Pulse Policy Secure

Ruckus WLC Guest Access Integration – SmartZone and ZoneDirector

Solution Guide
Table of Contents

Introduction ............................................................................................................................................... 5

Customer Challenges ........................................................................................................................... 5

Guest Access Solution with Wireless LAN Controllers ................................................................. 6

Default Configuration Settings on Pulse Policy Secure ................................................................. 6

Configuring Authentication Protocol sets for Guest Access ............................................................. 7

Configuring Guest Sign-In Policies ..................................................................................................... 8

Configuring a Guest Admin Realm ........................................................................................................ 10

Configuring User Roles for Guest User Account Manager ................................................................. 12

Configuring Location group for Guest Access ..................................................................................... 13

Configuring Guest Authentication Server .......................................................................................... 14

Configuring RADIUS Client on Pulse Policy Secure ........................................................................ 17

Configuring SMTP and SMS gateway settings on Pulse Policy Secure ........................................... 19

SMTP Settings for Guest User Accounts .......................................................................................... 19

SMSP Gateway Settings for Guest User Accounts ............................................................................. 20

Configuring Guest Access Settings on Pulse Policy Secure ............................................................... 23

Enabling Onboarding Feature ............................................................................................................ 24

Guest-Self Registration Configuration ............................................................................................... 26

Configuring Ruckus WLC with Pulse Policy Secure .......................................................................... 27

Ruckus SmartZone WLC Configuration ............................................................................................... 28

Ruckus ZoneDirector WLC Configuration ........................................................................................... 31

Configuring Pulse Policy Secure for Dot1x Authentication ............................................................... 33

Configuring User Role for Dot1x Authentication ............................................................................... 33

Configuring User Realm for Dot1x ..................................................................................................... 33

Configuring a Sign-In Policy for Dot1x ............................................................................................... 34

Configuring Location Group for Dot1x ............................................................................................... 35

Configuring Authentication Protocol Set for Dot1x .......................................................................... 36

Configuring RADIUS Client ............................................................................................................... 36

Ruckus WLC Dot1x Configuration ....................................................................................................... 38
Introduction

In current scenarios, guest access solution for wireless network can be deployed with leading Wireless LAN Controllers (WLC). Pulse Policy Secure (PPS) is a complete guest access management solution and simplifies an organization's ability to provide secure, differentiated guest user access to their networks.

Ruckus Wireless is a fast-growing wireless infrastructure vendor whose portfolio spans Access Points (APs), WLC and Management software. Ruckus Wireless ZoneDirector platform is targeted at medium-sized enterprises, while Ruckus Wireless SmartZone platform is targeted at Carriers and large enterprises.

Pulse Policy Secure already integrates with major wireless infrastructure vendors such as Cisco and Aruba, and integration with Ruckus will broaden Pulse Policy Secure inter-operability base. The inter-operability will be on two fronts:

* RADIUS/Dot1x
  * Guest Access

The Guest Access feature enables a guest/contractor to access a special self-registration URL and create their own guest account for internet access.

The primary target of the Dot1x integration is to support Ruckus Vendor Specific Attributes (VSAs). Standard attributes are expected to work well when the standard RADIUS dictionary is used with Ruckus WLC. Ruckus ZoneDirector and SmartZone support the same set of VSAs.

Guest Access handling between Ruckus ZoneDirector and SmartZone differs where ZoneDirector uses URL attributes in the redirection for session identification for the hotspot feature.

Customer Challenges

With BYOD proliferation, mobile workers and virtual offices are challenging IT's ability to deliver enterprise-grade security, manageability, and interoperability. It needs complete visibility of all devices that are accessing enterprise data from their protected resources. Increasing use of mobile devices and BYOD require uniform compliance enforcement for PCs and mobile devices regardless of ownership.

Enterprises need to control access for BYOD and guest users. Hence, it is essential to co-relate user identity information of BYOD and apply granular security policies based on roles. To minimize security risk, enterprise IT also requires device compliance check for BYOD.
Guest Access Solution with Wireless LAN Controllers

In current scenarios, guest access solution for wireless network can be deployed with leading wireless LAN controllers. In this guide, customer can deploy wireless network with WLCs and wireless network for guests. Guest authentication can be done with external authentication server. Pulse Policy Secure server can be positioned as external authentication server.

Default Configuration Settings on Pulse Policy Secure

This section describes the default configuration settings required on Pulse Policy Secure to communicate with a Wireless LAN Controller (WLC) for guest user account management.

Pulse Policy Secure server acts as Radius server that allows to centralize the authentication and accounting for the users. Guest user self-registration options need to be configured in the authentication server used for managing guest accounts and in sign-in policy settings. The following topics describe the default configuration settings on Pulse Policy Secure:

- Configuring Authentication Protocol sets for Guest Access
- Configuring Guest Sign-In Policies
- Configuring a Guest Admin Realm
- Configuring User Roles for Guest User Account Manager
- Configuring Location group for Guest Access
- Configuring Guest Authentication Server
Configuring Authentication Protocol sets for Guest Access

The ‘Guest’ is the default Authentication Protocol Set configured in Pulse Policy Secure.

To view the Authentication Protocol:


   *Figure 1: Authentication Protocols for Guest Access*

2. Select the protocol name you want as the default Authentication Protocol Set.

   *Figure 2: Default Authentication Protocol Sets*

3. You can make necessary changes and click Save Changes to save the settings.
Configuring Guest Sign-In Policies

The */guestadmin/ and */guest/ are the default Sign-In-Policies in Pulse Policy Secure. A Sign-In Policy is mapped with a default Authentication Realm.

To configure sign-in policy for guest:

1. Select Authentication > Signing In > Sign-in Policies to display the sign-in policies configuration page.

   Figure 3: Guest Sign-In Policies

2. Create a sign-in policy specifically for the guest user administrator.
3. The realm selected is the guest realm created previously.
You can make necessary changes or add realms in a Sign-in Policy and click **Save Changes** to save the settings.
Configuring a Guest Admin Realm

The ‘Guest Admin’ and ‘Guest’ are the default user realms in Pulse Policy Secure. A user realm is mapped with a default role.

**Note:** For a Guest Admin realm, Administrator has to create the role mapping rule for the user name who has rights for creating Guest accounts.

To configure a guest admin realm:

1. Select Users > User Realms.

*Figure 5: User Authentication Realm*

2. Click on a User Authentication Realm to view the settings.

*Figure 6 shows the New Authentication Realm.*
3. You can make necessary changes and click **Save Changes** to save the settings.
Configuring User Roles for Guest User Account Manager

The ‘Guest Admin’ and ‘Guest’ are the default user roles in Pulse Policy Secure. A user realm is mapped with a default role. To configure a user role for guest user account manager:

1. Select Users > User Roles.

   ![Figure 7: User Roles for Guest User Account Manager](image)

2. Click on a default user role to view the settings.

   ![Figure 8: Default User Role Settings](image)

3. You can make necessary changes and click **Save Changes** to save the settings.
Configuring Location group for Guest Access

The ‘Guest’ is the default location group configured in Pulse Policy Secure. A location group is mapped with a default sign-in policy and a default realm.

To view a Location Group:

1. Select **Endpoint Policy > Network Access > Location Group**.

   *Figure 9: Location Group for Guest Access*

2. Click ‘Guest’ as the default location group to view the settings.

   *Figure 10: Default Location Group*

3. You can make necessary changes and click **Save Changes** to the settings.
Configuring Guest Authentication Server

The ‘Guest Authentication’ is the default Authentication Server configured in Pulse Policy Secure. To configure the authentication server:

1. Select **Authentication > Auth. Servers**.

*Figure 11: Guest Authentication Server*

2. Click the default Authentication Server to view the settings.
3. Enter the configuration settings as described in Table 1.

*Figure 12 shows the default guest authentication server page.*
4. You can make necessary changes and click **Save Changes** to save the settings.
Table 1: Guest Authentication Server Configuration Settings

<table>
<thead>
<tr>
<th>Settings</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Guest User Account Managers</td>
<td>Select this option to allow guest user account managers (GUAM) to create guest user accounts on the local authentication server</td>
</tr>
<tr>
<td>Guest User Name Prefix</td>
<td>Specify the prefix to be used in auto generated guest usernames. It is recommended to retain the default guest_ so that you can rely on the naming convention in your role mapping rules.</td>
</tr>
<tr>
<td>Guest User Info Fields</td>
<td>(Optional) Add line items to represent fields that you want to appear on the configuration page for creating guest user accounts. For example, you can create fields for Company Name, Host Person, Meal Preference, and so on.</td>
</tr>
<tr>
<td>Instructions for Guest User Account Manager</td>
<td>(Optional) Add instructions to the GUAM that appear on the GUAM sign-in page. You can use the following HTML tags to format the text: &lt;b&gt;, &lt;br&gt;, &lt;font&gt;, &lt;noscript&gt;, and &lt;a href&gt;</td>
</tr>
<tr>
<td>Maximum Account Validity Period</td>
<td>Specify the number of hours the account is valid. The default is 24 hours.</td>
</tr>
</tbody>
</table>
Configuring RADIUS Client on Pulse Policy Secure

The Radius Framework on Pulse Policy Secure is configured with the default settings. You have to configure only the Radius client and a RADIUS Return Attributes Policy.

To configure RADIUS Client on Pulse Policy Secure:

1. Select **Endpoint Policy > Network Access > RADIUS Client > New RADIUS Client** to create a new RADIUS client.
   
   The New RADIUS Client screen appears.

   *Figure 13: Creating and Configuring New RADIUS Client – Ruckus WLC*

2. Configure the Ruckus WLC as RADIUS client and map with the default Location Group.
3. Select **Ruckus Wireless** as Make/Model and **Guest** as Location Group.
4. Note that Ruckus Request Password needs to be configured only for SmartZone Guest Access.
5. Click **Save Changes** to save the settings.
6. To create a new RADIUS Return Attribute policy navigate to **Endpoint Policy > Network Access > RADIUS Attributes > Return Attributes > New Policy**.

   The New RADIUS Return Attribute Policy screen appears.
7. Make necessary changes and click **Save Changes** to save the settings.
Configuring SMTP and SMS gateway settings on Pulse Policy Secure

The SMTP and SMS configuration settings must be configured to enable guest users to create user accounts on their own.

SMTP Settings for Guest User Accounts

1. On Pulse Policy Secure main page select **System > Configuration > Guest Access > SMTP Settings**.

   The SMTP Settings screen appears.

   *Figure 15: SMTP Settings*

2. Make necessary changes and click save changes to save the settings.
SMS Gateway Settings for Guest User Accounts

Short Message Service (SMS) is delivered through an SMS gateway service that supports HTTP, HTTPS, and SMTP (Simple Mail Transport Protocol) delivery. You need to subscribe to an external service to be able to deliver guest details using SMS. The SMS gateway sends SMS in formatted text message using HTTP/HTTPS interface (SMS message) and can also allow email message to be sent as an SMS. An example of an SMS gateway is clickatell.com. You should have a valid account with this third party.

To create an account with Clickatell:

1. Go to http://www.clickatell.com/products/sms_gateway.php, and choose the appropriate API sub-product (connection method) you wish to use.
2. Click on the registration hyperlink.
3. Select the Account type you would like to use (Local or International).
4. Enter your personal information to complete the registration form.
5. Accept the Terms & Conditions.
6. Click Continue - An email containing your login details such as account login name, password, and clientID will be sent to the email address you have provided.
7. Activate your account – When user has logged in, and user will be on the Clickatell Central landing page and HTTP API will be added to the account and client API ID will be issued to the account. A single account may have multiple API IDs associated with it.

To enable the SMS gateway settings using Pulse Policy Secure:


The SMS Gateway Settings screen appears.
2. Select the **Enable SMS Gateway Settings** check box.
3. Complete the configuration settings as described in Table 2.
4. Click **Save Changes**.
5. Click **Send Test SMS**.
Table 2: Guest Access SMS Gateway Settings Configuration

<table>
<thead>
<tr>
<th>Settings</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS Gateway Settings</td>
<td>Select the gateway type:</td>
</tr>
<tr>
<td>SMS Gateway Type</td>
<td>Clickatell – Select this option to send SMS as a text message.</td>
</tr>
<tr>
<td></td>
<td>Clickatell Email2SMS – Select this option to use email format as</td>
</tr>
<tr>
<td>API product ID</td>
<td>Specify the API product ID that you received from Clickatell during account creation.</td>
</tr>
<tr>
<td>SMS Gateway Login Name</td>
<td>Specify the SMS gateway login name.</td>
</tr>
<tr>
<td>SMS Gateway Login password</td>
<td>Specify the SMS gateway login password.</td>
</tr>
<tr>
<td>Text Message (SMS) Format</td>
<td>(Optional) Select the following fields:</td>
</tr>
<tr>
<td>Guest Account Start Time</td>
<td></td>
</tr>
<tr>
<td>Guest Account End Time</td>
<td></td>
</tr>
<tr>
<td>Guest Account Sign-in URL</td>
<td></td>
</tr>
<tr>
<td>The following options apply if you select Clickatell as gateway type.</td>
<td></td>
</tr>
<tr>
<td>SMS Gateway URL</td>
<td>Specify the SMS Gateway URL.</td>
</tr>
<tr>
<td></td>
<td>(Default) <a href="https://api.clickatell.com">https://api.clickatell.com</a> or <a href="http://api.clickatell.com">http://api.clickatell.com</a></td>
</tr>
<tr>
<td>HTTPS</td>
<td>Select this option to use a secure connection. If you don't select this option user will be notified about clear text transmission of guest user credentials.</td>
</tr>
<tr>
<td>Use Proxy Server</td>
<td>Select this option to access the internet or SMS gateway URL using a proxy server.</td>
</tr>
<tr>
<td>Address</td>
<td>Specify the address of the proxy server and its port.</td>
</tr>
<tr>
<td>Username</td>
<td>Specify the username of the proxy server.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify the password of the proxy server.</td>
</tr>
<tr>
<td>Send Test SMS</td>
<td></td>
</tr>
<tr>
<td>Mobile Number</td>
<td>Select the country name and then specify a valid phone number of the guest user. The phone number should not include country code or any special character such as +,*, and so on.</td>
</tr>
<tr>
<td>Source Mobile Number</td>
<td>Specify the sender ID configured in Clickatell Account.</td>
</tr>
</tbody>
</table>
Configuring Guest Access Settings on Pulse Policy Secure

2. Under Guest Access Configurations, Select the check box Enable Guest User Account Managers to administer Guest Accounts.
3. Under the Guest Self-Registration select Send guest user credentials via SMS/E-mail.
4. Click the SMS/E-mail settings link and make necessary changes.
5. Show credentials on screen after guest completes registration.
6. Maximum Account Validity Period for Self-Registered Guest – 24 hours is the default time period. You can change this as per the requirement.

Figure 17: Guest Access configuration

8. Select the sign-in policy that is created earlier. Under Configure Guest settings select the check boxes:
   - Use this sign-in policy for Guest and Guest admin to use specific pages.
   - Show Guest Self Registration link on the guest login page, The Register as Guest link appears on the guest login page.

**Enabling Onboarding Feature**

Enterprise onboarding feature provides automated onboarding of BYOD clients on premises (WLAN & LAN).

Pulse Policy Secure enables personal devices to be automatically configured for corporate access.

1. To enable this option in the Pulse Policy secure main page select **Authentication > Signing In > Sign-in Policies**.

   The Sign-in Policies tab displays the available sign-in policies.

2. Under the User URLs section select the default sign-in policy.

   The Sign-in Policy configuration screen appears.
3. Select the Show On-Boarding link on guest login page check box. A drop-down list appears next to it.
4. Select a required URL.
5. Click Save Changes to save the settings.

When this settings is done the Employees can onboard their device here appearing in an enterprise guest environment as shown in the Figure 20.

Figure 20: Onboarding Link Displayed in Guest Environment on Pulse Policy Secure Login Page
Guest-Self Registration Configuration

To enable Guest Self-Registration:

1. Navigate to Signing In > Sign-in Policies > User URLs.
2. Configure guest settings.
3. Send guest user credentials via SMS or Email.
4. Show credentials on screen after guest completes registration.

Figure 21: Guest-Self Registration Configuration

5. Enter name and make necessary changes.
6. Click Register.
Configuring Ruckus WLC with Pulse Policy Secure

Ruckus WLC is configured as Radius Client where Pulse Policy Secure is the Radius Server. Figure 22 illustrates the workflow of Guest Access on Pulse Policy Secure for Ruckus WLC.

Figure 22: Guest Access on Pulse Policy Secure for Ruckus WLC

To configure Ruckus WLC with Pulse Policy Secure:

1. Connect user/endpoint to the Ruckus Wireless network with open SSID over 802.1X with restricted access through ACLs.

2. Redirect Ruckus WLC guest to external (Pulse Policy Secure) captive portal when guest tries to access a web-resource.
3. Enter credentials on captive portal page.

4. For guest access authentication, Pulse Policy Secure provides guest user credentials to Ruckus SmartZone WLC’s management interface via REST API.

5. Ruckus WLC can encode the credentials and send it to a RADIUS server (Pulse Policy Secure) through Radius Access Request.

6. The RADIUS server validates the credentials and sends a RADIUS response, which contains standard RADIUS attributes and Vendor Specific Attributes.

7. Ruckus WLC provides network access to the guest by changing VLAN based on Pulse Policy Secure role-based policy.

Ruckus SmartZone WLC Configuration

The Ruckus SmartZone software platform provides unified software architecture across wireless LAN (WLAN) controllers, for appliance, virtualized and cloud environments for deployment flexibility.

To configure SmartZone WLC:

1. Make sure Access Points and WLC communication are working fine.
2. Configure PPS as Radius Server.
3. Go to Configuration > AP Zone > Zone Name > AAA servers > Create New.
4. Configure Name, IP Address, Shared Secret and Confirm Secret.

Figure 23: SmartZone WLC Configuration

To configure Hotspot (WISPr) service:
1. Go to Configuration > AP Zone > Zone Name > Hotspot (WISPr) > Create New.

Figure 24: SmartZone Hotspot Service

2. Configure Portal Name, Login URL text box with https://pps-ip/guest.

3. Configure Northbound Interface password as Ruckus Request Password on Radius Client page in Pulse Policy Secure.

Figure 25: Northbound Portal Interface – Ruckus SmartZone

To configure WLAN:
1. Go to Configuration > AP Zone > Zone Name > WLAN > Create New.
2. Configure Name, SSID, Authentication type as “Hotspot (WIPSr)”, Authentication Method as “open” and Encryption as “None”.
3. Select Hotspot configured from drop down list and select Authentication Server.

*Figure 26: SmartZone WLAN*
Ruckus ZoneDirector WLC Configuration

The following steps give configuration of Ruckus ZoneDirector WLC:

1. Make sure the Access Points and WLC communication are working fine.
2. Configure PPS as Radius Sever.
3. Go to Configuration > AP Zone > Zone Name > AAA servers > Create New.
4. Enter Name, select “Type” as “Radius”, IP Address, Shared Secret and Confirm Secret.

Figure 27: ZoneDirector WLC Configuration

To configure Hotspot (WISPr) service:

1. Go to Configuration > AP Zone > Zone Name > Hotspot Services > Create New.
2. Configure Name, Login page text box with https://pps-ip/guest.
3. Select authentication server configured in AAA servers.
Figure 28: ZoneDirector Hotspot Services

To configure WLAN:

1. Go to Configuration > AP Zone > Zone Name > WLAN > Create New.
2. Enter the Name, SSID, Authentication type as “Hotspot (WIPSr)”, Authentication method as “Open” and Encryption as “None”.
3. Select Hotspot services as “Guest PS” from drop down list.

Figure 29: ZoneDirector WLAN

4. Click OK to save changes to the settings.
Configuring Pulse Policy Secure for Dot1x Authentication

This section describes Pulse Policy Secure configuration required for dot1x authentication. It includes the following default configuration settings:

- Configuring User Role for Dot1x Authentication
- Configuring User Realm for Dot1x
- Configuring Sign-In Policy for Dot1x
- Configuring Location group for Dot1x
- Configuring Authentication Protocol Set for Dot1x

Configuring User Role for Dot1x Authentication

Pulse Policy Secure access management framework evaluates authentication requests to match endpoints to roles. You must configure user roles for the various types of endpoints authenticated by the MAC address authentication framework.

To create a user role:

1. Select Users > User Role to navigate to the role configuration page.
2. Click New Role to display the configuration page shown in Figure 30.
3. Complete the configuration for general options.
4. Save the configuration.

Figure 30: User Roles for Dot1x Authentication

Configuring User Realm for Dot1x

The user realm configuration associates the MDM server data with user roles.

To configure the realm and role mapping rules:
1. Select **Users > User Realms > New User Realm** to display the configuration page shown in Figure 31.

2. Make necessary changes and save the configuration.

   **Figure 31: User Realm for Dot1x Authentication**

![Image of User Realm configuration page]

### Configuring a Sign-In Policy for Dot1x

A sign-in policy associates devices with a realm.

To configure a sign-in policy:

1. Select **Authentication > Signing In > Sign-In Policies** to navigate to the sign-in policies configuration page.
2. Click **New URL** to display the configuration page shown in Figure 32.
3. Make necessary changes and save the configuration.
Figure 32: Sign-In Policy for Dot1x Authentication

Configuring Location Group for Dot1x

To configure Policy Secure 802.1x framework for non-suppliant endpoints, you must configure Location Group.

1. Select **Endpoint Policy > Network Access > Location Group**.
2. Complete the configuration as shown in Figure 33.
3. Save the configuration.

Figure 33: Location Group for Dot1x Authentication
Configuring Authentication Protocol Set for Dot1x

Switches from various vendors may use the Standard Password Authentication Protocol (PAP), CHAP, or EAP-MD5 protocols for MAC authentication. These protocols are not included in the default authentication protocol set for 802.1x deployments.

To add PAP, CHAP, and EAP-MD5 to the 802.1x protocol set:

1. Log into Policy Secure Web administrator interface.
2. Select Authentication > Signing In > AuthenticationProtocols Sets to display the Authentication Protocol Sets page.

Figure 34: Authentication Protocol Set

3. Click the 802.1x link to edit the 802.1x authentication protocol set configuration.
4. Use the selector buttons to add PAP, CHAP, and EAP-MD5-Challenge to the 802.1x authentication protocol set.

Configuring RADIUS Client

To configure a Radius Client:

2. Enter the Name, IP Address, Shared Secret and Make model as Ruckus Wireless. 

Figure 36: Ruckus SmartZone

3. Here Ruckus Request password should be the same which is configured in “NorthBound Polar Interface” of SmartZone WLC and select default location group.
Ruckus WLC Dot1x Configuration

To configure Ruckus WLC - SmartZone for dot1x:

1. Navigate to **Configuration > Service Profiles > Authentication Service**.
2. Enter the Name, IP Address, shared secret and confirm secret.

**Figure 37: Ruckus WLC Configuration - SmartZone**

3. Map the configured radius server on both realms “No Match” and “Unspecified”.
4. To view the Accounting Services go to Configuration > Service profiles > Accounting.

5. Enter the Name, IP Address, shared secret and confirm secret.

---

**Figure 38: Authentication Profile - Ruckus SmartZone**

![Authentication Profile - Ruckus SmartZone](image1)

**Figure 39: Accounting Services - Ruckus SmartZone**

![Accounting Services - Ruckus SmartZone](image2)
6. Map the configured radius server on both realms “No Match” and “Unspecified”.

**Figure 40: Accounting Profile - Ruckus SmartZone**

To configure AP Zones:

7. Go to **Configuration > AP Zones > Zone Name**.

8. Create New WLAN.
9. Enter the Name, SSID, Authentication Type as “Standard Usage”, Authentication Options as 802.1x EAP.

10. Under Encryption options select Method as WPA2, and Algorithm as AES.

---

Figure 41: Ruckus SmartZone AP Zones - WLAN

Figure 42: Authentication and Accounting Service – Ruckus SmartZone
To configure Authentication Server in Ruckus ZoneDirector:

1. Navigate to **Configure > AAA servers**.
2. Enter the Name, Type, IP address, shared secret and confirm secret.

*Figure 43: Authentication Server – Ruckus ZoneDirector*
To configure Accounting Server in Ruckus ZoneDirector:

1. Navigate to **Configure > Accounting server**.
2. Enter the Name, Type, IP address, shared secret and confirm secret.

Figure 44: Accounting Server – Ruckus ZoneDirector

3. Click **OK** to save the changes to the settings.
1. To configure WLAN, enter the Name and SSID.
2. Select Authentication Type as “Standard Usage”, and Authentication Option as 802.1x EAP.
3. Under Encryption options select Method as WPA2, Algorithm as AES, and advanced options as “Accounting Server”.

Figure 45: Ruckus ZoneDirector - WLAN

4. Save changes to the settings.