



RUCKUS Access Point Getting Started Guide

This Getting Started Guide provides getting started information for version 104.x and later RUCKUS base image access points (APs).

This document assumes familiarity with the RUCKUS ZoneFlex (ZF), ZoneDirector (ZD), SmartZone (SZ), and Unleashed Multisite Manager (UMM) product lines and the features of earlier releases.

NOTE: For RUCKUS APs running version 104.x and later, please be advised that:

- The RUCKUS AP may send a query to RUCKUS containing the AP's serial number. The purpose is to enable your AP to autonomously connect with a wireless LAN controller operated by your choice of cloud service provider. Ruckus may transmit back to the AP the Fully Qualified Domain Name (FQDN) or IP address of the controller that the AP will subsequently attempt to join. •
- Please be advised that this information may be transferred and stored outside of your country of residence where data protection standards may be different.

CERTIFICATE CHANGES

Beginning in November 2016, the existing default SSL device certificate on RUCKUS APs will expire. RUCKUS has been rolling out replacement certificates on APs since 2015. Build 104 makes the new replacement certificate the default SSL device certificate. All APs shipped from RUCKUS with release 104 and later will have the new replacement certificates for SSL authentication with SmartZone controllers.

Due to this change, APs with release 104 may not be able to join some older versions of SZ software. To address this limitation, the SZ has to be upgraded to 3.1.2 or later.

The certificate expiry will require all APs to have the new replacement certificates loaded and made default to be able to join SZ with certificate check beyond November 2016. If, after November 2016, the AP is not able to join SZ, please contact RUCKUS Support for assistance.

Standalone or Unleashed Multisite Manager-Managed Operation

RUCKUS APs are shipped from the factory with a single firmware image, referred to as the "base image." APs with the base image can only operate in standalone mode with or without a Unleashed Multisite Manager.

Controller-specific features (such as Smart Mesh networking) are unavailable when the AP is running a standalone AP base image.

Refer to the RUCKUS Indoor Access Point User Guide or the RUCKUS Outdoor Access Point User Guide for instruction on how to configure the AP for standalone and/or Unleashed Multisite Manager-managed operation.

Controller Management

In addition to standalone and Unleashed Multisite Manager, ZoneFlex APs can also be managed by RUCKUS ZoneDirector or SmartZone controller platforms. When the AP discovers one of these controllers on the network, the AP downloads the associated controller-specific image and replaces the base image with the controller-compatible AP firmware.

"Configure.me" SSID

Beginning with AP base image release 110.0, in the "configure.me-XXXXXX" SSID, where XXXXXX is the last 6 digits of the MAC address using the serial number as the WPA key. This SSID is not set up for DHCP and the AP is statically set to 10.154.231.125. So the client must be on the same subnet as that AP.

RUCKUS Cloud Discovery

RUCKUS Cloud Wi-Fi is WLAN Management-as-a-Service that enables enterprises with limited IT resources to easily set-up, monitor, and manage a high-performance multi-site WLAN of any size, without compromising on Wi-Fi performance.

Beginning with Release 104.0, all RUCKUS 802.11ac APs have the ability to discover and register with a RUCKUS Cloud controller (note that 802.11n APs do not have this capability). 11ac APs with 104 image will use secure HTTPS to query the AP Registrar to discover the remote/cloud controller. If found, the AP will utilize secure mechanisms (e.g., SSH port 22 and HTTPS port 11443) to communicate with the remote vSZ/Cloud controller to connect, and download firmware.

The AP will probe the AP Registrar more often in the first 14 days after initial power-up, and after that, less frequently. Once the AP finds a controller (ZD, SZ, or Cloud), it will no longer look for the AP Registrar.

NOTE: If APs are intended for management by RUCKUS Cloud controller, and you have any other RUCKUS controller on your local network, you must disable the option to "Automatically approve all AP join requests" from the controller UI before connecting the AP to the network. If not, the AP will register with the local controller first and will be unable to discover RUCKUS Cloud.

SmartZone AP Discovery Process

SmartZone controllers running version 2.5 and later include an LWAPP2SCG utility for migrating RUCKUS APs to SmartZone control.

RUCKUS APs running version 104.x and later can discover SmartZone controllers without the need to enable the LWAPP2SCG service on the controller and open ports 12223 and 21 on any firewalls or NAT devices between the controller and the APs.

NOTE: Some older APs may not be able to discover an SZ controller using this discovery process. If you encounter this issue, you have two options:

- First upgrade the AP to base image 104 or later.
- Enable LWAPP2SCG service on the SZ, and open ports 12223 and 21(if needed).

Controller Discovery Methods

There are four methods by which an AP can discover a (ZD or SZ) controller:

- *Method 1: Controller Discovery Using L2 Subnet*
- *Method 2: Controller Discovery Using DHCP*
- *Method 3: Controller Discovery Using DNS*
- *Method 4: Manually Setting the Controller IP Address in the AP Web Interface*

Method 1: Controller Discovery Using L2 Subnet

When the AP is powered on and connected to the same Layer 2 IP subnet as a controller, the AP looks for any SZ or ZD controller. It continues searching for a controller until it finds one, until the RUCKUS AP Registrar service assigns it a controller, or until the installer logs into the AP web interface and configures the controller IP address manually, or until the discovery agents are disabled on the AP.

SZ: When the AP finds an SZ controller on the same subnet and the controller is configured to automatically approve APs, the AP automatically updates the base image with the controller-compatible firmware image.

ZD: When the AP finds a ZD controller on the same subnet and the ZD controller is configured to add APs with the base image,

the AP automatically downloads the ZD-compatible firmware image.

NOTE: Ensure that "Automatically approve all join requests" is enabled on the Configure > Access Points > Access Point Policies page.

NOTE: If multiple SZ and ZD controllers exist on the network, the AP will attempt to associate with an SZ controller first before associating with a ZD controller. If it does not discover an SZ controller, it will begin searching for a ZD controller after a pause of about 30 seconds.

Method 2: Controller Discovery Using DHCP

If your APs will be deployed on different subnets from the controller, you can use DHCP (Option 43) or DHCPv6 (Option 17 or 52) to allow the AP to discover the controller when it boots up, upon requesting an IP address from the DHCP server.

SZ: Enter DHCP Option 43 Code 6, DHCPv6 Option 17 Code 6, or DHCPv6 Option 52.

ZD: Enter DHCP Option 43 Code 3, DHCPv6 Option 17 Code 3, or DHCPv6 Option 52.

Refer to the SZ or ZD user documents for instructions on how to configure your DHCP server to automatically provide the controller address to the AP using DHCP.

NOTE: For SmartZone, IPv6 discovery takes priority if both options are configured.

Method 3: Controller Discovery Using DNS

If your APs will be deployed on different subnets from the controller, you can also use DNS to allow the AP to discover the controller when it boots up.

Refer to the SZ or ZD user documents for instructions on how to configure your DNS server to automatically provide the controller address using DNS.

SZ: ruckuscontroller.<domain>

ZD: zonedirector.<domain>

Method 4: Manually Setting the Controller IP Address in the AP Web Interface

1. Go to **Administration > Management** page in the AP web interface.
2. Click **Set Controller Address Enabled**, then enter a primary controller IP address and optionally, a secondary controller IP address, and then click **Update Settings**.

FIGURE 1 Sample Administration > Management Page



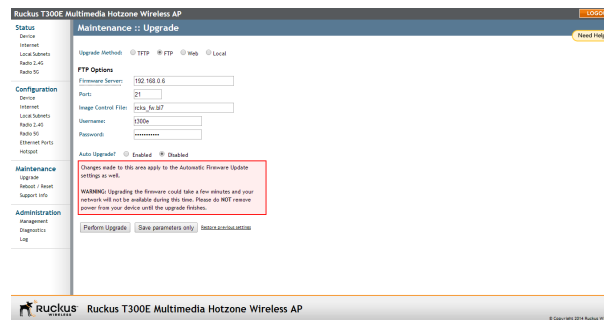
Returning the AP to the Base Image

After an AP has been upgraded to a controller-specific image as described above, you can return it to standalone/Unleashed Multisite Manager operation by upgrading the firmware back to a standalone AP base image.

Upgrade Information

To manually upgrade/downgrade the AP firmware, go to **Maintenance > Upgrade** in the AP web interface. Refer to the *RUCKUS Outdoor Access Point User Guide* or the *RUCKUS Indoor Access Point User Guide* for instructions on how to upgrade the AP firmware.

FIGURE 2 Sample Maintenance > Upgrade Page



NOTE: Once the upgrade (or downgrade) is complete, you must reset the AP to factory defaults, and log in again using the factory default user name and password (un: super; pw: sp-admin, IP address: 192.168.0.1) to configure the AP for standalone operation.

© 2022 CommScope, Inc. All rights reserved.

ARRIS, the ARRIS logo, COMMScope, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, and the Big Dog design are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.