Adtran

# vWLAN & BSAP

# 4.2.1 Release Notes

Release Notes

*6ABSRNR421-40C*

*June 2023*

# To the Holder of this Document

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

# Trademark Information

“Adtran” and the Adtran logo are registered trademarks of Adtran, Inc. Brand names and product names included in this document are trademarks, registered trademarks, or trade names of their respective holders.

# Disclaimer of Liability

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products are given “as is”, and any liability arising in connection with such hardware or software products shall be governed by Adtran’s standard terms and conditions of sale unless otherwise set forth in a separately negotiated written agreement with Adtran that specifically applies to such hardware or software products.

To the fullest extent allowed by applicable law, in no event shall Adtran be liable for errors in this document for any damages, including but not limited to special, indirect, incidental or consequential, or any losses, such as but not limited to loss of profit, revenue, business interruption, business opportunity or data, that may arise from the use of this document or the information in it.

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

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

Copyright © 2023 Adtran, Inc.
All Rights Reserved.

# Table of Contents

# 1. Introduction

The 4.2.1 firmware release for Adtran's vWLAN is a maintenance release that addresses customer issues that were uncovered in previous code releases.

The release is 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 8*.

Configuration guides, white papers, data sheets, and other documentation can be found on Adtran's Support Community, https://supportcommunity.adtran.com. The contents of these release notes will focus on the platforms listed in *Supported Platforms on page 4*.

# 2. Supported Platforms

The following models are supported in the vWLAN 4.2.1 release:

- vWLAN Virtual Appliance for VMware ESX/ESXi, 5.X, and 6.X.

**NOTE**

*The 4.2.1 release is not supported on any previous Bluesocket Appliances. Customers still using Bluesocket Appliances should upgrade to a Virtual Appliance.*

Table 1 lists the Bluesocket Access Point (BSAP) platforms that are supported in vWLAN version 4.2.1.

**Table 1. Supported Platforms**

| BSAP Platform |
|---|
| BSAP 1920/1925 |
| BSAP 1930/1935 |
| BSAP 1940 |
| BSAP 2020 |
| BSAP 2030/2035/2135 |
| BSAP 3040/3045 |
| BSAP 6040 |

**NOTE**

*Some older AP models may not support all features in this release or past releases. For information about supported features on your AP model, refer to the AP Feature Matrix, available online at* https://supportcommunity.adtran.com.

Table 2 lists the legacy vWLAN features not yet supported on the BSAP 6000 Series APs.

**Table 2. Legacy Features Not Yet Supported on BSAP 6000 Series**

| Feature |
|---|
| Layer 3 Mobility |
| Walled Garden with NAC |
| Dynamic RF (Set Once and Hold) |
| DMO/MRO/Convert Multicast/Broadcast to Unicast |
| 802.11r |
| CoS/QoS in User Role |
| DFS |
| Mesh Networking |

# 3. Required BSAP Firmware

As AP firmware is packaged with vWLAN, the associated version of BSAP firmware for vWLAN 4.2.1 is 4.2.1.

# 4. Wireless Regulatory Compliance

Based on the 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 in which the AP will be deployed and operated. Note that a single vWLAN instance can control and manage APs in different countries and regulatory domains, and that the channel and power settings are regulated by the county in which the individual AP is deployed and operating.

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; once the AP is placed into a domain, it scans the channels to discovery neighboring APs and select a valid channel.

# 5. System Notes

The following information applies to systems running vWLAN 4.2.1.

- All vWLAN systems (starting with vWLAN 3.3.0) require a minimum of 8 GB RAM.
- 16 GB of RAM is required for vWLAN installations of over 750 APs, 12500 Clients, or 25 domains.
- To support 50 + domains (up to 150), 16 GB RAM is required in addition to 128 GB HDD.
- If utilizing post-login redirection, note that as of Android release 5.0, many Android phones do not keep the Captive Network Assistant Window open after authentication, which can cause the post-login redirect to fail.

- In some cases, the software version displayed in the output of the **show version** command in the AP's CLI may not populate correctly for legacy APs. In these cases, the branch name can be used to verify the software version.

**CAUTION!**

*Upgrading to vWLAN 4.2.1 will remove support for WPA, TKIP, and WEP security. Any configurations with WPA+WPA2 will be migrated to WPA2/AES-CCMP. Any SSID using WEP will be migrated to an Open SSID.*

# 6. Release-Specific Upgrade Instructions

Starting with version 3.1.0, vWLAN image files now include BSAP firmware within the image. Once the image has been uploaded and the server has been upgraded, a domain task will appear for the administrator with the text "New AP firmware is available, select domain, AP template, apply and activate." Selecting this administrator task allows you to apply the firmware to all templates in all domains.

vWLAN can only be upgraded to 4.2.1 if it is currently on version 3.7.1 or greater with the appropriate Pre-Upgrade patch installed. Upgrade steps must occur in the following order:

**NOTE**

*AP firmware does not have to be upgraded to 3.7.1 and can instead be upgraded directly to 4.2.1.*

1. vWLANs on versions 2.3.0 to 2.6.1 must first upgrade to version 2.6.2.
2. vWLAN on versions 2.6.2 must then upgrade to version 2.8.0.
3. vWLANs on version 2.8.0 and later must then upgrade to version 3.7.1.
4. Once vWLAN is upgraded to version 3.7.1, a pre-upgrade patch must be installed before upgrading to 4.x (*Pre-Upgrade patch for 3.7.1*). In addition to addressing upgrade issues between 3.7.1 and any 4.x software versions, this patch also provides for an HTTP error fix during the upgrade and allows a vWLAN 1 GB or more image upgrade to occur.

**NOTE**

*The 3.7.1 Pre-Upgrade patch for 4.2.1 requires the following:*

- *That all previous patches are removed before installing the pre-upgrade patch. This may take three to four minutes and a warning may be displayed; ignore any warnings as this is expected behavior.*
- *That the **Must restart Admin Web Server** platform task is executed as soon a the patch is installed. Patch installation will display error warnings upon installation; ignore these warnings as this is expected behavior.*

5. After installing the patch, vWLAN can be upgraded from 3.7.1 to version 4.x

> **NOTE**
>
> *When upgrading to vWLAN version 4.2.1, during the vWLAN .img file upload, you may receive the following error: "POST request to webserver failed with status 502. Please refresh and try again."* ***Workaround:*** *Reboot vWLAN and then perform the upgrade.*

To upgrade your vWLAN virtual appliance, refer to the *Upgrading Bluesocket vWLAN Controllers and APs* guide available online at https://supportcommunity.adtran.com.

> **NOTE**
>
> *vWLAN 4.2.1 and later requires using BSAP firmware version 4.2.1 or later. BSAP 4.2.1 is not backward-compatible with previous vWLAN code versions.*

# 7. Features and Enhancements

There were no features or enhancements introduced in vWLAN 4.2.1.

# 8. Fixes

This section highlights major bug fixes in vWLAN 4.2.1.

- VW-15035 Fixed an issue in which 802.11ax wireless mode had to be added manually to existing AP templates.
- VW-15034 Fixed an issue in which the BSAP 6040 devices incorrectly reported a lock file error in the CLI console.
- VW-15032/ VW-15033 Fixed an issue in which the **Access Point User Manager** failed to allow new users online when under a heavy load.
- VW-15031 Fixed an issue in which the BSAP 6040 devices prompted to remove files when the devices were being returned to factory default settings.
- BSAP-6545 Fixed an issue in which Apple clients could take multiple attempts to associate with an SSID.
- BSAP-6520 Fixed an issue in which, in some cases, BSAP 6040 devices could intermittently lose connectivity with vWLAN.
- BSAP-6519 Fixed an issue in which BSAP 6040 devices failed to allow clients to quickly roam.
- BSAP-6518 Fixed an issue in which, when using a large number of locations (50 or more), clients could connect to BSAP 6040 devices before all locations were updated.
- BSAP-6516 Fixed an issue in which some BSAP 6040 devices would frequently reset their radios when configured to use **Continuous DynamicRF** mode.
- BSAP-6510 Fixed an issue in which the **802.11ax Radio State** parameter was not included in the CLI menu.

# 9. Errata

The following is a list of errata that still exist in vWLAN 4.2.1.

- BSAP-6513 BSAP 6040 devices will incorrectly block traffic if an **allow** rule matches any **deny** rule's IP/Subnet, regardless of whether the **allow** rule is listed first. For example, if we **allow** UDP 53 at the top of the firewall rules to **any** IP, with a DNS server that has an IP of 172.16.8.1, and then we **deny** anything to the subnet (172.0.0.0/8) at the bottom of the firewall rules, DNS traffic will be blocked as the IP address falls within the subnet being blocked. **Workaround:** Allow the traffic needed. There is an implicit deny rule for all other traffic not listed in the firewall rules.
- VW-14933 **Status** > **Logs** can fill the disk over time. **Workaround**: Periodically clear logs using the **Purge All Alarms and Logs** option for both domains and the vWLAN platform.
- VW-15135 After a fail-over event, MPSK clients will show an IP of **0.0.0.0** on the **Client Status Page**. Clients will still be able to connect without issue.
- VW-15132 An emailed **Dashboard** report may contain the old Adtran logo.
- VW-15121 In some cases, when upgrading a high-availability synced vWLAN pair to 4.2.1, APs can become stuck in the **Upgrading** state. **Workaround:** Restart vWLAN (navigate to **Administration** > **Restart** > **Restart vWLAN**). After a restart, all APs should then begin upgrading to the 4.2.1 image.
- VW-15086 In some cases, MacOS clients will not transition to new locations and obtain new IP addresses when using location groups.
- VW-15039 The **Wireless IDS Alerts** page in the GUI may fail to load when a large number of alerts are present.
- VW-15038 In some cases, SNMP may restart frequently.
- VW-14966 Branding images cannot contain spaces in the filename while being uploaded.
- VW-14879 Background scans will also be executed on the failover server which results in a UI error on the failover server. **Note:** The job will work as expected on the master node.
- VW-14874 APs that are on static channels may report neighboring APs on incorrect channels.
- VW-14845 The **User Name** column is missing the **Top Clients by Usage Over Time** scheduled report.
- VW-14784 Unified Access does not function properly due to DNS being blocked during web redirection.
- VW-14745 vWLAN jobs cannot be scheduled less than 6 hours in the future.
- VW-14681 Uploading a backup file with numerous old firmware versions may fail. **Workaround:** Before making a backup, delete all old unused firmware versions.
- VW-14507 AP jobs cannot be scheduled for APs with pending firmware upgrades.
- VW-14227 If you restrict all available channels except one, and then run a background scan, APs may choose to use a restricted channel.
- VW-14122 If a secondary server is converted to a standalone server, APs will display a DOWN state in the vWLAN GUI.
- VW-14112 The SNMP trap OID and TRAPOID number values are the same for everything.
- VW-14054 Continuous re-indexing of the vWLAN GUI can cause system instability in large scale deployments.
- VW-13995 The BSAP 3040 will not properly function in 80+80 MHz mode in non-DFS certified and configured deployments.
- VW-13897 The Max EIRP for Canada does not scale up to ISED allowed total limits.

- VW-13846/ VW-13530 Uploading a license for an AP that already exists, but is currently licensed with another country code, will fail. **Workaround:** Delete the AP license before uploading another.
- VW-13705 Creating mesh links between APs of a different type (or series) will cause sluggishness in the connection speeds between the APs. **This configuration is not recommended or supported.**
- VW-13641 When a role schedule is initiated to remove a role, currently authenticated clients in vWLAN may still display as authenticated in the vWLAN GUI, even though they are properly denied access.
- VW-13610 DynamicRF suggests **Channel 0** if all channels available to a particular AP model are excluded in the AP template.
- VW-13576 Specifying a MAC address that is all uppercase, while taking a traffic capture on an AP, causes the traffic capture to fail to start.
- VW-13548 By default, outdoor APs are set to **Indoor** in the **AP Details** menu. **Workaround**: In the vWLAN GUI, navigate to the **Status** > **APs** menu, select the particular AP, and change this setting back to **Outdoor**.
- VW-13515 In an extremely crowded RF environment (for example, APs with over 100 adjacencies), the DynamicRF channel algorithm may not pick the channel with the least interference.
- VW-13491 In rare cases, a DynamicRF change suggestion may fail to display a message on the **Status** > **APs** menu in the vWLAN GUI, but will be applied when accepting DynamicRF suggestions.
- VW-13489 The current channel being scanned by DynamicRF is not displayed in the **AP Status** menu.
- VW-13480 After performing a channel scan, the AP adjacency information produced by the AP performing the channel scan displays as all zeros.
- VW-13479 Adjacent APs running in 80 MHz mode are shown as running in 40 MHz mode in the vWLAN **Adjacent AP** GUI menu.
- VW-13184 The **Select All** button only selects the first 100 entries in vWLAN GUI tables.
- VW-12484 **Over Time** dashboard widgets can cease to display the latest data point available.
- VW-12353 When configuring custom language login forms, vWLAN may display invalid characters for some languages. When this occurs, instead of displaying the valid character, the browser displays **?**.
- VW-12330 If invalid entries are made when configuring the LDAP server, a valid error message might not be sent to the administrator.
- VW-12220 The administrative feature of downloading vWLAN dashboard widgets in **JPEG** formats does not function.
- VW-12149 Uploading the same AP firmware file twice in the vWLAN GUI results in the inability to choose a different firmware file from the drop-down menu. **Workaround:** Navigate away from the menu page and then navigate back again.
- VW-10881 In some cases, packet captures taken from the vWLAN GUI can miss packets. Adtran recommends to take multiple packet captures when attempting to diagnose an issue.
- VW-10261 When using the **Drop User** function, Apple MacBooks running OS X will retain a previously held IP address unless the timeout threshold is reached, causing web redirection via 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.
- VW-9350 Some customized login forms do not allow for full customization of the page. Instead, the page displays the same even if **Enable Complete Customization** is selected.
- VW-9349 When using a Google Chromebook on a captive portal, users are not automatically redirected to their final destination. However, manually refreshing the page or going to another page functions as expected and can redirect the user.

- VW-9213 The intended behavior of Hypertext Strict Transport Security (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 (for example, https://www.adtran.com), a certificate warning is returned that cannot be ignored or bypassed. Refer to http://caniuse.com #feat=stricttransportsecurity to determine which browsers support HSTS.
- VW-9129 The platform **NTP Server** setting does not return errors when invalid values are entered for its host name.
- VW-9089 The vWLAN high availability feature is not replicating **Hot Spot** login forms correctly.
- VW-8941 Some pages in the vWLAN GUI do not fully function when using Internet Explorer version 9. **Workaround:** Use a different browser, upgrade to a newer version of IE, or use the API.
- VW-8932 After executing any restart from the vWLAN GUI, the GUI page must be refreshed manually.
- VW-8893 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. The creator of the scheduled job must remove the job before the email configuration can be deleted.
- VW-8753 If an AP is manually edited, and a non-native location is selected for the **Location** field, the AP may not discover locations correctly.
- VW-8395 Using captive portal in the Catalan, German, Swedish, or Portuguese languages may display special characters instead of some letters.
- VW-8244 APs configured for **Mesh** mode can not perform an AP traffic capture.
- VW-5493 The API may become unresponsive if used from multiple sources simultaneously. It will become responsive again after a few minutes.
- VW-5034 When upgrading a large database (with many historical records and/or domains), the vWLAN system can take up to an hour to come up after the upgrade. **Workaround:** Implement high availability or specify a high control channel timeout value.
- VW-4744 While under heavy load, the GUI may report incorrect status information or it may sort the information improperly. The system will recover after a few minutes.
- VW-4180 Login form previews do not function properly when using the Opera browser.
- VW-2600 For the fast-roaming feature to function, 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.
- BSAP-6498 RADIUS authentication may fail when a Tunnel-Private-ID group is returned when using RADIUS from a Windows server.
- BSAP-6375 Wired packet capture on a BSAP 3040 will intermittently fail if the protocol is set to **Any**.
- BSAP-6227 Sending a configuration push to 1900 series APs will cause the AP to reboot if clients are connected.
- BSAP-6191 When more than one 5GHz channel is configured on a BSAP 203X series AP, it will fail to scan all AP adjacencies, which could cause DynamicRF to select a channel or power setting that is less than ideal.
- BSAP-6137 Due to a change in Samsung Galaxy mobile device behavior, any Samsung Galaxy phones using Android 9.0 or later may not reconnect to a captive portal network automatically after being de-authenticated as part of the transition process to the final role. **Workaround**: Create a new role, select the **Un-Registered** role type, and then select the same location in which users will be placed after authentication. Push this change out to the APs (the role will not be connected to any SSID as it is a dummy role). The phones will automatically reconnect after this change.

- BSAP-6002 An AP may operate on restricted channels if the AP radio is set to a channel width that requires more channels than are currently available as unrestricted, depending on the channel-restrictions set by the administrator.
- BSAP-5923 Changing the channel width when a Windows client is connected will result in a one-time AP reboot.
- BSAP-5059 In some cases, the 2.4GHz radio can be limited to only 124 client associations, even though the 5.0GHz radio operates normally.
- BSAP-2997 When starting a wireless packet capture, the capture cannot be properly stopped or deleted within the first **30** seconds or the AP may become stuck in traffic capture mode until a subsequent reboot. If a domain task appears after a packet capture, it indicates the AP never fully recovered after the packet capture and a new configuration must be applied to the AP, or a manual AP reboot must be performed, to recover the AP.
- BSAP-2308 If more than **86** users are associated with a particular AP, and a fail-over occurs, the associated users will not appear immediately in the secondary vWLAN GUI.
- The following APs have had their hardware revision updated, and require firmware version 3.3.0 or later to function:
  - BSAP 304X Revision F
  - BSAP 2020 Revision C
  - BSAP 203X Revision R
  - BSAP 2135 Revision D

  The hardware revision can be found on the label on the box and on the physical AP. APs may ship with version 3.2.1 by default. These APs must be upgraded to version 3.3.0 or later for them to function properly. Attempting to downgrade them to versions prior to 3.3.0 will present an error message.

# 10.Warranty and Contact Information

Warranty information can be found online by visiting www.adtran.com/warranty-terms.

To contact Adtran, choose one of the following methods:

| Department | Contact Information | |
|---|---|---|
| **Customer Care** | From within the U.S.:<br>From outside the U.S.: | (888) 4ADTRAN ((888)-423-8726)<br>+1 (256) 963-8716 |
| **Technical Support** | Support Community:<br>Product Support: | www.supportcommunity.adtran.com<br>www.adtran.com/support |
| **Training** | Email:<br>Adtran University: | training@adtran.com<br>www.adtran.com/training |
| **Sales** | For pricing and availability: | 1 (800) 827-0807 |