RELEASE NOTES

Ruckus SmartZone Release Notes

Supporting SmartZone 5.0

Part Number: 800-71871-001 Rev A
Publication Date: June 2018

Contents

New Features and Changed Behavior....7
New Features....7
ICX Switch Management....7
Cluster Geo-Redundancy Phase2....7
Multi-Language GUI Support....8
PCI Account Security....8
PCI Report Integration for SCI....9
WISPr Survivability and Support on AP....9
Per-Packet Tx Power Adaptation....9
Adaptive Radio Frequency (RF) Cell Sizing....9
Air-Time Decongestion....10
Transient Client Management....10
Packet Capture from SZ GUI....10
Zero-Touch Mesh Provisioning....11
Zone-Based Event Management....11
Directed Multicast Handling....11
Export Traffic Flow Log from AP Phase2....11
vSZ-D DHCP and NAT Tiered Licensing....12
Multi-Tunnel Support for Access Points....12
Wi-Fi Calling Support....13
vSZ-D 40G Support....13
TWAG on vSZ-D....13
Client Troubleshooting Support Enhancements....13
Bonjour Fencing for Chromecast and Custom Multicast Domain Name Server (mDNS) Services....14
Ability to Move AP Between SZ Clusters....14
URL Filtering Licensing....14
SCI Support for Measuring Latency Between SZ and AP....14
Ability to Enable SCI Integration on a Per-Domain/Zone Basis....15
Additional Telemetry Statistics....15
WLAN Template Enhancements....15
Setup Wizard Enhancements....15
M510 GUI Support....16
2.4 GHz Mesh Support on Dual-Band APs....16
DHCP/NAT Hierarchical Network Topology (HNT) Feature....16
Additional Enhancements....16
Changed Behavior....17
Geo Redundancy....17
ICX Registration....18

Hardware/Software Compatibility and Supported AP Models....19
Overview....19
Release Information....20
SZ300....20
SZ100....20
vSZ-H and vSZ-E....20
vSZ-D....20
Supported and Unsupported Access Point Models....20

Supported AP Models....21
Unsupported AP Models....21
Caveats, Limitations, and Known Issues....23
AP KPI Known Issues....23
AP Known Issues....23
M510 AP....28
AAA Known Issues....29
Application Recognition and Control (ARC) Known Issues....29
Bonjour Fencing Known Issues....31
Bonjour Gateway Known Issues....31
Control CLI Known Issues....31
Control Communicator Known Issues....31
Control Domain Known Issues....32
Control Platform Known Issues....32
Geo Redundancy Known Issues....32
Outbound firewall....32
ICX Known Issues and Limitations....33
General Category....33
ICX-M Known Issues and Limitations....33
General Category....33
Cluster Support....33
Configuration Backup and Restore....33
Firmware Upgrade....34
Ports....34
MSP Known Issues....34
Public API Known Issues....34
Rate Limiting Known Issues....34
Scalability, Stability, and Performance Known Issues....35
Session Manager Known Issues....35
SNMP Known Issues....35
Syslog Known Issues....35
System Known Issues....35
UI/UX Known Issues....37
Virtual SmartZone Known Issues....39
Virtual SmartZone Data Plane Known Issues....39
Visual Connection Diagnostics Known Issues....40
Wired Clients Known Issues....40
WISPr Known Issues....41
ZoneDirector to SmartZone Migration Known Issues....41
Resolved Issues....43
AP Resolved Issues....43
Application Recognition and Control (ARC) Resolved Issues....43
Bonjour Fencing Resolved Issues....44
Control Domain Resolved Issues....44
Public API Resolved Issues....44
System Resolved Issues....44
Virtual Data Plane Resolved Issues....44
Virtual SmartZone Resolved Issues....45
Upgrading to This Release....47

Before Upgrading to This Release 47
Data Migration Recommendations 48
Upgrade Considerations 48
Virtual SmartZone Recommended Resources 48
AP and Switch Resource Table 49
SmartZone Upgrade Paths 50
Multiple AP Firmware Support 51
Up to Two Previous Major AP Releases Supported 51
EoL APs and APs Running Unsupported Firmware Behavior 52
EoL APs 52
APs Running Unsupported Firmware Releases 52
Interoperability Information 53
AP Interoperability 53
Enabling ZoneFlex AP Discovery to a SmartZone Controller Using DHCP Option 43 53
Enabling ZoneFlex AP Discovery to a SmartZone Controller Using DNS 53
Redeploying ZoneFlex APs with SmartZone Controllers 54
Converting Standalone APs to SmartZone 54
ZoneDirector Controller and SmartZone Controller Compatibility 55
Client Interoperability 55

New Features and Changed Behavior

- New Features..... 7
- Changed Behavior..... 17

New Features

This section provides a high-level overview of several key features that are introduced in the SmartZone (SZ) software release 5.0.The SZ release 5.0 is applicable to the Ruckus SmartZone 300, SmartZone 100, vSZ-H, and vSZ-E controller platforms. For additional details, do refer to the SmartZone Controller Documentation Suite for Release 5.0.

ICX Switch Management

This release of SmartZone adds management and monitoring support for ICX switches. Similar to wireless control and management of APs, the SmartZone will begin providing similar functionality for switches. In this release, we are taking the first step towards a full-featured wired/wireless integration plan. This first step focuses on monitoring, status, usage visibility, and some basic management, including configuration backups and firmware management. This release does not focus on switch configuration management, which will be a Step2 focus.

For this release, the following functionality is provided:

- ICX switch registration and authentication
- Switch inventory (model, FW version, last backup, etc)
- Health and performance monitoring (status, traffic stats, errors, clients etc) with alarms
- Firmware upgrade
- Switch configuration file backup and restore
- Client troubleshooting - search by Client MAC to find the AP/switch port for that client

Cluster Geo-Redundancy Phase2

The SZ Cluster Geo-Redundancy feature was introduced (Phase1) in the SmartZone 3.6.0 release. Phase2 is being introduced in the 5.0 release, with additional enhancements expected in subsequent releases. Geo-redundancy addresses datacenter disaster recovery use cases for large customers, such as SPs and Large Enterprises. As such, it is only supported on the High-Scale SmartZone platforms, namely SZ300 and vSZ-H. It is not supported on SZ100 nor vSZ-E.

The functional highlights of Phase2 include:

1. Many(Active)-to-One(Standby) SZ cluster support - this design allows a single standby cluster to serve as a failover option for many distributed active clusters.
2. Different AAA servers can be configured on active and standby clusters.
3. Active and standby are still required to operate on the same firmware.

Multi-Language GUI Support

Due to the SmartZone's broad worldwide appeal and its applicability across diverse customer sets, we are enhancing the graphical user interface with support for several additional languages. In the past, we have supported multiple languages for end-user facing portals, but this new feature will provide multi-language support for the network administrator(s).

This release will support the following languages:

1. French
2. German
3. Italian
4. Japanese
5. Korean
6. Portuguese
7. Russian
8. Simplified Chinese
9. Spanish
10. Traditional Chinese

PCI Account Security

To support requirements for admin account controls in security-conscious organizations, as well to make PCI compliance very easy to manage, we are adding several dimensions of admin account security and controls. The following admin account features are being added:

1. **Session Idle Timeout** in the pre-5.0 release, each admin can control their own account preferences for idle timeout. By adding the session idle timeout to the account security profile, the network administrator can override individual admin preferences with an assigned idle timeout value, which may be necessary for compliance or to enforce a strict stance on admin account idle timeouts.
2. **Two-Factor Authentication** with two-factor authentication, we are adding the capability to provide both username/password authentication as well as SMS authentication before allowing the administrator to login on SmartZone. Two-factor authentication can be enabled for a group of administrator as long as they have phone numbers configured in their accounts. When this feature is enabled, the administrator be asked to test SMS authentication to ensure that it is working properly end-to-end, so that accounts are not locked out.
3. **Account Lockout from Unused Account** with this enhancement, the system will monitor login activity for each account, and if enabled, it will lock any unused account after a configurable period of time. This security feature ensures that idle network admin accounts are not left in the system indefinitely, which could be perceived as a security vulnerability.

In the 3.6.1 release, the account security framework was first added in SmartZone. This framework allows the admin account security settings to be defined as a profile and assigned to an admin group in a flexible way. The above features are being added to that same account security profile.

PCI Report Integration for SCI

In addition to the administrator account security features, which is important for easy PCI compliance, SmartZone (SZ) also provides detailed compliance information to SmartCell Insight (SCI) when a PCI report is triggered from SCI.

NOTE

The PCI report is delivered by SCI, but the SZ is providing some of the operational data needed to determine compliance.

WISPr Survivability and Support on AP

This feature is to allow native WISPr support on SmartZone (SZ) managed APs instead of requiring access to SZ. In other words, AP will support external portal redirect with survivability--when APs cannot reach the centralized SZ, therefore in the event AP to SZ connection fails, AP will continue to authenticate and admit clients it servers.

For this release, to make this function work, there are a few assumptions we adopted:

1. AP and the subscriber portal server shall not be on different sides of NAT server due to potential impact to service provider firewall policy.
2. Only Ruckus 11AC Wave 1 and newer APs support this feature.
3. In the event clients trying to roam, the clients will be going thru full re-auth process, in other words, no roaming support in this case. Roaming use case is valid and will be supported in later release.
4. AP with this function running may experience performance degradation.
5. External subscriber portal shall be able to parse the AP NBI (Northbound Interface) IP address from the URL enrichment message that the client sends to the portal server. With that step, the subscriber portal shall be able to send the client credential to the proper AP.

Per-Packet Tx Power Adaptation

This feature applies only to APs managed by this version of SmartZone.

This feature enables APs to transmit at the optimal MCS (Modulation and Coding Scheme) rate per client. The optimal MCS rate decision is based on client proximity (RSSI (Received Signal Strength Indicator)), using which an algorithm iterates to the lowest Tx power level while maintaining a constant, optimal MCS rate on a per management packet basis.

The benefits are realized through reduced channel interference for adjacent APs (in a multi-AP deployment) and an overall higher average throughput per client performance metric.

Adaptive Radio Frequency (RF) Cell Sizing

This feature applies only to APs managed by this version of SmartZone.

This feature enables APs to use RF statistics derived from periodic co-channel neighbor scans and RF interference estimates to adapt its transmit (Tx) and receive (Rx) cell sizes in real-time. APs track key RF performance metrics across neighboring Wi-Fi cells and these metrics are exchanged between cooperating neighbor APs driving network awareness among all APs.

This feature delivers a better overall user experience in dense AP deployments. The feature also can be useful in triaging performance and/or stability issues in over deployed or under deployed Wi-Fi networks.

Air-Time Decongestion

This feature applies only to APs managed by this version of SmartZone.

Management frames have been observed to completely overwhelm dense Wi-Fi environments. The problem is exacerbated by redundant Probe responses from co-located APs which completely saturate the available Wi-Fi spectrum. This results in poor connectivity and low per-client throughput numbers which lead to poor Client experience.

This feature enables proprietary techniques to limit Management Frame exchanges between APs and Clients in high density deployments.

This feature delivers increased Air-Time for users' data traffic and a better Quality of Experience for all clients using innovative schemes to minimize Management frame exchanges. Minimizing Management frame exchanges results in decongestion of the Wi-Fi spectrum which increases overall Network efficient for users' data traffic.

Transient Client Management

This feature applies only to APs managed by this version of SmartZone.

This feature mitigates the network performance degradation that connected clients experience in dense environments. This degradation is typical to Train stations, bus terminals and various public HotSpot venues where a transient but numerous clients can completely overwhelm the network and degrade performance for all clients, including previously connected clients.

This feature uses statistical methods to delay the AP's associations with transient clients. Venue administrators and IT administrators can tune configuration parameters based on typical dwell times and RSSI of these transient clients. Additional benefits are accrued with heursistics-based techniques are used to selectively respond to transient clients.

The main benefit from this feature is an efficient Air-Time utilization which minimizes Cellular to Wi-Fi hand-offs of transient clients.

Packet Capture from SZ GUI

In this release, the SmartZone is adding support for AP packet capture, managed from the SZ graphical interface. In past release, the AP packet capture feature was only supported from AP CLI, which made its use somewhat challenging for some admins. By pulling this functionality into the GUI, it simplifies use and provides an easy way to download packet captures to a local machine without having direct IP connectivity to APs.

For this implementation, the packet capture feature supports two modes:

1. **Streaming to Wireshark** - in this mode, the AP will stream its captured data directly to Wireshark. The station running Wireshark will need to have IP connectivity to the AP providing the capture data. In the Wireshark application, the administrator will identify the interface on the AP from which it would like to capture data.
2. **Saving to File** - in this mode, the AP will save the packets directly to a .pcap file, which will be pushed to the SmartZone console when the packet capture is stopped. The AP can create two separate packet capture files, each up to 10MB in size. If the packet capture exceeds 10MB, the AP will automatically start a second file. Both files will be sent to the SmartZone for download by the administrator. SmartZone will rotate the files in sequence when the maximum file size is reached.

The AP can capture across any interface, wireless or wired, and the web interface also provides packet type (management, control, data) filters when capturing over the wireless interface.

Zero-Touch Mesh Provisioning

Another feature focused on ease of use in this release, Zero-Touch Mesh Provisioning allows the administrator to deploy mesh APs without first provisioning them by connecting them to an Ethernet segment. This allows the customer to send mesh APs directly to the deploying site or installation team without "priming." The goal of this feature is to avoid a somewhat frustrating, and often unnecessary, step in the deployment process of mesh APs, without compromising security.

For security reasons, the mesh APs will not be automatically accepted by the SmartZone. To prevent misuse, the administrator must approve the APs if they are discovered by Zero-Touch Mesh, and the administrator must also enter some identifying details about the AP, such as the last few digits of the AP serial number.

NOTE
Zero Touch Mesh is only supported on 5Ghz.

Zone-Based Event Management

To address use cases common among Managed Service Providers, this release adds zone-based event management controls. This allows the network administrator to enable or disable event notifications (email, SNMP, storage in SZ database) on a per-zone basis. In some cases, customers have observed that due to differences in deployment sites and network demands, some zones experience may have more events than others. Due to the potential for "noisy" zones with excessive events and notifications, it is desirable to disable these events for those zones.

In addition, to make email events more manageable, we have added the zone name to event emails, which allows for more customizable filtering of noisy zones directly on the email client (i.e. email notifications from some zones can be moved to a "noisy zone" folder).

Directed Multicast Handling

In this release, we are bringing AP CLI features to the SmartZone for web user interface control. The AP's directed multicast feature determines how the AP handles multicast packets, whether converting them to unicast, leaving them as multicast, or dropping them altogether. In the SmartZone web user interface, there are separate controls for three separate forms of directed multicast logic:

- **Multicast traffic from wired client:** this enables/disables directed multicast logic on traffic being sent from a secondary AP port (non-trunk Ethernet ports designed for downlink connections, such as on wallplate APs).
- **Multicast traffic from wireless client:** This enables/disables directed multicast logic on traffic sent from wirelessly connected clients.
- **Multicast traffic from network:** This enables/disables directed multicast logic on traffic coming from the AP's uplink path, whether wired uplink to all trunk Ethernet ports or mesh AP.

Export Traffic Flow Log from AP Phase2

This feature is required in several countries as a form of retroactive investigation in case of legal violation by users. The basic use case was addressed in R3.6 and the R5.0 release is to complete the feature for the full scope of requested functionality.

The purpose is to provide syslog messaging for every new IP flow initiated by a UE. This flow data is to be sent to the syslog server by the AP without requiring "general" syslog information also to be sent. The following are supported in the release:

- Add WLAN/SSID to log message
- Add URL to log message
- Separate 5-tuple flow logging facility from normal AP syslog - allow admin to enable one or the other

- Support backup syslog server for AP-level syslog
- Support TCP for AP syslog

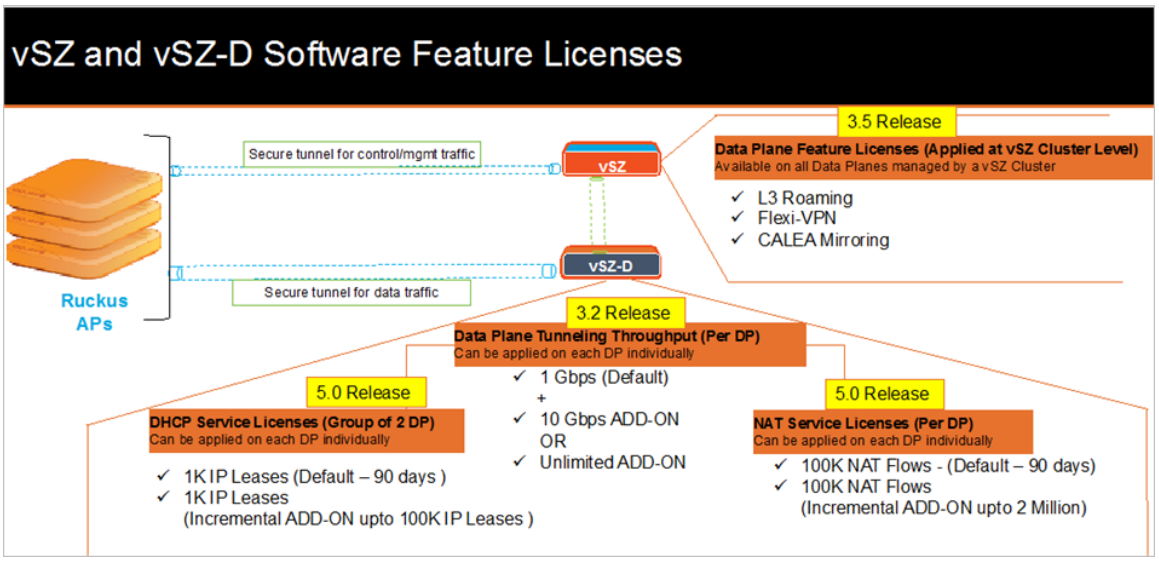
vSZ-D DHCP and NAT Tiered Licensing

This release introduces tiered licensing for DHCP and NAT features.

- The DHCP server license is available in tiers of 1K IP leases up to a maximum of 100K IP leases per data plane.
- The NAT function is available in tiers of 100K NAT flows/sessions up to a maximum of 2 million per data plane.

The illustration below provides details about the license tiers. Do also refer to the vSZ-D datasheet for the associated SKUs.

FIGURE 1 vSZ and vSZ-D software license tiers



Multi-Tunnel Support for Access Points

In prior Ruckus solutions, APs could only support a single tunnel to a data plane, as well as a local break out. In this release, we're adding support for Ruckus APs to provide multiple simultaneous tunnels to different data planes.

For 5.0, the AP will support a single Ruckus GRE tunnel (with our without encryption) while supporting up to three SoftGRE (without encryption) tunnels, in addition to local breakout option. The tunneling will be based on SSID configurations on the AP.

This feature is designed to help in common MSP (Managed Service Provider) use cases, where each of the MSP's customer will have the possibility to get its own tunnel directly to the data center.

Before configuring multiple tunnels, consider the following configuration prerequisites:

- Ensure that there is a reachable SoftGRE gateway and also verify that there is network connectivity.
- Ensure that the zone is configured with correct SoftGRE gateway information.
- Verify that the SSID to SoftGRE tunnel mapping is correct.
- Verify the SoftGRE tunnel configuration and run time status using the command **get softgre** *tunnel-index*. The tunnel index can be 1, 2, or 3.

Wi-Fi Calling Support

Due to increasing use of Wi-Fi for device connections, Wi-Fi Calling is seeing high demand by many SPs worldwide, which allows them to differentiate their Wi-Fi access.

Even though in Wi-Fi calling the end-user device and Mobile Packet Core communicate directly over encrypted tunnels, it is important for the Wi-Fi network to detect and prioritize this type of traffic for an optimal application experience. This feature will support Wi-Fi calling traffic recognition and prioritization above other network traffic, with visibility for Wi-Fi calling stats for the network operator. Moving forward beyond 5.0, the functionality will continue to see enhancements.

vSZ-D 40G Support

This release supports up to 40Gbps of packet forwarding bandwidth support. This assumes appropriate 40G Intel NIC (Network Interface Card) that support Intel DPDK (Data Plane Development Kit) are installed by the customer on the underlying hardware platform that hosts the vSZ-D. This is a licensed *ADD-ON* bandwidth feature as part of the *Unlimited* bandwidth ADD-ON SKU.

TWAG on vSZ-D

Due to the popularity among service providers for virtualization of Wi-Fi core components, alongside increasing demand for mobile data offload, there is a growing interest in a virtual TWAG (Trusted Wireless Access Gateway) solution to address the use case.

In this release, the virtual TWAG (vTWAG) on vSZ-D is delivered as a first phase. This feature set will match the functionality previously supported by the SCG200 product with TTG (Tunnel Terminating Gateway).

vTWAG supports GTP (General Tunneling Protocol) v1 and GTPv2 with integration to a single MNO (Mobile Network Operator) (single APN (Access Point Name)).

Client Troubleshooting Support Enhancements

The client connectivity troubleshooting feature has been a deeply appreciated feature since its addition in 3.5. However, one of the more common requests was to add historical troubleshooting to the feature. In this release, we are taking several steps to provide the same client troubleshooting in a historical way.

NOTE

Historical troubleshooting was added as a PoC/Beta feature in the 3.6 release, but it had some limitations. Those limitations are being addressed in the 5.0 release with the following enhancements:

- The real-time troubleshooting will still be supported, and now also support Guest and WebAuth WLAN types.
- The 3.6 PoC feature was only supported on the Essentials (SZ100 and vSZ-E) platforms. In this release, it will also be supported on High-Scale (SZ300 & vSZ-H) platforms.
- We have extended support for historical data to 5 days of failure data for the Essentials platforms and 3 days for the High-Scale platforms. When the admin selects a client to troubleshoot, the time line of connections and failures for that client will show up on the timeline, allowing the admin to select a failure case for deeper analysis.
- We have also incorporated a client search function by which administrators can search historical client and connected client tables for MAC, Hostname, and OS type data. This integration makes it easier for an admin to find a specific client, even if they do not know the MAC address.
- Finally, we have reworked the UI flow in some simple but helpful ways to make it easier to do historical and real-time troubleshooting.

Bonjour Fencing for Chromecast and Custom Multicast Domain Name Server (mDNS) Services

With this release, we have extended the functionality of the Bonjour fencing feature to support both Chromecast devices (as a pre-defined service) as well as allowing the admin to define custom mDNS strings for new services, undefined services, or new strings that have been introduced for pre-defined services that are already supported. This provides tremendous administrative adaptability for the common scenario that consumer-focused devices change implementions and administrators are caught off guard because the devices update automatically.

Ability to Move AP Between SZ Clusters

In a network environment where multiple SZ clusters are present, administrators may need to move APs from one cluster to another cluster. We're introducing this capability in this release to enable administrators to move an AP(s) from one SZ/vSZ cluster to another via the Web UI. In the past, operations teams could accomplish the same thing via the AP CLI, but this often posed problems due to unknown zone username/password combinations or the complexity of AP CLI scripts.

With this feature, you can search for an AP(s) with built-in search options, then select one or multiple APs from the search list and move them to a different cluster via IP (v4 or v6) or FQDN (Fully Qualified Domain Name) of the control interface of the new cluster. In case that moved AP cannot connect to the new cluster, it will fallback to its original cluster and stay in the staging zone, but its original configuration is lost (caution is advised).

URL Filtering Licensing

URL filtering feature, introduced in SZ 3.6 release, enhances and extends security by protecting end users from accessing malicious, fraudulent URLs or adult oriented websites on the Internet. Websites are categorized in 83+ categories ranging from adult, botnet, malware, spam, peer-to-peer etc. This feature is offered as a subscription service on a per AP per 1yr, 3yr or 5yr term.

With this release, URL filtering license is enforced on a system wide basis or granularly on a per zone basis if desired. By default, URL filtering licenses are distributed automatically to each zone that has a URL filtering enabled WLAN. For advanced use cases, there is a not to exceed license count configured per zone to prevent a single zone from consuming all available licenses from the global pool. Administrators are notified and shown warnings on the UI about upcoming license expiry. URL filtering feature is disabled at the zone level at the end of license term unless it is renewed.

SCI Support for Measuring Latency Between SZ and AP

With this feature, SCI helps in identifying connectivity and latency issues between AP and SmartZone. In this solution, the AP sends ping packets periodically to the SZ and measures the latency of the ping packets. This latency will be reported to SCI. SCI will then generate reports/dashboards and analytics based on latency measurements

The frequency of latency measurement corresponds to KPI reporting interval from SZ to SCI. Currently two reporting intervals are supported, which is 15 minutes and 3 minutes. Latency measurement interval is based on the reporting interval configuration on SZ.

Ability to Enable SCI Integration on a Per-Domain/Zone Basis

In Ruckus existing implementation, when controller is added to SCI (or) SCI is added to controller, KPIs/stats for all zones and domains are sent to SCI. This creates a couple issues in the customer network: (A) unnecessary traffic when some zones/domains data are not needed in SCI, and (B) SCI licenses are based on managed AP, so this consumes SCI licenses on those unwanted zones/domains.

This feature has a configuration on all SZ platforms to selectively send KPIs/statistics for certain zones or domains to SCI. The zones/domains for which data is sent to SCI is configurable on the controller web user interface as well as API.

Additional Telemetry Statistics

Added new MQTT (Message Queuing Telemetry Transport) protocol with aim to send stats from a Ruckus AP to a Cloud via SZ Controller. Following telemetry metrics can be captured from MQTT streaming:

- **Available in 5.0**:
  - Tx Frame Size Distribution
  - Tx MCS Distribution
  - Tx Radio Subframe PER count
- **Available from 3.6.1 and integrated to 5.0**:
  - Rx BSSID Channel Utilization
  - Tx Channel Utilization for Management Traffic
  - Rx Channel Utilization for Management Traffic

WLAN Template Enhancements

The WLAN template enhancements are valuable for scalable networks and networks that are taking advantage of multiple zones. Of course Ruckus has APIs available for some customers to leverage, but many customers do not have the expertise to utilize scripts with our APIs to make bulk configuration tasks across zones easy to perform. Since our current UI tools do not provide an easy way to make small changes in an operating network (though the zone template does allow cookie-cutter creation of NEW zones), we desire a way to alleviate this problem from the UI.

The primary use cases we are driving to meet are as follows:

- **Create new WLANs in zones:** Ability to use a WLAN template to create a new WLAN in a zone.
- **Modify existing WLANs in zones:** Ability to use WLAN template to modify existing WLANs in a zone.
- **Change multiple zones at once:** Ability to use WLAN templates to change settings in multiple zones at once.
- **Add/modify services/profiles to zones:** Ability to use WLAN templates to propagate a change to multiple zones at the same time

Setup Wizard Enhancements

In this release, we have added new features to the setup wizard, which the admin uses when a system is loaded from a default configuration. Namely, we have added a default AP country code setting, which changes both the default zone country code (Essentials platforms) as well as the default country code for newly created zones.

Additionally, to avoid extra time and effort required in bringing up a SmartZone to be used with a backed up configuration, we have added the ability to restore a new cluster from a configuration backup. This allows the administrator to skip a step during the setup wizard so that he/she does not have to wait for a default system to be provisioned/loaded and then perform a

configuration restore. He/she can simply do the restore from the wizard and the cluster is provisioned to that backed up configuration.

M510 GUI Support

In this release, we are supporting an AP model (M510) with cellular backhaul connections. To support this, and to provide configurability for AP behavior as well as settings from the cellular radio, we have added additional model-specific configurations for the M510 model.

2.4 GHz Mesh Support on Dual-Band APs

Ruckus SmartMesh on dual band access points currently uses exclusively the 5GHz band for mesh connectivity. This is problematic for certain countries which do not allow, or highly restrict 5GHz operation - for example Israel. In the past, customers in these countries have used single-band (2.4GHz-only) access points such as 7343 and 7352 for mesh applications, since these models do support mesh over 2.4GHz. This "work-around" is no longer viable however, as all Ruckus' single band AP's have now gone end-of-sale.

As a result, in order to continue to serve customers in these countries who wish to deploy mesh, Ruckus dual-band APs will support mesh over 2.4GHz from this release onwards.

DHCP/NAT Hierarchical Network Topology (HNT) Feature

- Only DHCP/NAT VLANs are supported at non gateway APs when the option *Enable on hierarchical APs* is selected. This is because the controller AP does not have capability to bridge other VLAN traffic.
- If the general port is part of the device Ethernet port configuration, then the VLANs of the general port configuration should be match with DHCP VLANs.
- APs with only one Ethernet port cannot be select as the hierarchical network gateway AP. The option *Enable on each AP* supports DHCP/NAT only for wireless clients. This is applicable for APs which have only one Ethernet port. For APs with multiple Ethernet ports DHCP/NAT on wired clients is supported.
- The option *Enable on each AP and Hierarchical network* does not support LACP (Link Aggregation Control Protocol) or bonding.
- When enabling the option DWPD (Dynamic Wan Port Detection), selecting of LAN port is not dependant on the state (link UP/DOWN) of Ethernet port. The first eligible port is selected for LAN.
- For MESH high availability to work, LAN Ethernet ports of controller APs must be connected through the same switch.

NOTE

- DHCP/NAT functionality is not tested with the cable modem APs in this release.
- This feature is tested with 1-hop mesh in this release.
- Ethernet connected for mesh AP is not supported

Additional Enhancements

The following additional enhancements have been made in the 5.0 release:

1. Added a facility in the console to provide factory default as well as administrator password recovery by interrupting the system boot process
2. The administrator has the configuration to disable APs from broadcasting an Island SSID.

3. AES-256 Ruckus GRE tunnel is now supported.
4. The web interface adopts a new enable or disable slider component instead of check boxes.
5. The web interface color scheme has been updated for easy usability.
6. The web interface adopts a new display method for critical warnings in the header.
7. The device description can now be changed through API (Application Programming Interface).

Changed Behavior

Geo Redundancy

The following are the changed behavior issues related to Geo Redundancy.

Configuration

- This release supports different primary AAA (Authentication, Authorization and Accounting) server configurations between active and standby cluster. Secondary server for non-proxy / proxy server is not supported.

Configuration backup

[SCG-80329, SCG-80330]

- Standby cluster will retain the last two configuration backup files per active cluster.
- All configuration backup files in the standby cluster will be deleted when cluster redundancy is enabled for the first time.

SSH monitor mechanism

[SCG-78862, SCG-84823]

- When a standby cluster is already assigned to an active cluster, this standby cluster keeps monitoring the active cluster state **through its own control interface** until the cluster redundancy in active cluster is disabled or certain active cluster from the standby cluster is deleted. Follow the below steps to change the standby cluster.
  - Disable cluster redundancy in active cluster, then enable it with new standby cluster IP address or
  - Change standby cluster IP address in active cluster, then delete active cluster in original standby cluster
- Standby cluster can configure to monitor three active clusters.
- Standby cluster is able to serve APs failover from one active cluster at a time.
- To enable cluster redundancy for monitoring health status of active cluster, standby cluster builds SSH connection to control the IP address or NAT server of active cluster through its own control interface. This means that the control interface of standby cluster is able to communicate with the control interface or to the NAT server of the active cluster, or the cluster redundancy will **not** work.

Upgrade

- For one node active cluster, APs connected to active cluster may failover to standby cluster when active cluster reboots.
- Standby cluster allows upgrade only when it is in *Monitor* mode, which means standby cluster does not serve any active cluster and **no** AP connects to it .

- All legacy configuration backup files in standby cluster will be removed on upgrade.
- After upgrading from release 3.6 or 3.6.1 to 5.0, click on **Sync Now** button in active cluster(s) to make sure all data is consistent between active and standby clusters.

Limitation

- In this release enabling geo redundancy is only for **one** node active/ standby cluster with the IPv4 address or dual stack (IPv4 + IPv6) control IP address. A standby cluster can still support up to three active clusters.

ICX Registration

The following is the registration of ICX on the controller.

ICX Registration

- For registering NON TPM ICX Models like 7250/7450/7750, use the following CLI command at controller.

```
ruckus> enable
ruckus# config
ruckus(config)# non-tpm-switch-cert-validate
```

- If the controller or ICX is behind the NAT server make sure to forward the TCP ports 443 and 22 through the NAT server.

Hardware/Software Compatibility and Supported AP Models

- Overview....19
- Release Information....20
- Supported and Unsupported Access Point Models....20

Overview

This section provides release information about the SmartZone 300 (SZ300), the SmartZone 100 (SZ100), Virtual SmartZone (vSZ), and Virtual SmartZone Data Plane (vSZ-D) features with notes on known issues, caveats, and workarounds.

- The SZ300 Flagship Large Scale WLAN Controller is designed for Service Provider and Large Enterprises, which prefer to use appliances. The Carrier Grade platform supports N+1 Active/Active clustering, comprehensive integrated management functionality, high performance operations and flexibility to address many different implementation scenarios.
- The SZ100, developed for the enterprise market, is the next generation midrange, rack-mountable WLAN controller platform for the enterprise and service provider markets. There are two SZ100 models: the SZ104 and the SZ124.
- The vSZ, which is available in *High Scale* and *Essentials* versions, is a Network Functions Virtualization (NFV) based WLAN controller for service providers and enterprises that desire a carrier-class solution that runs in the cloud. It supports all of the WLAN controller features of the industry leading, while also enabling the rollout of highly scalable and resilient wireless LAN cloud services.
- The vSZ-D offers organizations more flexibility in deploying the SZ data plane as needed in an NFV architecture-aligned fashion. Deploying vSZ-D offers secured tunneling of user data traffic that encrypts payload traffic, maintains flat network topology, enables mobility across L2 subnets, supports POS (Point of Sale) data traffic for PCI (Payment Card Industry) compliance, and offers differentiated per site policy control and QoS (Quality of Service), etc.

NOTE
By downloading this software and subsequently upgrading the controller and/or the AP to release 2.5.1.0.177 (or later), you understand and agree that:

- The AP may send a query to Ruckus containing the AP's serial number. The purpose of this 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.
- You also understand and agree that this information may be transferred and stored outside of your country of residence where data protection standards may be different.

Release Information

This section lists the version of each component in this release.

SZ300

- Controller Version: **5.0.0.0.675**
- Control Plane Software Version: **5.0.0.0.627**
- Data Plane Software Version: **5.0.0.0.675**
- AP Firmware Version:**5.0.0.0.753**

SZ100

- Controller Version: **5.0.0.0.675**
- Control Plane Software Version: **5.0.0.0.627**
- Data Plane Software Version: **5.0.0.0.215**
- AP Firmware Version: **5.0.0.0.753**

vSZ-H and vSZ-E

- Controller Version: **5.0.0.0.675**
- Control Plane Software Version: **5.0.0.0.627**
- AP Firmware Version: **5.0.0.0.753**

vSZ-D

- vSZ-D software version: **5.0.0.0.675**

Supported and Unsupported Access Point Models

Before upgrading to this release, check if the controller is currently managing AP models that are no longer supported in this release.

APs preconfigured with the SmartZone AP firmware may be used with the SZ300, SZ100, or vSZ in their native default configuration. APs factory-configured with the ZoneFlex-AP firmware may be used with the SZ100/vSZ when LWAPP discovery services are enabled.

On solo APs running release 104.x, the LWAPP2SCG service must be disabled. To disable the LWAPP2SCG service on an AP, log on to the CLI, and then go to enable **mode** > **config** > **lwapp2scg** > **policy deny-all**. Enter **Yes** to save your changes.

> **NOTE**
> Solo APs running release 104.x are capable of connecting to both ZD and SZ controllers. If an AP is running release 104.x and the LWAPP2SCG service is enabled on the SZ controller, a race condition will occur.

Supported AP Models

This release supports the following Ruckus AP models.

TABLE 1 Supported AP Models

11ac-Wave2		11ac-Wave1	
Indoor	**Outdoor**	**Indoor**	**Outdoor**
R720	T710	R700	T504
R710	T710S	R600	T300
R610	T610	R500	T300E
R510	T310C	R310	T301N
H510	T310S	R500E	T301S
C110	T310N		FZM300
H320	T310D		FZP300
M510	T811CM		
	T610S		
	E510		

Important Note About the PoE Power Modes of the R720, R710, T610, and R610 APs

NOTE
When the R720, R710, T610 series AP is connected to an 802.3af PoE power source, the USB interface and the second Ethernet port are disabled, and the AP radios do not operate in maximum capacity. For more information, refer to the latest Outdoor Access Point User Guide or Indoor Access Point User Guide.

Unsupported AP Models

The following AP models have reached end-of-life (EoL) status and, therefore, are no longer supported in this release.

TABLE 2 Unsupported AP Models

Unsupported AP Models				
SC8800-S	ZF7762-S-AC	ZF2741	ZF7762-AC	ZF7351
ZF7321	ZF7343	ZF7962	ZF7762-S	ZF2942
ZF7441	ZF7363-U	SC8800-S-AC	ZF7363	ZF2741-EXT
ZF7762	ZF7025	ZF7321-U	ZF7341	ZF7352
ZF7762-T	ZF7351-U	ZF7761-CM	ZF7343-U	ZF7781CM
R300	ZF7782	ZF7982	ZF7782-E	ZF7055
ZF7372	ZF7782-N	ZF7372-E	ZF7782-S	R730
C500	H500			

Caveats, Limitations, and Known Issues

- AP KPI Known Issues....23
- AP Known Issues....23
- AAA Known Issues....29
- Application Recognition and Control (ARC) Known Issues....29
- Bonjour Fencing Known Issues....31
- Bonjour Gateway Known Issues....31
- Control CLI Known Issues....31
- Control Communicator Known Issues....31
- Control Domain Known Issues....32
- Control Platform Known Issues....32
- Geo Redundancy Known Issues....32
- ICX Known Issues and Limitations....33
- ICX-M Known Issues and Limitations....33
- MSP Known Issues....34
- Public API Known Issues....34
- Rate Limiting Known Issues....34
- Scalability, Stability, and Performance Known Issues....35
- Session Manager Known Issues....35
- SNMP Known Issues....35
- Syslog Known Issues....35
- System Known Issues....35
- UI/UX Known Issues....37
- Virtual SmartZone Known Issues....39
- Virtual SmartZone Data Plane Known Issues....39
- Visual Connection Diagnostics Known Issues....40
- Wired Clients Known Issues....40
- WISPr Known Issues....41
- ZoneDirector to SmartZone Migration Known Issues....41

AP KPI Known Issues

The following are the known issues related to access point KPI.

- When the AP sends bidirectional traffic, the estimated AP capacity shown on the web interface is incorrect. **[SCG-65376]**

AP Known Issues

The following are the known issues related to APs.

- APs may not be balanced or distributed equally among the virtual data planes, when zone affinity is mapped to AP zones. **[SCG-69178]**
- iMAC, MAC pro, MAC book pro(model 9,2) MAC air (model6,2) and MAC mini clients are not able to associate with Z2 country code. **[SCG-71699]**

- If APs are discovering the controller on the network using DNS discovery and the DNS server address on the DHCP server is updated, solo APs will continue to use the previous DNS server address, which could result in their inability to discover the controller again on the network. **[SCG-34299]**

  Workaround: To resolve this issue, reboot solo APs after the DNS server address on the DHCP server is updated.
- Solo APs are unable to discover the controller via Option 52. This is because DHCPv6 solicit messages from solo APs do not include Option 52 information. **[SCG-34885]**
- Some of the options for the Certificate Store page may not show up on the Safari web browser. **[SCG-34971]**
- If only Option 52 (no DNS server address) is configured on the DHCPv6 server, APs are unable to obtain the controller's IP address from the Option 52 information and, therefore, are unable to discover the controller on the network. **[SCG-34981]**
- When the location information of a zone is configured, this information is inherited by APs that belong to the zone (unless AP-specific location information is configured). If the location information of the zone is cleared (deleted), this absence of location information is propagated to the APs. As a result, the APs retain the location information previously configured for the zone, which may no longer be valid. **[SCG-39848]**

  Workaround: To clear or update the location information on APs, do it at the AP level (instead of the zone level).
- When an AP switches to another cluster, authorized hotspot (WISPr) clients are unable to log off from the original portal page. **[SCG-41756]**
- Based on the current design, the minimum rate limit per station is 100kbps. As a result, the total rate (station number * 100kbps) will be higher than the SSID rate limit -- this is design intent. For example, if the rate limit for downlink is 10Mbps for one SSID, when an AP has 200 STAs associated with that SSID, the total rate will be 200 * 100kbps = 20,000kbps = 20 Mbps > 10Mbps. **[SCG-43697]**

  Workaround: Limit the maximum clients number per WLAN. Using the above example, you can set the maximum clients per WLAN to 100.
- The 5GHz recovery SSID interface has been disabled on the T710 and R710 APs. **[SCG-44242]**
- The R710 and R510 APs do not support the RTS packet size threshold when operating in 802.11ac 20MHz mode. **[SCG-45294]**
- Multicast traffic is always directed as unicast traffic, even when the AP has more than five clients associated with it. **[SCG-46967]**
- Client frame IP addresses are sometimes sent as 0.0.0.0 in AP-initiated accounting messages. **[SCG-47164]**
- Solo APs running release 100.x may be unable to obtain firmware from the controller's captive portal if the captive portal is behind NAT. **[SCG-47518]**

  Workaround: Disable NAT IP translation if the captive portal is behind NAT. On the CLI, run the command "no nat-ip-translation" in the **config** > **lwapp2scg** context.
- When wireless clients based on Intel Dual Band Wireless AC-7256 and Intel Centrino N 6300 AGN, and Samsung S5 mobile devices fail to perform Opportunistic Key Caching (OKC) roaming, they go through full 802.1x authentication instead. **[SCG-48792]**
- BEACON-MISS may be observed on the wlan63 interface of mesh APs if the channel on the root AP changes continuously. **[SCG-49635]**
- The WLAN scheduler closes a WLAN one hour ahead of schedule because the AP does not take into consideration daylight saving time (DST). **[SCG-50883]**

  Workaround: Make sure that the "Daylight Saving Time" check box on the **Access Points** > **System > Select the Zone > Configuration** page is not selected.

- Microsoft Surface 3 Pro does not respond to ADDBA request frames with Action frames, which can cause the AP to send frames to the client without AMPDU. **[SCG-51385]**
- Beginning with ZoneFlex standalone AP version 104.0, APs will delay joining a ZoneDirector in favor of joining a SmartZone controller for 30 seconds, if both controllers exist on the same L2 subnet. However, in some situations, the AP can still potentially join the ZD instead of the SZ when both controllers are set to auto approve. **[SCG-51529]**

  Workaround: Do not deploy both ZD and SZ controllers on the same L2 subnet, or there will be potential for APs to join the ZD instead of the SZ.
- The Ethernet port on the H510 AP does not auto negotiate the data transmission rate when the port speed is changed from 10Mbps to 100Mbps. **[SCG-51790]**
- The 802.1X Ethernet port (supplicant) on the H510 AP does not reply to EAP identity requests when the link is disconnected, and then reconnected. **[SCG-51975]**
- H510 802.1X enabled Ethernet interface configured for MAC-based authentication fails to authenticate supplicants. **[SCG-51986]**
- When the Ethernet port on the H510 AP is configured to use either MAC-based or port-based authentication, MAC authentication bypass cannot be enabled using the CLI. **[SCG-53376]**
- Client events are not shown by default on the **Monitor** > **Events** page. To view client events, set the **Category** filter to **Clients**, and then click **Load Data**. **[SCG-54202]**
- In a two-node cluster, Smart Monitor causes APs to lose connection with the controller. When an AP resumes its connection with the controller, the AP sends Accounting-On message to the controller, but the controller never forwards the same Accounting-On message to the AAA server. **[SCG-60852]**
- Rebooting the H510 AP using the CLI causes the AP to log a 'Kernel Panic' event. No operational effect is observed beyond the log message during reboot process.**[SCG-54682]**
- The cable modem-related status LEDs on the C110 AP cannot be disabled from the controller's web interface. **[SCG-56903]**
- On the controller's web interface, the LAN port status for the C110 is mislabeled. Additionally, LAN1/LAN2 mapping is incorrect. **[SCG-58332]**
- When the C110 AP is using an Ethernet backhaul (instead the CM), the cable modem serial number cannot be displayed on the access point detail page on the controller's web interface. **[SCG-59255]**
- The valid management traffic rates for the 5GHZ radio are 6Mbps, 12Mbps, and 24Mbps. Ruckus Wireless recommends restricting the management traffic rates to these values using the rate limiting features. **[SCG-60865]**
- The temperature and packet-per-second (PPS) cost metric drops for an indeterminate amount of time. **[SCG-61247]**
- When the 7273 AP starts downloading the latest firmware from a legacy zone and the controller control IP is unreachable, the AP stops responding. **[SCG-61448]**
- A UE can access a mismatched whitelist (valid MAC address but invalid IP list) after it has been connected to the WLAN for five minutes. **[SCG-62531]**
- When a mesh is formed in 80+80 MHz mode, wireless clients are unable to send and receive traffic reliably. [SCG-62866, SCG-63990]
- Configuring static link speed on the 2.5GHz Ethernet port of the R720 AP using the Ruckus AP CLI is unsupported. The port will auto negotiate to 2.5Gbps/1000Mbps/100Mbps. **[SCG-63519]**
- The AP starts ChannelFly for the 5GHZ radio 30 minutes later than the 2.4GHz radio. **[SCG-63561]**
- The H510 AP does not support PoE operating mode. **[SCG-64376]**
- Multicast/unicast communication still occurs even after client isolation is enabled for an APLBO WLAN. **[SCG-64652]**
- Client isolation across different WLANs mapped to different VLANs is not supported. **[SCG-65754]**

- Rogue AP detection does not work if the rogue AP's channel is not on the list of Ruckus AP operating channels. **[SCG-67158]**
- The PoE injector detection mechanism may be unreliable. Ruckus strongly recommends manually configuring the PoE injector to use 802.3at mode. **[SCG-67161]**
- LACP does not work on H320. **[SCG-67412]**
- The R710 AP stops responding as a result of memory leak and "Target Fail Detected" error. This issue occurs when the AP's MTU size for LAN1/LAN2 is set to a value greater than 1978 bytes. **[SCG-67512]**
- Wired client is seen as authorized after the AP upgrades or reboots. **[SCG-67987]**
- The force power modes (at+, at or af) are designed for interoperability with PoE injectors. No LLDP Power over MDI TLV is advertised by the AP. If, for any reason, forced at+ or at mode is configured when the AP is connected to a switch port, then the appropriate static power must be configured on the switch port. The switch port power static allocation must be higher than AP port (PD).
  - AF: Force AP to run at 802.3af power, 12.95W at PD
  - AT: Force AP to run at 802.3at power, 25W at PD
  - AT+: Force AP to run at 802.3at+ power, 35W at PD **[SCG-68042]**
- When an R720 AP is downgraded from release 3.5.1 to 3.5, it remains in AF mode and is unable to transition to AT power mode. **[SCG-68405]**

  Workarounds:

  - Reset the R720 to factory default settings.

  - Perform LLDP set via RKS CLI, and then reset the AP to “set LLDP power 25000”.
- In 80+80 MHz mode, when configuring static channel 36 as primary and 132-144 as secondary and upgrading from release 3.5 to3.5.1, the user will run into state where release 3.5.1 zone settings will show "no-data" in the secondary channel and the user will not be able to apply any configuration changes in the zone. **[SCG-68602]**

  Workaround: Edit the secondary channel field with available channels, and then apply the configuration.
- The "Mesh Mode" and "Mesh Role" columns incorrectly display "Auto," when they should actually display "Not Applicable" as the H320 AP does not support mesh. **[SCG-69227]**
- On an abrupt shutdown (power down) of the AP and the Single Accounting Session ID is enabled, the accounting start is seen instead of interim update after the UE roams to another AP. **[SCG-69945]**
- VLAN-ID value has zero (0) as the default value when the option Subopt-1 is selected for DHCP Relay under DHCP Option 82. **[SCG-70971]**
- Wireless Multicast communication happens between clients on the same AP and same WLAN, even when Client Isolation is enabled for that WLAN. **[SCG-73791]**
- When primary DHCP server is recovered, lease file copied from the secondary DHCP server may expire if it is copied prior to time synchronization. **[SCG-76058]**
- Airplay Bonjour service can be seen between clients connected to the same AP even if they are in different VLANs. **[SCG-73004]**
- URL filtering may need to do a reverse lookup of domain names from destination IP address in APs DNS cache. If a server (IP address) hosts multiple domains (or if the IP isn't present in DNS cache) the APs will not be able to categorize the URL correctly due to wrong domain name found against an IP address from APs DNS cache. **[SCG-74011]**
- Currently if AP-DHCP profile is enabled with DNS override, AP-DHCP profile settings take precedence. **[ER-5493]**

  Workaround: Change the settings of AP-DHCP profile to reflect the same as DNS override, to override the issue.
- LACP does not work on R510. **[SCG-67394]**

- This is a client limitation affecting devices MotoXStyle(6.0), Samsung Note4(5.0.1), Samsung Alpha(5.0.2), Samsung S7 X, Samsung S8 where they are unable to move to 5G band from 2.4G when the channel in use is an outdoor one. This happens when Band Balancing is enabled with Proactive or Strict options. **[SCG-70949]**
- For RKS-GRE or SoftGre the tunnel MTU may not reflect the correct value if the br0 interface MTU is set to non-default value. Default value being 1500. This could happen if customer is upgrading the code from 3.5 to 3.6 wherein if the tunnel MTU was configured for value lesser than 1500, after upgrade the MTU will be retained affecting the tunnel MTU set, which will depend on br0 interface MTU. May need to manually reset the mtu on the AP to 1500, to fix this behavior. **[SCG-73405]**
- If a zone that has been added to a report is deleted, the corresponding report will fail to be completed because the zone is missing.**[SCG-76181]**
- NAT IP and port configuration is only used by AP, therefore when it is configured by the controller, this configuration does not move it to the data plane. Data plane always reports the NAT information, which is configured through virtual data plane CLI.**[SCG-76345]**
- After creating an Ethernet profile for an Ethernet port and adding VLAN tag, the Ethernet profile is not available for AP T811 Lan3 and Lan4 Ethernet ports. The created profile is available for other APs.**[SCG-77639]**
- SNMPv1 gets enabled on the AP when enabling SNMPv2. **[SCG-77981]**
- ARC does not work properly when user defined ARC is created but it is not associated with any UTP profile.**[SCG-80218]**
- After the accounting service is disabled for a particular WLAN, Accounting Off messages are not initiated. **[SCG-47772, SCG-40827]**
- APs H510 and H320 due to difference in nomenclature in comparison to other APs is mapped to LAN1 instead of Ethernet (eth) 0 and eth1 (eth2 to Lan2 so on and finally, eth0 is mapped to LAN3 for H320 and LAN5 for H510.)

  Due to this difference in nomenclature during manual configuration LAN1 and LAN2 in the DHCP/NAT will be referring to eth1 and eth2 respectively instead of eth0 and eth1. Hence for the APs eth0 should be by default marked as WLAN always and depending on the manual configuration, client should connected the eth1 or eth2 to LAN switch for Hierarchical Network Configuration.

  Apart from this client can any time select the AP advanced option in web interface to configure /choose any other port such as eth3/eth4 depending on AP models and number of ports to be LAN. APs will mark one of the Ethernet ports as LAN. **[SCG-79169]**
- When IPSec tunnel WLAN is configured the first time, APs with this WLAN must be rebooted for this new configuration to be applied correctly. **[AP-8162]**
- APs and Controllers report on SCI still shows configuration details of the disabled partner domains and zones. **[SCG-80309]**
- AP model ZF-7372 (128 MB RAM) should not be used in high density environment. **[AP-7201]**
- When an AP that is assigned the default static IP of 192.168.0.1 is rebooted, it is unable to establish a tunnel with the controller. **[ER-3433]**
- Client isolation is not supported when a client roams from one AP to another in the same WLAN. **[SCG-66077]**
- SmartZone controller can only accept COA (Change of Authorization) or DM (Disconnect Message) to control the wireless client after the wireless client gets the IP address. **[SCG-73119]**
- It is recommended to use MDNS enabled when you deploy tunneled WLAN with Apple TV and airplay support. Just make sure that the Apple TV is not connected to the Ethernet tunneled port on the AP but on the WLAN tunnel or on the network Local Breakout in the core network. **[SCG-74976]**
- The AP E510 will be automatically rebooted when external antenna gain setting is modified. **[SCG-78247]**
- An AP reboot is required when enabling and disabling the non-Beamflex antenna (Part Number: 911-0505-DP01). **[SCG-81588]**

- AP Tx power is not reverting to default values after applying non-Beamflex antenna (Part Number: 911-0505-DP01) gain and switching back to a Beamflex antenna (Part Number: 902-2101-0000). **[SCG-81705]**

  Workaround : Set 3 dBi for 2.4 GHz and 5 dBi for 5 GHz, apply the configuration and disable the non-Beamflex antenna (Part Number: 911-0505-DP01). Another option is to factory reset the AP.
- SoftGRE tunnel re-establishment does not get re-initiated post fail over when both primary and secondary SoftGRE gateways are down. This occurs when three tunnels having primary and secondary gateways are all down but not when a single tunnel with primary and secondary gateways is configured. **[AP-8738]**

  Workaround:

  1. Reboot the AP

  2. Make all SoftGRE enabled WLANs as LBO and then re-configure these WLANs to respective SofTGRE profiles.
- AP does not auto negotiate with switch ports when the switch is configured with half duplex. **[SCG-78457]**
- Following are the limitations on packet capture. **[SCG-83772]**
  - Batch operation is not allowed. Users can only enter the packet capture dialog when a single AP is selected.
  - Even if a user specifies an interface, all interfaces are seen in Wireshark and the user can pick any interface to collect the packets, but the configured filters (frame type and MAC) will only be applied to the interface which is selected from web user interface or public API.
  - Even though users can see all the available interfaces from Wireshark station in the streaming mode, only the Wi-Fi interface that is enabled through the web user interface will work in promiscuous mode. Ethernet ports always work in promiscuous mode.
  - A user with proper privileges can stop an ongoing capturing task. For example, if administrator A starts capturing task on AP1, administrator B can stop this task at a later stage.
- The following are the Zero touch mesh limitations. **[SCG-48895 SCG-89397]**
  - Zero-touch mesh only supports 5Ghz
  - Zero-touch mesh only supports Solo AP 110+ and SZ AP 5.0+
  - When Solo AP upgrades from previous release (for example 104 or 106) to 110, AP needs a set factory option to activate zero-touch mesh
  - When Solo AP has the updated configuration (for example, WLAN configuration update), the AP needs a set factory option to activate zero-touch mesh
- Channel mismatch occurs between the AP and controller. **[SCG-81036]**
- AP does not allow association of more than 200 clients per WLAN when transient client MGMT is enabled though AP supports clients per radio of 256. **[SCG-81340]**
- AP reports the value as zero or not applicable to the controller when the connection failure bar is not displayed in the specified color codes on the web user interface. **[SCG-89427]**

M510 AP

- AP-to-AP communication in M510 does not work when the backhaul is LTE (Long Term Evolution). This may impact features like Fast Roaming, Bonjour Fencing and 11r. **[SCG-82513]**
- Power LED keeps blinking after M510 failover from Ethernet to LTE. This does not impact the functionality. **[SCG-89036]**
- When the power mode is **auto** and power injector is used, the AP power mode is automatically set to 802.11AF mode. [SCG-88994 SCG-88902]

  Workaround: Manually set the mode statically to 802.11AT and reboot the AP.
- Ruckus GRE tunnel cannot be re-established when LTE module is reset through AP CLI command.**[SCG-89127]**

Workaround: Reboot the AP.

- After rebooting the M510, USB power and GPS stay enabled even after disabling it from controller web user interface and the power mode is set as 802.11AT. **[SCG-84897]**
- The controller web user interface does not have the option to upgrade LTE firmware. **[SCG-84194]**

  Workaround: Use the AP CLI to upgrade LTE firmware.
- Cellular backhaul connection in M510 has roaming feature enabled by default and this option cannot be changed. **[SCG-82191]**
- M510 does not support SIM hot plug. It does not detect the SIM installation on the secondary SIM. **[SCG-81050**]
- Smart mesh support will come in the future release of M510. **[SCG-85203]**

AAA Known Issues

The following are the resolved issues related to the AAA server.

- The controller does not support multiple LDAP AAA server profiles that use the same IP address and port number. **[ER-3948]**
- The controller does not support the Chargeable-User-Identity (CUI) attribute through WISPr accounting messages. **[SCG-47816]**
- The R710 and T710 APs do not honor the idle timeout setting as received in the RADIUS access accept message. **[SCG-48133]**
- When the controller initiates a RADIUS Accounting Off message to an IPv6 Accounting server, the value of Ruckus-SCG-CBlade- IP in the message is zero '0'. This issue occurs when an AP abruptly goes offline and does not come back online within a certain period of time. **[SCG-62289]**
- In this release onwards, when WLAN with proxy authentication mode, only CCD (Client Connection Diagnostics) message on AAA radius proxy is supported. If AD (Active Directory) or LDAP (Lightweight Directory Access Protocol) server is selected as the authentication server in proxy mode, CCD message are not supported. **[SCG-80988]**
- Certain fields in the Client Diagnostic page could be blank when WLAN is web authenticated with proxy mode and uses AD/LDAP as the authentication server. **[SCG-78481]**

Application Recognition and Control (ARC) Known Issues

The following are the known issues related to ARC.

- ARC rate limiting for user-defined applications does not work on fragmented packets. **[SCG-65933]**
- ARC is unable to identify Vindictus traffic accurately. **[SCG-43487]**
- ARC with ARC / DPI engine is unsupported on the following AP models (<= 128 MB RAM platforms) **[SCG-50596]**:
  - ZF7982
  - ZF7782/ZF7782-S/ZF7782-N/ZF7782-EZF
  - 7781CM
  - R300
  - ZF7372/ZF7372-E
  - ZF7352

  - ZF7055
  - H500
- When ARC cannot determine the application that a device is using, the controller displays the device's IP address as the application name. **[SCG-47746]**
- The ARC engine that is used by ARC recognizes TFTP traffic based on port69. Since only the first packet of TFTP traffic uses port 69, only the first packet is detected as 'tftp'. [SCG-44064]
- Sometimes, an application that has been configured to be denied still passes data through the AP. **[SCG-61444]**
- ARC is unable to identify BitTorrent traffic accurately. **[SCG-43336]**
- When configuring a denial policy in ARC, take note of the following limitations: **[SCG-44384]**
  - When "google.com" is set as the ARC denial policy, traffic to the Google website may not be blocked because most Google traffic is encrypted. Google traffic is marked "Google(SSL)" or "SSL/TLS," which does not match the policy, so traffic is not denied.
  - When "music.baidu.com" is set as the ARC denial policy, traffic to the Baidu web site may not be blocked because most Baidu traffic is marked as "BaiduMusic" or "baidu", which does not match the policy, so traffic is not denied.
  - BitTorrent download traffic may be difficult to block unless the app IDs, such as "BitTorrent Series", "BBtor","eDonkey Series", "SoMud", etc, are specified in the policy. If you set the denial policy to "xxx. net", " xxx.cn", "xxx.org" , etc., ARC will be unable to block such traffic because ARC engine recognizes the app name without the domain extension.
  - To block Sina mail traffic, deny traffic to both "sina mail" and "sina.com."In the denial policy, the space character is taken into consideration. For example, if you block "qq game" or "sina video", users will still be able to access "qqgame" or "sinavideo" (no space character). Conversely, if you block "baidumusic" (no space character), traffic to "baidu music" will not be blocked.
  - When blocking Hotmail or Outlook.com traffic, set the denial policy to "live" or "live.com". If you block "hotmail" or "outlook.com", user will still be able to access Outlook.com.
- If a Skype P2P tunnel is set up before the Application Denial Policy is applied, the controller cannot identify the traffic and will allow the call through. **[SCG-52257]**
- When the uplink QoS is marked with DSCP, it marks both Dot1p and DSCP for clients configured with a static IP address. **[AP-3869]**
- Configuring a rate limit rule for a single direction impacts both the directions for clients configured with a static IP address. **[AP-4065]**
- ARC does not support clients that are assigned IPv6 addresses. **[AP-4835]**
- ARC is unable to apply policies consistently to apps that cannot be identified by Deep Packet Inspection (DPI). **[SCG-60339]**
- R600 is unable to detect and deny the 4shared app running on an Android device. **[SCG-70027]**
- Any change in ARC policy resets the pre-existing policy to null. R710/R610/R510 APs are not affected while other or the rest of the AP models are affected. **[AP-5480]**
- R710 AP in non gateway AP mode is not able to deny the tftp traffic. **[SCG-70475]**
- R600 AP detects Instagram as Facebook traffic. **[SCG-70636]**
- The ARC deny rule do not work on proxied YouTube streaming traffic. This issue occu because the signature package and DNS do not recognize this type of traffic as YouTube traffic. **[AP-5122]**
- Denial rule does not work for Skype application on R710 AP. **[AP-5225]**
- Clients are able to access Gmail and Google+ service access though the deny rule is set. **[AP-5226]**
- Clients are able to access eBay services though the deny rule is set. **[AP-5347]**
- Denial rule does not work for WhatsApp messenger on R710 AP. **[AP-5561]**

Bonjour Fencing Known Issues

The following are the known issues related to bonjour fencing.

- Bonjour fencing does not work on a mesh network. **[AP-4115]**
- If AirPlay Services are configured for hop0 fence, they may still be discoverable on an AppleTV outside hop0. **[AP-4455]**
- Bonjour Fencing might not work as expected with Apple TV 3 Rev. A (model A1469) and later versions. This is a known issue and will be fixed in upcoming releases. **[SCG-63167]**
- Bonjour Fencing is not supported for DHCP/NAT GW AP. **[SCG-64346]**
- The Bonjour service is unable to establish a fence using the fencing neighbor's RSSI. **[SCG-59625]**

Bonjour Gateway Known Issues

The following are the known issues and limitation related to Bonjour Gateway.

- **Limitation in Bonjour Gateway Rule**:

  Each Bonjour Gateway rule is configured to advertise per service from one VLAN (VLAN-X) to another VLAN (VLAN-Y). This is a limitation because the To VLAN (VLAN-Y) is just a single VLAN ID and does not allow configuration of a range (like VLAN100-VLAN164) or comma separated values (like VLAN100,VLAN119,VLAN140).

  A maximum of only 32 rules are allowed in a Bonjour Gateway Policy. This adds a limitation that only a specific service can span up to 32 other VLANS. Also if service-1 spans to 32 different VLANS then you cannot have other bonjour services [there are 20 such bonjour services present in R3.6 excluding Chromecast service] to span to other VLANS (due to maximum 32 rule limit). **[SCG-73134]**

Control CLI Known Issues

The following are the known issues related to Control CLI.

- The CLI configuration logic differs between configuring individual APs and configuring model-specific settings from the AP group context. **[SCG-52077]**
- When the SMTP settings on the controller are configured and the outbound firewall is enabled, the SMTP packets are dropped. **[SCG-64943]**

Control Communicator Known Issues

The following are the known issues related to Control Communicator.

- APs running earlier releases (for example, release 2.5) are unable to join the controller to upgrade their firmware. This issue occurs because of SSL incompatibility in earlier SmartZone releases. **[SCG-47886]**

Control Domain Known Issues

The following are the known issues related to Control Domain.

- If the NAT IP address is configured on the controller, the external subscriber portal (SP) can communicate with the control interface but not with the management interface. **[VSCG-1509 SCG-87235]**
- When Virtual Router Redundancy Protocol (VRRP) is used to set up redundant SZ-100 controllers and one of the controller is rebooted, it may be unable to obtain an IP address from the DHCP server. **[SCG-41046]**

  Workaround: To resolve this issue, Ruckus Wireless recommends assigning a static IP address to the SZ100 network interface.
- When rate limits are modified, the new limits are not applied to clients that are in the grace period. **[SCG-51422]**
- The forwarding service is unsupported on the SZ100, therefore related options are automatically removed when the controller software is newly installed. However, if forwarding service profiles were created in release 3.1.2 and the controller is upgraded to a newer release, these profiles are not automatically removed and can still be configured in the WLAN settings, but the settings are not applied. **[SCG-45440]**
- When a two-node cluster is freshly installed, the default node affinity profile is created for only one node, not for both nodes. **[SCG-46655]**
- Rebalance AP feature is not available for single node cluster. **[SCG-69261]**
- When you configure an internal DPSK name with full length, you may see the username truncated in the clients page. **[SCG-73259]**
- When testing an IPv6 accounting server, the NAS IP4 attribute is sent in the accounting message. **[SCG-61667]**

Control Platform Known Issues

The following are the known issues related to Control CLI.

- The ZoneDirector to SmartZone migration process uses IPv4 addresses. SmartZone currently does not support the migration of APs that are using only IPv6 addresses. **[SCG-58804]**

Geo Redundancy Known Issues

The following are the known issues related to Geo Redundancy.

Outbound firewall

- If cluster redundancy and outbound firewall are both necessary, enable cluster redundancy first and then outbound firewall. **[SCG-80538]**

ICX Known Issues and Limitations

The following are known issues and limitations related to ICX.

General Category

Caveats

- Do not configure telnet client <*any ip*> on ICX for firmware upgrade, configuration backup and restore to be successful. **[SCG-84917]**
- The option *no telnet server* configuration should not be configured on ICX. **[FI-186530]**

Limitations

- Connection to the controller fails when the SSH key is deleted and regenerated on the switch.

ICX-M Known Issues and Limitations

The following are known issues and limitations related to ICX-M.

General Category

Limitations

- Switch model (skew number) mismatch between general main page of switches and general tab of the corresponding switch. **[FI-185545]**
- The option *no telnet server* configuration should not be configured on ICX. **[FI-186530 SCG-84917]**

Cluster Support

Caveats

- When adding a new node to the existing cluster on the controller may not result in auto load of switch firmware in the controller cluster. **[SCG-88979]**

  Workaround: Load the switch firmware to the newly joined node in the cluster.

Limitations

- Geo-redundancy feature doesn't support ICX switches. **[SCG-82509]**

Configuration Backup and Restore

Limitation

- Configuration backup or restore or firmware upgrade scheduled at same time will result in failure of any one process. **[SCG-85322]**

Firmware Upgrade

Caveats

- Uploading of switch firmware by the super administrator without system domain resource access is not supported. **[SCG-89019]**

  Workaround: Upload the switch firmware to the controller using super administrator rights having access to system domain

Ports

Limitation

- Search based on POE (Power Over Ethernet) value is not supported. **[SCG-85353]**

MSP Known Issues

The following are the known issues related to the MSP feature.

- A UE can log on to a hotspot WLAN on one partner domain using the credentials of a local user on different partner domain. **[SCG-57260]**
- A partner administrator is able to obtain the status of a client on a different partner domain through the northbound interface. **[SCG-57518]**
- The MSP and MVNO features are mutually exclusive.

Public API Known Issues

The following are the known issues related to the Public API.

- Every SmartZone release is compatible with the three most recent major Public API versions. SmartZone release 3.5 is compatible with v3_0 (including v3_1), v4_0, and v5_0 of the public API. **[SCG-53762]**
- RESTful APIs (https://SCG_ManagementIP:8443/wsg/api/rest/) are not supported. **[SCG-64370]**
- Creating an AAA service for AP zones that are managed by MVNO using the Public API is currently unsupported. **[SCG-52111]**

Rate Limiting Known Issues

The following are the known issues related to rate limiting.

- Rate limiting affects fragmented traffic by 50% even when the configured threshold has not been reached. **[SCG-66092]**

Scalability, Stability, and Performance Known Issues

The following are the known issues related to scalability, stability, and performance.

- A SmartZone backup file exported from release 2.x cannot be imported to a controller running release 3.x. **[SCG-50908]**

Session Manager Known Issues

The following are the known issues related to the session manager.

- The session manager process does not handle the session timeout of WISPr clients after a UE roams from one AP to another. **[SCG-52369]**
- WISPr client session statistics are moved to historical data after client terminates layer 2 connection with AP, and not after logout. **[SCG-61369]**

SNMP Known Issues

The following are the known issues related to SNMP.

- The event type and SNMP trap for Event 518 do not match. **[SCG-49689]**
- AP SNMPv3 displays INFORM when the notification type is set to TRAP. **[SCG-56994]**

Syslog Known Issues

The following are the known issues related to syslog.

- When the primary syslog server is down, syslogs are sent to the secondary server. However, syslogs still show the IP address of the primary syslog server (instead of the secondary server). **[SCG-57263]**
- vSZ does not generate syslog messages about the number of free licenses that available. **[ER-4896]**
- Event 113 (AP configuration get failed) may fail to be generated.**[SCG-89372]**

System Known Issues

The following are the known issues related to the system.

- The controller's management interface IP address may not be changed from DHCP to static IP address mode. **[SCG-35281]**
- When the controller is added to the SCI, the **Monitor** > **Administrator Activities** page may show that an administrator (SCI) is logging on to the controller every five minutes. **[SCG-35320]**
- When setting up the SZ-100, the DNS IP address has to be configured manually because DNS IP address assignment via DHCP cannot be completed. **[SCG-38184]**
- To protect the virtual controller against denial-of-service (DoS) and other forms of network attacks, it strongly recommends installing it behind a firewall. **[SCG-38338]**

- The Ethernet port-based profile selection feature was added along with AD/LDAP enhancements. However, the related settings are unavailable on the web interface. **[SCG-39032]**
- If LDAP authentication is used to authenticate hotspot (WISPr) users, the full path to the LDAP server must be configured. Otherwise, users will be unable to log on to the hotspot using LDAP. **[SCG-40729]**
- When you restore the system using a cluster backup, configuration backup files may get deleted. Ruckus strongly recommends that you configure an FTP server to which you can automatically export configuration backups that you generate manually or using the backup scheduler.**[SCG-41960]**
- When the controller is installed on Microsoft Azure hypervisor and dynamic mode is enabled on the hypervisor, the controller's private and public IP addresses may change if the hypervisor is shut down. This will disconnect APs from the controller, as well as disconnect nodes that form the cluster. **[SCG-42367]**

  Workaround:

  - Do not shut down the Azure hypervisor, or;

  - Set a static IP address for the controller on the Azure hypervisor.
- When vSZ is upgraded from release 3.2 to a newer release, the web interface cannot be accessed using the Microsoft Internet Explorer 11. [SCG-48747]
- Cluster formation fails if nodes that are up and running are not syncing time with the configured upstream NTP server. **[SCG-49736]**
- When the Device Policy feature is enabled, the host name Chrome devices and Play Station appears as "N/A" on the web interface. This occurs because "DHCP option 12" does not exist in DHCP Discover and DHCP Request. **[SCG-50595]**
- In a cluster, if the controller to which an AP is connected gets rebooted, the AP moves to another controller in the same cluster. When the controller node that was rebooted comes up, the WISPR sessions on the AP will get terminated. This is a corner case and is not always observed. **[SCG-50826]**

  Workaround: Do nothing. Subsequent calls will work fine.
- SmartZone to SCI communications can be enabled through the web interface using the new SCI Management setting in the SZ web interface. However, this feature only works for SCI version 2.0 (and later). If you are using an older version of SCI (1.x), you will still need to execute the "ap-sci enable" command to allow SZ-SCI communications, even after upgrading the SZ to 3.4. **[SCG-51832]**
- Nessus reported "Database Reachable from the Internet" vulnerability on port 11311. Memproxy will access the memcache on the cluster interface via port 11311. For data synchronization across the cluster, it needs to be enabled on the cluster interface. **[SCG-53518]**
- Some 802.11w-capable (Protected Management Frames) devices (for example, Samsung and Nexus) may experience interoperability issues when the option 802.11w required is enabled. **[SCG-56879]**
- The APs on Google Maps sometimes appear off the map. This is a known issue with Google Maps for markers in high latitudes. **[SCG-61522]**
- After upgrading the controller from 3.2.x to 3.5 successfully, the web interface does not redirect to the logon page automatically. After the upgrade, it still shows the upgrade process page because of encryption enhancements in release 3.5. **[SCG-61661]**
- The data plane's DHCP ladder diagram is out of sequence. Visual Connection Diagnostics will perform a best-effort correction of the sequence, but it's not guaranteed. **[SCG-64571]**
- The WLAN group override of a VLAN can only be applied if the WLAN and WLAN group are of the same type (for example, both are configured with VLAN tags or both are configured for VLAN pooling). **[SCG-66832]**
- Tunnel WLAN does not support SSID with 32 characters when DHCP Option 82 is enabled under DHCP Relay scenario. **[SCG-69308]**

- The search text allows users to search text from the beginning of the string. For example, if the string is RuckusWirelesss, you should search for Ruckus instead of Wireless. **[SCG-76950]**
- Special characters are used as tokenizers for indexed texts in the system, and, when performing a search, special characters are used to separate search terms into smaller segments before performing a search. Therefore search terms with special characters are not supported and is ignored. **[SCG-76953]**
- The data plane's DHCP ladder diagram is out of sequence. Visual Connection Diagnostics will perform a best-effort correction of the sequence, but it's not guaranteed. **[SCG-78044 SCG-64571]**
- The sequence *RADIUS Access Accept*(AP to client) should be in front of ***Authentication Success*** of proxy web authentication tunnel WLAN. **[SCG-78053]**

  NOTE
  As there are many modules involved in reporting the messages, CCD (Client Connection Diagnostics) module collects all messages (from various modules) and tries to correct sequences if the messages are arrived out of sequence. However, it has been observed that under some special cases, messages may arrive at CCD way out of sequence and CCD cannot correct them. So, the sequence correction is a best effort approach and it's not guaranteed.

- To help ensure that the cluster firmware upgrade process can be completed successfully, the cluster interfaces of all nodes must be connected and up. **[SCG-34801]**
- When the system boots it does not display the IPv6 address since DHCP IPv6 address in the management IP address is not auto updated. **[SCG-77032]**

  Workaround: Restart the system for it to display the DHCP IPv6 address in the management IP address.
- The controller may be unable to renew its DHCP server-assigned IP address, which may cause all controller services to go down. **[SCG-40383]**
- IPv6 addresses for accounting servers on the SZ100 and vSZ are unsupported. Only accounting servers on the SZ300/ vSZ-H can be assigned IPv6 addresses. **[SCG-46917]**
- Syslog servers that are using IPV6 addresses are currently unsupported. **[SCG-53679]**
- Downloading the controller snapshot log and AP support log may fail if multiple attempts are performed in quick succession. **[SCG-61855]**
- Historical client statistics for TTG sessions are not populated in the report. [SCG-71877]

UI/UX Known Issues

The following are the known issues related to the UI/UX.

- The current client count may not be consistent with the client count that appears in the Traffic Analysis section. **[SCG-60424]**
- The local DB option for the authentication and accounting server is used in earlier releases for the ZeroIT feature. Although Zero IT has been removed in release 3.4, the local DB option is still visible on the web interface. **[SCG-47704]**
- On the Bonjour Gateway page, the Create button remains enabled after you select an existing policy. **[SCG-54420]**
- On iOS 8.x devices, EAP-FAST does not work without a RADIUS server certificate configured in Wi-Fi profile for the device. **[SCG-47946]**
- The AP management VLAN of legacy APs (for example, APs running release 3.1.1 or 3.1.2) cannot be configured from the controller's web interface. As a result, the AP Management VLAN field on the AP Monitor page cannot display the correct information. **[SCG-48255]**

Workaround: If you have APs in legacy AP zones, you can view the correct AP management VLAN from the AP CLI. Alternatively, upgrade the legacy AP zones to this release to resolve this issue.

- After client fingerprinting is enabled, the OS Type field on the Wireless Clients page no longer shows the IPv6 client's operating system. [SCG-48886]
- When the AP bundle is applied, there is no warning message to warn users that applying the bundle will upgrade and reboot all APs, resulting in a temporary service outage. **[SCG-55178]**
- Some cable modem termination systems (CMTSs) may show the "Reset CM" button on the user interface. Clicking this button only resyncs the signal and does not actually reboot the CM. **[SCG-56905, SCG-57683]**
- On the controller's web interface page for individual access points, the Restart Cable Modem button on the Restart tab is not functional. **[SCG-58881]**
- To support WISPr for MSP partners, the "username" attribute was added in the northbound interface query in this release. Customers who upgraded the controller from a previous release do not need to enable the northbound interface unless they intend to use the MSP feature. All requests from an external subscriber portal without a user name specified will still be accepted and considered as an MSP user. **[SCG-59160]**
- After an AP is moved from one zone to another, its historical data from its previous zone no longer appears on the web interface. **[SCG-61677]**
- After a backup configuration (from release 3.2 or 3.4) is restored, the web interface does not redirect automatically to the logon page. This issue occurs because of changes in the security certificates. **[SCG-61779]**
- During a TTG call flow, the DHCP server stats under Diagnostics are not updated. **[SCG-62316]**
- The AP traffic graph does not fit into the legacy AP report. **[SCG-62327]**
- When wireless clients are associated with the AP, the average client count may be displayed as in a non-integer value (for example, a decimal number). **[SCG-62513]**
- Predictive search on the user traffic and VLAN polling pages only shows results if the first three characters in the search string find a match. **[SCG-62718]**
- The server name is overridden by a ladder diagram in Internet Explorer 11. **[SCG-63365]**
- Mesh is not applicable to the DHCP NAT on Each AP case because, in this scenario, there is only one AP and no root AP. If a mesh AP is set up, clients connecting to it will be unable to obtain an IP address from a root AP. **[SCG-65453]**
- Modifying the settings of multiple APs in the same AP zone is not supported. **[SCG-66143]**
- If a global filter is applied to a zone, the Access Points page does not correctly display the APs that match the filter. **[SCG-65236]**
- Even after a WISPr client has signed out, the controller web interface continues to show the client in an authorized state. Manually de-authorizing the client does not change the status. **[SCG-80455]**
- Option of cloning of WLAN from one zone to other zone is removed in this release. **[SCG-73361]**
- The upload status of **Administration/Upgrade** menu on web administrative interface includes a flow of actions such as *upload file* and *validation file*. At times, the system is unable to process beyond this point before proceeding to the next step though the browser status bar displays the progress as uploading file to the controller. **[SCG-78425]**
- The channel background application sends the channel number without checking whether the current channel mode supports the channel number. **[SCG-60820]**
-
- Substring search does not work when using search boxes. **[SCG-82184]**

Virtual SmartZone Known Issues

The following are the known issues related to the Virtual SmartZone.

- After nodes in a vSZ cluster running on Microsoft Azure are set to factory settings, the nodes are assigned the same host name, instead of their instance names. When nodes in a cluster have duplicate host names, the vSZ cluster cannot be established. **[SCG-39957]**
- When the controller is behind a NAT server, APs are assigned both public and private IP addresses. **[SCG-46949]**
- Static routes in vSZ cannot be added in bulk. To add multiple static routes, you need to add each static route individually. **[SCG-49186]**
- WISPr client session statistics are not properly moved to historical data after logout. **[SCG-52507]**
- If multiple zones or AP groups exist in a domain or zone, it might take at least 30 seconds to expand the AP Status tree on the Health Dashboard screen. **[SCG-64543]**
- Client isolation is only supported on clients that are using IPv4 (not IPv6) addresses. **[SCG-64581]**
- A static route will not work if the network configuration is set to "Keep-Original." **[SCG-65463]**
- The Apple Captive Network Assistant (CNA) is not a fully functional browser. Therefore, it may not work with the controller's portals. **[SCG-67041]**
- Flexi-VPN option is not compatible with Dynamic VLAN setting in WLAN configuration. If one WLAN Authentication type is selected that has Dynamic VLAN enabled by default, uncheck that option if you want to use Flexi-VPN feature. **[SCG-73427]**

Virtual SmartZone Data Plane Known Issues

The following are the known issues related to Virtual SmartZone Data Plane.

-
- vDP external syslog messages of ***DHCP/NAT_Released*** are not supported in this release. **[SCG-72649]**
- vDP CLI can only support one user to login to view DHCP and NAT information. [SCG-72610]
- When NAT service is enabled in vDP core side L2-GRE does not work though it is configurable. **[SCG-71118]**
- Only static and statefull DHCPv6, IPv6 addressing is supported. **[SCG-59194]**
- When the internal DHCP server in vSZ-D is enabled, vSZ-D ignores DHCP requests from non-matched VLANs and does not forward these requests to Local Breakout. **[SCG-59772]**
- Modifying the data plane network configuration from the vSZ High Scale web interface can enable the IPv6 function to support IPv6 connections on vSZ-D release 3.5. **[SCG-62285]**
- There are no statistics for vSZ-D DHCP/NAT feature in vSZ. **[SCG-63511]**
- Overlapping L3 roaming subnet/VLAN settings on multiple vSZ-D is allowed but can impact UE connectivity. So this configuration should be avoided. [SCG-64238 SCG-82984]
- The alarm messages that appear on the dashboard do not disappear until an administrator clears them. Also, it is normal for the physical interface to be down as the controller is rebooting. **[SCG-64605]**
- If the primary and backup destination vSZ-Ds belong to the same vSwitch/ESXi server, Flexi-VPN UEs receive replies twice after the primary vSZ-D comes back online. **[SCG-66426]**
- When both Flexi-VPN and NAT DP are enabled and the DHCP server is not running on the vSZ-D server, Ruckus recommends enabling DHCP relay and using that as the forwarding profile. **[SCG-66850]**
- UE IPv4 traffic fails when the destination vSZ-D for Flexi-VPN is unavailable. **[SCG-67016]**

- The two-NIC architecture for the data traffic of vSZ-D does not work if one NIC is configured for vSwitch and the other NIC is configured for DirectIO. **[SCG-68163]**
- Users may experience unexpected drop in packets when the vSZ-D data interface is configured with Direct I/O and features based on inter-vSZ-D tunnels (such as Flexi-vpn/L3 Roaming/CALEA) are used. **[SCG-68535]**

  Workaround: Do not deploy both vSZ-D peers with Direct I/O on same Intel NIC (having multiple ports) or Intel NIC with consecutive MAC addresses.
- The SZ300's web interface shows inaccurate vSZ-D network usage. **[SCG-68696]**
- When using tunneled WLAN with vSZ-D DHCP/NAT feature with Radius-based profile, clients connected to the same WLAN will be able to see each other Multicast/Broadcast traffic even if they are in different subnets. **[SCG-72793]**
- If generated syslog events in vSZ-D are greater than 8,000 per second, there will be events dropped and not reaching external syslog server. **[SCG-72991]**
- Application of DiffServ values is not preserved on downlink IPv6 Tunnel header when the inner packet is also IPv6 is not supported. **[SCG-67593]**
- If a client connects to a WLAN that uses Radius profile based DHCP/NAT service, Web UI UE entry will report VLAN where NAT IP address belongs instead of the private one assigned by Radius server. **[SCG-72776]**
- IPv6 multicast traffic fails for RGRE wireless station. **[SCG-84658]**
- When multiple features are deployed to vSZ-D, upgrade process executed from vSZ web user interface may fail. **[SCG-89214]**

  Workaround: Upgrade it from vSZ-D CLI.

Visual Connection Diagnostics Known Issues

The following are the known issues related to Visual Connection Diagnostics.

- The data plane does not support WISPr to SP messages. **[SCG-62440]**
- Visual Connection Diagnostics does not work if a user opens two simultaneous user interface (UI) sessions (for example, by opening two browser tabs that both show the controller's web interface). **[SCG-63576]**
- Retransmission of physical layer packets, such as EAPOL, is not displayed on the Visual Connection Diagnostics live troubleshooting page. **[SCG-63199]**
- The connection failure counter does not increment when EAP fails. **[SCG-63193]**
- Even if an AP does not support Visual Connection Diagnostics, messages at the RAC can still be used to help identify potential issues associated with RADIUS connections. **[SCG-61281]**
- When the data plane receives the first DHCP message, it suppresses other DHCP messages for 180 seconds to prevent message flooding. **[SCG-61160]**

Wired Clients Known Issues

The following are the known issues related to wired clients.

- Only one VLAN can be assigned to the Ethernet interface. If the first client is assigned to one VLAN, the second client has to use the same VLAN. **[SCG-66362]**

- In a wired guest VLAN implementation, the wired client is authorized with a different VLAN even if the client fails wired 802.1X authentication. It can use the Ethernet profile's guest VLAN number to check whether the client is a guest or a normal user. **[SCG-67708]**

WISPr Known Issues

The following are the known issues related to WISPr.

- When the primary AAA server is unreachable, authentication messages are not forwarded to the secondary AAA server. **[SCG-49493]**
- After UEs that are using Internet Explorer are authenticated, they are sometimes redirected to hotspot logon page. **[SCG-47863]**
- WISPr does not support IPv6 clients. **[SCG-61036]**
- When configuring walled garden entries, it is recommended to use IP addresses (not DNS names) to help ensure that the walled garden rules are applied consistent. **[SCG-61183]**
- If the external portal is using HTTPS and a private/self-signed certificate, the pop-up login window does not appear on iOS devices, even if bypass CNA is disabled. **[SCG-65321]**
- Bypass CNA is unsupported on MacBook Air when the web proxy is enabled. **[SCG-67370]**
- The controller does not have a backup captive portal status, so it cannot redirect to the backup login page for logging out. This is a limitation for SZ ZD hotspot API (logout). **[SCG-88998]**

ZoneDirector to SmartZone Migration Known Issues

If you have a ZoneDirector controller on the same network, take note of this important information.

To ensure reliable network operations, it is recommended that ZoneDirector controllers and SmartZone controllers (SZ, vSZ and SAMs controllers) not be deployed on the same IP subnet or in such a way as the controllers share the same DHCP address scopes and domain name servers (DNS) as there may be limitations or restrictions in AP controller discovery capabilities. An effective network segmentation strategy should be developed when ZoneDirector and SmartZone controllers coexist on the same network.

- When migrating APs from ZoneDirector to SmartZone, if you want all APs to be located in same zone, migrate all APs at the same time. **[SCG-64377]**
- The migration results might not be up-to-date if web session times out or the web browser is refreshed before the migration process is completed. **[SCG-64679]**

Resolved Issues

- AP Resolved Issues....43
- Application Recognition and Control (ARC) Resolved Issues....43
- Bonjour Fencing Resolved Issues....44
- Control Domain Resolved Issues....44
- Public API Resolved Issues....44
- System Resolved Issues....44
- Virtual Data Plane Resolved Issues....44
- Virtual SmartZone Resolved Issues....45

AP Resolved Issues

The following are the resolved issues related to AP.

- Resolved an issue where the AP page configuration incorrectly allowed administrators to change mesh mode when DHCP-NAT was enabled. **[SCG-79713]**
- Resolved an issue where session termination caused in Accounting Stop packet was incorrect when the client was disconnected using Block operation. **[SCG-76876]**
- Resolved an issue where if a 3.5.1 SZ configuration backup was applied to a controller running 3.6 DHCP service was down for that zone. **[SCG-74919]**
- Resolved an issue where 802.1x operation of the Ethernet 1 (PoE) interface could not operate in supplicant or authenticator mode. **[SCG-67078, SCG-67079]**
- Resolved an issue where if an AP or one of the radio's on AP had no activity then the capacity was reported as '0'. **[SCG-74742]**
- Resolved an issue where when viewing the list of active clients on the controller, it incorrectly listed clients that have been disconnected. **[ER-5656]**
- Resolved an issue where API call for Access Point events returned the description as null. **[ER-6216]**
- Resolved an issue where WLAN did not get enabled when the AP's registration state changed from reject to approve. **[ER-6224]**
- Resolved an issue where if there is only one zone in the global filter and the global filter is currently used, deleting this global filter caused errors. **[ER-6281]**
- Resolved an issue where mesh view was not displaying all mesh APs in a zone. **[ER-6218]**

Application Recognition and Control (ARC) Resolved Issues

The following are the resolved issues related to ARC.

- Resolved an issue where on the Applications page, when a user selected a specific app, all clients that used this app in different domains were displayed on the page. **[SCG-64735]**

Bonjour Fencing Resolved Issues

- Bonjour Fencing supports for Google Chromecast Services. **[SCG-65552].**

Control Domain Resolved Issues

The following are the resolved issues for Control Domain.

- Resolved an issue where the AP could not move to the same Zone AP Group when DHCP/NAT was enabled. **[SCG-81356]**
- Resolved an issue where the SoftGRE tunnel statistics showed data of the last two-three days though the selected time period was 30 days. **[ER-6147]**
- Resolved an issue where AP administrator was not able to edit the guest pass portal. **[ER-6185]** Resolved an issue where the network tunnel statistics did not display for dual stack APs when queried with an IPv6 address. [SCG-57446]

Public API Resolved Issues

The following are the resolved issues related to the Public API.

- Resolved an issue where by changing the BSS minimum rate on WLAN through Public API defaulted the client isolation whitelist settings on the WLAN. **[ER-6228]**

System Resolved Issues

The following are the resolved issues related to System.

- Resolved an issue where the schedule backup did not work on restoring configuration. **[SCG-82275]**
- Resolved an issue where the controller now checks the validity of the added IPv6 static routes. **[SCG-81432]**
- Resolved an issue where incorrect key attributes was sent to the LDAP server for authentication. **[ER-6007]**
- Resolved an issue in the creation of User Traffic Profile rule that contains ICMPv6 protocol. **[ER-6115]**
- Resolved an issue where**Troubleshooting** > **Spectrum Analysis** output was not displaying data when you leave it enabled, navigate to some other page and then return to this menu. **[ER-6258]**
- Resolved an issue where if the SSID contains the keyword AP, reports related to this SSID will fail to be generated. **[ER-6338]**
- Resolved an issue where the SZ-100 setup wizard now validates the IPv6 address if the IPv6 prefix is not configured. **[SCG-40257]**

Virtual Data Plane Resolved Issues

The following are the resolved issues for Virtual Data Plane.

- Resolved an issue where when VLAN tag is enabled with access/core separation, static route cannot be persisted after rebooting. This is a configuration limitation for vSZ-D and SZ300 internal data plane. **[SCG-82367 ER-6160]**
- Internal data plane will shut down gracefully when shutdown or reboot is initiated from SZ300 control plane. **[ER-6240]**
- Resolved the memory leak caused by L2UF *disconnect* packets. **[ER-6447, ER-6442, ER-6317]**

Virtual SmartZone Resolved Issues

The following are the resolved issues related to Virtual SmartZone.

- For WISPr WLAN the NAS IP should be the same for access-request and accounting packets. **[SCG-73900]**
- A zone affinity profile can be deleted if it is in use by a SoftGRE zone. **[SCG-68651]**
- When the internal DHCP server in vSZ-D is enabled, the traffic is forwarded when no matching profile is found. **[SCG-64664]**
- Resolved an issue where the serial number of vSZ changed after reboot, especially seen in AWS based vSZ. **[ER-6235]**
- Resolved an issue setting NTP configuration in vSZ controllers. **[ER-6293]**

Upgrading to This Release

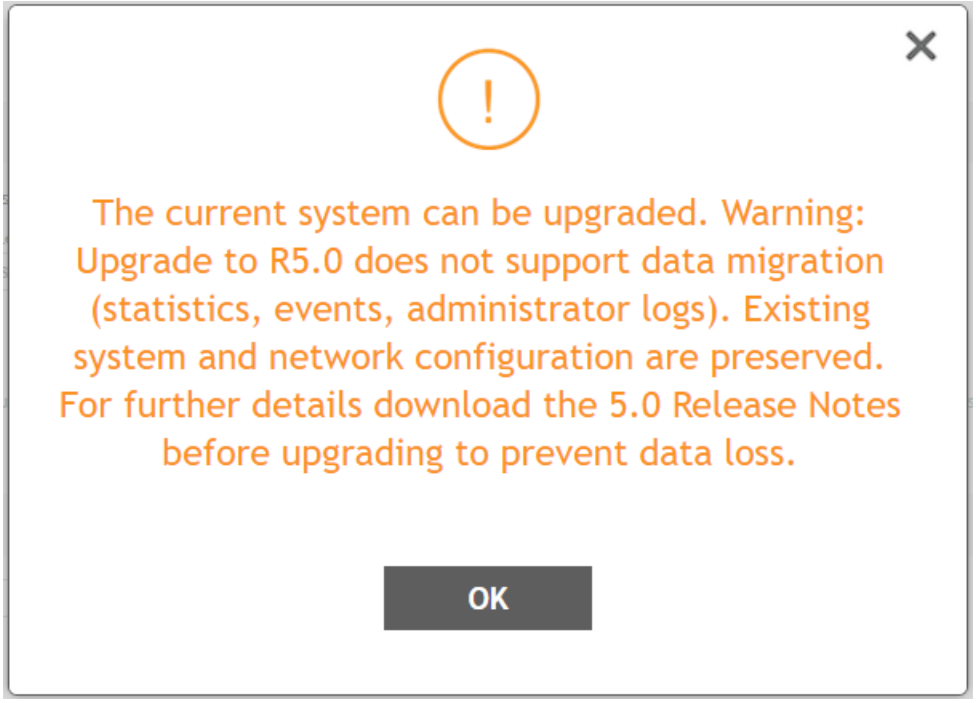
- Before Upgrading to This Release 47
- Virtual SmartZone Recommended Resources..... 48
- AP and Switch Resource Table..... 49
- SmartZone Upgrade Paths..... 50
- Multiple AP Firmware Support..... 51
- EoL APs and APs Running Unsupported Firmware Behavior..... 52

Before Upgrading to This Release

Due to underlying changes of the database in this release, data will be dropped during the upgrade. It is recommended that you read the following content carefully before upgrading to this release.

CAUTION
Data migration is not supported by the SmartZone (SZ) release 5.0 upgrade. Existing system and network configuration is preserved, but data such as status and statistics, alarms or events, administrator logs and mesh uplink history is not migrated to the new release. Contact Ruckus support for concerns or additional clarifications. [SCG-73771]

- The upgrade path is changed and is now limited to N-1 support. Only 3.6.0 or 3.6.1 releases can be upgraded to 5.0.
- When upgrading to the release 5.0 image from release 3.6 or 3.6.1, the system displays the following warning message about not supporting data migration (statistics, events, administrator logs) during the upgrade process.



Data Migration Recommendations

If you need to preserve your data or reports, consider the following recommended options before upgrading:

- Leverage an existing SCI platform to send statistics and reports to SCI before the upgrade.

  NOTE
  SCI comes with a free 90 day evaluation.

- Backup and export existing statistics and reports using Export tools or Streaming API before the upgrade.
- For Virtual SmartZone (vSZ) deployments—Add a separate SZ 5.0 node or cluster and attach newer APs and zones to the new cluster. Migrate all APs over a period of time, and then decommission the old cluster.
- Ruckus will be able to provide the Data Migration Tool to interested customers (only available to Essential controllers), and the Data Migration Tool Guide is downloadable from the support site.

  NOTE
  Use of the Data Migration Tool is not recommended for high-scale users running SZ300 or vSZ-H.

Upgrade Considerations

Before upgrading, consider these additional points.

- Before uploading a new AP patch, Ruckus strongly recommends that you save a cluster backup, in case you want to restore the previous AP patch.
- Before upgrading the controller, Ruckus strongly recommends that you back up the entire cluster. In case the upgrade fails, you can use the cluster backup to roll back the cluster to its previous state.
- When upgrading vSZ-E/vSZ-H, if the memory/CPU allocation of the current VM instance does not match the lowest resource level of the new VM instance to which the new vSZ-E/vSZ-H version will be installed, you will be unable to perform the upgrade. On the other hand, if the new VM instance has insufficient hard disk space, a warning message appears after you upload the upgrade image but you will still be able to perform the upgrade.

Virtual SmartZone Recommended Resources

Before upgrading vSZ to this release, verify that the virtual machine on which vSZ is installed has sufficient resources to handle the number of APs and wireless clients that you plan to manage. See the tables below for the virtual machine system resources that Ruckus recommends.

NOTE
These vSZ recommended resources may change from release to release. Before upgrading vSZ, always check the recommended resource tables for the release to which you are upgrading.

NOTE
It is recommended that there should be only one concurrent CLI connection per cluster when configuring vSZ.

TABLE 3 vSZ High Scale recommended resources

AP Count Range		Maximum Clients	Nodes per Cluster	AP Count per Node	vCPU	RAM	Disk Size	Preserved Events	Concurrent CLI Connection	Resource Level
From	**To**			**Max**	**Logic Processor [1][2][3]**	**GB[3]**	**GB**	**Max**	**Max (per node not per cluster)**	
10,001	30,000	300,000	4	10,000	24	48	600	3 M	4	8
	20,000	200,000	3							
5,001	10,000	100,000	1-2	10,000	24	48	600	3 M	4	7
2,501	5,000	50,000	1-2	5,000	12	28	300	2 M	2	6.5
1,001	2,500	50,000	1-2	2,500	6	22	300	1.5 M	2	6
501	1,000	20,000	1-2	1,000	4	18	100	600 K	2	5
101	500	10,000	1-2	500	4	16	100	300 K	2	4
1	100	2,000	1-2	100	2	13	100	60 K	2	3

TABLE 4 vSZ Essentials recommended resources

AP Count Range		Maximum Clients	Nodes per Cluster	AP Count per Node	vCPU	RAM	Disk Size	Preserved Events	Concurrent CLI Connection	Resource Level
From	**To**			**Max**	**Logic Processor [1][2]**	**GB**	**GB**	**Max**	**Max (per node not per cluster)**	
1025	3,000	60,000	4	1,024	8	18	250	10 K	2	3
	2,000	40,000	3							
501	1,024	25,000	1-2	1,024	8	18	250	10 K	2	2
101	500	10,000	1-2	500	4	16	100	5 K	2	1.5
1	100	2,000	1-2	100	2	13	100	1 K	2	1

NOTE

Logic Processor [1] vCPU requirement is based on Intel Xeon CPU E5- 2630v2 @2.60 GHz.
Logic Processor [2] Azure with low CPU throughput unsupported. The vSZ with the lowest resource plan (2 core CPU, 13 GB memory) can NOT be supported due to the low CPU throughput on Azure.

AP and Switch Resource Table

The below table lists the recommended resources between APs and switches.

These recommended resources may change from release to release. Before upgrading, always check the recommended resource tables for the release to which you are upgrading.

TABLE 5 AP and Switch resource table for 1 and 2 nodes

Profile	1 Node			2 Nodes		
Capacity	AP Mode	Mix Mode	Switch Mode	AP Mode	Mix Mode	Switch Mode

TABLE 5 AP and Switch resource table for 1 and 2 nodes (continued)

Profile	1 Node						2 Nodes					
SZ100	1024	0	512	25	0	51	1024	0	512	25	0	51
SZ300	10,000	0	5000	250	0	500	10,000	0	5000	250	0	500
vSZ-E L1	100	0	50	2	0	5	100	0	50	2	0	5
vSZ-E L1.5	500	0	250	12	0	25	500	0	250	12	0	25
vSZ-E L2	1,024	0	512	25	0	51	1,024	0	512	25	0	51
vSZ-H L3	100	0	50	2	0	5	100	0	50	2	0	5
vSZ-H L4	500	0	250	12	0	25	500	0	250	12	0	25
vSZ-H L5	1,000	0	500	25	0	50	1,000	0	500	25	0	50
vSZ-H L6	2,500	0	1250	62	0	125	2,500	0	1250	62	0	125
vSZ-H L6.5	5,000	0	2500	125	0	250	5,000	0	2500	125	0	250
vSZ-H L7	10,000	0	5000	250	0	500	10,000	0	5000	250	0	500

TABLE 6 AP and Switch resource table for 3 and 4 nodes

Profile	3 Nodes						4 Nodes					
Capacity	AP Mode		Mix Mode		Switch Mode		AP Mode		Mix Mode		Switch Mode	
SZ100	2,048	0	1,024	51	0	102	3,000	0	1,500	75	0	153
SZ300	20,000	0	10,000	500	0	1,000	30,000	0	15,000	750	0	1,500
vSZ-E L1	200	0	100	5	0	10	300	0	150	6	0	15
vSZ-E L1.5	1,000	0	500	25	0	50	1,500	0	750	36	0	75
vSZ-E L2	2,048	0	1,024	51	0	102	3,000	0	1,500	75	0	153
vSZ-H L3	200	0	100	5	0	10	300	0	150	6	0	15
vSZ-H L4	1,000	0	500	25	0	50	1,500	0	750	36	0	75
vSZ-H L5	2,000	0	1,000	50	0	100	3,000	0	1,500	75	0	150
vSZ-H L6	5,000	0	2,500	125	0	250	7,500	0	3,750	186	0	375
vSZ-H L6.5	10,000	0	5,000	250	0	500	15,000	0	7,500	375	0	750
vSZ-H L8	20,000	0	10,000	500	0	1,000	30,000	0	15,000	750	0	1,500

SmartZone Upgrade Paths

Before you upgrade the controller, verify that it is running a release build that can be upgraded to this release.

To help ensure that the cluster firmware upgrade process can be completed successfully, the cluster interfaces of all nodes must be connected and up. **[SCG-34801]**

TABLE 7 Previous release builds

Platform	Release Build
SZ300	3.6.0.0.510
SZ100	3.6.1.0.227
vSZ	

TABLE 7 Previous release builds (continued)

Platform	Release Build
vSZ-D	

If you are running an earlier version, you must first upgrade to appropriate version for your model, as shown in the above list, before upgrading to this release.

Multiple AP Firmware Support

The AP firmware releases that APs use are configured at the zone level. This means that APs that belong to one zone could use a different AP firmware release from APs that belong to another zone.

NOTE
SZ100/vSZ-E/SZ300/vSZ-H devices are referred to as controllers in this section.

NOTE
If you have AP zones that are using 3.4.x or 3.5.x and the AP models that belong to these zones support AP firmware 3.6 (and later), change the AP firmware of these zones to 3.6 (or later) to force these APs to upgrade their firmware. After you verify that all of the APs have been upgraded to AP firmware 3.6 (or later), proceed with upgrading the controller software to release 5.0.

NOTE
In earlier releases, Essentials controllers (vSZ-E or SZ100) automatically upgraded both the controller firmware and AP firmware when the system is upgraded. In release 3.5, however, the concept of *Multi-Zone* was introduced, which slightly changed the upgrade workflow where the system and the AP zones upgraded independently. When upgrading the controller to 5.0, the AP Zone firmware remains the same.

Up to Two Previous Major AP Releases Supported

This controller release can support up to two major AP firmware releases, including (1) the latest AP firmware release and (1) the most recent major AP firmware release. This is known as the N-1 (n minus one) firmware policy.

NOTE
A major release version refers to the first two digits of the release number. For example, 3.6 and 3.6.1 are considered part of the same major release version, which is 3.6.

The following releases can be upgraded to release 5.0:

- 3.6
- 3.6.x

The AP firmware releases that the controller will retain depend on the controller release version from which you are upgrading:

- If you are upgrading the controller from release 3.6.1, then the AP firmware releases that it will retain after the upgrade will be 5.0 and 3.6.1 (and 3.6 if this controller was previously in release 3.6).
- If you are upgrading the controller from release 3.6, then the AP firmware releases that it will retain after the upgrade will be 5.0 and 3.6.

All other AP firmware releases that were previously available on the controller will be deleted automatically.

EoL APs and APs Running Unsupported Firmware Behavior

Understanding how the SZ300/vSZ-H controllers handle APs that have reached End-of-Life (EoL) status and AP running unsupported firmware can help you design an upgrade plan that will minimize impact on wireless users in your organization.

NOTE
SZ300/vSZ-H devices are referred to as controllers in this section.

EoL APs

NOTE
To check if an AP that you are managing has reached EoL status, visit the ZoneFlex Indoor AP and ZoneFlex Outdoor AP product pages on the Ruckus Support website. The icons for EoL APs appear with the *END OF LIFE* watermark.

- An EoL AP that has not registered with the controller will be moved to the Staging Zone and its state set to Pending. This AP will be unable to provide WLAN service to wireless clients.
- The EOL AP affects the upgrade only in the following conditions. Otherwise, the upgrade is successful.
  1. Upgrade must be prior to the SZ 3.5 release.
  2. This is applicable only in SZ100 or vSZ-E controllers.

APs Running Unsupported Firmware Releases

- APs running AP firmware releases that are unsupported by the controller release can still connect to the controller.
- Once connected to the controller and assigned to a zone, the AP will be upgraded to the AP firmware assigned to the zone to which it belongs.

Interoperability Information

- AP Interoperability....53
- Redeploying ZoneFlex APs with SmartZone Controllers....54
- Converting Standalone APs to SmartZone....54
- ZoneDirector Controller and SmartZone Controller Compatibility....55
- Client Interoperability....55

AP Interoperability

APs with ordering number prefix 901- (example 901-T300-WW81) may now be supplied with an AP base image release 100.0 or later (including 104.0).

The AP base image is optimized for controller-discovery compatibility to support all Ruckus controller products including ZoneDirector, vSZ, SZ100, and SAMs.

Once the AP discovers and joins a controller (for example, the SZ100), the AP is updated to the compatible controller-specific AP firmware version. The updated AP firmware version becomes the factory-default image. The updated AP firmware version (for example, vSZ AP100.x) will remain persistent on the AP after reset to factory defaults.

An AP configured with base image release 100.0 may be managed by the FlexMaster management tool or may be used in standalone controller-less operation if controller discovery is disabled on the AP web interface.

Enabling ZoneFlex AP Discovery to a SmartZone Controller Using DHCP Option 43

To ensure reliable discovery of ZoneFlex APs to SmartZone controllers, the DHCP server must be configured to support DHCP Option 43 settings as outlined in the Getting Started Guide for your controller. DHCP option 43 sub codes 03 and 06 IP address assignments must both point to the SmartZone controller's control plane IP address to ensure reliable discovery services.

Enabling ZoneFlex AP Discovery to a SmartZone Controller Using DNS

To ensure reliable discovery of ZoneFlex APs to SmartZone controllers using DNS resolution, the DNS server must be configured to have two DNS entries. The first DNS entry must use the "RuckusController" prefix and the second entry the "zonedirector" prefix.

Refer to the *Getting Started Guide* for your SmartZone controller for instructions on how to connect the AP to the controller using DNS.

Redeploying ZoneFlex APs with SmartZone Controllers

NOTE
A supported ZoneFlex AP configured to operate with ZoneDirector will require an upgrade to a compatible SmartZone controller approved software release prior to interoperating with an SCG, SZ, vSZ, or SAMs controller.

Once the AP firmware is updated, the AP will no longer be able to communicate with its old ZoneDirector controller. The AP must be reset to factory default setting before attempting to configure the AP from the SmartZone controller.

NOTE
There are established ZoneDirector to SmartZone controller migration tools and procedures. Contact support.ruckuswireless.com for the latest available procedures and utilities.

Converting Standalone APs to SmartZone

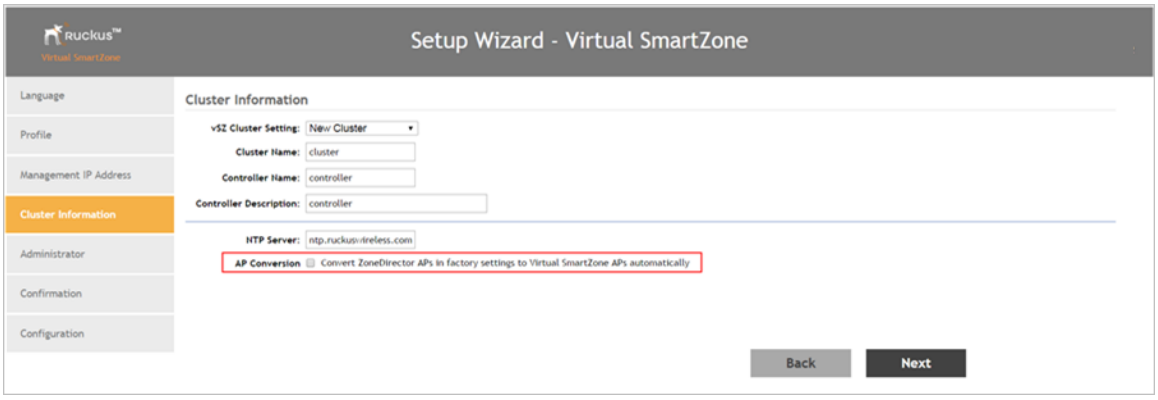
You can convert standalone ZoneFlex APs (those that are not managed by ZoneDirector) in factory default configuration to be managed by a SmartZone controller.

Follow these steps to convert standalone ZoneFlex APs to the SmartZone controller firmware so that they can be managed by the SZ300, SZ100, or vSZ

1. When you run the SmartZone Setup Wizard, select the **AP Conversion** check box on the **Cluster Information** page.

   NOTE
   The figure below shows the AP Conversion check box for the vSZ Setup Wizard. If you are setting up SZ300, or SZ100 the check box description may be slightly different.

   FIGURE 2 Select the AP Conversion check box to convert standalone ZoneFlex APs to controller APs



2. After you complete the Setup Wizard, connect the APs to the same subnet as the SmartZone controller.

   When the APs are connected to the same subnet, they will detect the SmartZone controller on the network, and then they will download and install the AP firmware from SmartZone controller. After the SmartZone firmware is installed on the APs, the APs will automatically become managed by the SmartZone controller on the network.

ZoneDirector Controller and SmartZone Controller Compatibility

If you have a ZoneDirector controller on the same network, take note of this important information.

To ensure reliable network operations, it is recommended that ZoneDirector controllers and SmartZone controllers (SCG, SZ, vSZ, SAMs controllers) not be deployed on the same IP subnet or in such a way as the controllers share the same DHCP address scopes and domain name servers (DNS) as there may be limitations or restrictions in AP controller discovery capabilities. An effective network segmentation strategy should be developed when ZoneDirector and SmartZone controllers coexist on the same network.

Client Interoperability

SmartZone controllers and ZoneFlex APs use standard protocols to interoperate with third party Wi-Fi devices. Ruckus qualifies its functionality on the most common clients.

Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com