



Unleashed

Configuration – Basic

Configuration Guide

Firmware Version: 200.12

Configuring your Unleashed WLAN

The Unleashed WLAN solution uses access points with an embedded software-based controller. This solution was designed for smaller installations requiring a low number of access points but desiring greater stability and visibility into the WLAN environment than other low-cost solutions. Unleashed access points are configured by a simple Web GUI and utilize proprietary technologies without the need for a stand-alone wireless controller.

Initial Unleashed Setup

- Chapter 1 - Getting Started
- Chapter 2 - Using the Setup Wizard
- Chapter 3 - Final Initial Configuration Steps in GUI
- Chapter 4 - Backup and Firmware

Chapter 1 - Getting Started

- 200.12 Supported Access Points – Access Networks Brand
- 200.12 Supported Access Points – Ruckus Brand
- Unpack and Install the Unleashed Master AP
- Connect to the Unleashed “Configure.me” SSID

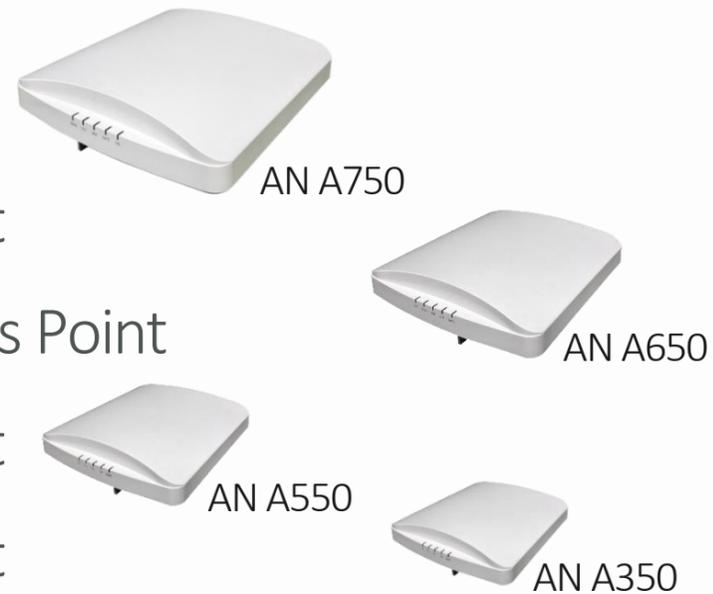
Chapter 1 - Getting started

200.12 Supported Access Points – Access Networks Brand

Indoor Access Points

Wi-Fi 6

- A750 4x4:4 Access Point
- A650 2x2:2/4x4:4 Access Point
- A550 2x2:2 Access Point
- A350 2x2:2 Access Point



Wi-Fi 5

- A610 3x3:3 Access Point
- A510 2x2:2 Access Point
- A320 2x2:2 Access Point



Outdoor Access Points

Wi-Fi 6

- B350 2x2:2 Access Point



Wi-Fi 5

- B310 2x2:2 Access Point



Chapter 1 - Getting started



Unpack and Install the Unleashed Master AP

Choose which Unleashed AP will become the Unleashed Master AP (the AP that performs all of the control functions of your Unleashed network). Any hard-wired Unleashed AP can be the Master.

*** Do NOT connect multiple APs to power and the network all at once.** In the initial setup stage, you should choose one AP as the Master AP and connect it to the network and power, and then complete the initial setup steps on this Master AP before connecting any other APs. Once setup is complete, you can continue connecting other APs to power and the network.

Once powered on and connected to the local network, the Unleashed AP will boot up and begin broadcasting a temporary unencrypted WLAN named "ConfigureMe-[xxxxxx]" (**[xxxxxx]** is the last 6 digits of the MAC address of the AP).

Chapter 1 - Getting started

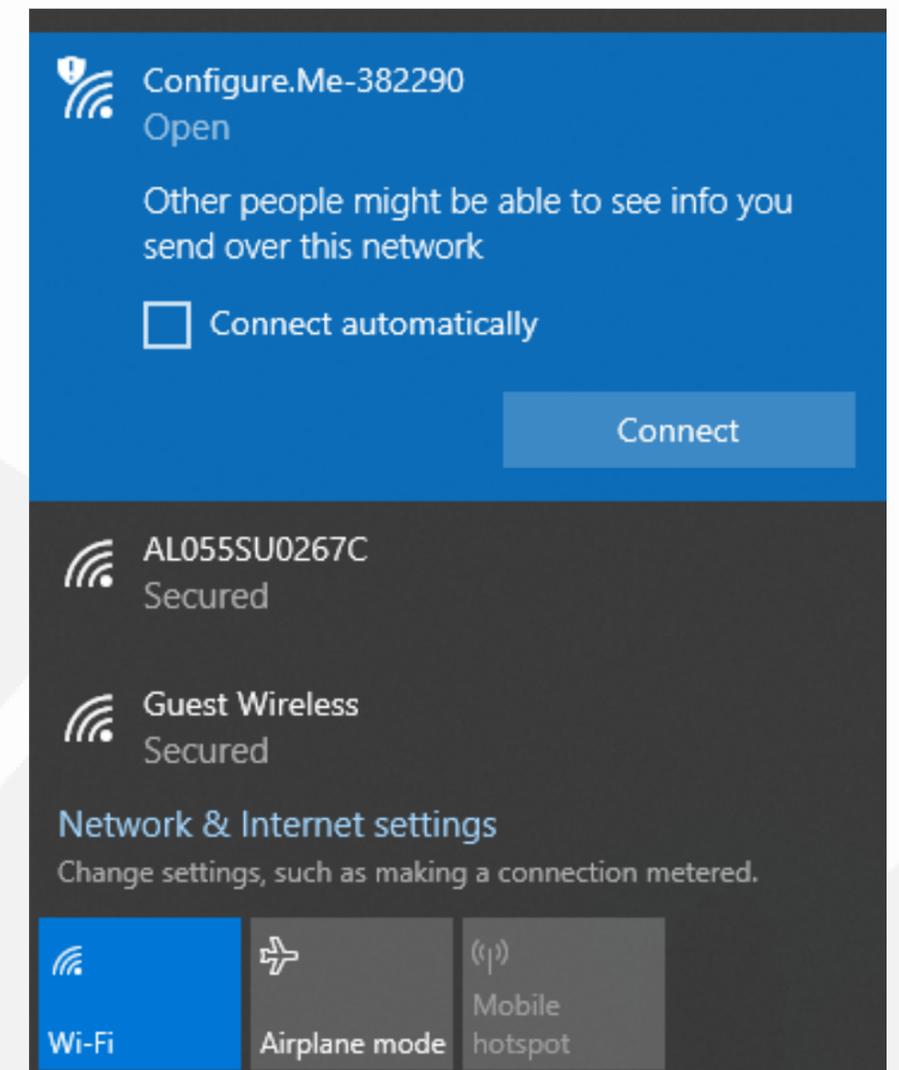


Connect to the Unleashed “Configure.me” SSID

Using the Wi-Fi configuration settings on your client device (such as a laptop or mobile device), select and associate to the Configure.Me-[xxxxxx] WLAN, and launch a web browser

In your browser's URL bar, enter the following address and press Enter: **unleashed.ruckuswireless.com**

***Note – In Unleashed deployments, the initial “Configure.Me-[xxxxxx]” WLAN does not require a password.**



Chapter 2 - Using the Setup Wizard

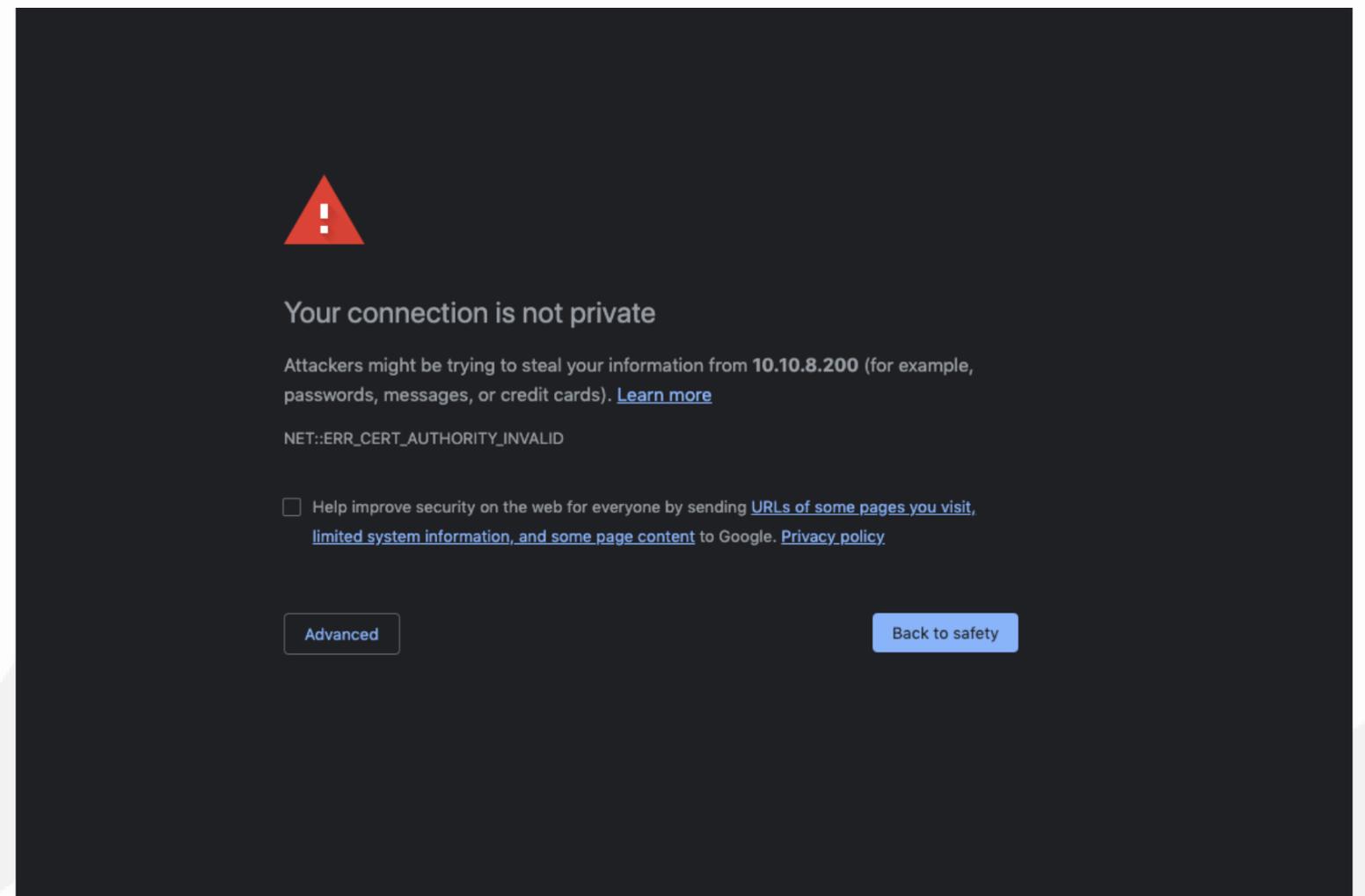
- Security Warning
- Basic Configuration Steps
- 5 Quick Steps for Setting Up the Unleashed System
- Complete the Setup Process
- System Settings & Rebooting

Chapter 2 - Using the Setup Wizard

Security warning

Depending on your browser, you may be presented with a security warning stating "This connection is not trusted" (Firefox) or "Your Connection is Not Private" (Chrome) or "There is a problem with this website's security certificate" (Internet Explorer). This is normal, as the Unleashed AP does not have an SSL certificate that is recognized by your browser.

Accept the exception as needed per browser and proceed.



Chapter 2 - Using the Setup Wizard



Basic Configuration Steps

Once you have accepted the security exception, you will be redirected to the “Unleashed Installation” wizard.

The “Unleashed Installation” wizard will guide you through the process of setting up the Unleashed Master AP.

The screenshot shows the "Unleashed Installation" wizard interface. At the top left is the "ACCESS NETWORKS" logo. The main heading is "Unleashed Installation" with a language dropdown menu set to "English". Below this, there are two main options: "Quick Install" and "Custom Install".

Quick Install is described as "This is the most simple and quick way to install" with "(Internal Gateway: Disabled; Mesh: Disabled)". It includes the following fields:

- Wireless LAN**
 - * Name (ESSID):
 - * Passphrase:
- Administrator**
 - * Admin Username:
 - * Password:
 - If a Unleashed ICX switch is managed by Unleashed then it will use the same login credentials as provided above.
 - * Country Code:

Custom Install is described as "Provide more advanced options to install".

At the bottom right, there is a "Version: 200.12.10.105.129" label, a "[Local Upgrade](#)" link, and a large black "Finish" button.

Chapter 2 - Using the Setup Wizard



Basic Configuration Steps

There are many ways of setting up an Unleashed Network by using the “Unleashed Installation” wizard.

This presentation will focus on the “Custom Install” process to setup the Unleashed Network.

Click on “Custom Install” to continue.

The screenshot shows the 'Unleashed Installation' web interface. At the top left is the 'ACCESS NETWORKS' logo. The page title is 'Unleashed Installation' with a language dropdown set to 'English'. There are two main sections: 'Quick Install' and 'Custom Install'. The 'Quick Install' section is highlighted with a grey background and contains the following fields: 'Wireless LAN' with 'Name (ESSID): AN-Wireless-1' and 'Passphrase:'; 'Administrator' with 'Admin Username: admin' and 'Password:'. A note below the password field states: 'If a Unleashed ICX switch is managed by Unleashed then it will use the same login credentials as provided above.' The 'Country Code:' is set to 'United States'. The 'Custom Install' section is currently unselected. At the bottom right, there is a 'Finish' button. A red arrow points from the text 'Click on “Custom Install” to continue.' to the 'Custom Install' link.

Chapter 2 - Using the Setup Wizard



Basic Configuration Steps

Ensure the “Advanced Install” option is selected from the list.

Click on the “Next” button to continue.

ACCESS NETWORKS

Unleashed Installation

Advanced Install This is the advanced way to install if one want to customize the configuration in more detail

UMM Install Use image from UMM to install an Unleashed network

* UMM Domain/IP: UMM address from where the Unleashed Network can retrieve configuration

Config Template Name: Configuration template pre-stored in UMM for the Unleashed Network

* System Name: Name your system 32 characters max using alphanumeric characters excluding space.

Back **Next**

Chapter 2 - Using the Setup Wizard



Step 1 - Set the System Name

Enter a System Name for the Unleashed system.

Click “Next” to continue.

***Note - A good suggestion could be name of the jobsite like “Smith_Residence”. Remember to use best practices from your company for the naming convention.**

The screenshot shows the ACCESS NETWORKS Setup Wizard interface. At the top, the logo "ACCESS NETWORKS" is visible. Below it, a progress bar shows five steps: 1. System (highlighted in orange), 2. IP setting, 3. Wireless LAN, 4. Administrator, and 5. Review. The main content area contains the following fields and options:

- Version:** 200.12.10.105.129
- * Name:** ANUC (with a red arrow pointing to the input field)
- * Country Code:** United States (dropdown menu)
- Mesh:**

Instructions on the right side of the form:

- Name your system 32 characters max using alphanumeric characters excluding space.
- Select the regulatory country code for the Unleashed Network.
- Select this check box to enable Mesh for the Unleashed Network.

At the bottom right, there are two buttons: "Back" and "Next" (with a red arrow pointing to the "Next" button).

Chapter 2 - Using the Setup Wizard

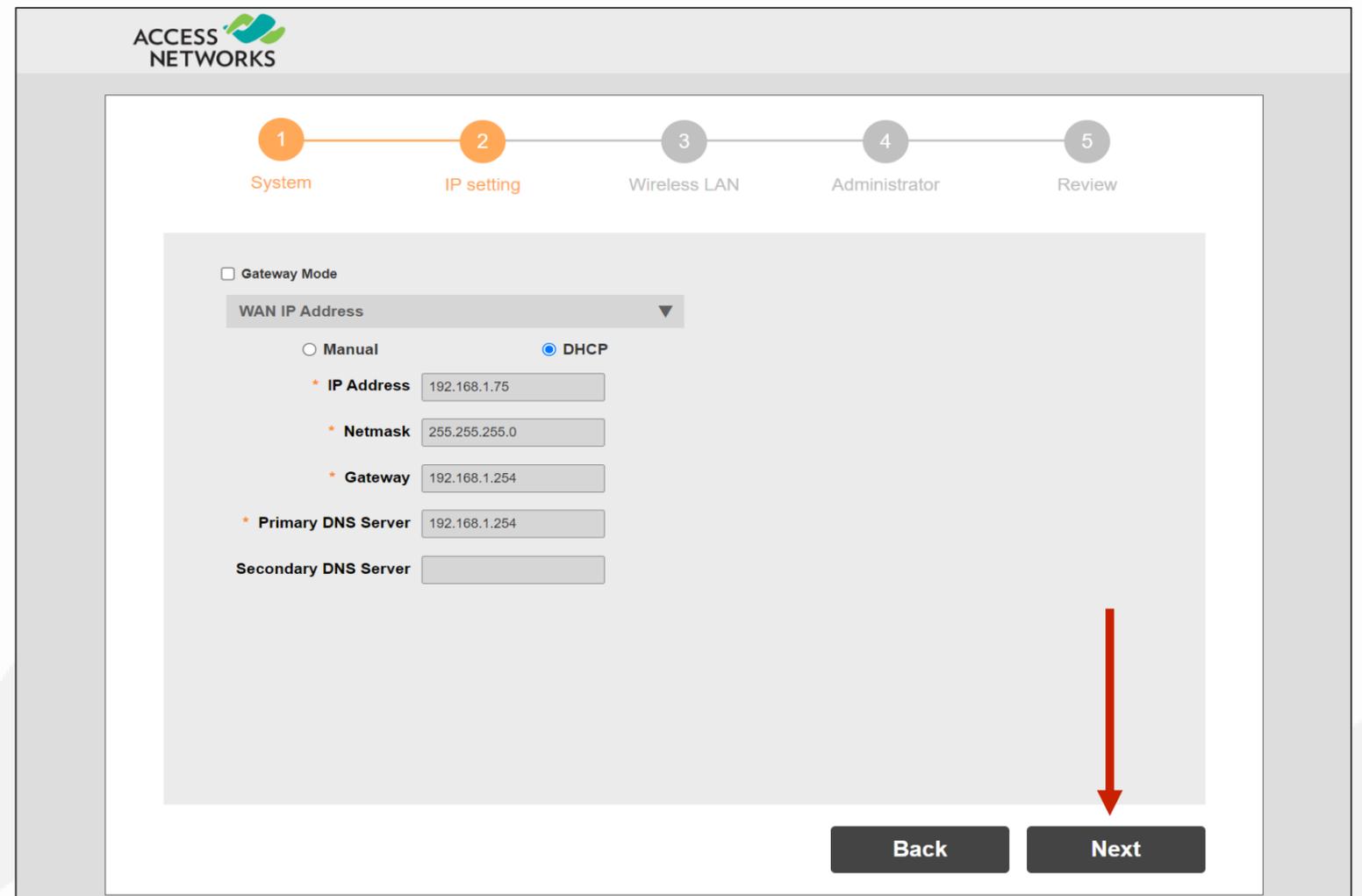
Step 2 - IP Address Settings

For most installations it is recommended to leave the “Gateway Mode” disabled.

It is also recommended to leave the Unleashed access points in “DHCP” mode.

A static “Management Interface” IP address should be established after the Setup Wizard is complete.

Click “Next” to continue.



ACCESS NETWORKS

1 System 2 IP setting 3 Wireless LAN 4 Administrator 5 Review

Gateway Mode

WAN IP Address

Manual DHCP

* IP Address 192.168.1.75

* Netmask 255.255.255.0

* Gateway 192.168.1.254

* Primary DNS Server 192.168.1.254

Secondary DNS Server

Back Next

Chapter 2 - Using the Setup Wizard



Step 3 - Wireless LAN

Enter a Name for your first wireless LAN.

Ensure “Yes” for “Password Protect (WPA2)” for this WLAN has been selected.

Enter a password for the WLAN.

Click “Next” to continue.

***Note - Best practice suggest the password must be no less than 12 characters and should also contain a combination of Uppercase, Lowercase, Number, and Special Character Symbols. An example of this is "E@syP@\$w0rd!".**

The screenshot shows the 'Wireless LAN' configuration step (Step 3) of the 'ACCESS NETWORKS' setup wizard. At the top, a progress bar indicates five steps: 1. System, 2. IP setting, 3. Wireless LAN (current step), 4. Administrator, and 5. Review. The main configuration area includes:

- Name (ESSID):** A text input field containing 'Smith Wireless'. A red arrow points to this field.
- Password Protect (WPA2):** Radio buttons for 'Yes' (selected) and 'No'. A red arrow points to the 'Yes' option.
- Password:** A masked password input field with a red arrow pointing to it.
- Help text:** 'Name your own wireless LAN. The name will be shown in wireless LAN list. It will be shown as "AN-Wireless-1" without changing.' and 'It is *highly recommended* setting password protection for wireless LAN. So only authorized users can join. Password can only contain between 8 and 64 characters and no spaces are allowed.'
- Navigation:** 'Back' and 'Next' buttons at the bottom right. A red arrow points down to the 'Next' button.

Chapter 2 - Using the Setup Wizard



Step 4 - Admin access

Enter a system “Admin Username:”.

Enter a system “Password:” and re-enter the password in “Confirm Password:”.

***Note – Follow the previously described guidelines when creating passwords.**

The screenshot shows the 'ACCESS NETWORKS' Setup Wizard at Step 4, 'Administrator'. A progress bar at the top indicates five steps: 1. System, 2. IP setting, 3. Wireless LAN, 4. Administrator (current step), and 5. Review. The main form area contains three input fields: '* Admin Username:' with the value 'admin', '* Password:' with masked characters, and '* Confirm Password:' with masked characters. Red arrows point to each of these three fields. To the right of the fields, there is explanatory text: 'This username and the following password will permit admin access to web interface after the set up is done.', 'The password can only contain between 4 and 32 characters and cannot include "" or "\$()", and no spaces are allowed.', and 'Enter the above password again.' Below this text is a note: 'If a Unleashed ICX switch is managed by Unleashed then it will use the same login credentials as provided above.' At the bottom left of the form is a 'Password Recovery:' checkbox, which is currently unchecked. At the bottom right of the form are two buttons: 'Back' and 'Next'.

Chapter 2 - Using the Setup Wizard



Step 4 - Password Recovery

It is recommended to configure the password recovery option. The password recovery option will allow your company to reset the password in the event of your original username or password are lost or forgotten.

To do so, select “Password Recovery”.

Enter a Security Email, Security Question and Security Answer. Again, by filling this information out, it will allow you to reset your password in the event of your username or password are forgotten.

Click “Next” to continue.

ACCESS NETWORKS

1 System 2 IP setting 3 Wireless LAN 4 Administrator 5 Review

* Admin Username: admin

* Password:

* Confirm Password:

This username and the following password will permit admin access to web interface after the set up is done.

The password can only contain between 4 and 32 characters and cannot include "" or "\$(", and no spaces are allowed.

Enter the above password again.

If a Unleashed ICX switch is managed by Unleashed then it will use the same login credentials as provided above.

→ Password Recovery:

→ * Security Email: joe@aavd.com

→ * Security Question: Create My Own Security

→ * Your Own Question: What's our logo icon?

→ * Security Answer:

The security email will be used to reset forgotten password

The security question will be used to reset forgotten password

your answer to security questions

Back Next

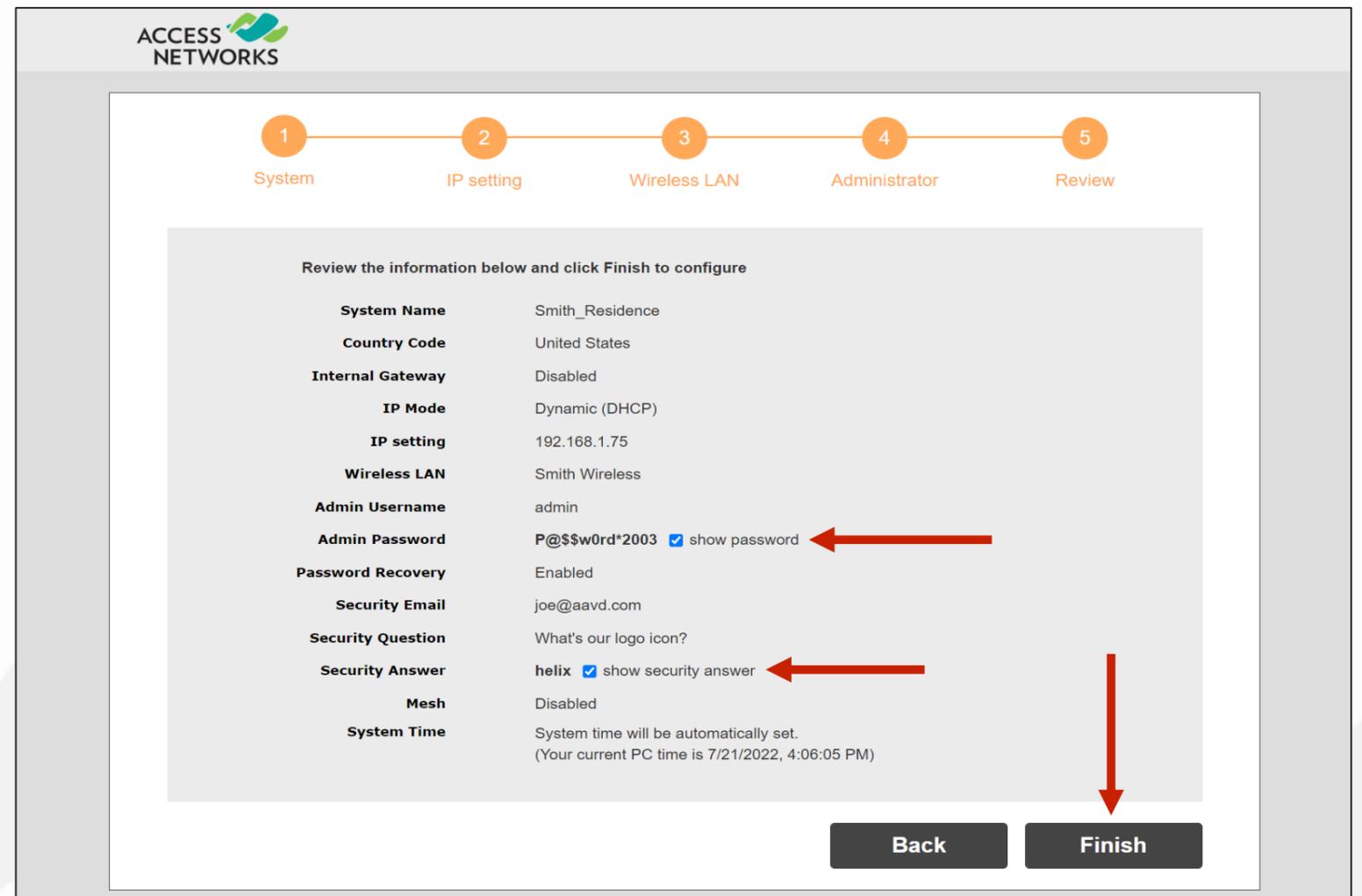
Chapter 2 - Using the Setup Wizard

Step 5 - Review

Review the information shown.

If you need to reveal the hidden password and the security answer, you can do so by clicking on the associated check box.

If everything is correct, select “Finish”.



ACCESS NETWORKS

1 System 2 IP setting 3 Wireless LAN 4 Administrator 5 Review

Review the information below and click Finish to configure

System Name	Smith_Residence
Country Code	United States
Internal Gateway	Disabled
IP Mode	Dynamic (DHCP)
IP setting	192.168.1.75
Wireless LAN	Smith Wireless
Admin Username	admin
Admin Password	P@\$w0rd*2003 <input checked="" type="checkbox"/> show password
Password Recovery	Enabled
Security Email	joe@aavd.com
Security Question	What's our logo icon?
Security Answer	helix <input checked="" type="checkbox"/> show security answer
Mesh	Disabled
System Time	System time will be automatically set. (Your current PC time is 7/21/2022, 4:06:05 PM)

Back Finish

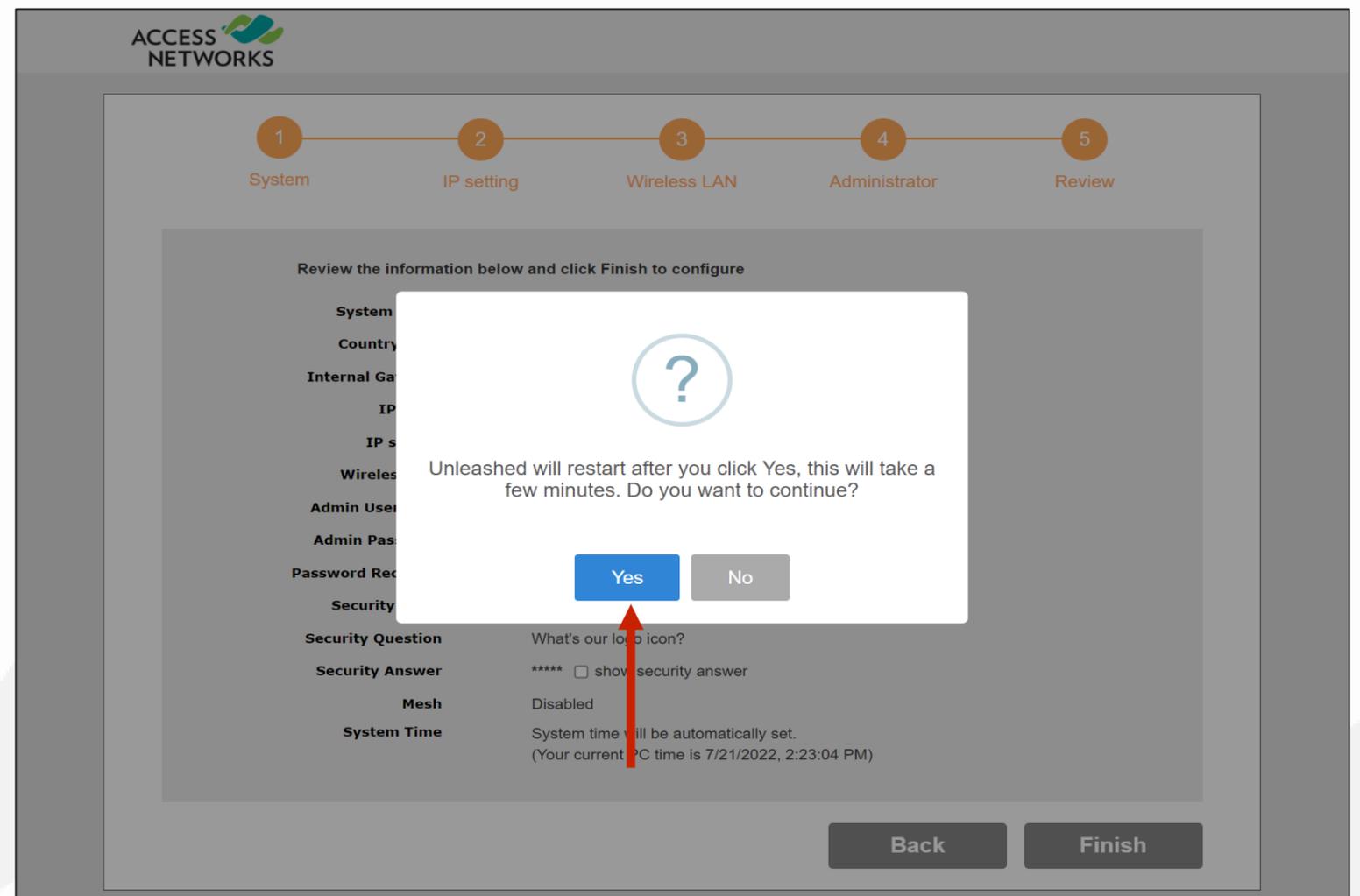
Chapter 2 - Using the Setup Wizard



Complete the setup process

A new pop-up will display verifying that you are aware that the Unleashed AP will reboot once you continue and that the process will take a few minutes.

Click on “Yes” to complete the setup.



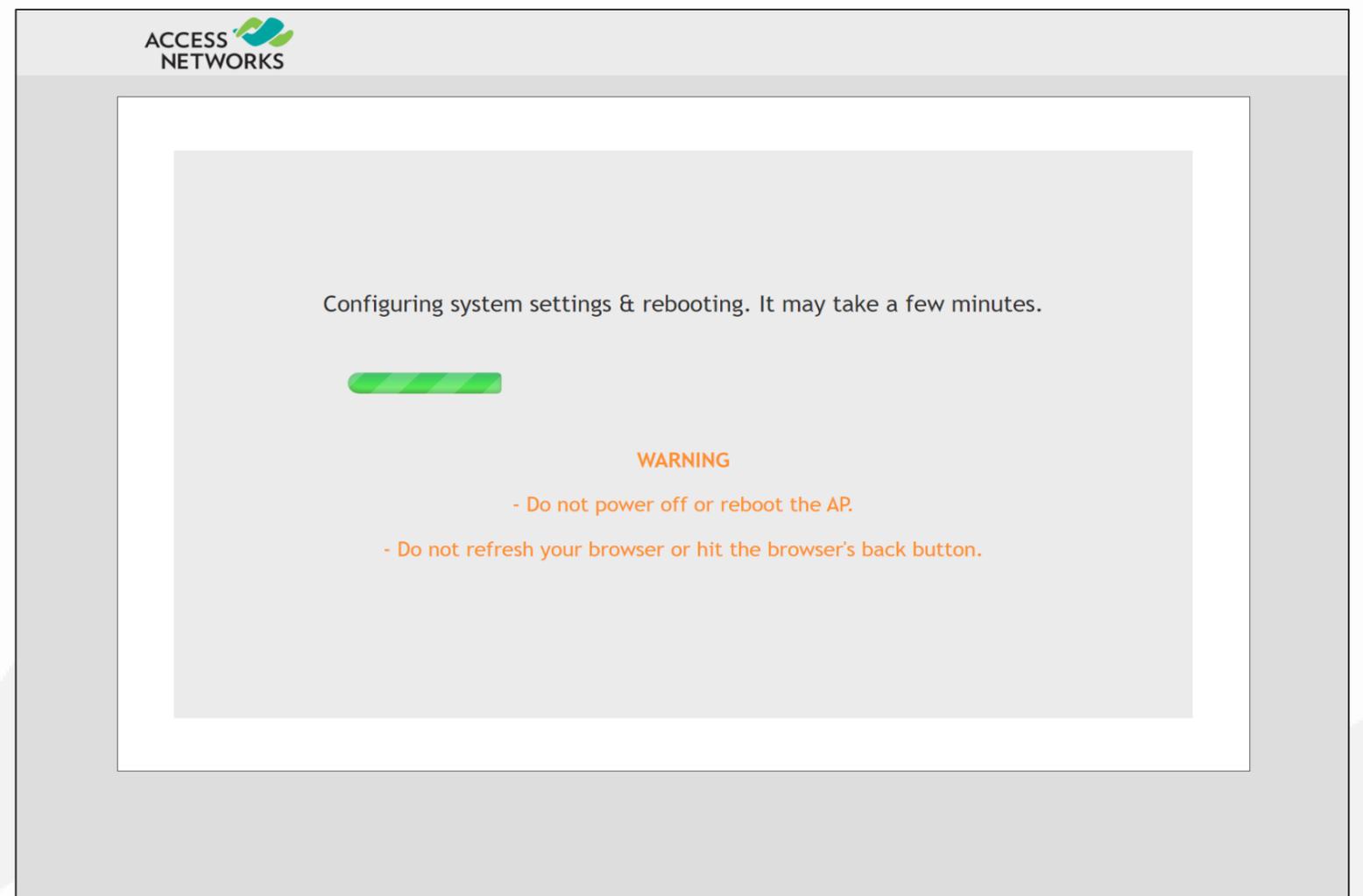
Chapter 2 - Using the Setup Wizard



System Settings & Rebooting

After clicking the Finish button, the Unleashed Master AP will apply all of the setting you have configured and then reboot. A "Configuring system settings & rebooting" page is displayed during this process.

Wait for the progress screen to complete before proceeding.



Chapter 2 - Using the Setup Wizard

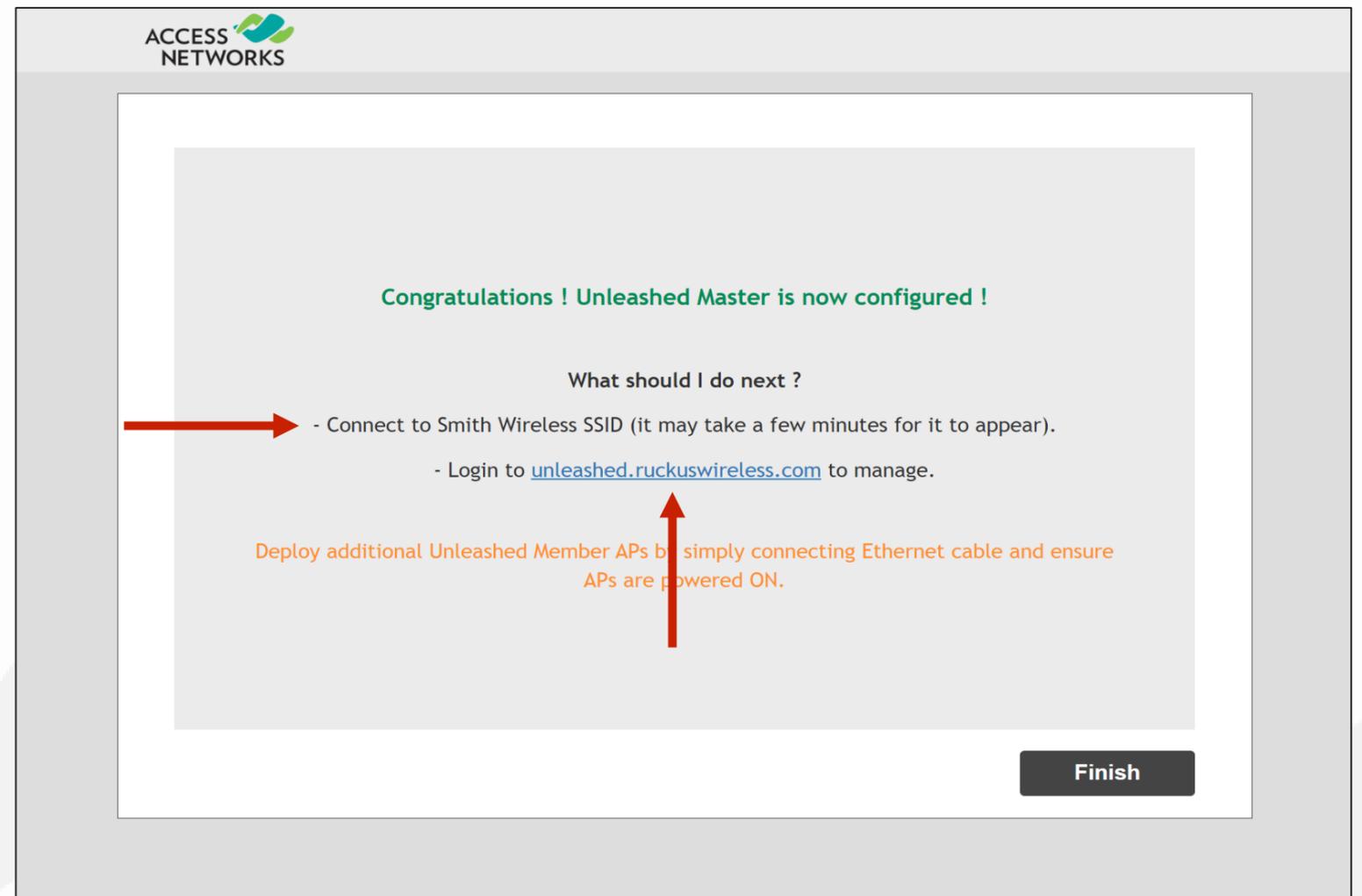


System Settings & Rebooting

Once the setup is complete, the "Congratulations!" screen appears.

After the access point has rebooted you will need to connect to the new WLAN you created. Our example is "Smith Wireless".

Click on "unleashed.ruckuswireless.com" after you have connected to your new WLAN. You will then be redirected to the login page.



Chapter 3 - Final Initial Configuration Steps in the GUI

- Reconnecting to the Master Access Point
- Unleashed Dashboard
- Configuring a Management Interface
- Creating a Guest Network
- Advanced Guest Network Isolation
- Adjusting Access Points for Best Channels/Performance Mode
- Automatic Channel Selection
- Adding Additional Unleashed Access Points
- Assigning Location Names to Access Points
- Assigning an Access Point as the Preferred Master

Chapter 3 - Final Initial Configuration Steps in the GUI

Reconnecting to the Unleashed Master Access Point

This is the login page for the new Unleashed Network.

Enter the created “Username”, “Password”, and click “Unleash” to login.

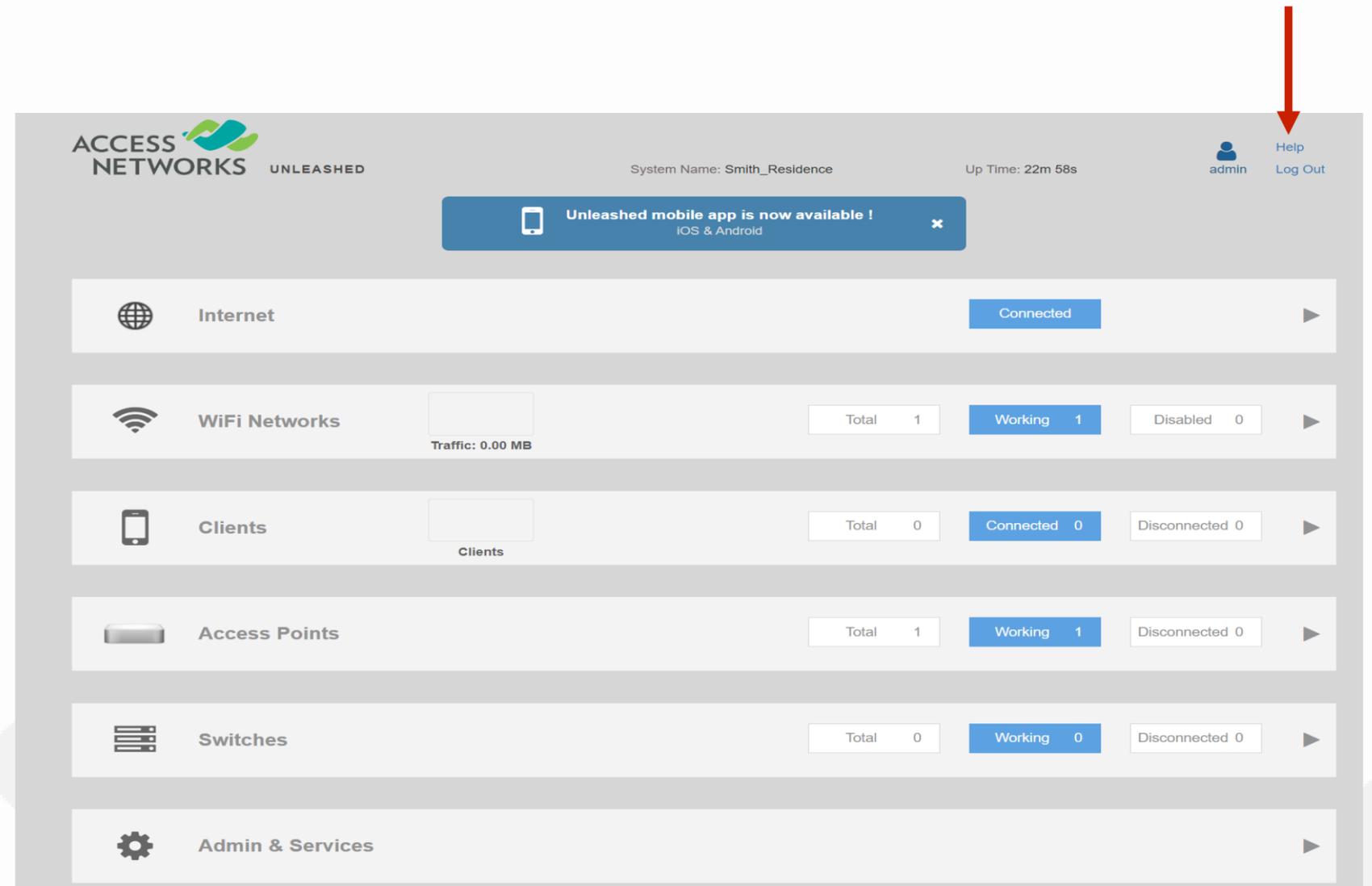


Chapter 3 - Final Initial Configuration Steps in the GUI

Unleashed Dashboard

After successful login, you will be presented with the Unleashed Dashboard, which displays an overview of your Access Networks Unleashed network.

***Note - At any point during the setup process, you can access the complete Unleashed User Guide by clicking on “Help” in the upper right corner of the Unleashed web interface.**



ACCESS NETWORKS UNLEASHED

System Name: Smith_Residence Up Time: 22m 58s

admin Help Log Out

Unleashed mobile app is now available !
iOS & Android

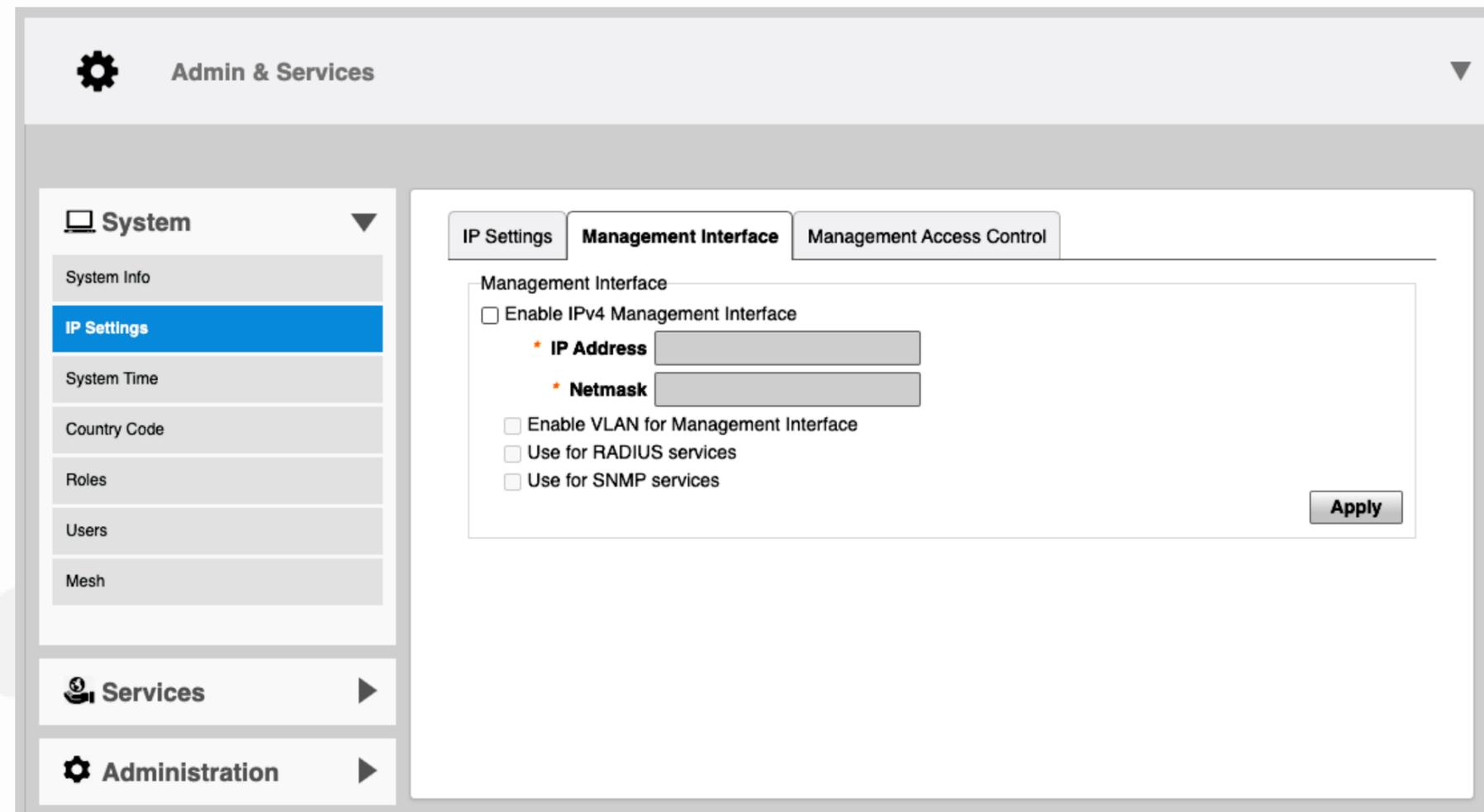
Category	Status	Total	Working	Disconnected
Internet	Connected	-	-	-
WiFi Networks	Traffic: 0.00 MB	1	1	0
Clients	Clients	0	0	0
Access Points		1	1	0
Switches		0	0	0
Admin & Services		-	-	-

Chapter 3 - Final Initial Configuration Steps in the GUI

Configuring a Management Interface

A **static** Management IP address can be configured to allow the administrator to manage the Unleashed network from a single IP address.

This Management IP address will navigate to Unleashed management console, regardless of which access point is currently the Master AP.



Chapter 3 - Final Initial Configuration Steps in the GUI

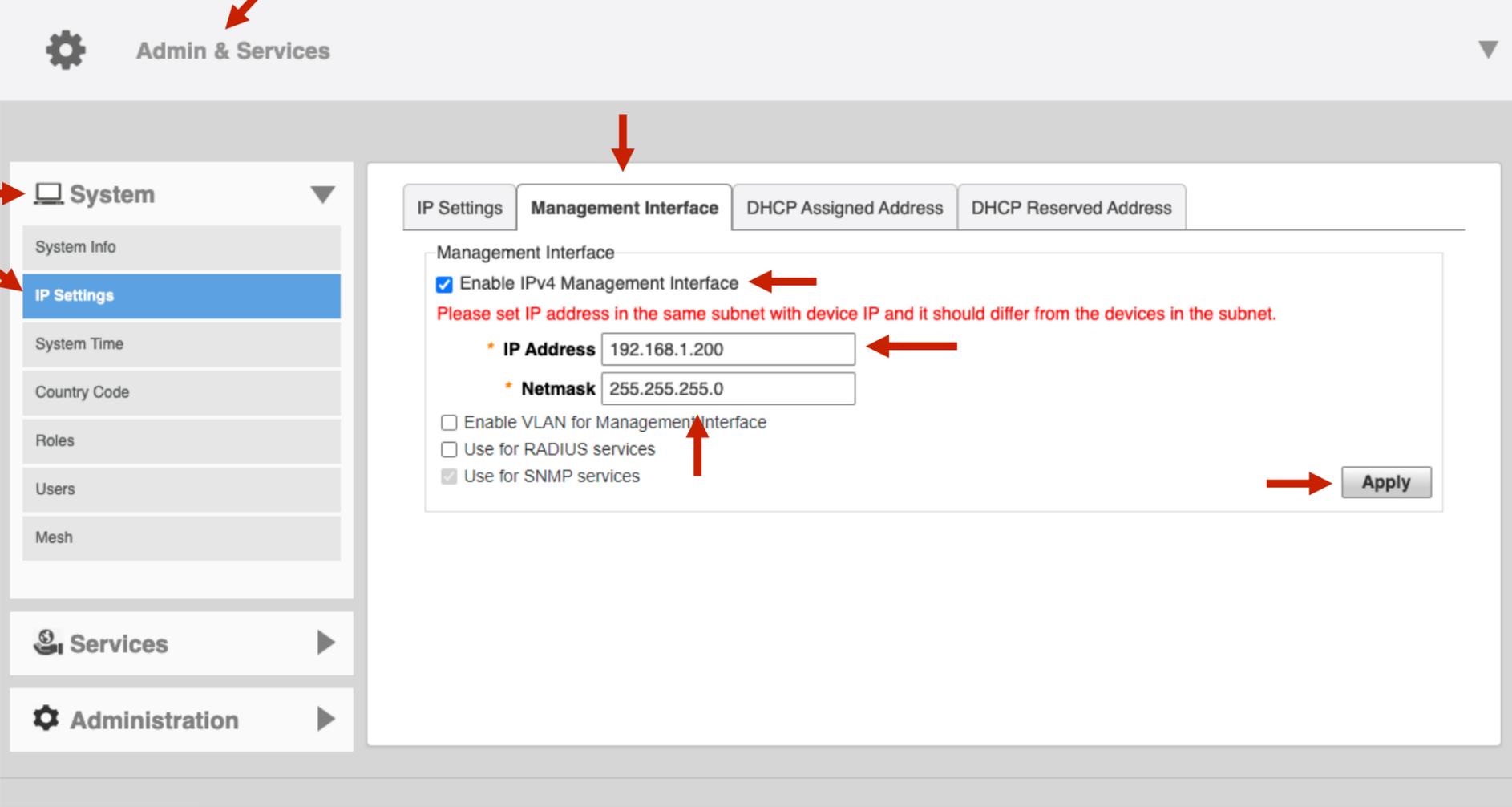
Configuring a Management Interface

Go to “Admin & Services”. Select “System” on the left menu bar to reveal “IP Settings” and choose it. Now click the “Management Interface” tab.

Select the check box next to “Enable IPv4” in the “Management Interface”.

Enter an IP Address and Netmask (Your standard Netmask is 255.255.255.0) and click “Apply”.

***Note - It's required the IP address of the “Management Interface” be on the same subnet of the AP(s) IP and it should differ from other devices in the subnet.**



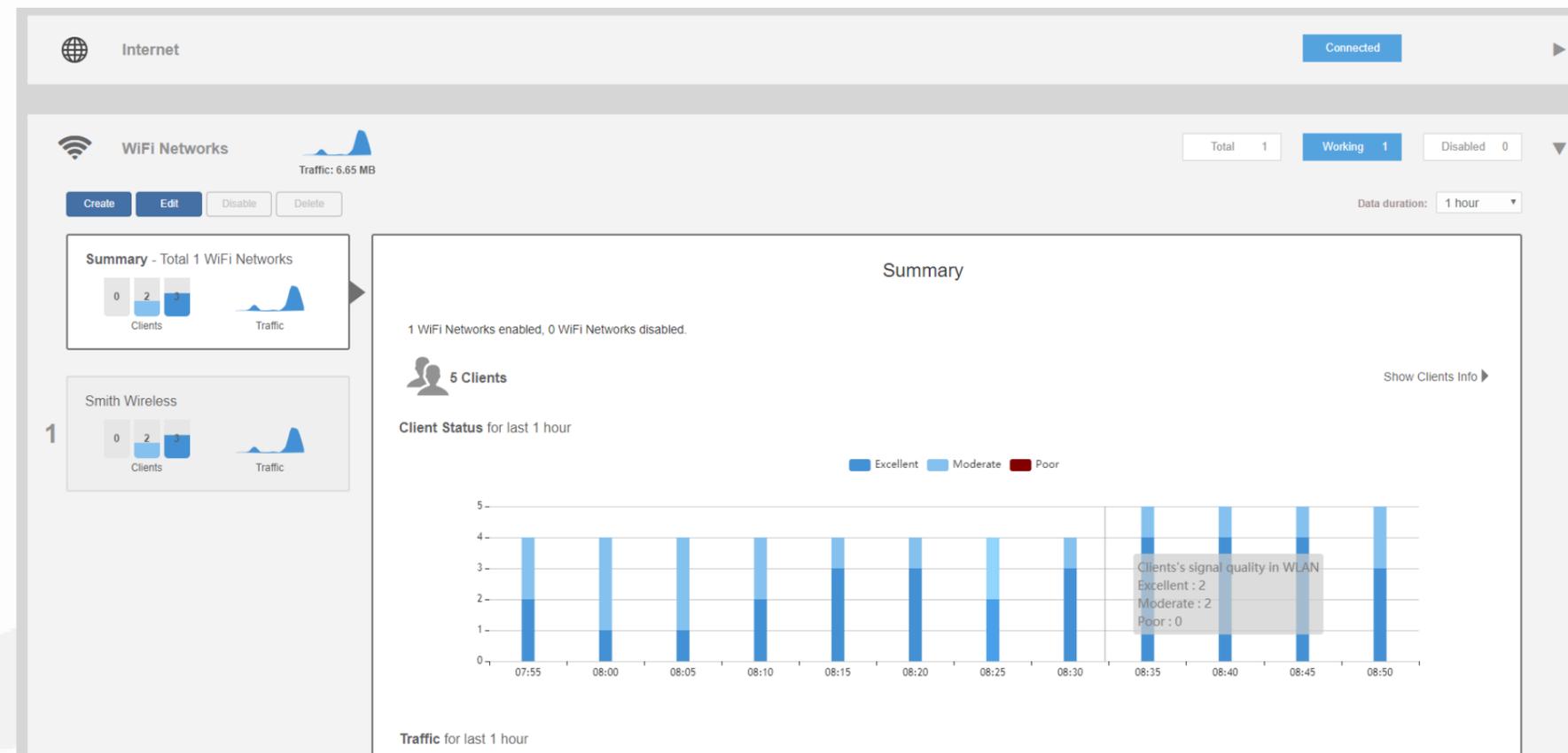
The screenshot shows the 'Admin & Services' configuration page. The left sidebar has 'System' selected, with 'IP Settings' highlighted. The main content area has the 'Management Interface' tab active. The 'Enable IPv4 Management Interface' checkbox is checked. The IP Address field contains '192.168.1.200' and the Netmask field contains '255.255.255.0'. The 'Use for SNMP services' checkbox is checked. The 'Apply' button is visible at the bottom right. Red arrows point to the 'Admin & Services' header, the 'System' menu item, the 'IP Settings' menu item, the 'Management Interface' tab, the 'Enable IPv4 Management Interface' checkbox, the IP Address field, the Netmask field, and the 'Apply' button.

Chapter 3 - Final Initial Configuration Steps in the GUI

Create a Guest Network

Every network deployment should have a “Guest SSID” to allow guests to have internet access but isolate them from the rest of the network devices.

To fully isolate Guest Wireless Clients we need to isolate them other devices connected to the same AP as well as all hosts on the same VLAN/Subnet.



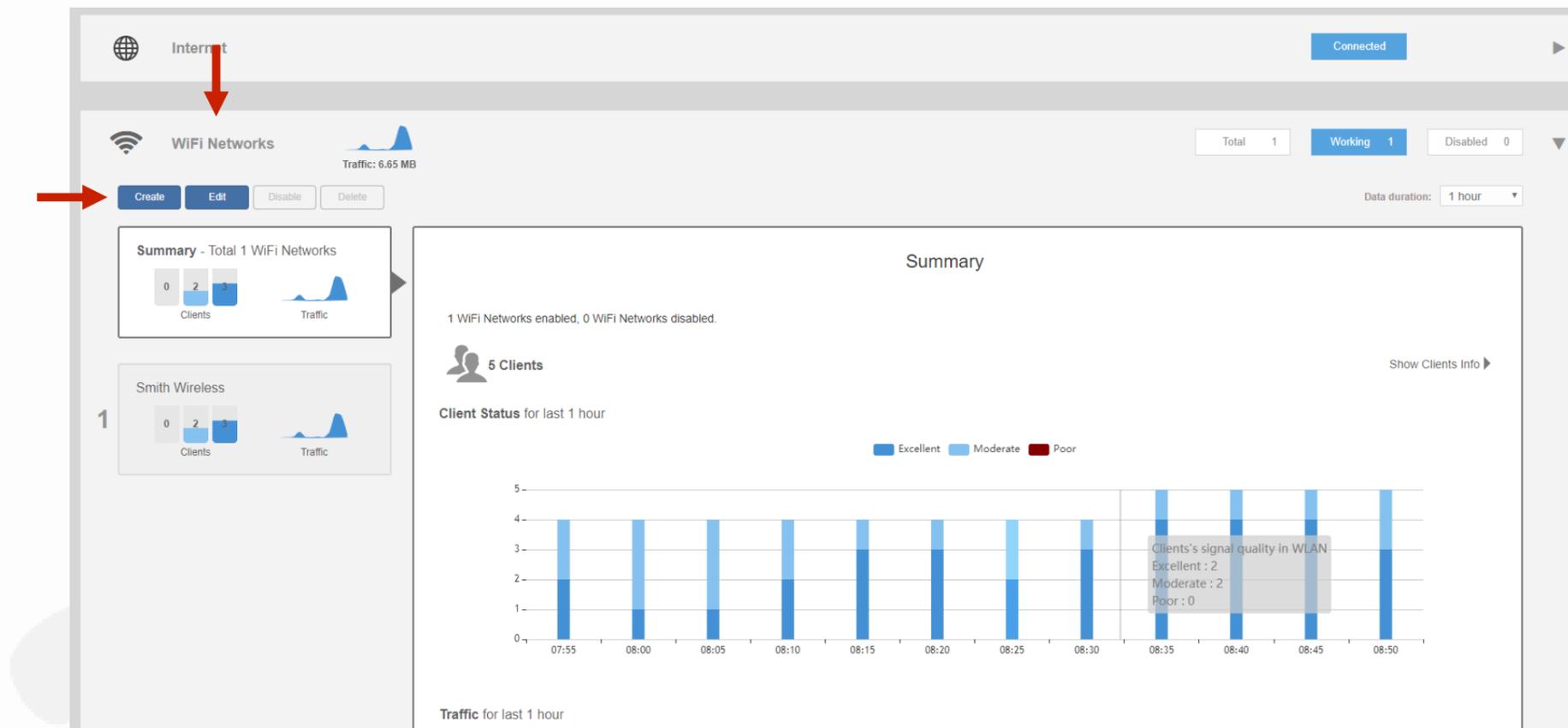
Chapter 3 - Final Initial Configuration Steps in the GUI

Create a Guest Network

First make a new WLAN.

Click anywhere in the “Wi-Fi Networks” section to expand the display of your deployed WLANs.

Now click on “Create” to open the “Create WLAN” pop-up page.



Chapter 3 - Final Initial Configuration Steps in the GUI

Create a Guest Network

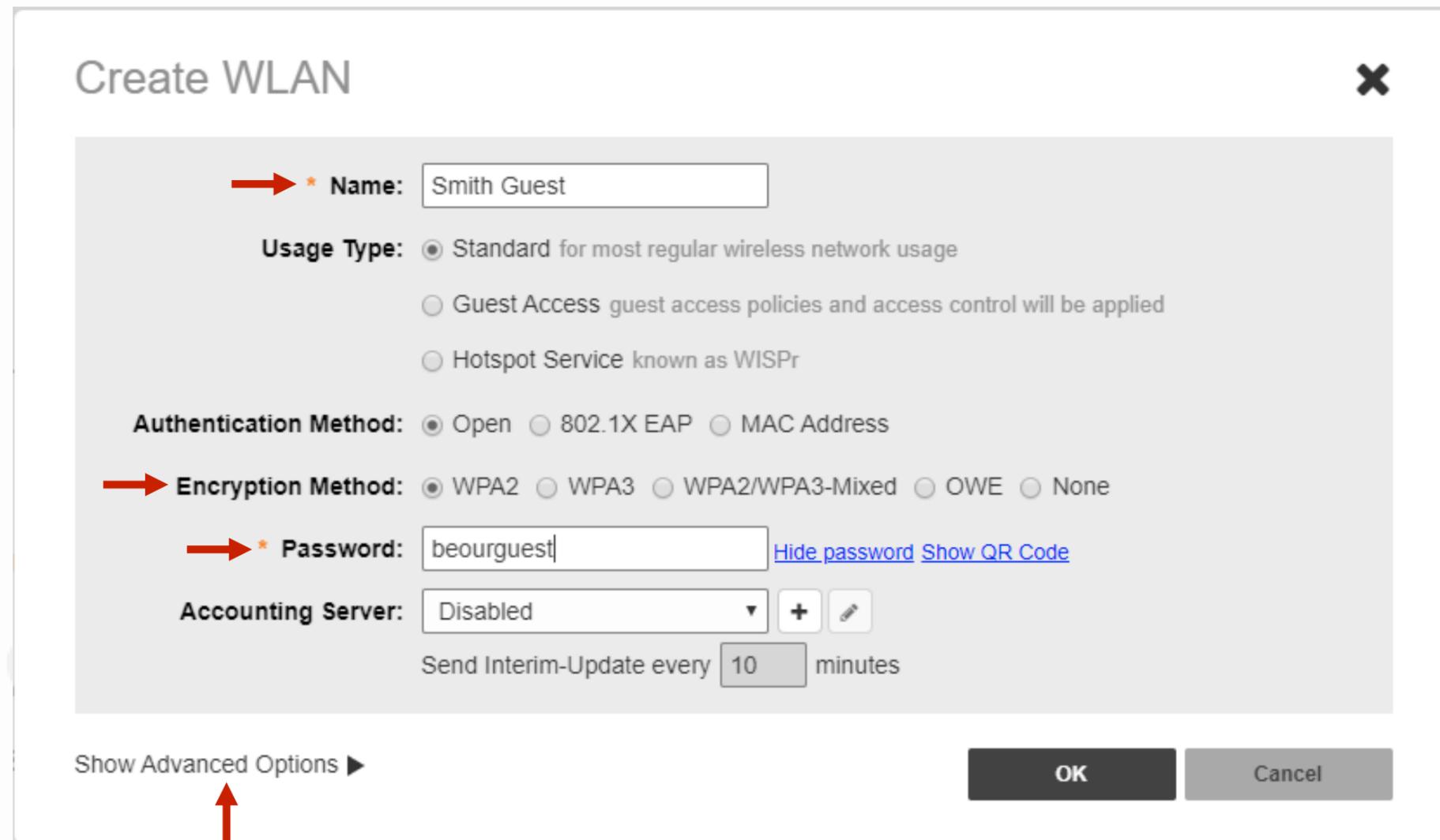
In the new dialog box, enter the SSID under “Name”.

Select the “WPA2” for the “Encryption Method”.

Enter in the passcode under “Password”.

Click on “Show Advanced Options”.

***Note –** Passphrases that are simple to remember will be used more often by your client. A good suggestion for a **SIMPLE** Guest WLAN passphrase is “beourguest”.



Create WLAN

Name: Smith Guest

Usage Type: Standard for most regular wireless network usage
 Guest Access guest access policies and access control will be applied
 Hotspot Service known as WISPr

Authentication Method: Open 802.1X EAP MAC Address

Encryption Method: WPA2 WPA3 WPA2/WPA3-Mixed OWE None

Password: beourguest [Hide password](#) [Show QR Code](#)

Accounting Server: Disabled

Send Interim-Update every 10 minutes

Show Advanced Options ▶

Chapter 3 - Final Initial Configuration Steps in the GUI



Create a Guest Network

Select the check box for “Wireless Client Isolation”.

This will ensure that guest network client devices are isolated from other wireless clients on the same AP.

The next step will be to isolate guest network client devices from all hosts on the same VLAN/Subnet.

The screenshot shows a configuration window titled "Hide Advanced Options" with a dropdown arrow. Below the title are five tabs: "Zero-IT & DPSK", "WLAN Priority", "Access Control", "Radio Control", and "Others". The "Others" tab is selected and contains the following settings:

- Force DHCP:** Enable Force DHCP. Disconnect client if client does not obtain valid IP address in seconds.
- Inactivity Timeout:** Terminate idle user session after minute(s)
- Wireless Client Isolation:** Isolate wireless client traffic from other clients on the same AP.
 Isolate wireless client traffic from all hosts on the same VLAN/subnet.
No AllowList
(Requires allowlist for gateway and other allowed hosts.)
- DTIM Interval:** (1-255) Defines the frequency of beacons that will include a DTIM
- Directed MC/BC Threshold:** (0-128) Defines the client count at which an AP will stop converting group-addressed data traffic to unicast
- Client Traffic Logging:** Send traffic flow data to syslog server
 Send connection records to syslog server
also available for download at Client Connection Logs section of Admin & Services -> Administration-> Diagnostics -> Client Troubleshooting tab

At the bottom right of the window are "OK" and "Cancel" buttons.

Chapter 3 - Final Initial Configuration Steps in the GUI

Create a Guest Network

Select the check box for “Isolate wireless client traffic from all hosts on the same VLAN/subnet.”

Now select the “+” symbol. This will allow you to create a “Allowlist” rule.

***Note - An “Allowlist” is used to identify the router as the only device that guest network client devices can communicate with. This will allow internet access while maintaining isolation from other devices.**

Hide Advanced Options ▼

Zero-IT & DPSK | WLAN Priority | Access Control | Radio Control | **Others**

Force DHCP: Enable Force DHCP. Disconnect client if client does not obtain valid IP address in seconds.

Inactivity Timeout: Terminate idle user session after minute(s)

Wireless Client Isolation: Isolate wireless client traffic from other clients on the same AP.
 Isolate wireless client traffic from all hosts on the same VLAN/subnet.

▼ + ←

(Requires allowlist for gateway and other allowed hosts.)

DTIM Interval: (1-255) Defines the frequency of beacons that will include a DTIM

Directed MC/BC Threshold: (0-128) Defines the client count at which an AP will stop converting group-addressed data traffic to unicast

Client Traffic Logging: Send traffic flow data to syslog server
 Send connection records to syslog server
also available for download at Client Connection Logs section of Admin & Services -> Administration-> Diagnostics -> Client Troubleshooting tab

OK Cancel

Chapter 3 - Final Initial Configuration Steps in the GUI

Create a Guest Network

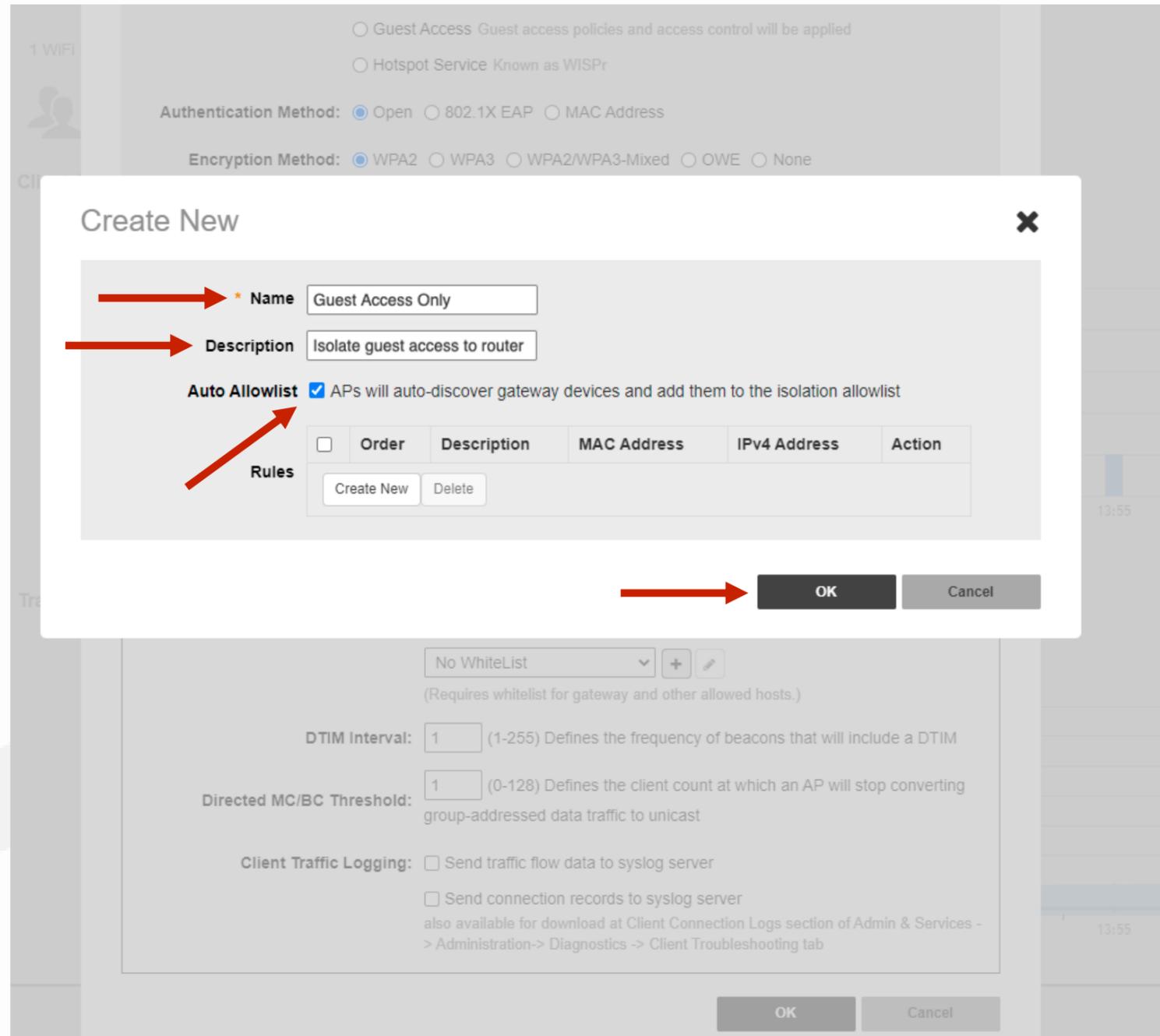
First select a “Name” for your “AllowList”.

Add a “Description” of your “AllowList”.

Ensure the “Auto Allowlist” check box is enabled.

Enabling this feature allows the Unleashed Master AP to identify the MAC address of the Gateway and automatically add it to the “Allowlist”

Click on “OK” to continue.



1 WiFi

Guest Access Guest access policies and access control will be applied

Hotspot Service Known as WISPr

Authentication Method: Open 802.1X EAP MAC Address

Encryption Method: WPA2 WPA3 WPA2/WPA3-Mixed OWE None

Create New

Guest Access Only

Isolate guest access to router

Auto Allowlist APs will auto-discover gateway devices and add them to the isolation allowlist

<input type="checkbox"/>	Order	Description	MAC Address	IPv4 Address	Action
<input type="button" value="Create New"/>	<input type="button" value="Delete"/>				

No WhiteList

(Requires whitelist for gateway and other allowed hosts.)

DTIM Interval: (1-255) Defines the frequency of beacons that will include a DTIM

Directed MC/BC Threshold: (0-128) Defines the client count at which an AP will stop converting group-addressed data traffic to unicast

Client Traffic Logging: Send traffic flow data to syslog server

Send connection records to syslog server
also available for download at Client Connection Logs section of Admin & Services -> Administration-> Diagnostics -> Client Troubleshooting tab

Chapter 3 - Final Initial Configuration Steps in the GUI

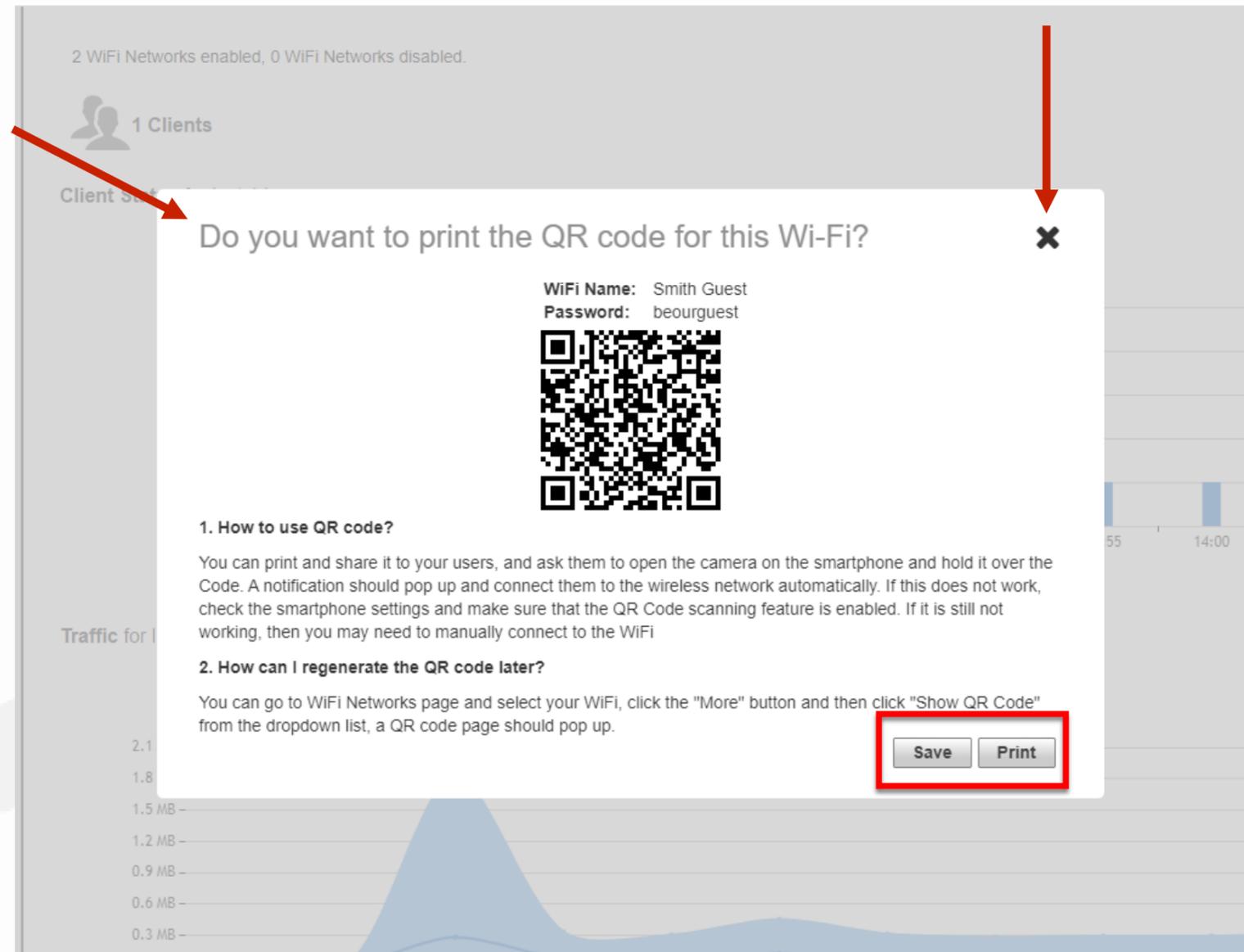
Create a Guest Network

The Guest WLAN is now active and all traffic from guest network client devices will be isolated, from all other client devices on the network, but will still have internet connectivity.

A new QR code window will now pop up.

The QR code is used to provide access for Guest client devices and can be printed or saved for later use.

Click on the “x” to continue.



Chapter 3 - Final Initial Configuration Steps in the GUI



Adjusting Access Points for Best Channels/Performance Mode

Under “Admin & Services”, select “System”.

From the sub menu select “Country Code”.

Select the option “Optimize for Performance”. This will enable all available 5GHz channels.

Click on “Apply” to continue.

The screenshot displays the 'Admin & Services' configuration interface. The left sidebar shows a menu with 'System' selected, and 'Country Code' highlighted in blue. The main content area shows the 'Country Code' configuration page. The 'Country Code' is set to 'United States'. Under 'Channel Optimization', three radio buttons are present: 'Optimize for Compatibility', 'Optimize for Interoperability', and 'Optimize for Performance', which is selected. An 'Apply' button is located at the bottom right of the configuration area. Red arrows point to the 'Admin & Services' header, the 'System' menu item, the 'Country Code' menu item, the 'Optimize for Performance' radio button, and the 'Apply' button.

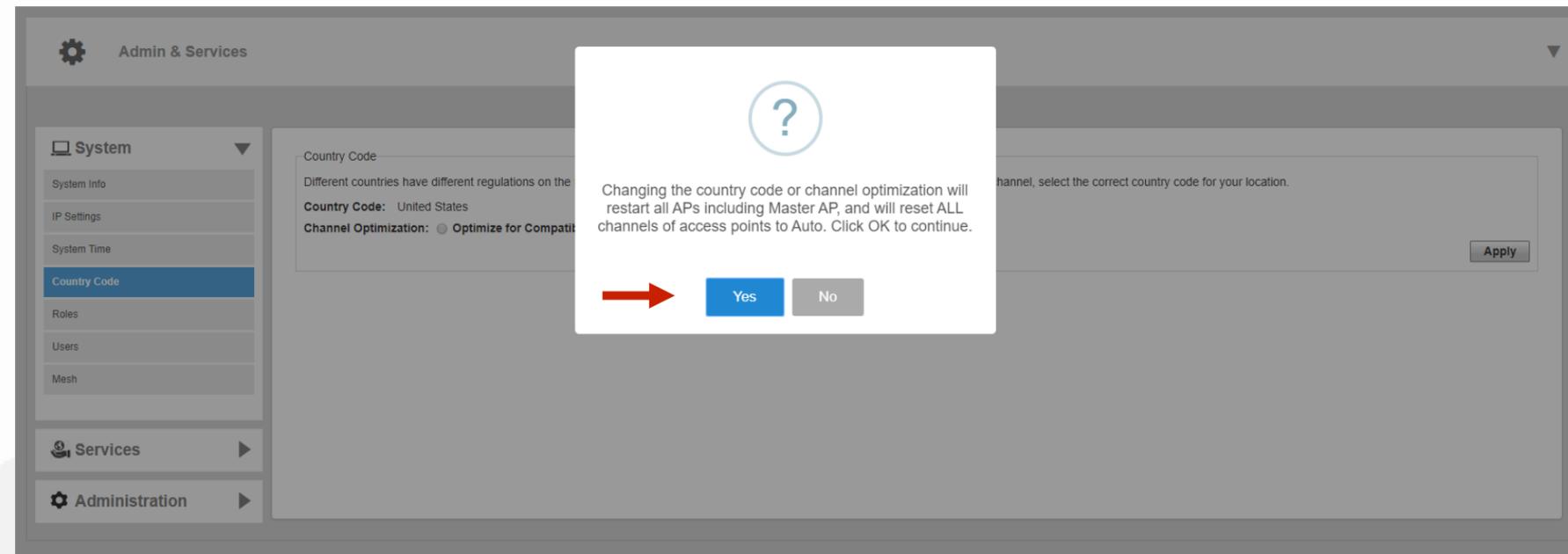
Chapter 3 - Final Initial Configuration Steps in the GUI

Adjusting Access Points for Best Channels/Performance Mode

A new dialog box will appear to verify that you indeed want to optimize all APs including the Master AP.

Click “Yes” to continue.

***Note:** After changing to performance mode all access points will reboot, it will then be necessary to review the channels available for automatic channel selection.

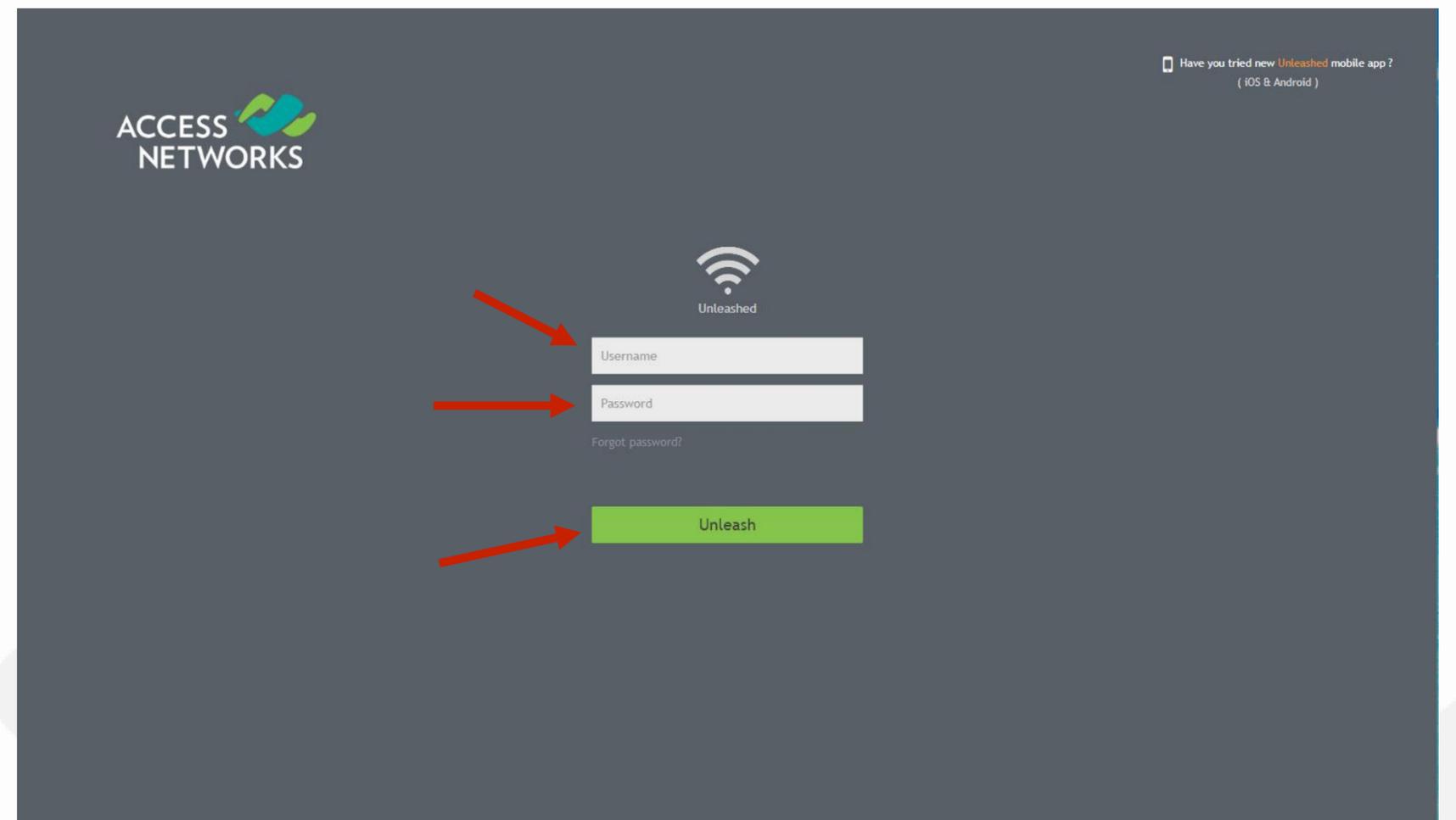


Chapter 3 - Final Initial Configuration Steps in the GUI

Adjusting Access Points for Best Channels/Performance Mode

After the system has completed the rebooting process, you will need to re-login.

Enter the created “Username”, “Password”, and click “Unleash” to login.



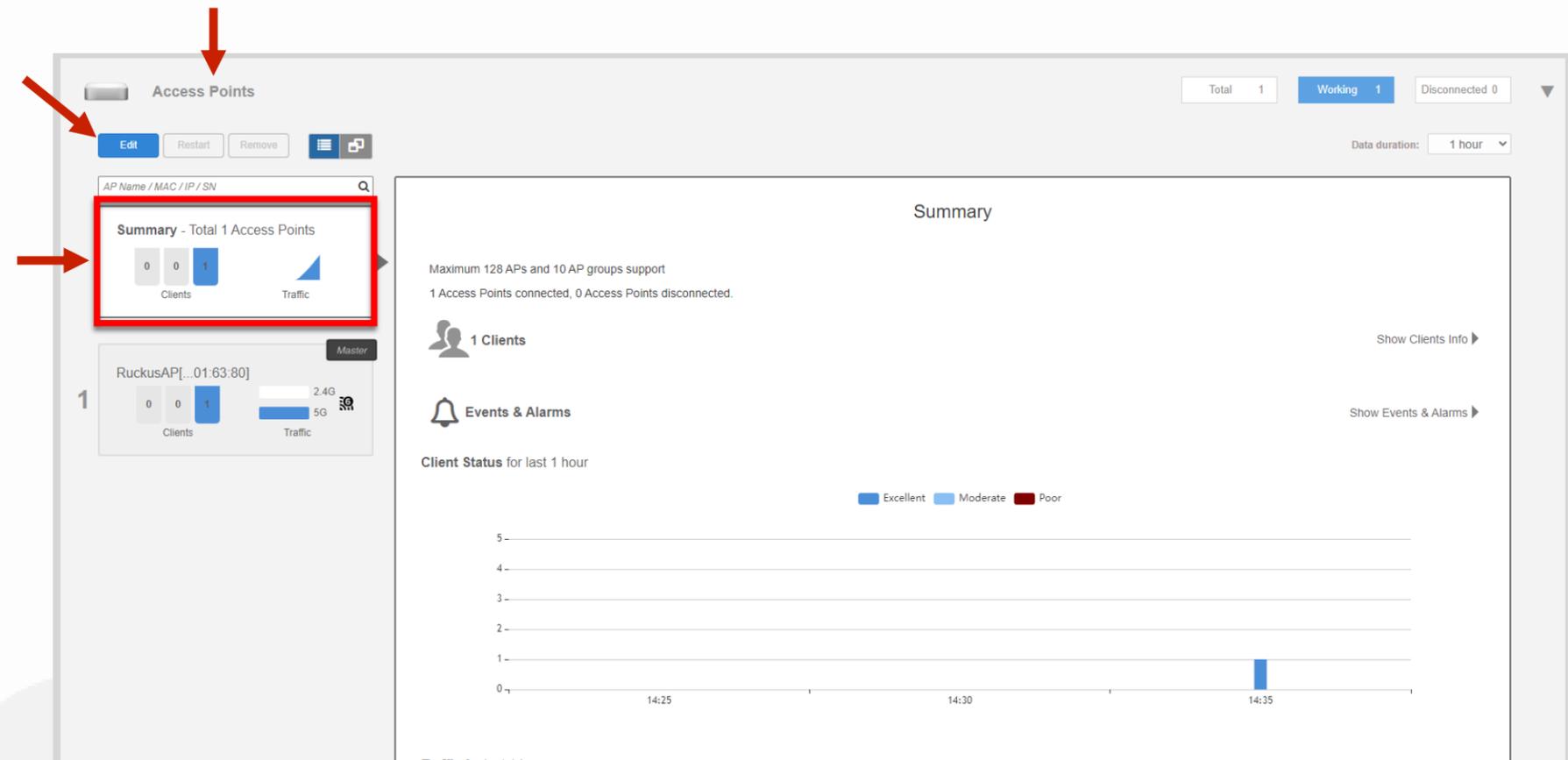
Chapter 3 - Final Initial Configuration Steps in the GUI

Adjusting Access Points for Best Channels/Performance Mode

Navigate back to “Access Points” and click anywhere in the “Access Points” section to expand the display of your deployed AP’s.

The “Summary” area is where you can make global changes for all connected Unleashed access points.

Click on “Summary” and select “Edit”.



The screenshot displays the 'Access Points' management interface. At the top, there are buttons for 'Edit', 'Restart', and 'Remove'. Below these is a search bar for 'AP Name / MAC / IP / SN'. The 'Summary' section is highlighted with a red box and contains the following information:

- Summary - Total 1 Access Points
- 0 Clients, 0 Traffic
- 1 RuckusAP[...]01.63.80] (Master)
- 0 Clients, 0 Traffic, 2.4G, 5G

On the right side of the interface, there is a 'Summary' panel with the following details:

- Maximum 128 APs and 10 AP groups support
- 1 Access Points connected, 0 Access Points disconnected.
- 1 Clients (with 'Show Clients Info' link)
- Events & Alarms (with 'Show Events & Alarms' link)
- Client Status for last 1 hour (with a bar chart showing status: Excellent, Moderate, Poor)

Chapter 3 - Final Initial Configuration Steps in the GUI



Adjusting Access Points for Best Channels/Performance Mode

Click on the tab labeled “Radio 2.4 GHz”.

Deselect the following channels “2, 3, 4, 5, 7, 8, 9 and 10”. This will limit automatic channel selection to channels 1,6,11 on 2.4GHz

Edit AP Group ✕

Name System Default

Radio (2.4G) Radio (5G) Other

Radio 2.4 GHz 1 2 3 4 5 6 7 8 9 10 11

Channelization Auto

Channel Auto

TX Power Auto

Call Admission Control Off

WLAN Service Enable

Protection Mode RTS/CTS

Finish **Cancel**

Chapter 3 - Final Initial Configuration Steps in the GUI



Adjusting Access Points for Best Channels/Performance Mode

Let's change the "Auto" settings for "Channelization" and "TX Power" for the 2.4 GHz Radio.

Under "Channelization", let's select "20" MHz wide channel instead of "Auto".

Now let's switch the "TX Power" from "Auto" to "Full" power.

Click on the tab labeled "Radio (5G)".

The screenshot shows the 'Edit AP Group' configuration window. At the top, the 'Name' field is set to 'System Default'. Below this, there are three tabs: 'Radio (2.4G)', 'Radio (5G)', and 'Other'. The 'Radio (2.4G)' tab is active. Under 'Radio 2.4 GHz', there are several settings: 'Channelization' is set to '20' (indicated by a red arrow pointing to the dropdown menu), 'Channel' is set to 'Auto', 'TX Power' is set to 'Full' (indicated by a red arrow pointing to the dropdown menu), 'Call Admission Control' is set to 'Off', 'WLAN Service' is set to 'Enable', and 'Protection Mode' is set to 'RTS/CTS'. At the top of the radio settings, there are checkboxes for channels 1 through 11, with channels 1, 6, and 11 checked. At the bottom right of the window, there are 'Finish' and 'Cancel' buttons.

Chapter 3 - Final Initial Configuration Steps in the GUI



Adjusting Access Points for Best Channels/Performance Mode

Review all the new channels that are now available for "ChannelFly".

Change "Channelization" from "Auto" to "80" Mhz.

Change "TX Power" from "Auto" to "Full" power.

Select "Finish" to continue.

Edit AP Group

Name System Default

Radio (2.4G) Radio (5G) Other

Radio 5.0 GHz Indoor 36 40 44 48 52 56 60 64 100 104 108
 112 116 120 124 128 132 136 149 153 157 161
Radio 5.0 GHz Outdoor 36 40 44 48 52 56 60 64 100 104 108
 112 116 120 124 128 132 136 149 153 157 161

Channelization 80

Channel Indoor Auto Outdoor Auto

TX Power Full

Call Admission Control Off

WLAN Service Enable



Finish

Cancel

Chapter 3 - Final Initial Configuration Steps in the GUI

Automatic Channel Selection (Self Healing)

Unleashed access point use two different techniques for “Self Healing” a wireless deployment by identifying interference and measuring performance, then automatically changing the channels each access point uses, to improve the client device experience.

“Background scanning” is used on the 2.4GHz spectrum as it keeps a historical record of how many other devices are broadcasting a specific channel and will then direct each AP to use the 2.4GHz channel that has the lowest number of direct interferers.

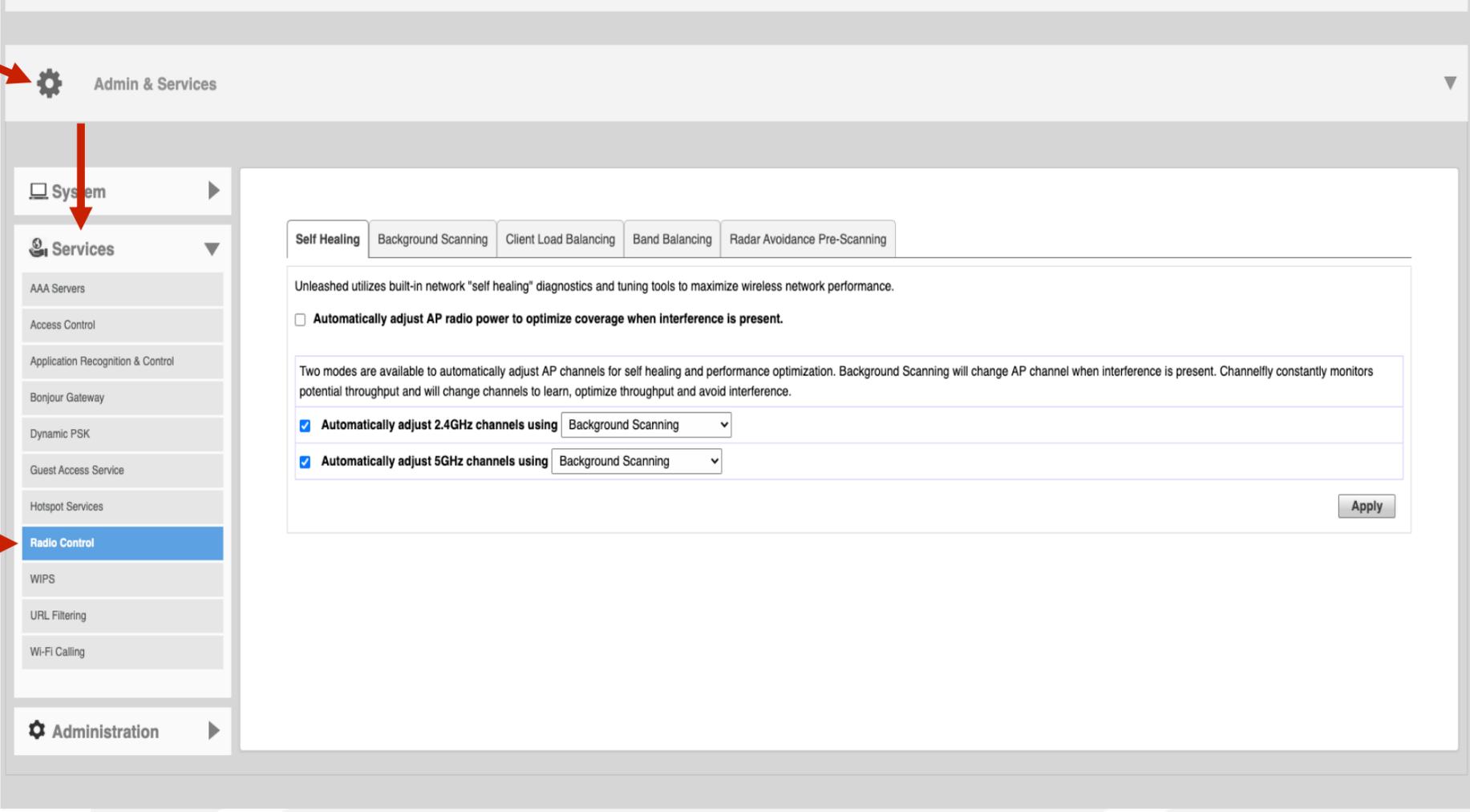
“Channel Fly” is used on the 5GHz spectrum as it not only records the number of direct interferers, but it also records the performance of authenticated devices and directs each AP to use the 5GHz channel that provides the best throughput for connected devices.

Chapter 3 - Final Initial Configuration Steps in the GUI

Automatic Channel Selection

Click anywhere on "Admin & Services" to reveal the sub menus.

Now select "Services" to reveal the sub menus. Select "Radio Control" from the left menu.



The screenshot displays the 'Admin & Services' configuration page. The left sidebar is expanded to show the 'Services' menu, with 'Radio Control' selected. The main content area shows the 'Self Healing' tab, which includes options for 'Automatically adjust AP radio power to optimize coverage when interference is present' (unchecked) and 'Automatically adjust 2.4GHz channels using Background Scanning' (checked). The 'Automatically adjust 5GHz channels using Background Scanning' option is also checked. An 'Apply' button is visible at the bottom right of the configuration area.

Chapter 3 - Final Initial Configuration Steps in the GUI

Automatic Channel Selection

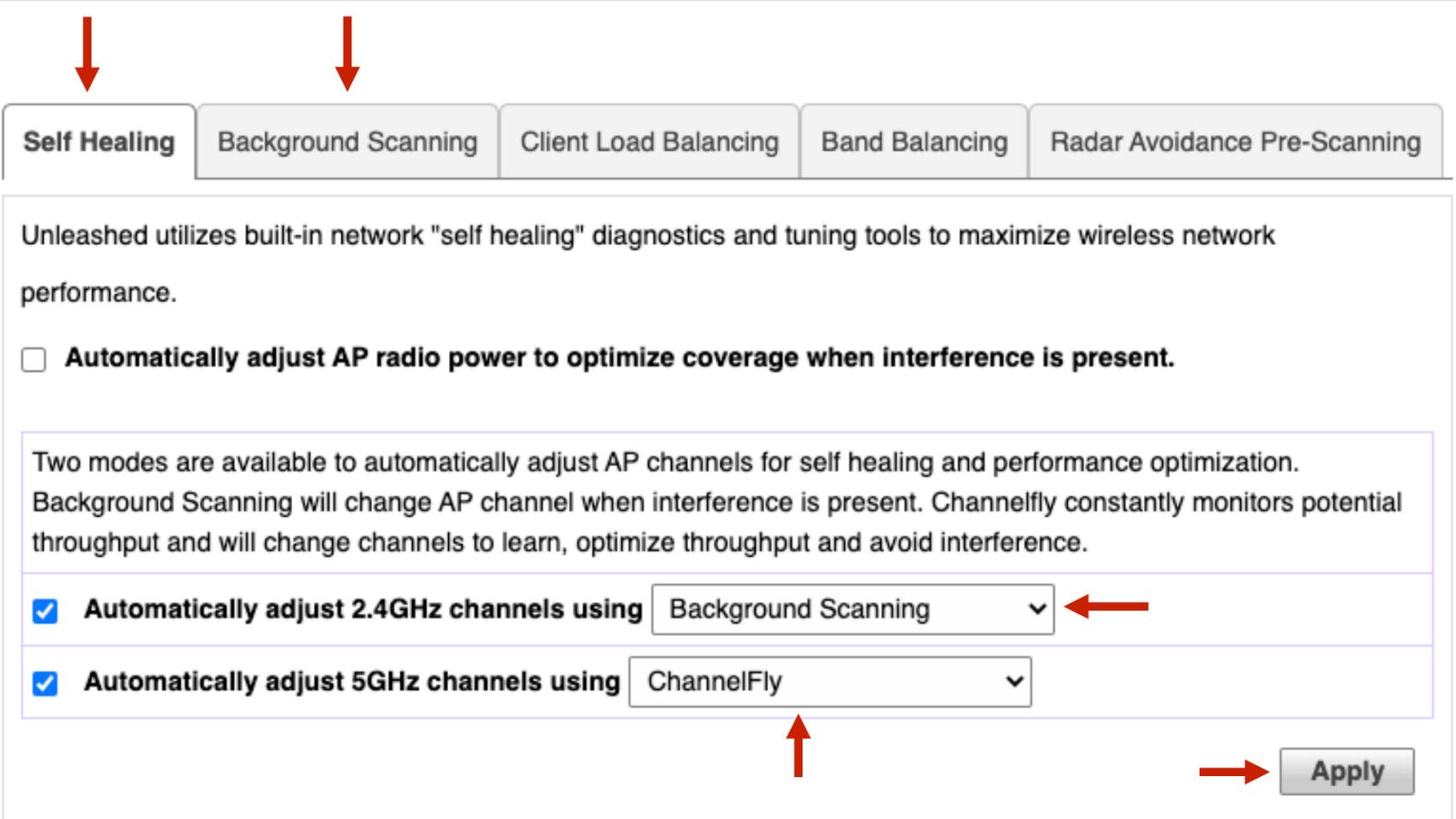
“Self Healing” will be the first tab that adjustments will be made.

Make sure 2.4GHz channels are using “Background Scanning”.

Make sure 5GHz channels are using “ChannelFly”.

Click on “Apply” to continue.

Then select the Tab labeled “Background Scanning”.



Self Healing Background Scanning Client Load Balancing Band Balancing Radar Avoidance Pre-Scanning

Unleashed utilizes built-in network "self healing" diagnostics and tuning tools to maximize wireless network performance.

Automatically adjust AP radio power to optimize coverage when interference is present.

Two modes are available to automatically adjust AP channels for self healing and performance optimization. Background Scanning will change AP channel when interference is present. Channelfly constantly monitors potential throughput and will change channels to learn, optimize throughput and avoid interference.

Automatically adjust 2.4GHz channels using Background Scanning

Automatically adjust 5GHz channels using ChannelFly

Apply

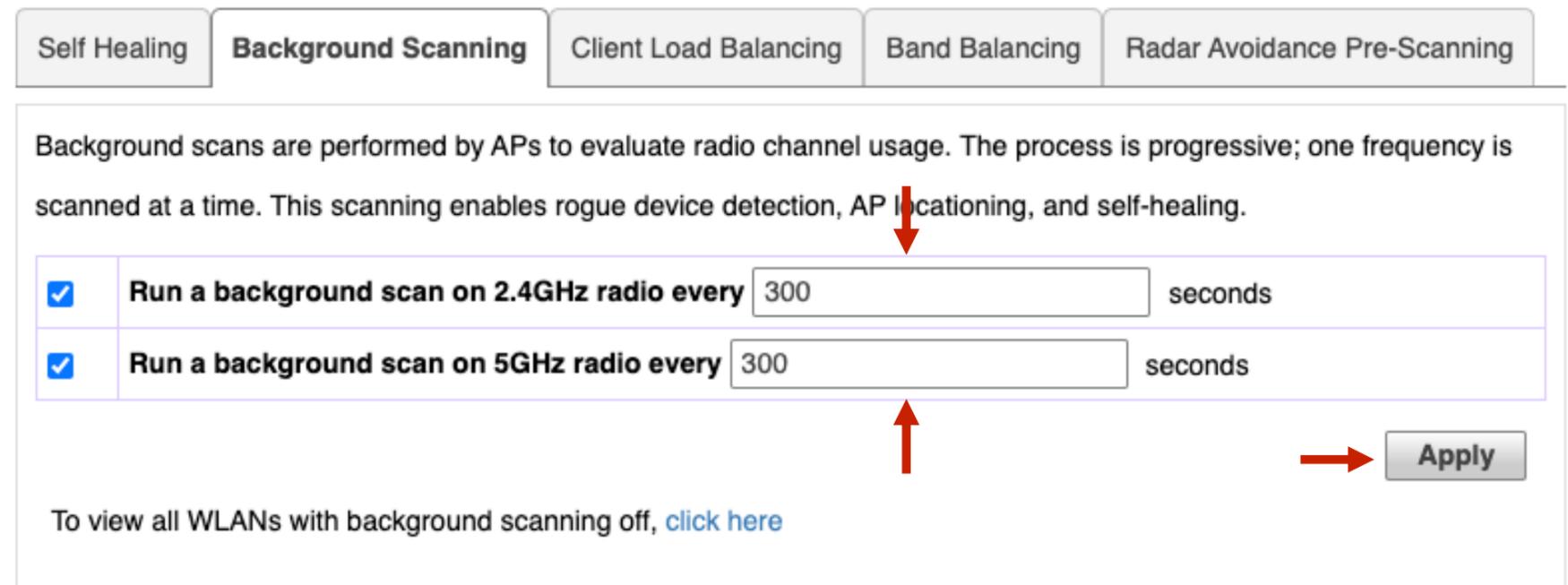
Chapter 3 - Final Initial Configuration Steps in the GUI

Automatic Channel Selection

Background scan on 2.4GHz radio should be set to every “300” seconds.

Background scan on 5GHz radio should be set to every “300” seconds.

After these changes have been made from the default settings, click on “Apply” to continue.



Self Healing **Background Scanning** Client Load Balancing Band Balancing Radar Avoidance Pre-Scanning

Background scans are performed by APs to evaluate radio channel usage. The process is progressive; one frequency is scanned at a time. This scanning enables rogue device detection, AP locationing, and self-healing.

<input checked="" type="checkbox"/>	Run a background scan on 2.4GHz radio every <input type="text" value="300"/> seconds
<input checked="" type="checkbox"/>	Run a background scan on 5GHz radio every <input type="text" value="300"/> seconds

To view all WLANs with background scanning off, [click here](#)

Chapter 3 - Final Initial Configuration Steps in the GUI

Adding Additional Unleashed Access Points

Deploying additional Unleashed member APs is simply a matter of connecting them via Ethernet to the same Layer 2 network switch and providing power. They will discover the Unleashed Master and join automatically. No additional steps are necessary.

The second and any additional APs that join an Unleashed network will automatically assume the role of Unleashed member AP. Thereafter, if the Master AP goes offline, one of the member APs will become the new Master and assume control of the Unleashed network.



***Note - Any (non-mesh) AP can become the Master if the preferred Master is offline, but when the Preferred Master comes back online, it will assume the Master role again.**

Chapter 3 - Final Initial Configuration Steps in the GUI

Adding Additional Unleashed Access Points

Note: When a member AP joins the Master for the first time, if the member AP is running a different firmware version than the Master, it will automatically download and upgrade (or downgrade) itself to the correct firmware version to match that of the Master, reboot, and then rejoin the Unleashed network once the proper firmware is running.

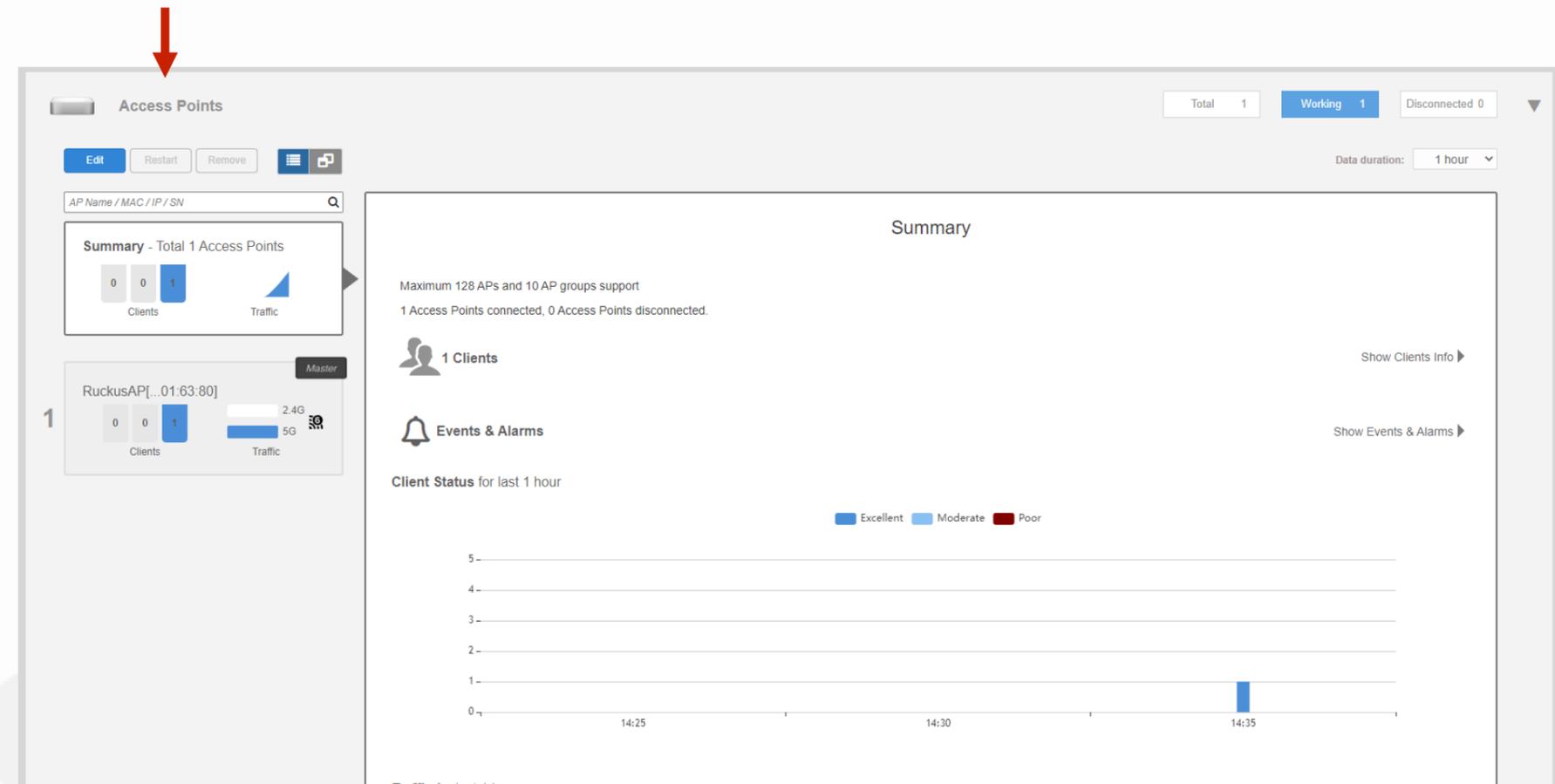


Chapter 3 - Final Initial Configuration Steps in the GUI

Assign Location Names to Access Points

As a part of your installation procedures, it is highly recommended that you label each access point with a description of where it was installed.

To make these changes proceed by clicking anywhere in the “Access Points” section to expand the display of your deployed AP’s.

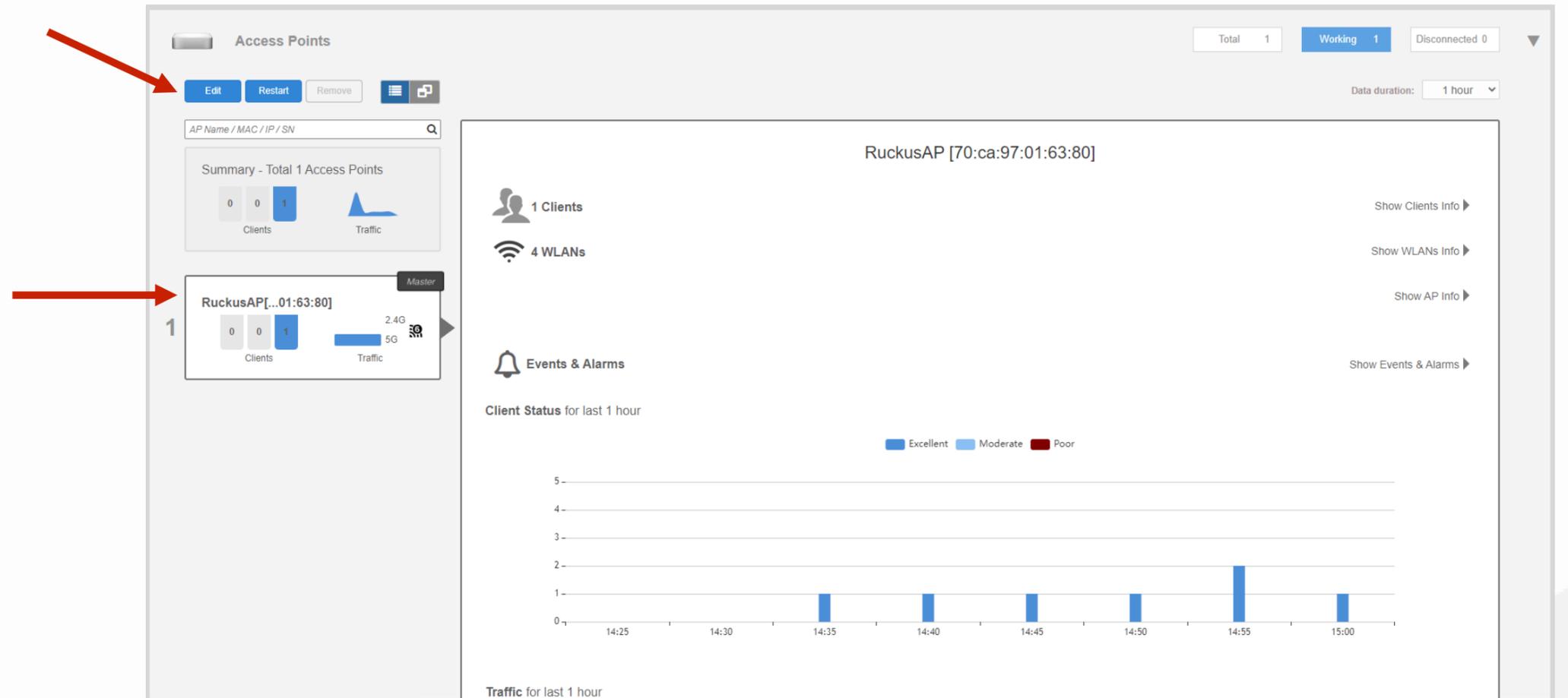


Chapter 3 - Final Initial Configuration Steps in the GUI

Assign Location Names to Access Points

Click on the AP you want to configure.

Then click “Edit”.



The screenshot displays the Ruckus GUI for configuring an Access Point. The main heading is "Access Points". At the top right, it shows "Total 1", "Working 1", and "Disconnected 0". Below this, there are buttons for "Edit", "Restart", and "Remove". A search bar is present with the text "AP Name / MAC / IP / SN".

The "Summary - Total 1 Access Points" section shows a bar chart for "Clients" with values 0, 0, and 1. Below this, the selected AP is "RuckusAP[...01:63:80]" with a "Master" tag. It also shows a bar chart for "Clients" with values 0, 0, and 1, and a "Traffic" bar chart showing 2.4G and 5G.

The right-hand side of the page contains several sections:

- 1 Clients**: Includes a "Show Clients Info" link.
- 4 WLANs**: Includes a "Show WLANs Info" link.
- Events & Alarms**: Includes a "Show Events & Alarms" link.

The "Client Status for last 1 hour" section features a bar chart with a legend for "Excellent" (blue), "Moderate" (light blue), and "Poor" (red). The x-axis shows time intervals from 14:25 to 15:00. The y-axis ranges from 0 to 5. The chart shows a single bar at 14:55 with a value of 2, which is colored blue (Excellent).

The "Traffic for last 1 hour" section is partially visible at the bottom.

Chapter 3 - Final Initial Configuration Steps in the GUI



Assign Location Names to Access Points

Enter the access point's "Device Name".

Enter the "Description" of the access point. It should be the same as the "Device Name".

Now add a good detailed location of the access point in the "Location" field. This description will allow anyone that services the Unleashed Network to quickly find the location of the access point.

Then select OK.

A screenshot of the 'Edit AP(60:d0:2c:38:22:90)' configuration window. The window has a title bar with a close button (X) and a tabbed interface with 'General', 'Radio 2.4 GHz', 'Radio 5.0 GHz', 'Network', and 'Other' tabs. The 'General' tab is active. The form contains the following fields: 'MAC Address' (60:d0:2c:38:22:90), 'Device Name' (Office), 'Description' (Office), 'Location' (Coat Closet - Inside the square), and 'GPS Coordinates' (Latitude and Longitude fields). Red arrows point to the 'Device Name', 'Description', and 'Location' fields. At the bottom right, there are 'OK' and 'Cancel' buttons, with a red arrow pointing to the 'OK' button. The background shows a blurred view of the main GUI with a 'Client Status for last 1 hour' section.

Chapter 3 - Final Initial Configuration Steps in the GUI



Assign an Access Point as the Preferred Master

By default, there is no preference as to which AP should become the Master AP; the first AP that is deployed automatically becomes the Master AP.

Using the Preferred Master setting, users can configure one AP to have priority. Any (non-mesh) AP can become the Master if the preferred Master is offline, but when the Preferred Master comes back online, it will assume the Preferred Master role again.

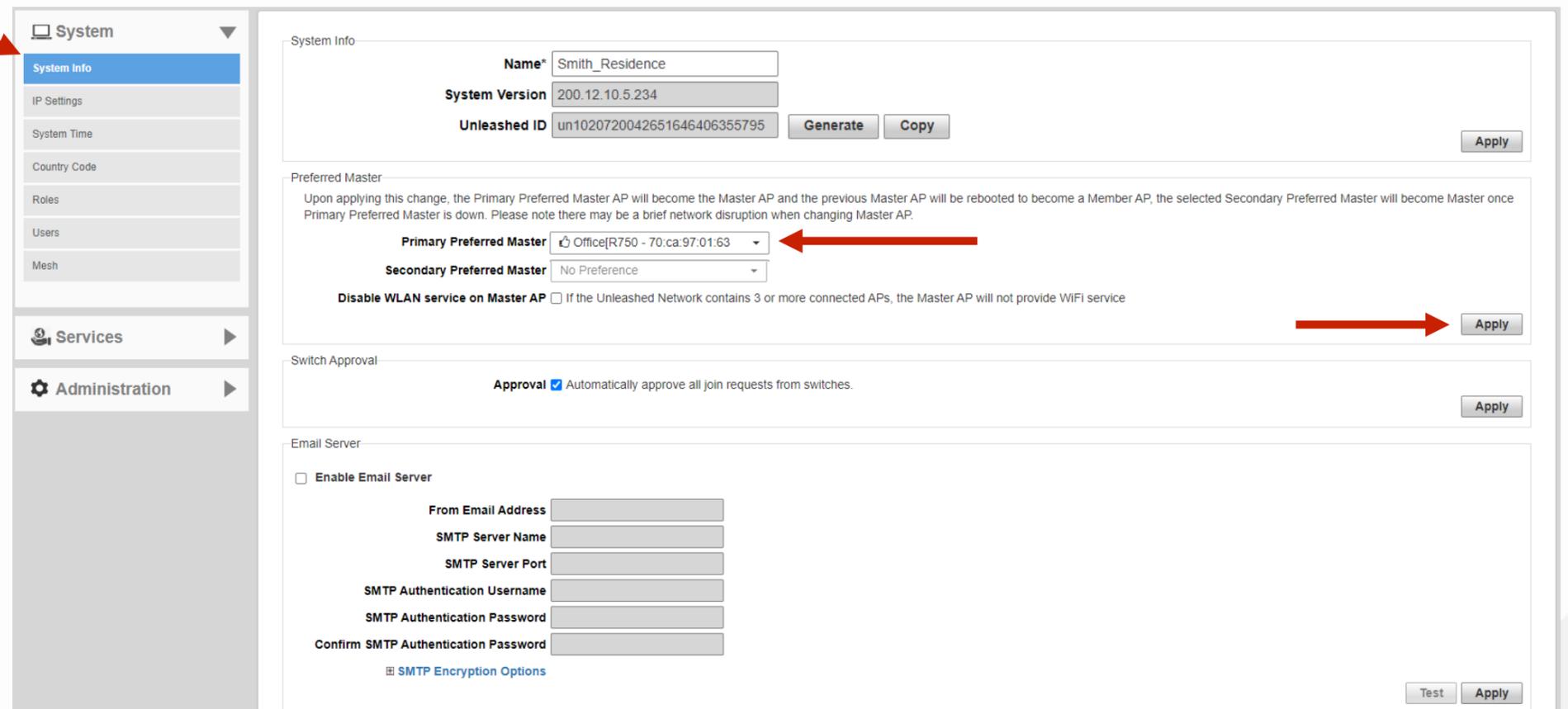
Chapter 3 - Final Initial Configuration Steps in the GUI

Assign an Access Point as the Primary Preferred Master

Click anywhere on "Admin & Services" to reveal the sub menus.

Now select "System Info". Under "Preferred Master", click on the drop-down arrow to reveal which AP you would like to make the "Primary Preferred Master".

Click on "Apply" to continue.



System

- System Info
- IP Settings
- System Time
- Country Code
- Roles
- Users
- Mesh

Services

Administration

System Info

Name: Smith_Residence

System Version: 200.12.10.5.234

Unleashed ID: un1020720042651646406355795

Generate Copy

Apply

Preferred Master

Upon applying this change, the Primary Preferred Master AP will become the Master AP and the previous Master AP will be rebooted to become a Member AP, the selected Secondary Preferred Master will become Master once Primary Preferred Master is down. Please note there may be a brief network disruption when changing Master AP.

Primary Preferred Master: Office[R750 - 70:ca:97:01:63]

Secondary Preferred Master: No Preference

Disable WLAN service on Master AP If the Unleashed Network contains 3 or more connected APs, the Master AP will not provide WIFI service

Apply

Switch Approval

Approval Automatically approve all join requests from switches.

Apply

Email Server

Enable Email Server

From Email Address

SMTP Server Name

SMTP Server Port

SMTP Authentication Username

SMTP Authentication Password

Confirm SMTP Authentication Password

SMTP Encryption Options

Test Apply

Chapter 4 - Backup and Firmware

- Backup Configuration
- How to do a Firmware Upgrade

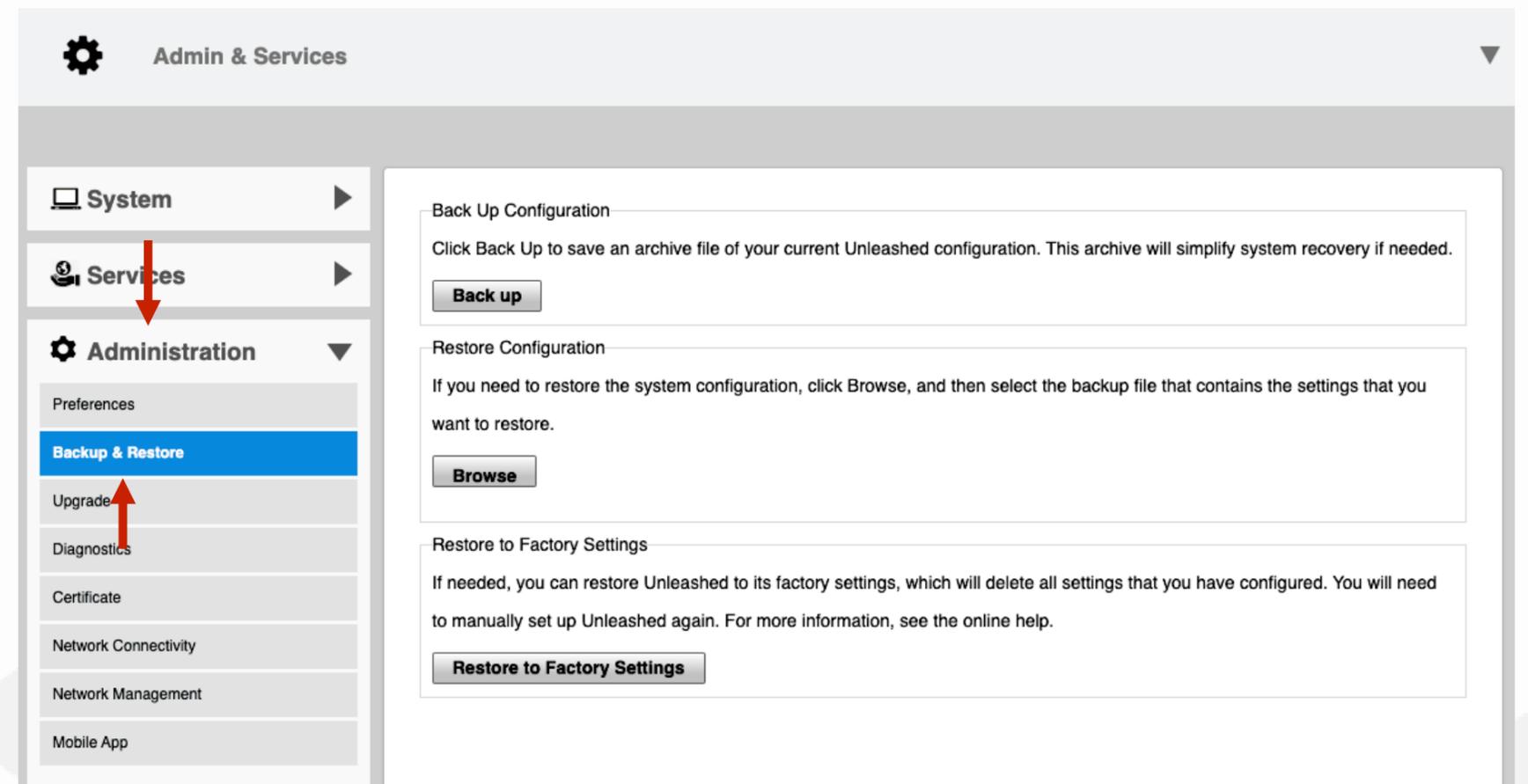
Chapter 4 - Backup and Firmware



Backup Configuration

After configuring the Management Interface, creating a Guest Network with Advanced Guest Network Isolation, ensuring the best possible performance settings, adding APs, and claiming the Preferred Master. Its now time to save your work by creating a backup.

Click on the “Administration” tab to reveal ”Backup and Restore”.



Chapter 4 - Backup and Firmware

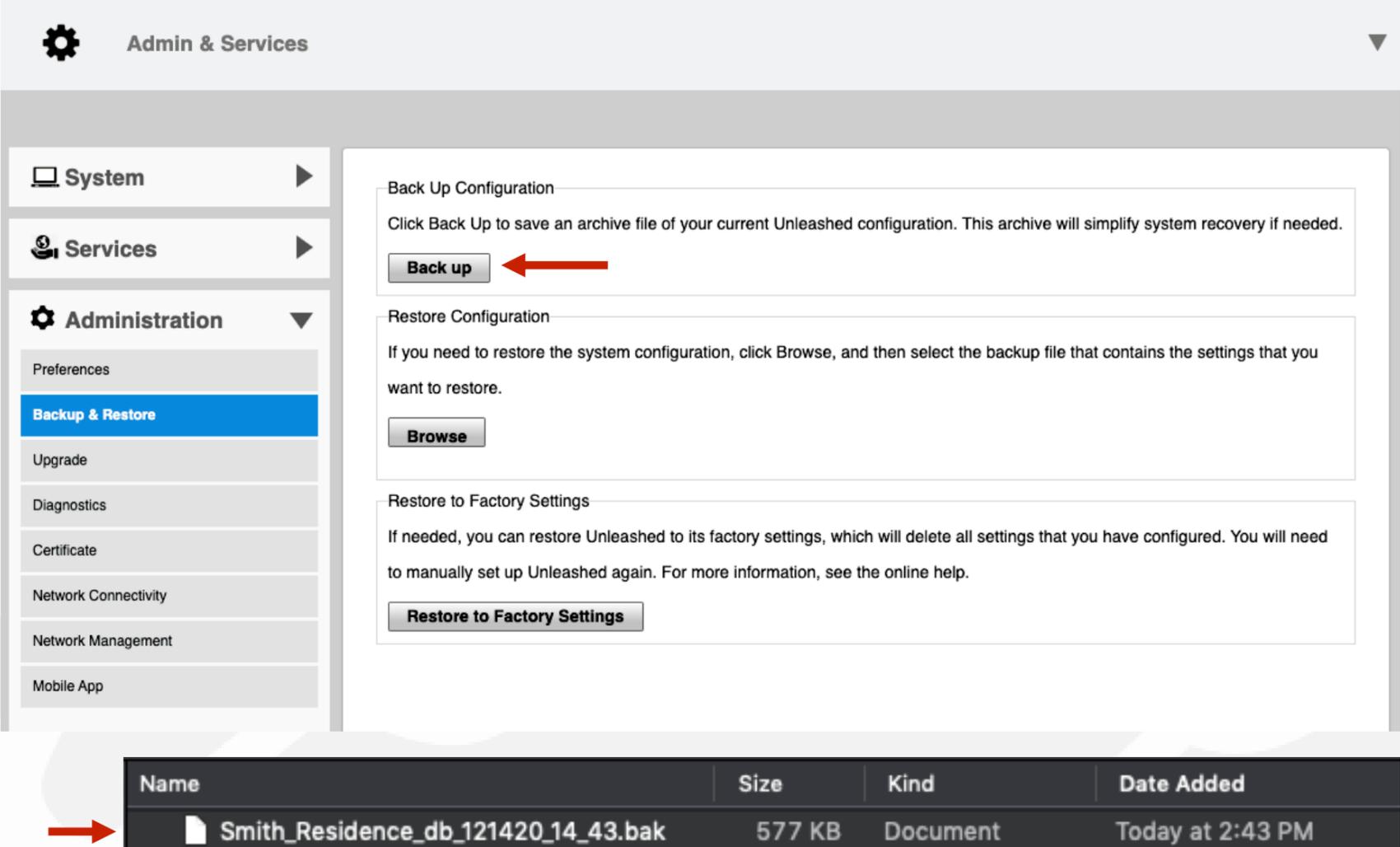
Backup Configuration

Select the "Backup" button.

This will create a back up file in your computer's "Downloads" folder with the following naming convention - "Project_Name_db_date_time.bak".

Move the backup file to an easy to find location for future use.

***Note - It's best practice to always backup any changes to the system. That way you can revert or restore as needed.**



The screenshot shows the 'Admin & Services' interface. On the left, the 'Administration' menu is expanded to 'Backup & Restore'. The main content area has three sections: 'Back Up Configuration' with a 'Back up' button (highlighted by a red arrow), 'Restore Configuration' with a 'Browse' button, and 'Restore to Factory Settings' with a 'Restore to Factory Settings' button. Below the interface, a table lists the backup file:

Name	Size	Kind	Date Added
 Smith_Residence_db_121420_14_43.bak	577 KB	Document	Today at 2:43 PM

Chapter 4 - Backup and Firmware

Firmware Upgrade

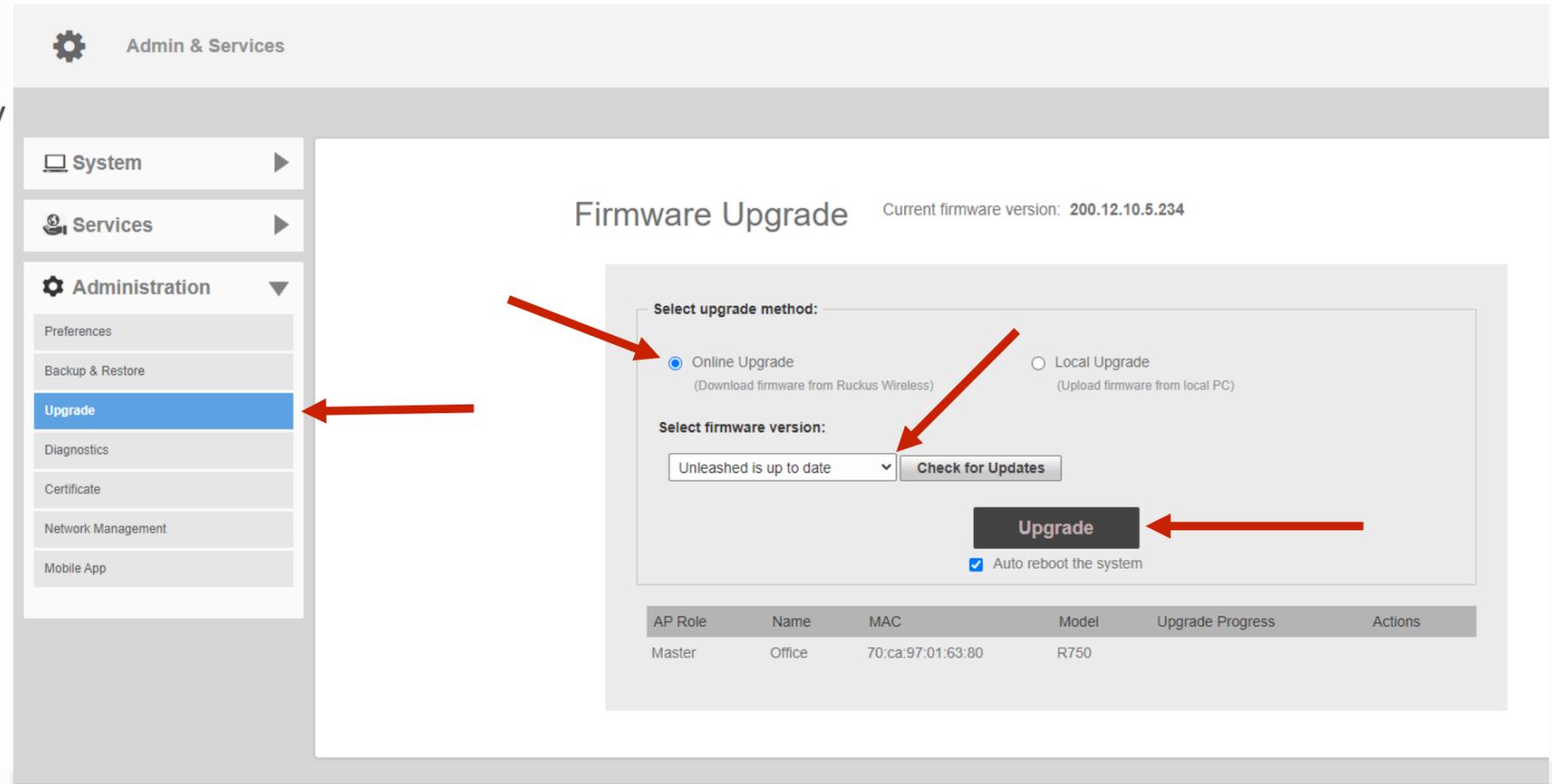
The last step in the configuration process is to verify that the firmware is current.

Select "Upgrade" on the left menu.

Click on "Online Upgrade" to continue.

Select the drop-down arrow to display the list of available upgrade options for your installation and choose the best version for your deployment.

Click on "Upgrade" if there's a new firmware available. After upgrading to a new version of firmware it is always recommended to immediately perform a new backup.



Admin & Services

System

Services

Administration

Preferences

Backup & Restore

Upgrade

Diagnostics

Certificate

Network Management

Mobile App

Firmware Upgrade

Current firmware version: 200.12.10.5.234

Select upgrade method:

Online Upgrade
(Download firmware from Ruckus Wireless)

Local Upgrade
(Upload firmware from local PC)

Select firmware version:

Unleashed is up to date

Auto reboot the system

AP Role	Name	MAC	Model	Upgrade Progress	Actions
Master	Office	70:ca:97:01:63:80	R750		

For more information on the different methods of performing upgrades for an Unleashed deployment, please refer to the File Management Guide that can be found here - <https://my.accessnetworks.com/kb/unleashed-standard-configuration-guides/>.

BASIC CONFIGURATION GUIDE Guide Firmware Version 200.12

- Access Networks Technical Services engineers are always available to assist you in the troubleshooting process.
- If you have any questions about the steps to follow on setting up your Unleashed Network or have an issue than what has been detailed in this presentation, please contact the Access Networks Technical Services department for assistance.
- For telephone, visit snp1.com/techsupport
- Email: support-case@accessnetworks.com
- Existing Access Networks partner can visit <https://my.accessnetworks.com/partners/> and either open a case or start a chat session by selecting the “Support” tab.

THANK YOU

CONTACT INFO

PHONE

661.383.9100

ADMINISTRATION

28482 Constellation Rd.
Valencia, CA 91355
accessnetworks.com

EMAIL

clientservices@accessnetworks.com