Cambium Networks™

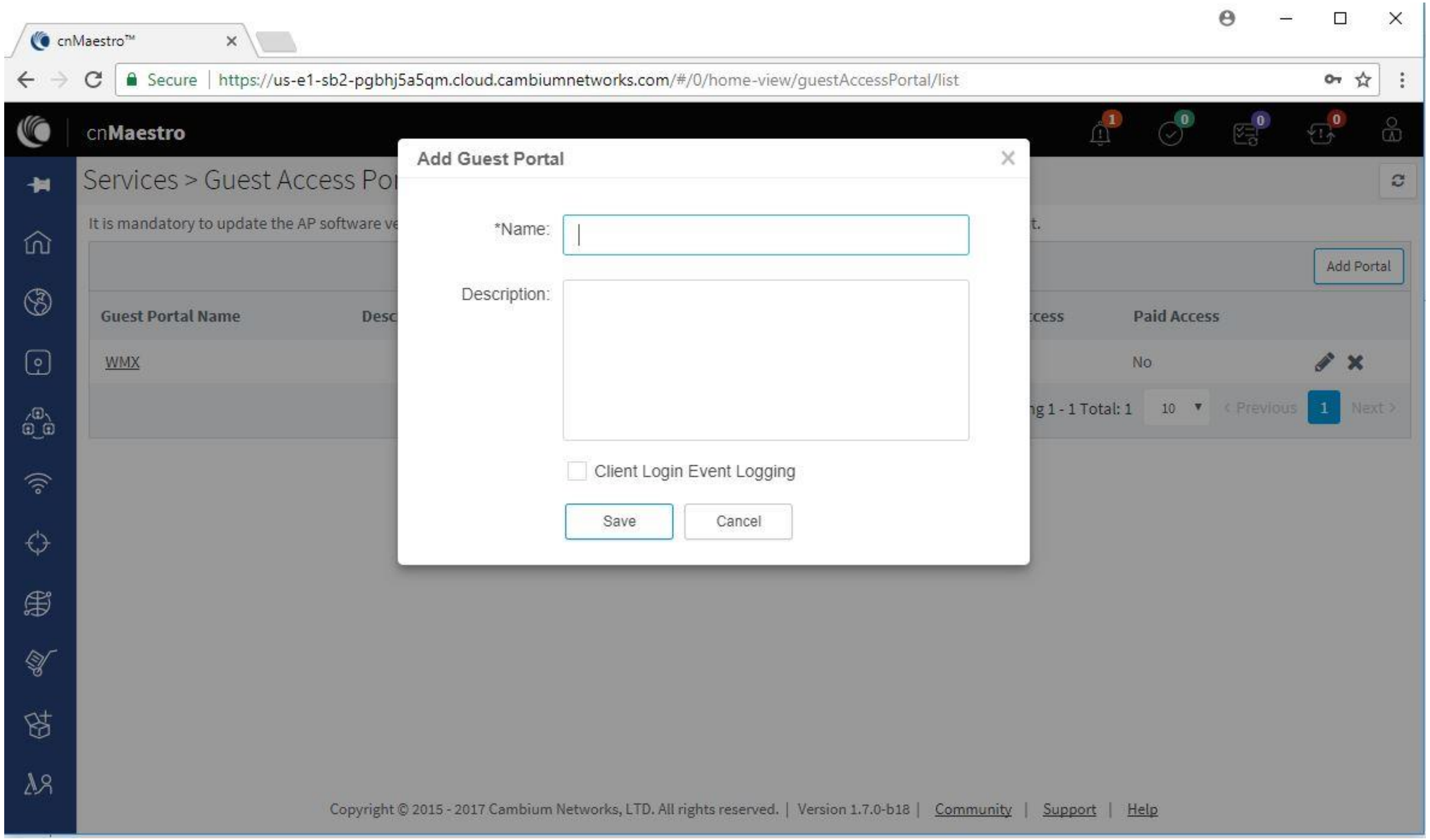
Guest WLAN without VLANs or Tunneling

Dave Moore
Sr Director, Wi-Fi Business Acceleration
Cambium Networks

cnPilot™

Create New Guest Portal

- Provide a Name and **write this down**. *You will need this name later when configuring the Guest WLAN*
    - Spaces are not allowed, but an underline is
- The Description is optional, but advisable
- Enabling Client Event Logging is advisable
- **Click Save** or this information will not be saved



cnMaestro™
Secure
https://us-e1-sb2-pgbhj5a5qm.cloud.cambiumnetworks.com/#/0/home-view/guestAccessPortal/list
cnMaestro
Services > Guest Access Por
Add Portal
Guest Portal Name
Desc
ccess
Paid Access
WMX
No
ng 1 - 1 Total: 1
10
‹ Previous
1
Next ›

It is mandatory to update the AP software ve ... t.

Add Guest Portal

*Name:

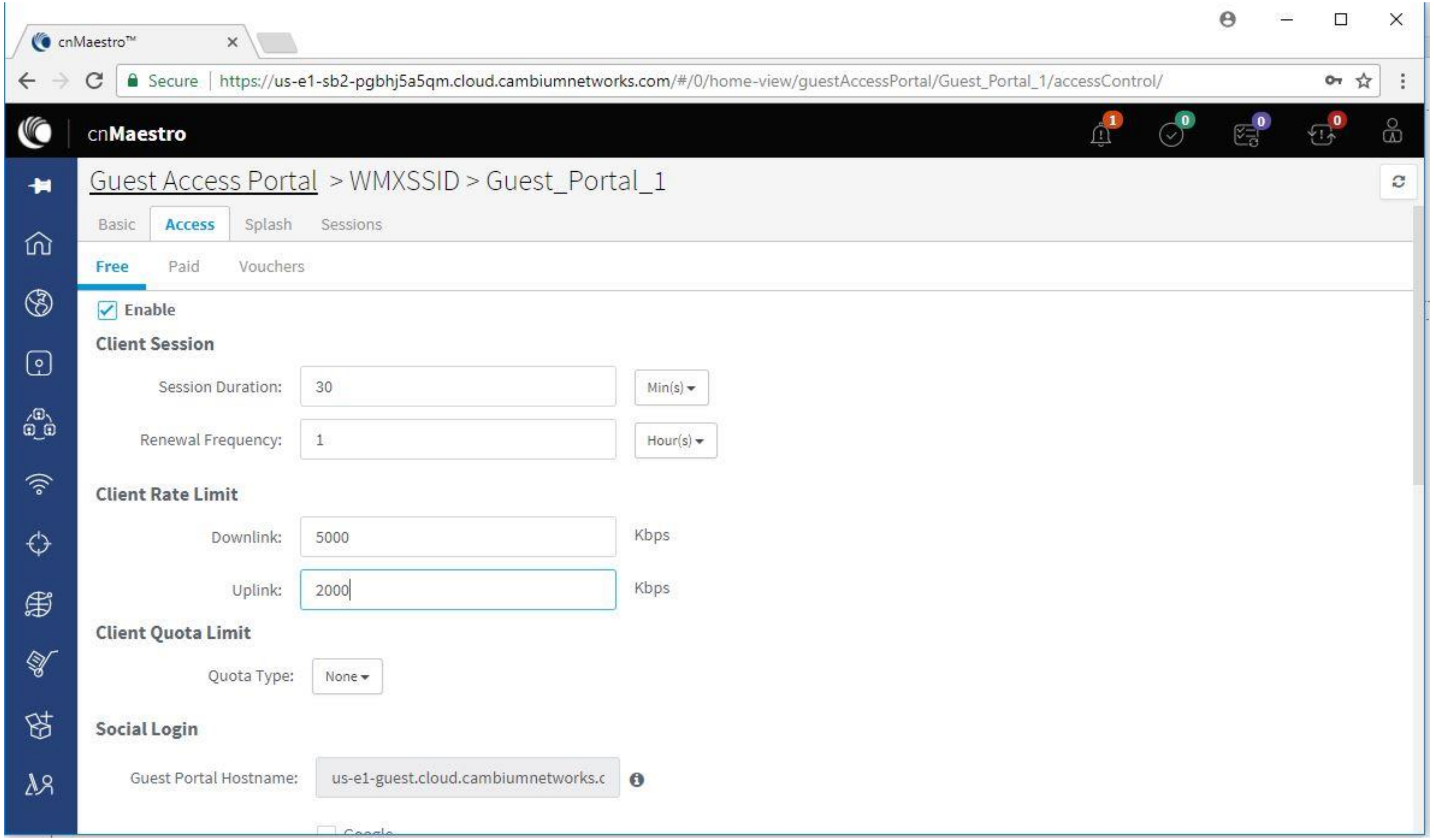
Description:

□ Client Login Event Logging

Copyright © 2015 - 2017 Cambium Networks, LTD. All rights reserved. | Version 1.7.0-b18 | Community | Support | Help

Configure Access Options

- If Free access is desired, enable and configure options
- Configure Paid and Voucher settings if desired
- **Click Save** at the bottom of the screen or these changes will not be saved.



https://us-e1-sb2-pgbhj5a5qm.cloud.cambiumnetworks.com/#/0/home-view/guestAccessPortal/Guest_Portal_1/accessControl/

Guest Access Portal > WMXSSID > Guest_Portal_1

☑ Enable

Client Session

Session Duration: 30 Min(s)

Renewal Frequency: 1 Hour(s)

Client Rate Limit

Downlink: 5000 Kbps

Uplink: 2000 Kbps

Client Quota Limit

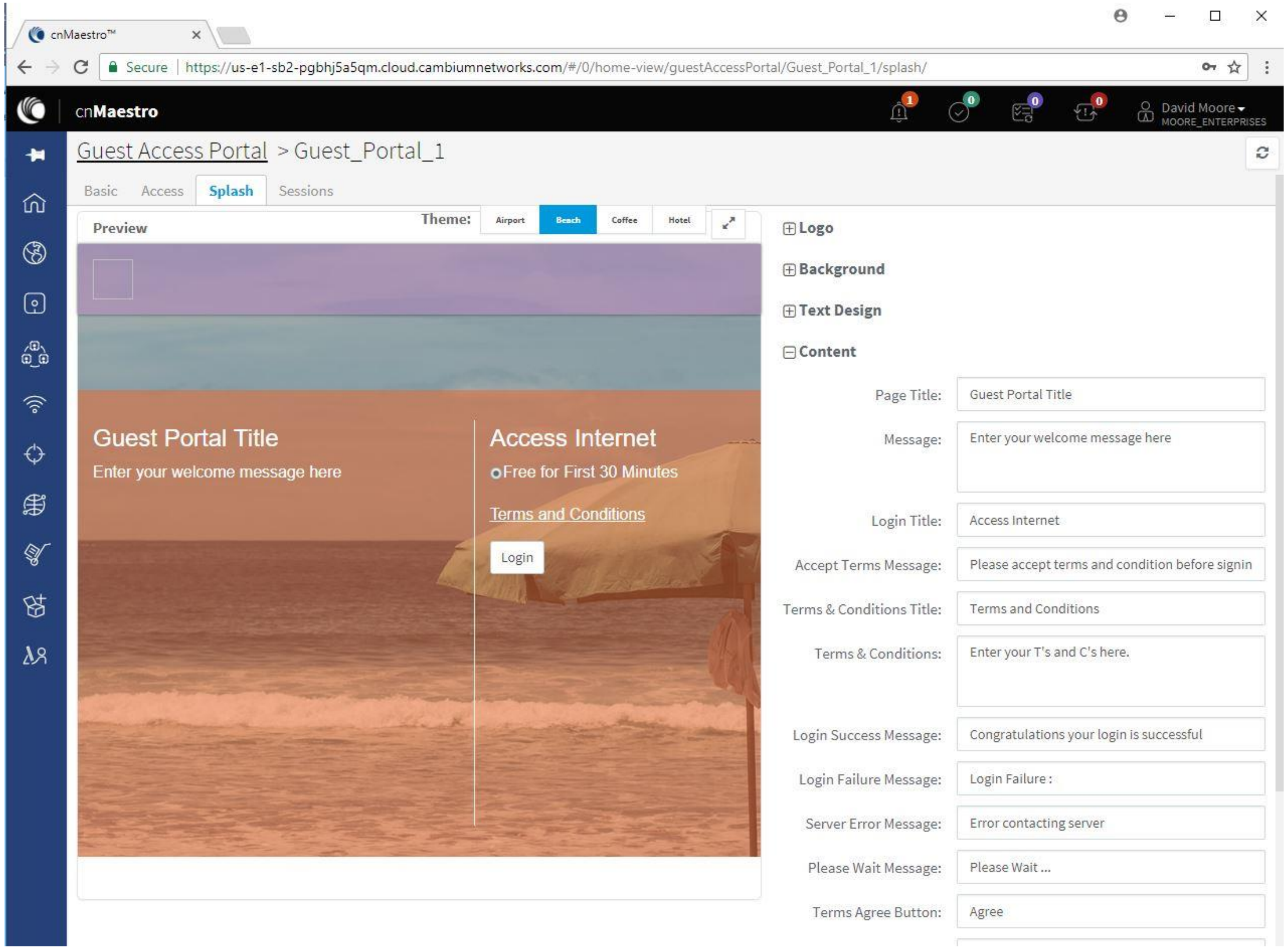
Quota Type: None

Social Login

Guest Portal Hostname: us-e1-guest.cloud.cambiumnetworks.c

Splash Page Configuration

- Choose the Theme desired
- Fill in Details
  - Title
  - Message
  - Terms and Conditions title and content
  - Free Access message details
  - Any others desired
- **Click Save** at the bottom of the screen or this will not be saved.



Page Title: Guest Portal Title

Message: Enter your welcome message here

Login Title: Access Internet

Accept Terms Message: Please accept terms and condition before signin

Terms & Conditions Title: Terms and Conditions

Terms & Conditions: Enter your T's and C's here.

Login Success Message: Congratulations your login is successful

Login Failure Message: Login Failure :

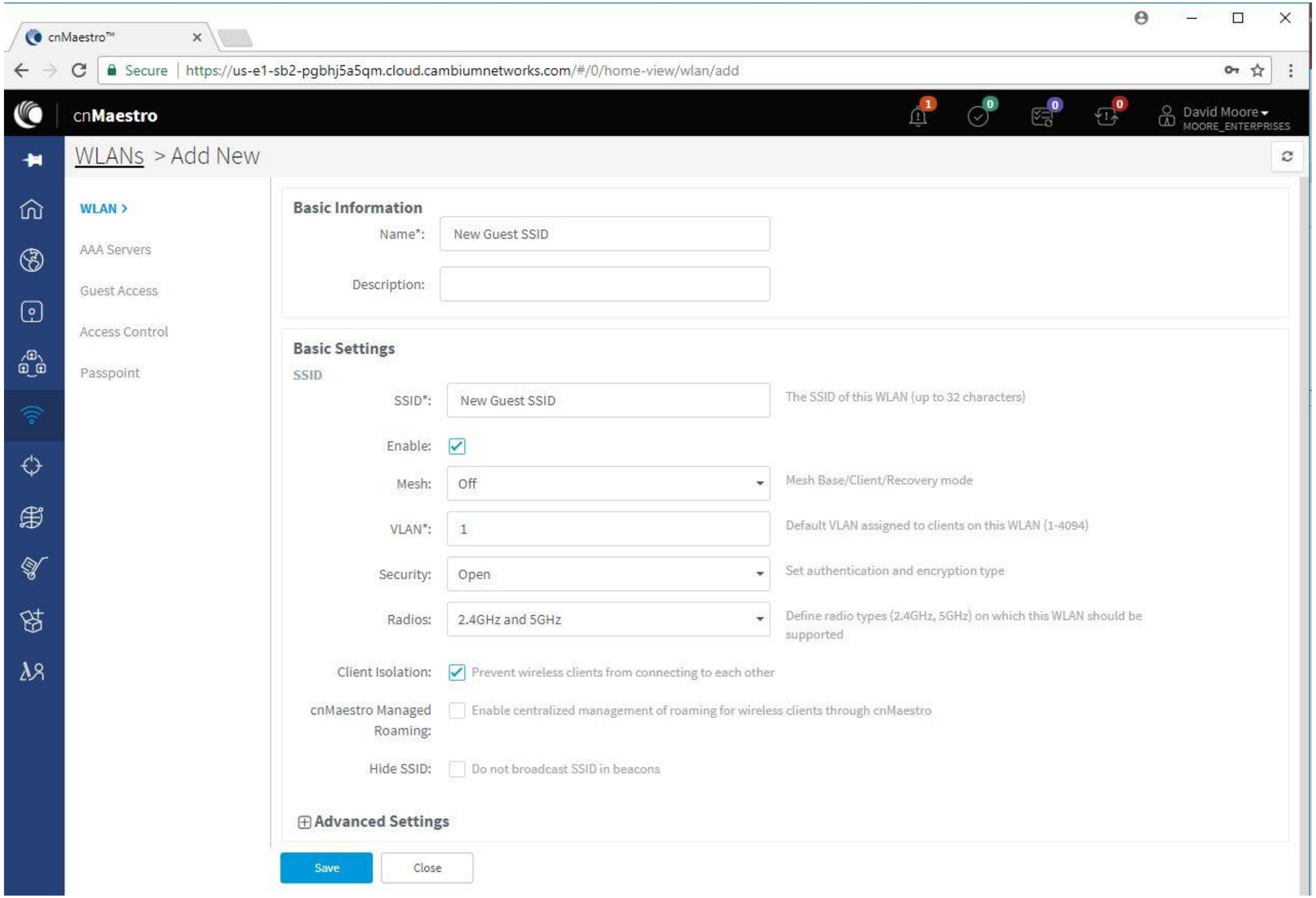
Server Error Message: Error contacting server

Please Wait Message: Please Wait ...

Terms Agree Button: Agree

Create new WLAN

- Add a new WLAN
- Provide a Name
- Enable Client Isolation to protect guests from each other
- **Click Save**



WLANs > Add New

Basic Information

Name*: New Guest SSID

Description:

Basic Settings

SSID

SSID*: New Guest SSID — The SSID of this WLAN (up to 32 characters)

Enable: ☑

Mesh: Off — Mesh Base/Client/Recovery mode

VLAN*: 1 — Default VLAN assigned to clients on this WLAN (1-4094)

Security: Open — Set authentication and encryption type

Radios: 2.4GHz and 5GHz — Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported

Client Isolation: ☑ Prevent wireless clients from connecting to each other

cnMaestro Managed Roaming: □ Enable centralized management of roaming for wireless clients through cnMaestro

Hide SSID: □ Do not broadcast SSID in beacons

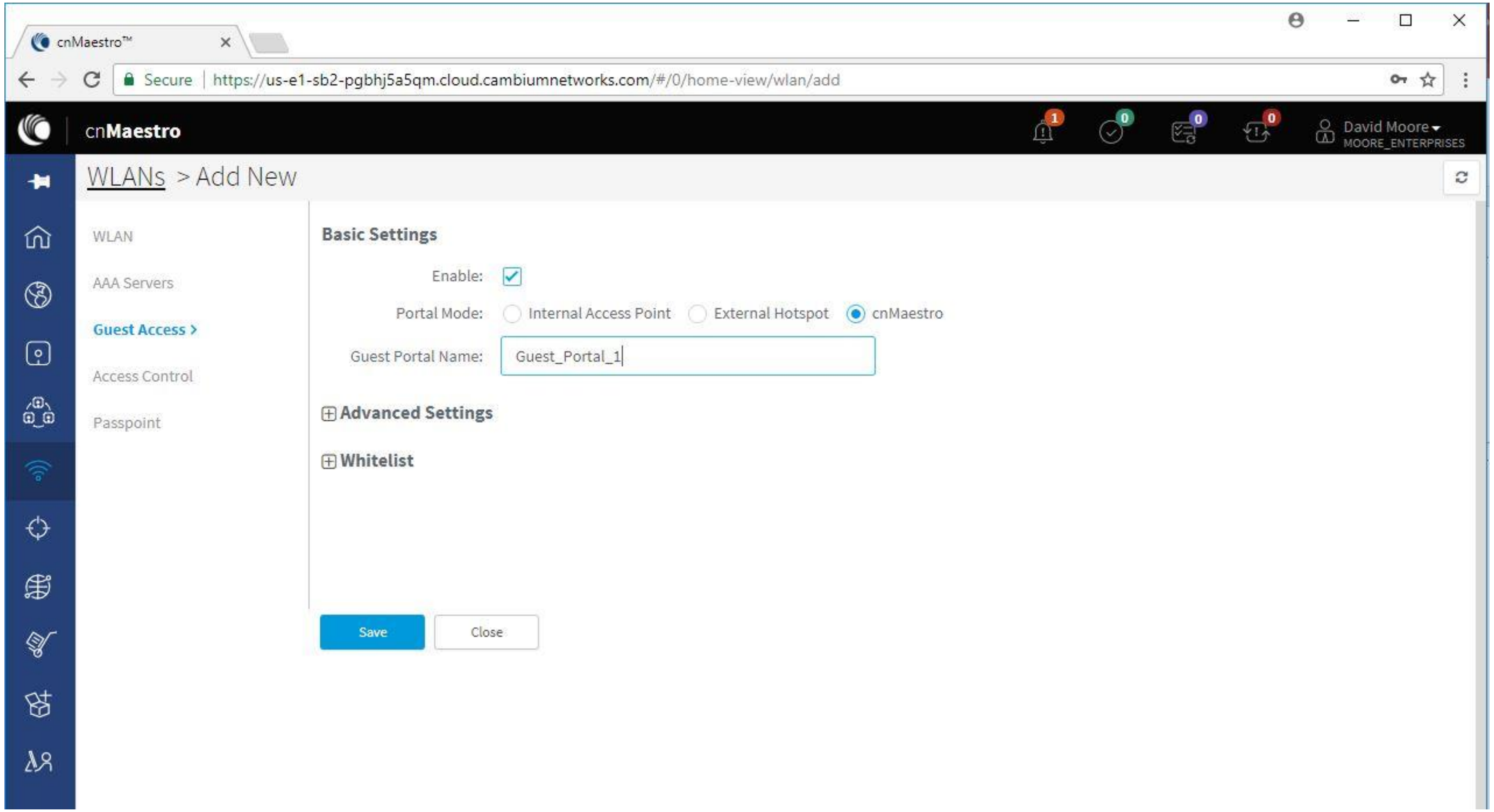
⊞ Advanced Settings

Save | Close

Cambium Networks™

Tie Guest Portal to Guest WLAN

- Enable Guest Access for WLAN
- Select cnMaestro for the Portal Mode
- Enter the ***exact name*** used for the Guest Portal created earlier
- Click Save



https://us-e1-sb2-pgbhj5a5qm.cloud.cambiumnetworks.com/#/0/home-view/wlan/add

WLANs > Add New

Basic Settings

Enable: ☑

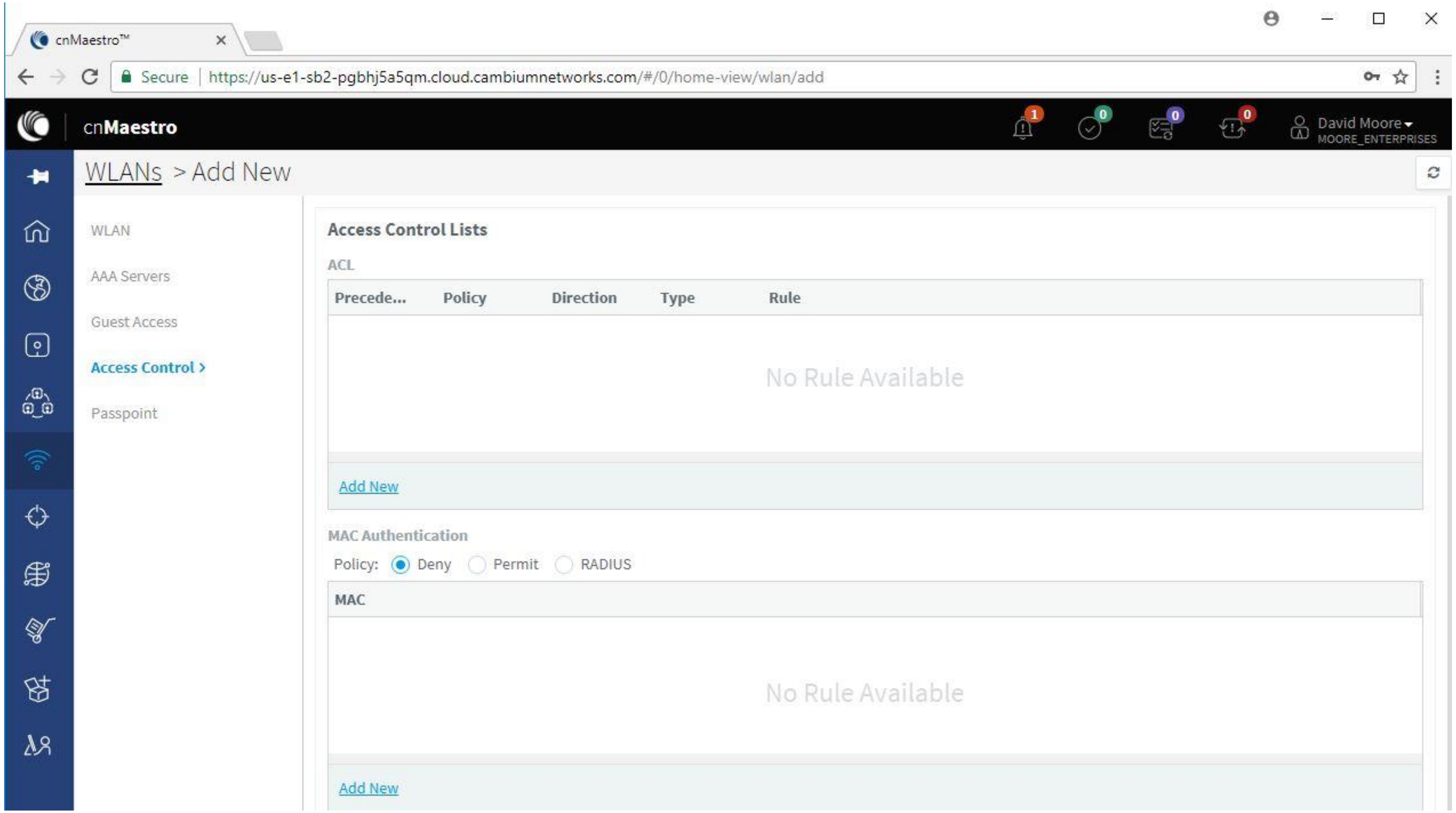
Portal Mode: ○ Internal Access Point ○ External Hotspot ● cnMaestro

Guest Portal Name: Guest_Portal_1

Cambium Networks™

Access Control List

- An Access Control List will be used to block Guests from the internal network
- If VLANs or Tunneling is used, this method may not be necessary, but it would not hurt to use it anyway.



Access Control Lists

ACL

Precede...	Policy	Direction	Type	Rule

No Rule Available

Add New

MAC Authentication

Policy: ● Deny ○ Permit ○ RADIUS

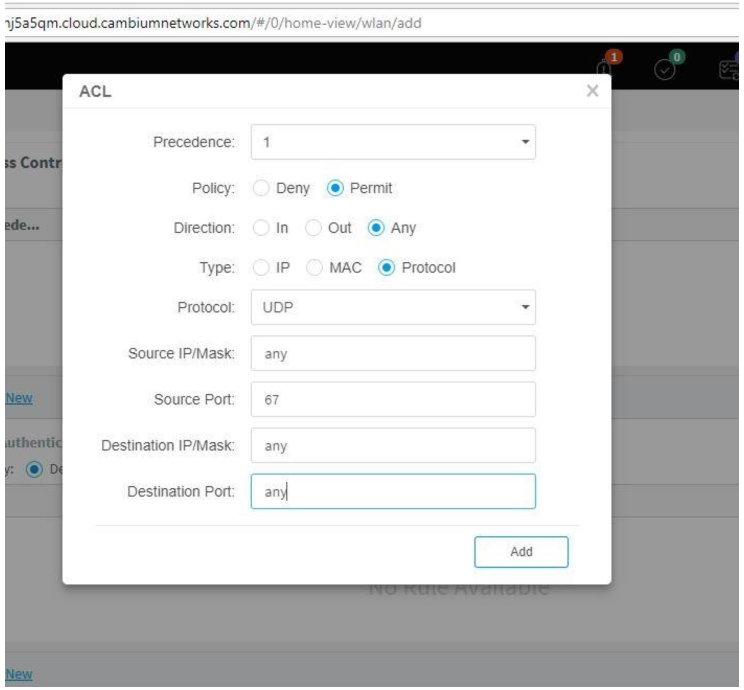
MAC

No Rule Available

Add New

ACL Entries to Allow DHCP Responses into WLAN

- Create 2 new entries for DHCP
  - UDP is most typically used
  - TCP is rarely used, but to be safe include this entry
- The order of entry is important
- *Pay careful attention to the Precedence number used, it is easy to accidentally overwrite a previously created entry*



j5a5qm.cloud.cambiumnetworks.com/#/0/home-view/wlan/add

ACL

Precedence: 1

Policy: ○ Deny ● Permit

Direction: ○ In ○ Out ● Any

Type: ○ IP ○ MAC ● Protocol

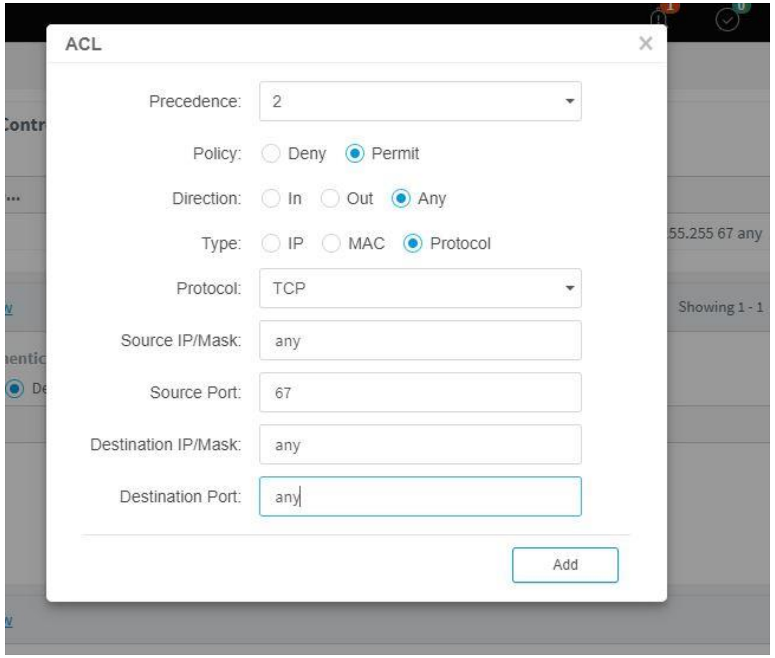
Protocol: UDP

Source IP/Mask: any

Source Port: 67

Destination IP/Mask: any

Destination Port: any



ACL

Precedence: 2

Policy: ○ Deny ● Permit

Direction: ○ In ○ Out ● Any

Type: ○ IP ○ MAC ● Protocol

Protocol: TCP

Source IP/Mask: any

Source Port: 67

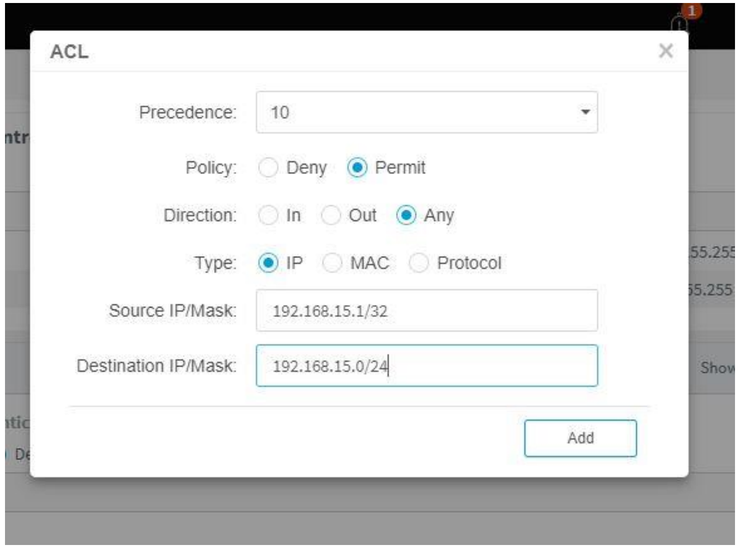
Destination IP/Mask: any

Destination Port: any

Cambium Networks™

ACL Entries to Allow DNS

- Two Entries are needed for DNS
  - One for DNS server to WLAN
  - One for WLAN to DNS Server
- In this example 192.168.15.1 is the DNS server.
- If more than one DNS server is utilized, there should be two entries for each one
- *Pay attention to the Precedence order as these entries must occur before deny entries added next*



Precedence: 10

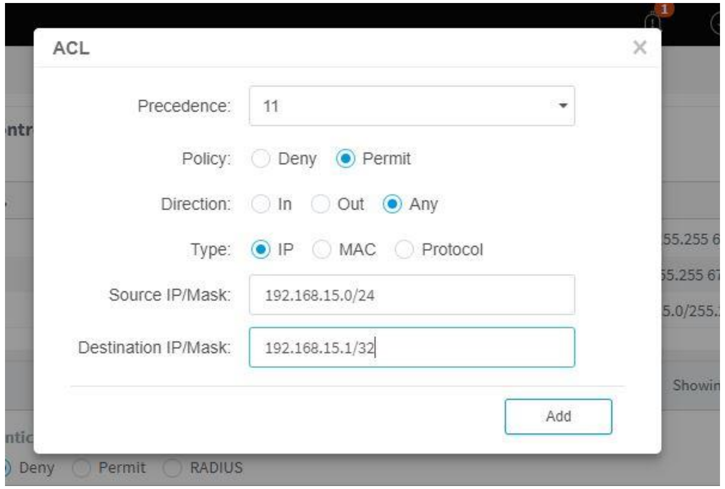
Policy: ○ Deny ● Permit

Direction: ○ In ○ Out ● Any

Type: ● IP ○ MAC ○ Protocol

Source IP/Mask: 192.168.15.1/32

Destination IP/Mask: 192.168.15.0/24



Precedence: 11

Policy: ○ Deny ● Permit

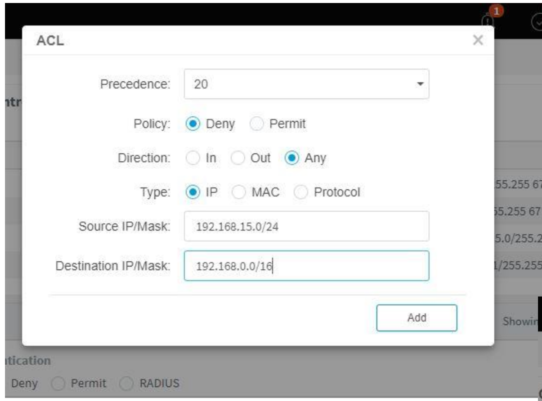
Direction: ○ In ○ Out ● Any

Type: ● IP ○ MAC ○ Protocol

Source IP/Mask: 192.168.15.0/24

Destination IP/Mask: 192.168.15.1/32

Block Access to Internal Subnets



ACL

Precedence: 20

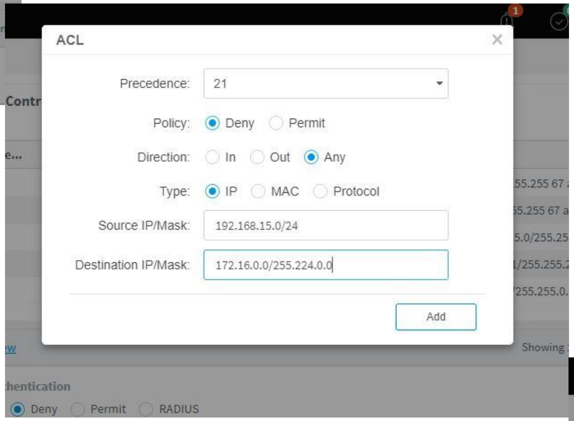
Policy: ● Deny ○ Permit

Direction: ○ In ○ Out ● Any

Type: ● IP ○ MAC ○ Protocol

Source IP/Mask: 192.168.15.0/24

Destination IP/Mask: 192.168.0.0/16



ACL

Precedence: 21

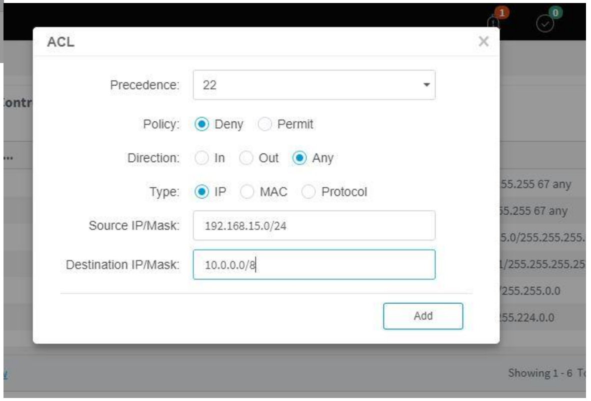
Policy: ● Deny ○ Permit

Direction: ○ In ○ Out ● Any

Type: ● IP ○ MAC ○ Protocol

Source IP/Mask: 192.168.15.0/24

Destination IP/Mask: 172.16.0.0/255.224.0.0



ACL

Precedence: 22

Policy: ● Deny ○ Permit

Direction: ○ In ○ Out ● Any

Type: ● IP ○ MAC ○ Protocol

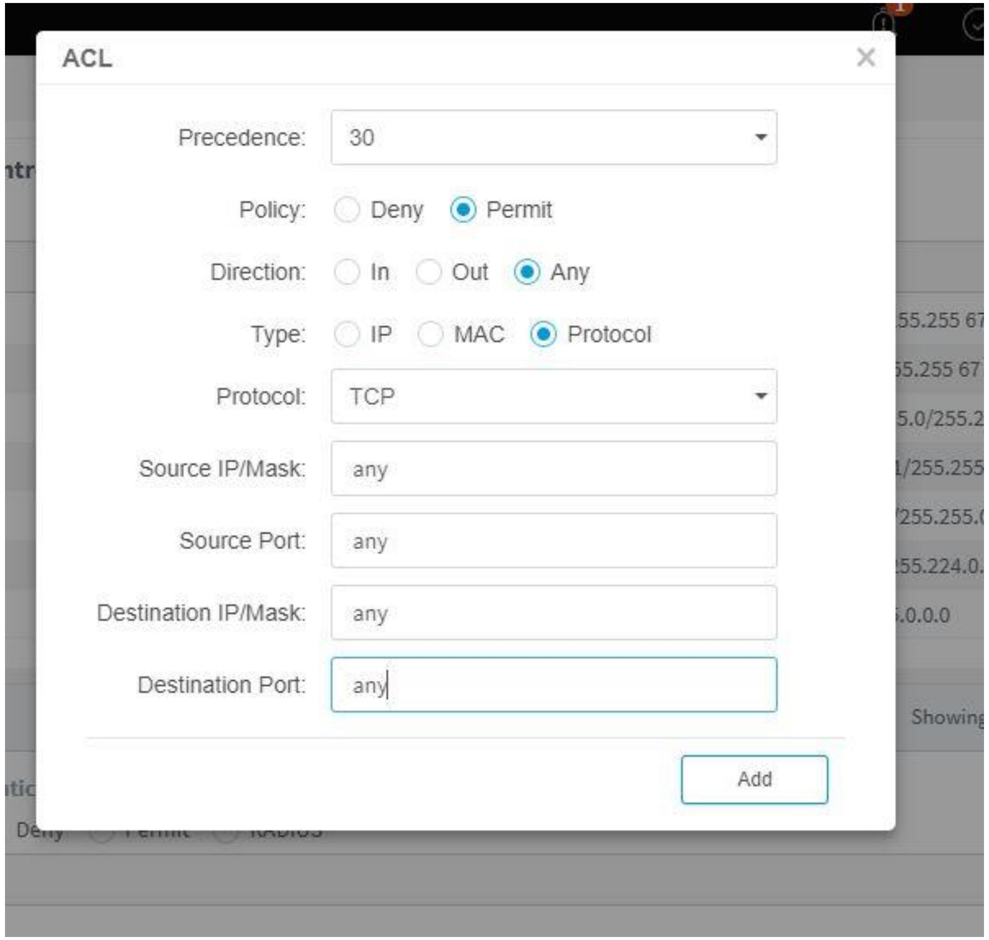
Source IP/Mask: 192.168.15.0/24

Destination IP/Mask: 10.0.0.0/8

- Three entries are needed to block access to private IP address subnets
- Each of these are deny statements
- In this example, the Guest WLAN subnet is 192.168.15/24.
- If there are multiple subnets used for the Guest WLAN, three deny entries are needed for each one

Allow Web Traffic to Guest WLAN

- The final ACL entry needs to be a permit statement to allow all TCP traffic
  - All valid web traffic is TCP-based
- There is an implicit deny for anything not specifically defined in the ACL list



ACL

Precedence: 30

Policy: ○ Deny ● Permit

Direction: ○ In ○ Out ● Any

Type: ○ IP ○ MAC ● Protocol

Protocol: TCP

Source IP/Mask: any

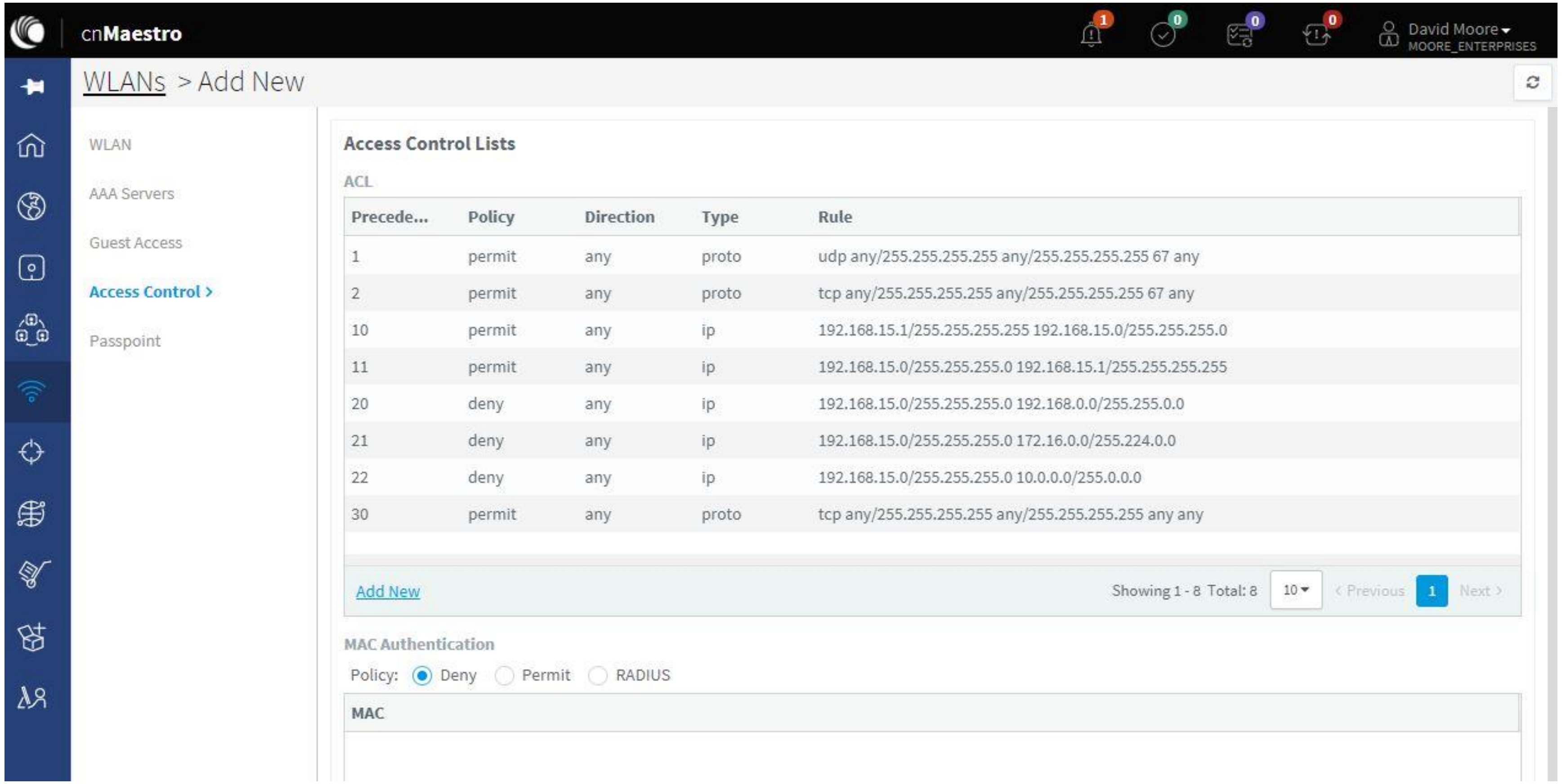
Source Port: any

Destination IP/Mask: any

Destination Port: any

ACL List Completed

- Check over the completed ACL
- Verify the precedence order
- Verify that Permit and Deny Policies are correctly entered
- It is possible to edit any of the entries
- **Click Save** at the bottom of the screen



Access Control Lists

ACL

Precede...	Policy	Direction	Type	Rule
1	permit	any	proto	udp any/255.255.255.255 any/255.255.255.255 67 any
2	permit	any	proto	tcp any/255.255.255.255 any/255.255.255.255 67 any
10	permit	any	ip	192.168.15.1/255.255.255.255 192.168.15.0/255.255.255.0
11	permit	any	ip	192.168.15.0/255.255.255.0 192.168.15.1/255.255.255.255
20	deny	any	ip	192.168.15.0/255.255.255.0 192.168.0.0/255.255.0.0
21	deny	any	ip	192.168.15.0/255.255.255.0 172.16.0.0/255.224.0.0
22	deny	any	ip	192.168.15.0/255.255.255.0 10.0.0.0/255.0.0.0
30	permit	any	proto	tcp any/255.255.255.255 any/255.255.255.255 any any

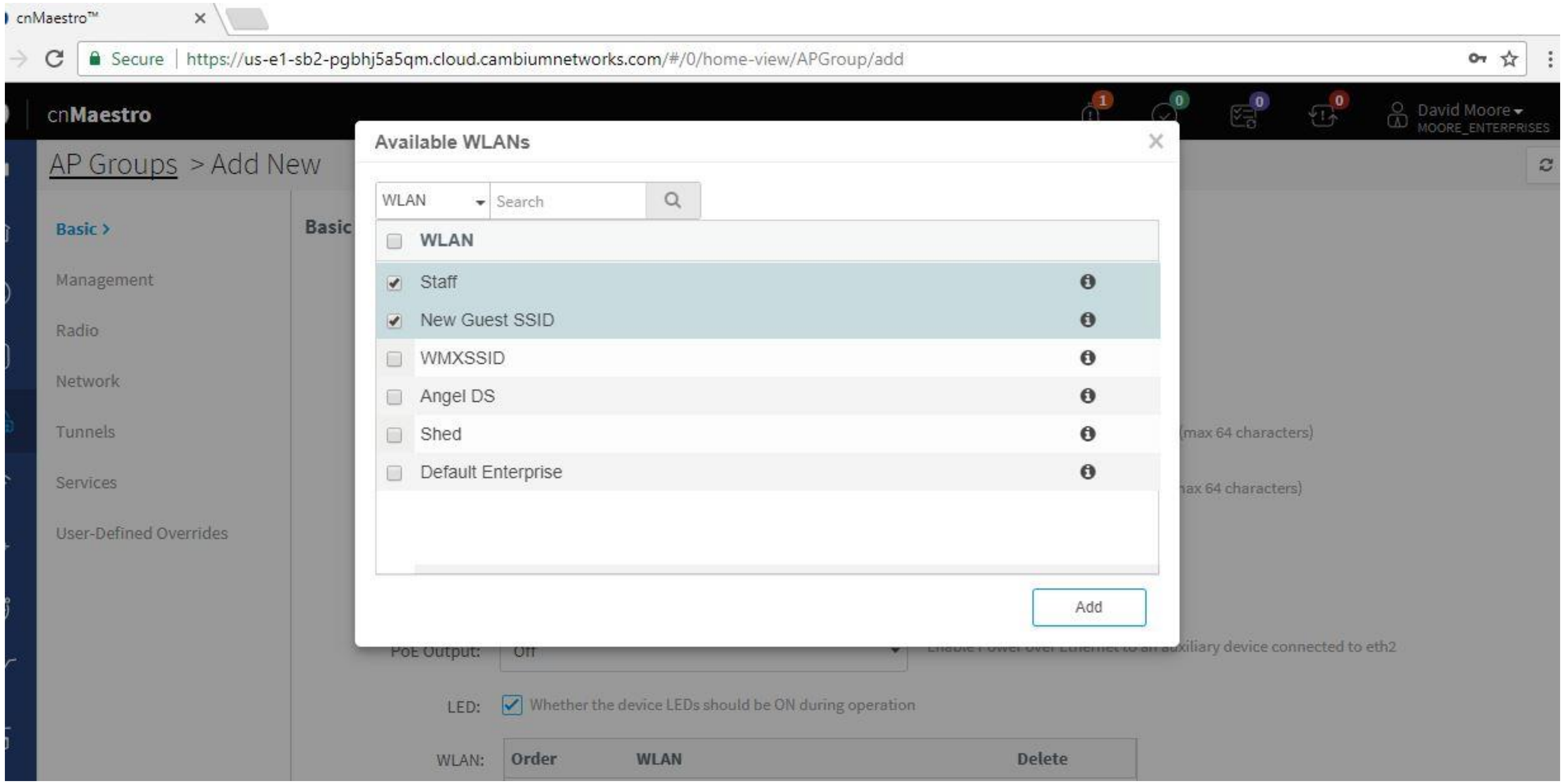
MAC Authentication

Policy: ● Deny ○ Permit ○ RADIUS

MAC

Add Guest WLAN into AP Group

- It is assumed that an AP Group has already been created. If not, add, configure an AP Group, and Claim APs into the Group when ready
- Add in the WLANs to be used by this AP Group, to include the newly created Guest WLAN
- **Click Save** at the bottom of the screen



Available WLANs

WLAN

□	WLAN
☑	Staff
☑	New Guest SSID
□	WMXSSID
□	Angel DS
□	Shed
□	Default Enterprise

PoE Output: Off — Enable Power over Ethernet to an auxiliary device connected to eth2

LED: ☑ Whether the device LEDs should be ON during operation

WLAN: Order | WLAN | Delete

JOB DONE

Cambium Networks™