

vWLAN

Web-Based Authentication (Captive Portal) in vWLAN

Basic Configuration Guide

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.

Trademark Information

“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.

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.



©2018 ADTRAN, Inc.
All Rights Reserved.

Revision History

Rev A	September 2018	Initial Release
-------	----------------	-----------------

Table of Contents

1	Overview	9
1.1	Intended Audience	9
1.2	Document Structure	9
1.3	Hazard and Conventional Symbols	10
1.4	Related Online Documents and Resources	11
2	Overview of Captive Portal	12
2.1	Walled Garden	13
3	Hardware and Software Requirements and Limitations	14
4	Configuring an SSID for Use with Captive Portal	15
5	Configuring Captive Portal	19
5.1	Walled Garden	19
5.2	Configuring External Server Authentication	22
5.2.1	Configuring Domain Accounting (Optional)	22
5.2.2	External RADIUS Web-based Authentication Server	24
5.2.3	External LDAP Web-based Authentication Server	28
5.2.4	External SIP2 Web-based Library Authentication Server	33
5.3	Configuring Local Server Authentication	38
6	Additional Options	40
6.1	Captive Network Assistant (CNA) Support	40
6.1.1	Loading an SSL Certificate	40
6.1.2	Redirect to a Hostname	42
6.1.3	Final Steps	43
6.2	HTTPS Redirection	46
6.3	DisableTLS 1.0	47
7	Troubleshooting	49
7.1	Testing	49
7.2	Common Problems	50
7.2.1	Logs	50
7.2.2	Client is not Redirected	50
7.2.3	Client receives an SSL warning	51
7.2.4	Cannot Login to the Splash Page	51
8	Warranty and Contact Information	52
8.1	Warranty	52
8.2	Contact Information	52

List of Figures

Figure 1.	Captive Portal Login Page	12
Figure 2.	Client Authentication Process	12
Figure 3.	Create or Edit an Existing SSID	15
Figure 4.	Enable SSID Broadcasting	15
Figure 5.	Specify the type of traffic this SSID will convert to Unicast	16
Figure 6.	Authentication Options Available when Captive Portal is Enabled	16
Figure 7.	SSID with WPA2-PSK Authentication	17
Figure 8.	SSID with WPA-PSK + WPA2-PSK Authentication	17
Figure 9.	Enabling Remote Site Survivability	18
Figure 10.	Navigate to the Location Configuration Menu	19
Figure 11.	Create a Network Location to Serve IP Addresses for Walled Garden	20
Figure 12.	Create a Role	20
Figure 13.	Specify the Role Name, Type, and Location	20
Figure 14.	Allow DNS Traffic Outbound for Walled Garden	21
Figure 15.	Create a Registered Role for Walled Garden	21
Figure 16.	Create an SSID and Enable Captive Portal for Walled Garden	22
Figure 17.	Create a Domain Accounting Server	23
Figure 18.	Accounting Server Name, Port Number, and Enable Option	23
Figure 19.	Shared Secret for Domain Accounting Server	23
Figure 20.	Domain Server Timeout Value and Retries	23
Figure 21.	Domain Server Interim Updates and Interim Update Interval	24
Figure 22.	Navigate to the Create Authentication Server Menu	24
Figure 23.	Create a RADIUS Server	25
Figure 24.	Name, IP Address, and Optional Accounting Server	25
Figure 25.	Specify the Port to be Used by the RADIUS Server	25
Figure 26.	Shared Secret/Password for the RADIUS Server	25
Figure 27.	Timeout Weight, Simultaneous Connections, and Server Precedence	26
Figure 28.	Select the Role for Users who do not Match any Configured Attributes	26
Figure 29.	Configure the Match Attributes and Assigned Roles for the RADIUS Server	27
Figure 30.	Verify a Successful RADIUS Server Connection	27
Figure 31.	Diagnostics Menu	28
Figure 32.	Navigating to the Authentication Server Menu	28
Figure 33.	Create an LDAP Server	29
Figure 34.	Name, IP Address, and Optional Accounting Server	29
Figure 35.	Specify the Port to be Used by the LDAP Server	29
Figure 36.	LDAP Bind User	29
Figure 37.	Shared Secret/Password for the Bind User	30
Figure 38.	LDAP Base Entry, Unique ID Attribute, and Bind All Queries Options	30
Figure 39.	Timeout Weight, Simultaneous Users, Precedence, Require SSL Options	31
Figure 40.	Select the Role for Users who do not Match any Configured Attribute	31
Figure 41.	Configure Match Attributes and Assigned Roles for the LDAP Server	32
Figure 42.	Verify a Successful LDAP Server Connection	32

Figure 43.	Diagnostics Menu	33
Figure 44.	Navigating to the Authentication Server Menu	33
Figure 45.	Create a SIP2 Server	34
Figure 46.	Name, IP Address, and Optional Accounting Server	34
Figure 47.	Specify the Port Number for the SIP2 Server	34
Figure 48.	SIP2 Administrator Option	34
Figure 49.	Optional Shared Secret/Password for SIP2 Server	34
Figure 50.	SIP2 Server Timeout Weight	35
Figure 51.	SIP2 Validate PIN/Password	35
Figure 52.	SIP2 Empty AO Institution ID	35
Figure 53.	SIP2 CP Location Code	35
Figure 54.	Simultaneous Users and Server Precedence	36
Figure 55.	Select the Role for Users who do not Match any Configured Attribute	36
Figure 56.	Configure Match Attributes and Assigned Roles for the SIP2 Server	36
Figure 57.	Verify a Successful SIP2 Server Connection	37
Figure 58.	Diagnostics Menu	38
Figure 59.	Navigating to the Internal User Authentication Menu	39
Figure 60.	Create Internal User	39
Figure 61.	Navigating to the Custom Certificate Menu	40
Figure 62.	Copy/Paste Custom Certificate Details	41
Figure 63.	Adding Certificate Chains	41
Figure 64.	Navigating to the Redirect to Hostname Option	42
Figure 65.	Enable Redirect to Hostname	42
Figure 66.	Enable Allow the AP to Look Up the vWLAN Name Using a DNS PTR Record Option	43
Figure 67.	Check the DNS Server Used to Resolve Hostname and that CNA is Enabled	44
Figure 68.	Navigate to the Network Interface Hostname Settings	45
Figure 69.	Set the Hostname for the Network Interface	45
Figure 70.	Navigating to the Domain Tasks under the Admin Tasks Menu	46
Figure 71.	Queued Platform Tasks	46
Figure 72.	Navigating to the HTTPS Redirection Option	47
Figure 73.	Navigate to the TLS 1.0 Setting	47
Figure 74.	Disable TLS 1.0 and Update the Platform Setting	48
Figure 75.	Test to Verify that a Client can Associate with the SSID	49
Figure 76.	Captive Portal Landing Page	49
Figure 77.	Log Messages	50

List of Tables

Table 1.	Topic List	9
Table 2.	Related Online Documents and Resources	11

1 Overview

This configuration guide describes the use of web-based authentication (Captive Portal) in ADTRAN's Bluesocket virtual wireless local area network (vWLAN) and Bluesocket Access Points (APs). Topics include an overview of Captive Portal, configuration considerations and procedures, additional options, and troubleshooting information.

1.1 Intended Audience

The intended audience for this information is the network administrator using the ADTRAN vWLAN products. The instructions assume familiarity with the intended use of the equipment, basic required installation and configuration skills, and knowledge of local and accepted networking practices.

1.2 Document Structure

Table 1 lists the topics contained in this document

Table 1. Topic List

Section	Topic	See Page...
1	Overview	9
2	Overview of Captive Portal	12
3	Hardware and Software Requirements and Limitations	14
4	Configuring an SSID for Use with Captive Portal	15
5	Configuring Captive Portal	19
6	Additional Options	40
7	Troubleshooting	49
8	Warranty and Contact Information	52

1.3 Hazard and Conventional Symbols

The following Hazard symbols are used throughout this guide:



WARNING!

Warning: Service affecting. Possible risk of system failure.



CAUTION!

Caution: Indicates that a failure to take or avoid a specific action could result in a loss of data.



NOTICE!

Notice: Provides information that is essential to the completion of a task.



NOTE

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

1.4 Related Online Documents and Resources

Refer to [Table 2](#) for additional information for this product.

Documentation for ADTRAN vWLAN products is available for viewing and download directly from the ADTRAN Support Community website.

Go to: <https://supportforums.adtran.com>

Table 2. Related Online Documents and Resources

Title	Part Number	Description
ADTRAN Bluesocket vWLAN Documentation		
vWLAN Quick Deployment and Configuration Guide		This guide discusses how to set up basic WiFi Network access using password-authenticated SSIDs (WPA2-Personal) as well as firmware and SSID management in vWLAN.
Bluesocket vWLAN Administrator's Guide	6ABSAG0001-31	This comprehensive guide contains information on all of the configuration settings available in the ADTRAN vWLAN software.
Installing and Renewing an SSL Certificate in vWLAN		This document explains how to install and renew a SSL certificate provided by a Certificate Authority, such as VeriSign, in vWLAN for software versions 2.2.1 and later.
Fully Customized Login Page Configuration Differences in vWLAN 2.5.0 and 2.5.1	6ABSCG0005-29	This configuration guide describes the differences in the HTML used for custom login pages between vWLAN release 2.5.0 and vWLAN release 2.5.1.
vWLAN Single Click Customized Login Page		This guide provides the basic steps for customizing (or creating) a login screen instead of using the default login screen.
vWLAN and BSAP Traffic Capture Guide		This guide provides the basic procedure for capturing traffic using vWLAN.
vWLAN External RADIUS 802.1x Authentication	6ABSCG0002-29	This configuration guide provides and in-depth look at external RADIUS 802.1x authentication and its configuration and use with ADTRAN Bluesocket vWLAN products.

2 Overview of Captive Portal

Web-based authentication (Captive Portal) is an authentication process in which clients typically connect to an open system service set identifier (SSID) and are then redirected to a login page, as shown in Figure 1, or Captive Portal (after opening a browser).

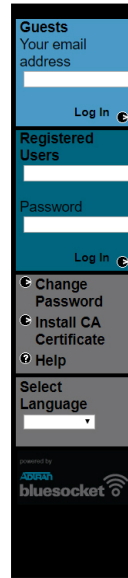


Figure 1. Captive Portal Login Page

This client authentication process requires no client-side configuration, although it can also be used with WPAPSK/WPA2PSK SSIDs, which requires the client to configure the preshared key. Figure 2 illustrates this process.

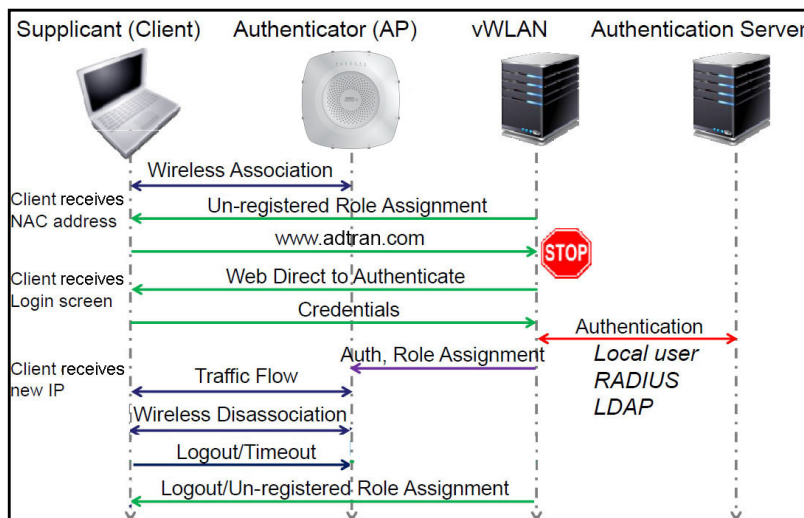


Figure 2. Client Authentication Process

During the authentication process, clients in the Un-registered role are redirected to the secure vWLAN login page (Captive Portal). The client initially receives an authen-

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



NOTE

Introduced in vWLAN 3.1 release, the Un-Registered role type is the only role that will allow web redirection.

Web-authenticated traffic is secured using HTTPS, however, subsequent over-the-air traffic is secured based on the SSID configuration. Please note you cannot achieve 802.11n data rates while using TKIP, but will be limited to legacy data rates only up to 54 Mbps. Authentication configuration includes configuring the following types of authentication: server authentication, local user authentication, SSID authentication, and MAC device authentication. In addition, you can configure login forms and images for specific domains, based on the SSID and the AP template (in that order).

2.1 Walled Garden

Walled Garden is a feature that allows a client connecting to the network to maintain the same IP address throughout the authentication process. The client is assigned an IP address from the target location, but will not be able to access the network until authentication is complete.

3 Hardware and Software Requirements and Limitations

This document describes Captive Portal configuration for vWLAN and APs running software versions 2.4 or later. Captive Portal is supported on all BSAPs.

The content of this guide assumes that you have licensed APs that are online, locations are active, and Roles are configured accordingly. Refer to the *vWLAN Quick Deployment and Configuration guide* for help getting started with vWLAN.

Also assumed is a familiarity with vWLAN and its configuration, as described in the *vWLAN Administrator's Guide*, available online at <https://supportforums.adtran.com>.

4 Configuring an SSID for Use with Captive Portal

To allow wireless clients to connect to the vWLAN network, each AP domain must have at least one SSID. To configure an SSID, connect to the GUI and follow these steps:

1. Navigate to the **Configuration** tab, and select **Wireless > SSIDs**. Here any previously configured SSIDs are listed, and the name, role, broadcast, authentication method, accounting server, and cipher type for each SSID is displayed. You can edit an already configured SSID by selecting the SSID from the list. To create a new SSID, select **Create SSID** from the bottom of the menu or select **Domain SSID** from the **Create** drop-down menu (at the top of the menu) as shown in [Figure 3](#).

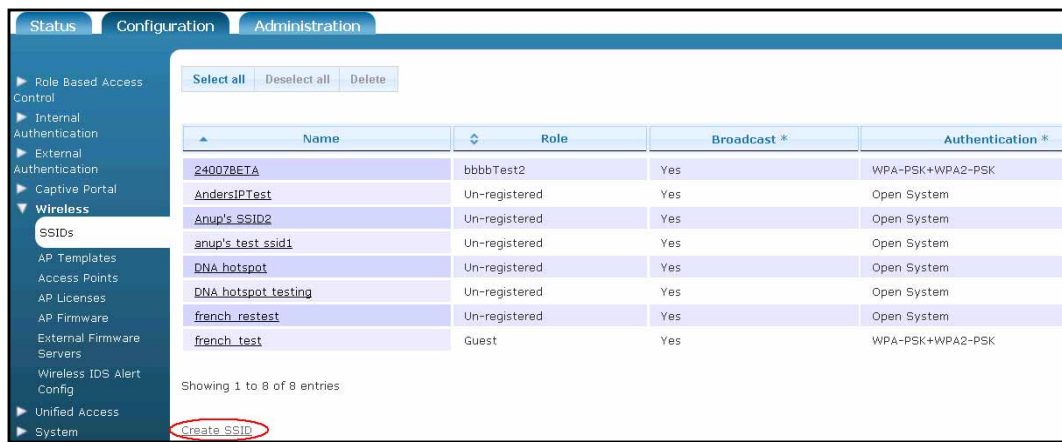


Figure 3. Create or Edit an Existing SSID

2. Enter a name for the SSID. SSID names can be up to 31 characters in length.
3. Next, enable SSID broadcasting by selecting the **Broadcast SSID** check box as shown in [Figure 4](#).

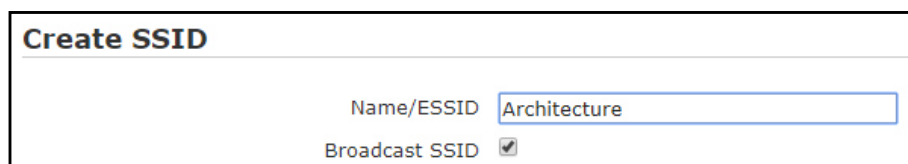


Figure 4. Enable SSID Broadcasting

4. Specify whether the SSID will convert multicast or broadcast network traffic to unicast traffic by selecting the appropriate option from the **Convert** drop-down menu as shown in [Figure 5](#). By default, **Convert broadcast and multicast to unicast** is enabled. Other options are **Disable**, **Convert broadcast to unicast**, and **Convert multicast to unicast**.

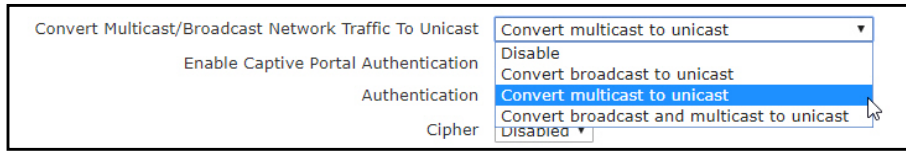


Figure 5. Specify the type of traffic this SSID will convert to Unicast



NOTE

If you do not choose to convert multicast network traffic to unicast traffic, you must allow multicast traffic in the default role of the SSID (Refer to the document [Using Multicast Conversion in vWLAN](#) available online at supportforums.adtran.com for additional information).

5. Captive Portal Authentication requires the check box next to **Enable Captive Portal Authentication** to be selected (see Figure 6). You can only specify an **Un-registered Role** when using Captive Portal. You can use the default **Un-registered** role or a previously configured Un-registered role (See [Configuring Captive Portal on page 19](#) for information on configuring Walled Garden, Un-registered roles, Captive Portal, and the Walled Garden feature).

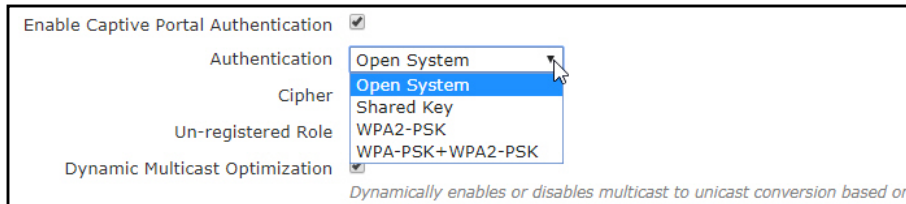


Figure 6. Authentication Options Available when Captive Portal is Enabled



NOTE

You must enable Captive Portal and choose an Un-registered role to allow clients to authenticate with web-based authentication. As of vWLAN release 3.1, the registered roles are hidden when **Enable Captive Portal Authentication** is selected.



NOTE

As of vWLAN release 3.1 wired equivalent privacy (WEP) was removed as an authentication method due to security vulnerabilities. Authentication choices include: **WPA2-PSK** and **WPA-PSK+WPA2-PSK**.

Descriptions of each authentication type are provided as follows:

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 only supports AES-CCM encryption. To select WPA2-PSK as the authentication method for this SSID, select **WPA2-PSK** from the **Authentication** menu as shown in Figure 7. **AES-CCM** will automatically be selected from the **Cipher** drop-down menu. You will also be prompted to specify a preshared key for this authentication type. Preshared keys must be eight digits or greater.

WPA-PSK+WPA2-PSK: WPA-PSK with WPA2-PSK is a personal authentication method that combines the features of WPA-PSK and WPA2-PSK. This method supports TKIP and AES-CCM encryption methods. To select WPA-PSK+WPA2-PSK as the authentication method for this SSID, select **WPA2-PSK+WPA2-PSK** from the **Authentication** menu, and specify whether the SSID will use **AES-CCM** only or **TKIP or AES-CCM** from the **Cipher** drop-down menu (see Figure 8). You will also be prompted to specify a preshared key for this authentication type. Preshared keys must be eight digits or greater.

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 and then they are redirected to the login page for Captive Portal authentication.

The screenshot shows the 'Create SSID' configuration page. The 'Authentication' dropdown is set to 'WPA2-PSK' and the 'Cipher' dropdown is set to 'AES-CCM'. The 'Preshared Key' and 'Preshared Key Confirmation' fields are filled with eight dots. The 'Un-registered Role' dropdown is set to 'Un-registered'. A red oval highlights the 'Preshared Key' and 'Preshared Key Confirmation' fields.

Figure 7. SSID with WPA2-PSK Authentication

The screenshot shows the 'Create SSID' configuration page. The 'Authentication' dropdown is set to 'WPA-PSK+WPA2-PSK' and the 'Cipher' dropdown is set to 'AES-CCM'. The 'Preshared Key' and 'Preshared Key Confirmation' fields are filled with eight dots. The 'Un-registered Role' dropdown is set to 'Un-registered'. A red oval highlights the 'Authentication' and 'Cipher' dropdowns.

Figure 8. SSID with WPA-PSK + WPA2-PSK Authentication



NOTE

TKIP use should be limited because it is not as secure as AES-CCM and it does not allow clients to use 802.11n data rates. You should only enable TKIP if you have legacy (pre-2005) clients in your network that cannot be upgraded.

6. Once you have selected the authentication, cipher, and preshared key (if necessary) information for the SSID, specify the login form to be associated with the SSID by selecting the appropriate form from the **Login Form** drop-down menu. By default, each SSID will use the default login form. If you have not created another login form, this will be the only option (refer to *Customizing vWLAN Login Forms and Images* in the *Bluesocket vWLAN Administrator's Guide* available online at supportforums.adtran.com for additional information). You can select another login form if one has been created.
7. As of vWLAN release 3.2.0, a feature was added that supports Remote Site Survivability for PSK and open SSIDs. If the connection between the AP and both the primary and secondary vWLAN is severed, new pre-shared key and open SSID clients will be able to connect. Select **Allow new clients to use the network when the vWLAN is down** and specify the **Role to be assigned when vWLAN is down** (see Figure 9).

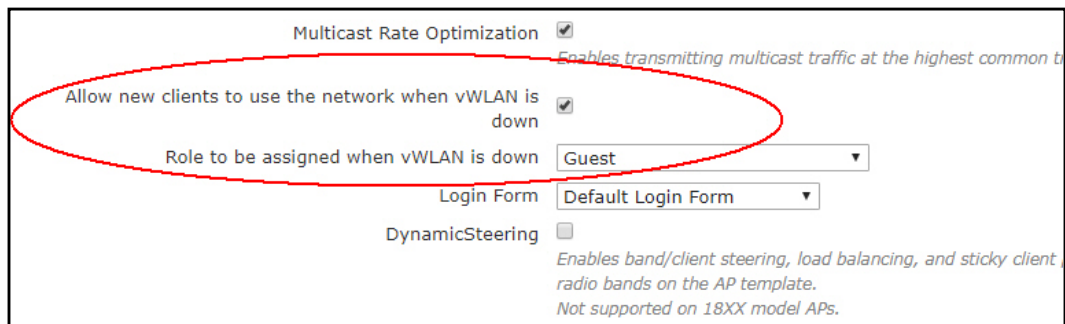


Figure 9. Enabling Remote Site Survivability



NOTE

Captive Portal must be enabled to use this feature.

8. The SSID has now been configured with all settings applicable to Captive Portal. Select **Create SSID**. A confirmation will be displayed indicating the SSID was successfully created.

5 Configuring Captive Portal

There are four parts to this section, Walled Garden, configuring external server authentication, configuring internal server authentication, and device authentication.

5.1 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 type to a registered role (Walled Garden).

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

1. Configure the location of the network that will serve the IP addresses.



NOTE

The location of the network must be different than that of the vWLAN, AP, DNS server, external servers, etc.

Navigate to the **Configuration** tab, and select **Role Based Access Control > Locations** as shown in [Figure 10](#). Any previously configured locations will be listed in the menu. If you want to edit a previously created location, select the location name from the list. To create a new location, either select **Create Location** at the bottom of this menu, or select **Domain Location** from the **Create** drop-down menu (at the top of the menu).

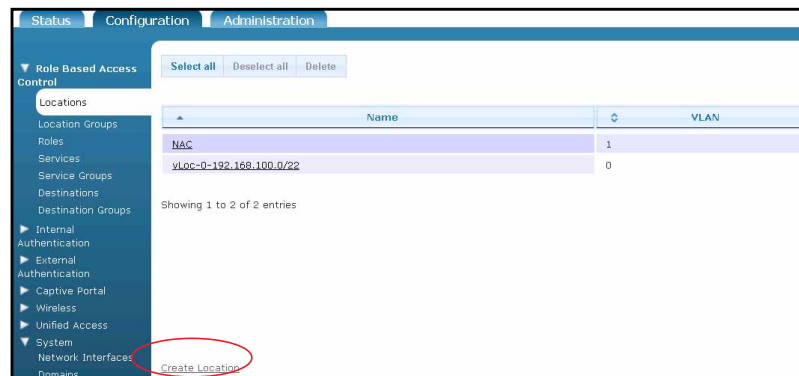


Figure 10. Navigate to the Location Configuration Menu

Enter the name of the location and its associated VLAN in the appropriate fields. Then enter the classless interdomain route (CIDR) for the location, which is the location's subnet and network mask (see [Figure 11](#)).



NOTE

Do not specify the native VLAN here since an Un-registered role cannot be created with the native VLAN.

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

Create Location

Name

VLAN ID

CIDR

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

[Back](#)

Figure 11. Create a Network Location to Serve IP Addresses for Walled Garden

2. Create a Role that will allow the client to obtain an IP address from the specified network location.



NOTE

Even though the client will be allowed to obtain an IP address from the network location, they will not be able to utilize the network until they authenticate via Captive Portal.

Navigate to the **Configuration** tab, and select **Role Based Access Control > Roles** as shown in Figure 12. Select **Create Role** at the bottom of this menu.



Figure 12. Create a Role

Enter a *Name* and specify **Un-registered Role** for the *Type* as shown in Figure 13. Select the name of the location that you created in Step 1 on page 19 for the *Location*.

Name

Type

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

Location

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

Native AP Vlan location for Un-registered roles.

the following policies.

Figure 13. Specify the Role Name, Type, and Location

IMPORTANT: Add a firewall rule that allows DNS traffic outbound as shown in Figure 14. Select **Create Role**.

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	DNS	Outgoing	Any
Allow		Outgoing	
Allow		Outgoing	
Allow		Outgoing	
Allow		Outgoing	

[Append Firewall Rule](#)

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](#)

Figure 14. Allow DNS Traffic Outbound for Walled Garden

3. Create another role and specify **Registered Role** for the *Type* and select the name of the location that you created in Step 1 on page 19 above for the *Location* (See Figure 15). This is the role in which the user should be placed after authenticating via Captive Portal.



NOTE

Be sure to place users into this role (via the attributes or default role selection when creating an external server) so that they do not transition IP addresses after authentication. See Step 7 on page 26 for discussion on selecting attributes and roles when configuring a RADIUS external server. Depending on the type of external server you are using, you can also refer to configuring an LDAP server on page 28 and configuring a SIP2 server on page 33.

Create Role

Name

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

Schedule

Location

Figure 15. Create a Registered Role for Walled Garden



NOTE

It is important that the Location of the registered role to be the same Location as the Un-registered role type for the Walled Garden feature to work properly.

4. Create an SSID, enable Captive Portal, and select the name of the Un-registered Role created in Step 2 on page 20 (See [Figure 16](#)). See [Configuring an SSID for Use with Captive Portal](#) on page 15 for additional SSID options.

Create SSID

Name/ESSID

Broadcast SSID

Enable Captive Portal Authentication

Un-registered Role

Figure 16. Create an SSID and Enable Captive Portal for Walled Garden

5.2 Configuring External Server Authentication

You can configure an external RADIUS web-based authentication, LDAP or AD, or Session Initiation Protocol 2 (SIP2) web-based library authentication server for vWLAN internal authentication. The credentials entered by the client are sent to the vWLAN and authenticated against a local user database, external Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) server, external web-based 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 (set when creating or editing the external server). To configure an authentication server for the specified domain, follow the steps for each server type as outlined in the following sections:

5.2.1 Configuring Domain Accounting (Optional)



NOTE

If you plan to use domain accounting, you must create the accounting server first so that it is available to associate with any external servers you create in the next steps.

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

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

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

1. Navigate to the **Configuration** tab, and select **External Authentication > Accounting** as shown in [Figure 17](#). Any previously configured accounting serv-

ers will be listed in the menu. If you want to edit a previously created accounting server, select the server name from the list. To create a new accounting server, either select **Create Accounting Server** at the bottom of this menu, or select **Domain Accounting Server** from the **Create** drop-down menu (at the top of the menu).

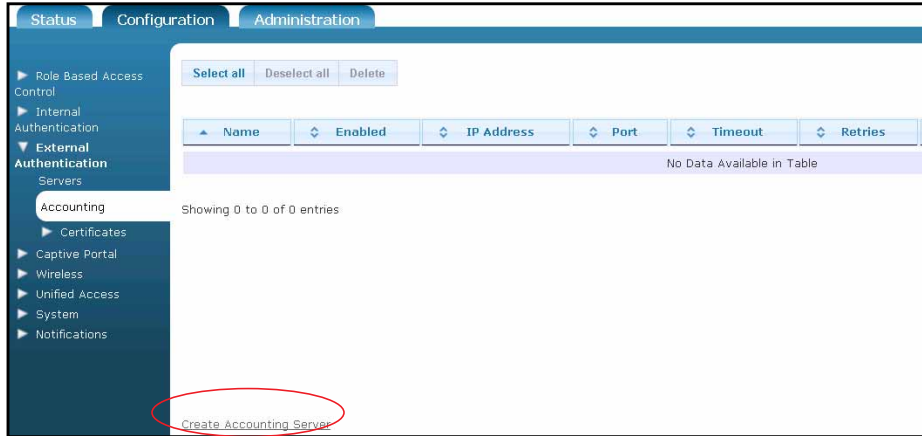


Figure 17. Create a Domain Accounting Server

2. Enter the name of the server, the server's IP address, and the port used by the server (**1813** by default) in the appropriate fields (See [Figure 18](#)). Enable the server by selecting the **Enabled** check box.

Create Accounting Server

Name

Enabled

IP Address

Figure 18. Accounting Server Name, Port Number, and Enable Option

3. Enter the shared secret for the accounting server, and the shared secret confirmation, in the corresponding fields (See [Figure 19](#)).

Shared Secret

Shared Secret Confirmation

Figure 19. Shared Secret for Domain Accounting Server

4. Specify the server timeout value (in seconds), and the number of times vWLAN will attempt to reconnect to the server in the corresponding fields as shown in [Figure 20](#). By default, the timeout value is set to **5** seconds, and the number of retries is set to **5**.

Timeout

Retries

Figure 20. Domain Server Timeout Value and Retries

5. Enable interim reporting updates by selecting the **Interim updates enabled** check box as shown in [Figure 21](#). 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.

Figure 21. Domain Server Interim Updates and Interim Update Interval

6. Select **Create Accounting Server** to create the server. A confirmation is displayed indicating that the server has been created. The server will now appear in the accounting server list (**Configuration tab, External Authentication > Accounting**), where you can display, edit, or delete the server.
7. Once the accounting server has been created, you can associate the server with an authentication method, SSID, or AP.

5.2.2 External RADIUS Web-based Authentication Server

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

1. Navigate to the **Configuration** tab, and select **External Authentication > Servers** as shown in [Figure 22](#). Any previously configured web-based authentication servers will be listed in the menu. If you want to edit a previously created web-based authentication server, select the server name from the list. To create a new authentication server, either select **Create Authentication Server** at the bottom of this menu, or select **Domain Authentication Server** from the **Create** drop-down menu (at the top of the menu).

Select either option to create a new authentication server.

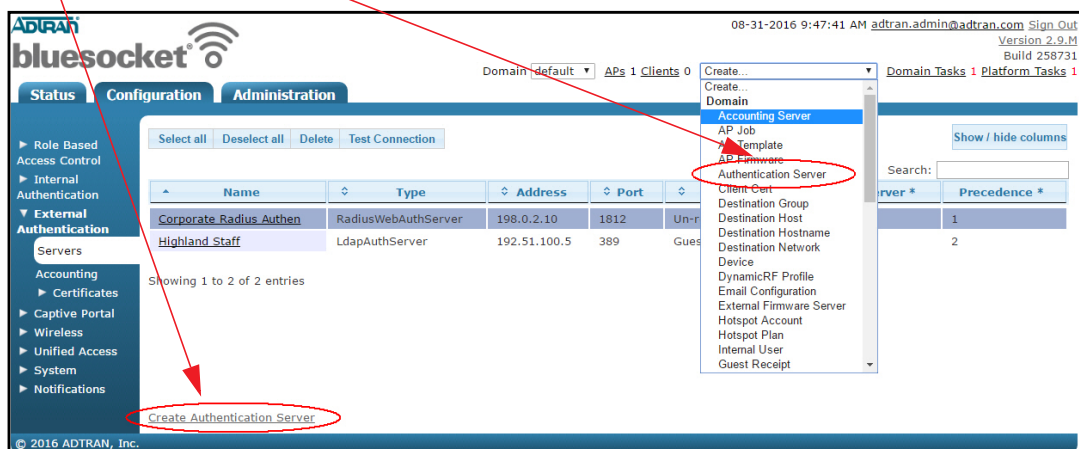
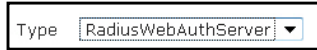


Figure 22. Navigate to the Create Authentication Server Menu

2. Select **RadiusWebAuthServer** from the **Type** drop-down menu as shown in [Figure 23](#)



Type

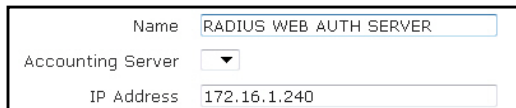
Figure 23. Create a RADIUS Server

3. Enter the name of the server and its IP address in the appropriate fields as show in [Figure 24](#). 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.



NOTE

You must create an accounting server first before it can be selected.



Name
Accounting Server
IP Address

Figure 24. Name, IP Address, and Optional Accounting Server

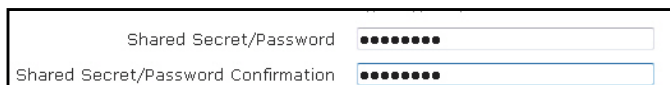
4. Specify the port to be used by the server as show in [Figure 25](#). If you are using a RADIUS server, the port is generally either 1645 or 1812.



Port
Typically, the port should be 1812 or 1645.

Figure 25. Specify the Port to be Used by the RADIUS Server

5. Enter the shared secret or password for the authentication server as show in [Figure 26](#).

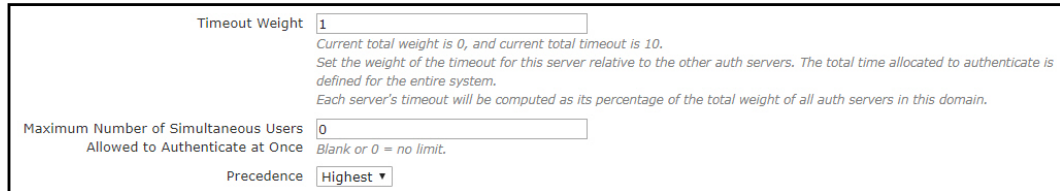


Shared Secret/Password
Shared Secret/Password Confirmation

Figure 26. Shared Secret/Password for the RADIUS Server

6. Specify the timeout weight, maximum number of simultaneous user authentications, and the precedence of the server as shown in [Figure 27](#). The timeout weight value is relative to the timeout weight of other authentication servers. The total time allocated to authenticate is defined for the entire vWLAN system. Each server's timeout is computed as a percentage of the total weight of all authentication servers on this domain. If you leave the maximum number of simultaneous authentications field blank, or enter a 0, that indicates there is no limit. You can specify the precedence level of the server as **Highest**, **Lowest**, or

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



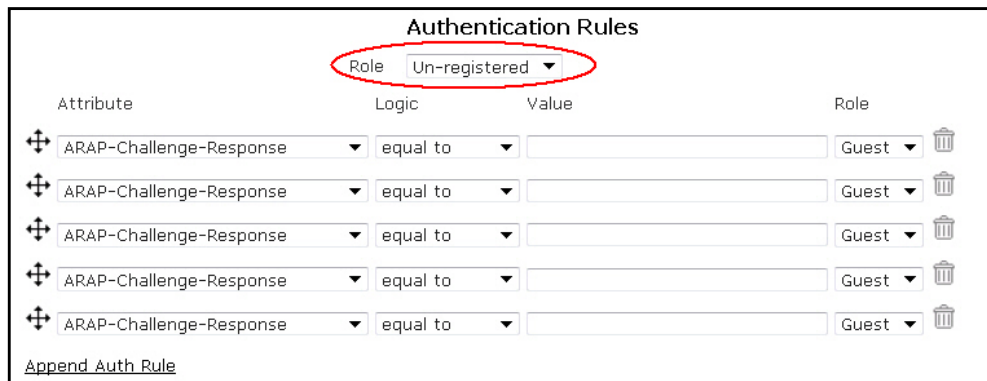
Timeout Weight
Current total weight is 0, and current total timeout is 10.
Set the weight of the timeout for this server relative to the other auth servers. The total time allocated to authenticate is defined for the entire system.
Each server's timeout will be computed as its percentage of the total weight of all auth servers in this domain.

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

Precedence

Figure 27. Timeout Weight, Simultaneous Connections, and Server Precedence

7. Specify the authentication rules for the server and the role given to a user who does not match the specified attributes (See Figure 28). First, select the role that is given to all clients that are successfully authenticated, but do not match any of the below configured attributes. For example, if you choose **Un-registered** from the drop-down menu, clients will never transition out of the Un-registered role unless they successfully authenticate and match one of the configured attributes. Select the role from the **Role** drop-down menu located in the center at the top of the **Authentication Rules** section.



Authentication Rules

Role

Attribute	Logic	Value	Role
ARAP-Challenge-Response	equal to	<input type="text"/>	Guest
ARAP-Challenge-Response	equal to	<input type="text"/>	Guest
ARAP-Challenge-Response	equal to	<input type="text"/>	Guest
ARAP-Challenge-Response	equal to	<input type="text"/>	Guest
ARAP-Challenge-Response	equal to	<input type="text"/>	Guest

[Append Auth Rule](#)

Figure 28. Select the Role for Users who do not Match any Configured Attributes

Next, select an attribute from the **Attribute** drop-down menu and choose the **Logic** used for authentication mapping. Logic types include **equal to**, **not equal to**, **starts with**, **ends with**, and **contains**. Then, specify a corresponding **Value** and select the **Role** in which this client will be placed. In Figure 29, a RADIUS server is configured to use a **User Name** attribute that is **equal to** the value **ann jenkins**, which assigns the client the role of **Guest**.

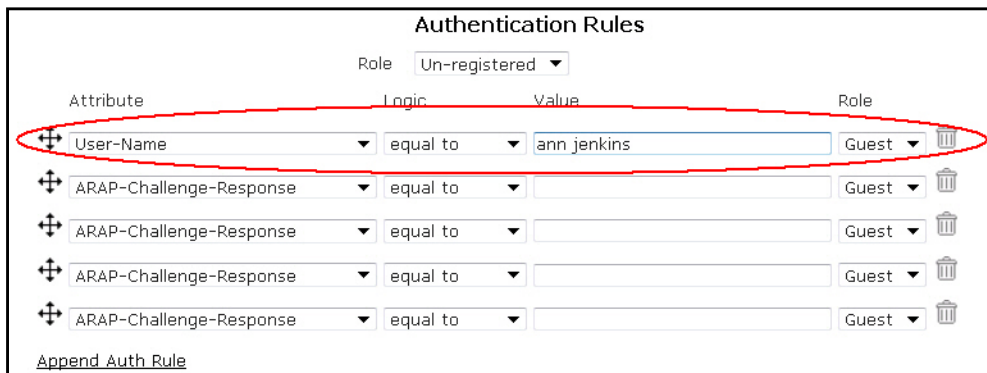


Figure 29. Configure the Match Attributes and Assigned Roles for the RADIUS Server

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

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



NOTE

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

9. Optional. Once the external server is created, you can verify it for a successful connection. Return to the **External Authentication > Servers** menu as shown in [Figure 30](#). Select the authentication server you just created from the list, and select the **Test Connection** button from the top of the menu.

Select the authentication server you want to verify.

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



Figure 30. Verify a Successful RADIUS Server Connection

You will be redirected to the **Diagnostics** menu (see Figure 31) which allows you to enter a username and password to test the authentication method. This menu can also be used to help verify what attributes the radius server returns so they can be used to match a user to a role.

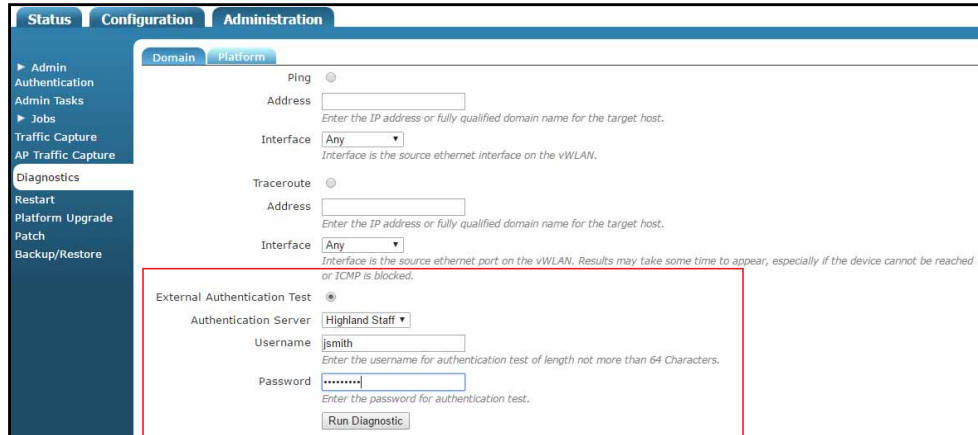


Figure 31. Diagnostics Menu

5.2.3 External LDAP Web-based Authentication Server

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

1. Navigate to the **Configuration** tab, and select **External Authentication > Servers** as show in Figure 32. Any previously configured LDAP authentication servers will be listed in the menu. If you want to edit a previously created LDAP authentication server, select the server name from the list. To create a new authentication server, either select **Create Authentication Server** at the bottom of this menu, or select **Domain Authentication Server** from the **Create** drop-down menu (at the top of the menu).

Select either option to create a new authentication server.

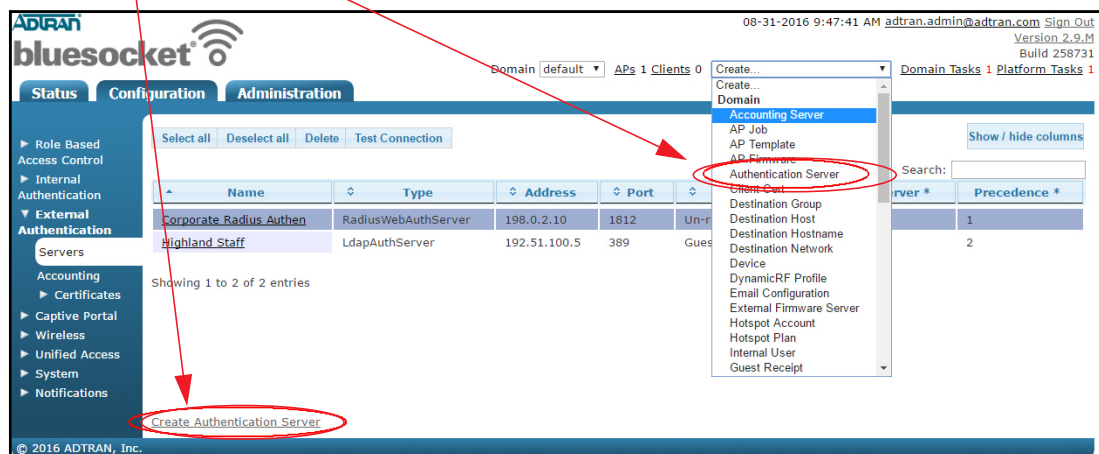


Figure 32. Navigating to the Authentication Server Menu

2. In the **New Authentication Server** menu, select **LdapAuthServer** from the **Type** drop-down menu as shown in [Figure 33](#).



A screenshot of a form field labeled 'Type' with a dropdown menu. The dropdown menu is open, and 'LdapAuthServer' is selected and displayed in the text box.

Figure 33. Create an LDAP Server

3. Enter the name of the server and its IP address in the appropriate fields as shown in [Figure 34](#). Optionally, specify if this authentication server will be associated with an accounting server by selecting the account server from the **Accounting Server** drop-down menu.



A screenshot of a form with three fields: 'Name' with the value 'LDAP Auth Server 1', 'Accounting Server' with a dropdown arrow, and 'IP Address' with the value '172.16.2.240'.

Figure 34. Name, IP Address, and Optional Accounting Server

4. Specify the port to be used by the server as shown in [Figure 35](#). 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.



A screenshot of a form field labeled 'Port' with the value '389'. Below the field is a note: 'Typically, the port should be 389 for LDAP and 636 if require SSL is checked.'

Figure 35. Specify the Port to be Used by the LDAP Server

5. Specify the name of the administrator user to which to bind the LDAP server as shown in [Figure 36](#). Enter the administrator's FQDN in the **LDAP Bind User** field.



A screenshot of a form field labeled 'LDAP Bind User' with the value 'cn=LDAP AuthUser, cn=Users, dc='. Below the field is a note: 'The name of an admin user to bind to the LDAP server with.'

Figure 36. LDAP Bind User



NOTE

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

The LDAP user field should be populated with the full name of the user, not the login name in AD. For example, use Bob Smith, not BSmith. All the name parts are used and added to each other to compose the full name. The resulting user name when using Bob and Smith as the first and last names respectively in AD is Bob Smith. Unless the LDAP user is in the root of AD, and the base entry specifies the root, you must specify where it is. This is referred to as the distinguished name. For example, if Bob Smith is in the users container, you would enter **CN=Bob Smith,CN=Users,DC=Bluesocket,DC=com** in the LDAP user field, where the first CN refers to common name, and the second CN refers

to container. If Bob Smith was in the root of AD, and the base entry specified the root, you could simply enter Bob Smith.



NOTE

Be sure not to 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.

- 6. Enter the shared secret or password for the previously created bind user as shown in [Figure 37](#).

A screenshot of a configuration window showing two text input fields. The first field is labeled "Shared Secret/Password" and contains a series of dots. The second field is labeled "Shared Secret/Password Confirmation" and also contains a series of dots.

Figure 37. Shared Secret/Password for the Bind User

- 7. Configure the LDAP base entry, unique ID attribute, and any LDAP filters as shown in [Figure 38](#). 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.

A screenshot of a configuration window with four sections. The first section is "LDAP Base Entry" with a text input field and a note: "An example base entry is cn=Users,dc=company,dc=com." The second section is "LDAP Unique ID Attribute" with a text input field and a note: "UID for openldap, sAMAccountName for AD." The third section is "LDAP Filters" with a text input field and a note: "Additional LDAP filters used when looking up Unique ID attributes. (An example is objectClass=Person)" The fourth section is "Bind All Queries As LDAP Bind User" with a checked checkbox and a note: "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."

Figure 38. LDAP Base Entry, Unique ID Attribute, and Bind All Queries Options

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

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

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

- 8. Configure the timeout weight, maximum number of simultaneous user authentications, server precedence, and whether SSL is used as shown in [Figure 39](#). The timeout weight is the value relative to the timeout weight of other

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

Timeout Weight: 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:

Figure 39. Timeout Weight, Simultaneous Users, Precedence, Require SSL Options

- Specify the authentication rules for the server and the role given to a user who does not match the specified attributes (see Figure 40). First, select the role that is given to all clients that are successfully authenticated, but do not match any of the configured attributes. For example, if you choose **Un-registered** from the drop-down menu, clients will never transition out of the Un-registered role unless they successfully authenticate and match one of the configured attributes. Select the role from the **Role** drop-down menu located in the center at the top of the **Authentication Rules** section.

Authentication Rules				
Attribute	Logic	Value	Role	
<input type="text" value="ARAP-Challenge-Response"/>	equal to	<input type="text"/>	<input type="text" value="Un-registered"/>	<input type="text" value="Guest"/>
<input type="text" value="ARAP-Challenge-Response"/>	equal to	<input type="text"/>	<input type="text" value="Un-registered"/>	<input type="text" value="Guest"/>
<input type="text" value="ARAP-Challenge-Response"/>	equal to	<input type="text"/>	<input type="text" value="Un-registered"/>	<input type="text" value="Guest"/>
<input type="text" value="ARAP-Challenge-Response"/>	equal to	<input type="text"/>	<input type="text" value="Un-registered"/>	<input type="text" value="Guest"/>
<input type="text" value="ARAP-Challenge-Response"/>	equal to	<input type="text"/>	<input type="text" value="Un-registered"/>	<input type="text" value="Guest"/>

[Append Auth Rule](#)

Figure 40. Select the Role for Users who do not Match any Configured Attribute

Next, manually specify the attribute type to use in the authentication rules (for example, **distinguishedname**) and choose the **Logic** used for authentication mapping (see Figure 41). Logic types include **equal to**, **not equal to**, **starts with**, **ends with**, and **contains**. Then, specify a corresponding **Value** and select the **Role** in which this client will be placed. In Figure 41, an LDAP server is configured to use a **distinguishedname** attribute, that contains the value **Faculty**, which assigns the user the role of **Architecture Faculty**.

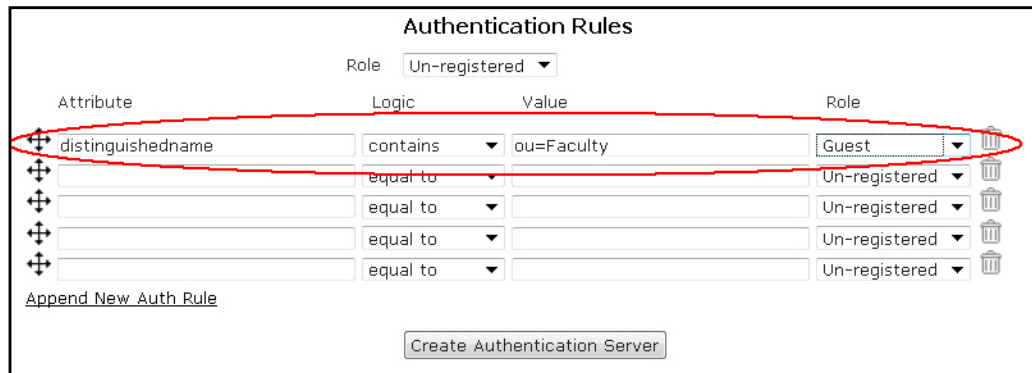


Figure 41. Configure Match Attributes and Assigned Roles for the LDAP Server

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

10. Select **Create Authentication Server**. A confirmation is displayed indicating that the server has been created. The server will now appear in the server list (**Configuration** tab, **External Authentication** > **Servers**), where you can display, edit, or delete the server.
11. Optional. Once the external server is created, you can verify it for a successful connection. Return to the **External Authentication** > **Servers** menu as shown in [Figure 42](#). Select the authentication server you just created from the list, and select the **Test Connection** button from the top of the menu.

Select the authentication server you want to verify.

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

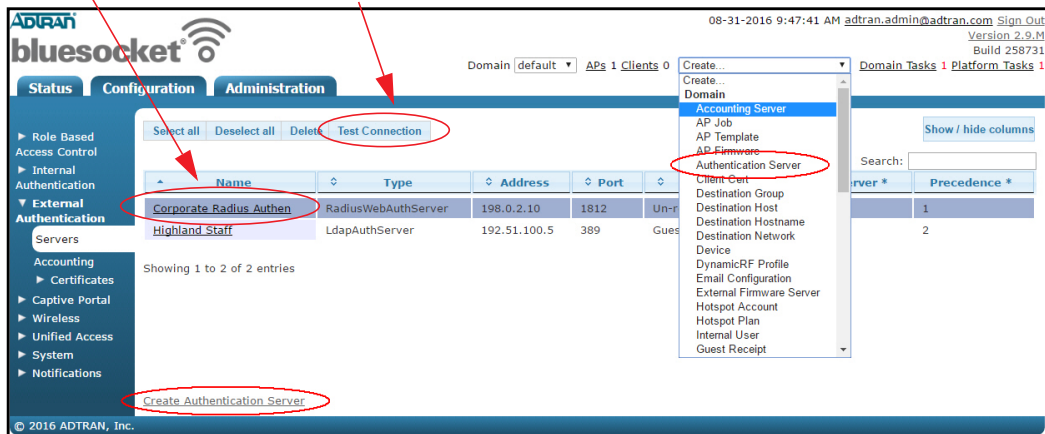


Figure 42. Verify a Successful LDAP Server Connection

You will be redirected to the **Diagnostics** menu which allows you to enter a username and password to test the authentication method (see [Figure 43](#)). This menu can also be used to help verify what attributes the LDAP server returns so they can be used to match a user to a role.

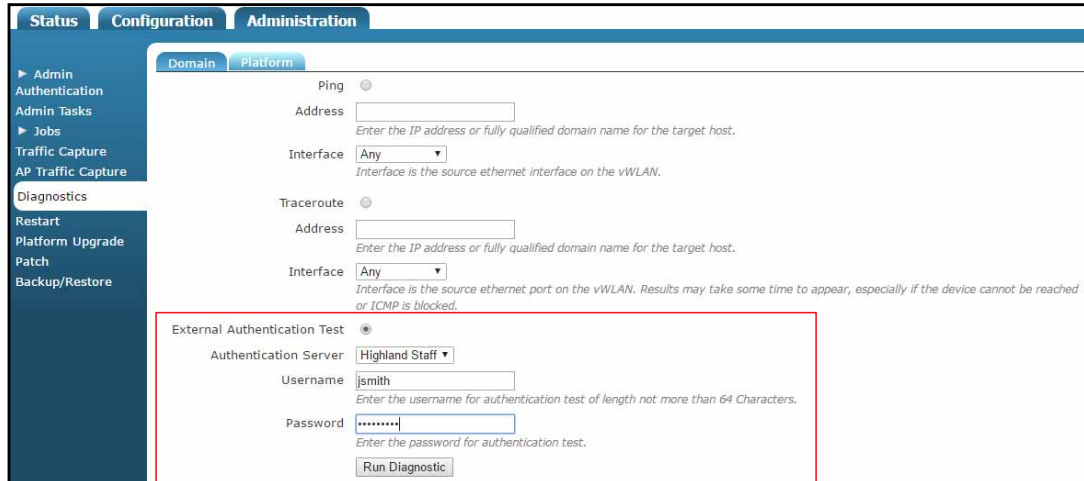


Figure 43. Diagnostics Menu

5.2.4 External SIP2 Web-based Library Authentication Server

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

1. Navigate to the **Configuration** tab, and select **External Authentication > Servers** as shown in [Figure 44](#). Any previously configured SIP2 authentication servers will be listed in the menu. If you want to edit a previously created SIP2 authentication server, select the server name from the list. To create a new authentication server, either select **Create Authentication Server** at the bottom of this menu, or select **Domain Authentication Server** from the **Create** drop-down menu (at the top of the menu).

Select either option to create a new

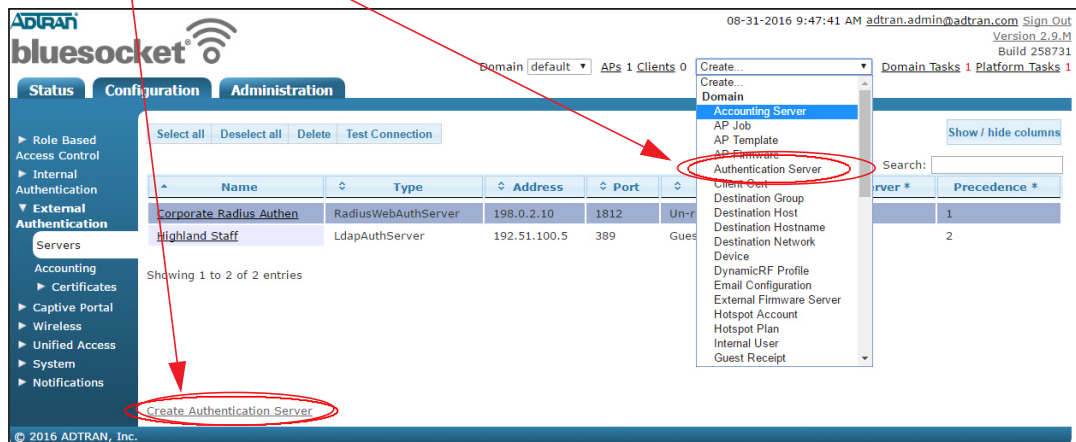


Figure 44. Navigating to the Authentication Server Menu

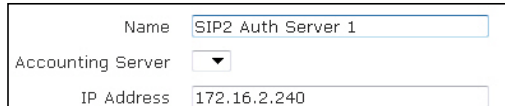
2. Select **SIP2AuthServer** from the **Type** drop-down menu as shown in [Figure 45](#).



A screenshot of a form field labeled 'Type' with a dropdown menu. The dropdown menu is open, and 'Sip2AuthServer' is selected.

Figure 45. Create a SIP2 Server

3. Enter the name of the server and its IP address in the appropriate fields. Optionally, specify if this authentication server will be associated with an accounting server by selecting the account server from the **Accounting Server** drop-down menu as show in [Figure 46](#)..



A screenshot of a form with three fields: 'Name' containing 'SIP2 Auth Server 1', 'Accounting Server' as a dropdown menu, and 'IP Address' containing '172.16.2.240'.

Figure 46. Name, IP Address, and Optional Accounting Server

4. Specify the port to be used by the server. If you are using a SIP2 server, the port is generally **6001** as shown in [Figure 47](#).



A screenshot of a form field labeled 'Port' with the value '6001'. Below the field is a note: 'Typically, the port should be 6001.'

Figure 47. Specify the Port Number for the SIP2 Server

5. Optionally, specify the name of the administrator user to which to bind the SIP2 server. Enter the administrator's FQDN in the **SIP2 Admin Name** field as shown in [Figure 48](#).



A screenshot of a form field labeled 'SIP2 Admin Name' with the value 'joesmith@adtran.com'. Below the field is a note: 'The name of an admin user to authenticate to the SIP2 server with.'

Figure 48. SIP2 Administrator Option



NOTE

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

6. Optionally, enter the shared secret or password for the authentication server as shown in [Figure 49](#).



A screenshot of a form with two fields: 'Shared Secret/Password' and 'Shared Secret/Password Confirmation'. Both fields are masked with dots.

Figure 49. Optional Shared Secret/Password for SIP2 Server

7. Specify the timeout weight for the server as shown in [Figure 50](#). This value is relative to the timeout weight of other authentication servers. The total time allocated to authenticate is defined for the entire vWLAN system. Each server's

timeout is computed as a percentage of the total weight of all authentication servers in this domain (the platform setting of **Timeout Value for Web Server** determines the total timeout that is divided based on weight).

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

Figure 50. SIP2 Server Timeout Weight

- Specify whether the user's PIN or password will be validated by selecting the **SIP2 Validate PIN/Password** check box as shown in [Figure 51](#).

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

Figure 51. SIP2 Validate PIN/Password

- Specify whether an empty AO institution ID is specified when communicating with the server by selecting the **SIP2 Specify an empty AO Institution ID** check box as shown in [Figure 52](#)

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

Figure 52. SIP2 Empty AO Institution ID

- 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 as shown in [Figure 53](#). Leave this field blank if you do not want a CP location code in the login message.

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

Figure 53. SIP2 CP Location Code

- Configure the maximum number of simultaneous users allowed to authenticate and the server precedence as shown in [Figure 54](#). Leaving the maximum number of simultaneous authentications field blank, or entering a 0, indicates there is no limit. You can specify the precedence level of the server as **Highest**,

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

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

Figure 54. Simultaneous Users and Server Precedence

- Specify the authentication rules for the server and the role given to a user who does not match the specified attributes (See Figure 55). First, select the role that is given to all clients that are successfully authenticated, but do not match any of the configured attributes. For example, if you choose **Un-registered** from the drop-down menu, clients will never transition out of the Un-registered role unless they successfully authenticate and match one of the configured attributes. Select the role from the **Role** drop-down menu located in the center at the top of the **Authentication Rules** section.

Authentication Rules

Role

Attribute	Logic	Value	Role
ARAP-Challenge-Response	equal to	<input type="text"/>	Guest
ARAP-Challenge-Response	equal to	<input type="text"/>	Guest
ARAP-Challenge-Response	equal to	<input type="text"/>	Guest
ARAP-Challenge-Response	equal to	<input type="text"/>	Guest
ARAP-Challenge-Response	equal to	<input type="text"/>	Guest

[Append Auth Rule](#)

Figure 55. Select the Role for Users who do not Match any Configured Attribute

Next, manually specify the attribute type to use in the authentication rules (for example, **PC: profile**) and choose the **Logic** used for authentication mapping as shown in Figure 56. Logic types include **equal to**, **not equal to**, **starts with**, **ends with**, and **contains**. Then, specify a corresponding **Value** and select the **Role** in which this client will be placed. In Figure 56, a SIP2 server is configured to use a **PC:profile** attribute, that contains the value **Adult**, which assigns the user the role of **Guest**.

Authentication Rules

Role

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

[Append New Auth Rule](#)

Figure 56. Configure Match Attributes and Assigned Roles for the SIP2 Server

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

13. Select **Create Auth Server**. A confirmation is displayed indicating that the server has been created. The server will now appear in the server list (**Configuration** tab, **External Authentication > Servers**), where you can display, edit, delete, or test the connection to the server.
14. Optional. Once the external server is created, you can verify it for a successful connection. Return to the **External Authentication > Servers** menu as shown in [Figure 57](#). Select the authentication server you just created from the list, and select the **Test Connection** button from the top of the menu.

Select the authentication server you want to verify.

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

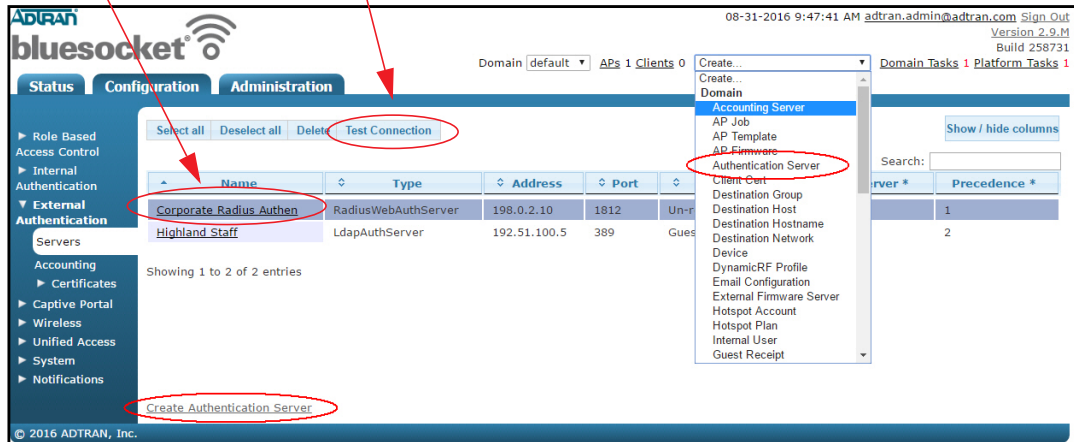


Figure 57. Verify a Successful SIP2 Server Connection

15. You will be redirected to the **Diagnostics** menu which allows you to enter a username and password to test the authentication method (see [Figure 58](#)). This menu can also be used to help verify what attributes the SIP2 server returns so they can be used to match a user to a role.

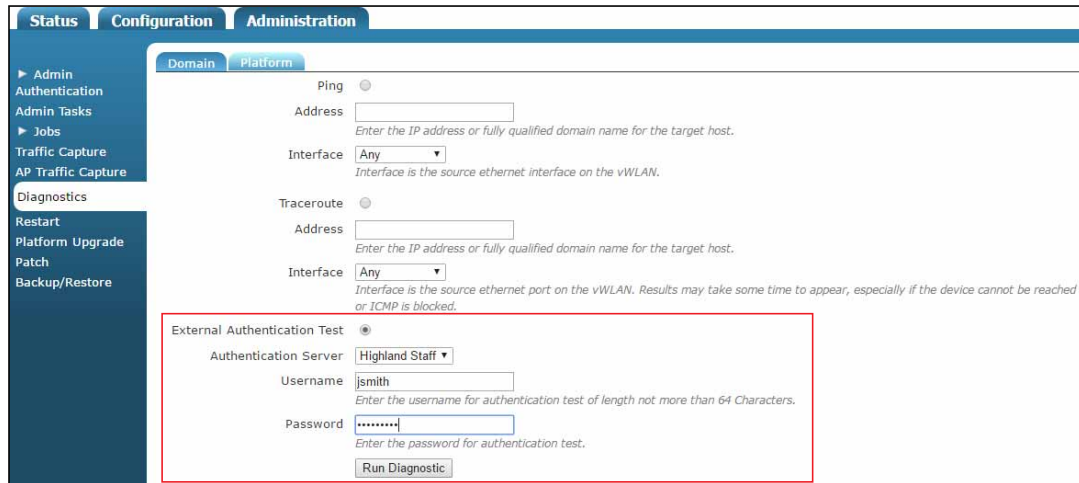


Figure 58. Diagnostics Menu

5.3 Configuring Local Server Authentication

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

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

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

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

1. Navigate to the **Configuration** tab, and select **Internal Authentication > Users** as shown in [Figure 59](#). Any previously configured internal users will be listed in the menu. If you want to edit a previously created internal user, select the user name from the list. To create a new internal user, either select **Create Internal User** at the bottom of this menu, or select **Domain Internal User** from the **Create** drop-down menu (at the top of the menu).

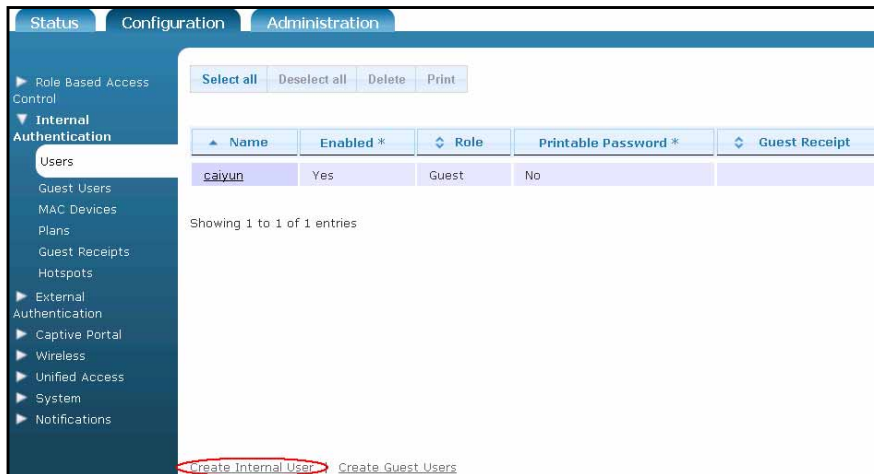


Figure 59. Navigating to the Internal User Authentication Menu

- Specify the user's name and password in the corresponding fields, and enable the user by checking the **Enabled** box (See Figure 60). Select the user's role from the **Role** drop-down menu. Optionally, select an accounting server to associate with this user from the **Accounting Server** drop-down menu. **Simultaneous User Authentication** allows you to specify the number of users with the same name that can be logged in at the same time. If you specify 0, there is no limit to how many users with the same name can be logged in simultaneously. Select the check box next to **Never expire** to specify that the user account does not expire.

The 'Create Internal User' form contains the following fields and values:

- Name: john doe
- Password: [masked]
- Password Confirmation: [masked]
- Enabled:
- Role: Guest
- Accounting Server: [empty]
- Simultaneous User Authentication: 0 (0 is unlimited)
- Expire User: Never expire

The 'Create Internal User' button at the bottom is circled in red.

Figure 60. Create Internal User

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

6 Additional Options

6.1 Captive Network Assistant (CNA) Support

As part of the AP template (**Configuration** tab, **Wireless > AP Templates**), the administrator can choose to enable or disable Captive Network Assistant (CNA). By default, CNA is enabled on the AP template. When CNA is enabled, vWLAN responds to the device's CNA request with a redirection 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 sign-in window automatically and prompts the user to enter their credentials in the vWLAN login page. For Microsoft NCSI, an information popup appears at the bottom right corner of the computer suggesting the user open a web browser to authenticate. If CNA is disabled, the device will connect using a web request via web browser which redirects to vWLAN Captive Portal.

When enabled, there are two supplementary configuration requirements that are necessary for CNA to function properly. A trusted SSL certificate must be loaded in vWLAN and vWLAN must be configured to redirect to a hostname (a DNS server and hostname may need to be configured).

6.1.1 Loading an SSL Certificate

1. Before you begin, be sure to have all of the certificate details. Navigate to the **Configuration** tab, select **System > Settings**, and then select the **Platform** tab as shown in [Figure 61](#). For a certificate upload, select **Certificate 1** or **Certificate 2** (depending if you are uploading to the first or second certificate)



NOTE

For detailed information, including how to generate a CSR and submit to a third party, see [Installing and Renewing an SSL Certificate in vWLAN](#) available online at support-forums.adtran.com.

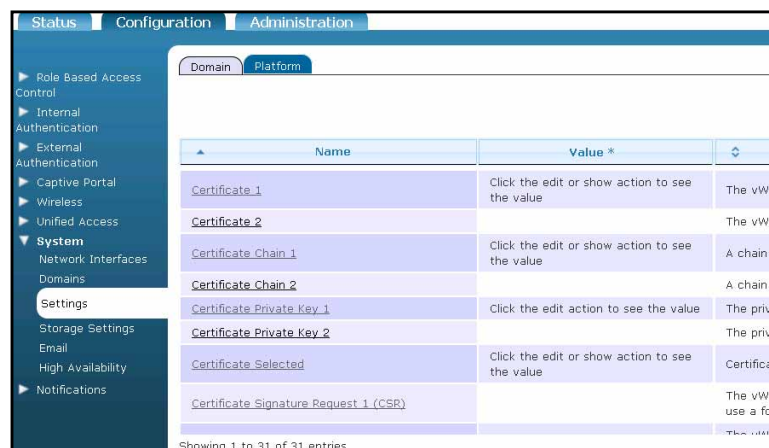


Figure 61. Navigating to the Custom Certificate Menu

- Copy and paste the text of the certificate into the **Certificate 1** or **Certificate 2** field (See [Figure 62](#)). Select **Update Platform Settings** to add the certificate.

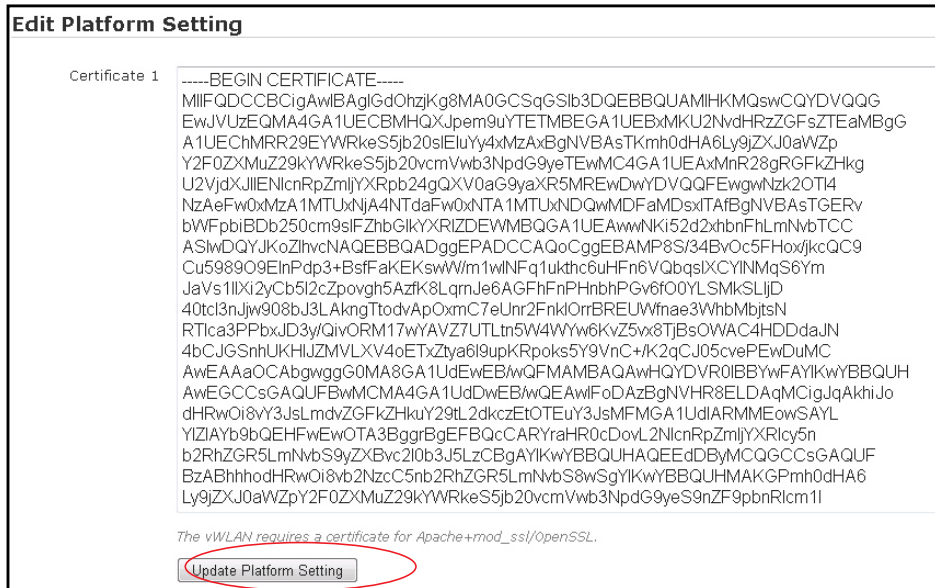


Figure 62. Copy/Paste Custom Certificate Details

- To add certificate chains using this method, select **Certificate Chain 1** or **Certificate Chain 2** in the **System > Settings** menu as shown in [Figure 63](#). If you did not generate the CSR request from the vWLAN, you will need to add the **Certificate Private Key**.



NOTE

Make sure that the number you use for Certificate Private Key and Certificate Chain (1 or 2) corresponds to the certificate number that you uploaded in Step 1 on page 40..



Figure 63. Adding Certificate Chains

- 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. Be sure to save your settings. You will receive a Platform Task *Must restart User Web Server and Admin Web Server*. Wait until you are finished configuring [Redirect to a Hostname](#) and [Final Steps](#) before executing queued Platform and Domain tasks.

6.1.2 Redirect to a Hostname

The redirect to hostname option requires both a forward (A record) and a reverse pointer (PTR record) in your organization’s DNS server for the public network interface and the fully qualified domain name (FQDN) of the vWLAN. The vWLAN and APs query the PTR record and redirect traffic based on the response. If there is no PTR record, clients are redirected to an IP address (rather than a hostname). This action can result in the receipt of a web browser security warning indicating a domain name mismatch. Clients use the A record to resolve the host name of vWLAN to an IP address.

1. Enable vWLAN to redirect to a host name by navigating to the **Configuration** tab, select **System > Settings**, and then select the **Platform** tab as shown in [Figure 64](#). Select the **Redirect to hostname** setting from the list.

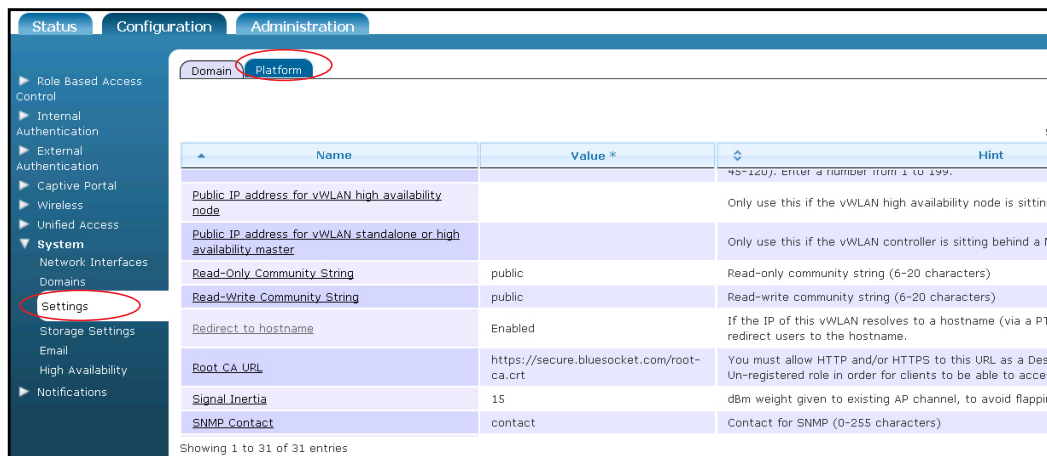


Figure 64. Navigating to the Redirect to Hostname Option

2. Change the **Redirect to Hostname** to **Enabled** using the drop-down menu, and select **Update Platform Setting** as shown in [Figure 65](#). You will receive confirmation that the setting has been changed and you will receive a Platform Task titled *Must restart User Web Server*. Wait until you are finished configuring [Redirect to a Hostname](#) and [Final Steps](#) before executing queued Platform and Domain tasks.

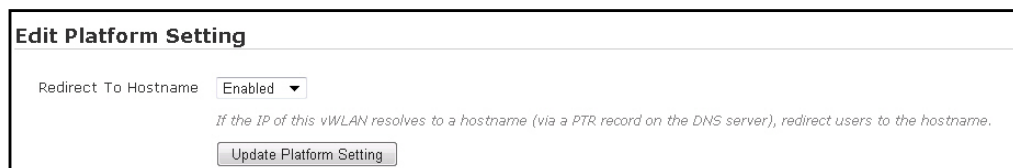


Figure 65. Enable Redirect to Hostname

- An AP looks up the vWLAN name using a DNS pointer record (PTR) when redirecting clients to a host name for authentication. This setting must be enabled when **Redirect to Hostname** is enabled. Navigate to the **Configuration** tab, select **System > Settings**, and then select the **Domain** tab as shown in [Figure 66](#). Ensure that the option **Allow the AP to look up the vWLAN name using a DNS PTR record** is enabled. You will receive a Domain Task titled *Must apply configuration to APs*. Wait until you are finished configuring [Final Steps](#) before executing queued Platform and Domain tasks.

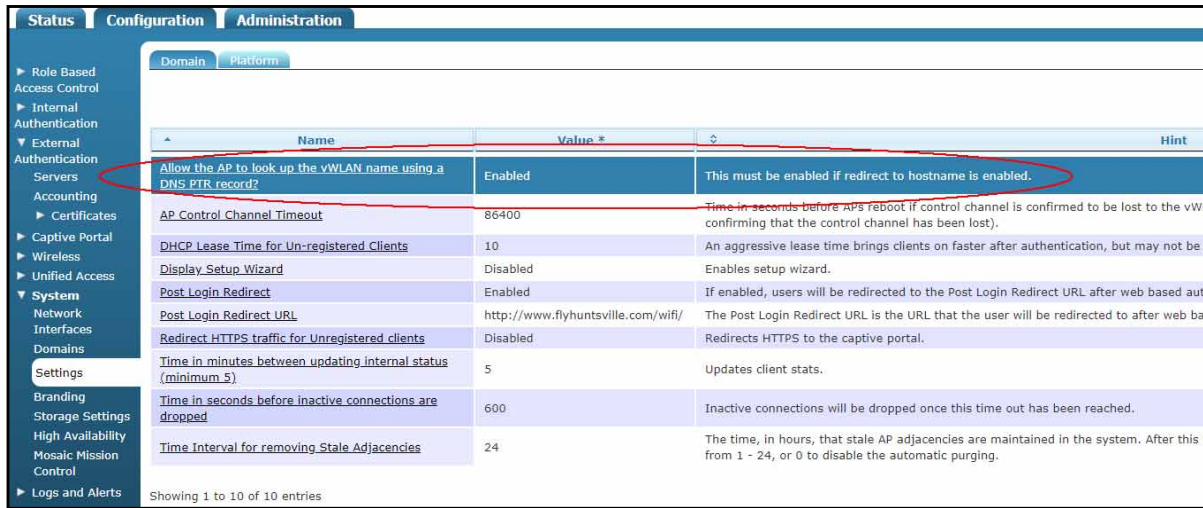


Figure 66. Enable Allow the AP to Look Up the vWLAN Name Using a DNS PTR Record Option

6.1.3 Final Steps

- Navigate to the AP template (**Configuration** tab, **Wireless > AP Templates**) and ensure that CNA support is enabled as shown in [Figure 67](#). If applicable, specify the DNS server to be used by clients in the Un-Registered role to resolve the host name (the AP will use its DNS server to resolve the name). Once the changes have been made to the template, select **Create AP Template** or **Update AP Template**. You will receive a Domain Task titled *Must apply configuration to APs*. Wait until [Step 4](#) on page 45 to execute queued Platform and Domain tasks.

Create AP Template

Name: root@adtran.com

SSH Password: [Redacted]

SSH Password Confirmation: [Redacted]

Login Form: Default Login Form

DNS Server(s) For NAC Users: 0.0.0.0
Set to 0.0.0.0 to use the DNS server from the AP's Native VLAN.
 A maximum of two DNS servers can be added separated by a comma.

Release	Server
1800v1 Firmware: [Dropdown]	vWLAN [Dropdown]
1800v2/1840 Firmware: [Dropdown]	vWLAN [Dropdown]
1920/1925 Firmware: [Dropdown]	vWLAN [Dropdown]
1930/1935/1940 Firmware: [Dropdown]	vWLAN [Dropdown]

Enable Captive Network Assistant:
Check to enable Apple CNA or Microsoft NCSI.
 *Requires Trusted Certificate on vWLAN.
 *Requires redirect to hostname to be enabled in platform settings.

Figure 67. Check the DNS Server Used to Resolve Hostname and that CNA is Enabled

The configuration for CNA support on vWLAN is complete. When enabled, CNA will display a popup window whenever a mobile 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.



NOTE

By default, vWLAN uses a preinstalled self-signed SSL certificate to encrypt web-based login transactions. The vWLAN uses the SSL certificate when clients connect to the Captive Portal (which uses HTTPS), or when administrators connect to the vWLAN GUI (which also uses HTTPS). In both cases, when using the default Bluesocket self-signed SSL certificate, users can receive a certificate error from the web browser indicating the certificate was not issued by a trusted CA. This happens because the Bluesocket self-signed certificate is not in the browser's list of trusted root certificate authorities and Bluesocket is not a CA. These errors can be avoided by either installing the self-signed certificate on each client in the browser's list of trusted root CAs, or by installing an SSL certificate (provided by a CA, such as VeriSign that matches the FQDN created on your organization's DNS server) on vWLAN that is already in the client's list of trusted root CAs. To install SSL certificates on vWLAN, refer to [Installing and Renewing an SSL Certificate in vWLAN](http://supportforums.adtran.com) available online at supportforums.adtran.com.

2. Change the network interface hostname setting. Navigate to the **Configuration** tab, and select **System > Network Interfaces** as shown in Figure 68. Select the **public** interface from the list.

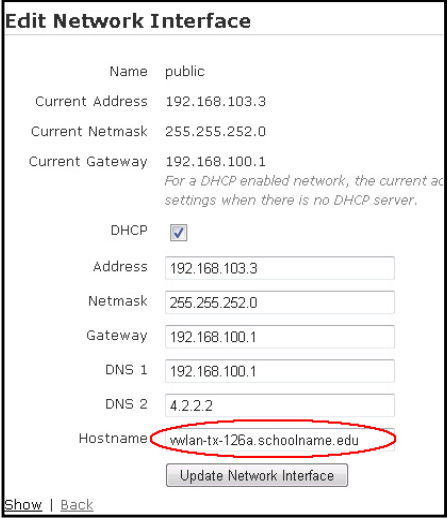


Name	DHCP *	Address *	Netmask *
private	Disabled	10.251.252.1	255.255.255.0
public	Disabled	192.168.103.3	255.255.252.0

Showing 1 to 2 of 2 entries

Figure 68. Navigate to the Network Interface Hostname Settings

3. Enter the hostname in the **Hostname** field and select **Update Network Interface** as shown in Figure 69.



Edit Network Interface

Name public

Current Address 192.168.103.3

Current Netmask 255.255.252.0

Current Gateway 192.168.100.1

For a DHCP enabled network, the current address settings when there is no DHCP server.

DHCP

Address 192.168.103.3

Netmask 255.255.252.0

Gateway 192.168.100.1

DNS 1 192.168.100.1

DNS 2 4.2.2.2

Hostname wlan-tx-126a.schoolname.edu

Update Network Interface

Show | Back

Figure 69. Set the Hostname for the Network Interface

4. Execute queued Platform and Domain tasks. Several of the changes you made in the previous sections, [Loading an SSL Certificate](#), [Redirect to a Hostname](#), and [Final Steps](#), generated Platform and Domain tasks that now need to be executed. Navigate to the **Administration** tab and select **Admin Tasks** (See [Figure 70](#)). Select the **Domain** or **Platform** tab (there will likely be tasks to execute within both tabs at this point). Alternatively, you can select the **Domain Tasks** or **Platform Tasks** links in the upper right-hand corner of any page to go directly to the tasks queue. [Figure 70](#) shows the queued tasks under the **Domain** tab.

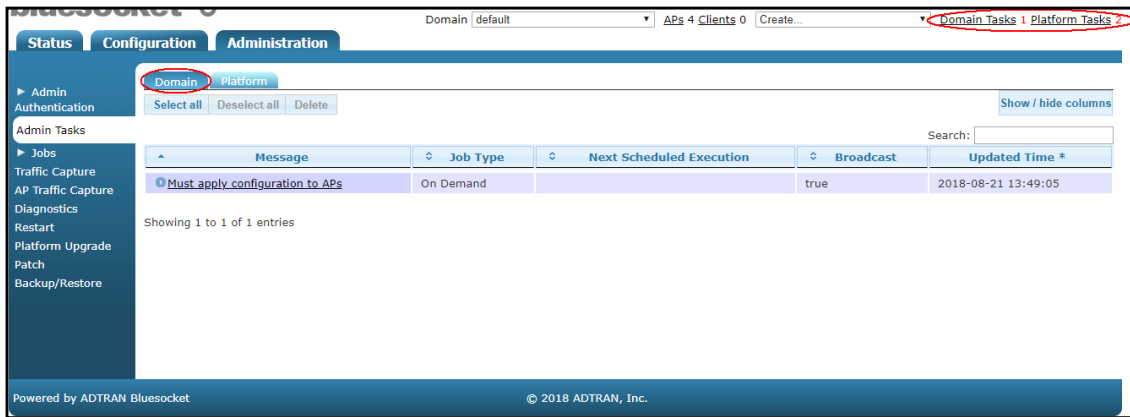


Figure 70. Navigating to the Domain Tasks under the Admin Tasks Menu

As soon as you select the name of a Message, the selected task will execute. Figure 71 shows the queued tasks under the **Platform** tab.

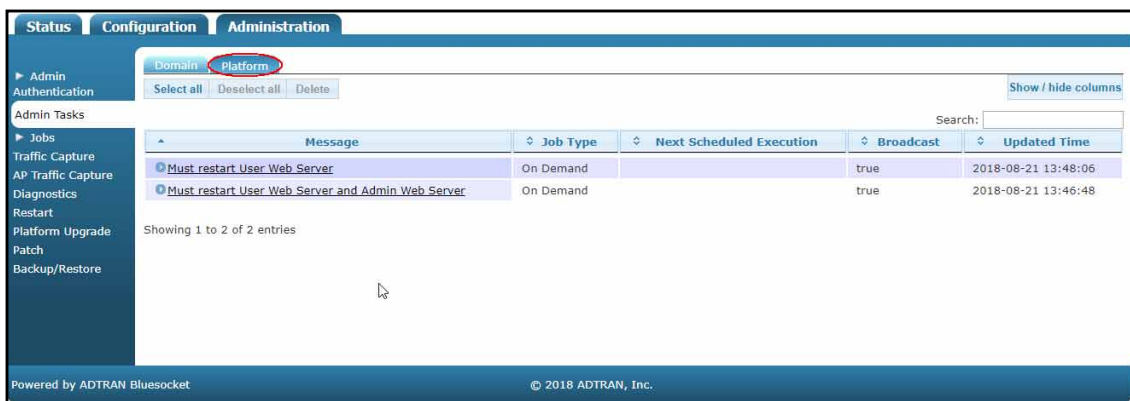


Figure 71. Queued Platform Tasks

6.2 HTTPS Redirection

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

1. Navigate to the **Configuration** tab, and select **System > Settings** and then select the **Domain** tab as shown in [Navigating to the HTTPS Redirection Option](#). Select the **Redirect HTTPS traffic for Unregistered clients** setting from the list. Enable the setting and select **Update Domain Setting**. You will receive a Domain Task titled *Must apply configuration to APs*. Be sure to execute this task (See Step 4 on page 45 for information on how to execute Platform and Domain tasks).

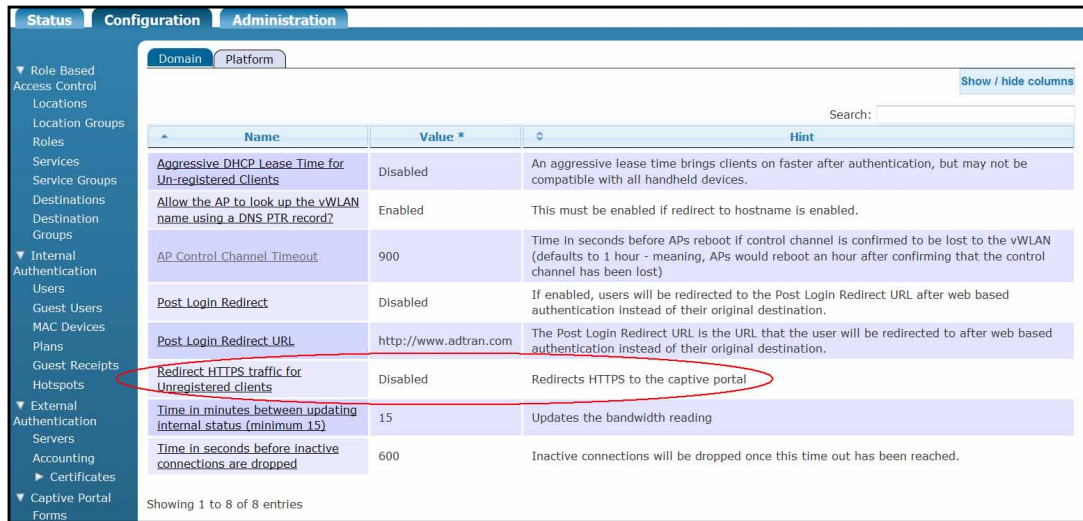


Figure 72. Navigating to the HTTPS Redirection Option

6.3 Disable TLS 1.0

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

To disable TLS 1.0, follow these steps:

1. Navigate to the Configuration tab and select **System > Settings**. Select the **Platform** tab and choose **Enable TLS 1.0** as shown in Figure 73.

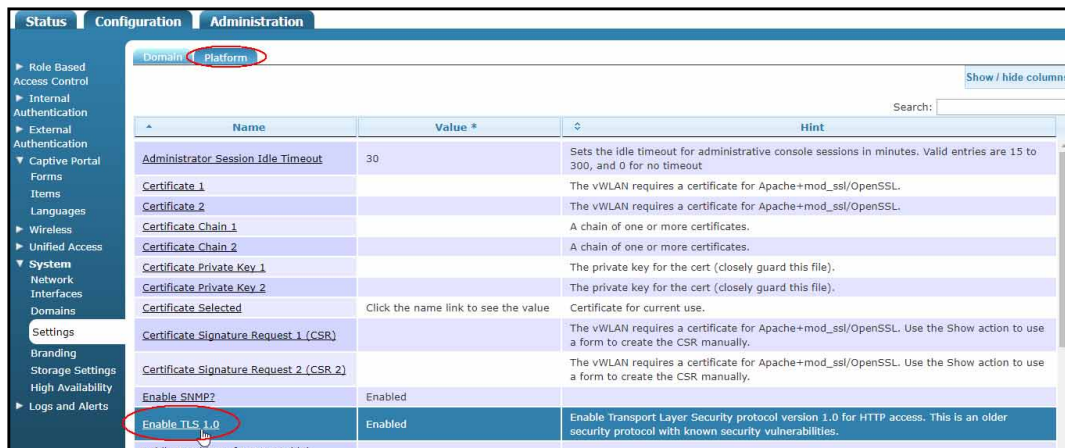


Figure 73. Navigate to the TLS 1.0 Setting

2. Select **Disable** from the drop-down menu. Next, select **Update Platform Setting** as shown in Figure 74. You will receive a Platform Task titled *Must reboot the system to activate TLS settings*. Be sure to execute this task (See Step 4 on page 45 for information on how to execute Platform and Domain tasks.



Figure 74. Disable TLS 1.0 and Update the Platform Setting

7 Troubleshooting

7.1 Testing

1. You should now be able to associate a client to your previously created SSID (See [Figure 75](#)). The client should receive an authentication (NAC) IP address or, if you created your own Un-Registered role type, an IP address from that location.

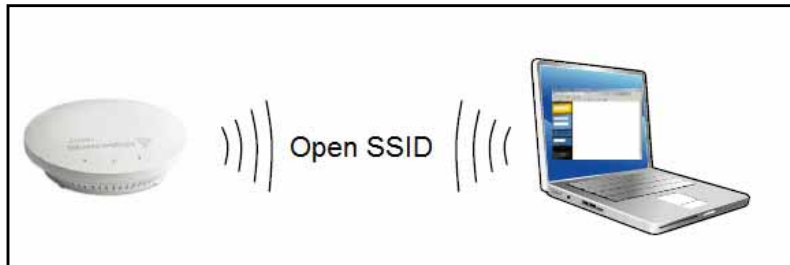


Figure 75. Test to Verify that a Client can Associate with the SSID

2. Open a web browser on the client and try to browse to an HTTP site (not in cache). The client should query DNS, and then make an HTTP Get. The AP will be monitoring for HTTP traffic and will intercept the client's HTTP Get and will redirect the client to the vWLAN. The client should then be presented with the web page to log into the network as shown in [Figure 76](#) (You may be presented with an SSL certificate warning before being presented with the web page depending on how you configured vWLAN in the steps above.)



Figure 76. Captive Portal Landing Page

3. The client should now be able to login with a username and password, which is authenticated against a local user database, external Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) server, external web-based 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 **Guests** box in blue in the figure above only requires an email address for log in. This box can be removed from the Captive Portal Form by unchecking **Allow Guest Logins**). Refer to the document [Fully Customized Login Page Configuration Differences in vWLAN 2.5.0 and 2.5.1](#) available online at supportforums.adtran.com for detailed information on customization of Captive Portal login menus.

7.2 Common Problems

7.2.1 Logs

The vWLAN log includes the **Service** it is associated with, the **Function** monitored by the log, the type of log message (**Operation**), the **Message** itself, the **Level** associated with the log, and the time the log was created. To view logs, navigate to the **Status** tab, and select **Logs**. Figure 77 shows information messages as well as error messages contained in the log.

Created Time	Service	Function	Operation	Message	Level
2018-08-21 14:30:57	web	authentication	successful	Login user test at [e8:50:8b:ee:16:00]/10.253.68.2 as role AllowAll	INFORMATION
2018-08-21 14:30:55	user	login	failed	Login user test at [e8:50:8b:ee:16:00]/10.253.68.2 has failed.	ERRORS
2018-08-21 14:30:53	user	login	failed	Login user test at [e8:50:8b:ee:16:00]/10.253.68.2 has failed.	ERRORS
2018-08-21 14:30:35	config	change	successful	Purged Log by root@adtran.com at 172.30.11.196	INFORMATION
2018-08-21 14:30:35	log	truncate	successful	Logs purged successfully	INFORMATION

Figure 77. Log Messages

7.2.2 Client is not Redirected

1. The client must be able to resolve DNS to be redirected to the login page. From a CMD prompt of a client try pinging or performing an nslookup for www.adtran.com to see if the fully qualified domain name resolves to an IP address. If redirecting to hostname, make sure the client is able to resolve DNS both the forward (A record) and a reverse pointer (PTR record). By default the vWLAN allows DNS in the Un-registered role to the DNS servers that the client is given. Also by default, (while in the Un-registered role), clients are given the DNS servers that are assigned to the AP. Check to make sure DNS servers are assigned to the AP. Alternatively, you can configure DNS servers under **Configuration > Wireless > AP Templates**, which will take precedence for the client, meaning the client will obtain the DNS server in the AP template and not the DNS server the AP has itself. You should also be able to see this in an AP Traffic Capture taken from the NAC interface (the interface responsible for Un-registered users). If you are using the apdiscovery hostname for AP discovery, only an A record is required (delete the PTR record).
2. Check to see if client is trying to go to an HTTP web page rather than HTTPS page. By default the AP only monitors HTTP requests from clients in the Un-registered role. If the client's home page is set to an HTTPS page, it will not be redirect by default. Have the client browse to an HTTP page or alternatively,

enable **Redirect HTTPS traffic for Unregistered clients** under **Configuration > System > Settings > Domain**.



NOTE

This option should only be enabled when needed due to extra resource consumption.

3. Ensure the Domain Setting **Allow the AP to look up the vWLAN name using a DNS PTR** record and the Platform Setting **Redirect to hostname** options are either both enabled (for redirect to hostname), or both disabled (redirect to IP).

7.2.3 Client receives an SSL warning

Allow HTTP access to the OCSP and CRL URLs of your SSL certificate in the Unregistered role as demonstrated in the document *Installing and Renewing an SSL Certificate in vWLAN* available online at supportforums.adtran.com.

7.2.4 Cannot Login to the Splash Page

1. All web authentication requests are sent directly from the vWLAN (public interface) to the authentication server. Conducting a vWLAN Traffic Capture (on the Public interface) filtered on the port used for authentication will show the authentication processes. For example, if using LDAP, you should see the bind user establish a connection with the server, complete the lookup for the user, and, if found, grant them access. You should be able to see that in the vWLAN traffic capture (if not using SSL-LDAP). Refer to the *vWLAN and BSAP Traffic Capture Guide* available online at supportforums.adtran.com for more information.
2. If using LDAP or AD, ensure the LDAP Bind user is checked in the external server.

8 Warranty and Contact Information

8.1 Warranty

Warranty information can be found at:

www.adtran.com/warranty.

8.2 Contact Information

For all customer support inquiries, please contact ADTRAN Customer Care:

Contact	Support	Contact Information
Customer Care	From within the U.S. From outside the U.S. Technical Support: ■ Web: Training: ■ Email: ■ Web:	1.888.4ADTRAN (1.888.423.8726) + 1.256.963.8716 www.adtran.com/support training@adtran.com www.adtran.com/training www.adtranuniversity.com
Sales	Pricing and Availability	1.800.827.0807