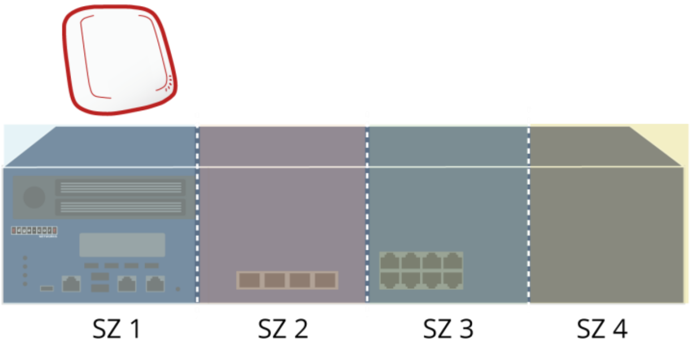
Concept of “Service Zone”

Service Zones are virtual partitions of the physical LAN side of a Controller.
Similar to VLANs, Service Zones can be separately managed and defined with their own user landing pages, network interface settings, DHCP servers, authentication options, policies, security settings, and so on. By associating Service Zones with a unique VLAN Tag (when using tag-based mode) and an SSID, administrator can flexibly separate wired and wireless networks with ease.



The LAN Side of The Controller

1. How to enable Service Zones

Service Zone is a logic partition of WLAN controller’s LAN. The concept of Service Zone is that it is a virtual gateway with customizable login pages and own gateway properties (such as VLAN tag, LAN IP address, DHCP server settings, authentication options, etc.). With up to nine independent Service Zone profiles, the WLAN controller is capable of servicing multiple hotspot franchises with a single device.

Administrators are able to check the status of the Service Zones from “*Main › System › Service Zone”*. Click on the Service Zone name to start configuring settings such as VLAN tag, LAN-side IP address, DHCP server settings and authentication options. For more details, please refer to *“2. How to configure Service Zone.”*

2. How to configure Service Zones

Service Zones are virtual partitions of the physical LAN side of the Controller. Similar to VLANs, they can be separately managed and defined with their own user landing pages, network interface settings, DHCP servers, authentication options, policies, security settings, and so on. By associating Service Zone with a unique VLAN Tag (when using tag-based mode) and an SSID, administrator can flexibly separate wired and wireless networks with ease.

Service Zone features include:
(1) VLAN, Isolation, NAT/Router Mode
(2) DHCP Server Option
(3) Authentication Settings
(4) Page Customization

(1) VLAN/IP Address, Isolation, NAT/Router Mode

VLAN/IP Address

IP address is the Controller's IP address for users connected to this Service Zone to reach the Controller. **Subnet mask** defines the size of the Service Zone network and range of IP addresses assigned to this Service Zone. To add additional IP ranges, enter these IP ranges to the **Network Alias List** and check **Enable.** Always remember to click **Apply** upon completion.

Isolation

- **Inter-VLAN Isolation**: In addition to isolation between clients in different VLANs, 2 clients within the same VLAN will also be isolated if their traffic comes in to the Controller from different physical ports. Note that Isolation is done when traffic passes through the Controller.
- **Clients Isolation**: All clients on the same Layer 2 network are isolated from one another in this Service Zone.
- **None**: No isolation will be applied to clients in this Service Zone.

Note:

1. When a switch or AP is deployed and the client is not directly connected to the controller, Station Isolation has to be enabled on the AP/switch to ensure isolation.
2. When "None" is selected, a switch port connecting to the LAN port of the WLAN controller may be shut down if the switch has loop protection enabled and there are more than 2 VLANs belong to one Service Zone.

NAT/Router Mode

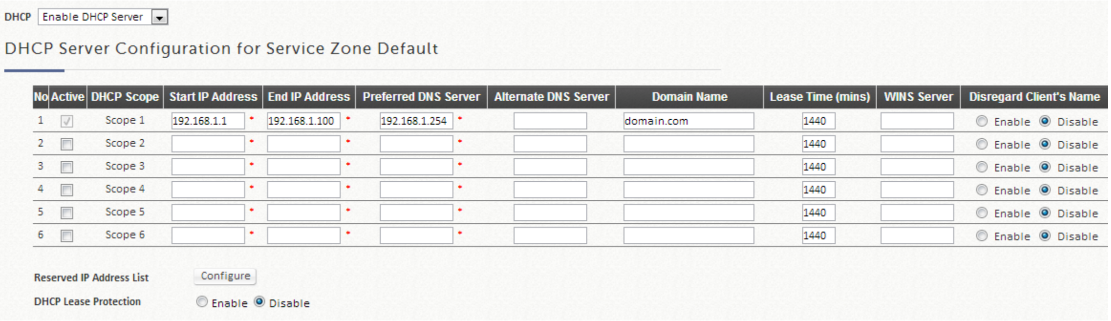
NAT is the acronym for Network Address Translation which translates private IP addresses for devices on the LAN side of a controller to a routable IP address before forwarding into uplink network. Private IP addresses are invisible to devices or routers on the WAN side of the controller, only the controller deploying the NAT knows their corresponding translation. This mode not only protects users on the LAN from being 'seen' by external devices but also solves the problem of limited public IP addresses.

Router mode, as the name suggests, is a network operating without address translation in and out of the Controller. Router mode can be used when using public IP addresses or when downstream devices require a routable IP address to be 'seen' by devices or servers on the WAN side.

(2) DHCP Server Option

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network. The controller supports independent DHCP settings for each Service Zone profile. Options include Disable

DHCP option, Enable built-in DHCP server or DHCP Relay.



DHCP Enable DHCP Server ▾

DHCP Server Configuration for Service Zone Default

No	Active	DHCP Scope	Start IP Address	End IP Address	Preferred DNS Server	Alternate DNS Server	Domain Name	Lease Time (mins)	WINS Server	Disregard Client's Name
1	☑	Scope 1	192.168.1.1 *	192.168.1.100 *	192.168.1.254 *		domain.com	1440		○ Enable ● Disable
2	□	Scope 2	*	*	*			1440		○ Enable ● Disable
3	□	Scope 3	*	*	*			1440		○ Enable ● Disable
4	□	Scope 4	*	*	*			1440		○ Enable ● Disable
5	□	Scope 5	*	*	*			1440		○ Enable ● Disable
6	□	Scope 6	*	*	*			1440		○ Enable ● Disable

Reserved IP Address List Configure

DHCP Lease Protection ○ Enable ● Disable

- DHCP Server Configuration – The default setting for DHCP Server is “Enable”. Select other options from the drop-down list.
- Define the IP range for issuing when using Enable DHCP Server (built-in). There are a total of six DHCP pools for configuration.
- Lease Time for each pool cannot be smaller than the twice value of Idle Timeout.
- Reserved IP Address List – A configuration list for reserving certain IP addresses within the DHCP Server IP range for specific devices such as an internal file server.
- DHCP lease protection – This is an optional checking mechanism on the Controller when Enabled, will check to see if the lease expired IP is currently online. If yes, the Controller will halt the issuing of this IP address until the user session terminates.
- Click “Apply” to activate changes.

(3) Authentication Settings

Once the administrator has properly configured the authentication servers under the Main Menu, he/she can customize authentication options for each Service Zone for downstream clients to login. Note that Authentication is always enabled by default.

Authentication Options: Administrators can designate configured authentication servers for use. Postfix will be used as authentication server identifier when more than one authentication server is enabled for service.

Portal URL: The specification of a desired landing page may be configured here. When enabled, the administrator can choose to set the URL of an opened browser after users’ initial login.

MAC Authentication: Once enabled, if the MAC address of the connected device is entered in the configured RADIUS Server, the Controller will automatically authenticate and grant immediate access to this device if authentication succeeds. Users will experience transparent login.

PPP Authentication: Point-to-Point Protocol (PPP) is a data link protocol commonly used in establishing a direct connection between two networking nodes. When this feature is enabled for service, end users may configure a dial-up connection setting with a valid username and password (support only Local and RADIUS users). Once the dial-up connection has been established, the user would have been authenticated successfully without further UAM login.

IP Address Range Assignment field configures the starting IP range which PPP can assign IP addresses to dial-up virtual interfaces. The assigned interface IP address is used to route between the networks on both side of the tunnel.

(4) Page Customization
Each Service Zone can be configured to have its unique Login Pages or Message Pages. There are three types of Login Pages: General Login Page, PLM Open Type Login Page (for Port Location Mapping free access), and PMS Billing Plan Selection Page. A Service Disclaimer page can be enabled if required. These pages are fully customizable to give administrators complete flexibility. Message Pages can also be customized and message pages include: Login Success Pages, Login Success Page for On-Demand Users, Login Fail Page, Device Logout Page, Logout Success Page, Logout Failed Page, and Online Device List.

There are three customization options to choose from apart from the Default Page: Customize with Template, Upload Your Own, and Use External Page.

Default: Standard Default Login Page with company logo. Service Disclaimer can be enabled if needed.
Customize with Template: For this option, a template is available for easy customization. The general layout has been set for the administrator but the contents can be customized. A color theme and a logo can be uploaded, and contents field such as Service Disclaimer, text colors can entered within the template presentation layout.
Upload Your Own: An HTML file can be uploaded as the Login Page. The "Download HTML Sample File" gives administrators a sample HTML code to edit from. Once this sample HTML code is downloaded, open the file with any browser, and right click and select "View Page Source". You may edit the HTML code with any text editor as long as the file is saved in .html format.
Use External Page: The Login Page can be a defined external URL. This option requires extensive knowledge of URL parameter utilization that works together with the Message Pages and should be organized carefully. For more details on External Login Page customization, please refer to the Technical Guide.

For a Preview of the custom page, click “Apply” followed by the “Preview” button. Similarly, the four options are available for Message Pages.