Wireless Configuration

B/G Mode - Select if you want to include both 802.11b and 11g devices (**Mixed**), or only 802.11b (**B_only**), 802.11g (**G_only**) device in the network.

Wireless Radio - Select On of Off the radio wave.

Wireless Network Name (SSID) - The Service Set Identifier of the wireless network.

Channel - Allows you to manually choose a channel. It's only selectable when *Auto Channel Scan* is disabled.

Auto Channel Scan - Select this option to allow the channel to be decided automatically.

Super G Mode - Select this option to enable the wireless signal rate of up to 108Mbps. You can choose with or without Turbo mode. (**Note**: You can only choose Super G or B/G mode for AP, these two mode cannot be enabled at the same time.)

WMM - Select **Enable** of **Disable** the Wi-Fi Multimedia (WMM) function. Enabling this feature will improve the user experience for multimedia application if the wireless device supports WMM as well.

SSID Broadcast - Select Enable or Disable the broadcast of SSID.

Security - Select the security setting of the network. The available authentication mechanisms include:

Disable (default) WEP WPA

B/G Mode Wiveless Pedia	Mixed		
Wireless Network Name	dlink net		
(SSID) Channel	📑 🛊 🗹 Auto Channel Sca	n	
Super G Mode	Disabled	+	
WMM	💿 Enable 🕥 Disable		
SSID Broadcast	💿 Enable 🛛 🔿 Disable		
Security	Disable ≑		

WPA2

If you select **WEP** as the security type, additional columns will appear with following options.

Authentication - Select Open System or Shared Key to be used on the network.

WEP Encryption - Select the key size (64-bit. 128-bit, or 152-bit).

Default Key - Select which defined key is active on the network.

WEP-Key - Enter a string as the key.

If you select **WPA-PSK** or **WPA2-PSK** as the security type, additional columns will appear with following options.

Cipher Type - Select TKIP or AES.

Passphrase - Enter a string as the Passphrase.

Basic	Wireless Adva	nce MAC filter
B/G M	lode	Mixed 🗧
Wirele	ess Radio	⊙ On ○ Off
Wirela	ess Network Name	dlink_net
Chanr	, nel	🔲 🛊 🗹 Auto Channel Scan
Super	G Mode	Disabled
WMM	[💿 Enable 🕜 Disable
SSID	Broadcast	💿 Enable 🔘 Disable
Securi	ty	WEP
Aut	hentication :	💿 Open System 🛛 🔘 Shared Key
WE	P Encryption :	•
	Default Key :	Keyl
	WEP-Key:	

Basic Wireless Adva	nce MAC filter	
B/G Mode	Mixed 🜩	
Wireless Radio	⊙ On ⊖ Off	
Wireless Network Name (SSID)	dlink_net	
Channel	📄 🛊 🗹 Auto Channel Scan	
Super G Mode	Disabled	
WMM	💿 Enable 🕜 Disable	
SSID Broadcast	Enable Disable	
Security	WPA	
Cipher Type:	💿 TKIP 🔘 AES 🛛 PSK / EAP: 💿 PSK 🔘 EAP	
Passphrase :	Confirmed Passphrase :	

If you select **WPA-EAP** or **WPA2-EAP** as the security type, additional columns will appear with following options.

Cipher Type - Select TKIP or AES.

Radius Server 1 - Enter the IP address, port used, and the secret of the Radius server 1

Radius Server 2 - Enter the IP address, port used, and the secret of the Radius server 2

Advanced Configuration

Transmit Data Rates - Select the maximum wireless signal rate of the AP. Default is **Auto**.

Transmit Power - Select the transmit power of the AP. Default is 100%.

Beacon Interval - Beacon is the packet sent by an AP to synchronize a network. Specify the interval to send a beacon. Default is **100** micro seconds.

RTS Threshold - The RTS threshold is not recommended to be changed unless you encounter inconsistent data flow. The default value is **2346**.

Fragmentation - Specify the fragmentation threshold that packets exceeding it will be fragmented. Default is **2346** bytes.

DTIM - DTIM (Delivery Traffic Indication Message) is a countdown informing clients of the next listening window for broadcast and multicast messages. The default value is **1**.

Preamble Type - Select Short or Long preamble.

	vance MAC filter
3/G Mode	Mixed 🖨
Wireless Radio	⊙ On ◯ Off
Wireless Network Nam	e dlink net
Sand) Channel	📄 🛊 🗹 Auto Channel Scan
uper G Mode	Disabled
₩MM	• Enable O Disable
SID Broadcast	💿 Enable 🔵 Disable
ecurity	WPA2 💠
Cipher Type:	💿 TKIP 🔘 AES 🛛 PSK / EAP: 🔘 PSK 💿 EAP
ADIUS Server 1	
IP	Port 1812 Shared Secret
ADIUS Server 2	
'dlink_net:192.	168.1.105' configuration
'dlink_net:192. sic Wireless Adv	168.1.105' configuration
'dlink_net:192. sic Wireless Adv Transmit Data Rates	168.1.105' configuration ance MAC filter Auto
'dlink_net: 192. sic Wireless Adv Transmit Data Rates Transmit Power	168.1.105' configuration ance MAC filter Auto + 100% +
'dlink_net: 192. sic Wireless Adv Transmit Data Rates Transmit Power Beacon Interval	168.1.105' configuration ance MAC filter Auto + 100% + 100 (msec, range:20~1000)
'dlink_net: 192. sic Wireless Adv Transmit Data Rates Transmit Power Beacon Interval RTS Threshold	168.1.105' configuration ance MAC filter Auto * 100% * 100 (msec, range :20~1000) 2346 (range: 256~2346)
'dlink_net: 192. sic Wireless Adv Transmit Data Rates Transmit Power Beacon Interval RTS Threshold Fragmentation	168.1.105' configuration ance MAC filter Auto * 100% * 100 (mee, range:20~1000) 2346 (range: 256~2346) 2346 (range: 1500~2346)
'dlink_net: 192. sic Wireless Adv Transmit Data Rates Transmit Power Beacon Interval RTS Threshold Fragmentation DTIM	168.1.105' configuration ance MAC filter Auto \$ 100% \$ 100 (meec, range: 20~1000) 2346 (range: 256~2346) 2346 (range: 1500~2346) 1 (Range: 1~5)
'dlink_net: 192. sic Wireless Adv Transmit Data Rates Transmit Power Beacon Interval RTS Threshold Fragmentation DTIM Preamble Type	168. 1. 105' configuration ance MAC filter Auto * 100% * 100 (msec, range: 20~1000) 2346 (range: 256~2346) 2346 (range: 1500~2346) 1 (Range: 1~5) • Short Preamble Long Preamble
'dlink_net: 192. sic Wireless Adv Transmit Data Rates Transmit Power Beacon Interval RTS Threshold Fragmentation DTIM Preamble Type	168.1.105' configuration ance MAC filter Auto • 100% • 100 (maec, range: 20~1000) 2346 (range: 256~2346) 2346 (range: 1500~2346) 1 (Range: 1~5) • Short Preamble Long Preamble

Mac Filter Configuration

MAC Address - Add MAC addresses to the MAC Address Control List. Select an entry on the Address Control List and click **Delete** if you want to remove that Mac address.

Disable MAC Filters - Not filtering based on the Mac addresses.

Accept MAC Filters listed below to access - When it is selected, only devices with a Mac address in the list are granted access.

Reject MAC Filters listed below to access - When it is selected, only devices with a Mac address in the list are not granted access.

MAC address	bbA	
 Disabled MAC Filts Accept MAC addres Reject MAC address 	rs Delete s listed below to access listed below to access	
IAC Address Control L	st	
No.	MAC address	1 2
1	00:50:20:95:48:48	

Configure the Access Point by Group

In **Group**, user can configure a group template for multiple access points' use.

Create a Group Template

Click "Add Group" icon (^{>>}) and a window will appear:

Enter the group name and choose which APs you want to include in this group. You can also add APs after a group is created.

P Name	IP	MAC
AP_2	192.168.1.106	00:19:5B:45:BD:97
[AI_I	192.100.1.109	00.15.55.45.55.05

In the Wireless tab, you can choose if want to enable the **Load Balance** function, and other options. When configuring load balance, **SSID**, **User Number Limit**, **Security**, and **MAC Filter** must need to be specified as well.

When the load balance is enabled, once the number of clients connect to an AP has reached to the threshold, the new client can only join other APs with connection limits available.

Note: For detailed explanation for rest of Wireless, Advanced, and MAC Filter functions, please refer to section 3.2.2 through 3.2.4.

Basic	Wireless Advance	MAC filter
	LoadBalance Select	💿 Enable 🔵 Disable
	B/G Mode	\$
	Wireless Radio	On Off
	Wireless Network Name (SSID)	filink_net2
	Channel	📄 🖨 🔲 Auto Channel Scan
	Super G Mode	\$
	WMM Function	• Enable Disable
	SSID Broadcast	💽 Enable 💿 Disable
	User Number Limit	60
	Security	Disable 💠
		OK

Click "OK" when you are done. The template with access points will appear in the database column.

Note: If you choose to apply the configuration template to an AP, the AP will reboot.

29 29 29 29 29		
→ Øxxxx1 (2) Øxxx1 (2) Øxx1 (2)<		

Edit a Group Template

Click "Configure Group Template" icon (^{Sel}) and an edit window will appear:

Note: For detailed explanation for rest of Wireless, Advanced, and MAC Filter functions, please refer to section 3.2.2 through 3.2.4.

Click "OK" when you are done.

Note: Change a configuration template will cause all APs in the group to reboot.

Add AP: If you want to add a new AP to the template, just click the "Add AP to selected group" icon (^{Sel}) and a window will appear.

Virele	S Advance MAC filter	9				
	LoadBalance Select B/G Mode Wireless Radio Wireless Network Name (SSID) Channel Super G Mode WMM Function SSID Broadcast User Number Limit Security	 Enable Mixed On Imme Imme Enable Enable Enable Disable 	Disable	an ÷		
_				OK	С	ancel

Add Gro	oup Ap			0
Manage	ement AP	list		
AP Na	me	IP Address	MAC Address	
∎ AP_	2	192.168.1.106	00:19:5B:45:BD:97	
<u> </u>				
			ок	Cancel

Delete AP/Template: If you want to remove an AP from the group, or delete a template, just select the AP or template (the entry will be

highlighted in gray), and click "Delete Group/AP" icon (²¹); then a warning message will appear.

Or

Show AP Configuration: Click "Show AP Configuration" icon (^{Show}) to display the configuration of selected AP.



Management

Monitoring

The Monitor function allows user to view the wireless system status.

Monitoring AP and Wireless Switch by List

In **Monitor** \rightarrow **AP**, user can choose three different views. View by **List** lists the information of wireless access points in the database column. If a failure happens, the icon will change from online (\bigcirc) to failed (\bigcirc).

Following options are provided:

- 1. **Filter Type:** User can enable the filter to narrow down the database display by various attributes
- 2. **Filter:** After the *Filter Type* is chosen, user can select the specific content.
- 3. **Managed AP:** Check this option if you just need to see managed AP only
- 4. **Configuration (**^{SC)}: User can view or modify the selected AP's configuration
- 5. **AP Connection (**^{Sol}): It will redirect user to the selected AP's *Utilization* page.
- 6. Reload Previous Configuration (^{S)}: Allows user to reverse AP to the previous configuration.
- 7. Save to Database (¹): To add a newly found



AP to database.

- 8. Delete from Database (^{IIII}): To delete an AP from database.
- 9. **Customize** (^{SI}): Users can change the view by adding/deleting attributes according their needs.



10. Replace: Right click the selected AP and choose "Replace".



Monitoring AP and Wireless Switch by Topology

Choose to view by **Topology** in **Monitor** \rightarrow **AP** offers user to visualize the status of AP and wireless switch on the floor plan. After

importing the map, user can drag the icons to their locations. If a failure happens, the icon will change from online (

) to failed (or)

Following options are provided:

- 1. **Configuration (**Section 2): User can view or modify the selected AP's configuration.
- 2. Reload Previous Configuration (^{Sel}): Allows user to reverse AP to the previous configuration.
- 3. Save to Database (¹): To add a newly found AP to database.
- 4. **Delete from Database (**): To delete an AP from database.
- 5. Save Topology Position (^{Leg}): To reserve the location user set for AP and wireless switch; otherwise it will return to the default when the Smart WLAN manager restarted.
- 6. **Zoom In (**): User can get a closer look of the floor plan.
- 7. Zoom Out (): User can choose to see the topology overview.



8. Load Map (^[S]): Import the picture file as the floor plan file. The file types supported are BMP, DIB, EMF, GIF, ICO, JPG, and WMF.



- 9. **Remove Map (**^[1]): Remove the current floor plan.
- 10. **Modify Map** (¹¹): User can resize the picture by pixels, and can preview before taking efforts. Rotation can also be done for appropriate view.

Preview	
	Width 884 pixels
61533585313	Height 571 pixels
	Preview
PENKNENEN R	
	Rotate
	Rotate Left Rotate Right

<u>Monitoring Clients</u> In Monitor \rightarrow Client, user can see the status of wireless clients connected.

Following options are provided:

- 1. Filter Type: User can enable the filter to narrow down the database display by various attributes
- 2. Filter: After the Filter Type is chosen, user can select the specific content.

D-LINK Smart WLAN Mar	neger						000
Servieni Idevi Tools Loo	Help						
< 1 H H & O A		8					
Se Maniter	Filler Type :		Risc		Clean Filter		
C AP		193212		Carlo Halen		19.4	
E. Client	AT_1	8018 SP45 ED 8D	1801991109	06130839281	30	grade	
🚬 Summary							
👉 Group							
🚰 Utilization							
👔 Firmware Upgrade							
100 King							
🖳 Switch Dissover Utility							
	-						

Monitoring Summary

In **Monitor**→**Summary**, a summary window will appear to provide following information:

Summary	0
Total AP	2
Managment AP	2
New AP	0
Load balance enable AP	0
Current Client	1
Last Polling Time:	2007.02.04 19:17:19
	OK

AP Status and Trouble Shooting

Status	List view	Tree view	Topology view	Description/Trouble shooting	Remark
Normal online AP				An AP links and works properly in the network.	
Changed AP				 A known AP which configuration has been changed. You can reload the original setting or save the current setting by: 1. Reload: double click to Reload old configuration, or 2. Save: press the save current 	
New AP				A new AP was discovered by WLAN Manager.	
Offline AP		6		 An existing AP lost the connection 1. Check the status of the connected switch and ensure the switch is online 2. Cold start the AP from the switch webpage 3. Cold start the AP detached the wire reconnected to switch 4. Factory reset 	Please check "Appendix" to do "Cold Start" and "Factory Reset".
Replaced AP				A existing AP was replaced by a new AP You can reverse AP to the previous configuration or save the current setting: Replace: double click to reverse the previous configuration Save: press the save current status	
DHCP error		₹;	-	 A AP cannot get IP from the DHCP server 1. Make sure the DHCP server for the AP is available. 2. If the DHCP server did not connect, please reconnect the DHCP server and wait about 60 seconds, then press the start polling from WLAN manager 3. If the DHCP server was connected, you can try any one of following methods: a. Cold start the AP from the switch webpage and Restart Shutdown the POE from switch. b. Cold start by the reconnected AP. c. Factory reset. d. Restart the port from web. 	Please check "Appendix" to do "Cold Start" and "Factory Reset".
Anti rogue key error		1	*	The Anti Rouge AP function of switch was enabled, but the key of AP and switch is not matched The AP key is different with connected switch, to active the system key manager Solution, you can try any one of following methods:	

				 Select the all managed system key Error Device All managed device change to same system key Disable the anti rouge function from switch 	
				4. Factory reset the AP and switch	
		_		 VVLAN Manager can discover AP successfully but cannot get configuration from AP correctly. Possible problems: 1. Password error: Delete the troubled AP and run discovery wizard to find 	
Not available				the AP again, make sure the password is correct before discover the AP.	
				2. Different subnet; change the management PC subnet and to,	
				a. Iry to cold start the AP by web, or	
				D. Thy to factory feset	
Unknown device		3		Unknown network devices	
Switch on line		1	and the second	The DES-1228P switch links and works properly in the network.	
				The existing DES-1228P lost the connection	
Switch offline		*	and the same same same	 Check the switch power, Check SNIMP community and cable and subnet 	
				3. factory reset the switch	
New Switch			a la	A new DES-1228P switch was discovered by WLAN Manager.	
Group apply AP				The AP setting is same with group setting	
Group not apply	8			The AP setting is different with group setting	

Note: If the discover utility can't find any switch or AP, please ensure there is only one NIC(network interface card) in your PC, multiple NIC may make the system work abnormally.

Utilization

In Utilization, user can monitor four different statistics by graphic reports.

Utilization>AP Users

It allows user to see the connected client numbers of an access point. You can select the display type by **Hour**, **Day**, or **Week**. The supported file format for exporting includes CSV and PDF.



<u>Utilization → AP Traffic</u>

It allows user to see the traffic volume of an access point in bytes. You can select the display type by **Hour**, **Day**, or **Week**. The supported file format for exporting includes CSV and PDF.



<u>Utilization→Client Info.</u>

It allows user to see the status history of a wireless client. The supported file format for exporting is CSV.

Manitor	Regin 2007/ 2/ 3 1	TE0.0213 64	907/ 2/ 4 💌	74.032	<u>स</u> क	11110	Espot	95		
Crosp Crosp Crosp Crosp Cross	510401146C A4, 001500148204	Dee_Poing 2011/2011 19:049 2011/2011 19:049 2011/2011 19:249 2011/2011 19:249 2011/2011 19:249 2011/2011 19:229	Olencular connect connect connect deconnect connect	R59 12 11 17 12 8	Mode g. vode g. vode g. vode g. vode g. vode	ΔΡ.Νκνκ ΑΡ.1 ΑΡ.1 ΑΡ.1 ΑΡ.1 ΑΡ.1 ΑΡ.1 ΑΡ.1	5500 Brid, tot Brid, tot Brid, tot Brid, tot	4P_M4C 081958458 081958458 081958458 081958458 081958458 081958458	APJP 1921681106 1921681106 1921681108 1921681108 1921681108	
Status Uninsun Davice Uninsun Davice Uninsun Davice Uninsun AP E E E E E E E E E E E E E E E E E E E	001764 T + 17 3 3014 (201764 T + 17 3 3014) (201764 T + 17 3 3014) (201764 T + 17 3 3010) (201764 T + 17 3 3010) (201764 T + 17 3 3310) (201764 T + 17 3 3310)	2 21 00 1958 4580 971 0 1 00 1958 4580 971 0 1 00 1958 4580 00 20 00 1958 4580 07 21 00 1958 4580 97 21 00 1958 4580 97 21 00 1958 4580 97 21 00 1958 4580 97	92 109 1,100 oc 92 109 1,105 oc 92 100 1,105 w 92 100 1,105 w 92 100 1,100 oc 92 100 1,100 oc 92 100 1,100 oc	lice Sala dos austrito "a foca antico "a foca antico "a foce lice	consil" ndigenton charg et ovelable"	₽4 ⁷				
Summing time to sector ling in	System Log Action L									CAP SUM

Utilization→**Load Balance**

It allows user to see the status of a load balance group. You can select the display type by **Hour**, **Day**, or **Week**. The supported file format for exporting is CSV.



Firmware Upgrade

The Smart WLAN Manager allows user to upgrade multiple devices' firmware all at once. To select a single device, just click on the device you want to select. To select multiple devices, hold down the **Ctrl** key while clicking on each additional device. To select an entire list, hold down the **Shift** key, click on the first device and then click on the last device on the list.

To upgrade the firmware by following steps:

- 1. Change to theon view by AP or switch.
- 2. Select the new image file by clicking "Browse" icon.
- 3. Select the devices
- 4. Select "Upgrade".

After firmware downloaded and upgraded, the device will reboot to complete the procedure.

Status None IP MAC SSD Chernel Firmware Venion Online AP_1 192.168.1.105 00.13.58.45.60 state_met 1 1.00.0014 Online AP_2 192.168.1.105 00.13.58.45.80 state_met 11 1.00.0014 Online AP_2 192.168.1.105 00.13.58.45.80 state_met 11 1.00.0014
Сонсти АР_1 192.168.1105 00.19.58.45.80 швиж _{стин} I 100.0014 Сонсти АР_2 192.168.1106 00.19.58.45.80 швиж _{стин} II 100.0014
Contras AP_2 192168,1106 00.1958-45.80 ulinit_met 11 1.00.0014

Log

The Smart WLAN Manager offers two kinds of log: Action Log and System Log. User can save logs by using Log \rightarrow Save Log As, and load a saved log by using Log \rightarrow Open Log. Log \rightarrow Clear Log allows user to clear all the records not saved.

Action Log records all actions user has made. It allows user to filter the log by **Date/Time** or **Description**.

In the following example, user chooses the type

"Description", enters "Group", and click " ". The filtered results are shown as below. To remove a filter, just delete the string entered and click ".

System Log records all system events happened. User can choose to display by levels he/she is interested in. Filtering can be used for System Log as well.

Log Type: Action Log 💠 Filter Type: Date/Time	◆ Filter: ◆ ◆ ● ● ₹ 1/1
Date/Time	Description
2007/2/4 下午 07:33:27	Save AP properties
2007/2/4下午 07:33:27	delete filter mac (0015004820ff) from AP 192.168.1.106(00:19:58:45:BD:97) success
2007/2/4 下午 07:33:27	set AP 192.168.1.106[00:19:58:45:BD:97] mac control filter to only allow success
2007/2/4 下午 07:33:27	set AP 192,168,1,106[00;19:58;45:BD:97] cts mode to auto success
2007/2/4 下午 07:33:27	set AP 192.168.1.106[00:19:58:45:BD:97] preamble type to short success
2007/2/4 下午 07:33:27	set AP 192.168.1.106[00:19:58:45:BD:97] dtim interval to 1 success
2007/2/4下午 07:33:27	set AP 192.168.1.106[00:19:58:45:BD:97] fragmentation to 2346 success
2007/2/4 下午 07:33:27	set AP 192.168.1.106[00:19:5B:45:BD:97] rts threshold to 2346 success
2007/2/4 下午 07:33:27	set AP 192.168.1.106[00:19:58:45:BD:97] beacon interval to 100 success
2007/2/4 下午 07:33:27	set AP 192.168.1.106[00:19:5B:45:BD:97] transmit power to 100% success
2007/2/4 下午 07:33:27	set AP 192.168.1.106[00:19:58:45:BD:97] tx rates to Auto success
2007/2/4 下午 07:33:27	
2007/2/4 下午 07:33:27	set AP 192.168.1.106[00:19:58:45:BD:97] wep64Key1 to 1234567890 success
2007/2/4下午 07:33:27	set AP 192.168.1.106[00:19:5B:45:BD:97] wep152 default Key to key1 success
2007/2/4 下午 07:33:27	set AP 192.168.1.106[00:19:58:45:BD:97] wep128 default Key to key1 success
2007/2/4下午 07:33:27	set AP 192.168.1.106[00:19:5B:45:BD:97] wep64 default Key to key1 success
2007/2/4 下午 07:33:27	set AP 192.168.1.106[00:19:58:45:8D:97] security type to wep-64bits-share success
2007/2/4下午 07:33:27	set AP 192.168.1.106[00:19:5B:45:BD:97] ssid broadcast to enable success
2007/2/4下午 07:33:27	set AP 192.168.1.106[00:19:58:45:8D:97] wmm function to enable success
2007/2/4下午 07:33:27	set AP 192.168.1.106[00:19:5B:45:BD:97] superg to disabled success
2007/2/4下午 07:33:27	set AP 192.168.1.106[00:19:58:45:8D:97] ssid to dlink_net success
2007/2/4下午 07:33:27	set AP 192.168.1.106[00:19:5B:45:BD:97] wireless radio to on success
2007/2/4下午 07:33:27	set AP 192.168.1.106[00:19:58:45:BD:97] bg mode to b/g success
2007/2/4下午 07:33:27	set AP 192.168.1.106[00:19:5B:45:BD:97] location to 5F_Right success
2007/2/4下午 07:33:27	set AP 192.168.1.106[00:19:58:45:BD:97] trap host to 0.0.0.0 success
2007/2/4 下午 07:33:27	set AP 192.168.1.106[00:19:58:45:BD:97] user limit to 60 success
2007/2/4下午 07:33:27	set AP 192.168.1.106[00:19:5B:45:BD:97] name to AP_2 success
2007/2/4 下午 07:33:27	set AP 192.168.1.106[00:19:58:45:BD:97] ip type to dhop success
2007/2/4 下午 07:33:12	set AP 192.168.1.106[00:19:58:45:BD:97] channel to 0 fail
2007/2/4下午 07:31:51	apply Group1 template to AP 192.168.1.105[00:19:5B:45:BD:8D] success
2007/2/4 下午 07:31:50	apply Group1 template to AP 192.168.1.106[00:19:58:45:8D:97] success

Log Type: Action Log 🔹 Filler Type: Description	n 🛊 Filet Group 📫 🖌 K 4 () () 🖏 121
Dats/Time	Description
2007/2/4 下午 07:31:51	apply Group1 temptate to AP 192 168 1.105(00.19:58:45:60; 80] success
2007/2/4 7 7 07:31:50	apply Group1 template to AP 132 168 1.106(00:19/58 45/80:39) success

Level Image: Transmission of the state of	
Date/Time Level Description 2007/244 TPF 07:3357 Cabcat JAP_2[100:1959:4580:97][192:1681.106] online 2007/244 TPF 07:3357 Cabcat JAP_2[100:1959:4580:97][192:1681.106] online 2007/244 TPF 07:3333 Cabcat JAP_2[100:1959:4580:97][192:1681.106] online 2007/244 TPF 07:3333 Cabcat JAP_2[100:1959:4580:97][192:1681.106] online 2007/244 TPF 07:3230 Debug JAP_2[100:1959:4580:97][192:1681.105] others in certe to "non-addate" 2007/244 TPF 07:3238 Debug JAP_2[100:1959:4580:80][192:1681.105] others in certe to "non-addate" 2007/244 TPF 07:3238 Debug JAP_2[100:1959:4580:80][192:1681.105] others in certe to "non-addate" 2007/244 TPF 07:3238 Debug JAP_2[100:1959:4580:80][192:1681.105] others in certe to "non-add" 2007/244 TPF 07:3238 Debug JAP_2[100:1959:4580:80][192:1681.105] others in certe to "non-add"	
2007/24/TF 07:3257 Cabical VP_2[1](0:1958 vf580 vf2[1]152:1681.106] online 2007/24/TF 07:3379 Cabical VP_2[1](0:1958 vf580 vf2[1]152:1681.106] online 2007/24/TF 07:3379 Cabical VP_2[1](0:1958 vf580 vf2[1]152:1681.106] online 2007/24/TF 07:323 Debug VP_2[1](0:1958 vf580 vf2[1]152:1681.106] online 2007/24/TF 07:323 Debug VP_2[1](0:1958 vf580 vf2[1]152:1681.105] online	
2007/24/FT (7:333) Critical (µP_2)[100:1968:4560:971_105:1681.106] offene 2007/24/FT (7:333) Debug (µP_2)[100:1969:8190:971_1152:1681.106] offene 2007/24/FT (7:333) Debug (µP_2)[100:1969:8190:971_1152:1681.106] offene 2007/24/FT (7:323) Debug (µP_2)[100:1969:8450:971_1152:1681.106] offene 2007/24/FT (7:323) Debug (µP_2)[100:1989:8450:971_1152:1681.106] offene 2007/24/FT (7:323) Debug (µP_2)[100:1989:8450:971_1152:1681.106] offene 2007/24/FT (7:323) Debug (µP_2)[100:1989:8450:91][132:1681.106] offene	
1907/24 17年 07:33:23 Debug IAP_2[100:1959:45580.97[1192:1681.106]status is set to "inot available" 1907/24 17年 07:32:30 Debug IAP_2[100:1959:45580.97][113:1681.106]status is set to "configuration changed" 1907/24 17年 07:32:38 Debug IAP_1[100:1959:45680.00][152:1681.105]status is set to "noned" 1907/24 17年 07:32:38 Calcul IAP_1[100:1959:4560.80][152:1681.105]andime	
1007/241千年(07:32:30 Debug) P.Z.[[10:1968,47500 37][19:2561.105] (How is vet to "configuration charged" 1007/241千年(07:32:38 Debug) P.T.[[10:1959,47500 30][19:21681.105] (How is vet to "normal" 10:7/241千年(07:32:38 Calcul) P.T.[[10:1959,45503 30][19:21681.105] (How is vet to "normal"	
1007/2/4 7半 07:32:38 Debug (AP_11_00:19:58:45:80:3D は1132:168.1.105) status is set to "nonad" 1007/2/4 7半 07:32:38 Catical (AP_11_00:19:58:45:80:3D は1132:168.1.105) online	
807/2/4 下午 07:32:28 Catical JAP_1L[00:19:58 #58D:80 L[19:21 68:1:105] online	
007/2/4 平平 07:32:28 Critical AP_21_00:1958 /680 97L[192:1681.106] online	
207/2/4 下午 07:32:12 Calical JAP_11_00:19:58:45:80:80_[192:168.1.105] office	
2007/2/4 平午 07:31:57 Debug [AP_11_(00:18:58):45:80 30 L[192:168.1.105] of stunits or efficient and a statistical of the statis	
2007/2/4 T/+ 07:31:55 Cilical [AP_2]_00:19:58 45:80 37[_192:1681.106] office	
2007/2/4 T ≠ 07:30:47 Debug IAP_2_000.19/98-45/80.37_(192.1681.106] Matus IX det to "configuration changed"	

APPENDIX

Cold Start the AP:

Please follow the instructions below to *cold start* your AP from DES-1228P switch Web UI:

- 1. Connect to the Switch configuration Web page about PoE port Settings
- 2. Select the AP connected port at switch, from port and to port and disable the PoE_Enable
- 3. Press "Apply" button and wait few seconds
- 4. Select the "From Port" and "To Port" and enable the PoE_Enable and wait about 1 minute
- 5. Active the WLAN Smart Manager and press start polling from toolbar

Tools -		_	_						2		
VES-1 228P ∭System	PoE Po	PoE Port Settings							0 Safeguard		
Gonfgaration Gonfgaration Gonfgaration Gonfgaration Gonfgaration Gonfgaration Gonfgaration Gonfgaration Gonfgaration	From Part	To Par	nt Po	E_Enable Disable:	Power limit Auto	*	Apply Refresh				
006	Pott	PoE Enable	Power limit	Power(M)	Votage(v)	Current(mA)	Classification	Status			
bio balan	01	Enabled	Auto	0.00	0.00	0.00	+	Nomial			
monorary	02	Enabled	Auto	0.00	0.00	0.00		Normal	1		
	03	Enabled	Auto	0.00	0.00	0.00	+	Normal	1		
	04	Enabled	otuA	0.00	0.00	0.00		Normal	1		
	85	Enabled	Auto	0.00	0.00	0.00	*	Normal	1		
	06	Enabled	Auto	0.00	0.00	0.00		Normal	1		
	07	Enabled	Auto	0.00	0.00	0.00		Normal	1		
	08	Enabled	Auto	0.00	0.00	0.00		Normal	1		
	09	Enshied	Auto	0.00	0.00	0:00	*	Normal	1		
	10	Enabled	Auto	0.00	0.00	0.00	τ.	Normal	1		
	11	Enshied	Auto	0.00	0.00	0.00	*	Normal	1		
	12	Enabled	Auto	0.00	0.00	0.00	τ	Normal	1-		
	13	Enabled	Auto	0.00	0.00	0.00	*	Normal			
The second se	14	Enabled	Auto	0.00	0.00	0.00	τ	Normal			
and the second s	15	Enabled	Auto	0.00	0.00	0.00		Normal	1		
	16	Enabled	Auto	0.00	0.00	0.00	τ	Normal			
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	17	Enabled	Auto	0.00	0.00	0.00	•	Normal			

Factory reset

Please follow the 2 steps for factory reset:

- 1. Reset the DWL-3140 AP to its factory default settings.
- 2. Restore the other devices on your network to their default settings, by pressing the Reset button on the top of the unit. Please note you will lose the current configuration settings by doing so.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Industry Canada statement:

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.