



DG-WU2008

User Manual

V1.0

2020-1-13

As our products undergo continuous development the specifications are subject to change without prior notice

COPYRIGHT

Copyright 2020 by Digisol Systems Ltd. All rights reserved.

Company has an ongoing policy of upgrading its products and it may be possible that information in this document is not up-to-date.

Please check with your local distributors for latest information. No part of this document can be copied or reproduced in any form without written consent from the company.

Trademark

DIGISOL™ is a trademark of Digisol Systems Ltd. All other trademarks are the property of the respective manufacturers.

☎ 1800-209-3444 (Toll Free)

✉ helpdesk@digisol.com sales@digisol.com www.digisol.com 2

Table of Contents

CHAPTER 1 INTRODUCTION	6
1.1 OVERVIEW	6
1.2 GET FAMILIAR WITH YOUR NEW CONTROLLER.....	7
1.3 PACKAGE CONTENT	7
CHAPTER 2: HARDWARE INTRODUCTION.....	8
HARDWARE:	8
CHAPTER 3: LOGIN WEB NETWORK MANAGEMENT.....	9
CHAPTER 4: WEB GUI CONFIGURATION.....	10
4.1 SYSTEM STATUS.....	10
4.1.A DEVICE INFO	10
4.1.B INTERFACE STATUS	11
4.1.C LAN IP FLOW	12
4.1.D APPLICATION FLOW	12
4.2 NETWORK CONFIGURE	13
4.2.A INTERFACE CONFIGURE	13
4.2.A.1 WAN CONFIGURE	13
4.2.A.2 LAN / DHCP	14
4.2.A.3 PHYSICAL PORT DEFINITION.....	15
4.2.A.4 SUBINTERFACE CONFIGURE.....	15
4.2.B ROUTE RULE	16
4.2.B.1 MULTI-LINE DEVERSATION RULES	16
4.2.B.2 STATIC ROUTE	17
4.2.B.2.1 STATIC ROUTING.....	17
4.2.B.2.2 ROUTING INFORMATION.....	17
4.2.C DDNS	18
4.2.D NAT/ PORT FORWARDING	19
4.2.D.1 PORT FORWARDING	19
4.2.D.2 DMZ HOST	20
4.2.D.3 SRC NAT	20
4.2.D.4 DST NAT	21
4.3 FLOW CONTROL POLICY.....	21
4.3.1 SMART FLOW CONTROL	21
4.3.2 BANDWIDTH CONTROL.....	22
4.3.3 FREE FLOW CONTROL.....	22
4.4 AC MANAGEMENT	23
4.4.1 AP LIST.....	23
4.4.2 AP CONFIGURE TEMPLATE	25
4.4.3 AP UPGRADE	26

4.5 AUTH INTERNET ACCESS	27
4.5.1 AUTH CONFIGURE.....	27
4.5.1.A PPPoE AUTHENTICATION.....	27
4.5.1.B PORTAL AUTHENTICATION.....	29
4.5.1.C IP AUTHENTICATION	31
4.5.1.D MAC AUTHENTICATION	32
4.5.1.E RADIUS BILLING.....	32
4.5.1.F NOTIFY PAGE.....	33
4.5.2 USER MANAGEMENT.....	33
4.5.2.A AUTH USER.....	33
4.5.2.B AUTH USER STATUS.....	34
4.5.2.C DEPARTMENT/ LEVEL DEFINITION	35
4.6 BEHAVIOR CONTROL.....	36
4.6.1 APPLICATION FIREWALL.....	36
4.6.2 URL REDIRECT	37
4.6.3 DOMAIN REDIRECT.....	37
4.6.4 MESSAGE PUSH CONFIGURE	38
4.7 OBJECT MANAGEMENT	39
4.7.1 BASIC OBJECT	39
4.7.1.A TIME OBJECT.....	39
4.7.1.B SOURCE IP OBJECT.....	39
4.7.1.C PORT OBJECT.....	40
4.7.1.D DESTINATION IP OBJECT	40
4.7.2 APPLICATION OBJECT	41
4.7.2.1 BUILT-IN APPLICATION OBJECT	41
4.7.2.1.A BUILT-IN APP OBJECT UPGRADE	41
4.7.2.1.B BUILT-IN APP OBJECT	41
4.7.2.2 CUSTOM APPLICATION OBJECT.....	42
4.7.2.2.A CUSTOMIZE APP OBJECT	42
4.7.2.2.B DEFINE APP BY DOMAIN	42
4.7.2.2.C DEFINE APP BY OBJECTIVE IP + PORT.....	43
4.8 SAFETY PROTECTION	43
4.8.1 IP-MAC BINDING	43
4.8.2 CONNECTION QUANTITY LIMIT.....	44
4.8.3 LAN ABNORMAL DETECTION.....	44
4.8.4 LAN ATTACK PROTECTION	45
4.8.5 WAN PING FORBID/ WAN LOGIN	45
4.9 LOG RECORD	46
4.9.1 LOG PARAMETERS	46
4.9.2 USER AUTH LOG.....	46
4.9.3 ONLINE USER LOG.....	47
4.9.4 INTERFACE FLOW LOG.....	47
4.9.5 SYSTEM LOG	48
4.10 VPN	48

4.10.1 PPTP.....	48
4.10.1.A PPTP VPN SERVER	48
4.10.1.B PPTP VPN ACCESS STATUS.....	49
4.10.2 L2TP.....	50
4.10.2.A L2TP VPN SERVER	50
4.10.2.B L2TP VPN ACCESS STATUS.....	51
4.10.3 VTUNS	51
4.10.3.1 VTUNS CONFIGURE	51
4.10.3.1.A PARAMETER SETTINGS	51
4.10.3.1.B TUNNEL MANAGEMENT.....	52
4.10.3.2 VTUNS STATUS.....	53
4.11 BPN (THIS FEATURE IS FOR FUTURE USE).....	53
4.11.A BPN SERVER.....	53
4.11.B BPN ACCESS STATUS.....	54
4.12 DEVICE MAINTENANCE	54
4.12.A FIRMWARE UPGRADE	54
4.12.B MODIFY PASSWORD.....	55
4.12.C PING DETECTION.....	55
4.12.D CONFIGURE FILE MAINTENANCE	56
4.12.E RESTART DEVICE.....	57
4.12.F TIMED TASK	58
4.12.G TIME SYNCHRONIZATION.....	58
4.12.H CLOUD CONFIGURE (FOR FUTURE USE).....	59
CHAPTER 5 TROUBLESHOOTING.....	60
1 WHY CAN'T I CONFIGURE THE CONTROLLER EVEN WHEN THE CABLE IS PLUGGED AND THE LED IS LIT?	60
2 WHAT CAN I DO IF MY ETHERNET CONNECTION DOES NOT WORK PROPERLY?	62

Chapter 1 Introduction

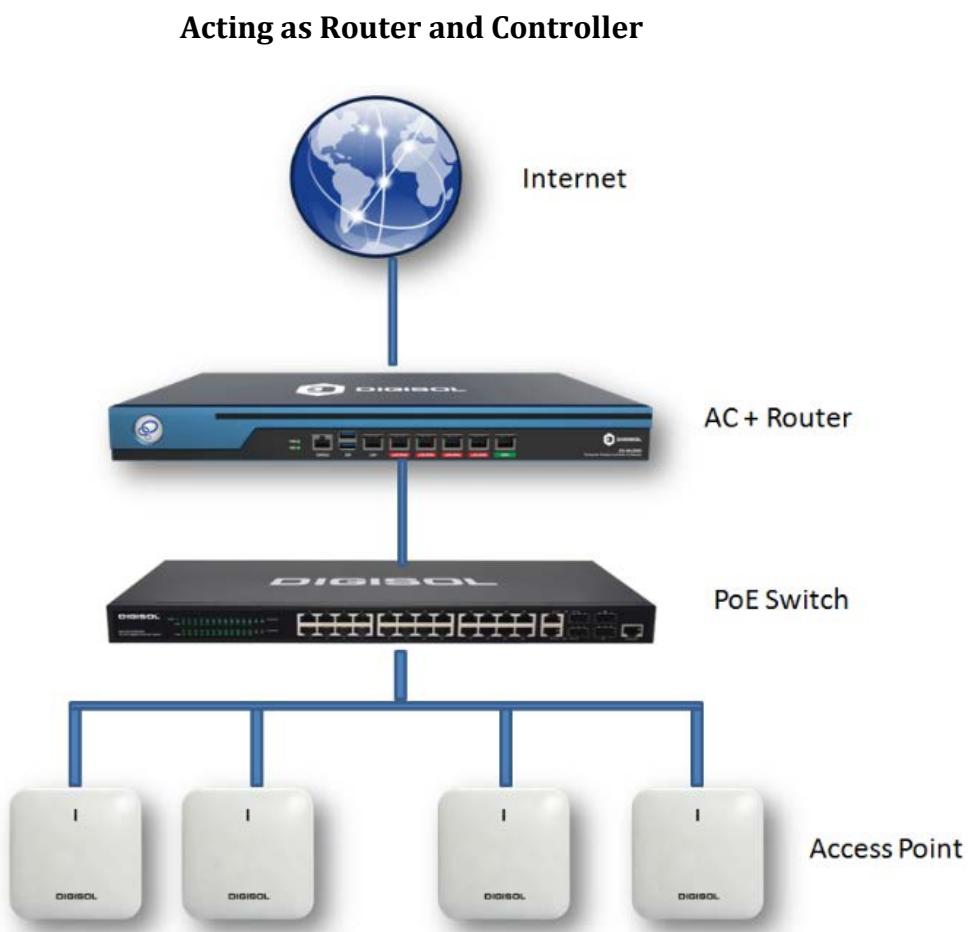
1.1 Overview

DG-WU2008 is a CAPWAP based WLAN Controller with main functions as Router, AC Controller, Management, VLAN Management functions.

When worked as a router, it can access into 512 end users, to do advertisement and captive portal authentication.

When worked as a controller, it can manage 512 nos FIT wireless access points.

The network connectivity will be as shown below:



☎ 1800-209-3444 (Toll Free)

✉ helpdesk@digisol.com ⏰ sales@digisol.com 🌐 www.digisol.com

1.2 Get Familiar with your new Controller

1. Connect the controller with computer by wired connection.
2. The default IP address of this controller is 172.16.0.1. By default DHCP Server is enabled only on LAN1 port (172.16.0.x/ 255.255.0.0).

This controller has individual IP address on each LAN port. For first time installation, connect PC to LAN1 port of controller. Default username/ password is admin/ admin.

1.3 Package Content

- DG-WU2008 Wireless Controller and Gateway
- Power Cord
- Quick Installation Guide
- Installation Guide CD (includes User Manual / QIG)
- Patch Cord (1 No.)
- Console Cable
- Rack Mounting Kit
- Earthing/Grounding Wire.

Chapter 2: Hardware Introduction

Hardware:



WAN1: WAN Port in Default mode.

WAN2/LAN5; WAN3/LAN4; WAN4/LAN3, LAN2: LAN Ports in default mode, but can set up as WAN ports in gateway operation mode based on requirement.

LAN1: LAN Port as default

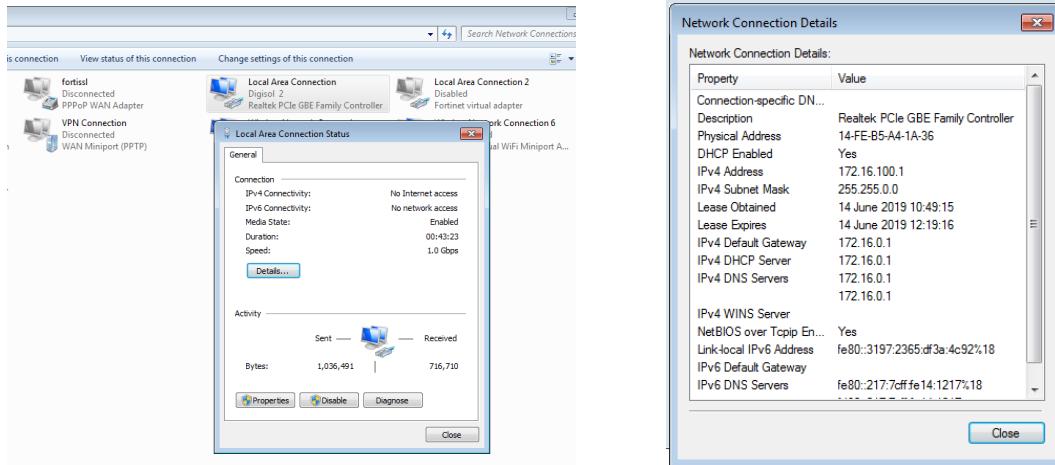
CONSOLE: Serial port

USB: Two for USB flash & USB keyboard, mainly to upgrade system.

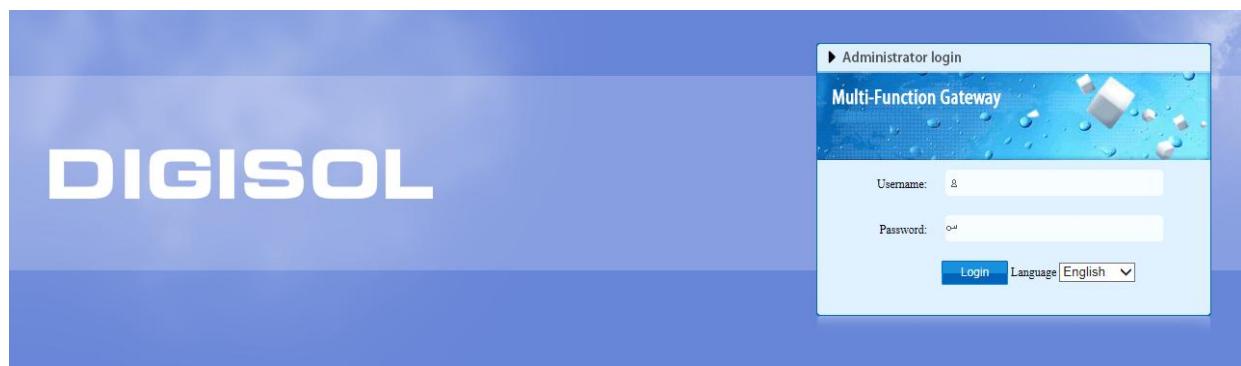
Power: To power ON the device, Power LED indicator will be on;

Chapter 3: Login Web Network Management

The default IP address of device is 172.16.0.1. Connect the PC to controller & PC will obtain the IP address directly from AC controller DHCP server.



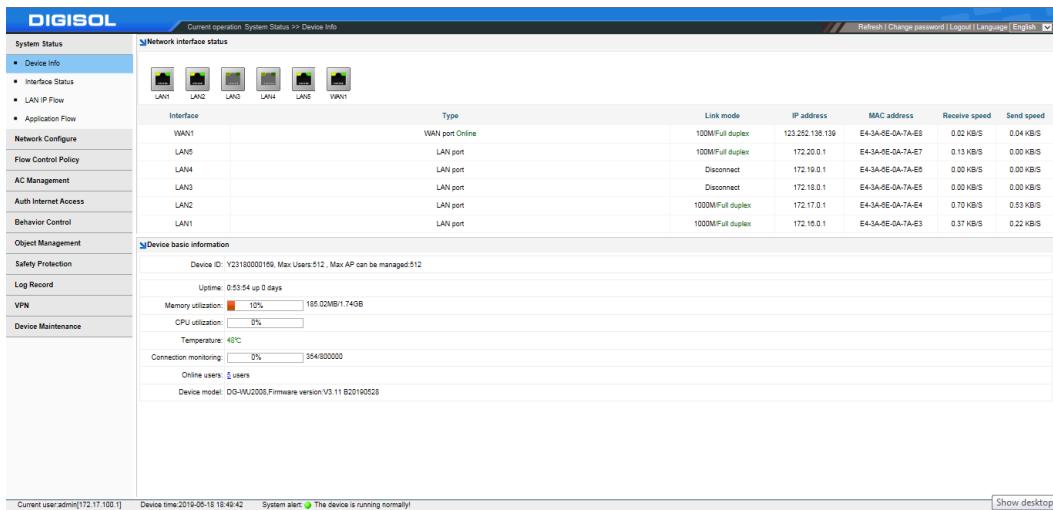
Input AC Controller's IP address **http://172.16.0.1:2011** into browser. It will display the below page.



Input username/ password as admin/ admin.

Chapter 4: WEB GUI Configuration

After logged into AC controller, following home page will be displayed:



The screenshot shows the DIGISOL DG-WU2008 Web GUI. The left sidebar contains navigation links: System Status, Device Info (selected), Interface Status, LAN IP Flow, Application Flow, Network Configure, Flow Control Policy, AC Management, Auth Internet Access, Behavior Control, Object Management, Safety Protection, Log Record, VPN, and Device Maintenance. The main content area has two tabs: 'Network interface status' and 'Device basic information'. The 'Network interface status' tab displays a table of interface ports (WAN1, LAN1, LAN2, LAN3, LAN4, LAN5, VANT) with their types (WAN port Online, LAN port), link modes (100M/Full duplex), IP addresses (e.g., 123.252.156.139, 172.20.0.1), MAC addresses (e.g., E4-3A-8E-0A-7A-E8, E4-3A-8E-0A-7A-E7), receive speeds (e.g., 0.02 kB/s, 0.13 kB/s), and send speeds (e.g., 0.04 kB/s, 0.00 kB/s). The 'Device basic information' tab shows device details: Device ID (Y23180000156), Max Users (512), Max AP can be managed (512), Uptime (0:53:54 up 0 days), Memory utilization (10%), CPU utilization (0%), Temperature (48°C), Connection monitoring (0%), and Online users (2 users). The footer shows the current user (admin), device time (2012-05-18 18:49:42), system alert (The device is running normally), and a 'Show desktop' button.

4.1 System Status

4.1.a Device Info

Display general information of Controller.

Network Interface Status: It displays the active interface port connectivity status, Link Speed, IP address, Mac Address, Receive/ Send speed.



Display Ports Status. Grayed out means nothing connected to above ports & green means connected.

Device Basic Information: Displays Device ID along with max User/ AP support detail.

It shows Device Uptime, CPU & Memory utilization, Temperature, Connection monitoring, online users, Device model & Firmware Version.

4.1.b Interface Status

Displays controller LAN/ WAN interface detail (Upstream/ Downstream bandwidth(KB), IP Address, Status, total Upstream/ downstream speed(KB/S), Flow(MB)

DIGISOL Current operation System Status >> Interface Status												
Interface status												
Line detection												
Interface name	Interface type	Upstream bandwidth(KB)	Downstream bandwidth(KB)	IP	Status	Connection quantity	Line quality	Upstream speed (KB/S)	Downstream speed(KB/S)	Total flow	downstream	Operation
LAN1	LAN port	-	-	172.16.0.1	Online	-	-	0.70	0.66	63.76MB	12.10MB	
LAN2	LAN port	-	-	172.17.0.1	Online	-	-	0.85	1.44	5.94MB	19.82MB	
LAN3	LAN port	-	-	172.18.0.1	Offline	-	-	0.00	0.00	0.00B	0.00B	
LAN4	LAN port	-	-	172.19.0.1	Offline	-	-	0.00	0.00	0.00B	0.00B	
LAN5	LAN port	-	-	172.20.0.1	Online	-	-	0.00	0.00	1.19MB	0.00B	
WAN1	Static IP	100000	100000	123.252.136.139	Online	250	No detection	0.49	1.03	8.49MB	22.16MB	

If you click Operation icon, it will display the respective interface detail as shown below:

DIGISOL Current operation System Status >> Interface Status												
Interface status												
Line detection												
Interface name	Interface type	Upstream bandwidth(KB)	Downstream bandwidth(KB)									
LAN1	LAN port	-	-									
LAN2	LAN port	-	-									
LAN3	LAN port	-	-									
LAN4	LAN port	-	-									
LAN5	LAN port	-	-									
WAN1	Static IP	100000	100000									
Interface details												
Interface name: WAN1												
Interface status: Enable												
Interface type: Ethernet port, Static IP												
Operation mode: 100Mbps Full duplex												
TCP/IP: 1350												
MTU: 1500												
MAC: E4-3A-0E-0A-7A-08												
IP address: 123.252.136.139												
Netmask: 255.255.255.248												
Default gateway: 123.252.136.137												
DNS server: 8.8.8.8, 4.2.2.3												
Online time: 11:30:48 up 8 days												
Line detection: Disable												
Smart QoS: Enable												
Bandwidth setting: 100000 / 100000												
Line package loss rate: 0												
Line delay: 0												
Line quality: No detection												

Line Detection

You can check the configured WAN connectivity under this option

DIGISOL Current operation System Status >> Interface Status												
Interface status												
Line detection												
Interface name	Interface type	Upstream bandwidth	Downstream bandwidth									
LAN1	LAN port	-	-	WAN detection								
LAN1.10(802.1Q)	LAN port	-	-	Detect all lines Detection IP:	(The default detection IP is 114.114.114.114)							
LAN1.11(MAC-VLAN)	LAN port	-	-	Line	Detection WAN2							
LAN2	LAN port	-	-		Detection WAN1							
LAN2.20(802.1Q)	LAN port	-	-									
LAN2.21(MAC-VLAN)	LAN port	-	-									
LAN3	LAN port	-	-									

1800-209-3444 (Toll Free)

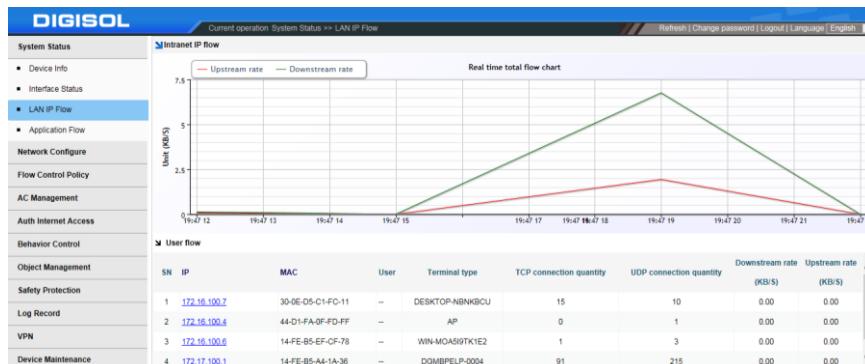
helpdesk@digisol.com

sales@digisol.com

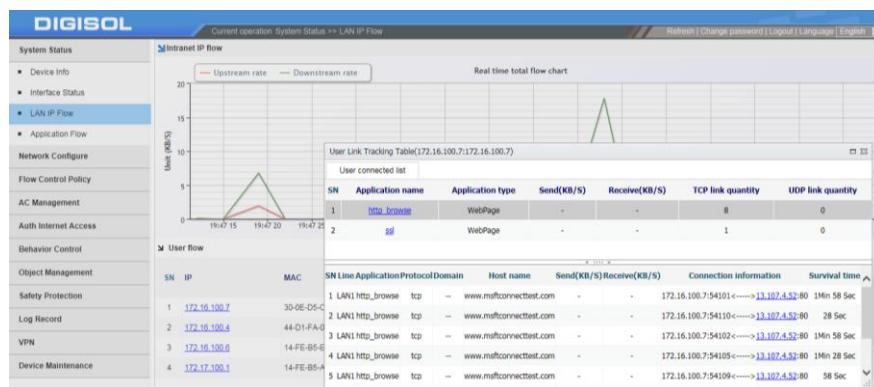
www.digisol.com

4.1.c LAN IP Flow

You can view the connected User sessions under this option.

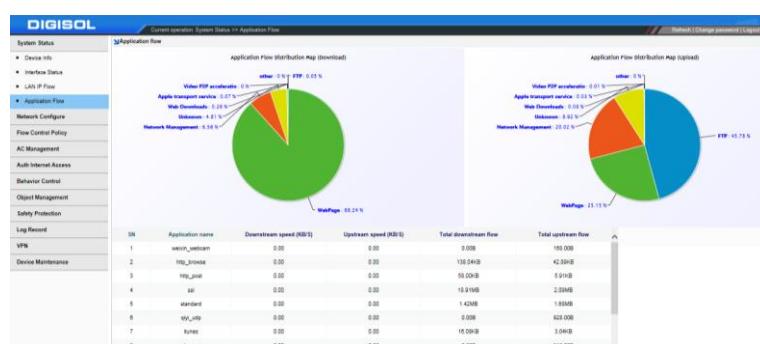


Click on desired User IP address to view the session logs:



4.1.d Application Flow

Display the user running applications flow chart.



 1800-209-3444 (Toll Free)

 helpdesk@digisol.com

 sales@digisol.com

 www.digisol.com

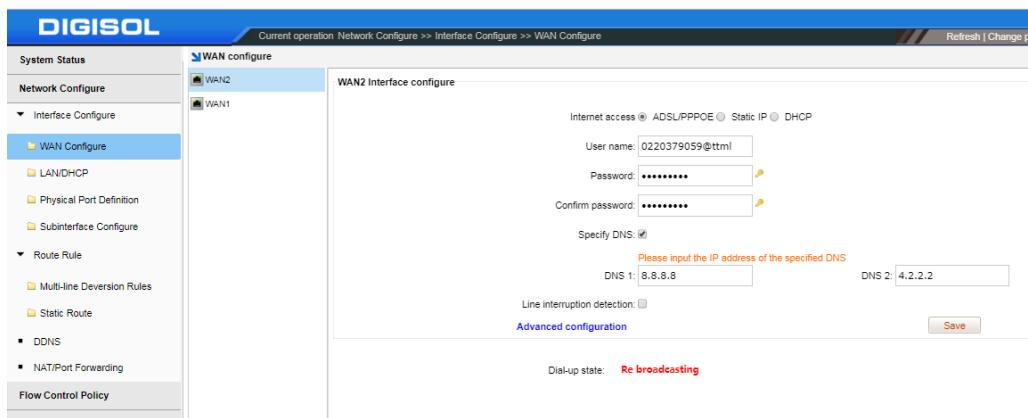
4.2 Network Configure

4.2.a Interface Configure

Under this tab you can configure WAN settings, DHCP Server configuration on each LAN port (172.x.x.x), Configurable WAN/ LAN port as per requirement & sub-interface for VLAN configuration. This tab options are described as below:-

4.2.a.1 WAN Configure

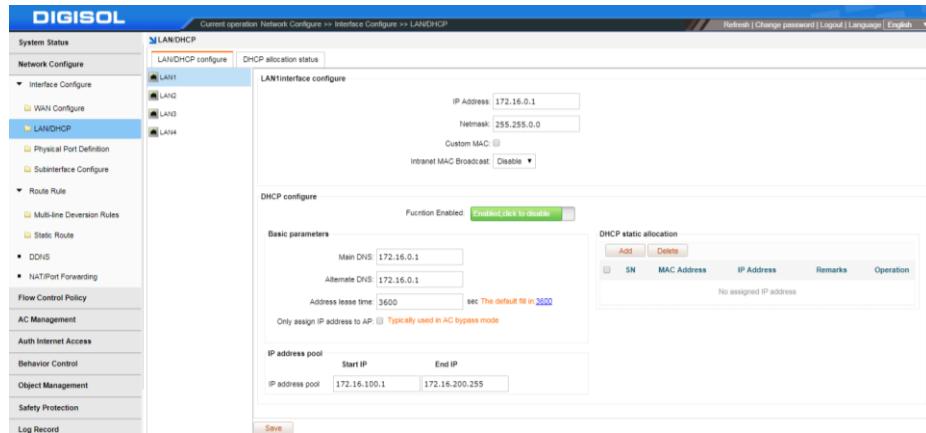
LAN1 & WAN1 are by default ports & rest all configurable into WAN/LAN ports as per customer requirement.



You can configure WAN1 in ADSL/ PPPoE, Static IP or DHCP mode as per settings provided by ISP to use it in Gateway mode.

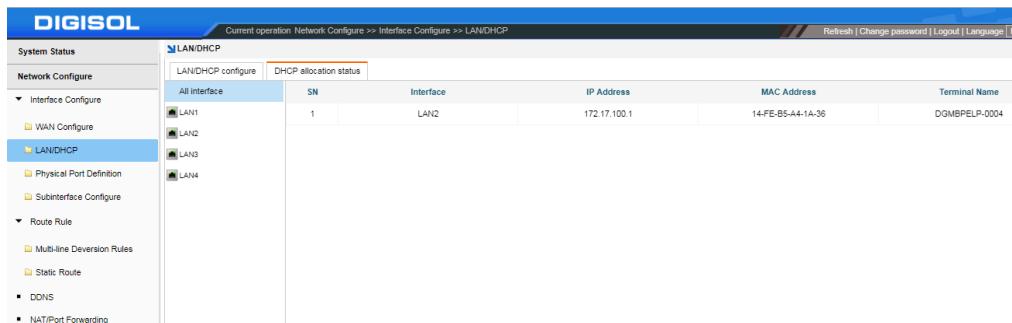
4.2.a.2 LAN/ DHCP

You can configure DHCP Server for respective LAN port under this tab. Every LAN port have different IP network. By default DHCP Server is enabled only on LAN1 interface.



Similarly, you can enable/ disable DHCP Server for other LAN interface if required.

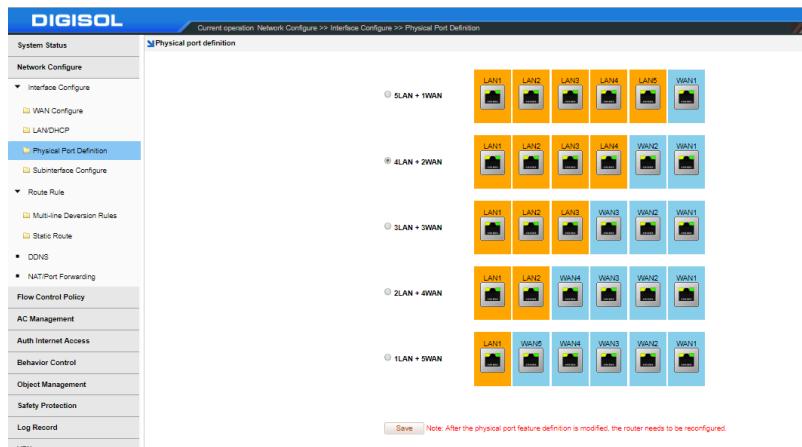
You can view the DHCP Client list of Respective LAN interface under “**DHCP Allocation Status**”.



All interface	SN	Interface	IP Address	MAC Address	Terminal Name
LAN1	1	LAN2	172.17.100.1	14-FE-B5-A4-1A-36	DGMBPELP-0004

4.2.a.3 Physical Port Definition

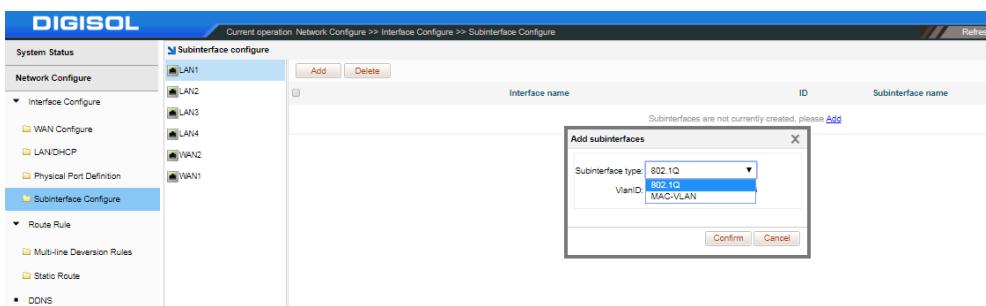
LAN1 & WAN1 are default ports. Rest all are configurable into LAN / WAN port as per the requirement. You can set desired LAN & WAN port combination under this tab.



4.2.a.4 Subinterface Configure

You can use this option to create different VLAN for connected AP or Wi-Fi Users. We can connect controller's LAN port with VLAN switch's trunk port, configure the VLAN id and associated parameters on both the devices so that the controller can manage the wireless AP under particular VLAN.

You can create sub-interface for every LAN port on this controller. Once you click **Add** tab, it will display following page:-

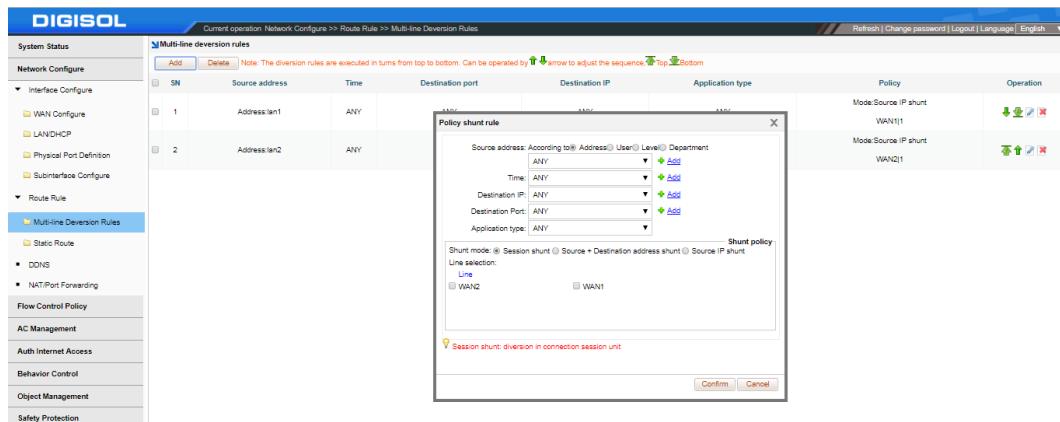


If you are using a switch with controller, you can add Subinterface type as 802.1Q else select MAC-VLAN if AP is directly terminated on controller& define VLAN ID.

4.2.b Route Rule

4.2.b.1 Multi-line Deversion Rules

You can use this option if multiple WAN is terminating on controller. You can set session shunt, source IP shunt and source IP +destination IP for some specific network traffic depending on desired WAN connection to minimize the internet utilization.



You need to create Source IP, Destination IP object under “**Object Management**” tab & map the defined object traffic to selected WAN interface.

Session Shunt:

It will divide the user's internet bandwidth as per the number of WAN terminated on controller by using this option.

Source + Destination address shunt

You can bind the source/ destination IP address to specific WAN interface to constraint the bandwidth congestion by using this option.

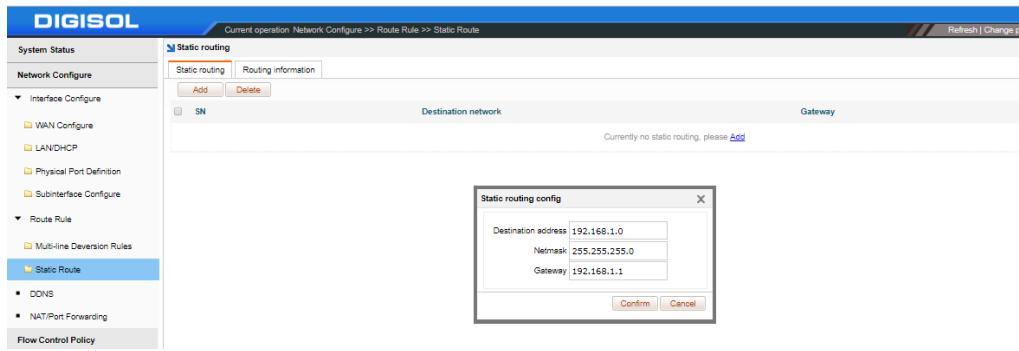
Source IP Shunt Line Selection:

You can route the user traffic through specific WAN interface by using this option.

4.2.b.2 Static Route

4.2.b.2.1 Static Routing

You can manually add static route to this device to define the path selection of traffic from one interface to another.



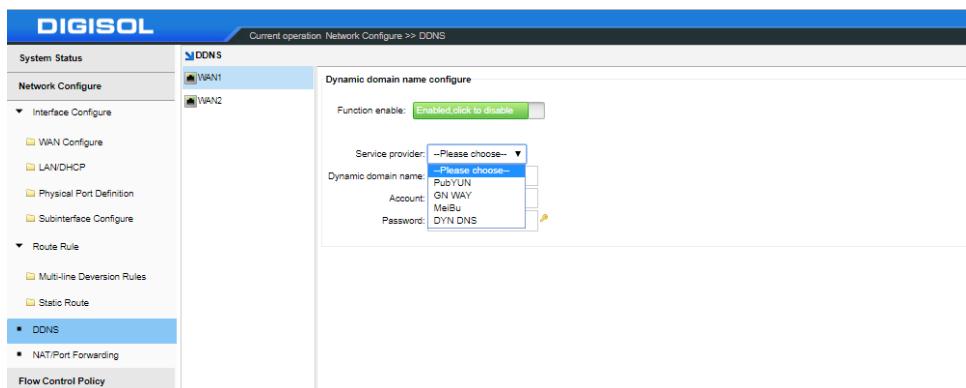
4.2.b.2.2 Routing Information

Displays the routing rule enabled on the controller under this tab.

SN	Destination address	Gateway	Interface	Routing type
1	123.252.136.130-255.255.255.248	--	WAN1	Network segment, local
2	127.0.0.0-255.0.0.0	--	WAN2	Network segment, local
3	172.18.0.0-255.255.0.0	--	LAN1	Network segment, local
4	172.17.0.0-255.255.0.0	--	LAN2	Network segment, local
5	172.18.0.0-255.255.0.0	--	LAN3	Network segment, local
6	172.19.0.0-255.255.0.0	--	LAN4	Network segment, local

4.2.c DDNS

Dynamic DNS (DDNS) is an Internet service that allows controller with varying public IP addresses to be located using Internet domain names . To use DDNS, you must setup an account with a DDNS provider such as DynDNS.org,etc. When you set up an account with a DDNS service, the host & domain name, username, password detail will be provided by the account provider.



☎ 1800-209-3444 (Toll Free)

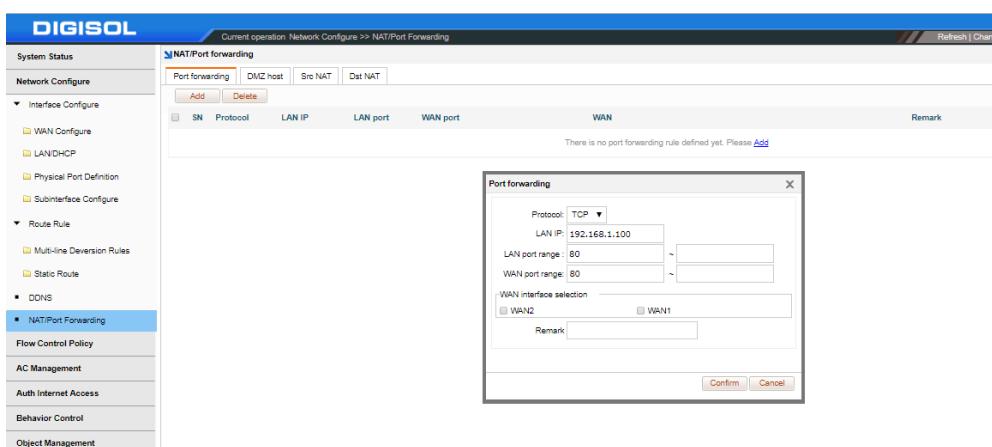
✉ helpdesk@digisol.com ☰ sales@digisol.com 🌐 www.digisol.com

4.2.d NAT/ Port forwarding

By default, the firewall of a controller blocks all connection attempts by devices on the Internet to devices in your local network. This is called inbound traffic. If you want devices on the Internet to connect to devices on your local network (for example, you have an IP Camera or an FTP server that you want to be accessible via the Internet), you will have to open the desired ports on controller.

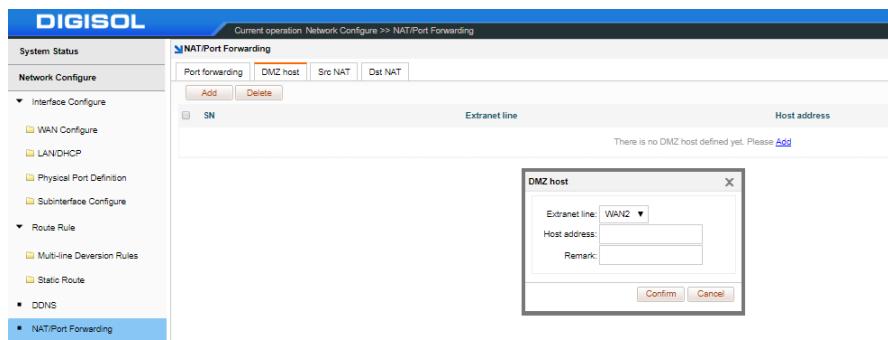
4.2.d.1 Port forwarding

Also called inbound firewall rules. You can create port forwarding rules that look into the header of each inbound packet, and either block it or forward it to specified devices on your local network, based on the source IP address, LAN/ WAN TCP port number, and other characteristics of the packet. Packets with different characteristics can be forwarded to different devices on your local network.



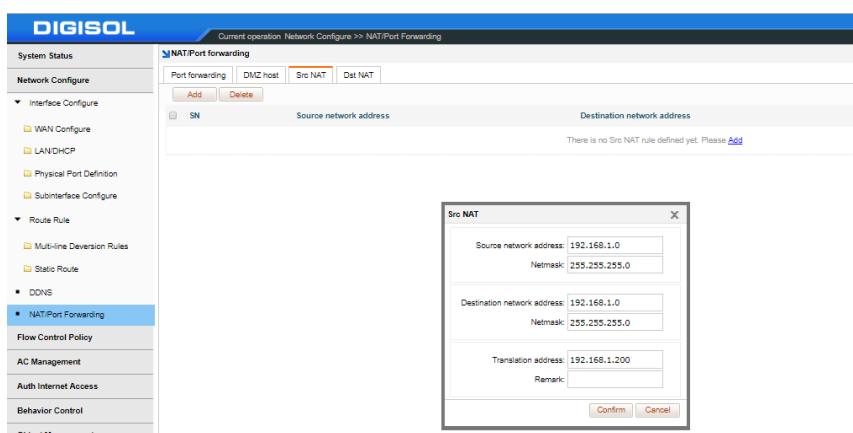
4.2.d.2 DMZ Host

If you use a DMZ to forward all inbound traffic to a device in your local network, that device loses all the protection of the device's firewall & It is totally exposed to the Internet.



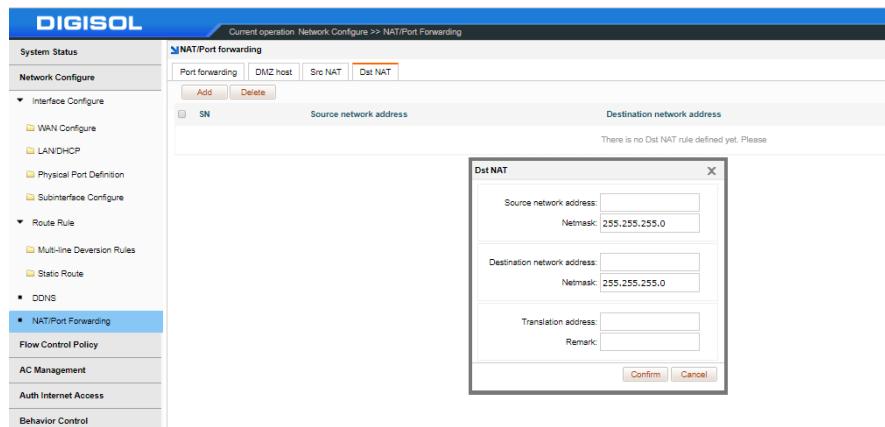
4.2.d.3 Src NAT

You can add a Source NAT rule under this tab.



4.2.d.4 Dst NAT

You can add a Destination NAT rule under this tab.

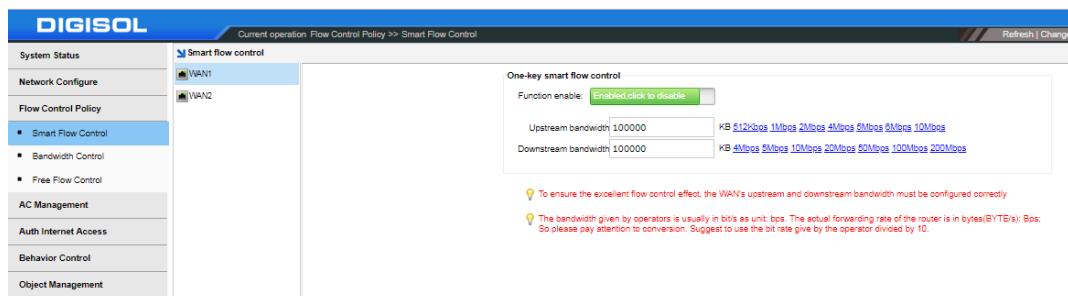


The screenshot shows the DIGISOL Web Interface with the 'NAT/Port Forwarding' tab selected. Under 'Dst NAT', there is a table with one row and columns for SN, Source network address, and Destination network address. A message at the bottom says 'There is no Dst NAT rule defined yet. Please'. A modal dialog titled 'Dst NAT' is open, containing fields for 'Source network address' (255.255.255.0) and 'Destination network address' (255.255.255.0). It also has fields for 'Translation address' and 'Remark'.

4.3 Flow Control Policy

4.3.1 Smart Flow Control

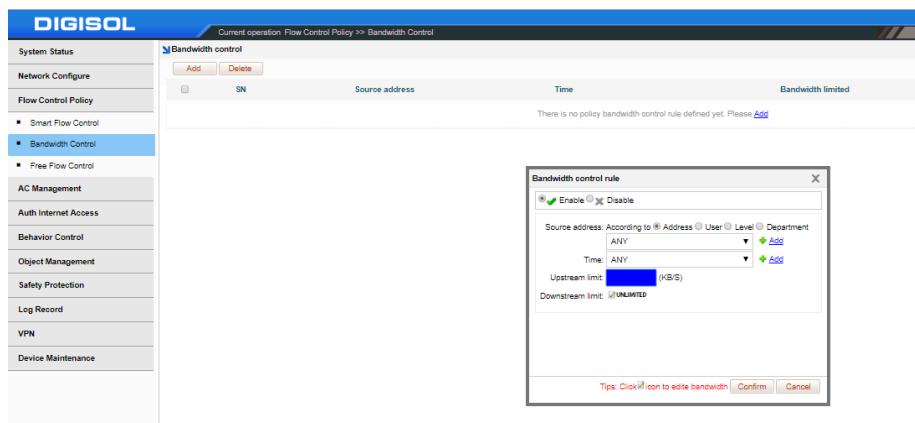
Under this tab you can set/ define bandwidth for respective WAN interface.



The screenshot shows the DIGISOL Web Interface with the 'Flow Control Policy' tab selected. Under 'Smart flow control', 'WAN1' is selected. A sub-dialog titled 'One-key smart flow control' shows 'Function enable' as 'Enabled.click to disable'. It lists 'Upstream bandwidth' (100000 KB/s) and 'Downstream bandwidth' (100000 KB/s) with dropdown menus for selection. A note at the bottom states: 'To ensure the excellent flow control effect, the WAN's upstream and downstream bandwidth must be configured correctly' and 'The bandwidth given by operators is usually in bits as unit bps. The actual forwarding rate of the router is in bytes(BYTE/s). So please pay attention to conversion. Suggest to use the bit rate give by the operator divided by 10.'

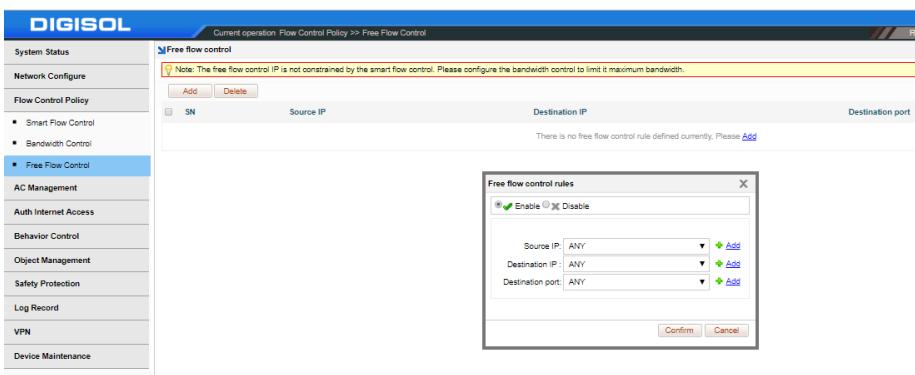
4.3.2 Bandwidth Control

You can define/ limit the bandwidth for specific Address Pool or User under this option. Set the Upstream/ Downstream limit in KB/S.



4.3.3 Free Flow Control

You can define IP pool under this tab for Free Flow control.



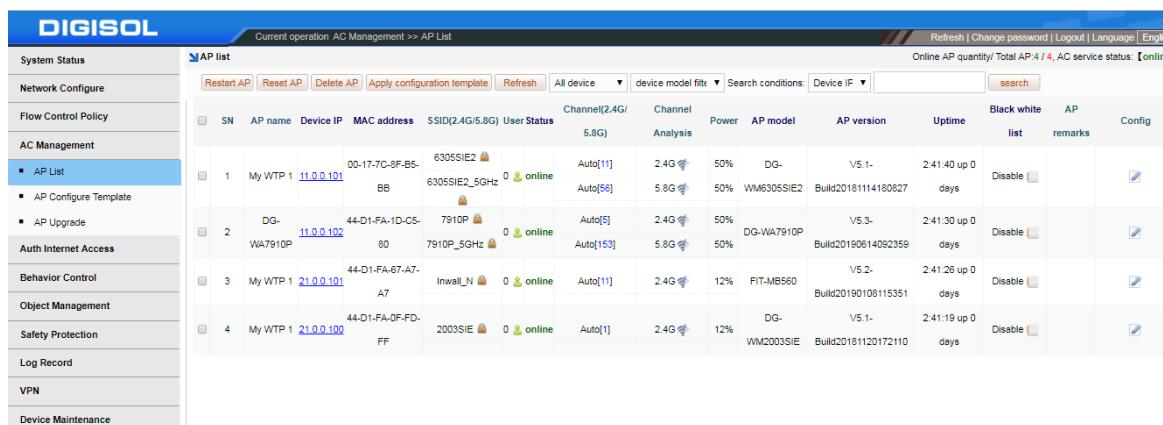
4.4 AC Management

The wireless controller can discover peer wireless AP regardless of whether these devices are connected to each other, located in the same Layer 2 broadcast domain, or attached to different IP subnet. When the controller discovers and validates AP, the controller takes over the management of the AP. You can replace AP configuration by AP Profile template created on the controller.

NOTE: By default AP will be in FAT Mode. You need to set it in FIT Mode to get it discovered on controller.

4.4.1 AP List

AP List displays the online/offline wireless AP list.



SN	AP name	Device IP	MAC address	SSID(2.4G/5.8G)	User Status	Channel(2.4G/5.8G)	Channel Analysis	Power	AP model	AP version	Uptime	Black white list	AP Config
1	My WTP 1	11.0.0.101	00-17-7C-9F-B5-BB	6305SIE2 6305SIE2_5GHz	0 online	Auto[11]	2.4G	50%	DG-	V5.1-	2:41:40 up 0 days	Disable	
2	DG-WA7910P	11.0.0.102	44-D1-FA-1D-C5-80	7910P_5GHz	0 online	Auto[5]	2.4G	50%	DG-WA7910P	V5.3-	2:41:30 up 0 days	Disable	
3	My WTP 1	21.0.0.101	44-D1-FA-67-A7-A7	Inwall_N	0 online	Auto[11]	2.4G	12%	FIT-MB560	V5.2-	2:41:26 up 0 days	Disable	
4	My WTP 1	21.0.0.102	44-D1-FA-0F-FD-FF	2003SIE	0 online	Auto[1]	2.4G	12%	DG-WM2003SIE	V5.1-	2:41:19 up 0 days	Disable	

You can do the following settings under this tab:

Restart AP: Restart the selected AP from the list.

Reset AP: Restore selected AP to factory default. (If AP is in FIT Mode, after reset it will be in same mode)

Delete AP: Delete the chosen wireless AP from the list.

Apply Configuration Template: You can push the respective model configuration template created on controller to desired AP from the list

Refresh: Refresh the displayed AP List.

☎ 1800-209-3444 (Toll Free)

✉ helpdesk@digisol.com

⌚ sales@digisol.com

🌐 www.digisol.com

All Device: Show the complete list of wireless AP connected to this controller

Online Device: Show the list of wireless AP which are online

Offline Device: Show the list of wireless AP which are offline

Device Model Filter: Select the desired model from filter list to display same model AP

Search Conditions: Search the wireless AP by IP address, MAC address, Device Name, Device Model & Version info

Name: Can mark AP with the location or model number or other information which can be easy to know this wireless AP.

Device IP: The wireless AP's IP address

MAC Address: MAC address of wireless AP

SSID: Shows the SSID of wireless AP

Users: Shows how many users are connected with wireless AP

Status: Displays if AP is Online/ Offline

Channel: Shows the wireless AP channel, including both the frequency bands.

Power: Shows the wireless AP RF power

AP Model: Model number of wireless AP

AP Version: Display AP firmware version

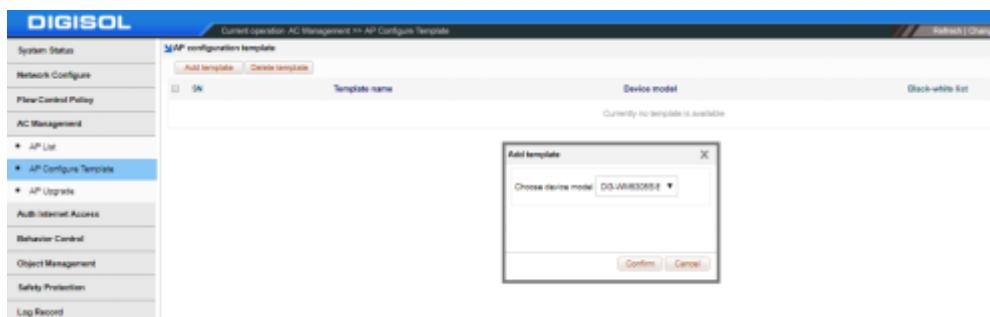
Uptime: Display running time of AP

Black White List: You can assign the Wi-Fi User Mac address by enabling this feature under Black/white List to allow/ block access to respective AP

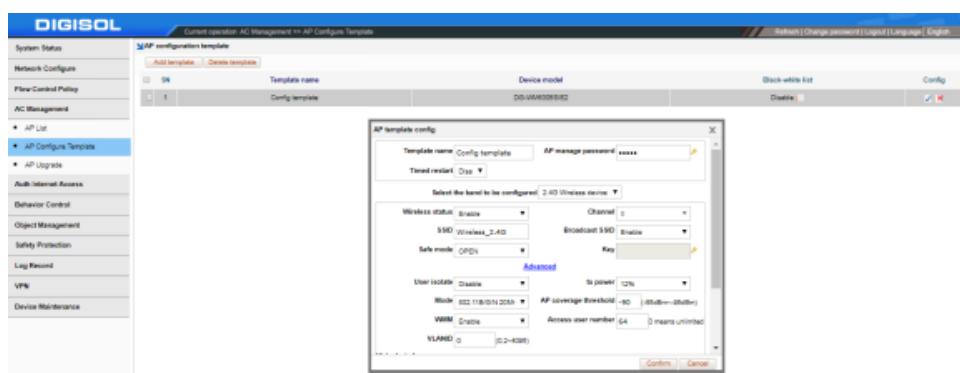
Config:  You can edit/ modify the configuration of respective AP under this option

4.4.2 AP Configure Template

Click ‘Add’ to create a template on controller. It will list the connected model in drop down menu. Just select the desired model & confirm the settings.

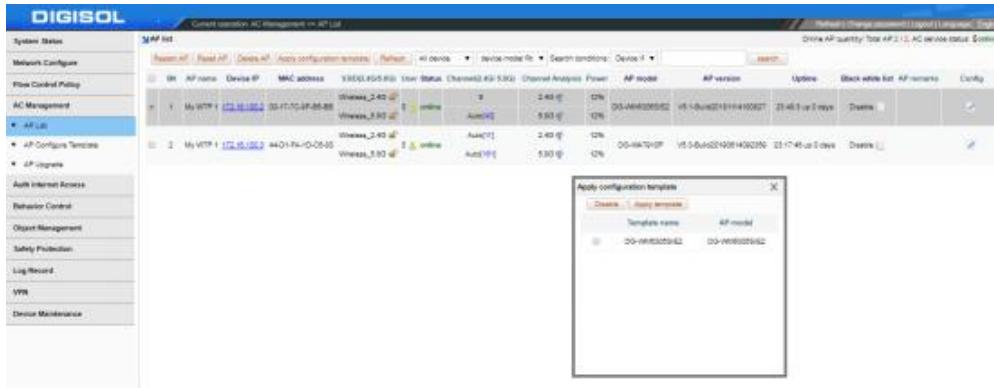


Once you confirm the settings, it will list the template. Click on **Config**  to configure the Wireless settings for respective AP model.



Go to AP List tab to push the configured template to respective AP model as shown below:-

Select the AP from the list & click on '**Apply Configuration Template**' to push the configuration.

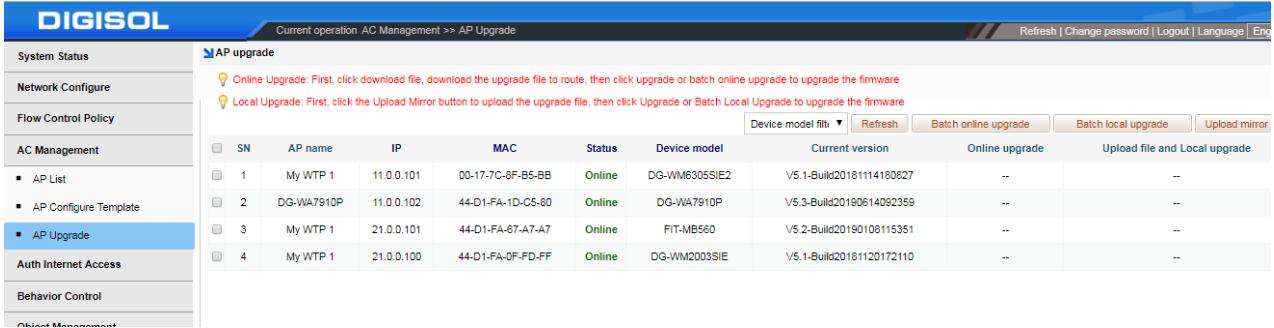


The screenshot shows the DIGISOL AC Management interface. On the left, there's a sidebar with options like System Status, Network Configure, Flow Control Policy, AC Management (with AP List selected), AP Configure Template, AP Upgrade, Auth Internet Access, Behavior Control, Object Management, Safety Protection, Log Record, VPR, and Device Maintenance. The main area is titled 'AP List' and shows a table of AP devices. One row is highlighted with a yellow background. A modal window titled 'Apply configuration template' is overlaid on the table, containing a dropdown menu with 'Choose ... Apply template' and a list of available templates: DG-WH1020SIE2 and DG-WH1020SIE2.

After applying the template, you can view the updated AP configuration under AP List.

4.4.3 AP Upgrade

You can view the current firmware version of connected AP's & latest if any under this option.



The screenshot shows the DIGISOL AC Management interface with the 'AP Upgrade' option selected in the sidebar. The main area is titled 'AP upgrade' and contains a table of AP devices. The table columns include SN, AP name, IP, MAC, Status, Device model, Current version, Online upgrade, and Upload file and Local upgrade. There are four rows in the table. Below the table are several buttons: 'Device model filter', 'Refresh', 'Batch online upgrade', 'Batch local upgrade', and 'Upload mirror'. A note at the top says: 'Online Upgrade: First, click download file, download the upgrade file to route, then click upgrade or batch online upgrade to upgrade the firmware' and 'Local Upgrade: First, click the Upload Mirror button to upload the upgrade file, then click Upgrade or Batch Local Upgrade to upgrade the firmware'.

Select the Batch online upgrade/ Batch local upgrade option to upgrade a set of AP's at a stretch.

 1800-209-3444 (Toll Free)

 helpdesk@digisol.com

 sales@digisol.com

 www.digisol.com

4.5 Auth Internet Access

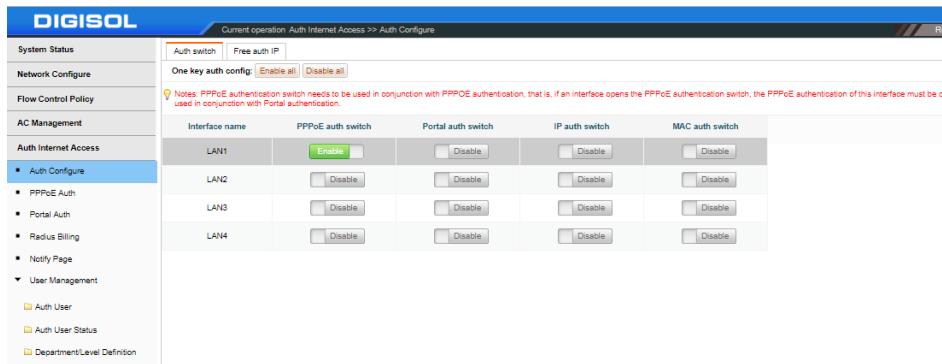
4.5.1 Auth Configure

You can configure four type of Authentication Method for specific LAN interface/ Sub-interface if any on this controller for Internet access.

- | | |
|--------------------------|-----------------------|
| 1. PPPoE Authentication | 3. IP Authentication |
| 2. Portal Authentication | 4. Mac Authentication |

4.5.1.a PPPoE Authentication

Enable PPPoE authentication on respective Interface as shown below:-



Interface name	PPPoE auth switch	Portal auth switch	IP auth switch	MAC auth switch
LAN1	Enable	Disable	Disable	Disable
LAN2	Disable	Disable	Disable	Disable
LAN3	Disable	Disable	Disable	Disable
LAN4	Disable	Disable	Disable	Disable

You can bypass certain Users by adding them under “**Free Auth IP**” section i.e) users can directly access the internet without using Authentication if any.



The dialog box has the following fields:

- Source IP: ANY
- Add button
- Cancel button

Click on **PPPoE Auth** tab to configure the PPPoE settings.

Enable PPPoE function. Specify the service name, Assign Gateway IP & IP address pool for PPPoE client under this tab.

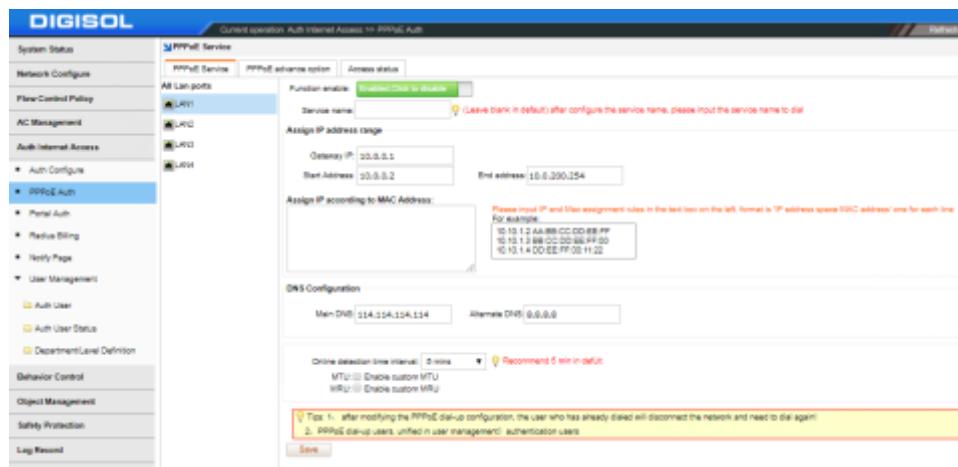
 1800-209-3444 (Toll Free)

 helpdesk@digisol.com

 sales@digisol.com



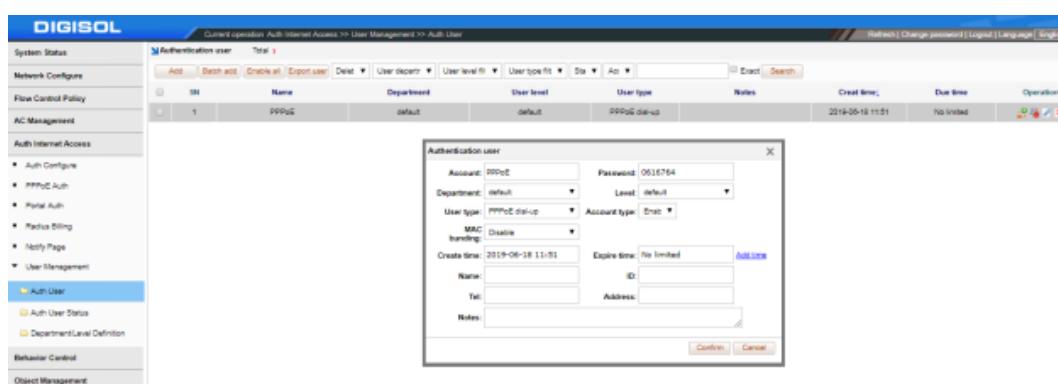
www.digisol.com



You can configure advanced setting for PPPoE Auth under this option as shown below:-



Now create a User account for PPPoE Auth Method under User Management>>Auth User tab.



The users connected through LAN1 interface will not be able to access the internet until and unless they dial PPPoE connection from their PC with user account set on controller.

Once user get connected through PPPoE dialer will be listed under Access Status tab in PPPoE Auth option on controller.



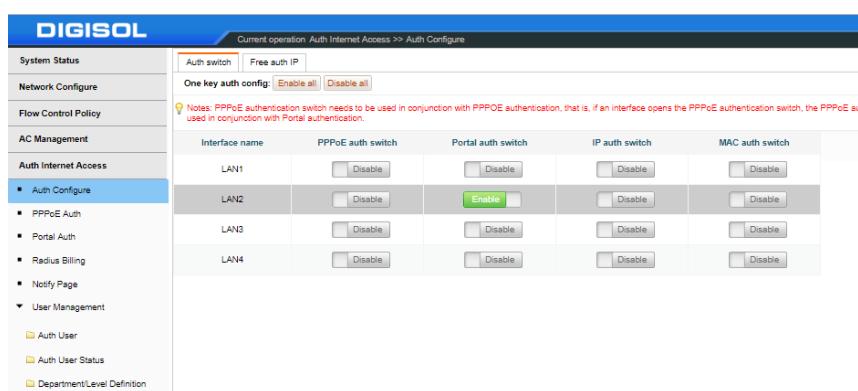
All LAN ports	IP	Access amount	Access time	Server IP	Assign IP	Operation	
LAN1-PPPoE	10.0.0.1	1	PPPoE	2019-05-19 12:15:29	10.0.0.1	10.0.0.1	

You can disconnect the PPPoE client from web GUI itself by clicking the icon highlighted below:-.



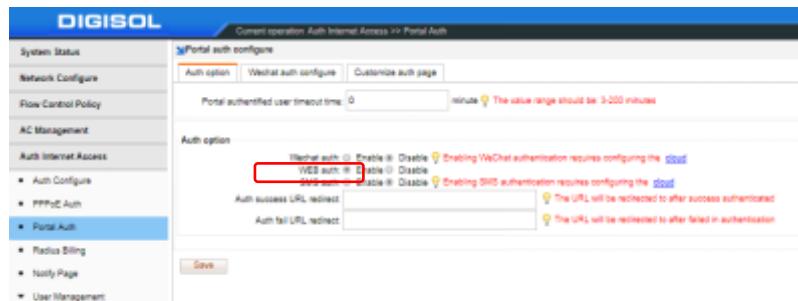
4.5.1.b Portal Authentication

Enable Portal authentication on respective Interface as shown below:-

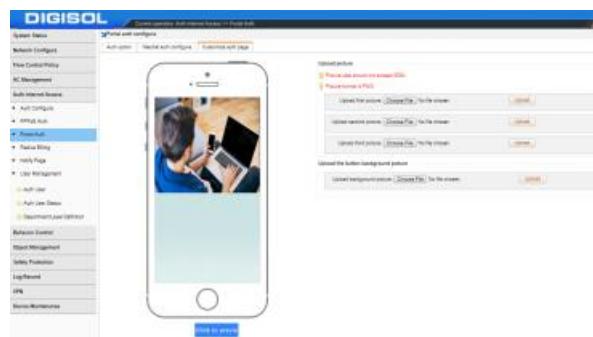


Interface name	PPPoE auth switch	Portal auth switch	IP auth switch	MAC auth switch
LAN1	<input type="button" value="Disable"/>	<input type="button" value="Disable"/>	<input type="button" value="Disable"/>	<input type="button" value="Disable"/>
LAN2	<input type="button" value="Disable"/>	<input checked="" type="button" value="Enable"/>	<input type="button" value="Disable"/>	<input type="button" value="Disable"/>
LAN3	<input type="button" value="Disable"/>	<input type="button" value="Disable"/>	<input type="button" value="Disable"/>	<input type="button" value="Disable"/>
LAN4	<input type="button" value="Disable"/>	<input type="button" value="Disable"/>	<input type="button" value="Disable"/>	<input type="button" value="Disable"/>

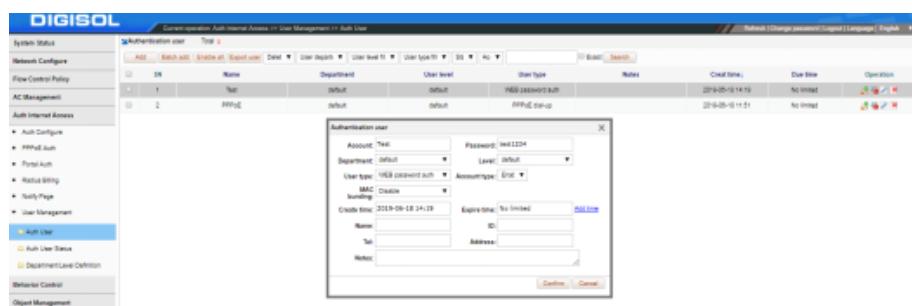
Click on Portal Auth tab to configure further settings.



You can customize the Web Login page by uploading the images as desired under “**Customize Auth Page**”.



Create a User account for Portal Auth Method under User Management>>Auth User tab.



The users connected through LAN2 interface will be prompted a Web page as shown below:-



Enter the username/ password created for Web authentication on controller to go online.

4.5.1.c IP Authentication

You can allow/ limit certain IP address to desired LAN interface of controller using this method.

Interface name	PPPoE auth switch	Portal auth switch	IP auth switch	MAC auth switch
LAN1	<input type="button" value="Create"/>	<input type="button" value="Disable"/>	<input type="button" value="Disable"/>	<input type="button" value="Create"/>
LAN2	<input type="button" value="Create"/>	<input type="button" value="Disable"/>	<input type="button" value="Disable"/>	<input type="button" value="Create"/>
LAN3	<input type="button" value="Create"/>	<input type="button" value="Disable"/>	<input checked="" type="button" value="Enable"/>	<input type="button" value="Create"/>
LAN4	<input type="button" value="Create"/>	<input type="button" value="Disable"/>	<input type="button" value="Disable"/>	<input type="button" value="Create"/>

You need to create User Account with desired IP address under User Management>>Auth User tab.

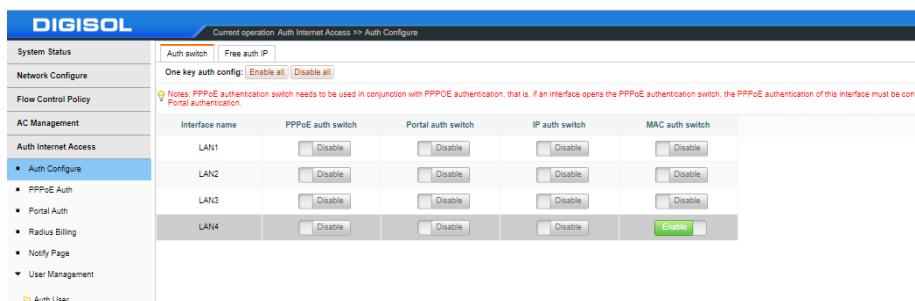
SN	Name	Department	User level	User type	Notes	Creat time,	Due time	Operation
1	Test	default	default	WEB password auth		2019-05-19 11:19	No limited	
2	Bhushan	default	default	IP address auth		2019-05-19 11:00	No limited	
3	Ashwini	default	default	WEB password auth		2019-05-19 10:53	No limited	
4	Pooja	default	default	WEB password auth		2019-05-19 10:44	No limited	
5	Samir	default	default	WEB password auth		2019-05-19 10:41	No limited	

Authentication user

IP address:
 Department: Level:
 User type: Account type:
 MAC bundling:
 Create time: Expire time:
 Name:
 ID:
 Tel:
 Address:
 Notes:

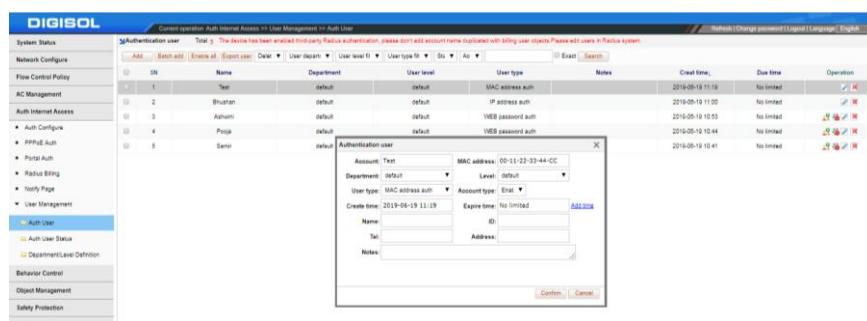
4.5.1.d MAC Authentication

You can allow/ limit certain MAC address to desired LAN interface of controller using this method.



The screenshot shows the DIGISOL Web Interface under 'Auth Internet Access >> Auth Configure'. The left sidebar has 'Auth User' selected. The main panel shows a table for MAC authentication switches across four LAN interfaces (LAN1 to LAN4). The 'MAC auth switch' for LAN4 is highlighted in green, indicating it is enabled. A note at the top right states: 'Note: PPPoE authentication switch needs to be used in conjunction with PPPoE authentication, that is, if an interface opens the PPPoE authentication switch, the PPPoE authentication of this interface must be config'.

You need to create User Account with desired IP address under User Management>>Auth User tab.

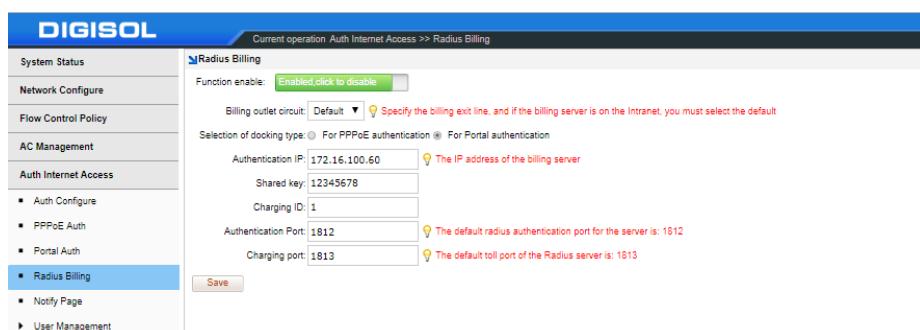


The screenshot shows the DIGISOL Web Interface under 'User Management >> Auth User'. The left sidebar has 'Auth User' selected. The main panel shows a list of existing users (Test, Bhutan, Athuri, Poja, Sanu) and an open modal dialog for creating a new user. The dialog fields include: Account: Test, MAC address: 00-11-22-33-44-CC, Department: default, Level: default, User type: MAC address auth, Create time: 2016-05-19 11:19, Expire time: no limited, and Notes: .

NOTE: You can set the schedule for defined Users to allow internet access for limited time period under all 4 authentication methods.

4.5.1.e Radius Billing

You can integrate Radius Server with this controller by configuring the below settings.



The screenshot shows the DIGISOL Web Interface under 'Auth Internet Access >> Radius Billing'. The left sidebar has 'Radius Billing' selected. The main panel shows configuration for a radius server. Fields include: Function enable: Enabled (click to disable), Billing outlet circuit: Default, Selection of docking type: For PPPoE authentication or For Portal authentication, Authentication IP: 172.16.100.60, Shared key: 12345678, Charging ID: 1, Authentication Port: 1812, and Charging port: 1813. A 'Save' button is at the bottom.

 1800-209-3444 (Toll Free)

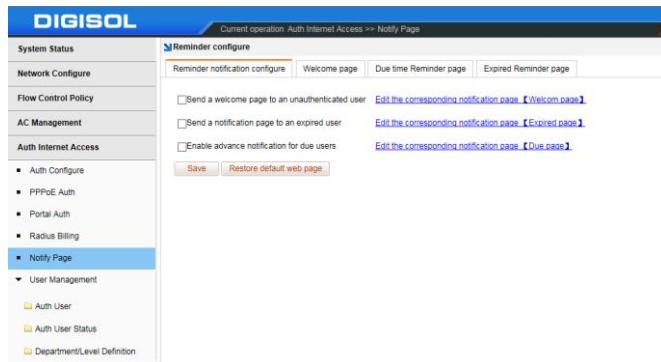
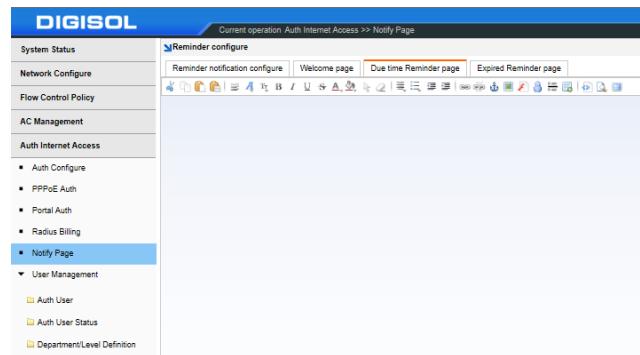
 helpdesk@digisol.com

 sales@digisol.com

 www.digisol.com

4.5.1.f Notify Page

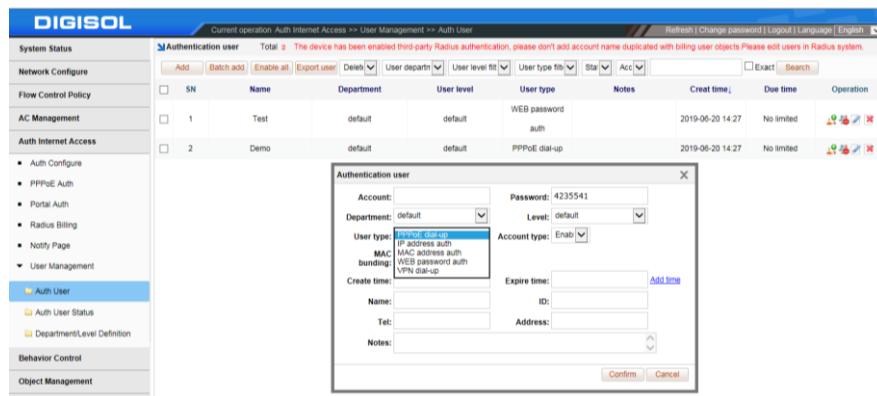
You can define a notification page under this tab.

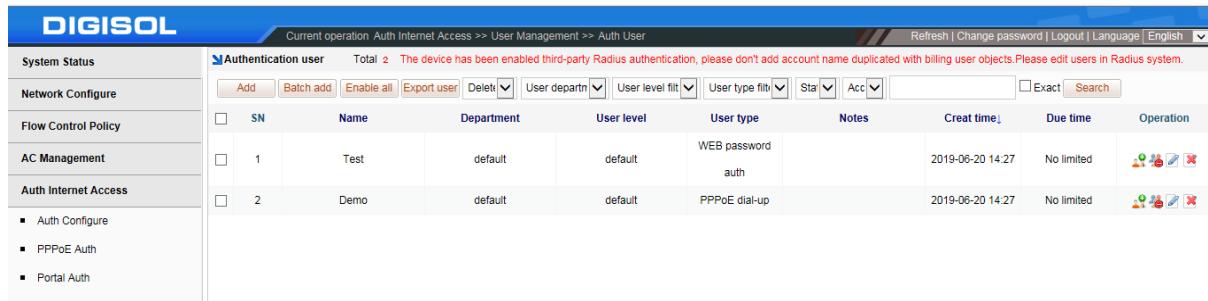
4.5.2 User Management

4.5.2.a Auth User

You can create the desired User Account for PPPoE Dial UP/ IP Address Auth/ MAC Address Auth/ Web Auth & VPN Dial UP under this tab.



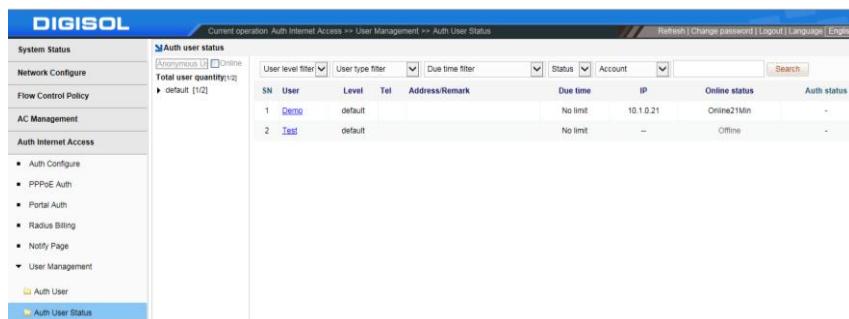
It will display the created users list as shown below:-



SN	Name	Department	User level	User type	Notes	Creat time	Due time	Operation
1	Test	default	default	WEB password auth		2019-06-20 14:27	No limited	
2	Demo	default	default	PPPoE dial-up		2019-06-20 14:27	No limited	

4.5.2.b Auth User Status

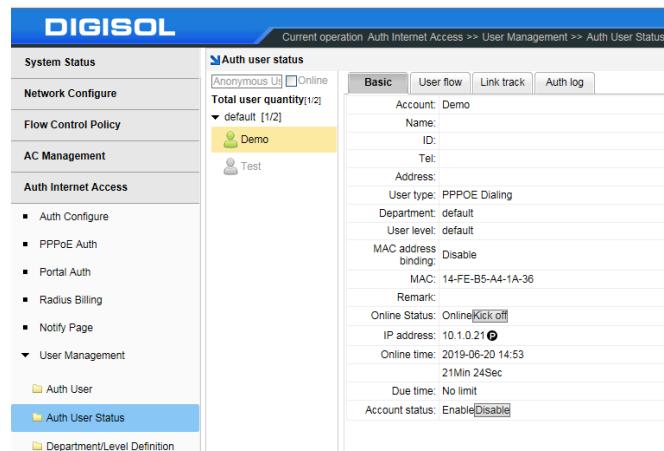
It displays the user Online/ Offline status along with uptime.



SN	User	Level	Tel	Address/Remark	Due time	IP	Online status	Auth status
1	Demo	default			No limit	10.1.0.21	Online1Min	-
2	Test	default			No limit	-	Offline	-

It will display the user session & details once you click on desired user from the list.

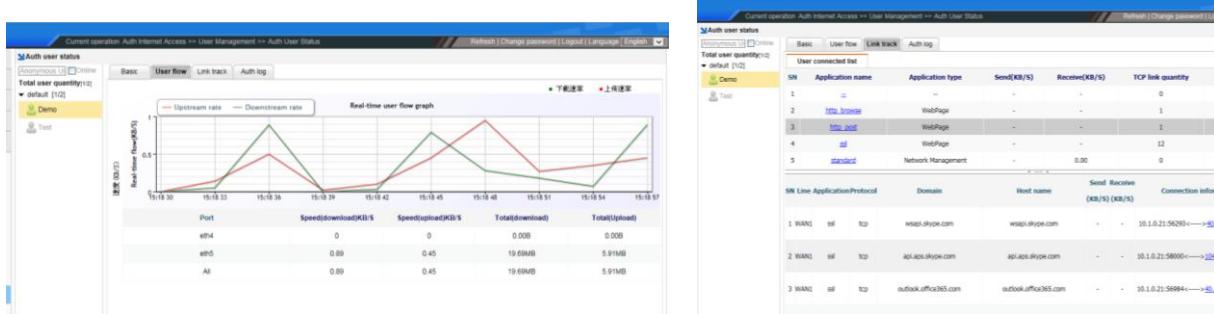
Basic Details:



Basic		User flow	Link track	Auth log
Account:	Demo			
Name:				
ID:				
Tel:				
Address:				
User type:	PPPOE Dialing			
Department:	default			
User level:	default			
MAC address binding:	Disable			
MAC:	14-FE-B5-A4-1A-36			
Remark:				
Online Status:	Online	Kick off		
IP address:	10.1.0.21			
Online time:	2019-06-20 14:53			
	21Min 24Sec			
	Due time: No limit			
Account status:	Enable	Disable		

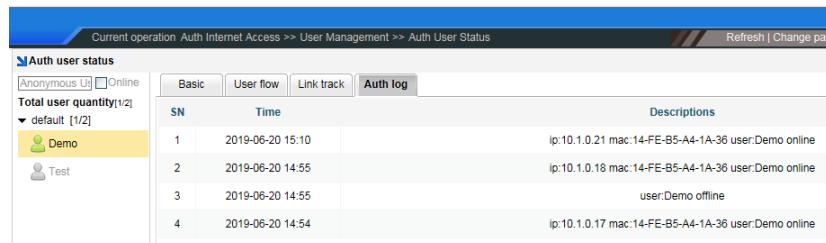
User Flow & Link Track

You can view the connected User Sessions & speed in graphical format.



User Auth Log:

It will display the authenticated user status.

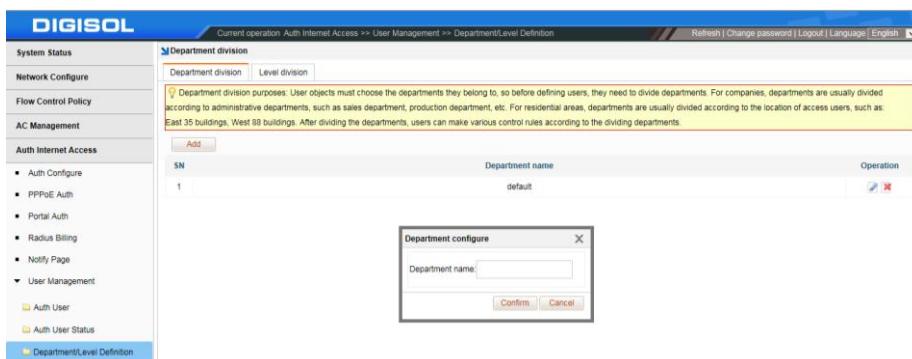


The table lists authentication events with their descriptions.

SN	Time	Descriptions
1	2019-06-20 15:10	ip:10.1.0.21 mac:14-FE-B5-A4-1A-36 user:Demo online
2	2019-06-20 14:55	ip:10.1.0.18 mac:14-FE-B5-A4-1A-36 user:Demo online
3	2019-06-20 14:55	user:Demo offline
4	2019-06-20 14:54	ip:10.1.0.17 mac:14-FE-B5-A4-1A-36 user:Demo online

4.5.2.c Department/ Level Definition

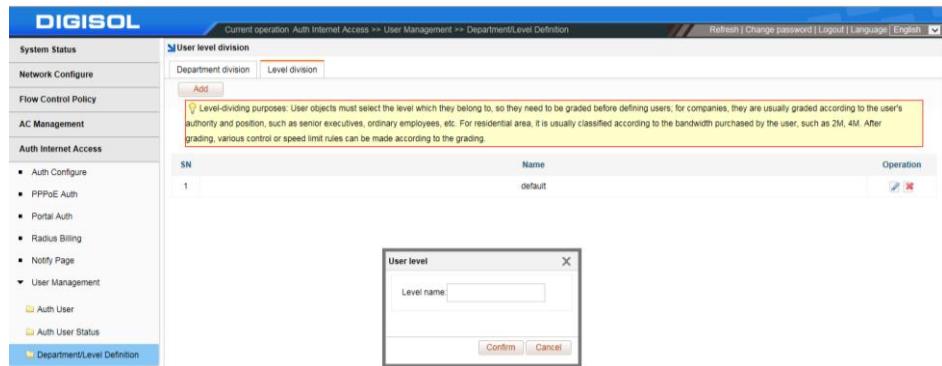
You can define multiple departments under this tab to isolate the users if any.



The interface allows adding new departments. A modal dialog titled "Department configure" is shown, prompting for the department name.

SN	Department name	Operation
1	default	

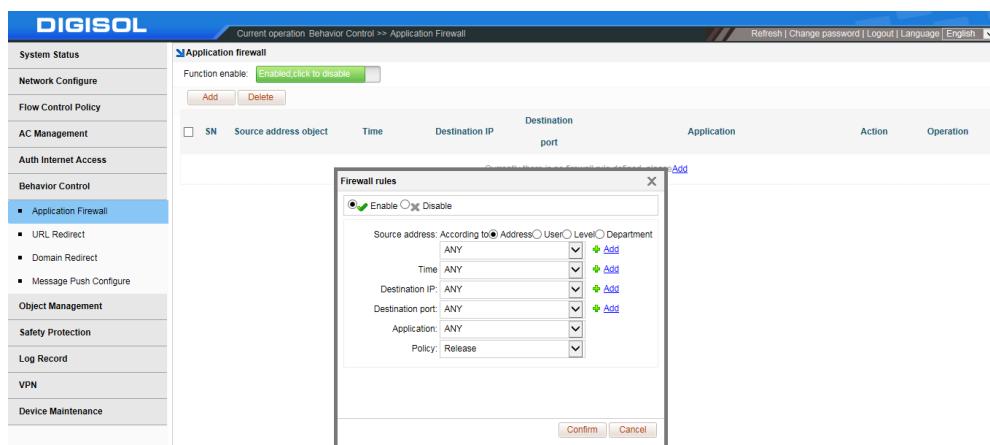
You can define different Levels under this tab for users if any.



4.6 Behavior Control

4.6.1 Application firewall

You can create firewall rule/ policy for Specific Address/ User/ Level or Department under this tab.

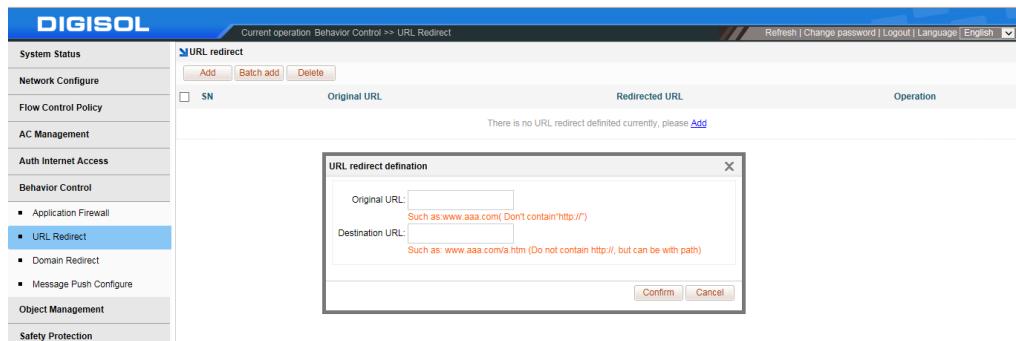


You can create object for Time/ Destination IP/Destination Port/ Application under **“Object Management”**.

Call that object under firewall tab to allow/ block the defined policy.

4.6.2 URL Redirect

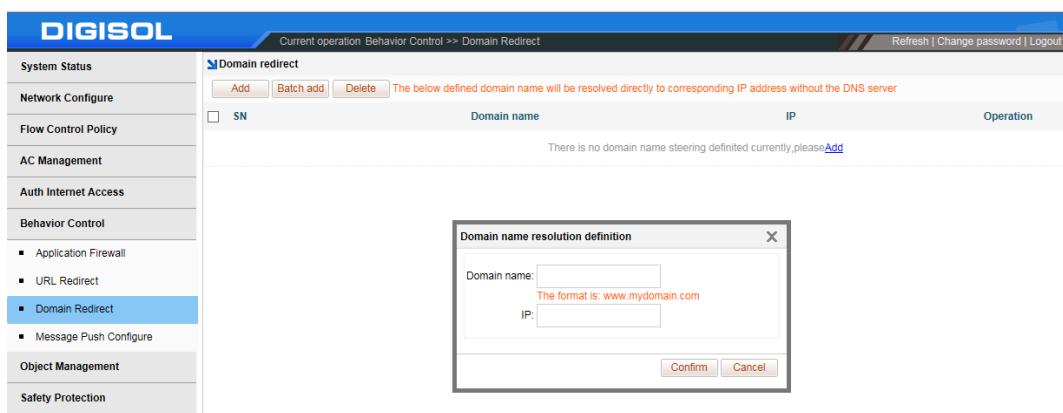
You can redirect any url to defined site on controller.



The screenshot shows the DIGISOL web interface under the Behavior Control section. The URL redirect sub-section is selected. A modal dialog titled "URL redirect definition" is open, asking for "Original URL" (e.g., www.aaa.com) and "Destination URL" (e.g., www.aaa.com/a.htm). The main table below shows no existing entries.

4.6.3 Domain Redirect

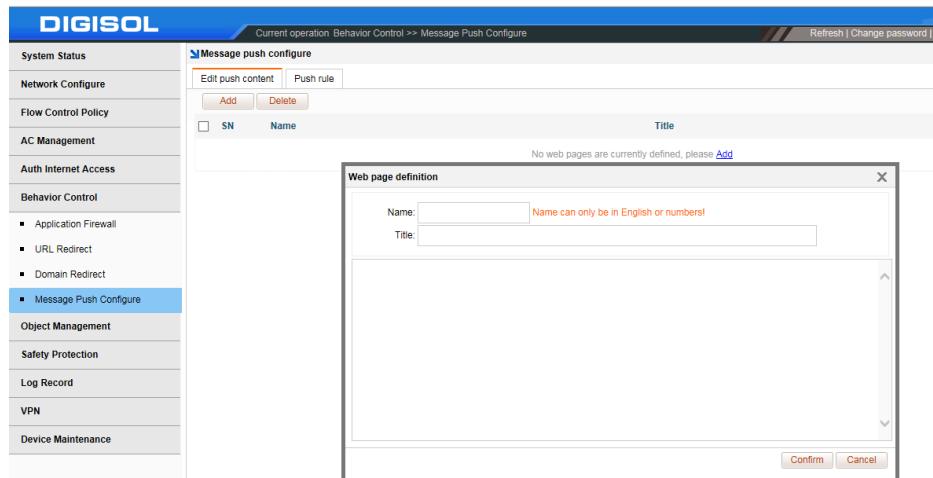
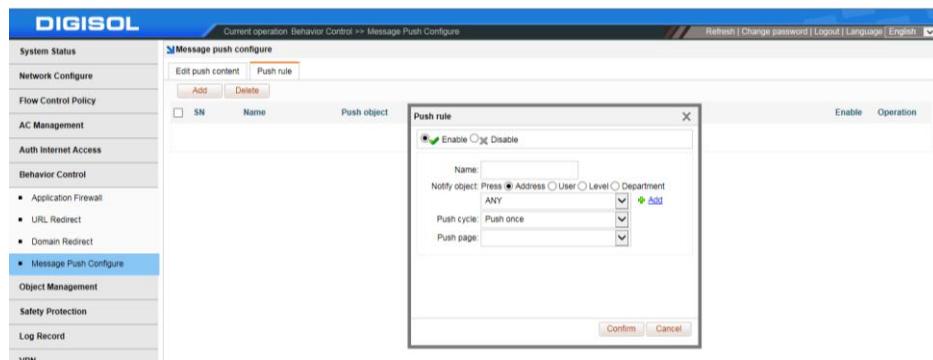
You can redirect any domain to defined fixed IP on controller.



The screenshot shows the DIGISOL web interface under the Behavior Control section. The Domain Redirect sub-section is selected. A modal dialog titled "Domain name resolution definition" is open, asking for "Domain name" (e.g., www.mydomain.com) and "IP". The main table below shows no existing entries.

4.6.4 Message Push Configure

You can configure message push settings under this tab.

4.7 Object Management

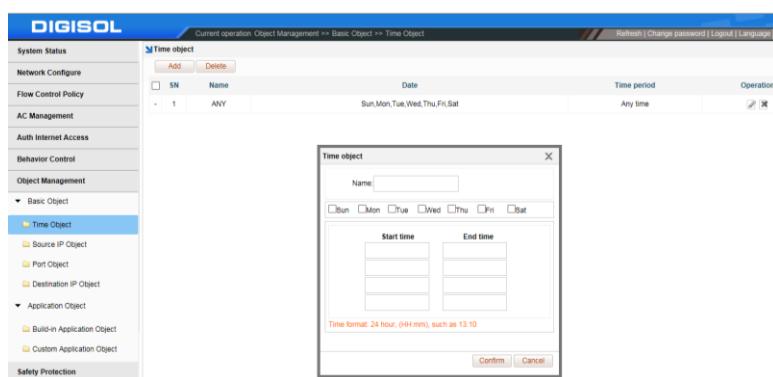
4.7.1 Basic Object

You can create basic object of Time, Source IP, Port & Destination IP under this tab.

4.7.1.a Time Object

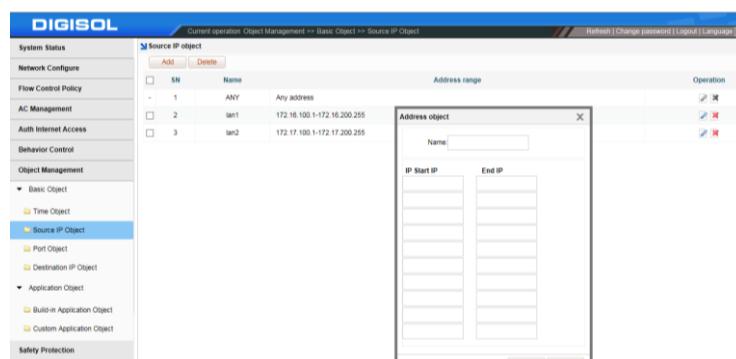
By default one object already exist on controller for any time.

If you want to define a rule/ policy for specific time slot, you can create a **Time** object as Shown below:-



4.7.1.b Source IP Object

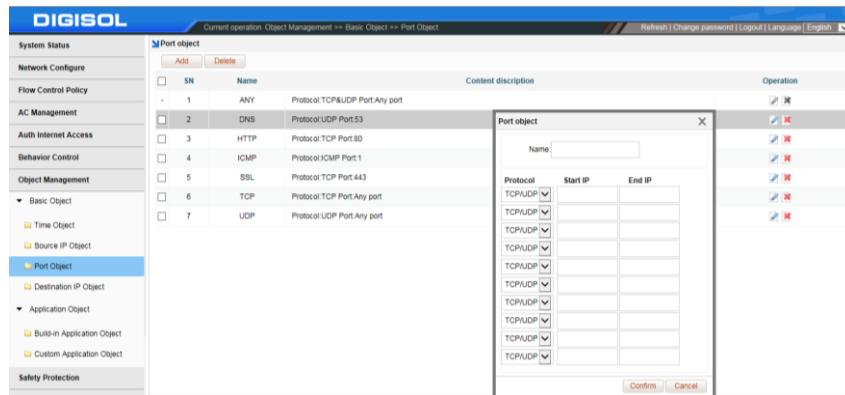
You can create Source IP object here if you want to create policy for certain local IP address range.



4.7.1.c Port Object

There are some predefined Port Object already created on Controller by default.

You can create an object for any customized port if required, under this tab.



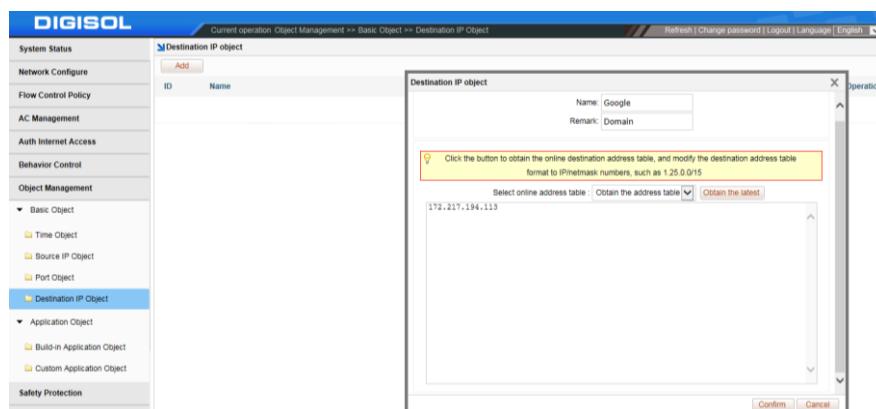
The screenshot shows the DIGISOL Object Management interface. On the left, there's a navigation tree with 'Object Management' selected, and 'Port Object' is highlighted. The main area displays a table of predefined port objects:

ID	Name	Description
1	ANY	Protocol TCP&UDP Port Any port
2	DNS	Protocol UDP Port 53
3	HTTP	Protocol TCP Port 80
4	ICMP	Protocol ICMP Port 1
5	SSL	Protocol TCP Port 443
6	TCP	Protocol TCP Port Any port
7	UDP	Protocol UDP Port Any port

A modal dialog titled 'Port object' is open, allowing the creation of a new port object. It has fields for 'Name', 'Protocol' (set to TCP/UDP), 'Start IP', and 'End IP'. There are also checkboxes for 'Operation' and a 'Confirm' button at the bottom.

4.7.1.d Destination IP Object

You can create an object for any online destination address if required, under this tab.



The screenshot shows the DIGISOL Object Management interface. The navigation tree on the left has 'Object Management' selected, and 'Destination IP Object' is highlighted. The main area shows a table of destination IP objects:

ID	Name
	Google

A modal dialog titled 'Destination IP object' is open, showing fields for 'Name' (set to Google) and 'Remark' (set to Domain). It includes a note about obtaining an online address table and a 'Select online address table' dropdown with 'Obtain the address table' and 'Obtain the latest' options. The 'Obtain the latest' button is highlighted. A 'Confirm' button is at the bottom.

4.7.2 Application Object

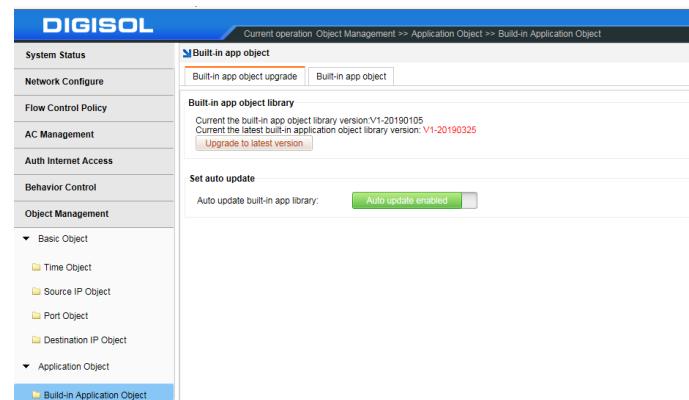
You can create application based object under this tab.

4.7.2.1 Built-in Application Object

4.7.2.1.a Built-in App Object Upgrade

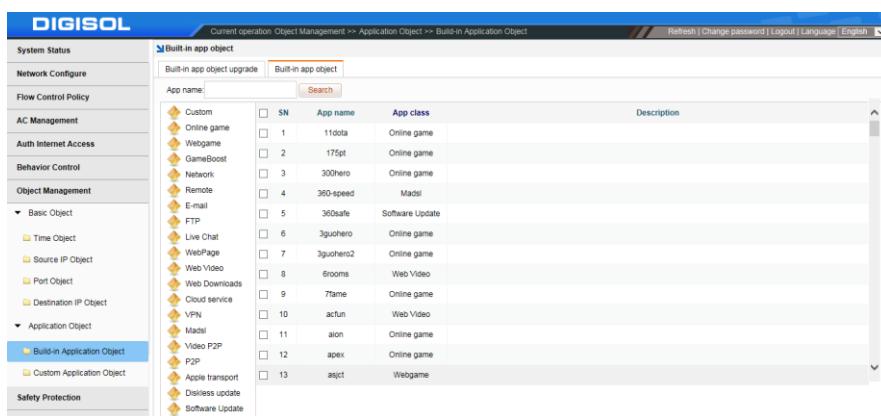
By default there are certain built-in application objects in controller. You can Upgrade the built-in object library under this tab.

If '**Auto update built-in library**' option is enabled, it will display the latest version if available to upgrade the same.



4.7.2.1.b Built-in App Object

In this tab, it will display the built-in object list.



 1800-209-3444 (Toll Free)

 helpdesk@digisol.com

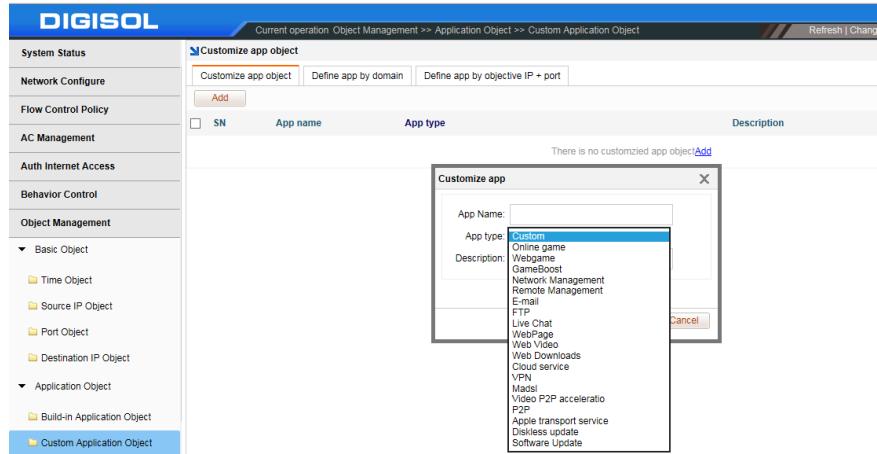
 sales@digisol.com

 www.digisol.com

4.7.2.2 Custom Application Object

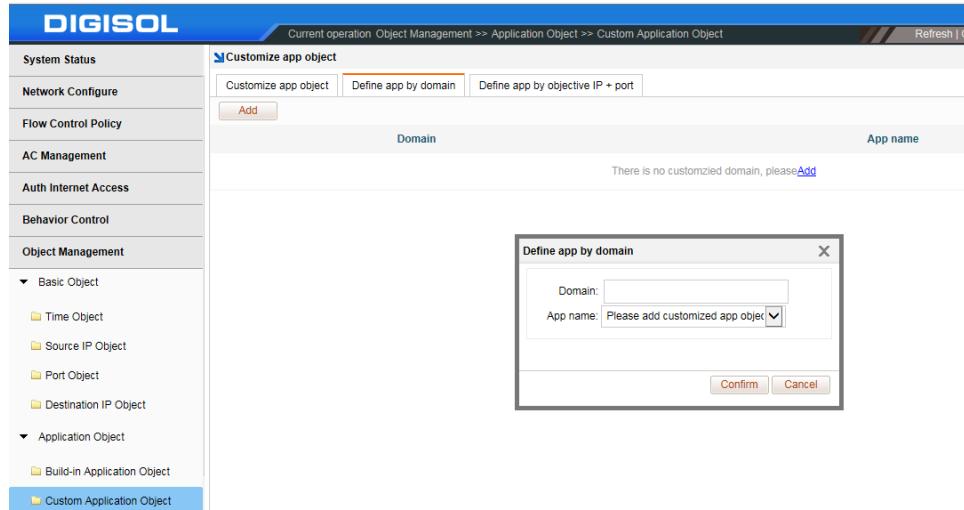
4.7.2.2.a Customize App Object

You can create new object under Custom which is not listed in built-in app object.



4.7.2.2.b Define App by Domain

You can create new object based on Domain under this tab.



4.7.2.2.c Define App by Objective IP + Port

You can define Local User IP Pool for respective customized object under this tab.



The screenshot shows the DIGISOL web interface with the title 'Object Management >> Application Object >> Custom Application Object'. On the left, there's a navigation menu with 'Custom Application Object' selected. In the center, there's a table header for 'Define app by objective IP + port' with columns 'SN', 'App name', and 'Content'. A message below the table says 'There is no custom address port object currently, please [Add](#)'. The main content area is a modal dialog titled 'Define app by objective IP + port' containing input fields for 'Start address', 'End address', 'Protocol' (set to 'TCP/UDP'), 'Start port', 'End port', and 'App name' (set to 'Please add customized app obj'). There are 'Confirm' and 'Cancel' buttons at the bottom of the dialog.

4.8 Safety Protection

4.8.1 IP-MAC Binding

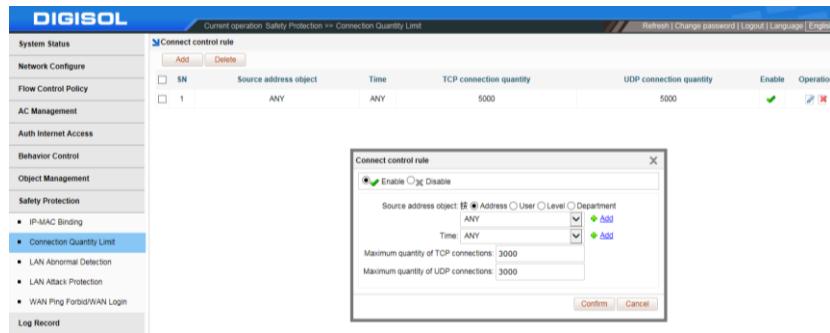
You can bind IP address for respective MAC Address under this tab.



The screenshot shows the DIGISOL web interface with the title 'Safety Protection >> IP-MAC Binding'. On the left, there's a navigation menu with 'IP-MAC Binding' selected. In the center, there's a table header for 'IP-MAC bind' with columns 'SN', 'User', 'IP Address', 'MAC address', and 'Enable Operation'. A message below the table says 'No MAC address is currently bound, please [Add](#)'. The main content area is a modal dialog titled 'IP-MAC binding rule' containing two radio buttons: 'Enable' (selected) and 'Disable', and input fields for 'IP Address' and 'MAC address'. There are 'Confirm' and 'Cancel' buttons at the bottom of the dialog.

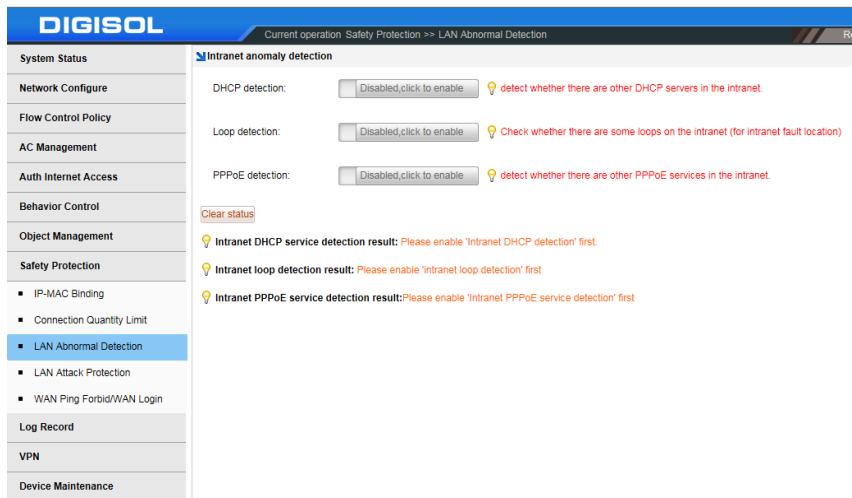
4.8.2 Connection Quantity Limit

You can define the concurrent TCP/ UDP connection for respective Address, User, Level or on department basis.



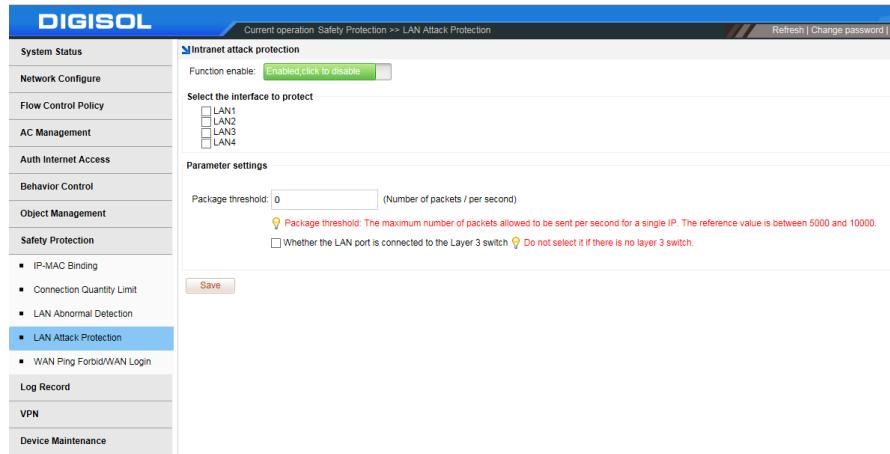
4.8.3 LAN Abnormal Detection

You can enable DHCP Detection, Loop Detection or PPPoE detection feature under this tab.



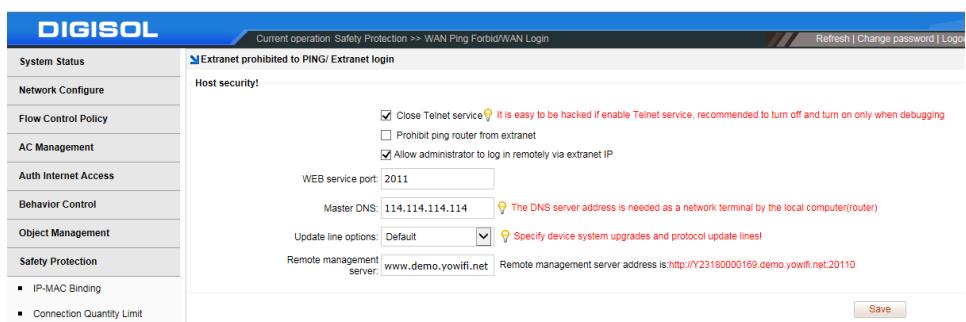
4.8.4 LAN Attack Protection

You can set the packet threshold for respective LAN interface under this tab.



4.8.5 WAN Ping Forbid/ WAN Login

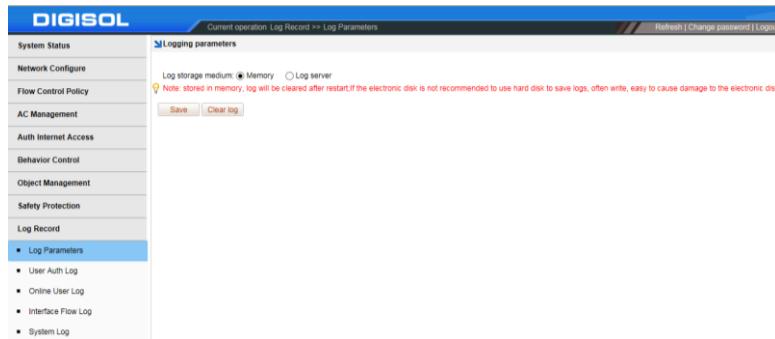
You can forbid remote ping, remote management of controller & close telnet service under this tab.



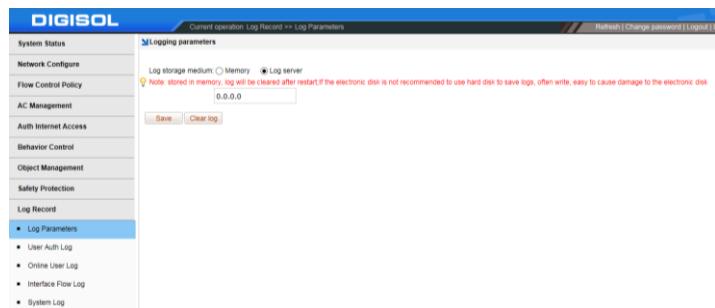
4.9 Log Record

4.9.1 Log Parameters

You can select below option to store the logs to internal memory but after reboot, it will clear the logs



You can specify Log Server IP if any, under this tab.



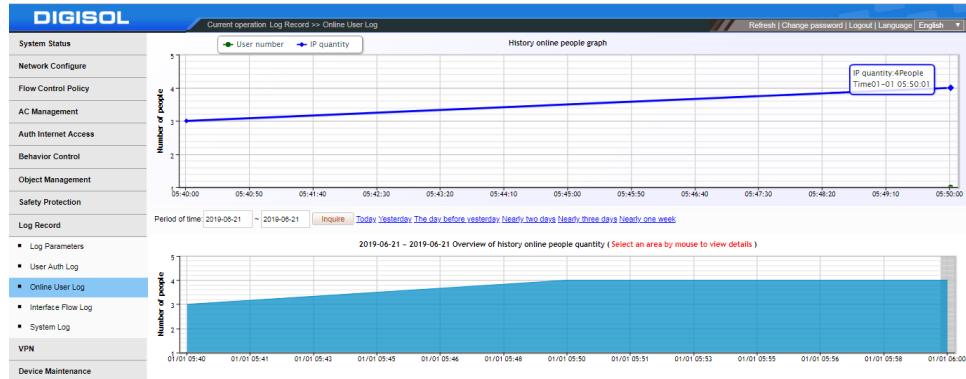
4.9.2 User Auth Log

You can view the Authenticated User log under this tab.

User auth log		
SN	Time	Description
1	2019-06-21 09:41:37	ip:10.1.0.2 mac:14-FE-B5-A4-1A-36 user:Demo online
<input type="button" value="Search"/> <input type="button" value="Home"/> <input type="button" value="Pre page"/> <input type="button" value="Next page"/> <input type="button" value="Last Page"/> <input type="button" value="Turn to page"/> <input type="text" value="1"/> <input type="button" value="GO"/> Total 1, Current page 1		

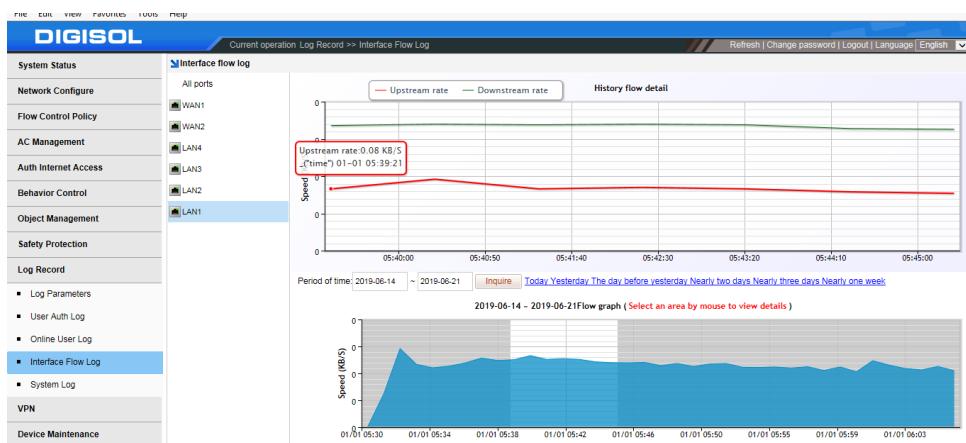
4.9.3 Online User Log

Here you can view the number of online Users at specific time interval in graphical format



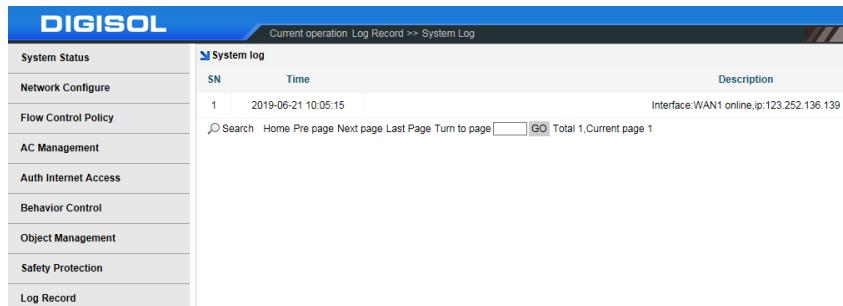
4.9.4 Interface Flow Log

Here you can view the upstream/ downstream rate of respective Interface at specific time interval.



4.9.5 System Log

You can view the system logs under this tab.



System log		
SN	Time	Description
1	2019-06-21 10:05:15	Interface:WAN1 online,ip:123.252.136.139

Search Home Pre page Next page Last Page Turn to page [] Total 1, Current page 1

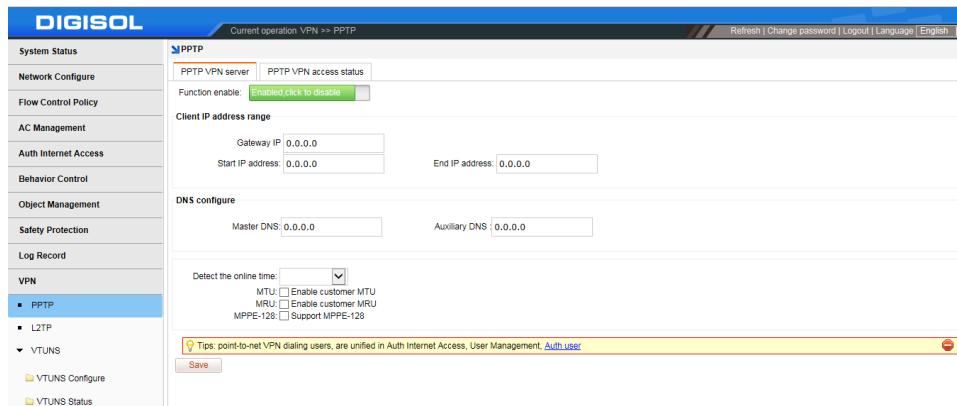
4.10 VPN

You can configure following VPN connectivity on this controller.

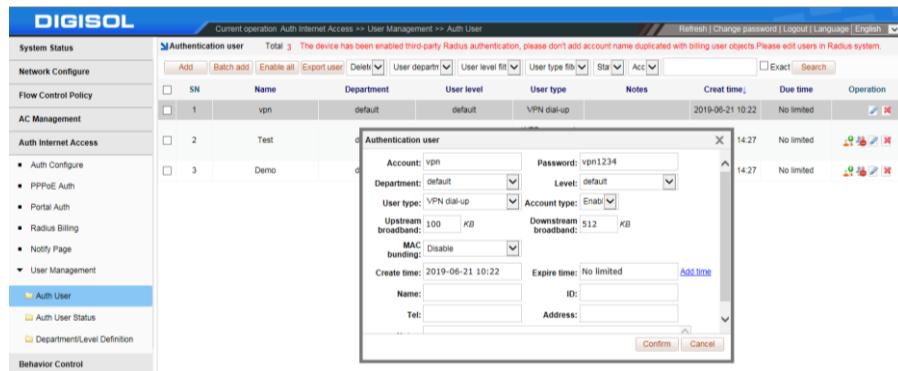
4.10.1 PPTP

4.10.1.a PPTP VPN Server

Configure PPTP Connectivity as shown below:-

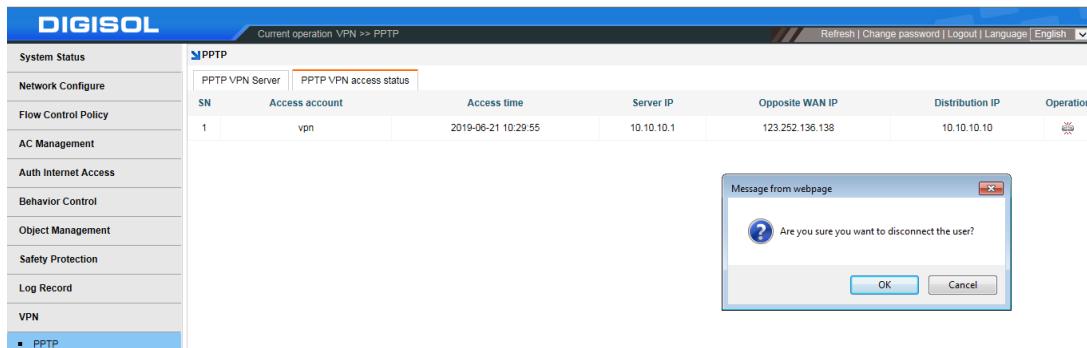


Once PPTP Server is configured, create a User for VPN Dial-UP under “Auth User”.



4.10.1.b PPTP VPN Access Status

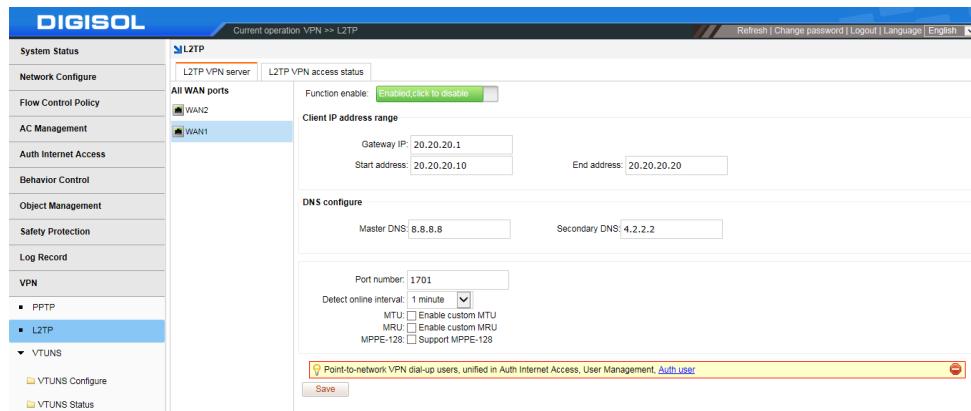
You can view the PPTP connectivity status under this option. You can also disconnect the connected user using the GUI.



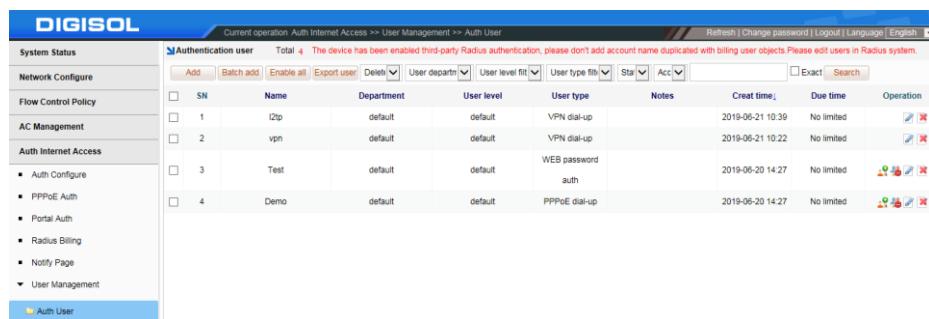
4.10.2 L2TP

4.10.2.a L2TP VPN Server

Configure L2TP Connectivity as shown below:-



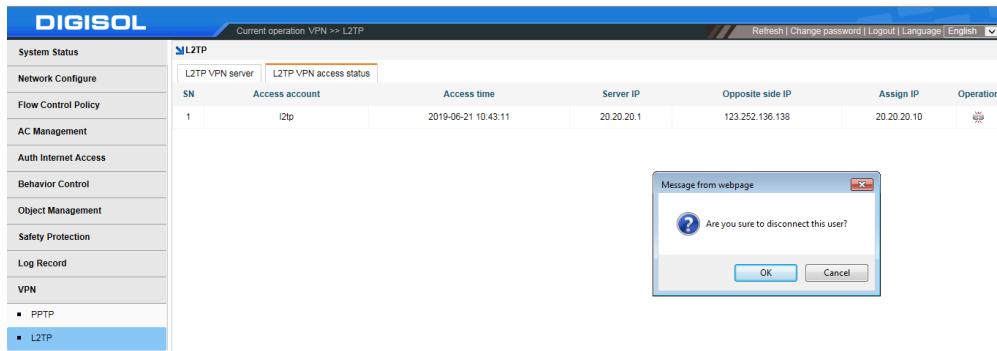
Once L2TP Server is configured, create a New User or you can use the same user account Configured for VPN Dial-UP under “Auth User”.



SN	Name	Department	User level	User type	Notes	Creat time	Due time	Operation
1	i2tp	default	default	VPN dial-up		2019-06-21 10:39	No limited	
2	vpn	default	default	VPN dial-up		2019-06-21 10:22	No limited	
3	Test	default	default	WEB password auth		2019-06-20 14:27	No limited	
4	Demo	default	default	PPPoE dial-up		2019-06-20 14:27	No limited	

4.10.2.b L2TP VPN Access Status

You can view the L2TP connectivity status under this option. You can also disconnect the connected user using the GUI.



The screenshot shows the DIGISOL web interface. The left sidebar has a tree structure with 'System Status', 'Network Configure', 'Flow Control Policy', 'AC Management', 'Auth Internet Access', 'Behavior Control', 'Object Management', 'Safety Protection', 'Log Record', 'VPN' (selected), and 'L2TP' (selected). The main content area has tabs 'L2TP VPN server' and 'L2TP VPN access status' (selected). A table lists a single connection: SN 1, Access account l2tp, Access time 2019-06-21 10:43:11, Server IP 20.20.20.1, Opposite side IP 123.252.136.138, Assign IP 20.20.20.10, and Operation (with a disconnect icon). A 'Message from webpage' dialog box is overlaid, asking 'Are you sure to disconnect this user?' with 'OK' and 'Cancel' buttons.

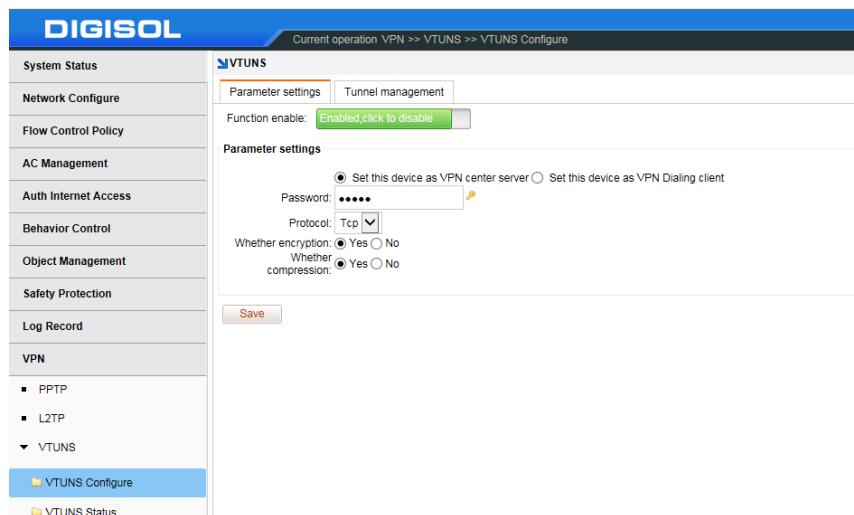
4.10.3 VTUNS

4.10.3.1 VTUNS Configure

You can configure Server-Client Tunnel using this option on controller. You would require controller at the remote site as well to form VTUNS.

4.10.3.1.a Parameter Settings

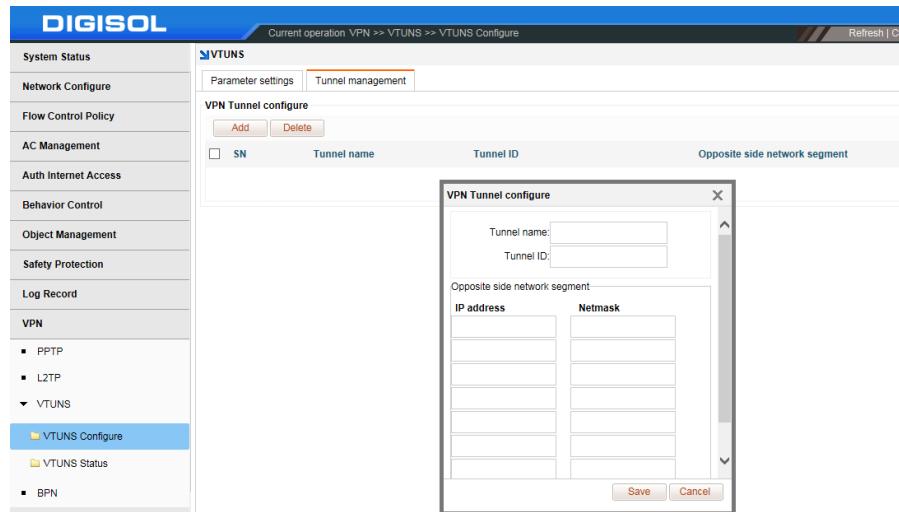
Set one end as VPN Server & define a password as shown below:-



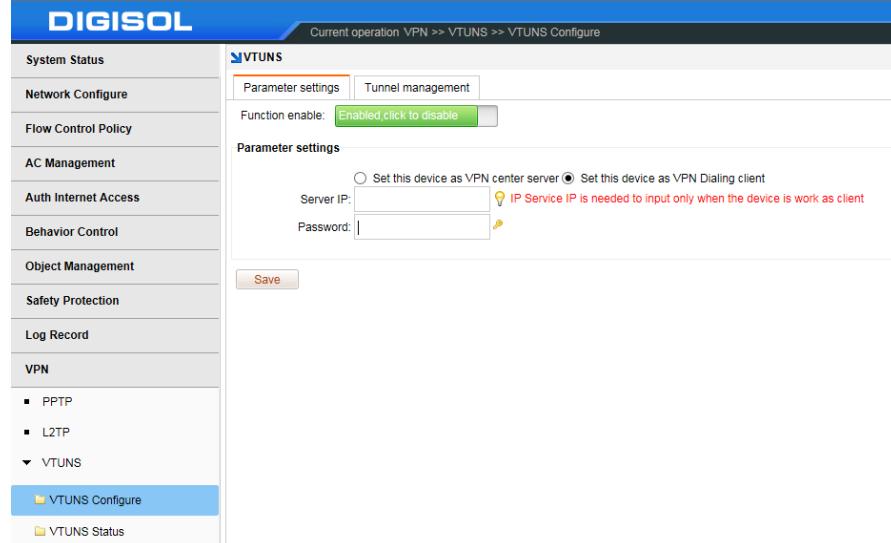
The screenshot shows the DIGISOL web interface. The left sidebar has a tree structure with 'System Status', 'Network Configure', 'Flow Control Policy', 'AC Management', 'Auth Internet Access', 'Behavior Control', 'Object Management', 'Safety Protection', 'Log Record', 'VPN' (selected), and 'VTUNS' (selected). The main content area has tabs 'Parameter settings' (selected) and 'Tunnel management'. Under 'Parameter settings', 'Function enable' is set to 'Enabled, click to disable'. The 'Parameter settings' section includes: 'Set this device as VPN center server' (radio button selected), 'Set this device as VPN Dialing client' (radio button unselected), 'Password' field containing '*****', 'Protocol' dropdown set to 'Tcp', 'Whether encryption' radio buttons ('Yes' selected, 'No' unselected), and 'Whether compression' radio buttons ('Yes' selected, 'No' unselected). A 'Save' button is at the bottom.

4.10.3.1.b Tunnel Management

You need to define a Tunnel Name, ID & remote local network along with netmask under this tab.

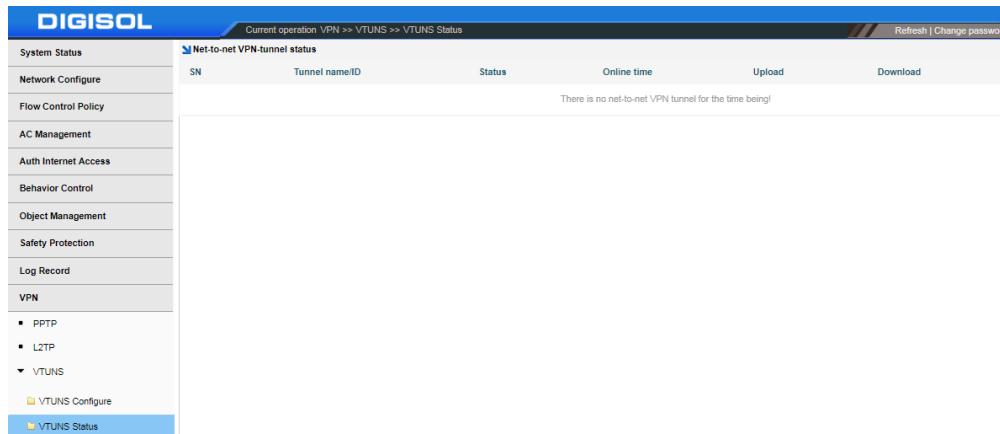


On Remote Controller, you need to set it as VPN Dialing Client. Enter the other controller IP as Server IP & specify the same password as defined on other controller.



4.10.3.2 VTUNS Status

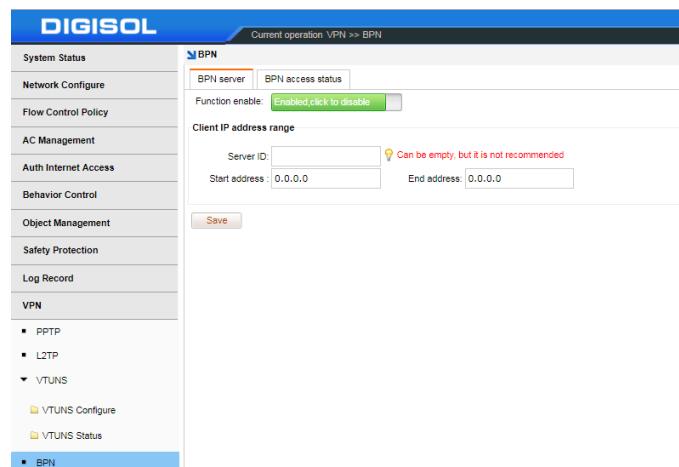
You can view the VTUNS status under this tab.



4.11 BPN (This feature is for future use)

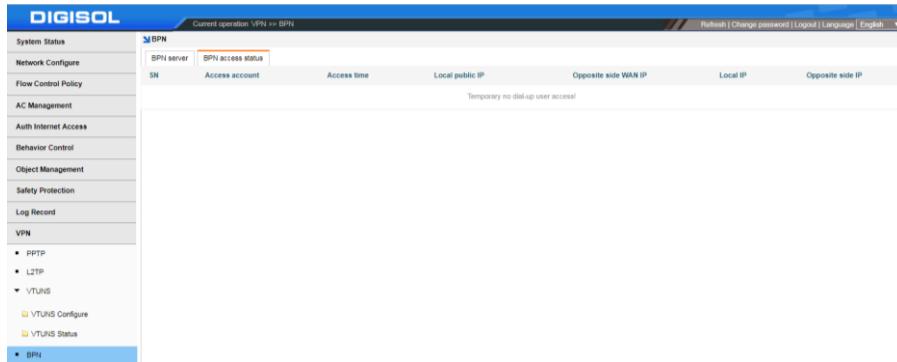
4.11.a BPN Server

You can configure BPN Server under this tab.



4.11.b BPN Access Status

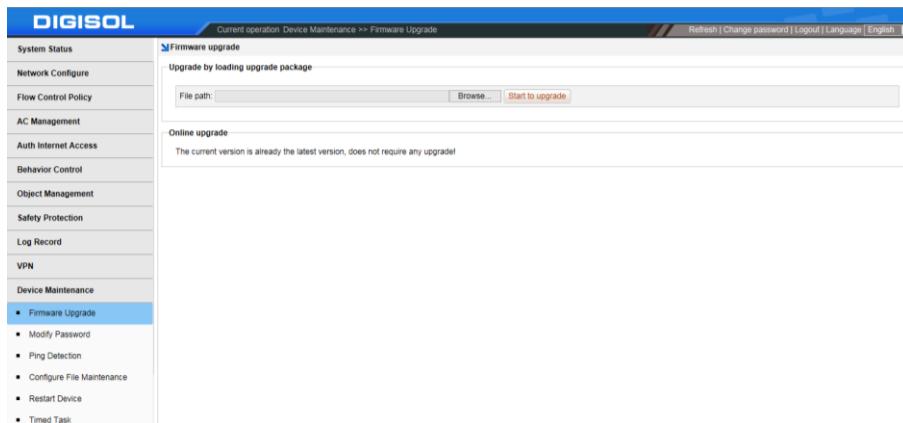
You can view the BPN Status under this option.



4.12 Device Maintenance

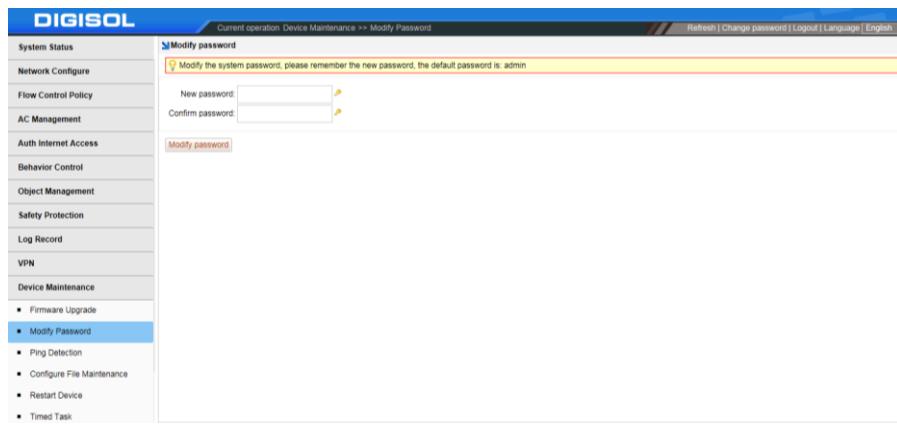
4.12.a Firmware Upgrade

You can upgrade the firmware on controller using this option.



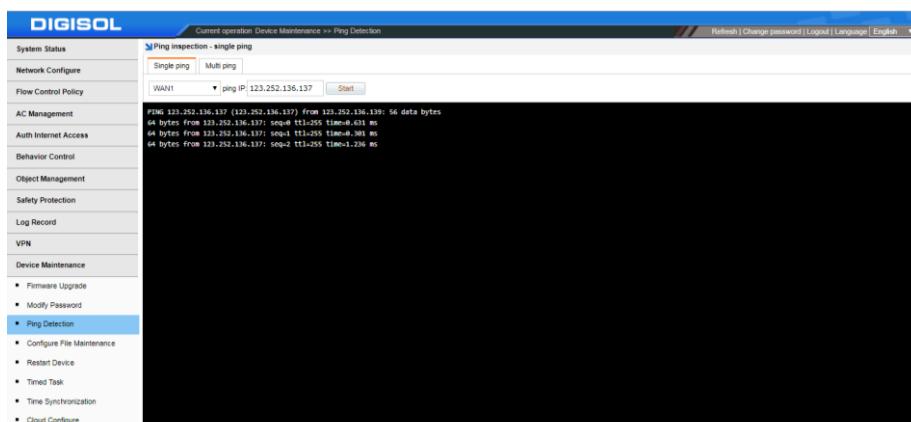
4.12.b Modify Password

You can set the management password under this tab.

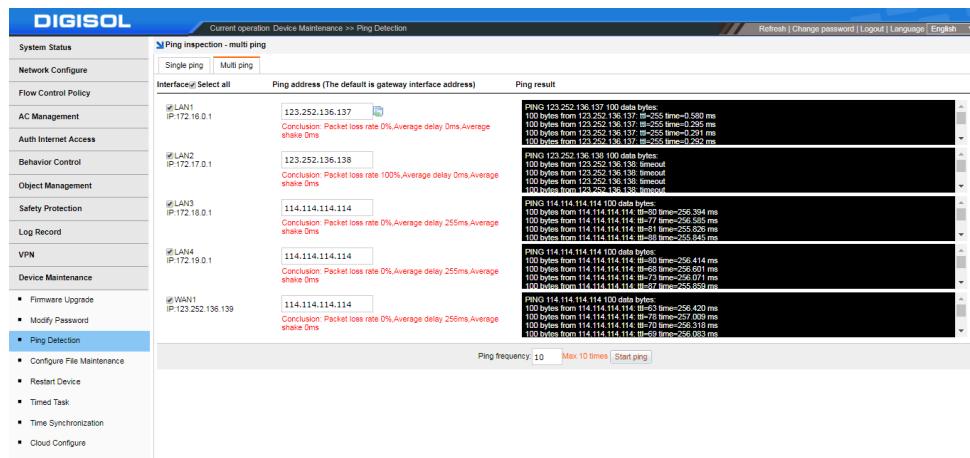


4.12.c Ping Detection

Here you can check the ping to respective WAN interface under this tab.

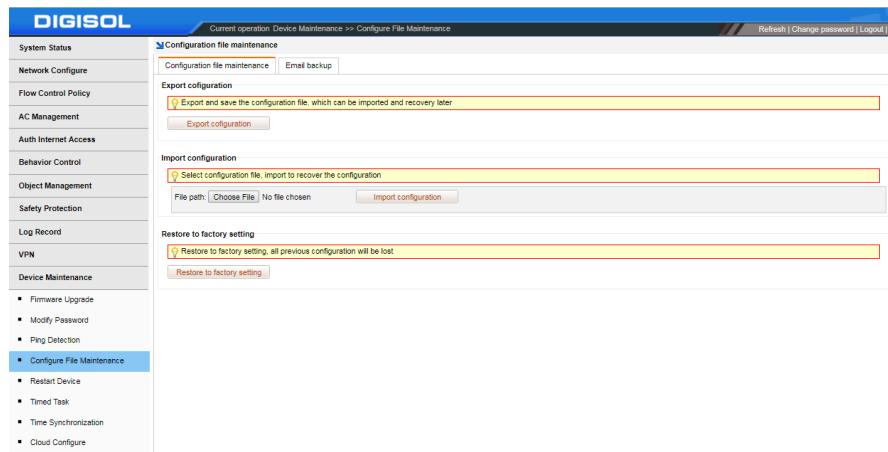


Here you can check the ping to multiple interfaces at a time.

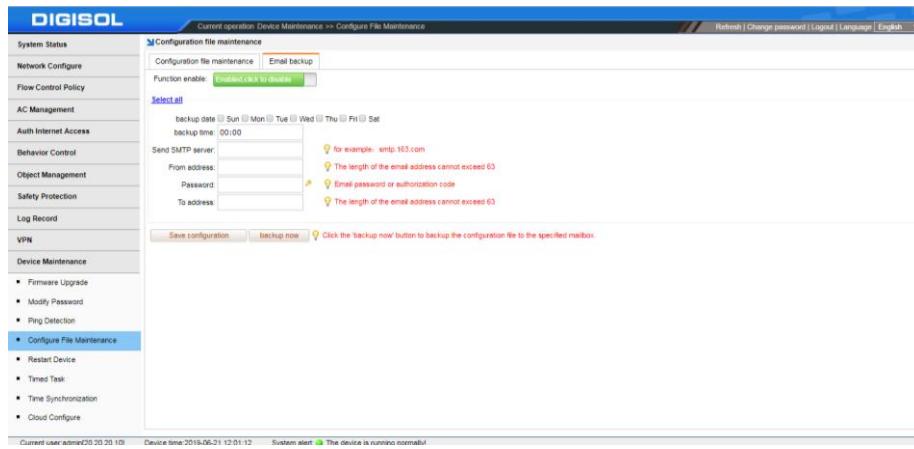


4.12.d Configure File Maintenance

Here you can import/ export controller configuration settings. You can reset the controller to default settings.

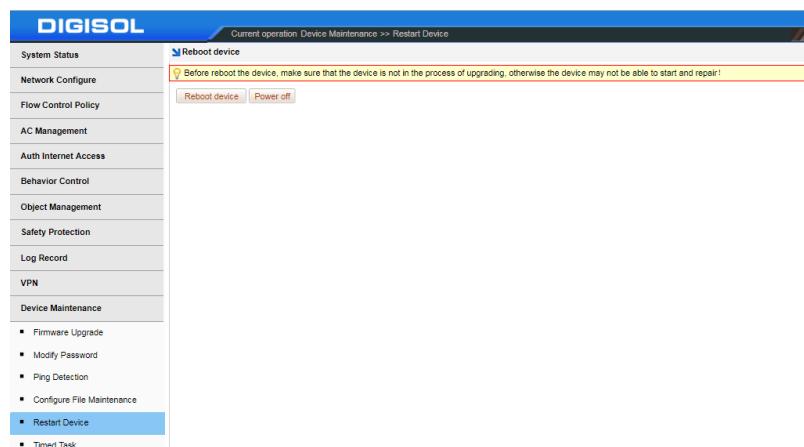


You can backup the configuration to Email ID.



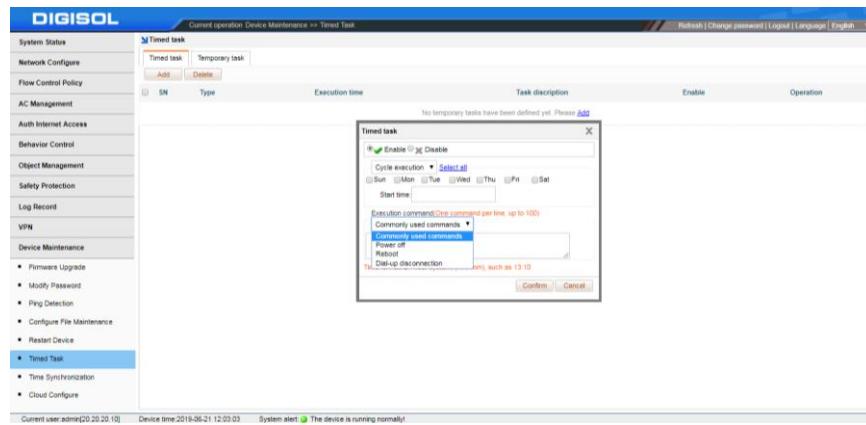
4.12.e Restart Device

You can reboot the device or Power it OFF under this option.



4.12.f Timed Task

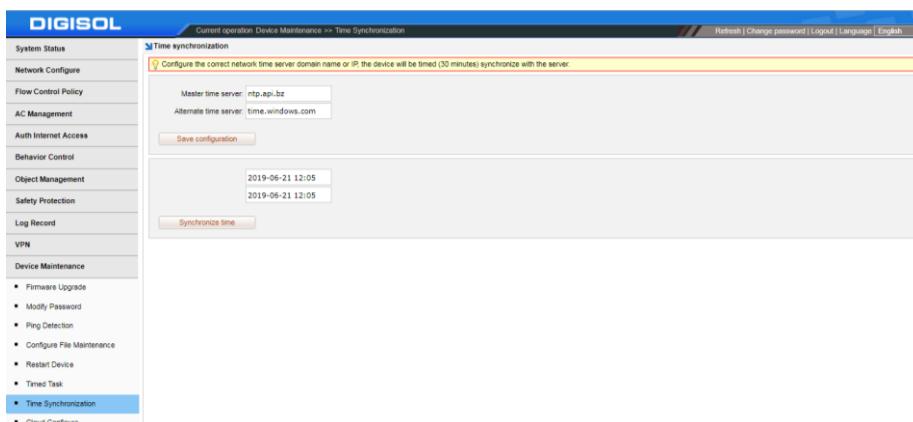
You can define a timed task under this option.



The screenshot shows the DIGISOL Device Maintenance interface with the 'Timed Task' option selected in the left sidebar. A modal window titled 'Timed task' is open, prompting the user to 'Configure the correct network time server domain name or IP, the device will be timed (30 minutes) synchronize with the server.' The modal includes fields for 'Master time server' (set to 'ntp.api.bz') and 'Alternate time server' (set to 'time.windows.com'), a 'Save configuration' button, and two date/time inputs (both set to '2019-06-21 12:05').

4.12.g Time Synchronization

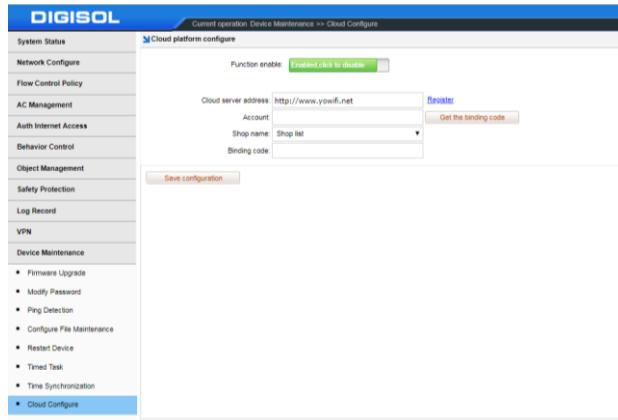
You can define a Time Server under this option.



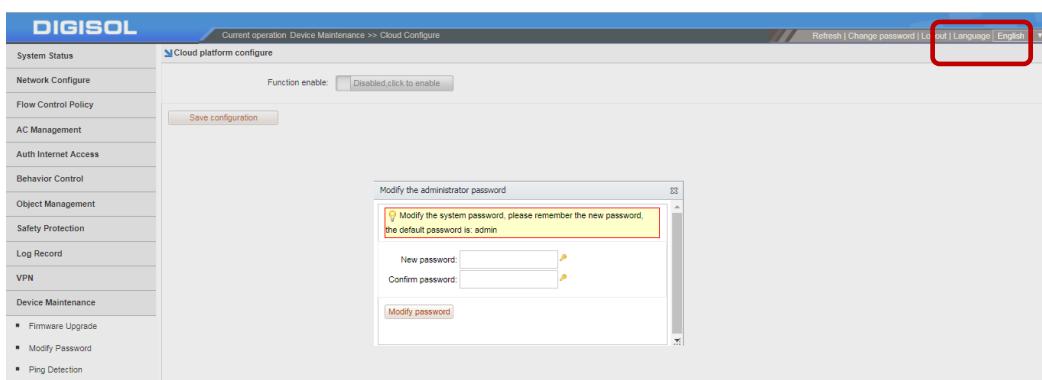
The screenshot shows the DIGISOL Device Maintenance interface with the 'Time Synchronization' option selected in the left sidebar. A modal window titled 'Time synchronization' is open, displaying the message: 'Configure the correct network time server domain name or IP, the device will be timed (30 minutes) synchronize with the server.' It contains fields for 'Master time server' (set to 'ntp.api.bz') and 'Alternate time server' (set to 'time.windows.com'), a 'Save configuration' button, and two date/time inputs (both set to '2019-06-21 12:05').

4.12.h Cloud Configure (For Future Use)

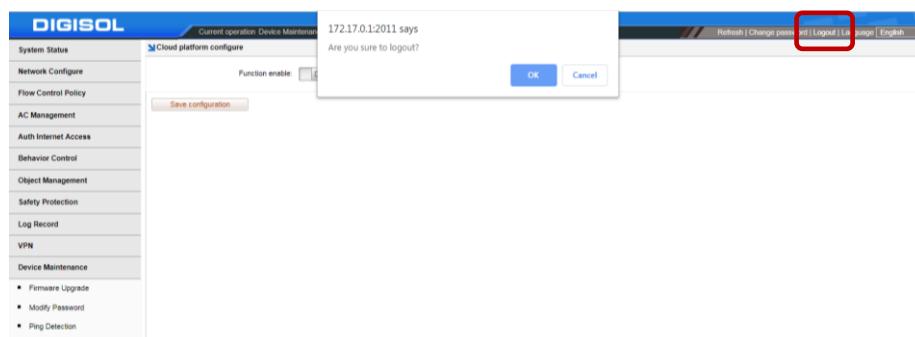
You can configure cloud settings under this option.



You can also change the Management password by clicking this option.



To logout the Web Interface, click the highlighted tab.



CHAPTER 5 Troubleshooting

This Chapter provides solutions to problems for the installation and operation of the Wireless Access Controller. You can refer to the following if you are having problems.

1 Why can't I configure the controller even when the cable is plugged and the LED is lit?

Do a Ping test to make sure that the Wireless Access Controller is responding.

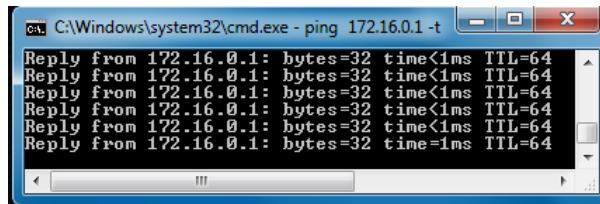
Go to **Start > Run**.

Type cmd.

Note: It is recommended that you use an Ethernet connection to configure it



1. Press OK.
2. Type **ipconfig** to get the IP of default gateway.
3. Type "**ping 172.16.0.1**". Assure that you ping the correct IP Address assigned to this wireless access controller. It will show four replies if you ping correctly.



Ensure that your Ethernet Adapter is working, and that all network drivers are installed properly. Network adapter names will vary depending on your specific adapter. The installation steps listed below are applicable for all network adapters.

1. Go to Start > Right click on “My Computer” > Properties .
2. Select the Hardware Tab.
3. Click Device Manager.
4. Double-click on “Network Adapters”.
5. Right-click on Wireless Card bus Adapter or your specific network adapter.
6. Select Properties to ensure that all drivers are installed properly.
7. Look under Device Status to see if the device is working properly.
8. Click “OK”.

2 What can I do if my Ethernet connection does not work properly?

- A. Make sure the RJ45 cable connects with the router.
- B. Ensure that the setting on your Network Interface Card adapter is "Enabled".
- C. If settings are correct, ensure that you are not using a crossover Ethernet cable, not all Network Interface Cards are MDI/MDIX compatible, and using a patch cable is recommended.
- D. If the connection still does not work properly, then you can reset it to default.

This product comes with One Year warranty. For further details about warranty policy and Product Registration, please visit support section of www.digisol.com