www.ruckuswireless.com

Ruckus Wireless™ SmartZone Controller™

What's New in Release 3.5

Ruckus Wireless, Inc.
350 West Java Drive
Sunnyvale, CA 94089 USA

Telephone (650) 265-4200
Fax (408) 738-2065

Contents

Ruckus Wireless, Inc.
350 West Java Drive
Sunnyvale, CA 94089 USA
Telephone (650) 265-4200
Fax (408) 738-2065

About This Document

This document provides a high level overview of the different features and capabilities introduced in the 3.5 release of the SmartZone Controller platforms. This document will help you understand the context in which the features operate, the key highlights of the features, as well as limitations and benefits of the features to the customer or service provider.

This document does not intend to replace other documents that may address the technical specifications of the features and the interface specifications of the features.

The sections that follow provide a quick overview of these features. For additional details, please refer to the *SmartZone Controller Documentation Suite* for Release 3.5.

Ruckus Wireless, Inc.
350 West Java Drive
Sunnyvale, CA 94089 USA
Telephone (650) 265-4200
Fax (408) 738-2065

1. Introduction

This document provides a high-level overview of several key features that are introduced in the SmartZone (SZ) software release 3.5. For detailed descriptions of these features and configuration help, refer to the respective 3.5 documentation guides.

The SZ release 3.5 is applicable to the Ruckus Wireless SmartZone 300, SmartCell Gateway 200, SmartZone 100, vSZ-H, and vSZ-E controller platforms. In this release, the SmartZone controller has a completely new UI with enhancements to visibility and troubleshooting as well as streamlined monitoring and configuration workflows as well as several UI-related features. Behind the new UI are many architectural enhancements that improve scalability, operations, and data access. For a complete list of supported access point models, refer to the *SmartZone 3.5 Release Notes*.

2. New Controller Model – SZ300

With the release of 3.5, we are introducing a new SmartZone appliance called the SmartZone 300 (SZ300). SZ300 is designed as the next generation carrier-grade controller with performance exceeding the SCG200. With separate control, management, and data planes, each SZ300 has 2x 10Gbps data planes, as well as 6x 1Gbps ports for management, control, and cluster support.

3. Redesigned UI

Along with system architecture changes, 3.5 has a completely redesigned and optimized UI experience. Look and feel have been modernized, menus have been consolidated to simplify monitoring and configuration actions, and many of the workflows are streamlined with contextual information and profile linking. Along with the new look and feel, there are a number of new features highlighted by the new UI, like mapping, health and traffic analysis, troubleshooting, spectrum analysis, and much more.

4. Client Connectivity Analysis

This feature is a troubleshooting tool that allows an administrator to focus on a specific client device and its connectivity status. It starts by detecting APs near the client or where the client is already connected and evaluating AP environmental health (e.g. channel, airtime utilization, client SNR, connection failure %, etc). The tool then tracks the step-by-step progress of the client's connection, through 802.11 stages, RADIUS, EAP authentication, captive portal redirects, encryption key setup, DHCP, roaming, and more (depending on WLAN type). Admins can identify information in each step, like EAP type or IP assigned to the UE, and then can pinpoint where/if a failure occurs during the process.

5. AP Health Analysis

Along with the new UI, AP health analysis is a central theme in 3.5. On the dashboard,

AP status is categorized based on health/performance thresholds defined by an administrator. On a map, APs are color-coded based on this status. We also list the top APs based on key health metrics, like interface latency, airtime utilization, and connection failures—this allows the administrator to focus his/her attention on troubleshooting. From the AP context, admins can analyze specific zones, AP groups, or APs to view historical health trends and compare individual APs against others in its group to look for isolated trouble spots or broader patterns.

6. Map Enhancements

Prior to 3.5, SmartZone had Google maps for outdoor APs. In 3.5, we've dramatically enhanced our mapping functionality to display both sites/floorplans as well as APs on the map. Admins can choose an AP to view details like health status, IP address, or other operational metrics, or admins can view a floorplan to see AP status and details across that floorplan. APs are color-coded by status, and administrators can overlay operational data—like operating channel, traffic, client count, airtime utilization—for each AP on the map.

7. Multi-Zone Support in SZ100/vSZ-E

Prior to 3.5, SCG200 and vSZ-H had a system hierarchy with domains, subdomains, and zones. In 3.5, we're introducing zones to the SZ100 and vSZ-E platforms. Zones allow administrators to segment the network into distinct operational groups. This allows for separation of profiles like WLANs and policies. Admins can also upgrade AP zones independently from the controller software and utilize AP releases going back N-2 releases. Zones can operate in different firmware versions and with different country codes.

8. MSP Domain Enhancements

This releases introduces a new domain concept called a "partner domain" (or an MSP domain). MSP use cases often dictate that each of the MSP's tenants/customers has a siloed set of configurations, profiles, and system objects, which are not shared with other tenants. In prior releases, we had either system-level or zone-level objects; with the introduction of operator domains, we have moved the majority of system-level objects into the operator domain so as to provide segmentation, privacy, scalability, and flexibility in implementations. This change alleviates some of the operational requirements of MSPs.

9. Enhanced Admin RBAC

The 3.5 administrative role-based access control has been refined to improve usability and simplify the creation of function-specific administrative roles. It is now easier to create administrators and attach them to predefined or custom admin roles, and it is easier to define limited-permission roles like modify or read-only.

10. vSZ-D Enhancements

In this release, we continue to improve scale and flexibility of our virtual data plane (vSZ-D). We're scaling up to 10 vSZ-Ds per vSZ and increasing the cluster count to 40. Admins will also be able to configure zone affinities, steering individual zones to one or more specific vSZ-Ds. We have also added vSZ-D support for DHCP/NAT, northbound L2oGRE tunneling, CALEA monitoring, and L3 roaming using Ruckus GRE tunnels.

11. DHCP/NAT in AP

In highly distributed environments, particularly those with only a few APs per site, we're introducing the ability for an AP or a set of APs to provide DHCP/NAT support to local client devices. This simplifies deployment by providing all-in-one functionality on the AP, which eliminates the need for a separate router and DHCP server for each site. It also eases site management by providing central control and monitoring of the distributed APs and their clients.

12. ZD to SZ Migration

The 3.5 release has a built-in ZD-to-SZ migration tool that simplifies the process of migrating ZD-managed APs to the SmartZone. This migration toolset is focused on migrating the APs and preserving operational configurations necessary to maintain AP connectivity, such as IP settings, mesh configuration, management VLAN, and more. It does not provide full migration of ZD configuration into SZ. This tool is initially designed to support SZ and ZD on the same site and may not support every deployment architecture without additional configuration of firewalls and/or port forwarding rules.

13. DPSK Enhancements

DPSK progress continues with new features, scale, and flexibility. In SCG200, vSZ-H, and SZ300, the number of DPSKs has increased from 20,000 to 50,000, with up to 10,000 per zone. SZ100 and vSZ-E are also increased from 10,000 to 20,000, with up to 10,000 per zone. We're also introducing the concept of group DPSKs, which allows a single DPSK to be reused by many devices. There can be up to 64 Group DPSKs in a zone. In 3.5, we also now allow the admin to specify the passphrase for a given DPSK; this is supported both in CSV import as well as manual generation from the UI. Admins can also specify a number-only DPSK, which makes guest scenarios or other "easy entry" scenarios a little more user-friendly. Finally, the CSV format and admin-defined password will now allow for ZD DPSK migration, starting with ZD 10.0, when admins can expor the ZD's DPSK.

14. CALEA Support

Utilizing the data plane of vSZ-D, we're introducing support for lawful traffic intercept, which allows some traffic to flow centrally to a CALEA server for investigation by law enforcement or government agencies. For some network operators, this allows them to

abide by local regulations required to operate a network as a service.

15. Operational Enhancements

Several operational enhancements have been made:

- Improved stats granularity (measurement and reporting intervals)
- New counters/KPIs have been added for better troubleshooting and stats review
- SNMP polling is supported for real-time AP/client stats snapshots

16. Public API Enhancements

Continued expansion of public API support, including:

- Retrieving zone and WLAN details
- AP group override settings
- AP override settings

17. AP Performance Enhancements

Low-level AP performance enhancements have been made to improve speed in tunnel mode WLANs. AP IPsec hardware acceleration has also been implemented to improve IPsec performance.

18. ChannelFly Enhancements

In 3.5, we continue to enhance ChannelFly by adding a cost metric to the channel change logic. The “cost” metric allows the AP to automatically adjust channel change aggressiveness based on client count (before and after a channel change) as well as traffic load patterns.

19. Topology Network View

As a part of the UI enhancement, we have added a topology health view, which allows administrators to view the system hierarchy (domain, subdomain, zone, apgroup) as a tree and to identify nodes in the tree with offline APs or APs that have crossed admin-defined performance/health thresholds.

20. Manual Client Isolation Whitelist

Prior versions of SmartZone allows client isolation whitelist, but the functionality was automatic. The AP would snoop DHCP offers to determine a UE’s IP gateway. Then APs

would only allow traffic to that destination. In 3.5, we've also added the ability for an admin to configure a manual whitelist entry, either to add non-gateway devices (e.g. printer) or to configure additional gateway MAC addresses that may be required for load balancing or other gateway architectures. The isolation whitelist can be auto only, manual only, or auto and manual.

21. Role-Based Policy Enhancements

In SZ 3.5, role policies have been enhanced with new functionality. When a UE/device is assigned to a role, you can now apply role-specific VLANs or VLAN pools. You can also apply a UTP to the role—UTPs in 3.5 have been enhanced with some L7 application policies as well as rate limiting based on L3/4 rules (note that role-based L7 policies will be enforced in a short-term release after 3.5.0). All WLAN types with ProxyAAA authentication now support role-based policy assignment. Admins can also change the precedence of WLAN, device OS, and role policies, which adds flexibility for different use cases.

22. Application Control (Rate Limit and QoS)

L7 application control has been expanded to include both rate limiting and QoS actions. Prior releases supported application deny policies. The L7 policy has now been integrated into User Traffic Profiles (UTP) for a more cohesive point of policy configuration.

23. Spectrum Analysis

3.5 introduces spectrum analysis to the SmartZone platforms. In this release, we support 11n as well as 11ac APs (both Wave1 and Wave2). Spectrum visibility includes real-time amplitude and utilization (i.e. duty cycle) graphs, a spectrum density view, and a swept spectrogram (waterfall) view. The utilization view allows the administrator to define a signal amplitude threshold. For dual-radio APs, when a radio is placed in spectrum mode, it will prevent clients from connecting; however, for APs with three radios, the 3rd radio can provide spectrum analysis of both 2.4 and 5 GHz bands without impacting client connectivity.

24. Bonjour Fencing

This release introduces a new Bonjour management feature called Bonjour Fencing. Fencing allows the admin to control the physical area in which a given Bonjour-based service is discoverable. This is accomplished by mapping devices advertising Bonjour services to nearby APs and allowing only that AP or its neighbors to advertise the Bonjour record. Effectively, this prevents users/devices from discovering Bonjour services that are not nearby, and thus are not relevant to their search.

25. Real-Time Client Health

Alongside all the other UI and health-related enhancements in 3.5, admins can view real-time client SNR and data rate, as well as historical traffic, to help troubleshoot connectivity problems.

26. Block UE After Repeat Auth Failures

As a Denial-of-Service (DoS) prevent measure, 3.5 introduces a feature to temporarily block a UE if it fails authentication too many times in a short period. The feature thresholds (number of failures, span of time to measure failures, and duration of block) are configurable by the administrator. This effectively prevents many authentication cracking attacks or other DoS attacks that consume AP resources.

27. LDAP over SSL

As straightforward as it sounds, 3.5 introduces the ability to support LDAPS, or “LDAP over SSL” connections. In this mode, the LDAP client and server initiate an encrypted session before any LDAP messages are transferred, thus providing an additional layer of data privacy.

28. Manually Block Client

This feature is a workflow improvement that allows administrators to select one or more wireless clients/devices and create a system/zone-wide block on them. This block prevents the UE from connecting to any AP on the system. This can be useful in situations where devices have been stolen or compromised, or in situations where a user has violated some acceptable use policies.

29. TestAAA Role Assignment

The TestAAA function has been enhanced to help the administrator determine which role attributes the AAA server is providing and how that maps to local roles on the SmartZone. This simplifies the deployment testing process by confirming that a user will be assigned to the proper role and policy.

30. Mark Rogues as Known

This functionality gives administrators more control over rogue classification. Some APs that are detected as “rogue,” may not actually be rogue. They may be known neighbors or lab equipment with similar settings. For this reason, admins can now mark detected rogues as known (i.e. safe), which prevents the AP from taking action against these discovered APs.

31. IPv6 Support for WSON

WSON (Wireless Self Optimization Network) is an architectural enhancement introduced in SZ 3.4 that allows for fast roaming and load balancing by sharing data between APs. In 3.5, SmartZone adds support for WSON in APs using IPv6 addressing—in 3.4, WSON supported IPv4 only.

32. Additional Enhancements

Many other enhancements have been made as well, including:

- Customized NAS-IP-Address in SCG-Radius
- Support Acct-Session-ID as a session key in COA/DM
- EPON/GPON status display on SZ UI
- WISPr with MAC bypass and DVLAN
- Protocol support for the Multiband Operation specification