



# Bluesocket vWLAN

## Release 3.7.0

Administrator's Guide

6ABSAG0001-31V

December 2020



## **Trademarks**

Any brand names and product names included in this manual are trademarks, registered trademarks, service marks, or trade names of their respective holders. Bluesocket, the Bluesocket logo, and vWLAN are trademarks or registered trademarks of ADTRAN, Inc.

## **To the Holder of this 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.

## **Software Licensing Agreement**

Certain ADTRAN systems may contain additional conditions for obtaining software upgrades.

## Third-Party Software

The software included in this product contains copyrighted software that is licensed under the GNU General Public License (GPL). For a list of third-party software and their licenses, go to <http://www.adtran.com/software/EULA>. You can obtain the complete corresponding source code of such software components from ADTRAN for a period of three years after our last shipment of this product by sending a money order or check for \$5 to:

ADTRAN, Inc, P.O. Box 933638, Atlanta, GA 31193-3638  
Please write **GPL Source for Bluesocket APs** in the memo line of your payment.

This offer is valid to anyone in receipt of this information.



901 Explorer Boulevard  
P.O. Box 140000  
Huntsville, AL 35814-4000  
Phone: (256) 963-8000  
www.adtran.com  
6ABSAG0001-31V  
All Rights Reserved.  
Printed in the U.S.A.

## Conventions



### NOTE

*Notes provide additional useful information.*



### CAUTION!

*Cautions signify information that could prevent service interruption or damage to equipment.*



### WARNING!

*Warnings provide information that could prevent injury or endangerment to human life.*

## Table of Contents

<b>1. ADTRAN Bluesocket vWLAN Overview</b>	<b>11</b>
<b>vWLAN versus Traditional WLAN</b>	<b>11</b>
<b>vWLAN Components</b>	<b>13</b>
<b>vWLAN Concepts</b>	<b>13</b>
Wireless Technology	13
Fully Distributed versus Centralized Data	14
Layer 2 versus Layer 3 Architectures	14
Out-of-band NAC	14
Multicast Support	14
Bandwidth Control	14
Class of Service (CoS)	15
User and Machine-based Authentication	15
Location Autodiscovery	16
Multi-tenant Support	16
WPA2-Multikey Support	17
<b>vWLAN Solutions</b>	<b>18</b>
<b>2. vWLAN Hardware and Software Requirements</b>	<b>20</b>
<b>Required Hardware</b>	<b>20</b>
<b>Resource Requirements</b>	<b>20</b>
External Resource Requirements	21
ADTRAN Bluesocket APs	21
<b>Software Requirements</b>	<b>26</b>
SNMP	27
Licenses	27
IPv6 and vWLAN	27
Layer 3 Mobility	27
GRE Tunneling	28
Mesh Networking	28
Layer 7 Device Fingerprinting Support	28
DFS Support	28
Setup Wizard Support	29
WPA2-Multikey Support	29
Link Layer Discovery Protocol (LLDP) Support	30
Override Location with TPGI Support	31
VLAN Support	31
Probe Request Database Support	32
<b>Client Device Support</b>	<b>33</b>
<b>Browser Support</b>	<b>34</b>
<b>VMware Support</b>	<b>34</b>
<b>3. vWLAN Installation</b>	<b>35</b>
<b>Step 1: Installing vWLAN</b>	<b>35</b>

---

Installing the vWLAN Hardware Appliance . . . . .	35
Installing the vWLAN Virtual Appliance on VMware . . . . .	36
<b>Step 2: Installing the APs Associated with vWLAN . . . . .</b>	<b>37</b>
<b>4. Introduction to the vWLAN's GUI . . . . .</b>	<b>39</b>
<b>vWLAN Menu Structure . . . . .</b>	<b>40</b>
<b>General GUI Shortcuts . . . . .</b>	<b>41</b>
<b>Additional GUI Options . . . . .</b>	<b>41</b>
<b>5. vWLAN Administrators . . . . .</b>	<b>43</b>
<b>Creating an Administrator . . . . .</b>	<b>43</b>
<b>Changing the Administrator's Password . . . . .</b>	<b>46</b>
<b>Specifying the Administrator's Role . . . . .</b>	<b>47</b>
<b>Specifying Administrator Authentication . . . . .</b>	<b>48</b>
RADIUS Administrator Authentication Considerations . . . . .	49
Configuring RADIUS Administrator Authentication . . . . .	50
<b>6. vWLAN Platform Configuration . . . . .</b>	<b>52</b>
<b>Configuring the vWLAN Network Interfaces . . . . .</b>	<b>52</b>
<b>Configuring a vWLAN Network Interface Static Route . . . . .</b>	<b>54</b>
<b>Changing the Administrator Session Idle Timeout . . . . .</b>	<b>55</b>
<b>Configuring the vWLAN Time Settings . . . . .</b>	<b>55</b>
<b>Configuring the Platform SNMP Parameters . . . . .</b>	<b>57</b>
<b>Configuring the vWLAN TLS 1.0 Setting . . . . .</b>	<b>58</b>
<b>Configuring vWLAN Platform Branding . . . . .</b>	<b>59</b>
<b>Verifying the vWLAN Software Version . . . . .</b>	<b>59</b>
<b>Performing System Maintenance . . . . .</b>	<b>61</b>
System Restart . . . . .	61
Configuring Backup or Restore Parameters . . . . .	62
Using Show Tech for Technical Support . . . . .	63
Managing the vWLAN Runtime Image . . . . .	64
Managing Patches . . . . .	66
<b>Restarting the vWLAN . . . . .</b>	<b>67</b>
<b>Configuring High Availability . . . . .</b>	<b>68</b>
High Availability Process . . . . .	68
Replicating Master Configuration Changes on the Node . . . . .	71
<b>Working with Certificates . . . . .</b>	<b>71</b>
Installing Certificates to vWLAN . . . . .	71
Uploading Certificates to vWLAN . . . . .	74
Configuring Additional vWLAN Settings for Certificates . . . . .	75
Managing vWLAN Certificate Settings . . . . .	79

<b>7. vWLAN Domain Configuration</b> .....	<b>85</b>
<b>Creating the Domain</b> .....	<b>85</b>
<b>Associating Administrators to a Domain</b> .....	<b>87</b>
<b>Configuring Domain Destinations</b> .....	<b>88</b>
<b>Creating Domain Destination Groups</b> .....	<b>90</b>
<b>Configuring Domain Services</b> .....	<b>91</b>
<b>Creating Domain Service Groups</b> .....	<b>92</b>
<b>Configuring Domain Locations</b> .....	<b>94</b>
<b>Configuring Domain Location Groups</b> .....	<b>95</b>
<b>Configuring Domain Roles</b> .....	<b>96</b>
Un-Registered Role Type .....	98
Registered Role Type .....	100
<b>Configuring Domain Role Schedules</b> .....	<b>105</b>
<b>Configuring Web-based (Captive Portal) Authentication</b> .....	<b>107</b>
Disable TLS 1.0 .....	109
External Server Authentication .....	109
Configuring Local User Authentication .....	126
Device Authentication .....	128
Bulk Import of Devices .....	130
<b>Configuring Domain Accounting</b> .....	<b>131</b>
<b>Configuring Domain Settings</b> .....	<b>133</b>
<b>Configuring Domain Users</b> .....	<b>136</b>
<b>Configuring Domain Branding</b> .....	<b>138</b>
<b>Domain Configuration Backup</b> .....	<b>138</b>
<b>8. Configuring vWLAN APs</b> .....	<b>140</b>
<b>Editing AP Firmware</b> .....	<b>140</b>
Uploading Locally Stored Firmware .....	140
Uploading Firmware Stored on a Server .....	141
Troubleshooting AP Firmware .....	143
<b>Associating APs with a Domain</b> .....	<b>145</b>
<b>Using AP Discovery to Connect APs to vWLAN</b> .....	<b>147</b>
AP Discovery Process .....	147
<b>Licensing APs</b> .....	<b>148</b>
Obtaining AP Licenses .....	148
Uploading License Files .....	148
<b>Configuring AP Templates</b> .....	<b>149</b>
Creating AP Templates .....	149
Configuring vWLAN for CNA Support .....	160
Configuring the DynamicRF Profile .....	162

---

Applying the AP Template to AP(s) . . . . .	164
<b>Configuring Additional AP Settings . . . . .</b>	<b>165</b>
<b>Viewing APs . . . . .</b>	<b>168</b>
Viewing AP Details . . . . .	169
<b>Viewing AP States . . . . .</b>	<b>170</b>
<b>Resetting and Rebooting APs . . . . .</b>	<b>171</b>
<b>Configuring AP Jobs . . . . .</b>	<b>173</b>
<b>9. vWLAN Setup Wizard . . . . .</b>	<b>175</b>
<b>Launching the Setup Wizard . . . . .</b>	<b>175</b>
<b>Using the Setup Wizard . . . . .</b>	<b>176</b>
Step 1: Configure the Administrator . . . . .	176
Step 2: Verifying the Primary and Guest Wireless Networks . . . . .	177
Step 3: Reviewing the Configuration . . . . .	179
<b>Applying the Setup Wizard Settings . . . . .</b>	<b>179</b>
<b>10. vWLAN Serial Console Configuration . . . . .</b>	<b>181</b>
<b>vWLAN Serial Console Configuration . . . . .</b>	<b>181</b>
Accessing the vWLAN Serial Console Menu . . . . .	181
vWLAN Serial Console Configuration Commands . . . . .	182
<b>AP Serial Console Configuration . . . . .</b>	<b>183</b>
Accessing the AP Serial Console Menu . . . . .	183
AP Serial Console Configuration Commands . . . . .	184
<b>11. vWLAN Wireless Configuration . . . . .</b>	<b>188</b>
<b>Configuring an SSID . . . . .</b>	<b>188</b>
<b>Configuring a Tunnel Profile . . . . .</b>	<b>198</b>
<b>Viewing Adjacent AP Neighbors . . . . .</b>	<b>201</b>
<b>12. vWLAN Unified Access Configuration . . . . .</b>	<b>202</b>
<b>Configuring Unified Access Groups . . . . .</b>	<b>202</b>
<b>Configuring Switches for Unified Access . . . . .</b>	<b>205</b>
<b>Unified Access Redundancy . . . . .</b>	<b>205</b>
<b>Viewing the Status of Unified Access Users . . . . .</b>	<b>206</b>
<b>13. Configuring Client Connections . . . . .</b>	<b>207</b>
<b>Customizing vWLAN Login Forms and Images . . . . .</b>	<b>207</b>
Basic Login Form Configuration . . . . .	208
Configuring Authentication using User Name and Password . . . . .	208
Configuring User Login Authentication Using an Email Address . . . . .	209
Specifying the Login Form Language . . . . .	210
Configuring External Redirects . . . . .	211

Configuring the User Service Agreement . . . . .	213
Specifying the Login Attempts Parameters . . . . .	214
Configuring the Visual Elements of the Login Form . . . . .	215
Uploading Images and Multimedia for Login Forms . . . . .	220
Customizing the Login Language . . . . .	221
Viewing Customized Login Pages . . . . .	225
<b>Configuring Guest Access Parameters . . . . .</b>	<b>227</b>
Configuring Guest Receipts . . . . .	227
Creating Guest User Accounts . . . . .	229
<b>Wireless HotSpot Account Generation . . . . .</b>	<b>231</b>
Hotspot Plan Configuration . . . . .	231
Hotspot Account Configuration . . . . .	233
Friends and Family Account Example Configuration . . . . .	237
<b>Configuring WPA2-Multikey Client Connections . . . . .</b>	<b>238</b>
WPA2-Multikey Use Cases and Authentication Process . . . . .	238
WPA2-Multikey Configuration Considerations . . . . .	240
Configuring the RADIUS Server for the WPA2-Multikey Feature . . . . .	240
Configuring the WPA2-Multikey Feature in vWLAN . . . . .	242
<b>14. Managing AP Networks . . . . .</b>	<b>244</b>
<b>Using Heat Maps . . . . .</b>	<b>244</b>
<b>Configuring Wireless IDS Alerts . . . . .</b>	<b>247</b>
<b>Managing Users and Locations . . . . .</b>	<b>252</b>
Viewing/Acknowledging Wireless IDS Alerts . . . . .	253
<b>15. vWLAN Management . . . . .</b>	<b>255</b>
<b>Managing Domain Storage Settings . . . . .</b>	<b>255</b>
<b>Configuring Notifications . . . . .</b>	<b>256</b>
Notification Templates . . . . .	256
Creating Notification Templates . . . . .	261
Information Messages . . . . .	264
<b>Administrative Tasks . . . . .</b>	<b>265</b>
<b>Configuring vWLAN Jobs . . . . .</b>	<b>265</b>
<b>Diagnostic Tools . . . . .</b>	<b>267</b>
Platform Administrator Diagnostic Tools . . . . .	267
Domain Administrator Diagnostic Tools . . . . .	268
Packet Captures . . . . .	269
<b>Viewing and Searching Logs . . . . .</b>	<b>271</b>
<b>Viewing Alerts . . . . .</b>	<b>272</b>
<b>Using the Reporting Dashboard . . . . .</b>	<b>273</b>
Customizing the Report Dashboard Widgets . . . . .	276
<b>16. vWLAN Implementation on Public and Private Networks . . . . .</b>	<b>280</b>
<b>17. Additional Resources . . . . .</b>	<b>282</b>



## List of Figures

Multi-tenant Network Topology . . . . .	17
Carrier Hosted Solution . . . . .	18
Enterprise Hosted and Managed Solution . . . . .	19
Small to Medium Business Hosted and Managed Solution . . . . .	19
Captive Portal Login Page . . . . .	107
Client Authentication Process . . . . .	108

---

## List of Tables

Traditional WLAN versus vWLAN . . . . .	12
BSAP 2000 Series . . . . .	24
BSAP 1900 Series . . . . .	24
WPA2-Multikey Supported RADIUS Attributes . . . . .	29
TLVs Included in LLDP Transmissions from AP . . . . .	31
BSAP 1800 Series AP Status and Radio LED Definitions . . . . .	37
BSAP 1800 Series AP Network LED Definitions . . . . .	38
Default Antenna Gain Values . . . . .	167
vWLAN Serial Console Configuration Commands . . . . .	182
Heat Map Signal Strength Color . . . . .	246
Supported RF Alerts in vWLAN . . . . .	247
Additional vWLAN Documentation . . . . .	282

## 1. ADTRAN Bluesocket vWLAN Overview

The ADTRAN Bluesocket virtual wireless local area network (vWLAN) is a wireless network solution that virtualizes the WLAN, providing a number of benefits to service providers, enterprise and small to medium sized businesses.

The vWLAN architecture is designed to support a greater number of APs within a single software instance than what is possible with traditional hardware controller based WLAN deployments. As wireless demand increases, customers can simply add additional APs and licenses to expand their network. vWLAN removes the complexities of dealing with controller capacity by splitting control and management functions from data-plane functions and centralizing the management and control of the network. Further, security and mobility are distributed at the edge of the network, the logical placement in networks that are designed for scalability and high availability. Adding additional access points (APs) to the vWLAN system is as easy as installing software licenses, which extends coverage to thousands of APs without concern about controller capacity.

vWLAN's architecture is the first of its kind to create a truly unified wireless and wired network which delivers maximum efficiency by separating the data-plane from the network management and control plane. This is achieved through the use of intelligent 802.11n APs, which can support user authentication and traffic forwarding decisions at the edge of the network. Forwarding data traffic directly to the wired network frees enormous capacity within the wireless controller. More capacity means the vWLAN can deliver enhanced wireless management and control performance with far less dedicated hardware than traditional wireless LAN controllers, reducing carbon emissions and energy costs up to 80 percent, thereby minimizing total cost of ownership. ADTRAN's fully virtualized, software-based solution gives customers the flexibility to run vWLAN on a hardware appliance or VMware vSphere ESX/ESXi Hypervisor.

In addition, vWLAN provides state-of-the-art security features that provide network access control (NAC), authentication server integration, enhanced guest access, and role-based policy enforcement. vWLAN's identity-based access control also removes restrictions that were part of traditional WLAN solutions and provides more flexibility in managing wireless access.

### vWLAN versus Traditional WLAN

Virtualizing the traditional WLAN provides methods for scaling the WLAN as the demands for the network changes. More users, more devices, better coverage through support for more APs, higher bandwidth for applications, and an ability to support APs behind network address translation (NAT) devices are all benefits provided by vWLAN.

The traditional WLAN was arranged so that a gateway providing value-added services was established behind any manufacturer's AP. In this network type, guest access and security services were provided, and access control and security expertise were incorporated. When AP controllers were introduced into the WLAN architecture, thin access points and 802.11n were also introduced. vWLAN, however, is the first and only WLAN to place control on VMware. Using a virtualized WLAN eliminates the cost and constraints of a physical wireless controller, as in traditional WLAN models, and moves the control and management of the network to the data center while applying security at the edge of the network.

WLAN virtualization effectively eliminates the wireless controller hardware, and associated cost and bandwidth usage, by moving the control and management of the network to the hypervisor, rather than the AP or wireless controller. In addition, the data-plane of the network, where firewall and security policies are applied, are moved to the AP; saving bandwidth and avoiding hardware limitations as well as allowing data to continue to flow if there is a network interruption.

Furthermore, vWLAN provides more effective high availability than traditional WLAN by removing the need to duplicate expensive controller hardware cost because the software provides a back up virtual control instance. With high availability, a control plane failover is achieved with zero packet loss, so that data moves over the network with no interruption.

*Table 1* outlines the differences between traditional WLAN and the ADTRAN Bluesocket vWLAN.

**Table 1. Traditional WLAN versus vWLAN**

Traditional WLAN	vWLAN
Physical hardware controller.	Virtual software controller (controller-less).
Hardware controller at each site.	One software instance.
150 APs supported.	Thousands of APs supported.
4,000 users supported.	48,000 users supported.
\$25,000 typical cost.	\$0 typical cost.
Upgraded by forklift upgrade process.	Upgraded by software upgrade.
All traffic (management, control, and data-plane) must travel through a hardware controller with a throughput of 20 to 30 Gbps.	Traffic is separated into management/control and data planes. Data-plane is aggregated by the throughput of the APs in terabytes.
Guest access requires additional hardware and software.	Guest access is included in the software.
Unified support for both wired and wireless access requires additional hardware.	Unified support for both wired and wireless access is included as a software option.
Does not support virtualization strategy.	Does support virtualization strategy.
Does contain a single point of failure (the hardware controller) and the data session is severed with a control plane interruption.	Does not contain a single point of failure (data center based) and the data session is unaffected with a control plane interruption.
High availability requires duplicate hardware controller, and failover results in packet loss.	High availability is included in the product, and failover results in zero packet loss.
Unwanted traffic travels on the network to hardware controller.	Unwanted traffic is turned away at the AP.
Centralized hardware provides a target for hackers as a centralized point of risk.	Does not have centralized hardware which removes the hacking risk.
Is not VMware Ready certified.	Is VMware Ready certified.
Less sustainability.	More sustainability through reduced energy costs, hardware waste disposal, and carbon emissions.

**Table 1. Traditional WLAN versus vWLAN (Continued)**

Traditional WLAN	vWLAN
Single tenant.	Multi-tenant.
Wireless users only.	Support for third-party APs or wired users.

## vWLAN Components

The vWLAN solution is comprised of three basic elements: a vWLAN appliance (hardware) or virtual appliance (VMware), the APs, and software. A license is required for each AP that will operate on the vWLAN. The vWLAN runs on a low-cost appliance (hardware) or a no-cost virtual appliance (VMware).

vWLAN includes wireless intrusion detection, Layer 3 mobility (tunnelling), secure web-based authentication (captive portal), fully customizable captive portals, 802.1X authentication, a stateful firewall enforced at the AP, per-user bandwidth allocation, guest access, high availability, and full scalability. Guest access ranges from simple guest access (where guests can simply enter an email address, click to accept terms and conditions, or both) to more advanced guest access (with lobby administrators, email validation, sponsored accounts, and self-sponsored accounts). Optionally, you can add support for unified access (wired or third-party APs).

## vWLAN Concepts

The following sections describe concepts with which you should be familiar in order to get the most benefit from your vWLAN installation.

### Wireless Technology

vWLAN uses various wireless technologies in its operation and is based largely on 802.11n. In the 802.11n wireless standard, wireless media is used more efficiently than in the 802.11a/b/g standards. Some example benefits provided by the 802.11n standard include the ability to use multiple input multiple output (MIMO), which uses spatial multiplexing to provide greater throughput. MIMO uses multiple radios and antennas, called radio chains, to take advantage of multipath (multiple paths of the same signal) by sending multiple independent signals, known as spatial streams, that travel different paths because of the space between transmit antennas (known as spatial diversity). Sending multiple independent streams of unique data using spatial diversity is referred to as spatial multiplexing, which provides greater throughput. For example, if a MIMO AP sends two unique data streams to a MIMO client station that receives both streams, the throughput is effectively doubled. If three unique streams are sent, the throughput is tripled. In addition to using multipath, MIMO also compensates for multipath using antenna diversity, providing greater antenna range. Antenna diversity can be described as listening with multiple antennas for the best received signal, which increases the odds of uncorrupted data. The ability to combine multiple smaller packets into a single larger packet (packet/frame aggregation), the ability to acknowledge a sequence of packets instead of a single packet (block acknowledgment), and the ability for an AP to transmit in 40 MHz mode (channel bonding or HT 40) are all also benefits provided by the 802.11n protocol.

## Fully Distributed versus Centralized Data

vWLAN data is fully distributed, which means that the data flows from the wireless client, to the AP, to the network. Using a fully distributed, rather than centralized, data flow allows limitless data-plane scalability because there is no central bottleneck at a wireless controller. It also allows user-based virtual local area networks (VLANs) at the edge of the network, Layer 2 and Layer 3 mobility, quality of service (QoS) and class of service (CoS) at the network edge, and high availability features.

## Layer 2 versus Layer 3 Architectures

Unlike other WLAN architectures, vWLAN is purely a Layer 2 architecture, meaning that a wireless client gets an IP address and receives and sends Address Resolution Protocol (ARP) messages to the network. There is no proxy, router, or NAT device between the wireless client and the network in vWLAN, as there is in a Layer 3 model. This allows simple voice deployments, and seamless support for Layer 2 applications. The vWLAN architecture for mobility extends the Layer 2 network to remote APs. The APs can tunnel between each other using EtherIP (IP protocol 97) over Layer 3 to keep the client's Layer 2 experience in tact. Therefore, it is possible for a client to connect to an AP in one subnet and to receive an IP address from a remote network to which another AP is connected.

## Out-of-band NAC

vWLAN is an out-of-band NAC solution, therefore, client authentication happens at the vWLAN. Once the client's integrity has been certified during captive portal authentication, the client's IP address is changed and the client's data is then locally switched (out-of-band) at the AP.

## Multicast Support

vWLAN's Layer 2 architecture allows multicast support without the need for protocol awareness of Distance Vector Multicast Routing Protocol (DVMRP) or Protocol Independent Multicast (PIM) sparse mode (PIM-SM) (multicast must be allowed at the AP firewall). vWLAN is user-based VLAN ready, which allows an administrator to shrink broadcast domains easily and to place users into the proper network or VLAN-based on credentials.



### NOTE

*On a per-SSID basis, you can determine if the system should convert multicast and/or broadcast packets to unicast frames for wireless clients (this is already done for wired clients). Enable this feature by selecting the appropriate check box if you want to apply firewall policies to multicast traffic. Refer to [Configuring an SSID on page 188](#) for more information.*

## Bandwidth Control

With a distributed data-plane architecture, vWLAN limits per-user bandwidth at the AP. vWLAN provides the following benefits with regard to bandwidth:

- Ability to limit bandwidth on a per-user basis, preventing one user from overusing the wireless media and wide area network (WAN) uplink.
- Ability to limit bandwidth in the downstream direction (to the client), limiting downloads from the

Internet.

- Ability to limit bandwidth in the upstream direction (from the client), preventing clients from running abusive servers or becoming expensive upload endpoints.
- Ability to configure bandwidth limits individually with different values for upstream or downstream bandwidths, tailoring bandwidth settings to the end user.
- Ability to specify bandwidth as Kbps, KBps, Mbps, or MBps, allowing the administrator the desired bandwidth granularity.
- Ability to scale to thousands of APs and thousands of users, allowing growth and reducing cost in the future.
- Ability to maintain QoS and bandwidth counters or parameters across AP roaming areas, enforcing the bandwidth policy even when a user moves to a new AP.
- Ability to produce little load impact on the access plane, preventing the AP performance from suffering when bandwidth control is enabled.

## Class of Service (CoS)

vWLAN supports CoS at the edge of the network, using two components: packet prioritization, and packet remarking. The following are the CoS features available in vWLAN:

- **Packet prioritization** is a CoS method that happens in the downstream direction (wired to wireless). It is useful to prioritize wireless traffic to certain roles, such as IP phone roles. The AP can prioritize based on the input wired packet CoS tags (either 802.1p or Differentiated Service Code Point (DSCP), or the greater of the two), or it can prioritize to a static value. Wireless multimedia (WMM) is required for the client and is enabled by default.
- **Packet remarking** is a CoS method that is used in the outgoing or upstream direction (wireless to wired). It is useful when the upstream networks are CoS aware of 802.1p or (DSCP). 802.1p uses the VLAN header to apply a priority on a packet (0 to 7, where 7 is the highest priority). DSCP uses the IP header to apply a priority on a packet (0 to 63, where 63 is the highest). When WMM is enabled, the 802.11p frames contain a prioritization based on application. The AP can directly convert the WMM prioritization to a packet marking (in 802.1p, DSCP, or both). Alternately, the administrator can choose to set a static 802.1p or DSCP mark for all traffic in the role. This is useful for roles like IP phones or other voice devices.

## User and Machine-based Authentication

Some WLAN models perform security and VLAN segmentation based on a specific port or service set identifier (SSID). In vWLAN, the security policy is determined solely on the user's identity. This policy (or role) contains information such as, VLAN, QoS, and CoS settings. In the vWLAN model, a single SSID is needed in the network per encryption type to the AP, and depending on the user credentials, the user receives a different policy (and VLAN) based on identity. For example, you might want an open SSID for a guest, a preshared key (PSK) SSID for scanners, and an 802.1X SSID for corporate users. Each authentication or encryption type is set on a per-SSID basis. This is all accomplished at Layer 2, so the same SSID can service multiple IP subnets and broadcast domains. In addition, because the central vWLAN control is at the appliance, APs coordinate tunneling for remote VLANs between APs, allowing wireless users on local networks to reach other remote networks through Layer 3 tunnels between APs.

Machine authentication allows the domain machine or computer to authenticate, using 802.1X, before the machine user logs into vWLAN. This process uses the host machine name (host/computername.domain) as the user name, and the computer's domain machine account password as the password. The domain machine account password is automatically created when the computer is registered to the domain, allowing group policies to be applied and login scripts to execute when the user logs into vWLAN, as well as allowing users who do not have a locally cached profile on the domain computer to access vWLAN. Machine authentication emulates the full wired connection experience. Without machine authentication, you cannot apply group policies or run login scripts to map drives, connected printers, etc. In addition, users that have not logged into the domain computer before cannot login to vWLAN. If you do not require group policies, login scripts, or the ability for non-cached domain users to login to vWLAN, you can opt not to implement machine authentication.

## Location Autodiscovery

vWLAN has an AP autodiscovery feature that automatically discovers the native VLAN that the APs are using, and creates a location (the networks the AP and its users can reach) in the vWLAN user interface. Local subnets of the AP are irrelevant in centralized data-plane architecture because all the traffic is tunneled, but it is important in distributed architectures because these are the user's access networks. Each AP location is the network, subnet mask, and VLAN ID of the AP. The AP automatically discovers its native location based on its IP address and subnet mask. By default, this location is assumed to be untagged, however, if a native location with a VLAN tag is selected on the AP's configuration page, the AP will report its native location with a configured native VLAN tag. The AP automatically ensures the untagging/tagging of packets from clients on the same native location. Non-native tagged VLANs can be configured on the system (by specifying the VLAN, subnet mask, and network), which enables wireless users to access the network through the APs on tagged networks. When vWLAN asks the APs to discover the VLAN, if the VLAN is found, then the location goes active and wireless clients can use it. Otherwise, clients are held without addresses until the location becomes valid. A location is defined as a the VLAN ID plus a subnet and netmask. Each location must have a Dynamic Host Control Protocol (DHCP) server for the AP to discover the location.

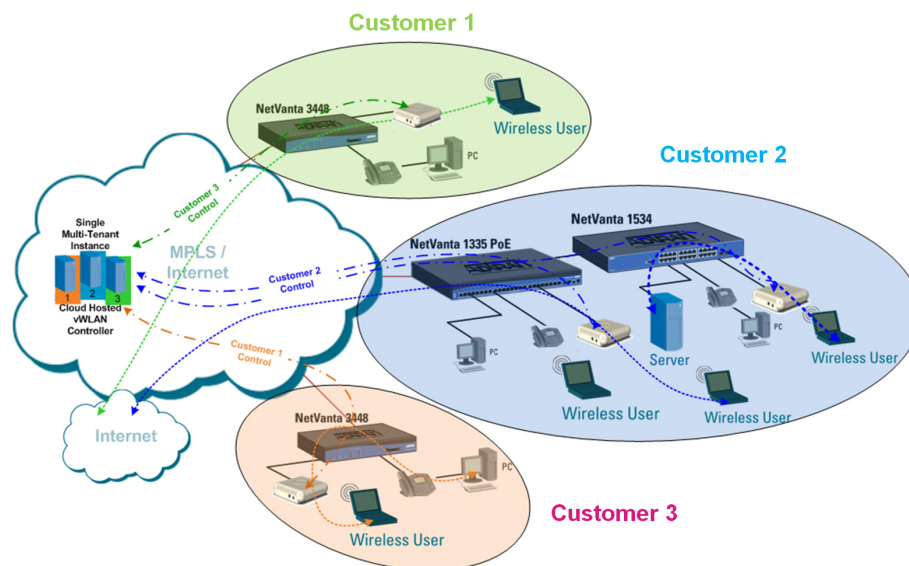
A user's location is determined by the assigned user role. The AP's native location is automatically discovered, and the vWLAN system automatically determines the APs that support those locations. In a large scale deployment, multiple subnets can be assigned to the same user role, and the system optimally assigns the user to a local location, eliminating the need to trunk the same VLANs across multiple sites.

## Multi-tenant Support

Multi-tenant vWLAN is a streamlined software solution that manages, configures, controls, and secures Wi-Fi APs, radio frequency (RF) spectrum, and users across separate customers or management domains. It can be deployed in the public or private cloud on both physical and virtual machines (hardware or VMware). Multiple customers, or tenants, use the same vWLAN software with individual APs, placing management of multiple domains under a single hardware or virtual appliance. The multi-tenant configuration allows multiple tenants to share resources and build efficient, highly scalable network infrastructures.



A multi-tenant vWLAN system is similar to multiple single-tenant vWLAN systems. Each of the systems is logically separate from the others for configuration, management, security, and control purposes. Therefore, whenever an AP must be logically separated from another AP, it can be configured in a different tenant. For example, if 50 different small food chain restaurants have the same vWLAN configuration in each, and all are owned and managed by the same owner, all the vWLAN systems can be configured in a single domain. However, if there are 50 different stores in a mall, with different vWLAN configurations and different owners, multiple domains are needed for vWLAN configuration. Lastly, if there is a large campus with several different colleges or schools, for example, a separate domain for each entity is needed in the vWLAN configuration. Multi-tenancy allows vWLAN to be configured so that, from an RF perspective, the adjacent APs will interact properly and not conflict with each other, even when configured in different domains, and each domain has its own management database, authentication, and control. Figure 1 illustrates a typical multi-tenant vWLAN topology.



**Figure 1. Multi-tenant Network Topology**

## WPA2-Multikey Support

Wi-Fi protected access version 2 (WPA2) with multikey support is a new security feature for the vWLAN 3.5.0 release. This feature provides the benefits of WPA2 level security for connected devices, while also providing additional security for each client by using a per-user preshared key, based on their device's MAC address. When configured, this feature provides a method for users to determine their own passwords for their connected devices, rather than using a generic password shared by all users connected to a single SSID. For example, in a typical wireless environment, whether business building, apartment complex, hotel, or university, a single Wi-Fi password is assigned to all users of a single SSID. Because this single password is used by all parties connecting to the network, it becomes very easy to compromise the security of the connections. With the introduction of WPA2-Multikey functionality, multiple users can connect to a single SSID, and use a preshared key unique to each user, for network connections. In this manner, devices used by people in different apartments, businesses, or rooms, are connected to the wireless network using a password unique to the device and user, rather than a single shared password for the entire apartment complex or business.

## vWLAN Solutions

vWLAN can be used by service providers, as well as enterprise and small to medium sized businesses. The following illustrations depict the use and deployment of vWLAN in these different hosted environments.

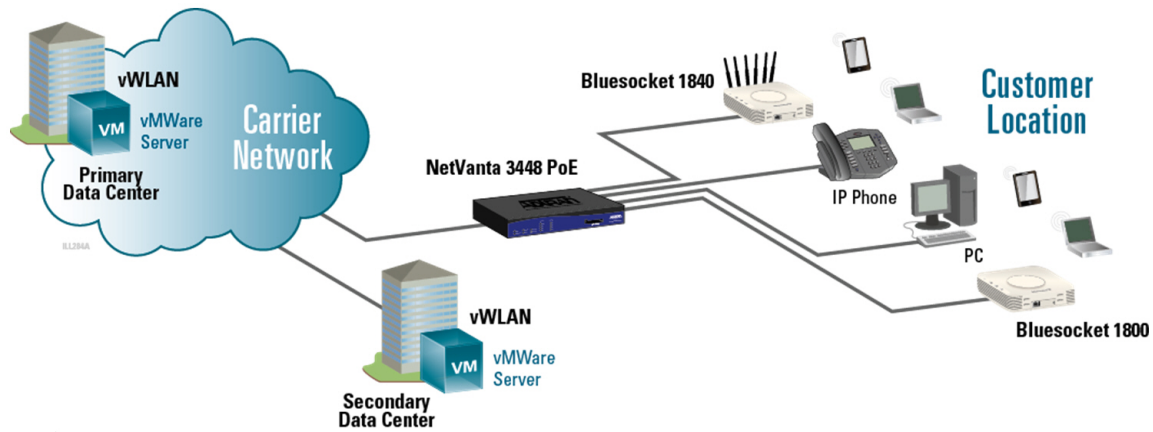


Figure 2. Carrier Hosted Solution

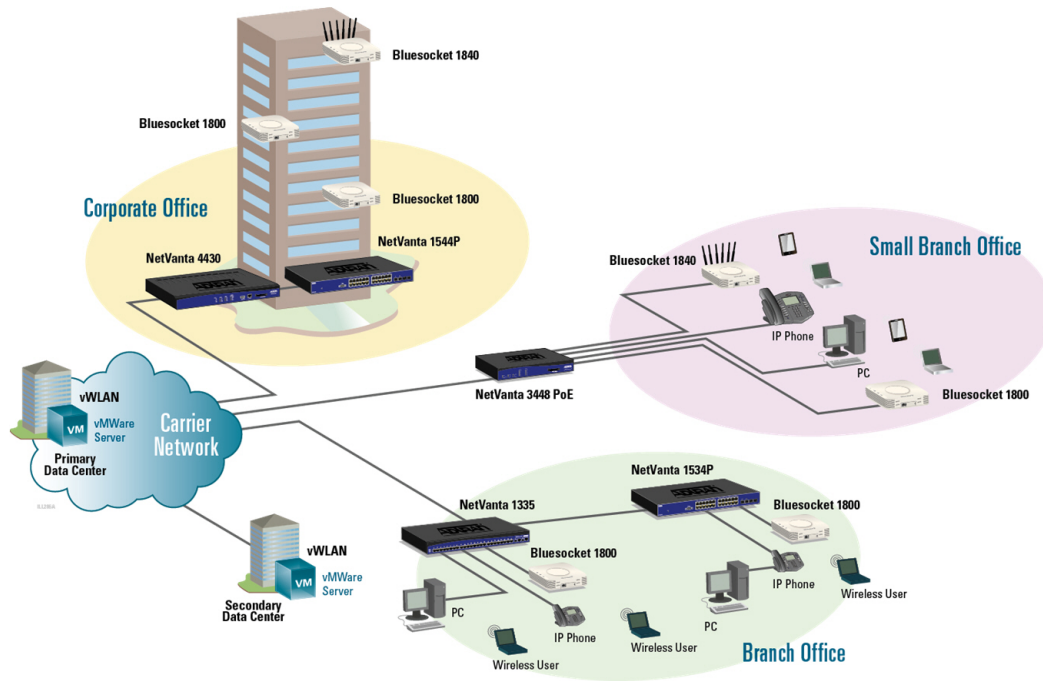


Figure 3. Enterprise Hosted and Managed Solution

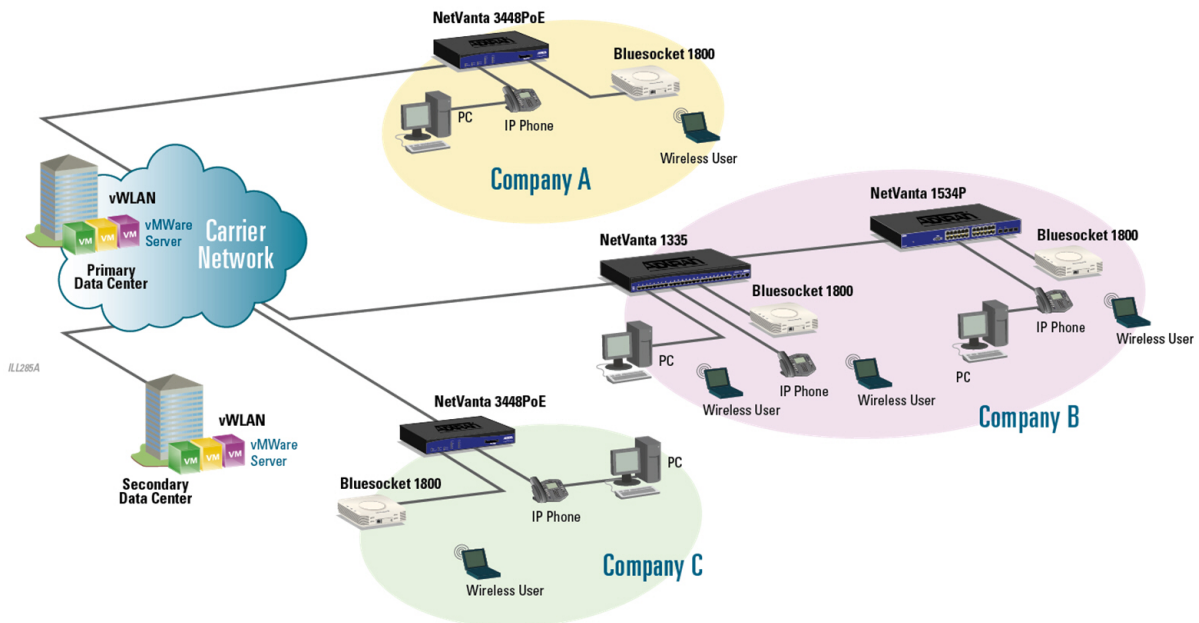


Figure 4. Small to Medium Business Hosted and Managed Solution

## 2. vWLAN Hardware and Software Requirements

The following sections outline the required hardware and software, and other information related to the ADTRAN Bluesocket vWLAN:

- [Required Hardware on page 20](#)
- [Resource Requirements on page 20](#)
- [Software Requirements on page 26](#)
- [Client Device Support on page 33](#)
- [Browser Support on page 34](#)
- [VMware Support on page 34](#)

### Required Hardware

vWLAN operates on a hardware appliance that runs vWLAN natively, or a virtual appliance running VMware vSphere ESX/ESXi Hypervisor. In addition, vWLAN must have an AP to operate.

### Resource Requirements

Regardless of the AP deployment size, the vWLAN virtual appliance requires the following resources:

- 40 GB of thick provisioned disk space for the virtual hard disk (.vmdk)
- One Ethernet network interface card for network connectivity (vmxnet)
- Four CPUs or cores and 8 GB RAM for any of the following:
  - up to 750 APs
  - up to 12500 clients
  - up to 25 domains
- Four CPUs or cores and 16 GB RAM for any of the following on systems running 3.3.0 or later:
  - over 750 APs
  - over 12500 clients
  - over 25 domains

#### 3.6.0 Release Resource Requirements

With the vWLAN 3.6.0 release, support for hosting up to 150 domains, 2048 APs, and 32,000 clients was introduced. The following are the hardware resource requirements for the 3.6.0 release:

- 8 GB RAM, 40 GB HDD, and four CPUs or cores for hosting any of the following:
  - up to 50 domains
  - up to 1400 APs
  - up to 22,000 clients
- 16 GB RAM, 128 GB HDD, and four CPUs or cores for hosting any of the following:
  - up to 150 domains
  - up to 2048 APs
  - up to 32,000 clients

**NOTE**

*When upgrading from a previous vWLAN release (for example, 3.5.0) to the 3.6.0 release, vWLAN will only support 50 domains, 1400 APs, and 22,000 clients. To deploy vWLAN 3.6.0 with 150 domains on a single vWLAN instance, you must deploy a new VM with the 3.6.0 OVA. Refer to the vWLAN 3.6.0 release notes for specific upgrade instructions (available online at <https://supportcommunity.adtran.com>).*

## External Resource Requirements

**DNS:** vWLAN should be placed on a network with DNS access and IP connectivity to the APs. When using a third-party SSL certificate (provided by a certificate authority for web-based authentication like captive portal), you must enable the **Redirect to hostname** option. The **Redirect to hostname** option requires both a forward (A record) and a reverse pointer (PTR record) in your organization's DNS server for the public network interface and the fully qualified domain name (FQDN) of the vWLAN. vWLAN and APs query the PTR record and redirect traffic based on the response. If there is no PTR record, clients are redirected to an IP address (rather than a host name). This action can result in the receipt of a web browser security warning indicating a domain name mismatch. Clients use the A record to resolve the host name of vWLAN to an IP address.

**DHCP:** vWLAN can be configured to use DHCP to obtain an IP address or a static IP address. By default, the public network interface (**Network** port) is configured as a DHCP client. DHCP is not supported on the private network interface (**MGMT** port) of the vWLAN hardware appliance. If you are using DHCP, vWLAN obtains an IP address from the network. If you disable DHCP, you can use the configured IP address, subnet mask, DNS, and host name settings. The default IP address, subnet mask, and gateway of the public network interface is 192.168.130.1, 255.255.255.0, and 192.168.130.254 respectively. If DHCP is enabled, as it is by default, vWLAN continues to try and obtain an IP address using DHCP, unless the gateway responds to Internet Control Message Protocol (ICMP), in which case it falls back to those settings. If you want to connect a computer directly to the public network interface of the hardware appliance for initial configuration, the computer must be configured for the default gateway IP address (192.168.130.254), and it must respond to ICMP in order for vWLAN to fall back to those settings. It is recommended that you connect to the private network interface port instead of the public network interface when initially configuring the hardware appliance. Alternatively, you can disable DHCP and configure the AP IP address using the VMware vSphere console.

## ADTRAN Bluesocket APs

vWLAN 3.2.0 and higher is compatible with the following models:

- BSAP 1920/1925
- BSAP 1930/1935
- BSAP 1940
- BSAP 2020
- BSAP 2030/2035
- BSAP 2135
- BSAP 3040/3045

**NOTE**

*The BSAP 18XX series has been discontinued and is not supported on version 3.2.0. If you are still using BSAP 18XX series devices, you must use version 3.1.0 or lower*

**NOTE**

*Some older AP models may not support all features in a release or past releases. For information on what your AP model supports, please consult the [AP Feature Matrix](http://support.adtran.com) located at <http://support.adtran.com>*

Each AP series has its own firmware. For example, the BSAP 1900 Series APs use their own firmware that is different from that of the 2000 or 3000 series firmware. There is one version of AP firmware for the BSAP 1920 Series, and a separate version of AP firmware that is shared by the 1930/1940 Series. Firmware selections are applied to the AP template, and then the template is applied to the AP (refer to [Configuring AP Templates on page 149](#)).

The supported Bluesocket APs are discussed in the following sections. All BSAPs support up to 8 SSIDs per radio.

## 1800 Series APs

**NOTE**

*The BSAP 18XX series has been discontinued and is not supported in version 3.2.0. If you are still using BSAP 18XX series devices, you must use version 3.1.0 or lower*

The 1800v1 and 1800v2 APs are 802.11a/b/g/n wireless APs with internal antenna arrays designed for ceiling mounting. These APs have dual radios of 2.4 GHz and 5 GHz, one auto-sensing 10/100/1000Base-T Gigabit Ethernet port, and include 802.3af compliant Power over Ethernet (PoE) support. The 1800v2 AP is plenum rated, while the 1800v1 is not.

The 1840 AP is an 802.11a/b/g/n wireless AP with the same coverage and throughput criteria as the 1800v2, however, it supports external antenna connections for more flexible deployment options, such as wall mounting. This AP has dual radios of 2.4 GHz and 5 GHz, six reverse polarity subminiature version A (RP-SMA) connections for external antennas, one auto-sensing 10/100/1000Base-T Gigabit Ethernet port, and includes 802.3af compliant PoE support.

**NOTE**

*There are no internal antennas on the 1840 AP. This model only supports externally connected antennas.*

On the transmit side, the AP transmits two spatial streams. One on antenna one and the other on antenna three for each band. Antenna two is for signal integrity; a diversity antenna in legacy terminology. On the receive side, all three antennas are used for one or two spatial streams from an 802.11n client and one spatial stream from a legacy client.:

**NOTE**

*To decode  $N$  spatial streams, the receiver needs  $M \geq N$  antennas. When  $M=N$ , antenna should be separated by 6 to 12 cm (1/4 to 1/2 wavelength) for 2.4 GHz and 3 to 6 cm for 5 GHz wavelengths on BOTH the transmitter and receiver to ensure orthogonal cross stream path. In this case, orthogonality is achieved by the distance between antennas. Additional spatial streams can be achieved if there is more orthogonal dimension available (such as field polarization of the antenna's E field). You need BOTH the transmitter and receiver's antenna properly aligned to achieve the orthogonal limit. Hence, this form of orthogonality is not used in Wi-Fi, however, it can be used in point-to-point static communication links.*

The BSAP 1800 Series do not support the following features:

- DFS functionality
- Mesh Networking
- Secure Copy Protocol (SCP)-based upgrades
- 802.11ac

## 1900 Series APs

The 1920, 1925, 1930, 1935, and 1940 Series high-performance APs are 802.11a/b/g/n/ wireless access points supporting MIMO antenna technology. These APs are dual band, supporting 2.4 GHz and 5 GHz, one auto-sensing 10/100/1000Base-T Gigabit Ethernet port, and include 802.3af compliant Power over Ethernet (PoE) support. The BSAP 1920/1925 and 1930/1935 are plenum rated while the BSAP 1940 is housed in an outdoor weather proof, salt spray resistant (IP67) enclosure with built-in carrier class antenna and Ethernet surge protection (GR-1089/6kV).

The BSAP 1900 Series operate using an associated template, two radios, 802.11n wireless standard, and can support up to 8 SSIDs per radio. In addition, the BSAP 1900 Series include smart and secure AP upgrade features. Included are AP pre-imaging, which allows the AP to download firmware while the unit is in operation (reducing downtime during software maintenance or upgrades), secure AP upgrades, which allow APs to download firmware from vWLAN or a local server using Secure Copy Protocol (SCP) (rather than unsecured and problematic Trivial File Transfer Protocol (TFTP)), and optional local secure AP upgrades, which allow APs to download firmware from a local SCP server (rather than using WAN bandwidth). [Table 1](#) outlines the BSAP 1900 Series by AP and radio type.

**Table 1. BSAP 1900 Series**

AP	Internal Antenna	External Antenna
2x2:2 1920 Series AP	BSAP 1920	BSAP 1925
3x3:3 Stream 1930 Series AP	BSAP 1930	BSAP 1935
3x3:3 Outdoor 1940 Series AP		BSAP 1940

**NOTE**

*The 1900 Series APs do not support the following:*

- Dual Mode. Instead, a BSAP 1900 Series AP configured for dual mode acts as if it is in AP mode.

For more information about the BSAP 1900 Series, refer to the quick start guide associated with the particular AP. These quick start guides are available online at <http://supportforums.adtran.com>.

**2000 Series APs**

The 2000 Series 802.11ac enterprise performance APs have much of the same functionality as the BSAP 1900 Series, and also operate using an associated template, dual band, and similar coverage and heat map patterns as the BSAP 1900 Series APs. The BSAP 2000 Series support the 802.11ac wireless standard but are backwards compatible with the 802.11n standard. They can support up to 8 SSIDs per radio and include the same smart and secure AP features as the BSAP 1900 Series APs.

The cost effective BSAP 2020 provides 4 internal MIMO antennas with 6 dBi gain on 5 GHz and 3 dBi gain on 2.4 GHz. The BSAP 2030 provides one integrated, six element high-efficiency Planar Inverted F Antenna (PIFA) array with 5.5 dBi gain (no external antennas are required). The BSAP 2035 provides six reverse-polarity subminiature version A (RP-SMA) antenna connectors; no integrated antennas are included with this model. Three antenna connectors support 2.4 GHz and three support 5 GHz communications. These antennas and connectors support two internal 802.11 radios: one 2.4 GHz 802.11b/g/n radio and one 5 GHz 802.11a/n/ac radio. The BSAP 2135 is housed in a weather resistant, industrial-grade enclosure with a built-in carrier class antenna and Ethernet surge protection.

[Table 2](#) outlines the BSAP 2000 Series by AP and radio type.

**Table 2. BSAP 2000 Series**

AP	Internal Antenna	External Antenna
2x2:2 Stream 2020 Series AP	BSAP 2020	
3x3:3 Stream 2030 Series AP	BSAP 2030	BSAP 2035
3x3:3 Outdoor 2135 Series AP		BSAP 2135



**NOTE**

*The 2000 Series APs do not support the following:*

- *Over-the-air Fairness. Instead, on a BSAP 2000 Series AP, any value is treated as no bias.*
- *Dual Mode. Instead, a BSAP 2000 Series AP configured for dual mode acts as if it is in AP mode.*

For more information about the BSAP 2000 Series, refer to the quick start guide and data sheet associated with the particular AP. These documents are available online at <http://supportforums.adtran.com> and [www.adtran.com](http://www.adtran.com).

**3040/3045 Series APs**

The BSAP 3040 and 3045 APs have much of the same functionality as the BSAP 1900 and 2000 Series APs, including support for up to 8 SSIDs per radio and the same smart and secure AP features. However, the BSAP 3000 Series offer carrier grade performance and supports the 802.11ac wave 2 wireless standard, while remaining backwards compatible with 802.11ac and 802.11n standards. The BSAP 3000 Series operates four radios: concurrent 2.4 and 5 GHz radios, and a dedicated dual band scanning/security radio.

The BSAP 3040 AP includes a total of 10 internal modular high efficiency PIFA omnidirectional antennas - four internal antennas with 6 dBi peak gain for the 5 GHz radio, four internal antennas with 4 dBi peak gain for the 2.4 GHz radio, one internal antenna with 3/5 dBi peak gain for the dual band scanning/security radio (2.4 GHz respectively) and one internal antenna with 4 dBi peak gain for the BLE radio. The BSAP 3045 AP includes a total of 8 RP-SMA connectors for external antennas and two internal modular high efficiency PIFA omnidirectional antennas - four RP-SMA connectors for external antennas for the 5 GHz radio, four RP-SMA connectors for external antennas for the 2.4 GHz radio, and one internal antenna with 3 dBi peak gain for the dual band scanning/security radio (2.45 GHz respectively).

AP	Internal Antenna	External Antenna
4x4:4 Stream 3000 Series AP	BSAP 3040	BSAP 3045

**NOTE**

*The 3000 Series APs do not support the following:*

- *Dual Mode. Instead, the BSAP 3000 series APs have a third radio for scanning, which means that they almost always operate in dual mode.*

For more information about the BSAP 3040 and 3045 Series APs, refer to the quick start guide and data sheet associated with the particular AP. These documents are available online at <http://supportforums.adtran.com> and [www.adtran.com](http://www.adtran.com).

## Software Requirements

The vWLAN appliance is designed to be installed anywhere, even behind NAT devices (refer to [vWLAN Implementation on Public and Private Networks on page 280](#)). It does not need access to any of the data VLANs. The appliance does not support VLANs, and has only a single IP address in VMware applications. The vWLAN hardware appliance has a second management-only port and IP address so the device can be reached without a serial cable. The APs can be configured on access or trunk ports. The APs must be able to communicate with the vWLAN appliance, therefore, the following traffic must be allowed between APs and the vWLAN appliance:



### NOTE

*In previous versions of vWLAN, APs were required to use Domain Naming Server (DNS) to communicate with vWLAN and determine if the vWLAN was active. In vWLAN release 2.6, this requirement has been removed so that the AP discovery process is not interrupted when APs are not configured for outbound DNS access because of firewall policies. DNS is still required, however, for BSAP 1800 Series upgrades.*

- UDP port 53 (DNS) is used for AP discovery communication between vWLAN and the AP (BSAP 1800 Series only).
- UDP port 69 (TFTP) is used for BSAP 1800 Series AP firmware and AP traffic captures. TFTP stateful firewall helper must be configured on the firewall as well, because the reply source port from vWLAN is not 69.
- Transmission Control Protocol (TCP) port 33334 is used for BSAP 1900 Series AP firmware and traffic captures.
- TCP port 33333 (control channel) is used for vWLAN communication configuration information, status polling, and control traffic to and from the AP.
- TCP port 28000 (RF channel) is used to send secure RF information from the AP to vWLAN.
- IP Protocol 97 (Ethernet IP) is used to send client data from AP to AP. This is not required for communication between the APs and vWLAN, but it is required between APs for Layer 3 mobility.
- TCP port 443 (Hypertext Transfer Protocol Secure (HTTPS)) is used if web-based authentication is enabled.
- TCP port 2335 (SCP) and port 3000 is used for vWLAN to vWLAN communication and secure firmware uploads.
- UDP port 1812 (Remote Authentication Dial-In User Service (RADIUS)) is used for RADIUS external 802.1X authentication between the AP and a third-party RADIUS server.

ADTRAN Bluesocket 1800, 1900, and 2000 Series APs are certified with the Wi-Fi Alliance. Any smart phones used with vWLAN should have Wi-Fi radio and the ability to support 802.1X.

vWLAN supports redirection of HTTP and HTTPS traffic for webpage authentication. HTTPS redirection is optional and must be enabled on the vWLAN, but should only be enabled when needed due to resource consumption.

## SNMP

As of vWLAN firmware release 2.5, Simple Network Management Protocol (SNMP) enhancements are included in vWLAN functionality. Now included in SNMP reports are AP-specific status information at the vWLAN platform level, vWLAN platform and system-specific information, and an SNMP MIB that reports SSID, user, MAC address, and online status of tiered and rogue APs on a single domain.

## Licenses

vWLAN is centralized management and control software that runs on an appliance (hardware) or virtual appliance (VMware) and scales by adding AP licenses, not more hardware. Each AP license is tied to the AP serial number, and no vWLAN appliance or VMware licenses are necessary. Optional features (such as unified access licenses) are licensed per AP.

When high availability is configured, all licenses are automatically transferred to the secondary vWLAN appliance.

If an AP is configured without a unified access license, the AP will not support wired users or third-party APs, and will not discover untrusted VLANs.

As of vWLAN firmware release 2.4.0, there are no high availability licenses. Instead, the high availability feature is included with the base vWLAN license. When you upgrade to the 2.4.0 firmware all APs will instantly have the high availability feature.

In the event of an AP failure, a return merchandise authorization (RMA) is processed, and typically, a new license is emailed to you. If you do not receive a new license on an RMA generated by ADTRAN, contact ADTRAN Customer Care at 888-423-8726 and reference the RMA number.

## IPv6 and vWLAN

Internet Protocol version 6 (IPv6) is not supported by the vWLAN appliance or VMware, although clients connecting to vWLAN can use IPv6 addresses. IPv6 clients in vWLAN are limited to medium access control (MAC) authentication using the default SSID role or 802.1X authentication, because IPv6 addresses cannot be web-authenticated at the vWLAN captive portal. IPv6 clients are supported in vWLAN by bridging the IPv6 traffic at the AP onto the proper VLAN.

## Layer 3 Mobility

As of vWLAN firmware release 2.9, Layer 3 mobility (tunneling) is automatic in vWLAN if the AP does not support a location (VLAN and subnet mask), or if the location is out of the user's role's location group. When Layer 3 mobility is active, traffic is tunneled to an AP that does support the location. The tunneling behavior is automatic if traffic can be routed between the APs on native AP VLANs, if EtherIP (protocol 97) is not blocked by any firewalls between the APs, and if the AP is not behind NAT. Configuring vWLAN for Layer 3 mobility requires verifying that traffic can be routed between APs, that EtherIP is not being dropped in any firewalls between APs, and that APs are not behind NAT.

## GRE Tunneling

Soft Generic Routing Encapsulation (GRE) tunneling can be enabled for both the AP and the SSID on BSAP 19xx and 20xx systems running firmware release 2.9 or later. When GRE tunneling is enabled, traffic to and from clients associated with a tunnel-enabled SSID is tunneled between the AP and the Wireless Aggregation Gateway (WAG) server defined in the tunnel profile associated with the AP template. Only one GRE tunnel can be enabled per AP. When enabled, the GRE tunneling behavior is automatic as long as the GRE external IP is not blocked by any firewall (IP protocol **47** and port **1723** should be allowed) and the primary or secondary WAG server is not down.

## Mesh Networking

Mesh networking is available on vWLAN BSAP 19xx systems running firmware release 2.5 or later and BSAP 2xxx systems running firmware release 3.1.0 or later. For more information about configuring vWLAN mesh networking, refer to the configuration guide *Mesh Networking in vWLAN*, available online at <https://supportcommunity.adtran.com>.

## Layer 7 Device Fingerprinting Support

Layer 7 Device Fingerprinting support is available on vWLAN systems running firmware release 2.6 or later. This feature allows network administrators to assign client roles based on detected connecting device types, operating systems, and vendors. Layer 7 Device Fingerprinting is supported on all BSAP models. For more information about configuring the vWLAN Layer 7 Device Fingerprinting feature, refer to the configuration guide *Layer 7 Device Fingerprinting in vWLAN*, available online at <https://supportcommunity.adtran.com>.

## DFS Support

Dynamic Frequency Selection (DFS) is supported on vWLAN systems running firmware release 2.6 or later. This feature provides the ability to use additional 5 GHz channels that are also used by radar systems. In order to use these channels, the AP scans the channel for the presence of radar before and during usage. If radar is detected on the channel, the AP moves off of the channel. DFS is required for European 5 GHz outdoor deployments. Without DFS, European 5 GHz indoor channels are limited to four channels. Employing DFS allows more channel selection, which results in more user capacity and less interference. For more information about DFS configuration in vWLAN, refer to the configuration guide *DFS in vWLAN*, available online at <https://supportcommunity.adtran.com>.

The following DFS channels for European countries are supported in vWLAN 2.6:

- 52, 56 (40 MHz pair)
- 60, 64 (40 MHz pair)
- 100, 104 (40 MHz pair)
- 108, 112 (40 MHz pair)
- 132, 136 (40 MHz pair)
- 116, 140 (20 MHz only channels)
- 80 MHz channel groups include 52, 56, 60, 64 and 100, 104, 108, 112

For firmware release 2.6, DFS is supported natively on the BSAP 1925, 1935, and 1940 Series. The BSAP 1920 and 1930 Series products will support DFS if they are using hardware revision K. As of firmware release 3.1, DFS is supported on the BSAP 2020 in Europe. Any BSAP unit that supports DFS is shipped with a “DFS Capable” sticker on the box and on the AP.

## Setup Wizard Support

In vWLAN firmware release 2.6, a vWLAN setup wizard is available. This wizard streamlines the wireless network configuration process for first time users. It provides a step-by-step system for configuring the first SSID and domain. For more information about using the setup wizard, refer to [vWLAN Setup Wizard on page 175](#).

## WPA2-Multikey Support

In vWLAN firmware release 3.5.0, support for WPA2-Multikey feature, where per-user preshared keys are used for client connections, is provided. When employed, the WPA2-Multikey feature makes use of a RADIUS server for client device authentication, and uses RADIUS attributes to provide secure connection information for each device. As part of the new feature, when using WPA2-Multikey, the AP performs the RADIUS MAC authentication, rather than vWLAN itself. When devices have completed the registration process, roles, locations, and VLAN settings are determined by the AP, based on the Tunnel-Password and Tunnel-Private-Group-ID attributes contained in the RADIUS ACCEPT messages. These attributes are used to provide the pairwise master key (PMK) and appropriate VLAN information for the authenticating client. Once the client has been authenticated, the AP tags all wireless traffic from the device with the VLAN number assigned by the RADIUS server in the Tunnel-Private-Group-ID attribute of the ACCEPT message.

WPA2-Multikey use supports the RADIUS attributes for RADIUS REQUEST and RADIUS ACCEPT packets outlined in [Table 3](#):

**Table 3. WPA2-Multikey Supported RADIUS Attributes**

RADIUS Packet Type	Attribute Value	Description
Request	1	User Name
Request	2	User Password
Request	31	Calling Station ID (wireless device MAC address)
Request	30	Called Station ID (AP MAC address plus SSID)
Request	4	NAS IP Address
Request	61	NAS Port Type (wireless)
Accept	69	Tunnel-Password (PMK)
Accept	81	Tunnel-Private-Group-ID (VLAN ID)

In addition, when the WPA2-Multikey feature is used, the AP tags VLAN frames without performing location discovery, removing the need to add all available locations manually to vWLAN. These locations are populated by the AP when it receives new VLAN information from the RADIUS server and are communicated to vWLAN as an Active or Inactive location. Therefore, client status location information is displayed as a VLAN value (for example, VLAN-325), and location status information includes the CIDR, VLAN ID, and AP.

When employed, the WPA2-Multikey feature allows each AP to cycle through up to **15** PMK keys when authenticating clients.

The WPA2-Multikey feature is supported natively on the BSAP 2020, 203x, 2135, and 304x Series. This feature is not supported on the BSAP 1900 Series.

For more information about the WPA2-Multikey feature, refer to the configuration guide [WPA2-Multikey and Rolling-PMK in vWLAN](#), available online at <https://supportcommunity.adtran.com>.

## Enhanced WPA2-Multikey Support

In vWLAN firmware release 3.7.0, enhancements to the WPA2-Multikey feature were introduced. These enhancements allow an external authentication server to compute PMKs, so that up to 1000 PMKs can be generated and validated externally and sent to connecting clients based on their MAC address.

Configuration of the enhanced WPA2-Multikey support simply relies on specifying that PMKs are generated at the external gateway, using a check box in the **Authentication Server** configuration menu (refer to [Configuring the WPA2-Multikey Feature in vWLAN on page 242](#) for more information).

Enhanced WPA2-Multikey support is not compatible with standard FreeRADIUS servers, and will only function if the external server is capable of extracting the necessary PMK generation information and returning a final PMK in an access-accept packet sent to the APs to which clients are connecting. Information required to generate the PMKs includes:

- A Nonce information: a random number generated at the AP
- S Nonce: information: a random number generated at the wireless client
- MIC: a message integrity check sent by the wireless client

Enhanced WPA2-Multikey is supported natively on the BSAP 202, 203x, 2135, and 304x Series products. It is not supported on the BSAP 1900 Series products.

## Link Layer Discovery Protocol (LLDP) Support

In vWLAN firmware release 3.7.0, LLDP support is introduced. LLDP is a standard Layer 2 protocol, 802.1AB, that is used to identify neighboring devices and determine their broadcast capabilities. With the introduction of LLDP support, AP discovery can be performed by LLDP without any additional vWLAN or AP configuration. By default, LLDP support is included on all BSAP 1930, 2030, and 3040 Series products.



### NOTE

*LLDP is not supported on BSAP 1920 or 2020 Series products.*

LLDP support in BSAP devices includes the transmission of LLDP information only; LLDP information from other devices is not received or stored on the BSAP.

The following list includes specific functionality and configuration parameters for LLDP support in vWLAN networks:

- LLDP support is enabled by default on all 2000 and 3040/3050 Series APs. There are no configurable parameters required to enable or disable LLDP support.
- APs only support the transmission of LLDP information. LLDP data is not received or stored on the AP.
  - The destination MAC address for LLDP information sent by the AP is always the multicast address **01:80:C2:00:00:0E**.
  - LLDP updates are sent automatically every **30** seconds.

*Figure 4* describes the Type, Length, Values (TLVs) that APs include with LLDP transmissions:

**Table 4. TLVs Included in LLDP Transmissions from AP**

Type	Value
Chassis ID	AP's MAC Address
Port ID	LAN-1
System Name	Serial Name
System Description	AP Name
Management Address	AP's IP Address
Capability enabled	Access Point

### Override Location with TPGI Support

As of vWLAN firmware release 3.5.0, when configuring the **Default** user role, you can optionally choose to override the location assigned to clients in this role by choosing to override their location with a Tunnel-Private-Group-ID (TPGI) value. When this option is enabled, and a TPGI with a value between **1** to **4095** exists, then clients connected in the **Default** role are assigned a location based on a VLAN ID assigned by the RADIUS server, and not the location associated with the role. Using the location override feature allows you to assign multiple locations quickly, without waiting for vWLAN to completely execute location discovery.

### VLAN Support

As of vWLAN firmware release 3.5.0, up to **4094** individual VLANs are supported on a vWLAN instance.

## Probe Request Database Support

In vWLAN firmware release 3.7.0, support for a probe request database stored on vWLAN was introduced. With this new feature, each AP supplies vWLAN with probe request data for connected clients that is stored in a database on vWLAN and can be accessed easily with an API call. This information can then be used to analyze connected client data, crowd movement, and client location trends.



### NOTE

*Probe requests are only supported in the BSAP 2000 Series products.*

When using this feature, probe request data is sent from the AP every **60** seconds, and the stored information provides location information for clients currently connected to vWLAN, as well as those connected within the last seven days.

The only configuration necessary to use this feature is to ensure that heat maps are enabled and that **Scan for Adjacent Wireless Clients** is enabled in the AP's template (refer to [Using Heat Maps on page 244](#) and [Configuring AP Templates on page 149](#) for more information). Unless these features are enabled, the probe request information is not stored on vWLAN.

Specific location information provided in the probe request frames that populate the database include:

- The X and Y coordinates of clients connected to each AP. These coordinates are based on heat map reporting within the AP; heat maps must be enabled on the AP to capture the X and Y coordinates of connected clients.
- Device status information for both currently connected and previously connected devices. Currently connected devices include the **connected\_to\_adtran\_ap** value and previously connected devices include the **scanned\_by\_adtran\_ap** value in their probe request frames.
- Database entry creation and update information, based on First Seen and Last Seen probe request data. This information provides a method for understanding which entries in the database are new, are expired, or are current.

The following client parameters are all included and stored in the vWLAN database:

- AP MAC address
- Wireless client MAC address
- RSSI (dBm)
- Channel number
- First Seen time stamp
- Last Seen time stamp
- XY coordinates

APIs are used to access this information from vWLAN. For more information about using APIs with vWLAN, refer to the configuration guide [Using APIs with vWLAN](#), available online at <https://supportcommunity.adtran.com>.



By default, no more than one million entries are stored in the Probe Request database and entries are cleared every **7** days. The vWLAN GUI can be used to specify a different storage time for Probe Request database entries. To change the default entry clearing schedule, connect to the vWLAN GUI and follow these steps:

1. Navigate to the **Configuration** tab, and select **System > Settings**. Select the **Domain** tab.
2. In the **Domain Settings** menu, select **Flush Client Scan Data Interval** from the list.
3. In the **Flush Client Scan Data Interval** menu, enter the number of days that entries should be stored before they are cleared in the appropriate field. Valid range is **0** to **30** days.
4. Select **Update Domain Settings** to apply the changes.

## Client Device Support

vWLAN is a standards compliant, software-based solution that functions with any client without the need for client-side software. The following devices are among (but not limited to) those supported by ADTRAN Bluesocket vWLAN:

- Windows NT, ME, Mobile, 2000, 2003, XP, Vista, Windows 7, Windows 8
- Macintosh OS8, OS9, OSX (PowerPC and Intel)
- iPhone, iPod, iPad
- All Linux products including RPM Packet Manager (RPM)-based Linux distributions and Debian Linux distributions
- Blackberry, Symbian, and PocketPC handheld devices
- Wireless client bridges (such as, AirEther or Engenius)
- Android



### NOTE

*Certain devices must be configured with a file repository that can communicate with vWLAN. If your device does not have a file repository recognized by vWLAN, you may be limited in your vWLAN management abilities from your device and unable to license APs, or upload patches, images, or other files.*

## Browser Support

vWLAN is heavily based on Hypertext Markup Language (HTML) 5, and supports the following browsers. vWLAN administrators are recommended to upgrade to the latest version of the browser for best performance.

- Internet Explorer 9.0 and later
- Mozilla Firefox 3.5 and later
- Google Chrome 4.0 and later
- Safari 3.0 and later
- Opera 10.0 and later
- Android 2 and later
- IOS 4.0 and later

## VMware Support

The ADTRAN Bluesocket vWLAN virtual appliance has been tested and is VMware Ready Certified on ESX/ESXi versions 4.X, 5.X, and 6.X. All standard VMware tools are supported. VMware Player is not supported or recommended for deployment.

### 3. vWLAN Installation

Once you have obtained your ADTRAN Bluesocket vWLAN hardware and software, you must install the vWLAN. The following sections describe the steps necessary for installing your vWLAN, as well as any installation options. These options include installing vWLAN using the ADTRAN Bluesocket vWLAN hardware appliance (which runs vWLAN natively), or installing the ADTRAN Bluesocket vWLAN virtual appliance on VMware vSphere ESX/ESXi Hypervisor.

vWLAN is a robust secure wireless solution, with an abundance of configuration options. Regardless, it is easy to set up a new vWLAN system and connect wireless users in less than an hour. There are two basic steps to installing the vWLAN: installing the vWLAN hardware appliance or vWLAN instance on a virtual machine, and connecting the APs to the vWLAN. The following sections outline vWLAN installation:

- [Step 1: Installing vWLAN on page 35](#)
- [Step 2: Installing the APs Associated with vWLAN on page 37](#)

#### Step 1: Installing vWLAN

You can install the ADTRAN Bluesocket vWLAN on either a hardware appliance supplied by ADTRAN (with vWLAN natively installed), or by using a virtual machine on which vWLAN is installed on a VMware vSphere ESX/ESXi Hypervisor. The following sections describe these installation options.

#### Installing the vWLAN Hardware Appliance

Follow these steps to configure the hardware appliance for vWLAN installation:

1. Place the ADTRAN Bluesocket vWLAN hardware appliance in the location where you will manage it. Insert the power cable into the power port (**Port A**) on the rear panel of the unit.
2. Locate a network with a DHCP server configured.
3. Connect the vWLAN hardware appliance to the network using the **Network** port (public network interface) on the rear panel of the unit. The **Network** port, or public network interface, is used to reach the APs, cloud connectivity where applicable, and vWLAN to vWLAN communication when using high availability. Do not use the port labeled **MGMT** (private network interface). The **MGMT** port, or private network interface, is designed for initial configuration using a computer without connecting to the Serial console or local network connectivity for out-of-band management.
4. Supply power to the hardware appliance by pressing the black **Power** button on the front panel of the unit. The appliance may take up to five minutes to boot, or longer if DNS is not configured.
5. Once the boot is complete, locate the IP address of the hardware appliance from either the DHCP server or from the serial console menu. You can access the serial console menu by connecting a computer to the **Serial/Console** port on the rear panel of the unit. When using the serial connection,

configure your connection to be 9600 baud, 8 data bits, odd parity bits (N), and 1 stop bit (no flow control). When prompted, enter the username **vwlan** and the password **vWI@nBlu3\$ock3t**.

**NOTE**

*In vWLAN firmware release 3.5.0, the default console password was changed from **vwlan** to **vWI@nBlu3\$ock3t**.*

If you are unable to connect using the console connection, and are unable to find the IP address in the DHCP server, connect a computer to the port labeled **MGMT** (private network interface) using a standard Gigabit Ethernet cable. The default IP address of the port is 10.251.252.1, with a network mask of 255.255.255.0. To reach the **MGMT** interface (private network interface), set the static IP address of the computer to something in the same subnet, for example 10.251.252.2, and then directly connect to the port.

**NOTE**

*For more information about serial console menu configuration of the vWLAN, refer to [vWLAN Serial Console Configuration on page 181](#).*

6. Once you have the unit's IP address, you can log in to the web-based graphical user interface (GUI) by entering the unit's IP address in a browser window in the following format: **https://<applianceipaddress>:3000**. The default administrative user name is **root@adtran.com** and the default password is **blueblue**. You should change this user name to match your domain. You will also be prompted (by the **Admin Task** menu) to change the password.
7. You can now begin configuring the APs associated with the vWLAN and other configuration tasks outlined in [vWLAN Administrators on page 43](#).

## Installing the vWLAN Virtual Appliance on VMware

There are two options for installing a vWLAN virtual machine. You can use an Open Virtualization Appliance (OVA) or a .vmdk/.vmx file. OVA installation is recommended because it streamlines installation through a compressed file that contains an Open Virtualization Format (OVF) virtual machine along with support files. You should only use a .vmdk or .vmx file if you need to customize the .vmx file before creating the virtual machine. Refer to the configuration guide [Getting Started with vWLAN on VMware](#) for specific OVA or .vmdk/.vmx installation instructions (available online at <https://supportcommunity.adtran.com>).

Follow these steps to configure the virtual machine for vWLAN installation:

1. Download the virtual machine file from ADTRAN's support site ([www.adtran.com](http://www.adtran.com)) to a location in your network. Obtaining the file requires a [www.adtran.com](http://www.adtran.com) login.
2. Load the virtual machine onto the server or computer of your choosing.
3. Connect the virtual machine to a virtual switch with a DHCP server configured and boot the virtual machine. It may take five minutes or longer to fully boot the machine.

4. Find the IP address of the vWLAN virtual appliance using the vCenter or vSphere client by navigating to **Summary**. If there is no DHCP server, use the VMware console menu to configure a static IP address.
5. Log in to the vWLAN virtual appliance by entering the unit's IP address in a browser window in the following format: **https://<applianceipaddress>:3000**. The default administrative user name is **root@adtran.com** and the default password is **blueblue**. You should change this user name to match your domain. You will also be prompted (by the **Admin Task** menu) to change the password.
6. You can now begin installing the APs associated with the vWLAN and other configuration tasks outlined in [vWLAN Administrators on page 43](#).

## Step 2: Installing the APs Associated with vWLAN

After you have installed the vWLAN appliance (hardware or VMware), you will need to install the APs associated with the vWLAN. To install APs, follow these steps:

1. Plug in an ADTRAN Bluesocket AP and connect it to the network. The APs can be installed anywhere in your network, even behind NAT devices.
2. Allow the AP to discover the vWLAN appliance to receive its configuration information. This process is called AP discovery, which is an algorithm that runs through discovery methods in this order: static configuration, DHCP vendor option 43, and cached vWLAN information. If no response to the discovery request is received, the algorithm moves to the next method in the list (except when using static configuration, which never queries the other discovery methods).

The following tables outline the status, radio, and network LEDs on the BSAP 1800 Series APs, which indicate the initialization status of the AP. To view the LED information for the BSAP 1900 or 2030 Series APs, refer to the quick start guide for the appropriate AP online at <https://supportcommunity.adtran.com>.

**Table 1. BSAP 1800 Series AP Status and Radio LED Definitions**

Status LED	2.4 Ghz LED	5 Ghz LED	Description
Yellow Solid	Off	Off	The unit is powering up.
Green Solid	Off	Off	The unit is initializing software and acquiring an IP address.
Green Flashing	Off	Off	The unit is discovering the vWLAN.
Green Solid	Green Solid/Flashing	Green Solid/Flashing	The radios are activated and passing traffic.
Orange Solid	Off	Off	The unit is upgrading software.

**Table 2. BSAP 1800 Series AP Network LED Definitions**

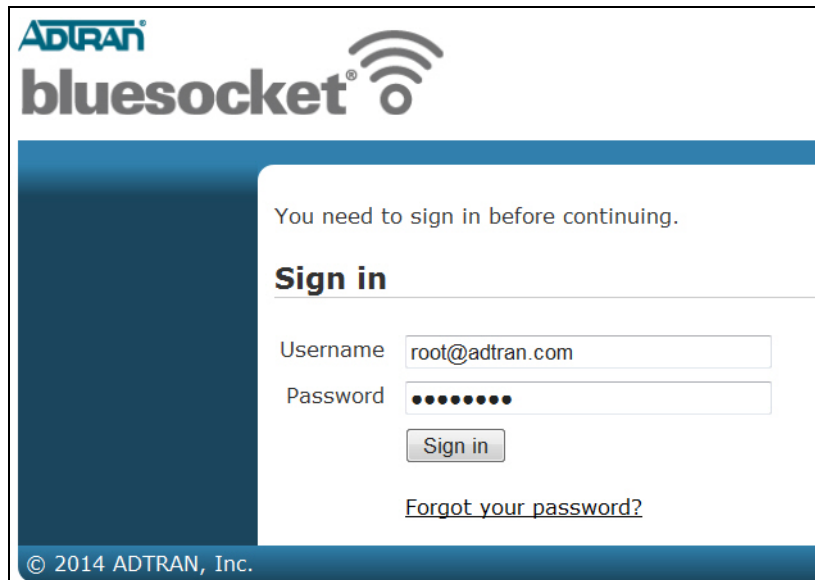
Network LED	Description
Off	No link is detected.
Amber Solid	A 10/100Base-T link is detected with no activity.
Amber Flashing	A 10/100Base-T link is detected with activity.
Green Solid	A 1000Base-T link is detected with no activity.
Green Flashing	A 1000Base-T link is detected with activity.

The network component that can be configured to facilitate AP discovery is an external DHCP server. This server can be configured to assign IP addresses to APs (as well as clients) associated with the vWLAN. When configuring the DHCP server, make sure to configure the Bluesocket DHCP Vendor option (**43**) on the server. For more details about AP discovery, refer to [Using AP Discovery to Connect APs to vWLAN on page 147](#).

3. Once the AP is installed and has been discovered, you can begin configuring the AP and the vWLAN. For more information about AP autodiscovery, refer to the guide [vWLAN Access Point Discovery](#) available online at <https://supportcommunity.adtran.com>.

## 4. Introduction to the vWLAN's GUI

After you have installed the vWLAN and an associated AP, you can begin configuring the vWLAN and AP parameters. Typically these configurations are accomplished using the vWLAN GUI, which is accessed by entering the IP address of the vWLAN instance into a browser window in the format: **https://<vWLANipaddress>:3000**. Enter the email address and password associated with the vWLAN instance at the prompt (default administrative user name is **root@adtran.com** and default password is **blueblue**).

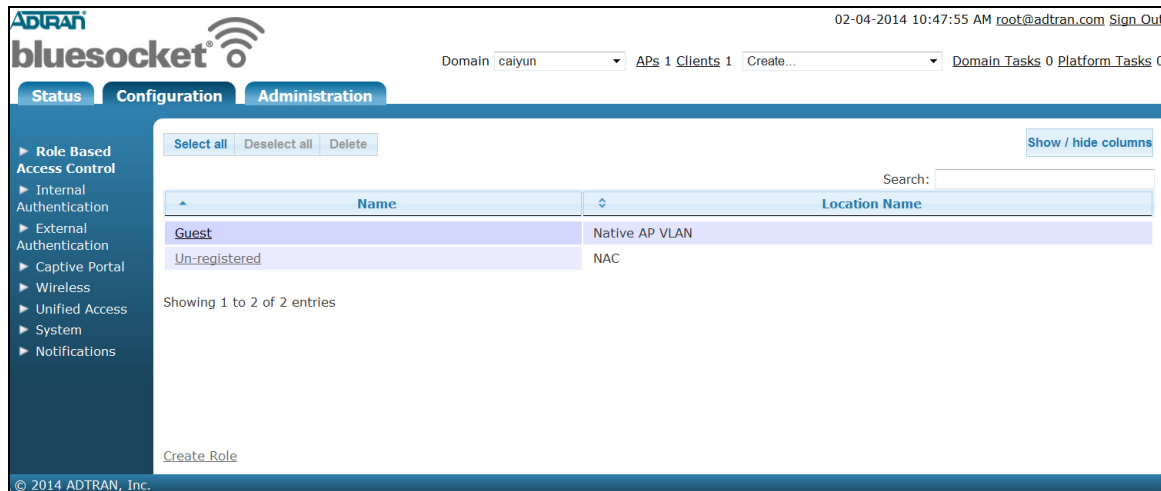


The following sections give you an overview of the vWLAN GUI and its built-in web server used for system management:

- [vWLAN Menu Structure on page 40](#)
- [General GUI Shortcuts on page 41](#)
- [Additional GUI Options on page 41](#)

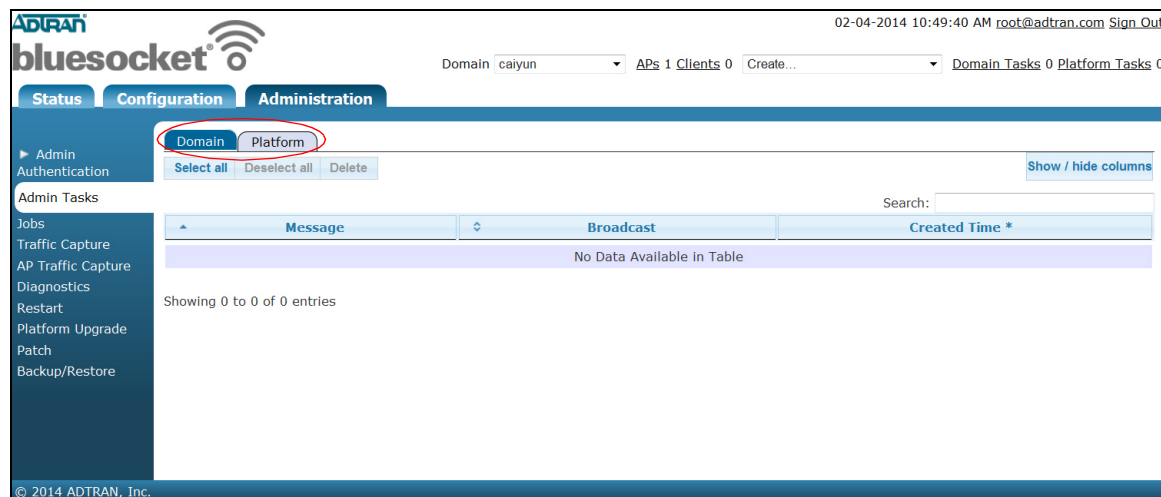
## vWLAN Menu Structure

The vWLAN GUI is structured so that main menu items appear in tabs at the top of the menu, menu items appear on the left of the menu, and shortcuts appear at the top. The main menu consists of three tabs: the **Status** tab, the **Configuration** tab, and the **Administration** tab. The following illustration depicts the vWLAN GUI layout.



Options available in the left menu depend on the tab selected (**Status**, **Configuration**, or **Administration**). The **Status** tab will display information about the status of vWLAN, APs, or vWLAN users. The **Configuration** tab will display menu options that relate to configuring users, APs, wireless settings, wired settings, user authentication, and much more. The **Administration** tab will display menu options that relate to administrator configuration, administration tasks, outstanding jobs, backup, restore, upgrade/patch options, and general vWLAN or AP maintenance.

In addition, there may be a **Platform** or **Domain** tab associated with a menu option, if you are logged in as an administrator who has platform access or configuration privileges. For example, if you navigate to the **Administration** tab, and select **Admin Tasks**, you will see the **Domain** and **Platform** tabs. The **Domain** tab will display administrative tasks related to a domain, and the **Platform** tab will display administrative tasks related to the vWLAN platform only.

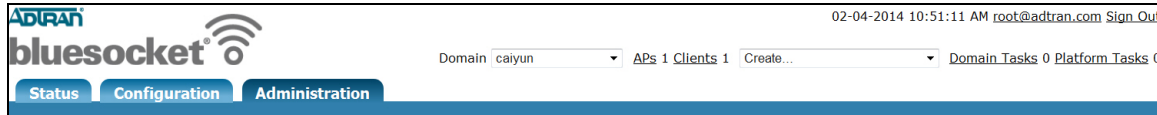


The following sections describe the general shortcuts available in the vWLAN GUI.



## General GUI Shortcuts

The GUI includes shortcuts and other information along the top of the menu.



Shortcuts and other information, and their purposes, are as follows:

- The **Domain** drop-down menu allows you to select the domain in which you would like to perform configuration, management, or monitoring tasks. If you are logged in as root@adtran.com, you can select from any domains you have created. If you are logged in as a domain administrator, you can only choose from the domains that you are allowed to access.
- The **APs** shortcut informs you of how many APs are licensed within the selected domain. Selecting the **APs** link opens the **Access Points** menu located in the **Status** tab.
- The **Clients** shortcut informs you how many users are currently connected to the selected domain. Selecting the **Clients** link opens the **Clients** menu on the **Status** tab.
- The **Create** drop-down menu provides a shortcut for creating most of the items listed in the left menu of the GUI. For example, to create an internal user, you can navigate to the **Configuration** tab, and select **Authentication > Internal > Users**, and then select **Create Internal User**, or you can select **Domain Internal User** from the **Create** drop-down menu. In the **Create** menu you can select from **Domain** menus (menus that pertain to domain configuration), or **Platform** menus (menus that pertain to platform configuration).
- The **Domain Tasks** shortcut informs you how many administration tasks are pending for the domain. Selecting this link opens the **Admin Tasks** menu, in the **Domain** tab of the **Administration** tab.
- The **Platform Tasks** shortcut informs you how many administration tasks are pending for the vWLAN platform. Selecting this link opens the **Admin Tasks** menu, in the **Platform** tab of the **Administration** tab.

## Additional GUI Options

In addition to the GUI shortcuts, you will find that there are several operations that apply to multiple menus. You can view, edit, or delete an item by selecting it from the list in the specific menu. Highlight the item you want to view, edit, or delete, and you will be directed to the configuration menu for that item. You can then make changes to the item from its configuration menu and select to apply the changes. Your ability to view, edit, or delete an item will only be available based on your permissions as an administrator. If you have full access, you can view, edit, or delete most items. If you only have read access, however, you cannot edit or delete items. Your permissions are determined when your administrative account is created (refer to [Specifying the Administrator's Role on page 47](#)).

In addition, the **Search** field, the **Show/hide columns** button, and the arrows that allow you to scroll through multiple pages of listings are included in most menus. You can search each listing by entering the search criteria in the **Search** field. Searches are completed by matching words or parts of words in the string, and searching and sorting can be completed at the same time. In addition, searches are executed across all columns in the menu and can include numerals and IP addresses. For example, if you were to search for information in the **Name** column, enter the string in the search field (for example, enter **College of** to find any names that begin with that string). Any information regarding **College of** is displayed.

The search and sort operations function differently depending on the GUI tab you have selected. The **Configuration** tab does not support numerical sorting for all fields. On the **Status** tab, however, numerical sorting is supported for all fields. In addition, when searching from the **Status** tab, special characters are ignored. for example, searching for 00:19:92:00:c9:60 will also return 00-19-92-00-c9-60.

A typical GUI menu is given below, in which each of these options are identified. There are a few other GUI options you will see as you navigate the vWLAN console, however, those are discussed in this document along with the specific task or menu that they accompany.

Name	Value *	Hint
<a href="#">AP Control Channel Timeout</a>	0	Time in seconds before APs reboot if control channel is confirmed to be lost to the vWLAN (defaults to 0, meaning APs reboot immediately after confirming the control channel is lost)
<a href="#">Post Login Redirect</a>	Disabled	If enabled, users will be redirected to the Post Login Redirect URL after web based authentication instead of their original destination.
<a href="#">Post Login Redirect URL</a>	http://www.adtran.com	The Post Login Redirect URL is the URL that the user will be redirected to after web based authentication instead of their original destination.
<a href="#">Redirect HTTPS traffic for Unregistered clients</a>	Disabled	Redirects HTTPS to the captive portal
<a href="#">Time in minutes between updating internal status (minimum 15)</a>	15	Updates the bandwidth reading
<a href="#">Time in seconds before inactive connections are dropped</a>	600	Inactive connections will be dropped once this time out has been reached.

Showing 1 to 6 of 6 entries

## 5. vWLAN Administrators

Now that you are familiar with the vWLAN GUI, you can begin to configure the vWLAN for your network. The first step in this process is to create the administrators that will be managing the network. vWLAN has two type of administrators: a platform administrator, and a domain administrator. The platform administrator configures the vWLAN settings for the entire vWLAN platform, while the domain administrator configures the settings for particular domains on the vWLAN network. One person can serve both of these functions, or you can separate the two and have one person as a platform administrator, and multiple other individuals as domain administrators. Configuring the administrators for the vWLAN network revolves around creating platform and domain administrators, changing the platform administrator's password, specifying the administrator roles, and specifying the method for administrator authentication. This section discusses different vWLAN administrator configuration tasks and the steps used to complete these tasks. This section includes the following sections:

- [Creating an Administrator on page 43](#)
- [Changing the Administrator's Password on page 46](#)
- [Specifying the Administrator's Role on page 47](#)
- [Specifying Administrator Authentication on page 48](#)

### Creating an Administrator

By default, one administrator account exists when vWLAN is first initialized. This administrator is the default platform administrator, who can manage the platform and all domains in the vWLAN network. The default platform administrator has a default user name of **root@adtran.com** and a default password of **blueblue**. The default platform administrator enjoys full administrative privileges of the platform and all domains.



#### NOTE

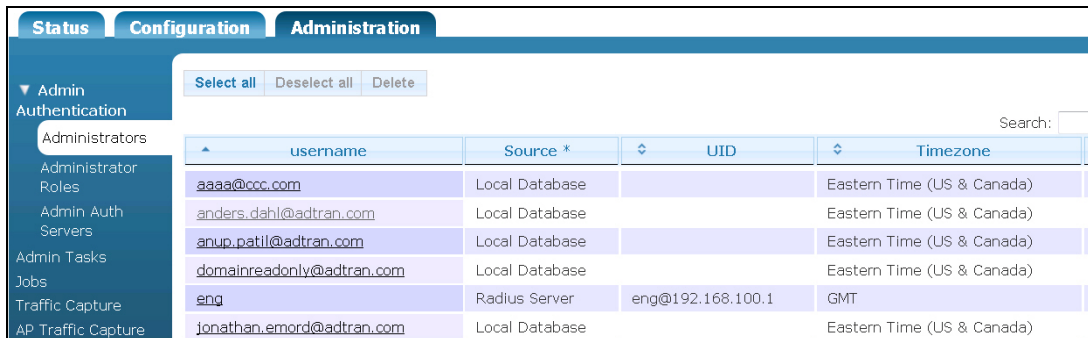
*You cannot change the administrative scope or role of the default platform administrator, or delete the default platform administrator. You can, however, change the user name, email address, password, and time zone for the default platform by selecting **root@adtran.com** (or the default platform administrator login if it has been changed) at the top right of the GUI menu. The default platform administrator will not be displayed in the **Administrators** menu as described below.*

You may need to create additional administrators for the platform or specific domains as part of your initial configuration tasks. In some cases, the default platform administrator will be the same individual as the domain administrator, however, in some vWLAN configurations, platform and domain administrators are separate. Domain administrators are used to manage APs, templates, SSIDs, authorization servers, users, login pages, dashboards, and much more for one or more domains. Domain administrators are optional, as most tasks can be handled by the platform administrator, but in larger deployments, domain administrators can be used to provide managed service to a subset of customers. For example, a service provider could leverage the vWLAN instance for a managed service or cloud-based offerings where they offer managed services or cloud-based services to their customers.

In this case, the service provider would likely be a platform administrator, while the service provider's customers would likely be domain administrators that have access only to their assigned domain. Another example is that a university, or other higher-education establishment, or other business enterprise might have a central IT department as the platform administrator, while the IT staff at remote campuses or offices would be domain administrators.

All administrators (except the default platform administrator) are configured from the **Configuration** tab menu. To create an administrator, follow these steps:

1. Navigate to the **Administration** tab, and select **Admin Authentication > Administrators**.



username	Source *	UID	Timezone
aaaa@ccc.com	Local Database		Eastern Time (US & Canada)
anders.dahl@adtran.com	Local Database		Eastern Time (US & Canada)
anup.patil@adtran.com	Local Database		Eastern Time (US & Canada)
domainreadonly@adtran.com	Local Database		Eastern Time (US & Canada)
eng	Radius Server	eng@192.168.100.1	GMT
jonathan.emord@adtran.com	Local Database		Eastern Time (US & Canada)

2. Select **Platform Administrator** (whether creating a platform or domain administrator) from the **Create** drop-down menu (at the top of the menu), or select **Create Administrator** from the bottom of the **Administrators** menu.



3. Enter the email address and password to be associated with this administrator in the appropriate fields. Confirm the password, and specify the administrator's time zone from the drop-down menu. Then specify the administrator's scope. The administrator's scope consists of the administrator's role (or permissions), and a specific domain associated with the administrator (if selecting domain permissions) or the platform (if selecting platform permissions). Specify the domain to be associated with this administrator by selecting the appropriate domain from the **Domain** drop-down menu (if selecting domain permissions), or select **Platform** from the **Domain** drop-down menu if selecting platform permissions. Each administrator account, including the platform administrator's, must have permissions for at least one domain.
4. Next, specify the administrator's role (or permissions) by selecting the appropriate option from the **Admin Role** drop-down menu. By default, five administrator roles exist:
  - **Domain Read-Write Permissions (Full-Access)** option allows administrators full access to configure and change configurations for the domain(s) to which they are assigned.
  - **Domain Read-Only Permissions** option allows administrators read-only access to the domain(s) to which they are assigned. They cannot make configuration changes to the domain.
  - **Domain Lobby Administrator** option allows administrators to view, create, change, and delete internal users and view the status of users, APs, and dashboards.
  - **Platform Read-Write Permissions (Full-Access)** option allows administrators full access to

configure and change configurations for the vWLAN platform.

- **Platform Read-Only Permissions** option allows administrators read-only access to the vWLAN platform, but does not allow them to make any configuration changes to the platform.

You can also apply a custom administrator role from this drop-down menu. Refer to [Specifying the Administrator's Role on page 47](#) for more information about creating custom roles.



#### NOTE

Platform access is required for administrators to create, view, update, or delete other administrators. Platform access is given by assigning full access by the platform administrator (**root@adtran.com** by default). Once assigned, the platform administrator can specify access for any other administrator to any domain.



#### NOTE

Platform access is required to be able to create domains or associate administrators with a domain. Refer to [Creating the Domain on page 85](#) for more information.

5. After specifying the administrator's email, password, time zone, and scope, select **Create Administrator**.

**Create Administrator**

Email

Password

Password Confirmation

Timezone

**Administrator Scopes**

Domain	Admin Role	
Platform	Domain Read-Write Permissions (Full-Access)	<a href="#">remove</a>
		<a href="#">remove</a>
		<a href="#">remove</a>

[Add more domains](#)

[Create Administrator](#)

6. You will receive confirmation that the new administrator has been created. The confirmation lists the domains associated with the administrator. You can select the listed domains to see all the administrators associated with the domain, and you can select **Edit** if you need to make changes to the administrator's password, email, or domain association.

- The newly created administrators are displayed in the **Administration** tab, in the **Admin Authentication > Administrators** menu. From this menu, you can make any necessary changes to the administrator's configuration.

username	Source *	UID	Timezone	Updated Time
aaaa@ccc.com	Local Database		Eastern Time (US & Canada)	2014-02-06 14:36:37
anders.dahl@adtran.com	Local Database		Eastern Time (US & Canada)	2014-01-23 11:23:08
anup.patil@adtran.com	Local Database		Eastern Time (US & Canada)	2014-02-10 16:06:23
domainreadonly@adtran.com	Local Database		Eastern Time (US & Canada)	2014-01-23 11:34:20
eng	Radius Server	eng@192.168.100.1	GMT	2014-02-11 13:29:55
jonathan_emord@adtran.com	Local Database		Eastern Time (US & Canada)	2014-02-10 10:11:04
liucaiyun@gmail.com	Local Database		Eastern Time (US & Canada)	2014-02-10 09:38:25
platformfull@adtran.com	Local Database		Eastern Time (US & Canada)	2014-01-23 11:42:20
platformreadonly@adtran.com	Local Database		Eastern Time (US & Canada)	2014-01-23 11:34:56
readonly@adtran.com	Local Database		Eastern Time (US & Canada)	2014-01-23 11:33:31

## Changing the Administrator's Password

When first logging into the vWLAN, you will be prompted to change the default platform administrator's password. To change the password, select the **root@adtran.com** link at the upper right portion of the menu. All other administrator passwords are configured from the **Administration** tab, **Admin Authentication > Administrators** menu. To change an administrator's (other than the default platform administrator's) password, follow these steps:

- From the **Administration** tab, **Admin Authentication > Administrators** menu, select the administrator you want to edit from the list (you must have write permissions to complete this action).
- Enter the new password in the **Password** field. Confirm the new password.
- Select **Update Administrator** to save the configuration.

**Edit Administrator**

Email:

Password:

Password Confirmation:

Timezone:

**Administrator Scopes**

Domain:  Admin Role:

[Add more domains](#)

[Show](#) | [Delete](#) | [Create](#) | [Back](#)

- You will receive confirmation that the changes have been successfully applied.

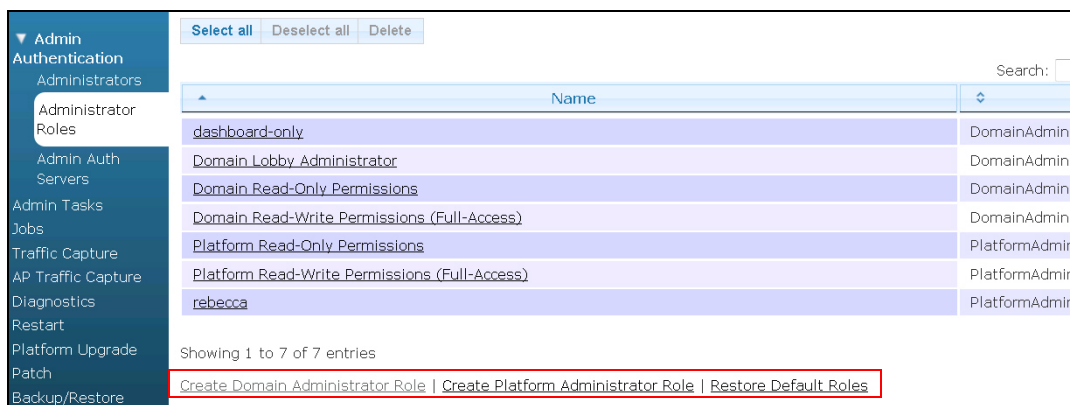
## Specifying the Administrator's Role

The administrator's role is the permissions that are assigned to specific administrator types. You can create a single role, with certain permissions, and apply it to multiple administrators. By default, five administrator roles exist:

- **Domain Read-Write Permissions (Full-Access)** option allows administrators full access to configure and change configurations for the domain(s) to which they are assigned.
- **Domain Read-Only Permissions** option allows administrators read-only permissions for the domain(s) to which they are assigned. They cannot make configuration changes for the domain.
- **Domain Lobby Administrator** option allows administrators to view, create, change, and delete internal users and view the status of users, APs, and dashboards.
- **Platform Read-Write Permissions (Full-Access)** option allows administrators full access to configure and change configurations for the vWLAN platform.
- **Platform Read-Only Permissions** option allows administrators read-only access to the vWLAN platform, but does not allow them to make any configuration changes to the platform.

You can create a custom role or edit an existing role, by following these steps:

1. Navigate to the **Administration** tab, and select **Admin Authentication > Administrator Roles**. The five default roles are listed in this menu. To edit an existing role, select the appropriate role from the list (you must have permissions set in your own administrator role to execute this action). To create a new administrator role, select **Create Domain Administrator Role** (to create a domain administrator role) or **Create Platform Administrator Role** (to create a platform administrator role).



2. If you are creating a new role, enter the name of the role in the **Name** field. Then select the appropriate permissions for the role by selecting the **Read**, **Update**, **Create**, **Destroy**, **None**, or **All** check box next to the action for which you are configuring permission. **None** indicates no permissions are given, and **destroy** indicates delete permissions are given. If you are editing a role,

you will make your changes using the same process. Action selections will vary based on whether you are configuring a platform or domain administrator role.

**Create Administrator Role**

Name

*Select actions that the administrator with this role should be able to perform.*

**Permissions**

Resources	None	Read	Update	Create	Destroy
Select All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
AP Licenses	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Admin Auth Servers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Admin Roles	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Admin Tasks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Administrators	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alarms	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ap Firmwares	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Backup/Restore	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Diagnostics	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Domains	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Email Configurations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
High Availability	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Info Messages	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Network Interfaces	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Notification Templates	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Patches	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Platform Settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Platform Upgrade	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Restarts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Snmp Trap Configurations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Storage Settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Syslog Configurations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Traffic Captures	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. Next, select **Create Admin Role** (or **Edit Admin Role**) to apply the changes.

Restarts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Snmp Trap Configurations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Storage Settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Syslog Configurations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Traffic Captures	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4. The new or updated administrator role is now displayed in the **Administrator Roles** menu, and the administrator role can be associated with new or existing administrators (refer to [Creating an Administrator on page 43](#)).

Roles are not domain specific, so the same role can be used in multiple domains. In addition, administrators can have multiple roles. For example, an administrator can have a read-write role for Domain 1, and a read-only role for Domain 2.

## Specifying Administrator Authentication

Administrator authentication can occur using an external RADIUS database. You can specify that administrators are authenticated using an external source by creating a RADIUS administrator authentication server (you must have authentication server permissions enabled to complete this task).



When an administrator connects to vWLAN, first the local database is checked for authentication. If a local administrator has been created (as described in [Creating an Administrator on page 43](#)), and the log in credentials presented match those listed in the local database, then the administrator is logged into vWLAN. If a locally created administrator attempts to connect to vWLAN and enters an incorrect password, an error is generated and the administrator cannot gain access to vWLAN.

When an administrator created with RADIUS credentials logs in for the first time, a local administration account (with permissions cloned from the local administrator) is created on the vWLAN so the system can track the administrator. The user name of the administrator is created based on the name and the IP address of the RADIUS server (for example, **name@<server ip address>**). The cloned information is stored on vWLAN, and also replicated on any backup vWLAN platforms.

**NOTE**

*If the master vWLAN platform is not functioning, and a backup vWLAN platform is in use, newly created administrators relying on RADIUS to log in will not have access. This happens because the cloned internal administrator cannot be created without the master vWLAN platform.*

If an administrator is configured with both local and RADIUS parameters and local login fails, the vWLAN system checks the login credentials against external RADIUS servers (in the order they are configured). The system continues checking until either it is successful or all servers fail. When a successful RADIUS authentication occurs, the administration credentials are cloned on the local database, and the administrator is logged into vWLAN.

## RADIUS Administrator Authentication Considerations

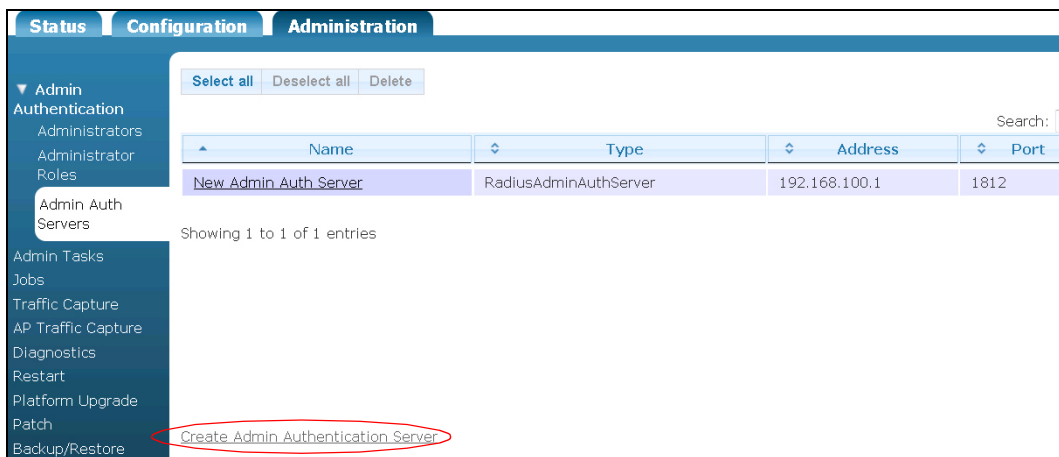
When using RADIUS authentication for administrators, you should keep the following items in mind when configuring the vWLAN network:

- RADIUS servers must be routable from vWLAN. They cannot be behind NAT at the local customer site. This in turn means that the IP address for each RADIUS administrator authentication server must be unique.
- When an external administrator authenticates, the system creates a local administrator to track the user. This means that each administrator must first log into the primary vWLAN platform, and if the first login is to a failover platform (for example, if high availability is in use), then the login will fail.
- Password Authentication Protocol (PAP) authentication is required between the vWLAN system and the RADIUS server, therefore, the RADIUS server must have a policy that supports PAP.
- The RADIUS server must have a RADIUS client configured with the IP address of the vWLAN instance and the shared secret to match what is configured in the **Admin Auth Servers** menu.

## Configuring RADIUS Administrator Authentication

Only a platform administrator user with **Admin Auth Servers** permissions can create, update, delete, or read RADIUS administrator authentication servers. If these actions are permitted, you can configure one or more RADIUS administrator authentication servers by specifying the address, port, shared secret, and timeout values of the RADIUS server, the preference for the RADIUS server, the authentication rules that match RADIUS attributes to specific administrators, and a default RADIUS authenticated administrator (in case none of the rules match). To configure a RADIUS server for administrator authentication, follow these steps:

1. Navigate to the **Administration** tab, and select **Admin Authentication > Admin Auth Servers**. If you want to edit a previously configured RADIUS server, select the appropriate server from the list. If you are creating a new RADIUS server for administrator authentication, either select **Platform Admin Authentication Server** from the **Create** drop-down menu (top of the vWLAN menu), or select **Create Admin Authentication Server** from the **Admin Auth Servers** menu.



2. Configure the server by specifying the server's name, IP address, port, shared secret/password (and confirmation) in the appropriate fields. Remember that each IP address must be unique for each server created.

### Create Authentication Server

Name

IP Address

Port

Shared Secret/Password

Shared Secret/Password Confirmation

3. Next, specify the timeout value and retry value for the RADIUS server. The timeout value is the time (in seconds) between attempts to connect to the RADIUS server. By default, this value is set to **5**

seconds. The retry value (**Retries**) is the number of times to retry the server before determining the server is unreachable. A value of **0** (default) indicates no retries are attempted.

Timeout	<input type="text" value="5"/>
	<i>Enter time in seconds between retries.</i>
Retries	<input type="text" value="0"/>
	<i>Enter RADIUS protocol retry count (0 = no retries).</i>

- After specifying the timeout and retry values, specify the precedence for this RADIUS server. The precedence is the order in which this server is used for authentication, in relation to other configured RADIUS servers. Select the appropriate precedence from the drop-down menu. Selections include **Highest**, **Lowest**, and **Fixed**. If you select **Fixed**, you can manually order the preference for all configured RADIUS servers used for administrator authentication by dragging and dropping the servers within the server list.

Precedence	<input type="text" value=""/>
------------	-------------------------------

- Specify the administrator to which this RADIUS authentication applies by selecting the appropriate administrator from the **Administrator** drop-down menu.

Authentication Rules	
Administrator	<input type="text" value="joesmith@adtran.com"/>

- Lastly, specify the RADIUS attributes that are associated with the administrator by selecting the appropriate RADIUS attribute from the left drop-down menu and the appropriate administrator from the right drop-down menu. You can arrange the order of these attributes by dragging and dropping the attributes within the list. Select **Create Admin Authentication Server** (or **Update Admin Authentication Server**) to apply the configuration.

Authentication Rules			
Administrator	<input type="text" value="anders.dahl@adtran.com"/>		
Attribute	Operator	CompareTo	Role
<input type="text" value="ARAP-Challenge-Response"/>	<input type="text" value="equal to"/>	<input type="text" value=""/>	<input type="text" value="anders.dahl@adtran.com"/>
<input type="text" value="ARAP-Challenge-Response"/>	<input type="text" value="equal to"/>	<input type="text" value=""/>	<input type="text" value="anders.dahl@adtran.com"/>
<input type="text" value="ARAP-Challenge-Response"/>	<input type="text" value="equal to"/>	<input type="text" value=""/>	<input type="text" value="anders.dahl@adtran.com"/>
<input type="text" value="ARAP-Challenge-Response"/>	<input type="text" value="equal to"/>	<input type="text" value=""/>	<input type="text" value="anders.dahl@adtran.com"/>
<input type="text" value="ARAP-Challenge-Response"/>	<input type="text" value="equal to"/>	<input type="text" value=""/>	<input type="text" value="anders.dahl@adtran.com"/>
Append Admin Auth Rule			
<input type="text" value="Create Admin Authentication Server"/>			

- Once the configuration is applied, the new (or updated) server appears in the **Admin Auth Servers** list.

## 6. vWLAN Platform Configuration

This chapter discusses the configuration of vWLAN as it applies to the platform itself. This configuration is completed by an administrator with full access to the platform, although it can be viewed by anyone with platform read permissions. Areas discussed in this section include:

- [Configuring the vWLAN Network Interfaces on page 52](#)
- [Configuring a vWLAN Network Interface Static Route on page 54](#)
- [Changing the Administrator Session Idle Timeout on page 55](#)
- [Configuring the vWLAN Time Settings on page 55](#)
- [Configuring the Platform SNMP Parameters on page 57](#)
- [Configuring the vWLAN TLS 1.0 Setting on page 58](#)
- [Configuring vWLAN Platform Branding on page 59](#)
- [Verifying the vWLAN Software Version on page 59](#)
- [Performing System Maintenance on page 61](#)
- [Restarting the vWLAN on page 67](#)
- [Configuring High Availability on page 68](#)
- [Working with Certificates on page 71](#)

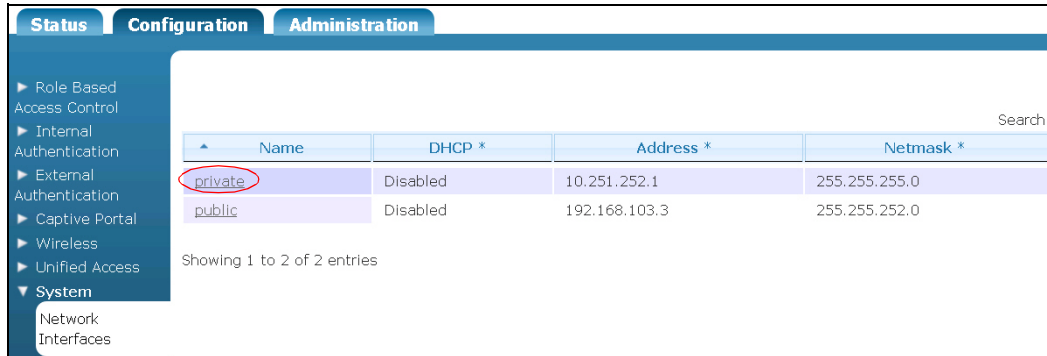
### Configuring the vWLAN Network Interfaces

The vWLAN network interfaces are the interfaces used to communicate with the private and public aspects of the vWLAN network, including routing to and communicating with the APs, connecting to the cloud network where applicable, communicating from vWLAN to vWLAN when using high availability, and configuring vWLAN without connecting to the Serial console. Network interfaces are configured by the platform administrator. By default, both the public and private network interfaces exist on the vWLAN hardware appliance. The public network interface can be configured with a private or public IP address, depending on the deployment scenario. The public network provides connection for APs and web-authenticated users, and the private network provides connection for SNMP and vWLAN management. For example, in an enterprise deployment with private WAN links, the private network interface is likely to be configured with private WAN links, and the public interface is likely to be configured with a private IP address that is routable on the corporate network. In a service provider cloud-based deployment, the public network interface is likely to be configured with a public IP address, however, it can also be configured with a private IP address behind NAT. APs must be configured to communicate with the public network interface, and vWLAN to vWLAN communication using high availability must be configured to communicate using the public network interfaces.

By default, the public network interface is configured as a DHCP client; however, this option can be disabled. The public network interface is labeled **Network** on the vWLAN hardware appliance. The private network interface is used to initially configure the vWLAN without connecting to the serial console port, or to configure local network connectivity for out-of-band management where applicable. The private network interface cannot be configured as a DHCP client. The private network interface is labeled **MGMT** on the vWLAN hardware appliance.

To configure a network interface, follow these steps:

1. Navigate to the **Configuration** tab, then **System > Network Interfaces**. The default configured public and private network interfaces are displayed in a list in the **Network Interfaces** menu. To configure one of these interfaces, select the interface from the list.



2. For the private interface, specify the IP address and network mask for the interface. Select **Update Network Interface** to apply the changes.

### Edit Network Interface

Name private

Address

Netmask

[Show](#) | [Back](#)

3. For the public interface, specify whether DHCP is enabled by selecting the **DHCP** check box. When DHCP is enabled, the current IP address, network mask, and IP gateway address are displayed in the **Network Interface** menu. When DHCP is enabled, you can disable DHCP and specify the IP address, network mask, default gateway, DNS servers, and host name for the network interface. Select **Update Network Interface** to apply the changes.

### Edit Network Interface

Name public

Current Address 10.17.115.11

Current Netmask 255.255.255.0

Current Gateway 10.17.115.254

For a DHCP enabled network, the current address reflects the DHCP address obtained from the DHCP server. The configurable items below are the fallback settings when there is no DHCP server.

DHCP

Address

Netmask

Gateway

DNS 1

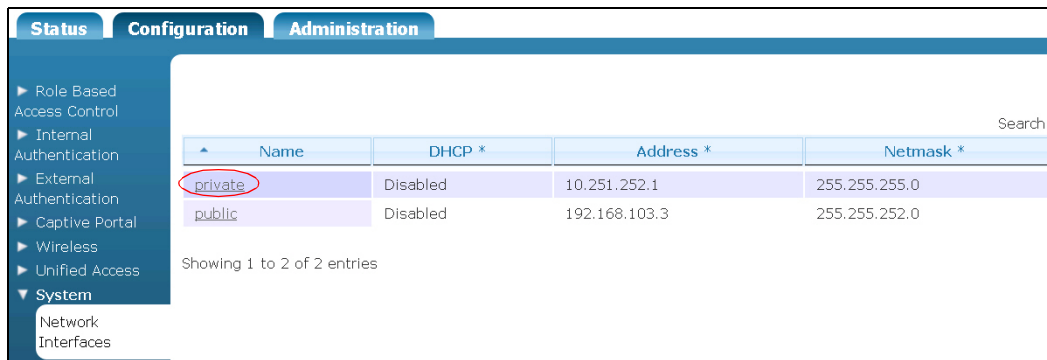
DNS 2

Hostname

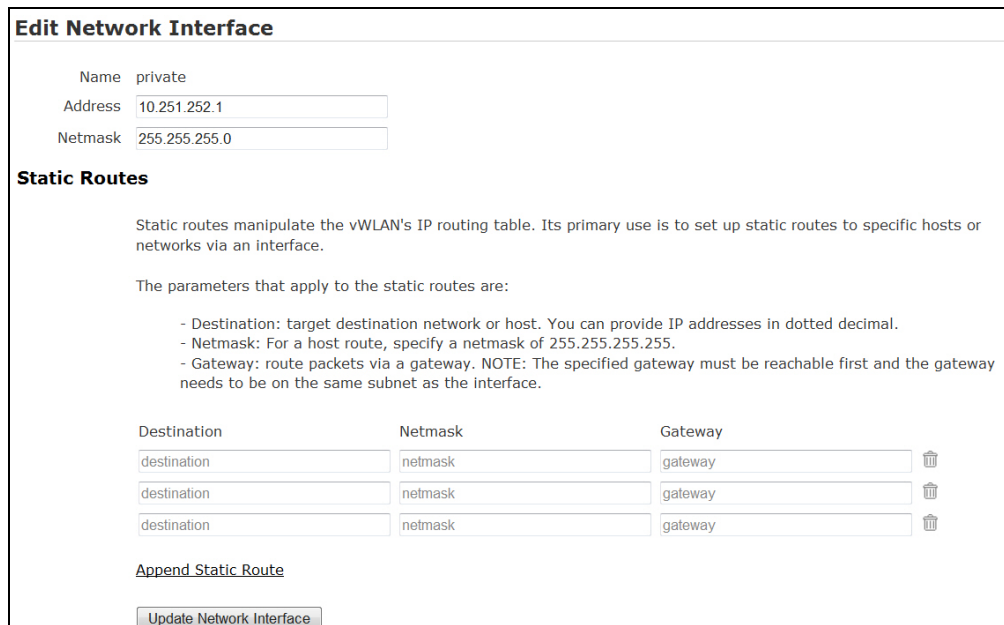
## Configuring a vWLAN Network Interface Static Route

You can optionally configure a static route to manage the vWLAN via the private or management interface from a remote network or to maximize routing paths on the public interface. To set this route, you must specify the route destination IP address, route network mask, and route gateway (must be the same subnet as the interface through which the route travels) on the network interface. You can specify a static route on either the public or private network interface, although the private route will always take precedence over the public one. When new routes are added to the interface, the network is restarted to apply the changes. Static routes are not restored from configuration backups or replicated in HA configurations.

1. To configure a static route to connect to vWLAN remotely, navigate to the **Configuration** tab, then **System > Network Interfaces**. The default configured public and private network interfaces are displayed in a list in the **Network Interfaces** menu. To configure a static route for one of these interfaces, select the interface from the list.



2. For either interface, enter the route destination, route network mask, and route gateway for the interface's static route. You can add multiple routes to the interface, and can choose to delete any routes by using the trash can icon next to the route you want to delete. Select **Append Static Route** and then **Update Network Interface** to apply the changes.



## Changing the Administrator Session Idle Timeout

The default administrator session idle timeout is 30 minutes. As of vWLAN firmware release 3.1.0, you can change the length of idle time before an administrative session will timeout.

1. Navigate to **System > Settings >** and select the **Platform** tab. Select **Administrator Session Idle Timeout**.

Name	Value *	Hint
Administrator Session Idle Timeout	30	Sets the idle timeout for administrative console sessions in minutes. Valid entries are 15 to 300, and 0 for no timeout
Certificate 1		The vWLAN requires a certificate for Apache+mod_ssl/OpenSSL.
Certificate 2		The vWLAN requires a certificate for Apache+mod_ssl/OpenSSL.
Certificate Chain 1		A chain of one or more certificates.
Certificate Chain 2		A chain of one or more certificates.
Certificate Private Key 1		The private key for the cert (closely guard this file).
Certificate Private Key 2		The private key for the cert (closely guard this file).
Certificate Selected	Click the name link to see the value	Certificate for current use.
Certificate Signature Request 1 (CSR)		The vWLAN requires a certificate for Apache+mod_ssl/OpenSSL. Use the Show action to use a form to create the CSR manually.

2. Specify the idle timeout for administrative console sessions. Valid entries are 15 to 300 minutes or 0 for no timeout. Select **Update Platform Setting**.

**Edit Platform Setting**

Administrator Session Idle Timeout

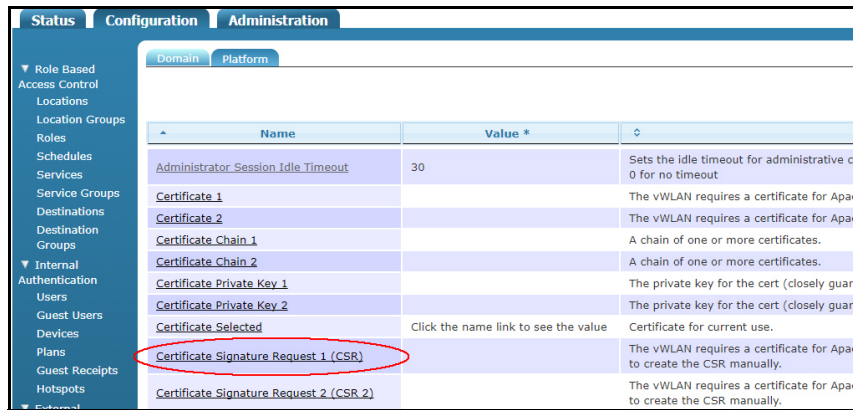
*Sets the idle timeout for administrative console sessions in minutes. Valid entries are 15 to 300, and 0 for no timeout*

[Show](#) | [Back](#)

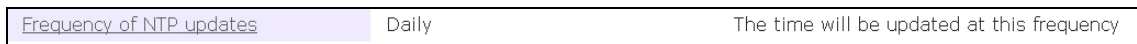
## Configuring the vWLAN Time Settings

The vWLAN time settings must be configured to use Network Time Protocol (NTP). These settings are configured from the platform administrator menu. To configure the vWLAN NTP update frequency and server used, follow these steps:

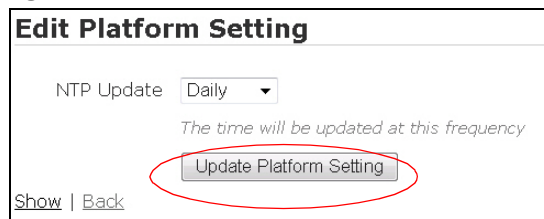
1. Navigate to the **Configuration** tab, then **System > Settings**. Select the **Platform** tab.



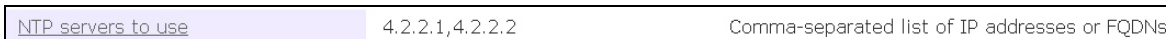
2. Select the task item labeled **Frequency of NTP Updates**.



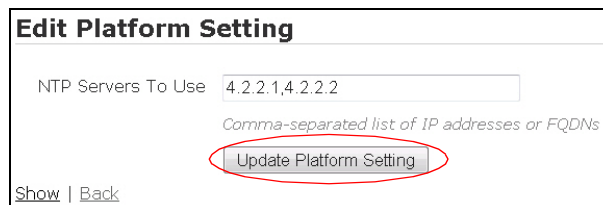
3. From the drop-down menu, select how often you would like vWLAN to receive NTP updates. Choices included are: **Daily**, **Hourly**, **Weekly**, or **Monthly**. When you have made your choice, select **Update Platform Setting**. You will receive confirmation that the changes have been made.



4. After setting the NTP update value, you should specify the NTP servers from which vWLAN receives the NTP updates. Navigate back to the **Configuration** tab, **System > Settings**, and select the **Platform** tab. Then select the task item labeled **NTP servers to use**.



5. In the appropriate field, enter the IP address or FQDN of the NTP server to be used by the vWLAN. Multiple servers can be specified by entering IP addresses or FQDNs separated by a comma, with no spaces. After entering the server IP address or FQDN, select **Update Platform Setting**. At this point, vWLAN immediately connects to the NTP server to sync to the proper time.



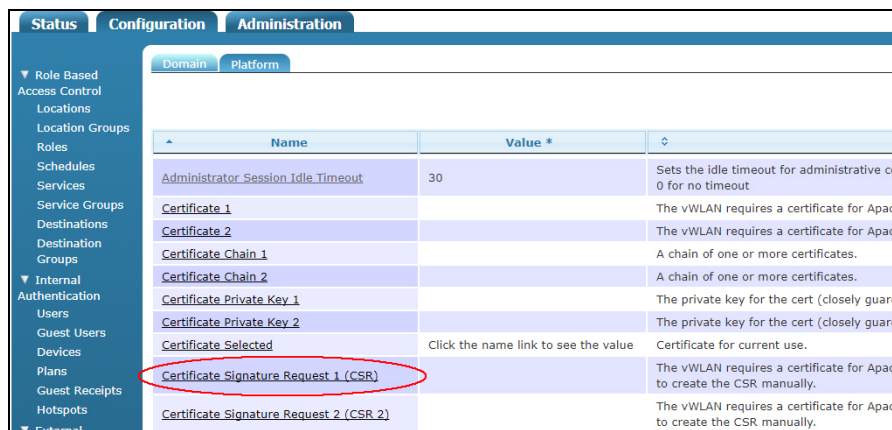


## Configuring the Platform SNMP Parameters

Simple Network Management Protocol is the Internet Engineering Task Force (IETF) industry-standard Application Layer protocol for remotely managing networks. SNMP provides management services that include automatic notification when unacceptable network conditions exist, status polling of network devices, and the ability to edit configuration settings. SNMP parameters are configured from the platform administrator menu. vWLAN supports SNMPv2c. By default, the vWLAN will have SNMP disabled for polling from external network management stations. Standard MIB-2 polling is supported. Vendor-specific MIBs are available online at [www.adtran.com](http://www.adtran.com). SNMP polling can be configured on a vWLAN platform-wide basis. SNMP traps can be configured on a per-domain basis. The following section discusses platform-wide SNMP polling configuration. For more information about per-domain SNMP trap configuration, refer to [Configuring Domain Settings on page 133](#).

To configure SNMP polling at the platform level in vWLAN, follow these steps:

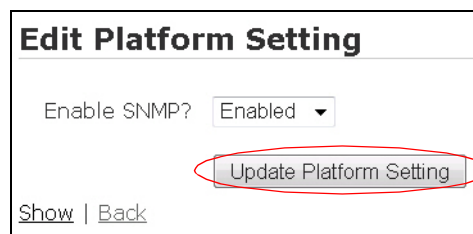
1. Navigate to the **Configuration** tab, **System > Settings**, and select the **Platform** tab.



2. Select the task item labeled **Enable SNMP?**



3. Select **Enabled** from the drop-down menu to enable SNMP and select **Update Platform Setting**. You will receive confirmation acknowledging that the changes have been made.



4. By default, the SNMP contact is named **Contact**, and the SNMP location is named **Location**. You can change these values by selecting the task items labeled **SNMP Contact** and **SNMP Location**. Enter the contact and location name in the appropriate field, using between 6 and 20 characters, and select **Update Platform Setting**. An **Admin Task** is created, showing the need to restart the SNMP daemon. Select the administrative task to restart SNMP and have the new settings take effect. Once

SNMP is enabled, both the public and private network interfaces on vWLAN will respond to the SNMP polls.

## Configuring the vWLAN TLS 1.0 Setting

By default, in the vWLAN 3.6.0 release, the vWLAN platform has Transport Layer Security version 1.0 disabled for Hypertext Transfer Protocol (HTTP) connections due to the known security vulnerabilities with this protocol. If necessary, you can choose to enable support for TLS 1.0 in the vWLAN platform by following these steps:

1. Navigate to the **Configuration** tab, and select **System > Settings**, and select the **Platform** tab.
2. Select the task item labeled **Enable TLS 1.0**.

Name	Value *	Hint
Administrator Session Idle Timeout	30	Sets the idle timeout for administrative console sessions in minutes. Valid entries are 15 to 300, and 0 for no timeout
Certificate 1	Click the name link to see the value	The vWLAN requires a certificate for Apache+mod_ssl/OpenSSL.
Certificate 2	Click the name link to see the value	The vWLAN requires a certificate for Apache+mod_ssl/OpenSSL.
Certificate Chain 1	Click the name link to see the value	A chain of one or more certificates.
Certificate Chain 2	Click the name link to see the value	A chain of one or more certificates.
Certificate Private Key 1	Click the name link to see the value	The private key for the cert (closely guard this file).
Certificate Private Key 2	Click the name link to see the value	The private key for the cert (closely guard this file).
Certificate Selected	Click the name link to see the value	Certificate for current use.
Certificate Signature Request 1 (CSR)	Click the name link to see the value	The vWLAN requires a certificate for Apache+mod_ssl/OpenSSL. Use the Show action to use a form to create the CSR manually.
Certificate Signature Request 2 (CSR 2)	Click the name link to see the value	The vWLAN requires a certificate for Apache+mod_ssl/OpenSSL. Use the Show action to use a form to create the CSR manually.
Enable SNMP?	Disabled	
Enable TLS 1.0	Disabled	Enable Transport Layer Security protocol version 1.0 for HTTP access. This is an older security protocol with known security vulnerabilities.
Public IP address for vWLAN standalone or high availability master	207.229.96.98	Only use this if the vWLAN controller is sitting behind a NAT device.
Read-Only Community String	public	Read-only community string (6-20 characters).
Read-Write Community String	public	Read-write community string (6-20 characters).

3. Select **Enabled** from the drop-down menu to enable TLS 1.0 support and select **Update Platform Setting**.

### Edit Platform Setting

Enable TLS 1.0 Enabled

*Enable Transport Layer Security protocol version 1.0 for HTTP access. This is an older security protocol with known security vulnerabilities.*

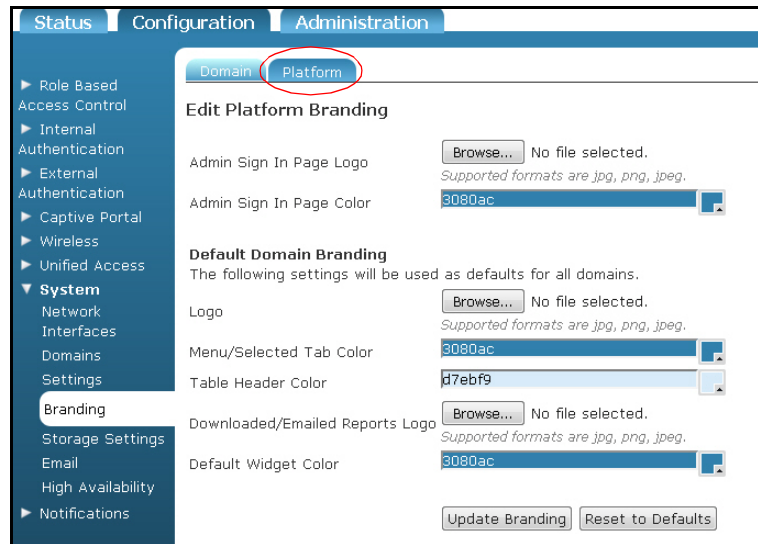
[Show](#) | [Back](#)

4. You will receive notification that a **Platform Task** has been created to restart vWLAN and apply the setting changes (refer to [Administrative Tasks on page 265](#) for more information about platform tasks).

## Configuring vWLAN Platform Branding

In vWLAN release 2.9.0, the option to brand the administrator's sign in page on the vWLAN platform was added. This feature allows you to add logos or change the colors of the administrator's sign in page, as well as specify the default logos and menu, table, or widget colors for any domains that are created on the platform. To access the vWLAN platform branding, and specify administrator sign in page or default domain branding settings, follow these steps:

1. Navigate to the **Configuration** tab, and select **System > Branding**, and then select the **Platform** tab.

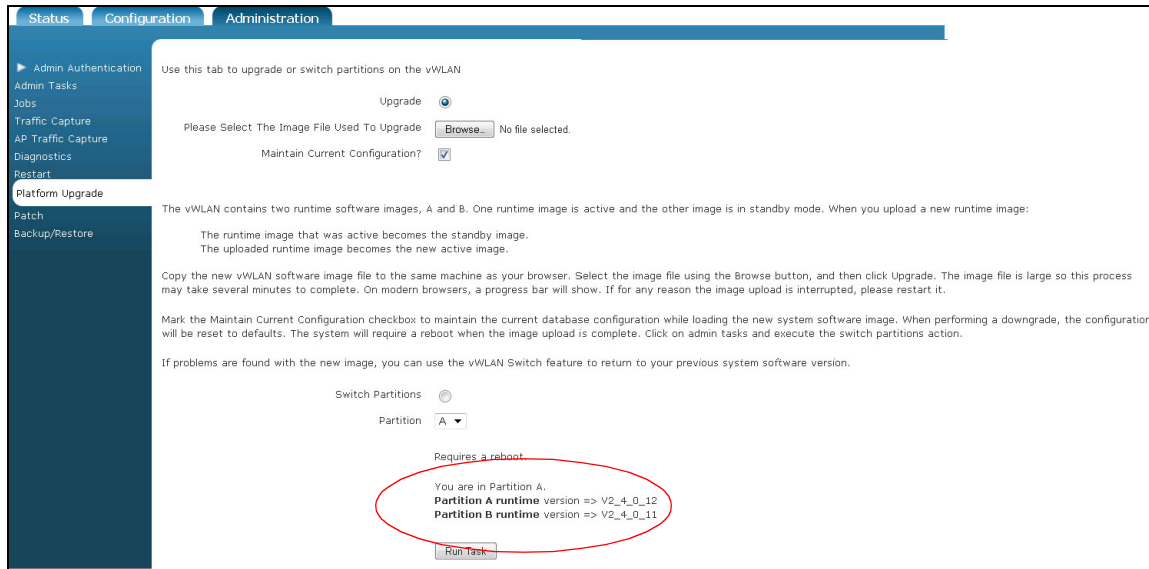


2. In the **Edit Platform Branding** menu, add any logos to the administrator's sign in page by uploading a logo file. Supported file formats are **.jpg**, **.png**, or **.jpeg**. In addition, you can specify the color of the administrator's sign in page by selecting a color in the **Admin Sign In Page Color** field.
3. Specify the default branding settings for any domains that are created by uploading your own logo for the domain login page or for downloaded or emailed reports. Supported file formats are **.jpg**, **.png**, or **.jpeg**. Domain logo file sizes are 265 pixels (width) by 60 pixels (height).
4. Specify the default colors for domain menus, tables, and widgets by selecting the appropriate colors in the menu, table, or widget fields.
5. Once you have uploaded all files and made your color selections, select **Update Branding** at the bottom of the menu to apply the changes. You can also reset branding to the default settings if necessary by selecting **Reset to Defaults**.

## Verifying the vWLAN Software Version

Upon initial installation of the vWLAN, or prior to upgrading, patching, or troubleshooting, you might need to verify the vWLAN software version. This task is completed by the platform administrator. To verify the vWLAN software version, follow these steps:

1. Navigate to the **Administration** tab, and select **Platform Upgrade**.



2. Scroll to the bottom of the menu and verify the partition the vWLAN is currently using (**A** or **B**), and view the current vWLAN software version. In the example below, the vWLAN software version is **V2\_4\_0\_12**.

You are in Partition A.  
**Partition A runtime** version => V2\_4\_0\_12  
**Partition B runtime** version => V2\_4\_0\_11



**NOTE**

*You might need to verify any patches that you have installed, as well as the vWLAN software version. To verify installed patches, refer to [Managing Patches on page 66](#). In addition, you might need to know the serial number of any APs when asking for technical support. AP serial numbers are displayed in the **Access Points** menu of the **Status** tab. If you need to know the serial number of the vWLAN hardware appliance, look for it on the bottom of the appliance. vWLAN instances installed in VMware do not have a serial number.*

## Performing System Maintenance

General system maintenance is performed by the platform administrator, and includes such tasks as restarting the system, compiling information for technical support, configuring backup or restore parameters, managing the vWLAN runtime image, and managing patches. These tasks are accessed by navigating to the **Administration** tab in the top of the menu. The system management tasks are described in the following sections.

### System Restart

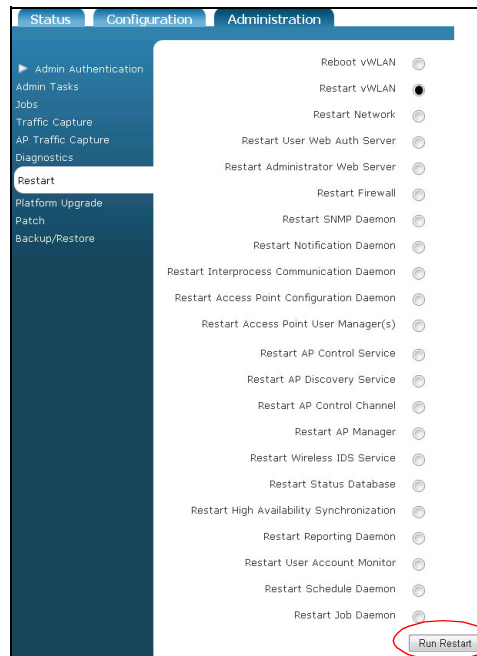
Some vWLAN configuration tasks, such as restoring defaults, require a system restart. To restart the vWLAN system, follow these steps:

1. Navigate to the **Administration** tab and select **Run Restart**.



2. Select the appropriate item to restart from the list in the restart menu by selecting the button next to the item you want to restart. Selections include restarting or rebooting the vWLAN appliance, the network, the user web-based authentication server, the administrator web server, the firewall, several daemons (such as the Interprocess Communication Daemon, which communicates between processes, and the AP Configuration Daemon that aids in AP configuration), the access point user manager, the AP control or discovery service, AP control channel, AP manager, the Wireless Intrusion Detection Service (W-IDS), the status database, the high availability synchronization, and

the user account monitor. You can select a single item at a time. To restart the vWLAN system only, as in the case of a patch installation, select **Restart vWLAN**, and then select **Run Restart**.



**i** **NOTE**

*Restarting the vWLAN appliance will interrupt network traffic if you do not have a high availability backup unit configured.*

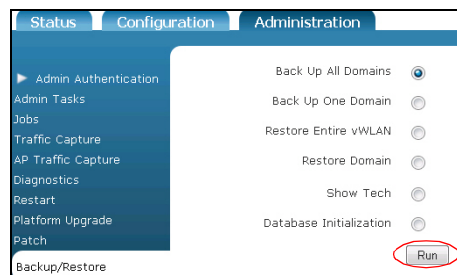
**i** **NOTE**

*Typically you should rely upon notifications from the **Admin Tasks** list in the GUI when tasks such as a restart should be completed. For example, when installing a patch, a **Platform Task** is created to alert you that you need to reboot.*

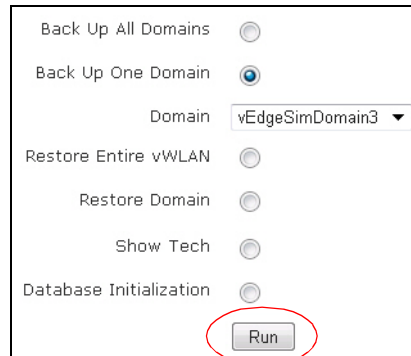
### Configuring Backup or Restore Parameters

The vWLAN system can be backed up on demand, and it can be restored from a saved backup or to the default settings. To perform a backup or restore, follow these steps:

1. Navigate to the **Administration** tab and select **Backup/Restore**.



2. Select the backup or restore task you would like to perform by selecting the button next to the appropriate item. You can choose to backup all domains, back up a single domain, restore the entire vWLAN, restore a domain, show technical information, or initialize the database. After making the appropriate selection, select **Run**.



The screenshot shows a maintenance interface with the following options and controls:

- Back Up All Domains:
- Back Up One Domain:
- Domain: vEdgeSimDomain3 (dropdown menu)
- Restore Entire vWLAN:
- Restore Domain:
- Show Tech:
- Database Initialization:
- Run:  (circled in red)

**NOTE**

*Backing up a domain creates a copy of the domain configuration, which can then be used as a backup configuration of the domain, or a configuration template for multiple tenant installations. Domain backups are not compatible across vWLAN software releases. You cannot backup a domain under an earlier vWLAN software release and restore it under a newer software version. You must take a replication snapshot after you restore a domain in a high availability configuration.*

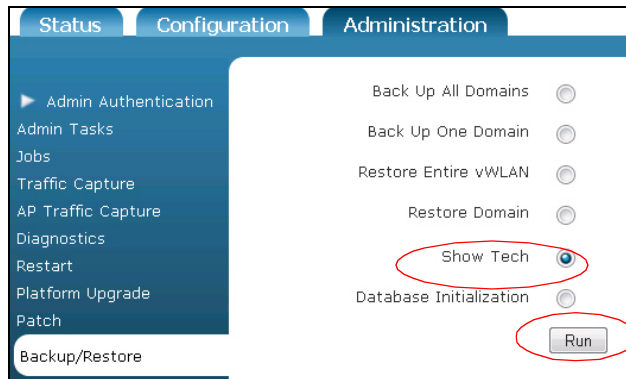
**NOTE**

*Restoring a configuration removes all existing vWLAN configuration. However, the IP address remains the same, so the box can be accessed after a configuration restoration.*

## Using Show Tech for Technical Support

In addition to maintaining the vWLAN platform, you can use the **Show Tech** option to compile information that will be helpful when an issue arises with vWLAN that requires you to contact technical support or engineering for advanced diagnostics. The **Show Tech** option compiles an encrypted file that contains the configuration, logs and alerts, and a time-stamped snapshot of vWLAN that can only be opened by ADTRAN technical support or ADTRAN engineering.

To run a **Show Tech**, navigate to the **Administration** tab and select **Backup/Restore**. Select **Show Tech** from the list and select **Run**.

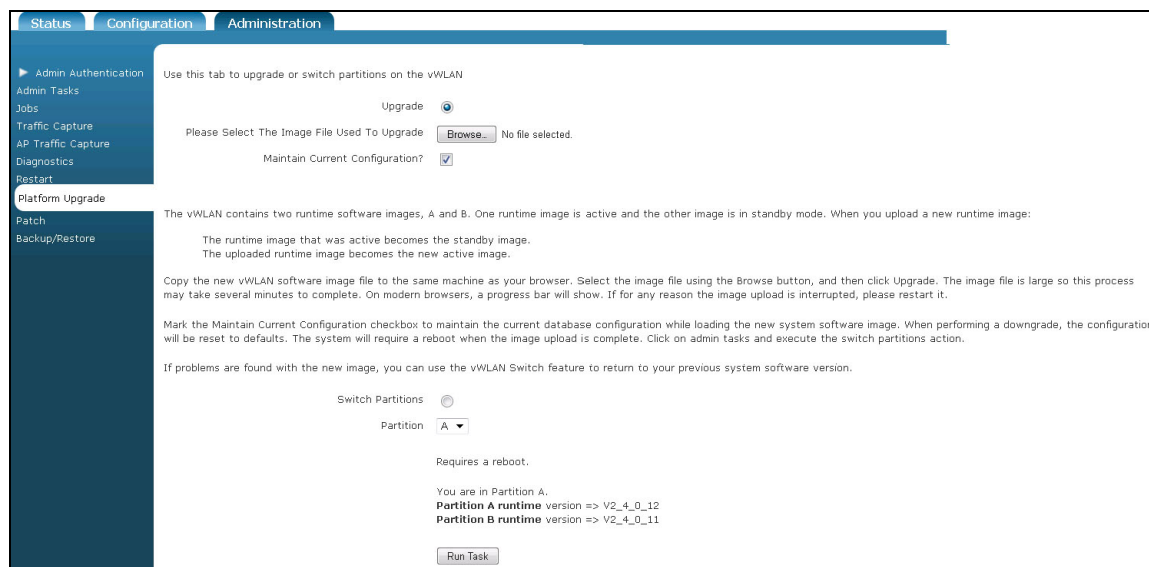


## Managing the vWLAN Runtime Image

vWLAN contains two runtime images: image A and image B. A runtime image consists of a unique software image and configuration. When one runtime image is active, the other is in standby mode. Runtime images are independent of each other, and when uploading a new software image to the runtime image, the runtime image that was active automatically becomes the standby image and the uploaded image automatically becomes the new active image once the system is rebooted. You can also switch between the runtime images from the GUI menu. For example, if you upload a new software image, and begin experiencing problems, you can switch back to your original pre-update runtime image.

To upload a new runtime image, follow these steps:

1. Navigate to the **Administration** tab and select **Platform Upgrade**.



2. Select the **Upgrade** button, and then select **Browse** to retrieve the appropriate software image from the correct location. Make sure to check the box labeled **Maintain current configuration**. This



feature allows you to maintain the current database configuration while loading the new system software image.

Use this tab to upgrade or switch partitions on the vWLAN

Upgrade

Please Select The Image File Used To Upgrade  No file selected.

Maintain Current Configuration?



#### NOTE

You can find software images online from the **Support** page at [www.adtran.com](http://www.adtran.com) or from the ADTRAN support community at <https://supportcommunity.adtran.com>.

3. Select **Run Task** to begin the image upload. On non-Internet Explorer browsers, a progress bar displays as the image uploads. Once the image is uploaded, the progress of the upgrade is displayed (in any browser).
4. Once the upgrade is complete, you must reboot the vWLAN system. To reboot the system, navigate to the **Administration** tab, select **Restart**, and select **Reboot vWLAN**. Then select **Run Restart** to reboot the box and apply the new runtime image. Alternatively, you can select **Platform Tasks** (at the top of the GUI) and select the reboot task from the task list (refer to [Administrative Tasks on page 265](#)).

To switch between an active runtime image and another previously loaded runtime image, follow these steps:

1. Navigate to the **Administration** tab and select **Platform Upgrade**.

The screenshot shows the Administration tab with the Platform Upgrade section selected. The interface includes a sidebar with navigation options: Admin Authentication, Admin Tasks, Jobs, Traffic Capture, AP Traffic Capture, Diagnostics, Restart, Platform Upgrade (selected), Patch, and Backup/Restore. The main content area contains the following text and controls:

Use this tab to upgrade or switch partitions on the vWLAN

Upgrade

Please Select The Image File Used To Upgrade  No file selected.

Maintain Current Configuration?

The vWLAN contains two runtime software images, A and B. One runtime image is active and the other image is in standby mode. When you upload a new runtime image:

- The runtime image that was active becomes the standby image.
- The uploaded runtime image becomes the new active image.

Copy the new vWLAN software image file to the same machine as your browser. Select the image file using the Browse button, and then click Upgrade. The image file is large so this process may take several minutes to complete. On modern browsers, a progress bar will show. If for any reason the image upload is interrupted, please restart it.

Mark the Maintain Current Configuration checkbox to maintain the current database configuration while loading the new system software image. When performing a downgrade, the configuration will be reset to defaults. The system will require a reboot when the image upload is complete. Click on admin tasks and execute the switch partitions action.

If problems are found with the new image, you can use the vWLAN Switch feature to return to your previous system software version.

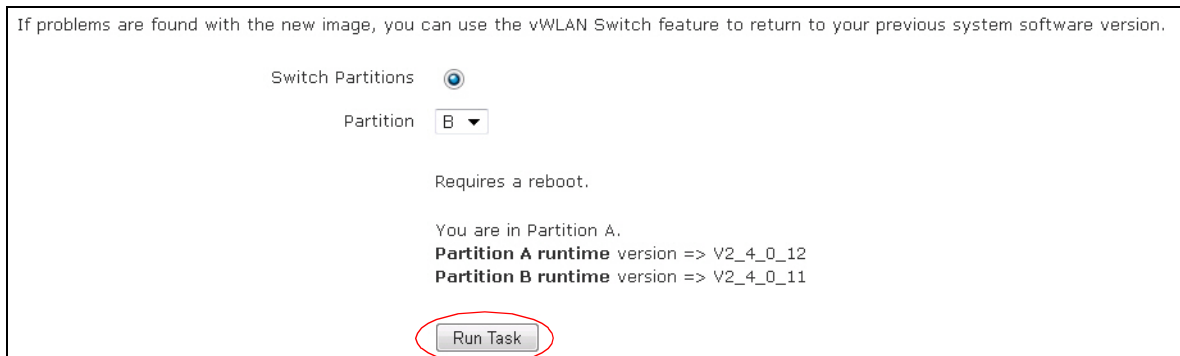
Switch Partitions

Partition

Requires a reboot.

You are in Partition A.  
**Partition A runtime version => V2\_4\_0\_12**  
**Partition B runtime version => V2\_4\_0\_11**

2. Select **Switch Partitions**, and select the partition you would like to use from the drop-down menu. You can verify the partition you are using, and its current firmware, by viewing the partition information on this menu.



3. Select **Run Task**.
4. Once the task is complete, you must reboot the vWLAN system. To reboot the system, select **Admin Tasks** and select the reboot task from the task list (refer to [Administrative Tasks on page 265](#)), or navigate to the **Administration** tab, select **Restart**, and then select **Reboot vWLAN**. Next, select **Run Restart** to reboot the appliance and switch partitions.

## Managing Patches

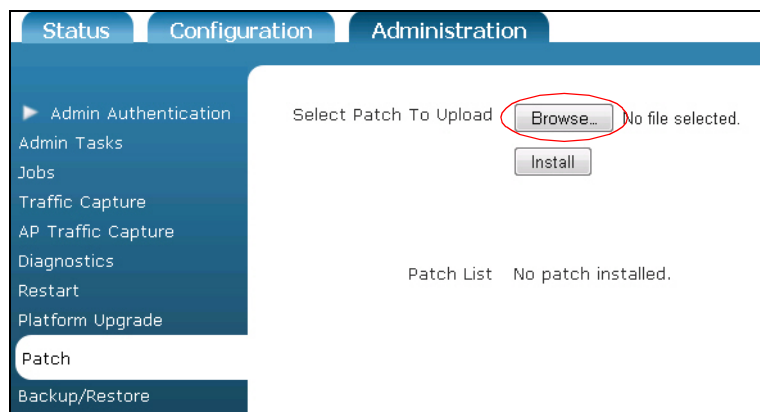
From time to time, vWLAN software patches are released. These patches can be uploaded into vWLAN by the platform administrator, and are used to ensure that your vWLAN network is running at optimal performance and has the latest feature set.

**i** **NOTE**

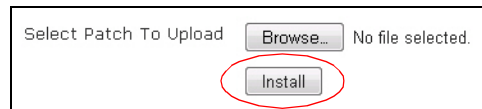
*In a high availability network configuration, each vWLAN platform must have patches installed individually (patches are not replicated between the primary and secondary vWLAN instances).*

To upload a vWLAN software patch, follow these steps:

1. Navigate to the **Administration** tab and select **Patch**.



2. Select the patch to install using the **Browse** button. Patches can be downloaded from the [Product Downloads](#) page at [www.adtran.com](http://www.adtran.com).
3. Select **Install**.

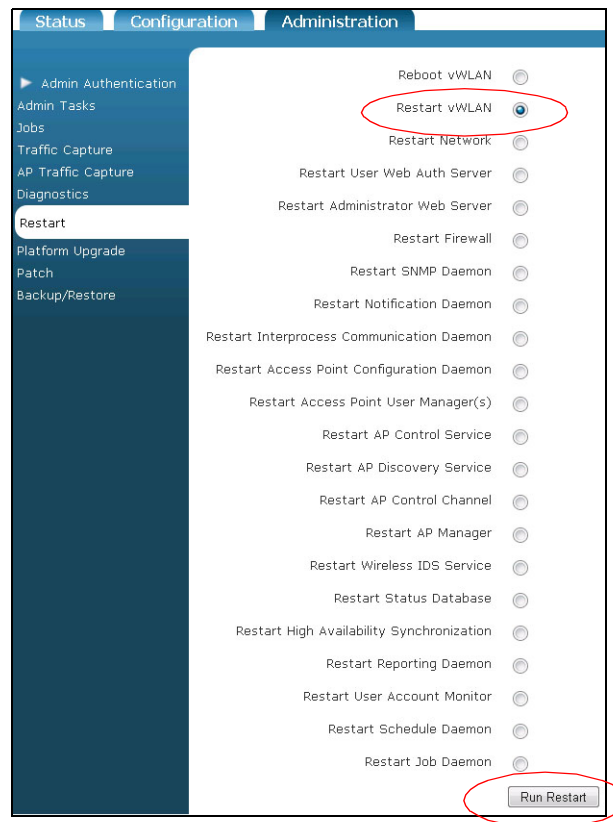


4. Any patches that you have installed will be visible in the **Patch list**. A **Platform Task** might display, if a reboot or restart is required. Patches can also be uninstalled from this page.

## Restarting the vWLAN

Restarting the vWLAN is often necessary after restoring the vWLAN to the default settings, changing runtime images, or making significant configuration changes. To restart the vWLAN follow these steps:

1. Navigate to the **Administration** tab and select **Restart**.
2. Select **Restart vWLAN** from the menu.
3. Select **Run Restart**.



## Configuring High Availability

High availability is a vWLAN failover feature that causes the AP on which it is enabled to connect to a secondary vWLAN system without disconnecting any clients. In a failover situation with high availability enabled, traffic continues to flow while the AP establishes a new control channel to the secondary vWLAN system. After the failover to the secondary vWLAN, the AP continues to allow new clients to connect and authenticate. When the primary vWLAN system is again available, the APs reconnect to the primary vWLAN, with no packet loss. In addition to configuring your domains, APs, and wireless security measures, you can configure your vWLAN failover by configuring high availability. When the high availability feature is configured, the primary AP licenses are automatically transferred to the standby vWLAN system.

### High Availability Process

When high availability is in use, the primary vWLAN licenses are automatically transferred to the standby appliance, and the static configuration of channel/power, adjacent AP list, and user accounts for each AP are synchronized between the two systems. During a failover event, when the APs move from the primary to secondary vWLAN, the connections are synchronized from the AP to the secondary vWLAN. The APs do not reboot, deauthorize clients, or discontinue operation.

When the AP first boots, the AP discovers a single IP address (either that of the primary or secondary vWLAN). If a secondary IP address is discovered, the AP will then reattach to the primary address.

In a failover situation, the AP is in one of the following states:

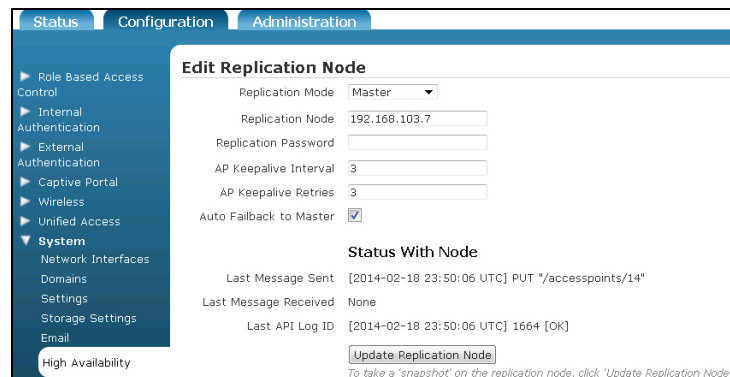
- **Discovery** indicates the AP is booting and attempting to find the vWLAN.
- **Connected to Primary** indicates the AP is connected to the primary vWLAN system and continually checks the state of the primary system. If the primary system fails, the AP connects to the secondary system.
- **Connected to Secondary** indicates the AP is connected to the secondary vWLAN system and continually checks the state of the primary system. If the primary system returns to service, the AP connects to the primary system.
- **Standby** indicates that if both the primary and secondary vWLAN system experience a failure, and a standby SSID is configured, the AP broadcasts the standby SSID. If no standby SSID is configured, the AP reboots. While in this standby mode, the AP continually attempts to establish a connection to either vWLAN. If one of the vWLAN systems becomes available, the AP leaves standby mode.
- In addition, you can configure a control channel timeout that will not reboot the AP even if the control channel is lost. Refer to [Configuring Domain Settings on page 133](#) for more information. In this case, the standby SSID is not up. Instead, the SSIDs are broadcast as normal, and existing clients remain connected, but new clients cannot connect.

During a vWLAN failure, if the primary vWLAN system is lost, all APs failover to the secondary vWLAN, and users remain connected. By default, the backup system is in read-only mode, so no configuration changes can be made. If the primary system is restored, then the vWLAN system resumes operation from the point at which the failover occurred. If a replacement appliance is obtained, the configuration must be restored on the primary vWLAN system by either using an old configuration file loaded on the primary system, or by promoting the secondary vWLAN system to the primary system and using the replacement as the new secondary system.

The primary and secondary public network interface IP addresses of the primary and secondary vWLAN systems are specified by the platform administrator of both systems. The configuration, licensing, AP firmware, report definitions, and notification settings of the primary vWLAN are replicated between the primary and secondary vWLAN appliances, with the primary system as a read-write configuration, and the secondary system as a read-only configuration. Software images, patches, certificates (unless they are vWLAN specific certificates or LDAP server certificates), redirection to a host name, administrative dashboards, and report, log, or alert data are not replicated. User and AP statuses are retrieved on demand from the AP during an AP failover. A key or shared secret is required between the two systems. When configuring high availability, you will configure the mode of the system (**Standalone**, **Master** (primary), or **Node** (secondary), the IP address of the master or node system, the password for communication between the two systems, the keepalive interval for APs, and the number of AP keepalive retries. You can also opt to configure automatic failback to the master system on the node system.

To configure high availability, follow these steps:

1. Navigate to the **Configuration** tab, and select **System > High Availability**. By default, the vWLAN system is set to **Standalone** replication mode.



2. To change the replication mode of the vWLAN system select the appropriate option (**Master** if this is the primary system or **Node** if this is a secondary system) from the **Replication Mode** drop-down menu.
3. If you are configuring a master system, you will need to enter the public network interface IP address of the secondary node in the **Replication Node** field, and the shared password between the systems in the **Replication Password** field. Then specify the AP keepalive interval and retry values in the appropriate fields. AP keepalive intervals and retries are set to **3** by default and cannot be set lower.

Lastly, check **Auto Failback to Master** to enable the AP to automatically return to the primary vWLAN system once it becomes available.

### Edit Replication Node

Replication Mode Master

Replication Node

Replication Password

AP Keepalive Interval

AP Keepalive Retries

Auto Failback to Master

**Status With Node**

Last Message Sent [2014-02-18 23:50:06 UTC] PUT "/accesspoints/14"

Last Message Received None

Last API Log ID [2014-02-18 23:50:06 UTC] 1664 [OK]

*To take a 'snapshot' on the replication node, click 'Update Replication Node'.*

4. Select **Update Replication Node** to apply the changes. A confirmation message (**Replication Node was successfully updated**) is displayed to indicate the changes have been made.
5. After configuring the master vWLAN system, you must configure the secondary vWLAN system following the same steps. Navigate to the **Configuration** tab, and select **System > High Availability** in the secondary vWLAN system. Select **Node** from the **Replication Mode** drop-down menu. Enter the public network interface IP address of the primary (master) system in the **Replication Node** field, and the shared password between the systems in the **Replication Password** field (this password should match the one used when configuring the master system).

### Edit Replication Node

Replication Mode Node

Replication Master

Replication Password

AP Keepalive Interval

AP Keepalive Retries

Auto Failback to Master

**Status With Node**

Last Message Sent [2014-02-18 23:50:06 UTC] PUT "/accesspoints/14"

Last Message Received None

Last API Log ID [2014-02-18 23:50:06 UTC] 1664 [OK]

*To take a 'snapshot' on the replication node, click 'Update Replication Node'.*



#### NOTE

*The node obtains the bottom three values from the master, and they are not configurable on a node vWLAN system.*

6. Select **Update Replication Node** to apply the changes. A confirmation message (**Replication Node was successfully updated**) is displayed to indicate the changes have been made. At this point the node obtains a configuration snapshot from the master. This requires TCP port 2335 to be allowed between the vWLAN public network interfaces. The snapshot can take a significant amount of time, particularly if there are many domains configured on the master. After the snapshot is complete, the node restarts to ensure all updates are in effect. After the restart, any configuration changes made to the master are automatically replicated to the node (using TCP port 3000 between the public network interfaces), except for those that generate an administration task (refer to [Replicating Master Configuration Changes on the Node on page 71](#)).

## Replicating Master Configuration Changes on the Node

In high availability configurations, configuration changes executed on the master system (for example, modifying SNMP) that generate an administration task are not automatically applied to the node system. To commit the change on the node system, you must manually apply the changes by logging into the node system and then manually applying the correct administration task as described in [Administrative Tasks on page 265](#).

## Working with Certificates

When vWLAN communicates with an LDAP server, SSL can be used to encrypt and authenticate the traffic. You can customize the way that certificates are handled in vWLAN by managing trusted certificates of authority (CAs), trusted servers, and client certificates as well as configuring the certificate settings in the vWLAN platform and the remote LDAP system. Certificate management tasks for vWLAN include installing new certificates, uploading certificates to vWLAN, and renewing certificates. Certificate management for the remote LDAP system includes managing LDAP CAs, trusted LDAP server certificates, and trusted LDAP client certificates (optional). Multiple certificates can be configured on vWLAN to aid in certificate renewal.



### NOTE

*The certificate on vWLAN is a per-platform item, while the LDAP certificates are a per-domain, per-LDAP server item.*

## Installing Certificates to vWLAN

By default, vWLAN uses a preinstalled self-signed SSL certificate to encrypt web-based login transactions. The vWLAN uses the SSL certificate when clients connect to the captive portal (which uses HTTPS), or when administrators connect to the vWLAN GUI (which also uses HTTPS). In both cases, when using the default Bluesocket self-signed SSL certificate, users can receive a certificate error from the web browser indicating the certificate was not issued by a trusted CA. This happens because the Bluesocket self-signed certificate is not in the browser's list of trusted root certificate authorities and Bluesocket is not a CA. These errors can be avoided by either installing the self-signed certificate on each client in the browser's list of trusted root CAs, or by installing an SSL certificate (provided by a CA, such as VeriSign) on vWLAN that is already in the client's list of trusted root CAs.

To install new SSL certificates on vWLAN, follow these steps:

1. Begin by generating a certificate signing request (CSR) in vWLAN. Navigate to the **Configuration** tab, select **System > Settings**, and select the **Platform** tab. Select the **Certificate Signature Request 1 (CSR)** item in the list, and then select **Show** at the bottom of the next page that appears. This action will take you to the CSR request form.



2. In the **Certificate 1 Request** form, specify the country name in the appropriate field. Country names are specified using a two letter code (for example, US for United States). Then enter the state or province name without abbreviations (for example, Alabama). Next, enter the locality name (city or town), your organization's name (spelling out symbols or leaving them out), your organizational unit's name (name of the department or organization unit within your organization making the request), and the FQDN (common name) for the certificate. The common name is the host name added to the domain name. For example, if the host name of vWLAN is **wireless**, and the domain name is **adtran.com**, enter **wireless.adtran.com**. If you are purchasing a wildcard certificate to install on multiple vWLAN systems, enter an asterisk instead of the host name, for example, **\*.adtran.com**. Enter an email address of the vWLAN administrator in the **Email Address** field. This address is not part of the certificate and is used to contact you if there is a problem with the CA. Optionally, enter an additional company name in the **An optional company name** field, and specify the key bit length



using the drop-down menu. Keys can be **2048** or **1024** bits in length, although most CAs require a minimum of **2048** bits. Select **Update Platform Setting** once the information has been entered.

The screenshot shows the 'Certificate 1 Request' form in the vWLAN Administrator's Guide. The form is under the 'Administration' tab and contains the following fields:

- Country Name: US (2 letter code)
- State or Province Name: Alabama (Full name)
- Locality Name: Hunsville (e.g. city)
- Organization Name: ADTRAN (e.g. company)
- Organizational Unit Name: Engineering (e.g. section)
- Fully Qualified Domain Name: wireless.adtran.com (e.g. bsc1.yourcompany.com)
- Email Address: joesmith@adtran.com
- An Optional Company Name: (empty)
- Key Bit Length: 2048 (dropdown menu)

The 'Update Platform Setting' button is circled in red.

- The public and private keys for certificate enrollment have been created. The public key, in the form of a CSR, is displayed. This is used for certificate enrollment. The private key is stored locally on the vWLAN (**Configuration** tab, **System** > **Settings**, **Platform** tab, **Certificate Private Key 1**).
- Copy and paste the entire text of the CSR into the appropriate space on your CA's enrollment form. Select **apache mod ssl** or **apache** as the server platform on your CA's enrollment form and complete any remaining steps required by the CA. This completes the CSR request.
- You should back up the private key by downloading it to a safe location. Navigate to the **Configuration** tab, select **System** > **Settings**, select the **Platform** tab, and select **Certificate Private Key 1**. Copy and paste the displayed text into a text editor (such as notepad), and save the file with a .key extension (for example, **privatekey.key**).

The screenshot shows the 'Platform' tab in the vWLAN Administrator's Guide. The table lists various certificates and private keys. The 'Certificate Private Key 1' row is circled in red.

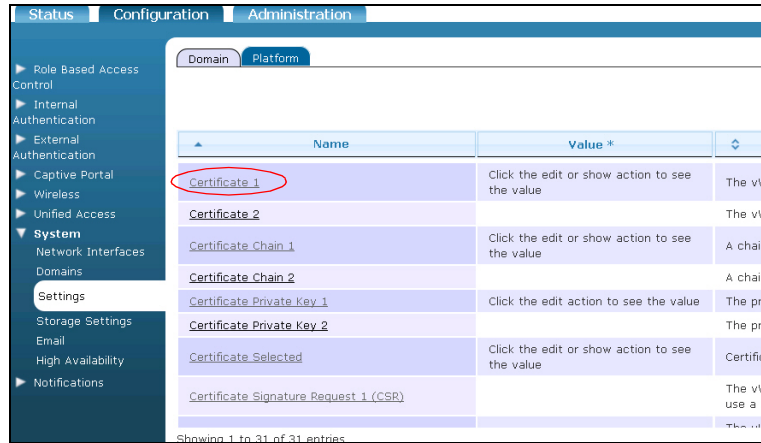
Name	Value *	Hint
Certificate 1	Click the edit or show action to see the value	The vWLAN requires a certificate for Apache+mod_ssl/G
Certificate 2	Click the edit or show action to see the value	The vWLAN requires a certificate for Apache+mod_ssl/G
Certificate Chain 1	Click the edit or show action to see the value	A chain of one or more certificates.
Certificate Chain 2	Click the edit or show action to see the value	A chain of one or more certificates.
Certificate Private Key 1	Click the edit action to see the value	The private key for the cert (closely guard this file).
Certificate Private Key 2	Click the edit action to see the value	The private key for the cert (closely guard this file).
Certificate Selected	Click the edit or show action to see the value	Certificate for current use

- After completing the CSR, the CA will send you the certificate or instructions to obtain the certificate. Some CAs send the certificate in text format, while others may send it in a certificate file with an extension such as .cer, .crt, or .pem. Once you have received the certificate, upload it to vWLAN.
- Repeat these steps for the second CSR.

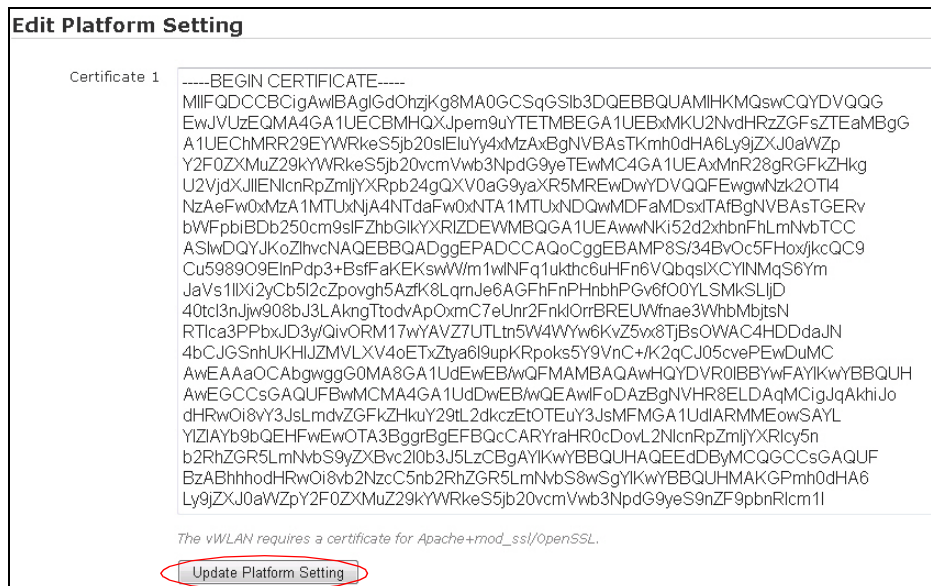
## Uploading Certificates to vWLAN

Certificates are uploaded to vWLAN using the **System > Settings** menu. To upload certificates for vWLAN, follow these steps:

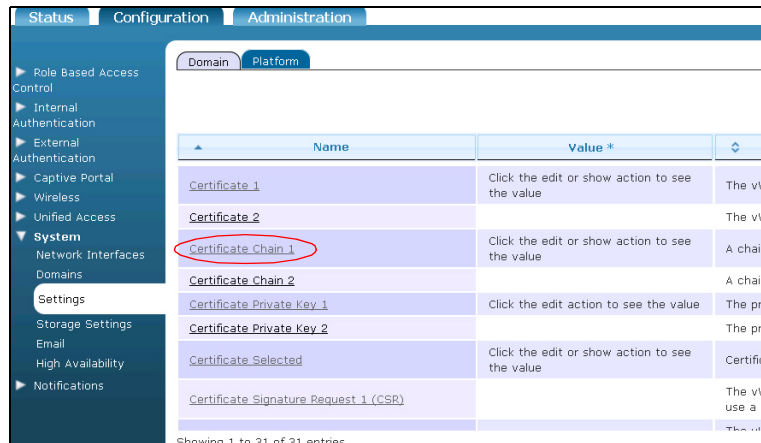
1. Navigate to the **Configuration** tab, select **System > Settings**, and select the **Platform** tab. For a certificate upload, select **Certificate 1** or **Certificate 2** (depending if you are uploading the first or second certificate).



2. Copy and paste the text of the certificate into the **Certificate 1** or **Certificate 2** field. Select **Update Platform Settings** to add the certificate.



3. To add certificate chains using this method, select **Certificate Chain 1** or **Certificate Chain 2** in the **System > Settings** menu.



4. Copy and paste the contents of the certificates received from the CA that will be chained into the **Certificate Chain 1** or **Certificate Chain 2** field. Make sure to include the BEGIN and END tags. Select **Update Platform Setting** to add the certificate chain. Repeat this process for a second certificate chain if necessary.



#### NOTE

*If you have installed a custom web server certificate, and the web server does not start after the custom certificate installation, you can remove the custom certificate using the **certificate cleanup** command. Issuing this command removes the certificate and recovers the system. Refer to [vWLAN Serial Console Configuration on page 181](#) for more information.*

## Configuring Additional vWLAN Settings for Certificates

In addition to installing and uploading certificates to vWLAN, additional items must be configured in vWLAN for proper certificate function. These items include adding a new host record and associated pointer to your organization's DNS server, enabling host name redirection in vWLAN, and allowing outgoing HTTP to the Online Certificate Status Protocol (OCSP) and certificate revocation list (CRL) URLs associated with certificates for the un-registered role. To complete these configuration items, follow these steps:

1. You must add a new host (A) record and an associated pointer (PTR) record using the IP address of the public network interface of the vWLAN system to your organization's DNS server to match the common name (FQDN) you used when generating the CSR. If these do not match, the user can receive a certificate error from the web browser indicating the name on the security certificate is invalid or does not match the name of the site. Once you have verified the names match, test the forward and reverse DNS entry using the **nslookup** command from the command prompt of a client (assuming the client is using the same DNS server as configured on the public network interface of the vWLAN).

- In vWLAN, navigate to the **Configuration** tab, select **System > Settings**, and select **Platform**. In this menu, scroll to and select the **Redirect to hostname** setting. This will allow you to enable host name redirection.

Name	Value *	Hint
Public IP address for vWLAN standalone or high availability master		Only use this if the vWLAN controller is sitting behind a
Read-Only Community String	public	Read-only community string (6-20 characters)
Read-Write Community String	public	Read-write community string (6-20 characters)
Redirect to hostname	Enabled	If the IP of this vWLAN resolves to a hostname (via a PTR record on the DNS server), redirect users to the hostname.
Root CA URL	https://secure.bluesocket.com/root-ca.crt	You must allow HTTP and/or HTTPS to this URL as a Domain Un-registered role in order for clients to be able to access

- Select **Enabled** from the drop-down menu. This will redirect users to the host name (rather than the public network interface IP address). Select **Update Platform Settings**.

### Edit Platform Setting

Redirect To Hostname

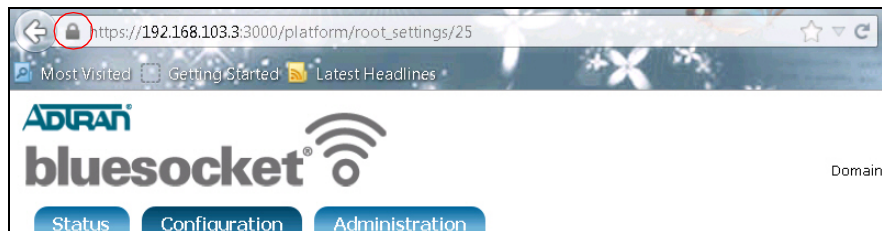
*If the IP of this vWLAN resolves to a hostname (via a PTR record on the DNS server), redirect users to the hostname.*

- Select **Platform Tasks** at the top of the GUI to apply the changes to the vWLAN system. This will take you to the **Administration** tab, **Admin Tasks** menu, and the **Platform** tab. Select the play icon next to **Must restart User Web Server** to restart the web server. Clients will not be able to access captive portal momentarily, but clients who are already connected will not be disconnected.

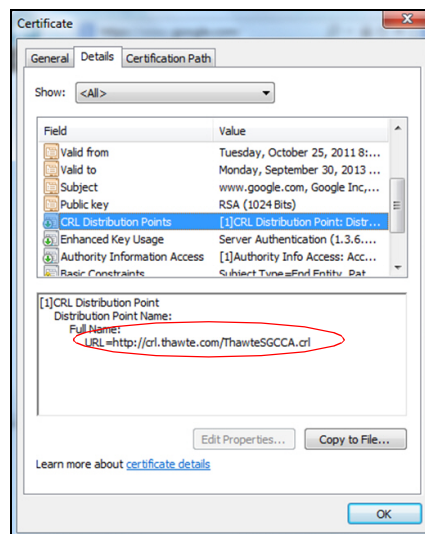
The screenshot shows the Bluesocket vWLAN Administrator's GUI. At the top right, the date and time are 02-27-2014 10:52:20 AM, and the user is root@adtran.com. The navigation tabs are Status, Configuration, and Administration. Under Administration, the Platform Tasks menu is selected and circled in red. The main content area shows a table with columns for Message, Broadcast, and Created Time, but it is currently empty with the message "No Data Available in Table".

- The last configuration task for certificates is to allow outgoing HTTP traffic to the OCSP and CRL URLs associated with the certificate in the un-registered role. These URLs are used to check the validity of the certificate. Some browsers will not redirect to the login page if they cannot validate the certificate. To find the URLs associated with your certificate, select the certificate in the **Configuration** tab **Settings** menu, on the **Platform** tab. Then select **Show** at the bottom of the menu that appears. The OCSP and CRL values are displayed along with other certificate

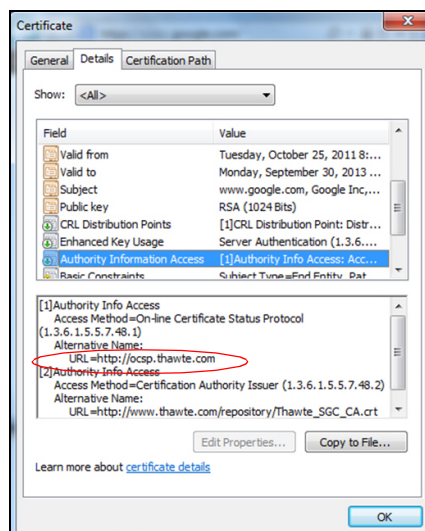
information. Alternatively, select the lock to the right of the address bar in the web browser and select **View Certificates** while on the login page of the vWLAN GUI.



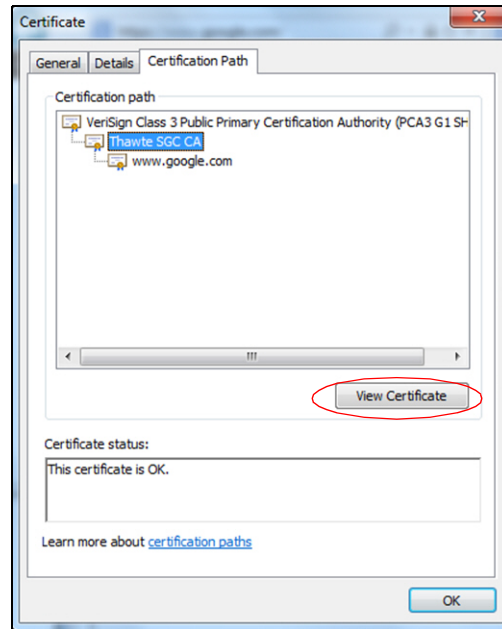
- From the **Certificate** menu, select the **Details** tab and select **CRL Distribution Points** in the **Field** menu. The URL is displayed in the detail pane.



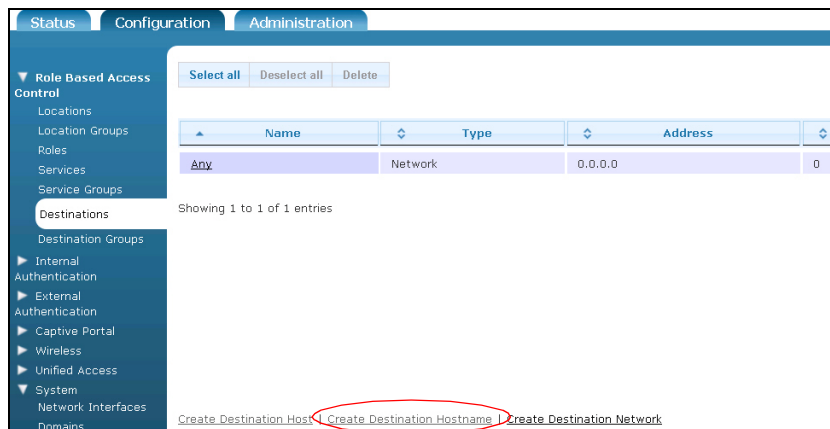
- In the same **Certificate** menu, on the **Details** tab, select **Authority Information Access** in the **Field** menu. The OCSP URL is displayed in the detail pane. Depending on your certificate, you might have one, both, or neither of these fields, but if you do have them, you should allow HTTP traffic to them from the vWLAN (refer to [Configuring Additional vWLAN Settings for Certificates on page 75](#)).



8. Repeat this process for all certificates in the chain. To ensure you have the information for all certificates in the chain, select the **Certification Path** tab in the **Certificate** menu. Select the next certificate up in the certification path and select **View Certificate**. Repeat Steps 6 and 7 for each certificate.



9. Once you have gathered all the URLs for all of the certificates in the chain, navigate to the **Configuration** tab and select **Role Based Access Control > Destinations**. Select **Create Destination Hostname** at the bottom of the menu.



10. In the new menu, specify the name for the destination host name, and enter the URL in the **Address** field. Select **Create Destination**. Repeat this step until all the URLs are added. Wildcards can be used to specify the destination host name. Acceptable formats are **\*.domain.com** or **domain.com**.

**Create Destination - Hostname**

Name

Address

[Back](#)

11. Return to the **Configuration** tab, and select **Role Based Access Control > Roles**. Select the **Un-registered** role. In the role menu, select **Append Firewall Rule**. Specify that the new rule allows outgoing HTTP traffic to the host names created in Steps 9 and 10, and select **Update Role**. Repeat this step until there is a firewall rule in the un-registered role that allows outgoing HTTP traffic for all of the URLs. This configuration can be leveraged for a walled garden network configuration. You must run a domain task to apply this change to the AP (refer to [Administrative Tasks on page 265](#) for more information).

**Edit Role**

Name

**Firewall Rules**

Network traffic is checked against the following policies.

If the service, direction, and destination match, the action is taken and checking ends.

There are several implicit policies that apply to this role (after the configured rules):

- DHCP is allowed to the AP
- DNS is allowed to the DNS servers that the client is given
- Unless previously allowed by a configured rule, HTTP traffic is redirected to the vWLAN. HTTPS traffic will be redirected if enabled under Domain Settings
- HTTP, HTTPS and ICMP are allowed only to the vWLAN

If no rule matches, the traffic is denied.

In most cases, you should not have to configure any firewall rules for the Un-registered role

Policy	Service	Direction	Destination	
<input type="button" value="⊕"/>	Allow	AndersTest	Both Ways	Any

[Show](#) | [Delete](#) | [Create](#) | [Back](#)

## Managing vWLAN Certificate Settings

The vWLAN certificate is used to secure the administrator and user web service. If you have platform administrative privileges, you can manage the vWLAN certificate settings on a platform basis. To manage these settings, follow these steps:

1. Navigate to the **Configuration** tab, and select **System > Settings**. In the **Platform** tab, you will find a summarized list of all the available platform settings that can be configured by the administrator. To

manipulate these settings, select the appropriate setting from the list. This will present certificate request forms, certificate chains, certificates, and certificate private keys.

Name	Value *	Hint
Certificate 1	Click the edit or show action to see the value	The vWLAN requires a certificate for Apache+mod_ssl/Op
Certificate 2		The vWLAN requires a certificate for Apache+mod_ssl/Op
Certificate Chain 1	Click the edit or show action to see the value	A chain of one or more certificates.
Certificate Chain 2		A chain of one or more certificates.
Certificate Private Key 1	Click the edit action to see the value	The private key for the cert (closely guard this file).
Certificate Private Key 2		The private key for the cert (closely guard this file).
Certificate Selected	Click the edit or show action to see the value	Certificate for current use

- In addition, from this menu you can control which certificate vWLAN is currently using. You can have two certificates loaded on vWLAN, which allows you to switch between them when one certificate is about to expire or to have one certificate assigned to each vWLAN system when using high availability. Select **Certificate Selected** to view the current certificate selection and change it if necessary. In the **Certificate Selected** menu, select either **Certificate 1** or **Certificate 2** and select **Update Platform Setting** to change the current certificate. Remember to restart vWLAN to apply the setting change.

**Edit Platform Setting**

SSL Selection

Certificate 1

Certificate 2

*Certificate for current use*

[Show](#) | [Back](#)

- Certificate chains, certificates, and keys can also be deleted from this menu. Select the item you want to delete. In the resulting menu, delete the text from the chain, certificate, or key box and select **Update Platform Settings**.

## Managing LDAP Certificates for vWLAN

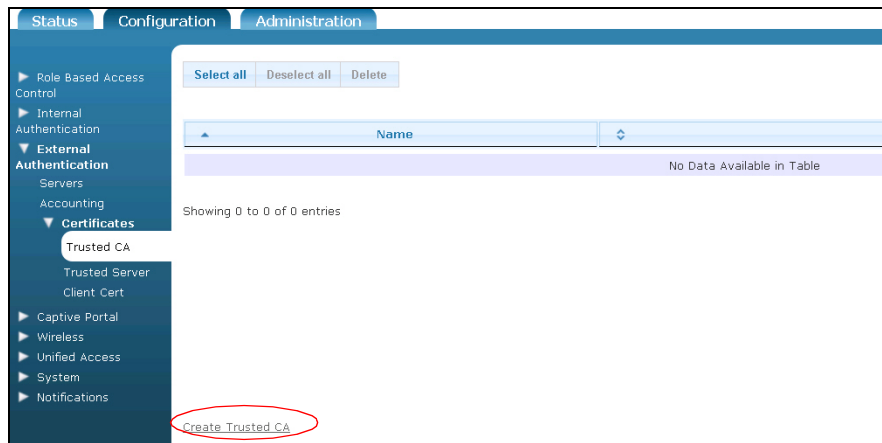
When certificates are manually uploaded to vWLAN, the certificates are then relayed back to the LDAP authentication server in a one-to-many relationship. For example, you can trust more than one CA in a chain, but each LDAP server can only have one trusted server certificate and one client certificate. The client certificate is optional in vWLAN. If a client certificate is not provided, there is no client authentication, and the authentication server must be configured accordingly. Similarly, if no server certificate is provided, then any server certificate is accepted. Each domain has its own group of certificates, but there are no default CA certificates. Instead, the administrator must upload these certificates on a per-domain basis.

To upload a trusted LDAP CA to vWLAN, connect to the GUI and follow these steps:

- Navigate to the **Configuration** tab, and select **External Authentication > External > Certificates > Trusted CA**. Here any previously configured trusted certificates are listed, and the action, name, and



certificate text for each trusted CA is displayed. You can edit an already configured certificate by selecting the certificate from the list. To create a new trusted CA, select **Create Trusted CA** from the bottom of the menu or select **Domain Trusted CA** from the **Create** drop-down menu (at the top of the menu).



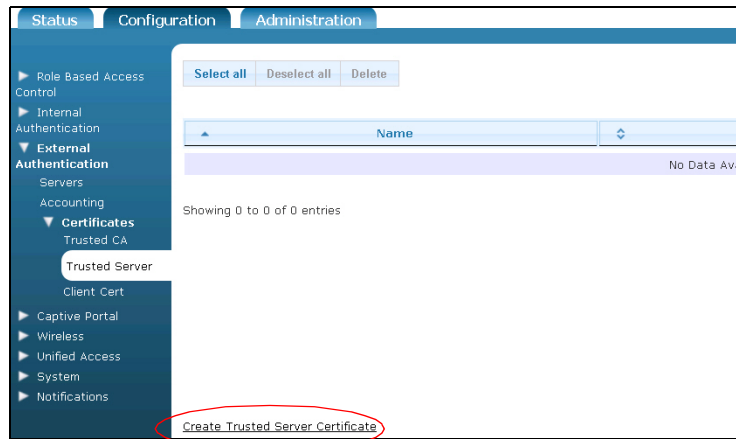
2. Enter the name for the CA in the **Name** field, and enter the CA text in the **Certificate text** field.

3. After entering the appropriate information, select **Create Trusted CA**. The created CA is now available for editing or deletion, and will appear in the Trusted CA list (**Configuration** tab, **External Authentication** > **Certificates** > **Trusted CA**).

To upload a trusted LDAP server certificate to vWLAN, follow these steps:

1. Navigate to the **Configuration** tab, and select **External Authentication** > **Certificates** > **Trusted Server**. Here any previously configured trusted servers are listed, and the action, name, and certificate text for each trusted server is displayed. You can edit an already configured server certificate by selecting the certificate from the list. To create a new trusted server, select **Create**

**Trusted Server Certificate** from the bottom of the menu or select **Domain Trusted Server** from the **Create** drop-down menu (at the top of the menu).



2. Enter the name for the server certificate in the **Name** field, and enter the certificate text in the **Certificate text** field.

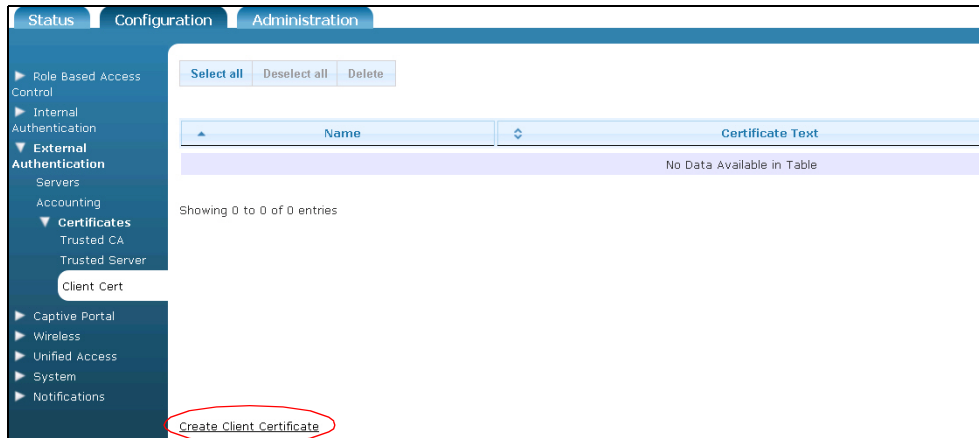
 A screenshot of the 'Create Trusted Server Certificate' form. It has a title bar 'Create Trusted Server Certificate'. Below the title bar, there is a 'Name' field and a 'Certificate Text' field. At the bottom of the form, there is a button labeled 'Create Trusted Server Certificate', which is circled in red.

3. After entering the appropriate information, select **Create Trusted Server Certificate**. The created server certificate is now available for editing or deletion, and will appear in the trusted server list (**Configuration** tab, **External Authentication** > **Certificates** > **Trusted Server**).

To upload a trusted LDAP client certificate to vWLAN, follow these steps:

1. Navigate to the **Configuration** tab, and select **External Authentication** > **Certificates** > **Client Cert**. Here any previously configured client certificates are listed, and the action, name, and certificate text for each client certificate is displayed. You can edit an already configured client certificate by selecting the certificate from the list. To create a new client certificate, select **Create**

**Client Certificate** from the bottom of the menu or select **Domain Client Cert** from the **Create** drop-down menu (at the top of the menu).



2. Enter the name for the certificate in the **Name** field, and enter the certificate text in the **Certificate text** field.

The screenshot shows the 'Create Client Certificate' form. It has a title bar 'Create Client Certificate'. Below the title bar, there are two input fields: 'Name' and 'Certificate Text'. The 'Name' field is a small text box, and the 'Certificate Text' field is a larger text area.

3. Enter the key information for the certificate in the **Key** field.



The image shows a screenshot of a web-based configuration interface. It features a large, empty text input field with the label "Key" in the top-left corner. Below the text field, at the bottom of the form, is a button labeled "Create Client Certificate". This button is highlighted with a red oval.

After entering the appropriate information, select **Create Client Certificate**. The created client certificate is now available for editing or deletion, and will appear in the client certificate list (**Configuration** tab, **External Authentication** > **Certificates** > **Client Cert**). An error is generated if the key and certificate do not match.

## 7. vWLAN Domain Configuration

Domains are separate management domain partitions within the vWLAN instance that are used to subdivide the vWLAN management. Domains are initially created by the platform administrator, and are then assigned a domain administrator. Creating domains includes creating the domain in vWLAN and optionally associating one or more other administrators to the domain. After domains have been created, there are several configuration options available to the domain administrator. These options include setting domain destinations, configuring services and groups within the domain, configuring domain locations, configuring domain roles and users, configuring authentication, performing a backup of the domain configuration, and restarting the domain. These tasks are described in the following sections of this chapter:

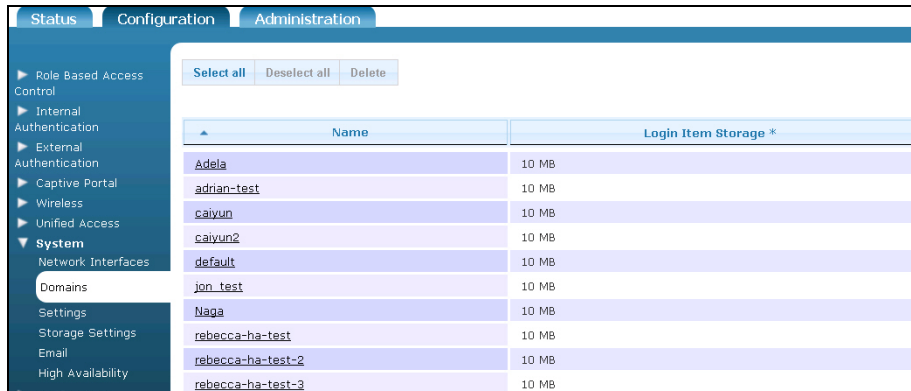
- [Creating the Domain on page 85](#)
- [Associating Administrators to a Domain on page 87](#)
- [Configuring Domain Destinations on page 88](#)
- [Creating Domain Destination Groups on page 90](#)
- [Configuring Domain Services on page 91](#)
- [Creating Domain Service Groups on page 92](#)
- [Configuring Domain Locations on page 94](#)
- [Configuring Domain Location Groups on page 95](#)
- [Configuring Domain Roles on page 96](#)
- [Configuring Domain Role Schedules on page 105](#)
- [Configuring Web-based \(Captive Portal\) Authentication on page 107](#)
- [Configuring Domain Accounting on page 131](#)
- [Configuring Domain Settings on page 133](#)
- [Configuring Domain Users on page 136](#)
- [Configuring Domain Branding on page 138](#)
- [Domain Configuration Backup on page 138](#)

### Creating the Domain

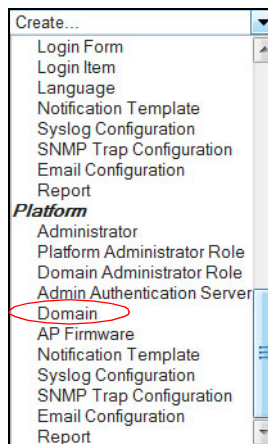
Domains and domain administrators are configured by platform administrators, or administrators with platform read and write permissions. Refer to [Specifying the Administrator's Role on page 47](#) for more information.

To create a domain, follow these steps:

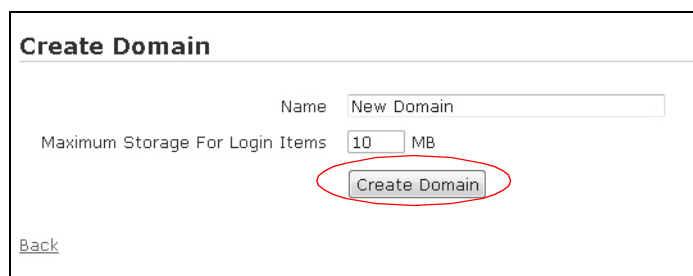
1. Navigate to the **Configuration** tab, **System > Domains**.



2. Or you can select **Platform > Domain** from the **Create** drop-down menu (at the top of the menu).



3. Enter a name for the new domain in the **Name** field and specify the maximum storage space for login items on the domain. Login items are the images and other files used in the login page for the particular domain. Each domain has a certain amount of storage space allotted to it, and this space can be specified as a specific amount of space per domain, per AP associated with the domain, or each domain storage space can be specified individually. Storage settings are set using the **Storage Settings** menu (refer to [Managing Domain Storage Settings on page 255](#) for more information). If the storage setting has been configured as fixed for the domain or per AP, this field cannot be edited. If the storage setting is specified on a per-domain basis, enter the storage limit in the appropriate field.



4. Select **Create Domain**. You will receive confirmation acknowledging the domain has been created.

- Once the domain has been created, you can view, edit, or delete the domain from the **Configuration** tab, **System > Domains** menu.
- Once the domain is created, you can create an administrator for the domain (if one did not already exist, or you want a different administrator), or you can begin configuring the specifics of the domain. Refer to [Creating an Administrator on page 43](#) or [Configuring Domain Destinations on page 88](#) for more information.

## Associating Administrators to a Domain

In addition to a domain administrator, other administrators can be associated with the domain. This association allows other administrators (such as platform administrators) to access, configure, and maintain a given domain.



### NOTE

*You must have platform read and write permissions to be able to associate an administrator with a domain. Refer to [Specifying the Administrator's Role on page 47](#) for more information.*

To associate an administrator with a domain, follow these steps:

- Navigate to the **Administration** tab, and select **Admin Authentication > Administrators**.

username	Source *	UID	Timezone
aaaa@ccc.com	Local Database		Eastern Time (US & Canada)
anders.dahl@adtran.com	Local Database		Eastern Time (US & Canada)
anup.patil@adtran.com	Local Database		Eastern Time (US & Canada)
domainreadonly@adtran.com	Local Database		Eastern Time (US & Canada)
eng	Radius Server	eng@192.168.100.1	GMT
jonathan.emord@adtran.com	Local Database		Eastern Time (US & Canada)

- From the **Administrators** list, select the administrator you want to associate with a domain.

username	Source *	UID
aaaa@ccc.com	Local Database	
anders.dahl@adtran.com	Local Database	
anup.patil@adtran.com	Local Database	
domainreadonly@adtran.com	Local Database	
eng	Radius Server	eng@192.168.100.1
jonathan.emord@adtran.com	Local Database	
liucaiyun@gmail.com	Local Database	
platformfull@adtran.com	Local Database	
platformreadonly@adtran.com	Local Database	
readonly@adtran.com	Local Database	
rebecca@adtran.com	Local Database	

Showing 1 to 14 of 14 entries  
[Create Administrator](#)

- Select the domain you would like to associate with this administrator by selecting the domain from the **Domain** drop-down menu. In addition, make sure to select the appropriate administrator role from the **Admin Role** drop-down menu.

**Edit Administrator**

Email:

Password:

Password Confirmation:

Timezone:

**Administrator Scopes**

Domain	Admin Role	
<input type="text" value="Platform"/>	<input type="text" value="Platform Read-Write Permissions (Full-Access)"/>	<a href="#">remove</a>
<input type="text" value="default"/>	<input type="text" value="Domain Read-Write Permissions (Full-Access)"/>	<a href="#">remove</a>

[Add more domains](#)

- Select **Update Administrator**. A confirmation is displayed when the action is complete.

## Configuring Domain Destinations

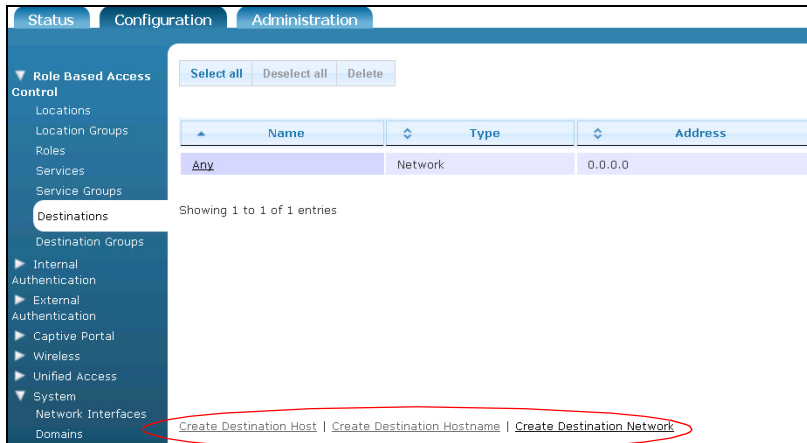
Domain destinations are used to specify which networks are accessible from a single domain. Destination locations can be used to specify which networks are available to roaming clients and users and which are not. When configuring a domain destination, you will specify the destination's host name, IP address, or network mask in the GUI. Destinations can also be grouped, so they use the same network resources (refer to [Creating Domain Destination Groups on page 90](#) for more information). Once a domain is created, you must use a role to allow or deny it. Refer to [Configuring Domain Roles on page 96](#) for more information. To configure a domain destination, follow these steps:



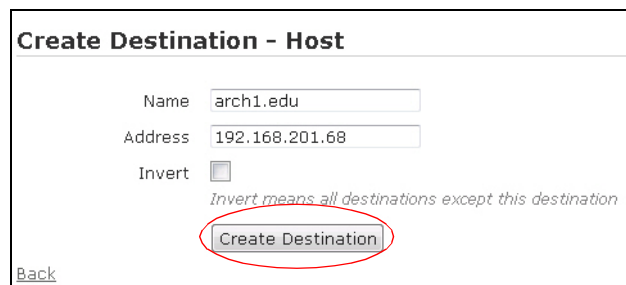
1. Verify that you are in the correct domain's administrative menu by selecting the appropriate domain in the **Domain** drop-down menu.



2. Navigate to the **Configuration** tab, and select **Role Based Access Control > Destinations**.



3. Select **Create Destination Host**, **Create Destination Hostname**, or **Create Destination Network** from the bottom of the **Destinations** menu, or select **Domain Destination Host** from the **Create** drop-down menu (at the top of the menu). You can optionally choose to select **Domain Destination Hostname** or **Domain Destination Network** from the **Create** list to create the same destination.
4. Enter the name of the destination and the destination's IP address in the appropriate fields. The destination's name is expressed in host name format, and must be between 1 and 64 characters in length. You can optionally specify that the destination is inverted, which specifies that all destinations except the one specified are available. If you are creating this destination from the **Destination Hostname** selection, you will be prompted for the same information in the **New Hostname** menu. In order to create a network area that only allows certain URLs through the AP firewall without requiring authentication, the **Destination Hostname** selection can only be used in an un-registered role. If you are creating this destination from the **Destination Network** selection, you will also be asked to enter the network mask for the destination in the **New Network** menu. Inverting the destination means that the destination is the opposite in the firewall rule. For example, if you allowed all traffic to an inverted destination, then all traffic is allowed to everything but this destination.

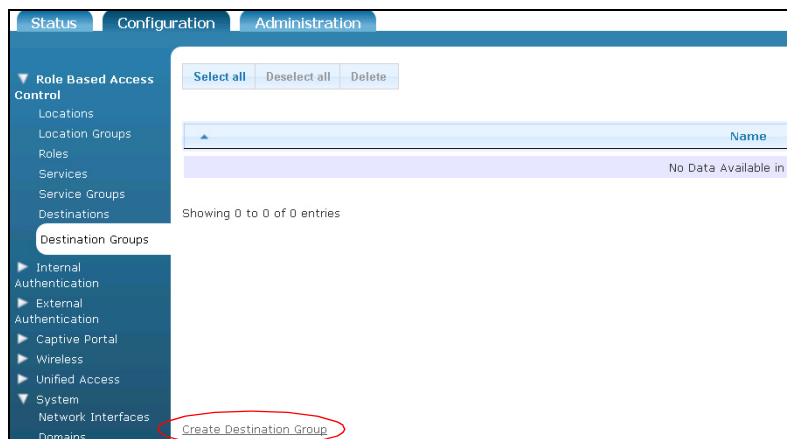


5. Select **Create Destination**. A confirmation is displayed indicating the destination has been created. The new destination will now appear in the list of destinations displayed in the **Configuration** tab **Role Based Access Control > Destinations** menu, where you can choose to display, edit, or delete the destination.
6. Once you have created the destination, associate it with a role so that it can be accessed. Refer to [Configuring Domain Roles on page 96](#).

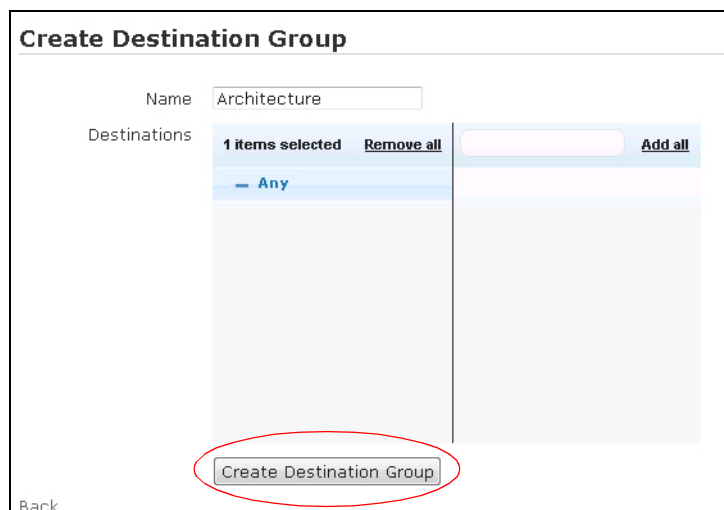
## Creating Domain Destination Groups

A domain destination group is a collection of domain destinations, that can be applied to firewall rules for a role in one step. To configure a domain destination group, follow these steps:

1. Navigate to the **Configuration** tab, and select **Role Based Access Control > Destination Groups**. Any previously configured destination groups will be listed in the menu. If you want to edit a previously created destination group, select the group name from the list. To create a new destination group, either select **Create Destination Group** at the bottom of this menu, or select **Platform Destination Group** from the **Create** drop-down menu (at the top of the menu).



2. Specify the name of the destination group, and select which destinations to add to the group from the list.



3. Select **Create Destination Group**. A confirmation is displayed indicating that the group has been created. The group will now appear in the group list (**Configuration** tab, **Role Based Access Control** > **Destination Groups**), where you can display, edit, or delete the group.
4. Once you have created the destination group, associate it with a role so that it can be accessed. Refer to [Configuring Domain Roles on page 96](#) for more information.

## Configuring Domain Services

Domain services are the services, protocols, and ports used by the domain. Typical domain services include DHCP, DHCP servers, DNS, HTTP, HTTPS, ICMP, etc. Services, like destinations, can also be grouped, which makes it easier to assign a set of services to a user role. Configured domain services are listed in the **Configuration** tab, **Role Based Access Control** > **Services** menu in the GUI.

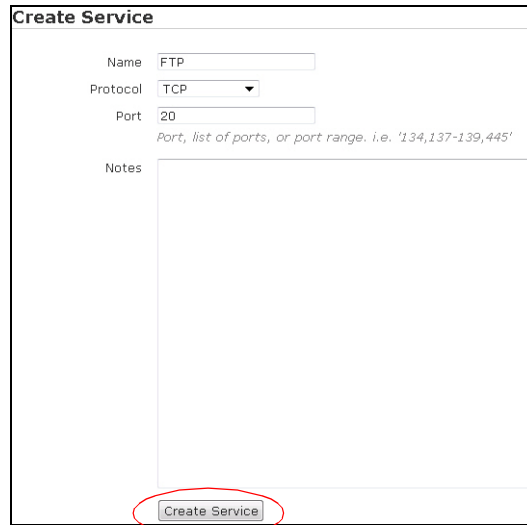
To configure a domain service, follow these steps:

1. Navigate to the **Configuration** tab and select **Role Based Access Control** > **Services**.

Name	Port
Any	0
DHCP	67
DHCP-Server	68
DNS	53
HTTP	80
HTTPS	443
ICMP	0
IMAP	143
KERBEROS	88
LDAP	389
MS-DATA	135

2. To edit a service, select the service from the list.
3. To create a new service, select **Create Service** at the bottom of the **Services** menu, or select **Domain Service** from the **Create** drop-down menu (at the top of the menu).
4. Enter the name of the service in the required field, and select the appropriate protocol from the **Protocol** drop-down menu. Depending on the protocol type selected, you will be prompted for the

port, or list of ports, used by this service. You can optionally add any notes about this service that you would like to be displayed in the configured services list.



**Create Service**

Name

Protocol

Port   
Port, list of ports, or port range. i.e. '134,137-139,445'

Notes

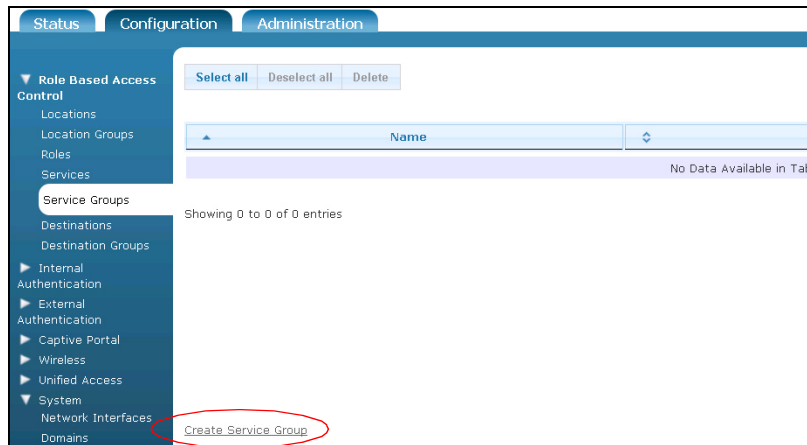
5. Select **Create Service**. A confirmation appears indicating the service has been created. The service will now appear in the list of configured services (**Configuration** tab, **Role Based Access Control > Services**) and can be displayed, edited, or deleted.
6. Once you have created the domain service, associate it with a role. Refer to [Configuring Domain Roles on page 96](#) for more information.

## Creating Domain Service Groups

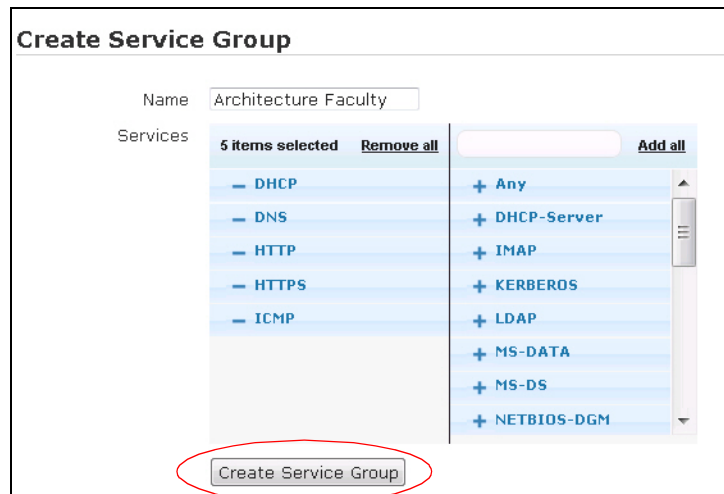
A domain service group is a collection of domain services, that can be applied to users or roles in one step. To configure a domain service group, follow these steps:

1. Navigate to the **Configuration** tab, and select **Role Based Access Control > Service Groups**. Any previously configured service groups will be listed in the menu. If you want to edit a previously created service group, select the group name from the list. To create a new service group, either

select **Create Service Group** at the bottom of this menu, or select **Domain Service Group** from the **Create** drop-down menu (at the top of the menu).



- Specify the name of the service group in the appropriate field, and select which services to include in the group by selecting the **+** (plus) sign next to the service.



- Select **Create Service Group**. A confirmation is displayed indicating that the group has been created. The group will now appear in the group list (**Configuration** tab, **Role Based Access Control** > **Service Groups**), where you can display, edit, or delete the group.
- Once you have created the service group, apply it to a role. Refer to [Configuring Domain Roles on page 96](#) for more information.

## Configuring Domain Locations

Domain locations are network locations for the domain. Locations are defined as the subnet, network mask, and VLAN ID associated with the domain. The NAC domain location is used for web-based authentication by allowing an AP to act as a temporary DHCP server and dispense temporary IP addresses to clients trying to connect to the network. The NAC subnet must not overlap with any other networks in the domain, and it can be edited to any class A, B, or C private network with a /14 subnet mask. When a user connects to vWLAN, the user's location (VLAN, subnet, network mask) is determined by the user role, which encompasses the AP's native VLAN/location, a static location, or a location group.

A user's location is determined by the user's role. Domain administrators can specify a VLAN ID and subnet, and the system automatically determines the APs that support that location. Managing locations is the same as managing the IP addressing of connecting clients, and can be handled in three main strategies: strict location, which bases the location on the user's role and identity; location groups, which base the location on user roles and identities; and default location, which bases locations on APs.

Strict location configuration means that a user role is configured for each specific location (VLAN ID and subnet), and when a user with the configured role connects, they will always be associated with the same location. In this scenario, APs will tunnel traffic to that location if necessary. For example, a guest user could receive a 172.16.0.0/24 location, regardless of the AP to which they connect. Location groups are used in large scale deployments in which multiple subnets can be assigned to the same user role. In this scenario, the vWLAN system optimally assigns the user to the local location, eliminating the need to trunk the same VLANs across multiple sites. The native AP VLAN location is used when a user is placed onto the AP's local network with no VLAN tag. This is useful if you want to distribute data to the network edge, and do not need to place users into specific networks based on their identity. In this scenario, if a user roams to another location, the traffic is tunneled back to the originating location to maintain IP addressing.

When locations are defined, the VLAN ID plus the subnet and network masks must match, or the location is deemed as not unique and therefore considered a different location. When vWLAN learns about a location, if it doesn't already exist, the vWLAN creates a location in the GUI. User roles can be mapped to specific locations. When the system automatically creates a new location, it will have a VLAN of 0 and a name starting with **vLoc** to signify that the location was created by vWLAN.

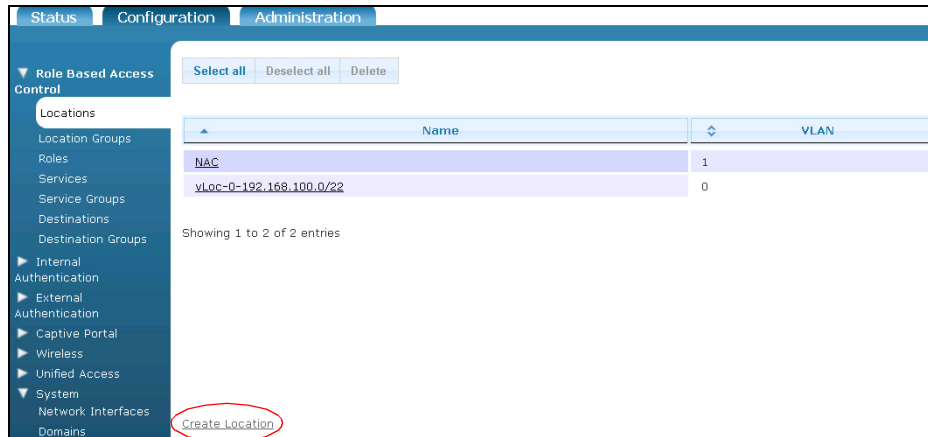
When the AP boots for the first time, it discovers its native subnet. If there is already a location in the GUI, the AP is associated to the location with a non-tagged VLAN. If a native location with a VLAN tag is configured on the AP, the AP reports its native location with the configured native VLAN tag. APs automatically ensure untagging and tagging of packets from clients on the same native location. In addition, APs automatically discover which tagged VLANs it can access by sending out DHCP requests to the configured VLANs on vWLAN. If an IP address is obtained on a VLAN, then that location is deemed active for the AP, and the DHCP address is released.

When a new location is specified in the vWLAN system, the vWLAN asks the APs to discover that VLAN. If the VLAN is found, then the location becomes active and clients can use it. If the VLAN is not found, clients attempting to access the network are held without a network address until the location becomes active.

If APs are moved to a different trunk or access port, the AP should be deleted or be returned to a native location of **Native AP Location** and rebooted, so that it will rediscover any available locations.

Domain locations are configured from the **Configuration** tab. To create a domain location, follow these steps:

1. Navigate to the **Configuration** tab, and select **Role Based Access Control > Locations**. Any previously configured locations will be listed in the menu. If you want to edit a previously created location, select the location name from the list. To create a new location, either select **Create Location** at the bottom of this menu, or select **Domain Location** from the **Create** drop-down menu (at the top of the menu).



2. Enter the name of the location and its associated VLAN in the appropriate fields. Then enter the classless interdomain route (CIDR) for the location, which is the location's subnet and network mask.

### Create Location

Name:

VLAN ID:

CIDR:

CIDR is the subnet/netmask(bits) of the location like 192.168.100.0/24.

[Back](#)

3. Select **Create Location**. A confirmation is displayed indicating that the location has been created. The location will now appear in the locations list (**Configuration** tab, **Role Based Access Control > Locations**), where you can display, edit, or delete the location.

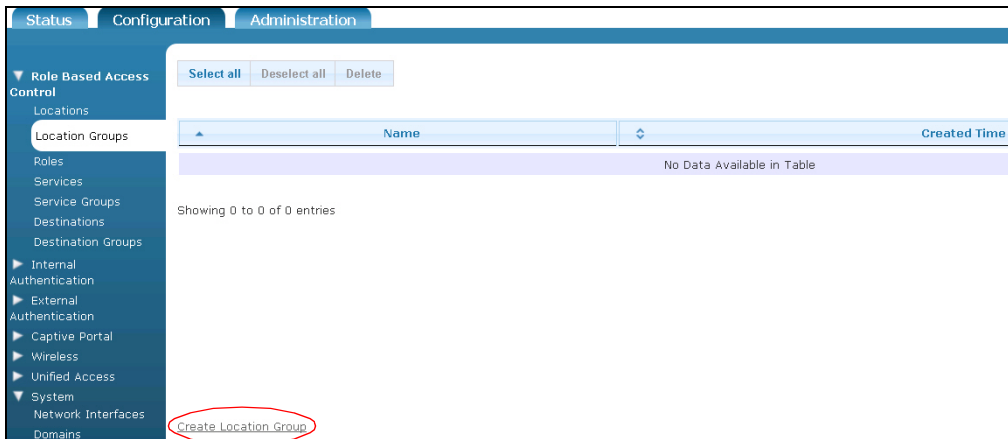
## Configuring Domain Location Groups

In large scale deployments of vWLAN, multiple subnets can be assigned to the same user role using location groups. When location groups are used, the system optimally assigns the users to the local location, which eliminates the need to trunk the same VLANs across multiple sites.

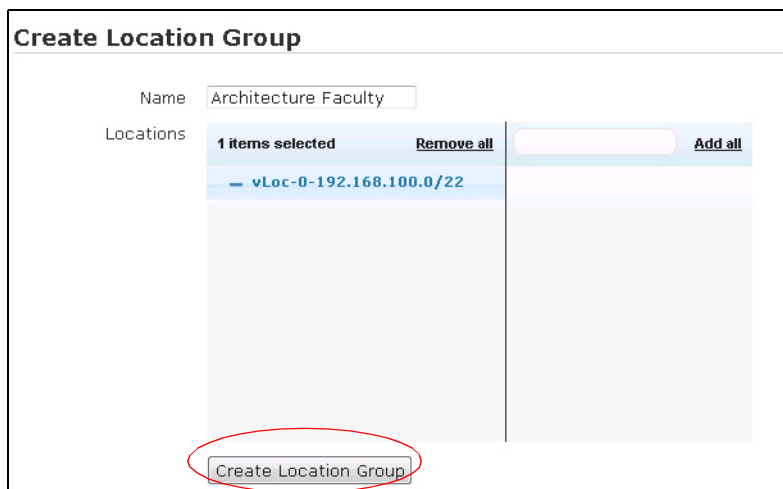
To create a domain location group, follow these steps:

1. Navigate to the **Configuration** tab, and select **Role Based Access Control > Location Groups**. Any previously configured location groups will be listed in the menu. If you want to edit a previously

created location group, select the group name from the list. To create a new location group, either select **Create Location Group** at the bottom of this menu, or select **Domain Location Group** from the **Create** drop-down menu (at the top of the menu).



2. Enter the name of the location group, and select the locations to be associated with the location group. Then, select **Create Location Group**.



3. A confirmation is displayed indicating that the group has been created. The group will now appear in the group list (**Configuration** tab, **Role Based Access Control** > **Locations**), where you can display, edit, or delete the group.

## Configuring Domain Roles

Domain roles are the roles of users that are connected to a specific domain, and include such features as firewall behavior, location elements, QoS settings, and CoS settings. User roles in vWLAN define the policy enforced per user at the AP before forwarding user traffic, based on traffic flow (location, firewall policies), bandwidth management, and packet marking and prioritization.

The role in which a user is placed is determined by the following items (in order):

1. Layer 7 device fingerprint (device type and operating system)



2. 802.1x (RADIUS, LDAP/AD)
3. MAC authentication
4. Wildcard MAC authentication
5. RADIUS MAC authentication
6. The default role from the SSID, unless the SSID is 802.1X, then the role from the RADIUS 1X server is used.
7. If the role remains un-registered at this point, the user can use web-based authentication to log in to any role.

By default, when a user connects for the first time and has not been authenticated, the user's role is un-registered.

When configuring a user role, it is important to realize that the user role determines where and how the client's traffic flows. You must specify the name of a user role, the location associated with the role, the CoS settings for the role, the bandwidth shaping parameters for the role, post-login redirection parameters, the firewall policies applied to the role, and the device rules applied to the role (Layer 7 fingerprint). By default, two roles already exist: **Un-registered** (which cannot be deleted) and **Guest**.

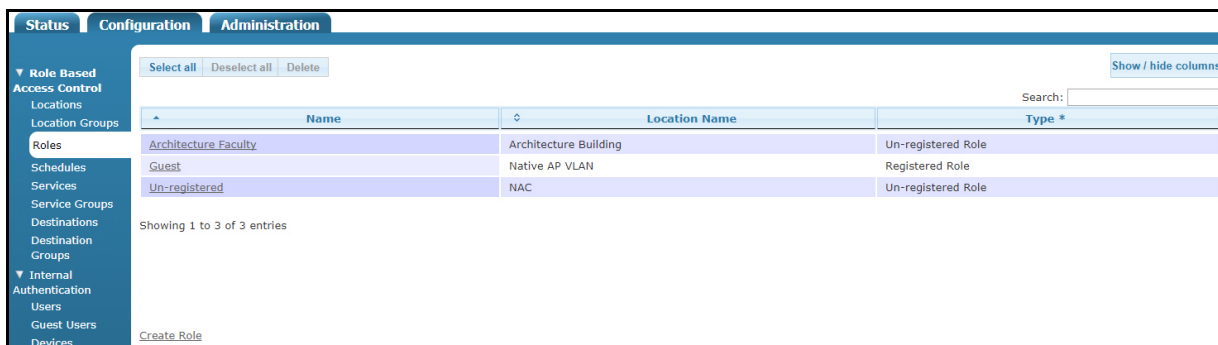


#### NOTE

*There can be interactions between a tunnel profile and a defined user role. Refer to [Configuring a Tunnel Profile on page 198](#) for more information.*

The following steps will guide you through creating un-registered and registered roles:

1. Navigate to the **Configuration** tab, and select **Role Based Access Control > Roles**. Any previously configured domain roles will be listed in the menu. If you want to edit a previously created domain role, select the role name from the list. To create a new domain role, either select **Create Role** at the bottom of this menu, or select **Domain Role** from the **Create** drop-down menu (at the top of the menu).



The Create Role page is displayed. The configuration options on this page will change depending on whether the role type selected is **Un-registered** or **Registered**.

## Un-Registered Role Type

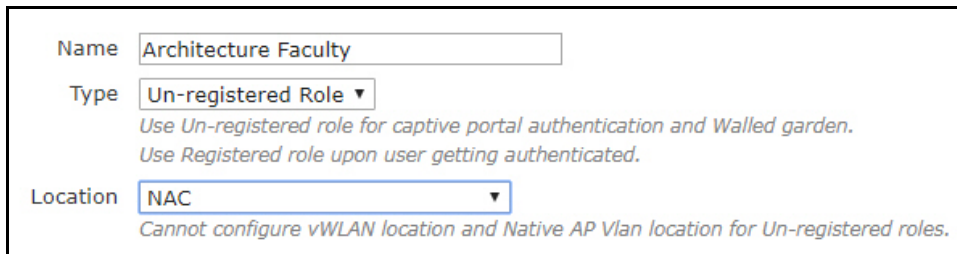
The un-registered role type can be configured two different ways: with the selected location as the Native AP VLAN (NAC address) or a non NAC server location, which is used when configuring the Walled Garden feature.

### NAC Location

When selected, the NAC location option redirects a client's Internet traffic to vWLAN for authentication. While in the un-registered role, the AP serves the client a temporary DHCP address (NAC address). After authentication, as the client transitions out of the un-registered role, the AP locally switches the traffic and the client receives a different DHCP address from the network.

The following steps are used to configure NAC address assignment:

1. Create an un-registered domain role and select **NAC** for the location



The screenshot shows a configuration form for a domain role. The 'Name' field is 'Architecture Faculty'. The 'Type' dropdown is set to 'Un-registered Role'. Below this, there is a note: 'Use Un-registered role for captive portal authentication and Walled garden. Use Registered role upon user getting authenticated.' The 'Location' dropdown is set to 'NAC'. Below this, there is a note: 'Cannot configure vWLAN location and Native AP Vlan location for Un-registered roles.'

Specify any firewall rules needed, however, in most cases you should not have to configure any firewall rules when the location is the NAC.

2. Create an SSID, enable captive portal, and select the name of the un-registered domain role created in Step 1 above.

### Walled Garden

As of vWLAN release 3.1.0, an option was added to captive portal that allows the client to keep the same IP address when transitioning out of an un-registered role to a registered role (Walled Garden).

The following steps are used to configure the Walled Garden feature:

1. Configure the location of the network that will serve the IP addresses. See [Configuring Domain Locations on page 94](#).

2. Create a domain role and specify **Un-registered Role** for the *Type* and select the name of the domain that you created in Step 1 above for the *Location*.

Name

Type **Un-registered Role**  
*Use Un-registered role for captive portal authentication and Walled garden.  
 Use Registered role upon user getting authenticated.*

Location **Architecture Building**  
**Locations**  
 NAC  
 Secure Wireless Connections  
**Architecture Building**  
**LocationGroups**

Add a firewall rule that allows DNS traffic outbound.

**Firewall Rules**

Network traffic is checked against the following policies.  
 If the service, direction, and destination match, the action is taken and checking ends.  
 There are several implicit policies that apply to this role (after the configured rules):  
 DHCP is allowed to the AP  
 DNS is allowed to the DNS servers that the client is given  
 Unless previously allowed by a configured rule, HTTP traffic is redirected to the vWLAN. HTTPS traffic will be redirected if enabled under Domain Settings  
 HTTP, HTTPS and ICMP are allowed only to the vWLAN  
 If no rule matches, the traffic is denied.  
 In most cases, you should not have to configure any firewall rules for the Un-registered role

Policy	Service	Direction	Destination
Allow	DNS	Outgoing	Any
Allow		Outgoing	
Allow		Outgoing	
Allow		Outgoing	
Allow		Outgoing	

Append Firewall Rule  
 Create Role

3. Create another domain role and specify **Registered Role** for the *Type* and select the name of the domain that you created in Step 1 above for the *Location*.

**Create Role**

Name

Type **Registered Role**  
*Use Un-registered role for captive portal authentication and Walled garden.  
 Use Registered role upon user getting authenticated.*

Schedule

Location **Architecture Building**

**NOTE**

*It is important that the domain location of the registered role to be the same domain location as the un-registered role for the Walled Garden feature to work properly.*

4. Create an SSID, enable captive portal, and select the name of the domain role created in Step 2 above. For information on configuring additional SSID options, see [Configuring an SSID on page 188](#).

**Create SSID**

Name/ESSID

Broadcast SSID

Enable Captive Portal Authentication

Un-registered Role

## Registered Role Type

The registered role type specifies the parameters for a client after they have been authenticated. The following steps outline the options available when configuring a registered role:

1. Begin by entering the name of the role in the appropriate field. Select **Registered Role** from the drop-down menu for the role *Type*. If applicable, select any associated schedule from the *Schedule* drop-down menu. The schedule specifies when clients can or cannot access the network. Refer to [Configuring Domain Role Schedules on page 105](#) for more information about schedule configuration. Also select the location associated with this role from the *Location* drop-down menu.

**Create Role**

Name

Type

Use Un-registered role for captive portal authentication and Walled garden.  
Use Registered role upon user getting authenticated.

Schedule

Location

2. Next specify whether 802.1X machine authentication will be enforced on the role. Machine authentication, or computer authentication, allows the domain machine or computer to authenticate before the user logs in when using a host name or machine name as the user name and the computer's domain machine account password as the password. Enabling this feature means that users who do not directly progress from machine authentication to user authentication are placed in the un-registered role, and allows group policies to be applied and login scripts to execute when the user logs in as well as allows users who do not have locally cached profiles on the domain computer to login. A valid 802.1X user without a valid device can also be placed in a role other than un-registered (for example, the guest role) to allow a user to use smart phones and other devices that cannot access the domain. When this feature is enabled, the vWLAN system will only allow the user to be placed in a role as long as valid machine authentication occurred. vWLAN can be configured to remember machine authentication (using the **Memory interval** field), that keeps devices that time out and then reconnect from being left in an un-registered role. Enable the feature by selecting the **Machine authentication enforcement** check box. Once you have enabled this feature, you will specify the role into which users are placed when authenticating, the role in which users are placed if their authentication fails, and the number of days the vWLAN will remember the machine authentication. Select these 802.1X authentication values from the appropriate drop-down menu.

Machine Authentication Enforcement	<input checked="" type="checkbox"/>
Prerequisite Role	Guest <small>Requires the user to be in this prerequisite role before being allowed to authenticate into this role. Applies only to 802.1x Authentication.</small>
Failed Role	Un-registered <small>Role the user is placed in if the user is NOT in the above prerequisite role before authenticating into this role. Applies only to 802.1x Authentication.</small>
Memory Interval	None <small>The number of days that vWLAN will remember a client machine authentication. Applies only to 802.1x Authentication.</small>

- Specify whether client-to-client traffic will be allowed on the AP by selecting the **Allow client to client** check box. Note that the firewall policy must also allow the traffic for client-to-client traffic to flow.

Allow Client To Client	<input type="checkbox"/>	<small>Allows Client to Client traffic on the same AP.</small>
------------------------	--------------------------	--

- Next, configure the CoS options. Specify the over-the-air fairness policy and packet prioritization parameters for the role.



#### NOTE

*Over-the-air-fairness only applies to 1800 Series APs. If you are using an ADTRAN Bluesocket 1900, 2000, or 3000 Series AP, any over-the-air fairness setting will be treated as **No Bias**.*

Over-the-air fairness is used in 1800 Series APs to deprioritize traffic for clients in a specific role, giving clients in other roles better wireless performance. For example, traffic can be deprioritized for guest roles, allowing corporate users more airtime to send wireless traffic, improving their performance in a congested RF environment. Select the over-the-air fairness type from the drop-down menu. Each new user role is set to **No Bias** by default.

The CoS priority override parameters specify on what criteria this user role's traffic is prioritized for incoming (wireless) traffic and how packets are remarked in outgoing (wired) traffic. It can be useful to prioritize wireless traffic to certain roles, such as IP phone roles. The AP can prioritize based on the input wired packet CoS tags (either DSCP or 802.1p or the greater of the two) or a static value.

- DSCP:** prioritization of traffic within the Ethernet and wireless driver based on the IP packet's DSCP code. DSCP stands for DiffServ (DS: Differentiated Service) Code Point and is specified in RFC 2474. Its value ranges from 0 to 63 where 63 has the highest priority. For example, the Wi-Fi driver supports DSCP prioritization to push packets with a specific dscp value to be pushed on to a specific TID (for Incoming traffic). TID is extracted from DSCP/QoS information in 802.11 QoS/IPv4/v6 headers (for Outgoing traffic). TID stands for Type Identification and generally corresponds to IP Precedence Value, and it is defined in RFC 791 with a value range from 0 to 7. Value 7 is the highest priority and meant for network control packets.
- 802.1p:** prioritization of traffic within the Ethernet and wireless driver based on the 802.1p code. This IEEE 802.1p signaling standard defines traffic prioritization at Layer 2 of the OSI model. It is used to prioritize packets as they traverse a network segment (subnet). A packet marked for higher priority receives preferential treatment at the congested subnet. On Ethernet network, 802.1p priority markings are carried in VLAN tags. The priority value ranges from 0 to 7 as the TID.
- Highest Priority (DSCP or 802.1p):** prioritization of traffic within the Ethernet and wireless driver based on the highest priority from DSCP and 802.1p code.

- **Static Value:** prioritization of traffic within the Ethernet and wireless driver based on the network administrator assigned fix value for both DSCP code and 802.1p code.

To specify the prioritization of the input wired packets for the user's role, select the appropriate value from the **CoS priority in override** drop-down menu.

**Class of Service**

Over The Air Fairness  De-prioritize traffic for clients in the role. This will give clients in other roles better wireless performance. Only applies to 1800 Series APs.

CoS Priority In Override  What to prioritize Wireless based on.

CoS Priority Out Override  What to remark Wired based on.

If you specify a **Static** value, you will be prompted to enter the value. Then select the appropriate priority from the **CoS Priority In** drop-down menu.

CoS Priority In Override  What to prioritize Wireless based on.

CoS Priority In

Next, specify the CoS packet remarking behavior for the user role. Packet remarking is applied by the AP in the outgoing/upstream (wireless to wired) direction. Remarking can be beneficial when the upstream network switches or routers are CoS aware of 802.1p or DSCP. 802.1p uses the VLAN header to apply a priority on a frame (priority ranges from 0 to 7, with 7 as the highest priority), and DSCP uses the IP header of the packet to apply a priority on the packet (priority ranges from 0 to 63, with 63 as the highest priority). 802.11 frames contain an application-based packet prioritization. The AP normally converts the WMM prioritization to a packet marking using 802.1p, DSCP, or both. Alternatively, the AP can set a static 802.1p or DSCP mark for all traffic in the role. To set the packet remarking parameters for the user role, select the appropriate value from the **CoS priority out override** drop-down menu. By default, this value is set to **No Remark**. If you specify a **Static** value, you will be prompted to enter the **CoS Priority Out** value. Select the appropriate priority from the **CoS Priority Out** drop-down menu.

CoS Priority Out Override  What to remark Wired based on.

CoS Priority Out



#### NOTE

*The **CoS Priority In** and **CoS Priority Out** drop-down menus are only available if you have selected **Static** for the **CoS Priority In Override** or **CoS Priority Out Override** values.*

5. After specifying the CoS parameters for the user role, you will specify the QoS parameters for the role by defining the bandwidth shaping rules. Using this type of traffic shaping allows you to specify the desired bandwidth granularity, using Kbps, KBps, Mbps, and MBps. In addition, it provides scalability while remaining agile, and allows the policy to follow a user even when they move to a different AP. Bandwidth can be limited on a per-user basis, preventing one user from overusing the

wireless media and wide area network (WAN) uplink, limited in the downstream (to the client) direction, limiting downloads from the Internet, and bandwidth can be limited in the upstream (from the client) direction, preventing clients from running abusive servers or becoming expensive upload endpoints. Upstream and downstream bandwidths can differ, and thus can be tailored to the customer.

**Bandwidth Shaping**

QoS Rate In  Kbits/second ▼  
*Bandwidth Limit in Incoming/Downstream (AP to Client) direction. Set to zero for no bandwidth limit.*

QoS Rate Out  Kbits/second ▼  
*Bandwidth Limit in Outgoing/Upstream (Client to AP) direction. Set to zero for no bandwidth limit.*



#### NOTE

*Any bandwidth value higher than 65535 Kbps (or the equivalent) is treated as 65535 Kbps by the AP, even though the system allows the bandwidth to be set at higher values. The only exception is if no limit (0) is specified, then no limit is enforced.*

To specify the bandwidth parameters for incoming (downstream) traffic, enter the bandwidth limit in the **QoS rate in** field, and specify the measurement type from the drop-down menu. By default, each role bandwidth limit is **0 Kbits/second**, indicating no bandwidth limit is enforced.

QoS Rate In  Kbits/second ▼  
*Bandwidth Limit in Incoming/Downstream (AP to Client) direction. Set to zero for no bandwidth limit.*

Next, specify the bandwidth parameters for outgoing (upstream) traffic by entering the bandwidth limit in the **QoS rate out** field, and specify the measurement type from the drop-down menu. By default, each role bandwidth limit is **0 Kbits/second**, indicating no bandwidth limit is enforced.

QoS Rate Out  Kbits/second ▼  
*Bandwidth Limit in Outgoing/Upstream (Client to AP) direction. Set to zero for no bandwidth limit.*

- After specifying the bandwidth parameters for the user role, you can specify the **Post Login Redirection** parameters for the role. These parameters are displayed to a user after successfully logging in using web-based authentication (captive portal). By default, a thank you message appears to each authenticated user. You change this message, and the redirection page, by entering text in the **Thank you HTML** field or a URL in the **URL Redirect** field. Entering a URL here overrides the user's original URL and the Post Login Redirect URL (you can view the Post Login Redirect URL by navigating to the **Configuration** tab and selecting **System > Settings**).

**Post Login Redirection**

Thank You HTML   
*If HTML text is entered here, it will be displayed after a user has logged in on the thank-you page. The user will not be automatically redirected.*

URL Redirect   
*URL to redirect after login. This value overrides the default URL found under settings.*

- Next, configure the firewall rules for the user role. vWLAN provides a full Layer 3 and Layer 4 stateful firewall at the AP. The firewall is configured by the domain administrator, who creates one or more policies within each role. For a given traffic flow, these policies are applied in order. The vWLAN firewall is an inclusive firewall, meaning the last policy is a **deny all** policy by default. When configuring the firewall, you need to make sure DHCP is allowed outbound from the client, and that the DHCP server is allowed inbound to the client, or specify that **Any** are allowed both directions.

The firewall rules operate by checking network traffic against the configured policies. If the service, direction and destination of the traffic match the policy, then the action is taken and traffic checking ends. If no policy matches, then traffic is denied. If there are no policies configured, then all traffic is denied. Policy matches are attempted in order, so make sure to arrange the policies as needed for your network (using the **[drag]** option to reposition a policy). Enter the action (**deny** or **allow**), the service or group to which to apply the policy, the traffic direction (**Incoming** or **Outgoing**), and the traffic's destination network in the appropriate fields using the drop-down menus. You can delete a policy by selecting **remove** next to the policy.

**Firewall Rules**

Network traffic is checked against the following policies.

If the service, direction, and destination match, the action is taken and checking ends.

If no rule matches, then the traffic is denied.

If there are no policies configured, then all traffic is denied.

**By default, there is an implicit deny any at the end of the policies. Any traffic that is not explicitly allowed by the admin will be blocked.**

**For a client to get an IP address - DHCP (or all traffic) must be allowed outgoing, and DHCP server (or all traffic) must be allowed incoming.**

Policy	Service	Direction	Destination		
+	Allow	DHCP	Outgoing	Any	
+	Allow	DHCP-Server	Incoming	Any	
+	Allow		Outgoing		
+	Allow		Outgoing		
+	Allow		Outgoing		

Append Firewall Rule

Create Role

**i** **NOTE**

*For highest client throughput or performance (for testing bandwidth, etc.), configure the role with no bandwidth limitation (0), and configure only a single firewall rule (set the rule to **allow any bothways any**). In this configuration, the AP firewall is bypassed, allowing for the highest client throughput.*

- Next, configure the device rules for the role. These rules specify the role a detected device is to use, based on the device's fingerprint. The fingerprint includes the device's type and ownership (corporate or other). The device is placed in the role specified in the **Destination Role** drop-down menu when the device is detected on the vWLAN network. This role overrides all other role



specifications (including those specified in SSID, MAC, RADIUS, and web authentication methods). Use the drop-down menus to specify the device's type, ownership, and destination role.

**Device Reassignment Rules**

The client's initial role is determined based on authentication but clients can immediately be reassigned to another destination role based on the Device Type, Ownership and Destination Role configured in the rules below. For example if Device Type is iPhone and Ownership is Corporate then role is Corporate

Final role will be determined based on the following rules.  
If no rule matches, then the source role will be the destination role.

Device Type      Ownership      Destination Role

[Append Device Reassignment Rules](#)

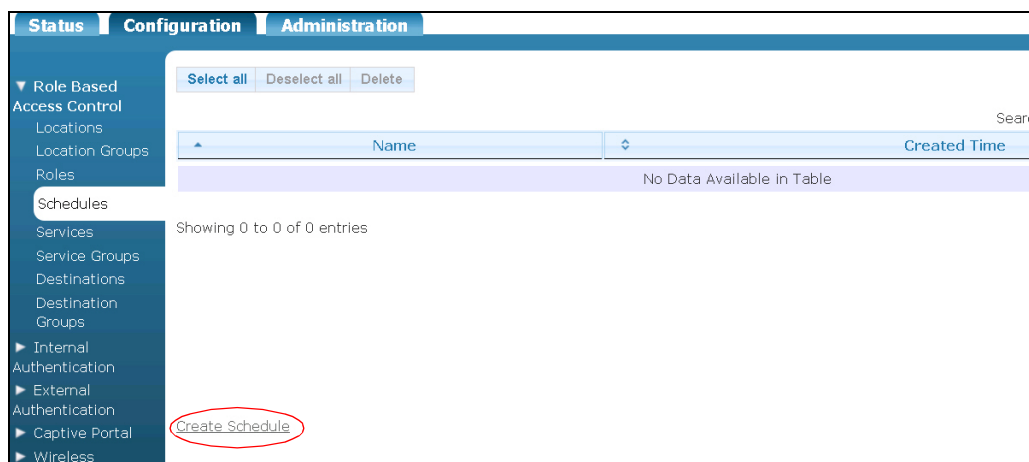
9. After you have configured the user role's name, location, CoS and QoS parameters, firewall restrictions, and device role, select **Create Role** at the bottom of the menu to create the role.
10. A confirmation is displayed indicating that the role has been created. The role will now appear in the role list (**Configuration** tab, **Role Based Access Control** > **Roles**), where you can display, edit, or delete the role.

## Configuring Domain Role Schedules

Domain role schedules specify the time in which clients can and cannot access the network. You can specify the days of the week, hours of the day, months, and days of the month that each created schedule is active, thus specifying when clients can or cannot access the network. Once a schedule is created, it must be associated with a role to take effect.

Schedules are all configurable from the **Configuration** tab. To configure the domain role schedule, follow these steps:

1. Navigate to the **Configuration** tab, and select **Role Based Access Control** > **Schedules**. Any previously configured domain role schedules will be listed in the menu. If you want to edit a previously created schedule, select the schedule name from the list. To create a new domain role schedule, either select **Create Schedule** at the bottom of this menu, or select **Domain Schedule** from the **Create** drop-down menu (at the top of the menu).



- Enter the name for the schedule in the **Name** field.

### Create Schedule

Name

- Next, specify the days of the week (Monday through Sunday) and hours of the day (0 through 23 hours) that client access is allowed by selecting the appropriate squares in the **Weekly Planner** table. For each square that is selected, a schedule rule is created.

Weekly Planner	Days	Hours																							
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
<b>Monday</b>																									
<b>Tuesday</b>																									
<b>Wednesday</b>																									
<b>Thursday</b>																									
<b>Friday</b>																									
<b>Saturday</b>																									
<b>Sunday</b>																									

Schedule: 17h00 to 18h00; Fri; Jan to Dec; 1 to 31 🗑️

Rules: [Add new schedule](#)

- To specify additional days, hours, months, or days of the months for the schedule, select the newly created schedule rule. From the schedule rule menu, you can use the slider bar on the right to specify the hours that client access is granted, and use the options on the left to specify the days, months, or days of the month that client access is granted. As you make your selections, they appear in the **Weekly Planner**.

Name

Weekly Planner	Days	Hours																							
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
<b>Monday</b>																									
<b>Tuesday</b>																									
<b>Wednesday</b>																									
<b>Thursday</b>																									
<b>Friday</b>																									
<b>Saturday</b>																									
<b>Sunday</b>																									

Schedule: 17h00 to 24h00; Fri; Jan to Apr, Jun to Dec; 1 to 22, 24 to 31 🗑️

Rules: **Schedule** ⌵

**Days of week** Hours: 24:00

Mon Tue Wed Thu **Fri** Sat

Sun All

---

**Months**

Jan Feb Mar Apr May Jun

Jul Aug Sep Oct Nov Dec

None

---

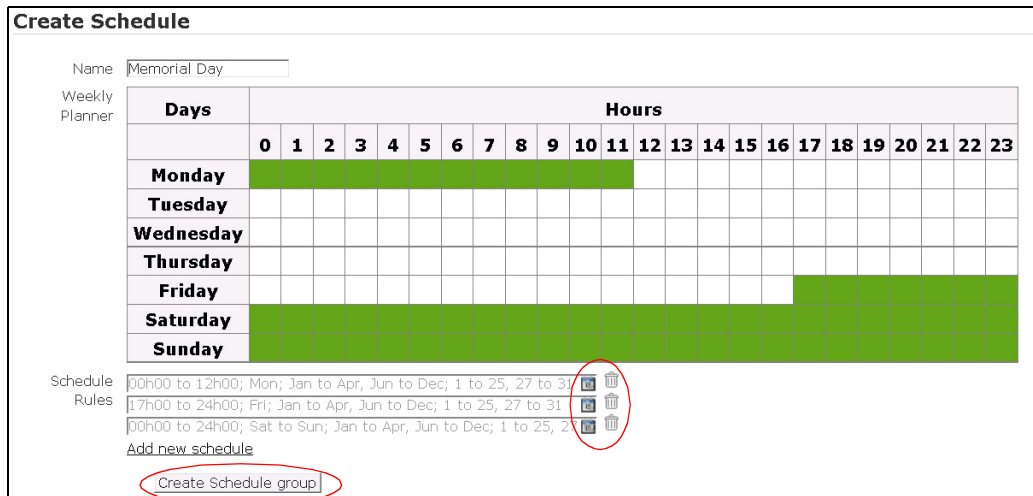
**Days of month**

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31					None

Hours: 17:00

Repeat the day and hour selection process until you have specified the times you would like the schedule to allow client access. In the example below, the schedule allows client access only on

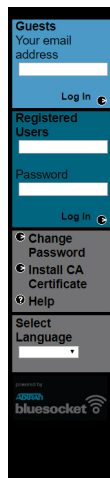
Memorial Day weekend. To delete a schedule rule, select the trash can icon next to the rule. To edit a rule, select the calendar icon next to the rule.



- When you have specified the hours, days, months, and days of the month for the schedule to allow client access, select **Create Schedule Group** at the bottom of the menu. The newly created schedule appears in the schedule list (**Configuration** tab, **Role Based Access Control** > **Schedule**). For the schedule to become active, associate it with a role as described in [Configuring Domain Roles on page 96](#).

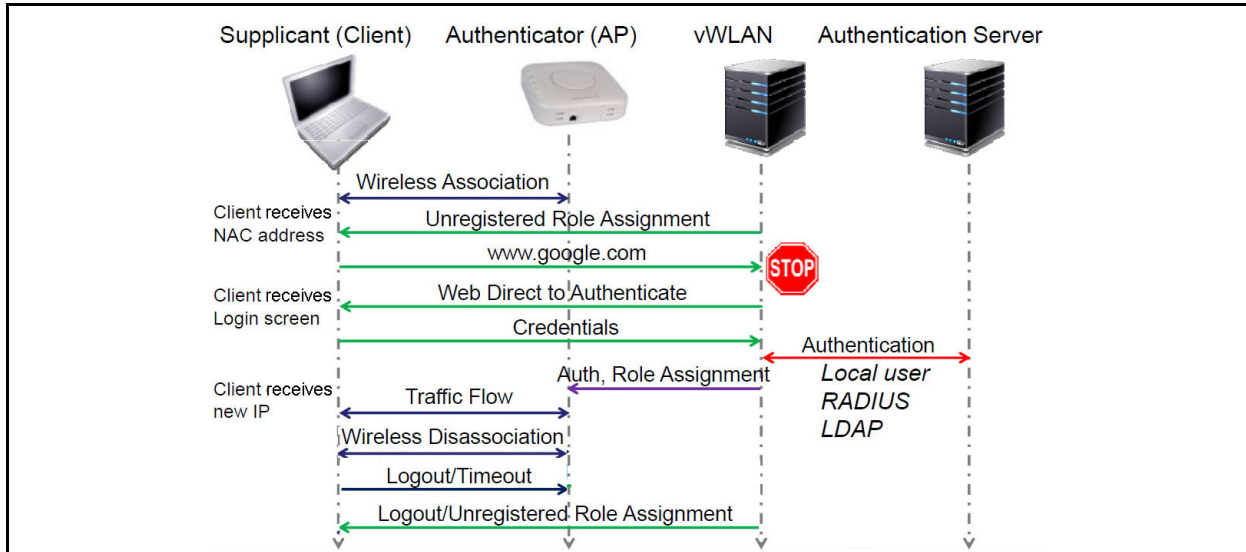
## Configuring Web-based (Captive Portal) Authentication

Web-based authentication (captive portal) is an authentication process in which clients typically connect to an open system SSID and are then redirected to a login page or captive portal (after opening a browser).



**Figure 1. Captive Portal Login Page**

This authentication process requires no client-side configuration, although it can also be used with WPAPSK/WPA2PSK SSIDs, which require the client to configure the preshared key. This authentication process typically occurs as described in [Figure 2](#).



**Figure 2. Client Authentication Process**

In the authentication process, clients in the un-registered role are redirected to the secure vWLAN login page (captive portal). The client initially receives an authentication (NAC) IP address (10.252.X.X or whatever the administrator has assigned) with a short lease time from the AP, and then the HTTP request is redirected to <https://vWLAN-ip/login.pl>. The credentials entered by the client are sent to vWLAN and authenticated against a local user database, external Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) server, external RADIUS server, or SIP2 library server (the local database is checked first, then the authentication servers are checked in the order specified by the administrator). The client is then placed into the proper authenticated role and will receive an IP address on their target location/network and begin to pass traffic.



#### NOTE

*Some client devices do not transfer automatically to a finalized IP address, but rather keep their assigned NAC IP address, which keeps them from passing traffic. Prior to vWLAN 2.6 release, these devices had to be manually disconnected and reconnected to the vWLAN network. With the included support of Layer 7 device fingerprinting in vWLAN 2.6, the BSAPs automatically detect devices that keep their NAC IP address and quickly deauthorize them so that they will automatically reconnect to vWLAN, transition to the final IP address, and begin transmitting data without the need for manual vWLAN administrator intervention.*

Web-authenticated traffic is secured using HTTPS, however, subsequent over-the-air traffic is secured based on the SSID configuration. For example, if the SSID is configured for open system, there is no over-the-air encryption. If the SSID is configured for WPA2PSK/AES, WPA2PSK+TKIP, WPA2PSK/AES, WPA2PSK+TKIP or AES, there is over-the-air encryption. Please note you cannot achieve 802.11n data rates while using TKIP, but will be limited to legacy data rates only up to 54 Mbps.

Authentication configuration includes configuring the following types of authentication: server authentication, local user authentication, SSID authentication, and MAC device authentication. In addition, you can configure login forms and images for specific domains, based on the SSID and the AP template (in that order).

## Disable TLS 1.0

Transport Layer Security (TLS) 1.0 is an older security protocol used between a client and server. This protocol has several known vulnerabilities. Therefore, to comply with modern security standards, there is an option to disable TLS 1.0.

To disable TLS 1.0, follow these steps:

1. Navigate to the **Configuration** tab and select **System > Settings**. Select the **Platform** tab and choose the option **Enable TLS 1.0**.

Name	Value *	Hint
Administrator Session Idle Timeout	30	Sets the idle timeout for administrative console sessions in minutes. Valid entries are 15 to 300, and 0 for no timeout
Certificate 1		The vWLAN requires a certificate for Apache+mod_ssl/OpenSSL.
Certificate 2		The vWLAN requires a certificate for Apache+mod_ssl/OpenSSL.
Certificate Chain 1		A chain of one or more certificates.
Certificate Chain 2		A chain of one or more certificates.
Certificate Private Key 1		The private key for the cert (closely guard this file).
Certificate Private Key 2		The private key for the cert (closely guard this file).
Certificate Selected	Click the name link to see the value	Certificate for current use.
Certificate Signature Request 1 (CSR)		The vWLAN requires a certificate for Apache+mod_ssl/OpenSSL. Use the Show action to use a form to create the CSR manually.
Certificate Signature Request 2 (CSR 2)		The vWLAN requires a certificate for Apache+mod_ssl/OpenSSL. Use the Show action to use a form to create the CSR manually.
Enable SNMP?	Enabled	
Enable TLS 1.0	Enabled	Enable Transport Layer Security protocol version 1.0 for HTTP access. This is an older security protocol with known security vulnerabilities.

2. Choose **Disable** from the drop-down menu. Next, select **Update Platform Setting**.

Enable TLS 1.0 Disabled

*Enable Transport Layer Security protocol version 1.0 for HTTP access. This is an older security protocol with known security vulnerabilities.*

**Update Platform Setting**

Show | Back

## External Server Authentication

You can configure an external RADIUS 1X, RADIUS web-based authentication, LDAP or AD, or Session Initiation Protocol 2 (SIP2) web-based library authentication server for vWLAN authentication. To configure an authentication server for the specified domain, follow the steps for each server type as outlined in the following sections.



### NOTE

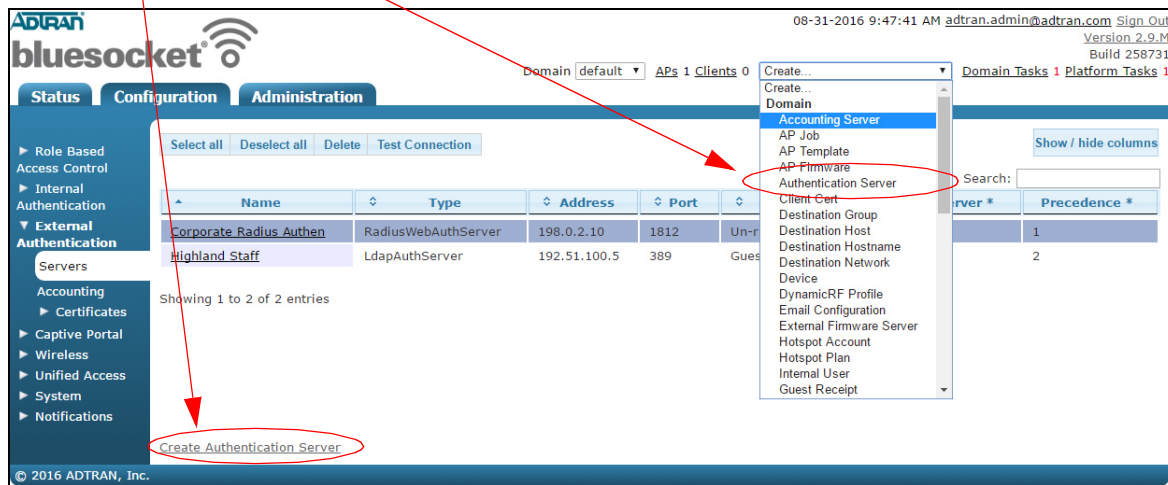
To configure a RADIUS server for use with the vWLAN WPA2-Multikey feature, refer to the server configuration steps outlined in [Configuring the RADIUS Server for the WPA2-Multikey Feature on page 240](#).

## External RADIUS 1X Authentication Server

To configure an external RADIUS 1x authentication server for use with vWLAN, follow these steps:

1. Navigate to the **Configuration** tab and select **External Authentication > Servers**. Any previously configured RADIUS 1X authentication servers will be listed in the menu. If you want to edit a previously created RADIUS 1X authentication server, select the server name from the list. To create a new authentication server, either select **Create Authentication Server** at the bottom of this menu, or select **Domain Authentication Server** from the **Create** drop-down menu (at the top of the menu).

Select either option to create a new authentication server.



2. Select **Radius1xAuthServer** from the **Type** drop-down menu.

**Create Authentication Server**

Type: **Radius1xAuthServer** ▼

Name: NPS1

Accounting Server: ▼

IP Address: 192.168.10.253

Port: 1812  
*Typically, the port should be 1812 or 1645.*

Shared Secret/Password: .....

Shared Secret/Password Confirmation: .....

**Backup**

Backup Address: .....

Backup Port: .....

*If backup address is specified, and this is not, this defaults to the same port as the primary server.*

Backup Password: .....

*If backup address is specified, and this is not, this defaults to the same password as the primary server.*

Backup Password Confirmation: .....

**Proxy**

Enable RADIUS Proxy:

*Proxy requests through vWLAN instead of sending directly from APs to external server.  
Note: Requires RADIUS client configured in external RADIUS Server with IP address of vWLAN and shared secret to match above.*

**Authentication Rules**

Role: Employee ▼

Attribute	Logic	Value	Role
User-Name	starts with	host/	Domain Computer ▼
ARAP-Challenge-Response	equal to		Guest ▼
ARAP-Challenge-Response	equal to		Guest ▼
ARAP-Challenge-Response	equal to		Guest ▼
ARAP-Challenge-Response	equal to		Guest ▼

[Append Auth Rule](#)

3. Next, enter the name of the server and its IP address in the appropriate fields. Optionally, specify if this authentication server will be associated with an accounting server by selecting the accounting server from the **Accounting server** drop-down menu.

Name: New Auth Server

Accounting Server: ▼

IP Address: .....

4. Next, specify the port to be used by the server. If you are using a RADIUS server, the port is generally either 1645 or 1812.

Port: 1812  
*Typically, the port should be 1812 or 1645.*

5. Next, enter the shared secret or password for the authentication server.

Shared Secret/Password: .....

Shared Secret/Password Confirmation: .....

- Optionally, specify the backup address, backup port, and backup shared secret or password for the server. This step is needed if a backup RADIUS server is configured. Otherwise, leave these fields blank.

**Backup**

Backup Address

Backup Port   
If backup address is specified, and this is not, this defaults to the same port as the primary server.

Backup Password   
If backup address is specified, and this is not, this defaults to the same password as the primary server.

Backup Password Confirmation

- Optionally, proxy all requests through the vWLAN to the RADIUS server versus from the AP directly to the RADIUS server by selecting the box next to **Enable RADIUS Proxy**.

**i** **NOTE**

*This feature requires a RADIUS client to be configured for the IP address of vWLAN and the shared secret to match above.*

**Proxy**

Enable RADIUS Proxy

Proxy requests through vWLAN instead of sending directly from APs to external server.  
Note: Requires RADIUS client configured in external RADIUS Server with IP address of vWLAN and shared secret to match above.

- Next, you must specify the authentication rules for the server and the role given to a user who does not meet the authentication rules. Select an appropriate role option from the **Role** drop-down menu. If you choose unregistered, and no authentication rules match, then web-based authentication can determine the assigned roles. The authentication rules for the server specify to which role users are assigned when they are authenticated. For RADIUS servers, select the appropriate attribute from the **Authentication Rules** drop-down menu. There are multiple attributes to choose from.
- Next, specify the logic type used for authentication mapping from the drop-down menu. You can select from **equal to**, **not equal to**, **starts with**, **ends with**, and **contains**. Then, fill in the appropriate value in the next field, and select the appropriate role from the drop-down menu. In the example below, a RADIUS 1x server is configured to use a **User Name** attribute, that contains the value **ann jenkins**, which assigns the user the role of **Guest**.

**Authentication Rules**

Role

Attribute	Logic	Value	Role
<input type="text" value="User-Name"/>	<input type="text" value="equal to"/>	<input type="text" value="ann jenkins"/>	<input type="text" value="Guest"/>
<input type="text" value="ARAP-Challenge-Response"/>	<input type="text" value="equal to"/>	<input type="text"/>	<input type="text" value="Guest"/>
<input type="text" value="ARAP-Challenge-Response"/>	<input type="text" value="equal to"/>	<input type="text"/>	<input type="text" value="Guest"/>
<input type="text" value="ARAP-Challenge-Response"/>	<input type="text" value="equal to"/>	<input type="text"/>	<input type="text" value="Guest"/>
<input type="text" value="ARAP-Challenge-Response"/>	<input type="text" value="equal to"/>	<input type="text"/>	<input type="text" value="Guest"/>

[Append Auth Rule](#)



Attributes are searched in order. You can move these attributes in any order you want, or add additional rules using the **Append Auth Rule** option. You can also remove an attribute by using the trash can icon.

10. Lastly, select **Create Auth Server** at the bottom of the menu. A confirmation is displayed indicating that the server has been created. The server will now appear in the server list (**Configuration** tab, **External Authentication > Servers**), where you can display, edit, or delete the server.

External RADIUS 1X servers support the following EAP types:

- Extensible Authentication Protocol (EAP)-Transport Layer Security (TLS)
- EAP-Tunneled Transport Layer Security (TTLS)
- Protected Extensible Authentication Protocol (PEAP)
- EAP-Flexible Authentication via Secure Tunneling (FAST)
- EAP-GSM Subscriber Identity Module (SIM)
- EAP-Authentication and Key Agreement (AKA)

APs send RADIUS requests to the RADIUS server, and therefore you must configure a RADIUS client in the RADIUS server for every AP. Alternatively, you can configure a RADIUS client in the RADIUS server with an IP range.

### External RADIUS Web-based Authentication Server

To configure a RADIUS web-based authentication server for use with vWLAN, follow these steps:



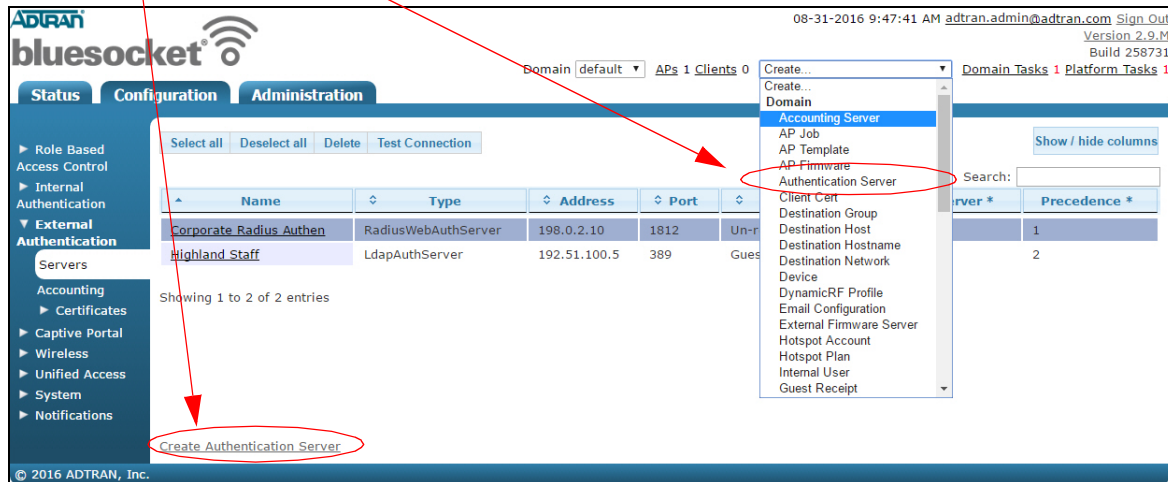
#### NOTE

*To configure a RADIUS server for use with the vWLAN WPA2-Multikey feature, refer to the server configuration steps outlined in [Configuring the RADIUS Server for the WPA2-Multikey Feature on page 240](#).*

1. Navigate to the **Configuration** tab, and select **External Authentication > Servers**. Any previously configured web-based authentication servers will be listed in the menu. If you want to edit a previously created web-based authentication server, select the server name from the list. To create a

new authentication server, either select **Create Authentication Server** at the bottom of this menu, or select **Domain Authentication Server** from the **Create** drop-down menu (at the top of the menu).

Select either option to create a new authentication server.



2. Select **RadiusWebAuthServer** from the **Type** drop-down menu.

Type

3. Next, enter the name of the server and its IP address in the appropriate fields. Optionally, specify if this authentication server will be associated with an accounting server by selecting the accounting server from the **Accounting Server** drop-down menu.

Name   
 Accounting Server   
 IP Address

4. Next, specify the port to be used by the server. If you are using a RADIUS server, the port is generally either 1645 or 1812.

Port   
*Typically, the port should be 1812 or 1645.*

5. Next, enter the shared secret or password for the authentication server.

Shared Secret/Password   
 Shared Secret/Password Confirmation

6. Specify the timeout weight, maximum number of simultaneous user authentications, and the precedence of the server. The timeout weight value is relative to the timeout weight of other authentication servers. The total time allocated to authenticate is defined for the entire vWLAN system. Each server's timeout is computed as a percentage of the total weight of all authentication servers on this domain. If you leave the maximum number of simultaneous authentications field blank, or enter a 0, that indicates there is no limit. You can specify the precedence level of the server

as **Highest**, **Lowest**, or **Fixed**. If you select **Fixed**, you can manually order the authentication servers in order of precedence.

Timeout Weight	<input type="text" value="1"/>	<small>Current total weight is 0, and current total timeout is 10.) Set the weight of the timeout for this server relative to the other auth servers. The total time allocated to authenticate is defined for the entire system. Each server's timeout will be computed as its percentage of the total weight of all auth servers in this domain.</small>
Maximum Number of Simultaneous Users Allowed to Authenticate at Once	<input type="text" value="10"/>	<small>Blank or 0 = no limit.</small>
Precedence	<input type="text" value="Highest"/>	

- Next, you must specify the authentication rules for the server and the role given to a user who does not meet the authentication rules. Select the role from the **Role** drop-down menu. If you choose un-registered, then the authentication rules determine the assigned role.



#### NOTE

In vWLAN firmware release 3.5.0, if you select the **Default** role from the **Role** menu, you can optionally choose to override the location assigned to clients in this role by selecting the **Override Location with TPGI** check box.

Enable Radius MAC Authentication	<input checked="" type="checkbox"/>		
SSIDs	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span>1 items selected</span> <span>Remove all</span> <span>Add all</span> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: left; padding: 2px;">- OpenMAC</td> <td style="text-align: right; padding: 2px;">+ newOpen</td> </tr> </table> </div>	- OpenMAC	+ newOpen
- OpenMAC	+ newOpen		
Override Location with TunnelPrivate-Group-ID	<input checked="" type="checkbox"/>		
Role	<input type="text" value="AllowAll"/>		



#### NOTE

When this option is enabled, and a Tunnel-Private-Group-ID (TPGI) with a value between **1** to **4095** exists, then clients connected in the **Default** role are assigned a location based on a VLAN ID assigned by the RADIUS server, and not the location associated with the role. Once this option is selected, the remaining RADIUS attributes become non-configurable. If this option is selected, and a TPGI does not exist, then clients are assigned a location based on the values specified in the **Default** role.

The authentication rules specify to which role users are assigned when they are authenticated. For RADIUS servers, select the appropriate attribute from the **Authentication Rules** drop-down menu. There are multiple attributes to choose from.

The screenshot shows the 'Authentication Rules' configuration window. At the top, there is a 'Role' dropdown menu set to 'Un-registered'. Below this is a table with columns: 'Attribute', 'Logic', 'Value', and 'Role'. There are five rows, each representing a rule. All rules have 'ARAP-Challenge-Response' in the 'Attribute' column, 'equal to' in the 'Logic' column, an empty text box in the 'Value' column, and 'Guest' in the 'Role' column. Each row has a trash can icon to its right. At the bottom left of the table area, there is a link that says 'Append Auth Rule'.

- Next, specify the logic type used for authentication mapping from the drop-down menu. You can select from **equal to**, **not equal to**, **starts with**, **ends with**, and **contains**. Then, fill in the appropriate value in the next field, and select the appropriate role from the drop-down menu. In the example below, a RADIUS 1x server is configured to use a **User Name** attribute, that contains the value **ann jenkins**, which assigns the user the role of **Guest**.

This screenshot is similar to the previous one but shows a specific rule configuration. The first rule has 'User-Name' in the 'Attribute' column, 'equal to' in the 'Logic' column, 'ann jenkins' in the 'Value' column, and 'Guest' in the 'Role' column. The other four rules below it are identical to the first screenshot, with 'ARAP-Challenge-Response' as the attribute and an empty value field. The 'Append Auth Rule' link is also present at the bottom left.

Attributes are searched in order. You can move these attributes in any order you want or add additional rules by selecting **Append Auth Rules**. You can also remove an attribute by using the trash can icon.

- Lastly, select **Create Auth Server**. A confirmation is displayed indicating that the server has been created. The server will now appear in the server list (**Configuration** tab, **External Authentication > Servers**), where you can display, edit, or delete the server.

**i** **NOTE**

*If this server will be used in conjunction with the vWLAN WPA2-Multikey feature, additional server configuration will be required. Refer to [Configuring the RADIUS Server for the WPA2-Multikey Feature on page 240](#) for more information about the specific RADIUS server configuration required for the WPA2-Multikey feature.*

10. Optional. Once the external server is created, you can verify it for a successful connection. Return to the **External Authentication > Servers** menu. Select the authentication server you just created from the list, and select the **Test Connection** button from the top of the menu.

Select the authentication server you want to verify.

Select the **Test Connection** button to be redirected to the **Diagnostics** menu.

Name	Type	Address	Port	Un-r
Corporate Radius Authen	RadiusWebAuthServer	198.0.2.10	1812	Un-r
Highland Staff	LdapAuthServer	192.51.100.5	389	Guest

You will be redirected to the **Diagnostics** menu which allows you to enter a username and password to test the authentication method. Refer to [External Authentication Test Results on page 269](#) for more information.

External Authentication Test

Authentication Server: Highland Staff

Username: jsmith

Password: .....



#### NOTE

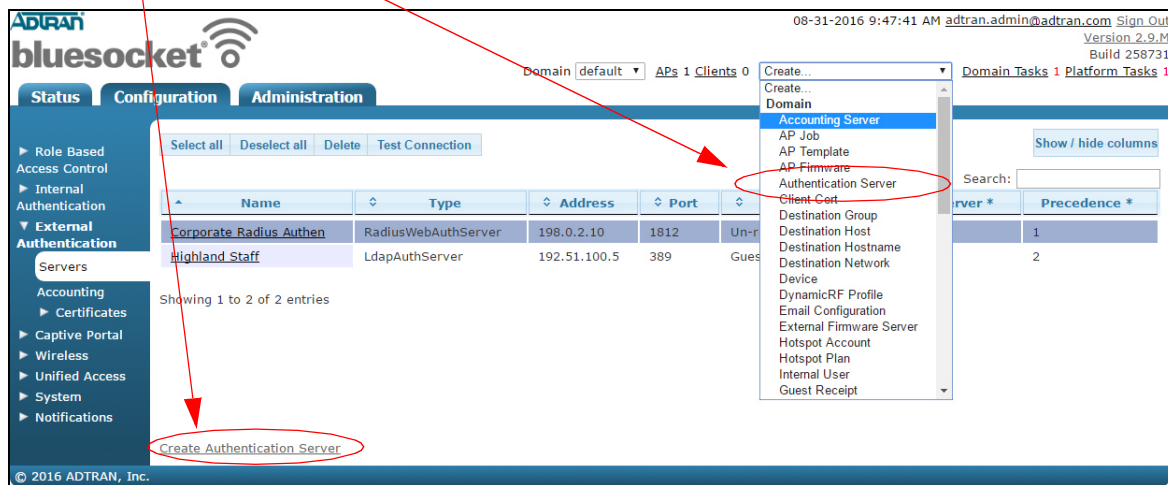
*External RADIUS web-based authentication uses PAP and requires a RADIUS client to be configured in the RADIUS server for the vWLAN instance.*

## External LDAP Web-based Authentication Server

To configure an LDAP authentication server for use with vWLAN, follow these steps:

1. Navigate to the **Configuration** tab, and select **External Authentication > Servers**. Any previously configured LDAP authentication servers will be listed in the menu. If you want to edit a previously created LDAP authentication server, select the server name from the list. To create a new authentication server, either select **Create Authentication Server** at the bottom of this menu, or select **Domain Authentication Server** from the **Create** drop-down menu (at the top of the menu).

Select either option to create a new authentication server.



2. In the **New Authentication Server** menu, select **LdapAuthServer** from the **Type** drop-down menu.

Type

3. Enter the name of the server and its IP address in the appropriate fields. Optionally, specify if this authentication server will be associated with an accounting server by selecting the account server from the **Accounting Server** drop-down menu.

Name

Accounting Server

IP Address

4. Specify the port to be used by the server. If you are using an LDAP server, the port is generally 389, unless Secure Socket Layer (SSL) is used, in which case the port is generally 636.

Port

*Typically, the port should be 389 for LDAP and 636 if require SSL is checked.*

- Specify the name of the administrator user to which to bind the LDAP server. Enter the administrator's FQDN in the **LDAP Bind User** field.

LDAP Bind User	<input "="" type="text" value="cn=LDAP AuthUser, cn=Users, dc="/>
<small>The name of an admin user to bind to the LDAP server with.</small>	

**NOTE**

*It is not recommended to use an administrative account. Using a standard account is sufficient. The entered account must match the user account configured in LDAP or AD.*

The LDAP user field should be populated with the full name of the user, not the login name in AD. For example, use Bob Smith, not BSmith. All the name parts are used and added to each other to compose the full name. The resulting user name when using Bob and Smith as the first and last names respectively in AD is Bob Smith. Unless the LDAP user is in the root of AD, and the base entry specifies the root, you must specify where it is. This is referred to as the distinguished name.

For example, if Bob Smith is in the users container, you would enter **CN=Bob**

**Smith,CN=Users,DC=Bluesocket,DC=com** in the LDAP user field, where the first CN refers to common name, and the second CN refers to container. If Bob Smith was in the root of AD, and the base entry specified the root, you could simply enter Bob Smith.

Make sure you do not confuse CNs (containers) with OUs (organizational units). OUs have an icon in AD that could be described as a folder in a folder, while CNs have an icon in AD that could be described as a folder. Built-in folders in AD are typically CNs, while folders you add are typically OUs.

Right-click the folder in AD, select **properties**, select the object tab, and refer to the object class to be certain you are using CN or OU. For example, if Bob Smith is in the Engineers OU, enter the following in the LDAP user field: **CN=BobSmith,OU=Engineers,DC=Bluesocket,DC=com**. CN refers to Common Name, and OU refers to Organizational Unit. Work from the bottom of the AD tree upwards. For example, if Bob Smith is in the Tech Support OU, which is in the Engineers OU, enter the following into the LDAP User field:

**CN=Bob Smith,OU=Techsupport,OU=Engineers,DC=Bluesocket,DC=com**.

CN refers to Common Name, and OU refers to Organizational Unit.

- Enter the shared secret or password for the previously created bind user.

Shared Secret/Password	<input type="password" value="....."/>
Shared Secret/Password Confirmation	<input type="password" value="....."/>

- Configure the LDAP base entry, unique ID attribute, and any LDAP filters. The **LDAP Base Entry** field specifies the starting point for LDAP database queries, and the **LDAP Unique ID attribute** field specifies the unique identifier used to distinguish each user record within the database. LDAP filters are used when looking up LDAP unique ID attributes.

LDAP Base Entry	<input type="text"/>	<small>An example base entry is cn=Users,dc=company,dc=com.</small>
LDAP Unique ID Attribute	<input type="text"/>	<small>UID for openldap, sAMAccountName for AD.</small>
LDAP Filters	<input type="text"/>	<small>Additional LDAP filters used when looking up Unique ID attributes. (An example is objectClass=Person)</small>
Bind All Queries As LDAP Bind User	<input checked="" type="checkbox"/>	<small>Check to Bind all Queries as the LDAP Bind User using Name/Password Authentication. If this option is not selected, then Anonymous Authentication will be used and the external LDAP/AD server must be configured to allow for anonymous binding.</small>

You can configure the system to bind all queries with the LDAP Bind User's credentials by checking the box next to **Bind all Queries as LDAP Bind User**. If this option is not selected, then Anonymous Authentication will be used and the external LDAP/AD server must be configured to allow anonymous binding.

The **LDAP Base Entry** should be populated with the location with which vWLAN should start to search for users in the LDAP or AD tree. For example, if all the users are in the Users container, then the base entry should be populated with **CN=Users,DC=Bluesocket,DC=com**. If the users are scattered about AD in different containers or organizational units, you can simply specify the root by entering **DC=Bluesocket,DC=com**.

The **LDAP Unique ID attribute** field specifies the unique ID attribute that identifies and distinguishes each user record in LDAP or AD. The unique ID attribute for AD is **sAMAccountName**.

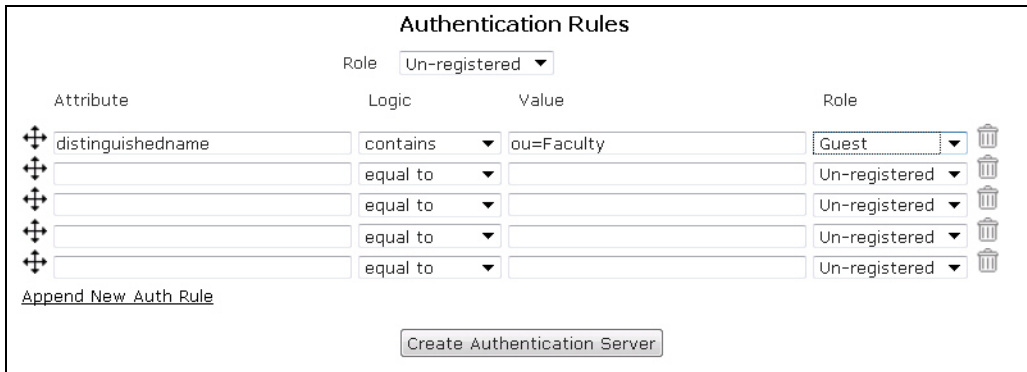
8. Configure the timeout weight, maximum number of simultaneous user authentications, server precedence, and whether SSL is used. The timeout weight is the value relative to the timeout weight of other authentication servers. The total time allocated to authenticate is defined for the entire vWLAN system. Each server's timeout is computed as a percentage of the total weight of all authentication servers on this domain. Leaving the maximum number of simultaneous authentications field blank, or entering a 0, indicates there is no limit. You can specify the precedence level of the server as **Highest**, **Lowest**, or **Fixed**. If you select **Fixed**, you can manually order the authentication servers in order of precedence. Enable SSL by selecting the **Require SSL** check box.

Timeout Weight	<input type="text" value="1"/>	<small>Current total weight is 0, and current total timeout is 10.) Set the weight of the timeout for this server relative to the other auth servers. The total time allocated to authenticate is defined for the entire system. Each server's timeout will be computed as its percentage of the total weight of all auth servers in this domain.</small>
Maximum Number of Simultaneous Users Allowed to Authenticate at Once	<input type="text" value="10"/>	<small>Blank or 0 = no limit.</small>
Precedence	<input type="text" value="Highest"/>	
Require SSL	<input type="checkbox"/>	

9. Next, you must specify the authentication rules for the server and the role given to a user who does not meet the authentication rules. Select the appropriate option from the **Role** drop-down menu. If you choose un-registered, then the authentication rules determine the assigned role. The authentication rules specify to which role users are assigned when they are authenticated. Manually enter the type of attribute to use in the authentication rules (for example, **distinguishedname**).
10. Next, specify the logic type used for authentication mapping from the drop-down menu (this applies to all servers). You can select from **equal to**, **not equal to**, **starts with**, **ends with**, and **contains**. Then fill in the appropriate value in the next field, and select the appropriate role from the drop-down



menu. In the example below, an LDAP server is configured to use a **distinguishedname** attribute, that contains the value **Faculty**, which assigns the user the role of **Architecture Faculty**.

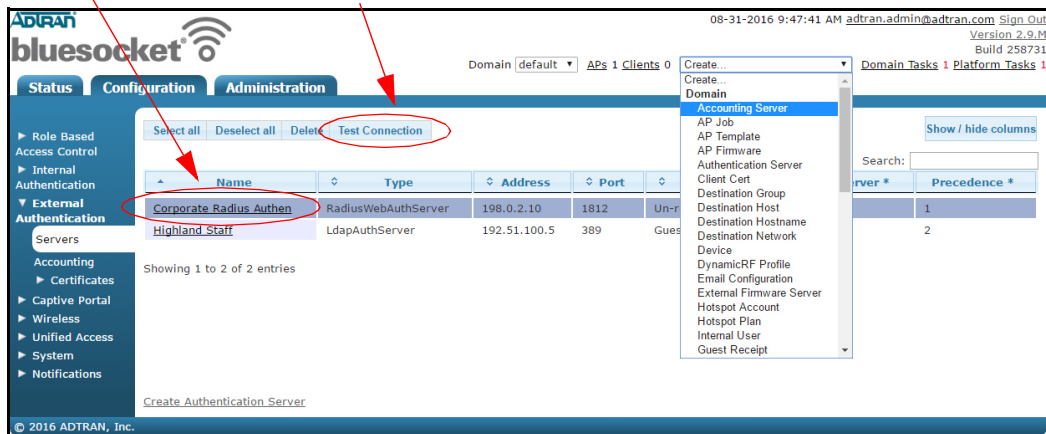


Attributes are searched in order. You can move these attributes in any order you want or add additional rules by selecting **Append New Auth Rule**. You can also remove an attribute by using the trash can icon.

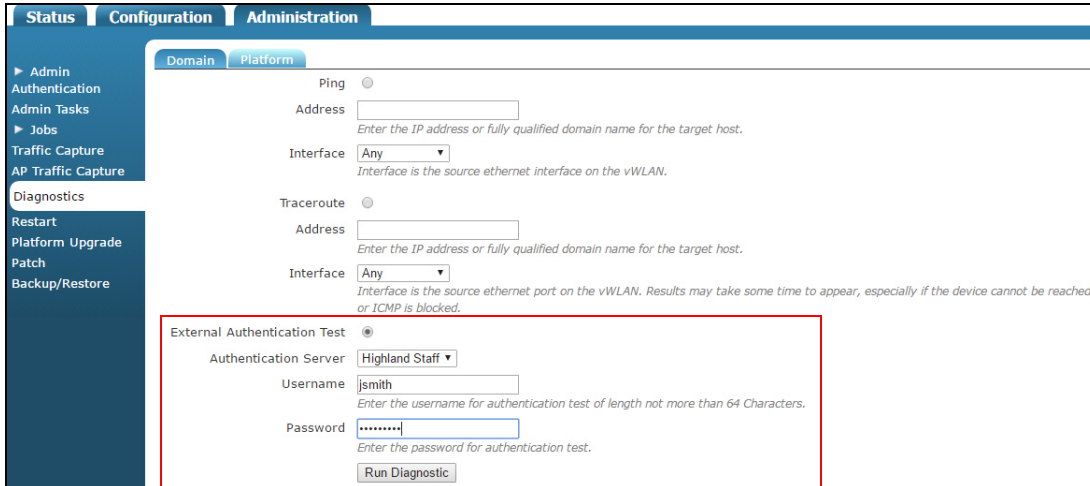
11. Lastly, select **Create Authentication Server**. A confirmation is displayed indicating that the server has been created. The server will now appear in the server list (**Configuration** tab, **External Authentication > Servers**), where you can display, edit, or delete the server.
12. Optional. Once the external server is created, you can verify it for a successful connection. Return to the **External Authentication > Servers** menu. Select the authentication server you just created from the list, and select the **Test Connection** button from the top of the menu.

Select the authentication server you want to verify.

Select the **Test Connection** button to be redirected to the **Diagnostics** menu.



You will be redirected to the **Diagnostics** menu which allows you to enter a username and password to test the authentication method. Refer to [External Authentication Test Results on page 269](#) for more information.

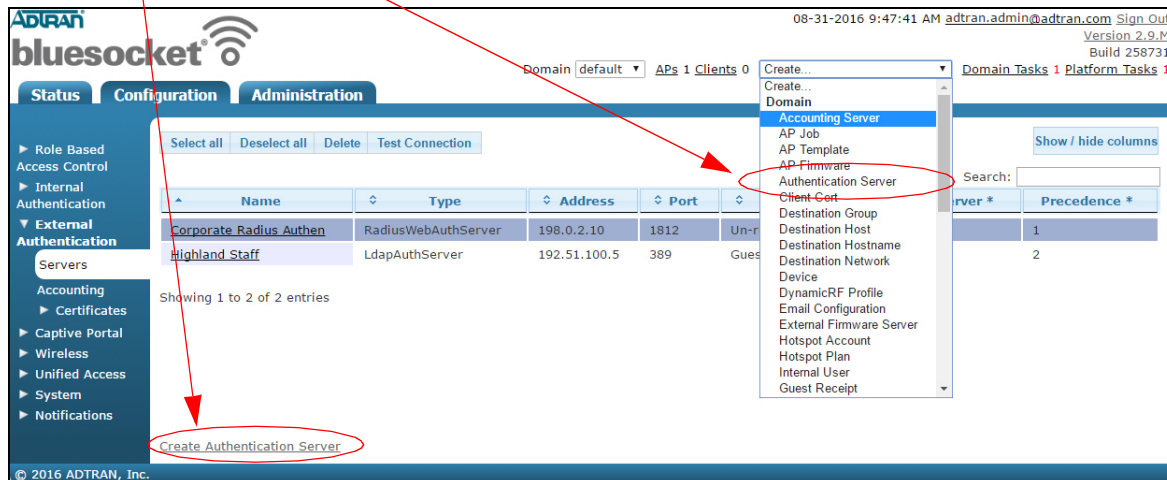


### External SIP2 Web-based Library Authentication Server

To configure a SIP2 authentication server (typically used in libraries) for user authentication, follow these steps:

1. Navigate to the **Configuration** tab, and select **External Authentication > Servers**. Any previously configured SIP2 authentication servers will be listed in the menu. If you want to edit a previously created SIP2 authentication server, select the server name from the list. To create a new authentication server, either select **Create Authentication Server** at the bottom of this menu, or select **Domain Authentication Server** from the **Create** drop-down menu (at the top of the menu).

Select either option to create a new authentication server.



2. Select **SIP2AuthServer** from the **Type** drop-down menu.



- Enter the name of the server and its IP address in the appropriate fields. Optionally, specify if this authentication server will be associated with an accounting server by selecting the account server from the **Accounting Server** drop-down menu.

Name	<input type="text" value="SIP2 Auth Server 1"/>
Accounting Server	<input type="text" value="▼"/>
IP Address	<input type="text" value="172.16.2.240"/>

- Specify the port to be used by the server. If you are using a SIP2 server, the port is generally **6001**.

Port	<input type="text" value="6001"/>
<i>Typically, the port should be 6001.</i>	

- Optionally, specify the name of the administrator user to which to bind the SIP2 server. Enter the administrator's FQDN in the **SIP2 Admin Name** field.

SIP2 Admin Name	<input type="text" value="joesmith@adtran.com"/>
<i>The name of an admin user to authenticate to the SIP2 server with.</i>	



#### NOTE

*The administrator and password for the SIP2 server are optional. If no administrator or password is set, then the SIP2 authentication occurs without them. However, if an administrator is specified, a password must also be specified for authentication to occur.*

- Optionally, enter the shared secret or password for the authentication server.

Shared Secret/Password	<input type="password" value="....."/>
Shared Secret/Password Confirmation	<input type="password" value="....."/>

- Specify the timeout weight for the server. This value is relative to the timeout weight of other authentication servers. The total time allocated to authenticate is defined for the entire vWLAN system. Each server's timeout is computed as a percentage of the total weight of all authentication servers in this domain (the platform setting of **Timeout Value for Web Server** determines the total timeout that is divided based on weight).

Timeout Weight	<input type="text" value="1"/>
<i>Current total weight is 0, and current total timeout is 10.)</i>	
<i>Set the weight of the timeout for this server relative to the other auth servers. The total time allocated to authenticate is defined for the entire system.</i>	
<i>Each server's timeout will be computed as its percentage of the total weight of all auth servers in this domain.</i>	

8. Specify whether the user's PIN or password will be validated by selecting the **SIP2 Validate PIN/Password** check box.

SIP2 Validate PIN/Password	<input checked="" type="checkbox"/>
SIP2 Specify An Empty AO Institution ID	<input type="checkbox"/>
SIP2 CP Location Code	<input type="text"/>
<i>Leave blank/empty to not send CP location code in the login message (93).</i>	

9. Specify whether an empty AO institution ID is specified when communicating with the server by selecting the **SIP2 Specify an empty AO Institution ID** check box.

SIP2 Validate PIN/Password	<input checked="" type="checkbox"/>
SIP2 Specify An Empty AO Institution ID	<input type="checkbox"/>
SIP2 CP Location Code	<input type="text"/>
<i>Leave blank/empty to not send CP location code in the login message (93).</i>	

10. Specify whether a CP location code is sent to the server, and what CP location code is sent, by entering the code in the **SIP2 CP Location Code** field. Leave this field blank if you do not want a CP location code in the login message.

SIP2 Validate PIN/Password	<input checked="" type="checkbox"/>
SIP2 Specify An Empty AO Institution ID	<input type="checkbox"/>
SIP2 CP Location Code	<input type="text"/>
<i>Leave blank/empty to not send CP location code in the login message (93).</i>	

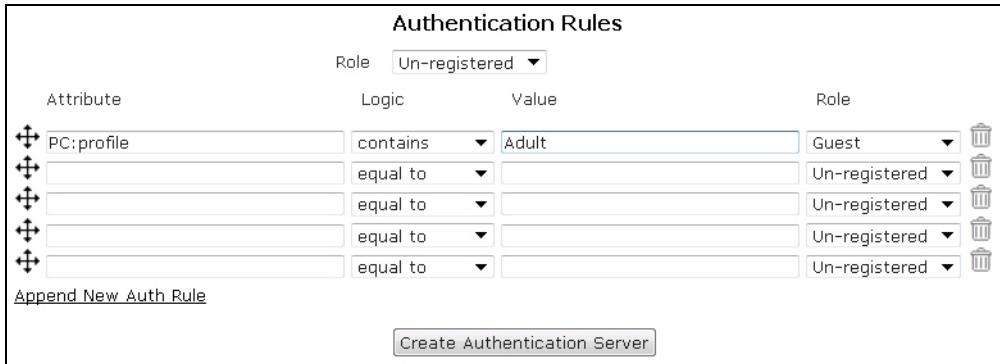
11. Configure the maximum number of simultaneous users allowed to authenticate and the server precedence. Leaving the maximum number of simultaneous authentications field blank, or entering a 0, indicates there is no limit. You can specify the precedence level of the server as **Highest**, **Lowest**, or **Fixed**. If you select **Fixed**, you can manually order the authentication servers in order of precedence.

Maximum Number of Simultaneous Users Allowed to Authenticate at Once	<input type="text" value="10"/>
<i>Blank or 0 = no limit.</i>	
Precedence	<input type="text" value="Highest"/>

12. Next, you must specify the authentication rules for the server and the role given to a user who does not meet the authentication rules. Specify a role by selecting the appropriate option from the **Role** drop-down menu. The authentication rules specify to which role users are assigned when they are authenticated. Manually enter the type of attribute to use in the authentication rules (for example, **attribute=PC: profile, logic=contains, value=Adult, and role=Adult**).

13. Next, specify the logic type used for authentication mapping from the drop-down menu (this applies to all servers). You can select from **equal to**, **not equal to**, **starts with**, **ends with**, and **contains**. Then, fill in the appropriate value in the next field, and select the appropriate role from the drop-down

menu. In the example below, a SIP2 server is configured to use a **PC:profile** attribute, that contains the value **Adult**, which assigns the user the role of **Architecture Faculty**.

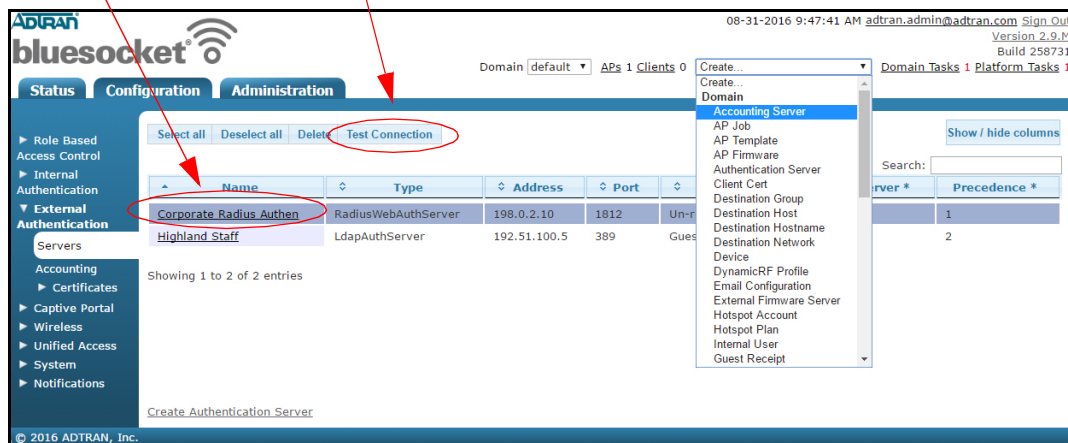


Attributes are searched in order. You can move these attributes in any order you want or add additional rules by selecting **Append New Auth Rule**. You can also remove an attribute by using the trash can icon.

14. Lastly, select **Create Auth Server**. A confirmation is displayed indicating that the server has been created. The server will now appear in the server list (**Configuration** tab, **External Authentication > Servers**), where you can display, edit, delete, or test the connection to the server.
15. Optional. Once the external server is created, you can verify it for a successful connection. Return to the **External Authentication > Servers** menu. Select the authentication server you just created from the list, and select the **Test Connection** button from the top of the menu.

Select the authentication server you want to verify.

Select the **Test Connection** button to be redirected to the **Diagnostics** menu.



You will be redirected to the **Diagnostics** menu which allows you to enter a username and password to test the authentication method. Refer to [External Authentication Test Results on page 269](#) for more information.

The screenshot shows the Configuration page with the Administration tab selected. The left sidebar contains navigation options: Admin Authentication, Admin Tasks, Jobs, Traffic Capture, AP Traffic Capture, Diagnostics, Restart, Platform Upgrade, Patch, and Backup/Restore. The main content area is divided into Domain and Platform tabs. Under the Platform tab, there are sections for Ping, Traceroute, and External Authentication Test. The External Authentication Test section is highlighted with a red box and contains the following fields:

- External Authentication Test:**
- Authentication Server:** Highland Staff (dropdown menu)
- Username:** jsmith (text input field)
- Password:** [masked] (password input field)
- Run Diagnostic:** (button)

## Configuring Local User Authentication

Local user authentication in vWLAN takes precedence over external server authentication and can be used for web-based authentication. Each local user authentication database record consists of the following:

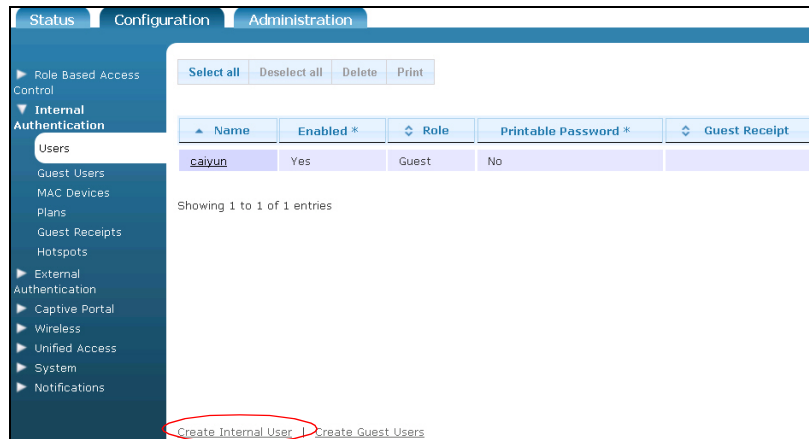
- User status (disabled, enabled)
- User name
- Role
- Number of active sessions
- User password
- Whether and how the user expires

By default, no local users exist in the vWLAN system.

To configure local user authentication for the specified domain, follow these steps:

1. Navigate to the **Configuration** tab, and select **Internal Authentication > Users**. Any previously configured internal users will be listed in the menu. If you want to edit a previously created internal user, select the user name from the list. To create a new internal user, either select **Create Internal**

**User** at the bottom of this menu, or select **Domain Internal User** from the **Create** drop-down menu (at the top of the menu).



- Specify the user's name and password in the appropriate field, and enable the user by checking the **Enabled** box. Then specify the user's role by selecting the appropriate role from the **Role** drop-down menu. Optionally, select an accounting server to associate with this user from the **Accounting Server** drop-down menu. Next, specify how many users of the same name can be logged in simultaneously by entering a value in the appropriate field. If you specify 0, there is no limit to how many users with the same name can be logged in simultaneously. Lastly, you can specify that the user account does not expire by selecting the **Never expire** check box.

**Create Internal User**

Name:

Password:

Password Confirmation:

Enabled:

Role:

Accounting Server:

Simultaneous User Authentication:   
*0 is unlimited.*

Expire User:  Never expire

- Select **Create Internal User**. A confirmation is displayed indicating that the user has been created. The user will now appear in the internal user list (**Configuration** tab, **Internal Authentication** > **Users**), where you can display, edit, or delete the user.
- Once users have been created, the local user database will be used as the primary web-based authentication method for connecting to vWLAN.

## Device Authentication

vWLAN has a local device authentication database, which takes precedence over all other methods of authentication. Each local device authentication database record consists of the following:

- Device name
- MAC address
- Statically assigned role

In addition, vWLAN has the ability to use wildcard MAC address authentication to place devices in a role based on the OUI or vendor. When configuring a wildcard MAC or a MAC address range for a device, use the wildcard character `%`. For example, if you were configuring a Polycom phone for MAC authentication, beginning with the OUI of `00:90:7a`, and placing the phone into a determined role, you can use the MAC address `00:90:7a:%:%:%`. Wildcards are only allowed on exactly the last three octets of the MAC address.



### NOTE

*In scenarios where the same MAC address can match a wildcard MAC address, and a normal MAC device, the MAC device takes precedence.*

In vWLAN firmware release 2.6, the Layer 7 device fingerprinting feature was introduced. This feature allows you to specify the type of device when adding it to the vWLAN system. Detected device information includes the device type, operating system, and vendor information. When the new device is added, you can specify whether the device type is a corporate device, or another type of device (**other**). This feature allows vWLAN to detect the device type when it connects to the vWLAN network, and automatically associates the device with a user role (configured in **Configuration > Roles**). In addition, you can add devices to vWLAN using a bulk import method. Details for Layer 7 device fingerprinting configuration are included in the following section, in [Configuring Domain Roles on page 96](#), and in the configuration guide [Layer 7 Device Fingerprinting for vWLAN](#), available online at <https://supportcommunity.adtran.com>.

To configure a device for use in device authentication, follow these steps:

1. Navigate to the **Configuration** tab, and select **Internal Authentication > Devices**. Any previously configured devices will be listed in the menu. If you want to edit a previously created device, select



the device name from the list. To create a new device, either select **Create Device** at the bottom of this menu, or select **Domain Device** from the **Create** drop-down menu (at the top of the menu).



- In the **Create Device** menu, enter the device name and the MAC address of the device in the appropriate fields. Select the **Enable MAC Authentication** check box to enable MAC authentication for the device (this option is enabled by default). Specify the device's assigned role using the **Role** drop-down menu. Optionally, associate the device with an accounting server by selecting an accounting server from the **Accounting server** drop-down menu. Optionally specify whether the device is a corporate-owned device (by selecting the **Corporate-Owned** check box) or specify the device is owned by someone else (by leaving the check box deselected). By default, the device is not configured as a corporate-owned entity. The role associated with the device can be specified in this menu, but if there is a role specified for the detected device type (refer to [Configuring Domain Roles on page 96](#)), that role will take precedence.

 A screenshot of the 'Create Device' form. It contains the following fields and options:
 

- Name:** A text input field with a placeholder 'Name of device'.
- Address:** A text input field with a placeholder 'To create an OUI-based MAC address range, append ':%:%:%%'. For example, to put phones starting with the OUI of 00:90:7a into a determined role, use the MAC address '00:90:7a:%:%:%%'. Wildcard characters are only supported in the OUI range format.'
- Enable MAC Authentication:** A checked checkbox with the label 'Select to authenticate device to the network using its MAC address'.
- Role:** A dropdown menu currently set to 'Guest'.
- Accounting server:** A dropdown menu.
- Corporate owned:** An unchecked checkbox with the label 'Select to mark device as corporate issued for Device Reassignment Rules configured in the client's initial role. The client's initial role is determined based on authentication, but clients can be immediately reassigned to another destination role based on the Device Type, Ownership and Destination Role configured in the rules. For Example if Device Type is iPhone and Ownership is corporate then role is Corporate.'

 At the bottom of the form, the 'Create Device' button is circled in red.

- Select **Create Device**. A confirmation is displayed indicating that the device has been created. The device will now appear in the device list (**Configuration** tab, **Internal Authentication** > **Devices**), where you can display, edit, or delete the device.
- The device will now be authenticated using device authentication.



#### NOTE

*In vWLAN, 802.1X authentication can override device authentication. So, if you match device authentication, and then complete 802.1X authentication, your role is determined by RADIUS 1X and not the MAC device.*

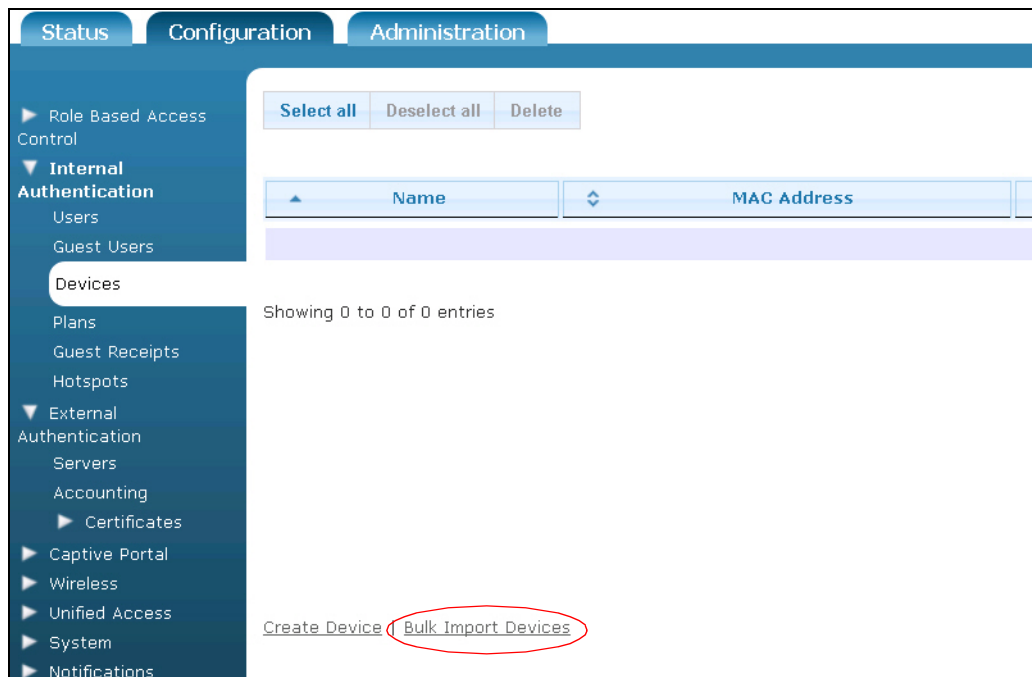
## Bulk Import of Devices

In addition to adding devices to vWLAN one at a time, you can optionally choose to import several devices at one time using the bulk import option. This option imports a CSV file that should include the device name, MAC address, assigned role, and associated accounting server (optional). For example, the CSV file should look like the following:

```
filename19,00:0c:22:55:b0:13,5,2
filename20,00:0c:22:55:b0:14,5
filename21,00:0c:22:55:b0:15,5,2
filename22,00:0c:22:55:b0:16,5,2
filename23,00:0c:22:55:b0:17,5,2
filename24,00:0c:22:55:b0:18,5,2
```

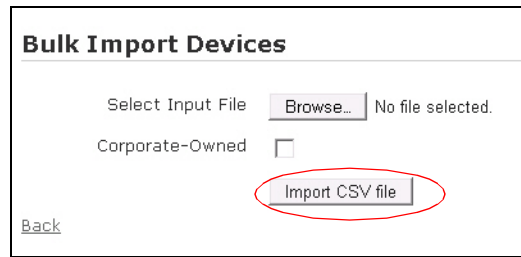
To import a CSV file of devices, follow these steps:

1. Navigate to the **Configuration** tab, and select **Internal Authentication > Devices**. Select **Bulk Import Devices** at the bottom of this menu.



2. In the **Bulk Import Devices** menu, use the **Browse** button to locate the CSV file that contains the device information for the devices you are adding to vWLAN. Next, specify whether the devices are

corporate-owned or not by selecting the **Corporate-owned** check box. Select **Import CSV file** to import the file.



The screenshot shows a web interface titled "Bulk Import Devices". It contains the following elements:

- A "Select Input File" label followed by a "Browse..." button and the text "No file selected."
- A "Corporate-Owned" label followed by an unchecked checkbox.
- An "Import CSV file" button, which is circled in red in the image.
- A "Back" link in the bottom left corner.

3. The imported devices will now appear in the device list (**Configuration** tab, **Internal Authentication > Devices**).

## Configuring Domain Accounting

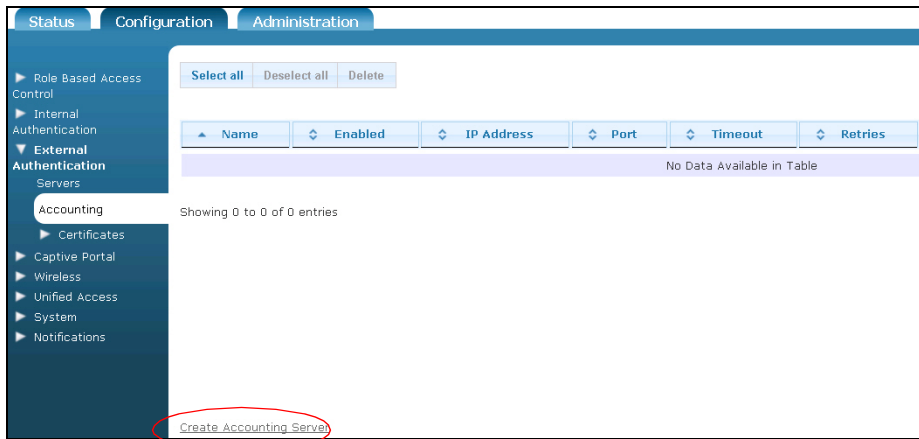
RADIUS accounting can be used to notify external systems about user's usage of the vWLAN system. When a client is authenticated, and joins the vWLAN system, a start request is sent to the accounting server. After a timeout period, when the client leaves the vWLAN system, a stop request is sent to the accounting server. Interim records can also be sent in periodic intervals, so that the external system can track vWLAN users at intervals. This can be helpful in tracking users that stay logged into the system for extended periods of time. To use accounting servers with vWLAN, you must configure the accounting server and then associate the server with one of the methods of authentication; RADIUS 802.1X, RADIUS web, LDAP, or SIP2 authentication servers, or local or MAC authentication. Accounting can also be used for a client that is assigned a default role using an SSID or unified access group by selecting the server in the SSID or unified access group configuration.

When configuring a RADIUS accounting server to use with vWLAN, note that the standard RADIUS accounting attributes apply, as well a vendor-specific attribute under the vendor code (**9967**).

To configure a RADIUS accounting server in vWLAN, follow these steps:

1. Navigate to the **Configuration** tab, and select **External Authentication > Accounting**. Any previously configured accounting servers will be listed in the menu. If you want to edit a previously created accounting server, select the server name from the list. To create a new accounting server,

either select **Create Accounting Server** at the bottom of this menu, or select **Domain Accounting Server** from the **Create** drop-down menu (at the top of the menu).



2. Enter the name of the server, the server's IP address, and the port used by the server (**1813** by default) in the appropriate fields. Enable the server by selecting the **Enabled** check box.

**Create Accounting Server**

Name

Enabled

IP Address

3. Enter the shared secret for the accounting server, and the shared secret confirmation, in the appropriate fields.

Shared Secret

Shared Secret Confirmation

4. Specify the server timeout value (in seconds), and the number of times vWLAN will attempt to reconnect to the server in the appropriate fields. By default, the timeout value is set to **5** seconds, and the number of retries is set to **5**.

Timeout

Retries

5. Enable interim reporting updates by selecting the **Interim updates enabled** check box. Additionally, specify the interim update interval (in seconds) by entering a value in the appropriate field. By default, the interim update interval is set to **300** seconds.

Interim Updates Enabled

Interim Update Interval In Seconds

6. Select **Create Accounting Server** to create the server. A confirmation is displayed indicating that the server has been created. The server will now appear in the accounting server list (**Configuration** tab, **External Authentication** > **Accounting**), where you can display, edit, or delete the server.
7. Once the accounting server has been created, you can associate the server with an authentication method, SSID, or AP. Refer to [Configuring Web-based \(Captive Portal\) Authentication on page 107](#), [Configuring an SSID on page 188](#), or [Configuring AP Templates on page 149](#) for information about associating an accounting server with authentication, SSID, or AP.

## Configuring Domain Settings

In addition to configuring the authentication method used by the vWLAN domain, you can also specify certain actions based on whether users or devices are authenticated or not. These actions include automatic redirection (post-login redirect), the default URL that is displayed to authenticating users (post login redirect URL), the maximum number of authentication logs to store, the redirect behavior for HTTPS

traffic of un-registered clients, and the timeout values for internal status updates, inactive connection drops (idle timeouts), and AP control channel timeouts. To alter these settings, follow these steps:

1. Navigate to the **Configuration** tab, and select **System** > **Settings**. Select the **Domain** tab. All settings listed in the menu are included in the vWLAN by default. You cannot create new settings or delete the existing settings for the domain here, but you can edit them. To edit an authentication setting, select the setting name label from the list.

The screenshot shows the Configuration page with the Domain tab selected. A table lists various settings for the domain. The table has three columns: Name, Value, and Hint. The settings are as follows:

Name	Value *	Hint
<a href="#">Aggressive DHCP Lease Time for Un-registered Clients</a>	Disabled	An aggressive lease time brings clients on faster after authentication, but may not be compatible with all handheld devices.
<a href="#">Allow the AP to look up the vWLAN name using a DNS PTR record?</a>	Enabled	This must be enabled if redirect to hostname is enabled.
<a href="#">AP Control Channel Timeout</a>	900	Time in seconds before APs reboot if control channel is confirmed to be lost to the vWLAN (defaults to 1 hour - meaning, APs would reboot an hour after confirming that the control channel has been lost)
<a href="#">Post Login Redirect</a>	Disabled	If enabled, users will be redirected to the Post Login Redirect URL after web based authentication instead of their original destination.
<a href="#">Post Login Redirect URL</a>	http://www.adtran.com	The Post Login Redirect URL is the URL that the user will be redirected to after web based authentication instead of their original destination.
<a href="#">Redirect HTTPS traffic for Unregistered clients</a>	Disabled	Redirects HTTPS to the captive portal
<a href="#">Time in minutes between updating internal status (minimum 15)</a>	15	Updates the bandwidth reading
<a href="#">Time in seconds before inactive connections are dropped</a>	600	Inactive connections will be dropped once this time out has been reached.

Showing 1 to 8 of 8 entries

2. The aggressive DHCP lease time setting, used to reconnect clients quickly after authentication, can be enabled or disabled from this menu. By default, aggressive DHCP lease time for unregistered clients is disabled. When enabled, it speeds up web authentication, although it may not be compatible with all handheld devices. To enable this setting, select **Aggressive DHCP Lease Time**

for **Un-registered Clients** from the list and select **Enabled** from the drop-down menu. Select **Update Domain Setting** to apply the change.

**Edit Domain Setting**

Aggressive DHCP Lease Time For Un-registered Clients Enabled ▾

*An aggressive lease time brings clients on faster after authentication, but may not be compatible with all handheld devices.*

Update Domain Setting

[Show](#) | [Back](#)

- By default, an AP looks up the vWLAN name using a DNS pointer record (PTR) when redirecting clients to a host name for authentication. This setting must be enabled when redirection to a host name is enabled. To disable this setting, select **Allow the AP to look up the vWLAN name using a DNS PTR record** from the list and select **Disabled** from the drop-down menu. Select **Update Domain Setting** to apply the change.

**Edit Domain Setting**

Allow The AP To Look Up The vWLAN Name Using A DNS PTR Record? Disabled ▾

*This must be enabled if redirect to hostname is enabled.*

Update Domain Setting

[Show](#) | [Back](#)

- The AP control channel timeout is the time, in seconds, before an AP reboots if the control channel is lost. By default, this value is set to **14,400** seconds, indicating the AP reboots four hours after confirming that the control channel is lost. To change this value, select **AP Control Channel Timeout** from the list, and enter a new value in the **Value** field. The maximum value that can be set is **4294967295** seconds. Select **Update Domain Setting** to apply the change.

**Edit Domain Setting**

AP Control Channel Timeout

*Time in seconds before APs reboot if control channel is confirmed to be lost to the vWLAN (defaults to 0, meaning APs reboot immediately after confirming the control channel is lost)*

Update Domain Setting

[Show](#) | [Back](#)

**i** **NOTE**

*If you have a standby SSID configured, you cannot make this value non-zero. Standby SSIDs and this feature are not compatible. If you want to use this field, you must delete all Standby SSIDs.*

- The automatic redirect of users (post-login redirect) is disabled by default. To enable the post-login redirect feature, select **Post Login Redirect** from the list, and select **Enable** from the drop-down menu. If automatic redirect is enabled, upon successful captive portal authentication, users are redirected to the Post Login Redirect URL, rather than their original destination. For example, you

can redirect users to [www.adtran.com](http://www.adtran.com) rather than their home page after successful authentication. Select **Update Domain setting** to apply the change.

**Edit Domain Setting**

Post Login Redirect

*If enabled, users will be redirected to the Post Login Redirect URL after web based authentication instead of their original destination.*

[Show](#) | [Back](#)

6. The default URL for redirected users is their original URL if post-login redirect is not enabled (see above). If post-login redirect is enabled, then the user is instead sent to the Post Login Redirect URL (<http://www.adtran.com> by default). To change this URL, select **Post Login Redirect URL** from the list and enter the new URL in the field. This new value becomes the URL to which users are redirected upon successful authentication when automatic redirect is enabled. Select **Update Domain setting** to apply the change.

**Edit Domain Setting**

Post Login Redirect URL

*The Post Login Redirect URL is the URL that the user will be redirected to after web based authentication instead of their original destination.*

[Show](#) | [Back](#)

7. By default, un-registered clients' HTTPS traffic is not redirected. For example, a user with the home page set to a secure HTTPS banking page will not be redirected when this feature is disabled. To enable the redirection of HTTPS traffic for un-registered users, select **Redirect HTTPS traffic for Unregistered clients** from the list, and select **Enable** from the drop-down menu. Enabling this feature redirects HTTPS traffic to the captive portal. Select **Update Domain setting** to apply the change.

**Edit Domain Setting**

Redirect HTTPS Traffic For Unregistered Clients

*Redirects HTTPS to the captive portal*

[Show](#) | [Back](#)

8. By default, the time between internal status updates is **15** minutes. This time interval is how quickly bandwidth updates are sent to the GUI or reports. To change this setting, select **Time in minutes between updating internal status** from the list, and enter a new value in the **Value** field. Updating

this value changes the time (in minutes) between internal status updates, which updates the bandwidth reading. Select **Update Domain setting** to apply the change.

**Edit Domain Setting**

Time In Minutes Between Updating Internal Status  
(minimum 15)

*Updates the bandwidth reading*

[Show](#) | [Back](#)



### CAUTION!

*ADTRAN recommends that you do not change this setting as the dashboard data will be impacted.*

- By default, the time before an inactive connection, or idle timeout (defined as having no wireless association to any AP), is dropped is **600** seconds. This timeout counter begins after a client is no longer associated with an AP. To edit this setting, select **Time in seconds before inactive connections are dropped** from the list, and enter a new value in the **Value** field. The default value is **10** minutes, and this value cannot be set for less than **1** second. If set to 1 second, any disconnected users are immediately dropped. This can be useful when logging out unified access users during a reboot of the computer. Updating this value causes inactive connections to be dropped when the time limit has been reached. Select **Update Domain setting** to apply the change.

**Edit Domain Setting**

Time In Seconds Before Inactive Connections Are  
Dropped

*Inactive connections will be dropped once this time out has been reached.*

[Show](#) | [Back](#)

## Configuring Domain Users

Domain users are those users that connect to the specific domain to access the vWLAN. User configuration at the domain level entails mapping these users to specific roles, such as guest, or another configured user role (refer to [Configuring Domain Roles on page 96](#) for user role information). Mapping users to a role is basically defining the role of this user. The procedure for mapping users to roles is the same as configuring a user (refer to [Configuring Local User Authentication on page 126](#)). You can either create new users and assign a role to them, or you can edit the roles of existing users.



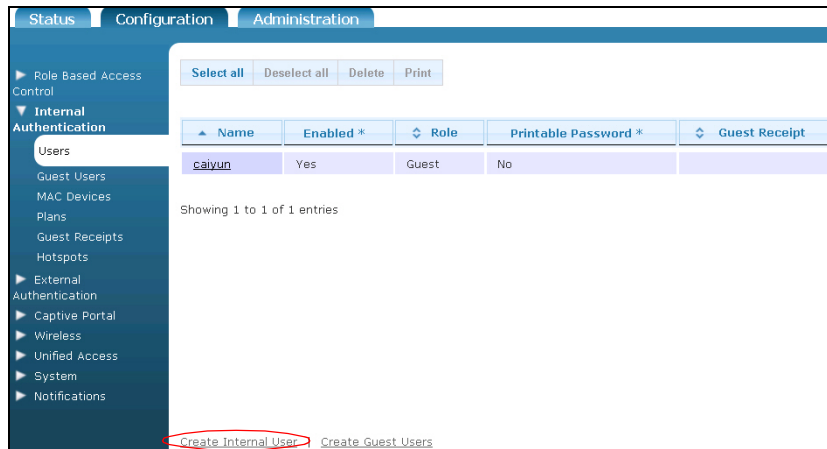
### NOTE

*Any edits made to the role currently assigned to the user are not applied until the next time the user logs in.*



To map users to a domain role, follow these steps:

1. Navigate to the **Configuration** tab, and select **Internal Authentication > Users**. Any previously configured users will be listed in the menu. If you want to edit a previously created internal user (in order to map them to a specific role), select the user name from the list. To create a new internal user, either select **Create Internal User** at the bottom of this menu, or select **Domain Internal User** from the **Create** drop-down menu (at the top of the menu).



2. In the **Create Internal User** menu, enter the user's name and password in the appropriate fields. Enable the user by checking the **Enabled** check box. Then specify the user's role by selecting the appropriate role from the **Role** drop-down menu. Role selection depends on which roles you have previously created (refer to [Configuring Domain Roles on page 96](#)). Optionally, associate an accounting server with this user using the **Accounting server** drop-down menu. Next, specify how many users can authenticate simultaneously by entering a value in the appropriate field. If you specify 0, there is no limit to how many users can authenticate simultaneously. Lastly, specify whether the user account will expire by selecting the **Never expire** check box.

### Create Internal User

Name:

Password:

Password Confirmation:

Enabled:

Role:

Accounting Server:

Simultaneous User Authentication:   
*0 is unlimited.*

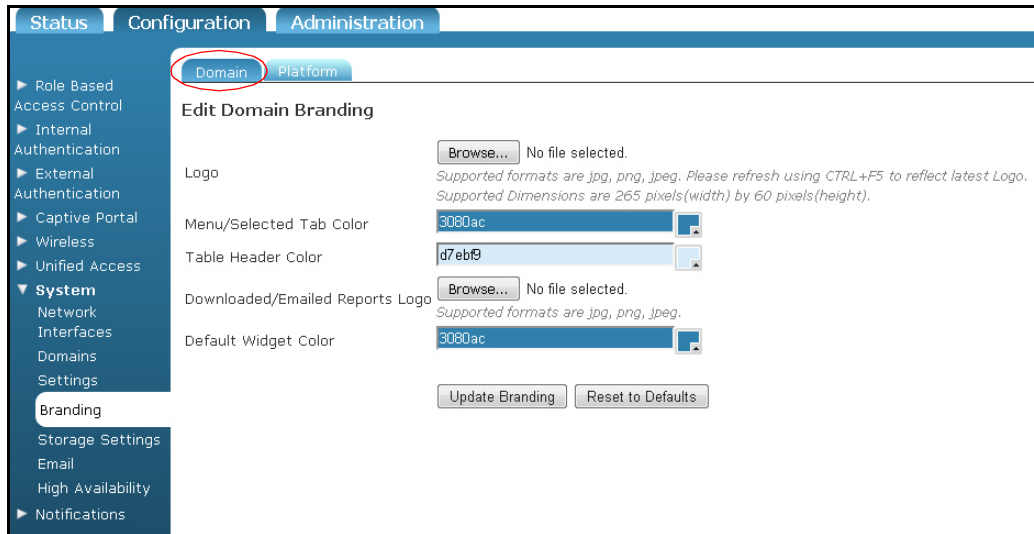
Expire User:  Never expire

3. Select **Create Internal User**. A confirmation is displayed indicating that the user has been created. The user will now appear in the internal user list (**Configuration** tab, **Internal Authentication > Users**), where you can display, edit, or delete the user.

## Configuring Domain Branding

In vWLAN release 2.9, the option to brand the domain was added. This feature allows you to add logos or change the colors of the domain menus, tables, or widgets. The default domain branding settings are configured using the vWLAN platform branding settings (refer to [Configuring vWLAN Platform Branding on page 59](#)). To access the domain branding, and change the default domain branding settings, follow these steps:

1. Navigate to the **Configuration** tab, and select **System > Branding**, and then select the **Domain** tab.



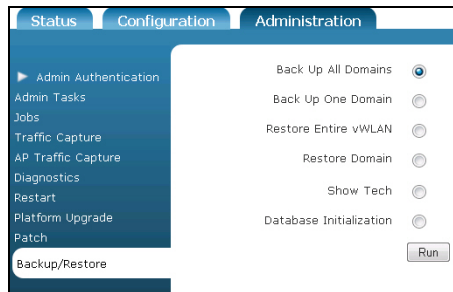
2. In the **Edit Domain Branding** menu, add any logos to the domain by uploading a logo file. Supported file formats are **.jpg**, **.png**, or **.jpeg**. Domain logo file sizes are 265 pixels (width) by 60 pixels (height). You can preview domain logos by selecting **CTRL+F5**.
3. Specify the colors for domain menus, tables, and widgets by selecting the appropriate colors in the menu, table, or widget fields.
4. Optionally specify the branding a logo for downloaded or emailed reports by uploading your own logo from a file. Supported file formats are **.jpg**, **.png**, or **.jpeg**.
5. Once you have uploaded all files and made your color selections, select **Update Branding** at the bottom of the menu to apply the changes. You can also reset branding to the default settings if necessary by selecting **Reset to Defaults**.

## Domain Configuration Backup

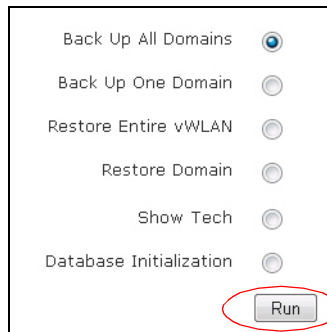
It is a good idea to back up the domain configuration periodically, in order to restore the system should an outage or some other unforeseen event occur. Domain backups can only be completed by platform administrators with read and write permissions (refer to [Specifying the Administrator's Role on page 47](#)).

To backup the domain configuration, follow these steps:

1. Navigate to the **Administration** tab, and select **Backup/Restore**.



2. Select the domain or domains that you want to backup by selecting the button next to the appropriate option. You can also choose to restore the domain or the entire vWLAN, save technical information about vWLAN, or initialize the vWLAN database. After making your selection(s), select **Run** to begin the backup or restore process.



## 8. Configuring vWLAN APs

vWLAN AP configuration is necessary so that the APs can communicate properly with the vWLAN instance, and so that any users or devices that are communicating with the APs are monitored and authenticated properly. AP configuration includes editing AP firmware, associating APs to a domain, connecting the AP to the cloud network using AP discovery, licensing the AP, configuring AP templates, and performing AP asset management. In addition, instructions are included in the following sections for displaying APs, managing AP configuration states, and resetting AP configuration. This chapter includes the following sections:

- [Editing AP Firmware on page 140](#)
- [Associating APs with a Domain on page 145](#)
- [Using AP Discovery to Connect APs to vWLAN on page 147](#)
- [Licensing APs on page 148](#)
- [Configuring AP Templates on page 149](#)
- [Configuring Additional AP Settings on page 165](#)
- [Viewing APs on page 168](#)
- [Viewing AP States on page 170](#)
- [Resetting and Rebooting APs on page 171](#)
- [Configuring AP Jobs on page 173](#)

### Editing AP Firmware

Upon first connecting the vWLAN, APs will upgrade their firmware to ensure they have the latest version. New firmware can be uploaded directly to the vWLAN using locally stored firmware, or you can choose to upgrade using firmware stored on an external server. When new firmware is uploaded to the vWLAN, you can apply it to the APs on specific domains by applying the firmware change to the default AP template or to a specific AP template. The administrator still must choose to apply the upgrade to the AP after the firmware upgrade is complete by either using an **Admin Task** or rebooting the AP (refer to [Performing System Maintenance on page 61](#)). Instructions for uploading both cloud-based and locally stored firmware are described in the following sections.

### Uploading Locally Stored Firmware

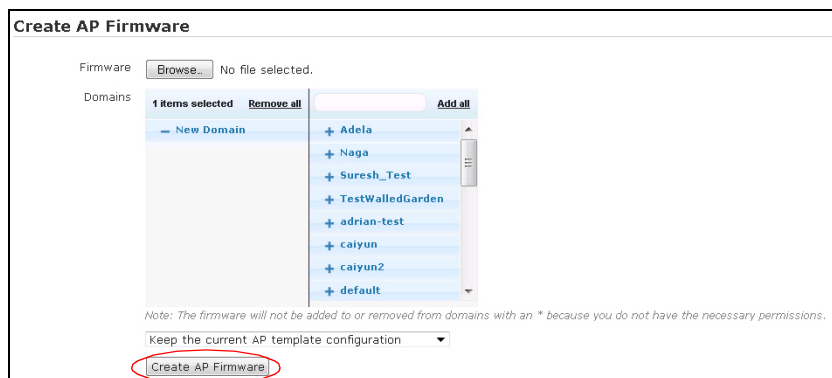
To upload or edit locally stored AP firmware manually, follow these steps:

1. Navigate to the **Configuration** tab, and select **Wireless > AP Firmware**. 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. Any previously configured APs will be listed in the menu. If you want to edit a previously configured AP, select the AP from the list. To upload new AP firmware, either select

**Create AP Firmware** at the bottom of this menu, or select **Domain AP Firmware** from the **Create** drop-down menu (at the top of the menu).



- Select the new firmware file from the location in which you stored the downloaded firmware by selecting **Browse**. Then, 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. Lastly, choose the template to which to apply the firmware change, or select **Keep Current AP Configuration** from the drop-down menu.

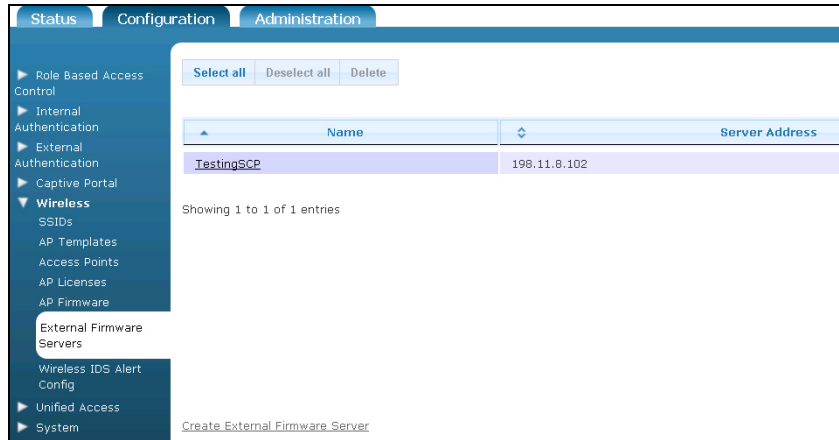


- Select **Create AP Firmware** (or **Update AP Firmware** if editing) to apply the changes. A confirmation is displayed indicating that the AP firmware has been successfully created or updated.
- Apply the new or updated firmware to the AP by applying the firmware to an AP template (refer to [Configuring AP Templates on page 149](#)) or rebooting the AP (refer to [Resetting and Rebooting APs on page 171](#)).

## Uploading Firmware Stored on a Server

To upload or edit AP firmware stored on a server, you must first upload the firmware to vWLAN (as described in [Uploading Locally Stored Firmware on page 140](#)) and to the remote server. Once the firmware has been uploaded to vWLAN, follow these steps:

1. Navigate to the **Configuration** tab, and select **Wireless > External Firmware Servers**. If you are going to edit previously uploaded firmware, select server from the list that you want to update with new firmware. To add a new firmware server, select **Create New External Firmware Server** from this menu, or **Domain External Firmware Server** from the **Create** drop-down menu (at the top of the menu).



2. In the **Create External Firmware Server** menu, enter the server name and IP address in the appropriate fields. If you are using an 1800 Series AP, this is all the configuration required and you can proceed to Step 4. If you are using a 1900 Series AP, continue to Step 3.

The screenshot shows the 'Create External Firmware Server' form. It is divided into two sections: '18xx APs - TFTP' and '19xx APs - SCP'. The '18xx APs - TFTP' section has fields for 'Name' (1925 Firmware Server) and 'Server Address' (192.168.3.1), which are highlighted with a red box. The '19xx APs - SCP' section has fields for 'Server Port' (22), 'SCP Username' (root@adtran.com), 'SCP Password' (masked with dots), 'SCP Password Confirmation' (masked with dots), and 'Firmware File Path'. A note below the 'Firmware File Path' field states: 'The system will upload the firmware file from the configured SCP user's home directory unless otherwise specified.' At the bottom, there is a 'Create External Firmware Server' button and a 'Back' link.

3. If you are using a 1900 Series AP, enter the SCP server port, user name, password, and password confirmation in the appropriate fields. By default, the external server will use port **22** for communication. In addition, enter the file path used to locate the firmware on the server in the **Firmware File Path** field. If no path is specified, the home directory is used.

**Create External Firmware Server**

**18xx APs - TFTP**

Name:

Server Address:

**19xx APs - SCP**

Server Port:   
Server Port will be set to 22 if left blank. The firewall should be configured to allow SCP traffic.

SCP Username:

SCP Password:

SCP Password Confirmation:

Firmware File Path:   
The system will upload the firmware file from the configured SCP user's home directory unless otherwise specified.

[Back](#)

4. Once you have entered the information, select **Create External Firmware Server** (or **Update External Firmware Server**) to apply the changes. A confirmation is displayed indicating that the firmware server has been successfully created, and the server will now appear in the firmware server list (**Configuration** tab, **Wireless** > **External Firmware Servers**).
5. Apply the new firmware to an AP using an AP template (refer to [Configuring AP Templates on page 149](#)) or by rebooting the AP (refer to [Resetting and Rebooting APs on page 171](#)).

## Troubleshooting AP Firmware

In a typical firmware upload, vWLAN first determines the hardware type to which the firmware pertains, it finds the appropriate secure key to read the header and other information stored with the firmware, and it composes a filename with the proper format to apply to an AP. vWLAN throttles the number of simultaneous firmware downloads, so it will assume a download slot is available. Otherwise, the AP is held until an open download slot is free. If an AP is not functioning properly, verify that the AP has the correct firmware. The following cases outline vWLAN and AP behavior when dealing with firmware.

### AP Connects to System But Does Not Have Correct Firmware

If an AP connects to the vWLAN system, but does not have the correct firmware, the AP's state will transition from down or unknown (in the domain, but booting) to an upgrading state. vWLAN will automatically download the proper firmware, upgrade the AP, and reboot the AP. Note that in this case, the AP will not have configured radios, service clients, etc.

### AP is Running and Firmware is Upgraded

When an AP is running, and a firmware upgrade has begun, the AP moves into an upgrading state. For an 1800 Series AP, this means the AP will upgrade the firmware, reboot as necessary, and return to an up state when ready for service. For a 1900 Series AP, this means that even while the AP is downloading new firmware, the AP radios remain functional and allow clients to access the network. The 1900 Series APs will enter a pending upgrade state, which indicates the AP has successfully received the new firmware image. The administrator must then complete the upgrade manually on the AP selecting **Admin Tasks** (this allows the AP to upgrade while continuing to service clients). All other commands to the AP are blocked until the firmware upgrade has been completed by the administrator.

## AP Firmware Matches the Alternative Partition Firmware

Whether an AP is connecting to vWLAN for the first time or the firmware is changed while the AP is running, if the firmware supplied matches the alternative partition firmware, then no download takes place.

## Interruptions During Upgrade

If any interruptions occur during a firmware upgrade, the AP might be affected. For an 1800 Series AP, the system will reboot the AP, or the administrator must reboot the AP. For a 1900 Series AP, however, each type of interruption is handled differently. 1900 Series AP firmware download interruptions are discussed below.

If the firmware download fails, which can occur if the firewall is blocking SCP traffic, you will see an error message that the firmware cannot be downloaded. In this case, the AP continues to function and waits for the administrator to reissue the upgrade after the issue has been remedied.

If the firmware is invalid, you will see a message indicating the firmware is invalid. In this case, the AP continues to function and waits for the administrator to reissue the upgrade after the issue has been remedied.

If the control channel is lost during the firmware download and no failover exists, then vWLAN moves the AP from the upgrading to the down state and frees the download slot. When the control channel is restored, the AP begins the download again and is automatically upgraded.

If the control channel is lost during the firmware download and a failover exists, then vWLAN moves the AP from the upgrading to the down state and frees the download slot. When the control channel is restored, if the vWLAN platforms are in sync, then the AP begins the download again and is automatically upgraded. If the vWLAN platforms are not in sync, then no changes are made until the units are synced again.

If the AP crashes or loses power during a firmware download, then vWLAN moves the AP from the upgrading to the down state and frees the download slot. When the AP is powered again, and connects to the control channel, the AP begins the download again and is automatically upgraded.

## Simultaneous Firmware Upgrades

Due to overhead, vWLAN prevents more than a specific number of APs from downloading firmware images at the same time. To accommodate for this, vWLAN counts the number of APs that are upgrading, and does not send an upgrade command to additional APs until the first APs are finished downloading the firmware.

## Newer AP Firmware

If the uploaded AP firmware is new, then it is possible the encryption has changed. In this case, a patch may be needed for vWLAN to support the new firmware. If the patch is not installed, then the firmware is treated as invalid until the proper patch is uploaded. Refer to [Performing System Maintenance on page 61](#) for information about installing patches.



## Associating APs with a Domain

After APs are discovered, they must be associated with a domain. To associate an AP with a domain, follow these steps:



### NOTE

*If you are an administrator with domain permission only, APs are not displayed under the **Status** or **Wireless** > **AP Licenses** menus until you upload an AP license. Licensing the AP assigns it to your domain. Administrators with platform permissions can see the APs displayed in the **Wireless** > **AP Licenses** menu, and can license and assign APs to a domain.*

1. Navigate to the **Configuration** tab, and select **Wireless** > **AP Licenses**. Select the **Platform** tab. Any previously configured APs will be listed in the menu. To associate one of these APs to a specific domain, select the APs you want to associate with a domain by selecting the AP name from the list (the selected APs will be highlighted in blue), and then selecting the appropriate domain from the drop-down menu in the bottom left of the page.

The screenshot shows the vWLAN Administrator's Guide interface. The 'Configuration' tab is active, and the 'Wireless' > 'AP Licenses' menu is selected. The 'Platform' sub-tab is chosen. A table lists APs with columns for Serial Number, MAC Address, IP Address, Domain, Firmware, Country, and vWLAN License. A dropdown menu 'Move AP(s) to domain' is highlighted with a red circle. Below the table, there is an 'Upload AP Licenses' button and a note: 'To select individual APs, click on the AP row, and it will change to a darker color, indicating the AP is selected. APs will not operate until they are moved into a domain.'

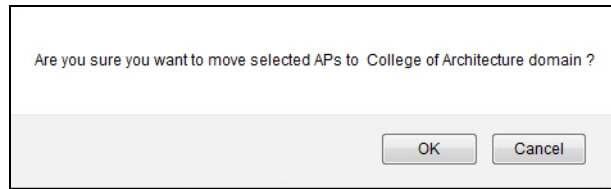
Serial Number	MAC Address	IP Address	Domain	Firmware *	Country *	vWLAN License *	
180113309040309	00:19:92:03:0d:40	192.168.102.235	caiyun	6.8.0-9	United States	Lifetime	Lifet
18021234567890			default		United States	Lifetime	Non
18022413040336			vikram_test		United States	Lifetime	Non
18022413040466			vikram_test		United States	Lifetime	Non
18023811040218	00:19:92:0a:5f:40		TestWalledGarden		United States	Lifetime	Lifet
18023811040999			default		Australia	Lifetime	Lifet
18024012040193			vikram_test		United States	Lifetime	Non
18024012040196			vikram_test		United States	Lifetime	Non
18024012040376	00:19:92:10:0f:40		vikram_test		United States	Lifetime	Non
18403309040352	00:19:92:03:12:a0		default		United States	Lifetime	Lifet
18409000000200	00:93:00:c8:a0:00		vEdgeSimDomain1		United States	Lifetime	Lifet



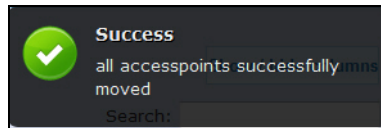
### NOTE

*APs must have a valid country and a vWLAN license in order to be moved to a domain.*

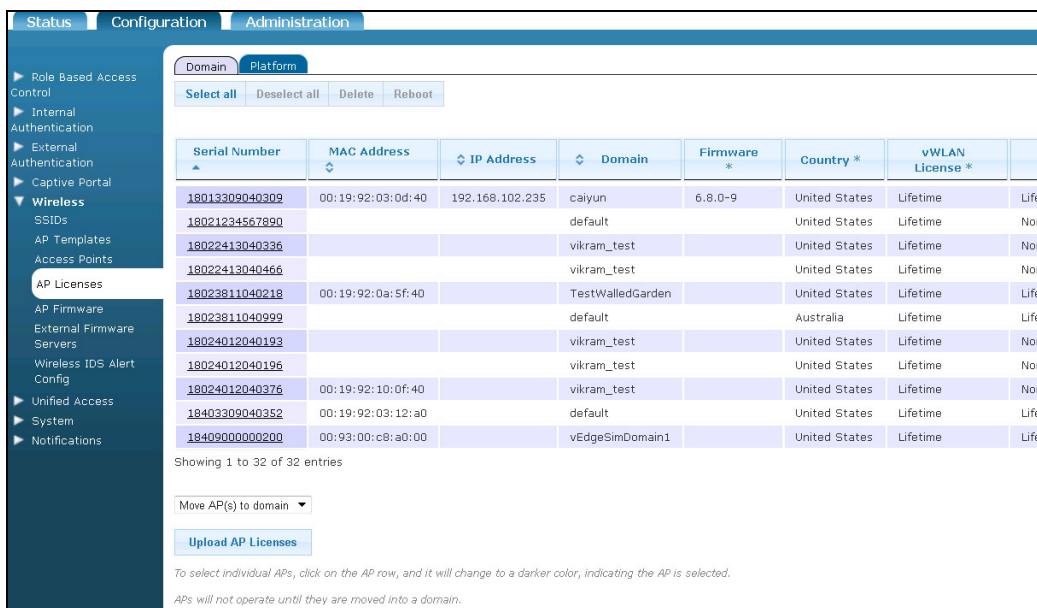
- At the prompt, select **OK** to change the domain of the APs.



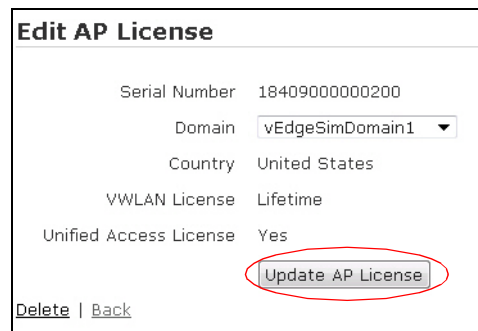
- A success message is displayed when the APs have been moved to the specified domain.



- The previous method for changing AP domains is suited for the movement of APs on a large scale. If you are only changing one AP domain, you can use the previous method, or alternatively, you can navigate to the **Configuration** tab, select **Wireless > AP Licenses**, select the **Platform** tab, and then select the AP from the list whose domain you want to change.



- Select the appropriate domain from the **Domain** drop-down list, and select **Update AP License**.



6. A confirmation message is displayed indicating the change was applied to the AP.
7. Either method you choose will update the AP(s) and their domains. If you upload the license at the **Domain** tab instead, the licensed APs are automatically moved into the proper domain.

## Using AP Discovery to Connect APs to vWLAN

The APs used in vWLAN use a process called AP discovery to automatically connect to the vWLAN network. When APs are installed, a few items must be specified in your network to facilitate the AP discovery process. Certain protocols must be allowed to pass between the AP and vWLAN for successful AP discovery and authentication. You can find the complete list of protocols that must be allowed in [Software Requirements on page 26](#). Keep these requirements in mind when configuring your firewall and any access control lists (ACLs).

### AP Discovery Process

The AP discovery process is based on an algorithm that attempts various discovery methods in a specific order. First, the process determines whether there is a static vWLAN configuration. If not, the algorithm determines whether DHCP vendor Option 43 is enabled. If nothing is found, the algorithm moves to the last step, which is to check for cached vWLAN configuration information.

The network component that can be configured to facilitate AP discovery is an external DHCP server. The server is configured to dispense IP addresses to APs and associated clients. When configuring a DHCP server, make sure to configure the ADTRAN Bluesocket DHCP vendor option (Option 43). To receive a DHCP vendor option, the AP first identifies itself as a Bluesocket AP using the Option 60 vendor class identifier. DHCP requests from the AP contain this field as a DHCP option with the value **BlueSecure.AP1500** (regardless of the actual hardware model). The AP also includes Option 43 (vendor-specific information) in the **Option 55: parameter Request List**. The DHCP server will respond with the Option 43 vendor-specific information field. If you are using an ADTRAN router or switch in your network, you can configure the unit as a DHCP server with the appropriate vendor options.



#### NOTE

*For more information about configuring DHCP servers to function with vWLAN AP discovery, refer to the configuration guide [vWLAN Access Point Discovery](#), available online at <https://supportcommunity.adtran.com>.*

The AP can be statically provisioned with vWLAN information using the serial console menu through a serial connection, or using IP access through SSH. Refer to [vWLAN Serial Console Configuration on page 181](#) for more information about serial console configuration.

When the AP is connected to the vWLAN, it is configured with the default AP template. For more information about AP templates and their configuration, refer to [Licensing APs on page 148](#).

## Licensing APs

Each AP is licensed for certain features based on its serial number. The AP licenses are the only relevant licenses in vWLAN; there are no VMware licenses. The AP licenses specify which features are available on your AP, with features like unified access licenses licensed on a per AP basis.



### NOTE

*APs will not be displayed in the **Status** or **Wireless** menus until they are licensed. Uploading a license to a domain assigns the AP to that domain. Platform administrators can view the APs in the **Wireless > AP Licenses** menu, license them, move them to a domain, etc.*

## Obtaining AP Licenses

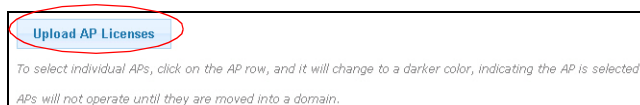
AP licenses are purchased by the customer, and are generated as a text file that is then sent to the customer. For new APs, these licenses come from the reseller or distributor. For replacement APs, the licenses will come from ADTRAN Customer Care. APs are initially in an unlicensed state. AP radios will not be operational until the AP is licensed by uploading the license file to vWLAN.

If a license was not received for a new AP, contact the reseller or distributor where the license was purchased. If a license was not received for a replacement AP on an RMA generated by ADTRAN, contact ADTRAN Customer Care at 888-423-8726 and reference the RMA number.

## Uploading License Files

Upload the license to the AP(s) by following these steps:

1. When the license file is returned from ADTRAN, you can upload the license file to vWLAN by navigating to the **Configuration** tab, and selecting **Wireless > AP Licenses**. Select the **Domain** tab if you are working with licenses for APs on a specific domain, or the **Platform** tab if you are working with licenses on the vWLAN platform and have permission to do so. Next, select **Upload AP Licenses** at the bottom of the menu.



2. Locate the appropriate license file returned to you from ADTRAN using the **Browse** button. Next, specify the domain to which the license file will apply from the **Domain** drop-down menu. Then select **Upload Licenses**.

3. If there are any errors, they will appear at the top of the form. After completing these steps, the licensing of the APs is complete. The next step in AP configuration is to configure the AP template(s).

## Configuring AP Templates

AP templates are templates used to configure multiple APs to the same parameters. Large installations or multi-site deployments of vWLAN require the ability to group APs to apply a similar configuration to them, which is accomplished in vWLAN by AP templates. Each template has its own unique configuration for settings, radios, firmware, and SSIDs. Each AP is associated to an AP template, and inherits the configuration contained within in the template. If an AP is moved to a different template, then the AP inherits the configuration from the new template. By default, each AP connected to the vWLAN is configured with a default template.

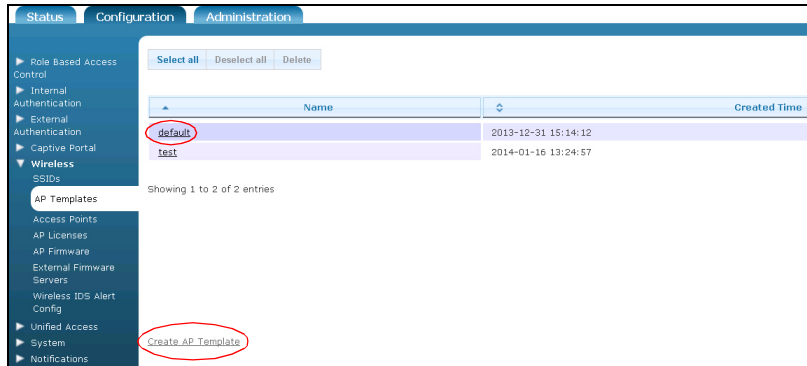
The settings for the default template are:

- Default login form is used.
- Radio modes are in AP mode.
- DynamicRF profile uses the **default** profile, which specifies DynamicRF mode as **Set Once and Hold**, with dynamic channel and transmit power configurations enabled.
- The 802.11b/g/n radio is set to the **802.11b/g/n** wireless mode, and the 802.11a/n/ac radio is set to the **802.11a/n/ac** wireless mode.
- There is no minimum transmit rate specified for either radio.
- 80 MHz mode is enabled on the 802.11a/n/ac radio only.
- Packet aggregation is enabled on both radios.
- The beacon interval for both radios is set to **200** ms.
- There are no SSIDs or access groups associated with the default AP template.
- The SSH password is **vWI@nBlu3\$ock3t**.
- The antenna mode is set to **3**.
- The DTIM value is set to **1**.
- The AP load maximum is set to **64**.
- The fragmentation threshold/RTS threshold is set to **2346**.
- Captive Network Assistant (CNA) is enabled.
- DFS is disabled.
- Layer 3 Mobility is enabled.
- Tunnel profile is disabled.

## Creating AP Templates

Depending on the role the AP will play in your vWLAN network, you might need to change the default template for the AP. You can create new templates and apply them to multiple APs. To create a new AP template and apply it to an AP, follow these steps:

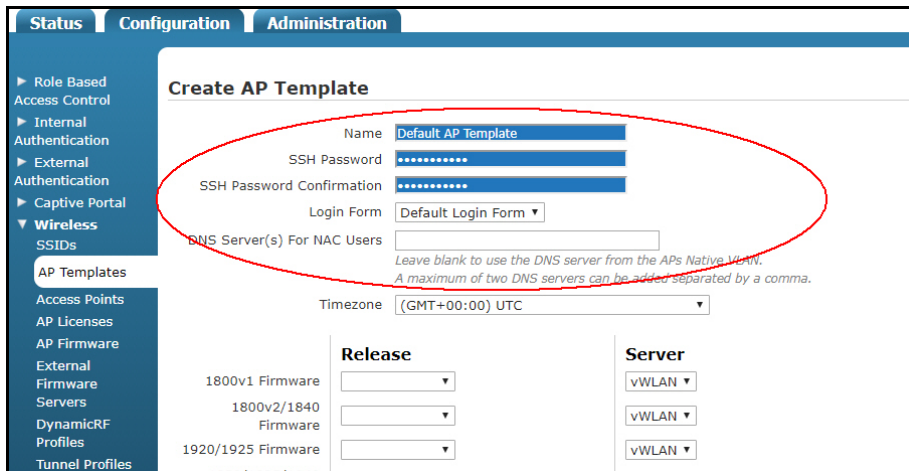
1. Navigate to the **Configuration** tab, and select **Wireless > AP Templates**. The first time you access this menu, the only AP template available in the default template. To create a new template, select **Create AP Template** at the bottom of the menu, or select **Domain AP Template** from the **Create** drop-down menu (at the top of the menu). If you would like to edit the default AP template, select the default template from the list and follow the steps below.



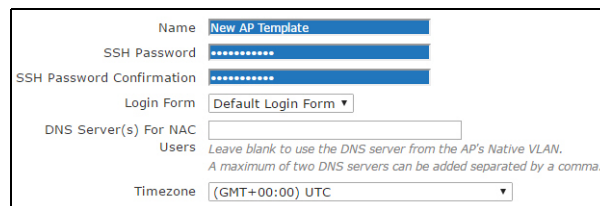
**NOTE**

*If you make changes to the default AP template, keep in mind that every AP using the default template will be affected, as well as any new APs added to the domain.*

2. Begin by entering the name, SSH password, login form, and DNS servers (for NAC and CNA users) for the template in the appropriate fields.



The SSH password is the password used to connect to the AP's serial console menu. The login form is the form used by clients when connecting to the AP (assuming it is not overridden at the SSID). You can choose the default login form, or select a custom form (refer to [Customizing vWLAN Login Forms and Images on page 207](#) for information about customizing login forms).



- Specify the timezone used by the APs associated with this template by selecting the appropriate option from the **Timezone** drop-down menu.

Timezone

- Specify the firmware used by the APs associated with this template. You can specify the firmware release version and the firmware location (vWLAN or an external server) using the drop-down menus.

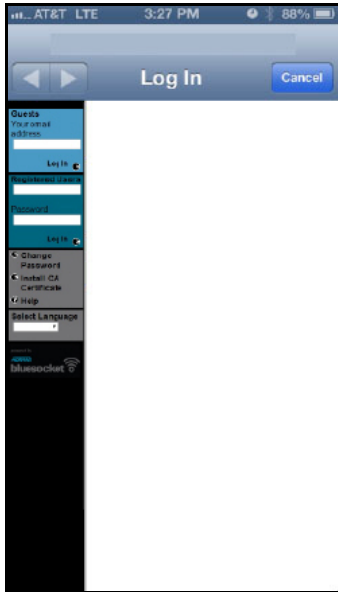
	Release	Server
1800v1 Firmware	<input type="text" value=""/>	<input type="text" value="vWLAN"/>
1800v2/1840 Firmware	<input type="text" value="2.9-M-255213"/>	<input type="text" value="vWLAN"/>
1920/1925 Firmware	<input type="text" value="2.9-M-255213"/>	<input type="text" value="vWLAN"/>
1930/1935/1940 Firmware	<input type="text" value="2.9-M-255213"/>	<input type="text" value="vWLAN"/>
2020 Firmware	<input type="text" value="2.9-M-255213"/>	<input type="text" value="vWLAN"/>
2030/2035/2135 Firmware	<input type="text" value="2.9-M-255213"/>	<input type="text" value="vWLAN"/>

- Next, specify whether Apple CNA and Microsoft Network Connectivity Status Indicator (NCSI) will be used. This option allows remote devices to store the credentials to networks requiring captive portal authentication so they do not have to be entered in manually every time they authenticate or reauthenticate to the network. By default, CNA is enabled on the AP template. To disable CNA, deselect the **Enable Captive Network Assistant** check box.

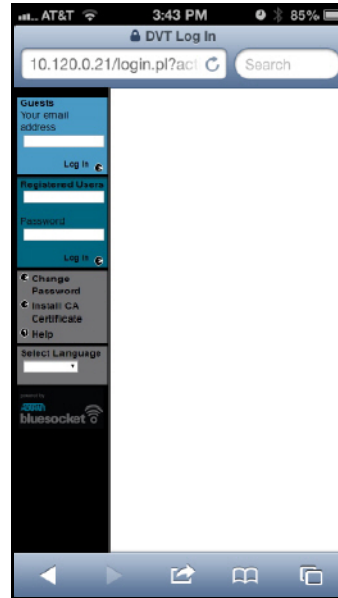
Enable Captive Network Assistant  *Check to enable Apple CNA or Microsoft NCSI.*  
*\*Requires Trusted Certificate on vWLAN.*  
*\*Requires redirect to hostname to be enabled in platform settings.*

When CNA is enabled, vWLAN responds to the device's CNA request with a redirection request to the vWLAN captive portal. The CNA device receives the redirection and detects that there is a captive portal in place. It then presents the CNA automatically and prompts the user to enter their credentials in the vWLAN login page. If CNA is disabled, the device will connect using a web request

which redirects to vWLAN captive portal. For Microsoft NCSI, an information popup appears at the bottom right corner of the computer suggesting the user open a web browser to authenticate.



Apple CNA with vWLAN captive portal (CNA enabled)



vWLAN captive portal using a web browser (CNA disabled)

For CNA to function properly, there are a few additional configuration steps that are required. Refer to [Configuring vWLAN for CNA Support on page 160](#) for specific CNA configuration instructions.

6. Specify whether to disable Layer 3 (L3) mobility. By default, L3 mobility is enabled which allows clients to roam without interruption across APs residing in different locations, as long as the APs are assigned to this template. If L3 mobility is disabled (by deselecting the check box), clients will be disconnected while roaming to and from APs in different locations. If both APs on which the client is roaming are in the same location, disabling L3 mobility will not interrupt roaming capabilities.



7. Next, specify whether APs associated with this template use DFS channels (5 GHz radio only). DFS channels are those channels that could be used by radar, and are thus scanned for the presence of radar before they are broadcast to connected clients. If radar is discovered on the DFS channel, the



AP disconnects from the channel and searches for other available channels free from interference. By default, DFS is disabled. Select the **Enable DFS** check box to enable the DFS feature.

Enable DFS	<input checked="" type="checkbox"/>
<i>Enabling DFS may result in a service disruption.</i>	



#### NOTE

*DFS can cause service interruptions when the AP is required to vacate a channel on which radar has been detected. In addition, this value is ignored if the AP hardware does not support DFS or if the value is not legal for the regulatory domain. For more information about DFS configuration, refer to the configuration guide [DFS in vWLAN](https://supportcommunity.adtran.com), available online at <https://supportcommunity.adtran.com>.*

8. Use the **Tunnel Profile** drop-down menu to specify whether to enable a tunnel profile. When a tunnel profile is enabled, all AP traffic is tunneled back to the central gateway specified by the tunnel profile. For more information about tunnel profiles, refer to [Configuring a Tunnel Profile on page 198](#).

Tunnel Profile	Disabled ▾
<i>Select a tunneling profile to enable tunneling of all traffic over GRE to a remote gateway. Enabling a tunneling profile automatically disables L3 mobility.</i>	



#### NOTE

*If a tunnel profile is enabled, Layer 3 Mobility automatically disables. In addition, there can be interactions between a tunnel profile and a defined user role. Refer to [Configuring a Tunnel Profile on page 198](#) for more information.*

9. Next, specify the radio mode for both radios in the AP by selecting the appropriate option from the **Radio Mode** drop-down menu. The radio modes are set independently for each radio. By default, the radio is set to **AP Mode**. You can choose one of the following settings:
- **Disabled** indicates the radio is disabled.
  - **AP Mode** (default) indicates the radio services clients in the 802.11 infrastructure mode.
  - **Sensor Mode** indicates the radio scans all channels, changing on the particular band at 100 ms intervals.
  - **AP/Sensor Mode** indicates the radio operates as an AP and a sensor using a time sharing algorithm. In this mode, when clients are not associated to the particular radio, the radio scans a different adjacent channel every second.
  - **AP/Sensor Client Aware Mode** indicates the radio operates in AP/Sensor Mode when clients are not present, but with added intelligence to change over to AP Mode when clients are present.
  - **Mesh Mode** indicates the radio is used for mesh networking. This option is only available on the 802.11a/n/ac radio. If the radio is configured in mesh mode, the **DynamicRF Profile** must have **DynamicRF Mode** set to **Set Once and Hold** on the mesh point, and no SSIDs or unified access groups can be specified for the mesh mode radio. For more information about configuring mesh networks in vWLAN, refer to the configuration guide [Mesh Networking in vWLAN](#), available online

at <https://supportcommunity.adtran.com>.

**i NOTE**

*If DFS is enabled, the mesh radio must still vacate channels with detected radar. This can cause mesh points to disconnect if the mesh portal detects radar or anything downstream of the mesh point to disconnect if radar is detected. vWLAN will attempt to move the mesh network to a new channel, but this may cause traffic disruption. For more information about DFS configuration, refer to the configuration guide [DFS in vWLAN](#), available online at <https://supportcommunity.adtran.com>.*

Per Radio Setting	
<b>Attribute</b>	802.11b/g/n (2.4 GHz)
Radio Mode	AP Mode
DynamicRF Profile	default
Wireless Mode	802.11b/g/n
Minimum Transmit Rate	No Minimum

802.11a/n/ac (5 GHz)	
Radio Mode	AP Mode
DynamicRF Profile	default
Wireless Mode	802.11a/n/ac
Minimum Transmit Rate	No Minimum

802.11a/n/ac is treated as 802.11a/n for 1800 and 1900 series APs.

**i NOTE**

*Dual mode for 1900 Series and 2000 Series APs acts as AP mode.*

10. Select the DynamicRF profile from the **DynamicRF Profile** drop-down menu. The **default** profile appears in this list, as well as any other profiles you have created. Make selections for both the 2.4 GHz and 5 GHz radios. DynamicRF profiles are created following the instructions outlined in [Configuring the DynamicRF Profile on page 162](#).

Per Radio Setting	
<b>Attribute</b>	802.11b/g/n (2.4 GHz)
Radio Mode	AP Mode
DynamicRF Profile	default
Wireless Mode	802.11b/g/n
Minimum Transmit Rate	No Minimum

802.11a/n/ac (5 GHz)	
Radio Mode	AP Mode
DynamicRF Profile	default
Wireless Mode	802.11a/n/ac
Minimum Transmit Rate	No Minimum

802.11a/n/ac is treated as 802.11a/n for 1800 and 1900 series APs.

11. Specify the wireless mode for each radio by choosing an option from the **Wireless Mode** drop-down menu. For the 802.11b/g/n radio, you can select from **802.11b**, **802.11g**, **802.11g/n**, or **802.11b/g/n**

(default) modes. For the 802.11a/n/ac radio, you can select from **802.11a**, **802.11a/n**, or **802.11a/n/ac** (2030/2035 Series BSAPs only).

Per Radio Setting	
<b>Attribute</b>	802.11b/g/n (2.4 GHz)
Radio Mode	AP Mode
DynamicRF Profile	default
Wireless Mode	802.11b/g/n
Minimum Transmit Rate	No Minimum

802.11a/n/ac (5 GHz)	
Radio Mode	AP Mode
DynamicRF Profile	default
Wireless Mode	802.11a/n/ac
<small>802.11a/n/ac is treated as 802.11a/n for 1800 and 1900 series APs.</small>	
Minimum Transmit Rate	No Minimum

- Specify the minimum transmit rate for each radio in the **Minimum Transmit Rate** drop-down menu. This setting specifies the required rate at which clients must be able to connect to the AP. If a client cannot connect at the specified rate, the AP will not allow the client to connect or to stay connected. The minimum transmit rate is set independently for each radio. Rate choices for the 802.11b/g/n radio are **1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54** Mbps. Rate choices for the 802.11a/n/ac radio are **6, 9, 12, 18, 24, 36, 48, or 54** Mbps. By default, no minimum transmit rate is specified.

Per Radio Setting	
<b>Attribute</b>	802.11b/g/n (2.4 GHz)
Radio Mode	AP Mode
DynamicRF Profile	default
Wireless Mode	802.11b/g/n
Minimum Transmit Rate	No Minimum

802.11a/n/ac (5 GHz)	
Radio Mode	AP Mode
DynamicRF Profile	default
Wireless Mode	802.11a/n/ac
<small>802.11a/n/ac is treated as 802.11a/n for 1800 and 1900 series APs.</small>	
Minimum Transmit Rate	No Minimum

**i** **NOTE**

*For the 2030 Series APs, any value specified is treated as **No Minimum**.*

- Specify the channel width for each radio using the drop-down menu. By default, the 802.11b/g/n radio is set to **20 MHz** and the 802.11a/n/ac radio is set to **40 MHz**. The 802.11b/g/n radio supports both **20 MHz** and **40 MHz** channel widths, while the 802.11a/n/ac radio supports **20 MHz, 40 MHz, and 80 MHz** channel widths. Enabling 40 MHz (Channel Bonding/HT 40) mode for each radio by selecting **40 MHz** from the drop-down menu. By default, 40 MHz mode is disabled on the 802.11b/g/n radio and enabled on the 802.11a/n/ac radio. Channel bonding is not recommended on the 2.4 GHz radio in enterprise deployments as there are only three non-overlapping channels. Channel bonding is only recommended on the 2.4 GHz radio in small office/home office (SOHO) deployments where there is only one AP deployed.

Minimum Transmit Rate	No Minimum	No Minimum
<small>For 3000 Series APs, any value is treated as 'No Minimum'.</small>		<small>For 2000/3000 Series APs, any value is treated as 'No Minimum'.</small>
Channel Width	20 MHz	40 MHz
<small>A value that is larger than the AP supports will be treated as the highest value the AP supports. If the secondary subchannel is not available, radio will automatically switch to smaller Channel Width settings.</small>		
Channel list	+	

**i NOTE**

*In order to use DFS channels in 40 MHz mode, the AP must monitor both channels in the pair for the presence of radar, and vacate both channels immediately if radar is detected on one of the channels. The same applies for the channels in 80 MHz mode. If the radio is set to 40 MHz mode, and a DFS channel without a 40 MHz pair is manually selected for the AP, the vWLAN system dials the AP back to 20 MHz mode for that AP.*

14. Channel list allows you to exclude channels in DFS and Dynamic RF. If DFS is enabled, you can optionally designate if special channels are used by the AP (such as channels that are only permitted on APs far enough away from weather radar or channels in some countries that are only permitted for indoor use). By default, all channels are included (if they are legal in the regulatory domain). To specify a channel to be excluded by the AP, select the minus sign to the left of the channel in the left-hand column. Move an excluded channel back to the included list by selecting the plus sign to the left of the channel in the right-hand column. If there are associated APs that are set with the channel, or use the channel for 40 MHz or 80 MHz mode, Dynamic RF will eliminate use of the specified channel the next time it runs.

Channel list

12 items selected **Remove all** **Add all**

- 5
- 6
- 7
- 8
- 9
- 10
- 12
- 13

+11

11 items selected **Remove all** **Add all**

- 36
- 40
- 44
- 48
- 52
- 60
- 64
- 149

+56

Channels in the left portion of the select box are included while channels in the right portion are excluded.  
 Included channels are only included if they are legal in the regulatory domain.  
 When a channel is added to the block list, all APs in the template that are using that channel (either as a primary or bonded channel) will automatically pick new channels.  
 DynamicRF will only use Non-Overlapping Channels 1, 6 and 11.

Channels in the left portion of the select box are included while channels in the right portion are excluded.  
 Included channels are only included if they are legal in the regulatory domain.  
 When a channel is added to the block list, all APs in the template that are using that channel (either as a primary or bonded channel) will automatically pick new channels.  
 This is a generic channel list valid for all the regulatories.Channels 52,56,60 and 64 are valid even if DFS is disabled for some regulatories and the AP channel list is populated as per regulatory domain.

15. Enable or disable packet aggregation on each radio by selecting the **Enable Packet Aggregation** check box. By default, packet aggregation is enabled on both radios.

Channel list +

**Enable Packet Aggregation**

Beacon Interval (ms) 200

Max Associations Load 64

For 1800 Series APs the max is 64 - any value higher than 64 is treated as 64.

Aggregation is always enabled on the 5 GHz radio for 2000/2100 series APs

200

64

For 1800 Series APs the max is 64 - any value higher than 64 is treated as 64.

16. Specify the beacon interval (in ms) for each radio. By default, both radios have a beacon interval of **200** ms. Valid range is **40** to **1000** ms. A minimum beacon interval of **200** ms is recommended, particularly when the radio is configured with multiple SSIDs.

Channel list	<input type="button" value="+"/>	
Enable Packet Aggregation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <small>Aggregation is always enabled on the 5 GHz radio for 2000/2100 series APs</small>
Beacon Interval (ms)	<input type="text" value="200"/>	<input type="text" value="200"/>
Max Associations Load	<input type="text" value="64"/> <small>For 1800 Series APs the max is 64 - any value higher than 64 is treated as 64.</small>	<input type="text" value="64"/> <small>For 1800 Series APs the max is 64 - any value higher than 64 is treated as 64.</small>

17. Specify the maximum AP associations load for each radio by entering a value in the **Max Associations Load** field. By default, the load maximum is set to **64** on both radios. The highest AP load maximum supported is **1024** (BSAP 1900 Series only). This value can be configured based on the per-user bandwidth required per application. For example, when 52 KB is required for an application, more users can be supported than if 10 MB is required for an application.

Channel list	<input type="button" value="+"/>	
Enable Packet Aggregation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <small>Aggregation is always enabled on the 5 GHz radio for 2000/2100 series APs</small>
Beacon Interval (ms)	<input type="text" value="200"/>	<input type="text" value="200"/>
Max Associations Load	<input type="text" value="64"/> <small>For 1800 Series APs the max is 64 - any value higher than 64 is treated as 64.</small>	<input type="text" value="64"/> <small>For 1800 Series APs the max is 64 - any value higher than 64 is treated as 64.</small>

**i** **NOTE**  
*The BSAP 1800 Series treat a value of 64, or anything greater than 64, as 64.*

18. Specify the delivery traffic indication message (DTIM) beacon interval. This value specifies how often broadcast and multicast beacons are sent in comparison to normal beacons. Interval range is from **1** to **255**. By default, both radio DTIM beacon intervals are set to **1**.

DTIM	<input type="text" value="1"/> <small>Send broadcast and multicast every (DTIM * beacon interval), values (1-255).</small>	<input type="text" value="1"/> <small>Send broadcast and multicast every (DTIM * Beacon Interval), values (1-255).</small>
Fragmentation Threshold	<input type="text" value="2346"/> <small>Packet length for fragmentation, values (256-2346 bytes).</small>	<input type="text" value="2346"/> <small>Packet length for fragmentation, values (256-2346 bytes).</small>
RTS Threshold	<input type="text" value="2346"/> <small>Packet length when RTS/CTS are used, values (256-2346 bytes).</small>	<input type="text" value="2346"/> <small>Packet length when RTS/CTS are used, values (256-2346 bytes).</small>
Antenna Mode	<input type="radio"/> 1 Antenna <input type="radio"/> 2 Antennas <input checked="" type="radio"/> 3 Antennas <small>Only applies when configured to a value less than what the AP supports.</small>	<input type="radio"/> 1 Antenna <input type="radio"/> 2 Antennas <input checked="" type="radio"/> 3 Antennas <small>Only applies when configured to a value less than what the AP supports.</small>

19. Set the fragmentation threshold value for both radios. This value is the packet length (in bytes) for fragmentation. Valid range is **256 to 2346** bytes, and by default, both radios are set to **2346** bytes. Typically, you will never need to change this value.

DTIM	<input type="text" value="1"/> <small>Send broadcast and multicast every (DTIM * beacon interval), values (1-255).</small>	<input type="text" value="1"/> <small>Send broadcast and multicast every (DTIM * Beacon Interval), values (1-255).</small>
Fragmentation Threshold	<input type="text" value="2346"/> <small>Packet length for fragmentation, values (256-2346 bytes).</small>	<input type="text" value="2346"/> <small>Packet length for fragmentation, values (256-2346 bytes).</small>
RTS Threshold	<input type="text" value="2346"/> <small>Packet length when RTS/CTS are used, values (256-2346 bytes).</small>	<input type="text" value="2346"/> <small>Packet length when RTS/CTS are used, values (256-2346 bytes).</small>
Antenna Mode	<input type="radio"/> 1 Antenna <input type="radio"/> 2 Antennas <input checked="" type="radio"/> 3 Antennas <small>Only applies when configured to a value less than what the AP supports.</small>	<input type="radio"/> 1 Antenna <input type="radio"/> 2 Antennas <input checked="" type="radio"/> 3 Antennas <small>Only applies when configured to a value less than what the AP supports.</small>

20. Set the request to send (RTS) threshold value for both radios. This is the packet length (in bytes) to determine when RTS or clear to send (CTS) are used. Values range from **256 to 2346**, and by default, both radios are set to **2346** bytes. Typically, you will never need to change this value.

DTIM	<input type="text" value="1"/> <small>Send broadcast and multicast every (DTIM * beacon interval), values (1-255).</small>	<input type="text" value="1"/> <small>Send broadcast and multicast every (DTIM * Beacon Interval), values (1-255).</small>
Fragmentation Threshold	<input type="text" value="2346"/> <small>Packet length for fragmentation, values (256-2346 bytes).</small>	<input type="text" value="2346"/> <small>Packet length for fragmentation, values (256-2346 bytes).</small>
RTS Threshold	<input type="text" value="2346"/> <small>Packet length when RTS/CTS are used, values (256-2346 bytes).</small>	<input type="text" value="2346"/> <small>Packet length when RTS/CTS are used, values (256-2346 bytes).</small>
Antenna Mode	<input type="radio"/> 1 Antenna <input type="radio"/> 2 Antennas <input checked="" type="radio"/> 3 Antennas <small>Only applies when configured to a value less than what the AP supports.</small>	<input type="radio"/> 1 Antenna <input type="radio"/> 2 Antennas <input checked="" type="radio"/> 3 Antennas <small>Only applies when configured to a value less than what the AP supports.</small>

21. Select the antenna mode for each radio. Choose from **1, 2, or 3** antennas.

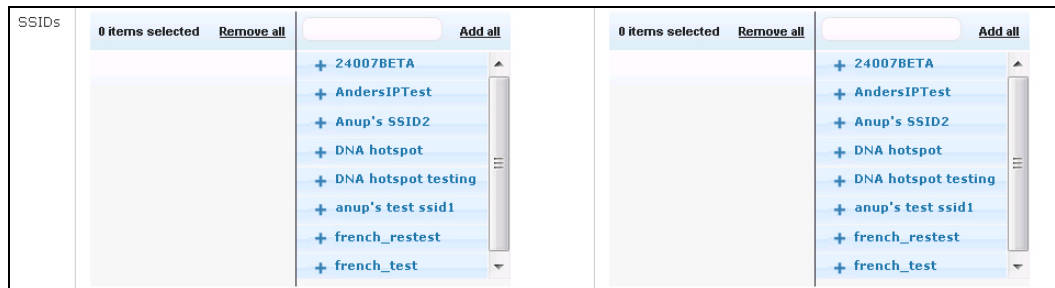
DTIM	<input type="text" value="1"/> <small>Send broadcast and multicast every (DTIM * beacon interval), values (1-255).</small>	<input type="text" value="1"/> <small>Send broadcast and multicast every (DTIM * Beacon Interval), values (1-255).</small>
Fragmentation Threshold	<input type="text" value="2346"/> <small>Packet length for fragmentation, values (256-2346 bytes).</small>	<input type="text" value="2346"/> <small>Packet length for fragmentation, values (256-2346 bytes).</small>
RTS Threshold	<input type="text" value="2346"/> <small>Packet length when RTS/CTS are used, values (256-2346 bytes).</small>	<input type="text" value="2346"/> <small>Packet length when RTS/CTS are used, values (256-2346 bytes).</small>
Antenna Mode	<input type="radio"/> 1 Antenna <input type="radio"/> 2 Antennas <input checked="" type="radio"/> 3 Antennas <small>Only applies when configured to a value less than what the AP supports.</small>	<input type="radio"/> 1 Antenna <input type="radio"/> 2 Antennas <input checked="" type="radio"/> 3 Antennas <small>Only applies when configured to a value less than what the AP supports.</small>

**i** **NOTE**

*This setting only applies when configured to a number less than the number of antennas supported by the AP.*

22. Specify the SSIDs to be associated with the radio. You can have the same SSID on both radios, or specify an SSID unique to each radio which allows clients to choose to which radio they want to connect. Associating specific SSIDs with each radio prevents the radios from advertising all available

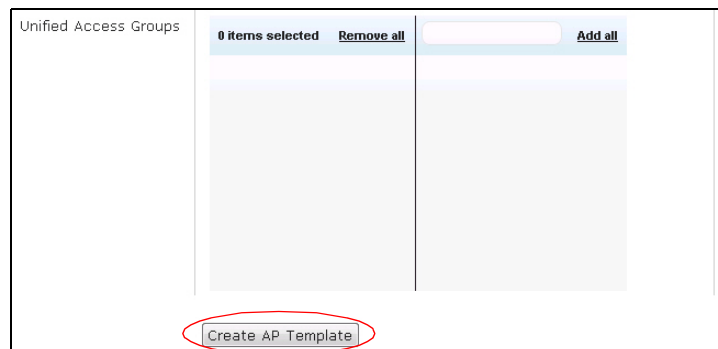
SSIDs. If you do not have any configured SSIDs to apply to the radio, refer to [Configuring an SSID on page 188](#).



#### NOTE

*SSIDs cannot be specified for a radio in **Mesh Mode**.*

23. Specify the unified access groups to be associated with the AP. Unified access groups are used by unified access clients to connect to the network. If you do not have any configured unified access groups to apply to the AP, refer to [Configuring Unified Access Groups on page 202](#).



#### NOTE

*Unified access groups cannot be specified for an AP with a radio in **Mesh Mode**.*



#### NOTE

*Clients connected to mesh LAN extensions or SSID on mesh points cannot ping or talk to mesh APs. To reach mesh APs, you must be on a network outside of the mesh network.*

24. After entering all the information for both radios, select **Create AP Template** to create the new template.

25. A confirmation is displayed indicating the AP template has been successfully created.

## Configuring vWLAN for CNA Support

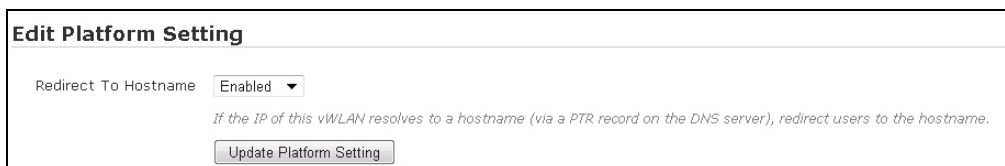
As part of the AP template, the administrator can optionally choose to enable or disable CNA (enabled by default). For CNA to function properly, however, there are additional configuration steps that are necessary. A custom certificate must be loaded on vWLAN because CNA has no method to allow the user that is accessing the network to accept the certificate. In addition, vWLAN must be configured to redirect to a host name, and a DNS server and hostname may need to be configured. These configurations should be completed before applying the AP template to any APs.

To configure vWLAN for CNA support, follow these steps:

1. Enable vWLAN to redirect to a host name by navigating to the **Configuration** tab, select **System > Settings**, and then select the **Platform** tab. Select the **Redirect to hostname** setting from the list.



2. Change the **Redirect to hostname** to **Enabled** using the drop-down menu, and select **Update Platform Setting**. You will receive confirmation that the setting has been changed.



3. Next, you must upload the appropriate certificate for CNA support. Make sure to have all of the certificate details and to upload the proper certificate. Navigate to the **Configuration** tab, select **System > Settings**, and then select the **Platform** tab. Upload the certificate as directed in [Managing vWLAN Certificate Settings on page 79](#). Make sure to save the setting.
4. Next, in the AP template (**Configuration** tab, **Wireless > AP Templates**), make sure that CNA support is enabled and optionally specify the DNS server to be used to resolve the host name (the AP will by default use its DNS server to resolve the name). Once the changes have been made to



the template, select **Create AP Template** or **Update AP Template**. Remember that all APs that use this template will also be updated.

**Create AP Template**

Name: root@adtran.com

SSH Password: [Redacted]

SSH Password Confirmation: [Redacted]

Login Form: Default Login Form

DNS Server(s) For NAC Users: 0.0.0.0  
Set to 0.0.0.0 to use the DNS server from the AP's Native VLAN.  
 A maximum of two DNS servers can be added separated by a comma.

Release:

- 1800v1 Firmware: [Dropdown]
- 1800v2/1840 Firmware: [Dropdown]
- 1920/1925 Firmware: [Dropdown]
- 1930/1935/1940 Firmware: [Dropdown]

Server:

- vWLAN: [Dropdown]
- vWLAN: [Dropdown]
- vWLAN: [Dropdown]
- vWLAN: [Dropdown]

Enable Captive Network Assistant:   
Check to enable Apple CNA or Microsoft NCSI.  
 \*Requires Trusted Certificate on vWLAN.  
 \*Requires redirect to hostname to be enabled in platform settings.

- The last configuration task for CNA support is to change the network interface host name setting. Navigate to the **Configuration** tab, and select **System > Network Interfaces**. Select the **public** interface from the list.

Name	DHCP *	Address *	Netmask *
private	Disabled	10.251.252.1	255.255.255.0
public	Disabled	192.168.103.3	255.255.252.0

Showing 1 to 2 of 2 entries

- Enter the host name in the **Hostname** field and select **Update Network Interface**. Do not forget to restart the vWLAN for the changes to take effect.

**Edit Network Interface**

Name: public

Current Address: 192.168.103.3

Current Netmask: 255.255.252.0

Current Gateway: 192.168.100.1  
For a DHCP enabled network, the current address settings when there is no DHCP server.

DHCP:

Address: 192.168.103.3

Netmask: 255.255.252.0

Gateway: 192.168.100.1

DNS 1: 192.168.100.1

DNS 2: 4.2.2.2

Hostname: wlan-tx-126a.schoolname.edu

Update Network Interface

Show | Back

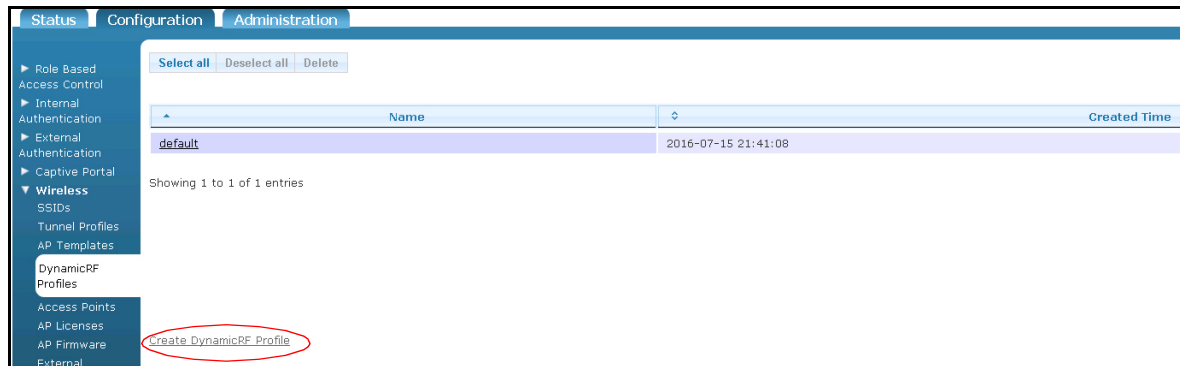
- The configuration for CNA support on vWLAN is complete. When enabled, CNA will display a popup window whenever an Apple client connects to the SSID associated with the AP template. The popup window redirects the user to the vWLAN login form. When disabled, CNA does not create a popup window, and the connected client is redirected to the vWLAN login form when a web browser is opened.

### Configuring the DynamicRF Profile

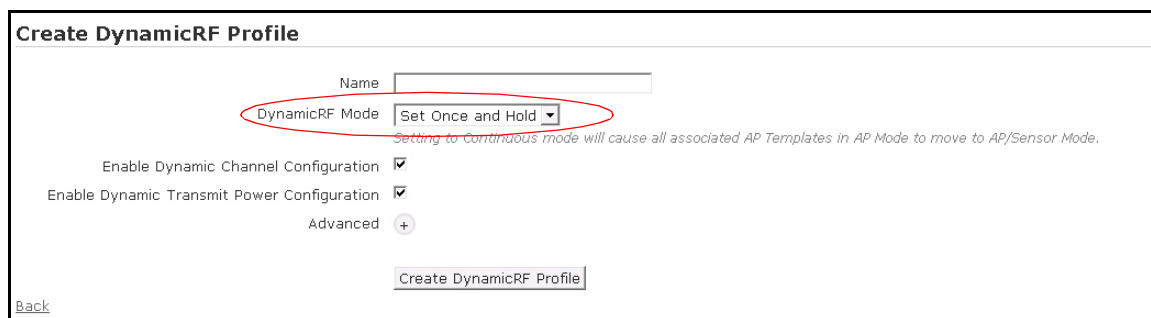
Configuring DynamicRF relies on two main configuration steps: configuring a DynamicRF profile, and applying the DynamicRF profile to the AP. The steps necessary to complete the DynamicRF profile are described in the following section; the steps to apply the DynamicRF profile to an AP template are included in [Configuring AP Templates on page 149](#).

There are various settings that can be configured for the DynamicRF profile. These settings include specifying the profile name and DynamicRF mode, enabling channel and power configuration, and specifying power thresholds. Each configurable DynamicRF profile setting is described in the following section. To configure various settings for the DynamicRF profile, follow these steps:

- In the vWLAN GUI, navigate to the **Configuration** tab, and select **Wireless > DynamicRF Profiles**.



- By default, a **Default** DynamicRF profile already exists. This profile uses all default values for DynamicRF settings. To create a new DynamicRF profile, select **Create DynamicRF Profile**. To edit an existing profile, select the profile name from the list.
- In the **Create DynamicRF Profile** menu, specify the name of the profile in the **Name** field. Specify the DynamicRF type by selecting either **Set Once and Hold** or **Continuous** from the **DynamicRF Mode** drop-down menu. Refer to the configuration guide, [DynamicRF in vWLAN](https://supportcommunity.adtran.com), available online at <https://supportcommunity.adtran.com> for additional information about when to use each of these settings.



**Set Once and Hold:** This is the default DynamicRF setting, and indicates that vWLAN only configures the RF power and channel settings for APs to achieve optimal RF performance a single time. After the initial configuration is set by DynamicRF, future changes to the channel and power settings must be made manually, or a background scan can be scheduled or run manually. In this mode, neighboring APs do not automatically respond to changes in the wireless environment.

**NOTE**

*It is possible to run DynamicRF in the background even when the DynamicRF mode is **Set Once and Hold**. This allows you to receive suggested radio setting changes that you can choose to manually accept later (refer to [Configuring AP Jobs on page 173](#)).*

**Continuous:** This setting indicates that vWLAN continuously evaluates the RF environment and modifies the AP's RF power and channel settings as needed to achieve optimal RF performance. In this mode, if the environment changes, the APs automatically increase or decrease power levels or change radio channels to account for the environmental changes. In general, you should not use continuous DynamicRF if your domain is extremely dynamic, or for real time traffic (such as voice).

**NOTE**

*If you are editing a previously created DynamicRF profile, and set it to **Continuous**, any associated AP templates will place the APs in AP/Sensor mode. This could cause a disruption to wireless communication. In addition, any change in channel or radio settings on the AP will cause clients to lose connectivity to that AP.*

4. Enable **Enable Dynamic Channel Configuration** by selecting the check box. This option is enabled by default, and specifies that DynamicRF will automatically assign the AP radio to the channel with the least amount of interference.
5. Enable **Enable Dynamic Transmit Power Configuration** by selecting the check box. This option is enabled by default, and specifies that DynamicRF will automatically change transmit power settings of the AP radio based on learned signal strength of other APs.
6. Optionally select the **Advanced** tab to configure transmit power settings for the DynamicRF profile.

**Create DynamicRF Profile**

Name

DynamicRF Mode Set Once and Hold Setting to Continuous mode will cause all associated AP Templates in AP Mode to move to AP/Sensor Mode.

Enable Dynamic Channel Configuration

Enable Dynamic Transmit Power Configuration

**Advanced** -

Transmit Power Interference Threshold  dBm Enter a number from 35 to 94.

Minimum Transmit Power 10 dBm (10 mW)

Maximum Transmit Power 30 dBm (1000 mW) When these are equal, DynamicRF will always use that specific power level for transmission.

[Back](#)

Specify the **Transmit Power Interference Threshold** by entering a value in the appropriate field. By default, the threshold is set to **-82 dBm**. Valid range is **-35 to -94 dBm**. This setting specifies that neighboring APs on the same channel with an RSSI of this setting or stronger will reduce transmit power. The stronger the threshold number, the more likely APs with neighbors on the same channel will reduce power.

Select the **Minimum Transmit Power** from the drop-down menu. By default, the minimum transmit power is set to **10 dBm (10 mW)**. Valid range is **30 dBm (1000 mW) to 1 dBm (1.3 mW)**. This setting specifies that the transmit power will never be lower than the specified value.

Select the **Maximum Transmit Power** from the drop-down menu. By default, the maximum transmit power is set to **30 dBm (1000 mW)**. Valid range is **30 dBm (1000 mW) to 1 dBm (1.3 mW)**. This setting specifies that the transmit power will never be higher than the specified value.

**i** **NOTE**

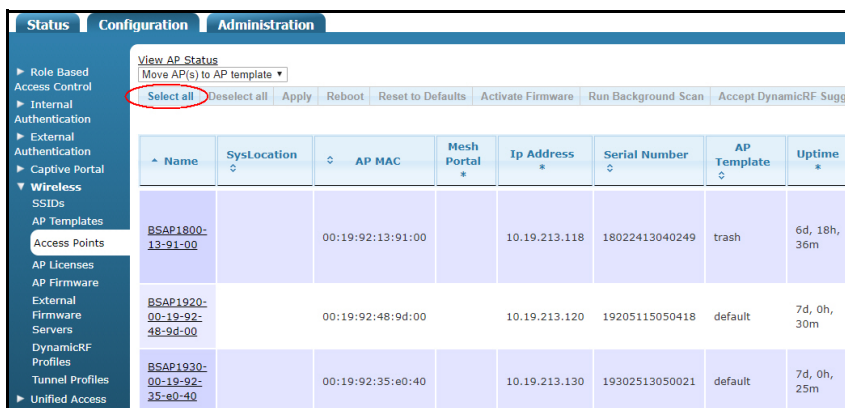
*When the minimum and maximum transmit power values are equal, DynamicRF always uses that specific power level for transmission. In addition, certain APs can only operate to a maximum power under 30 dBm (these parameters are visible in the AP details power configuration options). Setting the power level above this maximum results in the AP still functioning at the value below 30 dBm.*

7. Select **Create DynamicRF Profile** to create the profile. The profile must be associated with an AP template to be applied to an AP (refer to [Configuring AP Templates on page 149](#)).

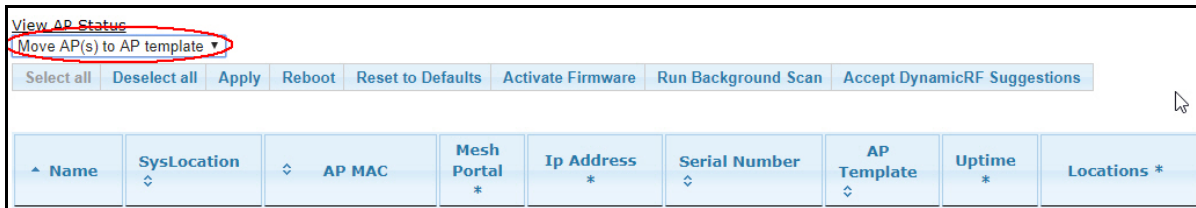
### Applying the AP Template to AP(s)

After you have created or updated the AP template, you must apply it to the AP for it to take effect. To apply the template to the AP(s), follow these steps:

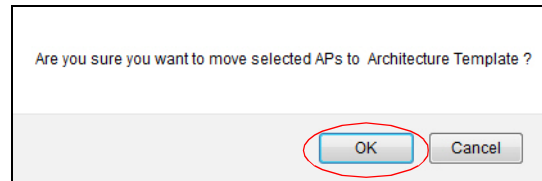
1. Navigate to the **Configuration** tab, and select **Wireless > Access Points**. Any configured APs are displayed in this menu. To change the template for an AP or multiple APs, you can either select the AP on which to change the template by selecting the AP from the list, or selecting **Select all**.



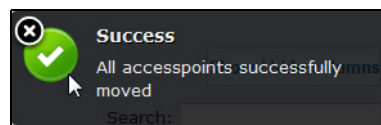
- Next, select the AP template that you want to apply to the selected APs from the **Move AP(s) to AP template** drop-down menu.



- You will be asked to verify that this is a change you want to make. Select **OK**.



- A confirmation is displayed to indicate that the AP template has been successfully applied to the selected APs, and an **Admin Task** is created. The changes will only take effect once the configuration is applied.



## Configuring Additional AP Settings

In addition to using templates, AP names can be configured to identify each AP. Locations are initially automatically discovered, however they may need to be changed if the AP is moved to another location or is on a tagged location. Radio channels and transmit power settings are automatically configured by DynamicRF (radio resource management), however, they can be manually configured based on the results of a site survey. When manually configuring channels and transmit power, be sure to disable DynamicRF mode in the DynamicRF profile so that DynamicRF will not automatically adjust your settings. You can opt to configure the radio channel and power settings for the AP before it is part of the vWLAN system. By preconfiguring the AP, and ensuring that DynamicRF is disabled in the AP template, the AP will not enter channel scanning mode when initialized and the preconfigured AP settings are used.

To configure these additional settings for an AP, follow these steps:

1. Navigate to the **Configuration** tab, and select **Wireless > Access Points**. Any configured APs are listed in this menu. Select from the list the AP whose settings you want to configure.

Name	SysLocation	AP MAC	Mesh Portal	Ip Address	Serial Number	AP Template	Uptime
BSAP3045-00-19-92-28-37-c0		00:19:92:28:37:c0		10.19.213.102	30454316050004	default	7d, 3h, 47m
BSAP3040-00-19-92-50-23-60		00:19:92:50:23:60		10.19.213.140	30404716052128	default	7d, 3h, 46m
BSAP2030-00-19-92-49-08-00		00:19:92:49:08:00		10.19.213.131	20300316050572	default	7d, 3h, 42m

2. Specify the name for the AP, its location, its template (if necessary), AP type, and the radio channel and signal power for each radio (assuming you have not used DynamicRF to choose the radio power and channel).

**Edit Access Point**

Serial Number: 19301413050413  
 AP MAC Address: 00:19:92:33:83:80  
 Country: United States  
 Name: 1930  
 SysLocation: Note the physical location of the AP  
 Location: Native AP VLAN  
 Access Point Template: default  
 Installed: Indoor

**Per Radio Settings**

<b>802.11b/g/n (2.4 GHz)</b>		<b>802.11a/n (5 GHz)</b>	
Channel: Auto (11)	Transmit Power: Auto (24 dBm [250 mW])	Channel: Auto (149)	Transmit Power: Auto (22 dBm [160 mW])
Antenna Gain (dBi): 4		Antenna Gain (dBi): 5	

Update Access Point

- Enter the name of the AP in the **Name** field. Host names must conform to RFC 952. If the AP is not named in its configuration, it receives a default name of the BSAP model paired with the MAC address. For example, a BSAP 1920 with the MAC address 00:19:92:00:79:e0 has a default name of **BSAP1920-00-19-92-00-79-e0**. If no MAC address exists for the AP (because it has not yet connected), then the default name is **BSAP-** followed by the serial number. This name is updated to the MAC address format once the AP connects. The AP name is used to easily identify APs in the vWLAN system.
- Optionally use the **SysLocation** field to specify the AP's physical location. This information can be used to help administrators when grouping APs.
- The **Location** drop-down menu specifies the VLAN used by the AP. This field is automatically populated during AP discovery, when the AP adds a VLAN tag (from those included in this drop-down menu) to an untagged VLAN. Typically this value does not need to be changed. For more

information about these locations, refer to [Configuring Domain Locations on page 94](#).

- Select the AP template from the **Access Point Template** drop-down menu. These AP templates are those created as described in [Configuring AP Templates on page 149](#).
- Specify whether the AP is an indoor or outdoor AP. By default, the AP is listed as indoor or outdoor based on the AP's serial number. If indoor is selected, all channels are available for the AP. If outdoor is selected, only the legal outdoor channels are available for the AP.
- Specify the channel used by each radio from the **Channel** drop-down menus. For the United States, the 802.11b/g/n radio channels range from **1** to **11**, and the 802.11a/n/ac radio channels range in intervals from **36** to **161**. Other countries may have a different set of allowed channels. The **Auto** option specifies that the vWLAN system will assign the radio channel to the AP. This is the default setting. To configure (or preconfigure) a specific channel for the AP, select the appropriate option from the drop-down menu. If DFS is supported by the AP platform, and is enabled in the AP template, DFS channels are available for selection on the 5 GHz radio.



#### NOTE

*Channels 120 through 128 are removed for European countries for DFS functionality.*

- Select the signal power for each radio from the **Transmit Power** drop-down menus. Signal strength ranges from **0** dBm to the maximum power supported by the AP, changing in increments of **1** dBm (corresponding mW values are also displayed). The maximum power supported is different per AP model. Refer to the configuration guide [DynamicRF in vWLAN](#), available online at <https://supportcommunity.adtran.com>, for more information.



#### NOTE

*Before specifying channel and transmit power settings manually, disable the DynamicRF mode in the DynamicRF profile used by the AP template.*

- Enter the antenna gain for each radio. External antenna gain can be configured for a value between **1** and **13** dBi for the 2.4 GHz radio and between **1** and **19** dBi for the 5 GHz radio. Internal antennas must remain at the default gain value (refer to Table 1 for default antenna gain values per radio). To change the antenna gain value, select the appropriate dBi from the **Antenna Gain** drop-down menu.

**Table 1. Default Antenna Gain Values**

AP Model	2.4 GHz Radio (dBi)	5 GHz Radio (dBi)
1920	3	4
1925	3	3
1930	4	5
1935	3	3
1940	5	7
2020	3	6

**Table 1. Default Antenna Gain Values**

AP Model	2.4 GHz Radio (dBi)	5 GHz Radio (dBi)
2030	4	5
2035	5	5
2120	5	6
2135	5	7

**NOTE**

*The FCC has strict regulations regarding antennas and their configuration. For more information about these rules, and their impact on vWLAN antenna gain configuration, refer to the [Bluesocket Compliance Notice](https://supportcommunity.adtran.com), available online at <https://supportcommunity.adtran.com>. In addition, higher value external antenna gain support is limited to those vWLAN products with certified third party antennas (BSAP 2035 Series and 2135 Series APs).*

3. Select **Update Access Point**. A confirmation is displayed indicating the new settings have been applied to the AP.

## Viewing APs

You can view the APs connected to vWLAN, their associated domains, and monitor the status of each AP in the network. In addition, you can view the APs connected to vWLAN, their associated domains, any connected users or devices, and monitor the status of each AP in the network.

**NOTE**

*The **APs** link in the top of the GUI menu indicates the number of APs that are licensed and assigned to the active domain.*

To view APs and AP licenses, navigate to the **Configuration** tab, and select **Wireless > AP Licenses**. Then select either the **Domain** (for APs on a specific domain) or **Platform** tab (for APs on the platform). In this menu, all configured or associated APs are displayed. The serial number, MAC address (if available), IP address (if available), domain, firmware version, country of operation, vWLAN license, unified access license, and AP status are displayed.



Serial Number	MAC Address	IP Address	Domain	Firmware	Country *	vWLAN License *	Unified Access License *	Status
18013309040309	00:19:92:03:0d:40	192.168.102.235	caiyun	6.8.0-9	United States	Lifetime	Lifetime	UpToDate
18021234567890			default		United States	Lifetime	None	Unknown
18022413040396			vikram_test		United States	Lifetime	None	Unknown
18022413040466			vikram_test		United States	Lifetime	None	Unknown
18023811040218	00:19:92:0a:5f:40		TestWalledGarden		United States	Lifetime	Lifetime	Unknown
18023811040999			default		Australia	Lifetime	Lifetime	Down
18024012040193			vikram_test		United States	Lifetime	None	Unknown
18024012040196			vikram_test		United States	Lifetime	None	Unknown
18024012040376	00:19:92:10:0f:40		vikram_test		United States	Lifetime	None	Unknown
1840300040352	00:19:92:03:12:a0		default		United States	Lifetime	Lifetime	Unknown
18400000000200	00:93:00:c8:a0:00		vEdgeSimDomain1		United States	Lifetime	Lifetime	Unknown

Showing 1 to 32 of 32 entries

Move AP(s) to domain: ▼

[Upload AP Licenses](#)

To select individual APs, click on the AP row, and it will change to a darker color, indicating the AP is selected.  
APs will not operate until they are moved into a domain.

## Viewing AP Details

To view the details of a particular AP's configuration, follow these steps:

1. Navigate to the **Status** tab, and select **Access Points**. Each configured AP is listed in the menu. Select the AP you want to view from the list.

Name	SysLocation	MAC Address	Mesh Portal	Serial Number	IP Address	Uptime	Locations *	Firmware *
BSAP1800-13-91-00		00:19:92:13:91:00		18022413040249	10.19.213.118	6d, 21h, 24m	vLoc-0-10.19.213.0/24	3.1.0-647193
BSAP1920-00-19-92-48-9d-00		00:19:92:48:9d:00		19205115050418	10.19.213.120	7d, 3h, 23m	vLoc-0-10.19.213.0/24	3.1.0-647193
BSAP1930-00-19-92-35-e0-40		00:19:92:35:e0:40		19302513050021	10.19.213.130	7d, 3h, 19m	vLoc-0-10.19.213.0/24	3.1.0-647193
BSAP2020-4a-de-60		00:19:92:4a:de:60		20211216050269		Unknown		

2. The selected AP details are displayed including the AP configuration, radio interfaces, associated SSIDs, and DynamicRF statistics (if applicable). In addition, from this menu you can select to edit the AP configuration, view maps, logs, alarms, alerts, traffic captures, and adjacent APs (if applicable) by using the links at the top right of the menu. These links bring up another menu, specifically filtered by the selected AP.

Links are provided to view additional AP details or edit the AP configuration.

Access Point Details														
Name Nick-1930					Model BSAP-1930					<a href="#">Edit Configuration</a> <a href="#">Not on a map yet</a> <a href="#">Logs</a> <a href="#">Alarms</a> <a href="#">Wireless IDS Alerts</a> <a href="#">AP Traffic Capture</a> <a href="#">Adjacent APs</a>				
SysLocation					DFS Hardware Ready No									
MAC Address 00:19:92:33:83:80					Firmware 2.9-M-255213									
Uptime 0d, 0h, 42m					AP Template <a href="#">default</a>									
Serial Number 19301413050413					Country United States									
IP Address 172.30.11.196					Error									
Active Locations vLoc-0-172.30.11.192/28, VLAN-100					Message									
					Status UpToDate									
					Last Calibration									
Interfaces														
Type	Radio Mode	Wireless Mode	Channel	Tx power	Max Allowed Tx Power	EIRP	Max Allowed EIRP	Antenna Gain	Noise Floor	Clients	Adjacent Aps	Co-Channel Aps	AdjacentChannel Aps	Channel Utilization
802.11b/g/n (2.4 GHz)	AP Mode	b/g/n	11 (20 MHz)	22 dBm	24 dBm	26 dBm	28 dBm	4 dBi	-103 dBm	0	2	0	0	12%
802.11a/n/ac (5 GHz)	AP Mode	a/n/ac	149 (40 MHz)	19 dBm	22 dBm	24 dBm	27 dBm	5 dBi	-106 dBm	0	1	0	0	0%
Unified Access Total								0						
								0						
SSIDs														
SSID	BSSID	Authentication	Cipher	Radio										
Nicks-Open	00:19:92:33:83:89	Open System	Disabled	802.11a/n/ac (5 GHz)										
Nicks-Open	00:19:92:33:83:81	Open System	Disabled	802.11b/g/n (2.4 GHz)										
DynamicRF Statistics														
802.11b/g/n (2.4Ghz)														
Channel	1	2	3	4	5	6	7	8	9	10	11			
Co-Channel Aps	1	0	0	0	0	1	0	0	0	0	0			
Adjacent-Channel Aps	0	2	2	2	2	0	1	1	1	1	0			
802.11a/n/ac (5Ghz)														
Channel	36	40	44	48	149	153	157	161						
Co-Channel Aps	0	0	0	0	0	0	0	1						

## Viewing AP States

You can also manage AP configuration by monitoring the state of the AP. After an AP completes discovery (and firmware upgrade), vWLAN automatically creates an entry for the AP in the AP list. By default, all new APs are associated to the default AP template, so the configuration for the AP (including radio and firmware settings) is based on the values in the default AP template.

When the AP is listed by vWLAN in the AP list, you can view the status of the AP. An AP's status can be viewed by navigating to the **Status** tab and selecting **Access Points**, or by looking at the **Configuration** tab, **Wireless > AP Licenses**. The status is listed in the **Status** column of the AP list.

The possible AP states include:

- **Up** indicates the AP is currently connected to the vWLAN system, but is not in a domain or is unlicensed.
- **Down** indicates the AP is not currently connected to the vWLAN system.
- **Unknown** indicates the state of the AP is unknown.
- **Unsupported** indicates the AP has a serial number which is not supported by vWLAN.
- **Upgrading** indicates the AP is in the process of loading the latest firmware.
- **PendingUpgrade** indicates the AP has downloaded a new firmware image, but it has not been applied.

- **Updating** indicates the AP is in the process of loading its configuration.
- **UpToDate** indicates the AP has the latest configuration and is operational.

When configuring an AP, in order to determine in what state the AP should be, several factors are considered in the following order:

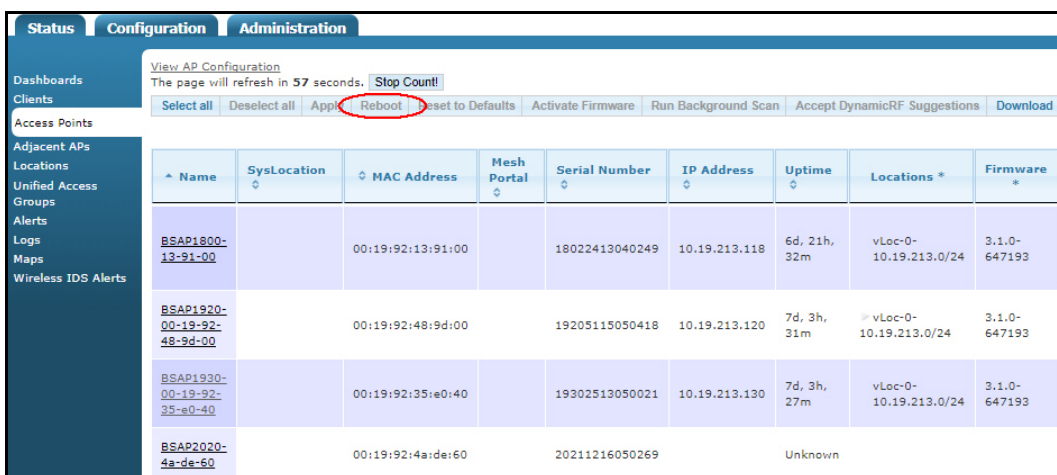
1. Is the serial number of the AP supported? If not, the AP should appear in the **Unsupported** state.
2. Does the message indicate the AP is connected or disconnected? If the message indicates the AP is disconnected, it should appear in the **Down** state.
3. Is the AP in a domain? If not, the AP should be in the **Up** state.
4. Is the AP running the latest firmware (based on the AP template configuration)? If not, the latest firmware is pushed to the AP, and the AP should enter the **Upgrading** state.
5. Is this the first time the AP has been connected while in the domain? If so, the AP receives the channel scanning configuration and should enter the **Updating** state.
6. If none of the other cases match, the AP receives the current AP configuration and should enter the **Updating** state.
7. Once the AP update is complete, the AP should enter the **UpToDate** state.

## Resetting and Rebooting APs

From time to time the AP might need to reset or rebooted. Although this action will disrupt network traffic, you can reset the AP to factory defaults to another firmware version, or reboot the AP from the GUI. In addition, you can configure the AP for disaster recovery support.

To reboot one or more APs, follow these steps:

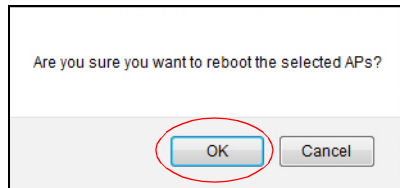
1. Navigate to the **Status** tab and select **Access Points**. Select one or more APs to reboot from the AP(s) in the list. Select **Reboot** from the top of the menu.



The screenshot shows the vWLAN Administrator's GUI. The top navigation bar includes 'Status', 'Configuration', and 'Administration'. The left sidebar contains various menu items like 'Dashboards', 'Clients', 'Access Points', 'Adjacent APs', 'Locations', 'Unified Access Groups', 'Alerts', 'Logs', 'Maps', and 'Wireless IDS Alerts'. The main content area displays a table of Access Points. Above the table, there are action buttons: 'Select all', 'Deselect all', 'Apply', 'Reboot', 'Reset to Defaults', 'Activate Firmware', 'Run Background Scan', 'Accept DynamicRF Suggestions', and 'Download'. The 'Reboot' button is circled in red. The table below has columns for Name, SysLocation, MAC Address, Mesh Portal, Serial Number, IP Address, Uptime, Locations, and Firmware.

Name	SysLocation	MAC Address	Mesh Portal	Serial Number	IP Address	Uptime	Locations *	Firmware *
BSAP1800-13-91-00		00:19:92:13:91:00		18022413040249	10.19.213.118	6d, 21h, 32m	vLoc-0-10.19.213.0/24	3.1.0-647193
BSAP1920-00-19-92-48-9d-00		00:19:92:48:9d:00		19205115050418	10.19.213.120	7d, 3h, 31m	vLoc-0-10.19.213.0/24	3.1.0-647193
BSAP1930-00-19-92-35-e0-40		00:19:92:35:e0:40		19302513050021	10.19.213.130	7d, 3h, 27m	vLoc-0-10.19.213.0/24	3.1.0-647193
BSAP2020-4a-de-60		00:19:92:4a:de:60		20211216050269		Unknown		

2. Select **OK** when prompted.



3. The AP will then reboot.

You can optionally choose to reboot an AP by creating a domain administration job to reboot all (or a subset) of the APs in the domain. Refer to [Configuring AP Jobs on page 173](#) for more information.

To restore an AP to default settings, navigate to the **Status** tab and select **Access Points** and follow these steps:

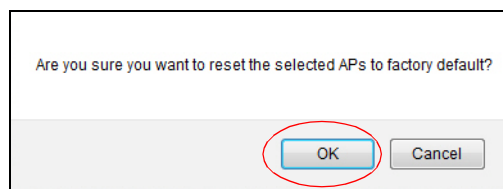
1. Select one or more APs to reset to the default settings by clicking on the AP(s) in the list. Select **Reset to Defaults** from the top of the menu.

View AP Configuration  
The page will refresh in 32 seconds. [Stop Count!](#)

Select all Deselect all Apply Reboot **Reset to Defaults** Activate Firmware Run Background Scan Accept DynamicRF Suggestions Download

Name	SysLocation	MAC Address	Mesh Portal	Serial Number	IP Address	Uptime	Locations *	Firmware *
BSAP1800-13-91-00		00:19:92:13:91:00		18022413040249	10.19.213.118	6d, 21h, 38m	vLoc-0-10.19.213.0/24	3.1.0-647193
BSAP1920-00-19-92-48-9d-00		00:19:92:48:9d:00		19205115050418	10.19.213.120	7d, 3h, 37m	vLoc-0-10.19.213.0/24	3.1.0-647193
BSAP1990-00-19-92-35-e0-40		00:19:92:35:e0:40		19302513050021	10.19.213.130	7d, 3h, 33m	vLoc-0-10.19.213.0/24	3.1.0-647193
BSAP2020-4a-da-60		00:19:92:4a:da:60		20211216050269		Unknown		
BSAP2030-00-19-92-49-08-00		00:19:92:49:08:00		20300316050572	10.19.213.131	7d, 3h, 32m	vLoc-0-10.19.213.0/24	3.1.0-647193

2. Select **OK** when prompted.



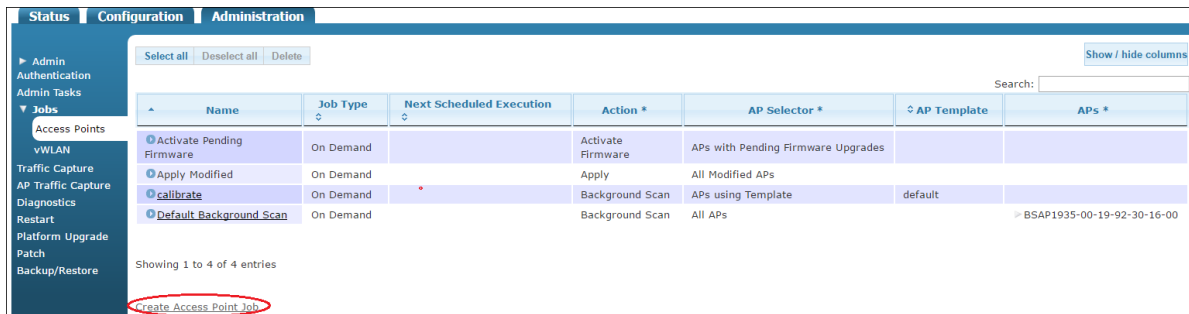
3. The AP will then reset to factory default settings. Any errors associated with the AP reset are displayed in the **Error** column of the **Status** tab **Access Points** menu. vWLAN configuration does not change when resetting APs to the default setting. Rather, only the AP-specific configuration (that which can be configured through the AP serial menu) is reset.

## Configuring AP Jobs

In addition to configuring APs using the steps previously described, you can also create jobs associated with AP configuration. These jobs are tasks that relate to AP configuration and can be applied to multiple APs at once. For example, to reboot multiple APs, apply a new configuration to multiple APs, calibrate multiple APs, or restore multiple APs to the default setting, rather than working through the configuration menus, you can create a single job to accomplish these tasks. You also have the ability to schedule AP jobs. By default, one AP job exists: to apply configurations to modified APs. This job is used by the system when the administrator makes wireless or firewall changes.

To create an AP job, follow these steps:

1. Navigate to the **Administration** tab and select **Jobs > Access Points**. In this menu, all current AP jobs are listed. Each listing includes the available actions for the job, the name of the job, the next scheduled execution time for the job, the action the job performs, the APs to which the job applies, the AP template to which the job applies, and the APs affected by the job. To create a new AP job, select **Create Access Point Job** at the bottom of this menu, or **Domain AP Job** from the **Create** drop-down menu (at the top of the menu).



Name	Job Type	Next Scheduled Execution	Action *	AP Selector *	AP Template	APs *
Activate Pending Firmware	On Demand		Activate Firmware	APs with Pending Firmware Upgrades		
Apply Modified	On Demand		Apply	All Modified APs		
calibrate	On Demand		Background Scan	APs using Template	default	
Default Background Scan	On Demand		Background Scan	All APs		BSAP1935-00-19-92-30-16-00

Showing 1 to 4 of 4 entries

[Create Access Point Job](#)

2. Enter a name for the job in the **Name** field.

### Create Access Point Job

Name

Action

AP Selector

Scheduled

[Back](#)

3. Select the appropriate action for the job from the **Action** drop-down menu. Selections include: **Apply**, **Reboot**, **Reset to Defaults**, **Background Scan**, **Activate Firmware**, and **Accept DynamicRF Suggestions**.
4. Next, select the APs to which the job applies from the **AP Selector** drop-down menu. Selections include: **All APs**, **All Modified APs**, **All APs with Errors**, **APs using Template**, **Selected APs**, and **APs with Pending Firmware Upgrades**. If you choose **APs using Template**, you will be prompted to specify a template. If you choose **Selected APs**, you will be prompted to select the APs from a list.

- To schedule the job, select the **Scheduled** check box to display the scheduling options. Use the **Frequency** drop-down menu to specify how often the job will run: **Daily**, **Weekly**, **Monthly**, or **One-time**. Select **Scheduled Date** to use the calendar to select the beginning date for the job. Use the **Scheduled Time** drop-down menus to specify the start time for the job.

Scheduled

Frequency One-time ▼

Scheduled Date

Scheduled Time 01 ▼ : 00 ▼ AM ▼

- Select **Create Access Point Job** to create the job.
- Once the job has been created, it will appear in the job list in the AP **Jobs** menu. To execute the job immediately, select the **Actions** arrow next to the job in the job list. You will receive a confirmation that the job has been completed.

Name	Job Type	Next Scheduled Execution	Action *	AP Selector *	AP Template	APs *
Activate Pending Firmware	On Demand		Activate Firmware	APs with Pending Firmware Upgrades		
Apply Modified	On Demand		Apply	All Modified APs		
Calibrate	On Demand		Background Scan	APs using Template	default	
Default Background Scan	On Demand		Background Scan	All APs		BSAP1935-00-19-92-30-16-00

## 9. vWLAN Setup Wizard

In vWLAN firmware release 2.6, a new setup wizard was added. The setup wizard allows users who are using vWLAN for the first time to easily configure the basic networking requirements to connect to and use vWLAN. The setup wizard provides a simple method for configuring the administrator, SSID, and domain. This chapter discusses how to launch the setup wizard and the configuration steps included in the wizard. Details for vWLAN configuration are not included in this section, but rather are discussed in [vWLAN Administrators on page 43](#), [vWLAN Platform Configuration on page 52](#), [vWLAN Domain Configuration on page 85](#), [vWLAN Wireless Configuration on page 188](#), and [Configuring Client Connections on page 207](#).

This chapter includes the following sections:

- [Launching the Setup Wizard on page 175](#)
- [Using the Setup Wizard on page 176](#)
- [Applying the Setup Wizard Settings on page 179](#)

### Launching the Setup Wizard

The first time you launch vWLAN, the setup wizard displays by default. If you have already created an administrator, and that administrator logs into the default domain for the first time, the setup wizard is also displayed. If this is not the first time you have launched vWLAN, or if the setup wizard does not launch, you can optionally launch the wizard manually. There are two methods for manually launching the setup wizard: enabling the wizard in the domain setting, or entering information in your web browser.

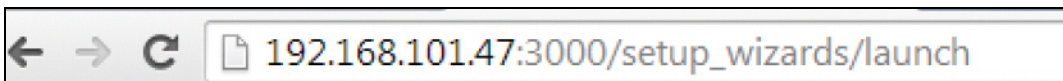
To launch the setup wizard manually by enabling the wizard, follow these steps:

1. Navigate to the **Configuration** tab, and select **System > Settings**. Then select the **Show or Hide Setup Wizard** option from the settings list.

Domain		Platform	
Name	Value *	Hint	Search: <input type="text"/>
Aggressive DHCP Lease Time for Un-registered Clients	Disabled	An aggressive lease time brings clients on faster after authentication, but may not be compatible with all handheld devices.	
Allow the AP to look up the vWLAN name using a DNS PTR record?	Enabled	This must be enabled if redirect to hostname is enabled.	
AP Control Channel Timeout	14400	Time in seconds before APs reboot if control channel is confirmed to be lost to the vWLAN (defaults to four hours - meaning, APs would reboot four hours after confirming that the control channel has been lost)	
Post Login Redirect	Disabled	If enabled, users will be redirected to the Post Login Redirect URL after web based authentication instead of their original destination.	
Post Login Redirect URL	http://www.adtran.com	The Post Login Redirect URL is the URL that the user will be redirected to after web based authentication instead of their original destination.	
Redirect HTTPS traffic for Unregistered clients	Disabled	Redirects HTTPS to the captive portal	
Show or hide setup wizard	Disabled	Enables setup wizard.	
Time in minutes between updating internal status (minimum 15)	15	Updates the bandwidth reading	
Time in seconds before inactive connections are dropped	600	Inactive connections will be dropped once this time out has been reached.	

- In the resulting menu, select **Enabled** from the **Show or Hide Setup Wizard** drop-down menu. Then select **Update Domain Setting** to launch the setup wizard.

A second method for launching the setup wizard is to use your web browser. To launch the wizard using your browser, navigate to your web browser and enter `/setup_wizards/launch` at the end of the URL address of your vWLAN system. For example, if your URL is **102.168.100.1:3000**, then **192.168.100.1:3000/setup\_wizards/launch** will launch the setup wizard.



#### NOTE

*You can only launch the setup wizard using this method if you are the network administrator, already logged into vWLAN, and your session has not timed out.*

## Using the Setup Wizard

Once the setup wizard has launched, you can use the wizard to create a default vWLAN network. The setup wizard works in two stages: configuring the administrator, and allowing vWLAN to configure a default wireless network, with default roles for connecting clients, primary wireless network settings, and default guest roles and network settings. After each wizard step, select **Next** to proceed to the next step. When you select **Next**, the wizard will automatically perform a validation to ensure that information has been entered correctly at each step. If incorrect information has been entered, you will have an opportunity to correct it before proceeding. You can also navigate through the wizard using the **Previous** and **Next** buttons. If you choose to go to a previous page, all information entered in the current page is saved. In addition, you will be able to review all your configurations before selecting **Finish** to implement the changes and exit the wizard.

To use the setup wizard to configure vWLAN, launch the wizard and follow these steps:

### Step 1: Configure the Administrator

The first step of the setup wizard is to configure the administrator. This step allows you to edit an already configured administrator profile. In this step you can change the current administrator's email, password, and timezone by entering the information in the correct fields and selecting the timezone from the drop-down menu.



**1 Step 1**  
Administrator

**2 Step 2**  
Setup Wireless Networks

**3 Summary**  
Review All

Email: root@adtran.com

Change Password:

Password: .....

Password Confirmation:

Current Timezone: Eastern Time (US & Canada)

Timezone: (-06:00) Central Time (US & Canada), Guadalajara, Mexico city

Cancel Previous Next Finish

**NOTE**

*Be cautious about changing the root@adtran.com administrator email address using the wizard. This change should be made using the root@adtran.com link at the top right of the vWLAN GUI.*

If this is the first time you have launched vWLAN, this is the default administrator information. If you do not want to change any of this information, simply deselect the **Change Password** check box. Once all the information has been entered, select **Next**.

## Step 2: Verifying the Primary and Guest Wireless Networks

In this step you are verifying default SSIDs for both a primary and guest network. These SSIDs are automatically added to the default AP template.

### Primary Wireless Network

The primary wireless network provides safe wireless access for corporate users on the vWLAN network. There are two different authentication methods provided with the primary wireless network: WPA2-PSK and Open System. If you select WPA2-PSK, you can configure a preshared key for the SSID. When a user connects to the network, they enter the preshared key to access the network. If Open System is selected, no authorization is required for the user to connect to the network, but rather the user is redirected to a third-party captive portal login page.

To configure the primary wireless network, follow these steps:

1. Enable the primary wireless network by selecting the **Primary Wireless Network** check box. By default, this box is selected.

- Specify the name of the primary wireless network SSID by entering the name in the **SSID Name** field.
- Specify whether the network will use WPA2-PSK or Open System by selecting the correct option from the **Authentication** drop-down menu. If you choose **WPA2-PSK**, you must specify the preshared key and preshared key confirmation in the appropriate fields.
- Choose whether captive portal will be enabled for the primary wireless network. If this feature is not enabled, any users that connect to vWLAN can access the Internet without limitation. If this feature is enabled, users that connect to vWLAN are redirected to a third-party captive portal login page before they are allowed to access the Internet through vWLAN. If you selected **Open System** as the authentication method for the primary wireless network, you must configure captive portal.

The screenshot displays the 'Step 2: Setup Wireless Networks' configuration screen. It is divided into two main sections: 'Primary Wireless Network' and 'Guest Wireless Network'.  
 - **Primary Wireless Network:** A checkmark is present. Fields include 'SSID Name' (text input), 'Authentication' (dropdown menu set to 'WPA2-PSK'), 'Preshared Key' (text input with placeholder 'Enter an 8+ digit value.'), 'Preshared Key Confirmation' (text input), and 'Captive Portal' (checkbox). A note below states: 'If checked, client will be redirected to the captive portal and you will have the opportunity to create a user in a subsequent step.'  
 - **Guest Wireless Network:** A checkmark is present. Fields include 'SSID Name' (text input with placeholder 'Enter guest SSID name') and 'Authentication' (dropdown menu set to 'Open System'). A note below states: 'If checked, guest SSID will be open with no encryption and guests will be redirected to the captive portal where they can enter an email address.'  
 At the bottom, there are four buttons: 'Cancel', 'Previous', 'Next', and 'Finish'.

- Next, optionally configure the guest wireless network.

## Guest Wireless Network

The guest wireless network provides Internet access for non-corporate users who do not require access to all of the vWLAN network. The guest wireless network only requires an SSID name. Once it is created, it functions as an open system SSID that allows any user to connect to it without a password or other authentication. Users who connect using this SSID are placed in a Guest role by vWLAN.

To configure the guest wireless network, follow these steps:

- Enable the guest wireless network by selecting the **Guest Wireless Network** check box.

- Specify the SSID for the guest network in the **SSID Name** field.

**1 Step 1** Administrator

**2 Step 2** Setup Wireless Networks

**3 Summary** Review All

**Primary Wireless Network**

SSID Name

Authentication **WPA2-PSK**

Preshared Key

Preshared Key Confirmation

Captive Portal

If checked, client will be redirected to the captive portal and you will have the opportunity to create a user in a subsequent step.

**Guest Wireless Network**

SSID Name

Authentication **Open System**

If checked, guest SSID will be open with no encryption and guests will be redirected to the captive portal where they can enter an email address.

**Cancel** **Previous** **Next** **Finish**

- Once the two networks have been configured, select **Next**.

### Step 3: Reviewing the Configuration

Once you have specified the administrator and wireless networks you can review all your information before finishing the wizard. After reviewing the configuration summary, if everything is correct, select **Finish**. If you need to make changes, use the **Previous** and **Next** buttons to navigate through the wizard and make changes.

You can select **Click to show further details** to display all the actions the wizard will complete once **Finish** is selected.

Select **Finish** when your changes are complete.

**1 Step 1** Administrator

**2 Step 2** Setup Wireless Networks

**3 Summary** Review All

**Administrator**

Email	root@adtran.com
Timezone	Central Time (US & Canada)
Change Password	Yes

**Guest Wireless Network**

Create Guest SSID	Yes
SSID name	gues
Authentication	Open System

**Primary Wireless Network**

Create Primary SSID	Yes
SSID name	testssid
Authentication	WPA2-PSK
Preshared Key	sharedkey
Preshared Key Confirmation	sharedkey

**(Click to show further details)**

**Cancel** **Previous** **Next** **Finish**

## Applying the Setup Wizard Settings

If this is the first time you have configured vWLAN, and you do not have an AP associated with the default domain or AP template, you will need to bring the AP into the domain and assign it the default AP template. Details for this action are described in [Associating APs with a Domain on page 145](#).

If you already have an AP in this domain, you must push the new configuration to the AP manually. To do so, select **Domain Task** at the top of the vWLAN menu. Details of this operation are described in [Administrative Tasks on page 265](#).

## 10. vWLAN Serial Console Configuration

In addition to using the GUI, certain parameters can be configured using the vWLAN or AP serial console. The following sections describe how to connect to the vWLAN and AP serial console, and the available serial console configuration commands. The following sections are included in this chapter:

- [vWLAN Serial Console Configuration on page 181](#)
- [AP Serial Console Configuration on page 183](#)



### NOTE

*Normally there is no need to access the AP serial console menu. The AP automatically discovers and communicates with vWLAN. It is recommended to use the serial console menu to configure the AP only in a lab or test environment, or where a predefined static IP address for the AP is desired. The only exception is in a situation where changing DHCP or DNS is not possible.*

### vWLAN Serial Console Configuration

The serial console menu can be used to configure some vWLAN parameters such as switching partitions, restarting the vWLAN, restoring default settings, performing reboots, and displaying certain configurations. Serial console configuration is generally used when troubleshooting. The sections below describe the available vWLAN serial console configuration commands.



### NOTE

*vWLAN serial console configuration is available from the serial console port when using the vWLAN hardware appliance. If you are running vWLAN on VMware, you can access the serial console menu by selecting the vWLAN virtual machine and the console tab in vSphere client.*

### Accessing the vWLAN Serial Console Menu

To access the vWLAN serial console menu using the **Serial** port, following these steps:

1. Connect the DB-9 (male) connector of your serial cable to the **Serial** port on the back of the appliance hardware.
2. Connect the other end of the serial cable to the PC.
3. Provide power to the unit as appropriate.
4. Once the unit is powered up, open a VT100 terminal session with the following settings: 9600 baud, 8 data bits, no parity, and 1 stop bit (no flow control). Select **<Enter>** to access the serial console menu.
5. At the vWLAN login prompt, enter the user name **vwlan** and the password **vwI@nBlu3\$ock3t**.

## vWLAN Serial Console Configuration Commands

There are several items you can configure once you have connected to the vWLAN serial console. [Table 1](#) outlines the available commands and describes their functionality.

**Table 1. vWLAN Serial Console Configuration Commands**

Command	Description
<b>dbinit</b>	Cleans the vWLAN database and restores the database to the default settings. This command requires a restart to take effect.
<b>ifconfig</b>	Displays a list of all network interface card settings. The <b>eth0</b> setting is the network interface, and the <b>eth1</b> setting is the management interface.
<b>processes</b>	Displays a list of all the currently running processes on the vWLAN.
<b>restart</b>	Restarts the vWLAN processes.
<b>switch</b>	Causes the vWLAN to switch to the alternative runtime image upon the next vWLAN reboot.
<b>reboot</b>	Reboots the vWLAN. This command is beneficial to use after executing the <b>switch</b> command.
<b>clean</b>	Cleans up old debug and log files.
<b>exit</b>	Exits the serial port session.
<b>admin recovery</b>	Resets the vWLAN root@adtran.com administrator password and returns the access permissions to the default settings.
<b>interface i</b> <ip address> <network mask> <gateway address>	Specifies a static IP address for the network interface.
<b>interface i dhcp</b>	Specifies the network interface uses DHCP for IP address assignment.
<b>m</b> <ip address> <network mask>	Specifies the management port interface IP address.
<b>certificate cleanup</b>	Removes any custom web server certificate. This command can be used when a web server will not start after installing a custom certificate. The command removes the custom certificate to recover the system and restarts the web server automatically.

## AP Serial Console Configuration

You can use the serial console menu to manually configure the AP's network configuration (IP address and default gateway), the IP address of vWLAN, and the site survey mode. The available AP serial console configuration is described in the following sections.



### NOTE

*Normally there is no need to access the AP serial console menu. The AP automatically discovers and communicates with the vWLAN. It is recommended to use the serial console menu to configure the AP only in a lab or test environment, or where a predefined static IP address for the AP is desired. The only exception is in a situation where changing DHCP or DNS is not possible.*

### Accessing the AP Serial Console Menu

You can access the AP's serial console menu using either a VT100 terminal emulation program or an Ethernet SSH client. To access the AP serial console menu using either method, follow these steps:

1. Connect a DB-9 to RJ-45 serial cable (rollover cable) to the AP's **CONSOLE** port, and connect the other end of the serial cable to the PC.



### NOTE

*The console port is not available on BSAP 1920 Series.*

2. Run a VT100 terminal emulation program with the following settings: 115,200 data rate, 8 data bits, no parity bits, 1 stop bit, and no flow control. Select **<Enter>** to access the serial console menu.
3. At the prompt, enter the user name **adm1n** and the password **vWl@nBlu3\$ock3t**.



### NOTE

*This is the default user name and password. If the AP has been configured with an AP template that has a different password, this password will change.*

OR

1. Configure an SSH client (for example, Putty) by ensuring that port **2335** is enabled.
2. Use the SSH client to connect to the AP using the AP's IP address (found in the DHCP server).

3. Log into the AP's serial console menu by entering the user name **adm1n** and the password **vWl@nBlu3\$ock3t** at the prompt.

**NOTE**

*This is the default user name and password. If the AP has been configured with an AP template that has a different password, this password will change.*

If the AP does not have any configuration from the vWLAN, connect to the serial console menu following these steps:

1. On the computer you are using to connect to the **Ethernet** port on the vWLAN appliance, create a static IP address on the same subnet as the AP. For example, create a static IP address of **192.168.190.2**.
2. Directly connect your computer to the **Ethernet** port. The **Ethernet** port is a standard Gigabit Ethernet port with a default IP address of **192.168.190.1**. Verify that there is IP connectivity by pinging the AP.
3. Configure an SSH client (for example, Putty) by ensuring that port **2335** is enabled.
4. Log into the AP's serial console menu by entering the user name **adm1n** and the password **vWl@nBlu3\$ock3t** at the prompt.

**NOTE**

*This is the default user name and password. If the AP has been configured with an AP template that has a different password, this password may change.*

## AP Serial Console Configuration Commands

There are several items you can configure once you have connected to the AP serial console menu. The following sections describe the BSAP serial console menu and some of the most frequently used options. You can also use the serial console to configure vWLAN mesh networking. Refer to the configuration guide [Mesh Networking in vWLAN](https://supportcommunity.adtran.com), available online at <https://supportcommunity.adtran.com>.

### Menus

The organization of the AP's serial console is in hierarchical menu trees. Once you have connected to the AP's serial console menu, you are presented with the main menu. You can then enter a number to access the corresponding options and additional menus.

```
|-----|
| Bluesocket Command Line Interface (CLI) |
|-----|
|-----System Status-----|
802.11 b/g Radio State: Inactive (Ch. -481)
802.11 a Radio State: Inactive (Ch. -481)
```



```

BSAP State: AP Interfaces Setup
|-----|
Configuring Radio: 802.11 b/g

(Main Menu)

1) Network Configuration
2) Save/Apply Configuration
3) Restore Defaults
4) Show Version Information
5) Reboot AP
a) Site Survey Configuration
e) Logout
f) Change Login Password

```

For example, to access the **Network Configuration** and its available options, from the main menu prompt, enter **1**:

```

Main->1
Network Cfg ->

```

## Viewing the Current Network Summary

To view the current network configuration for the AP, follow these steps:

1. From the **Main Menu**, select **1** to view the **Network Configuration**.
2. From the **Network Configuration** menu, select **8** to view the **Network Summary**.

```

Main ->1
Network Cfg ->8

```

```

|-----|
| Bluesocket Command Line Interface (CLI) |
|-----|
|-----System Status-----|
802.11 b/g Radio State: Inactive (Ch. -481)
802.11 a Radio State: Inactive (Ch. -481)
BSAP State: AP Interfaces Setup
|-----|
Configuring Radio: 802.11 b/g
(Network Configuration)
Acquiring IP Address - Please Wait

IP Address Mode: DHCP
IP Address: 0.0.0.0
Netmask: 0.0.0.0
Default Gateway: 0.0.0.0
Primary DNS: 0.0.0.0
Secondary DNS: 0.0.0.0
Domain Name: vwlantrain.com

```

```

Controller Addr Mode: Discover
Controller Addr Discover: 0.0.0.0
Controller Addr Primary(Secondary): 0.0.0.0(0.0.0.0)
Operating Mode: Controller Required
802.11b/g MAC: 00:19:92:09:d7:21
802.11a MAC: 00:19:92:09:d7:29
Ethernet MAC: 00:19:92:09:d7:20
Alias IP Address: 192.168.190.1
Hit Enter to continue...

```

## Specifying a Static IP Address

To specify a static IP address for the AP, follow these steps:

1. Select **1 (Set IP Address Mode)** from the **Network Configuration** menu.
2. From the **Enter IP Address Mode** menu, select **1** for **Static**.
3. Return to the **Network Configuration** menu and select **2 (Set IP Address)**.
4. Enter the IP address, network mask, gateway, and DNS information for the AP using the `<ip address> netmask <network mask> gw <gateway address> dns <dns address>` command.
5. Return to the **Main Menu** by selecting **P (Previous Menu)** and select **2 (Save/Apply Configuration)**.

```

Main ->1
Network Cfg ->1
Enter mode (0) ->1
Network Cfg ->2
Enter IP/netmask ->172.20.5.50 netmask 255.255.255.0 gw 172.20.5.1 dns
    172.16.0.240
Network Cfg ->P
Main ->2

```

## Specifying the AP Mode is Static

To specify the AP mode is static (a mode that is commonly used in an MSP scenario), and to enter the static IP address, follow these steps:

1. Select **5 (Set Controller Mode)** from the **Network Configuration** menu.
2. From the **Enter Controller Address Mode** menu, select **1** for **Static**.
3. Return to the **Network Configuration** menu and select **6 (Set Controller Address)**.
4. Enter the primary controller IP address using the `<ip address>` command or enter the primary and secondary controller IP addresses using the `<ip address> sec <ip address>` command.
5. Return to the **Main Menu** by selecting **P (Previous Menu)** and select **2 (Save/Apply Configuration)**.

```

Main ->1

```

```
Network Cfg ->5  
Enter mode (0) ->1  
Network Cfg ->6  
Enter Controller Addresses ->172.16.0.5  
Network Cfg ->P  
Main ->2
```

## 11. vWLAN Wireless Configuration

Once your vWLAN domains and APs have been configured, you must configure the wireless parameters for your AP. Wireless configuration revolves around configuring SSIDs, SSID security parameters, using an AP template model, understanding AP status indications, using DynamicRF, and configuring wireless roaming parameters and tunnel profiles. The following subjects are described in this section:

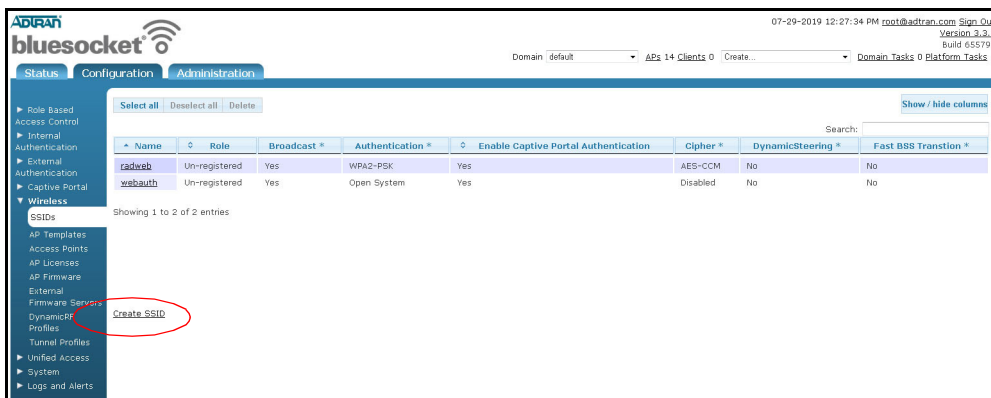
- [Configuring an SSID on page 188](#)
- [Configuring a Tunnel Profile on page 198](#)
- [Viewing Adjacent AP Neighbors on page 201](#)

SSIDs represent a particular 802.11 wireless LAN. In vWLAN, there can be up to 16 SSIDs per AP (8 per radio). An SSID provides a unique set of connection parameters by broadcasting independent security attributes. An SSID can be configured for both radios, for the 2.4 Ghz radio only, for the 5 GHz radio only, or for neither radio. In addition, SSIDs can be linked to the login page viewed by customers, allowing you to specify a specific login page based on SSID.

### Configuring an SSID

To allow wireless clients to connect to the vWLAN network, each AP domain must have at least one SSID. To configure an SSID, connect to the GUI and follow these steps:

1. Navigate to the **Configuration** tab, and select **Wireless > SSIDs**. Here any previously configured SSIDs are listed, and the name, role, broadcast, authentication method, accounting server, and cipher type for each SSID is displayed. You can edit an already configured SSID by selecting the SSID from the list. To create a new SSID, select **Create SSID** from the bottom of the menu or select **Domain SSID** from the **Create** drop-down menu (at the top of the menu).



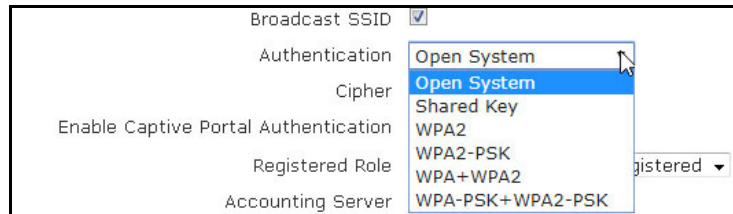
2. Enter a name for the SSID. SSID names can be up to 31 characters in length.
3. Next, enable SSID broadcasting by selecting the **Broadcast SSID** check box.

**Create SSID**

Name/ESSID

Broadcast SSID

4. Next, determine the type of authentication to be used by the SSID. Authentication options and methods can be influenced by the use of Captive Portal (discussed in Step 5 on [page 192](#)) so it is important to keep the desired Captive Portal settings for the SSID in mind when configuring the authentication parameters. Select the proper authentication method for the SSID from the **Authentication** drop-down menu. Authentication choices include: **Open System**, **Shared Key**, **WPA2**, **WPA2-PSK**, **WPA+WPA2**, **WPA-PSK+WPA2-PSK**.



Descriptions of each authentication type are provided as follows:

**Open System:** Open system authentication means that there is no client verification when a client attempts to connect to the SSID. With open system, you can choose not to use a cipher for data protection, or you can use wired equivalent privacy (WEP) as your cipher. To select open system as the authentication method for this SSID, without a cipher, select **Open System** from the **Authentication** drop-down menu and proceed to Step 7 on [page 194](#).



#### NOTE

*WEP use should be limited because it is not as secure as AES-CCM and it does not allow clients to use 802.11n data rates. You should only enable WEP if you have legacy (pre-2005) clients in your network that cannot be upgraded.*

- If you want to use WEP authentication with an open system, select **WEP** from the **Cipher** drop-down menu. Specify whether you will use a **64 Bit** or **128 Bit** key from the **WEP Key Size** drop-down menu. If you are using a **64 Bit** key, you will be prompted to enter up to 4 WEP keys of 10 hexadecimal characters each (at least one key is required). Then select the default key to use from the **Default** drop-down menu and proceed to Step 6 on [page 194](#).
- If you are using a **128 Bit** key, enter the 26 character hexadecimal key in the **128-Bit WEP Key** field, and proceed to Step 6 on [page 194](#).



#### NOTE

*WEP keys can be generated online at <http://www.wepkey.com/>. The hexadecimal characters generated for WEP keys can differ from PCs to MACs. Note that there are known issues at the AP level when using WEP with the BSAP 1800 Series.*

**Shared Key:** Shared key authentication means that clients connect to the SSID by presenting a key shared by the client and the SSID. To select shared key as the authentication method for this SSID, select **Shared Key** from the **Authentication** drop-down menu. When using shared keys, you must

use the WEP cipher. Select **WEP** from the **cipher** drop-down menu. Specify whether you will use a **64 Bit** or **128 Bit** key from the **WEP Key Size** drop-down menu.

**NOTE**

*WEP use should be limited because it is not as secure as AES-CCM and it does not allow clients to use 802.11n data rates. You should only enable WEP if you have legacy (pre-2005) clients in your network that cannot be upgraded.*

- If you are using a 64 Bit key, you will be prompted to enter up to 4 WEP keys of 10 hexadecimal characters each (at least one key is required). Then select the default key to use from the Default drop-down menu and proceed to Step 6 on [page 194](#).
- If you are using a 128 Bit key, enter the 26 character hexadecimal key in the 128-Bit WEP Key field, and proceed to Step 6 on [page 194](#).

**WPA2:** Wi-Fi protected access (WPA) 2 is an enterprise authentication method that allows clients to connect to the SSID with RADIUS 1X authentication using Advanced Encryption Standard and Counter Mode CBC MAC Protocol (AES-CCM) encryption. To select WPA2 as the authentication method for this SSID, select **WPA2** from the **Authentication** menu. **AES-CCM** will automatically be selected from the **Cipher** drop-down menu.

The screenshot shows the 'Create SSID' configuration interface. It includes fields for 'Name/ESSID' (set to 'Architecture') and 'Broadcast SSID' (checked). The 'Authentication' dropdown menu is set to 'WPA2' and the 'Cipher' dropdown menu is set to 'AES-CCM'. A red oval highlights these two dropdown menus. There is also an 'Enable Captive Portal Authentication' checkbox which is unchecked.

**WPA2-PSK:** WPA2 with PSK is a personal authentication method that allows you to specify a pass phrase used to connect to this SSID. This method supports AES-CCM encryption. To select WPA2-PSK as the authentication method for this SSID, select **WPA2-PSK** from the **Authentication** menu. **AES-CCM** will automatically be selected from the **Cipher** drop-down menu. You will also be prompted to specify a preshared key for this authentication type. Preshared keys must be eight digits or greater.

WPA2-PSK can be used with a registered or un-registered role. With a registered role, users are authenticated by providing the preshared key. Upon providing the correct preshared key, users are placed into the specified registered role. With an un-registered role, users are first authenticated by

providing the preshared key. Then, they are redirected to the login page for Captive Portal authentication.

A screenshot of a configuration form showing the following fields:

- Authentication: WPA2-PSK (dropdown menu)
- Cipher: AES-CCM (dropdown menu)
- Preshared Key: [Redacted with dots]
- Preshared Key Confirmation: [Redacted with dots]



#### NOTE

With the WPA2-PSK authentication method, as of vWLAN firmware release 3.5.0, you can optionally choose to configure multiple keys to be used on a per-client basis. This feature allows clients to authenticate each device with a different password, rather than using the single shared key for all connecting clients. Refer to [Configuring WPA2-Multikey Client Connections on page 238](#) for more information about configuring this feature.

**WPA+WPA2:** WPA with WPA2 is an enterprise authentication method that allows the end client to choose between WPA and WPA2. This method supports Temporal Key Integrity Protocol (TKIP) and AES-CCM encryption. To select WPA+WPA2 as the authentication method for this SSID, select **WPA+WPA2** from the **Authentication** menu, and specify whether the SSID will use AES-CCM only or **TKIP or AES-CCM** from the **Cipher** drop-down menu.

A screenshot of the 'Create SSID' configuration form with the following settings:

- Name/ESSID: Architecture
- Broadcast SSID:
- Authentication: WPA+WPA2 (dropdown menu)
- Cipher: AES-CCM (dropdown menu, with a mouse cursor pointing to it)
- Enable Captive Portal Authentication:
- Registered Role: Architecture Faculty Registered (dropdown menu)



#### NOTE

WPA is not as secure as WPA2. You should only enable WPA if you have legacy wireless clients in your environment that cannot be upgraded to a more recent wireless driver.



#### NOTE

TKIP use should be limited because it is not as secure as AES-CCM and it does not allow clients to use 802.11n data rates. You should only enable TKIP if you have legacy (pre-2005) clients in your network that cannot be upgraded.

**WPA-PSK+WPA2-PSK:** WPA-PSK with WPA2-PSK is a personal authentication method that combines the features of WPA-PSK and WPA2-PSK. This method supports TKIP and AES-CCM encryption methods. To select WPA-PSK+WPA2-PSK as the authentication method for this SSID, select **WPA2-PSK+WPA2-PSK** from the **Authentication** menu, and specify whether the SSID will use **AES-CCM** only or **TKIP or AES-CCM** from the **Cipher** drop-down menu. You will also be prompted to specify a preshared key for this authentication type. Preshared keys must be eight digits or greater.

WPA-PSK+WPA2-PSK can be used with a registered or un-registered role. With a registered role, users are authenticated by providing the preshared key. Upon providing the correct preshared key, users are placed into the specified registered role. With an un-registered role, users are first authenticated by providing the preshared key. Then, they are redirected to the login page for Captive Portal authentication

The screenshot shows the 'Create SSID' configuration interface. The 'Authentication' dropdown menu is set to 'WPA-PSK+WPA2-PSK'. The 'Cipher' dropdown menu is set to 'AES-CCM'. The 'Preshared Key' and 'Preshared Key Confirmation' fields are filled with asterisks. The 'Broadcast SSID' checkbox is checked, and the 'Multi Key' checkbox is unchecked. Red circles highlight the Authentication, Cipher, and Preshared Key fields.



#### NOTE

*TKIP use should be limited because it is not as secure as AES-CCM and it does not allow clients to use 802.11n data rates. You should only enable TKIP if you have legacy (pre-2005) clients in your network that cannot be upgraded.*

- If you are using the **WPA2-PSK** method for authentication, you can choose to use the multikey feature for client connections by selecting the **Multi Key** check box. Selecting this option means that each client connecting to the network uses a unique preshared key after authenticating with a RADIUS server. When this feature is enabled, Captive Portal Authentication is not available for client connections (the **Enable Captive Portal Authentication** check box cannot be selected), and a RADIUS authentication server must be specified from the **RADIUS Multi Key Authentication Server** drop-down menu, as shown below. Once the multikey feature has been enabled, and the



RADIUS authentication server has been specified, you can continue SSID configuration by proceeding to Step 10 on [page 195](#).

The screenshot shows the 'Create SSID' configuration interface. The 'Name/ESSID' field contains 'PSK SSID'. The 'Broadcast SSID' checkbox is checked. The 'Authentication' dropdown is set to 'WPA2-PSK'. The 'Cipher' dropdown is set to 'AES-CCM'. The 'Multi Key' checkbox is checked and circled in red. The 'Enable Captive Portal Authentication' checkbox is unchecked. The 'RADIUS Multi Key Authentication Server' dropdown is set to 'Local-FreeRadius' and is also circled in red. The 'DynamicSteering' checkbox is unchecked.



#### NOTE

When the WPA2-Multikey feature is enabled, not only is Captive Portal Authentication unavailable, but you also cannot specify a role for connecting clients. For more information about this feature, its configuration, and its use, refer to [Configuring WPA2-Multikey Client Connections on page 238](#), or refer to the configuration guide [WPA2-Multikey and Rolling-PMK in vWLAN](#), available online at <https://supportcommunity.adtran.com>.



#### NOTE

The RADIUS Multi Key Authentication Server can be configured using the RADIUS server configuration instructions provided in [External RADIUS Web-based Authentication Server on page 113](#).

- If not using Captive Portal Authentication, leave the box unchecked next to **Enable Captive Portal Authentication**. When Captive Portal is not selected, there are more available **Authentication** options versus when captive portal is selected. You can only specify a **Registered Role** when not using captive portal. You can use the default **Guest** registered role or a previously configured registered role (See [Configuring Domain Roles on page 96](#) for additional information on configuring roles).



#### NOTE

You must enable Captive Portal and choose an Un-registered role to allow clients to authenticate with web-based authentication. If you choose a Registered role (and bypass web and MAC authentication), you should either use a strong PSK to protect it, or limit the firewall policy on the role to protect your internal assets. Choosing a Registered Role also allows the SSID to be configured for RADIUS accounting (to track users).

If using Captive Portal Authentication, select the check box next to **Enable Captive Portal Authentication**. When Captive Portal is selected, there are fewer available **Authentication** options versus when captive portal is not selected. Also, you can only specify an **Un-registered Role** when using captive portal. You can specify the default **Un-registered** role or a previously configured un-registered role (See [Un-Registered Role Type on page 98](#) for information on configuring un-registered roles, Captive Portal, and the Walled Garden feature).

The screenshot shows the 'Create SSID' configuration page with the following settings:

- Name/ESSID: Architecture
- Broadcast SSID:
- Authentication: Open System
- Cipher: Disabled
- Enable Captive Portal Authentication:
- Registered Role: Architecture Faculty Registered

- Once you have selected the authentication, cipher, and preshared key (if necessary) information for the SSID, and configured the Captive Portal settings, specify the login form to be associated with the SSID by selecting the appropriate form from the **Login Form** drop-down menu. By default, each SSID will use the default login form. If you have not created another login form, this will be the only option (refer to [Customizing vWLAN Login Forms and Images on page 207](#) for more information). You can select another login form if one has been created, or you can choose to use the default form from the AP template.
- Specify an Accounting Server (if applicable). You can specify an accounting server if you are not enabling Captive Portal and only with certain authentication options. See [Configuring Domain Accounting on page 131](#) for information on configuring accounting servers.

The screenshot shows the 'Create SSID' configuration page with the following settings, and the Accounting Server field is highlighted with a red circle:

- Name/ESSID: Architecture
- Broadcast SSID:
- Authentication: Open System
- Cipher: Disabled
- Enable Captive Portal Authentication:
- Registered Role: Architecture Faculty Registered
- Accounting Server: accountingserver1

- Enable Remote Site Survivability (option only available when captive portal is enabled). As of vWLAN release 3.2.0, a feature was added that supports Remote Site Survivability for PSK and open SSIDs. If the connection between the AP and both the primary and secondary vWLAN is severed, new pre-shared key and open SSID clients will be able to connect. Select **Allow new**

clients to use the network when the vWLAN is down and specify the Role to be assigned when vWLAN is down.

The screenshot shows the 'Create SSID' configuration interface. The 'Role to be assigned when vWLAN is down' dropdown menu is highlighted with a red oval and set to 'Guest'. Other visible settings include: Name/ESSID: Architecture; Broadcast SSID: checked; Authentication: Open System; Cipher: Disabled; Enable Captive Portal Authentication: checked; Registered Role: Architecture Faculty Registered; Accounting Server: empty; Allow new clients to use the network when vWLAN is down: checked.



#### NOTE

*Captive Portal must be enabled to use this feature. Captive Portal is automatically enabled when a PSK SSIDs is created.*

10. Select **DynamicSteering** (optional) to enable this SSID to steer dual-band capable Wi-Fi clients between the 2.4 GHz and 5 GHz bands, which ensures optimal band utilization. This is a robust feature and additional details are provided in the [DynamicSteering in vWLAN Configuration Guide](#) available from the ADTRAN support community.



#### NOTE

*The SSID must be applied to both the 2.4 GHz and 5 GHz radios for each AP through the AP template. If DynamicSteering is enabled and the SSID is only used on one band, DynamicSteering will be disabled.*

The screenshot shows the 'DynamicSteering' checkbox checked and circled in red. Below it, there is a description: 'Enables band/client steering, load balancing, and sticky client prevention technology (including 802.11k and 802.11v). Requires SSID assigned to both radio bands on the AP template.' There are also two other options: 'Convert Multicast/Broadcast Network Traffic To Unicast' and 'Convert broadcast and multicast to unicast'.

11. Select **802.11r Fast BSS Transition** (optional) to enable continuous connectivity for wireless devices in motion, with fast, secure, and seamless handoffs from one base station to another managed Basic Service Set (BSS) within the same Extended Service Set (ESS)

The screenshot shows the '802.11r Fast BSS Transition' checkbox checked and circled in red. Below it, there is a description: 'Non 802.11r compliant clients will not be able to connect to this ssid. Not supported on 18xx and 30xx models. Enabling 802.11r on 30xx will not broadcast SSID.'

**i** **NOTE**

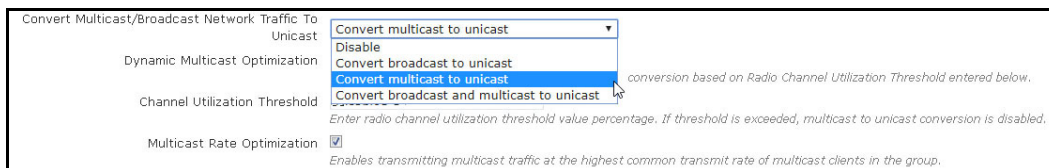
*This option is only available when WPA2-PSK or WPA-PSK+WPA2-PSK authentication methods are enabled. Non 802.11 compliant clients will not be able to connect to this SSID. In addition, if the WPA2-Multikey feature is enabled, this option is not available. For more information about the WPA2-Multikey feature, refer to the configuration guide [WPA2-Multikey and Rolling-PMK in vWLAN](https://supportcommunity.adtran.com), available online at <https://supportcommunity.adtran.com>.*

**i** **NOTE**

*Not supported on 18xx and 30xx models. Enabling 802.11r on 30xx will not broadcast SSID.*

- Specify whether the SSID will convert multicast or broadcast network traffic to unicast traffic by selecting the appropriate option from the **Convert** drop-down menu. By default, **Convert broadcast and multicast to unicast** is enabled. Other options are **Disable**, **Convert broadcast to unicast**, and **Convert multicast to unicast**.

Multicast transmissions are typically sent from one source to several destinations or to all destinations. From a security standpoint, it is difficult to configure the firewall properly for multicast transmissions between different client types. Converting multicast to unicast allows you to police traffic more efficiently to IP addresses or specific users. In addition, when multicast and broadcast transmissions are sent wirelessly, they use the lowest data rate available, resulting in lower performance than unicast transmissions. If traffic is converted from broadcast or multicast to unicast, it is sent using a higher data rate which improves performance, using less air time. Broadcast traffic must be sent to all clients, and therefore it is sent at the rate of the slowest client. Unicast traffic is sent to a single client, therefore it can be sent at the speed of each client rather than that of the slowest client.



**i** **NOTE**

*If you do not choose to convert multicast network traffic to unicast traffic, you must allow multicast traffic in the default role of the SSID (refer to [Step 7 on page 194](#) and [Configuring Domain Roles on page 96](#)). Note that the default role of an 802.1x SSID is **Un-registered**. If you do not allow multicast traffic in the SSID's default role, and you do not choose to convert multicast traffic to unicast traffic in the SSID, then multicast traffic from a unified access host or wireless client on another AP will not be seen.*

When **Convert multicast to unicast** or **Convert broadcast and multicast to unicast** is selected, additional multicast optimization options are available.

Dynamic Multicast Optimization	<input checked="" type="checkbox"/>	<i>Dynamically enables or disables multicast to unicast conversion based on Radio Channel Utilization Threshold entered below.</i>
Channel Utilization Threshold	<input type="text" value="80"/>	<i>Enter radio channel utilization threshold value percentage. If threshold is exceeded, multicast to unicast conversion is disabled.</i>
Multicast Rate Optimization	<input checked="" type="checkbox"/>	<i>Enables transmitting multicast traffic at the highest common transmit rate of multicast clients in the group.</i>

**Dynamic Multicast Optimization** automatically switches between sending multicast traffic over-the-air as unicast (converting to unicast) and sending natively as multicast to ensure the most efficient use of airtime. The switch point is based on the threshold configured in the Channel Utilization Threshold.

**Channel Utilization Threshold** is the radio channel utilization threshold value as a percentage. When this threshold is exceeded, multicast to unicast conversion is disabled. A log message (**Status > Logs**) is generated when multicast to unicast is toggled on/off.

**Multicast Rate Optimization** enables transmission of multicast traffic at the highest common transmit rate of the multicast clients in the group. In cases where DMO determines that it is more efficient to send traffic over-the-air as multicast, traffic is sent at the lowest data rate amongst connected clients instead of lowest 802.11 basic data rate. This optimization works in conjunction with DynamicSteering to ensure traffic is sent at the highest data rates possible.

13. Select **Tunnel WLAN Traffic** (optional) to tunnel SSID traffic to a Wireless Aggregation Gateway (WAG) if a tunnel profile is enabled in the AP template for an AP (refer to [Configuring a Tunnel Profile on page 198](#) for more information about tunnel profiles.)

DHCP Option 82 enables the WAG to prevent DHCP client requests from untrusted sources. When Tunnel WLAN Traffic is enabled, all client traffic connected to the SSID is GRE encapsulated. Upon receipt of a DHCP discover or request, the BSAP will add option 82 to these packets. You can specify the Circuit ID and Remote ID to be used from the drop-down menus.

Tunnel WLAN Traffic	<input checked="" type="checkbox"/>	<i>Not supported on 3XXX model APs.</i>
DHCP Option 82	<input checked="" type="checkbox"/>	
DHCP Option 82 Circuit ID	<input type="text" value="SSID"/>	
DHCP Option 82 Remote ID	<input type="text" value="HOSTNAME"/> <ul style="list-style-type: none"> <li>HOSTNAME</li> <li>HOSTNAME</li> <li>HOSTNAME+SYSLOCATION+MAC</li> <li>AP-RADIO-MAC</li> <li>CLIENT_MAC</li> </ul>	

14. Select **Create SSID**. A confirmation will be displayed indicating the SSID was successfully created.
15. The SSID is now available for editing or deletion, and can be applied to APs through AP templates (refer to [Configuring AP Templates on page 149](#)).

## Configuring a Tunnel Profile

Creating a tunnel profile provides the ability to tunnel SSID traffic to a specified gateway. Unlike Layer 3 mobility, which allows seamless roaming of SSIDs from one subnet to another subnet, this type of tunneling is used for routing AP traffic to a central location. With the tunneling profile enabled, a tunnel gets created from the AP to the WAG defined in the tunnel profile. All client traffic on the AP goes through the tunnel to the endpoint network instead of routing through the local network.

Using a tunnel profile requires the following:

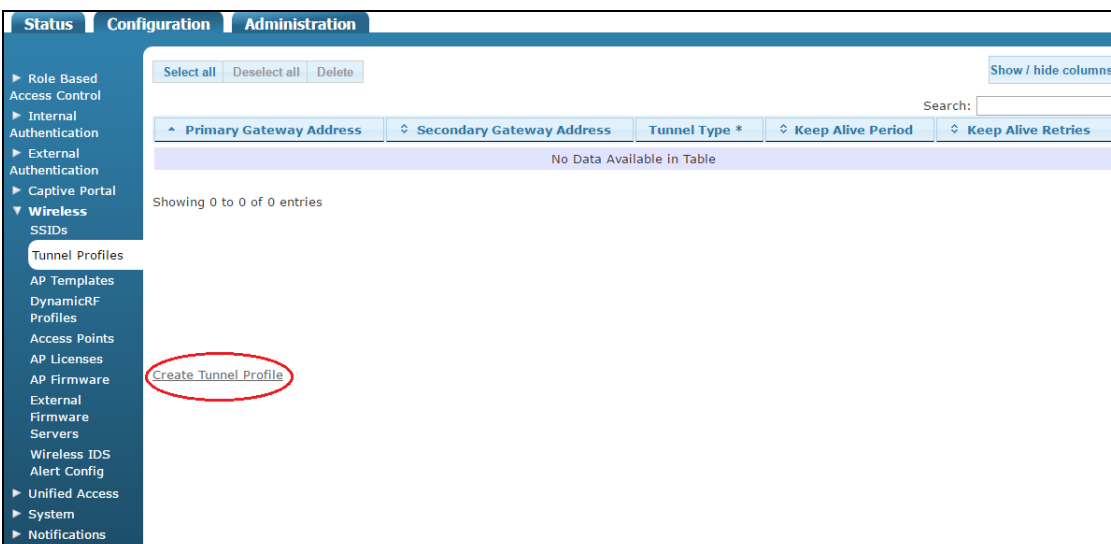
- Configuring the tunnel profile (refer to [Configuring a Tunnel Profile on page 198](#))
- Enabling the tunnel in the AP template (refer to [Configuring AP Templates on page 149](#))
- Enabling WLAN traffic for the SSID (refer to [Configuring an SSID on page 188](#))

In addition, there can be interactions between a tunnel profile and a defined user role (refer to [Configuring Domain Roles on page 96](#)). The following role definitions must be considered when configuring the tunnel profile:

- All quality of service (QoS) configurations must be handled by the WAG, and not the user role. There is no traffic shaping being handled by vWLAN for tunneled traffic.
- All firewall configurations are also handled by the WAG, and not the user role. Firewall rules are not enforced by vWLAN for tunneled traffic.
- vWLAN tunneling supports tagged VLANs. The location is specified within the role.
- Tunneled traffic flows do not support the location and location group feature of vWLAN.

To configure a tunnel profile, follow these steps:

1. Navigate to the **Configuration** tab and select **Wireless > Tunnel Profiles**. To create a new tunnel profile, select **Create Tunnel Profile** at the bottom of the menu. To edit a previously created tunnel profile, select the profile from the list.



- Specify the tunnel type using the drop-down menu.

**Create Tunnel Profile**

Select Tunnel Type **GRE Tunnel ▾**

Primary Gateway Address   
*Only IP Address is accepted.*

Secondary Gateway Address   
*Optional. Only IP Address is accepted.*

Keep Alive Period   
*Valid range is from 30 to 300.*

Keep Alive Retries   
*Valid range is from 2 to 10.*

[Back](#)

- Enter the IP address for the primary gateway that will serve as the termination point for the tunnel. Optionally, you may also enter a secondary gateway address.

**Create Tunnel Profile**

Select Tunnel Type **GRE Tunnel ▾**

Primary Gateway Address   
*Only IP Address is accepted.*

Secondary Gateway Address   
*Optional. Only IP Address is accepted.*

Keep Alive Period   
*Valid range is from 30 to 300.*

Keep Alive Retries   
*Valid range is from 2 to 10.*

[Back](#)

- Specify the keep alive period in seconds. This interval defines how often to send keep alive messages used to keep the tunnel open.

### Create Tunnel Profile

Select Tunnel Type

Primary Gateway Address   
*Only IP Address is accepted.*

Secondary Gateway Address   
*Optional. Only IP Address is accepted.*

Keep Alive Period   
*Valid range is from 30 to 300.*

Keep Alive Retries   
*Valid range is from 2 to 10.*

[Back](#)

- Specify the number of times to resend the keep alive message if no response is received before closing the tunnel.

### Create Tunnel Profile

Select Tunnel Type

Primary Gateway Address   
*Only IP Address is accepted.*

Secondary Gateway Address   
*Optional. Only IP Address is accepted.*

Keep Alive Period   
*Valid range is from 30 to 300.*

Keep Alive Retries   
*Valid range is from 2 to 10.*

[Back](#)



6. Select **Create Tunnel Profile** to create the profile.

### Create Tunnel Profile

Select Tunnel Type GRE Tunnel ▼

Primary Gateway Address   
*Only IP Address is accepted.*

Secondary Gateway Address   
*Optional. Only IP Address is accepted.*

Keep Alive Period   
*Valid range is from 30 to 300.*

Keep Alive Retries   
*Valid range is from 2 to 10.*

Create Tunnel Profile

[Back](#)

## Viewing Adjacent AP Neighbors

Because vWLAN operates using a distributed data plane architecture, APs must be aware of adjacent APs to guarantee fast client roaming times between APs. vWLAN uses DynamicRF and a centralized control plane to detect and optimize neighbor APs into clusters, and proactively shares client information (such as roles, 802.1X keys, and session information) between APs. vWLAN will automatically discover and configure neighbors, so no configuration is required, but you can view the adjacent neighbors detected.

To view autodetected AP adjacencies, connect to the GUI and follow these steps:

1. Navigate to the **Status** tab, and select **Adjacent APs**. In this menu, the APs adjacent to the domain are listed along with their source MAC address, SSID, channels, channel range, signal strength, sensor name, and last seen information.

Source MAC	SSID	Primary Channel	Channel Range	Signal (dBm)	Sensor Name	Last Seen
<a href="#">00:19:92:00:79:21</a>	1800	1	1 (20 MHz)	-84	BSAP1920-00-19-92-35-2d-40	2014-02-20 07:55:48 UTC
<a href="#">00:19:92:00:79:23</a>	1930	1	1 (20 MHz)	-84	BSAP1920-00-19-92-35-2d-40	2014-02-20 09:23:57 UTC
<a href="#">F8:E4:FB:85:8A:AF</a>	7WTTL	6	6 (20 MHz)	-81	BSAP1920-00-19-92-35-2d-40	2014-02-20 16:40:17 UTC
<a href="#">00:19:92:02:E6:81</a>	AdelaSSID	11	11 (20 MHz)	-83	BSAP1920-00-19-92-35-2d-40	2014-02-20 09:23:57 UTC
<a href="#">C0:25:5C:68:17:50</a>	Allscripts-BPARK	6	6 (20 MHz)	-76	BSAP1920-00-19-92-35-2d-40	2014-02-20 16:40:16 UTC
<a href="#">C0:25:5C:68:17:51</a>	Allscripts-Corporate	6	6 (20 MHz)	-75	BSAP1920-00-19-92-35-2d-40	2014-02-20 16:40:16 UTC
<a href="#">C0:25:5C:68:17:55</a>	Allscripts-Guest	6	6 (20 MHz)	-76	BSAP1920-00-19-92-35-2d-40	2014-02-20 16:40:17 UTC

Showing 1 to 90 of 90 entries

2. Selecting the entry link in the **Source MAC** column will attempt to locate the adjacency on a heat map (if configured).

## 12. vWLAN Unified Access Configuration

vWLAN supports unified access and third-party AP connections. Unified access and third-party AP users look like wireless users to vWLAN, and they operate using the same types of user authentication, roles, and policies as wireless clients. The difference, however, is that unified access and third-party AP users do not connect to an SSID. Rather, they connect to an untrusted VLAN. vWLAN software supports unified access and third-party AP user authentication and traffic forwarding decisions at the edge of the network. Therefore, no additional hardware is required, since the AP is used as an in-line policy enforcement device. Unified access and third-party AP traffic flows into the Bluesocket AP through an untrusted VLAN, where the traffic is authenticated and policed (at Layer 2), and then it flows out of the Bluesocket AP as wireless traffic would, through a trusted (either tagged or native) VLAN.

Unified access services require an additional unified access license for each AP that will support unified access users. By default, APs are not licensed for unified access users, and you must request a unified access license for each AP. Refer to [Licensing APs on page 148](#) for information about requesting licenses.

Configuring unified access support in vWLAN revolves around configuring a unified access group (which functions in similar fashion to an SSID for wireless users), configuring switches for unified access users, configuring unified access redundancy, and monitoring the status of unified access users. These subjects are covered in the following sections:

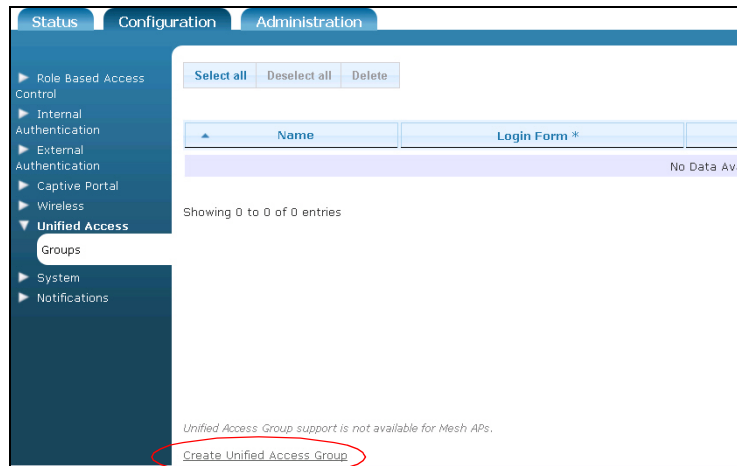
- [Configuring Unified Access Groups on page 202](#)
- [Configuring Switches for Unified Access on page 205](#)
- [Unified Access Redundancy on page 205](#)
- [Viewing the Status of Unified Access Users on page 206](#)

### Configuring Unified Access Groups

Unified access groups function in the same way that SSIDs function for wireless users. Unified access groups provide security attributes and a set of untrusted VLANs for connecting users. To configure a unified access group, follow these steps:

1. Navigate to the **Configuration** tab, and select **Unified Access > Groups**. Here any previously configured unified access groups are listed, and the name, login form, accounting server, and associated VLANs for each access group is displayed. You can edit an already configured access group by selecting the unified access group from the list. To create a new unified access group,

select **Create Unified Access Group** from the bottom of the menu or select **Domain Unified Access Group** from the **Create** drop-down menu (at the top of the menu).



2. Enter the name of the access group in the **Name** field. The name must conform to host name standards from RFC 952, and can be up to 32 characters long. This name will be displayed in active connections summaries.
3. Enter the roaming SSID for the unified access group in the **Roaming SSID** field. Roaming SSIDs determine whether roaming is allowed between Bluesocket and third-party APs. When unified access traffic is seen by the AP, vWLAN has no way to know whether that traffic is from a hard-wired client or bridged through a third-party AP. If this value is set in the unified access group, then vWLAN treats the unified access group as being from a third-party AP with the specified SSID. When specified, if a user roams to or from this unified access group to an actual BSAP with the same SSID, then the user does not have to reauthenticate. The roaming SSID can be up to 32 characters in length, and should match an advertised SSID on the AP.
4. Enter the DHCP override value in the **DHCP** field. This value overwrites the DHCP lease time configured on the network's DHCP server. If this value is set to 0, then no override takes place, and the clients receive the DHCP lease time from the normal DHCP server. By default, this value is set to **20** seconds. The valid range is **7** to **86400** seconds. This setting can be useful because it allows administrators to force a logout or timeout for unified access users. In web-based authentication, a logout forces the user to return to the un-registered role and reobtain a NAC address from the AP. Since the DHCP lease time from the network DHCP server can be lengthy, the AP must override it to force the client back to the NAC address without the need to manually release and renew the IP address (or reboot the AP).
5. Enter the VLANs associated with the unified access group by entering the VLANs (or a range of VLANs) in a list (separated by commas) in the **VLANs** field. The listed VLANs cannot be overlapping. This is a list of untrusted VLANs used by the unified access group to obtain access to the vWLAN network. Untrusted VLANs are VLANs that carry untrusted unified access group traffic from a port where the client is connected to the trunk port where the AP is connected. There are two restrictions to VLANs associated with unified access groups: an untrusted VLAN can only be a member of a single unified access group, and an untrusted VLAN cannot overlap with a trusted location. Therefore, no two unified access groups can share the same untrusted VLAN because the untrusted

VLAN tag is used to determine the unified access group, and if a trusted location exists with a specific VLAN, then that VLAN cannot be part of any unified access group.

**NOTE**

*VLAN IDs 0 and 1 are not allowed.*

6. Select the login form to associate with the unified access group from the **Login Form** drop-down menu. This is the login form that will be viewed by unified access group users connecting to the vWLAN network. You can select from a previously created login form, or use the default form. For more information about creating login forms, refer to [Customizing vWLAN Login Forms and Images on page 207](#).
7. Select the user role to associate with clients connecting to vWLAN through this unified access group from the **Role** drop-down menu. This role is the role in which all users are initially placed when connecting. Depending on the authentication strategy for unified access users, this should be either the **Un-registered** (default) role, or a specific role. For more information about creating roles, refer to [Configuring Domain Roles on page 96](#).
8. If you selected a specific role (rather than the default role of **Un-registered**), then you will be prompted to also specify an accounting server to associate with this unified access group. Select the accounting server from the **Accounting server** drop-down menu. The accounting server will track the user throughout their use of vWLAN. For more information about creating accounting servers, refer to [Configuring Domain Accounting on page 131](#).

**Create Unified Access Group**

Name   
Enter up to 32 characters.

Roaming SSID   
Enter up to 32 characters to allow third party roaming.

DHCP   
DHCP override (seconds).

VLAN   
Enter a list of VLANs i.e. 100,200-204,400.

Login Form

Role

Accounting server

**NOTE**

*To support 802.1X authentication for unified access group users or third-party APs, the switches or third-party APs should perform 802.1X authentication, and the unified access group should be set to a default role in vWLAN. Because authentication is performed on the front end, vWLAN assumes it received traffic from a user that has been authenticated, and therefore puts the user in a default role without further authentication.*

9. Once you have entered the correct information, select **Create Unified Access Group** to create the access group. You will receive confirmation that the access group has been created.
10. The created access group is now available for editing or deletion, and will appear in the unified access group list (**Configuration** tab, **Unified Access > Group**).

## Configuring Switches for Unified Access

In a vWLAN network, additional switches are often used when configuring unified access. You can configure a single switch or multiple switches to connect to vWLAN.

In a single switch configuration, the unified access users and the AP are on the same switch. To configure an AP that is connected to an edge switch to support both unified access and wireless users simultaneously, three configurations are necessary on the switch:

1. An untrusted VLAN must be added to the switch (to support unified access connections to vWLAN).
2. A unified access user port (or ports) must be configured as the access port(s) assigned to the untrusted VLAN.
3. The AP's port must be configured as an 802.1q trunk port (if it is not already), and the port must be configured to allow the untrusted VLAN.

In a multiple switch configuration, the unified access users and the AP are on different switches. To configure an AP that is connected to a different edge switch than the unified access users, two configurations are necessary:

1. An untrusted VLAN tag, for the untrusted VLAN used by unified access users, must be added to the switch uplink port on the first switch (the switch used by the unified access users).
2. The untrusted VLAN must then be trunked to the second switch (the switch used by the AP).

This configuration can be useful to support unified access users when all the APs in the vWLAN network are connected to dedicated Power over Ethernet (PoE) switches with no available ports.



### NOTE

*Although you can configure a multiple switch configuration for unified access to vWLAN, it is recommended to have clients and the AP on the same switch.*

## Unified Access Redundancy

There are two types of unified access redundancy available on vWLAN: vWLAN redundancy and unified access AP redundancy. vWLAN redundancy is achieved through high availability. If high availability is configured, then both unified access and wireless users will failover with zero packet loss during a vWLAN failover (refer to [Configuring High Availability on page 68](#) for more information about high availability).

Unified access AP redundancy can occur when an AP servicing an untrusted VLAN segment fails. Two scenarios can occur: first, if there is no other unified access licensed AP with access to that VLAN segment, then the segment is down and all users cannot pass traffic until the failed AP recovers. Second, if there are one or more APs with unified access licenses that can access that VLAN segment, then the system chooses the least loaded AP to take over the untrusted VLAN segment.

There may be some packet loss as the system detects the down event and reassigns the untrusted VLAN or as the switches relearn the bridge table. Client reauthentication is not required during unified access AP redundancy.

## Viewing the Status of Unified Access Users

vWLAN autodiscovers the VLANs that are available for APs with unified access licenses. The system detects whether two APs are on the same untrusted VLAN segment by determining if the two APs see the same client traffic, allowing the system to ensure that only one AP is active at any point on each untrusted VLAN segment. The administrator can view which APs are active on which segments, which gives insight to the load balancing used by vWLAN and facilitates troubleshooting.

To view the status of unified access groups, navigate to the **Status** tab, and select **Unified Access Groups**. The name, status, AP host name, roaming SSID, segment, and untrusted VLANs for each configured unified access group are displayed.

The screenshot shows the vWLAN administrator interface with the 'Status' tab selected. The left sidebar contains navigation options: Dashboards, Clients, Access Points, Adjacent APs, Locations, Unified Access Groups, Alarms, Logs, Maps, and Wireless IDS Alerts. The main content area displays a table with the following columns: Name, Status, AP Name, Roaming SSID, Segment, and Untrusted VLAN. A search bar is located above the table. Below the table, it indicates 'Showing 0 to 0 of 0 entries' and 'No Data Available in Table'.

Name	Status	AP Name	Roaming SSID	Segment	Untrusted VLAN
No Data Available in Table					

You can also view the status of unified access users by using the **Status** tab. Refer to [Diagnostic Tools on page 267](#) and [Managing Users and Locations on page 252](#) for more information about viewing and managing users.

## 13. Configuring Client Connections

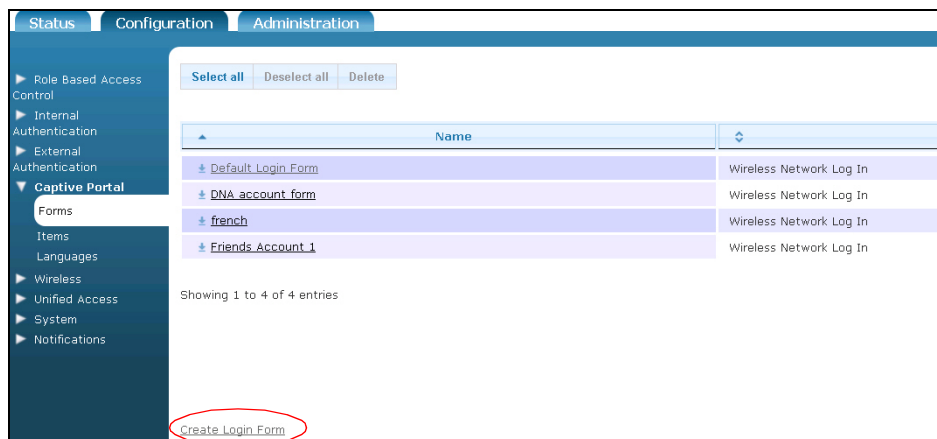
After you have configured the vWLAN platform, the APs, and the wireless and wired connections for vWLAN, you should configure the connections that clients will experience when connecting to vWLAN. Configuring client connections includes configuring the login forms and images displayed when clients connect to the network, specifying guest access parameters, and generating wireless hot spots. These tasks are discussed in the following sections:

- [Customizing vWLAN Login Forms and Images on page 207](#)
- [Configuring Guest Access Parameters on page 227](#)
- [Wireless HotSpot Account Generation on page 231](#)
- [Configuring WPA2-Multikey Client Connections on page 238](#)

### Customizing vWLAN Login Forms and Images

The login screens presented to users of the vWLAN system can be customized based on the authentication methods required on the vWLAN network. You can configure the settings for user and guest logins by creating a login form specific to a user profile, whether that profile is for internal users or guest access. A default login form exists when the vWLAN system is initiated. You can edit the default login form, or create a new one based on the needs of your network. Each login form includes defining to which AP templates the login form applies, which login type (email authentication, user name/password authentication) is presented, the terms of service for the user, specific login settings, captive portal settings, and the design of the login menu. Login forms are created and edited by the administrator for the specific domain.

To create or edit a login form, access the GUI and navigate to the **Configuration** tab, and select **Captive Portal > Forms**. The existing login forms are listed, and you can edit an existing login form by selecting the form from the list, or you can create a new form by selecting **Create Login Form** at the bottom of the menu, or by selecting **Domain Login Form** from the **Create** drop-down menu.

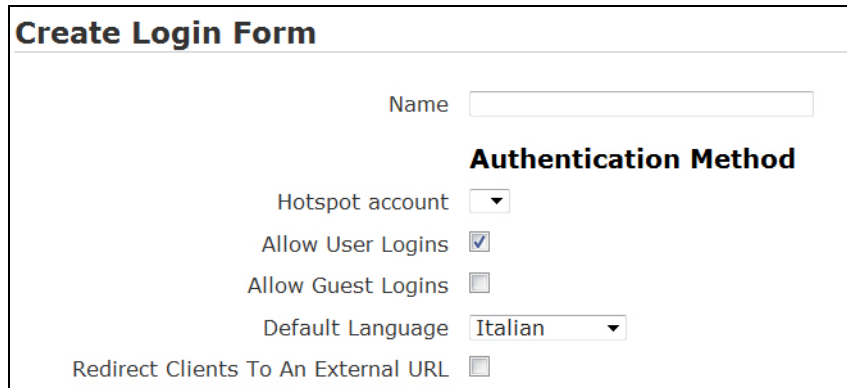


The following sections detail the configuration of a customized login form.

## Basic Login Form Configuration

To edit or create a new login form, select the appropriate login form from the list or select **Create Login Form** at the bottom of the menu, or select **Domain Login Form** from the **Create** drop-down menu. The first basic steps of configuring the login form include naming the login form, associating it with SSIDs, and specifying the AP templates that will use the login menu. To begin configuring or editing a login form, follow these steps:

1. Enter the name of the login form in the appropriate field. Associate a hotspot account with the login form by selecting an account from the **Hotspot account** drop-down menu (refer to [Wireless HotSpot Account Generation on page 231](#) for more information).



The screenshot shows a configuration window titled "Create Login Form". It contains the following fields and options:

- Name**: A text input field.
- Authentication Method**: A section header.
- Hotspot account**: A dropdown menu.
- Allow User Logins**: A checked checkbox.
- Allow Guest Logins**: An unchecked checkbox.
- Default Language**: A dropdown menu with "Italian" selected.
- Redirect Clients To An External URL**: An unchecked checkbox.

2. After configuring the basics of the login form, you will specify the type of user access and authentication the login form will use.

## Configuring Authentication using User Name and Password

You can configure the login form to allow users to access the Internet through vWLAN by using a user name and password. This method of access authentication allows users or guests to authenticate to the network by using an assigned user name and password (refer to [Configuring Domain Users on page 136](#) for more information about configuring the user's user name and password). This method is typically used for registered users, and can be displayed on the login menu simultaneously with the guest access menu or independently, depending on the needs of your network. You can create as many separate login forms for different types of users and roles as you need.

To configure authentication using a user name and password, follow these steps:

1. To specify that access authentication occurs through a user name and password, in the **Create Login Form** menu check the box next to the **Allow User Logins**. Selecting this option indicates that the login menu for vWLAN Internet access for connecting clients requires a user name and password



before logging into the system. This option is typically used for configured users' access, and can be used independently or in conjunction with email authentication (typically used for guest users).

**Authentication Method**

Hotspot account

**Allow User Logins**

Allow Guest Logins

Default Language

Redirect Clients To An External URL

2. Unlike with guest user access, you do not have to specify a role associated with the user name and password authentication because the user will already be associated with a configured role.
3. Enabling **Allow user logins** specifies that local users can access the Internet from the secure vWLAN login menu by entering a user name and password. Users see the following on the login menu:

**Registered Users**

User Name

Password

Log In

## Configuring User Login Authentication Using an Email Address

You can also configure the login form to allow users to access the Internet through vWLAN by using an email address.



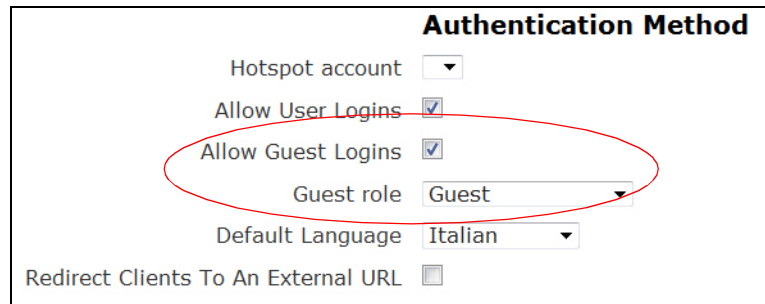
### NOTE

*The validity of an email address is not verified by the system. A user can enter any email address and it will be accepted. **a@b.c** is as valid an email as **adam@adtran.com**.*

To configure the user login authentication using an email address, follow these steps:

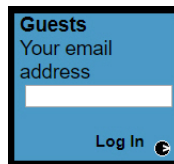
1. To specify that access authentication occurs through an email address, check the box next to **Allow Guest Logins**. Selecting this option indicates that the login page for vWLAN Internet access for connecting clients requires an email address before logging into the system. This option is typically

used for guest access, and can be used independently or in conjunction with user name and password authentication (typically used for registered users).



- In addition to indicating that guest logins are allowed, also specify the role that connected guests will have by selecting the appropriate option from the **Guest role** drop-down menu.

Enabling this option specifies that guest users can access the Internet from the secure vWLAN login menu by entering an email address. Users see the following on the login menu:

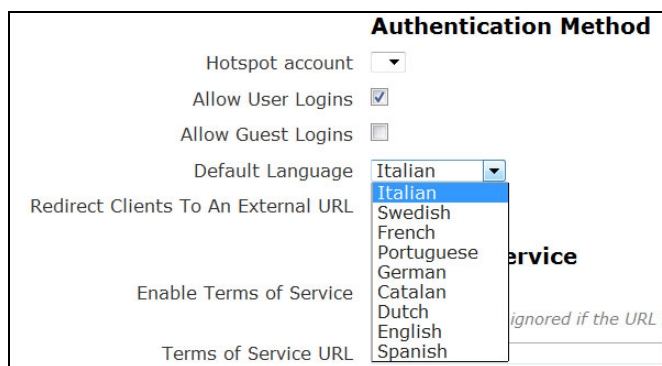


### Specifying the Login Form Language

You can optionally choose to specify a language other than English for the login form. Language selections include **Catalan, Dutch, English, French, German, Italian, Portuguese, Spanish, and Swedish** by default, or you can choose any other language configured on the vWLAN system (refer to [Customizing the Login Language on page 221](#)).

To specify the language used on the login form, follow these steps:

- Select the appropriate language from the **Default Language** drop-down menu.



- The selected language will be used on the user-facing login form.

## Configuring External Redirects

Some applications require using an external or third-party captive portal server. To configure external redirects, you must specify that clients are redirected to an external URL, provide the URL, and optionally specify the information that is passed to the external server. If you enable external redirects, you do not have to configure the additional parameters of the login form.

To configure external redirects, follow these steps:

1. Enable external redirection by selecting the **Redirect** check box. Then, provide the URL of the external server to which clients are being redirected.

Redirect Clients To An External URL

### Redirection To An External Captive Portal Server

Base URL of External Server

*Please ensure that the external server is reachable from the access points.  
The external server must notify vWLAN when login succeeds using an URL of the form:  
`https://VWLAN_IP/login.pl?which_form=reg&source=CLIENT_IP&macaddr=CLIENT_MAC  
&domain_id=DOMAIN_ID&login_form_id=LOGIN_FORM_ID&bs_name=NAME&bs_password=PASSWORD.`*

*For each of the following items, enter a string for the URI parameter if you wish it to be passed to the external server. Note that the first three items are required.*

vWLAN Domain ID	<input type="text" value="domain_id"/>
vWLAN Login Form ID	<input type="text" value="login_form_id"/>
Client's MAC Address	<input type="text" value="mac"/>
Client's Access Point MAC Address	<input type="text" value="ap"/>
Client's Access Point Name	<input type="text" value="ap_name"/>
vWLAN IP Address	<input type="text" value="controller"/>
Client's Original URL	<input type="text" value="destination"/>
Client's IP Address	<input type="text" value="source"/>
Client's Access Point SSID	<input type="text" value="ssid"/>
Client's VLAN ID	<input type="text" value="vlan"/>
AP Status	<input type="text"/>

Double Encoding of URI Parameters

Include RADIUS Option Vendor option



### NOTE

*You must ensure that the external server can be accessed from the AP and vWLAN. The external server must notify vWLAN when a client's login succeeds using a URL of the form: **`https://VWLAN_IP/login.pl?which_form=reg&source=CLIENT_IP&macaddr=CLIENT_MAC&domain_id=DOMAIN_ID&login_form_id=LOGIN_FORM_ID&bs_name=NAME&bs_password=PASSWORD.`***

2. Next, optionally specify whether vWLAN and its client information is passed to the external server. To specify that this information is passed along, enter a string for the uniform resource identifier (URI) parameter in the appropriate fields. You can specify that the client's AP MAC address, the client's AP name, the vWLAN IP address, the client's original URL, the client's MAC address, the client's IP address, the client's AP SSID, the client's VLAN ID, and the AP's status ID, are passed to the

external server by entering the information in the appropriate fields. In the example below, the fields are filled with the default values.

### Redirection To An External Captive Portal Server

Base URL of External Server

*Please ensure that the external server is reachable from the access points.  
The external server must notify vWLAN when login succeeds using an URL of the form:  
https://vWLAN\_IP/login.pl?which\_form=reg&source=CLIENT\_IP&macaddr=CLIENT\_MAC  
&domain\_id=DOMAIN\_ID&login\_form\_id=LOGIN\_FORM\_ID&bs\_name=NAME&bs\_password=PASSWORD.*

*For each of the following items, enter a string for the URI parameter if you wish it to be passed to the external server. Note that the first three items are required.*

vWLAN Domain ID	<input type="text" value="domain_id"/>
vWLAN Login Form ID	<input type="text" value="login_form_id"/>
Client's MAC Address	<input type="text" value="mac"/>
Client's Access Point MAC Address	<input type="text" value="ap"/>
Client's Access Point Name	<input type="text" value="ap_name"/>
vWLAN IP Address	<input type="text" value="controller"/>
Client's Original URL	<input type="text" value="destination"/>
Client's IP Address	<input type="text" value="source"/>
Client's Access Point SSID	<input type="text" value="ssid"/>
Client's VLAN ID	<input type="text" value="vlan"/>
AP Status	<input type="text"/>

Double Encoding of URI Parameters

Include RADIUS Option Vendor option

- Optionally, specify whether uniform resource identifier (URI) parameters are double encoded when sent to the external server. By default, this option is enabled. To disable it, deselect the **Double Encoding of URI Parameters** check box.

vWLAN Domain ID	<input type="text" value="domain_id"/>
vWLAN Login Form ID	<input type="text" value="login_form_id"/>
Client's MAC Address	<input type="text" value="mac"/>
Client's Access Point MAC Address	<input type="text" value="ap"/>
Client's Access Point Name	<input type="text" value="ap_name"/>
vWLAN IP Address	<input type="text" value="controller"/>
Client's Original URL	<input type="text" value="destination"/>
Client's IP Address	<input type="text" value="source"/>
Client's Access Point SSID	<input type="text" value="ssid"/>
Client's VLAN ID	<input type="text" value="vlan"/>
AP Status	<input type="text"/>

Double Encoding of URI Parameters

Include RADIUS Option Vendor option

- Optionally, specify whether a RADIUS option is sent to the external server on behalf of the connecting client. This option allows the RADIUS server to place the connecting client in a user role.

By default, this option is disabled. To enable it, select the **Include RADIUS Option Vendor option** check box.

vWLAN Domain ID	<input type="text" value="domain_id"/>
vWLAN Login Form ID	<input type="text" value="login_form_id"/>
Client's MAC Address	<input type="text" value="mac"/>
Client's Access Point MAC Address	<input type="text" value="ap"/>
Client's Access Point Name	<input type="text" value="ap_name"/>
vWLAN IP Address	<input type="text" value="controller"/>
Client's Original URL	<input type="text" value="destination"/>
Client's IP Address	<input type="text" value="source"/>
Client's Access Point SSID	<input type="text" value="ssid"/>
Client's VLAN ID	<input type="text" value="vlan"/>
AP Status	<input type="text"/>
Double Encoding of URI Parameters	<input checked="" type="checkbox"/>
Include RADIUS Option Vendor option	<input checked="" type="checkbox"/>
<input type="button" value="Create Login Form"/>	

After configuring the external redirect settings, you have completed the login form configuration. Select **Create Login Form** to create the form. A confirmation page is displayed to indicate the successful creation of the login form.

## Configuring the User Service Agreement

After configuring the type of user or guest login authentication used on this login form, if you are not using external redirection, you can specify the terms of service viewed by the user upon login. You can specify that no terms of service are displayed, or if there are terms of service displayed, that they are specific terms of service.



### NOTE

*If you have selected to redirect clients to an external URL, these menu options may not be available.*

To configure the terms of service for a login form, follow these steps:

1. In the **Create Login Form** menu, select the check box next to **Enable Terms of Service**. By selecting the check box you are specifying that terms of service are available for the user to view. Users view the terms of service by selecting them on the secure vWLAN login menu.

<b>Terms of Service</b>	
Enable Terms of Service	<input checked="" type="checkbox"/>
<small>This checkbox is ignored if the URL below is the default (invalid) one.</small>	
Terms of Service URL	<input type="text"/>
<small>Change to a valid URL (and allow the URL in the Unregistered role) to allow the user to click and see the Terms of Service.</small>	

2. Specify the URL for the terms of service. This is the URL to which the user is directed when they select the terms of service on the secure vWLAN login menu. In order for clients to be able to reach

this URL before authentication, the un-registered role must allow HTTP or HTTPS to this destination host name. You should create a destination host name and associate it to the firewall policy (refer to [Configuring Domain Roles on page 96](#)).

**Terms of Service**

Enable Terms of Service

*This checkbox is ignored if the URL below is the default (invalid) one.*

Terms of Service URL

*Change to a valid URL (and allow the URL in the Unregistered role) to allow the user to click and see the Terms of Service.*

After configuring the terms of service parameters for this login form, you can specify the login attempt settings for the form.

### Specifying the Login Attempts Parameters

After you have configured the basic settings, AP templates, access authentication parameters, and the terms of service settings, you can configure the login attempts settings for the login form. These settings include the maximum number of login attempts a user is allowed, and the delay (in minutes) before allowing a user to attempt to login again after the maximum number of login attempts has been reached.

**i** **NOTE**

---

*If you have selected to redirect clients to an external URL, these menu options may not be available.*

To specify the login attempts parameters, follow these steps:

1. From the **Create Login Form** menu, specify the maximum number of login attempts allowed for users on this login form by entering the number in the appropriate field. Entering **0** indicates there is no maximum number.

**Login Attempts**

Maximum Login Attempts

*Enter '0' for no max.*

Minutes To Delay After Maximum Failed Login Attempts

2. Next, specify the delay (in minutes) before a user can attempt to login again after the maximum number of failed login attempts has been reached. Enter the value in the appropriate field.

**Login Attempts**

Maximum Login Attempts

*Enter '0' for no max.*

Minutes To Delay After Maximum Failed Login Attempts

After configuring the login attempt settings, you can configure the visual elements of the login form.

## Configuring the Visual Elements of the Login Form

There are several ways you can customize the visual elements of the login form displayed by vWLAN. You can specify the background, foreground, and links color, the logos used on the page, which login form is on top, the font size used, the color of the login forms, the spacing around any logos on the page, the HTML spacing on the page, and also customize the HTML on the login or thank you menus.



### NOTE

*If you have selected to redirect clients to an external URL, these menu options may not be available.*

To customize the visual elements of the login form, follow these steps:

1. In the **Create Login Form** menu, specify a webpage title for the login menu in the **Web Page Title** field. Then, select the background, foreground, link, visited link, and active link colors for the menu. You can enter a web-based color code, or you can select a color from the swatches next to the appropriate fields.

The screenshot shows a configuration window titled "HTML Body" with the following fields and values:

Field	Value
Web Page Title	Wireless Network Log In
Background Color	ffffff
Foreground Color	333333
Link Color	3366cc
Visited Link Color	666666
Active Link Color	ffcc00

2. Next, specify the logo displayed on the login page. By default, an ADTRAN Bluesocket logo is displayed on the bottom left corner of the page. You can select the logo image from the **Top Left Login Image** and **Powered-By Logo** drop-down menus. If you have uploaded your own logo image to vWLAN, you can select it here (refer to [Uploading Images and Multimedia for Login Forms on page 220](#) for more information about uploading your own logo image). Optionally, you can specify whether internal users can change their passwords when connecting to vWLAN. By default, this option is enabled. To disable it, deselect the **Enable Change Password Button** check box. This option is displayed on the login form presented to the connecting user, and is available to clients

using internal authentication only. You can also specify that the Bluesocket logo is not displayed on the login page by selecting the **Enable Complete Customization** check box.

**Logos**

Top Left Login Image

Powered-By Logo

Enable Change Password Button  *Applies to internal authentication only.*

Enable Complete Customization

**i** **NOTE**

*If you select **Enable Complete Customization**, the entire page must be specified by the administrator. In addition, the Terms of Service check box must be deselected.*

- Specify which login form appears on top by selecting either **Guests** or **Users** from the **Top Login Form** drop-down menu. This option specifies which login appears first on the page. Then, select the font size for the page from the **Font Size** drop-down menu. You can select **Small**, **Medium**, or **Large**.

**Login Form**

Top Login Form

Font Size

- Specify the colors for the login fields (user and guest) and the date displayed on the login menu by entering a web-based color code or selecting a color from the swatches in the appropriate fields.

**Form Colors**

Form Background	<input type="text" value="000000"/>	
Users Background	<input type="text" value="6699cc"/>	
Users Foreground	<input type="text" value="000000"/>	
Guests Background	<input type="text" value="ffcc00"/>	
Guests Foreground	<input type="text" value="000000"/>	
Links Background	<input type="text" value="336699"/>	
Links Foreground	<input type="text" value="000000"/>	



5. Specify the spacing and location on the login menu of the logos, the login fields, and any customized HTML by entering the pixel values in the appropriate field. Also specify the total width allocated for the HTML (you can enter \* to display the HTML at the maximum width).

Spacing	
Pixels Above The Top Left Logo	<input type="text" value="18"/>
Pixels To The Left And Right of The Form Boxes	<input type="text" value="5"/>
Display Middle Line Between The Two Sides	<input checked="" type="checkbox"/>
Pixels Between The Form And The Customized HTML	<input type="text" value="40"/>
Pixels Between The Top And The Customized HTML	<input type="text" value="60"/>
Total Width Allocated For The HTML	<input type="text" value="*"/>

*Enter "\*" for max width.*

6. Specify any customized HTML that will appear on the right of the login menu in the appropriate field. You can add your own text, images, or multimedia files to the HTML displayed on the login menu by uploading files as described in [Uploading Images and Multimedia for Login Forms on page 220](#). Enter the file in the HTML table cell.



#### NOTE

*Uploaded images must have a source (SRC) relative to **local**. For example, ``. The domain ID must be included in the folder path (domain ID of 5 in the previous example). You can find the path for a specific image or preview the image by navigating to the **Configuration** tab and selecting **Authentication > Captive Portal > Items**.*

HTML	
Right Side Customization HTML	<div style="border: 1px solid gray; height: 100px;"></div>

Any images or multimedia can be uploaded in the "Captive Portal->Items->Create Login Item" section. This code will be placed inside an HTML table cell. Uploaded images must have a SRC relative to "local/domain\_id", i.e., ``. The SRC of an uploaded image can be found under the "item\_path" column in the "Captive Portal->Items" page.

To create custom HTML menus, use special HTML attributes to add the vWLAN specific forms and elements. For example, specify `<!--USERS-->` to create a user's login menu, specify `<!--GUESTS-->` to place a guest email login menu, and specify `<!--ADVANCED-->` to place a new account box. To fully customize the user's login form, you must create HTML that includes the `bs_name` and `bs_password` attributes, and then enter this custom code in the **Right Side Customization HTML** field.

In addition, the following apply when creating fully customized login pages:

- <!--HOSTNAME-->
- <!--ADVANCED-->
- <!--USERS-->
- <!--GUESTS-->
- <!--LINKS-->
- <!--LANGUAGE-->
- <!--REMOTEADDR-->

The following outlines the meaning of each HTML attribute:

- **HOSTNAME** specifies the vWLAN Hostname/URL
- **ADVANCED** creates a New Account box
- **USERS** creates a User Login Box
- **GUESTS** creates a Guest Login Box
- **LINKS** provides certificate download links
- **LANGUAGE** provides language change links
- **REMOTEADDR** specifies the client's IP address without NAT



#### NOTE

*In vWLAN release 2.5.1, additional HTML attributes were added. The differences between 2.5.0 HTML and 2.5.1 HTML are outlined in the configuration guide [Fully Customized Login page Configuration Differences in vWLAN 2.5.0 and 2.5.1](https://supportcommunity.adtran.com), available online at <https://supportcommunity.adtran.com>. The following examples are HTML for vWLAN 2.5.1 and later.*

For example, to create a single-click ToS page, enter the following:

```
<p align=center>
<BR>
<h1 align=center>Internet Use Policy</h1></p>
<div style="width: 600px;height: 300px;overflow: scroll;overflow-x: hidden;
border: 3px double #848484;outline:0;margin:0 auto;">
<p align=left> ***Insert EULA from customer here*** </p> </div>
<form method="POST" action="/login.pl" enctype="application/x-www-form-
urlencoded" name="custom_login" class="nospace">
  <p align="center">
    <input type="hidden" name="_FORM_SUBMIT" value="1" />
    <input type="hidden" name="which_form" value="reg" />
    <input type="hidden" name="bs_name" value="GUEST"/>
    <input type="hidden" name="bs_password" value="GUEST"/>
    <input type="hidden" name="destination" value="" />
    <input type="hidden" name="source" value="" />
    <input type="hidden" name="error" value="" />
    <input type="hidden" name="domain_id" value="" />
    <input type="hidden" name="login_form_id" value="" />
    <input type="hidden" name="macaddr" value="" />
  </p>
  <p align="center">
    <input type="SUBMIT" border="0" value="I Acknowledge Terms & Conditions"
```

```

    class="btn"/>
  </p>
</form>

```

To create a guest-only page, enter the following:

```

<p align=center> <BR>
<h1 align=center>Internet Use Policy</h1></p>
<div style="width: 600px;height: 300px;overflow: scroll;overflow-x: hidden;
  border: 3px double #848484;outline:0;margin:0 auto;">
<p align=left>
***Insert EULA from customer here***
</p> </div>
<form method="POST" action="/login.pl" enctype="application/x-www-form-
  urlencoded" name="custom_login" class="nospace">
  <p align="center">
    <input type="hidden" name="_FORM_SUBMIT" value="1" />
    <input type="hidden" name="which_form" value="guest" />
    <input type="hidden" name="destination" value="" />
    <input type="hidden" name="source" value="" />
    <input type="hidden" name="error" value="" />
    <input type="hidden" name="domain_id" value="" />
    <input type="hidden" name="login_form_id" value="" />
    <input type="hidden" name="macaddr" value="" />
  </p>
  <p align="center">
    Email: <input type="text" name="bs_email" id="l_bs_email" value=""
  size="26" /><br /><br />
    <input type="SUBMIT" border="0" value="I Acknowledge Terms & Conditions"
  class="btn"/>
  </p>
</form>

```

To create a user name and password login menu, enter the following:

```

<p align=center>
<BR>
<h1 align=center>Internet Use Policy</h1></p>
<div style="width: 600px;height: 300px;overflow: scroll;overflow-x: hidden;
  border: 3px double #848484;outline:0;margin:0 auto;">
<p align=left>
***Insert EULA from customer here***
</p>
</div>
<form method="POST" action="/login.pl" enctype="application/x-www-form-
  urlencoded" name="custom_login" class="nospace">
  <p align="center">
    <input type="hidden" name="_FORM_SUBMIT" value="1" />
    <input type="hidden" name="which_form" value="reg" />

```

```



```

7. Lastly, specify a customized thank you page by entering the HTML you want to use in the **Thank-you Customization HTML** field. This option specifies the thank you text displayed for the client after login. When fully customizing the thank you page, you can enter **<!--ADVANCED-->** somewhere in your HTML code to customize where the code is displayed.

After you have configured all the customization options for the login form, select **Create Login Form** to create the custom form.

## Uploading Images and Multimedia for Login Forms

You can optionally upload any of your own images, logos, or multimedia files for use with the vWLAN login form.



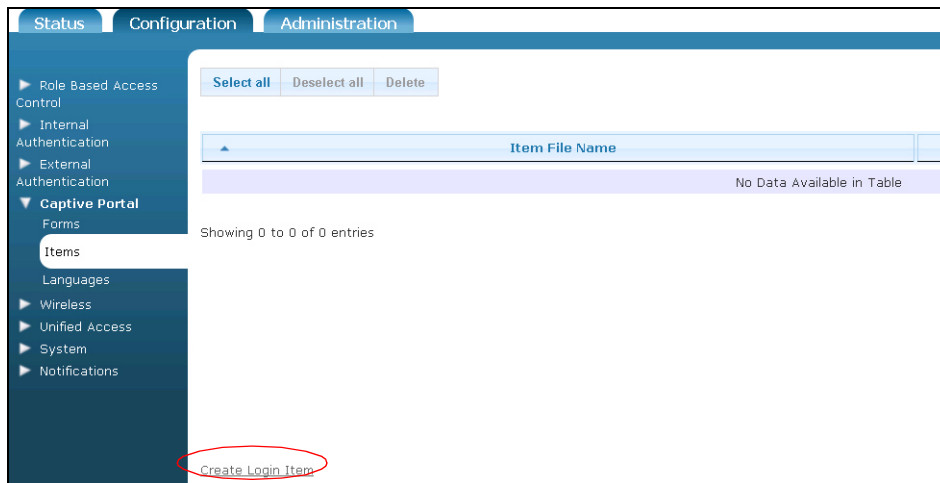
### NOTE

*Each domain has a specific amount of storage space for these files. Refer to [Managing Domain Storage Settings on page 255](#) for more information about the storage settings.*

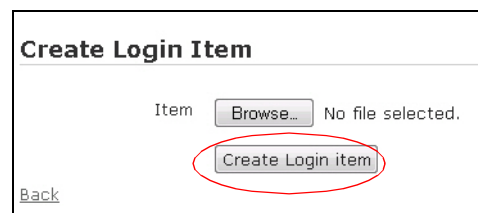
To upload these files, follow these steps:

1. Access the GUI and navigate to the **Configuration** tab, and select **Captive Portal > Items**. In the initial menu, any previously uploaded files are displayed in a list.

- To add a new image, select **Create Login Item** at the bottom of the menu, or select **Domain Login Item** from the **Create** drop-down menu.



- Use the **Browse** button to select an image from your location, and select **Create Login item**. The file is now available for you to select when creating a login form.

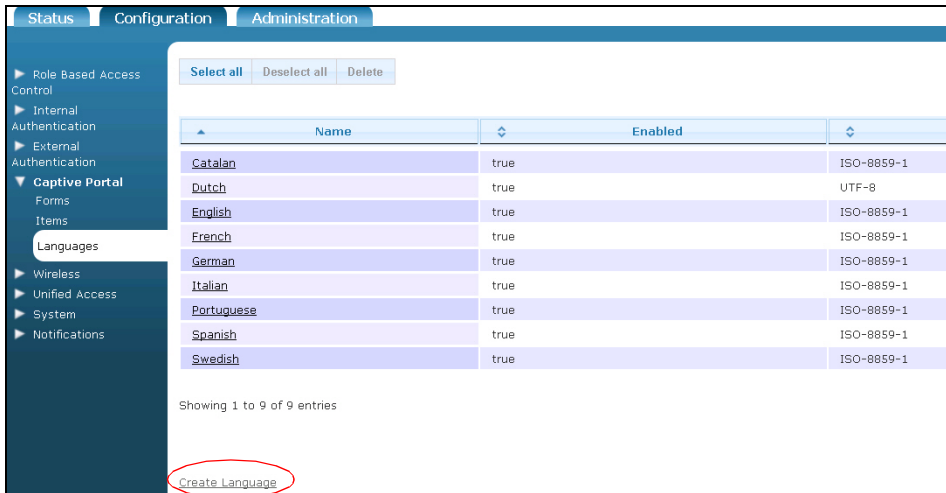


## Customizing the Login Language

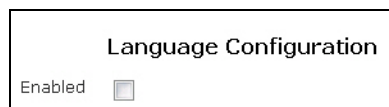
You can choose to customize the login languages available on vWLAN, if necessary. By default, vWLAN includes **English, Spanish, French, Italian, Swedish, Portuguese, German, Catalan, and Dutch**. To add a new language, follow these steps:

- Navigate to the **Configuration** tab, and select **Captive Portal > Languages**. Here the included list of languages for vWLAN is displayed. You can choose to edit or delete an existing language by selecting the appropriate language from the list. To add a new language to vWLAN, select **Create**

**Language** at the bottom of the menu, or select **Domain Language** from the **Create** drop-down menu.



2. Enable the language choice by selecting the **Enabled** check box.



3. Specify the language details by entering the language information in the appropriate fields. This information includes the language name, language code, character set, and the native language name.

The image shows a form titled 'Language Details' with four input fields:

- Name:
- Language Code:
- Character Set:
- Native Name:

- 4. Specify the translations for the login page prompts seen by registered users. You will need to enter translations for the page title, authentication server, user name, password, new password, reentering the new password, registered language selection, login button, and terms of service prompts.

Registered Users Translations	
Title	<input type="text"/>
Authentication Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
New Password	<input type="text"/>
New Password Confirmation	<input type="text"/>
Registered Language	<input type="text"/>
Login Button	<input type="text"/>
Terms of Service	<input type="text" value="I accept terms of service."/>

- 5. Specify the translations for the login page prompts seen by guest users. You will need to enter translations for the page title, email address, and login button prompts.

Guest Users Translations	
Title	<input type="text"/>
Email Address	<input type="text"/>
Login Button	<input type="text"/>

- 6. Specify the translations for the thank you menu. This is the page viewed by users, whether guest or registered, once they have logged in.

Post-Registration Translations	
Thank You Page	<input type="text"/>

- 7. Specify the translations for the links displayed to connected clients. You will need to enter translations for the change password, change language, hotspot account generation, login personal, install CA certificate, software download, localization, and help links.

Link Translations	
Change Password	<input type="text"/>
Change Language	<input type="text"/>
Hotspot Account Generation	<input type="text"/>
Login Personal	<input type="text"/>
Install CA Certificate	<input type="text"/>
Software Download	<input type="text"/>
Localization	<input type="text"/>
Help	<input type="text"/>

- Specify the translations for hotspot pages. You will need to enter translations for the sign up form, hours, days, weeks, months, proceed, checkout, cancel, sponsor name, and sponsor password fields.

Hotspot Sign-Up	
Signup For	<input type="text"/>
Hours	<input type="text"/>
Days	<input type="text"/>
Weeks	<input type="text"/>
Months	<input type="text"/>
Proceed Button	<input type="text"/>
Checkout Button	<input type="text"/>
Checkout Button	<input type="text"/>
Sponsor Name (Friends/Family)	<input type="text"/>
Sponsor Password (Friends/Family)	<input type="text"/>

- Specify the translation for hotspot confirmation. You will need to enter translations for the name, email, and description fields. In addition, enter any notes about the language configuration.

Hotspot Sign-Up Confirmation	
Name	<input type="text"/>
Email	<input type="text"/>
Description	<input type="text"/>

- Specify the translation for any thank you information.

Thank You Texts	
Thank You Text	Thank you. You are now a guest on the system.



## 11. Specify the translation for the various warnings and notices on the vWLAN system.

Warnings and Notices	
Check Terms of Service Reminder	Please accept the terms of service.
Redirect Text	You will be redirected after the registration process completes.
Create Account Failure Warning	Failed to create account.
Processing Error Warning	An error occurred processing your request.
Guest Login Disabled Warning	Guest logins are not allowed.
Already Log In Reminder	You are already logged in.
User Login Disabled Warning	User logins are not allowed.
Enter Password Reminder	Please enter a password.
Login Attempts Exceed Limit Warning	You have attempted the maximum number of login attempts. Please wait <i>%(minutes)</i> minute(s) to try again. <i>'%(minutes)'</i> will be replaced by the number of minutes.
Enter Value Reminder	Please enter a value.
Enter Username Reminder	Please enter a username.
Enter Email Reminder	Please enter an email address.
Enter Valid Email Reminder	Please enter a valid email address.
Login Failure Warning	The system could not log you in. Please close all browsers, reopen a browser, and attempt to log in again.
Embedded Symbol Disabled Warning	Embedded symbol(s) are not allowed.
Embedded White Space Disabled Warning	Embedded white space(s) are not allowed.
Embedded Symbol and White Space Disabled Warning	Embedded white space(s) and symbol(s) are not allowed.
Username Already Used Reminder	This username already logged in from another computer, only <i>%(num_of_logins)</i> login(s) per user allowed. <i>'%(num_of_logins)'</i> will be replaced by the number of simultaneous logins allowed.
Invalid Card Warning	Invalid card number.
Invalid Pin Warning	Invalid PIN.
Invalid Card or Pin Warning	Invalid card number or PIN.
SIP2 Connect Failure Warning	Cannot connect to SIP2 Server.
Server Type Invalid Warning	Invalid external server type.
Account Disable Reminder	This account has been disabled.
Maximum Logins Exceeded Warning	Maximum logins exceeded.
ID or Password Invalid Reminder	Incorrect user ID or password.
Name or Password Invalid Reminder	Invalid name or password.
<input type="button" value="Create Language"/>	

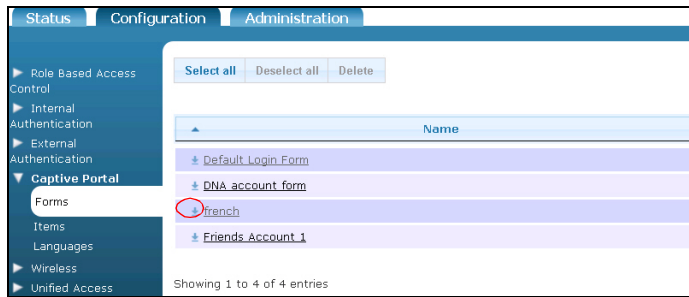
12. After entering all the translation information, create the language by selecting **Create Language** button at the bottom of the menu.

13. You will receive confirmation that the language has been successfully created, and the language will now appear in the language list (**Configuration** tab, **Captive Portal** > **Languages**). The language will also now be available to add to a customized login form.

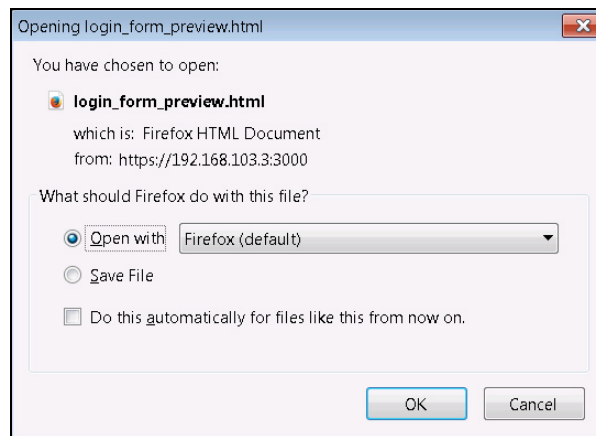
## Viewing Customized Login Pages

You can choose to preview your customized login page. These previews are not functional pages, for example, the links do not function, but they can be used to preview the design and layout of the login pages users or guests will see when accessing vWLAN. To view a login page preview, follow these steps:

1. Navigate to the **Configuration** tab and select **Captive Portal > Forms**. Select the download arrow next to the login form you want to view.



2. At the prompt, select **OK** to preview the login form in your browser.



3. Your browser will then display the login form preview. Keep in mind that the links will not function in this preview, and if you are using any special characters, the character settings may default to your browser's settings. Close the browser window when you have finished previewing the login form.



## Configuring Guest Access Parameters

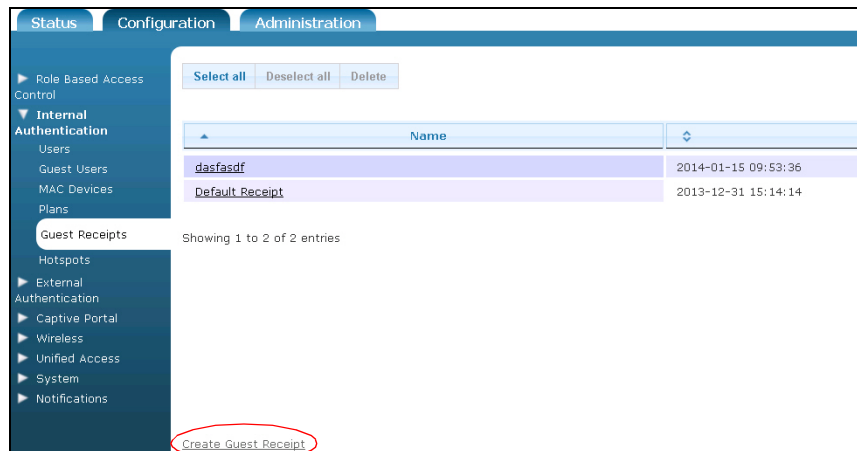
Guest access is configured by the administrator from the GUI. You can configure guest access to vWLAN by creating single or multiple guest user account(s), specifying the user name and password type, and associating the guest user with a connection plan and receipt type. The guest can then access vWLAN by using their assigned user name and password. You can also create specific guest receipts for different guest users, as well as specify the connection plans associated with the users. Each of these guest configuration tasks are described in the following sections.

### Configuring Guest Receipts

Guest receipts are used for guest user accounts to keep track of account user names, passwords, the number of users who can log in simultaneously under the account name, and the account generation, clean up, and expiration times. By default, one guest receipt exists in vWLAN (the **Default Receipt**), and it includes the user name and password for the account. You can edit the existing receipt template, or you can create new templates as necessary.

To create or edit guest receipts, follow these steps:

1. Connect to the GUI, and navigate to the **Configuration** tab and select **Internal Authentication > Guest Receipts**. To edit a receipt, select the appropriate receipt from the list. To create a new guest receipt, select **Create Guest Receipt** at the bottom of the menu, or select **Guest Receipt** from the **Create** drop-down menu.



2. Select a logo and icon image to use in the receipt. Select the **Browse** button to find the images from a specified location. If you do not want to use a logo or icon image, select the **Delete Logo Image** and **Delete Icon Image** check boxes.

**Create Guest Receipt**

Logo Image  No file selected.

Delete Logo Image

Icon Image  No file selected.

Delete Icon Image

3. Next, specify the name for the guest receipt in the **Name** field.

Name	
------	--

4. Specify the header for the receipt. The header is the information displayed at the top of the receipt. For example, the header below welcomes the guest and announces the purpose of the receipt.

Header	Welcome! We are glad you have chosen to stay with us. In this receipt you will find the particulars of your internet account while you are our guest.
--------	---

5. Specify the body of the receipt. The receipt body includes any additional text or instructions you want included in the receipt, as well as any of the following: guest user name, password, number of simultaneous users who can log in under this account, the time the account was created, the time the account will be cleaned up, or the time the account will expire and be deleted. Each option is specified in the characters **{{ }}** as follows:

- For the user name enter **{{name}}**
- For the password enter **{{password}}**
- For the number of simultaneous users enter **{{max\_num\_login}}**. If the value is **0**, the number of users is unlimited.
- For the account creation time enter **{{created\_at}}**
- For the clean up time if the user never logged in, enter **{{cleanup\_time}}**
- For the expiration time after user login, enter **{{expiry\_time}}**

For example, to display the user name associated with the account, you can enter **User Name: {{name}}** and when the receipt is generated, the actual user name is placed in the **{{name}}** field. The following example adds extra instructions and includes the account user name, password, number of simultaneous users allowed, account creation time, and account expiration time.

Body	<p>Your guest account has been created and is now ready to use. To access your account, follow these steps:</p> <ol style="list-style-type: none"> <li>1. Make sure your network adapter is set to "DHCP - Obtain an IP address automatically."</li> <li>2. Open your Web browser and enter your user name and password in the provided fields.</li> </ol> <p style="margin-left: 20px;">User Name: {{name}} Password: {{password}}</p> <p>Make sure to review your account details before use. Contact the front office if you need assistance.</p> <p>Account User Limit: {{max_num_login}} Account Creation Date: {{created_at}} Account Expiration Date: {{expiry_time}}</p> <p style="font-size: small; color: #ccc;">You can use any of the following attributes surrounded by curly braces. e.g. {{name}}, {{password}}, {{created_at}}, {{cleanup_time}}.</p> <p style="text-align: center;"><input type="button" value="Create Guest receipt"/></p>
------	--

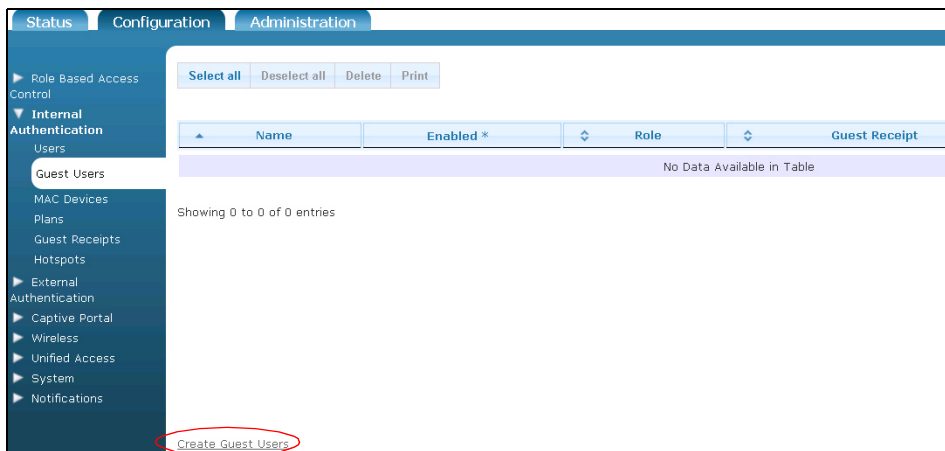
6. After configuring the receipt, select **Create Guest Receipt** to create the receipt. Once created, you will receive confirmation that the receipt has been created and the receipt will now appear in the receipt list (**Configuration** tab, **Internal Authentication** > **Guest Receipt**). You can now associate this receipt with any created guest users.

## Creating Guest User Accounts

Guest user accounts can be created for a single user, or for multiple users, by creating a single guest account. You can create guest access to the vWLAN by configuring multiple guest accounts at once, creating a user name and password for each guest, or by adding guest users to an external RADIUS or LDAP authentication server. Follow the steps below for the first two methods, and refer to [External Server Authentication on page 109](#) for information about creating external authentication servers.

To create a guest account, follow these steps:

1. Access the GUI and navigate to the **Configuration** tab, and select **Internal Authentication > Guest Users**. Select **Create Guest Users** at the bottom of the menu, or select **Domain Guest User(s)** from the **Create** drop-down menu.



### NOTE

*You can also access the guest user account menu by selecting **Create Guest Users** at the bottom of the **Users** menu (**Configuration** tab, **Internal Authentication > Users**). Choosing this option will redirect you to this menu.*

2. Specify the number of users to create. You can create between **1** and **500** users at a time. Enter a value in the **Number of Users** field.
3. Specify the user prefix in the **User Prefix** field. The prefix is used in the automatic generation of user names. By default, the prefix is specified as **user\_**, which generates user names of **user\_1**, **user\_2**, etc.



### NOTE

*If the user name does not end in an underscore (\_), and you are creating a single guest user, no number is appended to the user name. Otherwise, a unique number is always appended to the user name.*

4. Specify the user password generation method by selecting either **Unique Password** or **Default Password**. Unique password lengths can be specified in the **Password Length** field. By default, unique passwords are **8** characters in length, and are automatically generated and assigned. The default password is **password**.
5. Specify the guest receipt type for the user from the **Guest Receipt** drop-down menu. The guest receipt can include the user name, password, number of simultaneous users, creation time, cleanup time, and expiration time of the account. Refer to [Configuring Guest Receipts on page 227](#) for more information about configuring guest receipts.
6. Specify the hotspot connection plan to be used for the account by selecting a plan from the **Hotspot Plan** drop-down menu. Selections include minute, hourly, daily, weekly, and monthly plans, as well as any other plans you have created. Refer to [Hotspot Account Configuration on page 233](#) for more information about configuring connection plans.
7. Specify the account's expiration time (in minutes) using the sliding bar. Specify a time between **1** and **120** minutes.

**NOTE**

*The account expiration values will change depending on the hotspot plan associated with the user account.*

8. Select **Create Guest Users** to create the user account(s).

**Create Guest User(s)**

Number of Users: 1  
Number of users to create (1-500).

User Prefix: user\_  
The automatically generated usernames will start with the prefix. e.g. 'user\_' produces 'user\_1', 'user\_2', ...

Password Generation Method:  Unique Password  
 Default Password  
Choose a password generation method.

Password Length: 8

Guest Receipt: Default Receipt  
Select an existing guest receipt. This will be used to print out user(s) receipt(s).

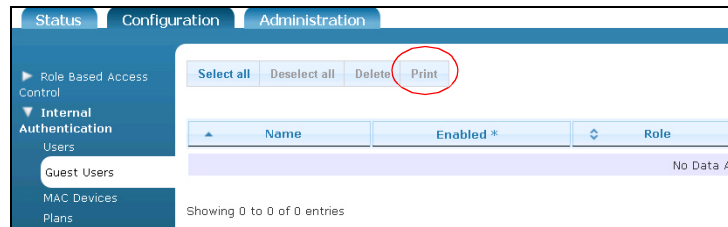
Hotspot Plan: Minute Plan  
Select an existing plan.

Expiry Time: 1  
1 120 Minutes

**Create Guest User(s)**

9. The guest user accounts appear in the **Guest User** menu. You can optionally print a receipt for the guest account from this menu by selecting **Print** at the top of the menu. If popups are allowed in your

browser, a popup window of the receipt is displayed. In addition, you can choose to view, edit, or delete the user accounts from this menu.



#### NOTE

*You can only delete, edit, or view the guest accounts that you yourself have created. This prevents one lobby administrator from accidentally interfering with another.*

## Wireless HotSpot Account Generation

vWLAN allows guest users easy access to the Internet. To avoid manual intervention by a front desk administrator, in a hotel for example, guests can be given the ability to create their own accounts, or to have accounts created by other employees or sponsors who are part of the organization. When configuring wireless hotspot accounts, you will need to specify whether the accounts can be created, over what duration, and how many times the same user can create the account over a certain period. In addition, you will need to specify whether a user can create the account themselves, or if a sponsor is required. You can also determine what credentials are necessary to create hotspot accounts, and whether passwords are chosen by the user, sponsor, or automatically assigned by the vWLAN system and emailed to the user.

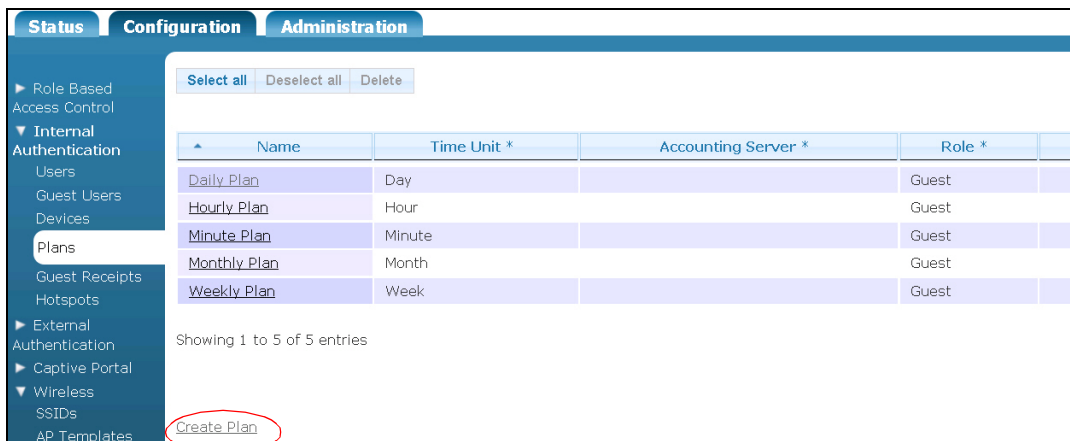
Users that access vWLAN using a hotspot account are given the ability to create the account on the secure vWLAN login menu. If the user must have a sponsor to create the account, the sponsor enters the proper credentials and creates the account for the user. The user then logs in to vWLAN. If the user has the ability to create the account, the system automatically logs the user into vWLAN at the same time the account is created. At the end of the account lifetime, which is either a fixed time period after login, or a fixed time specified by the account sponsor, the user is logged out and the account is deleted (or disabled if the administrator wants to prevent multiple logins).

When creating hotspot accounts, there are two areas that you will need to configure: the hotspot plan and the hotspot account. Overall, the hotspot plan functions as a template, in which the administrator sets the values for a specific type of account, and the hotspot account is the actual account used by a client to connect to the network. The hotspot account will follow the settings specified in the hotspot plan associated with the account. This section outlines both hotspot plan and hotspot account configuration.

### Hotspot Plan Configuration

Hotspot plans determine the access parameters used by a hotspot account. Five hotspot plans are available by default: a daily, hourly, minute, monthly, and weekly plan. These plans are configured to be used by guests on a daily, hourly, minute, monthly, or weekly basis. You have the option to create your own hotspot plan. To create a new plan, or edit an existing plan, follow these steps:

1. Navigate to the **Configuration** tab and select **Internal Authentication > Plans**. To edit an existing plan, select the plan from the list, or to create a new plan, select **Create Plan** at the bottom of the menu.



2. In the **Create Hotspot Plan** menu, enter the name of the plan in the **Name** field, and then select the **Enable The Plan To Be Used By Administrators For Guest Creation** check box if administrators will be able to assign the plan to guests they have created.
3. Next, specify the time unit used by the plan by selecting the appropriate unit from the **Time Unit** drop-down menu. Available selections are minute, hour, day, week, or month. Then specify the minimum and maximum units in the appropriate fields. These integer values depend on the time unit selected; for example, if a day is selected as the time unit, the minimum unit would be one and the maximum would range as high as 31. The minimum unit is set to **1** by default, and the maximum unit is set to **30** by default.
4. Specify the role associated with the hotspot plan by selecting the appropriate option from the **Role** drop-down menu. The available selections include any roles previously configured on the vWLAN system. This role is the role in which users assigned to this plan are placed when connecting to vWLAN.
5. Optionally select an accounting server to be associated with the plan from the **Accounting Server** drop-down menu.
6. Next, specify the login parameters for the account. These include specifying how many simultaneous active sessions are allowed on the plan (**Active Sessions**, set to **1** by default, **0** for unlimited sessions), the number of days before an account is removed due to inactivity (**Cleanup Time**, set to **30** by default), whether unlimited login attempts are allowed (**Unlimited Attempts Allowed**), the number of times a user can log in with the same email address (**Login Attempts**), and the number of days before the login attempts count is reset (**Login Interval**).



7. Once you have entered the hotspot plan specifics, select **Create Hotspot Plan**. Once created, the plan can be used during hotspot account creation.

**Create Hotspot Plan**

Name

Enable The Plan To Be Used By Administrators For Guest Creation

Time unit

Minimum Unit   
In integer format.

Maximum Unit   
In integer format.

Role

Description

Accounting Server

Active Sessions   
Number of simultaneous logins. 0 for unlimited.

Cleanup Time   
Number of days before account is removed if unused.

**Login Attempts details**

Unlimited Attempts Allowed   
Does not apply to Admin created Guests.

Login Attempts   
The number of times a user can log in with the same email address.

Login Interval   
Days before login attempts count is reset.

## Hotspot Account Configuration

Hotspot accounts are the accounts used by guests to access vWLAN. There are three types of hotspot accounts: friends and family, free spot, and DNA accounts. The following outline the different account types:

**Friends and Family:** Friends and family is a hotspot account type that allows an Active-Directory or a RADIUS authenticated user to create a free guest account. This type of account allows users to create their own accounts. The account is generated using email, and a valid email server must be configured for this account type (refer to [Email Account Configuration on page 260](#)). The login credentials are sent to the user, who can then use them to log into vWLAN.

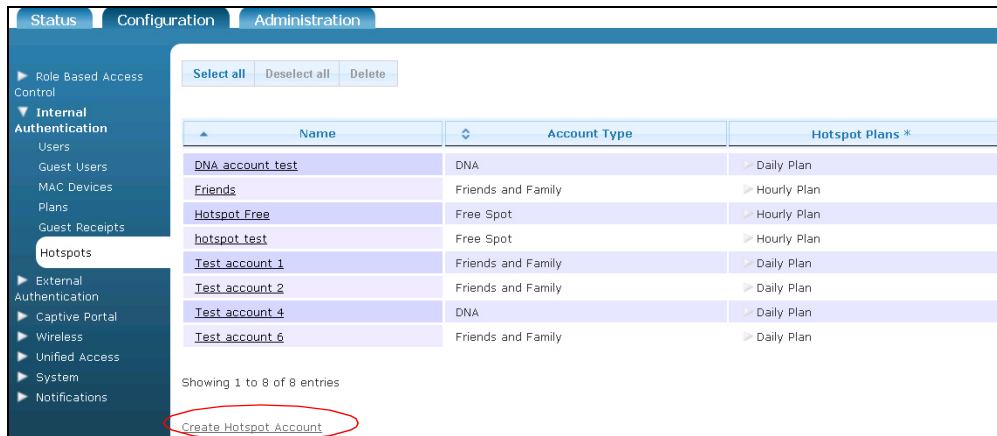
**Free Spot:** Free spot is a hotspot account type that allows users to create their own accounts with either an auto-generated password or a password set by the user. The login credentials are created by the user when they log into vWLAN.

**Guest DNA:** Guest DNA is a hotspot account that allows users to create a guest account and have the password emailed to a confirmed enterprise email account on an iPhone, Blackberry, or PDA. As with a Friends and Family account, a valid email server must be configured for this account type (refer to [Email Account Configuration on page 260](#)). The login credentials are sent to the user, who can then use them to log into vWLAN.

To create a hotspot account, follow these steps:

1. Navigate to the **Configuration** tab, and select **Internal Authentication > Hotspots**. Any previously created hotspot accounts are listed in this menu. You can choose to edit a previously created account by selecting the appropriate account from the list, or you can create a new account by

selecting **Create Hotspot Account** at the bottom of the menu, or selecting **Domain Hotspot Account** from the **Create** drop-down menu (at the top of the menu).

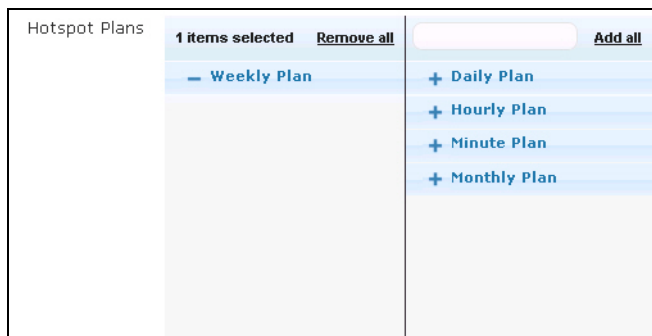


2. Enter the name for the hotspot account in the **Name** field.

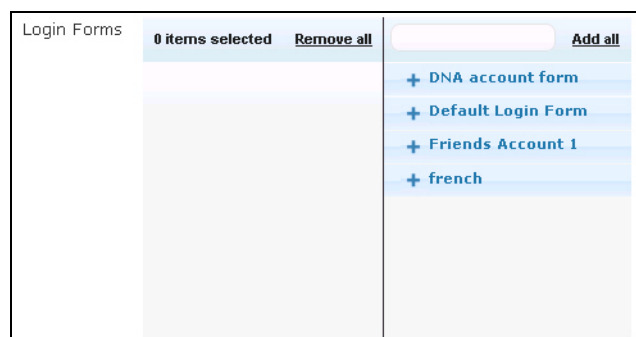
### Create Hotspot Account

Name

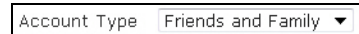
3. Specify any hotspot plans to be associated with this hotspot account by selecting the **+** (plus) sign next to any configured hotspot plans in the list, or selecting **Add All**.



4. Specify the login form to be used by this account by selecting the **+** (plus) sign next to any configured login forms in the list, or selecting **Add All**. Refer to [Customizing vWLAN Login Forms and Images on page 207](#) for more information about configuring login forms.



5. Specify the account type from the **Account type** drop-down menu. You can select **Friends and Family**, **Free Spot**, or **DNA**.



Account Type Friends and Family ▼

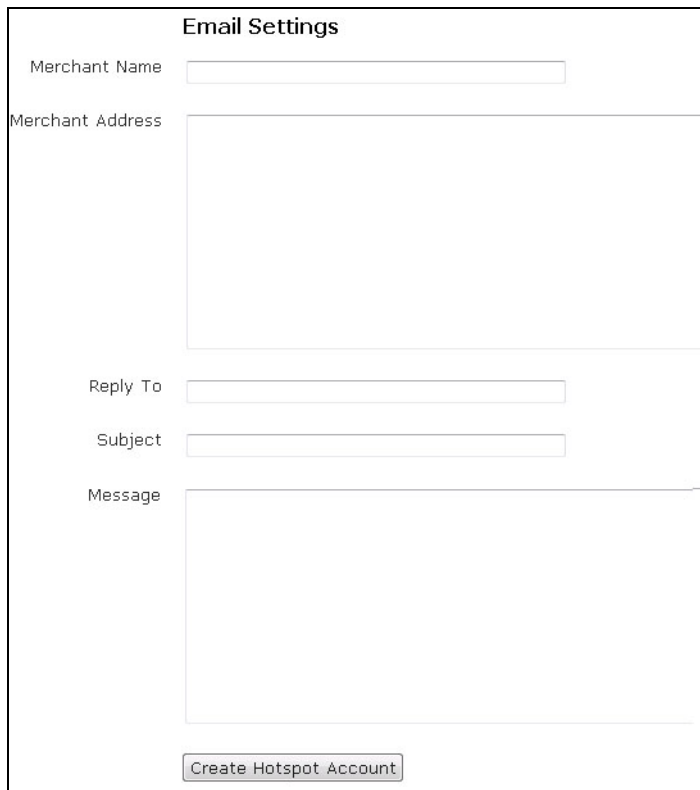
If you choose **Friends and Family** as the account type, you will be prompted to specify the IP address of the email server used to send information about the account and the authentication server used to authenticate the user. The email server can be selected from the **Email Configuration**

drop-down menu, and the authentication server can be selected from the **Auth Server** drop-down menu.



Account Type Friends and Family ▼  
Email Configuration ▼  
Authentication Server New Auth Server web ▼

In addition, for a **Friends and Family** account, you will be prompted to enter the email settings for the account. Specify the **Merchant Name**, **Merchant Address**, **Reply To**, **Subject**, and **Message** information for the email. This email is sent to the client who wants to connect to the vWLAN network, and should contain the login information. After this information is entered, you can select **Create Hotspot Account** to create the account.



**Email Settings**

Merchant Name

Merchant Address

Reply To

Subject

Message

If you choose **Free Spot** as the account type, you will be prompted to enter the IP address of the email server used to send information about the account. Select the IP address of the email server

from the **Email configuration** drop-down menu, and select **Create Hotspot Account** to create the account.



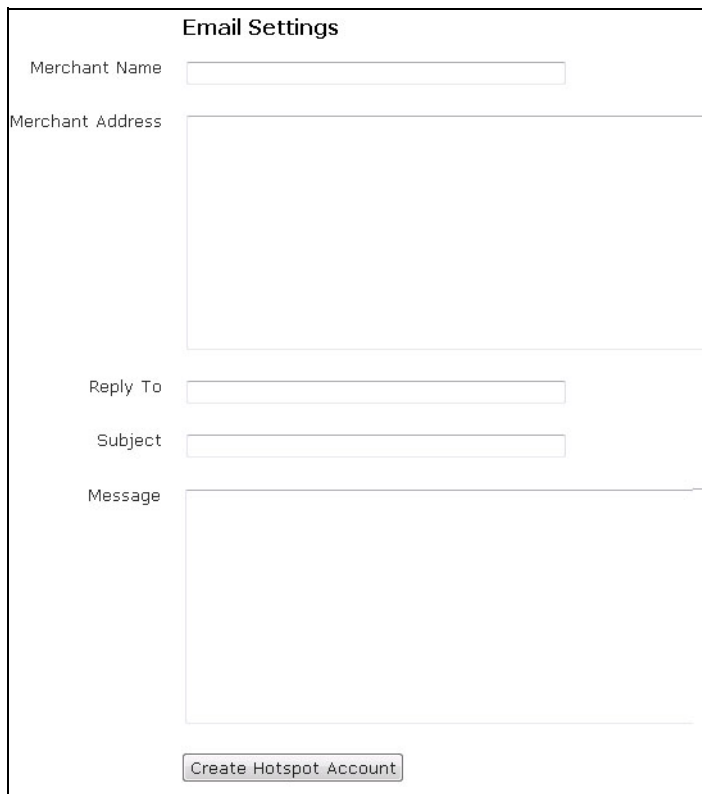
A screenshot of a web form for creating a hotspot account. It features two dropdown menus: 'Account Type' set to 'Free Spot' and 'Email Configuration' which is currently empty. Below these is a button labeled 'Create Hotspot Account'.

If you choose **DNA** as the account type, you will be prompted to specify the IP address of the email server used to send information about the account. The email server can be selected from the **Email configuration** drop-down menu.



A screenshot of a web form for creating a hotspot account. The 'Account Type' dropdown menu is set to 'DNA'. The 'Email Configuration' dropdown menu is currently empty. A 'Create Hotspot Account' button is visible at the bottom.

In addition, for a **DNA** account, you will be prompted to enter the email settings for the account. Specify the **Merchant Name**, **Merchant Address**, **Reply To**, **Subject**, and **Message** information for the email. This email is sent to the client who wants to connect to the vWLAN network, and should contain the login information. After this information is entered, you can select **Create Hotspot Account** to create the account.



A screenshot of the 'Email Settings' form. It contains several input fields: 'Merchant Name' (text), 'Merchant Address' (large text area), 'Reply To' (text), 'Subject' (text), and 'Message' (large text area). A 'Create Hotspot Account' button is located at the bottom of the form.

6. Once you have specified the account type, and any additional parameters, select **Create Hotspot Account** to create the account. You will receive confirmation that the account has been successfully created.

The screenshot shows the 'Create Hotspot Account' configuration page. It features a 'Name' input field, a 'Hotspot Plans' section with '0 items selected' and a list of plans (Daily, Hourly, Minute, Monthly, Weekly) with '+' icons, and a 'Login Forms' section with '1 item selected' and a list of forms (DNA account form, Friends Account 1, french) with '+' icons. At the bottom, there are dropdown menus for 'Account Type' (set to 'Free Spot') and 'Email Configuration' (set to 'adtran'). A red circle highlights the 'Create Hotspot Account' button.

## Friends and Family Account Example Configuration

In this example configuration, a Friends and Family hotspot account is created. This type of hotspot account allows users to create their own accounts for their guests. In this type of account, a registered user associates with the open SSID and is redirected to a splash page. On the splash page, users can select **Create New User** to create a Friends and Family account. This action redirects the user to another page, on which they can enter their user name and password (authenticated by internal user authentication, LDAP, or RADIUS web authentication), select a hotspot plan (minute, daily, weekly, etc.), and enter their guest's email address. Once the account is created, vWLAN emails the user name and password to the guest's email address just entered by the registered user.

To configure the Friends and Family account, complete the following:

1. Edit or create the hotspot plan to be used by this account. You can access hotspot plans by navigating to the **Configuration** tab and selecting **Internal Authentication > Plans**. This plan should be the one you want to be used with the Friends and Family account. Details of plan configuration are included in [Hotspot Plan Configuration on page 231](#).
2. Configure an email account for the hotspot account. Details of email account configuration is detailed in [Email Account Configuration on page 260](#).
3. Configure the Friends and Family hotspot account as described in [Hotspot Account Configuration on page 233](#). Be sure to select **Friends and Family** in the **Account Type** drop-down menu. When you make this selection, additional fields are displayed for you to complete. The **Merchant Name** and **Address** fields are your organization's name and address. The **Reply To** field is the source of the email. The **Subject** field is the subject line of the email, and the **Message** field indicates the body of

the email. Then select the previously configured email server and authentication servers from the appropriate drop-down menus. Select **Create Hotspot Account** when all the fields are complete.

4. Once the account has been created, vWLAN emails the specified email address with a user name and password for wireless access. The email appears as follows:

```
From: v wlan@adtran.com
To: test.user@adtran.com
Subject: Friends and Family Password (Subject)

Welcome to our wireless network! Your username and password can be found below: (Message)
User Name: test.user@adtran.com
Password: 66xk3y

ADTRAN WIRELESS (Merchant Name)
801 Explorer Blvd. (Merchant Address)
Huntsville, AL 35806
```

## Configuring WPA2-Multikey Client Connections

The WPA2-Multikey feature, introduced in vWLAN firmware release 3.5.0, provides a method for clients connecting to the vWLAN network to use a unique Wi-Fi password on a per-user basis, rather than a single password for all connections to the network. This feature is available when the authentication method used for an SSID is WPA2-PSK. When this feature is enabled, clients connecting to the Wi-Fi network for the first time use the default Wi-Fi password that is publicly shared with all users for their initial connection. Once they are connected to the network, a RADIUS server provides attributes that place the user in an a specific VLAN configured for first time network connections. Users are then prompted to create a unique password and are disconnected from the network. The newly created password is stored in the RADIUS server, and when the clients reconnect to the network, their unique password is used to authenticate their connection and they are placed in the VLAN configured for their service type. In this manner, each user connected to the network can be placed in a specific VLAN and their data and traffic rates can be monitored, all based on their specific user password.

The following sections outline the specifics of the WPA2-Multikey feature, its use cases, and its configuration process. For more specific information about the configuration of WPA2-Multikey feature, refer to the configuration guide [WPA2-Multikey and Rolling-PMK in vWLAN](https://supportcommunity.adtran.com), available online at <https://supportcommunity.adtran.com>.

### WPA2-Multikey Use Cases and Authentication Process

The WPA2-Multikey feature, used with WPA2-PSK authentication, is best suited for larger deployments where large numbers of APs are used in an environment where multiple clients are connecting to the APs, such as in an apartment complex or business building. Each AP is configured to broadcast two SSIDs: one for initial connections, and a second for registered users. The first SSID is configured as an open SSID, and is accessed using a shared Wi-Fi password. Once the client has connected to the open SSID, they are redirected to a configured captive portal, where they are requested to register and create a Wi-Fi password unique to them. After registering, the users then connect to a multikey SSID, configured with WPA2-Multikey enabled, and connect to the network. The specific processes for each of these connection types are outlined below.

When new, unregistered users first connect to the network, the following authentication process takes place:

1. The AP is configured with two SSIDs: one with open security, and one with WPA2-Multikey enabled. The SSID with open security is configured with RADIUS Web authentication and MAC authentication enabled, and uses a default role of **VLAN-X** (where **X** is the VLAN ID).
2. The client connects to the open SSID.
3. vWLAN sends a RADIUS ACCESS request, using RADIUS MAC authentication, to the RADIUS server.
4. The RADIUS server responds with an ACCESS-ACCEPT message for all users connecting to the open SSID.
5. Once the RADIUS response is received, vWLAN assigns the default role (VLAN-X) to the client.
6. The client then receives a DHCP address that is used to open a Web browser sending the client to the configured captive portal.
7. From the captive portal, the connecting client is requested to register and create a unique password. This completes the registration process.
8. At this point, the RADIUS server database is updated with the client's MAC address and corresponding password, and the client switches from the open SSID to the SSID with WPA2-Multikey enabled.

When a client that is already registered connects to the network, they connect to the SSID with WPA2-Multikey enabled using their previously configured unique password and the following authentication process takes place:

1. Once the client has connected with their unique password, the AP sends a RADIUS ACCESS request using RADIUS MAC authentication.
2. The RADIUS server responds with a RADIUS ACCESS ACCEPT message that includes the client's password and assigned VLAN ID.
3. The client is then prompted to enter their password.
4. If the client's password matches the information delivered in the RADIUS ACCESS ACCEPT message, the client is authenticated and placed in the specific VLAN configured for them. They then receive a DHCP address for their specific VLAN and can use that address to connect to the Internet. If the client's password does not match the information sent by the RADIUS server, they are disconnected from the network.
5. If the client roams to another AP (for example, in another apartment or business), another RADIUS transaction takes place.

## WPA2-Multikey Configuration Considerations

The following are configuration considerations and interactions with other vWLAN features that should be understood before using the WPA2-Multikey feature:

- When the WPA2-Multikey feature is enabled, the AP discovers new locations whenever new VLAN information is provided by the RADIUS server.
- Layer 3 mobility is not supported for clients connected to an SSID with WPA2-Multikey enabled.
- The client's MAC address and associated password are assumed to be added to the RADIUS server database by the network administrator. In addition, the VLAN configurations are also assumed to be configured and specified by the network administrator, and are not handled automatically by vWLAN.
- When the WPA2-Multikey feature is enabled, the AP performs the RADIUS MAC authentication, rather than vWLAN itself. In addition, the AP allows multiple clients to connect to the SSID using the multikey feature.
- The RADIUS Change of Authorization (CoA) DISCONNECT requests are honored and clients are disconnected when DISCONNECT requests are received.
- The client password information is included in RADIUS ACCEPT messages as the Tunnel-Password attribute, and the associated VLAN ID assigned to the client is included as the Tunnel-Private-Group-ID attribute.
- Multiple PMK keys can be sent by the RADIUS server for connecting clients. Up to **15** different keys can be used to provide client authentication. The authentication process cycles through all provided keys until a match is found and the client is authenticated.

## Configuring the RADIUS Server for the WPA2-Multikey Feature

In order for the WPA2-Multikey feature to function for client connections, some RADIUS server configuration must be completed before completing the WPA2-Multikey configuration in vWLAN. RADIUS server configuration consists of registering clients and users with the server, adding VLAN and PMK information for wireless clients, and triggering client disconnections using CoA Disconnect messages. The RADIUS server configuration that accompanies the WPA2-Multikey feature is in addition to the RADIUS server configuration needed for general vWLAN client authentication (as described in [External RADIUS Web-based Authentication Server on page 113](#)).



### NOTE

*The following configuration assumes you have already configured an external RADIUS server.*

To configure the RADIUS server for the WPA2-Multikey feature, connect to vWLAN and complete the following tasks:

- Configure the external RADIUS server for the vWLAN WPA2-Multikey feature
- Configure an external accounting server for the vWLAN WPA2-Multikey feature



## Configuring the External RADIUS Server for WPA2-Multikey

To use the WPA2-Multikey feature in vWLAN, you must have an external RADIUS server configured for client authentication, and the configuration must include the IP address of your RADIUS server, the ability to generate and trigger client COA messages, and a shared password.

Follow these steps to configure an external RADIUS server for the WPA2-Multikey feature:

1. In the vWLAN GUI, navigate to the **Configuration** tab, and select **External Authentication > Servers > Create Server**.
2. In the **Create Server** menu, enter the following information:
  - Specify the RADIUS server type as **RadiusMultikeyAuthServer**.
  - Enter a name for the server in the **Name** field.
  - Optionally select the **Compute PMK at external GW** check box to enable the enhanced version of the WPA2-Multikey feature. When this box is selected, up to **1000** PMKs can be generated by the external server. Refer to [Enhanced WPA2-Multikey Support on page 30](#) for specifics about this feature.
  - Enter the IP address of your RADIUS server in the appropriate field.
  - The **Port** value should be set to **1812** (that is the default setting).
  - Verify that the **Radius COA** check box is selected, and that the **Radius COA Port** value is set to **3799**.
  - Specify a Shared Secret/Password in the appropriate field. Make sure to note the password entered in this field as you will need it later in the configuration process.
3. Once the information for the RADIUS server has been entered, select **Create Authentication Server** to create the RADIUS server used by vWLAN for the WPA2-Multikey feature.

## Configuring the External Accounting Server for WPA2-Multikey

After configuring the external authentication server for use with the WPA2-Multikey feature, you must configure an external accounting server to work in tandem with the authentication server.

Follow these steps to configure an accounting server for the WPA2-Multikey feature:

1. In the vWLAN GUI, navigate to the **Configuration** tab, and select **External Authentication > Accounting > Create Accounting Server**.
2. In the **Create Accounting Server** menu, enter the following information:
  - Enter a name for the server in the **Name** field.
  - Verify that the **Enabled** check box is selected.
  - Enter the IP address of your RADIUS server in the appropriate field.
  - The **Port** value should be set to **1813** (that is the default setting).
  - Specify a Shared Secret/Password in the appropriate field. Make sure to note the password entered in this field as you will need it later in the configuration process.
3. Once the information for the accounting server has been entered, select **Create Accounting Server** to create the RADIUS server used by vWLAN for the WPA2-Multikey feature.

After configuring the RADIUS and accounting servers to use with the WPA2-Multikey feature, you can begin configuring the feature in vWLAN itself.

## Configuring the WPA2-Multikey Feature in vWLAN

To configure the WPA2-Multikey feature, you must configure two different SSIDs for the AP. One as an open SSID, and one with WPA2-Multikey enabled. The following steps outline the basic configurations for enabling and using the WPA2-Multikey feature:



### NOTE

*The following instructions assume you are familiar with configuring and using vWLAN, SSIDs, Captive Portal, and in general, the wireless network. The steps included below focus solely on items that must be configured for the WPA2-Multikey feature to function.*

1. Configure your wireless network with at least two VLANs: one for first time connections (using an Open SSID and shared Wi-Fi password), and one for registered users (using a WPA2-Multikey SSID). In addition, configure the RADIUS server with the appropriate attributes for both VLANs, and include any necessary RADIUS database information.
2. Configure an SSID for clients connecting to the network for the first time. This should be an SSID with open security and a shared password. In addition, captive portal should be enabled and configured for this SSID so that connected clients are redirected to the captive portal and can complete the registration process.
3. Configure a second SSID for previously registered clients to connect to the network. This SSID should use WPA2-PSK for authentication, have the multikey feature enabled, and be associated with the appropriate RADIUS server, as shown below:

**Create SSID**

Name/ESSID: PSK SSID

Broadcast SSID:

Authentication: WPA2-PSK

Cipher: AES-CCM

Multi Key:

Enable Captive Portal Authentication:

RADIUS Multi Key Authentication Server: Local-FreeRadius

DynamicSteering:



### NOTE

*The RADIUS server entered in the RADIUS MultiKey Authentication Server should be the same as the RADIUS server configured in [Configuring the External RADIUS Server for WPA2-Multikey on page 241](#).*

4. Once the SSID is created, apply the SSID to an AP template and then push the updated template to the vWLAN APs. Once the templates are applied to the APs, the WPA2-Multikey configuration is complete.

**NOTE**

*For more information about AP templates, and their configuration or application, refer to [Configuring AP Templates on page 149](#).*

## 14. Managing AP Networks

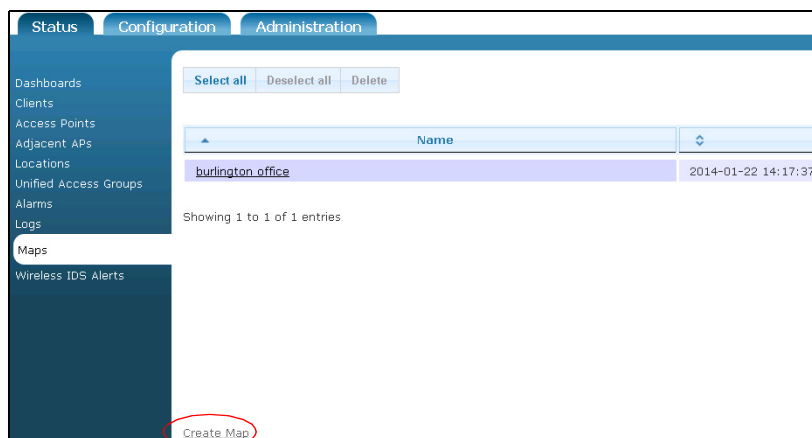
This section discusses vWLAN AP network management. AP management tasks include using AP heat maps, interpreting wireless IDS alerts and adjacencies, and managing AP users and locations. This chapter includes the following sections:

- [Using Heat Maps on page 244](#)
- [Configuring Wireless IDS Alerts on page 247](#)
- [Managing Users and Locations on page 252](#)

### Using Heat Maps

Heat maps are created based on the RF coverage of APs within the domain. Heat maps can be used to verify coverage areas, AP functionality and power usage, RF signal location, and environmental changes. Heat maps can also be used, using triangulation, to locate RF signals (select an AP in the **Adjacent APs** menu on the **Status** tab). To access the heat map associated with the domain, or to create a new map, access the GUI and follow these steps:

1. Navigate to the **Status** tab, and select **Maps**. Any previously created maps are listed in this menu. If you want to edit a previously created map, select the map from the list. To create a new map, select **Create Map** at the bottom of this menu, or select **Domain Map** from the **Create** drop-down menu.



2. In the **New Map** menu, enter the name for the map in the **Name** field.

**Create Map**

Name

Floor Map Image  No file selected.  
*Use a JPEG or PNG format image.*

Map Type

Map Environment

Accesspoints

0 items selected

- + Adela1
- + BSAP-18021234567890
- + BSAP-18023811040999
- + BSAP-18412112040350
- + BSAP-19201913050386
- + BSAP-19204212050686
- + BSAP1920-00-19-92-35-2d-40

Use Calibration

3. Upload a map file to the new map by selecting a file to upload from your location by selecting **Browse**.

Floor Map Image  No file selected.  
*Use a JPEG or PNG format image.*

4. Specify the map type (**Indoors** or **Outdoors**) from the **Map Type** drop-down menu and the map environment (**Open Space**, **Cubicles**, **Interior Walls**, or **Cubicles and Interior Walls**) from the **Map Environment** drop-down menu.

Map Type

Map Environment

5. Next, select the APs that you want to associate with this map using the + (plus) symbol. Specify if you want to use calibration by selecting the **Use Calibration** check box.

**NOTE**

*If the heat map is not calibrated precisely, the APs may not be displayed on the map.*

6. Select **Create Map** to create the map. A confirmation indicating the successful creation of the new map is displayed.

Once the map file has been uploaded, and the new map is created, the system will display the status map with the following information:

- AP coverage circles based on the current transmit power settings of the APs.
- If an AP is disconnected, the map reflects no power from the failed AP and increased power from the adjacent APs.
- Coverage area for either the 802.11b/g/n and 802.11a/n/ac radios (depending on the selection).
- Down or disconnected APs will be displayed as not having any coverage.
- Maps include the ability to view specific channels, spectrums, and changes in the environment.

In addition, RF signal strength is displayed on the heat map. [Table 1](#) indicates the signal strength and corresponding color on the heat map.

**Table 1. Heat Map Signal Strength Color**

Signal Strength (dBm)	Color
-35 or greater	Red
-50	Orange
-60	Yellow
-70	Green
-80	Blue
-85	Dark Blue

**Table 1. Heat Map Signal Strength Color (Continued)**

Signal Strength (dBm)	Color
Less than -85	Clear

## Configuring Wireless IDS Alerts

Wireless intrusion detection system (IDS) alerts are configured by the administrator for each domain in vWLAN. Wireless IDS alerts are based on RF alerts. In vWLAN, the RF alerts outlined in [Table 2](#) are enabled by default. In the GUI you can specify which alerts are enabled or disabled.

Each alert type is listed in the **Configuration** tab, **Wireless > Wireless IDS Alert Config** menu, with an ID number, severity level, enabled status, and description of each alert. The only configuration available for RF alerts is to enable or disable the alert per domain.

**Table 2. Supported RF Alerts in vWLAN**

RF Alert	Severity	Mode of AP Required to Detect	Alert Description
AirJack Attack	Warning	Sensor Mode Only	Airjack is a tool set that allows attackers to inject fake 802.11 packets in order to gain network access or create a DoS attack. Information about Airjack attacks is available online at <a href="http://sourceforge.net/projects/airjack/">http://sourceforge.net/projects/airjack/</a> .
AP Broadcasting Multiple SSID	Warning	Sensor Mode Only	The AP is broadcasting multiple SSIDs. This can indicate a spoof attempt.
AP Channel Change	Informational	Dual Mode or Sensor Mode	The AP has changed channels.
AP Denied Association	Informational	Dual Mode or Sensor Mode	An authorized AP denied an association request from a client.
AP Down	Informational	Sensor Mode Only	The AP is down.
AP in WDS Mode	Informational	Dual Mode or Sensor Mode	The AP is operating in WDS (bridge) mode.
AP Low Signal Strength	Informational	Sensor Mode Only	An AP with low signal strength is detected.
AP Overloaded	Informational	Dual Mode or Sensor Mode	An overloaded AP refuses new client associations.
AP Restarted	Informational	Sensor Mode Only	The AP has restarted.

**Table 2. Supported RF Alerts in vWLAN (Continued)**

RF Alert	Severity	Mode of AP Required to Detect	Alert Description
AP SSID Changed	Informational	Dual Mode or Sensor Mode	An AP has changed its SSID. If this action was not authorized, then there is a possible spoof in progress.
ASLEAP Attack	Severe	Sensor Mode Only	ASLEAP is a tool that exploits a weakness in CISCO proprietary LEAP protocol.
Authorized AP Down	Informational	Dual Mode or Sensor Mode	An authorized AP can no longer be heard by the sensor. This can indicate that the AP has failed or been removed from service.
Broadcast Attack	Informational	Sensor Mode Only	Many attacks use broadcast disassociate or deauthenticate frames to disconnect all users on the network, redirect them to a fake network, cause a DoS attack, or disclose a cloaked SSID.
Client Association Change	Warning	Dual Mode or Sensor Mode	Client has changed its association to a different AP. This can be caused by a rouge AP in the vicinity.
Client BSSID Changed	Warning	Dual Mode or Sensor Mode	Mobile station has changed its BSSID.
Client Limit	Informational	Dual Mode or Sensor Mode	Maximum client limit per AP has been reached. This can be due to a MAC spoofing client or real network density increase.
Client Rate Support Mismatch	Informational	Dual Mode or Sensor Mode	Specified mandatory data rate in probe request does not match the values advertised by the AP.
Client to Rogue AP	Severe	Dual Mode or Sensor Mode	An authorized client is connected to a rogue AP.
Deauthentication Flood	Severe	Sensor Mode Only	An attacker is conducting a DoS attack by flooding the network with 802.11 deauthentication frames in an attempt to disconnect users from APs.



**Table 2. Supported RF Alerts in vWLAN (Continued)**

RF Alert	Severity	Mode of AP Required to Detect	Alert Description
Dissassociation Traffic	Warning	Sensor Mode Only	This alarm indicates that a client is continuing to send traffic within 10 seconds of being disassociated from an AP.
Duration Attack	Severe	Sensor Mode Only	An attacker sends 802.11 frame with 0xFF in the duration field. This forces other mobile nodes in the range to wait until the value reaches zero. If the attacker sends Continue Packets with large durations, it prevents other nodes from operating for a long time. This can result in a DoS attack.
EAPOL ID Flood	Severe	Sensor Mode Only	Attacker tries to bring down an AP by consuming the EAP identifier space (0 to 255).
EAPOL Logoff Storm	Severe	Sensor Mode Only	An attacker floods the air with EAPOL logoff frames. It can result in DoS to all legitimate stations.
EAPOL Spoofed Failure	Severe	Sensor Mode Only	Spoofed EAP failure messages detected.
EAPOL Spoofed Success	Severe	Sensor Mode Only	Spoofed EAP success messages detected.
EAPOL Start Storm	Severe	Sensor Mode Only	Attacker floods the air with EAPOL start frames. This can result in DoS to all legitimate stations.
Fata-Jack Attack	Severe	Sensor Mode Only	A Fata-Jack device sends an authentication failure packet to a mobile node to prevent the client from receiving any vWLAN services.
Invalid Deauthentication Code	Warning	Dual Mode or Sensor Mode	Unknown deauthentication reason code. Some APs and drivers cannot handle improper reason codes.

**Table 2. Supported RF Alerts in vWLAN (Continued)**

RF Alert	Severity	Mode of AP Required to Detect	Alert Description
Invalid Disconnect Code	Warning	Dual Mode or Sensor Mode	Unknown disassociation reason code. Some APs and drivers cannot handle improper reason codes.
Invalid Probe Response	Severe	Dual Mode or Sensor Mode	An AP has responded to a client probe with a 0 length SSID, which is an invalid response that can create a fatal error with some client cards. This can be a faulty AP or an attacker specifically crafting the packet to disrupt the network.
Link Test	Informational	Dual Mode or Sensor Mode	Some products provide link testing capability that can use network bandwidth.
MSF Broadcom Exploit	Severe	Dual Mode or Sensor Mode	MSF-style poisoned exploit packet for Broadcom drivers. This can be used for client hijacking.
MSF D-link Exploit	Severe	Dual Mode or Sensor Mode	MSF-style poisoned 802.11 rate field in the beacon for a D-Link driver. This can be used for client hijacking.
MSF Netgear Exploit	Severe	Sensor Mode Only	MSF-style poisoned 802.11 over-sized options beacon for Netgear driver attacks. This can be used for client hijacking.
Netstumbler Probe	Informational	Dual Mode or Sensor Mode	Netstumbler is a wireless network scanning tool. It can be the precursor to a more serious attack.
Network Probe	Warning	Dual Mode or Sensor Mode	A client is probing the network, looking for a wireless AP, but it is not connecting. Many wireless cards and operating systems do this by default in an attempt to automatically find APs; however, this could be an operational issue indicating a misconfigured client.

**Table 2. Supported RF Alerts in vWLAN (Continued)**

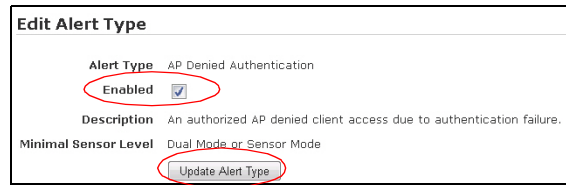
RF Alert	Severity	Mode of AP Required to Detect	Alert Description
Possible AP Spoof	Severe	Sensor Mode Only	A BSS timestamp mismatch in beacon or probe frames is likely to indicate an attempt to spoof the BSSID or SSID of an AP.
Rogue Ad-Hoc Client	Warning	Dual Mode or Sensor Mode	A rogue client in Ad-Hoc mode has been detected.
Rogue AP SSID Changed	Informational	Dual Mode or Sensor Mode	A rogue AP has changed the SSID.
Rogue AP	Severe	Dual Mode or Sensor Mode	A rogue AP has been detected. Check that this is not a newly installed AP or an AP belonging to a nearby organization.
SSID too long	Warning	Dual Mode or Sensor Mode	SSID length exceeds 32 bytes (larger than allowed by 802.11 standards). This indicates an SSID handling exploit.
Wellenreiter Probe	Informational	Dual Mode or Sensor Mode	Wellenreiter is a wireless network scanning tool.
WEP Disabled	Warning	Dual Mode or Sensor Mode	An AP is not using WEP encryption.

To enable or disable an RF alert, access the GUI and follow these steps:

1. Navigate to the **Configuration** tab, and select **Wireless > Wireless IDS Alert Config**. The supported RF alerts are listed in this menu. Select the appropriate Alert Type from the list to enable or disable the specified alarm.

Alert Type	Enabled	Description
<a href="#">AirJack Attack</a>	true	Airjack is a toolset that allows attackers to inject fake 802.11 packets in order to gain network access. The tool and its variants (wlan-jack, monkey-jack, essid-jack, cracker-jack) can be found here: <a href="http://www.airjack.com/">http://www.airjack.com/</a>
<a href="#">AP Broadcasting Multiple SSID</a>	true	The AP is broadcasting multiple SSIDs. This can indicate a spoof attempt
<a href="#">AP Channel Change</a>	false	The Access Point has changed channels.
<a href="#">AP Denied Association</a>	true	An authorized AP denied an association request from client.
<a href="#">AP Denied Authentication</a>	true	An authorized AP denied client access due to authentication failure.
<a href="#">AP Down</a>	false	The AP is down.
<a href="#">AP in WDS Mode</a>	false	AP is operating in WDS (bridge) mode.
<a href="#">AP Low Signal</a>	false	An AP with low signal strength is detected by BAP sensor.

2. Select or deselect the **Enabled** check box to enable or disable the alert. Select **Update Alert Type** to apply the changes.

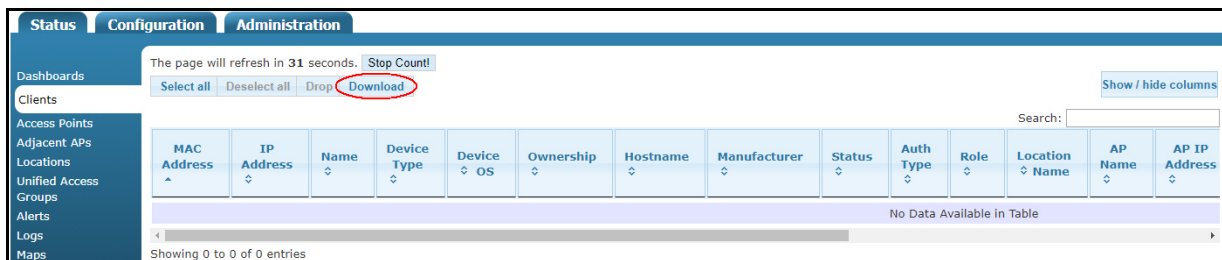


For instructions on viewing RFID alarms or alerts, refer to [Viewing/Acknowledging Wireless IDS Alerts on page 253](#). Refer to [SNMP Trap Configuration on page 257](#) and [Syslog Configuration on page 258](#) for more information.

## Managing Users and Locations

Users can be viewed by tracking them in the **Status** tab and selecting **Clients** in the GUI. This menu lists the user actions, status, name, MAC address, IP address, role, SSID, start time, login time, associated AP MAC address, associated AP IP address, associated AP name, bytes sent or received, VLAN used, unified access group, user location, authentication type, device type, device operating system, device ownership, device host name, and device manufacturer for each user. From this menu you can determine what actions should be taken for each user (drop, etc.) and determine who is connected to the domain, how long they've been connected, and how much traffic they are generating.

As of firmware release 3.1.0, you can select the **Download** button to download a CSV file of the table data. This download option is also available from the **Status >Access Points** menu.



To view the configuration details of a client, select a client from the list. A new menu presents the individual configuration information for the selected client

Each user is associated with a named AP. If the AP was not named in its configuration, it receives a default name of the BSAP model paired with the MAC address. For example, a BSAP 1920, with the MAC address 00:19:92:00:79:e0 has a default name of **BSAP-1920-00-19-92-00-79-e0**. The AP name can be used to easily identify which users are associated with which APs in the vWLAN system.

Locations can be monitored by navigating to the **Status** tab and selecting **Locations**. This menu lists the name, status, CIDR, VLAN, and available APs for every configured location on the domain. From this menu you can select the location from the list to view the location's configuration. Once a location is selected, the location details are displayed and you can choose to edit or delete the location. Selecting edit from this menu returns you to the **Editing location** menu, as described in [Configuring Domain Locations on page 94](#).

Name	Status	CIDR	VLAN
yLoc-0-192.168.0.0/16	INACTIVE	192.168.0.0/16	0
yLoc-0-192.168.100.0/22	ACTIVE	192.168.100.0/22	0
NAC	ACTIVE	10.252.0.0/14	1



**NOTE**

As of firmware release 3.5.0, the location information displayed for clients using an SSID with WPA2-Multikey enabled is either **Active** or **Inactive**. Active locations indicate a VLAN specified to the AP by the RADIUS server that has provided a DHCP discovery response. Inactive locations indicate that the AP did not receive a DHCP discovery response for the RADIUS-assigned VLAN. In addition, clients connected to an SSID with WPA2-Multikey enabled display the VLAN with which they are associated as their location name.

**Viewing/Acknowledging Wireless IDS Alerts**

Whenever an enabled RF alert is triggered, it is logged and can be viewed by navigating to the **Status** tab and selecting **Wireless IDS Alerts**. This menu lists all RF alerts, along with the source MAC address of the device that triggered the alarm, the alert type, the SSID, the sensor's name, and the time of the event. To view any RF alerts that have been triggered in the domain, access the GUI, navigate to the **Status** configuration tab, and select **Wireless IDS Alerts**. You can selectively acknowledge or delete individual alerts, or purge them all. You can also download the alerts in CSV format.

Source MAC	Alert Type	SSID	Sensor Name	Last Seen	Acknowledged
00:19:92:38:79:21	Rogue AP	ITestSsid	AP05	2018-01-26 19:03:34 UTC	No
00:19:92:38:64:02	Rogue AP	Dynamic_RF_Test_SSID_1	AP09	2018-01-25 16:09:19 UTC	No
00:19:92:38:64:06	Rogue AP	Dynamic_RF_Test_SSID_5	AP09	2018-01-25 16:09:19 UTC	No
00:19:92:38:70:E1	Rogue AP	ITestSsid	AP09	2018-01-26 19:53:58 UTC	No
00:19:92:80:2E:64	Rogue AP	PQ414RG_24	AP09	2018-01-26 19:53:58 UTC	No
00:19:92:80:2E:64	Rogue AP	PQ414RG_24	AP05	2018-01-26 19:03:34 UTC	No
00:19:92:DF:14:AF	Rogue AP	<no ssid>	AP25	2018-01-26 17:44:43 UTC	No
00:19:92:38:75:E1	Rogue AP	Dynamic_RF_Test_SSID_0	AP09	2018-01-26 14:43:21 UTC	No
00:19:92:80:2E:64	Rogue AP	PQ414RG_24	AP25	2018-01-26 20:06:29 UTC	No
00:19:92:28:2B:85	Rogue AP	<no ssid>	AP25	2018-01-26 14:59:16 UTC	No
00:19:92:38:79:21	Rogue AP	ITestSsid	AP09	2018-01-26 19:53:58 UTC	No
00:19:92:3D:4C:01	Rogue AP	TestSSID	AP29	2018-01-26 20:06:15 UTC	No
62:19:92:28:2B:86	Rogue AP	Testing1234	AP25	2018-01-26 14:59:16 UTC	No
00:19:92:38:64:08	Rogue AP	Dynamic_RF_Test_SSID_7	AP09	2018-01-25 16:12:37 UTC	No
00:19:92:28:64:05	Rogue AP	Dynamic_RF_Test_SSID_4	AP09	2018-01-25 16:10:26 UTC	No

Acknowledge an alert by selecting the alert you want to acknowledge and then select **Acknowledge**.

Source MAC	Alert Type	SSID	Sensor Name	Last Seen	Acknowledged
00:19:92:3B:79:21	Rogue AP	ITestSsid	AP05	2018-01-26 19:03:34 UTC	No
00:19:92:3B:64:02	Rogue AP	Dynamic_RF_Test_SSID_1	AP09	2018-01-25 16:09:19 UTC	No
00:19:92:3B:64:06	Rogue AP	Dynamic_RF_Test_SSID_5	AP09	2018-01-25 16:09:19 UTC	No
00:19:92:3B:70:E1	Rogue AP	ITestSsid	AP09	2018-01-26 19:53:58 UTC	No
00:19:92:80:2E:64	Rogue AP	PQ414RG_24	AP09	2018-01-26 19:53:58 UTC	No
00:19:92:80:2E:64	Rogue AP	PQ414RG_24	AP05	2018-01-26 19:03:34 UTC	No
00:19:92:DF:14:AF	Rogue AP	<no ssid>	AP25	2018-01-26 17:44:43 UTC	No
00:19:92:3B:75:E1	Rogue AP	Dynamic_RF_Test_SSID_0	AP09	2018-01-26 14:43:21 UTC	No
00:19:92:80:2E:64	Rogue AP	PQ414RG_24	AP25	2018-01-26 20:06:29 UTC	No
00:19:92:28:2B:B5	Rogue AP	<no ssid>	AP25	2018-01-26 14:59:16 UTC	No
00:19:92:3B:79:21	Rogue AP	ITestSsid	AP09	2018-01-26 19:53:58 UTC	No
00:19:92:3D:4C:01	Rogue AP	TestSSID	AP29	2018-01-26 20:06:15 UTC	No
62:19:92:28:2B:B6	Rogue AP	Testing1234	AP25	2018-01-26 14:59:16 UTC	No
00:19:92:3B:64:08	Rogue AP	Dynamic_RF_Test_SSID_7	AP09	2018-01-25 16:12:37 UTC	No
00:19:92:3B:64:05	Rogue AP	Dynamic_RF_Test_SSID_4	AP09	2018-01-25 16:10:36 UTC	No

**NOTE**  
*You must be logged in as a root user to have the ability to acknowledge alerts.*

A message containing the date and time of acknowledgment is displayed in the Acknowledged column.

Source MAC	Alert Type	SSID	Sensor Name	Last Seen	Acknowledged
00:19:92:3B:79:21	Rogue AP	ITestSsid	AP05	2018-01-26 19:03:34 UTC	Yes, by root@adtran.com at 2018-01-26 20:13:00
00:A0:C8:ED:7C:C4	Rogue AP	<no ssid>	AP25	2018-01-26 16:12:43 UTC	No
06:19:92:DF:14:AF	Rogue AP	ADTRAN_5GHZ_1758	AP25	2018-01-26 17:44:43 UTC	No
00:19:92:4F:08:44	Rogue AP	Dynamic_RF_Test_SSID_3	AP09	2018-01-26 14:43:21 UTC	No
00:19:92:4F:08:48	Rogue AP	Dynamic_RF_Test_SSID_7	AP09	2018-01-26 14:43:21 UTC	No
00:19:92:4F:08:41	Rogue AP	Dynamic_RF_Test_SSID_0	AP09	2018-01-26 14:43:21 UTC	No
00:19:92:4F:08:42	Rogue AP	Dynamic_RF_Test_SSID_1	AP09	2018-01-26 14:43:21 UTC	No
00:19:92:3B:75:E7	Rogue AP	Dynamic_RF_Test_SSID_6	AP09	2018-01-26 14:43:21 UTC	No
00:19:92:3B:75:E6	Rogue AP	Dynamic_RF_Test_SSID_5	AP09	2018-01-26 14:43:21 UTC	No
00:19:92:3B:75:E5	Rogue AP	Dynamic_RF_Test_SSID_4	AP09	2018-01-26 14:43:21 UTC	No

## 15. vWLAN Management

There are several management tasks that are associated with the maintenance and use of vWLAN. Typical management tasks include configuring and executing diagnostics, managing users, viewing and searching logs, using the dashboard, managing alarms, and managing administration tasks. The vWLAN management features described in this section are:

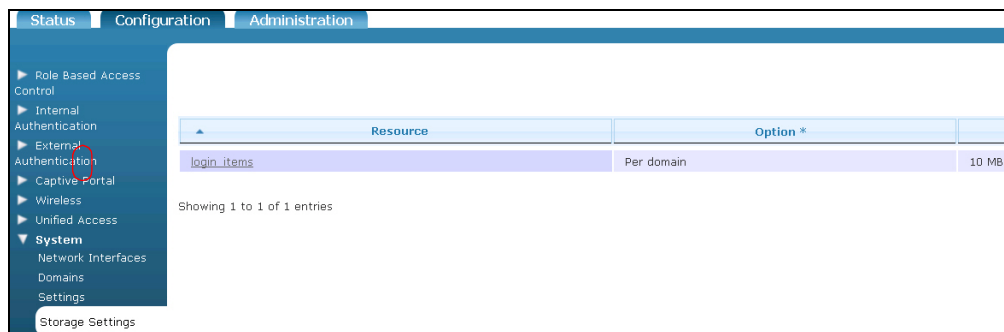
- [Managing Domain Storage Settings on page 255](#)
- [Configuring Notifications on page 256](#)
- [Administrative Tasks on page 265](#)
- [Configuring vWLAN Jobs on page 265](#)
- [Diagnostic Tools on page 267](#)
- [Viewing and Searching Logs on page 271](#)
- [Viewing Alerts on page 272](#)
- [Using the Reporting Dashboard on page 273](#)

### Managing Domain Storage Settings

Domain storage settings are the amount of storage allocated to a domain to store login items. Login items include all files that can be uploaded for captive portal configurations. Domain storage settings can be specified by allocating a specific amount of space for all domains, allocating a specific amount of space per domain AP, or by allocating space for each domain individually. If all domains have been allocated a fixed amount of storage, the storage is automatically applied to any new domains and cannot be changed except by editing the storage settings. In addition, new items cannot be uploaded to the domain if it will cause the domain to exceed its storage limit. Storage limits are automatically updated when adding, destroying, or moving APs within the domain.

To specify the domain storage setting for login items, follow these steps:

1. Navigate to the **Configuration** tab, and select **System > Storage Settings**. Select the storage setting item from the list.



2. Next, specify the storage space allocation method. To allocate a specific amount of storage space per domain, select **Allocate each domain \_\_\_\_\_ MB** and enter the amount (in MB).

To allocate a specific amount of storage space per AP on the domain, select **Allocate each domain \_\_\_\_\_ MB per AP** and enter the amount (in MB). If each domain has a fixed amount of storage per

AP, an AP cannot be moved or destroyed if it will cause the storage limit of the current domain to be reduced below the amount of storage already in use. If this selection is chosen, when new domains are created, their storage limit is **0** until an AP is added to the domain.

To allocate a specific amount of storage space on a per-domain basis, select **Specify the storage for each domain**. Then, enter the allotted space (in MB) in the appropriate field for each listed domain. If this method is chosen for allocating storage space, the space can be edited from the domain configuration (refer to [Creating the Domain on page 85](#)).

3. Select **Update Storage setting** to apply the changes.

## Configuring Notifications

vWLAN administrators can configure several types of notifications to be kept apprised of the functionality and condition of the vWLAN domain. The types of notifications created differ between the platform administrator and the domain administrator. The platform administrator creates notifications which provide a set of messages about the system, for example, high CPU or memory usage on the vWLAN system. The domain administrator creates notifications that can include information messages, SNMP traps, syslog notifications, email notifications, and any outstanding administrative tasks specific to APs or end users on the domain, but not about the vWLAN system itself. To configure these notifications, access the GUI and follow the steps outlined in the following sections.

### Notification Templates

Notification templates are the criteria used by vWLAN to determine when information messages are generated, and to organize these messages according to type. By default, three notification templates exist in vWLAN: debug, error, and info. These templates can be deleted, edited, or displayed, and you can also create your own templates. Each template allows you to configure the parameters surrounding the reporting of certain events through vWLAN. You can specify that notifications are emailed to specific people (one or more), that syslog messages are sent when events are detected, and that SNMP traps are sent when certain events are detected.



When creating templates, you will need to have previously configured SNMP, syslog, and an email address if you are going to use any of these notification features. To complete these actions, follow the steps outlined in the following sections.

## SNMP Trap Configuration

SNMP traps are used to communicate with external network management systems (NMSs) that certain events have occurred by using SNMP messages. To create an SNMP trap in vWLAN, follow these steps:

1. Navigate to the **Configuration** tab, and select **Notifications > SNMP Trap**. Select the **Domain** tab if you are creating an SNMP trap for a specific domain, and select the **Platform** tab if you are creating an SNMP trap for the vWLAN platform. Any previously configured traps will be listed in the menu. If you want to edit a previously created trap, select the trap from the list. To create a new SNMP trap, either select **Create SNMP Trap Configuration** at the bottom of this menu, or select **Platform SNMP Trap Configuration** from the **Create** drop-down menu (at the top of the menu).



2. In the new SNMP trap menu, enter the IP address of the vWLAN instance to which you want the trap associated. Entering **127.0.0.1** indicates the trap is associated with the local vWLAN, and will display in the corresponding **Alarms** menu (for the platform or domain from which it originated). Next, enter the community string associated with the trap. The community string can be any string, but might need to match a specific string to be received at the external NMS. In the example, the string is **Private**. Optionally, you can associate the trap with a previously configured notification template. By default, you can select from the debug, error, or info template. SNMP traps are also created to be associated with new templates, so you can opt to leave this blank. If you do create a new template

using this trap, you can associate this trap with the template by editing the trap after the template is complete (refer to [Configuring AP Templates on page 149](#)).

### Create SNMP Trap Configuration

IP Address:   
IP address of SNMP Trap Server. 127.0.0.1 means the local vWLAN box.

Community String:   
Community string can be between 6-20 characters.

Notification Templates

0 items selected <a href="#">Remove all</a>	<input type="text"/> <a href="#">Add all</a>
	<ul style="list-style-type: none"> <li><a href="#">+ debug_template</a></li> <li><a href="#">+ error_template</a></li> <li><a href="#">+ info_template</a></li> </ul>

*Choose your desired notification templates and move them to the left table.*

[Create SNMP Trap Configuration](#)

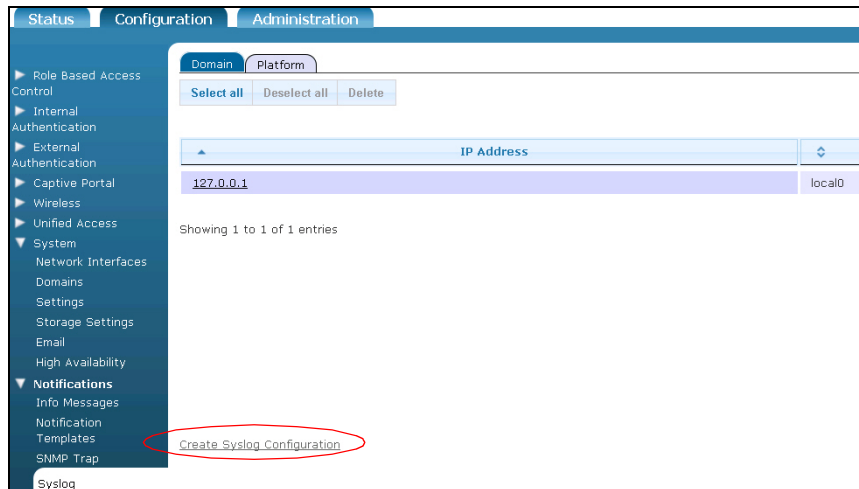
3. Select **Create SNMP trap configuration**. A confirmation is displayed indicating that the trap has been created. The trap will now appear in the SNMP trap list (**Configuration** tab, **Notifications** > **SNMP Trap**), where you can display, edit, or delete the trap.
4. If you are in the process of creating an SNMP trap in order to create a notification template, you can continue on to the next step of creating a syslog configuration. Once you have created the notification template, and you want to associate it with this SNMP trap, return to the **Configuration** tab, and select **Notifications** > **SNMP Trap** and edit the trap, making sure to select the correct template from the drop-down menu. If you are only configuring an SNMP trap, you have completed the configuration.

## Syslog Configuration

Syslog is used for managing the vWLAN system by aiding in the creation of generalized informational, analysis, or debug messages. Syslog functions so that the data can be reported by vWLAN, stored locally at vWLAN or an external syslog server, and analyzed later. To create a syslog notification, follow these steps:

1. Navigate to the **Configuration** tab, and select **Notifications** > **Syslog**. Then select the **Domain** tab if you are creating syslog reports for a specific domain, or select the **Platform** tab if you are creating syslog reports for the vWLAN system. Any previously configured logs will be listed in the menu. If you want to edit a previously created log, select the log from the list. To create a new syslog event,

either select **Create Syslog configuration** at the bottom of this menu, or select **Platform Syslog Configuration** from the **Create** drop-down menu (at the top of the menu).



- Enter the IP address of the vWLAN instance to which you want the log associated. Entering **127.0.0.1** indicates the syslog message is associated with the local vWLAN, and is displayed in the corresponding **Logs** menu (in either the platform administration or individual domain GUI, depending from which administration the message originated). Next, select the facility associated with the trap from the **Facility** drop-down menu. The facility is the type of system that is monitored by the syslog. vWLAN supports the use of local facilities (**local0** through **local7**) to monitor local use, but the facility is important for external syslog messages that have to be received and separated at the external syslog server. Optionally, you can associate the syslog notification with a previously configured notification template. By default you can select from the debug, error, or info template. Syslog notifications are also created to be associated with new templates, so you can opt to leave this blank. If you do create a new template using this syslog configuration, you can associate this syslog configuration with the template by editing the syslog notification after the template is complete (refer to [Notification Templates on page 256](#)).

### Create Syslog Configuration

IP Address   
IP address of syslog server. 127.0.0.1 means the local vWLAN box.

Facility

Notification Templates

0 items selected <a href="#">Remove all</a>	<input type="text"/> <a href="#">Add all</a>
	<a href="#">+ debug_template</a>
	<a href="#">+ error_template</a>
	<a href="#">+ info_template</a>

Choose your desired notification templates and move them to the left table.

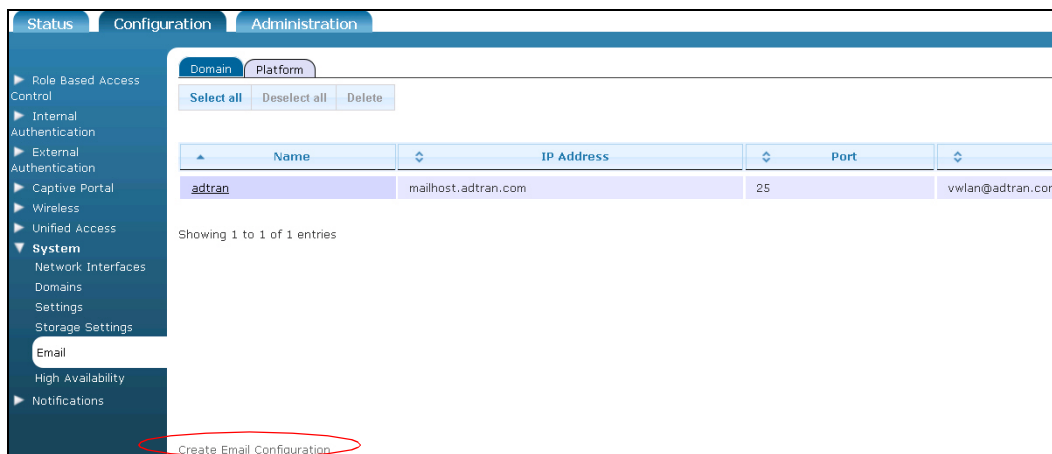
[Create Syslog Configuration](#)

3. Select **Create Syslog configuration**. A confirmation is displayed indicating that the syslog configuration has been created. The syslog notification will now appear in the syslog list (**Configuration** tab, **Notifications** > **Syslog**), where you can display, edit, or delete the notification.
4. If you are in the process of creating an syslog notification in order to create a notification template, you can continue on to the next step of creating email address(es) to associate with notifications. Once you have created the notification template, and you want to associate it with this syslog configuration, return to the **Configuration** tab, select **Notifications** > **Syslog**, and edit the notification, making sure to select the correct template from the drop-down menu. If you are only configuring a syslog notification, you have completed the configuration.

## Email Account Configuration

Email notification of certain events observed by vWLAN can be configured by configuring an email server account and associating it to the desired message types (through the notification template). To create an email server account for notifications, follow these steps:

1. Navigate to the **Configuration** tab, and select **System** > **Email**. If you are configuring an email server for a specific domain, select the **Domain** tab. If you are configuring an email server for the vWLAN system, select the **Platform** tab. Any previously configured email accounts will be listed in the menu. If you want to edit a previously created account, select the account from the list. To create a new email account, either select **Create Email Configuration** at the bottom of this menu, or select **Platform Email Configuration** from the **Create** drop-down menu (at the top of the menu).



2. Enter the name and IP address or host name of the email server in the appropriate fields. Next, enter the port number used by the server in the **Server Port Number** field (default port is **25**). Then, enter the return email address in the appropriate field. This is the email address to which responses to notifications should be sent. By default, the return email address is **vvlan@adtran.com**. Next, select the authentication method used by this email account from the drop-down list. Choices include **None** or **Login**. If you select **Login**, you will be prompted to enter an SMTP user name and password to associate with the account. You can also optionally choose to include email security by selecting **TLS** from the **Email Security** drop-down menu. If you enable email security, you will also be prompted to enable certificate verification. You can disable this option by deselecting the **Verify Certificate** checkbox. You should disable this option if the email server certificate is not signed by a commonly

trusted CA (such as VeriSign), if the name on the certificate does not match the server, or if the certificate is expired.

**Create Email Configuration**

Server name: Mail 1

Server IP Address Or Hostname: 172.1.1.59

Server Port Number: 25

Return Email Address: vwlan@adtran.com

Authentication Method: Login

SMTP User Name: root@adtran.com

SMTP Password: ●●●●●●

SMTP Password Confirmation:

Email Security: TLS

Verify Certificate:

Create Email Configuration

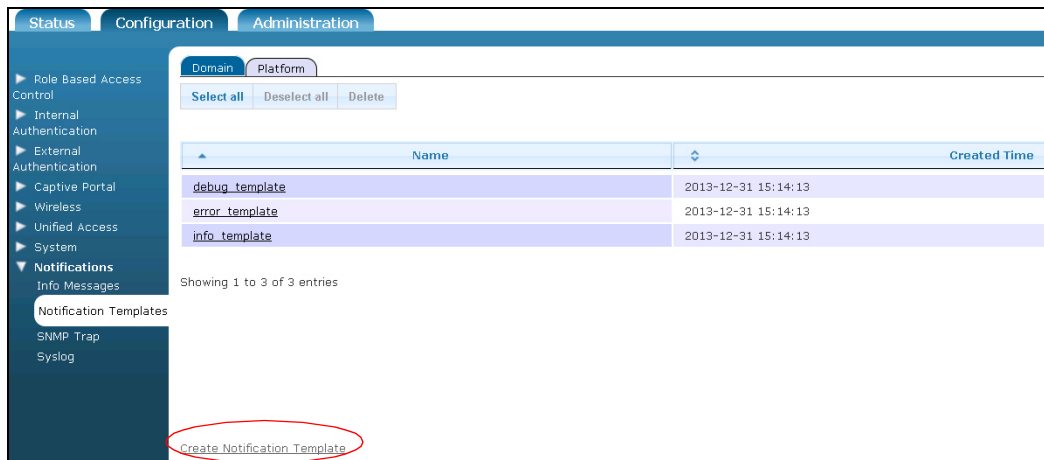
3. Select **Create Email Configuration**. A confirmation is displayed indicating that the email account has been created. The email account will now appear in the list (**Configuration** tab, **System** > **Email**), where you can display, edit, or delete the email account.
4. If you are in the process of creating an email account in order to create a notification template, you can continue on to the next step of creating the template.

## Creating Notification Templates

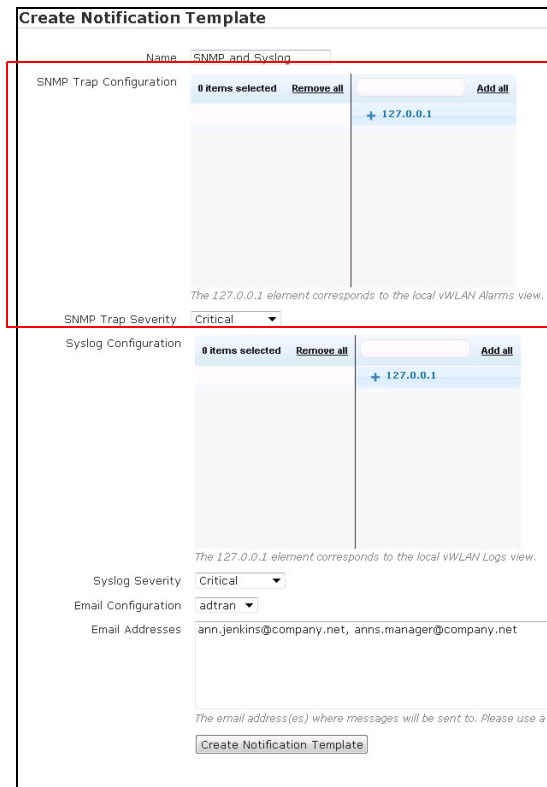
Notification templates are used to specify the kind of messages and notifications that are created by vWLAN. In addition, notification templates use any configured SNMP traps, syslogs, and email accounts to create customized notifications based on vWLAN systems and notification preferences, with the ability to send specific notifications to configured email accounts. By default, three notification templates exist in the vWLAN: debug, error, and info templates. These templates are used to determine what kind of informational messages are displayed, and each informational message is associated with a specific template. To create a notification template, or edit an existing template, follow these steps:

1. Navigate to the **Configuration** tab, and select **Notifications** > **Notification Templates**. If you are creating a notification template for a specific domain, select the **Domain** tab. If you are creating a notification template for the vWLAN system, select the **Platform** tab. Any previously configured templates will be listed in the menu. If you want to edit a previously created template, select the template from the list. To create a new notification template, either select **Create Notification**

**Template** at the bottom of this menu, or select **Platform Notification Template** from the **Create** drop-down menu (at the top of the menu).



2. Enter the name of the template in the **Name** field.
3. Optionally, you can select the SNMP trap configuration you want to associate to the template. If **127.0.0.1** is specified, this means that the SNMP trap is the vWLAN Alarms table. Select the SNMP trap destination from the list (to create an SNMP trap, refer to [SNMP Trap Configuration on page 257](#)). Then specify the SNMP trap severity from the **SNMP Trap Severity** drop-down menu.



4. Optionally, select the syslog configuration you want to associate with the template. If **127.0.0.1** is specified, this means that the syslog configuration is the vWLAN logs table. Select the vWLAN you

want to monitor from the list (to create a syslog notification, refer to [Syslog Configuration on page 258](#)). Then specify the syslog severity from the **Syslog Severity** drop-down menu.

Syslog Configuration

0 items selected Remove all

+ 127.0.0.1 Add all

The 127.0.0.1 element corresponds to the local vWLAN Logs view.

Syslog Severity Critical

- Optionally, you can specify the email notification type for this template. Specify the previously created email server handling the email notification (refer to [Email Account Configuration on page 260](#)), and enter an email address, or several email addresses separated by commas, to which to send the notifications. Once you have entered the name, SNMP trap, syslog, and email information, select **Create Notification Template**.

Create Notification Template

Name SNMP and Syslog

SNMP Trap Configuration

0 items selected Remove all

+ 127.0.0.1 Add all

The 127.0.0.1 element corresponds to the local vWLAN Alarms view.

SNMP Trap Severity Critical

Syslog Configuration

0 items selected Remove all

+ 127.0.0.1 Add all

The 127.0.0.1 element corresponds to the local vWLAN Logs view.

Syslog Severity Critical

Email Configuration adtran

Email Addresses ann.jenkins@company.net, anns.manager@company.net

The email address(es) where messages will be sent to. Please use a

Create Notification Template

- A confirmation is displayed indicating that the notification template has been created. The template will now appear in the notification template list (**Configuration** tab, **Notifications** > **Notification Templates**), where you can display, edit, or delete the template. In addition, the template will be used to generate specific informational messages based on the entered criteria. For example, the previous template configuration will result in an email notification to Ann Jenkins and her manager,

and an SNMP trap and syslog message sent to 127.1.1.1, whenever the vWLAN instance receives an event of critical status.

## Information Messages

Information messages are created when certain events occur within the vWLAN system. These messages document when certain configurations occurred, were implemented, failed, or succeeded, as well as when problems with the APs, vWLAN system, or the network occur. Information messages can be error or informational or debug messages and are classified using the notification template. In addition, information messages can track any configuration changes (creations, deletions, updates) and who authorized the change. Information message types are determined by notification templates, which allow you to classify the information notifications as you prefer.

Information messages cannot be created by the administrator, but rather, notification templates are created which then classify the message type when the specified events occur. You cannot delete informational messages, but you can edit the type of template to which they are associated.

To view information messages, follow these steps:

1. Navigate to the **Configuration** tab, and select **Notifications > Info Messages**. Select the **Domain** tab if you are working with messages for a specific domain, or select the **Platform** tab if you are working with messages for the vWLAN system. The messages that have been generated are listed, and include the product with which the message is associated (AP, vWLAN, etc.), the message type (action that generated the message), and the notification template associated with the message (info, error, etc.).

Message Type	Category	Template
802.1x_auth_successful	Auth	info_template
ap_command_failed	AP	error_template
ap_command_successful	AP	info_template
ap_config_failed	AP	error_template
ap_config_successful	AP	info_template
ap_connection_added	AP	info_template
ap_connection_deleted	AP	info_template
ap_firmware_failed	AP	error_template
ap_firmware_successful	AP	info_template
ap_firmware_updated	AP	info_template
ap_setting_added	AP	info_template

Showing 1 to 52 of 52 entries

2. To edit the type of template associated with a specific message, select the message from the list. Then, select the notification template to associate with the message from the drop-down menu. Available notification templates include error, info, and debug templates (by default), and any



additional templates you have created (refer to [Notification Templates on page 256](#)). Select **Update Info Message** to apply the template change.

**Edit Info Message**

Category AP

Message Type ap\_config\_failed

Notification Template error\_template

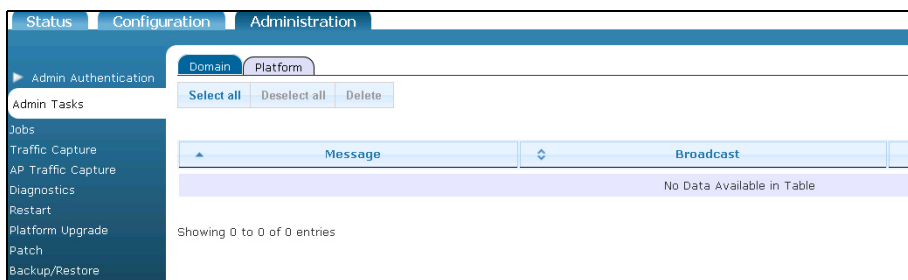
Update Info Message

## Administrative Tasks

Administrative tasks are pending tasks that affect the configuration of the vWLAN system or a specific domain. For example, when you configure vWLAN to switch partitions, an administrative task is created that indicates the vWLAN should be rebooted. Administrative tasks are listed in the top of the GUI (refer to [General GUI Shortcuts on page 41](#)) so that you can see what items need to be completed for root administration or domain maintenance or configuration. If there are no pending tasks, the number **0** is displayed in black. If there are pending tasks, the count of tasks is displayed in red. Administrative tasks are available to both platform and domain administrators.

To view and complete administrative tasks, access the GUI and follow these steps:

1. Navigate to the **Administration** tab, and select **Admin Tasks** or select **Domain Tasks** or **Platform Tasks** at the top of the GUI. If you want to work with tasks for a specific domain, select the **Domain** tab, or select the **Platform** tab to work with tasks for the vWLAN system. All active administrative tasks are listed in this menu. You can select to delete or execute the task by selecting the task from the list. Typically tasks should not be deleted unless you have already executed it another way or you want to abort a reboot.



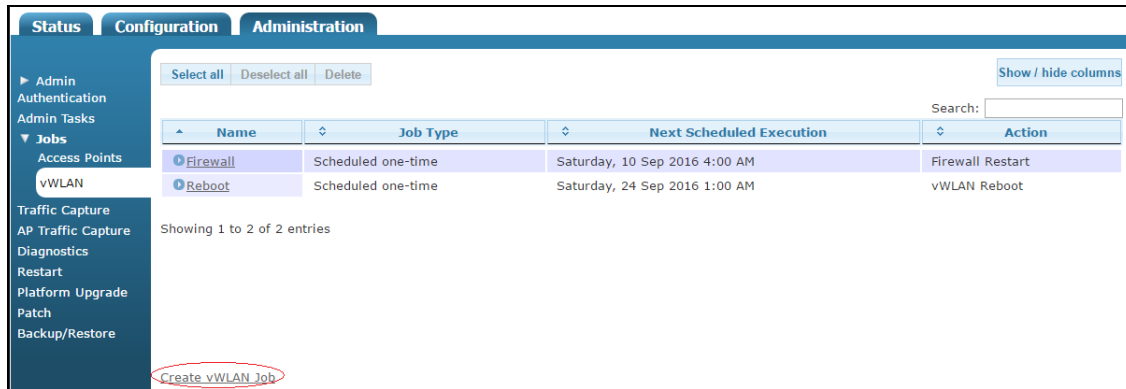
2. Select the arrow icon next to the task in the list to execute the task. When the task is completed, a message is generated indicating the successful execution of the task. You can then delete the task from the list. You can also monitor the number of administrative tasks for the vWLAN system, or a specific domain, by viewing the **Platform Tasks** or **Domain Tasks** count at the top of the GUI menu.

## Configuring vWLAN Jobs

To help manage vWLAN administration, you have the ability to create and schedule one-time or recurring vWLAN jobs. Scheduling administrative jobs provides the flexibility of having the system perform the associated task at a time and frequency of your choosing.

To create a vWLAN job, follow these steps:

1. Navigate to the **Administration** tab and select **Jobs > vWLAN**. In this menu, all current vWLAN jobs are listed. Each listing includes the name of the job, the job type, the next scheduled execution time for the job, and the action to be completed by the job. To create a new vWLAN job, select **Create vWLAN Job** at the bottom of this menu. To modify an existing job, select the job name from the list.



2. Enter the name for the job in the **Name** field.

**Create vWLAN Job**

Name

Action

Scheduled

[Back](#)

3. Select the appropriate action for the job from the **Action** drop-down menu.
4. To schedule the job, select the **Scheduled** check box to display the scheduling options. Use the **Frequency** drop-down menu to specify how often the job will run: **Daily**, **Weekly**, **Monthly**, or **One-time**. Select **Scheduled Date** to use the calendar to select the beginning date for the job. Use the **Scheduled Time** drop-down menus to specify the start time for the job.

Scheduled

Frequency

Scheduled Date

Scheduled Time  :

5. Select **Create vWLAN Job** to create the job.

6. Once the job has been created, it will appear in the job list in the **vWLAN Jobs** menu. To execute a job immediately, select the arrow next to the job in the job list. You will receive a confirmation that the job has been completed.

Name	Job Type	Next Scheduled Execution	Action
Firewall	Scheduled one-time	Saturday, 10 Sep 2016 4:00 AM	Firewall Restart
Reboot	Scheduled one-time	Saturday, 24 Sep 2016 1:00 AM	vWLAN Reboot

## Diagnostic Tools

Diagnostic tools are used by administrators to monitor the performance of the vWLAN system or a specific domain, and to uncover any potential problem areas or configurations. The diagnostic tools available are described in the following sections.

### Platform Administrator Diagnostic Tools

To access the platform administrator diagnostic tools, navigate to the **Administration** tab, and select **Diagnostics**. Then select the **Platform** tab. From the **Diagnostics** menu you can choose to ping a specified host (by entering the IP address or host name and selecting either the network or management interface), perform a traceroute for a specified host (by entering the IP address or host name and selecting either the network or management interface), view a list of network statistics, display the address resolution table, clear the address resolution table, show the state of all currently configured processes in the vWLAN system, show the IP information for the network interface, or connect to ADTRAN support. To configure any of these options, follow these steps:

1. Navigate to the **Administration** tab, select **Diagnostics**, select the **Platform** tab, and enter the appropriate options.

The screenshot shows the 'Platform' tab of the diagnostic tools interface. It contains the following elements:

- Ping**: Radio button selected. Includes an 'Address' input field and an 'Interface' dropdown menu (set to 'Any').
- Traceroute**: Radio button unselected. Includes an 'Address' input field and an 'Interface' dropdown menu (set to 'Any').
- Routes**: Radio button unselected. Description: 'List of vWLAN routes (including static routes).'.
- Netstat**: Radio button unselected. Description: 'List network statistics, e.g. socket status, queue depths, IP connections, etc..'
- ARP**: Radio button unselected. Description: 'Display address resolution table.'
- Clear ARP Cache**: Radio button unselected. Description: 'Clear address resolution table cache.'
- Show Processes**: Radio button unselected. Description: 'List the status (running/not running) of all processes.'
- Show Network Interface Parameters**: Radio button unselected. Description: 'Shows the IP information.'
- Phone Home to ADTRAN Support**: Radio button unselected. Includes a 'Port' input field.

At the bottom of the interface, a button labeled 'Run Diagnostic' is circled in red.

2. Select **Run diagnostic** at the bottom of the menu to complete the diagnostic actions selected. When the diagnostic task is complete, the results are displayed.

## Phone Home Support

In addition to other platform diagnostics, vWLAN supports a phone home feature. This feature creates a secure on-demand connection from vWLAN back to ADTRAN technical support, allowing technicians to access the vWLAN system by HTTPS and SSH for advanced diagnostics. Upon completion of the diagnostics, phone home can be terminated, and technical support will no longer have access to vWLAN. Phone home requires platform administrative access and contacting technical support to obtain a port number for phone home use. Port **2335** outgoing to **cse-support.bluesocket.com** must be allowed in any firewalls in front of the vWLAN system, and the vWLAN system should be able to resolve the DNS name cse-support.bluesocket.com. The platform administrator should provide technical support with read/write or read-only platform administrator credentials as applicable.

## Domain Administrator Diagnostic Tools

There are a number of diagnostic tools available to assist with verifying network connectivity on a domain. The tools provided from the Domain tab include ping, traceroute, and testing external server authentication. To execute a ping test or traceroute, specify a host (by entering the IP address or host name) and select either the network or management interface. To test an external authentication method, select the authentication server from the drop-down menu, then enter the username and password to use for authentication. The results of the diagnostic task are displayed once the task is complete.



### NOTE

*Additional information for executing an external server authentication test is provided in [External Authentication Test Results](#).*

To access the domain administration diagnostic tools, follow these steps:

1. Navigate to the **Administration** tab, select **Diagnostics**, select the **Domain** tab, and enter the information in the appropriate fields.

The screenshot shows the 'Domain' tab selected in the top navigation. Below the navigation are three sections: 'Ping', 'Traceroute', and 'External Authentication Test'. Each section has a radio button and a 'Run Diagnostic' button. The 'External Authentication Test' section is currently selected, and its 'Run Diagnostic' button is circled in red. The 'Authentication Server' dropdown is set to 'RadiusMacAuth'. The 'Username' and 'Password' fields are empty, with placeholder text below them: 'Enter Username' and 'Enter Password'. The 'Run Diagnostic' button is located at the bottom of the form.

2. Select **Run diagnostic** at the bottom of the menu. The results are displayed once the task is complete.

## External Authentication Test Results

Initiating a diagnostic test to verify external server authentication can be performed only if the external authentication servers are already configured in vWLAN. Refer to [External Server Authentication on page 109](#) for information on configuring an external server authentication method. A successful test connection will display a message indicating the success and specifying the role name where the client can be placed. For example,

```
Authentication Successful: Client shall be placed into "AllowedAll" role
```

Additionally, the message displayed will indicate the response attributes from the external authentication server, if available. Should the test fail, it could be due to a time out, invalid credentials, or other reasons. The reason will be indicated as part of the error message.

## Packet Captures

In addition to the ping and traceroute diagnostic features, administrators can also perform packet captures on specific APs or on vWLAN as a whole. Multiple packet captures can be run at once, and there is no limit to the number of captures that can be executed, although running a large number of captures at once can slow down the vWLAN system. These packet captures allow you to view the traffic traveling to and from specified APs or vWLAN, with a list of capture files that updates every three seconds.

## Domain Packet Captures

To configure a packet capture report for the APs on a domain, follow these steps:



### NOTE

*Configuring a wireless packet capture on an AP will place the AP into sensor mode (assuming the AP radio in question is not already in sensor mode). The AP will return to its normal mode when the capture is complete, or the action is stopped by an administrator.*

1. Navigate to the **Administration** tab, and select **AP Traffic Capture**.

- Specify the AP on which you want to capture packets by selecting the AP from the **AP** drop-down menu. Then, select whether you are capturing wireless or wired traffic from the **Capture Type** drop-down menu.

Attention: A Wireless traffic capture will put the AP into sensor mode and then return to AP mode when the capture is completed (or stopped by user).  
The list of captured files will update every 3 seconds.

AP: Adela1  
Capture Type: Wired  
Interface: BG(2.4Ghz)  
802.11b/g/n (2.4GHz) SSID: 24007BETA  
Protocol: Any  
IP Address:   
MAC Address:   
Maximum Packet Size: 1500  
The default value of maximum packet size is 1500. Range: 0~1500.  
Number of Packets: 10000  
The default number of packets to capture is 10000. Range: 0~1000000000000.  
Start Capture

- Next, specify the radio interface on which to capture packets. Make your selection from the **Interface** drop-down menu.

Interface: BG(2.4Ghz)

- Specify the SSID from the **SSID** drop-down menu. Then, specify the protocol from the **Protocol** menu and any IP addresses in the **IP address** field.

Interface: BG(2.4Ghz)  
802.11b/g/n (2.4GHz) SSID: 24007BETA  
Protocol: Any  
IP Address:   
MAC Address:

- Optionally, specify a MAC address from which to capture packets, and then specify the maximum packet size to capture and the maximum number of records to store. The maximum packet size is **1500** bytes by default, with a valid range of **0** to **1500** bytes. The number of records stored by default is **10000**, with a valid range of **0** to **1000000000000** records.

Maximum Packet Size: 1500  
The default value of maximum packet size is 1500. Range: 0~1500.  
Number of Packets: 10000  
The default number of packets to capture is 10000. Range: 0~1000000000000.  
Start Capture

**NOTE**

*There is a limit to the number of records you can store based on the size of the packets and the AP hardware disk available. Best practice is to clean up and delete packet captures as soon as they are no longer needed.*

6. Select **Start Capture** after entering the appropriate information. The packet capture downloads are displayed at the bottom of the **Packet Capture** menu.

## vWLAN Platform Packet Capture

To configure a packet capture report for the vWLAN system, follow these steps:

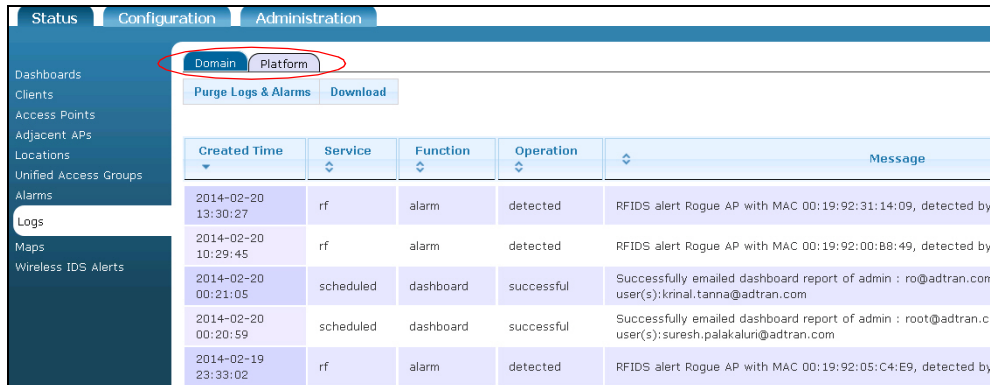
1. Navigate to the **Administration** tab, and select **Traffic Capture**.
2. Specify the **Ethernet interface** and the **Protocol** from the drop-down menus. By default, the **Public** interface is selected (the **Private** interface is only available if a network exists). Protocol selections include **Any**, **TCP**, **UDP**, or **ICMP**.
3. With all protocols except ICMP, you can also specify a port number in the **Port** field.

4. Next, optionally specify the IP address and network mask from which to capture traffic in the appropriate fields. This address can be either a source or destination address. Optionally, specify the MAC address from which to capture traffic for either the source or destination.
5. Specify the number of packets to capture in the **Number of Packets to Capture** field. By default, **10000** packets are captured.
6. Select **Start Capture** after entering the appropriate information. The packet capture downloads are displayed at the bottom of the **Packet Capture** menu.

## Viewing and Searching Logs

Logs are created based on the reports configured for the vWLAN system or a specific domain. You can view logs by navigating to the **Status** tab, and selecting **Logs**. Each log is listed, as well as the service it is associated with, the function monitored by the log, the type of log message, the message itself, the level associated with the log, and the time the log was created. In addition, administrator login and logout messages with associated IP addresses are included.

1. Navigate to the **Status** tab, and select **Logs**. If you want to view logs for a specific domain, select the **Domain** tab. If you want to view logs for the vWLAN system, select the **Platform** tab.



Created Time	Service	Function	Operation	Message
2014-02-20 13:30:27	rf	alarm	detected	RFIDS alert Rogue AP with MAC 00:19:92:31:14:09, detected by
2014-02-20 10:29:45	rf	alarm	detected	RFIDS alert Rogue AP with MAC 00:19:92:00:B8:49, detected by
2014-02-20 00:21:05	scheduled	dashboard	successful	Successfully emailed dashboard report of admin : ro@adtran.com user(s):krinal.tanna@adtran.com
2014-02-20 00:20:59	scheduled	dashboard	successful	Successfully emailed dashboard report of admin : root@adtran.co user(s):suresh.palalaluri@adtran.com
2014-02-19 23:33:02	rf	alarm	detected	RFIDS alert Rogue AP with MAC 00:19:92:05:C4:E9, detected by

2. You can search the log files for a specific entry by using the **Search** box at the top right of the logs list. You can search by service type, function, operation, or log level.
3. You can delete logs by selecting **Purge Logs & Alarms**, or you can choose to download a CSV file of the alarms by selecting **Download**.



## Viewing Alerts

In addition to using reports and logs to monitor the status of the vWLAN system or a specific domain, you can also view a list of all alerts generated on the system or domain. Administrators can view the generated alerts by navigating to the **Status** tab, and selecting **Alerts**. You choose between domain alerts (**Domain** tab) or platform alerts (**Platform** tab). In the **Alerts** menu, each recorded alert is listed, along with the service affected by the alert, the function and operation that generated the alert, the alert message, the alert type, and the time the alert occurred. Remember that when in the **Domain** tab, the alerts listed are those that affect the domain, and when in the **Platform** tab, the alerts listed are those that affect the entire vWLAN system.



### NOTE

*You can track alerts in syslog reports, SNMP traps, and email notifications. Refer to [SNMP Trap Configuration on page 257](#), [Syslog Configuration on page 258](#), and [Email Account Configuration on page 260](#) for more information.*



1. Navigate to the **Status** tab, and select **Alerts**. Choose the **Domain** or **Platform** tab.

Created Time	Service	Function	Operation	Message	Level	Acknowledged
2018-01-25T19:09:08+00:00	admin	login	failed	Admin authentication failed for root@adtran.com from 172.22.118.237	ERRORS	No
2018-01-25T19:09:02+00:00	admin	login	failed	Admin authentication failed for root@adtran.com from 172.22.118.237	ERRORS	No

2. Delete individual alerts by choosing the alert and then selecting **Delete** or remove all alerts by selecting **Purge All Alarms**. Acknowledge alerts by choosing an alert and then selecting **Acknowledge** or you can choose to download a comma separated value (CSV) file of the alerts by selecting **Download**.



#### NOTE

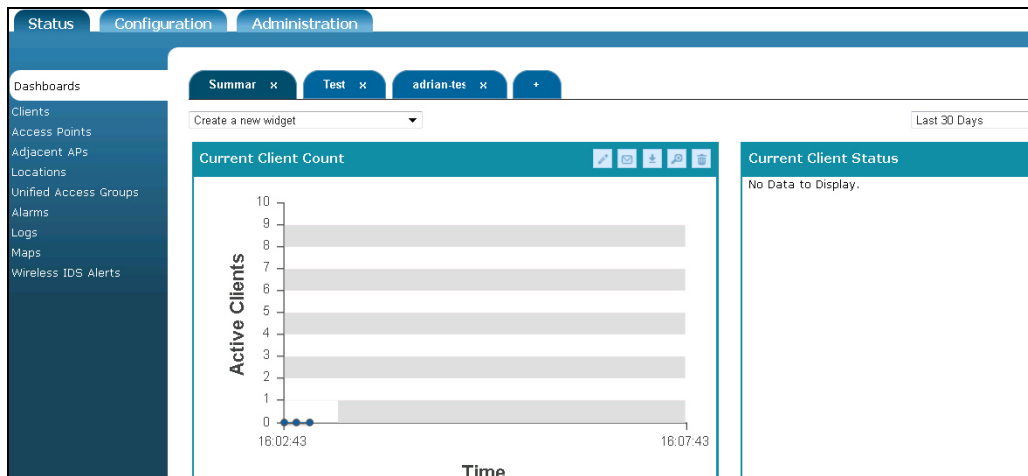
*You must be logged in as a root user to have the ability to acknowledge alerts.*

## Using the Reporting Dashboard

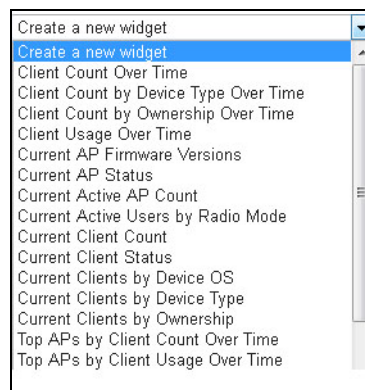
The vWLAN reporting dashboard is a collection of customized widgets that are available for you to view vWLAN information at a glance. Dashboards are used by administrators to view information about users, APs, roles, locations, SSIDs, bandwidth usage, and many other parameters used within the domain. Up to 12 widgets (2 x 6) can be configured on any one dashboard. Widgets can display either current information in real-time or historical information over time. Current widgets update in real-time while being viewed, and historical, over-time widgets present historical data over a specified amount of time (last 7 days, last 30 days, etc.). In addition, the details of any users, APs, roles, etc. can be viewed by selecting the item displayed in the widget. Domain administrators can configure which widgets are displayed, and thus which features of the domain to track, by selecting a widget to create. Creating multiple widgets allows you to create a perspective of the vWLAN network, both historically and in real-time. With the exception of the logo, each administrator's dashboard is completely separate from any others and can be fully customized to the individual's preference.

To use the reporting dashboard, follow these steps:

1. Navigate to the **Status** tab and select **Dashboards**.



2. To specify which information is summarized on the dashboard, create the appropriate widget from the **Create a new widget** drop-down menu.

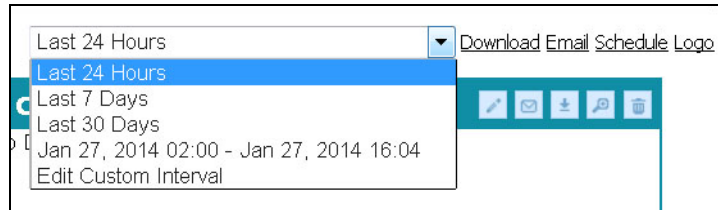


The widgets summarize the following information:

- **Client Count Over Time** is the total number of users on the domain and how long the users were active. This is a historical widget.
- **Client Count by Device Type Over Time** is summary of client counts based on device type. This is a historical widget.
- **Client Count by Ownership Over Time** is a summary of client counts based on device ownership (corporate or other). This is a historical widget.
- **Client Usage Over Time** is the total usage activity of users on the domain and how long the users were active. This is a historical widget.
- **Current AP Firmware Versions** is the total number of AP firmware versions on vWLAN. This is a current widget that displays information in real time.
- **Current AP Status** is the current status of configured APs. This is a current widget that displays information in real time.
- **Current Active AP Count** is the current count of active APs. This is a current widget that displays information in real time.

- **Current Active Users by Radio Mode** is the total number of active users on a per-radio mode basis. This is a current widget that displays information in real time.
  - **Current Client Count** is the current number of active users. This is a current widget that displays information in real time.
  - **Current Client Status** is the current status of active users. This is a current widget that displays information in real time.
  - **Current Clients by Device OS** is the current summary of associated wireless client's operating systems. This is a current widget that displays information in real time.
  - **Current Clients by Device Type** is the current summary associated wireless client's device types. This is a current widget that displays information in real time.
  - **Current Client Statistics by Device Ownership** is the current summary of associated wireless client's device ownership (corporate or other). This is a current widget that displays information in real time.
  - **Top APs by Client Count Over Time** is a listing of the APs with the most clients. This is a historical widget.
  - **Top APs by Client Usage Over Time** is a listing of the APs with the most client usage. This is a historical widget.
  - **Top Device Operating System by Client Count Over Time** is a summary of the type of operating system used by devices connected to vWLAN. This is a historical widget.
  - **Top Device Operating System by Usage Over Time** is a summary of the top ten device operating systems used by clients. This is a historical widget.
  - **Top Device Types by Client Count Over Time** is a summary of the top ten types of devices used by clients connected to vWLAN. This is a historical widget.
  - **Top Device Types by Usage Over Time** is a summary of the top ten device types used by clients. This is a historical widget.
  - **Top Clients by Usage Over Time** is a listing of the most active clients. This is a historical widget.
  - **Top Locations by Client Count Over Time** is a listing of the locations with the most clients. This is a historical widget.
  - **Top Locations by Usage Over Time** is a listing of the locations with the most activity. This is a historical widget.
  - **Top Roles by Client Count Over Time** is a listing of the roles with the most client connections. This is a historical widget.
  - **Top Roles by Usage Over Time** is a listing of the roles with the most client usage. This is a historical widget.
  - **Top SSIDs by Client Count Over Time** is a listing of the SSIDs with the most client connections. This is a historical widget.
  - **Top SSIDs by Client Usage Over Time** is a listing of the SSIDs with the most client activity. This is a historical widget.
3. To customize the historical reports of the report dashboard widgets, you can specify a time frame using the time frame drop-down menu at the top right of the **Dashboard** menu. Here you can specify

that information for the last 24 hours, last 7 days, last 30 days, a specific date range, or a customized time frame is displayed. Information for the last 2 months can be displayed on the report dashboard.



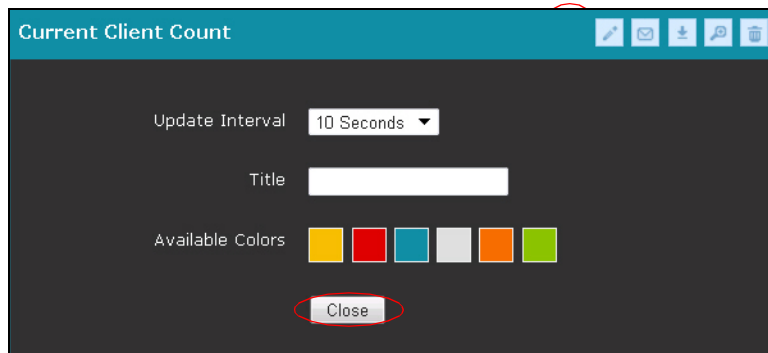
## Customizing the Report Dashboard Widgets

Report dashboard widgets can be customized in several ways. They can be moved around the dashboard menu by dragging and dropping. In addition, the display can be customized, and the widgets can be used to generate reports via email or download.

1. To customize a widget, select **Edit** at the top of the widget.



2. You can change the update interval, title, and color of the widget in the edit menu. After making changes, select **Close**.



3. You can also expand the widget to a full page summarization by selecting the magnifying glass at the top of the widget.

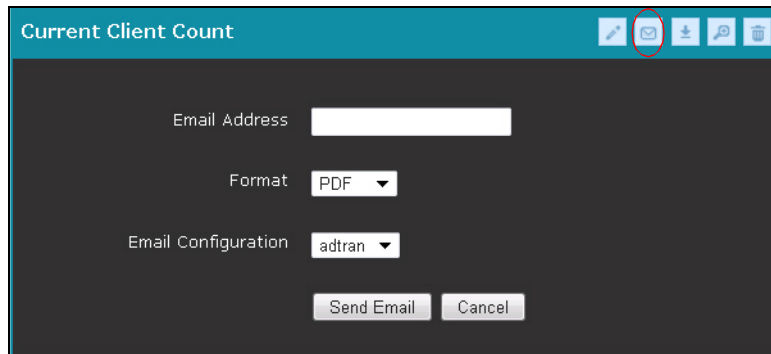


4. You can delete the widget by selecting the trash can icon at the top of the widget.

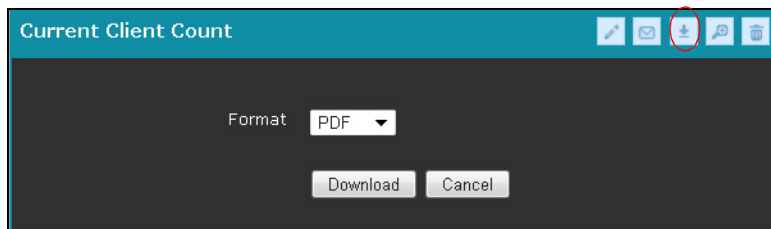


5. You can choose to email yourself a copy of the information contained in the widget by selecting the email icon from the top of the widget. Enter an email address in the appropriate field and choose the

file type from the **Format** drop-down menu (PDF, JPEG, or PNG). Lastly, select the email configuration from the drop-down menu, and select **Send Email**.



- 6. You can choose to download a copy of the information contained in the widget by selecting the download icon from the top of the widget. Specify the file format you would like to download from the **Format** drop-down menu (PDF, JPEG, PNG, or CSV) and select **Download**.



- 7. In addition, you can choose the download or email the entire set of over-time widgets, schedule an email widget report, or upload or change a logo to be included in the downloads by using the links at the top right of the report dashboard menu. To download or email real-time widgets, you must do so individually using the process outlined in Steps 5 and 6.

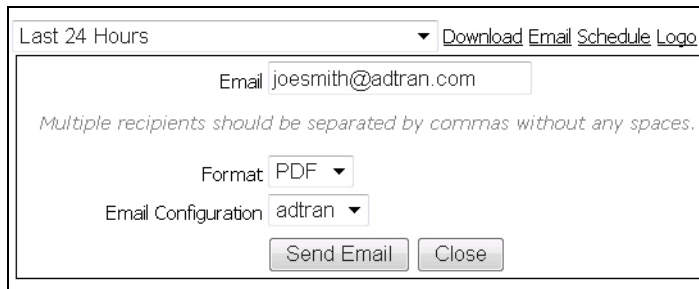


The **Download** link allows you to download the displayed over-time widgets in either PDF or CSV format.



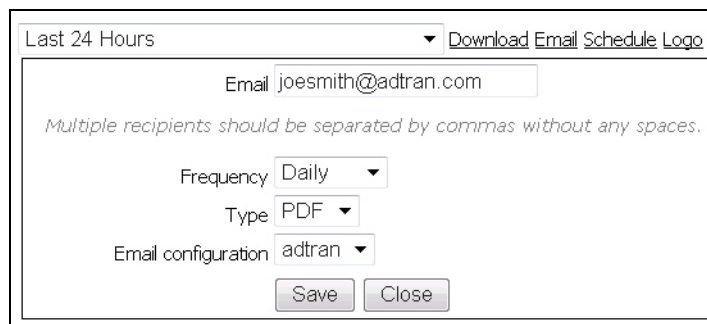
The **Email** link allows you to email the displayed over-time widgets in either PDF or CSV format. You must specify one or more email addresses in the **Email** field, select the format from the **Format**

drop-down menu, and specify the email configuration to use from the **Email Configuration** drop-down menu. Select **Send Email** to send the email to the specified recipients.

**NOTE**


*You must have an email configuration in place to send or receive emails and schedule dashboard actions. Refer to [Email Account Configuration on page 260](#) for more information.*

The **Schedule** link allows you email all the displayed widgets on a particular schedule. You can specify email addresses in the **Email** field, specify the email is sent daily, weekly or monthly using the **Frequency** drop-down menu, select the format from the **Format** drop-down menu (either PDF or CSV), and specify the email configuration to use from the **Email Configuration** drop-down menu. Select **Save** to create the email schedule.



The **Logo** link allows you to upload, change, or delete a logo associated with a particular domain to be included in the downloaded or emailed reports. To use the current logo, make no changes. To

delete a logo, select the **Logo** link and then select **Delete Logo**. To upload a new logo, select **Browse**, choose the file, and then select **Upload New Logo**.



The screenshot shows a web interface for managing logos. At the top, there is a dropdown menu set to "Last 30 Days" and a link "Download Email Schedule Logo". Below this, the "Current Logo" is displayed as the "bluesocket" logo. Underneath, there is a section "Select a logo to upload" with a "Browse..." button and the text "No file selected.". At the bottom of this section are three buttons: "Upload New Logo", "Delete Logo", and "Close".

**NOTE**

*The logo applies to all dashboards in the domain, so changing the logo impacts all other users in the domain.*

## 16. vWLAN Implementation on Public and Private Networks

Being a distributed architecture, vWLAN eliminates the need to deploy a wireless controller at each location. Instead, only APs are required at the customer premises. For real time security, RF changes and monitoring, and control and management, a persistent TCP secure TLS management and control channel is initiated by the AP upon installation and is maintained between the AP and the vWLAN. The APs can be behind a NAT device because vWLAN uses the observed IP address and port number of the control channel as an identification parameter for each AP. When vWLAN is deployed in the public cloud, most APs are likely to be behind NAT devices when they connect to vWLAN (because APs will usually not have public IP addresses). For private cloud deployments, even when the APs are fully routable to the vWLAN, the control channel is still used.

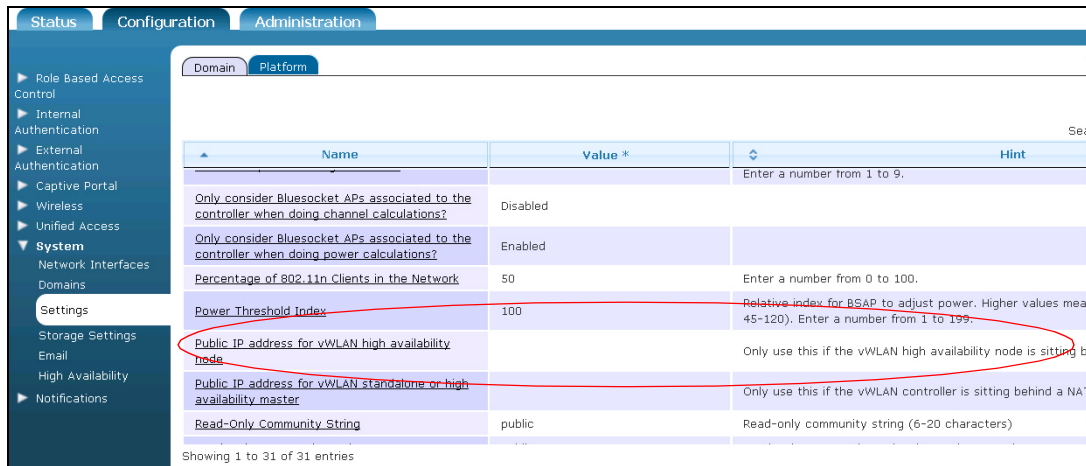
vWLAN can also exist behind a NAT device, but in this case, it must be on a one-to-one NAT configuration, where the vWLAN can be reached by the APs. The scenario for this implementation is placing the vWLAN behind a firewall (or within a demilitarized zone (DMZ)) where it is protected from the Internet, and all undesired ports and traffic is monitored and blocked by a unified threat management (UTM) product or other system. The AP must know the outside, public, or NAT IP address of the vWLAN for discovery, upgrade, control channel communication, RF channel communication, web-based authentication, and ping functionality. The administrator does this by specifying the public IP address for vWLAN in the Root settings. The public IP address of the secondary vWLAN must also be known for failover to function, so both IP addresses must be specified by the administrator. The only restriction is that if vWLAN is behind a NAT instance, then it assumes all APs are going to connect to the public IP address. Note that the two vWLAN systems will communicate through the IP addresses configured under the high availability configuration.

To configure the vWLAN for functioning behind NAT, follow these steps:

1. Ensure that the following traffic is allowed between the vWLAN and the APs:
  - UDP port 69 (TFTP) is used for BSAP 1800 Series AP firmware and AP traffic captures. TFTP stateful firewall helper must be configured on the firewall as well, because the reply source port from vWLAN is not 69.
  - Transmission Control Protocol (TCP) port 33334 is used for BSAP 1900 Series AP firmware and traffic captures.
  - TCP port 33333 (control channel) is used for vWLAN communication configuration information, status polling, and control traffic to and from the AP.
  - TCP port 28000 (RF channel) is used to send secure RF information from the AP to vWLAN.
  - TCP port 443 (Hypertext Transfer Protocol Secure (HTTPS)) is used if web-based authentication is enabled.
2. Ensure that the following traffic is allowed between vWLANs:
  - TCP port 2335 (SCP) and port 3000 is used for vWLAN to vWLAN communication and secure firmware uploads.



- Navigate to the **Configuration** tab, and select **System > Settings** and the **Platform** tab. Scroll to the **Public IP Address for vWLAN High Availability Mode** setting, and highlight the setting.



- Enter the public IP address in the appropriate field and select **Update Platform Setting**. The vWLAN is now configured with a public IP address for NAT functionality.

### Edit Platform Setting

Public IP Address For vWLAN High Availability Node

*Only use this if the vWLAN high availability node is sitting behind a NAT device.*

## 17. Additional Resources

*Table 1* below lists additional vWLAN documentation that can be beneficial to your understanding and use of vWLAN. All documents are available from the ADTRAN support community, located on the web at <https://supportcommunity.adtran.com>.

**Table 1. Additional vWLAN Documentation**

Document Title
<a href="#">AP Discovery in vWLAN</a>
<a href="#">VMware Quick Start Guide for vWLAN</a>
<a href="#">vWLAN External RADIUS-802.1X Authentication</a>
<a href="#">Mesh Networking in vWLAN</a>
<a href="#">Using APIs with vWLAN</a>
<a href="#">HTML Differences in vWLAN 2.5.0 and 2.5.1</a>
<a href="#">Layer 7 Device Fingerprinting in vWLAN</a>
<a href="#">DFS in vWLAN</a>
<a href="#">DynamicSteering in vWLAN</a>
<a href="#">DynamicRF in vWLAN</a>
<a href="#">WPA2-Multikey and Rolling-PMK in vWLAN</a>