



RELEASE NOTES

vWLAN vPatch-2-4-0-12
May 23, 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

Copyright © 2013 ADTRAN, Inc.
All Rights Reserved.

Contents

<i>Introduction</i>	4
<i>Supported Models</i>	4
<i>AP Licensing</i>	4
<i>System Notes</i>	5
<i>Installing vPatch</i>	7
<i>Fixes</i>	7
<i>Errata</i>	7
<i>Documentation Updates</i>	9

Introduction

vWLAN vPatch-2-4-0-12 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-2-4-0-12.

- 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. 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 activation keys are sent to the Customer. The Customer then enters the serial numbers and keys on the ADTRAN licensing tool, available at <http://www.adtran.com/licensing>. For new APs, these keys are sent by the reseller or distributor. For replacement APs, the keys will be emailed from ADTRAN to the registered owner of the product. 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 a return merchandise authorization (RMA) generated by ADTRAN, contact ADTRAN Customer Care at 888-423-8726, and reference the RMA number.

System Notes

vWLAN 2.4.0.12 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-2-4-0-12.

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

Running software version 2.4.0.12 is a prerequisite for installing vPatch 2-4-0-12.

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.

Previous Patches

This vPatch includes the fixes provided by the following patches and supersedes previous patches for vWLAN version 2.4.0.12.

- Heartbleed-TG5986
- RegenerateCerts-TG6350

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 2.4.0.12 requires using Bluesocket Access Point (BSAP) firmware version 6.8.0-18.

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 802.11a/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-2-4-0-12.

- Guest user accounts were not expiring after logging out and logging back in.
- The private key for the self-signed certificate is now regenerated in response to Heartbleed vulnerability.
- MAC authentication clients can now be tunneled between access points if location changes are made after the client has been authenticated.
- When APs were connecting, there was a condition where the TCP connection failed and the AP disconnected, an internal process would crash as a result. This caused secondary crashes to subscribed processes.
- The OpenSSL version was changed to avoid Heartbleed vulnerability (<http://www.us-cert.gov/ncas/alerts/TA14-098A>).
- The internal reporting process would queue up information but was unable to write to the database resulting in a memory leak and some reporting information being unavailable.
- Processes would restart leaving invalid client entries in the Status > Clients table in the UI.
- Guest user accounts were not expiring after logging out and logging back in.
- APs would revert unexpectedly from HA Node to HA Master.
- Diagnostic system files were not being produced.
- The Access Point User Manager process would restart causing a loss of network connectivity for clients.
- Improved performance of the search capability in the vWLAN.
- Processes would restart unexpectedly.
- If an internal process restarted, it was not possible for users to authenticate.
- APs would reboot if system processes restarted unexpectedly.
- Under some conditions, minor config changes to an AP Template would result in an internal process crash.
- Locations reported on the AP and vWLAN did not match causing users to be tunneled.
- In large deployments, clients could not authenticate until the Access Point User Manager service on the vWLAN was restarted.
- vLocations would appear in the GUI but not the User Management process.
- Improved performance of vWLAN doing periods of high client roaming activity.
- The user manager process may have restarted.

Errata

The following is a list of errata that still exist in vWLAN vPatch-2-4-0-12.

- Captive Portal fails to load when Redirect HTTPS Traffic for Unregistered Clients is enabled.
Workaround: Disable HTTPS Redirection.
- When Time in seconds before inactive connections are dropped is configured, the unit is not dropping the device at the appropriate time.
- Under extremely heavy loads, some user links on the Active User status page will be abbreviated to MAC addresses, and those clients will never drop from the system. **Workaround:** Drop the clients manually.

- The Search capability does not function on the Administrators tab. **Workaround:** Use the control+F in the browser to do your search.
- The API can become unresponsive if it is accessed 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 to customize the dashboard in 2.4.
- 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.
- An administrative task, **Please change the default admin password**, is appearing on a secondary HA box. This task should be deleted or ignored, because the password can only be changed on the Primary HA box.
- 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.
- The AP will redirect to the PTR record found regardless of the "Redirect to Hostname" option configured in vWLAN. To work around the issue, the PTR record can be deleted.
- Modifying the columns of any table with the Show/Hide Columns button causes the table to resize improperly. Refreshing the page will correct the problem.
- 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.
- Occasionally a user will persist in the Clients tab long after the user has left the system. To clear these users, manually drop them.
- Under a 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 will not update. Refreshing the page will correct the problem.
- 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 displayed 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 2.4.0.12 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](#)*