vWLAN & BSAP

3.6.0 Release Notes

Release Notes

To the Holder of this Document

This document is intended for the use of ADTRAN customers only for the purposes of the agreement under which the document is submitted, and no part of it may be used, reproduced, modified or transmitted in any form or means without the prior written permission of ADTRAN.

The contents of this document are current as of the date of publication and are subject to change without 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.

Table of Contents

1. Introduction

The 3.6.0 firmware release for ADTRAN's vWLAN is a major system release that adds new features and 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 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*.

2. Supported Platforms

The following models are supported in vWLAN 3.6.0:

- vWLAN Rackmount Appliance (1700900F2)
- vWLAN Virtual Appliance for VMware ESX/ESXi, 5.X, and 6.X.

The following Bluesocket Access Point (BSAP) models are supported in vWLAN 3.6.0:

- 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 3.6.0 is version 3.6.0.

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 int he 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

Upgrade from Previous vWLAN Release to 3.6.0

When upgrading directly from 3.5.0 (or earlier build) to 3.6.0, vWLAN supports 50 domains/ 1400APs/ 22K clients.

Support for 150 domains on a single vWLAN instance is achieved by deploying a new VM with the 3.6.0 OVA file.

> 🛈 **NOTE**
>
> *vWLAN 3.6.0 does not accept the 3.5.0 version backup file.*

The following steps will allow support for 150 domains while maintaining previous configurations:

1. Upgrade from 3.5.0 (or earlier release) to 3.6.0
2. Create a complete vWLAN backup file from 3.6.0
3. Deploy a new 3.6.0 OVA file on another VM (for example, VM-2)
4. Restore the backup file from Step 2 onto the new VM-2

General

The following information applies to systems running vWLAN 3.6.0.

- 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. Features and Enhancements

This section highlights major features and enhancements in vWLAN 3.6.0.

- Added support for up to 150 domains, 2048 APs, and 32,000 Clients.

7. Fixes

This section highlights major bug fixes in vWLAN 3.6.0.

- Fixed an issue in which changing the Dynamic RF profile settings caused the AP template Radio Mode to revert from AP/Sensor Client Aware Mode to AP/Sensor Mode.
- Fixed an issued in which the Ethernet Bridge option on a mesh point was not saved in a domain backup properly.
- Fixed an issue in which firewall rules were sometimes automatically created in a role.
- Fixed an issue in which the client count in the vWLAN GUI was incorrect in some cases.
- Fixed an issue in which setting the IP address of an external 1X Auth Server to 0.0.0.0 would prevent clients from connecting to the AP.
- Fixed an issue in which TLS 1.0 and 1.1 were not disabled by default in the Captive Portal and Administrative vWLAN UI. A toggle exists to turn both protocols back on, if needed.
- Fixed an issue in which administrator scope IDs were not included in the GET administrator API output.

8. Errata

The following is a list of errata that still exist in vWLAN 3.6.0.

- 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:** Go to the **Configuration->AP License** page, select the AP, and reboot them.
- Uploading a backup file with numerous old firmware versions may fail. **Workaround:** Before making a backup, delete all old unused firmware.
- 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 Job cannot be scheduled for APs with pending Firmware Upgrades.
- DynamicRF is not reducing TX power to minimum setting after background scan in cases where it should. **Workaround:** Use Continuous DynamicRF mode with client-aware AP/Sensor mode to adjust power properly.
- Client Status Page may contain inaccurate information on heavily loaded servers. The indexing will catch up over time.

- If you restrict all available channels save 1 and then run a background scan, the APs may choose a restricted channel.

- If a secondary server is converted to a standalone, APs will show down in the GUI.

- The SNMP Trap OID and TRAPOID number values are the same for everything.

- Continuous re-indexing of the vWLAN UI is causing 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.

- After clearing adjacent APs, BSAP 18XXs will not scan adjacencies again until they have been rebooted.

- Creating Mesh links between APs of a different type or series will cause sluggishness in the connection speeds. This is not recommended or supported.

- When a role schedule is initiated to remove a role, currently authenticated clients in vWLAN may still show as authenticated in the vWLAN GUI 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.

- 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.

- In an extremely crowded RF environment (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 but 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 80Mhz mode are shown in vWLAN's Adjacent AP page as 40Mhz.

- 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.

- The **Select All** button only selects the first 100 entries in the table in the GUI.

- Over time dashboard widgets cease to display the latest data point available.

- When configuring custom language login forms, vWLAN may display invalid characters for some 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 some cases, vWLAN's self-signed certificate is regenerated when the system reboots and the certificate must be re-saved. **Workaround**: Upload a custom certificate verified by a CA

- 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 GUI page on the Domain status page and the client count at the bottom of the GUI page do not match - even after multiple refresh cycles.

- Packet captures taken from the vWLAN UI often miss packets. In a lab environment during captive portal authentication with a RADIUS Web Server, 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.

- The platform NTP server setting did not return errors when invalid values were entered for its hostname.

- 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 using 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 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 system can take up to an hour to come up after the upgrade. **Workaround:** Implement HA or a high Control Channel timeout.

- 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.

- 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.

- 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.

- If using web authentication and the NAC, Samsung Galaxy phones running Android 9 will dissociate from the SSID when they receive the DHCP NAK and will not re-associate until the user manually selects the SSID. **Workaround**: Create a new role, select the **Un-registered** role type, and select the same location users are placed after authentication. Push the change to the AP.

- If an AP radio is set to a channel width that requires more channels than the are currently unrestricted according to the channel-restrictions set by the administrator, the AP may operate on restricted channels.

- Changing the channel width when a windows client is connected will result in a one time AP reboot.

- The 2.4GHz radio may only have 124 client associations, but the 5.0GHz radio operates normally.

- Only 52 clients can associate to a BSAP 1800, even though vWLAN indicates a 64 client limit.

- BSAP 1800s may run low on memory causing sporadic client and AP activity, or even a loss of connection with vWLAN requiring a manual hard reset before operation can resume.

- Wireless packet captures may not function properly on the 5GHz radio of a BSAP 1800 series AP.

- The UI will allow configuration of greater than 1024 schedules. Configuring greater than 1024 schedules can result in AP reboots.

- BSAP 1800 version 2 may use the incorrect Power Save Mode for clients resulting in missing packets and dropped connections.

- When starting a wireless packet capture, take care to allow the capture to begin before taking an action on it. If the capture must be stopped, wait at least 30 seconds to let the capture fully start. If a domain task pop-up is seen after a capture, it means the AP never fully recovered after the capture. Apply configuration to or reboot the AP to recover it.

- If greater than 86 users are associated with an AP and a failover occurs, the users 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.

- Utilizing SNMP on vWLAN can cause the server's memory to be heavily utilized.

9. 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 3.6.0 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 3.6.0. AP firmware does not have to be upgraded to 2.6.2 and can instead be upgraded directly to 3.6.0 with the second upgrade.

If you attempt to upgrade from a version prior to 2.6.2 to 3.6.0, 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, refer to the *Upgrading Bluesocket vWLAN Controllers and APs* guide available online at https://supportcommunity.adtran.com.

i	**NOTE**
	vWLAN 3.6.0 requires using BSAP firmware version 3.6.0. BSAP 3.6.0 is not backward-compatible with previous vWLAN code versions.

i	**NOTE**
	vWLAN systems running 2.3.X or earlier cannot be upgraded. Instead, a new system should be deployed with 3.6.0 and configuration parameters from the 2.3.X system should be manually ported to the 3.6.0 system. Attempting to upgrade a 2.3.X system could cause some vWLAN configuration parameters to be lost.

10.Warranty and Contact Information

Warranty and contact information for all ADTRAN products can be obtained using the information in the following sections.

Warranty

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

Contact Information

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