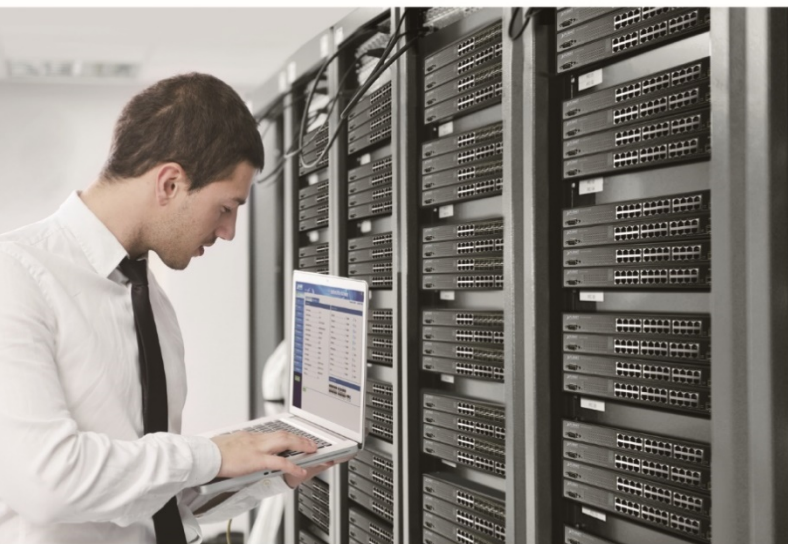




User's Manual

Industrial 5-Port 10/100/1000T VPN Security Gateway

▶ IVR-100 & IVR-300 Series



Copyright

Copyright (C) 2022 PLANET Technology Corp. All rights reserved.

The products and programs described in this User's Manual are licensed products of PLANET Technology. This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted.

No part of this User's Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means, electronic or mechanical including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of PLANET Technology.

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred. Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements and/or changes to this User's Manual at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

FCC Compliance Statement

This Equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE mark Warning



This is a class A device, In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

WEEE



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Trademarks

The PLANET logo is a trademark of PLANET Technology. This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies.

Revision

User's Manual of PLANET Industrial 5-Port 10/100/1000T VPN Security Gateway

Model: IVR-100, IVR-300, IVR-300W

Rev.: 1.1 (April, 2022)

Part No. EM-IVR-100_IVR-300 Series_v1.1

Table of Contents

Chapter 1. Product Introduction.....	7
1.1 Package Contents.....	7
1.2 Overview	8
1.3 Features	13
1.4 Product Specifications.....	15
Chapter 2. Hardware Introduction.....	19
2.1 Physical Descriptions	19
2.1.1 Front View	19
2.1.2 Top View.....	22
2.1.3 Wiring the Power Inputs.....	22
2.1.4 Wiring the Fault Alarm Contact	24
2.1.5 Dimensions	25
2.2 Hardware Installation	28
2.2.1 DIN-rail Mounting	28
2.2.2 Wall Mount Plate Mounting	29
2.2.3 Side Wall Mount Plate Mounting.....	31
2.2.4 Wi-Fi Antenna Installation	32
Chapter 3. Preparation	33
3.1 Requirements.....	33
3.2 Setting TCP/IP on your PC.....	33
3.2.1 Windows 7/8	33
3.2.2 Windows 10	37
3.3 Planet Smart Discovery Utility.....	39
Chapter 4. Web-based Management.....	42
4.1 Introduction.....	42
4.2 Logging in to the VPN Gateway	42
4.3 Main Web Page.....	44
4.4 System	46
4.4.1 Wizard.....	49
4.4.2 Dashboard	56
4.4.3 Status	58
4.4.4 System Service	59
4.4.5 Statistics.....	60
4.4.6 Connection Status.....	61

4.4.7	High Availability	61
4.4.8	RADIUS.....	63
4.4.9	Captive Portal	65
4.4.10	SNMP.....	66
4.4.11	NMS	67
4.4.12	Fault Alarm	69
4.4.13	Digital Input / Output	70
4.4.14	Modbus	72
4.4.15	Remote Syslog.....	73
4.5	Network	73
4.5.1	Priority.....	75
4.5.2	WAN.....	75
4.5.3	WAN Advanced.....	78
4.5.4	LAN	79
4.5.5	Multi-Subnet.....	79
4.5.6	VLAN.....	80
4.5.7	UPnP.....	80
4.5.8	Routing.....	81
4.5.9	RIP	82
4.5.10	OSPF	82
4.5.11	IGMP	83
4.5.12	IPv6.....	83
4.5.13	DHCP	84
4.5.14	DDNS.....	86
4.5.15	MAC Address Clone.....	88
4.6	Security	88
4.6.1	Firewall.....	90
4.6.2	MAC Filtering	92
4.6.3	IP Filtering.....	93
4.6.4	Web Filtering.....	95
4.6.5	Port Forwarding	96
4.6.6	QoS.....	97
4.6.7	DMZ	99
4.7	VPN	100
4.7.1	IPSec.....	101
4.7.2	IPsec Remote Server.....	105
4.7.3	GRE	105
4.7.4	PPTP.....	107
4.7.5	L2TP.....	108
4.7.6	SSL VPN.....	110

4.7.7	Certificates	111
4.7.8	VPN Connection	111
4.7.9	SD WAN	112
4.8	AP Control	112
4.8.1	Preference	115
4.8.2	AP Search	115
4.8.3	AP Management	116
4.8.4	AP Group Management	117
4.8.5	SSID Profile	118
4.8.6	Radio 2.4GHz Profile	119
4.8.7	Radio 5GHz Profile	120
4.8.8	Statistics AP Status	121
4.8.9	Map It	122
4.8.10	Upload Map	123
4.9	Wireless	123
4.9.1	2.4GHz WiFi	125
4.9.2	5GHz WiFi	126
4.9.3	MAC ACL	127
4.9.4	Wi-Fi Advanced	128
4.9.5	Wi-Fi Statistics	129
4.9.6	Connection Status	129
4.10	Maintenance	130
4.10.1	Administrator	131
4.10.2	Date and Time	132
4.10.3	Saving/Restoring Configuration	133
4.10.4	Firmware Upgrade	134
4.10.5	Reboot / Reset	135
4.10.6	Auto Reboot	136
4.10.7	Diagnostics	136
Appendix A: DDNS Application		138

Chapter 1. Product Introduction

Thank you for purchasing PLANET Industrial Security Gateway, IVR-100 and IVR-300 series. The descriptions of these models are as follows


IVR-100	Industrial 5-Port 10/100/1000T VPN Security Gateway
IVR-300	Industrial 5-Port 10/100/1000T VPN Security Gateway with Redundant Power
IVR-300W	Industrial 5-Port 10/100/1000T + 802.11ax Wi-Fi VPN Security Gateway

“VPN Gateway” mentioned in the manual refers to the above models.

1.1 Package Contents

The package should contain the following:

Model	IVR-100	IVR-300	IVR-300W
Item			
VPN Gateway	x 1	x 1	x 1
Quick Installation Guide	x 1	x 1	x 1
Wall-mount Kit	x 1	x 1	x 1
Dust Cap	x 5	x 5	x 5
CloudViewer QIG	x 1	x 1	x 1
RS485 3-pin Terminal Block	-	x 1	x 1
Dual band Wi-Fi Antenna	-	-	x 2
Antenna Dust Cap	-	-	x 2

 Note	<p>If any of the above items are missing, please contact your dealer immediately.</p>
--	---

1.2 Overview

Powerful Industrial VPN Security Solution

PLANET has launched the IVR-100 and IVR-300 Series Security Gateway for demanding applications. It features five Ethernet ports (4 LANs and 1 WAN), IEEE 11ax Wi-Fi capability (for IVR-300W), RS485 serial port (for IVR-300 / IVR-300W, and DI and DO interfaces. Incorporating SD-WAN function, it can greatly increase WAN optimization for multiple WAN links to be managed. Furthermore, its Dual-WAN Failover and Outbound Load Balance features can improve the network efficiency while the web-based interface provides friendly and user experience.

It's ideal for the harsh environment as it can operate stably at temperatures from **-40 to 75 degrees C**. Its compact **IP30** metal case allows either DIN-rail or wall mounting for efficient use of cabinet space.

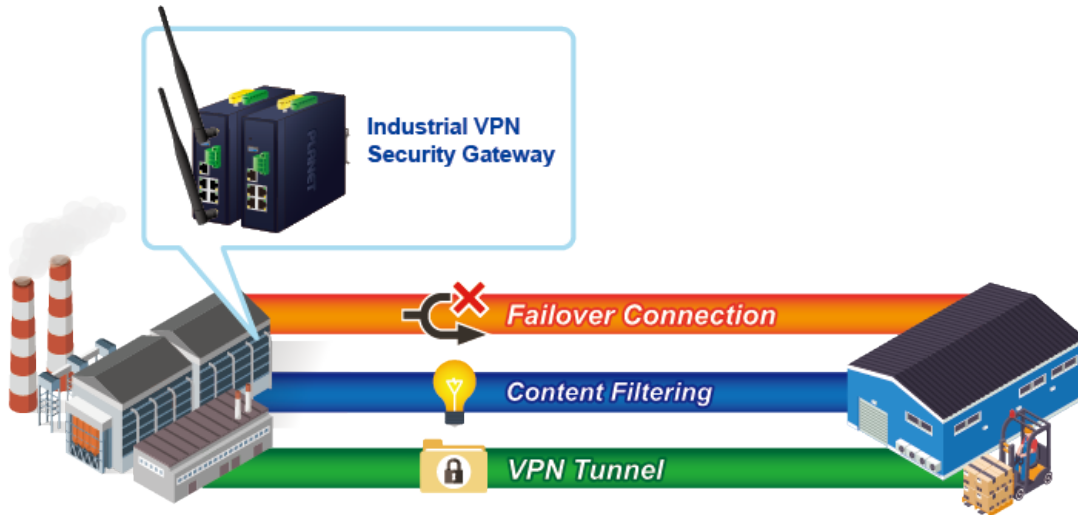


Wireless 11ax Brings Excellent Data Link Speed (For IVR-300W)

The IVR-300W is designed with high power amplifier and 2 highly-sensitive antennas which provide stronger signal and excellent coverage even in the wide-ranging or bad environment. With adjustable transmit power option, the administrator can flexibly reduce or increase the output power for various environments, thus reducing interference to achieve maximum performance. Equipped with the next-generation Wi-Fi 6 (802.11ax) wireless network standard, the total bandwidth reaches 1800Mbps, and the 2-stream transmission technology improves the transmission efficiency of multiple devices, making AR/VR/IoT applications smoother. The IEEE 802.11ax also optimizes MU-MIMO (Multi-User MIMO) mechanism to serve multiple devices simultaneously.

Ideal VPN Security Gateway Solution for Factories and Transportations

The IVR-100 and IVR-300 Series provides complete data security and privacy for accessing and exchanging the most sensitive data, built-in IPsec VPN function with DES/3DES/AES encryption and MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication, and GRE, SSL, PPTP and L2TP server mechanism. The full VPN capability in the IVR-100 and IVR-300 Series makes the connection secure, more flexible, and more capable.

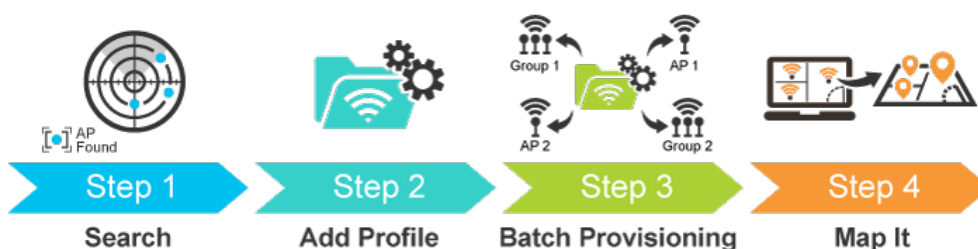


Centralized Remote Control of Managed APs

The IVR-100 and IVR-300 Series provides centralized management of PLANET Smart AP series via a user-friendly Web GUI. It's easy to configure AP for the wireless SSID, radio band and security settings. With a four-step configuration process, wireless profiles for different purposes can be simultaneously delivered to multiple APs or AP groups to minimize deployment time, effort and cost.

For example, to configure multiple smart APs of the same model, the IVR-100 and IVR-300 Series allows clustering them to a managed group for unified management. According to requirements, wireless APs can be flexibly expanded or removed from a wireless AP group at any time. The AP cluster benefits bulk provision and bulk firmware upgrade through single entry point instead of having to configure settings in each of them separately.

Simplified Cluster Management with 4 Steps



Wi-Fi Deployments and Authentication with Simplified Management (for IVR-300 Series)

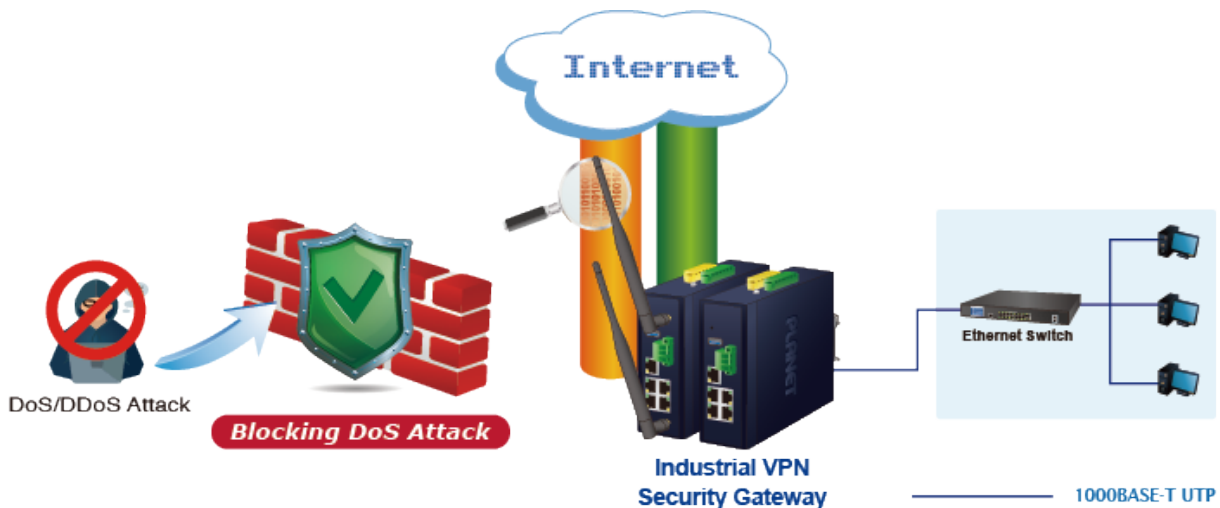
The IVR-300 Series also provides a built-in AP Controller, Captive Portal, RADIUS and a DHCP server to facilitate small and medium businesses to deploy secure employee and guest access services without any additional server. The IVR-300 Series can offer a secure Wi-Fi network with easy installation for your business.

Captive Portal



Excellent Ability in Threat Defense

The IVR-100 and IVR-300 Series has built-in SPI (stateful packet inspection) firewall and DoS/DDoS attack mitigation functions to provide high efficiency and extensive protection for your network. Thus, virtual server and DMZ functions can let you set up servers in the Intranet and still provide services to the Internet users.



Cybersecurity Network Solution to Minimize Security Risks

The cybersecurity feature included to protect the switch management in a mission-critical network virtually needs no effort and cost to install. For efficient management, the IVR-100 and IVR-300 Series are equipped with HTTPS web and SNMP management interfaces. With the built-in web-based management interface, the IVR-100 and IVR-300 Series offers an easy-to-use, platform independent management and configuration

facility. IVR-100 and IVR-300 Series supports SNMP and it can be managed via any management software based on the standard SNMP protocol.

Cost-effective Solution for RS-485 to Ethernet Application (for IVR-300 Series.)

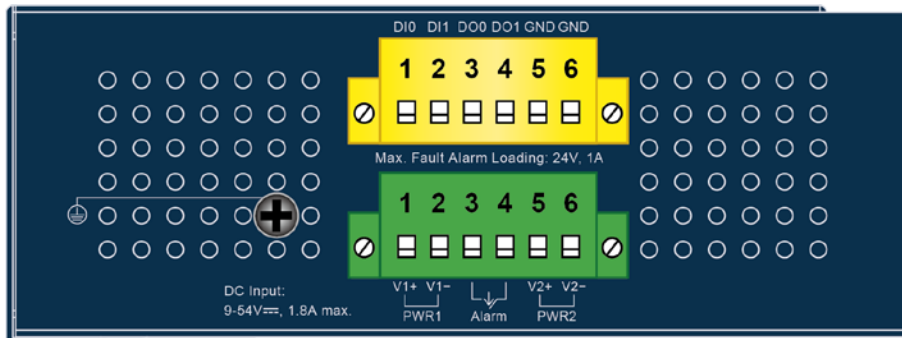
The IVR-100 and IVR-300 Series provides a feature that can convert the Serial RS-485 communication to IP networking. Ethernet signal allows two types of segments to connect easily, efficiently and inexpensively. The solution helps users and SIs save expenses as there is no need to replace the existing serial equipment and software system.

Convert Serial Communication to IP Networking



Convenient and Reliable Redundant Power System

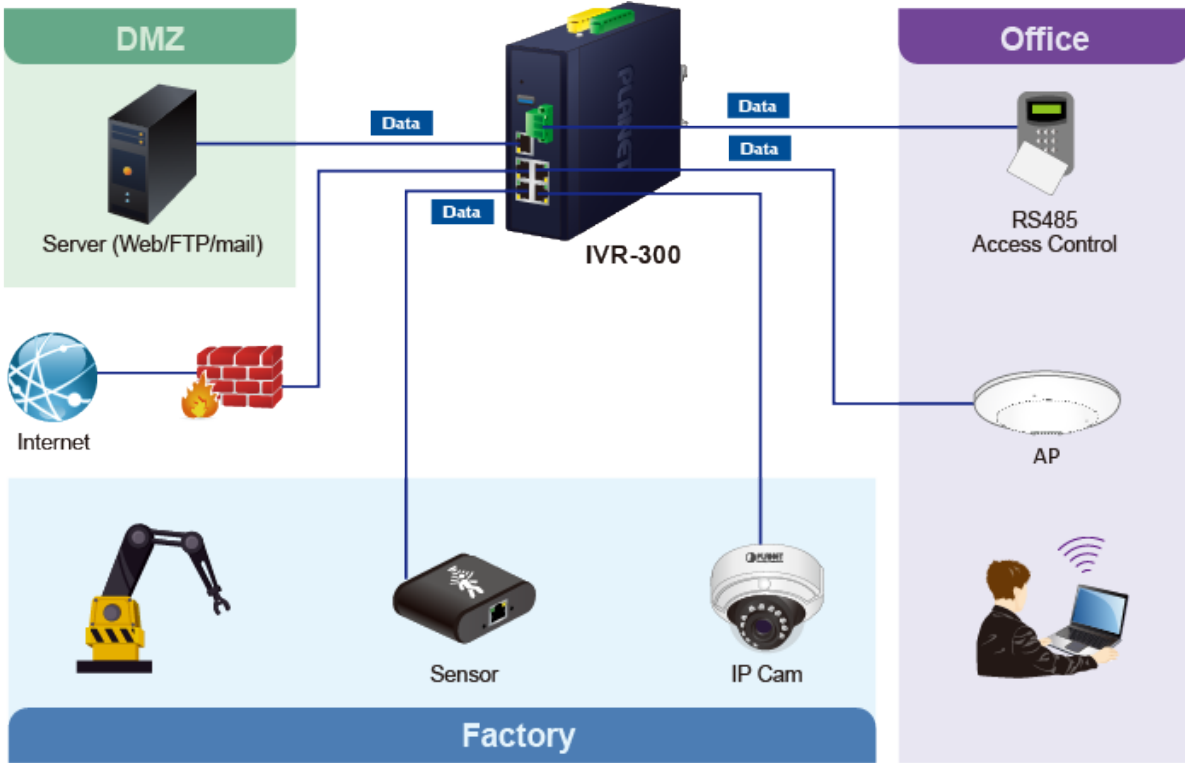
To facilitate transportation and industrial-level applications, the IVR-100 and IVR-300 Series provides an integrated power solution with a wide range of voltages (9~54V DC) for worldwide operability. It also provides dual-redundant, reversible polarity 9~54V DC power supply inputs for high availability applications.



Ideal VPN Security Gateway

PLANET IVR-100 and IVR-300 Series can work as a VPN security gateway in an industrial application for a company that has a factory and many different divisions. With IPSec/GRE/PPTP/L2TP/SSL VPN solutions, the IVR-100 and IVR-300 Series installed at the headquarters provides branches, vendors, and mobile workers with secure data communication no matter how long the distance would be.

The IVR-100 and IVR-300 Series connects dual WANs with up to two different ISPs. It creates a stable and qualified VPN connection for many important applications such as VoIP, video conferencing and data transmission.



1.3 Features

➤ **Hardware**

- 5 10/100/1000BASE-T RJ45 ports
- 1 undefined Ethernet port (LAN/WAN)
- Dual-WAN function
- 1 USB 3.0 port for system configuration backup and firmware upgrade
- 1 reset button
- 1 3-pin terminal block (RS485) (for IVR-300 Series)
- DIDO (for IVR-300 Series)

➤ **RF Interface Characteristics** (for IVR-300W)

- Features 2.4GHz (802.11b/g/n/ax) and 5GHz (802.11a/n/ac/ax) dual band for carrying high load traffic
- 2T2R MIMO technology for enhanced throughput and coverage
- Provides multiple adjustable transmit power control
- High speed up to 1.8Gbps (600Mbps for 2.4GHz or 1200Mbps for 5GHz) wireless data rate

➤ **Industrial Case and Installation**

- IP30 metal case
- Solid DIN-rail, wall-mount or side wall-mount design
- Supports 6KV DC Ethernet ESD protection
- Fault alarm for power input failure
- DC redundant power with reverse polarity protection
- -40 to 75 degrees C operating temperature

➤ **IP Routing Feature**

- Static Route
- Dynamic Route (RIPv1/v2)

➤ **Firewall Security**

- Cybersecurity
- Stateful Packet Inspection (SPI) firewall
- Blocks DoS/DDoS attack
- Content filtering
- MAC/IP filtering
- Blocks SYN/ICMP flooding
- NAT ALGs (Application Layer Gateway)

➤ **VPN Features**

- IPSec/Remote Server (Net-to-Net, Host-to-Net), GRE, PPTP Server, L2TP Server, SSL Server/Client (Open VPN)
- Max. Connection Tunnel Entries: 60 VPN tunnels,
- Encryption methods: DES, 3DES, AES, AES-128/192/256
- Authentication methods: MD5, SHA-1, SHA-256, SHA-384, SHA-512

➤ **Networking**

- Outbound load balancing for Ethernet WANs
- Auto-failover between Ethernet network WANs
- High Availability
- Captive Portal
- RADIUS Server
- Static IP/PPPoE/DHCP client for WAN
- DHCP server/NTP client for LAN
- Protocols: TCP/IP, UDP, ARP, IPv4, IPv6
- Port forwarding, QoS, DMZ, IGMP, UPnP, SNMPv1,v2c, v3
- MAC address clone
- DDNS: PLANET DDNS, Easy DDNS, DynDNS and No-IP

➤ **Others**

- Setup wizard
- Dashboard for real-time system overview
- Support for HTTP or HTTPS
- Auto reboot
- PLANET NMS System and Smart Discovery Utility for deployment management
- PLANET CloudViewer app for real-time monitoring
- Configuration backup and restoration via remote/USB port
- Firmware upgrade via remote/USB port

1.4 Product Specifications

Product	IVR-100	IVR-300	IVR-300W	
Hardware Specifications				
Copper Ports	5 10/100/1000BASE-T RJ45 Ethernet ports including 3 LAN ports (Ports 1 to 3) 1 LAN/WAN port (Port 4) 1 WAN port (Port 5)			
USB Port	1 USB 3.0 port	1 USB 3.0 port	1 USB 3.0 port	
Wireless Connector	-	-	Two RP-SMA female connectors	
Wireless Antenna	-	-	Two 5 dBi external antennas	
Serial Interface	-	1 x 3-pin terminal block for RS485		
DI & DO Interfaces	-	2 Digital Input (DI): Level 0: -24V~2.1V (±0.1V) Level 1: 2.1V~24V (±0.1V) Input Load to 24V DC, 10mA max.		
DI & DO Interfaces	-	2 Digital Output (DO): Open collector to 24V DC, 100mA max.		
Connector	Removable 6-pin terminal block for power input Pin 1/2 for Power 1, Pin 3/4 for fault alarm, Pin 5/6 for Power 2			
Reset Button	< 5 sec: System reboot > 5 sec: Factory default			
Enclosure	IP30 metal case			
Installation	DIN rail, desktop, wall-mounting			
Dimensions (W x D x H)	50 x 87.5 x 135 mm	50 x 135 x 135 mm	50 x 135 x 135 mm	
Weight	530g	712g	773g	
Power Requirements – DC	9~54V DC, 1.0A	9~54V DC, 1.8A	9~54V DC, 1.8A	
Power Consumption	No Loading	Max. 3.8 watts/ 12.97 BTU	Max. 3.7 watts/ 12.61 BTU	Max. 3.8 watts/ 12.95 BTU
	Full Loading	Max. 9 watts/ 30.71 BTU	Max. 8.7 watts/ 29.66 BTU	Max.15.6 watts/ 53.19 BTU
LED Indicators	System: P1 (Green) P2 (Green) Fault (Red)	System: P1 (Green) P2 (Green) Alarm (Red) I/O (Red)	System: P1 (Green) P2 (Green) Alarm (Red) I/O (Red)	

	<p>Ethernet Interfaces (Ports 1-4 and WAN Port):</p> <p>1000 LNK/ACT (Green)</p> <p>10/100 LNK/ACT (Amber)</p>	<p>Ethernet Interfaces (Ports 1-4 and WAN Port):</p> <p>1000 LNK/ACT (Green)</p> <p>10/100 LNK/ACT (Amber)</p>	<p>Ethernet Interfaces (Ports 1-4 and WAN Port):</p> <p>1000 LNK/ACT (Green)</p> <p>10/100 LNK/ACT (Amber)</p> <p>Wi-Fi:</p> <p>2.4G(Green)</p> <p>5G(Green)</p>
Advanced Functions			
VPN	<p>IPSec/Remote Server (Net-to-Net, Host-to-Net)</p> <p>GRE</p> <p>PPTP Server</p> <p>L2TP Server</p> <p>SSL Server/Client (Open VPN)</p>		
VPN Tunnels	Max. 60	Max. 60	Max. 60
VPN Throughput	Max. 60Mbps	Max. 108Mbps	Max. 108Mbps
Encryption Methods	DES, 3DES, AES or AES-128/192/256 encrypting		
Authentication Methods	MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication algorithm		
Management			
Basic Management Interfaces	<p>Web browser</p> <p>SNMP v1, v2c</p> <p>PLANET Smart Discovery utility and NMS controller supported</p>		
Secure Management Interfaces	TLSv1.2, SNMP v3		
System Log	System Event Log		
Others	<p>Setup wizard</p> <p>Dashboard</p> <p>System status/service</p> <p>Statistics</p> <p>Connection status</p> <p>Auto reboot</p> <p>Diagnostics</p>		
Standards Conformance			
Regulatory Compliance	CE, FCC		
Environment			
Operating	<p>Temperature: -40 ~ 75 degrees C</p> <p>Relative humidity: 5 ~ 90% (non-condensing)</p>		

Storage	Temperature: -40 ~ 85 degrees C Relative humidity: 5 ~ 90% (non-condensing)
----------------	--

■ **Wireless Specification for IVR-300W**

Model		
Wireless		
Standard		IEEE 802.11a/n/ac/ax 5GHz IEEE 802.11g/b/n/ax 2.4GHz
Band Mode		2.4G & 5G concurrent mode
Antenna		5 dBi external antennas with SMA connectors for Wi-Fi
Frequency Range	2.4GHz	America FCC: 2.412~2.462GHz Europe ETSI: 2.412GHz~2.472GHz
	5GHz	5.15GHz ~5.875GHz
Operating Channels	2.4GHz	America FCC: 1~11 Europe ETSI: 1~13
	5GHz	<u>America FCC:</u> Non-DFS: 36, 40, 44, 48, 149,153,157,161,165 DFS: 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140 <u>Europe ETSI:</u> Non-DFS: 36, 40, 44, 48 DFS: 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 5GHz channel list may vary in different countries according to their regulations.
Channel Width		
Data Transmission Rates		Transmit: 600 Mbps* for 2.4 GHz and 1200 Mbps* for 5 GHz Receive: 600 Mbps* for 2.4 GHz and 1200 Mbps* for 5 GHz *The estimated transmission distance is based on the theory. The actual distance may vary in different environments.
Transmission Power		11b: 23dbm+/- 1.5dbm @11Mbps 11g: 20dbm+/- 1.5dbm @54Mbps 11g/n: 20dBm +/- 1.5dbm @MCS7, HT20 17dBm@MCS7,HT40 11a: 19.5dBm +/- 1.5dbm @54Mbps 11a/n: 19.5dBm+/- 1.5dbm @MCS7, HT20 17dBm@MCS7, HT40 11ac HT20: 20+/-1.5dBm @MCS8 11ac HT40: 17+/-1.5dBm @MCS9

	<p>11ac HT80: 14.5+/-1.5dBm @MCS9 11ax HT20: 20+/-1.5dBm @MCS9 11ax HT40: 17 +/- 1.5dBm @MCS9 11ax HT80: 14.5 +/- 1.5dBm @MCS11</p>
Encryption Security	<p>WEP (64/128-bit) encryption security WPA / WPA2 (TKIP/AES) WPA-PSK / WPA2-PSK (TKIP/AES) / WPA3-PSK (TKIP/AES) 802.1x Authenticator</p>
Wireless Advanced	<p>Wi-Fi Multimedia (WMM) Auto channel selection Wireless output power management MAC address filtering</p>

Chapter 2. Hardware Introduction

2.1 Physical Descriptions

2.1.1 Front View

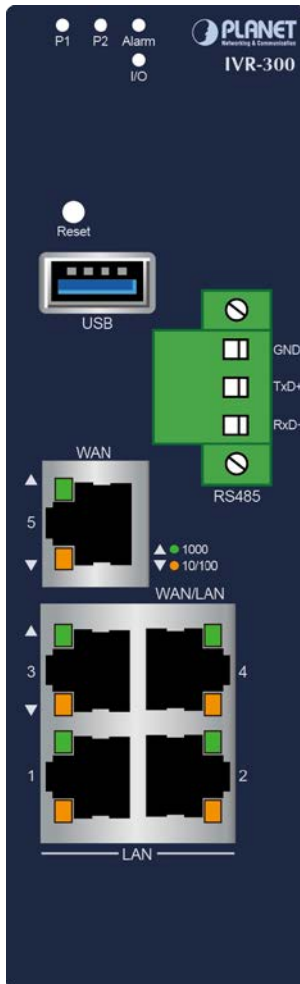
IVR-100 Front Panel



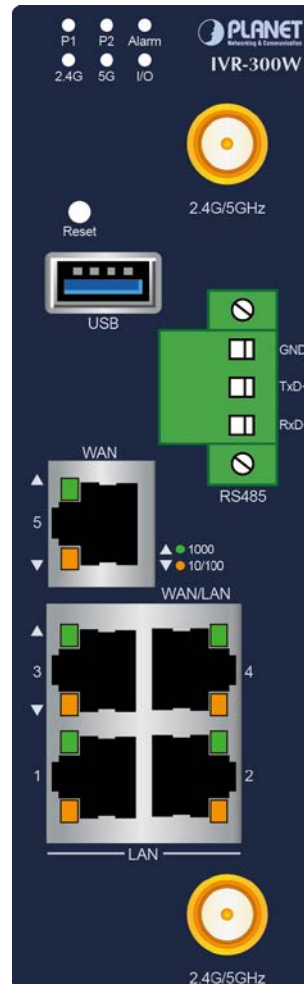
LED	Color	Function	
P1	Green	Lights to indicate DC power input 1 has power.	
P2	Green	Lights to indicate DC power input 2 has power.	
Fault	Red	Lights to indicate the either power or port fail	
1000 LNK/ACT	Green	Lights	Indicates the link through that port is successfully established at 1000Mbps
		Blinks	Indicates that the Switch is actively sending or receiving data over that port.
100 LNK/ACT	Amber	Lights	Indicates the link through that port is successfully established at 100Mbps.
		Blinks	Indicates that the Switch is actively sending or receiving data over that port.

Ports	
USB Port	USB 3.0 port for system configuration backup and restoration.
Reset Button	Power on the device and press the reset button for less than 5 seconds to reboot it or over 5 seconds to restore it to factory default settings.
Gigabit Ports 1-3	It is a LAN port for connecting to a switch.
Gigabit Port 4	Default is LAN port. It can be defined as LAN port or WAN port.
Gigabit Port 5	It is a WAN port for connecting to a perimeter gateway.

IVR-300 Front Panel



IVR-300W Front Panel



LED Definition:

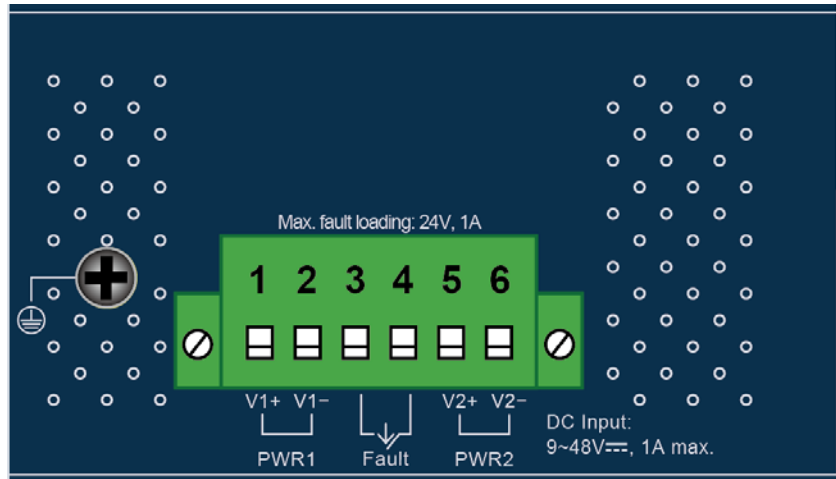
LED	Color	Function	
P1	Green	Lights to indicate DC power input 1 has power.	
P2	Green	Lights to indicate DC power input 2 has power.	
Alarm	Red	Lights to indicate the either power or port fail	
I/O	Red	Indicate Condition of Digital Input or Digital Output has triggered.	
2.4G	Green	Lights up when 2.4G Wi-Fi service is enabled (for IVR-300W)	
5G	Green	Lights up when 5G Wi-Fi service is enabled (for IVR-300W)	
1000 LNK/ACT	Green	Lights	Indicates the link through that port is successfully established at 1000Mbps
		Blinks	Indicates that the Switch is actively sending or receiving data over that port.
100 LNK/ACT	Amber	Lights	Indicates the link through that port is successfully established at 100Mbps.
		Blinks	Indicates that the Switch is actively sending or receiving data over that port.

Ports	
USB Port	USB 3.0 port for system configuration backup and restoration.
Reset Button	Power on the device and press the reset button for less than 5 seconds to reboot it or over 5 seconds to restore it to factory default settings.
Serial Interface	1 x 3-pin terminal block for RS485
Gigabit Ports 1-3	It is a LAN port for connecting to a switch.
Gigabit Port 4	Default is LAN port. It can be defined as LAN port or WAN port.
Gigabit Port 5	It is a WAN port for connecting to a perimeter gateway.

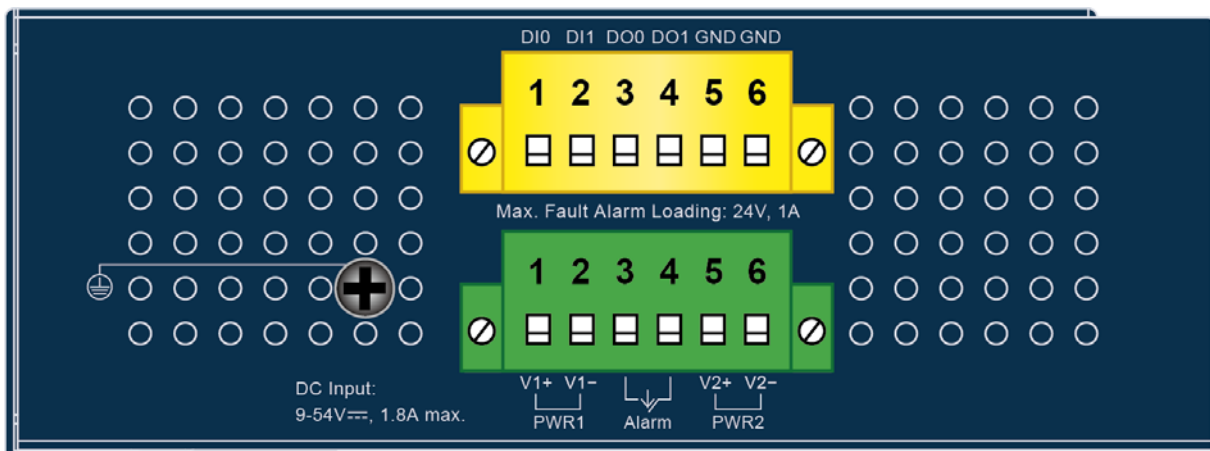
2.1.2 Top View

The upper panel of the Industrial Gateway consists of one terminal block connector within two DC power inputs.

IVR-100 Top View



IVR-300 Series Top View



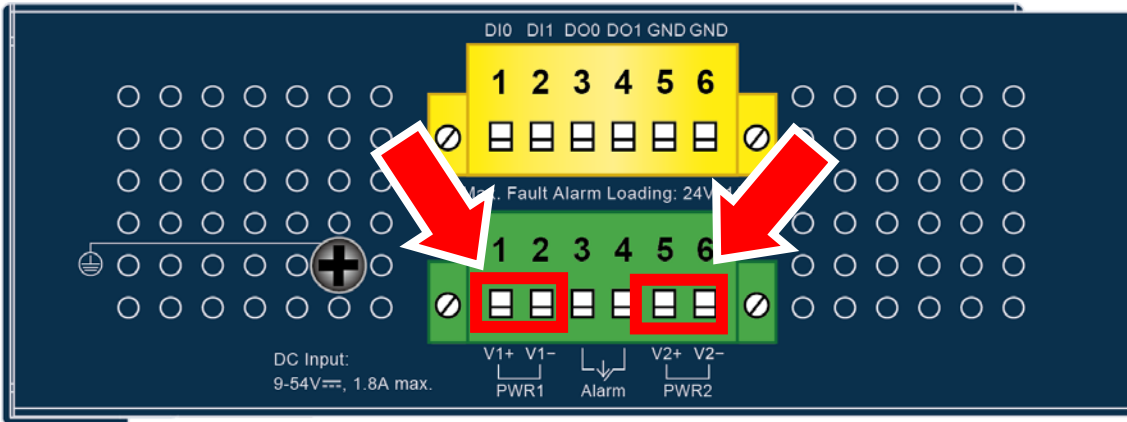
2.1.3 Wiring the Power Inputs

The 6-contact terminal block connector on the top panel of Industrial Gateway is used for two DC redundant power inputs. Please follow the steps below to insert the power wire.



When performing any of the procedures like inserting the wires or tightening the wire-clamp screws, make sure the power is OFF to prevent from getting an electric shock.

1. Insert positive and negative DC power wires into contacts 1 and 2 for POWER 1, or 5 and 6 for POWER 2.v



To avoid damage, please use the Industrial Gateway under its specification.

2. Tighten the wire-clamp screws for preventing the wires from loosening.



1	2	3	4	5	6
Power 1		Alarm		Power 2	
+	-			+	-



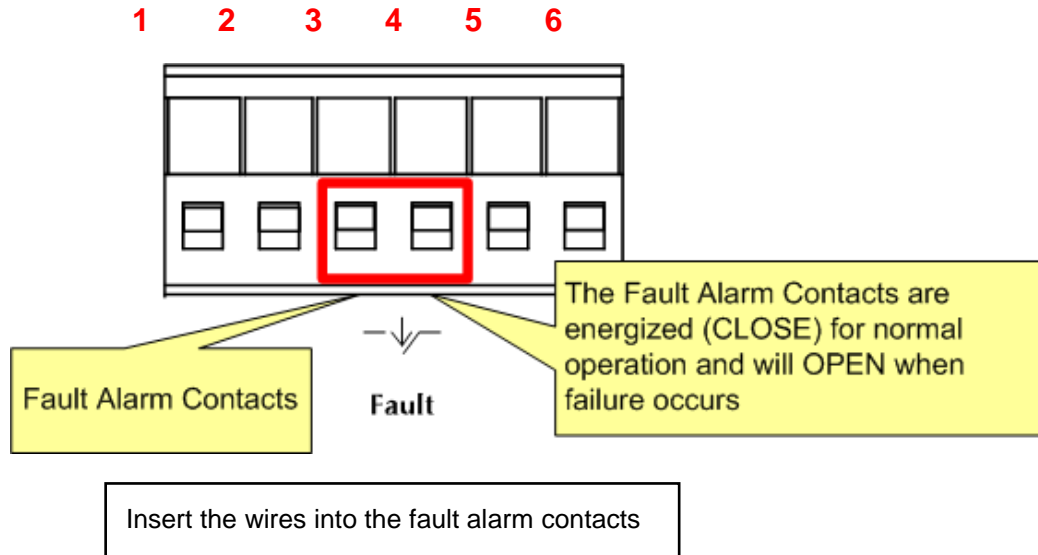
The wire gauge for the terminal block should be in the range from 12 to 24 AWG.



PWR1 and PWR2 must provide the **same DC voltage** while operating with dual power input.

2.1.4 Wiring the Fault Alarm Contact

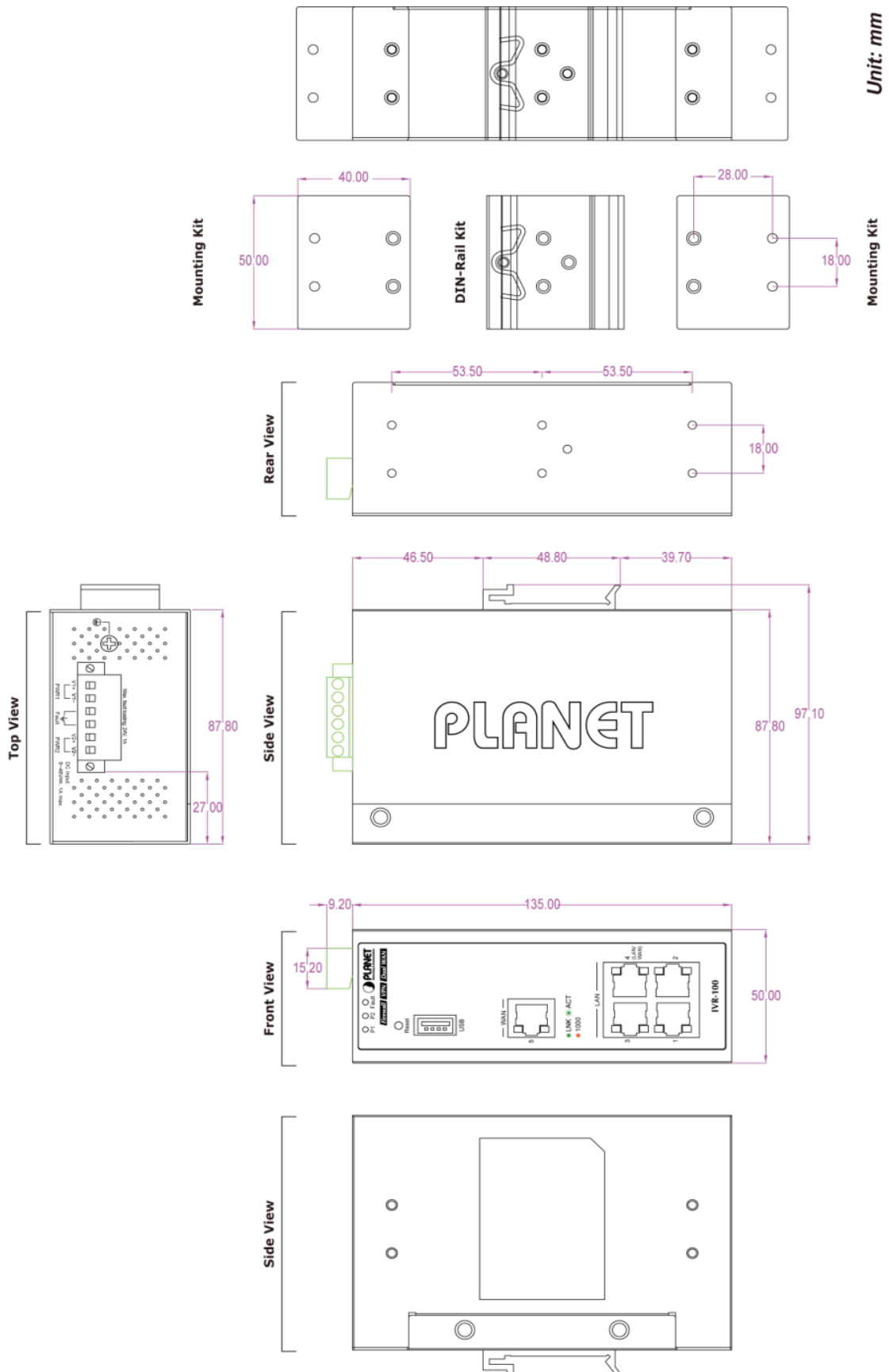
The fault alarm contacts are in the middle of the terminal block connector as the picture shows below. Inserting the wires, the Industrial Gateway will detect the fault status of the power failure and then forms an open circuit. The following illustration shows an application example for wiring the fault alarm contacts.



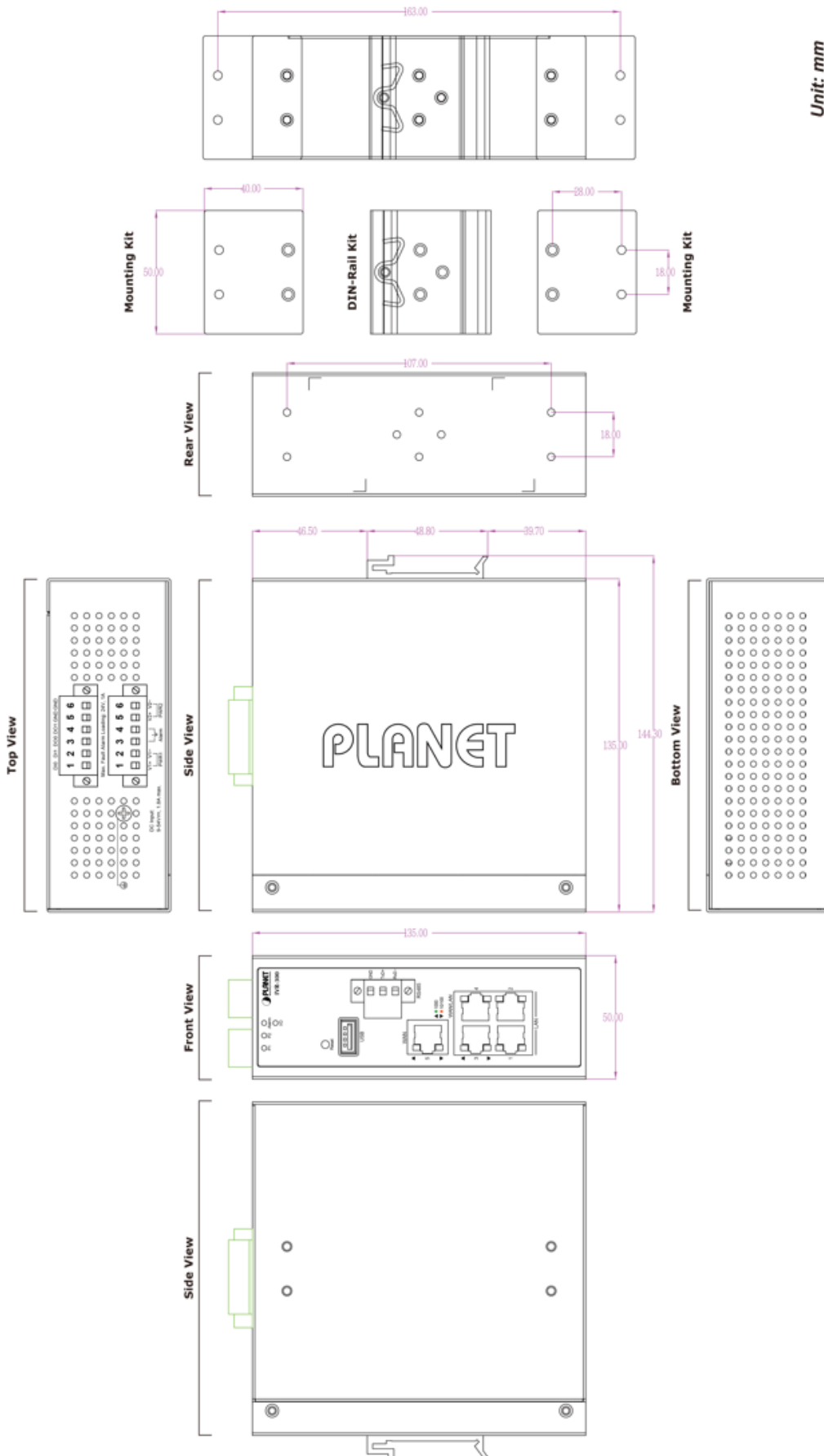
1. The wire gauge for the terminal block should be in the range between 12 and 24 AWG.
2. Alarm relay circuit accepts up to 24V, max. 1A currents.

2.1.5 Dimensions

IVR-100 Dimensions



IVR-300 Dimensions



Unit: mm

2.2 Hardware Installation

This section describes how to install the Industrial Gateway. There are three methods to install the Industrial Gateway -- DIN-rail mounting, wall mounting and side wall mounting. Basic knowledge of networking is assumed.

Please read the following sections and perform the procedures in the order being presented.

(The device shown on this chapter is just a representation of the said device.)

2.2.1 DIN-rail Mounting

Step 1: Lightly slide the DIN-rail into the track.



Step 2: Check whether the DIN-rail is tightly on the track.



Step 3: Connect your device to hub / switch.

- A. Connect one end of a standard network cable to the LAN port (port 1) of the device.
- B. Connect the other end of the cable to the hub / switch.



The UTP Category 5, 5e or 6 network cabling with RJ45 tips is recommended.

Step 4: Connect your device to internet.

- A. Connect one end of a standard network cable to the WAN port (port 5) of the device.
- B. Connect the other end of the cable to the LAN port of ISP network device (such as a modem).



If there is only one line connected to the outer network in your network environment, it is suggested that you use WAN port (port 5).

Step 5: Power on the device. When the device receives power, the Power LED should remain solid Green.

2.2.2 Wall Mount Plate Mounting

To install the Industrial Gateway on the wall, please follow the instructions below.

Step 1: Remove the DIN-rail from the Industrial Gateway. Use the screwdriver to loosen the screws to remove the DIN-rail.

Step 2: Place the wall-mount plate on the rear panel and use the screwdriver to screw the wall mount plate tightly on the Industrial Gateway.



Step 3: Use the hook holes at the corners of the wall mount plate to hang the Industrial Gateway on the wall.



Step 4: To remove the wall mount plate, reverse the steps above.

Step 5: Proceed with Steps 3, 4 and 5 in Section 2.2.1 DIN-rail Mounting to connect the network cabling and power on the device.

2.2.3 Side Wall Mount Plate Mounting

To install the Industrial Gateway on the wall, please follow the instructions below.

Step 1: Remove the DIN-rail from the Industrial Gateway. Use the screwdriver to loosen the screws to remove the DIN-rail.

Step 2: Place the wall-mount plate on the side panel and use the screwdriver to screw the wall mount plate tightly on the Industrial Gateway.



Step 3: Use the hook holes at the corners of the wall mount plate to hang the Industrial Gateway on the wall.



Step 4: To remove the wall mount plate, reverse the steps above.

Step 5: Proceed with Steps 3, 4 and 5 in Section 2.2.1 DIN-rail Mounting to connect the network cabling and power on the device.

2.2.4 Wi-Fi Antenna Installation

(For IVR-300W only)

Step 1: Fasten the two dual-band antennas to the antenna connectors on the front panel of the IVR-300W.

Step 2: You can bend the antennas to fit your actual needs.

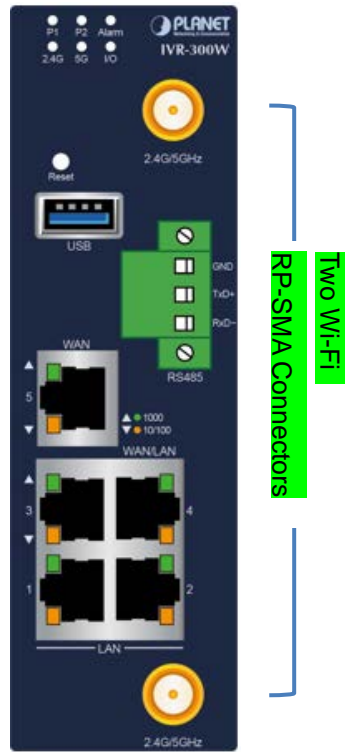


Figure 2-2: IVR-300W Front Panel

Chapter 3. Preparation

Before getting into the device's web UI, user has to check the network setting and configure PC's IP address.

3.1 Requirements

User is able to confirm the following items before configuration:

1. Please confirm the network is working properly; it is strongly suggested to test your network connection by connecting your computer directly to ISP.
2. Suggested operating systems: Windows 7 / 8 / 10.
3. Recommended web browsers: IE / Firefox / Chrome.

3.2 Setting TCP/IP on your PC

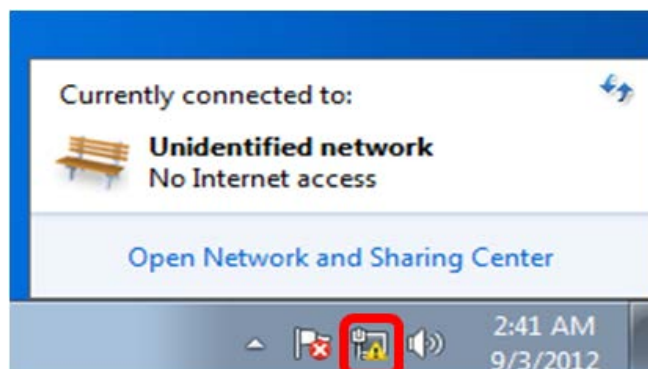
The default IP address of the VPN Gateway is 192.168.1.1, and the DHCP Server is on. Please set the IP address of the connected PC as DHCP client, and the PC will get IP address automatically from the VPN Gateway.

Please refer to the following to set the IP address of the connected PC.

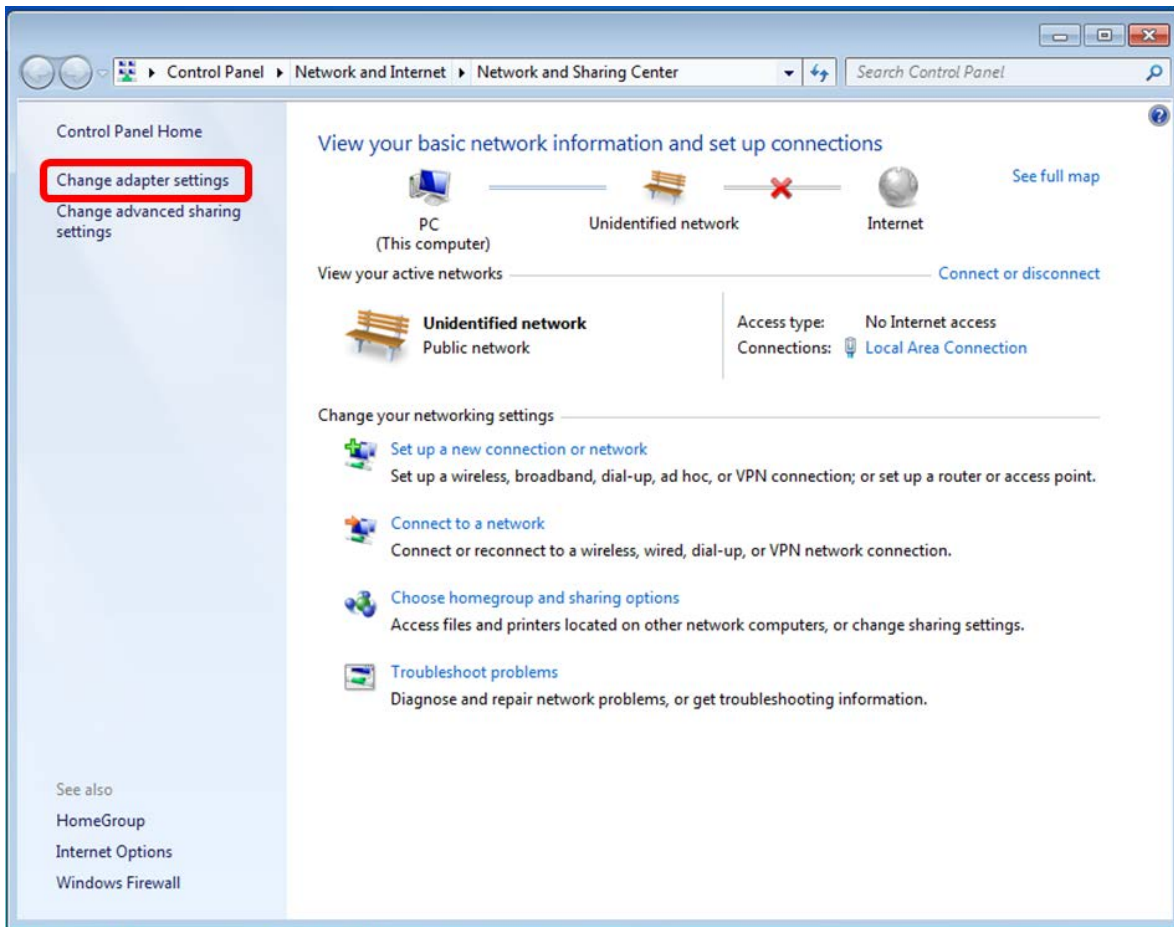
3.2.1 Windows 7/8

If you are using Windows 7/8, please refer to the following:

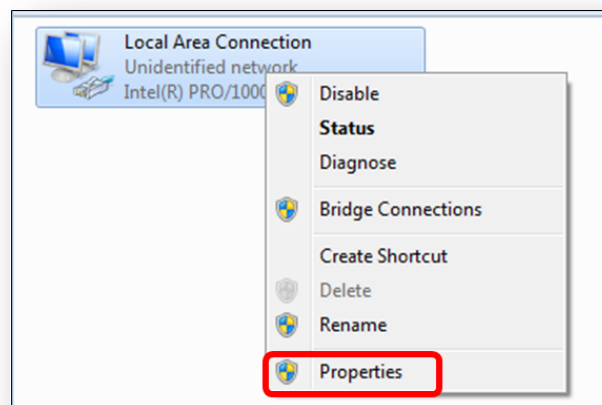
1. Click on the network icon from the right side of the taskbar and then click on "Open Network and Sharing Center".



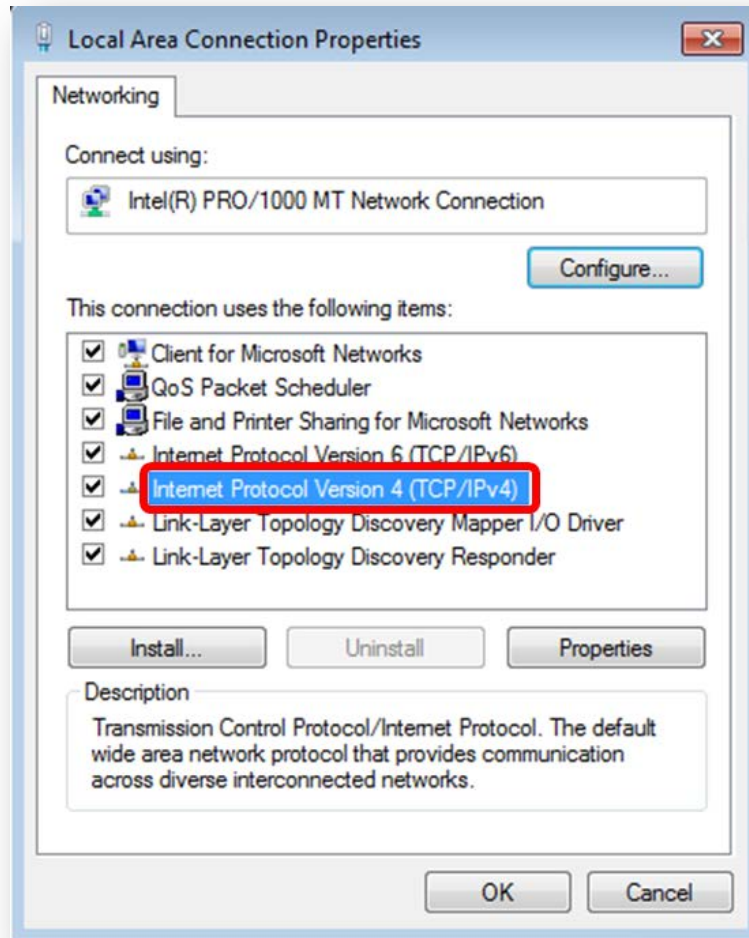
2. Click "Change adapter settings".



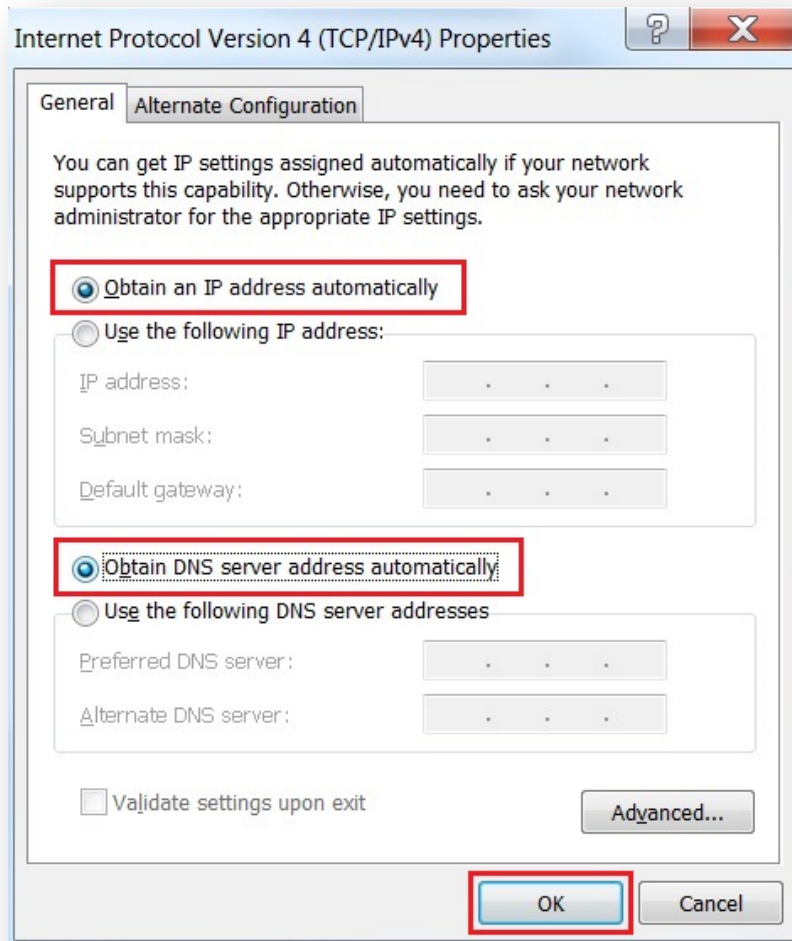
3. Right-click on the Local Area Connection and select Properties.



4. Select Internet Protocol Version 4 (TCP/IPv4) and click Properties or directly double-click on Internet Protocol Version 4 (TCP/IPv4).



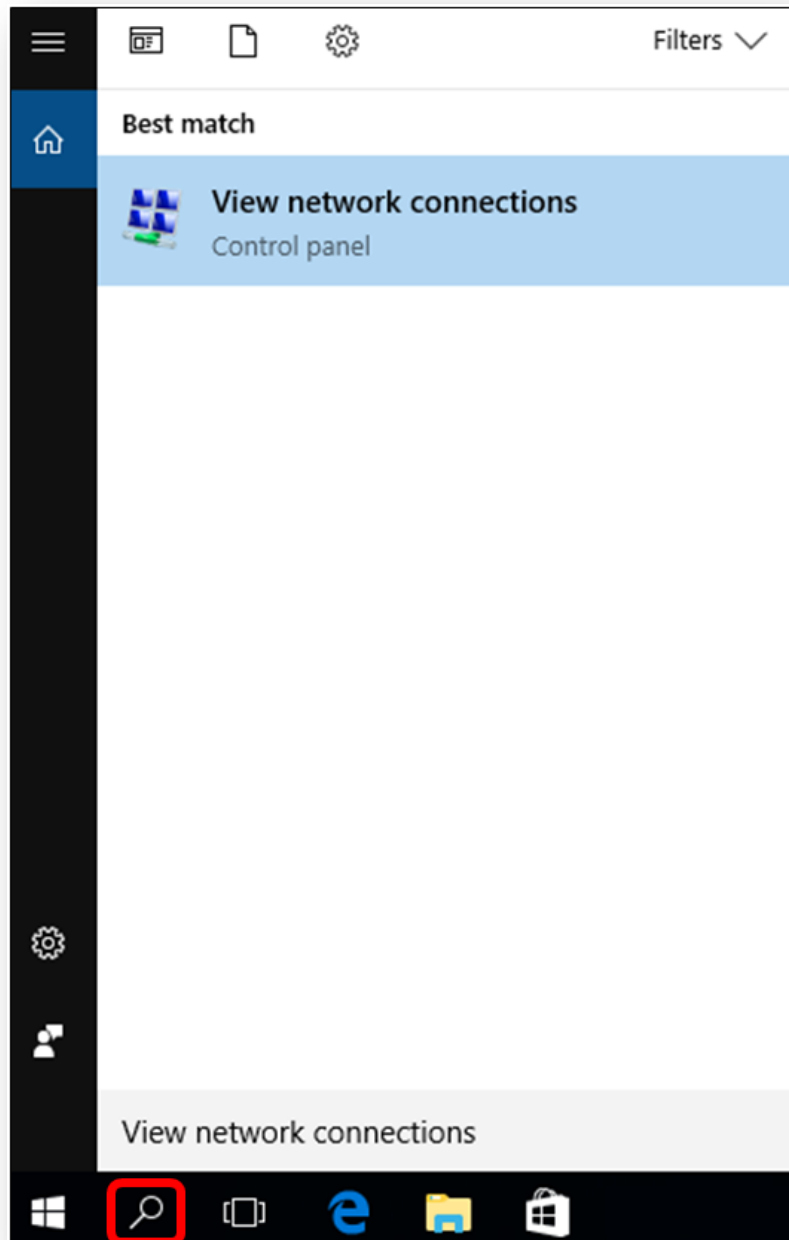
5. Select "Use the following IP address" and "Obtain DNS server address automatically", and then click the "OK" button.



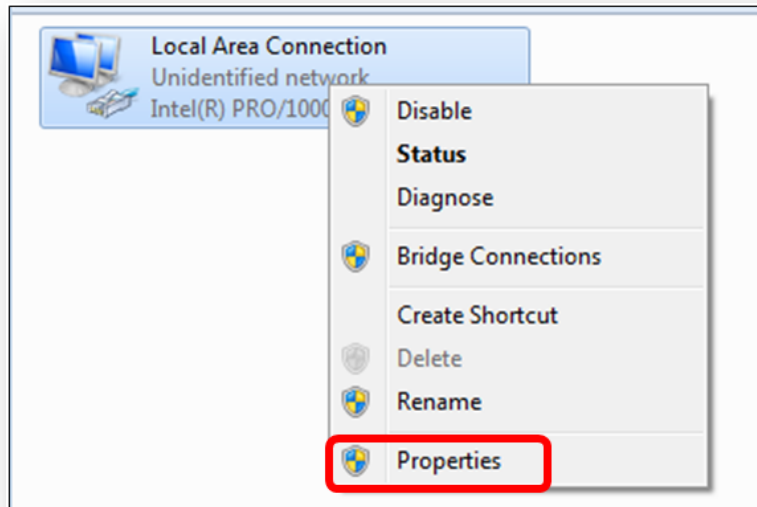
3.2.2 Windows 10

If you are using Windows 10, please refer to the following:

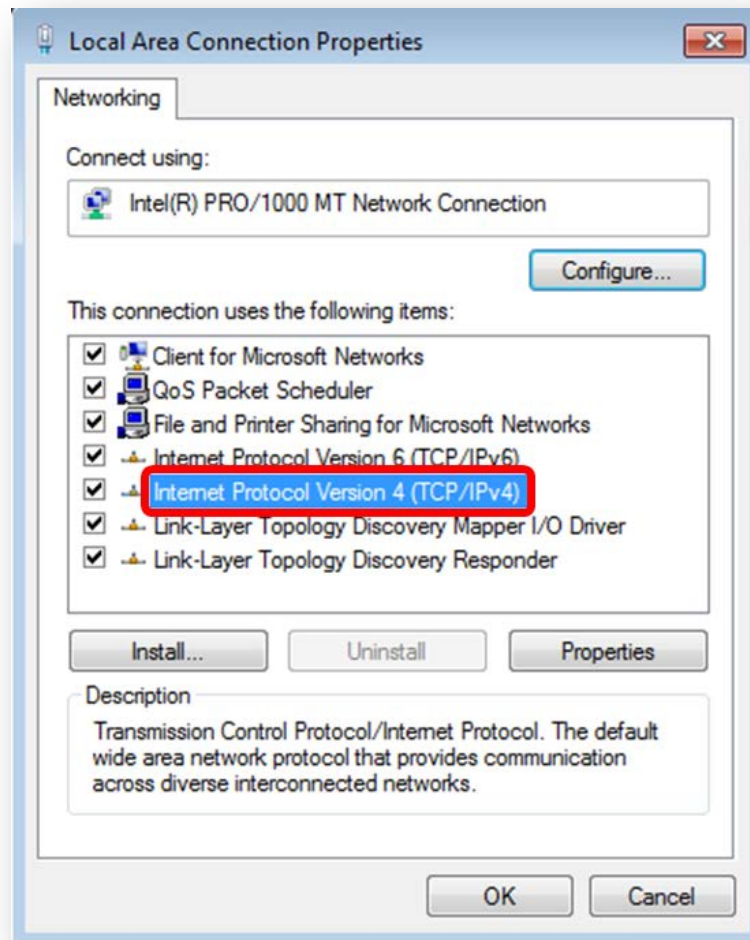
1. In the search box on the taskbar, type “View network connections”, and then select View network connections at the top of the list.



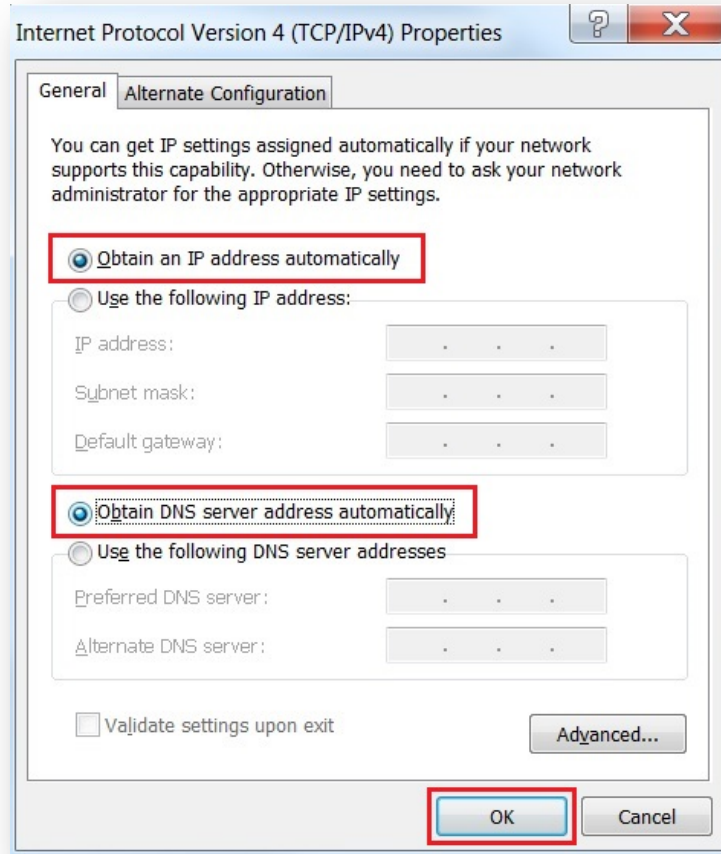
2. Right-click on the Local Area Connection and select Properties.



3. Select Internet Protocol Version 4 (TCP/IPv4) and click Properties or directly double-click on Internet Protocol Version 4 (TCP/IPv4).



4. Select "Use the following IP address" and "Obtain DNS server address automatically", and then click the "OK" button.



3.3 Planet Smart Discovery Utility

For easily listing the Gateway in your Ethernet environment, the search tool -- Planet Smart Discovery Utility -- is an ideal solution.

The following installation instructions are to guide you to running the Planet Smart Discovery Utility.

1. Download the Planet Smart Discovery Utility in administrator PC.
2. Run this utility as the following screen appears.

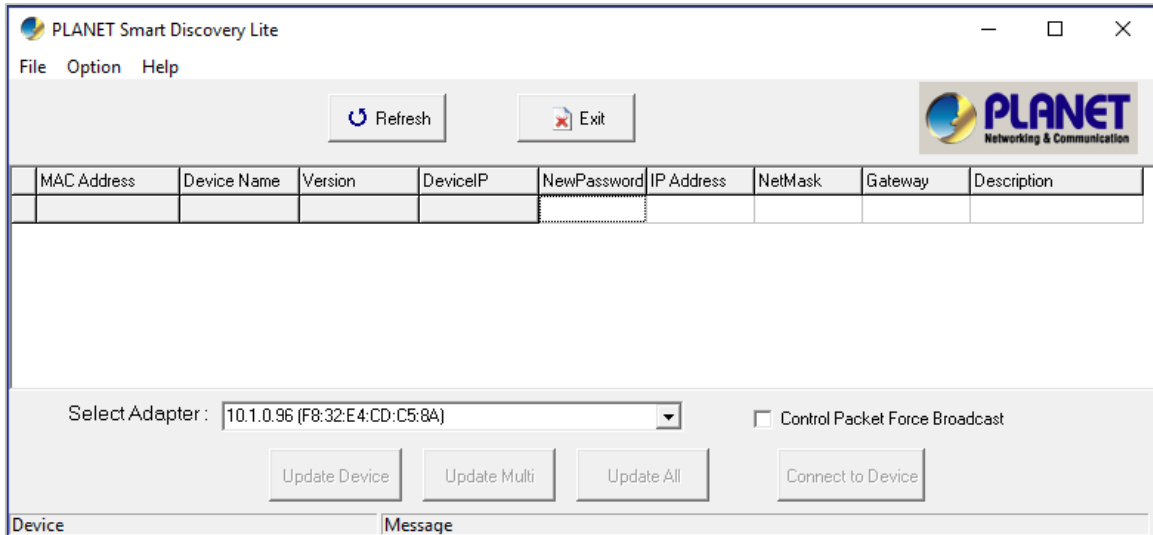


Figure: Planet Smart Discovery Utility Screen



If there are two LAN cards or above in the same administrator PC, choose a different LAN card by using the **“Select Adapter”** tool.

3. Press the **“Refresh”** button for the currently connected devices in the discovery list as the screen shows below:

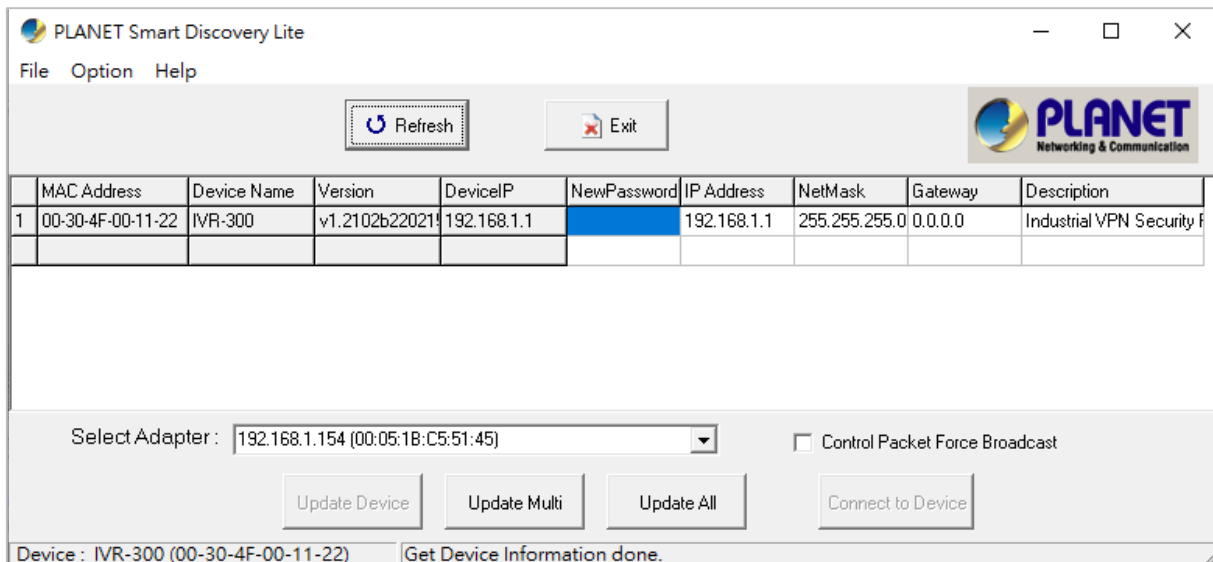


Figure: Planet Smart Discovery Utility Screen

1. This utility shows all necessary information from the devices, such as MAC address, device name, firmware version, and device IP subnet address. It can also assign new password, IP subnet address and description to the devices.
2. After setup is completed, press the **“Update Device”**, **“Update Multi”** or **“Update All”** button to take effect. The functions of the 3 buttons above are shown below:
 - **Update Device:** use current setting on one single device.

- **Update Multi:** use current setting on choose multi-devices.
- **Update All:** use current setting on whole devices in the list.

The same functions mentioned above also can be found in “**Option**” tools bar.

3. To click the “**Control Packet Force Broadcast**” function, it allows you to assign a new setting value to the device under a different IP subnet address.
4. Press the “**Connect to Device**” button and the Web login screen appears.

Press the “**Exit**” button to shut down the Planet Smart Discovery Utility.

Chapter 4. Web-based Management

This chapter provides setup details of the device's Web-based Interface.

4.1 Introduction

The device can be configured with your Web browser. Before configuring, please make sure your PC is under the same IP segment with the device.

4.2 Logging in to the VPN Gateway

Refer to the steps below to configure the VPN Gateway:

- Step 1.** Connect the IT administrator's PC and VPN Gateway's LAN port (port 1) to the same hub / switch, and then launch a browser to link the management interface address which is set to **http://192.168.1.1** by default.



The DHCP server of the VPN Gateway is enabled. Therefore, the LAN PC will get IP from the VPN Gateway. If user needs to set IP address of LAN PC manually, please set the IP address within the range between 192.168.1.2 and 192.168.1.254 inclusively, and assigned the subnet mask of 255.255.255.0.

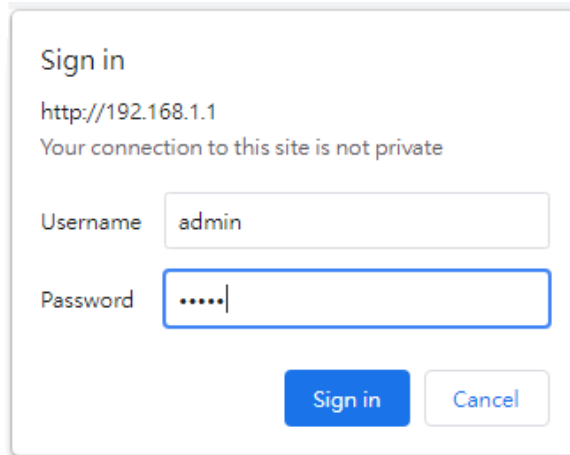
- Step 2.** The browser prompts you for the login credentials. (Both are "**admin**" by default.)

Default IP address: **192.168.1.1**
Default user name: **admin**
Default password: **admin**
Default 2.4GHz SSID: **PLANET_2.4G (for IVR-300W)**
Default 5GHz SSID: **PLANET_5G (for IVR-300W)**



Administrators are strongly suggested to change the default admin and password to ensure system security.

Web Login Screen as below:



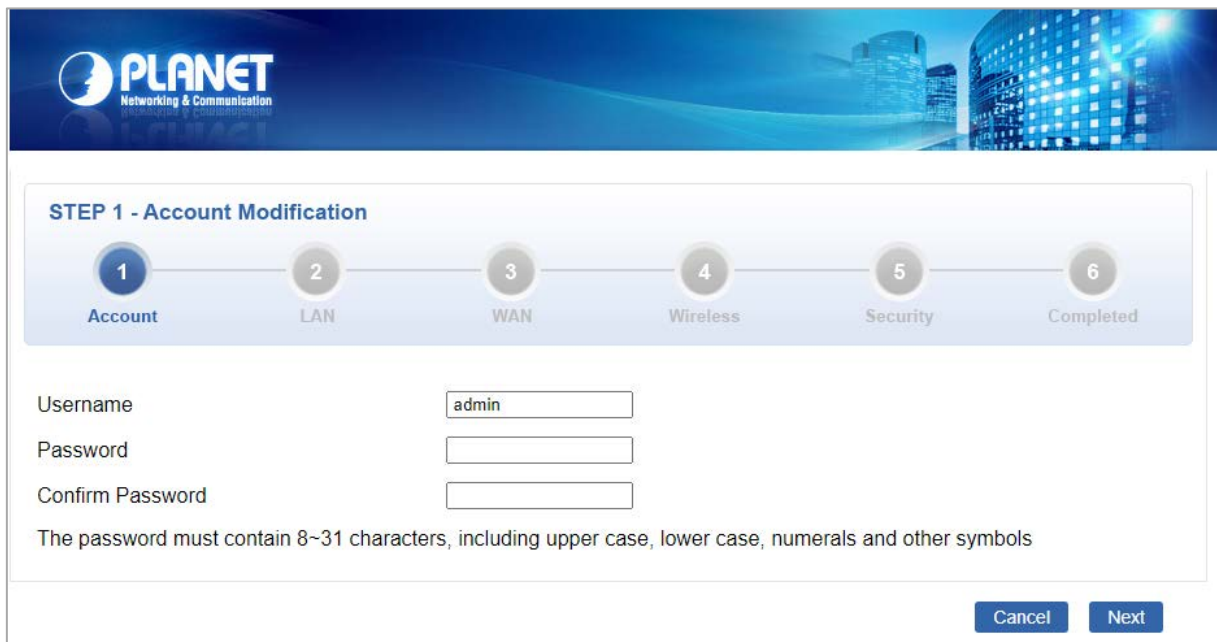
Sign in
http://192.168.1.1
Your connection to this site is not private

Username

Password

Please follow the wizard to do the first-time account modification.

The password must contain 8~31 characters, including upper case, lower case, numerals and other symbols



PLANET
Networking & Communication

STEP 1 - Account Modification

1 Account — 2 LAN — 3 WAN — 4 Wireless — 5 Security — 6 Completed

Username

Password

Confirm Password

The password must contain 8~31 characters, including upper case, lower case, numerals and other symbols

Figure: Account Modification

After modifying the new account and password, the main screen appears as shown below:



Figure Web Main Screen

Now, you can use the Web management interface to continue the Security Gateway management or manage the Security Gateway by console interface. Please refer to the user’s manual for more.

Administrators are strongly suggested to change the default password and Wi-Fi SSID on the first login to safeguard system security.



1. For security reason, **please change and memorize the new password after this first setup.**
2. Only accept command in lowercase letter under web interface.

4.3 Main Web Page

After a successful login, the main web page appears. The web main page displays the web panel, main menu, function menu, and the main information in the center as shown below

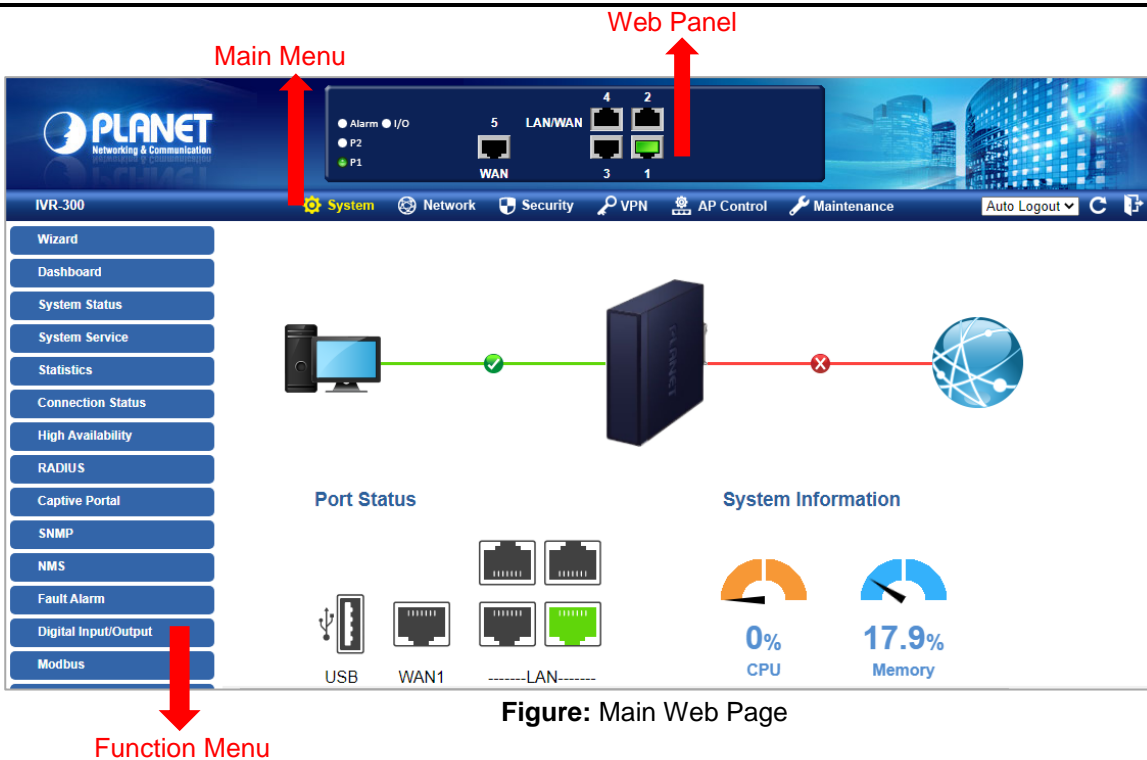


Figure: Main Web Page

■ **Web Panel**

The web panel displays the device's ports as shown below.



Figure: Web Panel

Object	Icon	Function
Ethernet port		To indicate the port without the RJ45 plug-in.
		To indicate network data is sending or receiving.

■ **Main Menu**

The main menu displays the product name, function menu, and main information in the center. Via the Web management, the administrator can set up the device by selecting the functions those listed in the function menu and button as shown below.



Figure: Function Menu

Object	Description
System	Provides System information of the Gateway.
Network	Provides WAN, LAN and network configurations of the Gateway.
Security	Provides Firewall and security configurations of the Gateway.
VPN	Provides VPN configuration of the Gateway.
AP Control	Provides AP Control configuration of the VPN Security Gateway
Wireless	Provides wireless configuration of the VPN Security Gateway (IVR-300W only)
Maintenance	Provides firmware upgrade and setting file restore/backup configuration of the Gateway.

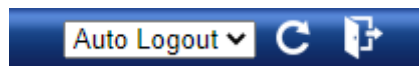




Figure: Function Button

Object	Description
	Click the " Refresh button " to refresh the current web page.
	Click the " Logout button " to log out the web UI of the Gateway.

4.4 System

Use the System menu items to display and configure basic administrative details of the Gateway. The System menu as shown below provides the following features to configure and monitor system.

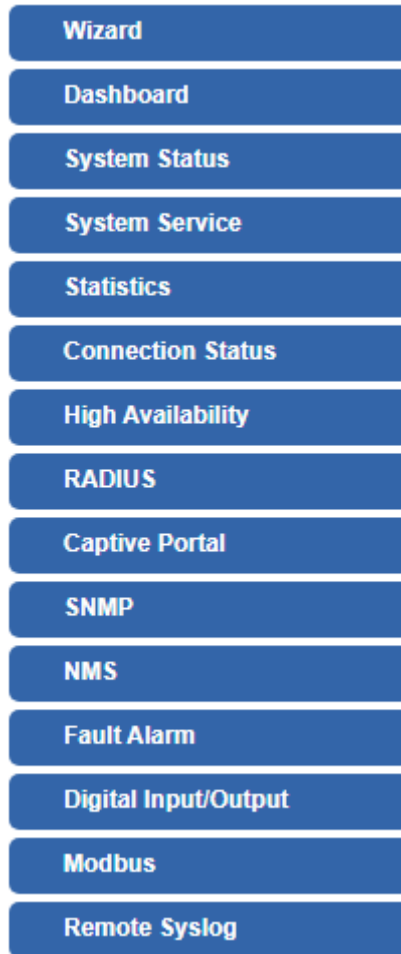


Figure: System Menu

Object	Description
Wizard	The Wizard will guide the user to configuring the Gateway easily and quickly.
Dashboard	The overview of system information includes connection, port, and system status.
System Status	Display the status of the system, Device Information, LAN and WAN.
System Service	Display the status of the system, Secured Service and Server Service
Statistics	Display statistics information of network traffic of LAN and WAN.
Connection Status	Display the DHCP client table and the ARP table
High Availability	Enable/Disable High Availability on VPN Security Gateway
RADIUS	Enable/Disable RADIUS on VPN Security Gateway
Captive Portal	Enable/Disable Captive Portal on VPN Security Gateway

SNMP	Display SNMP system information
NMS	Enable/Disable NMS on VPN Security Gateway
Fault Alarm	One relay output for power failure. Alarm relay current carry ability
Digital Input/Output	Digital Input/Output Control Configuration page
Modbus	Configure the Modbus TCP Mode on this page
Remote Syslog	Enable Captive Portal on VPN Security Gateway

4.4.1 Wizard

The Wizard will guide the user to configuring the Gateway easily and quickly. There are different procedures in different operation modes. According to the operation mode you switch to, please follow the instructions below to configure the Gateway via **Setup Wizard** as shown below



Figure: Setup Wizard

Step 1: Account Modification

Set up the Username and Password for the Account Modification as shown below.

Figure: Account Modification

Step 2: LAN Interface

Set up the IP Address and Subnet Mask for the LAN interface as shown below.

Figure 4-4-4: Setup Wizard – LAN Configuration

Object	Description
IP Address	Enter the IP address of your VPN Security Gateway The default is 192.168.1.1.
Subnet Mask	An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
DHCP Server	By default, the DHCP Server is enabled. If user needs to disable the function, please uncheck the box.
Start IP Address	By default, the start IP address is 192.168.1.100. Please do not set it to the same IP address of the VPN Security Gateway
Maximum DHCP Users	By default, the maximum DHCP users are 101, which means the VPN Security Gateway will provide DHCP client with IP address from 192.168.1.100 to 192.168.1.200 when the start IP address is 192.168.1.100.
Next	Press this button to the next step.
Cancel	Press this button to undo any changes made locally and revert to previously saved values.

Step 3: WAN Interface

The VPN Security Gateway supports two access modes on the WAN side as shown in below.

STEP 3 - Network Interface WAN

1
Account

2
LAN

3
WAN

4
Wireless

5
Security

6
Completed

WAN1

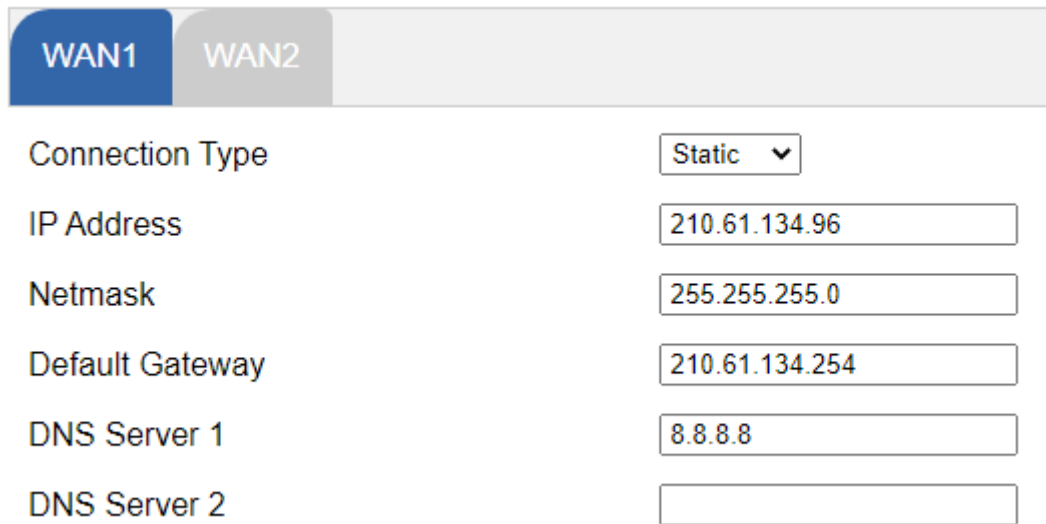
WAN2

Connection Type	<input type="text" value="DHCP"/>
IP Address	<input type="text"/>
Netmask	<input type="text"/>
Default Gateway	<input type="text"/>
DNS Server 1	<input type="text"/>
DNS Server 2	<input type="text"/>

Figure: Setup Wizard – WAN Configuration

Mode 1 -- Static IP

Select **Static IP Address** if all the Internet port's IP information is provided to you by your ISP. You will need to enter the **IP Address**, **Netmask**, **Default Gateway** and **DNS Server** provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The VPN Security Gateway will not accept the IP address if it is not in this format. The setup is shown below.



The screenshot shows the WAN1 configuration interface. At the top, there are two tabs: 'WAN1' (selected) and 'WAN2'. Below the tabs, the 'Connection Type' is set to 'Static'. The following fields are filled with the following values:

- IP Address: 210.61.134.96
- Netmask: 255.255.255.0
- Default Gateway: 210.61.134.254
- DNS Server 1: 8.8.8.8
- DNS Server 2: (empty)

Figure: WAN Interface Setup – Static IP Setup

Object	Description
IP Address	Enter the IP address assigned by your ISP.
Netmask	Enter the Netmask assigned by your ISP.
Default Gateway	Enter the Gateway assigned by your ISP.
DNS Server	The DNS server information will be supplied by your ISP.
Next	Press this button for the next step.
Previous	Press this button for the previous step.
Cancel	Press this button to undo any changes made locally and revert to previously saved values.

Mode 2 -- DHCP Client

Select DHCP Client to obtain IP Address information automatically from your ISP. The setup is shown below.

WAN1	WAN2
Connection Type	DHCP ▾
IP Address	<input type="text"/>
Netmask	<input type="text"/>
Default Gateway	<input type="text"/>
DNS Server 1	<input type="text"/>
DNS Server 2	<input type="text"/>

Figure: WAN Interface Setup – DHCP Setup

Step 4: Wireless Setting

(For IVR-300W only)

Set up the Wireless Settings as shown below.

STEP 4 - Network Interface Wireless

1
Account
2
LAN
3
WAN
4
Wireless
5
Security

2.4G WiFi Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SSID	<input type="text" value="PLANET_2.4G"/>
Hide SSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Bandwidth	<input type="text" value="20MHz"/> ▾
Channel	<input type="text" value="6"/> ▾
Encryption	<input type="text" value="Open"/> ▾
5G WiFi Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SSID	<input type="text" value="PLANET_5G"/>
Hide SSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Bandwidth	<input type="text" value="80MHz"/> ▾
Channel	<input type="text" value="36"/> ▾
Encryption	<input type="text" value="Open"/> ▾

Figure: Setup Wizard –Security Setting

Object	Description
2.4G Wireless Status	Allows user to enable or disable 2.4G Wi-Fi
Wireless Name (SSID)	It is the wireless network name. The default 2.4G SSID is "PLANET_2.4G"
Hide SSID	Allows user to enable or disable SSID
Bandwidth	Select the operating channel width, "20MHz" or "40MHz"
Channel	It shows the channel of the CPE. Default 2.4GHz is channel 6.
Encryption	Select the wireless encryption. The default is "Open"
Wi-Fi Multimedia	Enable/Disable WMM (Wi-Fi Multimedia) function

Object	Description
5G Wireless Status	Allows user to enable or disable 5G Wi-Fi
Wireless Name (SSID)	It is the wireless network name. The default 5G SSID is "PLANET_5G"
Hide SSID	Allows user to enable or disable SSID
Bandwidth	Select the operating channel width, "20MHz" or "40MHz" or "80MHz"
Channel	It shows the channel of the CPE. Default 5GHz is channel 36.
Encryption	Select the wireless encryption. The default is "Open"
Wi-Fi Multimedia	Enable/Disable WMM (Wi-Fi Multimedia) function

Step 5: Security Setting

Set up the Security Settings as shown The setup is shown below.

STEP 5 - Security Settings

1
Account

2
LAN

3
WAN

4
Wireless

5
Security

SPI Firewall	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Block SYN Flood	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Block ICMP Flood	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Block WAN Ping	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Remote Management	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Figure: Setup Wizard – Security Setting

Object	Description
SPI Firewall	The SPI Firewall prevents attack and improper access to network resources. The default configuration is enabled.
Block SYN Flood	SYN Flood is a popular attack way. DoS and DDoS are TCP protocols. Hackers like to use this method to make a fake connection that involves the CPU, memory, and so on. The default configuration is enabled.
Block ICMP Flood	ICMP is kind of a pack of TCP/IP; its important function is to transfer simple signal on the Internet. There are two normal attack ways which hackers like to use, Ping of Death and Smurf attack. The default configuration is disabled.
Block WAN Ping	Enable the function to allow the Ping access from the Internet network. The default configuration is disabled.
Remote Management	Enable the function to allow the web server access of the Gateway from the Internet network. The default configuration is disabled.

Step 6: Setup Completed

The page will show the summary of LAN, WAN and Security settings. The setup is shown below.

STEP 6 - Setup Completed

1
Account

2
LAN

3
WAN

4
Wireless

5
Security

6
Completed

LAN	Enable: Static IP: 192.168.1.1 / 255.255.255.0
WAN1	Enable: DHCP
WAN2	Enable: OFF
2.4G WiFi	Enable: ON SSID: PLANET_2.4G Bandwidth: 20MHZ Channel: 6 Encryption: Open Hide SSID: Disable
5G WiFi	Enable: ON SSID: PLANET_5G Bandwidth: 80MHZ Channel: 36 Encryption: Open Hide SSID: Disable
Security Settings	SPI Firewall: ON Block SYN Flood: ON Block ICMP Flood: OFF Block WAN Ping: OFF Remote Management: OFF

Figure: Setup Wizard – Setup Completed

Object	Description
Finish	Press this button to save and apply changes.
Previous	Press this button for the previous step.

4.4.2 Dashboard

The dashboard provides an overview of system information including connection, port, and system status. The setup is shown below.

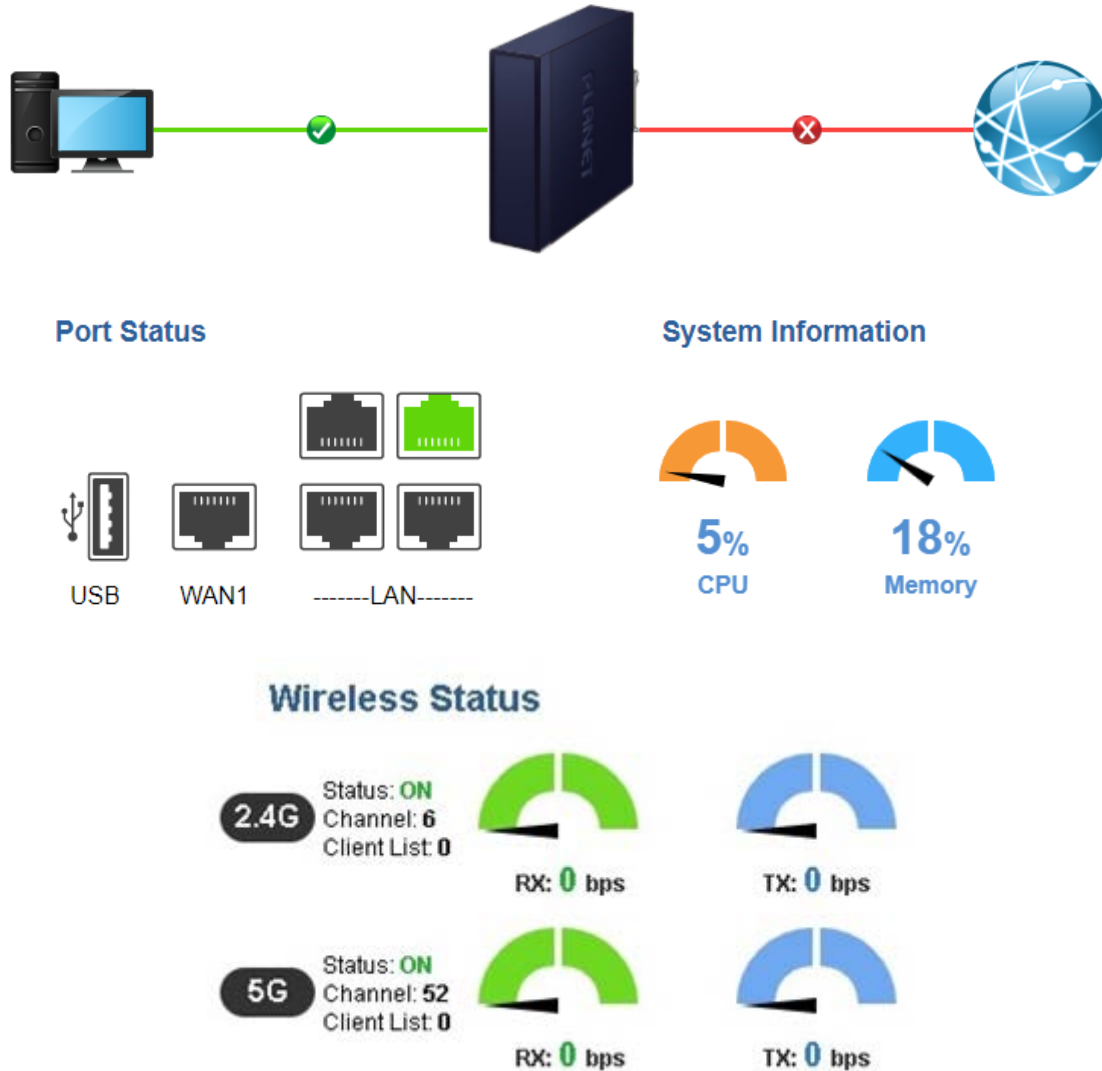


Figure: Dashboard

WAN/LAN Connection Status

Object	Description
	The status means WAN is connected to Internet and LAN is connected.
	The status means WAN is disconnected to Internet and LAN is connected.



The status means WAN is connected to Internet and LAN is disconnected.

Port Status

Object	Description
	Ethernet port is in use.
	Ethernet port is not in use.
	USB port is in use.
	USB port is not in use.

System Information

Object	Description
	Display the CPU loading
	Display the memory usage

Wireless Status

Object	Description
	Wireless is in use.
	Wireless is not in use.

4.4.3 Status

This page displays system information as shown below.

Device Information

Model Name	IVR-300
Firmware Version	v1.2102b220215
Current Time	2022-04-22 Friday 16:16:32
Running Time	0 day, 07:31:16
Power Status	PWR1:ON, PWR2:OFF
Alarm Status	Normal
DI and DO Status	Normal

WAN1

MAC Address	00:30:4F:00:11:23
Connection Type	DHCP
Display Name	WAN1
IP Address	
Netmask	
Default Gateway	

LAN

MAC Address	00:30:4F:00:11:22
IP Address	192.168.1.1
Netmask	255.255.255.0
DHCP Service	Enable
DHCP Start IP Address	192.168.1.100
DHCP End IP Address	192.168.1.200
Max DHCP Clients	101

For IVR-300W Only







2.4GHz WiFi	
Status	ON
SSID	PLANET_2.4G
Channel	6
Encryption	Open
MAC Address	A8:F7:E0:00:30:5A

5GHz WiFi	
Status	ON
SSID	PLANET_5G
Channel	36
Encryption	WPA2 Personal (TKIP+AES)
MAC Address	A8:F7:E0:87:85:5D

Figure: Status

4.4.4 System Service

This page displays system service information as shown below.

Server Service			
#	Action	Service	Status
1	 Enabled	DHCP Service	DHCP Table: 1
2	 Disabled	DDNS Service	Not enabled
3	 Disabled	Quality of Service	
4	 Disabled	High Availability	
5	 Disabled	RADIUS Service	
6	 Disabled	Captive Portal	

Secured Server Service			
#	Action	Service	Status
1	✔ Enabled	Cybersecurity	TLS 1.1, TLS 1.2, TLS 1.3
2	✔ Enabled	SPI Firewall	
3	✘ Disabled	MAC Filtering	(Active / Maximum Entries) 0 / 32
4	✘ Disabled	IP Filtering	(Active / Maximum Entries) 0 / 32
5	✘ Disabled	Web Filtering	(Active / Maximum Entries) 0 / 32
6	✘ Disabled	IPSec VPN Server	(Active / Maximum Tunnels) 0 / 32
7	✘ Disabled	GRE	(Active / Maximum Tunnels) 0 / 5
8	✘ Disabled	PPTP	(Active / Maximum Tunnels) 0 / 91
9	✘ Disabled	SSL VPN	(Active / Maximum Tunnels) 0 / 100
10	✘ Disabled	L2TP	(Active Tunnels) 0

Figure: System Service

4.4.5 Statistics

This page displays the number of packets that pass through the VPN Security Gateway on the WAN and LAN. The statistics are shown below.

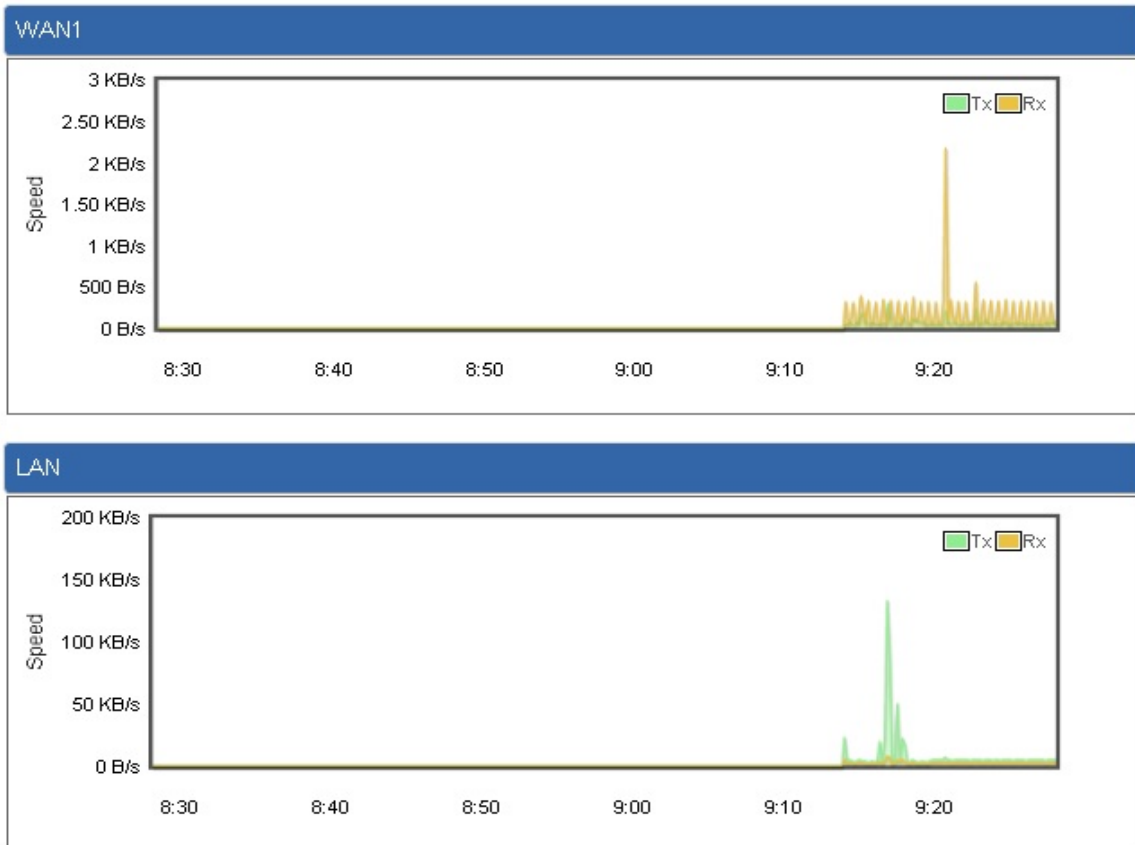


Figure: Statistics

4.4.6 Connection Status

The page will show the DHCP Table and ARP Table. The status is shown below.

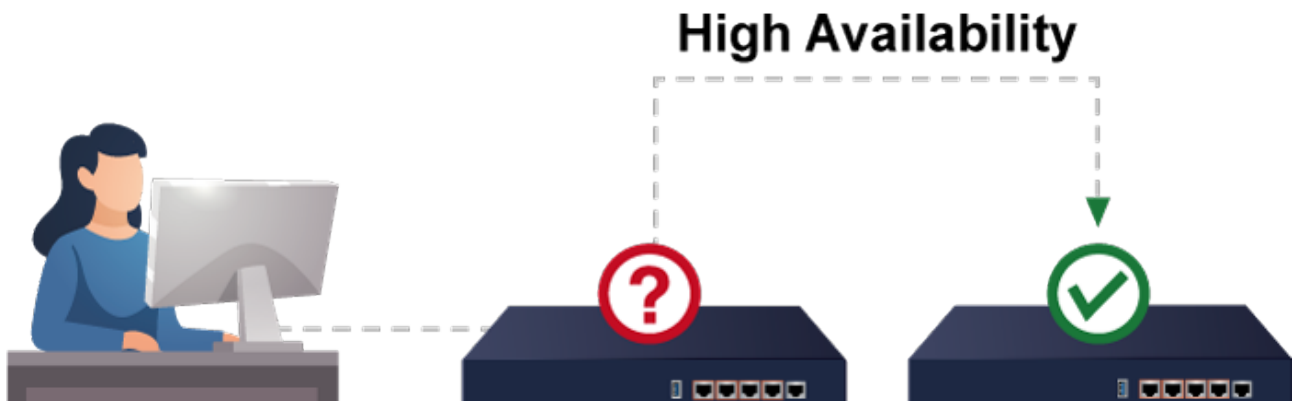
DHCP Table			
Name	IP Address	MAC Address	Expiration Time
ENM	192.168.1.154	00:05:1b:c5:51:45	Sat Apr 23 15:39:34 2022

ARP Table		
IP Address	MAC Address	ARP Type
192.168.1.154	00:05:1b:c5:51:45	dynamic

Figure: Connection Status


4.4.7 High Availability

High Availability (HA) is a redundant system that two IVR VPN Security Gateways can be set up in a master/slave configuration. The master VPN Security Gateway provides the Internet connection but, in the case of hardware or WAN connectivity failure, the slave (backup) VPN Security Gateway automatically takes over Internet connection. It provides redundant hardware and software that make the system available despite failures.



The page will show the High Availability configuration. The High Availability page is shown below.

High Availability Configuration

High Availability	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Username	<input type="text"/>
Password	<input type="text"/>
Mode	Master ▾
Virtual IP address	<input type="text"/>
Virtual IP Mask	<input type="text"/>
Interface	LAN ▾
Connected Status	

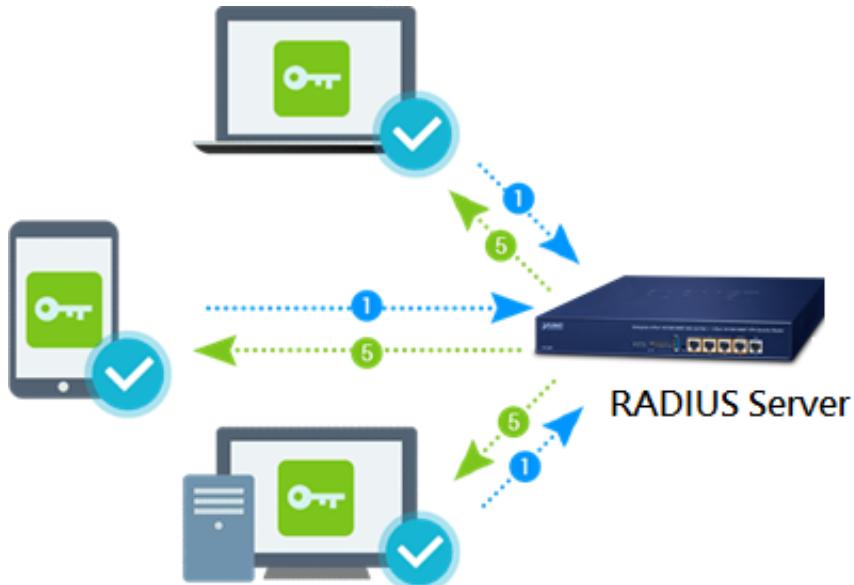
Apply Settings
Cancel Changes

Figure: High Availability

Object	Description
High Availability	Disable or enable the High Availability function. The default configuration is disabled.
Username	Create the username for the HA.
Password	Create the password for the HA.
Mode	Choose Master or Slave role.
Virtual IP Address	Assign an IP address as a virtual IP.
Virtual Mask	Assign a mask address as a virtual mask.
Interface	Use interface.
Connection Status	Display the HA status.

4.4.8 RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting.



The **RADIUS Server** page is shown below.

RADIUS

Server

Client

User Account

RADIUS Server Mode Enable Disable

Server Port

Apply Settings
Cancel Changes

Figure: RADIUS Server

Object	Description
RADIUS	Disable or enable the RADIUS function. The default configuration is disabled.
Server Port	UDP port number for authentication

The **RADIUS client** page is shown below.

RADIUS

Server
Client
User Account

Index	Name	Client IP Address	Secret Key	Description	Delete
	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/> / <input style="width: 50px;" type="text" value="32"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="background-color: #0056b3; color: white; border: none; padding: 2px 5px;" type="button" value="Add"/>

(up to 16 clients)

Figure: RADIUS Client

Object	Description
Name	Describe client's name
Client IP address	Describe client's IP address
Secret Key	The RADIUS server and client share a secret key that is used to authenticate the messages sent between server and client.
Description	Describe client's information

4.4.9 Captive Portal

Captive portal service gives the ability to organize a public (or guest) Wi-Fi zone with user authorization. A captive portal is the authorization page that forcibly redirects users who connect to the public network before accessing the Internet.



The Captive portal page is shown below.

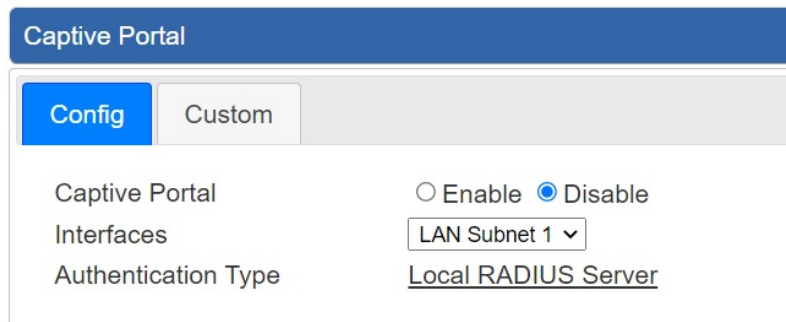


Figure: Captive portal

Object	Description
Captive portal	Disable or enable the Captive portal function. The default configuration is disabled.
Interface	Choose subnet interface <ul style="list-style-type: none"> ■ LAN Subnet 1 ■ LAN Subnet 2 ■ LAN Subnet 3 ■ LAN Subnet 4
Authentication Type	Support local RADIUS server

4.4.10 SNMP

This page provides SNMP setting as shown below.

SNMP

SNMP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SNMP Versions	SNMP v1,v2c ▼
Read Community	public
Write Community	private
Engine ID	
SNMP v3 Security Level	AuthPRiv ▼
SNMP v3 User Name	
SNMP v3 Auth Protocol	MD5 ▼
SNMP v3 Auth Password	
SNMP v3 Privacy Protocol	DES ▼
SNMP v3 Privacy Password	

System Identification

System Name	IVR-300
System Description	
System Location	
System Contact	sales@planet.com.tw

Figure: CloudViewer Server – Internet Configuration Page

Object	Description
Enable SNMP	Disable or enable the SNMP function. The default configuration is enabled.
Read/Write Community	Allows entering characters for SNMP Read/Write Community of the VPN Security Gateway
System Name	Allows entering characters for system name of the VPN Security Gateway
System Location	Allows entering characters for system location of the VPN Security Gateway
System Contact	Allows entering characters for system contact of the VPN Security Gateway
Apply Settings	Press this button to save and apply changes.
Cancel Changes	Press this button to undo any changes made locally and revert to previously saved values.

4.4.11 NMS

The IVR series can support both **NMS controller** and **CloudViewer** Sever for remote management.

PLANET's NMS Controller is a Network Management System that can monitor all kinds of deployed network devices, such as managed switches, media converters, routers, smart APs, VoIP phones, IP cameras, etc., compliant with the SNMP Protocol, ONVIF Protocol and PLANET Smart Discovery utility. The CloudViewer is a free networking service just for PLANET products. This service provides simplified network monitoring and real-time network status. Working with PLANET CloudViewer app, user can easily check network status, device information, and port and PoE statuses from Internet.

NMS Configuration screen appears as shown below.

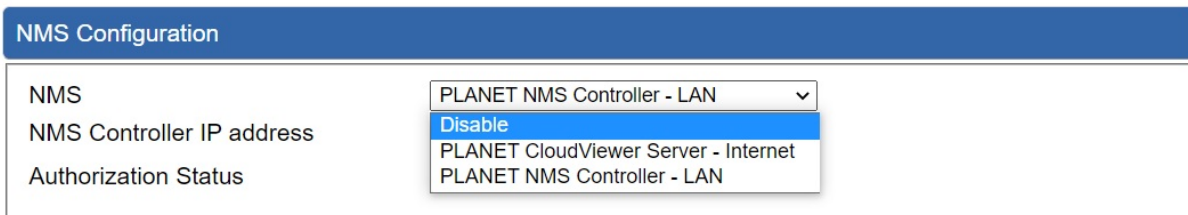


Figure: NMS Configuration Page

The NMS Controller – LAN Configuration screen appears as shown below.

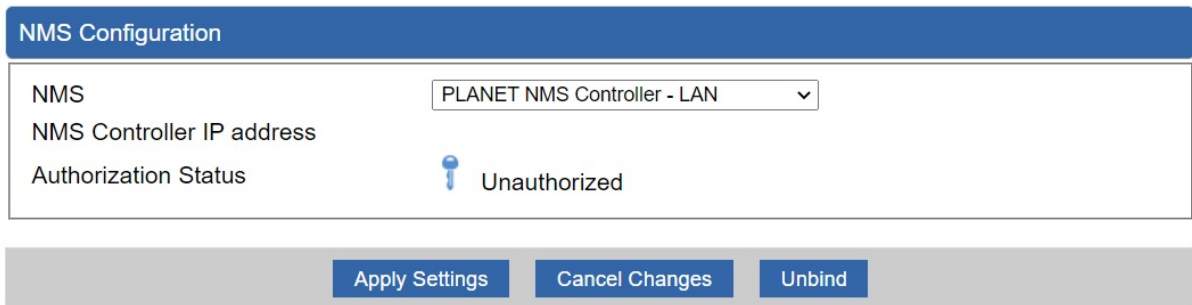


Figure: NMS Controller – LAN Configuration Page

Object	Description
• NMS Controller IP address	The IP address of NMS Controller
• Authorization Status	Indicate the authorization status of the switch to NMS Controller

The CloudViewer Server – Internet screen appears as shown below.

NMS Configuration	
NMS	<input type="text" value="PLANET CloudViewer Server - Internet"/>
Email	<input type="text"/>
Password	<input type="text"/>
Connection Status	Not enabled

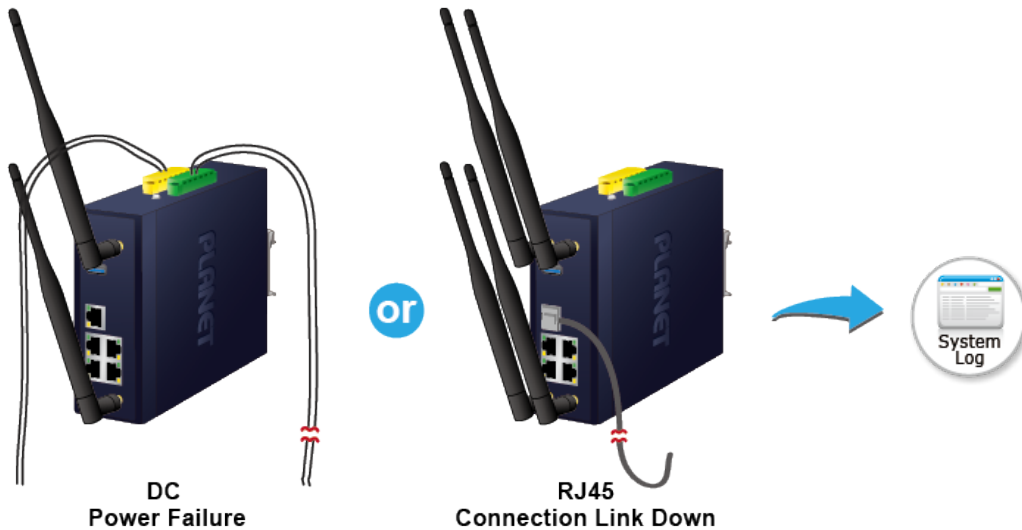
Figure: CloudViewer Server – Internet Configuration Page

Object	Description
• Email	The email registered on CloudViewer Server
• Password	The password of your CloudViewer account
• Connection Status	Indicate the status of connecting CloudViewer Server

4.4.12 Fault Alarm

The IVR series supports a Fault Alarm feature which can alert the users when there is something wrong with the device. With this ideal feature, the users would not have to waste time finding where the issue is. It will help to save time and human resource.

Fault Alarm Feature



This page provides fault alarm setting as shown below.

Fault Alarm Control Configuration					
Fault Alarm Output					
Enable	<input type="checkbox"/> Enable				
Record	<input type="checkbox"/> System Log				
Event	<input type="checkbox"/> Power Fail <input type="checkbox"/> Port Fail				
Power Alarm	<input type="checkbox"/> PWR1 <input type="checkbox"/> PWR2				
Port Alarm	1	2	3	4	5
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure: Fault Alarm

Object	Description
• Enable	Controls whether Fault Alarm is enabled.
• Record	Controls whether Record is sending System log or SMS.
• Event	Controls whether Port Failure or Power Failure or both is/are detected.
• Power Alarm	Controls whether faulty PWR1 or faulty PWR2 or both is/are detected.
• Port Alarm	Controls which port or all is/are detected for fault.

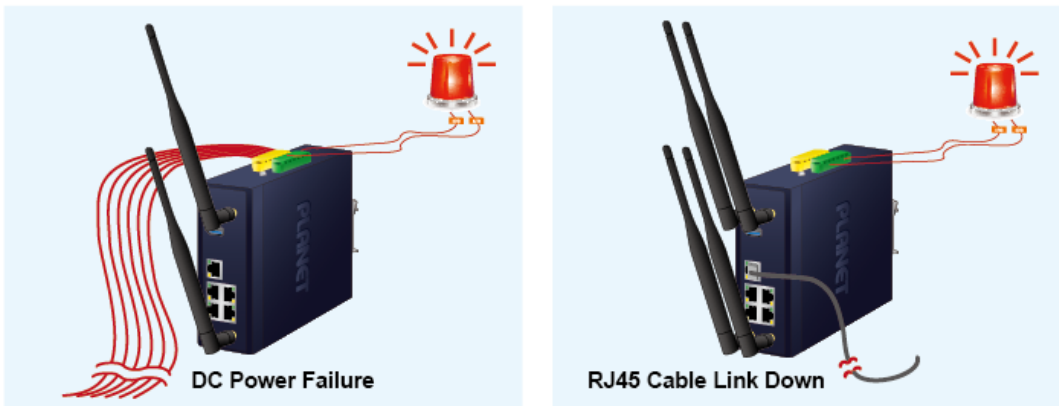
4.4.13 Digital Input / Output

The IVR-300/IVR-300W supports Digital Input and Digital Output on its upper panel. This external alarm enables users to use Digital Input to detect and log external device status (such as door intrusion detector), and send event alarm to the administrators. The Digital Output could be used to alarm the administrators if the IVR-300/IVR-300W port shows link down, link up or power failure.

Digital Input



Digital Output



This page provides Digital Input / Output setting as shown below.

Digital Input/Output Control Configuration											
Digital Input 0					Digital Input 1						
Enable	<input type="checkbox"/> Enable				Enable	<input type="checkbox"/> Enable					
DI Condition	High to Low ▾				DI Condition	High to Low ▾					
Event Description					Event Description						
Action	<input type="checkbox"/> System Log				Action	<input type="checkbox"/> System Log					
Digital Output 0					Digital Output 1						
Enable	<input type="checkbox"/> Enable				Enable	<input type="checkbox"/> Enable					
Action	<input type="checkbox"/> Power Fail <input type="checkbox"/> Port Fail <input type="checkbox"/> DI 0 <input type="checkbox"/> DI 1				Action	<input type="checkbox"/> Power Fail <input type="checkbox"/> Port Fail <input type="checkbox"/> DI 0 <input type="checkbox"/> DI 1					
DO Condition	High to Low ▾				DO Condition	High to Low ▾					
Power Alarm	<input type="checkbox"/> PWR1 <input type="checkbox"/> PWR2				Power Alarm	<input type="checkbox"/> PWR1 <input type="checkbox"/> PWR2					
Port Fail Alarm	1	2	3	4	5	Port Fail Alarm	1	2	3	4	5
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure: Digital Input / Output

Object	Description
<ul style="list-style-type: none"> • Enable 	<p>Check the Enable checkbox to enable Digital Input / output function. Uncheck the Enable checkbox to disable Digital input / output function.</p>
<ul style="list-style-type: none"> • Condition 	<p>As Digital Input:</p> <p>Allows user to select High to Low or Low to High. This means a signal received by system is from High to Low or from Low to High. It will trigger an action that logs a customized message or issue the message from the switch.</p> <p>As Digital Output:</p> <p>Allows user to select High to Low or Low to High. This means that when the switch is power-failed or port-failed, the system will issue a High or Low signal to an external device such as an alarm.</p>
<ul style="list-style-type: none"> • Event Description 	<p>Allows user to set a customized message for Digital Input function alarm.</p>
<ul style="list-style-type: none"> • Action 	<p>As Digital Input:</p> <p>Allows user to record alarm message to System log, syslog or issues out via SNMP Trap or SMTP.</p> <p>By default, SNMP Trap and SMTP are disabled. Please enable them first if you want to issue alarm message via them.</p> <p>As Digital Output:</p> <p>Allows user to monitor an alarm from port failure, power failure, Digital Input 0 (DI 0) and Digital Input 1(DI 1) which mean if Digital Output has detected these events, then Digital Output would be triggered according to the setting of Condition.</p>
<ul style="list-style-type: none"> • Power Alarm 	<p>Allows user to choose which power module that needs to be monitored.</p>
<ul style="list-style-type: none"> • Port Alarm 	<p>Allows user to choose which port that needs to be monitored.</p>

4.4.14 Modbus

The IVR-300/IVR-300W provides a feature that can convert the Serial RS485 communication to IP networking. Ethernet signal allows two types of segments to connect easily, efficiently and inexpensively. The solution helps users and SIs save expenses as there is no need to replace the existing serial equipment and software system.

Convert Serial Communication to IP Networking



This page provides Modbus Configuration setting as shown below.

Modbus Configuration	
Modbus TCP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Serial device	RS-485 ▼
Baudrate	9600 ▼
Databits	8 ▼
Parity	None ▼
Stopbits	1 ▼
TCP Slave Port	502

Figure: Modbus Configuration

Object	Description
• Modbus TCP	Indicates the Modbus TCP mode operation. Possible modes are: Enabled: Enable Modbus TCP mode operation. Disabled: Disable Modbus TCP mode operation.
• Serial device	Set up the Modbus Serial device to RS-485
• Baudrate	Select the Modbus Baudrate to 300 ~ 115200
• Databits	Set up the Modbus Databits to 8

• Parity	Set up the Modbus Parity to None, Odd or Even
• Stopbits	Set up the Modbus Stopbits to 1 or 2
• TCP Slave Port	Set up the Modbus TCP Slave Port.

4.4.15 Remote Syslog

This page provides remote syslog setting as shown below.

Remote Syslog

Enable	<input type="checkbox"/>
Syslog Server	<input style="width: 150px;" type="text"/>
Port Destination	<input style="width: 150px;" type="text"/> (1~65535)

Figure: Connection Status

Object	Description
• Enable	Controls whether remote syslog is enabled
• Syslog Server IP	Indicates the IPv4 host address of syslog server
• Port Destination	Configure port for remote syslog

4.5 Network

The Network function provides WAN, LAN and network configuration of the VPN Security Gateway as shown below.



Figure: Network Menu

Object	Description
Priority	Allows setting priority of WAN interface.
WAN	Allows setting WAN interface.
WAN Advanced	Allows setting WAN Advanced settings.
LAN	Allows setting LAN interface.
Multi-Subnet	Allows setting Multi-Subnet1 ~ Subnet4 interface.
VLAN	Disable or enable the VLAN function. The default configuration is disabled.
UPnP	Disable or enable the UPnP function. The default configuration is disabled.
Routing	Allows setting Route.
RIP	Disable or enable the RIP function. The default configuration is disabled.
OSPF	Disable or enable the OSPF function.

	The default configuration is disabled.
IGMP	Disable or enable the IGMP function. The default configuration is disabled.
IPv6	Allows setting IPv6 WAN interface.
DHCP	Allows setting DHCP Server.
DDNS	Allows setting DDNS and PLANET DDNS.
MAC Address Clone	Allows setting WAN MAC Address Clone.

4.5.1 Priority

This page provides SD WAN priority setting as shown below.

SD WAN Priority

No.	Group Name	Path	Services	Active	Action

SD WAN Configuration

Active Enable Disable

Group Name

Path

Service Port or Group Border Gateway Protocol

Figure: SD WAN Configuration

Object	Description
Active	■ Enable / Disable the Active
Group Name	■ Setting the Group Name.
Path	■ Setting the SD-WAN To / To SD-WAN
Service Port or Group	■ Setting the Service Port or Group Border Gateway Protocol

4.5.2 WAN

This page is used to configure the parameters for Internet network which connects to the WAN port of the VPN Security Gateway as shown below. Here you may select the access method by clicking the item value of WAN access type.

WAN1 Configuration

Display Name	<input type="text" value="WAN1"/>
Connection Type	<input type="button" value="DHCP"/> ▾
IP Address	<input type="text"/>
Netmask	<input type="text"/>
Default Gateway	<input type="text"/>
DNS Server 1	<input type="text"/>
DNS Server 2	<input type="text"/>


WAN2 Configuration

WAN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Display Name	<input type="text" value="WAN2"/>
Connection Type	<input type="button" value="DHCP"/> ▾
IP Address	<input type="text"/>
Netmask	<input type="text"/>
Gateway	<input type="text"/>
DNS Server 1	<input type="text"/>
DNS Server 2	<input type="text"/>

Figure: WAN Configuration

Object	Description		
	Please select the corresponding WAN Access Type for the Internet, and fill out the correct parameters from your local ISP in the fields which appear below.		
WAN Access Type	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%; vertical-align: top;">Static</td> <td> <p>Select Static IP Address if all the Internet ports' IP information is provided to you by your ISP (Internet Service Provider). You will need to enter the IP address, Netmask, Gateway, and DNS Server provided to you by your ISP.</p> <p>Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The VPN Security Gateway will not accept the IP address if it is not in this format.</p> <p>IP Address</p> <p>Enter the IP address assigned by your ISP.</p> <p>Netmask</p> </td> </tr> </table>	Static	<p>Select Static IP Address if all the Internet ports' IP information is provided to you by your ISP (Internet Service Provider). You will need to enter the IP address, Netmask, Gateway, and DNS Server provided to you by your ISP.</p> <p>Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The VPN Security Gateway will not accept the IP address if it is not in this format.</p> <p>IP Address</p> <p>Enter the IP address assigned by your ISP.</p> <p>Netmask</p>
Static	<p>Select Static IP Address if all the Internet ports' IP information is provided to you by your ISP (Internet Service Provider). You will need to enter the IP address, Netmask, Gateway, and DNS Server provided to you by your ISP.</p> <p>Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The VPN Security Gateway will not accept the IP address if it is not in this format.</p> <p>IP Address</p> <p>Enter the IP address assigned by your ISP.</p> <p>Netmask</p>		

Object	Description	
		Enter the Subnet Mask assigned by your ISP. Gateway Enter the Gateway assigned by your ISP. DNS Server The DNS server information will be supplied by your ISP.
	DHCP	Select DHCP Client to obtain IP Address information automatically from your ISP.

 Note	WAN IP, whether obtained automatically or specified manually, should NOT be on the same IP net segment as the LAN IP; otherwise, the VPN Security Gateway will not work properly. In case of emergency, press the hardware-based "Reset" button.
---	--

4.5.3 WAN Advanced

This page is used to configure the advanced parameters for Internet area network which connects to the WAN port of your VPN Security Gateway as shown below. Here you may change the setting for Load Balance Weight, Detect Interval, Detect Linkup Threshold, etc.

WAN1 Configuration

Load Balance Weight	<input type="text" value="3"/>	
External Connection Detection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Detect Interval	<input type="text" value="5"/>	Seconds
Detect Link Up Threshold	<input type="text" value="8"/>	Time(s)
Detect Link Down Threshold	<input type="text" value="3"/>	Time(s)
Custom Detect Host 1	<input type="text" value="8.8.8.8"/>	
Custom Detect Host 2	<input type="text" value="208.67.222.222"/>	

WAN2 Configuration

Load Balance Weight	<input type="text" value="2"/>	
External Connection Detection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Detect Interval	<input type="text" value="5"/>	Seconds
Detect Link Up Threshold	<input type="text" value="8"/>	Time(s)
Detect Link Down Threshold	<input type="text" value="3"/>	Time(s)
Custom Detect Host 1	<input type="text" value="8.8.8.8"/>	
Custom Detect Host 2	<input type="text" value="208.67.222.222"/>	

Figure: LAN Setup

Object	Description
Load Balance Weight	Load Balance Weight allows you to set a relative weight (from 1 - 10) for each WAN port.
External Connection Detection	Enable to detect the status of WAN connection.
Detect Interval	Set the detect interval as you need. The recommended value is 5 (default).
Detect Link Up Threshold	Set the times for detecting link up. The recommended value is 8 (default).
Detect Link Down Threshold	Set the times for detecting link down. The recommended value is 3 (default).
Custom Detect Host	The host is used to check whether the internet connection is alive or not.

4.5.4 LAN

This page is used to configure the parameters for local area network which connects to the LAN port of your VPN Security Gateway as shown below. Here you may change the settings for IP address, subnet mask, DHCP, etc.

LAN Configuration

IP Address	<input style="width: 90%;" type="text" value="192.168.1.1"/>
Netmask	<input style="width: 90%;" type="text" value="255.255.255.0"/>

Apply Settings
Cancel Changes

Figure: LAN Setup

Object	Description
IP Address	The LAN IP address of the VPN Security Gateway and default is 192.168.1.1 .
Net Mask	Default is 255.255.255.0 .

4.5.5 Multi-Subnet

This page provides multi-subnet setting as shown below.

Multi-Subnet Configuration

Name	Network	DHCP Server
LAN Subnet 1	IP Address <input style="width: 100px;" type="text" value="192.168.1.1"/> Netmask <input style="width: 100px;" type="text" value="255.255.255.0"/>	V
LAN Subnet 2	IP Address <input style="width: 100px;" type="text" value="192.168.3.1"/> Netmask <input style="width: 100px;" type="text" value="255.255.255.0"/>	<input checked="" type="checkbox"/>
LAN Subnet 3	IP Address <input style="width: 100px;" type="text" value="192.168.5.1"/> Netmask <input style="width: 100px;" type="text" value="255.255.255.0"/>	<input checked="" type="checkbox"/>
LAN Subnet 4	IP Address <input style="width: 100px;" type="text" value="192.168.7.1"/> Netmask <input style="width: 100px;" type="text" value="255.255.255.0"/>	<input checked="" type="checkbox"/>

Apply Settings
Cancel Changes

Figure: Multi-Subnet

4.5.6 VLAN

Please refer to the following sections for the details as shown below.

VLAN Configuration

VLAN Enable Disable

WAN Port

WAN VLAN ID

VLAN Table

Name	Subnet	VLAN ID	LAN Port 1	LAN Port 2	LAN Port 3	LAN Port 4	Action
Management Group	LAN Subnet 1 (192.168.1.1)		<input type="text" value="UNTAG"/>	<input type="text" value="UNTAG"/>	<input type="text" value="UNTAG"/>	<input type="text" value="UNTAG"/>	

VLAN Table Configuration

Name	Subnet	VLAN ID	LAN Port 1	LAN Port 2	LAN Port 3	LAN Port 4	
<input type="text"/>	<input type="text" value="Switch VLAN"/>	<input type="text"/>	<input type="text" value="OFF"/>	<input type="text" value="OFF"/>	<input type="text" value="OFF"/>	<input type="text" value="OFF"/>	<input type="button" value="Add"/>

Figure: VLAN Configuration

4.5.7 UPnP

Please refer to the following sections for the details as shown below.

UPnP Configuration

UPnP Enable Disable

Figure: VLAN Configuration

4.5.8 Routing

Please refer to the following sections for the details as shown below.

Routing config list

Number	Type	Destination	Netmask	Gateway	Interface	Comment	Action
Current Routing table in the system							
1		0.0.0.0	0.0.0.0	192.168.0.180		LOCAL	
2		0.0.0.0	0.0.0.0	192.168.1.18		WAN1	
3		0.0.0.0	0.0.0.0	192.168.1.19		WAN2	
4		192.168.0.0	255.255.255.0	0.0.0.0		LAN	
5		192.168.1.0	255.255.255.0	0.0.0.0		WAN1	
6		192.168.1.0	255.255.255.0	0.0.0.0		WAN2	

Add Route

Figure: Routing table

Add a routing rule

Type	<input type="text" value="Host"/>
Destination	<input type="text"/>
Netmask	<input type="text" value="255.255.255.255 /32"/>
Gateway	<input type="text"/>
Interface	<input type="text" value="LAN"/>
Comment	<input type="text"/>

Apply Settings
Cancel Changes

Figure: Routing setup

Routing tables contain a list of IP addresses. Each IP address identifies a remote VPN Security Gateway (or other network gateway) that the local VPN Security Gateway is configured to recognize. For each IP address, the routing table additionally stores a network mask and other data that specifies the destination IP address ranges that remote device will accept.

Object	Description
Type	There are two types: Host and Net. When the Net type is selected, user does not need to input the Gateway.
Destination	The network or host IP address desired to access.
Net Mask	The subnet mask of destination IP.

Object	Description
Gateway	The gateway is the router or host's IP address to which packet is sent. It must be the same network segment with the WAN or LAN port.
Interface	Select the interface that the IP packet must use to transmit out of the router when this route is used.
Comment	Enter any words for recognition.

4.5.9 RIP

Please refer to the following sections for the details as shown below.

RIP Configuration

Dynamic Route	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
RIP Versions	RIP 2 ▼

Apply Settings
Cancel Changes

Figure: OSPF Configuration table

4.5.10 OSPF

Please refer to the following sections for the details as shown below.

OSPF Configuration

OSPF	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Router ID	<input style="width: 80%;" type="text"/>
Area ID	<input style="width: 80%;" type="text" value="0"/>

Apply Settings
Cancel Changes

Figure:

Routing table

4.5.11 IGMP

Please refer to the following sections for the details as shown below.

IGMP Configuration	
IGMP Proxy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IGMP Versions	Auto ▼

Figure: Routing table

4.5.12 IPv6

This page is used to configure parameter for IPv6 internet network which connects to WAN port of the VPN Security Gateway as shown below. It allows you to enable IPv6 function and set up the parameters of the VPN Security Gateway's WAN. In this setting you may change WAN connection type and other settings.

IPv6 - WAN1	
Connection Type	DHCP ▼
IPv6 Address	<input type="text"/>
Subnet Prefix Length	64
Default Gateway	<input type="text"/>
IPv6 DNS Server 1	<input type="text"/>
IPv6 DNS Server 2	<input type="text"/>

IPv6 - WAN2	
Connection Type	DHCP ▼
IPv6 Address	<input type="text"/>
Subnet Prefix Length	64
Default Gateway	<input type="text"/>
IPv6 DNS Server 1	<input type="text"/>
IPv6 DNS Server 2	<input type="text"/>

IPv6 - LAN

Type Delegate Prefix from WAN Static

Static Address

Subnet Prefix Length

DHCPv6

Address Assign Stateless Stateful Passthrough Disable

Figure: IPv6 WAN setup

Object	Description
Connection Type	Select IPv6 WAN type either by using DHCP or Static.
IPv6 Address	Enter the WAN IPv6 address.
Subnet Prefix Length	Enter the subnet prefix length.
Default Gateway	Enter the default gateway of the WAN port.

4.5.13 DHCP

The DHCP service allows you to control the IP address configuration of all your network devices. When a client (host or other device such as networked printer, etc.) joins your network it will automatically get a valid IP address from a range of addresses and other settings from the DHCP service. The client must be configured to use DHCP; this is something called "automatic network configuration" and is often the default setting. The setup is shown below.

DHCP Configuration

DHCP Server Enable Disable

Start IP Address

Maximum DHCP Users

DNS Server Automatically Manually

Primary DNS Server

Secondary DNS Server

WINS

Lease Time minutes

Domain Name

Static DHCP List

Index	Device Name	IP Address	MAC Address	Delete
	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text" value="192.168.1.150"/>	<input style="width: 100%;" type="text" value="00:30:4F:00:00:01"/>	<input type="button" value="Add"/>

Figure: DHCP

Object	Description
DHCP Service	By default, the DHCP Server is enabled, meaning the VPN Security Gateway will assign IP addresses to the DHCP clients automatically. If user needs to disable the function, please set it as disable.
Start IP Address	By default, the start IP address is 192.168.1.100. Please do not set it to the same IP address of the VPN Security Gateway
Maximum DHCP Users	By default, the maximum DHCP users are 101, meaning the VPN Security Gateway will provide DHCP client with IP address from 192.168.1.100 to 192.168.1.200 when the start IP address is 192.168.1.100.
Set DNS	By default, it is set as Automatically, and the DNS server is the VPN Security Gateway's LAN IP address. If user needs to use specific DNS server, please set it as Manually, and then input a specific DNS server.
Primary/Secondary DNS Server	Input a specific DNS server.
WINS	Input a WINS server if needed.
Lease Time	Set the time for using one assigned IP. After the lease time, the DHCP client will need to get new IP addresses from the VPN Security Gateway Default is 1440 minutes.
Domain Name	Input a domain name for the VPN Security Gateway Default is Planet.

4.5.14 DDNS

The VPN Security Gateway offers the DDNS (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as **PLANET DDNS** (<http://www.planetddns.com>) and set up the domain name of your choice.

PLANET DDNS website provides a free DDNS (Dynamic Domain Name Server) service for PLANET devices. Whether the IP address used on your PLANET device supporting DDNS service is fixed or dynamic, you can easily connect the devices anywhere on the Internet with a meaningful or easy-to-remember name you gave. PLANET DDNS provides two types of DDNS services. One is **PLANET DDNS** and the other is **PLANET Easy DDNS** as shown below.

PLANET DDNS

For example, you've just installed a PLANET IP camera with dynamic IP like 210.66.155.93 in the network. You can name this device as "Mycam1" and register a domain as Mycam1.planetddns.com at PLANET DDNS (<http://www.planetddns.com>). Thus, you don't need to memorize the exact IP address but just the URL link: Mycam1.planetddns.com.

PLANET Easy DDNS

PLANET Easy DDNS is an easy way to help user to get your Domain Name with just one click. You can just log in to the Web Management Interface of your devices, say, your VPN Security Gateway, and check the DDNS menu and just enable it. You don't need to go to <http://www.planetddns.com> to apply for a new account. Once you enabled the Easy DDNS, your PLANET Network Device will use the format PLxxxxxx where xxxxxx is the last 6 characters of your MAC address that can be found on the Web page or bottom label of the device. (For example, if the VPN Security Gateway's MAC address is A8-F7-E0-81-96-C9, it will be converted into pt8196c9.planetddns.com)

DDNS Configuration	
Dynamic DNS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Interface	WAN1 ▾
DDNS Type	PLANET DDNS ▾
PLANET Easy DDNS	Disable ▾
User Name	<input style="width: 100%;" type="text"/>
Password	<input style="width: 100%;" type="password"/>
Host Name	<input style="width: 100%;" type="text"/>
Interval	<input style="width: 80%;" type="text" value="120"/> seconds
Connection Status	Not enabled

Figure: DDNS Configuration

Object	Description
DDNS Service	By default, the DDNS service is disabled. If user needs to enable the function, please set it as enable.
Interface	User is able to select the interface for DDNS service. By default, the interface is WAN 1.
DDNS Type	There are three options: <ol style="list-style-type: none"> 1. PLANET DDNS: Activate PLANET DDNS service. 2. DynDNS: Activate DynDNS service. 3. NOIP: Activate NOIP service. Note that please first register with the DDNS service and set up the domain name of your choice to begin using it.
Easy DDNS	When the PLANET DDNS service is activated, user is able to select to enable or disable Easy DDNS. When this function is enabled, DDNS hostname will appear automatically. User doesn't go to http://www.planetddns.com to apply for a new account.
User Name	The user name is used to log into DDNS service.
Password	The password is used to log into DDNS service.
Host Name	The host name as registered with your DDNS provider.
Interval	Set the update interval of the DDNS function.
Update Status	Show the connection status of the DDNS function.

4.5.15 MAC Address Clone

Clone or change the MAC address of the WAN interface. The setup is shown below.

The screenshot shows two configuration panels for WAN1 and WAN2. Each panel contains a 'Clone WAN MAC' section with radio buttons for 'Enable' and 'Disable' (currently 'Disable' is selected), and a 'MAC Address' input field. Below the panels are two buttons: 'Apply Settings' and 'Cancel Changes'.

Figure: MAC Address Clone

Object	Description
Clone WAN MAC	Set the function as enable or disable.
MAC Address	Input a MAC Address, such as A8:F7:E0:00:06:62.

4.6 Security

The Security menu provides Firewall, Access Filtering and other functions as shown below. Please refer to the following sections for the details.

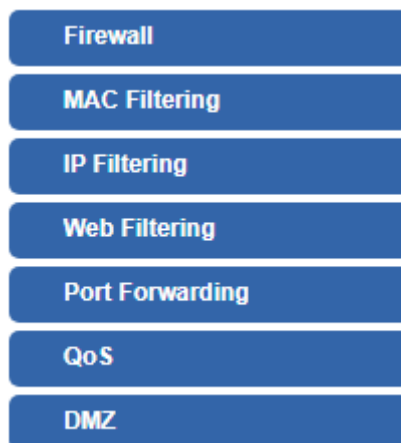


Figure: Security menu

Object	Description
Firewall	Allows setting DoS (Denial of Service) protection as enable.
MAC Filtering	Allows setting MAC Filtering.
IP Filtering	Allows setting IP Filtering.
Web Filtering	Allows setting Web Filtering.
Port Forwarding	Allows setting Port Forwarding.
QoS	Allows setting QoS.
DMZ	Allows setting DMZ.

4.6.1 Firewall

A "Denial-of-Service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service. The VPN Security Gateway can prevent specific DoS attacks as shown below.

Firewall Protection

SPI Firewall Enable Disable

DDoS

Block SYN Flood	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input type="text" value="30"/>	Packets/Second
Block FIN Flood	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="text" value="30"/>	Packets/Second
Block UDP Flood	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="text" value="30"/>	Packets/Second
Block ICMP Flood	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="text" value="5"/>	Packets/Second
Block IP Teardrop Attack	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Block Ping of Death	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Block TCP packets with SYN and FIN Bits set	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Block TCP packets with FIN Bit set but no ACK Bit set	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Block TCP packets without Bits set	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		

System Security

Block WAN Ping	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
HTTP Port	<input type="text" value="80"/>	
HTTPs Port	<input type="text" value="443"/>	
Remote Management	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Temporarily block when login failed more than	<input type="text" value="0"/>	(0 means no limit)
IP blocking period	<input type="text" value="0"/>	minute(s) (0 means permanent blocking)
Blocked IP	0.0.0.0	

NAT ALGs

FTP ALG	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
TFTP ALG	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
RTSP ALG	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
H.323 ALG	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
SIP ALG	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	

Figure: Firewall

Object	Description
SPI Firewall	<p>The SPI Firewall prevents attack and improper access to network resources.</p> <p>The default configuration is enabled.</p>
Block SYN Flood	<p>SYN Flood is a popular attack way. DoS and DDoS are TCP protocols. Hackers like to use this method to make a fake connection that involves the CPU, memory, and so on.</p> <p>The default configuration is enabled.</p>
Block FIN Flood	<p>If the function is enabled, when the number of the current FIN packets is beyond the set value, the VPN Security Gateway will start the blocking function immediately.</p> <p>The default configuration is disabled.</p>
Block UDP Flood	<p>If the function is enabled, when the number of the current UPD-FLOOD packets is beyond the set value, the VPN Security Gateway will start the blocking function immediately.</p> <p>The default configuration is disabled.</p>
Block ICMP Flood	<p>ICMP is kind of a pack of TCP/IP; its important function is to transfer simple signal on the Internet. There are two normal attack ways which hackers like to use, Ping of Death and Smurf attack.</p> <p>The default configuration is disabled.</p>
IP TearDrop	<p>If the function is enabled, the VPN Security Gateway will block Teardrop attack that is targeting on TCP/IP fragmentation reassembly codes.</p>
Ping Of Death	<p>If the function is enabled, the VPN Security Gateway will block Ping of Death attack that aims to disrupt a targeted machine by sending a packet larger than the maximum allowable size causing the target machine to freeze or crash.</p>
Block WAN Ping	<p>Enable the function to allow the Ping access from the Internet network.</p> <p>The default configuration is disabled.</p>
Remote Management	<p>Enable the function to allow the web server access of the VPN Security Gateway from the Internet network.</p> <p>The default configuration is disabled.</p>

4.6.2 MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network or Internet through the VPN Security Gateway. Use of such filters can be helpful in securing or restricting your local network as shown below.

MAC Filtering

MAC Filtering Enable Disable
Interface LAN WAN

MAC Filtering Rules

Index	Active	Device Name	MAC Address	Action
		abc	00:30:4F:00:00:01	Add

Apply Settings
Cancel Changes

Figure: MAC Filtering

Object	Description
Enable MAC Filtering	Set the function as enable or disable. When the function is enabled, the VPN Security Gateway will block traffic of the MAC address on the list.
Interface	Select the function works on LAN, WAN or both. If you want to block a LAN device's MAC address, please select LAN, vice versa.
MAC Address	Input a MAC address you want to control, such as A8:F7:E0:00:06:62.
Add	When you input a MAC address, please click the "Add" button to add it to the list.
Remove	If you want to remove a MAC address from the list, please click on the MAC address, and then click the "Remove" button to remove it.
Remove All	If you want to remove all MAC addresses from the list, please click the "Remove All" button to remove all.

4.6.3 IP Filtering

IP Filtering is used to deny LAN users from accessing the public IP address on internet as shown below. To begin blocking access to an IP address, enable IP Filtering and enter the IP address of the web site you wish to block.

IP Filtering

IP Filtering Enable Disable

IP Filtering Rules

No.	Active	Source IP	Destination IP	Port Range	Protocol	Action
<div style="background-color: #0056b3; color: white; padding: 5px 15px; display: inline-block; border-radius: 3px;">Add IP Filtering Rule</div>						

Figure: IP Filtering

Object	Description
IP Filtering	Set the function as enable or disable.
Add IP Filtering Rule	Go to the Add Filtering Rule page to add a new rule.

IP Filter Rule Setting

Enable	<input checked="" type="checkbox"/>	
Source IP Address	<input type="text"/> / <input type="text" value="32"/>	<input type="checkbox"/> Anywhere
Destination IP Address	<input type="text"/> / <input type="text" value="32"/>	<input type="checkbox"/> Anywhere
Destination Port	<input type="text"/> - <input type="text"/>	
Protocol	<input type="text" value="All"/>	

Apply Settings

Cancel Changes

Figure: IP Filter Rule Setting

Object	Description
Enable	Set the rule as enable or disable.
Source IP Address	Input the IP address of LAN user (such as PC or laptop) which you want to control.
Anywhere (of source IP Address)	Check the box if you want to control all LAN users.
Destination IP Address	Input the IP address of web site which you want to block.
Anywhere (of destination IP Address)	Check the box if you want to control all web sites, meaning the LAN user can't visit any web site.
Destination Port	Input the port of destination IP Address which you want to block. Leave it as blank if you want to block all ports of the web site.
Protocol	Select the protocol type (TCP, UDP or all). If you are unsure, please leave it to the default all protocol.

4.6.4 Web Filtering

Web filtering is used to deny LAN users from accessing the internet as shown below. Block those URLs which contain keywords listed below.

Web Filtering			
Web Filtering		<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Web Filtering Rules			
No.	Active	Filter Keyword	Action
Add Web Filtering Rule			

Figure: Web Filtering

Object	Description
Web Filtering	Set the function as enable or disable.
Add Web Filtering Rule	Go to the Add Web Filtering Rule page to add a new rule.

Web Filtering	
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Filter Keyword	<input type="text" value="ex. www.yahoo.com"/>
<input type="button" value="Apply Settings"/> <input type="button" value="Cancel Changes"/>	

Figure: Web Filtering Rule Setting

Object	Description
Active	Set the rule as enable or disable.
Filter Keyword	Input the URL address that you want to filter, such as www.yahoo.com.

4.6.5 Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall as shown below. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your VPN Security Gateway's NAT firewall.

Port Forwarding

Port Forwarding Enable Disable

Port Forwarding Rules

No.	Rule Name	Active	External Interface	Protocol	External Port Range	Internal IP	Internal Port Range	Action

Figure: Port Forwarding

Object	Description
Port Forwarding	Set the function as enable or disable.
Add Port Forwarding Rule	Go to the Add Port Forwarding Rule page to add a new rule.

Port Forwarding

Active
 Enable Disable

Rule Name

Protocol Both ▼

External Service Port ~

Virtual Server IP Address

Internal Service Port ~

Apply Settings
Cancel Changes

Figure: Port Forwarding Rule Setting

Object	Description
Rule Name	Enter any words for recognition.
Protocol	Select the protocol type (TCP, UDP or both). If you are unsure, please leave it to the default both protocols.
External Service Port	Enter the external ports you want to control. For TCP and UDP services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both

Object	Description
	the start and finish fields.
Virtual Server IP Address	Enter the local IP address.
Internal Service Port	Enter local ports you want to control. For TCP and UDP Services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields.

4.6.6 QoS

Please refer to the following sections for the details as shown below.

QoS - WAN1

Quality of Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Upstream	<input style="width: 50px;" type="text" value="0"/> Kbps
Downstream	<input style="width: 50px;" type="text" value="0"/> Kbps

QoS - WAN2

Quality of Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Upstream	<input style="width: 50px;" type="text" value="0"/> Kbps
Downstream	<input style="width: 50px;" type="text" value="0"/> Kbps

Upstream Bandwidth

Priority	Maximum Bandwidth	Bandwidth Value
Premium	<input style="width: 40px;" type="text" value="100"/> %	WAN1 <input style="width: 30px;" type="text" value="0"/> Kbps
		WAN2 <input style="width: 30px;" type="text" value="0"/> Kbps
Express	<input style="width: 40px;" type="text" value="100"/> %	WAN1 <input style="width: 30px;" type="text" value="0"/> Kbps
		WAN2 <input style="width: 30px;" type="text" value="0"/> Kbps
Standard	<input style="width: 40px;" type="text" value="100"/> %	WAN1 <input style="width: 30px;" type="text" value="0"/> Kbps
		WAN2 <input style="width: 30px;" type="text" value="0"/> Kbps
Bulks	<input style="width: 40px;" type="text" value="100"/> %	WAN1 <input style="width: 30px;" type="text" value="0"/> Kbps
		WAN2 <input style="width: 30px;" type="text" value="0"/> Kbps

Downstream Bandwidth

Priority	Maximum Bandwidth	Bandwidth Value
Premium	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps WAN2 <input type="text" value="0"/> Kbps
Express	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps WAN2 <input type="text" value="0"/> Kbps
Standard	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps WAN2 <input type="text" value="0"/> Kbps
Bulks	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps WAN2 <input type="text" value="0"/> Kbps

Service Priority

Protocol	Description	Priority	Action
<input type="text" value="AOL(TCP:5190)"/> ▼	AOL Instant Messenger protocol	<input type="text" value="Premium"/> ▼	<input type="button" value="Add"/>

Network Priority

Source Network	Protocol	Destination Port Range	Priority	Action
<input type="text"/> / <input type="text"/>	<input type="text" value="ALL"/> ▼	<input type="text"/> -- <input type="text"/>	<input type="text" value="Premium"/> ▼	<input type="button" value="Add"/>

4.6.7 DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network as shown below. Typically the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DMZ - WAN1

DMZ Enable Disable
 DMZ IP Address

DMZ - WAN2

DMZ Enable Disable
 DMZ IP Address

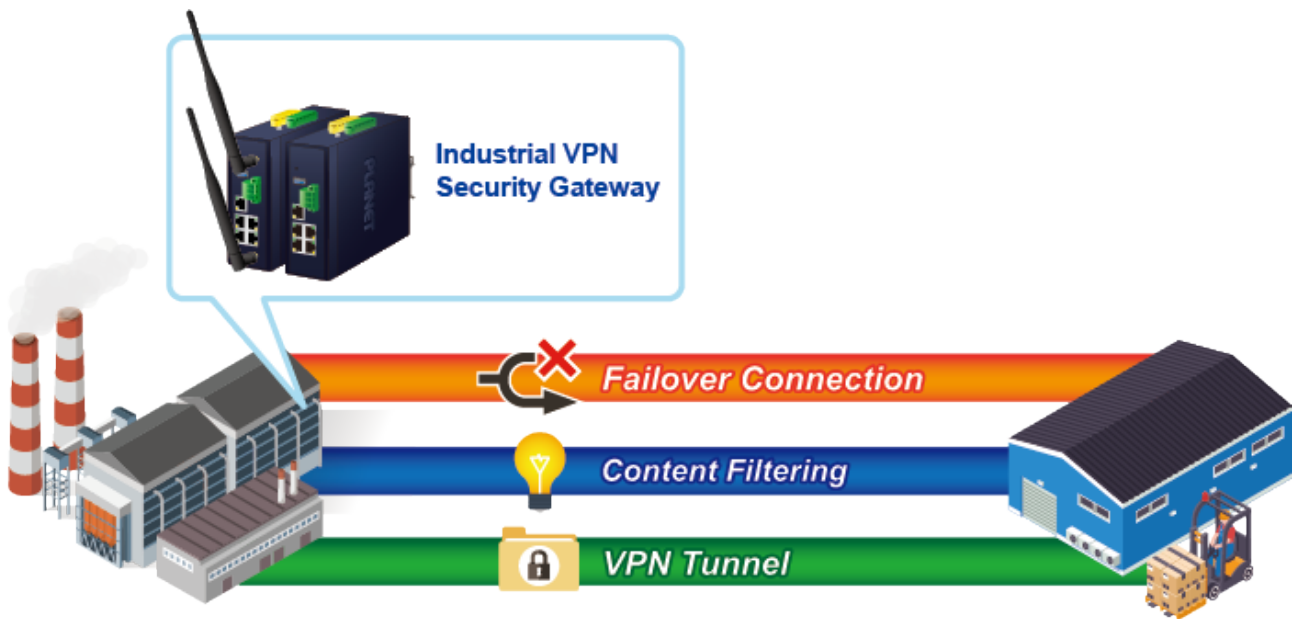
Apply Settings
Cancel Changes

Figure: DMZ

Object	Description
DMZ	Set the function as enable or disable. If the DMZ function is enabled, it means that you set up DMZ at a particular computer to be exposed to the Internet so that some applications/software, especially Internet/online game can have two way connections.
DMZ IP Address	Enter the IP address of a particular host in your LAN which will receive all the packets originally going to the WAN port/Public IP address above.

4.7 VPN

To obtain a private and secure network link, the **VPN** (Virtual Private Network) Security Gateway is capable of establishing VPN connections. When used in combination with remote client authentication, it links the business' remote sites and users, conveniently providing the enterprise with an encrypted network communication method. By allowing the enterprise to utilize the Internet as a means of transferring data across the network, it forms one of the most effective and secure options for enterprises to adopt in comparison to other methods.



The VPN menu provides the following features as shown below.



Figure: VPN Menu

Object	Description
IPsec	Allows setting IPsec function.
IPsec Remote Server	Disable or enable the IPsec Remote Server function. The default configuration is disabled.
GRE	Allows setting GRE function.
PPTP	Allows setting PPTP function.
L2TP	Allows setting L2TP function.
SSL VPN	Allows setting SSL VPN function.
Certificates	Download System CA Certificate
VPN Connection	Allows checking VPN Connection Status.

4.7.1 IPsec

IPsec (IP Security) is a generic standardized VPN solution. IPsec must be implemented in the IP stack which is part of the kernel. Since IPsec is a standardized protocol it is compatible to most vendors that implement IPsec. It allows users to have an encrypted network session by standard **IKE** (Internet Key Exchange). We strongly encourage you to use IPsec only if you need to because of interoperability purposes. When IPsec lifetime is specified, the device can randomly refresh and identify forged IKE's during the IPsec lifetime.

This page will allow you to modify the user name and passwords as shown below.

IPsec Configuration

IPsec Tunnels Enable Disable

IPsec Tunnel Lists

No.	Tunnel Name	Active	Status	Action

Figure: IPsec Configuration

Object	Description
Add IPsec Tunnel	Go to the Add IPsec Tunnel page to add a new tunnel.

IPsec Tunnel

Active Enable Disable

Tunnel Name

Type Net-to-Net Virtual Private Network ▼

Local Network

Local Netmask 255.255.255.0 /24 ▼

Remote Host/IP Address

Remote Network

Remote Netmask 255.255.255.0 /24 ▼

Detection

Dead Peer Detection

Time Interval Seconds Timeout Seconds Action Restart ▼

Authentication

Preshare Key

IKE Setting

Phase 1

IKE v1 v2

Connection Type Main Aggressive

ISAKMP AES (128 bit) ▼ SHA1 ▼ DH Group 2 (1024) ▼

IKE SA Lifetime hours

Phase 2

ESP AES (128 bit) ▼ SHA1 ▼

ESP Keylife hours

Perfect Forward Secrecy (PFS) Yes No

Figure: IPsec Tunnel

Object	Description
IPsec Tunnel Enable	Check the box to enable the function.
Tunnel Name	Enter any words for recognition.
Interface	This is only available for host-to-host connections and specifies to which interface the host is connecting. 1. WAN 1. 2. WAN 2.
Local Network	The local subnet in CIDR notation. For instance, "192.168.1.0".

Local Netmask	The netmask of this VPN Security Gateway
Remote IP Address	Input the IP address of the remote host. For instance, "210.66.1.10".
Remote Network	The remote subnet in CIDR notation. For instance, "210.66.1.0".
Remote Netmask	The netmask of the remote host.
Dead Peer Detection	<p>Set up the detection time of DPD (Dead Peer Detection).</p> <p>By default, the DPD detection's gap is 30 seconds, over 150 seconds to think that is the broken line.</p> <p>When VPN detects opposite party reaction time, the function will take one of the actions: "Hold" stand for the system will retain IPSec SA, "Clear" stand for the tunnel will clean away and waits for the new sessions, "Restart" will delete the IPSec SA and reset VPN tunnel.</p>
Preshare Key	Enter a pass phrase to be used to authenticate the other side of the tunnel. Should be the same as the remote host.
IKE	Select the IKE (Internet Key Exchange) version.
Connection Type	<ol style="list-style-type: none"> 1. Main. 2. Aggressive.
ISAKMP	<p>It provides the way to create the SA between two PCs. The SA can access the encoding between two PCs, and the IT administrator can assign to which key size or Preshare Key and algorithm to use. The SA comes in many connection ways.</p> <ol style="list-style-type: none"> 1. AES: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays. 2. 3DES: Triple DES is a block cipher formed from the DES cipher by using it three times. It can achieve an algorithm up to 168 bits. 3. SHA1: The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits. 4. SHA2: Either 256, 384 or 512 can be chosen 5. MD5 Algorithm: MD5 processes a variably long message into a fixed-length output of 128 bits. 6. DH Group: Either 1, 2, 5, 14, 15, 16, 17, or 18 can be chosen.
IKE SA Lifetime	You can specify how long IKE packets are valid.

ESP	<p>It offers AES, 3 DES, SHA 1, SHA2, and MD5.</p> <ol style="list-style-type: none"> 1. AES: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays. 2. 3DES: Triple DES is a block cipher formed from the DES cipher by using it three times. It can achieve an algorithm up to 168 bits. 3. SHA1: The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits. 4. SHA2: Either 256, 384 or 512 can be chosen. 5. MD5 Algorithm: MD5 processes a variably long message into a fixed-length output of 128 bits.
ESP Keylife	You can specify how long ESP packets are valid.
Perfect Forward Secrecy (PFS)	Set the function as enable or disable.

4.7.2 IPsec Remote Server

This section assists you in setting the IPsec Remote Server Configuration as shown below.

IPsec Remote Server Configuration

Remote Access Enable Disable

VPN Type IKEv2

Extensible Authentication Protocol MSCHAPv2

Account List

Index	Username	Password	Delete
	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	Add

Authentication

Certificate Self-signed certificate

Preshare Key

IPsec

Phase 1

ISAKMP DH Group

IKE SA Lifetime hours

Phase 2

ESP

ESP Keylife hours

4.7.3 GRE

This section assists you in setting the GRE Tunnel as shown below.

GRE Tunnel

GRE Tunnel Enable Disable

GRE Tunnel Lists

No.	Name	Enable	Through	Peer WAN IP Addr	Peer Subnet	Peer Tunnel IP	Local Tunnel IP	Local Netmask	Action
Add GRE Tunnel									

Figure: GRE Tunnel

Object	Description
GRE Tunnel	Set the function as enable or disable.
Add GRE Tunnel	Go to the Add GRE Tunnel page to add a new tunnel.

GRE Tunnel

Active Enable Disable

Tunnel Name

Through

Peer WAN IP Address

Peer Netmask

Peer Tunnel IP Address

Local Tunnel IP Address

Local Netmask

Figure: GRE Tunnel

Object	Description
Active	Check the box to enable the function.
Tunnel Name	Enter any words for recognition.
Through	This is only available for host-to-host connections and specifies to which interface the host is connecting. 1. LAN. 2. WAN 1. 3. WAN 2.
Peer WAN IP Address	Input the IP address of the remote host. For instance, "210.66.1.10".
Peer Netmask	The remote subnet in CIDR notation. For instance, "210.66.1.0/24".
Peer Tunnel IP Address	Input the Tunnel IP address of remote host.
Local Tunnel IP Address	Input the Tunnel IP address of remote host.
Local Netmask	Input the Tunnel IP address of the VPN Security Gateway

4.7.4 PPTP

Use the IP address and the scope option needs to match the far end of the PPTP server; its goal is to use the PPTP channel technology, and establish Site-to-Site VPN where the channel can have equally good results from different methods with IPsec. The PPTP server is shown in [Figure 4-8-6](#).

PPTP Server

PPTP Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Broadcast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Force MPPE Encryption	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
CHAP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
MSCHAP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
MSCHAP v2	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DNS1	<input type="text"/>
DNS2	<input type="text"/>
WINS1	<input type="text"/>
WINS2	<input type="text"/>
Server IP Address	<input type="text" value="192.168.10.1"/>
Clients IP Address Start	<input type="text" value="192.168.10.10"/>
Clients IP Address End	<input type="text" value="192.168.10.100"/>

Account List

Index	Username	Password	Delete
	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

Figure: PPTP server

Object	Description
PPTP Server	Set the function as enable or disable.
Broadcast	Enter any words for recognition.
Force MPPE Encryption	Set the encryption as enable or disable.
CHAP	Set the authentication as enable or disable.
MSCHAP	Set the authentication as enable or disable.
MSCHAP v2	Set the authentication as enable or disable.
DNS	When the PPTP client connects to the PPTP server, it will assign the DNS server IP address to client.
WINS	When the PPTP client connects to the PPTP server, it will assign the WINS server IP address to client.

Server IP Address	Input the IP address of the PPTP Server. For instance, "192.168.10.1".
Clients IP Address (Start/End)	When the VPN connection is established, the VPN client will get IP address from the VPN Server. Please set the range of IP Address. For instance, the start IP address is "192.168.10.10", the end IP address is "192.168.10.100".
User and Password	Create the username and password for the VPN client.

4.7.5 L2TP

This section assists you in setting the L2TP Server as shown below.

L2TP Server

L2TP Server Enable Disable

Server IP Address

Clients IP Address Start

Clients IP Address End

With IPsec Enable Disable

Preshare Key

Account List

Index	Username	Password	Delete
	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

IPsec

Phase 1

Connection Type Main Aggressive

ISAKMP DH Group

IKE SA Lifetime hours

Phase 2

ESP

ESP Keylife hours

Figure: L2TP Server

Object	Description
L2TP Server	Set the function as enable or disable.
Server IP Address	Input the IP address of the L2TP Server. For instance, "192.168.50.1".
Clients IP Address (Start/End)	When the VPN connection is established, the VPN client will get IP address from the VPN Server. Please set the range of IP Address. For instance, the start IP address is "192.168.50.100", the end IP address is

Object	Description
	"192.168.50.200".
With IPsec	Set the function as enable to make the L2TP work with IPsec encryption.
Preshare Key	Enter a pass phrase.
User and Password	Create the username and password for the VPN client.
Connection Type	<ol style="list-style-type: none"> 1. Main. 2. Aggressive.
ISAKMP	<p>It provides the way to create the SA between two PCs. The SA can access the encoding between two PCs, and the IT administrator can assign to which key size or Preshare Key and algorithm to use. The SA comes in many connection ways.</p> <ol style="list-style-type: none"> 1. AES: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays. 2. 3DES: Triple DES is a block cipher formed from the DES cipher by using it three times. It can achieve an algorithm up to 168 bits. 3. SHA1: The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits. 4. SHA2: Either 256, 384 or 512 can be chosen. 5. MD5 Algorithm: MD5 processes a variably long message into a fixed-length output of 128 bits. 6. DH Group: Either 1, 2, 5, 14, 15, 16, 17, or 18 can be chosen.
IKE SA Lifetime	You can specify how long IKE packets are valid.
ESP	<p>It offers AES, 3 DES, SHA 1, SHA2, and MD5.</p> <ol style="list-style-type: none"> 1. AES: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays. 2. 3DES: Triple DES is a block cipher formed from the DES cipher by using it three times. It can achieve an algorithm up to 168 bits. 3. SHA1: The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits. 4. SHA2: Either 256, 384 or 512 can be chosen. 5. MD5 Algorithm: MD5 processes a variably long message into a fixed-length output of 128 bits.
ESP Keylife	You can specify how long ESP packets are valid.

4.7.6 SSL VPN

This section assists you in setting the SSL Server as shown below.

SSL VPN

Server

Client

OpenVPN Server Enable Disable

Port

Tunnel Protocol

Virtual Network Device

Interface 192.168.1.1

VPN Network

Netmask

Set VPN as Default Gateway Enable Disable

Connect Server LAN to Client Enable Disable

Encryption Cipher

Hash Algorithm

Export client.ovpn

Remote Client Network Enable Disable

IP

Netmask

Figure: SSL Server

Object	Description
SSL VPN Server	Set the function as enable or disable.
Port	Set a port for the SSL Service. Default port is 1194.
Tunnel Protocol	Set the protocol as TCP or UDP.
Virtual Network Device	Set the Virtual Network Device as TUN or TAP.
Interface	User is able to select the interface for SSL service using.
VPN Network	The VPN subnet in CIDR notation. For instance, "192.168.20.0".
Network Mask	The netmask of the VPN.

Encryption Cipher	There are four encryption types: None, AES-128 CBC, AES-192 CBC or AES-256 CBC.
Hash Algorithm	There are five types of Hash Algorithm: None, SHA1, SHA1, SHA512 or MD5.
Export client.ovpn	Export a configuration for the SSL client. User is able to upload it to VPN client (such as Open VPN software).

4.7.7 Certificates

This page shows the VPN System Certificates status as shown below.

System Certificates

System CA Certificate
Download

System CA Certificate for HTTPS and VPN Server, please install to PC

Figure: System Certificates

4.7.8 VPN Connection

This page shows the VPN connection status as shown below.

VPN Connection Status

IPsec
GRE
PPTP
L2TP
SSL VPN

No.	Tunnel Name	Connected Time	Local IP	Remote IP	Local Subnet	Remote Subnet

Figure: VPN Connection Status

Object	Description
VPN Connection Status	Click the IPsec/GRE/.../SSL VPN bookmark to check the current connection status.

4.7.9 SD WAN

This page shows the SD WAN Configuration status as shown below.

SD WAN Configuration

SD WAN Enable Disable

SD WAN Lists

No.	Group Name	Local Subnet	Remote Subnet	Gateway	Action

SD WAN Configuration

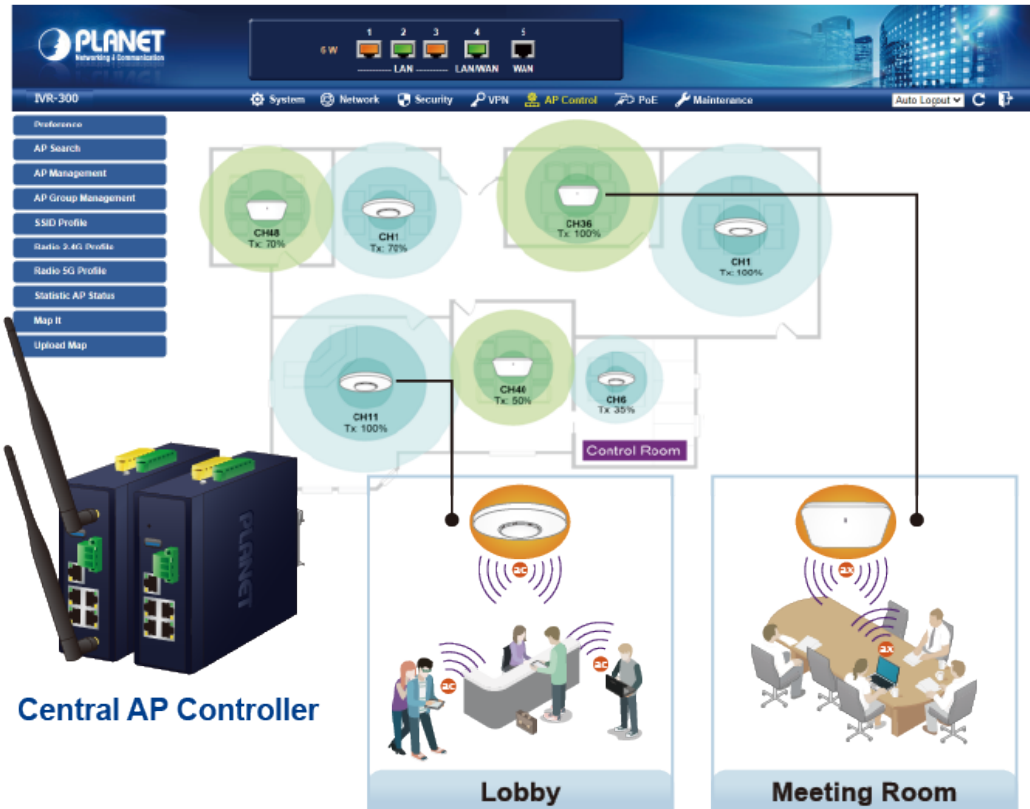
Group Name

IPsec Tunnel		Weight	Gateway
	<input type="checkbox"/>	<input style="width: 30px;" type="text" value="1"/>	WAN1 ()
	<input type="checkbox"/>	<input style="width: 30px;" type="text" value="1"/>	WAN2 ()

Figure: SD WAN Configuration

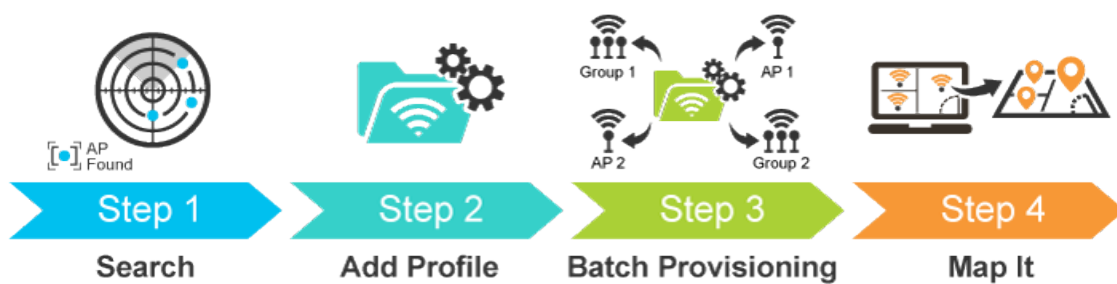
4.8 AP Control

The IVR-300/IVR-300W provides centralized management of PLANET Smart AP series via a user-friendly Web GUI. It's easy to configure AP for the wireless SSID, radio band and security settings. With a four-step configuration process, wireless profiles for different purposes can be simultaneously delivered to multiple APs or AP groups to minimize deployment time, effort and cost.



For example, to configure multiple smart APs of the same model, the IVR-300/IVR-300W allows clustering them to a managed group for unified management. According to requirements, wireless APs can be flexibly expanded or removed from a wireless AP group at any time. The AP cluster benefits bulk provision and bulk firmware upgrade through single entry point instead of having to configure settings in each of them separately.

Simplified Cluster Management with 4 Steps



The AP Control menu provides the following features for managing the system as shown below.



Figure: AP Control Menu

Object	Description
Preference	Edit region, RO community, RW community
AP Search	Search APs in the same domain
AP Management	Config APs IP Address, Subnet Mask, SSID and Radio Profiles
AP Group Management	Grouping same model AP
SSID Profile	Setup SSID Profile
Radio 2.4GHz Profile	Setup Radio 2.4GHz Profiles
Radio 5GHz Profile	Setup Radio 5GHz Profiles
Statistics AP Status	Show the status of managed APs
Map It	Edit the map of AP location and coverage
Upload Map	Search APs in the same domain


4.8.1 Preference

On this page, you can choose the device region of FCC or ETSI. Then edit RO community and RW community for public or private use. Select Apply or Reset. This screenshot is as shown below.

AP Preference

Region	ETSI
RO Community	public
RW Community	private

Figure: AP Preference



Device of FCC and device of ETIS cannot be shown at the same time.

4.8.2 AP Search

On this page, you can add new APs in your AP Control System.

Steps to follow:

Step 1. Press the **Search** button to discover PLANET devices.


Step 2. After waiting for a while, choose which AP you want to add.

Step 3. Press the **Apply** button to finish addition.

AP Search

 Filter by Model, MAC, IP





Num.	MAC Address	Device Type	Model No.	Version	Device IP	Device Description	<input type="checkbox"/>
1	a8:f7:e0:33:44:56	Wireless	WDAP-850AC	WDAP-850AC-AP-ETSI-V3.0-Build20210104135430	<u>192.168.1.253</u>		<input type="checkbox"/>









When using AP Search, the AP's IP Address must be the same as WS-Series Switch IP domain.

4.8.3 AP Management


On this page, you can manage your APs, including checking AP online status, configuring AP (IP address, Mask, SSID and Radio profile), rebooting AP, firmware update, and deleting AP in the AP Control system.

AP Management



 Apply Filter by Context 







● Online ● Offline ● Disable

☐	Status	AP Group	MAC Address	Device Type	Model No.	Version	IP Address	Device Description	Action
☐	●		a8:f7:e0:33:44:56	Wireless	WDAP-850AC	WDAP-850AC-AP-ETSI-V3.0-Build20210104135430	192.168.1.254		     

Status:

Object	Description
● ● ●	Connection status: online, offline, Wi-Fi disabled
	In progress: action in progress
✓	Finished/Successful: action finished and successful.
✗	Failed: action failed.

Action:

Object	Description
	Setting: edit setting and allocate profile to AP
	Link: link to the AP's web page
	Firmware Update: Upgrade AP's firmware
	Reboot: Reboot the AP
	Delete: Delete the AP from the control list LED Control: Control the AP's LED.
	Mouse-click in a sequential order: LED blink-> LED off-> LED on



To configure multiple APs at one time, select multiple APs and then choose one of the action icons on the top of the page. The "**Link**" action is not allowed for multiple APs.



To do profile provisioning to multiple AP groups at one time, select multiple AP groups, and then click the “**Apply**” button.

The “**Link**” action is not allowed for multiple APs or AP group.

4.8.5 SSID Profile

On the SSID profile configuration page, enter the value that you preferred and then click “**Apply**” to save the profile.

SSID Profile Filter by SSID Name 10 (10..16)

<input type="checkbox"/>	Num.	Model No.	SSID Name	SSID Broadcast	Security	Encryption	Client Isolation	Action
<input type="checkbox"/>	1	WDAP-850AC	WDAP-850ACP-10F	Disabled	WPA	Personal (Pre-Shared Key)	Enabled	

SSID Profile Configuration

SSID Profile Configuration	
Model No.	WDAP-850AC
SSID Configuration	
SSID Name	WDAP-850ACP-10F
Hide SSID	<input checked="" type="checkbox"/>
Client Isolation	Enable
VLAN Isolation	Enable
VLAN ID	3 (3 to 4094)
Security Configuration	
Encryption	WPA
Authentication Mode	Personal (Pre-Shared Key)
Cipher Suite	TKIP
Pre-Shared Key Format	Passphrase
Pre-Shared Key	WDAP-850ACP-10F

Action:

Object	Description
	Add new profile: Click it to add a new profile.
	Delete selected item: Click it to delete the selected profile.
	Edit: Click it to edit the profile.





Delete: Click it to delete the single profile.





4.8.6 Radio 2.4GHz Profile

On the Radio profile configuration page, enter the value that you preferred and then click “**Apply**” to save the profile.

Radio Profile 2.4GHz Filter by Profile Name

<input type="checkbox"/>	Num.	Model No.	Profile Name	Wireless Mode	Channel ID	Channel Bandwidth	Tx Power	Data Rate	Action
<input type="checkbox"/>	1	WDAP-850AC	Test 2.4GHz	11b/g/n mixed mode	Auto	40MHz	100%	N/A	 

Action:

Object	Description
	Add new profile: Click it to add a new profile.
	Delete selected item: Click it to delete the selected profile.
	Edit: Click it to edit the profile.
	Delete: Click it to delete the single profile.

Radio Profile 2.4GHz Configuration

Radio Profile Configuration	
Model No.	WDAP-850AC
Basic Setting	
Radio Profile Description	Test 2.4GHz
Wireless Mode	11b/g/n mixed mode
Channel Bandwidth	40MHz
Channel	Auto
Tx Power	100%
Client Limit	<input checked="" type="checkbox"/> 64 (0 to 64)
RSSI Threshold	-95 (-95 to -65) dBm

Action:

Object	Description
Apply Button:	Click this button to save the settings.
Back Button:	Click this button to return to the previous page.
Reset Button:	Click this button to reset all fields to default value.



Strongly suggest you to keep the values as default except the fields like Channel, Network Mode, Channel Bandwidth, Tx Power, IAPP, and Tx/Rx to prevent any unexpected error or impact on the performance.



WMM Capable is not allowed to be disabled.

4.8.7 Radio 5GHz Profile

On the Radio profile configuration page, enter the value that you preferred and then click “**Apply**” to save the profile.

Radio Profile 5GHz

<input type="checkbox"/>	Num.	Model No.	Profile Name	Wireless Mode	Channel ID	Channel Bandwidth	Tx Power	Data Rate	Action
<input type="checkbox"/>	1	WDAP-850AC	Test 5GHz-10F	11n/ac mixed mode	Auto	40MHz	100%	N/A	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Action:

Object	Description
	Add new profile: Click it to add a new profile.
	Delete selected item: Click it to delete the selected profile.
	Edit: Click it to edit the profile.
	Delete: Click it to delete the single profile.

Radio Profile 5GHz Configuration

Apply Back Reset

Radio Profile Configuration	
Model No.	WDAP-850AC
Basic Setting	
Radio Profile Description	Test 5GHz-10F
Wireless Mode	11n/ac mixed mode
Channel Bandwidth	40MHz
Channel	Auto
Tx Power	100%
Client Limit	<input checked="" type="checkbox"/> 64 (0 to 64)
RSSI Threshold	-95 (-95 to -65) dBm

Action:

- Apply Button:** Click this button to save the settings.
- Back Button:** Click this button to return to the previous page.
- Reset Button:** Click this button to reset all fields to default value.



- Strongly suggest you to keep the values as default except the fields like Channel, Network Mode, Channel Bandwidth, Tx Power, IAPP, and Tx/Rx to prevent any unexpected error or impact on the performance.
- WMM Capable is not allowed to be disabled.

4.8.8 Statistics AP Status

On this page, you can observe the current configuration of all managed APs.

Statistic > Managed APs Filter by Context 10 (10, 64)

Online
 Offline
 Disable

Num	Status	MAC Address	IP Address	Model No.	Name	firmware	AP Group	2.4GHz SSID Profile	5GHz SSID Profile	2.4GHz Radio Profile	5GHz Radio Profile
1		a8:f7:e0:46:2e:38	192.168.0.102	WDAP-C7200E		WDAP-C7200E-AP-FCC-V3.0-Build20200321122005					
2		a8:f7:e0:3c:5f:ab	192.168.0.101	WNAP-C3220E		WNAP-C3220E-AP-FCC-V3.0-Build20200422115453			N/A		N/A

Filter: You can filter the AP list by entering the keyword in the field next to the magnifier icon. The keyword should be in any context that belongs to the fields of this page.

4.8.9 Map It

On this page you can add managed APs to the actual position against the floor map. This is convenient to user to view and adjust the actual deployment by reference to its real transmission power and channel allocation.

Upload Map



Map	New Map ▾
Upload File	Choose File No file chosen
New Description	<input type="text"/>
File Size	Bytes

The interface consists of a left sidebar and a main map area. The sidebar contains a table of devices and configuration options.

I	S	Device Description	A
1	<input checked="" type="checkbox"/>	WDAP-C7200E	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	WNAP-C3220E	<input type="checkbox"/>

Configuration options in the sidebar include: AP Group, Band, Transparency, and Scale. The Scale section shows a value of 1:30.303030303030305m and a 'Cancel' button.

The main map area shows a floor plan with a coordinate grid (0 to 300m). A red box labeled '2' highlights a door. A dialog box labeled '3' asks 'What is the physical distance of the draw line?' with a 'Set' button.

The bottom screenshot shows the same floor plan with blue circles representing AP coverage areas. The Scale section now shows a value of 1:39.21568627450981m and a 'Set' button.

1. Click **"Scale"** to start to reset the map scale.
2. Press the set button to draw a line on the map. Fill its physical distance in the blank and press Set or Cancel. For example, in the graph below, set the door width to 0.8 m



You need to upload map image first before bringing managed APs to the actual position.

4.8.10 Upload Map

On this page, the system allows you to upload your floor map to the system.

Upload Map

Map	<input type="text" value="New Map"/>
Upload File	<input type="button" value="Choose File"/> No file chosen
New Description	<input type="text"/>
File Size	Bytes



The system allows user to upload up to 10 floor maps.

4.9 Wireless

(For IVR-300W Only)

The IVR-300W is designed with high power amplifier and 2 highly-sensitive antennas which provide stronger signal and excellent coverage even in the wide-ranging or bad environment. With adjustable transmit power option, the administrator can flexibly reduce or increase the output power for various environments, thus reducing interference to achieve maximum performance. Equipped with the next-generation Wi-Fi 6 (802.11ax) wireless network standard, the total bandwidth reaches 1800Mbps, and the 2-stream transmission technology improves the transmission efficiency of multiple devices, making AR/VR/IoT applications smoother. The IEEE 802.11ax also optimizes MU-MIMO (Multi-User MIMO) mechanism to serve multiple devices simultaneously.

The Wireless menu provides the following features as shown below.

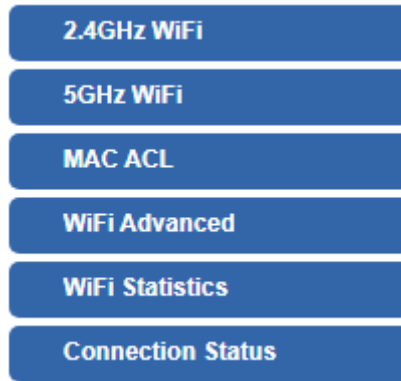


Figure: Wireless Menu

Object	Description
2.4GHz Wi-Fi	Allow to configure 2.4GHz Wi-Fi.
5GHz Wi-Fi	Allow to configure 5GHz Wi-Fi.
MAC ACL	Allow configure MAC ACL.
Wi-Fi Advanced	Allow to configure advanced setting of Wi-Fi.
Wi-Fi Statistics	Display the statistics of Wi-Fi traffic.
Connection Status	Display the connection status.

4.9.1 2.4GHz WiFi

This page allows the user to define 2.4GHz WiFi as shown below.

2.4GHz WiFi Configuration

Basic

Virtual AP1

Virtual AP2

Virtual AP3

Wireless Status Enable Disable

Wireless Name (SSID)

Hide SSID Enable Disable

Bandwidth ▾

Channel ▾

Encryption ▾

WiFi Multimedia Enable Disable

VLAN ID

Apply Settings

Cancel Changes

Figure: 2.4GHz WFI

Object	Description
Wireless Status	Allows user to enable or disable 2.4GHz Wi-Fi
Wireless Name (SSID)	It is the wireless network name. The default 2.4GHz SSID is "PLANET_2.4G"
Hide SSID	Allows user to enable or disable SSID
Bandwidth	Select the operating channel width, "20MHz" or "40MHz"
Channel	It shows the channel of the CPE. Default 2.4GHz is channel 6.
Encryption	Select the wireless encryption. The default is "Open"
Wi-Fi Multimedia	Enable/Disable WMM (Wi-Fi Multimedia) function

4.9.2 5GHz WiFi

This page allows the user to define 5GHz Wi-Fi as shown below.

5GHz WiFi Configuration

Basic

Virtual AP1

Virtual AP2

Virtual AP3

Wireless Status Enable Disable

Wireless Name (SSID)

Hide SSID Enable Disable

Bandwidth

Channel

Encryption

WiFi Multimedia Enable Disable

VLAN ID

Apply Settings
Cancel Changes

Figure: 5GHz WFI

Object	Description
Wireless Status	Allows user to enable or disable 5GHz Wi-Fi
Wireless Name (SSID)	It is the wireless network name. The default 5GHz SSID is "PLANET_5G"
Hide SSID	Allows user to enable or disable SSID
Bandwidth	Select the operating channel width, "20MHz" or "40MHz" or "80MHz"
Channel	It shows the channel of the CPE. Default 5GHz is channel 36.
Encryption	Select the wireless encryption. The default is "Open"
Wi-Fi Multimedia	Enable/Disable WMM (Wi-Fi Multimedia) function

4.9.3 MAC ACL

This page provides MAC ACL configuration as shown below.

MAC ACL

MAC ACL Enable Disable

MAC ACL Rules


Index	Active	Device Name	MAC Address	Action
		abc	00:30:4F:00:00:01	<div style="margin-bottom: 5px;">Add</div> <div>Scan</div>

Figure: MAC ACL

Object	Description
Active	Allows the devices to pass in the rule
Device Name	Set an allowed device name
MAC Address	Set an allowed device MAC address
Add	Press the “ Add ” button to add end-device that is scanned from wireless network and mark them
Scan	Connect to client list

4.9.4 Wi-Fi Advanced

This page allows the user to define advanced setting of Wi-Fi as shown below.

WiFi Advanced	
2.4GHz Mode	11 AX ▾
5GHz Mode	11 AX ▾
2.4GHz Maximum Associated Clients	32 (Range 1~64)
5GHz Maximum Associated Clients	32 (Range 1~64)
2.4GHz Coverage Threshold	-95 (-95dBm ~ -60dBm)
5GHz Coverage Threshold	-95 (-95dBm ~ -60dBm)
2.4GHz TX Power	Max(100%) ▾
5GHz TX Power	Max(100%) ▾

Figure: Wi-Fi advanced

Object	Description
2.4GHz Mode	11AC: Select 802.11B/G or 802.11N/G 11AX: Select 802.11B/G or 802.11N/G or 802.11AX
5GHz Mode	11AC: Select 802.11A or 802.11AN or 802.11AC 11AX: Select 802.11A or 802.11AN or 802.11AC or 802.11AX
2.4GHz Maximum Associated Clients	The maximum users are 64.
5GHz Maximum Associated Clients	The maximum users are 64.
2.4GHz Coverage Threshold	The coverage threshold is to limit the weak signal of clients occupying session. The default is -90dBm.
5GHz Coverage Threshold	The coverage threshold is to limit the weak signal of clients occupying session. The default is -90dBm.
2.4G TX Power	The range of transmit power is Max (100%), Efficient (75%), Enhanced (50%), Standard (25%) or Min (15%) . In case of shortening the distance and the coverage of the wireless network, input a smaller value to reduce the radio transmission power
5G TX Power	The range of transmit power is Max (100%), Efficient (75%), Enhanced (50%), Standard (25%) or Min (15%) . In case of shortening the distance and the coverage of the wireless network, input a smaller value to reduce the radio transmission power.

4.9.5 Wi-Fi Statistics

This page displays Wi-Fi statistics as shown below.

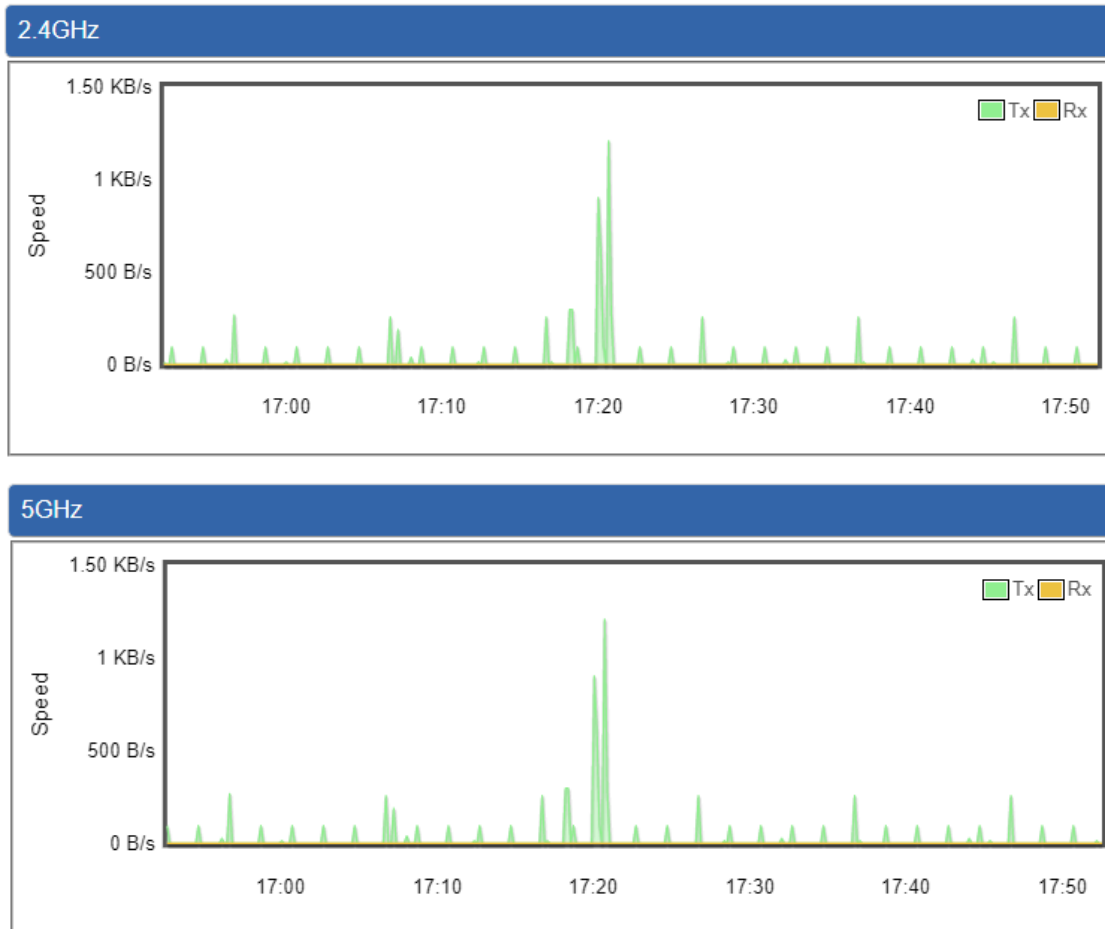


Figure: Wi-Fi statistics

4.9.6 Connection Status

This page shows the host names and MAC address of all the clients in your network as shown below.

Client List				
No.	Name	MAC Address	Signal	Connected Time

Figure: Connection status

Object	Description
Name	Display the host name of connected clients.
MAC Address	Display the MAC address of connected clients.
Signal	Display the connected signal of connected clients.
Connected Time	Display the connected time of connected clients.

4.10 Maintenance

The Maintenance menu provides the following features for managing the system as shown below.

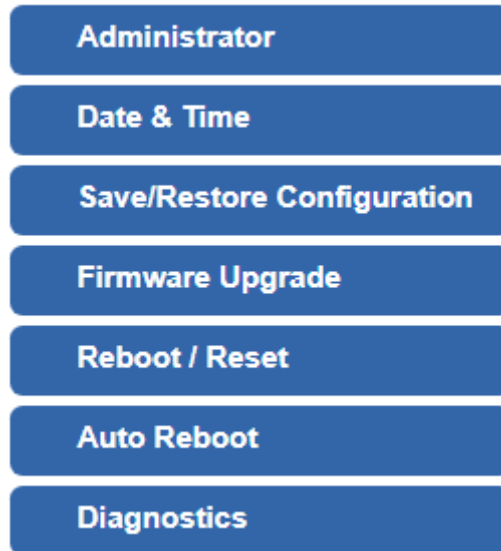


Figure: Maintenance Menu

Object	Description
Administrator	Allows changing the login username and password.
Date & Time	Allows setting Date & Time function.
Save/Restore Configuration	Export the VPN Security Gateway's configuration to local or USB sticker. Restore the VPN Security Gateway's configuration from local or USB sticker.
Firmware Upgrade	Upgrade the firmware from local or USB storage.
Reboot / Reset	Reboot or reset the system.
Auto Reboot	Allows setting auto-reboot schedule.
Diagnostics	Allows you to issue ICMP PING packets to troubleshoot IP.

4.10.1 Administrator

To ensure the VPN Security Gateway's security is secure, you will be asked for your password when you access the VPN Security Gateway's Web-based utility. The default user name and password are "**admin**". This page will allow you to modify the user name and passwords as shown below.

Account Password

Username	<input type="text" value="admin"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>

The password must contain 8-31 characters, including upper case, lower case, numerals and other symbols

Figure: account and password page

Object	Description
Username	Input a new username.
Password	Input a new password.
Confirm Password	Input password again.

4.10.2 Date and Time

This section assists you in setting the system time of the VPN Security Gateway. You are able to either select to set the time and date manually or automatically obtain the GMT time from Internet as shown below.

Date and Time

Current Time Year Month Day Hour Minute Second

Time Zone Select

NTP Client Update Enable Disable

NTP Server

Figure: date and time page

Object	Description
Current Time	Show the current time. User is able to set time and date manually.
Time Zone Select	Select the time zone of the country you are currently in. The VPN Security Gateway will set its time based on your selection.
NTP Client Update	Once this function is enabled, VPN Security Gateway will automatically update current time from NTP server.
NTP Server	User may use the default NTP sever or input NTP server manually.

4.10.3 Saving/Restoring Configuration

This page shows the status of the configuration. You may save the setting file to either USB storage or PC and load the setting file from USB storage or PC as shown below.

Save/Restore Configuration

Configuration Export

Configuration Import No file chosen

USB Backup/Upload Configuration

USB Storage Not Detected

Backup Settings to USB Storage

Load Settings from USB Storage Configuration disabled

Please format the Storage as FAT32 on a Windows PC before using it for backup

Figure: Saving/Restoring Configuration

■ Save Setting to PC

Object	Description
Configuration Export	Press the <input type="button" value="Export"/> button to save setting file to PC.
Configuration Import	Press the <input type="button" value="Choose File"/> button to select the setting file, and then press the <input type="button" value="Import"/> button to upload setting file from PC.

■ Save Setting to USB Storage

Object	Description
USB Storage	The status of USB storage.
Backup Settings to USB Storage	Press the <input type="button" value="Save"/> button to save setting file to USB storage.

Object	Description
Load Settings from USB Storage	Press the <input type="button" value="Upload"/> button to upload setting file from USB storage.
Unmount	Before removing the USB storage from the VPN Security Gateway, please press the <input type="button" value="Unmount"/> button first.

4.10.4 Firmware Upgrade

This page provides the firmware upgrade function as shown below.

Firmware Information

Firmware Version	v1.2102b220218
Last Upgrade Date	N/A

Firmware Upgrade

Select File No file chosen

USB Firmware Upgrade

USB Storage	Not Detected
Load Firmware from USB Storage	Not Found <input type="button" value="Upload"/>

Please format the Storage as FAT32 on a Windows PC before using it

Figure: firmware upgrade page

Object	Description
Choose File	Press the button to select the firmware.
Upgrade	Press the button to upgrade firmware to system.

4.10.5 Reboot / Reset

This page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, users have to re-log in the Web interface as shown below.

Reboot / Reset

Reboot Button Reboot

Reset Button Reset to Default

I'd like to keep the network profiles.
Keep your current network profiles and reset all other configuration to factory defaults.

Figure: reboot/reset page

Object	Description
Reboot	Press the button to reboot system.
Reset to Default	Press the button to restore all settings to factory default settings.
I'd like to keep the network profiles.	Check the box and then press the Reset to Default button to keep the current network profiles and reset all other configurations to factory defaults.

Object	Description
Interface	Select an interface of the VPN Security Gateway
Target Host	The destination IP Address or domain.
Number of Packets	Set the number of packets that will be transmitted; the maximum is 100.
Ping	The time of ping.



Be sure the target IP address is within the same network subnet of the VPN Security Gateway, or you have to set up the correct gateway IP address.

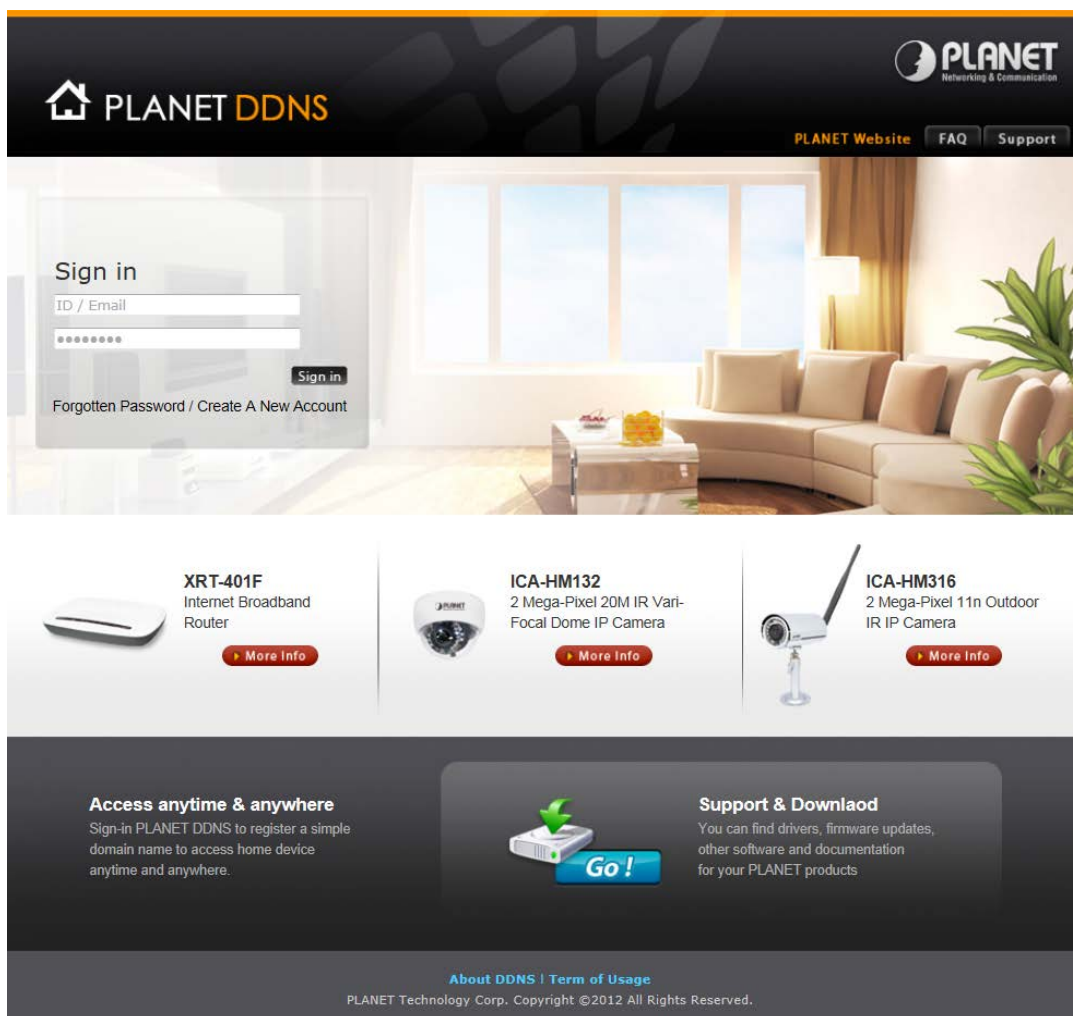
Appendix A: DDNS Application

Configuring PLANET DDNS steps:

Step 1: Visit DDNS provider's web site and register an account if you do not have one yet. For example, register an account at <http://planetddns.com>

Step 2: Enable DDNS option through accessing web page of the device.

Step 3: Input all DDNS settings.



The screenshot shows the PLANET DDNS website. At the top, there is a navigation bar with the PLANET logo and links for 'PLANET Website', 'FAQ', and 'Support'. The main content area features a 'Sign in' form with fields for 'ID / Email' and a password, a 'Sign in' button, and links for 'Forgotten Password / Create A New Account'. Below the form, there are three product cards: 'XRT-401F Internet Broadband Router', 'ICA-HM132 2 Mega-Pixel 20M IR Vari-Focal Dome IP Camera', and 'ICA-HM316 2 Mega-Pixel 11n Outdoor IR IP Camera', each with a 'More Info' button. At the bottom, there are two sections: 'Access anytime & anywhere' with a 'Go!' button and 'Support & Download' with a description of available resources. The footer contains 'About DDNS | Term of Usage' and 'PLANET Technology Corp. Copyright ©2012 All Rights Reserved.'