ADTRAN®

RELEASE NOTES

vWLAN 2.6.1
August 7, 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

Contents

Introduction

vWLAN 2.6.1 is a minor system release that adds one new feature 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 7*.

A list of new or updated documents for this release appears *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 2.6.1.

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

System Notes

vWLAN 2.6.1 is a software release that manages, configures, controls, and secures Wi-Fi access points (APs), the radio frequency (RF) spectrum and users, across 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.

Required BSAP Firmware

vWLAN 2.6.1 requires using Bluesocket Access Point (BSAP) firmware version 7.0.1.

VMware Memory Requirements

VMware deployments require at least 6GB of memory assigned to vWLAN.

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 + AES 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 2.6.1.

- AP Transmit Power is now represented in dBm and mW values rather than in percentages.

Fixes

This section highlights major bug fixes in vWLAN 2.6.1.

- Upgrading vWLAN from 2.5.x to 2.6.0 would result in a change to the AP Template named "default". The Channel Width for the 2.4GHz (bg) radio would be 40MHz and for the 5GHz (a) radio it would be 80MHz. Upon upgrade to 2.6.1, any AP Template where Channel Width is set to 40MHz on the 2.4GHz (bg) radio will be updated to be 20MHz. The use of 40MHz Channel Width on 2.4GHz (bg) radios is not recommended.
- Client traffic may get put in an incorrect VLAN, causing DHCP to fail.
- Hotspots will now send emails when TLS is enabled but not supported by the mail server.
- Added function to prevent NAC IP address conflicts.
- APs licensed in the U.S. appeared as DFS capable even though DFS will not be supported until a future release.
- The BSAP 1940 would display as a BSAP 1930 in the AP details page.
- The cipher selection has been adjusted to address the Logjam CVE-2015-4000 vulnerability.
- If an AP was configured with a name prior to that AP discovering vWLAN, then when the AP discovers vWLAN its name would change to the default for new APs.
- If an AP had users connected to it, and the AP was rebooted or disconnected, then the users stayed in vWLAN until one of these conditions occurred:

  1) They roamed to or connected to another AP, and then timed out from that AP.

  2) They were manually dropped from the Active Clients table.

  3) The vWLAN was rebooted.
- When uploading a new certificate, the admin web server had to be restarted to get the new certificate to apply.

- Dashboard widgets would change size unexpectedly in some cases when using IE9. Other browsers functioned correctly.
- Real-time widgets were not downloaded with the rest of the dashboards on the page when the page's download link was used.
- The iPhone 6 running iOS 8.1 displayed inconsistent behavior with vWLAN 2.6 using Captive Network Assistant. At times the CNA would function and at other times would not. This behavior was seen on both the 2.4 and 5 GHz radios. The customer was required to manually open the Safari browser in order to be redirected to the authentication log in page.
- The platform setting Default URL formerly was used to prevent web crawlers and other devices from obtaining the login page from the network side. The user was redirected to this URL. The system now sends a 404 Not Found response instead, so the field can be safely ignored.
- Changing root@adtran.com from Primary did not reflect on the Secondary.
- When logged in as root@adtran.com (Administrator), the user was prompted to change email address on Setup Wizard.
- Although MAC authentication was relabeled as device authentication, they appeared as MAC authentications in the logs.
- Importing a CSV file from Microsoft Excel did not always function correctly.
- The Restore Default Roles function did not prompt for confirmation.
- In the AP Template, the DFS Block Channel was the list of channels that should not be used for DFS. Channels on the left were allowed for DFS, while those on the right were not allowed. For Firefox 36.0.1 browser, the channels sometimes all showed up on the right side.
- When trying to locate an AP that was no longer present, the following error was displayed: **The page you were looking for doesn't exist. This could be caused by a mistyped address or the page may have moved.** The error should have read: **No detecting access points have been placed on the map, the map hasn't been calibrated yet, or this AP has not been seen in the last hour!**
- Scheduled reports were marked with UTC time when delivered via scheduled emails. Manually downloaded reports showed the correct GMT time for the administrator.
- Using the **Show or Hide Setup Wizard** setting, to show the wizard, set this field to enabled. To hide, set to disabled.
- The UI listed the vWLAN gateway as 192.168.130.254 even if it had been properly assigned statically or via DHCP.
- Bulk device upload failed when a large file was imported.
- The RADIUS Accounting Class Attribute was not sent.
- The Calling Station ID format was inconsistent with RADIUS web authentication and 802.1X.
- Chromebooks could not connect to an 802.1x SSID after connecting to a PSK SSID.
- The Role matrix did not properly validate the destination or device type.
- The Administrator was not alerted when a bulk device upload file contained an invalid accounting server.
- For best results when using a wired access group, a roaming SSID should be specified.
- Some AP models would show up incorrectly in the UI as other models. The BSAP 1800 would show as a BSAP 1840 and the BSAP 1935 would show up as a BSAP 1930.
- Under extremely heavy loads, some user links on the Active User status page were not abbreviated to MAC addresses, and those clients were never dropped from the system.

- Expanding Unified Access Groups in the UI resulted in an incorrectly rendered link.

Errata

The following is a list of errata that still exist in vWLAN 2.6.1.

- MP is detected as adjacent by MPP resulting in RF recommendations.
- To set the configuration for expiring a user, the "Expire User" box must first be checked.
- DFS messages refer to APs as a BAP instead of BSAP.
- The active user status page may not display connected hosts.
- When login forms are created they properly use the root setting URL that is in that platform setting, but if the setting is edited, the login forms are not updated to the new URL and instead will use the previously configured URL. Workaround: Edit the login form and select Update Login Form without changing any fields on the page.
- High Availability may fail with the following error message: "422 error: VLAN is not a number."
- For Accounting, RADIUS Class Attribute does not function for 802.1x authentication.
- Using the API to set an AP's domain_id to 0 is not allowed, but no error message is returned when it is attempted.
- If using the API, invalid data can be used for an authentication server's role_id, timeout_weight, accounting_server_id, or auth rule role_id. Take care when setting these attributes to ensure that they are valid values.
- After restoring a backup file of a single Domain to the vWLAN server, when attempting to execute the Must Restart Admin Web Server task, the Administrator could receive an error that reads: Error occurred while executing the table action. The issue is seen because a service is in the process of restarting, and when the Administrator issues the execution from the UI, it causes the error. It is important for System Administrators to note that the service has restarted, and further action is not required by the Administrator. Refresh the page to see the update.
- A SIP2 authentication server cannot have a CP location code of greater than 255 characters. If this is attempted, the authentication server will not be created/edited, and the user will be taken to a generic error page. Going back and correcting the CP location code length will fix the problem.
- On a friends and family hotspot page, the field Your email address is asking for the email address of the friend or family member, not the sponsor.
- When downloading logs or alarms, be sure to use the correct time zone of your administrator, otherwise the logs will be confusing.
- Timed out users are not being removed from the UI.
- If the power on the BG (2.4 GHz radio) is set to 0% or 0 dBm, then when an AP boots, the power may go to the maximum level. Workaround: Do not use the 0 dBm setting on the 2.4 GHz radio.
- Invalid authentication server rules can be created with API.
- The OUI 10:41:7F does not show Apple as the manufacturer.
- The Single Click Sign-on Captive Portal page may fail if all configured DNS servers are not operational.
- When using a Google Chromebook on a captive portal, the user is never automatically redirected to their final destination. Manually refreshing the page or going to another page will function as expected.

- vWLAN will return something for most API POST requests (either the created element or an error explaining why the POST failed), but POSTs for guest users (both successes and failures) return nothing to the requester.
- If you configure an email server and it cannot be reached, or if a policy on that server denies email, you will not be able to receive email from vWLAN. If you configure email and are not receiving it, contact the email server administrator.
- When running vWLAN on VMWare, the option to run a traffic capture on the private interface will not exist unless a private interface has been created for the VMWare.
- Locations may not become active after a domain restore.
- After deleting dashboard widgets, widgets below the deleted ones should move up to fill the empty space, but this occasionally does not function.
- As an Administrator, in order to preview the image that is selected on an existing Guest Receipt you must select the **Show** button on the bottom of the page. Selecting the **Guest Receipt** or the **Edit** button will not show the image file or the image file name.
- A virtual machine occasionally synchronizes time with the host even though vWLAN has disabled periodic time synchronization. **Workaround:** All virtual machines should be configured with NTP, and the Host ESXi server must have NTP enabled to ensure it has the correct time/time zone.
- Wireless IDS alerts are not generated for the following conditions: AP Down, AP SSID Change, and AP Channel Change.
- The Platform NTP server setting currently has no validation capabilities, therefore the setting will accept any value without returning an error. Make sure to enter the valid FQDN or the valid IP address when configuring this field.
- AP security settings pertaining to WPA, WPA2-PSK, and Enterprise may not be displayed properly in MIB browser when queried via SNMP.
- 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.
- Some clients are being assigned to the Unregistered role instead of the role assigned by the 802.1x authentication server.
- APs will sometimes report out-of-date adjacencies (up to 12 hours old). **Workaround**: Wait for the system to age them out or ignore the adjacency.
- The DNS Server given to APs must be able to resolve the DNS name of the vWLAN, otherwise captive portal redirection to a hostname will not function.
- Some fully customized captive portal hooks do not function as expected.
- If a patch is applied to vWLAN, an admin task prompt should appear to reboot the server for the pending patch activation. Occasionally, this prompt will appear after the reboot and should be ignored and deleted.
- To avoid problems with the Friends and Family HotSpot account creation, administrators should use **Daily** hotspots rather than creating a **24 Hour HotSpot**. The user account creation screen comes up as usual and the user is allowed to select the hotspot account **24 Hour HotSpot** and enter an email address and password. However, the required account time limit field cannot be selected causing the page to fail with an error message.

- If a hotspot account is reconfigured from one that uses an email setting to one that does not, the previous email setting will still be visible. This email setting will not be used by the hotspot account and can be safely ignored.
- On the **snmp_trap_configurations** show page there is a hint that reads: **IP address of vWLAN. 127.0.0.1 means the local vWLAN box**. This hint should read: **IP address of SNMP Trap Server. 127.0.0.1 means the local vWLAN box.**
- On the **syslog_configurations** show page there is a hint that reads: **IP address of vWLAN. 127.0.0.1 means the local vWLAN box**. This hint should read: **IP address of syslog server 127.0.0.1 means the local vWLAN box.**
- Some information in vWLAN is only accessible on an item's edit menu, but the edit menus cannot be accessed on an HA node. To access this information the item must be viewed on the HA master.
- During the initial connection and authentication process, the web redirection on Google Nexus and Droid Maxx devices will appear to get trapped on the thank you page. In most cases, the device has authenticated and received a proper IP address but the thank you page will never refresh. **Workaround:** Restart the browser to be directed to the designated webpage resource as expected.
- When using the API to configure a Boolean attribute, 1 and true will evaluate to true and all other values will evaluate to false.
- Some pages in the UI do not fully function using Internet Explorer 9. **Workaround:** Use a different browser or upgrade to a newer version of Internet Explorer. Alternately use the API.
- After executing any restart from the vWLAN GUI, the page must be refreshed manually.
- Notification Templates should be created with a name for the template but it is currently possible to create one without a name.
- The API can be used to create access groups without values for **login_form_id** or **role_id**. These are not valid configurations.
- If the default admin's password is changed through the link in the top right of the page, the standard **Please change the default admin password** platform task will not be removed. In this case the admin task can safely be deleted.
- Changing any of the SNMP root settings (communities, contact, description, location, system name) from their default values causes unexpected behavior. If SNMP is to be used, these should be left as defaults.
- CoS priorities are displayed on the role create and edit menus even when the priority override is not set to one of the static options. When a non-static option is selected the priority fields are ignored.
- The Client Count by Device Type Over Time widget sometimes shows unknown/other devices. These messages can be ignored.
- 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.
- Admin tasks to restart specific processes are not cleared after vWLAN is restarted or rebooted. In these cases, the tasks can be safely ignored and deleted.
- Upon upgrading to 2.6, if you have a 1940 AP that is configured in an ETSI Regulatory Domain (i.e., Europe, Russia, etc.), that AP will be disabled for the 5 Ghz band. **Workaround:** Enable the DFS feature or mark the AP as Indoor (if applicable) to re-enable the 5 Ghz radio.

- During the initial connection and authentication process, the web redirection on the Google Nexus devices will appear to get trapped on the thank you page. In most cases, the device has authenticated and received a proper IP address but the thank you page will never refresh. **Workaround:** Restart the browser to be directed to the designated webpage resource as expected.
- APs configured for Mesh mode do not allow an AP traffic capture.
- Validation dialog boxes have incorrect punctuation at the end of some messages.
- During the wizard flow, the tab key does not function to progress through the menus. **Workaround:** Use the mouse instead.
- 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.
- 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.
- Even when disabled, Captive Network Assistant may still pop-up when certain Apple devices try to connect.
- Even though a user is assigned to a role based on LDAP server authentication rules, users can still authenticate outside their schedule but cannot pass traffic.
- The Netstat utility output header in the GUI does not matching 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.
- During the initial connection and authentication process, the web redirection on the Google Nexus devices will appear to get trapped on the thank you page. In most cases, the device has authenticated and received a proper IP Address but the thank you page will never refresh. **Workaround:** Restart the browser to be directed to the designated webpage resource as expected.
- 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.
- 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.
- The API may become unresponsive if used from multiple sources simultaneously. It will become responsive again after a few minutes.
- 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.
- 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.
- The native AP VLAN Location should be a read-only field, but currently it can be edited.
- 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 is not updated. 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.
- 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 each other 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.
- DFS may detect radar falsely.

Release Specific Upgrade Instructions

vWLAN 2.2.1 and newer systems can be upgraded to vWLAN 2.6.1, and all configurations will be maintained.

To upgrade your vWLAN Virtual Appliance Please see the vWLAN upgrade guide located at https://supportforums.adtran.com/docs/DOC-7691..

NOTE vWLAN 2.6.1 requires using Bluesocket Access Point (BSAP) firmware version 7.0.1. BSAP 7.0.1 is not backward compatible with previous vWLAN code versions. Step 4.2 on page 7 should be skipped when using this version.

NOTE If upgrading from vWLAN 2.1.x or a previous version, use the process outlined in the ***vWLAN 2.1 Upgrade Guide*** on ADTRAN’s Support Community (https://supportforums.adtran.com/docs/DOC-5868) prior to the further upgrade to vWLAN 2.6.1.

NOTE Upon upgrading to vWLAN 2.6.1, if you have an AP that is configured in an ETSI Regulatory Domain the 5GH band will be disabled. To re-enable the radio enable the DFS feature, (if installed outdoors) or mark the AP as indoor (if installed indoors).

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).

- **VW-2306** - Internal RADIUS 802.1X Server
- **VW-2204** - 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.
- **VW-3165** - Expiration of MAC devices
- **VW-2205** - Credit card billing
- **VW-2209**, **VW-2208** - POP3
- **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 and APs
- **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.

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 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
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*.

Documentation Updates

The following documents were updated or newly released for vWLAN 2.6.1 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*
- *Configuring DFS in vWLAN*
- *Configuring Layer 7 Device Fingerprinting in vWLAN*