Adtran

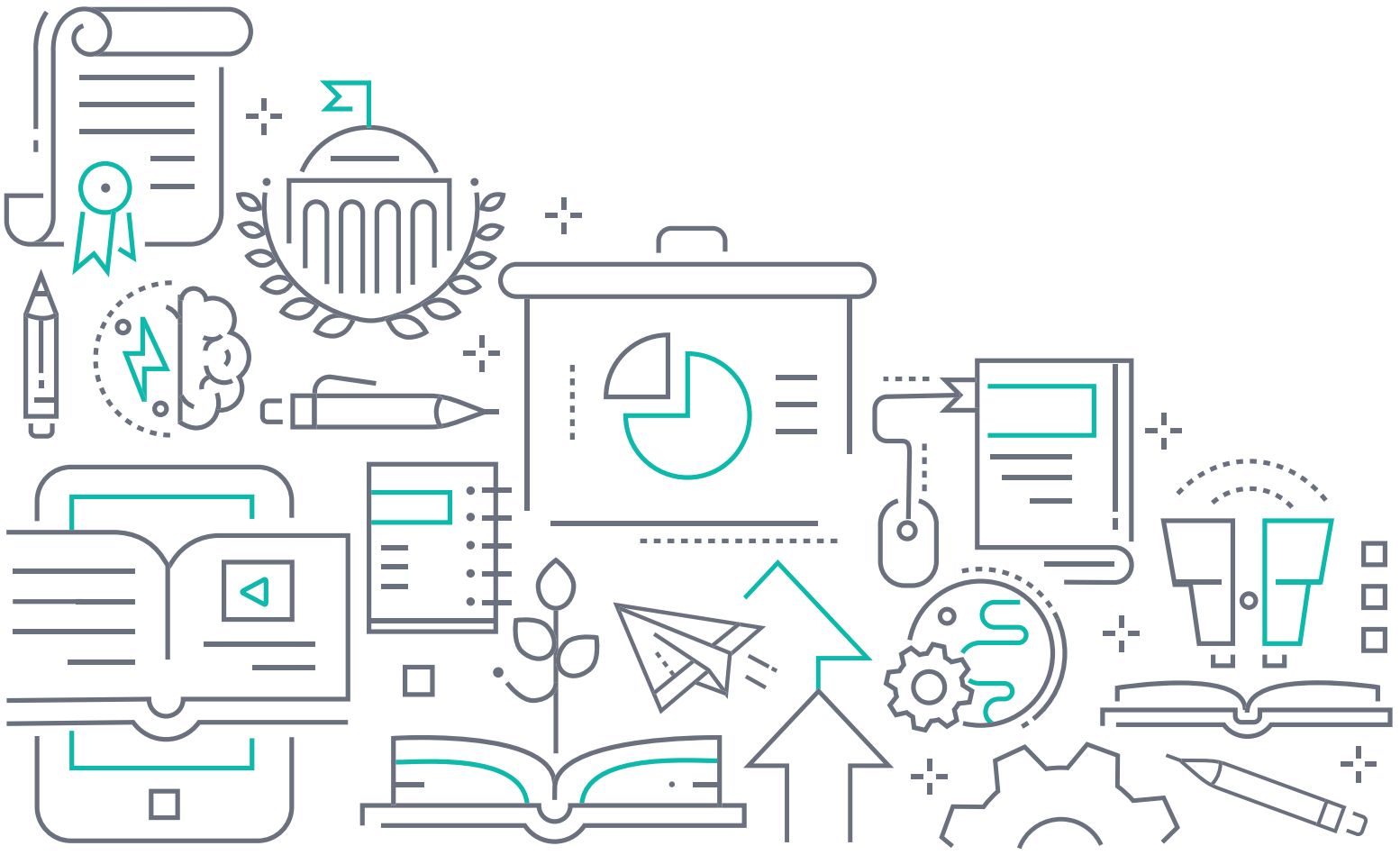
vWLAN & BSAP

4.1.0 Release Notes

Release Notes

6ABSRNR410-40B

April 2022



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 4.1.0 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 7*.

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 4.1.0 release:

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

NOTE

The 4.1.0 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 4.1.0.

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
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.

3. Required BSAP Firmware

Due to BSAP and vWLAN firmware versions being mutually exclusive, the associated version of BSAP firmware for vWLAN 4.1.0 is version 4.1.0.

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 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 4.1.0.

- 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.

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 4.1.0 if it is currently on version 3.7.1 or greater with the 4.1 Pre-Upgrade patch installed. Upgrade steps must occur in the following order:

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 to 3.7.0 must then upgrade to version 3.7.1.

4. Once vWLAN is upgraded to version 3.7.1, a patch must be installed (4.1 Pre-Upgrade patch)

> **NOTE**
>
> *The Pre-Upgrade patch for 4.1.0 requires 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 to version 4.1.0.

> **NOTE**
>
> *AP firmware does not have to be upgraded to 2.6.2 and can instead be upgraded directly to 4.1.0 with the fifth upgrade.*

If you attempt to upgrade from a version prior to 2.8.0 to 4.1.0, 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 4.1.0 and later requires using BSAP firmware version 4.1.0 or later. BSAP 4.1.0 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 4.1.0 and configuration parameters from the 2.3.X system should be manually ported to the 4.1.0 system. Attempting to upgrade a 2.3.X system could cause some vWLAN configuration parameters to be lost.*

7. Features and Enhancements

This section highlights the major features and enhancements in vWLAN 4.1.0:

- AD-195377 Added software support for the new WiFi-6 BSAP 6000 Series APs. Hardware is not yet available.

8. Fixes

This section highlights major bug fixes in vWLAN 4.1.0.

- VW-14873 Fixed an issue in which the **Status** table was missing associated **AP Names** for clients.
- VW-14872 Fixed an issue in which pre-configured multikey roles would cause upgrade failures.

- VW-14867 Fixed an issue in which the user manager process would restart under high load.
- VW-14864 Fixed an issue in which SSL certifications changes required a vWLAN restart to take effect.
- VW-14862 Fixed an issue where vWLAN would falsely report "UpdateMd5sum failed: Command Timeout".
- VW-14848 Fixed an issue in which large amounts of **Adjacent APs** data was causing high CPU usage.
- VW-14841 Fixed an issue in which APs would get stuck in the **Updating** status.
- VW-14836 Fixed an issue in which APs would remain in the **Unknown** state after a vWLAN upgrade until the system was rebooted.
- VW-14774 Fixed an issue in which scheduled email reports would only include the first dashboard tab when multiple tabs were configured.
- VW-14773 Fixed an issue with SSH security vulnerability.
- VW-14763 Fixed an issue in which interim updates were intermittently failing to send.
- VW-14755 Fixed an issue in which gathered user logs in large deployments could fill the disk.
- VW-14543 Fixed an issue in which, if the shared secret for RADIUS MAC Authentication is too long (64 characters), authentication would fail.
- VW-14501 Fixed an issue in which guest users could not be deleted if the administrator that created the users was deleted.
- BSAP-6336 Fixed an issue where Layer3 Mobility was always enabled, even when toggled off in the GUI.
- BSAP-6334 Fixed an issue in which Windows 10 device types were displayed as **Unknown**.
- BSAP-6284 Fixed an issue in which APs would get stuck in the **Updating** status.
- BSAP-6240 Fixed an issue in which site survey configuration in the BSAP CLI displayed the **Transmit Power** statistics incorrectly.
- BSAP-6233 Fixed an issue in which APs would get stuck in an **Updating** status until manually rebooted if any changes to **AP Role** configurations were made.
- BSAP-6122 Fixed an issue in which 304x AP LEDs were inconsistent with their configured radio modes.

9. Errata

The following is a list of errata that still exist in vWLAN 4.1.0.

- 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-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-14696 Some APs may become stuck in an **Upgrading** state when uploading new firmware. **Workaround:** In the GUI, navigate to **Configuration** > **AP License**, and select the affected APs from the list and manually reboot them.
- 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-14271 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.
- VW-14265 The **Client Status** GUI page may contain inaccurate information on heavily loaded servers; however, the indexing will catch up over time.
- 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 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-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-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-12248 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.
- 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-11121 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.
- VW-10997 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.
- 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-10823 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.
- VW-10302 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.
- 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-9031 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.
- 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-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-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-3648 The vWLAN GUI will allow configuration of more than **1024** schedules; however, configuring more than 1024 schedules can cause the AP to reboot.
- BSAP-2297 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.
- BSAP-2258 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.

- 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 **Unregistered** 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.

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