

HowTo: Setup Captive Portal DWC-1000 C1-Revision

[Requirements]

1. DWC-1000 with firmware 4.7.0.x and later

2. compatible AP with latest firmware (DWL-2600AP, DWL-3600AP, DWL-3610AP, DWL-6600AP, DWL-6610AP, DWL-6610APE, DWL-6620APS, DWL-7620AP, DWL-8600AP, DWL-8610AP, DWL-8610AP, DWL-8710AP)

3. fully configured and created VLAN and routing setup of your network

4. all APs are already configured for MultiSSID

For a correct CP-redirect and routing over the firewall it is mandatory that the DWC-1000 can't use Layer 3 VLAN interface for the CP-wireless. Otherwise the DWC-1000 will act as a router, so that there is not redirect at all.

[Topology]





[setup] 1.) L2 VLAN-Interface for CP-SSID

Network » VLAN » VLAN Settings										
The router supports virtual network isolation on the LAN with the use of VLANs. LAN devices can be configured to communicate in a subnetwork defined by VLAN identifiers.										
VLAN List										
Show 10	Show 10 v entries [Right click on record to get more options]									
Name 🗘	VLAN ID 😔	VLAN Type 🛛 😌	IP Address 😔	Subnet Mask ⊖	Captive Portal ⊖	Authentication Server Θ				
Default	1	VLAN (L3)	192.168.0.10	255.255.254.0	Free	None				
GuestWLAN	2	VLAN (without IP interface)	NA	NA	NA	NA				
Showing 1 to 2	Showing 1 to 2 of 2 entries 1 Next > Last >									
Add New \	/LAN									

2.) Default-Route & DNS at the DWC-1000 for routing

Network » LAN » LAN Settings

The LAN Configuration page allows you to configure the LAN interface of the router including defaul DHCP Server which runs on it and Changes here affect all devices connected to the router's LAN swi change to the LAN IP address will require all LAN hosts to be in the same subnet and use the new ac

AN Settings	
LAN Ping	
Allow Ping from LAN	ON
IP Address Setup	
IP Address	192.168.0.10
Subnet Mask	255.255.254.0
DHCP Setup	
DHCP Mode	None 🗸
Default Route	
Enable Default Route	III III
Gateway	192.168.0.9
DNS Server	8.8.8
SNAT	OFF



3.) Port-VLAN

Network » VLAN » Port VLAN

This page allows user to configure the port VLANs. A user can choose ports and can add them into a VLAN. In ore specific LAN port with a VLAN ID, you can associate a VLAN to a physical port. The VLAN Port table displays the that port and VLAN membership information. Go to the Available VLAN page to configure a VLAN membership that

Port VLANs List

Port Name	☆ Mode	⇔	PVID	⇔	VLAN Membership
Port1	General		1		1,2
Port2	Access		2		2
Port3	Access		1		1
Port4	Access		1		1

4.) SSID Profile VLAN & Captive Portal

SSID Configuration	
SSID	GuestWLAN
Captive Portal Type	Temporary User 🗸
Enable Redirect	OFF
Captive Portal Profile	
Choose Profile	Login Profile O Custom Profile
Login Profile Name	testcp Create a Profile
Captive Portal SLA Profile	
SLA Login Profile Name	default Create a Profile
Hide SSID	OFF
VLAN	2 Range: 1 - 4093]
MAC Authentication	O Local O Radius O Disable
Window ADD Commencies Made	

5.) Interfaces Watchguard XTM520

INTERFACE *	NAME (ALIAS)	ТҮРЕ	IPV4 ADDRESS	IPV6 ADDRESS	NIC CONFIG
0	External	External	192.168.10.37/24		Auto Negotiate
1	Trusted	Trusted	192.168.0.9/23		Auto Negotiate
2	Trusted_GUEST	Trusted	192.168.111.9/24		Auto Negotiate



6.) Firewall rules on XTM520

WatchGuard	Fireware Web	UI							
DASHBOARD SYSTEM STATUS	Policies	ADD POLICY							Filter
FIREWALL	ORDER 🗘	ACTION	POLICY NAME	ТҮРЕ	FROM	то	PORT	PBR	APP CONTROL
Firewall Policies	1	۲	ETP-proxy	FTP-proxy	Any-Trusted, Any-Optional	Any-External	tcp:21		
Mobile VPN IPSec Policies	2	٢	PHTTP-proxy	HTTP-proxy	Any-Trusted, Any-Optional	Any-External	tcp:80		
Aliases	3	٢	HTTPS-proxy	HTTPS-proxy	Any-Trusted, Any-Optional	Any-External	tcp:443		
Proxy Actions Traffic Management	4	~	WatchGuard Web UI	WG-Fireware-XTM-WebUI	Any-Trusted, Any-Optional, An	y-E Firebox	tcp:8080		
Scheduling	5		DNS	DNS	Any-Trusted, Any-Optional	Any-External	tcp:53 udp:53		Port 80 & 443 are
SNAT	6	~	CP_HTTP_HTTPS_DWC1k	test	192.168.111.0/24	192.168.0.10	tcp:443 tcp:80		required for CP redirect to IP Interface
Blocked Sites	7	~	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Optional	Firebox	tcp:4105 tcp:4117 tcp:4118		of DWC-1000
Blocked Ports	8		Outgoing	TCP-UDP	Any-Trusted, Any-Optional	Any-External	tcp:0 udp:0		
Quotas SUBSCRIPTION SERVICES	9	×	Any-Deny-CP	Any	192.168.111.0/24	192.168.0.0/23	Any		deny any other access
UTHENTICATION	10		Ping	Ping	Any-Trusted, Any-Optional	Any	ICMP (type: 8, code: 255)		from guest-network to internal network
/PN	11	~	Any-CP-OUT	Any	192.168.111.0/24	Any-External	Any		grand internet access
YSTEM	MOVE UP	MOVE DOWN	SAVE POLICY ORDER						to guest-network

Depending on your firewall, you might need to change the orders of the rules. Please contact your firewall vendor about this.