RELEASE NOTES

vWLAN & BSAP 2.9.0
November 7, 2016

Trademarks

Any brand names and product names included in this manual are trademarks, registered trademarks, or trade names of their respective holders.

To the Holder of the Manual

The contents of this manual are current as of the date of publication. ADTRAN reserves the right to change the contents without prior notice.

In no event will ADTRAN be liable for any special, incidental, or consequential damages or for commercial losses even if ADTRAN has been advised thereof as a result of issue of this publication.

Toll Fraud Liability

Be advised that certain security risks are inherent in the use of any telecommunications or networking equipment, including but not limited to, toll fraud, Denial of Service (DoS) attacks, loss or theft of data, and the unauthorized or illegal use of said equipment. ADTRAN OFFERS NO WARRANTIES, EITHER EXPRESSED OR IMPLIED, REGARDING THE PREVENTION, DETECTION, OR DETERRENCE OF TOLL FRAUD, NETWORKING ATTACKS, OR UNAUTHORIZED, ILLEGAL, OR IMPROPER USE OF ADTRAN EQUIPMENT OR SOFTWARE. THEREFORE, ADTRAN IS NOT LIABLE FOR ANY LOSSES OR DAMAGES RESULTING FROM SUCH FRAUD, ATTACK, OR IMPROPER USE, INCLUDING, BUT NOT LIMITED TO, HUMAN AND DATA PRIVACY, INTELLECTUAL PROPERTY, MATERIAL ASSETS, FINANCIAL RESOURCES, LABOR AND LEGAL COSTS. Ultimately, the responsibility for securing your telecommunication and networking equipment rests with you, and you are encouraged to review documentation regarding available security measures, their configuration and implementation, and to test such features as is necessary for your network.

ADTRAN Technical Support Community

For information on installing and configuring ADTRAN products, visit the ADTRAN Support Community, https://supportforums.adtran.com.

ADTRAN

Pre-Sales Technical Support
(800) 615-1176
networkdesign@adtran.com

Corporate Office
901 Explorer Boulevard
P.O. Box 140000
Huntsville, AL 35814-4000
Phone: (256) 963-8000
www.adtran.com

Post-Sales Technical Support
(888) 423-8726
support.adtran.com

Contents

Introduction

The 2.9.0 code releases for vWLAN and BSAP are major system releases that adds new features and addresses issues that were uncovered in previous code releases.

These releases are generally available code. Results obtained during internal testing have been evaluated and the code has been determined to be ready for general availability. Caveats discovered during testing but not addressed in this build are listed in *Errata on page 10*.

A list of new or updated documents for this release appears on *page 14*.

Configuration guides, white papers, data sheets, and other documentation can be found on ADTRAN's Support Forum, https://supportforums.adtran.com. The contents of these release notes will focus on the platforms listed below.

Supported Models

The following models are supported in vWLAN 2.9.0.

- vWLAN Rackmount Appliance (1700900F1/1700900F2)
- vWLAN Virtual Appliance for VMware ESX/ESXi 4.X and 5.X
- vWLAN Desktop Appliance (1700918F1)

The following models are supported in BSAP 2.9.0.

- BSAP 1800v1 and v2
- BSAP 1840
- BSAP 1920/1925
- BSAP 1930/1935
- BSAP 1940
- BSAP 2020
- BSAP 2030/2035/2135

Important Upgrade Note Specific to This Release

vWLAN can only be upgraded to 2.9.0 if it is currently on version 2.6.2 or higher. vWLANs on versions 2.2.1 to 2.6.1 must first upgrade to version 2.6.2 and then upgrade to version 2.9.0. AP firmware does not have to be upgraded to 2.6.2 and can instead be upgraded directly to 2.9.0 with the second upgrade.

If you attempt an upgrade from a version prior to 2.6.2 to 2.9.0, the upgrade will error out and the following message will appear in the upgrade alerts and platform alerts:

*** MUST BE RUNNING 2.6.2 TO UPGRADE TO THIS IMAGE! *** (Please upgrade to 2.6.2 prior to loading this image.)

Required BSAP Firmware

Due to BSAP and vWLAN firmware versions being mutually exclusive, the associated version of BSAP firmware for vWLAN 2.9.0 has been re-versioned to 2.9.0. From this point forward, vWLAN and BSAP firmware names will match.

> NOTE *Version 2.7.0 was a limited software release not made generally available.*

The table below shows a version explanation:

vWLAN Version	BSAP Version
2.5.0	6.9.0
2.5.1	6.9.1
2.6.0	7.0.0
2.6.1	7.0.1
2.6.2	2.6.2
2.7.0	2.7.0
2.8.0	2.8.0
2.9.0	2.9.0

Wireless Regulatory Compliance

Based on United States FCC and European DFS and ETSI regulations, ADTRAN validates the country in which the APs are being operated. This prevents the ADTRAN equipment from accidentally being used in an improper configuration.

When customers request AP licenses, they must specify the country where the AP will be deployed and operated. Note that a single vWLAN can control and manage APs in different countries and regulatory domains – and the channel and power settings are regulated by the country where the individual AP is deployed and operated.

Before the license is installed, the AP is in the platform and not associated to any domain, so the AP's radios are disabled by default. When the licenses are uploaded, the country code is then applied to licensed BSAPs. Allowed channels and power levels are determined by the country and the platform, and once the AP is placed into a domain, it will scan the channels to discover neighboring APs and choose a valid channel.

Features and Enhancements

This section highlights the major features, commands, and behavioral changes in vWLAN 2.9.0**.**

DynamicRF (Radio Resource Management) Enhancements

- **Multi-tenant Support**

  - Added the ability to configure multiple DynamicRF Profiles per domain/tenant that can be assigned to different groups of APs on a per radio basis via the AP template rather than having to use platform-level settings.

- **Dual AP/Sensor Radio Mode for BSAP 19XX and BSAP 2XXX Series**
  - Added the ability for BSAP 19XX Series and BSAP 2XXX Series units to service clients on the current channel while non-intrusively performing off-channel background scanning for sources of interference and wireless intrusion detection. Off-channel background scanning is performed every 10 seconds with a dwell time of 190 milliseconds. Dual AP/Sensor Radio mode can be paired with Continuous DynamicRF mode to continuously adapt to changes in the RF environment by automatically changing channel and TX power settings as appropriate. AP/Sensor Radio mode can be paired with Set Once and Hold DynamicRF mode to continuously provide channel and TX power suggestions. Note that while off-channel background scanning does not impact service, it does allocate minimal airtime to performing off-channel scans and may result in a negligible performance decrease.
- **Enhanced DynamicRF Statistics**
  - Number of co-channel/adjacent channel interferers per channel per radio with advanced statistics including noise floor and channel utilization.
- **Additional Knobs and Dials**
  - Added the ability to enable/disable dynamic channel and transmit power independently. The system can be set to automatically configure channel settings but transmit power settings can be statically set and vice versa.
  - Advanced Configuration
    - Minimum and maximum transmit power can be used to set boundaries. For example, if a predictive design or an onsite survey indicated that TX power should be within a specified range, the system can be configured with that range to stay within those boundaries. Setting minimum and maximum TX power values to the same value will push that specific value out to all APs rather than having to configure each AP/radio individually.
    - **Previous Power Threshold Index** previously represented in RSSI has been renamed **Transmit Power Interference Threshold** represented in more widely used and understood signal (dBm). For example, the default value is now -82 dBm. Adjacent ADTRAN APs in the same domain on the same or adjacent channels will attempt to reduce TX power with the goal of being heard at less than this value.
- **Simplified Configuration/Setup, Ease of Use.**
  - Added the ability to clearly distinguish between settings configured automatically by the system (designated by **auto**) versus settings statically configured by the administrator. The system will not override static settings. Simply reset APs to defaults under **Status > Access Points** to set back to **auto** rather than having to reset each access point individually.
  - Previous **Min Signal Strength Counted** setting is no longer configurable/exposed and is always -82 dBm appropriately to simplify and prevent misconfigurations.
  - Previous **Give Weight to Existing Channels** setting is no longer configurable/exposed and is always enabled appropriately with the exception of during on-demand or scheduled background scans to simplify and prevent misconfigurations.

- Previous **Signal Inertia** and **Percentage of 802.11ac Clients** settings are no longer configurable/exposed and set appropriately by the system to simplify and prevent misconfigurations.
- ADTRAN APs in the domain/tenant and third-party APs/sources of interference not part of the domain/tenant are always considered by the dynamic channel algorithm.
- Only ADTRAN APs in the domain/tenant on the same channel are considered by the dynamic transmit power algorithm. The algorithm will not reduce TX power of ADTRAN APs in the same domain/tenant on different or nonadjacent channels and the algorithm will not reduce TX power because of third-party APs/sources of interference.
- Calibration is now referred to as **Background Scan** and can now be run with or without applying channel and transmit power settings during the scan. For example, running a **Background Sca**n without making channel and transmit power settings during the scan to perform quarterly wireless IDS scans for PCI compliance. **Background Scan** whether on demand or scheduled is typically paired with APs in **AP Radio** mode and **Set Once and Hold** DynamicRF mode.
- If running APs in **AP Radio** mode and **Set Once and Hold** DynamicRF mode, tasks will be provided as reminder to set up **Background Scan**. When running in **AP Radio** mode**/Set Once and Hold** DynamicRF mode, APs can only see the channel they are on after the initial set-once-and-hold period during first bootup, therefore data regarding sources of interference or wireless IDS on other channels can become stale.
- Added the ability to select APs and run **Background Scan** or **Accept DynamicRF Suggestions** on AP status page.
- Added the ability to schedule one-time or recurring background scans.
- Added the ability to apply channel and TX power settings during background scan or receive suggestions thereafter that can be applied on demand or scheduled at later time.
- Dynamic configuration of TX power in more granular 1 dBm increments versus 3 dBm.

DynamicSteering Support

- Added support for Band/Client Steering, Client Load Balancing, and Sticky Client Prevention Technology with support for 802.11k and 802.11v.

Enhanced Client/AP Statistics

- Added signal strength, transmit rate, noise, channel utilization, AP/vWLAN uptime, SSID MAC address (BSSID), number of co-channel/adjacent channel interferers statistics with drill down per radio.
- Added a new framework for client statistics under **Status** > **Clients List** with a 5-minute polling interval and **Status** > **APs List** with a 1-minute polling interval for AP statistics rather than the previous 15-minute polling intervals.
- Added a new framework for real time client/AP statistics under **Status > Clients Details** (drill down on a specific client) or **Status > AP Details** (drill down on a specific AP). Statistics display in real time with each refresh.

Dashboard Branding

- Added the ability to customize logo and colors of web-based administrative console on a per-platform and per-domain/tenant basis with appropriate administrative permissions.

Soft GRE Tunneling

- Added the ability to tunnel SSID traffic leveraging soft GRE to the Wireless Aggregation Gateway (WAG). For example, a carrier/service provider SSID with the carrier's brand name can be offered as a value add to their subscribers anywhere the carrier/SP deploys Wi-Fi or to selectively tunnel guest traffic.

Authentication Test

- Added the ability to perform cloud-based authentication testing without having to dispatch to remote site with wireless client. Authentication testing will provide success or failure responses from backend authentication server, an indication of the role that will be assigned, and list of attributes passed back from authentication server. Attributes can be leveraged for dynamic role assignment; for example, if filter-id RADIUS attribute = student then role = student.

Job/Task Schedules

- Added the ability to schedule one time and recurring vWLAN and AP jobs/tasks.

TX Power/antenna gain Enhancements

- Configurable TX power is now limited to the maximum of which the hardware is capable rather than allowing configuration of 30 dBm when the product may not be capable of supporting 30 dBm.
- Configurable antenna gain for use with ADTRAN-certified antennas or equivalent.
- Reporting of actual TX power in status versus the configured TX power.
- Reporting of antenna gain in status.
- Reporting of Max Allowed TX power in status.
- Reporting of Max Allowed EIRP in status.

Dashboard Reports and Analytics Enhancements (Widgets)

- System Summary Widget
    - Added a new platform widget that provides platform information such as CPU, Disk, Memory Utilization, Uptime, Part/Serial Numbers, Software/Patch Versions, High Availability Status, and whether or not platform is called home to ADTRAN Product Support.
- Added unique client count to the Client Count Over Time widget.

L3 Mobility Enhancements

- Added the ability to disable Layer 3 mobility.
- Added the ability to allow tunneling to the private IP address if APs behind two different NATs. Previously tunneling was not allowed with this scenario. Domain/tenant serves as a mobility domain.

API Enhancements

- Added client search via API by MAC or IP address
- Added REST API Resource Filter to allow a user to pull MAC devices by role

Other/Miscellaneous

- Domain/tenant backup now includes AP settings such as licenses, static channel/TX power configurations, AP firmware, etc.
- Updated device fingerprint signatures
- Simplified the device configuration page.

Fixes

This section highlights major bug fixes in vWLAN 2.9.0.

- The Security Daemon was not automatically restarted on a domain restore. This caused authentication issues in the restored domain.
- When performing RADIUS MAC authentication, the NAS port type was not sent in the RADIUS packet to the server.
- The attribute pairs Called-Station-ID and Calling-Station-ID within a RADIUS packet were improperly switched when using RADIUS MAC authentication.
- A log file could be written to continuously which eventually used up the server's disk space resulting in the inability to log in.
- Emails from vWLAN were not sent using the configured sender address in the UI.
- Upgrading vWLAN to the same build resulted in a lost configuration.
- Timed out users were not being removed from the UI if the user's device attempted to roam while in the unregistered role.
- NTP updates did not occur regardless of the frequency chosen in the platform settings.
- A horizontal scroll bar did not display when viewing large floor maps.
- Switching domains on the **Administration** > **Backup/Restore** menu led to a server error.
- In rare cases, the locations shown in vWLAN for each AP were incorrect.
- After creating a Internal User, the print page no longer automatically appeared.
- The database logs related to High Availability consumed all the disk space on a server causing the web interface to become inactive and client connectivity to suffer.
- In certain cases, AP licenses disappeared from the UI.
- vWLAN was not in compliance with SNMP System Group according to RFC 1213.
- The Calling-Station-ID and Called-Station-ID RADIUS fields differed between the Access-Request and the Accounting-Request packets.
- Accounting-Request Start RADIUS packets contained incorrect Acct-Input-Octets and Acct-Input-Octets attributes.
- The 1X NAS identifier field in the Access-Request and Accounting-Start RADIUS packets differed from each other.
- An 802.1X Access-Request RADIUS message contained a blank Accounting Session ID.
- The domain logs in vWLAN would stop functioning properly.
- DynamicRF significantly increased CPU load in large deployments.
- In extremely large deployments (~1500 Aps), the output of the **show tech** command filled the disk.

- vWLAN heat maps did not scale correctly when migrating from a version prior to 2.6.1 to a version after.
- A mesh portal was detected as an adjacent AP by a connected mesh point resulting in
- RF recommendations.
- DFS messages used the acronym BAP instead of BSAP when referencing an AP.
- Occasionally, the first time an AP was moved to a domain it would ignore its configured radio power settings until reconfigured.
- Due to a Windows 10 specific DHCP issue commonly seen with the Microsoft Surface Pro, certain clients devices would not allow a user to log in if they took longer than half of the configured NAC DHCP lease (default of 10 seconds). A NAC DHCP lease setting named **Relaxed** was added to address this. ADTRAN recommends this option be enabled under **Configuration** > **System** > **Settings** > **DHCP Lease Time for Un-registered Clients** if Windows 10 devices are used.
- If DynamicRF was set to **Set Once and Hold** on upgrade, APs would change channel or power settings.
- Unified access was not assigning NAC addresses for wired users.
- BSAP 1920s incorrectly sent Ethernet pause frames.
- Virtual Ethernet failed to connect causing a memory leak in the APs.

Security Vulnerability Fixes

This section highlights major security vulnerability fixes in vWLAN 2.9.0.

- An option to disable TLS 1.0 due to security concerns has been added. This is enabled by default so that all browsers will function correctly. It is recommended that this be manually disabled in **Configuration** > **System** > **Platform** > **Settings**. Some versions of Internet Explorer and Microsoft Edge may not function correctly after disabling it.

Errata

The following is a list of errata that still exist in vWLAN 2.9.0.

- Editing an AP job several times can eventually cause the user to receive an internal server error. **Workaround:** Create a new job to replace the old one.
- If using a GRE Tunneling Profile on an SSID, using a role with a non-native VLAN assigned to it will not allow a connecting user to receive an IP address.
- When a role schedule is initiated to remove a role currently authenticated clients in vWLAN may still show as authenticated in the vWLAN UI though they are properly denied access.
- DynamicRF will suggest Channel 0 if all channels available to a particular AP model are excluded in the AP template.
- Specifying a MAC address that is all uppercase while taking an AP Traffic capture causes the capture to fail to start.
- By default, outdoor APs are set to Indoor in the AP details page. **Workaround:** Navigate to **Status** > **APs** and select the particular AP to change this setting back to Outdoor.
- In a frequently changing RF environment, if new RF changes have been detected since the last status was displayed, DynamicRF suggestions shown on the **Status** > **APs** menu may not be the exact settings pushed to the AP upon pressing accept.

- Depending on the size of domain backup and configuration, the domain restoration process may take more time than expected.
- In an extremely crowded RF environment (APs with over 100 adjacencies), the DynamicRF channel algorithm may not choose the channel with the least interference.
- The time zone entries for Moscow, St. Petersburg, and Volograd are incorrect in the AP template.
- In rare cases, a DynamicRF change suggestion may fail to display a message on the **Status** > **APs** menu but it will be applied when accepting DynamicRF suggestions.
- The current channel being scanned by DynamicRF is not shown in the AP Status Page.
- After channel scanning, the AP adjacency produced by the channel scanning AP will show as all zeros.
- Adjacent APs running in 80 MHz mode are shown in vWLAN's Adjacent AP menu as 40 Mhz.
- The Signal and TX Rate fields for clients connected to BSAP 18XXs do not display correct information. These statistics are not supported on the BSAP 18XX Series.
- Unless the maximum and minimum transmit power are set to the same value inside a DynamicRF profile, those specific power settings will never be automatically chosen for radios.
- When moving an AP from any AP template back to the default template, a domain task will be incorrectly generated to create a scheduled background scan.
- Channel Utilization in AP Details do not display properly for the BSAP 18XX Series. This statistic is not supported.
- Allowing client-to-client traffic cannot be applied using the **Apply** option but instead requires an AP reboot.
- The minimum transmit power is displayed as 0 dBm when the channel in the AP template is set to **Auto**.
- WEP encryption may function sporadically. **Workaround**: Use WPA2 authentication.
- The **Select All** button only selects the first 100 table entries in the UI.
- Bulk Import only allows a 1000 line CSV file to be uploaded at a time.
- vWLAN logs report client data usage as kilobytes but the unit measure displayed is bytes.
- Scheduled dashboard reports do not include data for Current Client or AP count.
- Over time dashboard widgets cease to display the latest data point available.
- vWLAN UI logs do not display RADAR detection events.
- When configuring custom language login forms, vWLAN displays invalid characters for certain languages. Instead of the valid character, the browser displays ?.
- If invalid entries are made when configuring the LDAP server, the Administrator may not receive a valid error message.
- The Timeout Weight setting should be a required field in the LDAP Server configuration and will automatically default to **1** if left blank on initial set up.
- The administrator feature of **Downloading Widgets** as **JPEG** does not function.
- Uploading the same AP firmware file twice results in the inability to choose a different firmware file. **Workaround:** Navigate away from the page and back again.
- In certain cases, vWLAN does not send RADIUS Accounting stop messages.

- The client count display on the UI is inaccurate and out of sync in a large system with multiple clients roaming. The client count at the top of the UI page on the Domain status page and the client count at the bottom of the UI page do not match - even after multiple refresh cycles.
- On a heavily loaded system, the Captive Portal may fail to load when Redirect HTTPS traffic for Unregistered Clients is
- enabled.
- Packet captures taken from the vWLAN UI often miss packets. In a lab environment during captive portal authentication with RadiusWebServer, a test sent 50 packets but the PCAP observed only 48. **Workaround:** Administrators are advised to take multiple Packet captures when attempting to diagnose an issue.
- When attempting to execute an traffic capture from the vWLAN UI on an AP that is in a down state, the capture will not begin, but the UI will not return an error.
- After upgrading, some pages may not load correctly due to browsers' cached sorting options. **Workaround:** Clear the browser cookies and cache.
- When using the Drop User function, Apple MacBooks running OS X will retain a previously held IP address unless the timeout threshold is reached. This can cause web redirection to the captive portal to fail if the client attempts to connect to a different SSID. **Workaround:** Disable the wireless interface on the MacBook prior to dropping the user.
- Some customized login forms do not allow full customization of the page. The page renders the same without regard to the **Enable Complete Customization** selection.
- When using a Google Chromebook on a captive portal, the user will never be automatically redirected to their final destination. Manually refreshing the page or going to another page will function as expected.
- The intended behavior of HSTS is fundamentally incompatible with vWLAN's HTTPS redirection of clients to the login form. For example, Google, Facebook, and Yahoo all use HSTS and will not redirect to the login form in browsers that support HSTS. If an attempt is made to redirect to an HTTPS site that does not use HSTS (https://www.adtran.com works for this), a certificate warning is returned that cannot be ignored or bypassed. See http://caniuse.com/#feat=stricttransportsecurity to determine which browsers support HSTS.
- Wireless IDS alerts are not generated for the following conditions: AP Down, AP SSID Change, and AP Channel Change.
- The platform NTP server setting does not return errors when invalid values were entered for
- its host name.
- High Availability is not replicating HotSpot Login Forms correctly.
- In case of 1X Authentication Failed, vWLAN GUI will display Unregistered Role even though Different Role was configured.
- Some pages in the UI do not fully function under IE9. **Workaround:** Use a different browser, upgrade to a newer version of IE, or use the API.
- After executing any restart from the vWLAN GUI, the page must be refreshed manually.
- If an administrator attempts to delete an Email Configuration that was used to schedule a Dashboard job by a different user/administrator, the deletion will fail. It will give the name of the Dashboard that has the job scheduled, but the administrator might not have access to that dashboard to clear the job. The creator of the Scheduled Job must remove the job before the Email Configuration is deleted.

- If an AP is manually edited and a non-native location is selected for the Location, the AP may not discover locations correctly.
- Using the captive portal in the Catalan, German, Swedish, and Portuguese languages may display special characters instead of certain letters.
- APs configured for Mesh mode do not allow an AP traffic capture.
- The API may become unresponsive if used from multiple sources simultaneously. It will become responsive again after a few minutes.
- When upgrading a large database (with many historical records and/or domains), the system can take up to an hour to come up after the upgrade. **Workaround:** Implement HA or a high Control Channel timeout.
- The ability to preview a login form does not function properly when using the Opera browser.
- For fast-roaming, adjacent APs must detect each other and add each other as neighbors. If APs are brought in at different times, it is possible for neighbor detection to fail and roaming to take longer.
- In some cases, while running in AP/Sensor mode on the 2.4Ghz radio, smaller packet sizes (<=512 Bytes) will take a larger performance hit than normally running AP/Sensor mode (~10%).
- Role Scheduling does not affect IPv6 based traffic because of lack of IPv6 support and therefor that traffic will be bridged onto the wire. **Workaround:** Block IPv6 in the upstream firewall if necessary.
- When the number of firewall rules configured in a role reaches 1024, an AP will continuously reboot. Note that each service/hostname/IP constitutes one rule. Items designated as **both ways** count as two rules for each line.
- In rare cases when using 4+ SSIDs on a BSAP 1900 Series AP, the channel shown in the vWLAN UI may not be the actual channel on which the AP is operating.
- The **Noise Floor** is not shown in AP details for the BSAP 2000 Series AP's 5Ghz radio.
- When creating or editing a Role, if the administrator sets the **CoS Priority Out Overrid**e field to **DSCP from 802.11** or **802.1p from 802.11**, the IP packet put onto the wire will not have the DSCP value correctly set.
- The 2.4 GHz radio may only have 124 client associations, whereas the 5.0 GHz radio operates normally.
- Only 52 clients can associate to a BSAP 1800, despite vWLAN indicating a 64 client limit.
- BSAP 1800s may run low on memory causing sporadic client and AP activity or even a lost connection with vWLAN requiring a manual hard reset before operation can resume.
- Wireless packet captures may not function properly on the 5 GHz radio of a BSAP 1800 Series.
- The UI will allow configuration of greater than 1024 schedules. Configuring greater than 1024 schedules can result in AP reboots.
- Certain devices will present a Captive Network Assistant (CNA) even if the feature is disabled in vWLAN.
- If greater than 86 users are associated to an AP and a failover occurs, they will not appear immediately in the UI of the secondary vWLAN.
- The Sony Xperia Tablet Z running Android version 4.2.2 may fail to authenticate using 802.1x due to an issue with the device itself.

Release Specific Upgrade Instructions

vWLAN can only be upgraded to 2.9.0 if it is currently on version 2.6.2 or greater. vWLANs on versions 2.2.1 to 2.6.1 must first upgrade to version 2.6.2 and then upgrade to version 2.9.0. AP firmware does not have to be upgraded to 2.6.2 and can instead be upgraded directly to 2.9.0 with the second upgrade.

If you attempt to upgrade from a version prior to 2.6.2 to 2.9.0, the upgrade will error out and the following message will appear in the upgrade alerts and platform alerts:

*** MUST BE RUNNING 2.6.2 TO UPGRADE TO THIS IMAGE! *** (Please upgrade to 2.6.2 prior to loading this image.)

To upgrade your vWLAN Virtual Appliance Please see the vWLAN upgrade guide located at https://supportforums.adtran.com/docs/DOC-7691.

NOTE vWLAN 2.9.0 requires using Bluesocket Access Point (BSAP) firmware version 2.9.0. BSAP 2.9.0 is not backward compatible with previous vWLAN code versions.

NOTE Upon upgrading to vWLAN 2.9.0, if you have an AP that is configured in an ETSI Regulatory Domain, the 5GHz band will be disabled. To re-enable the radio, enable the DFS feature (if installed outdoors), or mark the AP as indoor (if installed indoors). In versions prior to 2.9.0, the vWLAN UI used references to UNII-3 channels (149-161) for APs in the ETSI domain. These are not valid ETSI channels and references to them have been removed.

NOTE vWLAN systems running 2.1 or earlier are not able to be upgraded. Instead, a new system should be deployed with 2.9.0 and configuration parameters from the 2.1 system should be manually ported to the 2.9.0 system. Attempting to upgrade a 2.1 system could cause some vWLAN configuration parameters to be lost.

Documentation Updates

The following documents were updated or newly released for vWLAN 2.9.0 or later. These documents can be found on ADTRAN's Support Forum available at https://supportforums.adtran.com. You can select the hyperlink below to be immediately redirected to the document.

- *vWLAN Admin Guide*
- *Using APIs with vWLAN*
- *Configuring DynamicRF in vWLAN*
- *Band Steering in vWLAN*