# RELEASE NOTES

BSAP 6.7.0-23
December 23, 2013

## 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

BSAP 6.7.0-23 is a maintenance release that addresses customer 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 6*.

A list of new or updated documents for this release appears in *Documentation Updates on page 7*.

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 BSAP 6.7.0-23.

- BSAP 1800v1 and v2
- BSAP 1840
- BSAP 1920/1925
- BSAP 1930/1935
- BSAP 1940

## Wireless Regulatory Compliance

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

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

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

## Upgrade Instructions

Bluesocket Access Point firmware version 6.7.0.17 is the minimum version required for interoperability with vWLAN 2.3.0.09, but version 6.7.0.23 is strongly recommended. Both versions are backward compatible with vWLAN 2.2.1.20. In order to avoid access point downtime after the vWLAN is upgraded from 2.2.1.20 to 2.3.0.09, consider upgrading Bluesocket access points in advance.

To upload locally stored AP firmware manually, follow these steps:

1. Upload new AP firmware and apply to an AP template:

 

a. Navigate to the Configuration tab and select Wireless > AP Firmware.

b. If you are uploading firmware for a domain, select the Domain tab. If you are uploading firmware for the vWLAN platform, select the Platform tab.

c. To upload the new AP firmware, select Create AP Firmware at the bottom of this menu.

d. Select the new firmware file from the location in which you stored the downloaded firmware by selecting Browse.

e. Select the domains to which to apply the new AP firmware by using the + (plus) sign. If you are uploading to the domain view, the AP firmware will automatically be available in the domain.

f. Choose the template(s) to which to apply the firmware change.

g. Select Create AP Firmware (or Update AP Firmware if editing) to apply the changes. A confirmation is displayed indicating that the AP firmware has been successfully created or updated.

2. Apply the new or updated firmware to the AP by running the following domain tasks: Must apply configuration to APs and Must activate new AP firmware (in the case of 19XX model APs). Upgrade status can be monitored in the secure administrative GUI by navigating to Access Points on the Status tab.

## System Notes

As of vWLAN 2.2.x, AP firmware is not included in the vWLAN image. The latest AP firmware must be loaded in order to upgrade the APs.

### 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:

1. Use WPA2 (PSK or 802.1x) with advanced encryption standard (AES) when connecting 802.11n-based clients. A TKIP client will connect at a maximum transmit rate of 54 Mbps. It is highly recommended that WEP, WPA, and TKIP not be used, but WPA2 be used instead. Running in a mixed mode environment (i.e., with legacy clients) will impact the 802.11n client's performance.
2. 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.
3. 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.
4. Ensure that all 802.11n 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.

## Fixes

This section highlights major bug fixes in BSAP 6.7.0-23.

- When changing the traffic flow location in the role, clients were not moved to the new location.
- Clients associated to WPA/WPA2 SSIDs would be forced to reauthenticate when the RADIUS server failed to send the Master Session Key (MSK) within the MPPE-Send/Receive Keys.
- Clients could not connect to an 802.1X SSID on the BSAP 1800s.
- Certain clients were unable to get a DHCP address when moving from one SSID to another.
- Dynamic RF calibration failed to select the proper power and channel settings.
- Unsupported client negotiations between the client and AP caused the AP to reboot.
- Wired clients were intermittently unable to be redirected to the Captive Portal login page until after the AP was rebooted.
- BSAP 1930s rebooted with heavy roaming activity.
- Under certain circumstances, the BSAP 1940 rebooted while performing redirection to web authentication.
- It was not possible to log into a BSAP 1800v1 after changing the SSH password.

## Errata

The following is a list of errata that still exist in BSAP 6.7.0-23.

- AP doesn't support signficantly large port ranges in the role policies (I.e. 49152-65535).
- On BSAP 1900s, the 40 MHz mode cannot be enabled on the 2.4 GHz radio.
- The APs may stop accepting connections and require the AP to be rebooted.
- As part of location discovery, if DHCP is blocked on the AP's native network, DHCP release messages do not reach the DHCP server to clean up lease. Locations are still discovered.
- Users that moved from an open/unregistered SSID to an 802.1X SSID retained the NAC scope IP address.
- AP may reboot if it's servicing clients are in aggregation mode and the AP detects interference.
- When no SSID was configured in the AP template for a radio with the Radio Mode set to AP Mode or Dual Mode, RF alerts and adjacency information were not sent from the BSAP to the vWLAN.
- Dell Latitude 10-ST2e tablet devices running Windows 8 are not able to Authenticate via 802.1.x.
- If a default gateway is omitted from the BSAP network configuration and the RADIUS server(s) does not exist on the same broadcast domain, 802.1X (WPA/2-Enterprise) SSIDs come up as open SSIDs and do not enforce 802.1X authentication.
- BSAPs utilizing High Availability may not fall back to the primary even when configured to fall back.
- The AP doesn't support channel 56 in Taiwan.
- After sending an apply command, the BSAP remains in an Updating status and will not bring up its radios. A manual reboot of the AP clears the issue.

 

- Some mobile clients will not release NAC address until the radio is disabled and then re-enabled.
- Clients running a Virtual machine must operate in NAT mode versus Bridge mode.
- A NAS-IP-address or NAS-identifier is not present in the RADIUS Access-Request packet sent by the AP.
- If a DHCP offer contains certain options not requested in the DHCP discover, the location may not be added as an active location for the AP.
- Workaround: Ensure that DHCP offer options are only those requested in the DHCP discover.

## Documentation Updates

The following documents were updated or newly released for BSAP 6.7.0-23. 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 Administrator's Guide*
- *vWLAN AP Discovery*
- *Using APIs with vWLAN*
- *vWLAN Hardware Appliance Quick Start Guide*

 