vWLAN® 2.2.1 and BSAP 6.6.0 Release Notes

Software Version: V2.2.1.20

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

Access Point Software Version: V6.6.0

BSAP Models Covered: 1800 (v1 and v2), 1840, 1920, 1925, 1930, 1935, 1940

Document Date: February 15, 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. Please take a few moments to familiarize yourself with the contents of this document. Unless otherwise noted, vWLAN® refers to any Bluesocket vWLAN® product (hardware or virtual).

Contents

Important Notes

Important Notes - Upgrading

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 settingsmust be reconfigured when upgrading to vWLAN 2.2.1. Refer to Unsupported Features from 2.1 and Release Guidelines (**especially the VMware section**) below before upgrading. After upgrading, the administrator UI is available at https://<IP address>:3000, where IP is the IP of the unit, and the administrator user is root@adtran.com with password blueblue.

APs must be upgraded to the BSAP 6.6 release after the vWLAN is upgraded. The AP firmware is not included in the vWLAN image, so the latest AP firmware version must be downloaded.

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 at the following URL: https://supportforums.adtran.com

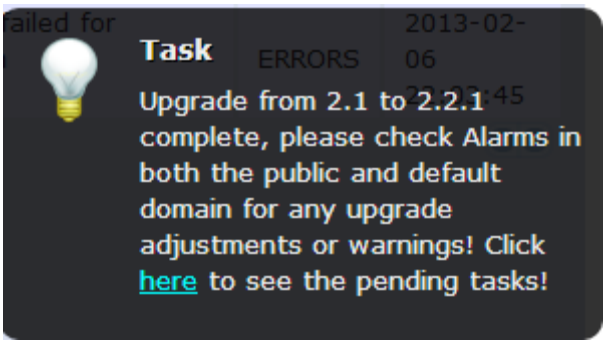
vWLAN 2.1 to vWLAN 2.2.1 Upgrade Considerations

1. Administrator UI is only reachable on port 3000 (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. Any local AP settings (not done at the AP Template level) are not retained.
4. Role-based inherited firewall policies are not retained.
5. Disabled MAC devices are not retained.
6. All local user expiration (or enablement in the future) must be reconfigured.
7. Internal 802.1x SSIDs are not brought forward. Backup 802.1x servers must be reconfigured.
8. Logs, Reports, Alarms are not brought forward.
9. All notifications and email settings must be reconfigured (or the default values can be used).
10. 2.2.1 uses a new API (REST), and all API-based apps must be rewritten. Refer to the administrative guide.
11. The VMware system requirements differ from 2.1 to 2.2.1. Refer to the section **Virtual Machine Bootup/Setup** under 2.2.1 Release Guidelines. Release 2.2.1 requires a new OVA.

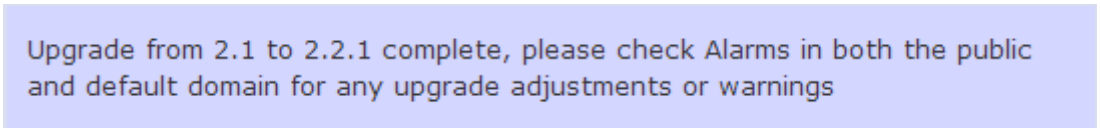
The next section shows how to view upgrade adjustments.

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:



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 and resolve them under your 2.1 configuration and then upgrade again.

Important Notes - BSAP-19XY Features Not Supported for Release 6.6.0

The new BSAP-19xy APs do not support the following features for Release 6.6.0:

- Dual Mode
- Minimum Transmit Rate
- Over the Air Fairness

Important Notes - Unsupported Features from vWLAN 2.1

The following lists features supported in 2.1 but not supported in 2.2.1.

- BlueProtect support
- 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.

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 customer support for suggestions.

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, 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. To acquire AP licenses, go to the **ap_licenses** tab. Make a license request and email it, your name, company name, and phone number to your sales representative or BluesocketLicense@ADTRAN.com . Existing lifetime vWLAN 2.1 licenses can be applied to vWLAN 2.2.1, and licenses in 2.1 are maintained in the upgrade from 2.1 to 2.2.1.

Licensed Features

When making the 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™.

V6.6.0 BSAP Features and Improvements

Major Access Point Features for Release 6.6.0

- There are five new APs supported under vWLAN 2.2.1, with BSAP 6.6 software:
    - BSAP-1920 – Indoor, Internal Antenna, 2x2
    - BSAP-1925 – Indoor, External Antenna, 2x2
    - BSAP-1930 – Indoor, Internal Antenna, 3-stream
    - BSAP-1935 – Indoor, External Antenna, 3-stream
    - BSAP-1940 – Outdoor, External Antenna, 3-stream
- Added a configurable reboot timeout after the control channel is lost. This allows the APs to continue to service authenticated users, if the WAN link is lost.
- Added support for SCP firmware upgrade for the new BSAP 19XX Series APs.
- When configuring an AP firmware on an external server (TFTP for 18x0 series, or SCP for 19xy series), the vWLAN no longer needs to download the firmware from the server, allowing the external server to be at a remote office/site behind a NAT device.
- When APs are upgrading for the first time, they now appear in the UI while they are upgrading.
- When the 1800 series APs detect non-802.11 interference, instead of the AP rebooting, vWLAN notifies the administrator of severe non-802.11 interference in the UI (and, optionally, sends an external Syslog, SNMP Trap, or email). The message is "*[BG or A]* r*adio: non-802.11 interference detected - change the channel and then reboot the AP*.
- Added the ability (on a per SSID basis) to optionally convert broadcast and multicast traffic to unicast traffic to optimize RF performance for applications such as multicast video that requires higher bandwidth.
- Added regulatory domain support for China on the BSAP 1800v2 and 1840 platforms.

V2.2.1 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).

- Added the support for Granular Administrative access, where adminstrators 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 Improvement 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.
- 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).

Bugs from vWLAN 2.1 that were fixed in the 2.2.1 Release

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.

- 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.

Bugs from vWLAN 2.2.0.17 and 2.2.1.19 that were fixed in the 2.2.1.20 Release

- 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.

V2.2.1 Release Guidelines

Virtual Machine Bootup/Setup

- The VM memory and CPU recommendations have changed between 2.1 and 2.2.1.

  Guideline: You should use 4 cores and 4 GB of RAM for 2.2.1.

- The VM file system requirement has grown between 2.1 and 2.2.1.

  Guideline: A vWLAN 2.1 Virtual Machine with a 7 Gig footprint can *not* be upgraded to 2.2.1. Instead, you must deploy the new 2.2.1 OVA (41 Gig footprint). You can: 1) reconfigure your system from scratch, or 2) downgrade the new OVA to 2.1, restore your 2.1 configuration there, and then upgrade to 2.2.1.

- VMware is not going to the fallback IP address if the network interface is set to DHCP and link is down on the network interface.

  Guideline: If DHCP is unavailable, ensure that the VMware interface has a link, and that the fallback IP gateway (192.168.130.254) is valid on that network.

Hardware Appliance

- Error messages appear in the serial console: EDAC MC0: UE page 0x0, offset 0x0, grain 0, row 3, labels ":": i3200 UE.

  Guideline: Ignore these messages, they are benign.

QoS

- 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.

  Guideline: This will be fixed in a future release.

Wired Support

- After upgrade from 2.1 to 2.2.1, there are no Wired Access Groups in the Status UI.

  Guideline: Restart the Access Point User Manager(s) and the groups will be shown.

Reports

- When generating a report, the list of Users contains a blank entry.

  Guideline: This entry tracks users in the Unregistered Role or Default SSID Roles.

- An administrator with only Create permissions and not Destroy permissions on Reports cannot create a second report because the first one must be deleted.

  Guideline: For reports, Create, Destroy, and Update permissions should usually be given.

- A platform administrator with Full access on Platform and Read-only access on Reports at the Domain level will receive an error when selecting the Domain report tab (if no report already exists).

  Guideline: Ignore the error, or give Create, Destroy, and Update permissions.

UI

- When using the UI search for sub-strings within a longer string, no search results show unless the entire string is matched.

  Guideline: Enter all the text from the beginning of the string.

- When an invalid file is uploaded on the *platform/ap_firmwares/new*, to the file is validated and the user is redirected to the *available_ap_firmwares/new* page.

  Guideline: Click back to the platform link and upload the firmware there.

- The *No file chosen* validation is not being done on the Create New AP Firmware page.The *Something went wrong* error appears.

  Guideline: Ignore the error. Click back and re-upload the firmware.

2.1 to 2.2.1 Upgrade

- Duplicate DHCP Server in services in Roles based Access Control.

  Guideline: Ignore the service, or delete it. It's the same port, so either DHCP Server or DHCP-Server can be used in firewall rules for port 68.

BSAP 6.6.0-25 Release Guidelines

- During a BSAP 19xx AP firmware upgrade, if the SCP connection is lost it will not be detected again for a period of 2 hours.

  Guideline: BSAP still reports accumulated byte counts. If the byte count is not increasing according to WAN link capacity, the administrator should check the server and optionally send updated server parameters.

- During a BSAP.18xx AP firmware upgrade, if the server parameters are incorrect or the AP could not reach the server, the AP will not recover.

  Guidelines: The only way to recover is to reboot the AP through a PoE reset or physically cycle the power on the AP. The customer must ensure the correctness and connectivity of the external TFTP server.

- APs not setting the Tx Power sent dynamically to value sent by vWLAN in ContinuousRF mode
  Guidelines: The user should manually set the recommended TX power by editing power and applying it to the AP.

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. (Packet Aggregation should be enabled for only the BSAP 19xy series, so in a mixed hardware environment, use AP templates specific to the hardware of the AP.) 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.

- It is highly recommended that all 802.11n client drivers are updated to the latest version before doing any system or performance testing.
- Running in a mixed mode environment (i.e. with legacy clients) will impact the 802.11n client's performance.

- It is highly recommended that WEP, WPA, and TKIP not be used, but WPA2 used instead.
- 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.

External 802.1x Server

- When using an external 802.1x Radius server, the following settings are recommended:
  - Increase the session timeout attribute to a high value (such as, 86,400 seconds) or do not set a value in the Radius attributes.
  - Ensure that the value for fast session resumption (fast reconnect under Windows) is disabled on both the server and the clients.

Appendix: New Multi-tenant Features from vWLAN 2.2

The following features were added since release 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

Copyright and Trademark Information