RELEASE NOTES

vWLAN vPatch-2-3-0-09
December 23, 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.

Contents

Introduction

vWLAN vPatch-2-3-0-09 is a combined patch that 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 7*.

A list of new or updated documents for this release appears in *Documentation Updates on page 9*.

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 vPatch-2-3-0-09.

- 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 software 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 vPatch-2-3-0-09.

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.

Running software version 2.3.0.09 is a prerequisite for installing vPatch 2-3-0-09.

Unsupported Features from vWLAN 2.1

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

- Time Based Licenses
- Internal RADIUS 802.1X Server
- Dynamic Role Assignment Using Secondary LDAP/Active Directory Lookup after RADIUS
- Expiration of MAC devices
- Credit card and PMS billing
- POP3
- Role-based Network Access Schedules
- Polling vWLAN via SNMP for AP Specific Information
- Ability to automate AP jobs (e.g., reboots, dynamic RF calibration) and automate backups.
- Redirect to ports other than 80 and 443
- Ability to import/export local users, MAC devices, APs, authorized stations
- Ability to override a role a user is in under Status>Active Users
- 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.

Previous Patches

This vPatch includes the fixes provided by the following patches and supersedes previous patches for vWLAN version 2.3.0.9.

- TimeoutDaemon-TG4540
- SnmpMgmtPort-TG4634
- WebAuth-TG4442
- MemoryIntegrity-TG4743
- UserPerformance-TG4693

- UserPerformance-TG4693-4791
- UserPerformance-TG4431-4693-4791

Installing vPatch

All previous patches will need to be removed prior to installing vPatch. Note that a reboot is necessary following the installation of vPatch.

Step 1. Navigate to the **Administration** tab and select **Patch**.

Step 2. Select the patch to delete and select **Delete**.

Step 3. Navigate to the **Administration** tab and select **Patch**.

Step 4. Select the patch to install using the **Browse** button.

Step 5. Select **Install**.

Step 6. Any patches that you have installed will be visible in the **Patch list**. A **Platform Task** should display stating that a reboot is required. Delete all other platform tasks that are not needed. Reboot the vWLAN.

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.

Fixes

This section highlights major bug fixes in vWLAN vPatch-2-3-0-09**.**

- Certifications for the following countries/regulatory domains have been completed for the following products. It is the customer's responsibility to comply with the local regulatory domain. vWLAN uses the country code applied to the license to assist customers with compliance.

    Argentina BSAP 1920

    Chile BSAP 1920

    India BSAP 1920, BSAP 1925

    Japan BSAP 1920, BSAP 1935

    Malaysia BSAP 1920

    Mexico BSAP 1920

    Philippines BSAP 1920

    Thailand BSAP 1920

    Vietnam BSAP 1920

- The Access Point Configuration Daemon could restart unexpectedly.
- Expired guest users were not cleared during the cleanup process.
- Upon a User Manager crash, the process would take longer than expected to recover.
- The vWLAN would not send the accounting session ID attribute to the accounting server.
- Devices in 802.1X deployments could not connect to the WLAN during periods of high client association activity.
- A memory leak was experienced related to an internal process issue.
- Allow SNMP to respond on the management interface (when present).
- Unused guest users were deleted before the cleanup time was reached.
- The CPU was over utilized with large web authentication deployments.
- When APs were licensed for Australia, certain DFS channels could be selected but SSIDs would not broadcast on those channels.

Errata

The following is a list of errata that still exist in vWLAN vPatch-2-3-0-09**.**

- When generating a report, an error will display around the start or stop time. Workaround: Adjust the time to UTC.
- The Wireless IDS Log Dashboard widget may fail to update until the Wireless IDS Service process is restarted.
- Internal interval status can be set lower than the noted minimum value of 15 minutes. It is strongly recommended that the value not be set below 15 minutes.
- Editing an active location in a location group will cause the location to be deleted from the location group. If the APs support the active location, they will tunnel client traffic. To workaround this issue, the User Manager service can be restarted.

- 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.
- If the default Guest role is modified or deleted, a new Guest role is 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 fails to load on the secondary AP. Setting any one of these items will avoid this issue.
- Very large configuration backups may not fully download.
- An error is returned when trying to view adjacent APs.
- The login form preview 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.
- If the administrator deletes items on a paginated tab, then pagination will be incorrect until the view is refreshed.
- For certain larger vWLAN deployments using VMware, sufficient memory dedicated to the VM may be required. ADTRAN recommends 6 GB. Additional memory requirements should be taken into consideration when planning for future expansion.
- When attempting to filter a list of AP licenses by partial MAC address, items will not match the filter until the complete octet is entered.
- New installations of vWLAN 2-2-1-20 with vPatch-2-2-1-20-2 display a duplicate DHCP Server service.
- Access Point BW, Active User BW, SSID BW, and Active User KB Uploaded/Downloaded data may be inconsistent.
- The Current Bandwidth Reported for an active user is incorrect.
- 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**.
- Locations appear inactive in the administrator GUI, when they are actually active and user traffic flows into the location successfully.
- 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.
- 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 vPatch-2-3-0-09 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*