

vWLAN® 2.2.1.20 Release Notes



Software Version: V2.2.1.20

vWLAN® Models Covered: Hardware Appliance, VMware ESX 4.0, 4.1, and 5.0

Document Date: May 17, 2013

These Release Notes list addenda or corrections to the user documentation, new features and fixes, known issues, and other important information about this release of the Bluesocket vWLAN system software. Unless otherwise noted, vWLAN® refers to any Bluesocket vWLAN® product (hardware or virtual).

Note: This release requires mandatory patch [vPatch-2-2-1-20-2](#) to address certain issues found and resolved post-release. Details of issues resolved are provided under [Fixes included in mandatory vPatch-2-2-1-20-2](#).

Contents

Important Notes..... 3

 Upgrading vWLAN 3

 Unsupported Features from vWLAN 2.1 3

 Discontinued Features 4

 vWLAN 2.1 to vWLAN 2.2.1 Upgrade Considerations 4

 Tracking Upgrade Alarms 5

 Recommended BSAP Firmware 6

 BSAP Interoperability and Performance 6

Background 7

User Documentation..... 7

AP Licensing 7

 Licensed Features 7

Wireless Regulatory Compliance 8

Version 2.2.1 vWLAN Release Features and Improvements 9

 Major Features for Release 2.2.1..... 9

 Major Improvements for Release 2.2.1 11

 Multi-tenant Features for vWLAN 2.2..... 12

Version 2.2.1-20 vWLAN Fixes 12

 Fixes included in mandatory vPatch-2-2-1-20-2..... 12

 Fixes from 2.2.0.17 and 2.2.1.19 to 2.2.1.20..... 13

 Fixes from 2.1 to 2.2.1 14

Version 2.2.1 vWLAN Errata 16

Important Notes

Upgrading vWLAN

vWLAN 2.2 systems can be upgraded to vWLAN 2.2.1, and all configurations will be maintained.

vWLAN 2.1 systems can be upgraded to vWLAN 2.2.1, but some features are not supported and some settings must be reconfigured when upgrading to vWLAN 2.2.1. These are outlined below. It is important to review these prior to beginning the upgrade process.

For a step-by-step guide through the upgrade from either 2.1 or 2.2 to 2.2.1, refer to the *vWLAN 2.2.1 Upgrade Guide* posted in the ADTRAN Support Community (<https://supportforums.adtran.com>).

Unsupported Features from vWLAN 2.1

The following lists features supported in 2.1 but not yet supported in 2.2.1. These are being considered for a future release of vWLAN.

- 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 and CAS Web Authentication
- 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
- Ability to inherit firewall rules

If you rely on the features above, then either find a suitable replacement/workaround or wait until a future release of vWLAN where these features may be available. Contact ADTRAN Technical Support for suggestions.

Discontinued Features

The following features have reached end of life or have been discontinued:

- BlueProtect support
- SVP (Spectralink Voice Protocol)
- Auto and Manual Containment – For legal reasons, the unlicensed spectrum cannot be contained. ADTRAN recommends locating rogue devices and disabling them.

vWLAN 2.1 to vWLAN 2.2.1 Upgrade Considerations

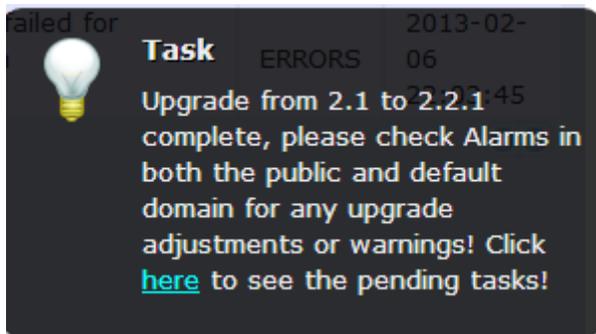
1. Administrator UI is only reachable at <https://<IP address>:3000>, where IP is the IP of the unit (regardless of the 2.1 setting).
2. All administrators are removed. There is one default administrator: root@adtran.com with a password of blueblue. New administrators can be created under 2.2.1 (using the granular model).
3. AP firmware is not included in the vWLAN image as of vWLAN 2.2.x. The AP firmware must be loaded on vWLAN for APs to boot properly.
4. Any local AP settings (not done 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 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 can be used).
11. 2.2.1 uses a new API (REST), and all API-based apps must be rewritten. Refer to the administrative guide.
12. The VMware system requirements differ from 2.1 to 2.2.1. Release 2.2.1 requires a new OVA.
 - a. The VM memory and CPU recommendations have changed between 2.1 and 2.2.1. It is recommended that 4 cores and 4 GB of RAM be used for 2.2.1.
 - b. The VM file system requirement has grown between 2.1 and 2.2.1. A vWLAN 2.1 Virtual Machine with a 7 Gig footprint cannot be upgraded directly to 2.2.1. Instead, a new 2.2.1 OVA (41 Gig footprint) must be deployed. Options are:

vWLAN® Release Notes

- i. Reconfigure the system from scratch
- ii. Downgrade the new OVA to 2.1, restore the 2.1 configuration there, and then upgrade to 2.2.1. Refer to the *vWLAN 2.2.1 Upgrade Guide* posted in the ADTRAN Support Community (<https://supportforums.adtran.com>) for more details.

Tracking Upgrade Alarms

During the upgrade from 2.1 to 2.2.1, 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 under 2.2.1. After the upgrade, this administrative task will show as a popup:



or under the Admin Tasks view:

Upgrade from 2.1 to 2.2.1 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 might see a message like this:

```
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 fixable, you can adjust your configuration under 2.2.1. Otherwise you can note all the issues, revert to version 2.1, and resolve them under your 2.1 configuration and then upgrade again.

Recommended BSAP Firmware

For this release, BSAP firmware version 6.6.0-25 or higher is required. BSAP firmware version 6.6.0-30 is recommended.

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:
 - Use WPA2 (PSK or 802.1x) with AES when connecting 802.11n-based clients. A TKIP client will connect at a maximum transmit rate of 54 Mbps.
 - 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.
 - 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.
 - Ensure that all 802.11n client drivers are updated to the latest version before doing any system or performance testing.
 - 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.
- To support multicast traffic between clients, do one of the following:
 1. 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.
 2. Allow the Multicast Destination IP Address in the Unregistered Role. The drawback is that this allows it for all users, so it should only be used if all users are allowed to receive the multicast streams.

Background

vWLAN is a software release that manages, configures, controls, and secures Wi-Fi access points, the 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 customers (or tenants) can use the same vWLAN software with their individual access points (APs). Many improvements were made to the software in vWLAN 2.2.1 (see below).

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

User Documentation

A full administration and configuration guide is available. You can download it from the ADTRAN support community (<https://supportforums.adtran.com>), along with the software and release notes.

AP Licensing

The vWLAN appliance includes a flexible AP licensing model where the customer purchases licenses for individual APs. By default, the appliance ships with no AP licenses. If a license wasn't received for a new AP, contact the reseller or distributor where the license was purchased. If a license wasn't received for a replacement AP on a RMA generated by ADTRAN, contact ADTRAN Customer Care at 888-423-8726 and reference the RMA number.

Licensed Features

When making a license request, one or more features can be selected:

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.

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 root domain 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, the APs will scan the channels to discover neighboring APs and optimize DynamicRF™.

Version 2.2.1 vWLAN Release Features and Improvements

Major Features for Release 2.2.1

- Added the ability to support multiple domains (tenants) and the ability for administrators to access one or more domains. Note that legacy vWLAN appliances (serial numbers beginning with 8000) can only support a single tenant. To support multiple tenants, upgrade to VMware or a new vWLAN appliance.
- Added the ability to customize the dashboard.
 - Instead of a static dashboard (as in 2.1), 2.2.1 offers a customizable (per domain and per administrator) dashboard with 11 available widgets (User Count/Time, Access Point Count/Time, User Status Count, AP Status Count, Bandwidth Total, Active User Bandwidth, Access Point Bandwidth, Role Bandwidth, Location Bandwidth, SSID Bandwidth, RFIDS Log).
- Added the ability to customize reports.
 - Along with the reports already available (Bandwidth, User Log In/Outs, User Count), new reports were added (User Roaming, Location Status, RF Adjacencies, RF Alarms, Trap Alarms). Reports are configurable across many dimensions including users, devices, APs, roles, SSIDs, locations, and time.
 - The reporting engine was overhauled to allow background report generation and scalable performance – an improvement over of 2.1.
- Added the ability to allow vWLAN to be behind a NAT device.
 - The vWLAN can now reside in the core of a network with port-forwarding allowing cloud-based APs to contact it, even though the vWLAN does not have a public IP address.
- Added the ability to configure DynamicRF™ per radio and per AP template.
 - DynamicRF™ is no longer global, but can now be configured per radio at the AP template. This means certain APs (or radios) can be in Continuous mode, while others are in Set Once and Hold and others are disabled (depending on the desired use case).

vWLAN® Release Notes

- Added the support for Granular Administrative access, where administrators are given the following:
 - Granular and individual access to up to 86 different resources.
 - Create, Read, Update, or Delete (or a combination of them) access to the resource.
 - The same (or different) access based on the Domain/Tenant the in which the administrator resides.
 - Optional access to platform-level settings (such as, setting the IP address of the unit).
- Added the ability for the administrator to have an individual time zone, separate from that of the unit. This allows an administrator (residing in a different time zone than the unit) to see the local time.
- Added Lobby Administrator centric Guest Users and Receipt views with the following capabilities:
 - Lobby administrators can now only view/edit/delete guests that they personally have created, and cannot manipulate other guests.
 - Longer guest/user names (up to 72 characters) can be created
 - Ability to create up to 500 bulk guests at once
 - Ability to support Multiple Guest Receipts
 - Ability to fully configure the Guest Receipt (including logo, text and variable substitution)
 - After creating guest(s), the system will automatically create a PDF to allow the administrator to print the guests without additional clicks.
 - Ability to quickly create a guest using a Plan (template) that is similar to the Plan used for Hotspot creation.
 - Automatic deletion of expired and unused accounts.
 - Ability for a domain administrator to see who created which guests and to see log messages of when the guests were created.

Major Improvements for Release 2.2.1

- Streamlined UI with AJAX updates for user and AP counts.
 - Top-level navigation was replaced with a modern left hand menu. All were based on HTML5, CSS3, AJAX and the latest web technologies including iPad functionality.
- Streamlined the AP template model.
 - The AP template is now the key building block for configuration, and is now a single UI page instead of three separate pages.
- Expanded the AP jobs (Calibrate, Reboot, Apply Configuration per AP Template, Modified APs, etc.) selections.
 - Jobs can be run on a more fine grained selection of APs, including modified APs, APs in error states, and APs in specific templates.
- Added the ability to fully customize notifications (SNMP, syslog, email).
 - Every informational message is now shown in the UI and is completely customizable.
 - The administrator can choose to send syslog messages, SNMP traps, or emails based on the individual log message (including a different configuration per tenant).
- Streamlined the administrator tasks.
 - Pop-up notifications have replaced the top-level red text informing the administrator of pending tasks.
 - A count of tasks is shown in the menu bar which the administrator can select and choose to execute or delete.
- Added support for VMware 5.0 and updated versions of VMware 4.1.
- Separated the administrator web server (on port 3000) from the web authentication web server (on port 80 and 443). This ensures client traffic does not interfere with administrators.
- Added a debug log message to notify when an AP discovers an IP location.

vWLAN® Release Notes

- Modified the UI to display what is permitted in the Unregistered Role (by default). The UI no longer adds confusing Deny All Firewall Rules (and the UI outlines what must be added to allow traffic).

Multi-tenant Features for vWLAN 2.2

- Bulk guest user creation, guest templates (plans), and guest receipts
- Granular (RW/RO) administrator access
- RADIUS administrator authentication
- RADIUS accounting
- RF location-based tracking
- Local (non-Cloud) AP firmware upgrade
- Wired user support
- 802.1X machine authentication
- Captive portal support for non-English languages
- HotSpot account generation and expiration
- Library web authentication SIP2
- Ability to locate a wireless entity on a heat map
- Support for certificates for LDAP over SSL

Version 2.2.1-20 vWLAN Fixes

Fixes included in mandatory vPatch-2-2-1-20-2

- After upgrading to vPatch-2-2-1-20-1, the vWLAN served the self-signed cert instead of the uploaded SSL certificate.
- Certificate chain only works if an extra new line character is added to certificate file.
- If a non-trusted certificate authority (CA) signs the mail server's certificate, email notification delivery failed on the vWLAN because the certificate cannot be validated.
- If a range of ports were configured in a service and applied to a role, APs would not receive a configuration.
- New users were not added to the connections table.
- Option "c" (certificate cleanup: Removes any custom web server certificate) in the console menu did not remove a custom web server certificate.
- Users are not added to the connection table and the user count in Active Users in the UI does not accurately reflect the users on the system.

vWLAN® Release Notes

- Client devices sometimes failed to be redirected to their original destination after successful web authentication.
- Scale/performance issues with more than 700 APs
- Delay in GUI accessibility after vWLAN was rebooted.
- When upgrading from 2.1 to 2.2.1.20, the HTML spacing in the Login Screen must be between 0 and 100.
- It is possible to delete the built-in Un-registered role by renaming and then deleting. However, it is not possible to re-create the role with its special properties.
- It was not possible to create more than 400 locations
- It was not possible to switch partitions using the console menu option.
- If a TCP and UDP service were added to a service group and that service group was applied to a role, all services (rather than just those defined in the service group) were allowed when that policy rule was processed during client activity.
- BSAP would get stuck in the "Channel Scanning" state.
- Some Android devices did not get redirected for web authentication.
- It was not possible to poll user status via the API.
- The administrative web GUI became inaccessible and web redirection for clients would not be possible.
- The system did not recover from a process restart and users were not able to connect.

Fixes from 2.2.0.17 and 2.2.1.19 to 2.2.1.20

- Internal User created by Hotspot functionality is not deleted from the system when the account expires.
- Unable to complete upgrade successfully from 2.2.1 multi-tenant conditional release to 2.2.1.19
- SNMP location, contact, and hostname field is changed to "Location" , "Contact", and "Host0, Host1, and so on" after upgrade from 2.1 to 2.2.1.19
- If a radio is disabled in the 2.1 configuration, upon upgrade to 2.2.1.19, the AP/template setting is migrated over as "dual-mode" rather than "disabled." Further, affected APs are not placed on a map and its hostname & location are not imported.
- If service names greater than 16 characters existed, a validation failure occurs when trying to maintain the current config. The result is that portions of the config will not be carried over.
- If there are both service and destination groups in the 2.1 configuration, it is possible for them to conflict and cause a validation failure when trying to maintain the current config during an upgrade to 2.2.1.19. The result is that portions of the config will not be carried over.
- If hostnames greater than 24 characters exist in the 2.1 configuration, a validation failure occurs when trying to maintain the current config. The result is that portions of the config will not be carried over.

Fixes from 2.1 to 2.2.1

The following list outlines bug fixes and other improvements since release 2.1:

- Policies in a role could not be moved using Google Chrome.
- Policies Row Management Options did not function using Google Chrome.
- The Ping Utility would accept invalid IP addresses.
- Deleting SSIDs and/or Wired Access Groups used by AP templates did not modify the APs.
- If root@adtran.com was changed to another email, root@adtran.com was not recreated during upgrade.
- The domain administrator had access to root administrator pages via direct URL entry.
- Admin Authentication: The Admin Auth Server precedence was not being replicated on the secondary vWLAN server.
- No adjacent APs were displayed if dynamic RF was disabled.
- No third-party adjacent APs were displayed if dynamic RF was configured to only consider Bluesocket APs.
- The vWLAN appliance was at 100 percent disk usage after 1 week with 50 Domains/500 APs/20K users.
- Logs did not display the proper average value (negative values were sometimes displayed).
- Upgrading vWLAN with Maintain Config checked did not maintain the Root Logs and Alarms.
- The message displayed after editing a location and making no changes was improved.
- The Average user count on the Log message was incorrect (outside the minimum/maximum ranges).
- Calibration end time was not being displayed.
- User count reports displayed an error in the number of users and a negative average user count.
- Guest users did not appear if the administrative user had read only access to guest access.
- HeatMaps were missing features such as *RSSI Cutoff and Filter with SSIDs*.
- HA Snapshot took longer than the countdown causing repeated 10 second loops until complete.
- Initial HA snapshot was successful but the status message displayed was not accurate.
- Logging Scalability tracking issues using vedge sim were corrected.
- vWLAN did not display an Unsupported AP error when a NetVanta 160 was connected to the system.
- Radius Admin Auth would return an incorrect role.
- vWLAN was sending outbound traffic to open source update sites.
- Blue-vWLAN-1.0-MIB.txt MIB file used illegal field names containing underscores.
- AP traffic capture filters did not function for VLAN tagged frames.

vWLAN® Release Notes

- APs were not being marked modified when changing AP Template System configurations.
- vWLAN would not restore after reboot.
- The Unlimited Hotspot Account Creation option should not have been available if the configured expiration had expired.
- BluesocketSyslogThread triggered an internal error.
- No radius accounting stop message was displayed when a local user expired.
- The guest account created time was updated every time a new account was created.
- The administrative user with no configured access for Analyze could still view everything under the Analyze tab.
- After restoring a configuration without applying it, the administrator was prompted to enter the administrator username and password before the configuration could be seen.
- The vWLAN controller was able to contact the TFTP server when Remote Location was selected under Wireless>Firmware.
- The attributes of services could not be modified when the selected protocol was Other.
- AP was going into an error state when a second capture on the wireless interface was started without stopping first.
- Page refresh would spawn another capture in Safari.
- A better method of tracking stale captures was required.
- The SNMP Trap generated for a Failed Internal User Login says RADIUS user instead of Internal user.
- The AP Restarted alarm was logged with a BSSID of 00:00:00:00:00:00.
- MIBs could not be loaded into Plixer Scrutinizer.
- DynamicRF was not reducing the power when appropriate.
- BSAPs appeared in Provision > Wireless > AP with an Unknown Platform and a Modified Config.
- Usernames with more than 64 Characters caused process crashes.
- The Shaping setting of Mbits/second incorrectly shaped traffic.
- Logging in with Guest Access account resulted in a 504 Server Timeout response.
- A non-standard SMTP port with the SMTP Authentication Method set to None would not function.
- Certain reports were blank when displayed.
- HA was out of sync with API error messages.
- vWLAN was running out of memory.
- Guest users could not authenticate when a fully customized login page was used and Allow guest logins was selected from the Login options.
- The source IP address could not be specified when getting Wired AP PCap.
- Requesting log was sent to vWLAN when an AP discovered a location.
- The UI did not indicate what was allowed in the unregistered role.
- The deny DHCP and deny ANY rules were automatically added when creating a role.

Version 2.2.1 vWLAN Errata

The following is a list of errata that still exist in vWLAN 2.2.1.20 with mandatory patch vPatch-2-2-1-20-2. These are separated into categories.

General

- If a PEM encoded X509 certificate is entered (in Configuration > Settings > Platform > Certificate File) with typographical errors that make the certificate unreadable, the Admin GUI cannot be restarted.
- Users are not being transitioned into their final Role after the Radius-Accept and will remain in the unregistered role.
- SNMP Contact Field cannot contain special characters or the vWLAN will not replicate to HA Node.
- Guest User Receipts allows GIF image file uploads which are unsupported.
 - The following error message is returned when a guest user is created and a GIF image file is used in the Guest Receipt: "We're sorry, but something went wrong. Retry the action, and if you continue to get this error, contact customer support."
- If the same image file was used in the Guest Receipt for both the Logo Image and Icon Image positions, and it is removed from only one of those positions, Guest User creation failed with the following error returned: "We're sorry, but something went wrong. Retry the action, and if you continue to get this error, contact customer support." Once the image has been added back, Guest User creation is successful
- When you allow HTTP/HTTPS outgoing to a destination hostname apple.com or *.apple.com in the un-registered role, the web request will get redirected to the login page instead of being allowed outbound.
- While the system allows the Role bandwidth to be higher values, any value higher than 65535 Kbps (or the equivalent) is treated at 65535 Kbps by the AP. The exception is if no limit (0) is specified, then no limit is enforced
- 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. If slow roaming is observed, an RF calibration is recommended.

Upgrade from 2.1 to 2.2.1

- SNMP community strings with less than 6 characters are converted to "public" during the migration from 2.1.0.14 to 2.2.1.20.
 - The following platform alarm is produced during migration:

config upgrade failed Failed to update RootSetting rw_community_string
error Validation failed: Value is invalid update
varRootSettingrw_community_string.update_attributes!value => ERRORS

vWLAN® Release Notes

- LDAP bind user is always used, regardless of how "Bind all Queries as LDAP Bind user" is configured. So, if the bind user is wrong, LDAP will fail.
- Special character stripped from LDAP/AD authentication server bind user when migrating from 2.1.0.14 to 2.2.1.20.
- Some characters in custom Web Login HTML code are removed or changed during an upgrade from the 2.1 platform to 2.2.1.20, resulting in possible failure to redirect clients.
- Migration from 2.1.0.14 to 2.2.1.20 fails to migrate NTP host as FQDN in 2.1.0.14.
 - The following platform alarm is produced during migration:

config upgrade failed Failed to update RootSetting ntp_servers error Validation failed: Value is invalid update
varRootSettingntp_servers.update_attributes!value => 4.2.2.1,
pool.ntp.org ERRORS
- Migration from 2.1.0.14 to 2.2.1.20 fails due to "Login image does not exist" in 2.1.0.14 web login form configuration.
 - The following platform alarm is produced during migration:

config upgrade failed Failed to update LoginForm error Validation failed: Login image Login image does not exist update varLoginForm1 = LoginForm.find_or_create_by_id!1, noleft => 0, login_attempts_minutes => 1, name => , hotspot_account_id => 1, r_t_padding => 60, title => , r_width => *, enable_tos => , powered_by => loginPower-black.gif, redirection_destination => destination, redirection_external
- Migration from 2.1.0.14 to 2.2.1.20 fails due to "Not a valid color" in 2.1.0.14 web login form configuration.
 - The following platform alarm is produced during migration:

config upgrade failed Failed to update LoginForm error Validation failed: L g bgcolor Not a valid color, L g bgcolor Not a valid color, L g fgcolor Not ... update varLoginForm6 = LoginForm.find_or_create_by_id!6, noleft => 0, login_attempts_minutes => 1, name =>, hotspot_account_id => 6, r_t_padding => 0, title =>, r_width => *, enable_tos => , powered_by => loginPower-black.gif, redirection_destination => destination, redirection_extem
- Custom HTML not supporting Chinese characters after upgrade to 2.2.1 from 2.1

Notifications and Reporting

- Notification emails do not include AP hostname and domain. Only the MAC address of the AP is included.
- Configuration changes are not recorded in system logs
- New reports cannot be generated by non-root admins.
- When creating a report, the page may continue to show "Report is still running" even though the report has finished. Refreshing the page in the browser should update the page. If for some reason the report has not yet finished over a long period of time, the Report service can be restarted to clear this condition by navigating to Administration->Restart and selecting Restart Reporting Daemon.
- Location Status report has no results. This report only shows changes in the statuses of locations. Naming of the report will be clarified in a future release.

User Interface

- When using the UI search for sub-strings within a longer string, no search results show unless the entire string is matched. If all the text from the beginning of the string is entered, the search will be successful.
- When creating a new platform AP firmware, if a file is selected that is not valid firmware, an error will be displayed but the UI will then redirect to the domain AP firmware page rather than the platform AP firmware page.
- Clicking on column to sort bandwidth download doesn't sort ascending/descending.
- When searching for AP Mac Address in Active Connections, it will return the wrong MAC address.
- Locations are showing inactive in the admin GUI, yet are actually active and traffic flow for users into the location is successful.
- vWLAN GUI reports: "One or more APs in an unlicensed state; AP Platform: Error; AP Error message: All radios disabled, Command Timeout, Retry command or Reboot BSAP. However, BSAP is licensed properly and an SSID is configured."
- Platform Traceroute utility does show error message for invalid IP address
- Platform Ping utility does not show error message for invalid IP address
- Some active users may show on AP page as Unknown users.

Copyright and Trademark Information

Copyright © 2012, 2013 ADTRAN, Inc. All rights reserved.

No part of this document may be reproduced in any form or by any means, electronic or manual, including photocopying without the written permission of ADTRAN, Inc.

The products described in this document may be protected by one or more U.S. patents, foreign patents, or pending patents.

This document is provided *as is* without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose or non-infringement. This publication could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein; these changes will be incorporated in new editions of the document. ADTRAN, Inc. may make improvements or changes in the products or the programs described in this document at any time.

Bluesocket, The Bluesocket Logo, vWLAN, Secure Mobility, BlueView, BlueProtect and BlueSecure are trademarks or registered trademarks of ADTRAN, Inc.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions

All other trademarks, trade names and company names referenced herein are used for identification purposes only and are the property of their respective companies.