RELEASE NOTES

vWLAN & BSAP 2.8.0
May 5, 2016

Trademarks

Any brand names and product names included in this manual are trademarks, registered trademarks, or trade names of their respective holders.

To the Holder of the Manual

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

In no event will ADTRAN be liable for any special, incidental, or consequential damages or for commercial losses even if ADTRAN has been advised thereof as a result of issue of this publication.

Toll Fraud Liability

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 Technical Support Community

For information on installing and configuring ADTRAN products, visit the ADTRAN Support Community, https://supportforums.adtran.com.

Pre-Sales Technical Support
(800) 615-1176
networkdesign@adtran.com

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

Post-Sales Technical Support
(888) 423-8726
support.adtran.com

Contents

Introduction

The 2.8.0 code releases for vWLAN and BSAP are major system releases that adds new features and addresses issues that were uncovered in previous code releases.

These releases are 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*.

A list of new or updated documents for this release appears on *page 10*.

Configuration guides, white papers, data sheets, and other documentation can be found on ADTRAN's Support Forum, https://supportforums.adtran.com. The contents of these release notes will focus on the platforms listed below.

Supported Models

The following models are supported in vWLAN 2.8.0.

- vWLAN Rackmount Appliance (1700900F1/1700900F2)
- vWLAN Virtual Appliance for VMware ESX/ESXi 4.X and 5.X (1951900G1)
- vWLAN Desktop Appliance (1700918F1)

The following models are supported in BSAP 2.8.0.

- BSAP 1800v1 and v2
- BSAP 1840
- BSAP 1920/1925
- BSAP 1930/1935
- BSAP 1940
- BSAP 2020
- BSAP 2030/2035/2135

Important Upgrade Note Specific to This Release

vWLAN can only be upgraded to 2.8.0 if it is currently on version 2.6.2. vWLANs on versions 2.2.1 to 2.6.1 must first upgrade to version 2.6.2 and then upgrade to version 2.8.0. AP firmware does not have to be upgraded to 2.6.2 and can instead be upgraded directly to 2.8.0 with the second upgrade.

If you attempt to upgrade from a version prior to 2.6.2 to 2.8.0, 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.)

Required BSAP Firmware

Due to BSAP and vWLAN firmware versions being mutually exclusive, the associated version of BSAP firmware for vWLAN 2.8.0 has been re-versioned to 2.8.0. From this point forward, vWLAN and BSAP firmware names will match.

Version 2.7.0 was a limited software release not made generally available.

The table below shows a version explanation:

vWLAN Version	BSAP Version
2.5.0	6.9.0
2.5.1	6.9.1
2.6.0	7.0.0
2.6.1	7.0.1
2.6.2	2.6.2
2.7.0	2.7.0
2.8.0	2.8.0

Wireless Regulatory Compliance

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

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, and once the AP is placed into a domain, it will scan the channels to discover neighboring APs and choose a valid channel.

Features and Enhancements

This section highlights the major features, commands, and behavioral changes in vWLAN 2.8.0.

- Added support for new Bluesocket Access Point 2020 (2x2, 11ac wave 1, indoor, internal antennas).
- Added support for SAML 2.0 Single Sign On (SSO) for administrators.
- Updated definitions for Layer 7 Device Fingerprinting.

Fixes

This section highlights major bug fixes in vWLAN 2.8.0.

- User entries were sometimes not removed from the UI once the user had been timed out.
- When using Machine Authentication, if the memory interval was set, users were not able to log in using user credentials again without re-authenticating their machine first.
- Using SNMP to poll vWLAN failed to return data if vWLAN had to poll APs for information.
- When the radius vender option under the external captive portal form was enabled, the vWLAN did not send the vender option in the Access-Request.
- Radius Mac Auth was sending an Authenticate Only service type in the Access-Request.
- Users stopped authenticating until the Access Point User Manager process was restarted.
- The Access Point User Manager process restarted when using High Availability between two servers.
- High Availability failed to replicate AP settings if DFS channels were being used in a mesh network and the Mesh Portal had not come online yet.
- In rare cases, timed out users were not removed from the UI properly.
- The OUI 10:41:7F did not show Apple as the manufacturer.
- The API could be used to create access groups without valid configurations.
- BSAPs were not blocking client traffic even though firewall rules had been created.
- Wireless packet captures taken from vWLAN did not capture all frames and reported data rates incorrectly.
- After upgrading, APs went into an Unknown State until rebooted.
- BSAPs licensed to Russia and set to 80MHz would reboot.
- In rare cases BSAP 2030s stopped beaconing on the 5 GHz radio until the unit was rebooted.
- The BG radio intermittently stopped functioning on the BSAP 1920 with the UI message: BG Radio: hardware unavailable.
- Wireless traffic captures showed a large number of malformed packets in Wireshark.
- IPv6 traffic was not being bridged.
- Several AP reboots were resolved.

Security Vulnerability Fixes

This section highlights major security vulnerability fixes in vWLAN 2.8.0.

- Resolved the Glibc (CVE-2015-7547) vulnerability.
- Upgraded NTP daemon to address security vulnerabilities.
- Resolved the Dropbear SSH vulnerabilities.

Errata

The following is a list of errata that still exist in vWLAN 2.8.0.

- Over time dashboard widgets cease to display the latest data point available.
- NTP updates are not occurring regardless of the frequency chosen in the platform settings. To force an NTP update, change the configured NTP server address(es).
- If an administrator incorrectly configures a Hotspot and an error message appears, some configuration options may no longer be visible.
- Switching domains on the **Administration > Backup/Restore** page leads to a server error.
- Guest Receipts incorrectly print two pages when printing for one account.
- When configuring custom language login forms, vWLAN displays invalid characters for certain 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.
- The client count display on the UI is inaccurate and can be out of sync in a large system with multiple clients roaming. The client count at the top of the UI page on the Domain status page and the client count at the bottom of the UI page do not match - even after multiple refresh cycles.
- On a heavily loaded system, the Captive Portal may fail to load when Redirect HTTPS traffic for Unregistered Clients is enabled.
- vWLAN is not in compliance with SNMP System Group according to RFC 1213.
- Packet captures taken from the vWLAN UI intermittently misses packets. In a lab environment during captive portal authentication with RadiusWebServer, 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 a 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.
- DynamicRF may significantly increase CPU load in large deployments.
- In extremely large deployments (~1500 Aps), the output of the **show tech** command can fill the disk.
- 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.
- MP is detected as adjacent by MPP resulting in RF recommendations.
- If the power on the 2.4Ghz radio of an AP is set to **0dBm** (1 mW), the power could be incorrectly set to **30dBm** (1000 mW) when booted.
- 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.

- In some instances the wireless packet captures fail to initiate properly. If this occurs, it may be necessary to restart the packet capture or restart the AP.
- Locations may not become active after a domain restore.
- Wireless IDS alerts are not generated for the following conditions: AP Down, AP SSID Change, and AP Channel Change.
- After an AP default location update, currently associated clients in the native AP location will not be updated automatically.
- 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.
- APs will sometimes report out-of-date adjacencies (up to 12 hours old).
- Some pages in the UI do not fully function under 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.
- Occasionally, the first time an AP is moved to a domain it will ignore its configured radio power settings. **Workaround:** Reconfigure the radio power settings.
- APs configured for Mesh mode do not allow a packet capture to be taken on the AP.
- iPad 3 (iOS 8.1) and iPad 2 (iOS 7.1) may have issues with redirection to the originally requested site after being redirected to login with Captive Portal.
- The API may become unresponsive if used from multiple sources simultaneously. It will become responsive again after a few minutes.
- Under heavy load, AP and client counts may be incorrect for a period of time but they will correct themselves.
- 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.
- 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 creating or editing a Role, if the administrator sets the **CoS Priority Out Overrid**e field to **DSCP from 802.11** or **802.1p from 802.11**, the IP packet put onto the wire will not have the DSCP value correctly set.
- The 2.4 GHz radio may only have 124 client associations, whereas the 5.0 GHz radio operates normally.
- BSAP 1800s may run low on memory causing sporadic client and AP activity or even a lose connection with vWLAN requiring a manual hard reset before operation can resume.
- Wireless packet captures may not function properly on the 5 GHz radio of a BSAP 1800 Series.
- Virtual Ethernet failing to connect causes a memory leak in the APs.
- BSAPs support up to 1024 schedule rules. If BSAPs are rebooting after adding schedules, the number of schedules will need to be reduced.
- 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.
- Certain devices will present a Captive Network Assistant (CNA) even though this feature is disabled in vWLAN.
- If greater than 86 users are associated to an AP and a failover occurs, they 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.

Release Specific Upgrade Instructions

vWLAN can only be upgraded to 2.8.0 if it is currently on version 2.6.2. vWLANs on versions 2.2.1 to 2.6.1 must first upgrade to version 2.6.2 and then upgrade to version 2.8.0. AP firmware does not have to be upgraded to 2.6.2 and can instead be upgraded directly to 2.8.0 with the second upgrade.

If you attempt to upgrade from a version prior to 2.6.2 to 2.8.0, 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 Please see the vWLAN upgrade guide located at https://supportforums.adtran.com/docs/DOC-7691.

vWLAN 2.8.0 requires using Bluesocket Access Point (BSAP) firmware version 2.8.0. BSAP 2.8.0 is not backward compatible with previous vWLAN code versions.

Upon upgrading to vWLAN 2.8.0, if you have an AP that is configured in an ETSI Regulatory Domain, the 5GHz band will be disabled. To re-enable the radio, enable the DFS feature (if installed outdoors), or mark the AP as indoor (if installed indoors).

vWLAN systems running 2.1 or earlier are not able to be upgraded. Instead, a new system should be deployed with 2.8.0 and configuration parameters from the 2.1 system should be manually ported to the 2.8.0 system. Attempting to upgrade a 2.1 system could cause some vWLAN configuration parameters to be lost.

If uploading firmware for the new BlueSocket 2020 APs, you must upload the firmware after the upgrade to 2.8.0 has completed. Otherwise, the software will not be applied to the templates properly.

Documentation Updates

The following documents were updated or newly released for vWLAN 2.8.0 or later. These documents can be found on ADTRAN's Support Forum available at https://supportforums.adtran.com. You can select the hyperlink below to be immediately redirected to the document.

- *vWLAN Admin Guide*
- *BSAP 2020 Quick Start Guide*

