RELEASE NOTES

vWLAN & BSAP 3.1.0
December 21, 2017

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 3.1.0 code releases for vWLAN and BSAP are major system releases that add features 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 9*.

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 3.1.0.

- vWLAN Rackmount Appliance (1700900F1/1700900F2)
- vWLAN Virtual Appliance for VMware ESX/ESXi 4.X, 5.X, and 6.X
- vWLAN Desktop Appliance (1700918F1)

The following models are supported in BSAP 3.1.0.

- BSAP 1800v1 and v2
- BSAP 1840
- BSAP 1920/1925
- BSAP 1930/1935
- BSAP 1940
- BSAP 2020
- BSAP 2030/2035/2135
- BSAP 3040/3045

vWLAN 3.1.0 Scale

Due to the large number of features in vWLAN 3.1.0, vWLAN's scale limits are now 1000 APs, with 24 roams/second across the server (~18000 clients will generally stay under this number with normal power settings) on the default vWLAN resources.

Ongoing testing to improve scale with an increase resources is ongoing.

Some older AP models may not support all features in a release or past releases. For information on what your AP model supports, please consult the AP feature matrix.

Required BSAP Firmware

Due to BSAP and vWLAN firmware versions being mutually exclusive, the associated version of BSAP firmware for vWLAN 3.1.0 is version 3.1.0.

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

This section highlights major features in vWLAN 3.1.0.

- Added captive portal authentication option that does not require change of IP address (NAC address) from un-registered to registered roles (Walled Garden).
- Added DynamicRF AP/Sensor Mode Client Aware option. With this option BSAPs will not perform background scanning or change channel/TX power settings when there are active clients preventing performance and real-time application impacts from typical Radio Resource Management (RRM) software. This has been made the default Radio Mode option going forward.
- Added Mesh support to BSAP 2XXX series access points.
- Added the ability to provide client access on the mesh (5Ghz) radio.
- Added support for 802.11r Fast BSS transition on BSAP 19xx and 2XXX series APs.
- Added support for Radius Proxy. Proxy 802.1X Radius requests through vWLAN instead of sending directly from APs to external server.
- AP firmware is now bundled within the vWLAN release. Upon upgrade provided with admin task to apply and activate firmware.
- Added DFS support for BSAP 2020 in Europe.
- Added support for creating more than 251 roles. 1000 roles now supported. Note 4 roles are reserved by vWLAN for internal use.
- Added support for API call for determining number of active clients on an access point by radio, total and detailed list.
- Added support for noise floor on 5 GHz 11ac radios.
- Updated default captive portal page with ADTRAN logo and new GUI aesthetics.
- Added ability to acknowledge alerts.
- Added ability to exclude channels from DynamicRF.
- Added **show 100**, **show all** button to "top" widgets on reporting and analytics reporting dashboard.
- UI enhancements around logs, alerts and wireless IDS alerts.

- Added ability to download list of APs (**Status>APs**) and list of Clients (**Status>Clients**) in CSV format.
- Added columns such as status, error, message and actions such as reset to defaults and run background scan to **configuration>APs** page so you do not need to navigate to **status>APs** to see this status information or perform these actions.
- Configurable administration GUI timeout.

Fixes

This section highlights major bug fixes in vWLAN 3.1.0.

- High Availability would fail to replicate properly if a large number of images were being replicated. Snapshots would fail in this scenario as well.
- On demand background scans would not work properly if the 2.4Ghz radio was disabled on a BSAP 3040.
- In some cases, accepting DynamicRF suggestions for a specific AP may have caused another AP to apply the same suggestions.
- Scheduling a Dashboard Report on the 31st day of the month would cause the report to fail.
- Lobby Admins could not download or email Dashboard Reports if the System Summary Widget was present.
- UTF-8 characters used in client usernames caused vWLAN's UI indexing mechanism to crash and display inconsistent data for clients in the UI.
- Periodic reporting was failing due to a process crash in vWLAN.
- UI counts became incorrect under a high user load. This is the first part of a larger fix for this issue. Some client count inconsistency may still be observed.
- vWLAN High Availability would periodically fail to replicate data when the database was large.
- Timed out users were not observed in the UI when searching Status > Clients by AP name.
- The vWLAN UI could have shown incorrect data due to an underlying process consuming too much memory on large systems.
- Corrected an issue which could, in rare circumstances, cause historical client data on the status dashboard to not be visible for some administrators.
- In some cases the time zone assigned to an administrator's account could not be changed.
- Updating an APTemplate, DynamicRF Profile, or Accesspoint during a background scan would cause APs to get stuck in calibration.
- Searched data could not be sorted.
- DynamicRF would not change the AP power if the delta of the change was less than 2dB.
- The message column data in Status->APs was not being cleared in some corner-cases.
- Making any change to an AP would set the power back to the max power the radio could transmit if the radio was configured for auto channel and power.
- APs would take several minutes to appear in the AP Status page after being licensed.
- Running a background scan caused BSAP 1800s to stop broadcasting SSIDs afterwards.
- In some cases, vWLAN would show the TX power as higher than the max allowed power for that radio.
- Timed out clients were intermittently associated in the system to an AP with a MAC address of FF:FF:FF:FF:FF:FF causing them to never be removed from the system properly.

- Scheduled Background Scan was not auto applying to All APs though the checkbox was selected.
- When placing APs on Maps in high density deployments, the green bar surrounding the AP name was in the way.
- Top Client Count Usage percentages on the vWLAN dashboard were incorrectly calculated.
- In some cases, DynamicRF messages on the Status->APs page would show recommendations that were not actually applied to the APs.
- The BSAP 3040 would cease to scan AP adjacencies, causing DynamicRF to make incorrect channel and power choices.
- Some AP adjacencies reported by a BSAP 3040 were incorrect.
- The AP traffic capture error message is using the AP MAC versus AP Name.
- Internal users created by a hotspot plan are not deleted after being used.
- If the hotspot plan's max and min were the same value a user could not be created.
- GRE tunneling required L3 Mobility to be enabled.
- vWLAN may have failed to authenticate users quickly when deployed in a large scale environment (10000+ Clients).
- Changing permissions in an admin role caused all admins with that role to have inconsistent permissions.
- After an idle user is timed out, the vWLAN log that shows the AP the user was connected to with a MAC containing all F's.
- Editing an AP job several times could eventually cause the user to receive an internal server error.
- The timezone entries for Moscow, St. Petersburg and Volograd were incorrect in the AP template.
- Allowing client to client traffic not applied with an "apply" but instead requires an AP reboot.
- Fixed an error involved with formatting of data from widgets when emailing that data to a user.
- The minimum Transmit power was displayed as 0dBm when the Channel was set to Auto inside the AP template.
- vWLAN logs reported client data usage as kilobytes, but the unit measure showed bytes.
- Scheduled dashboard reports did not include data for Current Client or AP count.
- Administrators could not sort by Auth Server Precedence.
- OpenSSL was upgraded to address all open OpenSSL vulnerabilities.
- When opening the vWLAN web UI with the link "https://<vwlan>:3000/administrators/sign_in" when already logged in, the Setup Wizard was automatically launching.
- If an administrator incorrectly configured a Hotspot and an error message popped up, then some configuration options may no longer have been visible.
- The timezone in the AP template for Moscow, St.Petersburg, and Volgograd was GMT +4 instead of GMT +3.
- vWLAN did not send RADIUS Accounting stop messages in certain cases.
- If a vWLAN administrator added an additional Radius Authentication server and wished to modify an existing Friends and Family hotspot, the account type had to be changed from Friends and Family to some other free spot/DNA to be able to edit the Authentication server.
- The API would create invalid authentication servers if an invalid role ID was provided for the default role, as well as any of the other roles.

- When using the API to create a machine authentication role, the prerequisite_role_ids attribute should have been required, but was not.
- Running an AP packet capture may have failed, and the AP may have shown a "Capturing" status until rebooted.
- If a hotspot account was reconfigured from one that used an email setting to one that did not, the previous email setting was still visible.
- After running a background scan, the BSAP 3040 would fully reboot before accepting the DynamicRF suggestions.
- In rare cases, DynamicRF may have set an AP to a larger value than was configured as the maximum in the DynamicRF template.
- Resolved KRACK Vulnerability (www.krackattacks.com for information).
- In some case Mesh Points may disconnect, requiring a reboot of the Mesh Portal to regain functionality.
- The BSAP 3040 may have intermittently stopped broadcasting SSIDs.
- A client that attempted to switch between the 2.4Ghz and 5Ghz radio on the same AP would be disconnected.
- A BSAP 3040 in Continuous DynamicRF mode may have eventually ceased scanning Channels.
- After a background scan the BSAP 3040s scanning radio would stop scanning the environment, which caused new AP adjacencies to be missed.
- Some multi-stream clients are only using 1 stream when communicating with APs.
- 802.11k and v capable clients band steered by a BSAP 3040 could not pass traffic.
- BSAP 3040 5Ghz output power was different when the 2.4GHz radio was enabled vs disabled.
- Clients were intermittently unable to authenticate to an AP until the AP was rebooted.
- The BSAP 3040 would advertise support for only 1 High Throughput Stream per client, effectively operating with 1 Antenna.
- The BSAP 3040 would count it's own Radios as AP adjacencies.
- Dual Mode would incorrectly shorten the client-servicing time after a scheduled DynamicRF scan, causing a drop in AP throughput.
- The BSAP 3040 may have rebooted due to a process failure.
- In rare cases where APs ran low of memory, they were not rebooting to resume normal operation correctly.
- A BSAP 3040 memory leak could have caused the AP to go to a Down state.
- If using DFS, APs may have changed to channel 36 every time after a radar detection.
- In some cases after a client associated to a radio it would be unable to send traffic.
- BSAP 1920s may have reboot periodically due to a software crash.
- Resolved Dropbear SSH Security Vulnerability CVE-2016-7406, CVE-2016-7407, CVE-2016-7408, CVE-2016-7409.
- Once 1024 firewall rules had been configured in a role the AP would continuously reboot.
- In rare cases when using 4+ SSIDs on a BSAP 1900 series AP, the channel shown in the vWLAN UI may not have been the channel the AP was actually operating on.
- The Noise Floor was not shown in AP details for the BSAP 2000 series AP's 5Ghz radio.

- The DHCP lease for the NAC IP address received during captive portal authentication may have shown 40 seconds rather than the configured time when observed in an AP traffic capture.

Errata

The following is a list of errata that still exist in vWLAN 3.1.0.

- Large scale deployments may result in out of memory conditions. As such vWLAN release 3.1 is limited to support 1000 Access Points.
- When an on-demand background scan is completed, a completion message will not be displayed for the BSAP 304X
- A location group can be created and assigned without any locations added to it. If a vWLAN is configured in this manner, vWLAN's user manager may crash. **Workaround:** Add locations to the group.
- After NOL is expired for a channel, vWLAN AP-config-page and AP-Status page show different channel numbers.
- Client Status Page may contain inaccurate information on heavily loaded servers. The indexing will catch up over time.
- While creating a new SSID using WPA2 security, the UI does not show the option to choose an accounting server. Workaround: Edit the SSID after it is created.
- If you restrict all available channels save 1 and then run a background scan, the APs may choose a restricted channel.
- If either Radio has the DynRF Profile set to Disabled, a background scan will fail to run on the AP that belongs to the AP template.
- The vWLAN API does not allow an administrator to update Dynamic RF profiles once created.
- Non-root users can not properly acknowledge alarms.
- Non-root users can not properly acknowledge WIDS alerts.
- If a secondary server is converted to a standalone, APs will show down in the UI.
- The SNMP Trap OID and TRAPOID number values are the same for everything.
- An AP cannot be managed from the unregistered role.
- 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.
- Utilizing SNMP on vWLAN can cause the server's memory to be heavily utilized.
- 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 different types or series causes sluggish connection speeds. This type of linking 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 UI even though they will be 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.
- In a frequently changing RF environment, if new RF changes have been detected since the last status was displayed, DynamicRF suggestions shown on the **Status** > **APs** menu may not be the exact settings pushed to the AP upon an accept.
- In an extremely crowded RF environment (APs with over 100 adjacencies), the DynamicRF channel algorithm may not choose 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 it 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 80 MHz mode are shown in vWLAN's Adjacent AP menu as 40 Mhz.
- 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.
- Unless the maximum and minimum transmit power are set to the same value inside a DynamicRF profile, those specific power settings will never be automatically chosen for radios.
- When moving an AP from any AP template back to the default template, a domain task will be incorrectly generated to create a scheduled background scan.
- The **Select All** button only selects the first 100 table entries in the UI.
- Bulk Import only allows a 1000 line CSV file to be uploaded at a time.
- Over time dashboard widgets cease to display the latest data point available.
- 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.
- 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 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.

- Packet captures taken from the vWLAN UI often miss 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 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 does not return errors when invalid values were entered for its host name.
- 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 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.
- 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 certain letters.
- APs configured for Mesh mode do not allow 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.
- Only 255 locations can be supported on a single AP. Adding a 256th will cause the AP to cyclically reboot until it is removed.
- Country information field for channels that are allowed in Russia (52+4 and 132+4) are missing in the Beacon.
- The BSAP 3040 does not request option 43 in the DHCP option 55 section of the DHCP discovery packet causing discovery to fail in some cases.
- If an AP radio is set to a channel width that requires more channels than are currently unrestricted according to the channel-restrictions set by the administrator, the AP may operate on restricted channels.
- The 2.4 GHz radio may only have 124 client associations, whereas the 5.0 GHz radio operates normally.
- Only 52 clients can associate to a BSAP 1800, despite vWLAN indicating a 64 client limit.
- 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.
- The UI will allow configuration of greater than 1024 schedules. Configuring greater than 1024 schedules can result in AP reboots.
- BSAPs support up to 1024 Schedule Rules. If the APs reboot after adding schedules, you need to reduce the number of schedules.
- 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 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

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". Clicking this admin task allows you to apply the firmware to all templates in all domains.

vWLAN can only be upgraded to 3.1.0 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 3.1.0. AP firmware does not have to be upgraded to 2.6.2 and can instead be upgraded directly to 3.1.0 with the second upgrade.

If you attempt to upgrade from a version prior to 2.6.2 to 3.1.0, 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 3.1.0 requires using Bluesocket Access Point (BSAP) firmware version 3.1.0. BSAP 3.1.0 is not backward compatible with previous vWLAN code versions.

vWLAN systems running 2.3X or earlier are not able to be upgraded. Instead, a new system should be deployed with 3.1.0 and configuration parameters from the 2.3.X system should be manually ported to the 3.1.0 system. Attempting to upgrade a 2.3.X system could cause some vWLAN configuration parameters to be lost.

