

Adtran

Bluesocket vWLAN
Administrator Guide

Product Release: 4.5.0
Document Issue: A
Document Number: 6BSAPAG450-31A

Disclaimer of Liability

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products are given “as is”, and any liability arising in connection with such hardware or software products shall be governed by Adtran’s standard terms and conditions of sale unless otherwise set forth in a separately negotiated written agreement with Adtran that specifically applies to such hardware or software products.

To the fullest extent allowed by applicable law, in no event shall Adtran be liable for errors in this document for any damages, including but not limited to special, indirect, incidental or consequential, or any losses, such as but not limited to loss of profit, revenue, business interruption, business opportunity or data, that may arise from the use of this document or the information in it.

“Adtran” and the Adtran logo are registered trademarks of Adtran, Inc. Brand names and product names included in this document are trademarks, registered trademarks, or trade names of their respective holders.

Copyright © 2024 Adtran, Inc.
All Rights Reserved

Contents

Disclaimer of Liability	2
Contents	3
List of Figures	12
List of Tables	13
Preface	14
To the Holder of this Document	14
Hazard and Conventional Symbols	14
Revision History	15
Warranty	15
Contact Information	15
Intended Audience	15
Related Online Documents and Resources	16
Adtran Bluesocket vWLAN Overview	17
vWLAN versus Traditional WLAN	18
vWLAN Components	19
vWLAN Concepts	20
Wireless Technology	20
Fully Distributed versus Centralized Data	20
Layer 2 versus Layer 3 Architectures	21
Out-of-band NAC	21
Multicast Support	21
Bandwidth Control	21
Class of Service	22
User and Machine-based Authentication	22
Location Autodiscovery	23
Multi-tenant Support	23
WPA2-Multikey Support	24
vWLAN Solutions	25
BSAP Models Supported by vWLAN 4.5.0	26
Introduction to the vWLAN GUI	27
vWLAN Menu Structure	28

General GUI Shortcuts	29
Additional GUI Options	29
vWLAN Administrators	31
Creating an Administrator	31
Changing the Administrator Password	34
Specifying the Administrator Role	34
Specifying Administrator Authentication	36
RADIUS Administrator Authentication Considerations	37
Configuring RADIUS Administrator Authentication	37
vWLAN Platform Configuration	40
Configuring the vWLAN Network Interfaces	40
Configuring a vWLAN Network Interface Static Route	42
Changing the Administrator Session Idle Timeout	44
Configuring the Platform SNMP Parameters	44
Configuring the vWLAN TLS 1.0 Setting	45
Configuring vWLAN Platform Branding	46
Verifying the vWLAN Software Version	47
Performing System Maintenance	48
System Restart	49
Configuring Backup or Restore Parameters	50
Using Show Tech for Technical Support	51
Managing the vWLAN Runtime Image	52
Managing Patches	54
Restarting the vWLAN	55
Configuring High Availability	55
High Availability Process	56
Replicating Master Configuration Changes on the Node	58
Working with Certificates	59
Installing Certificates to vWLAN	59
Uploading Certificates to vWLAN	61
Configuring Additional vWLAN Settings for Certificates	62
Managing vWLAN Certificate Settings	66
Managing LDAP Certificates for vWLAN	67
Uploading Trusted LDAP CA to vWLAN	67

Uploading Trusted LDAP Server Certificate to vWLAN	68
Uploading Trusted LDAP Client Certificate to vWLAN	69
vWLAN Domain Configuration	70
Creating the Domain	71
Associating Administrators to a Domain	72
Configuring Domain Destinations	73
Creating Domain Destination Groups	74
Configuring Domain Services	76
Creating Domain Service Groups	77
Configuring Domain Locations	78
Configuring Domain Location Groups	79
Configuring Domain Roles	80
Un-Registered Role Type	81
Walled Garden	82
Registered Role Type	83
Configuring Domain Role Schedules	87
Configuring Web-based (Captive Portal) Authentication	88
Disable TLS 1.0	90
External Server Authentication	91
External RADIUS IX Authentication Server	91
External RADIUS Web-based Authentication Server	93
External LDAP Web-based Authentication Server	96
External SIP2 Web-based Library Authentication Server	100
Configuring Local User Authentication	102
Device Authentication	104
Bulk Import of Devices	106
Configuring Domain Accounting	107
Configuring Domain Settings	109
Configuring Domain Users	112
Configuring Domain Branding	114
Domain Configuration Backup	115
Configuring vWLAN APs	116
Editing AP Firmware	116
Uploading Locally Stored Firmware	117

Uploading Firmware Stored on a Server	118
Troubleshooting AP Firmware	119
AP Connects to System But Does Not Have Correct Firmware	120
AP is Running and Firmware is Upgraded	120
AP Firmware Matches the Alternative Partition Firmware	120
Interruptions During Upgrade	120
Simultaneous Firmware Upgrades	121
Newer AP Firmware	121
Associating APs with a Domain	121
Using AP Discovery to Connect APs to vWLAN	122
AP Discovery Process	123
System Requirements	123
Components Used in AP Discovery Configurations	124
Required Ports and Protocols	124
Configuring AP Discovery Method	126
Statically Configuring BSAPs Using the CLI	126
Configuring DHCP Option 43 in Your Organization DHCP Server	127
AOS DHCP Option 43 Configuration	129
Microsoft Windows Server 2008 R2 DHCP Option 43 Configuration	131
ISC DHCP Option 43 Configuration	135
Cisco IOS DCHP Option 43 Configuration	136
Configuring an Entry for AP Discovery in Your Organization DNS Server	136
Caching a Previously Discovered vWLAN IP Address for AP Discovery	137
Verifying BSAP Discovery	138
Troubleshooting AP Discovery	138
Troubleshooting Required TCP or UDP Ports and Protocols	139
Troubleshooting Static AP Discovery	139
Troubleshooting DHCP Option 43 AP Discovery	139
Troubleshooting DNS AP Discovery	140
Licensing APs	141
Obtaining AP Licenses	141
Uploading License Files	141
Configuring AP Templates	142
Creating AP Templates	143

Configuring a LAN Profile	150
Configuring vWLAN for CNA Support	151
Configuring DFS for vWLAN	153
DFS Overview	153
System Requirements and Limitations	154
DFS and Channel Selection	155
Channel Bonding Support	156
DFS and Mesh Networking	156
Configuring DFS	157
Configuring the AP Template for DFS	157
Configuring the AP for DFS	160
DFS Troubleshooting in vWLAN	161
Information Messages	161
Viewing AP Details	163
Mesh Networking in vWLAN	164
Typical Mesh Networking Configurations	165
Multi-hop Mesh Networks	165
Point-to-Point Mesh Networks	166
Point-to-Multipoint Mesh Networks	167
Mesh Network Deployment Considerations	167
RF Line of Sight	168
Antenna Height	169
Antenna Position and Orientation	170
Antennas and Data Rates	170
vWLAN BSAP Mesh Network Functionality	170
System Requirements and Limitations	171
Mesh Networking Data Layer Traffic	172
Mesh Networking and Dynamic Frequency Selection (DFS)	172
Configuring BSAPs for Mesh Networking	173
Mesh Networking Configuration Order	173
BSAP Mesh Network Configuration Using the GUI	174
Creating a Mesh Networking AP Template	174
Configuring the Mesh Settings Per AP	176
Viewing Mesh Network Configurations	177

Configuring DynamicRF for vWLAN	178
DynamicRF Overview	178
DynamicRF Channel Algorithm	179
DynamicRF Power Algorithm	180
DynamicRF Operation on an AP First Boot	181
Configuring DynamicRF	183
Configuring the DynamicRF Profile	183
Applying the DynamicRF Profile to an AP	186
DynamicRF Use Cases	187
Continuous Mode	187
Set Once and Hold Mode	188
AP/Sensor Mode	188
AP/Sensor Client Aware Mode	189
DynamicRF Background Scans	189
Creating DynamicRF Background Scans	190
Using AP Jobs to Create a Background DynamicRF Scan	190
Running a Background Scan from the Status Tab	191
Manually Applying DynamicRF Suggestions	192
Running DynamicRF on a Heavily Scaled vWLAN System	192
Viewing DynamicRF Statistics	193
Applying the AP Template to AP(s)	194
Configuring Additional AP Settings	194
Viewing APs	197
Viewing AP Details	198
Viewing AP States	199
Resetting and Rebooting APs	200
Configuring AP Jobs	201
vWLAN Setup Wizard	203
Launching the Setup Wizard	203
Using the Setup Wizard	204
Step 1: Configuring the Administrator	205
Step 2: Verifying the Primary and Guest Wireless Networks	206
Primary Wireless Network	206
Guest Wireless Network	207

Step 3: Reviewing the Configuration	208
Applying the Setup Wizard Settings	208
vWLAN Serial Console Configuration	209
vWLAN Wireless Configuration	210
Configuring an SSID	210
Configuring a Tunnel Profile	217
Configuring DynamicSteering for vWLAN	219
Overview of DynamicSteering	219
Pre-association Steering	220
Idle-post Association Steering	220
Active Post-association Steering	221
Steering Safety Mechanisms	223
Configuring DynamicSteering	223
Viewing Adjacent AP Neighbors	225
vWLAN Unified Access Configuration	227
Configuring Unified Access Groups	227
Configuring Switches for Unified Access	230
Unified Access Redundancy	230
Viewing the Status of Unified Access Users	231
Configuring Client Connections	232
Customizing vWLAN Login Forms and Images	232
Basic Login Form Configuration	233
Configuring Authentication using User Name and Password	234
Configuring User Login Authentication Using an Email Address	235
Specifying the Login Form Language	236
Configuring External Redirects	236
Configuring the User Service Agreement	238
Specifying the Login Attempts Parameters	238
Configuring the Visual Elements of the Login Form	239
Uploading Images and Multimedia for Login Forms	246
Customizing the Login Language	247
Viewing Customized Login Pages	250
Configuring Guest Access Parameters	251
Configuring Guest Receipts	251

Creating Guest User Accounts	253
Wireless HotSpot Account Generation	255
Hotspot Plan Configuration	256
Hotspot Account Configuration	258
Friends and Family Account Example Configuration	260
Configuring WPA2-Multikey Client Connections	261
WPA2-Multikey Use Cases and Authentication Process	262
WPA2-Multikey Configuration Considerations	263
Configuring the RADIUS Server for the WPA2-Multikey Feature	263
Configuring the External RADIUS Server for WPA2-Multikey	264
Configuring the External Accounting Server for WPA2-Multikey	265
Configuring the WPA2-Multikey Feature in vWLAN	265
Managing AP Networks	267
Using Heat Maps	267
Configuring Wireless IDS Alerts	269
Managing Users and Locations	275
Viewing/Acknowledging Wireless IDS Alerts	276
vWLAN Management	278
Managing Domain Storage Settings	278
Configuring Notifications	279
Notification Templates	280
SNMP Trap Configuration	280
Syslog Configuration	282
Email Account Configuration	283
Creating Alert Templates	284
Log Messages	286
Administrative Tasks	287
Configuring vWLAN Jobs	288
Diagnostic Tools	289
Platform Administrator Diagnostic Tools	289
Phone Home Support	290
Domain Administrator Diagnostic Tools	290
External Authentication Test Results	291
Packet Captures	291

Domain Packet Captures	292
vWLAN Platform Packet Capture	293
Viewing and Searching Logs	293
Viewing Alerts	294
Using the Reporting Dashboard	295
Customizing the Report Dashboard Widgets	297
Implementing vWLAN on Public and Private Networks	301

List of Figures

Figure 1: Multi-tenant Network Topology	24
Figure 2: Carrier Hosted Solution	25
Figure 3: Enterprise Hosted and Managed Solution	25
Figure 4: Small to Medium Business Hosted and Managed Solution	26
Figure 5: Captive Portal Login Page	88
Figure 6: Client Authentication Process	89
Figure 7: DFS Hardware Ready	155
Figure 8: Mesh Points and Mesh Portals in vWLAN Mesh Networking	164
Figure 9: Multi-hop Mesh Network Topology	165
Figure 10: Point-to-Point Mesh Network Topology	166
Figure 11: Point-to-Multipoint Mesh Network Topology	167
Figure 12: RF Line of Sight	168
Figure 13: Configuring Antenna Height and RF Line of Sight	170
Figure 14: Wireless Environment with Company APs, Third-Party APs, and Ad-hoc Network ..	180
Figure 15: Two APs Using DynamicRF Power Algorithm	181
Figure 16: DynamicRF Order of Operation	181

List of Tables

Table 1: Related Online Documentation and Resources	16
Table 2: Traditional WLAN versus vWLAN	18
Table 3: Required Ports and Protocols	124
Table 4: ASCII to Hexadecimal Conversion	128
Table 5: AOS DHCPv4 Pool Configuration Commands	129
Table 6: Antenna Height and Minimum Clearance	169
Table 7: Default Antenna Gain Values	196
Table 8: 802.11v Condition and Behavior	221
Table 9: Heat Map Signal Strength Color	269
Table 10: Supported RF Alerts in vWLAN	269

Preface

To the Holder of this Document	14
Hazard and Conventional Symbols	14
Revision History	15
Warranty	15
Contact Information	15
Intended Audience	15
Related Online Documents and Resources	16

To the Holder of this Document

This document is intended for the use of Adtran customers only for the purposes of the agreement under which the document is submitted, and no part of it may be used, reproduced, modified or transmitted in any form or means without the prior written permission of Adtran.

The contents of this document are current as of the date of publication and are subject to change without notice.

Hazard and Conventional Symbols

The hazard symbols below are used throughout this guide:



WARNING!

Warning: Indicates service affecting and possible risk of system failure.



CAUTION!

Caution: Indicates possible loss of data.



NOTE

Note: Information that emphasizes or supplements important points of the main text.

Revision History

Revision	Description
Product Release: 4.5.0 Document Number: 6BSAPAG450-31A Document Issue: A Issue Date: December 2024	Initial release

Warranty

Warranty information can be found at: my.adtran.com/warranty

Contact Information

Contact	Contact Information
Technical Support:	US/Canada Toll Free: +1-888-423-8726 Outside US/Canada: +1-256-963-8716 www.adtran.com/support
Training:	www.adtran.com/training training@adtran.com
Sales:	+1-800-827-0807

Intended Audience

The intended audience for this information is network planning engineers and craft persons responsible for the installation of the equipment. This guide assumes familiarity with the intended use of the equipment, basic required installation skills, and knowledge of local and accepted safety practices.

Related Online Documents and Resources

The documents listed in [Table 1](#) contain additional information related to this product. You can view and download these documents from the [Adtran Support Community](#) website upon previous registration.

Table 1: Related Online Documentation and Resources

Title	Description
<u>BSAP 6000 Series Hardware Installation Guide</u>	This guide describes how to install and access Adtran Bluesocket 6000 series access point (BSAP).
<u>BSAP vWLAN CLI Reference Guide</u>	This guide describes how to access and use the vWLAN CLI and AP CLI
<u>vWLAN API Reference Guide</u>	This guide describes the use of an application programming interface (API) with vWLAN.
<u>BSAP vWLAN Configuration Guide</u>	This guide describes how to connect and manage the BSAP 6000 series using one of Adtran cloud management or on-premises services.

Chapter 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 supports 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 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 fully virtualized, software-based solution gives customers the flexibility to run vWLAN on 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 identity-based access control also removes restrictions that were part of traditional WLAN solutions and provides more flexibility in managing wireless access.

This chapter contains these sections:

vWLAN versus Traditional WLAN	18
vWLAN Components	19
vWLAN Concepts	20
vWLAN Solutions	25
BSAP Models Supported by vWLAN 4.5.0	26

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 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.

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 2](#) outlines the differences between traditional WLAN and the Adtran Bluesocket vWLAN.

Table 2: 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.

Traditional WLAN	vWLAN
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.
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: virtual appliance (VMware), the APs, and software. A license is required for each AP to operate on the vWLAN. The vWLAN runs on 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

These sections describe concepts that are important to get the most benefit from your vWLAN installation:

Wireless Technology	20
Fully Distributed versus Centralized Data	20
Layer 2 versus Layer 3 Architectures	21
Out-of-band NAC	21
Multicast Support	21
Bandwidth Control	21
Class of Service	22
User and Machine-based Authentication	22
Location Autodiscovery	23
Multi-tenant Support	23

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 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 integrity has been certified during captive portal authentication, the client IP address is changed and the client data is then locally switched (out-of-band) at the AP.

Multicast Support

vWLAN 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.



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. See [Configuring an SSID](#) for more information.

Bandwidth Control

With a distributed data-plane architecture, vWLAN limits per-user bandwidth at the AP. vWLAN provides these 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

vWLAN supports Class of Service (CoS) at the edge of the network, using two components: packet prioritization and packet remarking:

- **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 802.1p 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 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 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 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 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 location is determined by the assigned user role. The AP 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.

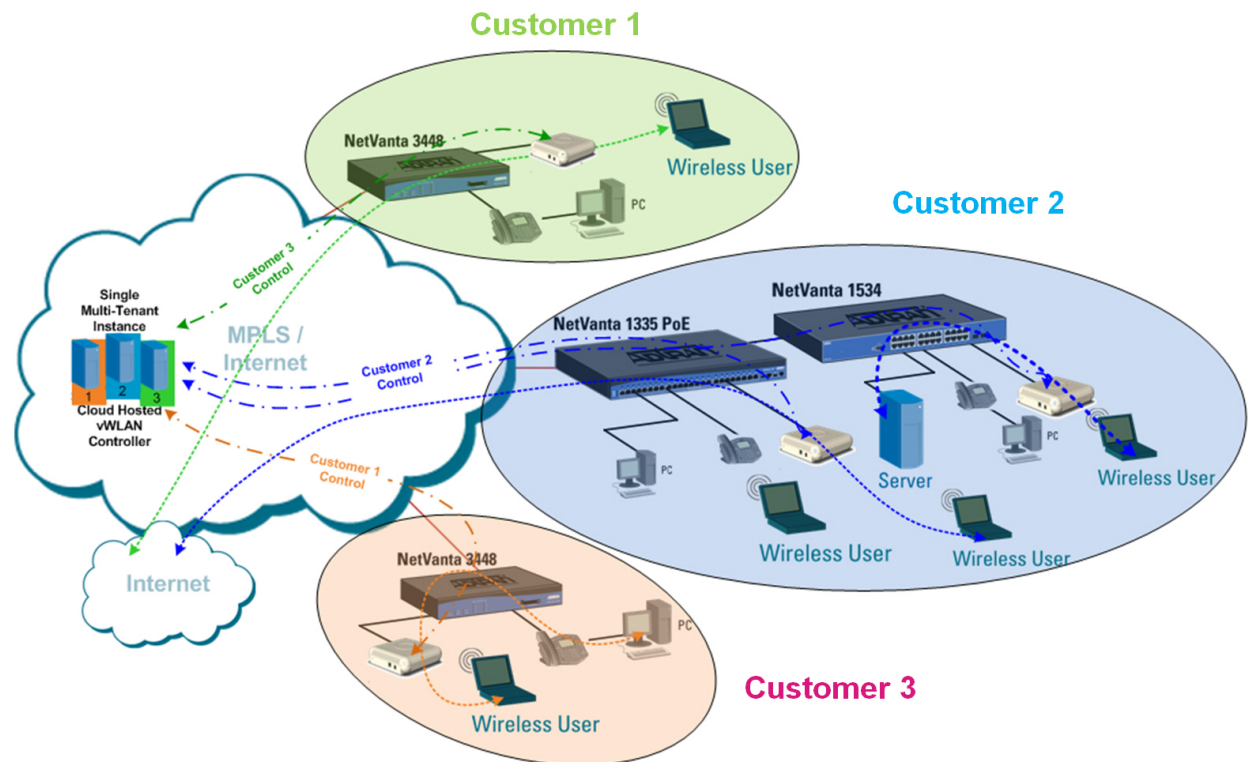
Multi-tenant Support

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: 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 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

Service providers and enterprise and small to medium sized businesses can use vWLAN. These illustrations depict the use and deployment of vWLAN in these different hosted environments.

Figure 2: Carrier Hosted Solution

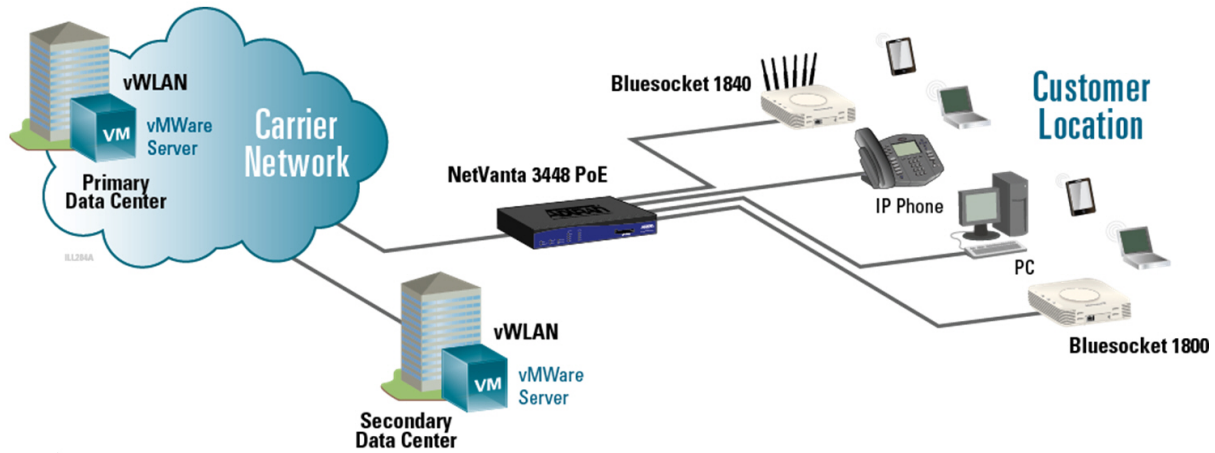


Figure 3: Enterprise Hosted and Managed Solution

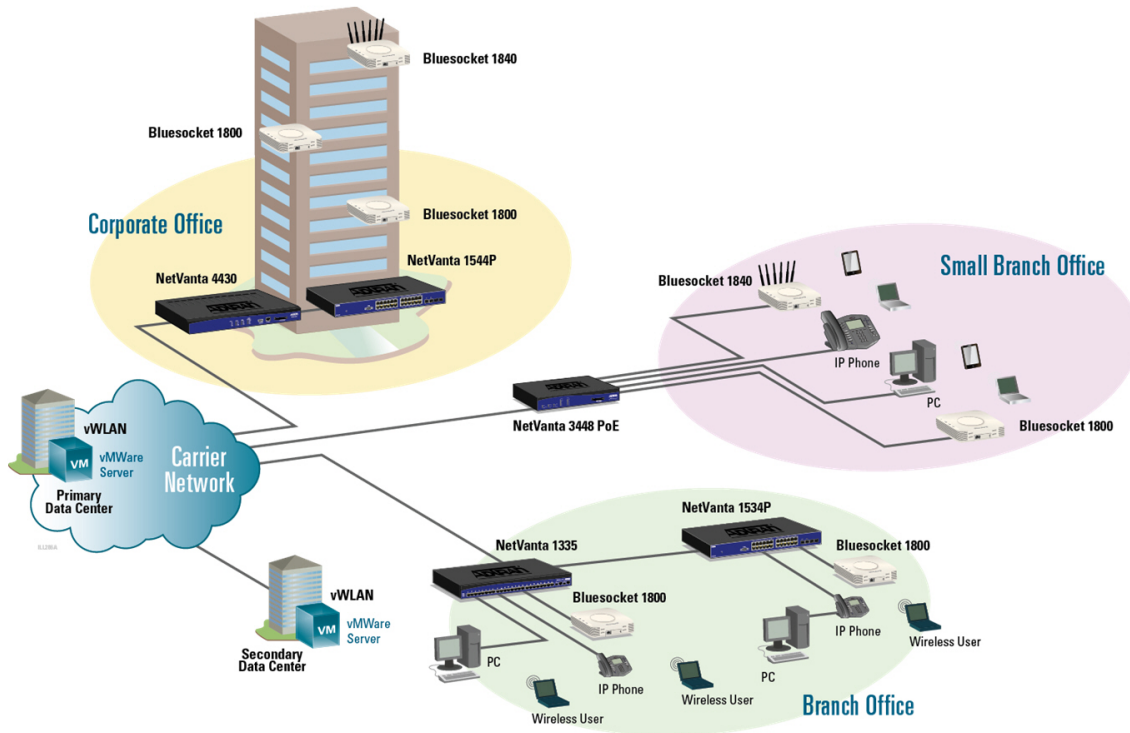
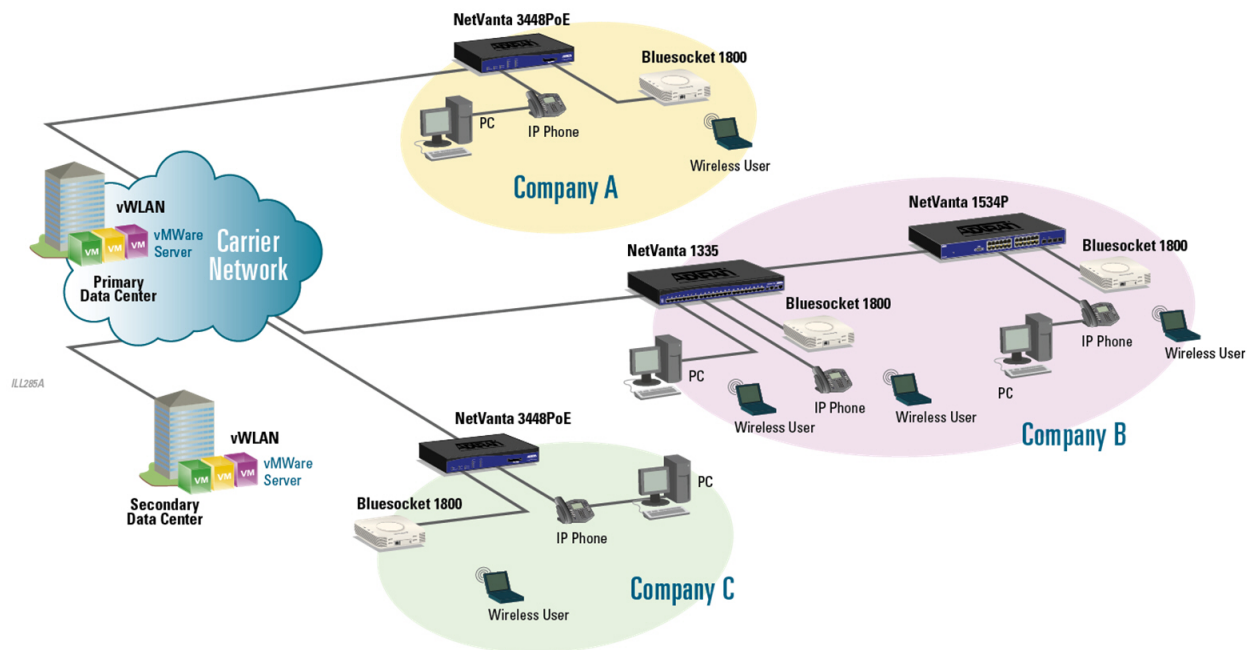


Figure 4: Small to Medium Business Hosted and Managed Solution



BSAP Models Supported by vWLAN 4.5.0

vWLAN 4.5.0 supports these BSAP models:

- BSAP 1920/1925
- BSAP 1930/1935
- BSAP 1940
- BSAP 2020
- BSAP 2030/2035
- BSAP 2135
- BSAP 3040/3045
- BSAP 6020
- BSAP 6040
- BSAP 6120



vWLAN 4.5.0 does not support BSAP 1800 series and earlier.

Chapter 2

Introduction to the vWLAN GUI

After you install the vWLAN and an associated AP, you can begin configuring the vWLAN and AP parameters.



See the *BSAP vWLAN Configuration Guide* for information about vWLAN requirements and the steps to install your vWLAN.

You can access the vWLAN GUI 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. The default administrative user name is **root@adtran.com**, and the default password is **blueblue**



Sign in

Username

Password

[Forgot your password?](#)

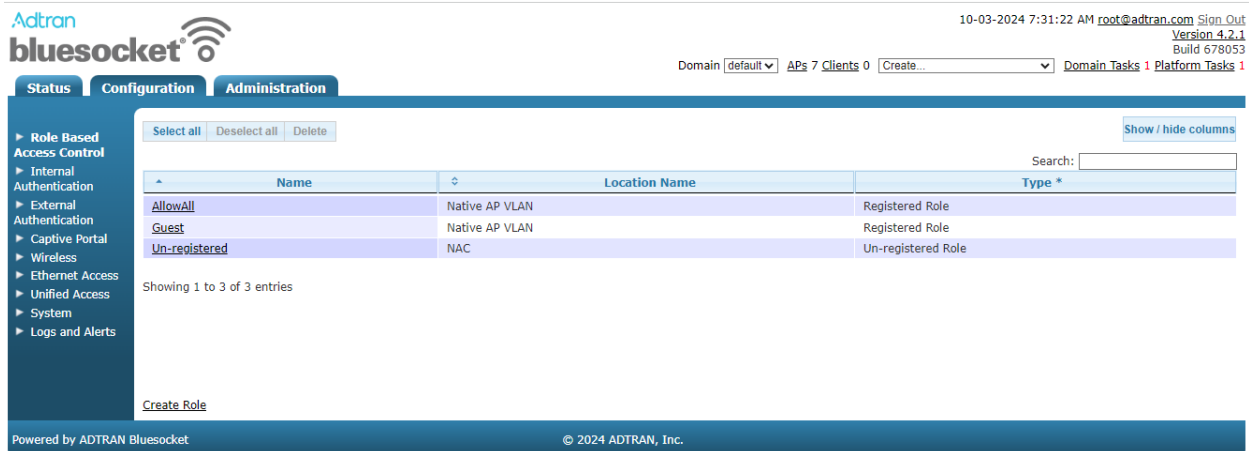
Powered by ADTRAN Bluesocket

These sections summarize the vWLAN GUI and its built-in web server used for system management:

vWLAN Menu Structure	28
General GUI Shortcuts	29
Additional GUI Options	29

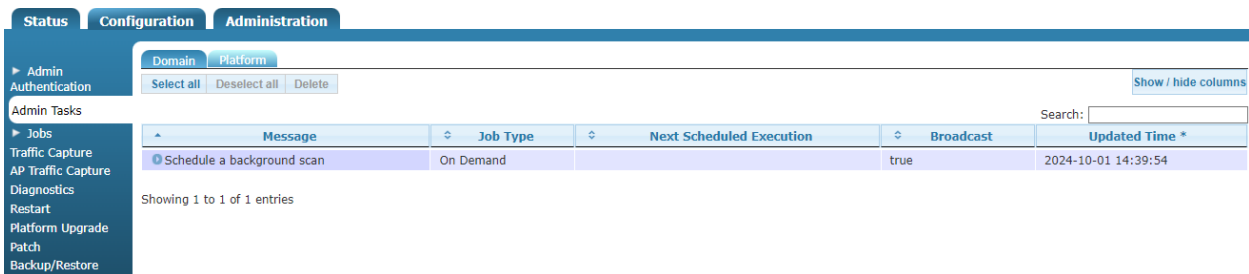
vWLAN Menu Structure

In the vWLAN GUI, 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: **Status**, **Configuration**, and **Administration**. This illustration depicts the vWLAN GUI layout.



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

In addition, you might see a **Platform** or **Domain** tab associated with a menu option, if you logged in as an administrator with 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 displays administrative tasks related to a domain, and the **Platform** tab displays administrative tasks related to the vWLAN platform only.



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** 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 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** 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** 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 (see [Specifying the Administrator Role](#)).

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, 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 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.

Domain		Platform		Show / hide columns	
				Search: <input type="text"/>	
^	Name	Value *	↕	Hint	
	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.	
	AP Control Channel Timeout	86400		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).	
	DHCP Lease Time for Un-registered Clients	10		An aggressive lease time brings clients on faster after authentication, but may not be compatible with all handheld devices.	
	Display Setup Wizard	Disabled		Enables setup wizard.	
	Flush Client Scan Data Interval	7		Range accepted from 0-30(In days), 0 means no data will be flushed out	
	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.	
	Time in minutes between updating internal status (minimum 5)	5		Updates client stats.	
	Time in seconds before inactive connections are dropped	600		Inactive connections will be dropped once this time out has been reached.	

Showing 1 to 10 of 10 entries

Chapter 3

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 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 these topics:

Creating an Administrator	31
Changing the Administrator Password	34
Specifying the Administrator Role	34
Specifying Administrator Authentication	36

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 has full administrative privileges of the platform and all domains.



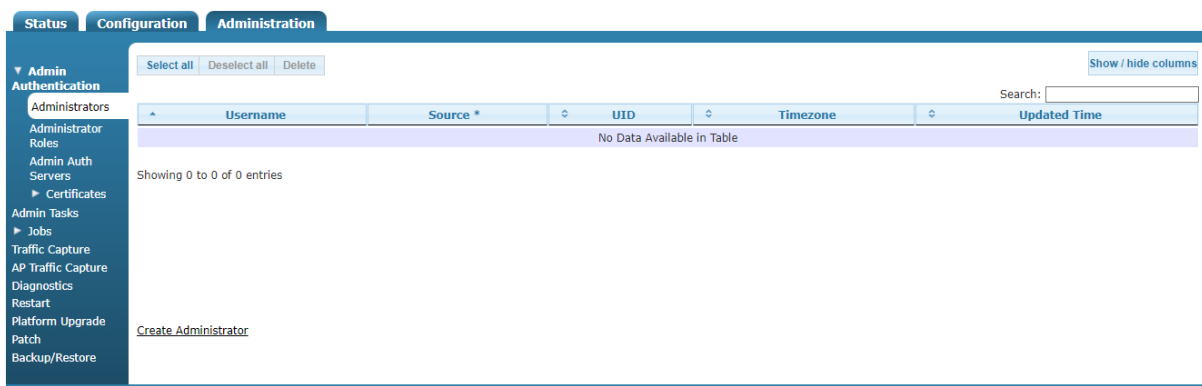
You cannot change the administrative scope or role of the default platform administrator, or delete the default platform administrator. You can, however, change the user name, email address, password, and time zone for the default platform by selecting **root@adtran.com** (or the default platform administrator 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 might 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 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.

Except the default platform administrator, you can configure all administrators from the **Configuration** tab menu. To create an administrator:

1. Navigate to **Administration > Admin Authentication > Administrators**.



2. Select **Platform Administrator** (whether creating a platform or domain administrator) from the **Create** menu at the top of the GUI, 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 time zone from the menu. Then specify the administrator scope. The administrator scope consists of the administrator 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** menu (if selecting domain permissions), or select **Platform** from the **Domain** menu if selecting platform permissions. Each administrator account, including the platform administrator, must have permissions for at least one domain.
4. Specify the administrator role (or permissions) by selecting the appropriate option from the **Admin Role** field. 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 field. See [Specifying the Administrator Role](#) for more information about creating custom roles.



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.



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

5. Click **Create Administrator** after specifying the administrator email, password, time zone, and scope.

Create Administrator

Email

Password

Password Confirmation

Timezone ▼

Administrator Scopes

Domain	Admin Role	
▼	▼	remove
▼	▼	remove
▼	▼	remove

[Add more domains](#)

[Back](#)

You will receive confirmation that the new administrator was 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 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 configuration.

Changing the Administrator Password

When first logging into the vWLAN, you will be prompted to change the default platform administrator 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 **Administration > Admin Authentication > Administrators**. To change an administrator (other than the default platform administrator) password:

1. Navigate to **Administration > Admin Authentication > Administrators**. Select the administrator you want to edit from the list. You must have write permissions to complete this action.
2. Enter the new password in the **Password** field. Confirm the new password.
3. Click **Update Administrator** to save the configuration.
You will receive confirmation that the changes were successfully applied.

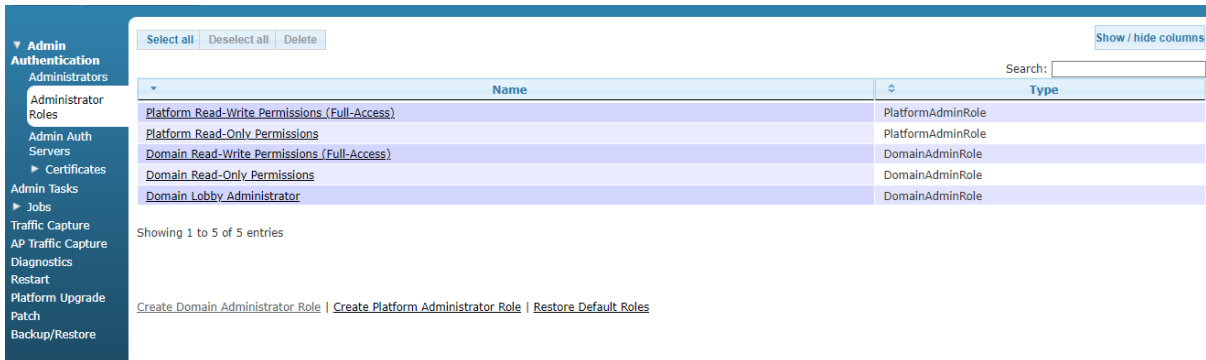
Specifying the Administrator Role

The administrator 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 domains to which they are assigned.
- **Domain Read-Only Permissions** option allows administrators read-only permissions for the domains 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.

To create a custom role or edit an existing role:

1. Navigate to **Administration > Admin Authentication > Administrator Roles**. This menu lists the five default roles. 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. Enter the name of the role in the **Name** field if you create a new role. Then select the appropriate permissions for the role by selecting the **Read, Update, Create, Destroy, None, or All** field next to the action for which you configure permission. **None** indicates no permissions are given, and **destroy** indicates delete permissions are given. If you edit a role, make your changes using the same process. Action selections will vary based on whether you configure a platform or domain administrator role.

Create Administrator Role

Name

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

Resources	None	Read	Update	Create	Destroy	All
Select All		<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"/>	<input type="checkbox"/>
AP Templates	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
AP Traffic Captures	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Access Point Jobs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Access Point Statuses	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Access Points	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Accounting Servers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Active User Statuses	<input type="checkbox"/>	<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"/>	<input type="checkbox"/>
Alarms	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Available AP Firmware	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Branding	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Client Certificates	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dashboard Tabs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dashboard Widgets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Destination Groups	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Destinations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Devices	<input type="checkbox"/>	<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"/>	<input type="checkbox"/>

3. Click **Create Admin Role** or **Edit Admin Role** to apply the changes. The new or updated administrator role is now displayed in the **Administrator Roles** menu. You can associate the administrator role with new or existing administrators. See [Creating an Administrator](#).



Roles are not domain specific, so the same role can be used in multiple domains.



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 was created (as described in [Creating an Administrator](#)), 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.



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.

This section contains these topics:

RADIUS Administrator Authentication Considerations	37
Configuring RADIUS Administrator Authentication	37

RADIUS Administrator Authentication Considerations

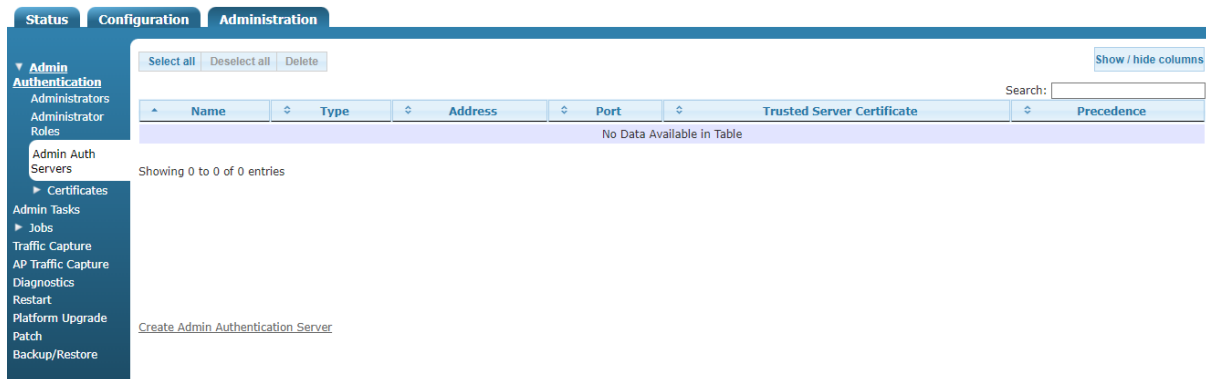
When you use RADIUS authentication for administrators, you should keep these items in mind when you configure the vWLAN network:

- 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:

1. Navigate to **Administration > Admin Authentication > Admin Auth Servers**. If you want to edit a previously configured RADIUS server, select the appropriate server from the list. If you create a new RADIUS server for administrator authentication, either select **Platform Admin Authentication Server** from the **Create** field on top of the vWLAN menu, or select **Create Admin Authentication Server** from the **Admin Auth Servers** menu.



2. Configure the server by specifying the servers name, IP address, port, shared secret/password (and confirmation) in the appropriate fields. Ensure that each IP address is unique for each server you create.

Create Authentication Server

Type:

Name:

IP Address:

Port:

Shared Secret/Password:

Shared Secret/Password Confirmation:

Timeout:
Enter time in seconds between retries.

Retries:
Enter RADIUS protocol retry count (0 = no retries).

Precedence:

Authentication Rules

Administrator:

Attribute	Operator	CompareTo	Administrator
<input type="text" value="ARAP-Challenge-Response"/>	<input type="text" value="equal to"/>	<input type="text"/>	<input type="text"/>
<input type="text" value="ARAP-Challenge-Response"/>	<input type="text" value="equal to"/>	<input type="text"/>	<input type="text"/>
<input type="text" value="ARAP-Challenge-Response"/>	<input type="text" value="equal to"/>	<input type="text"/>	<input type="text"/>
<input type="text" value="ARAP-Challenge-Response"/>	<input type="text" value="equal to"/>	<input type="text"/>	<input type="text"/>
<input type="text" value="ARAP-Challenge-Response"/>	<input type="text" value="equal to"/>	<input type="text"/>	<input type="text"/>

[Append Admin Auth Rule](#)

[Back](#)

3. 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.
4. 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 list. 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.
5. Specify the administrator to which this RADIUS authentication applies by selecting the appropriate administrator from the **Administrator** field.

6. Specify the RADIUS attributes that are associated with the administrator by selecting the appropriate RADIUS attribute from the left menu and the appropriate administrator from the right menu. You can arrange the order of these attributes by dragging and dropping the attributes within the list. Click **Create Admin Authentication Server** or **Update Admin Authentication Server** to apply the configuration.

After the configuration is applied, the new or updated server appears in the **Admin Auth Servers** list.

Chapter 4

vWLAN Platform Configuration

This chapter discusses the configuration of vWLAN as it applies to the platform. An administrator with full access to the platform completes this configuration, while users with platform read permissions can view this configuration. Areas discussed in this section include:

Configuring the vWLAN Network Interfaces	40
Configuring a vWLAN Network Interface Static Route	42
Changing the Administrator Session Idle Timeout	44
Configuring the Platform SNMP Parameters	44
Configuring the vWLAN TLS 1.0 Setting	45
Configuring vWLAN Platform Branding	46
Verifying the vWLAN Software Version	47
Performing System Maintenance	48
Restarting the vWLAN	55
Configuring High Availability	55
Working with Certificates	59

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. The platform administrator configures network interfaces. You can configure the public network interface 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. You can use the private network interface 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. You cannot configure the private network interface as a DHCP client.

To configure a network interface:

1. Navigate to **Configuration > System > Network Interfaces**. This menu lists the default configured public and private network interfaces. To configure one of these interfaces, select the interface from the list.

Name	DHCP *	Address *	Netmask *	Gateway *
private	Disabled	10.251.252.1	255.255.255.0	
public	Disabled	10.49.182.201	255.255.255.0	10.49.182.254

Showing 1 to 2 of 2 entries

After editing a network interface, an admin task will be created to signify that the vWLAN should be restarted. Click on the admin tasks link on the top bar to go to the admin task page and restart the network. This might impact all users on the vWLAN, so be careful when changing the settings.

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

Edit Network Interface

Name: private

Address:

Netmask:

Static Routes

Static routes manipulate the vWLAN's IP routing table. Their primary use is to set up static routes to specific hosts or networks via an interface.

The parameters that apply to the static routes are:

- Destination: Target destination network or host. You can provide IP addresses in dotted decimal.
- Netmask: For a host route, specify a netmask of 255.255.255.255.
- Gateway: Route packets via a gateway. NOTE: The specified gateway must be reachable first and the gateway needs to be on the same subnet as the interface.

Destination	Netmask	Gateway	
<input type="text" value="destination"/>	<input type="text" value="netmask"/>	<input type="text" value="gateway"/>	
<input type="text" value="destination"/>	<input type="text" value="netmask"/>	<input type="text" value="gateway"/>	
<input type="text" value="destination"/>	<input type="text" value="netmask"/>	<input type="text" value="gateway"/>	

[Append Static Route](#)

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

- For the public interface, specify whether DHCP is enabled by selecting the **DHCP** field. 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. Click **Update Network Interface** to apply the changes.

Edit Network Interface

Name public

Current Address 10.49.182.201

Current Netmask 255.255.255.0

Current Gateway 10.49.182.254

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

Static Routes

Static routes manipulate the vWLAN's IP routing table. Their primary use is to set up static routes to specific hosts or networks via an interface.

The parameters that apply to the static routes are:

- Destination: Target destination network or host. You can provide IP addresses in dotted decimal.
- Netmask: For a host route, specify a netmask of 255.255.255.255.
- Gateway: Route packets via a gateway. NOTE: The specified gateway must be reachable first and the gateway needs to be on the same subnet as the interface.

Destination	Netmask	Gateway	
<input type="text" value="destination"/>	<input type="text" value="netmask"/>	<input type="text" value="gateway"/>	
<input type="text" value="destination"/>	<input type="text" value="netmask"/>	<input type="text" value="gateway"/>	
<input type="text" value="destination"/>	<input type="text" value="netmask"/>	<input type="text" value="gateway"/>	

[Append Static Route](#)

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

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 high availability configurations.

To configure a static route to connect to vWLAN remotely,

- Navigate to **Configuration > 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.

[Status](#) | [Configuration](#) | [Administration](#)
[Show / hide columns](#)

Name	DHCP *	Address *	Netmask *	Gateway *
private	Disabled	10.251.252.1	255.255.255.0	
public	Disabled	10.49.182.201	255.255.255.0	10.49.182.254

Showing 1 to 2 of 2 entries

After editing a network interface, an admin task will be created to signify that the vWLAN should be restarted. Click on the admin tasks link on the top bar to go to the admin task page and restart the network. This might impact all users on the vWLAN, so be careful when changing the settings.

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

Edit Network Interface

Name: private

Address:

Netmask:

Static Routes

Static routes manipulate the vWLAN's IP routing table. Their primary use is to set up static routes to specific hosts or networks via an interface.

The parameters that apply to the static routes are:

- Destination: Target destination network or host. You can provide IP addresses in dotted decimal.
- Netmask: For a host route, specify a netmask of 255.255.255.255.
- Gateway: Route packets via a gateway. NOTE: The specified gateway must be reachable first and the gateway needs to be on the same subnet as the interface.

Destination	Netmask	Gateway	
<input type="text" value="destination"/>	<input type="text" value="netmask"/>	<input type="text" value="gateway"/>	
<input type="text" value="destination"/>	<input type="text" value="netmask"/>	<input type="text" value="gateway"/>	
<input type="text" value="destination"/>	<input type="text" value="netmask"/>	<input type="text" value="gateway"/>	

[Append Static Route](#)

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

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.

To change the administrator session idle timeout:

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

The screenshot shows the vWLAN configuration interface. The left sidebar contains a navigation menu with categories like Role Based Access Control, Internal Authentication, External Authentication, Captive Portal, Wireless, Ethernet Access, Unified Access, System, Network, Interfaces, Domains, Settings, Branding, Storage Settings, High Availability, Mosaic Mission Control, and Logs and Alerts. The main content area is titled 'Platform' and displays a table of settings. The 'Administrator Session Idle Timeout' setting is highlighted, showing a value of 30. The table has columns for Name, Value, and Hint. Other settings include Certificate 1, Certificate 2, Certificate Chain 1, Certificate Chain 2, Certificate Private Key 1, Certificate Private Key 2, Certificate Selected, Certificate Signature Request 1 (CSR), Certificate Signature Request 2 (CSR 2), Enable SNMP?, and 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?	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.

Showing 1 to 26 of 26 entries

3. Specify the idle timeout for administrative console sessions. Valid entries are 15 to 300 minutes or 0 for no timeout. Click **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](#)

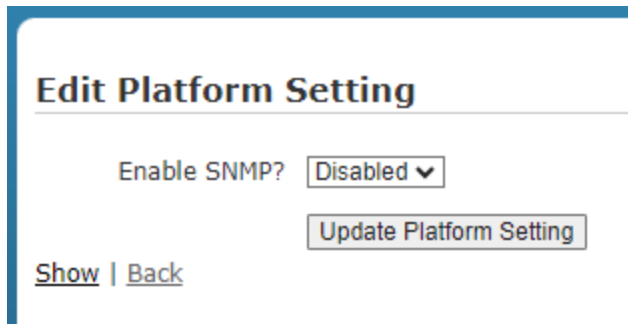
Configuring the Platform SNMP Parameters

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. You can configure SNMP parameters from the platform administrator menu. vWLAN supports SNMPv2c. By default, SNMP is disabled on vWLAN for polling from external network management

stations. Standard MIB-2 polling is supported. Vendor-specific MIBs are available online at www.adtran.com. You can configure SNMP polling on a vWLAN platform-wide basis and SNMP traps on a per-domain basis. The next sections describe platform-wide SNMP polling configuration. For more information about per-domain SNMP trap configuration, see [Configuring Domain Settings](#).

To configure SNMP polling at the platform level in vWLAN:

1. Navigate to **Configuration** > **System** > **Settings**, and then select the **Platform** tab.
2. Select the task item labeled **Enable SNMP?**.
3. Select **Enabled** from the **Enable SNMP?** field to enable SNMP and select **Update Platform Setting**. You will receive confirmation acknowledging that the changes were made.



The screenshot shows a web interface titled "Edit Platform Setting". It features a dropdown menu for "Enable SNMP?" currently set to "Disabled". Below the dropdown is a button labeled "Update Platform Setting". At the bottom left, there are two links: "Show" and "Back".

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 using these steps:

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

3. Select **Enabled** from the **Enable TLS 1.0** field to enable TLS 1.0 support, and then select **Update Platform Setting**.



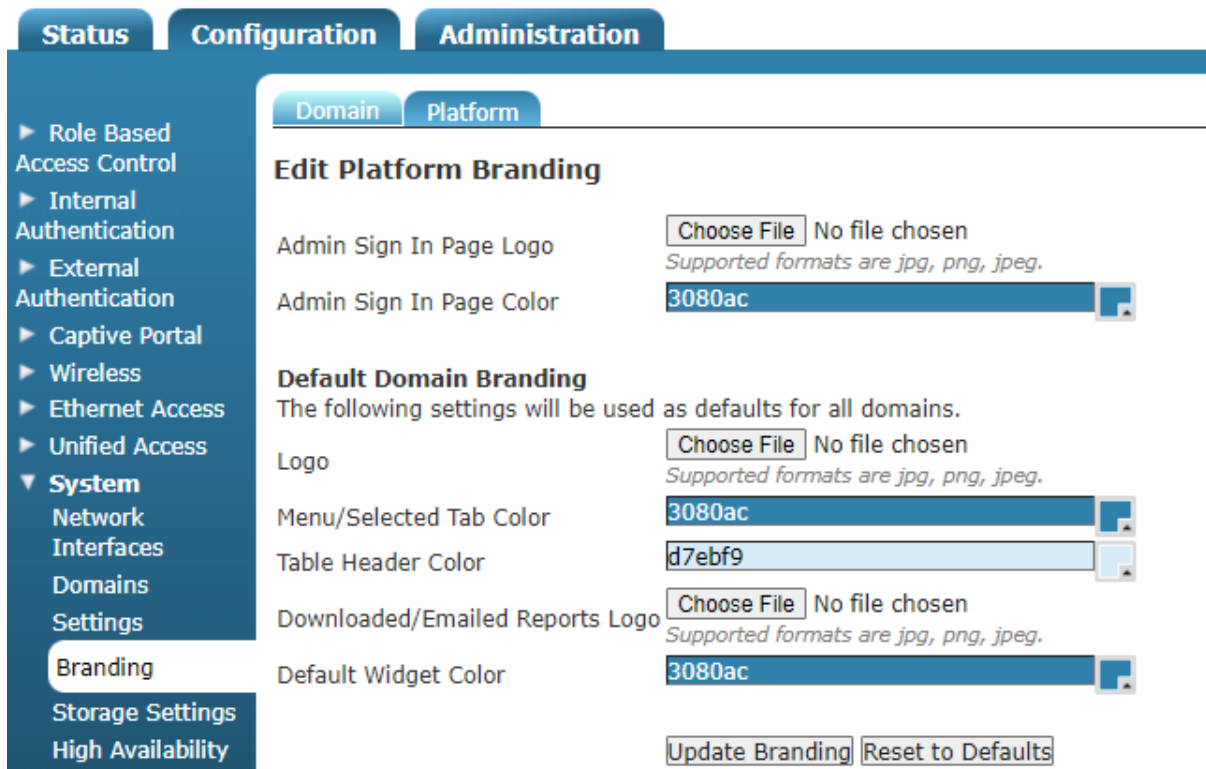
You will receive notification that a **Platform Task** was created to restart vWLAN and apply the setting changes. See [Administrative Tasks](#) for more information about platform tasks.

Configuring vWLAN Platform Branding

In vWLAN release 2.9.0, the option to brand the administrator sign in page on the vWLAN platform was added. This feature allows you to add logos or change the colors of the administrator 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:

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



2. In the **Edit Platform Branding** menu, add any logos to the administrator 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 sign in page by selecting a color in the **Admin Sign In**

Page Color field.

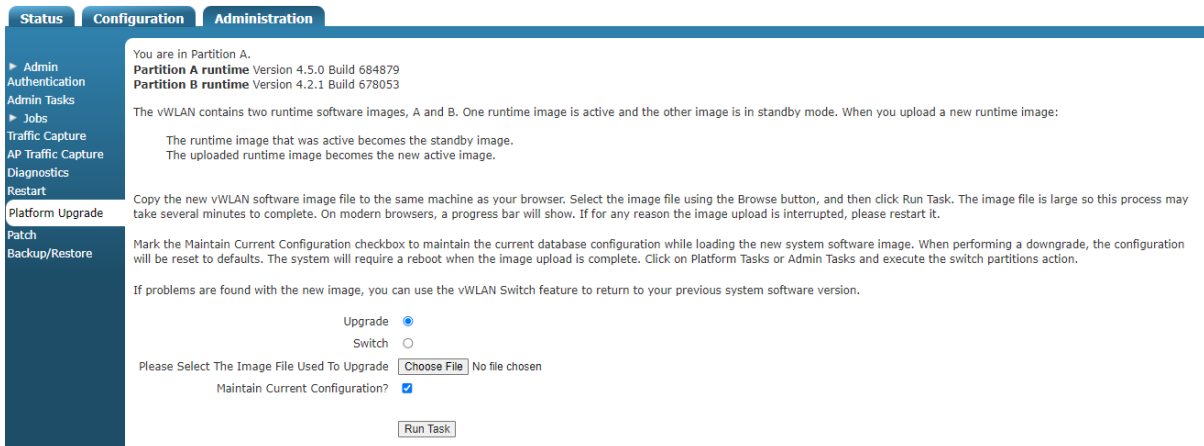
- Specify the default branding settings for any domains that are created by uploading your own logo for the domain login page or for downloaded or emailed reports. Supported file formats are **.jpg**, **.png**, or **.jpeg**. Domain logo file sizes are 265 pixels (width) by 60 pixels (height).
- Specify the default colors for domain menus, tables, and widgets by selecting the appropriate colors in the menu, table, or widget fields.
- 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:

- Navigate to **Administration > Platform Upgrade**.



The screenshot shows the 'Administration' tab selected in the top navigation bar. The left sidebar contains a menu with 'Platform Upgrade' highlighted. The main content area displays the following information:

- You are in Partition A.
- Partition A runtime Version 4.5.0 Build 684879
- Partition B runtime Version 4.2.1 Build 678053

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 Run Task. 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 Platform Tasks or 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.

Upgrade
 Switch

Please Select The Image File Used To Upgrade No file chosen

Maintain Current Configuration?

- Verify the partition the vWLAN is currently using (**A** or **B**), and view the current vWLAN software version. In the preceding example, the vWLAN software version is **4.5.0**.



You might need to verify any patches that you installed, as well as the vWLAN software version. To verify installed patches, see [Managing Patches](#). 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. vWLAN instances installed in VMware do not have a serial number.

Performing System Maintenance

The platform administrator performs general system maintenance, which 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. You can access these tasks by navigating to the **Administration** tab in the top of the menu.

The system management tasks are described in these sections:

System Restart	49
Configuring Backup or Restore Parameters	50
Using Show Tech for Technical Support	51
Managing the vWLAN Runtime Image	52
Managing Patches	54

System Restart

Some vWLAN configuration tasks, such as restoring defaults, require a system restart.

To restart the vWLAN system:

1. Navigate to **Administration > Restart**.



2. Select the appropriate item to restart from the list in the restart menu by selecting the field next to the item you want to restart. 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 click **Run Restart**.

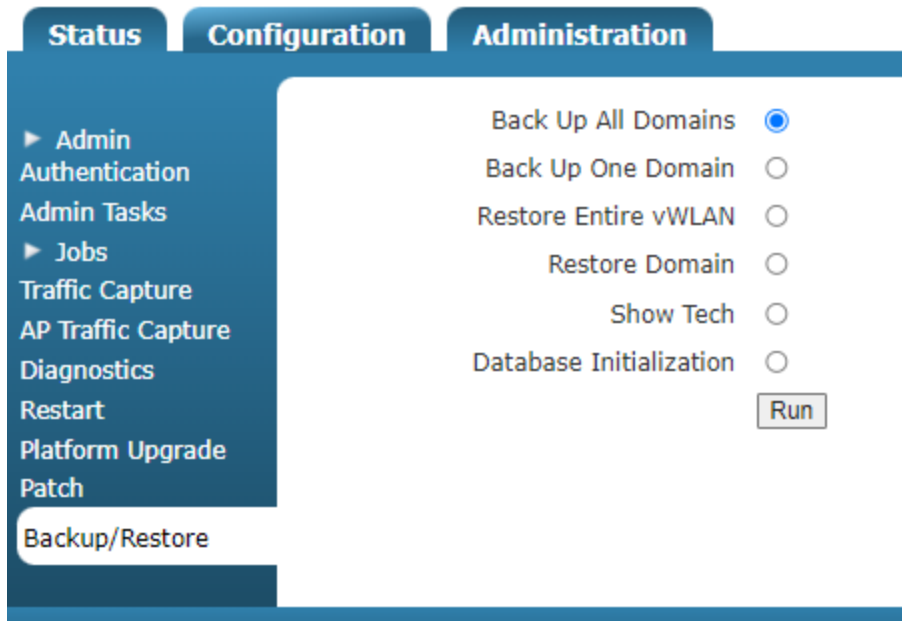


Typically you should rely upon notifications from the **Admin Tasks** list in the GUI when tasks such as a restart should be completed. For example, when you install a patch, a **Platform Task** is created to alert you that you need to reboot.

Configuring Backup or Restore Parameters

You can back up the vWLAN system and restore it from a saved backup or to the default settings. To perform a backup or restore:

1. Navigate to **Administration > Backup/Restore**.



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



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 back up 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.

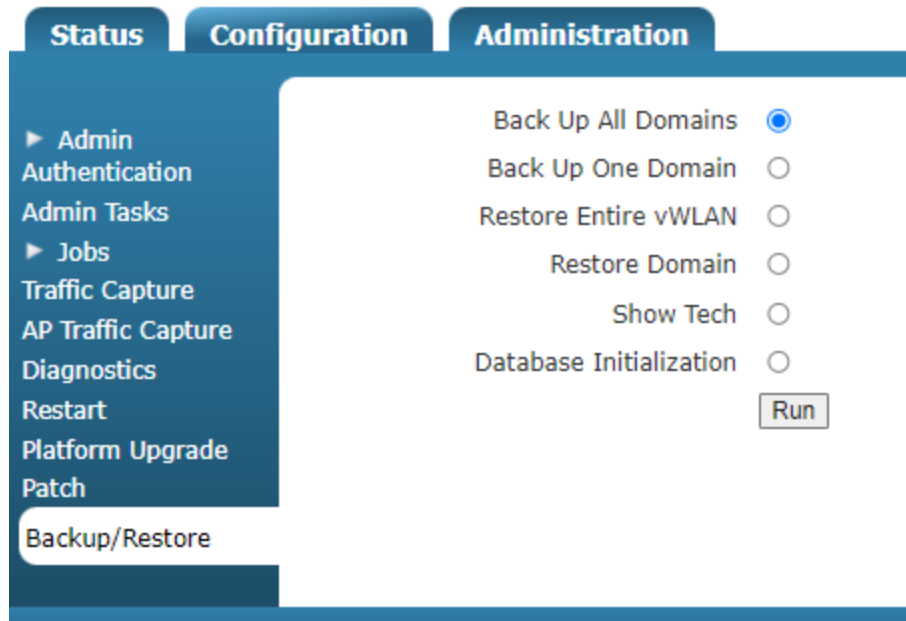


Restoring a configuration removes all existing vWLAN configuration. The IP address remains the same, so you can access the box after a configuration restoration.

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 **Administration > Backup/Restore**. Select **Show Tech** from the list, and then click **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 you upload 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:

1. Navigate to **Administration > Platform Upgrade**.

The screenshot shows the vWLAN GUI with the following content:

- Navigation:** Status, Configuration, Administration (selected).
- Left Menu:** Admin, Authentication, Admin Tasks, Jobs, Traffic Capture, AP Traffic Capture, Diagnostics, Restart, Platform Upgrade (selected), Patch, Backup/Restore.
- Main Content:**
 - You are in Partition A.
 - Partition A runtime Version 4.5.0 Build 684879
 - Partition B runtime Version 4.2.1 Build 678053
 - 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 Run Task. 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 Platform Tasks or 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.
 - Upgrade (selected)
 - Switch
 - Please Select The Image File Used To Upgrade No file chosen
 - Maintain Current Configuration?
 -

2. Select the **Upgrade** field, and then click **Choose File** to retrieve the appropriate software image from the correct location. Make sure to select the **Maintain Current Configuration** field. This feature allows you to maintain the current database configuration while loading the new system software image.



You can find software images online from the Adtran website.

3. Click **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). Once the upgrade is complete, you must reboot the vWLAN system.
4. Navigate to **Administration > Restart**. Select **Reboot vWLAN**, and then click **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. See [Administrative Tasks](#).

To switch between an active runtime image and another previously loaded runtime image:

1. Navigate to **Administration > Platform Upgrade**.
2. Select **Switch**, and select the **Partition** you want to use. You can verify the partition you are using, and its current firmware, by viewing the partition information on this menu.
3. Click **Run Task**.
Once the task is complete, you must reboot the vWLAN system.
4. Select **Admin Tasks** and select the reboot task from the task list (see [Administrative Tasks](#)), or navigate to **Administration > Restart**, and then select **Reboot vWLAN**. Next, click **Run Restart** to reboot the appliance and switch partitions.

Managing Patches

From time to time, vWLAN software patches are released. You can upload these patches into vWLAN by the platform administrator and use them to ensure that your vWLAN network runs at optimal performance and has the latest feature set.



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:

1. Navigate to **Administration** > **Patch**.

The screenshot shows the Administration menu with 'Patch' selected. The main content area displays the 'Select Patch To Upload' section with a 'Choose File' button and 'No file chosen' text. Below this is an 'Install' button. The 'Patch List' section shows two entries, each with a radio button and a 'Delete' button:

- Package name: 4.5-0-p01, Version: 4-5-0-684879
- Package name: callhomesupport, Version: 4-5-0-684879

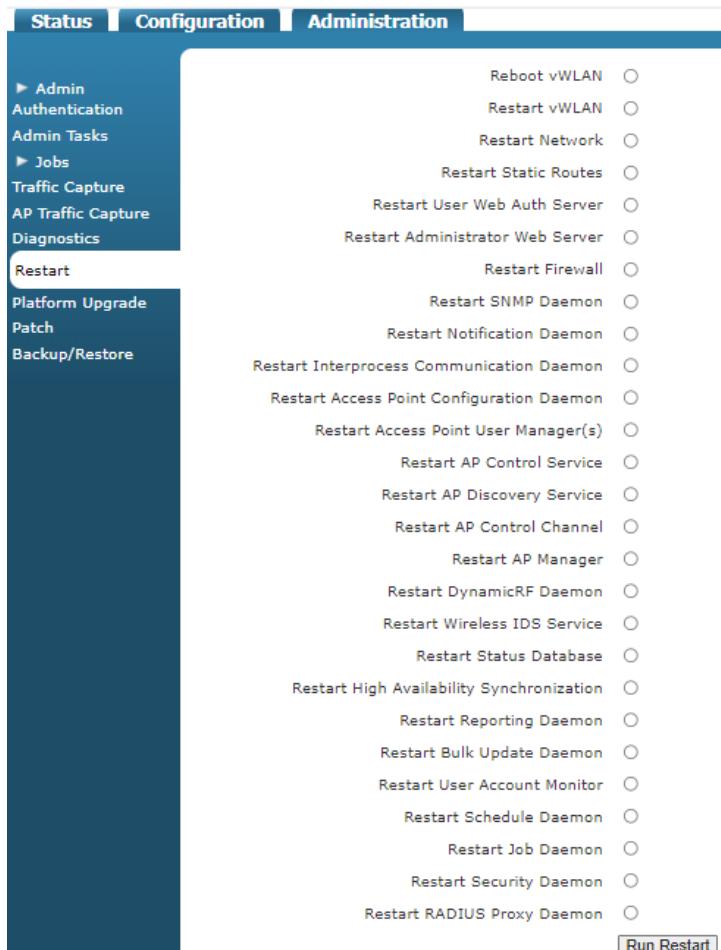
2. Select the patch to install using **Choose File**. You can download patches from the [Product Downloads](#) page.
3. Select **Install**.

Any patches that you installed are listed in the **Patch List**. A **Platform Task** might display, if a reboot or restart is required. You can also uninstall patches from this page.

Restarting the vWLAN

Restarting the vWLAN is often necessary after you restore the vWLAN to the default settings, change runtime images, or make significant configuration changes. To restart the vWLAN:

1. Navigate to **Administration > Restart**.
2. Select **Restart vWLAN** from the menu, and then click **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.

This section contains these sections:

High Availability Process	56
Replicating Master Configuration Changes on the Node	58

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 these states:

- **Discovery** indicates that the AP boots and attempts to find the vWLAN.
- **Connected to Primary** indicates that 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 that 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. See [Configuring Domain Settings](#) 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 you cannot make any configuration changes. 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, you must restore the configuration 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 vWLANs, 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 fallback to the master system on the node system.

To configure high availability:

1. Navigate to **Configuration** > **System** > **High Availability**. By default, the vWLAN system is set to **Standalone** replication mode.
2. Select a **Replication Mode** of the vWLAN system. Select **Master** if this is the primary system or **Node** if this is a secondary system.

The screenshot displays the 'Edit Replication Node' configuration page. The left sidebar shows the navigation menu with 'High Availability' selected under the 'System' category. The main content area contains the following fields and options:

- Replication Mode:** A dropdown menu set to 'Master'.
- Replication Node:** An empty text input field.
- Replication Password:** An empty text input field.
- AP Keepalive Interval:** A text input field containing the value '3'.
- AP Keepalive Retries:** A text input field containing the value '3'.
- Auto Failback to Master:** A checked checkbox.

Below the configuration fields is a section titled 'Status With Master' with the following information:

- Last Message Sent: None
- Last Message Received: None
- Last API Log ID: None

At the bottom of the form, there is an 'Update Replication Node' button and a note: 'To take a 'snapshot' on the replication node, click 'Update Replication Node'.'

3. 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 if you configure a master system. 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. Select **Auto Failback to Master** to enable the AP to automatically return to the primary vWLAN system once it becomes available.
4. Click **Update Replication Node** to apply the changes. A confirmation message (**Replication Node was successfully updated**) displays to indicate that the changes were made. After you configure the master vWLAN system, you must configure the secondary vWLAN system.

5. Navigate to **Configuration > System > High Availability** in the secondary vWLAN system. Select **Node** from the **Replication Mode** field. Enter the public network interface IP address of the primary (master) system in the **Replication Master** field, and then enter the shared password between the systems in the **Replication Password** field. This password should match the one used when you configure 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 Master

Last Message Sent None

Last Message Received None

Last API Log ID None

[Update Replication Node](#)

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



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

6. Click **Update Replication Node** to apply the changes. A confirmation message (**Replication Node was successfully updated**) is displayed to indicate the changes were 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 (see [Replicating Master Configuration Changes on the Node](#)).

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](#).

Working with Certificates

When vWLAN communicates with an LDAP server, you can use SSL 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). You can configure multiple certificates on vWLAN to aid in certificate renewal.



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

This section contains these topics:

Installing Certificates to vWLAN	59
Uploading Certificates to vWLAN	61
Configuring Additional vWLAN Settings for Certificates	62
Managing vWLAN Certificate Settings	66
Managing LDAP Certificates for vWLAN	67

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 list of trusted root certificate authorities and Bluesocket is not a CA. You can avoid these errors by either installing the self-signed certificate on each client in the browser 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 list of trusted root CAs.

To install new SSL certificates on vWLAN:

1. Begin by generating a certificate signing request (CSR) in vWLAN. Navigate to **Configuration > System > Settings**, and then select the **Platform** tab. Select the **Certificate Signature Request 1 (CSR)** item from 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.

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

- 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 name (spelling out symbols or leaving them out), your organizational unit 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 then select the key bit length. Keys can be **2048** or **1024** bits in length, although most CAs require a minimum of **2048** bits. Click **Update Platform Setting** after you entered the information.

Certificate 1 Request

Country Name
2 letter code

State or Province Name
Full name

Locality Name
e.g. city

Organization Name
e.g. company

Organizational Unit Name
e.g. section

Fully Qualified Domain Name
e.g. bsc1.yourcompany.com

Email Address

An Optional Company Name

Key Bit Length

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

The public and private keys for certificate enrollment are created. The public key, in the form of a CSR, is displayed. You can use this for certificate enrollment. The private key is stored locally on the vWLAN under **Configuration > System > Settings > Platform > Certificate Private Key 1**.

- Copy and paste the entire text of the CSR into the appropriate space on your CA enrollment form. Select **apache mod ssl** or **apache** as the server platform on your CA enrollment form and complete any remaining steps required by the CA. This completes the CSR request.
- Back up the private key by downloading it to a safe location. Navigate to **Configuration > System > Settings**, select the **Platform** tab, and then 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**.

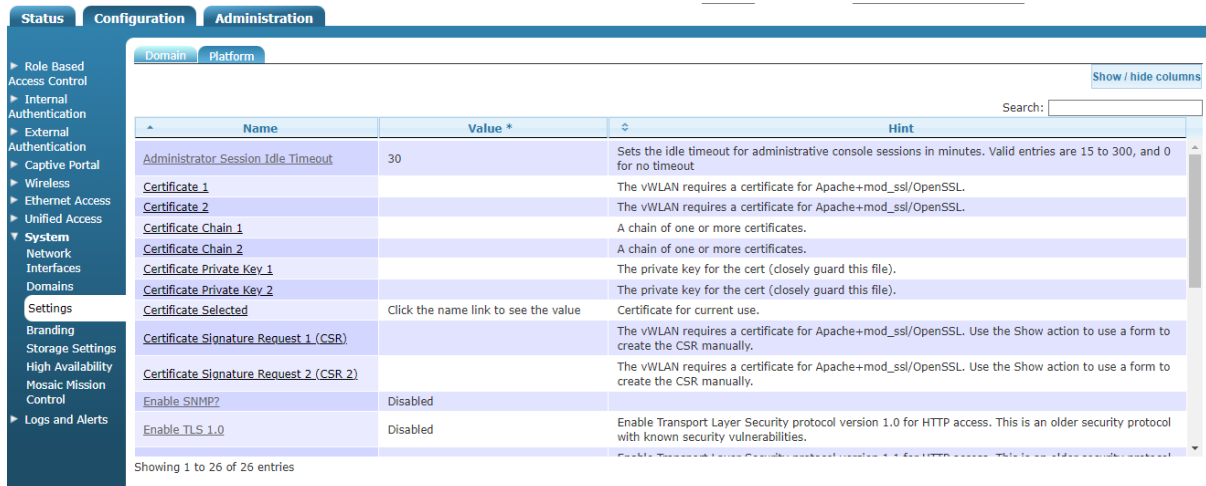
After you complete the CSR, the CA will send you the certificate or instructions to obtain the certificate. Some CAs send the certificate in text format, while others might send it in a certificate file with an extension such as .cer, .crt, or .pem. Once you received the certificate, upload it to vWLAN.

- 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:

- Navigate to **Configuration > System > Settings**, and then select the **Platform** tab. For a certificate upload, select **Certificate 1** or **Certificate 2** depending on whether you upload the first or second certificate.



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?	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.

- Copy and paste the text of the certificate into the **Certificate 1** or **Certificate 2** field. Click **Update Platform Settings** to add the certificate.
- Select **Certificate Chain 1** or **Certificate Chain 2** from the **System > Settings** menu to add certificate chains using this method.
- 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.



If you 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. See *BSAP vWLAN CLI Reference Guide* for more information.

Configuring Additional vWLAN Settings for Certificates

In addition to installing and uploading certificates to vWLAN, you must configure additional items in vWLAN for proper certificate function. These items include adding a new host record and associated pointer to your organization 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:

1. 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 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. After you verified the names match, test the forward and reverse DNS entry using the **nslookup** command from the command prompt of a client. Ensure that the client uses the same DNS server as configured on the public network interface of the vWLAN.
2. In vWLAN, navigate to **Configuration > System > Settings**, and then select **Platform**. In this menu, select the **Redirect to hostname** item. This will allow you to enable host name redirection.

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 SNMP2	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.

Showing 1 to 26 of 26 entries

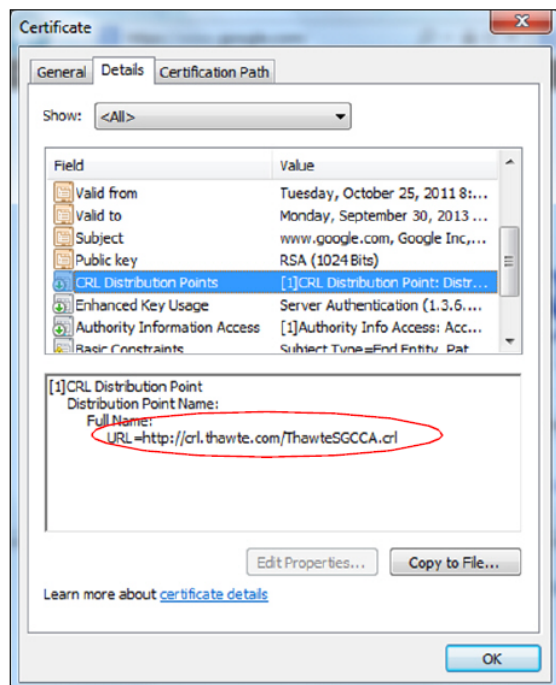
3. Select **Enabled** from the **Redirect To Hostname** field. This will redirect users to the host name (rather than the public network interface IP address). Click **Update Platform Setting**.

Edit Platform Setting

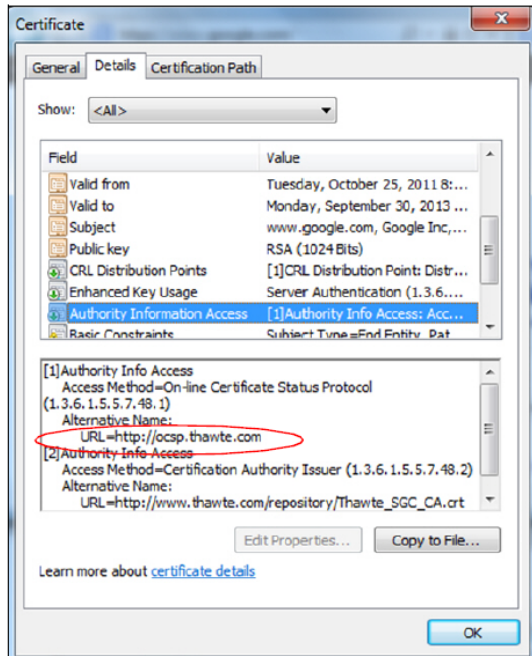
Redirect To Hostname

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

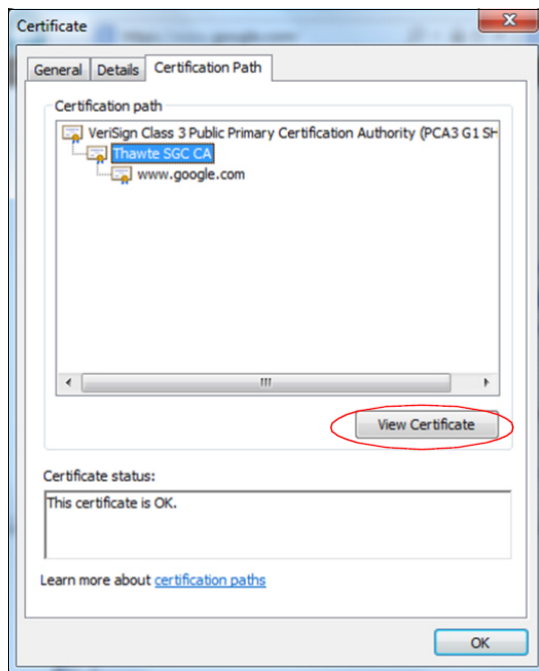
4. Select **Platform Tasks** at the top of the GUI to apply the changes to the vWLAN system. This will take you to the **Administration** tab, **Admin Tasks** menu, and the **Platform** tab. Select the play icon next to **Must restart User Web Server** to restart the web server. Clients will temporarily lose access captive portal, but the connected clients will not be disconnected. 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. You can use these URLs to check the validity of the certificate. Some browsers will not redirect to the login page if they cannot validate the certificate.
5. To find the URLs associated with your certificate, select the certificate from **Configuration > Settings > Platform**. Then, click **Show**. The OCSP and CRL values are displayed along with other certificate information. Alternatively, select the lock icon on the address bar in the web browser and select **View Certificates** while on the login page of the vWLAN GUI.
6. 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.



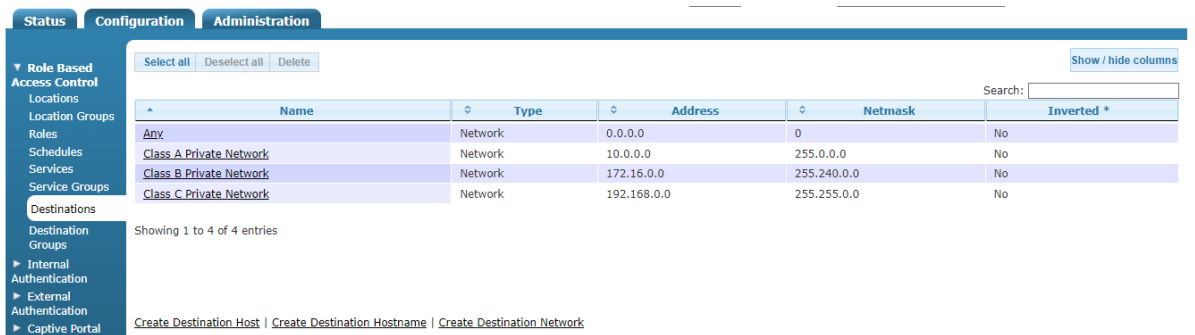
7. In the same **Certificate** menu, on the **Details** tab, select **Authority Information Access** in the **Field** menu. The OCSP URL is displayed in the detail pane. Depending on your certificate, you might have one, both, or neither of these fields, but if you do have them, you should allow HTTP traffic to them from the vWLAN.



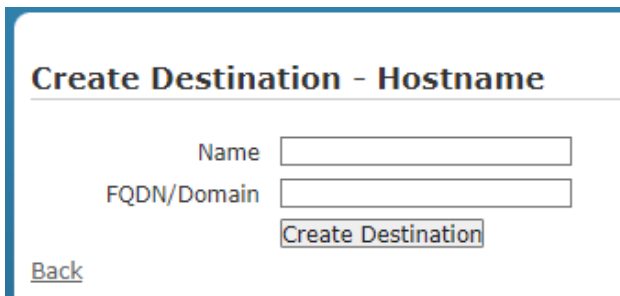
8. Repeat this process for all certificates in the chain. To ensure you have the information for all certificates in the chain, select the **Certification Path** tab in the **Certificate** menu. Select the next certificate up in the certification path and select **View Certificate**. Repeat Steps 6 and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



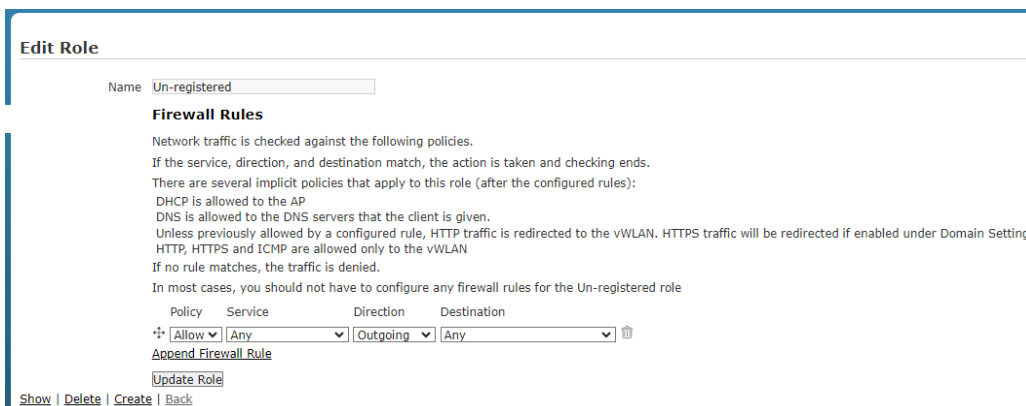
- After you gathered all the URLs for all of the certificates in the chain, navigate to **Configuration > Role Based Access Control > Destinations**. Select **Create Destination Hostname** at the bottom of the menu.



- In the new menu, specify the name for the destination host name, and enter the URL in the **FQDN/Domain** field. Click **Create Destination**. Repeat this step until all the URLs are added. You can use wildcards to specify the destination host name. Acceptable formats are ***.domain.com** or **domain.com**.



- 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 click **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 (see [Administrative Tasks](#) for more information).



Managing vWLAN Certificate Settings

You can use the vWLAN certificate 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:

1. Navigate to **Configuration > System > Settings**. In the **Platform** tab, you will find a summarized list of all the available platform settings. The administrator can configure these settings. 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
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 SNMP2	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.

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.

2. 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 click **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](#)

You can also delete certificate chains, certificates, and keys 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 click **Update Platform Settings**.

Managing LDAP Certificates for vWLAN

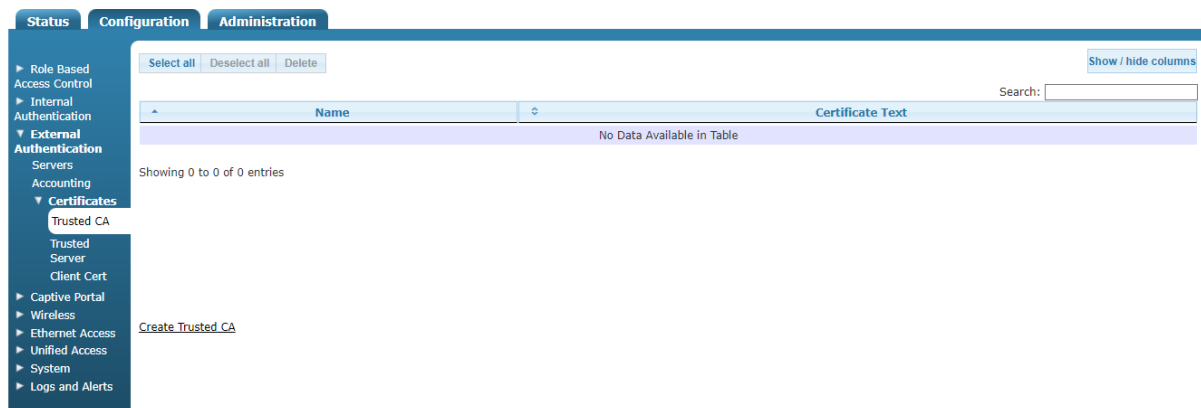
When certificates are manually uploaded to vWLAN, the certificates are then relayed back to the LDAP authentication server in a one-to-many relationship. For example, you can trust more than one CA in a chain, but each LDAP server can only have one trusted server certificate and one client certificate. 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.

Uploading Trusted LDAP CA to vWLAN	67
Uploading Trusted LDAP Server Certificate to vWLAN	68
Uploading Trusted LDAP Client Certificate to vWLAN	69

Uploading Trusted LDAP CA to vWLAN

To upload a trusted LDAP CA to vWLAN:

1. Navigate to **Configuration > 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** menu at the top of the GUI.



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

3. Click **Create Trusted CA**. The created CA is now available for editing or deletion, and will appear in the Trusted CA list under **Configuration > External Authentication > Certificates > Trusted CA**.

Uploading Trusted LDAP Server Certificate to vWLAN

To upload a trusted LDAP server certificate to vWLAN:

1. Navigate to **Configuration > 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** menu at the top of the GUI.

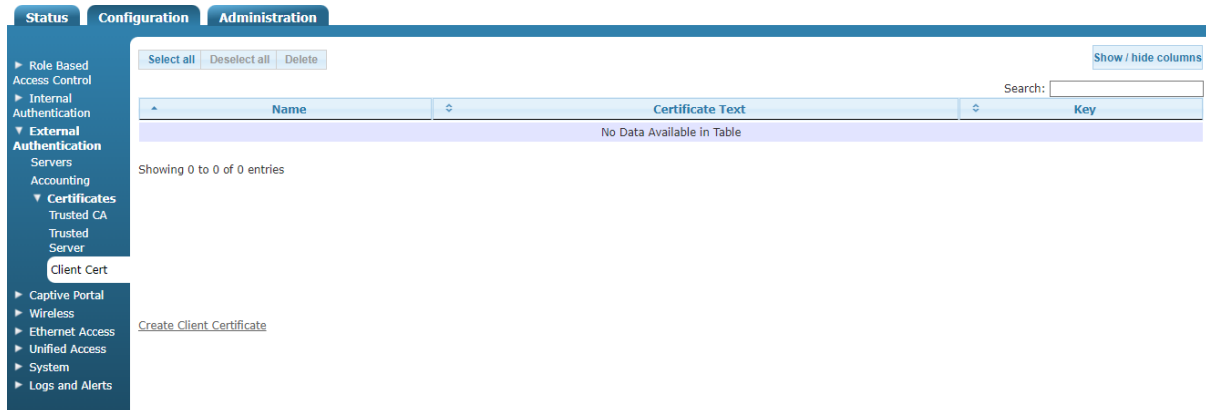
2. Enter the name for the server certificate in the **Name** field, and enter the certificate text in the **Certificate text** field.

3. Click **Create Trusted Server Certificate**. The created server certificate is now available for editing or deletion, and will appear in the trusted server list under **Configuration > External Authentication > Certificates > Trusted Server**.

Uploading Trusted LDAP Client Certificate to vWLAN

To upload a trusted LDAP client certificate to vWLAN:

1. Navigate to **Configuration > 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** menu at the top of the GUI.



2. Enter the name for the certificate in the **Name** field, enter the certificate text in the **Certificate text** field, and enter the key information for the certificate in the **Key** field.
3. Click **Create Client Certificate**. The created client certificate is now available for editing or deletion, and will appear in the client certificate list under **Configuration > External Authentication > Certificates > Client Cert**). An error is generated if the key and certificate do not match.

Chapter 5

vWLAN Domain Configuration

Domains are separate management domain partitions within the vWLAN instance that you can use to subdivide the vWLAN management. The platform administrator initially creates domains and assigns a domain administrator to manage each domain. Creating domains includes creating the domain in vWLAN and optionally associating one or more other administrators to the domain. After domains were 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. This chapter describes these tasks:

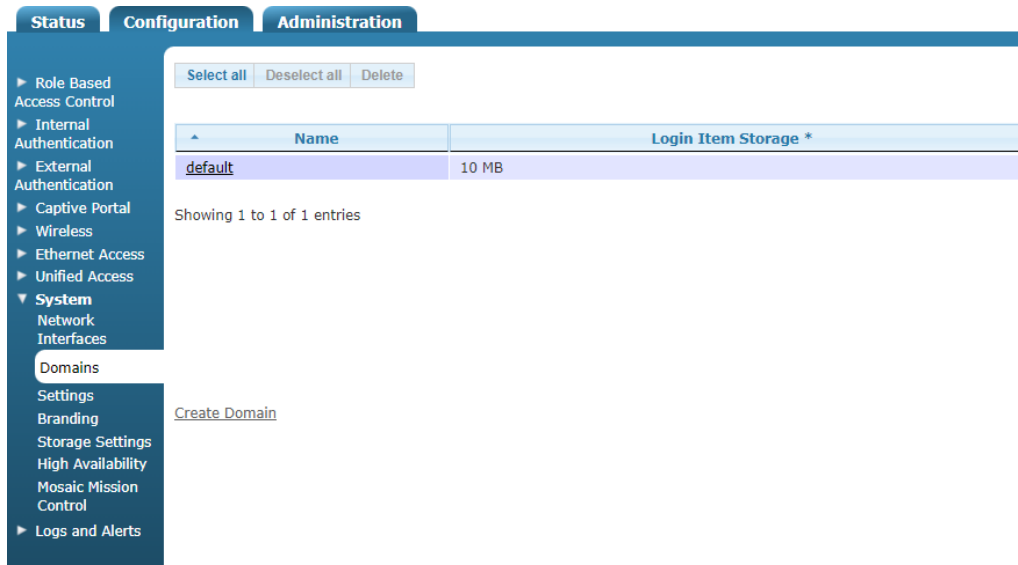
Creating the Domain	71
Associating Administrators to a Domain	72
Configuring Domain Destinations	73
Creating Domain Destination Groups	74
Configuring Domain Services	76
Creating Domain Service Groups	77
Configuring Domain Locations	78
Configuring Domain Location Groups	79
Configuring Domain Roles	80
Configuring Domain Role Schedules	87
Configuring Web-based (Captive Portal) Authentication	88
Configuring Domain Accounting	107
Configuring Domain Settings	109
Configuring Domain Users	112
Configuring Domain Branding	114
Domain Configuration Backup	115

Creating the Domain

Platform administrators or administrators with platform read and write permissions configure domains and domain administrators. See [Specifying the Administrator Role](#) for more information.

To create a domain:

1. Navigate to **Configuration > System > Domains**. Or, you can select **Platform > Domain** from the **Create** menu at the top of the GUI.



2. 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 (see [Managing Domain Storage Settings](#) for more information). If the storage setting was 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.

The screenshot shows the 'Create Domain' form. It has the following fields and elements:

- Name**: A text input field.
- Maximum Storage For Login Items**: A field with a value of '10' and 'MB' units.
- Create Domain**: A button.
- Back**: A link.

3. Click **Create Domain**. You will receive confirmation acknowledging the domain was created.

After you created the domain, you can view, edit, or delete the domain from **Configuration > System > Domains**. You can create an administrator for the domain if not already exist or you want a different administrator. You can begin configuring the specifics of the domain. See [Creating an Administrator](#) or [Configuring Domain Destinations](#) for more information.

Associating Administrators to a Domain

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



You must have platform read and write permissions to associate an administrator with a domain. See [Specifying the Administrator Role](#) for more information.

To associate an administrator with a domain:

1. Navigate to **Administration > Admin Authentication > Administrators**.

The screenshot shows the 'Administration' tab selected in the top navigation bar. The left sidebar is expanded to 'Admin Authentication' > 'Administrators'. The main content area displays a table with the following columns: Username, Source, UID, Timezone, and Updated Time. The table is currently empty, with the message 'No Data Available in Table' centered below the column headers. Above the table, there are buttons for 'Select all', 'Deselect all', and 'Delete', and a 'Show / hide columns' link. Below the table, there is a 'Showing 0 to 0 of 0 entries' message and a 'Create Administrator' link.

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

3. Select the domain you want to associate with this administrator by selecting the domain from the **Domain** field. In addition, make sure to select the appropriate administrator role from the **Admin Role** field.

Edit Administrator

Email

Password

Password Confirmation

Timezone

Administrator Scopes

Domain	Admin Role	
<input style="width: 50px;" type="text" value="default"/>	<input style="width: 150px;" type="text" value="Domain Read-Only Permissions"/>	remove
Add more domains		
<input type="button" value="Update Administrator"/>		

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

4. Click **Update Administrator**. A confirmation is displayed when the action is complete.

Configuring Domain Destinations

You can use domain destinations to specify which networks are accessible from a single domain. Use destination locations to specify which networks are available to roaming clients and users and which are not. When you configure a domain destination, you will specify the destination host name, IP address, or network mask in the GUI. You can group destinations, so they use the same network resources (see [Creating Domain Destination Groups](#) for more information). After you create a domain, you must use a role to allow or deny it. See [Configuring Domain Roles](#) for more information.

To configure a domain destination:

1. Verify that you are in the correct domain administrative menu by selecting the appropriate domain from the **Domain** menu at the top of the GUI.
2. Navigate to **Configuration > Role Based Access Control > Destinations**.

Status Configuration Administration

▼ Role Based Access Control

- Locations
- Location Groups
- Roles
- Schedules
- Services
- Service Groups
- Destinations
- Destination Groups
- ▶ Internal Authentication
- ▶ External Authentication
- ▶ Captive Portal

Select all Deselect all Delete [Show / hide columns](#)

Search:

Name	Type	Address	Netmask	Inverted *
Any	Network	0.0.0.0	0	No
Class A Private Network	Network	10.0.0.0	255.0.0.0	No
Class B Private Network	Network	172.16.0.0	255.240.0.0	No
Class C Private Network	Network	192.168.0.0	255.255.0.0	No

Showing 1 to 4 of 4 entries

[Create Destination Host](#) | [Create Destination Hostname](#) | [Create Destination Network](#)

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** menu at the top of the GUI. You can optionally choose to select **Domain Destination Hostname** or **Domain Destination Network** from the **Create** menu to create the same destination.
4. Enter the name of the destination and the destination IP address in the appropriate fields. The destination 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 create this destination from the **Destination Hostname** selection, you will be prompted for the same information in the **New Hostname** menu.

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 create 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.

Create Destination - Host

Name

Address

Invert

Invert means all destinations except this destination

[Back](#)

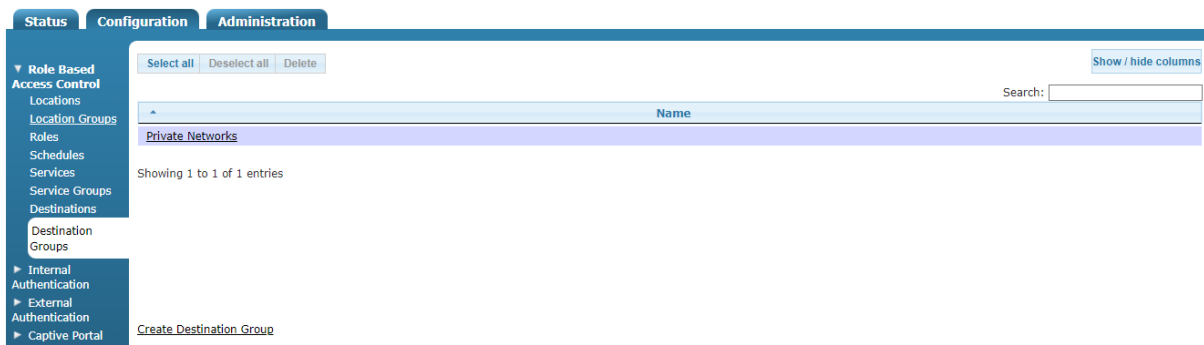
5. Click **Create Destination**. A confirmation is displayed indicating the destination was created. The new destination will now appear in the list of destinations displayed in the **Configuration > Role Based Access Control > Destinations** menu, where you can choose to display, edit, or delete the destination.

Once you created the destination, associate it with a role to enable access. See [Configuring Domain Roles](#).

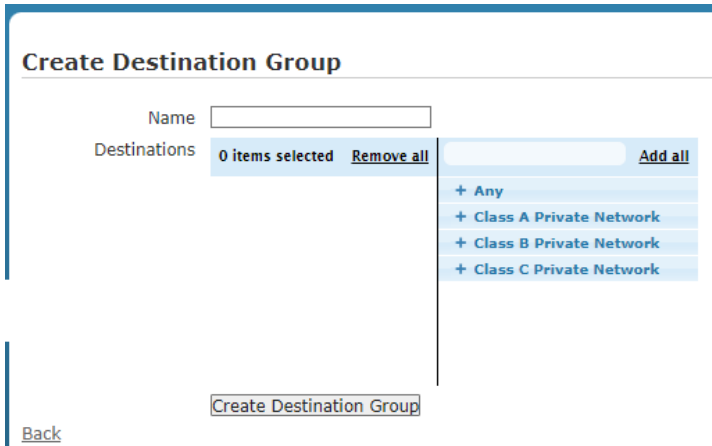
Creating Domain Destination Groups

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:

1. Navigate to **Configuration > Role Based Access Control > Destination Groups**. This menu lists the previously configured destination groups. 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** menu at the top of the GUI.



- Specify the name of the destination group, and add destinations to the group from the list.



- Click **Create Destination Group**. A confirmation is displayed indicating that the group was created. The group will now appear in the group list under **Configuration > Role Based Access Control > Destination Groups**, where you can display, edit, or delete the group. After you created the destination group, associate it with a role to enable access. See [Configuring Domain Roles](#) 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, and so on. You can also group services, like destinations, which makes it easier to assign a set of services to a user role. Configured domain services are listed under **Configuration > Role Based Access Control > Services**.

To configure a domain service:

1. Navigate to **Configuration > Role Based Access Control > Services**.

Name	Port	Notes
AH	0	
Any	0	
DHCP	67	
DHCP-Server	68	
DNS	53	
ENCAP	0	
ESP	0	
HTTP	80	
HTTPS	443	
ICMP	0	
IMAP	143	
IPv6-Nonxt	0	
KERBEROS	88	
LDAP	389	
MPLS-in-IP	0	

Showing 1 to 29 of 29 entries

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** menu at the top of the GUI.
4. Enter the name of the service in the required field, and select the appropriate protocol from the **Protocol** field. 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 want to displayed in the configured services list.

Create Service

Name

Protocol

Notes

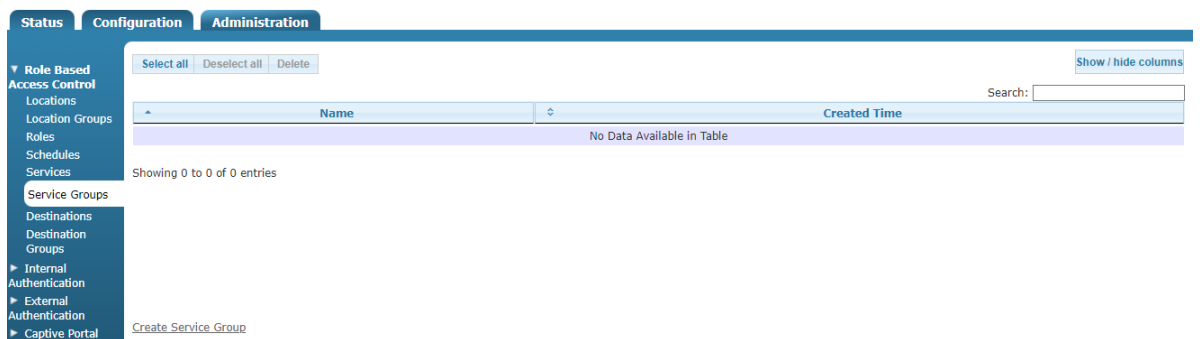
[Back](#)

5. Select **Create Service**. A confirmation appears indicating the service was created. The service will now appear in the list of configured services under **Configuration > Role Based Access Control > Services**, where you can display, edit, or delete the service.
Once you created the domain service, associate it with a role. See [Configuring Domain Roles](#) for more information.

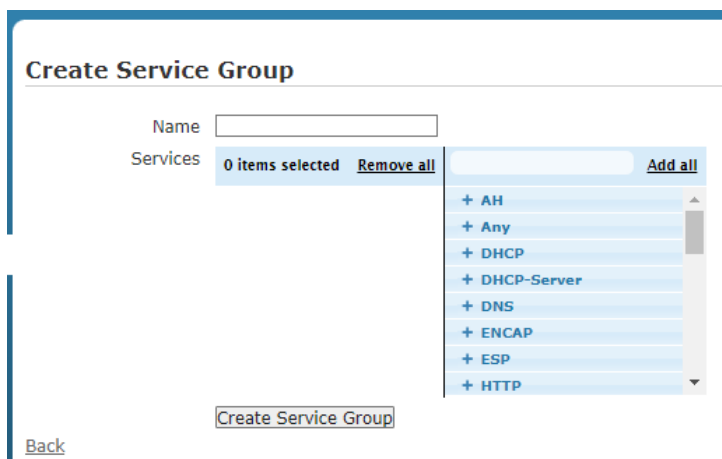
Creating Domain Service Groups

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:

1. Navigate to **Configuration > Role Based Access Control > Service Groups**. This menu lists any previously configured service groups. 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** menu at the top of the GUI.



2. Specify the name of the service group in the appropriate field, and add services to the group by selecting the plus sign next to the service.



3. Select **Create Service Group**. A confirmation is displayed indicating that the group was 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 created the service group, apply it to a role. See [Configuring Domain Roles](#) 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. You can use the NAC domain location 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 you can edit to any class A, B, or C private network with a /14 subnet mask. When a user connects to vWLAN, the user role determines the user location (VLAN, subnet, network mask), which encompasses the AP native VLAN/location, a static location, or a location group.

The user role determines a user location. 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 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 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 does not already exist, the vWLAN creates a location in the GUI. You can map user roles 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.

To create a domain location:

1. Navigate to **Configuration > Role Based Access Control > Locations**. This menu lists any previously configured locations. 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** menu at the top of the GUI.

Name	VLAN	CIDR
178	178	10.49.178.0/24
192	192	10.49.192.0/24
198	198	10.49.198.0/24
NAC	1	10.252.0.0/14
vLoc-0-10.49.191.0/24	0	10.49.191.0/24
vLoc-0-10.49.192.0/24	0	10.49.192.0/24

Showing 1 to 6 of 6 entries

[Create Location](#)

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 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 was created. The location will now appear in the locations list under **Configuration > Role Based Access Control > Locations**, where you can display, edit, or delete the location.

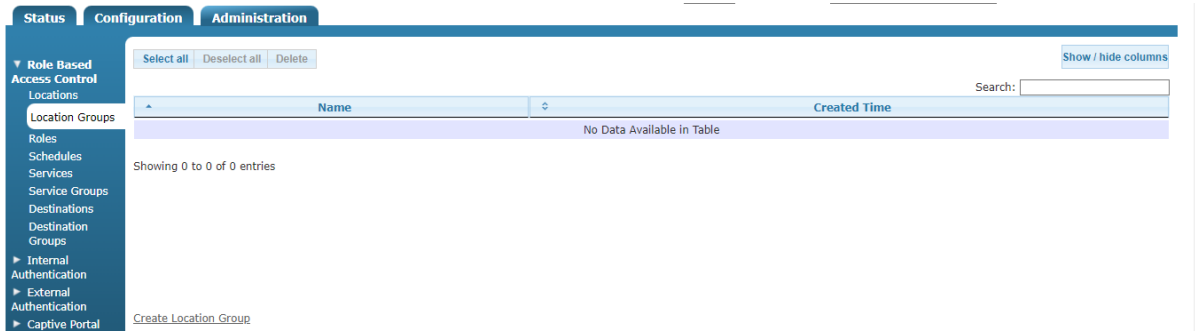
Configuring Domain Location Groups

In large scale deployments of vWLAN, you can assign multiple subnets 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.

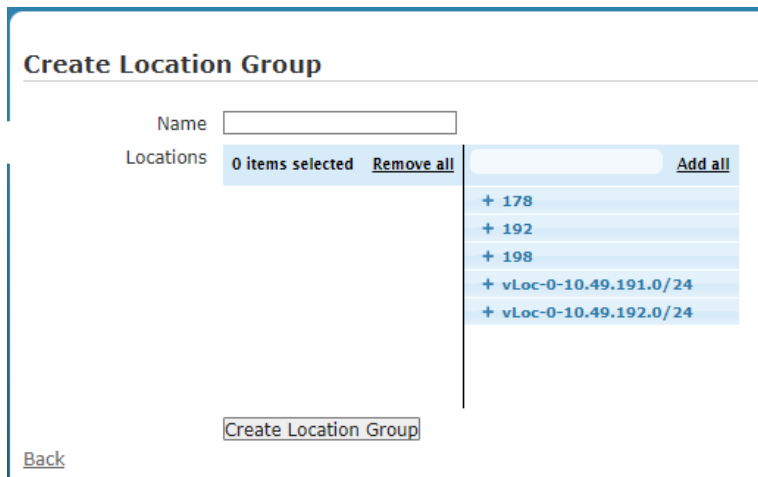
To create a domain location group:

1. Navigate to **Configuration > Role Based Access Control > Location Groups**. This menu lists any previously configured location groups. 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** menu at the top of the GUI.



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



A confirmation is displayed indicating that the group was created. The group will now appear in the group list under **Configuration > 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 system places a user in a role based on these 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

- The default role from the SSID, unless the SSID is 802.1X, then the role from the RADIUS 1X server is used.
- If the role remains un-registered at this point, the user can use web-based authentication to log in to any role.

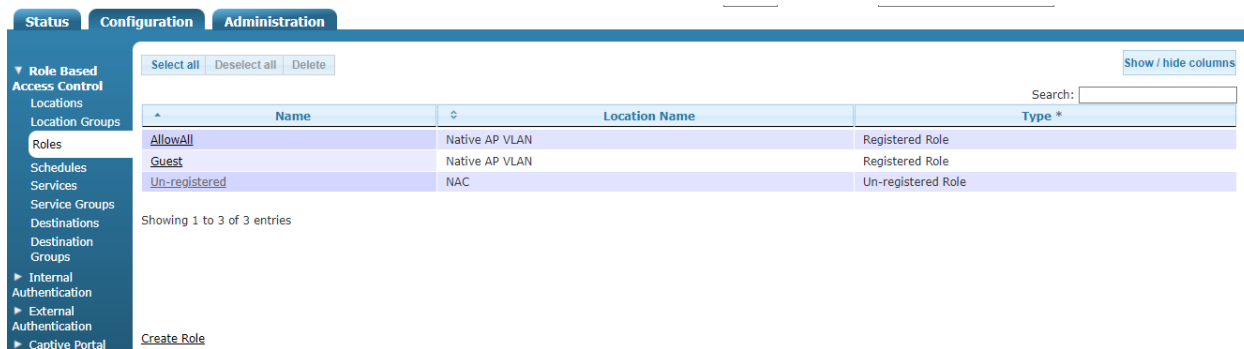
By default, when a user connects for the first time and was not authenticated, the user role is un-registered.

When you configure a user role, it is important to realize that the user role determines where and how the client 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**.



There can be interactions between a tunnel profile and a defined user role. See [Configuring a Tunnel Profile](#) for more information.

To create un-registered and registered roles, navigate to **Configuration > Role Based Access Control > Roles**. This menu lists any previously configured domain roles. 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** menu at the top of the GUI.



The Create Role page displays. The configuration options on this page change depending on the selected role type:

- Un-Registered Role Type 81
- Walled Garden 82
- Registered Role Type 83

Un-Registered Role Type

You can use the default **Un-registered** role type with the location set as NAC, which is available on the Roles page. To configure the un-registered role type with a non NAC server location, which is used when you configure the Walled Garden feature:

- On the Create Role page, enter a name for the un-registered role and select **Un-registered Role** from the **Type** field.

Create Role

Name

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

Location **178** ▼
Cannot configure vWLAN location and Native AP Vlan location for Un-registered roles.

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 (Note: Do not configure DNS server in the same subnet as the location selected for the unregistered role type).
 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

[Append Firewall Rule](#)
[Create Role](#)

[Back](#)

2. Select the location associated with the role from the **Location** field.
3. Specify any firewall rules needed. In most cases you do not have to configure any firewall rules for the un-registered role.
4. Click **Create Role**.

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).

To configure the Walled Garden feature:

1. Configure the location of the network that will serve the IP addresses. See [Configuring Domain Locations](#).
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 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 **178** ▼
Cannot configure vWLAN location and Native AP Vlan location for Un-registered roles.

Locations

178

192

Walled Garden-1

LocationGroups

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):

3. Add a firewall rule that allows DNS traffic outbound.
4. Create another domain role and specify **Registered Role** for **Type** and select the name of the domain that you created in Step 1 for the **Location**.



Make sure that the domain location of the registered role is the same domain location as the un-registered role for the Walled Garden feature to work properly.

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

Registered Role Type

The registered role type specifies the parameters for a client after they were authenticated. These steps outline the options available when you configure a registered role:

1. Enter the name of the role in the appropriate field.

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 **Native AP VLAN**

Machine Authentication Enforcement

Allow Client To Client
Allows Client to Client traffic on the same AP.

Class of Service

CoS Priority In Override **DSCP**
What to prioritize Wireless based on.

CoS Priority Out Override **No Remark**
What to remark Wired based on.

Bandwidth Shaping

QoS Rate In **0.0** **Kbits/second**
Bandwidth Limit in Incoming/Downstream (AP to Client) direction. Set to zero for no bandwidth limit.

QoS Rate Out **0.0** **Kbits/second**
Bandwidth Limit in Outgoing/Upstream (Client to AP) direction. Set to zero for no bandwidth limit.

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.

2. Select **Registered Role** from the role **Type**. If applicable, select any associated schedule from the **Schedule** field. The schedule specifies when clients can or cannot access the network. See [Configuring Domain Role Schedules](#) for more information about schedule configuration.
3. Select the location associated with this role from the **Location** field.
4. 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 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. This allows group policies to be applied and login scripts to execute when the user logs in and allows users who do not have locally cached profiles on the domain computer to login. You can also place a valid 802.1X user without a valid device 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. You can configure vWLAN 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** field. Once you 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 field.

5. Select **Allow Client To Client** if you want to allow client-to-client traffic on the AP. The firewall policy must also allow the traffic for client-to-client traffic to flow.

6. Configure the CoS options. Specify the packet prioritization parameters for the role.

The CoS priority override parameters specify on what criteria this user role traffic is prioritized for incoming (wireless) traffic and how packets are remarked in outgoing (wired) traffic. You can use it 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.

To specify the prioritization of the input wired packets for the user role, select the appropriate value from the **CoS Priority In Override** field:

- **DSCP**: prioritization of traffic within the Ethernet and wireless driver based on the IP packet 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. Use it 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.

If you specify a **Static** value, select the appropriate priority from the **CoS Priority In** field.

Specify the CoS packet remarking behavior for the user role. The AP applies packet remarking in the outgoing or upstream (wireless to wired) direction. Remarkings are 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** field. By default, this value is set to **No Remark**. If you specify a **Static** value, select the appropriate priority from the **CoS Priority Out** field.



The **CoS Priority In** and **CoS Priority Out** fields are only available if you selected **Static** for the **CoS Priority In Override** or **CoS Priority Out Override** values.

- 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. You can limit bandwidth 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.



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 list. By default, each role bandwidth limit is **0 Kbits/second**, indicating no bandwidth limit is enforced.

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 list. By default, each role bandwidth limit is **0 Kbits/second**, indicating no bandwidth limit is enforced.

- 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 original URL and the Post Login Redirect URL. You can view the Post Login Redirect URL by navigating to **Configuration > System > Settings**.
- Configure the firewall rules for the user role. vWLAN provides a full Layer 3 and Layer 4 stateful firewall at the AP. The domain administrator configures the firewall and 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 you configure 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 destination network in the appropriate fields. You can delete a policy by clicking delete icon 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	Any	Outgoing	Any	
+	Allow	Any	Outgoing	Any	
+	Allow	Any	Outgoing	Any	
+	Allow	Any	Outgoing	Any	
+	Allow	Any	Outgoing	Any	

[Append Firewall Rule](#)

VoWiFi Priority Configuration

Enable VoWiFi

Device Reassignment Rules

The client's source role is determined based on the initial authentication.


Once the client has authenticated, the client may be placed into a new destination role based on the device type and ownership configured in the rules below. For example, if "Device Type" is iPhone and "Ownership" is Corporate then the client will be placed into role named as the "Destination Role".

The destination role will be determined based on the following rules.

If no rule matches, then the client's role will not be changed.

[Append Device Reassignment Rules](#)

[Create Role](#)



For highest client throughput or performance for testing bandwidth and so on, configure the role with no bandwidth limitation (0), and configure only a single firewall rule by setting the rule to **Allow Any Both Ways Any**. In this configuration, the AP firewall is bypassed, allowing for the highest client throughput.

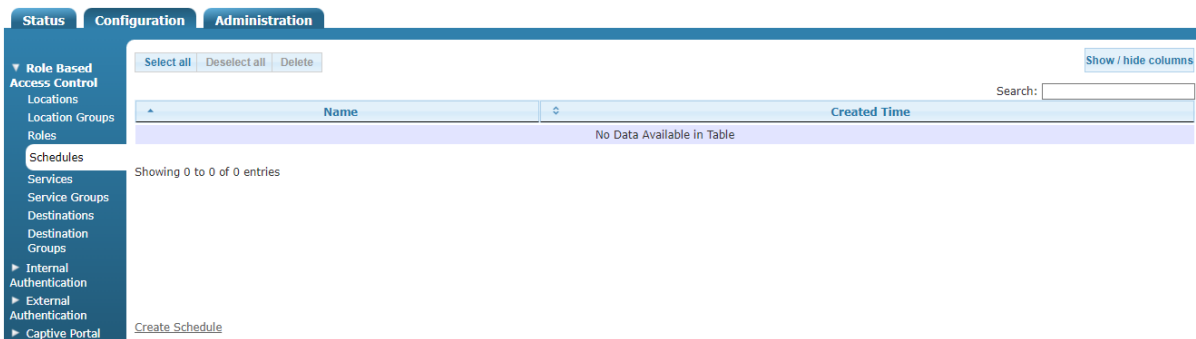
10. Select **Enable VoWiFi** to configure VoWiFi priority. This enables the AP to prioritize wireless traffic to or from a configured IP address. It will modify the IP header DSCP field to the configured value. This feature is supported only on 6000 series APs.
To maintain optimal AP packet processing performance, we recommend you to configure only a maximum of five IP addresses for this configuration.
11. Configure the device rules for the role. These rules specify the role a detected device is to use, based on the device fingerprint. The fingerprint includes **Device Type** and **Ownership** (corporate or other). The device is placed in the role specified in the **Destination Role** field 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 fields to specify the device type, ownership, and destination role.
12. Click **Create Role**.
A confirmation is displayed indicating that the role was created. The role will now appear in the role list under **Configuration > Role Based Access Control > Roles**, where you can display, edit, or delete the role.

Configuring Domain Role Schedules

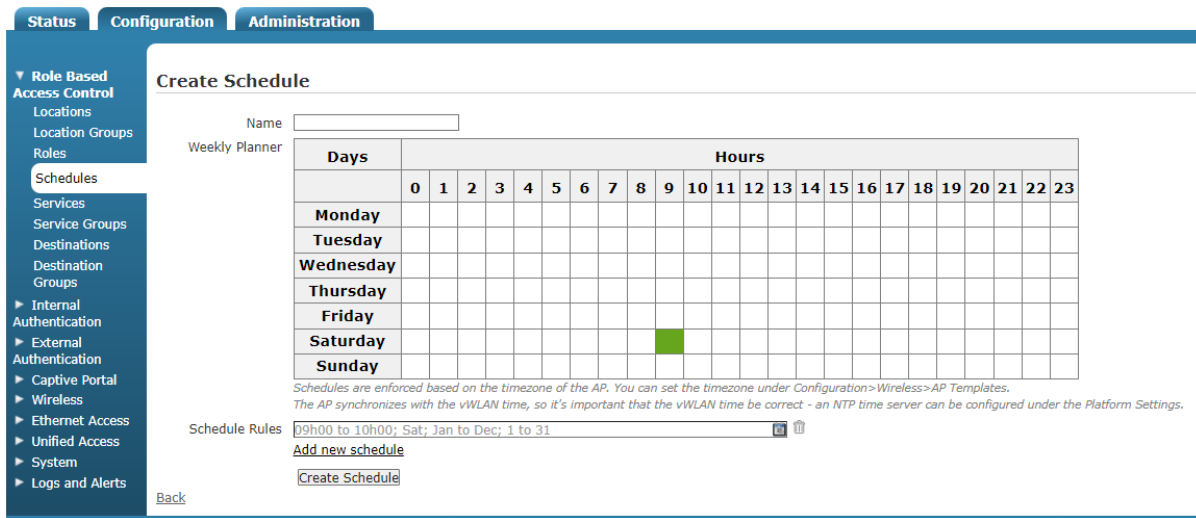
Domain role schedules specify the time in which clients can and cannot access the network. You can specify the days of the week, hours of the day, months, and days of the month that each created schedule is active, thus specifying when clients can or cannot access the network. After you create a schedule,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

To configure the domain role schedule:

1. Navigate to **Configuration > Role Based Access Control > Schedules**. This menu lists any previously configured domain role schedules. 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** menu at the top of the GUI.



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



3. 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.
4. 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**.

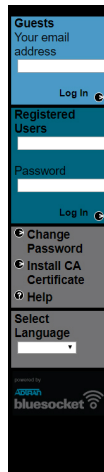
Repeat the day and hour selection process until you have specified the times you would like the schedule to allow client access. In the example below, the schedule allows client access only on Memorial Day weekend. To delete a schedule rule, click the delete icon next to the rule. To edit a rule, select the calendar icon next to the rule.

5. Click **Create Schedule** at the bottom of the menu. The newly created schedule appears in the schedule list under **Configuration > Role Based Access Control > Schedule**. For the schedule to become active, associate it with a role as described in [Configuring Domain Roles](#).

Configuring Web-based (Captive Portal) Authentication

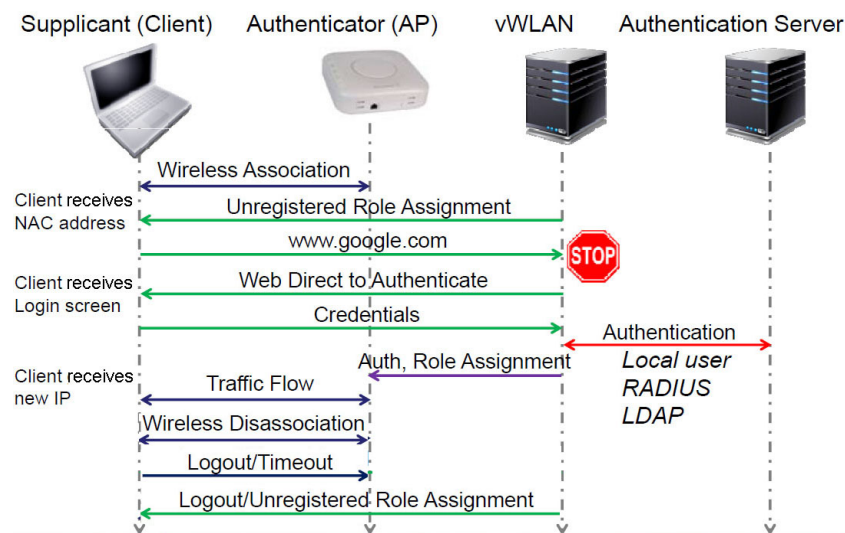
Web-based authentication (captive portal) is an authentication process in which clients typically connect to an open system SSID and are then redirected to a login page or captive portal (after opening a browser).

Figure 5: 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 6](#).

Figure 6: 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.



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/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 these types of authentication:

- server authentication
- local user authentication

- SSID authentication
- 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	90
External Server Authentication	91
External RADIUS IX Authentication Server	91
External RADIUS Web-based Authentication Server	93
External LDAP Web-based Authentication Server	96
External SIP2 Web-based Library Authentication Server	100
Configuring Local User Authentication	102
Device Authentication	104
Bulk Import of Devices	106

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. To comply with modern security standards, there is an option to disable TLS 1.0.

To disable TLS 1.0:

1. Navigate to **Configuration > 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?	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.

Showing 1 to 26 of 26 entries

2. Select **Disabled** from the **Enable TLS 1.0** field. Click **Update Platform Setting**.

The screenshot shows the 'Edit Platform Setting' page. The 'Enable TLS 1.0' dropdown menu is set to 'Disabled'. Below this, there is a note: 'Enable Transport Layer Security protocol version 1.0 for HTTP access. This is an older security protocol with known security vulnerabilities.' A red circle highlights the 'Update Platform Setting' button.

External Server Authentication

You can configure an external RADIUS IX, 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, complete the steps for each server type as outlined in these sections.



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

External RADIUS IX Authentication Server

To configure an external RADIUS IX authentication server for use with vWLAN:

1. Navigate to **Configuration > External Authentication > Servers**. This menu lists any previously configured RADIUS IX authentication servers. If you want to edit a previously created RADIUS IX 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** menu at the top of the GUI.

The screenshot shows the 'Servers' page under 'External Authentication'. The table is empty, displaying 'No Data Available in Table'. The 'Create Authentication Server' link is visible at the bottom.

Name	Type	Address	Port	Proxy Enabled	Role	Accounting Server *	Precedence
No Data Available in Table							

2. Select **Radius1xAuthServer** from the **Type** field.

The screenshot shows the 'Create Authentication Server' configuration page. The 'Type' dropdown menu is highlighted with a blue box and an arrow pointing to the selected 'Radius1xAuthServer' option. Other fields include Name (NPS1), Accounting Server, IP Address (192.168.10.253), Port (1812), Shared Secret/Password, Backup Address, Backup Port, Backup Password, Backup Password Confirmation, Enable RADIUS Proxy (checked), and Authentication Rules.

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 accounting server from the **Accounting server** field.
4. Specify the port to be used by the server. If you use a RADIUS server, the port is generally either 1645 or 1812.
5. Enter the shared secret or password for the authentication server.
6. 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.
7. Optionally, proxy all requests through the vWLAN to the RADIUS server versus from the AP directly to the RADIUS server by selecting **Enable RADIUS Proxy**.



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

8. 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** field. 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** list. There are multiple attributes to choose from.
9. Specify the logic type used for authentication mapping. 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 list.

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 delete icon.

10. Select **Create Auth Server** at the bottom of the menu. A confirmation is displayed indicating that the server was created. The server will now appear in the server list under **Configuration > External Authentication > Servers**, where you can display, edit, or delete the server.

External RADIUS 1X servers support these 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.

For more information, see [vWLAN External RADIUS 802.1x Authentication](#).

External RADIUS Web-based Authentication Server



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

To configure a RADIUS web-based authentication server for use with vWLAN:

1. Navigate to **Configuration > External Authentication > Servers**. This menu lists any previously configured web-based authentication servers. 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** menu at the top of the GUI.

2. Select **RadiusWebAuthServer** from the **Type** field.

Type

Name

Accounting Server

IP Address

Port
Typically, the port should be 1812 or 1645.

Shared Secret/Password

Shared Secret/Password Confirmation

Timeout Weight
*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.*

Maximum Number of Simultaneous Users Allowed to Authenticate at Once
Blank or 0 = no limit.

Precedence

Enable Radius MAC Authentication

Override Location with TunnelPrivate-Group-ID

Authentication Rules

Role

Attribute	Logic	Value	Role
ARAP-Challenge-Response	equal to		Guest
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](#)

[Create Authentication Server](#)

- 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.
- Specify the port to be used by the server. If you are using a RADIUS server, the port is generally either 1645 or 1812.
- Enter the shared secret or password for the authentication server.
- 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 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.
- 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** field. If you choose un-registered, the authentication rules determine the assigned role.



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** field.



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, 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** field. There are multiple attributes to choose from.

- 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**.

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 delete icon.

- Click **Create Authentication Server**. A confirmation is displayed indicating that the server was created. The server will now appear in the server list under **Configuration > External Authentication > Servers**, where you can display, edit, or delete the server.



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

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

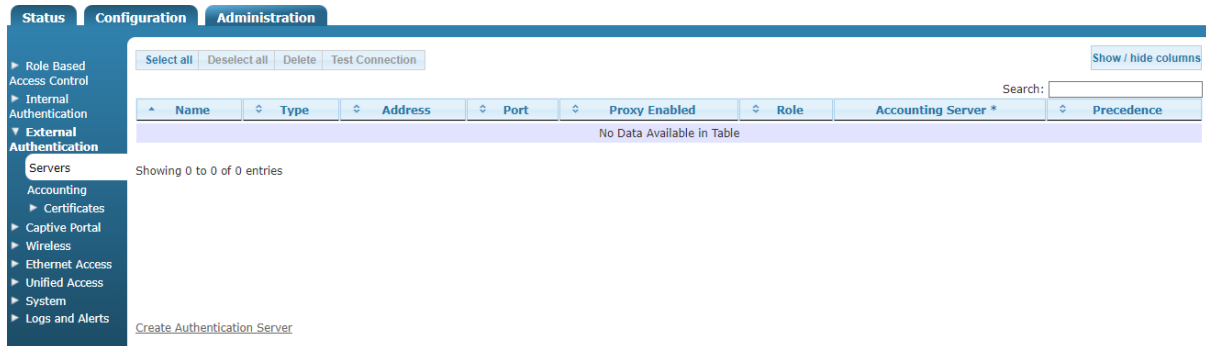


External RADIUS web-based authentication uses PAP and requires a RADIUS client to be configured in the RADIUS server for the vWLAN instance.

External LDAP Web-based Authentication Server

To configure an LDAP authentication server for use with vWLAN:

1. Navigate to **Configuration > External Authentication > Servers**. This menu lists any previously configured LDAP authentication servers. 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** menu at the top of the GUI.



2. In the **Create Authentication Server** menu, select **LdapAuthServer** from the **Type** field.

Create Authentication Server

Type:

Name:

Accounting Server:

IP Address:

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

LDAP Bind User:
The name of a user to bind to the LDAP server with.

Shared Secret/Password:

Shared Secret/Password Confirmation:

LDAP Base Entry:
An example base entry is cn=Users,dc=company,dc=com.

LDAP Unique ID Attribute:
UID for openldap, sAMAccountName for AD.

LDAP Filters:
Additional LDAP filters used when looking up Unique ID attributes.
 (An example is objectClass=Person)

Bind All Queries As LDAP Bind User:
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.

Timeout Weight:
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.

Maximum Number of Simultaneous Users Allowed to Authenticate at Once:
Blank or 0 = no limit.

Precedence:

Require SSL:

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** field.
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.

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



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.

6. Enter the shared secret or password for the previously created bind user.
7. 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.

You can configure the system to bind all queries with the LDAP Bind User credentials by selecting **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 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** field.

9. 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** field. 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. Specify the logic type used for authentication mapping (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 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**.

Authentication Rules

Role: Un-registered ▼

Attribute	Logic	Value	Role
distinguishedname	contains ▼	ou=Faculty	Guest ▼
	equal to ▼		Un-registered ▼
	equal to ▼		Un-registered ▼
	equal to ▼		Un-registered ▼
	equal to ▼		Un-registered ▼

[Append New Auth Rule](#)

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 delete icon.

11. Click **Create Authentication Server**. A confirmation is displayed indicating that the server was created. The server will now appear in the server list under **Configuration > External Authentication > Servers**, where you can display, edit, or delete the server.

Optionally, 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.

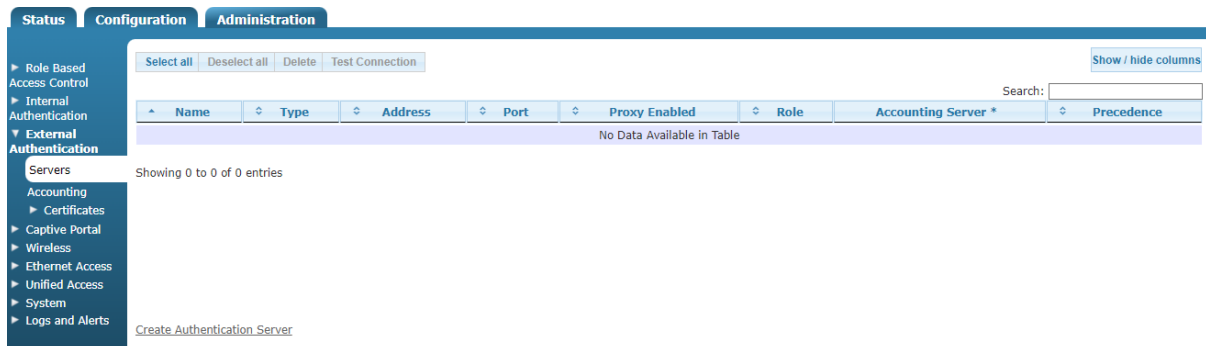
You will be redirected to the **Diagnostics** menu which allows you to enter a username and password to test the authentication method. See [External Authentication Test Results](#) for more information.

The screenshot shows the Adtran web interface. On the left is a navigation menu with the following items: Admin Authentication, Admin Tasks, Jobs, Access Points, vWLAN, Traffic Capture, AP Traffic Capture, Diagnostics (highlighted), Restart, Platform Upgrade, Patch, and Backup/Restore. The main content area is titled 'Administration' and has two tabs: 'Domain' and 'Platform'. Under the 'Platform' tab, there are three diagnostic tools: 'Ping', 'Traceroute', and 'External Authentication Test'. The 'External Authentication Test' tool is selected with a radio button. It includes an 'Authentication Server' dropdown menu, a 'Username' input field with the placeholder 'Enter Username', a 'Password' input field with the placeholder 'Enter Password', and a 'Run Diagnostic' button. The 'Ping' tool has a radio button, an 'Address' input field with the placeholder 'Enter the IP address or fully qualified domain name for the target host.', and an 'Interface' dropdown menu with 'Any' selected and the placeholder 'Interface is the source ethernet interface on the vWLAN.'. The 'Traceroute' tool has a radio button, an 'Address' input field with the placeholder 'Enter the IP address or fully qualified domain name for the target host.', and an 'Interface' dropdown menu with 'Any' selected and the placeholder 'Interface is the source ethernet port on the vWLAN. Results may take some time to appear, especially if the device cannot be reached or ICMP is blocked.'

External SIP2 Web-based Library Authentication Server

To configure a SIP2 authentication server (typically used in libraries) for user authentication:

1. Navigate to **Configuration > External Authentication > Servers**. This menu lists any previously configured SIP2 authentication servers. 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** menu at the top of the GUI.



2. Select **SIP2AuthServer** from the **Type** field.

Create Authentication Server

Type:

Name:

Accounting Server:

IP Address:

Port:
Typically, the port should be 6001.

SIP2 Admin Name:
The name of a user to authenticate to the SIP2 server with.

Shared Secret/Password:

Shared Secret/Password Confirmation:

Timeout Weight:
*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.*

SIP2 Validate PIN/Password:

SIP2 Specify An Empty AO Institution ID:

SIP2 CP Location Code:
Leave blank/empty to not send CP location code in the login message (93).

Maximum Number of Simultaneous Users Allowed to Authenticate at Once:
Blank or 0 = no limit.

Precedence:

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** field.
4. Specify the port to be used by the server. If you use a SIP2 server, the port is generally **6001**.
5. Optionally, specify the name of the administrator user to which to bind the SIP2 server. Enter the administrator FQDN in the **SIP2 Admin Name** field.



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.

6. Optionally, enter the shared secret or password for the authentication server.
7. 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 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).
8. Specify whether the user PIN or password will be validated by selecting the **SIP2 Validate PIN/Password** field.
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** field.
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.
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.
12. 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** field. 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**.

Continue with these steps:

1. Specify the logic type used for authentication mapping (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 list. 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**.

Authentication Rules

Role

Attribute	Logic	Value	Role
<input type="text" value="PC:profile"/>	<input type="text" value="contains"/>	<input type="text" value="Adult"/>	<input type="text" value="Guest"/>
<input type="text"/>	<input type="text" value="equal to"/>	<input type="text"/>	<input type="text" value="Un-registered"/>
<input type="text"/>	<input type="text" value="equal to"/>	<input type="text"/>	<input type="text" value="Un-registered"/>
<input type="text"/>	<input type="text" value="equal to"/>	<input type="text"/>	<input type="text" value="Un-registered"/>
<input type="text"/>	<input type="text" value="equal to"/>	<input type="text"/>	<input type="text" value="Un-registered"/>

[Append New Auth Rule](#)

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 delete icon.

2. Click **Create Authentication Server**. A confirmation is displayed indicating that the server was created. The server will now appear in the server list under **Configuration > External Authentication > Servers**, where you can display, edit, delete, or test the connection to the server.

Optionally, 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.

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

The screenshot shows the 'External Authentication Test' configuration page. It features a left-hand navigation menu with categories like 'Admin', 'Authentication', 'Jobs', and 'Diagnostics'. The main content area is divided into 'Domain' and 'Platform' tabs. Under the 'Platform' tab, there are three sections: 'Ping', 'Traceroute', and 'External Authentication Test'. The 'External Authentication Test' section is selected and contains the following fields and controls:

- External Authentication Test**: A radio button that is selected.
- Authentication Server**: A dropdown menu.
- Username**: A text input field with the placeholder 'Enter Username'.
- Password**: A text input field with the placeholder 'Enter Password'.
- Run Diagnostic**: A 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:

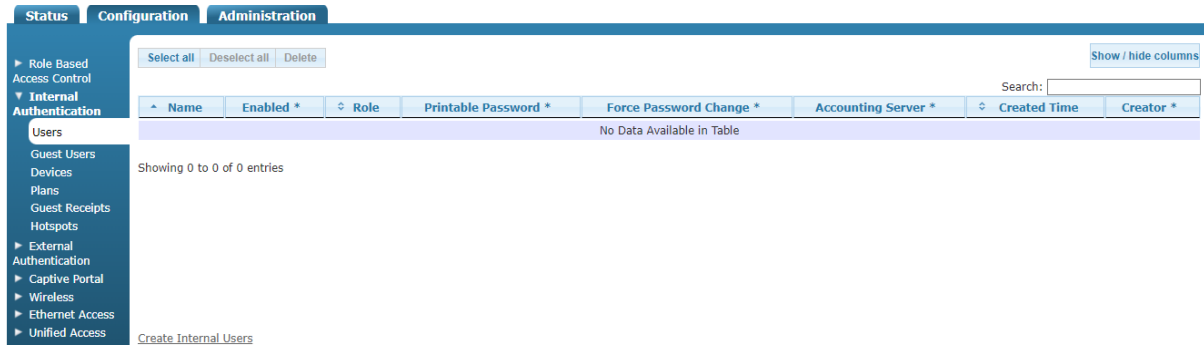
- User status (disabled, enabled)
- User name
- Role
- Number of active sessions
- User password
- Whether and how the user expires

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

To configure local user authentication for the specified domain:

1. Navigate to **Configuration > Internal Authentication > Users**. This menu lists any previously configured internal users. 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** menu at the top of the GUI.



- Specify the user name and password in the appropriate field, and enable the user by selecting the **Enabled** field. Then, specify the user role by selecting the appropriate role from the **Role** field. Optionally, select an accounting server to associate with this user from the **Accounting Server** field. 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 User** field.

Create Internal User

Name

Password

Password Confirmation

Password Expiration
Force password change on the next login.

Enabled

Role

Accounting Server

Simultaneous User
0 is unlimited.

Never Expire User

[Back](#)

- Click **Create Internal User**. A confirmation is displayed indicating that the user was created. The user will now appear in the internal user list under **Configuration > Internal Authentication > Users**, where you can display, edit, or delete the user.
After you create users, 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 configure a Polycom phone for MAC authentication, begin with the OUI of **00:90:7a**, and place 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.



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. The Layer 7 device fingerprinting feature provides status information, statistics, analytics, and reports based on the device type, operating system, manufacturer, host name, and ownership (corporate/business owned, or guest) of devices being used on the vWLAN network. In addition, device-specific connection policies can be enforced based on the device type and ownership. This feature allows you track Apple IOS, Android, Windows, MAC OS, and other operating systems while in use on the vWLAN network. Layer 7 device fingerprinting is part of vWLAN context-aware role-based access control where vWLAN examines user credentials, device type, device ownership, location, and date and time to enforce a policy.

When Layer 7 device fingerprinting is configured in vWLAN, as a device connects to the network, its transmitted DHCP discovery packet is inspected for Option 55 which includes the device fingerprint information, device type, operating system, and vendor. This information is sent to the vWLAN system which then determines the device role in the vWLAN network based on the detected device fingerprint and the device configuration options in vWLAN. Roles can be configured so that a matrix of rules is enforced based on the detected device information, allowing network administrators to control network access, bandwidth usage, and other network resources based on a device reported information.



Layer 7 device fingerprinting support is available on vWLAN systems running firmware release 2.6 or later and BSAP models using firmware 7.0.0.

Layer 7 device fingerprinting takes place only if the connecting device supports it by providing DHCP Option 55 information.

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

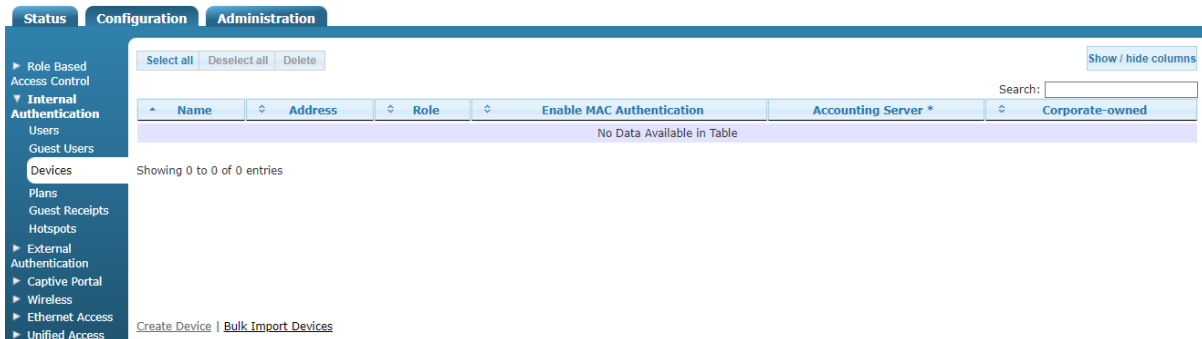
with a user role (configured in **Configuration > Roles**). In addition, you can add devices to vWLAN using a bulk import method. Details for Layer 7 device fingerprinting configuration are included in [Configuring Domain Roles](#).



With the included support of Layer 7 device fingerprinting, BSAPs automatically detect devices that do not authenticate correctly (retain their NAC IP address), and quickly deauthorize them so they will automatically reconnect to vWLAN for authentication. This process is known as selective deauthentication.

To configure a device for use in device authentication:

1. Navigate to **Configuration > Internal Authentication > Devices**. This menu lists any previously configured devices. 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** menu at the top of the GUI.



2. 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** field to enable MAC authentication for the device (this option is enabled by default). Specify the device assigned role using the **Role** field. Optionally, associate the device with an accounting server by selecting an accounting server from the **Accounting server** field. Optionally, specify whether the device is a corporate-owned device by selecting the **Corporate-Owned** field or specify the device is owned by someone else by leaving the field deselected). By default, the device is not configured as a corporate-owned entity. You can specify the role associated with the device in this menu, but if there is a role specified for the detected device type (see [Configuring Domain Roles](#)), that role will take precedence.

Create Device

Name
Name of device

MAC Address
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
Select to authenticate device to the network using its MAC address

Role

Accounting server

Corporate Owned
Select to make this device a corporate-owned device. This device will be subject to the device reassignment rules as configured in the role that the client will initially authenticate into. Once the client has authenticated, the client may be placed into a new destination role based on the device type and ownership. To review or change any device reassignment rules, navigate to the Roles webpage and edit a role.

[Back](#)

3. Click **Create Device**. A confirmation is displayed indicating that the device was created. The device will now appear in the device list under **Configuration > Internal Authentication > Devices**, where you can display, edit, or delete the device.

The device will now be authenticated using device authentication.



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.

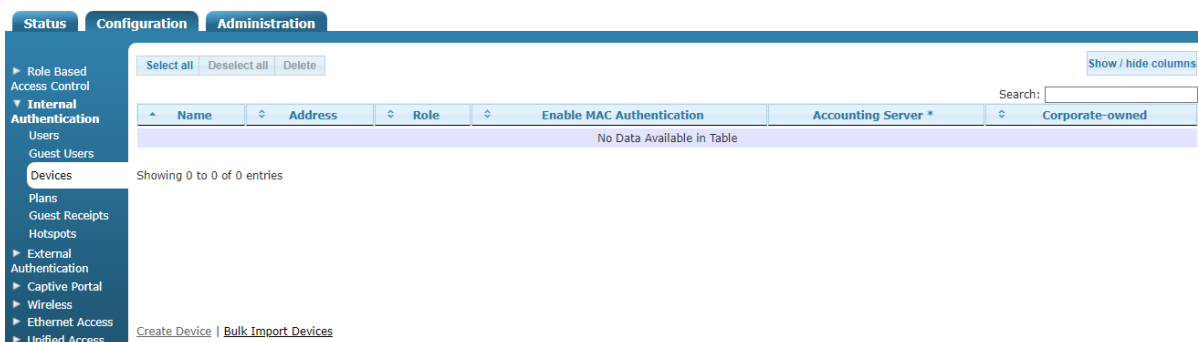
Bulk Import of Devices

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 this:

```
finename19,00:0c:22:55:b0:13,5,2
finename20,00:0c:22:55:b0:14,5
finename21,00:0c:22:55:b0:15,5,2
finename22,00:0c:22:55:b0:16,5,2
finename23,00:0c:22:55:b0:17,5,2
finename24,00:0c:22:55:b0:18,5,2
```

To import a CSV file of devices:

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



2. In the **Bulk Import Devices** menu, use the **Choose File** 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** field.

Bulk Import Devices

Select Input File No file chosen
Select text/plain/csv files with a limit of 2000 lines.

Corporate-Owned

[Back](#)

3. Click **Import CSV file** to import the file.
The imported devices will now appear in the device list under **Configuration** > **Internal Authentication** > **Devices**.

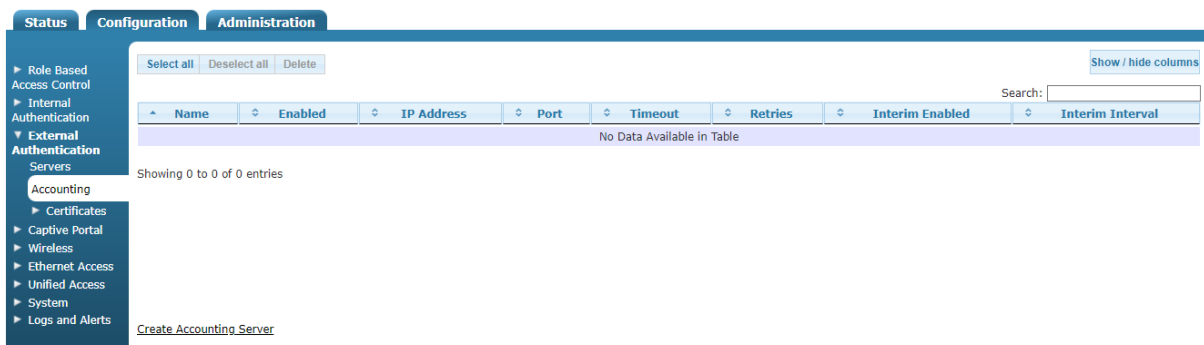
Configuring Domain Accounting

You can use RADIUS accounting to notify external systems about user 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 helps 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. You can also use accounting 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 you configure 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:

1. Navigate to **Configuration > External Authentication > Accounting**. This menu lists any previously configured accounting servers. 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** menu at the top of the GUI.



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

Create Accounting Server

Name

Enabled

IP Address

Port

Shared Secret

Shared Secret Confirmation

Timeout

Retries

Interim Updates Enabled

Interim Update Interval In Seconds

[Back](#)

3. Enter the shared secret for the accounting server, and the shared secret confirmation, in the appropriate fields.
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**.
5. Enable interim reporting updates by selecting the **Interim Updates Enabled** field. 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.
6. Click **Create Accounting Server** to create the server. A confirmation is displayed indicating that the server was created. The server will now appear in the accounting server list under **Configuration > External Authentication > Accounting**, where you can display, edit, or delete the server.

After you created the accounting server, you can associate the server with an authentication method, SSID, or AP. See [Configuring Web-based \(Captive Portal\) Authentication](#), [Configuring an SSID](#), or [Configuring AP Templates](#) for information.

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:

1. Navigate to **Configuration > 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 Adtran configuration interface with the 'Domain' tab selected. The 'Settings' section is expanded, and a table of domain settings is displayed. The table has three columns: Name, Value, and Hint. The settings listed are:

Name	Value *	Hint
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.
AP Control Channel Timeout	14400	Time in seconds before APs reboot if control channel is confirmed to be lost to the vWLAN (defaults to 24 hours - meaning, APs would reboot 24 hours after confirming that the control channel has been lost). Minimum allowed value is 300 seconds.
DHCP Lease Time for Un-registered Clients	10	An aggressive lease time brings clients on faster after authentication, but may not be compatible with all handheld devices.
Display Setup Wizard	Disabled	Enables setup wizard.
Flush Client Scan Data Interval	7	Range accepted from 0-30(In days), 0 means no data will be flushed out
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.
Time in minutes between updating internal status (minimum 5)	5	Updates client stats.
Time in seconds before inactive		

Showing 1 to 10 of 10 entries

2. Configure the aggressive DHCP lease time setting. Use this setting to reconnect clients quickly after authentication. By default, aggressive DHCP lease time for unregistered clients is disabled. When enabled, it speeds up web authentication, although it might not be compatible with all hand-held devices. To enable this setting, select **DHCP Lease Time for Un-registered Clients** from the list and select **Enabled** from the list. Click **Update Domain Setting** to apply the change.

Edit Domain Setting

DHCP Lease Setting Default ▼

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

[Update Domain Setting](#)

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

3. Allow the AP to look up the vWLAN name using a DNS pointer record (PTR) record. By default, an AP looks up the vWLAN name using a DNS PTR when redirecting clients to a host name for authentication. You must enable this setting 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 list. Click **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](#)

- Set the AP control channel timeout, which 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 **AP Control Channel Timeout** field. The maximum value is **4294967295** seconds. Click **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 24 hours - meaning, APs would reboot 24 hours after confirming that the control channel has been lost). Minimum allowed value is 300 seconds.

[Update Domain Setting](#)

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



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.

- Configure post-login redirect feature. The automatic redirect of users (post-login redirect) is disabled by default. To enable it, select **Post Login Redirect** from the list, and then select **Enabled**. 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 rather than their home page after successful authentication. Click **Update Domain setting** to apply the change.

Edit Domain Setting

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.

[Update Domain Setting](#)

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

- Set the post login redirect URL. The default URL for redirected users is their original URL if post-login redirect is not enabled. 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. Click **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.

[Update Domain Setting](#)

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

7. Redirect HTTPS traffic for unregistered clients. By default, HTTPS traffic from un-registered clients 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 **Enabled** from the field. Enabling this feature redirects HTTPS traffic to the captive portal. Click **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. Set the time between internal status updates. By default, this time is set to **5** 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 (minimum 5)** from the list, and enter a new value in the field. Updating this value changes the time (in minutes) between internal status updates, which updates the bandwidth reading. Click **Update Domain setting** to apply the change.

Edit Domain Setting

Time In Minutes Between Updating Internal Status
(minimum 5)

Updates client stats.

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



We recommend 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 field. The default value is **10** minutes, and you cannot set a value less than **1** second. If set to 1 second, any disconnected users are immediately dropped. This is useful when logging out unified access users during a reboot of the computer.

Updating this value causes dropping of inactive connections when the time limit is reached. Click **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 (see [Configuring Domain Roles](#) 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 (see [Configuring Local User Authentication](#)). You can either create new users and assign a role to them, or you can edit the roles of existing users.



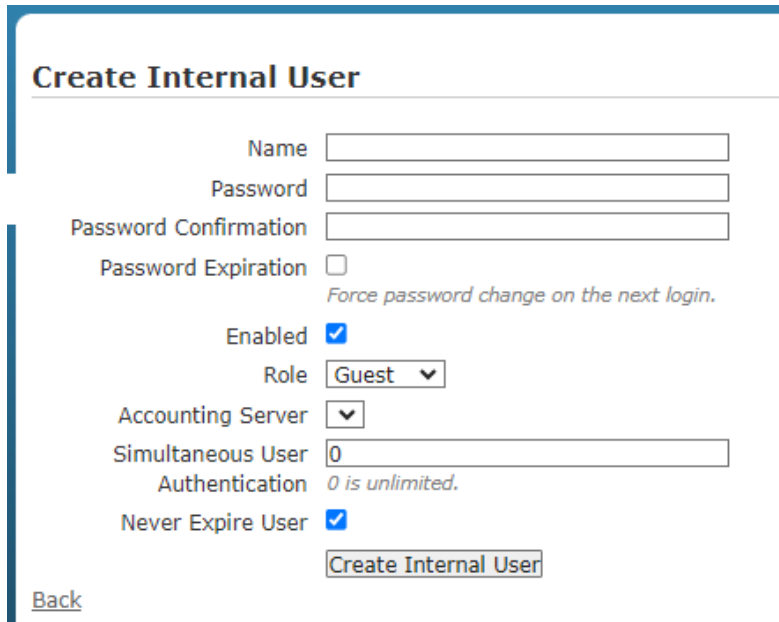
Any edits made to the role currently assigned to the user are not applied until the next time the user logs in.

To map users to a domain role:

1. Navigate to **Configuration > Internal Authentication > Users**. This menu lists any previously configured users. 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** menu at the top of the GUI.

The screenshot displays the 'Users' configuration page in the Adtran GUI. The navigation menu on the left includes 'Internal Authentication' and 'Users'. The main content area features a table with the following columns: Name, Enabled *, Role, Printable Password *, Force Password Change *, Accounting Server *, Created Time, and Creator *. The table is currently empty, showing 'No Data Available in Table'. Above the table are buttons for 'Select all', 'Deselect all', and 'Delete', and a search box. Below the table, it says 'Showing 0 to 0 of 0 entries' and a 'Create Internal Users' link.

2. In the **Create Internal User** menu, enter the user name and password in the appropriate fields. Select the **Password Expiration** field to force the user to change the password on the next login. Enable the user by selecting the **Enabled** field. Specify the user role by selecting the appropriate role from the **Role** field. Role selection depends on which roles you previously created (see [Configuring Domain Roles](#)). Optionally, associate an accounting server with this user using the **Accounting Server** field. 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. Specify whether the user account will expire by selecting the **Never Expire User** check box.



The screenshot shows the 'Create Internal User' configuration form. It includes the following fields and options:

- Name**: Text input field.
- Password**: Text input field.
- Password Confirmation**: Text input field.
- Password Expiration**: Check box (unchecked) with the text *Force password change on the next login.*
- Enabled**: Check box (checked).
- Role**: Dropdown menu with 'Guest' selected.
- Accounting Server**: Dropdown menu.
- Simultaneous User Authentication**: Text input field with '0' entered and the text *0 is unlimited.*
- Never Expire User**: Check box (checked).
- Create Internal User**: Button.
- Back**: Link.

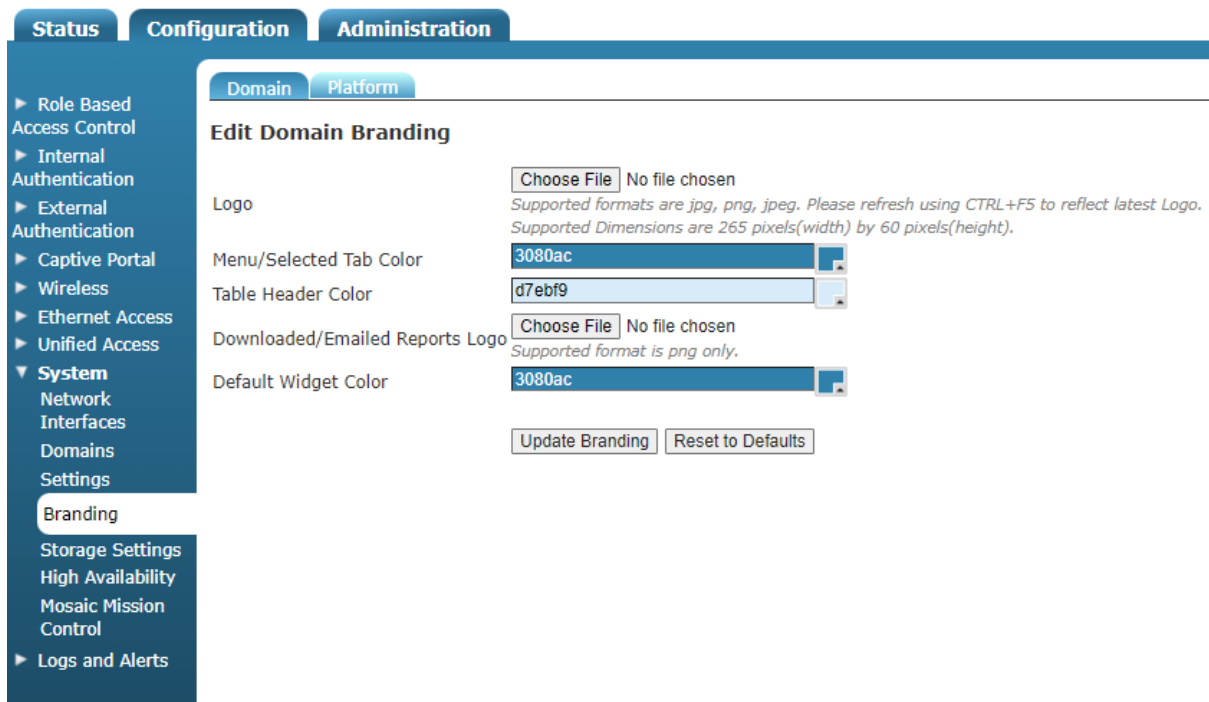
3. Click **Create Internal User**. A confirmation is displayed indicating that the user was created. The user will now appear in the internal user list under **Configuration > Internal Authentication > Users**, where you can display, edit, or delete the user.

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. See [Configuring vWLAN Platform Branding](#).

To access the domain branding, and change the default domain branding settings, follow these steps:

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



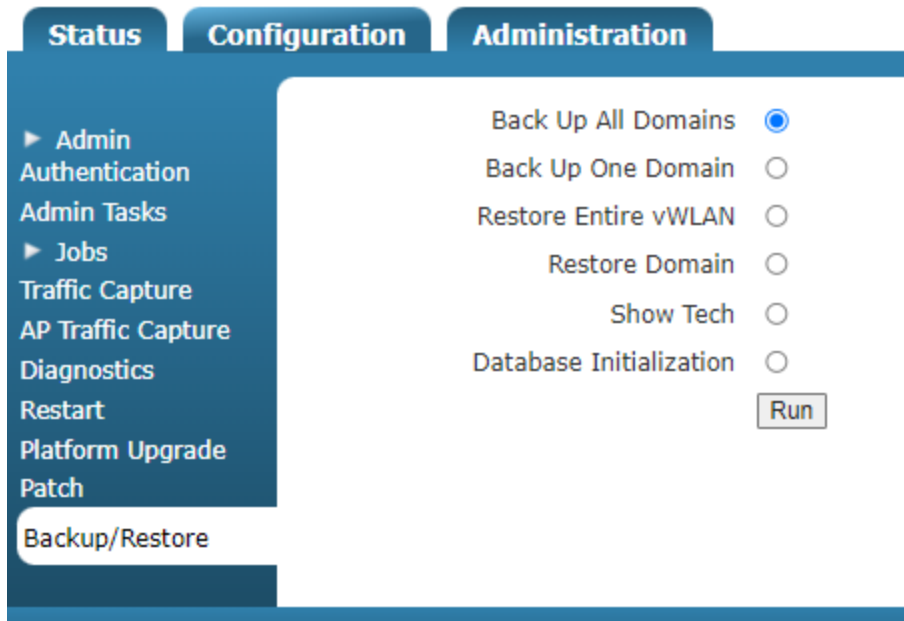
2. In the **Edit Domain Branding** menu, add any logos to the domain by uploading a logo file. Supported file formats are **.jpg**, **.png**, or **.jpeg**. Domain logo file sizes are 265 pixels (width) by 60 pixels (height). You can preview domain logos by pressing **CTRL+F5**.
3. Specify the colors 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. Click **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

We recommend to back up the domain configuration periodically, in order to restore the system when an outage or some other unforeseen event occur. The platform administrators with read and write permissions can only back up the domains (see [Specifying the Administrator Role](#)).

To backup the domain configuration:

1. Navigate to **Administration > Backup/Restore**.



2. Select the domain or domains that you want to backup by selecting the field 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, click **Run** to begin the backup or restore process.

Chapter 6

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 communicate 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 this chapter to display APs, managing AP configuration states, and resetting AP configuration. This chapter includes these sections:

Editing AP Firmware	116
Associating APs with a Domain	121
Using AP Discovery to Connect APs to vWLAN	122
Licensing APs	141
Configuring AP Templates	142
Configuring Additional AP Settings	194
Viewing APs	197
Viewing AP States	199
Resetting and Rebooting APs	200
Configuring AP Jobs	201

Editing AP Firmware

Upon first connecting the vWLAN, APs will upgrade their firmware to ensure they have the latest version. You can upload new firmware 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 (see [Performing System Maintenance](#)).

Instructions to upload both cloud-based and locally stored firmware are described in these sections:

Uploading Locally Stored Firmware	117
Uploading Firmware Stored on a Server	118
Troubleshooting AP Firmware	119

AP Connects to System But Does Not Have Correct Firmware 120

AP is Running and Firmware is Upgraded 120

AP Firmware Matches the Alternative Partition Firmware 120

Interruptions During Upgrade 120

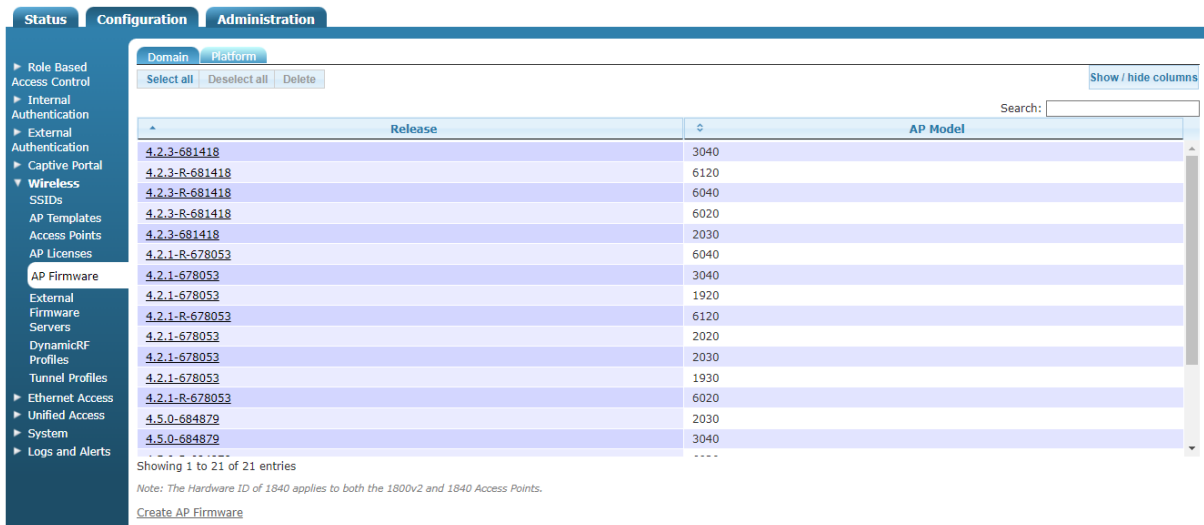
Simultaneous Firmware Upgrades 121

Newer AP Firmware 121

Uploading Locally Stored Firmware

To upload or edit locally stored AP firmware manually:

1. Navigate to **Configuration > Wireless > AP Firmware**. To upload firmware for a domain, select the **Domain** tab. To upload firmware for the vWLAN platform, select the **Platform** tab. This menu lists any previously configured APs. If you want to edit a previously configured AP, select the AP from the list. To upload new AP firmware, either click **Create AP Firmware** at the bottom of this menu or select **Domain AP Firmware** from the **Create** menu at the top of the GUI.



2. Select the new firmware file from the location in which you stored the downloaded firmware by selecting **Choose File**. Then, select the domains to which you want to apply the new AP firmware by using the + (plus) sign. If you upload to the domain view, the AP firmware will automatically be available in the domain. Choose the template to which you want to apply the firmware change or select **Keep the current AP template configuration**.

Create AP Firmware

Firmware No file chosen

Domains **0 items selected**

*Note: The firmware will not be added to or removed from domains with an * because you do not have the necessary permissions.*

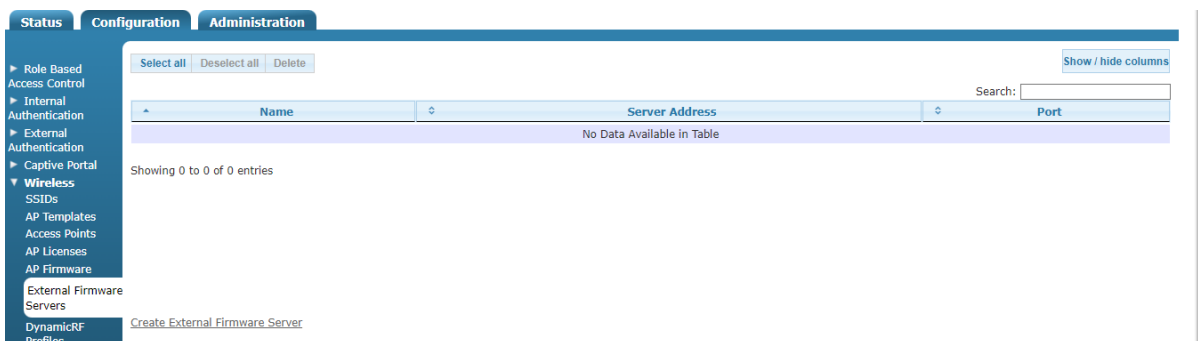
[Back](#)

3. Select **Create AP Firmware** or **Update AP Firmware** to apply the changes. A confirmation is displayed indicating that the AP firmware was successfully created or updated.
4. Apply the new or updated firmware to the AP by applying the firmware to an AP template (see [Configuring AP Templates](#)) or rebooting the AP (see [Resetting and Rebooting APs](#)).

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](#)) and to the remote server. After you upload the firmware to vWLAN, complete these steps:

1. Navigate to **Configuration > Wireless > External Firmware Servers**. If you want 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 External Firmware Server** from this menu or **Domain External Firmware Server** from the **Create** menu at the top of the GUI.



2. In the **Create External Firmware Server** menu, enter the server name and IP address in the appropriate fields.

Create External Firmware Server

All AP Models

Name

Server Address

Secure Copy Protocol (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](#)

3. 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.
4. Click **Create External Firmware Server** or **Update External Firmware Server** to apply the changes. A confirmation is displayed indicating that the firmware server was successfully created, and the server will now appear in the firmware server list under **Configuration > Wireless > External Firmware Servers**.
5. Apply the new firmware to an AP using an AP template (see [Configuring AP Templates](#)) or by rebooting the AP (see [Resetting and Rebooting APs](#)).

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 file name 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 does not function properly, verify that the AP has the correct firmware. These cases outline vWLAN and AP behavior when dealing with firmware:

AP Connects to System But Does Not Have Correct Firmware	120
AP is Running and Firmware is Upgraded	120
AP Firmware Matches the Alternative Partition Firmware	120
Interruptions During Upgrade	120
Simultaneous Firmware Upgrades	121
Newer AP Firmware	121

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 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. In this case, the AP will not have the configured radios, service clients, and so on.

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 6000 Series APs, this means the AP will upgrade the firmware, reboot as necessary, and return to an up state when ready for service. For legacy APs, this means that even while the AP is downloading new firmware, the AP radios remain functional and allow clients to access the network. The legacy 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 administrator completes the firmware upgrade.

AP Firmware Matches the Alternative Partition Firmware

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

Interruptions During Upgrade

If any interruptions occur during a firmware upgrade, the AP might be affected. For 6000 Series APs, the system will reboot the AP, or the administrator must reboot the AP. For legacy APs, however, each type of interruption is handled differently. Legacy AP firmware download interruptions are discussed below.

If the firmware download fails due to a firewall 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 resolving the issue.

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 resolving the issue.

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, 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, it is possible that the encryption has changed. In this case, vWLAN might require a patch to support the new firmware. If the patch is not installed, then the firmware is treated as invalid until the proper patch is uploaded. See [Performing System Maintenance](#) for information about installing patches.

Associating APs with a Domain



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.

After APs are discovered, you must associate them with a domain. To associate an AP with a domain:

1. Navigate to **Configuration > Wireless > AP Licenses**. Select the **Platform** tab. This menu lists any previously configured APs. 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 **Move AP(s) to domain** field.

The screenshot shows the vWLAN Administrator interface. The left sidebar contains a navigation menu with options like Role Based Access Control, Internal Authentication, External Authentication, Captive Portal, Wireless SSIDs, AP Templates, Access Points, AP Licenses (selected), AP Firmware, External Firmware, Servers, DynamicRF Profiles, Tunnel Profiles, Ethernet Access, Unified Access, System, and Logs and Alerts. The main content area is titled 'Configuration' and 'Administration'. Under 'Administration', the 'Platform' tab is active, showing a table of APs. The table has columns: Serial Number, MAC Address, IP Address, Domain, Firmware, Country, vWLAN License, Unified Access License, and Status. The first three rows are highlighted in blue. Below the table, there is a 'Move AP(s) to domain' dropdown menu and an 'Upload AP Licenses' button. A note at the bottom states: '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 *	Unified Access License *	Status
20301416051557	00:19:92:4b:fd:00	10.49.191.21	default	4.5.0-684879	United States	Lifetime	Lifetime	UpToDate
30404716050294	00:19:92:4f:3e:20	10.49.191.24	default	4.5.0-684879	United States	Lifetime	Lifetime	UpToDate
30404716050302	00:19:92:4f:3f:20	10.49.199.2	None	4.5.0-684879	None	None	None	Down
60200823050009	00:19:92:2d:84:c0	10.49.191.19	default	4.5.0-R-684879	United States	Lifetime	Lifetime	UpToDate
60201723051343	00:19:92:2f:81:20	10.49.192.187	default	4.5.0-R-684879	United States	Lifetime	Lifetime	UpToDate
60400723051011	00:19:92:2d:05:80	10.49.192.183	default	4.5.0-R-684879	United States	Lifetime	Lifetime	UpToDate
60400723051013	00:19:92:2d:05:c0	10.49.191.18	default	4.5.0-R-684879	United States	Lifetime	Lifetime	UpToDate
61204922050131	00:19:92:2a:d6:e0	10.49.191.20	default	4.5.0-R-684879	United States	Lifetime	Lifetime	UpToDate



APs must have a valid country and a vWLAN license to be moved to a domain.

2. At the prompt, select **OK** to change the domain of the APs. A success message is displayed when the APs was moved to the specified domain.

This method for changing AP domains is suited for the movement of APs on a large scale.

If you want to change only one AP domain, you can use the preceding method, or alternatively, you can use this method:

1. Navigate to **Configuration > Wireless > AP Licenses**, select the **Platform** tab, and then select the AP from the list for which you want to change the domain.
2. Select the appropriate domain from the **Domain** field, and select **Update AP License**.

Edit AP License

Serial Number 20301416051557

Domain

Country United States

vWLAN License Lifetime

Unified Access License Yes

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

3. A confirmation message displays indicating the change was applied to the AP.
Either method you choose will update the APs 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, you must specify a few items in your network to facilitate the AP discovery process. You must allow certain protocols 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 [System Requirements](#). Keep these requirements in mind when configuring your firewall and any access control lists (ACLs).

This sections contains these topics:

AP Discovery Process	123
System Requirements	123
Configuring AP Discovery Method	126

Verifying BSAP Discovery	138
Troubleshooting AP Discovery	138

AP Discovery Process

The cloud-based approach of the Adtran Bluesocket vWLAN distributed architecture allows vWLAN components, primary and secondary vWLANs and Bluesocket APs to be deployed anywhere. This type of flexibility supports several different deployment scenarios:

- Primary and secondary vWLAN systems deployed centrally at corporate headquarters or data centers in a private-cloud network
- Secondary vWLAN systems deployed at remote disaster recovery sites or data centers
- Both vWLAN systems deployed in a hosted public-cloud model
- The primary system deployed at a corporate headquarters while the secondary system is deployed in a hosted model
- A mixture of deployments

You can deploy BSAPs locally to the vWLAN system or at remote sites, or behind network address translation (NAT) devices such as routers or firewalls.

Whatever deployment scenario is used, the you must configure BSAPs with a method to discover the primary and secondary vWLAN. AP discovery is based on an algorithm that attempts various discovery methods in a specific order. Discovery methods, in order of precedence, include: statically configuring the BSAP using the CLI, configuring Dynamic Host Control Protocol (DHCP) Option 43 in your organization DHCP server, your organization domain naming system (DNS) server, or caching a previously discovered vWLAN system. If one discovery method fails, then the next method is attempted (unless the BSAP is statically configured).

This section describes the AP discovery methods, ports and protocols, and sample AP discovery configurations for AOS DHCP servers, Microsoft Windows Server 2008 R2 Enterprise DHCP and DNS servers, Internet Systems Consortium (ISC) DHCP servers, and Cisco Internetwork Operating System (IOS) DHCP servers.

System Requirements

This section describes AP discovery configurations for vWLAN virtual appliances (VMware) and BSAPs running vWLAN software versions 2.2.1 and later.

Before configuring AP discovery, ensure you have basic understanding of the following:

- Adtran Bluesocket vWLAN and BSAPs
- AOS (if applicable)
- Microsoft Windows Server 2008 R2 Enterprise DHCP and DNS servers (if applicable)
- ISC DHCP servers (if applicable)

- Cisco IOS DHCP servers (if applicable)
- DHCP

Components Used in AP Discovery Configurations

The information in this section was created in a specific lab environment. All of the devices used had a default configuration. The configurations presented in this section were tested and found to function as expected. These components were used in testing:

- Virtual appliance (VMware) running vWLAN software 2.2.1 and later
- BSAPs
- AOS DHCP server
- Microsoft Windows Server 2008 R2 Enterprise DHCP and DNS server
- ISC DHCP server
- Cisco IOS DHCP server



If your network is active, make sure you understand the potential impact of any command issued on these devices. If you experience difficulty configuring the Microsoft Windows Server R2 Enterprise DHCP and DNS server, ISC DHCP server, or Cisco IOS DHCP server, contact Microsoft, ISC, or Cisco respectively for assistance. Microsoft Server R2 Enterprise, ISC DHCP servers, or Cisco IOS are not supported.

Required Ports and Protocols

These ports and protocols are required to be open as necessary between the vWLAN and BSAPs, between primary and secondary vWLAN systems when using high availability, between the vWLAN and authentication servers when using various methods of authentication, between BSAPs when using Layer 3 mobility (tunneling), and between BSAPs and authentication when using external Remote Authentication Dial-In User Service (RADIUS) 802.1x authentication. Ensure that any firewalls or access control lists (ACLs) allow the ports and protocols outlined in [Table 3](#) as applicable.



The ports and protocols described in [Table 3](#) are a comprehensive list of ports and protocols that must be open as necessary. These ports and protocols are not limited to AP discovery.⁷

Table 3: Required Ports and Protocols

Port Type and Number	Port Protocol	Purpose
Transmission Control Protocol (TCP) port 33333	Transport Layer Security (TLS)	Secure control/management channel between vWLAN and BSAPs.

Port Type and Number	Port Protocol	Purpose
TCP port 33334	Secure Copy Protocol (SCP)	Used on the BSAP 1900 Series to transfer firmware between vWLAN and the BSAP or between BSAPs and a third-party SCP server. Also used for AP traffic capture file transfer between vWLAN and the BSAP.
TCP port 28000	Transport Layer Security (TLS)	Used to secure wireless Internet distribution systems (IDS) channels between vWLAN and BSAPs.
TCP port 2335	TLS	Used for communication between primary and secondary vWLAN systems for high availability.
TCP port 3000	Hypertext Transfer Protocol Secure (HTTPS)	Used for communication between primary and secondary vWLAN systems for high availability and access to the vWLAN web-based graphical user interface (GUI).
TCP port 80	Hypertext Transfer Protocol (HTTP)	Required for captive portals between vWLAN and the BSAPs in vWLAN releases prior to 2.2.1.
TCP port 443	HTTPS	Required for captive portals between vWLAN and the BSAPs.
UDP port 1812 or 1645	RADIUS	Required for RADIUS web-based authentication and RADIUS administrative authentication between the BSAP and the authentication server. Also required for RADIUS external 802.1x authentication between the BSAP and the authentication server.
UDP port 1813 or 1646	RADIUS	Required when using RADIUS accounting between vWLAN and an accounting server.

Port Type and Number	Port Protocol	Purpose
TCP port 389	Lightweight Directory Access Protocol (LDAP)	Required for LDAP or Microsoft Active Directory (AD) authentication between vWLAN and an authentication server.
UDP port 636	LDAP over Secure Socket Layer (SSL)	Required for LDAP or AD authentication between vWLAN and an authentication server.
TCP port 6001	Standard Interchange Protocol (SIP2)	Required for SIP2 authentication between vWLAN and the library authentication server.
	IP protocol 97	Required for Layer 3 roaming between BSAPs.

In vWLAN firmware versions previous to 2.6, APs were required to use DNS to communicate with vWLAN and determine if the vWLAN was active. In vWLAN release 2.6, this requirement was removed so that the AP discovery process is not interrupted when APs are not configured for outbound DNS access because of firewall policies.

Configuring AP Discovery Method

These sections describe the four types of AP discovery methods:

Statically Configuring BSAPs Using the CLI	126
Configuring DHCP Option 43 in Your Organization DHCP Server	127
Configuring an Entry for AP Discovery in Your Organization DNS Server	136
Caching a Previously Discovered vWLAN IP Address for AP Discovery	137



If a vWLAN is not discovered, the AP attempts to connect to a server at the 76.164.174.46 IP address. This server is for future use. If you are attempting to connect to a different vWLAN, see [Troubleshooting AP Discovery](#) to determine why the AP did not connect.

Statically Configuring BSAPs Using the CLI

You can configure each BSAP for static discovery mode and populate the vWLAN public network interface IP address using the CLI (console port or secure shell (SSH)). It is only necessary to populate the primary vWLAN public network interface IP address. For more information about how to statically configure BSAPs using CLI, see the *BSAP CLI Reference Guide*.



Configuring BSAPs using the CLI is not recommended for large scale deployments because each BSAP must be configured individually.

Configuring DHCP Option 43 in Your Organization DHCP Server

When a BSAP sends a DHCP discovery message to obtain an IP address, it includes DHCP Option 60. DHCP Option 60 is the vendor class identifier (VCI). The VCI is a string that identifies the BSAP to the DHCP server. The VCI used by all BSAPs regardless of model is **BlueSecure.API500**.

Vendor-Specific Information

On the DHCP server, the vendor-specific information is mapped to the VCI string. When the DHCP server sees a recognizable VCI in a DHCP discovery message from a BSAP, it returns the mapped vendor-specific information in its DHCP offer to the BSAP as DHCP Option 43. On the DHCP server, Option 43 is defined in each DHCP pool that offers IP addresses to the BSAPs.

RFC 2132 states that DHCP servers must return vendor-specific information as DHCP Option 43. The RFC allows vendors to define encapsulated vendor-specific options. The encapsulated vendor-specific options are all included in the DHCP offer encoded as a sequence of code, length, and value within Option 43. The definition of encapsulated vendor-specific options is specific to the vendor.

When DHCP servers are programmed to offer vWLAN public network interface IP addresses as Option 43 for BSAPs, the encapsulated vendor-specific options are defined in this manner:

Code: 127 (in decimal format)

Length: A count of the characters of the ASCII string in the Value field (in decimal format)

Value: ASCII string that is a comma separated list of primary vWLAN public network interface IP addresses followed by secondary vWLAN public network interface IP addresses. Secondary vWLAN public network interface IP addresses start with F, denoting failover. No spaces should be embedded in the list.

This is sample information for the code, length, and value of DHCP Option 43:

Primary vWLAN public network interface IP address: 192.168.130.1

Secondary vWLAN public network interface IP address: 192.168.130.2

Code: 127

Length: 28

Value: 192.168.130.1,F192.168.130.2



The secondary vWLAN public network interface IP address starts with F, denoting failover. When high availability is enabled, the secondary vWLAN public network interface IP address is automatically configured; however, it is best practice to include the secondary vWLAN IP address in DHCP Option 43 in case the BSAP is unable to obtain a configuration from the primary vWLAN system.

Converting DHCP Values to Hexadecimal Values

Depending on the DHCP server, it might be necessary to convert DHCP values to hexadecimal values. For example, the Microsoft DHCP server allows you to enter the code value in decimal format, and the value in ASCII characters, and the length is calculated automatically. The ISC

DHCP server and the Cisco IOS server, however, require the values to be converted to hexadecimal format. In addition, values converted to hexadecimal format can be beneficial in troubleshooting.

This is an example of DHCP code and length values from the previous example converted from decimal format to hexadecimal format:

127=7f (Code value)

28=1c (Length value)

This is an example of DHCP values converted from ASCII to hexadecimal format using the conversions described in [Table 4](#):

192.168.130.1 is converted as 1=31, 9=39, 2=32, .=2e, 1=31, 6=36, 8=38, .=2e, 1=31, 3=33, 0=30, .=2e, 1=31, resulting in 3139322e3136382e3136382e3133302e31.

F192.168.130.2 is converted as F=46, 1=31, 9=39, 2=32, .=2e, 1=31, 6=36, 8=38, .=2e, 1=31, 3=33, 0=30, .=2e, 1=32, resulting in 463139322e3136382e3133302e32.

Table 4: ASCII to Hexadecimal Conversion

ASCII Value	Hexadecimal Value
0	30
1	31
2	32
3	33
4	34
5	35
6	36
7	37
8	38
9	39
.	2e
,	2c
F	46

The DHCP Option 43 from the preceding example appears as follows when converted to hexadecimal format:

7f1c3139322e3136382e3133302e312c463139322e3136382e3133302e32

In order for the BSAP to discover the vWLAN, the DHCP server must be programmed to return the primary and secondary vWLAN public network interface IP addresses based on the VCI of the BSAP. You must program the DHCP server to recognize the VCI for the BSAP and then define the vendor-specific information. The semantics of DHCP server configuration vary based on the DHCP server vendor. Steps for configuring the various tested DHCP servers are outlined in these sections:

AOS DHCP Option 43 Configuration	129
Microsoft Windows Server 2008 R2 DHCP Option 43 Configuration	131
ISC DHCP Option 43 Configuration	135
Cisco IOS DHCP Option 43 Configuration	136

AOS DHCP Option 43 Configuration

You can configure the AOS DHCP server using the CLI or the GUI. To configure the AOS DHCP server using the CLI:

1. Access the AOS server CLI and enter Global Configuration mode.
2. Create a DHCPv4 pool by specifying the network, DNS server, and default router. Use the commands outlined in [Table 5](#) to configure the DHCPv4 pool.

Table 5: AOS DHCPv4 Pool Configuration Commands

Prompt	Command	Description
(config)#	ip dhcp-server pool <i><name></i>	Creates a DHCPv4 server pool and enters the pool configuration mode.
(config-dhcp)#	network <i><ipv4 address></i> <i><subnet mask></i>	Specifies the subnet number and mask for the DHCPv4 pool.
(config-dhcp)#	dns-server <i><ipv4 address></i>	Specifies the default DNS server to use for the DHCPv4 client.
(config-dhcp)#	default-router <i><ipv4 address></i>	Specifies the default primary router to use for the DHCPv4 client.

3. Add Option 43 to the DHCPv4 server pool using the **option <number> ascii <string>** command. Enter the command as follows:

```
(config-dhcp)#option 43 ascii 192.168.130.1,F192.168.130.2
```

4. Enter the **do write** command to save the configuration. The CLI configuration of the AOS DHCPv4 server pool is complete.

To configure the AOS DHCPv4 server pool using the AOS GUI:

1. Access the AOS server GUI and navigate to **System > DHCP Server**. Select the **DHCP Pools** tab and enter the server pool name in the **Pool Name** field. Select **Add**.

The screenshot shows the 'DHCP Server Settings' window with the 'DHCP Pools' tab selected. A red circle highlights the 'Add New DHCP Server pool' section, where the 'Pool Name' field is set to 'AP Management' and the 'Add' button is visible. Below this, a table lists existing DHCP server pools:

Name	Subnet/Host	IP Address
Subnet	subnet	192.168.20.0/24
Lab	subnet	192.168.30.0/24
Home	subnet	192.168.10.0/24

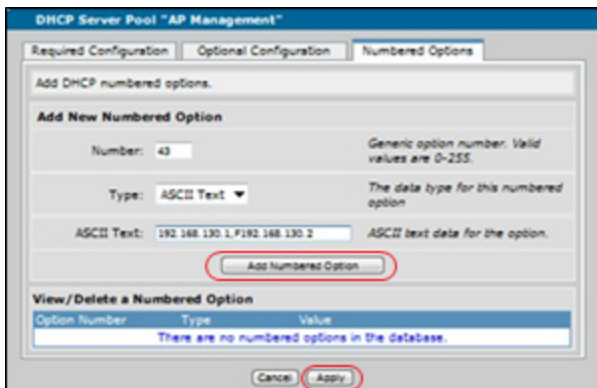
2. In the **DHCP Server Pool** configuration menu, select the **Required Configuration** tab and enter the subnet address, subnet mask, and default gateway in the appropriate fields.

The screenshot shows the 'DHCP Server Pool "AP Management"' configuration window with the 'Required Configuration' tab selected. A red circle highlights the 'IP Addresses' section, where the 'Assign IP addresses to all DHCP clients on a subnet' radio button is selected. The 'Subnet Address' is set to 192.168.130.0 and the 'Subnet Mask' is set to 255.255.255.0. Below this, the 'Default Gateway' is set to 192.168.130.254.

3. Select the **Optional Configuration** tab and enter the DNS servers in the appropriate fields.

The screenshot shows the 'DHCP Server Pool "AP Management"' configuration window with the 'Optional Configuration' tab selected. The 'Domain Name' field is empty. The 'Primary DNS' is set to 4.2.2.1, the 'Second DNS' is set to 4.2.2.3, and the 'Third DNS' is empty. The 'Primary WINS', 'Secondary WINS', 'TFTP Server', 'NTP Server', and 'Timezone offset' fields are also empty. The 'NAP' checkbox is unchecked.

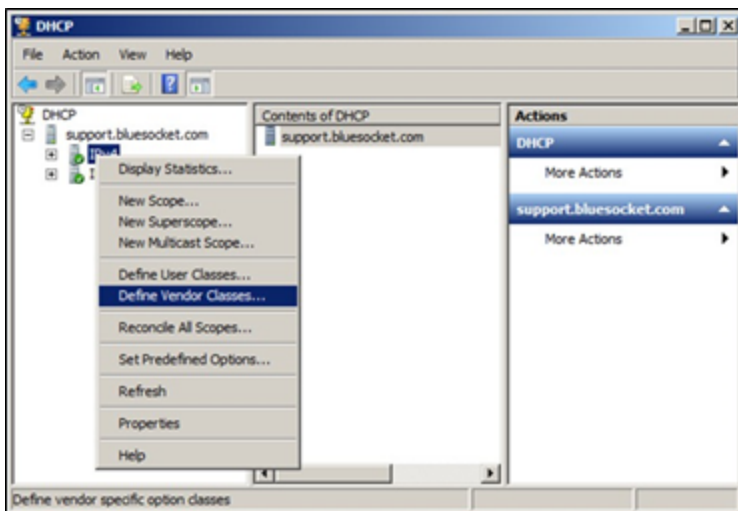
4. Select the **Numbered Options** tab and enter **43** in the **Number** field. Select **ASCII Text** from the **Type** field, and enter the vWLAN public network IP addresses in the **ASCII Text** field. Separate each address by a comma (with no spaces between addresses). The secondary address should begin with F. Select **Add Numbered Option**, and then select **Apply**. The AOS DHCPv4 server pool configuration is complete.



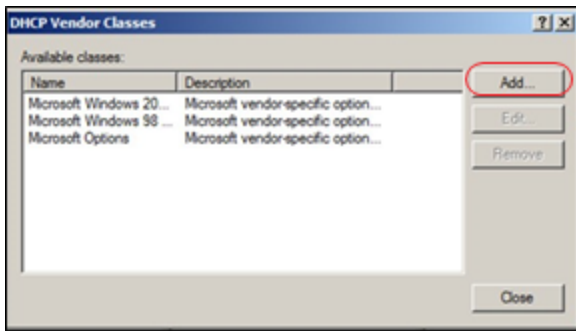
Microsoft Windows Server 2008 R2 DHCP Option 43 Configuration

Configure the DHCP Option 43 on the Microsoft Windows Server R2 Enterprise DHCP server by defining the vendor class, configuring the predefined Option 43, and configuring the option for the BSAP DHCP scope. To complete this configuration:

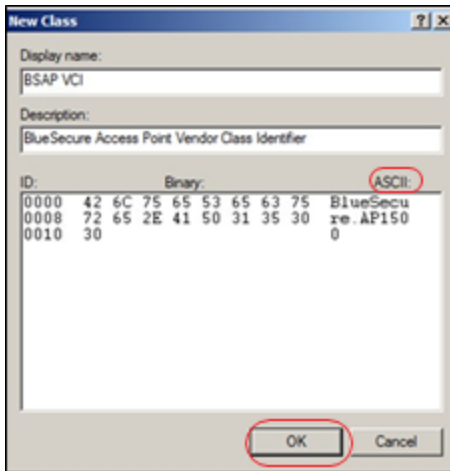
1. Access the Microsoft Windows Server 2008 R2 and navigate to **Start > Administrative Tools > DHCP**.
2. In the left pane of the **DHCP** menu, right-click **IPv4** and select **Define Vendor Classes**.



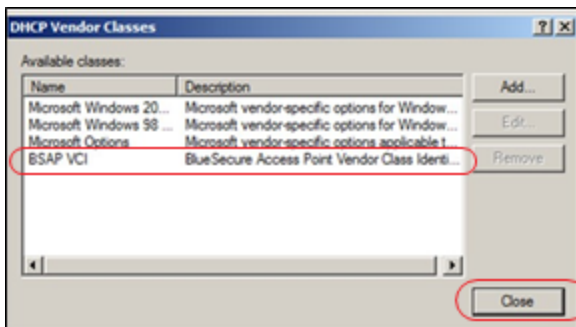
3. In the **DHCP Vendor Classes** menu, select **Add**.



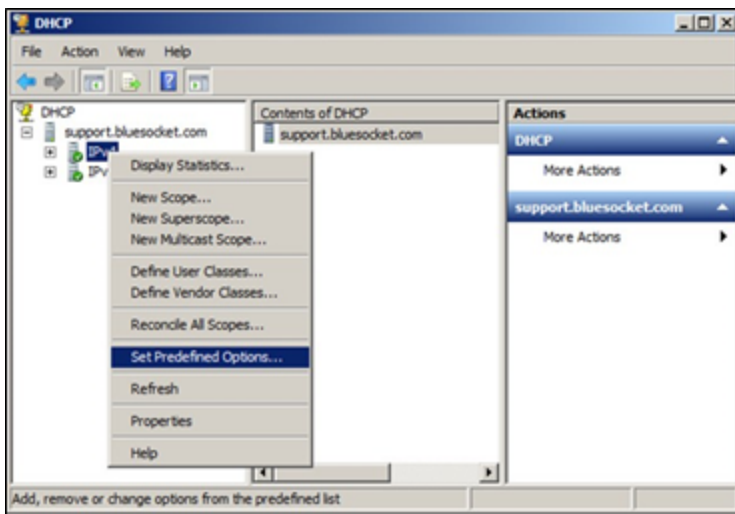
4. In the **New Class** menu, enter the display name and description of the vendor class in the appropriate fields. Select the **ASCII** field, enter **BlueSecure.API500**, then select **OK**.



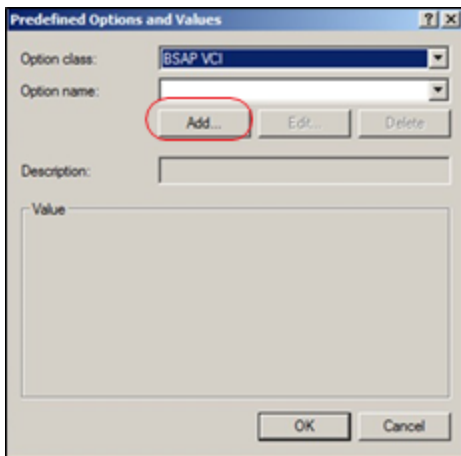
5. In the **DHCP Vendor Classes** menu, verify the name and description of the newly created class. Once the class is verified, select **Close**.



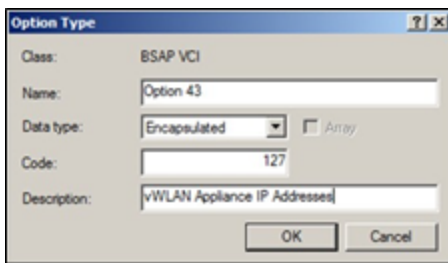
6. In the left pane of the DHCP menu, right-click IPv4 and select Set Predefined Options.



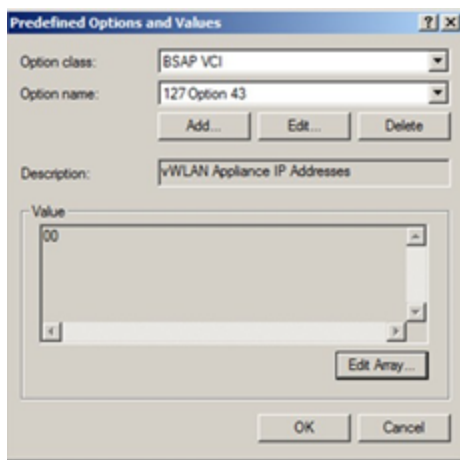
- In the **Predefined Options and Values** menu, select the newly created option class from the **Option class** drop-down menu (created in Step 4). Select **Add**.



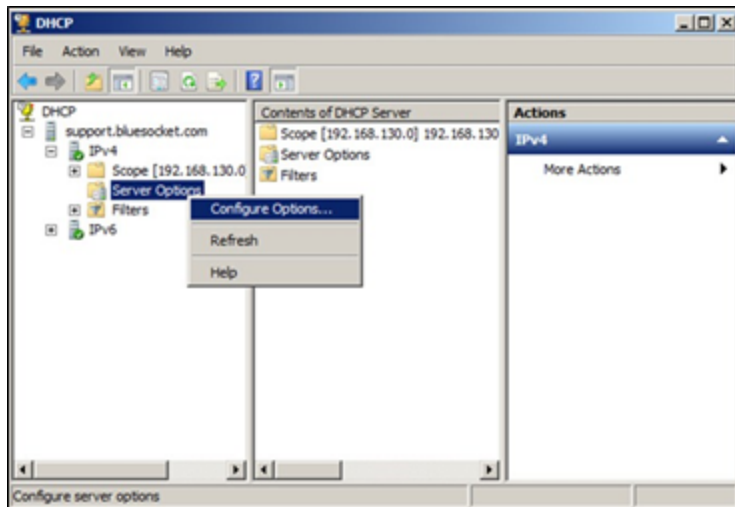
- In the **Option Type** menu, enter the name and description of the option in the appropriate fields. Select **Encapsulated** from the **Data type** drop-down menu and enter **127** in the **Code** field. Select **OK**.



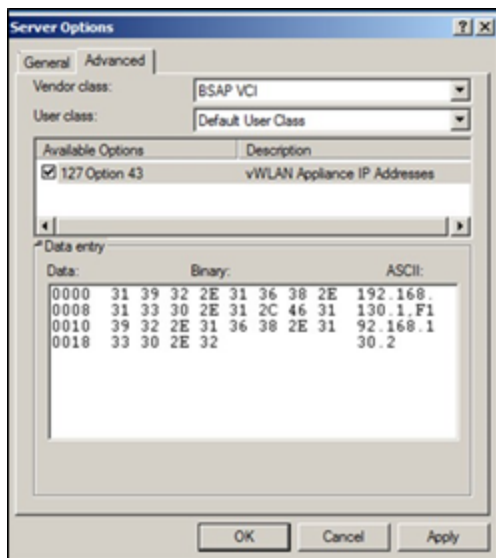
- In the **Predefined Options and Values** menu, verify the name and description of the newly created option. Select **OK**.



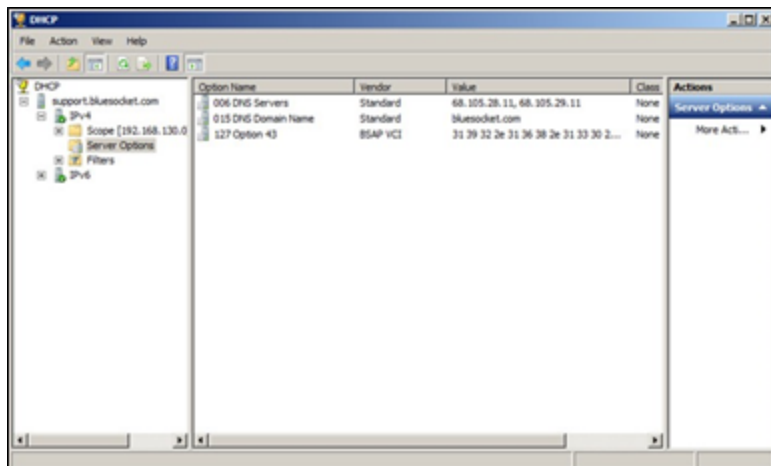
10. In the left pane of the **DHCP** menu, expand the **IPv4** menu and right-click **Server Options** under the scope that will service the BSAPs (**Scope 192.168.130.0** in the example below). Select **Configure Options**.



11. In the **Server Options** menu, select the **Advanced** tab. Select the vendor class created in Step 4 from the **Vendor class** drop-down menu. Select the check box next to the option created in Step 8 in the **Available Options** pane. Then, select **ASCII** in the **Data Entry** pane and enter the vWLAN public network interface IP addresses. The addresses should be separated by a comma (with no spaces between the addresses), and the secondary address should begin with F. You must delete the . that is preinserted into the field. After entering the appropriate information, select **Apply** and then select **OK**.



- In the **DHCP** menu, navigate to **IPv4 > Scope > Server Options** and verify that the displayed option name, vendor, and value are correct. If so, configuration of the Microsoft Windows Server 2008 R2 DHCP server is complete.



ISC DHCP Option 43 Configuration

To configure the DHCP Option 43 for AP discovery in the ISC DHCP server:

- Access the ISC DHCP server and add the **Option 60** VCI.
- Add the vendor-encapsulated options (Option 43) using these settings:

```
if option vendor-class-identifier = "BlueSecure.AP1500" {option vendor-encapsulated-options
7f:1c:31:39:32:2e:33:30:2e:31:2c:46:31:39:32:2e:31:36:38:2e:31:33:30:2e:3
2;}
```

The hexadecimal string in this step is assembled as a sequence of **code/length/value** settings converted to hexadecimal format and separated by colons. For information about these values and their conversion, see [Vendor-Specific Information](#).

Cisco IOS DHCP Option 43 Configuration

To configure the DHCP Option 43 for AP discovery in the Cisco IOS DHCP server:

1. Access the Cisco IOS DHCP server and enter configuration mode in the CLI.
2. Create a DHCP pool and configure the necessary parameters, including the default router and DNS server. Use these commands:

```
ip dhcp pool <pool name>  
network <ip address> <mask>  
default-router <ip address>  
dns-server <ip address>
```

3. Add Option 60 using this command:

```
option 60 ascii "BlueSecure.AP1500"
```

4. Add Option 43 using this command:

```
option 43 hex 7f1c3139322e3136382e3133302e312c463139322e3136382e3133302e32
```

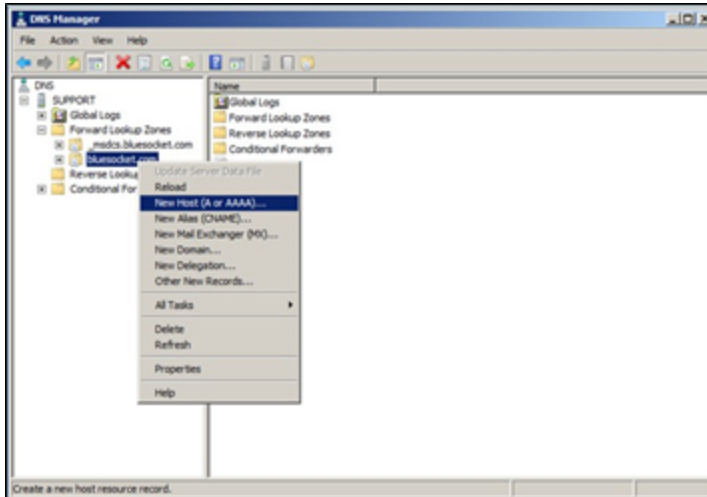
The hexadecimal string in this step is assembled as a sequence of **code/length/value** settings converted to hexadecimal format and separated by colons. For information about these values and their conversion, see [Vendor-Specific Information](#).

Configuring an Entry for AP Discovery in Your Organization DNS Server

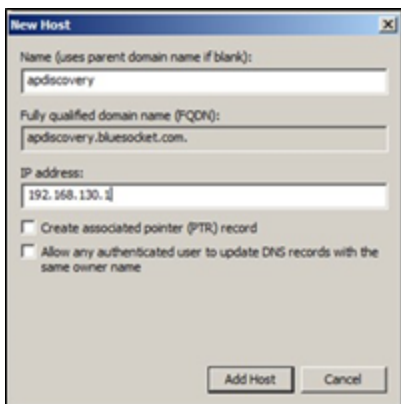
You can configure a host (A) record in your organization DNS server to facilitate AP discovery using the name `apdiscovery` and the public network interface IP address of the primary vWLAN system. When high availability is enabled, the secondary vWLAN system IP address is automatically configured. It is best practice to also configure an A record with the public network interface IP address of the secondary vWLAN system in case the BSAP is unable to obtain a configuration from the primary vWLAN. An associated pointer record (PTR) is not required for AP discovery.

To configure the DNS entry for AP discovery on the Microsoft Windows Server 2008 R2 Enterprise DNS server:

1. In the Windows server, navigate to **Start > Administrative Tools > DNS**.
2. In the left pane of the **DNS Manager** menu, expand the **Forward Lookup Zones** menu, and right-click the appropriate zone. Select **New Host (A or AAAA)**.



3. In the **New Host** menu, specify **apdiscovery** in the **Name** field, and enter the public network interface IP address of the primary vWLAN system. Select **Add Host**.



4. Repeat Steps 2 and 3 to configure the secondary vWLAN system public network interface IP address. The Windows Server 2008 R2 Enterprise is now configured with DNS entries for AP discovery.

Caching a Previously Discovered vWLAN IP Address for AP Discovery

The BSAP remembers or caches the vWLAN public network interface IP address from the last successful AP discovery. We recommend to configure one of the AP discovery methods permanently in the BSAP when used in production. If the BSAP is reset to factory default settings, it will not remember the last discovered vWLAN address. Without one of the AP discovery methods configured, the BSAP will not discover the vWLAN.

You can verify that the BSAP has successfully discovered the vWLAN using the GUI or CLI of the BSAP. To verify that using the GUI:

- Connect to the BSAP GUI and navigate to **Configuration > AP licenses > Platform**. You must have administrative access. The BSAP is automatically displayed in this menu in preparation for licensing, and it will display an associated domain when it successfully discovered vWLAN. If the AP is licensed and assigned a domain, it is also displayed in the GUI under **Configuration > Wireless > Access Points** and **Status > Access Points**.
- If you do not have platform administrative privileges for the vWLAN, but instead have domain administrative access, the AP will not be displayed in any of the previously mentioned menus until a license is uploaded in the **Configuration > Wireless > AP licenses > Domain** menu. Proceed to license the AP and then navigate to **Configuration > Wireless > Access Points** or **Status > Access Points** to verify the AP has discovered the vWLAN.

Verifying BSAP Discovery

To verify that the BSAP has successfully discovered vWLAN using the BSAP CLI:

1. In the BSAP CLI, select option **1** at the **Main Menu** for network configuration.
2. In the **Network Configuration Menu**, select option **8** for network summary information.
3. Verify the vWLAN public network interface IP address is populated under **Controller Address**. For more information, see the *BSAP CLI Reference Guide*.



If a vWLAN is not discovered, the AP attempts to connect to a server at the following IP address: **76.164.174.46**. This server is for future use. If you attempt to connect to a different vWLAN, see [Troubleshooting AP Discovery](#) to determine why the AP did not connect.

When the AP is connected to the vWLAN, it is configured with the default AP template. For more information, see [Licensing APs](#) and [Configuring AP Templates](#).

Troubleshooting AP Discovery

Troubleshooting the BSAP discovery functionality relies upon verifying the ports and protocols allowed between the vWLAN and the BSAPs, the static AP discovery configuration, the DHCP Option 43 configuration, and the DNS configuration. These troubleshooting methods are described in these sections:

Troubleshooting Required TCP or UDP Ports and Protocols	139
Troubleshooting Static AP Discovery	139
Troubleshooting DHCP Option 43 AP Discovery	139
Troubleshooting DNS AP Discovery	140

Troubleshooting Required TCP or UDP Ports and Protocols

Verify that you allow the appropriate ports and protocols in any firewall or ACL between the vWLAN and BSAPs, between the primary and secondary vWLAN systems (when using high availability), between the vWLAN and any authentication servers, between BSAPs when using Layer 3 mobility (tunnelling), and between BSAPs and any authentication servers when using external RADIUS 802.1x authentication. You can configure the firewall or ACL to log dropped packets to verify that all ports or protocols are allowed. If the BSAP is unable to establish a control channel (TCP port 33333) to the vWLAN, it will automatically reboot every 3 minutes until a control channel is established.

Troubleshooting Static AP Discovery

To troubleshoot static AP discovery, log into the BSAP using the CLI and verify that the **Controller Address Mode** is set to **Static** and the **Controller Address** is the appropriate vWLAN public network interface IP address. For more information, see the *BSAP CLI Reference Guide*.

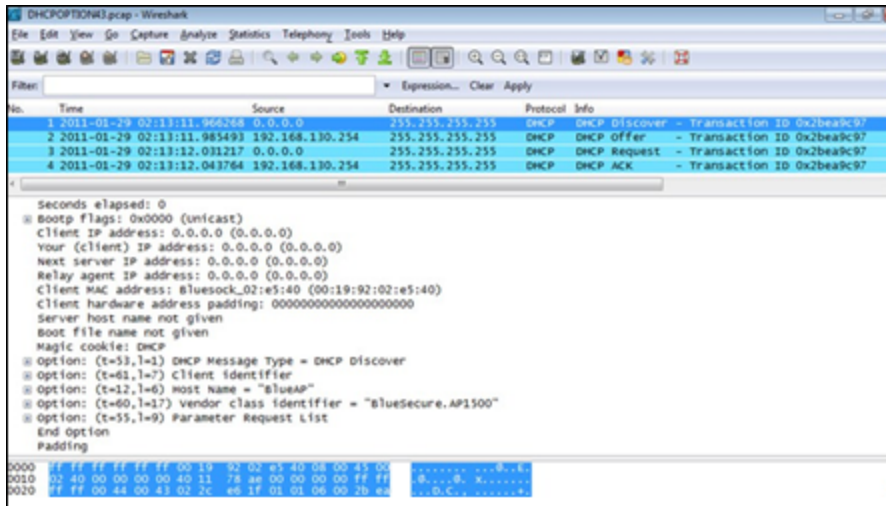
Troubleshooting DHCP Option 43 AP Discovery

To troubleshoot DHCP Option 43 configuration, perform a traffic capture on the wired interface of another BSAP that is in the same subnet of the problem BSAP. Begin the capture and reboot the problem BSAP to capture the broadcast DHCP traffic while the BSAP attempts to obtain an IP address during the boot process. To begin the BSAP traffic capture, connect to the vWLAN GUI and navigate to **Administration > AP Traffic Capture**, or if you use vWLAN release 2.3 or later, navigate to **Administration > Traffic Capture** for vWLAN system information.

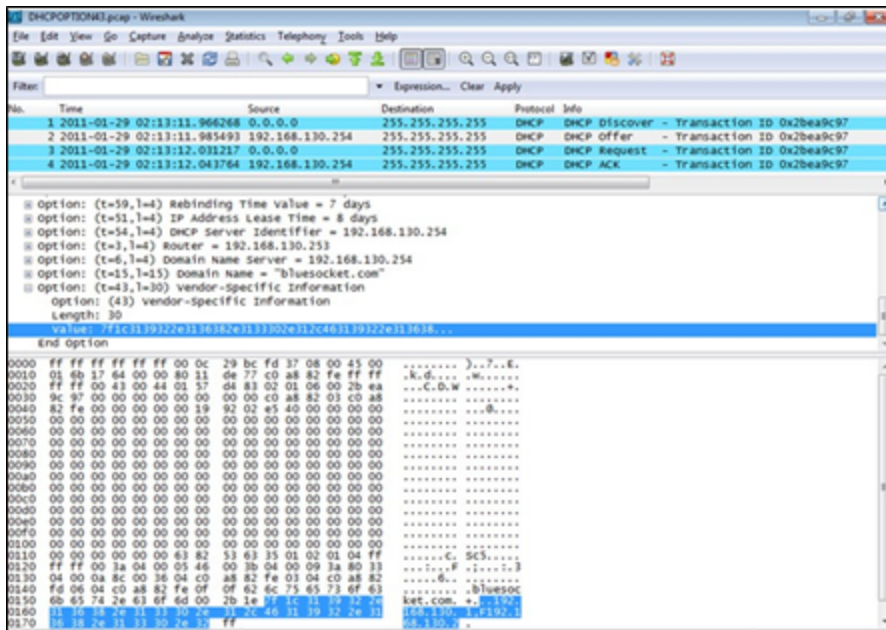
This is an example of a traffic capture on the wired interface of a BSAP that is in the same subnet of the problem BSAP. For static discovery, configure the BSAP in the same subnet of the problem BSAP for the vWLAN to be discovered and used to perform a traffic capture. You can use [Wireshark](#) to open and analyze the traffic capture file.



Analyze the DCHP discovery to make sure that Option 60 from the BSAP includes the appropriate VCI, **BlueSecure.API500**.



Analyze the DHCP Offer from the DHCP server to make sure Option 43 includes the appropriate code, length, or value settings. These settings are converted to hexadecimal format. see [Vendor-Specific Information](#) for more information about hexadecimal format conversion.



If you do not perform a traffic capture using the vWLAN GUI, you have the option to mirror the switchport on which the BSAP is attached and perform a traffic capture there. In addition, you can run a traffic capture on a wired client in the same subnet, run a traffic capture on the gateway, or run a traffic capture on the DHCP server. Verify the Option 60 and Option 43 configurations in all traffic captures.

Troubleshooting DNS AP Discovery

To troubleshoot DNS AP discovery, you can perform a traffic capture. Because DNS does not broadcast traffic, you cannot perform the traffic capture on another BSAP in the same subnet as the problem BSAP. Instead, you can mirror the switchport on which the problem BSAP is attached and perform a traffic capture there, run a traffic capture on a wired client in the same

subnet, run a traffic capture on the gateway, or run a traffic capture on the DNS server. You can then analyze the traffic to make sure the BSAP sends a DNS request for AP discovery, and that the DNS server replies with the public network interface IP address of the vWLAN.

In addition to the traffic capture, you can troubleshoot DNS configuration using a name server (NS) lookup for AP discovery. Enter the `nslookup` command from the command prompt of a wired client in the same subnet as the problem BSAP to verify that the IP address of vWLAN is returned. Make sure that the BSAP is configured to use the same DNS servers as the wired client. For example, enter this command at the command prompt:

```
C:\nslookup apdiscovery
```

You should receive the public network interface IP address of the vWLAN after you enter this command.

Licensing APs

Each AP is licensed for certain features based on its serial number. The AP licenses are the only relevant licenses in vWLAN, and 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.



APs are not 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, and so on.

This section contains these topics:

Obtaining AP Licenses	141
Uploading License Files	141

Obtaining AP Licenses

AP licenses purchased by the customer 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.

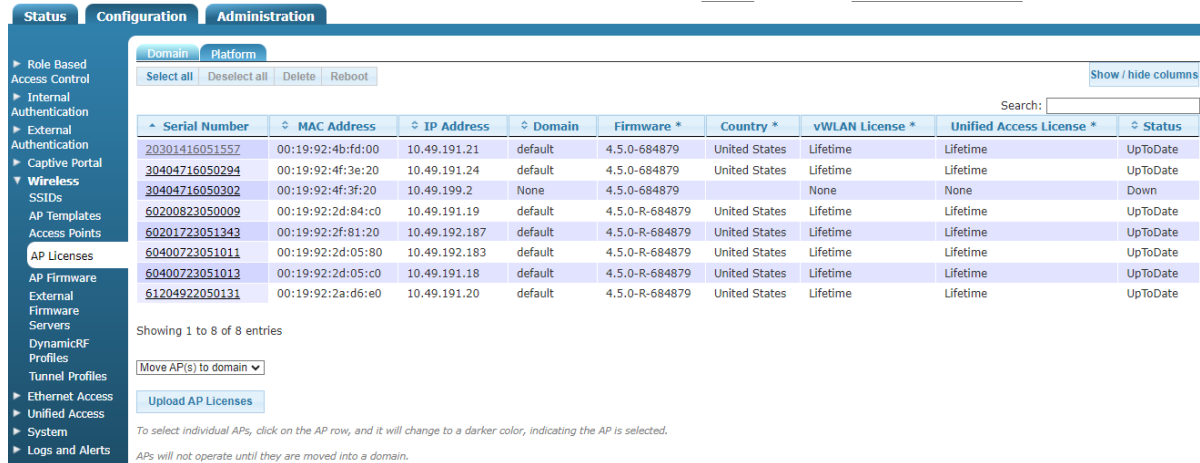
If a license was not received for a new AP, contact the reseller or distributor where the license was purchased. If a license was not received for a replacement AP on an RMA generated by Adtran, contact Adtran Customer Care at 888-423-8726 and reference the RMA number.

Uploading License Files

To upload the license to the APs:

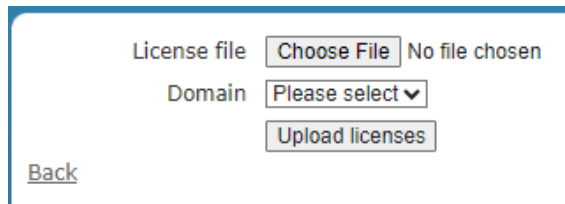
1. When the license file is returned from Adtran, you can upload the license file to vWLAN by navigate to **Configuration > Wireless > AP Licenses**. Select the **Domain** tab if you are working with licenses for APs on a specific domain, or the **Platform** tab if you are working with licenses

on the vWLAN platform and have permission to do so. Click **Upload AP Licenses** at the bottom of the menu.



Serial Number	MAC Address	IP Address	Domain	Firmware *	Country *	vWLAN License *	Unified Access License *	Status
20301416051557	00:19:92:4b:fd:00	10.49.191.21	default	4.5.0-684879	United States	Lifetime	Lifetime	UpToDate
30404716050294	00:19:92:4f:3e:20	10.49.191.24	default	4.5.0-684879	United States	Lifetime	Lifetime	UpToDate
30404716050302	00:19:92:4f:3f:20	10.49.199.2	None	4.5.0-684879	None	None	None	Down
60200823050009	00:19:92:2d:84:c0	10.49.191.19	default	4.5.0-R-684879	United States	Lifetime	Lifetime	UpToDate
60201723051343	00:19:92:2f:81:20	10.49.192.187	default	4.5.0-R-684879	United States	Lifetime	Lifetime	UpToDate
60400723051011	00:19:92:2d:05:80	10.49.192.183	default	4.5.0-R-684879	United States	Lifetime	Lifetime	UpToDate
60400723051013	00:19:92:2d:05:c0	10.49.191.18	default	4.5.0-R-684879	United States	Lifetime	Lifetime	UpToDate
61204922050131	00:19:92:2a:d6:e0	10.49.191.20	default	4.5.0-R-684879	United States	Lifetime	Lifetime	UpToDate

2. Locate the appropriate license file returned to you from Adtran using the **Choose File** button. Specify the domain to which the license file will apply from the **Domain** field. Then click **Upload Licenses**.



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 templates.

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, 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/ax (2.4 GHz) radio is set to the **802.11b/g/n/ax** wireless mode, and the 802.11a/n/ac/ax (5 GHz) radio is set to the **802.11a/n/ac/ax** 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 **vWl@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.

This section contains these topics:

Creating AP Templates	143
Configuring vWLAN for CNA Support	151
Configuring DFS for vWLAN	153
Mesh Networking in vWLAN	164
Configuring DynamicRF for vWLAN	178
Applying the AP Template to AP(s)	194

Creating AP Templates

Depending on the role the AP plays 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:

1. Navigate to **Configuration > 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** menu at the top of the GUI.
 - To edit the default AP template, select the default template from the list.

Name	Created Time
421	2024-10-01 14:35:49
default	2022-12-30 02:06:23



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. Enter the name, SSH password, login form, and DNS servers (for NAC and CNA users) for the template in the appropriate fields.

Create AP Template

Name

SSH Password

SSH Password Confirmation

Login Form

DNS Server(s) For NAC Users

Leave blank to use the DNS server from the APs Native VLAN.
A maximum of two DNS servers can be added separated by a comma.

Timezone

Release	Server
1920/1925 Firmware <input type="text"/>	<input type="text" value="vWLAN"/>
1930/1935/1940 Firmware <input type="text"/>	<input type="text" value="vWLAN"/>
2020 Firmware <input type="text"/>	<input type="text" value="vWLAN"/>
2030/2035/2135 Firmware <input type="text"/>	<input type="text" value="vWLAN"/>
3040/3045 Firmware <input type="text"/>	<input type="text" value="vWLAN"/>
6020 Firmware <input type="text"/>	<input type="text" value="vWLAN"/>
6120 Firmware <input type="text"/>	<input type="text" value="vWLAN"/>
6040 Firmware <input type="text"/>	<input type="text" value="vWLAN"/>

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 SSH password is the password used to connect to the AP serial console menu. The login form is the form used by clients when connecting to the AP. Make sure that the form is not overridden at the SSID. You can choose the default login form, or select a custom form. See [Customizing vWLAN Login Forms and Images](#) for information.

3. Specify the timezone used by the APs associated with this template by selecting the appropriate option from the **Timezone** field. 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).
4. Specify whether you use Apple CNA and Microsoft Network Connectivity Status Indicator (NCSI). This option allows remote devices to store the credentials to networks requiring captive portal authentication so you do not need to enter it 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** field.

When CNA is enabled, vWLAN responds to the device 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 you open a web browser to authenticate.

For CNA to function properly, a few additional configuration steps are required. See [Configuring vWLAN for CNA Support](#).

- 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 field, 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.

Enable L3 Mobility	<input checked="" type="checkbox"/>	<i>Check to Enable L3 mobility on APs assigned to this template. Enabling L3 mobility enables an AP from tunneling a roamed client traffic to home agent.</i>
Enable DFS	<input type="checkbox"/>	
Scan for Adjacent Wireless Clients	<input type="checkbox"/>	<i>Supported only on BSAP 2000 series.</i>
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>
LAN Profile	Disabled	<i>Eth Port is disabled when LanProfile value is Disabled</i>

Per Radio Setting	
Attribute	802.11b/g/n/ax (2.4 GHz)
Radio Mode	AP/Sensor Client Aware Mode
DynamicRF Profile	default
Wireless Mode	802.11b/g/n/ax
Minimum Transmit Rate	No Minimum
Channel Width	20 MHz

Attribute	802.11a/n/ac/ax (5 GHz)
Radio Mode	AP/Sensor Client Aware Mode
DynamicRF Profile	default
Wireless Mode	802.11a/n/ac/ax
Minimum Transmit Rate	No Minimum
Channel Width	40 MHz

- Specify whether APs associated with this template use DFS channels (5 GHz radio only). DFS channels are those channels that radar could use and this way are 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** field to enable the DFS feature.



DFS can cause service interruptions when the AP is required to vacate a channel on which radar was 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, see [Configuring DFS for vWLAN](#).

- Use the **Tunnel Profile** field 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, see [Configuring a Tunnel Profile](#).



If a tunnel profile is enabled, Layer 3 Mobility automatically disables. In addition, there are interactions between a tunnel profile and a defined user role. See [Configuring a Tunnel Profile](#) for more information.

8. Use the **LAN Profile** field to enable the LAN-2 port on the AP, allowing wired devices to access the Internet. By default, this setting is disabled, which indicates that the LAN-2 port is disabled. For more information, see [Configuring a LAN Profile](#).



LAN profiles are supported only on the 2030 and 3040 APs.

9. Specify the radio mode for both radios in the AP by selecting the appropriate option from the **Radio Mode** field. The radio modes are set independently for each radio. By default, the radio is set to **AP Mode**.



The 3000 series, 6040, and 6120 APs always operate in AP mode and have a dedicated third scanning radio. The 6020 APs do not have this scanning radio.

You can choose one of these settings:

- **Disabled** indicates that the radio is disabled.
- **AP Mode** (default) indicates that the radio services clients in the 802.11 infrastructure mode.
- **Sensor Mode** indicates that the radio scans all channels, changing on the particular band at 100 ms intervals.
- **AP/Sensor Mode** indicates that 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 that 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 that 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, see [Mesh Networking in vWLAN](#).



The Mesh networking support is not available for BSAP 3000 and 6000 series.



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 might cause traffic disruption. For more information, see [Configuring DFS for vWLAN](#).



Dual mode for 1900 Series and 2000 Series APs acts as AP mode.

10. Select the DynamicRF profile from the **DynamicRF Profile** field. The **default** profile appears in this list, as well as any other profiles that you created. Make selections for both the 2.4 GHz and 5 GHz radios. See [Configuring the DynamicRF Profile](#).
11. Specify the wireless mode for each radio by choosing an option from the **Wireless Mode** list. For the 802.11b/g/n/ax (2.4 GHz) radio, you can select from **802.11b**, **802.11g**, **802.11g/n**, **802.11b/g/n**, or **802.11b/g/n/ax** (default) modes. **802.11b/g/ax** is supported only for 6000 series APs.
For the 802.11a/n/ac/ax (5 GHz) radio, you can select from **802.11a**, **802.11a/n**, **802.11a/n/ac**, or **802.11a/n/ac/ax** (default) modes. **802.11a/n/ac/ax** is treated as **802.11a/n** for 1900 series APs and **802.11ac** for 2000 and 3000 series APs. **802.11a/n/ax** is supported only for 6000 series APs.
12. Specify the minimum transmit rate for each radio from the **Minimum Transmit Rate** field. 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.



For the 2030 Series APs, any value specified is treated as **No Minimum**.

Continue with these steps:

1. Specify the channel width for each radio using the list. 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 list. 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.



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.

2. 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.

The screenshot displays the 'Channel list' configuration section. It features two columns of channel numbers. The left column shows channels 1, 10, 11, 12, 13, 2, 3, and 4, each with a minus sign to its left, indicating they are included. The right column is empty, indicating no channels are excluded. Below the columns are two buttons: 'Remove all' and 'Add all'. Below the channel list, there is explanatory text: '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.'

Below the channel list, there are several configuration fields:

- Enable Packet Aggregation:** A checked checkbox.
- Beacon Interval (ms):** A text input field containing '200'.
- Max Associations Load:** A text input field containing '64'.
- DTIM:** A text input field containing '1'.
- Fragmentation Threshold:** A text input field containing '2346'.
- RTS Threshold:** A text input field containing '2346'.

Below these fields, there is explanatory text: 'Send broadcast and multicast every (DTIM * beacon interval), values (1-255). Packet length for fragmentation, values (256-2346 bytes). Packet length when RTS/CTS are used, values (256-2346 bytes).'

3. Enable or disable packet aggregation on each radio by selecting the **Enable Packet Aggregation** field. By default, packet aggregation is enabled on both radios.
4. 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.
5. 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.
6. 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**.
7. 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.
8. 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.

9. Select the antenna mode for each radio. Choose from **1**, **2**, or **3** antennas.

The screenshot shows two side-by-side configuration panels for radio settings. Each panel has an 'Antenna Mode' section with radio buttons for 1, 2, 3, and 4 antennas. In the left panel, '4 Antennas' is selected. Below this is a 'SSIDs' section with a search bar, '0 items selected', 'Remove all', and 'Add all' buttons. A dropdown menu is open showing '+ 421'. Below the SSIDs is a 'Unified Access Groups' section with similar controls. At the bottom of the left panel is a 'Create AP Template' button. The right panel is identical but has '1 Antenna' selected.



This setting only applies when configured to a number less than the number of antennas supported by the AP.

10. Specify the SSIDs that you want to associate 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, see [Configuring an SSID](#).



SSIDs cannot be specified for a radio in **Mesh Mode**.

11. Specify the unified access groups that you want to associate 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, see [Configuring Unified Access Groups](#).



Unified access groups cannot be specified for an AP with a radio in **Mesh Mode**.



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.

12. Click **Create AP Template**.

A confirmation is displayed indicating the AP template was successfully created.

Configuring a LAN Profile

You can use a LAN profile to enable the LAN-2 port on the AP, allowing wired devices to access the Internet. The AP authenticates the wired device connected the LAN-2 port using the MacAuthBypass server. Based on the device MAC-address, the server assigns a VLAN for the connected device.



LAN profiles are supported only on the 2030 and 3040 APs.

To configure a LAN profile:

1. Navigate to **Configuration > Ethernet Access > LAN Profiles**.
 - To create a new LAN profile, click **Create LAN Profile** at the bottom of the menu.
 - To edit a previously created LAN profile, select the profile from the list.

2. Enter a name for the LAN profile. The **Enable RadiusMACAuthBypass** field is selected by default.

Create LAN Profile

Profile Name

Enable RadiusMACAuthBypass

MacAuthBypass Server

Access Mode

In Single Client Mode, AP authenticates only one wired client, other clients are permitted to access LAN-2 port without further authentication.

[Back](#)

3. Select the **MacAuthBypass Server** that you want to use for authenticating the connected device. By default, **Access Mode** is set to **Single Client Mode**. In this mode, AP authenticates only one wired device, other devices are permitted to access the LAN-2 port without further authentication.
4. Click **Create Lan Profile**.

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. You must load a custom certificate on vWLAN because CNA has no method to allow the user that is accessing the network to accept the certificate. In addition, configure vWLAN to redirect to a host name and then configure a DNS server and hostname. Complete these configurations before applying the AP template to any APs.

To configure vWLAN for CNA support:

1. Enable vWLAN to redirect to a host name by navigating to **Configuration > System > Settings**, and then select the **Platform** tab. Select the **Redirect to hostname** setting from the list.

The screenshot shows the 'Platform' tab in the configuration interface. The table below represents the data visible in the table:

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?	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.

2. Select **Enabled** from the **Redirect to hostname** to field, and then click **Update Platform Setting**. You will receive confirmation that the setting was changed.

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.

3. 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 > System > Settings**, and then select the **Platform** tab. Upload the certificate as directed in [Managing vWLAN Certificate Settings](#). Make sure to save the setting.

- In the AP template under **Configuration > 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. After you made the changes to the template, click **Create AP Template** or **Update AP Template**. Remember that all APs that use this template will also be updated.

Create AP Template

Name

SSH Password

SSH Password Confirmation

Login Form

DNS Server(s) For NAC Users

Leave blank to use the DNS server from the APs Native VLAN.
A maximum of two DNS servers can be added separated by a comma.

Timezone

	Release	Server
1920/1925 Firmware	<input type="text"/>	<input type="text" value="vWLAN"/>
1930/1935/1940 Firmware	<input type="text"/>	<input type="text" value="vWLAN"/>
2020 Firmware	<input type="text"/>	<input type="text" value="vWLAN"/>
2030/2035/2135 Firmware	<input type="text"/>	<input type="text" value="vWLAN"/>
3040/3045 Firmware	<input type="text"/>	<input type="text" value="vWLAN"/>
6020 Firmware	<input type="text"/>	<input type="text" value="vWLAN"/>
6120 Firmware	<input type="text"/>	<input type="text" value="vWLAN"/>
6040 Firmware	<input type="text"/>	<input type="text" value="vWLAN"/>

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.

- Change the network interface host name setting. Navigate to **Configuration > System > Network Interfaces**. Select the **public** interface from the list.

6. Enter the host name in the **Hostname** field and click **Update Network Interface**. Restart the vWLAN for the changes to take effect.

Edit Network Interface

Name public
 Current Address 10.49.182.201
 Current Netmask 255.255.255.0
 Current Gateway 10.49.182.254

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

Static Routes

Static routes manipulate the vWLAN's IP routing table. Their primary use is to set up static routes to specific hosts or networks via an interface.

The parameters that apply to the static routes are:

- Destination: Target destination network or host. You can provide IP addresses in dotted decimal.
- Netmask: For a host route, specify a netmask of 255.255.255.255.
- Gateway: Route packets via a gateway. NOTE: The specified gateway must be reachable first and the gateway needs to be on the same subnet as the interface.

Destination	Netmask	Gateway	
<input type="text" value="destination"/>	<input type="text" value="netmask"/>	<input type="text" value="gateway"/>	
<input type="text" value="destination"/>	<input type="text" value="netmask"/>	<input type="text" value="gateway"/>	
<input type="text" value="destination"/>	<input type="text" value="netmask"/>	<input type="text" value="gateway"/>	

[Append Static Route](#)

[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 DFS for vWLAN

This section contains these topics:

DFS Overview	153
System Requirements and Limitations	154
Configuring DFS	157
DFS Troubleshooting in vWLAN	161

DFS Overview

Dynamic frequency selection (DFS) is a feature of the 802.11h protocol that allows wireless local area networks (WLANs) to operate on the same 5 GHz channels used by radar systems. When enabled, DFS causes the access point (AP) to continually search for radar pulses in the frequency channel in which it is operating. If radar is detected, the AP discontinues operation on that channel and searches for a new channel without detected radar. DFS is required for European 5 GHz outdoor vWLAN deployments, and without DFS, European 5 GHz indoor AP channels are limited to only four channels. The major benefit to using DFS is more channel availability, which results in more user capacity for high density deployments, less interference, higher throughput, and improved performance.

When DFS is enabled in vWLAN, the vWLAN system coordinates the channel selection of APs to ensure optimal channel occupancy and that APs use only the approved channels. vWLAN operates in this manner when using DFS:

1. The AP connects to the network (whether internal network or the Internet).
2. The AP discovers vWLAN via AP discovery.
3. vWLAN determines the country for which the AP is licensed, and the DFS domain for the AP is determined.
4. The default AP template is applied to the AP, and the AP enters channel scanning mode. This step detects RF neighbors for roaming and optimal channel and power settings. It is important to note that DFS channels (those with possible radar interference) are only scanned during the initial scanning period, and active AP beaconing is only done on non-DFS channels.
5. Once the channel scanning is complete, vWLAN decides which channel is optimal for the AP. This channel will most likely be a DFS channel (when DFS is enabled).
6. After a 60 second channel availability check, if no radar is detected, the channel is assigned and the AP begins allowing traffic to pass.

If radar is detected, the AP immediately looks for another channel without radar interference. The AP stays off the channel on which radar was detected for 30 minutes.

The method used by the AP when it changes channels due to radar detection operates as follows:

1. If the AP detects radar on the current channel, it stops data service to connected clients within 200 ms. This channel is added to the blocked channel list on the AP for 30 minutes.
2. The AP then moves to a new channel within 10 seconds. During this time, the AP can transmit data for an aggregated time period of 60 ms. The AP sends a channel switch announcement (CSA) to the connected clients so they are aware of the channel change and do not attempt to probe to find a new channel.
3. The AP changes to a new channel and monitors the new channel for radar signals for 60 seconds. If radar is detected, the AP changes channels again and begins the process over. If no radar is detected, the new channel is broadcast to the clients.

System Requirements and Limitations

This section describes DFS configuration for vWLAN 1900 Series APs running vWLAN software versions 2.6 and AP firmware 7.0.0 or later, and vWLAN 2000 and 2100 Series APs running vWLAN software versions 3.1.0 and later.

For firmware release 2.6, DFS is supported natively on the BSAP 1925, 1935, and 1940 Series hardware. The BSAP 1920 and 1930 Series products will support DFS if they are using hardware revision K or higher. Each 192x and 193x Series unit that supports DFS is shipped with a "DFS Hardware Ready" sticker, as appears below, on the box and on the AP.

Figure 7: DFS Hardware Ready

For firmware release 3.1.0, DFS is supported natively on the BSAP 2020 and 2100 Series hardware in European countries.

For firmware release 3.3.0, DFS is additionally supported on the BSAP 203x Series hardware in European countries, and the BSAP 2100, 203x, and 304x Series hardware in the United States.

The AP firmware version determines whether DFS operation is allowed for the BSAP licensed in a specific area. The following outlines the DFS support for APs licensed in European countries and the United States:

- Firmware release 2.6 allows for DFS operation with 1900 Series APs licensed in a European country only.
- Firmware release 3.1.0 allows for DFS operation with 2020 and 2100 Series APs licensed in a European country only.
- Firmware release 3.3.0 allows for DFS operation with 2135, 203x Series, and 304x Series APs licensed in a European country, and 2135 and 203x Series APs licensed in the United States.

DFS channels are only available on clients that support them. If a client does not support DFS channels, it will not scan them and therefore will not see the service set identifier (SSID) associated with those channels.

This section contains these topics:

DFS and Channel Selection	155
Channel Bonding Support	156
DFS and Mesh Networking	156

DFS and Channel Selection

When an AP detects a radar signal on its current channel, it switches to a new channel. The new channel will always be in the same channel width, for example, 40 MHz. The set of channels considered by the AP include DFS channels when DFS is supported and enabled. The list of valid channels available to the AP include the DFS channels for the country in which the AP is licensed. The blocked channel list includes any channels on which the AP recently detected radar (or which are explicitly blocked by an administrator).

For European countries, supported DFS channels are:

- 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.
- Channels 36 to 48 and 52 to 64 are not allowed in outdoor deployments.

Channel Bonding Support

APs supporting 802.11n 40 MHz mode use two channels at once. In 40 MHz, the AP radio uses two adjacent 20 MHz channels. In the 5.0 GHz spectrum, strict channel pairing is enforced, for example, channel 40 can only be paired with 36 and not with 44. These pairs are independent of the country of operation as long as both channels in the pair are valid for the country. When using DFS in the 40 MHz mode, the AP monitors both channels in the pair for radar interference and leaves both channels immediately if radar is detected on one of the channels. The same requirement applies when using 80 MHz, where four channels are used. If a DFS channel that does not have a 40 MHz pair is manually selected for the AP, the vWLAN system will dial the AP back to 20 MHz mode for that AP. Dynamic RF will always select a 40 MHz channel when the AP is configured for 40 MHz.

DFS and Mesh Networking

When using mesh networking with DFS enabled, it is important to note that each part of the mesh network must check the channel for radar before it can support downstream mesh points. For a single hop mesh network, this means that it will take 60 seconds before the mesh point transmits traffic after the mesh portal has connected. For a two hop mesh network, this delay grows to 120 seconds.

If a mesh portal detects radar on its current channel, it must vacate the channel. The mesh portal issues a channel switch announcement, causing any associated mesh points to disconnect. If a mesh point detects radar on its current channel, a channel switch announcement is issued, and that portion of the mesh network and any downstream mesh points are disconnected. At this point, the vWLAN system will move the mesh portal to a new channel.

If a mesh uplink (mesh portal or mesh point servicing downstream mesh points) detects radar on its current channel, it stops data services to connected clients within 200 ms and issues a channel switch announcement. It then moves to a new channel within 10 seconds of the radar detection event. During this 10 second time period, the device can transmit data as many times as necessary for an aggregated time period of 60 ms. Once the device moves to a new channel, it must monitor the new channel for radar signals for the next 60 seconds (if the channel is a DFS channel). If it detects radar on the new channel, the process begins again.

If a mesh device downstream detects radar on its current channel, it communicates the radar detection event to the mesh device upstream to which it is connected. When the upstream portal device receives the radar detection event from the downstream device, it reacts as if it detected the radar, issues a channel switch announcement, and proceeds to change channels.

Only a single channel is configured for a mesh portal. If the mesh portal detects radar interference, it will move channels. The channel block list applies only to the mesh portal and not the mesh point. If the mesh portal and mesh points use different AP templates, only the mesh portal template block list applies.

Mesh portals change channels in only two cases: the administrator changes the mesh portal channel, or radar is detected. Mesh points change channels in only two cases as well: if the upstream mesh device changes channels or if the upstream devices changes channels because radar is detected.

Configuring DFS

You can configure DFS in vWLAN using the AP template and the AP configurations. These topics describe the necessary AP configuration to enable and use DFS:

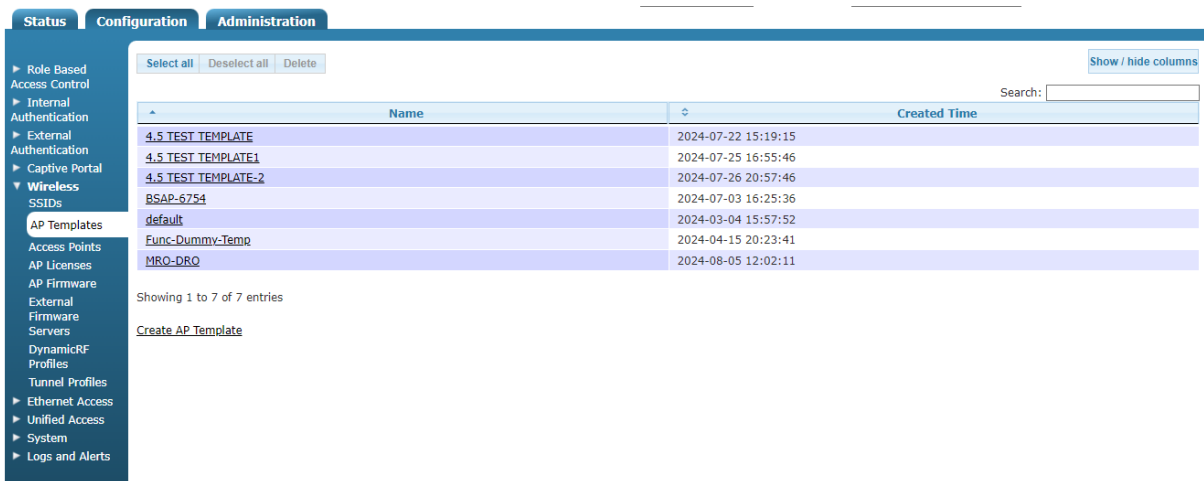
- Configuring the AP Template for DFS157
- Configuring the AP for DFS160


Configuring the AP Template for DFS

The vWLAN administrator can choose for APs to use DFS channels by configuring the AP template to allow it. Each AP template contains a field that enables or disables DFS. By default, DFS is disabled. Once DFS is enabled, you can optionally specify whether the AP uses special channels (such as channels that are only permitted on APs far enough away from weather radar or channels in certain countries that are only permitted for indoor use).

To configure the AP template for DFS:

1. Navigate to **Configuration > Wireless > AP Templates**. The first time you access this menu, the only AP template available is 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** menu at the top of the GUI. To edit the default AP template, select the default template from the list.



 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. Enable DFS in the AP template by selecting the **Enable DFS** field.

Edit AP Template

Name	Default	
SSH Password	*****	
SSH Password Confirmation	*****	
Login Form	Default Login Form ▼	
DNS Server(s) For NAC Users	<input type="text"/>	
	<small>Leave blank to use the DNS server from the APs Native VLAN. A maximum of two DNS servers can be added separated by a comma.</small>	
Timezone	(GMT+00:00) UTC ▼	
	Release	Server
1920/1925 Firmware	4.5-M-684063 ▼	vWLAN ▼
1930/1935/1940 Firmware	4.5-M-684063 ▼	vWLAN ▼
2020 Firmware	4.5-M-684063 ▼	vWLAN ▼
2030/2035/2135 Firmware	4.5-M-684063 ▼	vWLAN ▼
3040/3045 Firmware	4.5-M-684063 ▼	vWLAN ▼
6020 Firmware	4.5.0-M-684063 ▼	vWLAN ▼
6120 Firmware	4.5.0-M-684063 ▼	vWLAN ▼
6040 Firmware	4.5.0-M-684063 ▼	vWLAN ▼
Enable Captive Network Assistant	<input checked="" type="checkbox"/>	
	<small>Check to enable Apple CNA or Microsoft NCSI. *Requires Trusted Certificate on vWLAN. *Requires redirect to hostname to be enabled in platform settings.</small>	
Enable L3 Mobility	<input checked="" type="checkbox"/>	
	<small>Check to Enable L3 mobility on APs assigned to this template. Enabling L3 mobility enables an AP from tunneling a roamed client traffic to home agent.</small>	
Enable DFS	<input type="checkbox"/>	

- Optionally specify whether the AP uses special channels (such as channels that are only permitted on APs far enough away from weather radar or channels in certain countries that are only permitted for indoor use). Available DFS channels are listed in [DFS and Channel Selection](#).

To specify a specific channel for the AP, under the **Per Radio Setting** menu, click **Channel list**. Specify that a channel is allowed by clicking and dragging the channel to the allowed list column (on the left). Specify that a specific channel cannot be used by the AP by clicking and dragging the channel to the blocked list column (on the right).

Selected channels are only included if they are legal in the regulatory domain. When a selected channel is blocked, all APs in the template that are using that channel (either as a primary or bonded channel) will automatically pick new channels.

Per Radio Setting

Attribute **802.11b/g/n/ax (2.4 GHz)**

Radio Mode **AP/Sensor Client Aware Mode**
3xxx and 6xxx series BSAP's always operates in AP mode and have a dedicated 3rd scanning radio. The scanning radio is not available on the 6020 AP's.

DynamicRF Profile **default**

Wireless Mode **802.11b/g/n/ax**

Minimum Transmit Rate **No Minimum**
802.11b/g/ax is supported only for 6000 series APs.
For 3000/6000 Series APs, any value is treated as 'No Minimum'.
Minimum Transmit Rate is supported only for 1900 series APs.

Channel Width **20 MHz**

Channel list ⊕

0 items selected Remove all Add all

- 1
- 10
- 11
- 12
- 13
- 2
- 3
- 4

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.

802.11a/n/ac/ax (5 GHz)

Radio Mode **AP/Sensor Client Aware Mode**
3xxx and 6xxx series BSAP's always operates in AP mode and have a dedicated 3rd scanning radio. The scanning radio is not available on the 6020 AP's.

DynamicRF Profile **default**

Wireless Mode **802.11a/n/ac/ax**

Minimum Transmit Rate **No Minimum**
802.11a/n/ac is treated as 802.11a/n for 1800 and 1900 series APs.
802.11a/n/ax is supported only for 6000 series APs.
For 2000/3000/6000 Series APs, any value is treated as 'No Minimum'.
Minimum Transmit Rate is supported only for 1900 series APs.


Channel Width **40 MHz**

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.

0 items selected Remove all Add all

- 132
- 136
- 140
- 149
- 153
- 157
- 161
- 165

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 regulators. Channels 52, 56, 60 and 64 are valid even if DFS is disabled for some regulators and the AP channel list is populated as per regulatory domain.

- As of vWLAN firmware release 3.1.0, the configuration of channels used on a per-radio basis configures the channels used for both DFS and DynamicRF.
 - The channels listed are a generic channel list valid for all the regulatory domains. Channels 52, 56, 60, and 64 are valid even if DFS is disabled for some regulatory domains and the AP channel list is populated as per regulatory domain.
- 

 - If there are associated APs that are set with the channel, or use the channel for 40 MHz or 80 MHz mode, the next time DynamicRF runs it changes the APs to not use the specified channel. For 40 MHz mode, this implies that blocking channel 36 also blocks channel 40. For 80 MHz mode, this implies that blocking channel 100 also blocks channels 104, 108, and 112.
 - 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.

4. Click **Create AP Template** or **Update AP Template** if no other changes are needed for the AP template.

Once the template was created or updated, you must apply it to the APs for the changes to take effect.

Configuring the AP for DFS

In addition to DFS configuration in the AP template, you can also configure DFS channels in the AP configuration. If the AP platform supports DFS, and it is enabled in the AP template, you can choose to select a DFS channel for the 5 GHz radio.

To configure DFS settings for an AP:

1. Navigate to **Configuration > Wireless > Access Points**. This menu lists any configured APs. Select the AP from the list.

Name	SysLocation	AP MAC	Mesh Portal	Ip Address	Serial Number	AP Template	Uptime	Locations	Firmware	Channel (Channel Width)	TX Power
BSAP2030-00-19-92-4b-fd-00		00:19:92:4b:fd:00		10.49.191.26	20301416051557	default	5d, 0h, 52m	vLoc-0-10.49.191.0/24	4.5-M-684063	2.4GHz=Sensor (20 MHz) 5GHz=Sensor (40 MHz)	2.4 GHz+ dBm 5 GHz+ dBm
BSAP3040-00-19-92-4f-3e-00		00:19:92:4f:3e:00		10.49.191.24	30404716050293	default	5d, 0h, 51m	vLoc-0-10.49.191.0/24	4.5-M-684063	2.4GHz=Sensor (20 MHz) 5GHz=Sensor (40 MHz)	2.4 GHz+ dBm 5 GHz+ dBm
BSAP6020-00-19-92-4f-3e-00		00:19:92:2d:84:c0		10.49.191.27	60200823050009	default	5d, 0h, 53m	vLoc-0-10.49.191.0/24	4.5.0-M-684063	2.4GHz=Sensor (20 MHz) 5GHz=Sensor	2.4 GHz+ dBm 5 GHz+ dBm

2. Specify the channel used by each radio from the **Channel** fields. 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 might 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 a specific channel for the AP, select the appropriate option from the list. If DFS is supported by the AP platform and enabled in the AP template, DFS channels are available for selection on the 5 GHz radio.



Channels 120 through 128 are not available for European countries for DFS functionality due to a 10 minute channel availability check. In addition, channel 116 is not available for 40 MHz mode.

3. Specify whether the AP is an indoor or outdoor AP. By default, the AP is listed as indoor or outdoor based on the AP serial number. If indoor is selected, all channels are available for the AP. If outdoor is selected, only the outdoor channels are available for the AP.

Edit Access Point

Serial Number

AP MAC Address

Country

Name

SysLocation

Location

Access Point Template

Changing AP template may set 5Ghz channel to Auto. Please reconfigure if needed.

Installed

Per Radio Settings

	802.11b/g/n/ax (2.4 GHz)	802.11a/n/ac/ax (5 GHz)
Channel	<input type="text" value="Auto (11)"/>	<input type="text" value="Auto (149)"/>
Transmit Power	<input type="text" value="Auto (10 dBm [10 mW])"/>	<input type="text" value="Auto (26 dBm [400 mW])"/>
Antenna Gain (dBi)	<input type="text" value="4"/>	<input type="text" value="5"/>

- Click **Update Access Point**. You will then need to manually apply the changes to the AP using the domain task link at the top of the vWLAN GUI.
 With modification of the AP template and the AP channel selection, DFS is enabled and configured for vWLAN.

DFS Troubleshooting in vWLAN


Within vWLAN, there are information messages, event reports, and status information that you can use to confirm DFS configuration. This section contains these topics:

Information Messages	161
Viewing AP Details	163

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.

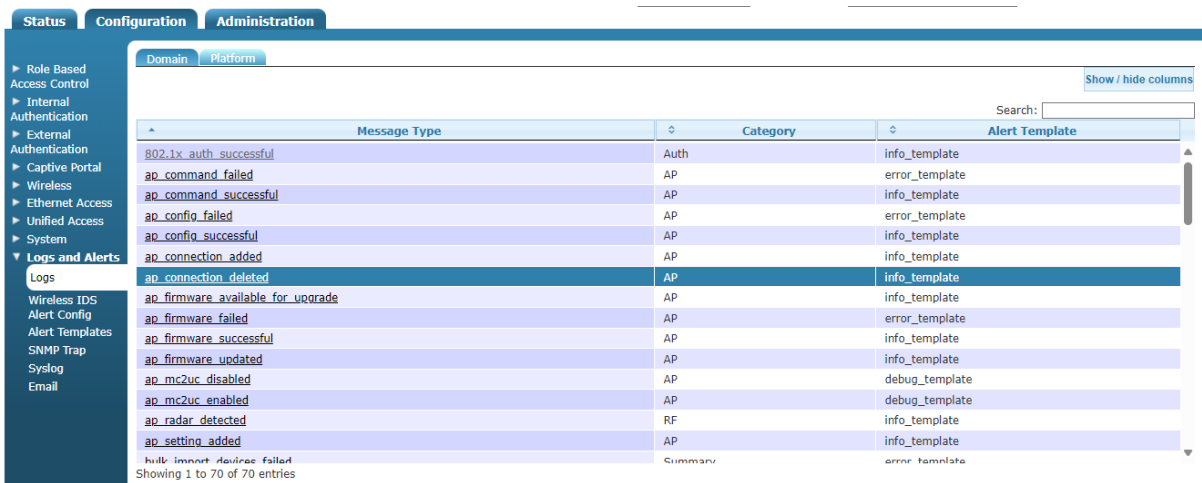
Information messages are error, information, or debug messages and are classified using the notification template. In addition, information messages can track any configuration changes (creations, deletions, or updates) and who authorized the change. Notification templates determine information message types, which allow you to classify the information notifications as you prefer.

 For more information, see [Creating Alert Templates and Log Messages](#).

The administrators cannot create information messages. Instead, they create notification templates that classify the message type when the specified events occur. You cannot delete information messages, but you can edit the type of template to which they are associated.

To view information messages:

1. Navigate to **Configuration > Notifications > Info Messages**. Select the **Domain** tab if you work with messages for a specific domain or select the **Platform** tab if you work with messages for the vWLAN system. DFS messages are at the domain level. The generated messages are listed and include the product with which the message is associated (AP, vWLAN, and so on), the message type (action that generated the message), and the notification template associated with the message (info, error, and so on).



Message Type	Category	Alert 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_available_for_upgrade	AP	info_template
ap_firmware_failed	AP	error_template
ap_firmware_successful	AP	info_template
ap_firmware_updated	AP	info_template
ap_mc2uc_disabled	AP	debug_template
ap_mc2uc_enabled	AP	debug_template
ap_radar_detected	RF	info_template
ap_setting_added	AP	info_template

By default, DFS information messages are associated with the Info Notification template (which generates a log message).

2. Select the message from the list to edit the type of template associated with a specific message. Select the notification template to associate with the message from the list. Available notification templates include error, info, and debug templates (by default), and any additional templates you created. Click **Update Info Message** to apply the template change.

Edit Info Message

Category **Auth**

Message Type **802.1x_auth_successful**

Alert Template **info_template** ▼

Update Info Message

[Back](#)

Viewing AP Details

Viewing the details of an AP allows you to verify its configuration. To view the details of a particular AP configuration, navigate to **Status > Access Points**. This menu lists each configured AP. Select the AP you want to view from the list.

Name	SysLocation	MAC Address	Mesh Portal	Serial Number	IP Address	Uptime	Locations *	Firmware *	Channel (Channel Width)	TX Power *	Total Clients
BSAP2030-00-19-92-4b-fd-00		00:19:92:4b:fd:00		20301416051557	10.49.191.26	5d, 1h, 2m	vLoc-0-10.49.191.0/24	4.5-M-684063	2.4GHz=Sensor (20 MHz) 5GHz=Sensor (40 MHz)	2.4 GHz = 30 dBm 5GHz=30 dBm	0
BSAP3040-00-19-92-4f-3e-00		00:19:92:4f:3e:00		30404716050293	10.49.191.24	5d, 1h, 1m	vLoc-0-10.49.191.0/24	4.5-M-684063	2.4GHz=Sensor (20 MHz) 5GHz=Sensor (40 MHz)	2.4 GHz = 30 dBm 5GHz=30 dBm	0
BSAP6020-00-19-92-2d-84-c0		00:19:92:2d:84:c0		60200823050009	10.49.191.27	5d, 1h, 2m	vLoc-0-10.49.191.0/24	4.5.0-M-684063	2.4GHz=Sensor (20 MHz) 5GHz=Sensor (40 MHz)	2.4 GHz = 0 dBm 5GHz=0 dBm	0

The details of the selected AP are displayed, including the AP configuration, radio interfaces, any associated clients, and any configured SSIDs associated with the AP. In addition, from this menu you can select to view maps, logs, alarms, alerts, and APs adjacent to the selected AP by using the links at the top right of the menu. These links bring up the view, specifically filtered by the AP in question.

Access Point Details

Name BSAP3040-00-19-92-4F-3e-20	Model BSAP-3040	Edit Configuration
SysLocation	DFS Hardware Ready Yes	Not on a map yet
MAC Address 00:19:92:4f:3e:20	Firmware 4.5.0-684879	Logs
Uptime 10d, 2h, 28m	AP Template d21	Alerts
Serial Number 30404716050294	Country United States	Wireless IDS Alerts
IP Address 10.49.191.24	Error	AP Traffic Capture
Active Locations vLoc-0-10.49.191.0/24	Message DynamicRF suggests: 2.4 GHz: Channel 1 Power 10 dBm 5 GHz: Channel 157 Power 10 dBm	Adjacent APs
	Status UpToDate	
	Last Background Scan	

Interfaces

Type	Radio Mode	Wireless Mode	Channel	Tx power	Max TX Power	Antenna Gain	EIRP	Max EIRP	Noise Floor	Clients	Adjacent APs	Co-located APs
802.11b/g/n/ax (2.4 GHz)	AP Mode	b/g/n/ax	11 (20 MHz)	22 dBm	22 dBm	4 dBi	26 dBm	26 dBm	-89 dBm	0	15	5
802.11a/n/ac/ax (5 GHz)	AP Mode	a/n/ac/ax	149 (40 MHz)	22 dBm	22 dBm	6 dBi	28 dBm	28 dBm	-103 dBm	0	13	3
Unified Access										0		
Total										0		

LAN Port Statistics

Interface	Profile Name	PHY Status	Port Auth Status	VLAN	Clients	Tx (in Bytes)	Rx (in Bytes)	Link Speed
LAN-2	Disabled	Down	Blocked	0	0	0	0	0 Mbps

SSIDs

SSID	BSSID	Authentication	Cipher	Radio
------	-------	----------------	--------	-------

Mesh Networking in vWLAN

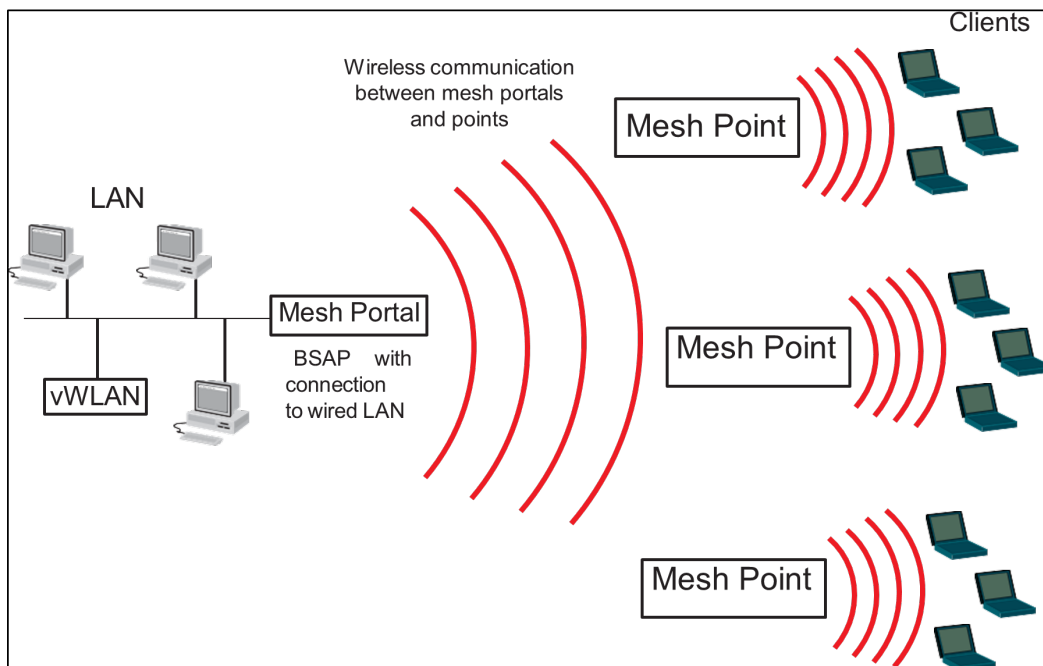
Mesh networking in vWLAN allows BSAPs to connect and communicate with each other or with other BSAP networks without the restriction of wired connections. Mesh networking can extend reach for traditional LANs where wired LAN infrastructure is not available. It provides a wireless bridge between two or more buildings or locations.



The Mesh networking support is not available for BSAP 3000 and 6000 series.

Mesh networking infrastructure is configured in a hierarchical structure, where master devices (mesh portals) act as a parent device to other non-master child devices (mesh points). Mesh portals are BSAPs that forward traffic between a mesh network and a wired LAN, and mesh points are BSAPs that have a wireless backhaul link upstream toward the wired network (and the mesh portal). Each mesh network consists of one mesh portal and multiple mesh points. [Figure 8](#) demonstrates the relationship of mesh points and the mesh portal within the vWLAN mesh network.

Figure 8: Mesh Points and Mesh Portals in vWLAN Mesh Networking



This section contains these topics:

Typical Mesh Networking Configurations	165
Mesh Network Deployment Considerations	167
vWLAN BSAP Mesh Network Functionality	170
System Requirements and Limitations	171
Configuring BSAPs for Mesh Networking	173

Typical Mesh Networking Configurations

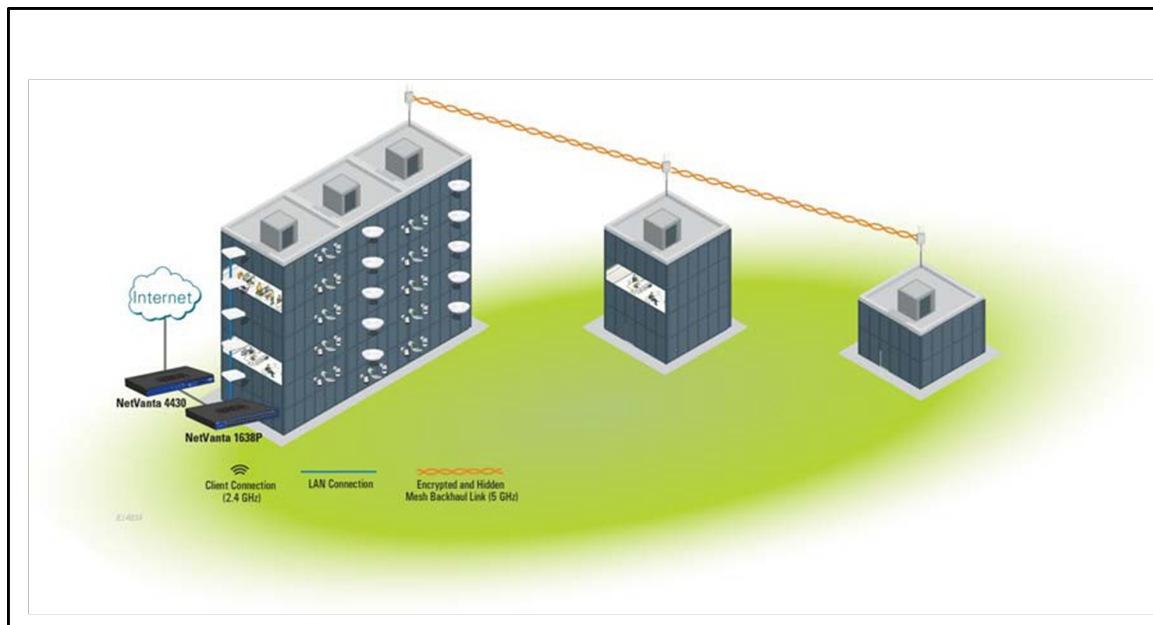
You can use mesh networking in a variety of ways to connect multiple sites wirelessly, often producing a cost savings over T1 or fiber connections. Mesh networks are created using multiple-hop connections, point-to-point connections, and point-to-multipoint connections. These network configurations are discussed in these sections.


- Multi-hop Mesh Networks165
- Point-to-Point Mesh Networks166
- Point-to-Multipoint Mesh Networks167

Multi-hop Mesh Networks

Multi-hop mesh networks (see Figure 9) are formed when one mesh portal connects to multiple mesh points in a single line and the portal uses a routing technique to pass information along a wireless path until it reaches its destination. This type of network is used when distance becomes an issue in typical point-to-point or point-to-multipoint configurations. You can configure multi-hop networks for no more than three hops deep.

Figure 9: Multi-hop Mesh Network Topology



 Data throughput is reduced approximately 50 percent with each hop in a multi-hop network design.

You can use multi-hop mesh networks to provide access where traditional cabling configurations are impractical. For example, a business wants to add wireless access to a pavilion outside of their main company infrastructure. You can mount a mesh portal on the main building with access to the internal network. You can mount the mesh point on the pavilion to provide wired or wireless connectivity.

Point-to-Point Mesh Networks

A point-to-point mesh network is formed when you use only two BSAPs to create a bridge link between two wired networks. Point-to-point connections typically use directional antennas, and can provide long-range outdoor links.

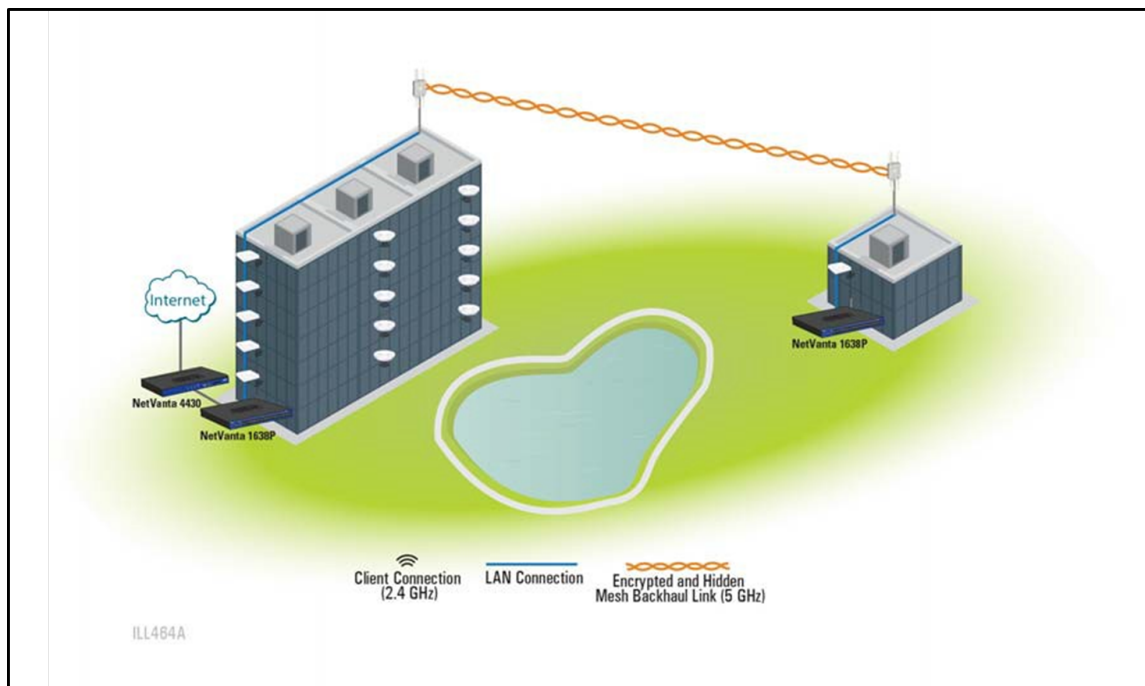
Use point-to-point mesh networks to connect two campus buildings, Building 1 and Building 2, where only one of them, for example Building 1, has access to the Internet (see [Figure 10](#)). Instead of installing fiber connections through the parking lot or using microwave connections to extend Internet access to Building 2, achieve point-to-point bridging utilizing Adtran secure, reliable, and affordable mesh networking solution.

With point-to-point bridging, you can deploy an outdoor AP on top of Building 1 as a mesh portal (MPPI) cabled to the network with Internet access. Then deploy a second AP on Building 2 as a mesh point (MP2). The mesh portal in Building 1 might be referred to as the parent and the mesh point in Building 2 might be referred to as the child. MP2 can form a secure over-the-air uplink on the 5 GHz radio to MPPI. By connecting MP2 to an Ethernet switch in Building 2, traffic from Building 2 can be backhauled to Building 1 and ultimately out to the Internet, all while maintaining VLAN tagging across the uplink.



Careful planning is required when you implement a point-to-point mesh network. If the point-to-point connection is used for redundancy, it can create unintended consequences, such as if someone enables the BPDU filter. You must perform the Fresnel zone and RF line-of-sight calculations before you install mesh networks.

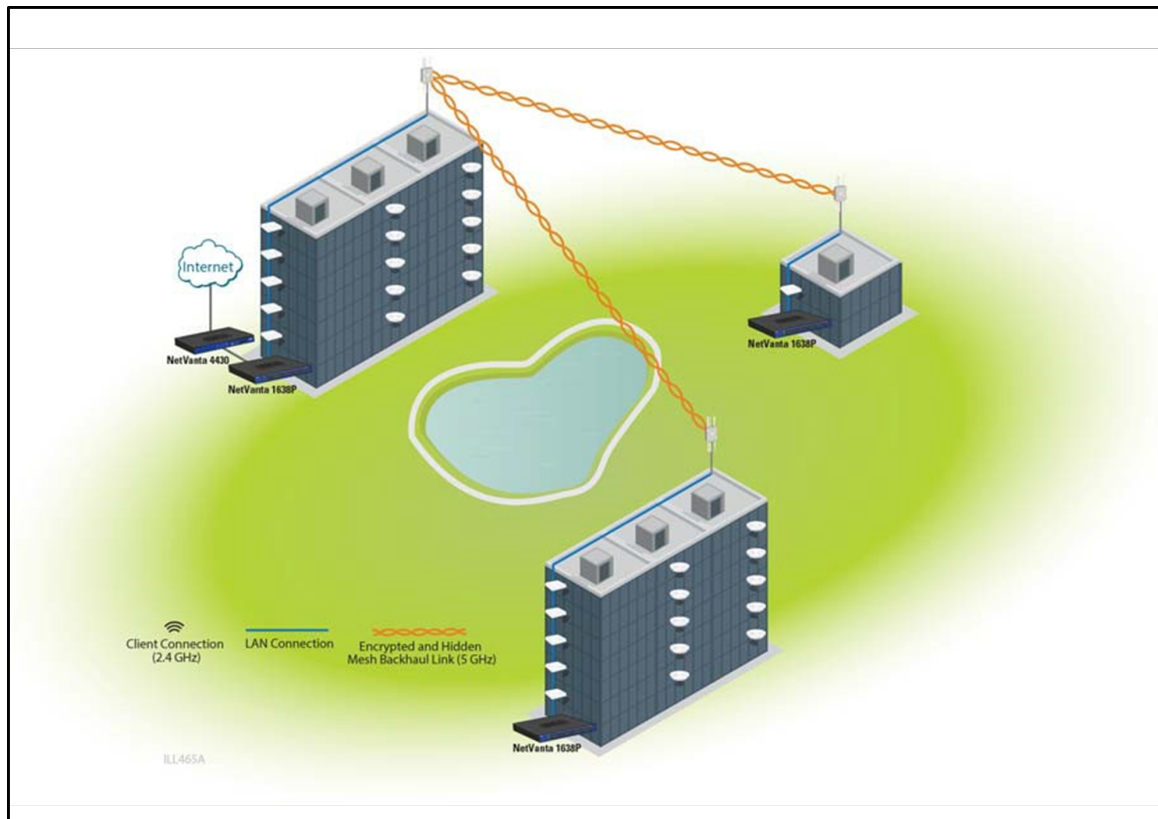
Figure 10: Point-to-Point Mesh Network Topology



Point-to-Multipoint Mesh Networks

Point-to-multipoint mesh networks use one mesh portal to communicate with up to five mesh points. In this type of network, there is always one mesh portal acting as a master, while all other connected mesh points are treated as nodes. A typical point-to-multipoint network has a central mesh portal that connects to other mesh points, forming a hub-and-spoke configuration. [Figure 11](#) illustrates a point-to-multipoint mesh network.

Figure 11: Point-to-Multipoint Mesh Network Topology



Point-to-multipoint configurations allow you to extend point-to-point bridging by adding a third building without Internet access (Building 3) to the scenario described in the previous section. You can deploy an additional outdoor AP as a mesh point (MP3) on the top of Building 3. This configuration creates one parent mesh portal and multiple mesh point children.



Even though this wireless link allows access to buildings without cabling, it is still a wireless link that is shared by all users. Careful attention to bandwidth considerations and wireless design should be done to ensure success of the installation.

Mesh Network Deployment Considerations

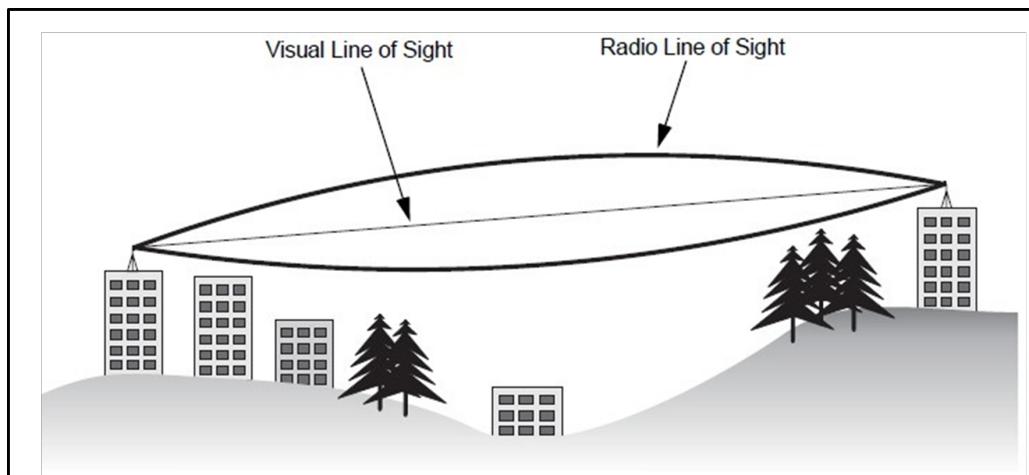
To configure a well-functioning mesh network, you must consider several items: link budgeting, how to install outdoor antennas, and other mesh-specific deployment considerations such as familiarity with the Fresnel zone, radio frequency (RF) line of sight issues, free-space path loss, and proper antenna configurations. These considerations are discussed briefly in these sections:

RF Line of Sight	168
Antenna Height	169
Antenna Position and Orientation	170
Antennas and Data Rates	170

RF Line of Sight

The RF line of sight is the area along the radio link path through which the bulk of the radio signal power travels between two antennas. This area is known as the first Fresnel zone of the radio link. For a radio link not to be affected by obstacles along its path, no object, including the ground, must intrude within 60 percent of the first Fresnel zone. A clear line of sight ensures reliable wireless links between the antennas. [Figure 12](#) illustrates the concept of a good RF line of sight.

Figure 12: RF Line of Sight



If there are obstacles in the radio path, there might still be a radio link, but the quality and strength of the signal will be affected. Calculating the maximum clearance from objects on a path is important as it directly affects the decision on antenna placement and height. It is especially critical for long-distance links, where the radio signal could be easily lost.

When you plan the radio path for mesh networking links, consider these factors:

- Avoid any partial line of sight between the antennas.
- Be cautious of trees or other foliage near the path. They might grow and obstruct the path.
- Be sure there is enough clearance from buildings and that no building construction will eventually block the path.
- Check the topology of the land between the antennas using topographical maps, aerial photos, or satellite image data.
- Avoid a path that might incur temporary blockage due to the movement of cars, trains, or aircraft.

Antenna Height

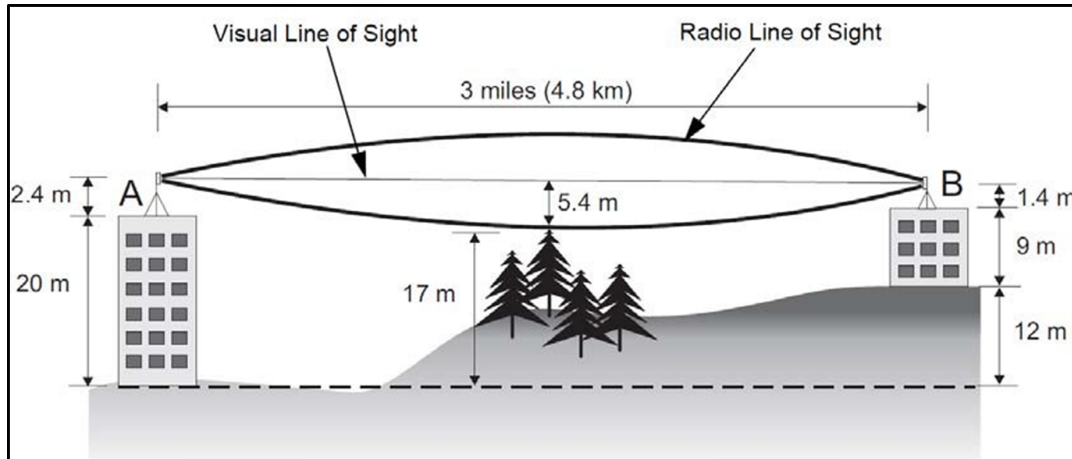
Antenna height is an important consideration in the deployment of mesh networks, along with antenna strengths and RF line of sight. Usually, a reliable wireless link is best achieved by mounting the antennas at each end high enough for a clear radio line of sight between them. The minimum height required depends on the distance of the link, obstacles that might be in the path, topology of the terrain, and the curvature of the earth (for links over three miles). For long-distance links, a mast or pole might be needed to attain the minimum required height. Use the information in [Table 6](#) to estimate the required minimum clearance for the ground or path obstruction.

Table 6: Antenna Height and Minimum Clearance

Total Link Distance	Max Clearance for 60% of First Fresnel Zone at 5.8 GHz	Approximate Clearance for Earth Curvature	Total Clearance Required at Midpoint of Link
0.24 mile (402 m)	4.5 ft (1.4 m)	0	4.5 ft (1.4 m)
0.5 mile (805 m)	6.4 ft (1.95 m)	0	6.4 ft (1.95 m)
1 mile (1.6 km)	9 ft (2.7 m)	0	9 ft (2.7 m)
2 miles (3.2 km)	12.7 ft (3.9 m)	0	12.7 ft (3.9 m)
3 miles (4.8 km)	15.6 ft (4.8 m)	1.8 ft (0.5 m)	17.4 ft (5.3 m)
4 miles (6.4 km)	18 ft (5.5 m)	3.2 ft (1.0 m)	21.2 ft (6.5 m)
5 miles (8 km)	20 ft (6.1 m)	5 ft (1.5 m)	25 ft (7.6 m)
7 miles (11.3 km)	24 ft (7.3 m)	9.8 ft (3.0 m)	33.8 ft (10.3 m)
9 miles (14.5 km)	27 ft (8.2 m)	16 ft (4.9 m)	43 ft (13.1 m)
12 miles (19.3 km)	31 ft (9.5 m)	29 ft (8.8 m)	60 ft (18.3 m)
15 miles (24.1 km)	35 ft (10.7 m)	45 ft (13.7 m)	80 ft (24.4 m)
17 miles (27.4 km)	37 ft (11.3 m)	58 ft (17.7 m)	95 ft (29 m)

To avoid any obstruction along the path, you must add the height of the object to the minimum clearance required for a clear RF line of sight. [Figure 13](#) illustrates these principles. In this example, a mesh network is used to connect building A to building B, which is located three miles away. Midway between the two buildings is a small tree-covered hill. [Table 6](#) shows that for a three-mile link, the object clearance required at the midpoint is 17.4 ft. The treetops on the hill are at an elevation of 56 ft, so the antennas at each end of the link need to be at least 73 ft high. Building A is six stories high (66 ft), so a 7.5 ft mast or pole must be constructed on its roof to achieve the required antenna height. Building B is only three stories high (30 ft), but is located at an elevation that is 39 ft higher than building A. To mount an antenna at the required height on building B, a mast or pole of only 4.3 ft is needed.

Figure 13: Configuring Antenna Height and RF Line of Sight



Antenna Position and Orientation

After you determine the required antenna height, consider these other factors affecting the precise position of the mesh networking antennas:

- Prefer directional antennas, when possible, over the default omni-directional antennas for mesh links. This is especially true for point-to-point applications. The antenna type directly affects the performance of a link.
- Be sure that there are no other radio antennas within 6 feet (2 m) of the BSAP.
- Place the BSAP away from power and telephone lines.
- Avoid placing the BSAP too close to any metallic, reflective surfaces, such as roof-installed air conditioning equipment, tinted windows, wire fences, or water pipes.
- Position the BSAP antennas at both ends of the link with the same polarization direction, either horizontal or vertical.

Antennas and Data Rates

When you plan to deploy a mesh network, be sure to take into account the maximum distance and data rates available for the various antenna options. You must always calculate the Fresnel zone. Additionally, calculate the bandwidth requirements on the other side of the meshed links to make sure they fit well within the bandwidth provided by the length, which is approximately 50% of the data rate of the link.

vWLAN BSAP Mesh Network Functionality

A mesh network is formed in vWLAN when a BSAP is connected to the network as a mesh portal. When the mesh portal becomes active, it receives its vWLAN configuration on its wired interface, and subsequently uses a mesh SSID for communication. Once the mesh portal is configured and available, other BSAPs configured as mesh points can establish uplink connections to the mesh portal, establish a connection to vWLAN through the mesh portal, and begin using the mesh SSID. You can configure multiple mesh points as part of the mesh network, and can be configured through a connection to the mesh portal or to previously configured mesh points.

When configured as a mesh portal, a BSAP requires no special configuration changes since its connection to vWLAN is over the wired interface. When configured as a mesh point, a BSAP attempts to connect to its configured uplink parent BSAP. A mesh point will continue to scan for its uplink parent until it is successful or until new provisioning information is received. While a mesh point is in the process of establishing its connection with vWLAN, its wired port is in the disabled state. This means that any traffic received on the wired port that is not destined for the BSAP fallback port is discarded. Once the mesh point establishes its connection with vWLAN over the mesh network, it checks the wired port mode derived as part of its configuration. If the wired port mode is enabled, any traffic received on the wired interface is backhauled through the mesh network to the mesh portal. If the wired port mode is disabled, all traffic received on the wired interface continues to be discarded unless directly destined for the BSAP fallback port. BSAPs used in the mesh network reserve the 5 GHz radio exclusively for mesh connections and control channel operations; wireless clients cannot connect to the mesh-only radio. Client access is only available via the 2.4 GHz radio.

Once the mesh portal and all mesh points have been successfully associated with each other, and have received and acted upon their configuration from vWLAN, the mesh network is considered active. The vWLAN can then control all BSAPs in the mesh network. Once the mesh network is active, wireless clients can connect to configured SSIDs on BSAP radios not configured for mesh networking.

Mesh Network Security and SSIDs

Each mesh portal and mesh point uses a specific SSID for secure, over-the-air, mesh backhaul communications. This SSID is automatically configured as a hidden or non-broadcast SSID and automatically secured with WPA2/AES encryption. There is no need to create mesh SSIDs or configure complex encryption settings.

Mesh Reformation

Once the mesh network is active, extended interruptions to any uplink in the network, changes to a mesh point configured uplink, or changes to core mesh configuration settings, cause a mesh point to revert to passively listening to beacons on all channels on both radios. Scanning both radios for the new mesh network requires the mesh point to drop its SSIDs and client associations on any radios not configured for mesh networking. The mesh network is reformed once an uplink mesh point or mesh portal is discovered.

System Requirements and Limitations

Mesh networking is available on BSAPs as outlined in [vWLAN Product Feature Matrix](#). Third-party AP mesh implementations are not compatible with vWLAN mesh networking and third-party AP access (Unified User Access) is not supported on APs in the mesh network.

Mesh networking in vWLAN supports a maximum number of three hops and five nodes per mesh portal. After the first hop in the mesh network, traffic throughput is roughly halved. We recommend to use similar APs when building a mesh network (for example, 193x with 193x BSAPs or 192x with 192x BSAPs).

When a mesh point operates with LAN extensions, the vWLAN system does not authenticate or manage users on the wired port.

The mesh portal determines the BSAP operating channel based on Dynamic RF channel scanning or a static configuration. You can configure the channel at any time through a static configuration change performed by an administrator.

Enable spanning tree in the mesh network to prevent loops. vWLAN AP traffic capturing is not permitted on BSAPs in the mesh network.

Perform AP firmware updates as usual on APs operating in the mesh network. Maintain the mesh configuration through the reboot after a new version of AP firmware is activated.



During firmware upgrades of mesh APs, do not apply domain tasks until all APs completed the download and are in the pending state.

Mesh Networking Data Layer Traffic

All traffic from a BSAP using the mesh SSID or mesh radio is switched through the network without changing any of the existing VLAN tags or tunnel endpoints.

A wired client on a mesh point LAN extension has the VLAN tag applied before reaching the BSAP (based on port or network configuration). The traffic is directly switched through the AP to its uplink.

Dynamic radio frequency (RF) scanning on a mesh portal radio is configured for **Set Once** and **Hold** when the radio is configured for mesh networking. This means that after the initial configuration of the mesh portal channel by the channel scanning process, the mesh portal channel does not automatically change, but rather an RF recommendation is sent to the system administrator. The administrator can update the mesh portal channel by editing the BSAP configuration.

In addition, radio calibration is not performed on a radio in mesh network mode.

Mesh Networking and Dynamic Frequency Selection (DFS)

The DFS feature was introduced in vWLAN firmware release 2.6, with native support 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.

When you use mesh networking with DFS enabled, it is important to note that each part of the mesh network must check the channel for radar before it can support downstream mesh points. For a single hop mesh network, this means that it will take 60 seconds before the mesh point transmits traffic after the mesh portal has connected. For a two hop mesh network, this delay grows to 120 seconds.

If a mesh portal detects radar on its current channel, it must vacate the channel. This will cause any associated mesh points to disconnect. If a mesh point detects radar on its current channel, that portion of the mesh network and any downstream mesh points are disconnected. At this point, the vWLAN system will move the mesh portal to a new channel.

If a mesh uplink (mesh portal or mesh point servicing downstream mesh points) detects radar on its current channel, it stops data services to connected clients within 200 ms. It then moves to a new channel within 10 seconds of the radar detection event. During this 10 second time period, the device can transmit data as many times as necessary for an aggregated time period of 60 ms. Once the device moves to a new channel, it must monitor the new channel for radar signals for the next 60 seconds (if the channel is a DFS channel). If it detects radar on the new channel, the process begins again.

If a mesh device downstream detects radar on its current channel, it communicates the radar detection event to the mesh device upstream to which it is connected. When the upstream portal device receives the radar detection event from the downstream device, it reacts as if it detected the radar and proceeds to change channels.

Only a single channel is configured for a mesh portal. If the mesh portal detects radar interference, it will move channels. The channel block list applies only to the mesh portal and not the mesh point. If the mesh portal and mesh points are using different AP templates, only the mesh portal template block list applies.

Mesh portals change channels in only two cases: the administrator changes the mesh portal channel, or radar is detected. Mesh points change channels in only two cases as well: if the upstream mesh device changes channels or if the upstream devices changes channels because radar is detected.

For more information about DFS and its configuration in vWLAN, see [Configuring DFS for vWLAN](#).

Configuring BSAPs for Mesh Networking

By default, mesh networking is not configured on a BSAP. To form a mesh network, you must configure the BSAPs with the information needed to connect to the mesh network. This information is removed upon a factory default of the BSAP or when an AP template without mesh functionality configured is applied to the BSAP. Configure these parameters on the BSAP for mesh networking to function:

- Set **Mesh Mode** to **portal** or **point**. By default, this setting is **Off**.
- Specify **Mesh Country Code**. This a two-to-three digit code chosen from the list.
- Set **MAC Address of Uplink AP** to the mesh uplink AP Ethernet MAC address. By default, this value is all zeros.
- Specify **MAC address of the Override MAC**. This setting is optional. By default, this value is all zeros.

This section contains these topics:

Mesh Networking Configuration Order	173
BSAP Mesh Network Configuration Using the GUI	174
Creating a Mesh Networking AP Template	174
Configuring the Mesh Settings Per AP	176
Viewing Mesh Network Configurations	177

Mesh Networking Configuration Order

Configure most operations of a mesh networking BSAP in the same manner as other BSAPs in the vWLAN system. Typically, the mesh networking implementation follows this order:

1. Supply power to the BSAPs.
2. The BSAPs discover the vWLAN.
3. The BSAPs are licensed, placed into a domain, and upgraded, if needed.

4. Configure a mesh networking AP template on the vWLAN. See [Creating a Mesh Networking AP Template](#).
5. Apply the mesh networking template to the BSAPs used for mesh networking, specifying whether the AP is a mesh portal or a mesh point.
6. Configure the Ethernet bridge mode for the mesh point BSAPs. See [Configuring the Mesh Settings Per AP](#).
7. Configure the channel for the mesh portal (optional). See [Configuring the Mesh Settings Per AP](#).
8. Configure the uplink for one or more mesh points. See [Configuring the Mesh Settings Per AP](#).
9. Apply the configuration to the appropriate BSAPs.
10. The BSAPs reboot and the mesh network becomes active.
11. The mesh networking BSAPs are moved into their proper physical locations.
12. Dynamic AP discovery and channel scanning is performed for wireless client connections and typical vWLAN operations.
13. The BSAPs can be visualized on the AP heat map in the vWLAN.

BSAP Mesh Network Configuration Using the GUI

You can use the vWLAN GUI for the majority of the mesh configuration necessary for the BSAP. The two basic steps for GUI configuration of mesh networking are to create an AP template for mesh networking, and to configure the specific mesh settings on a per-AP basis.



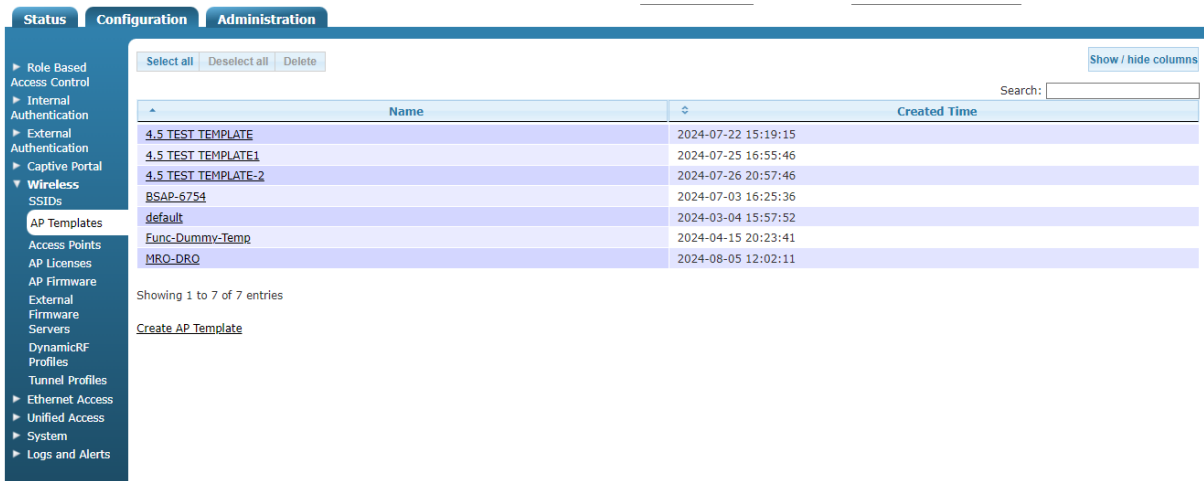
You can configure certain elements of the vWLAN mesh network using the CLI. For more information, see the *BSAP vWLAN CLI Reference Guide*.


To complete the GUI configuration for mesh networking, see these sections.

Creating a Mesh Networking AP Template	174
Configuring the Mesh Settings Per AP	176

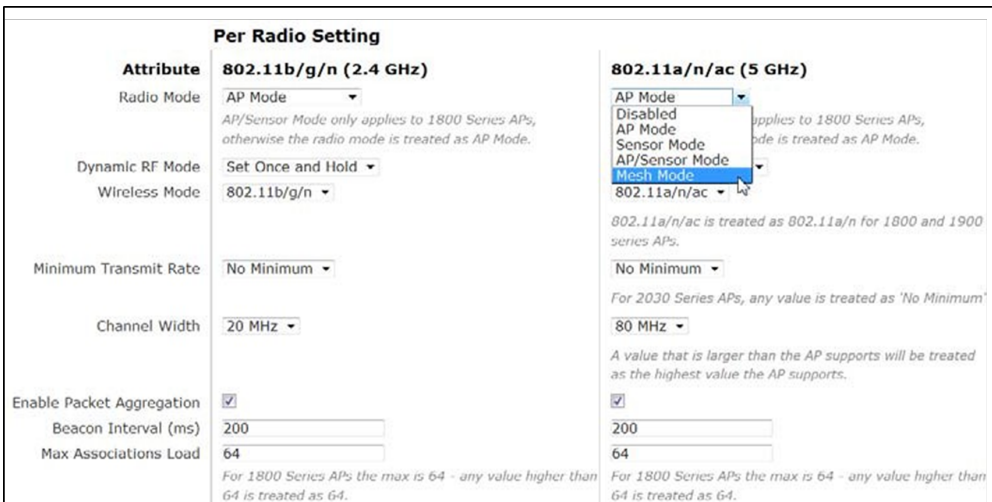
Creating a Mesh Networking AP Template

1. Connect to the vWLAN GUI and navigate to **Configuration > Wireless > AP Templates**. Select **Create AP Template** from the bottom of the menu. Here you will begin configuring the AP template for mesh networking. In this configuration, specify the radio, radio channel, and additional mesh networking attributes for the mesh portals and mesh points.



 When an AP is moved into a domain, it is automatically assigned the default template. Setting the 802.11a radio to mesh mode on the default template results in all new APs being provisioned for mesh networking, which might not be the desired behavior.

- In the template, specify the name of the AP template, the SSH password, login form, domain name system (DNS) servers, and appropriate network settings as you normally would for an AP template. Then, specify the AP is in mesh network mode by selecting **Mesh Mode** from the 802.11a/n/ac **Radio Mode** field. Mesh networking is only available on the 802.11a/n/ac radio.



- Set the **Dynamic RF Mode** setting to **Set Once and Hold** when the radio is configured for mesh networking. This means that after the initial configuration of the mesh portal channel by the channel scanning process, the mesh portal channel does not automatically change, but rather an RF recommendation is sent to the system administrator. The administrator can update the mesh portal channel by editing the BSAP configuration. In addition, radio calibration is not performed on a radio in mesh network mode. You cannot specify SSIDs or access groups for a radio in mesh mode. Otherwise, configure all radio settings as you would for any other AP template. When the configuration parameters are complete, click **Create AP Template** from the bottom of the menu. The newly created template is now displayed under **Configuration > Wireless > AP Templates** menu. You can apply it to APs as they are added to the network.



All traffic from a BSAP using the mesh SSID or mesh radio is switched through the network without changing any of the existing VLAN tags or tunnel endpoints.

Configuring the Mesh Settings Per AP

Once an AP template with mesh networking enabled is applied to an AP, you can make further configurations to the specific AP. These configurations include the AP mesh mode, the uplink AP, and the Ethernet bridge setting. To access these configurations:

1. Navigate to **Configuration > Wireless > Access Points**. Select the AP to update from the list.
2. In the **Edit Access Point** menu, ensure that the AP is configured to use an AP template with mesh mode enabled, and select whether the AP is a mesh portal or mesh point from the **Mesh Mode** field. A mesh portal always has a connection to the vWLAN over the wired port, and a mesh point always has a wireless connection to the vWLAN. If you configure a mesh portal, click **Update Access Point** once the mesh mode is specified.

Edit Access Point

Serial Number

AP MAC Address

Country

Name

SysLocation

Location

Access Point Template

Mesh Mode

Channel b/g/n(2.4 GHz)

TXPower b/g/n(2.4 GHz)

Channel a/n/ac(5 GHz)

TXPower a/n/ac(5 GHz)

If you configure a mesh point, you must also specify **Uplink AP** and set **Ethernet Bridge** to **Enabled** or **Disabled**. The uplink AP is the AP to which this mesh point should connect. Only BSAPs that have a matching mesh network configuration are available for selection as an uplink AP. You cannot save the AP configuration until an uplink AP was selected for the mesh point.

The Ethernet bridge setting allows a LAN extension to exist on the mesh point by specifying whether the bridging of the AP wired interface is enabled or disabled. You cannot configure this setting for non-mesh APs or for mesh portal APs.



You can tag or untag upstream wired traffic before reaching the BSAP based on port or network configuration.

Make your selections from the appropriate fields and click **Update Access Point**.

Edit Access Point

Serial Number

AP MAC Address

Country

Name

SysLocation

Location

Access Point Template

Mesh Mode

Uplink AP

Ethernet Bridge


Channel b/g/n(2.4 GHz)

TXPower b/g/n(2.4 GHz)

Channel a/n/ac(5 GHz)

TXPower a/n/ac(5 GHz)

3. Apply the configuration or reboot the AP for the updated mesh network configuration settings to take effect.

 When you made changes to mesh portal settings, all attached mesh points change accordingly. When you made changes to mesh point settings, they are applied to a single mesh point. You cannot change the domain of a mesh point in the vWLAN. You must change it on the mesh portal to which the points are connected.

Viewing Mesh Network Configurations

You can view mesh configurations using the vWLAN GUI by either viewing the AP status or a related AP map. To view the AP configuration, navigate to the **Status** tab and select **Access Points**. Included in the AP information is the associated mesh portal for each AP.

View AP Configuration												
The page will refresh in 55 seconds. <input type="button" value="Stop Count!"/>												
<input type="button" value="Select all"/> <input type="button" value="Deselect all"/> <input type="button" value="Apply"/> <input type="button" value="Reboot"/> <input type="button" value="Reset to Defaults"/> <input type="button" value="Activate Firmware"/> <input type="button" value="Run Background Scan"/> <input type="button" value="Accept DynamicRF Suggestions"/> <input type="button" value="Download"/> <input type="button" value="Show / hide columns"/>												
Name	SysLocation	MAC Address	Mesh Portal	Serial Number	IP Address	Uptime	Locations *	Firmware *	Channel (Channel Width)	TX Power *	Total Clients	
BSAP2030-00-19-92-4b-fd-00		00:19:92:4b:fd:00		20301416051557	10.49.191.26	5d, 1h, 2m	vLoc-0-10.49.191.0/24	4.5-M-684063	2.4GHz=Sensor (20 MHz) 5GHz=Sensor (40 MHz)	2.4 GHz = 30 dBm 5GHz=30 dBm	0	
BSAP3040-00-19-92-4f-3e-00		00:19:92:4f:3e:00		30404716050293	10.49.191.24	5d, 1h, 1m	vLoc-0-10.49.191.0/24	4.5-M-684063	2.4GHz=Sensor (20 MHz) 5GHz=Sensor (40 MHz)	2.4 GHz = 30 dBm 5GHz=0 dBm	0	
BSAP6020-00-19-92-2d-84-c0		00:19:92:2d:84:c0		60200823050009	10.49.191.27	5d, 1h, 2m	vLoc-0-10.49.191.0/24	4.5.0-M-684063	2.4GHz=Sensor (20 MHz) 5GHz=Sensor (40 MHz)	2.4 GHz = 0 dBm 5GHz=0 dBm	0	

Showing 1 to 5 of 5 entries

To view the mesh topology on the AP map, navigate to the **Status** tab and select **Maps**. This menu lists any previously created maps. Each AP in the mesh network is represented on a map and has a link connecting it to its uplink address along with an arrow indicating the direction of traffic flow. To create a new AP map, complete the steps outlined in [Using Heat Maps](#).



Configuring DynamicRF for vWLAN

This section describes DynamicRF configuration for vWLAN and APs running software versions 2.9 or later. DynamicRF is supported on all BSAPs, with the exception of BSAP 6020. This section contains these topics:

DynamicRF Overview	178
Configuring DynamicRF	183
DynamicRF Use Cases	187
DynamicRF Background Scans	189
Running DynamicRF on a Heavily Scaled vWLAN System	192
Viewing DynamicRF Statistics	193

DynamicRF Overview

DynamicRF, Adtran Radio Resource Management (RRM) technology, is designed to maximize performance and adapt to interference in WLAN networks by automatically configuring optimal radio settings based on information an AP receives from the wireless environment.

DynamicRF functions in the WLAN network by learning about neighboring sources of interference, such as additional Bluesocket APs, third-party APs, ad-hoc networks, and channel interference. Once sources of interference are discovered, DynamicRF uses an algorithm to automatically configure optimal AP radio settings, such as channel settings and transmit power, to help prevent co-channel and adjacent-channel interference. The algorithm provides the optimal channel on which the AP should operate as well as determines if transmit power should be reduced on the AP radio.

To understand how DynamicRF functions, it is important to understand these concepts:

- 2.4 GHz and 5 GHz radio operation
- Radio frequency (RF) planning and overlapping channels
- RF interference

For more information about these concepts, and in particular their function within a Bluesocket wireless deployment, you should read and understand the guide [Avoiding RF Interference with a Successful Bluesocket Wireless Deployment](#) before using DynamicRF.

The algorithm used by DynamicRF functions in two ways to optimize radio settings for connected APs through dynamic channel and the dynamic power algorithm operations.



DynamicRF does not replace predictive network designs, RF planning, or onsite surveys. Engineering and design are required to determine network requirements, AP placement and installation, and other wireless network considerations. Best practice is to remove sources of network interference, such as printers, rogue APs, and video cameras, through strong corporate network policies. DynamicRF is a tool that can operate within these policies and provide APs an ability to adapt to changes in the network. See [DynamicRF Use Cases](#) for more information.

This section contains these topics:

DynamicRF Channel Algorithm	179
DynamicRF Power Algorithm	180
DynamicRF Operation on an AP First Boot	181

DynamicRF Channel Algorithm

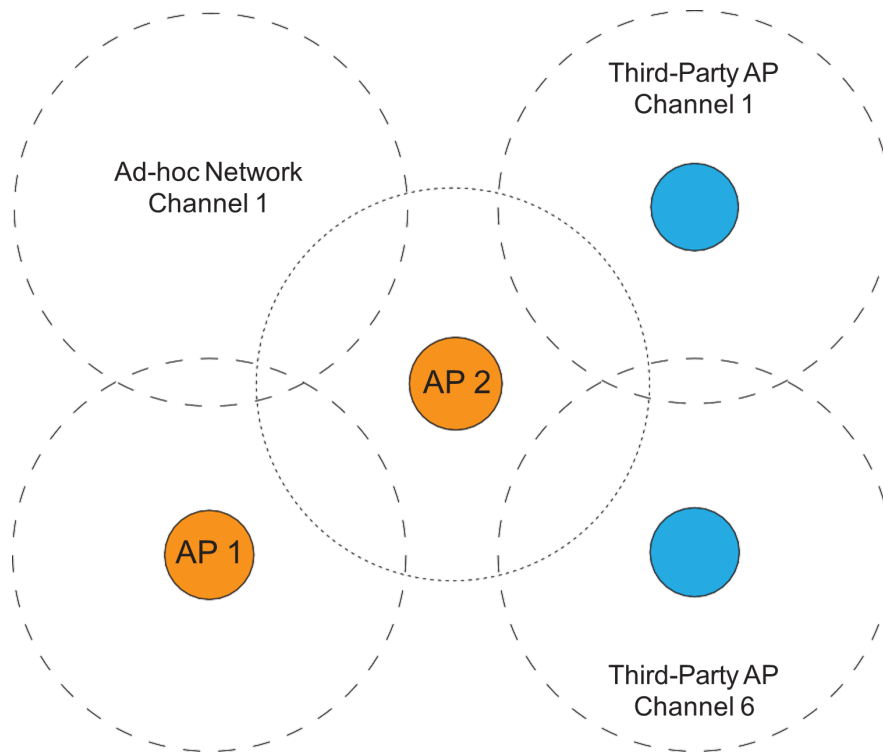
The dynamic channel algorithm operation used by DynamicRF employs RF planning concepts based around overlapping channels and channel interference from other APs to help select a channel plan for Bluesocket APs. When DynamicRF operation begins, APs evaluate their current AP adjacencies. An adjacency is detected by scanning the frequency band and listening for any other APs or ad-hoc networks that are being broadcast at a Received Signal Strength Indicator (RSSI) higher than the transmit power interface threshold set in the DynamicRF profile (see [Configuring the DynamicRF Profile](#)).

When all networks are detected, each AP calculates its channel utilization, which is a calculation of how much the surrounding APs use the channel. After this value is calculated, the information is sent back to vWLAN, and DynamicRF analyzes the data and selects the best channel for AP operation.

Operation Example

In a typical network setting, with multiple APs and ad-hoc networks, the DynamicRF channel algorithm is used to determine the best operation channels for APs within the wireless environment. [Figure 14](#) describes a wireless environment in which there are two company APs (orange), two third-party APs from another company (blue), and an ad-hoc network. In the illustration, the dotted lines represent the APs effective range of coverage.

Figure 14: Wireless Environment with Company APs, Third-Party APs, and Ad-hoc Network



In this example, DynamicRF is enabled on both AP 1 and AP 2. The adjacencies for AP 1 include an ad-hoc network adjacency on channel 1, and the adjacencies for AP 2 include adjacencies from third-party APs on channels 1 and 6. DynamicRF calculates the channel utilization for each AP based on these adjacencies, and then selects channel 11 for AP 2 operations and channel 6 for AP 1 operations. These selections allow the least amount of overlap possible while also conforming to normal channel planning concepts.

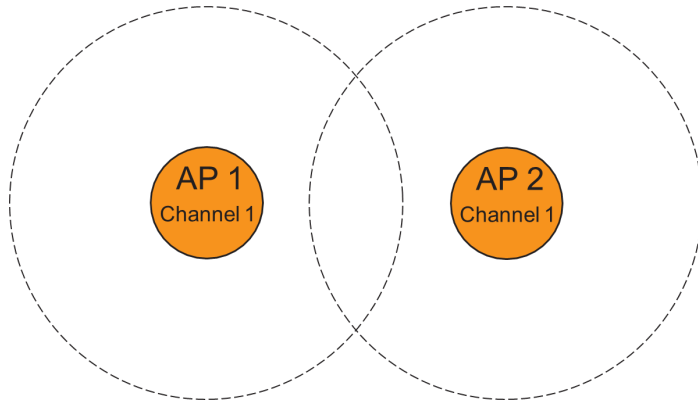
DynamicRF Power Algorithm

The dynamic power algorithm operation used by DynamicRF operates similarly to the channel algorithm operation in that it detects Bluesocket AP adjacencies. However, when adjacency data is sent back to vWLAN, DynamicRF sets transmit power for an AP by considering only the adjacencies from APs in the same domain. If an adjacent AP is detected on the same channel, at a power level higher than the Transmit Power Interference Threshold specified in the DynamicRF profile, DynamicRF reduces one or both of the APs' power. The channel is then scanned again by each AP, and the power reduction takes place again if the APs still detect each other at a high RSSI. The power algorithm always takes place after the channel algorithm has run and set channels for the AP (or it runs independently if it is run without the channel algorithm).

Operation Example

In this example, DynamicRF was already used to properly set the appropriate channels for all working APs. [Figure 15](#) below illustrates two APs, AP 1 and AP 2, that although not directly next to each other, can still hear each other on the same channel at a signal strength above the configured transmit power interference threshold setting of -80 dBm.

Figure 15: Two APs Using DynamicRF Power Algorithm

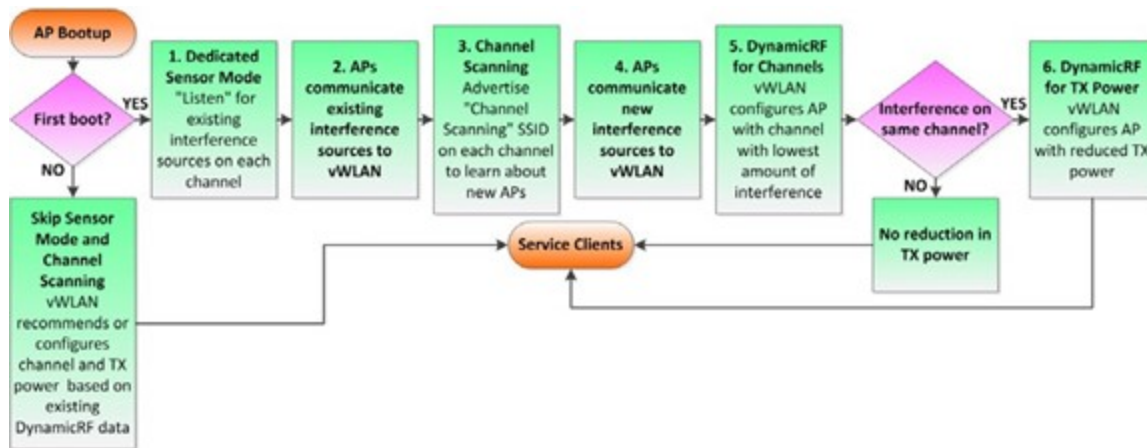


To address this interference, DynamicRF steps power down on one or both APs from 30 dBm to 29 dBm. Both APs once again listen and calculate the signal strength of the other signal. If it is still above the threshold, power is reduced again and the steps are repeated until the APs cannot hear each other at a signal strength higher than the transmit power interface threshold value.

DynamicRF Operation on an AP First Boot

DynamicRF is used from the first moment the AP begins operation. The next sections outline the order in which AP operations occur and their impact in DynamicRF operation. Figure 16 visually outlines this process.

Figure 16: DynamicRF Order of Operation



The configuration of the DynamicRF mode setting for the AP radio can affect the DynamicRF operation as it is described below. If the DynamicRF mode is set to **Set Once and Hold** (default) or **Continuous**, DynamicRF operates as described. If DynamicRF mode is set to **Disabled**, you must configure all radio settings manually. In addition, if some specifics of AP configuration are set to auto, DynamicRF operation can be affected. See [Configuring the DynamicRF Profile](#).

- **Dedicated Sensor Mode:** When Bluesocket APs are added or moved into a domain for the first time, both the 2.4 GHz and 5 GHz radios of the AP enter dedicated sensor mode once their firmware upgrade is complete. They stay in this mode for one minute, in which the radios do not service clients but rather listen for sources of interference on each channel. Interference types detected during this time include neighboring Bluesocket APs, third-party APs, and ad-hoc networks on each channel.
- **Communicate Interference to vWLAN:** Once the APs have listened for interference during the dedicated sensor mode, they pass the list of learned interference sources and these source signal strengths to vWLAN over the secure management and control channel. While the APs are in sensor mode, and not beaconing, neighboring active APs do not detect these APs. Once interference sources are communicated to vWLAN, if the AP is booting up for the first time in this domain, it begins channel scanning. If this is not the first boot of the AP, the AP does not begin channel scanning, but rather, DynamicRF configures or recommends radio channel and transmit power settings based on the information gathered and set in the DynamicRF profile.
- **Channel Scanning Mode:** If this is the first boot for the AP in this domain, it enters channel scanning mode for three minutes after the initial one minute in dedicated sensor mode. While in this mode, the 2.4 GHz and 5 GHz radios send a channel scanning beacon SSID on each non-overlapping channel per radio. These channels are determined by the country in which the AP operates. For example, in the United States, the channel scanning SSID is broadcast on channels 1 and 36 for the first minute (for the 2.4 GHz and 5 GHz radios respectively), 6 and 48 for the second minute, and 11 and 161 for the third minute. During this period, any new Bluesocket APs that boot up concurrently learn about each other, and any existing active neighboring Bluesocket APs learn about the new APs when the new APs visit the channel on which the existing active APs are operating.
- **Communicate Interference to vWLAN:** After the channel scanning mode, APs report any newly detected sources of interference to vWLAN over the secure management and control channel. Using this information, and information specified in the DynamicRF profile, DynamicRF configures or recommends radio channel and transmit power settings.
- **DynamicRF for Channel Assignment:** Once the AP was through the dedicated sensor and channel scanning modes, vWLAN runs a dynamic channel algorithm using the data it receives from the APs. This algorithm determines the number of neighboring interference sources on each channel and takes into account AP and ad-hoc network sources of interference and signal strength information. You can configure these settings as described in [Configuring the DynamicRF Profile](#). Once the algorithm has run, channels and transmit power settings are assigned to the AP. The AP is configured with the channel with the lowest amount of interference, neighboring APs, and ad-hoc networks. If these values result in a tie, signal strength information is used to make a channel assignment decision.
- **DynamicRF for Transmit Power Settings:** After the radio channel has been configured, the DynamicRF power algorithm is used to determine if radio transmit power should be reduced. If there are sources of interference, such as neighboring Bluesocket APs in the same domain, on the same channel with an RSSI equal to or higher than the configured power threshold, transmit power is reduced.




Transmit power is reduced only if neighboring APs are Bluesocket APs in the same domain and on the same channel. Third-party APs do not impact transmit power.

The lower the power threshold is configured to be (see [Configuring the DynamicRF Profile](#)), the more likely APs with interference or neighbors on the same channel and in the same domain will reduce power. APs without interference, or neighbors on the same channel, do not automatically result in reduced transmit power. vWLAN reduces transmit power only to mitigate interference, not to create a specific amount of cell overlap.

Configuring DynamicRF

This section contains these topics:

Configuring the DynamicRF Profile	183
Applying the DynamicRF Profile to an AP	186



Prior to vWLAN version 3.1.0, the default mode for DynamicRF was **Set Once** and **Hold**, such that channels and power would not change after the first boot. As of vWLAN 3.1.0, new APs will default to Client-aware AP/Sensor mode and the DynamicRF profile will default to Continuous mode. These settings will allow new APs to run Dynamic RF out of the box and adapt to channel and power changes in the environment without manual intervention.

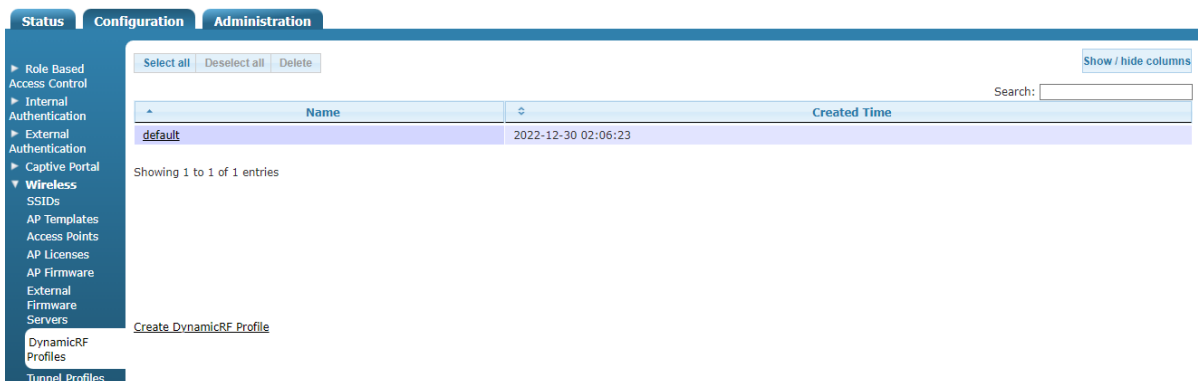
While the new default mode allows dynamic changes, we recommend that an on-site technical administrator evaluate the changes for special situations and adjust the settings, if needed.

Configuring the DynamicRF Profile

There are various settings that you can configure 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 this section.

To configure various settings for the DynamicRF profile:

1. In the vWLAN GUI, navigate to **Configuration > 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, click **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** field. See [DynamicRF Use Cases](#) for additional information about when to use each of these settings.

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.
 Sets threshold for reducing power based on signal from adjacent ADTRAN APs in the same domain on the same/adjacent channels.

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.

[Create DynamicRF Profile](#)

[Back](#)

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.



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 (see [Creating DynamicRF Background Scans](#)).

Continuous: This setting indicates that vWLAN continuously evaluates the RF environment and modifies the AP 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) or in high-throughput environments.

As of vWLAN 3.1.0, Client-Aware AP/Sensor mode was added as a selection under Radio Settings in the AP template, allowing the AP to background scan for better channels. When a better channel is found, the AP will queue up a change, but will not implement it until all clients are idle. This practice eliminates issues with clients not following channel changes during data transmission.



We recommend to always use Client-Aware AP/Sensor mode with a Continuous DynamicRF profile.



If you edit 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.

3. Enable **Enable Dynamic Channel Configuration** by selecting the field. 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.
4. Enable **Enable Dynamic Transmit Power Configuration** by selecting the field. 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.
5. Optionally select the **Advanced** tab to configure transmit power settings for the DynamicRF profile.

Specify **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 **Minimum Transmit Power**. 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 **Maximum Transmit Power**. 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.



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.

6. Click **Create DynamicRF Profile** to create the profile.



Often it is desired to limit 2.4GHz power levels lower than 5GHz power levels due to the 2.4GHz frequencies traveling much farther distances. We recommend to create separate profiles for 2.4GHz and 5GHz operation and apply them to the AP template accordingly.

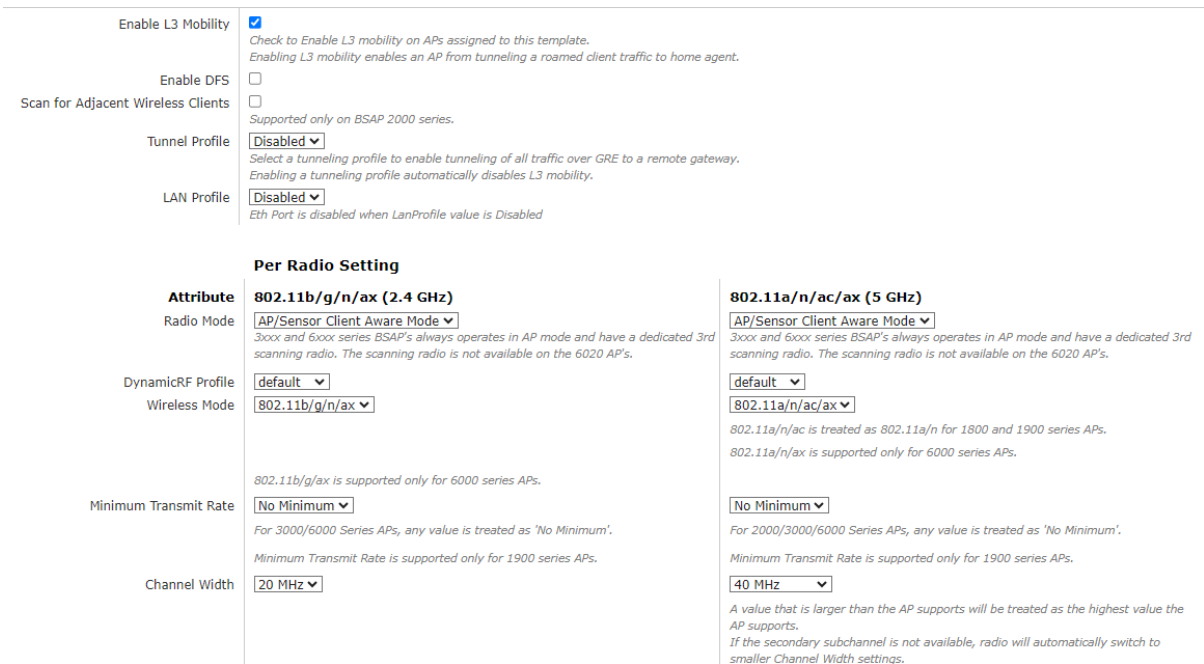
Applying the DynamicRF Profile to an AP

To apply the DynamicRF profile to an AP radio, access the AP template used by the AP and apply the profile:

1. In the vWLAN GUI, navigate to **Configuration > Wireless > AP Templates**.



2. Select the AP template from this list if you edit a template, or click **Create AP Template** from the bottom of the menu if you create a new template.
3. To add the DynamicRF profile to the template, in the **Create AP Template** or **Edit AP Template** menu, navigate to the **Per Radio Setting** menu. Select a DynamicRF profile from the **DynamicRF Profile** field. The default profile appears in this list, as well as any other profiles you created. Make selections for both the 2.4 GHz and 5 GHz radios.



4. To apply the DynamicRF profile to the AP template, click **Update AP Template** from the bottom of the **Edit AP Template** menu. All APs that use this template will be updated with the new DynamicRF profile.



If the DynamicRF profile is set to **Continuous** mode, all APs that use this template will change from AP mode to AP/Sensor mode. This could cause an interruption in wireless connection.

DynamicRF Use Cases

This section provides more detailed information about DynamicRF use cases, such as when the AP DynamicRF mode is set to one of the following:

- **Continuous Mode** (most responsive to changes in the RF environment)
- **Set Once and Hold** (most stable, relies on DynamicRF settings at first boot)
- **AP/Sensor Mode** (able to service clients while performing off-channel background scans; BSAP 1900 and 2000 Series only)
- **AP/Sensor Client Aware Mode**

Details of each DynamicRF mode, as well as considerations for their use, are described in these sections:

Continuous Mode	187
Set Once and Hold Mode	188
AP/Sensor Mode	188
AP/Sensor Client Aware Mode	189

Continuous Mode

In DynamicRF, Continuous mode is most responsive to changes in the RF environment. It is most frequently used in a dynamic environment where automatic changes to power or channel settings are important.

These considerations are important when deciding to use DynamicRF Continuous mode:

- There can be client disruption with power and channel changes. You should not use DynamicRF Continuous mode where service disruptions are critical issues. In addition, this mode might impact real time applications.
- For continuous adaptation to changes in the RF environment through automatic channel and power setting changes, the AP radio mode should be set to AP/Sensor Client Aware or AP/Sensor Mode when using DynamicRF Continuous mode. If the DynamicRF mode is set to Set Once and Hold with an AP radio in AP/Sensor Client Aware Mode or AP/Sensor Mode, channel and transmit power setting suggestions are provided, but not automatically made.
- If another AP goes online on the same channel as an existing AP, the existing AP might change channels or reduce transmit power to help prevent interference based on the DynamicRF settings. Additionally, if an AP goes down, neighboring Bluesocket APs in the same domain might increase transmit power to compensate for the nonfunctional AP.

Set Once and Hold Mode

In DynamicRF, Set Once and Hold mode allows the APs to pick the best power and channel settings DynamicRF finds at the AP first boot for a starting point before manually adjusting power settings or channels as needed or in tandem with an on-site survey.

These considerations are important when deciding to use DynamicRF Set Once and Hold mode:

- In Set Once and Hold mode, DynamicRF can suggest transmit power changes based on changes in the environment (after an on-demand or scheduled scan is completed and the AP radio is set to AP/Sensor Mode). While DynamicRF is in Set Once and Hold mode, the system administrator can look and determine what channel and power settings should be accepted.
- When DynamicRF is in Set Once and Hold mode, and the AP radio mode is set to AP mode, the BSAP 1900 and 2000 Series APs are able to service clients on the current channel. These APs also report any adjacencies or sources of interference if the source is operating on the same channel as the AP.
- DynamicRF Set Once and Hold mode is typically paired with an on-demand or scheduled background scan, see [DynamicRF Background Scans](#). Given that the wireless environment can change quickly, vWLAN will create a task to schedule a scan when DynamicRF is operating in this mode.

AP/Sensor Mode

When the AP radio is set to AP/Sensor Mode, the BSAP 1900 and 2000 Series APs can service clients on the current channel while non-intrusively performing off-channel background scanning on other channels for sources of interference and wireless intrusion detection. Off-channel background scanning is performed every 10 seconds with a dwell time of 190 ms.



Off-channel background scanning can cause a negligible loss of throughput performance (<10 percent).

Understanding AP/Sensor (Dual) AP Radio Mode

AP/Sensor Mode, commonly referred to as dual mode, is a radio mode that allows APs to service clients normally on one channel, while being aware of adjacencies and RF changes on other channels. While generic AP radio mode can only detect adjacencies from other APs on the same channel on which it is currently operating, the AP/Sensor Mode can listen to other channels for adjacencies by performing off-channel scanning. Off-channel scanning is achieved by allowing the AP to switch to a different channel than the one it is servicing once every 10 seconds. When it is ready to switch, it buffers client traffic and dwells on a different channel for 190 ms to check for adjacencies before resuming client service.

While this switch can negligibly impact throughput performance (<10 percent), it also allows DynamicRF to make decisions based on adjacencies on other channels.

When an AP radio set to AP/Sensor Mode is paired with DynamicRF in Continuous mode, DynamicRF can determine if there is a better channel on which the AP should operate based on channel utilization data received from off-channel scanning.

If a better channel is found, a channel change notification is sent to the clients and the AP moves to the other channel. Although this can cause a slight service disruption, the overall performance gain received from operating on the best channel can outweigh this risk.



You should not use the Continuous DynamicRF mode for critical and real time applications, such as voice and video traffic that cannot easily handle latency.

When an AP radio set to AP/Sensor Mode is paired with DynamicRF in Set Once and Hold mode, the system administrator can receive DynamicRF suggestions from each channel and then decide whether to push those suggested changes to the APs at their convenience, or based on a schedule.

The **Radio Mode** specified in the AP template determines AP radio modes. To set the radio mode to AP/Sensor Mode, access the vWLAN GUI and navigate to the **Configuration > Wireless > AP Templates**, and select the proper template from the list.

In the template menu, navigate to the **Per Radio Setting** section, and use the **Radio Mode** field to select AP/Sensor Mode for either the 2.4 GHz radio, the 5 GHz radio, or both.

Per Radio Setting

Attribute	802.11b/g/n/ax (2.4 GHz)	802.11a/n/ac/ax (5 GHz)
Radio Mode	AP/Sensor Client Aware Mode	AP/Sensor Client Aware Mode
DynamicRF Profile	AP Mode	default
Wireless Mode	AP/Sensor Mode	802.11a/n/ac/ax

operates in AP mode and have a dedicated 3rd scanning radio. The scanning radio is not available on the 6020 AP's.

3000 and 6000 series BSAP's always operates in AP mode and have a dedicated 3rd scanning radio. The scanning radio is not available on the 6020 AP's.

802.11b/g/ax is supported only for 6000 series APs.

802.11a/n/ac is treated as 802.11a/n for 1800 and 1900 series APs.

802.11a/n/ac is supported only for 6000 series APs.

Once the changes are complete, select Edit AP Template at the bottom of the menu. These changes will impact all APs configured to use this template.

AP/Sensor Client Aware Mode

The AP/Sensor Client Aware Mode was added in vWLAN 3.1.0. This mode functions the same as AP/Sensor Mode except that channel changes only occur when no clients are actively transmitting. When a channel change is needed, the change is queued and pushed out when either no clients are connected or when all connected clients are idle. We recommend using AP/Sensor Client Aware Mode with a Continuous DynamicRF profile.



The AP/Sensor Client Aware Mode carries the same performance degradation as AP/Sensor Mode.


DynamicRF Background Scans

You can determine DynamicRF suggestions by a background scan. This non-service impacting scan looks for improved channel and power settings and also provides the ability to accept or clear any DynamicRF suggestions. You can schedule these scans, as well as the ability to apply the suggested changes.

Creating DynamicRF Background Scans

You can determine DynamicRF-suggested radio settings using background scans in vWLAN. These scans allow configured APs to keep servicing clients while simultaneously scanning the wireless environment for suggested changes in radio settings. There are several methods to create background scans for DynamicRF, the suggestions from which can be manually or automatically accepted. These sections outline the steps to create these scans and accept the suggested changes:

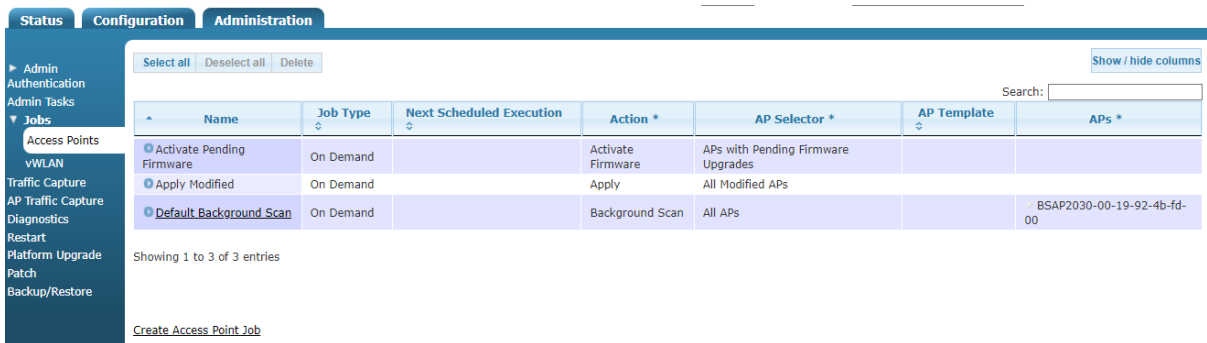
- Using AP Jobs to Create a Background DynamicRF Scan190
- Running a Background Scan from the Status Tab191
- Manually Applying DynamicRF Suggestions192

 Off-channel background scans do not impact wireless service as they can allocate minimal airtime to perform off-channel scans, but they can result in a negligible throughput performance decrease (<10 percent).

Using AP Jobs to Create a Background DynamicRF Scan

To create a DynamicRF scan that runs in the background using an AP job:

1. In the vWLAN GUI, navigate to **Administration > Jobs > Access Points**. From this menu, select **Create Access Point Job** to begin configuring a DynamicRF background scan.



2. In the **Create Access Point Job** menu, specify the parameters of the job by entering the job name in the appropriate field, selecting **Background Scan** from the **Action** field, specifying the duration of the scan, and specifying which APs will perform the scan.

You can optionally choose to automatically apply any radio channel and power suggestions when the scan is complete by selecting the **Automatically Apply Channel and Transmit Power Suggestions During Scan** field. If you do not want to automatically apply these suggestions, for example to avoid wireless service interruption, you can retrieve the suggestions and apply them manually later as described in [Manually Applying DynamicRF Suggestions](#). In addition, you can choose to optionally schedule the scan by selecting the **Scheduled** field. Once selected, you can specify the frequency, start time, and start date of the scan. Once you have specified the parameters of the scan, click **Create Access Point Job** to create the job.

Create Access Point Job

Name

Action **Apply**

AP Selector **All APs**

Scheduled

Frequency **One-time**

Scheduled Date

Scheduled Time **01:00 AM**

Schedules are enforced based on the timezone of the AP. You can set the timezone under Configuration>Wireless>AP Templates. The AP synchronizes with the vWLAN time, so it's important that the vWLAN time be correct - an NTP time server can be configured under the Platform Settings.

Scheduler collects jobs every 15 minutes.

[Create Access Point Job](#)

[Back](#)

- Click the play arrow in front of the job in the **Jobs > Access Points** menu to run the job. If you selected to automatically apply the suggested channel and power changes once the scan is complete, you need not take any further action to implement the DynamicRF suggestions. If you chose to manually apply the suggested changes, see [Manually Applying DynamicRF Suggestions](#).


Running a Background Scan from the Status Tab

In addition to creating an AP job to run a DynamicRF background scan, you can also run a background scan from the **Status** tab in the vWLAN GUI. Using this method to run a background scan utilizes dual mode on the selected APs, which allows the APs to service channels while performing off-channel scanning of other channels for adjacent APs.

To run a background scan on selected APs from the Status tab, follow these steps:

- In the vWLAN GUI, navigate to **Status > Access Points**. Select from the list the APs on which you wish to run a background scan. Then, click **Run Background Scan** from the top of the menu.

Name	SysLocation	MAC Address	Mesh Portal	Serial Number	IP Address	Uptime	Locations *	Firmware *	Channel (Channel Width)	TX Power *	Total Clients
BSAP2030-00-19-92-4b-fd-00		00:19:92:4b:fd:00		20301416051557	10.49.191.21	10d, 2h, 11m	vLoc-0-10.49.191.0/24	4.5.0-684879	2.4GHz=1 (20 MHz) 5GHz=36 (40 MHz)	2.4 GHz = 11 dBm 5GHz=20 dBm	0
BSAP3040-00-19-92-4e-3e-20		00:19:92:4f:3e:20		30404716030294	10.49.191.24	14m	vLoc-0-10.49.191.0/24	4.5.0-684879	2.4GHz=11 (20 MHz) 5GHz=149 (40 MHz)	2.4 GHz = 22 dBm 5GHz=22 dBm	0
BSAP6020-00-19-92-2d-84-c0		00:19:92:2d:84:c0		60200823050009	10.49.191.19	10d, 2h, 16m	vLoc-0-10.49.191.0/24	4.5.0-R-684879	2.4GHz=1 (20 MHz) 5GHz=36 (40 MHz)	2.4 GHz = 22 dBm 5GHz=22 dBm	0
BSAP6020-00-19-92-00-19-92-00-19-92		00:19:92:2f:81:20		60201723051343	10.49.192.187	10d, 2h, 10m	vLoc-0-10.49.192.0/24	4.5.0-R-684879	2.4GHz=8 (20 MHz) 5GHz=167 (40 MHz)	2.4 GHz = 20 dBm	0

 Using this option runs a Default Background Scan (found in **Administration > Jobs > Access Points**). By default, the scan does not automatically apply DynamicRF settings to the APs. In addition, if the AP selected from **Status > Access Points** belongs to an AP template whose DynamicRF Profile set to **Disabled**, the background scan will not run on the selected AP as noted in



the **Message Column**.

2. Apply the suggested changes as described in [Manually Applying DynamicRF Suggestions](#).

Manually Applying DynamicRF Suggestions

To manually apply DynamicRF suggestions to your APs, at your convenience:

1. In the vWLAN GUI, navigate to the **Status > Access Points**. Any suggested changes for DynamicRF are listed in the **Message** column of the menu.
2. Select from the list the APs to which you want to apply the suggestions and then click **Accept DynamicRF Suggestions** at the top of the menu to apply the radio and power suggestions to the selected APs.

Name	SysLocation	MAC Address	Mesh Portal	Serial Number	IP Address	Uptime	Locations *	Firmware *	Channel (Channel Width)	TX Power *	Total Clients
BSAP2030-00-19-92-4b-fd-00		00:19:92:4b:fd:00		20301416051557	10.49.191.21	10d, 2h, 11m	vLoc-0-10.49.191.0/24	4.5.0-684879	2.4GHz=1 (20 MHz) 5GHz=36 (40 MHz)	2.4 GHz = 11 dBm 5GHz=20 dBm	0
BSAP3040-00-19-92-4e-3e-20		00:19:92:4f:3e:20		30404716030294	10.49.191.24	14m	vLoc-0-10.49.191.0/24	4.5.0-684879	2.4GHz=11 (20 MHz) 5GHz=149 (40 MHz)	2.4 GHz = 22 dBm 5GHz=22 dBm	0
BSAP6020-00-19-92-2d-84-c0		00:19:92:2d:84:c0		60200823050009	10.49.191.19	10d, 2h, 15m	vLoc-0-10.49.191.0/24	4.5.0-R-684879	2.4GHz=1 (20 MHz) 5GHz=36 (40 MHz)	2.4 GHz = 22 dBm 5GHz=22 dBm	0
BSAP6020-00-19-92-		00:19:92:2f:81:20		60201723051343	10.49.192.187	10d, 2h, 10m	vLoc-0-10.49.192.0/24	4.5.0-R-684879	2.4GHz=8 (20 MHz)	2.4 GHz = 20 dBm	0

Alternatively, you can create an AP job to accept DynamicRF suggestions. When creating a job (as described in [Using AP Jobs to Create a Background DynamicRF Scan](#)), select **Accept DynamicRF Suggestions** from the **Action** field.

Running DynamicRF on a Heavily Scaled vWLAN System

When operating DynamicRF on a large vWLAN system with over 750 APs, we recommend to use caution with any DynamicRF settings and background scans as to not overload the system. A general recommendation is to utilize Continuous DynamicRF mode with AP/Sensor Client Aware Mode.

If an administrator wants to run a background scan, we recommend to execute it on smaller batches of APs for an extended period of time (for example, 100APs for 3 hours) to balance the load of the DynamicRF process and ensure the best results. You should logically group these APs, as in a specific building or location.

Viewing DynamicRF Statistics

You can view the major causes of interference detected by DynamicRF, including both the number of co-channel and adjacent channel sources of interference, by viewing detailed statistics for each AP.

To view DynamicRF statistics on the AP, in the vWLAN GUI, navigate to the **Status > Access Points**. This menu lists each configured AP. Select the AP you want to view from the list.

Name	SysLocation	MAC Address	Mesh Portal	Serial Number	IP Address	Uptime	Locations	Firmware	Channel (Channel Width)	TX Power	Total Clients
BSAP2030-00-19-92-4b-fd-00		00:19:92:4b:fd:00		20301416051557	10.49.191.21	10d, 2h, 11m	vLoc-0-10.49.191.0/24	4.5.0-684879	2.4GHz=1 (20 MHz) 5GHz=36 (40 MHz)	2.4 GHz = 11 dBm 5GHz=20 dBm	0
BSAP3040-00-19-92-4f-3e-20		00:19:92:4f:3e:20		30404716050294	10.49.191.24	14m	vLoc-0-10.49.191.0/24	4.5.0-684879	2.4GHz=11 (20 MHz) 5GHz=149 (40 MHz)	2.4 GHz = 22 dBm 5GHz=22 dBm	0
BSAP6020-00-19-92-2d-84-c0		00:19:92:2d:84:c0		60200823050009	10.49.191.19	10d, 2h, 16m	vLoc-0-10.49.191.0/24	4.5.0-R-684879	2.4GHz=1 (20 MHz) 5GHz=36 (40 MHz)	2.4 GHz = 22 dBm 5GHz=22 dBm	0
BSAP6020-00-19-92-00-19-92-		00:19:92:2f:81:20		60201723051343	10.49.192.187	10d, 2h, 10m	vLoc-0-10.49.192.0/24	4.5.0-R-684879	2.4GHz=8 (20 MHz) 5GHz=157	2.4 GHz = 20 dBm	0

The selected AP details are displayed including the AP configuration, radio interfaces, associated SSIDs, and DynamicRF statistics. From this detailed menu, you can view the adjacent APs, any co-channel APs, and DynamicRF statistics.

Access Point Details

Name: Nick-1930 | Model: BSAP-1930 | Edit Configuration | Not on a map yet

SysLocation: DFS Hardware Ready No | Firmware: 2.9-M-255213 | Logs

MAC Address: 00:19:92:33:83:80 | Uptime: 0d, 0h, 42m | AP Template: default | Alarms

Serial Number: 19301413050413 | Country: United States | Wireless IDS Alerts

IP Address: 172.30.11.196 | Error | AP Traffic Capture

Active Locations: vLoc-0-172.30.11.192/28, VLAN-100 | Message | Adjacent APs

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	Adjacent Channel 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								0						
Total								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

	1	2	3	4	5	6	7	8	9	10	11
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			

Applying the AP Template to AP(s)

After you created or updated the AP template, you must apply it to the AP for it to take effect:

1. Navigate to **Configuration > Wireless > Access Points**. This menu lists any configured APs. 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**.

Name	SysLocation	AP MAC	Mesh Portal	Ip Address	Serial Number	AP Template	Uptime	Locations	Firmware	Channel (Channel Width)	TX Power
BSAP2030-00-19-92-4b-fd-00		00:19:92:4b:fd:00		10.49.191.21	20301416051557	421	10d, 2h, 36m	vLoc-0-10.49.191.0/24	4.5.0-684879	2.4GHz=1 (20 MHz) 5GHz=36 (40 MHz)	2.4 GHz=11 dBm 5 GHz=20 dBm
BSAP3040-00-19-92-4f-3e-20		00:19:92:4f:3e:20		10.49.191.24	30404716050294	421	11d, 2h, 39m	vLoc-0-10.49.191.0/24	4.5.0-684879	2.4GHz=11 (20 MHz) 5GHz=149 (40 MHz)	2.4 GHz=22 dBm 5 GHz=22 dBm
BSAP6020-00-19-92-2d-84-c0		00:19:92:2d:84:c0		10.49.191.19	60200823050009	421	10d, 2h, 41m	vLoc-0-10.49.191.0/24	4.5.0-R-684879	2.4GHz=1 (20 MHz) 5GHz=36 (40 MHz)	2.4 GHz=22 dBm 5 GHz=22 dBm

2. Select the AP template that you want to apply to the selected APs from the **Move AP(s) to AP template** field.

You will be asked to verify that this is a change you want to make.

3. Select **OK**.

A confirmation is displayed to indicate that the AP template is 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, you can configure AP names to identify each AP. Locations are initially automatically discovered, but you might need change them 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), but you can manually configure them based on the results of a site survey. When you are 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:

1. Navigate to **Configuration > Wireless > Access Points**. This menu lists any configured APs. 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	Locations	Firmware	Channel (Channel Width)	TX Power
BSAP2030-00-19-92-4b-fd-00		00:19:92:4b:fd:00		10.49.191.21	20301416051557	421	10d, 2h, 36m	vLoc-0-10.49.191.0/24	4.5.0-684879	2.4GHz=1 (20 MHz) 5GHz=36 (40 MHz)	2.4 GHz=11 dBm 5 GHz=20 dBm
BSAP3040-00-19-92-4f-3e-20		00:19:92:4f:3e:20		10.49.191.24	30404716050294	421	11d, 2h, 39m	vLoc-0-10.49.191.0/24	4.5.0-684879	2.4GHz=11 (20 MHz) 5GHz=149 (40 MHz)	2.4 GHz=22 dBm 5 GHz=22 dBm
BSAP6020-2d-84-c0		00:19:92:2d:84:c0		10.49.191.19	60200823050009	421	10d, 2h, 41m	vLoc-0-10.49.191.0/24	4.5.0-R-684879	2.4GHz=1 (20 MHz) 5GHz=36 (40 MHz)	2.4 GHz=22 dBm 5 GHz=22 dBm

- Specify the name for the AP, its location, its template, if necessary, AP type, and the radio channel and signal power for each radio, if you did not use DynamicRF to choose the radio power and channel.

Edit Access Point

Serial Number: 20301416051557

AP MAC Address: 00:19:92:4b:fd:00

Country: United States

Name: BSAP2030-00-19-92-4b-fd-00

SysLocation: Note the physical location of the AP

Location: vLoc-0-10.49.191.0/24

Access Point Template: 421

Installed: Indoor

Changing AP template may set 5GHz channel to Auto. Please reconfigure if needed.

Per Radio Settings

802.11b/g/n/ax (2.4 GHz)		802.11a/n/ac/ax (5 GHz)	
Channel: Auto (1)	Transmit Power: Auto (11 dBm [13 mW])	Channel: Auto (36)	Transmit Power: Auto (20 dBm [100 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 BSAP1920 with the MAC address 00:19:92:00:79:e0 has a default name of **BSAPI920-00-19-92-00-79-e0**. If no MAC address exists for the AP because it was not connected yet, 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.



The maximum character limit for an AP name is 63 characters. The valid characters include alphanumeric (a to z, A to Z, and 0 to 9) and hyphen (-). AP names must start and end with an alphanumeric character and not a hyphen. Other than hyphens, the AP name cannot contain any special characters.

- Optionally, use the **SysLocation** field to specify the AP physical location. This information helps administrators when grouping APs.
- The **Location** field 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 list to an untagged VLAN. Typically, you do not have to change this value. For more information about these locations, see [Configuring Domain Locations](#).
- Select the AP template from the **Access Point Template** field. These AP templates are the ones created as described in [Configuring AP Templates](#).
- Specify whether the AP is an indoor or outdoor AP. By default, the AP is listed as indoor or outdoor based on the AP 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** field. 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 might 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 field. 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.



Channels 120 through 128 are removed for European countries for DFS functionality.

- Select the signal power for each radio from the **Transmit Power** fields. 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. See [Configuring DynamicRF for vWLAN](#).



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 (see [Table 7](#) for default antenna gain values per radio). To change the antenna gain value, select the appropriate dBi from the **Antenna Gain** field.

Table 7: Default Antenna Gain Values

AP Model	2.4 GHz Radio (dBi)	5 GHz Radio (dBi)
1920	3	4
1925	3	3

AP Model	2.4 GHz Radio (dBi)	5 GHz Radio (dBi)
1930	4	5
1935	3	3
1940	5	7
2020	3	6
2030	4	5
2035	5	5
2120	5	6
2135	5	7

- Click **Update Access Point**. A confirmation is displayed indicating the new settings were applied to the AP.



The FCC has strict regulations regarding antennas and their configuration. For more information about these rules and their impact on vWLAN antenna gain configuration, see [Bluesocket Compliance Notice](#).

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).

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.



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 **Configuration > 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.

The screenshot shows the 'Administration' tab with the 'Platform' sub-tab selected. A table lists 8 APs. The first row is highlighted in blue, indicating it is selected. Below the table, there are controls for moving APs to a domain and uploading licenses.

Serial Number	MAC Address	IP Address	Domain	Firmware *	Country *	vWLAN License *	Unified Access License *	Status
20301416051557	00:19:92:4b:fd:00	10.49.191.21	default	4.5.0-684879	United States	Lifetime	Lifetime	UpToDate
30404716050294	00:19:92:4f:3e:20	10.49.191.24	default	4.5.0-684879	United States	Lifetime	Lifetime	UpToDate
30404716050302	00:19:92:4f:3f:20	10.49.199.2	None	4.5.0-684879	None	None	None	Down
60200823050009	00:19:92:2d:84:c0	10.49.191.19	default	4.5.0-R-684879	United States	Lifetime	Lifetime	UpToDate
60201723051343	00:19:92:2f:81:20	10.49.192.187	default	4.5.0-R-684879	United States	Lifetime	Lifetime	UpToDate
60400723051011	00:19:92:2d:05:80	10.49.192.183	default	4.5.0-R-684879	United States	Lifetime	Lifetime	UpToDate
60400723051013	00:19:92:2d:05:c0	10.49.191.18	default	4.5.0-R-684879	United States	Lifetime	Lifetime	UpToDate
61204922050131	00:19:92:2a:d6:e0	10.49.191.20	default	4.5.0-R-684879	United States	Lifetime	Lifetime	UpToDate

Viewing AP Details

To view the details of a particular AP configuration, navigate to **Status > Access Points**. This menu lists each configured AP. Select the AP you want to view from the list.

The screenshot shows the 'View AP Configuration' page for a selected AP. The table lists details for four APs. The third row is circled in red, indicating it is the selected AP.

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		

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.

Access Point Details

Name BSAP3040-00-19-92-4f-3e-20	Model BSAP-3040	Edit Configuration
SysLocation	DFS Hardware Ready Yes	Not on a map yet
MAC Address 00:19:92:4f:3e:20	Firmware 4.5.0-684879	Logs
Uptime 10d, 2h, 28m	AP Template _221	Alarms
Serial Number 30404716050294	Country United States	Wireless IDS Alerts
IP Address 10.49.191.24	Error	AP Traffic Capture
Active Locations vLoc-0-10.49.191.0/24	Message	Adjacent APs
	DynamicRF suggests: 2.4 GHz: Channel 1 Power 10 dBm 5 GHz: Channel 157 Power 10 dBm	
	Status UpToDate	
	Last Background Scan	

Interfaces

Type	Radio Mode	Wireless Mode	Channel	TX power	Max TX Power	Antenna Gain	EIRP	Max EIRP	Noise Floor	Clients	Adjacent APs	Co-ct APs
802.11b/g/n/ax (2.4 GHz)	AP Mode	b/g/n/ax	11 (20 MHz)	22 dBm	22 dBm	4 dBi	26 dBm	26 dBm	-89 dBm	0	<u>15</u>	<u>5</u>
802.11a/n/ac/ax (5 GHz)	AP Mode	a/n/ac/ax	149 (40 MHz)	22 dBm	22 dBm	6 dBi	28 dBm	28 dBm	-103 dBm	0	<u>13</u>	<u>3</u>
Unified Access										0		
Total										0		

LAN Port Statistics

Interface	Profile Name	PHY Status	Port Auth Status	VLAN	Clients	Tx (in Bytes)	Rx (in Bytes)	Link Speed
LAN-2	Disabled	Down	Blocked	0	0	0	0	0 Mbps

SSIDs

SSID	BSSID	Authentication	Cipher	Radio
------	-------	----------------	--------	-------

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 status can be viewed by navigating to **Status > Access Points**, or by looking at **Configuration > Wireless > AP Licenses**. The status is listed in the **Status** column of the AP list.

The possible AP states include:

- **Up** indicates that the AP is currently connected to the vWLAN system, but is not in a domain or is unlicensed.
- **Down** indicates that the AP is not currently connected to the vWLAN system.
- **Unknown** indicates that the state of the AP is unknown.
- **Unsupported** indicates that the AP has a serial number which is not supported by vWLAN.
- **Upgrading** indicates that the AP is in the process of loading the latest firmware.
- **PendingUpgrade** indicates that the AP has downloaded a new firmware image, but it has not been applied.
- **Updating** indicates that the AP is in the process of loading its configuration.
- **UpToDate** indicates that the AP has the latest configuration and is operational.

When you configure an AP, to determine in what state the AP should be, several factors are considered in this 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:

1. Navigate to **Status > Access Points**. Select one or more APs to reboot from the APs in the list. Select **Reboot** from the top of the menu.

Name	SysLocation	MAC Address	Mesh Portal	Serial Number	IP Address	Uptime	Locations *	Firmware *	Channel (Channel Width)	TX Power *	Total Clients
BSAP2030-00-19-92-4b-fd-00		00:19:92:4b:fd:00		20301416051557	10.49.191.21	10d, 2h, 11m	vLoc-0-10.49.191.0/24	4.5.0-684879	2.4GHz=1 (20 MHz) 5GHz=36 (40 MHz)	2.4 GHz = 11 dBm 5GHz=20 dBm	0
BSAP3040-00-19-92-4e-3e-20		00:19:92:4f:3e:20		30404716030294	10.49.191.24	14m	vLoc-0-10.49.191.0/24	4.5.0-684879	2.4GHz=11 (20 MHz) 5GHz=149 (40 MHz)	2.4 GHz = 22 dBm 5GHz=22 dBm	0
BSAP6020-00-19-92-2d-84-c0		00:19:92:2d:84:c0		60200823050009	10.49.191.19	10d, 2h, 16m	vLoc-0-10.49.191.0/24	4.5.0-R-684879	2.4GHz=1 (20 MHz) 5GHz=36 (40 MHz)	2.4 GHz = 22 dBm 5GHz=22 dBm	0
BSAP6020-00-19-92-		00:19:92:2f:81:20		60201723051343	10.49.192.187	10d, 2h, 10m	vLoc-0-10.49.192.0/24	4.5.0-R-684879	2.4GHz=8 (20 MHz)	2.4 GHz = 20 dBm	0

2. Select **OK** when prompted.
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. See [Configuring AP Jobs](#) for more information.

To restore an AP to default settings:

1. Navigate to **Status > Access Points**.
2. Select one or more APs to reset to the default settings by clicking on the APs in the list. Click **Reset to Defaults** from the top of the menu.
3. Select **OK** when prompted.

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 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. The system uses this job when the administrator makes wireless or firewall changes.

To create an AP job:

1. Navigate to **Administration > Jobs > Access Points**. This menu lists all current AP jobs. 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** menu at the top of the GUI.

The screenshot shows the 'Administration' tab with the 'Jobs' menu expanded to 'Access Points'. A table lists three jobs:

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		
Default Background Scan	On Demand		Background Scan	All APs		BSAP2030-00-19-92-4b-fd-00

Below the table, it says 'Showing 1 to 3 of 3 entries' and there is a 'Create Access Point Job' link at the bottom.

2. Enter a name for the job in the **Name** field.

Create Access Point Job

Name

Action

AP Selector

Scheduled

Frequency

Scheduled Date

Scheduled Time :

Schedules are enforced based on the timezone of the AP. You can set the timezone under Configuration>Wireless>AP Templates.
The AP synchronizes with the vWLAN time, so it's important that the vWLAN time be correct - an NTP time server can be configured under the Platform Settings.
Scheduler collects jobs every 15 minutes.

[Create Access Point Job](#)

[Back](#)

3. Select the appropriate action for the job from the **Action** field. Selections include: **Apply**, **Reboot**, **Reset to Defaults**, **Background Scan**, **Activate Firmware**, and **Accept DynamicRF Suggestions**.
4. Select the APs to which the job applies from the **AP Selector** field. 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 must specify a template. If you choose **Selected APs**, you must select the APs from a list.
5. To schedule the job, select the **Scheduled** field to display the scheduling options. Use the **Frequency** field 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** fields to specify the start time for the job.
6. Click **Create Access Point Job** to create the job.
Once the job was created, it will appear in the job list in the AP **Jobs** menu. To execute the job immediately, click the **play** icon next to the job in the job list. You will receive a confirmation that the job was completed.

Chapter 7

vWLAN Setup Wizard

In vWLAN firmware release 2.6, a new setup wizard was added. The setup wizard allows users who use 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](#), [vWLAN Platform Configuration](#), [vWLAN Domain Configuration](#), [vWLAN Wireless Configuration](#), and [Configuring Client Connections](#).

This chapter includes these sections:

Launching the Setup Wizard	203
Using the Setup Wizard	204
Applying the Setup Wizard Settings	208

Launching the Setup Wizard

The first time you launch vWLAN, the setup wizard displays by default. If you 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 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:

1. Navigate to **Configuration > System > Settings**. Then select the **Display Setup Wizard** option from the settings list.

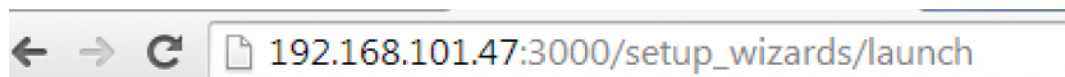
The screenshot shows the 'Domain' configuration page in the Adtran interface. The 'Display Setup Wizard' field is highlighted in blue, indicating it is the target for the next step. The table below lists various domain settings:

Name	Value *	Hint
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.
AP Control Channel Timeout	14400	Time in seconds before APs reboot if control channel is confirmed to be lost to the vWLAN (defaults to 24 hours - meaning, APs would reboot 24 hours after confirming that the control channel has been lost). Minimum allowed value is 300 seconds.
DHCP Lease Time for Un-registered Clients	10	An aggressive lease time brings clients on faster after authentication, but may not be compatible with all handheld devices.
Display Setup Wizard	Disabled	Enables setup wizard.
Flush Client Scan Data Interval	7	Range accepted from 0-30(In days), 0 means no data will be flushed out
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.
Time in minutes between updating internal status (minimum 5)	5	Updates client stats.
Time in seconds before inactive		

2. In the resulting menu, select **Enabled** from the **Display Setup Wizard** field. Then click **Update Domain Setting** to launch the setup wizard.

The screenshot shows the 'Edit Domain Setting' page. The 'Display Setup Wizard' dropdown menu is set to 'Enabled'. Below the dropdown is the text 'Enables setup wizard.' and a button labeled 'Update Domain Setting'. At the bottom left, there are links for 'Show' and 'Back'.

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.



You can only launch the setup wizard using this method if you are the network administrator, already logged into vWLAN, and your session was not timed out.

Using the Setup Wizard

After the setup wizard 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 was entered correctly at each step. If incorrect information was 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 can 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 complete these steps:

Step 1: Configuring the Administrator	205
Step 2: Verifying the Primary and Guest Wireless Networks	206
Step 3: Reviewing the Configuration	208

Step 1: Configuring 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 email, password, and timezone by entering the information in the correct fields and selecting the timezone from the drop-down menu.



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 verify default SSIDs for both a primary and guest network. These SSIDs are automatically added to the default AP template.

Primary Wireless Network	206
Guest Wireless Network	207

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:

1. Enable the primary wireless network by selecting the **Primary Wireless Network** field. By default, this field is selected.
2. Specify the name of the primary wireless network SSID by entering the name in the **SSID Name** field.
3. Specify whether the network will use WPA2-PSK or Open System by selecting the correct option from the **Authentication** field. If you choose **WPA2-PSK**, you must specify the preshared key and preshared key confirmation in the appropriate fields.
4. 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.

5. 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. vWLAN places users who connect using this SSID in a Guest role by vWLAN.

To configure the guest wireless network:

1. Enable the guest wireless network by selecting the **Guest Wireless Network** field.
2. Specify the SSID for the guest network in the **SSID Name** field.

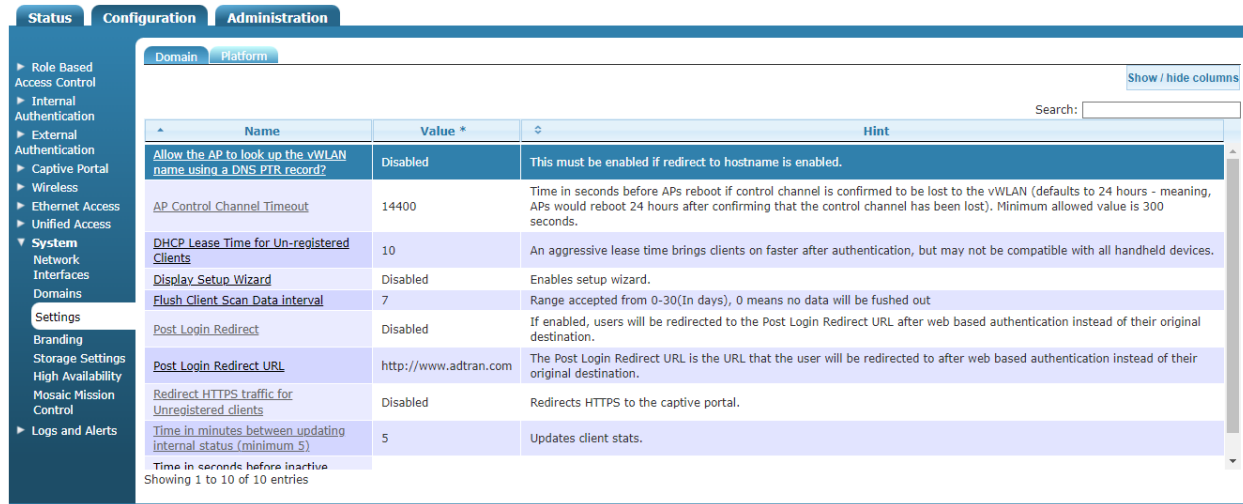
3. Click **Next**.

Step 3: Reviewing the Configuration

After you 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, click **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.



The screenshot shows the 'Configuration' tab in the Adtran interface. The table below lists various settings:

Name	Value *	Hint
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.
AP Control Channel Timeout	14400	Time in seconds before APs reboot if control channel is confirmed to be lost to the vWLAN (defaults to 24 hours - meaning, APs would reboot 24 hours after confirming that the control channel has been lost). Minimum allowed value is 300 seconds.
DHCP Lease Time for Un-registered Clients	10	An aggressive lease time brings clients on faster after authentication, but may not be compatible with all handheld devices.
Display Setup Wizard	Disabled	Enables setup wizard.
Flush Client Scan Data Interval	7	Range accepted from 0-30(In days), 0 means no data will be flushed out
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.
Time in minutes between updating internal status (minimum 5)	5	Updates client stats.
Time in seconds before inactive		

Showing 1 to 10 of 10 entries

Applying the Setup Wizard Settings

If this is the first time you 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](#).

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](#).

Chapter 8

vWLAN Serial Console Configuration

In addition to using the GUI, you configure certain parameters using the vWLAN or AP serial console. For more information, see the *BSAP vWLAN CLI Reference Guide*.

Chapter 9

vWLAN Wireless Configuration

After your vWLAN domains and APs were 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. This chapter contains these sections:

Configuring an SSID	210
Configuring a Tunnel Profile	217
Configuring DynamicSteering for vWLAN	219
Viewing Adjacent AP Neighbors	225

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. You can configure an SSID for both radios, for the 2.4 Ghz radio only, for the 5 GHz radio only, or for neither radio. In addition, you can link SSIDs 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:

1. Navigate to **Configuration > Wireless > SSIDs**. This menu lists any previously configured SSIDs.
 - To 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** menu at the top of the GUI.

The screenshot shows the 'Administration' tab in the configuration interface. A table lists the configured SSIDs. The table has columns for Name, Role, Broadcast, Authentication, Enable Captive Portal Authentication, Cipher, DynamicSteering, and Fast BSS Transition. One SSID is listed with Name '421', Role 'AllowAll', Broadcast 'Yes', Authentication 'Open System', Enable Captive Portal Authentication 'No', Cipher 'Disabled', DynamicSteering 'No', and Fast BSS Transition 'No'. Below the table, there is a 'Create SSID' button.

Name	Role	Broadcast *	Authentication *	Enable Captive Portal Authentication	Cipher *	DynamicSteering *	Fast BSS Transition *
421	AllowAll	Yes	Open System	No	Disabled	No	No

2. Enter a name for the SSID. SSID names can be up to 31 characters.

The 'Create SSID' configuration page includes the following fields and options:

- Name/ESSID:
- Broadcast SSID:
- Authentication:
- Cipher:
- Enable Captive Portal Authentication:
- Registered Role:
- Accounting Server:
- DynamicSteering:
- Convert Multicast/Broadcast Network Traffic To Unicast:
- Dynamic Multicast Optimization:
- Channel Utilization Threshold:
- Multicast Rate Optimization:
- Tunnel WLAN Traffic:

There is a 'Create SSID' button at the bottom of the form and a 'Back' link at the bottom left.

3. Enable SSID broadcasting by selecting the **Broadcast SSID** field.
4. Determine the type of authentication to be used by the SSID. The use of Captive Portal (discussed in step 6) can influence authentication options and methods so it is important to keep the required Captive Portal settings for the SSID in mind when you configure the authentication parameters. Select the proper authentication method for the SSID from the **Authentication** field. Authentication choices include: **Open System**, **WPA2-Enterprise**, **WPA2-PSK**, **WPA3-Enterprise 192-Bit**, **WPA3-Open**, **WPA3-Personal**, and **WPA3-Personal Transition**. 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. To select open system as the authentication method for this SSID, without a cipher, select **Open System** from the **Authentication** field and proceed to step 6.

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 Advanced Encryption Standard and Counter Mode CBC MAC Protocol (AES-CCM) encryption. To select WPA2-PSK as the authentication method for this SSID, select **WPA2-PSK** from the **Authentication** menu.

AES-CCM is selected by default from the **Cipher** field. You will also be prompted to specify a preshared key for this authentication type. Preshared keys must be eight digits or greater.

You can use WPA2-PSK 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.



With the WPA2-PSK authentication method, as of vWLAN firmware release 3.5.0 and later, 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. See [Configuring WPA2-Multikey Client Connections](#) for more information about configuring this feature.

WPA2-Enterprise: This method allows clients to connect to the SSID with AES-CCM encryption. It uses the RADIUS 802.1X authentication server for client authentication. To select this authentication method for this SSID, select **WPA2-Enterprise** from the **Authentication** menu. **AES-CCM** is selected by default from the **Cipher** field.

When this method is enabled, Captive Portal Authentication is not available for client connections (you cannot select the **Enable Captive Portal Authentication** field), and you must specify **RADIUS 802.1X Authentication Server**.

WPA3-Open: WPA-3 Open authentication method allows clients to connect to the SSID without passwords, but it encrypts all wireless data traffic. This method supports AES-CCM encryption. To select WPA3-Open as the authentication method for this SSID, select **WPA3-Open** from the **Authentication** menu. **AES-CCM** is selected by default from the **Cipher** field.



If you configure WPA3 authentication methods on the legacy APs, WPA2 methods is used for authentication.



WPA3-Open authentication method is supported only on 6000 series APs. Non-6000 series APs operate with Open System authentication with Cipher disabled.

WPA3-Enterprise 192-Bit: This method allows clients to connect to the SSID with GCMP-256-bit encryption more securely than the WPA2-Enterprise authentication method. It uses the RADIUS 802.1X authentication server for client authentication. To select this authentication method for this SSID, select **WPA3-Enterprise 192-Bit** from the **Authentication** menu. **GCMP-256** is selected by default from the **Cipher** field. When this method is enabled, Captive Portal Authentication is not available for client connections, but you cannot select the **Enable Captive Portal Authentication** field and you must specify **RADIUS 802.1X Authentication Server**.



WPA3-Enterprise 192-Bit authentication method is supported only on 6000 series APs. On non-6000 series APs, WPA2-Enterprise fall back is not supported because of 192-bit certificate incompatibility.

WPA3-Personal: This method allows Wi-Fi 6 certified clients to connect the SSID more securely than the WPA2-PSK authentication method. This method supports AES-CCM encryption. To select this authentication method for this SSID, select **WPA3-Personal** from the **Authentication** menu. **AES-CCM** is selected by default from the **Cipher** field. You will also be prompted to specify a preshared key for this authentication type. Preshared keys must be eight digits or greater.

You can use WPA3–Personal 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.



WPA3–Personal authentication method is supported only on 6000 series APs. Non–6000 series APs operate with WPA2–PSK authentication.

WPA3–Personal Transition: This authentication method supports both WPA3 and WPA2 clients and allows legacy clients to connect to the SSID using the WPA2–PSK authentication method. This method supports AES–CCM encryption. To select this authentication method for this SSID, select **WPA3–Personal Transition** from the **Authentication** menu. **AES–CCM** is selected by default from the **Cipher** field. You will also be prompted to specify a preshared key for this authentication type. Preshared keys must be eight digits or greater.

You can use WPA3–Personal Transition 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.

- If you use the **WPA2–PSK** method for authentication, choose to use the multikey feature for client connections by selecting the **Multi Key** field. 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** field cannot be selected), and you must specify a RADIUS authentication server from the **RADIUS Multi Key Authentication Server** menu. After you enable the multikey feature and specify the RADIUS authentication server, you can continue SSID configuration by proceeding to Step 10.

Create SSID

Name/ESSID

Broadcast SSID

Authentication

Cipher

Multi Key

Enable Captive Portal Authentication

RADIUS Multi Key Authentication Server

DynamicSteering



When the WPA2–Multikey feature is enabled, Captive Portal Authentication is unavailable, and you cannot specify a role for connecting clients. For more information about this feature, its configuration, and its use, see [Configuring WPA2–Multikey Client Connections](#) or [WPA2–Multikey and Rolling–PMK in vWLAN](#).



You can configure the RADIUS Multi Key Authentication Server using the RADIUS server configuration instructions provided in [External RADIUS Web-based Authentication Server](#).

6. If you do not use Captive Portal Authentication, leave the **Enable Captive Portal Authentication** field cleared. 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](#) for additional information on configuring roles.



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 you use Captive Portal Authentication, select the **Enable Captive Portal Authentication** field. 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](#) for information on configuring un-registered roles, Captive Portal, and the Walled Garden feature.

7. After you select the authentication, cipher, and preshared key (if necessary) information for the SSID, and configure the Captive Portal settings, specify the login form to be associated with the SSID by selecting the appropriate form from the **Login Form** field. By default, each SSID will use the default login form. If you did not create another login form, you can only use this option. See [Customizing vWLAN Login Forms and Images](#) for more information. You can select another login form if you already created one, or you can choose to use the default form from the AP template.
8. 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](#).

9. 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 **Role to be assigned when vWLAN is down**.



You must enable Captive Portal to use this feature. Captive Portal is automatically enabled when a PSK SSIDs is created.

Create SSID

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
- Accounting Server: (empty)
- Allow new clients to use the network when vWLAN is down: (circled in red)
- Role to be assigned when vWLAN is down: Guest (circled in red)

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 [Configuring DynamicSteering for vWLAN](#).



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.

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)



This option is only available when **WPA2-Enterprise, WPA2-PSK, WPA3-Enterprise 192-Bit, WPA3-Personal, or WPA3-Personal Transition** 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, see [WPA2-Multikey and Rolling-PMK in vWLAN](#).



Not supported on 3000 series AP models. Enabling 802.11r on 30xx will not broadcast SSID.

12. Specify whether the SSID converts multicast or broadcast network traffic to unicast traffic by selecting the appropriate option from the list. 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. It is sent at the rate of the slowest client. Unicast traffic is sent to a single client, and it can be sent at the speed of each client rather than that of the slowest client.

Convert Multicast/Broadcast Network Traffic To Unicast

Dynamic Multicast Optimization

Channel Utilization Threshold

Multicast Rate Optimization

Convert multicast to unicast

Disable

Convert broadcast to unicast

Convert multicast to unicast

Convert broadcast and multicast to unicast

conversion based on Radio Channel Utilization Threshold entered below.

Enter radio channel utilization threshold value percentage. If threshold is exceeded, multicast to unicast conversion is disabled.

Enables transmitting multicast traffic at the highest common transmit rate of multicast clients in the group.



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. See Step 7 and [Configuring Domain Roles](#). Note that the default role of an 802.1x SSID is **n-registered**. If you do not allow multicast traffic in the SSID 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

Dynamically enables or disables multicast to unicast conversion based on Radio Channel Utilization Threshold entered below.

Channel Utilization Threshold

Enter radio channel utilization threshold value percentage. If threshold is exceeded, multicast to unicast conversion is disabled.

Multicast Rate Optimization

Enables transmitting multicast traffic at the highest common transmit rate of multicast clients in the group.

- **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.

Continue with these steps:

1. 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. See [Configuring a Tunnel Profile](#) 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

Not supported on 3XXX model APs.

DHCP Option 82

DHCP Option 82 Circuit ID

DHCP Option 82 Remote ID

HOSTNAME

HOSTNAME

HOSTNAME+SYSLOCATION+MAC

AP-RADIO-MAC

CLIENT_MAC

2. Click **Create SSID**. A confirmation will be displayed indicating the SSID was successfully created.

The SSID is now available for editing or deletion, and can be applied to APs through AP templates. See [Configuring AP Templates](#).

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 routes 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:

- Configuring the tunnel profile
- Enabling the tunnel in the AP template (see [Configuring AP Templates](#))
- Enabling WLAN traffic for the SSID (see [Configuring an SSID](#))

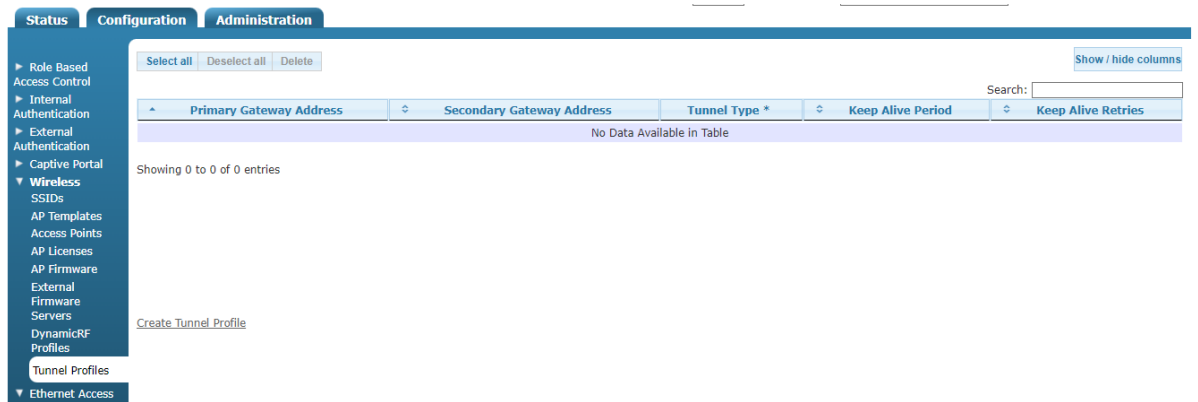
In addition, there can be interactions between a tunnel profile and a defined user role. See [Configuring Domain Roles](#). Consider these role definitions when configuring the tunnel profile:

- The WAG handles all quality of service (QoS) configurations, and not the user role. vWLAN does not handle traffic shaping for tunneled traffic.
- The WAG also handles all firewall configurations, and not the user role. vWLAN does not enforce firewall rules 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:

1. Navigate to the **Configuration > 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.



2. Specify the tunnel type.

The screenshot shows the 'Create Tunnel Profile' configuration form. The form includes the following fields and options:

- Select Tunnel Type:** A dropdown menu set to 'GRE Tunnel'.
- Primary Gateway Address:** A text input field with the note 'Only IP Address is accepted.'
- Secondary Gateway Address:** A text input field with the note 'Optional. Only IP Address is accepted.'
- Keep Alive Period:** A text input field set to '30' with the note 'Valid range is from 30 to 300.'
- Keep Alive Retries:** A text input field set to '5' with the note 'Valid range is from 2 to 10.'
- Create Tunnel Profile:** A button to submit the form.
- Back:** A link to return to the previous page.

3. Enter the IP address for the primary gateway that will serve as the termination point for the tunnel. Optionally, you can also enter a secondary gateway address.
4. Specify the keep alive period in seconds. This interval defines how often to send keep alive messages used to keep the tunnel open.
5. Specify the number of times to resend the keep alive message if no response is received before closing the tunnel.
6. Click **Create Tunnel Profile** to create the profile.

Configuring DynamicSteering for vWLAN

This section contains these topics:

Overview of DynamicSteering	219
Steering Safety Mechanisms	223
Configuring DynamicSteering	223

Overview of DynamicSteering

DynamicSteering is Adtran innovative solution for steering dual-band clients between radios. Using bidirectional steering, DynamicSteering ensures that clients are connected to the best radio based on their signal conditions. Bidirectional band steering includes upgrade steering (2.4 GHz to 5 GHz) and downgrade steering (5 GHz to 2.4 GHz) which allows optimal utilization of both bands.



DynamicSteering was introduced in software version 2.9.0 and is only available for vWLAN and Bluesocket APs (BSAPs) running software versions 2.9.0 or later. DynamicSteering is supported on all BSAPs.

Traditional band steering is often approached unidirectionally (2.4 GHz to 5 GHz) and steers clients using pre-association steering (upon first connection). The result is an over-saturated 5 GHz spectrum with slow initial associations or connection times, and in some cases, no connection at all. DynamicSteering results in a more balanced spectrum usage and only performs pre-association steering when the load or channel utilization is high. It monitors clients and automatically matches them to the appropriate radio on the appropriate AP, delivering consistent, predictable performance and eliminating sticky clients.

A dual-band AP with DynamicSteering enabled makes steering decisions based on:

- Wireless client capabilities
- Signal Strength on the current band
- Signal Strength on the target band
- Medium utilization on current and target bands
- Steering history

There are three primary types of steering supported in vWLAN and described in these sections:

Pre-association Steering	220
Idle-post Association Steering	220
Active Post-association Steering	221

Pre-association Steering

Used only during overloaded conditions, pre-association steering aims to connect dual-band clients to a band that is not overloaded. A band is considered overloaded when its average medium utilization over the span of a minute exceeds 70 percent. If the AP sees a dual-band client sending probe requests and the probe requests on the non-overloaded band exceed a threshold (20 dB), a blacklist is installed to deny associations and suppress probe responses on the overloaded band. This is to encourage the client to associate on the non-overloaded band. The steering safety mechanisms, explained in [Steering Safety Mechanisms](#), are applied to ensure that clients being pre-association steered are not orphaned if they persistently try to associate to the blacklisted band on a given AP.

DynamicSteering avoids steering a client too often by incorporating pre-association steering only when high utilization conditions exist. Otherwise, it performs post-association steering, allowing the client to determine the algorithm used to associate to a band.

Idle-post Association Steering

The AP monitors activity for all of its associated clients for a time period (10 seconds). This value is chosen to account for the fact that some clients periodically send packets (such as an Address Resolution Protocol (ARP) every 15 seconds) as a form of keepalive. These keepalive packets can result in a client never being classified as idle and therefore, will not be idle-post association steered.

When a dual-band client does become idle, its uplink signal strength is evaluated to determine if it would be a candidate for steering to a different band. This evaluation is accomplished by comparing the signal strength on the non-serving bands to a set threshold.

A separate threshold is defined for upgrade steering (-65 dBm) and downgrade steering (-90 dBm) in non-overload conditions. The thresholds for non-overload steering effectively disable downgrade steering for two reasons. First, modern Wi-Fi clients generally roam on their own from 5 GHz to 2.4 GHz once the signal becomes sufficiently weak. Secondly, even at relatively weak signal strength, the 5 GHz performance is typically better than 2.4 GHz, especially if a 40 MHz channel width or higher is used in 5 GHz and only a 20 MHz channel width is used in 2.4 GHz.

Once the determination is made to steer the client, one of these two mechanisms can be used, Legacy (non Base Service Set (BSS) Transition Management (BTM) compliant) or 802.11v (BTM compliant).

Legacy

The legacy approach first installs a blacklist (denying associations and suppressing probe requests) on the currently serving AP band and then forcibly disassociates the client. Probe responses are withheld on the previously serving AP band until the client associates again on a different band or one of the steering safety mechanisms (explained in [Steering Safety Mechanisms](#)) aborts the steering. If the client still tries to authenticate with the previously serving AP band, it is rejected. This is usually sufficient to encourage the client to select a different band.

802.11v

802.11v is a standard defined mechanism that allows an AP to indicate to a client that it should move to a new band and provides a prioritized list of candidate APs. For clients that advertise this capability when associating, the AP attempts to use this mechanism instead of the legacy

mechanism. There is significant variation in how well various client implementations respond to 802.11v BTM requests as explained in [Table 8](#).

Table 8: 802.11v Condition and Behavior

Condition	Behavior
Idle steering must succeed before attempting active steering	This behavior assumes a client that rejects or otherwise fails to move to the desired band under idle conditions is more likely to do the same when active.
Idle steering fails	If idle BTM steering fails, reverts to legacy steering and considers the device as BTM unfriendly for 600 seconds.
Repeated active steering fails BTM unfriendly timer	If BTM active steering repeatedly fails, active steering is not performed again until both an active steering unfriendliness timer expires (600 seconds) and then a BTM idle steer succeeds.
BTM-based steering operating in best effort case	If the uplink signal strength falls below a threshold (12 dB) on the serving channel, BTM-based steering is used without blacklists, and a failure is not counted against the client.
Clients accepting BTM requests specifying a different BSSID	If the client accepts the BTM request but specifies a different basic service set identifier (BSSID), BTM-based steering is used without blacklists, and a failure is not counted against the client. This helps account for environments with multiple APs operating within the same extended service set (ESS) where a client might see a stronger AP and decides to transition to it.



Not all clients honor BTM requests in the same manner. The AP will use the blacklist and probe response-withholding scheme to improve the reliability of the transition.

Active Post-association Steering

For clients that support 802.11k and 802.11v, DynamicSteering can take advantage of these standards to steer them while they are actively exchanging data. This was not possible with the legacy steering mechanism due to the time it took for a client to re-associate, which often lead to application failures.

By utilizing the 802.11v BSS transition management, the clients that support it are able to transition in a much shorter period of time and applications survive the transition with limited impact. For a client to become eligible for active steering, it must first be successfully idle

steered using BTM. Once a client is deemed eligible, certain conditions must be met for it to be active steered. These conditions and the necessary triggers are explained in the sections that follow.

Non-overloaded Active Steering

Non-overloaded active steering is dependent on the conditions present on the serving band which can be the 2.4 GHz or 5 GHz band since DynamicSteering utilizes bidirectional band steering.

1. While on the 2.4 GHz band, both an uplink signal threshold (40 dB) and a downlink PHY rate threshold (50,000 Kbps) must be exceeded to transition to 5 GHz. Both conditions are required to ensure that the client has both a strong enough signal and is not experiencing a high packet error.
2. For a client currently being served on the 5 GHz band, either the uplink signal threshold (40 dB) or the downlink PHY rate (6,000 Kbps) dropping below the threshold is sufficient to start the active steering evaluation process to 2.4 GHz. This more relaxed policy attempts to account for the fact that the PHY rate might stay relatively high even when the signal threshold has dropped significantly.

Once a trigger occurred for non-overload steering, the AP estimates the downlink and uplink throughput for that client using the Tx and Rx byte counters (sampled at the beginning and end of a 1-second interval). At the second sample, the last downlink PHY rate is obtained and used to compute an estimated airtime on the currently serving band. The AP then requests the client perform an 802.11k beacon measurement on the candidate band. From this downlink RSSI measurement, the AP attempts to estimate an Modulation and Coding Scheme (MCS) index value (<http://mcsindex.com/>) that will be achieved by that client (taking into account both the AP and the client capabilities on the candidate band). From this and the previously measured throughput, an airtime value is computed. This value is then used to determine whether the client can fit on the candidate band without causing an overload. This is accomplished by adding the estimated airtime to the last measured medium utilization and comparing the result against a safety threshold as follows:

- For 2.4 GHz, 50 percent of medium utilization plus the projection
- For 5 GHz, 60 percent medium utilization plus the projection

If this threshold is not exceeded, the steer is allowed to proceed and the estimated airtime is added to a projected airtime increase that is maintained until a new medium utilization measurement is obtained.

Overloaded Active Steering

For overloaded active steering, the trigger is the overload event itself.

1. The AP estimates the airtime of all active steering eligible clients on the overloaded band. This is accomplished using the same technique as described above when a single client measurement is triggered. These values are then sorted by airtime in descending order.
2. Each client is requested in-turn to perform an 802.11k beacon measurement to assess its performance on the candidate band. From this, a decision is made in the same manner as above to either steer the client to that band or not depending on the risk of overload. The estimated rate on the target band must be a configurable amount better than the rate on

the current band. Once the handling for one client is completed, consideration then proceeds to the next client with a new 802.11k beacon measurement request.

This process continues until all active steering eligible clients are either exhausted or the medium utilization falls below the safety threshold (after removing the estimated airtime amount from the currently overloaded band).

Any time active steering is performed (either for offloading purposes or due to an individual client crossing of the thresholds), the medium utilization measurement immediately following the event triggers a steering blackout period (15 minutes). During this period, active upgrade steers are not allowed in an effort to assess more accurately the previous active steers without further active steers adding uncertainty to the data. Active downgrade steers are still permitted to ensure clients can maintain connectivity. Idle steers are also permitted during this blackout because these clients are not currently active and should not impact the utilization measurements until they become active.

Steering Safety Mechanisms

Some safety features implemented with DynamicSteering ensure capable clients do not switch to cellular from Wi-Fi because of steering which helps prevent clients from being steered too frequently. At a high level, these safety mechanisms exist:

1. Separate timers for legacy and BTM-based steering
 - When a client is steered, this timer is started, and the AP is prevented from further steering attempts until it expires.
 - Legacy – 300 seconds
 - BTM – 30 seconds
 - The maximum amount of time the AP allows for a client to re-associate after being steered before declaring a failure is 15 seconds.
2. When using the legacy steering approach or BTM steering, the AP will abort the steering if the client tries to authenticate on the old band too many times (three times within two seconds).

Configuring DynamicSteering

DynamicSteering configuration settings are only applied within the same SSID. For dual-band APs, each radio interface (2.4 GHz and 5 GHz) must have the SSID applied to both radios through the AP template.

DynamicSteering is configured in vWLAN using the SSID configuration menu. This section describes the steps necessary to enable and use DynamicSteering. By default, DynamicSteering is disabled.

To configure an SSID to use DynamicSteering:

1. Navigate to **Configuration > Wireless > SSIDs**. This menu lists any previously configured SSIDs.

2. Select either an existing SSID from the list or create a new SSID by selecting **Create SSID**.
3. Select the **DynamicSteering** option to enable the feature. Make any additional SSIDs setting changes as necessary and click **Update SSID** or **Create SSID** to save the settings. A confirmation will display indicating the SSID was successfully created.



You must apply the SSID 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.

4. To apply the SSID to both radios on the applicable APs, navigate to **Configuration > Wireless > AP Templates**. Select the AP template that provides the configuration settings for your APs (or the default AP template, if applicable). Remember that all APs that use this template will also be updated.
5. Select the SSID on which you enabled DynamicSteering and apply to both the 2.4 GHz and 5 GHz radios. Make any additional changes to the AP template as necessary and click **Update AP Template**.

Antenna Mode	<input type="radio"/> 1 Antenna <input type="radio"/> 2 Antennas <input type="radio"/> 3 Antennas <input checked="" type="radio"/> 4 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 type="radio"/> 3 Antennas <input checked="" type="radio"/> 4 Antennas <small>Only applies when configured to a value less than what the AP supports.</small>
SSIDs	0 items selected Remove all <input type="text"/> Add all + 421	0 items selected Remove all <input type="text"/> Add all + 421
Unified Access Groups	0 items selected Remove all <input type="text"/> Add all	

[Create AP Template](#)

You successfully enabled DynamicSteering on your SSID and applied it to the AP. Once the AP template is applied to your AP, the new configuration settings will take effect.

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:

1. Navigate to **Status > 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.

Select all Deselect all Delete Purge Adjacent APs Download Show / hide columns							
Last 30 Days <input type="text" value="Search:"/>							
Source MAC	SSID	Primary Channel	Channel Range	Signal (dBm)	Sensor Name	Last Seen	
B4:A2:5C:0E:0E:D0	000011111_CNM_SIT_MIG	1	1 (20 MHz)	-73	BSAP6040-00-19-92-2d-05-80	2024-10-16 09:56:45 UTC	
B4:A2:5C:70:7B:A0	0011_SS_CNM_SIT migration	6	6 (20 MHz)	-65	BSAP6040-00-19-92-2d-05-80	2024-10-16 11:32:53 UTC	
00:04:56:9C:80:50	0111111111111111_cnPilot_RGVN	1	1 (20 MHz)	-68	BSAP6040-00-19-92-2d-05-80	2024-10-16 01:47:26 UTC	
00:26:07:7D:06:08	0111111111111111_cnPilot_RGVN	1	1 (20 MHz)	-64	BSAP6040-00-19-92-2d-05-80	2024-10-16 00:29:49 UTC	
00:04:56:9C:80:40	0111111111111111_cnPilot_RGVN	1	1 (20 MHz)	-71	BSAP6040-00-19-92-2d-05-80	2024-10-16 11:32:53 UTC	
00:C8:50:BD:91:40	0111_CNMSIT_Voucher	1	1 (20 MHz)	-62	BSAP6040-00-19-92-2d-05-80	2024-10-16 03:32:05 UTC	
00:04:56:BD:91:40	0111_CNMSIT_Voucher	1	1 (20 MHz)	-64	BSAP6040-00-19-92-2d-05-80	2024-10-16 11:32:53 UTC	
00:04:56:BD:86:10	01_CNM_SIT_ESS	1	1 (20 MHz)	-72	BSAP6040-00-19-92-2d-05-80	2024-10-16 11:32:53 UTC	
BC:A9:93:E2:59:90	&%\$01_@_CNM_SIT_Sanity	1	1 (20 MHz)	-67	BSAP6040-00-19-92-2d-05-80	2024-10-16 11:32:53 UTC	

Showing 1 to 100 of 1,330 entries

2. Selecting the entry link in the **Source MAC** column will attempt to locate the adjacency on a heat map (if configured).

Chapter 10

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. See [Licensing APs](#) 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 these sections:

Configuring Unified Access Groups	227
Configuring Switches for Unified Access	230
Unified Access Redundancy	230
Viewing the Status of Unified Access Users	231

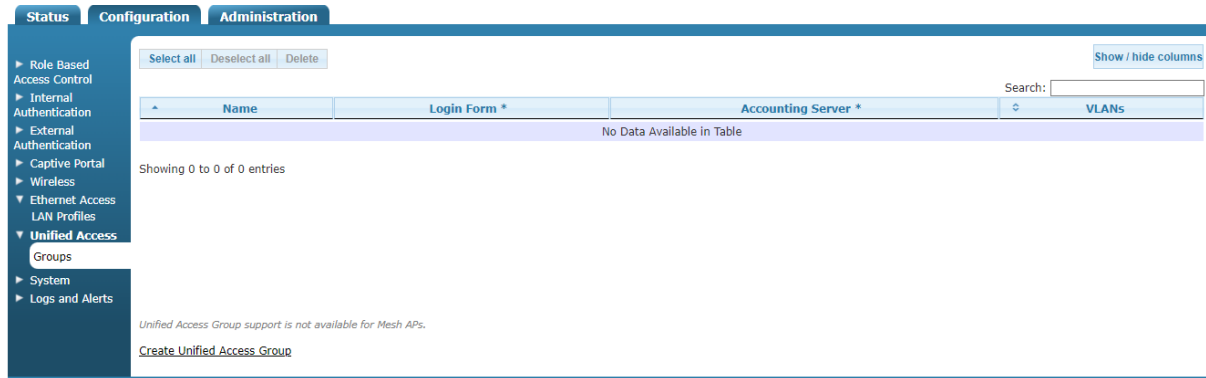
Configuring Unified Access Groups

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:

1. Navigate to **Configuration > 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** menu at the top of the GUI.



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 the AP sees unified access traffic, 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 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 **VLAN** 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.



VLAN IDs **0** and **1** are not allowed.

6. Select the login form to associate with the unified access group from the **Login Form** field. 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, see [Customizing vWLAN Login Forms and Images](#).
7. Select the user role to associate with clients connecting to vWLAN through this unified access group from the **Role** field. 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, see [Configuring Domain Roles](#).

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** field. The accounting server will track the user throughout their use of vWLAN. For more information about creating accounting servers, see [Configuring Domain Accounting](#).



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.

8. Click **Create Unified Access Group** to create the access group. You will receive confirmation that the access group was created.

The created access group is now available for editing or deletion, and will appear in the unified access group list under **Configuration > 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. Add an untrusted VLAN to the switch to support unified access connections to vWLAN.
2. Configure a unified access user port (or ports) as the access port(s) assigned to the untrusted VLAN.
3. Configure the AP port as an 802.1q trunk port (if it is not already) and configure the port 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. Add an untrusted VLAN tag, for the untrusted VLAN used by unified access users, to the switch uplink port on the first switch (the switch used by the unified access users).
2. Trunk the untrusted VLAN to the second switch (the switch used by the AP).
This configuration is 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.



Although you can configure a multiple switch configuration for unified access to vWLAN, the clients and the AP should be 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. You can achieve vWLAN redundancy 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 (see [Configuring High Availability](#) for more information).

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, 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, the system chooses the least loaded AP to take over the untrusted VLAN segment.

There might 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 auto-discovers 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 **Status > 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 displays the 'Unified Access Groups' status page. The top navigation bar includes tabs for 'Status', 'Configuration', and 'Administration'. A left-hand navigation menu lists various system components. The main content area features a table with the following columns: Name, Status, AP Name, Roaming SSID, Segment, and Untrusted VLAN. A search bar is located above the table. The table is currently empty, with the message 'No Data Available in Table' displayed below the column headers. Below the table, it indicates 'Showing 0 to 0 of 0 entries'.

You can also view the status of unified access users by using the **Status** tab. See [Diagnostic Tools](#) and [Managing Users and Locations](#) for more information about viewing and managing users.

Chapter 11

Configuring Client Connections

After you configure 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. This chapter describes these tasks:

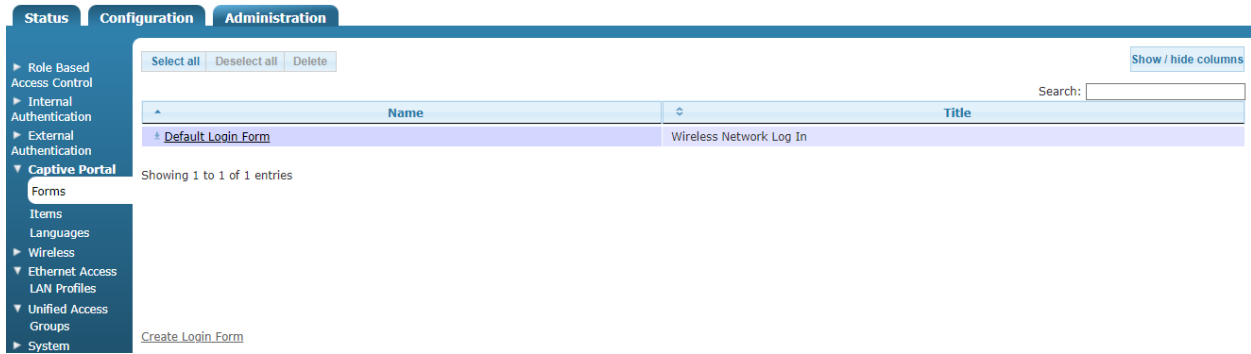
Customizing vWLAN Login Forms and Images	232
Configuring Guest Access Parameters	251
Wireless HotSpot Account Generation	255
Configuring WPA2-Multikey Client Connections	261

Customizing vWLAN Login Forms and Images

You can customize the login screens presented to users of the vWLAN system 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. The administrator for the specific domain creates and edits login forms.

To create or edit a login form, access the GUI and navigate to **Configuration > Captive Portal > Forms**. The existing login forms are listed. 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** menu.



These sections detail the configuration of a customized login form:

- Basic Login Form Configuration 233
- Configuring Authentication using User Name and Password 234
- Configuring User Login Authentication Using an Email Address 235
- Specifying the Login Form Language 236
- Configuring External Redirects 236
- Configuring the User Service Agreement 238
- Specifying the Login Attempts Parameters 238
- Configuring the Visual Elements of the Login Form 239
- Uploading Images and Multimedia for Login Forms 246
- Customizing the Login Language 247
- Viewing Customized Login Pages 250

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:

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** field (see [Wireless HotSpot Account Generation](#) for more information).

Create Login Form

Name

Authentication Method

Hotspot account

Allow User Logins

Allow Guest Logins

Default Language

Redirect Clients To An External URL

Install CA Enabled

Remove if you do not require a CA certificate.

- 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 (see [Configuring Domain Users](#) for more information about configuring the 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, specify that access authentication occurs through a user name and password by selecting the **Allow User Logins** field. 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 user accesses, and can be used independently or in conjunction with email authentication (typically used for guest users).

Create Login Form

Name

Authentication Method

Hotspot account

Allow User Logins

Allow Guest Logins

Default Language

Redirect Clients To An External URL

Install CA Enabled

Remove if you do not require a CA certificate.

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.

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:

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.



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:

1. Specify that access authentication occurs through an email address by selecting the **Allow Guest Logins** field. 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).

Create Login Form

Name

Authentication Method

Hotspot account

Allow User Logins

Allow Guest Logins

Default Language

Redirect Clients To An External URL

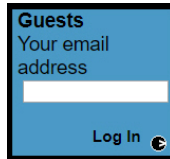
Install CA Enabled

Remove if you do not require a CA certificate.

2. Specify the role that connected guests will have by selecting the appropriate option from the **Guest role** field.

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 (see [Customizing the Login Language](#)).

To specify the language used on the login form, select the appropriate language from the **Default Language** field. The selected language will be used on the user-facing login form.

Create Login Form

Name

Authentication Method

Hotspot account

Allow User Logins

Allow Guest Logins

Default Language

Redirect Clients To An External URL

Install CA Enabled

Remove if you do not require a CA certificate.

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:

1. Enable external redirection by selecting the **Redirect Clients To An External URL** field. Then, provide the URL of the external server to which clients are being redirected.

Redirect Clients To An External URL

Install CA Enabled
Remove if you do not require a CA certificate.

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

vWLAN Login Form ID

Client's MAC Address

Client's Access Point MAC Address

Client's Access Point Name

vWLAN IP Address

Client's Original URL

Client's IP Address

Client's Access Point SSID

Client's VLAN ID

AP Status

AP Template

Double Encoding of URI Parameters

Include RADIUS Option Vendor option



You must ensure that the external server are accessed from the AP and vWLAN. The external server must notify vWLAN when a client 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.`

- 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 AP MAC address, the client AP name, the vWLAN IP address, the client original URL, the client MAC address, the client IP address, the client AP SSID, the client VLAN ID, and the AP 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.
- 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, clear the **Double Encoding of URI Parameters** field.
- 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** field.

After configuring the external redirect settings, you 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 do not use 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.



If you selected to redirect clients to an external URL, these menu options might not be available.

To configure the terms of service for a login form:

1. In the **Create Login Form** menu, select the **Enable Terms of Service** field. By selecting this field you specify 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.

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.

Login Attempts

Maximum Login Attempts Enter '0' for no max.

Minutes To Delay After Maximum Failed Login Attempts

HTML Body

Web Page Title

Background Color

Foreground Color

Link Color

Visited Link Color

Active Link Color

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 (see [Configuring Domain Roles](#)).

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 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 is reached.



If you selected to redirect clients to an external URL, these menu options might not be available.

To specify the login attempts parameters:

1. In 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 **Maximum Login Attempts** field. Entering **0** indicates there is no maximum number.

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.

Login Attempts

Maximum Login Attempts Enter '0' for no max.

Minutes To Delay After Maximum Failed Login Attempts

HTML Body

Web Page Title

Background Color

Foreground Color

Link Color

Visited Link Color

Active Link Color

2. 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 **Minutes To Delay After Maximum Failed Login Attempts** field.

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.



If you have selected to redirect clients to an external URL, these menu options might not be available.

To customize the visual elements of the login form:

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.

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.

Login Attempts

Maximum Login Attempts Enter '0' for no max.

Minutes To Delay After Maximum Failed Login Attempts

HTML Body

Web Page Title

Background Color

Foreground Color

Link Color

Visited Link Color

Active Link Color

- 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** fields. If you uploaded your own logo image to vWLAN, you can select it here (see [Uploading Images and Multimedia for Login Forms](#) 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, clear the **Enable Change Password Button** field. 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** field.

Logos

Top Left Login Image

Powered-By Logo

Enable Change Password Button
Applies to internal authentication only.

Enable Complete Customization

Login Form

Top Login Form

Font Size

Form Colors

Form Background

Users Background

Users Foreground

Guests Background

Guests Foreground

Links Background

Links Foreground



If you select **Enable Complete Customization**, the administrator must specify the entire page. In addition, the **Terms of Service** field must be cleared.

- Specify which login form appears on top by selecting either **Guests** or **Users** from the **Top Login Form** field. This option specifies which login appears first on the page. Then, select the font size for the page from the **Font Size** field. You can select **Small**, **Medium**, or **Large**.
- 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.
- 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=""/>
	<small>Enter "" for max width.</small>
	HTML
Right Side Customization HTML	<div style="border: 1px solid black; height: 100px; width: 100%;"></div>
	<small>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.</small>

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](#). Enter the file in the HTML table cell.



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**.

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 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 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, these will apply when creating fully customized login pages:

- `<!--HOSTNAME-->`
- `<!--ADVANCED-->`
- `<!--USERS-->`
- `<!--GUESTS-->`
- `<!--LINKS-->`
- `<!--LANGUAGE-->`
- `<!--REMOTEADDR-->`

These 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 IP address without NAT



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 [Fully Customized Login page Configuration Differences in vWLAN 2.5.0 and 2.5.1](#). The examples that follow are HTML for vWLAN 2.5.1 and later.

For example, to create a single-click ToS page, enter this:

```
<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 this:

```
<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 this:

```

<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="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">
    User Name: <input type="text" name="bs_name" value="" size="10"/> <br />
    Password: <input type="password" name="bs_password" value="" size="10" /><br />
    <input type="SUBMIT" border="0" value="I Acknowledge Terms & Conditions"
class="btn"/>
  </p>
</form>

```

- 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.

Thank-you Customization HTML

Enter HTML for Thank-you page. Insert <!--ADVANCED--> in somewhere to customize where the advanced text will be placed.

After you configure all the customization options for the login form, click **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.



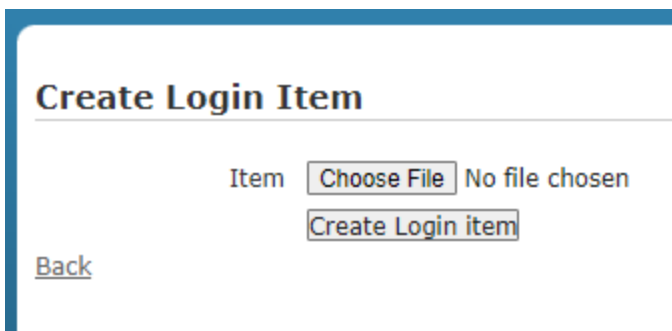
Each domain has a specific amount of storage space for these files. Refer to [Managing Domain Storage Settings](#) for more information about the storage settings.

To upload these files:

1. Access the GUI and navigate to **Configuration** > **Captive Portal** > **Items**. This menu lists any previously uploaded files.
2. Select **Create Login Item** at the bottom of the menu or select **Domain Login Item** from the **Create** menu to add a new image.



3. Use the **Choose File** button to select an image from your location, and then click **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:

1. Navigate to **Configuration > 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** menu.

The screenshot shows the 'Languages' configuration page. The table lists the following languages:

Name	Enabled	Character Set
Catalan	true	ISO-8859-1
Dutch	true	UTF-8
English	true	ISO-8859-1
French	true	ISO-8859-1
German	true	ISO-8859-1
Italian	true	ISO-8859-1
Portuguese	true	ISO-8859-1
Spanish	true	ISO-8859-1
Swedish	true	ISO-8859-1

At the bottom of the table, it says 'Showing 1 to 9 of 9 entries' and there is a 'Create Language' link.

2. Enable the language choice by selecting the **Enabled** field.

Create Language

Language Configuration

Enabled

Language Details

Name

Language Code

Character Set

Native Name

Registered Users Translations

Title

Authentication Server

Username

Password

New Password

New Password Confirmation

Registered Language

Login Button

Terms of Service

Guest Users Translations

Title

Email Address

Login Button

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.
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.
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.
6. Specify the translations for the thank you menu. This is the page viewed by users, whether guest or registered, once they logged in.

Post-Registration Translations

Thank You Page

Link Translations

Change Password

Change Language

Hotspot Account Generation

Login Personal

Install CA Certificate

Software Download

Localization

Help

Hotspot Sign-Up

Signup For

Hours

Days

Weeks

Months

Proceed Button

Checkout Button

Checkout Button

Sponsor Name (Friends/Family)

Sponsor Password (Friends/Family)

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.
8. 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.
9. 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

Email

Description

Notes

Notes

Thank You Texts

Thank You Text

10. Specify the translation for any thank you information.

11. Specify the translation for the various warnings and notices on the vWLAN system.

Warnings and Notices	
You must enable JavaScript in your browser to log in.	You must enable JavaScript in your browser to log in.
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.
Password Expired Reminder	Your password has expired. Please change it to continue.
Password and Confirmation Do Not Match Warning	Password and confirmation do not match.
New Password Must Be Different From Current Password Warning	New password must be different from current password.
Password Can Only be Changed on Master Error	Sorry, at this time, passwords can only be changed on the master.

12. After entering all the translation information, create the language by clicking **Create Language** button at the bottom of the menu.

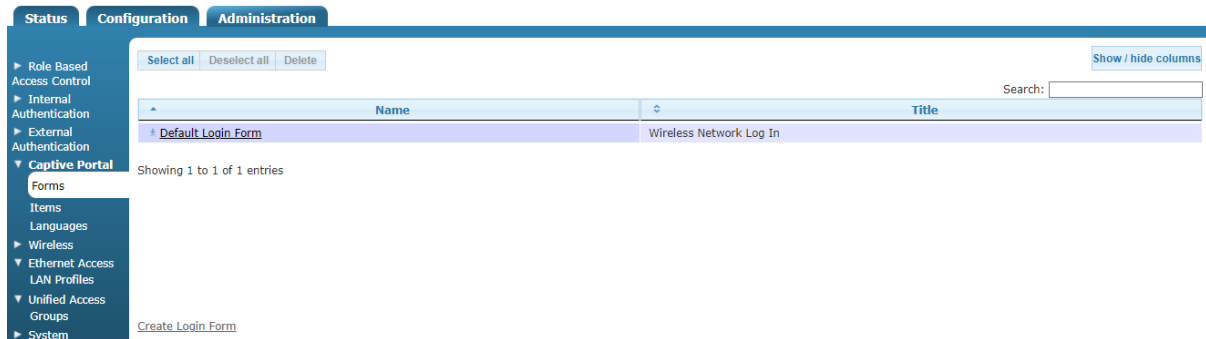
You will receive confirmation that the language was successfully created, and the language will now appear in the language list under **Configuration > Captive Portal > Languages**. The language will also now be available to add to a customized login form.

Viewing Customized Login Pages

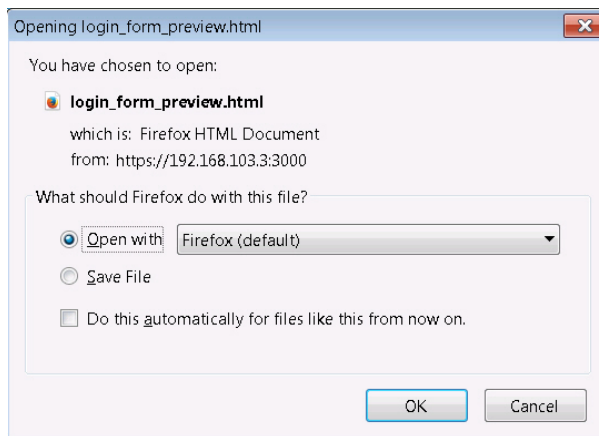
You can choose to preview your customized login page. These previews are not functional pages, for example, the links do not function, but you can use them to preview the design and layout of the login pages. Users or guests will see when accessing vWLAN.

To view a login page preview:

1. Navigate to **Configuration > Captive Portal > Forms**. Click the download icon next to the login form item you want to view.



2. At the prompt, click **OK** to preview the login form in your browser.



Your browser will then display the login form preview. Keep in mind that the links will not function in this preview, and if you use any special characters, the character settings might default to your browser settings. Close the browser window when you finished previewing

the login form.

Login pour Invités

Votre adresse de courrier électronique

Identifiez-vous

Login pour Utilisateurs

Configuring Guest Access Parameters

The administrator configures the guest access 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 these sections:

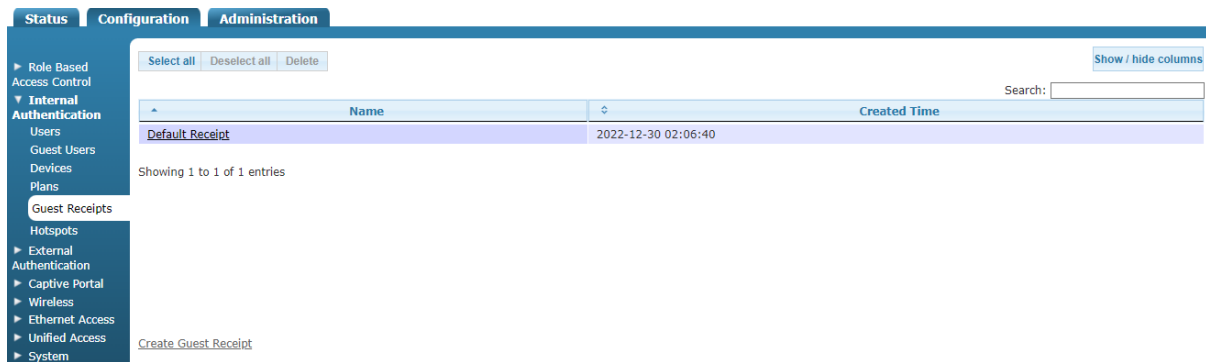
Configuring Guest Receipts	251
Creating Guest User Accounts	253

Configuring Guest Receipts

You can use guest receipts 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 under 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:

1. Connect to the GUI, and navigate to **Configuration > 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** menu.



2. Select a logo and icon image to use in the receipt. Click **Choose File** 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** fields.

Create Guest Receipt

Logo Image No file chosen

Delete Logo Image

Icon Image No file chosen

Delete Icon Image

Name

Header

Body

You can use any of the following attributes surrounded by curly braces. e.g. {{name}}, {{password}}, {{created_at}}, {{max_num_login}}, {{expiry_time}}, {{cleanup_time}}.

3. Specify the name for the guest receipt in the **Name** field.
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.
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.

This example adds extra instructions and includes the account user name, password, number of simultaneous users allowed, account creation time, and account expiration time:

Body

```
Your guest account has been created and is now ready to use.
To access your account, follow these steps:

1. Make sure your network adapter is set to "DHCP - Obtain an IP address automatically."
2. Open your Web browser and enter your user name and password in the provided fields.

    User Name: {{name}}
    Password: {{password}}

Make sure to review your account details before use. Contact the front office if you need assistance.

Account User Limit: {{max_num_login}}
Account Creation Date: {{created_at}}
Account Expiration Date: {{expiry_time}}
```

You can use any of the following attributes surrounded by curly braces. e.g. `{{name}}`, `{{password}}`, `{{created_at}}`, `{{cleanup_time}}`.

Create Guest receipt

6. Click **Create Guest Receipt** to create the receipt. Once created, you will receive confirmation that the receipt was created and the receipt will now appear in the receipt list under **Configuration > Internal Authentication > Guest Receipt**. You can now associate this receipt with any created guest users.

Creating Guest User Accounts

You can create guest user accounts for a single user or 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 see [External Server Authentication](#) for information about creating external authentication servers.

To create a guest account:

1. Access the GUI and navigate to **Configuration > Internal Authentication > Guest Users**. Select **Create Guest Users** at the bottom of the menu or select **Domain Guest User(s)** from the **Create** menu.

The screenshot shows the Adtran configuration interface. The top navigation bar includes 'Status', 'Configuration', and 'Administration'. The left sidebar shows a tree view with 'Internal Authentication' expanded to 'Users'. The main content area displays a table with columns: Name, Enabled *, Role, Guest Receipt, and Created Time. The table is currently empty, showing 'No Data Available in Table'. A search bar is located at the top right of the table area. Below the table, there is a 'Create Guest Users' link.



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.

- 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.

The screenshot shows the 'Create Guest User(s)' configuration form. The form includes the following fields and options:

- Number of Users:** A text input field containing the value '1'. Below it is the text: 'Number of users to create (1-500).'.
- User Prefix:** A text input field containing the value 'user_'. Below it is the text: 'The automatically generated usernames will start with the prefix. e.g. 'user_' produces 'user_1', 'user_2', ...'.
- Password Generation Method:** Two radio buttons: 'Unique Password' (selected) and 'Default Password'. Below them is the text: 'Choose a password generation method.'.
- Enabled:** A checked checkbox.
- Password Length:** A text input field containing the value '8'.
- Guest Receipt:** A dropdown menu with 'Default Receipt' selected. Below it is the text: 'Select an existing guest receipt. This will be used to print out user(s) receipt(s).'.
- Hotspot Plan:** A dropdown menu with 'Minute Plan' selected. Below it is the text: 'Select an existing plan.'.
- Simultaneous User Authentication:** A text input field containing the value '1'. Below it is the text: '0 is unlimited.'.
- Expiry Time After First Login:** A text input field. Below it is the text: 'Enter a value between 1-120 Minutes.'.

At the bottom of the form is a button labeled 'Create Guest User(s)'.

- 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**, and so on.



If the user name does not end in an underscore (**_**), and you create a single guest user, no number is appended to the user name. Otherwise, a unique number is always appended to the user name.

- Specify the user password generation method by selecting either **Unique Password** or **Default Password**. Specify unique password lengths 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** field. The guest receipt can include the user name, password, number of simultaneous users, creation time, cleanup time, and expiration time of the account. See [Configuring Guest Receipts](#) 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** field. Selections include minute, hourly, daily, weekly, and monthly plans, as well as any other plans you created. See [Hotspot Account Configuration](#) for more information about configuring connection plans.
7. Specify the account expiration time (in minutes) using the sliding bar. Specify a time between **1** and **120** minutes.



The account expiration values will change depending on the hotspot plan associated with the user account.

8. Click **Create Guest Users** to create the user account(s).

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.



You can only delete, edit, or view the guest accounts that you 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 contains these topics:

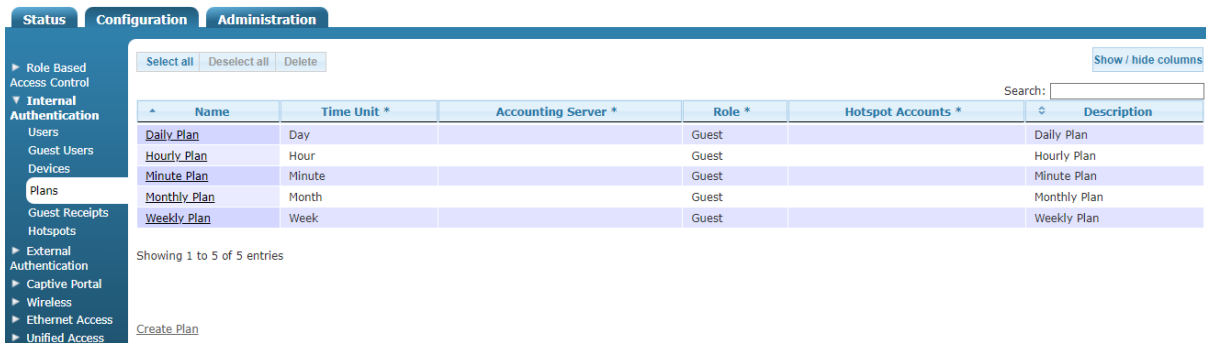
- Hotspot Plan Configuration 256
- Hotspot Account Configuration 258
- Friends and Family Account Example Configuration 260

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:

1. Navigate to **Configuration > Internal Authentication > Plans**. To edit an existing plan, select the plan from the list. 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** field if administrators will be able to assign the plan to guests they created.

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 used or 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.

[Create Hotspot Plan](#)

- Specify the time unit used by the plan by selecting the appropriate unit from the **Time Unit** field. 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.
- Specify the role associated with the hotspot plan by selecting the appropriate option from the **Role** field. 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.
- Optionally select an accounting server to be associated with the plan from the **Accounting Server** field.
- 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**).
- Click **Create Hotspot Plan** to create the plan. Once created, you can use the plan during hotspot account creation.

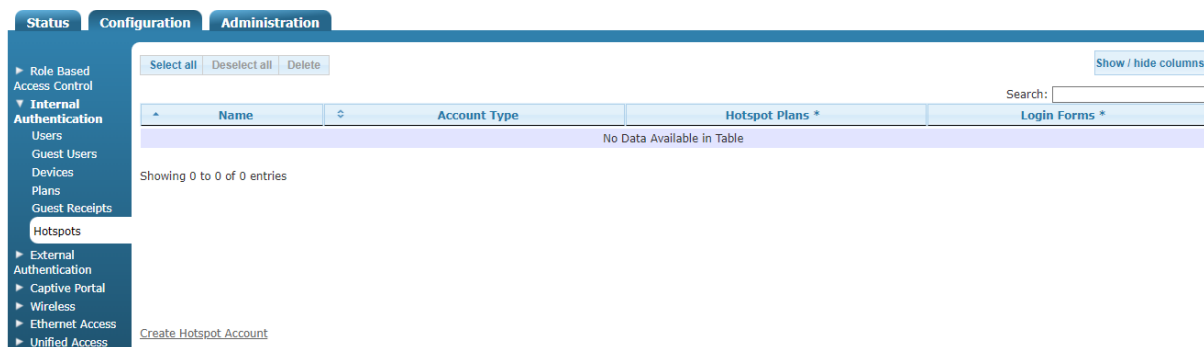
Hotspot Account Configuration

Hotspot accounts are the accounts used by guests to access vWLAN. There are three types of hotspot accounts:

- **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 (see [Email Account Configuration](#)). The login credentials are sent to the user, who can then use them to log into vWLAN.
- **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** 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 (see [Email Account Configuration](#)). The login credentials are sent to the user, who can then use them to log into vWLAN.

To create a hotspot account:

1. Navigate to **Configuration > Internal Authentication > Hotspots**. This menu lists any previously created hotspot accounts. You can choose to edit a previously created account by selecting the appropriate account from the list. To create a new account, select **Create Hotspot Account** at the bottom of the menu or select **Domain Hotspot Account** from the **Create** menu at the top of the GUI.



2. Enter the name for the hotspot account in the **Name** field.

Create Hotspot Account

Name

Hotspot Plans **0 items selected** [Remove all](#) [Add all](#)

- + Daily Plan
- + Hourly Plan
- + Minute Plan
- + Monthly Plan
- + Weekly Plan

Login Forms **0 items selected** [Remove all](#) [Add all](#)

- + Default Login Form

Account Type

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**. See [Customizing vWLAN Login Forms and Images](#) for more information about configuring login forms.
5. Specify the account type from the **Account type** field. You can select **Friends and Family**, **Free Spot**, or **DNA**.

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. Select the email server from the **Email Configuration** field and select the authentication server from the **Authentication Server** field.

Account Type

Email Configuration

Authentication Server

Email Settings

Merchant Name

Merchant Address

Reply To

Subject

Message

[Create Hotspot Account](#)

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, click **Create Hotspot Account** to create the account.

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** field, and click **Create Hotspot Account** to create the 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** field.

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.

6. Click **Create Hotspot Account** after you specify the account type and any additional parameters. You will receive confirmation that the account was successfully created.

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 email address. Once the account is created, vWLAN emails the user name and password to the guest email address just entered by the registered user.

To configure the Friends and Family account:

1. Edit or create the hotspot plan to be used by this account. You can access hotspot plans by navigating to **Configuration > 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](#).
2. Configure an email account for the hotspot account. Details of email account configuration is detailed in [Email Account Configuration](#).
3. Configure the Friends and Family hotspot account as described in [Hotspot Account Configuration](#). Be sure to select **Friends and Family** from the **Account Type** field. When you make this selection, additional fields are displayed for you to complete. The **Merchant Name** and **Address** fields are your organization 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 fields. Click **Create Hotspot Account** when all the fields are complete.

Once the account is 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 WPA2-Multikey feature is not supported on 1900 series APs.

These sections outline the specifics of the WPA2-Multikey feature, its use cases, and its configuration process.

WPA2-Multikey Use Cases and Authentication Process	262
WPA2-Multikey Configuration Considerations	263
Configuring the RADIUS Server for the WPA2-Multikey Feature	263
Configuring the WPA2-Multikey Feature in vWLAN	265

For more specific information about the configuration of WPA2-Multikey feature, see [WPA2-Multikey and Rolling-PMK in vWLAN](#).

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 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 this authentication process takes place:

1. Once the client 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 password and assigned VLAN ID.
3. The client is then prompted to enter their password.

4. If the client 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 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 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](#)).



Make sure that you already configured an external RADIUS server.

To configure the RADIUS server for the WPA2-Multikey feature, connect to vWLAN and complete these tasks:

Configuring the External RADIUS Server for WPA2-Multikey	264
Configuring the External Accounting Server for WPA2-Multikey	265

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.

To configure an external RADIUS server for the WPA2-Multikey feature:

1. In the vWLAN GUI, navigate to **Configuration > External Authentication > Servers > Create Authentication Server**.
2. In the **Create Authentication Server** menu:
 - 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** field to enable the enhanced version of the WPA2-Multikey feature. When this field is selected, the external server can generate up to **1000** PMKs.
 - Enter the IP address of your RADIUS server in the appropriate field.
 - Set the **Port** value to **1812** (that is the default setting).
 - Verify that the **Radius COA** field 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. Click **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.

To configure an accounting server for the WPA2-Multikey feature:

1. In the vWLAN GUI, navigate to **Configuration > External Authentication > Accounting > Create Accounting Server**.
2. In the **Create Accounting Server** menu:
 - Enter a name for the server in the **Name** field.
 - Verify that the **Enabled** field is selected.
 - Enter the IP address of your RADIUS server in the appropriate field.
 - Set the **Port** value 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. Click **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.

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. These steps outline the basic configurations for enabling and using the WPA2-Multikey feature:



You must be familiar with configuring and using vWLAN, SSIDs, Captive Portal, and in general, the wireless network. The steps that follow 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. For more information, see [Configuring an](#)

SSID.



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](#).

4. Apply the created 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.



For more information about AP templates and their configuration or application, see [Configuring AP Templates](#).

Chapter 12

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 these sections:

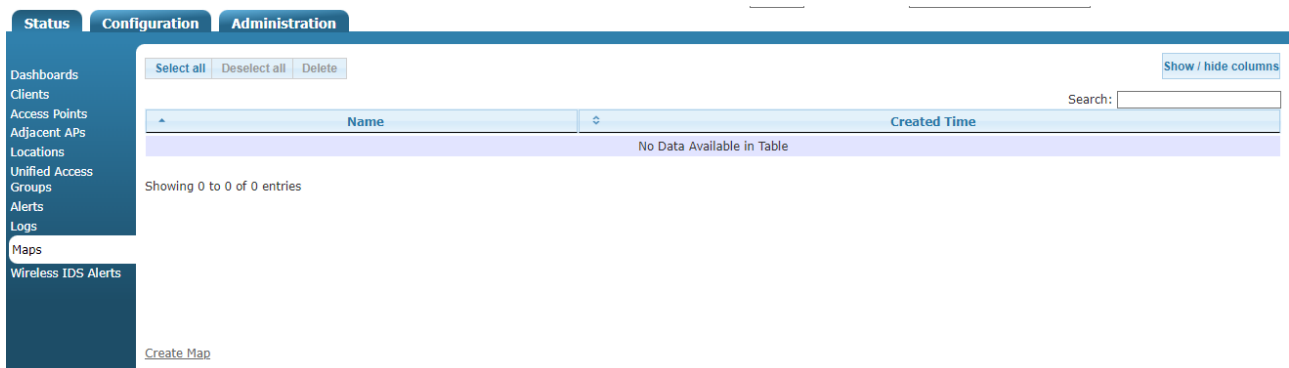
Using Heat Maps	267
Configuring Wireless IDS Alerts	269
Managing Users and Locations	275

Using Heat Maps

You can create heat maps based on the RF coverage of APs within the domain. Use heat maps to verify coverage areas, AP functionality and power usage, RF signal location, and environmental changes. You can also use heat maps, 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:

1. Navigate to **Status** > **Maps**. This menu list any previously created maps. 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** menu.



2. Enter the name for the map in the **Name** field.

Create Map

Name

Floor Map Image No file chosen
Use a JPEG or PNG format image.

Map Environment

Accesspoints **0 items selected**

- + BSAP2030-00-19-92-4b-fd-00
- + BSAP3040-00-19-92-4f-3e-20
- + BSAP6020-00-19-92-2d-84-c0
- + BSAP6020-00-19-92-2f-81-20
- + BSAP6040-00-19-92-2d-05-80
- + BSAP6040-00-19-92-2d-05-c0
- + BSAP6120-00-19-92-2a-d6-e0

Use Calibration

Unit Feet

Meters

3. Upload a map file to the new map by selecting a file to upload from your location by selecting **Choose File**.
4. Specify the map environment (**Open Space, Cubicles, Interior Walls, Cubicles and Interior Walls, Outdoor Open Space, Woods, Buildings, or High Buildings**) from the **Map Environment** field.
5. 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** field.



If the heat map is not calibrated precisely, the APs might not be displayed on the map.

6. Click **Create Map** to create the map. A confirmation indicating the successful creation of the new map is displayed.

Once the map file was 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 9](#) indicates the signal strength and corresponding color on the heat map.

Table 9: Heat Map Signal Strength Color

Signal Strength (dBm)	Color
-35 or greater	Red
-50	Orange
-60	Yellow
-70	Green
-80	Blue
-85	Dark Blue
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 10](#) are enabled by default. In the GUI, you can specify which alerts are enabled or disabled.

Each alert type is listed in the **Configuration > Logs and Alerts > 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 10: 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 http://sourceforge.net/projects/airjack/ .

RF Alert	Severity	Mode of AP Required to Detect	Alert Description
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.
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.

RF Alert	Severity	Mode of AP Required to Detect	Alert Description
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.
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.

RF Alert	Severity	Mode of AP Required to Detect	Alert Description
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.
Invalid Disconnect Code	Warning	Dual Mode or Sensor Mode	Unknown disassociation reason code. Some APs and drivers cannot handle improper reason codes.

RF Alert	Severity	Mode of AP Required to Detect	Alert Description
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.
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.

RF Alert	Severity	Mode of AP Required to Detect	Alert Description
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 rouge AP has changed the SSID.
Rogue AP	Severe	Dual Mode or Sensor Mode	A rouge 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 **Configuration > Logs and Alerts > Wireless IDS Alert Config**. This menu lists the supported RF alerts. Select the appropriate **Alert Type** from the list to enable or disable the specified alarm.

Alert Type	Enabled	Required AP Mode	Description
Airjack Attack	Enabled	Sensor Mode Only	Airjack is a toolset that allows attackers to inject fake 802.11 packets in order to gain network access or create a DoS attack.
AP Broadcasting Multiple SSID	Enabled	Sensor Mode Only	The AP is broadcasting multiple SSIDs. This can indicate a spoof attempt
AP Channel Change	Disabled	Dual Mode or Sensor Mode	The Access Point has changed channels.
AP Denied Association	Enabled	Dual Mode or Sensor Mode	An authorized AP denied an association request from client.
AP Denied Authentication	Enabled	Dual Mode or Sensor Mode	An authorized AP denied client access due to authentication failure.
AP Down	Disabled	Sensor Mode Only	The AP is down.
AP in WDS Mode	Disabled	Dual Mode or Sensor Mode	AP is operating in WDS (bridge) mode.
AP Low Signal Strength	Disabled	Sensor Mode Only	An AP with low signal strength is detected by BAP sensor.
AP Overloaded	Enabled	Dual Mode or Sensor Mode	An overloaded AP refuses new clients from associating with it.

Showing 1 to 40 of 40 entries

2. Select or clear the **Enabled** field to enable or disable the alert. Click **Update Alert Type** to apply the changes.

Edit Alert Type

Alert Type AP Denied Association

Enabled

Description An authorized AP denied an association request from client.

Minimal Sensor Level Dual Mode or Sensor Mode

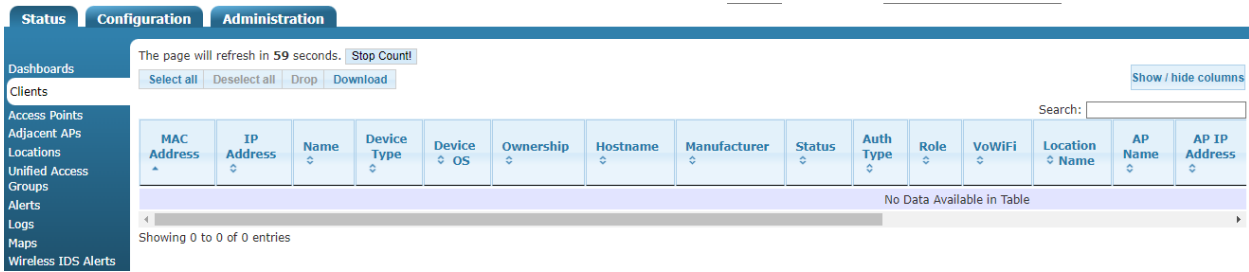
[Back](#)

For instructions on viewing RFID alarms or alerts, see [Viewing/Acknowledging Wireless IDS Alerts](#). See [SNMP Trap Configuration](#) and [Syslog Configuration](#) for more information.

Managing Users and Locations

You can view users 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, and so on) and determine who is connected to the domain, how long they were connected, and how much traffic they are generating.

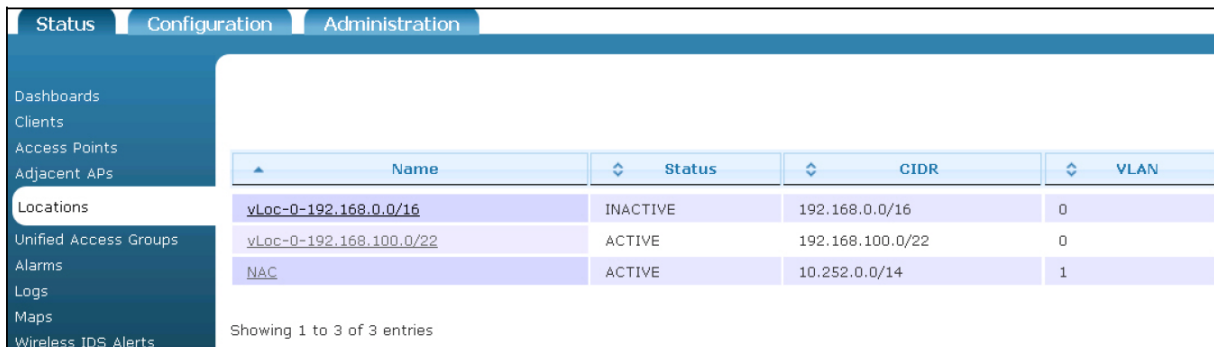
As of firmware release 3.1.0, you can select the **Download** button to download a CSV file of the table data. This download option is also available from the **Status > Access Points** menu.



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 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](#).



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 you can view it 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 name, and the time of the event. To view any RF alerts that are 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
00:19:92:4F:3F:09	Rogue AP	3040-1x-Non-native-SSID	BSAP6040-00-19-92-2d-05-80	2024-10-17 13:09:39 UTC	No
00:19:92:2D:06:61	Rogue AP	basement-11ac	BSAP6040-00-19-92-2d-05-c0	2024-10-17 13:38:32 UTC	No
CC:66:18:CD:C4:7A	Rogue AP	Adtran-c470	BSAP6040-00-19-92-2d-05-80	2024-10-17 13:09:39 UTC	No
88:5B:DD:79:5A:25	Rogue AP	advaoptical.com	BSAP6040-00-19-92-2d-05-80	2024-10-17 13:09:38 UTC	No
38:F8:F6:00:26:6C	Rogue AP	WIFI_AMUNTY_5G	BSAP6040-00-19-92-2d-05-80	2024-10-17 13:09:38 UTC	No
00:19:92:4F:3F:0C	Rogue AP	3040-Alexa_Multikey	BSAP6040-00-19-92-2d-05-80	2024-10-17 13:09:39 UTC	No
00:19:92:28:48:0C	Rogue AP	6040-Beacon-CI-UNREG-NAC	BSAP6040-00-19-92-2d-05-80	2024-10-17 13:09:38 UTC	No
00:19:92:45:9C:A9	Rogue AP	multi_Open	BSAP6040-00-19-92-2d-05-c0	2024-10-06 17:54:10 UTC	No
38:F8:F6:56:27:FA	Rogue AP	INTROP-ADTN	BSAP6040-00-19-92-2d-05-80	2024-10-17 13:09:38 UTC	No
38:F8:F6:00:21:EC	Rogue AP	WIFI_GLMRQA_5G	BSAP6040-00-19-92-2d-05-80	2024-10-17 13:09:39 UTC	No
00:19:92:4B:D0:89	Rogue AP	2030-1x-Non-native-SSID	BSAP6040-00-19-92-2d-05-80	2024-10-16 07:27:47 UTC	No
00:19:92:2D:85:29	Rogue AP	KVM-SSID-TEST	BSAP6040-00-19-92-2d-05-80	2024-10-17 04:16:56 UTC	No
38:F8:F6:75:4D:AA	Rogue AP	INTROP-ADTN	BSAP6040-00-19-92-2d-05-80	2024-10-17 13:09:38 UTC	No
00:19:92:4F:3F:0B	Rogue AP	3040-Alexa-Open	BSAP6040-00-19-92-2d-05-80	2024-10-17 13:09:39 UTC	No
38:F8:F6:74:61:EA	Rogue AP	Adtran-61e0	BSAP6040-00-19-92-2d-05-80	2024-10-17 13:09:39 UTC	No
38:F8:F6:75:4D:AA	Rogue AP	INTROP ADTN	BSAP6040-00-19-92-2d-05-80	2024-10-17 13:09:39 UTC	No

Acknowledge an alert by selecting the alert you want to acknowledge and then select **Acknowledge**.

Log 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.

Chapter 13

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	278
Configuring Notifications	279
Administrative Tasks	287
Configuring vWLAN Jobs	288
Diagnostic Tools	289
Viewing and Searching Logs	293
Viewing Alerts	294
Using the Reporting Dashboard	295

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 you can upload for captive portal configurations. You can specify domain storage settings 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 are 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, you cannot upload new items 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:

1. Navigate to **Configuration > System > Storage Settings**. Select the storage setting item from the list.

The screenshot shows a web interface with a navigation menu on the left and a table of storage settings. The navigation menu includes sections for Role Based Access Control, Internal Authentication, External Authentication, Captive Portal, Wireless, Ethernet Access, Unified Access, System (Network, Interfaces, Domains, Settings, Branding), Storage Settings, and High Availability. The Storage Settings section is highlighted. The table below shows one entry for 'login_items' with a value of 10 MB.

Resource	Option *	Value *
login_items	Per domain	10 MB

Showing 1 to 1 of 1 entries

2. Specify the storage space allocation method. To allocate a specific amount of storage space per domain, select **Allocate each domain __MB** and enter a value in MB. To allocate a specific amount of storage space per AP on the domain, select **Allocate each domain __MB per AP** and enter a value 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 you choose this method for allocating storage space, you can edit the space from the domain configuration (see [Creating the Domain](#)).

The screenshot shows the 'Edit Storage Setting' form. It has three radio button options for the Storage Strategy: 'Allocate each domain 10 MB', 'Allocate each domain MB per AP', and 'Specify the storage for each domain'. The 'Specify the storage for each domain' option is selected. Below the radio buttons is a 'Default' field with the value '10' and 'MB' next to it. There is an 'Update Storage setting' button and a 'Show | Back' link at the bottom.

3. Click **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 these sections:

Notification Templates	280
SNMP Trap Configuration	280
Syslog Configuration	282
Email Account Configuration	283
Creating Alert Templates	284
Log Messages	286

Notification Templates

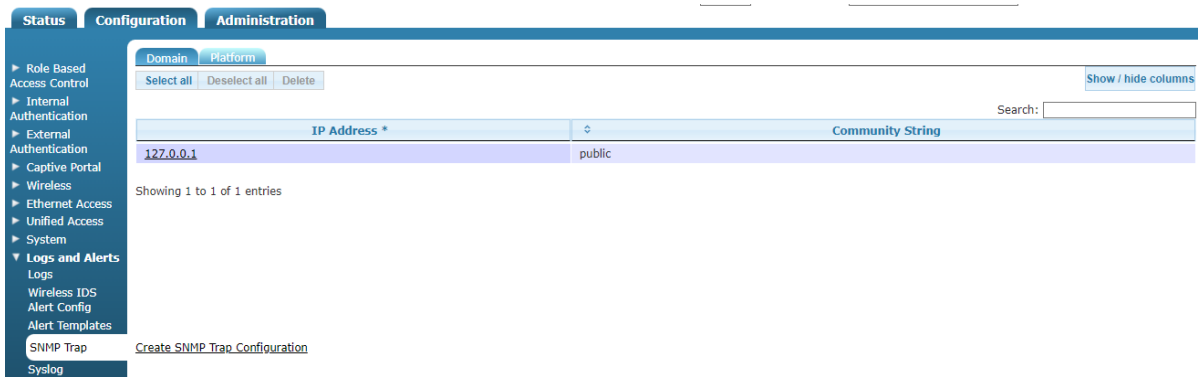
Notification templates are the criteria used by vWLAN to determine when information messages are generated, and to organize these messages according to type. By default, three notification templates exist in vWLAN: debug, error, and info. These templates can be deleted, edited, or displayed, and you 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 want use any of these notification features. To complete these actions, follow the steps outlined in the next sections.

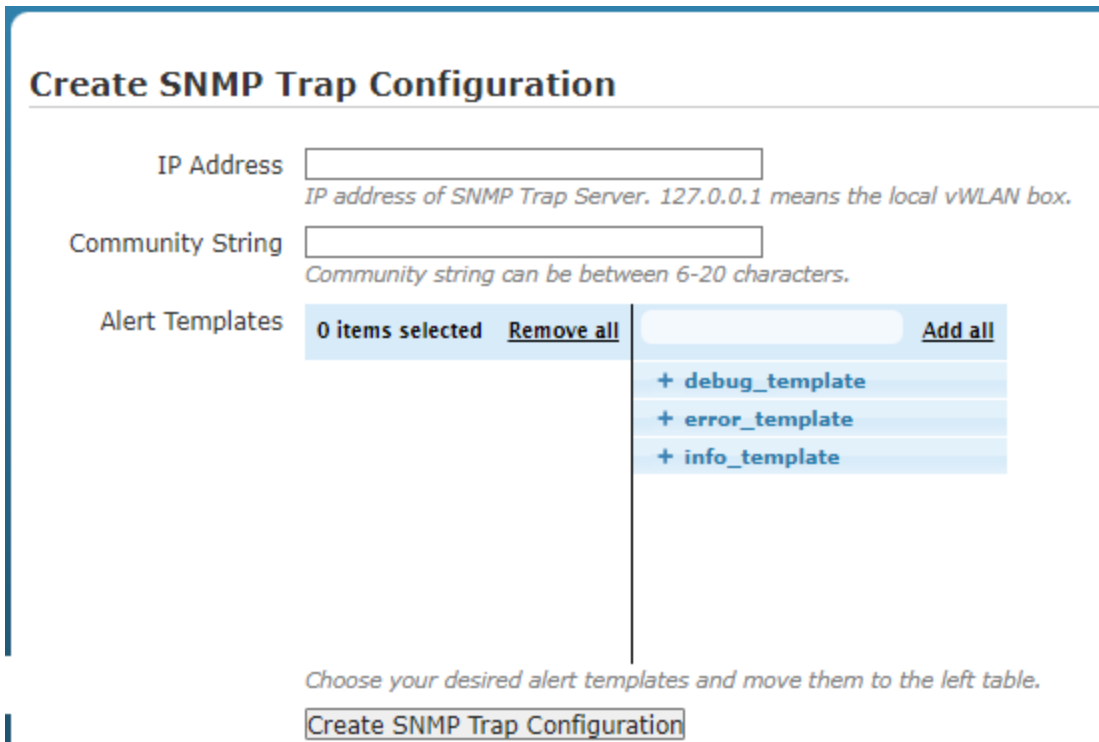
SNMP Trap Configuration

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:

1. Navigate to **Configuration > Logs and Alerts > SNMP Trap**. Select the **Domain** tab if you create an SNMP trap for a specific domain, and select the **Platform** tab if you create an SNMP trap for the vWLAN platform. This menu lists any previously configured traps. 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** menu at the top of the GUI.



2. 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 (see [Configuring AP Templates](#)).



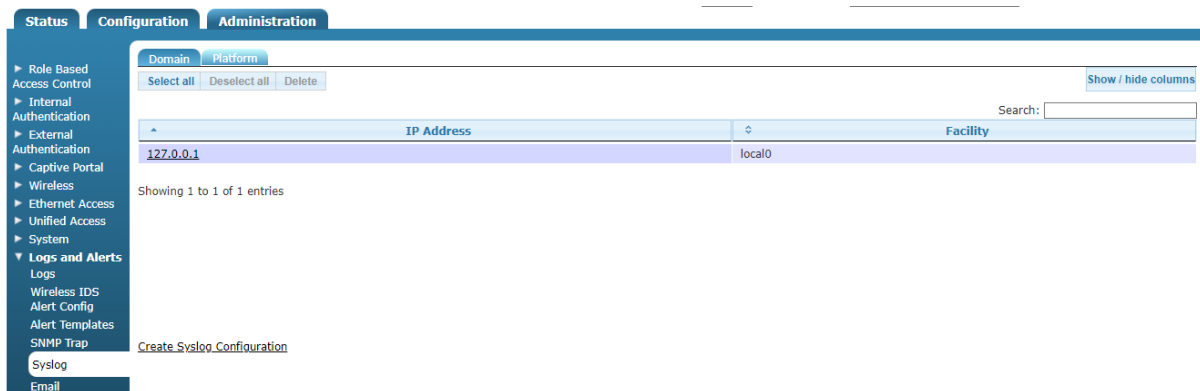
3. Click **Create SNMP trap configuration**. A confirmation is displayed indicating that the trap was created. The trap will now appear in the SNMP trap list under **Configuration > Notifications > SNMP Trap**, where you can display, edit, or delete the trap.
 If you are in the process of creating an SNMP trap in order to create a notification template, you can continue on to the next step of creating a syslog configuration. After you create the notification template, and you want to associate it with this SNMP trap, return to

Configuration > **Notifications** > **SNMP Trap** and edit the trap, making sure to select the correct template from the field. If you only want to configure an SNMP trap, the configuration is complete.

Syslog Configuration

You can use Syslog for managing the vWLAN system by aiding in the creation of generalized informational, analysis, or debug messages. Syslog allows vWLAN to report data and store it locally or in an external syslog server later analysis. To create a syslog notification:

1. Navigate to **Configuration** > **Logs and Alerts** > **Syslog**. Then, select the **Domain** tab if you want to create syslog reports for a specific domain, or select the **Platform** tab if you create syslog reports for the vWLAN system. This menu lists any previously configured logs. 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** menu at the top of the GUI.



2. 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).

Create Syslog Configuration

IP Address

IP address of syslog server. 127.0.0.1 means the local vWLAN box.

Facility

Alert Templates **0 items selected** [Remove all](#) [Add all](#)

- + debug_template
- + error_template
- + info_template

Choose your desired alert templates and move them to the left table.

[Create Syslog Configuration](#)

[Back](#)

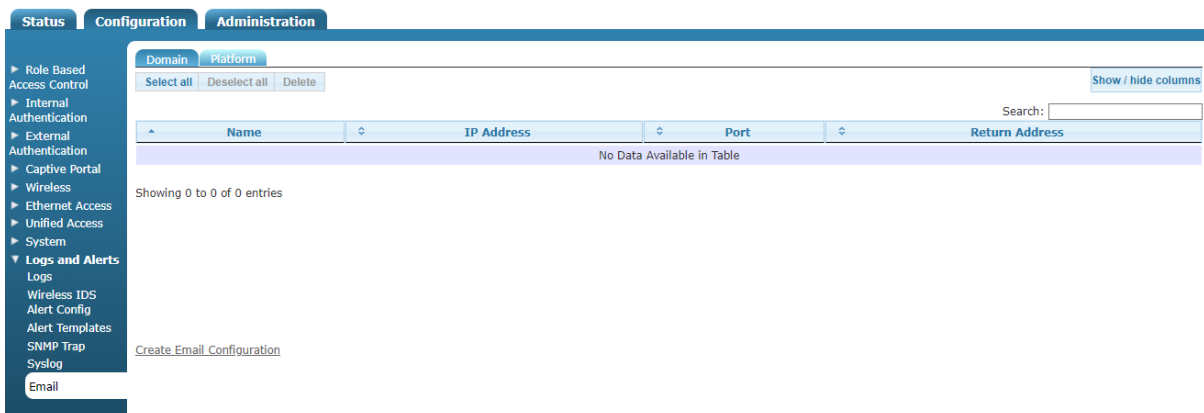
3. Select the facility associated with the trap from the **Facility** field. The facility is the type of system that is monitored by the syslog. vWLAN supports the use of local facilities (**local0** through **local7**) to monitor local use, but the facility is important for external syslog messages 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 (see [Notification Templates](#)).
4. Click **Create Syslog configuration**. A confirmation is displayed indicating that the syslog configuration was created. The syslog notification will now appear in the syslog list under **Configuration > Logs and Alerts > Syslog**, where you can display, edit, or delete the notification.

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. After you create the notification template, and you want to associate it with this syslog configuration, return to the **Configuration > Logs and Alerts > Syslog**, and edit the notification, making sure to select the correct template from the field. If you only want to configure a syslog notification, the configuration is complete.

Email Account Configuration

You can configure email notification of certain events observed by vWLAN 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:

1. Navigate to **Configuration > Logs and Alerts > Email**. If you want to configure an email server for a specific domain, select the **Domain** tab. To configure an email server for the vWLAN system, select the **Platform** tab. This menu lists any previously configured email accounts. 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** menu at the top of the GUI.



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

vwlan@adtran.com.

Create Email Configuration

Server name

Server IP Address Or Hostname

Server Port Number

Return Email Address

Authentication Method

SMTP User Name

SMTP Password

SMTP Password Confirmation

Email Security

Verify Certificate

[Create Email Configuration](#)

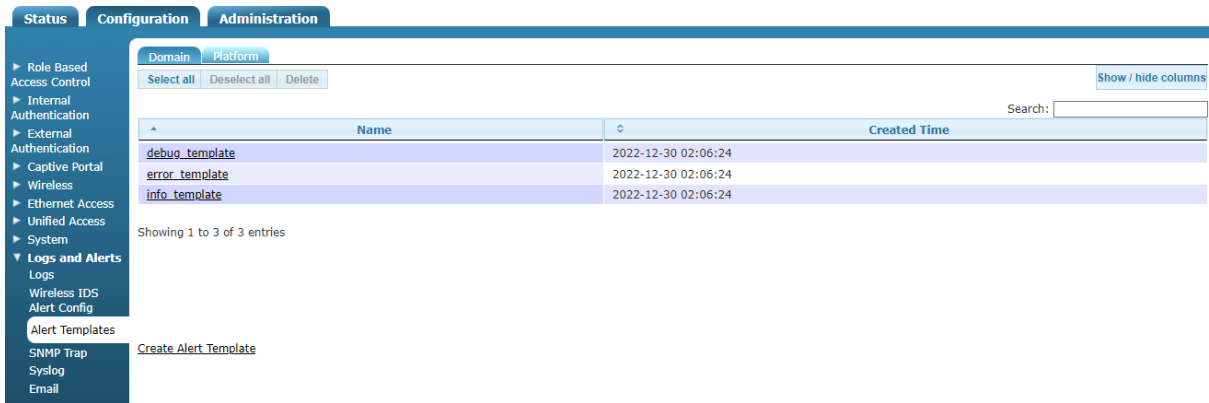
[Back](#)

3. Select the authentication method used by this email account from the 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** field. If you enable email security, you will also be prompted to enable certificate verification. You can disable this option by clearing the **Verify Certificate** field. 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.
4. Click **Create Email Configuration**. A confirmation is displayed indicating that the email account was created. The email account will now appear in the list under **Configuration > Logs and Alerts > Email**, where you can display, edit, or delete the email account.
If you are in the process of creating an email account to create a notification template, you can continue on to the next step of creating the template.

Creating Alert Templates

You can use alert templates to specify the kind of messages and alerts that are created by vWLAN. In addition, alert templates use any configured SNMP traps, syslogs, and email accounts to create customized alerts based on vWLAN systems and alert preferences, with the ability to send specific alerts to configured email accounts. By default, three alert templates exist in the vWLAN: debug, error, and info templates. Use these templates to determine what kind of informational messages are displayed, and each informational message is associated with a specific template. To create an alert template, or edit an existing template:

1. Navigate to **Configuration > Logs and Alerts > Alert Templates**. If you want to create an alert template for a specific domain, select the **Domain** tab. To create an alert template for the vWLAN system, select the **Platform** tab. This menu lists any previously configured templates. If you want to edit a previously created template, select the template from the list. To create a new alert template, either select **Create Alert Template** at the bottom of this menu or select **Platform Alert Template** from the **Create** menu at the top of the GUI.



2. Enter the name of the template in the **Name** field.
3. Optionally, 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, see [SNMP Trap Configuration](#)). Then specify the SNMP trap severity from the **SNMP Trap Severity** list.

Create Alert Template

Name

SNMP Trap Configuration 0 items selected [Remove all](#) [Add all](#)

- + 127.0.0.1

The 127.0.0.1 element corresponds to the local vWLAN Alarms view.

SNMP Trap Severity

Syslog Configuration 0 items selected [Remove all](#) [Add all](#)

- + 127.0.0.1

The 127.0.0.1 element corresponds to the local vWLAN Logs view.

Syslog Severity

Email Configuration

Email Addresses

The email address(es) where messages will be sent to. Please use a comma to separate multiple email addresses.

[Create Alert Template](#)

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, see [Syslog Configuration](#)). Then specify the syslog severity from the **Syslog Severity** list.
5. Optionally, specify the email notification type for this template. Specify the previously created email server handling the email notification (see [Email Account Configuration](#)), and enter an email address, or several email addresses separated by commas, to which to send

the notifications. After you enter the name, SNMP trap, syslog, and email information, click **Create Alert Template**.

A confirmation is displayed indicating that the alert template was created. The template will now appear in the alert template list under **Configuration > Logs and Alerts > Alert 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.

Log Messages

Log 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. Log messages can be error or informational or debug messages and are classified using the notification template. In addition, log messages can track any configuration changes (creations, deletions, updates) and who authorized the change. Notification templates determine log message types, which allow you to classify the log notifications as you prefer.

The administrator cannot create log messages, but rather, can create notification templates, 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 log messages:

1. Navigate to **Configuration > Logs and Alerts > Logs**. Select the **Domain** tab if you work with messages for a specific domain, or select the **Platform** tab if you work with messages for the vWLAN system. This menu lists the generated messages and includes the product with which the message is associated (AP, vWLAN, and so on), the message type (action that generated the message), and the notification template associated with the message (info, error, and so on).

Message Type	Category	Alert 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_available_for_upgrade	AP	info_template
ap_firmware_failed	AP	error_template
ap_firmware_successful	AP	info_template
ap_firmware_updated	AP	info_template
ap_mc2uc_disabled	AP	debug_template
ap_mc2uc_enabled	AP	debug_template
ap_radar_detected	RF	info_template
ap_setting_added	AP	info_template
bulk_import_devices_failed	Summary	error_template

2. Select the message from the list to edit the type of template associated with a specific message. 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 created (see [Notification Templates](#)).

Edit Info Message

Category AP

Message Type ap_config_failed

Alert Template error_template ▼

Update Info Message

[Back](#)

3. Click **Update Info Message** to apply the template change.

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 (see [General GUI Shortcuts](#)) 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:

1. Navigate to **Administration > Admin Tasks**. Or, select **Domain Tasks** or **Platform Tasks** from the menu 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. This menu lists all active administrative tasks. You can select to delete or execute the task by selecting the task from the list. Typically you should not delete tasks unless you already executed it another way or you want to abort a reboot.

Message	Job Type	Next Scheduled Execution	Broadcast	Updated Time *
Schedule a background scan	On Demand		true	2024-10-01 14:39:54

Showing 1 to 1 of 1 entries

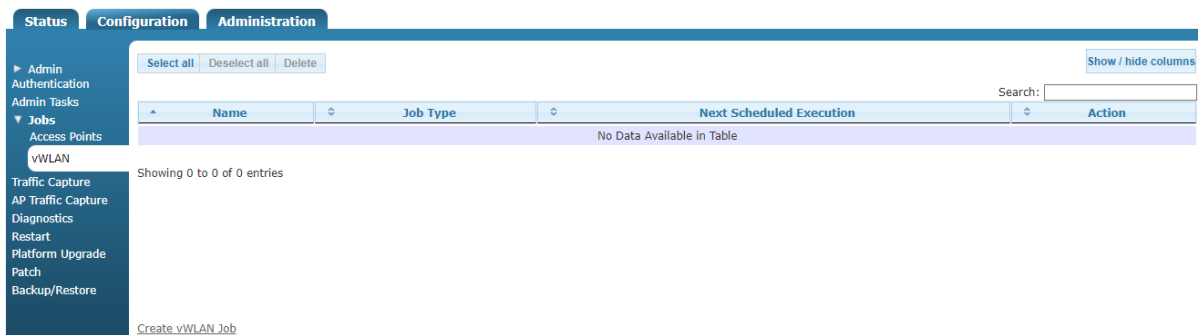
2. Click the play icon next to the task in the list to execute the task. When the task is completed, a message is generated indicating the successful execution of the task. You can then delete the task from the list. You can also monitor the number of administrative tasks for the vWLAN system, or a specific 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 can 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:

1. Navigate to **Administration** > **Jobs** > **vWLAN**. This menu lists all current vWLAN jobs. 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.

3. Select the appropriate action for the job from the **Action** field.
4. To schedule the job, select the **Scheduled** field to display the scheduling options. Use the **Frequency** field 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** field to specify the start time for the job.
5. Click **Create vWLAN Job** to create the job.

Once the job is created, it will appear in the job list in the **vWLAN Jobs** menu. To execute a job immediately, select the play next to the job in the job list. You will receive a confirmation that the job is completed.

Diagnostic Tools

Administrators use diagnostic tools 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 these sections:

Platform Administrator Diagnostic Tools	289
Phone Home Support	290
Domain Administrator Diagnostic Tools	290
External Authentication Test Results	291
Packet Captures	291
Domain Packet Captures	292
vWLAN Platform Packet Capture	293

Platform Administrator Diagnostic Tools

To access the platform administrator diagnostic tools, navigate to **Administration > 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
- Connect to Adtran support

To configure any of these options:

1. Navigate to **Administration > Diagnostics**, select the **Platform** tab, and enter the appropriate options.

The screenshot shows the 'Platform' tab in the diagnostic tools menu. The 'Ping' tool is selected with a radio button. Below it is an 'Address' input field with a placeholder 'Enter the IP address or fully qualified domain name for the target host.' and an 'Interface' dropdown menu with 'Any' selected and a note 'Interface is the source ethernet port on the vWLAN.' Other tools listed include Traceroute, Routes, Netstat, ARP, Clear ARP Cache, Show Processes, Show Network Interface Parameters, and Phone Home to ADTRAN Support. A 'Run Diagnostic' button is located at the bottom of the form.

2. Click **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 menu, then enter the username and password to use for authentication. The results of the diagnostic task are displayed once the task is complete.



Additional information for executing an external server authentication test is provided in [External Authentication Test Results](#).

To access the domain administration diagnostic tools:

1. Navigate to **Administration** > **Diagnostics**, select the **Domain** tab, and enter the information in the appropriate fields.

2. Click **Run diagnostic** at the bottom of the menu. The results are displayed once the task is complete.

External Authentication Test Results

You can initiate a diagnostic test to verify external server authentication only if the external authentication servers are already configured in vWLAN. See [External Server Authentication](#) for information. 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. If the test fails, it could be due to a time out, invalid credentials, or other reasons. The reason is 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. You can run multiple packet captures at once, and there is no limit to the number of captures that you can execute, 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



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.

To configure a packet capture report for the APs on a domain:

1. Navigate to **Administration** > **AP Traffic Capture**.
2. Specify the AP on which you want to capture packets by selecting the AP from the **AP** field. Then, select whether you capture wireless or wired traffic from the **Capture Type** field.

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: BSAP2030-00-19-92-4b-fd-00

Capture Type: Wired

Interface: BG(2.4Ghz)

802.11b/g/n/ax (2.4GHz) SSID: 421

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.

3. Specify the radio interface on which to capture packets. Make your selection from the **Interface** field.
4. Specify the SSID from the **SSID** field. Then, specify the protocol from the **Protocol** menu and any IP addresses in the **IP address** field.
5. 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.



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. Click **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:

1. Navigate to **Administration** > **Traffic Capture**.
2. Specify the **Ethernet interface** and the **Protocol**. 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. Specify a port number in the **Port** field for all protocols, except ICMP.

4. 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. Click **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 **Status** > **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.

Navigate to **Status** > **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	Level
2024-10-18 12:29:04	rf	alarm	detected	RFIDS alert Rogue AP with MAC AC:13:9C:09:07:9B, detected by AP 00:19:92:2d:05:80	INFORMATION
2024-10-18 12:25:24	rf	alarm	detected	RFIDS alert Rogue AP with MAC CC:A6:84:C0:43:19, detected by AP 00:19:92:2d:05:80	INFORMATION
2024-10-18 12:25:10	rf	alarm	detected	RFIDS alert Rogue AP with MAC CC:66:18:1A:8B:C5, detected by AP 00:19:92:2d:05:80	INFORMATION
2024-10-18 12:24:10	rf	alarm	detected	RFIDS alert Rogue AP with MAC 00:88:D6:D8:D4:B7, detected by AP 00:19:92:2d:05:80	INFORMATION
2024-10-18 12:23:59	rf	alarm	detected	RFIDS alert Rogue AP with MAC 38:F8:F6:49:C9:4D, detected by AP 00:19:92:2d:05:80	INFORMATION
2024-10-18 12:22:53	rf	alarm	detected	RFIDS alert Rogue AP with MAC 00:04:56:BF:1A:FF, detected by AP 00:19:92:2d:05:80	INFORMATION
2024-10-18 12:18:01	rf	alarm	detected	RFIDS alert Rogue AP with MAC 20:08:B2:3F:84:C1, detected by AP 00:19:92:2a:d6:e0	INFORMATION
2024-10-18 12:17:09	rf	alarm	detected	RFIDS alert Rogue AP with MAC 38:F8:F6:B9:A6:4A, detected by AP 00:19:92:2d:05:80	INFORMATION
2024-10-18 12:16:56	rf	alarm	detected	RFIDS alert Rogue AP with MAC 38:F8:F6:DC:C9:4A, detected by AP 00:19:92:2d:05:80	INFORMATION
2024-10-18 12:16:17	rf	alarm	detected	RFIDS alert Rogue AP with MAC 00:19:92:1B:1B:09, detected by AP 00:19:92:2d:05:80	INFORMATION
2024-10-18 12:16:00	rf	alarm	detected	RFIDS alert Rogue AP with MAC 38:F8:F6:74:E2:43, detected by AP 00:19:92:2d:05:80	INFORMATION
2024-10-18 12:15:49	rf	alarm	detected	RFIDS alert Rogue AP with MAC 88:5B:DD:79:91:BC, detected by AP 00:19:92:2d:05:80	INFORMATION
2024-10-18 12:14:28	rf	alarm	detected	RFIDS alert Rogue AP with MAC 00:19:F2:90:5F:77, detected by AP 00:19:92:2d:05:c0	INFORMATION
2024-10-18 12:12:18	rf	alarm	detected	RFIDS alert Rogue AP with MAC B4:80:5D:B4:3A:05, detected by AP 00:19:92:2d:05:80	INFORMATION
2024-10-18 12:08:44	rf	alarm	detected	RFIDS alert Rogue AP with MAC 38:38:F2:56:1C:24, detected by AP 00:19:92:2d:05:80	INFORMATION
2024-10-18 12:06:33	rf	alarm	detected	RFIDS alert Rogue AP with MAC 40:BE:ED:0E:0E:E1, detected by AP 00:19:92:2d:05:80	INFORMATION

You can search the log files for a specific entry by using the **Search** button at the top right of the logs list. You can search by service type, function, operation, or log level. You can delete logs by selecting **Purge All 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 **Status > 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.

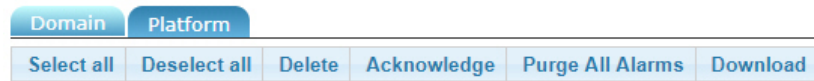


You can track alerts in syslog reports, SNMP traps, and email notifications. See [SNMP Trap Configuration](#), [Syslog Configuration](#), and [Email Account Configuration](#) for more information.

1. Navigate to **Status > Alerts**. Select the **Domain** or **Platform** tab.

Created Time	Service	Function	Operation	Message	Level	Acknowledged
2024-10-09T10:12:43+00:00	admin	login	failed	Admin authentication failed for root@adtran.com from 172.21.241.38	ERRORS	No
2024-10-09T10:12:38+00:00	admin	login	failed	Admin authentication failed for root@adtran.com from 172.21.241.38	ERRORS	No
2024-10-09T10:12:30+00:00	admin	login	failed	Admin authentication failed for root@adtran.com from 172.21.241.38	ERRORS	No
2024-10-04T10:05:02+00:00	admin	login	failed	Admin authentication failed for dev1@adtran.com from 10.1.103.51	ERRORS	No
2024-10-04T10:04:56+00:00	admin	login	failed	Admin authentication failed for dev@adtran.com from 10.1.103.51	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**.



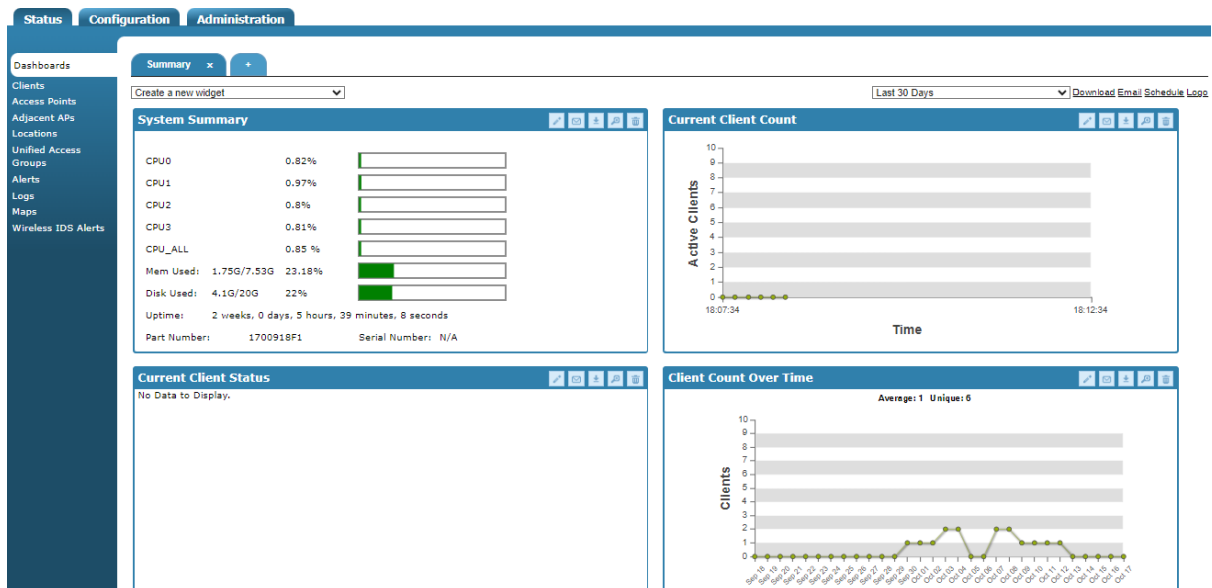
Log in as a root user to have the ability to acknowledge alerts.

Using the Reporting Dashboard

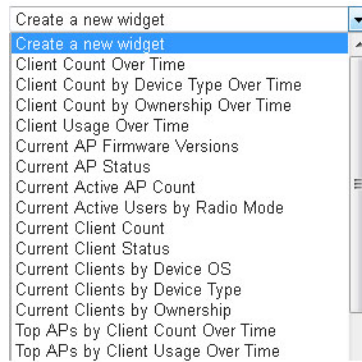
The vWLAN reporting dashboard is a collection of customized widgets that are available for you to view vWLAN information at a glance. Administrators use dashboards to view information about users, APs, roles, locations, SSIDs, bandwidth usage, and many other parameters used within the domain. You can configure up to 12 widgets (2 x 6) 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, you can view the details of any users, APs, roles, and so on, 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 dashboard is completely separate from any others and can be fully customized to the individual preference.

To use the reporting dashboard:

1. Navigate to **Status > Dashboards**.



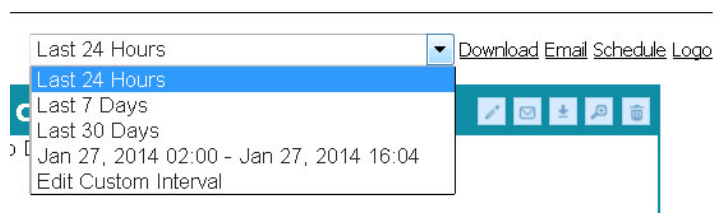
2. To specify which information is summarized on the dashboard, create the appropriate widget from the **Create a new widget** menu.



The widgets summarize:

- **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 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 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 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, specify a time frame using the time frame 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.



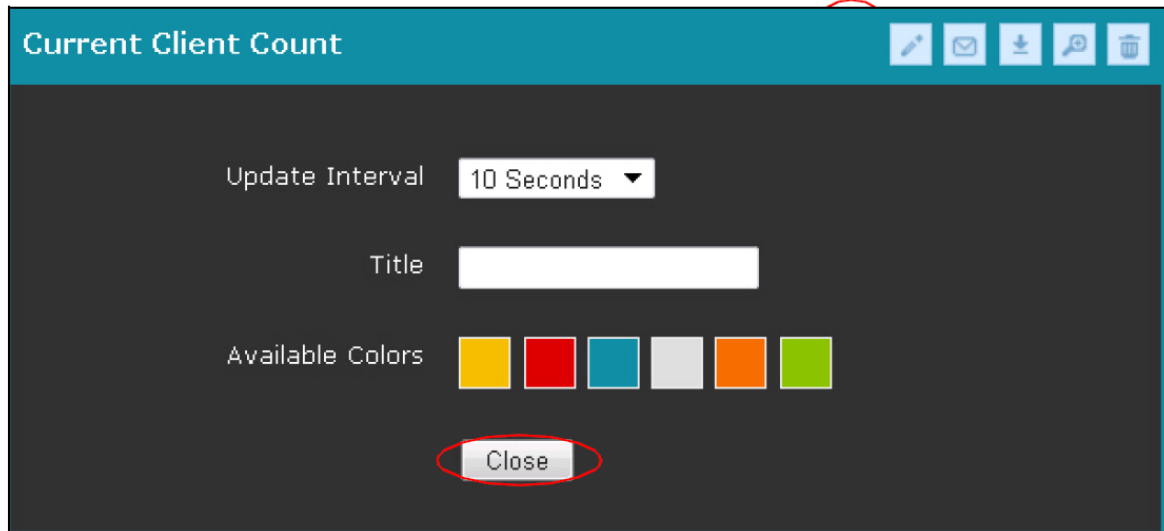
Customizing the Report Dashboard Widgets

You can customize report dashboard widgets in several ways. You can move them around the dashboard menu by dragging and dropping. In addition, you can customize the display and use the widgets to generate reports through email or download.

1. Select **Edit** at the top of the widget to customize a widget.



2. Change the update interval, title, and color of the widget in the edit menu. After making changes, click **Close**.



3. Expand the widget to a full page summarization by selecting the magnifying glass at the top of the widget.



4. Delete the widget by selecting the delete icon at the top of the widget.



5. 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** field (PDF, JPEG, or PNG). Select the email configuration from the menu, and click **Send Email**.

- 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** menu (PDF, JPEG, PNG, or CSV) and click **Download**.

- 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** menu, and specify the email configuration to use from the **Email Configuration** menu. Click **Send Email** to send the email to the specified recipients.


Last 24 Hours [Download Email Schedule Logo](#)

Email

Multiple recipients should be separated by commas without any spaces.

Format

Email Configuration

 You must have an email configuration in place to send or receive emails and schedule dashboard actions. Refer to [Email Account Configuration](#) 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** menu, select the format from the **Format** 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.

Last 24 Hours [Download Email Schedule Logo](#)

Email

Multiple recipients should be separated by commas without any spaces.


Frequency

Type


Email configuration

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 click **Upload New Logo**.

Last 24 Hours [Download Email Schedule Logo](#)

Current Logo 

Select a logo to upload No file chosen

 The logo applies to all dashboards in the domain, so changing the logo impacts all other users in the domain.

Implementing vWLAN 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:

1. Ensure that the following traffic is allowed between the vWLAN and the APs:
 - 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 are used for vWLAN to vWLAN communication and secure firmware uploads.
3. Navigate to **Configuration > System > Settings**. Select the **Platform** tab.
4. Scroll to the **Public IP Address for vWLAN high availability node** setting and select it.

Status Configuration Administration

Domain Platform

Show / hide columns

Search:

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?	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.

Showing 1 to 26 of 26 entries

5. Enter the public IP address in the appropriate field and click **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.