WiNG 5 Captive Portal

Device Self Registration

Published: April 2017

Extreme Networks, Inc.
Phone / +1 408.579.2800
Toll-free / +1 888.257.3000

www.extremenetworks.com

P/N XXXXX-XX

Contents

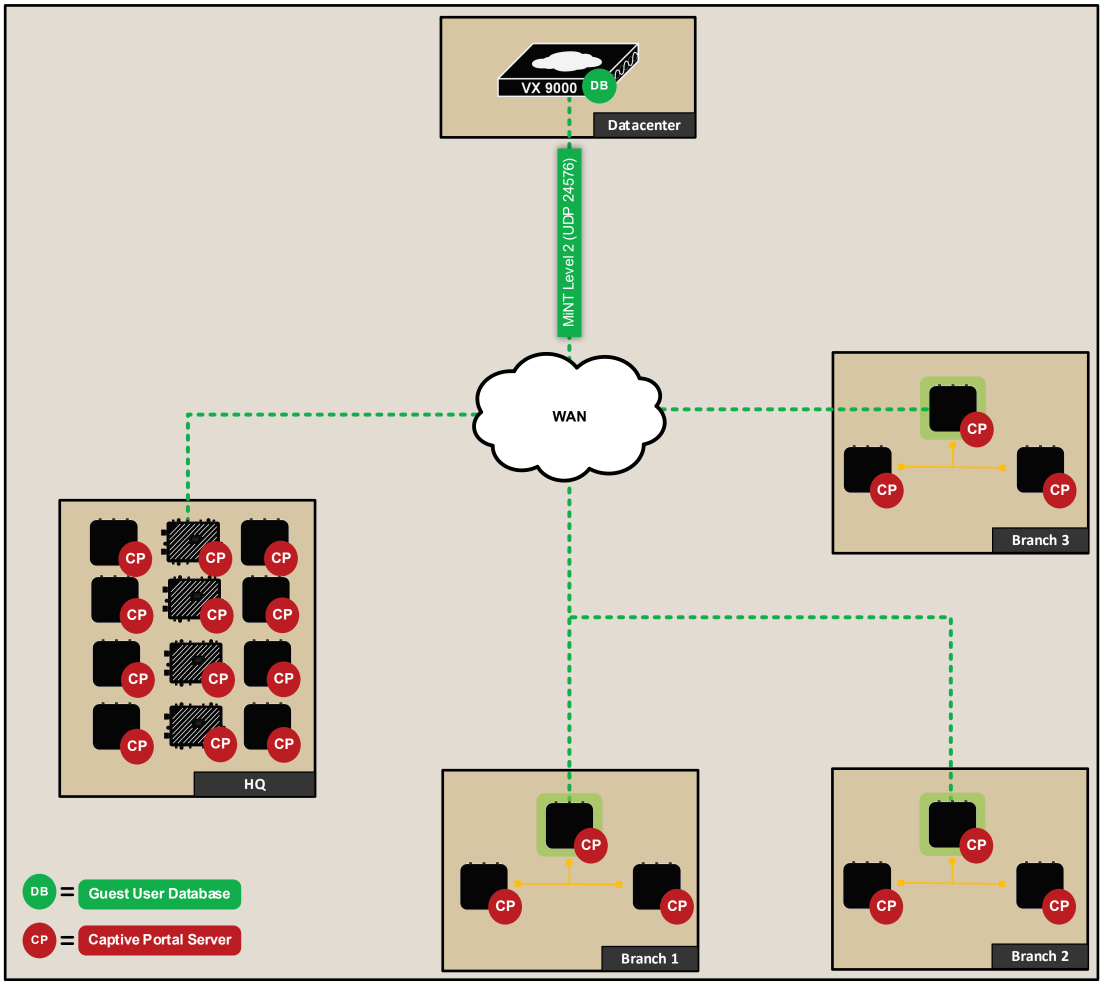
Overview

WiNG 5.8 release brought in a new Guest Self Registration functionality along with Guest User analytics included into some of the top WiNG 5 Controllers – NX7500, NX9XX0 and VX9000. Guest Self Registration allows guest users to register via a simple onboarding process using a HTML form or via social media profiles like Facebook or Google+. After registration a guest user record is created which allows for a seamless mobility between the APs or even locations without prompting a user for login or registration anymore.

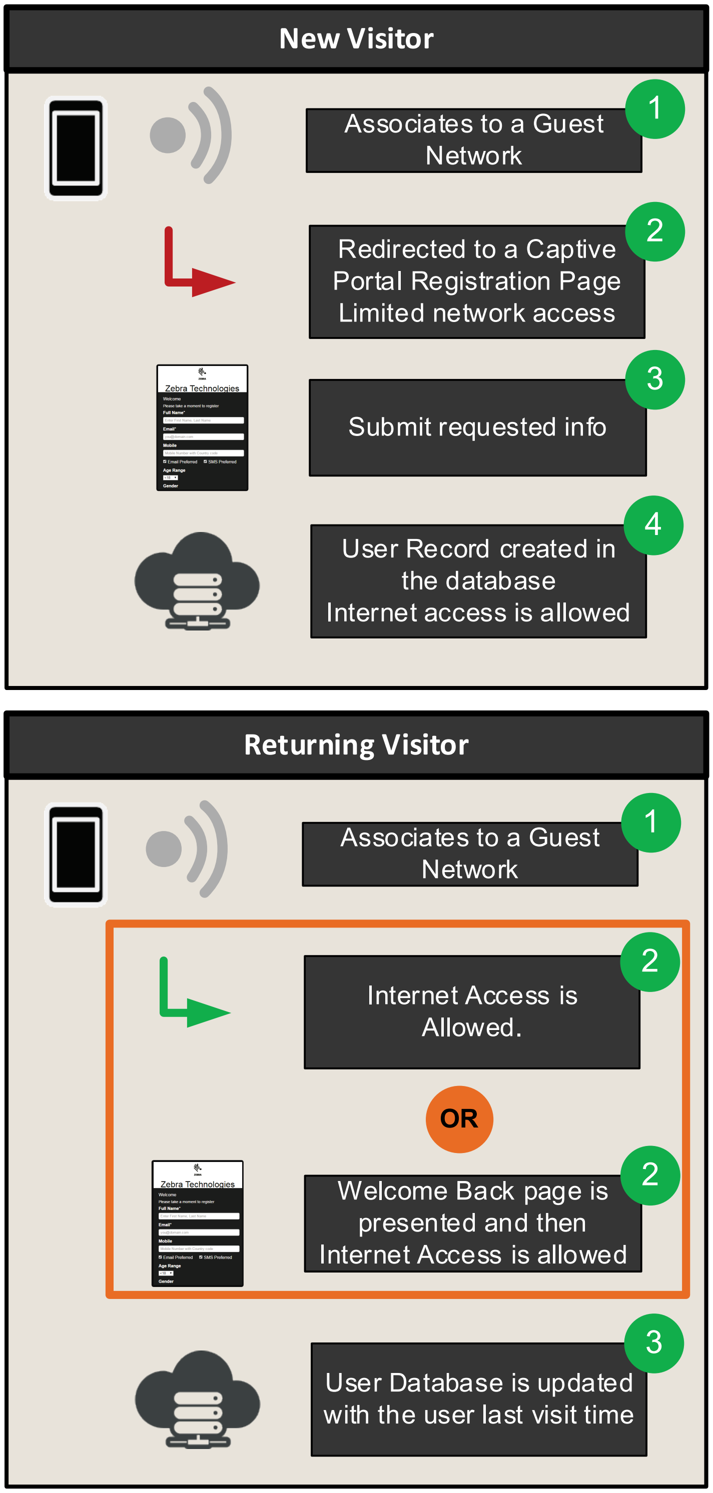
This functionality comes out of the box with no additional licensing required.

Multiple use-cases and registration flows are available. This HowTo guide will focus on one specific use case where guest users will register using an HTML form without any data validation. This is a supplemental guide to the general "*WiNG5 How To Captive Portals*"guide, which is a recommended pre-requisite to this document.

Topology



Device Registration Flow



New Visitor

1 Associates to a Guest Network

2 Redirected to a Captive Portal Registration Page
Limited network access

3 Submit requested info

4 User Record created in the database
Internet access is allowed

Returning Visitor

1 Associates to a Guest Network

2 Internet Access is Allowed.

OR

2 Welcome Back page is presented and then Internet Access is allowed

3 User Database is updated with the user last visit time

Configuration

Components

In order to complete the configuration as quickly as possible the following configuration order is recommended:

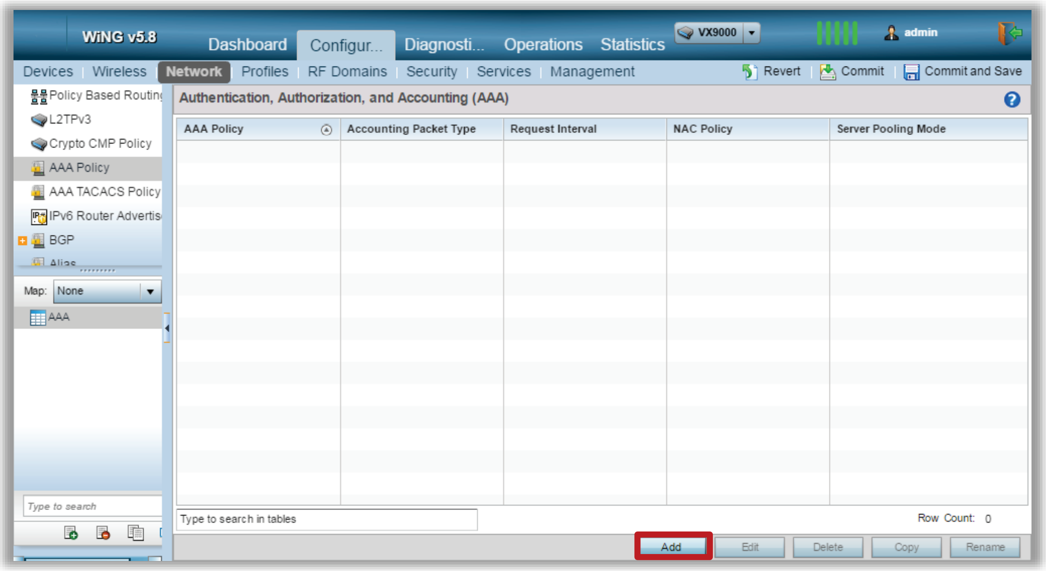
- AAA Policy
- RADIUS Server Policy
- Database Server
- Captive Portal Policy
- Wireless LAN

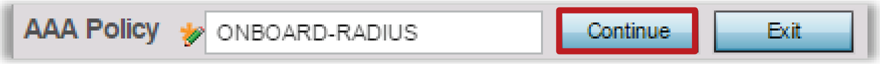
Configuration – AAA Policy

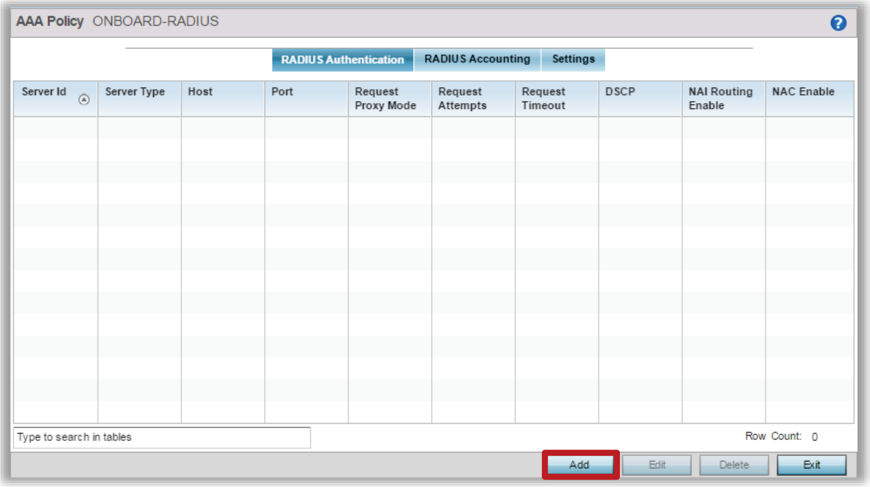
The AAA Policy in device registration scenario will point to the onboard RADIUS server running on a centralized controller that supports guest registration database (NX75XX, NX9XX0, VX9000). This AAA Policy will be used by both Captive Portal Policy to specify device registration server, as well as by the Wireless LAN to perform initial MAC authentication to determine device record presence.

AAA Policy Configuration – Web UI

Configuration -> Network -> AAA Policy -> Add:



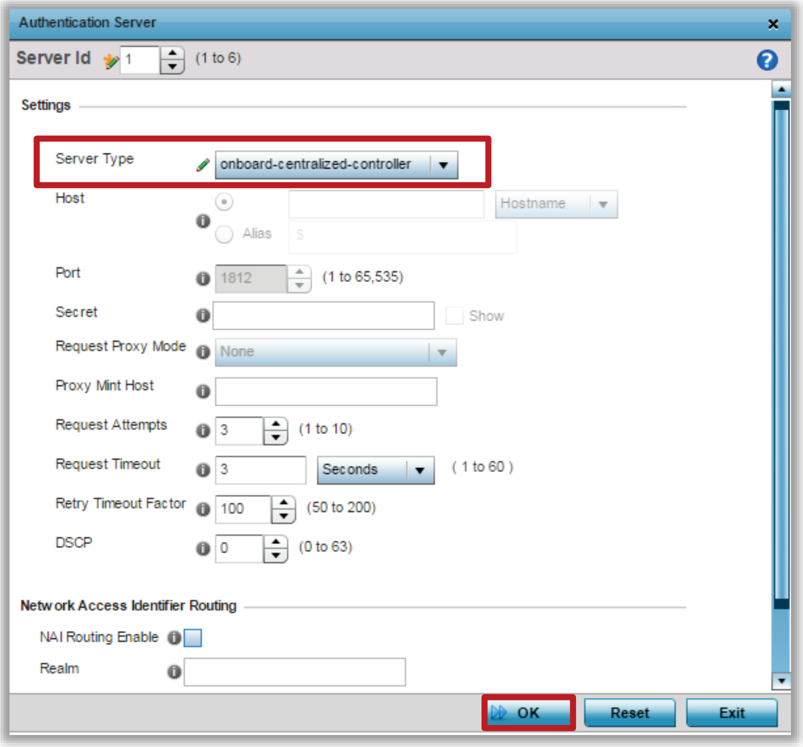

AAA Policy: ONBOARD-RADIUS



AAA Policy ONBOARD-RADIUS

Server Id	Server Type	Host	Port	Request Proxy Mode	Request Attempts	Request Timeout	DSCP	NAI Routing Enable	NAC Enable

Row Count: 0



Authentication Server

Server Id 1 (1 to 6)

Settings

Server Type: onboard-centralized-controller

Host: ○ ○ Alias $

Port: 1812 (1 to 65,535)

Secret: □ Show

Request Proxy Mode: None

Proxy Mint Host:

Request Attempts: 3 (1 to 10)

Request Timeout: 3 Seconds (1 to 60)

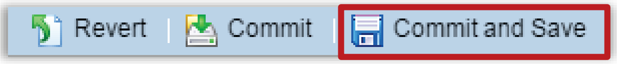
Retry Timeout Factor: 100 (50 to 200)

DSCP: 0 (0 to 63)

Network Access Identifier Routing

NAI Routing Enable: □

Realm:



AAA Policy Configuration – CLI

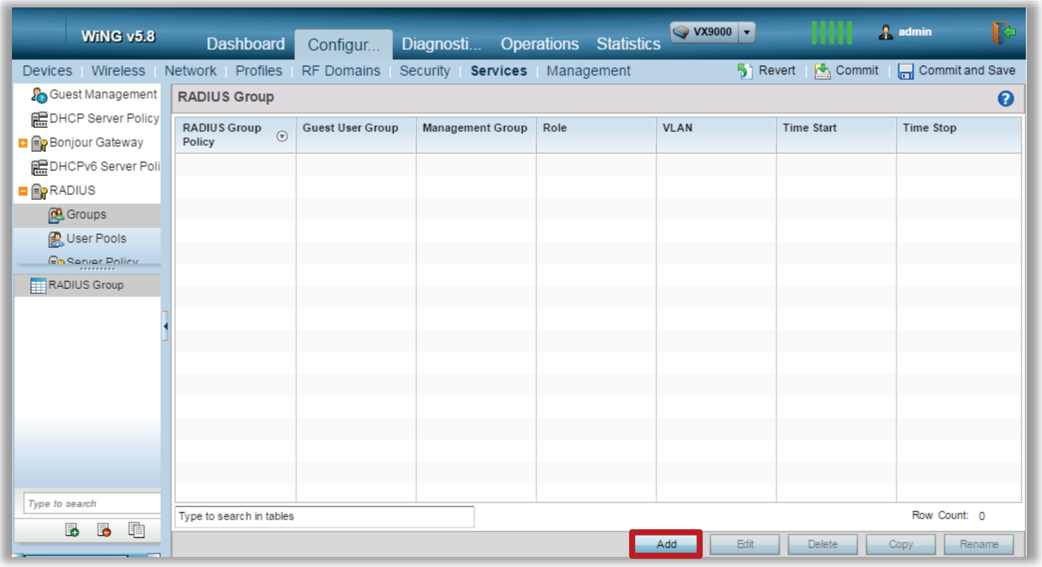
```
!
aaa-policy ONBOARD-RADIUS
 authentication server 1 onboard centralized-controller
!
```

Configuration – RADIUS Server Policy

RADIUS Server running on the centralized controller will provide an interface for the AP to communicated with the device registration database. RADIUS Group must be created for the registered devices, as well as the RADIUS Server policy in order to start the RADIUS service. RADIUS Group can optionally be limited for clients associated to a certain SSID to add additional security.

RADIUS Server Configuration – Web UI

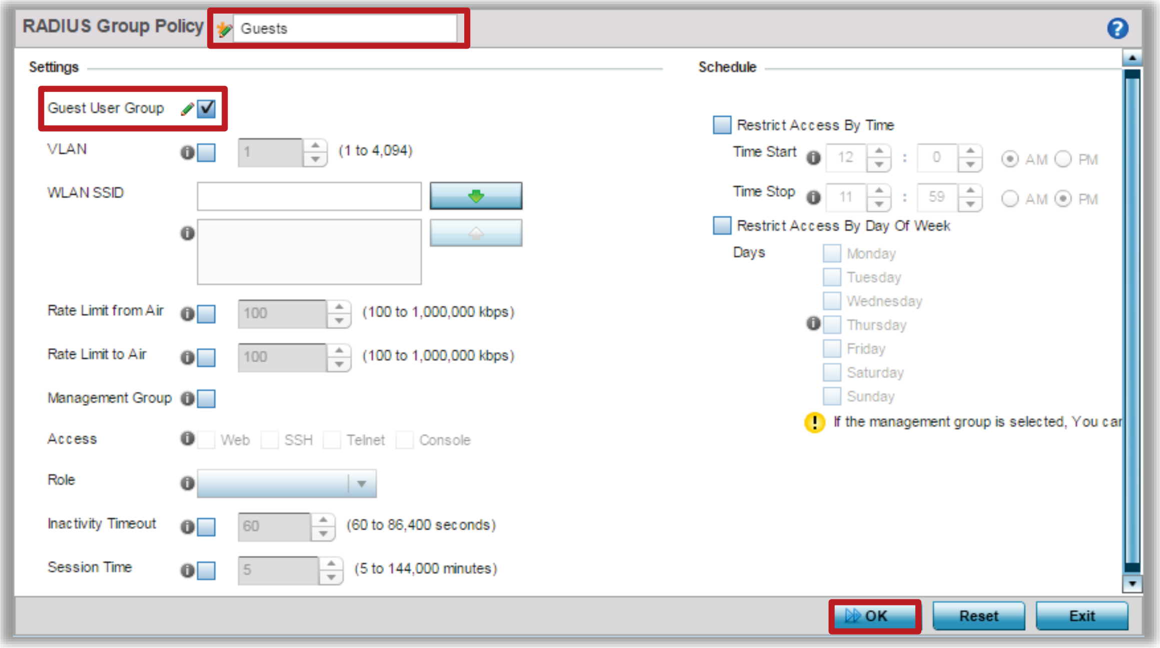
Configuration -> Services -> RADIUS -> Groups -> Add:



RADIUS Group

RADIUS Group Policy	Guest User Group	Management Group	Role	VLAN	Time Start	Time Stop

Row Count: 0



RADIUS Group Policy: Guests

Settings

Guest User Group ☑

VLAN □ 1 (1 to 4,094)

WLAN SSID

Rate Limit from Air □ 100 (100 to 1,000,000 kbps)

Rate Limit to Air □ 100 (100 to 1,000,000 kbps)

Management Group □

Access □ Web □ SSH □ Telnet □ Console

Role

Inactivity Timeout □ 60 (60 to 86,400 seconds)

Session Time □ 5 (5 to 144,000 minutes)

Schedule

□ Restrict Access By Time

Time Start 12 : 0 ● AM ○ PM

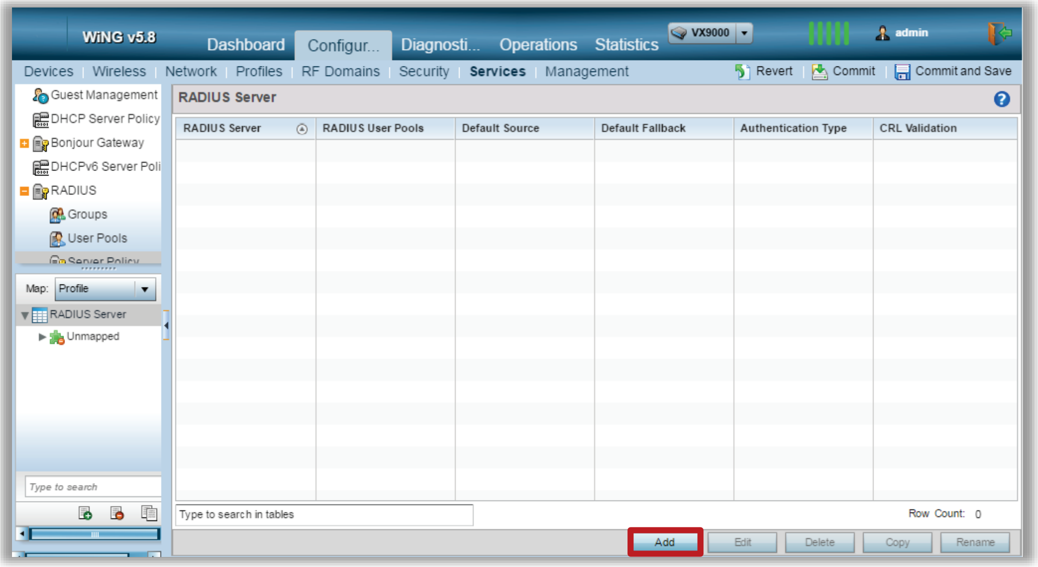
Time Stop 11 : 59 ○ AM ● PM

□ Restrict Access By Day Of Week

Days □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

If the management group is selected, You car

Configuration -> Services -> RADIUS -> Server Policy -> Add:

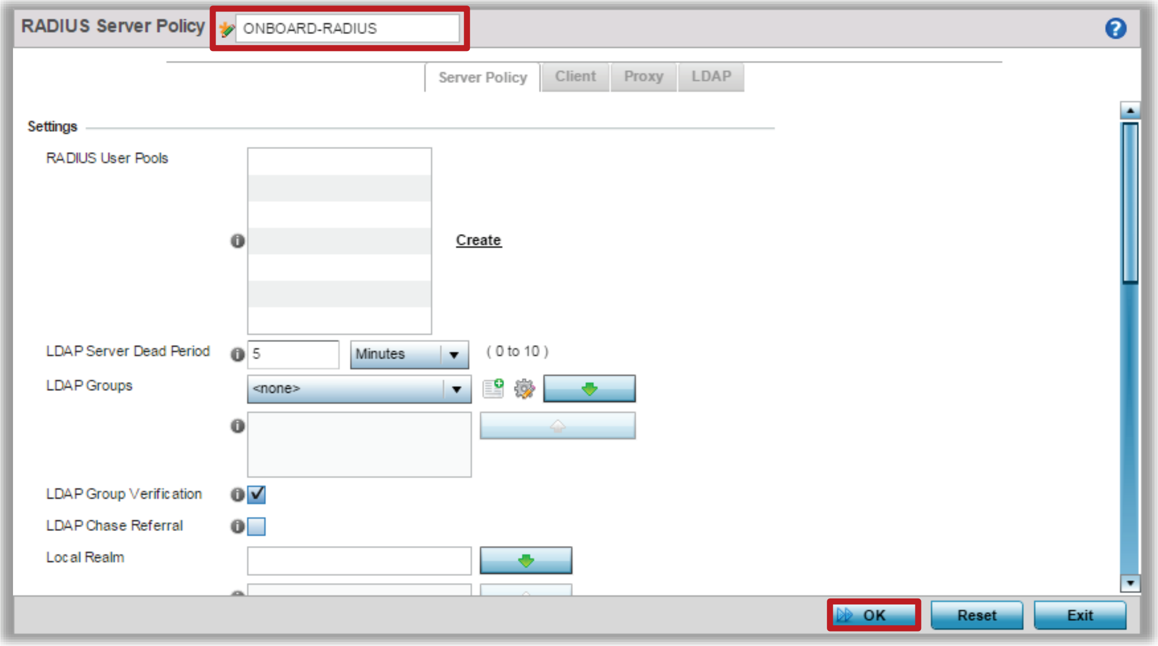


RADIUS Server

RADIUS Server	RADIUS User Pools	Default Source	Default Fallback	Authentication Type	CRL Validation

Type to search in tables

Row Count: 0

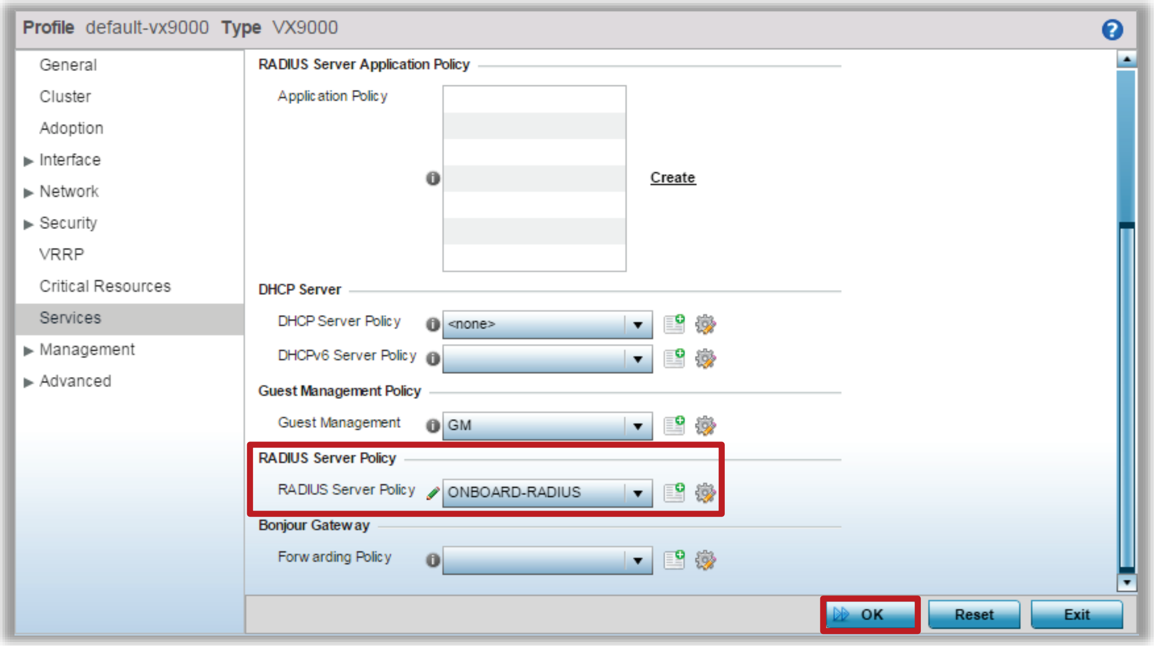


RADIUS Server Policy: ONBOARD-RADIUS

Settings

RADIUS User Pools	
LDAP Server Dead Period	5 Minutes (0 to 10)
LDAP Groups	<none>
LDAP Group Verification	☑
LDAP Chase Referral	☐
Local Realm	

Configuration -> Profiles -> {select VX/NX profile} -> Services:



Profile default-vx9000 Type VX9000

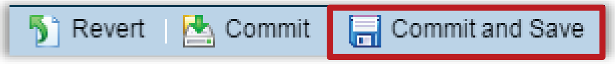
DHCP Server Policy: <none>

DHCPv6 Server Policy:

Guest Management: GM

RADIUS Server Policy: ONBOARD-RADIUS

Forwarding Policy:



RADIUS Server Configuration – CLI

```
!
radius-group Guests
 guest
!
radius-server-policy ONBOARD-RADIUS
!
profile vx9000 default-vx9000
 no autoinstall configuration
 no autoinstall firmware
 use radius-server-policy ONBOARD-RADIUS
 ...
!
```

Configuration – Database (CLI Only)

Starting with WiNG 5.8.4 release database server process does not automatically start on a VX or NX controller. It is required to manually start the process using database policy configuration object.

There are 2 deployment models possible for the database server:

- Standalone – no redundancy for database contents. Data can optionally be backed up at scheduled time intervals to an external location
- Replica Set – three nodes required, two of them will sync full data set, while third node will act as an arbiter in database primary elections.

Configuration - Standalone Database Server

Standalone Database Server Configuration - CLI

```
!
database-policy default
!
vx9000 06-7A-29-AE-E1-EB
 use profile default-vx9000
 use rf-domain AWS-DC-FRANKFURT
 hostname VX-1
 license AAP VX-DEFAULT-64AAP-LICENSE
 license ADSEC DEFAULT-ADV-SEC-LICENSE
 license VX {license string}
 use database-policy default
!
```

Standalone Database Server Verification - CLI

```
#show database status
--------------------------------------------------------------------------------
        MEMBER              STATE                     ONLINE TIME
--------------------------------------------------------------------------------
  localhost            PRIMARY            6 days 0 hours 9 min 32 sec
--------------------------------------------------------------------------------
[*] indicates this device. license VX {license string}
```

Configuration – Replica Set Database Deployment

In this scenario replica sets consist of at least a primary, one or more secondary servers and an arbiter. An arbiter is a lightweight database server process which stores no data, it participates in replica set heart beats and primary elections. Arbiters are good candidates for location outside of a data center as their data requirements are light, and the external location provides prevents the single point of failure scenario previously mentioned.

The primary and secondary devices **must** be of the same device type: NX9600-NX9600, NX9500-NX9500, VX9000-VX9000, NX7500-NX7500 (Captive-portal database only).

Arbiters may be any device type that supports the arbiter role: NX9600, NX9500, VX9000, NX7500, NX5500.

Replica Set Database Server Configuration (Repeat steps for each node) - CLI

```
!
database-policy replica-set
 replica-set member {IP Address or FQDN of the primary} priority 200
 replica-set member {IP Address or FQDN of the secondary} priority 1
 replica-set member {IP Address or FQDN of the arbiter} arbiter
!
vx9000 06-7A-29-AE-E1-EB
 use profile default-vx9000
 use rf-domain AWS-DC-FRANKFURT
 hostname VX-1
 license AAP VX-DEFAULT-64AAP-LICENSE
 license ADSEC DEFAULT-ADV-SEC-LICENSE
 license VX {license string}
 use database-policy replica-set
!
```

Replica Set Database Server Verification (Repeat steps for each node) - CLI

```
PRIMARY#show database status
--------------------------------------------------------------------------------
        MEMBER              STATE                     ONLINE TIME
--------------------------------------------------------------------------------
  172.31.0.49*         PRIMARY           5 days 21 hours 46 min 48 sec
  172.31.2.248         SECONDARY         5 days 21 hours 46 min 29 sec
  172.31.5.121         ARBITER           5 days 21 hours 40 min 51 sec
--------------------------------------------------------------------------------
[*] indicates this device.
```

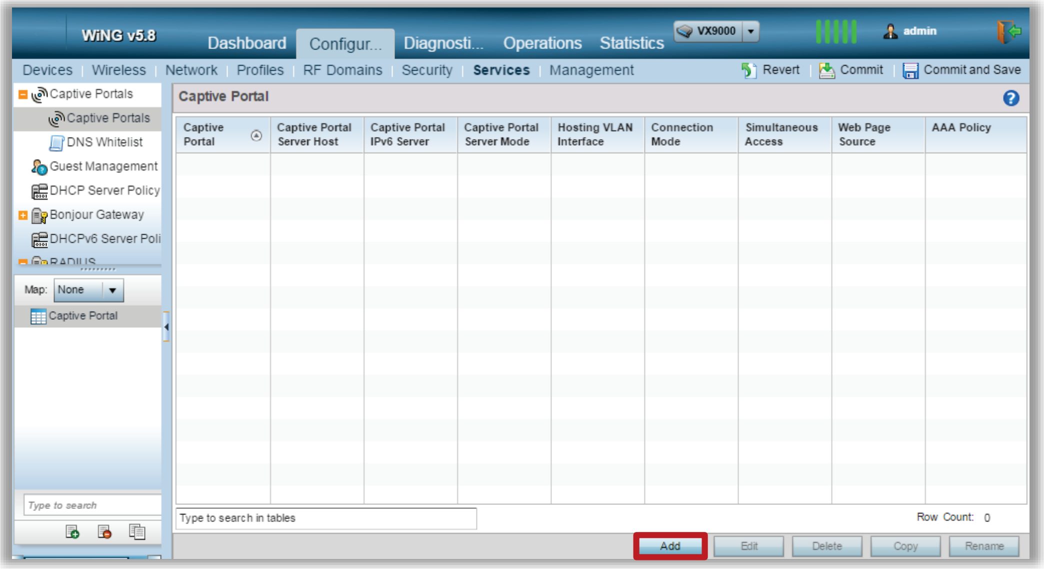
Configuration – Captive Portal Policy

Captive Portal Policy determines a set of rules how a user should be authenticated on a guest network, as well as where Captive Portal server process is hosted and captive portal webpage location.

In this example Captive Portal server is hosted directly on each Access Point in a distributed manner, with pages also hosted internally on each AP. This way client can load captive portal webpage with much less latency, distributing the web server load across all APs in order to scale for multi-thousand AP deployments:

Captive Portal Policy Configuration – Web UI

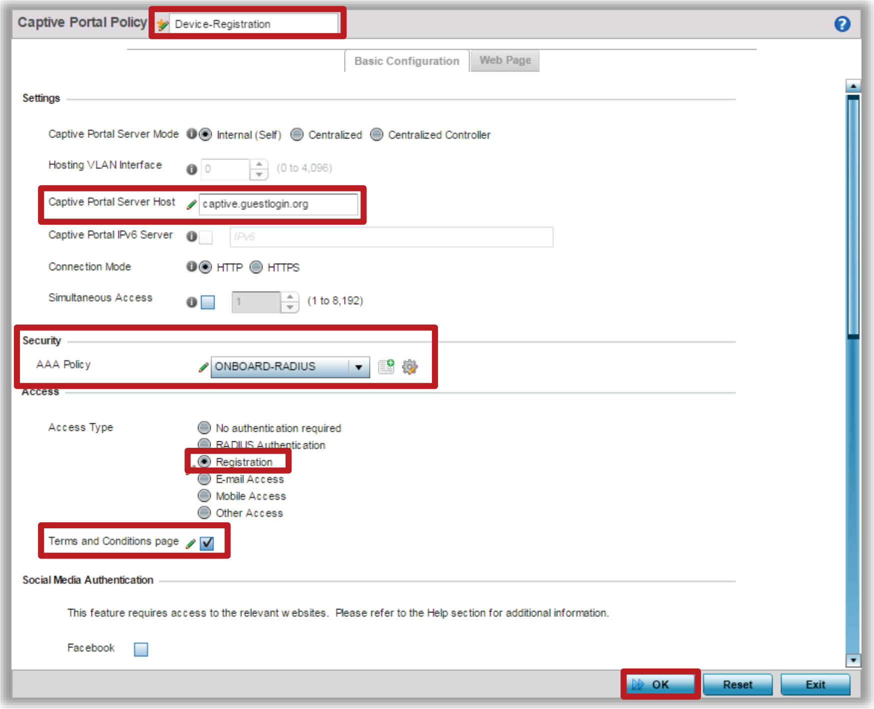
Configuration -> Services -> Captive Portals -> Add:



Captive Portal

Captive Portal	Captive Portal Server Host	Captive Portal IPv6 Server	Captive Portal Server Mode	Hosting VLAN Interface	Connection Mode	Simultaneous Access	Web Page Source	AAA Policy

Row Count: 0



Captive Portal Policy: Device-Registration

Settings

Captive Portal Server Mode ● Internal (Self) ○ Centralized ○ Centralized Controller

Hosting VLAN Interface 0 (0 to 4,096)

Captive Portal Server Host captive.guestlogin.org

Captive Portal IPv6 Server □ IPv6

Connection Mode ● HTTP ○ HTTPS

Simultaneous Access □ 1 (1 to 8,192)

Security

AAA Policy ONBOARD-RADIUS

Access

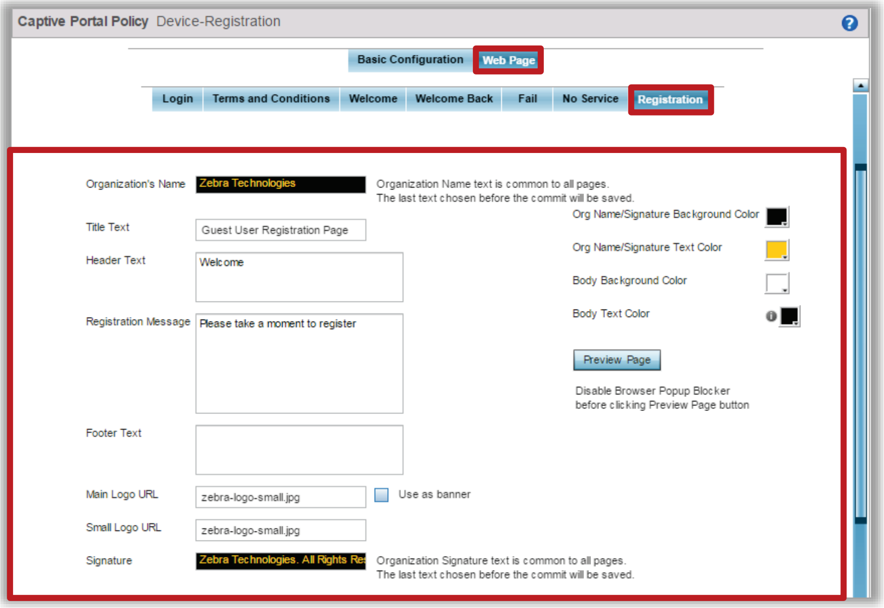
Access Type
○ No authentication required
○ RADIUS Authentication
● Registration
○ E-mail Access
○ Mobile Access
○ Other Access

Terms and Conditions page ☑

Social Media Authentication

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

Facebook □



Captive Portal Policy Device-Registration

Organization's Name: Zebra Technologies
Organization Name text is common to all pages.
The last text chosen before the commit will be saved.

Title Text: Guest User Registration Page

Header Text: Welcome

Registration Message: Please take a moment to register

Footer Text:

Main Logo URL: zebra-logo-small.jpg □ Use as banner

Small Logo URL: zebra-logo-small.jpg

Signature: Zebra Technologies. All Rights Res
Organization Signature text is common to all pages.
The last text chosen before the commit will be saved.

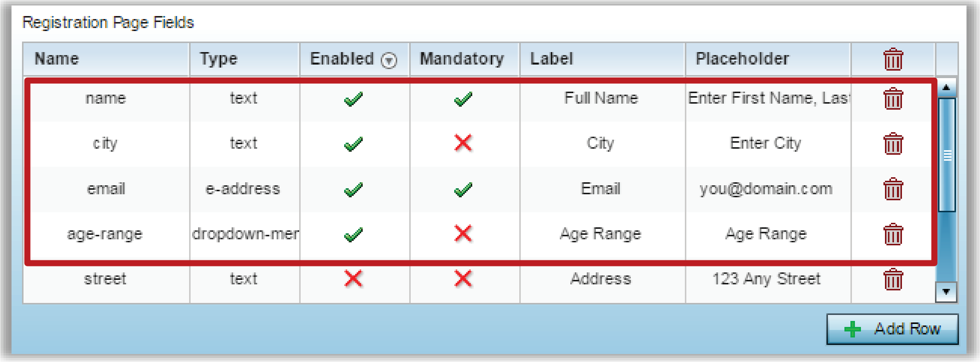
Org Name/Signature Background Color ■

Org Name/Signature Text Color 🟨

Body Background Color □

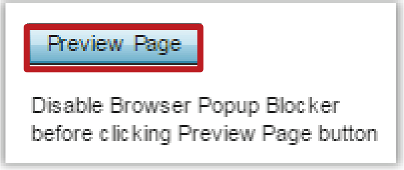
Body Text Color ■

Disable Browser Popup Blocker
before clicking Preview Page button



Registration Page Fields

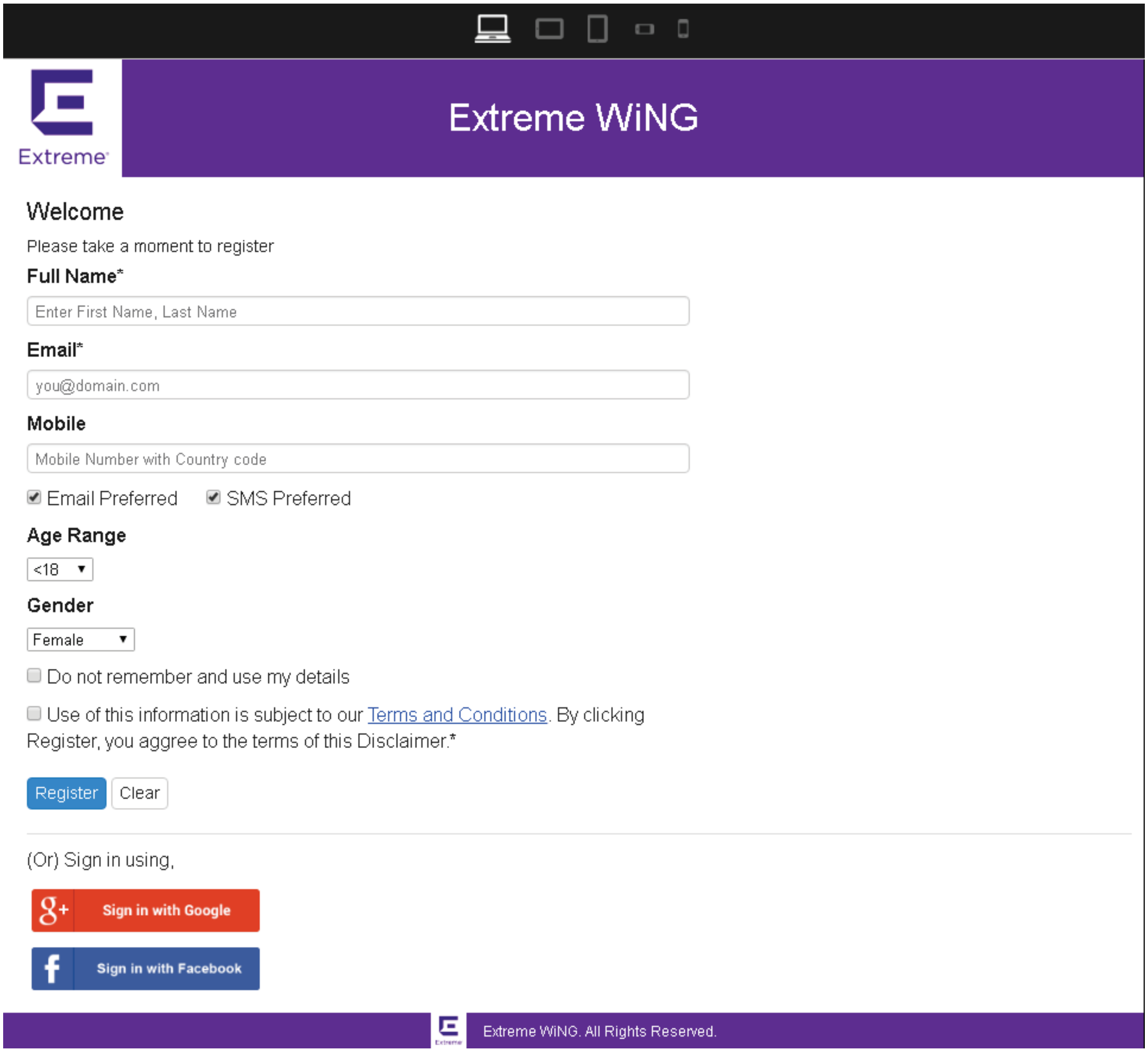
Name	Type	Enabled	Mandatory	Label	Placeholder
name	text	✓	✓	Full Name	Enter First Name, Las
city	text	✓	✗	City	Enter City
email	e-address	✓	✓	Email	you@domain.com
age-range	dropdown-mer	✓	✗	Age Range	Age Range
street	text	✗	✗	Address	123 Any Street



Disable Browser Popup Blocker
before clicking Preview Page button

Note

In order to view logo pictures with the preview page feature, image files should be loaded into the root of the flash:/ partition of the controller (regardless of where the captive portal is hosted).



Welcome

Please take a moment to register

Full Name*

Enter First Name, Last Name

Email*

you@domain.com

Mobile

Mobile Number with Country code

☑ Email Preferred ☑ SMS Preferred

Age Range

<18 ▾

Gender

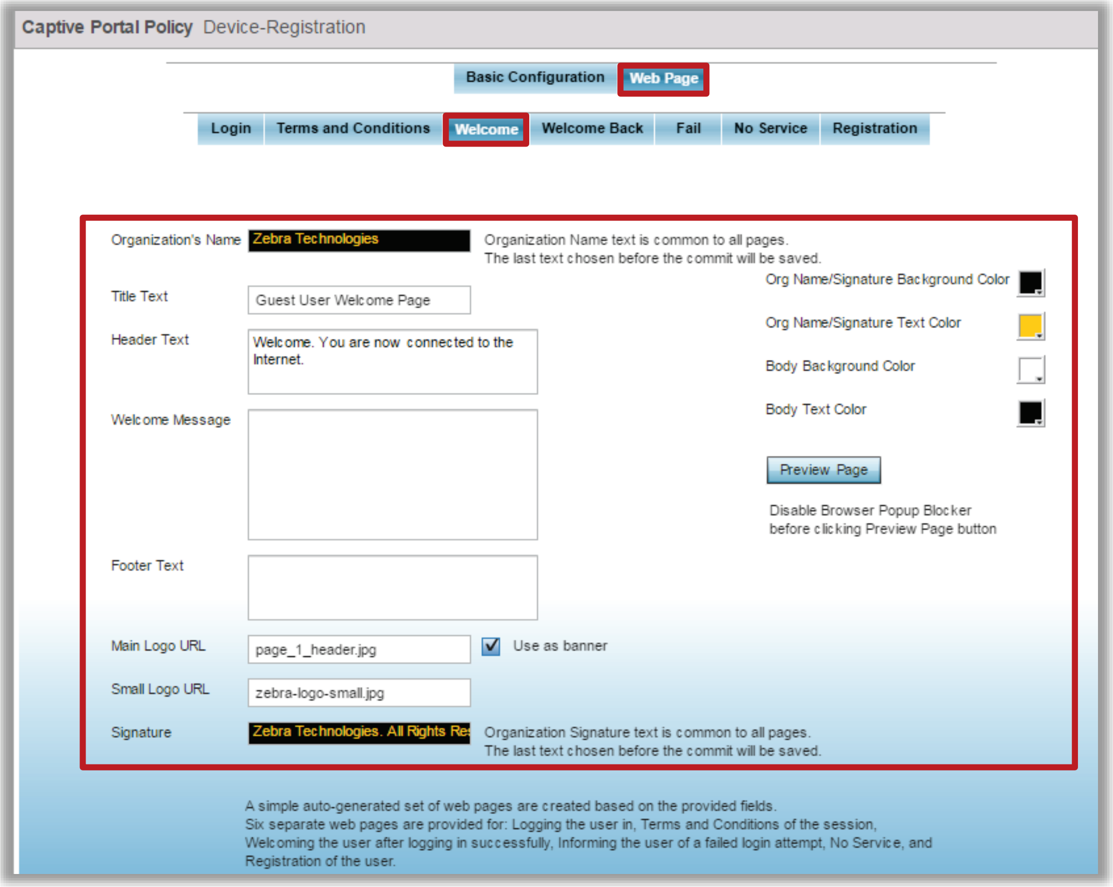
Female ▾

□ Do not remember and use my details

□ Use of this information is subject to our Terms and Conditions. By clicking Register, you aggree to the terms of this Disclaimer.*

(Or) Sign in using,

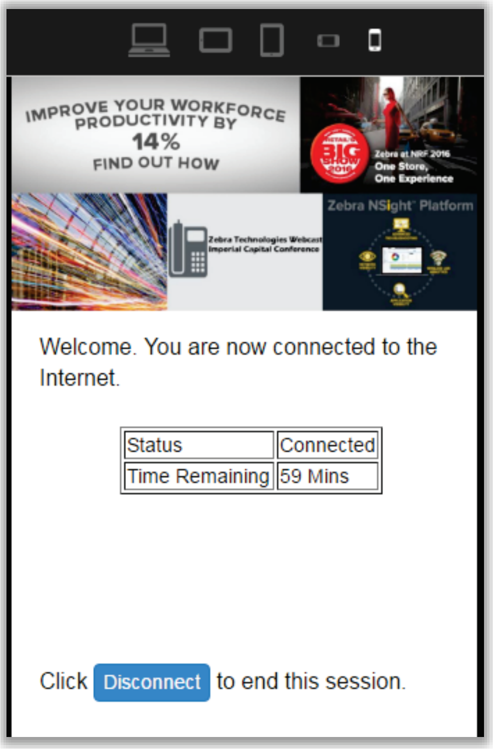
Extreme WiNG. All Rights Reserved.



Captive Portal Policy Device-Registration

Organization's Name	Zebra Technologies	Organization Name text is common to all pages. The last text chosen before the commit will be saved.
Title Text	Guest User Welcome Page	Org Name/Signature Background Color ■
		Org Name/Signature Text Color 🟨
Header Text	Welcome. You are now connected to the Internet.	Body Background Color □
		Body Text Color ■
Welcome Message		Preview Page Disable Browser Popup Blocker before clicking Preview Page button
Footer Text		
Main Logo URL	page_1_header.jpg	☑ Use as banner
Small Logo URL	zebra-logo-small.jpg	
Signature	Zebra Technologies. All Rights Re	Organization Signature text is common to all pages. The last text chosen before the commit will be saved.

A simple auto-generated set of web pages are created based on the provided fields.
Six separate web pages are provided for: Logging the user in, Terms and Conditions of the session,
Welcoming the user after logging in successfully, Informing the user of a failed login attempt, No Service, and
Registration of the user.

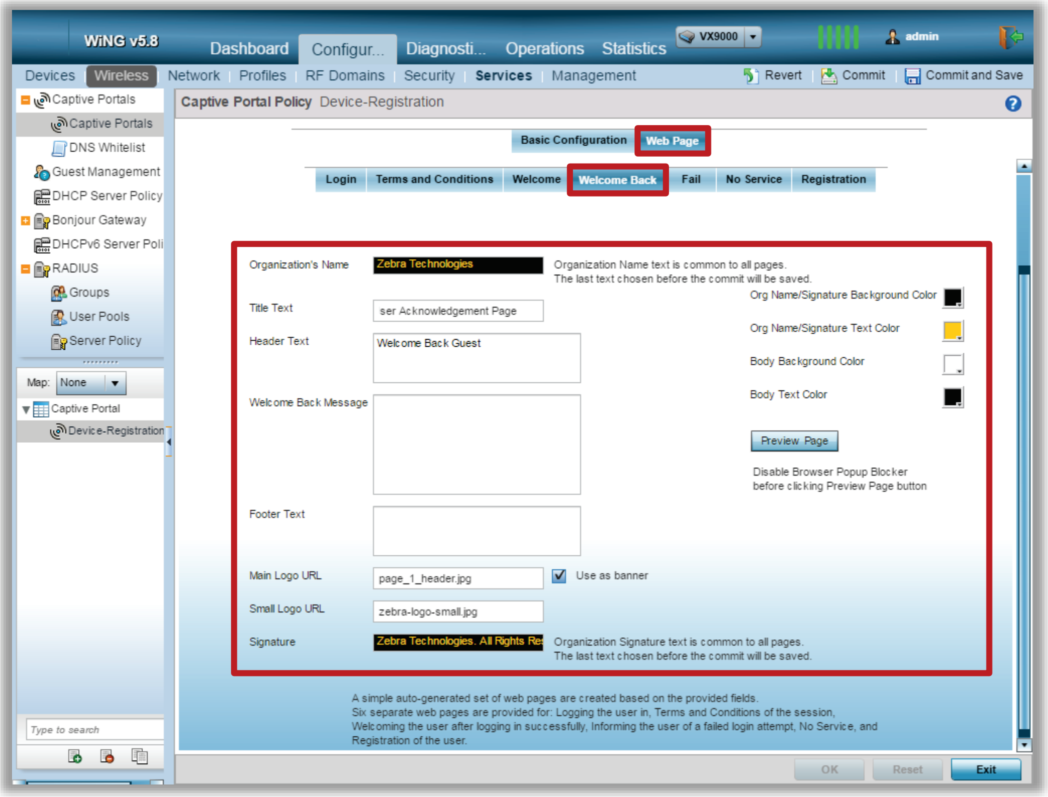


IMPROVE YOUR WORKFORCE PRODUCTIVITY BY
14%
FIND OUT HOW
Zebra at NRF 2016
One Store,
One Experience
Zebra Technologies Webcast
Imperial Capital Conference
Zebra NSight Platform

Welcome. You are now connected to the Internet.

Status	Connected
Time Remaining	59 Mins

Click Disconnect to end this session.



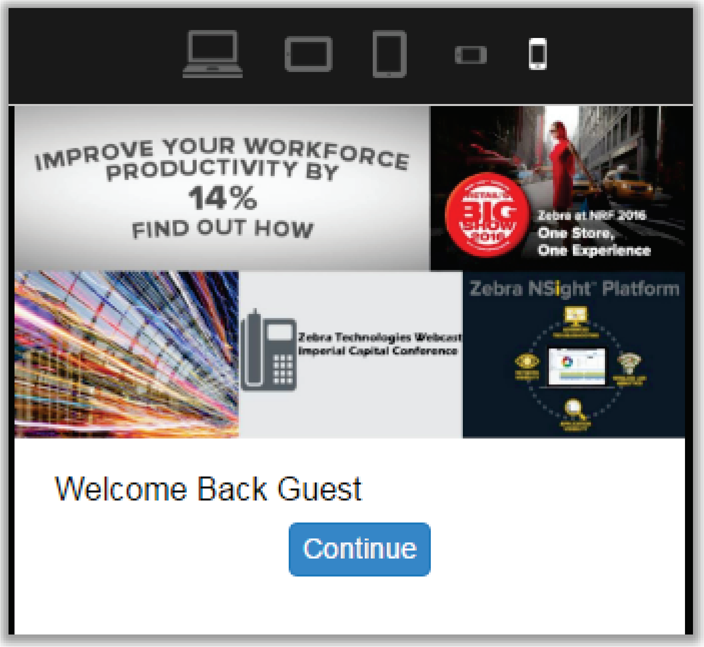
Captive Portal Policy Device-Registration

Organization's Name	Zebra Technologies	Organization Name text is common to all pages. The last text chosen before the commit will be saved.
Title Text	ser Acknowledgement Page	
Header Text	Welcome Back Guest	
Welcome Back Message		
Footer Text		
Main Logo URL	page_1_header.jpg	☑ Use as banner
Small Logo URL	zebra-logo-small.jpg	
Signature	Zebra Technologies. All Rights Re	Organization Signature text is common to all pages. The last text chosen before the commit will be saved.

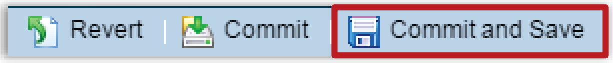
Org Name/Signature Background Color	■
Org Name/Signature Text Color	🟨
Body Background Color	□
Body Text Color	■

Disable Browser Popup Blocker before clicking Preview Page button

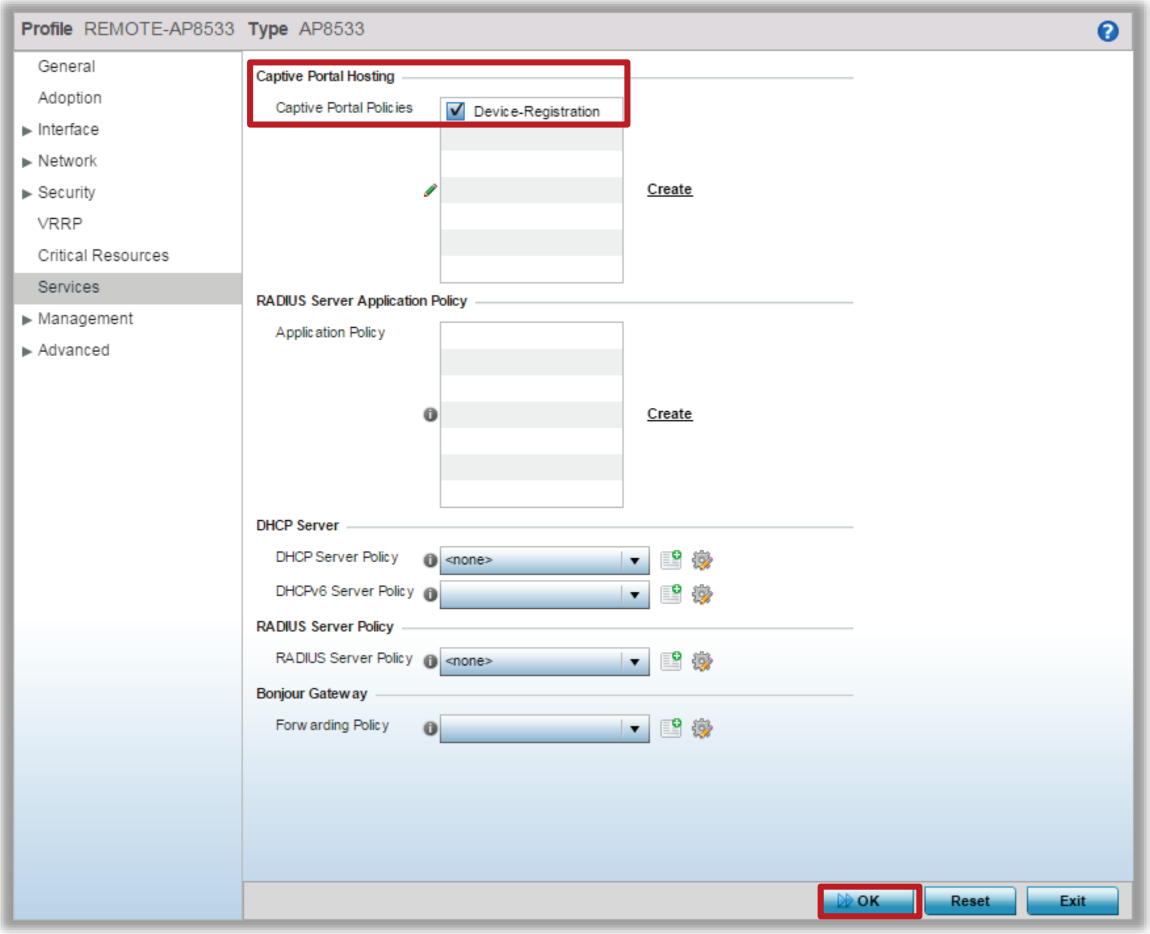
A simple auto-generated set of web pages are created based on the provided fields.
Six separate web pages are provided for: Logging the user in, Terms and Conditions of the session, Welcoming the user after logging in successfully, Informing the user of a failed login attempt, No Service, and Registration of the user.



Welcome Back Guest



Configuration -> Profiles > {select AP Profile} > Services:



Profile REMOTE-AP8533 **Type** AP8533

General
Adoption
▶ Interface
▶ Network
▶ Security
VRRP
Critical Resources
Services
▶ Management
▶ Advanced

Captive Portal Hosting

Captive Portal Policies ☑ Device-Registration — Create

RADIUS Server Application Policy

Application Policy — Create

DHCP Server

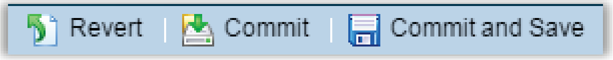
DHCP Server Policy: <none>
DHCPv6 Server Policy:

RADIUS Server Policy

RADIUS Server Policy: <none>

Bonjour Gateway

Forwarding Policy:



Captive Portal Policy Configuration – CLI

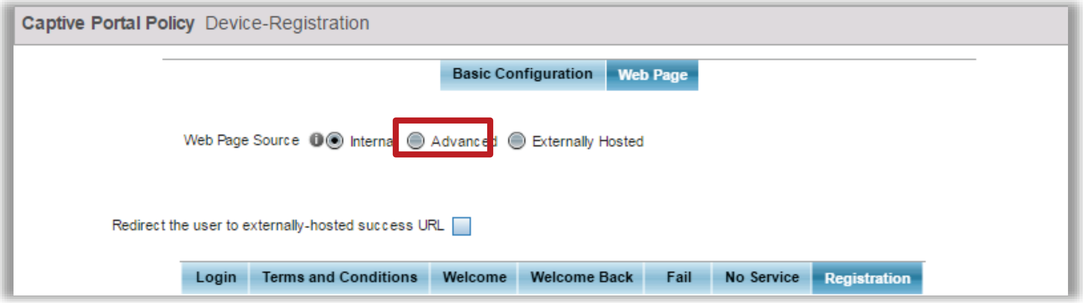
```
!
captive-portal Device-Registration
 access-type registration
 server host captive.guestlogin.org
 terms-agreement
 use aaa-policy ONBOARD-RADIUS
 webpage internal org-name Extreme Networks
 webpage internal org-signature Extreme Networks. All Rights Reserved.
 webpage internal welcome description Welcome. You are now connected to the Internet.
 webpage internal welcome main-logo z-1.jpg
 webpage internal welcome main-logo use-as-banner
 webpage internal welcome body-background-color #ffffff
 webpage internal welcome body-font-color #333333
 webpage internal acknowledgement main-logo page_1_header.jpg
 webpage internal acknowledgement main-logo use-as-banner
 webpage internal acknowledgement small-logo extreme-logo-small.jpg
 webpage internal acknowledgement body-background-color #ffffff
 webpage internal acknowledgement body-font-color #333333
 webpage internal registration main-logo extreme-logo-small.jpg
 webpage internal registration small-logo extreme-logo-small.jpg
 webpage internal registration org-background-color #ffffff
 webpage internal registration org-font-color #000000
 webpage internal registration body-background-color #333333
 webpage internal registration body-font-color #ffffff
 webpage internal registration field city type text enable label "City" placeholder "Enter City"
 no webpage internal registration field street enable
 webpage internal registration field name type text enable mandatory label "Full Name" placeholder "Enter
First Name, Last Name"
 no webpage internal registration field zip enable
 no webpage internal registration field via-sms enable
 no webpage internal registration field mobile enable
 webpage internal registration field age-range type dropdown-menu enable label "Age Range" title "Age
Range"
 webpage internal registration field email type e-address enable mandatory label "Email" placeholder
"you@domain.com"
 no webpage internal registration field via-email enable
!
profile ap8533 REMOTE-AP8533
 no mint mlcp vlan
 no autoinstall configuration
 no autoinstall firmware
 ...
 interface radio1
 interface radio2
 interface radio3
 interface bluetooth1
  shutdown
 interface ge1
  switchport mode trunk
  switchport trunk native vlan 1
  no switchport trunk native tagged
  switchport trunk allowed vlan 1
 interface ge2
 interface vlan1
  ip address dhcp
  ip address zeroconf secondary
  ip dhcp client request options all
 interface pppoe1
 use firewall-policy default
 use captive-portal server Device-Registration
 logging on
 logging buffered debugging
 service pm sys-restart
 router ospf
 dpi
 dpi metadata voice-video
 dpi metadata http
 dpi metadata ssl
!
```

Uploading Custom Logo files to APs

In order to automatically upload custom logo images on to the Access Points, it is possible to enable captive portal auto-upload functionality inside the Captive Portal policy. After that it is only required to upload image file once to the controller, from where it can be automatically pushed down to all Access Points via respective RF Domain Managers.

Captive Portal Logo Auto Upload – Web UI

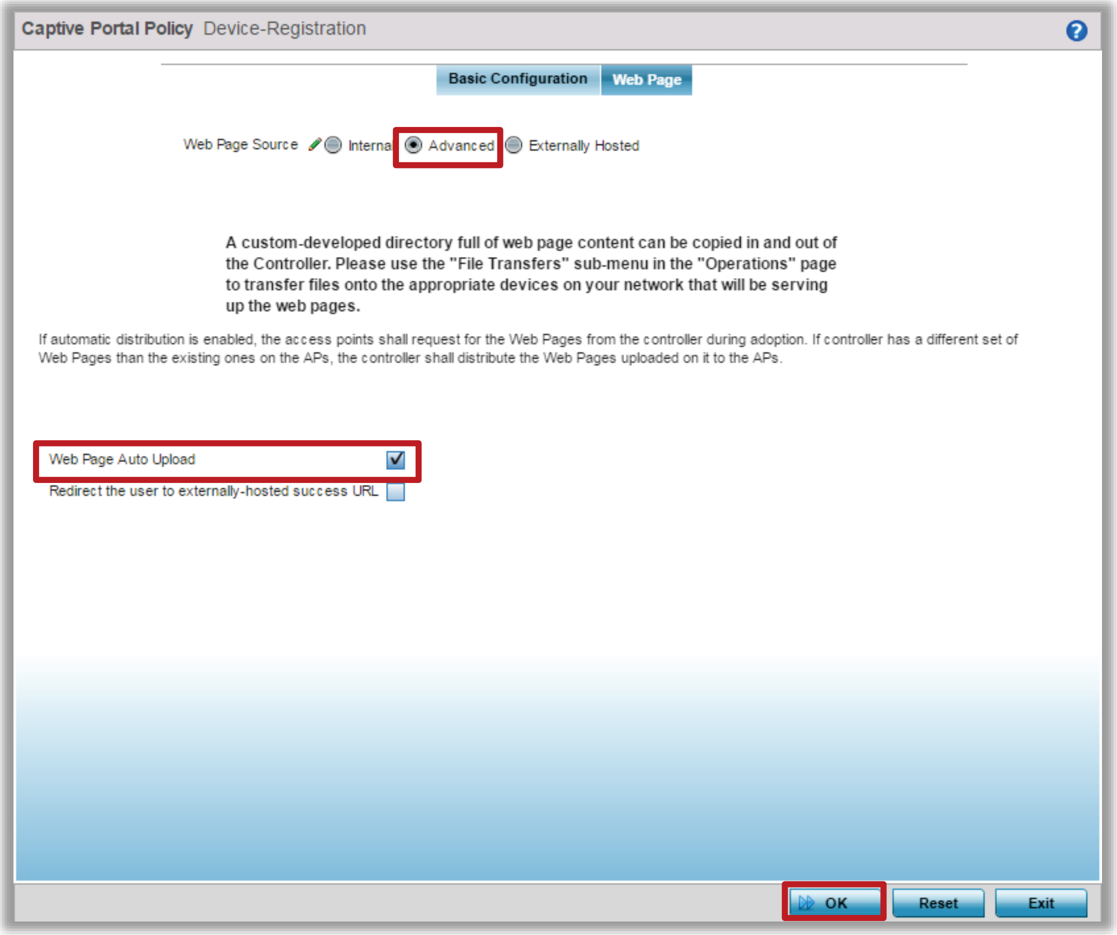
Configuration -> Services -> Captive Portals -> {select CP Policy} -> Edit -> Web Page:



Captive Portal Policy Device-Registration

Web Page Source ● Interna ○ Advanced ○ Externally Hosted

Redirect the user to externally-hosted success URL □



Captive Portal Policy Device-Registration

Web Page Source ○ Interna ● Advanced ○ Externally Hosted

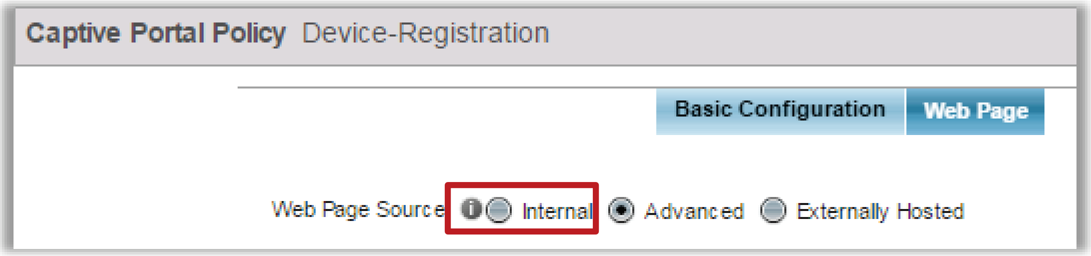
A custom-developed directory full of web page content can be copied in and out of the Controller. Please use the "File Transfers" sub-menu in the "Operations" page to transfer files onto the appropriate devices on your network that will be serving up the web pages.

If automatic distribution is enabled, the access points shall request for the Web Pages from the controller during adoption. If controller has a different set of Web Pages than the existing ones on the APs, the controller shall distribute the Web Pages uploaded on it to the APs.

Web Page Auto Upload ☑

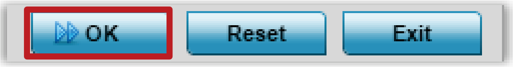
Redirect the user to externally-hosted success URL □

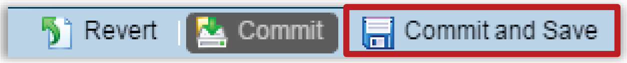
Next, change the Web Page Source back to Internal, hit **OK** and **Commit&Save**:



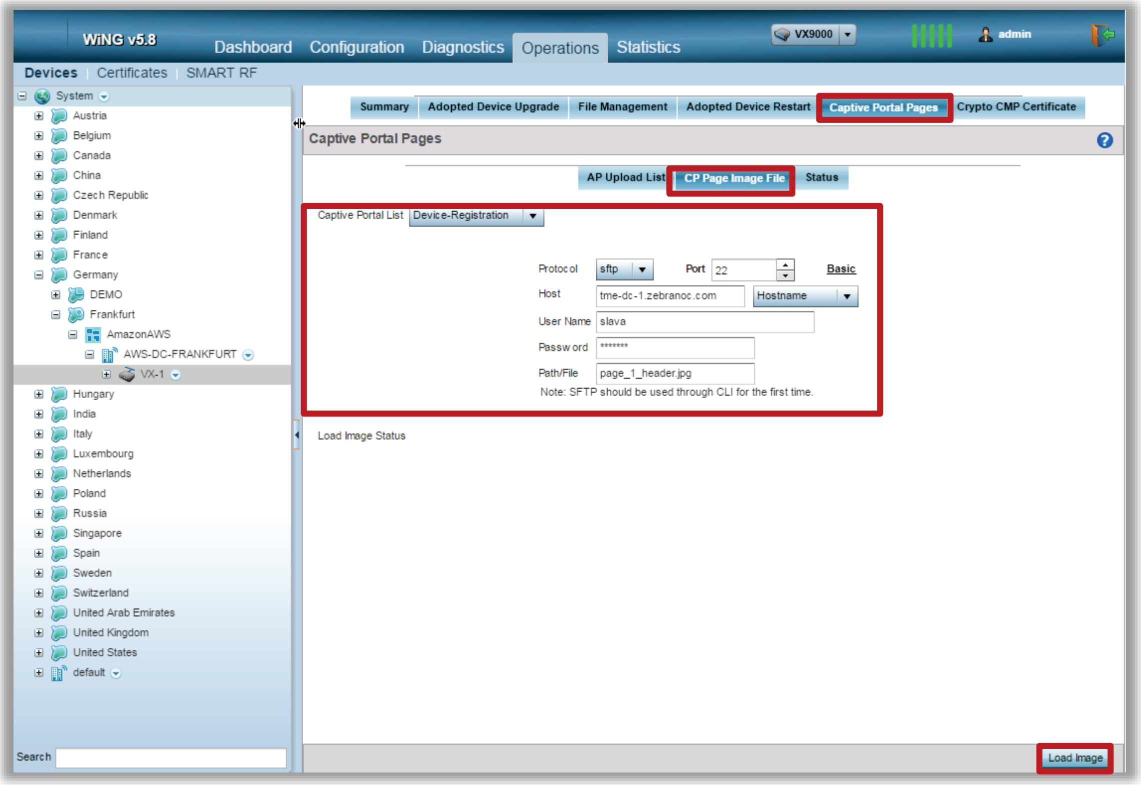
Captive Portal Policy Device-Registration

Web Page Source ○ Internal ● Advanced ○ Externally Hosted





Operation -> {select VX/NX controller} -> Captive Portal Pages -> CP Page Image File:



Captive Portal Pages

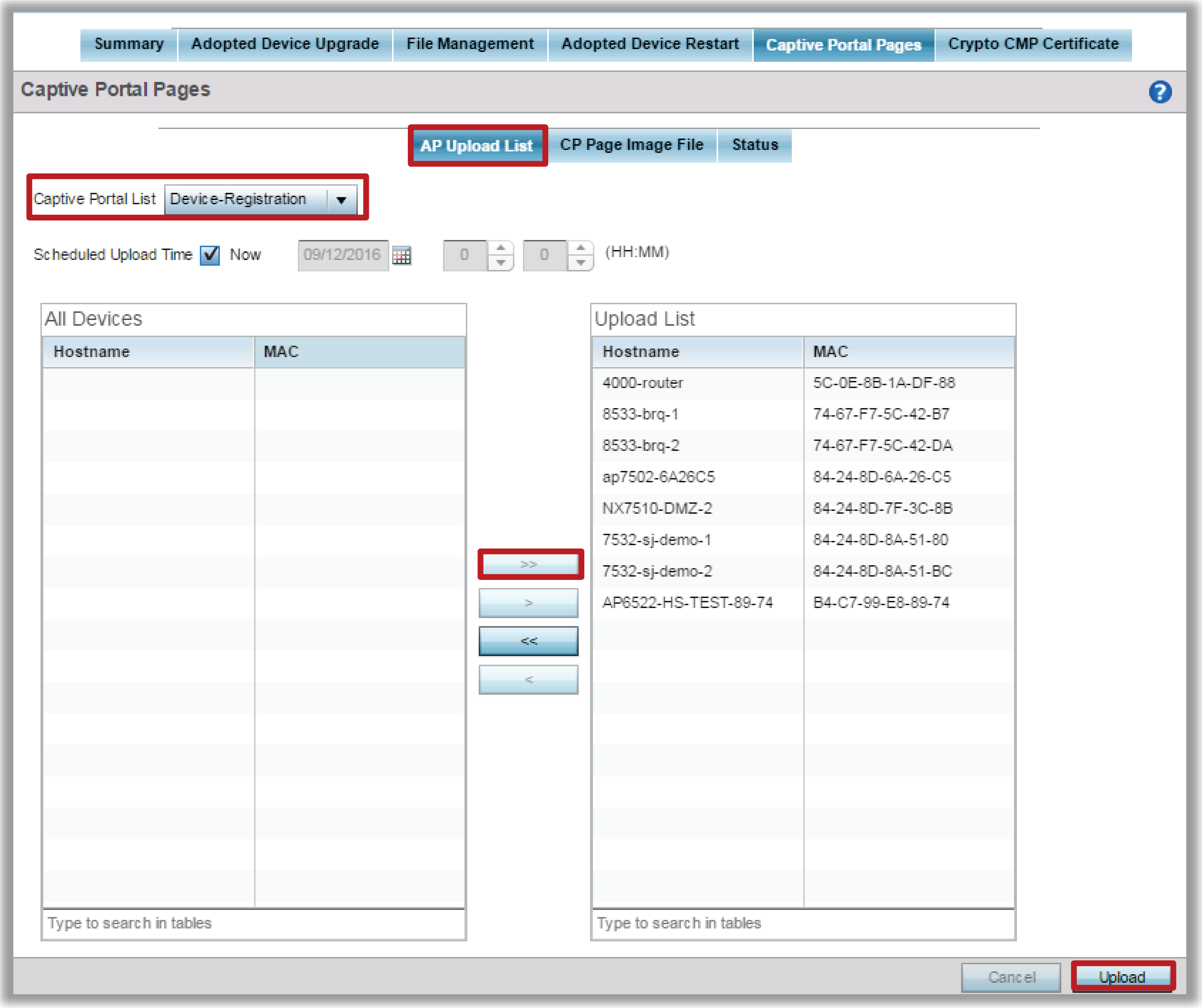
Captive Portal List: Device-Registration

Protocol: sftp
Port: 22
Host: tme-dc-1.zebranoc.com (Hostname)
User Name: slava
Password: *******
Path/File: page_1_header.jpg
Note: SFTP should be used through CLI for the first time.

Load Image Status

Repeat the steps for all custom logo files used during configuration.

Operation -> {select VX/NX controller} -> Captive Portal Pages -> AP Upload List:



Captive Portal List: Device-Registration

Scheduled Upload Time ☑ Now 09/12/2016 0 0 (HH:MM)

All Devices

Hostname	MAC

Type to search in tables

Upload List

Hostname	MAC
4000-router	5C-0E-8B-1A-DF-88
8533-brq-1	74-67-F7-5C-42-B7
8533-brq-2	74-67-F7-5C-42-DA
ap7502-6A26C5	84-24-8D-6A-26-C5
NX7510-DMZ-2	84-24-8D-7F-3C-8B
7532-sj-demo-1	84-24-8D-8A-51-80
7532-sj-demo-2	84-24-8D-8A-51-BC
AP6522-HS-TEST-89-74	B4-C7-99-E8-89-74

Type to search in tables

Captive Portal Auto Upload – CLI

```
!
 access-type registration
 server host captive.guestlogin.org
 terms-agreement
 use aaa-policy ONBOARD-RADIUS
 webpage-auto-upload
 ...
!
VX-1#captive-portal-page-upload load-file Device-Registration
sftp://{user}:{pass}@{file_server_address}/page_1_header.jpg
```

Repeat steps for all image files used during configuration. Manual upload can be triggered using following command:

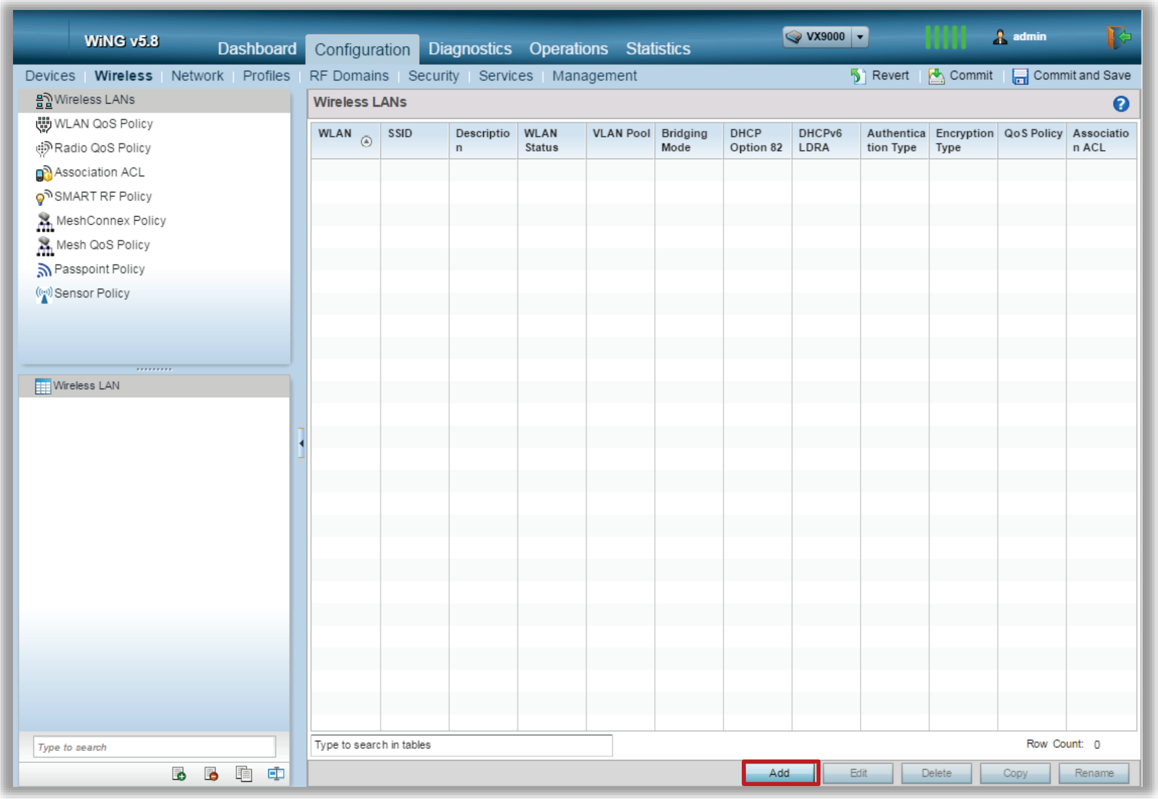
```
VX-1#captive-portal-page-upload Device-Registration <all | rf-domain {RF Domain Name}>
```

Configuration – Wireless LAN

Wireless LAN configuration determines the exact registration / login workflow for new and returning visitors. In this example we are utilizing MAC authentication as primary authentication method to determine whether a device & user record is present in the user database. If it is present, captive portal authentication phase is bypassed or optionally a welcome-back page is presented before network access is granted. If device MAC is not in the database, the user is redirected to a registration page for onboarding.

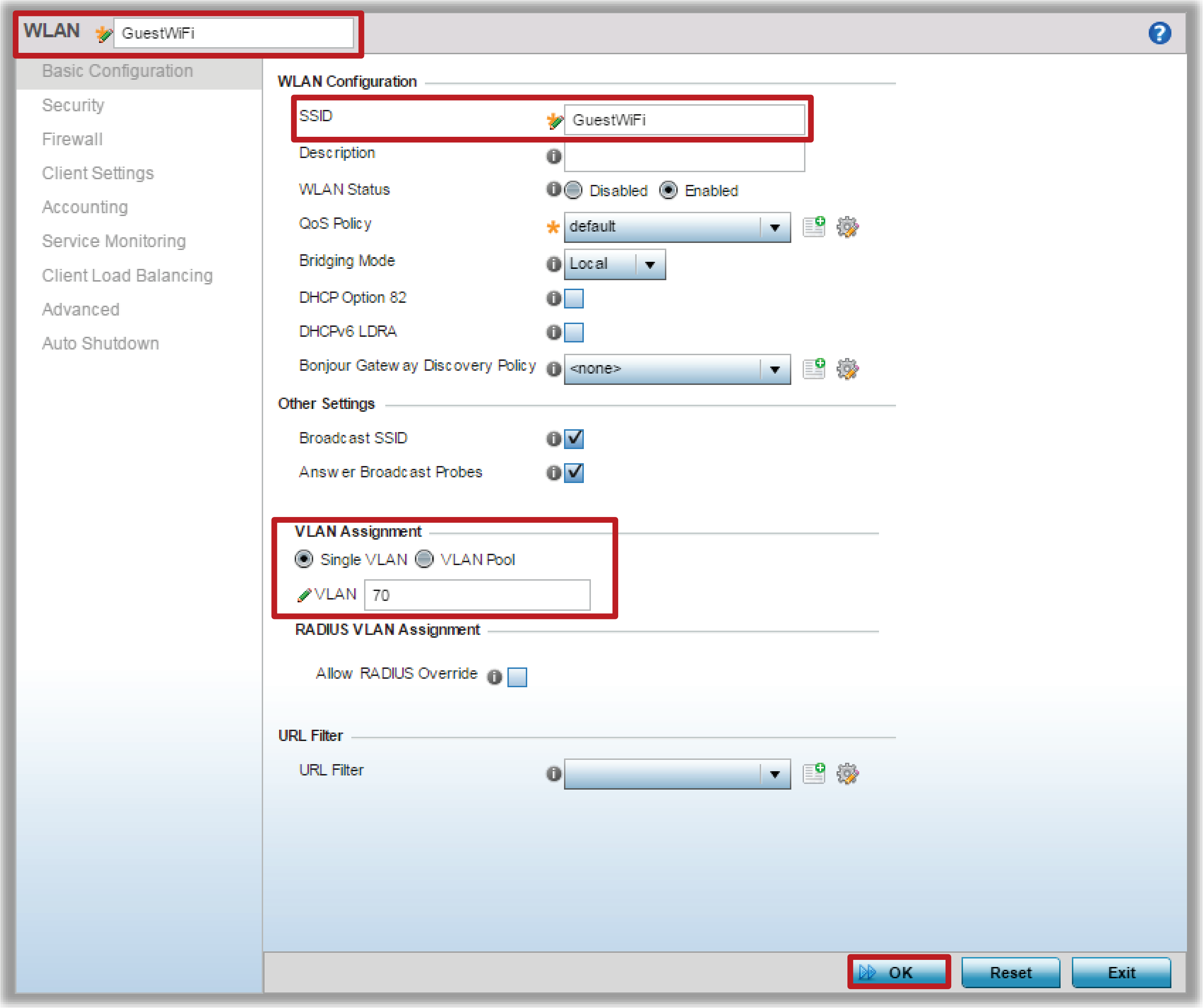
Wireless LAN Configuration – Web UI

Configuration -> Wireless -> Wireless LANs -> Add:



Wireless LANs

WLAN	SSID	Description	WLAN Status	VLAN Pool	Bridging Mode	DHCP Option 82	DHCPv6 LDRA	Authentication Type	Encryption Type	QoS Policy	Association ACL



WLAN: GuestWiFi

WLAN Configuration

SSID: GuestWiFi

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

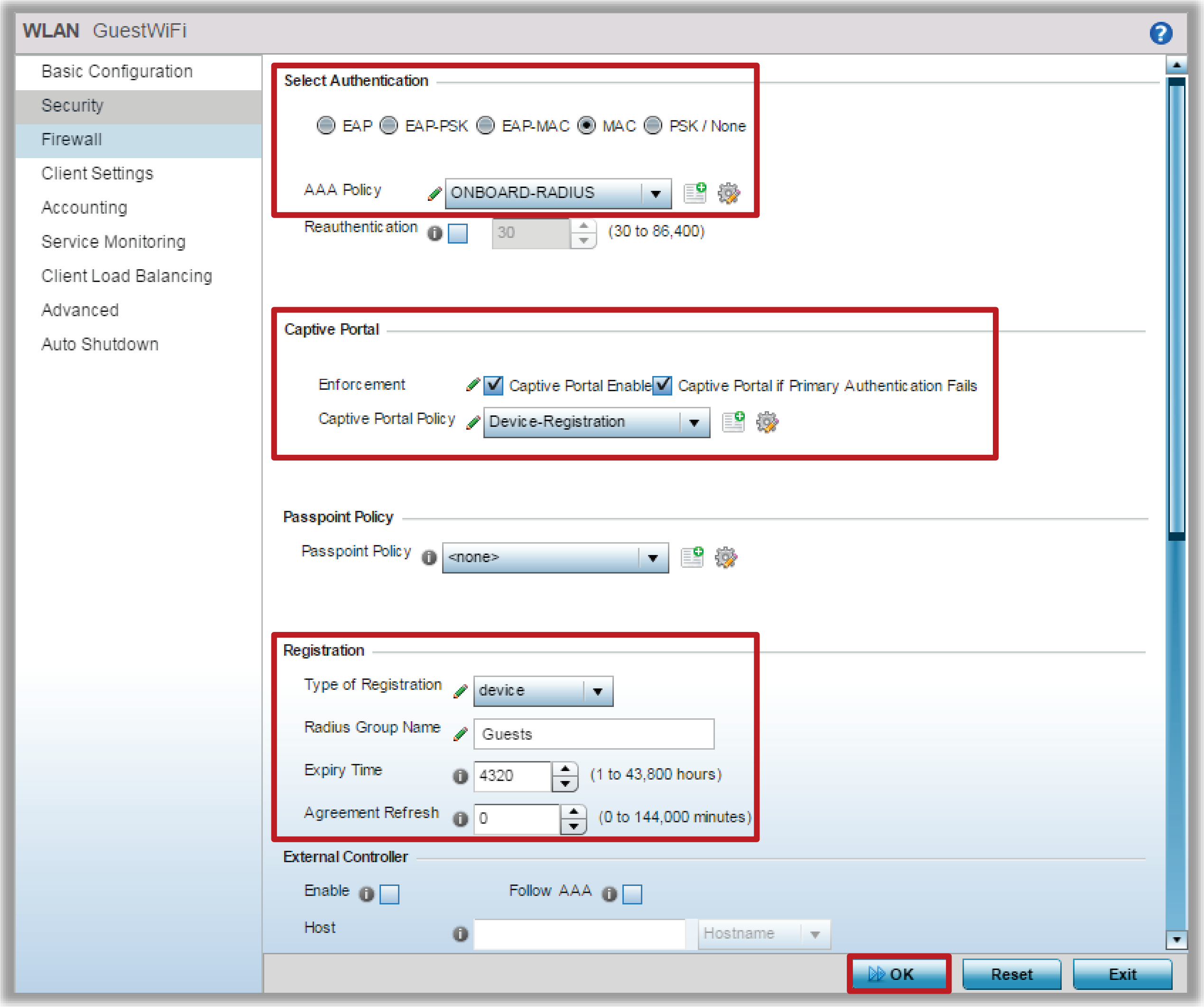
VLAN: 70

RADIUS VLAN Assignment

Allow RADIUS Override: □

URL Filter

URL Filter:



Select Authentication

○ EAP ○ EAP-PSK ○ EAP-MAC ● MAC ○ PSK / None

AAA Policy: ONBOARD-RADIUS

Reauthentication □ 30 (30 to 86,400)

Captive Portal

Enforcement: ☑ Captive Portal Enable ☑ Captive Portal if Primary Authentication Fails

Captive Portal Policy: Device-Registration

Passpoint Policy

Passpoint Policy: <none>

Registration

Type of Registration: device

Radius Group Name: Guests

Expiry Time: 4320 (1 to 43,800 hours)

Agreement Refresh: 0 (0 to 144,000 minutes)

External Controller

Enable □ Follow AAA □

Host: Hostname

The following is optional to make the device registration functionality work.

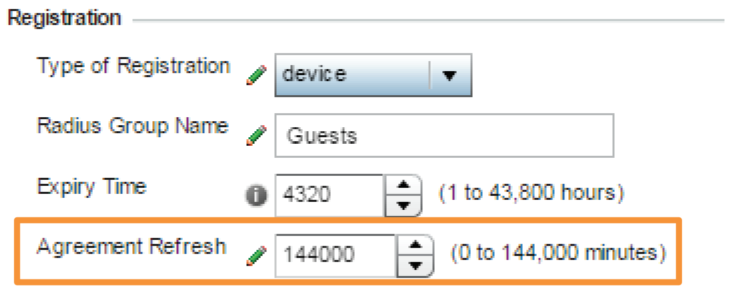
Welcome Back page can be used in order to greet a visitor when he comes back next day, or moves to another store.

Other configuration items are highly recommended for most of the public wifi deployments. Optional configuration items are marked in orange.

To enable welcome back page upon customer return in the same or another store it is required to enable **Agreement Refresh** timeout. Once Agreement Refresh timeout hits the user will see **agreement_view.html** page with terms and conditions. However if the device firewall session is expired and client connects before agreement refresh is expired – welcome back page will be thrown. Welcome Back page timeout is therefore determinted by the following 4 timeouts:

- Wireless Client Firewall Session Hold Time (wireless-client hold-time, default 30 seconds)
- Wireless Client Inactivity Timeout (wireless-client inactivity-timeout, default 30 mins)
- Captive Portal Access Time (access-time, default 24 hours)
- Captive Portal Inactivity Timeout (inactivity-timeout, default 10 minutes)

Whichever timer hits first will trigger a client hostpot state to become cleared and as a result will trigger welcome back page. It is recommended to keep all timers within 30 min / 1 hour range to account for roaming back events.



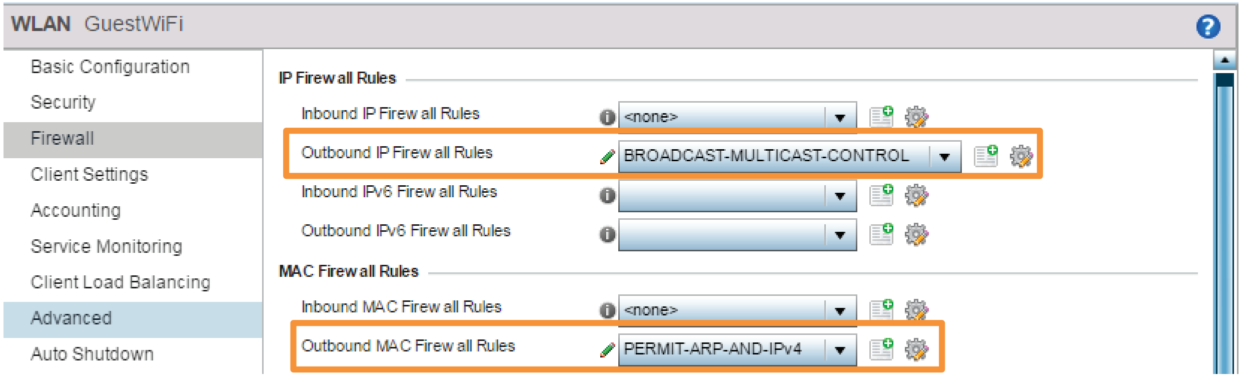
Registration

Type of Registration: device

Radius Group Name: Guests

Expiry Time: 4320 (1 to 43,800 hours)

Agreement Refresh: 144000 (0 to 144,000 minutes)



WLAN GuestWiFi

IP Firewall Rules

Inbound IP Firewall Rules: <none>

Outbound IP Firewall Rules: BROADCAST-MULTICAST-CONTROL

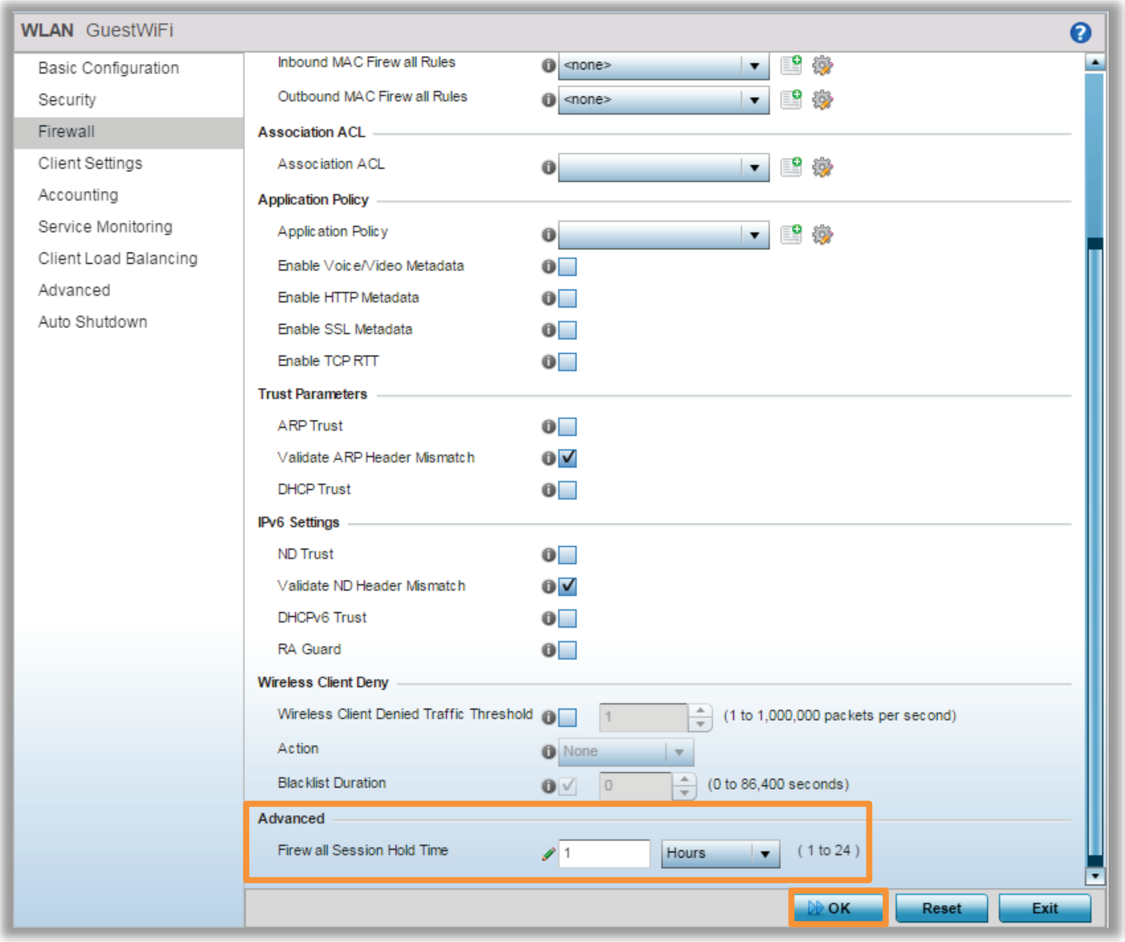
Inbound IPv6 Firewall Rules:

Outbound IPv6 Firewall Rules:

MAC Firewall Rules

Inbound MAC Firewall Rules: <none>

Outbound MAC Firewall Rules: PERMIT-ARP-AND-IPv4



Inbound MAC Firewall Rules <none>

Outbound MAC Firewall Rules <none>

Association ACL

Association ACL

Application Policy

Application Policy

Enable Voice/Video Metadata □

Enable HTTP Metadata □

Enable SSL Metadata □

Enable TCP RTT □

Trust Parameters

ARP Trust □

Validate ARP Header Mismatch ☑

DHCP Trust □

IPv6 Settings

ND Trust □

Validate ND Header Mismatch ☑

DHCPv6 Trust □

RA Guard □

Wireless Client Deny

Wireless Client Denied Traffic Threshold □ 1 (1 to 1,000,000 packets per second)

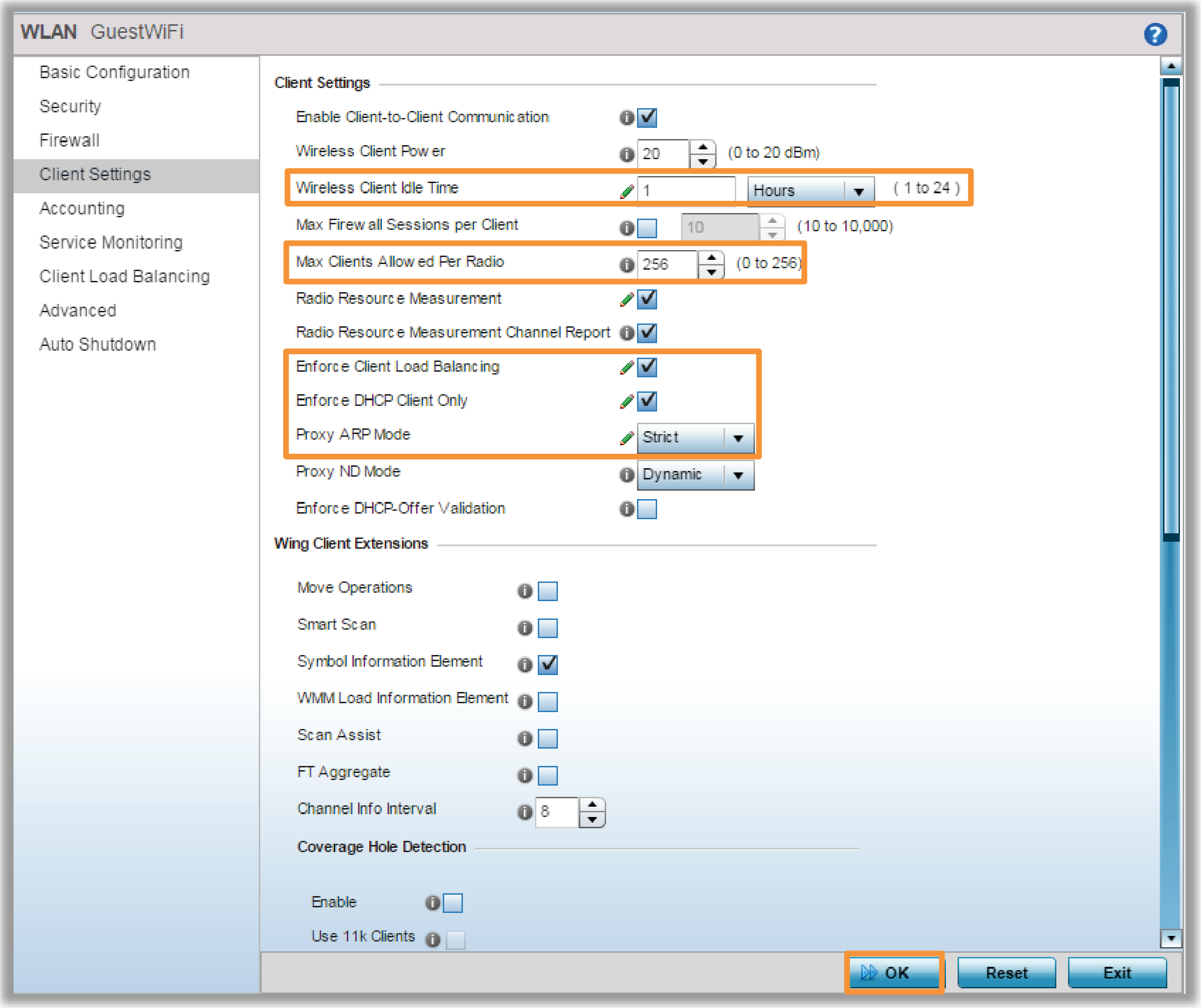
Action None

Blacklist Duration ☑ 0 (0 to 86,400 seconds)

Advanced

Firewall Session Hold Time 1 Hours (1 to 24)

Enable 802.11k, enfore DHCP only wireless client, enable strict Proxy ARP, enable load balancing in order to prefer dual-band capable clients to steer to 5GHz:



Client Settings

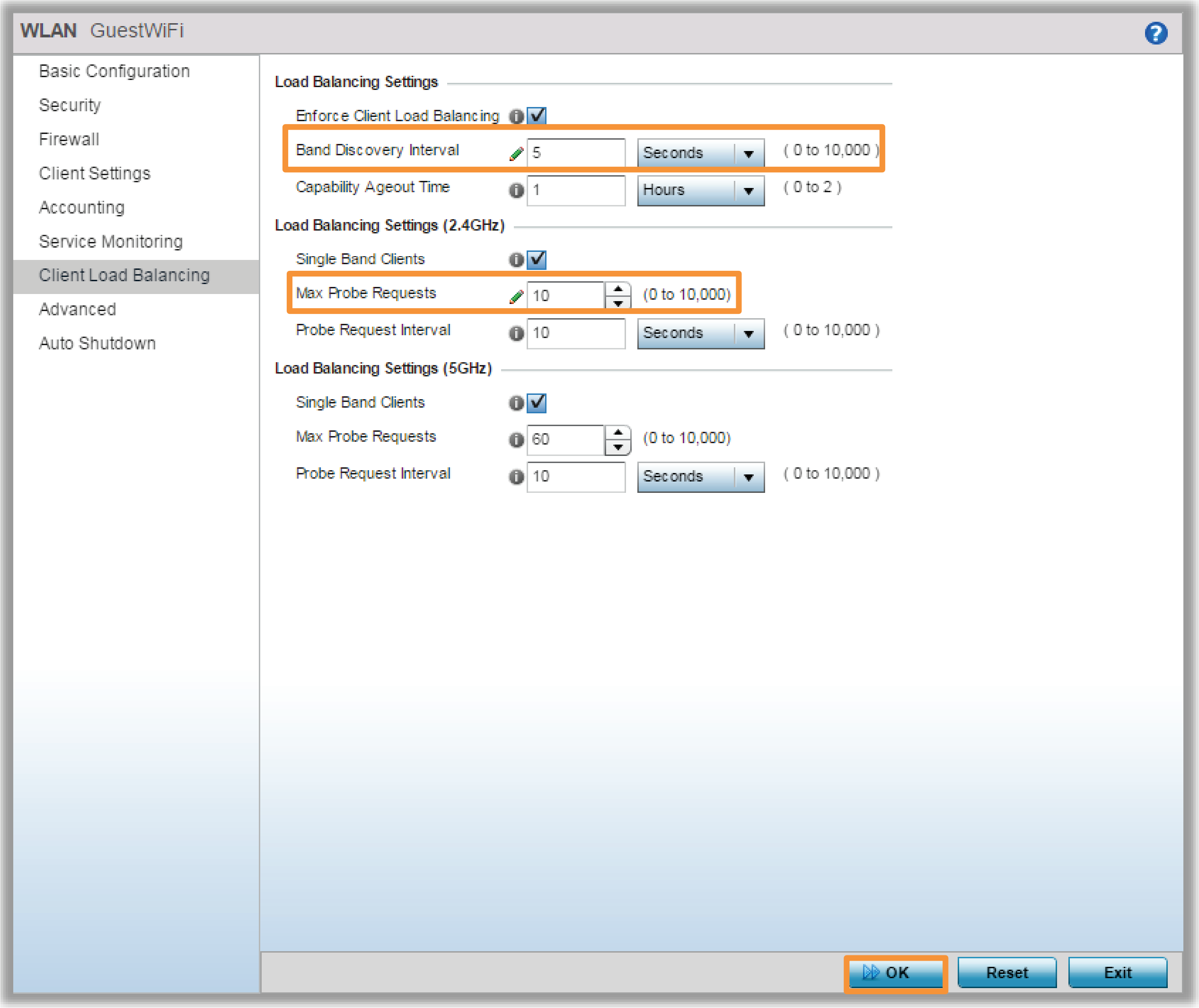
Enable Client-to-Client Communication ☑
Wireless Client Pow er 20 (0 to 20 dBm)
Wireless Client Idle Time 1 Hours (1 to 24)
Max Firew all Sessions per Client □ 10 (10 to 10,000)
Max Clients Allow ed Per Radio 256 (0 to 256)
Radio Resource Measurement ☑
Radio Resource Measurement Channel Report ☑
Enforce Client Load Balancing ☑
Enforce DHCP Client Only ☑
Proxy ARP Mode Strict
Proxy ND Mode Dynamic
Enforce DHCP-Offer Validation □

Wing Client Extensions

Move Operations □
Smart Scan □
Symbol Information Element ☑
WMM Load Information Element □
Scan Assist □
FT Aggregate □
Channel Info Interval 8

Coverage Hole Detection

Enable □
Use 11k Clients □



Load Balancing Settings

Enforce Client Load Balancing ☑

Band Discovery Interval 5 Seconds (0 to 10,000)

Capability Ageout Time 1 Hours (0 to 2)

Load Balancing Settings (2.4GHz)

Single Band Clients ☑

Max Probe Requests 10 (0 to 10,000)

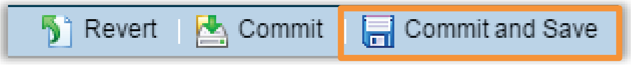
Probe Request Interval 10 Seconds (0 to 10,000)

Load Balancing Settings (5GHz)

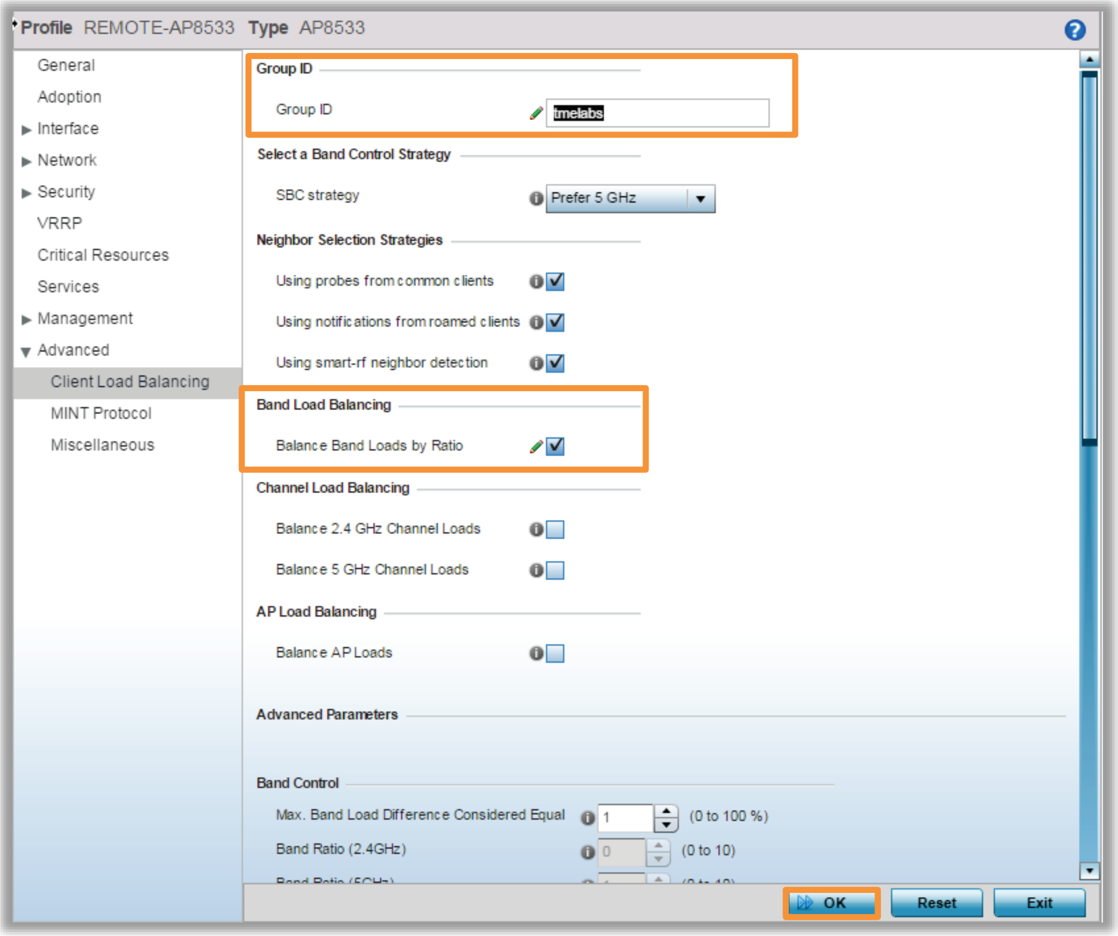
Single Band Clients ☑

Max Probe Requests 60 (0 to 10,000)

Probe Request Interval 10 Seconds (0 to 10,000)



Configuration -> Profiles -> {select AP Profile} -> Edit -> Advanced -> Client Load Balancing:



Profile REMOTE-AP8533 Type AP8533

Group ID

Group ID: tmelabs

Select a Band Control Strategy

SBC strategy: Prefer 5 GHz

Neighbor Selection Strategies

Using probes from common clients ☑

Using notifications from roamed clients ☑

Using smart-rf neighbor detection ☑

Band Load Balancing

Balance Band Loads by Ratio ☑

Channel Load Balancing

Balance 2.4 GHz Channel Loads □

Balance 5 GHz Channel Loads □

AP Load Balancing

Balance AP Loads □

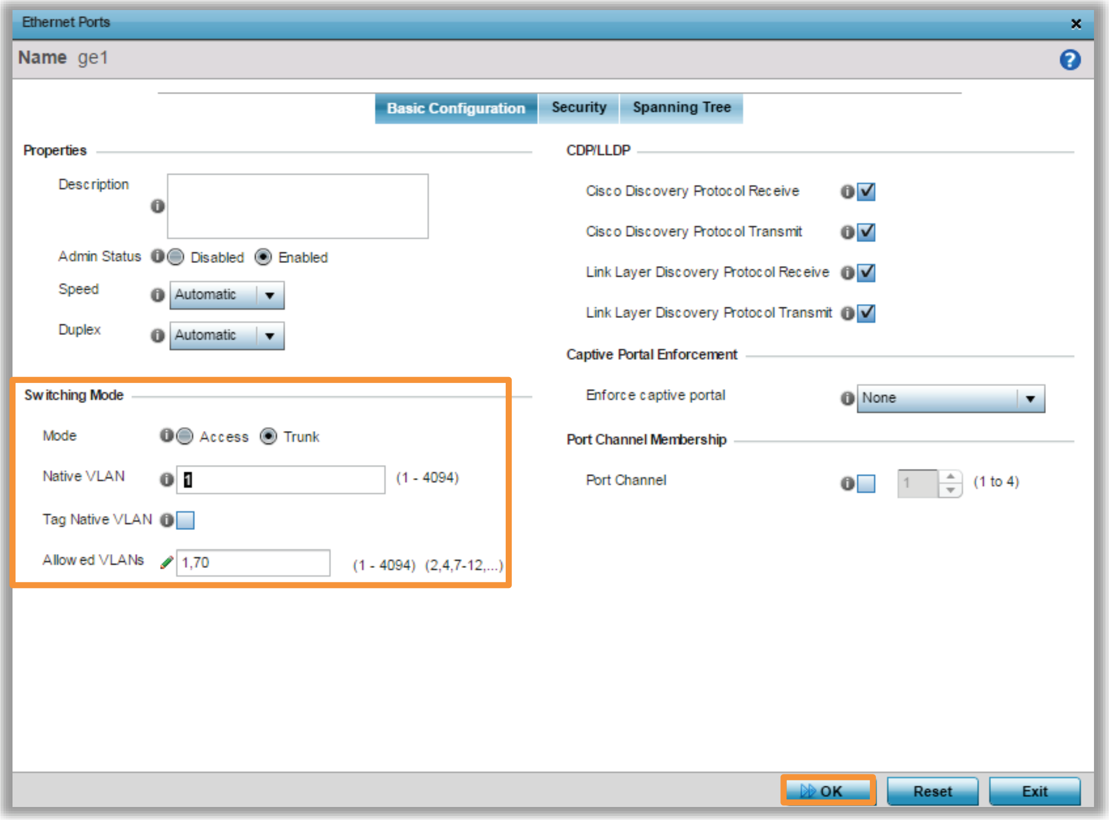
Advanced Parameters

Band Control

Max. Band Load Difference Considered Equal: 1 (0 to 100 %)

Band Ratio (2.4GHz): 0 (0 to 10)

Configuration -> Profiles -> {select AP Profile} -> Interfaces -> Ethernet Ports -> ge1:



Ethernet Ports

Name ge1

Properties

- Description:
- Admin Status: ○ Disabled ● Enabled
- Speed: Automatic
- Duplex: Automatic

Switching Mode

- Mode: ○ Access ● Trunk
- Native VLAN: 1 (1 - 4094)
- Tag Native VLAN: □
- Allowed VLANs: 1,70 (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 ☑

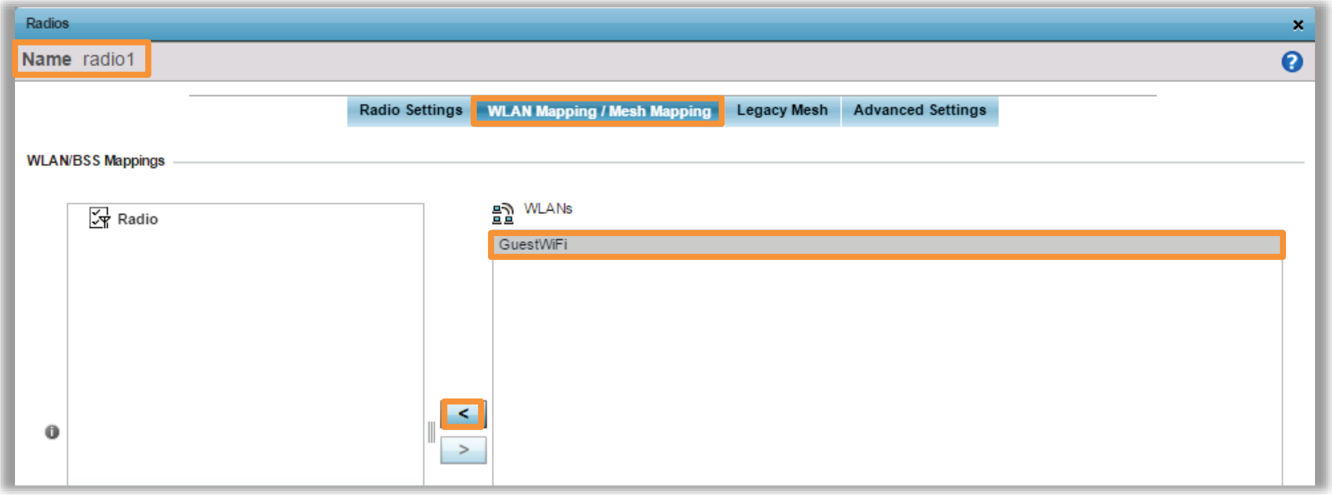
Captive Portal Enforcement

- Enforce captive portal: None

Port Channel Membership

- Port Channel □ 1 (1 to 4)

Configuration -> Profiles -> {select AP Profile} -> Interfaces -> Radios -> Radio {Index} -> Edit:

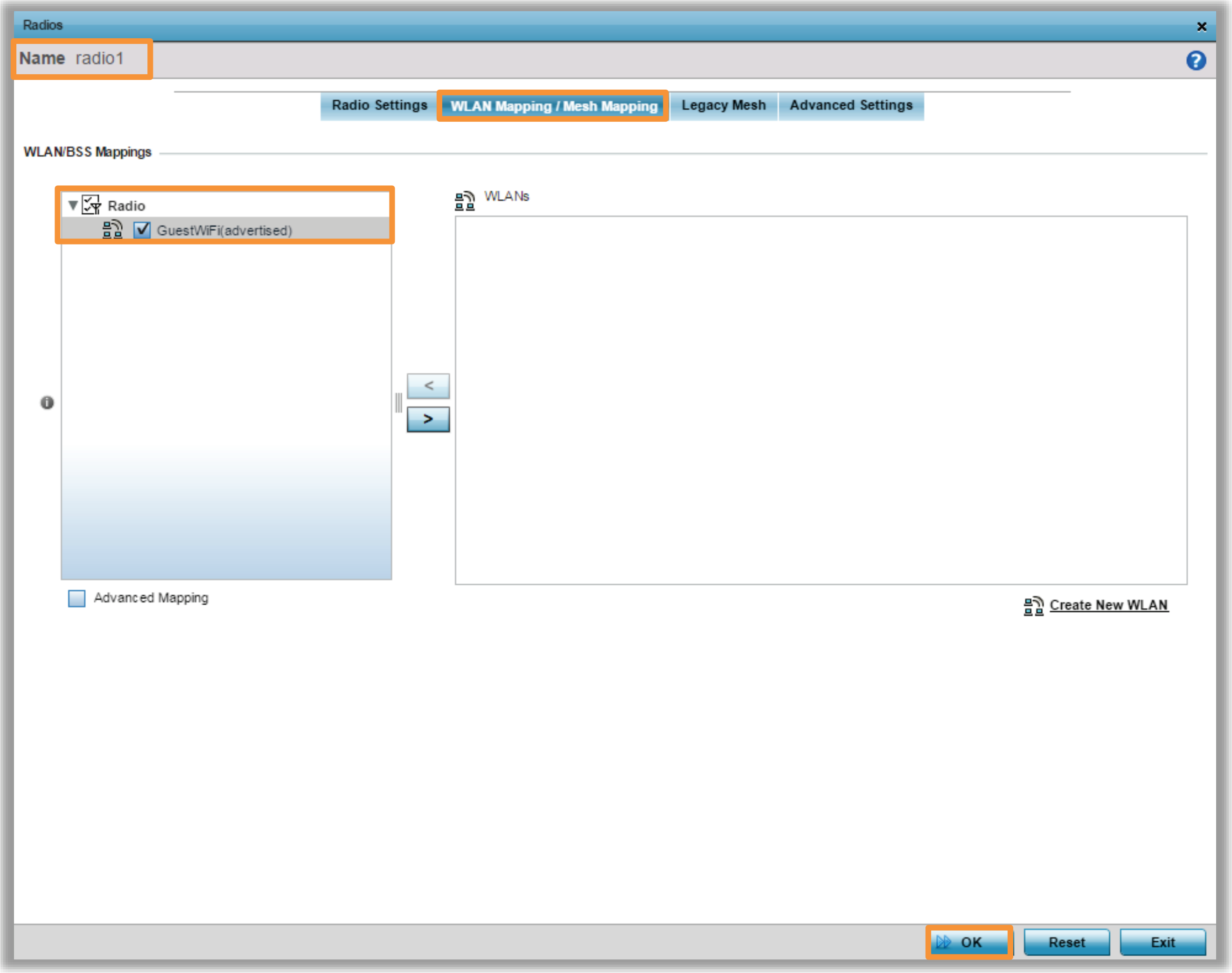


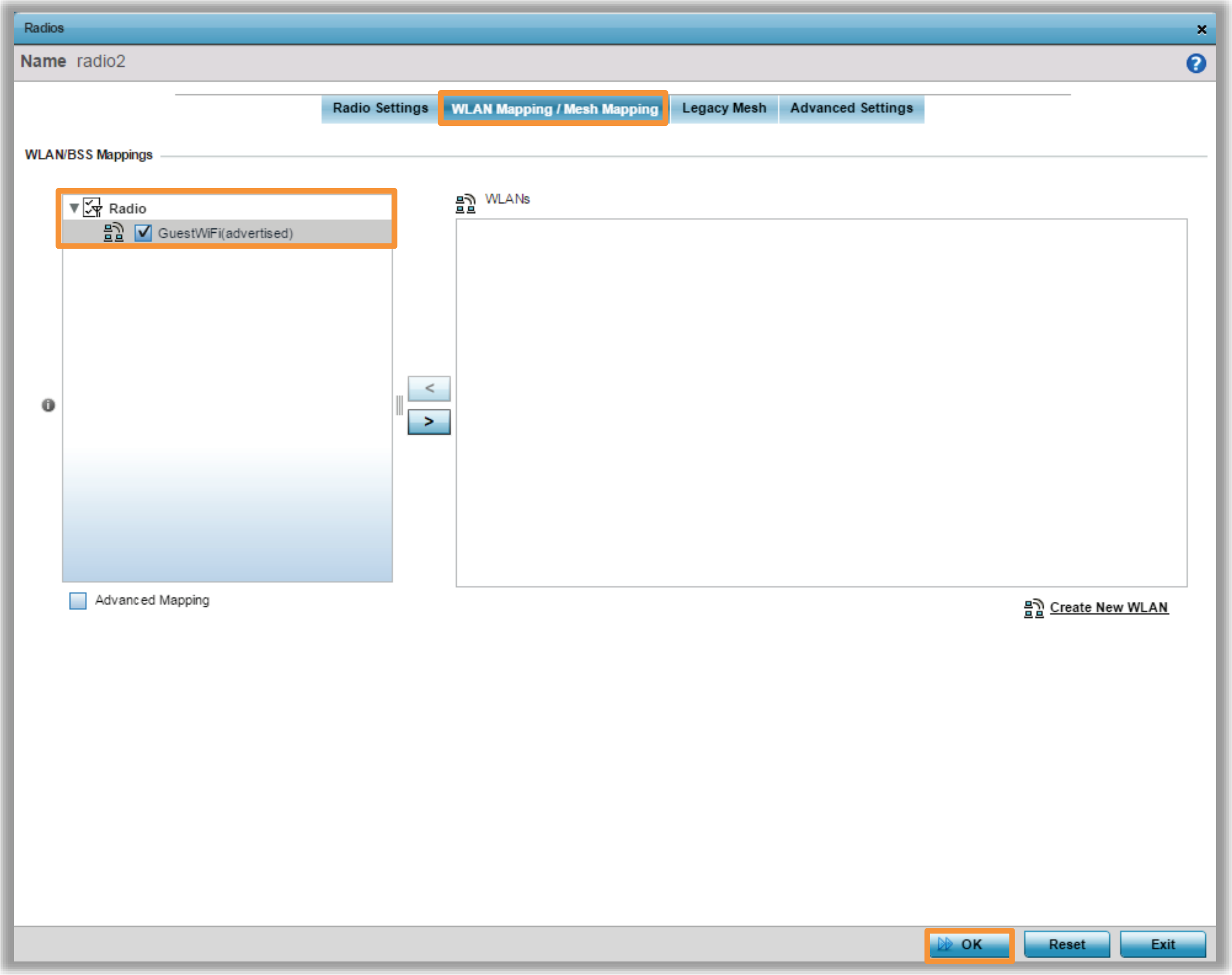
Radios

Name radio1

WLAN/BSS Mappings

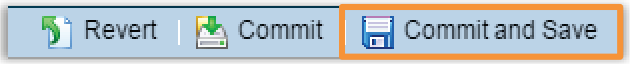
GuestWiFi


Radios
Name radio1
Radio Settings
WLAN Mapping / Mesh Mapping
Legacy Mesh
Advanced Settings
WLAN/BSS Mappings
Radio
☑ GuestWiFi(advertised)
WLANs
<
>
□ Advanced Mapping
Create New WLAN
OK
Reset
Exit



Name radio2

Radios
Radio Settings
WLAN Mapping / Mesh Mapping
Legacy Mesh
Advanced Settings
WLAN/BSS Mappings
Radio
☑ GuestWiFi(advertised)
WLANs
<
>
□ Advanced Mapping
Create New WLAN
OK
Reset
Exit



Revert
Commit
Commit and Save

Wireless LAN Configuration – CLI

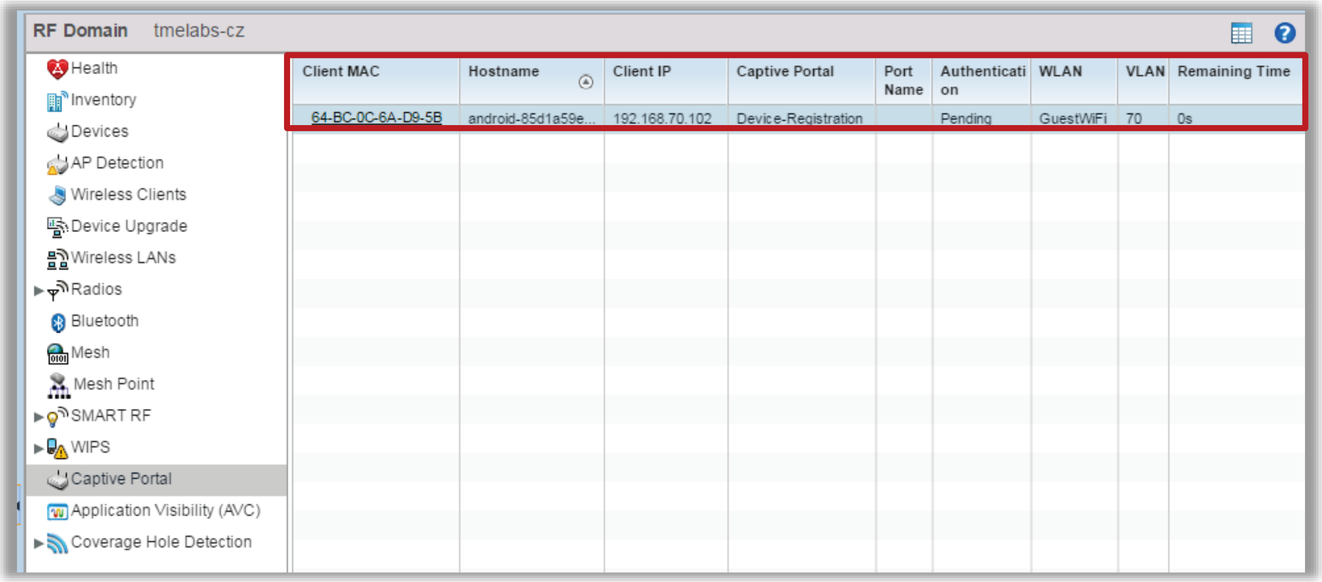
```
!
 wlan GuestWiFi
 ssid GuestWiFi
 vlan 70
 bridging-mode local
 encryption-type none
 authentication-type mac
 wireless-client hold-time 3600
 wireless-client inactivity-timeout 3600
 radio-resource-measurement
 client-load-balancing
 client-load-balancing max-probe-req 2.4ghz 10
 client-load-balancing band-discovery-intvl 5
 use aaa-policy ONBOARD-RADIUS
 use captive-portal Device-Registration
 captive-portal-enforcement fall-back
 registration device group-name Guests expiry-time 4320 agreement-refresh 144000
 use ip-access-list out BROADCAST-MULTICAST-CONTROL
 use mac-access-list out PERMIT-ARP-AND-IPv4
 proxy-arp-mode strict
 enfore-dhcp
 no nsight client-history
!
profile ap8533 REMOTE-AP8533
 no mint mlcp vlan
 no autoinstall configuration
 no autoinstall firmware
 use radius-server-policy ONBOARD-TLS
 ...
 interface radio1
  wlan GuestWiFi bss 1 primary
 interface radio2
  wlan GuestWiFi bss 1 primary
  mu-mimo
 interface radio3
 interface bluetooth1
  shutdown
 interface ge1
  switchport mode trunk
  switchport trunk native vlan 1
  no switchport trunk native tagged
  switchport trunk allowed vlan 1,70
 interface ge2
 interface vlan1
  ip address dhcp
  ip address zeroconf secondary
  ip dhcp client request options all
 interface pppoe1
 use firewall-policy default
 use captive-portal server Device-Registration
 logging on
 logging buffered debugging
 service pm sys-restart
 router ospf
 dpi
 dpi metadata voice-video
 dpi metadata http
 dpi metadata ssl
!
```

Verification

Web UI

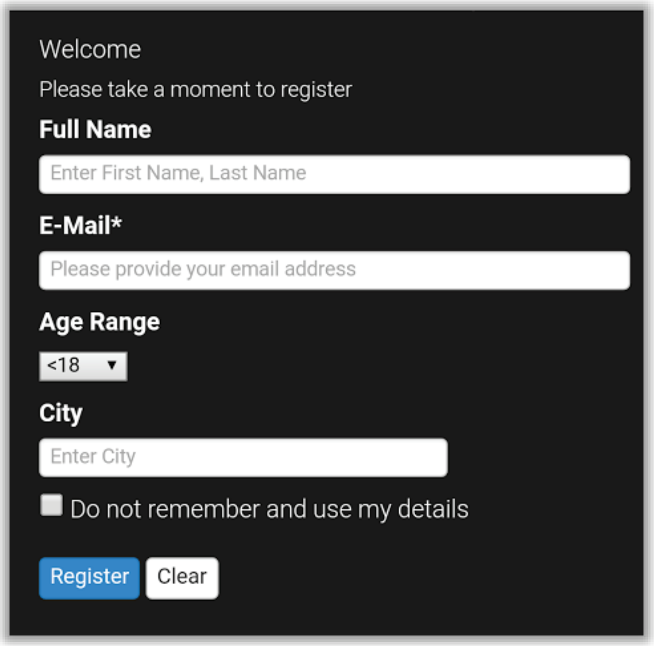
1. Associate a Wireless Client to the GuestWiFi SSID. Device should be automatically redirected to the registration.html page.
2. Verify that the Captive Portal State for the client is set to Pending and on the device browser redirects to a registration page:

   Statistics -> System -> {select RF Domain} -> Captive Portal:



Client MAC	Hostname	Client IP	Captive Portal	Port Name	Authentication	WLAN	VLAN	Remaining Time
64-BC-0C-6A-D9-5B	android-85d1a59e...	192.168.70.102	Device-Registration		Pending	GuestWiFi	70	0s

3. Register a User supplying requested information.



Welcome

Please take a moment to register

Full Name

Enter First Name, Last Name

E-Mail*

Please provide your email address

Age Range

<18 ▾

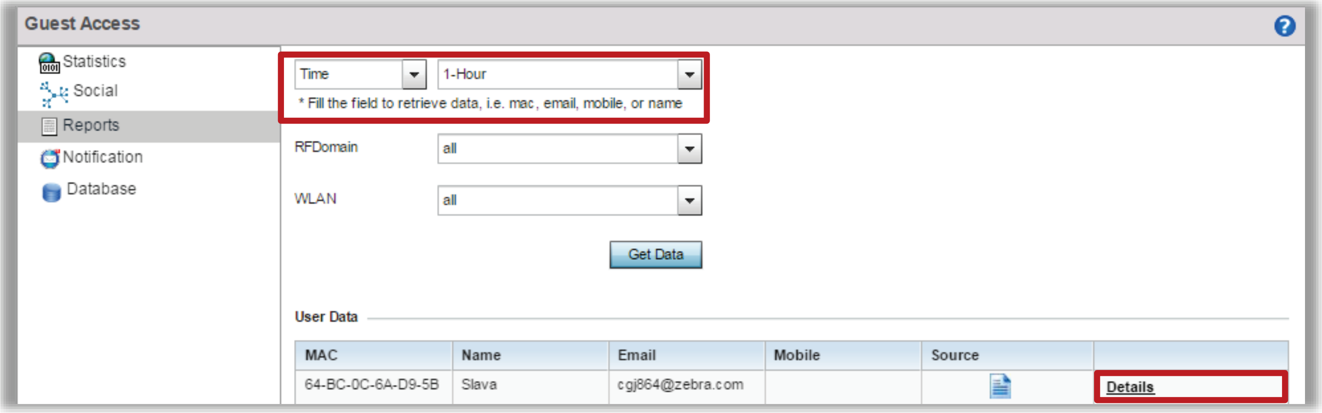
City

Enter City

☐ Do not remember and use my details

4. Verify that User/Device Record has been created in the Database

   Statistics -> Guest Access -> Reports:



Guest Access

Time: 1-Hour

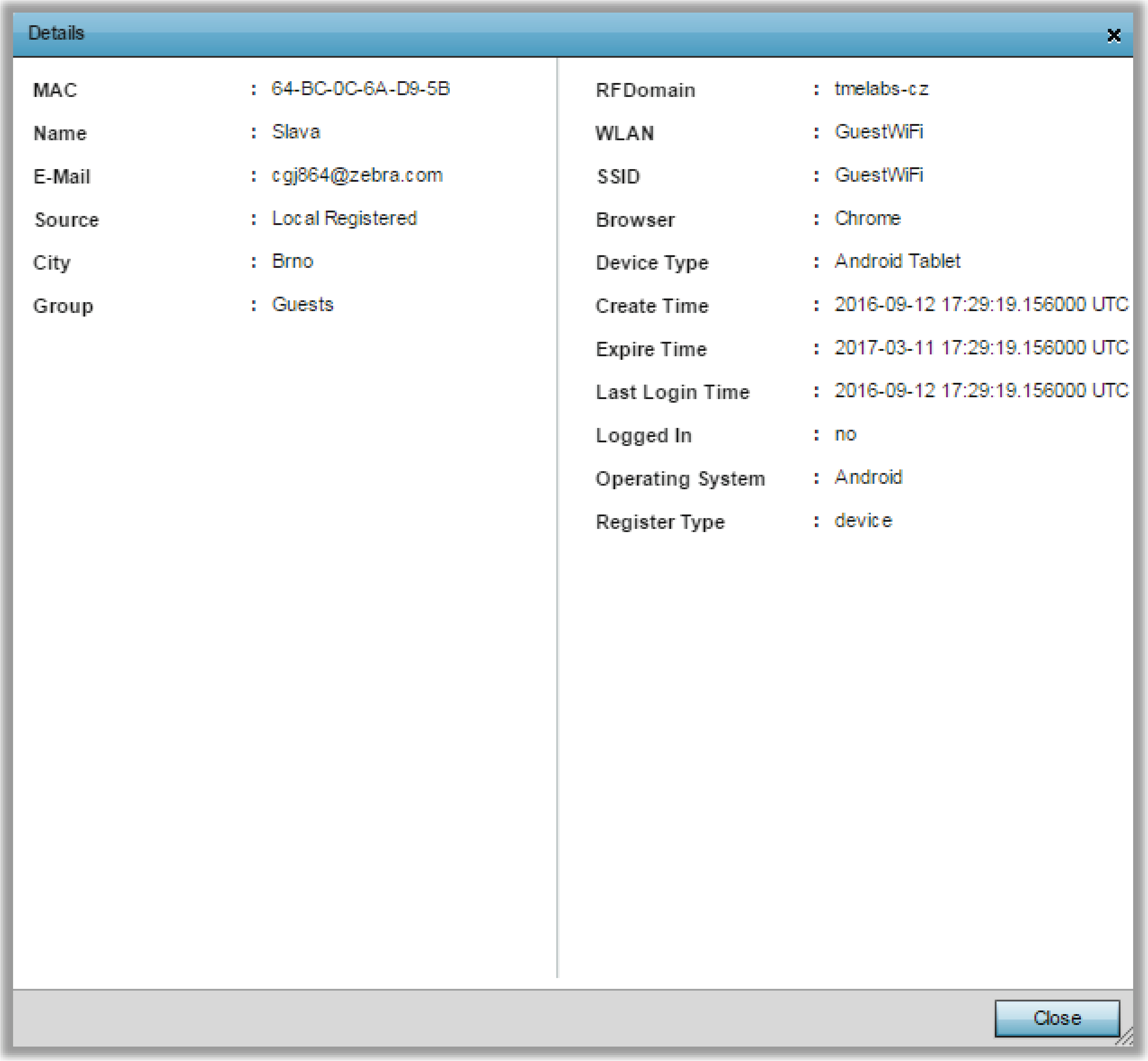
* Fill the field to retrieve data, i.e. mac, email, mobile, or name

RFDomain: all

WLAN: all

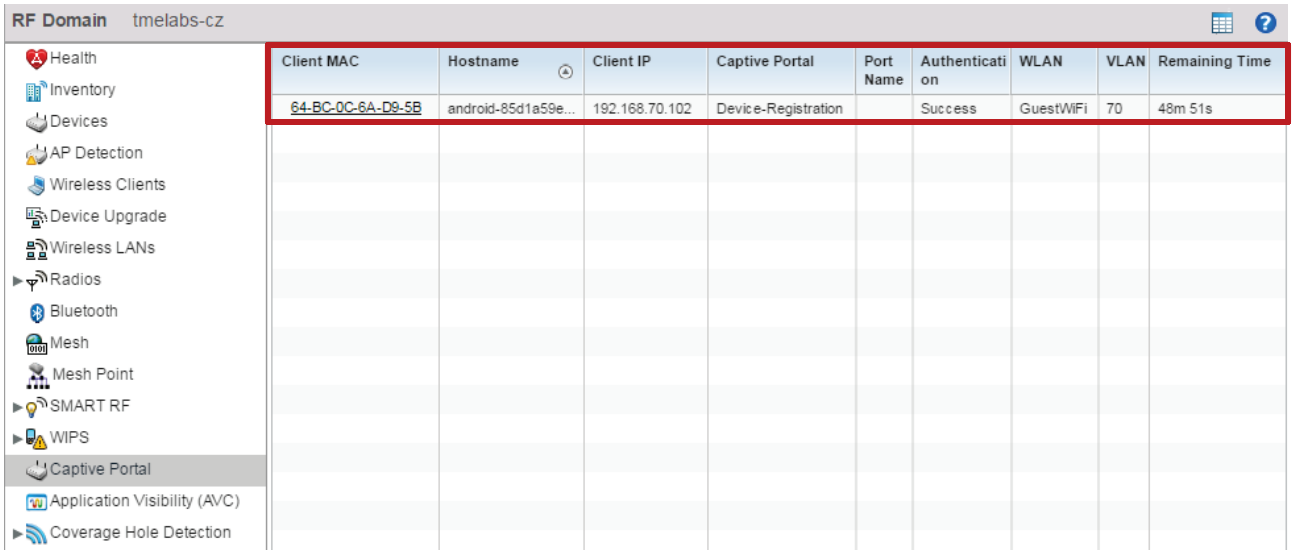
User Data

MAC	Name	Email	Mobile	Source	
64-BC-0C-6A-D9-5B	Slava	cgj864@zebra.com			Details



Details

MAC	: 64-BC-0C-6A-D9-5B	RFDomain	: tmelabs-cz
Name	: Slava	WLAN	: GuestWiFi
E-Mail	: cgj864@zebra.com	SSID	: GuestWiFi
Source	: Local Registered	Browser	: Chrome
City	: Brno	Device Type	: Android Tablet
Group	: Guests	Create Time	: 2016-09-12 17:29:19.156000 UTC
		Expire Time	: 2017-03-11 17:29:19.156000 UTC
		Last Login Time	: 2016-09-12 17:29:19.156000 UTC
		Logged In	: no
		Operating System	: Android
		Register Type	: device



RF Domain tmelabs-cz

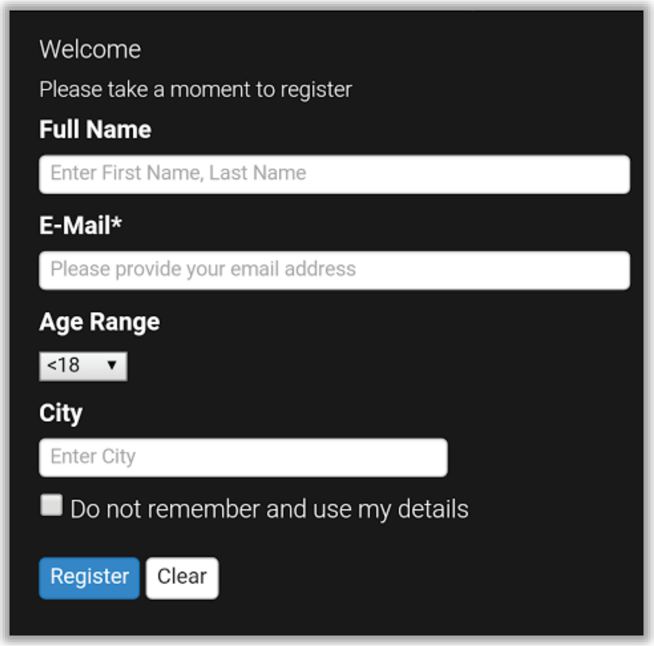
Client MAC	Hostname	Client IP	Captive Portal	Port Name	Authentication	WLAN	VLAN	Remaining Time
64-BC-0C-6A-D9-5B	android-85d1a59e...	192.168.70.102	Device-Registration		Success	GuestWiFi	70	48m 51s

CLI

1. Associate a Wireless Client to the GuestWiFi SSID. Device should be automatically redirected to the registration.html page.
2. Verify that the Captive Portal State for the client is set to Pending and on the device browser redirects to a registration page:

```
VX-1#show captive-portal sessions on {RF Domain Name}
=====================================================================================================================
=========
CLIENT                    IPv4      CAPTIVE-PORTAL      WLAN/PORT           VLAN          STATE SESSION TIME
LOGIN SOURCE
---------------------------------------------------------------------------------------------------------------------
---------
64-BC-0C-6A-D9-5B  192.168.70.102 Device-Registration GuestWiFi            70          Pending       0:00:00
n/a
=====================================================================================================================
=========
Total number of captive portal sessions displayed: 1
```

3. Register a User supplying requested information.



Welcome

Please take a moment to register

Full Name

Enter First Name, Last Name

E-Mail*

Please provide your email address

Age Range

<18 ▾

City

Enter City

□ Do not remember and use my details

Register Clear

4. Verify that User/Device Record has been created in the Database

```
VX-1#show captive-portal sessions on {RF Domain Name}
===========================================================================================================
=========
CLIENT                   IPv4     CAPTIVE-PORTAL     WLAN/PORT          VLAN         STATE SESSION TIME
LOGIN SOURCE
-----------------------------------------------------------------------------------------------------------
---------
64-BC-0C-6A-D9-5B  192.168.70.102 Device-Registration GuestWiFi          70         Success      0:55:31
n/a
===========================================================================================================
=========
Total number of captive portal sessions displayed: 1
VX-1#show guest-registration client time 1-Hour
-----------------------------------
ATTRIBUTE      VALUE
-----------------------------------
city           Brno
loggedin       yes
group          Guests
ssid           GuestWiFi
llogintime     2016-09-12 18:56:18.094000 UTC
createtime     2016-09-12 18:56:18.094000 UTC
devtype        Android Tablet
exptime        2017-03-11 18:56:18.094000 UTC
mac            64-BC-0C-6A-D9-5B
wlan           GuestWiFi
rfd            tmelabs-cz
agerange       25-34
regtype        device
browser        Unknown
os             Android
email          user@domain.com
name           Slava
-----------------------------------
```

Appendix

Database Management and Monitoring

Enable Database Events

It is recommended to enable the Database events in the Event System policy so that attention is drawn towards any error condition in the NSight Database. They will be generated by default on the event log on the console, but the user might want to receive them in some other manner, like Email or SNMP.

Database-election-fail requires manual intervention to select primary database node.

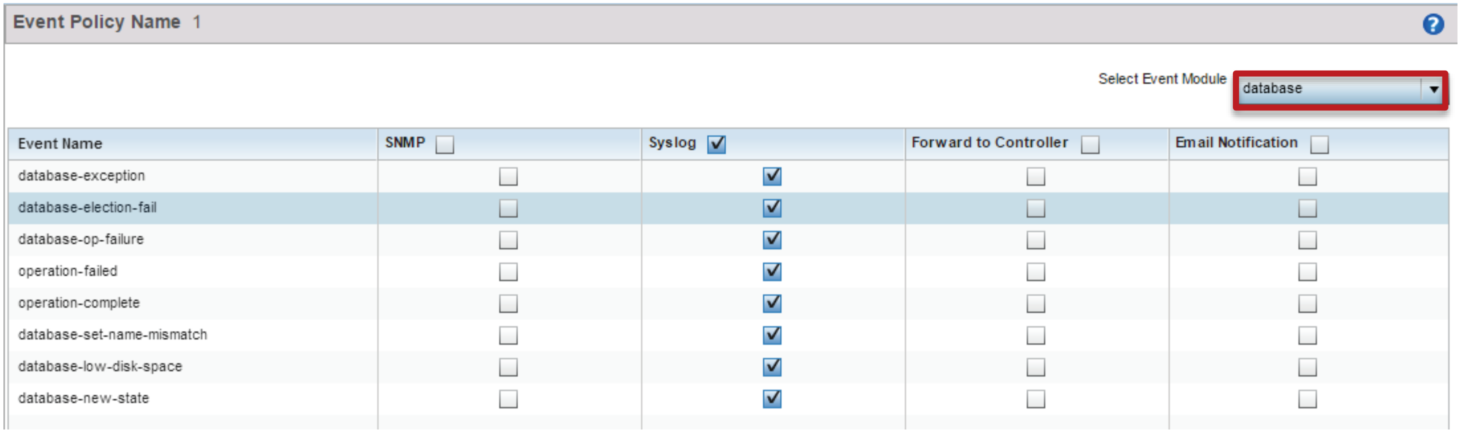
Database-exception indicates that the database is corrupted and needs manual intervention.

Operation failed and operation complete are generated in response to the success or failure of database backup and restore.

List of all database related events:

Event	Description
`DATABASE-4-DATABASE_SET_NAME_MISMATCH: MongoDB replica set name mismatch on host {host}`	Identified host do not have a database-policy applied. Check the configuration on the identified hosts.
`DATABASE-5-DATABASE_NEW_STATE: Database server is now {RS_PRIMARY|RS_SECONDARY}`	Triggered when the role of a replica member changes.
`DATABASE-4-DATABASE_OP_FAILURE: {Message}`	Triggered when a database operation fails, e.g. backup or restore. Check `flash:/log/mongod.log` file for details.
`DATABASE-6-DATABASE_OPERATION_COMPLETE: scheduled backup for database {database} {successful | failed}`	Triggered when a scheduled backup has completed successfully or failed.
`DATABASE-4-DATABASE_LOW_DISK_SPACE: Available disk space {space} is below threshold {threshold}`	Triggered when available disk space on the database storage volume falls below the configured low-disk-space-threshold.
`DATABASE-1-DATABASE_STORAGE_MISMATCH: Database server did not start because data files are incompatible with the current storage engine`	Triggered after upgrading to 5.8.2.0 and the database server was not migrated to new schema. Refer to migration of legacy NSight deployments chapter.

Database Events Configuration:



Event Policy Name 1

Select Event Module: database

Event Name	SNMP □	Syslog ☑	Forward to Controller □	Email Notification □
database-exception	□	☑	□	□
database-election-fail	□	☑	□	□
database-op-failure	□	☑	□	□
operation-failed	□	☑	□	□
operation-complete	□	☑	□	□
database-set-name-mismatch	□	☑	□	□
database-low-disk-space	□	☑	□	□
database-new-state	□	☑	□	□

```
VX(config-event-system-policy-1)#show context include-factory | grep database
 event database database-exception syslog default snmp default forward-to-switch default email default
 event database database-election-fail syslog default snmp default forward-to-switch default email default
 event database database-op-failure syslog default snmp default forward-to-switch default email default
 event database operation-failed syslog default snmp default forward-to-switch default email default
 event database operation-complete syslog default snmp default forward-to-switch default email default
 event database database-low-disk-space syslog default snmp default forward-to-switch default email default
 event database database-set-name-mismatch syslog default snmp default forward-to-switch default email
default
 event database database-new-state syslog default snmp default forward-to-switch default email default
VX(config-profile-VX9000)#show context include-factory | grep disk-space
database low-disk-space-threshold 30
```

Database Backup and Restore

The Captive Portal Database can be exported to an external storage for backup, either on-demand or scheduled at specified time intervals. Customers are encouraged to make backups regularly or at least before any system changes or firmware upgrades.

Database Export: Backup the Database files on FTP server with specified IP address, username and password

On-demand database backup

```
PRIMARY#database-backup database captive-portal <destination-URL>
// The Destination URL can be specified using FTP or SFTP
```

Scheduled Database Backup:

The database backup can be scheduled for a later time. The period of recurrence can be specified. The configuration should be done in the device context.

Scheduled database backup configuration (reoccurrence time in hours):

```
PRIMARY#self
PRIMARY(config-device-06-71-B1-5D-77-51)#database backup database captive-portal <destination URL> start-
date <MM/DD/YYYY> start-time <HH:MM> reoccurrence <time in hours>
// The Destination URL can be specified using FTP or SFTP
// reoccurrence specified the time period after which the backup will be repeated
```

Database restore from backup:

```
PRIMARY#database-restore database captive-portal <source-URL>
// The Source URL can be specified using FTP or SFTP
```

Best Practices on Captive Portal Database Management:

It is important to note the points below to prevent any database corruption

- Enable all database related events to monitor database health and operations status.
- Make regular database backups.

- Deploy replica set members to ensure high availability and data redundancy.

User Entries Import / Export

Guest Registration database allows for on demand user entries export in JSON or CSV format. It also allows to import user entries in JSON format.

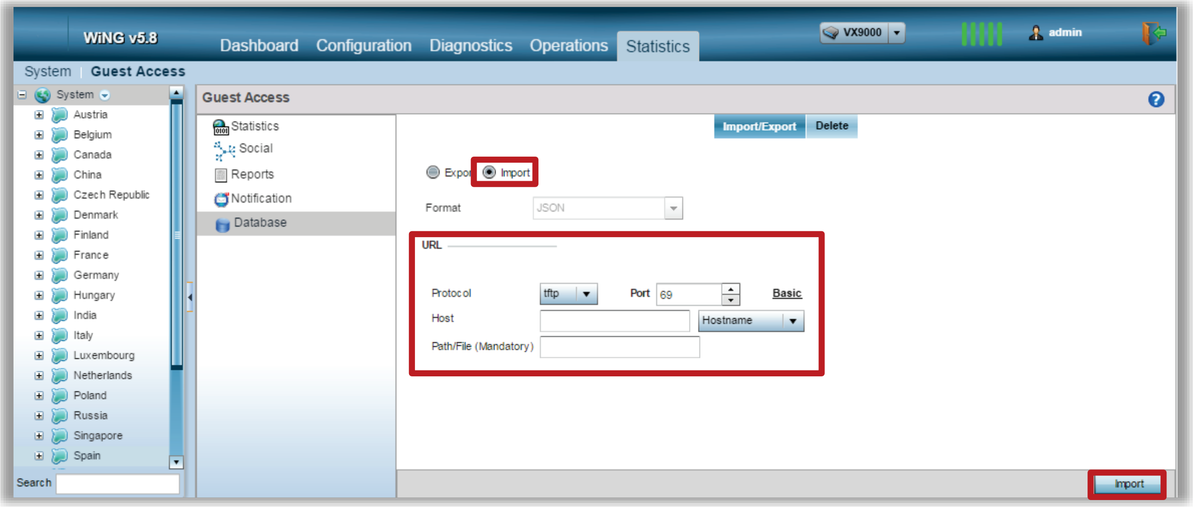
Below example shows an example user entry that is stored in the database. This format should be maintained if it is required to import user entries from an external source, mandatory key/value pairs are marked in green:

```
{"loggedin" : "no", "group" : "Samsung", "ssid" : "DEMO", "llogintime" : { "$date" : "2016-01-
01T01:01:19.670-0500" }, "regtype" : "device", "devtype" : "Samsung Smart TV", "exptime" : { "$date" :
"2021-01-01T01:01:22.775-0400" }, "mac" : "70-48-0F-89-2B-5F", "details" : "70-48-0F-89-2B-5F", "rfd" :
“STORE-1", "wlan" : "DEMO", "os" : "Samsung OS", "createtime" : { "$date" : "2016-01-01T01:01:19.670-0500"
}, "browser" : "Other" }
```

Following provides an example command for import and export of database entries:

User Entries Import – Web UI

Statistics -> Guest Access -> Database -> Import/Export:



○ Expor ● Import

Format JSON

URL

Protocol tftp Port 69 Basic

Host Hostname

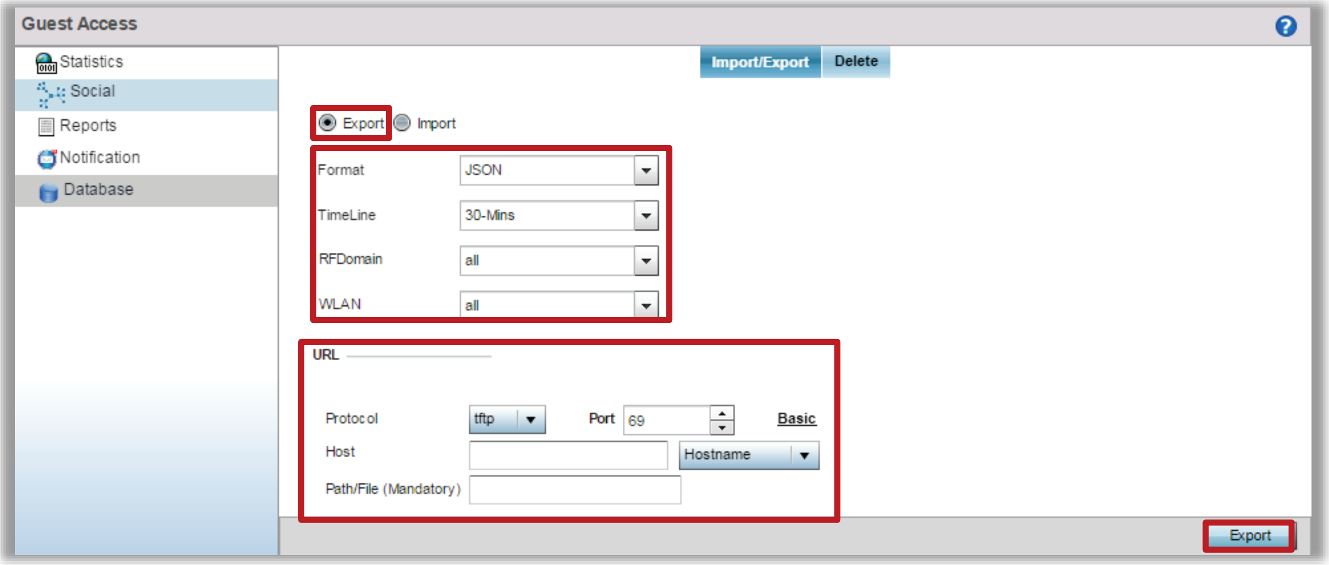
Path/File (Mandatory)

User Entries Import – CLI

```
VX-1#service guest-registration import format json {TFTP/FTP/SFTP URL}
```

User Entries Export – Web UI

Statistics -> Guest Access -> Database -> Import/Export:



● Export ○ Import

Format: JSON

TimeLine: 30-Mins

RFDomain: all

WLAN: all

Protocol: tftp

Port: 69

Host: Hostname

Path/File (Mandatory):

User Entries Export – CLI

```
VX-1#service guest-registration export format {csv | json} {URL} rfdomain {RF Domain Name} time {30-Mins |
2-Hours | 5-Hours | 1-Day | 1-Week | 1-Month | all} wlan {WLAN name}
```

User Entries Purging

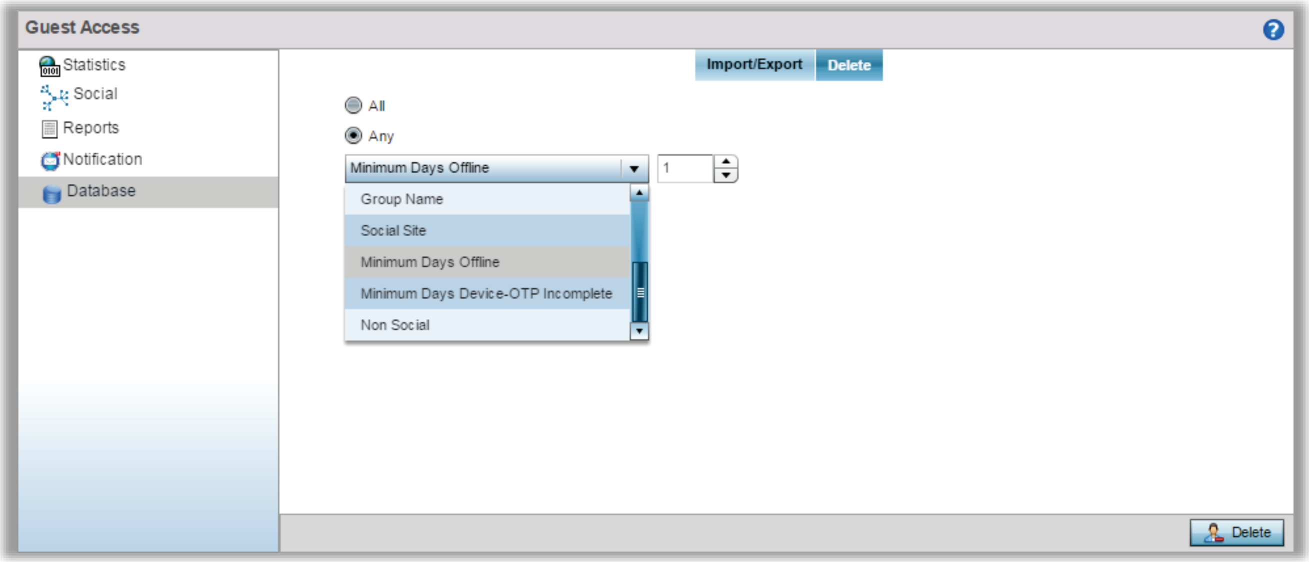
In case guest database is reaching its limit, it is possible to purge unused or otherwise less important user records using the following matching criteria:

- Users who have not accessed the network for a specified minimum number of days
- Users belonging to a particular user group
- Users registered through social authentication (Facebook/Google)
- Users not registered through social authentication
- Incomplete user registrations that use One-Time-Passcode (One-Time-Passcode not used)

Purge Match Criteria	Description
email	An entry(ies)with specific Email address
group	Entries that belong to a specific RADIUS Group
mac	Entry containing MAC of the device
mobile	An entry(ies) with specific Phone number
name	Full Name
non-social	All user not using a social media site to log in
offline-for	All users that were offline for <1-999> days
otp-incomplete-for	All entries with one-time-passcode incomplete for <1-999> days
social	All entries using a specific social media site to log in
wlan	All entries that belong to a specific WLAN
all	All Users

Deleting a User Record – Web UI:

Statistics -> Guest Access -> Database -> Delete:



○ All
● Any
Minimum Days Offline 1

Deleting a User Record – CLI:

```
VX-1#service guest-registration delete ?
  all                 Delete all users
  email               Email address
  group               Group
  mac                 MAC address
  mobile              Mobile phone number
  name                Full name
  non-social          All users not using a social site to log in
  offline-for         Specify minimum amount of time offline
  otp-incomplete-for  Specify minimum amount of time registration with
                      one-time-passcode incomplete
  social              Social site used to log in
  wlan                Wireless LAN
```

Database Service Commands

These commands should only be used as directed by support staff or as in documented procedures outlined in this guide.

Command	Description
`service database drop {nsight | captive-portal} collection {WORD}`	Drops the specified collection from the selected database.
`service database remove-all-files`	Removes all files related to the database server. Requires the database server to be stopped. Reloads the device after execution.
`service database replica-set {add | delete} member {A.B.C.D | WORD}`	Allows direct manipulation of the replica-set members.
`service database server {start|stop|restart}`	Starts, stops or restarts the database server.
`service database use-secondary-storage`	The VX9000 default partition table is limited to a partitions with a maximum size of 2 terabytes. This command provides support for an additional virtual disk with a partition table format supporting partition sizes in excess of 2 terabytes. This command should be used only as documented in the “Using secondary storage” section of

	this guide.

VX9000 Secondary Storage Options

The current VX9000 has a disk size limitation on the default disk of 2 Terabytes. Should this not be of a sufficient size for the database server storage, the VX9000 can use a second virtual disk. When using a second disk, the VX9000 can support disks with sizes greater than 2 Terabytes.

Note

Consult the Virtual Hosting platform's documentation to determine how to provision an additional virtual disk for the VX9000 guest installation. Once this additional disk has been provisioned and the VX9000 guest restarted, secondary storage can be enabled.

Warning

Enabling secondary storage does not copy data files to the new location.

Careful consideration should be given when considering enabling secondary storage. The best time to enable it is immediately after provisioning the guest instance, before enabling Captive Portal.

If there is a requirement to enable secondary storage after the initial provisioning of the VX9000 guest instance, it is advised that backups of the database be taken before enabling secondary storage. After secondary storage is enabled, the database can be restored.

Alternatively, if the VX9000 instance is a member of a replica-set and is not the primary, the database server will perform a full data sync after it is restarted using the new storage disk.

To enable secondary storage, execute the following command:

```
PRIMARY#service database use-secondary-storage

************************************  WARNING  *************************************
** Execution of this command will configure this device to store the database     **
** files on a secondary drive.  This device will reload after execution.          **
** NOTE: Current database files will be erased.                                   **
************************************************************************************
Are you sure you want to proceed? (y/n): y
Enabling secondary storage on sdb.................complete.
Using sdb for secondary database storage
PRIMARY#
```

Automatic Captive Portal Database Snapshots

By default, Captive Portal registration database does automatic database snapshots to provide a first level recovery mechanism. It is set to 00:00 every day and up to 7 latest snapshots will be stored:

```
VX-1#show guest-registration backup-snapshots
-----------------------------------------------------------------------------
File                                    Size        Creation Time
-----------------------------------------------------------------------------
users_20160906-0000.json               15054        09-06-2016 00:00
users_20160907-0200.json               15054        09-07-2016 00:00
users_20160908-0000.json               15054        09-08-2016 00:00
users_20160909-0000.json               15054        09-09-2016 00:00
users_20160910-0000.json               15054        09-10-2016 00:00
users_20160911-0000.json               15054        09-11-2016 00:00
users_20160912-0000.json               15054        09-12-2016 00:00
-----------------------------------------------------------------------------
```

Scaling

Controller Platform	Maximum Number of Records
NX75X0	1 Million
NX9XX0	2 Million
VX9000	2 Million

VX9000 VM Hardware Requirements

Capacity (User Entries)	1 Million	2 Million
CPU	6 Core @2.5GHz	12 Core @2.5 GHz
Memory	16 GB	32 GB
Storage	500 GB	1 TB

Event System Policy

Certain events related to the Captive Portal activity can be captured and processed at the external Syslog server or sent out as an SNMP trap:

```
VX(config-event-system-policy-<POLICY-NAME>)#show context include-factory | include captive

 event captive-portal inactivity-timeout syslog default snmp default forward-to-switch default email
default
 event captive-portal session-timeout syslog default snmp default forward-to-switch default email default
 event captive-portal no-service-page-sent syslog default snmp default forward-to-switch default email
default
 event captive-portal server-monitor-state-change syslog default snmp default forward-to-switch default
email default
 event captive-portal vlan-switch syslog default snmp default forward-to-switch default email default
 event captive-portal client-disconnect syslog default snmp default forward-to-switch default email default
 event captive-portal client-removed syslog default snmp default forward-to-switch default email default
 event captive-portal auth-success syslog default snmp default forward-to-switch default email default
default
 event captive-portal purge-client syslog default snmp default forward-to-switch default email default
 event captive-portal allow-access syslog default snmp default forward-to-switch default email default
 event captive-portal data-limit-exceed syslog default snmp default forward-to-switch default email default
 event captive-portal auth-failed syslog default snmp default forward-to-switch default email default

Sep 12 21:17:21 2016: 8533-brq-1 : %CAPTIVE-PORTAL-6-AUTH_SUCCESS: Captive-portal authentication success
for client 64-BC-0C-6A-D9-5B(192.168.70.102) user ''
```

Troubleshooting

Remote-Debug Captive Portal

Starting from WiNG 5.8.1 release new remote-debug functionality allows an administrator to perform a live troubleshooting on captive portal related events filtered by specific client at certain location or an AP.

```
VX-1#remote-debug captive-portal rf-domain {RF Domain Name} clients {Client MAC} max-events {count}
duration {count in seconds} events all
Printing up to 999 messages from each remote system for upto 999 seconds. Use Ctrl-C to abort
[8533-brq-1] 19:16:51.397: radius:aaa-policy ONBOARD-VX user: 64-BC-0C-6A-D9-5B mac: 64-BC-0C-6A-D9-5B
server_is_candidate: 1 0 0 0 0 0 (ra
[8533-brq-1] 19:16:51.398: radius:access-req sent to wireless controller to be proxied to 127.0.0.1:1812.
(attempt 1) for 64-BC-0C-6A-D9-5B
[8533-brq-1] 19:16:51.439: radius:rx access-reject for 64-BC-0C-6A-D9-5B (radius.c:3711)
[8533-brq-1] 19:16:51.439: radius:failover to captive-portal for non data-ready MU 64-BC-0C-6A-D9-5B
(radius.c:3752)
[8533-brq-1] 19:16:51.810: client:Hotspot client IP: 192.168.70.102, vlan: 70, Mac: 64-BC-0C-6A-D9-5B
(hs_main.c:2552)
[8533-brq-1] 19:16:51.810: client:Hotspot client 64-BC-0C-6A-D9-5B is being redirected on wlan 7 and vlan
70 (hs_main.c:2569)
[8533-brq-1] 19:16:51.819: client:read: client 64-BC-0C-6A-D9-5B, num_bytes: 187, p_sess->buf: GET
/generate_204 HTTP/1.1
User-Agent: Dalv
[8533-brq-1] 19:16:51.819: client:Hotspot policy on wlan 7 and vlan 70 for client 64-BC-0C-6A-D9-5B
(hs_main.c:2106)
[8533-brq-1] 19:16:51.819: client:cpstats server: captive.extremenoc.com for client 64-BC-0C-6A-D9-5B
(hs_main.c:655)
[8533-brq-1] 19:16:51.819: client:Client 64-BC-0C-6A-D9-5B, ap_mac: 74-67-F7-5C-42-B7, ssid: GuestWiFi
(hs_main.c:999)
[8533-brq-1] 19:16:51.819: client:Client 64-BC-0C-6A-D9-5B, server: captive.extremenoc.com, reg_type: 1
(hs_main.c:1001)
[8533-brq-1] 19:16:51.819: client:mu_mac: 64-BC-0C-6A-D9-5B redirect url:
https://captive.extremenoc.com:444/Device-Registration/registration
[8533-brq-1] 19:17:21.48: client:captive-portal registration req [HS_REG_REQ] received for 64-BC-0C-6A-D9-
5B (extif.c:1181)
[8533-brq-1] 19:17:21.48: client:user registration request/info sent to user-db (extif.c:644)
[8533-brq-1] 19:17:21.48: client:reg status [Successfully registered the user details] [2] for 64-BC-0C-6A-
D9-5B (extif.c:1214)
[8533-brq-1] 19:17:21.48: client:sent guest registration response to cgi for 64-BC-0C-6A-D9-5B
(extif.c:1220)
[8533-brq-1] 19:17:21.49: client:adding client 64-BC-0C-6A-D9-5B to hotspot user cache (usercache.c:339)
[8533-brq-1] 19:17:21.49: client:change fdb hotspot auth state for client 64-BC-0C-6A-D9-5B (extif.c:1015)
[8533-brq-1] 19:17:21.49: client:hotspot session timeout 3600 for client 64-BC-0C-6A-D9-5B (extif.c:1072)
[8533-brq-1] 19:17:21.49: client:set_hotspot_state() with state=1, reset_stats=0 for client 64-BC-0C-6A-D9-
5B (config.c:1262)
[8533-brq-1] 19:17:21.49: client:hotspot auth success received for mu 64-BC-0C-6A-D9-5B (extif.c:1252)
[8533-brq-1] 19:17:21.215: client:client:64-BC-0C-6A-D9-5B cpstats ip : 1.1.1.2 (failover.c:376)
```

General Captive Portal Troubleshooting Q&A

Q: Wireless Client is not being redirected to the landing page, is this a bug?

A: Most likely not. Verify and make sure the following checks out:

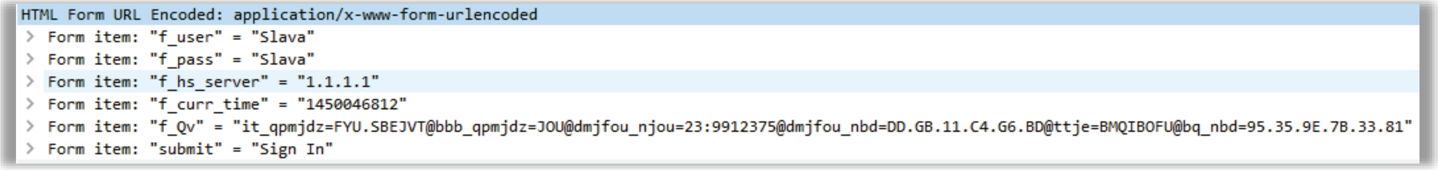
1. Client can resolve names via configured DNS server and client can reach internet / external networks under normal conditions without Captive Portal.
2. Captive Portal server is assigned to the device that should perform client capture and redirection. In “Self” mode captive portal server should be assigned to the Access Point profile, in “Centralized” or “Centralized-Controller” mode Captive Portal server should be assigned to the Wireless Controller.
3. Captive Portal server mode matched the architecture selected. I.e. “Self” mode should only be used when Captive Portal server is running in a distributed architecture on each Access Point. “Centralized” mode should be used on a single controller with real IP address or FQDN of the controller. “Centralized-controller” mode should be used whenever a cluster of controllers is deployed with virtual hostname.

4. If Centralized-controller mode is used SVI must be present in the Guest User VLAN with an IPv4 address to perform capture and redirection.
5. DNS whitelist must contain FQDNs or IP addresses of all the external web servers as permit rules. Additionally, all the contents of the pages that refer to external sources (like ads or videos) must also be allowed in the DNS whitelist.
6. IP Access Lists assigned inbound direction on the Guest WLANs allow communication to captive portal server address on ports 444 (https mode) or 880 (http mode). In case captive portal server is running on the Access Point without any SVI in the Guest User VLAN, communication to an IP address 1.1.1.1 should be allowed.

Q: Client is able to get to landing page and submit data, but Captive Portal on the AP/Controller still block access to the client.

A: Check the following:

1. Make sure client side script is present to allow a client to make a HTTP POST and submit user credentials or terms&agreement accept to the captive portal server (usually a problem when using custom or externally hosted web pages). Verify by taking a packet capture filtered by the client's IP address and look into the contents of HTTP POST. For example:



```
HTML Form URL Encoded: application/x-www-form-urlencoded
> Form item: "f_user" = "Slava"
> Form item: "f_pass" = "Slava"
> Form item: "f_hs_server" = "1.1.1.1"
> Form item: "f_curr_time" = "1450046812"
> Form item: "f_Qv" = "it_qpmjdz=FYU.SBEJVT@bbb_qpmjdz=JOU@dmjfou_njou=23:9912375@dmjfou_nbd=DD.GB.11.C4.G6.BD@ttje=BMQIBOFU@bq_nbd=95.35.9E.7B.33.81"
> Form item: "submit" = "Sign In"
```

2. Run remote-debug captive-portal command from the CLI with client MAC as a filter and monitor the messages reported when client presses Submit or Login button.