CERIO Corporation

DR-3000

CenOS5.0 Access Controller with VPN Gateway

(60/128 APs)

User's Manual

1. Software Configuration

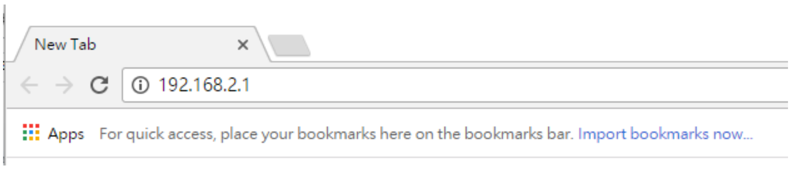
DR-3000 supports web-based configuration. Upon the completion of hardware installation, **DR-3000** can be configured through a PC/NB by using its web browser such as Internet Explorer 6.0 or later.

- **Default IP Address**: 192.168.2.1
- **Default Subnet Mask**: 255.255.255.0
- **Default Username and Password**

MODE	Router mode	
Management Account	Root Account	
Username	root	
Password	default	

Launch Web Browser

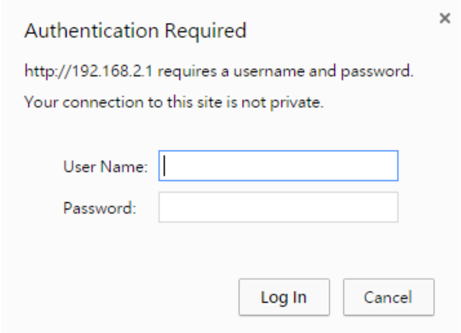
Launch as web browser to access the web management interface of system by entering the default IP Address, http://192.168.2.1, in the URL field, and then press Enter.



New Tab

192.168.2.1

Apps For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...



Authentication Required

http://192.168.2.1 requires a username and password.
Your connection to this site is not private.

User Name:

Password:

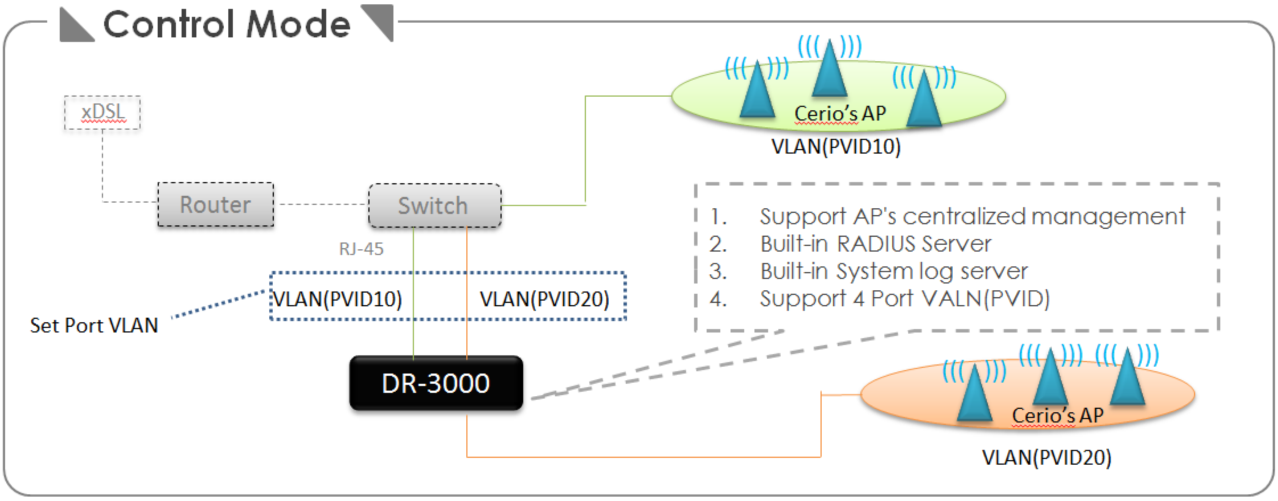
Log In Cancel

Please use default Users name: **"root"** and default password **"default"** to login.

2. Operating Mode Introduction

2.1 Control Mode

When the Control Mode is selected then DR-3000 will be pure AP centralized management controller, the system built-in RADIUS server, system log server and support port VLAN (PVID) setup. The Control mode can via VPN tunnel go to centralized management AP's

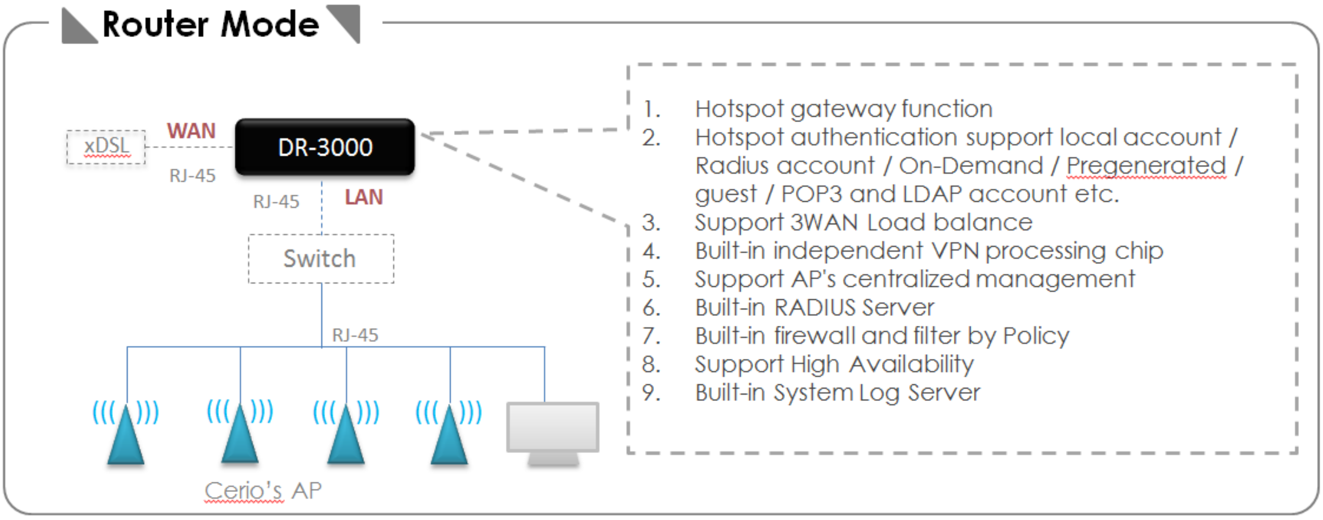


1. Support AP's centralized management
2. Built-in RADIUS Server
3. Built-in System log server
4. Support 4 Port VALN(PVID)

2.2 Router Mode

When administrator select use Route mode then system can set 1WAN 3LAN Router also can select 3WAN 1LAN or 4WAN outbound load balancer.

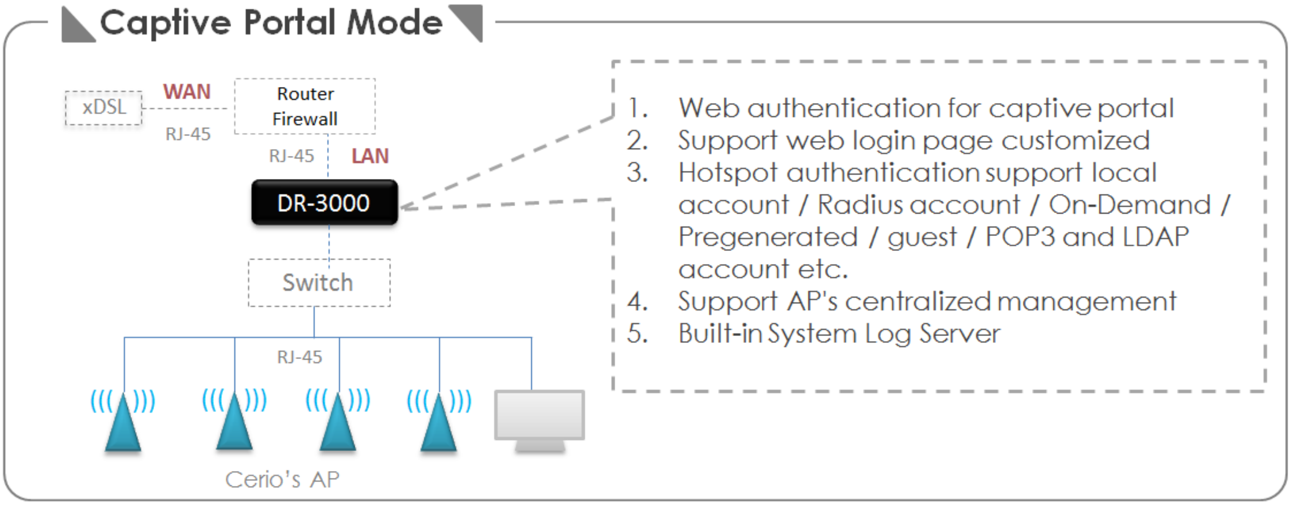
This Router mode support IP Routing setup/Firewall/HA/VPN/Multi-WAN/QoS enforcement and Built-in AAA Radius server.



1. Hotspot gateway function
2. Hotspot authentication support local account / Radius account / On-Demand / Pregenerated / guest / POP3 and LDAP account etc.
3. Support 3WAN Load balance
4. Built-in independent VPN processing chip
5. Support AP's centralized management
6. Built-in RADIUS Server
7. Built-in firewall and filter by Policy
8. Support High Availability
9. Built-in System Log Server

2.3 Captive Portal Mode

If the environment already has a router or firewall device, administrator demand is only to add the new page hotspot function, this time can be switched to Captive Portal mode and connected in parallel to the router or firewall equipment can be completed.



1. Web authentication for captive portal
2. Support web login page customized
3. Hotspot authentication support local account / Radius account / On-Demand / Pregenerated / guest / POP3 and LDAP account etc.
4. Support AP's centralized management
5. Built-in System Log Server

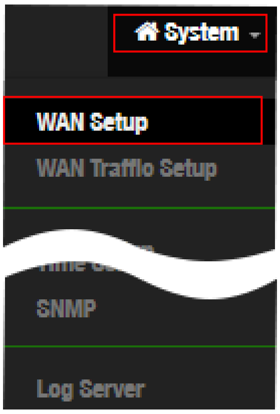
3. System Configuration

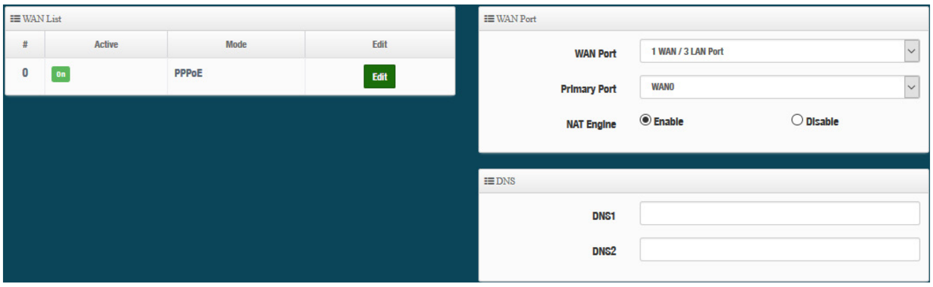
CERIO's DR-3000 is multifunctional authentication Gateway, support multi-WAN outbound load balance and can centralized managed CenOS5.0 AP. The DR-3000 Built-in hardware independent VPN engine administrator can build a secure tunnel in the network environment and support High Availability can make sure that the network is working normally.

3.1 WAN Setup

Administrator can set one WAN or multi-WAN load balance in the WAN Setup function.

Please click System ➔ WAN Setup





WAN List

#	Active	Mode	Edit
0	On	PPPoE	Edit

WAN Port

WAN Port: 1 WAN / 3 LAN Port

Primary Port: WAN0

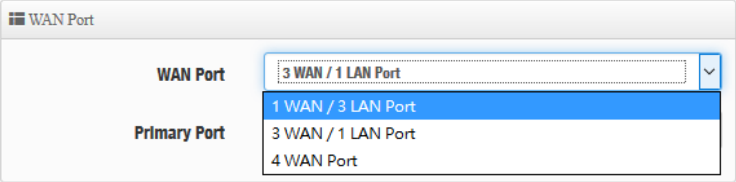
NAT Engine: ● Enable ○ Disable

DNS

DNS1:

DNS2:

WAN Port Setup



WAN Port

WAN Port	3 WAN / 1 LAN Port
Primary Port	

- **WAN Port:** Administrator can select 1 WAN/3 LAN or 3 WAN/1 LAN or 4WAN port, the default is 1 WAN/3 LAN Port.

  When setting is different

  The physical network ports are defined as follows:

  1 WAN / 3 LAN: ETH1 is the WAN port, ETH2 is the first LAN port, ETH3 is the second LAN port, and ETH4 is the third LAN port.

  3 WAN / 1 LAN: EHT1 is the LAN port, ETH2 is the first WAN port, ETH3 is the second WAN port, and ETH4 is the third WAN port.
- **Primary Port:** If set 3 WAN or 4WAN function, administrator must select one primary for WAN Port.
- **NAT Engine:** If enable the function then NAT will up performance, but firewall and routing rule of DR-3000 will auto disable.

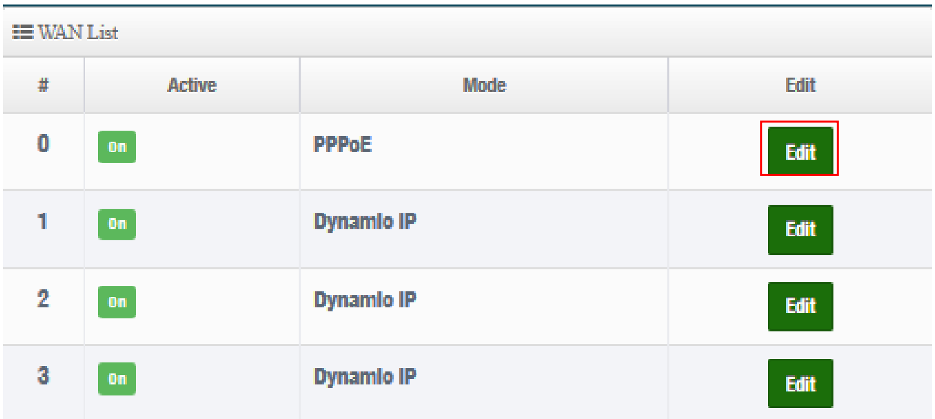
Notice

If administrator choose 3WAN or 4WAN, please click save button system will display WAN function setup on WAN List.

WAN List

Administrator can set four connection types for the WAN port: Static IP, Dynamic IP, PPPoE and PPTP, at the same time can also Enable or Disable for NAT or DMZ functions.

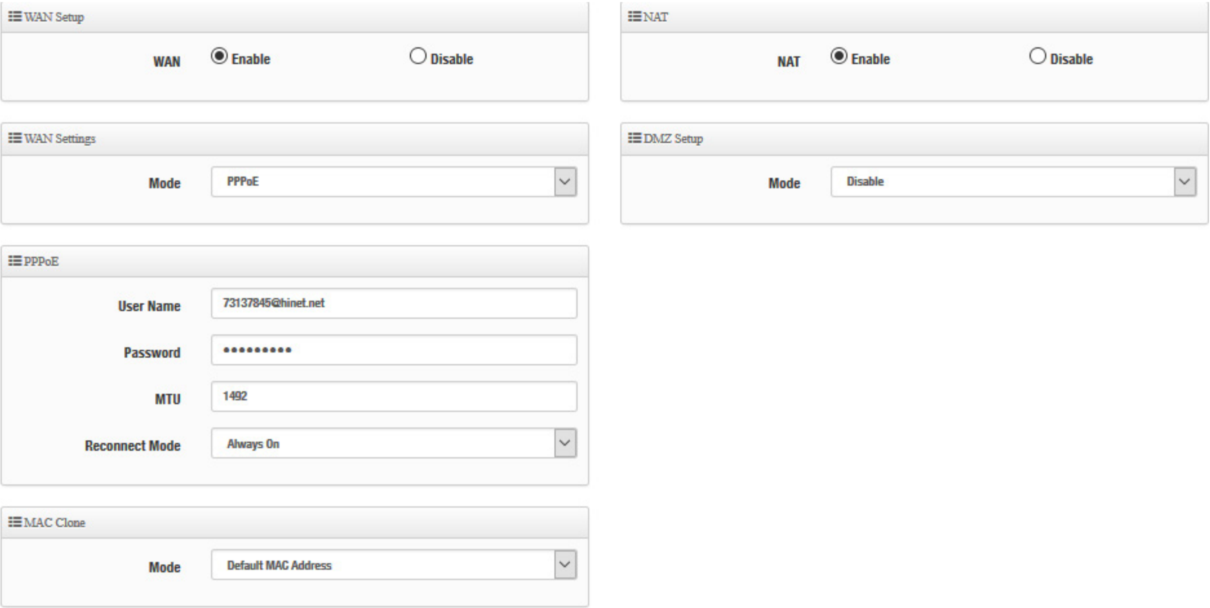
Please click Edit button in WAN List.



WAN List

#	Active	Mode	Edit
0	On	PPPoE	Edit
1	On	Dynamic IP	Edit
2	On	Dynamic IP	Edit
3	On	Dynamic IP	Edit

- **Edit:** Administrator can set WAN function.



WAN Setup
WAN ● Enable ○ Disable

NAT
NAT ● Enable ○ Disable

WAN Settings
Mode: PPPoE

DMZ Setup
Mode: Disable

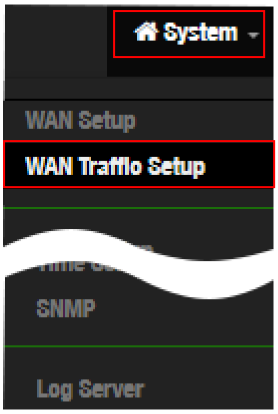
PPPoE
User Name: 73137845@hinet.net
Password: •••••••••
MTU: 1492
Reconnect Mode: Always On

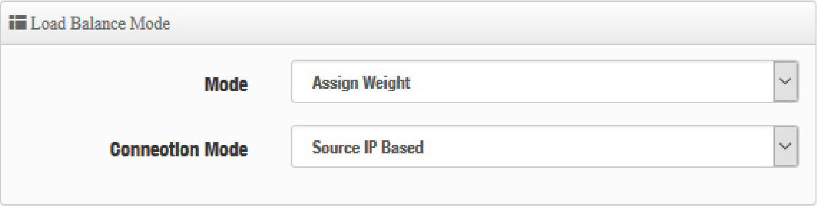
MAC Clone
Mode: Default MAC Address

- **WAN Setup:** Administrator can set Enable or Disable for the WAN Port function.
- **WAN Settings:** Administrator can select Static IP, Dynamic IP, PPPoE and PPTP type of the WAN Port.
- **MAC Clone:** The MAC address is a 12-digit HEX code uniquely assigned to hardware as identification. Some ISPs require you to register a MAC address in order to access to Internet. If not, you could use default MAC or clone MAC from a PC.
- **NAT:** Administrator can set Enable or Disable the NAT function. If Disable NAT function administrator must manual to set routing.
- **DMZ:** DMZ is a physical or logical sub-network that separates an internal local area network (LAN) from other untrusted networks, usually the Internet. External-facing servers, resources and services are located in the DMZ so they are accessible from the Internet but the rest of the internal LAN remains unreachable. This provides an additional layer of security to the LAN as it restricts the ability of hackers to directly access internal servers and data via the Internet.

3.2 WAN Traffic Setup

WAN Traffic setup function improves the distribution of workloads across multiple computing resources. WAN Traffic function aims to optimize network resource use maximize throughput or minimize response time and avoid overload of any single WAN port resource.
If administrator set multi-WAN configuration, administrator can assign weights or speed weights to WAN in the **"WAN traffic setup"** function to indicate the percentage of traffic that should be sent to each WAN.

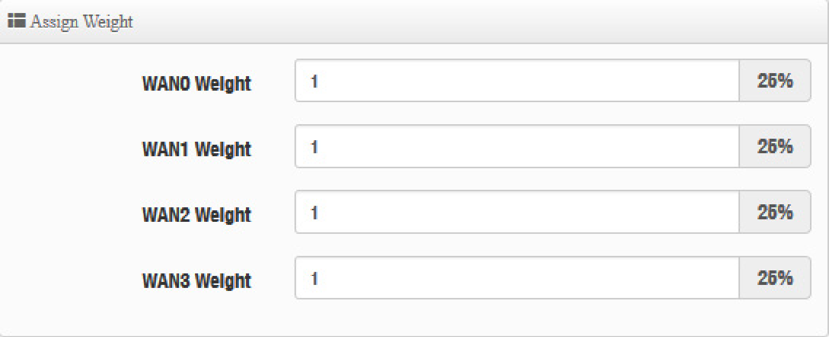



Load Balance Mode

Mode: Assign Weight

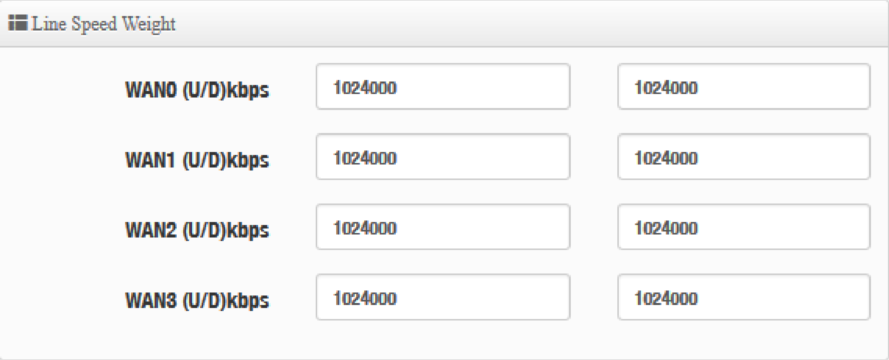
Connection Mode: Source IP Based

- **Mode:** If set multi-WAN, administrator can select Load Balance by Assign Weight or Line Speed Weight.
  - **Assign Weight:** The WAN Assign Weight function can setup handle more requests and handle fewer requests. Assigning weights to WAN allows the DR-3000 appliance to determine how much traffic each load balanced server can handle, and therefore more effectively balance load. The Weight set Max=10 unit.


Assign Weight

WAN0 Weight	1	25%
WAN1 Weight	1	25%
WAN2 Weight	1	25%
WAN3 Weight	1	25%

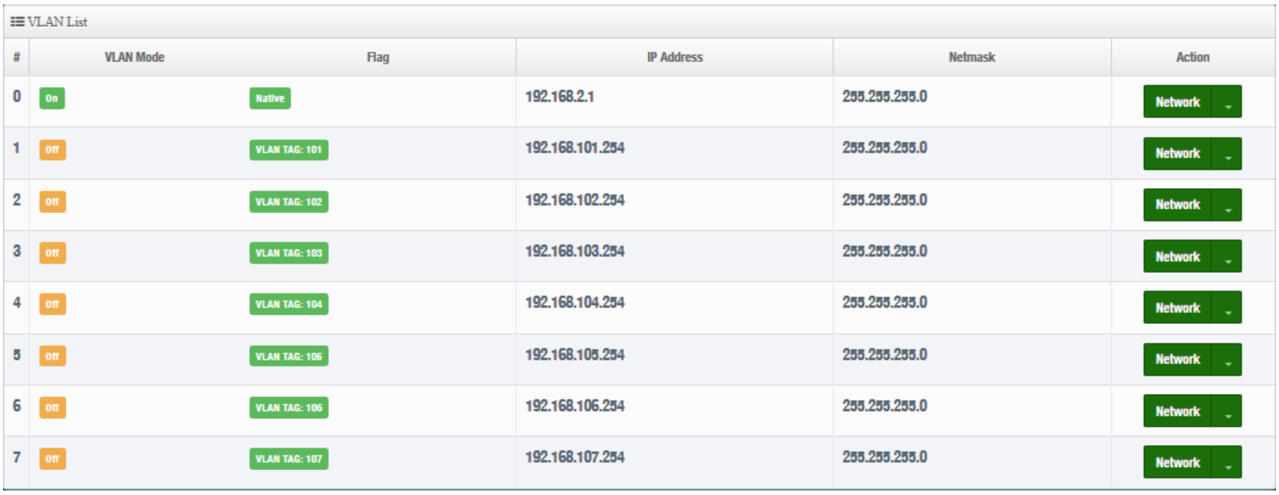
  - **Line Speed Weight:** The function requires administrator to definitely specify the real upload and download line speed of each WAN interface, the system will calculates the maximum bandwidth for all WAN interfaces and then the flow distribution.


Line Speed Weight

WAN0 (U/D)kbps	1024000	1024000
WAN1 (U/D)kbps	1024000	1024000
WAN2 (U/D)kbps	1024000	1024000
WAN3 (U/D)kbps	1024000	1024000

3.3 VLAN Setup

Here are the instructions to setup the local IP Address / Netmask / Gateway / DNS and change settings Tag VLAN functions.



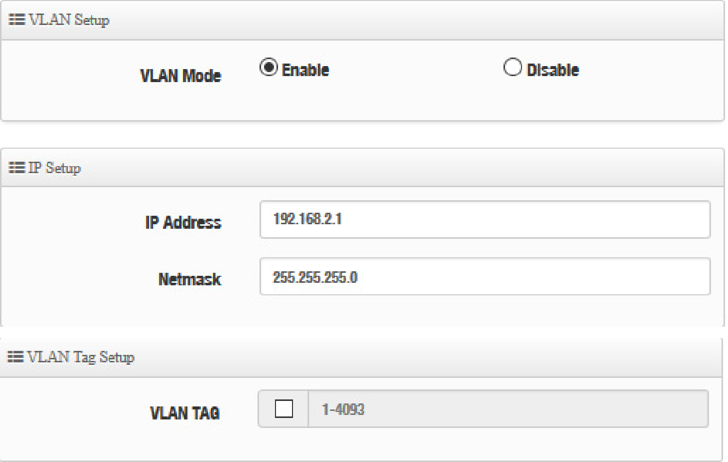
VLAN List

#	VLAN Mode	Flag	IP Address	Netmask	Action
0	On	Native	192.168.2.1	255.255.255.0	Network ⌄
1	Off	VLAN TAG: 101	192.168.101.254	255.255.255.0	Network ⌄
2	Off	VLAN TAG: 102	192.168.102.254	255.255.255.0	Network ⌄
3	Off	VLAN TAG: 103	192.168.103.254	255.255.255.0	Network ⌄
4	Off	VLAN TAG: 104	192.168.104.254	255.255.255.0	Network ⌄
5	Off	VLAN TAG: 105	192.168.105.254	255.255.255.0	Network ⌄
6	Off	VLAN TAG: 106	192.168.106.254	255.255.255.0	Network ⌄
7	Off	VLAN TAG: 107	192.168.107.254	255.255.255.0	Network ⌄

- **VLAN Mode**：Display on/off for the VLAN network.
- **Flag**：Display master VLAN and VLAN Tag No. information.
- **IP Address**：Display IP Address for VLAN Network.
- **NetMask**：Display IP netmask.
- **Action**：The button can set VLAN network functions and DHCP Server.

3.3.1 Network Button

Administrator can click Network ⌄ button to set VLAN network functions.



VLAN Setup

VLAN Mode ● Enable ○ Disable

IP Setup

IP Address: 192.168.2.1

Netmask: 255.255.255.0

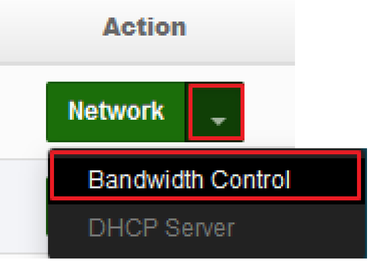
VLAN Tag Setup

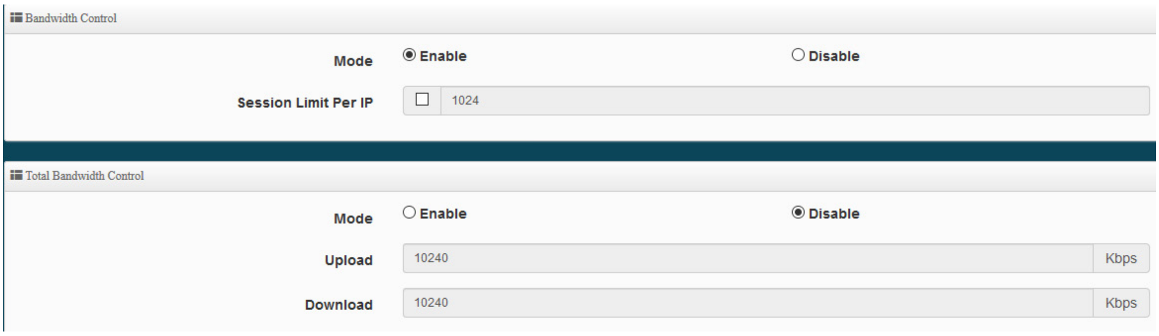
VLAN TAG ☐ 1-4093

- ✓ **VLAN Mode**：Administrator can select Enable or disable for the VLAN Network.
- ✓ **IP Mode**：Administrator can select enable or disable function for VLAN IP.
- ✓ **IP Address/ NetMask**：Administrator can set IP address and netmask for the VLAN.

3.3.2 Pull-down menu @ Bandwidth Control

Administrators can set bandwidth limit the max/min bandwidth of the Wi-Fi users, Bandwidth control can set IP/MASK , IP Range, Port(Service), SIP, RTP/RTSP and WEB.





Bandwidth Control

Mode ● Enable ○ Disable

Session Limit Per IP □ 1024

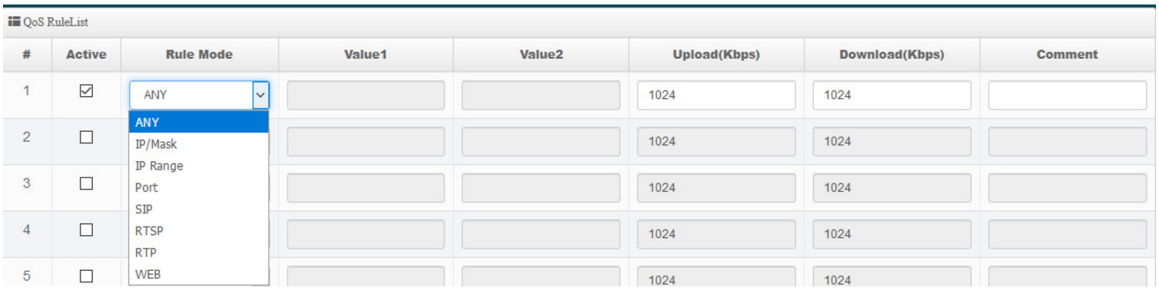
Total Bandwidth Control

Mode ○ Enable ● Disable

Upload 10240 Kbps

Download 10240 Kbps

- ➢ **Session Limit Per IP:** Session limit by all IP address
- ➢ **Total Bandwidth Control:** UP/Download bandwidth limit by VLAN
- ➢ **OoS Rule List:** Administrator can set IP/MASK , IP Range, Port(Service), SIP, RTP/RTSP and WEB to management bandwidth, Max can set 10 rule.



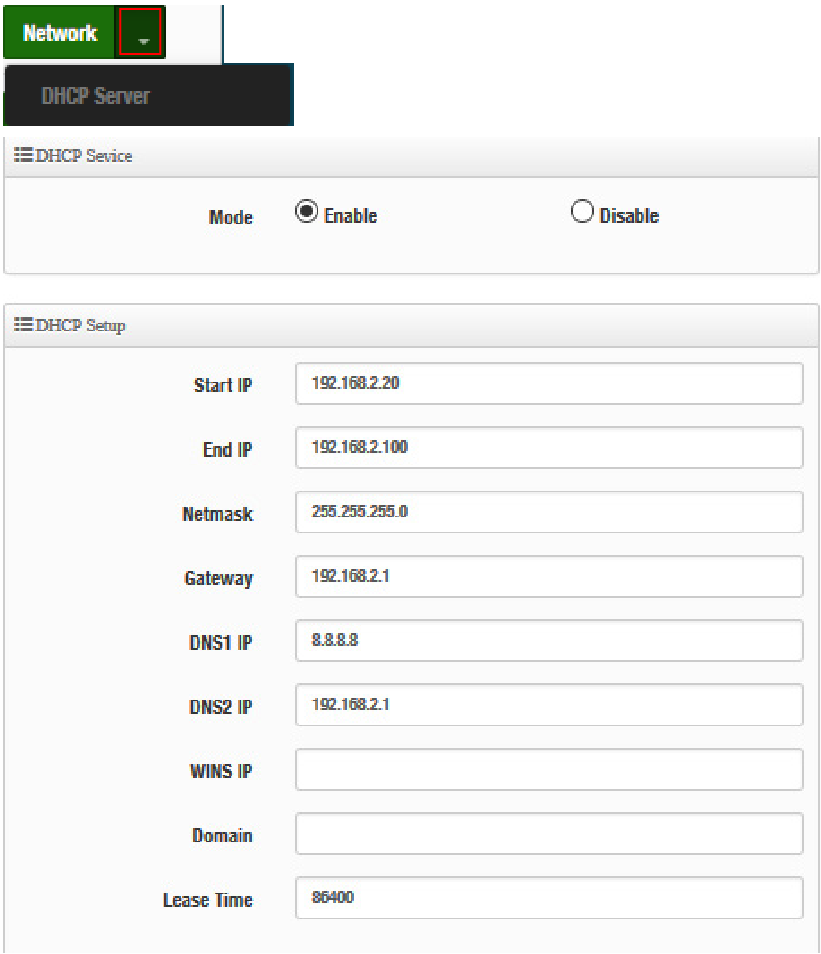
QoS RuleList

#	Active	Rule Mode	Value1	Value2	Upload(Kbps)	Download(Kbps)	Comment
1	☑	ANY			1024	1024	
2	□				1024	1024	
3	□				1024	1024	
4	□				1024	1024	
5	□				1024	1024	

- **Any:** Bandwidth control by any protocol.
- **IP/MASK:** Bandwidth control by a subnet.
- **IP Range:** Bandwidth control by IP range.
- **Port:** Bandwidth control by port (service), ex. FTP port (20,21)
- **SIP:** Bandwidth control by Session Initiation Protocol.
- **RTSP/RTP:** Bandwidth control by Streaming.
- **WEB:** Bandwidth control by web protocol.

3.3.3 Pull-down menu @ DHCP Server

Administrator can set DHCP function. Please click Network ⌄ pull-down button to set DHCP Server.



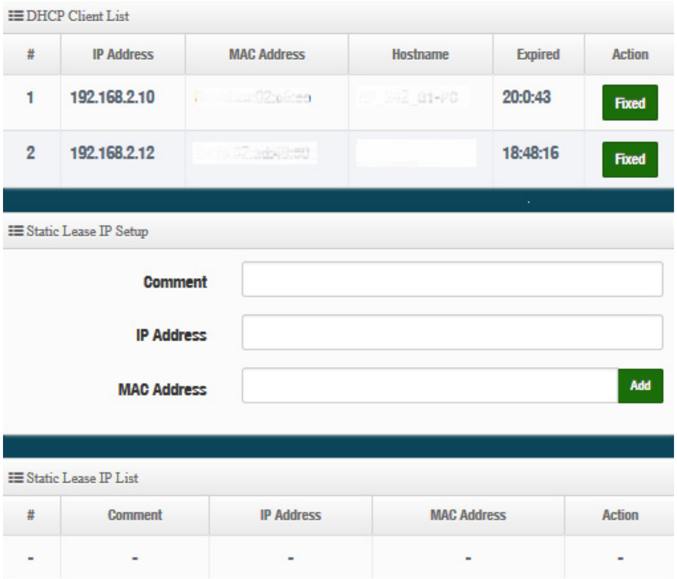
DHCP Sevice

Mode ● Enable ○ Disable

DHCP Setup

Start IP	192.168.2.20
End IP	192.168.2.100
Netmask	255.255.255.0
Gateway	192.168.2.1
DNS1 IP	8.8.8.8
DNS2 IP	192.168.2.1
WINS IP	
Domain	
Lease Time	86400

- ✓ **Mode:** Administrator can select enable / disable the function
- ✓ **Start IP:** Set Start IP for DHCP Service.
- ✓ **End IP:** Set End IP for DHCP Service.
- ✓ **Netmask: Set IP Netmask, the default is 255.255.255.0**
- ✓ **Gateway: Set Gateway IP for DHCP Service.**
- ✓ **DNS (1-2) IP:** Set DNS IP for DHCP Service.
- ✓ **WINS IP:** Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.
- ✓ **Domain:** Enter the domain name for this network.
- ✓ **Lease Time:** The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is **86400** seconds



DHCP Client List

#	IP Address	MAC Address	Hostname	Expired	Action
1	192.168.2.10	[redacted]	[redacted]	20:0:43	Fixed
2	192.168.2.12	[redacted]	[redacted]	18:48:16	Fixed

Static Lease IP Setup

Comment

IP Address

MAC Address Add

Static Lease IP List

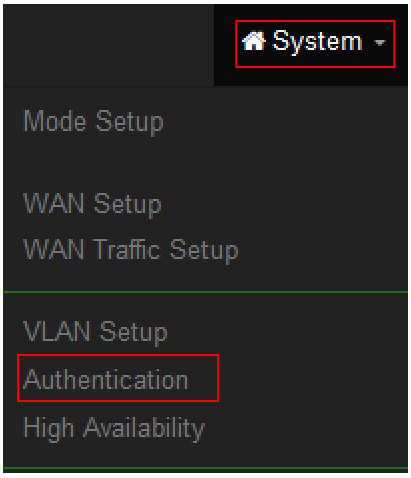
#	Comment	IP Address	MAC Address	Action
-	-	-	-	-

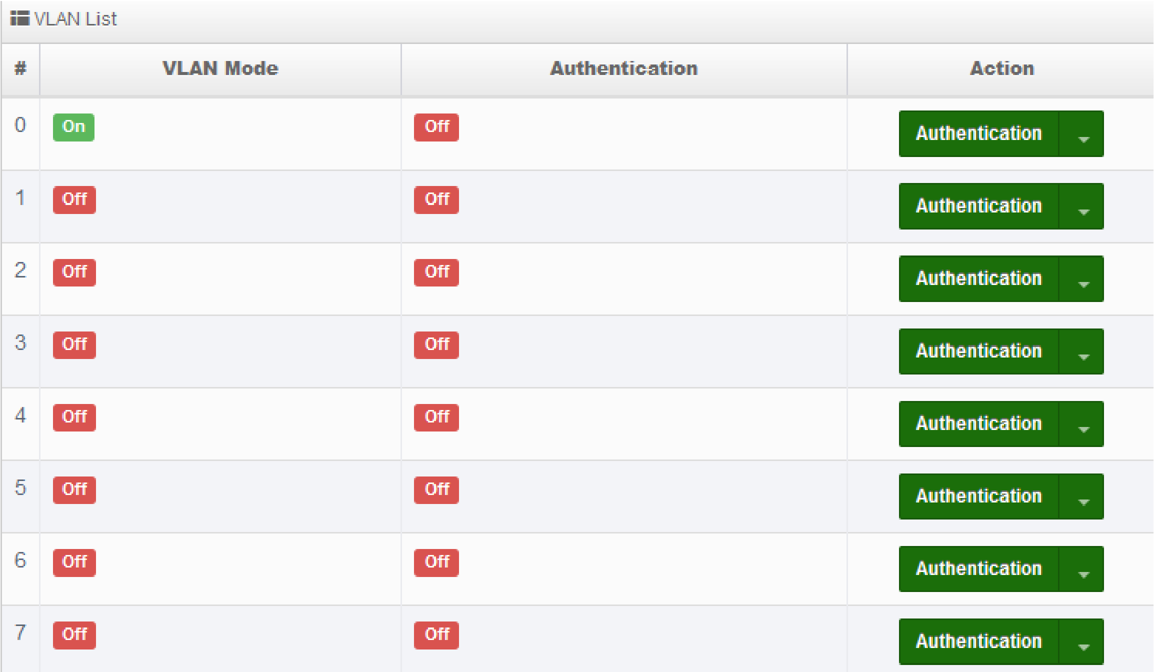
- **DHCP Client List:** Administrator can view IP address used status of client users on each DHCP Server.
- **Static Lease IP Setup:** Administrator can set be delivered fixed IP address to the users.

3.4 Authentication(Hotspot Setup)

The function is for hotspot Authentication. It supports authentication for local users / RADIUS Server / OAuth2.0 and Guest. RADIUS Server authentication support PoP3 / LDAP(AD) and Package.

Please click on **System -> Authentication**





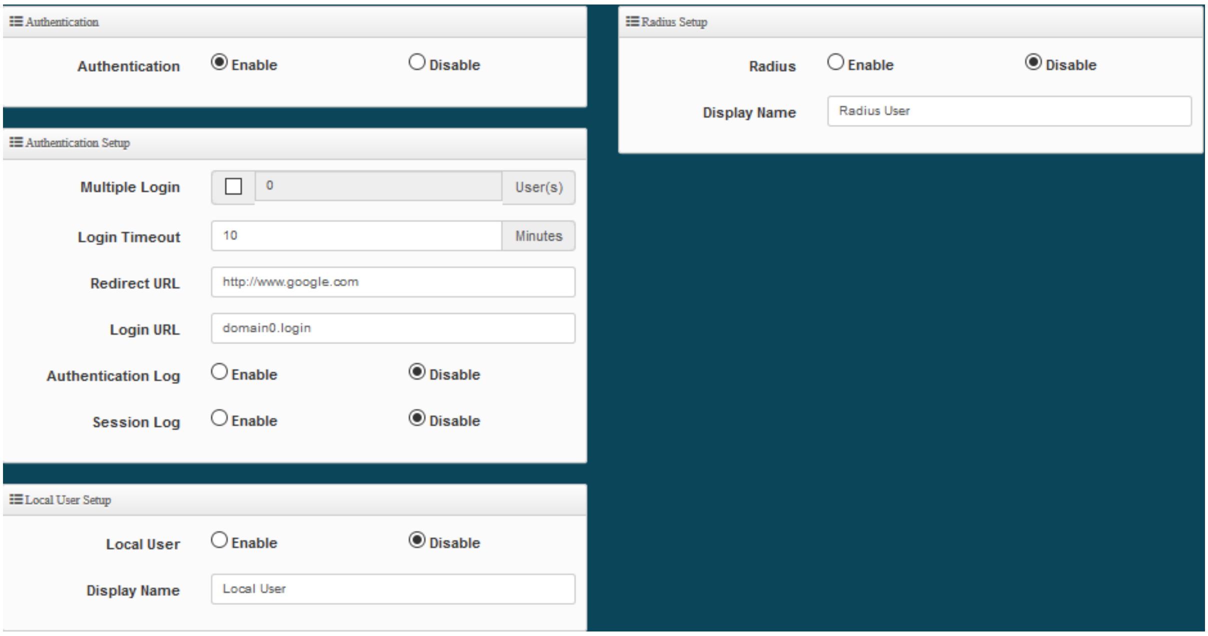
VLAN List

#	VLAN Mode	Authentication	Action
0	On	Off	Authentication ⌄
1	Off	Off	Authentication ⌄
2	Off	Off	Authentication ⌄
3	Off	Off	Authentication ⌄
4	Off	Off	Authentication ⌄
5	Off	Off	Authentication ⌄
6	Off	Off	Authentication ⌄
7	Off	Off	Authentication ⌄

- **#**：Display 8 VLANs list of Authentication.
- **VLAN Mode**：Displays VLAN on/off status.
- **Authentication**：Displays VLAN# whether enable or disable web authentication.
- **Action**：The function has 2 buttons (Authentication and Dropdown)

# Authentication Button:

Authentication ⌄：By clicking the Authentication button, administrator can enable or disable this function.



Authentication

Authentication	● Enable	○ Disable

Authentication Setup

Multiple Login	□ 0 User(s)	
Login Timeout	10 Minutes	
Redirect URL	http://www.google.com	
Login URL	domain0.login	
Authentication Log	○ Enable	● Disable
Session Log	○ Enable	● Disable

Local User Setup

Local User	○ Enable	● Disable
Display Name	Local User	

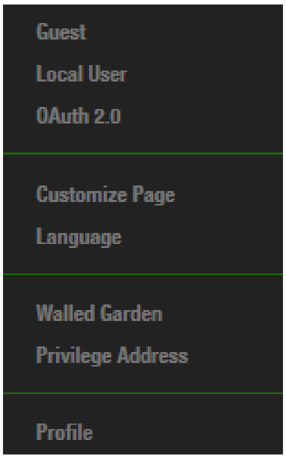
Radius Setup

Radius	○ Enable	● Disable
Display Name	Radius User	

- **Authentication**：Administrator can enable or disable authentication function.
- **Multiple Login**：Administrator can set one account to multiple users simultaneously login and the users can set limit.(0 = not limited)
- **Login Timeout**：After account login for some time no traffic, system will automatic timeout for account. Administrator can enter a time(Minutes).
- **Redirect URL**：After the success of the login, system will redirect to URL. Administrator can enter web site URL.
- **Login URL**：Administrator can set URL for login page.
- **Authentication Log:** Account authentication log will copy to syslog server.
- **Session Log**：If network have Syslog server. Administrator can to system➔management setting IP address for syslog server and enable the function. Account session log will copy to syslog server.
- **Local User**：Administrator can enable authentication for local user. Create user account can to reference **"3.3.2 Local User".**
- **RADIUS**：Authentication support remote RADIUS Server. Administrator can enter security information for remote RADIUS Server.

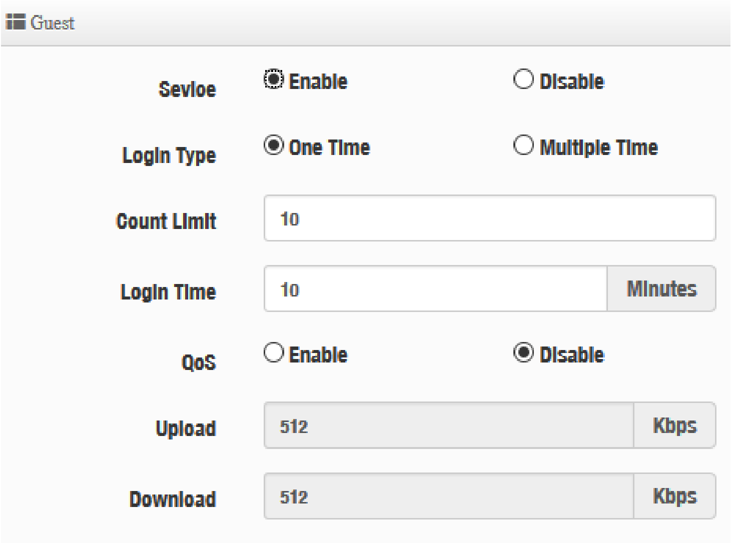
# Authentication Dropdown Button

：By Clicking the Dropdown button, Administrators can set authentication functions.



3.4.1 Guest

Administrator can enable or disable guest authentication. If enabled, the administrator can set guest Count Limit / login time and type and flow control.



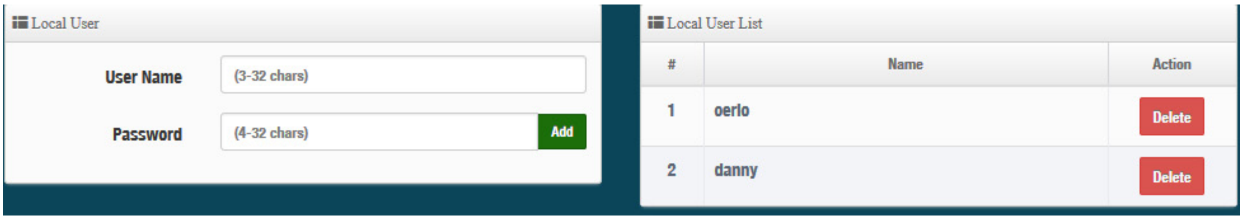
Guest

Sevice	● Enable	○ Disable
Login Type	● One Time	○ Multiple Time
Count Limit	10	
Login Time	10	Minutes
QoS	○ Enable	● Disable
Upload	512	Kbps
Download	512	Kbps

- ➢ **Service**：Administrator can select enable or disable this function.
- ➢ **Login Type :**
  - ● **One Time:** Login to start counting until the end of time.
  - ● **Multiple Times:** logout time will stop counting until the next re-login to time start counting.
- ➢ **Count Limit:** Administrator can set guest limit.
- ➢ **Login Time:** Within a certain timeframe with no traffic, the system will auto logout.
- ➢ **QoS:** Administrator can restrict the traffic of guest. Traffic management can set users upload and download traffic.

3.4.2 Local User

Administrator can create local user account for web login.



Local User

User Name	(3-32 chars)
Password	(4-32 chars) Add

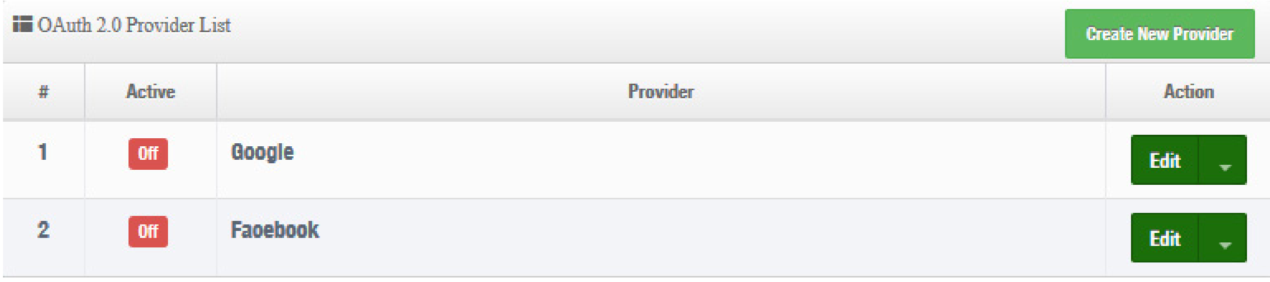
Local User List

#	Name	Action
1	cerio	Delete
2	danny	Delete

- ➢ **User Name**： Administrator can create users account.
- ➢ **Password**：Set account password.

3.4.3 OAuth2.0

The OAuth2.0 function supports Facebook and Google by default. Users can add additional OAuth2.0 servers through UI settings.



OAuth 2.0 Provider List

#	Active	Provider	Action
1	Off	Google	Edit
2	Off	Faoebook	Edit

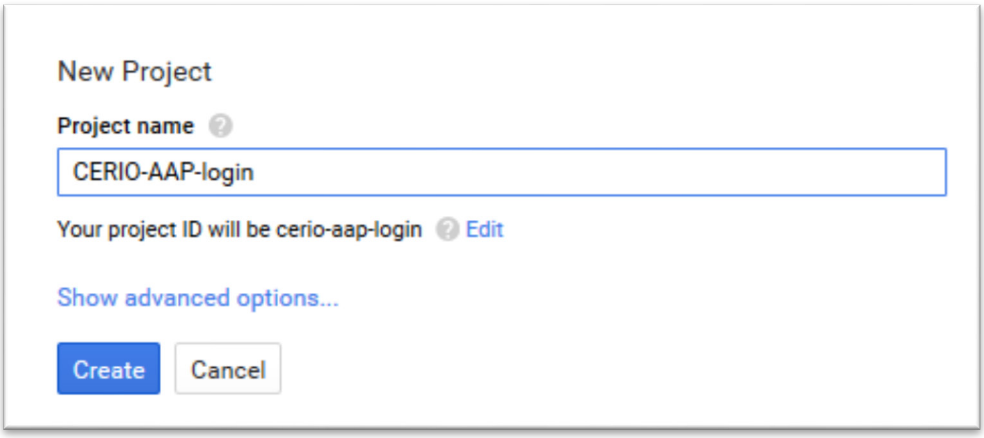
- **#**：Display items.
- **Active**：Display on/off status for the authentication.
- **Provider**：Display authentication server. The system default use authentication server for Google and Facebook

➔ Sample for Google OAuth2.0 setup

lease complete the application on the Google website to receive an account ID and password, follow the steps below.

Step.1 Please go to the **Google Developers Console page** and **create a project**

(Reference https://developers.google.com/identity/protocols/OAuth2)

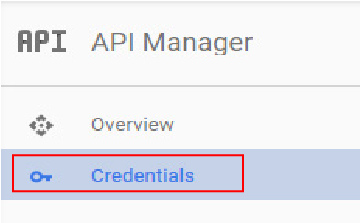


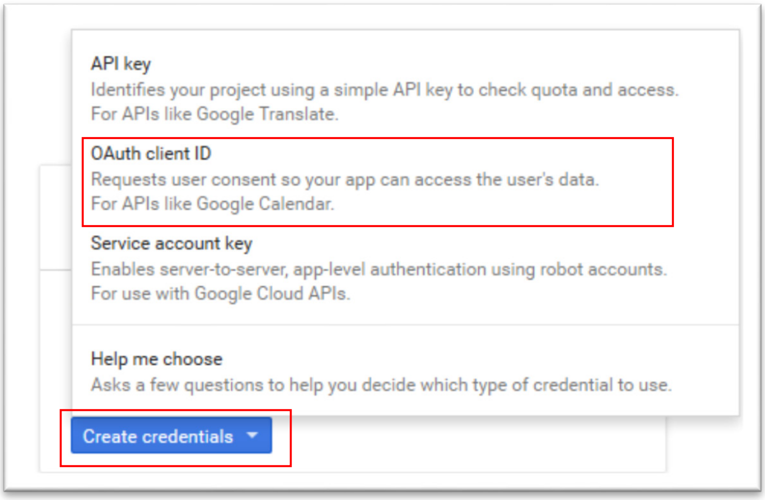
New Project

Project name: CERIO-AAP-login

Your project ID will be cerio-aap-login

Step.2 Click Credentials to create OAuth client ID in the API manager page.





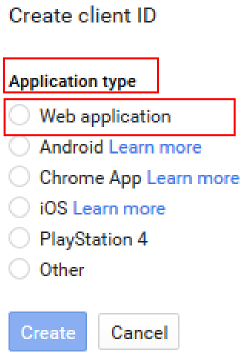
API key
Identifies your project using a simple API key to check quota and access.
For APIs like Google Translate.

OAuth client ID
Requests user consent so your app can access the user's data.
For APIs like Google Calendar.

Service account key
Enables server-to-server, app-level authentication using robot accounts.
For use with Google Cloud APIs.

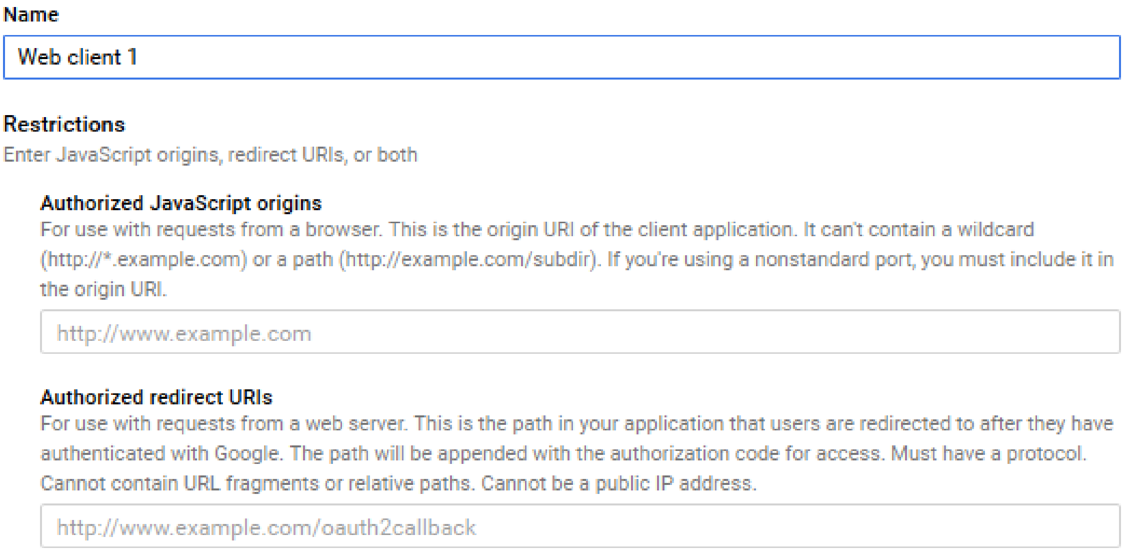
Help me choose
Asks a few questions to help you decide which type of credential to use.

Step.3 Select web application in the "Application Type" section and set **"Restrictions"** URL.



Create client ID

Application type
○ Web application
○ Android Learn more
○ Chrome App Learn more
○ iOS Learn more
○ PlayStation 4
○ Other



Name
Web client 1

Restrictions
Enter JavaScript origins, redirect URIs, or both

Authorized JavaScript origins
For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (http://*.example.com) or a path (http://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.

http://www.example.com

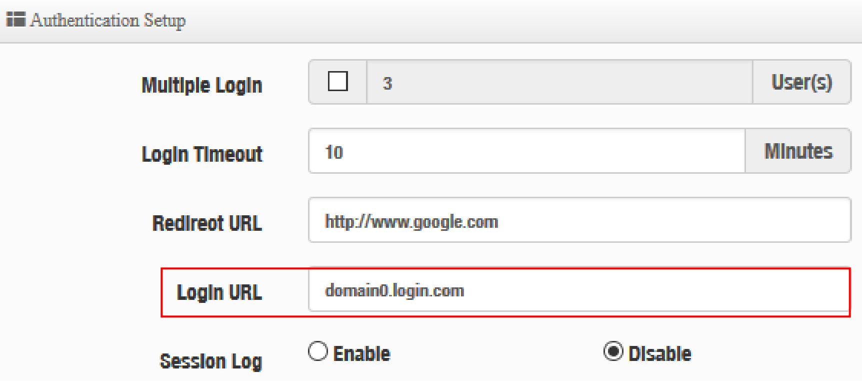
Authorized redirect URIs
For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

http://www.example.com/oauth2callback

Step.4 Set Authorized JavaScript origins and Authorized redirect URLs (important)

Administrator must set login URL in the device function. After complete set of login URL go to the **"Restrictions"** function in web page. Follow the steps below to set login URLs

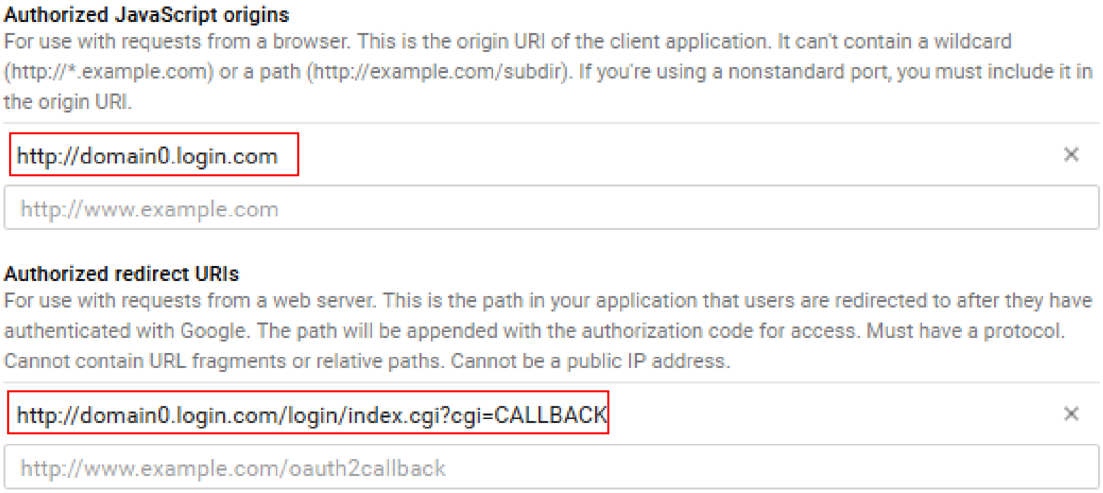
- Setup login URL in the device. Please Click **system→Authentication** and enable the function.
- The "Authentication Setup" page to set Login URL


Authentication Setup

Multiple Login	□ 3 User(s)
Login Timeout	10 Minutes
Redirect URL	http://www.google.com
Login URL	domain0.login.com
Session Log	○ Enable ● Disable

After complete set of login URL go to the **"Restrictions"** function in web page. Copy and paste the login URL from the system display into the "Restriction" page on the Google Developer website.

- Google Authorized JavaScript origins URL is **http://domain0.login.com** (same as Login URL)
- Google Authorized redirect URLs is **http://domain0.login.com/login/index.cgi?cgi=CALLBACK**


Authorized JavaScript origins

For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (http://*.example.com) or a path (http://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.

http://domain0.login.com

http://www.example.com

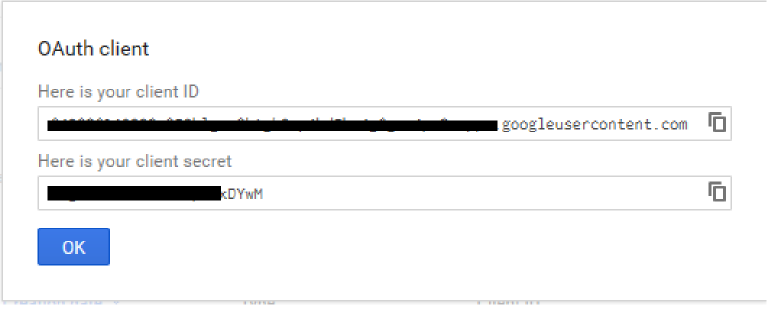
Authorized redirect URIs

For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

http://domain0.login.com/login/index.cgi?cgi=CALLBACK

http://www.example.com/oauth2callback

Step.5 After completing the "Restrictions" setup, click the create button. An OAuth Client page will pop-up with your "client ID" and "client secret". Administrators must copy and paste their client ID and secret into the OAuth 2.0 Setup page in our software UI.



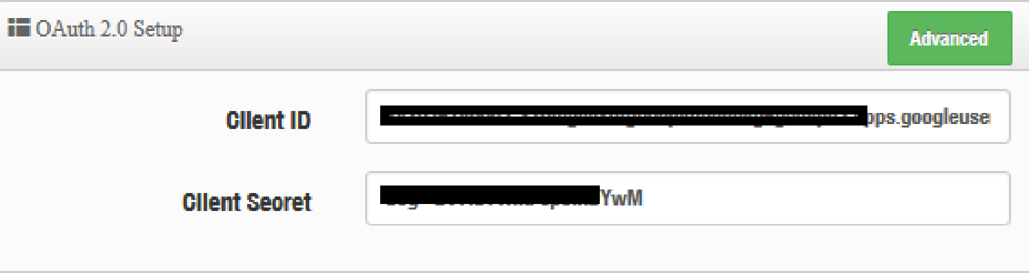
OAuth client

Here is your client ID

[redacted]googleusercontent.com

Here is your client secret

[redacted]kDYwM



OAuth 2.0 Setup

Client ID: [redacted]pps.googleuse

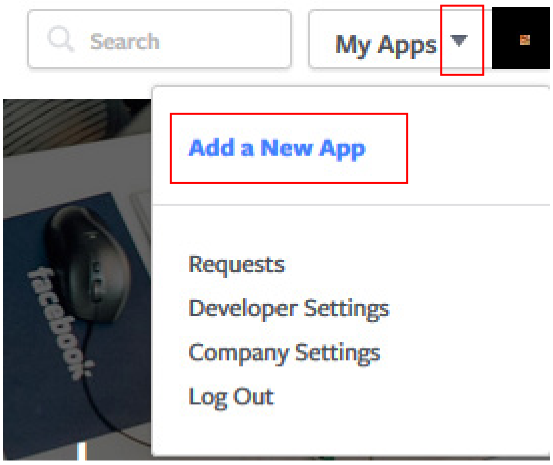
Client Secret: [redacted]YwM

Save and reboot the AP system, complete the setup.

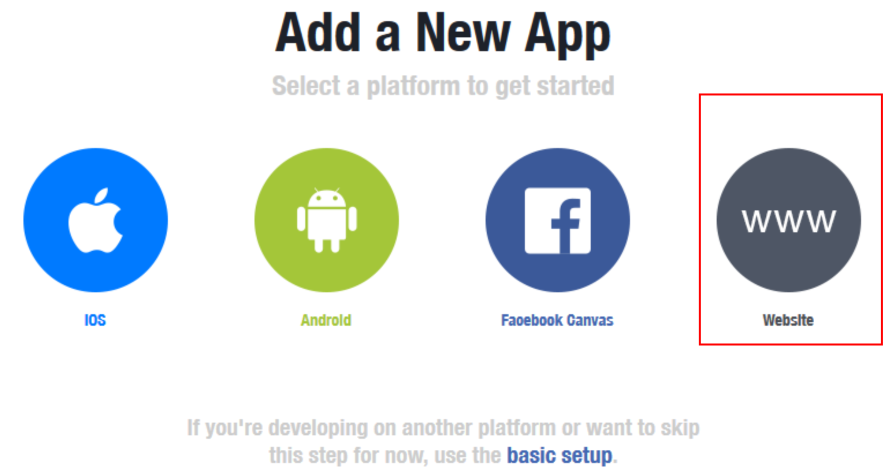
➔ Sample for Facebook OAuth2.0 setup

Please complete the application on the Facebook website to receive an account ID and password, follow the steps below.

Step.1 Please to Facebook developer's page and add a New App



Step.2 Select WWW function

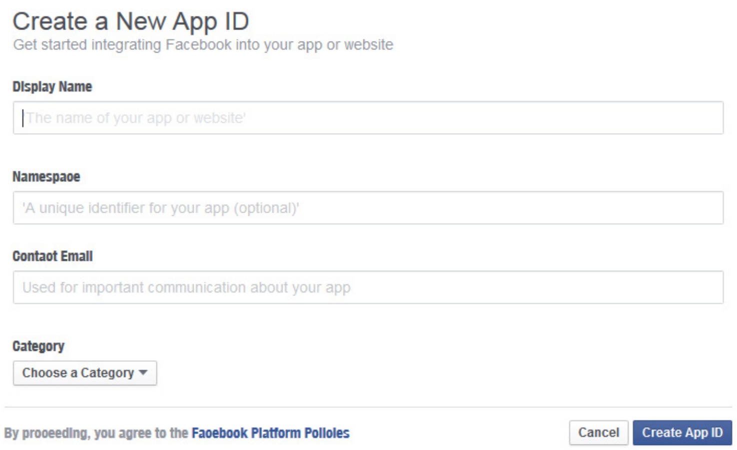


Add a New App

Select a platform to get started

If you're developing on another platform or want to skip this step for now, use the **basic setup**.

Step.3 Administrator must set www for your information.



Create a New App ID

Get started integrating Facebook into your app or website

Display Name

'The name of your app or website'

Namespaoe

'A unique identifier for your app (optional)'

Contaot Emall

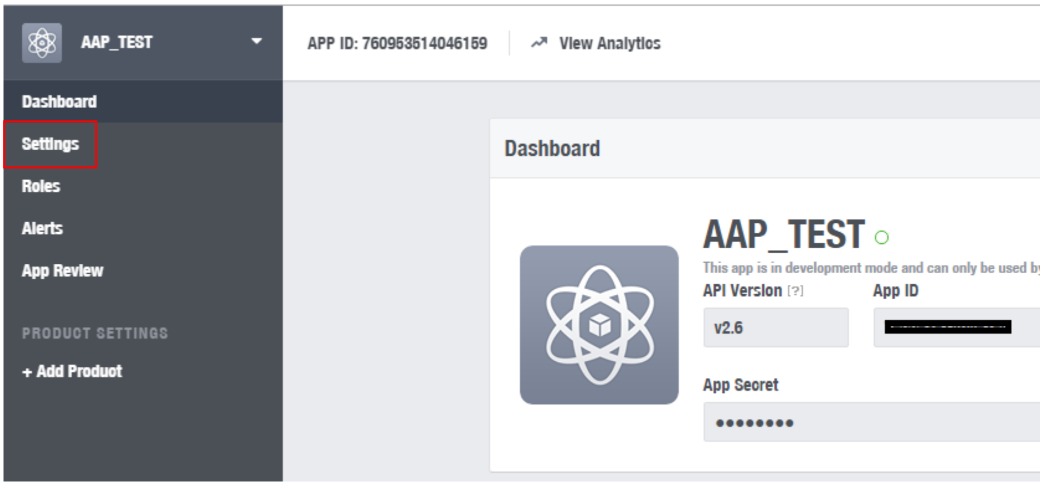
Used for important communication about your app

Category

Choose a Category ▾

By prooeedIng, you agree to the Faoebook Platform Polloles

Step.4 Please click **"Setting"** and add Platform



APP ID: 760953514046159

Dashboard

AAP_TEST

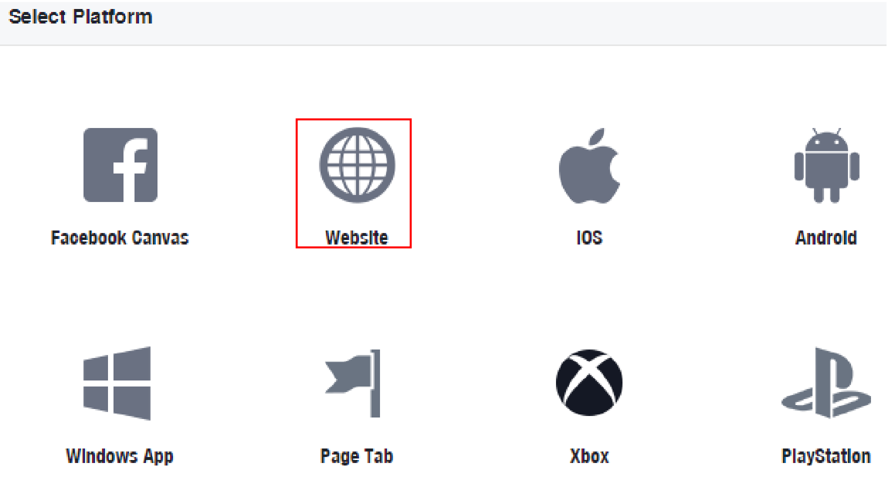
This app is in development mode and can only be used b

API VersIon [?] v2.6

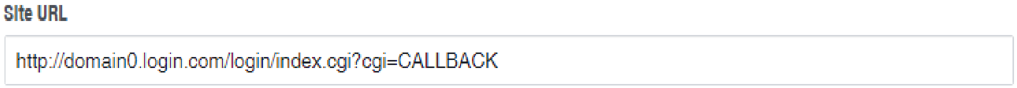
App ID [redacted]

App Seoret ••••••••

Step.5 Select Platform for "**Website**"



Step.6 Enter URL is **http://domain0.login.com/login/index.cgi?cgi=CALLBACK**

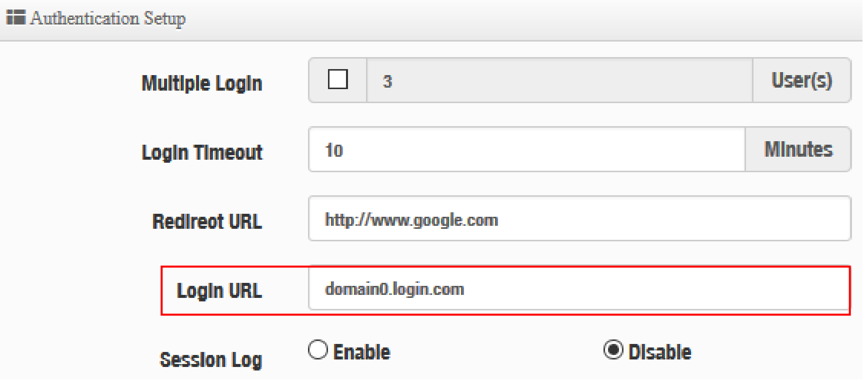


Site URL

http://domain0.login.com/login/index.cgi?cgi=CALLBACK

Administrator must set login URL in the device function. After complete set of login URL go to the "**Facebook** Site URL" function in web page. Follow the steps below to set login URLs

- Setup login URL in the device. Please Click **system→Authentication** and enable the function.
- The **"Authentication Setup"** page to set Login URL

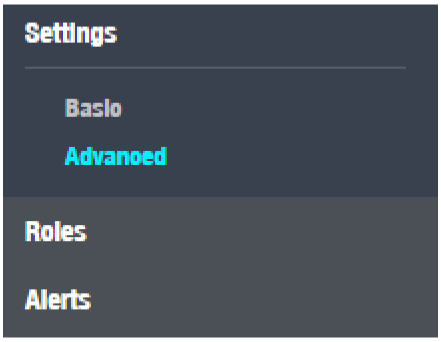


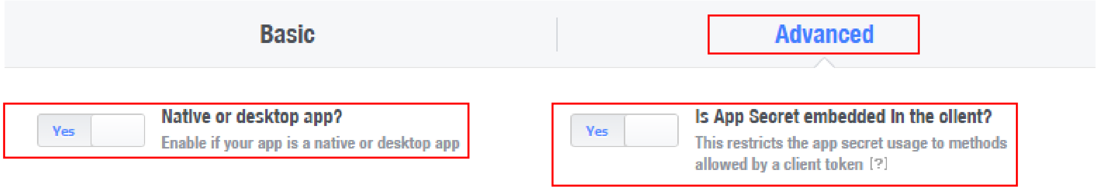
Authentication Setup

Multiple Login	□ 3 User(s)
Login Timeout	10 Minutes
Redirect URL	http://www.google.com
Login URL	domain0.login.com
Session Log	○ Enable ● Disable

After complete set of login URL go to the "**Facebook** Site URL" function in web page. Copy and paste the login URL from the system display into the "Site URL" page on the Facebook website.

Step.7 Click Advanced function to enable the **"Native or desktop app?"** and **"Is App Secret embedded in the client? "**

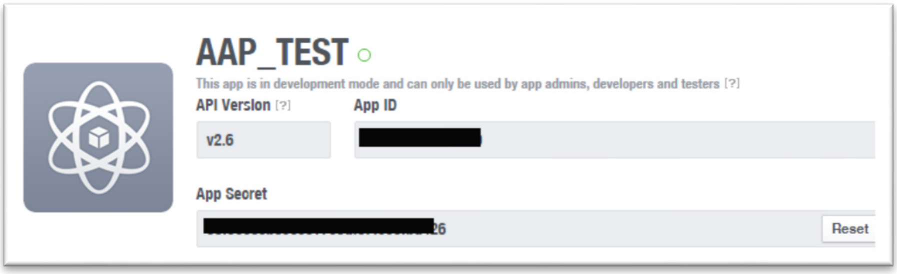




Yes — Native or desktop app?
Enable if your app is a native or desktop app

Yes — Is App Secret embedded in the client?
This restricts the app secret usage to methods allowed by a client token [?]

Step.8 After completing the "**Facebook** Site URL" setup. Administrators must copy and paste their App ID and App secret into the OAuth 2.0 Setup page in our software UI.



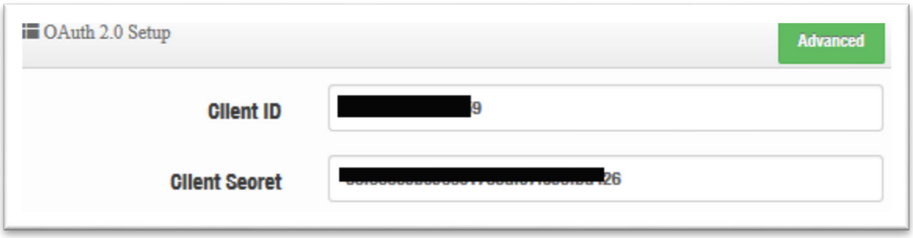
AAP_TEST ○

This app is in development mode and can only be used by app admins, developers and testers [?]

API Version [?]: v2.6

App ID: [redacted]

App Secret: [redacted]26 Reset



OAuth 2.0 Setup

Client ID: [redacted]9

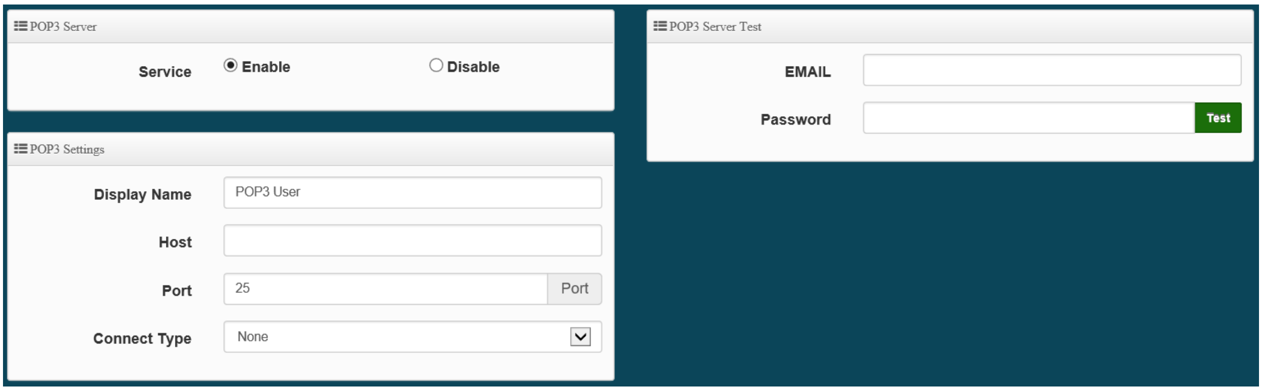
Client Secret: [redacted]26

Notice

Client ID and Client Secret setup by third parties such as Facebook and Google are subject to change. The instructions above follow the 2016 setup procedure. Any future changes to the Facebook/Google process may lead to our instructions becoming invalid.

3.4.4 POP3 Server

The purpose of this integrated function is to allow clients to link a POP3 server for receiving emails from a remote server.



POP3 Server

Service ● Enable ○ Disable

POP3 Settings

Display Name: POP3 User
Host:
Port: 25 Port
Connect Type: None

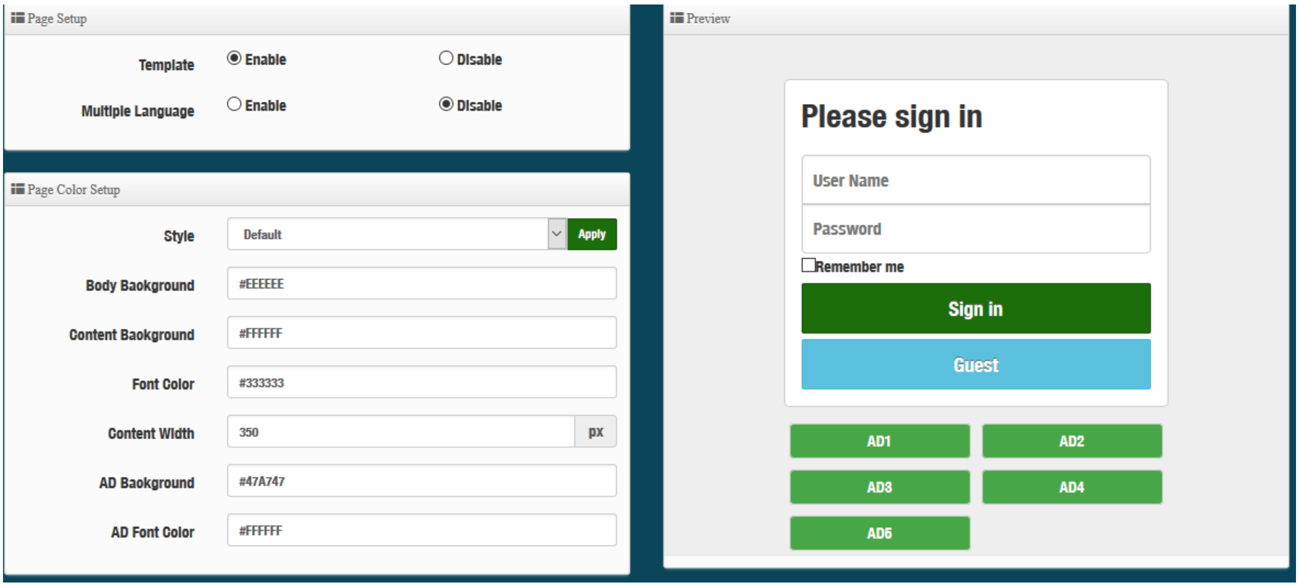
POP3 Server Test

EMAIL:
Password:

- **POP3 Server**：Click "Enable" or "Disable" to activate this function
- **Display Name**：Set the "Display Name" based on the appropriate POP3 user or client
- **Host :** Define the desired Host server name
- **Port :** Input the proper port number for the corresponding server
- **Connect Type :** Select the Connect type with options of "STARTTLS", "SSL/TTL", or "None"
- **POP3 Server Test :** Use this tool to test if the POP3 server is operating correctly with your selected email

3.4.5 Customize Page

This function is to customize the user Login Page. This supports Multiple Language and allows comprehensive customization through HTML editing.



Page Setup

Template ● Enable ○ Disable
Multiple Language ○ Enable ● Disable

Page Color Setup

Style: Default
Body Background: #EEEEEE
Content Background: #FFFFFF
Font Color: #333333
Content Width: 350 px
AD Background: #47A747
AD Font Color: #FFFFFF

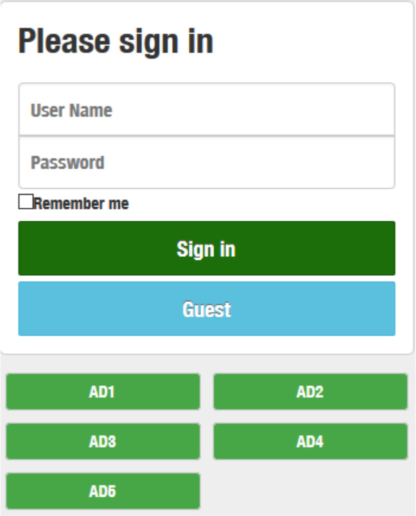
Preview

Please sign in
User Name
Password
□ Remember me

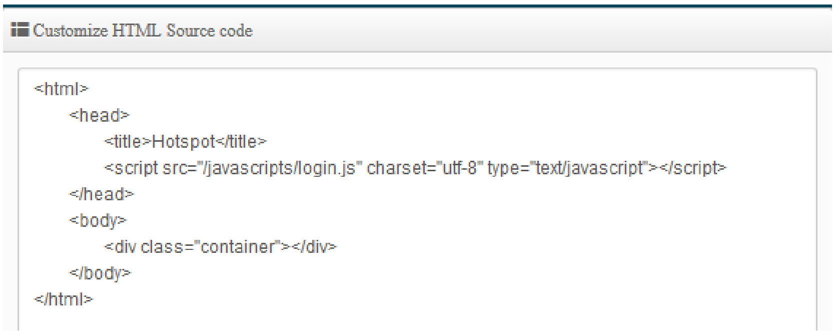
Page Setup

➢ **Template：** Administrator can select Enable or disable.

- Select enable to active default Login Page

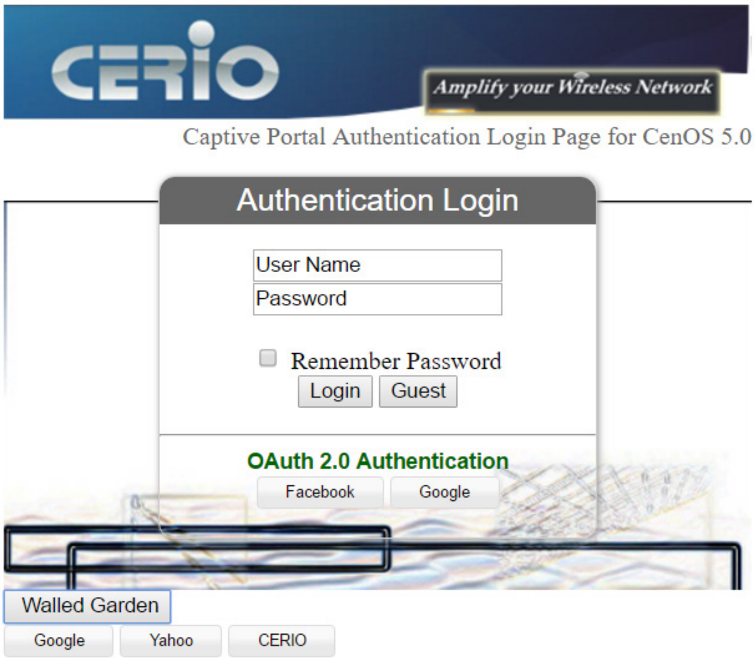


- Select disable to active HTML Source code window for customization


Customize HTML Source code

```
<html>
    <head>
        <title>Hotspot</title>
        <script src="/javascripts/login.js" charset="utf-8" type="text/javascript"></script>
    </head>
    <body>
        <div class="container"></div>
    </body>
</html>
```

Sample: See sample login page below that is customized by html coding *(sample login page html code templates are available on Cerio website)*

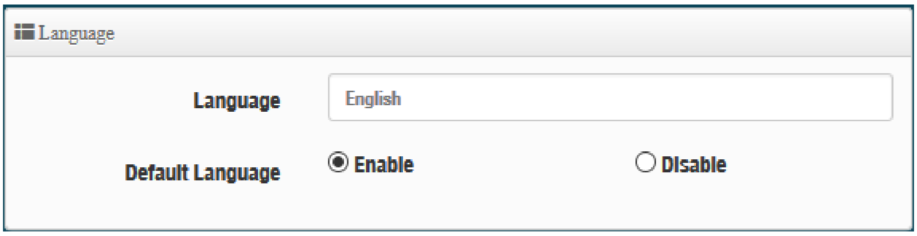


The following function uses the enabled Template

- **Multiple Language**：Administrator can select enable or disable multiple language for login page. Administrator must to Language function create new language.
- **Page Color Setup**：Administrator can change the login page color.

3.4.6 Language

Administrator can create other language for login page.

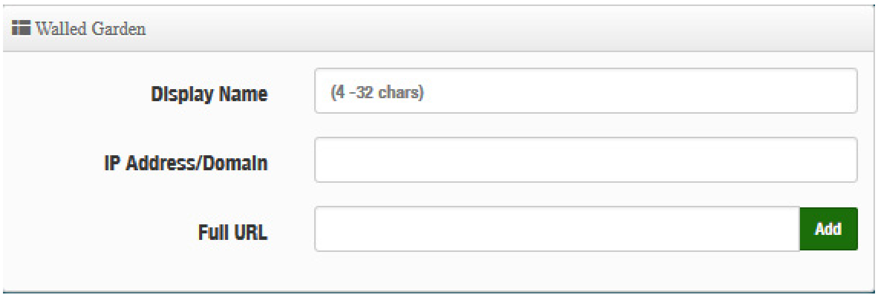


Language

Language	English
Default Language	● Enable ○ Disable

3.4.7 Walled Garden

This function provides certain free services or advertisement web pages for users to access the websites listed before login and authentication. User without the network access right can still have a chance to experience the actual network service free of charge in Walled Garden URL list.



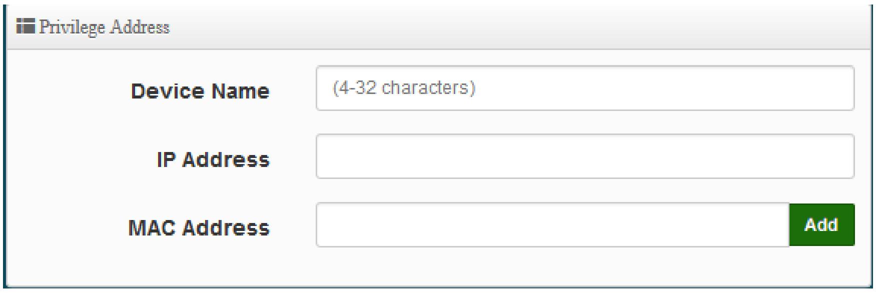
Walled Garden

Display Name	(4 -32 chars)
IP Address/Domain	
Full URL	Add

- **Display Name:** Set name of Website.
- **IP Address/Domain:** Set IP or Domain of the Open the website.
- **Full URL:** Set full website name.

3.4.8 Privilege Address

This function provides local device can access Internet without authentication. If there are some workstations belonging NGS Access Point that need to access to network without authentication, enter the IP or MAC address of these workstations in this list.

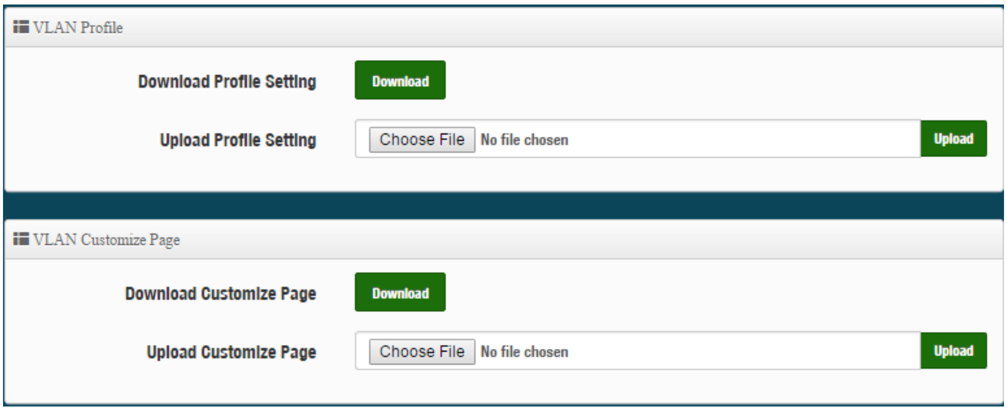

Privilege Address

Device Name	(4-32 characters)
IP Address	
MAC Address	

- **Device Name:** Enter Device or Users Name.
- **IP Address:** Enter used IP Address of Device or Users PC.
- **MAC Address:** Enter MAC Address of Device or Users PC.

3.4.9 Profile

Administrator can backup current authentication configuration and login page for HTML Source code. But also can recover.


VLAN Profile

Download Profile Setting	Download
Upload Profile Setting	Choose File No file chosen

VLAN Customize Page

Download Customize Page	Download
Upload Customize Page	Choose File No file chosen

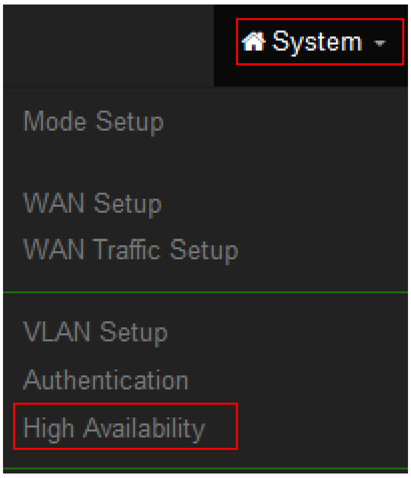
Click “**Save”** button to save your changes. Then click **Reboot** button to activate your changes.

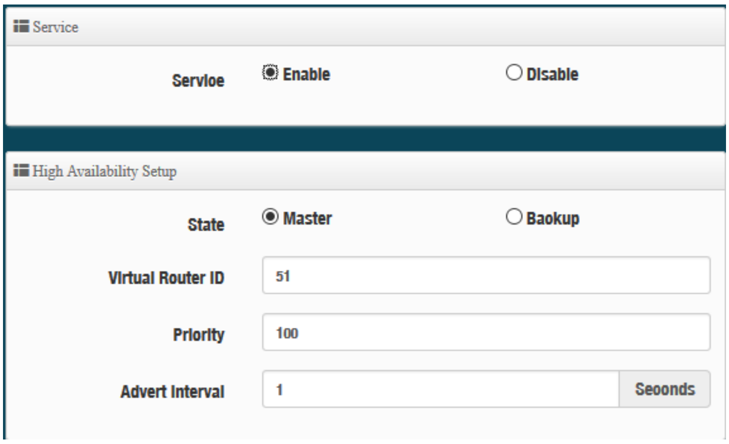
3.5 High Availability

When Gateway systems downtime working, the all network will can't normal work. If administrator set the high availability feature will be able to reduce the accidental interruption of the network and prevent against data loss.

CERIO DR-3000 support system backup of the high availability function can mirror backup to many DR-3000.

Please click **"System"➔ "High Availability"** to set the function.





Service

Service ● Enable ○ Disable

High Availability Setup

State ● Master ○ Backup

Virtual Router ID 51

Priority 100

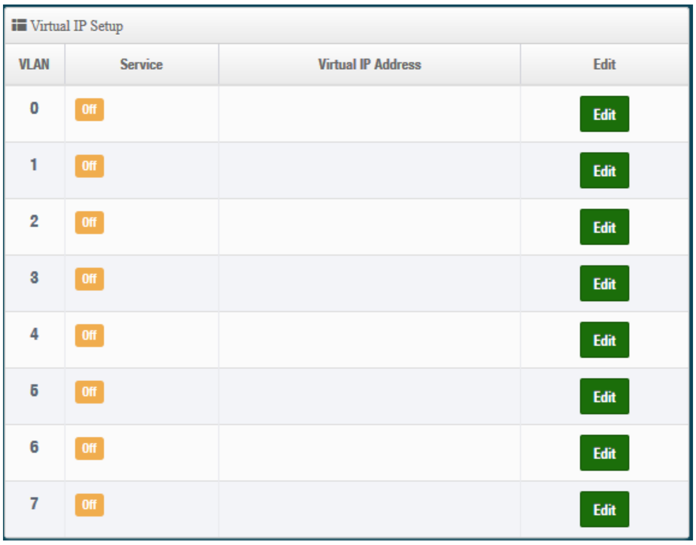
Advert Interval 1 Seconds

- **Service:** Administrator can select Enable or Disable the HA function.

High Availability Setup

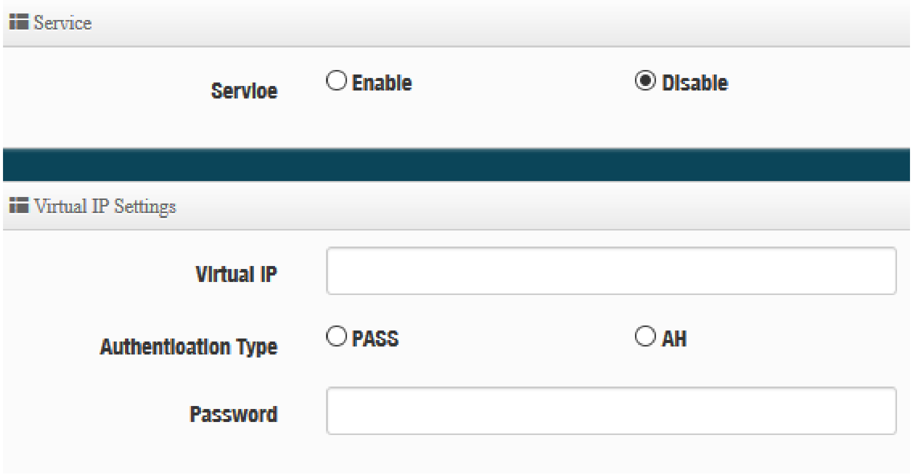
- **State:** Administrator can set HA type of the Master or Backup.
- **Virtual Router ID:** Administrator must set same virtual router ID in all the high availability devices
- **Priority:** Administrator can set the priority level.
- **Advert Interval:** After how many sec to the recovery.

Virtual IP Setup: Administrator can set HA function in different VLAN.



Virtual IP Setup

VLAN	Service	Virtual IP Address	Edit
0	Off		Edit
1	Off		Edit
2	Off		Edit
3	Off		Edit
4	Off		Edit
5	Off		Edit
6	Off		Edit
7	Off		Edit



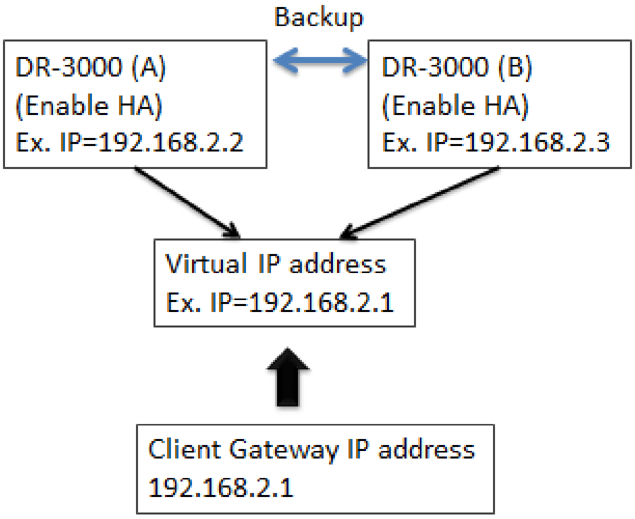
Service

Service	○ Enable	● Disable

Virtual IP Settings

Virtual IP		
Authentication Type	○ PASS	○ AH
Password		

- **Virtual IP:** Administrator must set a Virtual IP address for HA device. (The following concepts)

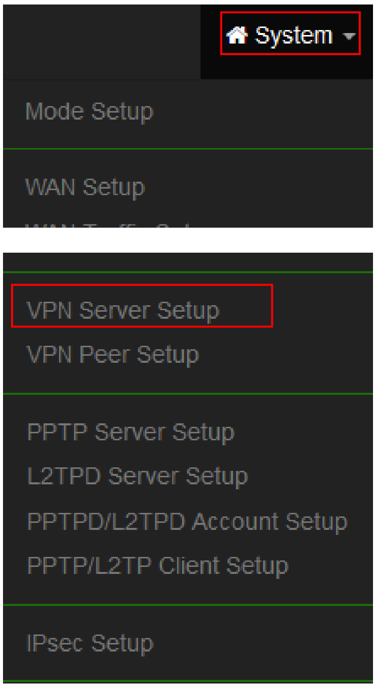


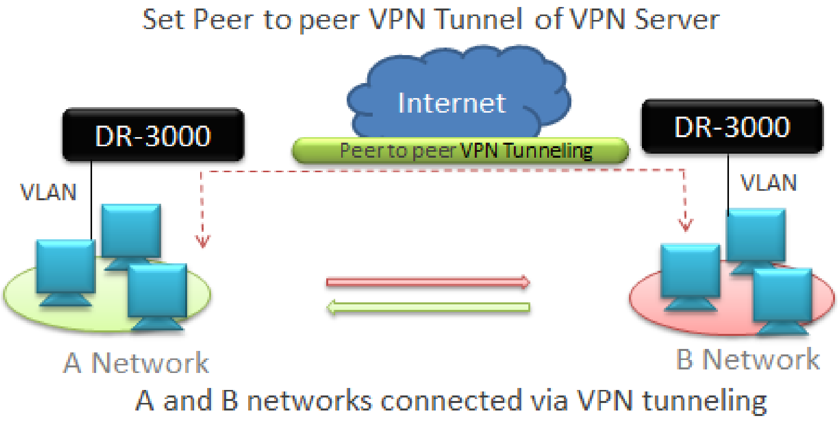
- **Authentication Type:** Administrator can select PASS or AH type for HA security.
- **Password:** Administrator can set password for the HA security.

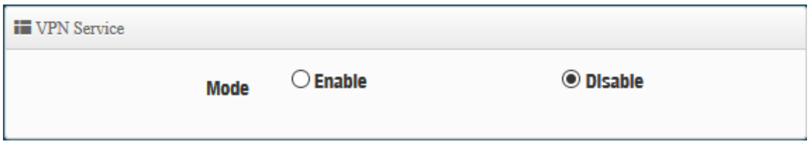
3.6 VPN Server Setup

Notice **This VPN function support three protocol are VPN Server、PPTP/L2TP and IPsec, the VPN tunnel of these three types only select one VPN protocol to used it.**

Please click **"System"➔"VPN Server Setup"** create VPN function.




Set Peer to peer VPN Tunnel of VPN Server
Internet
Peer to peer VPN Tunneling
DR-3000
DR-3000
VLAN
VLAN
A Network
B Network
A and B networks connected via VPN tunneling

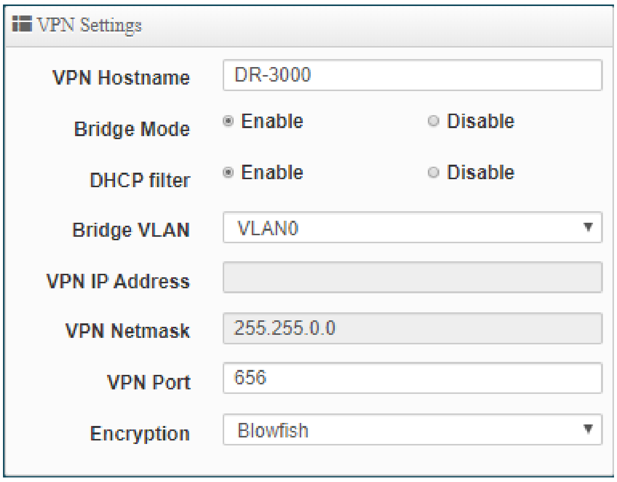


VPN Service

Mode ○ Enable ● Disable

VPN Service

- **Mode**: Administrator can select Enable or Disable the VPA function.



VPN Settings

VPN Hostname	DR-3000
Bridge Mode	● Enable ○ Disable
DHCP filter	● Enable ○ Disable
Bridge VLAN	VLAN0 ▾
VPN IP Address	
VPN Netmask	255.255.0.0
VPN Port	656
Encryption	Blowfish ▾

VPN Settings

- **VPN Hostname:** Administrator can set a VPN host name. Each VPN host name can't be the same and can't have special symbols.
- **Bridge Mode:** Administrator can select bridge mode by VLAN or Manual.
- **DHCP filter**: You can choose to enable or disable it. When it is enabled, it can prevent the DHCP server IPs of the physical area network at both ends from sending IPs out of bounds.

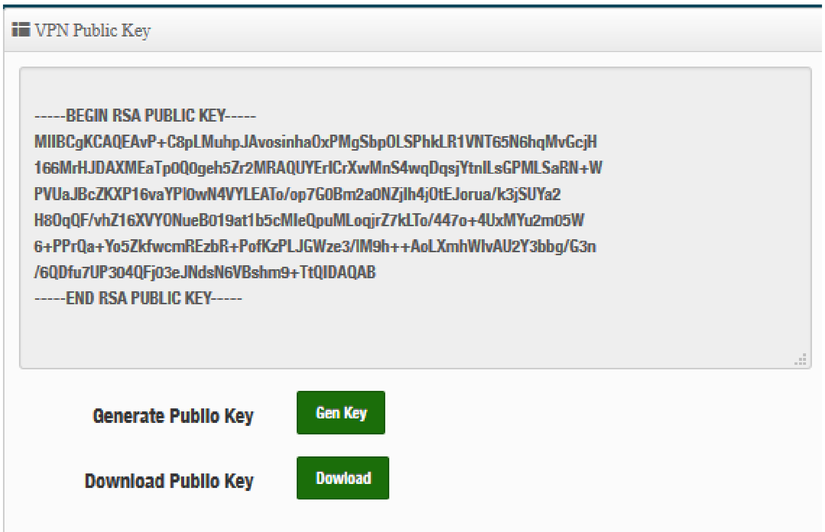
(You only need to enable this function unilaterally. If the DHCP filter is turned on at both ends, the network logic will be incorrect and the VPN cannot be successfully connected)

- **Bridge VLAN:** If bridge mode select VLAN, administrator can select set VLAN 0~7 for VPN bridge.
- **VPN IP Address/Netmask:** If bridge mode select manual, administrator must set an IP address/netmask for the VPN link and must set routing of LAN.

Notice	1. **If administrator choose use bridge mode then VPN both sides beneath need use same c class network.** 2. **If administrator choose use manual set IP address then must set IP routing of LAN**

- **VPN Port:** Administrator can set Port for VPN.
- **Encryption**: Select VPN security of encryption type.

VPN Public Key



VPN Public Key

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAvP+C8pLMuhpJAvosinha0xPMgSbpOLSPhkLR1VNT65N6hqMvGcjH
166MrHJDAXMEaTp0Q0geh5Zr2MRAQUYErICrXwMnS4wqDqsjYtnILsGPMLSaRN+W
PVUaJBcZKXP16vaYPl0wN4VYLEATo/op7G0Bm2a0NZjlh4j0tEJorua/k3jSUYa2
H8OqQF/vhZ16XVY0NueB019at1b5cMleQpuMLoqjrZ7kLTo/447o+4UxMYu2m05W
6+PPrQa+Yo5ZkfwcmREzbR+PofKzPLJGWze3/IM9h++AoLXmhWlvAU2Y3bbg/G3n
/6QDfu7UP304QFj03eJNdsN6VBshm9+TtQIDAQAB
-----END RSA PUBLIC KEY-----
```

Generate Publlo Key: Gen Key

Download Publlo Key: Dowload

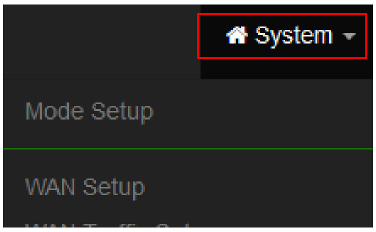
- **Generate Public Key:** Administrator can click the button to regenerate the VPN public key.
- **Download Public Key:** Administrator can click the button to download the VPN public key.

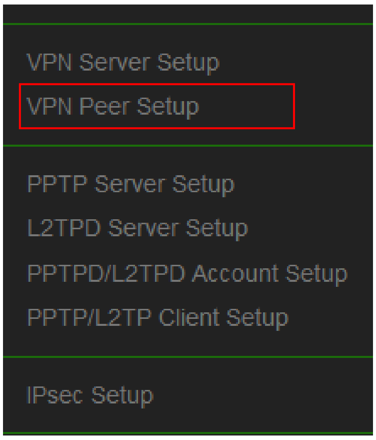
3.7 VPN Peer Setup

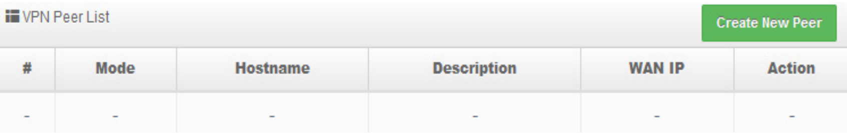
Notice	**When administrator set 3.6 VPN server is complete, this page must setup a real IP address and upload VPN key of the other end.**

Administrator can create new VPN connection for the VPN Peer.

Please click "**System**"➔"**VPN Peer Setup**"





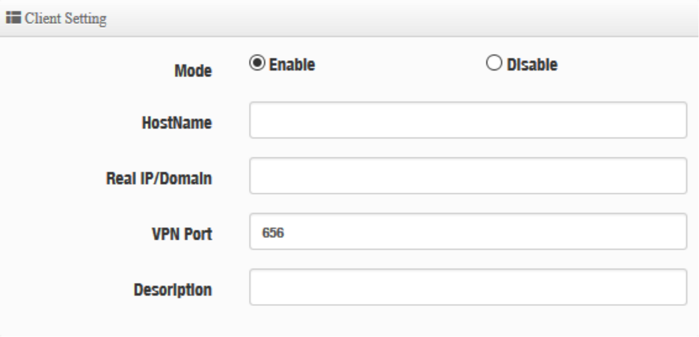


VPN Peer List

Create New Peer

#	Mode	Hostname	Description	WAN IP	Action
-	-	-	-	-	-

Create New Peer: Administrator can click the button to create a VPN bridge(peer to peer).



Client Setting

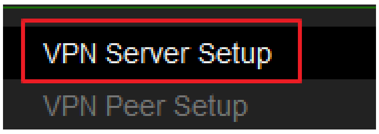
Mode	● Enable ○ Disable
HostName	
Real IP/Domain	
VPN Port	656
Description	

- **Mode:** Administrator can select Enable or Disable the service.
- **HostName:** Administrator can set VPN host name in this field.
- **Real IP/Domain:** Administrator can set remote real IP address or Domain name in this field.
- **VPN Port:** Administrator can set connection Port for VPN.
- **Description:** Enter the description for the VPN Peer.

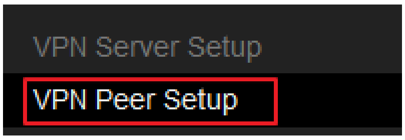
Basic instructions for setting the program

In the two end points A and B for example

1. Set the VPN server on the A side, and download and store the VPN Public Key, the A Public Key upload it to the B endpoint for authentication. The same is true for the B endpoint setting. (Two-end exchange public key)



2. Establish remote VPN Server information and upload the remote Public Key to this location.

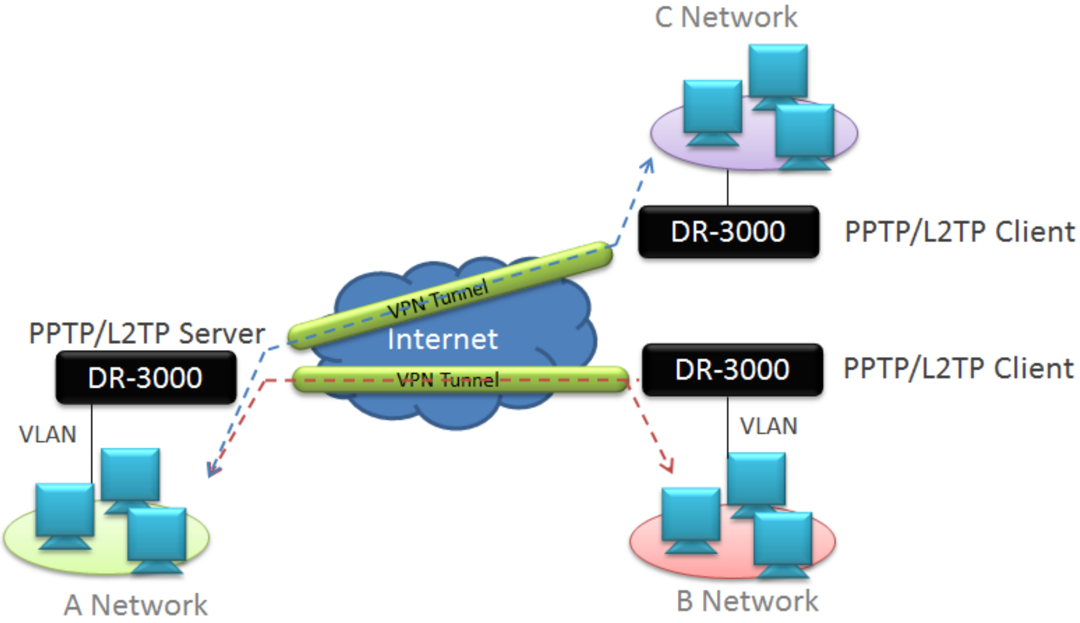


3. After completion, administrator can use ping command go to ping remote network IP address. If A ping to B side can get respond indicates that the VPN tunnel has been successfully established.

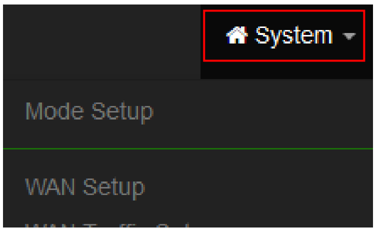
3.8 PPTP/L2TP Server Setup

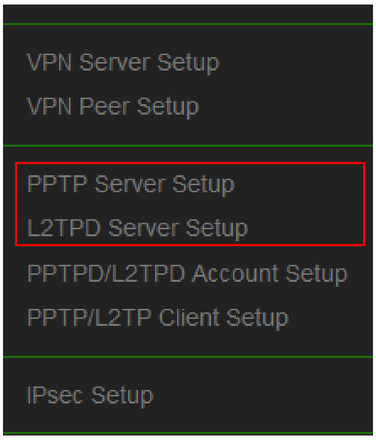
Notice	**This VPN function support three protocol are VPN Server 、PPTP/L2TP and IPsec, the VPN tunnel of these three types only select one VPN protocol to used it.**

Use the PPTP / L2TP protocol to build a VPN tunnel; administrator can setup PPTP / L2TP server of the VPN tunnel in the function.

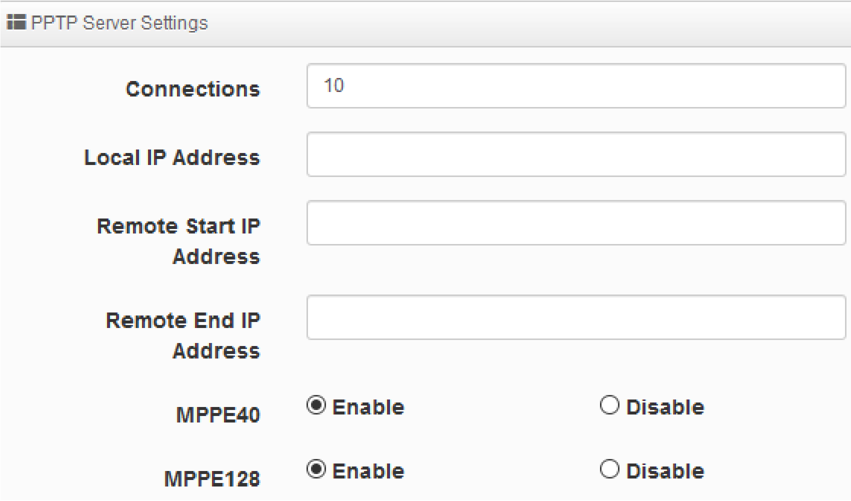


Please click “**System**”➔”**PPTP/L2TP Server Setup**”





PPTP Server:



PPTP Server Settings

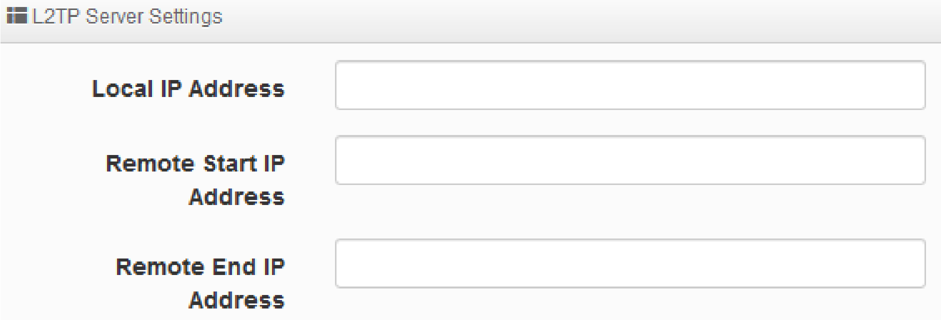
Connections	10	
Local IP Address		
Remote Start IP Address		
Remote End IP Address		
MPPE40	● Enable	○ Disable
MPPE128	● Enable	○ Disable

- **Connections:** Administrator can set connected VPN client Qty.
- **Local IP Address:** Set virtual IP address for VPN server.
- **Remote Start/ End IP Address:** Set start to end IP address for dynamic configuration, can give VPN client automatically obtain a virtual IP address.

Notice	**This IP address is set as a VPN-specific virtual IP address tunnel, the IP address can't set same subnet of the WAN and LAN (network).**

- **MPPT40/128:** Administrator can choose use VPN security for 40 or 128 bit.

L2TP Server:

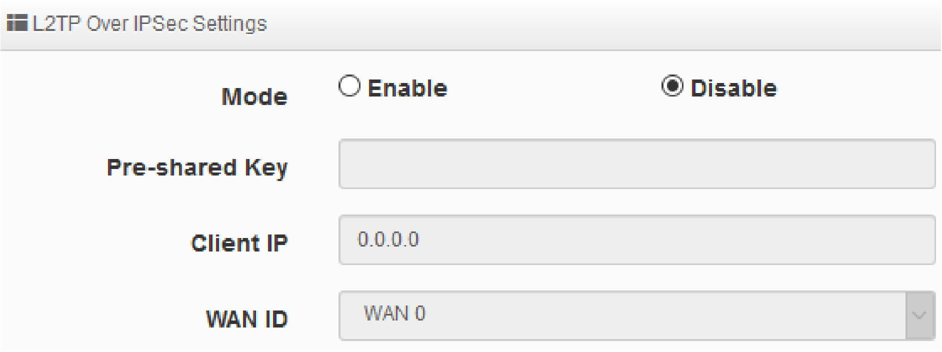


L2TP Server Settings

Local IP Address	
Remote Start IP Address	
Remote End IP Address	

- **Local IP Address:** Set virtual IP address for VPN server.
- **Remote Start/ End IP Address:** Set start to end IP address for dynamic configuration, can give VPN client automatically obtain a virtual IP address.

Notice	**This IP address is set as a VPN-specific virtual IP address tunnel, the IP address can't set same subnet of the WAN and LAN (network).**



L2TP Over IPSec Settings

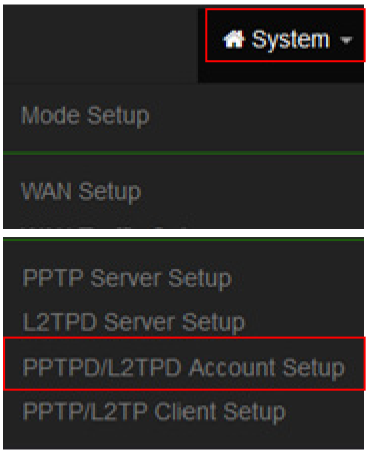
Mode	○ Enable	● Disable
Pre-shared Key		
Client IP	0.0.0.0	
WAN ID	WAN 0	

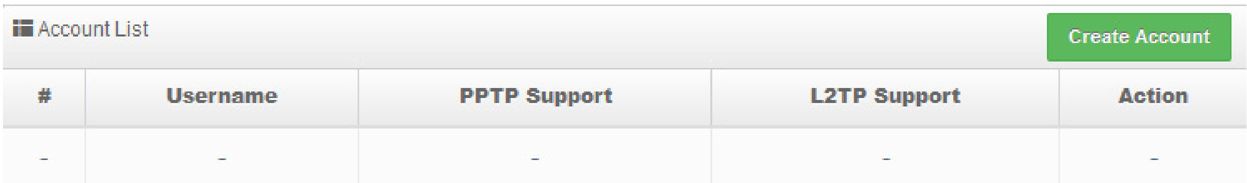
- **Mode:** Administrator can choose Enable or disable this function.
- **Pre-shared Key:** Set a security key for Pre-shared Key
- **Client IP:** Set a IP address of client.
- **WAN ID:** Select a access passage.

3.9 PPTP/L2TP Account Setup

Create PPTP / L2TP authentication account with maximum of 10 VPN accounts.

Please click “System”➔”PPTP/L2TP Account Setup”



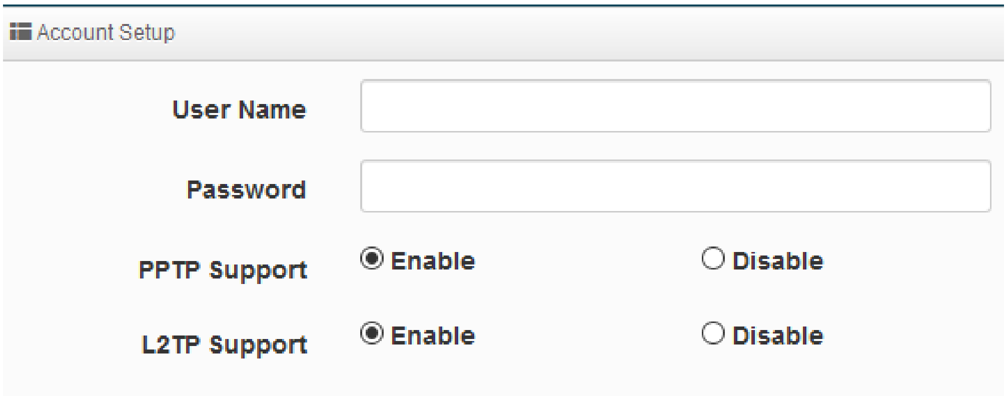


Account List

Create Account

#	Username	PPTP Support	L2TP Support	Action
-	-	-	-	-

- **Create Account:** Administrator can click the button to create authentication account of client.



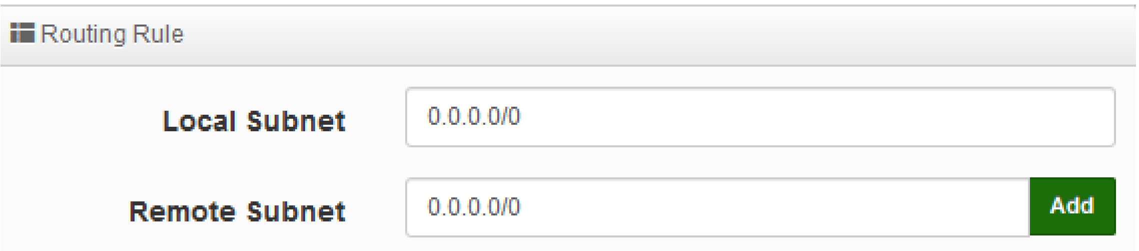
Account Setup

User Name		
Password		
PPTP Support	● Enable	○ Disable
L2TP Support	● Enable	○ Disable

- **User Name/Password:** Set authentication account of name/password.
- **PPTP/L2TP Support:** Set account used to PPTP or L2TP protocol.

Routing Rule:

Set routing of both network



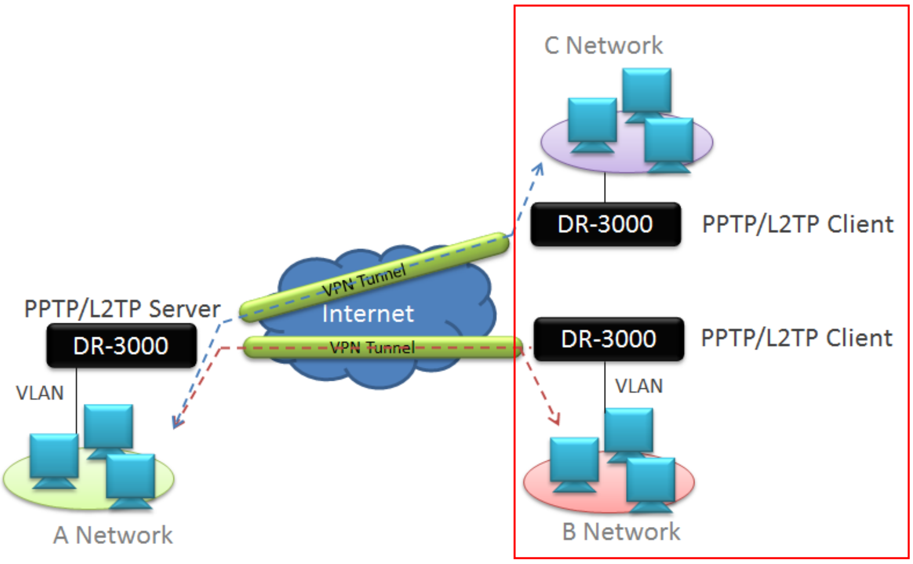
Routing Rule

Local Subnet	0.0.0.0/0
Remote Subnet	0.0.0.0/0

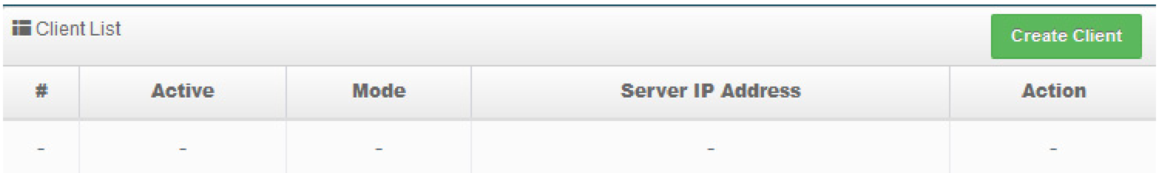
- **Local Subnet:** Set network subnet of local.
- **Remote Subnet:** Set network subnet of Remote.

3.10 PPTP/L2TP Client Setup

If remote have PPTP/L2TP VPN server, administrator can used PPTP/L2TP client function connection to remote VPN server.



Please click "System"➔"PPTP/L2TP Client setup"

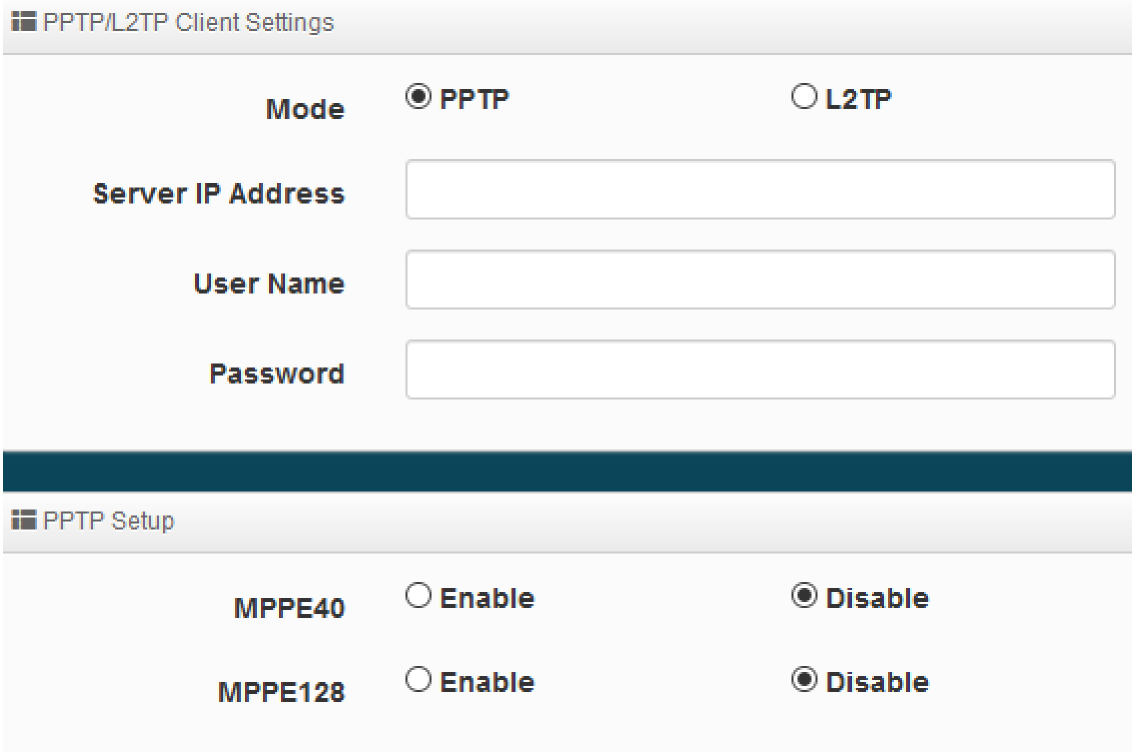


Client List

Create Client

#	Active	Mode	Server IP Address	Action
-	-	-	-	-

➢ **Create Client:** Administrator can click the button to set PPTP/L2TP Client function.



PPTP/L2TP Client Settings

Mode	● PPTP	○ L2TP
Server IP Address		
User Name		
Password		

PPTP Setup

MPPE40	○ Enable	● Disable
MPPE128	○ Enable	● Disable

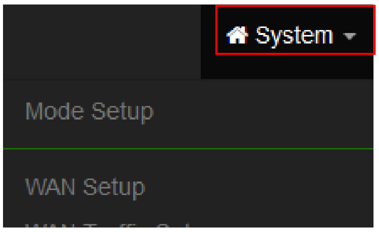
- **Mode:** Administrator can select use PPTP or L2TP protocol connection to remote VPN server. If VPN server used PPTP Protocol then please choose PPTP.
- **Server IP Address:** Administrator must set remote VPN server used real IP address.
- **User Name / Password:** Set VPN authentication account and password (Please Refer to 3.9 Account Setup)
- **MPPE40/128:** Base on remote VPN server used security.

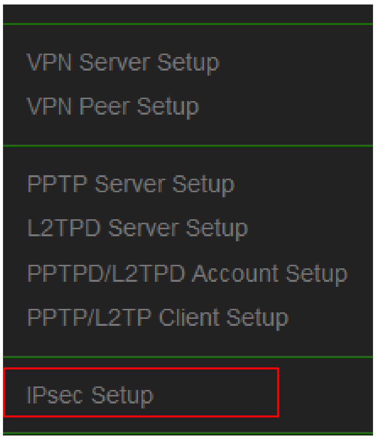
3.11 IPSec Setup

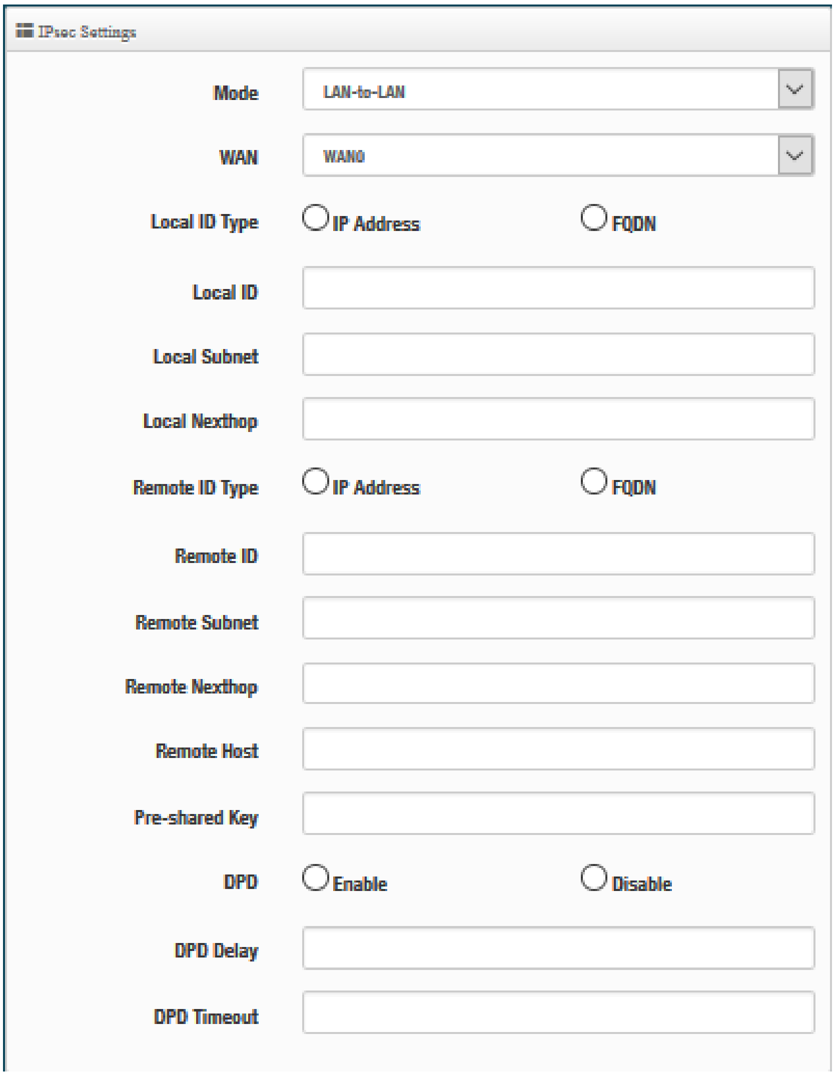
Notice **This VPN function support three protocol are VPN Server 、PPTP/L2TP and IPsec, the VPN tunnel of these three types only select one VPN protocol to used it.**

Administrator can create new VPN connection for the IPSec.

Please Click “**System**”➔”**IPSec Setup**”







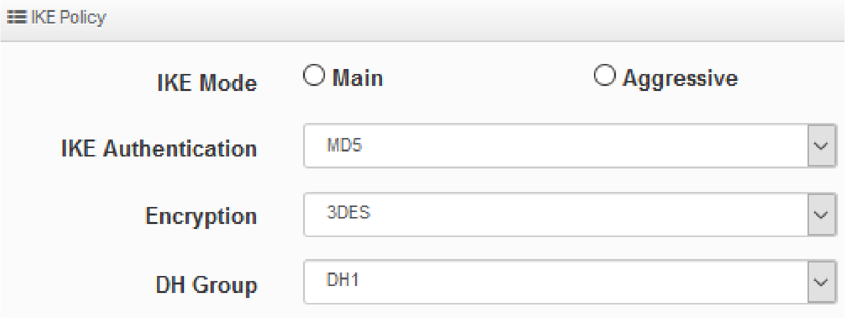
IPsec Settings

Mode	LAN-to-LAN	
WAN	WAN0	
Local ID Type	○ IP Address	○ FQDN
Local ID		
Local Subnet		
Local Nexthop		
Remote ID Type	○ IP Address	○ FQDN
Remote ID		
Remote Subnet		
Remote Nexthop		
Remote Host		
Pre-shared Key		
DPD	○ Enable	○ Disable
DPD Delay		
DPD Timeout		

- **Mode:** Administrator can be according to different needs select use LAN to LAN or Client to LAN.
- **WAN:** Administrator can choose use specific WAN Port connection.
- **Local ID Type:** Administrator can select use IP address or FQDN for Local IP Type.
- **Local Subnet:** Administrator must set Local Subnet for the VPN "LAN to LAN".
- **Local Nexthop:** Administrator can add a VPN Next hop address for Local.
- **Remote ID Type:** Administrator can select use IP address or FQDN for Remote IP Type.
- **Remote Subnet:** Administrator must set remote Subnet for the VPN "LAN to LAN".
- **Remote Nexthop:** Administrator can add a VPN Next hop address for Remote
- **Pre-shared Key:** Enter Pre-shared Key for VLAN.
- **DPD:** DPD (Dead peer detection) is a method that network devices use to verify the current existence and availability of other peer devices. The system can waiting for DPD acknowledgements (R-U-THERE-ACK messages) from the peer.
- **DPD Delay:** Administrator can set delay time (seconds) for DPD.
- **DPD Timeout:** Administrator can set timeout of times for DPD.

IKE Policy:

This function is verification the VPN identity. The VPN to establish a connection with each other must be certified to establish a trust relationship between each other, this function supports IKE Phase 1/2.

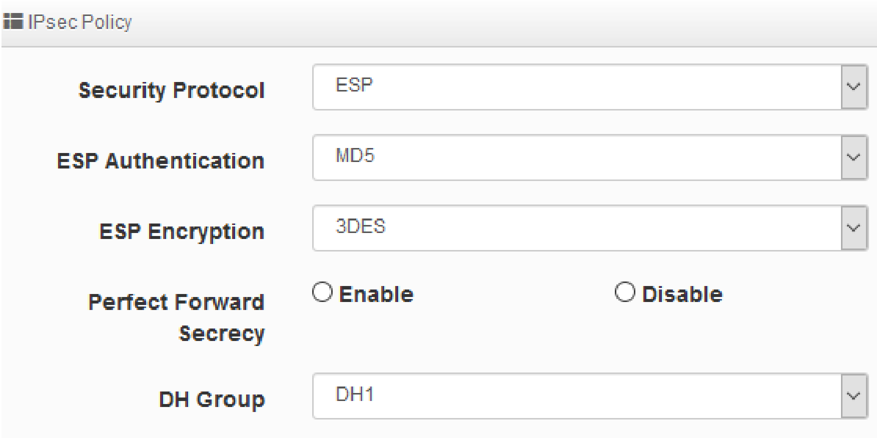


IKE Policy

IKE Mode	○ Main	○ Aggressive
IKE Authentication	MD5	
Encryption	3DES	
DH Group	DH1	

- ➢ **IKE Mode:** Administrator can select Main or Aggressive of the IKE. If device uses Router mode then suggest use Main mode is high security.
- ➢ **IKE Authentication:** Administrator can select authentication method for MD5, SHA1, SHA2_256.
- ➢ **Encryption:** Set encryption method for IKE. Administrator can select use 3DES and AES128/192/256.
- ➢ **DH Group:** Diffie-Hellma is key exchange. Allows two devices to establish a shared secret over an unsecure network. In terms of VPN it is used in the in IKE or Phase1 part of setting up the VPN tunnel. This DH Group support DH1/2/5/14.

IPSec Policy:



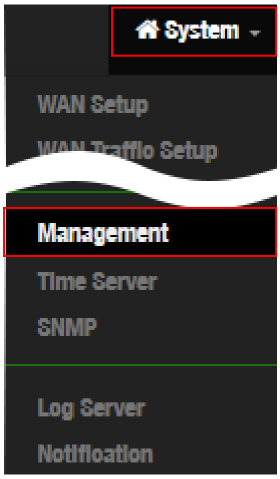
IPsec Policy

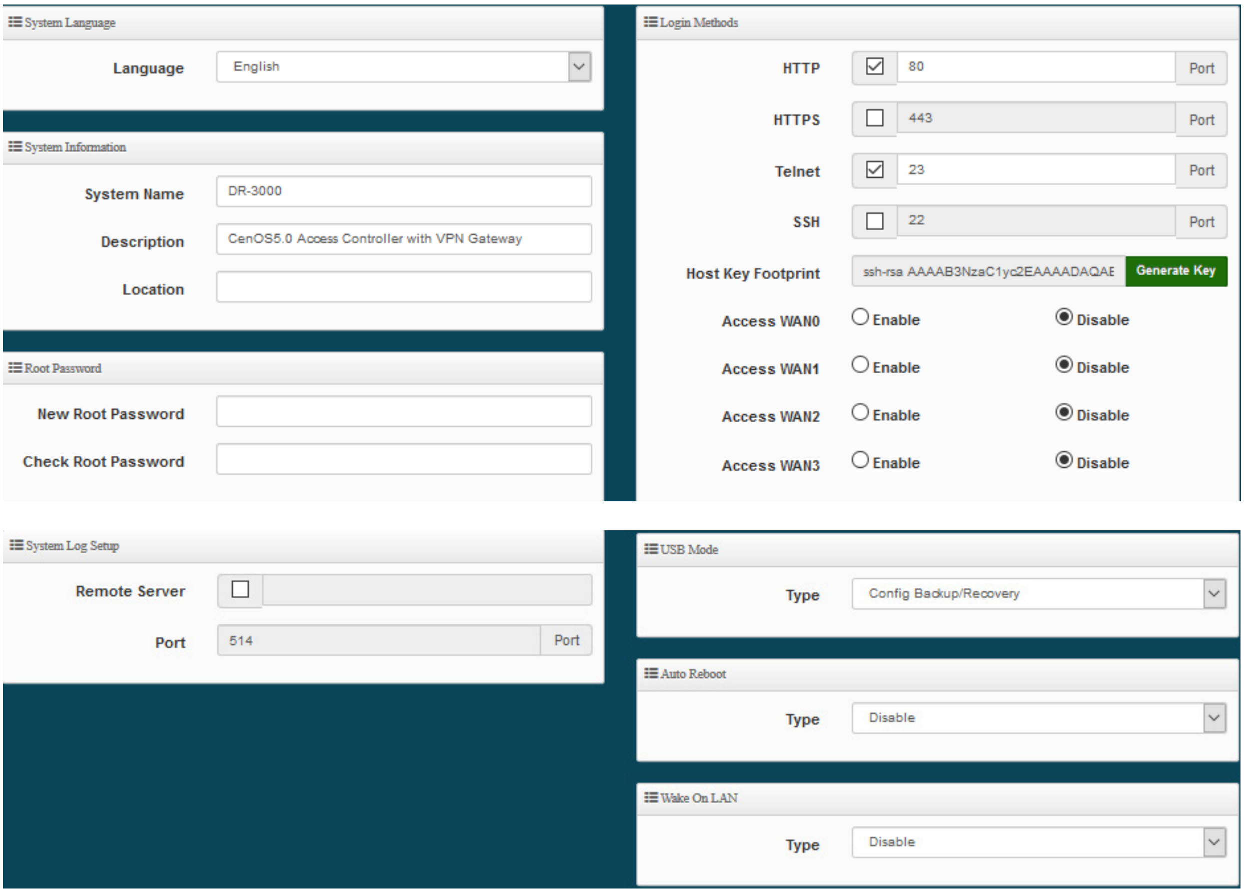
Security Protocol	ESP	
ESP Authentication	MD5	
ESP Encryption	3DES	
Perfect Forward Secrecy	○ Enable	○ Disable
DH Group	DH1	

- ➢ **Security Protocol:** The IPSec security use ESP protocol.
- ➢ **ESP Authentication:** Administrator can select authentication method for MD5, SHA1, SHA2_256.
- ➢ **ESP Encryption:** Set encryption method for ESP. Administrator can select use 3DES and AES128/192/256.
- ➢ **Perfect Forward Secrecy:** Administrator can select enable or disable for DH Group.

3.12 Management

Administrators can specify geographical location of the system via instructions in this page and modify system login password and select use system login protocol by 80, 443, 23, 22 Port.
The management page support syslog server function and system auto reboot function.





System Language

Language	English

System Information

System Name	DR-3000
Description	CenOS5.0 Access Controller with VPN Gateway
Location	

Root Password

New Root Password	
Check Root Password	

Login Methods

HTTP	☑	80	Port
HTTPS	□	443	Port
Telnet	☑	23	Port
SSH	□	22	Port
Host Key Footprint	ssh-rsa AAAAB3NzaC1yc2EAAAADAQAE	Generate Key	
Access WAN0	○ Enable	● Disable	
Access WAN1	○ Enable	● Disable	
Access WAN2	○ Enable	● Disable	
Access WAN3	○ Enable	● Disable	

System Log Setup

Remote Server	□	
Port	514	Port

USB Mode

Type	Config Backup/Recovery

Auto Reboot

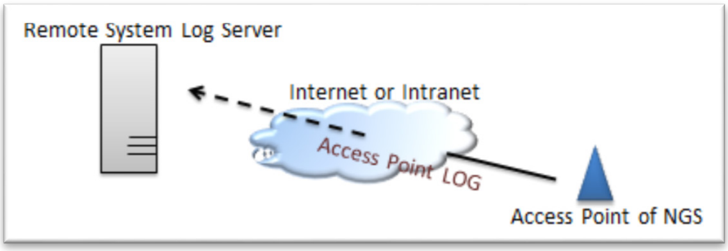
Type	Disable

Wake On LAN

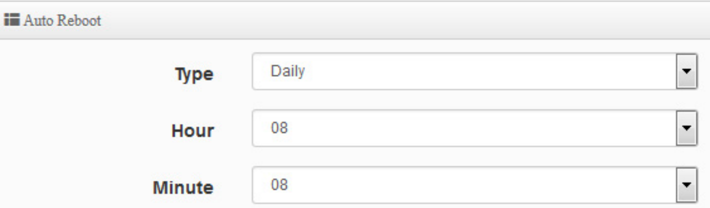
Type	Disable

- **System Information:** Administrator can set the system name / Description and Location.
- **Root Password:** Administrator can change system login password.
- **Login Methods:** Administrator can set system login protocol of the http/https/telnet and ssh.

- **Access WAN# :** If enable this WAN# then external (Internet) will can access management interface for DR-3000. The default is Disable. (This function can only be used in Router mode)
  - **System Log Setup:** Administrator can be backup system log or authentication log to remote server. Please enter IP address and port of remote syslog server.



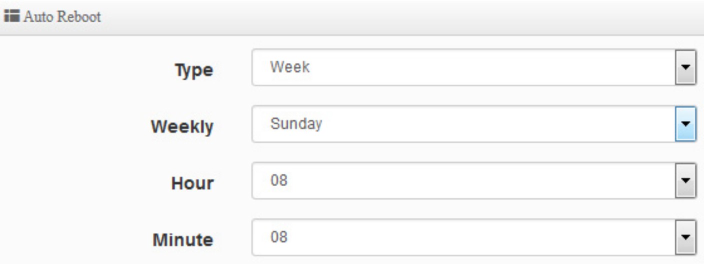
  - **Auto Reboot:** The functions can Auto-reboot the system by Date/time management.
    - **Daily：** Setting time to system reboot.



Auto Reboot

Type	Daily
Hour	08
Minute	08

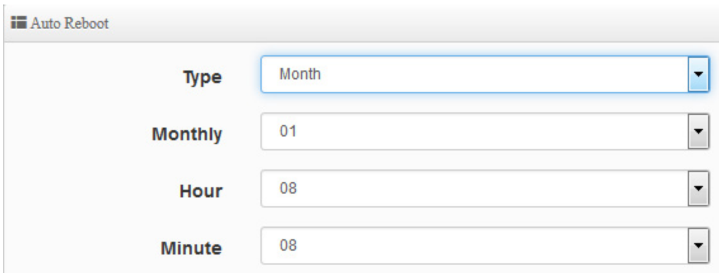
    - **Weekly :** Setting frequency (ex. Weekly) and time of system reboot



Auto Reboot

Type	Week
Weekly	Sunday
Hour	08
Minute	08

    - **Monthly :** Setting Every month, fixed date and time to system reboot



Auto Reboot

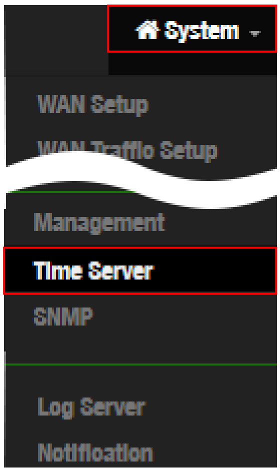
Type	Month
Monthly	01
Hour	08
Minute	08

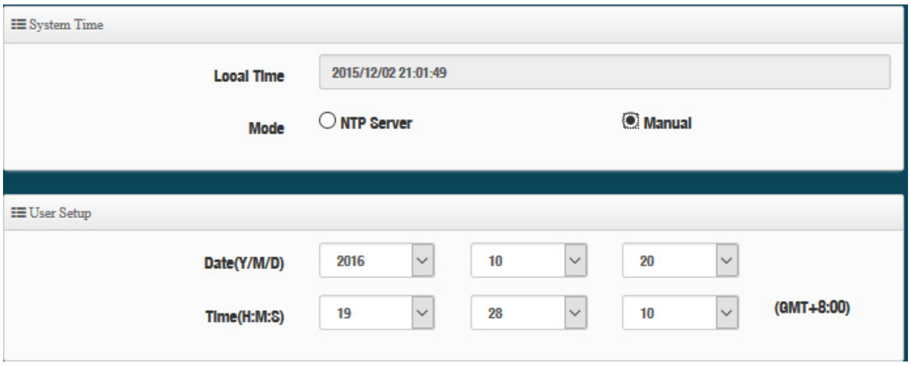
  - **Wake On LAN:** The functions can Auto-Wake LAN device via system by Date/time management.

3.13 Time Server

Administrator can select manual or via a NTP server to modify system time for the right local time. If select update the system time for manual, when administrator reboot system the system time will reply default.

If select update the system time for the NTP Server, system must set gateway and DNS server, the system can be connected internet.




System Time

Local Time: 2015/12/02 21:01:49

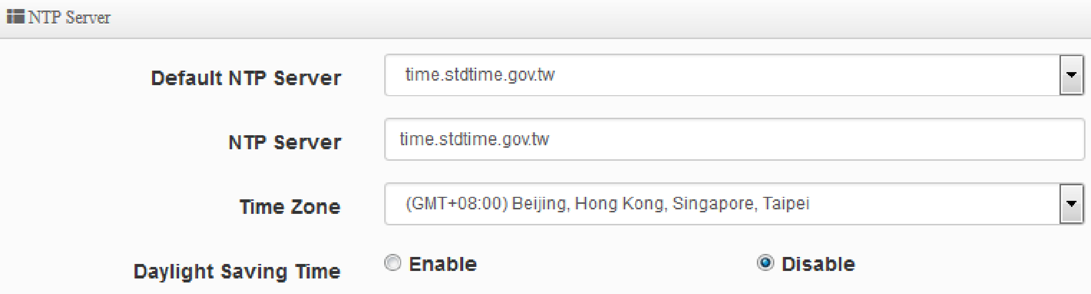
Mode: ○ NTP Server ● Manual

User Setup

Date(Y/M/D): 2016 / 10 / 20

Time(H:M:S): 19 / 28 / 10 (GMT+8:00)

- **Mode:** Administrator can select NTP Server or Manual.
  - **NTP Server:** System can auto update the system time. Administrator needs setting as NTP Server.


NTP Server

Default NTP Server: time.stdtime.gov.tw

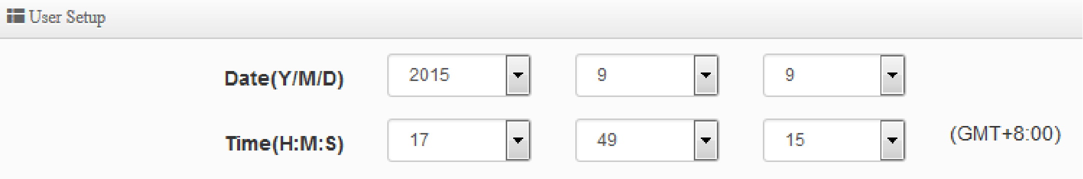
NTP Server: time.stdtime.gov.tw

Time Zone: (GMT+08:00) Beijing, Hong Kong, Singapore, Taipei

Daylight Saving Time: ○ Enable ● Disable

- ✓ **Default NTP Server:** Administrator can select NTP Server.
- ✓ **NTP Server:** Administrator can setting as NTP Server.
- ✓ **Time Zone:** Administrator can select a desired time zone from the drop-down list.
- ✓ **Daylight saving Time:** Enable or disable Daylight saving.

- **Manual:** Administrator need to set the system time.

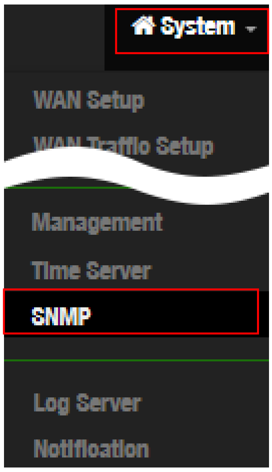

User Setup

Date(Y/M/D): 2015 / 9 / 9

Time(H:M:S): 17 / 49 / 15 (GMT+8:00)

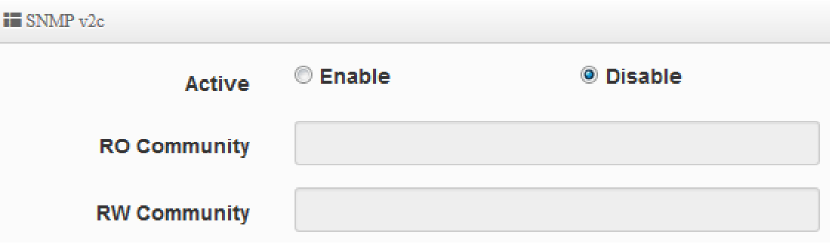
3.14 SNMP

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely.



Please click on **System -> SNMP** and follow the below setting.

SNMP v2c function

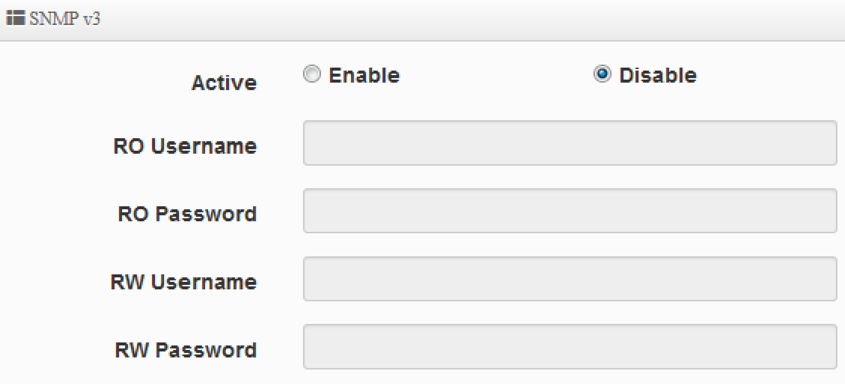


SNMP v2c

Active	○ Enable	● Disable
RO Community		
RW Community		

- **Active:** Administrator can select Enable or Disable the service.
- **RO Community:** Set a community string to authorize read-only access.
- **RW Community:** Set a community string to authorize read/write access.

SNMP v3 function



SNMP v3

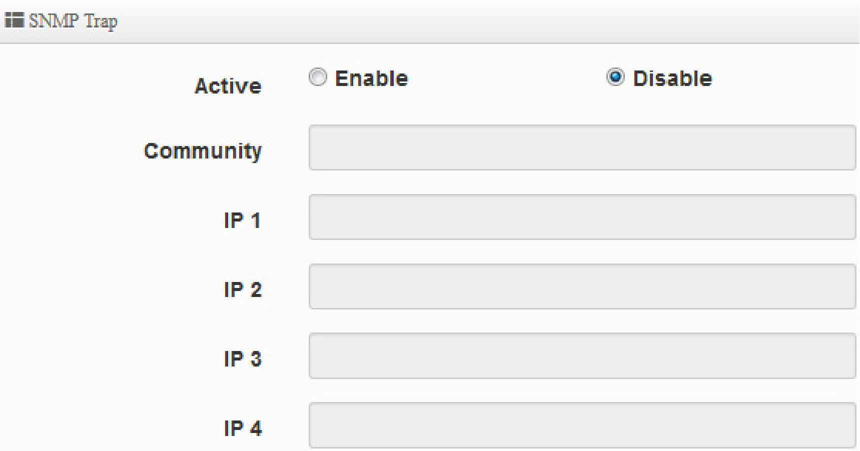
Active	○ Enable	● Disable
RO Username		
RO Password		
RW Username		
RW Password		

- **Active:** Administrator can select Enable or Disable the service.
- **RO username:** Set a community string to authorize read-only access.

- **Ro password:** Set a password to authorize read-only access.
- **RW username:** Set a community string to authorize read/write access.
- **RW password:** Set a password to authorize read/write access.

SNMP Trap

Events such as cold start interface up & down, and association & disassociation will report to an assigned server.



SNMP Trap

Active ○ Enable ● Disable

Community

IP 1

IP 2

IP 3

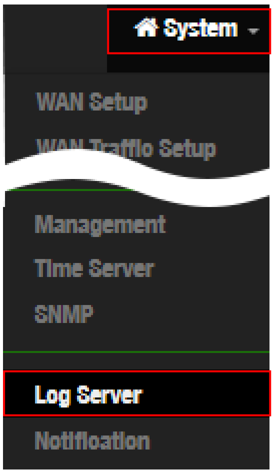
IP 4

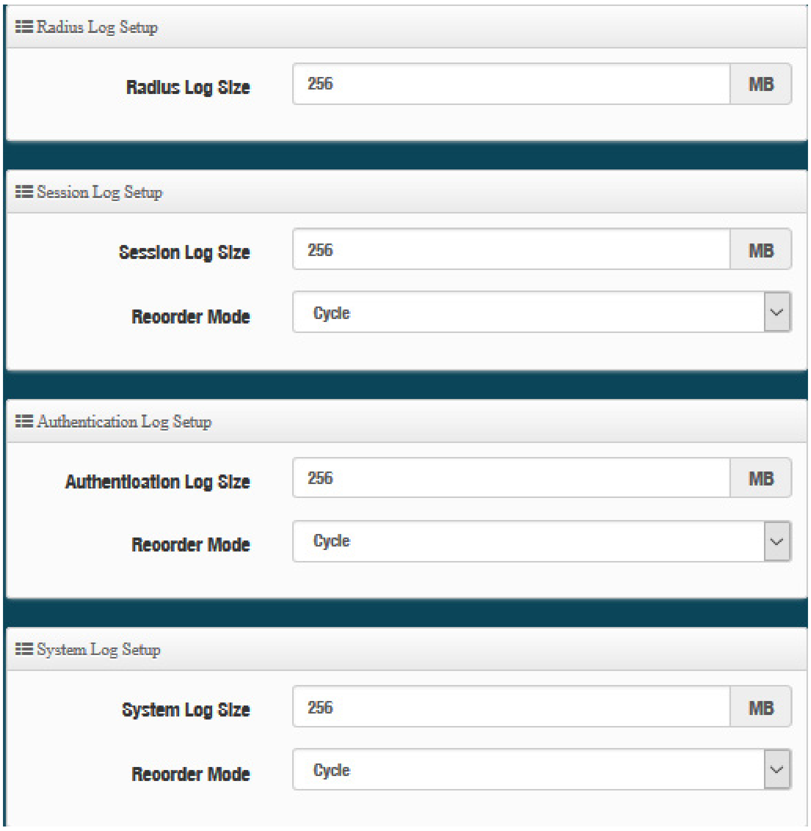
- **Active:** Administrator can select Enable or Disable the service.
- **Community:** Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
- **IP(1~4) :** Enter the IP addresses of the remote hosts to receive trap messages.

3.15 Log Server Setup

If devices used CERIO products and support syslog server function, the devices log can be transferred to this server and record devices log. Administrator can set storage space for the session/authentication and devices system log.

System can use e-mail send log Message to administrator.





Radius Log Setup

Radius Log Size: 256 MB

Session Log Setup

Session Log Size: 256 MB

Reoorder Mode: Cycle

Authentication Log Setup

Authentioation Log Size: 256 MB

Reoorder Mode: Cycle

System Log Setup

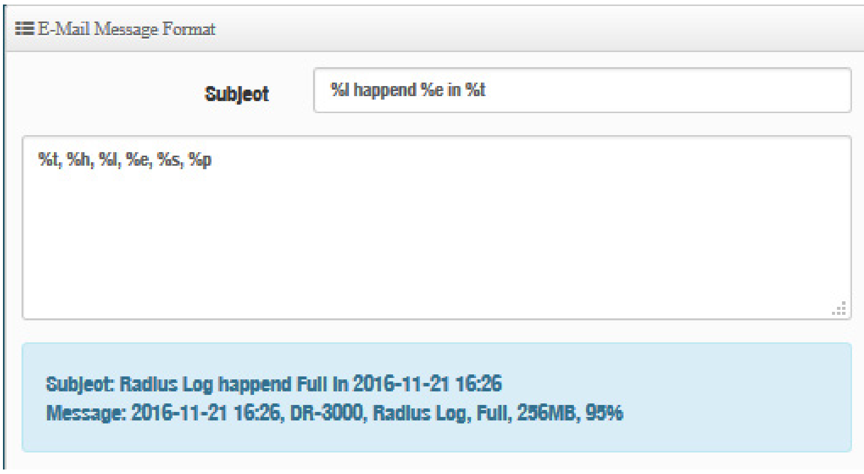
System Log Size: 256 MB

Reoorder Mode: Cycle

- **Log Size:** Administrator can set storage space for RADIUS/session/authentication and system log.(max.512MB)
- **Recorder Mode:** The function can auto clear Log information or stop services.
  - **Cycle:** System will auto clear log by cycle.
  - **Retention Period:** System will auto clear log by Retention Period. Administrator can set days for retention period. (Max. 90 days)
  - **Stop Service:** If the system storage is full, the system will auto stop recording.

E-Mail Message setting

Administrator can set E-Mail messenger format and set **3.16 Notification Setup** function send e-mail to administrator.

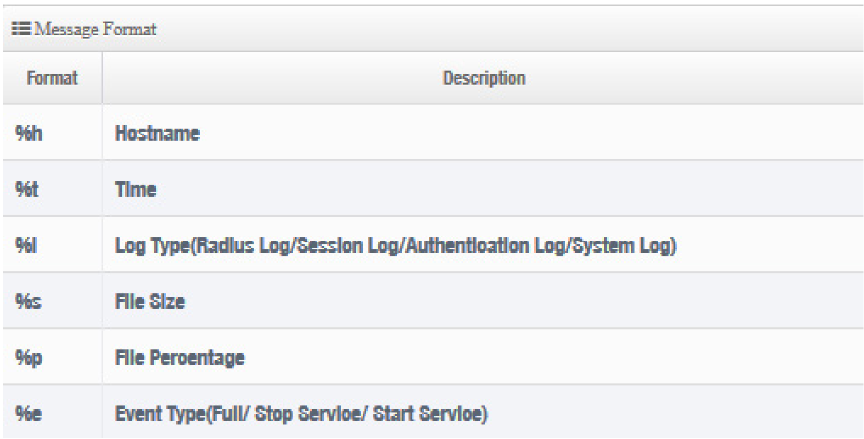


E-Mail Message Format

Subject: %l happend %e in %t

%t, %h, %l, %e, %s, %p

Subject: Radius Log happend Full in 2016-11-21 16:26
Message: 2016-11-21 16:26, DR-3000, Radius Log, Full, 256MB, 95%



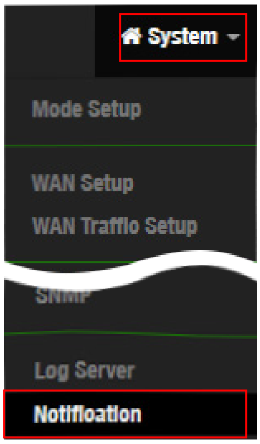
Message Format

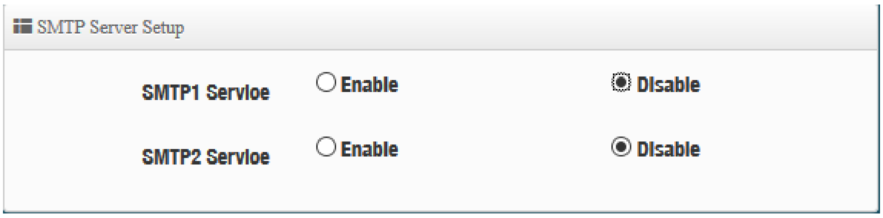
Format	Description
%h	Hostname
%t	Time
%l	Log Type(Radius Log/Session Log/Authentication Log/System Log)
%s	File Size
%p	File Percentage
%e	Event Type(Full/ Stop Service/ Start Service)

3.16 Notification Setup

Administrator can automatically send the notification of Radius Log, Session Log, Authentication Log and System Log to 2 particular E-mail addresses. The E-Mail setting support SMTP server test, when administrator once the setup complete of the SMTP server will can use the test tool to confirm SMTP is working properly.

Please click **“System”** ➔ **“Notification”** functions of Notification E-mail Setup will appear and enter the related information and select the desired items and then apply the settings.

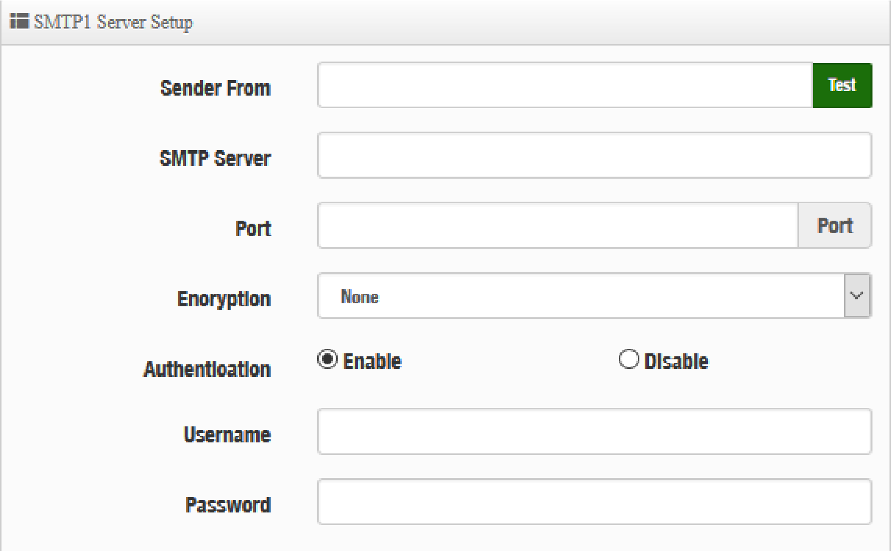




SMTP Server Setup

SMTP1 Service	○ Enable	● Disable
SMTP2 Service	○ Enable	● Disable

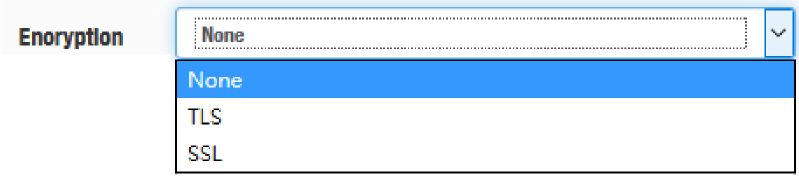
- ➢ **SMPT1/2 Service:** Administrator can select Enable or Disable the SMPT functions. If administrator select enable the function will following explains how to configure the SMTP functions.



SMTP1 Server Setup

Sender From	[ ] Test
SMTP Server	[ ]
Port	[ ] Port
Encryption	None
Authentication	● Enable ○ Disable
Username	[ ]
Password	[ ]

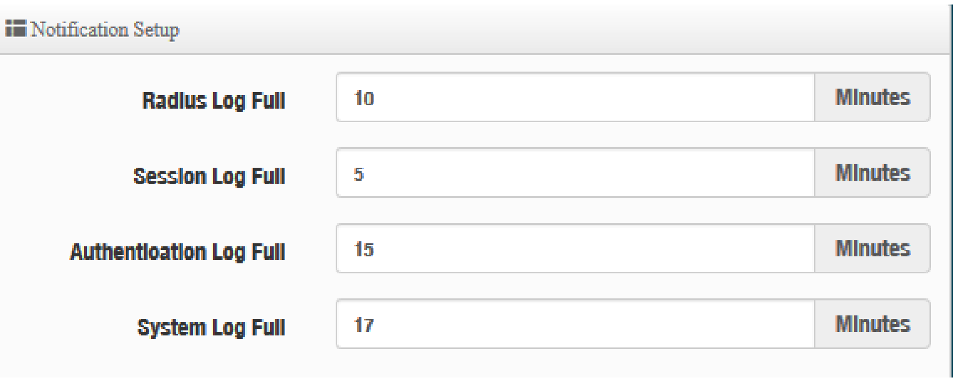
- ➢ **Sender From:** Administrator can set E-Mail address by from.
- ➢ **SMTP Server:** Administrator can set E-Mail SMTP server.
- ➢ **Port:** Administrator can set SMPT Server used Port.
- ➢ **Encryption:** Administrator can select use TLS or SSL encryption type for the SMPT Server.



- ➢ **Authentication:** If SMTP Server must use authentication, Administrator can select enable the SMTP server authentication for E-Mail user account.

Notification Setup

Administrator can set time for the RADIUS, Session, Authentication and system log send to administrator E-Mail.

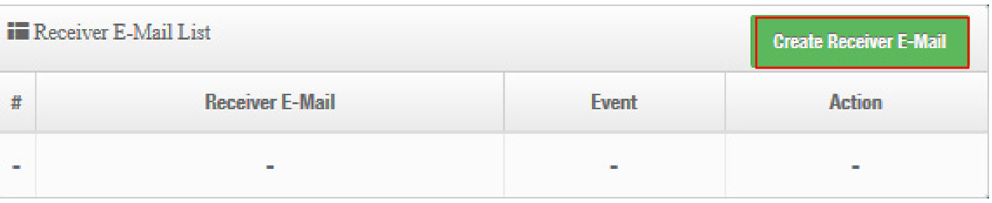


Notification Setup

Radius Log Full	10	Minutes
Session Log Full	5	Minutes
Authentication Log Full	15	Minutes
System Log Full	17	Minutes

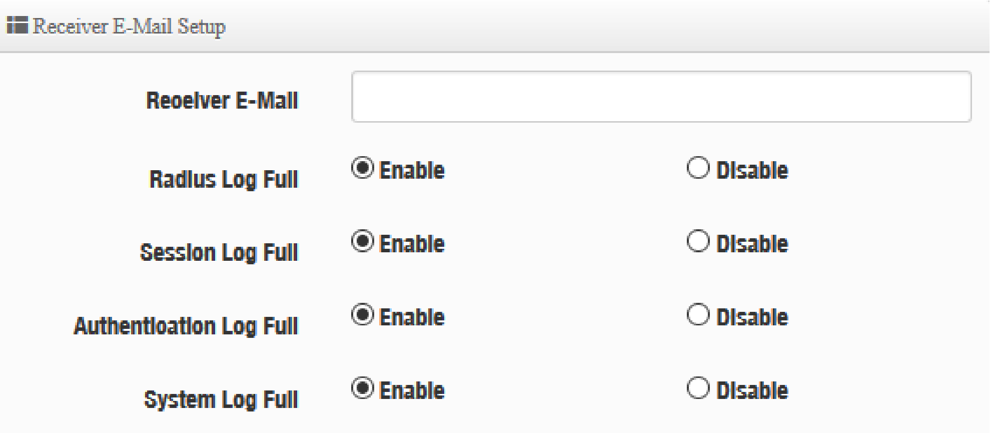
Receiver E-Mail List

Administrator can click “Create Receiver E-Mail” button to set administrator E-mail address.



Receiver E-Mail List

#	Receiver E-Mail	Event	Action
-	-	-	-



Receiver E-Mail Setup

Receiver E-Mail		
Radius Log Full	● Enable	○ Disable
Session Log Full	● Enable	○ Disable
Authentication Log Full	● Enable	○ Disable
System Log Full	● Enable	○ Disable

- **Receiver E-Mail:** Administrator can set received e-mail address.
- **Log Full:** Administrator can select the Radius, Session, Authentication and System Log to receive.

4. AP Control

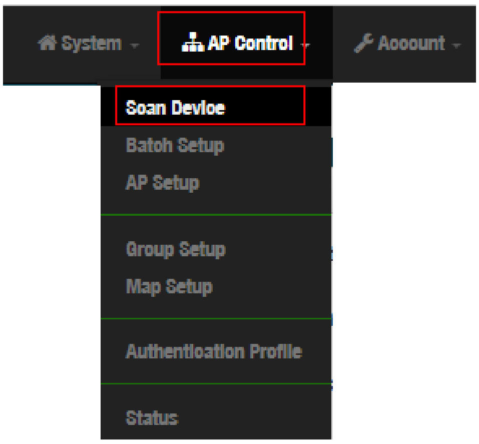
This function is primarily to control all the CERIO managed AP.

Administrator can use AP Control functions to centralize management of APs in the network architecture. AP control Setting functions have “Scan Device”, “Batch Setup”, “AP Setup”, “Group / Map setup” and Authentication Profile setup etc..

Please click **“AP Control”** to enter AP Management settings

4.1 Scan Device

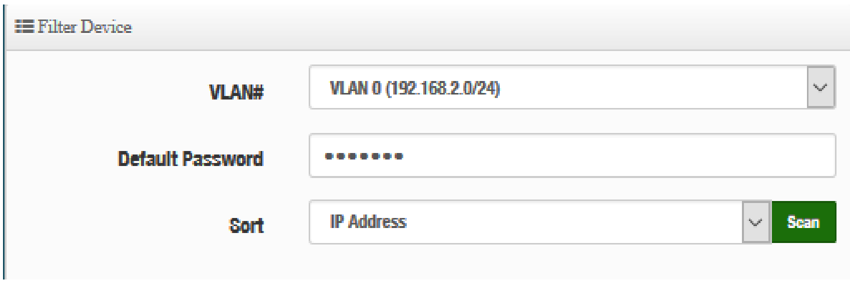
This management page can discover all managed APs in the network. Administrator can set IP address / Password and VLAN tag for managed APs. After the setup is complete, Administrator must import all managed APs to databases.



Centralized Management APs operating Instructions:

1) Click **“Scan Device”** to discover Access Points in the network architecture.
2) Set IP address for all managed Access Points and reboot managed Access Points.
3) Re-Scan managed APs and Import to databases.
4) Centralize managed AP settings by clicking “**AP control**” ➔ **“Batch setup”**
5) After the setup is complete for managed APs function, administrator must reboot all managed APs.

This management page can discover all managed APs in the network. Administrator can set IP address / Password and VLAN tag for managed APs. After the setup is complete, Administrator must import all managed APs to databases.



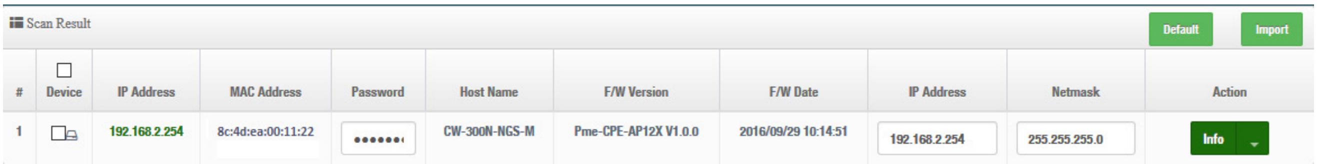
Filter Device

VLAN# VLAN 0 (192.168.2.0/24)

Default Password ●●●●●●●

Sort IP Address

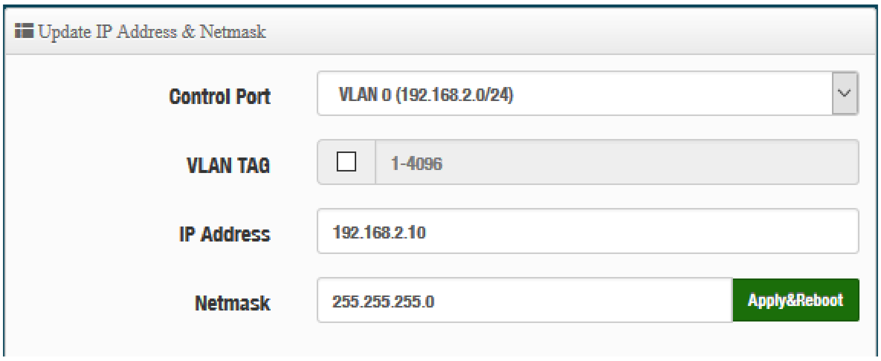
- ➢ **VLAN# :** Administrator can select VLAN network to discovery managed Aps
- ➢ **Default Password:** Set login system password by managed Aps.
- ➢ **Sort**: Administrator can select discovery managed Aps Type. (IP or MAC)



Scan Result

#	☐ Device	IP Address	MAC Address	Password	Host Name	F/W Version	F/W Date	IP Address	Netmask	Action
1		192.168.2.254	8c:4d:ea:00:11:22	•••••••	CW-300N-NGS-M	Pme-CPE-AP12X V1.0.0	2016/09/29 10:14:51	192.168.2.254	255.255.255.0	Info

- **#：** Display managed APs items.
- **Device：**Administrator can select all or single for managed Aps**.**
- **IP Address：** Display IP address for managed AP.
- **MAC Address：**Display MAC address for managed AP.
- **Host Name：**Display host name for managed AP.
- **F/W Version：**Display firmware version for managed AP.
- **F/W Date：**Display firmware Release date for managed AP.
- **IP Address：**Administrator can set single IP address for Managed AP.
- **Netmask：**Administrator can set single Netmask for Managed AP.
- **Default：**Administrator click the button will can reset to default for select managed APs.



Update IP Address & Netmask

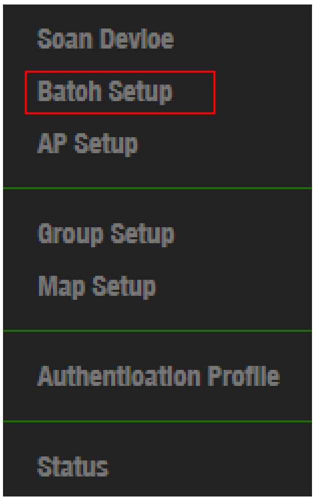
Control Port	VLAN 0 (192.168.2.0/24)
VLAN TAG	☐ 1-4096
IP Address	192.168.2.10
Netmask	255.255.255.0

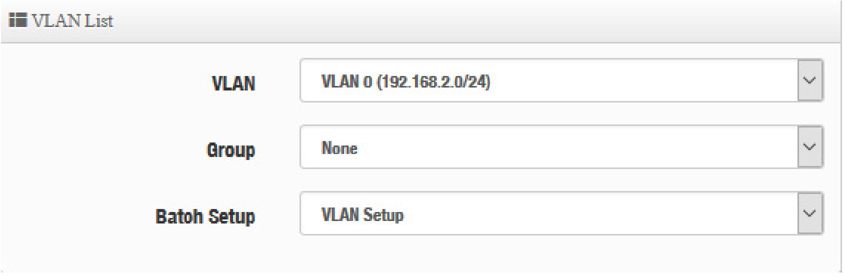
- **Control Port：**Administrator can change VLAN network for managed APs.
- **VLAN TAG：**Administrator can set VLAN TAG ID for managed APs.
- **IP Address：**Administrator can set IP address for managed APs, the IP address is auto-incrementally.
- **NetMask：**Administrator can set NetMask for managed APs.

When the setting managed APs is completed, please click Apply & Reboot button to complete the setup process.

4.2 Batch Setup

The AP control function supports centralized configuration of managed APs. Administrator can change VLAN network / Group and batch setup for managed APs.





VLAN: VLAN 0 (192.168.2.0/24)

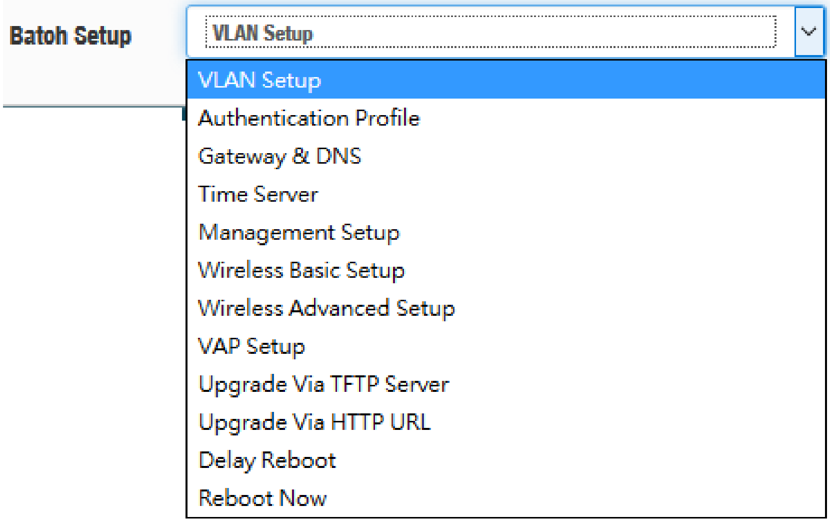
Group: None

Batoh Setup: VLAN Setup

➢ **LAN**：When VLAN Tag function is enabled (please refer to 4.1 System VLAN Setup), administrator can change VLAN tag for managed APs.

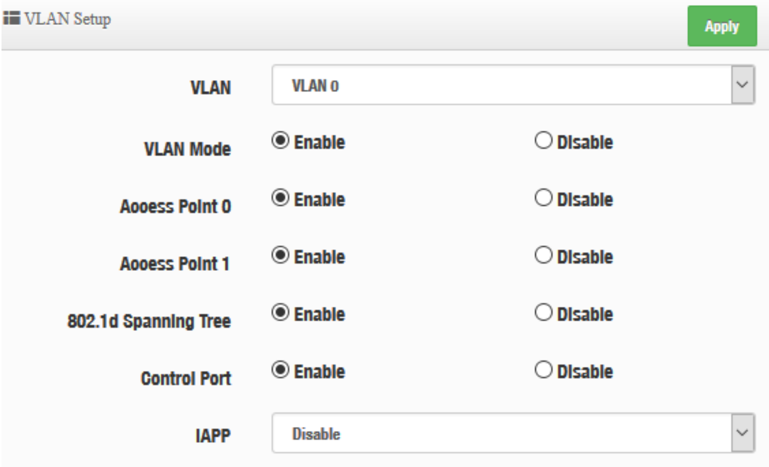
➢ **Group**：When AP Groups are created (please refer to 4.2.4 Group setup), Administrators can select and change group settings of managed APs.

➢ **Batch Setup**：Administrator can centralize setting changes for managed APs.



Batoh Setup: VLAN Setup

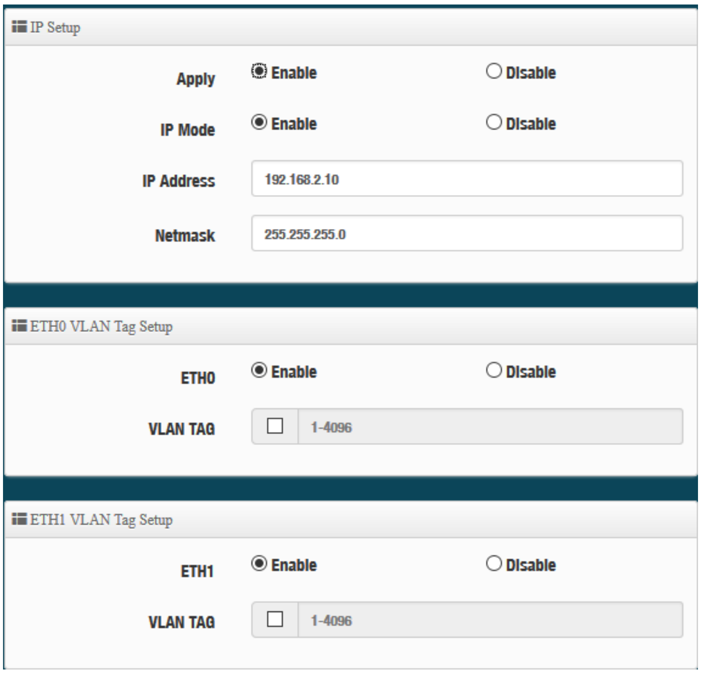
- **VLAN Setup**：Administrator can set VLAN Tag, IP address and Wi-Fi on/off for the managed APs.



VLAN Setup — Apply

VLAN	VLAN 0	
VLAN Mode	● Enable	○ Disable
Access Point 0	● Enable	○ Disable
Access Point 1	● Enable	○ Disable
802.1d Spanning Tree	● Enable	○ Disable
Control Port	● Enable	○ Disable
IAPP	Disable	

- ✓ **VLAN**：The function can select VLAN (please refer to 3.2 Configure VLAN Setup) for managed APs.
- ✓ **VLAN Mode**：Administrator can enable or disable VLAN mode of the managed APs.
- ✓ **Access Point0/1**：Administrator can enable or disable 2.4 or 5G radio of the managed APs. (Access Point 0 is radio 2.4G, Access Point 1 is radio 5G)
- ✓ **802.1d Spanning Tree**：Administrator can enable or disable the function.(please refer to 3.2.1 Configure Network ➔ 802.1d Spanning Tree)
- ✓ **Control Port**：The function administrator can enable or disable of the managed APs (please refer to 3.2.1 Configure Network ➔ Control Port)
- ✓ **IAPP**：The function administrator can enable or disable of the managed APs (Please refer to 3.2.1 Configure Network ➔ IAPP)



IP Setup

Apply	● Enable	○ Disable
IP Mode	● Enable	○ Disable
IP Address	192.168.2.10	
Netmask	255.255.255.0	

ETH0 VLAN Tag Setup

ETH0	● Enable	○ Disable
VLAN TAG	□ 1-4096	

ETH1 VLAN Tag Setup

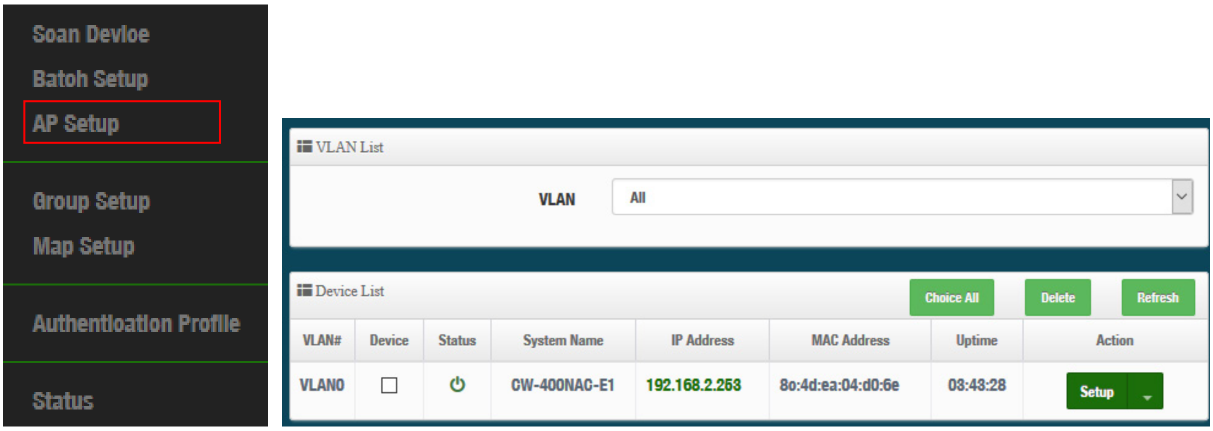
ETH1	● Enable	○ Disable
VLAN TAG	□ 1-4096	

- ✓ **IP Setup**：Administrator can set IP address and Netmask of the managed APs.
- ✓ **ETH0/1 VLAN Tag Setup**：Administrator can set VLAN Tag or disable VLAN function of the managed APs.

- **Authentication Profile**：After creating Profiles, See: “4.2.6 Authentication Profile” users can conveniently apply Authentication profiles
- **Gateway & DNS:** Setting Gateway and DNS for managed APs.
- **Time Server:** Setting System Time for managed APs. (Please refer to 5.2 Configure Time Server)
- **Management Setup:** Setting system name/ system login port and system log server service for managed APs. (Please refer to 5.1 system management)
- **Wireless Batch Setup:** Setting Wi-Fi configurations for managed APs. (Please refer to 3.6 Wireless Basic Setup)
- **Wireless Advanced Setup:** Setting Wi-Fi Advanced settings for managed APs. (Please refer to 3.6.3 Wireless Advanced Setup)
- **VAP Setup**：Wi-Fi SSID / channel or security settings for managed APs. (Please refer to 3.2.3 Configure Radio 0/1)
- **Upgrade via TFTP Server:** Administrator can centrally upgrade firmware via TFTP Server for the managed APs.
- **Upgrade via HTTP Server:** Administrator can centrally upgrade firmware via HTTP Server for the managed APs.
- **Delay Reboot:** Administrators can set managed APs to reboot after the wait time
- **Reboot:** Administrator can reboot managed APs.

4.3 AP Setup

Administrator can monitor statuses and modify managed APs information.



VLAN List

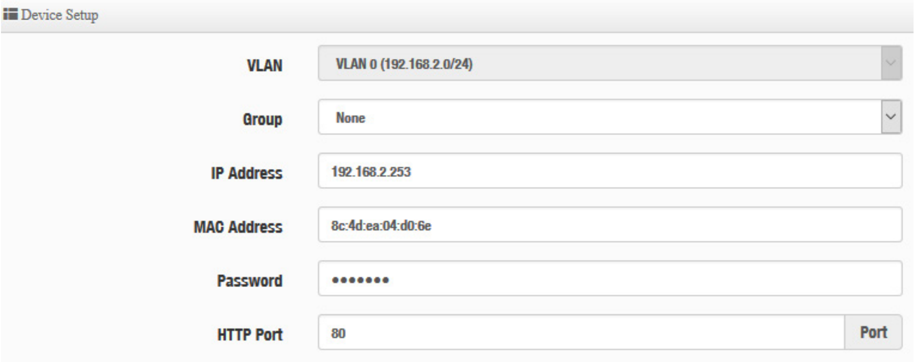
VLAN: All

Device List

VLAN#	Device	Status	System Name	IP Address	MAC Address	Uptime	Action
VLAN0	☐	⏻	CW-400NAC-E1	192.168.2.253	8c:4d:ea:04:d0:6e	03:43:28	Setup

➢ **VLAN**：Select desired VLAN for AP setup

➢ **Setup**：Administrator can modify IP addresses, system login passwords, and web login port for managed APs. If administrator has change AP devices, administrator can modify MAC address of the new managed AP.

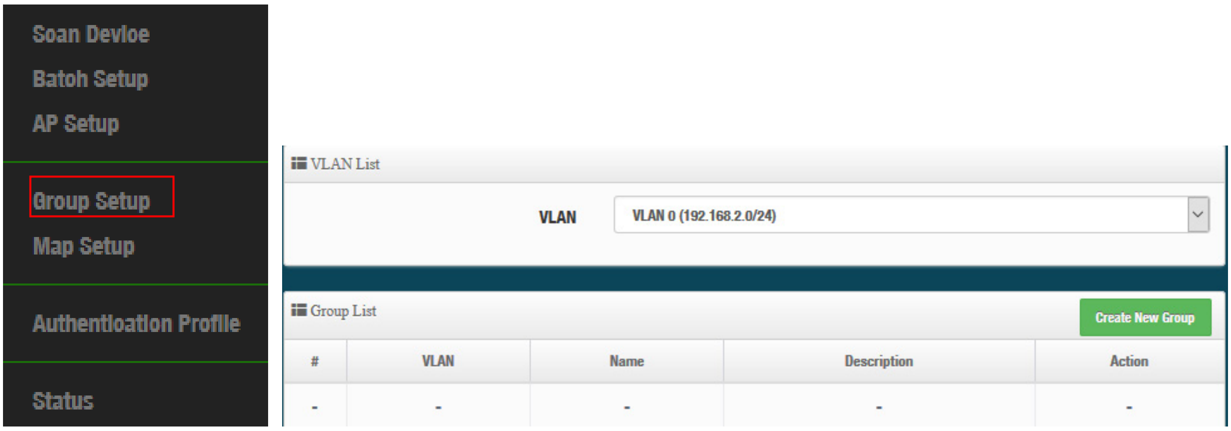


Device Setup

VLAN	VLAN 0 (192.168.2.0/24)
Group	None
IP Address	192.168.2.253
MAC Address	8c:4d:ea:04:d0:6e
Password	•••••••
HTTP Port	80 Port

4.4 Group Setup

Administrator can create Groups within the same VLAN.



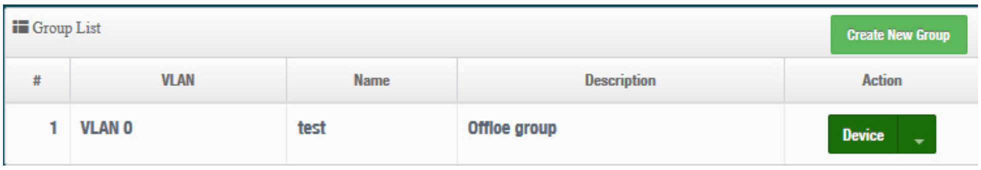
VLAN List

VLAN: VLAN 0 (192.168.2.0/24)

Group List

#	VLAN	Name	Description	Action
-	-	-	-	-

- ➢ **VLAN**：Select VLAN.
- ➢ **Create New Group**：Click the button to create a new AP Group



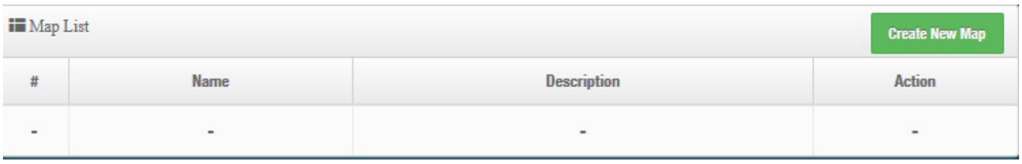
Group List

#	VLAN	Name	Description	Action
1	VLAN 0	test	Office group	Device

✓ **Device button**：Administrator can select managed APs and import them into the Group.

4.5 Map Setup

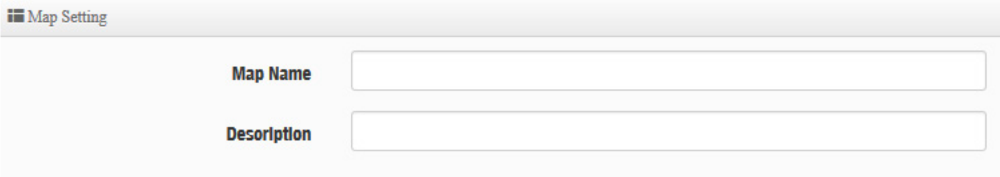
The Map Setup feature allows administrators to upload a floor plan image to DR-3000 server and then use the image to import the map into the AP user interface. Once the image is uploaded, administrators can use the Map Setup function to map out the locations of the AP network.



Map List Create New Map

#	Name	Description	Action
-	-	-	-

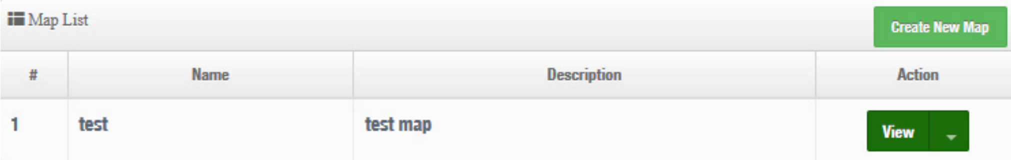
Administrator can click **"Create New Map"** button to upload Map image.



Map Setting

Map Name	
Description	

- ➢ **Map Name:** Administrator can set Map name.
- ➢ **Description:** Administrator can set description for map.

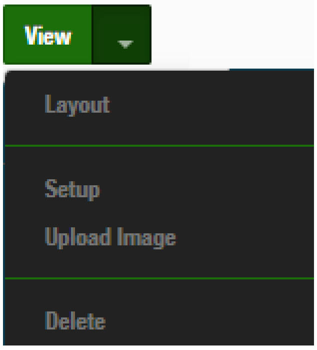


Map List Create New Map

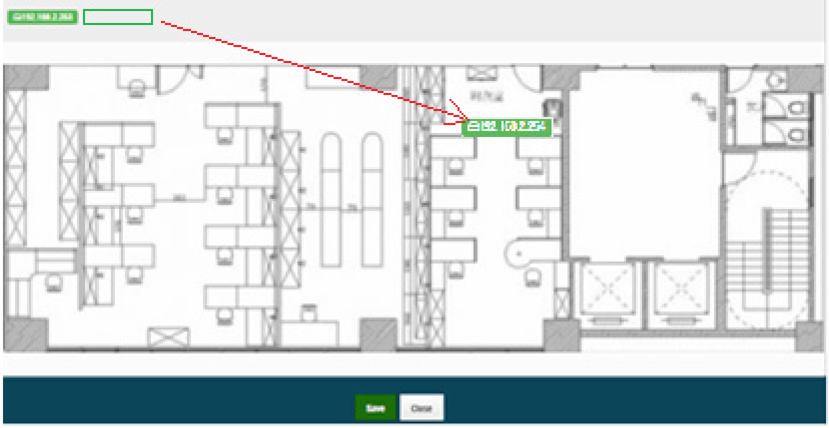
#	Name	Description	Action
1	test	test map	View

：Once the Map is created and properly in the Map List, administrators can click the "Layout" button in the action tab to map out the AP network. Managed APs will appear in the "Device List" section of the layout page. Administrators can simply drag the AP (IP Address) to the correct installation location.

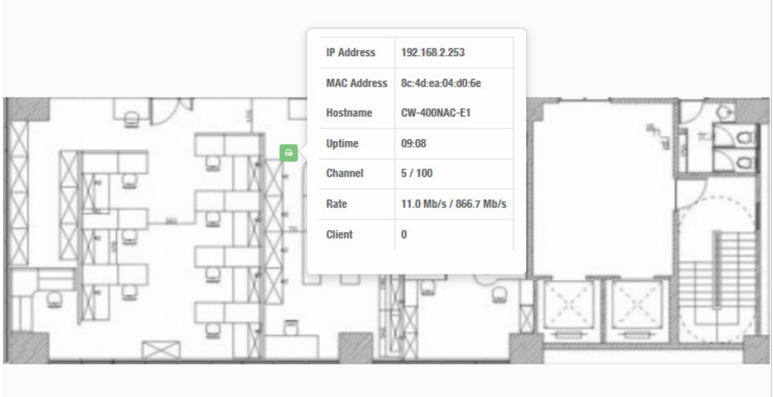
Operation sequence for View Pull-down menu



1) Administrator must first click **"Upload Image"** to upload the image.
2) Administrators can click the **"Layout"** function to map out the AP network.



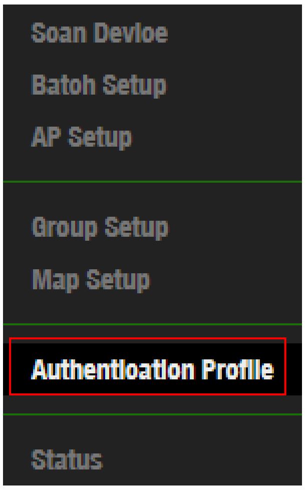
3) Once complete, administrators can click the “**View”** button to monitor AP statuses and locations.

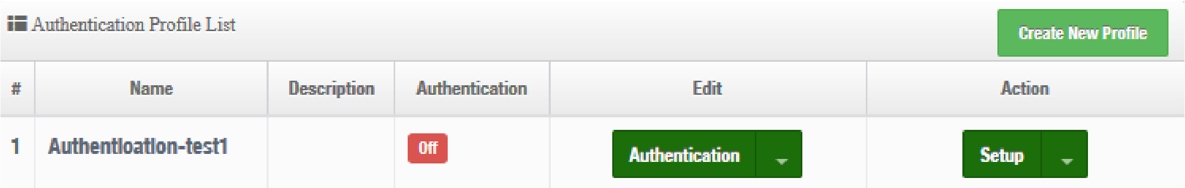


IP Address	192.168.2.253
MAC Address	8c:4d:ea:04:d0:6e
Hostname	CW-400NAC-E1
Uptime	09:08
Channel	5 / 100
Rate	11.0 Mb/s / 866.7 Mb/s
Client	0

4) If administrator must modify the description of the Map, please click “Setup” to modify.

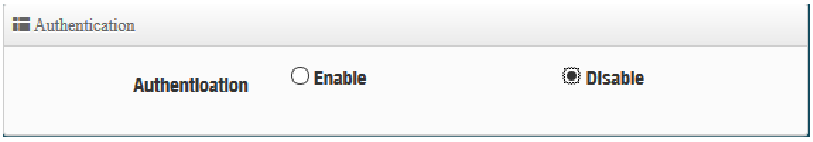
4.6 Authentication Profile





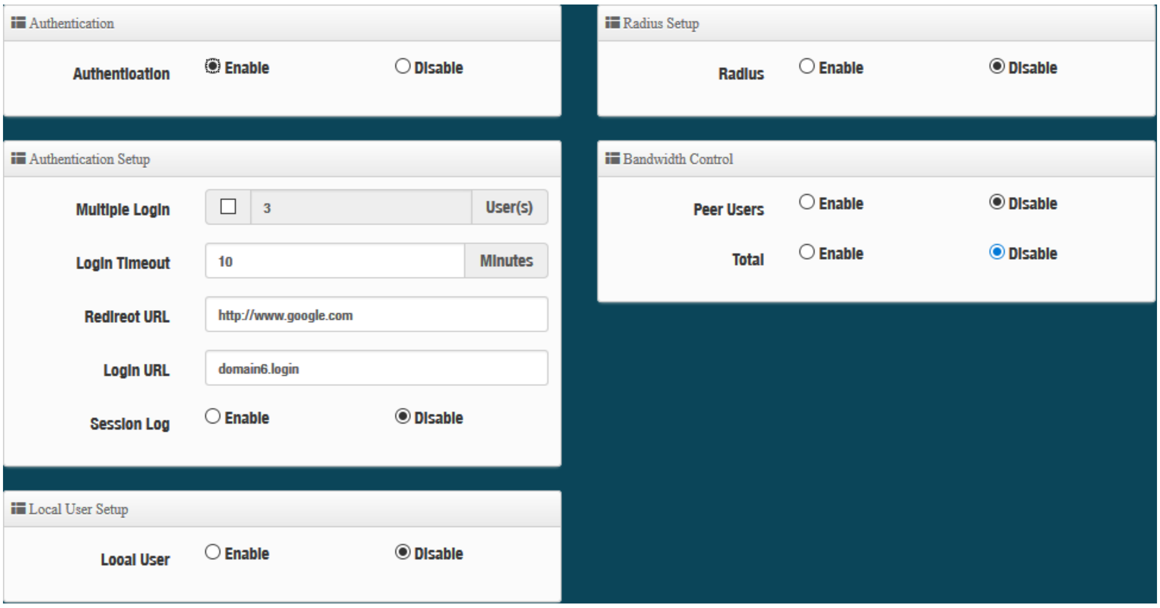
#	Name	Description	Authentication	Edit	Action
1	Authentloation-test1		Off	Authentication	Setup

- **Create New Profile：** Administrator can create authentication profile.
- **Edit：** Click the Authentication button to Enable or Disable authentication function.



Authentication

Authentloation ○ Enable ● Dlsable



Authentication

Authentication ● Enable ○ Disable

Authentication Setup

Multiple Login □ 3 User(s)

Login Timeout 10 Minutes

Redirect URL http://www.google.com

Login URL domain6.login

Session Log ○ Enable ● Disable

Local User Setup

Local User ○ Enable ● Disable

Radius Setup

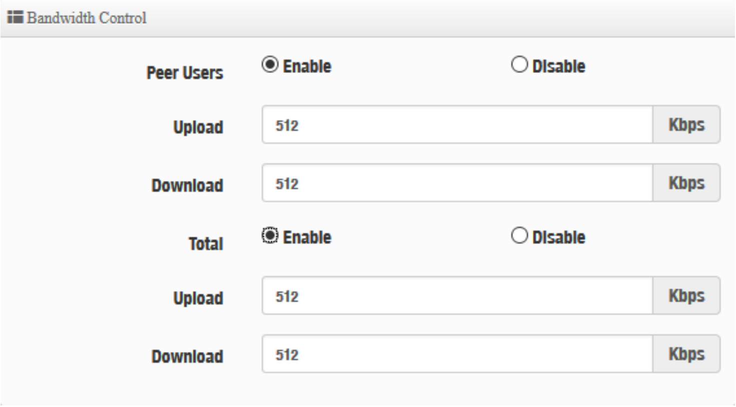
Radius ○ Enable ● Disable

Bandwidth Control

Peer Users ○ Enable ● Disable

Total ○ Enable ● Disable

- **Multiple Login：** Administrator can set one account to multiple users simultaneously login and the users can set limit.(0 = not limited)
- **Login Timeout：** After account login for some time no traffic, system will automatic timeout for account. Administrator can enter a time(Minutes).
- **Redirect URL：** After the success of the login, system will redirect to URL. Administrator can enter web site URL.
- **Login URL：** Administrator can set URL for login page.
- **Authentication / Session Log：** Administrator can start the managed APs for authentication and session Log. The managed APs account authentication and session log will copy to DR-3000 log server (Administrator must set syslog server IP address for managed APs). Log server for more details, refer to **"2.11 Log Server Setup"**.
- **Local User：** Administrator can enable authentication local user in managed AP.
- **RADIUS：** Authentication support remote RADIUS Server. Administrator can enter security information for remote RADIUS Server.
- **Bandwidth Control：** Administrator can be control traffic by Users or total.



Bandwidth Control

Peer Users ● Enable ○ Disable

Upload 512 Kbps

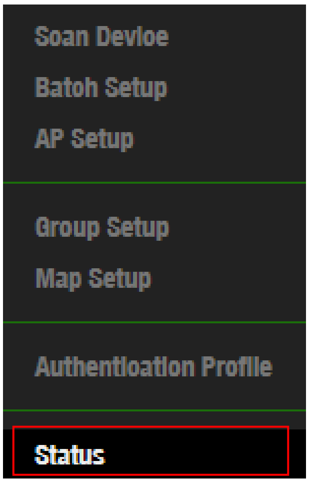
Download 512 Kbps

Total ● Enable ○ Disable

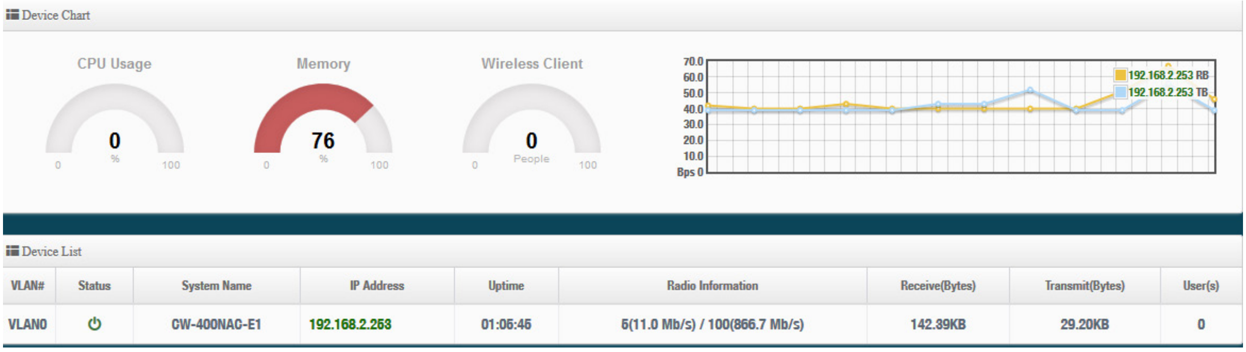
Upload 512 Kbps

Download 512 Kbps

4.7 Status



Administrator can monitor Tx/Rx flow information, show online users and check system CPU / Memory information and on/off line for the managed APs. The information data display support graphical interface.

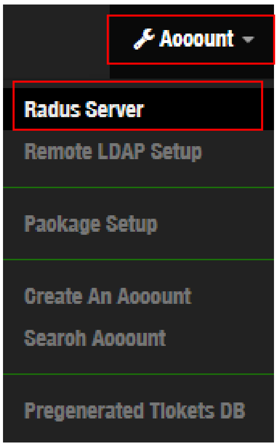


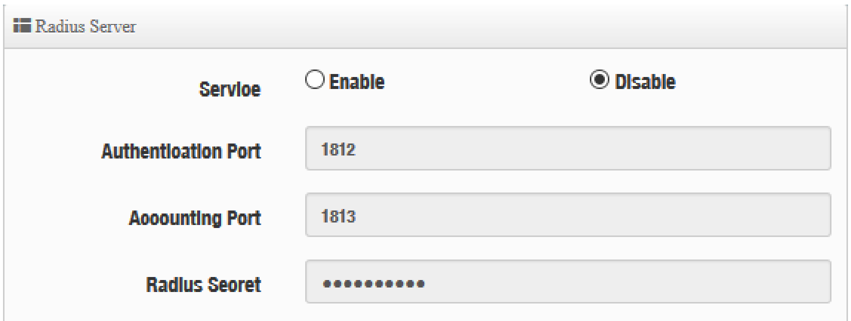
VLAN#	Status	System Name	IP Address	Uptime	Radio Information	Receive(Bytes)	Transmit(Bytes)	User(s)
VLAN0	⏻	CW-400NAC-E1	192.168.2.253	01:06:45	5(11.0 Mb/s) / 100(866.7 Mb/s)	142.39KB	29.20KB	0

5. Account

This function is a RADIUS server, and allows managed Cerio APs to utilize the RADIUS server authentication of DR-3000, and its many authentication types. When managed Cerio APs enable authentication through external RADIUS server, administrators must first set the IP address of DR-3000 in each managed access point to properly redirect authentication clients.
Cerio’s DR-3000 Account functions support Package, Pregenerated Tickets and remote LDAP(AD) authentication type.

5.1 RADIUS Server





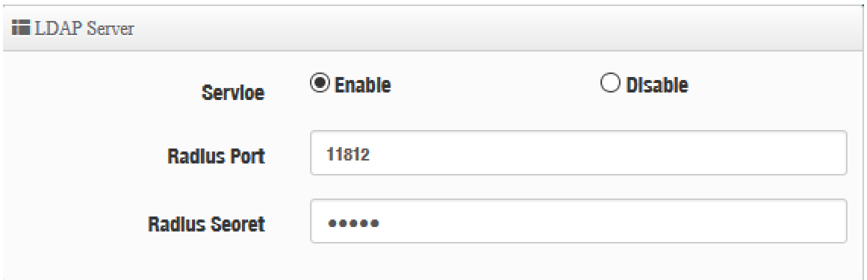
Radius Server

Service	○ Enable ● Disable
Authentication Port	1812
Accounting Port	1813
Radius Secret	••••••••••

- **Service:** Administrator can select Enable or Disable the RADIUS Server.
- **Authentication Port:** Administrator can set authentication port for RADIUS Server, the default port is 1812.
- **Accounting Port:** Administrator can set accounting port for RADIUS Server, the default port is 1813.
- **Radius Secret:** Administrator can set password (Secret key) for RADIUS Server.

5.2 Remote LDAP Setup

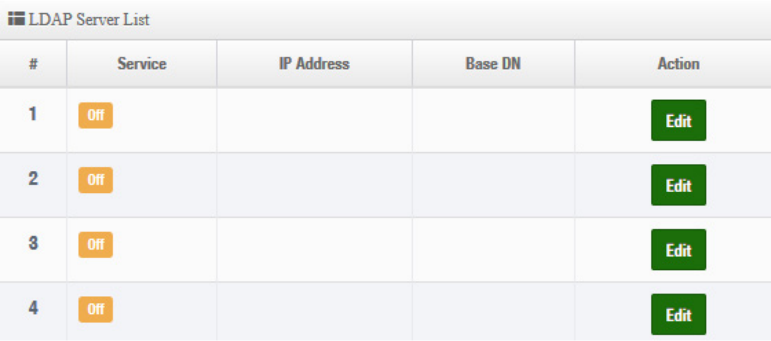
Remote LDAP Setup enables Remote LDAP authentication for managed access points. Administrators wishing to enable Remote LDAP authentication must copy and paste DR-3000’s LDAP Server **“RADIUS Port”** number into the managed APs “Authentication Port” box, which is found in the managed Cerio APs **“Radius Setup”** window.
Administrator can set up 4 remote LDAP Server.



LDAP Server

Service	● Enable ○ Disable
Radius Port	11812
Radius Secret	•••••

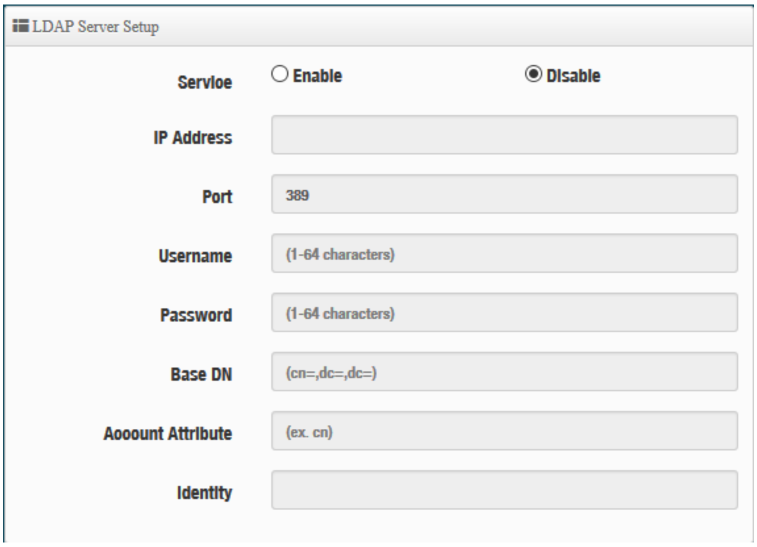
- **Service:** Administrator can select Enable or Disable the authentication function.
- **Radius Port:** Administrators can set the Radius server port of the DR-3000 to provide Cerio managed APs links. If Cerio managed APs set this Radius Port will can use remote LDAP(AD) type to authentication.
- **Radius Secret:** Administrator can set password (Secret key) for RADIUS Server.



LDAP Server List

#	Service	IP Address	Base DN	Action
1	Off			Edit
2	Off			Edit
3	Off			Edit
4	Off			Edit

- **Edit:** Administrator can click Edit to set remote LDAP Server information.



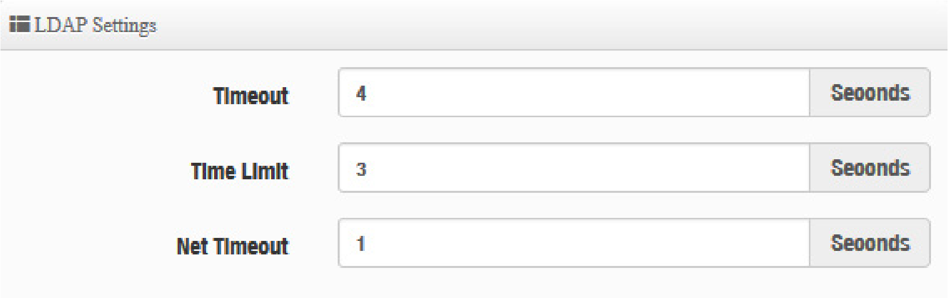
LDAP Server Setup

Service	○ Enable ● Disable
IP Address	
Port	389
Username	(1-64 characters)
Password	(1-64 characters)
Base DN	(cn=,dc=,dc=)
Account Attribute	(ex. cn)
Identity	

- **Service:** Administrator can select Enable or Disable the function.
- **IP Address:** Set IP address for remote LDAP(AD) server.
- **Port:** Set Port for remote LDAP(AD) server.
- **Username:** Set login account for remote LDAP(AD) server.
- **Password:** Set login account use password for remote LDAP(AD) server.
- **Base DN:** Set Base DN path for remote LDAP(AD) server.
- **Account Attribute:** Set LDAP cn account for remote LDAP(AD) server.

LDAP Setting

Administrator can set remote LDAP(AD) timeout.

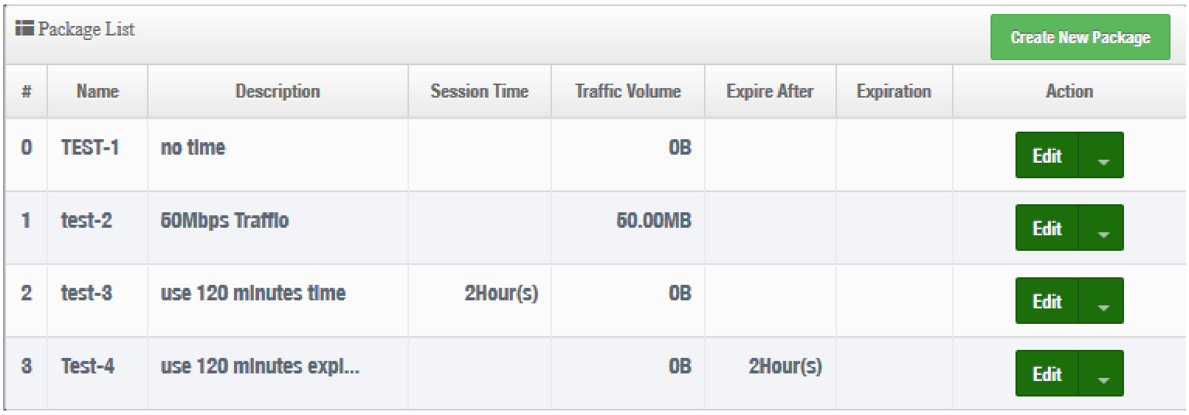


LDAP Settings

Timeout	4	Seconds
Time Limit	3	Seconds
Net Timeout	1	Seconds

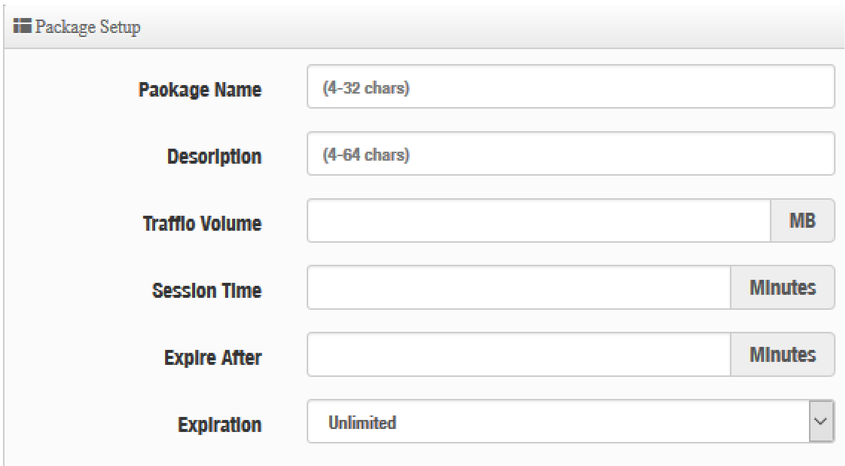
5.3 Package Setup

Administrator can set internet time rules for package authentication type.



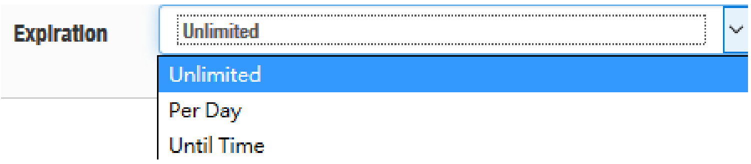
#	Name	Description	Session Time	Traffic Volume	Expire After	Expiration	Action
0	TEST-1	no time		0B			Edit
1	test-2	50Mbps Traffic		50.00MB			Edit
2	test-3	use 120 minutes time	2Hour(s)	0B			Edit
3	Test-4	use 120 minutes expi...		0B	2Hour(s)		Edit

- **Create New Package:** Administrator can click **"Create New Package"** button to set package rules.
- **# :** Package list (0~9) is Network control server (SP-800) code, administrator can choose code to print account.



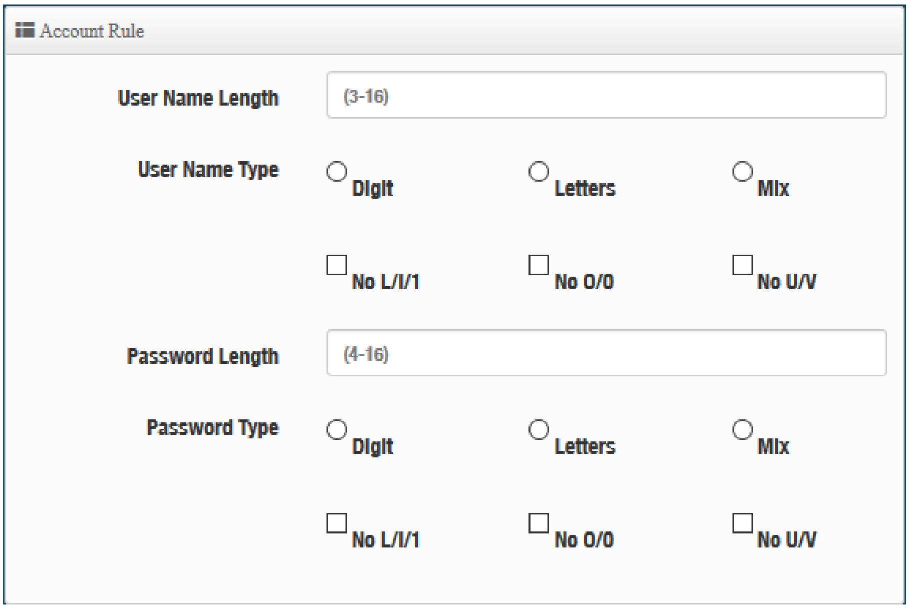
Package Name	(4-32 chars)
Description	(4-64 chars)
Traffic Volume	MB
Session Time	Minutes
Expire After	Minutes
Expiration	Unlimited

- **Package Name:** Administrator can set Identify name for the package rules.
- **Description**: Administrator can set the description for package rules.
- **Traffic Volume:** Administrator can set authentication account use traffic limit for the package rules.
- **Session Time:** Administrator can set authentication account use session limit for the package rules. (After the account is signed in, the system will begin counting until the set time is used up. The counting will stop when users log out, and begin counting again once the user signs back in.)
- **Expire After:** Administrator can set authentication account use how many hours expire.(After the account is signed in, the system start counted time until the end time.)
- **Expiration**: Administrator can select Unlimited or Per Day or Until Time.



Expiration: Unlimited

- ✓ **Unlimited:** After the account is signed in, the system does not count the time
- ✓ **Per Day:** After the account is signed in, the system start counted time until the end time.
- ✓ **Until Time**: After the account is signed in, the system will begin counting until the set time is used up. The counting will stop when users log out, and begin counting again once the user signs back in.



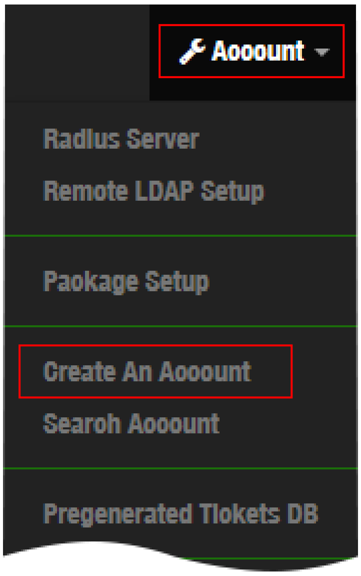
Account Rule

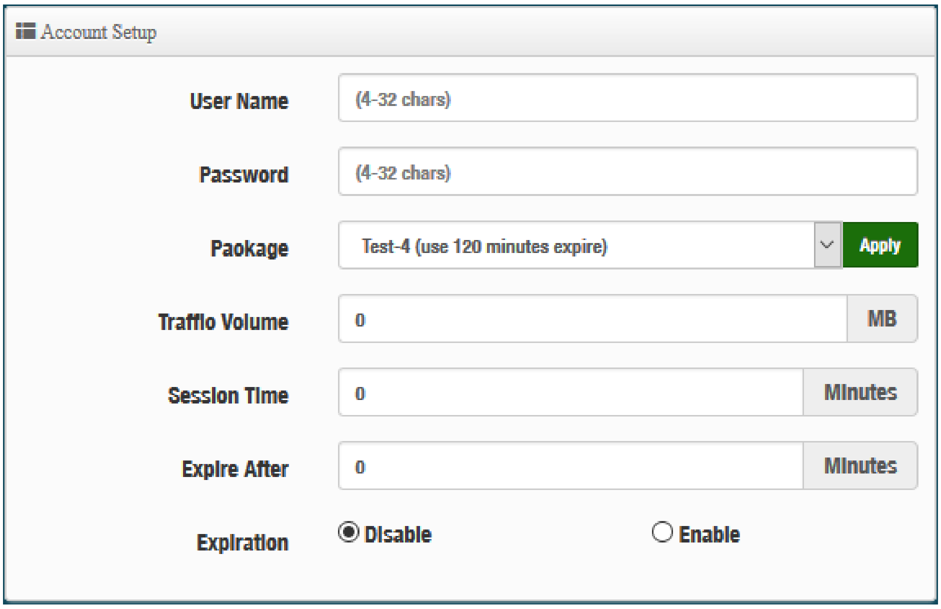
User Name Length	(3-16)		
User Name Type	○ Digit	○ Letters	○ Mix
	□ No L/l/1	□ No O/0	□ No U/V
Password Length	(4-16)		
Password Type	○ Digit	○ Letters	○ Mix
	□ No L/l/1	□ No O/0	□ No U/V

- ➢ **User Name Length:** Administrator can set account length limit for package rules.
- ➢ **User Name Type:** Administrator can create account use digit or Letters or Mix for package rules. If administrator select Letters or Mix can filter L/l/digit 1 and O/ digit 0 and U/V for letters and Mix.
- ➢ **Password Length:** Administrator can set password length limit for account.
- ➢ **Password Type:** Administrator can set password use digit or Letters or Mix for account. If administrator select Letters or Mix can filter L/l/digit 1 and O/ digit 0 and U/V for letters and Mix.

5.4 Create An Account

Administrator can set and create an account of validity for the RADIUS Server.
Please click **"Account"➔"Create an account"**

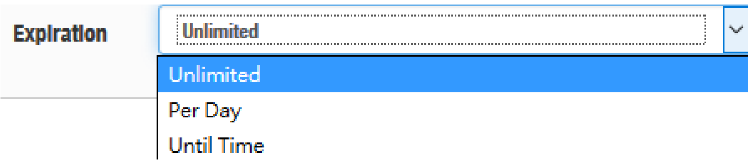



Account Setup

User Name	(4-32 chars)
Password	(4-32 chars)
Package	Test-4 (use 120 minutes expire) Apply
Traffic Volume	0 MB
Session Time	0 Minutes
Expire After	0 Minutes
Expiration	● Disable ○ Enable

- **User Name**：Administrator can set an account for RADIUS Server.
- **Password**：Enter Password for user name account.
- **Package:** Administrator can choose apply mechanically Package function policy.
- **Traffic Volume:** Administrator can set authentication account use traffic limit for the package rules.
- **Session Time:** Administrator can set authentication account use session limit for the package rules. (After the account is signed in, the system will begin counting until the set time is used up. The counting will stop when users log out, and begin counting again once the user signs back in.)

- **Expire After:** Administrator can set authentication account use how many hours expire.(After the account is signed in, the system start counted time until the end time.)
- **Expiration**: Administrator can select Unlimited or Per Day or Until Time.



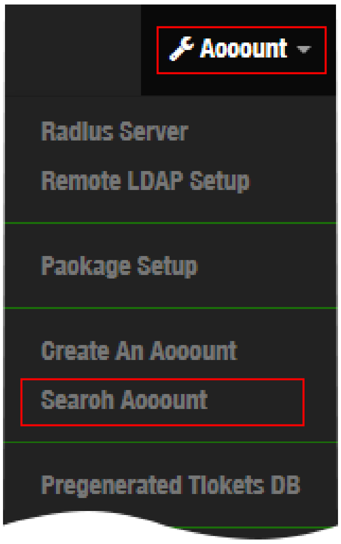
Expiration: Unlimited

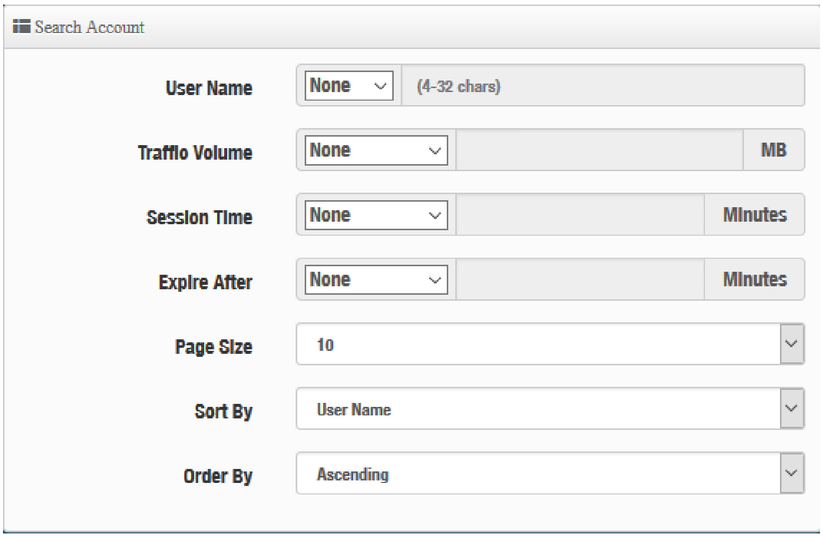
- **Unlimited:** After the account is signed in, the system does not count the time
- **Per Day:** After the account is signed in, the system start counted time until the end time.
- **Until Time**: After the account is signed in, the system will begin counting until the set time is used up. The counting will stop when users log out, and begin counting again once the user signs back in.

5.5 Search Account

Administrator can search all account in the databases. The search function built-in smart-search engine, administrator can set want to query account the conditions.

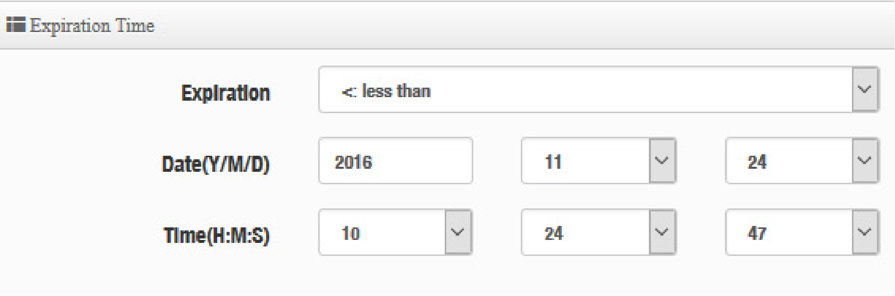
Please click **“Account”→”Search Account”**





Search Account

User Name	None	(4-32 chars)	
Traffic Volume	None		MB
Session Time	None		Minutes
Expire After	None		Minutes
Page Size	10		
Sort By	User Name		
Order By	Ascending		



Expiration Time

Expiration	<: less than		
Date(Y/M/D)	2016	11	24
Time(H:M:S)	10	24	47

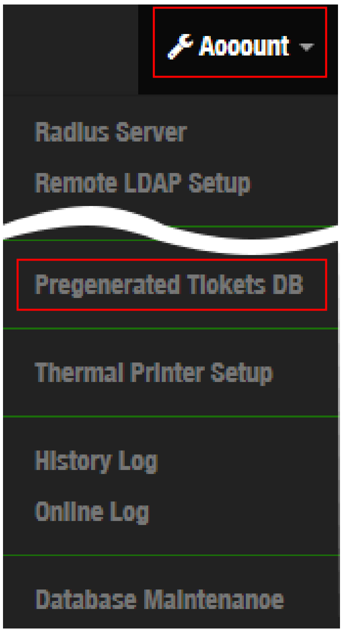
Administrators can choose different data type in the search engines.

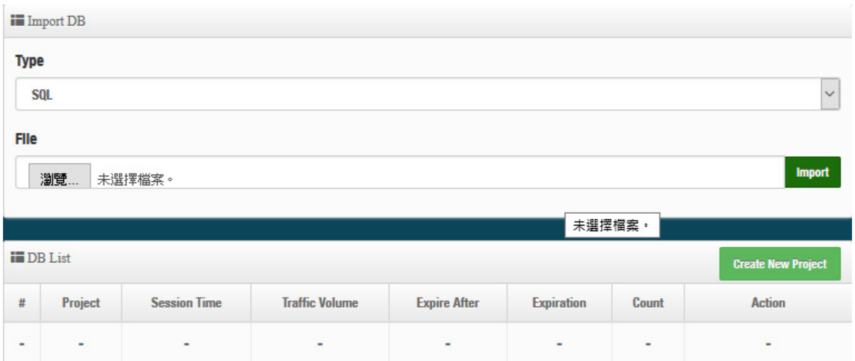
- **None:** The program doesn't judge characters, search all the information
- **Greater then:** Search values for greater than
- **Equal:** Search values for equal.
- **Less then:** Search values for less then.
- **Between:** Search values for between.
- **Like:** Search similar strings.

5.6 Pregenerated Tickets DB

Administrators can use system auto create accounts in a databases.

Please click **"Account"➔"Pregenerated Tickets DB"** to create databases.





Import DB

Type: SQL

File: 瀏覽... 未選擇檔案。 Import

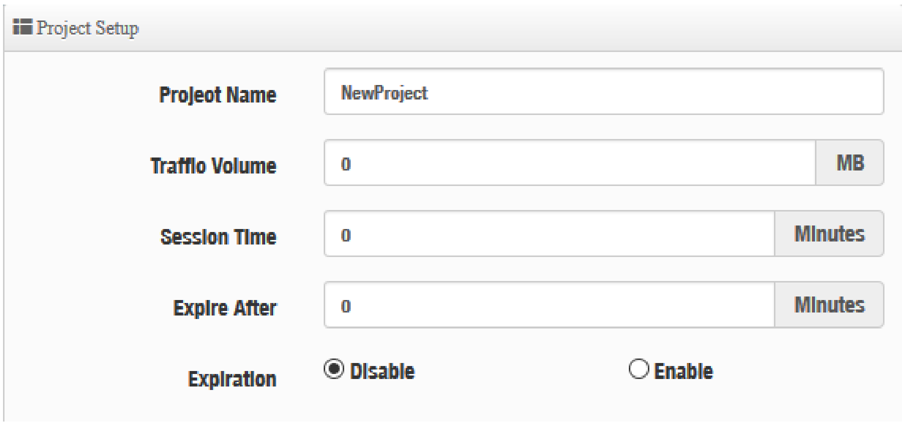
未選擇檔案。

DB List

Create New Project

#	Project	Session Time	Traffic Volume	Expire After	Expiration	Count	Action
-	-	-	-	-	-	-	-

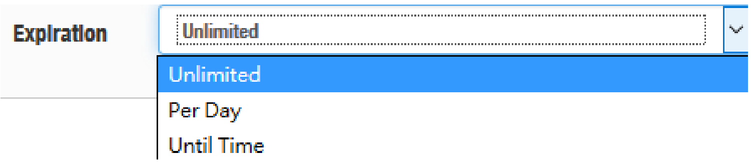
Administrator can click Create New Project to set function.



Project Setup

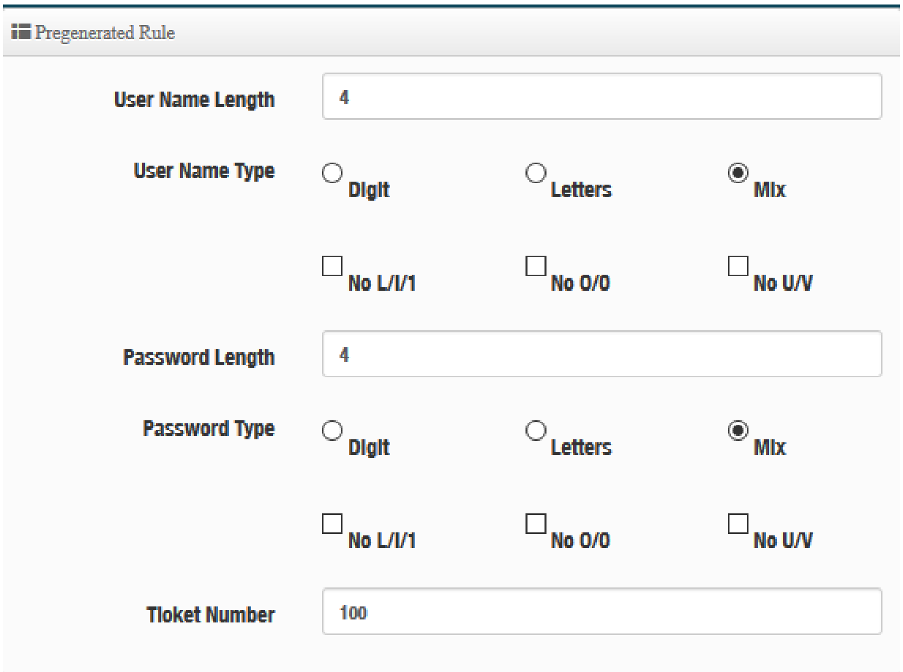
Projeot Name	NewProject	
Traffio Volume	0	MB
Sesslon Tlme	0	Mlnutes
Explre After	0	Mlnutes
Explratlon	● Dlsable	○ Enable

- **Project Nama:** Administrator can set a Databases name.
- **Traffic Volume:** Administrator can set authentication account use traffic limit for the package rules.
- **Session Time:** Administrator can set authentication account use session limit for the package rules. (After the account is signed in, the system will begin counting until the set time is used up. The counting will stop when users log out, and begin counting again once the user signs back in.)
- **Expire After:** Administrator can set authentication account use how many hours expire.(After the account is signed in, the system start counted time until the end time.)
- **Expiration**: Administrator can select Unlimited or Per Day or Until Time.



Explratlon: Unlimited

- **Unlimited:** After the account is signed in, the system does not count the time
- **Per Day:** After the account is signed in, the system start counted time until the end time.
- **Until Time**: After the account is signed in, the system will begin counting until the set time is used up. The counting will stop when users log out, and begin counting again once the user signs back in.



Pregenerated Rule

User Name Length	4		
User Name Type	○ Digit	○ Letters	● Mix
	□ No L/l/1	□ No O/0	□ No U/V
Password Length	4		
Password Type	○ Digit	○ Letters	● Mix
	□ No L/l/1	□ No O/0	□ No U/V
Ticket Number	100		

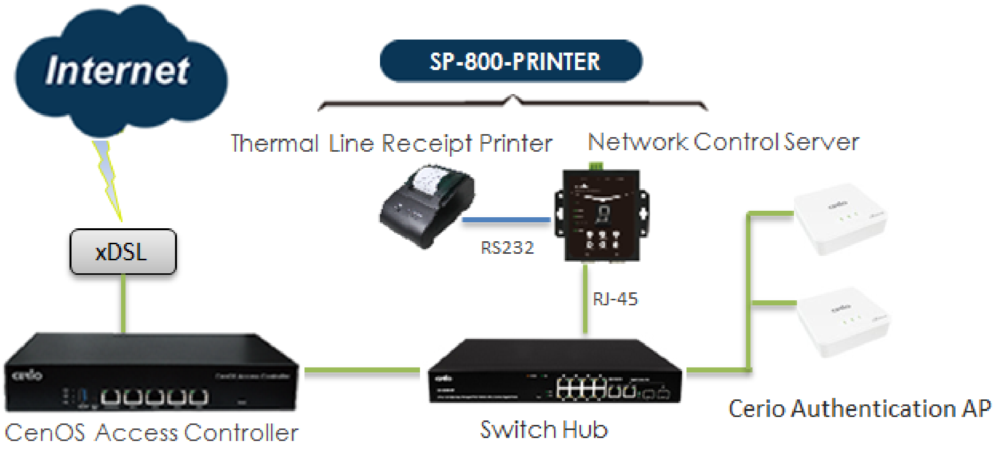
- **User Name Length:** Administrator can set account length limit for package rules.
- **User Name Type:** Administrator can create account use digit or Letters or Mix for package rules. If administrator select Letters or Mix can filter L/l/digit 1 and O/ digit 0 and U/V for letters and Mix.
- **Password Length:** Administrator can set password length limit for account.
- **Password Type:** Administrator can set password use digit or Letters or Mix for account. If administrator select Letters or Mix can filter L/l/digit 1 and O/ digit 0 and U/V for letters and Mix.
- **Ticket Number:** Administrator can set number in the databases, the system will auto create accounts.

5.7 Thermal Printer Setup

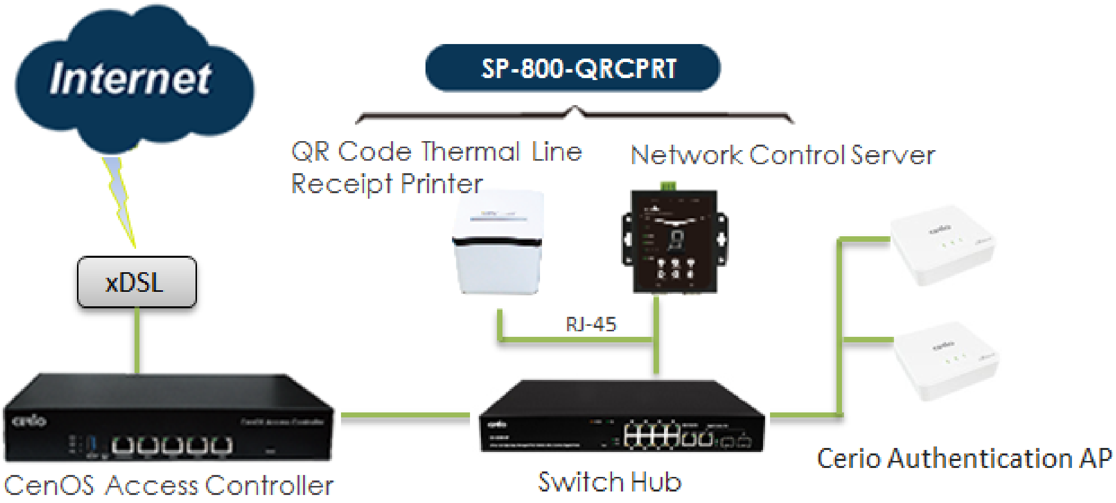
The function must match Account Ticket Generator POS System for Cerio's SP-800-PRINTER / SP-800-QRCPRT.

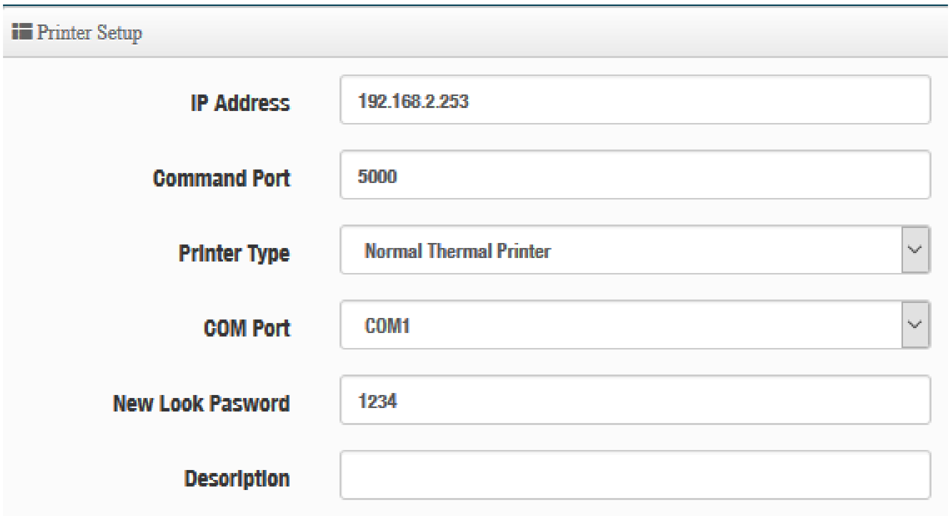
Application architecture is as follows.

# Match SP-800-PRINTER



# Match SP-800-QRCPRT




Printer Setup

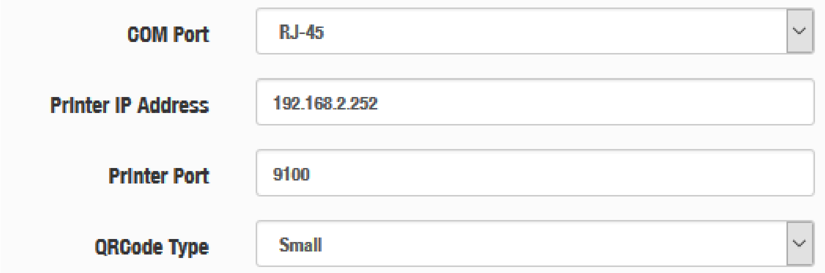
IP Address	192.168.2.253
Command Port	5000
Printer Type	Normal Thermal Printer
COM Port	COM1
New Look Pasword	1234
Description	

- **IP Address:** Please set IP address for Network control server (SP-800)
- Command Port: Enter command port for Network control server (SP-800)
- **Printer Type:** Administrator can select Normal Thermal Printer or QR Code Thermal Printer.

- ● **Normal Thermal Printer:** If use Cerio's SP-800-PRINTER POS system, administrator can select Normal Thermal Printer function.
- ● **QR Code Thermal Printer:** If use Cerio's SP-800-QRCPRT POS system, administrator can select QR Code Thermal Printer function.

➢ **COM Port:** Administrator can select connected COM1/2 or RJ-45 for Printer Port.

- ● **RJ-45:** If printer type selected QR Code Thermal Printer, administrator can select use RJ-45 and set Printer IP address.



COM Port	RJ-45
Printer IP Address	192.168.2.252
Printer Port	9100
QRCode Type	Small

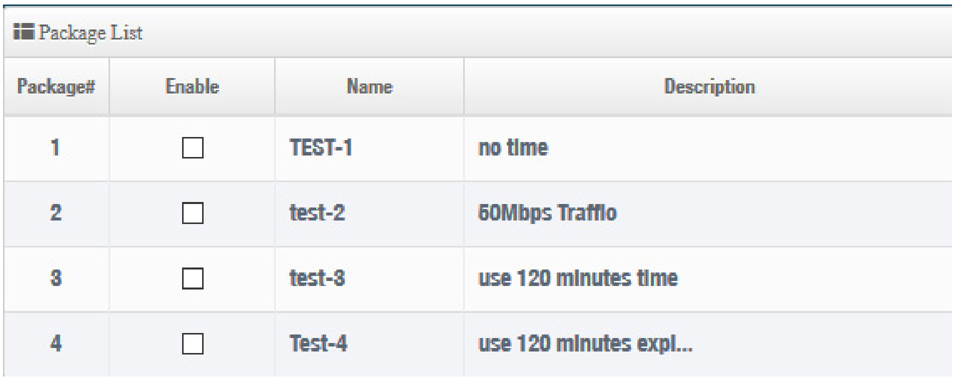
- ✓ **Printer IP Address:** Administrator can set IP address for QR code Printer.
- ✓ **Printer Port:** Administrator can set Port for QR code Printer. The default Port is 9100 for Cerio's SP-800-QRCPRT
- ✓ **QR Code Type:** Administrator can select print QR Code size or close.

➢ **New Look Password:** The password is Network control server(SP-800) connect to DR-3000 use key lock. Administrator can change password, default password is 1234

➢ **Description:** Administrator can enter Description.

# Package List

Print tickets account must have created Package; administrator can refer to "4.3 Package Setup" description.



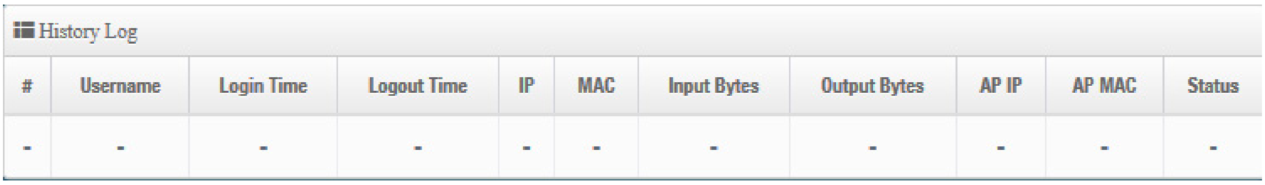
Package List

Package#	Enable	Name	Description
1	□	TEST-1	no time
2	□	test-2	50Mbps Traffic
3	□	test-3	use 120 minutes time
4	□	Test-4	use 120 minutes expi...

Administrator can choose box to enable Packages rule.

5.8 History Log

The Page can display account login/logout information.



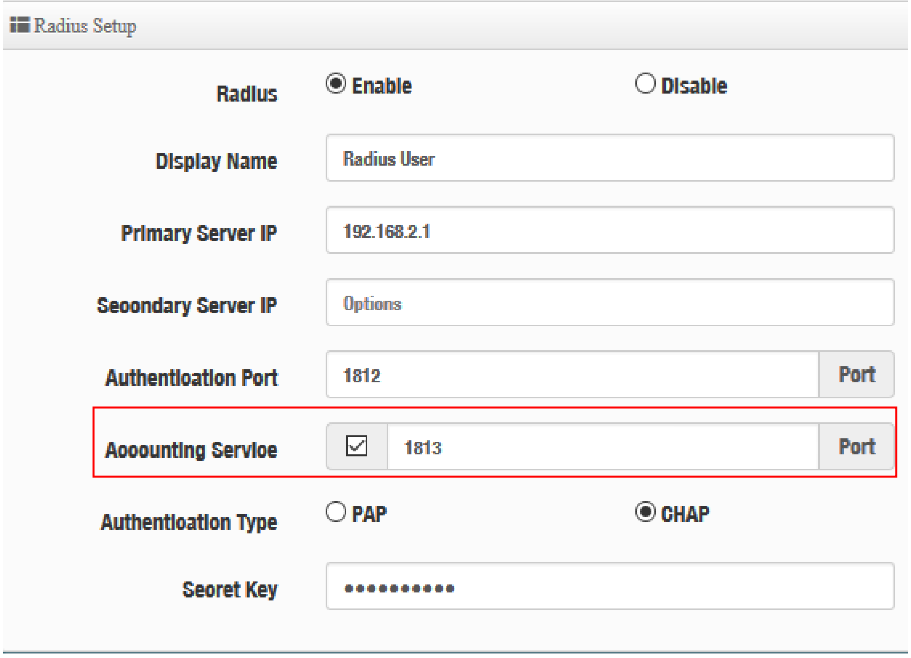
History Log

#	Username	Login Time	Logout Time	IP	MAC	Input Bytes	Output Bytes	AP IP	AP MAC	Status
-	-	-	-	-	-	-	-	-	-	-

5.9 Online Log

The Page can display online user information. The online user information must match Cerio's AP's; Administrator must enable RADIUS Accounting Port 1813 in the Cerio's AP's, as follows

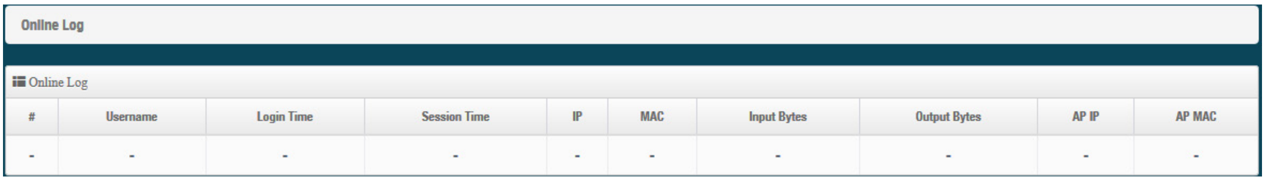
# Cerio's APs for CenOS5.0 interface



Radius Setup

Radius	● Enable	○ Disable
Display Name	Radius User	
Primary Server IP	192.168.2.1	
Seoondary Server IP	Options	
Authentioation Port	1812	Port
Aooounting Servioe	☑ 1813	Port
Authentioation Type	○ PAP	● CHAP
Seoret Key	●●●●●●●●●●●	

# DR-3000 online Log page



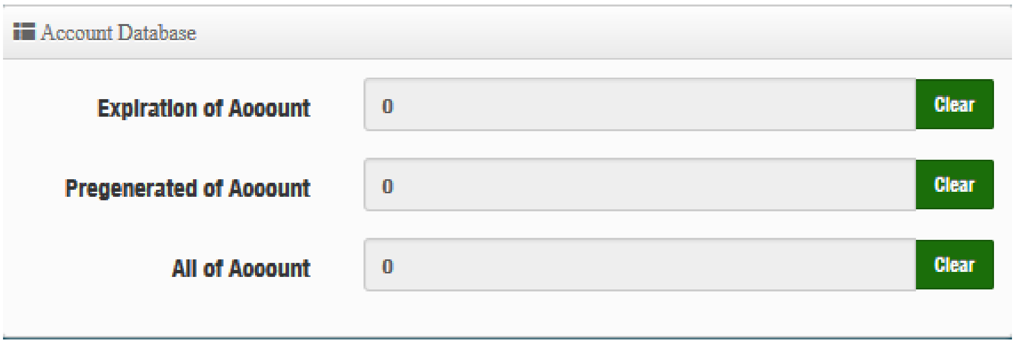
Online Log

Online Log

#	Username	Login Time	Session Time	IP	MAC	Input Bytes	Output Bytes	AP IP	AP MAC
-	-	-	-	-	-	-	-	-	-

5.10 Database Maintenance

Administrator can clear account for Expiration / Pregenerated / All databases.



Account Database

Expiration of Account	0	Clear
Pregenerated of Account	0	Clear
All of Account	0	Clear

Notice — Administrator click "Clear" button, the databases all account will be deleted.

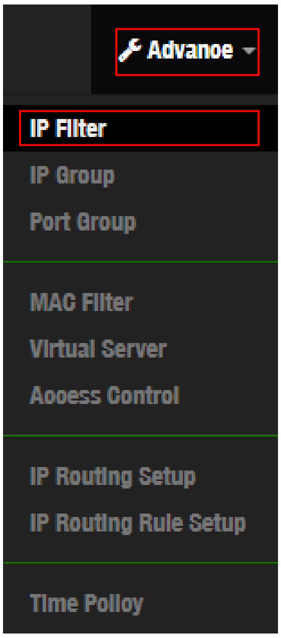
6. Advance

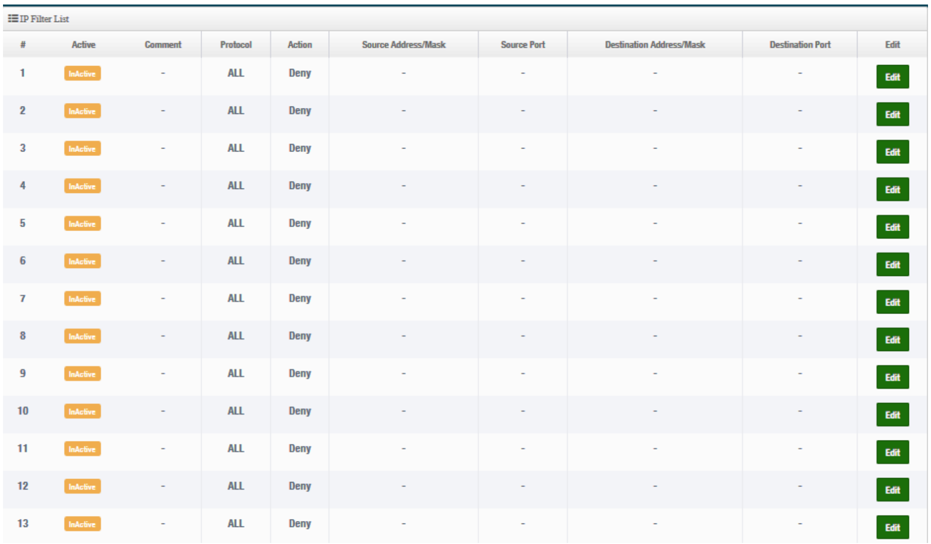
6.1 IP Filter

Can allow or deny filter ingress or egress packets from specific source and/or to destination IP address on wired (LAN) or Wireless (WAN) ports. Filter rules support IP/ Port Groups, could be used to filter unicast or multicast packets on different protocols as shown in the IP Filter Setup. Important to note that IP filter rules has precedence over Access control rules.

Administrator can set IP Filter rules: 64

Please click **"Advance"** ➔ **"IP Filter"** setup.

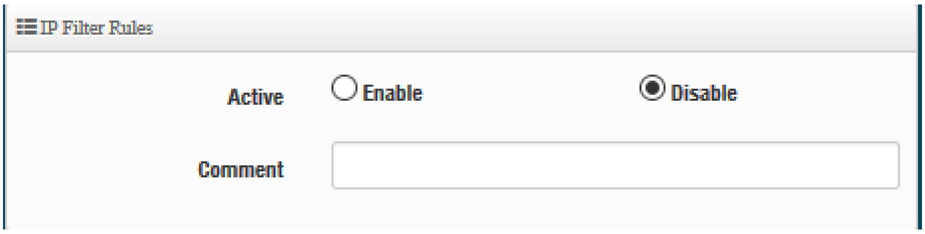




IP Filter List

#	Active	Comment	Protocol	Action	Source Address/Mask	Source Port	Destination Address/Mask	Destination Port	Edit
1	InActive	-	ALL	Deny	-	-	-	-	Edit
2	InActive	-	ALL	Deny	-	-	-	-	Edit
3	InActive	-	ALL	Deny	-	-	-	-	Edit
4	InActive	-	ALL	Deny	-	-	-	-	Edit
5	InActive	-	ALL	Deny	-	-	-	-	Edit
6	InActive	-	ALL	Deny	-	-	-	-	Edit
7	InActive	-	ALL	Deny	-	-	-	-	Edit
8	InActive	-	ALL	Deny	-	-	-	-	Edit
9	InActive	-	ALL	Deny	-	-	-	-	Edit
10	InActive	-	ALL	Deny	-	-	-	-	Edit
11	InActive	-	ALL	Deny	-	-	-	-	Edit
12	InActive	-	ALL	Deny	-	-	-	-	Edit
13	InActive	-	ALL	Deny	-	-	-	-	Edit

- Please click **Edit** button to setting IP filter.



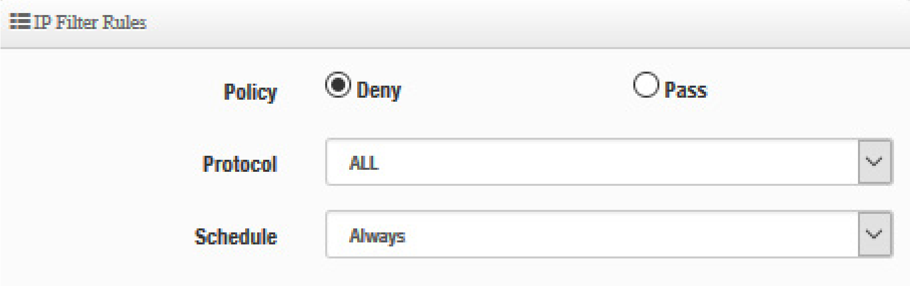
IP Filter Rules

Active ○ Enable ● Disable

Comment

- **Active:** Administrator can selected Enable or Disable for the IP filter rules function.
- **Comment:** Enter rule description.

IP Filter Rules



IP Filter Rules

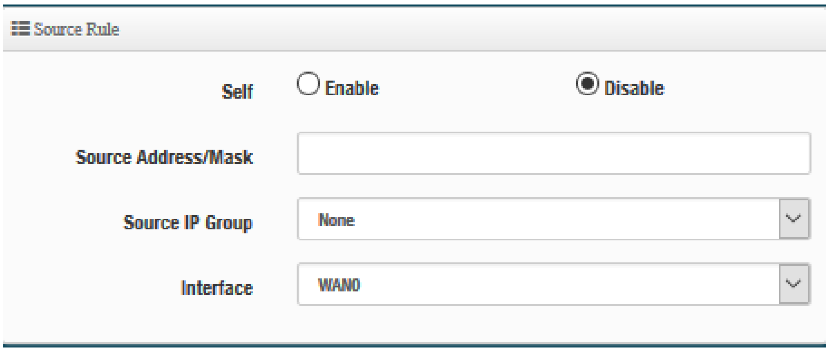
Policy ● Deny ○ Pass

Protocol ALL

Schedule Always

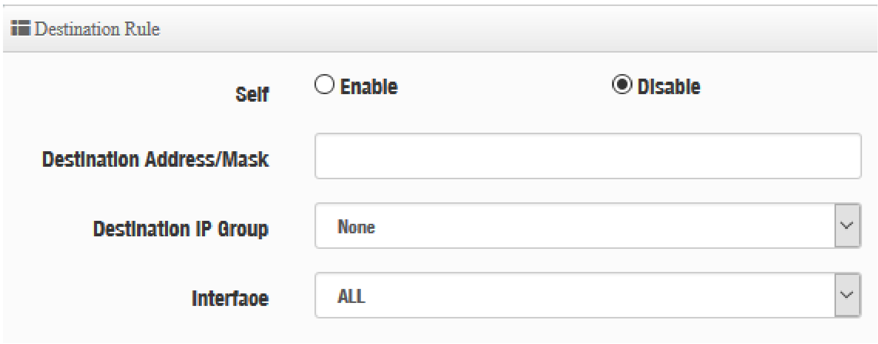
- **Policy:** Administrator can select Deny or Pass for IP filter rules.
- **Protocol:** Administrator can select type for IP protocol.
- **Schedule:** Can choose to use rule by “**Time Policy**”.

Source Rule


Source Rule

Self	○ Enable	● Disable
Source Address/Mask		
Source IP Group	None	
Interface	WAN0	

- **Self:** Administrator can choose Enable or Disable, if administrator select Enable, the source is self.
- **Source Address/Mask:** Administrator can set IP address and Mask for source.
- **Source IP Group:** Administrator can select belonging to group for IP Address.
- **Interface:** Administrator can select interface for source.

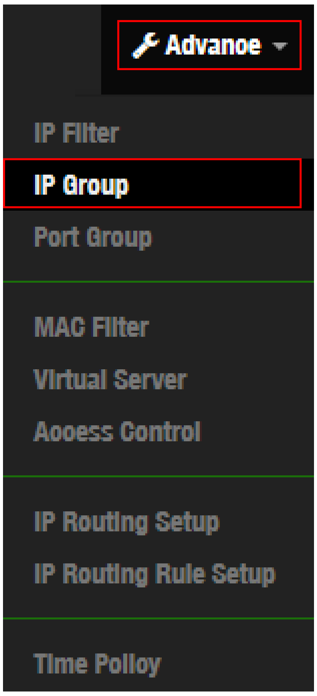

Destination Rule

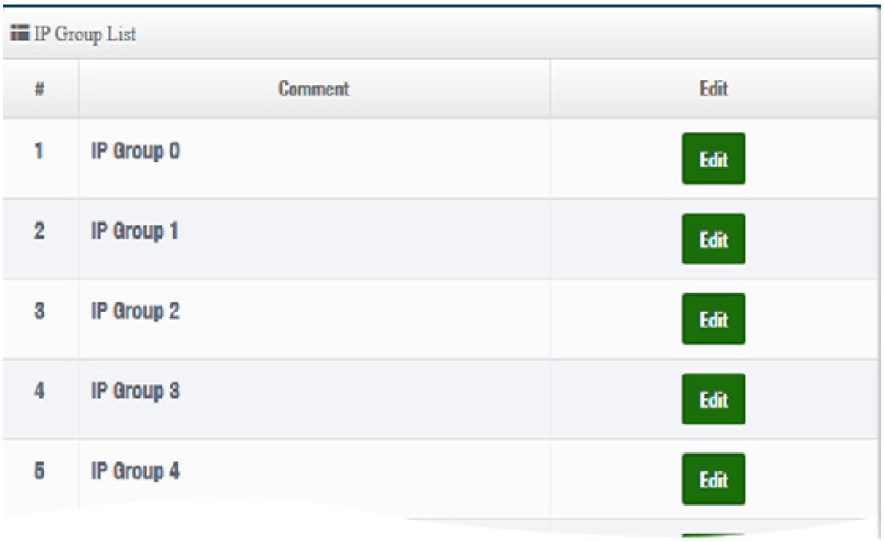
Self	○ Enable	● Disable
Destination Address/Mask		
Destination IP Group	None	
Interfaoe	ALL	

- **Self:** Administrator can choose Enable or Disable, if administrator select Enable, the source is self.
- **Destination Address/Mask:** Administrator can set IP address and Mask for destination.
- **Destination IP Group:** Administrator can select belonging to group for IP Address.
- **Interface:** Administrator can select interface for destination.

6.2 IP Group

Administrator can create IP group for IP address range or subnet.

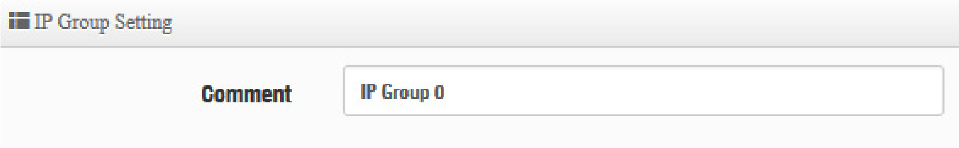




IP Group List

#	Comment	Edit
1	IP Group 0	Edit
2	IP Group 1	Edit
3	IP Group 2	Edit
4	IP Group 3	Edit
5	IP Group 4	Edit

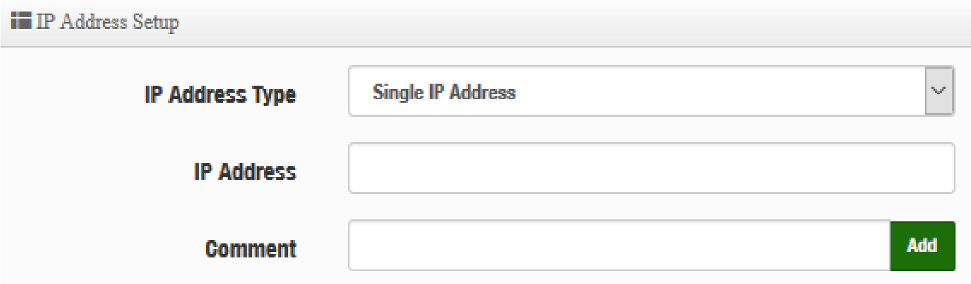
Please click "**Edit**" button to create new IP Groups.



IP Group Setting

Comment: IP Group 0

- **Comment:** Enter IP Group description.



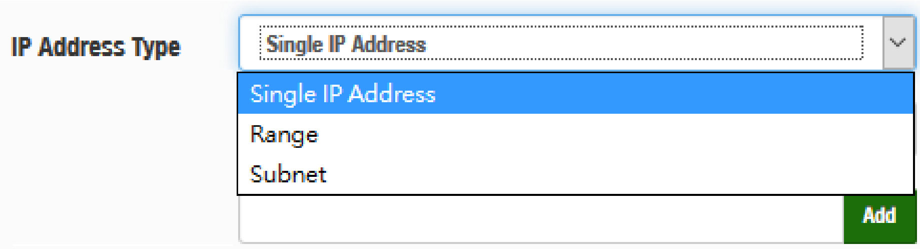
IP Address Setup

IP Address Type: Single IP Address

IP Address:

Comment:

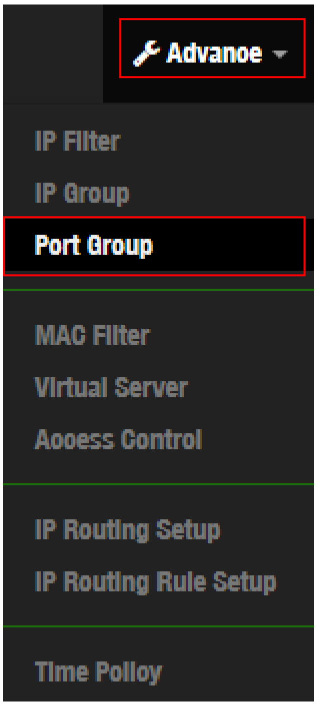
- **IP Address Type:** Administrator can select single / range / subnet type to set IP Address.

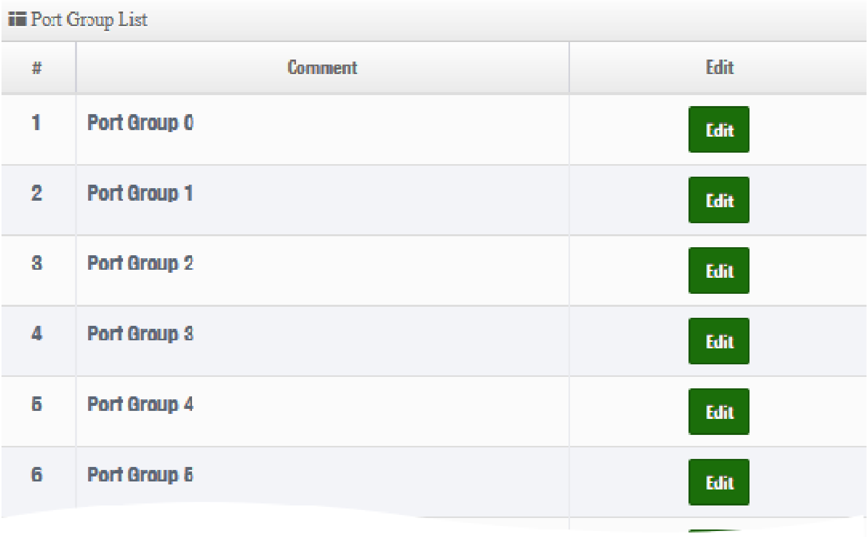


- **Single IP Address:** Enter single IP Address.
- **Range:** Enter start / end IP address.
- **Subnet:** Enter Net/MasK.

6.3 Port Group

Administrator can create Port group

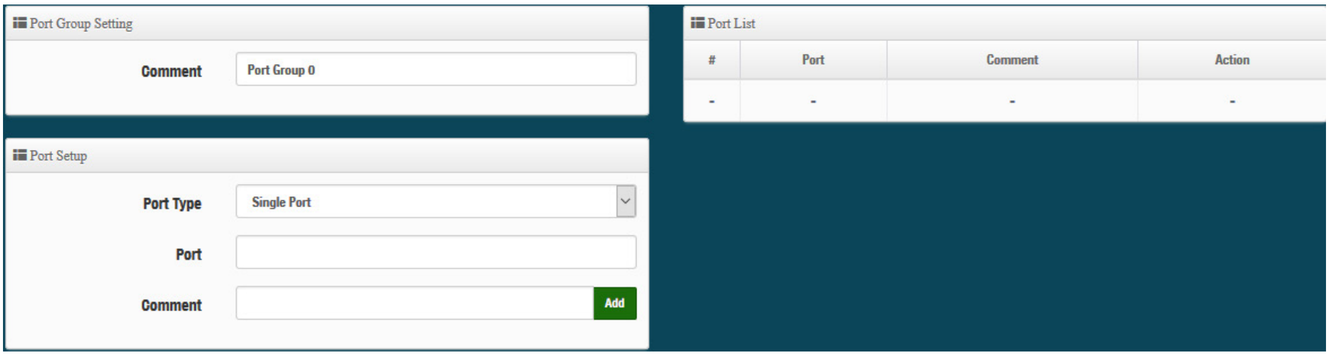



Port Group List

#	Comment	Edit
1	Port Group 0	Edit
2	Port Group 1	Edit
3	Port Group 2	Edit
4	Port Group 3	Edit
5	Port Group 4	Edit
6	Port Group 5	Edit

.

Please click "**Edit**" button to create new Port Groups.


Port Group Setting

Comment: Port Group 0

Port Setup

Port Type: Single Port

Port:

Comment: Add

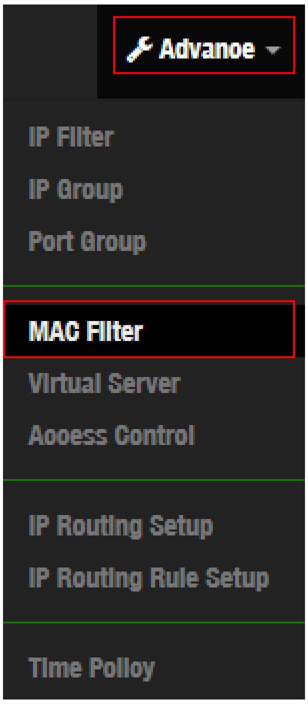
Port List

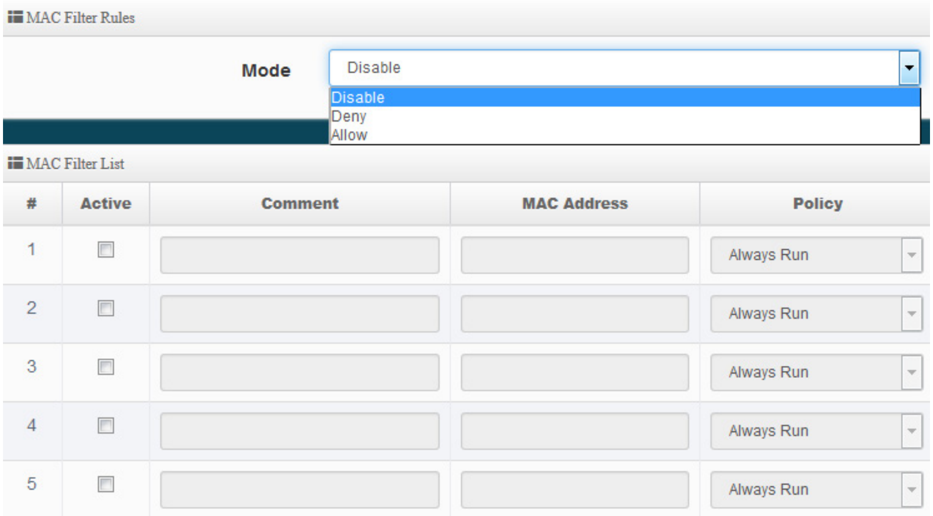
#	Port	Comment	Action
-	-	-	-

- ➢ **Comment:** Enter Port Group description.
- ➢ **Port Type:** Administrator can select single or range Port.
- ➢ **Port:** Administrator can set service port.

6.4 MAC Filter

Allows creating MAC filter rules to allow or deny unicast or multicast packets from limited number of MAC addresses. Important and must note. That MAC filter rules have precedence over IP Filter rules.




MAC Filter Rules

Mode: Disable

MAC Filter List

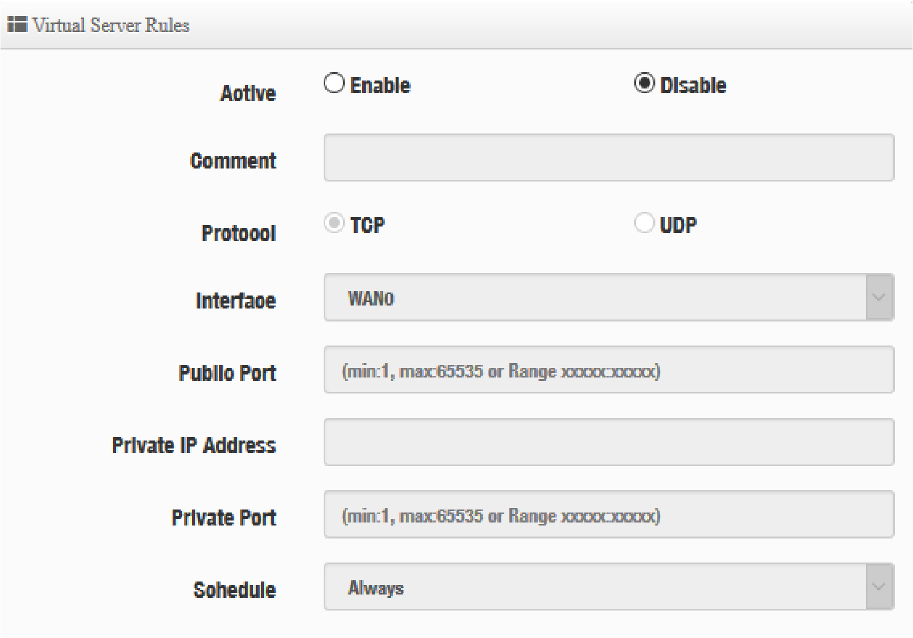
#	Active	Comment	MAC Address	Policy
1	□			Always Run
2	□			Always Run
3	□			Always Run
4	□			Always Run
5	□			Always Run

- **Mode:** Administrator can select Deny or Allow.
  - **Deny:** The MAC Filter List will be **denied** to access (LAN to WAN). Others will be allowed.
  - **Allow:** The MAC Filter List will be **allowed** to access (LAN to WAN). Others will be denied.
- **Comment:** Enter the description of MAC filter rule.
- **MAC Address:** Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the MAC Filter List.
- **Policy:** Administrator can select to use rule by **"Time Policy".**

6.5 Virtual Server

The **"Virtual Server"** can also referred to as "Port Forward" as well and used interchangeably. Resources in the network can be exposed to the Internet users in a controlled manner including on-line gaming, video conferencing or others via Virtual Server setup. Don't repeat ports' usage to avoid confusion.

Suppose you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), and port 80 to another (B in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.



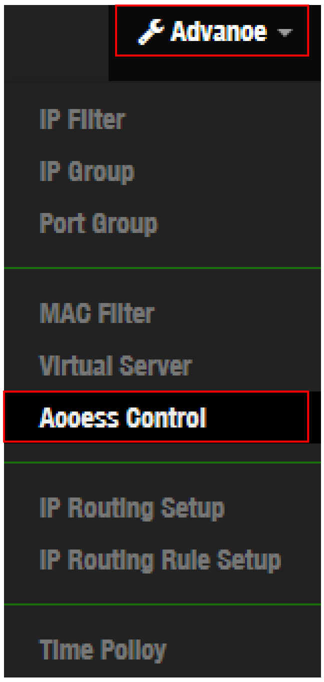
Virtual Server Rules

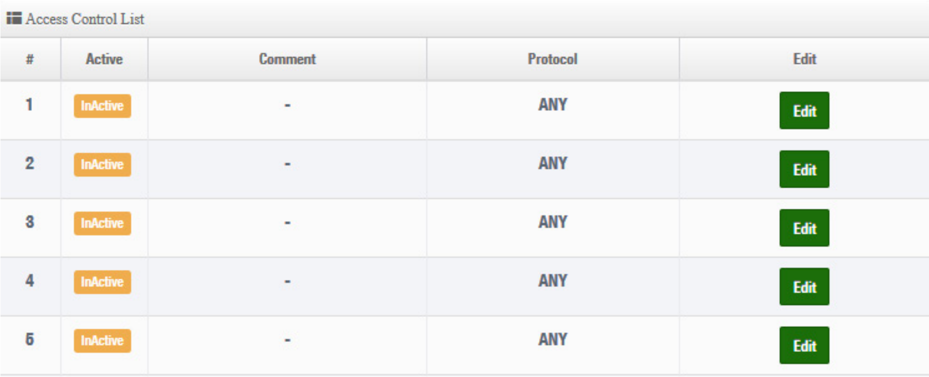
Aotive	○ Enable	● Dlsable
Comment		
Protoool	● TCP	○ UDP
Interfaoe	WAN0	
Publlo Port	(min:1, max:65535 or Range xxxxx:xxxxx)	
Prlvate IP Address		
Prlvate Port	(min:1, max:65535 or Range xxxxx:xxxxx)	
Sohedule	Always	

- **Active:** Administrator can select Virtual server rule to Enable or disable.
- **Comment:** Enter the description of virtual server rule.
- **Protocol:** Administrator can select service protocol of TCP or UDP.
- **Public Port:** Enter service port No. for public.
- **Private IP Address:** Enter corresponding IP address for internal.
- **Private Port:** Enter internal service port No. for private.
- **Schedule :** Administrator can select to used rule of **“Time Policy”**

6.6 Access Control

The Access Control function administrator can to block or allow specific kinds of TCP/UDP/ICMP protocol, such as Internet access, designated services, and websites. The Access Control function can set 20 profiles. Please click on **Advance -> Access Control** and follow the below setting.

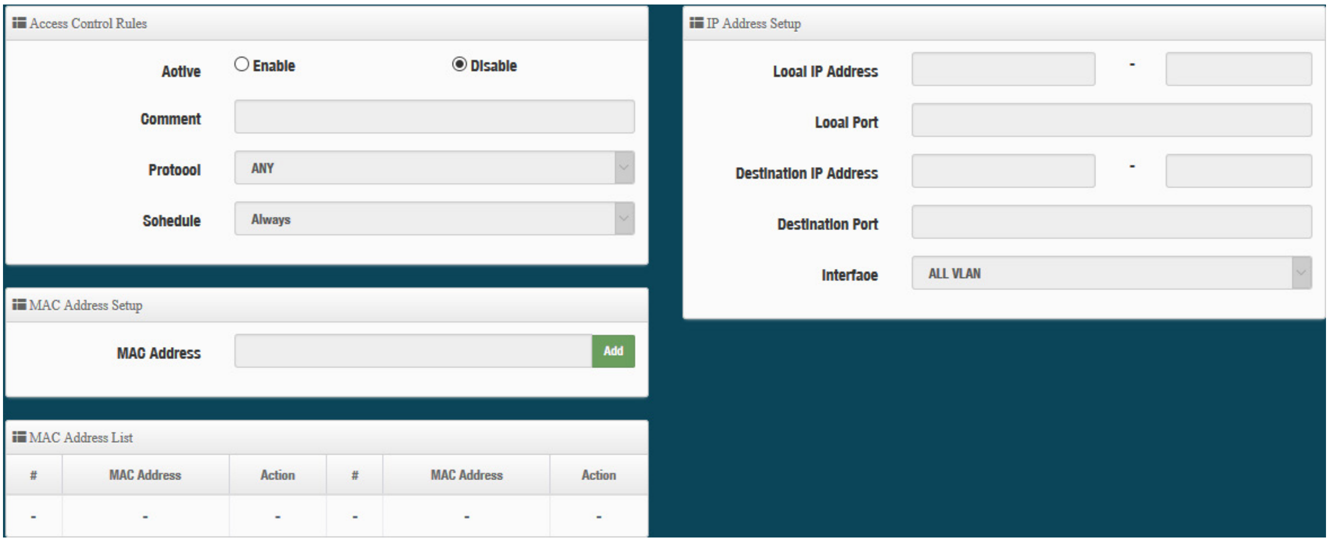




Access Control List

#	Active	Comment	Protocol	Edit
1	InActive	-	ANY	Edit
2	InActive	-	ANY	Edit
3	InActive	-	ANY	Edit
4	InActive	-	ANY	Edit
5	InActive	-	ANY	Edit

- **#**：Display access control list.
- **Active**：Display Active or InActive for the access control rule.
- **Comment:** Display information for the rule.
- **Protocol**：Display information for the protocol.
- **Edit**：Administrator can click the button to set Access Control rule.



Access Control Rules

Active	○ Enable ● Disable
Comment	
Protocol	ANY
Schedule	Always

MAC Address Setup

MAC Address	Add

MAC Address List

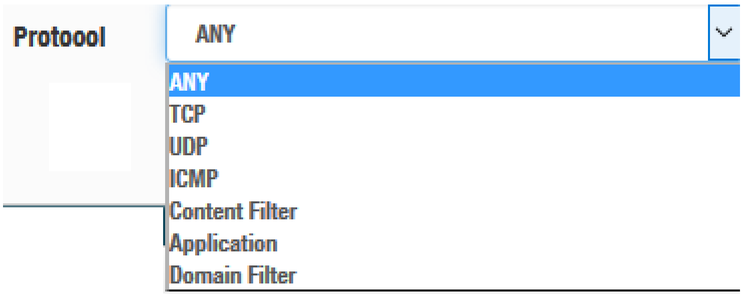
#	MAC Address	Action	#	MAC Address	Action
-	-	-	-	-	-

IP Address Setup

Local IP Address	-
Local Port	
Destination IP Address	-
Destination Port	
Interface	ALL VLAN

# Access control rules：

- **Active**：Administrator can select Enable or Disable for the Access control rule.
- **Comment**：Administrator can enter comment for the role.
- **Protocol**：Administrator can to select management protocol by TCP/UDP/ICMP/Content Filter/Application and Domain Filter.

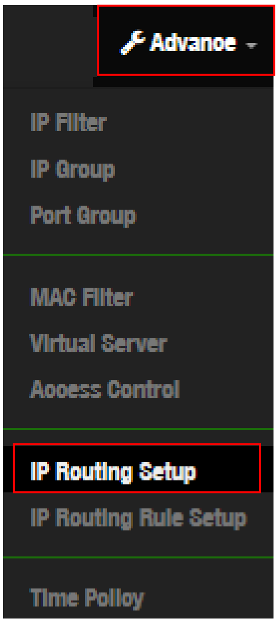


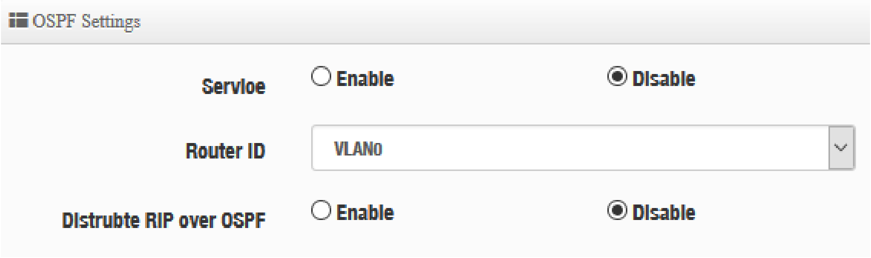
Protocol

- ✓ **ANY:** Select **"Any"** is all deny Protocol, administrator can filter local IP / IP range go to destination IP / IP range and use protocol.
- ✓ **TCP:** Deny TCP Protocol, Administrator can set TCP protocol and assign IP / IP range.
- ✓ **UDP:** Deny UDP Protocol, Administrator can set UDP protocol and assign IP / IP range.
- ✓ **ICMP:** Deny ICMP Protocol, Administrator can assign IP / IP range.
- ✓ **Content Filter:** Administrator can set web Keyword to filter.
- ✓ **Application:** System built-in multiple applications data, Administrator can select application data to filter.
- ✓ **Domain:** Administrator can set domain name to filter.
  - ● **Schedule**：The rule can apply Time Policy.

6.7 IP Routing Setup

The IP Routing Settings allows configure routing feature in the gateway. The system supports RIP(Routing Information Protocol) and OSPF(Open Shortest Path First) dynamic routing and allows you to manually configure static network routes. Please click on Advance -> IP Routing and follow the below setting.





OSPF Settings

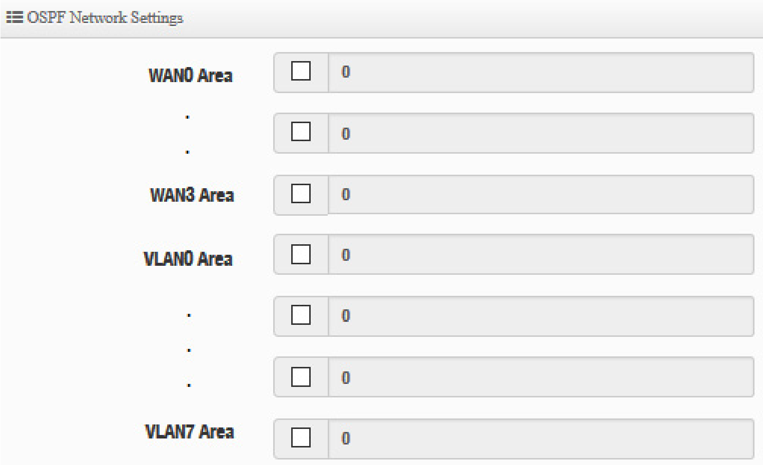
Service	○ Enable	● Disable
Router ID	VLAN0	
Distrubte RIP over OSPF	○ Enable	● Disable

- **OSPF Settings :**

  OSPF (Open Shortest Path First) is a router protocol used to find the best path for packets as they pass through a set of connected networks.

  - **Service:** Administrator can select enable or disable Service for OSPF.
  - **Route ID:** Administrator can select WAN0~3 and VLAN0~7 interface (IP) for the Route ID.
  - **Distribute RIP over OSPF:** Administrator can select enable or disable, if select enable system can allow RIP routes will redistributed into OSPF.

  OSPF Network Setting



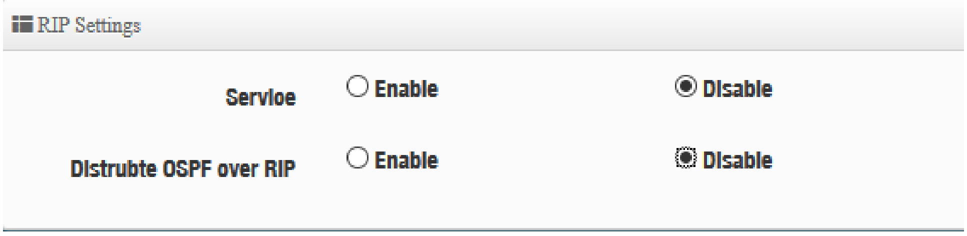
OSPF Network Settings

WAN0 Area	□	0
.	□	0
.		
WAN3 Area	□	0
VLAN0 Area	□	0
.	□	0
.		
.	□	0
VLAN7 Area	□	0

  ✓ **#Area:** Represents the area code of the OSPF routing protocol, which can be any digit in decimal, default is 0.

- **RIP Settings :**

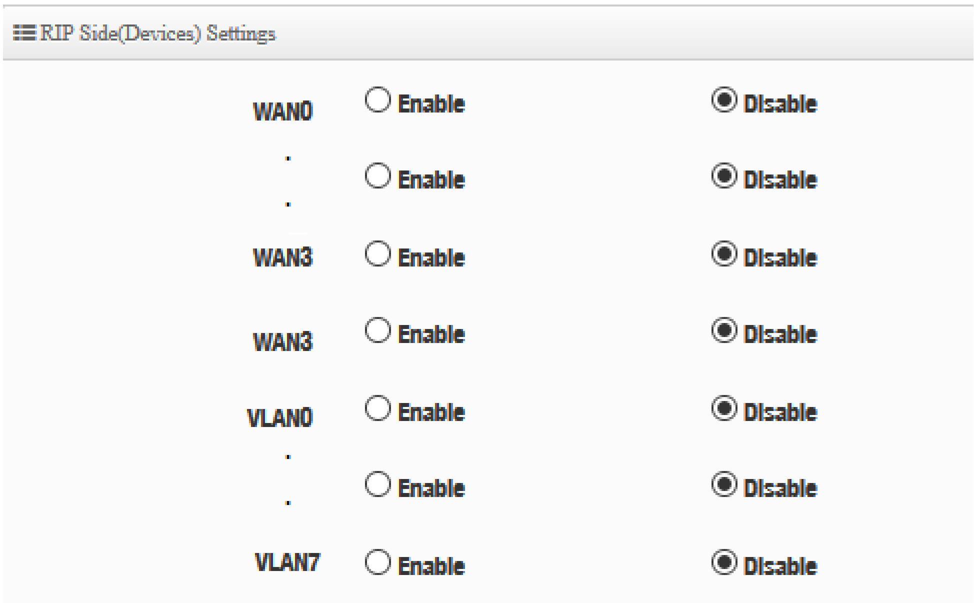
  RIP defines a way for routers, which connect networks using the IP, to share information about how to route traffic among networks. RIP prevents routing loops by implementing limit on the number of hops allowed in a path from source to destination. The maximum number of hops allowed for RIP is 15, which limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance and the route is considered unreachable.



RIP Settings

Service	○ Enable	● Disable
Distrubte OSPF over RIP	○ Enable	● Disable

  - **Service:** Administrator can select enable or disable Service for RIP.
  - **Distribute OSPF over RIP:** Administrator can select enable or disable, if select enable system can allow OSPF routes will redistributed into RIP.

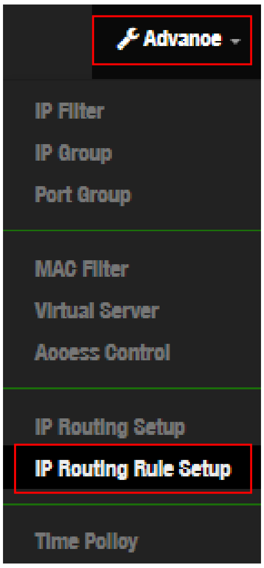


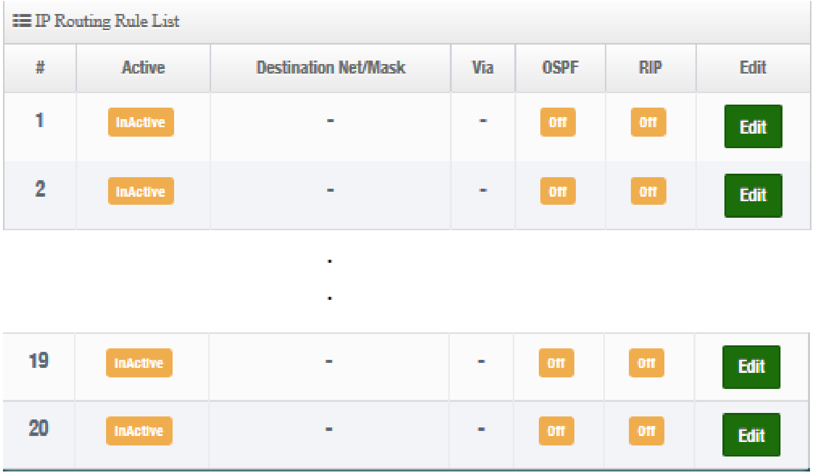
☰ RIP Side(Devices) Settings

WAN0	○ Enable	● Disable
.	○ Enable	● Disable
.		
WAN3	○ Enable	● Disable
WAN3	○ Enable	● Disable
VLAN0	○ Enable	● Disable
.	○ Enable	● Disable
.		
VLAN7	○ Enable	● Disable

- ✓ **RIP Side(Devices) Settings:** Administrator can choose enable or deniable for WAN/LAN interface

6.8 IP Routing Rule Setup

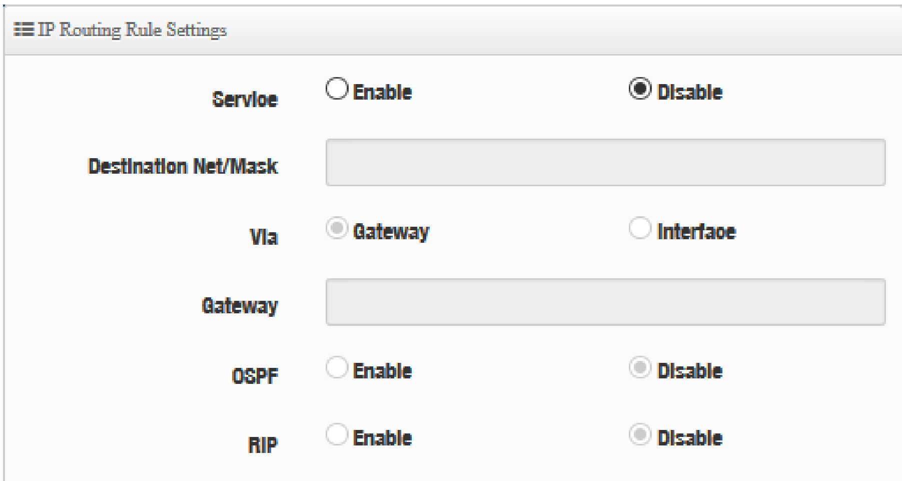




☰ IP Routing Rule List

#	Active	Destination Net/Mask	Via	OSPF	RIP	Edit
1	InActive	-	-	Off	Off	Edit
2	InActive	-	-	Off	Off	Edit
.						
.						
19	InActive	-	-	Off	Off	Edit
20	InActive	-	-	Off	Off	Edit

Please click **Edit** button to setting IP Routing Rule.

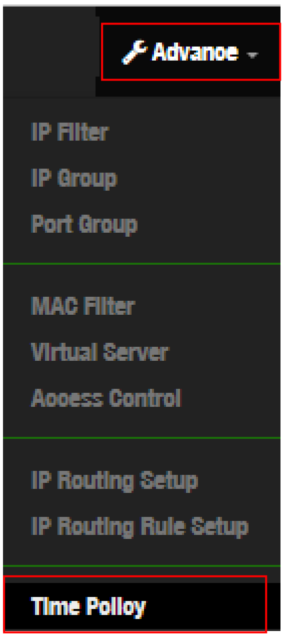


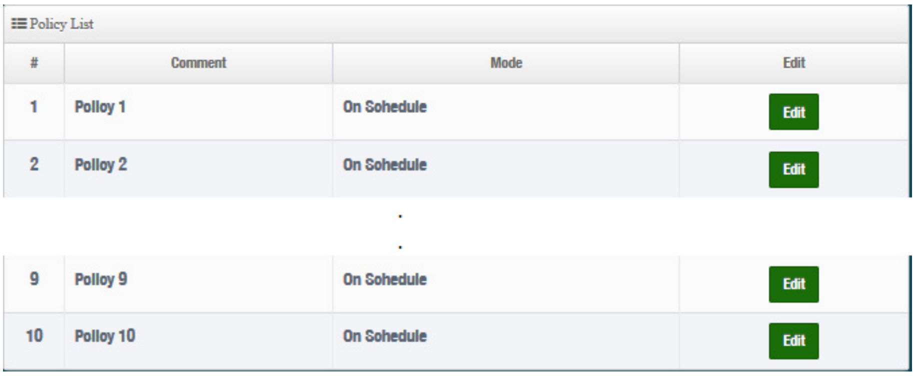
☰ IP Routing Rule Settings

Service	○ Enable	● Disable
Destination Net/Mask		
Via	● Gateway	○ Interface
Gateway		
OSPF	○ Enable	● Disable
RIP	○ Enable	● Disable

- **Service:** Administrator can select Enable or Disable for the IP Routing Rule.
- **Destination Net/Mask:** If administrator select enable for service, will be able set destination Net/Mask.
- **Via:** Administrator can select use Gateway or Interface
  - **Gateway:** enter Gateway IP address.
  - **Interface:** Select WAN / LAN interface.
- **OSPF/RIP:** Administrator can select enable or disable, if select enable will apply "**IP Routing Setup**" of **OSPF/RIP** function.

6.9 Time Policy

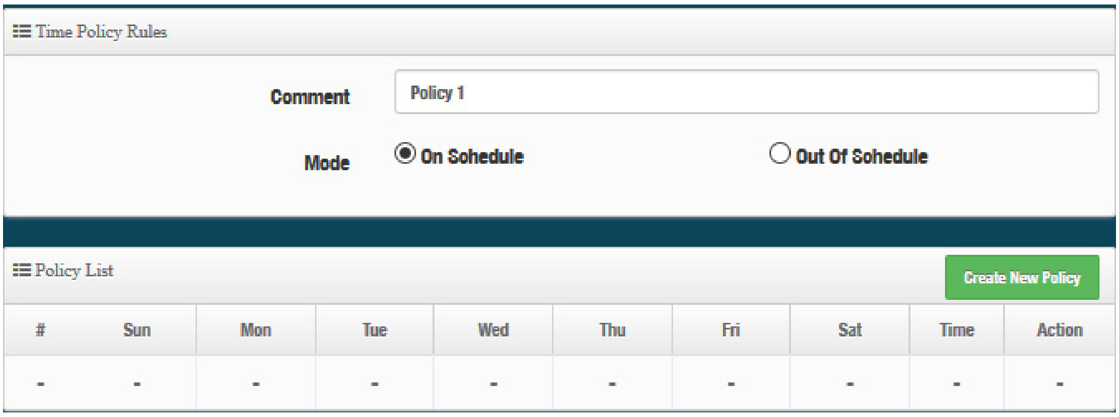




☰ Policy List

#	Comment	Mode	Edit
1	Policy 1	On Schedule	Edit
2	Policy 2	On Schedule	Edit
.			
.			
9	Policy 9	On Schedule	Edit
10	Policy 10	On Schedule	Edit

Please click **Edit** button to setting IP Routing Rule.



Time Policy Rules

Comment: Policy 1

Mode: ● On Schedule ○ Out Of Schedule

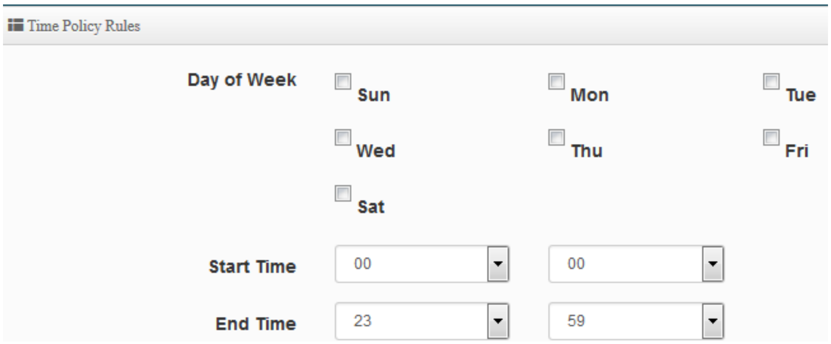
Policy List

#	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Action
-	-	-	-	-	-	-	-	-	-

- ➢ Comment: Enter the description of Time Policy rule.
- ➢ Mode: Administrator can select on schedule or Out of schedule to execution the rules.

Create New Policy button:

Administrator can set time for week / start time and end time.



Time Policy Rules

Day of Week: □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Start Time: 00 00

End Time: 23 59

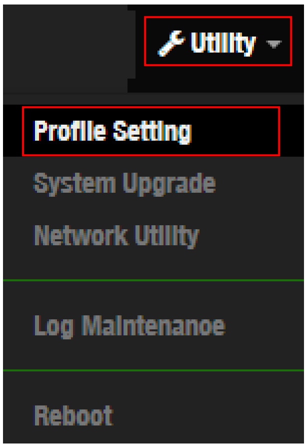
Click “**Save**” button to add schedule to policy. There are 10 schedule maximum allowed in the each time policy. All schedules can be edited or removed in the each time policy. Click Reboot button to activate your changes.

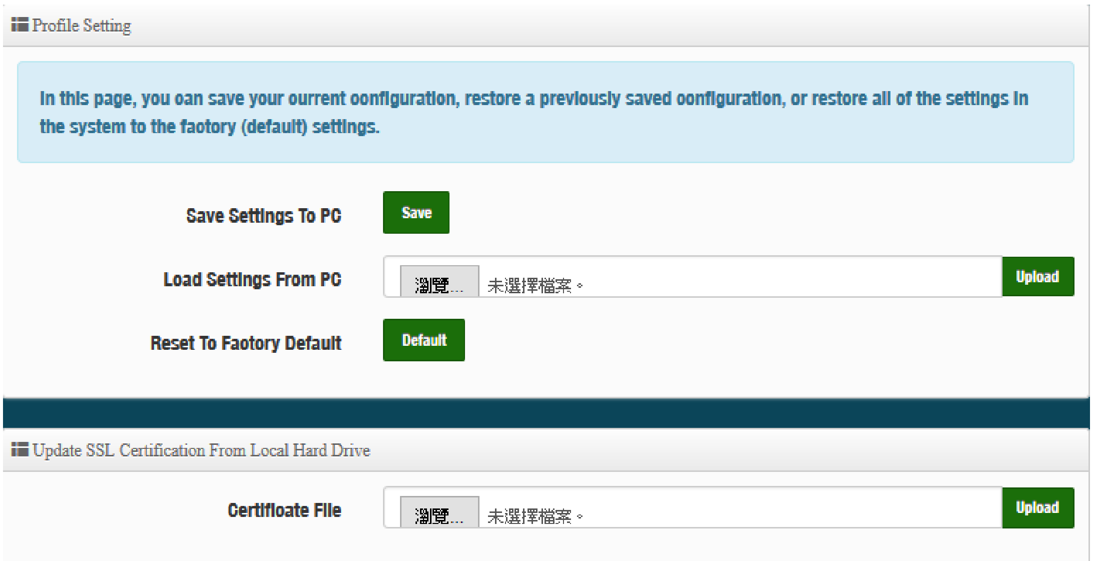
7. Utility

7.1 Profile Setting

This Functions purpose is to backup current configuration, restore prior configuration or reset back to factory default configurations.

Please click on **Utility -> Profile Setting** and follow the below setting




Profile Setting

In this page, you can save your current configuration, restore a previously saved configuration, or restore all of the settings in the system to the factory (default) settings.

Save Settings To PC [Save]

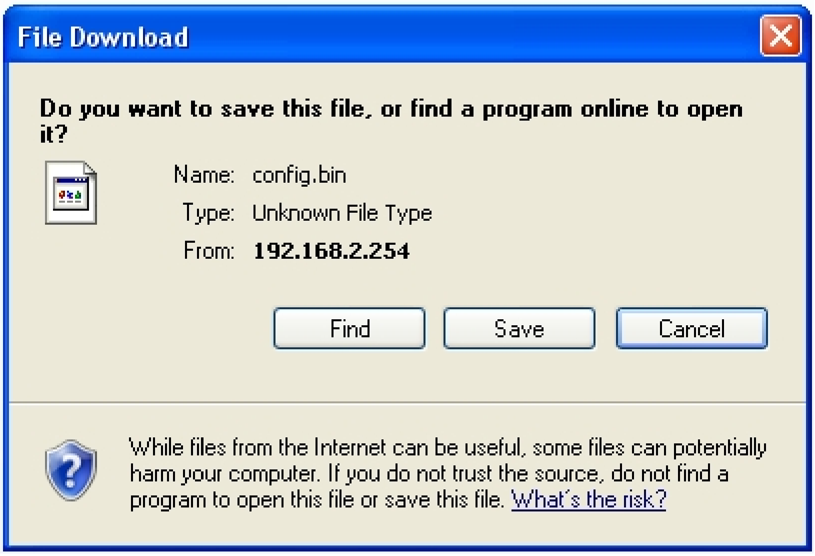
Load Settings From PC [瀏覽... 未選擇檔案。] [Upload]

Reset To Factory Default [Default]

Update SSL Certification From Local Hard Drive

Certificate File [瀏覽... 未選擇檔案。] [Upload]

- **Save Settings to PC:** Click ***Save*** button to save the current configuration to a local disk.



File Download

Do you want to save this file, or find a program online to open it?

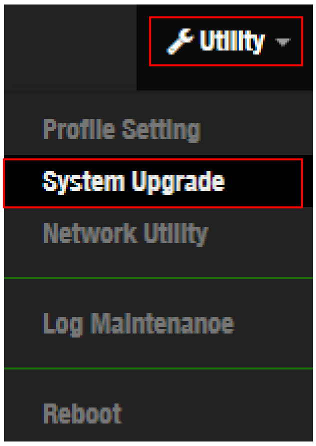
Name: config.bin
Type: Unknown File Type
From: 192.168.2.254

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

- **Load Settings from PC:** Click ***Browse*** button to locate a configuration file to restore, and then click ***Upload*** button to upload.
- **Reset To Factory Default:** Click ***Default*** button to reset back to the factory default settings and expect **Successful** loading message**.** Then, click ***Reboot*** button to activate.

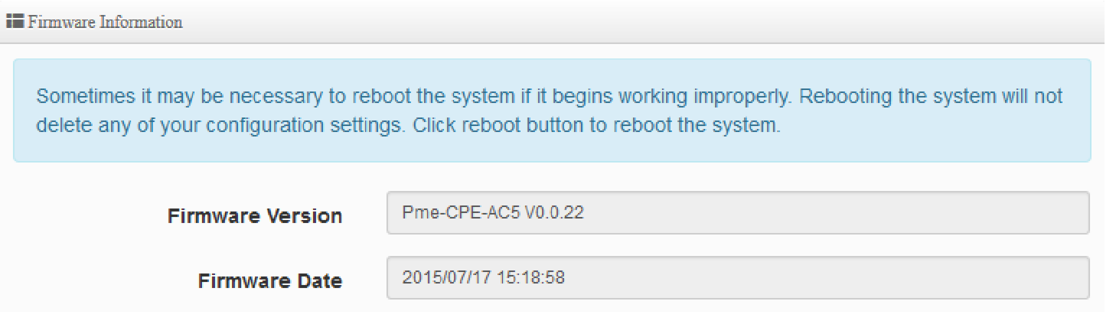
7.2 System Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around 2 minutes to upgrade due to complexity of firmware. To upgrade system firmware, click Browse button to locate the new firmware, and then click Upgrade button to upgrade.



Firmware Information:

Display the system firmware information.



Firmware Information

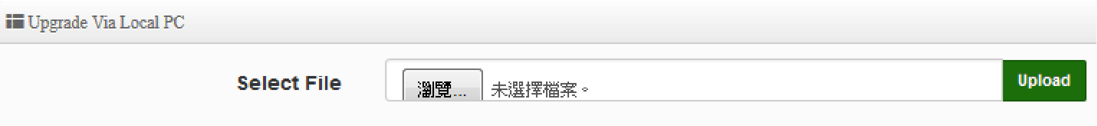
Sometimes it may be necessary to reboot the system if it begins working improperly. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.

Firmware Version: Pme-CPE-AC5 V0.0.22

Firmware Date: 2015/07/17 15:18:58

Upgrade Via Local PC and TFTP Server:

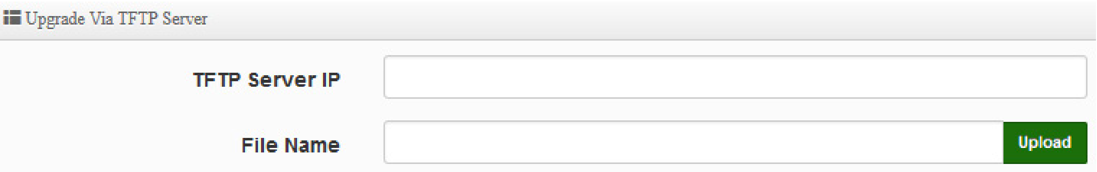
The upgrade firmware will support via local PC and TFTP Server and HTTP URL to upgrade system.



Upgrade Via Local PC

Select File: 瀏覽... 未選擇檔案。

- **Select File:** Administrator can select Firmware file in Local PC.

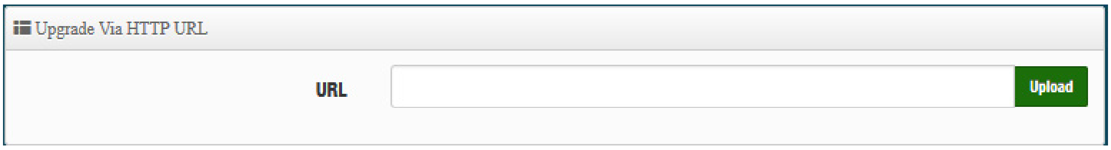


Upgrade Via TFTP Server

TFTP Server IP

File Name

- **TFTP Server:** Enter IP address for TFTP Server.
- **File Name:** Enter file name.



Upgrade Via HTTP URL

URL

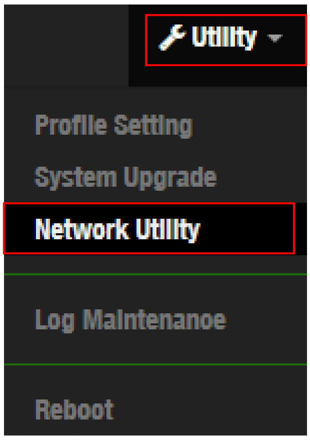
- **URL:** Administrator can enter path for Firmware file.

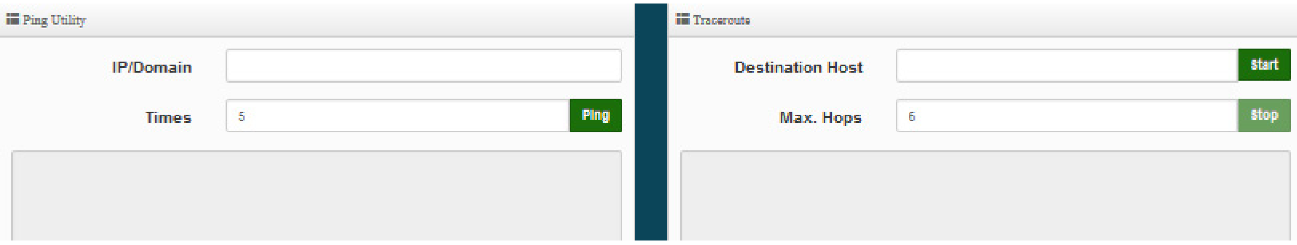
Notice

1. *To prevent data loss during firmware upgrade, please back up current settings before proceeding*
2. *Do not interrupt during firmware upgrade including power on/off as this may damage system.*

7.3 Network Utility

The administrator can diagnose network connectivity via the PING or TRACEROUTE utility. Please click on **Utility** -> **Network Utility** and follow the below setting.





IP/Domain:

Times: 5

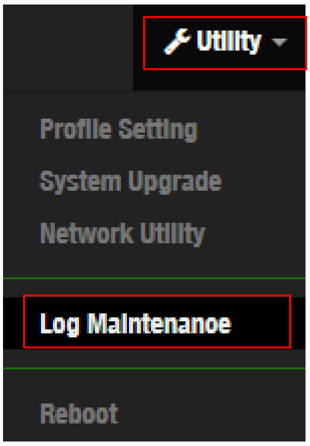
Destination Host:

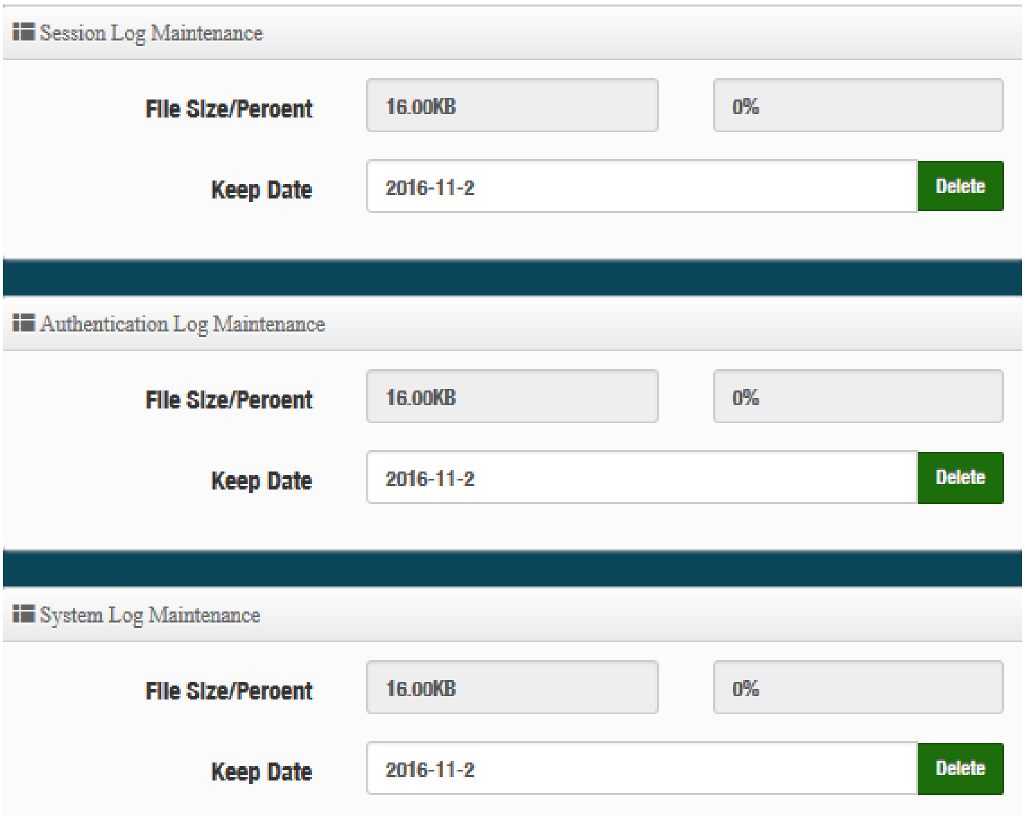
Max. Hops: 6

- **Ping**: This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the **Result** field while running the PING test.
  - **IP/Domain**： Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ping button to proceed. The ping result will be shown in the Result field.
  - **Count**： By default, its 5 and the range is from 1 to 50. It indicates number of connectivity test.
- **Traceroute**： Allows tracing the hops from the CenOS 5.0 AP device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the **Start** button, click **Stop** button to stopped test.
  - **Destination Host**: Specifies the Destination Host for the finding the route taken by ICMP packets across the network.
  - **MAX Hop**: Specifies the maximum number of hops (max time-to-live value) trace route will probe.

7.4 Log Maintenance

Administrator can monitor Log storage status for Session/Authentication and System.
Please click on **Utility ->Log Maintenance** and follow the below setting.





Session Log Maintenance

File Size/Percent: 16.00KB 0%

Keep Date: 2016-11-2 Delete

Authentication Log Maintenance

File Size/Percent: 16.00KB 0%

Keep Date: 2016-11-2 Delete

System Log Maintenance

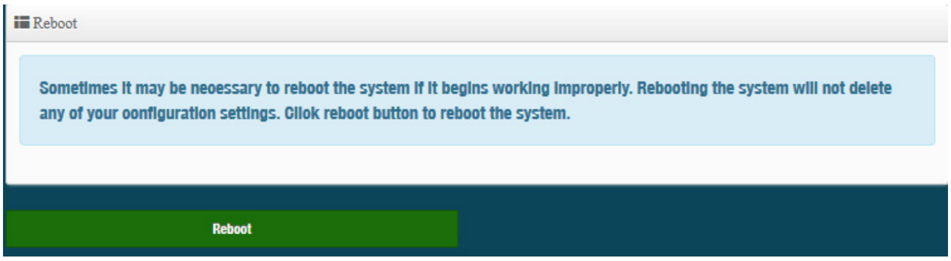
File Size/Percent: 16.00KB 0%

Keep Date: 2016-11-2 Delete

- **File Size/Percent:** Display used volume and percentage.
- **Keep Date:** Display creation date.
  - **Delete button:** Administrator can click “delete” button to clear log information.

7.5 Reboot

This function allows user to restart system with existing or most current settings when changes are made. Click **Reboot** button to proceed and take around three minutes to complete.



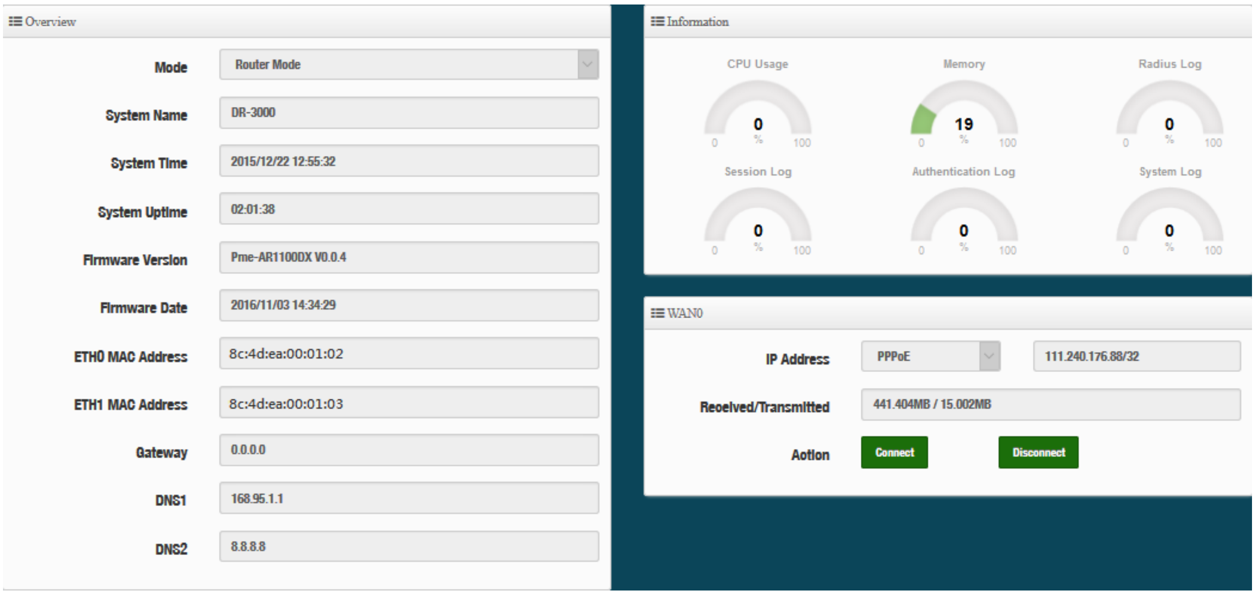
Reboot

Sometimes it may be neoessary to reboot the system if it begins working improperly. Rebooting the system will not delete any of your oonfiguration settings. Cliok reboot button to reboot the system.

8. Status

8.1 Overview

Detailed information on System, Network can be reviewed via this page.



Overview

Mode	Router Mode
System Name	DR-3000
System Time	2015/12/22 12:55:32
System Uptime	02:01:38
Firmware Version	Pme-AR1100DX V0.0.4
Firmware Date	2016/11/03 14:34:29
ETH0 MAC Address	8c:4d:ea:00:01:02
ETH1 MAC Address	8c:4d:ea:00:01:03
Gateway	0.0.0.0
DNS1	168.95.1.1
DNS2	8.8.8.8

Information

CPU Usage	0 %
Memory	19 %
Radius Log	0 %
Session Log	0 %
Authentication Log	0 %
System Log	0 %

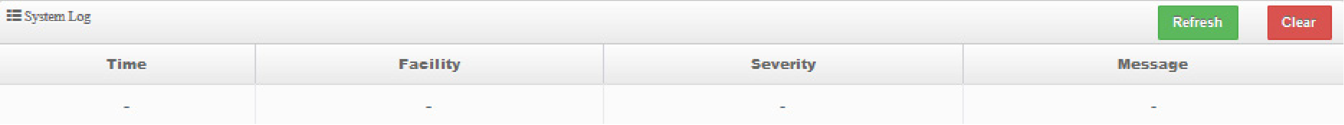
WAN0

IP Address	PPPoE	111.240.176.88/32
Reoeived/Transmitted	441.404MB / 15.002MB	
Aotion	Connect	Disconnect

- ➢ **WAN#:** Display information for WAN Port setting. Administrator can click Action button to connect or disconnect for WAN Ports.

8.2 Local System Log

The system log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.

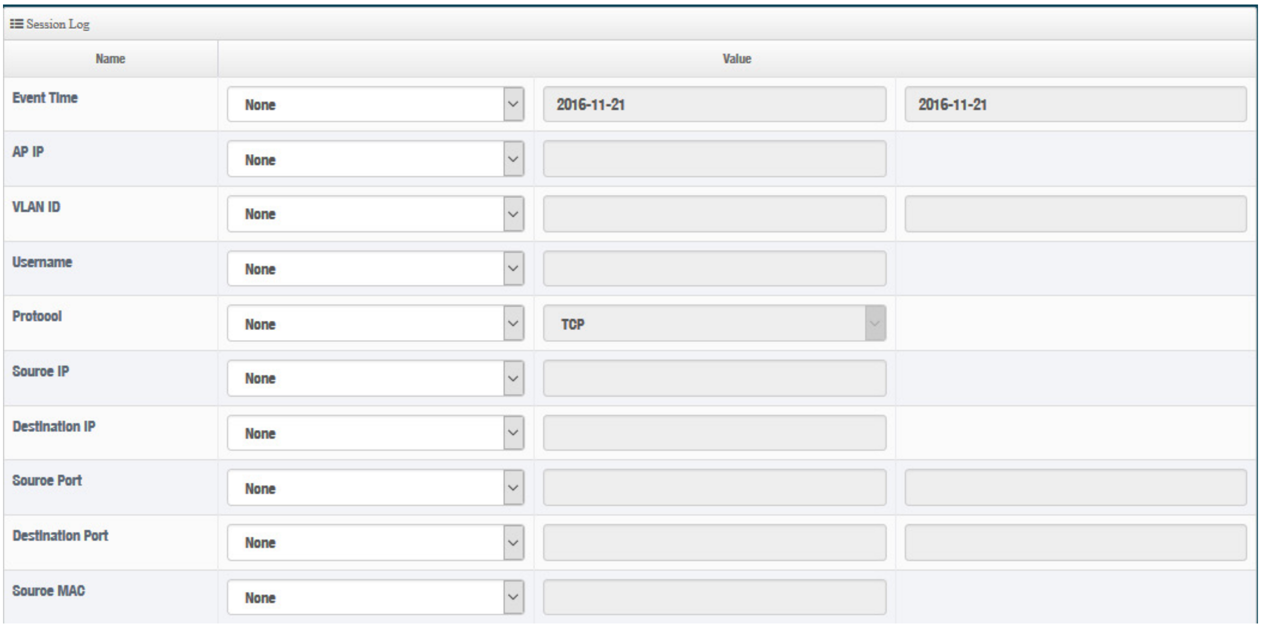


Time	Facility	Severity	Message
-	-	-	-

- **Time** ： The date and time when the event occurred.
- **Facility** ： It helps users to identify source of events such “System” or “User”
- **Severity** ： Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message** ： Description of the event.
- Click **“Refresh”** button to renew the log
- Click “**Clear”** button to clear all the record.

8.3 Session Log

If enable syslog server and session log in Cerio's AP, the page can record account for session log. Session log page built-in smart-search function will display account use session information, administrator can use keyword or date approach to discover.

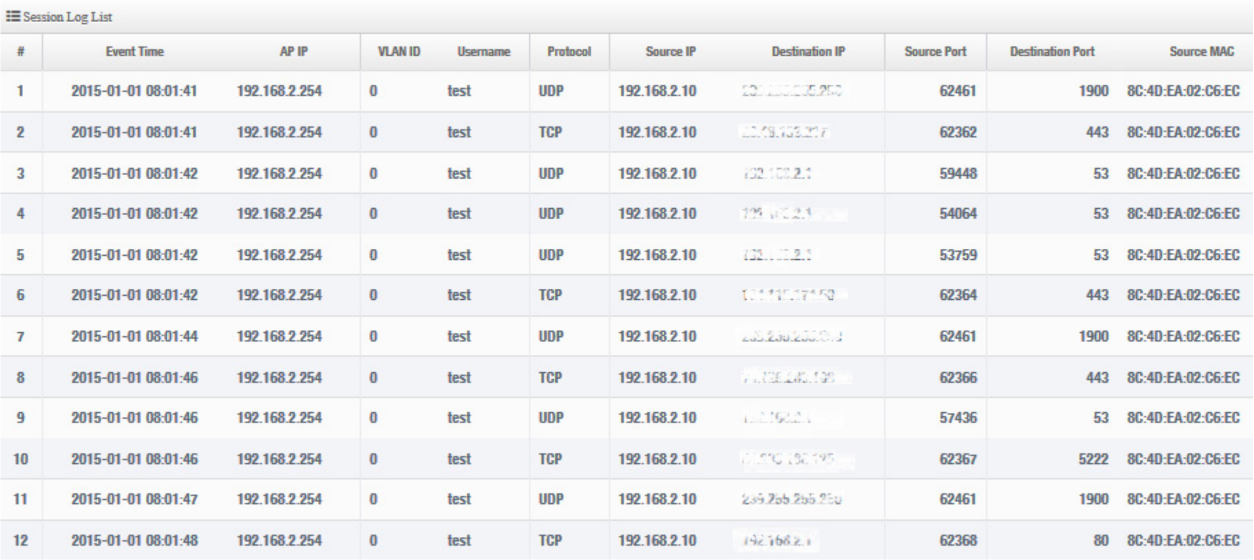


Name	Value		
Event Time	None	2016-11-21	2016-11-21
AP IP	None		
VLAN ID	None		
Username	None		
Protoool	None	TCP	
Souroe IP	None		
Destination IP	None		
Souroe Port	None		
Destination Port	None		
Souroe MAC	None		

Administrators can choose different data type in the search engines.

- **None:** The program doesn't judge characters, search all the information
- **Greater then:** Search values for greater than
- **Equal:** Search values for equal.
- **Less then:** Search values for less then.

- ➢ **Between:** Search values for between.
- ➢ **Like:** Search similar strings.

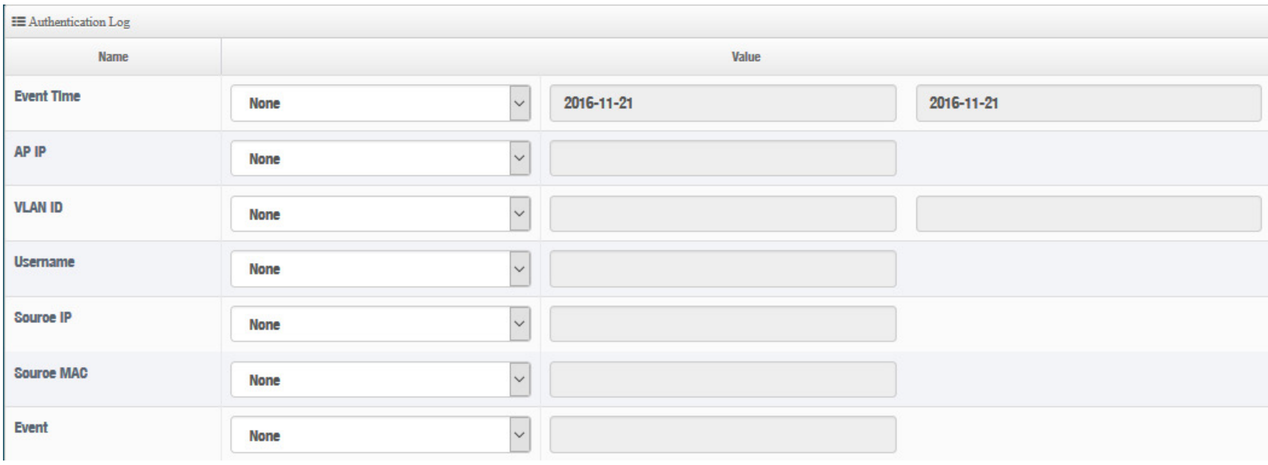


Session Log List

#	Event Time	AP IP	VLAN ID	Username	Protocol	Source IP	Destination IP	Source Port	Destination Port	Source MAC
1	2015-01-01 08:01:41	192.168.2.254	0	test	UDP	192.168.2.10	[redacted]	62461	1900	8C:4D:EA:02:C6:EC
2	2015-01-01 08:01:41	192.168.2.254	0	test	TCP	192.168.2.10	[redacted]	62362	443	8C:4D:EA:02:C6:EC
3	2015-01-01 08:01:42	192.168.2.254	0	test	UDP	192.168.2.10	[redacted]	59448	53	8C:4D:EA:02:C6:EC
4	2015-01-01 08:01:42	192.168.2.254	0	test	UDP	192.168.2.10	[redacted]	54064	53	8C:4D:EA:02:C6:EC
5	2015-01-01 08:01:42	192.168.2.254	0	test	UDP	192.168.2.10	[redacted]	53759	53	8C:4D:EA:02:C6:EC
6	2015-01-01 08:01:42	192.168.2.254	0	test	TCP	192.168.2.10	[redacted]	62364	443	8C:4D:EA:02:C6:EC
7	2015-01-01 08:01:44	192.168.2.254	0	test	UDP	192.168.2.10	[redacted]	62461	1900	8C:4D:EA:02:C6:EC
8	2015-01-01 08:01:46	192.168.2.254	0	test	TCP	192.168.2.10	[redacted]	62366	443	8C:4D:EA:02:C6:EC
9	2015-01-01 08:01:46	192.168.2.254	0	test	UDP	192.168.2.10	[redacted]	57436	53	8C:4D:EA:02:C6:EC
10	2015-01-01 08:01:46	192.168.2.254	0	test	TCP	192.168.2.10	[redacted]	62367	5222	8C:4D:EA:02:C6:EC
11	2015-01-01 08:01:47	192.168.2.254	0	test	UDP	192.168.2.10	[redacted]	62461	1900	8C:4D:EA:02:C6:EC
12	2015-01-01 08:01:48	192.168.2.254	0	test	TCP	192.168.2.10	[redacted]	62368	80	8C:4D:EA:02:C6:EC

8.4 Authentication Log

If enable syslog server and authentication log in Cerio's AP, the page can record account for authentication log. Authentication log page built-in smart-search function will display account use session information, administrator can use keyword or date approach to discover.

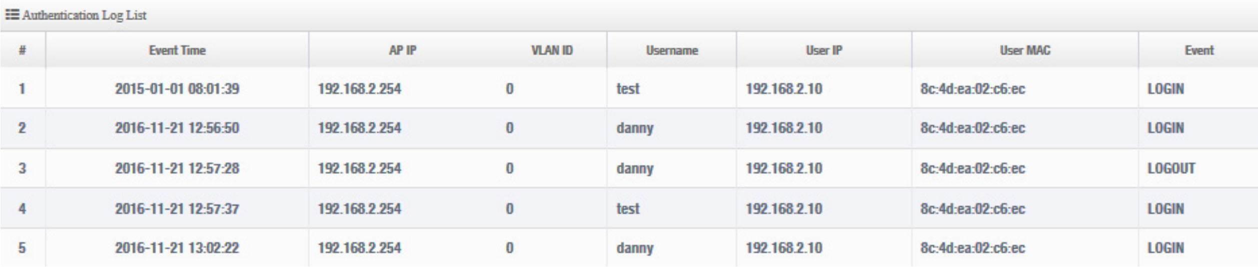


Authentication Log

Name	Value		
Event Time	None	2016-11-21	2016-11-21
AP IP	None		
VLAN ID	None		
Username	None		
Souroe IP	None		
Souroe MAC	None		
Event	None		

Administrators can choose different data type in the search engines.

- ➢ **None:** The program doesn't judge characters, search all the information
- ➢ **Greater then:** Search values for greater than
- ➢ **Equal:** Search values for equal.
- ➢ **Less then:** Search values for less then.
- ➢ **Between:** Search values for between.
- ➢ **Like:** Search similar strings.

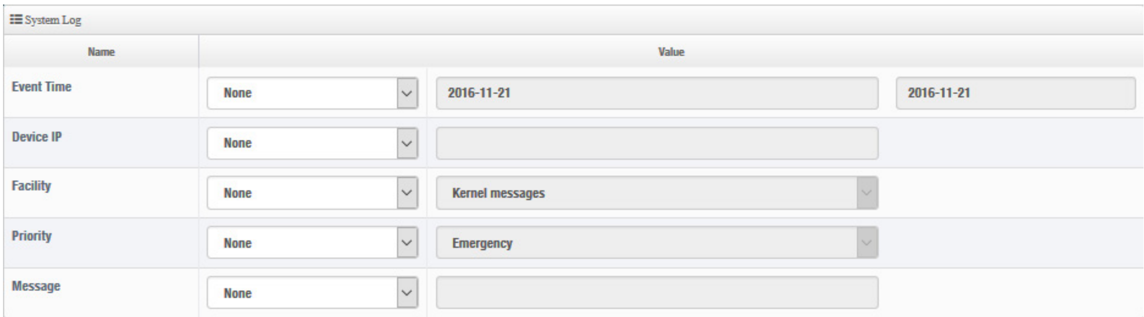


Authentication Log List

#	Event Time	AP IP	VLAN ID	Username	User IP	User MAC	Event
1	2015-01-01 08:01:39	192.168.2.254	0	test	192.168.2.10	8c:4d:ea:02:c6:ec	LOGIN
2	2016-11-21 12:56:50	192.168.2.254	0	danny	192.168.2.10	8c:4d:ea:02:c6:ec	LOGIN
3	2016-11-21 12:57:28	192.168.2.254	0	danny	192.168.2.10	8c:4d:ea:02:c6:ec	LOGOUT
4	2016-11-21 12:57:37	192.168.2.254	0	test	192.168.2.10	8c:4d:ea:02:c6:ec	LOGIN
5	2016-11-21 13:02:22	192.168.2.254	0	danny	192.168.2.10	8c:4d:ea:02:c6:ec	LOGIN

8.5 System Log

If administrator enable syslog server in Cerio's AP, the page can record system log for Cerio APs.

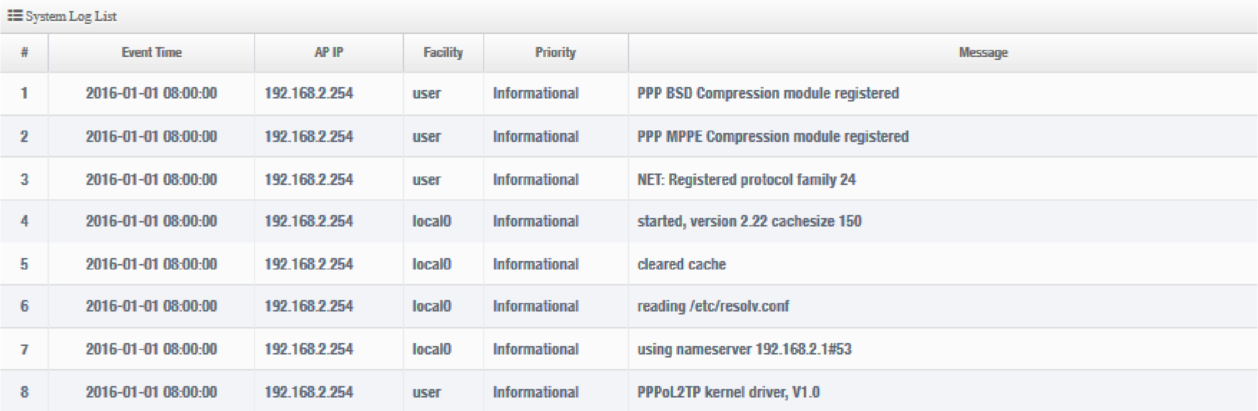


System Log

Name	Value		
Event Time	None	2016-11-21	2016-11-21
Device IP	None		
Facility	None	Kernel messages	
Priority	None	Emergency	
Message	None		

Administrators can choose different data type in the search engines.

- **None:** The program doesn't judge characters, search all the information
- **Greater then:** Search values for greater than
- **Equal:** Search values for equal.
- **Less then:** Search values for less then.
- **Between:** Search values for between.
- **Like:** Search similar strings.



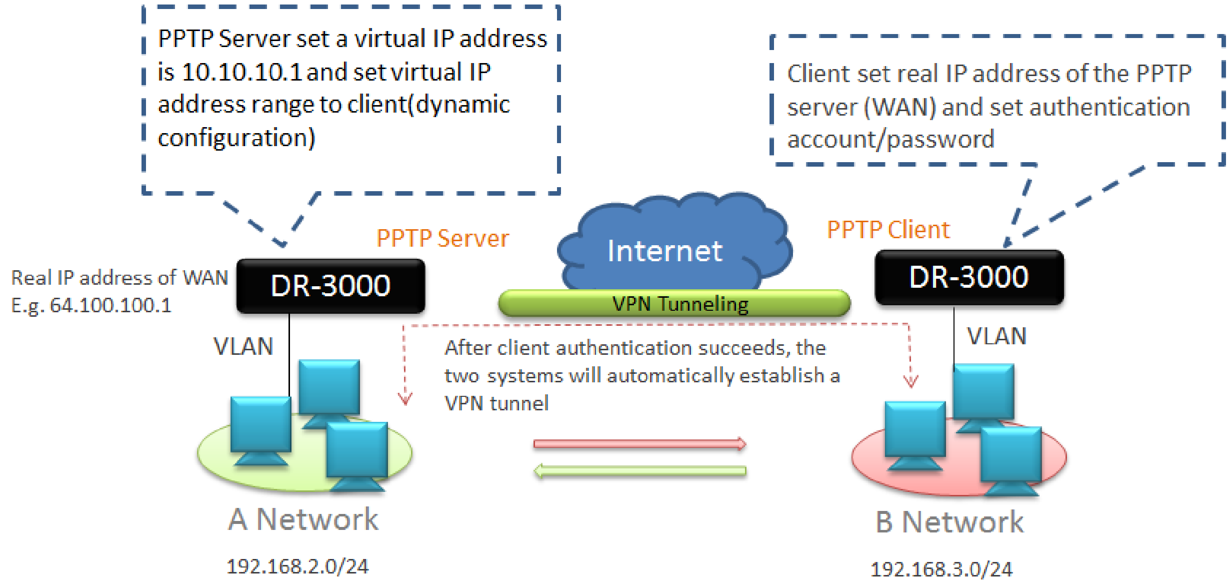
System Log List

#	Event Time	AP IP	Facility	Priority	Message
1	2016-01-01 08:00:00	192.168.2.254	user	Informational	PPP BSD Compression module registered
2	2016-01-01 08:00:00	192.168.2.254	user	Informational	PPP MPPE Compression module registered
3	2016-01-01 08:00:00	192.168.2.254	user	Informational	NET: Registered protocol family 24
4	2016-01-01 08:00:00	192.168.2.254	local0	Informational	started, version 2.22 cachesize 150
5	2016-01-01 08:00:00	192.168.2.254	local0	Informational	cleared cache
6	2016-01-01 08:00:00	192.168.2.254	local0	Informational	reading /etc/resolv.conf
7	2016-01-01 08:00:00	192.168.2.254	local0	Informational	using nameserver 192.168.2.1#53
8	2016-01-01 08:00:00	192.168.2.254	user	Informational	PPPoL2TP kernel driver, V1.0

9. Technical documents

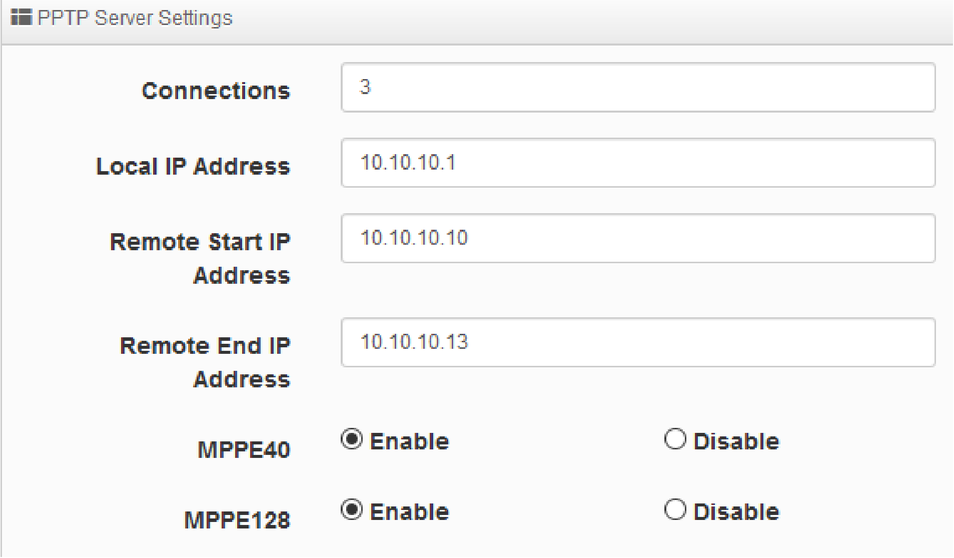
9.1 Example for PPTP/L2TP setup

Create a VPN tunnel use server / client bridge for the PPTP / L2TP protocol, if PPTP server set virtual IP address is 10.10.10.1 then must also set start to end IP address for dynamic configuration, can give VPN client automatically obtain a virtual IP address. The following concept map


PPTP Server set a virtual IP address is 10.10.10.1 and set virtual IP address range to client(dynamic configuration)
Client set real IP address of the PPTP server (WAN) and set authentication account/password
PPTP Server
Internet
PPTP Client
Real IP address of WAN
E.g. 64.100.100.1
DR-3000
VPN Tunneling
DR-3000
VLAN
After client authentication succeeds, the two systems will automatically establish a VPN tunnel
VLAN
A Network
192.168.2.0/24
B Network
192.168.3.0/24

PPTP Server setup step

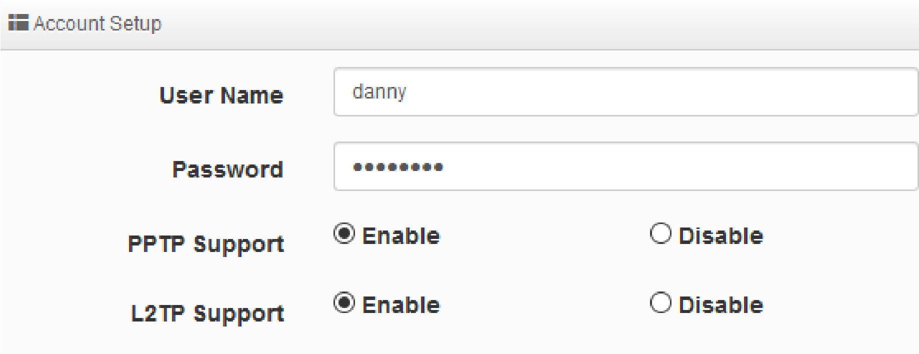
1. Enable PPTP/LTP Server and set VPN used virtual IP address. (Refer to 3.8 /3.9 for instructions)



PPTP Server Settings

Connections	3	
Local IP Address	10.10.10.1	
Remote Start IP Address	10.10.10.10	
Remote End IP Address	10.10.10.13	
MPPE40	● Enable	○ Disable
MPPE128	● Enable	○ Disable

2. Create authentication of client account and password



Account Setup

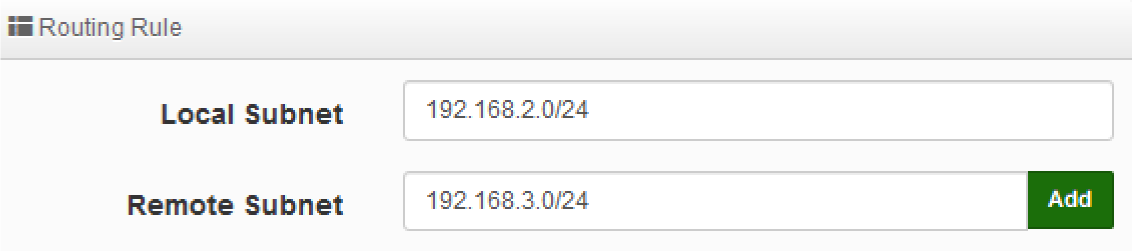
User Name: danny

Password: ••••••••

PPTP Support: ● Enable ○ Disable

L2TP Support: ● Enable ○ Disable

Setup routing between the two networks



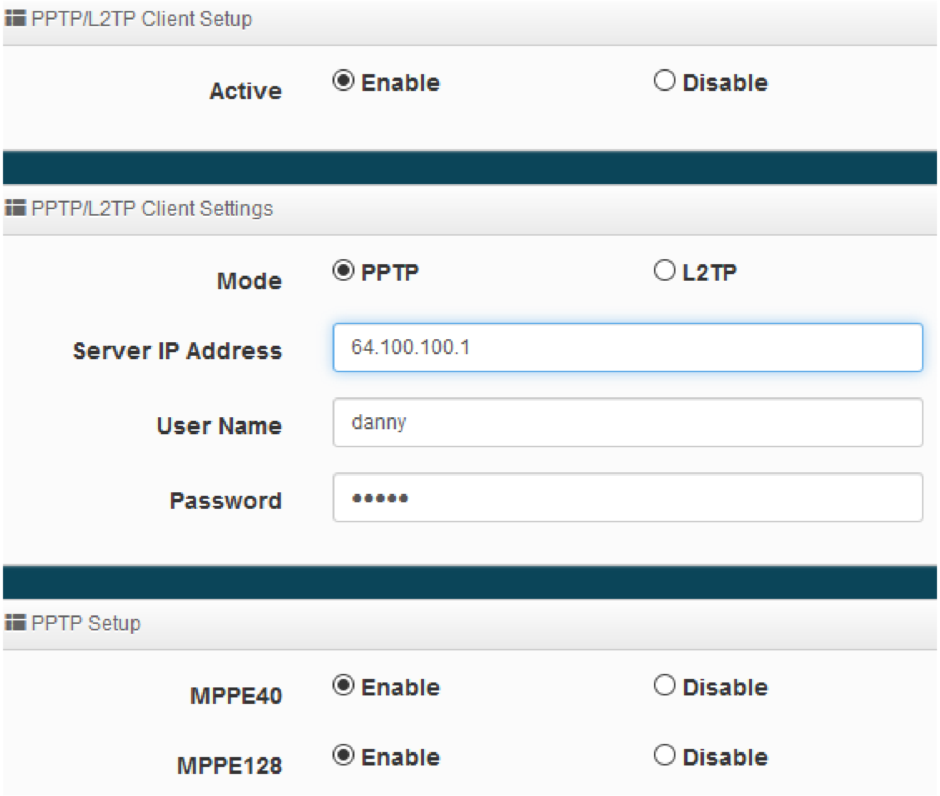
Routing Rule

Local Subnet: 192.168.2.0/24

Remote Subnet: 192.168.3.0/24

PPTP Client setup step

1. Set real IP address of remote VPN server and authentication account / password.



PPTP/L2TP Client Setup

Active: ● Enable ○ Disable

PPTP/L2TP Client Settings

Mode: ● PPTP ○ L2TP

Server IP Address: 64.100.100.1

User Name: danny

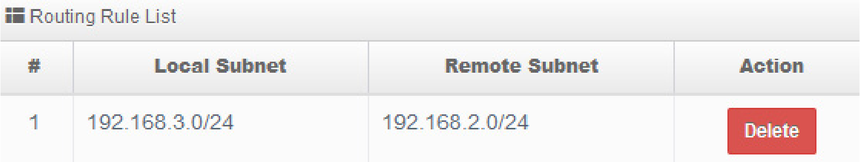
Password: •••••

PPTP Setup

MPPE40: ● Enable ○ Disable

MPPE128: ● Enable ○ Disable

2. Setup routing between the two networks

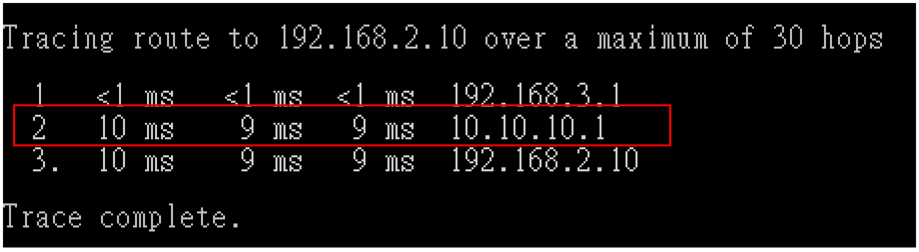


Routing Rule List

#	Local Subnet	Remote Subnet	Action
1	192.168.3.0/24	192.168.2.0/24	Delete

When the setting is complete, the both of the network will be through the VPN tunnel for data transmission.

Administrator can track the discovery, both network is used VPN tunnel to transmission.



```
Tracing route to 192.168.2.10 over a maximum of 30 hops

  1    <1 ms    <1 ms   <1 ms   192.168.3.1
  2    10 ms     9 ms    9 ms   10.10.10.1
  3.   10 ms     9 ms    9 ms   192.168.2.10

Trace complete.
```

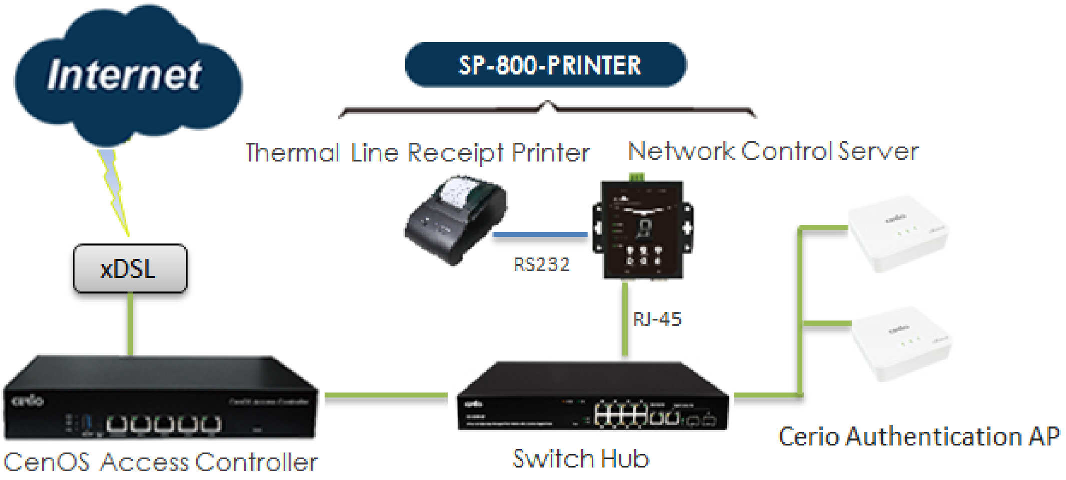
9.2 Hotspot function used POS system application

Notice | Cerio's POS system device by optional.

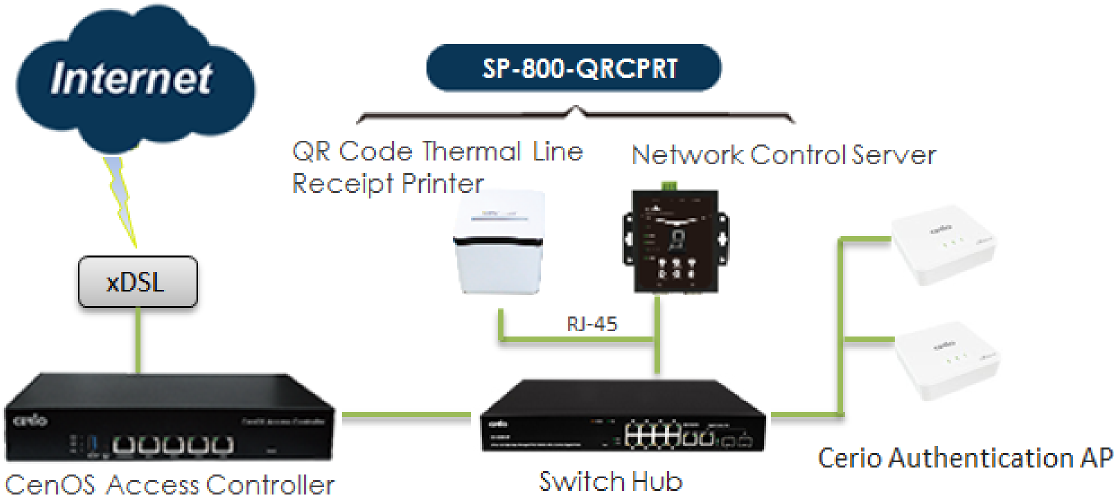
POS system is authentication device of the special use network control server (SP-800) + Thermal printer. You can refer to SP-800-PRINTER and SP-800-QRCPRT for Cerio's .

Administrator can use SP-800 to generate a new account for the remote control Cerio's Web authentication device and print authentication account.

Cerio's controller mounted SP-800-PRINTER for POS system application diagram

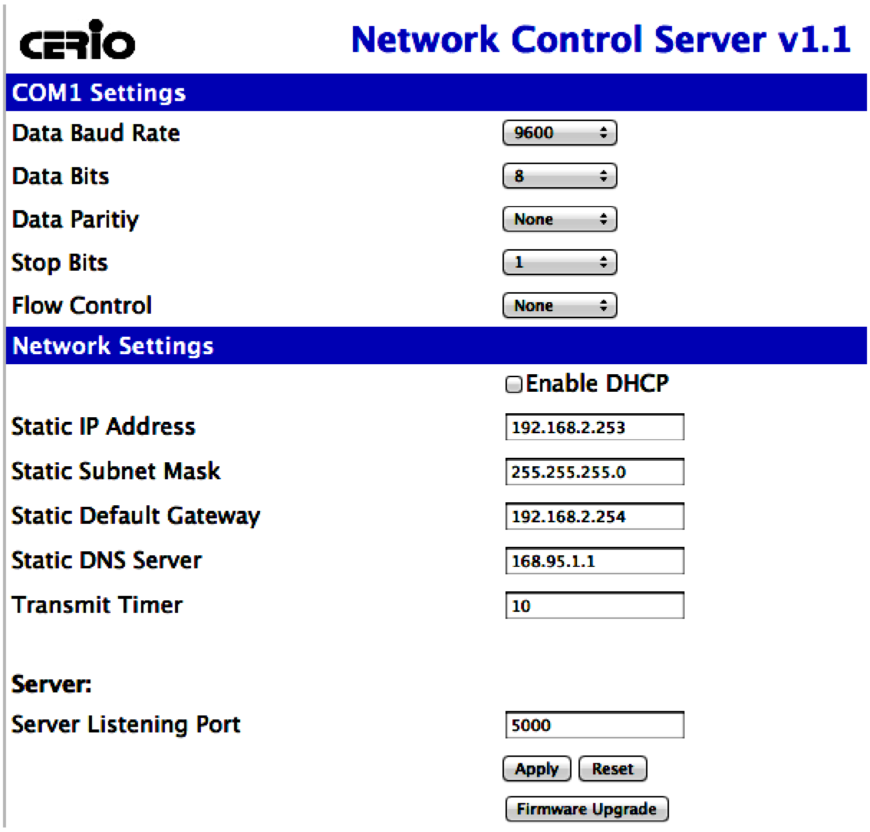


Cerio's controller mounted SP-800-QRCPRT for POS system application diagram.



Login management interface for SP-800

Network control server(SP-800) built-in web management interface. After install POS system architecture, administrator can use network connect to SP-800 interface and management.
The SP-800 manager URL is **http://192.168.2.253/setting.htm**, please open IE or Firefox browser and enter URL address to set function.



Network Control Server v1.1

COM1 Settings

Data Baud Rate	9600
Data Bits	8
Data Paritiy	None
Stop Bits	1
Flow Control	None

Network Settings

	□ Enable DHCP
Static IP Address	192.168.2.253
Static Subnet Mask	255.255.255.0
Static Default Gateway	192.168.2.254
Static DNS Server	168.95.1.1
Transmit Timer	10

Server:

Server Listening Port	5000

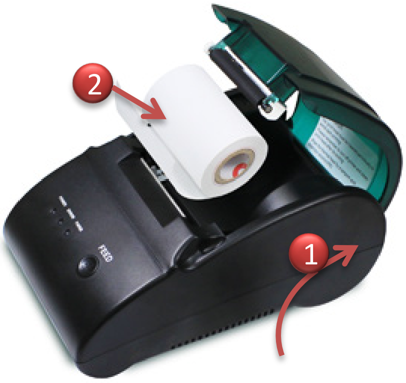
- **COM1 Setting:** Recommend use default。
- **Network Setting:**
  - **Enable DHCP:** Administrator can select enable or disable DHCP client.
  - **Static IP Address:** Administrator can set IP address for SP-800.
  - **Static DNS Server:** Administrator can set IP address for DNS server.。
  - **Transmit Timer:** system to detect controller connect status (millisecond).
  - **Server Listening Port:** SP-800 connection to controller use Port. (SP-800 and controller must be set the same port).

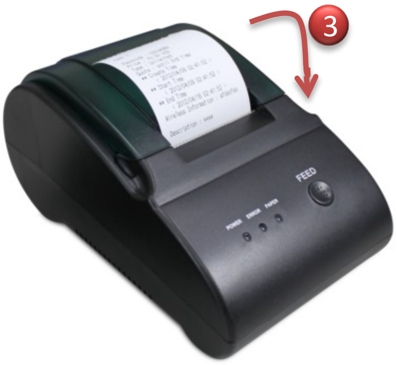
After setting is complete, please click Apply button.

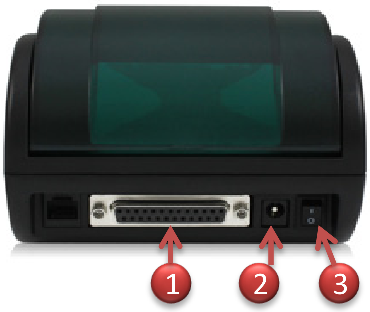
Install normal thermal printer

# Install step for thermal paper

1) Open the cover for thermal printer
2) Place the thermal paper in the printer groove
3) After pull the paper out a small portion please close the lid for thermal printer



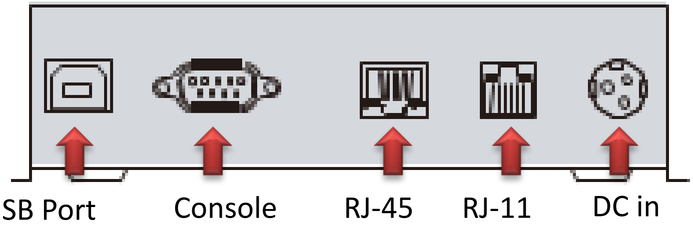




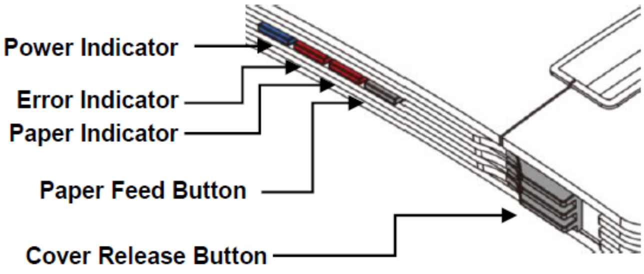
1) SP-800 connection to thermal printer use console port
2) DC Power in.
3) Power on/off switch.

Install QR Code thermal printer

Behind the printer connection functions support USB / console / RJ-45 /RJ-11 and Power.
As follows



PS. Connect the controller only need to use RJ-45 and power.

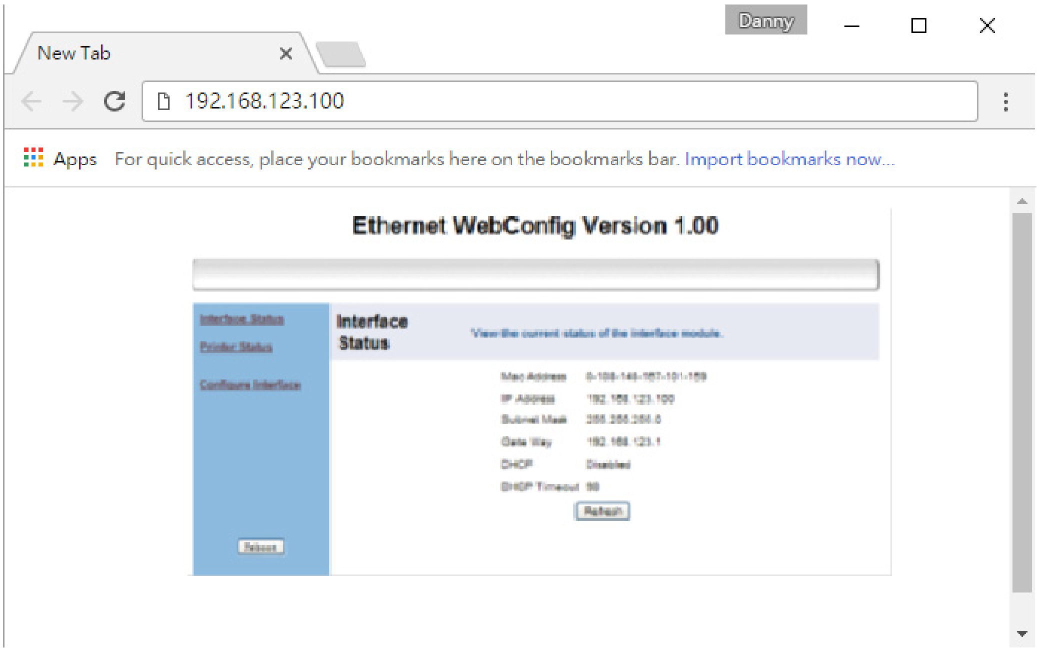


# Login web page for QR Code printer.

The QR Code printer support web management interface, administrator can login web page and modify IP address for the QR Code printer.

QR Code Printer default IP address: **192.168.123.100**

As follows


Danny
New Tab
192.168.123.100
Apps
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

Ethernet WebConfig Version 1.00

Interface Status
Printer Status
Configure Interface

Interface Status

View the current status of the interface module.

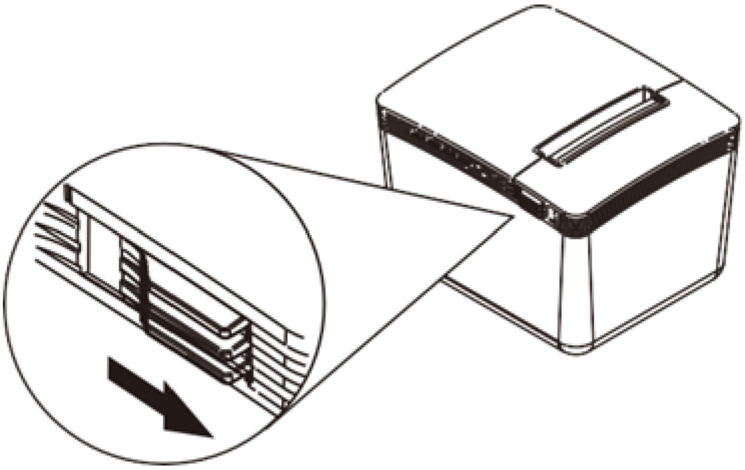
Mac Address	0-108-140-157-101-159
IP Address	192.168.123.100
Subnet Mask	255.255.255.0
Gate Way	192.168.123.1
DHCP	Disabled
DHCP Timeout	60

Refresh

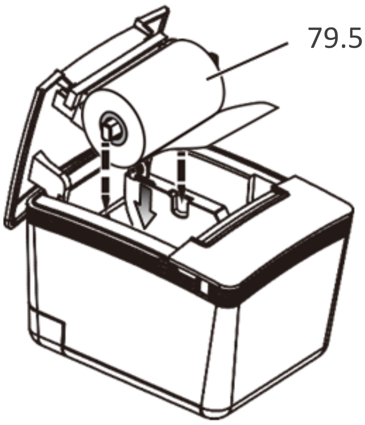
Reboot

# Install or Replace Paper Roll for QR code printer

1) Pull the Cover Release Button to open the Cover.



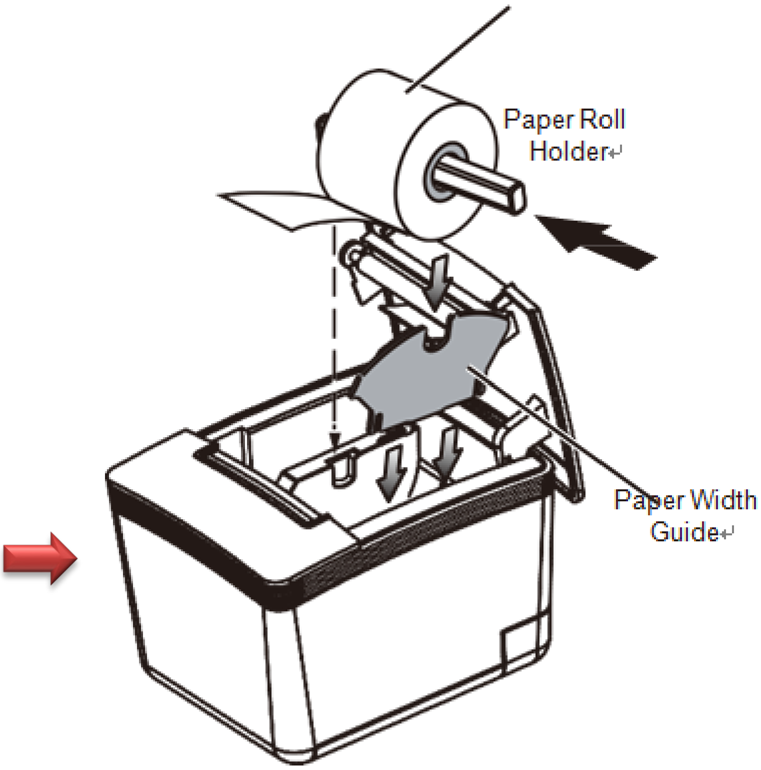
2) Roll out and install the Paper Roll with Holder into the Printer. (with the edges of the paper roll holder fitted onto the holder slots)



79.5mm size for thermal paper

57.5mm size for thermal paper

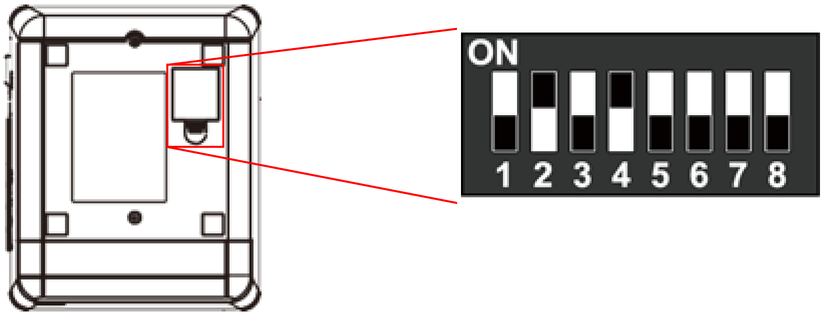
When using a paper roll in smaller width, install the Paper Width Guide first, and then install the paper roll with holder.



3) Please close the lid for thermal printer.

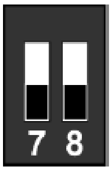
# DIP Switch Setting for QR code Printer

DIP Switch in printer bottom.

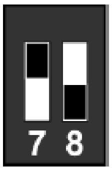


DIP	Function	ON	OFF
1	Paper Cutter	No	Yes*
2	Audio Alarm	Yes *	No
3	Print Density	Dark	Light *
4	Two-byte Character Code	*No	Yes
5	Character Per Line	42	48 *
6	Cutter with Cash Drawer	Yes	No *
7 & 8	Baud Rate Setting	---	OFF*

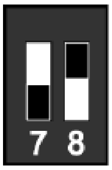
# Baud Rate Setting (DIP 7, DIP 8)



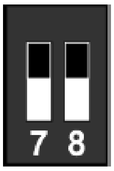
19200
(*Default)



9600



115200



38400

Set web authentication steps for POS system

Cerio’s Web Authentication System consists of the controller and SP-800 + Printer; administrator can use SP-800 remote control Cerio’s controller to create an account and print out.
The architecture can refer to “**POS system application**” description

Set web authentication steps, as follows

(Take Cerio’s DR-3000 as the case)

Steps1

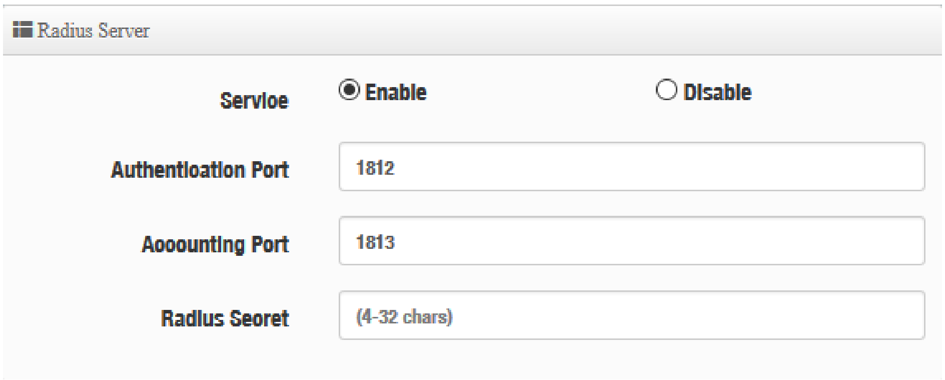
Login SP-800 web interface to set IP address and set same network segment
You can refer to “Login management interface for SP-800”

Steps2

If SP-800 with QR code Printer, administrator must set IP address for QR code Printer (same network segment for your network). You can refer to “Install QR Code printer”

Steps3

Login Cerio’s Controller “DR-3000” page (Refer controller user manual) to enable RADIUS Server.
As follows
Please click menu **“Account”➔”RADIUS Server”** for Cerio’s DR-3000

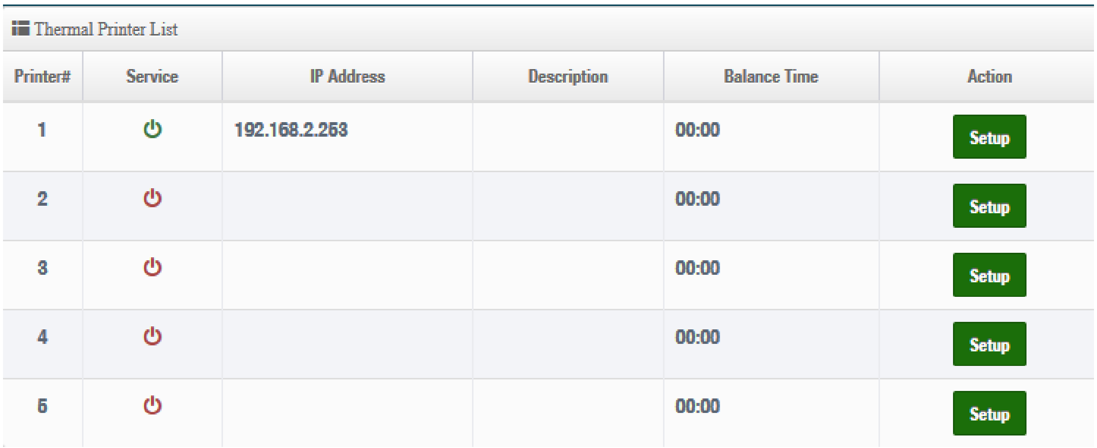


Radius Server

Servloe	● Enable	○ Dlsable
Authentloatlon Port	1812	
Aoooountlng Port	1813	
Radlus Seoret	(4-32 chars)	

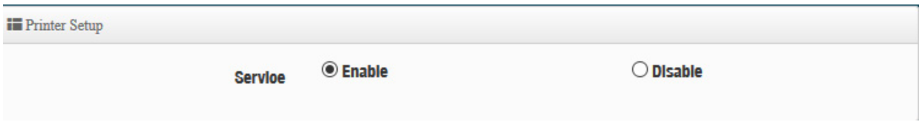
Steps4

Set the connection between DR-3000 and SP-800. Please click menu **“Account”➔**” **Thermal Printer Setup**” to enable function, as follows



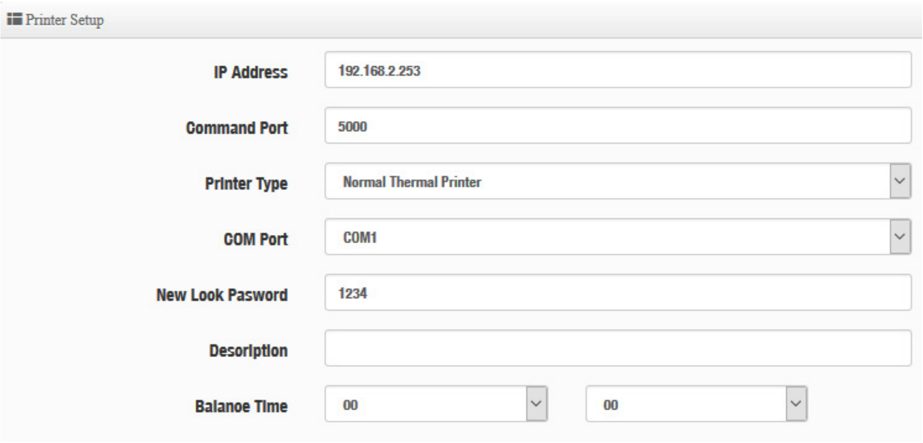
Thermal Printer List

Printer#	Service	IP Address	Description	Balance Time	Action
1	⏻	192.168.2.253		00:00	Setup
2	⏻			00:00	Setup
3	⏻			00:00	Setup
4	⏻			00:00	Setup
5	⏻			00:00	Setup



Printer Setup

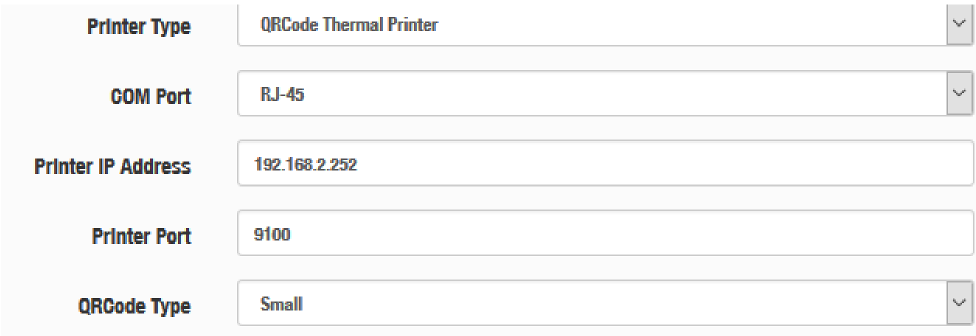
Service ● Enable ○ Disable



Printer Setup

IP Address	192.168.2.253
Command Port	5000
Printer Type	Normal Thermal Printer
COM Port	COM1
New Look Pasword	1234
Description	
Balance Time	00 00

- ➢ **IP address:** Please enter IP address for SP-800 (You can refer to Login SP-800)
- ➢ **Command port:** Please enter Command for SP-800 (You can refer to Login SP-800)
- ➢ **Printer Type:** Administrator can select Printer for normal or QR Code Printer.
- ● **QR code Printer**：If select QR Code printer, administrator must choose use connection for IP address or com Port.(Recommend use IP address manner.)



Printer Type	QRCode Thermal Printer
COM Port	RJ-45
Printer IP Address	192.168.2.252
Printer Port	9100
QRCode Type	Small

- ✓ **Printer IP Address**：Please enter IP address for QR code printer. (You can refer to Install QR Code Printer).
- ✓ **Printer Port**：Please enter command port for QR Code Printer. (You can refer to Install QR Code Printer)
- ✓ **QR Code Type**：Administrator can select print out size for QR code.
- ➢ **COM Port:** Please select connection type for printer.

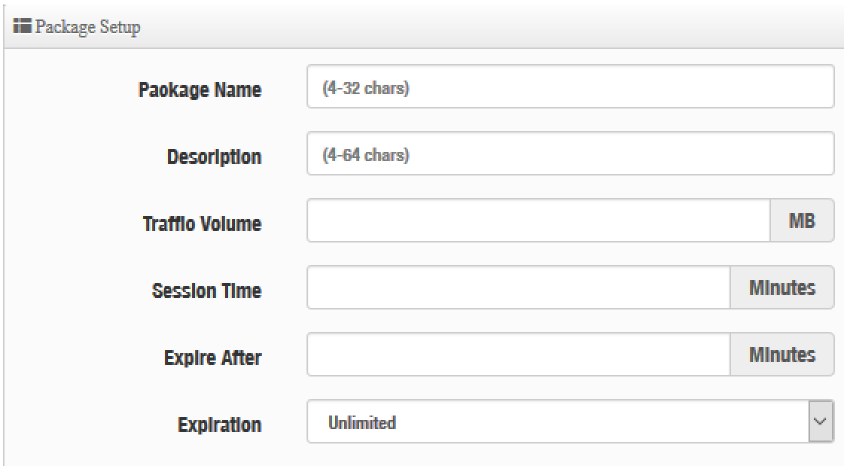
Notice

1. **If use normal thermal printer and connect to com1 port of the SP-800, please select COM1**
2. **If use QR Code Printer, please select RJ-45**

- ➢ **New Lock Password**：Enter pass key of the DR-3000 to connect SP-800
- ➢ **Description**：Administrator can enter description.

Steps5

Setup internet time rules for package authentication type (DR-3000). Please click menu "**Account**" ➔ "**Package setup**". As follows

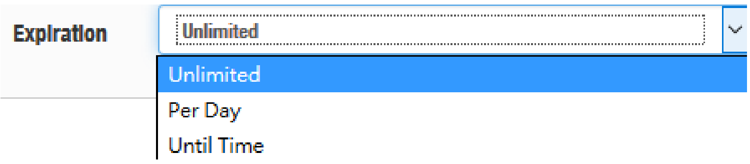


Package Setup

Paokage Name	(4-32 chars)
Desorlption	(4-64 chars)
Traffio Volume	MB
Sesslon Time	Mlnutes
Explre After	Mlnutes
Explratlon	Unlimited

- ➢ **Package Name:** Administrator can set Identify name for the package rules.
- ➢ **Description**: Administrator can set the description for package rules.
- ➢ **Traffic Volume:** Administrator can set authentication account use traffic limit for the package rules.
- ➢ **Session Time:** Administrator can set authentication account use session limit for the package rules. (After the account is signed in, the system will begin counting until the set time is used up. The counting will stop when users log out, and begin counting again once the user signs back in.)
- ➢ **Expire After:** Administrator can set authentication account use how many hours expire.(After the account is signed in, the system start counted time until the end time.)

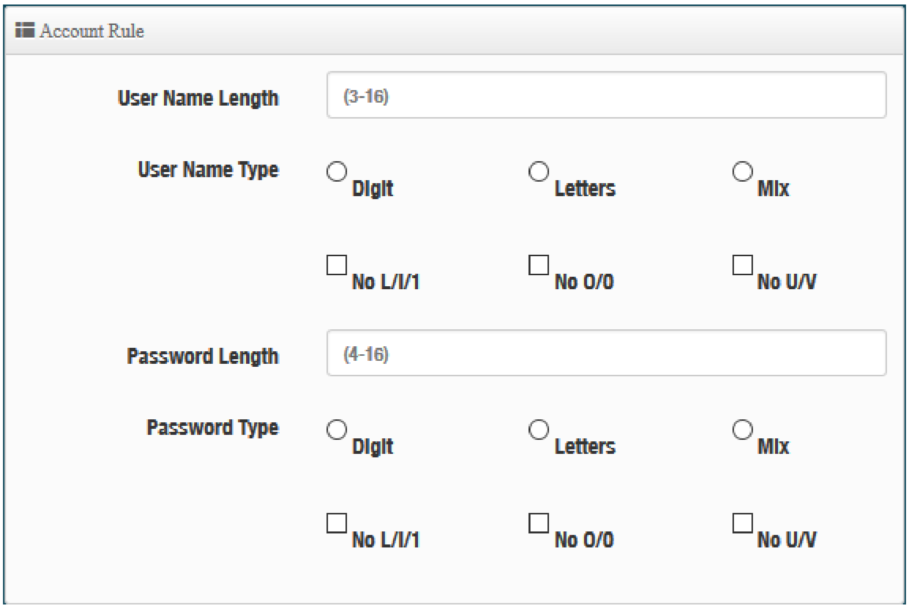
- **Expiration**: Administrator can select Unlimited or Per Day or Until Time.



Expiration: Unlimited

Unlimited
Per Day
Until Time

- ✓ **Unlimited:** After the account is signed in, the system does not count the time
- ✓ **Per Day:** After the account is signed in, the system start counted time until the end time.
- ✓ **Until Time**: After the account is signed in, the system will begin counting until the set time is used up. The counting will stop when users log out, and begin counting again once the user signs back in.



Account Rule

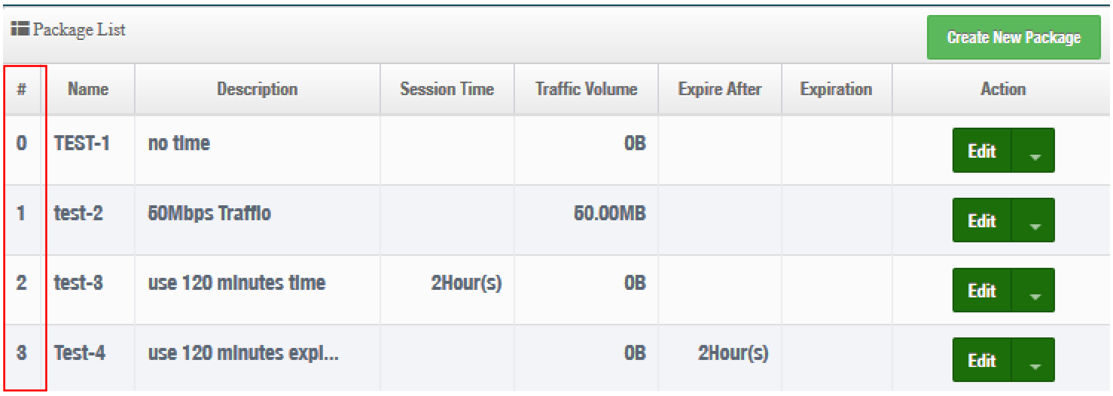
User Name Length: (3-16)

User Name Type: ○ Digit ○ Letters ○ Mix
□ No L/I/1 □ No O/0 □ No U/V

Password Length: (4-16)

Password Type: ○ Digit ○ Letters ○ Mix
□ No L/I/1 □ No O/0 □ No U/V

PS. Package list (0~9) is Network control server (SP-800) code, administrator can choose number to print out account.



Package List

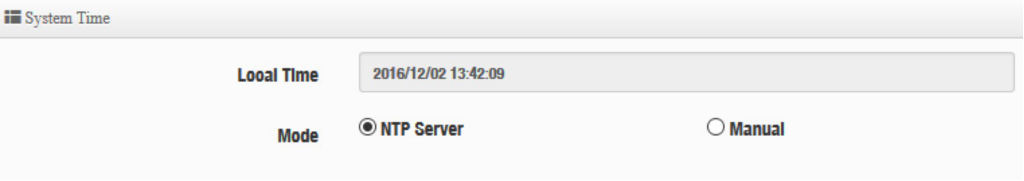
Create New Package

#	Name	Description	Session Time	Traffic Volume	Expire After	Expiration	Action
0	TEST-1	no time		0B			Edit
1	test-2	50Mbps Traffic		50.00MB			Edit
2	test-3	use 120 minutes time	2Hour(s)	0B			Edit
3	Test-4	use 120 minutes expi...		0B	2Hour(s)		Edit

Steps6

The system time is very important, administrator must set system time is right. Please click DR-3000 menu “**System**”➔”**Time Server**” to set system time.

PS. Recommend select update the system time for the NTP Server



System Time

Looal Time	2016/12/02 13:42:09
Mode	● NTP Server ○ Manual

The above procedure will complete the DR-3000 setting

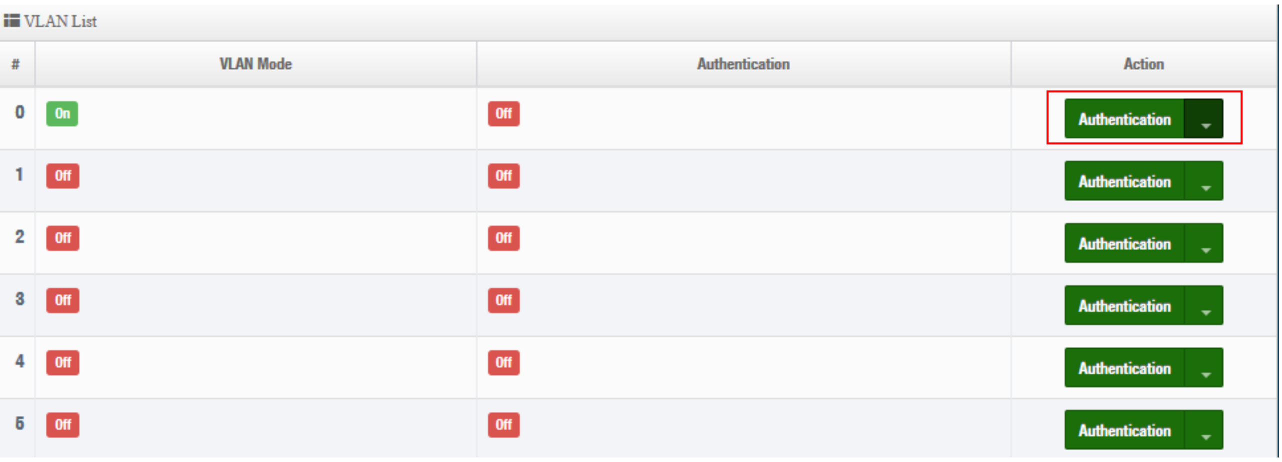
# Enable Web authentication for Access Point

Hot spots web authentication architecture must be with combine Cerio's CenOS5.0 access point. As follows

Steps7

Enable Web authentication for Cerio’s CenOS5.0 Access Point. (You can refer user manual for Access Point), As follows for Cerio’s Access Point.

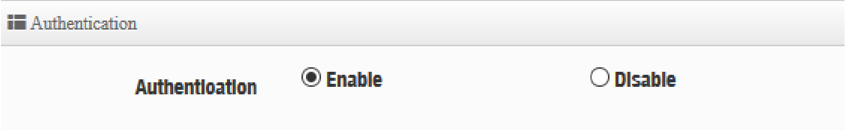
1) Enables web authentication function. Please click “System”➔”Authentication” for Cerio’s Access Point.



VLAN List

#	VLAN Mode	Authentication	Action
0	On	Off	Authentication
1	Off	Off	Authentication
2	Off	Off	Authentication
3	Off	Off	Authentication
4	Off	Off	Authentication
5	Off	Off	Authentication

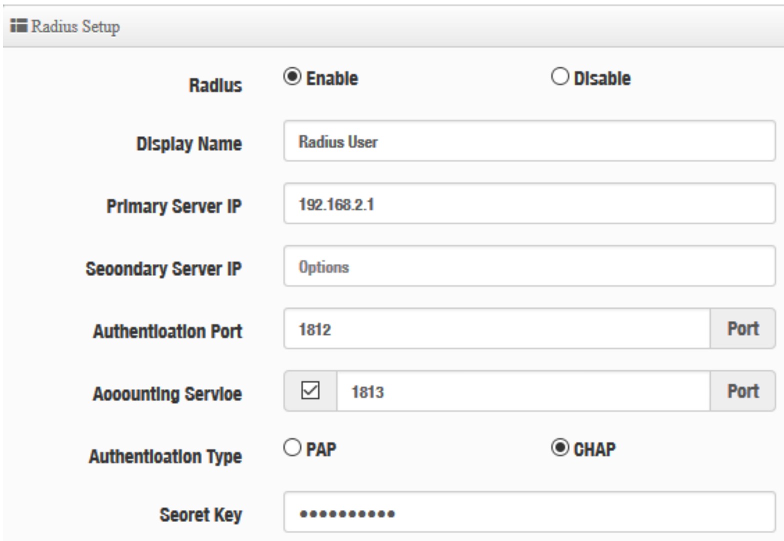
2) Click Authentication button and enable the function.



Authentication

Authentloatlon	● Enable ○ Dlsable

3) Enable authentication for RADIUS Server and set IP address for DR-3000.



Radius Setup

Radius	● Enable	○ Disable
Display Name	Radius User	
Primary Server IP	192.168.2.1	
Secondary Server IP	Options	
Authentication Port	1812	Port
Accounting Service	☑ 1813	Port
Authentication Type	○ PAP	● CHAP
Secret Key	••••••••••	

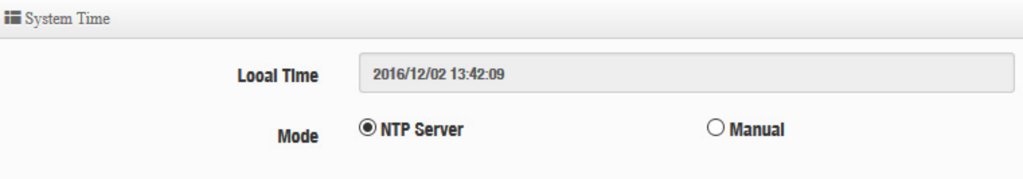
Steps8

Set system time for Cerio's Access Point. Please click menu "System"➔"Time server".

Steps9

The system time is very important, administrator must set system time is right. Please click (Cerio's Access Point) menu "**System**"➔"**Time Server**" to set system time.

PS. Recommend select update the system time for the NTP Server



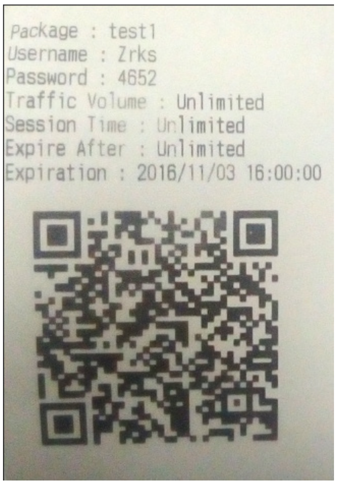
System Time

Local Time	2016/12/02 13:42:09	
Mode	● NTP Server	○ Manual

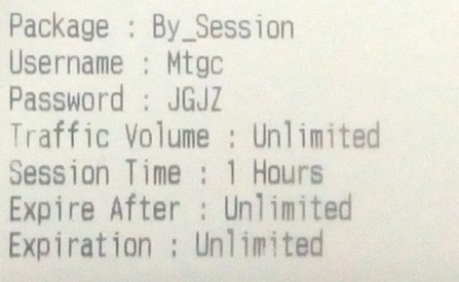
This completes all architecture settings

Administrator can click SP-800 "Print" button will print account and password of the tickets.

As follows



```
Package : test1
Username : Zrks
Password : 4652
Traffic Volume : Unlimited
Session Time : Unlimited
Expire After : Unlimited
Expiration : 2016/11/03 16:00:00
```



```
Package : By_Session
Username : Mtgc
Password : JGJZ
Traffic Volume : Unlimited
Session Time : 1 Hours
Expire After : Unlimited
Expiration : Unlimited
```