

DAP-2695 Version 1.13

Wireless AC

AC1750 Dual Band Access Point

User Manual

Business Class Networking

Table of Contents

Product Overview	4
Introduction	4
Features	5
Package Contents	6
System Requirements	6
Hardware Overview	7
LEDs	7
Connections	7
Basic Installation	8
Hardware Setup	8
Method 1 - PoE with PoE Switch or Router	8
Method 2 - PoE without PoE Switch or Router	9
Web User Interface	.10
Web User Interface Wireless	
	11
Wireless	11 11
Wireless Access Point Mode	11 11 13
Wireless Access Point Mode WDS with AP Mode	11 11 13 15
Wireless Access Point Mode WDS with AP Mode WDS Mode	11 11 13 15 17
Wireless Access Point Mode WDS with AP Mode WDS Mode Wireless Client Mode	11 11 13 15 17 18
Wireless Access Point Mode WDS with AP Mode WDS Mode Wireless Client Mode Wireless Security	11 13 15 17 18 18
Wireless Access Point Mode WDS with AP Mode WDS Mode Wireless Client Mode Wireless Security Wireless Security	11 13 15 17 18 18 19
Wireless Access Point Mode WDS with AP Mode WDS Mode Wireless Client Mode Wireless Security Wireless Security Wired Equivalent Privacy (WEP) Wi-Fi Protected Access (WPA / WPA2)	11 13 15 17 18 18 19 21
Wireless Access Point Mode WDS with AP Mode WDS Mode Wireless Client Mode Wireless Security Wireless Security Wired Equivalent Privacy (WEP) Wi-Fi Protected Access (WPA / WPA2) LAN	11 13 15 17 18 18 19 21 22

Multi-SSID27
VLAN
VLAN List29
Port List
Add/Edit VLAN31
PVID Settings32
Intrusion
Schedule
Internal RADIUS Server35
ARP Spoofing Prevention
Bandwidth Optimization37
AP Array
AP Array Scan
Configuration Settings40
Auto-RF44
Load Balance45
Captive Portal46
Authentication Settings-Web Redirection Only 46
Authentication Settings- Username/Password48
Authentication Settings- Passcode
Authentication Settings- Remote RADIUS52
Authentication Settings- LDAP54
Authentication Settings- POP356
Login Page Upload58
IP Filter Settings59
MAC Bypass60

DHCP Server61	
Dynamic Pool Settings61	
Static Pool Setting62	
Current IP Mapping List63	
Filters64	
Wireless MAC ACL64	
WLAN Partition65	
Traffic Control	1 /
Uplink/Downlink Setting66	Kn
QoS67	
Traffic Manager68	
Status69	Tre
Device Information70	
Client Information71	
WDS Information Page72	
Channel Analyze73	
Stats Page74	
Ethernet Traffic Statistics74	_
WLAN Traffic Statistics75	Те
Log76	An
View Log76	_
Log Settings77	Ce
Maintenance Section78	
Administration79	
Limit Administrator79	
System Name Settings80	
Login Settings80	
Console Settings80	
SNMP Settings81	

Central WiFiManager Settings	81
Firmware and SSL Upload	82
Configuration File Upload	83
Time and Date Settings	84
Configuration and System	85
System Settings	86
Help	87
Knowledge Base	88
Wireless Basics	88
Wireless Installation Considerations	89
Troubleshooting	90
Troubleshooting Why can't I access the web-based configuration	90
-	
Why can't I access the web-based configuration	90
Why can't I access the web-based configuration utility?	90 90
Why can't I access the web-based configuration utility? What can I do if I forgot my password?	90 90 91
Why can't I access the web-based configuration utility? What can I do if I forgot my password? How to check your IP address?	90 90 91 92
Why can't I access the web-based configuration utility? What can I do if I forgot my password? How to check your IP address? How to statically assign an IP address?	90 90 91 92 93

Product Overview Introduction

D-Link, an industry pioneer in wireless networking, introduces a solution for businesses seeking to deploy next generation 802.11ac LANs. D-Link unveils its new DAP-2695, designed specifically for business-class environments such as large or enterprise corporations to provide secure and manageable dual band wireless LAN options for network administrators.

Versatile Access Point

The DAP-2695 Access Point allows network administrators to deploy a highly manageable and extremely robust dual band wireless network. All six antennas are detachable and can provide optimal wireless coverage in either 2.4GHz (802.11g and 802.11n) or 5GHz (802.11ac, 802.11a, and 802.11n) bands. Enclosed in a plenum-rated metal chassis, the DAP-2695 Access Point adheres to strict fire codes for placement in air passageways. For advanced installations, this new high-speed Access Point has integrated 802.3at Power over Ethernet (PoE) support, allowing installation of this device in areas where power outlets are not readily available.

Enhanced Performance

The DAP-2695 delivers reliable wireless performance with maximum wireless signal rates of up to 1750Mbps. This, coupled with support for Wi-Fi Multimedia[™] (WMM) Quality of Service features, makes it an ideal access point for audio, video, and voice applications. Additionally, the DAP-2695 supports load balance features to ensure maximum performance.

Security

To help maintain a secure wireless network, the DAP-2695 provides the latest in wireless security technologies by supporting both Personal and Enterprise versions of WPA and WPA2 (802.11i) with support for RADIUS server back end. To further protect your wireless network, MAC Address Filtering, Wireless LAN segmentation, Disable SSID Broadcast, Rogue AP Detection, and Wireless Broadcast Scheduling are also included.

The DAP-2695 includes support for up to 16 VLANs for implementing multiple SSIDs to further help segment users on the network. The DAP-2695 also includes a wireless client isolation mechanism, which limits direct client-to-client communication.

Power Usage

This device is an Energy Related Product (ErP) with High Network Availability (HiNA), and automatically switches to a power-saving Network Standby mode within 1 minute of no packets being transmitted. It can also be turned off through a power switch to save energy when it is not needed. **Network Standby:** 4.98 watts **Switched Off:** 0.24 watts

**Only compliant with 802.3at PoE switch and 802.3af standard can't supply sufficient power for DAP-2695

^{*} Maximum wireless signal rate derived from IEEE Standard 802.11ac, 802.11g, 802.11a, and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

Features

- Provide Ethernet to Wireless LAN bridge fully IEEE 802.3/u/ab compatible on the Ethernet side and fully interoperable with IEEE 802.11ac and b/g/n/a compliant equipment
- Compatible with IEEE 802.11b high rate standard to provide wireless 11Mbps data rate
- Compatible with IEEE 802.11g higher speed standard to provide wireless 54Mbps data rate
- Compatible with IEEE 802.11a higher speed standard to provide wireless 54Mbps data rate
- Compatible with IEEE 802.11n higher speed standard to provide wireless 450Mbps data rate
- Compatible with 802.11ac higher speed standard to provide wireless 1300Mbps data rate
- Operation at 2.4~2.5GHz and 5.15~5.85GHz frequency band to meet worldwide regulations
- Supports IEEE 802.11ac and b/g/n/a wireless data encryption with 64/128-bit WEP for security
- Allows auto fallback data rate for reliability, optimized throughput and transmission range
- Web-based configuration and management
- Supports enhanced security WPA-PSK and WPA2-PSK, RADIUS client, and Cipher negotiation
- Supports one 802.3at PoE port
- Supports two 10/100/1000M Ethernet ports
- AP Mode, WDS Mode, WDS with AP, and Wireless Client Mode
- Supports SNMP v1,v2,v3
- Support Trap server (SNMP v1, v2c)
- Support AP Manager II and D-View 6.0
- Support AP Array and AP Array Setup Tool
- Support Port Redundancy
- Support one RJ-45 console port for debug

***Only compliant with 802.3at PoE switch and 802.3af standard can't supply sufficient power for DAP-2695

^{*} Maximum wireless signal rate derived from IEEE Standard 802.11ac, 802.11g, 802.11a, and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

^{**}Please note that operating frequency ranges vary depending on the regulations of individual countries and jurisdictions. The DAP-2695 isn't supported in the 5.25~5.35GHz and 5.47 ~ 5.725GHz frequency ranges in some regions.

Package Contents

- DAP-2695 802.11ac Power over Ethernet (PoE) Access Point
- Six Detachable Antennas
- Mounting Plate and Hardware
- Ethernet Cable
- Console Cable
- CD (with software and user manual)

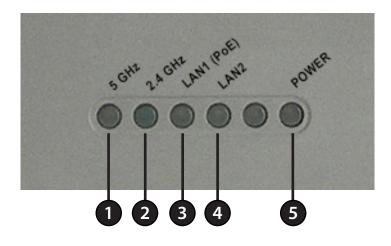
Note: No PSU supplied. To power the units use an D-Link PoE switch or the D-Link DPE-101GI PoE injector.

System Requirements

- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet Adapter
- Internet Explorer 11, Safari 7, Firefox 28, or Google Chrome 33 and Above (for configuration)

Hardware Overview

LEDs



Connections



1	5GHz	When lit, the access point is operating at 5GHz. This light will blink when there is wireless traffic.
2	2.4GHz	When lit, the access point is operating at 2.4GHz. This light will blink when there is wireless traffic.
3	LAN1 (PoE)	Solid light when the Ethernet port is connected to a power over Ethernet (PoE) port, such as a router or switch. The light will blink when there is traffic through LAN port.
4	LAN2	Solid light when the Ethernet port is connected to a working port, such as a router or switch. The light will blink when there is traffic through LAN port.
5	Power	The light will blink during boot up. Once solid, the access point is ready.

1	Reset Button	Press and hold for six seconds to reset the access point to the factory default settings.
2	Console Port	Connect the supplied console cable to configure using a command line interface.
3	LAN2 Port	Connect to your network with an Ethernet cable.
4	LAN1 (PoE) Port	Connect to a Power over Ethernet (PoE) switch or router.
5	Power Receptor	Connect the supplied power adapter. (*Note no longer used, replaced by PoE)

Basic Installation Hardware Setup

To power the access point, you can use one of the following 2 methods:

Method 1 - Use if you have a PoE switch or router.

Method 2 - Use if you do not have a PoE switch or router and do not have a power outlet near the location of the access point.

Method 1 - PoE with PoE Switch or Router

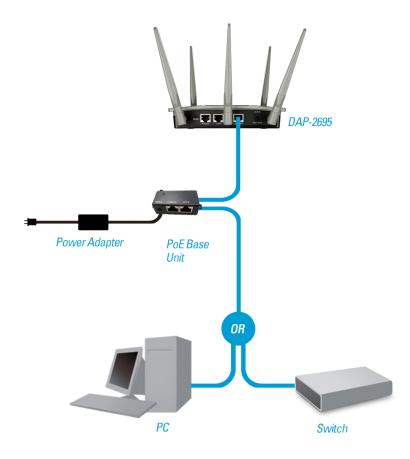
- 1. Connect one end of your Ethernet cable to the LAN1 (PoE) port on the access point.
- 2. Connect the other end into one port on a PoE switch or router.



Method 2 - PoE without PoE Switch or Router

1. Connect one end of an Ethernet cable into the **Data In** port on the PoE base unit and the other end into one port on your switch, router, or computer.

- 2. Connect one end of an Ethernet cable into the P+Data Out port on the PoE base unit and the other end into the LAN1 (PoE) port on the Access Point.
- 3. Use the supplied power adapter. Connect the power adapter to the **Power In** receptor on the PoE adapter.
- 4. Connect the power cable to the power adapter and then connect the other end into a power outlet.
- 5. Purchase separately a DPE-101GI PoE injector if you need to connect the Access Point without a PoE Switch.



Web User Interface

The DAP-2695 supports an elaborate web user interface where the user can configure and monitor the device. Launch a web browser, type the IP address of the access point (Default setting is http://192.168.0.50 or https://192.168.0.50) and then press Enter to login. Most of the configurable settings are located in the left menu of the web GUI which contains section called **Basic Settings**, **Advanced Settings** and **Status**.

D-Link [®]				DAP-2695
🔶 Home 🕺 Maintenanc	e 👻 📙 Configura	ation 👻 👙 System	💋 Logout	🕐 Help
DAP-2695 Basic Settings	System Informati	on		
Advanced Settings	Model Name Firmware Version System Name Location System Time Up Time Operation Mode(2.4GHz) Operation Mode(5GHz) MAC Address(2.4GHz) IP Address	DAP-2695 1.00 16:38:25 06/06/2013 D-Link DAP-2695 01/01/1970 20:34:51 0 Days, 20:34:52 Access Point Access Point 00:24:01:ab:c0:10 00:24:01:ab:c0:18 192:168.0.50		

Wireless

On the wireless settings page, you can setup the basic wireless configuration for the access point. The user can choose from 4 different wireless modes:

Access Point - Used to create a wireless LAN

WDS with AP - Used to connect multiple wireless networks while still functioning as a wireless access point

WDS - Used to connect multiple wireless networks

Wireless Client - Used when the access point needs to act as a wireless network adapter for an Ethernet enabled device

Access Point Mode

Wireless Band: Select either 2.4 GHz or 5 GHz from the drop-down menu.

Mode: Select Access Point from the drop-down menu.

- Network Name (SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network. The SSID can be up to 32 characters and is case-sensitive.
 - **SSID Visibility:** Select **Enable** to broadcast the SSID across the network, thus making it visible to all network users. Select **Disable** to hide the SSID from the network.

Auto Channel Selection: This feature when enabled automatically selects the channel that provides the best wireless performance. The channel selection process only occurs when the AP is booting up. To manually select a channel, set this option to Disable and select a channel from the drop-down menu.



Channel: To change the channel, first toggle the *Auto Channel Selection* setting to **Disable**, and then use the drop-down menu to make the desired selection.

Note: The wireless adapters will automatically scan and match the wireless settings.

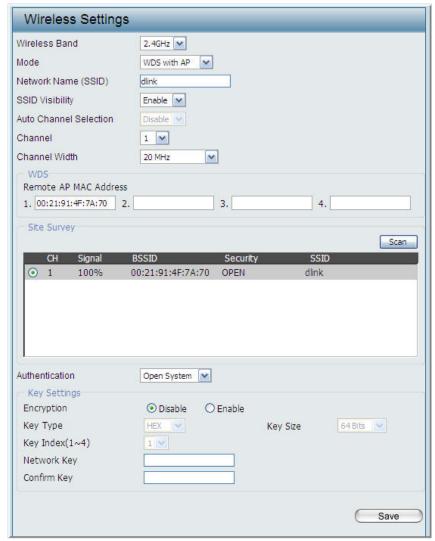
Channel Width: Allows you to select the channel width you would like to operate in. Select 20 MHz if you are not using any 802.11n wireless clients. Auto 20/40 MHz allows you to connect to both 802.11n and 802.11b/g or 802.11a wireless devices on your network.

Authentication: Use the drop-down menu to choose Open System, Shared Key, WPA-Personal, WPA-Enterprise, or 802.1x.

- Select **Open System** to communicate the key across the network (WEP).
- Select **Shared Key** to limit communication to only those devices that share the same WEP settings. If multi-SSID is enabled, this option is not available.
- Select WPA-Personal to secure your network using a password and dynamic key changes. No RADIUS server is required.
- Select **WPA-Enterprise** to secure your network with the inclusion of a RADIUS server.
- Select 802.1X if your network is using port-based Network Access Control.

WDS with AP Mode

- Wireless Band: Select either 2.4GHz or 5GHz from the drop-down menu.
 - Mode: WDS with AP mode is selected from the drop-down menu.
- Network Name (SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is dlink. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.
 - SSID Visibility: Enable or Disable SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users.
- Auto Channel Selection: Enabling this feature automatically selects the channel that will provide the best wireless performance. This feature is not supported in WDS with AP mode. The channel selection process only occurs when the AP is booting up.
 - **Channel:** All devices on the network must share the same channel. To change the channel, use the drop-down menu to make the desired selection. (Note: The wireless adapters will automatically scan and match the wireless settings.)
 - Channel Width: Allows you to select the channel width you would like to operate in. Select 20 MHz if you are not using any 802.11n wireless clients. Auto 20/40 MHz allows you to connect to both 802.11n and 802.11b/g or 802.11a wireless devices on your network.



Remote AP MAC Address: Enter the MAC addresses of the APs on your network that will serve as bridges to wirelessly connect multiple networks.

Site Survey: Click on the Scan button to search for available wireless networks, then click on the available network that you want to connect with.

Authentication: Use the drop-down menu to choose Open System, Shared Key, or WPA-Personal.

- Select Open System to communicate the key across the network.
- Select Shared Key to limit communication to only those devices that share the same WEP settings. If multi-SSID is enabled, this option is not available.
- Select WPA-Personal to secure your network using a password and dynamic key changes. No RADIUS server is required.

WDS Mode

Wireless Band: Select either 2.4GHz or 5GHz from the drop-down menu.

Mode: WDS is selected from the drop-down menu.

- Network Name (SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.
 - SSID Visibility: Enable or Disable SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users.
- Auto Channel Selection: Enabling this feature automatically selects the channel that will provide the best wireless performance. This feature is not supported in WDS mode.
 - **Channel:** All devices on the network must share the same channel. To change the channel, use the drop-down menu to make the desired selection.
 - Channel Width: Use the drop-down menu to choose 20 MHz or Auto 20/40 MHz.
- Remote AP MAC Address: Enter the MAC addresses of the APs on your network that will serve as bridges to wirelessly connect multiple networks.

Wireless Band	2.4GHz 💉	
Mode	WDS 💌	
Network Name (SSID)	dlink	
SSID Visibility	Enable 💌	
Auto Channel Selection	Disable 😒	
Channel	1 💌	
Channel Width	20 MHz	
WDS		
Remote AP MAC Addres		
1. 00:21:91:4F:7A:70	2 3	4.
CH Signal	BSSID Security	SSID dlink
○ 1 100%	00:21:91:4F:7A:70 OPEN	dink
O 1 100%		550000000 V
O 1 100%	00:21:91:4F:7A:70 OPEN	Second
O 1 100% Authentication Key Settings	00:21:91:4F:7A:70 OPEN Open System 💌 Open Sisable O Enable	Second
O 1 100% Authentication Key Settings Encryption	00:21:91:4F:7A:70 OPEN Open System 💌 Open Sisable O Enable	dink
O 1 100% Authentication Key Settings Encryption Key Type	00:21:91:4F:7A:70 OPEN Open System 💌 Open Signable O Enable HEX V K	dink
O 1 100% Authentication Key Settings Encryption Key Type Key Index(1~4)	00:21:91:4F:7A:70 OPEN Open System 💌 Open Signable O Enable HEX V K	dink
O 1 100% Authentication Key Settings Encryption Key Type Key Index(1~4) Network Key	00:21:91:4F:7A:70 OPEN Open System 💌 Open Signable O Enable HEX V K	dink

Site Survey: Click on the Scan button to search for available wireless networks, then click on the available network that you want to connect with.

Authentication: Use the drop-down menu to choose Open System, Shared Key, or WPA-Personal.

- Select Open System to communicate the key across the network.
- Select Shared Key to limit communication to only those devices that share the same WEP settings.
- Select WPA-Personal to secure your network using a password and dynamic key changes. No RADIUS server is required.

Wireless Client Mode

Wireless Band: Select either 2.4 GHz or 5 GHz from the drop-down menu.

Mode: Wireless Client is selected from the drop-down menu.

Network Name (SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is dlink. The SSID can be easily changed to connect to an existing wireless network.

SSID Visibility: This option is unavailable in Wireless Client mode.

- Auto Channel Selection: Enabling this feature automatically selects the channel that will provide the best wireless performance. This feature is not supported in Wireless Client mode.
 - **Channel:** The channel used will be displayed, and matches the AP that the DAP-2695 is connected to when set to Wireless Client mode.
 - Channel Width: Use the drop-down menu to choose 20 MHz or Auto 20/40 MHz.
 - Site Survey: Click on the Scan button to search for available wireless networks, then click on the available network that you want to connect with.

Authentication: Will be explained in the next topic.

Wireless Setting	js			
Wireless Band	2.4GHz 💌			
Mode	Wireless Client 💌			
Network Name (SSID)	dlink			
SSID Visibility	Enable 😒			
Auto Channel Selection	Enable 🔽			
Channel	1 💌			
Channel Width	Auto 20/40 MHz 💌			
Site Survey				
	A. 6 (2017)	14		an
CH Signal	BSSID	Security	/ SSID	
0 1 78%	00:21:91:84:DD:69	WEP	DAP-1522	<u>^</u>
0 1 100%	00:18:02:6D:B2:E0	OPEN	kay2553	=
O 1 100%	00:21:91:4F:7A:70	OPEN	dlink	
0 1 62%	00:22:80:F8:4F:FF	OPEN	6666-P	
O 2 64%	00:05:5D:35:20:64	OPEN	dlink	
0 2 78%	00:18:84:A5:23:3D	OPEN	FON_Kay	~
Authentication	Open System 💌			
Key Settings				
Encryption	Disable	Enable		
Кеу Туре	HEX 👽		Key Size 64 Bits 🔽	
Key Index(1~4)	1 👻			
Network Key				
Confirm Key				
	1			
Wireless MAC Clone				
Enable				
MAC Source	Auto 💌			
MAC Address		:	: Scan	
	MAC Address		1000 - 10	

Wireless Security

Wireless security is a key concern for any wireless network installed. Unlike any other networking method wireless networks will broadcast it's presence for anyone to connect to it. Today, wireless security has advanced to a level where it is virtually impenetrable.

There are mainly two forms of wireless encryption and they are called Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP was the first security method developed. It is a low level encryption but better than now encryption. WPA is the newest encryption standard and with the advanced WPA2 standard wireless networks have finally reach a point where the security is strong enough to give users the peace of mind when installing wireless networks.

Wired Equivalent Privacy (WEP)

WEP provides two variations called Open System and Shared Key.

Open System will send a request to the access point and if the key used matches the one configured on the access point, the access point will return a success message back to the wireless client. If the key does not match the one configured on the access point, the access point will deny the connection request from the wireless client.

Shared Key will send a request to the access point and if the key used matches the one configured on the access point, the access point will send a challenge to the client. The client will then again send a confirmation of the same key back to the access point where the access point will either return a successful or a denial packet back to the wireless client.

- **Encryption:** Use the radio button to disable or enable encryption.
- Key Type*: Select HEX or ASCII.
- Key Size: Select 64 Bits or 128 Bits.
- Key Index (1-4): Select the 1st through the 4th key to be the active key.
 - Key: Input up to four keys for encryption. You will select one of these keys in the Key Index drop-down menu.

**Hexadecimal (HEX) digits consist of the numbers 0-9 and the letters A-F.

*ASCII (American Standard Code for Information Interchange) is a code that represents English letters using numbers ranging from 0-127.

Wireless Band	2.4GHz 💌		
Mode	Access Point		
Network Name (SSID)	dlink		
SSID Visibility	Enable 💌		
Auto Channel Selection	Disable 💉		
Channel	1 💌		
Channel Width	20 MHz 💉		
Authentication	Open System		
Key Settings			
Encryption	🔿 Disable 🛛 💿 Enable		
Кеу Туре	HEX M	Key Size	64 Bits 💌
Key Index(1~4)	1 💌		
Network Key	•••••		
Confirm Key	•••••		

Wi-Fi Protected Access (WPA / WPA2)

WPA was created by the Wi-Fi Alliance to address the limitations and weaknesses found in WEP. This protocol is mainly based on the 802.11i standard. There are also two variations found in WPA called WPA-Personal (PSK) and WPA-Enterprise (EAP).

WPA-EAP requires the user to install a Radius Server on the network for authentication. WPA-Personal does not require the user to install a Radius Server on the network.

Comparing WPA-PSK with WPA-EAP, WPA-PSK is seen as a weaker authentication but comparing WPA-PSK to WEP, WPA-PSK is far more secure than WEP. WPA-EAP is the highest level of wireless security a user can use for wireless today.

WPA2 is an upgrade of WPA. WPA2 yet again solves some possible security issues found in WPA. WPA2 has two variations called WPA2-Personal (PSK) and WPA2-Enterprise (EAP) which is the same as found with WPA.

- WPA Mode: When WPA-Personal is selected for Authentication type, you must also select a WPA mode from the drop-down menu: AUTO (WPA or WPA2), WPA2 Only, or WPA Only. WPA and WPA2 use different algorithms. AUTO (WPA or WPA2) allows you to use both WPA and WPA2.
- **Cipher Type:** When you select WPA-Personal, you must also select AUTO, AES, or TKIP from the pull down menu.
- **Group Key Update:** Select the interval during which the group key will be valid. The default value of 1800 is recommended.
 - Pass Phrase: When you select WPA-Personal, please enter a Pass Phrase in the corresponding field.

Vireless Band	2.4GHz 💌
lode	Access Point
Network Name (SSID)	dlink
SSID Visibility	Enable 💌
Auto Channel Selection	Disable 💌
Channel	1 💌
Channel Width	20 MHz
Authentication	WPA-Personal
PassPhrase Settings	
WPA Mode	AUTO (WPA or WPA2)
Cipher Type	Auto 🗹 Group Key Update Interval 1800 (Seconds)
Manual	O Periodical Key Change
Activated From	Sun 💙 : 00 💙 : 00 💙
Time Interval	(1~168)hour(s)
PassPhrase	•••••
Confirm PassPhrase	•••••

- WPA Mode: When WPA-Enterprise is selected, you must also select a WPA mode from the drop-down menu: AUTO (WPA or WPA2), WPA2 Only, or WPA Only. WPA and WPA2 use different algorithms. AUTO (WPA or WPA2) allows you to use both WPA and WPA2.
- **Cipher Type:** When WPA-Enterprise is selected, you must also select a cipher type from the drop-down menu: Auto, AES, or TKIP.
- Group Key Update Interval: Select the interval during which the group key will be valid. 1800 is the recommended value as a lower interval may reduce data transfer rates.

Network Access Protection: Enable or disable Microsoft Network Access Protection.

RADIUS Server: Enter the IP address of the RADIUS server.

RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the RADIUS secret.

Wireless Settings	
Wireless Band	2.4GHz 💌
Mode	Access Point
Network Name (SSID)	dlink
SSID Visibility	Enable 💌
Auto Channel Selection	Disable 💌
Channel	1 💌
Channel Width	20 MHz
Authentication	WPA-Enterprise 💌
RADIUS Server Settings	
WPA Mode	AUTO (WPA or WPA2)
Cipher Type	Auto Group Key Update Interval 1800 (Seconds)
Network Access Protect	ion
Network Access Protection	⊙ Disable ○ Enable
Primary RADIUS Server	Setting
RADIUS Server	192.168.0.100 RADIUS Port 1812
RADIUS Secret	•••••
	Save

LAN

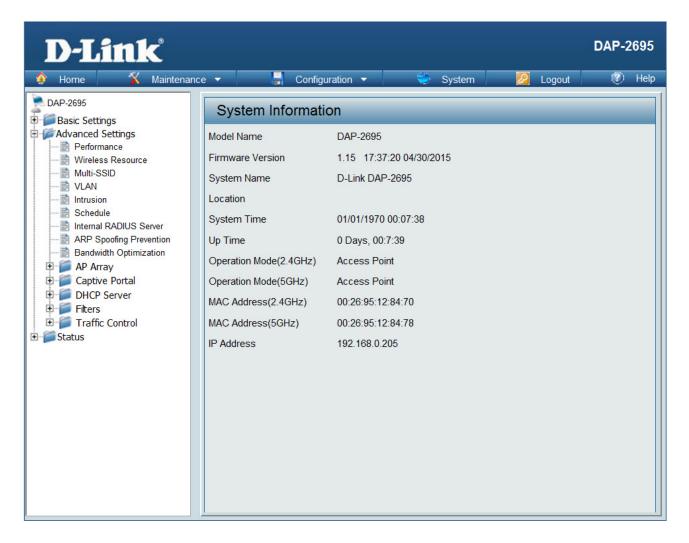
LAN is short for Local Area Network. This is considered your internal network. These are the IP settings of the LAN interface for the DAP-2695. These settings may be referred to as private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.

- Get IP From: Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2695. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.
- IP Address: The default IP address is 192.168.0.50. Assign a static IP address that is within the IP address range of your network.
- Subnet Mask: Enter the subnet mask. All devices in the network must share the same subnet mask.
- **Default Gateway:** Enter the IP address of the gateway/router in your network.
 - **DNS:** Enter a DNS server IP address. This is usually the local IP address of your gateway/router.

Home Maintenance Configuration System Logout Help DAP-2895 Basic Settings Get IP From Static IP (Manual) IP IP Address IP Address IP Address IP Address IP Address IP Address Subnet Mask 255.255.255.0 Default Gateway DNS Save	D-Link [®]				DAP-2695
	DAP-2695	LAN Settings Get IP From IP Address Subnet Mask Default Gateway	Static IP (Manual) V 192.168.0.50	Logout	Help Save

Advanced Settings

In the Advanced Settings Section the user can configure advanced settings concerning Performance, Multiple SSID, VLAN, Security, Quality of Service, AP Array, Web Redirection, DHCP Server, Filters and Scheduling. The following pages will explain settings found in the Advanced Settings section in more detail.



Performance

On the Performance Settings page the users can configure more advanced settings concerning the wireless signal and hosting.

Wireless Band: Select either 2.4GHz or 5GHz.

Wireless: Use the drop-down menu to turn the wireless function On or Off.

Wireless Mode: The different combination of clients that can be supported include Mixed 802.11n, 802.11g and 802.11b, Mixed 802.11g and 802.11b and 802.11n Only in the 2.4 GHz band and Mixed 802.11n, 802.11a, 802.11a only, and 802.11n Only in the 5 GHz band. Please note that when backwards compatibility is enabled for legacy (802.11a/g/b) clients, degradation of 802.11n wireless performance is expected.

Data Rate*: LAN. The AP will adjust the base transfer rate depending on the base rate of the connected device. If there are obstacles or interference, the AP will step down the rate. This option is enabled in Mixed 802.11g and 802.11b mode (for 2.4 GHz) and 802.11a only mode (for 5 GHz). The choices available are Best (Up to 54), 54, 48, 36, 24, 18, 12, 9, 6 for 5 GHz and Best (Up to 54), 54, 48, 36, 24, 18, 12, 9, 6, 11, 5.5, 2 or 1 for 2.4 GHz.

Beacon Interval (25-500): Beacons are packets sent by an access point to synchronize a wireless network. Specify a value in milliseconds. The default (100) is recommended. Setting a higher beacon interval can help to save the power of wireless clients, while setting a lower one can help a wireless client connect to an access point faster.

DTM Interval (1-15): Select a Delivery Traffic Indication Message setting between 1 and 15. 1 is the default setting. DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

Wireless band	5GHz 👻
Wireless	On 👻
Wireless Mode	Mixed 802.11ac 👻
Data Rate	Best(Up to 1300) 👻 (Mbps)
Beacon Interval (40-500)	100
DTIM Interval (1-15)	1
Transmit Power	100% 🔻
WMM (Wi-Fi Multimedia)	Enable 👻
Ack Time Out (5GHz, 25~200)	25 (µs)
Short GI	Enable 👻
IGMP Snooping	Disable 👻
Multicast Rate	Disable 🔻 (Mbps)
Multicast Bandwidth Control	Disable 👻
Maximum Multicast Bandwidth	100 kbps
HT20/40 Coexistence	Disable 👻
Transfer DHCP Offer to Unicast	Disable 👻

Wireless: Use the drop-down

- **Transmit Power:** This setting determines the power level of the wireless transmission. Transmitting power can be adjusted to eliminate overlapping of wireless area coverage between two access points where interference is a major concern. For example, if wireless coverage is intended for half of the area, then select 50% as the option. Use the drop-down menu to select 100%, 50%, 25%, or 12.5%.
- WMM (Wi-Fi Multimedia): WMM stands for Wi-Fi Multimedia. Enabling this feature will improve the user experience for audio and video applications over a Wi-Fi network.

Ack Time Out To effectively optimize throughput over long distance links enter a value for Acknowledgement Time Out between 25 and 200 (2.4 GHZ, 64~200): microseconds for 5 GHz or from 64 to 200 microseconds in the 2.4 GHz in the field provided.

- Short GI: Select Enable or Disable. Enabling a short guard interval can increase throughput. However, be aware that it can also increase the error rate in some installations due to increased sensitivity to radio-frequency installations.
- IGMP Snooping: Select Enable or Disable. Internet Group Management Protocol allows the AP to recognize IGMP queries and reports sent between routers and an IGMP host (wireless STA). When IGMP snooping is enabled, the AP will forward multicast packets to an IGMP host based on IGMP messages passing through the AP.

Multicast Rate : Select the multicast rate for 2.4GHz and 5GHz band.

- Maximum Multicast Set the multicast packets maximum bandwidth pass through rate from the Ethernet interface to the Access Point. Bandwidth :
- Multicast Bandwidth Adjust the multicast packet data rate here. The multicast rate is supported in AP mode, (2.4 GHZ and 5 GHZ) and WDS Control: with AP mode, including Multi-SSIDs.
- HT20/40 Coexistence : Enable this option to reduce interference from other wireless networks in your area. If the channel width is operating at 40MHz and there is another wireless network's channel over-lapping and causing interference, the Access Point will automatically change to 20MHz.
- Transfer DHCP Offer to Enable to transfer the DHCP Offer to Unicast from LAN to WLAN, suggest to enable this function if stations number is larger than 30. Unicast :

Wireless Resource Control

The Wireless Resource Control window is used to configure the wireless connection settings so that the device can detect the better wireless connection in your environment.

Wireless band: Select 2.4GHz or 5GHz.

- **Band Steering:** Use the drop-down menu to **Enable** the Band Steering function. When the wireless clients support both 2.4GHz and 5GHz and the 2.4GHz signal is not strong enough, the device will use 5GHz as higher priority.
- **Band Steering Age:** Enter the time in seconds to specify the interval of updating information.
- Band Steering Diff: The Band Steering difference value is equal to the number of 5GHz wireless client connections minus the number of 2.4GHz wireless client connections. If the number of 5GHz wireless client connections minus the number of 2.4GHz wireless client connections exceed this value, the extra 5GHz wireless client connections will be forced to connect to the 2.4GHz band and not the 5GHz band.



Band SteeringEnter the maximum 5GHz connection attempts allowed before the 5GHz preferred function will be disabled for the wire-Refuse Num:less station connection.

Connection Limit: Select **Enable** or **Disable**. This is an option for load balancing. This determines whether to limit the number of users accessing this device. The exact number is entered in the User Limit field below. This feature allows the user to share the wireless network traffic and the client using multiple APs. If this function is enabled and when the number of users exceeds this value, or the network utilization of this AP exceeds the percentage that has been specified, the DAP-2695 will not allow clients to associate with the AP.

Section 3 - Configuration

User Limit: Set the maximum amount of users that are allowed access (zero to 64 users) to the device using the specified wireless band. The default setting is 20.

11n Preferred: Use the drop-down menu to **Enable** the 11n Preferred function. The wireless clients with 802.11n protocol will have higher priority to connect to the device.

- Network Utilization: Set the maximum utilization of this access point for service. The DAP-2695 will not allow any new clients to associate with the AP if the utilization exceeds the value the user specifies. Select a utilization percentage between 100%, 80%, 60%, 40%, 20%, or 0%. When this network utilization threshold is reached, the device will pause one minute to allow network congestion to dissipate.
 - Aging out: Use the drop-down menu to select the criteria of disconnecting the wireless clients. Available options are **RSSI** and **Data Rate**.
 - **RSSI Threshold:** When **RSSI** is selected in the **Aging out** drop-down menu, select the percentage of RSSI here. When the RSSI of wireless clients is lower than the specified percentage, the device disconnects the wireless clients.
- **Data Rate Threshold:** When **Data Rate** is selected in the **Aging out** drop-down menu, select the threshold of data rate here. When the data rate of wireless clients is lower than the specified number, the device disconnects the wireless clients.
 - ACL RSSI: Use the drop-down menu to **Enable** the function. When enabled, the device denies the connection request from the wireless clients with the RSSI lower than the specified threshold below.
- ACL RSSI Threshold: Set the ACL RSSI Threshold.

Multi-SSID

The device supports up to four multiple Service Set Identifiers. You can set the Primary SSID in the Basic > Wireless section. The SSID's factory default setting is dlink. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

Enable Multi-SSID: Check to enable support for multiple SSIDs.

Band: Select 2.4GHz or 5GHz.

- Index: You can select up to three multi-SSIDs. With the Primary SSID, you have a total of four multi-SSIDs.
- **SSID:** Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.
- **SSID Visibility:** Enable or Disable SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users.

Security: The Multi-SSID security can be Open System, WPA-Personal, or WPA-Enterprise. For a detailed description of the Open System parameters please go to page 23. For a detailed description of the WPA-Personal



parameters please go to page 24. For a detailed description of the WPA-Enterprise parameters please go to page 25.

Priority: Select the priority level of the SSID selected.

WMM (Wi-Fi WMM stands for Wi-Fi Multimedia. Enabling this feature will improve the user experience for audio and video applications over a Wi-Fi Multimedia): network.

Encryption: When you select Open System, toggle between Enable and Disable. If Enable is selected, the Key Type, Key Size, Key Index (1~4), Key, and Confirm Keys must also be configured.

Key Type: Select HEX or ASCII.

Key Size: Select 64-bit or 128-bit.

Key Index (1-4): Select from the 1st to 4th key to be set as the active key.

Key: Input up to four keys for encryption. You will select one of these keys in the Key Index drop-down menu.

WPA Mode: When you select either WPA-Personal or WPA-Enterprise, you must also choose a WPA mode from the drop-down menu: AUTO (WPA or WPA2), WPA2 Only, or WPA Only. WPA and WPA2 use different algorithms. AUTO (WPA or WPA2) allows you to use both WPA and WPA2. In addition, you must configure Cipher Type, and Group Key Update Interval.

Cipher Type: Select Auto, AES, or TKIP from the drop-down menu.

Group Key Update Interval: Select the interval during which the group key will be valid. The default value of 1800 seconds is recommended.

Pass Phrase: When you select WPA-Personal, please enter a Pass Phrase in the corresponding field.

Confirm Pass Phrase: When you select WPA-Personal, please re-enter the Pass Phrase entered in the previous item in the corresponding field.

RADIUS Server: When you select WPA-Enterprise, enter the IP address of the RADIUS server. In addition, you must configure RADIUS Port and RADIUS Secret.

RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the RADIUS secret.

VLAN

VLAN List

The DAP-2695 supports VLANs. VLANs can be created with a Name and VID. Mgmt (TCP stack), LAN, Primary/Multiple SSID, and WDS connection can be assigned to VLANs as they are physical ports. Any packet which enters the DAP-2695 without a VLAN tag will have a VLAN tag inserted with a PVID. The VLAN List tab displays the current VLANs.

VLAN Status: Use the radio button to toggle to Enable. Next, go to the Add/Edit VLAN tab to add or modify an item on the VLAN List tab.

VLAN Mode: The current VLAN mode is displayed.

🔅 Home 🔏 Maintena	nce 🔻 🔚	Configuration 🔻	💝 System	n 💋 Logout	🕐 He
DAP-2895	VLAN Settin	gs			
Advanced Settings	VLAN Status : VLAN Mode : S	Disable C Enabl tatic(2.4G), Static(5G)	le	Save	
- Multi-SSID	VLAN List	Port List Add/	Edit VLAN	PVID Setting	
Voral Internation Schedule Internal RADIUS Server ARP Spoofing Prevention Bandwidth Optimization AP Array Oraptive Portal DHCP Server Filters Filters Traffic Control Status	VID VLAN Nai	Mgmt, Li Primary(5-2(2,4G), 5 (2,4G), 5 (2,4G), V (2,4G), V (2,4G), V (2,4G), V (2,4G), V (5,4G), 5- (5G), 5- (5G), 5- VV-2(5G) (5G), 5-	AN Ports ANI, LAN2, 2.46), 5-1(2.46), 1), 5-3(2.46), 5-4 5-7(2.46), W-1 Y-2(2.46), W-3 V-4(2.46), W-3 V-4(2.46), W-5 V-4(2.46), W-5 V-4(2.46), M-5 V-4(2.46), M-5 V-4(2.46), M-5 V-4(2.46), M-5 V-4(2.46), M-5 V-4(2.46), M-4 V-4(2.46), M-5 V-4(2.46), M-4 V-4(2.46), M-4 V-4(2.46)	3	Edit Delete

Port List

The Port List tab displays the current ports. If you want to configure the guest and internal networks on a Virtual LAN (VLAN), the switch and DHCP server you are using must also support VLANs. As a prerequisite step, configure a port on the switch for handling VLAN tagged packets as described in the IEEE 802.1Q standard.

- VLAN Status: Use the radio button to toggle to Enable. Next, go to the Add/Edit VLAN tab to add or modify an item on the VLAN List tab.
 - **Port Name:** The name of the port is displayed in this column.

Tag VID: The Tagged VID is displayed in this column.

- Untag VID: The Untagged VID is displayed in this column.
 - **PVID:** The Port VLAN Identifier is displayed in this column.

VLAN Statu:	s : ODisable	💿 Enable 🔚 Si	ave	
VLAN Mode	: Static			
VLAN List	Port List	Add/Edit VLAN	PVID Setting	
Port Name	Tag VII)	Untag VID	PVID
Mgmt			1	1
LAN			1	1
dlink			1	1
dlink1			1	1
dlink2			1	1
dlink3			1	1
W-1			1	1
W-2			1	1
W-3			1	1
W-4			1	1

Add/Edit VLAN

The Add/Edit VLAN tab is used to configure VLANs. Once you have made the desired changes, click the Save button to let your changes take effect.

- VLAN Status: Use the radio button to toggle to Enable.
 - VLAN ID: Provide a number between 1 and 4094 for the Internal VLAN.
- **VLAN Name:** Enter the VLAN to add or modify.

LAN List Por	t List	Add/Edit	VLAN		PVID Sett	ing	
VLAN ID (VID)	1	VLAN Na	me lī	lefault		_	
Port	Select All	Mgmt	LAN			3	
Untag	All	۲	0				
Tag	All	0	0				
Not Member	All	0	0				
MSSID Port	Select All	Primary	S-1	S-2	S-3		
Untag	All	۲	۲	۲	•		
Tag	All	0	0	0	0		
Not Member	All	\bigcirc	0	0	0		
WDS Port	Select All	W-1	W-2	W-3	W-4		
Untag	All	۲	0	0	۲		
Tag	All	0	0	0	0		
Not Member	All	0	0	0	0		

PVID Settings

The PVID Setting tab is used to enable/disable the Port VLAN Identifier Auto Assign Status as well as to configure various types of PVID settings. Click the Save button to let your changes take effect.

VLAN Status:	Use the radio button to toggle between Enable and Disable.
PVID Auto Assign Status:	Use the radio button to toggle PVID auto assign status to Enable.

VLAN Se	ttings					
VLAN Status VLAN Mode	: ODisable Static	Enable	Sav	•		
VLAN List	Port List	Add/Edit V	IAN	PVID Setting		
		⊙ Disable	OEnable	9		
Port PVID	Mgmt L	AN	-			
MSSID Por PVID	t Primary S	5-1 S-2	S-3 1	_	-	-
WDS Port PVID	W-1 V 1 1	V-2 W-3	W-4	_	-	-
					C	Save

Intrusion

The Wireless Intrusion Protection window is used to set APs as All, Valid, Neighborhood, Rogue, and New. Click the Save button to let your changes take effect.

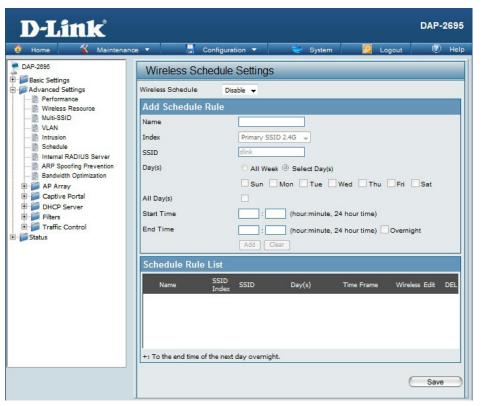
- Wireless Band: Select 2.4GHz or 5GHz.
 - AP List: The choices include All, Valid, Neighbor, Rogue, and New.
 - **Detect:** Click this button to initiate a scan of the network.



Schedule

The Wireless Schedule Settings window is used to add and modify scheduling rules on the device. Click the Save button to let your changes take effect.

- Wireless Schedule: Use the drop-down menu to enable the device's scheduling feature.
 - Name: Enter a name for the new scheduling rule in the field provided.
 - Index: Use the drop-down menu to select the desired SSID.
 - SSID: This read-only field indicates the current SSID in use. To create a new SSID, go to the Wireless Settings window (Basic Settings > Wireless).
 - **Day(s):** Toggle the radio button between All Week and Select Day(s). If the second option is selected, check the specific days you want the rule to be effective on.
 - All Day(s): Check this box to have your settings apply 24 hours a day.
 - Start Time: Enter the beginning hour and minute, using a 24-hour clock.
 - End Time: Enter the ending hour and minute, using a 24-hour clock.



Internal RADIUS Server

The DAP-2695 features a built-in RADIUS server. Once you have finished adding a RADIUS account, click the Save button to let your changes take effect. The newly-created account will appear in this RADIUS Account List. The radio buttons allow the user to enable or disable the RADIUS account. Click the icon in the delete column to remove the RADIUS account. We suggest you limit the number of accounts below 30.

User Name: Enter a name to authenticate user access to the **D-Link** DAP-2695 internal RADIUS server. 🕺 Maintenance 🔻 - Configuration -Help Password: Enter a password to authenticate user access to the DAP-2695 Internal RADIUS Server Basic Settings internal RADIUS server. The length of your password Advanced Settings Add RADIUS Account Performance should be 8~64. Wireless Resource User Name Multi-SSID Password - D VLAN - 📄 Intrusion Status Enable 🚽 Status: Toggle the drop-down menu between Enable and Schedule Internal RADIUS Server Disable. - ARP Spoofing Prevention User Name Bandwidth Optimization E AP Array E Captive Portal **RADIUS Account List:** Displays the list of users. DHCP Server E Filters E Traffic Control Status

Save

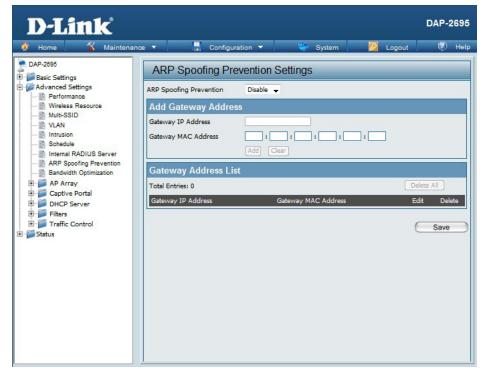
ARP Spoofing Prevention

The ARP Spoofing Prevention feature allows users to add IP/MAC address mapping to prevent arp spoofing attack.

ARP Spoofing Prevention: This check box allows you to enable the arp spoofing prevention function.

Gateway IP Address: Enter a gateway IP address.

Gateway MAC Address: Enter a gateway MAC address.



Bandwidth Optimization

The Bandwidth Optimization window allows the user to manage the bandwidth of the device and arrange the bandwidth for various wireless clients. When the Bandwidth Optimization rule is finished, click the **Add** button. To discard the Add Bandwidth Optimization Rule settings, click the **Clear** button. Click the **Save** button to let your changes take effect.

Enable Bandwidth	•	Bandwidth Optimization		
Optimization:	Optimization function.	Enable Bandwidth Optimization	Enable 💌	
Downlink Bandwidth:	Enter the downlink bandwidth of the device in	Downlink Bandwidth	80 Mbits/sec	
	Mbits per second.	Uplink Bandwidth	80 Mbits/sec	
Uplink Bandwidth:	Enter the uplink bandwidth of the device in Mbits	Add Bandwidth O	ptimization Rule	
	per second.	Rule Type	Allocate average BW for each station	
Allocato avorado PM/	AD will distribute average bandwidth for each	Band	2.4 GHz 💌	
Allocate average BW for each station:	AP will distribute average bandwidth for each client.	SSID Index	Primary SSID V	
		Downlink Speed	Kbits/sec 💟	
Allocate maximum BW	Specify the maximum bandwidth for each connected client. Reserve certain bandwidth for future clients.	Uplink Speed	Add Clear	
for each station:		Bandwidth Optimi		
			CCID	
	The weight of 11b/g/n and 11a/n client are 10%/20%/70% ; 20%/80%. AP will distribute different bandwidth for 11a/b/g/n clients.	Band Type	Index Downlink Speed Uplink Speed Edit Del	
for a/b/g/n stations:				
Allocate specific BW	All clients share the total bandwidth.			
for SSID:				
Rule Type:	Use the drop-down menu to select the type			
	that is applied to the rule. Available options are:			
	Allocate average BW for each station, Allocate maximum BW for each station, Allocate			
	different BW for 1a/b/g/n stations, and Allocte			
	specific BW for SSID.	1		
			Save	

Section 3 - Configuration

Band: Use the drop-down menu to toggle the wireless band between 2.4GHz and 5GHz.

- SSID Index: Use the drop-down menu to select the SSID for the specified wireless band.
- **Downlink Speed:** Enter the limitation of the downloading speed in either Kbits/sec or Mbits/sec for the rule.
 - Uplink Speed: Enter the limitation of the uploading speed in either Kbits/sec or Mbits/sec for the rule.

AP Array

AP Array Scan

The AP Array window is used to create up to 32 APs on a local network to be organized into a single group in order to increase ease of management. Click the **Save** button to let your changes take effect. Central WiFiManager and AP Array are mutually exclusive functions.

Enable AP Array:	Select the check box to enable the AP array function. The three modes that are available are Master , Backup Master , and Slave . APs in the	D-Link Home 🖇 Maintena	DAP-2660 Ince 👻 📓 Configuration 👻 🤯 System 🛛 🖉 Logout 🛞 Help
	same array will use the same configuration. The configuration will sync the Master AP to the Slave	DAP-2660	AP Array Scan
	AP and the Backup Master AP when a Slave AP and a Backup Master AP join the AP array.	Wireless Resource Wireless Resource Mult-SSD VLAN Intrusion	Master Backup Master Slave AP Array Name AP Array Password
AP Array Name:	Enter an AP array name for the group here.		Scan AP Array List Scan Connection Status Disconnect AP Array List
AP Array Password:	Enter an AP array password for the group here. This password must be the same on all the APs in the group.	AP Array AP Array AP Array AP Array Scan Configuration Settings Auto-RF Auto-RF Captive Portal Grive Portal Grive Portal Grive Filters	Array Name Master IP MAC Master Backup Slave Total Master Slave Total
Scan AP Array List:	Click this button to initiate a scan of all the available APs currently on the network.	Traffic Control Status Status	Current Members Index Role IP Address MAC Address Location
Connection Status:	Display the AP array connection status.	Ethernet WLAN	
AP Array List:	This table displays the current AP array status for the following parameters: Array Name, Master IP, MAC, Master, Backup Master, Slave, and Total.		Save
Current Members:	This table displays all the current array members. The DAP-2660 AP array feature supports up to eight AP array members.		

Configuration Settings

In the AP array configuration settings windows, users can specify which settings all the APs in the group will inherit from the master AP. Make the required selection in this window and click the **Save** button to accept the changes made.

Enable AP Array Configuration:	, 5	AP Array Configuration
		Enable AP Array Configuration
Wireless Basic Settings:		Clear all
5	5 5 1	Wireless Basic Settings
Wireless Advanced Settings:	settings that the APs in the group will inherit.	Wireless Advanced Settings
5		Multiple SSID & VLAN
Multiple SSID & VLAN:	Select this option to specify the multiple SSIDs and VLAN settings that the APs in the group will inherit.	Advanced Functions
		Administration Settings
Advanced Functions:	Select this option to specify the other advanced settings that the APs in the group will inherit.	Save
Administration Settings:	Select this option to specify the administrative settings that the APs in the group will inherit.	

Section 3 - Configuration

SSID Visibility: Select this option to enable SSID visibility.

Auto Channel Selection: Select this option to use auto channel selection.

Channel Width: Select this option to use the same channel width.

Security: Select this option to use the same wireless security.

Captive Profile: Select this option to use the same captive profile settings.

Band: Select this option to use the same wireless band.

Wireless Advanced Settings

Wireless: Select this option to use the same wireless settings.

Wireless Mode: Select this option to use the same wireless mode.

Data Rate: Select this option to use the same data rate.

Beacon Interval: Select this option to use the same beacon interval.

DTIM Interval: Select this option to use the same DTIM interval.

Transmit Power: Select this option to use the same transmit power.

WMM (Wi-Fi Select this option to use the same WMM settings. Multimedia):

Ack Time Out: Select this option to use the same ACK timeout value.

Wireless ACL: Select this option to use the same wireless ACL settings.

Wireless Basic Settings

Wireless Basic Setting	is 🗹		
Network Name (SSID)		SSID Visibility	
Auto Channel Selection		Channel Width	
Security		Captive Profile	
Band			

Wireless Advanced Set	tings 🗹		
Wireless		Wireless Mode	
Data Rate		Beacon Interval	
DTIM Interval		Transmit Power	
WMM (Wi-Fi Multimedia)		Ack Time Out	
Wireless ACL		Short GI	
Link Integrity		Connection Limit	V
IGMP Snooping			

Short GI: Select this option to use the same short GI settings.

Link Integrity: Select this option to use the same link integrity settings.

Connection Limit: Select this option to use the same connection limit value.

IGMP Snooping:: Select this option to use the same IGMP snooping settings.

Multiple SSID & VLAN

SSID: Select this option to use the same multi-SSIDs.

SSID Visibility: Select this option to use the same SSID visible.

Security: Select this option to use the same wireless security settings.

WMM: Select this option to use the same WMM settings.

Captive Profile: Select this option to use the same captive profile settings.

VLAN: Select this option to use the same VLAN settings.

Advanced Functions

Schedule Settings:	Select this	option t	to use	the	same	schedule
	settings.					

QoS Settings: Select this option to use the same Quality of Service settings.

Log Settings: Select this option to use the same log settings.

Time and Date Settings: Select this option to use the same time and date settings.

Advanced Functions 🛛	2		
Schedule Settings		QoS Settings	
Log Settings		Time and Date Settings	
ARP Spoofing Prevention		Bandwidth Optimization	
Captive Portal		Auto RF	
Load Balance		DHCP server Settings	

Multiple SSID & VLA	AN 🗹		
SSID		SSID Visibility	
Security		WMM	
Captive Profile		VLAN	

ARP Spoofing Select this option to use the same ARP spoofing prevention settings. **Prevention:**

Bandwidth Select this option to use the same bandwidth optimization settings. **Optimization:**

Captive Portal: Select this option to use the same captive portal settings.

Auto RF: Select this option to use the same auto-RF settings.

Load Balance: Select this option to use the same load balancing settings.

DHCP Server Settings: Select this option to use the same DHCP server settings.

Administration Settings

System Name Settings: Select this option to use the same system name. SNMP Settings: Select this option to use the same SNMP settings. Login Settings: Select this option to use the same login settings.

Console Settings: Select this option to use the same console settings.

Limit Administrator: Select this option to use the same limit administrator settings.

Ping Control Setting: Select this option to use the same ping control settings.

Administration Setting	s 🗹		
System Name Settings		SNMP Settings	
Login Settings		Console Settings	
Limit Administrator		Ping Control Setting	

Auto-RF

In this windows, users can view and configure the automatic radio frequency settings as well as configure the the auto-initiate period and threshold values. Click the **Save** button to accept the changes made.

Enable: Auto-RF:	Select to Enable or Disable the auto-RF feature here.	Auto-RF		
	here.	Enable Auto-RF	Disable 🖌	
Initiate Auto-RF:	Click the Auto-RF Optimize button to initiate the	Initiate Auto-RF	Auto-RF Optimize	
	auto-RF optimization feature.	Auto-Initiate	Disable 💉	
Auto-Initiate:	Select the Enable or Disable the auto-initiate	Auto-Initiate Period	24 (hours)	
Auto-Initiate:	feature here.	RSSI Threshold	40%	
		RF Report Frequency	10 (Seconds)	
Auto-Initiate Period:	After enabling the auto-initiate option, the auto- initiate period value can be entered here. This value must be between 1 and 24 hours.		Save	
RSSI Threshold:	Select the RSSI threshold value here. This value is listed in the drop-down menu in increments of 10% from 10% to 100% .			
RF Report Frequency:	Enter the RF report frequency value here.			

Load Balance

In this window, users can view and configure the AP array's load balancing settings. Click the Save button to accept the changes made.

Enable Load Balance:	Select to Enable or Disable the load balance feature here.	E Load Balance		
		Enable Load Balance	Disable 💌	
Active Threshold:	Enter the active threshold value here.	Active Threshold	0	
			Save	

Captive Portal

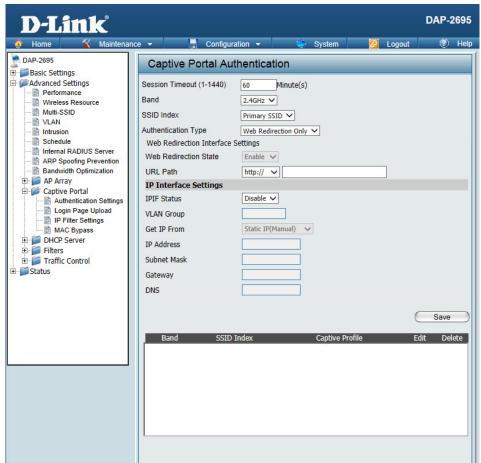
Authentication Settings-Web Redirection Only

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, user can view and configure the Captive Portal settings. After selecting Web Redirection Only as the Authentication Type, we can configure the redirection website URL that will be applied to each wireless client in this network.

	Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.	D-Link Home Maintenan	DAP-2695 ice - 📑 Configuration - 🛸 System 😥 Logout 🔅 Help		
	value is of minutes.	DAP-2695	Captive Portal Authentication		
Band :	Select 2.4GHz or 5GHz.	Settings Advanced Settings Setformance Wireless Resource	Session Timeout (1-1440) 60 Minute(s) Band 2.4GHz		
SSID Index :	Select the SSID for this Authentication.	Multi-SSID VLAN Intrusion	SSID Index Primary SSID Authentication Type Web Redirection Only Web Redirection Interface Settings		
Authentication Type :	Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the Web Redirection option.	Internal RADIUS Server ARP Spoofing Prevention Bandwidth Optimization Gandwidth Optimization Ar Array Captive Portal Authentication Settings Login Page Upload If Filter Settings MAC Bypass MAC Bypass DHCP Server Elters	ARP Spoofing Prevention AP Array Captive Portal Advantantication Settings Difference Portal Authentication Settings Difference Settings MAC Bypass	ARP Spoofing Prevention Web Redirection State Enable On, Bandwidth Optimization URL Path http:// Ote Authentication Settings IP Interface Settings /e'll Join Page Upload VLAN Group IP Filter Settings Get IP From Static IP ACP Server IP Address IP Address	Web Redirection State Enable URL Path http:// ~ IP Interface Settings IPIF Status Disable ~ VLAN Group Get IP From Static IP(Manual) ~
Web Redirection State :	Default setting is Enable when select Web Redirection Only.	⊕ 📁 Traffic Control ⊕ 📁 Status	Subnet Mask Gateway DNS		
URL Path :	Select whether to use either HTTP or HTTPS here. After selecting either http:// or https://, enter the URL of the website that will be used in the space provided.		Save Save Save Save Save Save Save Save		
IPIF Status :	Select to Enable or Disable the Captive Portal with its IP interface feature here.				
VLAN Group :	Enter the VLAN Group ID here.				

Section 3 - Configuration

- Get IP From : Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2695. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.
 - IP Address : Assign a static IP address that is within the IP address range of your network.
- Subnet Mask : Subnet Mask : Enter the subnet mask. All devices in the network must share the same subnet mask.
 - **Gateway :** Enter the IP address of the gateway/router in your network.
 - **DNS**: Enter a DNS server IP address. This is usually the local IP address of your gateway/router.



Authentication Settings- Username/Password

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, user can view and configure the Captive Portal settings. After selecting Username/Password as the Authentication Type, we can configure the Username/Password authentication that will be applied to each wireless client in this network.

Session	Enter the session timeout value here. This value	and the second second		
timeout(1-1440) :	can be from 1 to 1440 minutes. By default, this	D-Link [®]	DAP-269	95
	value is 60 minutes.	🔶 Home 🌋 Maintenand	ice 🕶 🔚 Configuration 👻 💝 System 🙋 Logout 📧 H	elp
		DAP-2695	Captive Portal Authentication	
Band :	Select 2.4GHz or 5GHz.	Advanced Settings Advanced Settings Performance Wireless Resource Multi-SSID	Session Timeout (1-1440) 60 Minute(s) Band 2.4GHz SSID Index Primary SSID	
SSID Index :	Select the SSID for this Authentication.	VLAN Intrusion Checkedule Internal RADIUS Server	Authentication Type Username/Password Web Redirection Interface Settings	
Authentication Type :	Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the Username/Password option.	ARP Spoofing Prevention Bandwidth Optimization Captive Portal Captive Portal Login Page Upload IP Filter Settings MAC Bypass DHCP Server Filters Filters Traffic Control	Web Redirection State Disable URL Path http:// IP Interface Settings IPIF Status Disable VLAN Group Get IP From Static IP(Manual) IP Address Subnet Mask	
Web Redirection State :	Default is Disable or select Enable to enable the website redirection feature.	⊕- j Status	Gateway DNS Username/Password Settings Username	
URL Path :	Select whether to use either HTTP or HTTPS here. After selecting either http:// or https://, enter the URL of the website that will be used in the space provided.		Password Add Clear Username Edit Delete	
IPIF Status :	Select to Enable or Disable the Captive Portal with its IP interface feature here.		Save Band SSID Index Captive Profile Edit Delete	
VLAN Group :	Enter the VLAN Group ID here.			

Section 3 - Configuration

- Get IP From : Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2695. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.
 - IP Address : Assign a static IP address that is within the IP address range of your network.
- Subnet Mask : Subnet Mask : Enter the subnet mask. All devices in the network must share the same subnet mask.
 - **Gateway :** Enter the IP address of the gateway/router in your network.
 - **DNS :** Enter a DNS server IP address. This is usually the local IP address of your gateway/router.
 - **Username:** Enter the username for the new account here.
 - Password: Enter the password for the new account here.

D-Link [®]			a <u>. 7</u> .0		DAP-2695
🔶 Home 🕺 Maintenand	ce 👻 📙	Configuration 👻	🐑 System	💋 Logout	🕐 Hel
DAP-2695 Basic Settings Horromance Wireless Resource Multi-SSID VLAN Intrusion Schedule ARP Spoofing Prevention Bandwidth Optimization PAP Array Captive Portal Authentication Settings Urg Pare Upload PIF Fitter Settings DHCP Server Filters Status	Session Timeout Band SSID Index Authentication Ty	2.4GHz Primary Pe Usernarr Interface Settings In State Disable http:// ettings Disable	Minute(s)	Edit	Delete
	Band	SSID Index	Captive Pro	file E	Save dit Delete

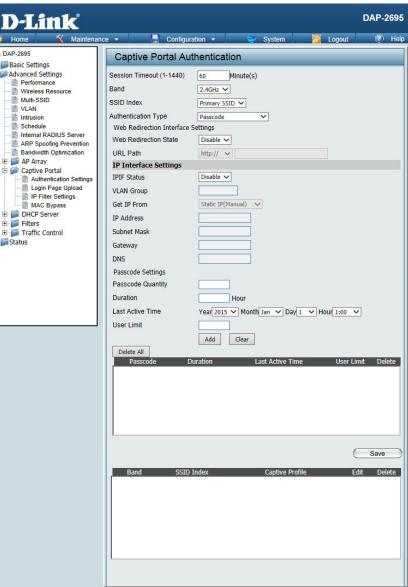
Authentication Settings- Passcode

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, user can view and configure the Captive Portal settings. After selecting Passcode as the Authentication Type, we can configure the Passcode authentication that will be applied to each wireless client in this network.

	Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.	
Band :	Select 2.4GHz or 5GHz.	
SSID Index :	Select the SSID for this Authentication.	
Authentication Type :	Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the Passcode option.	E
Web Redirection State :	Default is Disable or select Enable to enable the website redirection feature.	÷
URL Path :	Select whether to use either HTTP or HTTPS here. After selecting either http:// or https://, enter the URL of the website that will be used in the space provided.	
IPIE Status ·	Select to Enable or Disable the Cantive Portal	

elect to Enable or Disable the with its IP interface feature here.

VLAN Group: Enter the VLAN Group ID here.



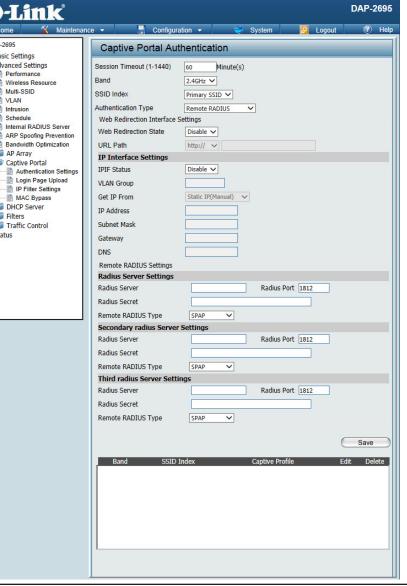
Section 3 - Configuration

Get IP From :	Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your	D-Link	DAP-2695
		🔶 Home 🌋 Maintenanc	e 🕶 📕 Configuration 👻 💝 System 💋 Logout 🛞 Help
	network, or if you wish to assign a static IP address	DAP-2695	Captive Portal Authentication
	to the DAP-2695. When Dynamic IP (DHCP) is	Advanced Settings	Session Timeout (1-1440) 60 Minute(s)
	selected, the other fields here will be grayed out.	Wireless Resource	Band 2.4GHz V
	Please allow about 2 minutes for the DHCP client	VLAN	SSID Index Primary SSID V Authentication Type Passcode V
	to be functional once this selection is made.	Schedule	Web Redirection Interface Settings
		ARP Spoofing Prevention	Web Redirection State
IP Address :	Assign a static IP address that is within the IP	Bandwidth Optimization AP Array	URL Path http:// V
	address range of your network.	Captive Portal Authentication Settings	IPIF Status Disable 🗸
	address range of your network.	Login Page Upload	VLAN Group
Subnet Mask :	Subnet Mask : Enter the subnet mask. All devices	MAC Bypass DHCP Server	Get IP From Static IP(Manual) V IP Address
Subhet Mask :		Filters Traffic Control	Subnet Mask
	in the network must share the same subnet mask.	⊞ 🎬 Status	Gateway
_			DNS Passcode Settings
Gateway :	Enter the IP address of the gateway/router in		Passcode Quantity
	your network.		Duration Hour
			Last Active Time Year 2015 V Month Jan V Day 1 V Hour 1:00 V
DNS:	Enter a DNS server IP address. This is usually the		Add Clear
	local IP address of your gateway/router.		Delete All Passcode Duration Last Active Time User Limit Delete
			Possiciule Duration Last Active nine User Linnic Derete
Passcode Quantity:	Enter the number of ticket that will be used here.		
Duration:	Enter the duration value, in hours, for this		
	passcode.		
			Save
Last Active Day:	Select the last active date for this passcode here.		Band SSID Index Captive Profile Edit Delete
	Year, Month and Day selections can be made.		
Here I.I. M			
User Limit:	Enter the maximum amount of users that can use		
	this passcode at the same time		

Authentication Settings- Remote RADIUS

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, user can view and configure the Captive Portal settings. After selecting Remote RADIUS as the Authentication Type, we can configure the Remote RADIUS authentication that will be applied to each wireless client in this network.

Session	Enter the session timeout value here. This value			
timeout(1-1440):	can be from 1 to 1440 minutes. By default, this value is 60 minutes.	D-Link [®]		
	value is of minutes.	DAP-2695	Cap	
		Basic Settings		
Band :	Select 2.4GHz or 5GHz.	Advanced Settings Performance	Session Band	
		Wireless Resource	SSID Inc	
	Select the SSID for this Authentication.	VLAN	Authenti	
SSID IIIdex :	Select the SSID for this Authentication.		Web R	
		Internal RADIUS Server ARP Spoofing Prevention	Web R	
Authentication Type :	Select the captive portal encryption type here.	Bandwidth Optimization AP Array	URL P	
	Options to choose from are Web Redirection,	Captive Portal	IP Inte IPIF St	
	•	Login Page Upload	VLAN C	
	Username/Password, Passcode, Remote	MAC Bypass	Get IP	
	RADIUS, LDAP and POP3. In this section we'll	DHCP Server Filters	IP Addr	
	discuss the Remote RADIUS option.	🗉 🃁 Traffic Control	Subnet	
	•	⊡ 📁 Status	Gatewa	
Web Redirection State :	Default is Disable or select Enable to enable the		DNS	
web Redirection State :			Remote Radius	
	website redirection feature.		Radius	
			Radius	
URL Path :	Select whether to use either HTTP or HTTPS		Remote	
one rath.			Radius	
	here. After selecting either http:// or https://,		Radius	
	enter the URL of the website that will be used		Remote	
	in the space provided.		Third I	
	• •		Radius	
	Coloct to Evolution or Disciple the Contine Dortal		Radius	
IPIF Status :	Select to Enable or Disable the Captive Portal		Remote	
	with its IP interface feature here.			
			Ba	
VI AN Group :	Enter the VLAN Group ID here.			



- Get IP From : Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2695. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.
- IP Address : Assign a static IP address that is within the IP address range of your network.
- Subnet Mask : Subnet Mask : Enter the subnet mask. All devices in the network must share the same subnet mask.
 - **Gateway :** Enter the IP address of the gateway/router in your network.
 - **DNS :** Enter a DNS server IP address. This is usually the local IP address of your gateway/router.
- Radius Server: Enter the RADIUS server's IP address here
 - Radius Port: Enter the RADIUS server's port number here
- Radius Port: Enter the RADIUS server's shared secret here
- **Remote Radius Type:** Select the remote RADIUS server type here. Currently, only SPAP will be used.

D-Link			10	DAP	-2695
🔶 Home 🏾 🌠 Maintenan	ce 🔻 📙 Config	uration 👻 😓 Sys	tem 💋	Logout 📿	Help
	Captive Portal A Session Timeout (1-1440) Band SSID Index Authentication Type Web Redirection Interfac Web Redirection Interfac Web Redirection State URL Path IP Interface Settings IPIF Status VLAN Group Get IP From IP Address Subnet Mask Gateway DNS Remote RADIUS Settings Radius Server Radius Server	uthentication	tem	Logout	Help

Authentication Settings- LDAP

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, user can view and configure the Captive Portal settings. After selecting LDAP as the Authentication Type, we can configure the LDAP authentication that will be applied to each wireless client in this network.

Session timeout (1-1440) Enter the session timeout value here. This value can **D-Link** DAP-2695 : be from 1 to 1440 minutes. By default, this value is 60 minutes. Configuration DAP-2695 Captive Portal Authentication Basic Settings Band: Select 2.4GHz or 5GHz. Advanced Settings Session Timeout (1-1440) 60 Minute(s) Performance Band 2.4GHz 🗸 Wireless Resource Multi-SSID Primary SSID V SSID Index **SSID Index**: Select the SSID for this Authentication. VI AN Authentication Type IDAP Intrusion V Schedule Web Redirection Interface Settings Internal RADIUS Server Authentication Type: Select the captive portal encryption type here. Web Redirection State Disable V ARP Spoofing Prevention - Bandwidth Optimization URI Path http:// V Options to choose from are Web Redirection, 🗄 🧊 AP Array **IP Interface Settings** Username/Password, Passcode, Remote RADIUS, E Captive Porta **IPIF Status** Disable 🗸 Authentication Setting Login Page Upload LDAP and POP3. In this section we'll discuss the LDAP VLAN Group IP Filter Settings Static IP(Manual) 🗸 Get IP From MAC Bypass option. E DHCP Server IP Address 🗄 🃁 Filters Subnet Mask 🗄 🃁 Traffic Control Web Redirection State: Default is Disable or select Enable to enable the Status Gateway website redirection feature. DNS LDAP Settings Serve **URL Path**: Select whether to use either HTTP or HTTPS here. Port 389 After selecting either http:// or https://, enter the URL Authenticate Mode Simple V Username of the website that will be used in the space provided. Password Base DN (ou=,dc=) **IPIF Status :** Select to Enable or Disable the Captive Portal with Account Attribute (ex.cn) its IP interface feature here. Auto Copy Identity Save VLAN Group: Enter the VLAN Group ID here. Get IP From: Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2695. When Dynamic IP (DHCP) is selected, the other fields here will be graved out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

Section 3 - Configuration

- **IP Address :** Assign a static IP address that is within the IP address range of your network.
- Subnet Mask : Subnet Mask : Enter the subnet mask. All devices in the network must share the same subnet mask.
 - Gateway: Enter the IP address of the gateway/router in your network.
 - **DNS :** Enter a DNS server IP address. This is usually the local IP address of your gateway/router.
 - Server: Enter the LDAP server's IP address or domain name here.
 - **Port:** Enter the LDAP server's port number here.
- Authenticate Mode: Select the authentication mode here. Options to choose from are Simple and TLS.
 - Username: Enter the LDAP server account's username here.
 - **Password:** Enter the LDAP server account's password here.
 - **Base DN:** Enter the administrator's domain name here
 - Account Attribute: Enter the LDAP account attribute string here. This string will be used to search for clients.
 - Identity: Enter the identity's full path string here. Alternatively, select the Auto Copy checkbox to automatically add the generic full path of the web page in the identity field.

Authentication Settings- POP3

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, user can view and configure the Captive Portal settings. After selecting POP3 as the Authentication Type, we can configure the POP3 authentication that will be applied to each wireless client in this network.

Session	Enter the session timeout value here. This value	D 79-1 °		DAP-2695
timeout(1-1440) :	can be from 1 to 1440 minutes. By default, this	D-Link [®]		11
	value is 60 minutes.	🔶 Home 🌋 Maintenand	ce 🕶 🔒 Configuration 👻 🏐 System 🙋 Logout	(?) Help
		DAP-2695	Captive Portal Authentication	
Band :	Select 2.4GHz or 5GHz.	Advanced Settings	Session Timeout (1-1440) 60 Minute(s)	
Dana		···· Division Wireless Resource	Band 2.4GHz V	
	Select the SSID for this Authentication.	Multi-SSID	SSID Index Primary SSID Authentication Type POP3	
SSID IIIdex :	Select the SSID for this Authentication.	Schedule	Authentication Type POP3 V Web Redirection Interface Settings	
		Internal RADIUS Server	Web Redirection State Disable 🗸	
Authentication Type :	Select the captive portal encryption type here.	Bandwidth Optimization P Array	URL Path http:// V	
	Options to choose from are Web Redirection,	Captive Portal Authentication Settings	IP Interface Settings	
	Username/Password, Passcode, Remote	Login Page Upload	VLAN Group	
	RADIUS, LDAP and POP3. In this section we'll		Get IP From Static IP(Manual) V	
	discuss the POP3 option.	🗄 📁 📁 Filters	IP Address	
			Gateway	
Web Redirection State :	Default is Disable or select Enable to enable the		DNS	
	website redirection feature.		POP3 Settings	
			Port 110	
URL Path :	Select whether to use either HTTP or HTTPS		Connection Type None V	
one ruth.	here. After selecting either http:// or https://,			
	enter the URL of the website that will be used			Save
			Band SSID Index Captive Profile	Edit Delete
	in the space provided.			
IPIF Status :	Select to Enable or Disable the Captive Portal			
	with its IP interface feature here.			
			L	
VLAN Group :	Enter the VLAN Group ID here.			

Get IP From : Static IP (Manual) is chosen here. Choose this **D-Link DAP-2695** option if you do not have a DHCP server in 🔏 Maintenance 👻 Configuration 🔶 Home Heln your network, or if you wish to assign a static DAP-2695 **Captive Portal Authentication** IP address to the DAP-2695. When Dynamic Basic Settings Advanced Settings Minute(s) Session Timeout (1-1440) 60 IP (DHCP) is selected, the other fields here will Performance Band 2.4GHz 🗸 Wireless Resource be grayed out. Please allow about 2 minutes Multi-SSID SSID Index Primary SSID V VLAN for the DHCP client to be functional once this Authentication Type POP3 ~ Intrusion Schedule Web Redirection Interface Settings selection is made. Internal RADIUS Server Web Redirection State Disable 🗸 ARP Spoofing Prevention Bandwidth Optimization **URL Path** http:// V 🗄 🧊 AP Array **IP Address : IP Interface Settings** Assign a static IP address that is within the IP E 📁 Captive Portal Disable 🗸 **IPIE Status** Authentication Settings address range of your network. 📄 Login Page Upload VLAN Group IP Filter Settings Get IP From Static IP(Manual) MAC Bypass 1 DHCP Server TP Address Subnet Mask : Subnet Mask : Enter the subnet mask. All devices 🕀 🃁 Filters 🗄 🧉 Traffic Control Subnet Mask in the network must share the same subnet E Status Gateway mask. DNS POP3 Settings Server Gateway : Enter the IP address of the gateway/router in Port 110 Connection Type your network. None V Save DNS: Enter a DNS server IP address. This is usually the SSID In Edit Delete local IP address of your gateway/router. Server: Enter the POP3 server's IP address or domain name here. Port: Port: Enter the POP server's port number here.

D-Link DAP-2695 User Manual

Connection Type: Select the connection type here. Options to

choose from are None and SSL/TLS.

Login Page Upload

In this window, users can upload a custom login web page that will be used by the captive portal feature. Click the **Browse** button to navigate to the login style, located on the managing computer and then click the **Upload** button to initiate the upload.

- Upload Login Style From Local Hard Drive: In this field the path to the login style file, that will be uploaded, will be displayed. Alternatively, the path can be manually entered here.
- Login Page Style List : Select the wireless band and login style that will be used in each SSID here. Click Download button to download the template file for login page and Click Del button to delete the template file.

D-Link [®]							D/	AP-20	695
🔹 Home 🏾 🐔 Maintenanc	ce 🔻 🚽 Config	guration 🔻	۲	System		🖉 Log	jout	٢	Help
DAP-2695 Basic Settings Advanced Settings Advanced Settings Advanced Settings Advanced Settings Advanced Settings Schedule Intrusion Schedule Intrusion APP Spoofing Prevention Bandwidth Optimization APP Array Captive Portal Authentication Settings Login Page Upload IP Filter Settings MAC Bypass DHCP Server Filters Traffic Control Status	Login Page Uplo	m Local Hard le : 457216 By 2.4GHz • Pri ©	∕te(s) S-1 S ⊙ (0	-2 S-3	」 浄現 ○ ○ ○ ○ ○ ○	0	S-7 Down C		Det

.

IP Filter Settings

Enter the IP address or network address that will be used in the IP filter rule. For example, an IP address like 192.168.70.66 or a network address like 192.168.70.0. This IP address or network will be inaccessible to wireless clients in this network.

_ _ . .

Wireless Band :	Wireless Band : Select 2.4GHz or 5GHz.	
IP Address:	IP Address: Enter the IP address or network address	
Subnet Mask:	Subnet Mask: Enter the subnet mask of the IP address or networks address]
Upload IP Filter File:	Upload IP Filter File: To upload a IP filter list file, click Browse and navigate to the IP filter list file saved on the computer, and then click Upload.	
Download IP Filter File:	Download IP Filter File: To download IP Filter list file, click Download and to save the IP Filter list.	•••••

.

.

D-Link [®]			DAP-2695
🔹 Home 🥻 Maintenanc	e 🔻 🔡 Configura	tion 🔻 👙 System	💋 Logout 🛛 🕖 Help
Porte Array Captive Portal Captive Performance Wireless Resource Multi-SSID Vireless Resource Multi-SSID VIAN Intrusion Schedule Internal RADIUS Server ARP Spoofing Prevention Bandwidth Optimization Captive Portal Captive Portal Dappage Upload Piter Settings MAC Bypags MAC Bypags	IP Filter Settings Wireless Band SSID Index IP Address Subnet Mask ID IP Address	2.4GHz Primary SSID Add Subnet Mask	Delete
	Upload IP Filter File		
	Upload File :	2	列覽 Upload
	Download IP Filter File		
	Load IP Filter File to Local Hard Driver :	Download	Save

MAC Bypass

The DAP-2695 features a wireless MAC Bypass. Once a user is finished with these settings, click the Save button to let the changes take effect.

Wireless Band:	Select the wireless band for MAC Bypass.	D-Link	DAP-2695
SSID Index:	Select the SSID for MAC Bypass.	Home Maintenanc DAP-2695	e - 🔚 Configuration - 🤤 System 💋 Logout 🔞 Help
	Enter each MAC address that you wish to include in your bypass list, and click Add.	Basic Settings Advanced Settings Performance Wireless Resource Multi-SSID VLAN	WAC Bypass Settings Wireless Band 2.4GHz • SSID Index Primary SSID • MAC Address : : : : : :
	When a MAC address is entered, it appears in this list. Highlight a MAC address and click the Delete icon to remove it from this list.	AP Array	ID MAC Address Delete
-	To upload a MAC bypass list file, click Browse and navigate to the MAC bypass list file saved on the computer, and then click Upload.	MAC Bypass MAC Bypass DHCP Server Filters Traffic Control Control	Upload MAC File Upload MAC File Load MAC File Download MAC File Download Driver :
	To download MAC bypass list file, click Download and to save the MAC bypass list.		Save

Load

DHCP Server

Dynamic Pool Settings

The DHCP address pool defines the range of the IP address that can be assigned to stations in the network. A Dynamic Pool allows wireless stations to receive an available IP with lease time control. If needed or required in the network, the DAP-2695 is capable of acting as a DHCP server.

Function Enable/Disable: Dynamic Host Configuration Protocol (DHCP) assigns dynamic IP addresses to devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign new IP addresses. Select Enable to allow the DAP-2695 to function as a DHCP server.

- IP Assigned From: Input the first IP address available for assignment on your network.
- The Range of Pool (1-254): Enter the number of IP addresses available for assignment. IP addresses are increments of the IP address specified in the "IP Assigned From" field.



- Subnet Mask: All devices in the network must have the same subnet mask to communicate. Enter the subnet mask for the network here.
 - Gateway: Enter the IP address of the gateway on the network.
 - WINS: Specify the Windows Internet Naming Service (WINS) server address for the wireless network. WINS is a system that determines the IP address of a network computer that has a dynamically assigned IP address.
 - **DNS:** Enter the IP address of the Domain Name System (DNS) server. The DNS server translates domain names such as www.dlink.com into IP addresses.

Domain Name: Enter the domain name of the network, if applicable. (An example of a domain name is: www.dlink.com.)

Lease Time: The lease time is the period of time before the DHCP server will assign new IP addresses.

Static Pool Setting

The DHCP address pool defines the range of IP addresses that can be assigned to stations on the network. A static pool allows specific wireless stations to receive a fixed IP without time control.

- Function Enable/Disable: Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to wireless devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign IP addresses. Select Enable to allow the DAP-2695 to function as a DHCP server.
 - Assigned IP: Use the Static Pool Settings to assign the same IP address to a device every time you start up. The IP addresses assigned in the Static Pool list must NOT be in the same IP range as the Dynamic Pool. After you have assigned a static IP address to a device via its MAC address, click Apply; the device will appear in the Assigned Static Pool at the bottom of the screen. You can edit or delete the device in this list.
 - Assigned MAC Address: Enter the MAC address of the device requesting association here.
 - Subnet Mask: Define the subnet mask of the IP address specified in the "IP Assigned From" field.
 - Gateway: Specify the Gateway address for the wireless network.
 - WINS: Specify the Windows Internet Naming Service (WINS) server address for the wireless network. WINS is a system that determines the IP address of a network computer with a dynamically assigned IP address, if applicable.
 - DNS: Enter the DNS server address for your wireless network.
 - Domain Name: Specify the domain name for the network.

Static Pool Settings	
DHCP Server Control	
Function Enable/Disable	Enable 💌
Static Pool Setting	
HostName	
Assigned IP	
Assigned MAC Address	
Subnet Mask	255.255.255.0
Gateway	
WINS	
DNS	
Domain Name	dlink-ap
	Save
Host Name MAC Address	IP Address Edit Delete
l	

Current IP Mapping List

This window displays information about the current assigned DHCP dynamic and static IP address pools. This information is available when you enable DHCP server on the AP and assign dynamic and static IP address pools.

	These are IP address pools the DHCP server has assigned using the dynamic pool setting.	Current IP Mapping List Current DHCP Dynamic Pools	
Binding MAC Address:	The MAC address of a device on the network that is assigned an IP address from the DHCP dynamic pool.	Host Name Binding MAC Address Current DHCP Static Pools Host Name Binding MAC Address	Assigned IP Address Lease Time
Assigned IP Address:	The current corresponding DHCP-assigned IP address of the device.		
Lease Time:	The length of time that the dynamic IP address will be valid.		
Current DHCP Static Pools:	These are the IP address pools of the DHCP server assigned through the static pool settings.		
Binding MAC Address:	The MAC address of a device on the network that is within the DHCP static IP address pool.		
Assigned IP Address:	The current corresponding DHCP-assigned static IP address of the device.		
Binding MAC Address:	The MAC address of a device on the network that is assigned an IP address from the DHCP dynamic pool.		

Assigned IP Address: The current corresponding DHCP-assigned static IP address of the device.

Filters

Wireless MAC ACL

This page allows the user to configure Wireless MAC ACL settings for access control.

Wireless Band: Displays the current wireless band rate.

Access Control List: Select **Disable** to disable the filters function.

Select **Accept** to accept only those devices with MAC addresses in the Access Control List. All other devices not on the list will be rejected.

Select **Reject** to reject the devices with MAC addresses on the Access Control List. All other devices not on the list will be accepted.

- MAC Address: Enter each MAC address that you wish to include in your filter list, and click Apply.
- MAC Address List: When you enter a MAC address, it appears in this list. Highlight a MAC address and click Delete to remove it from this list.
 - **Current Client** This table displays information about all the current **Information:** connected stations.

Wireless MAC	ACL Se	ttings			
Wireless Band	2,40	Hz 👻			
Access Control List	Acce	ept 💌			
MAC Address]:[]:[]:[]]:	. Add	
ID MAC Ad	dress		Delete		
Current Client Informat MAC Address	SSID	Band	Authenticat	ion Signal	Add
00:1F:3B:AD:35:0B	dlink	N	OPEN	98%	
Upload ACL File					
Upload File :				Browse Upload	1
Download ACL File				biowse	
Load ACL File to Local	Hard Do	wnload			
Driver :		Milodo			
				0	Save

WLAN Partition

This page allows the user to configure a WLAN Partition.

- Link Integrity: Select Enable or Disable. If the Ethernet connection between the LAN and the AP is disconnected, enabling this feature will cause the wireless segment associated with the AP to be disassociated from the AP.
- Ethernet WLAN Access: The default is Enable. When disabled, all data from the Ethernet to associated wireless devices will be blocked. Wireless devices can still send data to the Ethernet.

Internal Station Connection: The default value is Enable, which allows stations to intercommunicate by connecting to a target AP. When disabled, wireless stations cannot exchange data on the same Multi-SSID. In Guest mode, wireless stations cannot exchange data with any station on your network.

WLAN Partition				
Wireless Band	2.4GHz 👻			
Link Integrity	Disable 🔻			
Ethernet to WLAN Access	Enable 👻			
Internal Station Connection				
Primary SSID	Enable	O Disable	🔘 Guest mode	
Multi-SSID 1	Enable	O Disable	🔘 Guest mode	
Multi-SSID 2	Enable	O Disable	🔘 Guest mode	
Multi-SSID 3	Enable	O Disable	O Guest mode	
Multi-SSID 4	Enable	O Disable	O Guest mode	
Multi-SSID 5	Enable	O Disable	O Guest mode	
Multi-SSID 6	Enable	O Disable	O Guest mode	
Multi-SSID 7	Enable	O Disable	🔘 Guest mode	
				Save

Traffic Control Uplink/Downlink Setting

The uplink/downlink setting allows users to customize the downlink and uplink interfaces including specifying downlink/uplink bandwidth rates in Mbits per second. These values are also used in the QoS and Traffic Manager windows. Once the desired uplink and downlink settings are finished, click the **Save** button to let your changes take effect.

Downlink Bandwidth: The downlink bandwidth in Mbits per second.

Uplink Bandwidth: Uplink Bandwidth: The uplink bandwidth in Mbits per second.

🇌 Home 🥻 Maintenan	ce 🔻 🚽 🤤 (Configuration 🔻	😌 System	💋 Logout	🕖 Helj
DAP-2895	Uplink and D	ownlink Setti	ng		
Advanced Settings Advanced Settings Berformance Wireless Resource Wuth-SSID	LAN1 LAN2	Downlink	Uplink		
- VLAN	2.4GHz	5GH	łz		
VLAN Intrusion Intrusion Arb Spoofing Prevention Bandwidth Optimization AP Array Captive Portal Dynamic Pool Settings Current IP Mapping List Fifters Cos Cast Casting Cos Casting Cast Casting Casting Casting Casting Casting Cast Casting Cast Casting	Downlink Interface Primary-ssid Multi-ssid4 WDS1 WDS5 Uplink Interface Primary-ssid Multi-ssid4 WDS1 WDS5	Multi-ssid1 Multi-ssid5 WD52 WD56 Multi-ssid1 Multi-ssid5 WD52 WD56	Multi-ssid2 Multi-ssid6 WD53 WD57 Multi-ssid2 Multi-ssid6 WD53 WD57	Multi-ssid3 Multi-ssid7 WD54 WD58 Multi-ssid3 Multi-ssid7 WD54 WD58	
	Downlink Bandwidth(Uplink Bandwidth(1~			6	Save

QoS

Quality of Service (QoS) enhances the experience of using a network by prioritizing the traffic of different applications. The DAP-2695 supports four priority levels. Once the desired QoS settings are finished, click the **Save** button to let your changes take effect.

- **Enable QoS:** Check this box to allow QoS to prioritize traffic. Use the drop-down menus to select the four levels of priority. Click the Save button when you are finished.
- Downlink Bandwidth: Downlink Bandwidth: The downlink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.
 - Uplink Bandwidth: Uplink Bandwidth: The uplink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.

QoS Enable QoS					
Advanced QoS					
Downlink Bandwidth	100 Mbits	sec /			
Uplink Bandwidth	100 Mbits	s/sec			
ACK/DHCP/ICMP/DNS Priority	Highest Priority	🚽 Limit	100	% Port	53,67,68,546,547
Web Traffic Priority	Third Priority	- Limit	100	% Port	80,443,3128,8080
Mail Traffic Priority	Second Priority	Limit	100	% Port	25,110,465,995
Ftp Traffic Priority	Low Priority	- Limit	100	% Port	20,21
User Defined-1 Priority	Highest Priority	Limit	100	% Port	0 - 0
User Defined-2 Priority	Second Priority	Limit	100	% Port	0 - 0
User Defined-3 Priority	Third Priority	- Limit	100	% Port	0 - 0
User Defined-4 Priority	Low Priority	Limit	100	% Port	0 - 0
Other Traffic Priority	Low Priority	Limit	100	%	

Traffic Manager

The traffic manager feature allows users to create traffic management rules that specify how to deal with listed client traffic and specify downlink/ uplink speed for new traffic manager rules. Click the **Save** button to let your changes take effect.

Traffic Manager: Use the drop-down menu to Enable the traffic manager feature.

- Unlisted Client Traffic: Select Deny or Forward to determine how to deal with unlisted client traffic.
- Downlink Bandwidth: The downlink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.
 - Uplink Bandwidth: Uplink Bandwidth: The uplink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.

Traffic Manage	r
Traffic Manager	Disable 🔻
Unlisted Clients Traffic	O Deny Forward
Downlink Bandwidth	100 Mbits/sec
Uplink Bandwidth	100 Mbits/sec
Add Traffic Manag	er Rule
Name	
Client IP(optional)	
Client MAC(optional)	
Downlink Speed	Mbits/sec
Uplink Speed	Mbits/sec
	Add Clear
Traffic Manager R	ules
Name Client	IP Client MAC Downlink Speed Uplink Speed Edit Del
	Save

Status

In the Status Section the user can monitor and view configuration settings of the access point. Here the user can also view statistics about client information, WDS information and more. The following pages will explain settings found in the Status section in more detail.

D-Link Home X Maintena	nce 🔻 📑 Configuration	🔹 👻 System 💋 Logout	DAP-2695
DAP-2695			e ricip
Basic Settings	Device Information		
Advanced Settings Performance	Ethernet MAC Address:	Firmware Version:1.10 78:54:2e:aa:ea:00	
Wireless Resource Multi-SSID	Wireless MAC Address(2.4GHz):	Primary: 78:54:2e:aa:ea:00 SSID 1~7: 78:54:2e:aa:ea:01 ~ 78:54:2e:aa:ea:07	,
Intrusion Schedule Internal RADIUS Server	Wireless MAC Address(5GHz):	Primary: 78:54:2e:aa:ea:08 SSID 1~7: 78:54:2e:aa:ea:09 ~ 78:54:2e:aa:ea:0f	2
ARP Spoofing Prevention	Ethernet		
Bandwidth Optimization AP Array	IP Address	192.168.0.50	
E Captive Portal	Subnet Mask	255.255.255.0	
Authentication Settings Login Page Upload	Gateway	N/A	
MAC Bypass	DNS		
E DHCP Server	Wireless (2.4GHz)		
E Filters	Network Name (SSID)	dlink	
Traffic Control Status	Channel	11	
Device Information	Data Rate	Auto	
Client Information WDS Information	Security	None	
Channel Analyze	Wireless (5GHz)		
🗉 📁 Statistics	Network Name (SSID)	dlink	
⊞…🃁 Log	Channel	149	
	Data Rate	Auto	
	Security	None	
	AP Array		
	AP Array	d-link	
	Role	Slave	
	Location		
	Device Status		
	CPU Utilization	0%	
	Memory Utilization	11%	
	Central WiFiManager		
	Connection Status	Disconnect	
	Server IP		
	Service Port		
	Live Port		
	Group ID		

Device Information

This page displays the current information like firmware version, Ethernet and wireless parameters, as well as the information regarding CPU and memory utilization.

Device Information:	This read-only window displays the
	configuration settings of the DAP-2695,
	including the firmware version and the
	device's MAC address.

D-Link [®]		DAP-2	695
🔶 Home 🕺 Maintenand	ce 🔻 🚽 Configuration	👻 💝 System 🛛 🖉 Logout 🖤	Help
DAP-2695	Device Information		
	Ethernet MAC Address: Wireless MAC Address(2.4GHz):	Firmware Version: 1.10 78:54:2e:aa:ea:00 Primary: 78:54:2e:aa:ea:00 SSID 1~7: 78:54:2e:aa:ea:01 ~ 78:54:2e:aa:ea:07 Primary: 78:54:2e:aa:ea:08 SSID 1~7: 78:54:2e:aa:ea:09 ~ 78:54:2e:aa:ea:0f 192.168.0.50 255.255.255.0 N/A dlink 11 Auto None dlink 149 Auto	
	Security	None	
	AP Array		
	AP Array Role	d-link Slave	
	Device Status		
	CPU Utilization	0%	
	Memory Utilization	11%	
	Central WiFiManager		
	Connection Status	Disconnect	
	Server IP		
	Service Port		
	Live Port		
	Group ID		

Client Information

This page displays the associated clients SSID, MAC, band, authentication method, signal strength, and power saving mode for the DAP-2695 network.

Client Information: This window displays the wireless client information for clients currently connected to the DAP-2695.

- **SSID:** Displays the SSID of the client.
- MAC: Displays the MAC address of the client.
- **Band:** Displays the wireless band that the client is connected to.
- Authentication: Displays the type of authentication being used.
 - **RSSI:** Displays the client's signal strength.
- **Power Saving Mode:** Displays the status of the power saving feature.



WDS Information Page

This page displays the access points SSID, MAC, band, authentication method, signal strength, and status for the DAP-2695's Wireless Distribution System network.

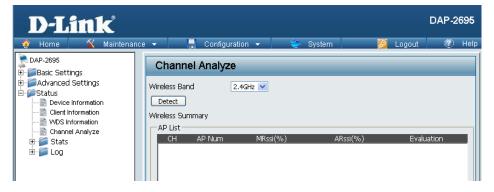
- **WDS Information:** This window displays the Wireless Distribution System information for clients currently connected to the DAP-2695.
 - Name: Displays the SSID of the client.
 - MAC: Displays the MAC address of the client.
 - Authentication: Displays the type of authentication being used.
 - **Signal:** Displays the client's signal strength.
 - Status: Displays the status of the power saving feature.



Channel Analyze

Wireless Band: Select either 2.4Ghz or 5GHz.

- **Detect:** Click the Detect button to scan.
- AP List: This will list the transmitting channels and quality.



Stats Page Ethernet Traffic Statistics

Displays wired interface network traffic information.

Ethernet Traffic Statistics: This page displays transmitted and received count statistics for packets and bytes.

D-Link					DAP-2695
🔗 Home 🦷 🔏 Mainten:	ance 🔻	🚽 Configuration 🚽	🖌 👙 System	💋 Logo	ut 🕐 Help
DAP-2695 Basic Settings Advanced Settings	Eth	ernet Traffic Statis	tics		
			LAN1	LAN2	Clear Refresh
Device Information Glient Information	Transn	nitted Count			
	Transm	nitted Packet Count	0	5280	
	Transm	nitted Bytes Count	0	4578032	
Ethernet	Droppe	d Packet Count	0	0	
WLAN	Receiv	ed Count			
⊞*j⊃ Log	Receive	ed Packet Count	0	6508	
	Receiv	ed Bytes Count	0	740886	
	Droppe	d Packet Count	0	0	

WLAN Traffic Statistics

Displays throughput, transmitted frame, received frame, and WEP frame error information for the AP network.

WLAN Traffic Statistics: This page displays wireless network statistics for data throughput, transmitted and received frames, and frame errors.

D-Link DAP-2695			
🔶 Home 🥻 Maintenanc	e 👻 📙 Configuration 👻	💝 System	💋 Logout 🛛 🕅 Help
DAP-2695	WLAN Traffic Statistics		
Generatings Generatings Generatings Generatings Generatings		2.4GHz	Clear Refresh 5GHz
Device Information Glient Information	Transmitted Count Transmitted Packet Count	2270	4552
		3270	4552
	Transmitted Bytes Count	445102	1270008
Ethernet	Dropped Packet Count	3605	0
₩LAN 	Transmitted Retry Count	0	0
tog	Received Count Received Packet Count	592	0
			-
	Received Bytes Count	169762	0
	Dropped Packet Count	0	0
	Received CRC Count	0	0
	Received Decryption Error Count	0	0
	Received MIC Error Count	0	0
	Received PHY Error Count	0	0

Log **View Log**

The AP's embedded memory holds logs here. The log information includes but is not limited to the following items: cold start AP, upgrading firmware, client associate and disassociate with AP, and web login. The web page holds up to 500 logs.

View Log: The AP's embedded memory displays system and network messages including a time stamp and message type. The log information includes but is not limited to the following items: cold start AP, upgrading firmware, client associate and disassociate with AP, and web login. The web page holds up to 500 logs.

D-Link [®]			DAP-2695
🔶 Home 🏾 🕺 Maintenanci	e 🔻 📙 Configur	ation 👻	👙 System 🛛 👰 Logout 🛛 🕅 Help
DAP-2695 Basic Settings Advanced Settings Catual Status Device Information	View Log		
	First Page Last Page Page 1 of 11	Previous	Next Clear
Client Information	Time	Priority	Message
	Uptime 0 day 20:53:02	[Wireless]	2.4G:Deauth:Aging STA 10:0E:2B:AE:B6:90
E Stats	Uptime 0 day 20:43:29	[Wireless]	2.4G:Association Success:STA 10:0E:2B:AE:B6:90
Ethernet	Uptime 0 day 20:43:07	[Wireless]	2.4G:Association Success:STA 10:0E:2B:AE:B6:90
E-12 WLAN	Uptime 0 day 20:42:55	[Wireless]	2.4G:Association Success:STA 10:0E:2B:AE:B6:90
View Log	Uptime 0 day 20:41:03	[Wireless]	2.4G:Received disassociate:STA 10:0E:2B:AE:B6:90 (reason 1)
	Uptime 0 day 20:32:54	[Wireless]	2.4G:Association Success:STA 10:0E:2B:AE:B6:90
	Uptime 0 day 20:32:50	[Wireless]	2.4G:Received disassociate:STA 10:0E:28:AE:86:90 (reason 1)
	Uptime 0 day 20:32:19	[Wireless]	2.4G:Association Success:STA 10:0E:2B:AE:B6:90
	Uptime 0 day 20:32:14	[Wireless]	2.4G:Received disassociate:STA 10:0E:2B:AE:B6:90 (reason 1)
	Uptime 0 day 20:31:43	[Wireless]	2.4G:Association Success:STA 10:0E:2B:AE:B6:90
	Uptime 0 day 20:31:38	[Wireless]	2.4G:Received disassociate:STA 10:0E:2B:AE:B6:90 (reason 1)
	Uptime 0 day 20:31:07	[Wireless]	2.4G:Association Success:STA 10:0E:2B:AE:B6:90
	Uptime 0 day 20:31:01	[Wireless]	2.4G:Received disassociate:STA 10:0E:2B:AE:B6:90 (reason 1)
	Uptime 0 day 20:30:30	[Wireless]	2.4G:Association Success:STA 10:0E:2B:AE:B6:90
	Uptime 0 day 20:06:47	[Wireless]	2.4G:Deauth:Aging STA F0:7D:68:07:2C:80
	Uptime 0 day 19:56:45	[Wireless]	2.4G:Association Success:STA F0:7D:68:07:2C:B0
	Uptime 0 day 19:56:45	[Wireless]	2.4G:Received Deauth:STA 00:24:01:AB:C0:10 (reaso n 6)
	Uptime 0 day 19:56:44	[Wireless]	2.4G:Received Deauth:STA 00:24:01:AB:C0:10 (reaso n 6)

Log Settings

Enter the log server's IP address to send the log to that server. Check or uncheck System Activity, Wireless Activity, or Notice to specify what kind of log type you want it to log.

Log Server/IP Address:	Enter the IP address of the server you would like to send the DAP-2695 log to.	D-Link Home X Maintenance	e 🔻 📄 Configuration 🕬	🔹 💓 System	C 😥 Logout	AP-2695
Log Type: E-mail Notification: E-mail Log Schedule:	Check the box for the type of activity you want to log. There are three types: System Activity, Wireless Activity, and Notice. Support Simple Mail Transfer Protocol for log schedule and periodical change key. It can not support Gmail SMTP port 465. Please set to Gmail SMTP port 25 or 587. Use the drop-down menu to set the e-mail log schedule.	DAP-2695 Advanced Settings Status Cient Information Cient Information Channel Analyze Stats Ethernet MUAN Cog View Log Log Settings	Log Settings Log Settings Log Server / IP Address Log Type Email Notification Email Notification Outgoing mail server (SMTP) Authentication SSL/TLS From Email Address To Email Address Email Server Address SMTP Port User Name Password Confirm Password Email Log Schedule	 ✓ System Activity ✓ Wireless Activity ✓ Notice ✓ Enable 		

Schedule

0 💽 hours or when Log is full

Save

Maintenance Section

In the Status Section the user can monitor and view configuration settings of the access point. Here the user can also view statistics about client information, WDS information and more. The following pages will explain settings found in the maintenance section in more detail.



Administration Limit Administrator

Check one or more of the five main categories to display the various hidden administrator parameters and settings displayed on the next five pages. Each of the five main categories display various hidden administrator parameters and settings.

Limit Administrator VLAN Check the box provided and the

- **ID:** enter the specific VLAN ID that the administrator will be allowed to log in from.
- Limit Administrator IP: Check to enable the Limit Administrator IP address.
 - IP Range: Enter the IP address range that the administrator will be allowed to log in from and then click the Add button.

D-Link [®]		DAP-2695
🛕 Home 🥻 Maintenar	ce 🕶 🔚 Configuration 👻 💝 System 🛛 🙋 Logout	🕐 Help
DAP-2695	Administration Settings	
Basic Settings Advanced Settings Status	Limit Administrator Imit Administrator Limit Administrator Imit Administrator Limit Administrator Imit Administrator Imit Administrator Imit Administrator IP Range From: To: IP Range From: To: Item From To Delete Imit Administrator	Add)
	System Name Settings	
	Login Settings 🔳	
	Console Settings 🔳	
	SNMP Settings	
	Ping Control Setting 🔳	
	Central WiFiManager Setting 🔳	
	E	Save

System Name Settings

Each of the five main categories display various hidden administrator parameters and settings.

System Name: The name of the device. The default name is D-Link DAP-2695.

Location: The physical location of the device, e.g. 72nd Floor, D-Link HQ.

System Name Sett	ngs 🗹	
System Name	D-Link DAP-2553	
Location		

Login Settings

Each of the five main categories display various hidden administrator parameters and settings.

User Name: Enter a user name. The default is admin.

Old Password: When changing your password, enter the old password here.

Login Settings 🛛	
Login Name	admin
Old Password	
New Password	
Confirm Password	

New Password: When changing your password, enter the new password here. The password is case-sensitive. "A" is a different character than "a." The length should be between 0 and 12 characters.

Confirm Password: Enter the new password a second time for confirmation purposes.

Console Settings

Each of the five main categories display various hidden administrator parameters and settings.

- Status: Status is enabled by default. Uncheck the box to disable the console.
- **Console Protocol:** Select the type of protocol you would like to use, Telnet or SSH.

Console Settings 🗹		
Status	Enable	
Console Protocol	⊙ Telnet ◯ SSH	
Timeout	3 Mins	

Time-out: Set to 1 Min, 3 Mins, 5 Mins, 10 Mins, 15 Mins or Never.

SNMP Settings

Each of the five main categories display various hidden administrator parameters and settings.

Status:	Check the box to enable the SNMP	SNMP Settings M	
	functions. This is enabled by default.	Status	Enable
Public Community String:	Enter the public SNMP community string.	Public Community String	public
· · · · · · · · · · · · · · · · · · ·	p =p	Private Community String	private
Private Community String:	Enter the private SNMP community	Trap Status	Enable
	string.	Trap Server IP	

Central WiFiManager Settings

The Central WiFiManager section is used to create a set of APs on the Internet to be organized into a single group in order to increase ease of management. Central WiFiManager and AP Array are mutually exclusive functions.

	Select to enable or disable the Central	Central WiFiManager Setting 🛛	ing 🔽
WiFiManager :	WIFIManager.	Enable Central WiFiManager	Disable 🔻

Firmware and SSL Upload

This page allows the user to perform a firmware upgrade. A Firmware upgrade is a function that upgrade the running software used by the access point. This is a useful feature that prevents future bugs and allows for new features to be added to this product. Please go to your local D-Link website to see if there is a newer version firmware available.

Firmware and SSL You can upload files to the access point. **Certification Upload:**

Upload Firmware from The current firmware version is displayed **Local Hard Drive:** above the file location field. After the latest firmware is downloaded, click on the "Choose File" button to locate the new firmware. Once the file is selected. click on the "Open" and "Upload" button to begin updating the firmware. Please don't turn the power off while upgrading.

Upload SSL Certification After you have downloaded a SSL

from Local Hard Drive: certification to your local drive, click "Choose File." Select the certification and click "Open" and "Upload" to complete the upgrade.

D-Link		DAP-2695
🏠 Home 🏾 🌠 Maintena	nce 🕶 📙 Configuration 👻 💭 System 🛛 💋 Lo	gout 🕐 Help
DAP-2695 Dasic Settings Data Advanced Settings Data Status	Firmware and SSL Certification Upload	
	Update Firmware From Local Hard Drive	
	Firmware Version 1.00	
	Upload Firmware From File : Choose File No file chosen Upload	
	Update SSL Certification From Local Hard Drive	
	Upload Certificate From File : Choose File No file chosen Upload	
	Upload Key From File : Choose File No file chosen Upload	

Configuration File Upload

This page allows the user to backup and recover the current configuration of the access point in case of a unit failure.

	You can upload and download configuration files of the access point.	D-Lini
Upload Configuration File:	Browse to the saved configuration file you have in local drive and click "Open" and "Upload" to update the configuration.	DAP-2895 Basic Settings Advanced Settings Status
Download Configuration		
File:	Click "Download" to save the current configuration file to your local disk. Note that if you save one configuration file with the administrator's password now, after resetting your DAP-2695 and then updating to this saved configuration file, the password will be gone.	

D-Link										DAP-2	090
🕨 Home 🦷 🔏 Maintenance	-		Configuration	•	ັ 👙 ຊ	System		P	Logout	0	Help
DAP-2695 Basic Settings Advanced Settings Status	Upload Upload Down	d Config I File : Ioad Cor	uration File U uration File Choose File) No file ch		ownloa	Upload)			

Time and Date Settings

Enter the NTP server IP, choose the time zone, and enable or disable daylight saving time.

Current Time:	Displays the current time and date settings.	
Enable NTP Server:	Check to enable the AP to get system time from an NTP server from the Internet.	
NTP Server:	Enter the NTP server IP address.	÷
Time Zone:	Use the drop-down menu to select your correct Time Zone.	
Enable Daylight Saving:	Check the box to enable Daylight Saving Time.	
	Use the drop-down menu to select the correct Daylight Saving offset.	
Set the Date and Time Manually:	A user can either manually set the time for the AP here, or click the Copy Your Computer's Time Settings button to copy the time from the computer in use (Make sure that the computer's time is set correctly).	

D-Link [®]					DAP-2	695				
🔶 Home 🤺 Maintena	ance 👻 📙 Configu	ration 👻 👙	System	💋 Logout	۲	Help				
DAP-2695 Basic Settings	Time and Date	Time and Date Settings								
	Time Configuration	Time Configuration								
	Current Time	01/01/1970 21:0	7:35							
	Automatic Time Co	nfiguration								
	Enable NTP Server									
	NTP Server									
	Time Zone	(GMT+08:00) Ula	aan Bataar		~					
	Enable Daylight Saving									
	Daylight Saving Dates	Mor DST Start Jar DST End Jar	n 💌 🛛 İst 💌	Sun 💌 12	rent Time 2 am 💌 2 am 💌					
	Set the Date and T	ime Manually								
	Date And Time	Year 2013 Hour 11 💌	Minute 1	Day Second	9 💙 45 💙					
		Copy Your Comp	uter's Time Setting	15						
				0	Save	\supset				

Configuration and System

These options are the remaining option to choose from in the top menu. Configuration allows the user to save and activate or discard the configurations done. System allows the user to restart the unit, perform a factory reset or clear the language pack settings. Logout allows the user to safely log out from the access point's web configuration. Help allows the user to read more about the given options to configure without the need to consult the manual. The following pages will explain settings found in the configuration and system section in more detail.

J	D-L	ini	K							DAP-2	695
<u></u>	Home		Maintenance	-	🚽 Configuration 👻	۵	System		Logout		Help
					↓				+		
					📄 Configuration 👻		y	/stem	2	Logout	
					Save and Activate			The current bro	Carlos and a second second second	and the second second second	

System Settings On this page the user can restart the unit, perform a factory reset of the access point or clear the added language pack.

Restart the Device:	Click Restart to restart the DAP-2695.
	Click Restore to restore the DAP-2695 back to factory default settings.
Clear Language Pack:	Click to clear the current Language pack running.

D -Link	•				DAP-2695
🏠 Home 🏾 🔏 Ma	intenance 🔻	🚽 Configuration 👻	🛬 System	💋 Logout	🕐 Help
DAP-2695 Basic Settings	Sy	stem Settings			
🃁 Advanced Settings 🍯 Status	Resta	rt the Device	Restart		
	Resto	re to Factory Default Settings	Restore		

Help

The help page is useful to view a brief description of a function available on the access point in case the manual is not present.

Help: Scroll down the Help page for topics and explanations.

Basic Settings

Wireless Settings

Allow you to change the wireless settings to fit an existing wireless network orto customize your wireless network.

Wireless Band

Operating frequency band. Choose 2.4GHz for visibility to legacy devices and for longer range. Choose 5GHz for least interference; interference can hurt performance. This AP will operate one band at a time.

Application

This option allows the user to choose for indoor or outdoor mode at the 5G Band.

Mode

Select a function mode to configure your wireless network. Function modes include AP, WDS (Wireless Distribution System) with AP, WDS and Wireless Client. Function modes are designed to support various wireless network topology and applications.

Network Name (SSID)

Also known as the Service Set Identifier, this is the name designated for a specific wireless local area network (WLAN). The factory default setting is "dink". The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

SSID Visibility

Indicate whether or not the SSID of your wireless network will be broadcasted. The default value of SSID Visibility is set to "Enable," which allow wireless clients to detect the wireless network. By changing this setting to "Disable," wireless clients can no longer detect the wireless network and can only connect if they have the correct SSID entered.

Auto Channel Selection

If you check Auto Channel Scan, everytime when AP is booting up, the AP will automatically find the best channel to use. This is enabled by default.

Channel

Indicate the channel setting for the DAP-2553. By default, the AP is set to Auto Channel Scan. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network.

Channel Width

Allows you to select the channel width you would like to operate in. Select 20MHz if you are not using any 802.11n wireless clients. Auto 20/40MHz allows your to use both 802.11n and non-802.11n wireless devices in your network

Authentication

Knowledge Base Wireless Basics

D-Link wireless products are based on industry standards to provide high-speed wireless connectivity that is easy to use within your home, business or public access wireless networks. D-Link wireless products provides you with access to the data you want, whenever and wherever you want it. Enjoy the freedom that wireless networking can bring to you.

WLAN use is not only increasing in both home and office environments, but in public areas as well, such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are allowing people to work and communicate more efficiently. Increased mobility and the absence of cabling and other types of fixed infrastructure have proven to be beneficial to many users.

Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards, allowing wireless users to use the same applications as those used on a wired network.

People use WLAN technology for many different purposes:

- **Mobility** productivity increases when people can have access to data in any location within the operating range of their WLAN. Management decisions based on real-time information can significantly improve the efficiency of a worker.
- Low implementation costs WLANs are easy to set up, manage, change and relocate. Networks that frequently change can benefit from WLAN's ease of implementation. WLANs can operate in locations where installation of wiring may be impractical.
- Installation and network expansion by avoiding the complications of troublesome cables, a WLAN system can be fast and easy during installation, especially since it can eliminate the need to pull cable through walls and ceilings. Wireless technology provides more versatility by extending the network beyond the home or office.
- Inexpensive solution wireless network devices are as competitively priced as conventional Ethernet network devices. The DAP-2695 saves money by providing users with multi-functionality configurable in four different modes.
- Scalability Configurations can be easily changed and range from Peer-to-Peer networks, suitable for a small number of users to larger Infrastructure networks to accommodate hundreds or thousands of users, depending on the number of wireless devices deployed.

Wireless Installation Considerations

The D-Link Access Point lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

- 1. Keep the number of walls and ceilings between the access point and other network devices to a minimum. Each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
- 2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a
- 3. 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
- 4. Building Materials make a difference. A solid metal door or aluminum studs may have a negative effect on the range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
- 5. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
- 6. If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone in not in use.

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-2695. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows[®] XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

Why can't I access the web-based configuration utility?

When entering the IP address of the D-Link access point (192.168.0.50 for example), you are not connecting to a website on the Internet or have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:
 - Internet Explorer 7.0 or higher, Chrome, Firefox, or Safari 4 or higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows[®] firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.
- Configure your Internet settings:

Go to Start > Settings > Control Panel. Double-click the Internet Options Icon. From the Security tab, click the button to restore the settings to their defaults.

Click the Connection tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click OK. Go to the Advanced tab and click the button to restore these settings to their defaults. Click OK three times.

- Close your web browser (if open) and open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link access point in the address bar. This should open the login page for your the web management.
- If you still cannot access the configuration, unplug the power to the access point for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

What can I do if I forgot my password?

If you forgot your password, you must reset your access point. Unfortunately, this process will change all your settings back to the factory defaults.

To reset the access point, locate the reset button (hole) on the rear panel of the unit. With the access point powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the access point will go through its reboot process. Wait about 30 seconds to access the access point. The default IP address is 192.168.0.50. When logging in, the username is admin and leave the password box empty.

How to check your IP address?

After you install your network adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

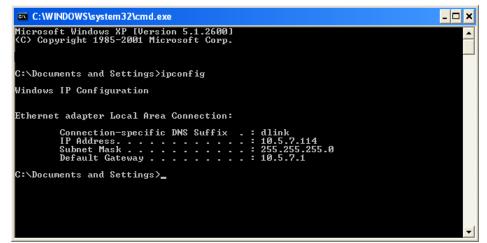
Click on Start > Run. In the run box type cmd and click OK.

At the prompt, type ipconfig and press Enter.

This will display the IP address, subnet mask, and the default gateway of your adapter.

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.

If you are connecting to a wireless network at a hotspot (e.g. hotel, coffee shop, airport), please contact an employee or administrator to verify their wireless network settings.



How to statically assign an IP address?

If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

Step 1:

Windows[®] 2000: Click on Start > Settings > Control Panel > Network Connections

Windows XP: Click on Start > Control Panel > Network Connections Windows Vista®: Click on Start > Control Panel > Network and Internet > Network and Sharing Center > Manage network connections

Step 2:

Right-click on the Local Area Connection which represents your network adapter and select Properties.

Step 3:

Highlight Internet Protocol (TCP/IP) and click Properties.

Step 4:

Click Use the following IP address and enter an IP address that is on the same subnet as your network or the LAN IP address on your router. Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.0.1). Set Primary DNS the same as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5:

Click OK twice to save your settings.

	automatically if your network supports ed to ask your network administrator fo				
🔘 Obtain an IP address autom	atically				
Ose the following IP addres	5.				
IP address:	192.168.0.52				
Subnet mask:	255 . 255 . 255 . 0				
Default gateway:	192.168.0.1				
Obtain DNS server address	automatically				
💿 Use the following DNS serv	er addresses:				
Preferred DNS server:	192.168.0.1				
Alternate DNS server:					
	Advanced.				

Technical Specifications

Standards

- IEEE 802.11ac
- IEEE 802.11n
- IEEE 802.11g
- IEEE 802.11a
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3ab
- IEEE 802.3at
- IEEE 802.3x

Network Management

- Web Browser interface (HTTP, Secure HTTP (HTTPS))
- AP Manager II
- SNMP Support (D-View Module, Private MIB)
- Command Line Interface (Telnet, Secure SSH Telnet)

Security

- WPA[™] Personal/Enterprise
- WPA2[™] Personal/Enterprise
- WEP[™] 64-/128-bit

Wireless Frequency Range

• 2.4 to 2.4835 GHz and 5.15 to 5.85 GHz**

Operating Voltage

• 48V/0.5A or 802.3af PoE

Antenna Type

- 3x Detachable 4 dBi Omni antennas @2.4GHz
- 3x Detachable 6 dBi Omni antennas @5GHz

LEDs

- Power
- LAN1 (PoE)
- LAN2
- 2.4 GHz
- 5 GHz

Temperature

- Operating: 0°C to 40°C
- Storing: -20°C to 65°C

Humidity

- Operating: 10%~90% (non-condensing)
- Storing: 5%~95% (non-condensing)

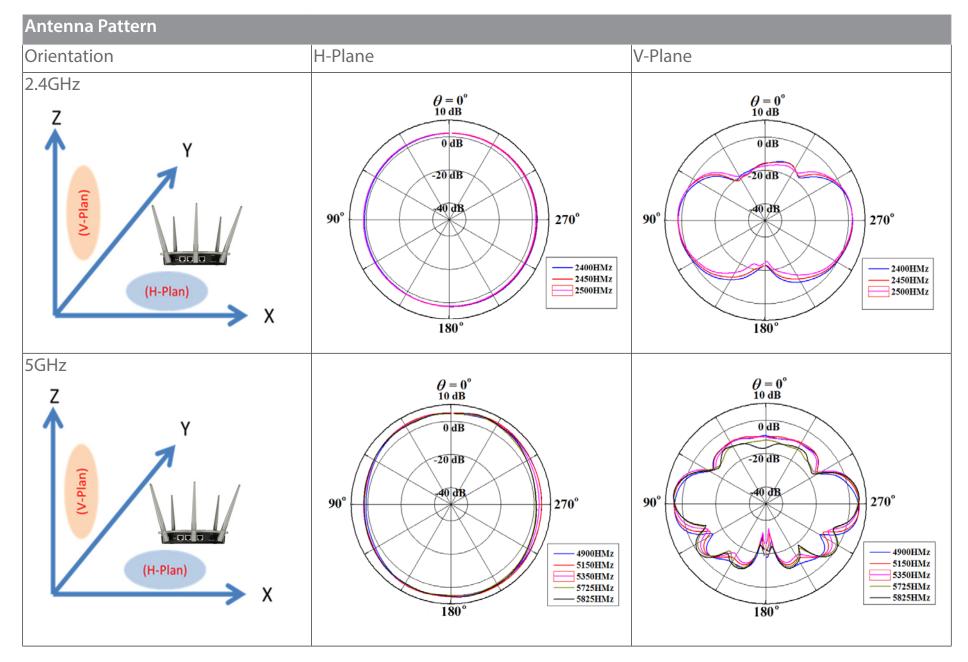
Certifications

- FCC Class B
- CE
- UL
- IC
- C-Tick
- CSA
- Wi-Fi

Dimensions

- L = 198.8 mm
- W = 190 mm
- H = 36.5 mm

Antenna Pattern



FREE Central WiFiManager Software

With the easy-to-use web-based interface you can...

- Configure once and apply to multiple Access Points
- Install on Windows PC
- Access on any device using a web-browser, e.g. smartphone or notebook
- Utilise user authentication and access control
- Monitor your entire wireless network in real time¹
- Access detailed reports
- Optimise your bandwidth



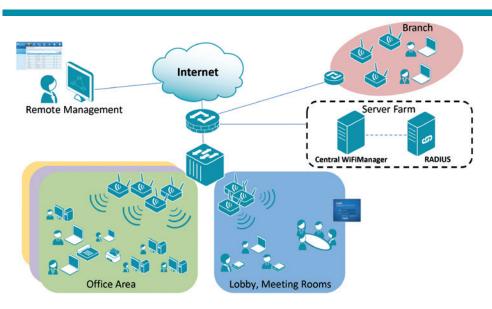
Connect to More www.dlink.com/wifidownload



DOWNLOAD

NOW

FREE Central WiFiManager



Available on the following products²:

DAP-2695

Wireless AC1750 Indoor Access Point Designed to support small to medium business or enterprise environments. Secure, manageable dual-band wireless LAN options.

DAP-2660

Wireless AC1200 Indoor Ceiling Access Point Providing enhanced speeds of Wireless AC as well as dual-band connectivity to reduce

connectivity to reduce interference, for a faster and more efficient network.



DAP-2310

Access Point

deployments.

Wireless N Indoor

Ideal for creating or

expanding capacity of a

wireless network; mainly

used in high-traffic areas

such as airports, coffee

shops, sports venues,

and university campus

DAP-2360

Wireless N PoE Access Point

For advanced indoor installations, this highspeed Access Point has integrated PoE support, allowing installation in areas where power outlets are not readily available.



DAP-2690

Wireless N Simultaneous Dual-Band PoE Access Point

Designed for indoor installation where power outlets are not readily available. Enables deployment of a highly manageable, robust and secure wireless network.



DAP-2330 Wireless N PoE

Access Point Ideal for wireless networks in high- traffic areas such as airports, coffee shops, shopping centres, sporting venues, hotels and campus deployments. PoE offers installation where power outlets are not available.





2. Visit dlink.com for selected Hardware & Software versions.

Connect to More www.dlink.com/wifidownload