RELEASE NOTES

vWLAN & BSAP 2.6.2
December 4, 2015

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
application.engineer@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 2.6.2 code releases for vWLAN and BSAP are minor system releases that add one new feature and address 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 6*.

A list of new or updated documents for this release appears *on page 12*.

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 2.6.2.

- 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 2.6.2.

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

Required BSAP Firmware

Due to BSAP and vWLAN firmware versions being mutually exclusive, the associated version of BSAP firmware for vWLAN 2.6.2 has been re-versioned to 2.6.2. From this point forward, vWLAN and BSAP firmware names will match. 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**

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 2.6.2.

- Added RADIUS-based MAC Address Authentication.

Fixes

This section highlights major bug fixes in vWLAN 2.6.2.

- A process crash in vWLAN caused RADIUS clients to be unable to authenticate or roam periodically.
- vWLAN failed to transition the user to the correct role when Machine Authentication was enforced.
- Resolved BSAP Impersonation Vulnerability (ADTSA-BS1001). See https://supportforums.adtran.com/docs/DOC-7891 for details.
- AP Licenses uploaded via the Domain tab may fail to process correctly if a large number (1000+) of APs are licensed on the system.
- Uploading license files that contained licenses for APs that already existed on the system would delete the description and syslocation of the APs.
- APs licensed for Russia could not use frequencies 5250 to 5350 indoors.
- Upgrading from 2.1 failed if the AP templates did not have a specific login form selected.
- When created, Login forms would use the root setting URL from the corresponding platform setting. However, if the setting was edited, the login forms were not updated to the new URL.
- No error message was returned if an AP's domain ID was set to an invalid value of 0 via the API.
- Invalid authentication server rules could be created via the API.
- An inactive primary DNS server could cause a DNS failure for Captive Portal users regardless of the activity of a working secondary DNS server.
- The platform NTP server setting did not return errors when invalid values were entered for its hostname.
- When using the API to configure a Boolean attribute, both **1** and **true** would evaluate to true and all other values would evaluate to false.
- The API could be used to create access groups without valid configurations.
- CoS priorities were displayed on the role create and edit pages even when the priority override was not set to one of the static options. When a non-static option was selected, the priority fields were ignored.
- The 1900 and 2000 series BSAPs could start to disallow new sessions if a large amount of sessions (7K+) were already active
- In some cases, DFS could not be configured on DFS-capable APs.

- APs would not upgrade if the firmware file name contained special characters.
- In BSAP 1800s, the supported channel width of the HT Information field in 802.11 WLAN management frames was not being set, which led client devices to assume that 20 MHz was the preferred channel width.
- Intermittently, clients could not pass traffic on BSAPs in a heavily saturated RF environment.

Errata

The following is a list of errata that still exist in vWLAN 2.6.2.

- In a large system with frequently roaming clients, the client count may not match in every instance in the UI - even after refreshing the page.
- Updating an authentication server using the API will cause the authentication rules to be appended rather than replaced. The GUI still functions as expected.
- Captive Portal fails to load when **Redirect HTTPS traffic for unregistered clients** is enabled under high load.
- If a vWLAN administrator adds an additional Radius Authentication server and wishes to modify an existing Friends and Family hotspot, the account type must be changed from Friends and Family to some other free spot/DNA to be able to edit the Authentication server. After editing they must switch back to Friends and Family.
- The API will create invalid authentication servers if an invalid role ID is provided for the default role as well as any of the roles.
- vWLAN is not in compliance with SNMP System Group according to RFC 1213.
- Devices that run the latest version of Android 6.x.x will see the BYOD information listed in the UI as **Unknown Device** in the device type and **Unknown OS** is the device OS.
- Packet captures taken from the vWLAN UI often miss packets. **Workaround:** Administrators are advised to take multiple Packet captures when attempting to diagnose an issue.
- The API does not return **prerequisite_role_ids** or **failed_role_ids** for roles configured for machine authentication. **Workaround:** These IDs can be obtained from the GUI.
- When using the API to create a machine authentication role, the **prerequisite_role_ids** attribute should be required, but it is not.
- Captive portal authentication on a Samsung Galaxy running older versions of Android 4.x.x may not redirect properly, even when the device is placed in the proper role and location.
- When attempting to execute an AP traffic capture from the vWLAN UI, if an AP in a down state is selected the capture will correctly not start, 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 **show tech** can fill the disk.
- Replication can fail to replicate AP settings if DFS channels are being used in a mesh network and the MP has not come online yet.
- The API can be used to set a role's location to NAC, even though this should not be and could cause authentication issues.
- After upgrading, some pages may not load correctly due to browser’s cached sorting options. Clearing the browser cookies and cache resolves the issue.

- When using the "Drop User" function, Apple Macbooks running OS X will retain the IP address that it previously held unless the timeout threshold is reached, which can cause Web redirection to the captive portal to fail if the client attempts to connect to a different SSID. Disabling the wireless interface on the Macbooks prior to dropping the users prevents the problem.
- A Mesh Portal will be detected as an Adjacent AP by a connected Mesh Point resulting in RF recommendations.
- If using the API, invalid data can be used for an authentication server's **role_id**, **timeout_weight**, **accounting_server_id**, or **auth rule role_id**.
- A SIP2 authentication server cannot have a CP location code of greater than 255 characters. If attempted, the authentication server will not be created/edited, and the user will be taken to a generic error page. Correcting the CP location code length will fix the problem.
- On a Friends and Family hotspot page, the field **Your email address** is asking for the email address of the friend or family member, not the sponsor.
- The Current AP Status dashboard widget does not display data for any APs in the ChannelScanning state.
- In rare cases, timed out users are not being removed from the UI properly.
- If the power on the BG (2.4 GHz radio) is set to 0% or 0 dBm, then when an AP boots, the power may go to the maximum level. **Workaround**: Do not use the 0 dBm setting on the 2.4 GHz radio.
- The OUI 10:41:7F does not show Apple as the manufacturer.
- When editing or viewing an access point configuration the terms Ethernet Bridge and LAN Extension are used interchangeably.
- Some customized login forms don't allow for 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.
- API POSTs to the guest_users URL will not return a success or failure to the requester.
- Locations may not become active after a domain restore.
- A virtual machine occasionally synchronizes time with the host even though vWLAN has disabled periodic time synchronization. Manually disabling this sychronization in the ESXi host resolves this.
- Wireless IDS alerts are not generated for the following conditions: AP Down, AP SSID Change, and AP Channel Change.
- AP security settings pertaining to WPA, WPA2-PSK, and Enterprise may not be displayed properly in the MIB browser when queried via SNMP.
- If a user connects to a WPA-enterprise SSID and 802.1X authentication fails, the user will be given the un-registered role regardless of the SSID's configured default role.
- In some cases, AP adjacencies are reported up to 12 hours later than they are detected which will skew the reported time in the vWLAN Adjacent AP's page.

- The DNS Server assigned to APs must be able to resolve the DNS name of vWLAN, otherwise captive portal redirection to a host name will not function.
- If a patch is applied to vWLAN, an admin task should appear to reboot the server for the pending patch activation. Occasionally, the task will appear after the reboot and should be ignored and deleted.
- An hourly Friends and Family Hostspot cannot be created properly using a time limit of 24 hours. **Workaround**: Use the **daily** setting.
- During the initial connection and authentication process, web redirection on Google Nexus and Droid Maxx devices will appear to get trapped on the thank you page. In most cases, the device has authenticated and received a proper IP address but the thank you page does not refresh. **Workaround:** The user must restart the browser to be directed to the designated webpage resource as expected.
- Some pages in the UI do not fully function using IE9. Use a different browser, upgrade to a newer version of IE, or use the API.
- When vWLAN is configured for high availability and an email configuration is deleted, the secondary's email configuration will be deleted while the primary's will not.
- Attempting to download and save a dashboard widget as a JPEG results in a 0 byte file.
- The standard **Please change the default admin password** platform task will not be removed if the default admin's password is changed using the link in the top-right of the page. In this case the admin task can safely be deleted.
- Changing any of the SNMP root settings (communities, contact, description, location, system name) from their default values will cause SNMP polls to exhibit unexpected behavior. If SNMP is to be used these should be left as defaults.
- Occasionally, the first time an AP is moved to a domain it will ignore its configured radio power settings until reconfigured.
- Admin tasks to restart specific processes will not be cleared after vWLAN has been restarted or rebooted. In these cases the tasks can be safely ignored and deleted.
- APs configured for Mesh mode can not perform an AP traffic capture.
- Using a Captive Portal pages' default language may not always properly function for users redirected to the page.
- iPad 3 (iOS 8.1) and iPad 2 (iOS 7.1) may not be redirected to the originally requested site after logging into a Captive Portal.
- Even with Captive Network Assistant disabled, it may still appear when certain Apple devices try to connect.
- When previewing a Captive Portal page, drop down menus will not function as they do in production.
- When upgrading vWLAN from 2.4 to 2.5+, after the reboot the upgrade can take a long period of time (an hour or longer) and the system will not be responsive during this time. When upgrading a large system with multiple domains and many users, consider a High Availability pair, and then upgrade the primary fully before the backup. Alternately, consider a long control channel timeout so the wireless can be used while the unit is upgrading.
- An API GET request on the service_groups URL does not return child services.
- An API GET request on the destination_groups URL does not return child destinations.
- The UI and API may become unresponsive for a short period of time if the API is used from multiple sources simultaneously.

- The API may become unresponsive for a short period of time if several Aps are rebooting.
- When using partial input in UI search fields, some searches may not complete.
- The ability to preview a login form does not function properly when using the Opera browser.
- BSAP 1800s may run low on memory causing sporadic client and AP activiy, or even a loss of connection with vWLAN requiring a manual hard reset before operation can resume.
- IPv6 traffic is not being bridged across BSAPs when a client using an IPv6 address authenticates.
- Wireless packet captures may not function properly on the 5GHz radio of a BSAP 1800 series AP.
- Utilizing DFS functionality may result in DFS falsely detecting radar transmissions which will cause the AP to change channels dropping clients connected to the AP.
- The 2.4GHz radio is disabled intermittently when dynamic RF mode is set to **Continuous**.
- 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 UI allows configuration of more than 1024 schedules although more than 1024 may 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, 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.

Release Specific Upgrade Instructions

vWLAN 2.2.1 and newer systems can be upgraded to vWLAN 2.6.2, and all configurations will be maintained.

To upgrade your vWLAN Virtual Appliance Please see the vWLAN upgrade guide located at https://supportforums.adtran.com/docs/DOC-7691..

vWLAN 2.6.2 requires using Bluesocket Access Point (BSAP) firmware version 2.6.2. BSAP 2.6.2 is not backward compatible with previous vWLAN code versions.

Upon upgrading to vWLAN 2.6.2, 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).

ADTRAN recommends vWLAN systems running 2.1 or earlier are not upgraded. Instead, a new system should be deployed with 2.6.2 and configuration parameters from the 2.1 system should be manually ported to the 2.6.2 system. Attempting to upgrade a 2.1 system could cause some vWLAN configuration parameters to be lost.

Documentation Updates

The following documents were updated or newly released for vWLAN 2.6.2 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*
- *Configuring DFS in vWLAN*
- *Configuring Layer 7 Device Fingerprinting in vWLAN*

