RELEASE NOTES

vWLAN 2.4.0
February 25, 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.

ADTRAN

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 2.4.0 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 2.4.0.

- 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. 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 2.4.0 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 2.4.0.

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 2.4.0 until they can be supported under the multi-tenant architecture.

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 vWLAN 2.1 but not supported in 2.4.0.

- **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-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 2.4.0, and all configurations will be maintained.

> **NOTE** vWLAN 2.4.0.12 requires using Bluesocket Access Point (BSAP) firmware version 6.8.0.09. BSAP 6.8.0.09 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 2.4.0, but certain features are not supported and some settings must be reconfigured when upgrading to vWLAN 2.4.0. 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 2.4.0.12 software image (2.4.0.12)

- 6.8.0.09 AP firmware for the appropriate AP models

- vWLAN version 2.4.0 Release Notes (available in download area at http://support.adtran.com)

- vWLAN version 2.4.0 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 2.4.0 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 2.4.0.

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 2.4.0, 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 2.4.0 (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 2.4.0 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 2.4.0. Release 2.4.0 requires a new Open Virtualization Archive (OVA).

    a. The VM memory and CPU recommendations have changed between 2.1 and 2.4.0. It is recommended that 4 cores and 6 GB of RAM be used for 2.4.0.

    b. The VM file system requirement has increased from 2.1 to 2.4.0. A vWLAN 2.1 Virtual Machine with a 7 GB footprint cannot be upgraded directly to 2.4.0. Instead, a new 2.4.0 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 2.4.0. 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 2.4.0, 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:
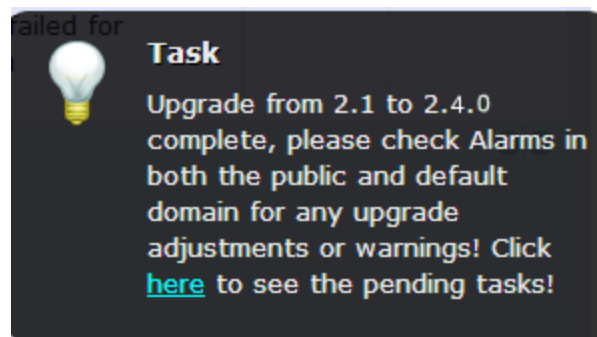
Or it will appear under the Admin Tasks view:

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 2.4.0. 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 2.4.0 requires using Bluesocket Access Point (BSAP) firmware version 6.8.0.

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 2.4.0.

- **Enhanced UI and usability**

  • Refreshed, intuitive, HTML5-based administrative user interface (UI) with a bright, crisp, modern look and feel

  • Forms, fonts, font sizes, and colors are consistent throughout the product

  • Pages divided into sections with titles and page breaks

  • Admin Auth moved to Administration

  • Domain tasks appear in red

  • Navigation menus are no more than three levels deep

  • Status is linked to configuration and vice versa

  • Preferences, such as the columns chosen to display, are saved in client side cookies

  • Infinite scroll allows continuous scrolling without going page by page

  • Logs are sorted newest to oldest by default

- Column headers always displayed
- No need to scroll all the way to the bottom of a long list in order to scroll to the right
- Many default values have been added, for example, the common ports used for authentication
- Ability to simply drill down into a line without having to click a show (folder) or edit (pencil) action

- **Enhanced status**
  - Ability to see number of clients per access point and per radio
  - AP Details View
    - Ability to drill down for detailed AP information such as the clients that are associated to the radio, number of clients per radio, radio interface settings, etc.
    - Quick links to edit the AP configuration, see the AP on the floor plan, see logs regarding the AP, see alarms regarding the AP, see wireless IDS alerts from the AP, run a traffic capture on the AP, and see APs that are adjacent to the AP
  - Client Details View
    - Ability to drill down for detailed client information with quick links to logs regarding the client and to run a traffic capture to capture the client's traffic

- **Enhanced Dashboard/Reporting**
  - Customizable dashboards with real time and historical widgets (charts and graphs)
    - Client Count Over Time
    - Client Usage Over Time
    - Current AP Firmware Versions
    - Current AP Status
    - Current Active AP Count
    - Current Active Users by Radio Mode
    - Current Client Count
    - Current Client Status
    - Top APs by Client Count Over Time
    - Top APs by Client Usage Over Time
    - Top Clients by Usage Over Time
    - Top Locations by Client Count Over Time
    - Top Locations by Usage Over Time
    - Top Roles by Client Count Over Time
    - Top Roles by Client Usage Over Time
    - Top SSIDS by Client Count Over Time
    - Top SSIDS by Client Count Over Time
  - Reports show instantly without waiting for job to run
  - Real time widgets update while you are watching and historical widgets present historical data
  - Ability to create multiple dashboards or tabs for customized perspectives

- Ability to have more than one report on the system at any given time
- Ability to download and email the entire dashboard (or just one widget) in PDF (containing charts and graphs) and CSV (containing data only) format
- Ability to filter historical widgets by time and date (last 24 hours, last 7 days, last 30 days, custom)
- Ability to customize report logo
- The color red is no longer used in charts and graphs
- **Support for sending secure email alerts (TLS)**
- **Usernames of Active Users appear on secondary following a failover event**
- **Ability to export Logs, Alarms, and W-IDS Alerts**
- **Additional AP Scale with multi-tenant**
    - Support for 1500 APs on vWLAN Appliance hardware and vWLAN Virtual Appliance (VMware) with minimum system requirements (500 APs were previously supported)
- **Support for new vWLAN 1U hardware appliance**
- **Support for high availability is now included without requiring the purchase of a high availability license per access point**

Fixes
This section highlights major bug fixes in vWLAN 2.4.0.

- When generating a report, an error would display around the start or stop time.
- The Wireless IDS Log Dashboard widget failed to update until the Wireless IDS Service process was restarted.
- Internal interval status could be set lower than the noted minimum value of 15 minutes.
- Editing an active location in a location group caused the location to be deleted from the group. If the APs supported the active location, they would tunnel client traffic.
- The Access Point Configuration Daemon would restart unexpectedly.
- If any Syslog server was created without a valid facility selected, no logs or alarms would be available in the user interface.
- When upgrading, the total width allocated for the HTML in vWLAN 2.1 could be configured to exceed its boundaries (1000) causing a portion of the upgrade to fail.
- DynamicRF would recommend setting power levels which could not be selected.
- Disk storage could fill up due to excess logging of process exceptions.
- When creating a CSR using the CSR option, the vWLAN would not create a Private Key if there was anything entered in the Certificate field.
- Web login form language was incorrectly assigned.
- Clients were not placed into a Role after a Radius Accept when using 802.1x if the SSID was first created with a different authentication type and then changed to Radius Authentication.
- the boot message event, **Starting in-memory queuing server beanstalkd [fail]**, appeared on the virtual appliance even though all processes started correctly.
- A role could be deleted even if it was referenced by a Hotspot Plan.

- BSAP host names containing dashes caused sorting and filtering to fail on the **Status** > **Access Points** menu.

- NAC VLAN ID could not be changed in the user interface even though it appeared in a text field.

- When a MAC device authentication was deleted or changed, clients were not disassociated.

- When clients were redirected, the splash page would not load until the web server was restarted.

- Clarified LDAP binding options help text.

- If the default Guest role was modified or deleted, a new Guest role was created after an upgrade or reboot.

- If there are no Login Items, Guest Receipts, Maps, or AP Firmware set on the primary AP, then an HA snapshot failed to load on the secondary AP.

- A location with a /0 subnet could be created.

- Very large configuration backups would fully download.

- Automatically created v-Locations could not be renamed.

- The help text for HA Node Snapshot was missing.

- Domain Restore text was incorrect and insufficient.

- An error was returned when trying to view adjacent APs.

- When redirecting to an external server, the string returned contained special characters.

- For larger vWLAN deployments using VMware, additional memory dedicated to the VM was required.

- When filtering a list of AP licenses by partial MAC address, items would not match the filter until an octet was entered completely.

- Access Point BW, Active User BW, SSID BW, and Active User KB Uploaded/Downloaded data was inconsistent.

- The Current Bandwidth Reported for an Active User was incorrect.

- Calibration sometimes resulted in radio transmit power being set to very low levels.

- Active locations with user traffic successfully flowing into the location successfully appeared inactive in the administrator GUI.

- The count in the User Count Report was not accurate.

Errata
The following is a list of errata that still exist in vWLAN 2.4.0.

- Search capability does not function under the Administrators tab. Workaround: Use Control+F in the browser window to search.

- The API may become unresponsive if used from multiple sources simultaneously. It will become responsive again after a few minutes.

- When using RADIUS Admin Auth, the Dashboard modifications do not persist across logins. Workaround: Use a local administrator on a custom dashboard.

- 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.

- 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.

- Captive Portal fails to load when Redirect HTTPS Traffic for Unregistered Clients is enabled.

- The AP will redirect to the PTR record found regardless of the "Redirect to Hostname" option configured in vWLAN. To workaround the issue, the PTR record can be deleted.

- When using External Redirects for HTTPS, the vWLAN will send a different string to the external server based on the port to which users are destined.

- In large deployments, it was possible that clients could not authenticate until the Access Point User Manager service on the vWLAN was restarted.

- Running a Show Tech renders the administrative GUI interface unavailable until the Show Tech completes and becomes available for download.

- Very rarely, Locations may appear in the GUI, but not in the User Management process. Restarting the Interprocess Communication Daemon will remedy this situation.

- The user manager process may restart. If clients are unable to authenticate for a brief period, please contact ADTRAN Technical Support for troubleshooting assistance.

- Occasionally a user will persist in the Clients tab long after the user has left the system. To clear these users, manually drop them.

- While under heavy load, the GUI may report incorrect status information or it may sort the information improperly. The system will recover after a few minutes.

- The API may become unresponsive when a large number of APs are booting at the same time. 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 Message and Last Calibration columns are missing from the Access Points page. However, if you view the details of any access point, the information is still viewable there.

- 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 2.4.0 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*