RELEASE NOTES

vWLAN 2.5.0
October 31, 2014

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 4
Supported Models 4
AP Licensing 4
System Notes 5
Upgrade Instructions 6
Features and Enhancements 10
Fixes 10
Errata 12
Documentation Updates 15

Introduction

vWLAN 2.5.0 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 12*.

A list of new or updated documents for this release appears in *Documentation Updates on page 15*.

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 2.5.0.

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

AP Licensing

The vWLAN appliance includes a flexible access point (AP) licensing model where the customer purchases licenses for individual APs. By default, 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 or per site 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*.

System Notes

vWLAN 2.5.0 is a software release that manages, configures, controls, and secures Wi-Fi access points (APs), the radio frequency (RF) spectrum, and users, across a 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. Many other improvements were made to the software in vWLAN 2.5.0.

To use vWLAN, two products are required - the vWLAN solution itself and Bluesocket access points.

VMware Memory Requirements

As of vWLAN version 2.4.0.12, VMware deployments require 6GB of memory assigned to vWLAN.

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-2202** - Role-based Network Access Schedules
- **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, MAC devices, APs, authorized stations
- **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.

Upgrade Instructions

vWLAN 2.2.1 and newer systems can be upgraded to vWLAN 2.5.0, and all configurations will be maintained.

> **NOTE** vWLAN 2.5.0 requires using Bluesocket Access Point (BSAP) firmware version 6.9.0. BSAP 6.9.0 is not backward compatible with previous vWLAN code versions. Step 4.2 on page 7 should be skipped when using this version.

vWLAN 2.1 systems can be upgraded to vWLAN 2.5.0, but certain features are not supported and some settings must be reconfigured when upgrading to vWLAN 2.5.0. These are outlined in *Unsupported Features from vWLAN 2.1 on page 5*. It is important to review these prior to beginning the upgrade process.

Upgrading ADTRAN products to the latest version of firmware is explained in detail in the *vWLAN 2.2.1 Upgrade Guide*, available at https://supportforums.adtran.com.

> **NOTE** If upgrading from vWLAN 2.1.x or a previous version, use the process outlined in the ***vWLAN 2.1 to 2.3.0 Upgrade Guide*** on ADTRAN's Support Community (https://supportforums.adtran.com)

To upgrade your vWLAN Virtual Appliance follow these steps:

Step 1. Download the vWLAN software, access point (AP) firmware, release notes, and other documentation. These files are available from http://support.adtran.com unless otherwise specified:

- vWLAN Version 2.5.0 software image (2.5.0)
- 6.9.0 AP firmware for the appropriate AP models
- vWLAN version 2.5.0 Release Notes (available in download area at http://support.adtran.com)
- vWLAN version 2.5.0 Admin Guide (available in the Support Community at https://supportforums.adtran.com)

Step 2. Review the release notes and other documentation.

It is important to take the time to closely review the Release Notes to become familiar with the new features and improvements, resolved issues, upgrade considerations, and open errata in this release.

Step 3. Back up the previous vWLAN version.

1. In the secure web-based administrative console of vWLAN go to the **Administration** tab and select **Backup/Restore**.
2. Select **Back up all domains** and click **Run.** Be sure to store your backup configuration in a safe and secure place.

Step 4. Install the AP firmware for the appropriate AP models on vWLAN.

1. Upload new AP firmware and apply to an AP template:
   a. Navigate to the **Configuration** tab and select **Wireless > AP Firmware**.
   b. If you are uploading firmware for a domain, select the **Domain** tab. If you are uploading firmware for the vWLAN platform, select the **Platform** tab.
   c. To upload the new AP firmware, select **Create AP Firmware** at the bottom of this menu.
   d. Select the new firmware file from the location in which you stored the downloaded firmware by selecting **Browse**.
   e. Select the domains to which to apply the new AP firmware by using the + (plus) sign. If you are uploading to the domain view, the AP firmware will automatically be available in the domain.
   f. Choose the template(s) to which to apply the firmware change.
   g. Select **Create AP Firmware** (or **Update AP Firmware** if editing) to apply the changes. A confirmation is displayed indicating that the AP firmware has been successfully created or updated.
2. This step should only be taken if the AP firmware is backward compatible with older versions of vWLAN. Apply the new or updated firmware to the AP by running the following domain tasks: **Must apply configuration to APs** and **Must activate new AP firmware** (in the case of 19XX model APs)**.** Upgrade status can be monitored in the secure administrative GUI by navigating to **Access Points** on the **Status** tab.

Refer to the BSAP Release Notes for further details on the BSAP firmware.

Step 5. Upgrade vWLAN using the vWLAN version 2.5.0 software image file.

1. In the secure administrative GUI console of vWLAN, go to the **Administration** tab and select **Platform Upgrade**.
2. Making sure **Maintain Current Configuration** is selected, browse for and select the vWLAN software image.
3. Select **Run Task.** After the upgrade is complete a message will be displayed indicating the upgrade is complete and that the system is pending a partition switch.
4. Select **Platform Tasks** in the top menu, and execute the P**ending partition switch – must reboot vWLAN** task.

Upgrade Considerations

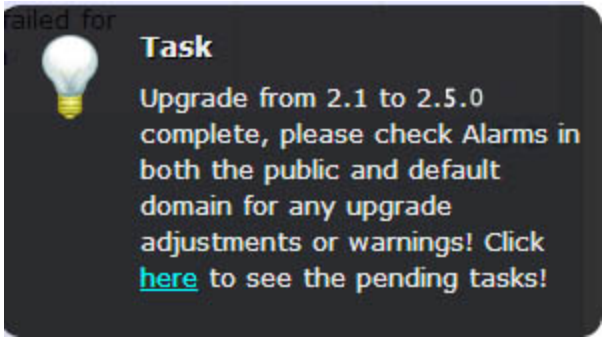
The following section is applicable when upgrading from vWLAN 2.1 to vWLAN 2.5.0.

1. The administrator's user interface (UI) at **https://**<*IP address*>**:3000**, where <*IP address*> is the address of the unit regardless of the 2.1 setting.
2. When upgrading to vWLAN 2.5.0, previously configured administrators are removed. After upgrading there will be one default administrator, **root@adtran.com**, with a password of **blueblue**. New administrators can be created under 2.5.0 (using the granular model).
3. AP firmware is not included in the vWLAN image. The AP firmware must be loaded on vWLAN for APs to boot properly.

4. Any local (overriden template) AP settings (those not configured at the AP Template level) are not retained.
5. Role-based inherited firewall policies are not retained.
6. Disabled MAC devices are not retained.
7. All local user expiration (or enablement in the future) must be reconfigured.
8. Internal 802.1X service set identifiers (SSIDs) are not brought forward. Backup 802.1X servers must be reconfigured.
9. Logs, reports, alarms are not brought forward.
10. All notifications and email settings must be reconfigured or the default values to which they revert can be used.
11. vWLAN 2.5.0 uses a new application programming interface (API), representational state transfer (REST), and all API-based apps must be rewritten. Refer to the administrative guide.
12. The VMware system requirements differ from 2.1 to 2.5.0. Release 2.5.0 requires a new Open Virtualization Archive (OVA).
    a. The VM memory and CPU recommendations have changed between 2.1 and 2.5.0. It is recommended that 4 cores and 6 GB of RAM be used for 2.5.0.
    b. The VM file system requirement has increased from 2.1 to 2.5.0. A vWLAN 2.1 Virtual Machine with a 7 GB footprint cannot be upgraded directly to 2.5.0. Instead, a new 2.5.0 OVA (41 GB footprint) must be deployed. Your options are:
        i. Reconfigure the system from scratch.
        ii. Downgrade the new OVA to 2.1, restore the 2.1 configuration there, and then upgrade to 2.5.0. For more details refer to the *vWLAN Upgrade Guide* available at https://supportforums.adtran.com.

Tracking Upgrade Alarms

During the upgrade from 2.1 to 2.5.0, the vWLAN system will adjust the configuration of the system. In certain cases, incongruent data may be present on the 2.1 system (for example, a custom login page without a Guest Role selected) which is no longer valid from 2.3.0 forward. After the upgrade, this administrative task will display as a popup:



Or it will appear under the Admin Tasks view:

> Upgrade from 2.1 to 2.5.0 complete, please check Alarms in both the public and default domain for any upgrade adjustments or warnings

If you then click on the Alarms view, you will see a message similar to this:

Failed to update LoginForm error Validation failed: Role Not a valid role, Role Not a valid role update varLoginForm1 = LoginForm.find_or_create_by_id!1, noleft => 0, login_attempts_minutes => 1, name => Default, hotspot_account_id => 1, r_t_padding => 74, title => Wireless Network Log In, r_width => *, enable_tos => , powered_by => loginPower-black.gif, redirection_destination => destination, redirection_externaldestination

The error will describe the problem. In this case, Login Form with ID 1 had an invalid role and therefore, was not imported. This could cause other issues as well. If the issue is minor and can be fixed, you can adjust your configuration under 2.5.0. Otherwise you can note all issues, revert to version 2.1, resolve the issues under your 2.1 configuration, and upgrade again.

Required BSAP Firmware

vWLAN 2.5.0 requires using Bluesocket Access Point (BSAP) firmware version 6.9.0.

BSAP Interoperability and Performance

802.11n 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 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 2.5.0.

- Support for Mesh on BSAP 1900 series
    - Point-to-point Bridging
    - Point-to-multipoint Bridging
    - Multiple Hop Mesh
    - Ethernet Port Bridging
- Support for new 2030 Series 802.11ac 3 stream indoor APs
- Support for new vWLAN Desktop Appliance
- Enhanced platform information and AP specific information now available via SNMP (Enterprise-specific MIBs)
- Ability for internal user to change password via captive portal
- Added username column to "Top Clients" widgets
- Ability to add static routes to vWLAN to manage vWLAN via Management or Public interfaces from remote network
- Removed validation from SIP2 admin and password field as some SIP2 implementations do not support "93 admin login"
- Set default value of 14400 seconds (4 hours) for control channel timeout so out of the box access points will continue to service clients for 4 hours if the control channel between the access point and vWLAN is down
- Enhanced external redirects to 3rd party captive portals
    - Ability to add radius option and AP status parameters
    - Ability to enable/disable double encoding of parameters
- Added "Aggressive DHCP least time for unregistered clients" setting under configuration>system>settings>domain. This adjusts the DHCP lease time/redirect_pause from 10/15 to 8/12. An aggressive lease time brings clients on faster after authentication but may not be compatible with all handheld devices
- Enhanced API to find all users on a specific AP

Fixes

This section highlights major bug fixes in vWLAN 2.5.0**.**

- The RADIUS accounting process on vWLAN stopped which resulted in accounting messages not being sent to the Radius Accounting Sever.
- In some cases hard drive space could have been mismanaged so that the disk would become full, causing a loss of vWLAN functionality.
- Internal process errors resulted in the Admin UI becoming sluggish.
- Replication failed when admin updated an account's password with an invalid password (fewer than eight characters).

- Creating a PSK with fewer than eight characters caused the SSID to be unusable along with other SSIDs associated with the template used by the SSID.
- When configured to redirect to an external captive portal server, a user that failed to authenticate (e.g., incorrect credentials) received the default (local to the vWLAN) captive portal form and was not redirected again to the external captive portal server.
- Secondary LDAP and/or RADIUS web authentication did not occur when Redirection To An External Captive Portal Server was configured.
- Acquiring a snapshot on the High Availability node would overwrite SSL certificate values with those from the master.
- The Location Discovery process would not finish until the User Management process was restarted.
- After a domain was restored, the UI would not properly display certain statuses.
- When a Custom Interval was set for Dashboards, the Dashboard would not render the Date Range correctly.
- Guest User Accounts were not expiring after logging out and logging back in.
- The private key for the self-signed certificate is regenerated in response to Heartbleed vulnerability.
- User management could sometimes crash during roaming activity.
- MAC authentication clients were tunneled between access points if location changes were made after the client was authenticated.
- In certain cases, when APs were connecting, the TCP connection failed and the AP disconnected causing an internal process to crash. This caused secondary crashes to subscribed processes.
- The Shared Secret/Password field in an authentication server would appear to be empty even though the shared secret/password was input correctly.
- The OpenSSL version was upgraded to address the Heartbleed vulnerability (CVE-2014-0160).
- The internal reporting process would queue information but be unable to write to the database resulting in a memory leak and some reporting information being unavailable.
- It was possible for a process to restart leaving invalid client entries in the Status > Clients table in the UI.
- AP radios were reported as off until the vWLAN is rebooted.
- APs reverted unexpectedly from HA Node to HA Master.
- The Access Point User Manager process would restart causing a loss of network connectivity for clients.
- Locations were not being populated in the user interface.
- APs reverted unexpectedly from HA Node to HA Master.
- Improved performance of search capability within vWLAN.
- Invalid CIDR notation in a Location caused clients to be placed in the incorrect VLAN.
- After upgrading, the HA node had a Platform Task indicating to Upload AP firmware and change the Admin Password.
- Resolved some issues with internal processes such as User Management that could result in authentication failing, APs rebooting, or no impact to the client at all.
- The Search capability could not be used under the Administrators tab.
- APs were reported as Down in the Administrative UI while they were still servicing clients.
- Clients were tunneled even though both the AP and vWLAN had active locations.

- Under certain conditions, minor configuration changes to an AP Template would result in the crash of an internal process.
- When using RADIUS Admin Auth, the Dashboard modifications did not persist across logins.
- System memory threshold exceeded events reported in system logs were false.
- Locations reported on the AP and vWLAN did not match which caused users to be tunneled.
- On a secondary HA unit, an Admin Task **Please change the default admin password** would appear even though the admin password could only be changed on the primary HA unit.
- The AP redirected to the PTR record found regardless of the Redirect to Hostname option configured in vWLAN.
- When using External Redirects, the vWLAN would send a different string to the external server based on the port to which users were destined.
- In large deployments, it was possible that clients could not authenticate until the Access Point User Manager service on the vWLAN was restarted.
- Occasionally, a user would persist in the Clients tab long after the user had left the system.
- The Message and Last Calibration columns were missing from the Access Points page.

Errata

The following is a list of errata that still exist in vWLAN 2.5.0.

- Disable the use of SSLv3 to prevent vulnerabilities associated with it (specifically CVE-2014-3566).
- The Current Active Users by Radio Mode widget shows a null value.
- A duplicate 802.1X authentication server can be created but not edited.
- Internal Users may timeout before the set expiry time is reached.
- An AP may render incorrect available SSIDs when attempting a wireless packet capture.
- Downloading large numbers of logs can cause the UI to become unresponsive.
- If a user does not have Domain Level Admin Task Read Permissions they cannot log into the Admin UI if there is a task ready.
- 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.
- The UI is not properly rendering the page in Google Chrome.
- Setting a vary large value in the System Settings > Timeout Value for Web Server can cause the Captive Portal to run out of available web sessions. This field is now limited to 30 seconds.
- Internal users can stop timing out and the box CPU will be high. **Workaround:** Restart the User Account Monitor.
- 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 them manually.
- Guest users cannot be deleted from guest_users using the API.
- When upgrading from 2.1 to 2.5, if a Login form does not come forward, then any AP Template using that form may also not transfer. **Workaround:** Pay close attention to the alarms and adjust your configuration accordingly.

- In vWLAN 2.5, Auth Rules do not allow a final role of Un-registered. Any Auth Rule from 2.1 with a final role of Un-registered will be dropped when upgrading. Revisit your authentication strategy if you see this upgrade alarm.
- During the upgrade from 2.1 to 2.5, if destinations are not brought forward due to other errors (such as mismatched networks), then a destination group might also have an error. Review and rebuilt the group as needed.
- vWLAN 2.5 only supports OUI based Wildcard MAC devices. Any non-OUI wildcard MAC devices are discarded (with an error) during the upgrade.
- When upgrading from 2.1 to 2.5, the Dynamic RF Power Threshold Index must be between 1 and 199. If it is not, the default value of 100 is used. If you have been using a value over 199, use 199 for the 2.5 release. An alarm is shown with this error.
- When upgrading from 2.1 to 2.5, if you have a Destination Network, the netmask must match the network. For example, 192.168.0.1/255.255.255.0 does not work, the value must be 192.168.0.0/255.255.255.0. Either edit the Destination before or after the upgrade. An alarm is shown if the upgrade rejects the value.
- When upgrading from 2.1 to 2.5, if your firewall rules contain references to destinations or groups that do not exist, an upgrade alarm is given. Review any alarms and confirm the roles have the proper firewall rules. Recreate the rules as they should be (as likely the 2.1 configuration was in error).
- The Access Points page (Status > Access Points) cannot be sorted by the Total Clients column.
- vWLAN requires having the proper time configred, as items like logs, dashboard reports and alarms require it. When upgrading from 2.1 to 2.5, if you do not have an NTP server configured, you will receive an upgrade alarm (after reboot). At this point, the default NTP servers will be configured. Modify these as desired.
- When upgrading from 2.1 to 2.5, the administrator root CA URL must be valid (such as www.adtran.com) and not contain a wildcard (such as *.adtran.com). If the URL is not valid, the setting is not brought forward and a warning is given.
- AP licenses that do not contain a valid vWLAN license will not migrate from 2.1 to 2.5. Licenses for regulatory domains that are not supported in 2.5 will not migrate. See your sales representative for the proper license based on your regulatory domain.
- When upgrading from 2.1 to 2.5, if you are fully customizing the login page and specify the **noleft** login page - do so with a number (0 or 1) versus a letter such as o. Otherwise the page will not carry through.
- During a 2.1 to 2.5 upgrade, it is possible that Access point configurations will not be maintained for several reasons. If this happens, edit the AP and restore the configuration of your choosing. Reasons include:

  1) Regulatory Domain license is not valid in 2.5 - contact your sales representative for a valid license.

  2) Duplicate AP name - 2.5 requires AP hostnames to be unique - choose a new name for the AP.

  3) The AP does not appear in the proper place or is off the border of a map - place the AP onto the proper map/location.
- Changing the IP address in an active Radius1xAuthServer does not generate a Domain Task.

- 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 during this time. When upgrading a large system (with mulitple domains, and many users), you should consider a High Availability pair (which is free in 2.4), and then upgrade the primary fully before the backup. Alternately consider a long control channel timeout so the wireless is usable 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 upgrading from 2.1 to 2.5, the control channel timeout is set to 4 hours (14,400 seconds) so that by default, in the event the management and control channel between the APs and vWLAN goes down, the APs will continue to service clients for 4 hours. Since Standby SSIDs are only supported with a control channel timeout of 0, they are not maintained when upgrading from 2.1 to 2.5. If Standby SSIDs are necessary, please set the control channel timeout to 0 and recreate the Standby SSIDs.
- If during an upgrade from 2.1 to 2.5, an illogical message such as **Failed to update LoginItem error Is a directory - /alternative//var/local/logs** appears, it is likely caused by an engineer who is doing debug on your box. The error can be safely ignored.
- In 2.5, you can only have one unique authentication server (i.e. RADIUS 1x) for a single IP address. If you have multiple servers (when upgrading from 2.1), all but the first is lost. In 2.5, you can use RADIUS attributes to match different filter rules and derive different roles for the same Auth Server/SSID.
- In 2.5, SNMP community names must be between 6 and 20 characters (per the standard). Names that do not meet this requirement are lost when upgrading from 2.1, and are replaced by the 2.5 defaults (public/private).
- If DNS is not available during the upgrade from 2.1 to 2.5, servers that used hostnames (such as ldap.university.edu) will not be brought forward during the upgrade. Ensure that DNS is available and the server names resolve.
- When upgrading from 2.1 to 2.5, if you have a Login form that does not have a Guest Role selected, the Login form will not migrate. Any referenced images that are missing will also not migrate and could prevent the Login form from migrating.
- If you have more than 1500 APs, consider using multiple domains. You can split the APs up by physical location or logical grouping. This allows you separately configure and manage devices without interfering with others.
- After you select the AP you want to look at and begin the capture, it immediately resets to the first AP in the line (visually confusing), even though the capture is looking at the AP you previously selected. It also resets to "Wired" as soon as you start it after you have selected "Wireless."
- Captive Portal may fail to load when Redirect HTTPS Traffic for Unregistered Clients is enabled.
- When the "Time in seconds before inactive connections are dropped" is configured, devices may not drop at the time configured.
- The User Manager service will restart unexpectedly.
- The API may become unresponsive if used from multiple sources simultaneously. It will become responsive again after a few minutes.
- When upgrading from 2.1 to 2.5, you may have to reboot some BSAP-18x0 series APs an additional time for them to be fully upgraded.

- 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 but cannot be reached.
- When upgrading a large database (with many historical records and/or domains), the system can take up to an hour to come up after an upgrade. Implementing HA or high Control Channel timeout will help 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, Locations may appear in the GUI, but not in the User Management process. Restarting the Interprocess Communication Daemon will remedy this situation.
- 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.
- After deleting one or more AP licenses from the platform>ap_licenses GUI page, the count below the table does not update. Refreshing the page will correct this.
- The login form preview does not function properly when using the Opera browser. Other browsers function properly.
- If the administrator deletes items on a paginated tab, then pagination will be incorrect until the view is refreshed.
- New installations of vWLAN 2-2-1-20 with vPatch-2-2-1-20-2 display a duplicate DHCP Server service.
- For fast-roaming, adjacent APs must detect 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.

Documentation Updates

The following documents were updated or newly released for vWLAN 2.5.0 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*
- *Mesh Network in vWLAN*

