vWLAN & BSAP

3.7.1 Release Notes

Release Notes

6ABSRNR371-40A

July 2021

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.

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

Table of Contents

1. Introduction

The 3.7.1 firmware release for ADTRAN's vWLAN is a major system release that addresses several security updates and 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 6*.

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*.

NOTE

Several security upgrades are included in the vWLAN 3.7.1 release. ADTRAN recommends that you upgrade all vWLAN and BSAP instances within your network to the 3.7.1 release as soon as possible to take advantage of these security updates.

2. Supported Platforms

The following models are supported in the vWLAN 3.7.1 release:

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

NOTE

The 3.7.1 release is not supported on any previous Bluesocket Appliances. Customers still using Bluesocket Appliances should upgrade to a Virtual Appliance.

The following Bluesocket Access Point (BSAP) models are supported in vWLAN 3.7.1:

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

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.

3. Required BSAP Firmware

Due to BSAP and vWLAN firmware versions being mutually exclusive, the associated version of BSAP firmware for vWLAN 3.7.1 is version 3.7.1.

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 3.7.1.

- 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.
- 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.
- 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.

6. Fixes

This section highlights major bug fixes in vWLAN 3.7.1.

- Fixed several security issues, including kernel upgrades and other vulnerabilities, as outlined in the *ADTSA-2021003: Multiple Bluesocket Vulnerabilities* security advisory (available online from the *ADTRAN Security Advisory page* of the ADTRAN Support Community).

- Fixed an issue in which LAN profiles could not be configured correctly.
- Fixed an issue in which interim updates were intermittently failing to send.

7. Errata

The following is a list of errata that still exist in vWLAN 3.7.1.

- Unified Access does not function properly due to DNS being blocked during web redirection.
- 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.
- vWLAN jobs can not be scheduled less than 6 hours in the future.
- Some APs may become stuck in an upgrading state while upgrading new firmware. **Workaround:** Navigate to the **Configuration** > **AP License** menu, select the AP(s) from the list, and then reboot them.
- Uploading a backup file with numerous old firmware versions may fail. **Workaround:** Before making a backup, delete all old unused firmware versions.
- Using the CSV to download device information from a widget will only download the top 10 entries, even if more are shown.
- If the shared secret for RADIUS MAC authentication is too long (64 characters), authentication will fail.
- AP jobs cannot be scheduled for APs with pending firmware upgrades.
- DynamicRF is not reducing TX power to the minimum setting after a background scan in cases where it should. **Workaround:** Use the **Continuous** DynamicRF mode with client-aware **AP/ Sensor** mode to adjust the power properly.
- The **Client Status** GUI page may contain inaccurate information on heavily loaded servers; however, the indexing will catch up over time.
- If you restrict all available channels except one, and then run a background scan, APs may choose to use a restricted channel.
- If a secondary server is converted to a standalone server, APs will display a DOWN state in the vWLAN GUI.
- The SNMP trap OID and TRAPOID number values are the same for everything.
- Continuous re-indexing of the vWLAN GUI can cause system instability in large scale deployments.
- The BSAP 3040 will not properly function in 80+80 MHz mode in non-DFS certified and configured deployments.
- The Max EIRP for Canada does not scale up to ISED allowed total limits.
- 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.
- 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.**
- 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.

- DynamicRF suggests **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 a traffic capture on an AP, causes the traffic capture to fail to start.
- 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**.
- 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.
- 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.
- The current channel being scanned by DynamicRF is not displayed in the **AP Status** menu.
- After performing a channel scan, the AP adjacency information produced by the AP performing the channel scan displays as all zeros.
- Adjacent APs running in 80 MHz mode are shown as running in 40 MHz mode in the vWLAN **Adjacent AP** GUI menu.
- The **Select All** button only selects the first 100 entries in vWLAN GUI tables.
- **Over Time** dashboard widgets can cease to display the latest data point available.
- 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 **?**.
- If invalid entries are made when configuring the LDAP server, a valid error message might not be sent to the administrator.
- The **Timeout Weight** setting should be a required field in the LDAP server configuration and will automatically default to **1** if it is left blank upon initial server configuration.
- The administrative feature of downloading vWLAN dashboard widgets in **JPEG** formats does not function.
- 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.
- In some cases, vWLAN's self-signed certificate is regenerated when the system reboots, and the certificate must be saved again. **Workaround**: Upload a custom certificate verified by a CA.
- The **Client Count** displayed in the **Domain Status** page of the vWLAN GUI is inaccurate and out-of-sync in a large system with multiple roaming clients. Even after multiple refresh cycles, the **Client Count** displayed at the top and bottom of the **Domain Status** menu do not match.
- 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.
- When attempting to execute a packet capture from the vWLAN GUI on an AP that is in a DOWN state, the packet capture behaves as expected (does not begin), but the GUI will not display an error.
- After upgrading the vWLAN instance, some GUI pages may not load correctly due to the 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, 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.
- 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.
- 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.
- 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.
- The platform **NTP Server** setting does not return errors when invalid values are entered for its host name.
- The vWLAN high availability feature is not replicating **Hot Spot** login forms correctly.
- If a user connects to a WPA Enterprise SSID, and 802.1X authentication fails, the user is given the **Unregistered** role regardless of the SSID's configured default role.
- 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.
- After executing any restart from the vWLAN GUI, the GUI 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. The creator of the scheduled job must remove the job before the email configuration can be deleted.
- If an AP is manually edited, and a non-native location is selected for the **Location** field, the AP may not discover locations correctly.
- Using captive portal in the Catalan, German, Swedish, or Portuguese languages may display special characters instead of some letters.
- APs configured for **Mesh** mode can not perform 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 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.
- 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.
- Login form previews do not function properly when using the Opera browser.
- 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.

- Sending a configuration push to 1900 series APs will cause the AP to reboot if clients are connected.
- 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.
- 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.
- Changing the channel width when a Windows client is connected will result in a one-time AP reboot.
- In some cases, the 2.4GHz radio can be limited to only 124 client associations, even though the 5.0GHz radio operates normally.
- The vWLAN GUI will allow configuration of more than **1024** schedules; however, configuring more than 1024 schedules can cause the AP to reboot.
- 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.
- 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 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.
- Using SNMP on vWLAN can cause the server's memory to be heavily utilized.

8. 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 3.7.1 if it is currently on version 2.8.0 or greater. vWLANs on versions 2.2.1 to 2.6.1 must first upgrade to version 2.6.2, then upgrade to version 2.8.0, and then upgrade to version 3.7.1. AP firmware does not have to be upgraded to 2.6.2 and can instead be upgraded directly to 3.7.1 with the third upgrade.

If you attempt to upgrade from a version prior to 2.8.0 to 3.7.1, the upgrade will error out and the following message will appear in the upgrade alerts and platform alerts:

*** MUST BE RUNNING 2.8.0 TO UPGRADE TO THIS IMAGE! *** (Please upgrade to 2.8.0 prior to loading this image.)

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 3.7.1 requires using BSAP firmware version 3.7.1. BSAP 3.7.1 is not backward-compatible with previous vWLAN code versions.

NOTE

vWLAN systems running 2.3.X or earlier cannot be upgraded. Instead, a new system should be deployed with 3.7.1 and configuration parameters from the 2.3.X system should be manually ported to the 3.7.1 system. Attempting to upgrade a 2.3.X system could cause some vWLAN configuration parameters to be lost.

9. Warranty and Contact Information

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

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