



# ExtremeWireless WiNG with Aruba ClearPass

**Abstract:** This document covers integration of ExtremeWireless WiNG with Aruba ClearPass Guest Manager functionality with Sponsored Guest Self-Registration login in combination with WiNG 5 Captive Portal.

Published: November 2016

Extreme Networks, Inc.  
145 Rio Robles  
San Jose, California 95134  
Phone / +1 408.579.2800  
Toll-free / +1 888.257.3000  
[www.extremenetworks.com](http://www.extremenetworks.com)

©2016 Extreme Networks, Inc. All rights reserved. Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. All other registered trademarks, trademarks, and service marks are property of their respective owners. For additional information on Extreme Networks trademarks, see [www.extremenetworks.com/company/legal/trademarks](http://www.extremenetworks.com/company/legal/trademarks).

# Contents

---

<b>Pre-Requisites .....</b>	<b>3</b>
<b>Overview .....</b>	<b>3</b>
<b>Part 1 - Configuring ClearPass to enable Sponsored Guest Registration.....</b>	<b>6</b>
Step 1 – Configure RADIUS Service Rules and Configure RADIUS Clients .....	6
Step 2 – Configure SMTP message delivery in Policy Manager .....	8
Step 3 – Configure Guest Login Settings .....	9
Step 4 – Enable Guest Registration and Sponsor Confirmation .....	11
Step 5 – Change default Guest Receipt format.....	14
<b>Part 2 – Configuring WiNG to Authenticate Guests to Aruba ClearPass.....</b>	<b>15</b>
Step 1 – Configure AAA Policy.....	15
Step 2 – Configure WiNG Captive Portal .....	18
Step 3 – Create Guest Wireless LAN .....	21
Step 4 – Assign WLAN to the Access Point Profile .....	23
Step 5 – Allow Guest VLAN on the GE1 port of the Access Point Profile .....	25
Step 6 – Assign Captive Portal Policy to the Access Point Profile .....	26
<b>Part 3 - Validation .....</b>	<b>27</b>
<b>Revision History .....</b>	<b>31</b>

## Pre-Requisites

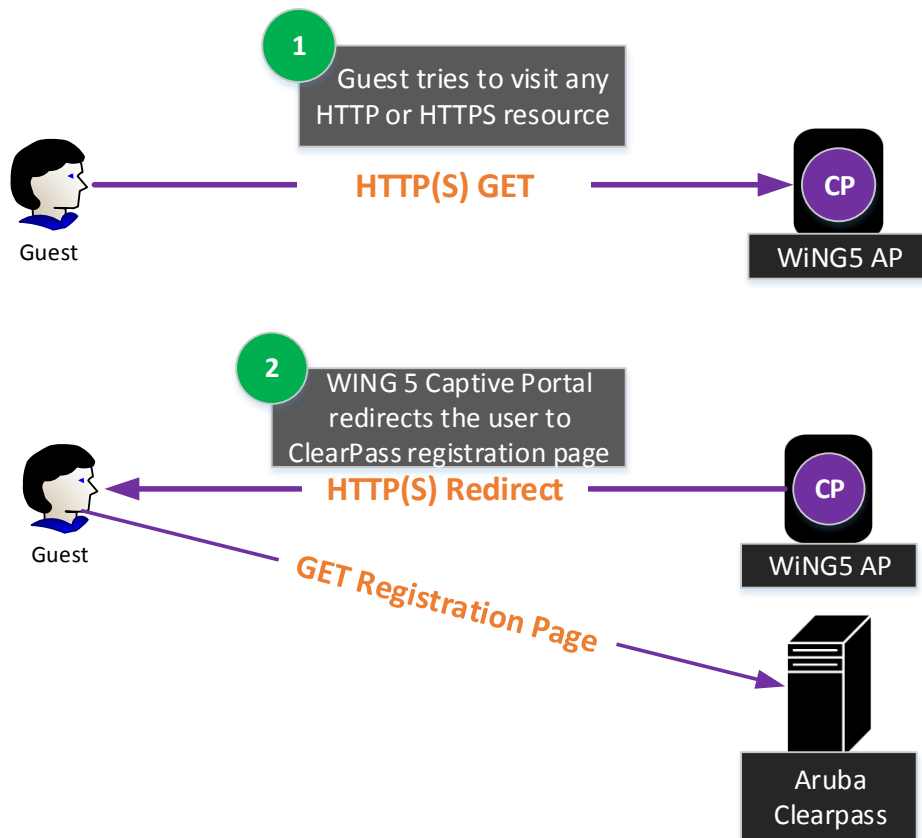
- WiNG firmware version 5.8.4.1-003R
- Aruba ClearPass Policy Manager version 6.6.0

## Overview

Aruba ClearPass allows guest users to register themselves by filling in the registration form with a sponsor email or phone number provided during registration. After guest user account is created a random username and passcode will be generated and an approval request sent to a sponsor specified during the registration.

Sponsor must confirm guest account in order to activate it. Upon account activation guest user will be allowed to log in via a captive portal using generated username and passcode.

Following diagram outlines Guest Registration and Authentication Flow:



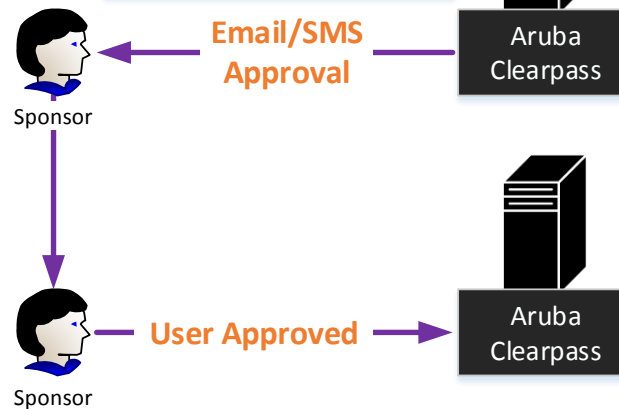
**3** User is presented with Clearpass Guest Self Registration Page

Please complete the form below to gain access to the network.

Visitor Registration	
* Sponsor's Email:	<input type="text"/> <small>Email of the person sponsoring this account.</small>
* Your Name:	<input type="text"/> <small>Please enter your full name.</small>
* Email Address:	<input type="text"/> <small>Please enter your email address. This will become your username to log into the network.</small>
* Confirm:	<input type="checkbox"/> I accept the terms of use
<b>Register</b>	

\* required field

**4** After registration submission, a sponsor will get an approval request to activate guest user account



**5** Upon Sponsor approval guest will receive notification that her account is ready



Guest

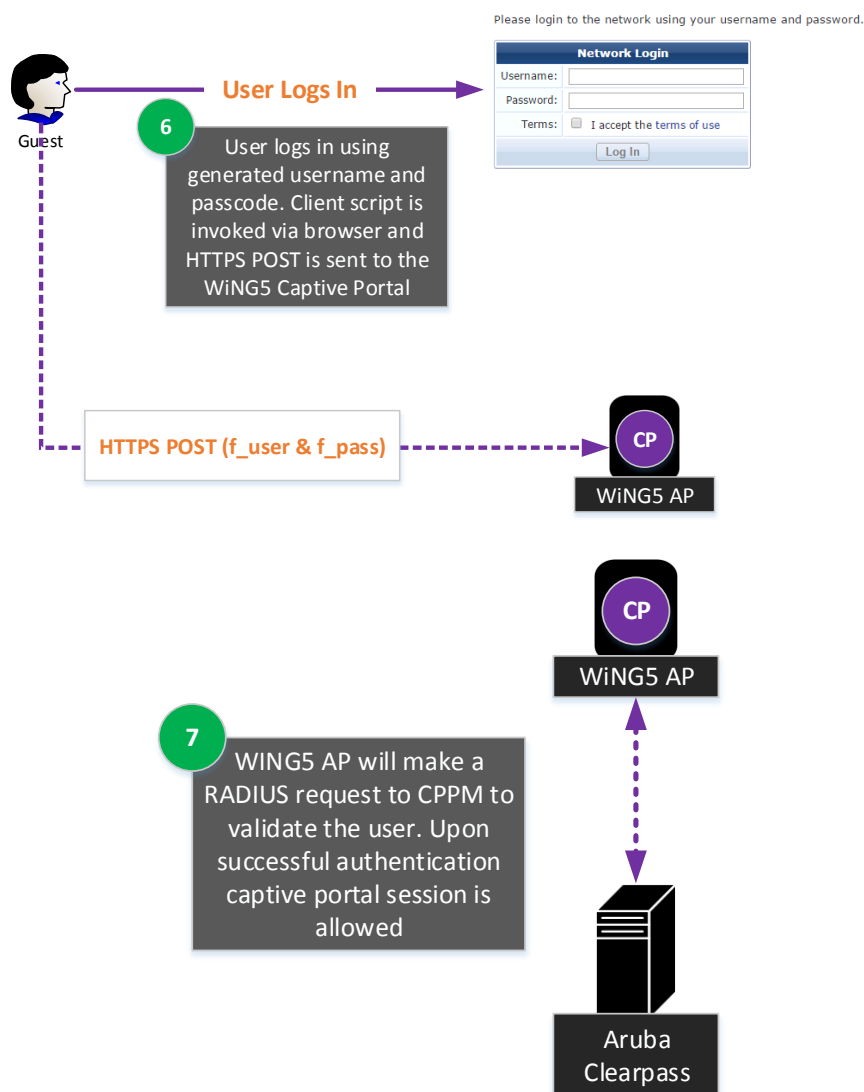
**Email / SMS Confirmation**



WiFi Network: CPPM

#### Guest Account and Wi-Fi Instructions:

- 1 Make sure your wireless adapter is set to dynamically obtain an IP address
- 2 Connect to the wireless network: **CPPM**
- 3 Enter credentials:
  - Username: **user0**
  - Password: **secret0**
- 4 Account expires: Saturday, November 26, 2016 22:56



# Part 1 - Configuring ClearPass to enable Sponsored Guest Registration

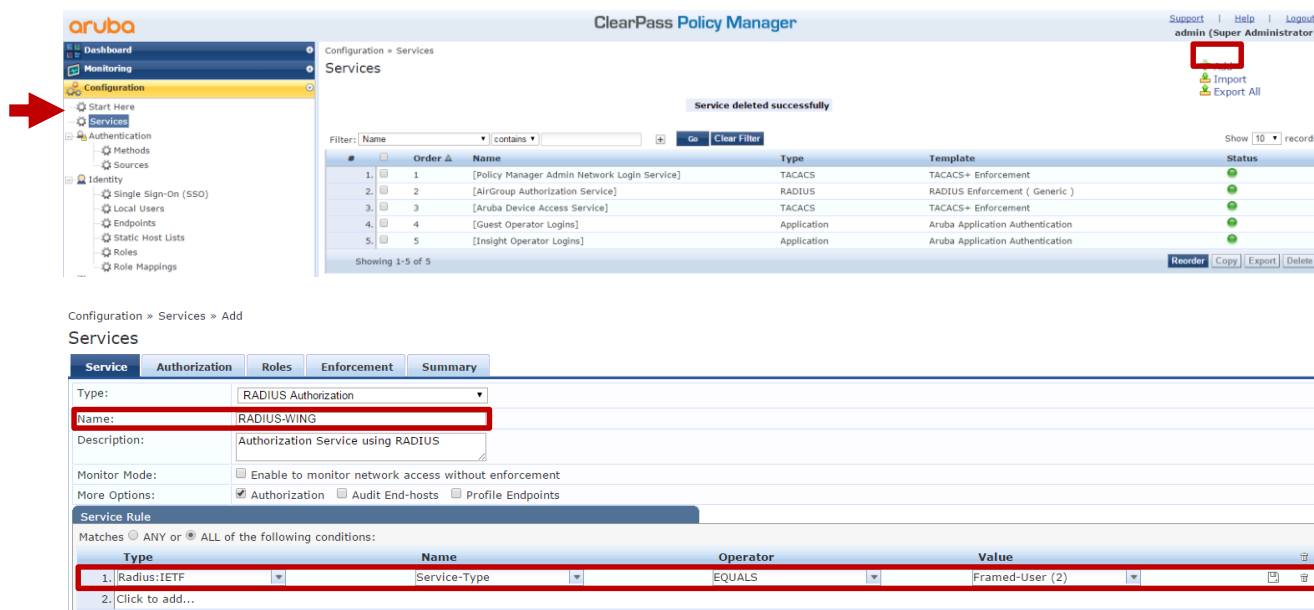
The configuration of ClearPass Policy manager consists of the following steps:

1. Configure RADIUS Service Rules and configure RADIUS Clients to allow WiNG Access Points to make RADIUS requests towards CPPM.
2. Configure SMTP message delivery in Policy Manager to allow sending guest receipts via email.
3. Configure Guest Registration login settings to allow integration with WiNG Captive Portal.
4. Enable Guest Registration and Sponsor confirmation
5. Change default guest receipt format.

## Step 1 – Configure RADIUS Service Rules and Configure RADIUS Clients

In order for ClearPass to allow RADIUS communication RADIUS service rules must be configured first, followed by RADIUS Client configuration.

RADIUS services can be configured under **Policy Manager → Configuration → Services** tab:



Configuration » Services » Add Services

**Service** | Authorization | Roles | Enforcement | Summary

Type: RADIUS Authorization

Name: RADIUS-WING

Description: Authorization Service using RADIUS

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☒ Authorization ☐ Audit End-hosts ☐ Profile Endpoints

**Service Rule**

Matches ANY or ALL of the following conditions:

Type	Name	Operator	Value
1. RADIUS:IETF	Service-Type	EQUALS	Framed-User (2)
2. Click to add...			

Configuration » Services » Add

## Services

Service **Authorization** Roles Enforcement Summary

Strip Username Rules: ☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

Authorization Details: Additional authorization sources from which to fetch role-mapping attributes -

[Guest User Repository] [Local SQL DB]

Remove View Details Modify

--Select to Add--

Next > **Save** Cancel

Next navigate to **Network → Devices** tab and create a new entry for WiNG Access Points. In this example an AP will make a RADIUS request directly to the CPPM without proxying it through the controller, hence we need to add a management subnet of the Access Points as a RADIUS Client identifier:

aruba ClearPass Policy Manager

Configuration » Network » Devices

Network Devices

Device deleted successfully

Filter: Name contains Go Clear Filter Show 10

#	Name	IP or Subnet Address	Description
Export			

Dashboard Monitoring Configuration

- Start Here
- Services
- Authentication
  - Methods
  - Sources
- Identity
  - Single Sign-On (SSO)
  - Local Users
  - Endpoints
  - Static Host Lists
  - Roles
  - Role Mappings
- Posture
- Enforcement
  - Policies
  - Profiles
- Network
  - Devices**
  - Device Groups
  - Proxy Targets
  - Event Sources

**Add Device**

Device SNMP Read Settings SNMP Write Settings CLI Settings

Name: WiNG-APs

IP or Subnet Address: 192.168.50.0/24 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)

Description:

RADIUS Shared Secret: ..... Verify: .....

TACACS+ Shared Secret: ..... Verify: .....

Vendor Name: Motorola

Enable RADIUS CoA: ☒ RADIUS CoA Port: 3799

Attributes

Attribute	Value
1. Click to add...	

Add Cancel

## Step 2 – Configure SMTP message delivery in Policy Manager

To allow ClearPass to send guest receipts information and notifications to guest users and sponsors, SMTP relay server must be configured.

Navigate to **Policy Manager** → **Administration** → **External Servers** → **Messaging Setup**:

aruba ClearPass Policy Manager

Support | Help | Logout  
admin (Super Administrator)

Administration » External Servers » Messaging Setup

Messaging

Configure SMTP mail server for email notifications :

SMTP Server

SMTP Settings

Server name:	<input type="text" value="smtp.upcmail.cz"/>	Connection Security:	<input type="text" value="None"/>
User Name:	<input type="text"/>	Port:	<input type="text" value="25"/>
Password:	<input type="password"/>	Connection timeout:	<input type="text" value="30"/> seconds
Verify Password:	<input type="password"/>		
Default From Address:	<input type="text" value="cpcp@upcmail.cz"/>		

Send Test Email Send Test SMS **Save**



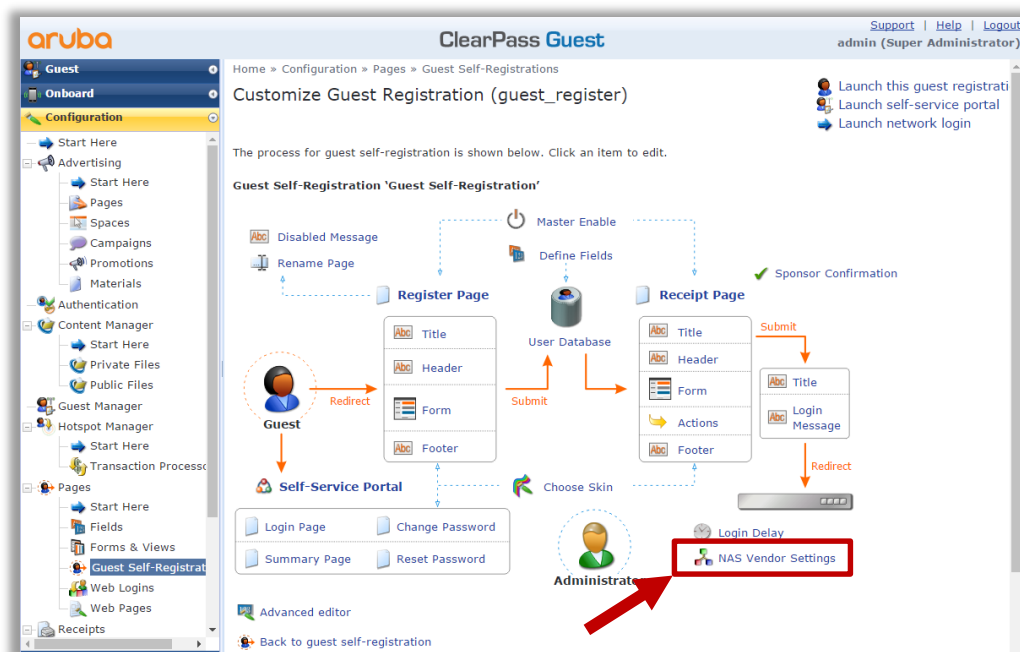
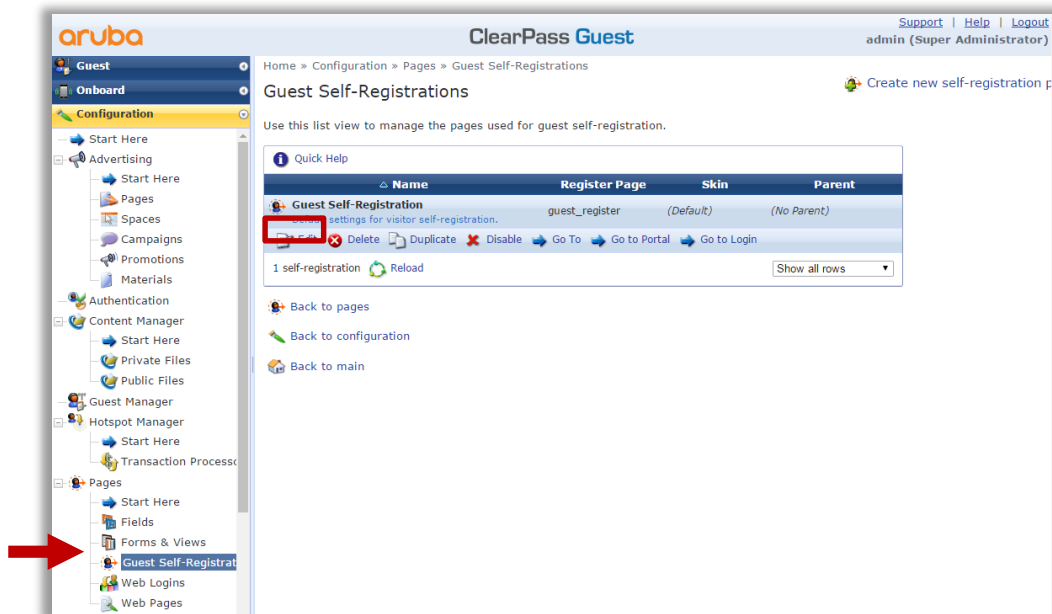
## Step 3 – Configure Guest Login Settings

In order to integrate CPPM Captive Portal with WiNG 5 Captive Portal it is necessary to configure Guest Login settings on Clearpass to invoke client-side php script to send HTTP POST to WiNG Captive Portal with username and password.

Login to Guest Manager UI by navigating to

[https://<ClearPass\\_IP\\_or\\_FQDN>/guest/guest\\_index.php](https://<ClearPass_IP_or_FQDN>/guest/guest_index.php)

Navigate to **Configuration → Pages → Self Registration → Guest Self Registration → Edit.**



IP Address field should be equal to the virtual FQDN configured under WiNG Captive Portal Policy:

Customize Guest Registration	
<b>Login</b> Options controlling logging in for self-registered guests.	
Enabled:	Enable guest login to a Network Access Server ▼
* Vendor Settings:	Motorola Select a predefined group of settings suitable for standard network configurations.
Login Method:	Controller-initiated — Guest browser performs HTTP form submit ▼ Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.
* IP Address:	captive.wingsecure.com Enter the IP address or hostname of the vendor's product here.
Secure Login:	Secure login using HTTPS ▼ Select a security option to apply to the web login process.
<b>Default Destination</b> Options for controlling the destination clients will redirect to after login.	
* Default URL:	http://www.extremenetworks.com Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	<input type="checkbox"/> Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.
<input type="button" value="Save Changes"/> <input type="button" value="Save and Continue"/>	

\* required field

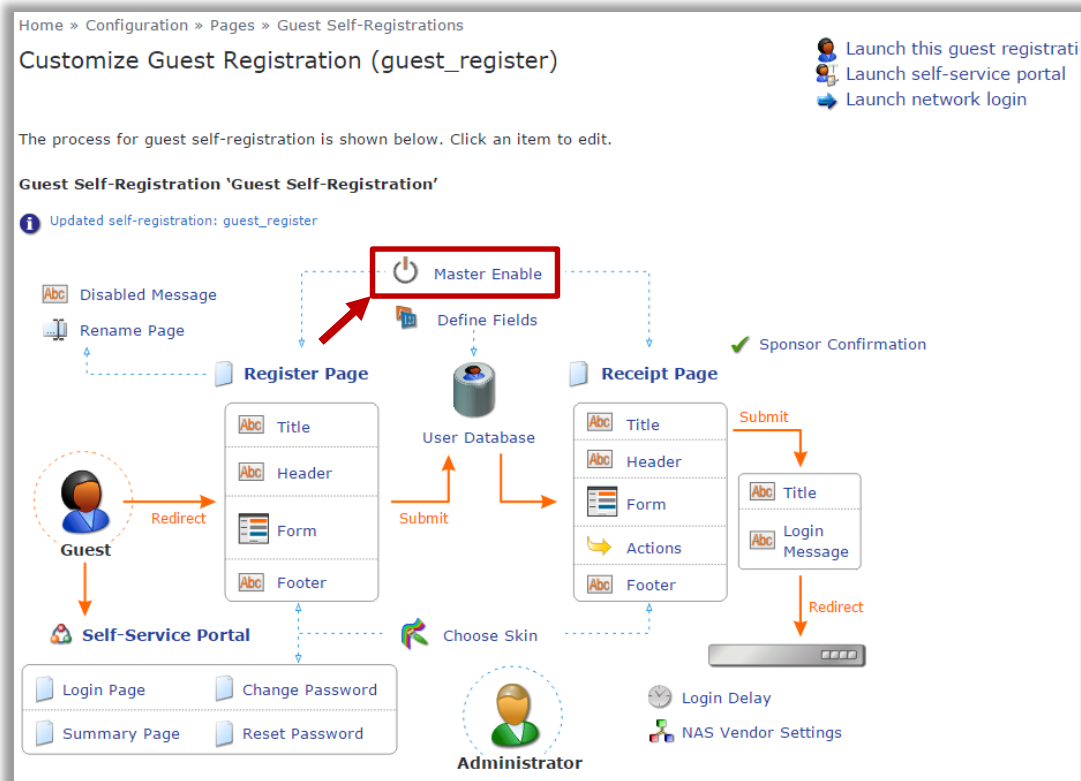
## Note

Currently a bug exists on ClearPass that does not allow to use HTTP connection mode of the Captive Portal, because it will continue to send HTTP POST to a secure port 444 using HTTP.

## Step 4 – Enable Guest Registration and Sponsor Confirmation

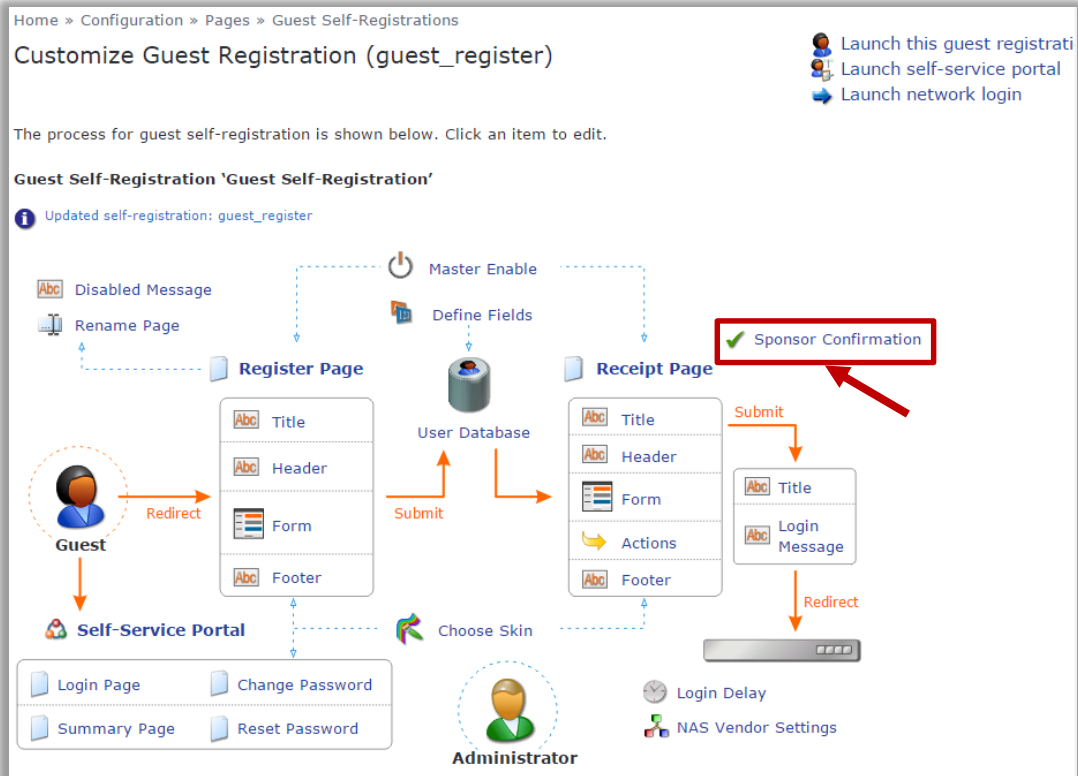
It is also necessary to globally enable guest registration, as well enforce sponsor confirmation for each guest user account created.

Navigate to **Configuration → Guest Self-Registration → Edit Guest Registration** template:



Customize Guest Registration	
<b>Basic Properties</b> Options controlling basic operation of guest self-registration.	
* Name:	Guest Self-Registration <small>Enter a name to identify the guest self-registration instance. This is visible only to administrators.</small>
Description:	Default settings for visitor self-registration. <small>Enter comments about this instance of guest self-registration. This is visible only to administrators.</small>
Enabled:	<input checked="" type="checkbox"/> Enable guest self-registration
* Register Page:	guest_register <small>Enter the base page name for the guest registration page.</small>
* User Database:	ClearPass Policy Manager <small>Self provisioned guest accounts are created using this service handler.</small>
* Skin:	ClearPass Guest Skin ▾ <small>Choose the skin for the self-registration pages.</small>
Prevent CNA:	<input checked="" type="checkbox"/> Enable bypassing the Apple Captive Network Assistant <small>The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.</small>
Advertising:	<input type="checkbox"/> Enable Advertising Services content

**Save Changes** **Save and Continue**



### Customize Guest Registration

#### Sponsorship Confirmation

Enabled: ☒ Require sponsor confirmation prior to enabling the account

Authentication: ☐ Require sponsors to provide credentials prior to sponsoring

If checked, the sponsor will need to successfully authenticate prior to approving the request. The sponsor's operator profile must have the Guest Manager > Remove Accounts privilege.

#### Email Delivery

\* Email Field: (Use Default: sponsor\_email)   
The field containing the sponsor's email address.

Email Confirmation: Sponsorship Confirmation   
The plain text or HTML print template to send to the sponsor.

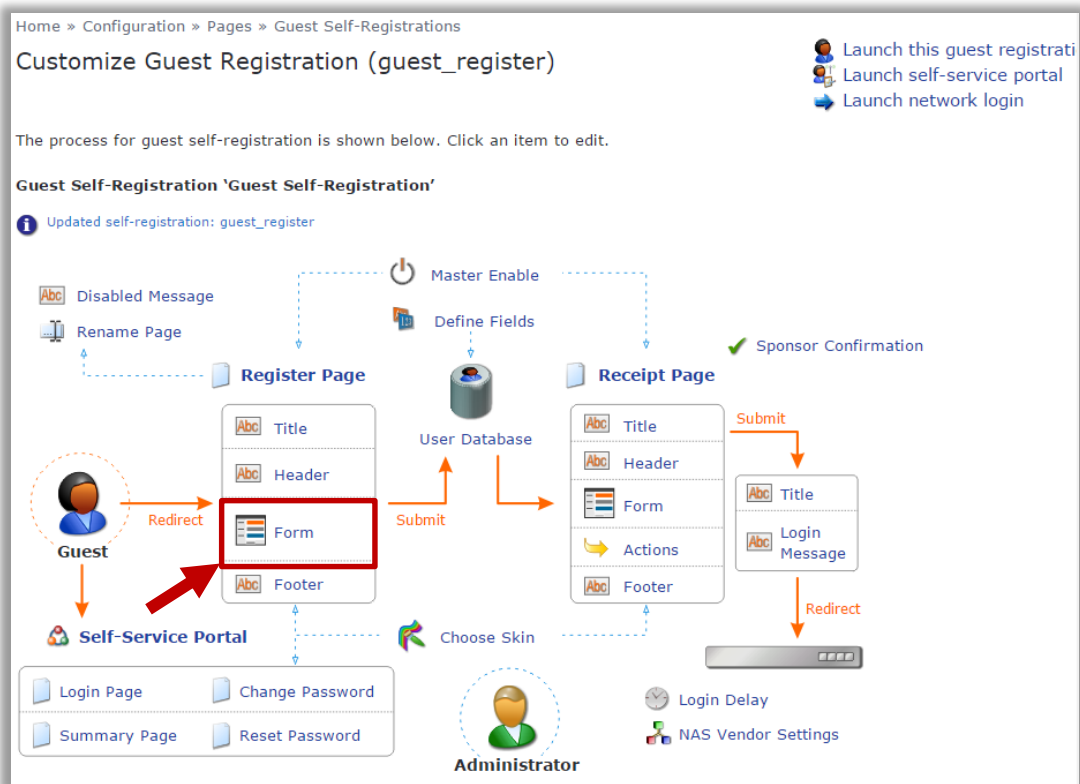
\* Email Skin: (Use Default: ClearPass Guest Skin)   
The format in which to send email receipts.

\* Send Copies: Do not send copies   
Specify when to send visitor account receipts to the recipients in the Copies To list.

Reply-To: ☐ Allow the reply-to address to be overridden   
If checked, the reply-to address will be overridden by the guest's email field.

**Save Changes** **Save and Continue**

## Enable Sponsor Email field for the Self Registration Page:



Quick Help Preview Form

Rank	Field	Type	Label	Description
10	sponsor_name	text	Sponsor's Name:	Name of the person sponsoring this account.
15	sponsor_email	text	Sponsor's Email:	Email of the person sponsoring this account.
	Edit	Edit Base Field	Remove	Insert Before  Insert After <b>Enable Field</b>
20	visitor_name	text	Your Name:	Please enter your full name.

## Step 5 – Change default Guest Receipt format

Under Guest UI view navigate to **Configuration → Guest Manager**. Change default Site SSID to the one currently used in production:

The screenshot displays the Aruba ClearPass Guest configuration interface. The left sidebar contains a navigation menu with the following items: Guest, Onboard, Configuration, Start Here, Advertising, Start Here, Pages, Spaces, Campaigns, Promotions, Materials, Authentication, Content Manager, Start Here, Private Files, Public Files, **Guest Manager** (highlighted with a red arrow), Hotspot Manager, Start Here, Transaction Process, Pages, Start Here, Fields, Forms & Views, Guest Self-Registration, Web Logins, Web Pages, Receipts, Start Here, and Digital Pass Template. The main content area is titled 'ClearPass Guest' and shows the 'Configuration' tab. The 'Receipt Options' section is expanded, and the 'Site SSID' field is highlighted with a red box, showing the value 'CPPM'. The 'Save Configuration' button at the bottom is also highlighted with a red box.

**Configuration**

**Guest Manager**

**Receipt Options**

Site SSID:   
The SSID of the wireless LAN, if applicable. This will appear on guest account print receipts.

**Save Configuration**

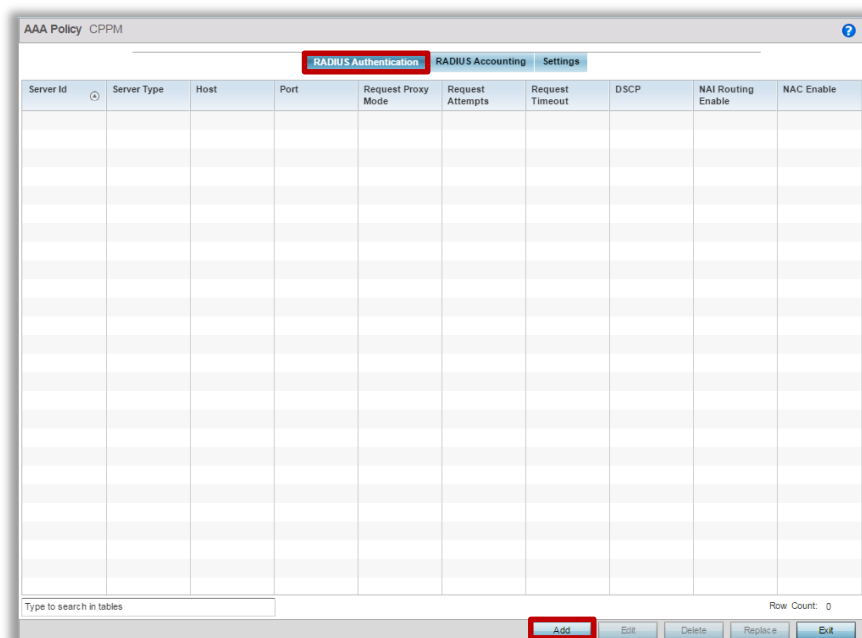
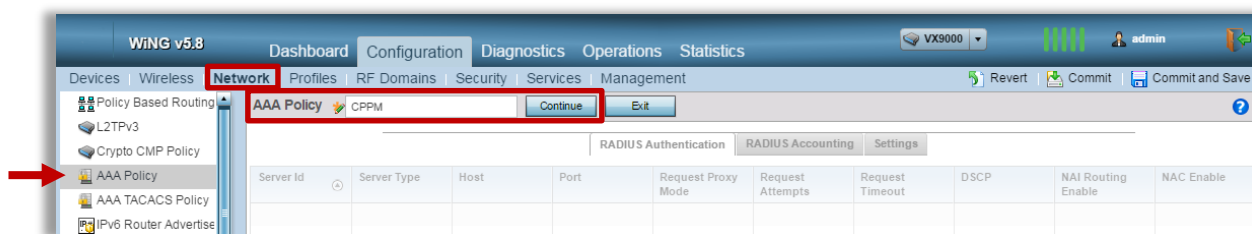
## Part 2 – Configuring WiNG to Authenticate Guests to Aruba ClearPass

The configuration of ExtremeWireless WiNG consists of the following steps:

1. Configure AAA Policy to specify CPPM as Authentication Server.
2. Configure WiNG Captive Portal to redirect guests to CPPM pages.
3. Create Guest Wireless LAN.
4. Assign WLAN to Access Point Profile.
5. Allow Guest VLAN on the AP GE1 port.
6. Assign Captive Portal Server to the AP Profile.

### Step 1 – Configure AAA Policy

Navigate to **Configuration → Network → AAA Policy → Add**:



Authentication Server

Server Id 1 (1 to 6)

Settings

Server Type Host

Host 192.168.10.135 IP Address

Port 1812 (1 to 65,535)

Secret wingsecure Show

Request Proxy Mode None

Proxy Mint Host

Request Attempts 3 (1 to 10)

Request Timeout 3 Seconds (1 to 60)

Retry Timeout Factor 100 (50 to 200)

DSCP 0 (0 to 63)

Network Access Identifier Routing

NAI Routing Enable

Realm

Realm Type Prefix Suffix

Strip Realm

OK Reset Exit

[illegible]



Accounting Server

Server Id 1 (1 to 6)

Settings

Server Type Host

Host 192.168.10.135 IP Address

Port 1813 (1 to 65,535)

Secret wingsecure Show

Request Proxy Mode None

Proxy Mint Host

Request Attempts 3 (1 to 10)

Request Timeout 5 Seconds (1 to 60)

Retry Timeout Factor 100 (50 to 200)

DSCP 34 (0 to 63)

Network Access Identifier Routing

NAI Routing Enable

Realm

Realm Type Prefix Suffix

Strip Realm

OK Reset Exit

AAA Policy CPPM

RADIUS Authentication RADIUS Accounting Settings

RADIUS Authentication

Protocol for MAC, Captive-Portal Authentication PAP CHAP MS-CHAP MS-CHAPv2 Cisco VSA Audit Session Id

RADIUS Accounting

Accounting Packet Type Start/Interim/Stop

Request Interval 30 Minutes (1 to 60)

Accounting Server Preference Prefer Same Authentication Server Host

RADIUS Address Format

Format Dash Delimiter (aa-bb-cc-dd-ee-ff)

Case Uppercase

Attributes Username / Password

Server Pooling

Server Pooling Mode Failover Load Balanced

EAPWireless Client Settings

Client Attempts 3 (1 to 10)

Request Timeout 3 (1 to 60 seconds)

ID Request Timeout 30 (1 to 60 seconds)

Retransmission Scale Factor 100 (50 to 200)

Access Request Attributes

Accounting Delay Time

Accounting Multi Session Id

Chargeable User Id

Add Framed IP Address

Framed MTU 1400 (100 to 1,500)

RFC5580 Location Information None

RFC5580 Operator Name

Service-Type framed

NAS IPv6 Address

Proxy NAS Identifier originator

Proxy NAS IPv4/IPv6 Address proxier

OK Reset Exit

Revert Commit Commit and Save

## Step 2 – Configure WiNG Captive Portal

Navigate to **Configuration → Services → Captive Portals**. Create new Captive Portal Policy to redirect Guests to CPPM server:

WiNG v5.8 Dashboard Configuration Diagnostics Operations Statistics

Devices | Wireless | Network | Profiles | RF Domains | Security | **Services** | Management

Captive Portals

Captive Portal Policy	Captive Portal Server Host	Captive Portal IPv6 Server	Captive Portal Server Mode	Hosting VLAN Interface	Connection Mode	Simultaneous Access	Web Page Source	AAA Policy
DEVICE-ONBOARD	capitive.zebranoc.com	Not Set	Internal (Self)	0	HTTPS	Not Set	Internal	ONBOARD-VX
Device-Registration	capitive.zebranoc.com	Not Set	Internal (Self)	0	HTTPS	Not Set	Internal	ONBOARD-VX
Z-GUEST	capitive.wingsecure.com	Not Set	Internal (Self)	0	HTTPS	Not Set	Internal	ONBOARD-VX

Row Count: 3

Add Edit Delete Copy Rename Replace

Captive Portal Policy CPPM

Basic Configuration Web Page

Settings

Captive Portal Server Mode ☒ Internal (Self) ☐ Centralized ☐ Centralized Controller

Hosting VLAN Interface 0 (0 to 4,096)

Captive Portal Server Host capitive.wingsecure.com

Captive Portal IPv6 Server ☐ IPv6

Connection Mode ☒ HTTP ☒ HTTPS

Simultaneous Access 1 (1 to 8,192)

Security

AAA Policy CPPM

Access

Access Type ☐ No authentication required ☒ RADIUS Authentication ☐ Registration ☐ E-mail Access ☐ Mobile Access ☐ Other Access

Terms and Conditions page ☒

Social Media Authentication

This feature requires access to the relevant websites. Please refer to the Help section for additional information.

Facebook ☐ Google ☐

OK Reset Exit

**Captive Portal Policy CPPM**

Basic Configuration | Web Page

**Bypass**

Bypass Captive Portal Detection ☐

**Client Settings**

Radius VLAN Assignment ☐

Post Authentication VLAN ☐ ID 1 (1 to 4,096) ☐ Alias S

Client Access Time  (10 to 10,080 minutes)



Inactivity Timeout  Hours (1 to 24)

**Loyalty App**

Enable ☐

App Name

**DNS Whitelist**

DNS Whitelist   

**Accounting**

Enable RADIUS Accounting ☐

Enable Syslog Accounting ☐

Syslog Host  Hostname

Syslog Port

**Data Limit**

Limit  (1 to 102,400 MegaBytes)

Action

**Logout FQDN**

Logout FQDN  (e.g., logout.guestaccess.com)

Localization

OK Reset Exit

Permit IP address or FQDN of the CPPM server in the DNS whitelist to allow client communication for initial registration and login:

**Name CPPM**

Whitelist Entries

DNS Entry	Match Suffix
★ 192.168.10.135	IPv4 Address No

+ Add Row

OK Reset Exit

Captive Portal Policy CPPM

Basic Configuration Web Page

Post Authentication VLAN ☐ ID 1 (1 to 4,096) ☐ Alias 5

Client Access Time 120 (10 to 10,080 minutes)

Inactivity Timeout 2 Hours (1 to 24)

Loyalty App

Enable ☐

App Name <none>

DNS Whitelist

DNS Whitelist CPPM

Accounting

Enable RADIUS Accounting ☒

Enable Syslog Accounting ☐

Syslog Host

Syslog Port 514

Data Limit

Limit 1 (1 to 102,400 MegaBytes)

Action Log Only

Logout FQDN

Logout FQDN (e.g., logout.guestaccess.com)

Localization

FQDN (e.g., local.guestaccess.com)

Response <local><site>WING\_TAG\_RF\_DC

Redirection Ports

Destination Ports for Redirection (e.g., 1080,8001,8080-8090)

OK Reset Exit

Captive Portal Policy CPPM

Basic Configuration Web Page

Web Page Source ☐ Internal ☐ Advanced ☒ Externally Hosted

Login URL	https://192.168.10.135/guest/guest_register_login.php?_browser=1	★
Agreement URL	https://192.168.10.135/guest/terms.php?_browser=1	★
Welcome URL	http://www.extremenetworks.com	★
Fail URL	https://192.168.10.135/guest/guest_register_login.php?_browser=1	★
Welcome Back URL	http://www.extremenetworks.com	★
No Service URL	https://192.168.10.135/guest/service_unavailable.php?_browser=1	★
Registration URL	https://192.168.10.135/guest/guest_register.php?_browser=1	★

A set of pre-existing web pages outside of the Controller are specified by the provided URLs.  
Four separate URLs point to external web pages for: Logging the user in, Welcoming the user after logging in successfully and Informing the user of a failed login attempt.

OK Reset Exit

Revert | Commit | Commit and Save

## Step 3 – Create Guest Wireless LAN

Navigate to **Configuration → Wireless → Wireless LANs**. Create a new Wireless LAN for Guest Users:

WiNG v5.8 Dashboard Configuration Diagnostics Operations Statistics

Devices **Wireless** Network Profiles RF Domains Security Services Management

Wireless LANs

WLAN	SSID	Description	WLAN Status	VLAN Pool	Bridging Mode	DHCP Option 82	DHCPv6 LDRA	Authentication Type	Encryption Type	QoS Policy	Association ACL
8021X	ZDemo-8021X		Enabled	100,200	Local	X	X	EAP	CCMP	default	
ccast	ccast		Enabled	1	Local	X	X	None	CCMP	default	
DEVICE-ONBOARD	DEVICE-ONBOARD	registration	Enabled	\$GUEST	Tunnel	X	X	MAC Address	None	default	
Guest-WiFi	Guest-WiFi	registration	Enabled	70	Tunnel	X	X	MAC Address	None	default	
MobilePSK	MobilePSK		Enabled	100	Local	X	X	None	CCMP	default	
peap	peap		Enabled	\$CORP-VLAN	Local	X	X	EAP	CCMP	default	
SecuredAccess	SecuredAccess		Enabled	10	Local	X	X	EAP	CCMP	default	
test	test		Enabled	\$TEST	Tunnel	X	X	None	CCMP	default	
tls	tls		Enabled	\$CORP-VLAN	Local	X	X	EAP-PSK	CCMP	default	

Row Count: 9

Add Edit Delete Copy Rename Replace

WLAN Configuration

SSID: CPPM

Description:

WLAN Status: Disabled Enabled

QoS Policy: default

Bridging Mode: Local

DHCP Option 82:

DHCPv6 LDRA:

Bonjour Gateway Discovery Policy: <none>

Other Settings

Broadcast SSID: ☒

Answer Broadcast Probes: ☒

VLAN Assignment

Single VLAN VLAN Pool

VLAN: 70

RADIUS VLAN Assignment

Allow RADIUS Override: ☐

URL Filter

URL Filter: <none>

OK Reset Exit

**WLAN CPPM**

Basic Configuration  
Security  
Firewall  
Client Settings  
Accounting  
Service Monitoring  
Client Load Balancing  
Advanced  
Auto Shutdown

Select Authentication

☐ EAP ☐ EAP-PSK ☐ EAP-MAC ☐ MAC ☒ PSK / None

AAA Policy

Reauthentication ☐ 30 (30 to 86,400)

Captive Portal

Enforcement ☒ Captive Portal Enable ☐ Captive Portal if Primary Authentication Fails

Captive Portal Policy

Passpoint Policy

Passpoint Policy

Registration

Type of Registration

Radius Group Name

Expiry Time  (1 to 43,800 hours)

Agreement Refresh  (0 to 144,000 minutes)

External Controller

Enable ☐

Host  Hostname

Proxy Mode

OK Reset Exit

**WLAN CPPM**

Basic Configuration  
Security  
Firewall  
Client Settings  
Accounting  
Service Monitoring  
Client Load Balancing  
Advanced  
Auto Shutdown

Protected Management Frames (802.11w)

Mode ☒ Disabled ☐ Optional ☐ Mandatory

SA Query Attempts  (1 to 10)

SA Query Retry Timeout  (100 to 1,000 milliseconds)

Advanced RADIUS Configuration

NAS Identifier

NAS Port

☒ RADIUS Dynamic Authorization

Radio Rates

Rates for 2.4 GHz WLAN  Select

Rates for 5 GHz WLAN  Select

Transition

Fast BSS Transition ☐

Fast BSS Transition Over DS ☒

HTTP Analysis

Enable ☐

Filter

Filter Out Images ☐

Filter Post ☐

Strip Query String ☐

Forward To Syslog Server

Enable ☐

Host  Hostname

OK Reset Exit



Revert



Commit



Commit and Save

## Step 4 – Assign WLAN to the Access Point Profile

Go to **Configuration → Profiles → <Select AP Profile> → Edit → Interface → Radios → Edit**:

The screenshot shows the WiNG v5.8 Configuration interface. The left sidebar has a red arrow pointing to the 'Radios' tab under the 'Interface' section. The main area displays a table of radios for profile REMOTE-AP8533. The 'radio2' row is highlighted with a red border.

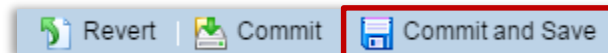
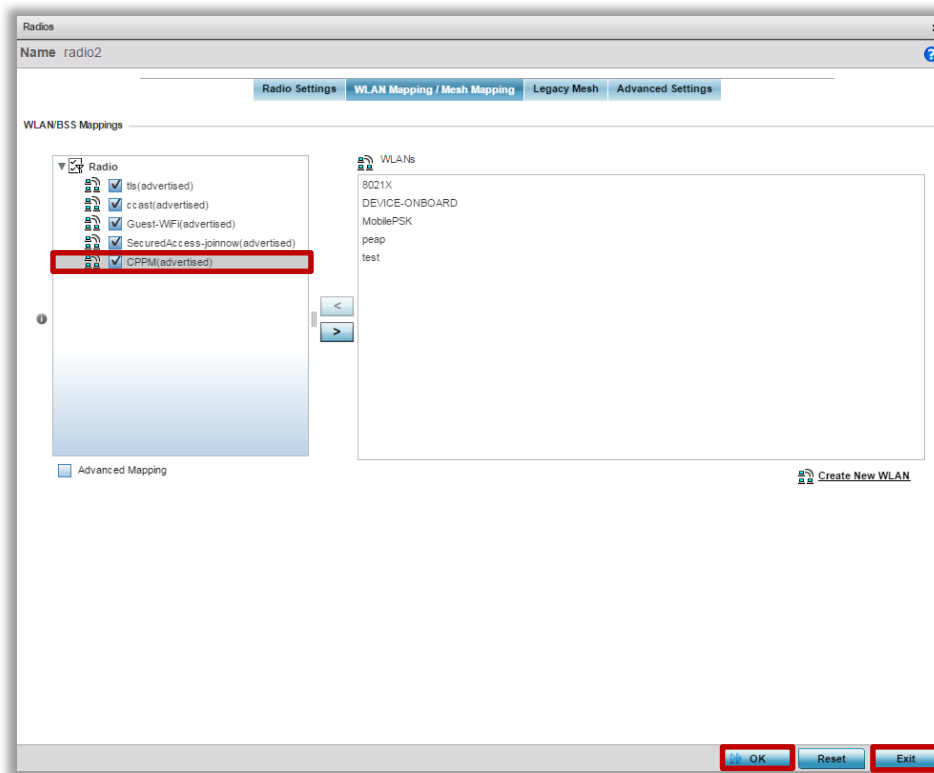
Name	Type	Description	Admin Status	RF Mode	Channel	Transmit Power
radio1	Radio	radio1	Enabled	2.4 GHz WLAN	smart	smart
radio2	Radio	radio2	Enabled	5 GHz WLAN	smart	smart
radio3	Radio	radio3	Enabled	Sensor	smart	smart

At the bottom right, the 'Edit' button is highlighted with a red border.

The screenshot shows the 'Radios' configuration window for 'radio2'. The 'WLAN Mapping / Mesh Mapping' tab is selected in the top bar. The 'WLAN Mapping / Mesh Mapping' section is active, showing a list of WLANs on the right. The 'radio2' row is highlighted in the main table.

WLANs
8021X
CPPM
DEVICE-ONBOARD
MobilePSK
peap
test

At the bottom right, the 'Exit' button is highlighted with a red border.





## Step 5 – Allow Guest VLAN on the GE1 port of the Access Point Profile

Within the Access Point Profile navigate to **Interface** → **Ethernet Ports** → **ge1** → **Edit**.

Ethernet Ports

Name ge1

Basic Configuration Security Spanning Tree

Properties

Description

Admin Status ☐ Disabled ☒ Enabled

Speed

Duplex

Switching Mode

Mode ☐ Access ☒ Trunk

Native VLAN  (1 - 4094)

Tag Native VLAN

Allowed VLANs  (1 - 4094) (2,4,7-12,...)

CDP/LLDP

Cisco Discovery Protocol Receive ☒

Cisco Discovery Protocol Transmit ☒

Link Layer Discovery Protocol Receive ☒

Link Layer Discovery Protocol Transmit ☒

Captive Portal Enforcement

Enforce captive portal

Port Channel Membership

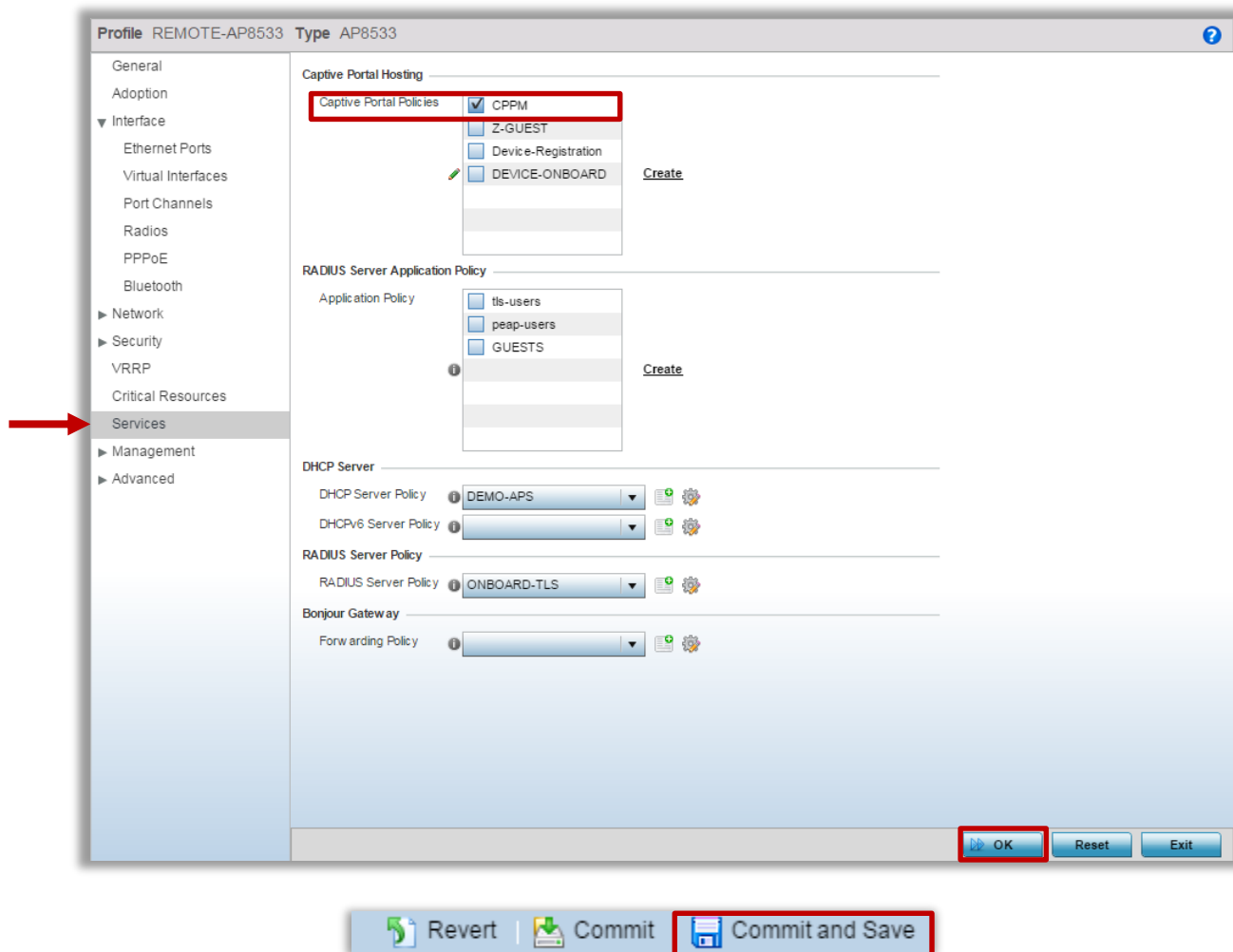
Port Channel  (1 to 4)

OK Reset Exit

Revert | Commit | Commit and Save

## Step 6 – Assign Captive Portal Policy to the Access Point Profile

Inside the AP Profile go to **Services** and assign Captive Portal Policy in order to start the hotspot service:



## Part 3 - Validation

Validation is performed by associating a client device to the Guest SSID and verifying that a network connectivity is established. Upon association automatic popup should appear redirecting to the ClearPass Login page:

Network Login

Username:

Password:

Terms: ☐ I accept the terms of use

Log In

Need an account? **Click Here**

Guest needs to register using the registration form and provide a Sponsor Email Address:

Please complete the form below to gain access to the network.

**Visitor Registration**

\* Sponsor's Email:   
Email of the person sponsoring this account.

\* Your Name:   
Please enter your full name.

\* Email Address:   
Please enter your email address.  
This will become your username to log into the network.

\* Confirm: ☒ I accept the terms of use

**Register**



\* required field

Already have an account? [Sign In](#)

After the registration the auto generated Username and Password will appear on the Receipt Page, however the “**Log In**” button will be grayed out before Sponsor approves an account:

The details for your guest account are shown below.

Your account is currently awaiting confirmation. This page will refresh every 30 seconds.

Visitor Registration Receipt	
Sponsor's Email:	vdementyev@extremenetworks.com
Guest's Name:	John
Account Username:	 john@mail.com
Guest Password:	 520523
Activation Time:	Sunday, 20 November 2016, 2:03 PM
Expiration Time:	Monday, 21 November 2016, 2:03 PM
Account Status:	Disabled
<input type="button" value="Log In"/>	

A sponsor will meanwhile receive an approval request via Email:

## A guest is requesting visitor access

### GuestManager Receipt

#### Your Account Details


Username: john@mail.com

Full Name: John

Phone:



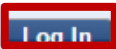
A visitor has requested access naming you as the sponsor. Please [click here](#) to confirm the request.

A guest has requested your confirmation for guest access

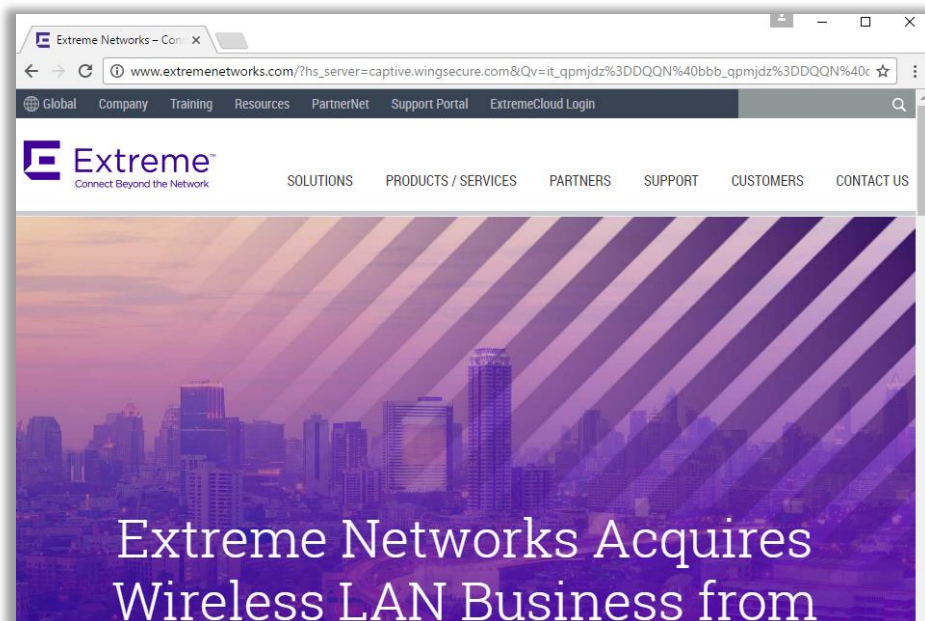
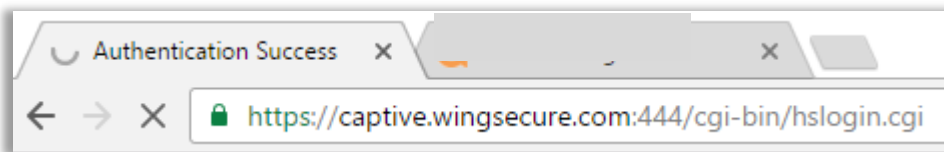
Visitor Registration Receipt	
Sponsor's Email:	vdementyev@extremenetworks.com
Guest's Name:	John
Account Username:	 john@mail.com
Activation Time:	Sunday, 20 November 2016, 2:03 PM
Expiration Time:	Monday, 21 November 2016, 2:03 PM
<input checked="" type="button" value="Confirm"/> <input type="button" value="Reject"/>	

After Sponsor will confirm Guest Registration “**Log In**” button will become active for the Guest and additional notification will be sent out:

The details for your guest account are shown below.

Visitor Registration Receipt	
Sponsor's Name:	admin
Sponsor's Email:	vdementyev@extremenetworks.com
Guest's Name:	John
Account Username:	 <b>john@mail.com</b>
Guest Password:	 <b>520523</b>
Activation Time:	Sunday, 20 November 2016, 2:03 PM
Expiration Time:	Monday, 21 November 2016, 2:03 PM
Account Status:	Enabled
	

After clicking “**Log In**” client will automatically submit username and password and will send an HTTPS POST to WiNG Captive Portal, so an Access Point will initiate a RADIUS request to CPPM. After Successful authentication client will be redirected to the Welcome Page configured on the Captive Portal:



On WiNG Client Statistics (**Statistics** → **<RF Domain>** → **Wireless Clients** → **<Select Your Client>**) you can see current Captive Portal authentication state and guest username:

Statistics

Wireless Client9C-D3-6D-98-7F-05

Health

Details

Traffic

WMM TSPEC

Association History

Graph

Wireless Client

MAC Address	9C-D3-6D-98-7F-05
Hostname	DESKTOP-S1GKDEP
Vendor	Netgear Inc
State	Data-Ready
IP Address	192.168.70.164
WLAN	CFPM
Radio MAC	74-67-F7-75-E4-ED
VLAN	70

User Details

UserName	john@mail.com
Authentication	none
Encryption	none
Captive Portal Auth.	✔ Yes

RF Quality Index

RF Quality Index	✔ 89 (Good)
Average Retry Number	0
SNR	36
Signal	-56
Noise	-92
Error Rate	0

Association

AP Hostname	8533-brq-2
AP	74-67-F7-5C-42-DA
Radio	8533-brq-2-R1
Radio Id	<u>74-67-F7-5C-42-DA-R1</u>
Radio Number	1
Band	11bgn

Parameter	Transmit	Receive
Total Bytes	469,202,626	1,071,711,710
Total Packets	763,613	1,331,146
User Data Rate	0	0
Physical Layer Rate	120	144
Tx Dropped Packets	65	
Rx Errors		0

Refresh

Exit

It is also possible to see current active Captive Portal sessions under the RF Domain statistics:

RF Domain <span>tmelabs-cz</span>								
	Client MAC	Hostname	Client IP	Captive Portal	Authentication	WLAN	VLAN	Remaining Time
Health	9C-D3-6D-98-7F-05	DESKTOP-S1GKDEP	192.168.70.164	CPPM	Success	CPPM	70	1h 9m 45s
Inventory								
Devices								
AP Detection								
Wireless Clients								
Device Upgrade								
Wireless LANs								
Radios								
Bluetooth								
Mesh								
Mesh Point								
SMART RF								
WIPS								
Captive Portal								
Application Visibility (AVC)								
Coverage Hole Detection								

## Revision History

---

Date	Revision	Changes Made	Author
11/20/2016	1.0	Initial Revision	Viacheslav Dementyev