RELEASE NOTES

vWLAN 2.8.0-P01 Patch
August 16, 2016

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

The 2.8.0-P01 patch for vWLAN that addresses an issue that was uncovered in a previous code release.

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 6*.

Supported Models

The following models are supported in vWLAN 2.8.0-P01. The patch can be applied to the following models if they are running vWLAN version 2.8.0. The vWLAN 2.8.0-P01 patch is only compatible with vWLAN version 2.8.0.

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

Wireless Regulatory Compliance

Based on United States FCC and European DFS and ETSI regulations, ADTRAN validates the country in which the APs are being operated. This prevents the ADTRAN equipment from accidentally being used in an improper configuration.

When customers request AP licenses, they must specify the country where the AP will be deployed and operated. Note that a single vWLAN can control and manage APs in different countries and regulatory domains – and the channel and power settings are regulated by the country where the individual AP is deployed and operated.

Before the license is installed, the AP is in the platform and not associated to any domain, so the AP's radios are disabled by default. When the licenses are uploaded, the country code is then applied to licensed BSAPs. Allowed channels and power levels are determined by the country and the platform, and once the AP is placed into a domain, it will scan the channels to discover neighboring APs and choose a valid channel.

Fixes

This section highlights major bug fixes in vWLAN patch 2.8.0-P01.

- Timed out users were not being removed from the UI if the user's device attempted to roam while in the un-registered role.

Errata

The following is a list of errata that still exist in vWLAN Version 2.8.0 with the vWLAN 2.8.0-P01 patch applied.

- Over time dashboard widgets cease to display the latest data point available.
- NTP updates are not occurring regardless of the frequency chosen in the platform settings. To force an NTP update, change the configured NTP server address(es).

- If an administrator incorrectly configures a Hotspot and an error message appears, some configuration options may no longer be visible.

- Switching domains on the **Administration > Backup/Restore** page leads to a server error.

- Guest Receipts incorrectly print two pages when printing for one account.

- When configuring custom language login forms, vWLAN displays invalid characters for certain languages. Instead of the valid character, the browser displays ?.

- If invalid entries are made when configuring the LDAP server, the Administrator may not receive a valid error message.

- The Timeout Weight setting should be a required field in the LDAP Server configuration and will automatically default to **1** if left blank on initial set up.

- The administrator feature of **Downloading Widgets** as **JPEG** does not function.

- Uploading the same AP firmware file twice results in the inability to choose a different firmware file. **Workaround:** Navigate away from the page and back again.

- The client count display on the UI is inaccurate and can be out of sync in a large system with multiple clients roaming. The client count at the top of the UI page on the Domain status page and the client count at the bottom of the UI page do not match - even after multiple refresh cycles.

- On a heavily loaded system, the Captive Portal may fail to load when Redirect HTTPS traffic for Unregistered Clients is enabled.

- vWLAN is not in compliance with SNMP System Group according to RFC 1213.

- Packet captures taken from the vWLAN UI intermittently misses packets. In a lab environment during captive portal authentication with RadiusWebServer, a test sent 50 packets but the PCAP observed only 48. **Workaround:** Administrators are advised to take multiple Packet captures when attempting to diagnose an issue.

- When attempting to execute a traffic capture from the vWLAN UI on an AP that is in a down state, the capture will not begin, but the UI will not return an error.

- DynamicRF may significantly increase CPU load in large deployments.

- In extremely large deployments (~1500 Aps), the output of the **show tech** command can fill the disk.

- When using the Drop User function, Apple MacBooks running OS X will retain a previously held IP address unless the timeout threshold is reached. This can cause web redirection to the captive portal to fail if the client attempts to connect to a different SSID. **Workaround:** Disable the wireless interface on the MacBook prior to dropping the user.

- MP is detected as adjacent by MPP resulting in RF recommendations.

- If the power on the 2.4Ghz radio of an AP is set to **0dBm** (1 mW), the power could be incorrectly set to **30dBm** (1000 mW) when booted.

- When using a Google Chromebook on a captive portal, the user will never be automatically redirected to their final destination. Manually refreshing the page or going to another page will function as expected.

- In some instances the wireless packet captures fail to initiate properly. If this occurs, it may be necessary to restart the packet capture or restart the AP.

- Locations may not become active after a domain restore.

- Wireless IDS alerts are not generated for the following conditions: AP Down, AP SSID Change, and AP Channel Change.

- After an AP default location update, currently associated clients in the native AP location will not be updated automatically.
- High Availability is not replicating HotSpot Login Forms correctly.
- In case of 1X Authentication Failed, vWLAN GUI will display Unregistered Role even though Different Role was configured.
- APs will sometimes report out-of-date adjacencies (up to 12 hours old).
- Some pages in the UI do not fully function under IE9. **Workaround:** Use a different browser, upgrade to a newer version of IE, or use the API.
- After executing any restart from the vWLAN GUI, the page must be refreshed manually.
- Occasionally, the first time an AP is moved to a domain it will ignore its configured radio power settings. **Workaround:** Reconfigure the radio power settings.
- APs configured for Mesh mode do not allow a packet capture to be taken on the AP.
- iPad 3 (iOS 8.1) and iPad 2 (iOS 7.1) may have issues with redirection to the originally requested site after being redirected to login with Captive Portal.
- The API may become unresponsive if used from multiple sources simultaneously. It will become responsive again after a few minutes.
- Under heavy load, AP and client counts may be incorrect for a period of time but they will correct themselves.
- When upgrading a large database (with many historical records and/or domains), the system can take up to an hour to come up after the upgrade. **Workaround:** Implement HA or a high Control Channel timeout.
- For fast-roaming, adjacent APs must detect each other and add each other as neighbors. If APs are brought in at different times, it is possible for neighbor detection to fail and roaming to take longer.
- When creating or editing a Role, if the administrator sets the **CoS Priority Out Overrid**e field to **DSCP from 802.11** or **802.1p from 802.11**, the IP packet put onto the wire will not have the DSCP value correctly set.
- The 2.4 GHz radio may only have 124 client associations, whereas the 5.0 GHz radio operates normally.
- BSAP 1800s may run low on memory causing sporadic client and AP activity or even a lose connection with vWLAN requiring a manual hard reset before operation can resume.
- Wireless packet captures may not function properly on the 5 GHz radio of a BSAP 1800 Series.
- Virtual Ethernet failing to connect causes a memory leak in the APs.
- BSAPs support up to 1024 schedule rules. If BSAPs are rebooting after adding schedules, the number of schedules will need to be reduced.
- BSAP 1800 version 2 may use the incorrect Power Save Mode for clients resulting in missing packets and dropped connections.
- When starting a wireless packet capture, take care to allow the capture to begin before taking an action on it. If the capture must be stopped, wait at least 30 seconds to let the capture fully start. If a domain task pop-up is seen after a capture, it means the AP never fully recovered after the capture. Apply configuration to or reboot the AP to recover it.
- Certain devices will present a Captive Network Assistant (CNA) even though this feature is disabled in vWLAN.

- If greater than 86 users are associated to an AP and a failover occurs, they will not appear immediately in the UI of the secondary vWLAN.

- The Sony Xperia Tablet Z running Android version 4.2.2 may fail to authenticate using 802.1x due to an issue with the device itself.

Release Specific Upgrade Instructions

To apply the patch, you must first be running vWLAN version 2.8.0. Please see *vWLAN 2.8.0 Release Notes* and then upgrade using the vWLAN upgrade guide located at https://supportforums.adtran.com/docs/DOC-7691.

Once upgraded, see the section of the document called "Applying a Patch to vWLAN" to properly apply the patch.