RELEASE NOTES

vWLAN & BSAP 3.0.1

June 14, 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

Copyright © 2017 ADTRAN, Inc.
All Rights Reserved.

Contents

Copyright © 2017 ADTRAN, Inc.

Introduction

The 3.0.1 code releases for vWLAN and BSAP are maintenance releases that 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*.

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 3.0.1.

- 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 3.0.1.

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

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.

Important Upgrade Note Specific to This Release

vWLAN can only be upgraded to 3.0.1 if it is currently on version 2.6.2 or higher. vWLAN on version 2.2.1 to 2.6.1 must first upgrade to version 2.6.2 and then upgrade to version 3.0.1. AP firmware does not have to be upgraded to 2.6.2 and can instead be upgraded directly to 3.0.1 with the second upgrade.

If you attempt an upgrade from a version prior to 2.6.2 to 3.0.1, 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.)

Copyright © 2017 ADTRAN, Inc.

Required BSAP Firmware

Due to BSAP and vWLAN firmware versions being mutually exclusive, the associated version of BSAP firmware for vWLAN 3.0.1 is version 3.0.1.

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.

Fixes

This section highlights major bug fixes in vWLAN 3.0.1.

- The vWLAN System Summary dashboard widget failed to load properly.
- Newly deployed BSAP 304Xs may have caused the error **SendContinuousDualModeSetting failed: Command Timeout** in the Error Column in vWLAN.
- vWLAN failed to upgrade due to incorrectly marked **Installed At** APs.
- vWLAN failed to upgrade due mesh points not having a mesh portal selected.
- In certain cases, 802.1X RADIUS Accounting messages were not sent.
- DynamicRF failed to set APs to proper channels and power in large deployments (~700 APs).
- APs became stuck in the Channel Scanning status after upgrading.
- Upgrading vWLAN failed if APs were misconfigured (marked installed **Outdoors** and set in an AP template with **DFS Disabled** while licensed in the ETSI countries).
- Stored user bandwidth utilization information filled up the vWLAN disk causing a loss of service.
- In large user deployments (5000+ unique wireless users), vWLAN would take several hours to upgrade.
- vWLAN sometimes failed to authenticate users when deployed in a large scale environment.
- Running a Showtech fails to complete when collecting AP logs.
- vWLAN servers under heavy load (500+ APs and 5K clients) would experience greater than 1 minute load times and very slow changes in AP status. In addition, DynamicRF failed to run properly once the server was in this state.
- vWLAN's BYOD tables (used for quicker device mapping on future logins) grew very large and used a large amount of memory.
- The **Status > APs** page in the vWLAN UI took greater than 1 minute to load.

Copyright © 2017 ADTRAN, Inc.

- After upgrading from 2.6.2 or earlier to 2.8.0 or 2.9.0, some maps would not render properly without uploading the maps again.
- Changing the DynamicRF profile on an AP template from **Set Once and Hold** to **Continuous** did not render and change until the AP is manually rebooted.
- In certain cases, the client count in the UI on the **Status** pages was incorrect.
- AP power and channel settings as well as antenna gain settings were not retained in a Domain backup.
- When using a GRE Tunneling profile on an SSID and a role with a non-native VLAN assigned to it connecting users did not receive an IP address.
- vWLAN would accept a negative antenna gain value which resulted in a cyclical reboot of the AP.
- The vWLAN API aptemplates resource would not return an SSID ID List.
- Depending on the size of a Domain backup and configuration, the Domain restoration process would take more time than usual.
- WEP encryption functions sporadically. **Workaround**: Use WPA2 authentication.
- vWLAN UI logs did not display RADAR detection events.
- 64-bit WEP and Shared Security were not functioning.
- BSAPs blocked DNS to and from the vWLAN server when in the unregistered role.
- The BSAP 3040 may have rebooted due to packet fragmentation.
- Under certain conditions clients intermittently could not connect to BSAP 20XY series APs due to incorrect probe responses.
- An AP could have become idle and not properly communicate or communicated it's status back to vWLAN.
- Resolved Dropbear SSH Security Vulnerability CVE-2016-7406, CVE-2016-7407, CVE-2016-7408, CVE-2016-7409 - EVAN DBL CHECK.
- APs configured for DFS may have started to constantly run a Channel Availability Check.
- When set to AP/Sensor mode on the 5Ghz radio, BSAP 2030s and BSAP 2020s would experience a memory leak.
- Rarely, an AP stopped responding to traffic on the 2.4 GHz radio until rebooted or a configuration was pushed.
- Rarely, the BSAP 2020/2030 Series APs ceased broadcasting their SSID on the 5 GHz radio.
- Role Scheduling does not affect IPv6-based traffic because IPv6 is not supported, therefore IPv6 traffic will be bridged onto the wire. **Workaround**: Block IPv6 in the upstream firewall if necessary.
- The BSAP 2020 experienced problems with multiple 5 GHz SSIDs on the same AP.

Errata

The following is a list of errata that still exist in vWLAN 3.0.1.

- Continuous re-indexing of the vWLAN UI is causing system instability in large scale 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.
- GRE tunneling requires L3 Mobility to be enabled.

Copyright © 2017 ADTRAN, Inc.

- Creating Mesh links between APs of different types or series causes sluggish connection speeds. This type of linking is not recommended or supported.
- Editing an AP job several times eventually can cause the user to receive an internal server error. **Workaround**: Create a new job to replace the old one.
- 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.
- The time zone entries for Moscow, St. Petersburg, and Volgograd are incorrect in the AP template.
- 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.
- Allowing client-to-client traffic cannot be applied using the **Apply** option but instead requires an AP reboot.
- The minimum transmit power is displayed as 0 dBm when the channel in the AP template is set to **Auto**.
- 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.
- vWLAN logs report client data usage as kilobytes but the unit measure displayed is bytes.
- Scheduled dashboard reports do not include data for Current Client or AP count.
- 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.

Copyright © 2017 ADTRAN, Inc.

- 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.
- Wireless IDS alerts are not generated for the following conditions: AP Down, AP SSID Change, and AP Channel Change.
- 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.

Copyright © 2017 ADTRAN, Inc.

- 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.
- 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.
- Changing the channel width when a windows client is connected will result in a one time AP reboot.
- When the number of firewall rules configured in a role reaches 1024, an AP will continuously reboot. Note that each service/hostname/IP constitutes one rule. Items designated as **both ways** count as two rules for each line.
- In some cases while running in AP/Sensor mode on the 2.4 Ghz radio, smaller packet sizes (<=512 Bytes) will cause greater performance degradation than normally running AP/Sensor mode (~10%).
- In rare cases when using 4+ SSIDs on a BSAP 1900 Series AP, the channel shown in the vWLAN UI may not be the actual channel on which the AP is operating.
- The **Noise Floor** is not shown in AP details for the BSAP 2000 Series AP's 5Ghz radio.
- 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.
- 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.

Copyright © 2017 ADTRAN, Inc.

- 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.
- On a heavily loaded system, the Captive Portal may fail to load when **Redirect HTTPS traffic for Unregistered Clients** is enabled.

Release Specific Upgrade Instructions

vWLAN can only be upgraded to 3.0.1 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 3.0.1. AP firmware does not have to be upgraded to 2.6.2 and can instead be upgraded directly to 3.0.1 with the second upgrade.

If you attempt to upgrade from a version prior to 2.6.2 to 3.0.1, 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 3.0.1 requires using Bluesocket Access Point (BSAP) firmware version 3.0.1. BSAP 3.0.1 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 3.0.1 and configuration parameters from the 2.3.X system should be manually ported to the 3.0.1 system. Attempting to upgrade a 2.3.X system could cause some vWLAN configuration parameters to be lost.

Copyright © 2017 ADTRAN, Inc.