

RUCKUS Unleashed 200.16 Troubleshooting Guide

Supporting Release 200.16

© 2024 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMScope DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMScope, COMMScope AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMScope HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see <https://www.commscope.com/trademarks>. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

About This Guide.....	4
Introduction.....	4
Reporting an Issue.....	4
Troubleshooting.....	4
Initial Deployment Considerations.....	4
Master AP Election.....	7
Troubleshooting Dedicated Master AP.....	10
Troubleshooting the Gateway Feature.....	14
Performing Firmware Upgrades.....	17
Troubleshooting Client Authentication Issues.....	19
Client Connection Troubleshooting.....	21
Wireless Mesh Considerations.....	23
Using the Management Interface.....	25
Configuring DHCP Service.....	26
General Configuration Questions.....	29
Debugging.....	31
Understanding LED Behavior.....	36
Built-In Memory Diagnostic Tool.....	37

About This Guide

Introduction

The *RUCKUS Unleashed Troubleshooting Guide* provides basic troubleshooting information for diagnosing common issues with RUCKUS Unleashed APs and RUCKUS Unleashed networks.

For users who are already familiar with RUCKUS ZoneDirector systems, the RUCKUS Unleashed troubleshooting methods are generally similar. Where they are different, this guide provides details on the differences.

This guide contains a collection of common questions and answers about RUCKUS Unleashed network deployments. Common issues include initial deployment issues, Master AP selection and election issues, using the Gateway feature, upgrading the network, mesh-related issues, and DHCP-related issues.

Reporting an Issue

If a customer experiences an issue with their RUCKUS Unleashed network, they can first seek advice from other RUCKUS Unleashed users on the **RUCKUS Unleashed Forums**:

<https://community.ruckuswireless.com/t5/Unleashed/bd-p/unleashed>

Customers with a valid support contract can look for answers to many questions in the RUCKUS Support Knowledge Base:

https://support.ruckuswireless.com/answers/search?article_id=&query=Unleashed

If the Support Forums and Knowledge Base are unable to provide a solution, customers with a valid support contract can submit a support ticket request for further assistance to Technical Support through the RUCKUS Support website:

<https://support.ruckuswireless.com/contact-us>

When reporting an issue, please provide the following information:

- Release version number
- AP models
- Description of the client device having issues connecting or accessing the RUCKUS Unleashed network (PC, web interface, mobile app, and so on)
- Specific steps that led to the situation
- In most cases, the debug information of the Master AP would be helpful for problem analysis (from the RUCKUS Unleashed dashboard, select **Admin & Services > Administer > Diagnostics > Debug Info**)

Troubleshooting

Initial Deployment Considerations

Q: I just received my RUCKUS Unleashed APs. How do I set up my RUCKUS Unleashed network?

A: You can configure one AP as your initial Master AP by following any of the three following options. Once the RUCKUS Unleashed Master AP is configured, simply connect other RUCKUS Unleashed APs to the same network and they will automatically become member APs and form your RUCKUS Unleashed network.

NOTE

You may want to first make sure the Master AP is running the latest firmware before adding additional member APs, to save time upgrading the whole network after the member APs are connected.

Use any of the following options to configure the initial Master AP:

Option 1: Using a Wi-Fi client device

As soon as the AP boots up and is connected to a local network, it begins broadcasting a temporary unencrypted WLAN with an SSID named Configure.Me-xxxxxx on both radios. The "xxxxxx" is the last 3 octets of the MAC address of the AP.

1. Using your wireless client's Wi-Fi configuration settings, select and associate to the Configure.Me-xxxxxx WLAN.
2. Launch a web browser and browse to any web page. You will be automatically redirected to unleashed.ruckuswireless.com.

NOTE

For Unleashed release 200.5 and later, you can enter any domain name.

3. The browser will be redirected to the RUCKUS Unleashed Setup Wizard. Follow the instructions to configure your initial RUCKUS Unleashed network.

Option 2: Using a wired client device

If you have some way to learn the RUCKUS Unleashed AP's IP address, or are able to discover the RUCKUS Unleashed AP on your Microsoft Windows network using UPnP, or Apple Mac OS network using Bonjour discovery, you can set up the RUCKUS Unleashed network using a wired client using the following procedure:

1. Connect the client device to the same network as the RUCKUS Unleashed AP with an Ethernet cable. Make sure the client can ping the AP's IP address.
2. Launch a web browser and enter the IP address of the RUCKUS Unleashed AP, and press **Enter**.
3. The browser screen will be redirected to the RUCKUS Unleashed Setup Wizard. Follow the instructions to configure your initial RUCKUS Unleashed network.

NOTE

You may be able to find the RUCKUS Unleashed AP's IP address by checking your DHCP server's leased address list. For Unleashed 200.5 and later releases, UPnP and Bonjour services are enabled in an RUCKUS Unleashed AP when it is in factory default state. Windows devices can detect RUCKUS Unleashed APs on the Window Network. Apple devices can detect the RUCKUS Unleashed AP using Bonjour service by searching for the service type `_ruckus-unleashed._tcp`.

Option 3: Using the RUCKUS Unleashed mobile app on a mobile device

Install the RUCKUS Unleashed mobile app on your mobile device, open the app, select **Typical Install**, and follow the instructions.

Q: My Wi-Fi device successfully connects to Configure.Me_xxxxxx WLAN but the device cannot reach the RUCKUS Unleashed AP's web UI. What should I do?

A: The RUCKUS Unleashed AP provides DHCP service on the Configure.Me_xxxxxx WLAN, therefore the connected client is expected to receive a dynamically assigned IP address automatically. If the client device is configured to use a static IP address (either configured for this WLAN or for a different WLAN), the client device may be unable to connect to the RUCKUS Unleashed AP. The easiest way is to configure the client's Wi-Fi interface to obtain a dynamic IP address from DHCP.

Troubleshooting

Initial Deployment Considerations

NOTE

Note that different Unleashed AP releases offer IP addresses in different ranges, as shown in the following table. If the wireless device cannot receive an IP address, an alternative is to statically set the IP address to be in the same subnet as the AP, allow the device to connect to the AP, and then proceed with setup troubleshooting steps. Another potential cause of network issues is if the local wired network happens to be in the same subnet as the AP's WLAN IP subnet.

TABLE 1 Unleashed IP Addresses as Per Release

Unleashed Release	AP's WLAN Interface IP Address	Client IP Address Range	Remarks
200.0	192.168.101.1	192.168.101.31~.253	The LAN network IP addresses cannot overlap with 192.168.101.1/24, otherwise network reachability issues can occur.
200.1, 200.2, 200.3	169.254.1.1	169.254.1.31~.253	Some Apple devices (incl. iPhone and iPad) don't work well with IP addresses assigned in this subnet. Therefore, the Unleashed Mobile App on these devices may encounter errors when setting up an Unleashed network.
200.4 and later	10.154.231.125	10.154.231.130~.180	Under the assumption that this address most likely will not overlap with customers' LAN IP assignment.

Q: My device can access the web interface, but it fails in running the Setup Wizard. What can I do?

A: Try to access the web interface again or set the AP to the factory default state and restart the initialization process. If the process continues to fail, follow the guidelines in Reporting an Issue to contact RUCKUS Support.

Q: Do all member APs need to be upgraded to join a Master AP that is running a different RUCKUS Unleashed image version?

A: Yes, the member APs must be upgraded to the same version as the Master AP to form a RUCKUS Unleashed network. In most cases, in most cases you can connect the member APs to the same subnet as the Master AP, and as long as the RUCKUS Unleashed Master AP can reach the RUCKUS firmware image server, firmware upgrades for all connected APs will be performed automatically.

Q: I have multiple Unleashed APs that potentially can have different image versions installed. How do I check their version numbers and perform the firmware upgrades before installation to avoid any potential problems?

A: Before running the Unleashed setup, you can connect to the AP via SSH and run the following CLI commands:

- To check AP version: `get version`.
- To upgrade an image from the AP CLI, one easy way is to load the AP image onto a TFTP server, and then use the following commands:
 - `fw set control <image file name>`
 - `fw set proto tftp`
 - `fw set host <TFTP server address>`
 - `fw update`
 - `reboot`

Q: I have an Unleashed Network running already and plan to add a new AP to the network. However, the new AP doesn't seem to be able to join the existing Unleashed Network. What should I do?

A: If the new AP is loaded with the same firmware version as the existing Unleashed Master AP, but the new AP cannot be seen on the Master AP's web UI, the issue is most likely caused by one of the following reasons:

- The new AP failed to receive a valid IP address. Check your DHCP server.
- The new AP is connected to a different network from the existing Unleashed network. Make sure the AP is connected to the same subnet as the existing Master AP.
- The new AP already has configuration on it. In this case, factory reset the AP by using a pin to push into the "Reset" hole for 10 seconds while the AP is powered on.

- The total number of APs in the Unleashed network has reached its maximum. As of release 200.8, the maximum number of supported APs is 128 (this applies to 802.11ac wave 2 and 802.11ax APs only).

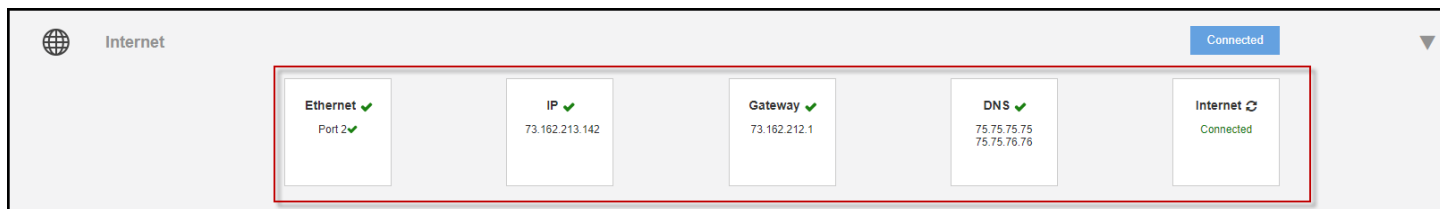
If the new AP is loaded with a different Unleashed image, the Unleashed Master AP will try to upgrade the new AP's firmware to match that of the Master using images stored on the RUCKUS firmware server. In this case, you should check the following:

- Ensure that the AP model of the new AP is supported by the version that the Master AP is running. If not, you will need to upgrade the existing Unleashed Network first, for the new AP to participate.
- Ensure that the Master AP can reach the RUCKUS image server so it can locate the appropriate image and instruct the new AP to install it.
- Alternatively, download the desired AP image onto an administrative PC and upgrade the new AP image by using AP CLI in an SSH session.

Q: How do I check whether the Unleashed Master has a connection to the Internet?

A: Beginning with Unleashed 200.6, the top component on the Dashboard, "Internet," can be expanded to display the Ethernet port status, IP address, gateway and DNS servers, and Internet connection status.

FIGURE 1 Internet Tab

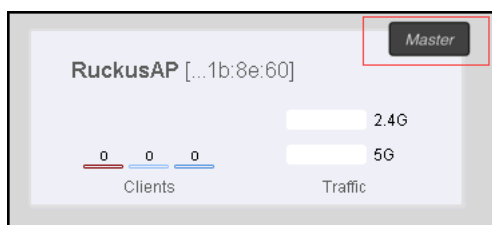


Master AP Election

Q: How do I identify which AP is the Master AP?

A: The CTL LED of the Master AP is solid green at all times. On the RUCKUS Unleashed web interface, the Master AP box is labeled as the Master in the upper-right corner, as shown in the following figure. The RUCKUS Unleashed mobile app provides a similar icon to denote the Master AP.

FIGURE 2 Identifying the Master AP



Q: Is it possible to force RUCKUS Unleashed AP to become a member AP?

A: Yes, an AP can be set to never become a Master using the AP CLI. To configure an AP to always assume the role of member, SSH to that AP and issue the following AP CLI command:

```
set election role 1
```

To clear the setting, use the following AP CLI command:

```
set election role 0
```

FIGURE 3 Using the Set election role Command

```
rkscli: set election
Error: parameter error
Usage: set election {options}
    -> debug <1=ERROR 2=WARN 4=INFO 8=DEBUG>
    -> role <0=Clear 1=Member>

rkscli: set election role 1
Fix role set ok
OK
```

Q: Is it possible to designate a specific RUCKUS Unleashed AP as the Master AP?

A: Starting with release 200.5, you can configure an AP to be the "preferred Master." Prior to release 200.5, the only option was to set all other APs as member APs using CLI command. By default, without any specific configuration, RUCKUS Unleashed APs automatically elect the most appropriate AP to be the Master AP.

Q: What happens if the Master AP is disconnected or goes down?

A: After the member APs fail to connect to the Master AP for 30 seconds, the election mechanism begins and a new Master AP is elected. During this period of time, existing wireless clients may remain connected, but no new clients can associate with the WLAN.

The exception is if the Gateway function is enabled (only possible on the Master AP). In this case, Master AP election will not happen because the Gateway AP needs a physical WAN connection and no other APs can automatically replace it.

Q: When the Master AP is disconnected, how long will it take for the RUCKUS Unleashed network to resume operation?

A: WLAN service is impacted for about 80 seconds, but the member APs will experience WLAN downtime for only a few seconds.

After member APs lose connection to the Master AP for 30 seconds, the new Master AP election begins. Afterwards, member APs will join and receive configuration from the new Master AP. The process takes about 40 seconds. However, even if a member AP loses its connection to the Master AP, the existing WLAN service continues, although new clients will not be authenticated during this period of time. When a new Master AP is elected, member APs will experience WLAN downtime for a few seconds before normal operation resumes.

Q: Will the old configuration be lost if the Master AP is disconnected from the network?

A: No. For Unleashed 200.2 and later releases, all member AP's keep a copy of the configuration, and when a new AP is elected as the master, it restores the configuration from this copy.

In Unleashed 200.0 and 200.1 releases, the Standby Master AP stores the configuration, and it may take the Master AP role if it loses connection to the Master AP.

Q: What are the Master AP election criteria?

A: Master AP election factors include the following criteria:

- Initial setting (the first AP that is configured to be the Master AP)
- Manually configured preference (supported in 200.5 and later release)
- Configured as member AP only by AP CLI command
- Processing power of the AP model
- Free memory size
- Mesh role (only a Root AP of the Mesh network can be a Master AP)
- If Mesh is enabled, the number of downlink Mesh nodes (the fewer the downlink Mesh nodes, the higher the chance to be the Master AP)
- AP system uptime (the longer the uptime, the higher the chance to be a Master AP)
- MAC address as the last arbitrator

Q: Can a Mesh AP be elected as the Master AP?

A: No, a Mesh AP, which has no Ethernet connection for uplink, cannot assume the role of the Master AP.

Q: I cannot see any RUCKUS Unleashed web interface displayed in my browser. It seems there is no AP assuming the role of RUCKUS Unleashed Master AP. How do I investigate the situation?

A: Make sure the administrative PC is connected to a RUCKUS Unleashed SSID), and enter the following URL in your browser: <https://10.154.231.125:9090>. You should be redirected to the RUCKUS Unleashed web interface.

Note that if mesh is enabled on your network, only Root APs (that is, APs connected to the Internet through a wired interface) can become the RUCKUS Unleashed Master AP. One of the criteria to become the Root AP is that an AP can contact its gateway through a wired interface. Therefore, if your default gateway of your network becomes unreachable, none of the RUCKUS Unleashed APs can become the Root AP of the Mesh network, and there will be no RUCKUS Unleashed Master AP on your network. The exception to the above is when the **gateway** function is enabled; in this case the Gateway AP is the Master AP regardless of whether mesh is enabled, or whether its gateway is reachable or not.

If the Root AP problem does not apply to your situation, find the IP address of any of the APs and enter "http://<any AP IP address>" in your web browser to access the web interface.

If there continues to be no response (despite knowing the IP address of one of the APs), you can use SSH into the AP to connect to the AP, and perform the following actions:

- Enter the **get election** AP CLI command. The output shows the status of all RUCKUS Unleashed APs and should display one APs as **Master**. Ping the IP address of the Master AP from a device connected to the same network. If the AP is not reachable, there may be an access denial policy configured in one of your devices on your network. If the AP responds to the ping, enter the IP address of the AP in your web browser and check whether the RUCKUS Unleashed web interface is displayed

FIGURE 4 Using the get election Command

```
rksc11:
rksc11:
rksc11: get election
The local AP's ip address is 172.18.171.3, Election role is master, Fix role is NO, Debug level is ERROR
mac_address ipaddress role configID station_rate free_memory mesh_enabled mesh_node mesh_node_type model version bak_version system
board_type last_seen
-----
F0:b0:52:39:ce:20 172.18.171.3 master 37 48 149868 0 0 R500 200.5.10.0.20 200.2.9.13.186 2596 zf7752-3-29-4bss Thu Mar 16 10:35:20
2017
d4:68:4d:25:86:70 172.18.171.15 member 37 48 164936 0 0 R500 200.5.10.0.20 200.3.9.13.14890424 0 zf7752-3-29-4bss Thu Mar 16 10:3
5:18 2017
OK
```

- If Mesh is enabled, enter the **get mesh** command to check the Mesh status. Only an AP in "ROOT" Mesh mode can be the Master AP.
- If everything looks correct, but the network still does not appear to show an AP assuming the Master AP role, you may require help from RUCKUS Support. Follow the guidelines in Reporting an Issue to contact RUCKUS Support.

Q: What happens if a disconnected Master AP is reconnected back to the network after a new Master AP has been elected?

A: The two Master APs will communicate with each other to elect one AP to serve as the Master AP, and the other AP will become a member AP and join the master AP.

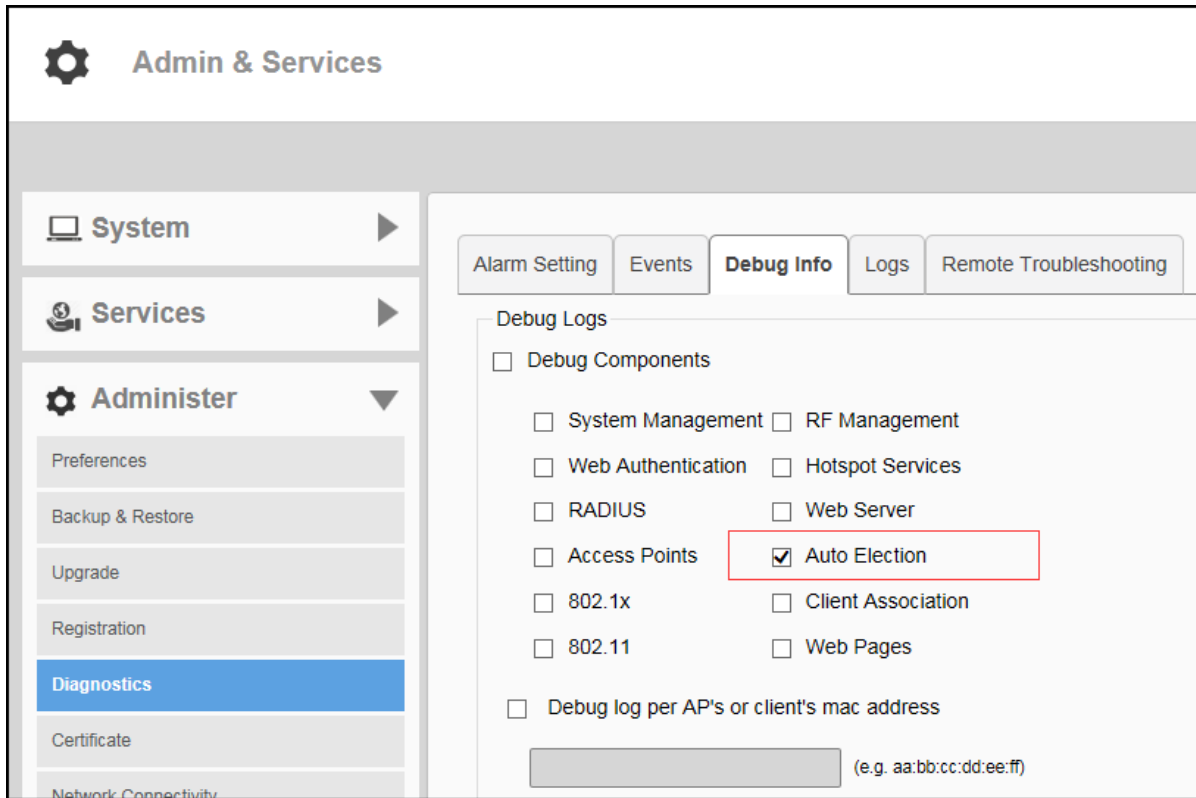
Q: How do I enable debugging logs for Master election?

A: From the RUCKUS Unleashed dashboard, select **Admin & Services > Administer > Diagnostics > Debug Info**, and select the **Auto Election** check box.

Troubleshooting

Troubleshooting Dedicated Master AP

FIGURE 5 Selecting Auto Election



Alternatively, use SSH to connect to a RUCKUS Unleashed AP and manually turn on election log debugging on that particular AP using the **set election debug** command.

In the example, X is a number representing the debug level: 1 shows messages only in case of error, and 8 generates all messages for debugging purposes.

FIGURE 6 Using the set election debug 8 Command to General All Messages

```
rksccli: set election
Error: parameter error
Usage: set election {options}
       -> debug <1=ERROR 2=WARN 4=INFO 8=DEBUG
       -> role <0=Clear 1=Member>

rksccli:
rksccli: set election debug 8
Debug level set ok
OK
```

Troubleshooting Dedicated Master AP

Q: I just received my RUCKUS Unleashed APs. How do I set up Dedicated Master mode?

A: Dedicated Master mode is supported only for the R750 AP or R850 AP. You can select the **Dedicated Master** option in the **System** page of the Unleashed Setup Wizard. After the setup is complete, the AP will run as the Dedicated Master.

FIGURE 7 Enabling the Dedicated Master: Setup Wizard

The screenshot shows the 'Unleashed Setup Wizard' interface. At the top, it displays 'Version: 200.13.6.1.275'. Below this are several configuration fields:

- Name:** A text input field containing 'Ruckus-Unleashed'. A note to the right states: 'Name your system 32 characters max using alphanumeric characters excluding space.'
- Country Code:** A dropdown menu set to 'United States'. A note to the right states: 'Select the regulatory country code for the Unleashed Network.'
- Mesh:** A checked checkbox. A note to the right states: 'Select this check box to enable Mesh for the Unleashed Network.'
- Mesh Name (ESSID):** A text input field containing 'Mesh-461902002437-694'. A note to the right states: 'Each mesh-enabled Unleashed requires a unique name(SSID) for the mesh WLAN for the backbone traffic.'
- Mesh Passphrase:** A text input field containing 'T-ESIDnEDPuaQsv9dRKNS' and a 'Generate' button.
- Dedicated Master:** An unchecked checkbox, which is highlighted with a red rectangular border. A note to the right states: 'Select this check box to enable Dedicated Master for the Unleashed Network. The radio function of Dedicated Master AP will be disabled and Wi-Fi service cannot be provided.'

You can configure Dedicated Master using one of the following methods.

Option 1: Using a Wi-Fi client device

After the Unleashed AP boots up and is connected to a local network, the AP begins to broadcast a temporary unencrypted WLAN with an SSID named Configure.Me-xxxxxx on both the radios. The "xxxxxx" is the last 3 octets of the MAC address of the AP.

1. Using the Wi-Fi configuration settings of your wireless client, select and associate to the Configure.Me-xxxxxx WLAN.
2. Launch a web browser and browse any web page.

You are automatically redirected to unleashed.ruckuswireless.com.

NOTE

For Unleashed 200.5 and later, you can enter any domain name.

The browser is redirected to the Unleashed Setup Wizard. Follow the on-screen instructions to configure your initial Unleashed network.

Option 2: Using a wired client device

If you have some way of getting the IP address of the Unleashed AP or if you can discover the Unleashed AP on your Microsoft Windows network using UPnP or the Apple Mac OS network using Bonjour discovery, you can set up the Unleashed network using a wired client using the following procedure.

1. Connect the client device to the same network as the Unleashed AP with an Ethernet cable. Make sure the client can ping the IP address of the AP.
2. Launch a web browser, enter the IP address of the Unleashed AP, and press **Enter**.

The browser is redirected to the Unleashed Setup Wizard. Follow the on-screen instructions to configure your initial Unleashed network.

NOTE

You may be able to find the IP address of the Unleashed AP by checking the leased address list of your DHCP server. For Unleashed 200.5 and later releases, UPnP and Bonjour services are enabled in an Unleashed AP when it is in the factory default state. Windows devices can detect Unleashed APs on the Windows network. Apple devices can detect the Unleashed AP using Bonjour service by searching for the service type: _ruckus-unleashed._tcp.

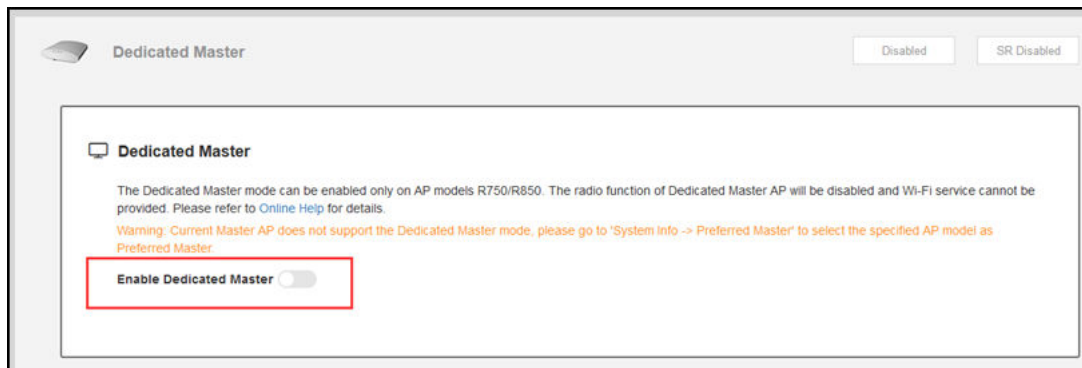
Q: My Unleashed network runs in bridge mode, but how do I change it to Dedicated Master mode?

A: After the upgrade of your Unleashed network to Unleashed 200.13, go to the **Dedicated Master** component in the Unleashed dashboard and click the **Enable Dedicated Master** option. Your Unleashed network changes to Dedicated Master mode after reboot.

Troubleshooting

Troubleshooting Dedicated Master AP

FIGURE 8 Enabling the Dedicated Master: Unleashed Dashboard



NOTE

The **Enable Dedicated Master** option can be enabled only when the Master AP is an R750 AP or an R850 AP. Make sure the current Master of your Unleashed network is an R750 AP or R850 AP.

NOTE

After the R750 AP or R850 AP is enabled for Dedicated Master mode, the AP works in a fixed controller mode without having any AP-specific radio parameter settings. If you want to recover AP radio function, you must reset the AP to factory settings.

Q: How does a member AP join the Dedicated Master?

A: After the Dedicated Master is set up, a member AP can join Dedicated Master by following any of the following three methods:

- Power on the member AP in the same network as the Dedicated Master.
- If a member AP and the Dedicated Master are in different IP subnets, you can add Option 43 for the DHCP server in the member AP subnet and add the Dedicated AP list in optionruckus_info.zdiplist.

```
#Ruckus Option 43 configuration as below:
option space ruckus_info;
option ruckus_info.zdiplist code 3 = text;
vendor-option-space ruckus_info;
option ruckus_info.zdiplist "10.223.26.121";
```

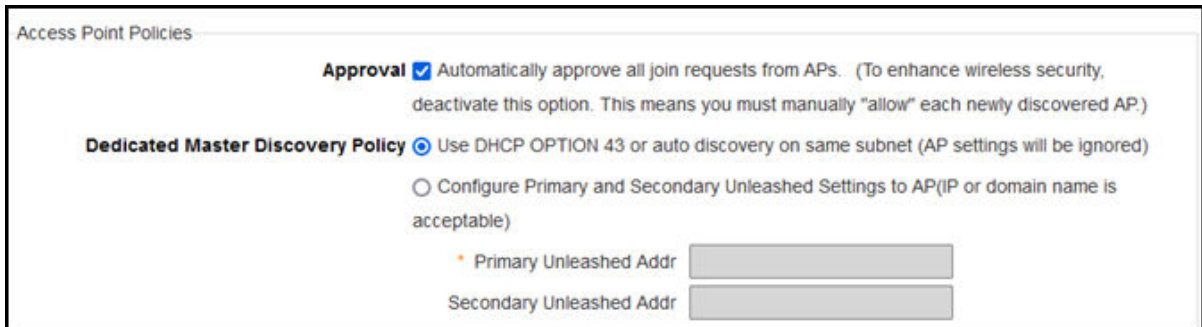
- Set the Dedicated Master IP address in the member AP CLI.

```
rkscli: set director ip 192.168.80.13 192.168.80.8
** Please reboot for this change to take effect
OK
```

NOTE

By default, the member AP is kept in the pending status. You must manually approve the member AP to join the Dedicated Master or go to **Admin & Services > System > System Info** to edit the configuration and auto-approve the AP that joins the Dedicated Master.

FIGURE 9 Auto-Approving an AP to Join the Dedicated Master



Q: How do I upgrade a mismatched member AP in the Dedicated network?

A: Dedicated Master supports the upgrade of mismatched member APs automatically. Go to **Admin & Services > Administration > Upgrade**, and select **Local Upgrade** to preload the same firmware version image as the Dedicated Master. Preloading of up to four AP model images to the Dedicated Master is supported. Connect the mismatched AP to the Dedicated Master, and the AP will upgrade automatically.

Q: Is migration of a ZoneDirector AP to the Dedicated Master network supported?

A: Yes, the migration of a ZoneDirector AP to the Dedicated Master network is supported. Refer to the *RUCKUS ZoneDirector AP Migration to Unleashed Network User Guide*.

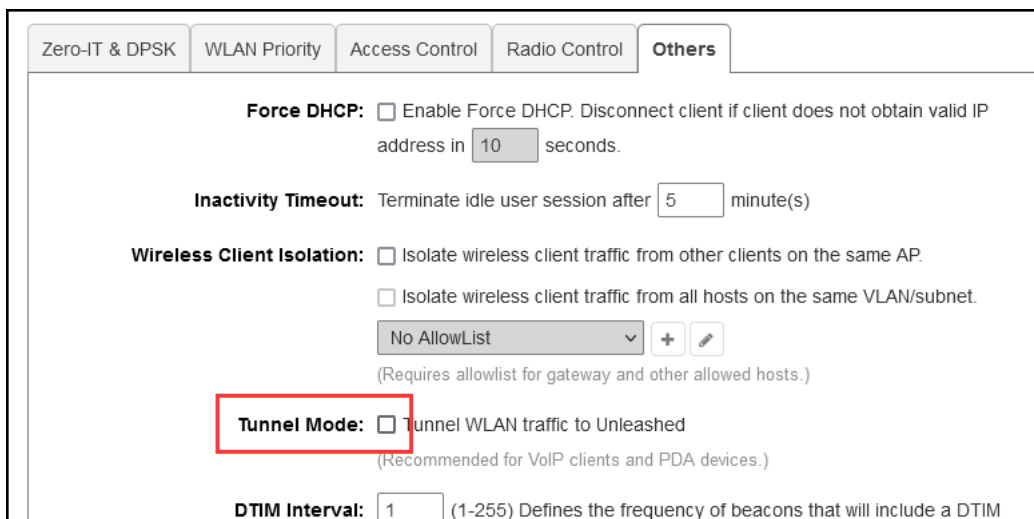
Q: Does Dedicated Master support more number of clients and APs than Unleashed bridge mode?

A: Dedicated Master mode supports a maximum of 4,000 clients (only 2,048 with Unleashed bridge mode). There is no change in the number of APs supported.

Q: Does Dedicated Master mode support Tunnel configuration, and how do I enable Tunnel mode?

A: Yes, Dedicated Master mode supports Tunnel configuration. From the Unleashed dashboard, go to **WiFi Networks** and select a Wi-Fi network to edit. Click **Show Advanced Options**, select the **Others** tab, and click the **Tunnel Mode** check box.

FIGURE 10 Enabling Tunnel Mode



Q: What happens if the Dedicated Master is disconnected or goes down?

Troubleshooting

Troubleshooting the Gateway Feature

A: All the APs join the Dedicated Master network with the member APs having a fixed role. When a Dedicated Master is down, all member APs continue to run as member APs, and there is no new Master elected.

You can assign a new Dedicated Master to this network or set up one member AP using the Unleashed Setup Wizard after resetting it to factory default settings.

Q: Does Dedicated Master support Smart Redundancy, and how do I set up Smart Redundancy?

A: Yes, Dedicated Master supports Smart Redundancy. Use one of the following methods set up Smart Redundancy:

- Select one member AP (R750 or R850) as the peer Dedicated Master AP.
- Set up two Dedicated Master APs. Enter the IP address of the secondary Dedicated Master and the same secret as the peer Dedicated Master in the **Dedicated Master** component.
-

Q: How do I check the status of the peer Dedicated Master in Smart Redundancy?

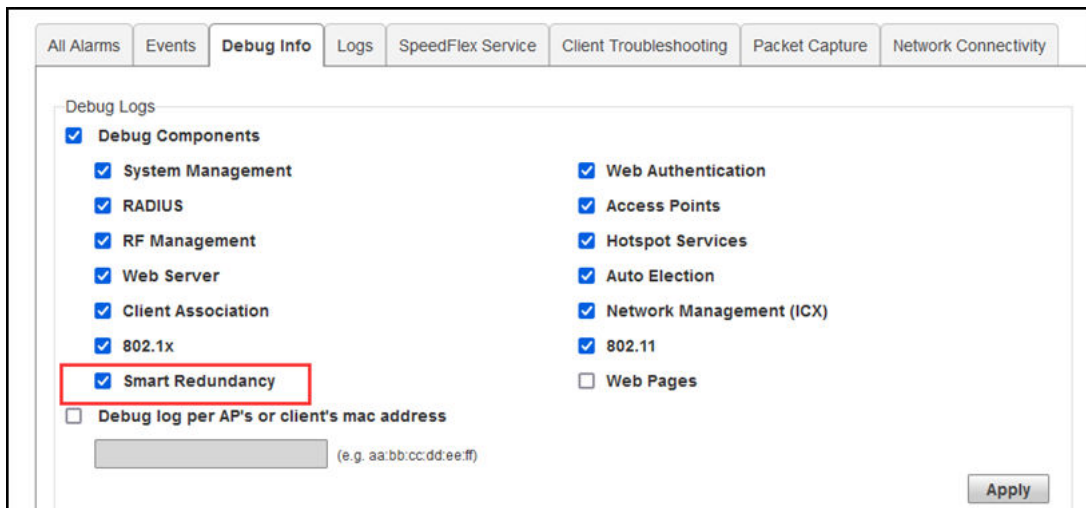
A: You can use the following two methods to check the status of the peer Dedicated Master in Smart Redundancy:

- In the active Dedicated Master dashboard, in the **Dedicated Master** component, you can check the Dedicated Master and peer Dedicated Master information.
- Log in to the peer Dedicated Master web interface to check the status.

Q: How do I enable debugging logs for Smart Redundancy?

A: Go to **Admin & Services > Administration > Diagnostics**, select the **Debug Info** tab, and select the **Smart Redundancy** check box.

FIGURE 11 Enabling Debugging Logs for Smart Redundancy



Troubleshooting the Gateway Feature

Q: How do I setup the Unleashed Gateway Network?

A: There are 2 ways to enable the Gateway feature:

- Option 1: Enable AP Gateway Mode while running the initial **Setup Wizard**:

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

AP Gateway Mode: Disabled Enabled Select WAN Port LAN1

WAN Port IP: Dynamic (DHCP) Static (Manual) PPPoE

* IP Address: 172.18.140.1

* Netmask: 255.255.255.0

* Gateway: 172.18.140.254

Primary DNS Server: 172.18.100.35

Secondary DNS Server: 172.18.100.45

DHCP server: Enabled NAT: Enabled

* LAN Port IP: 10.10.0.1

* LAN Port Netmask: 255.255.0.0

* Starting IP: 10.10.0.2

* Ending IP: 10.10.7.209

Number of IPs: 2000

Lease Time: Twelve hours

- Option 2: From the Dashboard, go to **System > IP Settings** and enable **Gateway Mode**.


Troubleshooting

Troubleshooting the Gateway Feature

Gateway Mode

WAN Selection: PORT 2

LAN & WLAN IP Address: Router IP 10.106.0.1, Netmask 255.255.0.0



WAN IP Address: DHCP (selected), IP Address 192.168.100.141, Netmask 255.255.255.0, Gateway 192.168.100.100, Primary DNS Server 10.10.10.10, Secondary DNS Server

LAN & WLAN Client IP Addresses: Starting IP 10.106.0.2, Ending IP 10.106.7.209, Number of IPs 2000, Lease Time Twelve hours

Q: On the Gateway AP, can I configure more than one port to be the WAN port?

A: No. Only one Ethernet port can be configured as the WAN (wide area network) port for the unleashed gateway.

NOTE

Only the H350 AP and the H550 AP support dual WAN ports, where one Ethernet port is configured as the active WAN port and the other Ethernet port is configured as the standby WAN port for the Unleashed gateway. At any given point, only one Ethernet port acts as the active WAN port. The traffic moves through the active WAN port. If the active WAN port fails, the traffic is automatically switched to the standby WAN port until the active WAN port recovers.

Q: Once a gateway AP is configured, can I choose a different Unleashed AP to be the Gateway AP?

A: No. The Gateway AP has to be the Master AP, and one Ethernet port should be configured as the WAN port, which acts as the backhaul link for the Unleashed network.

Q: If the Gateway (and Master) AP is down, how do I recover the network?

A: In 200.3 and 200.4 releases, if the Gateway/Master AP is out of service, the user should pick a member AP to serve as the Gateway AP, reset it to factory defaults, and re-configure it as the new Master/Gateway AP.

With release 200.5 and later, a new recovery mechanism has been introduced: If the Master/Gateway AP fails for any reason, the customer can use an existing Member AP to replace the previous Master AP. To do so, connect the previous Master AP's Ethernet cable to this member AP and allow it to set up the desired network topology. This member AP will become the new master after 3 minutes automatically, and will establish an Unleashed network with all of the previous configuration settings.

Q: My AP only has one Ethernet port. Can it be used as a Gateway AP?

A: Yes, APs such as R310 and T300 that have only one Ethernet port can also be configured in Gateway mode. If mesh is supported on the AP model (such as the T300 series), the AP can also be the gateway for any wired or wireless clients of any downlink mesh APs. The R310 does not support mesh, so it will be unable to serve as a Root AP, and would therefore only be able to service Wi-Fi clients, in this scenario.

Q: Should the DHCP Server function be enabled on the Gateway AP?

A: Yes, the internal DHCP server must be enabled on the Gateway AP. The Gateway AP provides IP addresses for all APs and clients.

Q: How is the IP address of the Gateway AP's WAN interface assigned?

A: There are 3 ways to assign the IP address of a Gateway AP's WAN port:

- By an external DHCP server.
- Manually configured.
- By an external PPPoE server.

NOTE

For APs H350 and H550, the IP address of the Gateway AP's standby WAN interface is assigned by DHCP or manual configuration.

Q: Can a Member AP join the Gateway/Master AP through the WAN port of the Gateway/Master AP?

A: No. A member AP can only join a Gateway/Master AP from the Gateway/Master AP's LAN port, and there should be only one Unleashed network in one IP subnet.

In 200.3 and 200.4 releases, this topology restriction is not enforced; that is, a customer can still set up such an unsupported topology.

Starting from release 200.5, the LWAPP service is disabled on the WAN port of the Gateway AP. Therefore, all discovery packets coming from a Member AP will be ignored on the Gateway/Master AP.

In either case, the "outer" AP may assume the Master role and cause the Unleashed UI to display confusing information.

Q: Can I set WAN and LAN addresses of the Gateway AP to be in the same subnet?

A: No, the IP address range of the WAN network and the IP address range of the LAN network cannot overlap with each other.

Q: If Gateway mode is enabled, how is the IP addresses assignment accomplished for APs and clients?

A: All Member APs and clients obtain their IP addresses from the Gateway/Master AP's internal DHCP server.

Q: How do I investigate issues with Member APs or clients failing to receive an IP address?

A: Check the following:

- Ensure that the Gateway feature is enabled and the DHCP service is properly configured.
- Check that the client is configured to use a DHCP-assigned IP address.
- Capture all DHCP packets to better understand the root cause.

Q: Can mesh be enabled while Gateway mode is enabled?

A: Yes. Mesh is supported in gateway mode with the caveat that, in 200.3 and 200.4 releases, if PPPoE is enabled, mesh can be enabled, but the Master AP itself won't enable its mesh downlink. All member APs can serve mesh normally. This restriction is removed in 200.5 and later releases.

Performing Firmware Upgrades

Q: When should I use online upgrade and when should I use local upgrade to upgrade my system?

A: Online upgrade is the recommended way to upgrade the RUCKUS Unleashed network. However, it requires the RUCKUS Unleashed network to be able to reach to the RUCKUS Image server.

Troubleshooting

Performing Firmware Upgrades

Local upgrade can be useful in some situations, including:

1. No or very limited Internet access from the RUCKUS Unleashed network.
2. For some reason a special image version is needed, which is not included in the supported online upgrade images.

Q: How do I know which firmware versions are available for online upgrade?

A: On the RUCKUS Unleashed web UI, go to **Administer > Upgrade**, you will see a version dropdown list.

Current firmware version 200.2.9.13.14685531.

Select upgrade method:

Online Upgrade (Download firmware from Ruckus Wireless) Local Upgrade (Upload firmware from local PC)

Select firmware version:

200.2.9.13.100

Upgrade

Auto reboot the system

AP Role	Name	Mac	Model	Upgrade Progress
Master		6c:aa:b3:3d:64:30	R500	
Member		d4:68:4d:20:02:70	R710	

Q: What is the effect of the "Auto reboot the system" option shown on the Upgrade page?

A: When "Auto reboot" is enabled, all APs will reboot automatically after a successful image upgrade to make the new image version effective. Alternatively, the user can opt to manually reboot all APs at a more convenient time.

Q: Can a RUCKUS Unleashed AP join a RUCKUS Unleashed Network running a different firmware version?

A: If the existing RUCKUS Unleashed network can reach the RUCKUS image server and support the new AP model, the new AP's image will be updated to be the same as the image version of the existing network.

If the new AP model is not supported, you will have to upgrade the image version of the existing RUCKUS Unleashed network first to an image that can support the AP model of the new AP.

Q: Can a RUCKUS Blue AP join a RUCKUS Blue Network running a different firmware version?

Q: What do I do if the firmware fails to download during the online upgrade?

A: Make sure your Internet connection is working well, then press the **cancel** button on the Upgrade page to retry. The alternative is to find all required images from RUCKUS Support site (support.ruckuswireless.com) and download the images to your administrative PC, and use local upgrade instead.

Q: What should I do if some APs fail to upgrade their images?

A: On the web UI, go to **Access Points** page, make sure the AP is still in **Working** state. Then press **Cancel** to retry. If it still does not work, reboot the AP and retry.

Q: I want to downgrade RUCKUS Unleashed Network to its previous version. How do I do it?

A: Image downgrade is supported only by using the local upgrade method. You will have to download your previous image files, and run local upgrade on each AP. Also note that downgrade sets the system to factory default state to avoid configuration inconsistency.

Q: Where can I find the RUCKUS Unleashed images for local upgrade?

A: You can visit the RUCKUS Support website site (support.ruckuswireless.com), login with your customer account, and then search for RUCKUS Unleashed AP images.

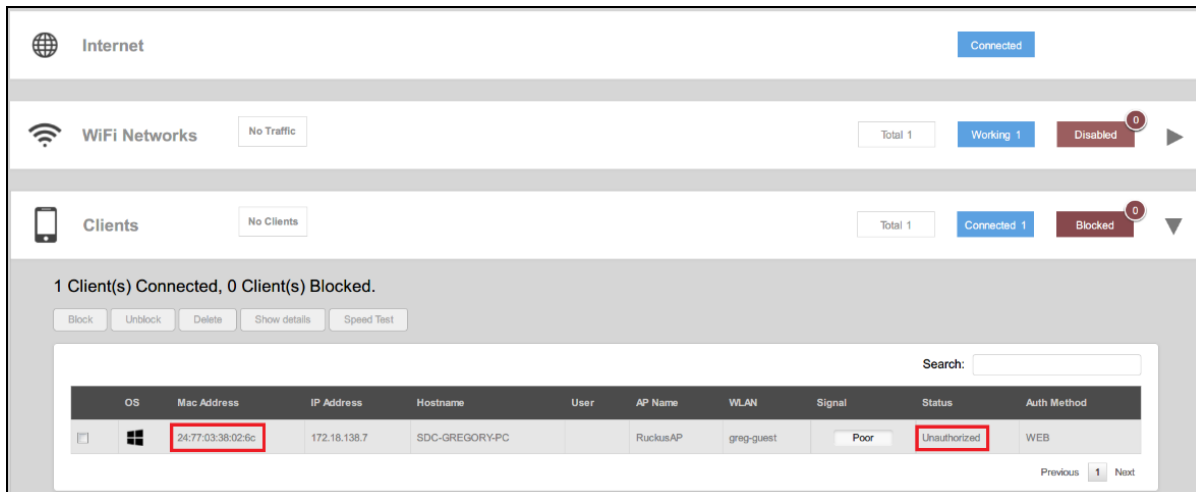
Q: What will happen if in the middle of an image upgrade the network connection on my admin PC goes down?

A: As long as AP's connection is intact, the upgrade should continue in the background. Visit the Upgrade page to see the progress.

Troubleshooting Client Authentication Issues

Q: If the users of Guest or Hotspot (WISPr) WLAN claim their device cannot access the login page, what can I check?

A: First, you can go to the RUCKUS Unleashed web UI and check the Clients list to see whether the client is shown:

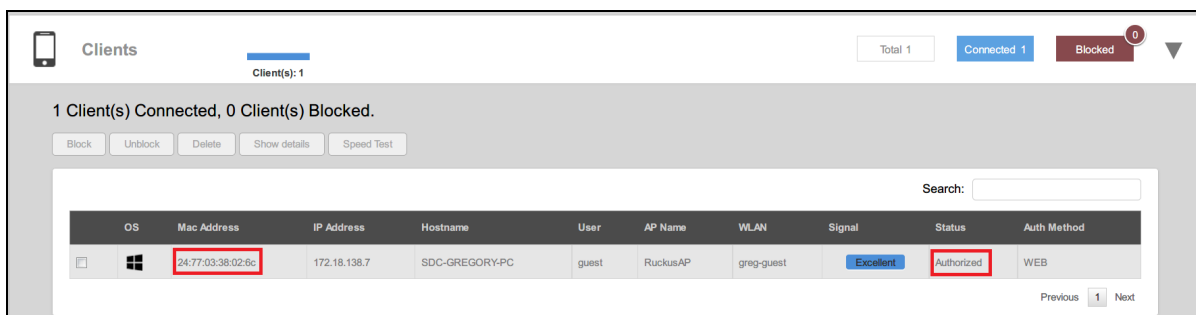


If the client is not displayed in the Clients list, check the WLAN configuration and make sure the client is associated to the correct WLAN.

If client association is fine for Hotspot/WISPr WLAN, check whether the configured portal server is accessible from the client device. Open a web browser on the client and visit the portal server URL configured on the WLAN configuration directly. If the client cannot visit the portal server, there might be a network issue or an access policy is blocking the client's portal access. Ensure that the portal server's domain name or IP address has been added into the "Walled Garden" list in the WISPr configuration.

Q: What can I check for reasons why my device still cannot access the Internet after I submitted the username/password on a Hotspot/WISPr WLAN, or a guest key on a Guest WLAN?

First, check the RUCKUS Unleashed web UI to confirm that your client status is "Authorized" after submitting credentials.



On a Guest WLAN, if the client is not shown as authorized, the input guest pass key might be incorrect, or the key already expired. You can go to **Services -> Guest Access Services** and check the **Admin Generated Guest Passes** table to check it.

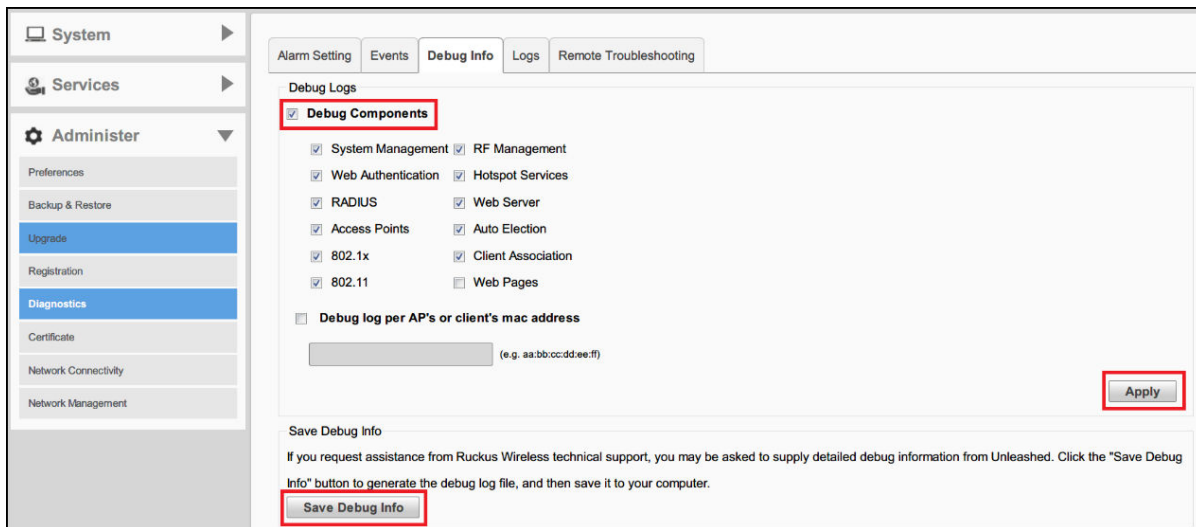
Troubleshooting

Troubleshooting Client Authentication Issues

On a Hotspot/WISPr WLAN if the client is not shown as authorized, you need to confirm with the authentication server to check the authentication result.

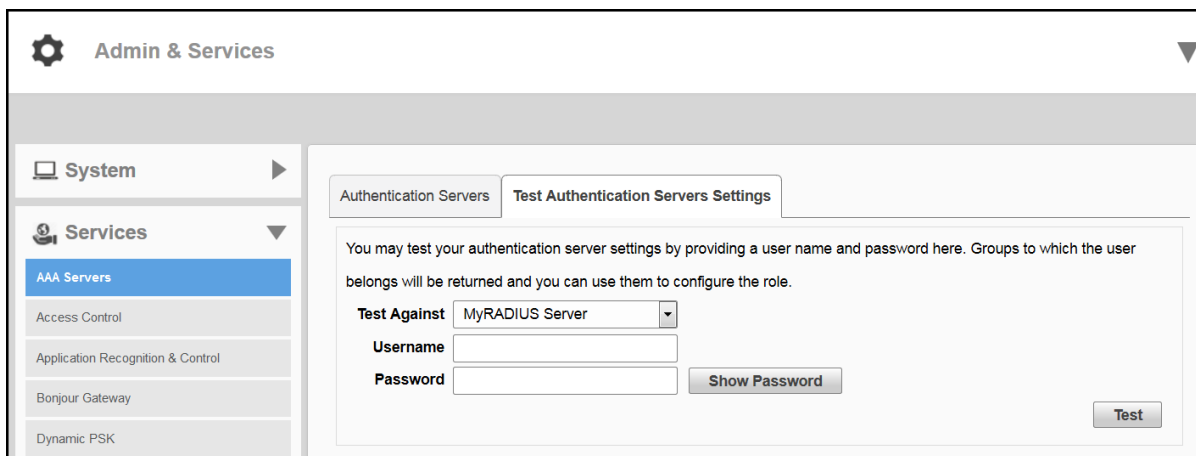
If the problem persists, you can follow the instructions to turn on the debugging log, go through the client connection procedure, and then send the debug file to RUCKUS Customer Support for analysis.

On the **Debug Info** tab, check all **Debug Components**, and repeat client login steps, then click **Save Debug Info**. Provide that file to the Customer Support for further diagnostics.



Q: How do I test whether user accounts exist on an AAA (RADIUS or AD) server?

A: You can test RADIUS or Active Directory user entries from the RUCKUS Unleashed web UI: go to **Admin & Services > Services > AAA Servers**, and select the **Test Authentication Servers Settings** tab.



Q: I configured a Guest WLAN for my users but they complained that whenever they use HTTPS to visit a page, the browser pops up a warning message informing the user that the certificate of the portal page cannot be untrusted. How can I enhance the user experience?

A: You can import your own SSL certificate using the web UI: go to **Admin & Services > Administer > Certificate** and follow the instructions to import an SSL certificate.

Client Connection Troubleshooting

The client connectivity trace feature is designed to help customers diagnose wireless client connection issues to determine why a client fails to connect to the wireless network.

To perform a client connectivity trace:

1. Open the **Clients** section, and select the problematic client from the list.

NOTE

Alternatively, go to **Admin & Services > Administration > Diagnostics > Client Troubleshooting**, and locate the **Client Connection Logs** section.

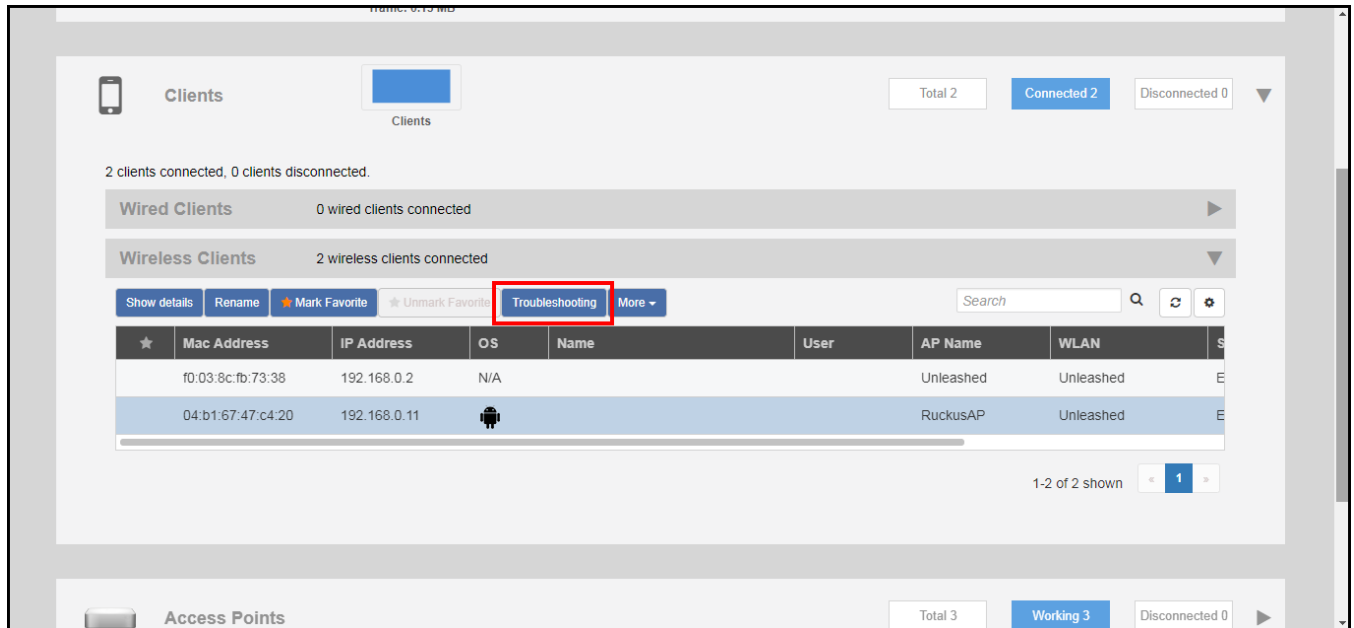
NOTE

As of release 200.8, client connection traces can be performed on clients connected to the following WLAN types:

- WPA2
- Web Auth
- Hotspot
- Guest Access

2. Click **Troubleshooting**.

FIGURE 12 Click Troubleshooting to perform client connectivity trace



The *Troubleshooting* screen appears.

Troubleshooting

Client Connection Troubleshooting

3. In *Connectivity Trace*, click the **Start** button to begin. The association trace begins. The page refreshes to display detailed results.

FIGURE 13 Click Start to begin connectivity trace

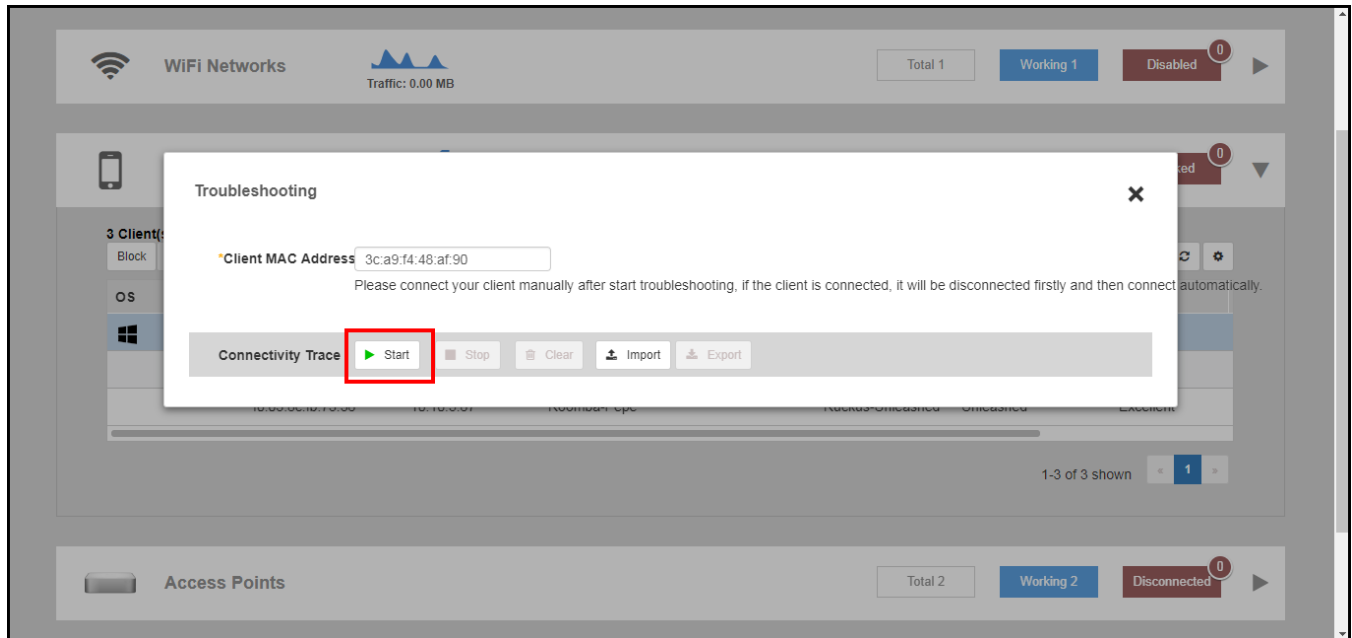
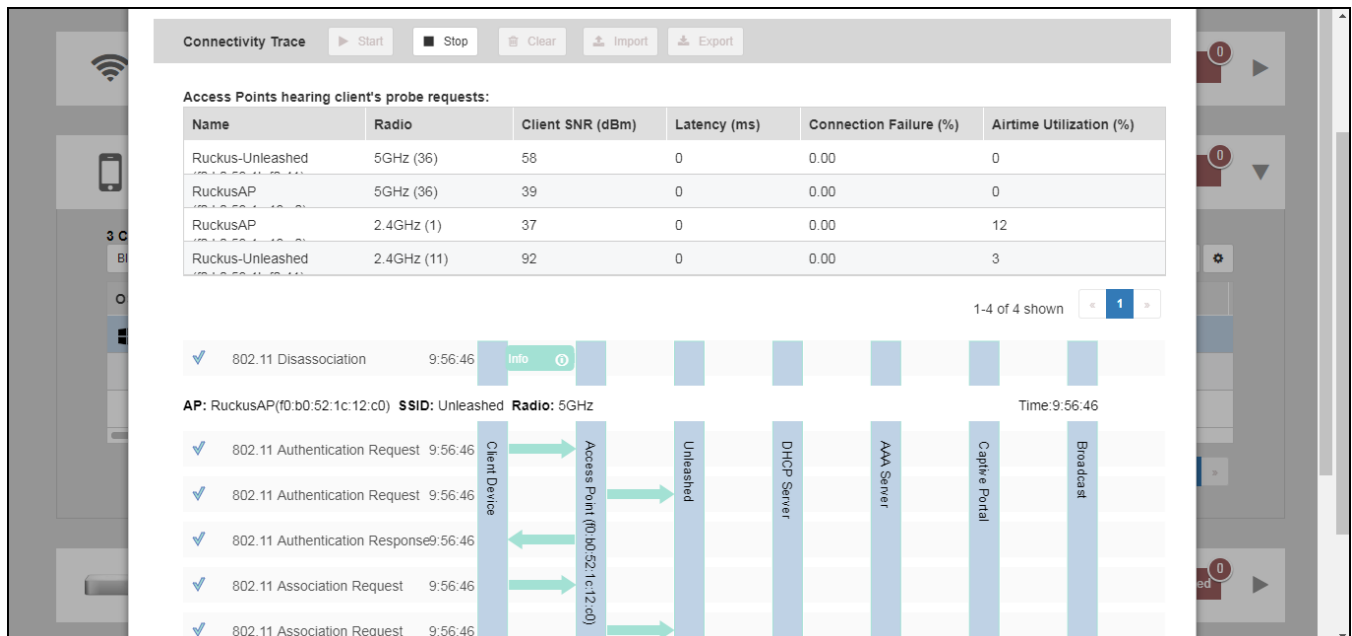


FIGURE 14 Connectivity trace in progress



4. Examine the results to isolate the problematic step in the process.
5. If needed, you can download the client connectivity data to a file, which can later be imported for analysis. Click **Export** to download the data file and save it to your local computer. Click **Import** to import a previously exported file back into Unleashed.

Wireless Mesh Considerations

Q: How do I add an AP to a RUCKUS Unleashed network to make it a wireless Mesh AP?

A: First, connect the AP to the same network as the rest of the RUCKUS Unleashed APs through Ethernet. After the AP joins the network and receives the configuration (including the Mesh link encryption key), the AP is ready to be used as a wireless Mesh AP. You can disconnect the Ethernet link of the AP and move it to the desired location, and it will form a Mesh connection to an uplink AP automatically.

NOTE

Beginning with release 200.6, you can also pre-approve APs to join the Mesh network using the Zero Touch Mesh. To do so, go to **Admin & Services > System > Mesh**, and enter the serial numbers of APs that you want to pre-approve for Mesh auto-configuration.

Q: How do I change the Mesh role of an AP?

A: If Mesh is enabled in the RUCKUS Unleashed network, you must change the Mesh role per AP. From the dashboard, click **Access Points**. Select the AP you want to configure, click **Edit**, and select the **Mesh** tab. For **Mesh Mode**, select the AP's Mesh role as **Auto** (default), **Root AP**, **Mesh AP**, or **Disable** from the list.

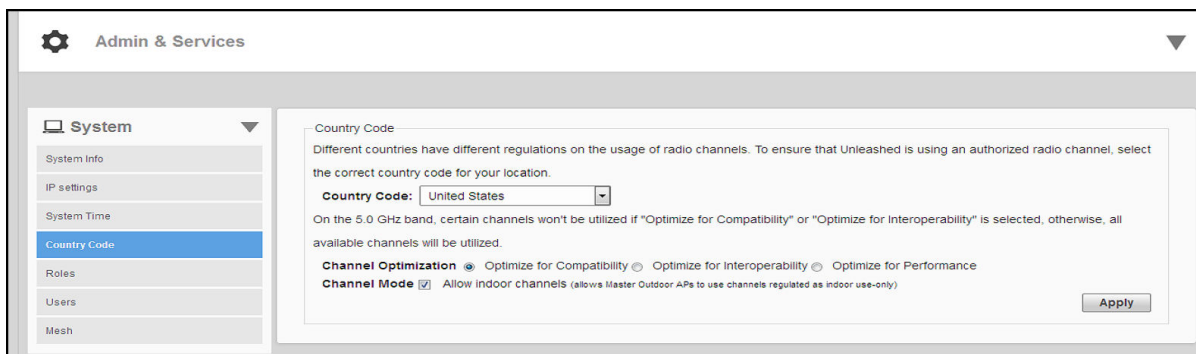
NOTE

The **Mesh AP** mode is not available for the Master AP.

Q: Can a Mesh connection be established between an outdoor AP and an indoor AP?

A: Yes, but note that according to the regulations of your country setting, outdoor APs may not be allowed to use certain indoor channels. If the indoor AP stays on an indoor-only channel, the outdoor AP will not be able to connect to it. In this case, you can either fix the channel of the 5 GHz radio on the indoor APs, or, if a statutory permit exists, configure the outdoor AP to allow it to use indoor channels.

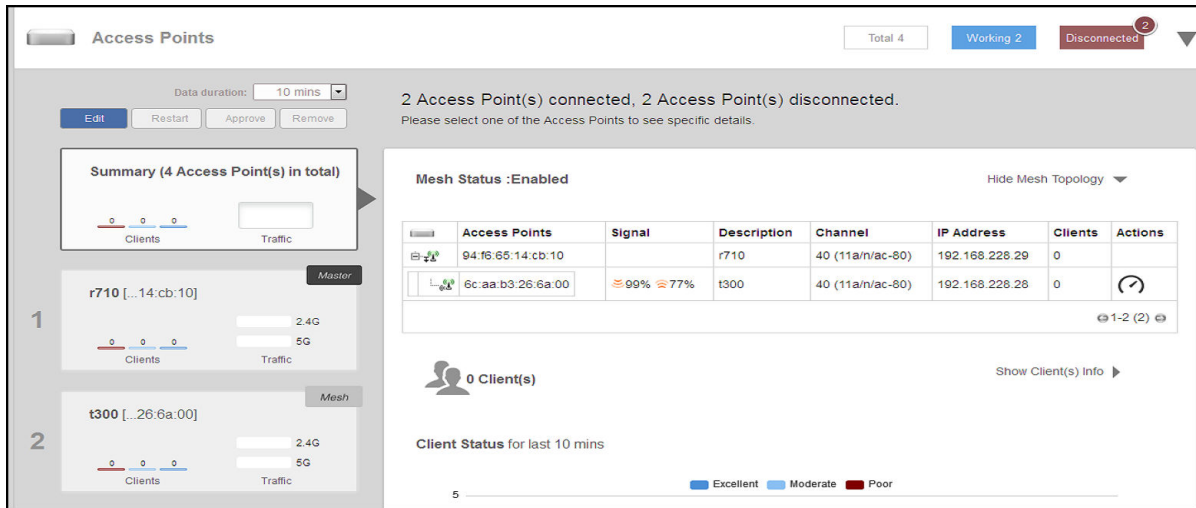
FIGURE 15 Setting Country Code



Q: How can I view the Mesh network topology?

A: You can check the Mesh topology on the web interface by selecting **Devices > Summary AP** box. You can choose to display or hide the Mesh topology by clicking **Show Mesh Topology** or **Hide Mesh Topology**.

FIGURE 16 Showing Mesh Topology



Q: What can I do if a Mesh AP cannot find an uplink connection?

A: There may be a number of reasons why the Mesh AP cannot find an uplink connection:

- The APs, either the intended Mesh AP or the uplink AP, may not support Mesh. For example, R310 AP and H320 AP do not support Mesh.
- The Mesh AP may not be properly configured. It is always a good practice to ensure an AP can join a RUCKUS Unleashed network through an Ethernet connection before making it a Mesh AP.
- The signal from the uplink AP may be too weak. Try moving the AP to a different location to see if the signal improves.
- The uplink AP stays on a channel that the Mesh AP cannot utilize. Note that an outdoor AP may not be able to utilize certain indoor channels, and the Mesh AP model may not support a DFS channel that the uplink AP is using.
- Check the running release: release 200.0 does not support mesh.
- In release 200.1, there was an issue (ER-3691) reported where the Mesh uplink search may not start right after the Ethernet cable is disconnected, until the AP is rebooted. This issue has been resolved in 200.2 and later releases.

If the AP is accessible (either wired or wireless), use SSH to connect to it and enter the following CLI debugging commands. If you cannot interpret the results, refer to Reporting an Issue to contact RUCKUS Support.

- On a Root AP:
 - `get mesh`
 - `get channel wifi1`
 - `get scanresults wifi1`
- On a Mesh AP:
 - `get mesh`
 - `get channel wifi1`
 - `get scanresults wifi1`

Q: Is Mesh supported on all RUCKUS Unleashed APs?

A: Mesh has been supported since release 200.1. For Unleashed 200.6 and earlier, Mesh is supported on all AP models except R310 and H320.

Q: What happens if the Master AP becomes a Mesh AP?

A: If a Master AP becomes a Mesh AP (for example, its uplink becomes a wireless link), it will give up its Master AP role after a reboot. The new Master AP will be elected from among the Root APs automatically. Your RUCKUS Unleashed network will be adjusted automatically after a few minutes.

Q: How do I recover an isolated Mesh AP?

A: When a Mesh AP becomes isolated (unable to connect to the Master AP through either the Ethernet or wireless Mesh interface), it begins broadcasting a "Recover.Me" SSID, which allows an administrator to connect wirelessly to the problem AP and begin troubleshooting and making configuration changes. The Recover.Me SSID includes the last six digits of the MAC address of the AP (using the following format: recover.me-<last six digits of MAC address>) so that you can identify which Mesh AP is having issues.

In Unleashed 200.6 and later, the Recover.Me SSID allows clients to access the AP via the AP's IP address **169.254.1.1**. When a client is unable to get an IP address automatically (no DHCP server), it will usually assign itself an address in the range **169.254.x.x**, which will be able to reach the isolated AP on 169.254.1.1.

NOTE

Some clients may be unable to automatically assign an address in the 169.254.x.x range. In this case, the user must configure a static IP address manually.

To troubleshoot an isolated Mesh AP, connect to the Recover.Me SSID and use SSH to access the AP CLI. Once connected, log in using the user name and password of the RUCKUS Unleashed network, and perform troubleshooting tasks such as checking that the Mesh name and password match those in the web interface of the RUCKUS Unleashed Master AP, saving debug information, and checking other configuration settings.

Using the Management Interface

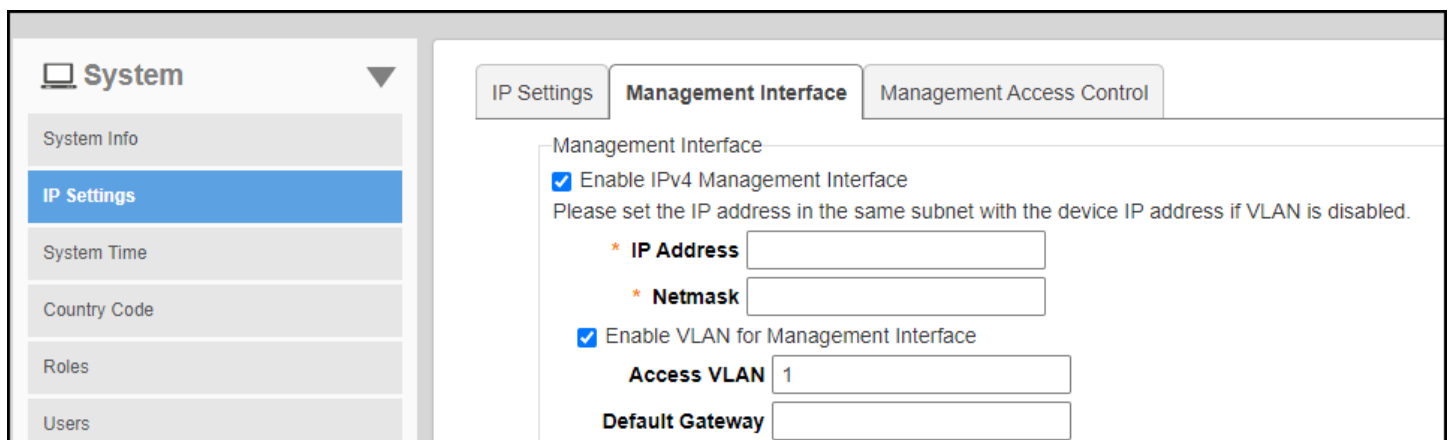
Q: Can the Management Interface IP address still be used to access the Master AP if the Master changes?

A: Yes, it can. The Management IP address configuration is shared among all Unleashed APs, and the Master AP is in charge of responding to it.

Q: Does Unleashed support management VLAN on the Management Interface?

A: Yes, from 200.10 release, Unleashed supports management VLAN on the Management Interface.

FIGURE 17 Management VLAN Support on Management Interface



Q: Should the management IP address be in the same subnet as the AP's device IP address?

A: Yes, it should. Unleashed APs do not support VLANs, so it is not recommended to configure the management IP in a different subnet.

Q: Can a member AP utilize the IP address of the Management Interface to connect to the Master AP?

Troubleshooting

Configuring DHCP Service

A: No. The Management Interface can only provide web (and optionally RADIUS and SNMP) services, it is not used for member APs to connect to the Master AP.

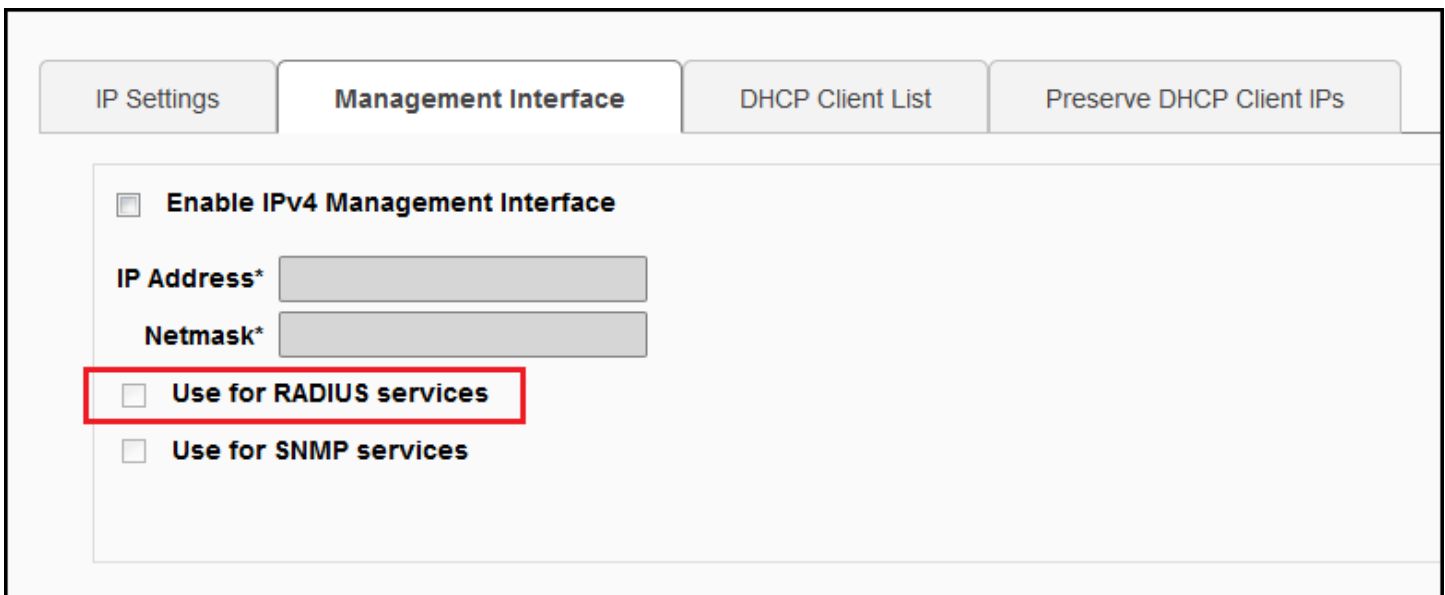
Q: Why does the Management Interface stop working once I enable Gateway mode?

A: Because if Gateway mode is enabled on an Unleashed Network, the Master AP is fixed. In this situation, the device IP would be the same as a management IP, so the Gateway/Master AP does not support the management IP interface feature.

Q: Can the Management Interface be used for communication with a RADIUS server?

A: Yes, you can enable the check box **Use for RADIUS services** to enable RADIUS authentication via the Management Interface. This is important in an Unleashed network so that each AP's individual IP address does not need to be configured on the RADIUS server as an authorized RADIUS client.

FIGURE 18 Use Management Interface for RADIUS service



The screenshot shows a web interface with four tabs: "IP Settings", "Management Interface", "DHCP Client List", and "Preserve DHCP Client IPs". The "Management Interface" tab is active. Below the tabs, there is a section with the following options:

- Enable IPv4 Management Interface
- IP Address*
- Netmask*
- Use for RADIUS services (highlighted with a red box)
- Use for SNMP services

Configuring DHCP Service

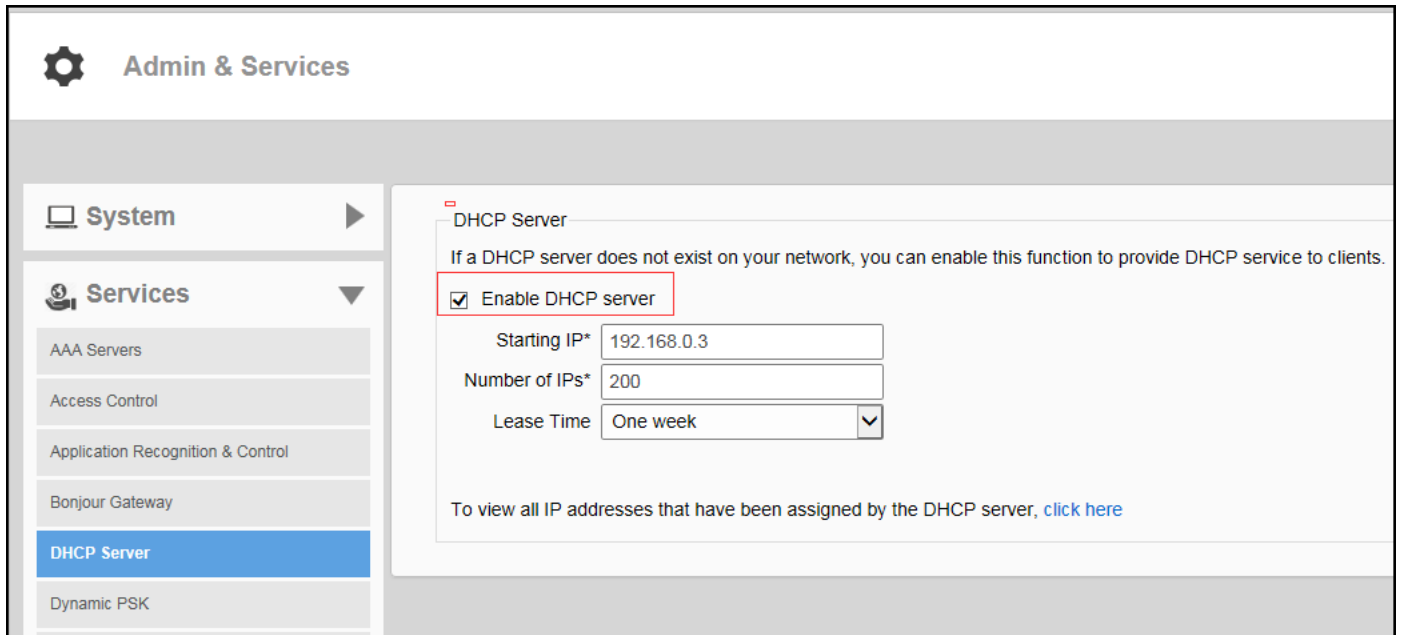
Q: How do I enable the internal DHCP server in an Unleashed network?

A: Unleashed DHCP functionality depends on which release you are running.

The Gateway mode feature was not supported in releases 200.0, 200.1 and 200.2. In these early releases, the Master AP could be configured with a static IP address and the DHCP server could be enabled.

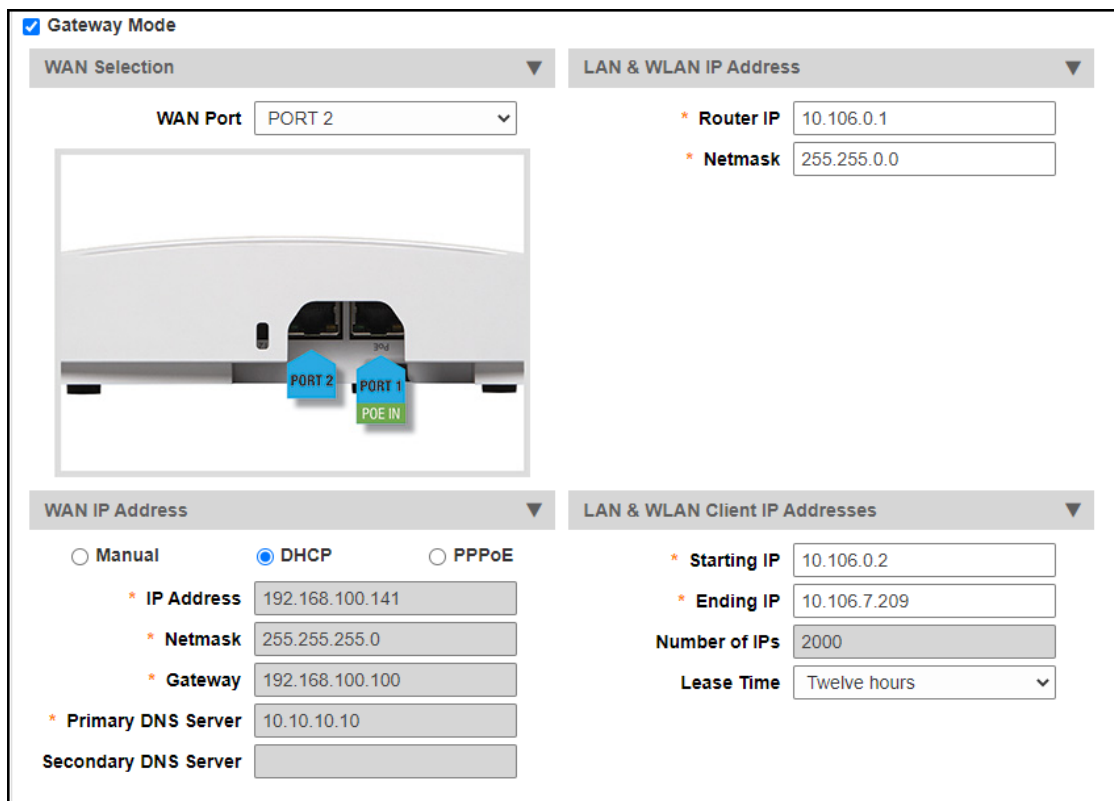
To enable DHCP server on those Unleashed releases, go to *Admin & Services > Services > DHCP Server*.

FIGURE 19 Enable DHCP Server



Beginning in release 200.3 and later. In later releases, the Gateway Mode configuration page has been moved to the *IP Settings* page:

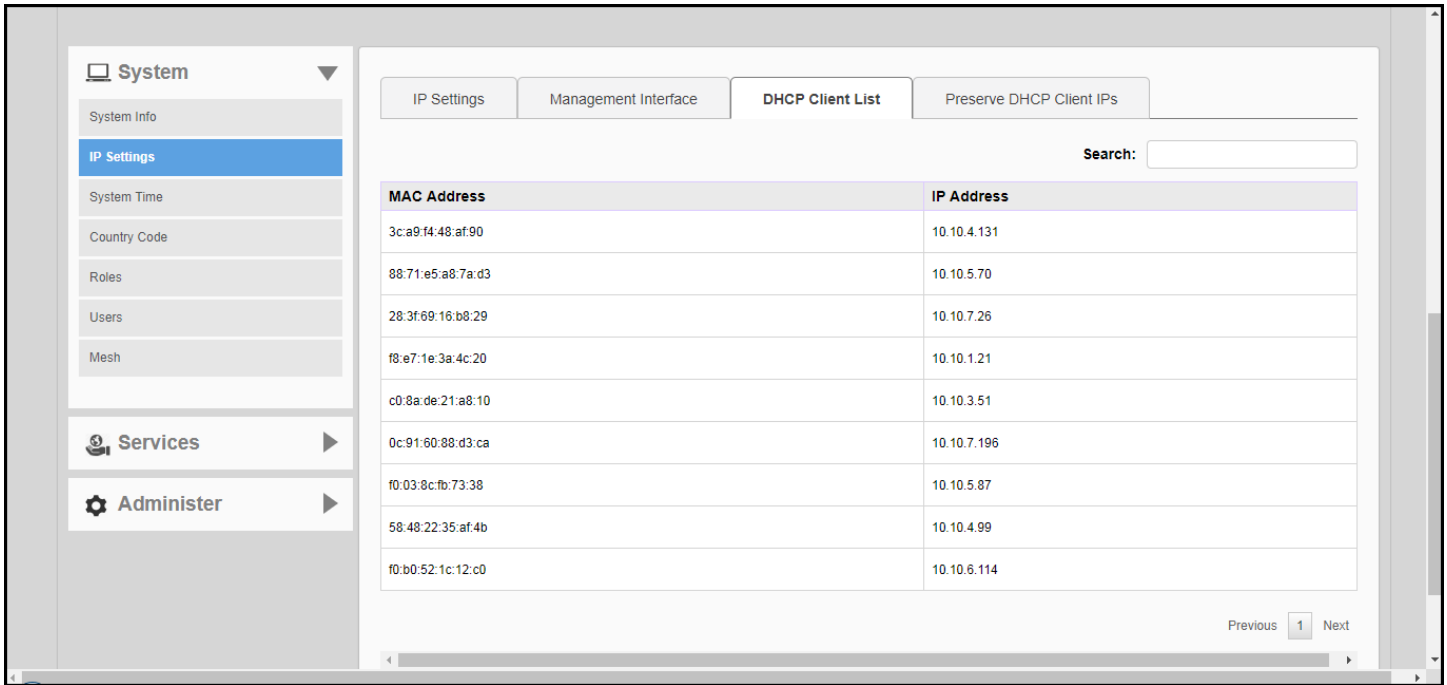
FIGURE 20 Gateway Mode on the IP Settings page



Q: How do I check the leased IP addresses from the DHCP server?

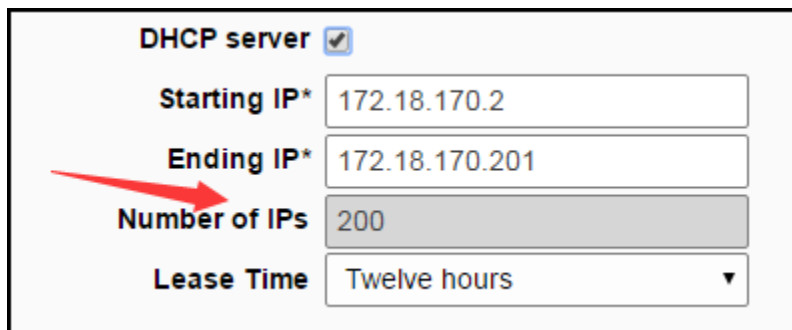
A: The list of IP addresses leased by the DHCP server can be seen on the following page: **System > IP Settings > DHCP Client List**.

FIGURE 21 DHCP client list



Q: What is the maximum number of IPs addresses supported by the internal DHCP server?

A: The number of IPs is manually configured using the **Number of IPs** and the **Ending IP** address settings on the DHCP server configuration screen.



Q: How do I assign DNS server information in the internal DHCP address offers?

A: Go to **Admin & Services > System > IP settings**.

The screenshot shows the 'IP Settings' configuration page in RUCKUS Unleashed. It includes tabs for 'IP Settings', 'Management Interface', and 'DHCP Client List'. A warning message states: 'Warning: Upon enabling Gateway, all devices will reboot immediately.' The 'Gateway Mode' is set to 'Manual' with a checked checkbox. Below this, the 'IP Address' is 172.18.170.11, 'Netmask' is 255.255.255.0, and 'Gateway' is 172.18.170.254. The 'Primary DNS Server' (172.18.100.35) and 'Secondary DNS Server' (172.18.100.45) fields are highlighted with a red box. Other settings include 'DHCP server: Enabled', 'NAT: Enabled', 'LAN Port IP Address: 10.10.0.1', 'LAN Port Netmask: 255.255.0.0', 'Starting IP: 10.10.0.2', 'Ending IP: 10.10.7.209', 'Number of IPs: 2000', and 'Lease Time: Twelve hours'.

General Configuration Questions

Q: I am familiar with RUCKUS ZoneDirector configuration, and I'm curious why I can't find the AP group and WLAN group settings on the RUCKUS Unleashed UI. What am I missing?

A: To simplify RUCKUS Unleashed configuration, AP groups and WLAN groups are not supported.

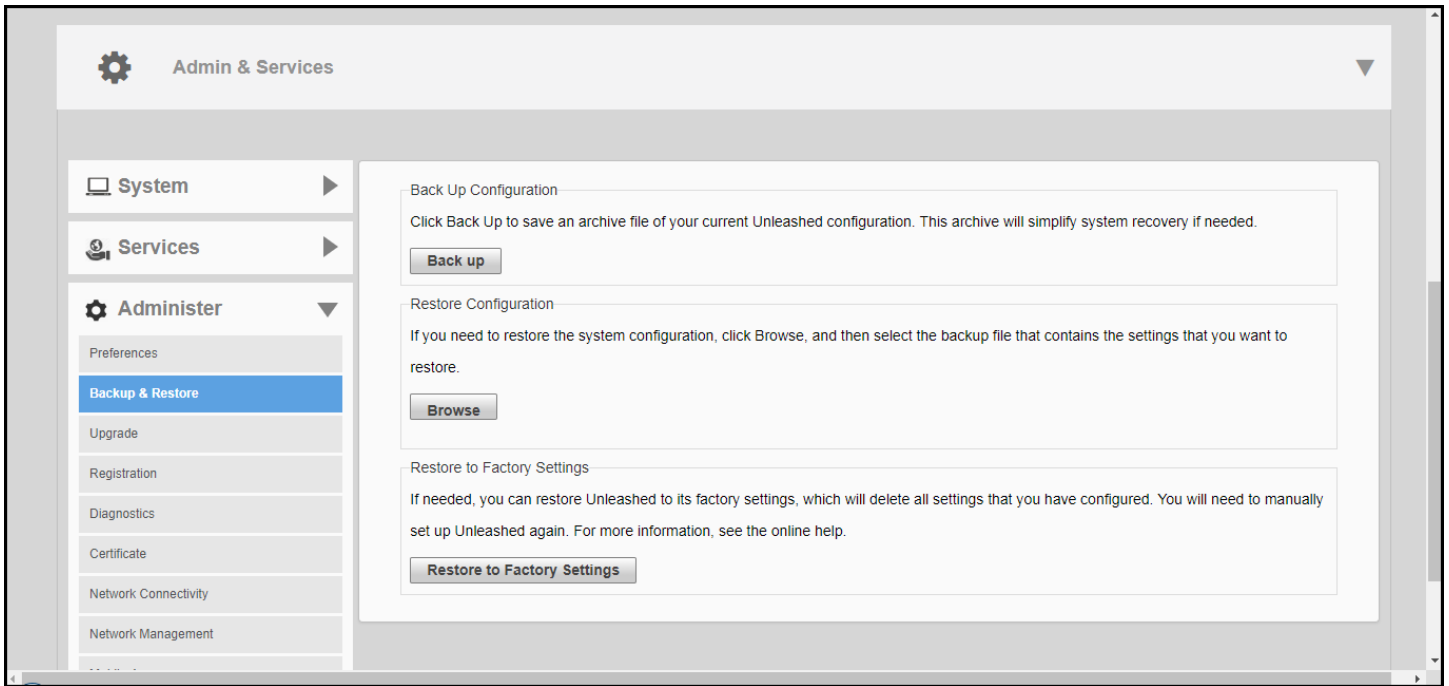
Q: How do I save an existing configuration or restore my previous configuration?

A: You can backup and restore your RUCKUS Unleashed system configuration settings using the *Admin & Services > Administer > Backup & Restore* page.

Troubleshooting

General Configuration Questions

FIGURE 22 Backup & Restore Page



Q: Since AP Groups/WLAN Groups are not supported, how can I set up a WLAN to be advertised on only one radio (2.4G or 5G)?

A: Edit the WLAN and click Show Advanced Options. On the Radio Control tab, you can select All Radios, 2.4 GHz Only, or 5 GHz only.

FIGURE 23 By default, all WLANs are enabled on both radios

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

Wireless Media Management:

Fast BSS Transition: Enable 802.11r FT Roaming
Recommended to enable 802.11k Neighbor-list Report for assistant.

Radio Resource Management: Enable 802.11k Neighbor-list Report
Recommended to enable 802.11k Neighbor-list Report for assistant.

Background Scanning: Enable
(All radio will preform background scanning)

Load Balancing: Enable
(Applies to this WLAN only.it may not be active on other WLANs)

Band Balancing: Enable
Applies to this WLAN only. Band Balancing might be enabled on other WLANs

802.11d: Support for 802.11d (only applies to radios configured to operate in 2.4 GHz band)

Enable WLAN on: ▼

- All Radios
- 2.4 GHz only
- 5 GHz only

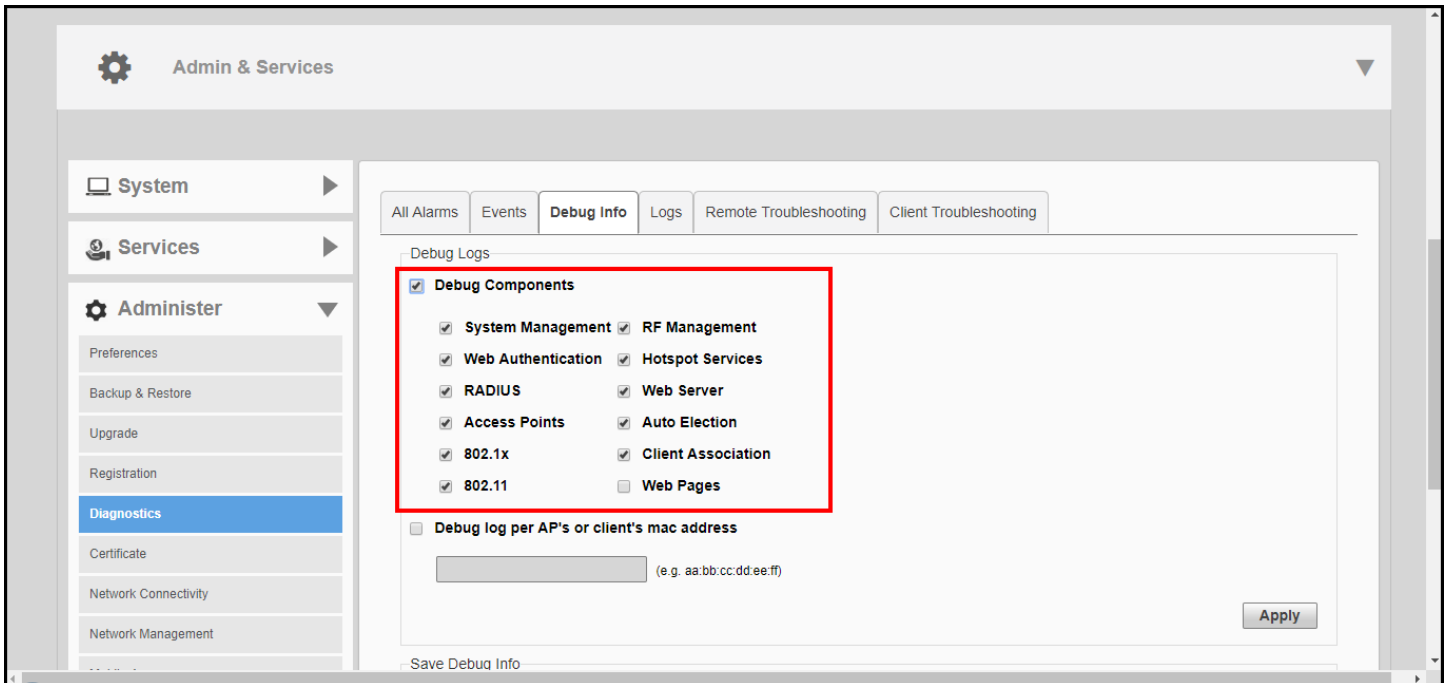
OK Cancel

Debugging

Q: RUCKUS Customer Support asked me to turn on debug logging and recreate my problem for diagnosis. How do I enable the logs? And, how do I know which logs need to be enabled?

A: Debug logs can be enabled on the web UI on the following page: *Admin & Services > Administer > Diagnostics > Debug Info*.

FIGURE 24 Select which debug components to include in debug logs



If you are not sure which logs to enable, the recommendation is to enable most of them. One exception is the **Web Pages**, component, which generates many log messages. Unless you are analyzing a web UI issue, do not enable this log.

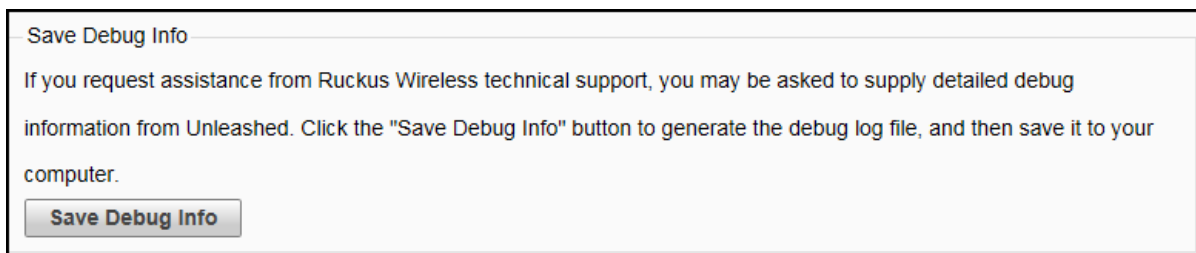
NOTE

Generating debug log messages impacts AP performance. Remember to disable debug logs after the logs have been collected.

Q: How do I save debug information?

A: Go to **Admin & Services > Administer > Diagnostics > Debug Info**, and click the **Save Debug Info** button. Save the package to your local computer and send it to RUCKUS Customer Support.

FIGURE 25 Saving Debug Info



Q: After SSH into my Master AP, I noticed a different CLI prompt which is not the RUCKUS AP CLI. It doesn't take any AP CLI commands either. What's wrong?

A: The Master AP provides a Master-style CLI, closer to the ZoneDirector controller CLI. You can use the **ap-mode** command to enter AP CLI mode, and **quit** to exit back to Master CLI mode.

FIGURE 26 The ap mode command

```

Please login: admin
Password:
Welcome to Ruckus Unleashed Network Command Line Interface
ruckus> enable
ruckus# ap-mode
You have all rights in this mode.
ruckus (ap-mode) #
ruckus (ap-mode) # quit
No changes have been saved.
ruckus# █

```

Q: I suspect that my Master AP may mysteriously crash/reboot at times. But I do not have anything to provide for RUCKUS customer support for analysis. What can I do?

A: You can help to collect the debugging information if you know that an AP in the Master role may potentially experience a mysterious crash or reboot. To do so, enable the log reporting mechanism in advance, and, if the AP indeed experiences a problem, it may be able to send its log files out to a preconfigured server before it reboots.

To enable this debug logging feature, go to **Admin & Services > Administer > Diagnostics > debug Info**, and enable **Upload debug logs to remote server**. Enter the **Host** IP address, and click **Apply** to save your changes.

FIGURE 27 Upload Debug Logs

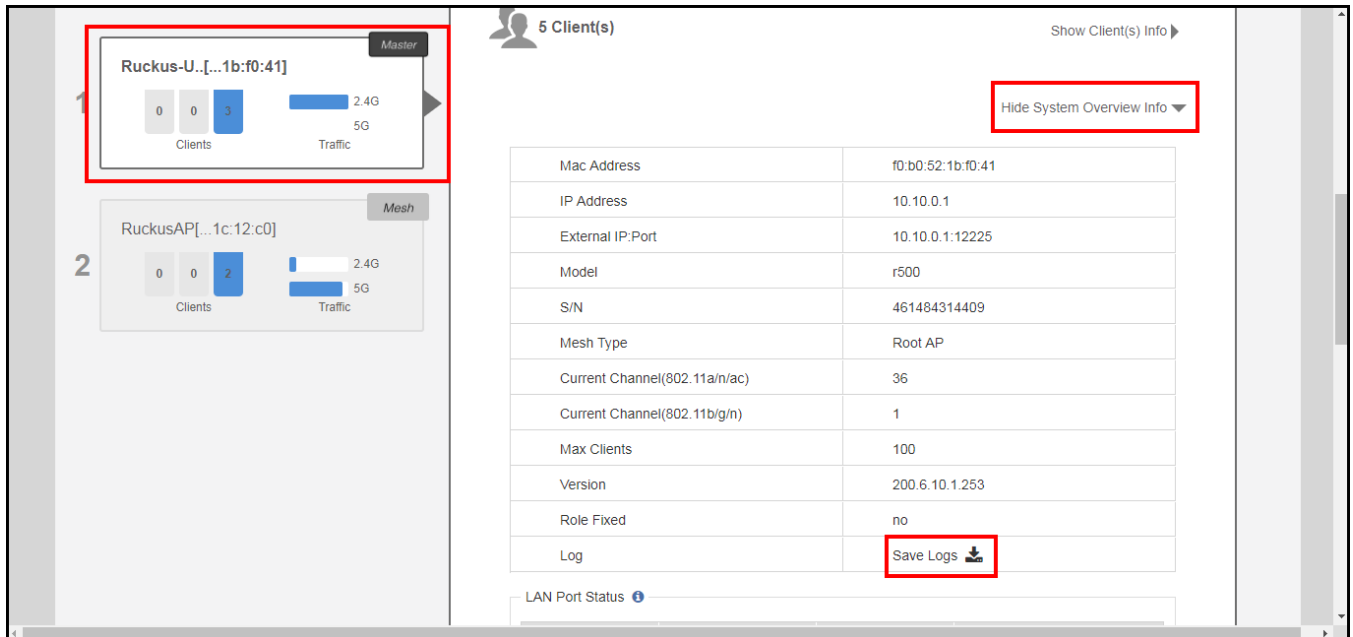
Once you have the logs, you can report the issue following the reporting method described at the beginning of this guide.

Q: One of my member APs has crashed or rebooted. The RUCKUS support representative asked me to provide the AP's support information for analysis. How do I collect this information?

A: There are two ways to retrieve an AP's support information:

1. Save the AP support info from the web UI: **Access Points > select the AP > ShowAP Info**, and then click **Save Logs** to save it to your administrative PC.

FIGURE 28 Saving AP Logs



2. Through AP's CLI: SSH to AP, log in to AP's CLI, execute the following commands and save the console output to a file:

- `support`
- `support show`

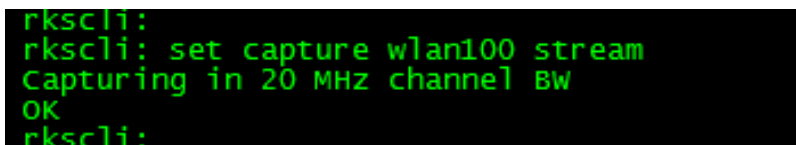
Q: How do I capture packets on an Unleashed AP?

A: Unleashed APs support remote packet capture using the same methods as a ZoneDirector controller.

You can SSH to the Unleashed AP, and run the following CLI command to enable remote packet capture:

```
set capture wlan100 stream
```

FIGURE 29 set capture wlan100 stream



And replace "stream" with "idle" to stop streaming:

```
set capture wlan100 idle
```

NOTE

The above command works in a Member AP. On a Master AP running 200.3 or later image, you need to go to AP CLI mode in SSH session using the `ap-mode` CLI command:

FIGURE 30 set capture wlan100 idle

```

Please login: admin
Password:
Welcome to Ruckus Unleashed Network Command Line Interface
ruckus> enable
ruckus# ap-mode
You have all rights in this mode.
ruckus(ap-mode)# set capture wlan100 stream
Capturing in 20 MHz channel BW
OK
ruckus(ap-mode)# set capture wlan100 idle

OK
ruckus(ap-mode)# quit
No changes have been saved.
ruckus# █

```

If the Master AP is running 200.2 or earlier, you can enter the CLI debug mode and use the following `remote_ap_cli` command with the Master AP's MAC address:

FIGURE 31 Using the `remote_ap_cli` command to execute a command on a remote AP

```

Please login: admin
Password:
Welcome to Ruckus Unleashed Network Command Line Interface
ruckus> enable
ruckus# debug
You have all rights in this mode.
ruckus(debug)# remote_ap_cli -a f8:e7:1e:0e:ba:c0 "set capture wlan100 stream"
---- Command 'rkscli -c "set capture wlan100 stream "' executed at f8:e7:1e:0e:ba:c0
Stream capture is running on wifi3, please set it to idle mode.
remote_ap_cli "-a" "f8:e7:1e:0e:ba:c0" ""set" "capture" "wlan100" "stream""
ruckus(debug)#
ruckus(debug)# remote_ap_cli -a f8:e7:1e:0e:ba:c0 "set capture wlan100 idle"
---- Command 'rkscli -c "set capture wlan100 idle "' executed at f8:e7:1e:0e:ba:c0
OK
remote_ap_cli "-a" "f8:e7:1e:0e:ba:c0" ""set" "capture" "wlan100" "idle""
ruckus(debug)#
ruckus(debug)# quit
No changes have been saved.
ruckus# █

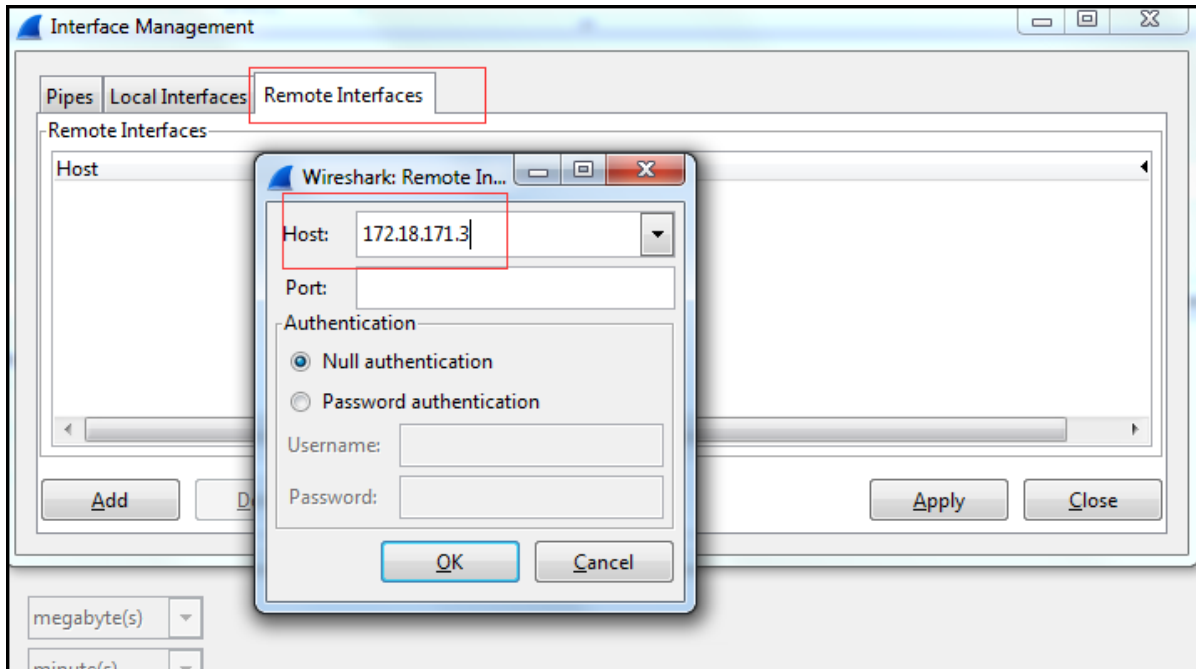
```

You may also need to use the following AP CLI command to learn the AP's IP address:

```
get ipaddr wan
```

Start Wireshark on a PC, type the AP's IP address to capture the packets:

FIGURE 32 Configure remote interface in Wireshark UI



Understanding LED Behavior

The following tables describe the behavior of the Power, Controller (DIR/CTL), and AIR LEDs for RUCKUS Unleashed Master and member APs.

The CTL (Controller) LED is the same as the DIR (Director) LED; older APs are labeled "DIR" while newer APs are labeled "CTL."

You can use the LED states to troubleshoot AP issues such as network connectivity issues, Master AP election issues, potential hardware failure issues, and controller connection status.

TABLE 2 Power LED Status

POWER LED	Status	State	Reason	Action
<i>Image Booting</i>	Solid RED	Bootup in progress.	If the state lasts more than 30 sec, it indicates AP failed to complete booting.	Either a manufacturing error or an AP hardware issue. Contact RUCKUS Support about RMA process.
<i>Network Configuration</i>	Flashing Green	AP firmware image booted. No routable IP received or assigned.	Network issue.	Check DHCP server configuration.
<i>Normal Operation</i>	Solid Green	Routable IP address received.	All good	

TABLE 3 CTL (DIR) LED Status

CTL (DIR) LED	Status	State	Reason	Action
RUCKUS Unleashed member AP mode	Off	AP is a RUCKUS Unleashed member AP.	All good	

TABLE 3 CTL (DIR) LED Status (continued)

CTL (DIR) LED	Status	State	Reason	Action
Locating	Slowly Flashing Green (every 2 sec)	RUCKUS Unleashed Master AP discovery in progress.	Unable to contact RUCKUS Unleashed Master, and AP cannot become a Master AP itself (because it is a Mesh AP, or Gateway Mode is enabled on the network, or the AP is configured as non-Master).	If the AP stays in this state for more than two minutes, check Internet access, firewall settings, DNS, and Master AP status. Also, check why the AP cannot become the Master itself.
Receiving	Fast Flashing Green (twice a sec)	Receiving configuration or image upgrade.		Wait until it ends.
RUCKUS Unleashed Master mode	Solid Green	AP is the RUCKUS Unleashed Master.	All good	

TABLE 4 AIR LED Status

AIR LED	Status	State	Reason	Action
Standalone/Root/non-Mesh AP	Off	AP is operating in standalone or Root or non-Mesh AP	All good	None
Mesh AP	Solid Green	AP is functioning as Mesh AP (MAP)	Wireless signal to uplink AP is good.	None
Mesh AP	Blinking Solid Green (2 Hz)	AP is functioning as a Mesh AP (MAP)	Wireless signal to uplink AP is good.	None
Mesh AP	Blinking Solid Green (0.5 Hz)	AP is functioning as a Mesh AP (MAP)	AP is searching for mesh uplink.	None

Built-In Memory Diagnostic Tool

The built-in memory diagnostic tool is an internal tool for recording or dumping the memory allocated. Users can analyze if there was a memory leak or double freeing (freeing memory more than once) of the information record.

Use the following command in the shell environment to use the built-in memory diagnostic tool:

padinfo -p pid option

FIGURE 33 Using the Built-in Memory Diagnostic Tool Command

```
padinfo -p <pid> <option>>
-p <pid>: the process id
option:
-d <enable|disable|enable-xx[,enable-yy][disable-xx[,disable-yy]]>: enable or disable memory leak debug
  enable: enable memory leak debug
  enable-xx[,enable-yy]: also enable further debug option, at present support:history.
    example: "enable-history" or "enable-history,yyy.zzz"
  disable: disable all memory debug
  disable-xx[,yy]: disable further debug option
-s <uclibc|leak|history|all>: show memory statistic info of uclibc or memory leak statistic debug info or flush history record or all.For example: "uclibc" or "uclibc,leak,history"
-c <n>: show top n allocations (by default 50) when dumping memory leak statistic debug info
-l <n[,m,o]>: set pointers/backtrace/history max entries, the set is not support dynamically. First number is pointers max limit,second is backtrace max line limit. third is history items per file
  example: "20000" or "20000,5000,20000"
  The actual max entries are less than config for some consume in third part or fragment. For example Pointers limitation 201400 the actual max is 111888.
-u: show memory debug status
-r: Delete the storage directory when the debug function is disable
```

TABLE 5 Command Parameters

Command	Parameter	Description
padinfo -p	pid	Process ID
	option -d <i>enable disable enable-xx[,enable-yy] disable-xx[,disable-yy]</i>	enable: Enable memory leak debug enable-xx[,enable-yy]: Enable further debug option, at present support: history disable: disable all memory debug disable-xx[,yy]: disable further debug option
	-s <i>uclibc leak history all</i>	Show memory statistic information of uclibc or memory leak statistic debug information or flush history record or all.
	-c <i>n</i>	Show top n allocations (by default 50) when dumping memory leak statistic debug information.
	-l <i>n[,m,o]</i>	Set pointers (maximum limit), backtrace (maximum line limit), and history n: maximum limit for pointers m: maximum line limit of backtrace o: history items per file The set is not supported dynamically.
	-u	Show memory debug status (enabled or disabled)
	-r	Delete the storage directory when the debug function is disabled

Following is an example to show the memory statistic information of uclibc, memory leak statistic debug information, and flush history record.

```
ruckus$ padinfo -p 1204 -s all
send msg failed:errno =111: correction refused
ruckus$ padinfo -p 1124 -s all
memory statistic info of uclibc:
total bytes allocated           = 70553600
total bytes in use              = 26452872
total bytes freed               = 44100728
total allocated mmap space     = 311296
number of free chunks           = 22794
number of fastbin blocks       = 165
space in freed fastbin blocks   = 7008

memory leak statistic debug info:
top 50 allocations:
caller [icxd_snmp.c] line[4689] size[476] allocation:[64], mem_size[30464]
caller [icxd_snmp.c] line[3957] size[28] allocation:[10], mem_size[280]
```

Following is an example to show the maximum limit for pointers, backtrace, and history items.

```
ruckus$ padinfo -p 1124 -d enable -l 20480 10240 20480
target process memory debug is enable(further options:callchain.plugin)
The Active limitation of record is pointer items[20480], backtrace items[10240], History items[20480]
```

Following is an example to show the memory debug status (enabled or disabled).

```
ruckus$ padinfo -u
ruckus$padinfo -p 1204 -u
```

Following is an example to delete the storage directory when the debug function is disabled.

```
ruckus$ padinfo -r
ruckus$padinfo -p 1204 -r
```

Sample Built-In Memory Diagnostic Tool Process

Here is a sample procedure to use the built-in diagnostic tool.

1. Use SSH to access the Master AP shell.
2. Check the debug tool status by default.

```
padinfo -u
```

3. Query the process pid.

```
ps | grep emfd
```

4. Enable the emfd process debug.

```
padinfo -p 1204 -d enable
```

5. Display the memory statistics information as needed.

```
padinfo -p 1204 -s all
```

6. Move the debug files to a remote server.

```
tftp -p -l /var/tmp/mem_diag/mem_event tftpServer
```

NOTE

Use the following command if **mem_history_*** files existed:

```
tftp -p -l /var/tmp/mem_diag/mem_history_* tftpServer
```

mem_history_* is the record of memory malloc when customer enables the debug tool.

For example, if **mem_history_0** or **mem_history_1** file existed, use the appropriate command accordingly:

```
tftp -p -l /var/tmp/mem_diag/mem_history_0 tftpServer
tftp -p -l /var/tmp/mem_diag/mem_history_1 tftpServer
```

7. Disable the debug function after the debug is completed.

```
padinfo -p 1204 -d disable
```

8. Delete the storage directory after the debug function is disabled.

```
padinfo -r
```

All of the built-in memory diagnostic summary files are located in the following AP path: `/var/tmp/mem_diag/`.

TABLE 6 File Names in the Summary File

Name	Description
info_file_raw	Internal statistic raw data
paduclibcinfo.dat	Uclibc information
Mem_history_*	Record of pointer actions
mem_event	Event message

The following example is a sample summary file (if the debug files are in the AP path):

```
ruckus$ cd /var/tmp/mem_diag/
ruckus$ ls -alh
drwxr-xr-x  2 root      root      140 Feb 6 09:04  .
drwxrwxrwt 30 root      root      2.7K Feb 7 02:44  ..
```

Troubleshooting

Built-In Memory Diagnostic Tool

```
-rw-r--r--    1 root    root    4.9M Feb 6 02:31 mem_event
-rw-r--r--    1 root    root    5.0M Feb 6 02:31 mem_history_0
-rw-r--r--    1 root    root    5.0M Feb 6 06:23 mem_history_1
-rw-r--r--    1 root    root    5.0M Feb 6 09:04 mem_history_2
-rw-r--r--    1 root    root    60 Feb 6 02:31 status
```




© 2024 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>