RELEASE NOTES

vWLAN 2.3.0
August 12, 2013

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 2.3.0 is a major system release that adds new features and addresses customer 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 13*.

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 2.3.0.

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

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. High Availability - enables zero packet loss failover. High availability can be enabled on a per AP or per site basis, to allow more high-profile tenants to have failover, while others do not.
3. Wired - enables support for authenticating 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, and are generated as a text file which is then sent to the customer. For new APs, these licenses come from the reseller or distributor. For replacement APs, the licenses will come from ADTRAN Customer Care. APs are initially in an unlicensed state. AP radios will not be operational until the AP is licensed by uploading the license file to vWLAN.

If a license was not received for a new AP, contact the reseller or distributor where the AP was purchased. If a license was not received for a replacement AP on an return merchandise authorization (RMA) generated by ADTRAN, contact ADTRAN Customer Care at 888-423-8726, and reference the RMA number.

System Notes

vWLAN 2.3.0 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 2.3.0.

To use vWLAN, two products are required - the vWLAN solution itself and Bluesocket 802.11n access points. Certain features from vWLAN 2.1 were removed from vWLAN 2.3.0 until they can be supported under the multi-tenant architecture.

Unsupported Features from vWLAN 2.1

The following features were supported in vWLAN 2.1 but not supported in 2.3.0.

- **VW-3722** - Time Based Licenses
- **VW-2306** - Internal RADIUS 802.1X Server
- **VW-2204** - Dynamic Role Assignment Using Secondary LDAP/Active Directory Lookup after RADIUS
- **VW-3165** - Expiration of MAC devices
- **VW-2205** - Credit card and PMS billing
- **VW-2209**, **VW-2208** - POP3
- **VW-2202** - Role-based Network Access Schedules
- **VW-3954** - Polling vWLAN via SNMP for AP Specific Information
- **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-3902** - Ability to override a role a user is in under Status>Active Users
- **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 systems can be upgraded to vWLAN 2.3.0, and all configurations will be maintained.

vWLAN 2.3.0 requires using Bluesocket Access Point (BSAP) firmware version 6.7.0.

vWLAN 2.1 systems can be upgraded to vWLAN 2.3.0, but certain features are not supported and some settings must be reconfigured when upgrading to vWLAN 2.3.0. 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.

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 2.3.0 software image (V2_3_0_09.img)
- 6.7.0-17 AP firmware for the appropriate AP models
- vWLAN version 2.3.0 Release Notes (available in download area at http://support.adtran.com)
- vWLAN version 2.3.0 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 6.7.0-17 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. 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 2.3.0 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 version 2.3.0 software image (V2_3_0_09.img).
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 2.3.0.

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 2.3.0, 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 2.3.0 (using the granular model).
3. AP firmware is not included in the vWLAN image. As of vWLAN 2.2.x, the AP firmware must be loaded on vWLAN for APs to boot properly. If you are upgrading from 2.2.1, you can optionally first upgrade the APs to 6.7.0 in 2.2.1. Then they will retain the firmware and function in 2.3.0.
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 2.3.0 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 2.3.0. Release 2.3.0 requires a new Open Virtualization Archive (OVA).

    a. The VM memory and CPU recommendations have changed between 2.1 and 2.3.0. It is recommended that 4 cores and 4 GB of RAM be used for 2.3.0.

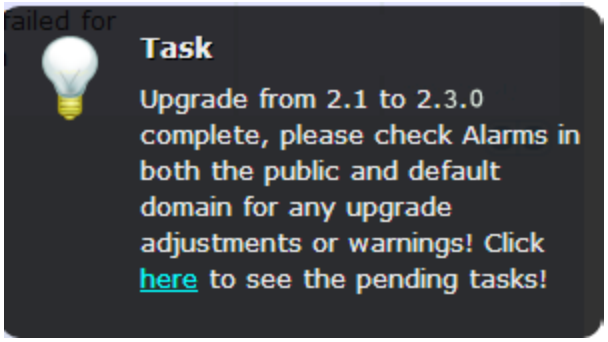
    b. The VM file system requirement has increased from 2.1 to 2.3.0. A vWLAN 2.1 Virtual Machine with a 7 GB footprint cannot be upgraded directly to 2.3.0. Instead, a new 2.3.0 OVA (41 GB footprint) must be deployed. Your options are:

        i. Reconfigure the system from scratch.

        ii. Downgrade the new OVA to 2.1, restore the 2.1 configuration there, and then upgrade to 2.3.0. 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 2.3.0, 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 2.3.0 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 2.3.0. 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 2.3.0 requires using Bluesocket Access Point (BSAP) firmware version 6.7.0.

BSAP Interoperability and Performance

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

1. Use WPA2 (PSK or 802.1X) with advanced encryption standard (AES) when connecting 802.11n-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 client's performance.
2. Enable 802.11n Wireless Mode, 40 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 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 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 2.3.0**.**

- Added the ability to maintain IP addressed after restoring a configuration file.
- Added the ability to upload images such as WPAD, terms of service HTML, miscellaneous HTML help pages, etc.
- Added the ability to renew the SSL certificate without affecting the currently installed certificate.
- Enabled the display of certificate information (such as, OCSP and CRL URLs) in the UI.
- Added a column to Active User status that identifies associated APs by their configured name instead of MAC address.
- Added support for vWLAN side traffic capture under Multitenant.
- Added support for Apple CNA and Microsoft NCSI.
- Enhanced the search and sorting capabilities.
- Enhanced status notifications to include the AP host name (rather than the MAC address) in all views , the name and IP address of the AP for an active user, and User count per Role widget.

- Added the Login page preview.
- Added an audit trail for all administrator's changes.
- Enhanced the RF collector to avoid duplicate alarm detection, ensure SnR integrity, and purge logs faster.
- Enhanced security for SQL injection and send file vulnerability.
- The scale on vWLAN Virtual Appliance for VMware was increased by removing the hard maximum limit of 1500 access points (APs). The ability to scale APs and users for the vWLAN Virtual Appliance on VMware is based on the VMware server's hardware (CPU/cores, memory). The VMware server resource requirements dedicated to vWLAN Virtual Appliance for 1500 AP deployment are 4 CPUs/cores and 4 GB memory. Additional APs and users can be supported by dedicating additional CPUs/cores and memory to the vWLAN Virtual Appliance. The number of tenants cannot be scaled based on hardware and remains at the hard maximum limit of 50.
- The client density was increased on the BSAP 1900 Series by removing the hard maximum limit of 64 associated clients per radio. The maximum associated clients per radio on BSAP 1900 Series can now be configured to values greater than 64 with a default value of 64. The hard maximum limit of 64 associated clients per radio remains for the BSAP 1800 Series.

  The maximum associated clients per radio should be chosen carefully based on the per-user bandwidth requirement of the applications in use on the network. For example, in a greenfield deployment with 802.11n radios and 3 stream clients only, the maximum data rate is 450 Mbps. However, actual throughput is typically 50 to 60 percent of the maximum data rate, or around 270 Mbps in a clean RF environment with no interference. Keeping in mind that Wi-Fi is a shared medium, all the clients that are associated to the radio will be sharing an actual throughput of 270 Mbps. Therefore, if the applications have a per-user bandwidth requirement of 1.08 Mbps, up to 250 clients per radio can be supported. If the applications have a higher per-user bandwidth requirement, 10 Mbps for example, only 27 clients per radio can be supported. Note that this scenario is based on a best case greenfield deployment with 802.11n radios and 3 stream clients only, in a clean RF environment, with no interference. Single stream 802.11n clients will have a maximum data rate of 150 Mbps, dual stream 802.11n clients will have 300 Mbps, and legacy 802.11a/g clients will have 54 Mbps. If there is a mixture of client types (single stream, dual stream, and legacy) on the network, you should plan for the most prevalent client type.

  While the maximum associated clients per radio on BSAP 1900 Series can now be configured to values greater than 64, it is important to remember that Wi-Fi is a shared medium. The more users associated to the radio, the lower the throughput for each user to share from the pool of available bandwidth. Customers should plan accordingly for coverage AND capacity (client density), not just coverage. Areas with high user density, such as libraries, cafeterias, lecture halls, conference centers, etc., that may only require one access point for coverage purposes, may require multiple access points for capacity purposes.

Fixes

This section highlights major bug fixes in vWLAN 2.3.0.

- vWLAN only supported 1168 MAC devices, and if overloaded, locations could not be discovered.
- The unit was unable to load the secure GUI administration interface or login page for web authentication. The unit was able to associate to the SSID but not to pass traffic.
- For 802.1X auth, the comparison operators **start with**, **end with**, and **contain** did not function with non-alpha numeric expressions with backslash (\).

- After the administrator login page loaded successfully and valid credentials were entered, an error was returned.
- If no DNS server was entered in the AP template, it caused the APs to reboot.
- 802.1X users were not transitioned to their final role after a Radius-Accept until all processes were restarted.
- The Self Signed Certificate's common name displayed as **_default_** for clients being redirected to the Public IP of the vWLAN (behind NAT).
- When APs were licensed for Australia, certain DFS channels could be selected but SSIDs would not broadcast on these channels.
- LDAP over SSL authentication would fail.
- Printing an Internal User caused HA to become unsynchronized.
- Guest users were deleted from the system before the cleanup time configured in the plan was reached.
- When an administrator located in a time zone ahead of UTC created a report with a stop date in their time zone (i.e., greater than UTC), it failed with a form validation error.
- It was not possible to create more than 400 locations.
- The AP's host name was not included in email notifications.
- If a non-trusted certificate authority (CA) signed the mail server's certificate, email notification delivery failed on the vWLAN because the certificate could not be validated.
- Migration from 2.1.0.14 to 2.2.1.20 failed to migrate the NTP host as FQDN in 2.1.0.14.
- Migration from 2.1.0.14 to 2.2.1.20 failed because the 2.1.0.14 login image could not be found.
- Migration from 2.1.0.14 to 2.2.1.20 failed due to an invalid color in 2.1.0.14 web login form configuration.
- If a range of ports was configured in a service and applied to a role, the APs would not receive a configuration.
- It was not possible to switch partitions using the console menu option.
- New users were not added to the connections table.
- Option c (certificate cleanup: Removes any custom web server certificate) in the console menu did not remove any custom web server certificate.
- If a PEM encoded X509 certificate was entered (in **Configuration > Settings > Platform > Certificate File**) with typographical errors that made the certificate unreadable, the administrator GUI could not be restarted and would remain unavailable.
- Users were not added to the connection table and the user count in UI Active Users did not accurately reflect the users on the system.
- If a TCP and UDP service were added to a service group and that service group was applied to a role, all services (rather than only those defined in the service group) were allowed when that policy rule was processed during client activity.
- Client devices sometimes failed to be redirected to their original destination after successful web authentication.
- Scale/performance issues would occur in configurations with more than 700 APs.
- Selecting the column to sort bandwidth download would not toggle between ascending and descending sorting order.

- Configuration changes were not being logged anywhere in vWLAN.
- If the SNMP Contact Field contained special characters, the vWLAN would not replicate to HA Node.
- Incorrect MAC addresses were returned when searching for an AP's MAC address in Active Connection.
- After upgrading from 2.1 to 2.2.1, custom HTML would not support Chinese characters.
- An error message was returned when a guest user was created and a GIF image file was used in the Guest Receipt.
- Delay in GUI accessibility after vWLAN is rebooted.
- When upgrading from 2.1 to 2.2.1.20, the HTML spacing in the Login menu had to be between 0 and 100.
- If the same image file was used in the Guest Receipt for both the Logo Image and Icon Image positions, and it is removed from only one of those positions, Guest User creation failed.
- BSAP would become unresponsive in the Channel Scanning state.
- It was possible to delete the built-in unregistered role by renaming it and then deleting it. However, it was not possible to recreate the role with the original role's special properties.
- Some Android devices would not be redirected for web authentication.
- It was not possible to poll user status using the API.
- NTP server settings would accept only IP address and not the URL and the IP address.
- The administrative GUI became inaccessible and web redirection for clients was not possible.
- The system would not recover from a process restart and users were unable to connect.
- Logs could not be exported.
- vWLAN GUI returned AP errors even though the BSAP was properly licensed and an SSID was configured.
- Outgoing HTTPS traffic to a destination hostname **apple.com** or ***.apple.com** in the unregistered role was redirected. HTTPS traffic to any other URL was successful.
- The IP address of the AP did not appear in **Status > Active Connections > All Connections**.
- No logging message was recorded when an Admin User logged into the system.

Errata

The following is a list of errata that still exist in vWLAN 2.3.0.

- Very large configuration backups may not fully download.
- If the default Guest role is modified or deleted, a new Guest role is created after an upgrade or reboot.
- Previous versions of vWLAN allowed the time interval of user interface (UI) updates to be set lower than 15 minutes.
- An error is returned when trying to view adjacent APs.
- The ability to preview a login form does not function properly when using the Opera browser. Other browsers function properly.
- When redirecting to an external server, the expected string returned cannot contain special characters.
- The default domain read-only admin role cannot add widgets to the dashboard. The workaround is for a platform administrator to modify this setting to add all permissions to Dashboard rights.

- If the administrator is on a paginated tab and items are deleted, then pagination will be incorrect until the view is refreshed.
- For certain larger vWLAN deployments using VMware, additional memory may be required.
- When filtering a list of AP licenses by partial MAC address, items will not match the filter until an octet is entered completely.
- Access Point BW, Active User BW, SSID BW, and Active User KB Uploaded/Downloaded data may be inconsistent.
- When creating a report, the screen may continue to display **Report is still running** when the report has finished. Refreshing the page in the browser should update the screen. If the report does not finish for long period of time, the Report service can be restarted to clear this condition by navigating to **Administration** > **Restart** and selecting **Restart Reporting Daemon**.
- The Current Bandwidth Reported for an Active User is incorrect.
- SNMP community strings with fewer than six characters are converted to public during the migration from 2.1.0.14 to 2.2.1.20.
- The following platform alarm is produced during migration: **config upgrade failed Failed to update RootSetting rw_community_string error Validation failed: Value is invalid update varRootSettingrw_community_string.update_attributes!value => ERRORS**
- An LDAP/AD Bind user must be configured even if **Bind all Queries as LDAP Bind user** is not selected.
- Special characters are stripped from LDAP/AD authentication server bind user when migrating from 2.1.0.14 to 2.2.1.20.
- Locations appear inactive in the administrator GUI, when they are actually active and user traffic flows into the location successfully.
- Certain characters in custom Web Login HTML code are being removed or changed during upgrade from the 2.1 to 2.2.1.20 resulting in failure to redirect clients.
- The count in User Count Report is not accurate.
- The Location Status report contains no results. This report only shows changes in the statuses of locations. Naming of the report will be clarified in a future release.
- 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 2.3.0 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 Administrator's Guide*
- *vWLAN AP Discovery*
- *Using APIs with vWLAN*
- *vWLAN Hardware Appliance Quick Start Guide*

