RUCKUS
COMMSCOPE

Deployment Guide

Migration of Access Points from ZoneDirector Wireless Controller to Unleashed

July 2022

Table of Contents

Intended Audience

This document provides available strategies and procedures to migrate existing RUCKUS access points from ZoneDirector Wireless Controller to Unleashed. Step-by-step procedures for configuration and testing are demonstrated.

This document is written for and intended for use by technical engineers with some background in ZoneDirector, Unleashed administration, TFTP (Trivial File Transport Protocol), DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System) and 802.11/wireless engineering principles.

For more information on how to configure Ruckus Networks products, please refer to the appropriate Ruckus user guide available on the Ruckus support site.

Ruckus Support Site	https://support.ruckuswireless.com/
Ruckus Knowledge Base Articles (KBA)	https://support.ruckuswireless.com/answers/
Ruckus Community	https://community.ruckuswireless.com/
Ruckus Documentation	https://docs.commscope.com/
Ruckus Licensing Manager	https://support.ruckuswireless.com/liman
Warranty Programs	https://support.ruckuswireless.com/programs-warranty_registration

Overview

RUCKUS announced End of Sale(EoS) and End of Life(EoL) dates for ZoneDirector 1200. The RUCKUS ZoneDirector 1200 will go EoL and will no longer be available for purchase after August 31, 2022. For more information on EoS/EoL milestones and Replacement options, please refer to *RUCKUS End of Sale Announcement for ZoneDirector 1200 - https://support.ruckuswireless.com/documents/4144-ruckus-end-of-sale-announcement-for-zonedirector-1200*

One of the Replacement options available to End customers of RUCKUS ZoneDirector 1200/1205 is Unleashed Solution. This document describes how to convert ZoneDirector 1200 access points to Unleashed Access Point.

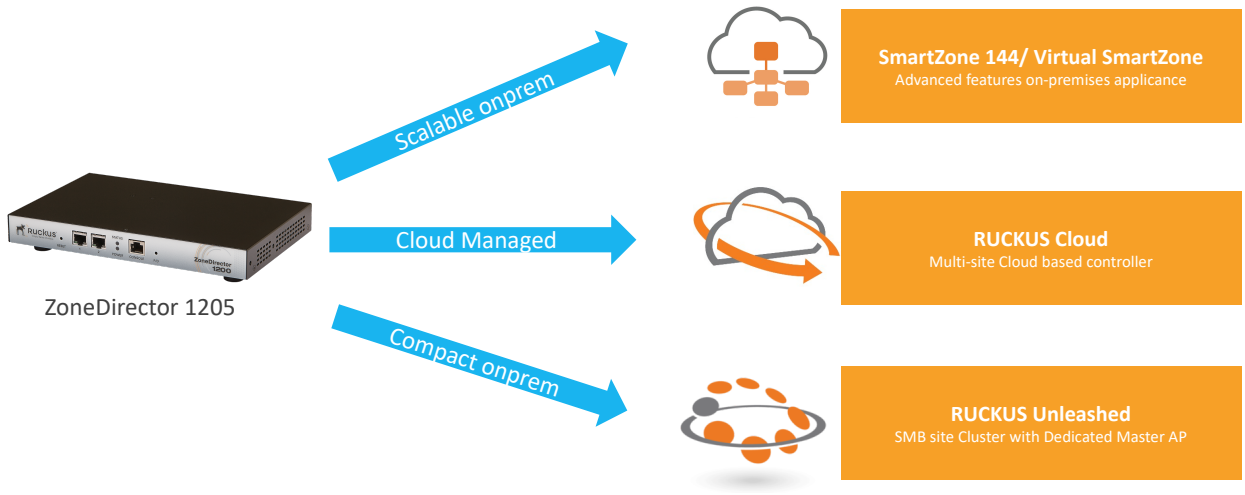


Figure 1: Migration paths available for ZoneDirector 1200/1205

Ruckus Unleashed and Unleashed Multi-Site manager

Ruckus Unleashed enables controller-less Wi-Fi architecture for small business environments with superior performance, lower costs and simplified management. Separate controllers and access point licenses are no longer needed, significantly reducing up-front costs. With a simplified web interface deploying Unleashed is very easy.

Ruckus Unleashed is custom designed to help small business owners grow their business, deliver an excellent customer experience and manage costs while supporting Wi-Fi and a variety of mobile devices with minimal IT staff.

Unleashed access points have built-in controller capabilities, including user access controls, guest networking functions, advanced Wi-Fi security, Zero Touch Smart Mesh and traffic management. Unleashed can monitor, backup/restore, firmware upgrade up to 8 ICX Switches. As businesses grow to multiple sites or a larger scale deployment, Ruckus offers an easy migration path to controller-based Wi-Fi, using the same Wi-Fi access point.

Ruckus Unleashed Multi-Site Manager (UMM) is a new NMS platform for Unleashed, ZoneDirector, P300 bridges. If you have Unleashed networks deployed across multiple small sites, Unleashed Multi-Site Manager is the one-stop solution for management, monitoring and reporting. It is a complete management platform that is intuitive and easy to use. It enables Unleashed networks to be securely monitored and managed from anywhere in the world with a single sign-on.

What's Covered Here

This document is not an exhaustive description of all possible solutions. It focuses on migrating Access points from ZoneDirector 1200 to Unleashed solution. Configuration migration is not part of this How-to Guide. Also, the AP (Access Points) model supported by Unleashed is not explained in this document. Please refer to Unleashed release notes before deciding on firmware version.

External tool in helping Unleashed firmware selection https://indhradhanush.github.io/rksunlfw/

For ZD to Unleashed feature parity visit respective Unleashed version user guide at https://docs.commscope.com/

General Considerations

The following are general considerations and assumptions applicable for all procedures.

- Access Point should be online in ZoneDirector and connected by Wired uplink port.
- If Link Aggregation enabled in Access Point interfaces, it should be disabled before doing migration.

  Watchdog support pack may be required to download the Unleashed Image from Ruckus Support portal. Reach your local Sales team to purchase support pack.

Preparation and Migration

Outline of migration process

Migrating RUCKUS access points from ZD to Unleashed has the following major steps:

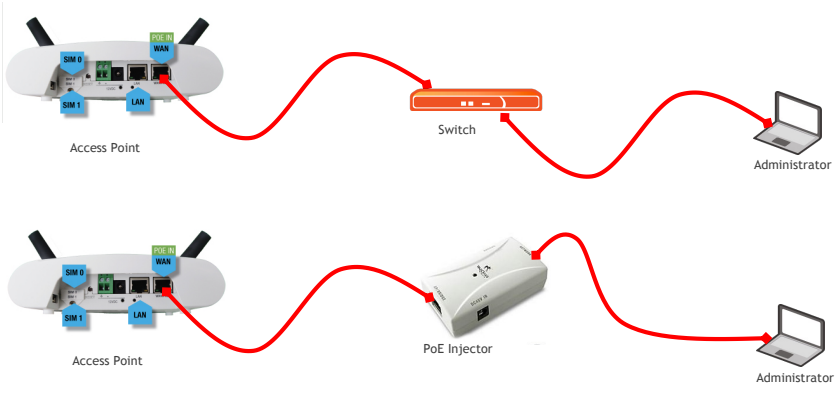
- Prepare the Unleashed Master AP by installing Unleashed firmware into 1 AP and finishing initial setup.
- Convert ZD managed APs image to Unleashed and let APs discover Unleashed Master to join the cluster.

> *ZoneDirector managed AP runs the same version firmware as ZD firmware version e.g., 10.5.1. Similarly, Unleashed Master and Member APs run same version firmware e.g., 200.10, To move an AP from ZD to Unleashed, a firmware change is required from ZD code to Unleashed code.*

Preparing Unleashed Master

Unleashed Solution is a Cluster based solution, in which one of the AP is selected as "Master" which provides the configuration master file to all the member APs of the cluster.

1. Obtain the correct unleashed image onto your PC for your AP model at https://support.ruckuswireless.com/software?filter=82#firmwares
2. Select the AP. You may pick one of the ZD-Managed AP and change firmware to Unleashed and dedicate it as Master. Alternatively, you may pick a new Unleashed AP and dedicate it as Master. In this following steps we are going to pick an existing ZD-managed AP and change its firmware to Unleashed. While selecting an AP it is recommended to choose higher end model such as R750 and R850 as dedicated master.
3. Connect PC and AP - You will need to power the AP externally via a power adapter or via an inline power injector and connect AP's WAN port to PC via Ethernet cable, or with a PoE switch powering the AP and only your PC connected. ZD should not be discoverable back by AP.



4. Factory default the AP by holding in the reset button for 10 seconds. This will reset the APs IP address to 192.168.0.1.
5. Configure a 192.168.0.x (other than .1) on the PC Ethernet interface: Eg. IP address 192.168.0.20 and subnet mask 255.255.255.0. Remember to change the auto IP address setting back when done working with the AP

6. If AP is powered up, you should be able to point a browser to 192.168.0.1 and get a connection. In case you could not get access to the UI, SSH into the AP CLI using its default IP and credentials (super/sp-admin) and enable HTTP/HTTPS.

```
rkscli# set http enable
rkscli# set https enable
```

7. Log into Web GUI using the default username and password (super/sp-admin), if not changed via CLI.
8. Navigate to the Maintenance -> Upgrade page
9. Click on the "Local" Upgrade Method and browse to where you have the 200.x.x.x image loaded and then click the “Upgrade" button.
10. Once AP is upgraded to the Unleashed firmware. Perform a factory reset to clean remnants of ZD from the Access point and reboot the AP.
11. After resetting Unleashed AP should provide Configure-Me SSID. Connect to it and install Unleashed. Follow instruction in this video for installation instructions:

    Web GUI: https://www.youtube.com/watch?v=koUNH9OaadQ or https://www.youtube.com/watch?v=z4zbJcBSuuw

    Mobile app: https://www.youtube.com/watch?v=4__1rnxiU6g

Procedures of Migration

Deploying additional Unleashed member APs is simply a matter of connecting them via Ethernet to the same Layer 2 network 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.

All the APs can be migrated from ZD to Unleashed by the same method we have outlined in previous section “Preparing Unleashed Master” (except step 11, since second AP can auto discover Master and get configuration). To migrate multiple APs at once, the following two procedures available:

1. Zone Director’s Remote CLI tool
2. External Tool: Crossbreeder

Both methods do not retain any configuration including WLAN (Wireless LAN) and login configuration.

Procedure 1: ZoneDirector’s Remote CLI tool

An inbuilt Remote CLI tool of ZD to issue command to all/select ZD-managed Access points. Using this tool an administrator can configure all or selected APs to download and upgrade to Unleashed firmware without the need to know the IP address, admin username and password of each access points.

Allows to migrate multiple APs, depending on File (FTP/TFTP/HTTP) server, DHCP server and LAN link speed.

All access points are factory reset and no configuration retained.

Any AP disconnected from ZD cannot be upgraded using this method.

Procedure 2: External Tool: Crossbreeder

This procedure describes an AP migration tool, using which ZD APs can be upgraded to an Unleashed firmware and factory reset. This tool requires the knowledge of the IP address, admin username and password of each access points.

Allows to migrate multiple APs, depending on File (FTP/TFTP/HTTP) server, DHCP server and LAN link speed.

All access points are factory reset and no configuration retained.

This procedure requires the list of AP IP addresses to be upgraded to Unleashed firmware.

Procedure 1: Zone Director's Remote CLI tool

Migration of ZD to Unleashed involves full upgrade of access points from ZD's firmware to Unleashed firmware. ZoneDirector Managed Access points can be converted to Unleashed by issuing command 'fw' via ZD's Remote-CLI tool. This tool runs the given command in all or selected access points. The Unleashed firmware will then discover Unleashed-Master using one of the discovery methods or becomes a Unleashed Master, if no other Master found.

Network Diagram

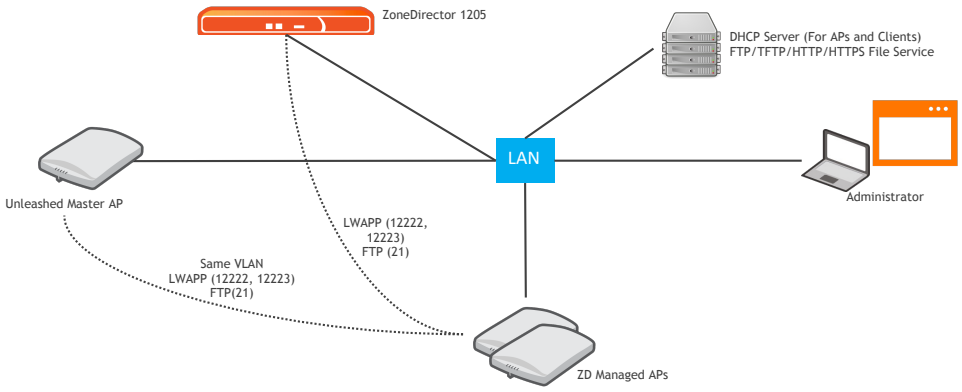


Figure 2: LAN connectivity for ZD to Unleashed Migration

Pre-Requisites for the migration

To successfully follow the steps in this procedure, the following equipment (at a minimum) is needed and assumed:

- ZoneDirector (1200) CLI Admin access
- Verify the Access Point cert status before starting the migration process. Please refer to the Knowledge Base Article (KBA) on Ruckus Support site for procedure to update the cert.

This migration involves upgrade to Unleashed firmware. In order to work successfully, please confirm that the following requirements are met:

- TFTP Server E.g. https://pjo2.github.io/tftpd64/ or use preferred choice of FTP server. APs support TFTP, FTP, HTTP, HTTPS methods for fw upgrade
- ZoneDirector and APs have IP connectivity with support for the following protocols: LWAPP control (should be in place already) and FTP (port 21)
- Unleashed AP Master and Member APs are in same VLAN.

Preparations and Migration

1. Store the Unleashed firmware downloaded in a TFTP Server.
2. CLI commands required to be executed in ZoneDirector to push APs to upgrade to solo intermediate firmware.

```
ruckus(debug)# remote_ap_cli -A "fw set proto tftp"
ruckus(debug)# remote_ap_cli -A "fw set control <AP-
                               Model>_200.12.10.105.100.bl7"
ruckus(debug)# remote_ap_cli -A "fw set host 10.10.10.214"
ruckus(debug)# remote_ap_cli -A "fw update"
ruckus(debug)# remote_ap_cli -A "set factory"
ruckus(debug)# remote_ap_cli -A "reboot"
```

To run these commands only in specific single AP, replace -A argument with -a ap_mac in the command. For e.g.

```
ruckus(debug)# remote_ap_cli -a d8:38:fc:35:d5:b0 "fw set proto tftp"
ruckus(debug)# remote_ap_cli -a d8:38:fc:35:d5:b0 "fw set control <AP-
                               Model>_200.12.10.105.100.bl7"
ruckus(debug)# remote_ap_cli -a d8:38:fc:35:d5:b0 "fw set host 10.10.10.214"
ruckus(debug)# remote_ap_cli -a d8:38:fc:35:d5:b0 "fw update"
ruckus(debug)# remote_ap_cli -a d8:38:fc:35:d5:b0 "set factory"
ruckus(debug)# remote_ap_cli -a d8:38:fc:35:d5:b0 "reboot"
```

Execution screenshots

```
ruckus(debug)# remote_ap_cli -A "fw set control R610_200.12.10.105.100.bl7"
---- Command 'rkscli -c "fw set control R610_200.12.10.105.100.bl7 "'
executed at d8:38:fc:35:d5:b0
Control file: R610_200.12.10.105.100.bl7
OK
---- Command 'rkscli -c "fw set control R610_200.12.10.105.100.bl7 "'
executed at 90:3a:72:24:47:10
Control file: R610_200.12.10.105.100.bl7
OK
---- Command Execution Summary:
         success: 2
         failure: 0
           total: 2
remote_ap_cli -A fw set control R610_200.12.10.105.100.bl7
ruckus(debug)# remote_ap_cli -A "fw set proto tftp"
---- Command 'rkscli -c "fw set proto tftp "' executed at d8:38:fc:35:d5:b0
OK
---- Command 'rkscli -c "fw set proto tftp "' executed at 90:3a:72:24:47:10
```

```
OK

---- Command Execution Summary:

         success: 2

         failure: 0

           total: 2

remote_ap_cli -A fw set proto tftp

ruckus(debug)# remote_ap_cli -A "fw set proto host 10.3.6.25"

---- Command 'rkscli -c "fw set proto host 10.3.6.25 "' executed at
d8:38:fc:35:d5:b0

OK

---- Command 'rkscli -c "fw set proto host 10.3.6.25 "' executed at
90:3a:72:24:47:10

OK

---- Command Execution Summary:

         success: 2

         failure: 0

           total: 2

remote_ap_cli -A fw set proto host 10.3.6.25
ruckus(debug)# remote_ap_cli "fw update"
---- Command 'rkscli -c "fw update "' executed at d8:38:fc:35:d5:b0

fw: Updating rcks_wlan.bkup ...

v54_fw_update: download 10.3.7.228 section=rcks_fw.main image=Image2
ctl_file=R610_200.12.10.105.100.bl7 (/writable/fw/main.cntl) local=0

imghdr.{hdr_len=160, bin_len=15892320}
fw_flash_read_open: kernel open(/dev/ubi1_0) rootfs open(/dev/ubi1_1)
flash id is 0
bdSave: sizeof(bd)=0x7c, sizeof(rbd)=0xd0
  caching flash data from /dev/mtd14 [ 0x00000000 - 0x00010000 ]
  updating flash data [0x00008000 - 0x000080d0] from [0xbeae7a68 -
0xbeae7b38]
_erase_flash: offset=0x0 count=1
Erasing 64 Kibyte @ 0 -- 100 % complete
  caching flash data from /dev/mtd14 [ 0x00000000 - 0x00010000 ]
  verifying flash data [0x00008000 - 0x000080d0] from [0xbeae7a68 -
0xbeae7b38]
**fw(2525) : Completed
fw: Updating rcks_wlan.main ...

Image1 FW check ...

MD5 = 5A4C0E4BC23EF37937A7D495CA92784F

---- Command 'rkscli -c "fw update "' executed at 90:3a:72:24:47:10

fw: Updating rcks_wlan.bkup ...
```

```
v54_fw_update: download 10.3.7.228 section=rcks_fw.main image=Image2
ctl_file=R610_200.12.10.105.100.bl7 (/writable/fw/main.cntl) local=0
imghdr.{hdr_len=160, bin_len=15892320}
fw_flash_read_open: kernel open(/dev/ubi1_0) rootfs open(/dev/ubi1_1)
flash id is 0
bdSave: sizeof(bd)=0x7c, sizeof(rbd)=0xd0
  caching flash data from /dev/mtd14 [ 0x00000000 - 0x00010000 ]
  updating flash data [0x00008000 - 0x000080d0] from [0xbeae7a68 -
0xbeae7b38]
_erase_flash: offset=0x0 count=1


Erasing 64 Kibyte @ 0 -- 100 % complete
  caching flash data from /dev/mtd14 [ 0x00000000 - 0x00010000 ]
  verifying flash data [0x00008000 - 0x000080d0] from [0xbeae7a68 -
0xbeae7b38]
**fw(2525) : Completed
fw: Updating rcks_wlan.main ...

Image1 FW check ...

MD5 = 5A4C0E4BC23EF37937A7D495CA92784F

---- Command Execution Summary:
         success: 2
         failure: 0
           total: 2
remote_ap_cli fw update
ruckus(debug)# remote_ap_cli -A "set factory"
---- Command 'rkscli -c "set factory "' executed at d8:38:fc:35:d5:b0
Factory defaults will take effect after reboot
OK
---- Command 'rkscli -c "set factory "' executed at 90:3a:72:24:47:10
Factory defaults will take effect after reboot
OK
---- Command Execution Summary:
         success: 2
         failure: 0
           total: 2
remote_ap_cli -A set factory
ruckus(debug)# remote_ap_cli -A "reboot"
---- Command 'rkscli -c "reboot "' executed at d8:38:fc:35:d5:b0
OK
---- Command 'rkscli -c "reboot "' executed at 90:3a:72:24:47:10
OK
---- Command Execution Summary:
```

```
          success: 2
          failure: 0
            total: 2
remote_ap_cli -A reboot
ruckus(debug)#
```

3. After about 10-15 minutes (can take longer if the number of APs are large) if administrative PC is on same network as the unleashed master AP, enter the following URL http://unleashed.ruckuswireless.com in your browser. You should be redirected to the Unleashed web UI.
4. If the above doesn't apply to your situation, figure out any AP's IP address, and enter "http://<any AP IP address>" in the URL bar of your browser to access the Unleashed web interface.
5. If there is still no response (and one of the APs' IP addresses is known), you can SSH into the AP and perform the following:

   Type the "get election" AP CLI command. It shows the status of all Unleashed APs, and should display one AP marked as **Master**. Ping that AP's IP address from a device connected to the same network. If the AP is not reachable, maybe there is an access denial policy configured on your network in one of your devices. If the AP is responding, type that AP's IP address in a browser's URL bar and check whether the Unleashed web UI can be displayed.

Start configuring your network from the Unleashed Master web UI.

Procedure 2: External tool: Crossbreeder

Crossbreeder is troubleshooting and automating some simple commonly used tasks for Ruckus APs such as factory reset, update firmware etc. It does not rely on any controller. Instead, it runs through a list of IP addresses supplied by the user to contact each AP directly via SSH. This utility is built for windows and macOS platforms.

Crossbreeder is a 3rd party tool and it can be downloaded from https://github.com/andreacoppini/crossbreeder and no installation needed.

It can be used for bulk AP firmware upgrade and bulk 'set scg ip <ip>' commands provisioning in case mDNS, DHCP, DNS based provisioning options are not available. Please note, admin's computer running Crossbreeder should be able reach Access point's IP address & SSH port.

Network Diagram

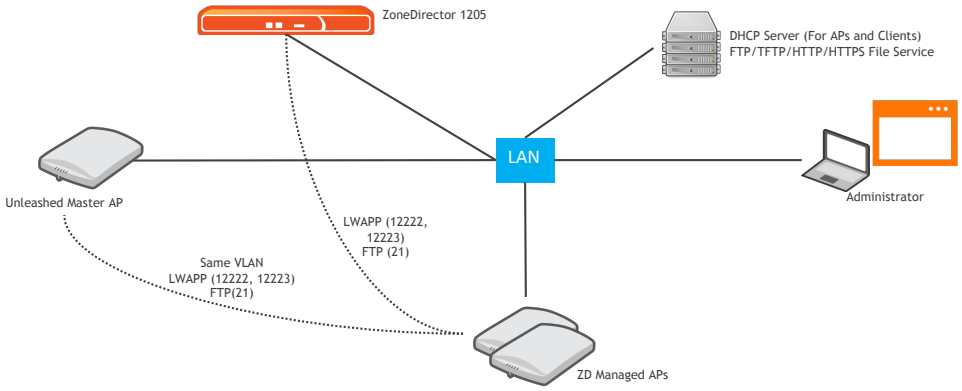


Figure 2: LAN connectivity for ZD to Unleashed Migration

Pre-Requisites for the migration

To successfully follow the steps in this method, the following equipment (at a minimum) is needed and assumed:

- Verify the Access Point cert status before starting the migration process. Please refer to the Knowledge Base Article (KBA) on Ruckus Support site for procedure to update the cert.

This migration is a multiple stage process that involves upgrade to solo firmware. In order to work successfully, please confirm that the following requirements are met:

- TFTP Server E.g. https://pjo2.github.io/tftpd64/ or use preferred choice of FTP server. APs support TFTP, FTP, HTTP, HTTPS methods for fw upgrade
- DHCP Server, DNS Server for network services
- Administrator's PC/Laptop's IP reachability to all the target APs.

Preparations and Migration

1. Store the Unleashed firmware downloaded in a TFTP Server.
2. Download the AP list from ZD, Download Crossbreeder-template from software.
3. Copy the IP addresses from ZD ap list to Crossbreeder template and upload into Crossbreeder.
4. Populate AP username, password and click go. It should fetch AP details.
5. Select Reset AP to factory default and Reboot AP. Make sure ZD is disconnected from APs.
6. After a few minutes, check AP status by step 3.
7. Uncheck factory default and reboot AP options, Check Change firmware, fill in Server (TFTP/FTP/HTTP/HTTPS) details, Firmware file name from Server. Click Go.
8. While Crossbreeder upgrading, open another Crossbreeder instance, upload csv file, enter username and password, click Go to verify the status of AP's firmware.
9. Once APs are upgraded to Unleashed firmware, they will identify the Unleashed and join cluster.
10. After about 10-15 minutes (can take longer if the number of APs are large) if administrative PC is on same network as the unleashed master AP, enter the following URL http://unleashed.ruckuswireless.com in your browser. You should be redirected to the Unleashed web UI.
11. If the above doesn't apply to your situation, figure out any AP's IP address, and enter "http://<any AP IP address>" in the URL bar of your browser to access the Unleashed web interface.
12. If there is still no response (and one of the APs' IP addresses is known), you can SSH into the AP and perform the following:

    Type the "get election" AP CLI command. It shows the status of all Unleashed APs, and should display one AP marked as **Master**. Ping that AP's IP address from a device connected to the same network. If the AP is not reachable, maybe there is an access denial policy configured on your network in one of your devices. If the AP is responding, type that AP's IP address in a browser's URL bar and check whether the Unleashed web UI can be displayed.

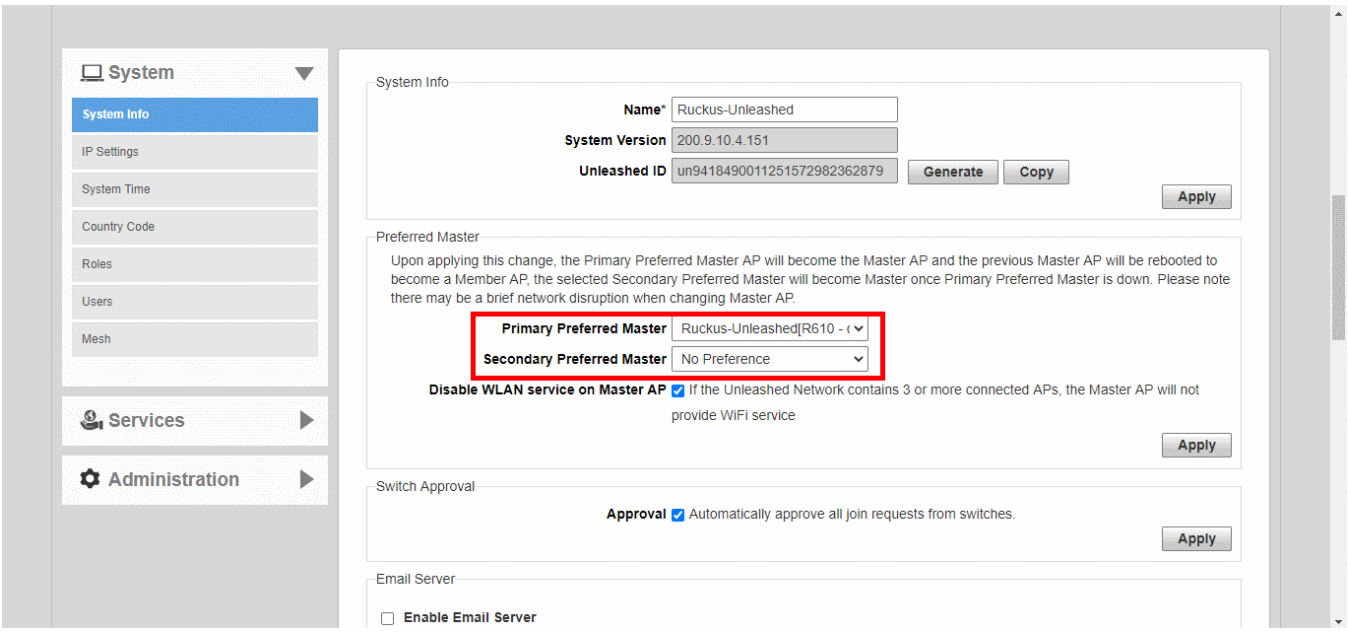
Start configuring your network from the Unleashed Master web UI.

Further Recommended Configuration

Preferred Master

Unleashed Solution from version 200.7 supports Preferred Master AP. This setting allows admin to designate primary and secondary preferred APs as Master. By default, first AP that's deployed automatically become master. Once its down, master election will take place.

Configure Primary and Secondary Preferred Master at Admin & Services -> System -> System Info -> Preferred Master Section



From 200.9, Unleashed allows configuration of up to two preferred Master APs. If the primary preferred Master AP is offline, the secondary preferred Master will assume the Master role. When the primary preferred Master returns online, it will resume the role again once it rejoins the Unleashed network.

Disable WLAN Service Master AP

This feature allows an admin to set the Master AP to focus on controller tasks only. When enabled, the Master AP provides only controller functionality and does not provide WLAN services. This takes off the load from Master and focus on controller functionality.

Introduced in Unleashed version 200.9

Management Interface

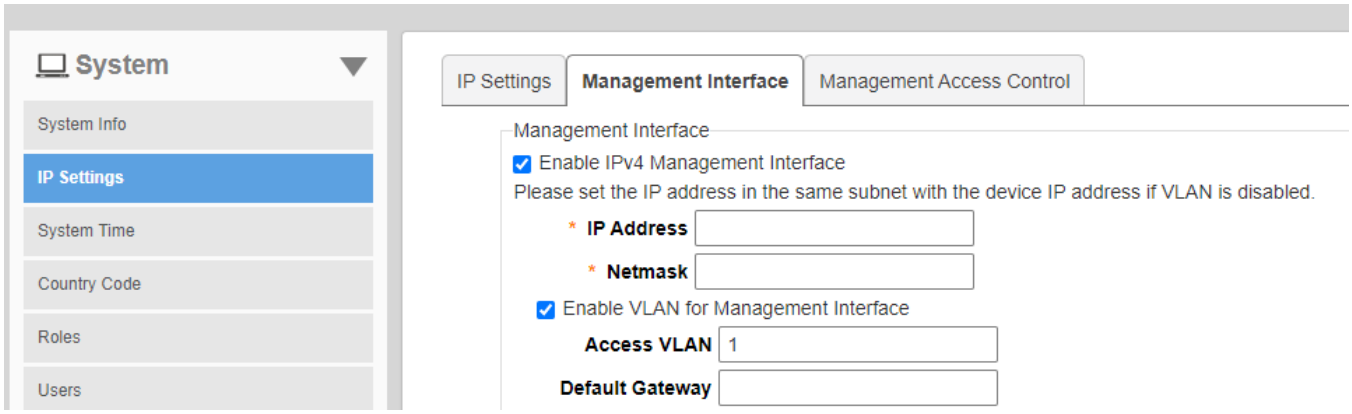
The Management IP address can be configured to allow an administrator to manage the Unleashed network from a single IP address, regardless of which Unleashed AP is currently the Unleashed Master AP.

The Management IP can be reached from anywhere on the network as long as it is routable via the default Gateway configured in Device IP Settings. Then, you only have to remember one IP address.

Introduced in Unleashed version 200.2

Management VLAN

This adds ability to assign VLAN ID to Management VLAN which permits management interface to reside on different VLAN from client traffic network



Introduced in Unleashed version 200.10

Ref: https://docs.commscope.com/bundle/unleashed-200.10-troublshootingref/page/GUID-06BD65BC-B300-4F74-8285-4F785075D761.html

Management ACL

Adds ability to assign Access Control List (ACL) to the management interface for enhance security.

Introduced in Unleashed version 200.10

How to configure: https://www.youtube.com/watch?v=PgHU1GXXl1s

Summary

Unleashed provides a controller-less option for small to medium-sized Wi-Fi deployments where up to 128 access points can be deployed in a self-healing, redundant wireless network with no controller required, while still providing many of the enterprise-class features that traditionally required a Ruckus WLAN controller (e.g., ZoneDirector or SmartZone controller).

Unleashed access points have built-in controller capabilities including user access controls, guest networking features, advanced Wi-Fi security and traffic management. As businesses grow to multiple sites or a larger scale deployment, Ruckus offers an easy migration path to cloud-based or controller-based Wi-Fi, using the same Ruckus access points.

This guide will help you in upgrading your ZoneDirector Access Points to Unleashed and from there you can use various technical resources available at below link to build your Unleashed Network.

https://docs.commscope.com/bundle?labelkey=unl-200.12&labelkey=&labelkey=enterprise-network&labelkey=unl&name_filter.field=title&name_filter.value=&rpp=10&sort.field=title&sort.value=asc#

Further Reading and References

Ruckus Best Practices, Guides, and TechNotes:
https://support.ruckuswireless.com/product_families/22-ruckus-best-practices-guides-and-technotes

Knowledge base articles:
https://support.ruckuswireless.com/answers?search_format=coveo#sort=relevancy

FAQ Ruckus AP certificate refresh:
https://support.ruckuswireless.com/articles/000005390

Ruckus Firmware Selector: https://indhradhanush.github.io/rksunlfw/

Unleashed AP not registering with Master AP: https://support.ruckuswireless.com/articles/000005680

How to force Standby-Master Role in Unleashed: https://support.ruckuswireless.com/articles/000006295

Connecting new unleashed AP to Master if there is no DHCP in the network:
https://support.ruckuswireless.com/articles/000006013

Can I setup Ruckus Unleashed network remotely?: https://support.ruckuswireless.com/articles/000005204

Ruckus Unleashed Product page: https://www.commscope.com/product-type/enterprise-networking/control-management/controller-less/controller-less/

Terms of Use

Third Party Websites and Services. This document contains links to Internet sites and services maintained by third parties. These links are provided for your reference only. We do not control, operate or endorse in any respect information, products, or services on such third-party sites and are not responsible for such information, products, or services. Many third-party sites and services have their own terms of use and privacy policies that differ from ours. This Agreement and the Privacy Policy only apply to our Site and do not apply to any other site or service.

For full Terms of Use visit https://support.ruckuswireless.com/TOS

RUCKUS solutions are part of CommScope's comprehensive portfolio for Enterprise environments (indoor and outdoor).

We encourage you to visit commscope.com to learn more about:

- RUCKUS Wi-Fi Access Points
- RUCKUS ICX switches
- SYSTIMAX and NETCONNECT: Structured cabling solutions (copper and fiber)
- imVision: Automated Infrastructure Management
- Era and OneCell in-building cellular solutions
- Our extensive experience about supporting PoE and IoT

www.ruckusnetworks.com

Visit our website or contact your local RUCKUS representative for more information.

RUCKUS®
COMMSCOPE