Adtran

vWLAN & BSAP

4.2.3 Release Notes

Release Notes

6ABSRNR423-40A

October 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

Table of Contents

1. Introduction

The 4.2.3 firmware release for Adtran's vWLAN is a maintenance release that addresses customer issues that were uncovered in previous code releases. This release consists of an AP build (4.2.3) for the BSAP 6000 Series, and a vWLAN patch that is installed on top of vWLAN 4.2.1.

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 the 4.2.3 AP build associated with vWLAN version 4.2.1.

Table 1. Supported Platforms

BSAP Platform
BSAP 6020
BSAP 6040
BSAP 6120

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 Yet Not Supported on BSAP 6000 Series

Feature
Dynamic RF (Set Once and Hold)
DMO/MRO/Convert Multicast/Broadcast to Unicast
802.11r

Table 2. Legacy Features Yet Not Supported on BSAP 6000 Series (Continued)

Feature
CoS/QoS in User Role
DFS
Mesh Networking

3. Required BSAP Firmware

The 4.2.3 AP build is not packaged with vWLAN. This is a stand-alone build that works in conjunction with vWLAN 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

For the 4.2.3 AP build to function correctly with vWLAN running 4.2.1, two steps are required for the AP upgrade. First, the vWLAN patch must be installed on the vWLAN instance, and second, the 4.2.3 AP firmware must be uploaded to vWLAN and applied to the 6000 Series APs.

Step 1: Install the vWLAN Patch

To install the vWLAN patch on the vWLAN instance running 4.2.1, follow these steps:

> **NOTE**
>
> *This step must be completed before attempting to install the AP build or upgrade the APs.*

1. Verify if any patches are currently installed in the vWLAN instance by navigating to **Administration** > **Patch** in the vWLAN GUI. If **Package name: 4.2.1-p01, Version: 4.2.1-678053** is listed, select the radio button next to the patch and then select **Uninstall**. The fix originally addressed with this patch is included in the newer patch. No Platform or Domain task is required to complete this process.
2. Download the 4.2.1-p08 patch from the vWLAN Current Feature Release Patches space in the Adtran Support Community.
3. Once the 4.2.1-p01 patch is removed, or if it was not installed, and you have downloaded the 4.2.1-p08 patch, navigate to the **Administration** tab in the vWLAN GUI and select **Patch** > **Browse** > **Install**. Install the 4.2.1-p08 patch as prompted. No restart is required after the patch installation.

> **NOTE**
>
> *Patch installations may result in a **sudo: unable to resolve host** error message. These installation error messages can be safely ignored.*

Step 2: Upload the AP Firmware and Upgrade the BSAP 6000s

To upgrade the BSAP 6000 Series APs, follow these steps:

> **NOTE**
>
> ***ONLY** the BSAP 6000 devices should upgraded with this patch.*

1.Upload the 4.2.3 AP firmware for the BSAP 6000s to the vWLAN instance.
2. In the vWLAN GUI, navigate to the **Configuration** tab, and then to **Wireless** > **AP Firmware** > **Platform**. Select the **Create AP Firmware** option at the bottom of the menu, and then **Browse** to find the 4.2.3 AP firmware in the list.
3. Once the 4.2.3 firmware is located, select **All Domains**, and from the drop-down menu select **Apply this Firmware to all templates**. Then select **Create AP Firmware** to install the firmware and prepare for installation on the APs. Once selected, a **Domain Task** is generated. Repeat this process for all models of the 6000 Series APs.
4. To finalize the upgrade, select the **Domain Task** option at the top right of the GUI, and then execute the **Must apply configuration to APs** task. Once you receive a notification that the task has been completed, the AP installation and upgrade procedure is complete. Repeat this process for each Domain.

7. Features and Enhancements

This section highlights features or enhancements introduced in the 4.2.3 AP build associated with vWLAN 4.2.1.

- AD-260564 Added support for the BSAP 6020 to choose a non-interfering channel while the AP is booting. This channel selection algorithm allows the AP to choose a channel while in the booting process, independently of the DynamicRF feature, thus avoiding interfering with other channels or active clients when the AP is initialized.
- AD-222219 Added support for Layer 3 Mobility in the BSAP 6000 Series.
- AD-209803 Added support for Captive Portal with NAC in the BSAP 6000 Series.

8. Fixes

This section highlights major bug fixes in the 4.2.3 AP build associated with vWLAN 4.2.1.

- VW-15206 Fixed an issue in which the firewall rules in the Un-Registered Role could not be edited or deleted.
- VW-15204 Fixed an issue in which the BSAP 6040 devices incorrectly broadcast SSIDs even when they were configured as non-broadcast SSIDs.
- BSAP-6637 Fixed an issue where BSAP 6000 Series APs could reboot when Layer 3 mobility was enabled.
- BSAP-6632 Fixed an issue in which the BSAP 6000 Series APs would not allow RADIUS or PSK clients to connect when a particular RADIUS Request was observed.
- BSAP-6631 Fixed an issue in which the BSAP 6000 Series APs would continually reboot when moved to an AP template using **Mesh Mode**. Mesh Mode is not yet supported in the 6000 Series APs.
- BSAP-6612 Fixed an issue in which the walled-garden captive portal feature was not functioning correctly.
- BSAP-6600 Fixed an issue in which the BSAP 6040 devices failed to discover vWLAN via a DNS A record.
- BSAP-6599/ BSAP-6596 Fixed an issue in which the BSAP 6040 devices could fail to upgrade and become stuck in the Upgrading state.
- BSAP-6597 Fixed an issue in which the BSAP 6040 devices would incorrectly block all traffic unless a rule with the **Allow All**, **Any**, and **Both Ways** settings specified was appended at the end of the firewall rules.
- BSAP-6595 Fixed an issue in which the BSAP 6040 devices could block DNS connections when a walled garden role with specific firewall rules was employed.
- BSAP-6566 Fixed an issue in which the BSAP 6040 devices could lose their vWLAN address upon an AP upgrade.
- BSAP-6527 Fixed an issue in which the BSAP 6040 devices could change their discovery mode from **Static** to **Auto** following a software upgrade or downgrade.
- BSAP-6513 Fixed an issue in which BSAP 6040 devices could incorrectly block traffic if an **allow** rule matched any **deny** rule's IP/Subnet, regardless of whether the **allow** rule was listed first.

9. Errata

The following is a list of errata that still exist in the 4.2.3 AP build associated with vWLAN 4.2.1.

- 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=strictttransportsecurity to determine which browsers support HSTS.
- VW-9089 The vWLAN high availability feature is not replicating **Hot Spot** login forms correctly.
- 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-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-15205 In some cases, high availability may become out of sync following a domain name change.
- VW-15185 The BSAP 6040 devices do not yet support Layer 3 mobility. **Workaround:** Create a new AP template for the 6040 devices with disabled L3 mobility.
- VW-15171 **Dashboard Reports** may fail to email if the **Report Logo** size is too large.
- 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-15011 When upgrading 1,000 APs or more, they may display a **Down** state after upgrading until vWLAN is rebooted.
- VW-14966 Branding images cannot contain spaces in the filename while being uploaded.
- 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-14925 In some cases, Device Fingerprinting may fail to fingerprint new devices.
- 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-14112 The SNMP trap OID and TRAPOID number values are the same for everything.
- 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-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-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-13479 Adjacent APs running in 80 MHz mode are shown as running in 40 MHz mode in the vWLAN **Adjacent AP** GUI menu.
- 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-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.
- BSAP-6644 Whenever the vWLAN controller pushes configurations to the 6020 Series AP, the AP triggers the automatic channel selection algorithm and selects the best available channel, regardless of the configuration.

- BSAP-6602 APs may not auto-fallback to the high availability master after a failover event.
- BSAP-6579 Error messages associated with the **command timeout**, **retry,** or **reboot bsap** commands may be incorrectly displayed.
- BSAP-6572 BSAP 6040 APs may reset their radios when using **Continuous DynamicRF** mode, which is indicated in the vWLAN logs as **ap service VAP(s) ath1, ath2, ath3 Reset by autorecovd**.
- BSAP-6498 RADIUS authentication may fail when a Tunnel-Private-ID group is returned when using RADIUS from a Windows server.
- 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-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.: From outside the U.S.:	(888) 4ADTRAN ((888)-423-8726) +1 (256) 963-8716
Technical Support	Support Community: Product Support:	www.supportcommunity.adtran.com www.adtran.com/support
Training	Email: Adtran University:	training@adtran.com www.adtran.com/training
Sales	For pricing and availability:	1 (800) 827-0807