# RELEASE NOTES

vWLAN 2.6.0
June 12, 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

vWLAN 2.6.0 is a major system release that adds new features and addresses issues that were uncovered in previous code releases.

This 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 8*.

A list of new or updated documents for this release appears in *on page 16*.

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 2.6.0.

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

# System Notes

vWLAN 2.6.0 is a software release that manages, configures, controls, and secures Wi-Fi access points (APs), the radio frequency (RF) spectrum and users, across single or multiple separate customers (tenants). It can be deployed in the public or private cloud, on physical appliances, and/or virtual machines. Multiple tenants can use the same vWLAN software with their individual APs.

## Required BSAP Firmware

**vWLAN 2.6.0 requires using Bluesocket Access Point (BSAP) firmware version 7.0.0.**

## VMware Memory Requirements

VMware deployments require at least 6GB of memory assigned to vWLAN.

## BSAP Interoperability and Performance

802.11n/ac wireless client interoperability is only guaranteed for Wi-Fi Alliance certified clients. For the highest 802.11n/ac performance, follow these steps:

1. Use WPA2 (PSK or 802.1X) with advanced encryption standard (AES) when connecting 802.11n/ac-based clients. A TKIP client will connect at a maximum transmit rate of 54 Mbps. It is highly recommended that WEP, WPA, and TKIP not be used, but WPA2 + AES be used instead. Running in a mixed mode environment (i.e., with legacy clients) will impact the 802.11n/ac client's performance.
2. Enable 802.11n and ac Wireless Modes, 80 MHz channel bandwidth (for 802.11a radio), and Packet Aggregation mode. These are configured under the 802.11 radios in the GUI in the AP template.
3. Enable 802.11n/ac on the wireless client devices (in the hardware/firmware options). For example, with the Linksys 802.11n card, use the Windows configuration interface (under Properties > Driver) and

 

enable IBSS mode for 80211a/b/g/n/auto.

4. Ensure that all 802.11n/ac client drivers are updated to the latest version before doing any system or performance testing.
5. To support multicast traffic between clients, do one of the following:
   - On the SSID, convert multicast to unicast, and then allow the Multicast Destination IP Address (or all addresses) in the Client Role(s). This is the recommended option in an environment where only certain users should receive the multicast streams.
   - Allow the Multicast Destination IP Address in the Unregistered Role. The drawback to the Unregistered Role is it allows multicast for all users. Therefore, it should only be used if all users are allowed to receive the multicast streams.

## Features and Enhancements

**This section highlights the major features, commands, and behavioral changes in vWLAN 2.6.0.**

- **Layer 7 Device Fingerprinting**

  The ability to provide status information, analytics, and reports on the device type, operating system, manufacturer, hostname, and ownership of the devices being used on the network. In addition, the ability to provide device specific policies based on device type and ownership.

- **Zero IT Setup**

  Targeted at small businesses using ProCloud or Service Providers onboarding many small businesses to their cloud-managed service offering. With this web-based wizard driven approach, small businesses can enjoy a fully functional employee and guest network in minutes with just a few clicks and keystrokes. All configurations such as network names, passwords, blocking guest traffic from the employee network, etc. are put into place automatically and users can click more info to learn exactly what's going to be performed and where within the system.

- **Dynamic Frequency Selection (DFS) Support for Bluesocket Access Point (BSAP) 1900 Series in Europe**

  Support for Dynamic Frequency Selection (DFS) on the BSAP 1920,1925,1930,1935 (On hardware revision K or better for BSAP 1920 and 1930 models only) and 1940 in Europe only. DFS provides the ability to use additional 5 GHz channels that are also used by radar systems. In order to use these channels, the AP must scan the channel for the presence of radar before and during usage and if radar is detected automatically move off the channel. DFS is required for European 5 GHz outdoor deployments and without DFS European 5 GHz indoor channels are limited to just 4. More channels result in more user capacity required for high density deployments such as stadiums. More channels also results in less interference, higher throughput and performance.

 

- **Removed DNS Requirement from APDiscovery Process**

  Previous revisions of vWLAN and ProCloud required the BSAP to communicate with the vWLAN using DNS to determine if the vWLAN was alive. This requirement has been removed from vWLAN 2.6 as this would break auto discovery when APs did not have outbound DNS access because of a firewall policy. Please note that the BSAP 18x0 series still uses DNS discovery during firmware upgrades.

- **Web-based Authentication Usability Enhancement**

  During the web-based authentication process, clients are provided with a temporary IP address (NAC Address) from the BSAP before they authenticate or are in the "un-registered" role of the system. Upon authentication, clients transition to an IP address from their final network. Some mobile clients in the field have exhibited the behavior of holding on to the temporary IP address and not transitioning to their final IP address. This results in the client having to manually disconnect and reconnect in order to transition IP addresses and pass traffic. With the introduction of Layer 7 Device Fingerprinting, the BSAP will automatically detect the devices who exhibit this particular behavior and quickly deauth them from the wireless network so they will automatically reconnect, transition IP addresses and be able to pass traffic without any manual intervention.

- **The addition of nine new widgets (reports and analytics):**
  - Client Count by Device Type Over Time
  - Client Count by Ownership Over Time
  - Current Clients by Device OS
  - Current Clients by Device Type
  - Current Clients by Ownership
  - Top Device OS by Client Count Over Time
  - Top Device OS by Usage Over Time
  - Top Device Types by Client Count Over Time
  - Top Device Types by Usage Over Time
- **The ability to bulk import the MAC addresses of devices to mark them corporate owned/issued or for MAC address authentication.**

## Fixes

**This section highlights major bug fixes in vWLAN 2.6.0.**

- Upgraded OpenSSL to the latest version to address several security issues.
- Webserver would not start on the V3 vWLAN hardware appliance.
- SSL certificate hostname would be validated even though certificate validation was not enabled.
- Resolved some performance issues with the reporting engine.
- A system performance log file improperly logs verbose amounts of data eventually causing shared memory to deplete. This may cause sluggishness in the web server as well as a failed upgrade.

 

- No Port Number field appeared in the AP traffic capture when TCP/UDP was selected.
- If APs were added and removed up to 2048 times, new APs could not be added.
- Internal Users did not expire when they were set to expire.
- Extensive improvements were made to the User Management process. Prior to these improvements, clients would periodically stop authentication, role assignment, etc in a particular Domain until the User Management process was restarted.
- The Location Status field on Location Status page was not sorting properly.
- Too many locations caused a visual overlap on the AP details page.
- The logs displayed could not be downloaded when filtered by criteria entered in the Adjacent APs search field.
- DNA hotspot configuration did not send email if TLS security was disabled.
- External redirect did not function in vWLAN 2.5.1.
- Custom HTML code that functioned in 2.5.0-12 would not function in 2.5.1-7.
- Prior to 2.6, TLS-based Gmail did not function for email for DNA Hotspots. You had to use port 465 and SSL-based Gmail.
- Critical Vulnerability CVE-2015-023, named Ghost, was patched by upgrading the glibc libraries.
- The HA Page allowed the browser to change the user account password if one had been saved.
- Creating MAC devices via the API failed because the ID was already in use.
- Rebooting the vWLAN resulted in the message: Sorry Page Cannot Be Displayed.
- When needing to reset an administrator's password, the email that was sent contained a link to the IP address of vWLAN as opposed to the configured hostname resulting in a certificate warning if a certificate was installed.
- Downloaded adjacent AP table did not display the **Signal (dBm)** or **Sensor Name** columns.
- Out of date VM tools may lead to a vWLAN reboot.
- Locations were reported as INACTIVE until Restart Status Database was run.
- When updating an AP template applied to uplink mesh APs, the administrator was warned about disabling mesh even though mesh was not being disabled.
- The Current Active Users by Radio Mode widget displayed a null value.
- A duplicate 802.1X authentication server could be created but not edited.
- The **Timeout Value for Web Server** should include the unit of measure.
- An AP rendered incorrect available SSIDs when attempting a wireless packet capture.
- Downloading a large number of logs caused the UI to become unresponsive.
- The UI was not properly rendering the page in Google Chrome.
- Setting a very large value in the System Settings **Timeout Value for Web Server** caused Captive Portal to run out of available web sessions. This field is now limited to 30 seconds.
- Guest users cannot be deleted from guest_users using the API.
- Captive Portal fails to load when Redirect HTTPS traffic for unregistered clients is enabled.

 

## Errata

**The following is a list of errata that still exist in vWLAN 2.6.0.**

- When using a Google Chromebook on a captive portal, the user is never automatically redirected to their final destination. Manually refreshing the page or going to another page will function as expected.
- APs licensed in the U.S. appear as though they are DFS capable even though DFS will not be supported until release 2.7.
- The 2.2.0 conditional release cannot be upgraded directly to 2.6.0. The unit must be upgraded to 2.2.1 or higher before upgrading to 2.6.0.
- When configuring web redirection, it is important that the AP and vWLAN configurations be in sync. If a login form is modified or the SSID or a template is changed, the configuration must be pushed to the AP. If it is not pushed to the AP it is possible for web redirection to fail. **Workaround:** If web redirection is failing, reboot the AP, restart services on vWLAN, or both.
- If an AP with users connected to it is rebooted or disconnected, the users may stay in vWLAN until one of these conditions occur: 1) They roam to or connect to another AP and then time out as normal from that AP, 2) they are manually dropped from the Active Clients table, or 3) the vWLAN is rebooted.
- When uploading a new certificate, the admin web server must be restarted to apply the new certificate.
- The intended behavior of HSTS is 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. When redirecting to an HTTPS site that does not use HSTS (https://www.adtran.com works for this), the certificate warning still appears, but it will be possible to ignore it and go to the login form anyway. See http://caniuse.com/#feat=stricttransportsecurity to determine which browsers support HSTS.
- vWLAN will return something for most API POST requests (either the created element or an error explaining why the POST failed), but POSTs for guest users (both successes and failures) return nothing to the requester.
- If an email server is configured and it is unreachable or if a policy on that server denies email, emails will not be sent from vWLAN. **Workaround:** If email is configured but no email is being received, contact the email server administrator.
- When running vWLAN on VMWare, the option to run a traffic capture on the private interface will not exist unless a private interface has been created for the VMWare.
- Dashboard widgets may behave improperly in IE9. Other browsers function correctly.
- After deleting dashboard widgets, widgets below the deleted ones should move up to fill the empty space, but this occasionally does not function.
- When the page's download link is used, real-time widgets are not downloaded with the rest of the dashboards on the page .
- As an Administrator, in order to preview the image that is selected on an existing Guest Receipt you must select the **Show** button on the bottom of the page. Selecting the **Guest Receipt** or the **Edit** button will not show the image file or the image file name.
- A virtual machine occasionally synchronizes time with the host even though vWLAN has disabled periodic time synchronization. **Workaround:** All virtual machines should be configured with NTP, and the Host ESXi server must have NTP enabled to ensure it has the correct time/timezone.
- Wireless IDS alerts are not generated for the following conditions: AP Down, AP SSID Change, and AP Channel Change.

 

- The iPhone 6 running iOS 8.1 displayed inconsistent behavior with vWLAN 2.6 using Captive Network Assistant. At times the CNA will function and at other times it will not. This behavior was seen on both the 2.4 and 5 GH radios. **Workaround:** Manually open the Safari browser in order to be redirected to the authentication log in page.
- The Platform NTP server setting currently has no validation capabilities, therefore the setting will accept any value without returning an error. Make sure to enter the valid FQDN or the valid IP address when configuring this field.
- AP security settings pertaining to WPA, WPA2-PSK, and Enterprise may not be displayed properly in MIB browser when queried via SNMP.
- After an AP default location update, currently associated clients in the native AP location will not be updated automatically.
- The platform setting Default URL formerly was used to prevent web crawlers and other devices from getting the login page from the network side. The user previously was redirected to this URL. The system now sends a 404 error instead, so the field no longer has a meaning and can be safely ignored.
- Changing the default administrative user login (root@adtran.com) on the Primary vWLAN system does not change it on the Secondary vWLAN system as it should. **Workarounds:**

  1. Take another snapshot from the Secondary as the new administrator is updated on the Secondary system to match the change on the Primary system.

  2. Follow the detailed steps below to promote the Secondary system to Standalone then return it to a Replication node:

     a) Promote the Replication Node to **Standalone** using the **High Availability** drop-down list.

     b) After selecting **Standalone**, select the **Update Replication Node** radio button. The message **Replication Node was successfully updated** will appear.

     d) Select the administrative user (root@adtran.com) at the top right and change it to match the user that was set in the Primary system (for example, john@adtran.com).

     f) Select the **Update Administrator** radio button to save the change. The message **Administrator successfully updated** will appear.

     h) To return the node Replication, in the UI, navigate to **Configuration > System > High Availability**.

     i) Select **Node** in the drop-down list.

     j) Enter the IP address of the Primary system.

     k) Enter the password that was used when high availability was originally configured on the Primary system.

     l) Select the **Update Replication Node** radio button to bring high availability back in sync. The default administrator login (john@adtran.com) is now configured on both the Primary and Secondary systems.
- High Availability does not replicate the HotSpot Login Forms correctly.
- When logged in as root@adtran.com (Administrator), an erroneous prompt to change the email address appears.
- Although MAC authentication has been relabeled as device authentication, they still appear as MAC auths in the logs.

 

- Importing a CSV file from Microsoft Excel does not always work correctly. **Workaround:** Use the CSV (Comma delimited) to import instead of CSV (Macintosh) or CSV (MS-DOS).
- Restore Default Roles does not prompt for confirmation.
- In the AP Template, the DFS Block Channel is the list of channels that should not be used for DFS. Channels on the left are allowed for DFS, while those on the right are not allowed. For Firefox 36.0.1 browser, the channels sometimes all show up on the right side. The administrator should add them to the left side.
- Some clients are being assigned to the Unregistered role instead of the role assigned by the 802.1x auth server.
- APs will sometimes report out-of-date adjacencies (up to 12 hours old). **Workaround**: Wait for the system to age them out or ignore the adjacency.
- The DNS Server given to APs must be able to resolve the DNS name of the vWLAN, otherwise captive portal redirection to a hostname will not function.
- When trying to locate an AP that is no longer there, the following error may be displayed: **The page you were looking for doesn't exist. This could be caused by a mistyped address or the page may have moved.** The error should say: **No detecting access points have been placed on the map, the map hasn't been calibrated yet, or this AP has not been seen in the last hour!**
- Some fully customized captive portal hooks do not function as expected.
- Scheduled reports are marked with UTC time when delivered via scheduled emails. Manually downloaded reports show the correct GMT time for the administrator.
- In the **Show or Hide Setup Wizard** setting, to show the wizard, set this field to enabled, to hide, set to disabled.
- The third generation vWLAN hardware appliance may pull a second DHCP address.
- If a patch is applied to vWLAN, an admin task prompt should appear to reboot the server for the pending patch activation. Occasionally, this prompt will appear after the reboot and should be ignored and deleted.
- The API for logs is not functioning.
- To avoid problems with the Friends and Family HotSpot account creation, administrators should use **Daily** hotspots rather than creating a **24 Hour HotSpot**. The user account creation screen comes up as usual and the user is allowed to select the hotspot account **24 Hour HotSpot** and enter an email address and password. However, the required account time limit field cannot be selected causing the page to fail with an error message.
- If a hotspot account is reconfigured from one that uses an email setting to one that does not, the previous email setting will still be visible. This email setting will not be used by the hotspot account and can be safely ignored.
- When trying to create a mixed mesh, a cryptic validation error message may display. When configuring a mesh do not use all the same values for Regulatory Domain, DFS capability, and DFS enabled settings.
- On the **snmp_trap_configurations** show page there is a hint that reads: **IP address of vWLAN. 127.0.0.1 means the local vWLAN box**. This hint should read: **IP address of SNMP Trap Server. 127.0.0.1 means the local vWLAN box.**
- On the **syslog_configurations** show page there is a hint that reads: **IP address of vWLAN. 127.0.0.1 means the local vWLAN box**. This hint should read: **IP address of syslog server 127.0.0.1 means the local vWLAN box.**

 

- Some information in vWLAN is only accessible on an item's edit menu, but the edit menus cannot be accessed on an HA node. To access this information the item must be viewed on the HA master.
- During the initial connection and authentication process, the web redirection on the Google Nexus 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 will never refresh. **Workaround:** Restart the browser to be directed to the designated webpage resource as expected.
- The UI may list the vWLAN gateway as 192.168.130.254 even if it has been properly assigned statically or via DHCP.
- When using the API to configure a Boolean attribute, 1 and true will evaluate to true and all other values will evaluate to false.
- Internal users may not properly time out resulting unresponsive UI.
- Certain 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.
- Bulk device upload may fail when a large import file is used. **Workaround:** Upload multiple smaller files.
- It is possible to create a Notification Template without a name.
- RADIUS Accounting Class Attribute is not sent.
- 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 may 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.
- The API can be used to create access groups without values for **login_form_id** or **role_id**. These are not valid configurations.
- In certain circumstances, client device information (OS, Type) may be missing from the Active Users view until the client performs a DHCP event.
- The Called Station ID format is inconsistent with RADIUS web authentication and 802.1X.
- If the default admin's password is changed through the link in the top right of the page, the standard **Please change the default admin password** platform task will not be removed. In this case the admin task can safely be deleted.
- Chromebooks cannot connect to an 802.1x SSID after connecting to a PSK SSID. **Workaround:** Disable automatic connection on the PSK SSID.
- Changing any of the SNMP root settings (communities, contact, description, location, system name) from their default values causes unexpected behavior. If SNMP is to be used, these should be left as defaults.
- If an AP is manually edited and a non-native Location is selected, the AP may not discover locations correctly.
- CoS priorities are displayed on the role create and edit menus even when the priority override is not set to one of the static options. When a non-static option is selected the priority fields are ignored.
- DataTables warnings are displayed on new vWLAN deployments.
- The Client Count by Device Type Over Time widget sometimes shows unknown/other devices. These messages can be ignored.

 

- The Client Count by Device Type Over Time widget shows device types that were not used over the widget's interval. These messages can be ignored.
- The Role matrix does not properly validate destination or device type. **Workaround:** Ensure destination and device types are valid.
- Occasionally, the first time an AP is moved to a domain it will ignore its configured radio powers. **Workaround:** Reconfigure the radio powers.
- Admin tasks to restart specific processes are not cleared after vWLAN has been restarted or rebooted. In these cases the tasks can be safely ignored and deleted.
- Due to restrictions in ETSI (specifically, channels 36 to 64 are not allowed outdoors in Europe), ADTRAN strongly recommends against mixing mesh APs that are designated as Indoor and Outdoor. Ensure all APs in the mesh are designated either one or the other.
- The web portal will occasionally load a blank page when an iPad user is manually selecting Google Chrome as the browser. This issue does not appear with the Safari browser or if the Captive Network Assistant feature is in use. Workaround: Use the Safari browser instead.
- Upon upgrading to 2.6, if you have a 1940 AP that is configured in an ETSI Regulatory Domain (i.e., Europe, Russia, etc.), that AP will be disabled for the 5 Ghz band. **Workaround:** Enable the DFS feature if installed outdoors, or mark the AP as Indoor (if installed indoors) to re-enable the 5 Ghz radio.
- In a mesh network, it is important that all APs have the same DFS capabilities (enabled or disabled) and are in the same regulatory domain. Consistent channel usage must be supported throughout the mesh, because APs can dynamically change channels when RADAR is detected.
- The Admin is Not Alerted When Bulk Device Upload File Contains Invalid Accounting Server. The Admin must ensure the accounting server is valid.
- APs configured for Mesh mode do not allow an AP traffic capture.
- Validation pop-ups have incorrect punctuation at the end of some messages.
- During the wizard flow, the tab key does not function to progress through the menus. **Workaround:** Use the mouse instead.
- When using a wired access group, for best results you should always specify a roaming SSID.
- If a client is associated to an SSID that does static web authentication and a non-default language is selected from the dropdown on the login page, the language on the login page is changed correctly and the post-login page will be in that language. If the client is disassociated and re-associated, the login page will be back in the default language and if a different language is not selected from the drop down, the post-login page will still be in the non-default language selected earlier.
- During the initial connection and authentication process, on Samsung Focus devices running Windows Mobile 7.5, the device will receive a NAC address and be immediately directed to the captive portal login page and the user can enter credentials as expected. However, with this device or OS there is a delay in negotiating an IP address and the web redirection will fail. It will take up to approximately one minute for the device to negotiate a proper IP address. After this process completes, if the user restarts the browser they will be directed to the designated webpage resource as expected.
- After being redirected to login with Captive Portal, iPad 3 (iOS 8.1) and iPad 2 (iOS 7.1) sometimes have issues with redirection to the originally requested site.
- The BSAP 1800 AP that has a tag that states it is a Model 1800 shows up as a Model BSAP-1840 in the UI. The Model 1935 that has a tag that states it is a Model 1935 shows up as a Model BSAP-1930 in the UI.

 

- Even when disabled, Captive Network Assistant may still pop-up when certain Apple devices try to connect.
- Even though a user is assigned to a role based on LDAP server authentication rules, users can still authenticate outside their schedule but cannot pass traffic.
- The Netstat utility output header in the GUI does not match the output header in the SSH session.
- Preview web portals will not respond to the change language drop-down list. Deployed web portals will correctly change the language.
- Preview web portals will not respond to the change password link. Deployed web portals will allow changing passwords.
- During the initial connection and authentication process, the web redirection on Google Nexus 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 will never refresh. **Workaround:** Restart the browser to be directed to the designated webpage resource as expected.
- The API cannot be used to configure the AP's Channel to Auto.
- The API cannot be used to back up or restore the configuration.
- Under extremely heavy loads, some user links on the Active User status page will not be abbreviated to MAC addresses, and those clients will never drop from the system. **Workaround:** Drop the clients manually.
- When upgrading vWLAN from 2.4 to 2.5, the upgrade can take a long period of time (an hour or longer) because all dashboard data is preserved during the upgrade. The data is restored after the reboot, so the system will not be responsive to ping or web requests during this time. When upgrading a large system (with multiple domains and many users), consider a High Availability pair (now an included feature in 2.4), and then upgrade the primary fully before the backup. Alternately, consider a long control channel timeout so Wi-Fi still functions when the box is down and upgrading.
- An API GET request on service_groups does not return child services.
- An API GET request on destination_groups does not return child destinations.
- When initiating an AP traffic capture, the variables associated with the capture are reset in the UI. This means that the settings shown do not reflect the settings for the capture that is currently running.
- When the time in seconds before inactive connections are dropped is configured, devices are not dropped at appropriate time.
- The API may become unresponsive if used from multiple sources simultaneously. It will become responsive again after a few minutes.
- Email notifications are not being created and sent when the Secondary vWLAN server goes off line, when it comes back on line, or when a location is created and used that points to a location that cannot be reached.
- The performance of the UI can suffer if the API is being heavily used.
- Under heavy load, AP and client counts may be incorrect for a period of time but they will be corrected.
- 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. Implementing HA or a high Control Channel timeout will alleviate this issue.
- Modifying the columns of any table with the **show/hide columns** button will cause the table to resize improperly. Refreshing the page will correct this.

 

- Very rarely, vLocations may appear in the GUI, but not the User Management process. Restarting the Interprocess Communication Daemon will fix this.
- The native AP VLAN Location should be a read-only field, but currently it can be edited.
- Expanding Unified Access Groups in the UI can result in the link being rendered incorrectly.
- While under heavy load, the GUI may report incorrect status information or sort the information improperly. The system will recover after a few minutes.
- The API may become unresponsive when a large number of APs are booting. The system will recover on its own after a few minutes.
- When using UI search fields, some searches may not complete with partial input.
- After deleting one or more AP licenses from the /platform/ap_licenses GUI page, the count below the table is not updated. Refreshing the page will correct this.
- If a user is logged into the UI looking at one domain and uses the API to get information from another domain the UI will display the AP and user counts from the domain accessed by the API, but the domain dropdown will still display the domain selected originally in the UI.
- The ability to preview a login form does not function properly when using the Opera browser. Other browsers function properly.
- After the administrator deletes items on a paginated tab, the pagination will be incorrect until the view is refreshed.
- For fast-roaming, adjacent APs must detect each other and add each other as neighbors. If APs are brought in at different times it's possible for neighbor detection to fail and roaming to take longer.
- For outdoor APs in Europe, there is a slight chance that upon RADAR detection the AP will start scanning an indoor-only channel. The system immediately corrects itself, but this can lead to a 90 second (versus 60 second) CAC check.
- Sometimes BYOD information will not be shown in the UI. It will show up after some time or when the client reconnects.

## Release Specific Upgrade Instructions

vWLAN 2.2.1 and newer systems can be upgraded to vWLAN 2.6.0, and all configurations will be maintained.


vWLAN 2.6.0 requires using Bluesocket Access Point (BSAP) firmware version 7.0.0. BSAP 7.0.0 is not backward compatible with previous vWLAN code versions. Step 4.2 on page 7 should be skipped when using this version.


If upgrading from vWLAN 2.1.x or a previous version, use the process outlined in the ***vWLAN 2.1 Upgrade Guide*** on ADTRAN's Support Community (https://supportforums.adtran.com/docs/DOC-5868) prior to the further upgrade to vWLAN 2.6.0.

 


For information on known misnomers to the Layer 7 Device Fingerprinting feature, please see https://supportforums.adtran.com/docs/DOC-7713.


Upon upgrading to vWLAN 2.6.0, if you have an AP that is configured in an ETSI Regulatory Domain the 5GH 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).

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

### Unsupported Features from vWLAN 2.1

The following features were supported in the non multi-tenant version of vWLAN (2.1) but are not currently supported in the multi-tenant version (2.5).

- **VW-2306** - Internal RADIUS 802.1X Server
- **VW-2204** - Dynamic Role Assignment Using Secondary LDAP/Active Directory Lookup after RADIUS. ADTRAN recommends using RADIUS attributes for dynamic role assignment instead of making a secondary lookup to LDAP/AD for best performance. ADTRAN will not port this functionality to the multi-tenant version of vWLAN.
- **VW-3165** - Expiration of MAC devices
- **VW-2205** - Credit card billing
- **VW-2209**, **VW-2208** - POP3
- **VW-2115**, **VW-3211** - Ability to automate AP jobs (e.g., reboots, dynamic RF calibration) and automate backups.
- **VW-3870** – Redirect to ports other than 80 and 443
- **VW-2198** - Ability to import/export local users and APs
- **VW-3841** - Admin Access Allow Control List

If you rely on any of the features above, you must either find a suitable replacement/workaround or wait until a future release of vWLAN when these features are available. Contact ADTRAN Technical Support for suggestions.

## AP Licensing

The vWLAN appliance includes a flexible access point (AP) licensing model where the customer purchases licenses for individual APs. The appliance ships with no AP licenses.

### Licensed Features

One or more of the following features can be selected when licensing vWLAN:

 

1. vWLAN AP license - required for the AP to enable its radio and service wireless clients. Without this license, the AP does not function.
2. Wired - enables support for wired users and users on third-party APs. Wired licenses can be enabled on a per AP basis.

### Obtaining AP Licenses

AP licenses are purchased by the customer. Upon purchase, Activation Keys are sent to the customer via email. Activation Keys are not yet activated against any serial number. The customer must perform the activation process to obtain the license file. The customer would simply apply the Activation Keys to the hardware serial numbers they wish to license using the ADTRAN Licensor found at www.adtran.com/licensing. The license process will also register the hardware to the email address tied to the customer's ADTRAN login.

#### Process Overview

1. Log into www.adtran.com/licensing using the email address you want registered to the hardware
2. Enter the SERIAL NUMBER, ACTIVATION KEY pair(s) into the licensing tool
3. Download the license file
4. Apply the license in vWLAN

To download a license file again later, simply enter the serial number into the licensing tool.

For more instructions or to watch a video detailing bulk licensing methods, please visit the ADTRAN Support Community: *https://supportforums.adtran.com/docs/DOC-7021*.

For detailed information about applying licenses to vWLAN for Bluesocket Access Points, please visit the ADTRAN Support Community: *https://supportforums.adtran.com/docs/DOC-5017*.

You may verify eligiblity for ADTRAN Technical Support at the following link: *http://www.adtran.com/web/page/portal/Adtran/wp_support_eligibilty*.

For assistance with licensing, or technical support of your Bluesocket product, please open a support case at *www.adtran.com/supportcase*.

## Documentation Updates

The following documents were updated or newly released for vWLAN 2.6.0 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*
- *Configuring DFS in vWLAN*
- *Configuring Layer 7 Device Fingerprinting in vWLAN*

 