RELEASE NOTES

vWLAN 2.5.1
March 19, 2015

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 © 2015 ADTRAN, Inc.
All Rights Reserved.

Contents

Introduction

vWLAN 2.5.1 is a minor system release that adds new features and addresses 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 10*.

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 2.5.1.

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

AP Licensing

The vWLAN appliance includes a flexible access point (AP) licensing model where the customer purchases licenses for individual APs. 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 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. Upon purchase, Activation Keys are sent to the customer via email. Activation Keys are not yet activated against any serial number. The customer must perform the activation process to obtain the license file. The customer would simply apply the Activation Keys to the hardware serial numbers they wish to license using the ADTRAN Licensor found at www.adtran.com/licensing. The license process will also register the hardware to the email address tied to the customer's ADTRAN login.

Process Overview

1. Log into www.adtran.com/licensing using the email address you want registered to the hardware
2. Enter the SERIAL NUMBER, ACTIVATION KEY pair(s) into the licensing tool
3. Download the license file

Copyright © 2015 ADTRAN, Inc.

4. Apply the license in vWLAN

To download a license file again later, simply enter the serial number into the licensing tool.

For more instructions or to watch a video detailing bulk licensing methods, please visit the ADTRAN Support Community: *https://supportforums.adtran.com/docs/DOC-7021*.

For detailed information about applying licenses to vWLAN for Bluesocket Access Points, please visit the ADTRAN Support Community: *https://supportforums.adtran.com/docs/DOC-5017*.

You may verify eligiblity for ADTRAN Technical Support at the following link: *http://www.adtran.com/web/page/portal/Adtran/wp_support_eligibilty*.

For assistance with licensing, or technical support of your Bluesocket product, please open a support case at *www.adtran.com/supportcase*.

System Notes

vWLAN 2.5.1 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 2.5.1.

To use vWLAN, two products are required - the vWLAN solution itself and Bluesocket access points.

VMware Memory Requirements

VMware deployments require 6GB of memory assigned to vWLAN.

Unsupported Features from vWLAN 2.1

The following features were supported in the non multi-tenant version of vWLAN (2.1) but are not currently supported in the multi-tenant version (2.5).

- Internal RADIUS 802.1X Server
- Dynamic Role Assignment Using Secondary LDAP/Active Directory Lookup after RADIUS. ADTRAN recommends using RADIUS attributes for dynamic role assignment instead of making a secondary lookup to LDAP/AD for best performance. ADTRAN will not port this functionality to the multi-tenant version of vWLAN.
- Expiration of MAC devices
- Credit card billing
- POP3
- 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
- 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 2.5.1, and all configurations will be maintained.

> NOTE vWLAN 2.5.1 requires using Bluesocket Access Point (BSAP) firmware version 6.9.1. BSAP 6.9.1 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 and from there they can be upgraded to vWLAN 2.5.1. It is important to note that certain features are not supported and some settings must be reconfigured when upgrading from 2.1 to 2.5 though. 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.

> 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) prior to the further upgrade to vWLAN 2.5.1.

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 2.5.1 software image (2.5.1)
- 6.9.1 AP firmware for the appropriate AP models
- vWLAN version 2.5.1 Release Notes (available in download area at http://support.adtran.com)
- vWLAN version 2.5.1 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 2.5.1 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

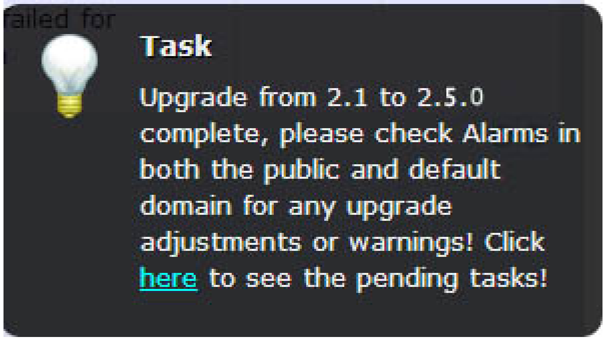
The following section is applicable when upgrading from vWLAN 2.1 to vWLAN 2.5.1 (through any intermediate upgrade steps).

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 2.5.1, 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 2.5.1 (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 (overridden 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 2.5.1 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 2.5.1. Release 2.5.1 requires a new Open Virtualization Archive (OVA).
    a. The VM memory and CPU recommendations have changed between 2.1 and 2.5.1. It is recommended that 4 cores and 6 GB of RAM be used for 2.5.1.
    b. The VM file system requirement has increased from 2.1 to 2.5.1. A vWLAN 2.1 Virtual Machine with a 7 GB footprint cannot be upgraded directly to 2.5.1. Instead, a new 2.5.1 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 2.5.1. For more details refer to the *vWLAN Upgrade Guide* available at https://supportforums.adtran.com.

Tracking Upgrade Alarms

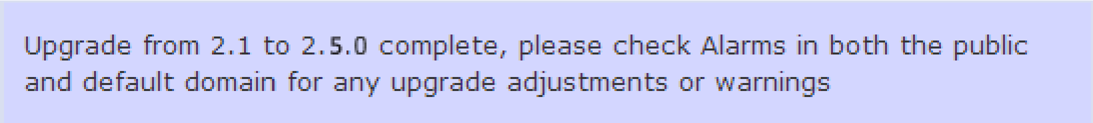
During the upgrade from 2.1 to 2.5.1, the vWLAN system will adjust the configuration of the system. In certain cases, incongruent data may be present on the 2.1 system (for example, a custom login page without a Guest Role selected) which is no longer valid from 2.3.0 forward. After the upgrade, this administrative task will display as a popup:



Task

Upgrade from 2.1 to 2.5.0 complete, please check Alarms in both the public and default domain for any upgrade adjustments or warnings! Click here to see the pending tasks!

Or it will appear under the Admin Tasks view:



Upgrade from 2.1 to 2.5.0 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:

Copyright © 2015 ADTRAN, Inc.

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 2.5.1. 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 2.5.1 requires using Bluesocket Access Point (BSAP) firmware version 6.9.1.

BSAP Interoperability and Performance

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

1. Use WPA2 (PSK or 802.1X) with advanced encryption standard (AES) when connecting 802.11n/ac-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/ac client's performance.
2. Enable 802.11n and ac Wireless Modes, 80 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/ac 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/ac 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 2.5.1**.**

- Added support for Role Based Access Control Schedules.

  - The ability to schedule when Wi-Fi access is or is not available via the role. For example, a library could prevent guests from using the internet from their parking lot when they are closed for business and allow access during normal business hours.
  - Note that Role Based Access Control Schedules configured in 2.1 will need to be reconfigured in 2.5.1.
- Added support for Kenya country regulatory domain for BSAP 1920.
- Added support for Turkey country regulatory domain for BSAP 1930, 1935 and 1940.
- Added support for St. Vincent, St Lucia, Barbados, Dominica and Grenada country regulatory domain for BSAP 1920, 1925 and 1940.

Fixes

This section highlights major bug fixes in vWLAN 2.5.1**.**

- SSLv3 was disabled to prevent vulnerabilities associated with it (specifically CVE-2014-3566).
- Internal users timed out before the set expiry time was reached.
- If a user did not have Domain Level Admin Task read permissions, they could not log into the Admin UI if there was a task ready.
- Internal users would stop timing out and CPU usage would noticeably increase until the User Account Monitor was restarted.
- The Access Points page (**Status** > **Access Points**) could not be sorted by the Total Clients column.

Errata

The following is a list of errata that still exist in vWLAN 2.5.1**.**

- The process to rotate log files will not execute. This will result in disk space filling up due to large log files and a sluggish UI as large files are maintained.
- If the MAC address, Login Form ID, and Domain ID fields were not being sent to the vWLAN in the login request, then the client would not be logged in. The client would be sent back to the internal or external login form.
- Changes were made in 2.5.1 to the operation of Captive Portal to improve performance. If the login page was fully customized using examples from 2.5.0 or before, these changes would cause an issue where users would be redirected to the splash screen but would be presented with a 500 Internal Server Error after they attempt to login.
- APs configured for Mesh mode do not allow an AP traffic capture.
- In large deployments, it was possible that clients could not authenticate until the Access Point User Manager service on the vWLAN was restarted.
- If a client is associated to an SSID that does static web authentication and a non-default language is selected from the dropdown on the login page, the language on the login page is changed correctly and the post-login page will be in that language. If the client is disassociated and re-associated, the login page will be back in the default language and if a different language is not selected from the drop down, the post-login page will still be in the non-default language selected earlier.
- Intermapper cannot parse vWLAN 2.5 MIBs completely.

- When needing to reset an administrator's password, the email that is sent contains a link to the IP address of vWLAN rather than the configured hostname. If a certificate is installed, this results in a certificate warning.
- Downloaded adjacent AP tables do not display Signal (dBm) or Sensor Name columns.
- Calibration may not select the appropriate channels and power settings.
- After being redirected to login with Captive Portal, iPad 3 (iOS 8.1) and iPad 2 (iOS 7.1) sometimes have issues with redirection to the originally requested site.
- The BSAP 1800 AP that has a tag that states it is a Model 1800 shows up as a Model BSAP-1840 in the UI. The Model 1935 that has a tag that states it is a Model 1935 shows up as a Model BSAP-1930 in the UI.
- Even when disabled, Captive Network Assistant may still pop-up when certain Apple devices try to connect.
- When updating an AP template applied to uplink mesh APs, the administrator will be warned about disabling mesh even though mesh is not being disabled.
- If a user is assigned to a role containing a schedule, a user can still authenticate to LDAP when associating at a time outside their schedule but cannot pass traffic.
- The Netstat utility output header in the GUI does not match the output header in the SSH session.
- Preview web portals will not respond to the change language drop-down list. Deployed web portals will correctly change the language.
- Preview web portals will not respond to the change password link. Deployed web portals will allow changing passwords.
- The Current Active Users by Radio Mode widget shows a null value.
- A duplicate 802.1X authentication server can be created but not edited.
- An AP may render incorrect available SSIDs when attempting a wireless packet capture.
- Downloading large numbers of logs can cause the UI to become unresponsive.
- The API cannot be used to configure the AP's Channel to Auto.
- The API cannot be used to back up or restore the configuration.
- The UI is not properly rendering the page in Google Chrome.
- Setting a vary large value in the System Settings > Timeout Value for Web Server can cause the Captive Portal to run out of available web sessions. This field is now limited to 30 seconds.
- Under extremely heavy loads, some user links on the Active User status page will not be abbreviated to MAC addresses, and those clients will never drop from the system. **Workaround:** Drop the clients manually.
- Guest users cannot be deleted from guest_users using the API.
- When upgrading vWLAN from 2.4 to 2.5, the upgrade can take a long period of time (an hour or longer) because all dashboard data is preserved during the upgrade. The data is restored after the reboot, so the system will not be responsive to ping or web requests during this time. When upgrading a large system (with multiple domains and many users), consider a High Availability pair (now an included feature in 2.4), and then upgrade the primary fully before the backup. Alternately, consider a long control channel timeout so Wi-Fi still functions when the box is down and upgrading.
- An API GET request on service_groups does not return child services.

- An API GET request on destination_groups does not return child destinations.
- When initiating an AP traffic capture, the variables associated with the capture are reset in the UI. This means that the settings shown do not reflect the settings for the capture that is currently running.
- Captive Portal fails to load when Redirect HTTPS traffic for unregistered clients is enabled.
- When the time in seconds before inactive connections are dropped is configured, devices are not dropped at appropriate time.
- The API may become unresponsive if used from multiple sources simultaneously. It will become responsive again after a few minutes.
- 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.
- The performance of the UI can suffer if the API is being heavily used.
- Under heavy load, AP and client counts may be incorrect for a period of time but they will be corrected.
- 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. Implementing HA or a high Control Channel timeout will alleviate this issue.

- 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. Implementing HA or a high Control Channel timeout will alleviate this issue.

- Modifying the columns of any table with the **show/hide columns** button will cause the table to resize improperly. Refreshing the page will correct this.
- Very rarely, vLocations may appear in the GUI, but not the User Management process. Restarting the Interprocess Communication Daemon will fix this.
- Expanding Unified Access Groups in the UI can result in the link being rendered incorrectly.
- While under heavy load, the GUI may report incorrect status information or 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. The system will recover on its own after a few minutes.
- When using UI search fields, some searches may not complete with partial input.
- 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.
- If a user is logged into the UI looking at one domain and uses the API to get information from another domain the UI will display the AP and user counts from the domain accessed by the API, but the domain dropdown will still display the domain selected originally in the UI.
- The ability to preview a login form does not function properly when using the Opera browser. Other browsers function properly.
- After the administrator deletes items on a paginated tab, the pagination will be incorrect until the view is refreshed.
- For fast-roaming, adjacent APs must detect 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.

Documentation Updates

The following documents were updated or newly released for vWLAN 2.5.1 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*
- *Mesh Network in vWLAN*

Copyright © 2015 ADTRAN, Inc.