6950 SW Hampton St., Ste 308
Tigard, OR 97223
ULMBR-0002-I

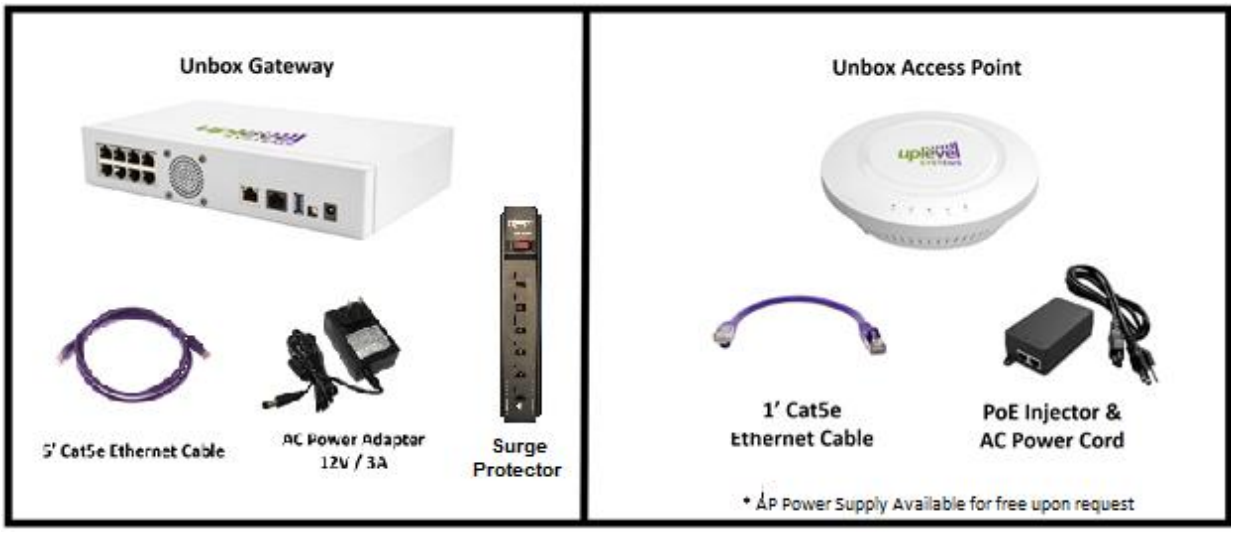
Unbox Quick Start Guide

To Our Partners

Welcome to Uplevel Systems! We are so excited to have you as a part of the team. As a partner, Uplevel team members want to empower you to grow your business as easily and efficiently as possible. Our goal is to provide you with as much information as possible and provide you the tools you need to succeed. If there is ever any assistance or materials we can better provide for you, please contact Uplevel Support at support@uplevelsystems.com or (971) 770-2468.

Before logging into you Uplevel Unbox Gateway, locate a "Your Uplevel System has Shipped" email from our team as well as Welcome Letter along with this one located in the box with your login information. This will allow you to login to our online portal and access the system dashboard and controls. Once you locate this login information, login and begin setting up the system.

Verify Contents



*One additional Cat5e (or Cat 6) cable will be needed beyond what is provided in the box to connect the PoE injector to the AP. The cable length necessary is specific to the deployment environment. Be sure to use Cat5e and Cat6 cables to ensure proper performance.

Figure 1 – System Components

Missing Items?

If any items are missing from your package, please contact an Uplevel Support Engineer, by

emailing support@uplevelsystems.com or by phone at (971) 770-2468.

Setting Up using Dynamic IP Addresses

This section describes how to set up Unbox as into a network that can provide an IP address via DHCP to the Internet port of the Unbox gateway. Typically, this DHCP server will run in an ISP's cable modem or DSL router, but it can come from other servers in a more advanced deployment. The important characteristics are:

- The "upstream" Internet connection from the Unbox gateway can *provide* an IP address via DHCP
- The device or network that provides that address also provides connectivity to the Internet

See Connecting using a Static IP from the ISP for the case where static IP addresses are used to provide Internet connectivity instead of DHCP.

Connect Gateway and Access Point

An 802.3at (30W) PoE injector is supplied to provide power to the Unbox Access Point (AP). The Unbox Gateway does not support PoE directly so this PoE injector provides power to be indirectly supplied to the AP when configured as shown in Figure 2.

Note that Uplevel Switches (not shown) ***do*** support PoE, so in the event a switch is also deployed within the network then there is no need for the PoE injector.

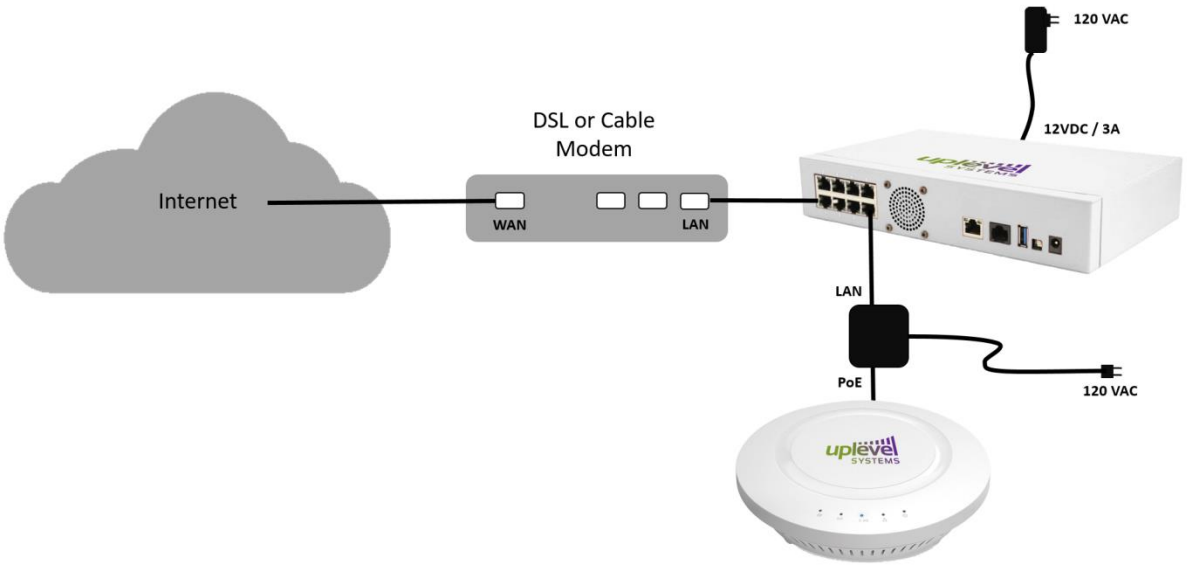


Figure 2 – System Configuration using PoE

Connect the system as shown in Figure 2 using the Ethernet cables provided. It is essential to use Cat5e or Cat6 rated Ethernet cables in these connections. Using lower rated cables will lead to problems with PoE power distribution, and will degrade network data delivery in both configurations.

Port 1 on the Unbox Gateway, i.e., the lower left port on the Ethernet panel of the Gateway is reserved for Internet and should be directly connected to the DSL or Cable Modem's LAN port using the supplied five-foot Ethernet cable. Unbox does not replace the service provider's termination equipment or service providers router.

Ideally, the service provider modem should have a DHCP server enabled on its LAN interface, or the Internet service provider should provide an IP address via DHCP from the central office. In a typical cable modem or DSL environment, the service provider router will typically have a DHCP server enabled to serve addresses through its LAN ports. For PON networks, the service provider will commonly server an IP address directly to the LAN interface. In either case, it is important to know whether the equipment connected to the Unbox Internet port is serving an IP address via DHCP. For more information about your particular service providers equipment and capabilities please contact your service provider. Note that the Unbox Gateway will require one IP address from the service provider's DHCP address pool when using DHCP.

For some circumstances, such as dedicated circuits, or in cases where it has been requested, Unbox can support the use of a static IP addresses on the Internet port. To learn more about how to set configure the gateway from static to dynamic IP addresses check out the Uplevel Unbox Training Guide.

A one foot Ethernet cable has been provided to connect between the Unbox Gateway and the LAN port on the PoE injector. An additional Cat6 or Cat5e Ethernet cable (not provided) will be needed for the connection between the PoE port on the PoE injector and the AP. Any of the remaining Ethernet Ports 2 through 8 on the Gateway can be used to connect the Access Point.

You'll want to ensure the PoE injector's LAN cable is plugged into one of the remaining ports and PoE side is plugged into the AP directly with ***nothing in between***. Ensure that there is a direct cable connection between the PoE injector's PoE port and the Access Point, with no switches or routers intervening. The Gateway will automatically detect the Access Point and configures the Ethernet port appropriately. The other Ethernet ports may be used to connect customer Ethernet devices such as computers and printers.

The order in which power is applied to the system is not critical. It will take about 5 minutes for the system to fully boot and become manageable from the dashboard. When power is connected to the Unbox Gateway, the Power (**P**) and Port 1 LEDs on the back of the unit will light green. In addition, any ports with active Ethernet links unit will also have their

corresponding LEDs lit. Once power has been applied to the Gateway make sure to allow for the box to fully boot up before unplugging the box again.

As the AP boots, you will initially notice its Power LED turn amber and begin flashing. The Ethernet LED should also turn blue to indicate a valid Ethernet connection. When the AP has booted up completely, its Power LED stops flashing and becomes solid amber. The 2.4G and 5G lights on the AP will not light up, since there are no Wi-Fi SSIDs configured at this time.

Connecting using a Static IP from the ISP

When the service provider's equipment does not use DHCP, then it is necessary to use static IP addressing. This section describes how to configure the Internet connection of the Unbox gateway accordingly.

Static IP Addressing on the Internet Connection

It is necessary to physically connect to the gateway in order to configure a static IP. This requirement exists so that any misconfiguration can be immediately detected and corrected before you leave the customer site. There is a very real opportunity to “strand” a unit when static IP addresses are configured remotely and a wrong value is entered.

To configure a Obtain a suitable RS232C serial cable terminated in a standard RJ-45 jack (also known as "Cisco style"). Obtain a suitable serial terminal program such as PuTTY. PuTTY can be downloaded from http://www.putty.org. Set the serial terminal program settings to:

- 115200 baud
- No parity, 8 data bits, 1 stop bit
- No hardware flow control
-

Connect the RJ-45 jack on the RS232C serial cable to the port marked "Console" on the UG-101. See the picture below.

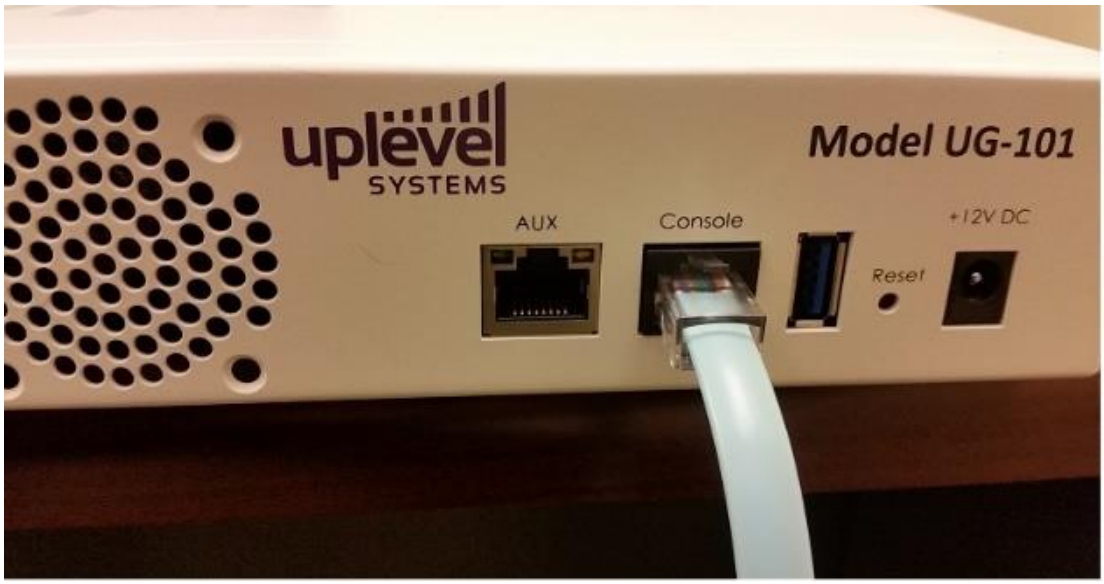


Figure 3a – Static IP Configuration

Connect the other end of the serial cable (USB side, or DB-9 if a DB-9 cable is being used) to your computer, and start the serial terminal program. Power on the UG-101 and wait approximately 3 minutes. You should now see on the serial terminal program:

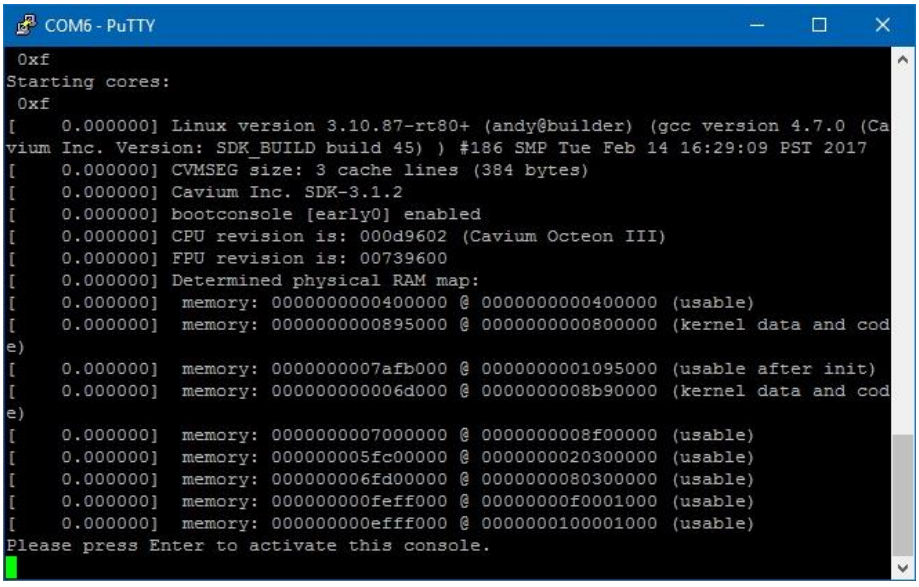


Figure 3b – Static IP Configuration

Hit enter to activate the serial console. In a few seconds, are presented with a prompt:

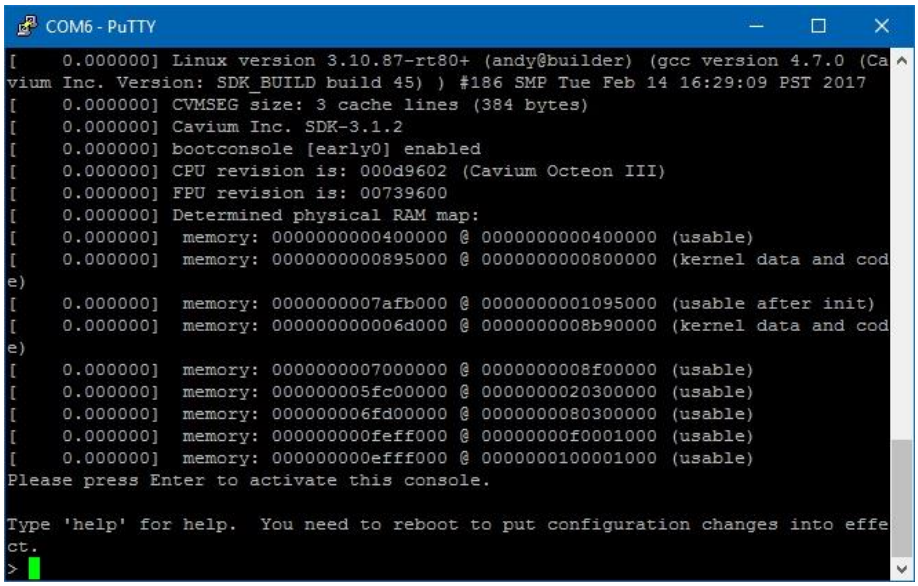


Figure 3c – Static IP Configuration

You may type **help** to see the available commands:

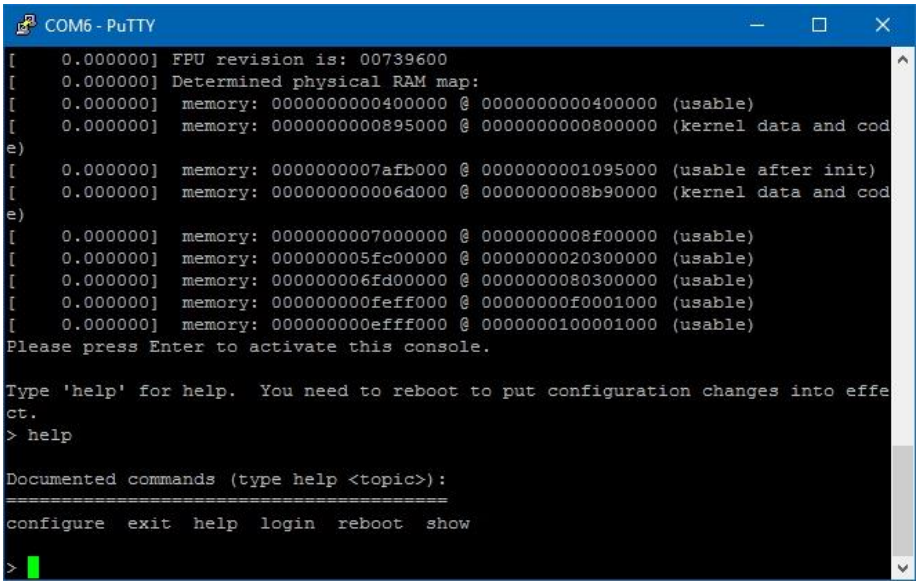


Figure 3d – Static IP Configuration

To see the current serial settings, type **show**

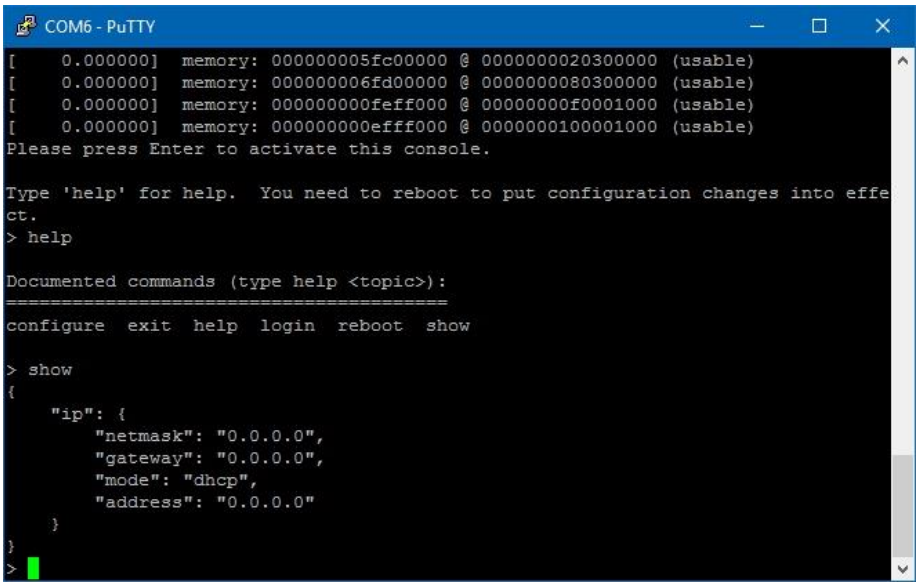


Figure 3e – Static IP Configuration

To configure the system for static IP, type first **configure** followed by **ip**

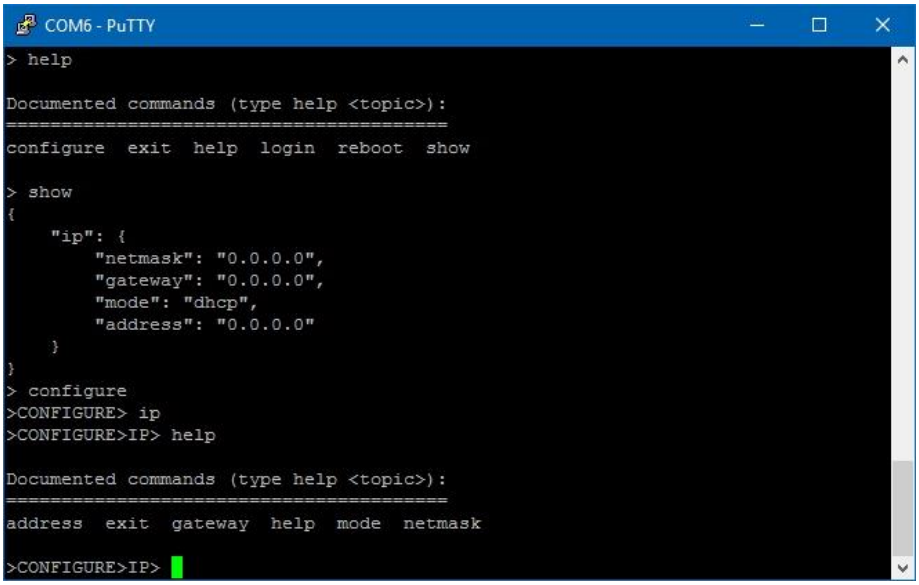


Figure 3f – Static IP Configuration

The parameters needed for static IP mode are usually the IP address, the netmask, the gateway, and the mode of operation (either "dhcp" or "static"). Set these parameters according to the following screen by typing in the command followed by the value:

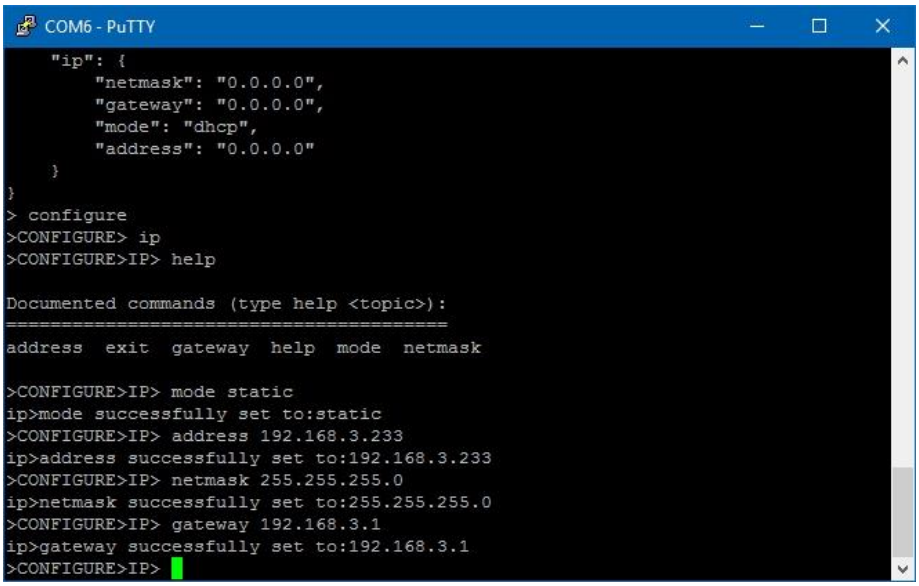


Figure 3g – Static IP Configuration

Once the parameters have been entered, type **exit** twice to quit the configuration process.

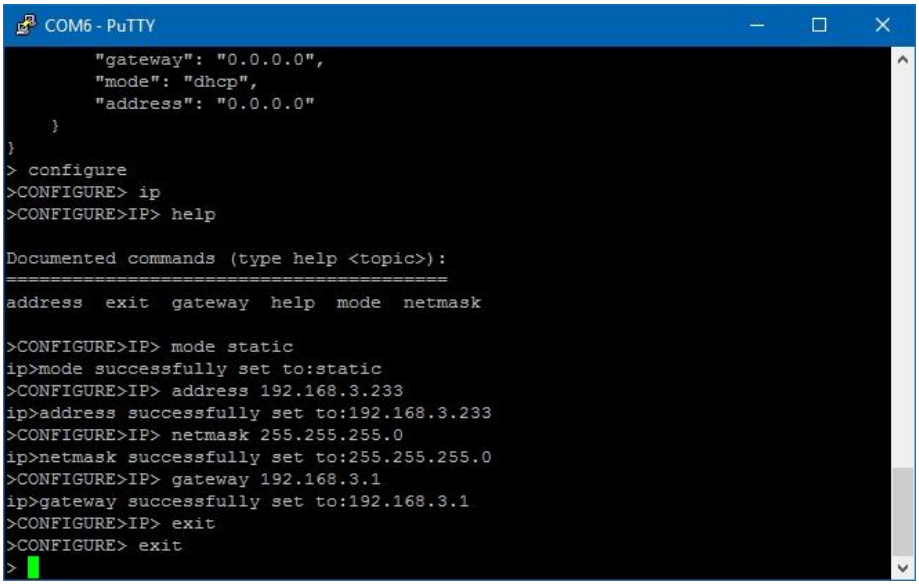


Figure 3h – Static IP Configuration

You may now confirm the settings before applying them by using the **show** command

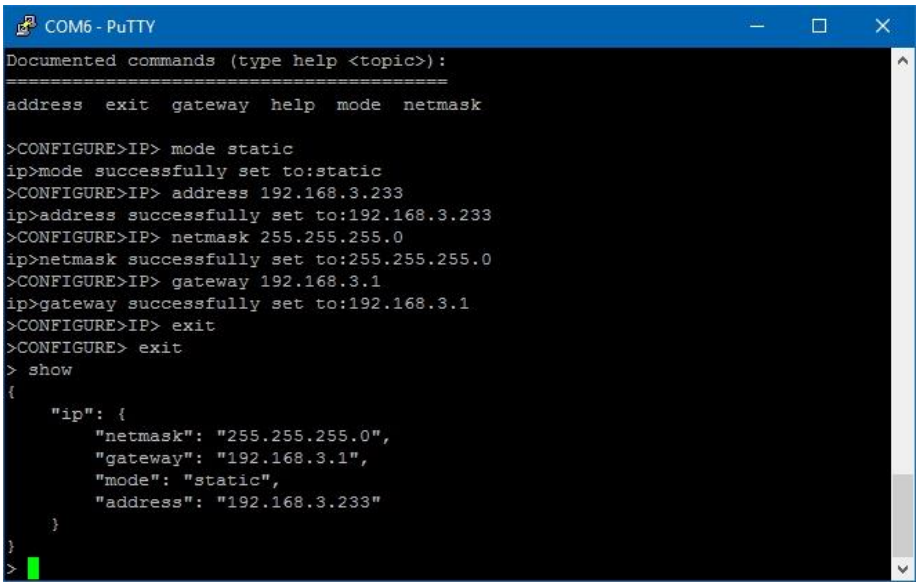


Figure 3i – Static IP Configuration

To apply the parameters, simply reboot the UG-101 using the **reboot** command:

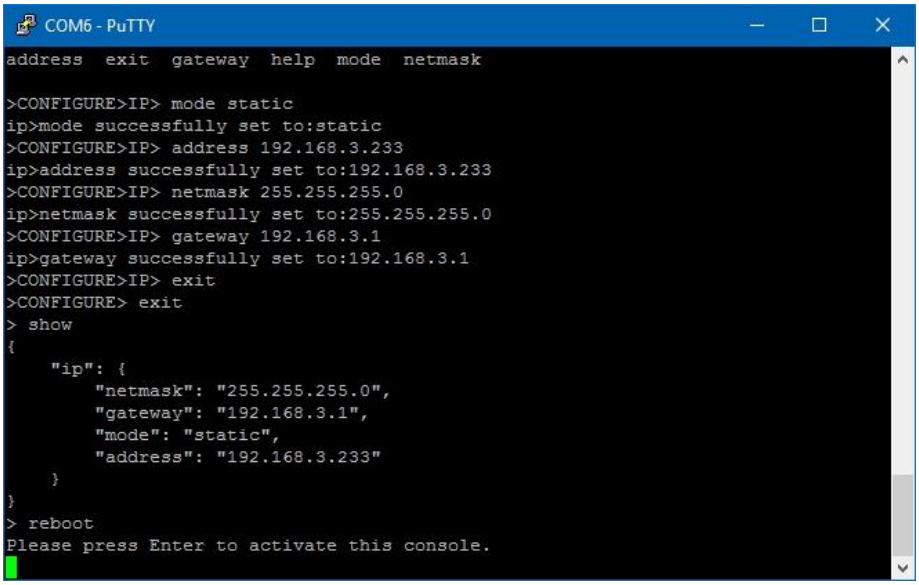


Figure 3j – Static IP Configuration

Ignore further output to the console after typing in **reboot**. In approximately 3 minutes, the configuration will be applied and the UG-101 will be rebooted. Once the UG-101 has come back up, you may verify on the serial console that the static IP settings are now being used, by typing the **show** command:

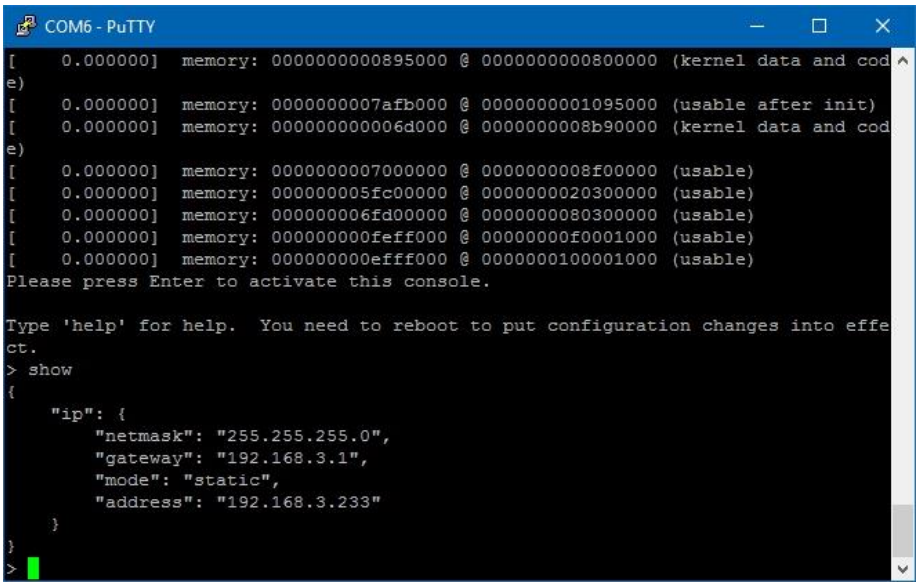


Figure 3k – Static IP Configuration

To revert to DHCP mode, simply repeat the above steps, but this time type **mode dhcp** rather than **mode static**. The remaining parameters such as address and gateway are irrelevant and can be ignored. The UG-101 will obtain these automatically from the DHCP server. That is, when mode is indicated as 'dhcp', the parameters 'netmask', 'gateway', and 'address' may be set to any value without harm.

Verify Ethernet Operation

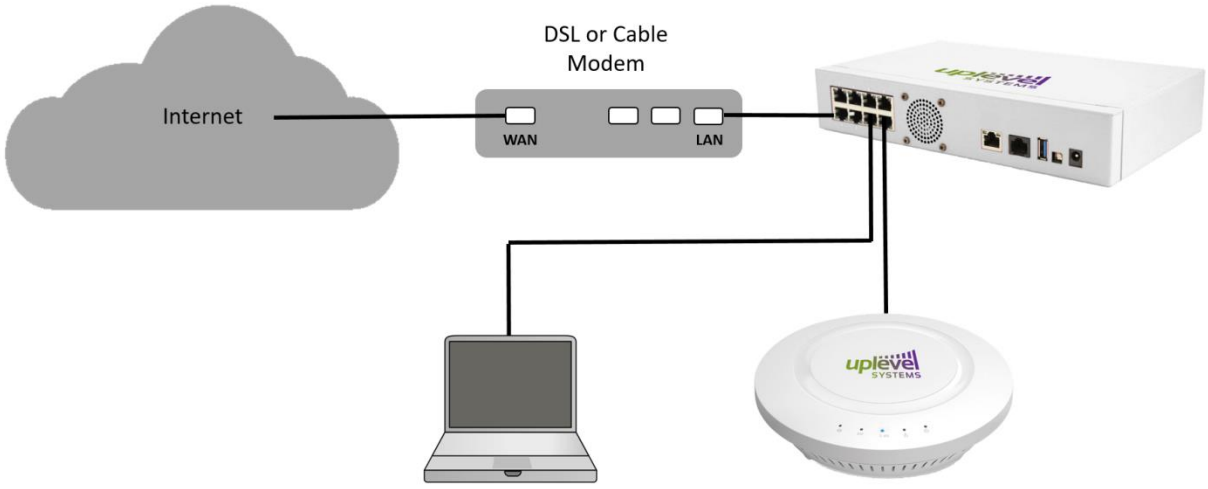


Figure 4 – Laptop Connection to Test Operation

To verify operation, connect a laptop to port 5 on the Unbox Gateway using an Ethernet cable as shown in Figure 4. Disable Wi-Fi on the laptop. Configure the laptop's Ethernet interface to obtain an IP address using DHCP, and verify that the laptop has received an address from the Unbox Gateway.

Open an Internet browser on the laptop and browse to any Internet address such as http://www.google.com. The web page should appear if everything is configured and working correctly. Please remember to allow for roughly 5 minutes after connecting the Gateway to the Internet and applying power for the Gateway to power up and become fully functional.

Ensuring Connectivity

Using a standard web browser, go to www.uplevelsystems.com and click on the **Log In** menu item at the top right of the page.

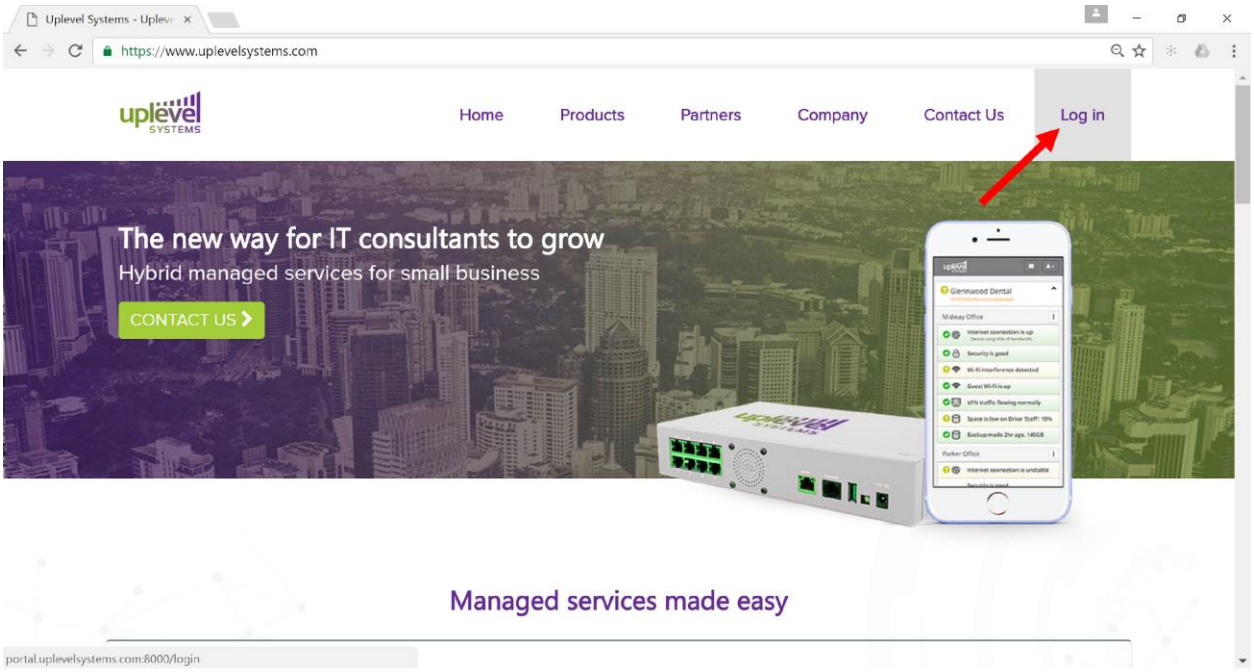


Figure 5– Accessing Log in

Enter your username and password when prompted as shown in Figure 6. The login credentials are found in the Welcome Letter from Uplevel Systems.

Figure 6 – Enter Credentials

After providing your login credentials, you will be presented with the dashboard view shown below in Figure 7. The dashboard view contains the status for all services, sites, and customers on a single page.

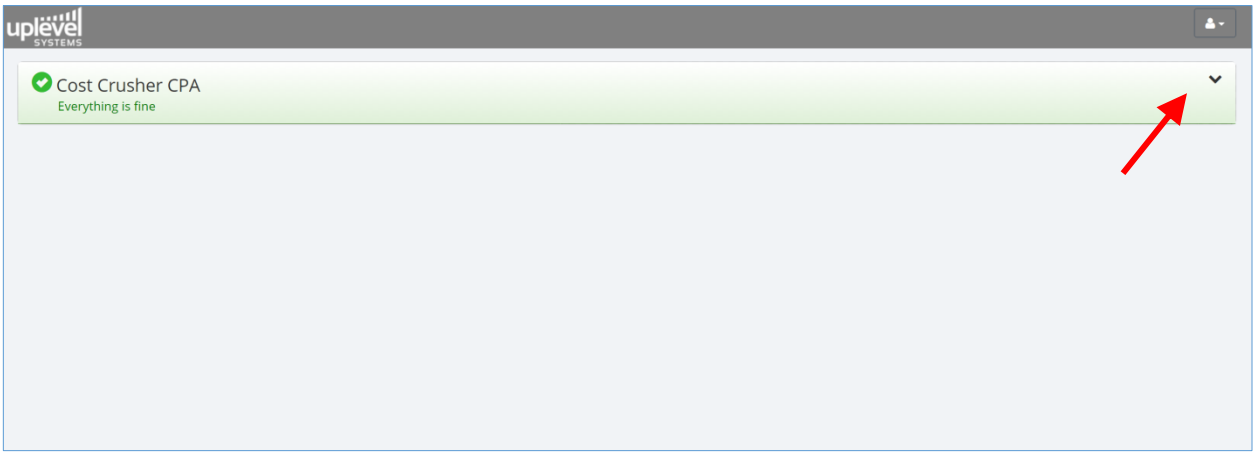


Figure 7 – Company Level Dashboard View

Expand the company, in this example "Cost Crusher CPA", to see the status of each service at each location by clicking on the down arrow (⌄) to the right of the company name.

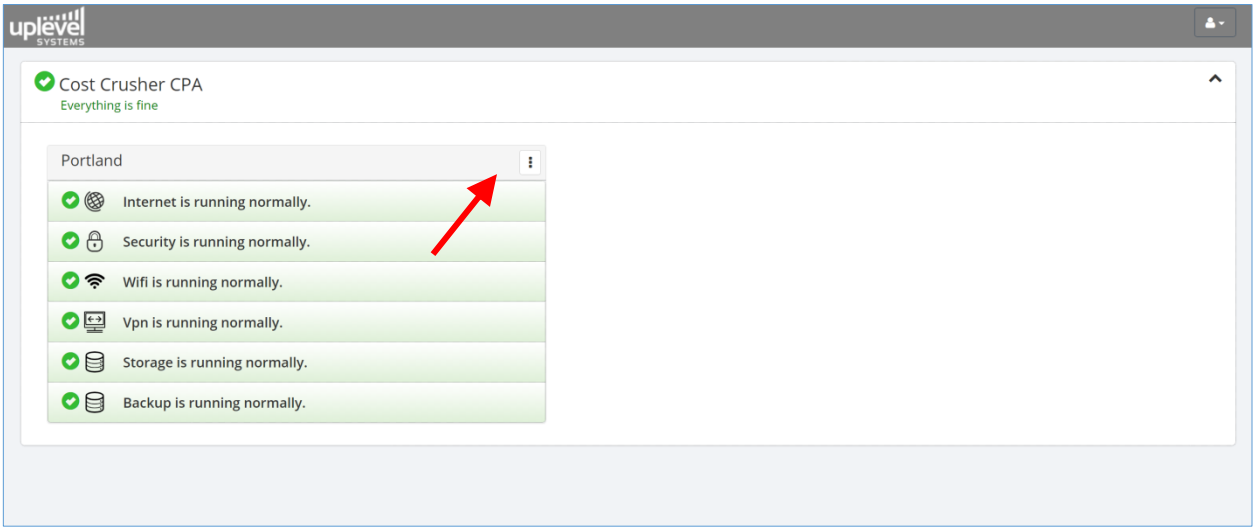


Figure 8 – Site Level Dashboard View

In Figure 8, you can view the status of each service that is running and ensure that the internet is properly connecting and AP is functioning properly. These statuses actively show the overall health of each function of each customer and each site. These statuses can also be sent be email alert. To setup email notifications please visit the "Email Notifications" Section of this document. By clicking on the vertical ellipses (⋮) to the right of the location name, in this example "**Portland"**, you can access the site configuration by selecting **Configure…** as shown in Figure 9.

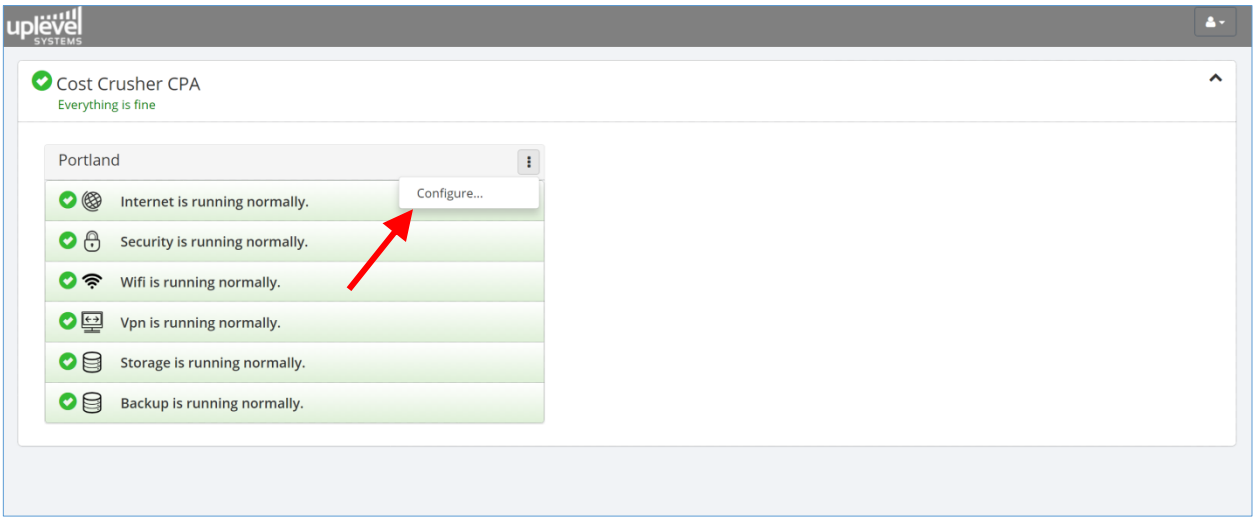


Figure 9 – Accessing the Configuration

When you access the site configuration in this manner, you will be taken to the Overview tab of the Configuration View as shown in Figure 10. The Overview tab defaults to a single group called employees. Here you can see the various ports of this group. This is also where the SSID and storage drives will also appear in this overview. To enable multiple groups check the box in the bottom left corner.

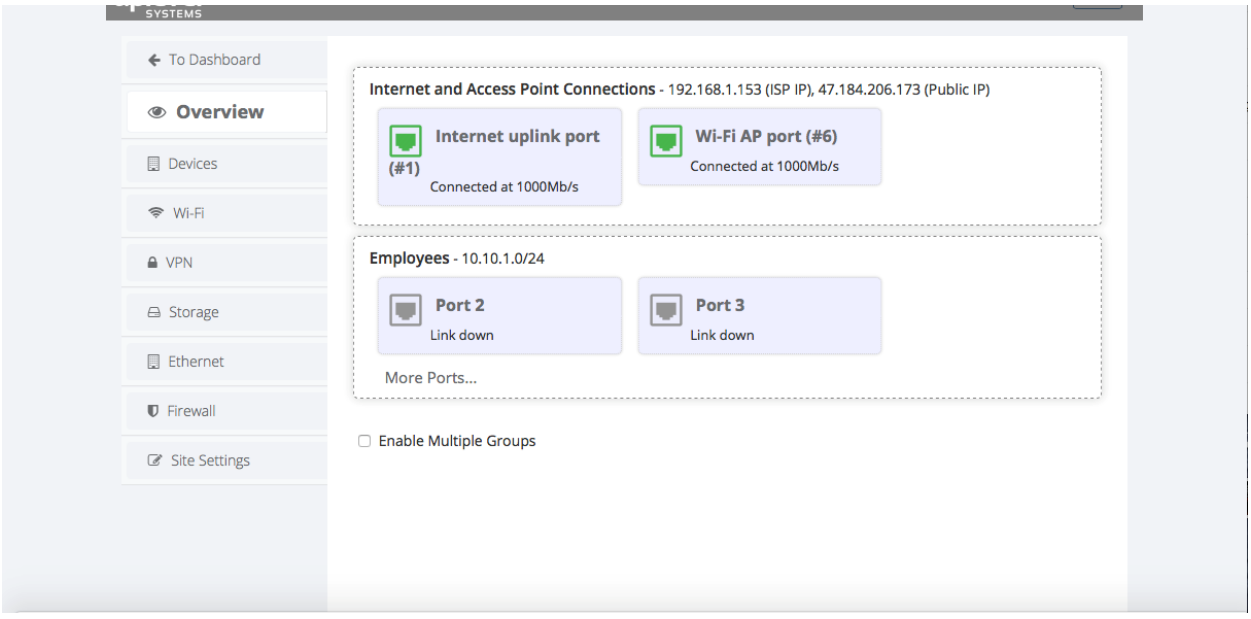


Figure 10 - Group Overview

In Figure 10 above, all Ethernet ports are assigned to the **Everyone** group, except port 1, which is connected to the Internet, and port 6, which in this case is connected to the Wi-Fi Access

Point. Once a device is plugged into a port on the Gateway the port will then appear green or blue to indicate connectivity.

Setting LAN IP's

Setting Local Network IP addresses can help to integrate the system into an existing networks IP ranges with existing devices. This can be done by proceeding to the Site Settings tab found on the right hand side of dashboard in Figure 10. This Site Settings Tab as seen in Figure 11 will allow you to view and edit the customer and site names, and software versions.

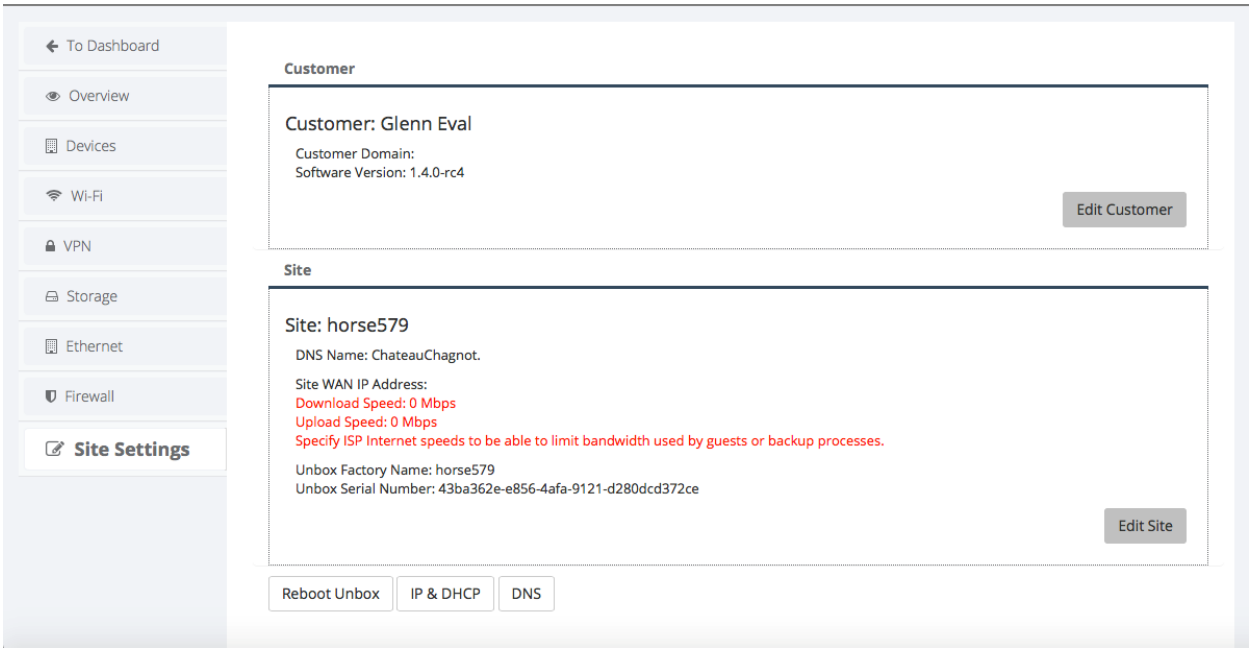


Figure 11 – Site Settings

By selecting the IP & DHCP button found at the bottom of the screen will provide a window to configure IP ranges for each group. This will allow you to specify Static and Dynamic IP ranges as seen in Figure 12.

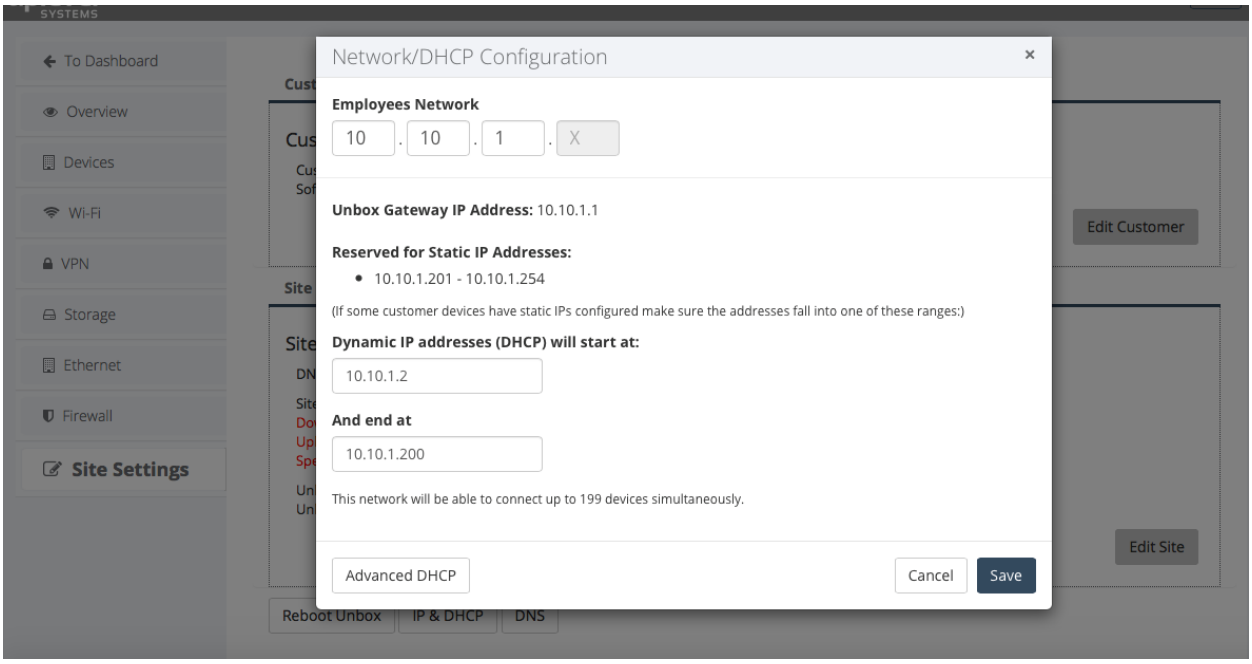


Figure 12 – IP & DHCP Configuration

This will allow for you to specify the IP range for the employees group where the box will then check and allocate the remaining groups based on acceptable IP addresses. These are automatically set to /24 ranges however this can be modified by selecting the Advanced DHCP button found at the bottom where each individual IP range can be set for its group.

Setting a Customer Domain

When first setting up a client it is also important to specify its Customer Domain. This can be done by going to Site Settings (Figure 11) and editing the customer. This allows for you to input the domain of the customer. NOTE: This is entirely different than the Domain name of their website and rather can/should be a subset of their website domain. For instance if your website is www.uplevelsystems.com then an appropriate customer domain maybe Costcrusher.Uplevelsystems.com. This will automatically configure the Site domain to Site1.Costcrusher.Uplevelsystems.com.

Enabling Wi-Fi Network

For security reasons, configure the Unbox Gateway before connecting other Ethernet devices, such as servers and printers, to it. In Figure 10 you will see a tab to the left side

this will allow you to configure the various Wi-Fi networks. There are no Wi-Fi networks configured at this point so none are shown on the overview tab. To configure a Wi-Fi group, click on the Wi-Fi tab in the left menu.

Enabling Corporate Wi-Fi

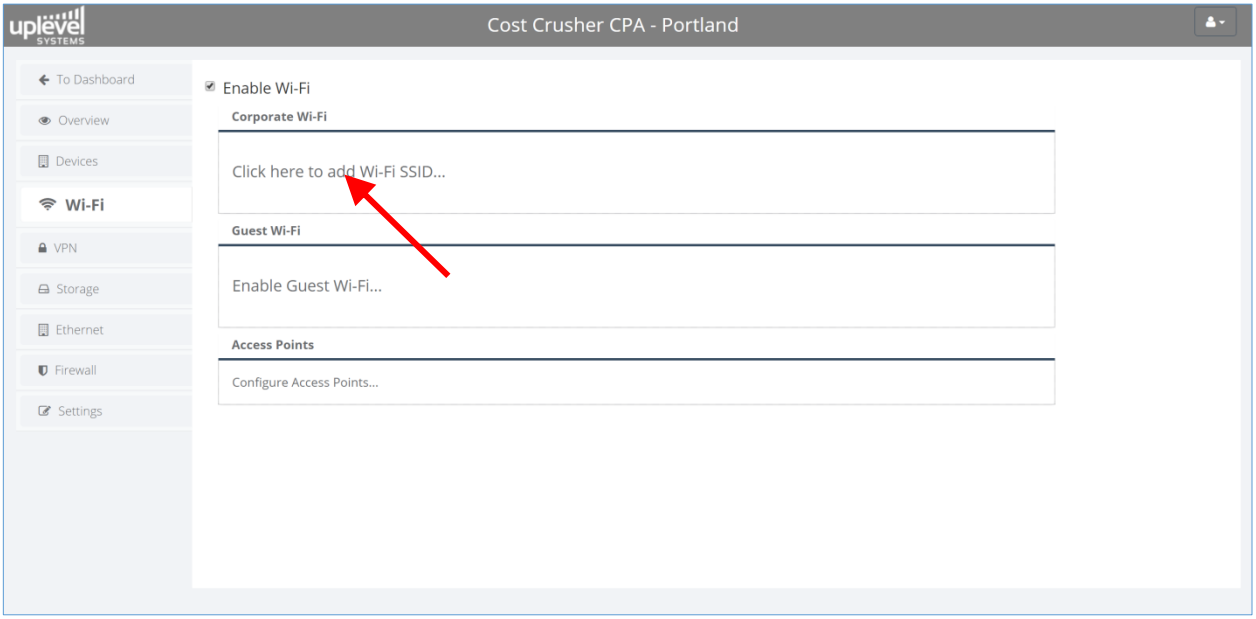


Figure 13 – Wi-Fi Configuration Overview

Under the **Corporate Wi-Fi** section, select **Click here to add Wi-Fi SSID…** to configure a new Wi-Fi network. This will open a Wi-Fi configuration window.

When the window opens, check the **Enable Wi-Fi** checkbox to enable the network and change its name to **AllEmployees**. Type in a strong password. Make sure the Everyone group can access this Wi-Fi network. When completed with your changes click on the **Save** button as shown in Figure 14.

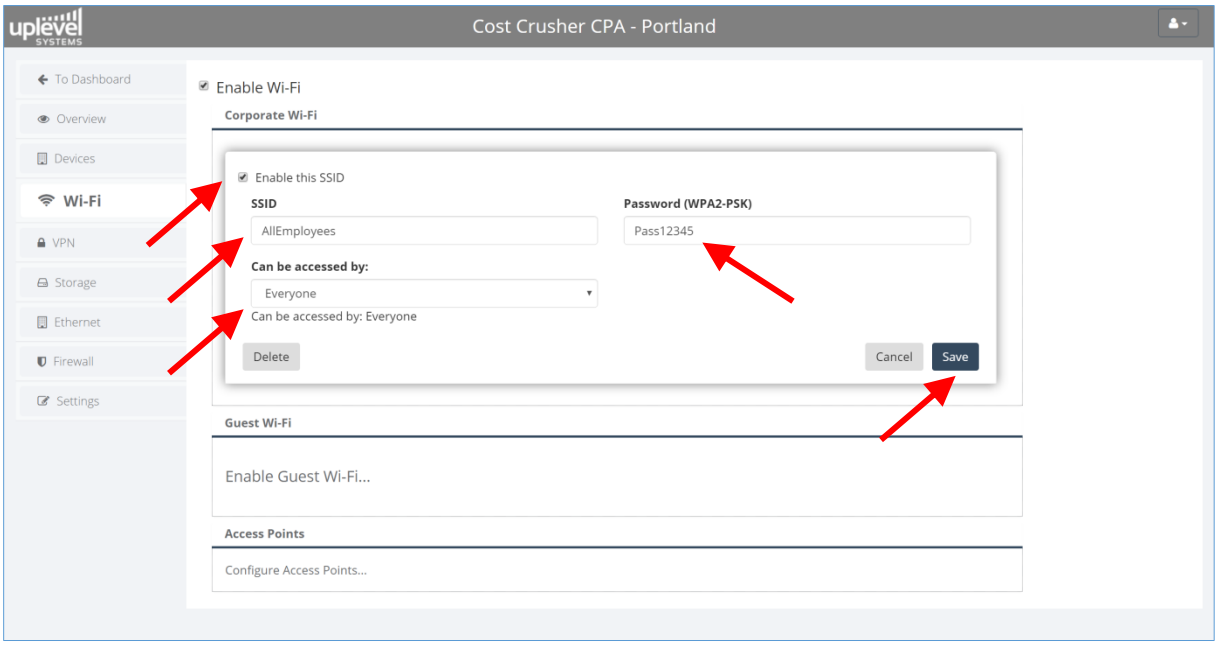


Figure 14 – Corporate Wi-Fi Configuration

Once configured, it takes about 2 minutes for the changes to take effect, at which point the system should be advertising just one SSID: **AllEmployees**. When the SSID is active, the 2.4G LED on the AP will glow blue and the 5G LED will glow green. Use a laptop or phone to verify that the Unbox AP is broadcasting the Wi-Fi network SSID that has just been configured.

Enabling Guest Wi-Fi

When setting up guest Wi-Fi the process is very similar to Corporate Wi-Fi. Under the Wi-Fi tab press Guest Wi-Fi as shown in Figure 15.

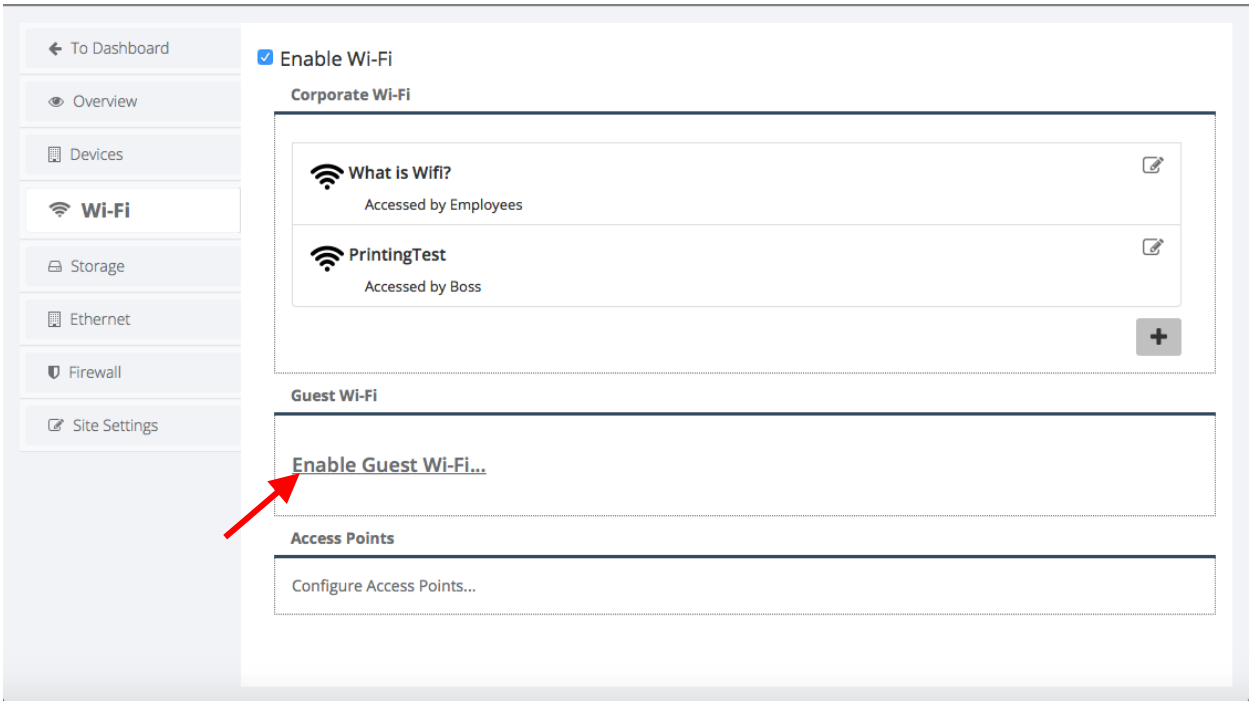


Figure 15 – Guest Wi-Fi Configuration

This will give you the option to select an SSID and optional password for the group. Different than Corporate Wi-Fi or any additional Wi-Fi group, the Guest Wi-Fi allows for a specified percentage of the bandwidth allotted. This however requires that the Site Settings be configured prior. To do this click on Site Settings in the left panel.

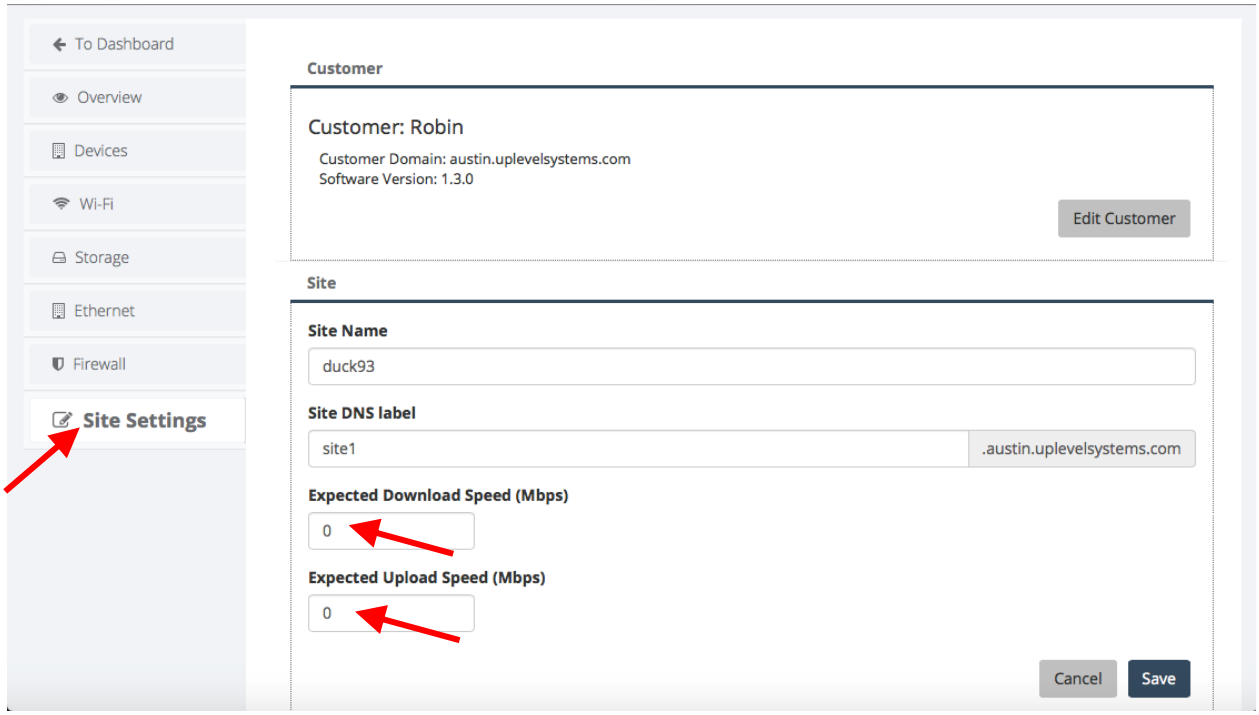


Figure 16 – Site Settings Configuration

From here you will be able to see the details of the different locations as well as the specific customer name. In order to set the specific percentage of bandwidth a speed test must be run on the network to determine the overall expected upload and download speeds for the network.

A speed test is highly recommended on all new and existing networks as actual experienced speeds may vary from those advertised by the internet service provider. When speed testing, we further recommend using one provided by the internet service provider as these tend to be more accurate than general speed tests. However, a general speed test is worthwhile is the service provider does not provide their own speed testing tools.

The results of the speed test are can be used to configure the parameters that the Gateway will use to restrict the guest Wi-Fi bandwidth and should be placed as shown in Figure 16. To determine the best practices for operating a speed test please look at our Evaluation Guide found as an appendix to this Start Up Guide.

Configuring the Expected Upload and Download Speeds should be done prior to setting a bandwidth percentage allotted for the guest Wi-Fi.

Once the site speeds are configured, the guest Wi-Fi can then be set up by going to the Wi-Fi tab and selecting "Configure Guest Wi-Fi" this will allow for a Wi-Fi SSID and password to be set as well as a Guest Wi-Fi bandwidth limit. Attempting specify the guest bandwidth limit to the Site Settings download and upload speeds being defined will result in an error message.

Verify Wi-Fi Operation

To test the Wi-Fi connection, use the laptop or another Wi-Fi client device to connect to the **AllEmployees** network or **GuestWi-Fi** (i.e. SSID) and provide the network password (**pass12345** in our example above). Verify that you can access the Internet by browsing to a web page such as http://www.google.com. A basic configuration is now complete.

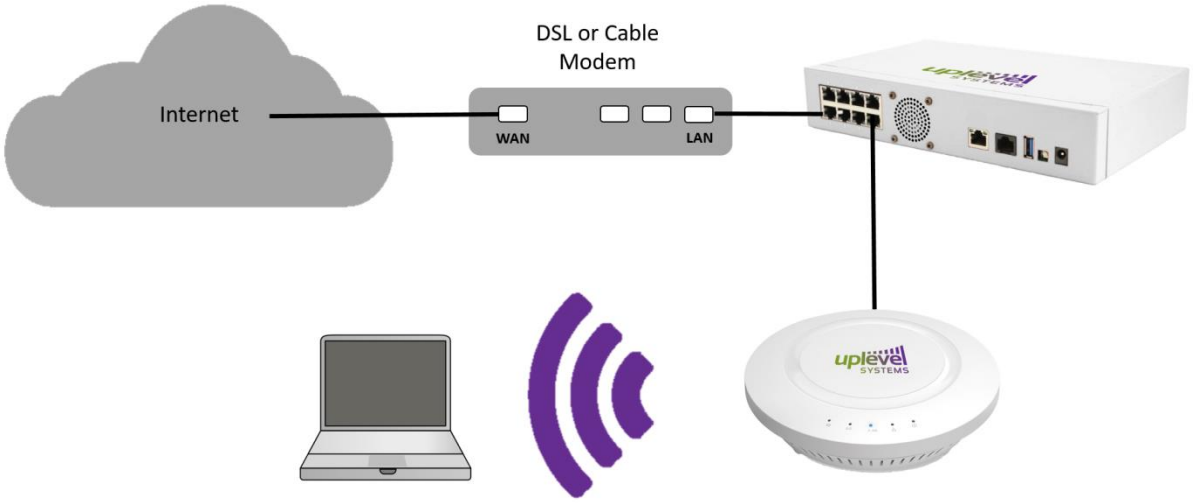


Figure 17 – Wi-Fi Test Configuration

Storage and Backups

In order to initiate a backup go to the storage tab located on the left side of the dashboard.

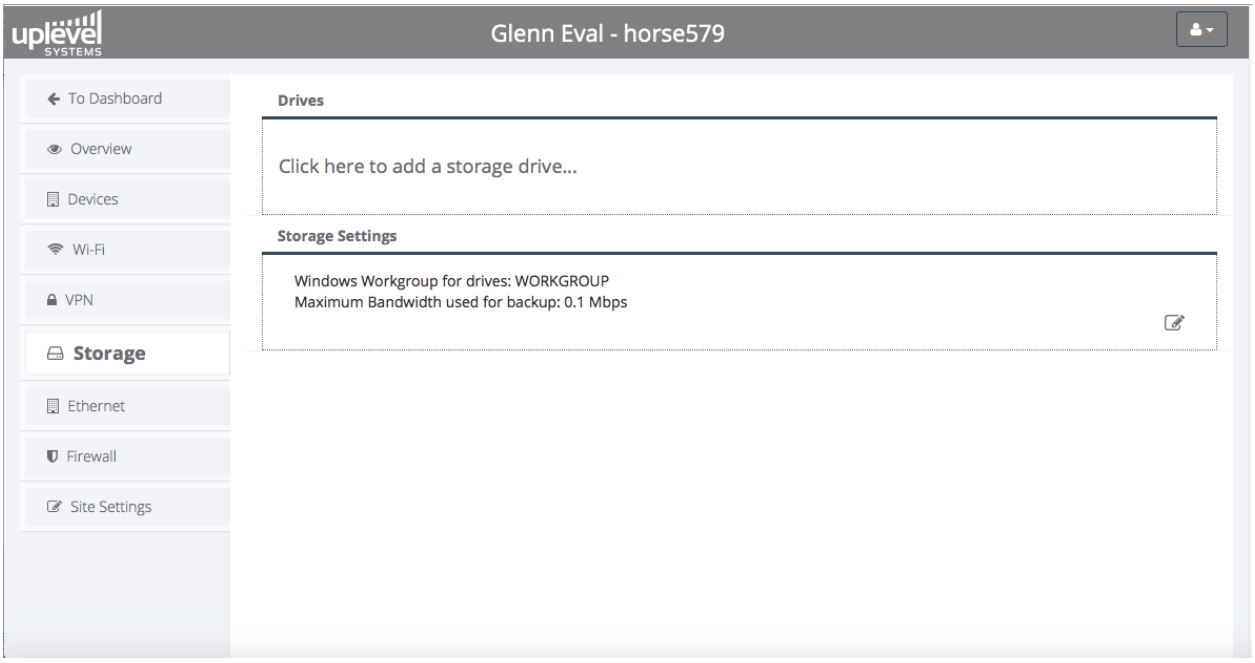


Figure 18 – Storage Overview

Figure 18 will you to add a Storage Drive and specify its size. This will also provide the local IP address that can be used to map the Drive. All of these storage devices will not appear in the Storage overview as well as the Overview page.

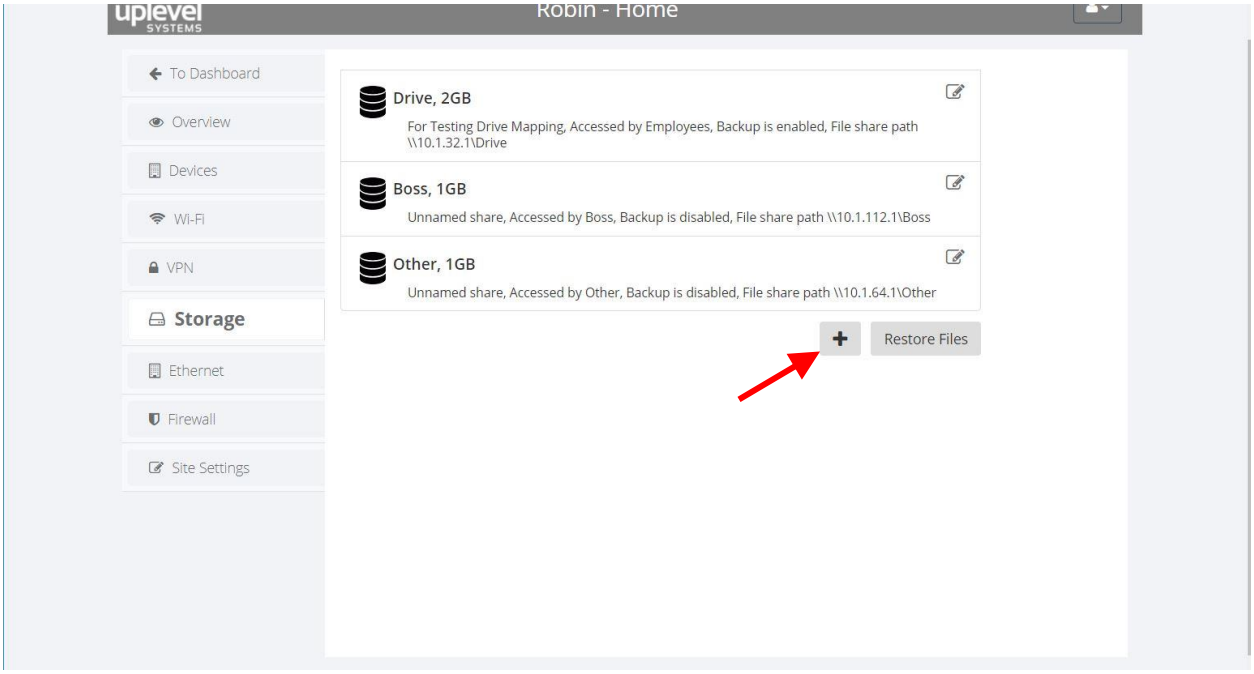


Figure 18a – Storage Overview

Firewall

Stateful Firewall

There is a stateful firewall built into the system that blocks any unsolicited traffic from the internet. This means any traffic that is not a response to a request from inside the LAN is automatically dropped. You can however punch a hole through this firewall to allow specific ports from the internet access. To do so click on the Firewall tab located in the left panel. This will bring you to the standard Port Blocking page where you can Click here to add a firewall rule... and specify the Rule name, Port, and Local IP address for the rule as seen in Figure A.

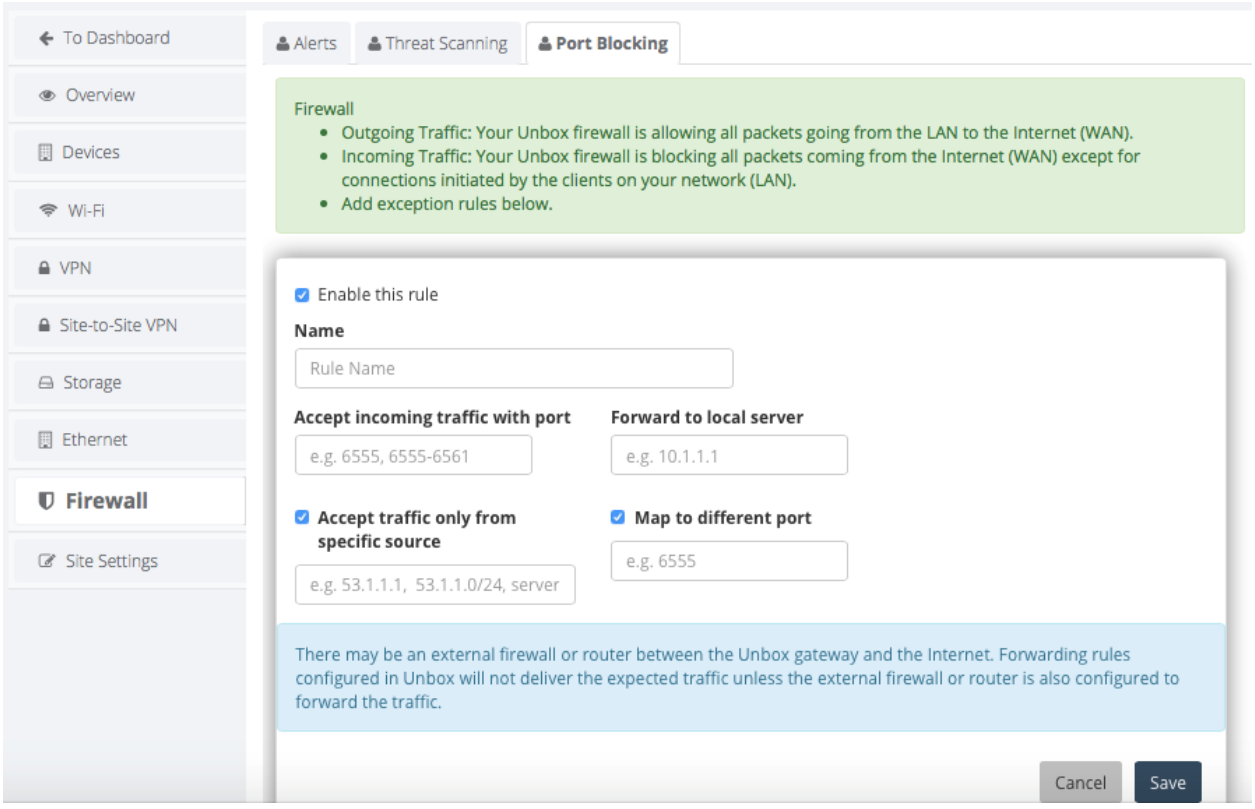


Figure A – Port Blocking Rules

IPS/IDS Firewall

By clicking on the Threat Scanning tab located in the top panel of the Firewall page

you can set the initial alerting and blocking rules for the particular customer as seen in Figure B. This is done on a per client basis however the alerts for each site may vary greatly. It is here where you can also set email alerting for this particular customer.

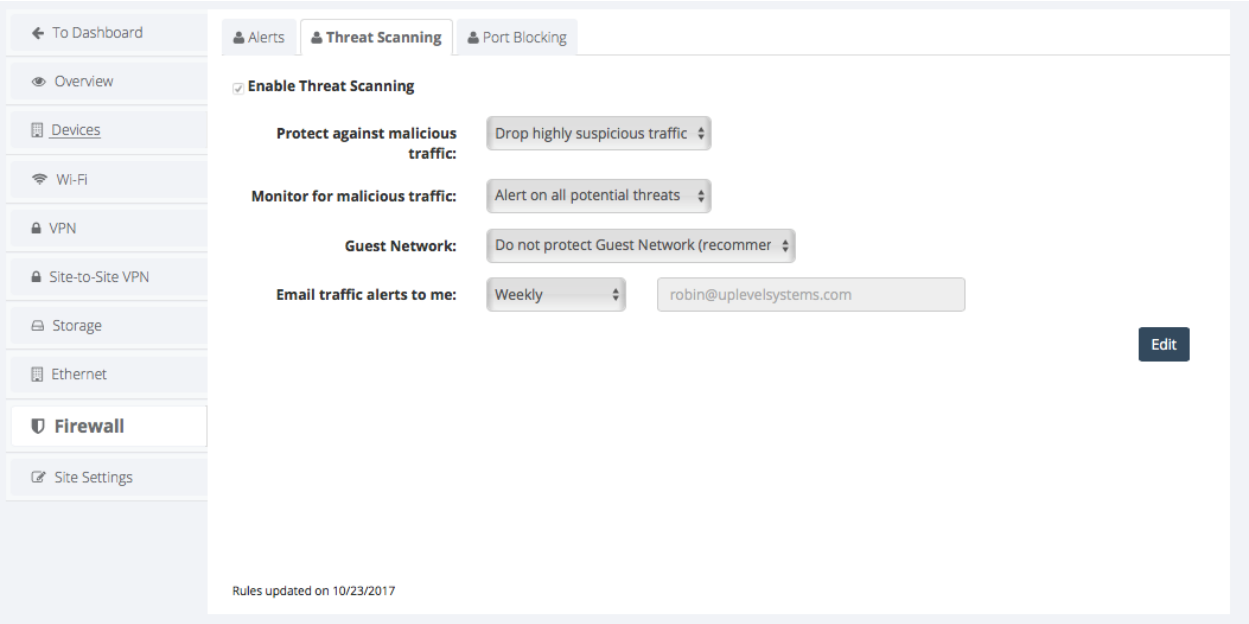
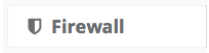


Figure B – Threat Scanning Rules

Once these rules are initially set you will begin to see alerting on the traffic in the 

tab located at the top of the 

tab.

Email Notifications

To enable email notifications Click on the account button  at any point in the upper right hand corner of the screen. This will produce a drop down menu seen in Figure 19 where you can select Account Settings to proceed to the general account overview.

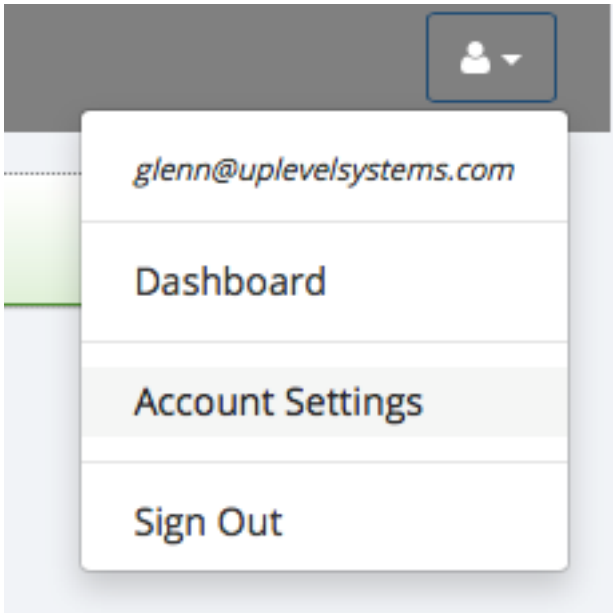


Figure 19 – Account Settings

This will give you a general overview of the account settings as seen in Figure 20.

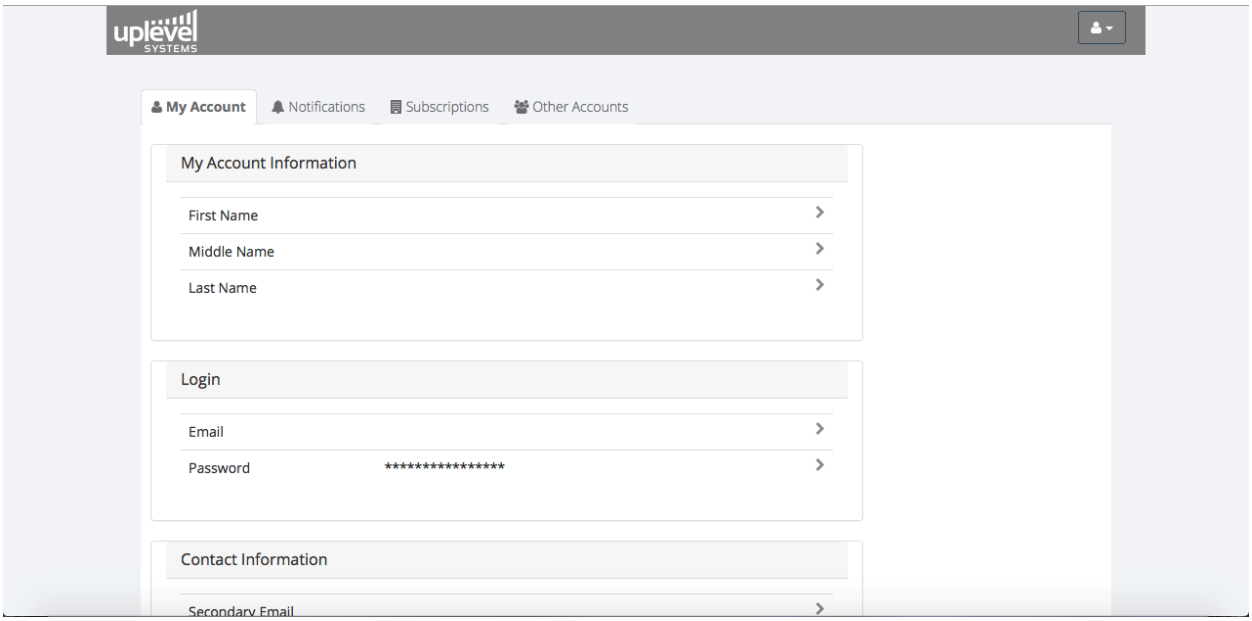


Figure 20 – Account Overview

From you can select Notifications in the menu bar at the top of the screen. Which will take you to a customizable notification screen. Once you have selected the check box indicating "Send email when an issue is detected" Figure 20 will appear allowing you the ability to customize the email

notifications you receive upon issue.

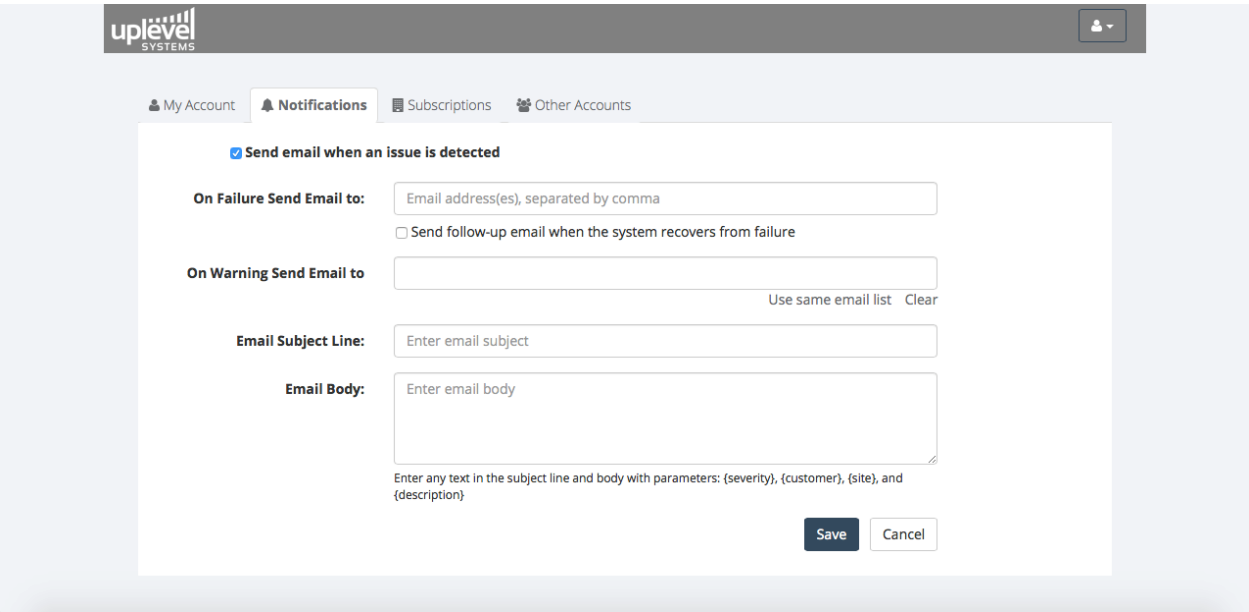


Figure 21 – Email Notifications

You can specify multiple emails for warnings and failures as well as the ability to customize the subject and body of the email it self. This is done using the varying commands found in curly brackets and described at the bottom of the page. An example of this can be seen in Figure 22.

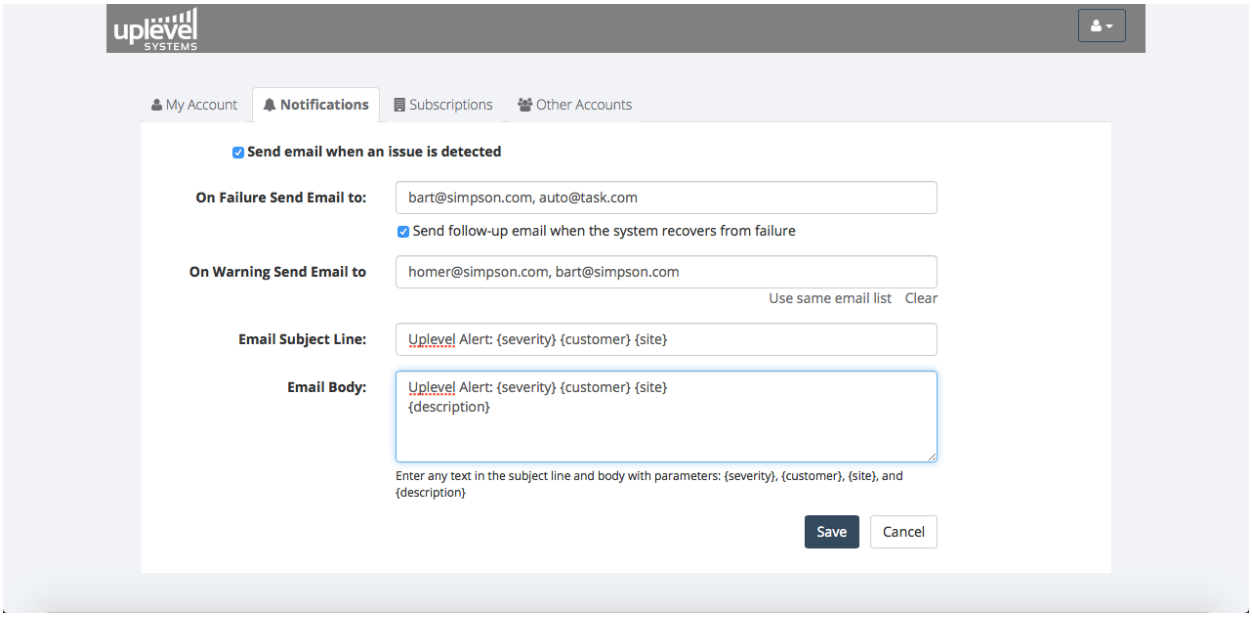


Figure 22 – Email Notifications

Conclusion

For any further questions or explanation of the Uplevel products please contact support@uplevelsystems.com or consult the Upleavel Unbox User Guide.