices:

Tues January 14th 2025

http://192.168.0.6/admin/contr_acis.jsp

2025/01/14 04:17:57 | Help |

Ruckus WIRELESS ZoneDirector - CorpNet

Dashboard Monitor **Configure** Administer

Access Control

☒ **L2-L7 Access Control**

This enables WLAN admin to define access control policies for client devices using L2-L7 parameters.

L2/MAC address Access Control

You can define L2/MAC access control lists and apply them to WLANs later. Set up an L2/MAC access control list to allow or deny wireless addresses.

<input type="checkbox"/>	Name	Description	Restriction	Actions
Create New				
	Name*	Allowed Devices		
	Description			
	Restriction	<input checked="" type="radio"/> Only allow all stations listed below <input type="radio"/> Only deny all stations listed below		
	MAC Address	00:02:2D:44:66:88		Create New
	Stations	00:18:DE:01:34:67 delete 00:18:DE:22:55:99 delete 00:02:2D:23:56:89 delete 00:02:2D:44:66:88 delete		
OK Cancel				
Create New Delete 0-0 (0)				

Now that I have all 4 devices' MAC Addresses entered I will click the **OK button** to apply the changes.

Moving on to the next part of the lab , I now need to create an Access Policy to restrict traffic from Game consoles:

- Implement a device access policy called NoGames that blocks gaming consoles from the wireless network.

On this same **Configure > Access Control** menu, I can scroll down to **Device Access Policy**:

Robert Carpenter
github.com/robertmcarpenter
Tues January 14th 2025

Access Control

System

WLANs

Access Points

Access Control

Maps

Roles

Users

Guest Access

Hotspot Services

Hotspot 2.0 Services

Mesh

AAA Servers

DHCP Relay

Alarm Settings

Services

WIPS

Certificate

Bonjour Gateway

L2-L7 Access Control

This enables WLAN admin to define access control policies for client devices using L2-L7 parameters.

L2/MAC address Access Control

You can define L2/MAC access control lists and apply them to WLANs later. Set up an L2/MAC access control list to allow or deny wireless devices based on their MAC addresses.

<input type="checkbox"/>	Name	Description	Restriction	Actions
<input type="checkbox"/>	Allowed Devices		Only allow listed stations	Edit Clone

[Create New](#) [Delete](#) 0-0 (0)

Search Terms ☐ Include all terms ☐ Include any of these terms

L3/4/IP address Access Control

You can define L3/4/IP address access control lists and apply them to WLANs later. Set up a L3/4/IP address access control list to allow or deny wireless devices based on their IP addresses.

<input type="checkbox"/>	Name	Description	Default Mode	Actions
<input type="checkbox"/>				

[Create New](#) [Delete](#) 0-0 (0)

Search Terms ☐ Include all terms ☐ Include any of these terms

Device Access Policy

Admin can define device access policy to either allow/deny, and/or rate-limit wireless client devices based on their OS type and VLAN.

<input type="checkbox"/>	Name	Description	Default Mode	Actions
<input type="checkbox"/>				

[Create New](#) [Delete](#) 0-0 (0)

Search Terms ☒ Include all terms ☐ Include any of these terms

Precedence Policy

Precedence policies are used to define the order in which VLAN and rate limiting policies are applied when the WLAN settings, AAA server configuration or DHCP settings conflict.

Once here I'll click **Create New**.

The Lab has asked us to name this policy "**NoGames**." I'll enter that , then in the drop down menu for OS, I'll select "**Gaming**."

Device Access Policy

Admin can define device access policy to either allow/deny, and/or rate-limit wireless client devices based on their OS type and VLAN.

<input type="checkbox"/>	Name	Description	Default Mode	Actions
<input type="checkbox"/>				

Create New

Name*

Description

Default Mode Default Action if no rule is matched: ☒ Deny all by default ☐ Allow all by default

Rules

<input type="checkbox"/>	Order	Description	OS/Type	Type	Uplink	Downlink	VLAN
<input type="checkbox"/>	1		Gaming	Deny	Disabled	Disabled	

[Create New](#) [Advanced](#)

I'll also need to ensure that the **Type** is set to **Deny**, and that the Uplink and Downlink are also **Disabled**.

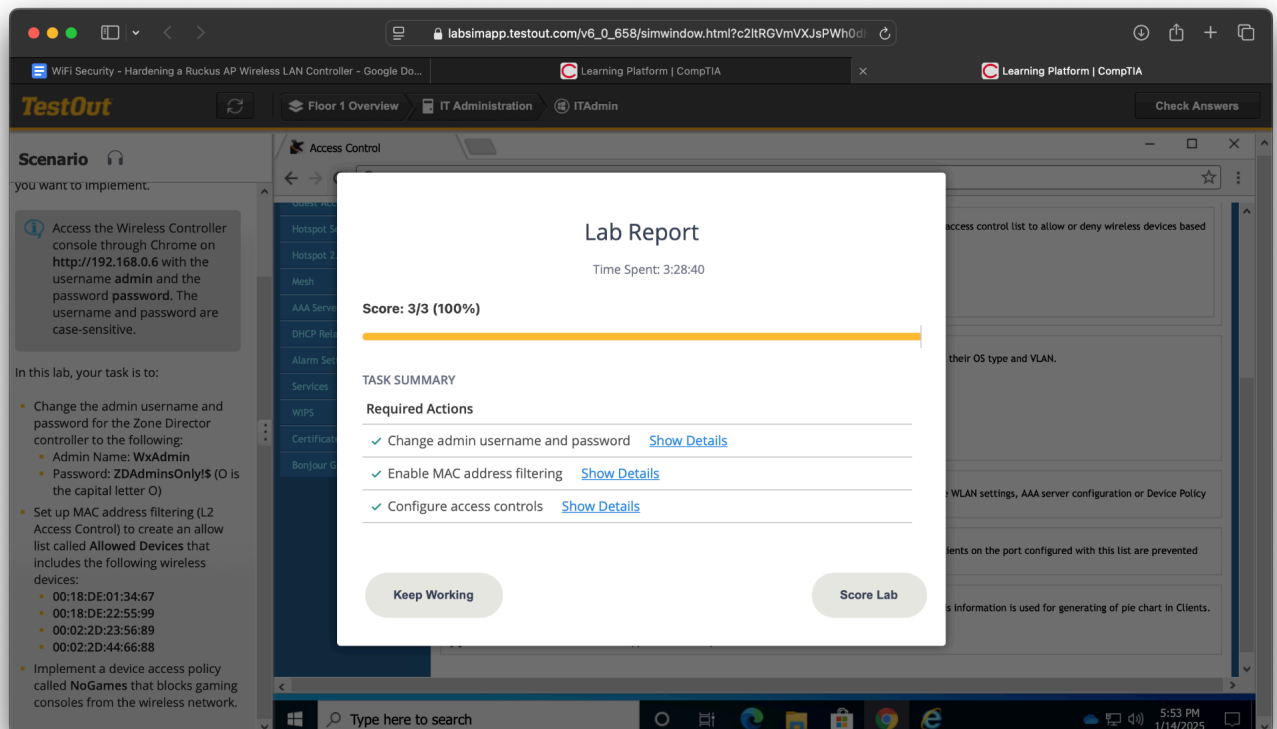
Robert Carpenter
github.com/robertmcarpenter
Tues January 14th 2025

After I enter all the rules I will click **Save** then **OK**.

At this point I have completed all tasks for this lab which are:

- **Change the admin username and password for the Zone Director controller to the following:**
 - **Admin Name: WxAdmin**
 - **Password: ZDAdminsOnly\$ (O is the capital letter O)**
- **Set up MAC address filtering (L2 Access Control) to create an allow list called Allowed Devices that includes the following wireless devices:**
 - **00:18:DE:01:34:67**
 - **00:18:DE:22:55:99**
 - **00:02:2D:23:56:89**
 - **00:02:2D:44:66:88**
- **Implement a device access policy called NoGames that blocks gaming consoles from the wireless network.**

This now concludes this lab on hardening a Ruckus WLAN Controller!



Robert Carpenter

github.com/robertmcarpenter

Tues January 14th 2025