Pulse Policy Secure

Ruckus WLC Guest Access Integration – SmartZone and ZoneDirector

Solution Guide

Document Version	**2.0**
Published	**December 2018**

Pulse Secure, LLC
2700 Zanker Road, Suite 200
San Jose, CA 95134
www.pulsesecure.net

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

BYOD Enablement and Guest Access with Ruckus WLC – SmartZone and ZoneDirector

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at www.pulsesecure.net. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.”

Ruckus Wireless, Ruckus Wireless SmartZone, Ruckus Wireless ZoneDirector, and Ruckus Wireless Logo are trademarks of Ruckus Wireless, Inc. For additional information on Ruckus Wireless products, visit www.ruckuswireless.com

© 2018 by Pulse Secure, LLC. All rights reserved

Table of Contents

© 2018 by Pulse Secure, LLC. All rights reserved

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

© 2018 by Pulse Secure, LLC. All rights reserved

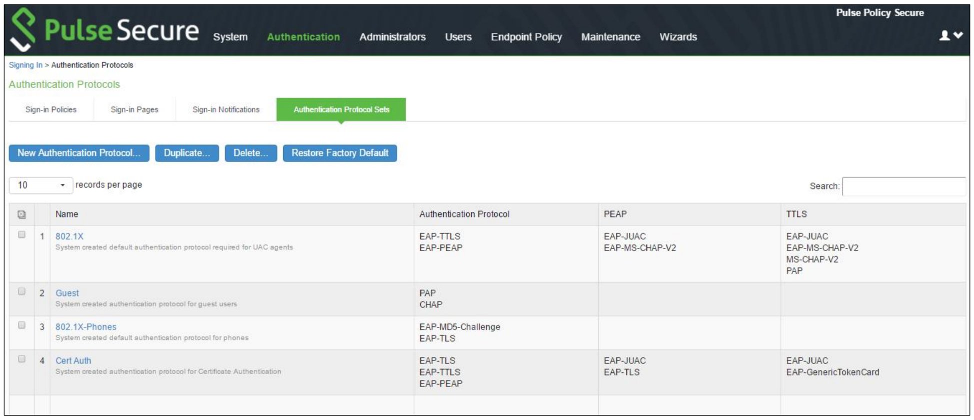
Configuring Authentication Protocol sets for Guest Access

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

To view the Authentication Protocol:

1. Select **Authentication > Signing In > Authentication Protocol Sets**.

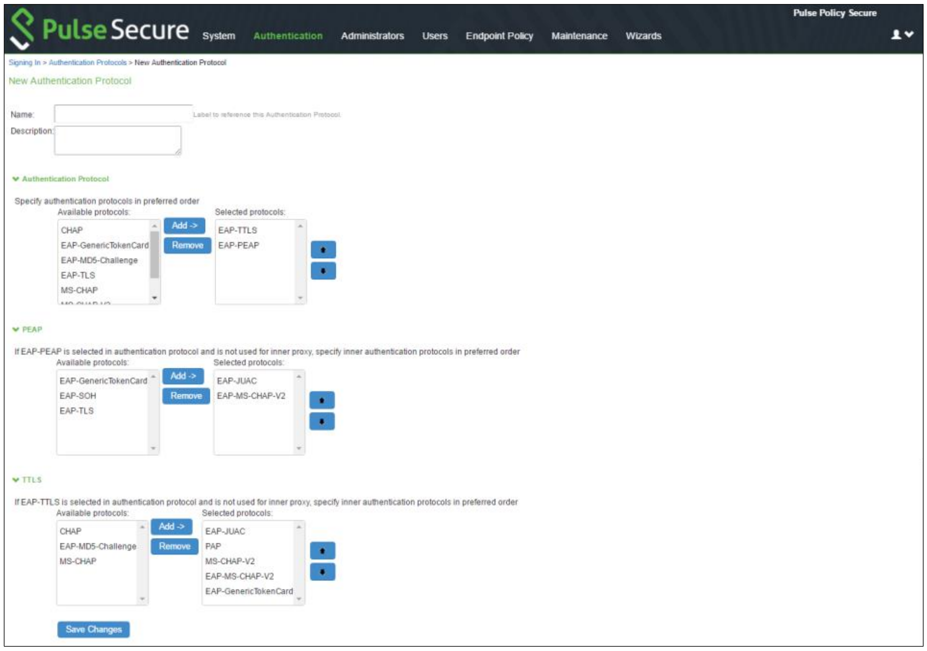
Figure 1: Authentication Protocols for Guest Access



		Name	Authentication Protocol	PEAP	TTLS
□	1	802.1X System created default authentication protocol required for UAC agents	EAP-TTLS EAP-PEAP	EAP-JUAC EAP-MS-CHAP-V2	EAP-JUAC EAP-MS-CHAP-V2 MS-CHAP-V2 PAP
□	2	Guest System created authentication protocol for guest users	PAP CHAP		
□	3	802.1X-Phones System created default authentication protocol for phones	EAP-MD5-Challenge EAP-TLS		
□	4	Cert Auth System created authentication protocol for Certificate Authentication	EAP-TLS EAP-TTLS EAP-PEAP	EAP-JUAC EAP-TLS	EAP-JUAC EAP-GenericTokenCard

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

Figure 2: Default Authentication Protocol Sets



Name: Label to reference this Authentication Protocol
Description:

Authentication Protocol

Specify authentication protocols in preferred order

Available protocols: CHAP, EAP-GenericTokenCard, EAP-MD5-Challenge, EAP-TLS, MS-CHAP

Selected protocols: EAP-TTLS, EAP-PEAP

PEAP

If EAP-PEAP is selected in authentication protocol and is not used for inner proxy, specify inner authentication protocols in preferred order

Available protocols: EAP-GenericTokenCard, EAP-SOH, EAP-TLS

Selected protocols: EAP-JUAC, EAP-MS-CHAP-V2

TTLS

If EAP-TTLS is selected in authentication protocol and is not used for inner proxy, specify inner authentication protocols in preferred order

Available protocols: CHAP, EAP-MD5-Challenge, MS-CHAP

Selected protocols: EAP-JUAC, PAP, MS-CHAP-V2, EAP-MS-CHAP-V2, EAP-GenericTokenCard

3. You can make necessary changes and click **Save Changes** to save the settings.

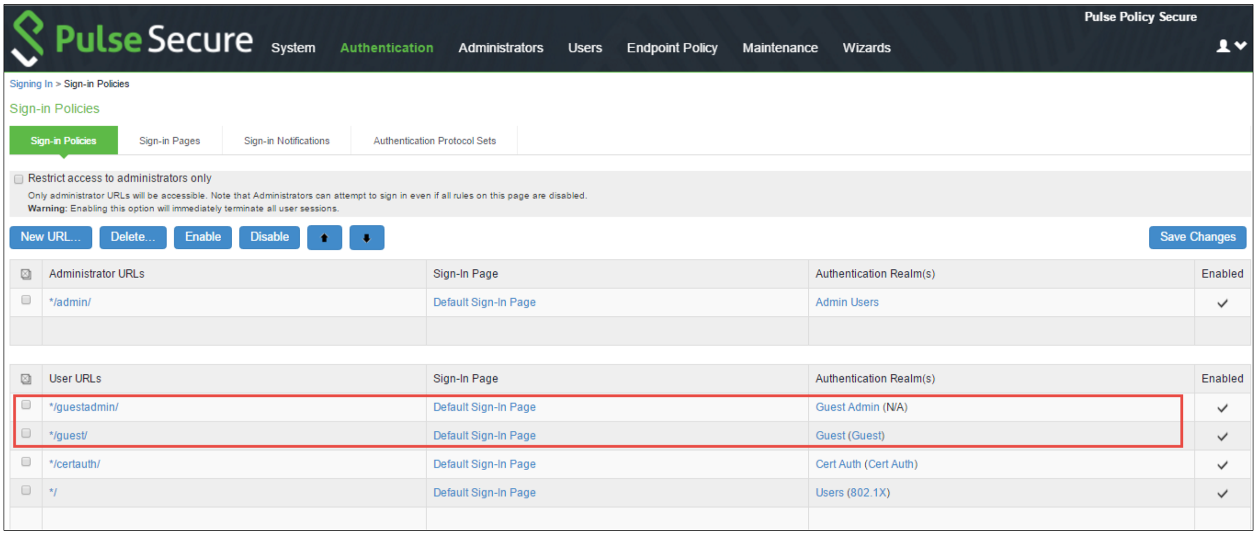
Configuring Guest Sign-In Policies

The */guestadmin/ and */guest/ are the default Sign-In-Polices 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



□ Restrict access to administrators only

Only administrator URLs will be accessible. Note that Administrators can attempt to sign in even if all rules on this page are disabled.
Warning: Enabling this option will immediately terminate all user sessions.

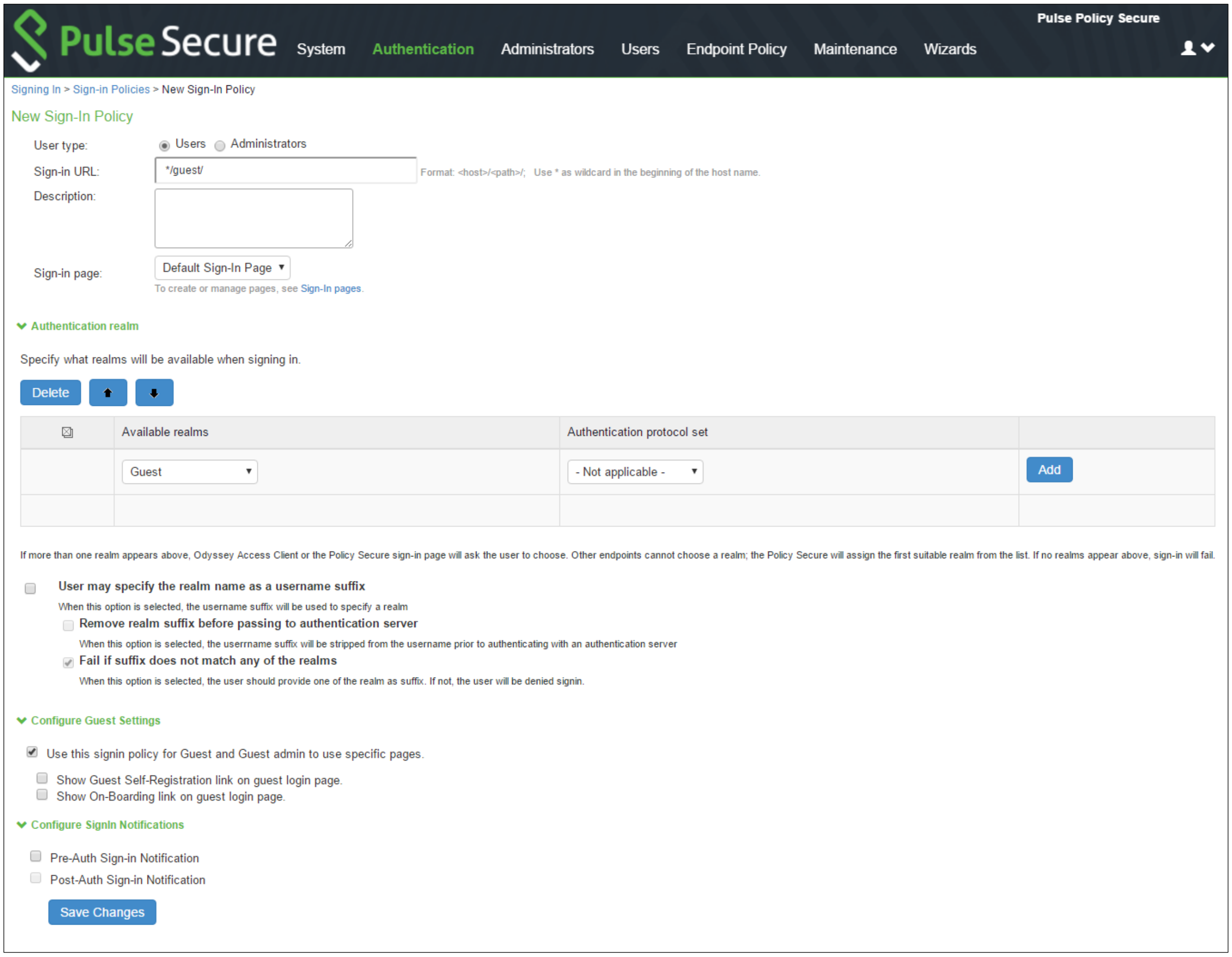
☒	Administrator URLs	Sign-In Page	Authentication Realm(s)	Enabled
□	*/admin/	Default Sign-In Page	Admin Users	✓

☒	User URLs	Sign-In Page	Authentication Realm(s)	Enabled
□	*/guestadmin/	Default Sign-In Page	Guest Admin (N/A)	✓
□	*/guest/	Default Sign-In Page	Guest (Guest)	✓
□	*/certauth/	Default Sign-In Page	Cert Auth (Cert Auth)	✓
□	*/	Default Sign-In Page	Users (802.1X)	✓

2. Create a sign-in policy specifically for the guest user administrator.
3. The realm selected is the guest realm created previously.

© 2018 by Pulse Secure, LLC. All rights reserved

Figure 4: Default Guest Sign-In Policy



Signing In > Sign-in Policies > New Sign-In Policy

New Sign-In Policy

User type: ● Users ○ Administrators

Sign-in URL: */guest/ Format: <host>/<path>/; Use * as wildcard in the beginning of the host name.

Description:

Sign-in page: Default Sign-In Page ▾

To create or manage pages, see Sign-In pages.

Authentication realm

Specify what realms will be available when signing in.

Delete ⬆ ⬇

□	Available realms	Authentication protocol set	
	Guest ▾	- Not applicable - ▾	Add

If more than one realm appears above, Odyssey Access Client or the Policy Secure sign-in page will ask the user to choose. Other endpoints cannot choose a realm; the Policy Secure will assign the first suitable realm from the list. If no realms appear above, sign-in will fail.

□ **User may specify the realm name as a username suffix**

When this option is selected, the username suffix will be used to specify a realm

□ **Remove realm suffix before passing to authentication server**

When this option is selected, the userrname suffix will be stripped from the username prior to authenticating with an authentication server

☑ **Fail if suffix does not match any of the realms**

When this option is selected, the user should provide one of the realm as suffix. If not, the user will be denied signin.

Configure Guest Settings

☑ Use this signin policy for Guest and Guest admin to use specific pages.

□ Show Guest Self-Registration link on guest login page.

□ Show On-Boarding link on guest login page.

Configure SignIn Notifications

□ Pre-Auth Sign-in Notification

□ Post-Auth Sign-in Notification

Save Changes

You can make necessary changes or add realms in a Sign-in Policy and click **Save Changes** to save the settings.

© 2018 by Pulse Secure, LLC. All rights reserved

Configuring a Guest Admin Realm

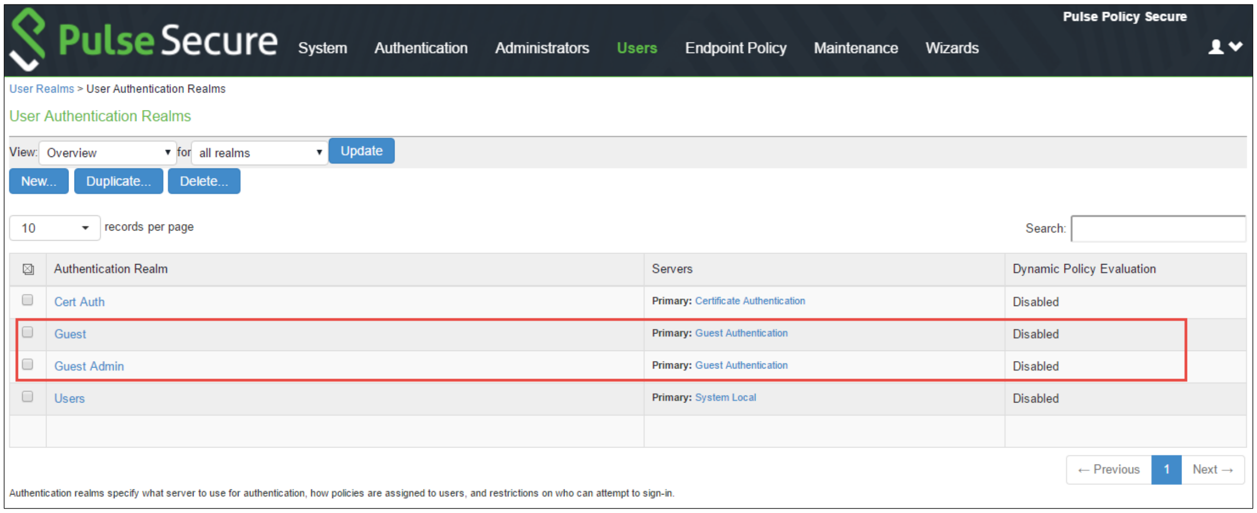
The 'Guest Admin' and 'Guest' are the default user realms in Pulse Policy Secure. A user realm is mapped with a default role.

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



User Realms > User Authentication Realms

User Authentication Realms

	Authentication Realm	Servers	Dynamic Policy Evaluation
□	Cert Auth	Primary: Certificate Authentication	Disabled
□	Guest	Primary: Guest Authentication	Disabled
□	Guest Admin	Primary: Guest Authentication	Disabled
□	Users	Primary: System Local	Disabled

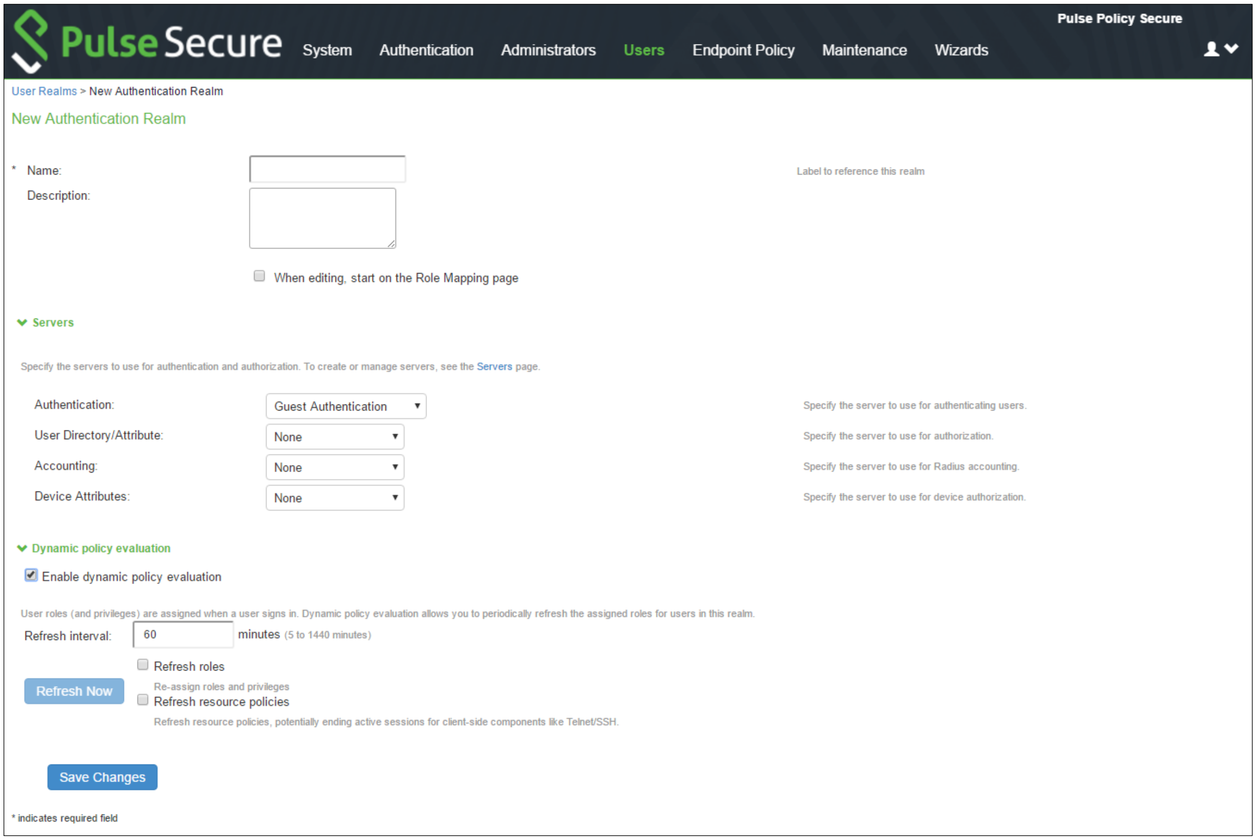
Authentication realms specify what server to use for authentication, how policies are assigned to users, and restrictions on who can attempt to sign-in.

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

Figure 6 shows the New Authentication Realm.

© 2018 by Pulse Secure, LLC. All rights reserved

Figure 6: User Realm - Role Mapping Page



User Realms > New Authentication Realm

New Authentication Realm

* Name: | Label to reference this realm

Description:

□ When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the Servers page.

Authentication:	Guest Authentication	Specify the server to use for authenticating users.
User Directory/Attribute:	None	Specify the server to use for authorization.
Accounting:	None	Specify the server to use for Radius accounting.
Device Attributes:	None	Specify the server to use for device authorization.

Dynamic policy evaluation

☑ Enable dynamic policy evaluation

User roles (and privileges) are assigned when a user signs in. Dynamic policy evaluation allows you to periodically refresh the assigned roles for users in this realm.

Refresh interval: 60 minutes (5 to 1440 minutes)

□ Refresh roles
Re-assign roles and privileges

Refresh Now

□ Refresh resource policies
Refresh resource policies, potentially ending active sessions for client-side components like Telnet/SSH.

Save Changes

* indicates required field

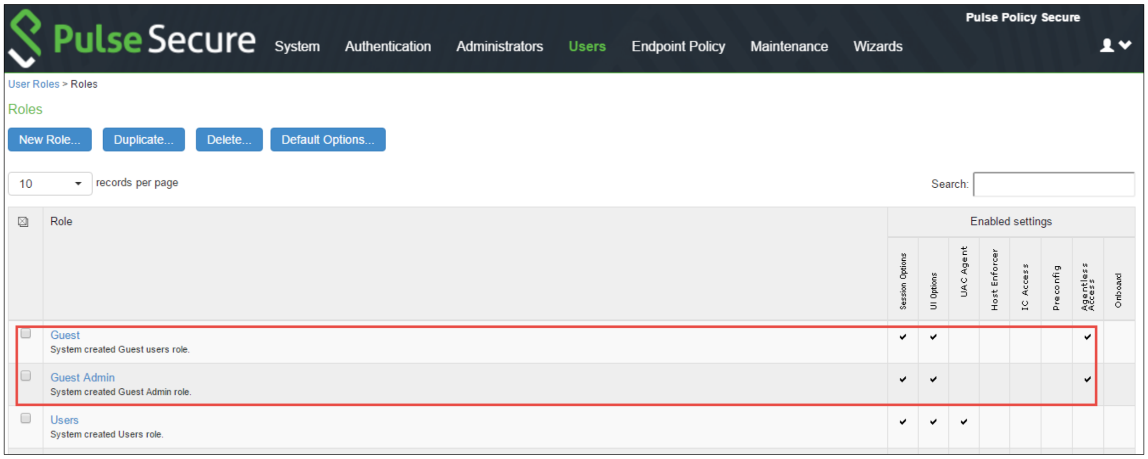
3. You can make necessary changes and click Save Changes to save the settings.

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.

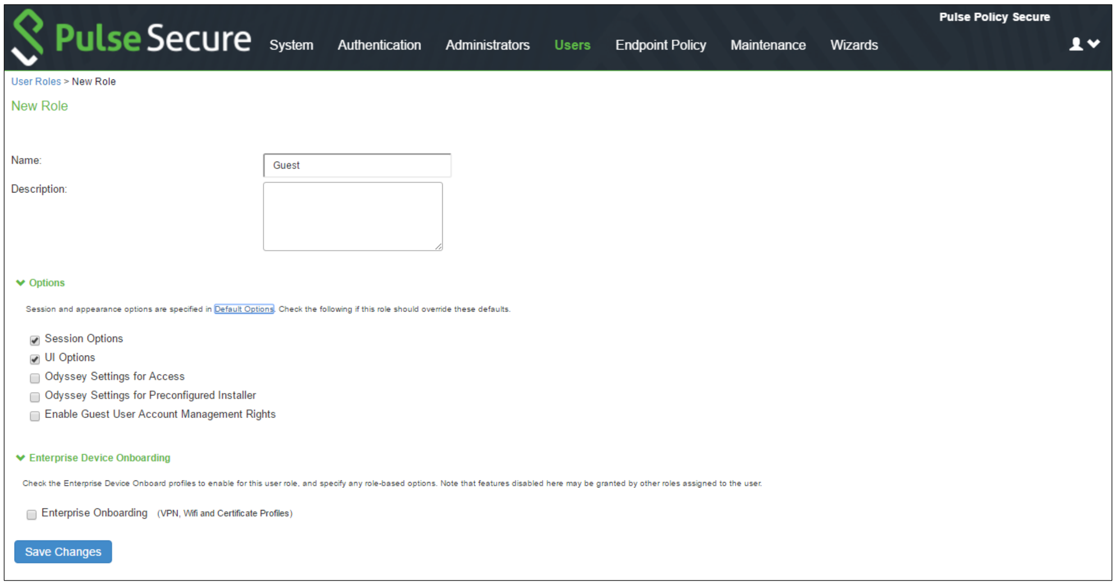
Figure 7: User Roles for Guest User Account Manager



☐	Role	Session Options	UI Options	UAC Agent	Host Enforcer	IC Access	Preconfig	Agentless Access	Onboard
☐	Guest System created Guest users role.	✓	✓					✓	
☐	Guest Admin System created Guest Admin role.	✓	✓					✓	
☐	Users System created Users role.	✓	✓	✓					

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

Figure 8: Default User Role Settings



Name: Guest

Description:

Session and appearance options are specified in Default Options. Check the following if this role should override these defaults.

☑ Session Options
☑ UI Options
☐ Odyssey Settings for Access
☐ Odyssey Settings for Preconfigured Installer
☐ Enable Guest User Account Management Rights

Check the Enterprise Device Onboard profiles to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.

☐ Enterprise Onboarding (VPN, Wifi and Certificate Profiles)

3. You can make necessary changes and click **Save Changes** to save the settings.

© 2018 by Pulse Secure, LLC. All rights reserved

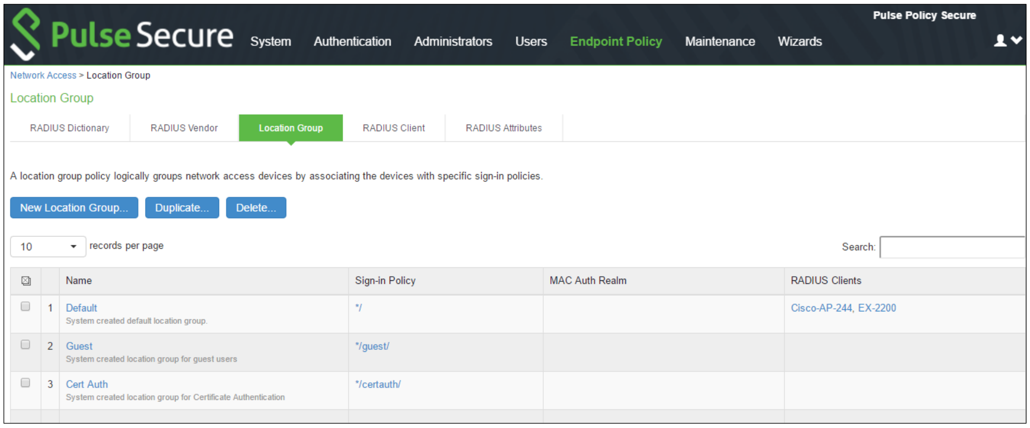
Configuring Location group for Guest Access

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



Network Access > Location Group

Location Group

A location group policy logically groups network access devices by associating the devices with specific sign-in policies.

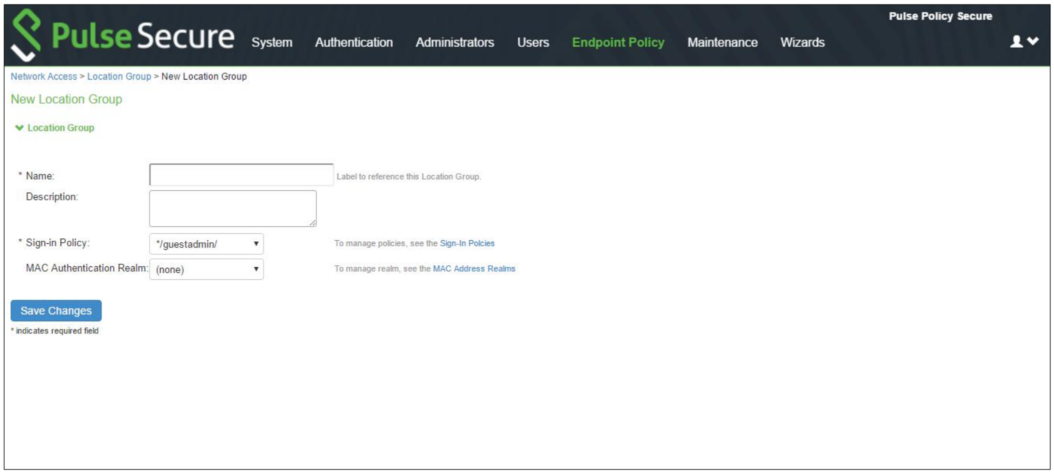
10 records per page

Search:

☒		Name	Sign-in Policy	MAC Auth Realm	RADIUS Clients
□	1	Default System created default location group.	*/		Cisco-AP-244, EX-2200
□	2	Guest System created location group for guest users	*/guest/		
□	3	Cert Auth System created location group for Certificate Authentication	*/certauth/		

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

Figure 10: Default Location Group



Network Access > Location Group > New Location Group

New Location Group

Location Group

* Name: Label to reference this Location Group.

Description:

* Sign-in Policy: */guestadmin/ To manage policies, see the Sign-In Polcies

MAC Authentication Realm: (none) To manage realm, see the MAC Address Realms

* indicates required field

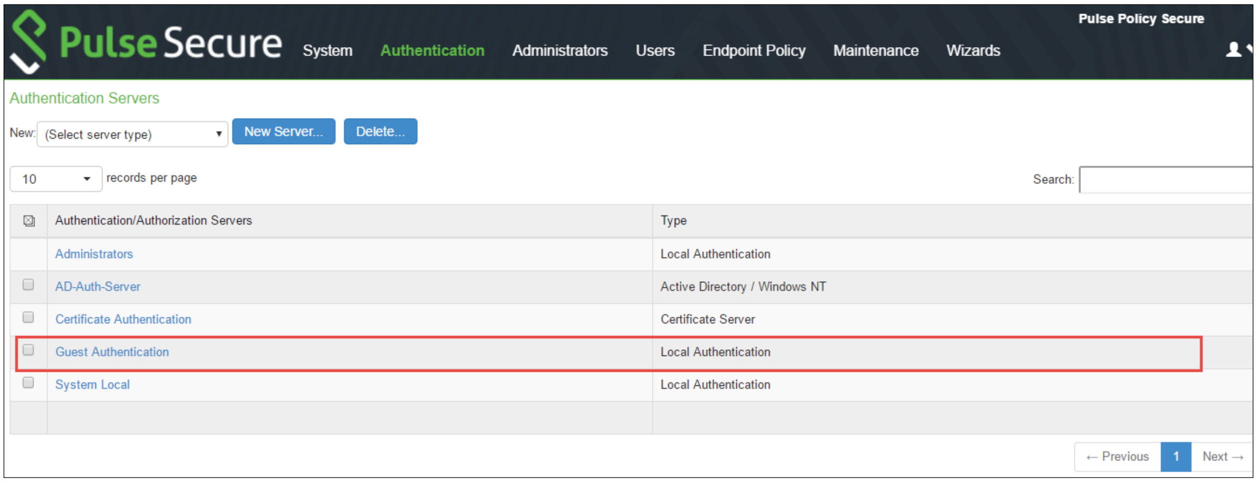
3. You can make necessary changes and click **Save Changes** to the settings.

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



Authentication Servers

New: (Select server type)

10 records per page

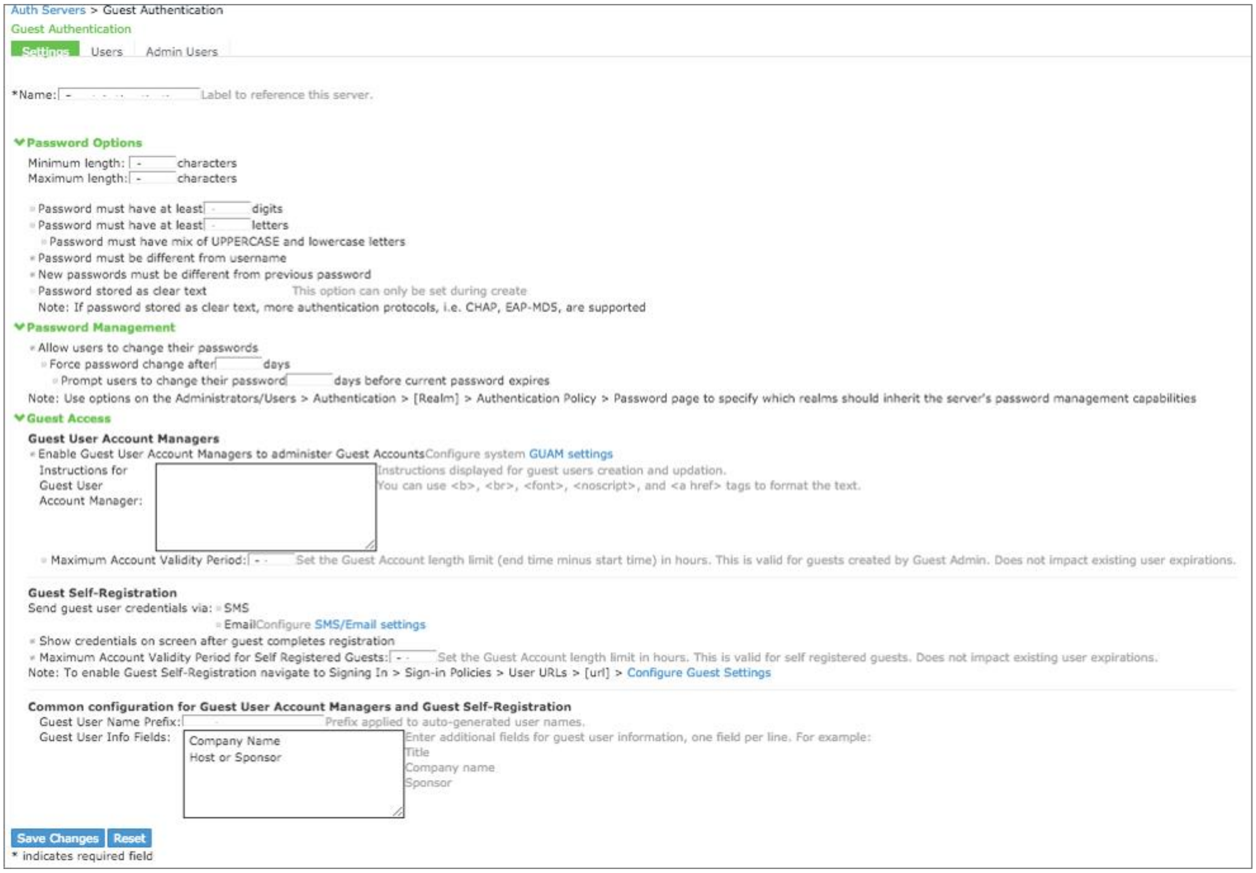
	Authentication/Authorization Servers	Type
	Administrators	Local Authentication
□	AD-Auth-Server	Active Directory / Windows NT
□	Certificate Authentication	Certificate Server
□	Guest Authentication	Local Authentication
□	System Local	Local Authentication

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.

© 2018 by Pulse Secure, LLC. All rights reserved

Figure 12: Guest Authentication Server Settings



Auth Servers > Guest Authentication

Guest Authentication

*Name: Label to reference this server.

Password Options

Minimum length: - characters
Maximum length: - characters

□ Password must have at least - digits
□ Password must have at least - letters
□ Password must have mix of UPPERCASE and lowercase letters
□ Password must be different from username
□ New passwords must be different from previous password
□ Password stored as clear text This option can only be set during create
Note: If password stored as clear text, more authentication protocols, i.e. CHAP, EAP-MD5, are supported

Password Management

□ Allow users to change their passwords
□ Force password change after days
□ Prompt users to change their password days before current password expires
Note: Use options on the Administrators/Users > Authentication > [Realm] > Authentication Policy > Password page to specify which realms should inherit the server's password management capabilities

Guest Access

Guest User Account Managers
□ Enable Guest User Account Managers to administer Guest AccountsConfigure system GUAM settings
Instructions for Guest User Account Manager: Instructions displayed for guest users creation and updation.
You can use <b>, <br>, <font>, <noscript>, and <a href> tags to format the text.

□ Maximum Account Validity Period: - Set the Guest Account length limit (end time minus start time) in hours. This is valid for guests created by Guest Admin. Does not impact existing user expirations.

Guest Self-Registration
Send guest user credentials via: □ SMS
□ EmailConfigure SMS/Email settings
□ Show credentials on screen after guest completes registration
□ Maximum Account Validity Period for Self Registered Guests: - Set the Guest Account length limit in hours. This is valid for self registered guests. Does not impact existing user expirations.
Note: To enable Guest Self-Registration navigate to Signing In > Sign-in Policies > User URLs > [url] > Configure Guest Settings

Common configuration for Guest User Account Managers and Guest Self-Registration
Guest User Name Prefix: Prefix applied to auto-generated user names.
Guest User Info Fields:
Company Name
Host or Sponsor

Enter additional fields for guest user information, one field per line. For example:
Title
Company name
Sponsor

* indicates required field

4. You can make necessary changes and click Save Changes to save the settings.

Table 1: Guest Authentication Server Configuration Settings

Settings	Guidelines
Enable Guest User Account Managers	Select this option to allow guest user account managers (GUAM) to create guest user accounts on the local authentication server
Guest User Name Prefix	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.
Guest User Info Fields	(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.
Instructions for Guest User Account Manager	(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: <b>, , <font>, <noscript>, and <a href>
Maximum Account Validity Period	Specify the number of hours the account is valid. The default is 24 hours.

© 2018 by Pulse Secure, LLC. All rights reserved

Configuring RADIUS Client on Pulse Policy Secure

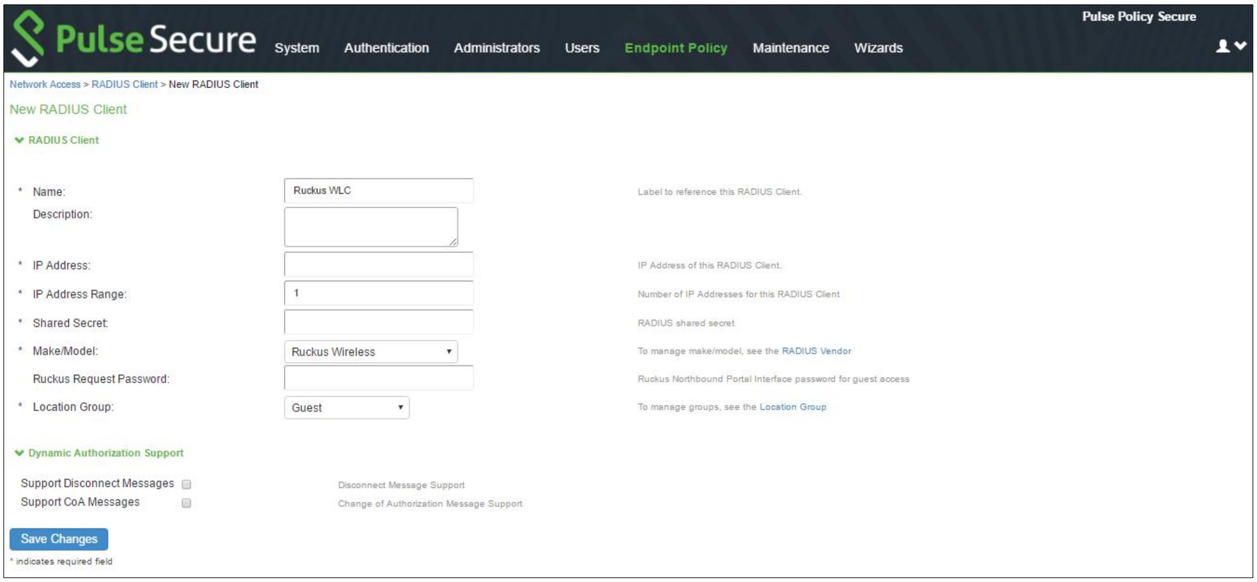
The Radius Framework on Pulse Policy Secure is configured with the default settings. You have to configure only the Radius client and a RADIUS Return Attributes Policy.

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



Network Access > RADIUS Client > New RADIUS Client

New RADIUS Client

RADIUS Client

* Name:	Ruckus WLC	Label to reference this RADIUS Client.
Description:		
* IP Address:		IP Address of this RADIUS Client.
* IP Address Range:	1	Number of IP Addresses for this RADIUS Client
* Shared Secret:		RADIUS shared secret
* Make/Model:	Ruckus Wireless	To manage make/model, see the RADIUS Vendor
Ruckus Request Password:		Ruckus Northbound Portal Interface password for guest access
* Location Group:	Guest	To manage groups, see the Location Group

Dynamic Authorization Support

Support Disconnect Messages	☐	Disconnect Message Support
Support CoA Messages	☐	Change of Authorization Message Support

Save Changes

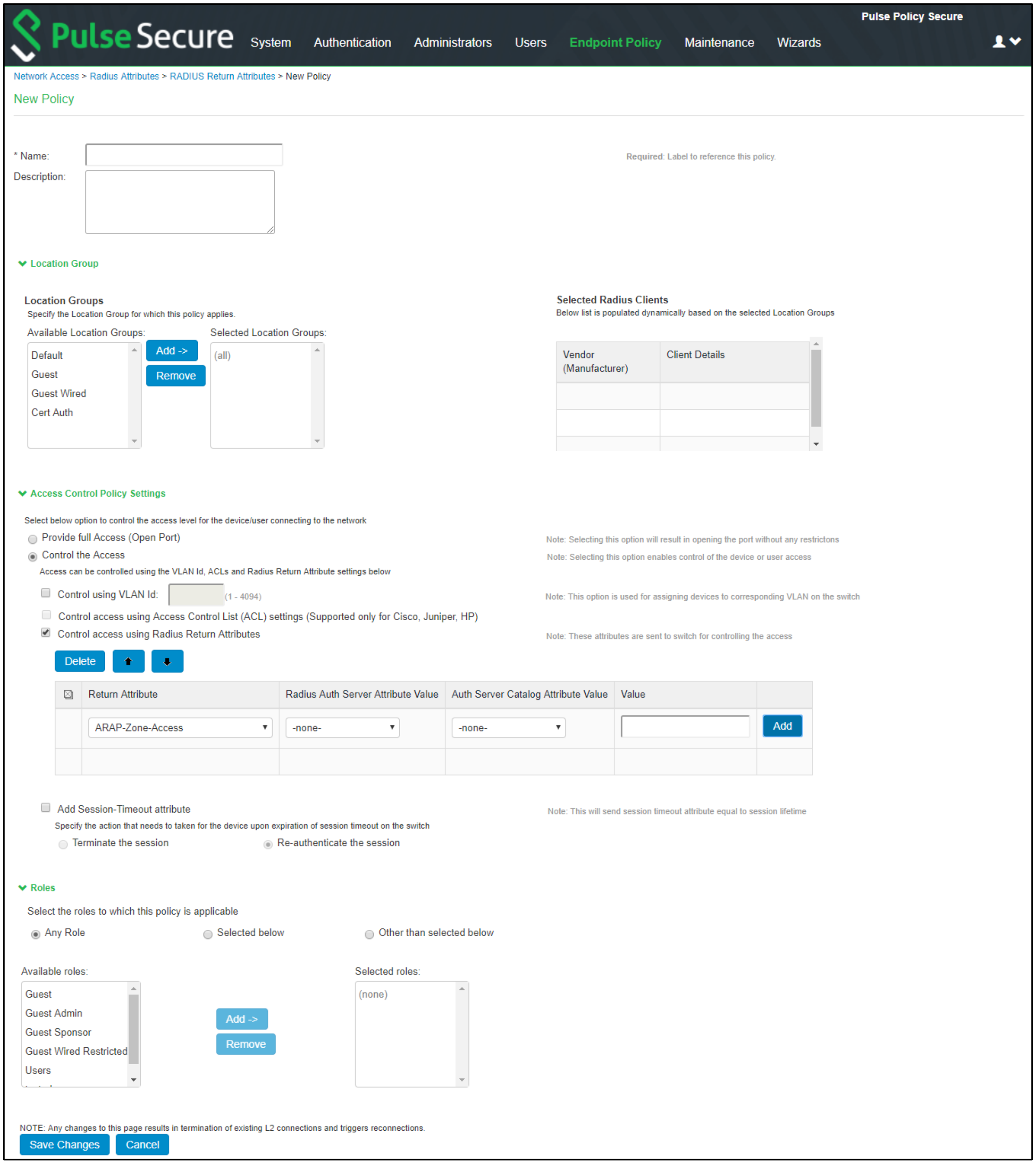
* indicates required field

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.

© 2018 by Pulse Secure, LLC. All rights reserved

Figure 14: New RADIUS Return Attribute Policy



Network Access > Radius Attributes > RADIUS Return Attributes > New Policy

New Policy

* Name:

Required: Label to reference this policy.

Description:

Location Group

Location Groups

Specify the Location Group for which this policy applies.

Available Location Groups: Default, Guest, Guest Wired, Cert Auth

Add -> Remove

Selected Location Groups: (all)

Selected Radius Clients

Below list is populated dynamically based on the selected Location Groups

Vendor (Manufacturer)	Client Details

Access Control Policy Settings

Select below option to control the access level for the device/user connecting to the network

○ Provide full Access (Open Port) — Note: Selecting this option will result in opening the port without any restrictons

● Control the Access — Note: Selecting this option enables control of the device or user access

Access can be controlled using the VLAN Id, ACLs and Radius Return Attribute settings below

☐ Control using VLAN Id: (1 - 4094) — Note: This option is used for assigning devices to corresponding VLAN on the switch

☐ Control access using Access Control List (ACL) settings (Supported only for Cisco, Juniper, HP)

☑ Control access using Radius Return Attributes — Note: These attributes are sent to switch for controlling the access

Delete

☒	Return Attribute	Radius Auth Server Attribute Value	Auth Server Catalog Attribute Value	Value	
	ARAP-Zone-Access	-none-	-none-		Add

☐ Add Session-Timeout attribute — Note: This will send session timeout attribute equal to session lifetime

Specify the action that needs to taken for the device upon expiration of session timeout on the switch

○ Terminate the session ● Re-authenticate the session

Roles

Select the roles to which this policy is applicable

● Any Role ○ Selected below ○ Other than selected below

Available roles: Guest, Guest Admin, Guest Sponsor, Guest Wired Restricted, Users

Add -> Remove

Selected roles: (none)

NOTE: Any changes to this page results in termination of existing L2 connections and triggers reconnections.

Save Changes Cancel

7. Make necessary changes and click **Save Changes** to save the settings.

© 2018 by Pulse Secure, LLC. All rights reserved

Configuring SMTP and SMS gateway settings on Pulse Policy Secure

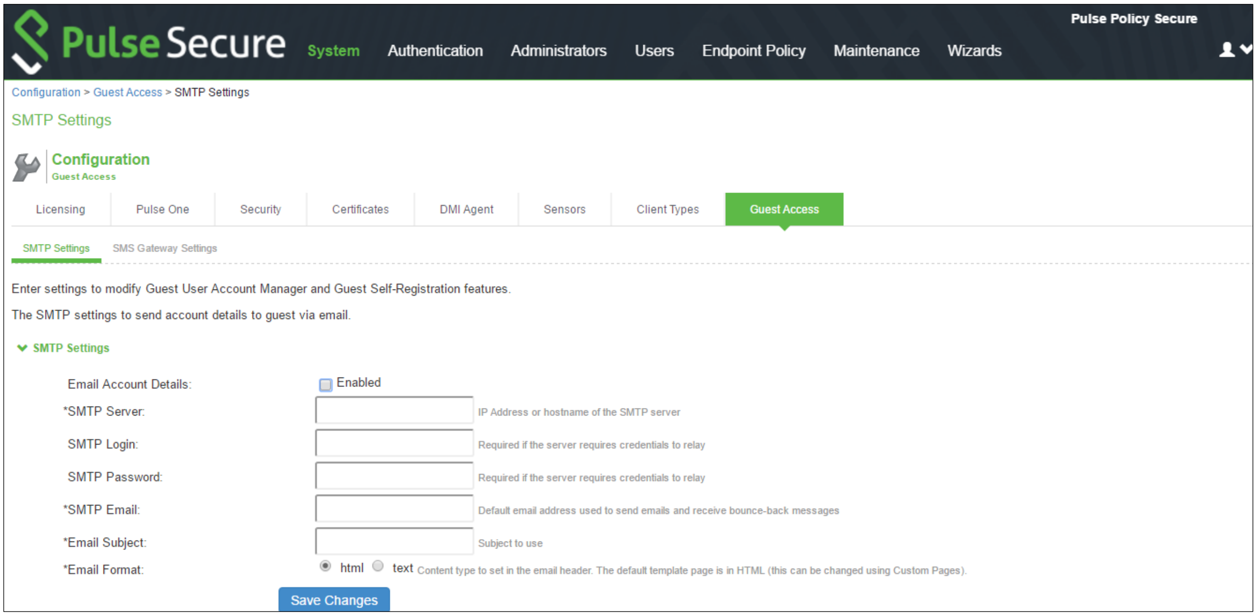
The SMTP and SMS configuration settings must be configured to enable guest users to create user accounts on their own.

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



Enter settings to modify Guest User Account Manager and Guest Self-Registration features.

The SMTP settings to send account details to guest via email.

Email Account Details:	□ Enabled	
*SMTP Server:		IP Address or hostname of the SMTP server
SMTP Login:		Required if the server requires credentials to relay
SMTP Password:		Required if the server requires credentials to relay
*SMTP Email:		Default email address used to send emails and receive bounce-back messages
*Email Subject:		Subject to use
*Email Format:	● html ○ text	Content type to set in the email header. The default template page is in HTML (this can be changed using Custom Pages).

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.

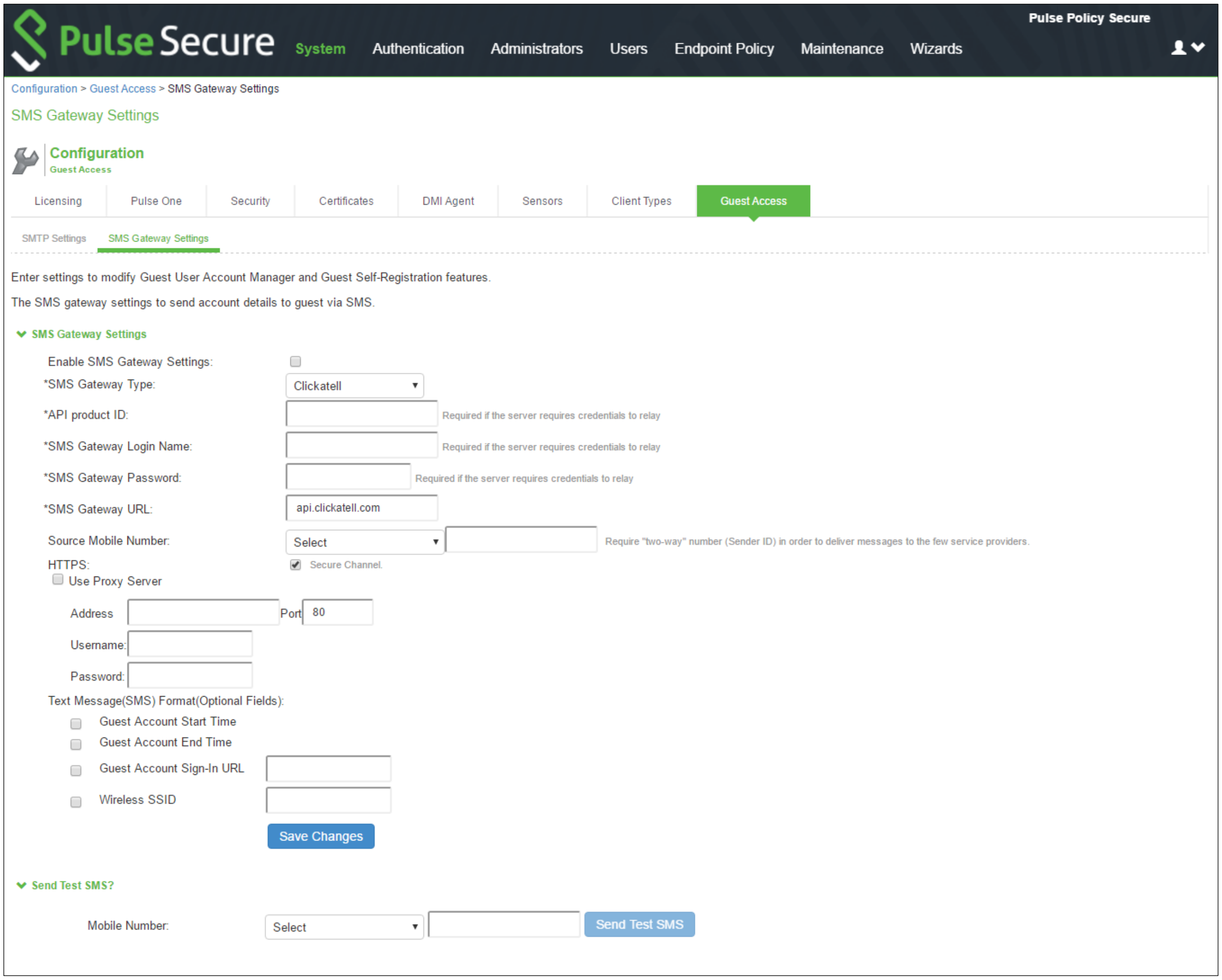
To enable the SMS gateway settings using Pulse Policy Secure:

1. On Pulse Policy Secure main page select System > Configuration > Guest Access > SMS Gateway Settings.

   The SMS Gateway Settings screen appears.

© 2018 by Pulse Secure, LLC. All rights reserved

Figure 16: Guest Access SMS Gateway Settings



SMS Gateway Settings

Enter settings to modify Guest User Account Manager and Guest Self-Registration features.

The SMS gateway settings to send account details to guest via SMS.

SMS Gateway Settings

Enable SMS Gateway Settings: □

*SMS Gateway Type: Clickatell

*API product ID: Required if the server requires credentials to relay

*SMS Gateway Login Name: Required if the server requires credentials to relay

*SMS Gateway Password: Required if the server requires credentials to relay

*SMS Gateway URL: api.clickatell.com

Source Mobile Number: Select Require "two-way" number (Sender ID) in order to deliver messages to the few service providers.

HTTPS: ☑ Secure Channel.

□ Use Proxy Server

Address Port 80

Username:

Password:

Text Message(SMS) Format(Optional Fields):

□ Guest Account Start Time

□ Guest Account End Time

□ Guest Account Sign-In URL

□ Wireless SSID

Send Test SMS?

Mobile Number: Select

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**.

© 2018 by Pulse Secure, LLC. All rights reserved

Table 2: Guest Access SMS Gateway Settings Configuration

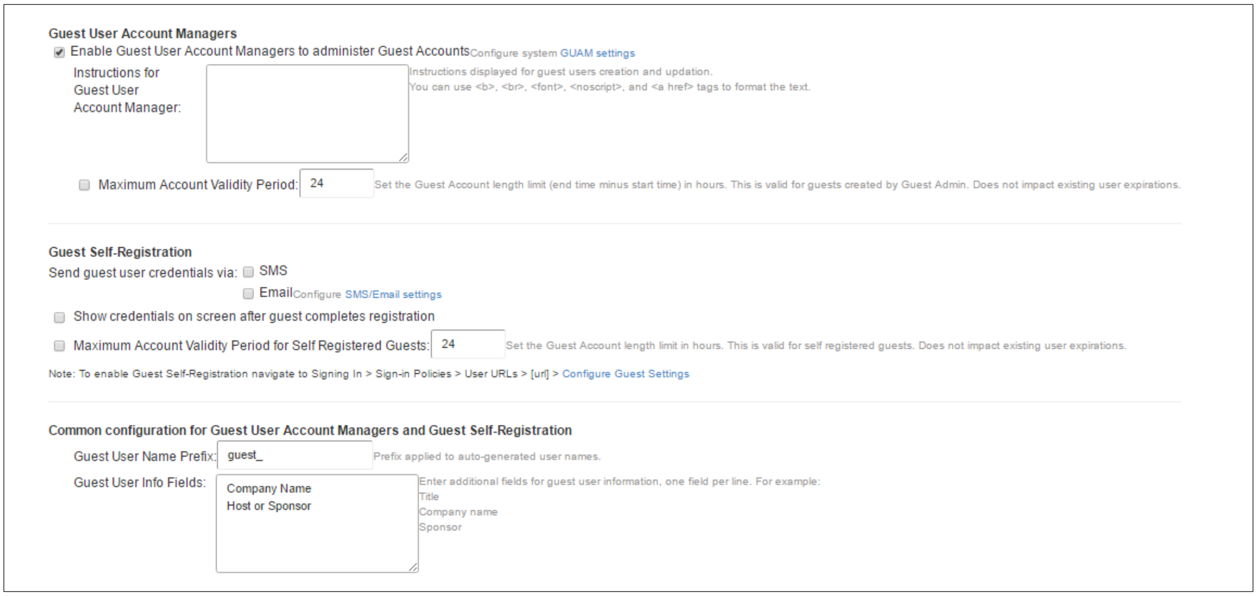
Settings	Guidelines
SMS Gateway Settings	
SMS Gateway Type	Select the gateway type: Clickatell – Select this option to send SMS as a text message. Clickatell Email2SMS – Select this option to use email format as
API product ID	Specify the API product ID that you received from Clickatell during account creation
SMS Gateway Login Name	Specify the SMS gateway login name.
SMS Gateway Login password	Specify the SMS gateway login password.
Text Message (SMS) Format	(Optional) Select the following fields: Guest Account Start Time Guest Account End Time Guest Account Sign-in URL
The following options apply if you select Clickatell as gateway type.	
SMS Gateway URL	Specify the SMS Gateway URL. (Default) https://api.clickatell.com or http://api.clickatell.com
HTTPS	Select this option to use a secure connection. If you don't select this option user will be notified about clear text
Use Proxy Server	Select this option to access the internet or SMS gateway URL using a proxy server.
Address	Specify the address of the proxy server and its port.
Username	Specify the username of the proxy server.
Password	Specify the password of the proxy server.
Send Test SMS	
Mobile Number	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.
Source Mobile Number	Specify the sender ID configured in Clickatell Account

© 2018 by Pulse Secure, LLC. All rights reserved

Configuring Guest Access Settings on Pulse Policy Secure

1. On Pulse Policy Secure main page select Authentication > Auth. Servers > System Local > Settings.
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



Guest User Account Managers

☑ Enable Guest User Account Managers to administer Guest Accounts Configure system GUAM settings

Instructions for Guest User Account Manager: Instructions displayed for guest users creation and updation.
You can use <b>, <br>, <font>, <noscript>, and <a href> tags to format the text.

☐ Maximum Account Validity Period: 24 Set the Guest Account length limit (end time minus start time) in hours. This is valid for guests created by Guest Admin. Does not impact existing user expirations.

Guest Self-Registration

Send guest user credentials via: ☐ SMS
☐ Email Configure SMS/Email settings

☐ Show credentials on screen after guest completes registration

☐ Maximum Account Validity Period for Self Registered Guests: 24 Set the Guest Account length limit in hours. This is valid for self registered guests. Does not impact existing user expirations.

Note: To enable Guest Self-Registration navigate to Signing In > Sign-in Policies > User URLs > [url] > Configure Guest Settings

Common configuration for Guest User Account Managers and Guest Self-Registration

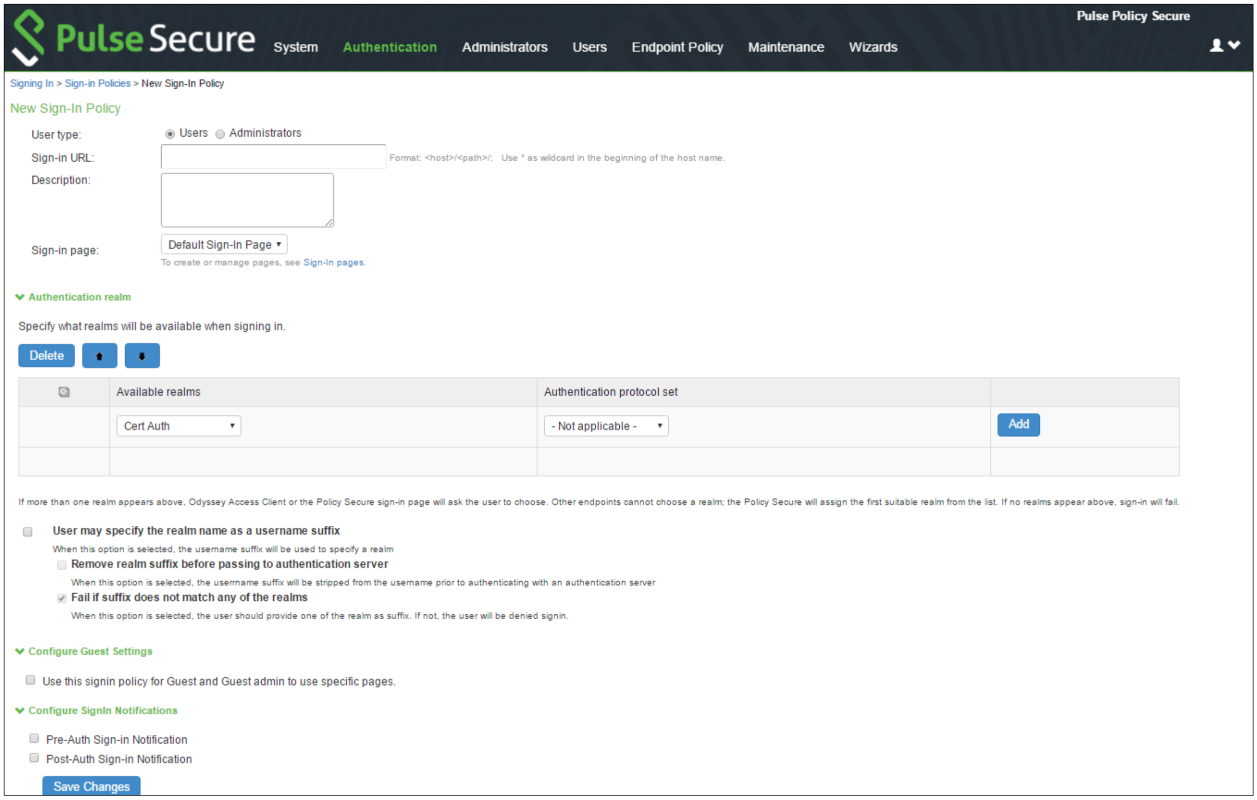
Guest User Name Prefix: guest_ Prefix applied to auto-generated user names.

Guest User Info Fields: Company Name
Host or Sponsor

Enter additional fields for guest user information, one field per line. For example:
Title
Company name
Sponsor

7. On Pulse Policy Secure main page select Authentication >Signing In >Sign-In Policies.

Figure 18: Sign-In Policy



Signing In > Sign-in Policies > New Sign-In Policy

New Sign-In Policy

User type: ● Users ○ Administrators

Sign-in URL: Format: <host>/<path>/;   Use * as wildcard in the beginning of the host name.

Description:

Sign-in page: Default Sign-In Page

To create or manage pages, see Sign-In pages.

Authentication realm

Specify what realms will be available when signing in.

Delete

□	Available realms	Authentication protocol set	
	Cert Auth	- Not applicable -	Add

If more than one realm appears above, Odyssey Access Client or the Policy Secure sign-in page will ask the user to choose. Other endpoints cannot choose a realm; the Policy Secure will assign the first suitable realm from the list. If no realms appear above, sign-in will fail.

□ **User may specify the realm name as a username suffix**

When this option is selected, the username suffix will be used to specify a realm

□ **Remove realm suffix before passing to authentication server**

When this option is selected, the username suffix will be stripped from the username prior to authenticating with an authentication server

☑ **Fail if suffix does not match any of the realms**

When this option is selected, the user should provide one of the realm as suffix. If not, the user will be denied signin.

Configure Guest Settings

□ Use this signin policy for Guest and Guest admin to use specific pages.

Configure SignIn Notifications

□ Pre-Auth Sign-in Notification

□ Post-Auth Sign-in Notification

Save Changes

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.

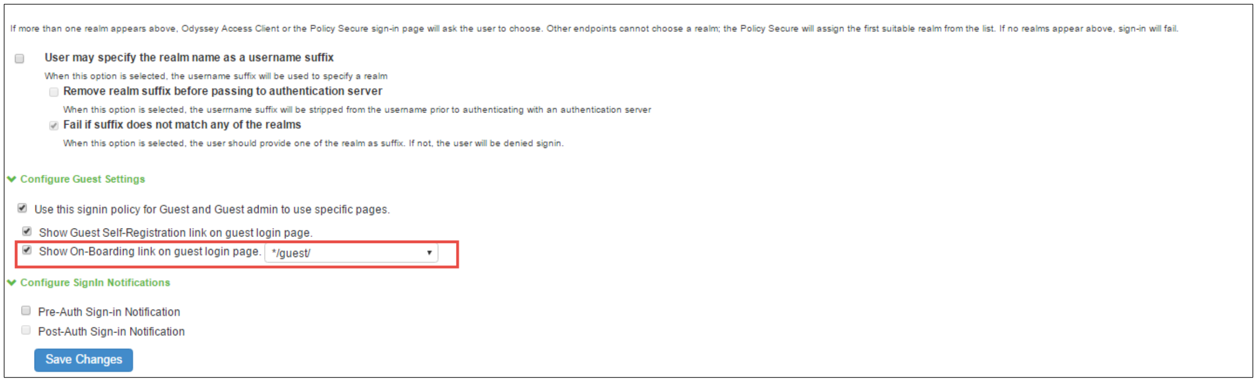
   The Sign-in Polices tab displays the available sign-in policies.

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

   The Sign-in Policy configuration screen appears.

© 2018 by Pulse Secure, LLC. All rights reserved

Figure 19: Enabling On-Boarding Link



If more than one realm appears above, Odyssey Access Client or the Policy Secure sign-in page will ask the user to choose. Other endpoints cannot choose a realm; the Policy Secure will assign the first suitable realm from the list. If no realms appear above, sign-in will fail.

□ **User may specify the realm name as a username suffix**

When this option is selected, the username suffix will be used to specify a realm

□ **Remove realm suffix before passing to authentication server**

When this option is selected, the username suffix will be stripped from the username prior to authenticating with an authentication server

☑ **Fail if suffix does not match any of the realms**

When this option is selected, the user should provide one of the realm as suffix. If not, the user will be denied signin.

☑ Use this signin policy for Guest and Guest admin to use specific pages.

☑ Show Guest Self-Registration link on guest login page.

☑ Show On-Boarding link on guest login page. */guest/

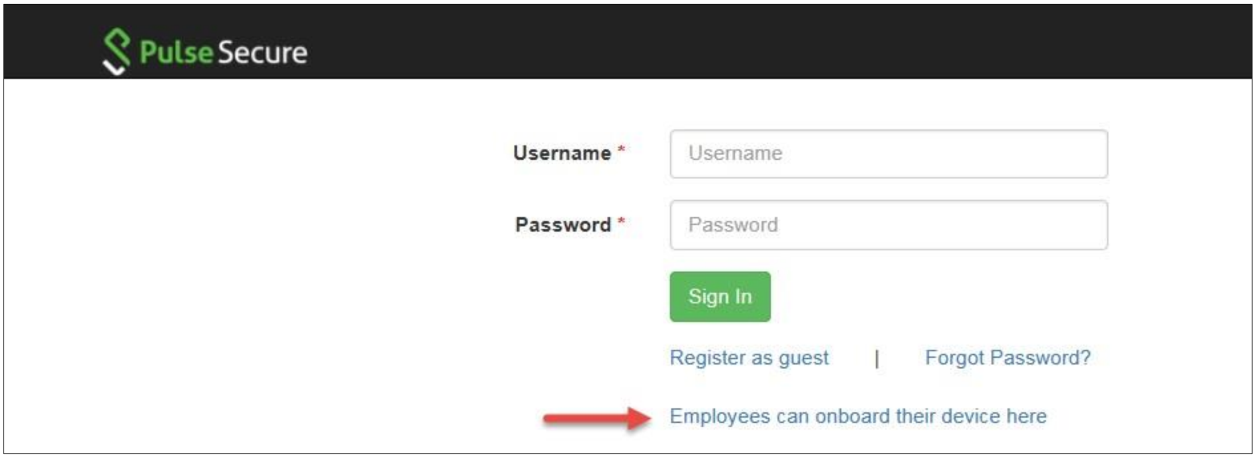
□ Pre-Auth Sign-in Notification

□ Post-Auth Sign-in Notification

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



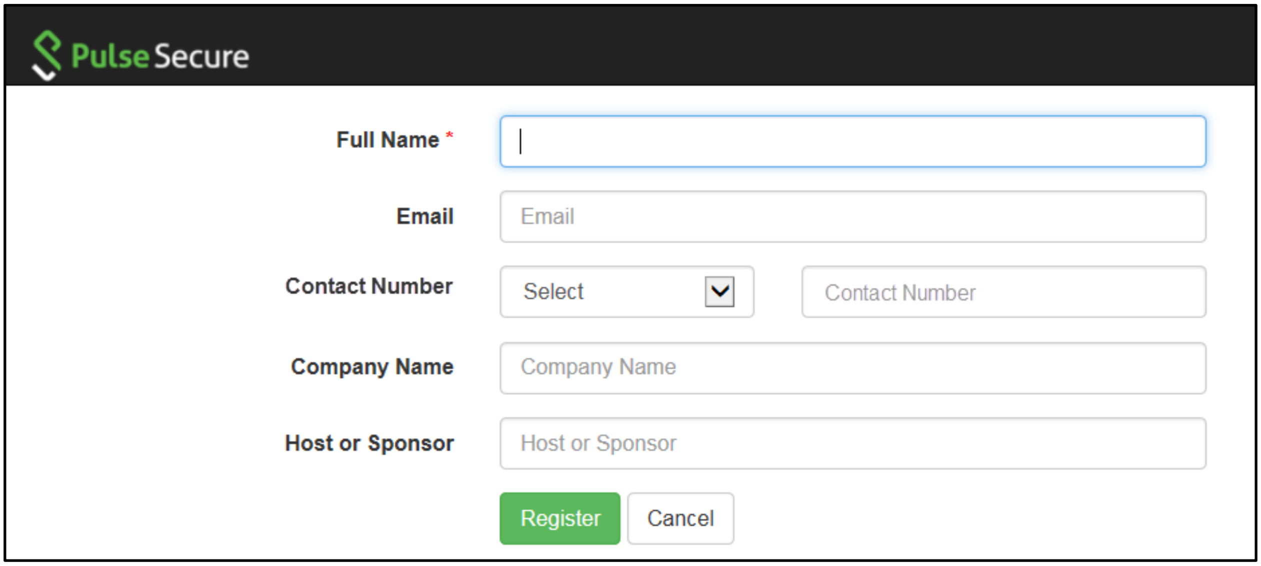
Pulse Secure
Username *
Username
Password *
Password
Sign In
Register as guest | Forgot Password?
Employees can onboard their device here

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



Full Name *

Email

Contact Number

Company Name

Host or Sponsor

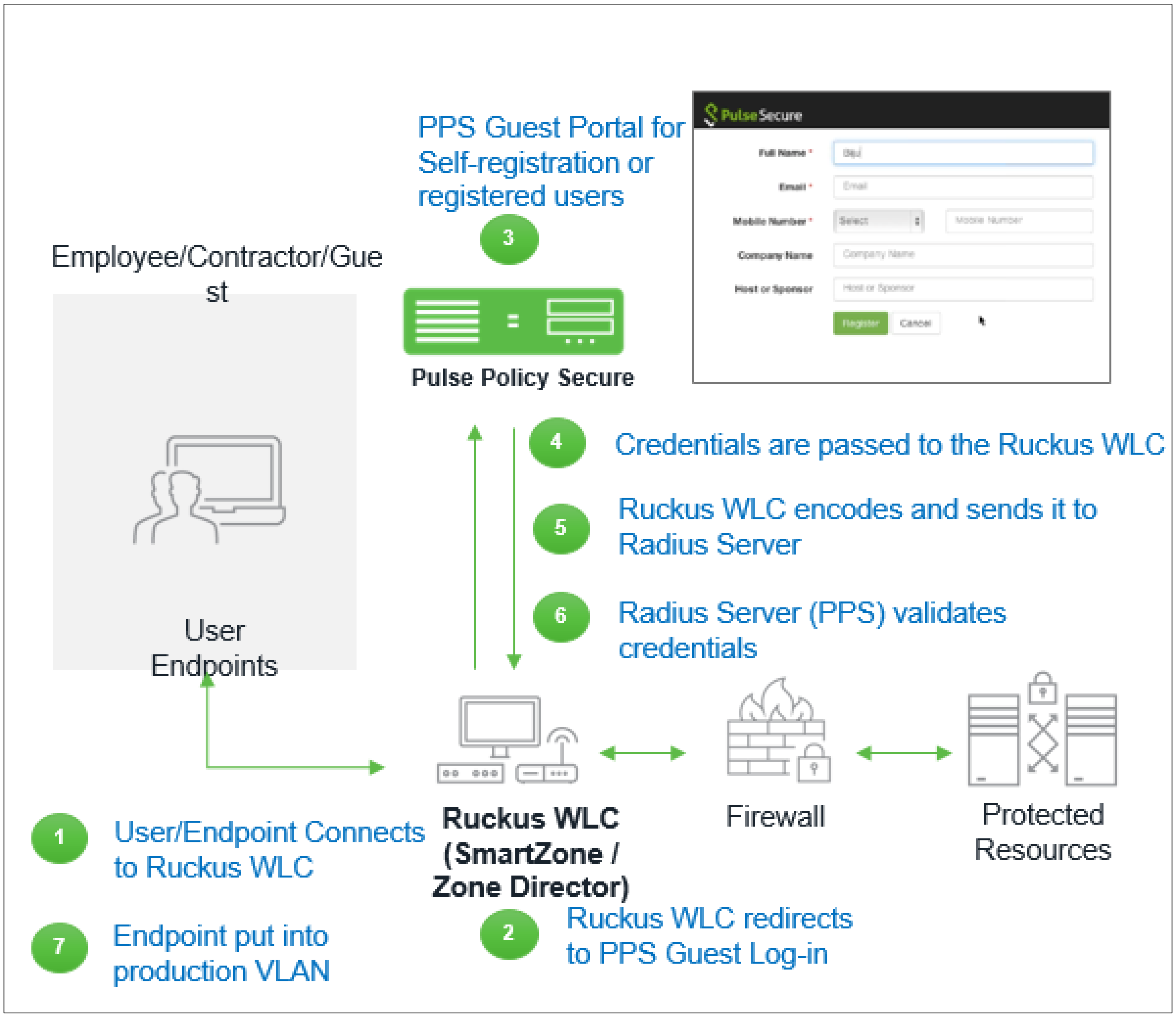
5. Enter name and make necessary changes.
6. Click **Register**.

© 2018 by Pulse Secure, LLC. All rights reserved

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


PPS Guest Portal for Self-registration or registered users
3
Employee/Contractor/Guest
Pulse Policy Secure
PulseSecure
Full Name *
Biju
Email *
Email
Mobile Number *
Select
Mobile Number
Company Name
Company Name
Host or Sponsor
Host or Sponsor
Register
Cancel
4
Credentials are passed to the Ruckus WLC
5
Ruckus WLC encodes and sends it to Radius Server
6
Radius Server (PPS) validates credentials
User Endpoints
Ruckus WLC (SmartZone / Zone Director)
Firewall
Protected Resources
1
User/Endpoint Connects to Ruckus WLC
7
Endpoint put into production VLAN
2
Ruckus WLC redirects to PPS Guest Log-in

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.

© 2018 by Pulse Secure, LLC. All rights reserved

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.

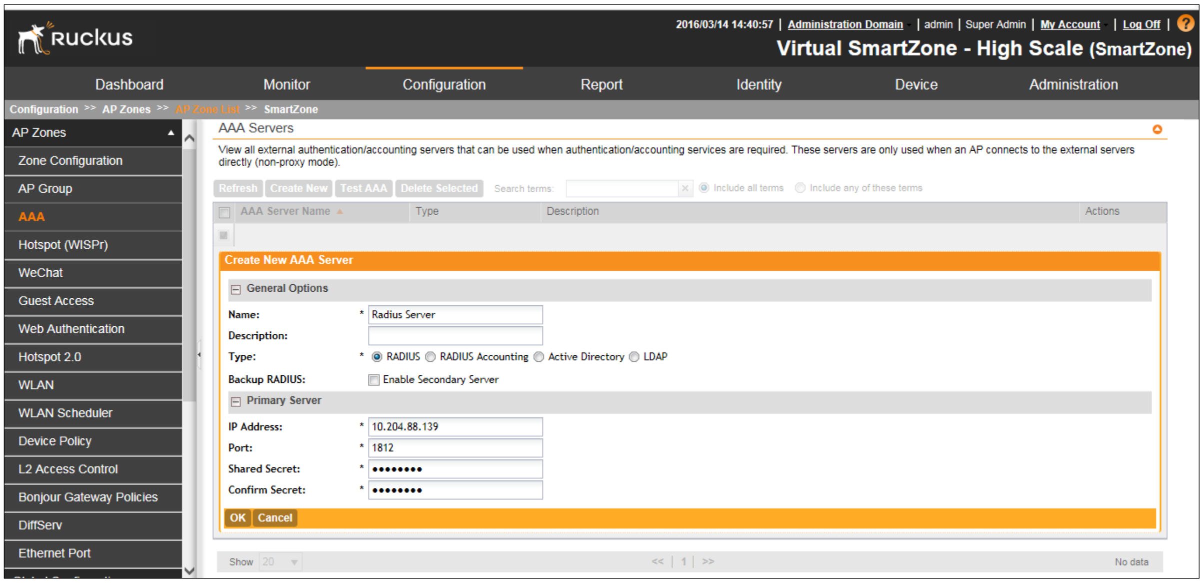
Ruckus SmartZone WLC Configuration

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 Sever.
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



View all external authentication/accounting servers that can be used when authentication/accounting services are required. These servers are only used when an AP connects to the external servers directly (non-proxy mode).

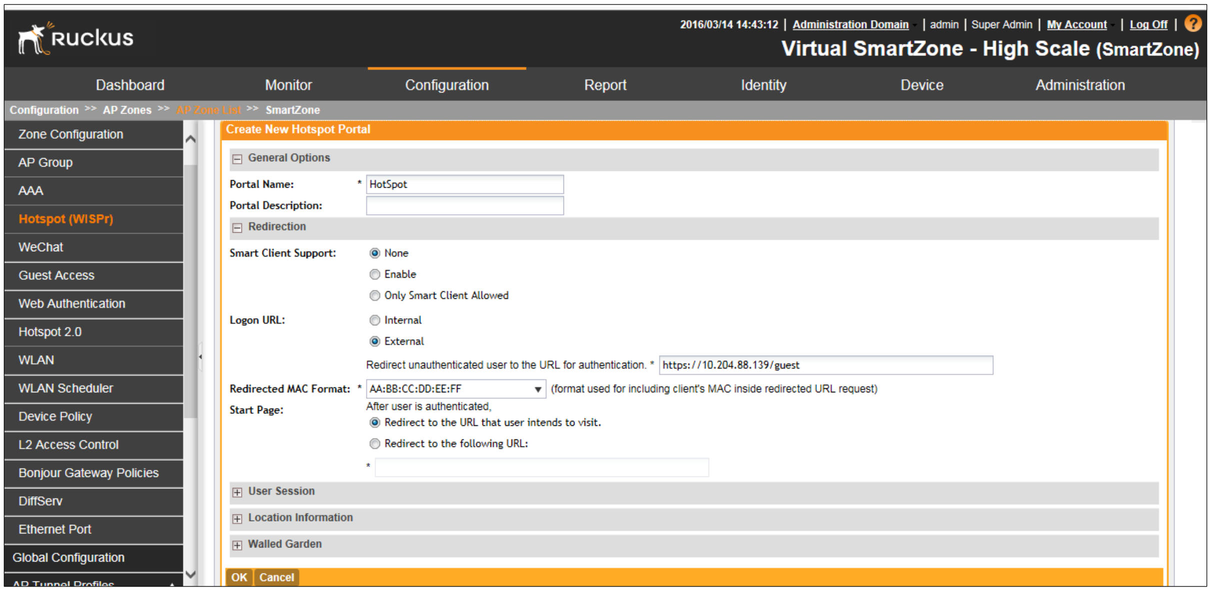
Name: * Radius Server
Description:
Type: * ● RADIUS ○ RADIUS Accounting ○ Active Directory ○ LDAP
Backup RADIUS: □ Enable Secondary Server
IP Address: * 10.204.88.139
Port: * 1812
Shared Secret: * ••••••••
Confirm Secret: * ••••••••

To configure Hotspot (WISPr) service:

© 2018 by Pulse Secure, LLC. All rights reserved

1. Go to **Configuration > AP Zone > Zone Name > Hotspot (WISPr)> Create New**.

Figure 24: SmartZone Hotspot Service



Create New Hotspot Portal

⊟ General Options

Portal Name: * HotSpot

Portal Description:

⊟ Redirection

Smart Client Support: ● None ○ Enable ○ Only Smart Client Allowed

Logon URL: ○ Internal ● External

Redirect unauthenticated user to the URL for authentication. * https://10.204.88.139/guest

Redirected MAC Format: * AA:BB:CC:DD:EE:FF (format used for including client's MAC inside redirected URL request)

Start Page: After user is authenticated, ● Redirect to the URL that user intends to visit. ○ Redirect to the following URL: *

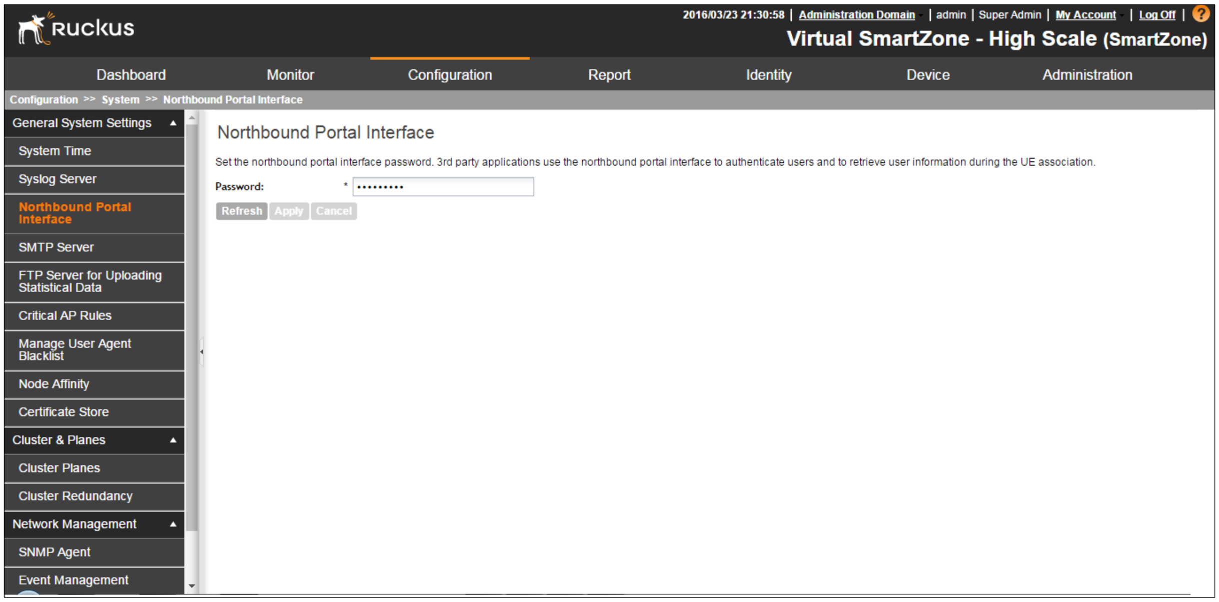
⊞ User Session

⊞ Location Information

⊞ Walled Garden

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



Northbound Portal Interface

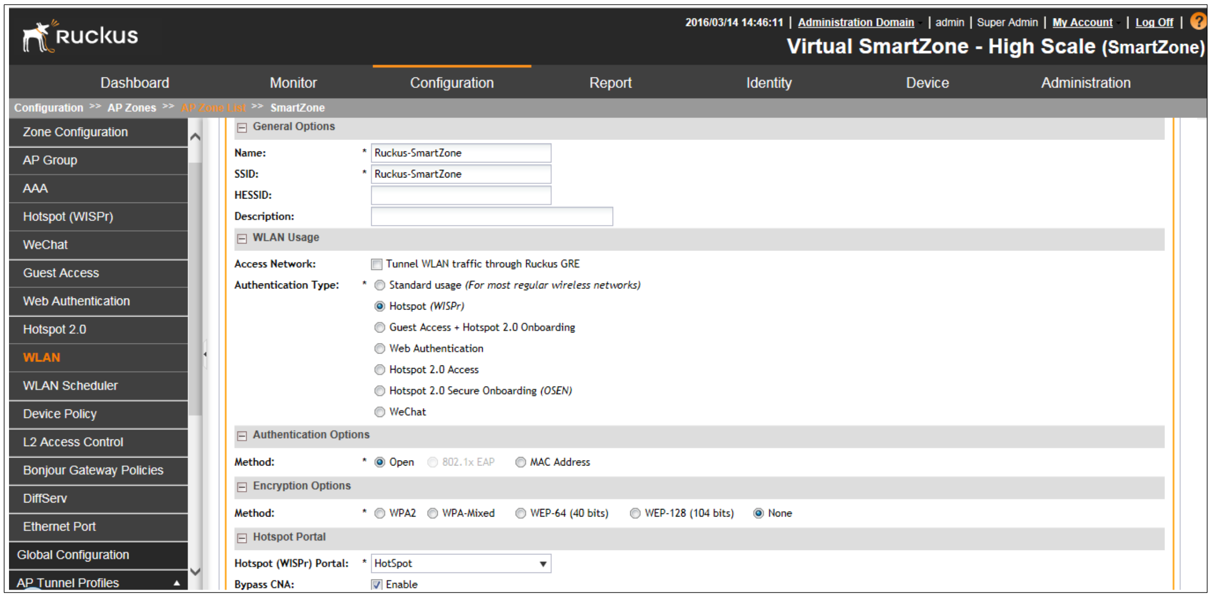
Set the northbound portal interface password. 3rd party applications use the northbound portal interface to authenticate users and to retrieve user information during the UE association.

Password: * •••••••••

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



⊟ General Options

Name: * Ruckus-SmartZone

SSID: * Ruckus-SmartZone

HESSID:

Description:

⊟ WLAN Usage

Access Network: □ Tunnel WLAN traffic through Ruckus GRE

Authentication Type: *
○ Standard usage *(For most regular wireless networks)*
● Hotspot *(WISPr)*
○ Guest Access + Hotspot 2.0 Onboarding
○ Web Authentication
○ Hotspot 2.0 Access
○ Hotspot 2.0 Secure Onboarding *(OSEN)*
○ WeChat

⊟ Authentication Options

Method: * ● Open ○ 802.1x EAP ○ MAC Address

⊟ Encryption Options

Method: * ○ WPA2 ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ● None

⊟ Hotspot Portal

Hotspot (WISPr) Portal: * HotSpot ▼

Bypass CNA: ☑ Enable

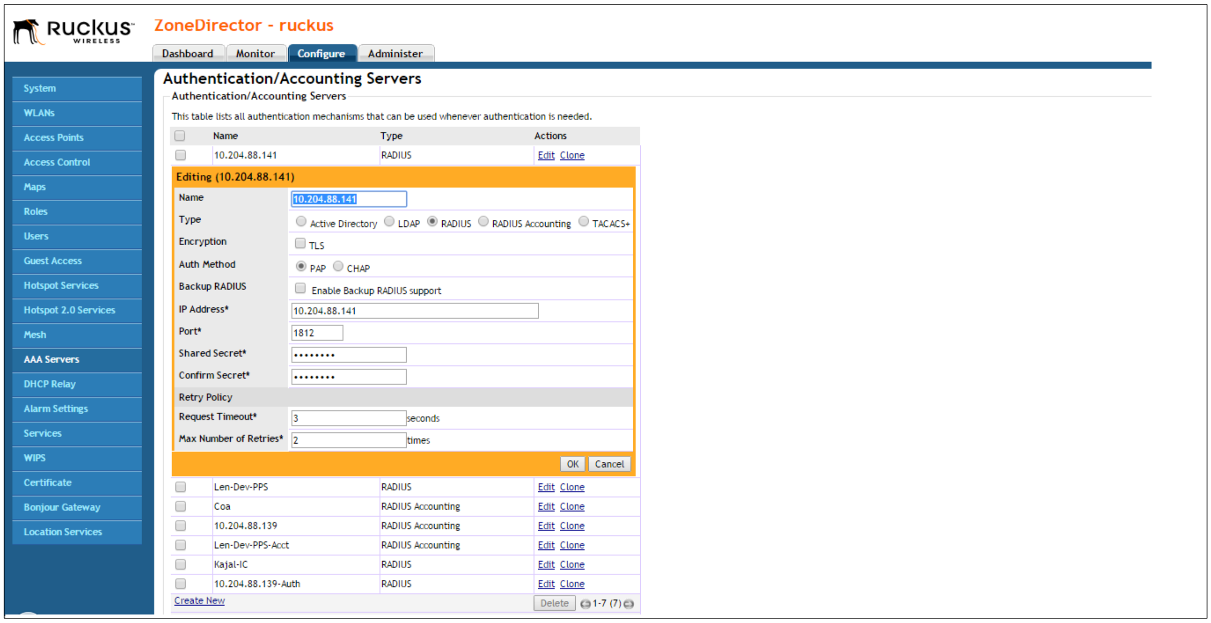
© 2018 by Pulse Secure, LLC. All rights reserved

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



Authentication/Accounting Servers

Authentication/Accounting Servers

This table lists all authentication mechanisms that can be used whenever authentication is needed.

□	Name	Type	Actions
□	10.204.88.141	RADIUS	Edit Clone

Editing (10.204.88.141)

Name	10.204.88.141
Type	○ Active Directory ○ LDAP ● RADIUS ○ RADIUS Accounting ○ TACACS+
Encryption	□ TLS
Auth Method	● PAP ○ CHAP
Backup RADIUS	□ Enable Backup RADIUS support
IP Address*	10.204.88.141
Port*	1812
Shared Secret*	••••••••
Confirm Secret*	••••••••
Retry Policy	
Request Timeout*	3 seconds
Max Number of Retries*	2 times

OK Cancel

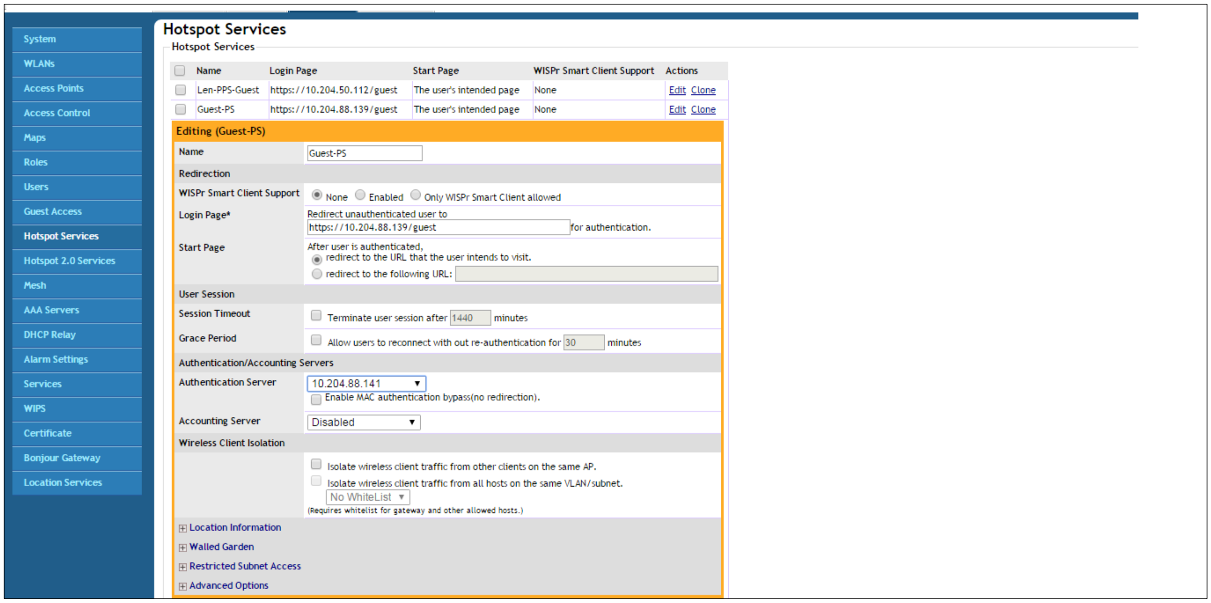
□	Name	Type	Actions
□	Len-Dev-PPS	RADIUS	Edit Clone
□	Coa	RADIUS Accounting	Edit Clone
□	10.204.88.139	RADIUS Accounting	Edit Clone
□	Len-Dev-PPS-Acct	RADIUS Accounting	Edit Clone
□	Kajal-IC	RADIUS	Edit Clone
□	10.204.88.139-Auth	RADIUS	Edit Clone

Create New   Delete 1-7 (7)

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



Hotspot Services

Hotspot Services

□	Name	Login Page	Start Page	WISPr Smart Client Support	Actions
□	Len-PPS-Guest	https://10.204.50.112/guest	The user's intended page	None	Edit Clone
□	Guest-PS	https://10.204.88.139/guest	The user's intended page	None	Edit Clone

Editing (Guest-PS)

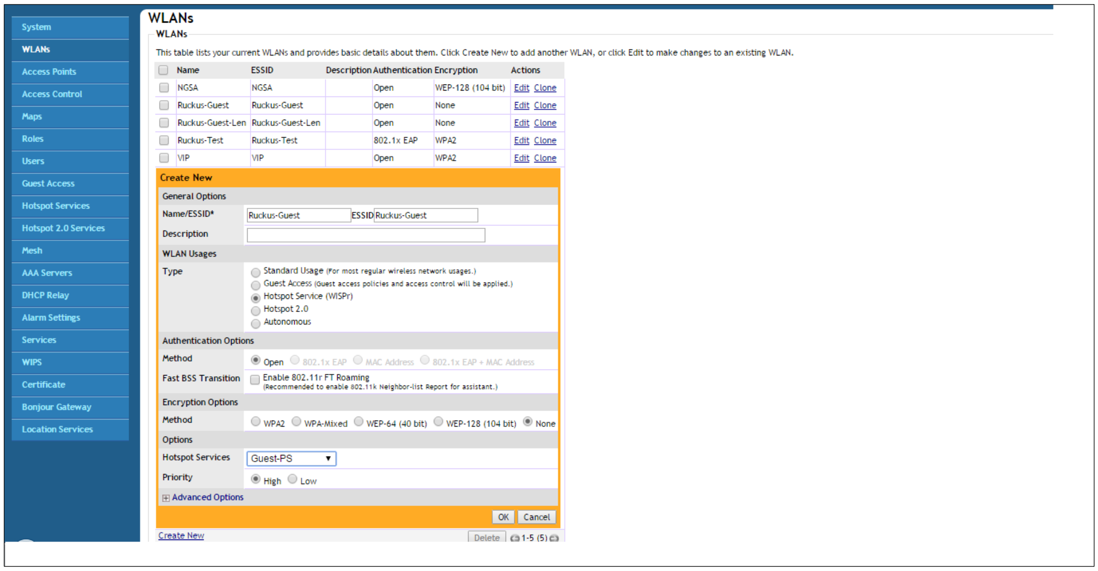
Name	Guest-PS
Redirection	
WISPr Smart Client Support	● None ○ Enabled ○ Only WISPr Smart Client allowed
Login Page*	Redirect unauthenticated user to https://10.204.88.139/guest for authentication.
Start Page	After user is authenticated, ● redirect to the URL that the user intends to visit. ○ redirect to the following URL:
User Session	
Session Timeout	□ Terminate user session after 1440 minutes
Grace Period	□ Allow users to reconnect with out re-authentication for 30 minutes
Authentication/Accounting Servers	
Authentication Server	10.204.88.141 ▾ □ Enable MAC authentication bypass(no redirection).
Accounting Server	Disabled ▾
Wireless Client Isolation	
	□ Isolate wireless client traffic from other clients on the same AP. □ Isolate wireless client traffic from all hosts on the same VLAN/subnet. No WhiteList ▾ (Requires whitelist for gateway and other allowed hosts.)

⊞ Location Information
⊞ Walled Garden
⊞ Restricted Subnet Access
⊞ Advanced Options

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



WLANs

WLANs

This table lists your current WLANs and provides basic details about them. Click Create New to add another WLAN, or click Edit to make changes to an existing WLAN.

□	Name	ESSID	Description	Authentication	Encryption	Actions
□	NGSA	NGSA		Open	WEP-128 (104 bit)	Edit Clone
□	Ruckus-Guest	Ruckus-Guest		Open	None	Edit Clone
□	Ruckus-Guest-Len	Ruckus-Guest-Len		Open	None	Edit Clone
□	Ruckus-Test	Ruckus-Test		802.1x EAP	WPA2	Edit Clone
□	VIP	VIP		Open	WPA2	Edit Clone

Create New

General Options	
Name/ESSID*	Ruckus-Guest ESSID Ruckus-Guest
Description	
WLAN Usages	
Type	○ Standard Usage (For most regular wireless network usages.) ○ Guest Access (Guest access policies and access control will be applied.) ● Hotspot Service (WISPr) ○ Hotspot 2.0 ○ Autonomous
Authentication Options	
Method	● Open ○ 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address
Fast BSS Transition	□ Enable 802.11r FT Roaming (Recommended to enable 802.11k Neighbor-list Report for assistant.)
Encryption Options	
Method	○ WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ● None
Options	
Hotspot Services	Guest-PS ▾
Priority	● High ○ Low

⊞ Advanced Options

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

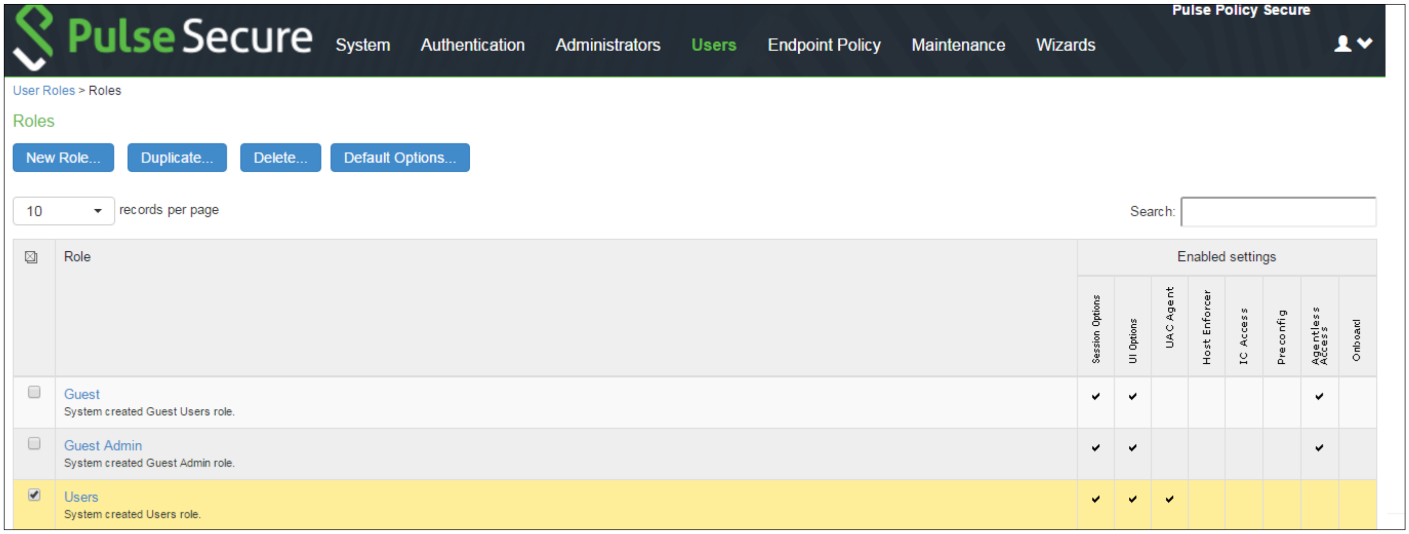
Configuring User Role for Dot1x Authentication

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



User Roles > Roles

Roles

New Role... Duplicate... Delete... Default Options...

10 records per page

Search:

☐	Role	Enabled settings							
		Session Options	UI Options	UAC Agent	Host Enforcer	IC Access	Preconfig	Agentless Access	Onboard
☐	Guest System created Guest Users role.	✓	✓					✓	
☐	Guest Admin System created Guest Admin role.	✓	✓					✓	
☑	Users System created Users role.	✓	✓	✓					

Configuring User Realm for Dot1x

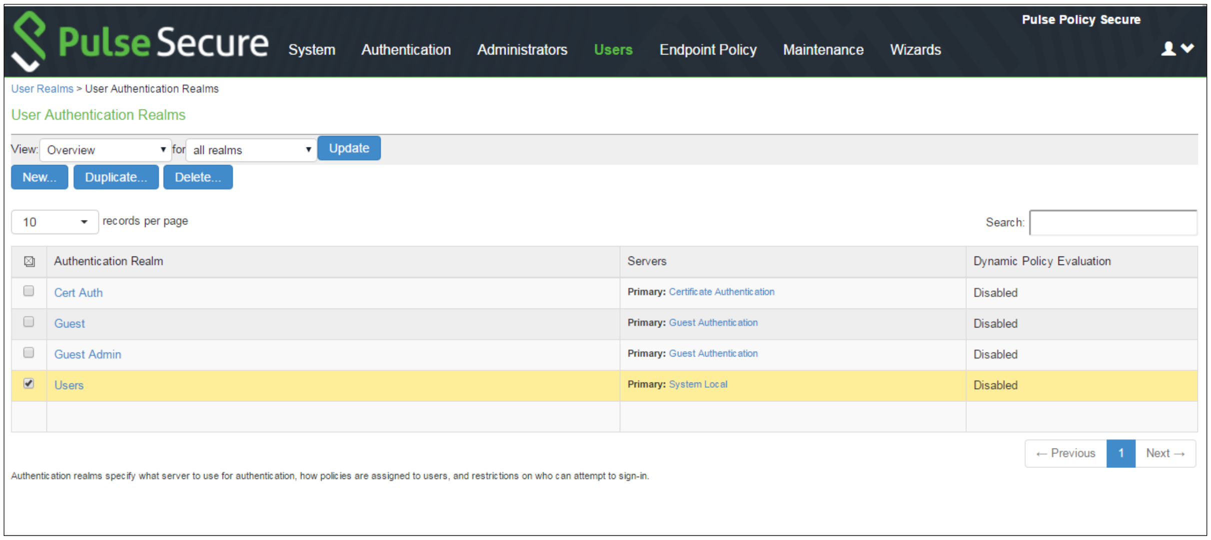
The user realm configuration associates the MDM server data with user roles.

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



User Realms > User Authentication Realms

User Authentication Realms

View: Overview for all realms Update

New... Duplicate... Delete...

10 records per page Search:

☐	Authentication Realm	Servers	Dynamic Policy Evaluation
☐	Cert Auth	**Primary:** Certificate Authentication	Disabled
☐	Guest	**Primary:** Guest Authentication	Disabled
☐	Guest Admin	**Primary:** Guest Authentication	Disabled
☑	Users	**Primary:** System Local	Disabled

← Previous 1 Next →

Authentication realms specify what server to use for authentication, how policies are assigned to users, and restrictions on who can attempt to sign-in.

Configuring a Sign-In Policy for Dot1x

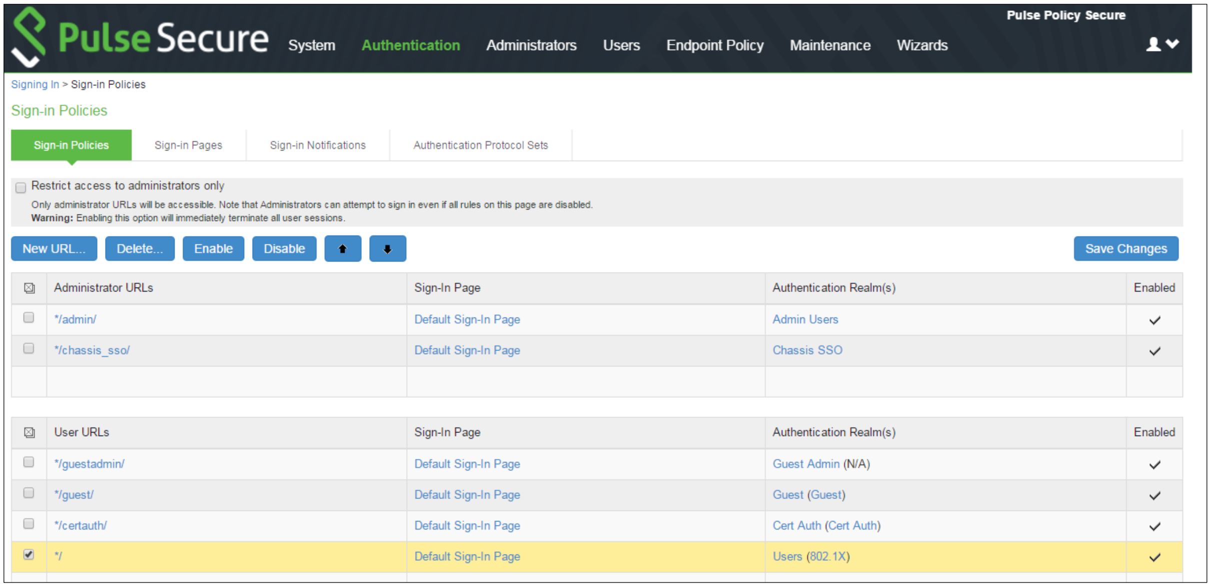
A sign-in policy associates devices with a realm.

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.

© 2018 by Pulse Secure, LLC. All rights reserved

Figure 32: Sign-In Policy for Dot1x Authentication



Signing In > Sign-in Policies

Sign-in Policies

□ Restrict access to administrators only

Only administrator URLs will be accessible. Note that Administrators can attempt to sign in even if all rules on this page are disabled.
Warning: Enabling this option will immediately terminate all user sessions.

□	Administrator URLs	Sign-In Page	Authentication Realm(s)	Enabled
□	*/admin/	Default Sign-In Page	Admin Users	✓
□	*/chassis_sso/	Default Sign-In Page	Chassis SSO	✓

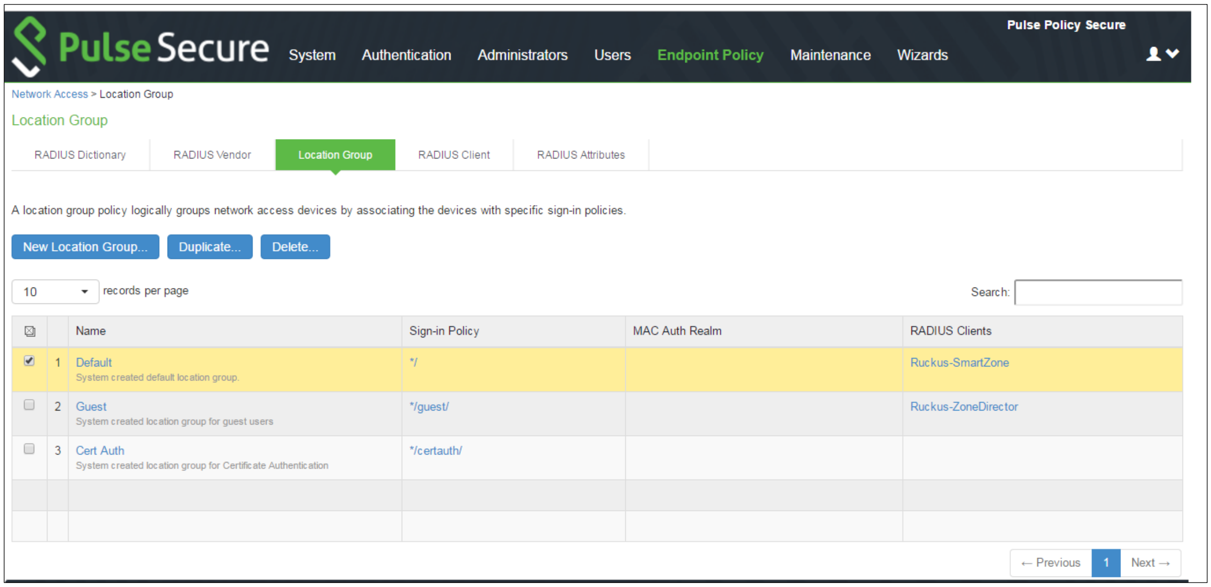
□	User URLs	Sign-In Page	Authentication Realm(s)	Enabled
□	*/guestadmin/	Default Sign-In Page	Guest Admin (N/A)	✓
□	*/guest/	Default Sign-In Page	Guest (Guest)	✓
□	*/certauth/	Default Sign-In Page	Cert Auth (Cert Auth)	✓
☑	*/	Default Sign-In Page	Users (802.1X)	✓

Configuring Location Group for Dot1x

To configure Policy Secure 802.1x framework for non-supplicant 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



Network Access > Location Group

Location Group

A location group policy logically groups network access devices by associating the devices with specific sign-in policies.

10 records per page

Search:

□		Name	Sign-in Policy	MAC Auth Realm	RADIUS Clients
☑	1	Default System created default location group.	*/		Ruckus-SmartZone
□	2	Guest System created location group for guest users	*/guest/		Ruckus-ZoneDirector
□	3	Cert Auth System created location group for Certificate Authentication	*/certauth/		

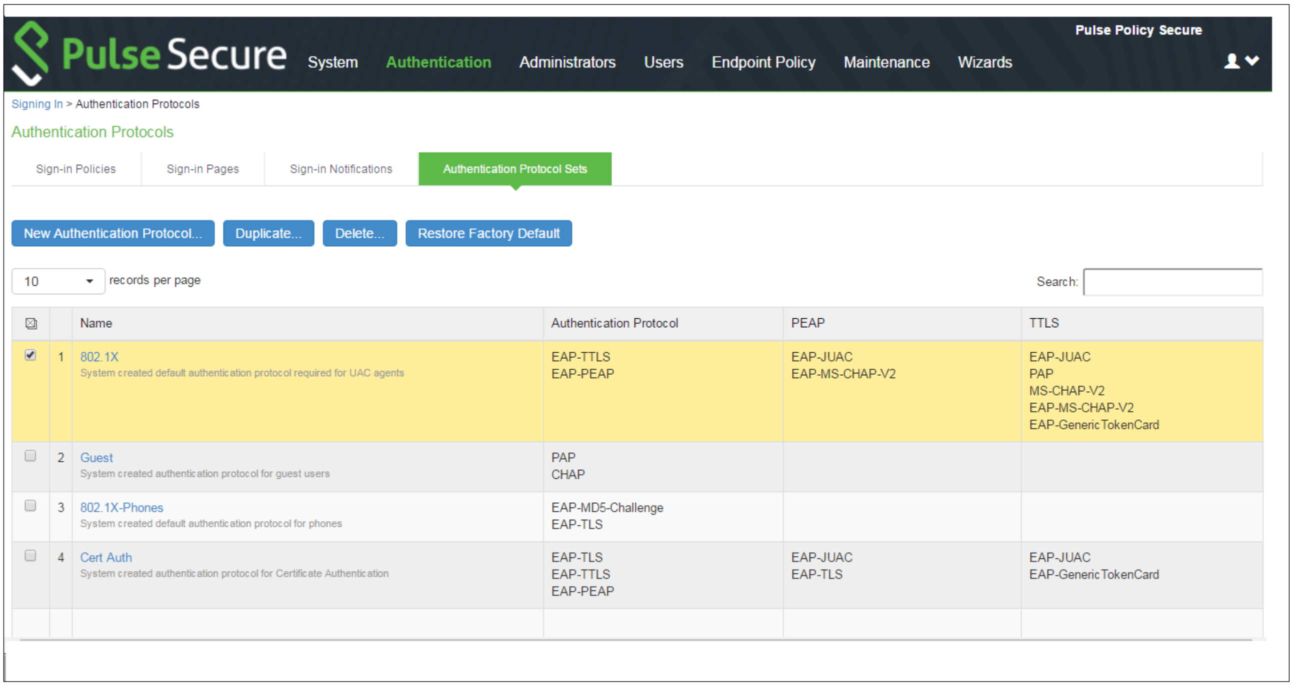
Configuring Authentication Protocol Set for Dot1x

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 > Authentication Protocols Sets to display the Authentication Protocol Sets page.

Figure 34: Authentication Protocol Set



☒		Name	Authentication Protocol	PEAP	TTLS
☑	1	802.1X System created default authentication protocol required for UAC agents	EAP-TTLS EAP-PEAP	EAP-JUAC EAP-MS-CHAP-V2	EAP-JUAC PAP MS-CHAP-V2 EAP-MS-CHAP-V2 EAP-GenericTokenCard
□	2	Guest System created authentication protocol for guest users	PAP CHAP		
□	3	802.1X-Phones System created default authentication protocol for phones	EAP-MD5-Challenge EAP-TLS		
□	4	Cert Auth System created authentication protocol for Certificate Authentication	EAP-TLS EAP-TTLS EAP-PEAP	EAP-JUAC EAP-TLS	EAP-JUAC EAP-GenericTokenCard

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.

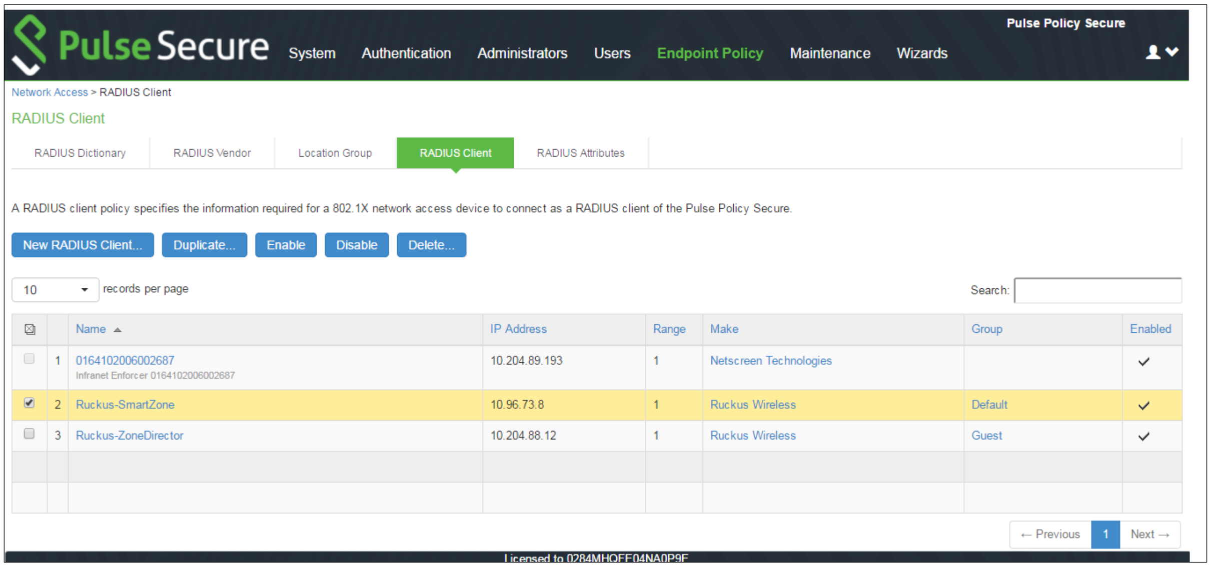
Configuring RADIUS Client

To configure a Radius Client:

1. Select Endpoint Policy > Network Access > RADIUS Client.

© 2018 by Pulse Secure, LLC. All rights reserved

Figure 35: Radius Client – Ruckus WLC



Network Access > RADIUS Client

RADIUS Client

RADIUS Dictionary | RADIUS Vendor | Location Group | RADIUS Client | RADIUS Attributes

A RADIUS client policy specifies the information required for a 802.1X network access device to connect as a RADIUS client of the Pulse Policy Secure.

New RADIUS Client... | Duplicate... | Enable | Disable | Delete...

10 records per page   Search:

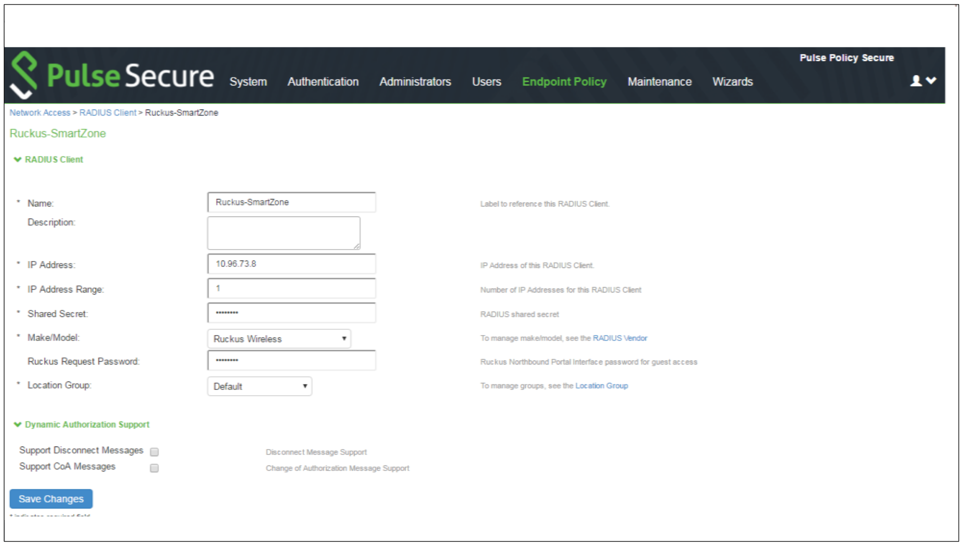
☐		Name ▲	IP Address	Range	Make	Group	Enabled
☐	1	0164102006002687 Infranet Enforcer 0164102006002687	10.204.89.193	1	Netscreen Technologies		✓
☑	2	Ruckus-SmartZone	10.96.73.8	1	Ruckus Wireless	Default	✓
☐	3	Ruckus-ZoneDirector	10.204.88.12	1	Ruckus Wireless	Guest	✓

← Previous | 1 | Next →

Licensed to 0284MHQEF04NA0P9E

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

Figure 36: Ruckus SmartZone



Network Access > RADIUS Client > Ruckus-SmartZone

Ruckus-SmartZone

RADIUS Client

* Name:	Ruckus-SmartZone	Label to reference this RADIUS Client.
Description:		
* IP Address:	10.96.73.8	IP Address of this RADIUS Client.
* IP Address Range:	1	Number of IP Addresses for this RADIUS Client
* Shared Secret:	••••••••	RADIUS shared secret
* Make/Model:	Ruckus Wireless	To manage make/model, see the RADIUS Vendor
Ruckus Request Password:	••••••••	Ruckus Northbound Portal Interface password for guest access
* Location Group:	Default	To manage groups, see the Location Group

Dynamic Authorization Support

Support Disconnect Messages	☐	Disconnect Message Support
Support CoA Messages	☐	Change of Authorization Message Support

Save Changes

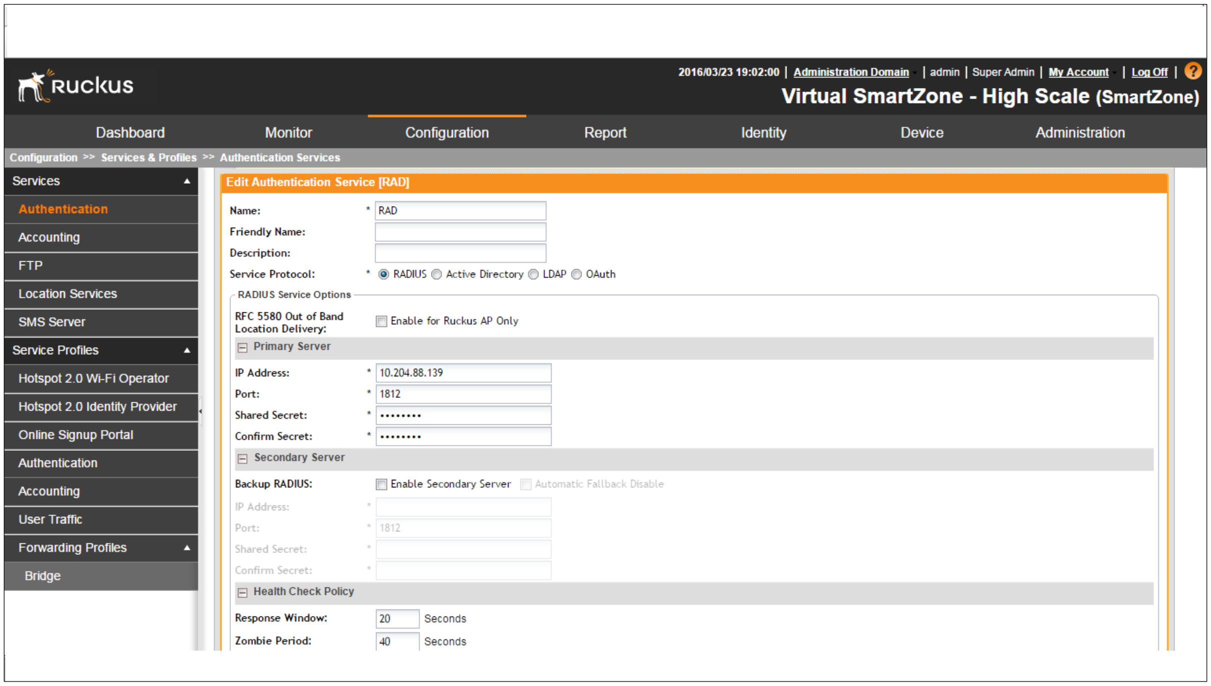
3. Here Ruckus Request password should be the same which is configured in "NorthBound Polar Interface" of SmartZone WLC and select default location group.

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


Ruckus
2016/03/23 19:02:00 | Administration Domain | admin | Super Admin | My Account | Log Off | ?
Virtual SmartZone - High Scale (SmartZone)
Dashboard
Monitor
Configuration
Report
Identity
Device
Administration
Configuration >> Services & Profiles >> Authentication Services
Services
Authentication
Accounting
FTP
Location Services
SMS Server
Service Profiles
Hotspot 2.0 Wi-Fi Operator
Hotspot 2.0 Identity Provider
Online Signup Portal
Authentication
Accounting
User Traffic
Forwarding Profiles
Bridge

Edit Authentication Service [RAD]

Name: * RAD

Friendly Name:

Description:

Service Protocol: * ● RADIUS ○ Active Directory ○ LDAP ○ OAuth

RADIUS Service Options

RFC 5580 Out of Band Location Delivery: □ Enable for Ruckus AP Only

⊟ Primary Server

IP Address: * 10.204.88.139

Port: * 1812

Shared Secret: * ••••••••

Confirm Secret: * ••••••••

⊟ Secondary Server

Backup RADIUS: □ Enable Secondary Server □ Automatic Fallback Disable

IP Address: *

Port: * 1812

Shared Secret: *

Confirm Secret: *

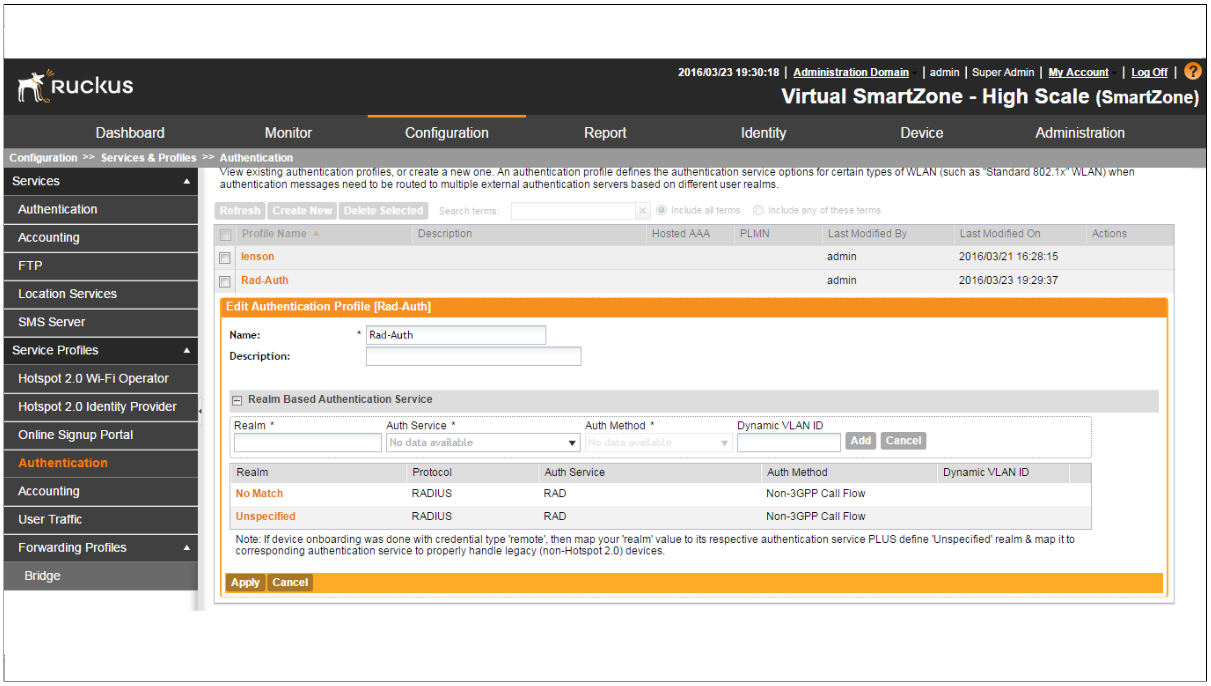
⊟ Health Check Policy

Response Window: 20 Seconds

Zombie Period: 40 Seconds

3. Map the configured radius server on both realms “No Match” and “Unspecified”.

Figure 38: Authentication Profile - Ruckus SmartZone



View existing authentication profiles, or create a new one. An authentication profile defines the authentication service options for certain types of WLAN (such as "Standard 802.1x" WLAN) when authentication messages need to be routed to multiple external authentication servers based on different user realms.

Profile Name	Description	Hosted AAA	PLMN	Last Modified By	Last Modified On	Actions
lenson				admin	2016/03/21 16:28:15	
Rad-Auth				admin	2016/03/23 19:29:37	

Edit Authentication Profile [Rad-Auth]

Name: * Rad-Auth

Description:

Realm Based Authentication Service

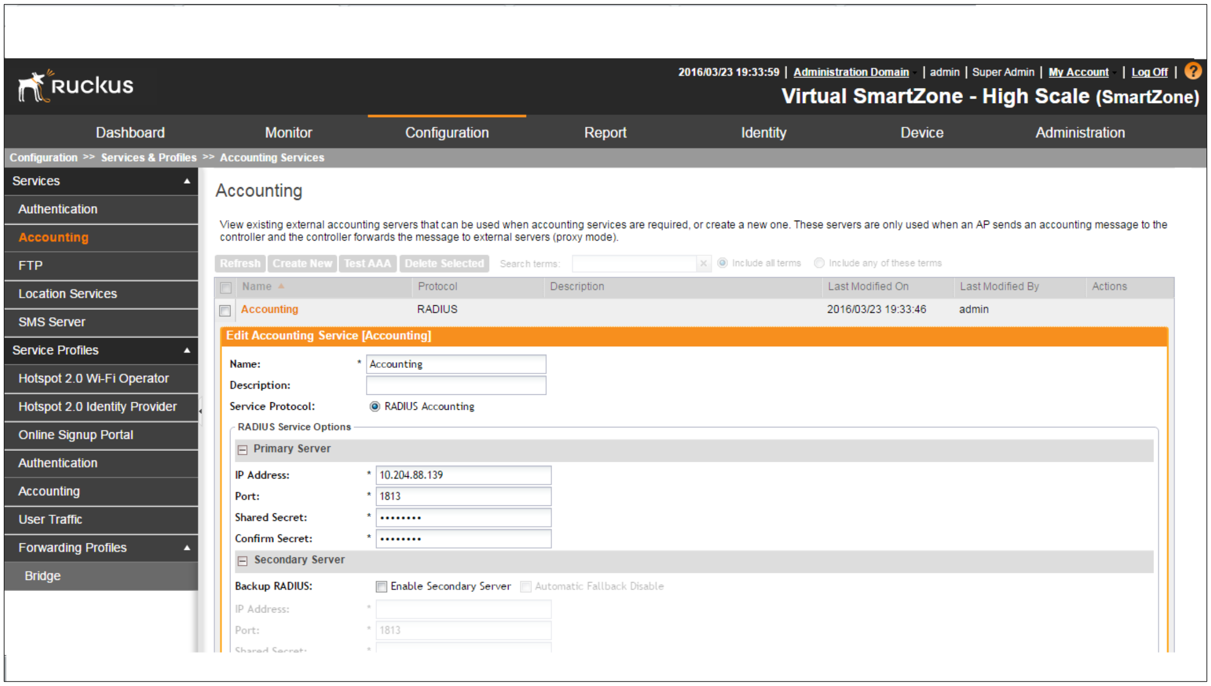
Realm * | Auth Service * No data available | Auth Method * No data available | Dynamic VLAN ID

Realm	Protocol	Auth Service	Auth Method	Dynamic VLAN ID
No Match	RADIUS	RAD	Non-3GPP Call Flow	
Unspecified	RADIUS	RAD	Non-3GPP Call Flow	

Note: If device onboarding was done with credential type 'remote', then map your 'realm' value to its respective authentication service PLUS define 'Unspecified' realm & map it to corresponding authentication service to properly handle legacy (non-Hotspot 2.0) devices.

4. To view the Accounting Services go to Configuration > Service profiles > Accounting.
5. Enter the Name, IP Address, shared secret and confirm secret.

Figure 39: Accounting Services - Ruckus SmartZone



Accounting

View existing external accounting servers that can be used when accounting services are required, or create a new one. These servers are only used when an AP sends an accounting message to the controller and the controller forwards the message to external servers (proxy mode).

Name	Protocol	Description	Last Modified On	Last Modified By	Actions
Accounting	RADIUS		2016/03/23 19:33:46	admin	

Edit Accounting Service [Accounting]

Name: * Accounting

Description:

Service Protocol: ● RADIUS Accounting

RADIUS Service Options

Primary Server

IP Address: * 10.204.88.139

Port: * 1813

Shared Secret: * ••••••••

Confirm Secret: * ••••••••

Secondary Server

Backup RADIUS: □ Enable Secondary Server □ Automatic Fallback Disable

IP Address: *

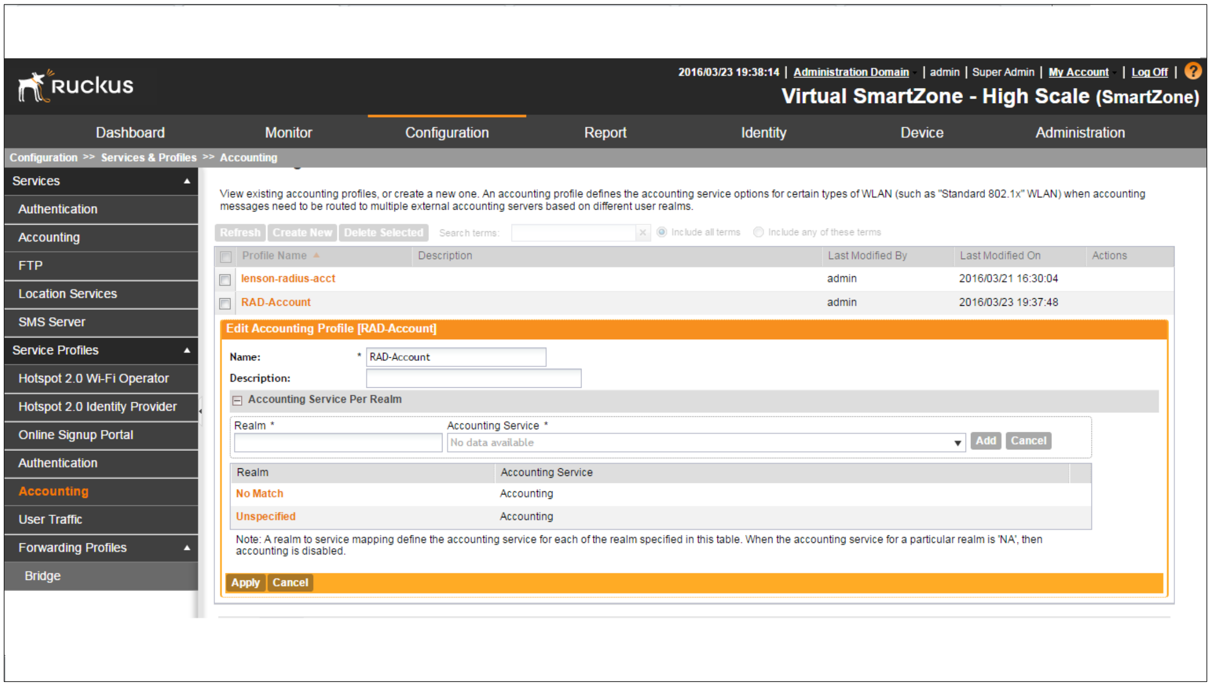
Port: * 1813

Shared Secret: *

© 2018 by Pulse Secure, LLC. All rights reserved

6. Map the configured radius server on both realms “No Match” and “Unspecified”.

Figure 40: Accounting Profile - Ruckus SmartZone



View existing accounting profiles, or create a new one. An accounting profile defines the accounting service options for certain types of WLAN (such as "Standard 802.1x" WLAN) when accounting messages need to be routed to multiple external accounting servers based on different user realms.

Profile Name	Description	Last Modified By	Last Modified On	Actions
lenson-radius-acct		admin	2016/03/21 16:30:04	
RAD-Account		admin	2016/03/23 19:37:48	

Edit Accounting Profile [RAD-Account]

Name: * RAD-Account

Description:

Accounting Service Per Realm

Realm *

Accounting Service * No data available

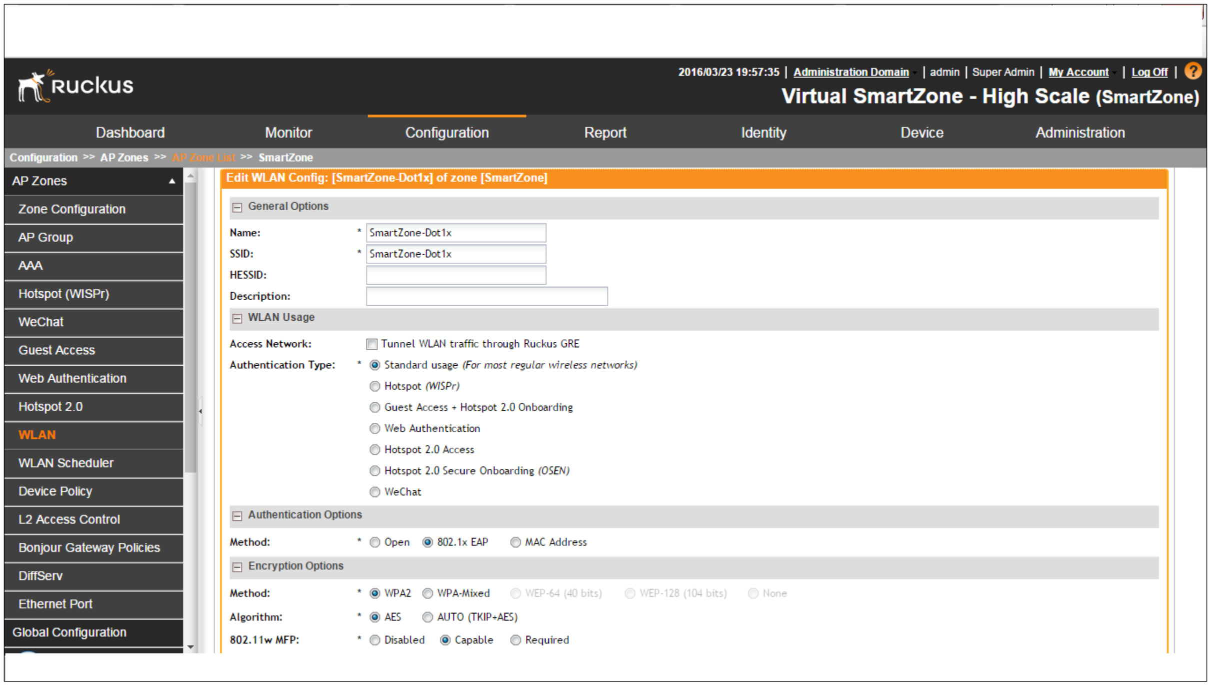
Realm	Accounting Service
No Match	Accounting
Unspecified	Accounting

Note: A realm to service mapping define the accounting service for each of the realm specified in this table. When the accounting service for a particular realm is 'NA', then accounting is disabled.

To configure AP Zones:

7. Go to Configuration > AP Zones > Zone Name.
8. Create New WLAN.

Figure 41: Ruckus SmartZone AP Zones - WLAN



Edit WLAN Config: [SmartZone-Dot1x] of zone [SmartZone]

General Options

Name: * SmartZone-Dot1x

SSID: * SmartZone-Dot1x

HESSID:

Description:

WLAN Usage

Access Network: □ Tunnel WLAN traffic through Ruckus GRE

Authentication Type: * ● Standard usage *(For most regular wireless networks)*
○ Hotspot *(WISPr)*
○ Guest Access + Hotspot 2.0 Onboarding
○ Web Authentication
○ Hotspot 2.0 Access
○ Hotspot 2.0 Secure Onboarding *(OSEN)*
○ WeChat

Authentication Options

Method: * ○ Open ● 802.1x EAP ○ MAC Address

Encryption Options

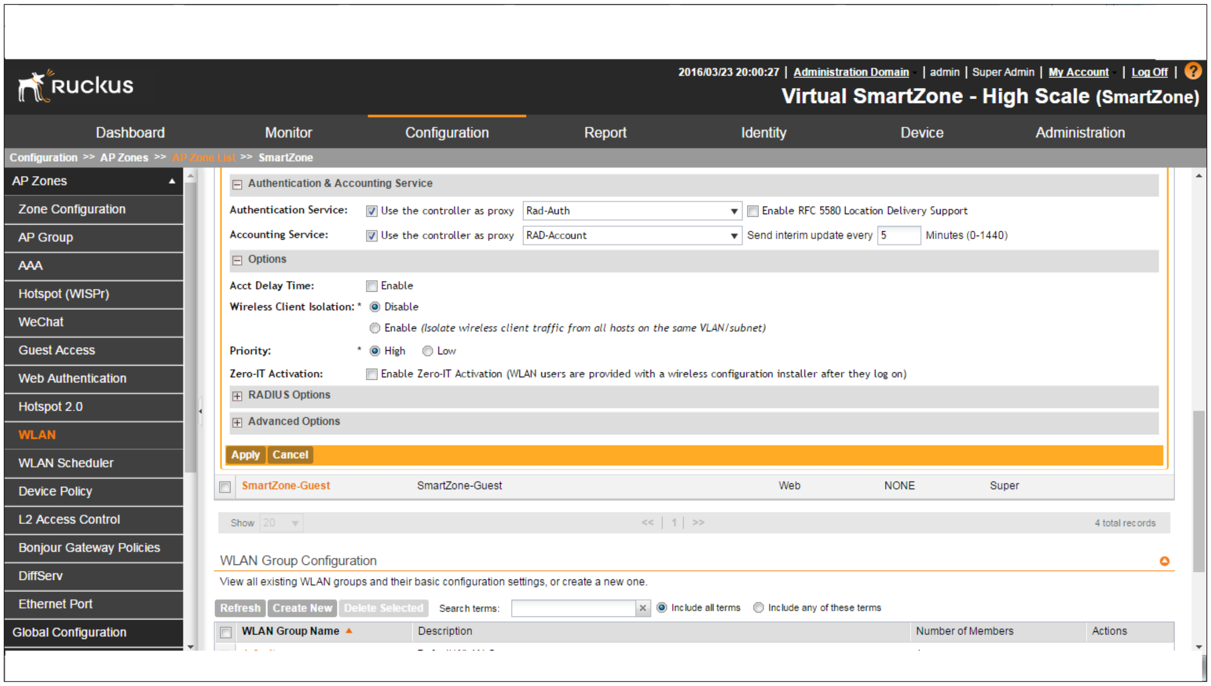
Method: * ● WPA2 ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ○ None

Algorithm: * ● AES ○ AUTO (TKIP+AES)

802.11w MFP: * ○ Disabled ● Capable ○ Required

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 42: Authentication and Accounting Service – Ruckus SmartZone



Authentication & Accounting Service

Authentication Service: ☑ Use the controller as proxy Rad-Auth □ Enable RFC 5580 Location Delivery Support

Accounting Service: ☑ Use the controller as proxy RAD-Account Send interim update every 5 Minutes (0-1440)

Options

Acct Delay Time: □ Enable

Wireless Client Isolation: * ● Disable
○ Enable *(Isolate wireless client traffic from all hosts on the same VLAN/subnet)*

Priority: * ● High ○ Low

Zero-IT Activation: □ Enable Zero-IT Activation (WLAN users are provided with a wireless configuration installer after they log on)

RADIUS Options

Advanced Options

Apply Cancel

□	SmartZone-Guest	SmartZone-Guest	Web	NONE	Super

Show 20 << | 1 | >> 4 total records

WLAN Group Configuration

View all existing WLAN groups and their basic configuration settings, or create a new one.

Refresh Create New Delete Selected Search terms: ● Include all terms ○ Include any of these terms

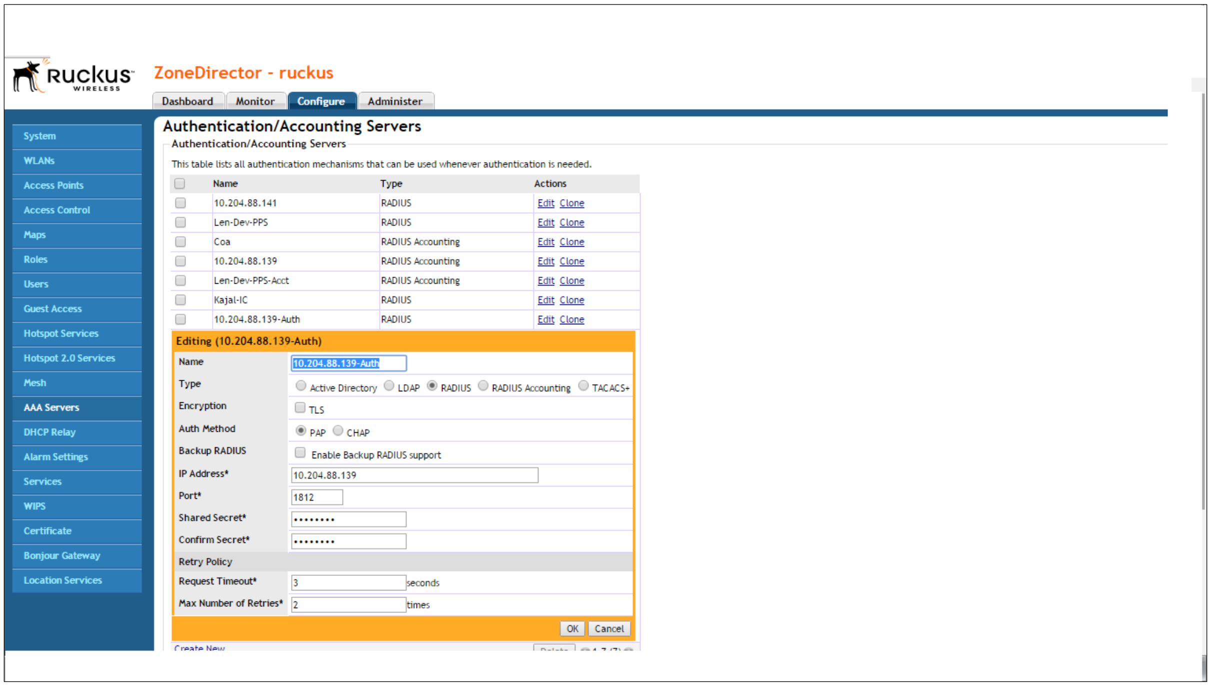
□	WLAN Group Name ▲	Description	Number of Members	Actions

11. Under Authentication and Accounting Service, check Controller as a proxy and select configured Radius Authentication and Accounting Server using drop down.
12. Configure Northbound Portal Interface.

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



Authentication/Accounting Servers

Authentication/Accounting Servers

This table lists all authentication mechanisms that can be used whenever authentication is needed.

□	Name	Type	Actions
□	10.204.88.141	RADIUS	Edit Clone
□	Len-Dev-PPS	RADIUS	Edit Clone
□	Coa	RADIUS Accounting	Edit Clone
□	10.204.88.139	RADIUS Accounting	Edit Clone
□	Len-Dev-PPS-Acct	RADIUS Accounting	Edit Clone
□	Kajal-IC	RADIUS	Edit Clone
□	10.204.88.139-Auth	RADIUS	Edit Clone

Editing (10.204.88.139-Auth)

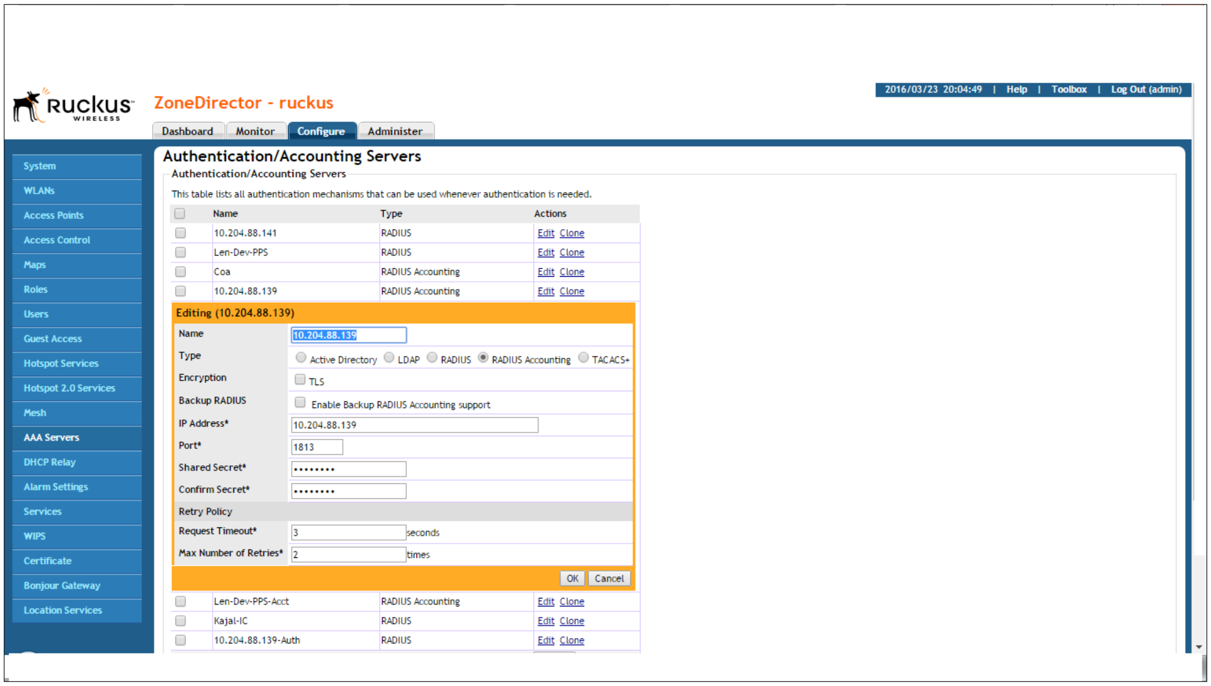
Name	10.204.88.139-Auth
Type	○ Active Directory ○ LDAP ● RADIUS ○ RADIUS Accounting ○ TACACS+
Encryption	□ TLS
Auth Method	● PAP ○ CHAP
Backup RADIUS	□ Enable Backup RADIUS support
IP Address*	10.204.88.139
Port*	1812
Shared Secret*	••••••••
Confirm Secret*	••••••••
Retry Policy	
Request Timeout*	3 seconds
Max Number of Retries*	2 times

© 2018 by Pulse Secure, LLC. All rights reserved

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



Authentication/Accounting Servers

Authentication/Accounting Servers

This table lists all authentication mechanisms that can be used whenever authentication is needed.

□	Name	Type	Actions
□	10.204.88.141	RADIUS	Edit Clone
□	Len-Dev-PPS	RADIUS	Edit Clone
□	Coa	RADIUS Accounting	Edit Clone
□	10.204.88.139	RADIUS Accounting	Edit Clone

Editing (10.204.88.139)

Name	10.204.88.139
Type	○ Active Directory ○ LDAP ○ RADIUS ● RADIUS Accounting ○ TACACS+
Encryption	□ TLS
Backup RADIUS	□ Enable Backup RADIUS Accounting support
IP Address*	10.204.88.139
Port*	1813
Shared Secret*	••••••••
Confirm Secret*	••••••••
Retry Policy	
Request Timeout*	3 seconds
Max Number of Retries*	2 times

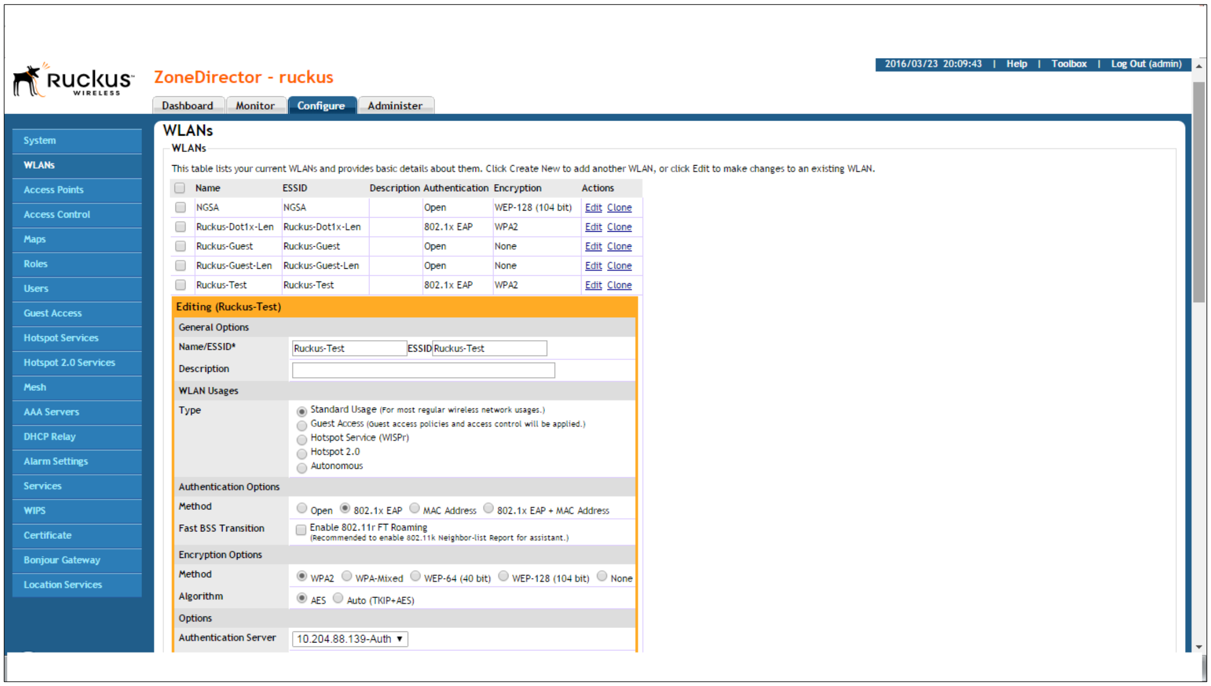
OK Cancel

□	Name	Type	Actions
□	Len-Dev-PPS-Acct	RADIUS Accounting	Edit Clone
□	Kajal-IC	RADIUS	Edit Clone
□	10.204.88.139-Auth	RADIUS	Edit Clone

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



WLANs

WLANs

This table lists your current WLANs and provides basic details about them. Click Create New to add another WLAN, or click Edit to make changes to an existing WLAN.

□	Name	ESSID	Description	Authentication	Encryption	Actions
□	NGSA	NGSA		Open	WEP-128 (104 bit)	Edit Clone
□	Ruckus-Dot1x-Len	Ruckus-Dot1x-Len		802.1x EAP	WPA2	Edit Clone
□	Ruckus-Guest	Ruckus-Guest		Open	None	Edit Clone
□	Ruckus-Guest-Len	Ruckus-Guest-Len		Open	None	Edit Clone
□	Ruckus-Test	Ruckus-Test		802.1x EAP	WPA2	Edit Clone

Editing (Ruckus-Test)

General Options

Name/ESSID*: Ruckus-Test ESSID Ruckus-Test

Description:

WLAN Usages

Type:
● Standard Usage (For most regular wireless network usages.)
○ Guest Access (Guest access policies and access control will be applied.)
○ Hotspot Service (WISPr)
○ Hotspot 2.0
○ Autonomous

Authentication Options

Method: ○ Open ● 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address

Fast BSS Transition: □ Enable 802.11r FT Roaming (Recommended to enable 802.11k Neighbor-list Report for assistant.)

Encryption Options

Method: ● WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ○ None

Algorithm: ● AES ○ Auto (TKIP+AES)

Options

Authentication Server: 10.204.88.139-Auth ▾

4. Save changes to **the settings.**