RUCKUS® SMARTZONE

Ultra-scalable and resilient network controllers for network-as-a-service providers and large enterprises

BENEFITS

Easily host competitive managed service offerings
Multi/tiered-tenant, tenant/sub-tenant segmentation, and virtual/physical network controller options support sophisticated Network-as-a-Service offerings with complex service levels.

Scale networks on-demand
With Virtual SmartZone, customers can deploy private clouds on AWS Cloud, Azure Cloud, and Google Cloud Platform, minimizing up-front costs and maximizing deployment and scaling flexibility.

Bolster network resiliency
SmartZone protects against catastrophic failures by providing intra-cluster, and inter-cluster failover with cluster-redundancy and active/active clusters that yields higher availability than hot standby.

Personalize tenant dashboards
Comprehensive APIs make it easy for third-party applications to provision, configure and monitor access points and switches. Build branded and customized dashboards for tenant administrators.

Automated network discovery and provisioning
Auto-discovery and auto-configuration of APs and switches reduce guesswork, lowers the cost of administration, and speed up deployment using predefined rules.

Pay-as-you-grow
SmartZone network controller can manage up to 10K access points, 150K clients, and up to 20 Gbps of throughput depending on the model. With perpetual, migratable, and per-AP/per-switch licenses, you get a better return on your investment.

Expedite troubleshooting
With Visual Connection Diagnostics, IT can speed-up and simplify troubleshooting and wireless client problem resolution. IT can also detect and respond more quickly to network degradation with SmartZone's dashboard metrics.

Enable next-gen Wi-Fi roaming
Manage hotspot and Wi-Fi roaming between owned and unowned networks with HotSpot 2.0 Release 3, RadSec security, and Google Orion support.

Enjoy additional advanced features
SmartZone also supports converged wired-wireless management, content filtering, rogue AP detection and mitigation, client load balancing, airtime fairness, guest onboarding, capacity-based admission control, and more.

RUCKUS SmartZone network controllers simplify the complexity of scaling and managing wired switches, and wireless access points through a common interface to support private-cloud network-as-a-service (NaaS) offerings in addition to general enterprise networks. All physical and virtual SmartZone appliances support network configuration, monitoring, provisioning, discovery, planning, troubleshooting, performance management, security, and reporting. SmartZone's single, user-friendly web interface handles network visibility from the wireless edge to the network core and enabled IT administrators to perform day-to-day management tasks, troubleshoot user connectivity problems, and define and monitor user and application policies without requiring advanced network skills and CLI expertise.

MULTI-SERVICE AND MOBILE NETWORK OPERATORS

Operator deployments are among the most complex in the world, with some operators simultaneously delivering public access Wi-Fi, and Wi-Fi as a managed service to their enterprise and small business customers. Virtual SmartZone – High Scale (vSZ-H) version allows operators to flexibly deploy switches and access points to address these scenarios while working within the unique constraints of the operator's public and private networks.

SERVICE PROVIDERS

Internet service providers are delivering Wi-Fi-as-a-Service (WaaS) and Network-as-a-Service (NaaS) to create new revenue streams while simultaneously simplifying their customer's need to manage an increasingly complex network component. The tiered multi-tenancy vSZ-H enables service providers to implement multi-tier business and operational models across geographic and commercial boundaries.

ENTERPRISES

The need for employees and customers to have the best user experience is driving organizations in every vertical to adopt the best possible network infrastructure. SmartZone 144 (SZ144) and Virtual SmartZone – Essentials (vSZ-E) allow all enterprises to deploy an affordable and highly resilient wired and wireless network to support Bring Your Own Devices (BYOD), media-rich applications, and the IoT. Additionally, SmartZone provides information technology (IT) and operational technology (OT) departments with intuitive, visual tools to centrally manage the end-user experience in distributed and remote offices. SmartZone's active/active redundancy architecture provides the budget flexibility that comes from having no idle capacity.

Audience	Physical	Virtual
Mid to Large Enterprises	SmartZone 144 (SZ144)	Virtual SmartZone - Essentials (vSZ-E)
Operators and Service Providers	SmartZone 300 (SZ300)	Virtual SmartZone - High Scale (vSZ-H)

OPERATIONS, ADMINISTRATION AND MANAGEMENT

Multi-tier tenancy

The administrative hierarchy provides multi-tier tenancy management flexibility for service providers, allowing administrators to create and reuse configuration profiles within domains and zones. Role-based access control (RBAC) with pre-grouped administration permissions makes common roles easier to set up. Define read-only or modify permissions that apply across zones, and easily add new administrator profiles and set permissions that apply across tenants.

Only: vSZ-H

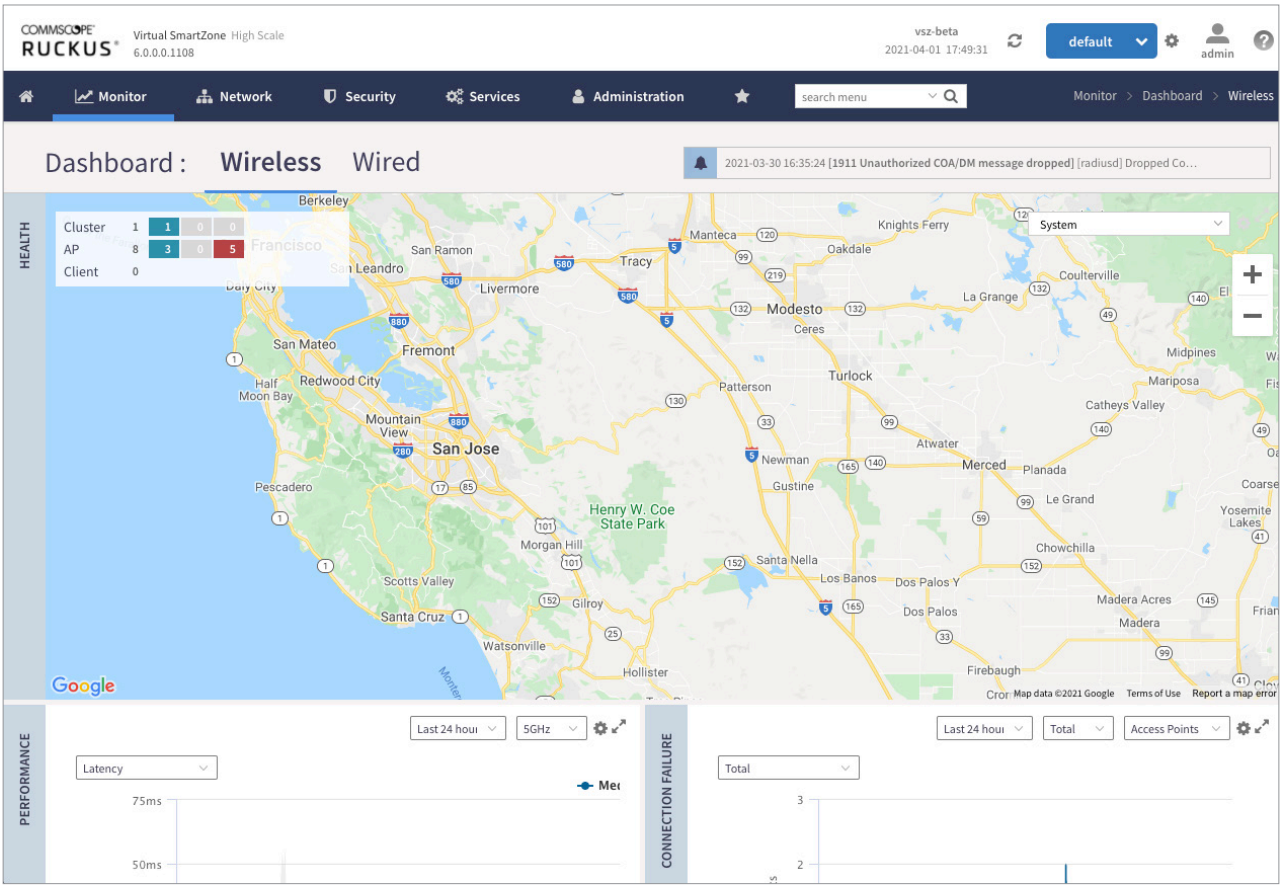
Partner domain

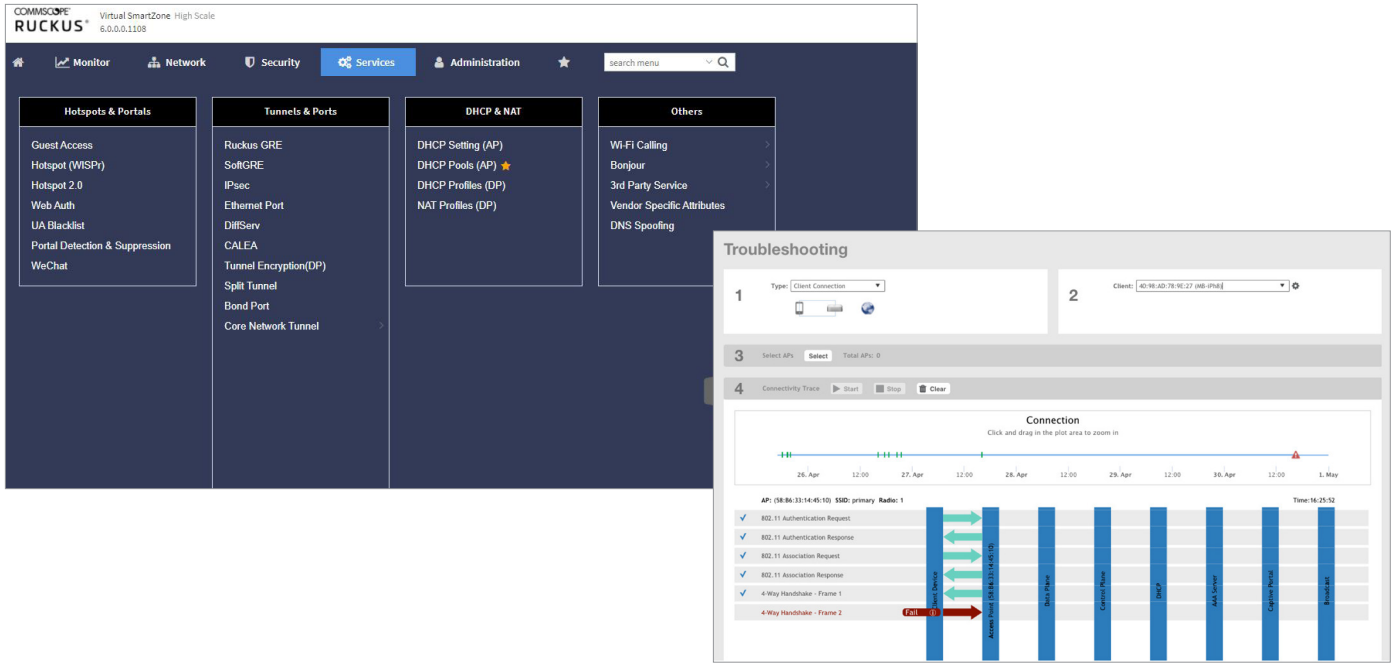
The Partner Domain enables operators to separate tenants with their own unique set of configurations, profiles, and system objects that are not shared with other tenants. This creates a wall between tenants to ensure privacy and alleviate operational headaches associated with tenant management. Also, service providers can personalize the administrative dashboard for their tenants with unique logos and text.

Only: vSZ-H

Administrative dashboard and menus

The Dashboard is a customizable and contextually rich interface that is optimized for large-scale networks. With Search, administrators can quickly find a specific menu, and often used menus can be added to the Favorite menu to quickly perform routine tasks such as AP and switch configuration. Submenus are also organized into groups such as Clients, Troubleshooting, Application Control, Access Control, Wireless, and Wired. Visual settings for the Dashboard personalize network alerts and statistics which are preserved throughout subpages. The topology of the entire network can be viewed in several ways with Topology or Ball views. Additional charts and views include maps, health, traffic analysis, spectrum analysis, and more. The Connection Failure dashboard metric for wireless connections lets administrators check system-wide connection failure trends and identify connection anomalies caused by systematic problems.





Visual connection diagnostics

Visual Connection Diagnostics for wireless clients speeds and simplifies troubleshooting and client problem resolution. This troubleshooting tool allows an administrator to focus on a specific client device and its connection status. An intuitive interface 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, and roaming. Administrators can view each step, like IP address assignment, and pinpoint where in the process a failure occurred. This enhanced visibility helps determine the likely cause of client problems and, based on the failure stage, gives useful guidance for remediation. Visual Connection Diagnostics supports open, PSK, 802.1X, and WISPr networks.

Network management APIs

A large library of well-documented REST-APIs enables 3rd party applications to invoke just about any configuration change presented within the SmartZone OS graphical user interface (GUI) or command-line interface (CLI). This allows IT managers of 3rd party applications to access SmartZone OS functions from within their management systems and issue direct commands without creating error-prone custom scripts.

A full set of near real-time MQTT/protocol buffer data streams enable 3rd party applications to ingest all network data, statistics, and alarms (from the client, AP, switch, WLAN, controller, cluster) with little delay, no fidelity loss, and no need to create a firewall pinhole. These data streams enable the recreation of SmartZone dashboard elements or custom dashboards for internal and external consumption. RUCKUS makes use of this capability to enable its network analytics and reporting software.

Each SmartZone network controller supports access to a complete set of network machine-level metrics enabling it to plug directly into existing automated backend systems and to provide a 'headless' interface for the network infrastructure.

Zone autonomy

Multi-Zone is used to segment the WLAN into independent organizational units. IT can create policies that group AAA, DPSKs, Hotspot portals, Bonjour policies, and WebAuth portals and assign them to one or multiple zones. Different zones can operate using different firmware versions or different country codes.

Administrators can also upgrade AP/switch zones independently from the controller software and manage APs with firmware up to two releases old. IT can update firmware one zone at a time or within a dedicated test zone before upgrading the entire network. Administrators can also group switches into Switch Groups to software upgrade an entire group or monitor the group as a whole and identify top talker ports across the group for example.

Switch CLI configuration

CLI (Command Line Interface) commands for switches can be used through a remote CLI session to a specific switch or via CLI templates that apply a CLI configuration to a group of switches based on predefined policies, or CLI templates can be used to streamline the deployment to multiple devices at the same time.

Multi-language support

10 languages are supported for end-user-facing portals and for network administrators to ease support across the world. Language support is included for: Spanish, Brazilian Portuguese, French, German, Italian, Russian, Simplified Chinese, Traditional Chinese, Korean and Japanese.

Lawful intercept

SmartZone WLAN controllers support lawful intercept of encrypted traffic to maintain CALEA compliance on public or government-owned networks. Enable the mirroring of client traffic to a LIG (Lawful Intercept Gateway) over L2oGRE (Soft-GRE).

SECURITY AND POLICY

URL filtering

URL Filtering for wireless clients allows businesses to create and enforce content policies that protect users from inappropriate and harmful websites while maintaining access to allowed URLs. Policies are granularly applied at a wireless LAN or user group level with override whitelist/blacklist options. Rich dashboards provide real-time visibility into millions of URLs, classified into 83+ categories, being allowed or denied. Additionally, URL Filtering supports Safe Search for Google, YouTube, and Bing.

Automated enhanced client security / DPSK

RUCKUS patented Dynamic Pre Shared Key (DPSK) enhances client security by automating randomized passphrase keys for use with each device. SmartZone supports up to 50,000 DPSKs, with up to 25,000 per zone. Group DPSK, user-specified passphrase, and number-only DPSK further enhance client security in all settings.

Group DPSK allows IT to create a DPSK that can be shared by multiple different devices, with up to 500 Group DPSKs in a zone. Administrators can also specify a number-only DPSK, which makes guest or other "easy entry" scenarios more user-friendly.

DPSK Type	System Max	Domain Max	Zone Max	Comments
Unbound	50,000	25,000	500	Only Unbound DPSKs in the system
Bound	50,000	25,000	25,000	Only Bound DPKs in the system
Group	50,000	25,000	500	Only Group DPSKs in the system
Combination	50,000	25,000	25,000	Keeping the above limits in consideration

WIDS / WIPS / rogue AP detection

SmartZone includes Wireless Intrusion Detection and Prevention System (WIDS/WIPS) functionality, enabling rogue AP detection. Rogue access points exhibiting malicious behavior such as spoofing the SSID or BSSID of a connected RUCKUS AP are prevented from connecting clients to the network.

APs can be categorized as Ignore, Known, Rogue, and Malicious to minimize disruption towards allowed APs or lab equipment, and thus prevent the network from acting against these discovered APs. Classification rules enable rogue AP detection by SSID match, MAC OUI, and RSSI threshold.

Role-based policy management

Granular role-based policies for wireless clients enable the creation of policy groups segmented by user role, domain, location, OS type, certificate status, VLAN, and many more factors. Roles are assigned during the authentication phase of new user onboarding, then VLAN, OS, and L3-7 policies are assigned as desired. Policy enforcement actions include allow, deny, and rate-limit based on VLAN or VLAN pool and L3/L4 Access Control Lists (ACLs).

Hotspot 2.0 / Passpoint

SmartZone creates a powerful network to accept cellular customer traffic. Manage hotspot and Wi-Fi roaming between owned and compliant 3rd party networks with HotSpot 2.0 Release 3 and RadSec security. Hotspot 2.0 is automatic and requires no user intervention after proper device provisioning. SmartZone also supports Google's Orion Wifi initiative. Self-service provisioning can be accomplished by the RUCKUS Cloudpath® security and policy management platform.

Isolation whitelist

Administrators can manually configure a whitelist entry for a wireless device, either to add non-gateway devices such as printers or to allow additional gateway MAC addresses that may be required for load balancing or other functions. The isolation whitelist can be auto-only, manual-only, or auto and manual.

mDNS / Bonjour Management

mDNS broadcast storms are minimized using mDNS / Bonjour Management which detects Bonjour services (such as AirPlay, Apple TV, and other Apple network services) and other custom mDNS- based services such as Chromecast across VLANs and subnets for both wired and wireless networks. SmartZone is preconfigured with common Bonjour service types, making Bonjour service detection automatic.

Bonjour Fencing allows administrators to control the physical area that Bonjour-based services are discoverable. This is accomplished by mapping to nearby APs devices that are advertising Bonjour services and allowing only that AP or its neighbors to advertise the Bonjour record. This prevents users/devices from discovering Bonjour services that are not nearby and thus not relevant to their search.

Two-factor authentication

SmartZone operational security is enhanced with two-factor authentication, requiring administrators or a group of administrators to provide both username/password authentication as well as SMS authentication before login.

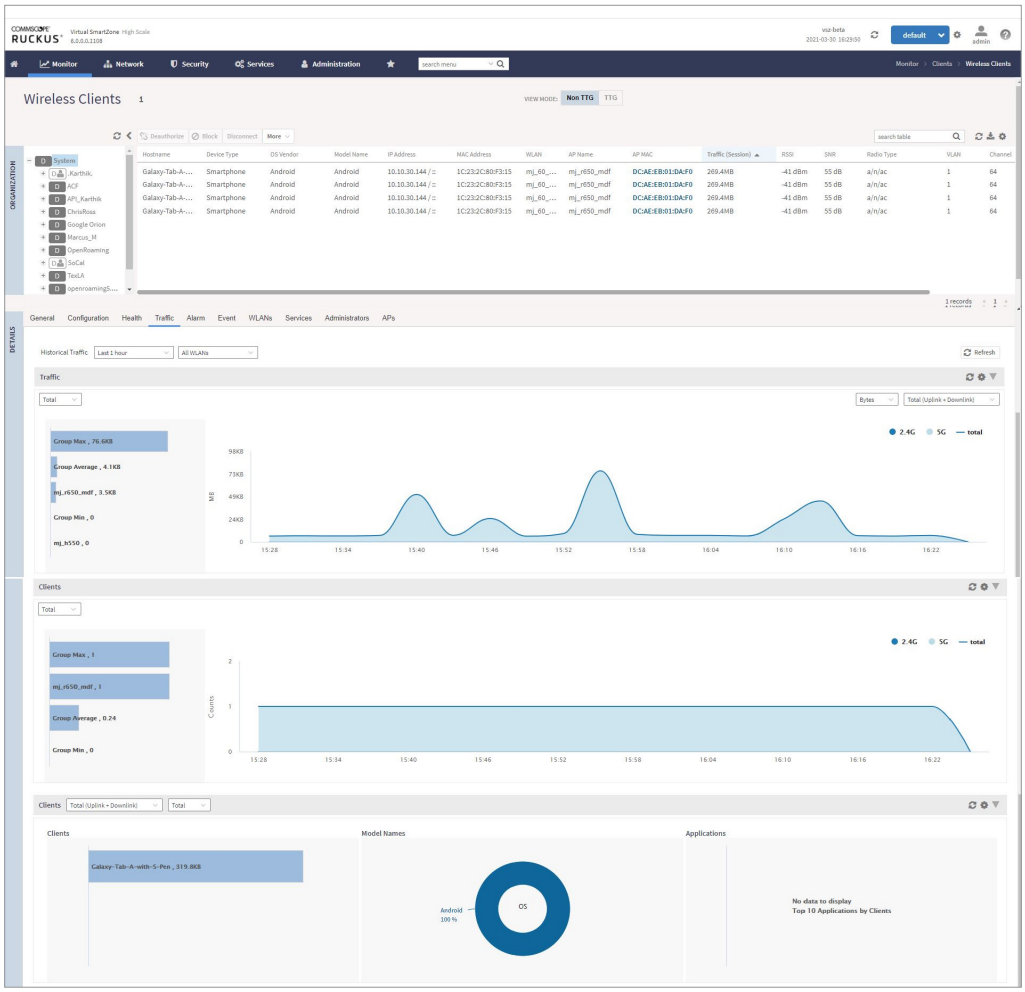
Social login support

Administrators can utilize social media login credentials to connect user devices through SmartZone. The following popular social media login methods are supported: Facebook, Google, LinkedIn, and Microsoft.

NETWORK INTELLIGENCE

Traffic analysis

Traffic analysis displays domain, zone, AP/Switch group, WLAN, and AP traffic and client trends over time. Quickly find the most heavily loaded AP/Switches/Ports or top network users and devices. View client OS types and application consumption for wireless clients. Filter statistics by the band (2.4 GHz, 5 GHz,



or both) and traffic direction (uplink, downlink, or both), and monitor client load over time.

Indoor and outdoor maps

With Maps, centrally view all sites at the same time with Google Maps integration and display sites, floorplans, and APs on the map. Simplify routine checkups of AP health on a site-by-site basis with one click. Inspect the status of APs across floorplans to find online, flagged, and offline APs. View health and traffic data for each AP to evaluate site performance. Administrators can choose an AP to view details like health status, IP address, or other operational metrics. 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.

Layer 7 application visibility and control

Robust Layer 7 application recognition and control for wireless clients pinpoint top applications and top users, among other metrics. SmartZone allows rate-limiting, blocking, and QoS actions by application to support organizational network usage policies. The application signature database is updated independently of SmartZone firmware upgrades, ensuring that administrators can always manage and control the latest applications.

Super-KPIs

Unique network metrics ("super-KPIs") enable IT to more quickly detect and react to potential Wi-Fi user experience degradation. SmartZone proactively monitors a core set of metrics that consistently correlate well with common problems, and presents a summary metric as a starting point for problem isolation. Using aggregate measurements that capture a broad range of problems associated with the Wi-Fi network simplifies troubleshooting by narrowing the scope and location of the problem. These holistic, historical, smart metrics include Latency, Airtime Utilization, and Connection Failure.

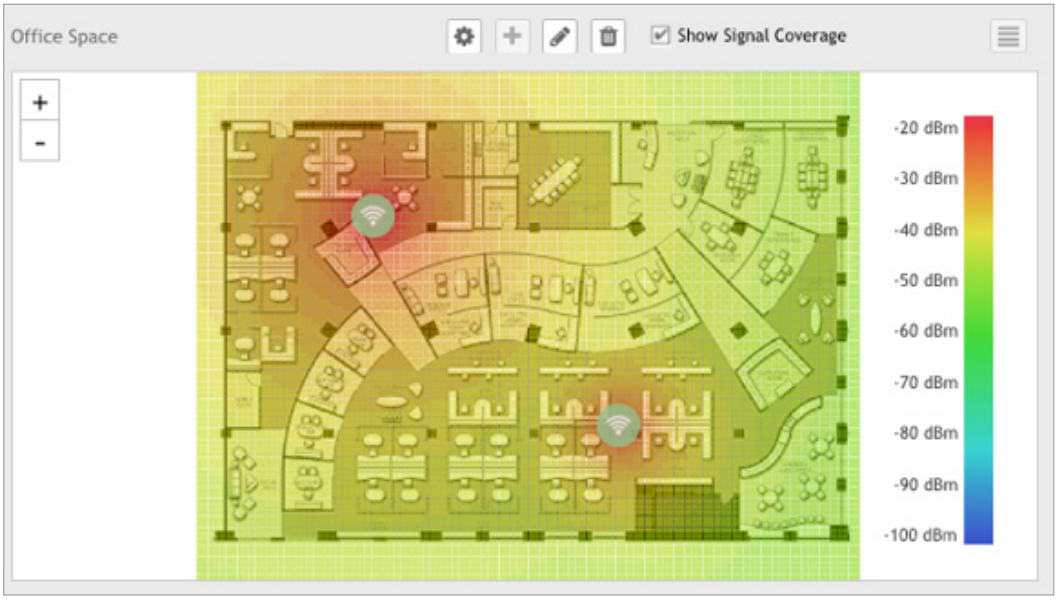
RF Coverage Heatmap

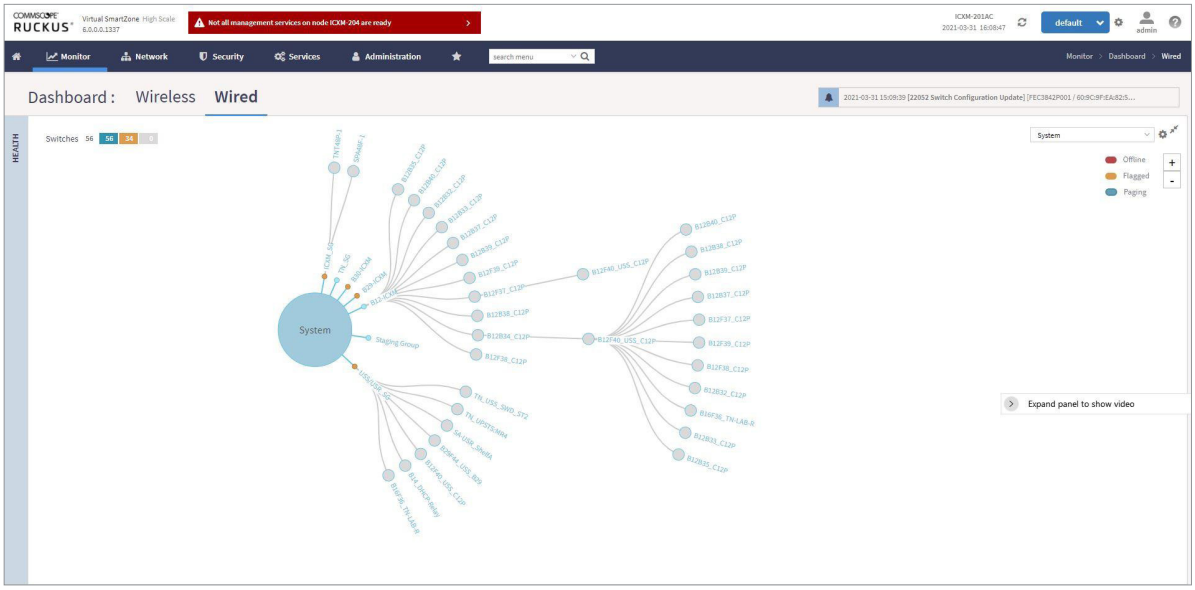
The RF Coverage Heatmap tool visually presents approximated signal strength per AP that is overlaid on top of any imported floor-plan. This enables IT to quickly spot possible AP coverage gaps within the intended area.

AP and switch health

AP health is a key indicator of user experience quality and with SmartZone, this information is presented front-and-center. 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. SmartZone automatically identifies APs that cross performance thresholds and visually ranks the worst-performing APs. With this data and historical trend analysis, admins can easily compare individual APs with groups of APs to look for isolated trouble spots or identify broader patterns.

Switch health monitors switch CPU and memory trends, power supply/fan status and temperature readings, monitor key events and raise alarms based on predefined rules, monitor port status.





Cluster health

Monitor and flag cluster node status and keep critical cluster health alerts highlighted within the Dashboard through status symbols showing Green/ Yellow/Red for each cluster node. Displays historical line charts and allows threshold settings for Cluster Health, spanning CPU, RAM and disk utilization, port/ interface usage, and packet rates.

Client health

Check on real-time client performance metrics, connectivity, and traffic. View client signal-to-noise ratio (SNR) and data rate, as well as historical traffic, to help troubleshoot connectivity problems.

Topology health

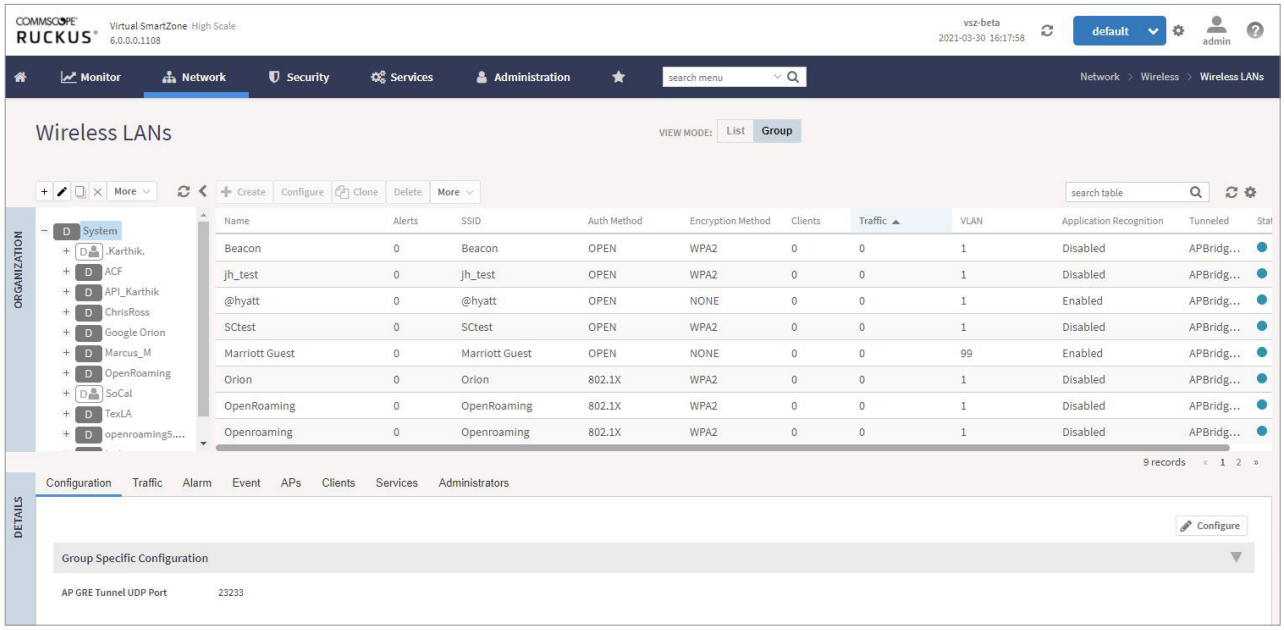
The Topology and Ball view contained within the Dashboard uses a system hierarchy tree to enable easy identification of Wi-Fi problems inside domains, zones, and AP groups. With a Green, Yellow, and Red status indicator, locate offline access points or access points with poor performance.

Spectrum analysis

On-demand real-time spectrum analysis makes use of existing radios within the AP, removing the requirement to have dedicated APs for spectrum reporting. Visualize RF spectrum by real-time energy, real-time utilization, density, energy waterfall, and utilization waterfall. While an AP conducts a spectrum scan, clients are offloaded to nearby APs to minimize connection disruptions. In the case of APs with three radios, the 3rd radio can provide spectrum analysis of both 2.4 and 5 GHz bands without impacting client connectivity. Spectrum Analysis is supported on Wi-Fi 4, Wi-Fi 5 and Wi-Fi 6 APs.

Report generation and export

View rich statistics on subscribers (including client fingerprinting), APs, SSIDs, switches, backhaul (mesh), and the SmartZone cluster itself, with granularity as low as three minutes with 14 days storage. Reports encompassing durations of hours to weeks can be generated for a variety of key performance indicators (KPIs) and exported in multiple formats. For operators seeking richer information RUCKUS Analytics, a cloud service for network analytics and assurance, powered by machine learning (ML) and artificial intelligence (AI), delivers comprehensive visibility into the operation of RUCKUS enterprise networks. The service accelerates troubleshooting and helps IT teams meet their network SLAs. RUCKUS Analytics supports SmartZone and RUCKUS Cloud control and management architectures.



CONNECTIVITY

SmartMesh wireless backhaul

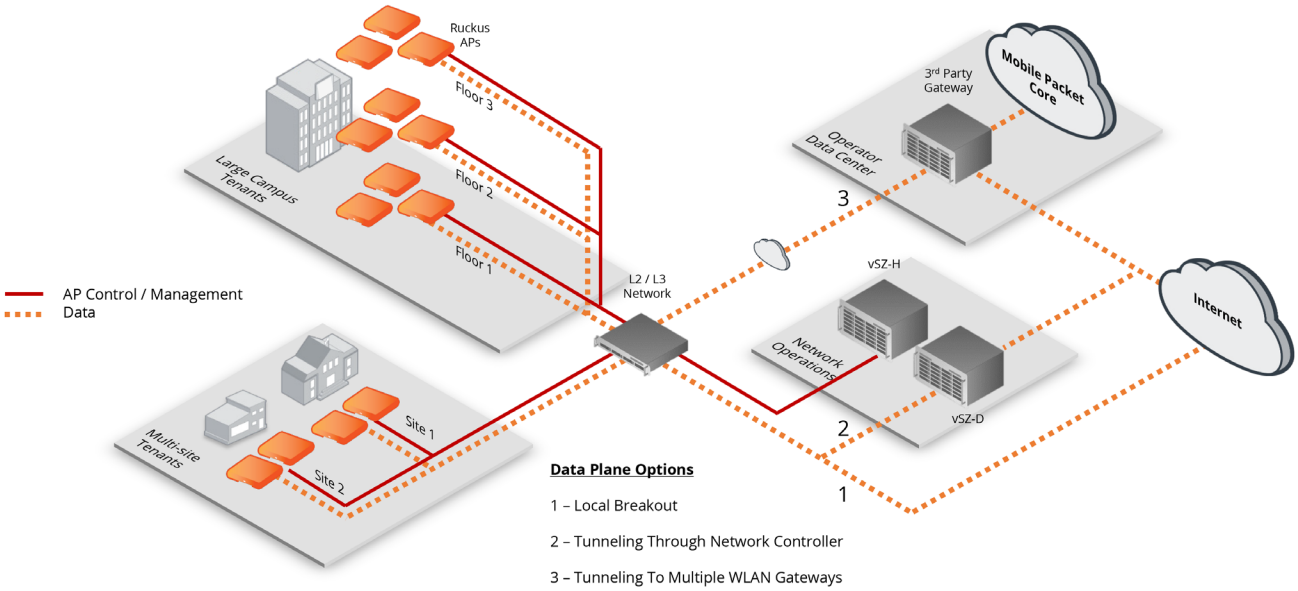
RUCKUS SmartMesh and zero-touch mesh provisioning simplify creating wireless backhaul redundancy through self-forming, self-healing mesh networks that are enabled with a single checkbox on the administrative interface without the need to pre-provision the AP. With RUCKUS APs and BeamFlex®+ technology, APs adapt to changing conditions to further ensure a solid mesh connection between APs, making use of the 5 GHz band to backhaul AP traffic to a point where wireline facilities are available. Mesh backhaul configurations dynamically reconfigured to reroute traffic over different paths as conditions change.

Connectivity optimizations

SmartZone managed APs discover neighboring APs over-the-air and build encrypted communication channels to share network load, operating channels, roaming, and other relevant RF parameters. This enables smarter roaming and load balancing behavior and is supported on both IPv4 or IPv6 networks.

Radio and Wi-Fi optimization

- **BeamFlex+:** BeamFlex+ adaptive antenna technology increases every RUCKUS AP's performance and range. Multiple antenna elements inside each AP manipulate RF patterns in real-time to maximize, on a per-packet basis, signal gain for each client, while accommodating changes in client device orientation. This technology mitigates radio interference, noise-related performance issues, and improves application flows especially for mobile devices.
- **ChannelFly®:** The ChannelFly dynamic channel management technology in all RUCKUS APs improves wireless performance in highly congested environments by dynamically switching a client to a better channel when the one it's using starts to degrade. This capability allows APs to automatically select the optimum 2.4 and 5 GHz channels to maximize performance and minimize interference. ChannelFly also supports a channel-change cost metric that refines client channel migration using channel capacity prediction models and initial learning and settling time updates.
- **AI-Driven Cloud Radio Resource Management (RRM):** A centralized algorithm that runs in the RUCKUS Analytics cloud and aiming to deliver zero interfering links for all access points (APs) managed by SmartZone. Cloud RRM continuously gathers RF data from all access points, making optimal choices for channel re-use and channel bandwidth selection to maximize bandwidth allocation. This new technology relies on sophisticated machine learning, artificial intelligence, graph algorithms, and cloud scale computation to jointly optimize channel and channel width. This method optimizes across all combinations of channels and channel widths to search for the optimal values across the network.
- **Capacity-Based Admission Control:** To help ensure existing clients' quality of service during periods of heavy load, RUCKUS APs implement a capacity-based client access control algorithm that declines connection requests from new clients if already-connected clients are at risk of service quality degradation.



- **Adaptive RF Cell Sizing:** SmartZone improves performance in networks with under-deployed or over-deployed APs by dynamically enlarging or reducing RF cell sizes which reduces channel interference from adjacent APs and increases overall average throughput per client.
- **Adaptive Traffic Load Balancing:** Real-time adaptive band balancing within AP radio bands helps improve user and network performance as environmental factors change. Client-aware machine learning recalibrates device load on a per AP and 2.4 vs 5 GHz radio band basis.

ARCHITECTURE

Separate control and data plane

The SmartZone platform addresses deployment and latency constraints with traditional WLAN architectures by implementing a customized local MAC architecture that places all essential WLAN services including authentication and association requests within the RUCKUS AP. This enables all SmartZone controllers to separate control and management traffic from data traffic while optimizing for both using SSH-based and GRE-based protocols, thus improving deployment flexibility and network latency.

A single SmartZone controller placed within a centralized data center can manage multiple remote sites without forcing all authentication requests or client data to tunnel through the SmartZone controller.

User traffic is bridged through the local L2/L3 network which improves latency between clients and services. Branch office deployments and direct integration between APs and local IT infrastructure Active Directory, LDAP, RADIUS, DHCP, DNS, and Firewalls are also enabled.

Payloads being transmitted over a public network connection, such as the Internet, are encrypted with SmartZone.

Multi-data plane support

Operators can route traffic simultaneously to multiple non-hosting managed service providers and enterprises from one access point to maximize infrastructure reuse and investment returns.

Each RUCKUS AP can host multiple data plane routing topologies simultaneously with mix-use between a single RUCKUSGRE tunnel, up to three SoftGRE tunnels, and a local data breakout option.

Active / active cluster redundancy

Active/active network controller clusters deliver higher availability and resiliency than traditional N+1 standby architectures and ensure redundancy while balancing AP and switch loading between controllers with zero idle controller capacity.SmartZone controllers support multiple layers of redundancy to ensure WLAN/LAN survivability in the event of catastrophic network failures. Multiple controller nodes within a cluster allow APs and switches to associate to any surviving controller in the event of a controller failure. If an entire cluster

goes off-line within a data center, APs and switches can fail-over to a different cluster hosted in a different data center geographically to assure network survivability. Additionally, the many-to-one cluster architecture furthers high-availability while reducing redundant cluster costs by allowing a single standby cluster to serve as a failover option for many distributed active clusters.

Only: vSZ-H

AP and switch survivability

SmartZone minimizes the impact of lost connectivity between the controller and the AP or Switch by placing essential WLAN services within the AP or Switch. WAN link outages or controller failures do not affect the normal operation of WLAN services. Native WISPr support on SmartZone managed devices allow the access points and switches to continue authenticating clients even without a connection to the SmartZone.

Switch configuration backup and restore

SmartZone backs up every switch configuration file on an ongoing basis at configurable intervals and can restore the last seven versions of a switch configuration. This provides the network administrator with the reassurance they can always go back to a known working configuration in the event the network does not behave as expected after a switch configuration change.

Control software and firmware upgrades

APs and switches can be upgraded individually or in groups. Administrators can granularly control switch firmware upgrades either immediately or scheduled across a managed network with a single operation.

Offload DHCP/NAT services

DHCP/NAT services are provided by the AP or separately in large networks by the RUCKUS Virtual SmartZone Data Plane (vSZ-D). By decoupling the management of APs which is done through SmartZone and the routing and management of WLAN traffic through the vSZ-D, operators can quickly replicate WLAN deployments across multiple sites while minimizing capital expenditures associated with separate routers and DHCP servers.

DHCP	Up to 100,000 IP address leases per vSZ-D (in increments of 1,000 IP address leases
NAT	Up to 2 million sessions flows per vSZ-D (in increments of 100,000 session flows)

Product information	
Products	• P01-S300-WW10: SmartZone 300 (SZ300)—redundant AC power, six (6) Fans, two (2) 10 Gbps data cards, and six (6) 1 GigE ports. No power cords included. • P01-S300-WW00: SmartZone 300 (SZ300)—redundant DC power, six (6) Fans, two (2) 10 Gbps data cards, and six (6) 1 GigE ports. Includes two DC power cables. • P01-S144-XX00: SmartZone 144 (SZ144)—four (4) 10 GigE and four (4) 1 GigE ports • L09-VSCG-WW00: Virtual SmartZone 3.0 or newer software virtual appliance, 1 instance, includes 1 AP license • P01-D144-UN00: SmartZone Data Plane Appliance, with 4x10GigE and 4 GigE ports (10Gbps throughput) • L09-vSZD-WW00: Virtual Data Plane 3.2 or newer software virtual appliance
Management Licenses/upgrade licenses	• L09-0001-SG00: Access Point management license for SZ144/vSZ 3.X, 1 RUCKUS AP access point • L09-0001-SGCX: Switch management license for SZ144/SZ300/vSZ 5.X, 1 RUCKUS ICX switch • L09-vSZD-SVCM: Virtual Data Plane Services (CALEA Mirroring), 1 instance ADD ON • L09-vSZD-SVL3: Virtual Data Plane Services (L3 Roaming), ADD ON (Needs minimum 2 instances) • L09-vSZD-SVFX: Virtual Data Plane Services, Flexi-VPN ADD-ON (Needs minimum 2 instances) • L09-vSZD-SNAT: Virtual Data Plane Services (NAT), 100K Sessions - 1 instance ADD ON • L09-vSZD-SDHP: Virtual Data Plane Services (DHCP Server), 1K IP Leases - 1 instance ADD ON • L09-vSZD-BW10: Virtual Data Plane 3.2 or newer software virtual appliance, 1 instance (throughput up to 10 Gbps per instance) • L09-vSZD-BWUL: Virtual Data Plane 3.2 or newer software - No throughput cap license • L09-0001-RXGW: Soft GRE tunnel license from AP to 3rd party concentrator
Accessories and Spares	• 902-S310-AC00: KIT, SPARE, AC Power Supply, SZ300 (use with 902-1174-xx00 power cord) • 902-S301-DC00: KIT, SPARE, DC Power Supply, SZ300 • 902-S320-0000: KIT, SPARE, FAN ASSY, SZ300 (6 fans) • 902-S330-0000: KIT, SPARES, Slide Rail Rack Mount Kit, SmartZone 300 • 902-S340-0000: KIT, SPARE, Console Cable, (RJ45 to USB), SZ300 • 902-S350-0000: KIT, SPARE (FRU), Hard Disk Drive, SZ300 • 902-S351-0000: KIT, SPARE (FRU), Solid State Disk 64GB, SZ300 • L09-0001-RXGW: Soft GRE tunnel license from AP to 3rd party concentrator • L09-0001-SGHA: Per AP management license for High Availability. Supported products (Standby mode only): SZ-300, vSZ-H. For each AP on Standby Cluster only
URL Filtering	• S01-URL1-1LSZ: SmartZone URL Filtering 1 year subscription for 1 AP • S01-URL1-3LSZ: SmartZone URL Filtering 3 year subscription for 1 AP • S01-URL1-5LSZ: SmartZone URL Filtering 5 year subscription for 1 AP • S21-URL1-1LSZ: SmartZone URL Filtering 1 year subscription renewal for 1 AP • S21-URL1-3LSZ: SmartZone URL Filtering 3 year subscription renewal for 1 AP • S21-URL1-5LSZ: SmartZone URL Filtering 5 year subscription renewal for 1 AP

PLEASE NOTE: When ordering the AC power cord, you must specify the destination region by indicating -US, -EU, -CN, -IN, -JP, -KR, -SA, -UK or -UN instead of -XX.

Capacity	SZ300	VSZ-H	SZ144	VSZ-E
Managed APs	• Up to 10,000 per controller • Up to 30,000 per cluster	• Up to 10,000 per controller • Up to 30,000 per cluster	• Up to 2,000 per controller • Up to 6,000 per cluster	• Up to 1,024 per controller • Up to 3,000 per cluster
Managed Switches*	• Up to 2,000 per controller • Up to 6,000 per cluster	• Up to 2,000 per controller • Up to 6,000 per cluster	• Up to 400 per controller • Up to 1,200 per cluster	• Up to 200 per controller • Up to 600 per cluster
WLANs	• Up to 2,048 per zone • Up to 65,534 per cluster	• Up to 2,048 per zone • Up to 65,534 per cluster	• Up to 2,048 per cluster	• Up to 2,048 per cluster
VLANS	• Up to 4,094	• Up to 4,094	• Up to 4,094	• Up to 4,094
Concurrent Devices	• Up to 100,000 per vSZ-H • Up to 300,000 per vSZ-H cluster • Up to 150,000 per SZ300 • Up to 450,000 per SZ300 cluster	• Up to 100,000 per vSZ-H • Up to 300,000 per vSZ-H cluster • Up to 150,000 per SZ300 • Up to 450,000 per SZ300 cluster	• Up to 40,000 per controller • Up to 120,000 per cluster	• Up to 25,000 per controller • Up to 60,000 per cluster

* Each managed switch added to a cluster/controller reduces the capacity count for managed APs by 5.

	VIRTUAL DATA PLANE (VSZ-D)	APPLIANCE DATA PLANE (SZ144-D)
Hypervisor support	• VMware • KVM	• N/A
Dynamic data plane scaling	Options: • 1 Gbps • 10 Gbps • Or even higher throughput capacities	Options: • 1 Gbps or 10Gbps
Integration with vSZ controller	• 20 vSZ-D instances per vSZ instance • 80 vSZ instances per vSZ cluster of 4 instances • Each vSZ-D runs as an independent virtual machine • Instance that is managed by the vSZ controller	• 20 SZ100-D appliances per vSZ instance • 80 SZ100-D appliances per vSZ cluster of 4 instances
Flexible configuration	• Encrypted tunnel aggregation from all types of WLANs (captive portal, 802.1x, HS2.0), VLANs, DHCP relay, NAT traversal	
Services	• DHCP server/NAT • Layer 3 roaming • Lawful Intercept (CALEA) • vTWAG* • Flexi-VPN Note: All available services for data plane can be used on any data plane product. * TWAG functionality is available on vSZ-D only.	
Northbound tunnels	• L2oGRE • QinQ • GTP** ** TWAG on vSZ-D	

Key functionality		
Device Management	• RUCKUS Wi-Fi APs supported: R850, R750, R730, R720, R710, R650, R610, R550, R510, R320, R310, M510, H510, H320, C110, E510, T811CM, T750, T710, T710S, T610, T610S, T504, T310, T301, FZM300, FZP300 • RUCKUS ICX 7000 series switches running FastIron 8.0.80 and above supported; FastIron 80.0.90a required for Zero-Touch Provisioning	
Device Type Support	• Wi-Fi APs, Switches	
Controller Expansion	• Up to 4 controllers in N+1 active-active mode, supporting non-disruptive capacity expansion	
Controller Redundancy	• 3+1 distributed data preserving with N+1 redundancy within a cluster	
Cluster Redundancy	• Geo-redundancy between clusters; many-to-one cluster support	
Data Offload	• Local offload of traffic directly to the Internet	
AP	• WPA, WPA2-AES, 802.11i, 802.1x/EAP, PSK, WISPr, WEP, WPA3, Enhanced Open, MAC Address* • Fast EAP-SIM re-authentication • EAP-SIM, EAP-AKA, EAP-AKA over WLAN for 802.1x • Wi-Fi Locations with the SZ AAA-Proxy functionality enabled	
User Database	• Internal database up to 25,000 users • External: RADIUS, LDAP, Active Directory	
Access Control	• L2 (MAC address-based)L3/4 (IP and Protocol based) • L2 client isolation • Management interface access control	• Time-based WLANs • Device type access policies • Two-factor authentication password, SMS
Wireless Intrusion Detection (WIDS/WIPS)	• Rogue AP detection / prevention • Evil-twin/AP spoofing detection • Ad hoc detection	
AAA	• RADIUS (primary and backup)	
Hotspot	• WISPr, Wi-Fi CERTIFIED, Passpoint™, HotSpot 2.0*	
Guest Access	• Supported	
Captive Portal	• Supported	
Mesh	• Self-healing, Self-forming, Zero-touch provisioning	
DHCP Server	• Up to 100,000 IP address leases per vSZ-D (in increments of 1,000 IP address leases)	
NAT	• Up to 2 million sessions flows per vSZ-D (in increments of 100,000 session flows)	
Media	• 802.11e/WMM, U-APSD, Wi-Fi Calling Prioritization*	
mDNS Bonjour Fencing	• Supported	
WISPr	• WISPr authentication, SZ downlink AP Survivability*	
Software Queues	• Per traffic type (4), per client	
SmartCast Traffic Classification	• Automatic, heuristics and TOS based or VLAN-defined	
Rate Limiting	• Supported	
WLAN Prioritization	• Supported	
Client Load Balancing	• Automatic	
Band Load Balancing	• Supported	

* SmartZone controllers do not contain embedded radios or antennas

Key functionality *(continued)*		
AP Provisioning	• L3 or L2 auto-discovery • Auto-software upgrade • Automatic channel optimization	
Configuration Management	• Secure multi-operator login (RBAC) • Large scale (bulk) AP management tools • Switch software and firmware upgrades • Switch configuration management to be supported in an upcoming SmartZone release • Per zone firmware versioning control • Configuration audit trails	• Alarm and event notification (SNMP V1 / V2 / V3) • Event Logging (Syslog) • Integrated on-board remote accessible EMS functionality • RESTful APIs (JSON) • Web-UI • CLI

Physical characteristics		
Hypervisor Support for VSZ	• VMware 6.5, KVM CentOS 7.3 and above, Hyper-V Windows 2012 R2 and above, AWS, Azure, GCE	
Power	• Dual (redundant) AC or DC hot-swappable power supplies • DC power consumption: 1400W • Power Rating: -36 to -72VDC • AC power consumption: 1500W • Power Rating: 100-127VAC/200-240VAC, 47-63HZ • SZ144: AC power consumption: 250W	
Dimensions	• SZ300: 2RU rack mountable: 430 mm (W) x 518 mm (D) x 88.6 mm (H); 16.93 in (W) x 20.4 in (D) x 3.48 in (H) • SZ144/144-D: 1RU rack mountable: 438 mm (W) x 292.1 mm (D) x 44 mm (H); 17.25 in (W) x 11.5 in (D) x 1.73 in (H)	
Weight	• SZ300: 24.3 kg; 53.6 lbs • SZ144/144-D: 5 kg; 11.02 lbs	
Connections	SZ300 • Control, management, cluster ports • Six 10/100/1000 Mbps, RJ-45 ports • Data: Four 10Gbps data ports (SFP+) • Console ports: two RJ-45, one front, one rear • USB ports: two front, two rear • Serial port	SZ144 • 4 - 1GbE ports • 4 - 10GbE ports
SZ300 LED	• Front panel LEDs, one rear LED	
SZ300 Fans	• Six redundant, field-swappable fans in three sets	
Mean-Time-Between-Failure (MBTF)	SZ 300 at 25C: • AC version: 44126 hours • DC version: 39094 hours	SZ144/144-D: at 25C: • AC: 48649 hours • AC: w/ 10G 45818 hours
Environmental Conditions	SZ300 • Operating Temperature: 5°C (41°F) – 55°C (131°F)Operating Humidity: 5% to 85%, non-condensing • Humidity storage: 95%, non-condensing	• SZ144/144-D: • Operating Temperature: 0°C (32°F) – 40°C (104°F) • Operating Humidity: 5% to 85%, non-condensing • Humidity storage: 95%, non-condensing

Regulatory/certifications		
EMC (for SZ144, SZ300)	• FCC/ICES-003-Emissions (USA/Canada) • CISPR 22-Emissions (International) • EN55022-Emissions (Europe) • EN55024-Immunity (Europe) • EN61000-3-2-Harmonics (Europe) • EN61000-3-3-Voltage flicker (Europe)	• CE-EMC Directive 89/336/EEC (Europe) • VCCI Emissions (Japan) • AS/NZS: CISPR 22 Emissions (Australia/New Zealand) • BSMI CNS13438 (Taiwan) • CCC Certification (China)
Safety (for SZ144, SZ300)	• UL60950-1/CSA 60950-1 (USA/Canada) • EN60950-1 (Europe) • IEC60950-1 (International), CB Certificate & Report including all international deviations • CE-Low Voltage Directive 73/23/EEE (Europe) • CCC Certification (China)	
Miscellaneous (for SZ144, SZ300)	• NEBS level 3 design	

About RUCKUS Networks

RUCKUS Networks builds and delivers purpose-driven networks that perform in the demanding environments of the industries we serve. Together with our network of trusted go-to-market partners, we empower our customers to deliver exceptional experiences to the guests, students, residents, citizens and employees who count on them.

www.ruckusnetworks.com

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

PA-114067.9-EN (03/23)