RELEASE NOTES

Ruckus SmartZone Release Notes for AP T310 series

Supporting AP T310 series

Part Number: 800-71830-001 Rev A
Publication Date: January 2018

Copyright Notice and Proprietary Information

Destination Control Statement

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, RUCKUS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. Ruckus does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. Ruckus does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to Ruckus that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL RUCKUS, ARRIS, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIES, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF RUCKUS HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS.

If you are dissatisfied with the Materials or with the associated terms of use, your sole and exclusive remedy is to discontinue their use.

Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

Contents

New and Changed Features in Release 3.6

New Features in Release 3.6

This section provides a high-level overview of several key features that are introduced in the SmartZone (SZ) software release 3.6. For detailed descriptions of these features and configuration help, refer to the respective 3.6 documentation guides.

The SZ release 3.6 is applicable to the Ruckus SmartZone 300, SmartCell Gateway 200, SmartZone 100, vSZ-H, and vSZ-E controller platforms. For additional details, do refer to the SmartZone Controller Documentation Suite for Release 3.6.

Geo-Redundancy for Controller Clusters High Availability

The SZ Cluster Geo-redundancy is a highly desirable feature by Service Providers and large enterprises that own multiple controller clusters. It provides disaster recovery solution for these customers. In this initial implementation phase, the feature allows installation of active and dedicated backup clusters across different datacenters with regular transport network connection. The backup clusters and active clusters will not be in active-active mode. It will rather function in active-backup mode at all time. The feature is available on SZ300 and vSZ-H platforms only.

This release features One active cluster to One dedicated backup cluster mapping. In the backup cluster, you may choose to have the same nodes as in the active cluster, in which you will be able to backup all the zones from active to backup cluster and in the event of failure, all APs will be failed over to the backup cluster or you may choose to have less number of backup controller nodes in the backup cluster than the active cluster, in which you will only be able to backup selected zones from the active cluster and have APs in those zones failed over to backup in case of failure. Auto re-homing is not supported.

Controller SKUs are exactly the same on both active and standby clusters . There is no special controller SKU to form a standby cluster. The difference is on AP capacity license and supports:

1. Active cluster, which has regular AP capacity licenses and regular support.
2. Standby cluster, which has new AP capacity licenses and new HA support.

FIGURE 1 Cluster High Availability

Geo Redundancy Configuration Pointers

As users of this new feature, following are the pointers during configuration.

1. Login credentials of the super administrator and system administrator should be the same in active and standby clusters. If active cluster admin password is modified, do modify the standby cluster admin password accordingly.
2. You need to set factory manually on standby cluster after disabling cluster HA.
3. Only standby cluster has limited configuration permission. Most features are read only since it is mainly for backup purpose.
4. Configuration synchronization for management ACL may break the cluster connection (br2 on standby cluster). Also management ACL is not configurable on standby cluster.
5. ZoneTemplate - On using the zone template, the cluster redundancy state is set to:
   a. Enable: When AP firmware version is >= 3.6 and system wide cluster redundancy is enabled.
   b. Disable: When AP firmware version is < 3.6 and system wide cluster redundancy is disabled.
6. GeoRedundancy standby cluster only works for one active cluster.
7. When active cluster is set to factory default, you can only make it as active cluster again by:
   a. Restoring the entire cluster or
   b. Enabling the cluster redundancy again
8. When standby cluster is set to factory default, you can only make it as standby cluster again by:
   a. Restore entire cluster or
   b. Click on **Sync Now** on the active cluster
9. Once the new AP is managed by the active cluster, you need to use **Sync Now** configuration for the standby cluster to guarantee that AP can failover. Reason, standby cluster rejects APs which are not in the active cluster configuration.
10. Rehome per domain and per zone are not supported.
11. Flagged APs will turn to online state after failover to standby cluster and reverts to flagged state after 3 minutes recalculation.
12. On control IP address list changing (modify or node join or remove), click **Sync Now** to update the IP address list on the controller.
13. Update of cluster GeoRedundancy configuration by public API is only supported on active cluster. **Pause** and **Rehome** are not supported on standby cluster.
14. Active and standby cluster require running the exact same models, IP mode, interface numbers, KSP with AP patches / firmware used by cluster redundancy enabled zones.
15. Cluster GeoRedundancy is only supported on physical controllers of SZ300 and vSZ-H without authorized external data plane.
16. User must have specific permissions for the below operation:
    a. **ReHome AP**: SZ Management + Full access
    b. **Synchronize configuration to standby cluster**: SZ Management + Full access
    c. **Pause daily configuration synchronize**: SZ Management + Modify
    d. **Modify Cluster GeoRedundancy configuration**: SZ Management + Modify

    [SCG-70095, SCG-69858, SCG-70044, SCG-69152, SCG-70606 and SCG-70607]

2-Step 802.1X + Wispr Authentication

This feature is designed to address several use cases that require multiple stages of authentication. By requiring both 802.1X and WISPr, customer can accomplish work flows where devices and users must both be authenticated. For example in education, libraries, or other deployments where devices may be shared by users, the 802.1X exchange is often used for device authentication at Layer2. However, the user must still authenticate, which can be accomplished by a WISPr workflow using a web portal. The 802.1X + WISPr functionality requires both authentication mechanisms to pass in order to authorize the user on the WLAN.

URL Filtering

The URL filtering feature 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. Deep Packet Inspection (DPI) Engine extracts hostnames and URLs from users browsing data. URLs and hostname category is then determined from a local database of recently browsed websites. If requested URL is not found in the local database, Ruckus securely requests website classification and reputation from Webroot threat intelligence service. End user identity is not sent to the threat intelligence service. This allows security administrators to customize and deploy policies for safely browsing the web.

URL filtering is now a common requirement from many customers in different market segments such as hospitality, education, retail stores, public facing venues and others where access to objectionable material or websites might be unwelcome. When it comes to children there are laws enacted by U.S. Congress such as Children's Internet Protect Act (CIPA) to keep students safe.

With the URL filtering feature, the administrator can now create an SSID and allow or deny access to a category of websites for all users that join this SSID. Since there are countless websites, for ease of configuration, the URL filtering feature provides five (5) pre-defined filter policies as well as a custom options to build a filtering policy from over 80 different categories. The policy choices are as follows:

1. None (No filtering)
2. No adult content (no adult content or nudity)
3. Clean and safe (No adult content plus, no malware, spyware, phishing, botnet or spamware)
4. Child and student friendly (clean and safe plus no alcohol, intimate apparel, dating, or weapons)
5. Strict (Child and student friendly plus no streaming media, personal storage and, games)
6. Custom category group: (Defined by the network admin is a grouping of multiple URL categories)

In addition to the category based approach to protection, the feature also supports admin-defined whitelists (list of allowed URLs) as well as blacklists (list of denied URLs). Also, the feature adds support for Google, YouTube, and Bing Safe Search functionality enforcement.

In case of HTTPS access filtering, the feature supports domain name lookup only. URL filtering licenses are required to turn this feature on.

NOTE
In the 3.6 release, license enforcement will not be strict; however, in follow-on releases, it will be strictly enforced.

Historical Visual Connection Diagnostics

In the 3.6 release, we are introducing a beta phase of historical visual connection diagnostics (VCD). In the 3.5 release, we introduced visual connection diagnostics for client connectivity troubleshooting, which is a real-time tool to evaluate the client connection process and troubleshoot where problems exist. We are continuing to build on this functionality by supporting historical client connection failure troubleshooting, so that administrators can search for a client and see historical problems experienced by this client.

With historical VCD, the admin can now perform troubleshooting on connection failures that happened to clients in the past 24 hours. This functionality is only supported on the SZ100 and vSZ-Essentials product variants in 3.6. In future releases, we plan to continue enhancing this by increasing the length of time as well as extending to the High-Scale SZ products. For this beta phase, the administrator must enable

historical VCD globally within the CLI, and then must enable the functionality on a per-zone basis in the SZ GUI. This is to ensure that the admin is aware of the risks of enabling a beta feature. As we collect more information during this beta phase, we will plan the next steps of feature evolution for 3.6.1 and subsequent SZ releases.

Group Health Charts

In the SmartZone dashboard and AP pages, we have historically focused on individual AP health data. In the 3.6 release, we are introducing a new way to view performance data by showing historical performance trends across groups of APs. In other words, we have a new type of chart to show what is normal for the network.

These new group health charts are accessible on the dashboard under the map section, or on the AP page by selecting a System, Zone, or AP Group in the group tree hierarchy. This new chart type is based on a display concept called a box plot, which allows us to see a distribution of health and performance across many APs.

For each time interval, the administrator can now view what is normal for the network, by looking at three sets of data on the chart:

1. Median - for a group of APs, this line on the chart displays the middle value from the set of samples at that time period.
2. Min-Max Range - for a group of APs, this area of the chart displays the full range of values for all APs at that time. This allows the administrator to answer what is the scope from worst to best on a given metric.
3. Likely Range - for a group of APs, this area of the chart shows the value for the middle 50% of APs. In other words, how is the middle half performing.

This view allows an administrator to visualize performance for a large set of APs at the same time, instead of reviewing AP performance one-by-one, or instead of only focusing on worst performers. This allows an administrator to answer questions about norms and trends across a deployment.

Export UE Session Syslog from AP to Syslog Server

To comply with legal requirements from various countries for Internet activity forensics, SmartZone is introducing a feature that allows the AP to send UE (User Equipment) session messages to an external syslog server. In 3.6, this is considered as phase1 of the feature.

In this release, the AP sends 5-tuple (source and destination MAC, source and destination IP, port) information to a syslog server for every new IP flow for every UE. This feature is configurable at the AP Zone level, and must be enabled on a per-WLAN basis.

Support 64 VLANs

In previous releases, Ruckus APs have supported up to 32 VLANs for clients. In this release, for ONLY 11ac Wave2 APs, will support 64 dynamic VLANs per AP. The purpose of this functionality is to improve scale and flexibility for large deployments, or custom deployments with many VLAN policy assignments.

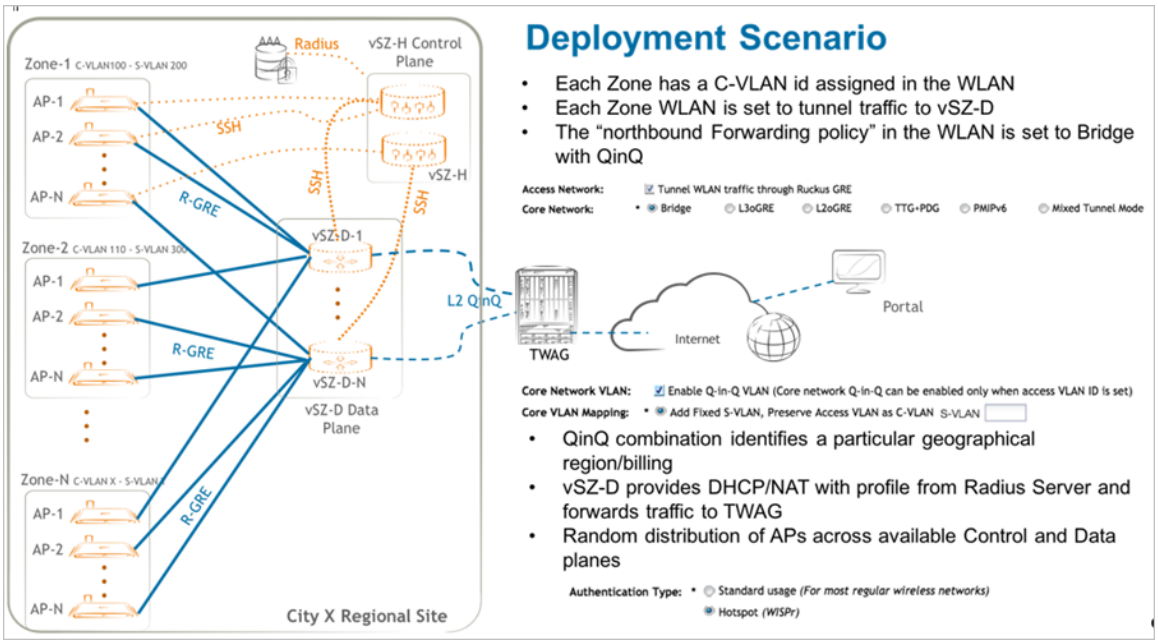
In this implementation, the VLANs can be assigned by dynamic connectivity policy (RADIUS, DPSK, OS, etc) or they can be assigned by VLAN pooling functionality.

> NOTE
> Only 64 VLANs are supported on 11ac Wave2 APs. Configuring more than 32 VLANs on older AP models may cause AP instability and have adverse effects on AP operations. It is strongly recommended to refrain from configuring more than 32 VLANs on those APs.

Radius Profile based DHCP/NAT

This feature implements Radius aware functionality on vSZ-D, which allows choosing appropriate DHCP or NAT profile to serve clients.

FIGURE 2 Radius Profile based DHCP/NAT Deployment



RF Coverage Heatmap

In this release, we are introducing the first phase of RF coverage heatmap visualization. In this initial release of the feature, the SmartZone provides a static visualization of RF coverage on an indoor floor plan map by leveraging a standard path loss model to estimate coverage . The AP's actual transmit power is taken into consideration in the coverage estimate, but the sites actual RF characteristics are not incorporated. The coverage heatmaps are enabled by a simple show RF coverage checkbox that can be enabled from the map view.

Limit AP Number per Zone

This feature is primarily for MSP use cases where an MSP may have multiple customers, each with their own zone and number of APs. The feature is designed to provide the operator with control over AP license consumption on a per-zone basis, to avoid over subscription by a tenant.

In today's SZ platform, licenses are applied and enforced system-wide. But looking at a MSP scenario as an example, we see the problem. For example, a provider purchases a total of 500 AP licenses, and has 2 SMB customers, in Zone A (300 APs) and Zone B (200 APs), respectively. Zone A & Zone B customers each bought their share of AP licenses. But during implementation, the SMB using Zone A deploys additional APs, up to 315. As the other tenant attempts to deploy their 200, the SmartZone rejects their final 15 APs, due to over-subscription of licenses.

Another use case, the number of bought support licenses should be more than 90% of the APs managed by SZ or the SZ cannot be upgraded. So, when you have zone A customer bought support licenses for all of his APs and zone B customer did not buy any, then the system-wide audit will give a bought support license count less than 90% hence not upgradeable. So, zone A customer is being penalized for zone B's behavior.

This feature is applicable to all SZ based license types.

SCG 200 As A Control-Plane Only Node

Ruckus SCG200 controller has announced EOS and will be officially EOS by January 2018. To help prepare existing customers for planned migration to SZ300, Ruckus offers this SCG200 as a control-plane node (SCG200-C) option for existing customers to upgrade to R3.6.

SCG200-C is a Control Plane only option of the existing SCG200 SKUs. Functionality of the SCG200-C has all R3.6 features, excluding completely DP (Data Plane) related features and Geo-Redundancy. It is able to support the same scale as the regular SCG200 in prior releases.

SCG200-C will be able to manage LBO and Direct tunneling over SoftGRE. R-GRE tunneling from AP to the SCG200-C will not be supported. Existing customers who are using SCG200 data plane (SCG200-D) will need to migrate to other Ruckus data plane options that are managed by SCG200-C:

- vSZ-D/Virtual (for data plane termination) is supported and managed by SCG200-C.

  NOTE
  Cluster Geo-redundancy is not supported on the SCG200-C.

The upgrade eligibility verification error message is not able to list all the WLAN configuration details for Ruckus GRE tunnel at same time. [SCG-74202]

Show Rogue AP Location

This feature visually identifies the estimated location area of a rogue AP on a map within the SZ GUI. By locating a rogue AP, administrators can easily take action to manually remove or further investigate the rogue AP or provide forensics. For this release, rogue APs are located only from the rogue AP report page. By selecting a rogue AP from the table and clicking the "Locate Rogue" button, a map will pop-up to show the rogue's estimated location on a floorplan. In situations where the rogue AP is only detected by a single AP, the system will identify the single detecting AP, without attempting to show a location estimate (due to the inherent inaccuracy).

NOTE
This feature is only supported for rogues on an indoor map. Rogue location is determined by RF trilateration, which has well-known accuracy limitations. For that reason, this feature is provided as a convenience only, to facilitate the identification of a rogue's general location.

Configurable Rogue Classification Policy

The purpose of this feature is to provide administrative control over classifications of rogue APs. Specifically, network admins would like to automatically configure a set of classification policies that are automatically enforced by the system, to either ignore harmless rogues or to escalate rogues with specific behaviors and provide automated containment.

In prior releases, the Ruckus rogue feature supported a static set of rogue classification behaviors, following this logic: if the detected AP is not managed by the same SZ system, it is "rogue." Additionally, if the rogue is on the same LAN, spoofing the AP's SSID, or spoofing the AP's BSSID, it is considered a "malicious rogue" and should be automatically contained with active measures by the detecting AP.

In this release, we're introducing a configurable policy for rogue classification, with the following parameters:

1. Same SSID - this is supported prior to 3.6, but now admins can enable or disable this rule from the policy.
2. Same BSSID - this is supported prior to 3.6, but now admins can enable or disable this rule from the policy.
3. Same Network - this is supported prior to 3.6, but now admins can enable or disable this rule from the policy.
4. RSSI - this is a new parameters that allows the admin to classify an AP based on its RSSI. This is commonly used for rogue APs that are on the fringe of an AP's listening reach, and thus outside the physical area of concern.

5. SSID - this is a new parameter that allows the admin to classify an AP based on its advertised SSID. Of course we know that spoofing the AP is often malicious, but there may be neighbor networks with known SSIDs, or some other devices that advertise well-known SSIDs, for which the admin may want to classify the rogue differently, such as making it a "known" rogue.
6. MAC OUI - this is a new parameters that allows the admin to classify the AP based on its MAC address organizationally unique identifier (OUI). Some devices may be purpose-specific, or from a known product manufacturer, and thus classified either more loosely or more strictly as rogues.

In addition to the new policy rule types, we have added new classification types:

1. Ignore - used to ignore a rogue.
2. Known - used to identify that the rogue is not harmful.
3. Rogue – the classic type, used to identify that a rogue is unwanted or unknown, but may not require preventative actions.
4. Malicious – used to identify rogues for which containment action is required

In addition, the rogue page display now provides the ability to manually classify rogues according to these new types. Filters can also be applied to view rogue by type.

NonProxy AAA Role-Based Policy for SZ

In prior releases, the SmartZone architecture provided role-based policies (assigning specific traffic or connectivity rules to users/devices), but it was only supported for authentication flows that were "proxied" through the SmartZone itself. However, within distributed enterprises and MSP environments, there is increasing interest to provide 802.1X connectivity alongside role-based policies. To support this architecture type, the SmartZone APs needed enhancement to fully resolve role policies without requiring SmartZone interaction. This feature is an extension of the work we've done in the past releases for Proxy AAA. All role-based policies (UTP (rate limit, L3/4 ACL, L7 ACL, Bonjour (3.6)), VLAN, VLAN pool, and any others) are supported in this architecture.

This feature is an extension of the work we've done in the past releases for Proxy AAA. All role-based policies (rate limiting, L3-7, URL filtering), VLAN, VLAN pool, and others) are supported in this architecture for non-proxied authentication flows.

2-Step MAC Authentication & 802.1X Authentication

This feature is an enhancement to the SmartZone software to simultaneously support 802.1X and MAC Address authentication mechanisms in which both methods must pass for a user to successfully authenticate. This is to validate that both the user and the device are authorized.

When the administrator selects the WLAN type with authentication method "802.1X & MAC," the following behavior will happen:

1. MAC address authentication proceeds as with a WLAN with authentication type *MAC Address*.
2. If MAC address authentication is successful, 802.1X/EAP authentication proceeds as with a WLAN with authentication type *802.1X EAP*.
3. If both are successful, the UE is authorized to access the WLAN.

Report Wired Port Clients Stats

This function enhances the current wired port client stats reporting by support client stats for devices on ports that do not require authentication. In prior releases, we only provided statistics for clients that were 802.1X authenticated. In this release, the Ethernet port can be configured (disabled by default) to report client statistics, even if no authentication is enabled.

In addition to stat visibility, the administrator can also disconnect the client devices from the port. Each AP Ethernet port can support up to 16 devices.

Adaptive Band Balancing

In this release, SmartZone APs add functionality for Adaptive Band Balancing. In prior releases, band balancing logic was only enacted during the initial connection stage. At that time, the AP decides how to adjust its responses in an attempt to steer the client to a preferred radio band. In this release, the band balancing logic has been enhanced such that the AP can re-balance client connections after they have connected to the AP. This allows for dynamic optimization in case of some common scenarios:

1. If capacity significantly changes on one radio or the other, the AP can adjust client count per radio to maximize aggregate capacity.
2. If prior clients are properly balanced across bands, but a large number of incoming clients (or recently connected clients) are not dual-band, or are disproportionately preferring one band over the other, the AP can re-adjust already connected clients (that are more amenable to either band) to seek a more optimal balance of client load.

Group and Unbound DPSK Scale Increase and Design Change

In prior releases of SmartZone, there are two types of DPSK that are stored in the AP, instead of the SmartZone: Unbound DPSKs and Group DPSKs. Unbound DPSKs are DPSKs for which a specific MAC will be bound after first use-but the DPSK has not been used yet. Group DPSKs are DPSKs that can be simultaneously be used by a group of client devices.

In prior releases, the database scale limit of Unbound DPSK and Group DPSKs was kept separate, at 256 Unbound and 64 Group DPSKs. However, due to interest in increasing the number of Group DPSKs, we have blended the database, such that both Unbound and Group DPSKs are pulled from the same maximum pool of 320 DPSKs (256+64=320). This allows either Unbound or Group DPSKs to scale higher, or to have any mixture of Unbound and Group DPSKs up to a maximum total of 320.

DPSK Supports Role VLAN Setting

This enhancement is a simple adjustment to the VLAN application logic. In prior releases, if the DPSK is assigned to a Role, the Role's VLAN was not applied to the DPSK, due to the definition of a VLAN natively for the DPSK itself. However, some customers have requested the ability to override a DPSK VLAN by assigning that DPSK to a specific role, thus gaining the benefits of both DPSK policy as well as role-based policy in one workflow. So in this release, the VLAN of a role will now override the VLAN of a DPSK.

Google Maps Enhancements and Changes

The following UI enhancements have been made in the 3.6 release:

1. API Change - As background, when an application like SmartZone integrates Google Maps functionality, the system uses Google's APIs to interact with Google Map functionality. For every API use, an API key is used for tracking and authentication by the Google service. In the SmartZone application, this single was generating a high number of API transactions. Due to the high cost of maintenance for a single ubiquitous API key, and to provide deeper flexibility for customers, we have adjusted the API key behavior such that the default setting is to send API calls without an API key. In most cases, this functionality works without issue and users will not notice the behavior change. However, in some cases where there is very high usage of the Map API, we have provided a function for administrators to input their own API key, which can be generated from the Google API console.
2. Google Address Auto-Convert - In past releases, in order to place an imported indoor floor plan image on the Google Map, we required GPS coordinates, which identify the exact location for that indoor map. However, typing GPS coordinates can be cumbersome, so in this release, we've implemented two functions that simply the process. First, for the "address" field, we now integrate with Google to provide an auto-search and auto-complete feature, to identify a location using Google's services. Second,

when the address is entered and the user selects the GPS fields, the system will auto-populate GPS coordinates based on the address entered. This eases admin burden when setting up indoor maps.

3. **Show mesh links between mesh-connected APs on Google map -** On the Google map, when two APs are shown and are connected using Ruckus mesh, the map will now show a dashed line indicating that the two APs are connected via mesh. This helps identify topology and back haul relationships in a spatial perspective. If the admin hovers the cursor over the mesh link, he/she can identify additional details about the mesh link, such as root/mesh nodes, uplink and downlink traffic, and uplink/downlink SNR.
4. **Map Icon Clustering -** In this release, we've also added a function such that when the admin zooms out on a Google map, as the indoor map icons get closer together, they will eventually cluster together into a single icon, making the UI display much cleaner and easier to see the number of locations/sites in an area. By clicking the clustered icon, the system will zoom in to show all the maps in the area.
5. **Icon size -** In this release, AP map icons were also adjusted (made smaller) to improve the UI display and avoid clutter caused by larger icons.

UI Enhancements

The following UI enhancements have been made in the 3.6 release:

1. **Added AP CLI Commands to SmartZone GUI -** In this release, the SmartZone GUI adds support for a few commands that were previously only available in the AP CLI:
   a. **DTIM Interval -** In the WLAN context, administrators can now adjust the DTIM interval.
   b. **Directed Threshold –** In the WLAN context, administrators can now change the directed threshold, which controls the number of clients per radio at which the AP will stop converting multicast into unicast.
   c. **RTS/CTS Protection -** In the AP radio context, for the 2.4 GHz radio, administrators can now manually set the protection mode.
2. **Create WLAN from WLAN Group -** This enhancement simply adds a feature so that administrators can now create a WLAN from within the WLAN Group create/edit context. This avoids workflow "back-and-forth" caused when the admin did not already create a WLAN prior to creating a WLAN group.
3. **Default AP Group is Now Editable** In SmartZone, every Zone contains a default AP Group. In prior releases, this AP Group always inherited the configuration of the zone itself, with no possibility for overrides. But, many customer scenarios prefer to adjust each of the AP Group with some unique configuration, so the default AP Group now allows for this.
4. **Preview Tab Enhancements in AP, WLAN, and Client pages -**In AP, WLAN, and Client UI pages, some subtle enhancements have been made for navigation and workflow.
   a. **Automatically select system node of group tree -** When these UI pages are first opened, the UI will automatically select the "System" on the group tree hierarchy and highlight the first entry in the table. This improves the experience of "preview" contextual information at the bottom of the page in a tabbed menu format.
   b. **Improve tab load time within UI -** In the "preview" tabs at the bottom of the screen, the load time of this information has been improved.
   c. **Show loading icon when tabs are refreshing -** If the administrator is viewing data that is being refreshed, or loading slowly, a UI icon will now be shown to indicate that the task is in progress.
5. **Added Neighbor AP information to non-mesh zones -** In prior release, the administrator would view the **AP Page** > **Mesh View Mode** in order to see AP neighbor data. This required mesh to be enabled. In this release, we have made the AP neighbor information available in other View Modes on the AP page (the neighbor table is in the General tab).

6. **Automatically open/edit a profile/service entry when it is double-clicked -** When viewing a table of profiles/objects (WLAN, AAA, Policies, etc), if the administrator double-clicks one, it will automatically open the edit dialog.
7. **Allow custom time zoom in health/traffic charts -** In all Health and Traffic time line charts, the admin can now select a customized time range by dragging across the chart. This allows a narrower focus on the data, if the preset time spans (1hr, 24hr, 7days, 14days) do not provide the desired perspective.
8. **Channel change event indicators displayed on AP Capacity and AP Client Count charts -** On AP Capacity health charts and AP Client Count traffic charts, we have now added indicators showing when the AP radio has changed channels. This allows the admin to evaluate the impact of a channel change on operating behavior, like radio capacity and client connectivity.
9. **Expand main work area by reducing left navigation menu –** We have added a new UI feature to expand the main work area by minimizing the left navigation menus. By default, the UI will display text menu links on the left side. When minimized, the left menus will be minimized to icons, which improves overall usable space for the main pane of the UI.
10. **Added Time Zone display to report generation scheduling –** To ensure that the report scheduling is utilizing the preferred time zone, a time zone selector has been added to the report scheduling function.
11. **Ruckus AP Tunnel Stats - Added Zone Search Function -** For Ruckus AP tunnel stats, a Zone search function has been added to more easily identify the desired zone.

Bonjour Fencing Enhancements

Some minor updates have been made to the Bonjour Fencing functionality:

1. In this release, we've added support for Bonjour Fencing in Tunneled WLANs.
2. Previously, each Fencing policy could only have 32 wired device rules. In 3.6, we have increased this to 512.
3. Previously, each AP and each Bonjour service could only have a single wired device mapped to it. In this release, we have increased it to 4.

vSZ Resource Profile

In this release, the virtual SmartZone adds another VM resource profile tier. In prior releases, the vSZ-E (Essentials) supported only 100 APs or 1,000 APs. In this release, we have added a profile tier for 500 APs, giving customers more flexibility in their VM resource provisioning.

Report 802.11 Client Types to SCI

The goal of this enhancement is to provide more data about client 802.11 support to SCI, such that SCI's reports can provide more granular traffic and client stats for the mixture of 802.11 standards.

- 802.11b
- 802.11g
- 802.11n
- 802.11a
- 802.11ac

SZ300 Maximum Concurrent Client Support

SZ300 maximum concurrent client (user equipment) support does increase from 300K to 450K per 4-node cluster. **[SCG- 65603]**

Changed Features for Release 3.6

The following are the behavior changes in this release.

AP Behavior Changes

- In any given zone, APs can be configured with same number of VLANs. For instance, 64 VLAN APs will be in a zone without 32VLAN APs to avoid client roaming issues.**[SCG-73014]**
- APIs /v6_0/cluster/status and /v6_0/cluster/nodeStatus are deprecated in this release. It is recommended to use the new API / v6_0/cluster/statewhich serves the same purpose as the deprecated APIs. This API adds cluster/state URI such as:
  - Cluster state - In service cluster, which supports AP/DP connection
  - Node state - In service node, which supports AP/DP connection
  - Management state - In service refers to all services on SZ node to create or update the configuration on the node. **[SCG-71781, SCG-70287, SCG-69644, SCG-71020]**
- The controller method must add deprecate setting in the API version annotation for the cluster status URI to be deprecated. **[SCG-77781]**
- Maps does not load without Google Maps API Key when SCG is accessed using IPV6 address. **[SCG-70224]**
- Add CLI commands ap-cert-expired-check and no ap-cert-expired-check to allow and disallow the AP connect by using expired certificate. **[SCG-71075]**

  NOTE
  It is recommended to update the AP certificates before installing or upgrading to release 3.6

  NOTE
  The time taken to implement the CLI command setting is about 5 minutes. There are no corresponding events or errors since APs cannot connect with expired certificate.

- RADIUS returned DHCP/NAT pools are only effective for MAC authentication while using MAC+WISPr (Dual) authentication. **[SCG-71773]**
- The controller cannot identify old certificates. This means that there is no specific error message if the AP cannot connect to the controller due to AP certification expiry. **[SCG-69412]**
- AP MTU behavior change: In previous releases, when you modify Tunnel MTU to a manual value this modifies AP Tunnel interfaces but also local interface (br0). In 3.6, modifications to Manual Tunnel MTU value will only affect AP Tunnel interfaces (but not anymore br0.

  NOTE
  If you had configured 1300 for example in 3.5, then you will have that MTU value assigned to br0 and br8. When you modify this configuration in 3.6 Web UI to 1400, br8 will change to 1400 but br0 will remain configured to 1300.

  Workaround: May need to manually modify br0 MTU on the AP to configure the correct value. **[SCG-73405]**

Control Domain

The following are the changed features related to Control Domain.

For IPv6 auto configuration, control plane supports stateful mode from this release onwards. Stateless mode is no longer supported. The current behavior is:

- Control plane ignores M and O flags and prefixes A flag in RA packets.

- Control plane always gets the IP address from DHCPv6, if the option is not set to static.
- Control plane does not auto generate the IPv6 address from RA packet prefixes.
- DNSv6 only comes from the user's input.
- Router and prefix lifetime are ignored. [SCG-72010]

Bonjour Fencing System Behavior

- Dynamic changes in Bonjour Fence policy with different Hop values for bonjour services will not be effective unless all bonjour services are restarted from the bonjour servers. [AP-6137]
- If a bonjour service is fenced by a single AP in a Zone, then the configuration persists even after AP reboots. For example, screen sharing service fenced only by a neighboring AP, then the configuration persist even after AP reboot. However if the same service is fenced by multiple APs in a Zone, then the configuration does not persist after the AP reboots. For example: Fencing is enabled for screen sharing service with device MAC-1,2,3 by the neighboring AP and with device MAC-4,5,6,7 by the anchor AP. If the anchor AP reboots, it has fencing rules for 4,5,6,7 (in kernel) but it does not persist the neighboring AP fencing configuration which has the device MAC 1,2,3.

  Currently with the multiple wired devices support, bonjour fencing rules for anchor AP is stored in RSM buffers and the remaining fencing rules are stored in the kernel. This optimization is done to prevent high memory consumption at the RSM buffers. In this release, the system has 512 rules with 32 policies supported with 4 devices, which is an overall of (512*32*4) 65536 fencing rules per AP. This needs to be stored in a text format, which results in high consumption of memory.

  Workaround: If the AP reboots, it will lose configuration support of multiple wired devices. Client need to apply Bonjour Fencing configuration from the controller, again, which will get transferred to the AP for the feature to work. [AP-6146]

Public API Port Change

The following is the port change in this release.

The Public API port has changed from 7443 to 8443 (which is the same port as being used by the Web user interface). It is highly recommended to customers to update any of their API scripts.

> NOTE
> For backwards compatibility port 7443 is still available, but **not recommended.**

System Behavior Change

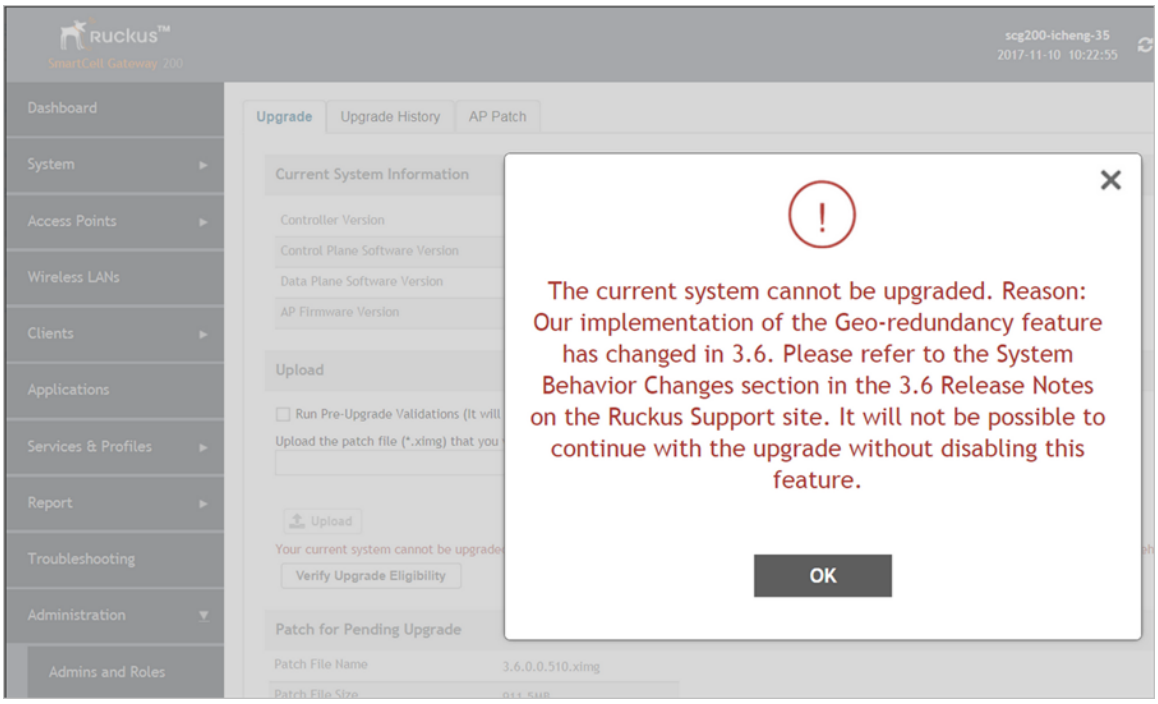
- In previous releases, Communicator process (handling AP-Controller communication) was running as a standalone application only in SCG-200/SZ-300 controllers and in vSZ-H when using Resource levels 7-8. In other cases, this process was consolidated inside Core application. Starting with 3.6 release, Communicator process is a standalone application for all controller models and resource levels. So, when you upgrade Controllers with Core application to 3.6 this new service will appear with a default WARNING log level. All AP-Controller communication logs will be part of that service instead of Core service (that will continue to exist). [SCG-72468]
- Statistic data persisting and business logic handling facility are separated from the Communicator to a newly created *StatsHandler* application for the objective of controlling and managing responsibility separation. New system logs have been added for this feature. [SCG-62929]
- Alarms related to data plane (for SCG 200 only) are not supported in this release. These alarms are retained in the system on upgrade to 3.6, which needs to manually acknowledged or cleared. [SCG-71930]

- External NAS IP configuration under the advance settings of WLAN is only applicable when CALEA is also enabled on WLAN. [SCG-73905]
- Users could get the errors *MissingKeyMapError* or *NoApiKeys* even after joining a cluster. It is recommended that users use their own Google API key by using the below link if they encounter these errors. [SCG-73804]

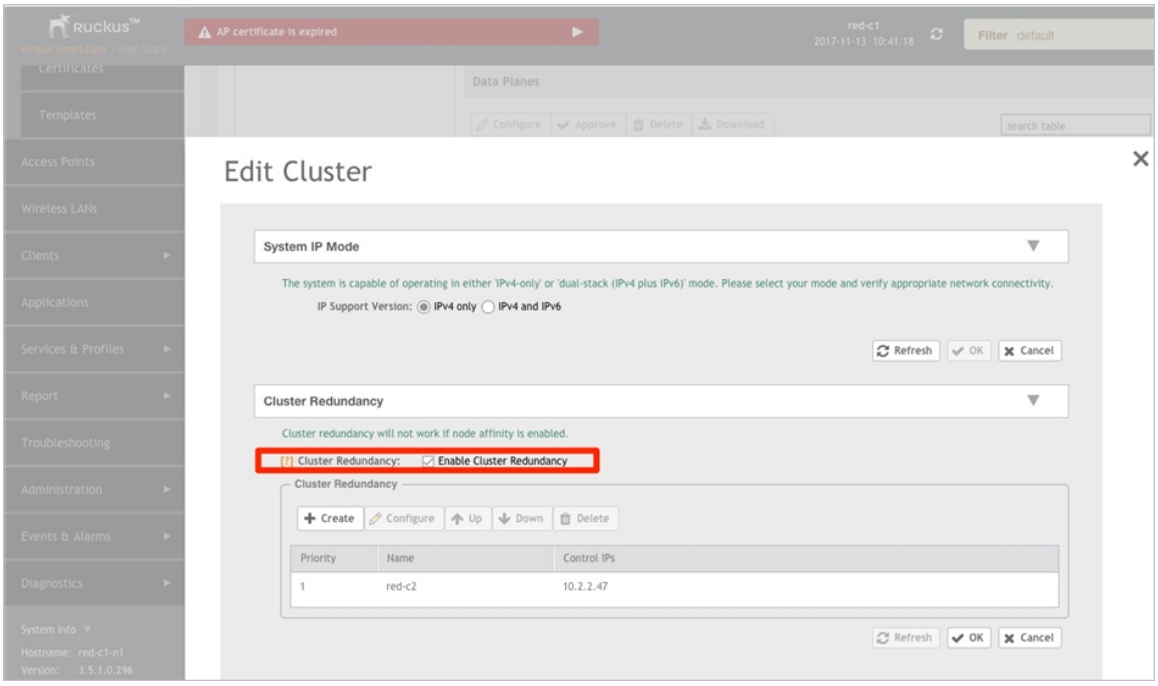
  `API Key`

- Users needs to add a script (HTML tags) for the portal title to have a HTML effect on the user equipment browser. This procedure is also for guest access portal and smart client instruction. [SCG-73352]
- TTG feature is not supported from 3.6 release and upwards. [SCG-32706]
- Option of cloning of WLAN from one zone to other zone is removed in this release. [SCG-73361]
- Implementation of the Geo-Redundancy feature has changed in 3.6. If you have enabled cluster redundancy in the controller, you will not be able to upgrade to this release. To continue with the upgrade, you would first need to disable the cluster redundancy feature and reapply the upgrade. [SCG-76062]

  The following message is also seen in the web interface.

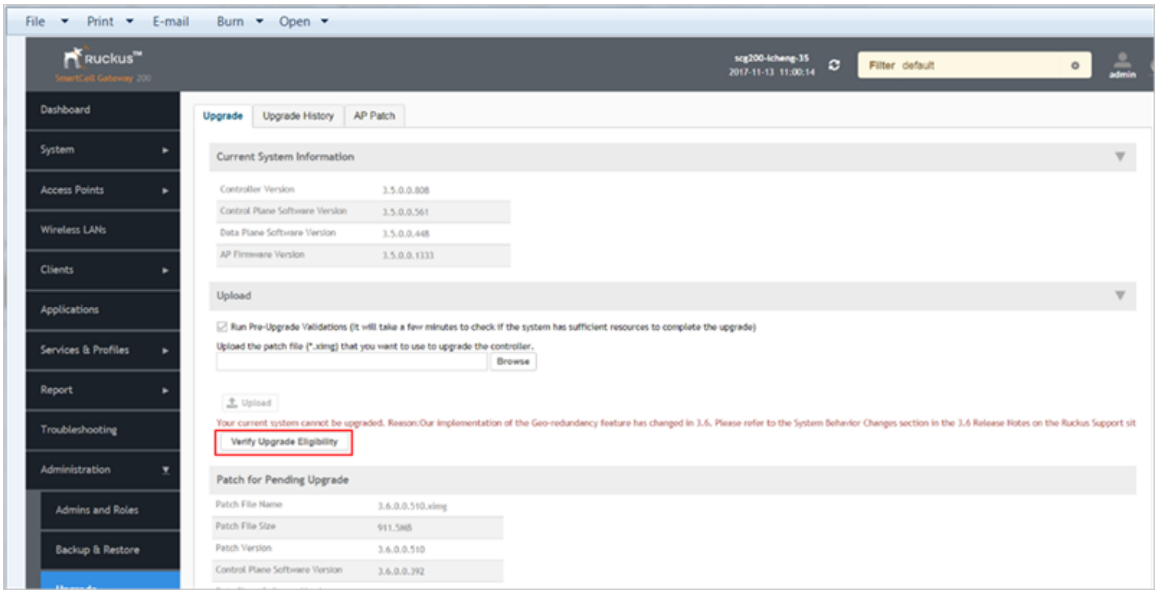


To disable the legacy cluster geo-redundancy, login to the web interface and navigate to **System** > **Cluster** > **Configuration** > **Configure** . Uncheck the *Enable Cluster Redundancy* option. Click *OK* to save the changes.



To reapply the upgrade, navigate to **Administration** > **Upgrade**. Click the *Verify Upgrade Eligibility* option to proceed with the upgrade provided all validations are passed.

NOTE
Refer to the *Performing the Upgrade* section in the Administrator Guide for upgrade details.



SNMP Walk Scripts

For SNMP walk scripts:

- Avoid running walk scripts when there are plenty of offline APs in the system.
- If there is a return timeout try to increase the timeout value by adding:

```
-t <seconds> (1 default value)
```

vSZ Resource Profile

In this release, the virtual SmartZone adds another VM resource profile tier. In prior releases, the vSZ-E (Essentials) supported only 100 APs or 1,000 APs. In this release, we have added a profile tier for 500 APs, giving customers more flexibility in their VM resource provisioning.

Hardware/Software Compatibility and Supported AP Models

Overview

This section provides release information about the SmartZone 300 (SZ300), the SmartCell Gateway 200 (SCG200), 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 SCG200, developed for the service provider market, combines a WLAN access controller with Wi-Fi traffic aggregation, along with a built-in carrier-grade element management system in a 2U rack-mountable, all-in-one hardware form factor.
- 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 SCG200, 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 data traffic for PCI compliance, and offers differentiated per site policy control and QoS, 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 Wireless 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 Wireless 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.

BSD 3-Clause for New and Revised Licenses for URL Filtering

A permissive license similar to the BSD 2-Clause License, but with a 3rd clause that prohibits others from using the name of the project or its contributors to promote derived products without written consent.

Release Information

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

T310c, T310s, and T310n APs are supported as new AP models on SZ 3.6 GA release. The GA released SZ build 3.6.0.0.510 software does not natively support these AP models, and requires adding the new AP models bundle patch software to support these APs.

NOTE
See Adding a New AP Model on page 28 for adding the new AP model software to the controller.

SZ 300

- Controller Version: **3.6.0.0.510**
- Control Plane Software Version: **3.6.0.0.392**
- Data Plane Software Version: **3.6.0.0.510**
- AP Firmware Version: **3.6.0.0.771**

SCG 200

- Controller Version: **3.6.0.0.510**
- Control Plane Software Version: **3.6.0.0.392**
- AP Firmware Version: **3.6.0.0.771**

SZ 100

- Controller Version: **3.6.0.0.510**
- Control Plane Software Version: **3.6.0.0.392**

- Data Plane Software Version: **3.6.0.0.148**
- AP Firmware Version: **3.6.0.0.771**

vSZ-H and vSZ-E

- Controller Version: **3.6.0.0.510**
- Control Plane Software Version: **3.6.0.0.392**
- AP Firmware Version: **3.6.0.0.771**

vSZ-D

- vSZ-D software version: **3.6.0.0.510**

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.

In R3.6 GA , Ruckus has released T310c, T310s, T310n and T310d APs as new AP models, which require SZ AP patch to be applied on the R3.6 GA build.

APs preconfigured with the SmartZone AP firmware may be used with the SZ300, SCG200, SZ100, or vSZ in their native default configuration. APs factory-configured with the ZoneFlex-AP firmware may be used with the SCG200/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 Wireless AP models.

TABLE 1 Supported AP Models

11ac-Wave2		11ac-Wave1		11n	
Indoor	Outdoor	Indoor	Outdoor	Indoor	Outdoor
R720	T710	R700	T504	R300	ZF7782
R710	T710s	R600	T300	ZF7982	ZF7782-E
R610	T610	R500	T300E	ZF7372	ZF7782-N
R510	T310c	C500	T301N	ZF7372-E	E ZF7782-S
H510	T310d	H500	T301S	ZF7352	ZF7781CM
C110	T310s	R310	FZM300	ZF7055	
H320	T310n		FZP300		

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	Unsupported AP Models
SC8800-S	SC8800-S-AC
ZF7321	ZF7321-U
ZF7441	ZF7761-CM
ZF7762	ZF7762-AC
ZF7762-T	ZF7762-S
ZF7762-S-AC	ZF7363
ZF7343	ZF7341
ZF7363-U	ZF7343-U
ZF7025	ZF7351
ZF7351-U	ZF2942
ZF2741	ZF2741-EXT
ZF7962	

Adding a New AP Model

This SmartZone release supports the registration of new AP models that were not yet available when this SmartZone version was released.

Before starting this procedure, verify that the controller is running on release version 3.6 GA release (Build 3.6.0.0.510).

This procedure will upgrade all APs that are registered with the Zone. During the upgrade process, service outage will occur as the APs will restart automatically to complete the upgrade.

In the Enterprise controller version, the default Zone must be changed to reflect the AP patch version before the new AP is connected to the network. In the High Scale controller version, the new AP registers to the staging Zone and it needs to be moved to a specified Zone with the AP patch version.

NOTE
Before uploading the new AP patch, Ruckus strongly recommends saving a cluster backup. If you need to restore the controller to the previous AP patch, you can use this cluster backup. Before uploading the new AP patch, Ruckus strongly recommends saving and exporting a configuration backup file. If you need to restore the configuration in case of anomaly, you can restore the configuration backup.

Follow these steps to register the new AP model with the controller.

1. Log on to the Ruckus support site.
2. Download the patch file, which enables the controller to support the new AP model.

   For the T310 model, the patch file is `ap_t310_patch_pkg-3.6.0.0-771.noarch.patch .`

3. Move the patch file to a location that you can access from the computer that you are using to access the controller's web interface.
4. Log on to the controller's web interface.
5. Navigate to the **Administration** > **Upgrade** screen.
6. In the **AP Patch** tab, click **Browse** to select the downloaded file in the option, **Upload the AP patch** (*.patch) that you want to patch.
7. Click **Upload**.

   Depending on your web browser a browse or open dialog box appears.
8. Click **Apply Patch**.
9. Manually change the AP firmware (using the option **Change AP firmware** in the SmartZone web interface) to the latest AP image (3.6.0.0.709) in the default zone for an Enterprise controller version or specify the zone for a High Scale controller version.
10. Navigate to the **Monitor** > **Access Points** page, to verify that the new AP model added to the controller is listed on **AP list** page. In addition, verify that all AP's in the default or specific zone are upgraded to build 3.6.0.0.709.
11. In the **Registration State** column, verify that the new AP model is approved.

You have completed adding new AP model to the controller.

Caveats, Limitations, and Known Issues

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]**

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]**

- Connection failures are calculated at 90 seconds interval. If during that time there are only failed attempts (even a single one) and no successful ones, the system will display 100% connection failure. But you can go to AP health tab to see the total number of failure and successful connection attempts during that period. [SCG-73311]
- If an AP or one of the radio's on AP has no activity then the capacity is reported as '0'. [SCG-74742]

AP Known Issues

The following are the known issues related to APs.

- 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]
- 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]
- The AP is unable to obtain the correct WLAN list for the new zone when an AP is moved from one zone to another zone, which is using a whitelist with high number of entries. For example, 10 WLANs with 64 entries. [SCG-68407]
- 802.1x operation of the Ethernet 1 (PoE) interface may not operate in supplicant or authenticator mode. [SCG-67078, SCG-67079]
- Calea mirroring fails when the packet size is more than 1440 and the option *dont fragment* is set. [AP-4034]
- 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.

  Workaround: To resolve this issue, reboot solo APs after the DNS server address on the DHCP server is updated. [SCG-34299]
- 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.

  Workaround: To clear or update the location information on APs, do it at the AP level (instead of the zone level). [SCG-39848]
- 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.

  Workaround: Limit the maximum clients number per WLAN. Using the above example, you can set the maximum clients per WLAN to 100. [SCG-43697]
- 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.

  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. **[SCG-47518]**
- 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).

  Workaround: Make sure that the "Daylight Saving Time" check box on the **Access Points** > **System > Select the Zone > Configuration** page is not selected. **[SCG-50883]**
- 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.

  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. **[SCG-51529]**
- 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]**
- Rebooting the H510 AP using the CLI causes the AP to log a 'Kernel Panic' eve **[SCG-60852]**nt. 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]**
- 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.
- 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]**
- Client isolation is not supported when a client roams from one AP to another in the same WLAN. **[SCG-66077]**
- 802.1x operation of the Eth1 (PoE) interface may not operate in supplicant or authenticator mode. **[SCG-67078, SCG-67079]**
- 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]**
- The R710 AP stops responding after the AP's Ethernet port speed is configured to 100 full duplex and its ports are connected to the Netgear Switch M4100. **[SCG-67707]**
- 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.

  Workarounds:

  - Reset the R720 to factory default settings.

  - Perform LLDP set via RKS CLI, and then reset the AP to “set LLDP power 25000”. **[SCG-68405]**
- When an AP is moved from one zone to another zone that is using a whitelist with a high number of entries (for example, 10 WLANs with 64 entries), the AP is unable to obtain the correct WLAN list for the new zone. **[SCG-68407]**
- 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.

  Workaround: Edit the secondary channel field with available channels, and then apply the configuration. **[SCG-68602]**
- 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]**.
- If 802.11R Roaming and Single Accounting Session ID are enabled and when a client roams from AP1 to AP2, the Class and Chargeable-User-Identity attributes are missing in the Interim-Update packet that is sent out by AP2. **[SCG-70831]**
- 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]**
- If a 3.5.1 SZ configuration backup is applied to a controller running 3.6 DHCP service will be down for that zone .

  Workaround: Disable and reconfigure DHCP/NAT service through the user interface. **[SCG-74919]**
- Wireless Multicast communication happens between clients on the same AP and same WLAN, even when Client Isolation is enabled for that WLAN. **[SCG-73791]**
- Different APs may generate the same Acct-session-id value in Radius Accounting traffic for two clients. **[SCG-76210]**
- If network connectivity between primary and secondary APs running DHCP service is not correct, upon recovery of primary AP DHCP service may fail for several minutes. **[SCG-76056]**
- 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.

  Workaround: Change the settings of AP-DHCP profile to reflect the same as DNS override, to override the issue. [ER-5493]
- 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]**

AVC Known Issues

The following are the known issues related to AVC.

- AVC rate limiting for user-defined applications does not work on fragmented packets. **[SCG-65933]**
- AVC is unable to identify Vindictus traffic accurately. **[SCG-43487]**
- AVC with Trend Micro 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 AVC cannot determine the application that a device is using, the controller displays the device's IP address as the application name. **[SCG-47746]**

- The Trend Micro engine that is used by AVC 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]**
- AVC is unable to identify BitTorrent traffic accurately. **[SCG-43336]**
- Strange traffic flows with inconsistent uplink and downlink are displayed on the AVC page in release 3.4. [SCG-44169] When configuring a denial policy in AVC, take note of the following limitations:
  - When "google.com" is set as the AVC 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 AVC 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., AVC will be unable to block such traffic because Trend Micro 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. **[SCG-44384]**
- The AVC denial policy requires both the user-defined app and app port mapping, instead of only the user-defined app name. **[SCG-44724]**
- 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]**
- On the Applications page, when a user selects a specific app, all clients that have used this app in different domains are displayed on the page. **[SCG-64735]**
- AVC does not support clients that are assigned IPv6 addresses. **[AP-4835]**
- AVC identifies YouTube as "googlevideo.com." **[SCG-61150]**
- AVC is unable to apply policies consistently to apps that cannot be identified by Deep Packet Inspection (DPI). **[SCG-60339]**
- When AVC cannot determine the application that a device is using, the controller displays the device's IP address as the application name. **[SCG-47746]**
- 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]**
- Clients are able to access eBay services though the deny rule is set. **[AP-5347]**
- Clients are able to access Gmail and Google+ service access though the deny rule is set. **[AP-5226]**
- The ARC deny rule does not work on proxied YouTube streaming traffic. This issue occurs 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]**
- Denial rule does not work for WhatsApp messenger on R710 AP. **[AP-5561]**

- 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]

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 Fencing is unsupported for Google Chromecast Services. [SCG-65552]

Bonjour Gateway Known Issues

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

- Bonjour gateway does not work when the Apple TV and MACBook Air are in two different VLAN's on the same WLAN on the same AP. [SCG-73788]
- 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]
- 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]

Cassandra Known Issues

The following are the known issues related to cassandra .

- WISPr authentication may fail if the CNR receives an invalid home server type. [SCG-52520]

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 setting up the SZ100, the DNS IP address has to be configured manually because DNS IP address assignment via DHCP cannot be completed. [SCG-38184]
- 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 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]

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]
- Network tunnel statistics are not displayed for dual stack APs when queried with an IPv6 address. [SCG-57446]
- 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.

  Workaround: To resolve this issue, Ruckus Wireless recommends assigning a static IP address to the SZ100 network interface. [SCG-41046]
- When rate limits are modified, the new limits are not applied to clients that are in the grace period. [SCG-51422]
- When you restore the system using a cluster backup, configuration backup files may get deleted. Ruckus Wireless 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 testing an IPv6 accounting server, the NAS IP4 attribute is sent in the accounting message. [SCG-61667]
- 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]
- DPSK may fail to work after upgrade under certain conditions: Controller is upgraded to 3.6 (but not the zone), zone configuration using DPSK is modified, and finally the zone is upgraded to 3.6.

  Workaround: Create or delete a DPSK in the zone. This operation will trigger sending new (and different) DPSK configuration to the AP, which will resolve the issue. [SCG-73628]
- Cluster backup is not visible on the web interface or in CLI even after it is successfully copied from the FTP server only if both backups share the same timestamp and version. [SCG-74488]
- Resetting TOS QoS configuration for AP control traffic (using command 'no ap-control-mgmt-tos') will not revert back to the default *no QoS marking*. Assigning any other possible value will work.[SCG-74695]
- The AP local-subnet discovery does not work properly in the default-enabled state due to the data plane design limitation. This only affects SZ-100 controller in port group 1. [SCG-75012]

Data Plane Known Issues

The following are the known issues related to the data plane.

- IPv6 stateless addresses are unsupported. [SCG-59194]

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.

- Creating an AAA service for AP zones that are managed by MVNO using the Public API is currently unsupported. [SCG-52111]
- 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]

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]

System Known Issues

The following are the known issues related to the system.

- If you are restoring a backup configuration which includes more than 100 indoor maps you will not be redirected automatically to login page. Instead you need to open a new login page manually. [SCG-74911]
- 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]
- Administrators who do not have the privilege to manage alarms may be able to clear or acknowledge alarms in bulk. [SCG-34126]

- 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]
- To protect the virtual controller against denial-of-service (DoS) and other forms of network attacks, Ruckus Wireless 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]
- The controller may be unable to renew its DHCP server-assigned IP address, which may cause all controller services to go down. [SCG-40383]
- 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 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.

  Workaround:

  - Do not shut down the Azure hypervisor, or;

  - Set a static IP address for the controller on the Azure hypervisor. [SCG-42367]
- IPv6 addresses for accounting servers on the SZ100 and vSZ are unsupported. Only accounting servers on the SCG200 can be assigned IPv6 addresses. [SCG-46917]
- 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 SCG to which an AP is connected gets rebooted, the AP moves to another SCG in the same cluster. When theSCG 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.

  Workaround: Do nothing. Subsequent calls will work fine. [SCG-50826]
- 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]
- Syslog servers that are using IPV6 addresses are currently unsupported. [SCG-53679]
- 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]

- Downloading the SCG200 snapshot log and AP support log may fail if multiple attempts are performed in quick succession. [SCG-61855]
- 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]
- Controllers are not able to display the IPv6 gateway on the control interface. [SCG-72261]
- NAS IP setting in WLAN configuration only applies to Radius Authentication packets, and not to Accounting. [SCG-73900]

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 SZ100 Setup Wizard does not validate the IPv6 address if the IPv6 prefix is not configured. [SCG-40257]
- 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]
- After the accounting service is disabled for a particular WLAN, Accounting Off messages are not initiated. [SCG-47772, SCG-40827]
- 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.

  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. [SCG-48255]
- 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]
- The channel background application sends the channel number without checking whether the current channel mode supports the channel number. [SCG-60820]

- 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]

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]
- 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 can impact UE bootp and ARP packets when vSZ-D runs the DHCP/NAT service. [SCG-64238]
- 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]
- When the internal DHCP server in vSZ-D is enabled, the DHCP discover/request messages from UEs are not forwarded to Local Breakout if no matching DHCP profile is found. This is design intent. To override this behavior, enable DHCP relay in the WLAN configuration. [SCG-64664]
- 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.

  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. **[SCG-68535]**
- 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]**

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]**
- A zone affinity profile cannot be deleted if it is in use by a SoftGRE zone. **[SCG-68651]**
- 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]**

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, Ruckus Wireless recommends using 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]
- A zone template created with HS2.0 settings, WISPr WLAN and Radius accounting applied to create a new zone will fail to work properly.

  Workaround: Once the zone is created, disable and re-enable Radius accounting service. [SCG-71137]

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 (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.

- 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

AAA Resolved Issues

- Resolved an issue where wired client did not use the configured secondary authentication server when the primary authentication server was unavailable. [SCG-52194]

AVC Resolved Issues

The following are the resolved issues related to AVC.

- Resolved an issue where AVC now works with DHCP/NAT on APs. [SCG-64358]

AP Resolved Issues

The following are the resolved issues related to AP.

- Resolved an issue where the H320 AP did not support mesh. If the H320 AP was assigned to a controller's zone, which was mesh enabled, the Ethernet profile of the H320 AP could not be changed. [SCG-69297]
- Resolved an issue where CoA was used to apply rate limit to a user's web authentication session and as a result subsequent web authentication session of the same user has the same rate limit. [SCG-68381]
- Resolved an issue where configuration push to APs failed when SoftGRE IPv4 MTU value was set between 850 and 1279 bytes in a SoftGRE tunnel profile attached to a dual mode zone. [SCG-67583]
- Resolved an issue where malicious devices were still seen as "SSID spoofing" on the Rogue AP/Malicious AP list after the same SSID was removed on the Ruckus AP. [SCG-67332]
- Resolved an issue where the AP WLAN group became default after quitting the configuration mode of the AP on the controller CLI. [ER-5661]
- Resolved an issue where R500 and H500 APs rebooted due to Kernel Panic and Watchdog Timeout. [ER-5700]
- Resolved an issue where MAP rebooted with the reason *problem detected* when 50 clients were connected to the AP. [SCG-74094]
- Resolved an issue where Kernel panic was observed when the MAP roamed between two RAP. [SCG-77145]

- Resolved an issue where under extreme client count (60+) on Mesh AP it was observed that kernel panic and target hung approximately every 4 hours when the mesh AP frequently changed the uplink between two root APs. **[SCG-74329, SCG-77145]** .

Bonjour Fencing Resolved Issues

- Resolved an issue where bonjour fencing did not support Tunnel WLANs. This only applies to SZ-100 . **[AP-3842]**

Rate Limiting Resolved Issues

- Resolved an issue where when rate limiting is enabled, the throughput for voice traffic was restricted to around 128kbps (128kbps in case of UTP rate-limit and 100kbps for SSID rate-limit). **[SCG-51924]**

System Resolved Issues

The following are the resolved issues related to the system.

- Resolved an issue where the application category field was reported as zero in AVC GPB streams for external systems. **[SCG-65936]**
- Resolved an issue related to the WPA KRACK vulnerability. For information on security incidents and responses, see https://www.ruckuswireless.com/security. **[AP-6463]**
- Resolved an issue where icons on the dashboard were not loading on Google Chrome. **[SCG-65180]**
- Resolved an issue where on a WLAN where both the tunnel and proxy ARP services were enabled, the proxy ARP service stopped working when the tunnel service was disabled. **[SCG-68987]**
- Resolved an issue where the IPv6 SoftGRE MTU was incorrect when the MTU for a dual stack zone was set to 1500 bytes. **[SCG-67497]**
- Resolved an issue where smart roam was not working as required. **[ER-5684]**
- Resolved an issue where the controller's user interface display of memory size differed from CLI's display of memory. **[ER-5588]**
- Resolved an issue where the internal IP subnet for AP-DP communication in tunneled WLANs may conflict with the client's address space. A new SZ CLI command has been introduced to modify this subnet. **[ER-5376]**

```
ap-internal-subnet <IP-subnet-address>
```

- Resolved an issue where Client Isolation feature in SoftGRE or SoftGRE+IPSec mode can now be enabled or disabled. **[SCG-75504]**
- Resolved an issue where controllers SZ300, vSZ-H, SZ100 and SZ-E support IPv6 zones with Ruckus GRE tunnels. **[SCG-61781]**

UI/UX Resolved Issues

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

- Resolved an issue where the current implementation of L3 roaming did not allow users to select VLAN-based roaming for one set of vSZ-D, while using subnet-based roaming for another set of vSZ-D on same vSZ system. **[SCG- 64729]**
- Resolved an issue where the current implementation of L3 roaming was not allowing users to select VLAN-based roaming for one set of vSZ-D, while using subnet-based roaming for another set of vSZ-D on same vSZ system. **[SCG-64729]**

Virtual Data Plane Resolved Issues

The following are the resolved issues related to the virtual data plane.

- Resolved an issue where the set-factory command on the vSZ-D CLI did not completely reset the vSZ-D to the default settings. [SCG-68228]
- Resolved an issue where if the AP IP mode on vSZ was set to IPv6 only, managed APs was unable to establish tunnels with vSZ-D. [SCG-39206]
- Resolved an issue where when Sub-Option 1 Type 4 is selected under Option 82, vSZ-D did not forward Sub-Option 1 inside Option 82 in a DHCP Relay scenario. [SCG-68497]

Virtual SmartZone Resolved Issue

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

- Resolved an issue where backup of virtual machine on Hyper-V failed when vSZ was online. [ER-5609]
- Resolved an issue where the WLAN's SSID was not advertised from the AP when the IPv6 tunnel was configured for a WLAN. [SCG-69363]

WISPr Resolved Issues

- Resolved an issue where when WISPr user rate limit was throttled by CoA, the same CoA rate limit was applied to the same user on the next logon. [SCG-68309]

XSS Vulnerability Resolved Issue

- Fixed several XSS vulnerability issues with the Guest Pass template review. [SCG-71733]

KRACK Vulnerability Fix

About This Release

This release fixes multiple vulnerabilities (also known as KRACK vulnerabilities) discovered in the four-way handshake stage of the WPA2 protocol. The Common Vulnerabilities and Exposures (CVE) IDs that this release addresses include:

- CVE-2017-13077
- CVE-2017-13078
- CVE-2017-13079
- CVE-2017-13080
- CVE-2017-13081
- CVE-2017-13082

IMPORTANT
If you are running a release that is later (or newer) than the AP builds listed below, DO NOT apply this fix. Contact Ruckus Support for the appropriate KRACK fix for your build.

- 3.5.1.0.1010
- 3.4.2.0.384

For more information about KRACK vulnerabilities, visit the Ruckus Support Resource Center at https://support.ruckuswireless.com/krack-ruckus-wireless-support-resource-center.

SmartZone 3.6 Release

SmartZone 3.6 release supports the following AP firmware versions:

- 3.6.0.0.709 (this release)
- 3.5.1.x (any 3.5.1 AP firmware, except any build later than 3.5.1.0.1010)
- 3.4.2.x (any 3.4.2 AP firmware, except any build later than 3.4.2.0.384)

NOTE
Build number 3.6.0.0.510 includes the KRACK fixes.

To ensure that wireless network users connecting to the APs running these firmware versions are protected against KRACK attacks, you need to deploy the corresponding patch file for each of these AP firmware versions (see below for instructions).

To locate the KRACK vulnerability patches you need for your controller, go to https://support.ruckuswireless.com/product_families/11-smartzone-products, and then click **Software Downloads** for your controller platform to view the available patches.

NOTE
This 3.6 release includes fixes for the KRACK security vulnerabilities. For more information see https://support.ruckuswireless.com/security and https://support.ruckuswireless.com/krack-ruckus-wireless-support-resource-center

Patching AP Firmware 3.5.1.0.x

This AP firmware version supports the following AP models:

TABLE 3 Supported AP Models

C110	H500	R500E	R710	T301S	T710S	ZF7781CM	ZF7982
C500	H510	R510	R720	T504	ZF7055	ZF7782	
FZM300	R300	R600	T300	T610	ZF7352	ZF7782-E	
FZP300	R310	R610	T300E	T610S	ZF7372	ZF7782-N	
H320	R500	R700	T301N	T710	ZF7372-E	ZF7782-S	

If your controller currently has this AP firmware version 3.5.1.0.x (except any build later than 3.5.1.0.1010), you must apply the following AP patch bundle:

scg-ap-3.5.1.0-1026.noarch.patch

For instructions, see Applying an AP Security Patch on page 51.

Patching AP Firmware 3.4.2.x

AP firmware 3.4.2.x supports the following AP models:

TABLE 4 Supported AP Models

C110	H510	R510	T300	T610	ZF7352	ZF7782-E
C500	R300	R600	T300E	T610S	ZF7372	ZF7782-N
FZM300	R310	R610	T301N	T710	ZF7372-E	ZF7782-S
FZP300	R500	R700	T301S	T710S	ZF7781CM	ZF7982
H500	R500E	R710	T504	ZF7055	ZF7782	

If your controller currently has AP firmware version 3.4.2.x (any 3.4.2 AP firmware, except any build later than 3.4.2.0.384), you must apply the following AP patch bundle:

scg-ap-3.4.2.0-405.noarch.patch

For instructions, see Applying an AP Security Patch on page 51.

Applying an AP Security Patch

Before you begin this procedure, copy the AP patch file that you want to apply to a location that you can access from your computer.

IMPORTANT
This patch only needs to be applied to a single node. After you apply this patch to a node, it will be propagated automatically to other nodes in the cluster.

Follow these steps to apply an AP security patch:

1. Log on to the SmartZone web interface.
2. Go to the page for uploading AP patches.
   - On the web interface, go to **Administration** > **Upgrade**, and then click the **AP Patch** tab.
3. In **Patch File Upload**, click **Browse** go to the location where you saved the AP patch file (with *.patch file name extension).
4. Click **Open**.
5. On the **AP Patch** tab, click **Upload**. After the patch file is uploaded, the section is populated with the Start time, AP firmware version number and AP model number.
6. Click **Apply Patch**.

   After the patch file is applied, the AP patch information is populated with the following information:
   - Name of the patch file
   - Size of the patch file
   - AP firmware version number
   - AP model number
7. Go to **Configuration** > **AP Zone**.
8. On the **AP Zone List** page, click a zone name.
9. Click **Change AP Firmware**.
10. In the **Change AP Firmware** dialog, click the upgrade button that corresponds to the AP patch file that you uploaded earlier. A confirmation message appears.

11. Click **Yes**.

    When the controller completes updating the AP firmware of the zone, a message appears and notifies you that the zone's AP firmware was updated successfully.
12. Go to **Configuration** > **Access Points** and click a zone from the domain tree.
13. On the **AP List** page, check the value for the **Configuration Status** column.

    If it shows `Downloading Firmware...`, this indicates that the APs that belong to the zone are in the process of downloading and installing the updated AP firmware.

You have completed applying an AP security patch.

Protecting Clients That Have Not Yet Been Patched

Client devices that have not yet been patched with this release are vulnerable to KRACK attacks. To help protect these unpatched clients, Ruckus strongly recommends uploading and executing the EAPOL-No-Retry AP CLI script that was created for this specific purpose.

Enabling the eapol-no-retry feature (disabled by default) prevents the host access point daemon (hostapd) from retrying the third EAPOL key in a four-way handshake and the first EAPOL key in a group key handshake, which are parts of the WPA2 protocol that have been found to be vulnerable to KRACK attacks. Note that enabling this feature may introduce connectivity delay in high density client environments due to EAPOL packet loss during the four-way or group key handshake period.

Available AP CLI Scripts for Enabling EAPOL-No-Retry

Every AP firmware that is supported by this release has a corresponding AP CLI script for enabling EAPOL-No-Retry. The following are the scripts that are currently available.

- Enable-EAPOL-No-Retry-AP-CLI-Script-3.6.0.0.709 -v1.txt

Uploading the AP CLI Scripts

Before you begin this procedure, obtain all the scripts that you require from Ruckus Support and copy them to a location that you can access from your computer.

Follow these steps to upload an AP CLI script:

1. Go to **Administration** > **Common** > **AP CLI Script**.
2. In **Select AP Zone**, choose the AP zone for which you want to upload the script.
3. In **Upload AP CLI Script**, click **Browse**, select the AP CLI script, and click **Open**.
4. Click **Upload**.
5. Repeat Steps 2-3 for every script that you want to upload to the controller.

Executing the AP CLI Scripts

After you have uploaded all the scripts that you require from Ruckus Support and copied them to a location that you can access from your computer, you can execute the scripts.

Follow these steps to execute an AP CLI script:

1. Go to **Administration** > **Common** > **AP CLI Script**.
2. In **Select AP Zone**, choose the AP zone for which you want to run the script.

3. Click **Execute**.
4. Click the Execution Status column, and then verify that all of the APs that belong to the zone have executed the script successfully.

Available AP CLI Scripts for Disabling EAPOL-No-Retry

If you want to disable EAPOL-No-Retry, upload and execute the following scripts the same way you uploaded and executed the scripts to enable EAPOL-No-Retry:

- Disable-EAPOL-No-Retry-AP-CLI-Script-3.6.0.0.709 -v1.txt

Upgrading to This Release

Overview

This section lists important information that you must be aware of when upgrading the controller to this release.

Step-by-step instructions for performing the upgrade are provided in the corresponding Administrator Guide for your controller platform.

NOTE
Before uploading a new AP patch, Ruckus Networks strongly recommends that you save a cluster backup, in case you want to restore the previous AP patch.

NOTE
Before upgrading the controller, Ruckus Networks 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.

NOTE
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 Wireless 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.

vSZ High Scale recommended resources

TABLE 5 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]	GB	GB	Max	Max	
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

vSZ Essentials recommended resources

TABLE 6 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	
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.

Supported Upgrade Paths

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

New AP bundle image upgrade path (T310x new install) - Apply the AP patch bundle 3.6.0.0.xxx to the controller system running (build 3.6.0.0.xxx) and change the image on the required zone for T310x support.

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]**

The table below lists previous releases that can be upgraded to this release.

TABLE 7 Previous release builds that can be upgraded to this release

Platform	Release Build
SZ300 SCG200 SZ100 vSZ (vSCG) vSZ-D	3.4.0.0.976
	3.4.1.0.208
	3.4.2.0.152
	3.4.2.0.169
	3.4.2.0.176
	3.5.0.0.808
	3.5.0.0.832
	3.5.1.0.296
	3.5.1.0.862
	3.6.0.0.510

Multiple AP Firmware Support in the SCG200/vSZ-H

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
Some older AP models only support AP firmware 3.1.x and earlier. If you have these AP models, note that the controller cannot be upgraded to this release.

NOTE
If you have AP zones that are using 3.2.x and the AP models that belong to these zones support AP firmware 3.4 (and later), change the AP firmware of these zones to 3.4 (or later) to force these APs to upgrade their firmware. After you verify that all of the APs have been upgraded to AP firmware 3.4 (or later), proceed with upgrading the controller software to release 3.6.

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 3.6, the AP Zone firmware remains the same.

Up to Three Previous Major AP Releases Supported

Every SCG200/vSZ-H release can support up to three major AP firmware releases, including (1) the latest AP firmware release and (2) two of the most recent major AP firmware releases. This is known as the N-2 (n minus two) firmware policy.

NOTE
A major release version refers to the first two digits of the release number. For example, 3.5 and 3.5.1 are considered part of the same major release version, which is 3.5.

The following releases can be upgraded to release 3.6:

- 3.5.x
- 3.5
- 3.4.x

- 3.4

The AP firmware releases that the SCG200/vSZ-H will retain depend on the SCG200/vSZ-H release version from which you are upgrading:

- If you are upgrading the SCG200/vSZ-H from release 3.5, then the AP firmware releases that it will retain after the upgrade will be 3.6 and 3.5 (and 3.4 if this controller was previously in release 3.4)
- If you are upgrading the SCG200/vSZ-H from release 3.4, then the AP firmware releases that it will retain after the upgrade will be 3.6 and 3.4.

All other AP firmware releases that were previously available on the SCG200/vSZ-H will be deleted automatically.

EoL APs and APs Running Unsupported Firmware Behavior

Understanding how the SCG200 handles APs that have reached EoL status and AP running unsupported firmware can help you design an upgrade plan that will minimize impact on wireless users in your organization.

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 Wireless Support website. The icons for EoL APs appear with the *END OF LIFE* watermark.

- An EoL AP that has not registered with the SCG200 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.
- If an EoL AP is already being managed by the SCG200 and you attempt to upgrade the controller, the firmware upgrade process will be unsuccessful. The web interface may or may not display a warning message (see Upgrading With Unsupported APs). You will need to move the EoL AP to the Staging Zone to upgrade the controller successfully.

APs Running Unsupported Firmware Releases

- APs running AP firmware releases that are unsupported by the SCG200 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

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 Wireless controller products including ZoneDirector, SCG200, vSZ, SZ- 100, 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 AP 100.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

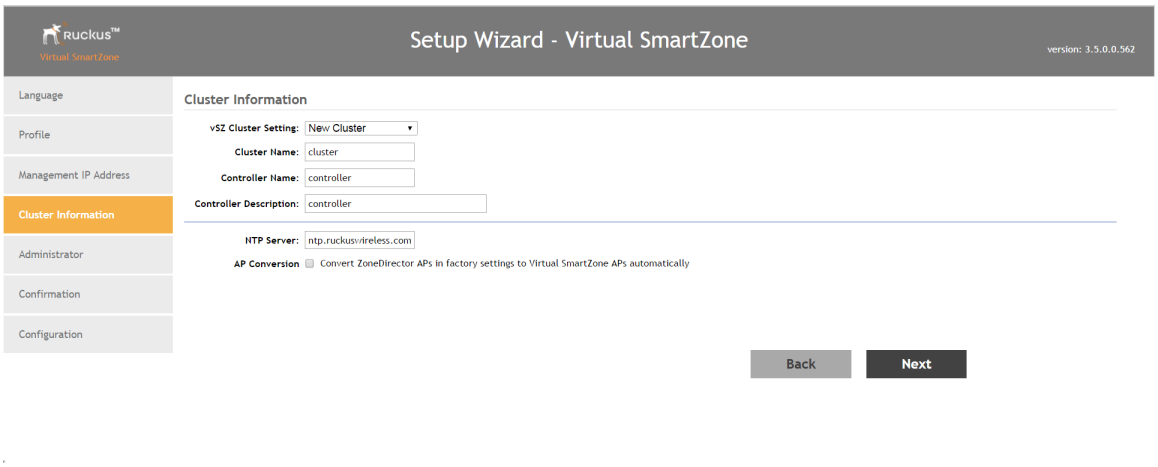
You can convert standalone ZoneFlex APs (those that are not managed by ZoneDirector)in factory default configuration to be managed by a SmartZone controller.

Follow these steps to convert standalone ZoneFlex APs to the SmartZone controller firmware so that they can be managed by the SZ300, SCG200, 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, SCG200, or SZ100 the check box description may be slightly different.

FIGURE 3 Select the AP Conversion check box to convert standalone ZoneFlex APs to SCG 200/SZ100/vSZ 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 Wireless qualifies its functionality on the most common clients.

350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com