User Manual

Wireless Controller

D-Link Corporation

http://www.dlink.com

User Manual

DWC-1000
Wireless Controller
Version 3.01

Copyright Notice

Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

Limitations of Liability

UNDER NO CIRCUMSTANCES SHALL D-LINK OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE D-LINK PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF D-LINK IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, D-LINK WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. D-LINK WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT D-LINK RECEIVED FROM THE END-USER FOR THE PRODUCT.

Table of Contents

List of Figures

Chapter 1. Introduction

D-Link Wireless Controller (DWC), DWC-1000, is a full-featured wireless LAN controller designing for small network environment. The centralized control function contains various access point management functions, such as fast-roaming, inter-subnet roaming, automatic channel and power adjustment, self-healing etc. The advanced wireless security function, including rouge AP detection, captive portal, wireless intrusion detection system (WIDS), offers a strong wireless network protection avoiding attacks from hackers. After license upgrade optimal network security is provided via features such as virtual private network (VPN) tunnels, IP Security (IPsec), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and Secure Sockets Layer (SSL). Empower your road warriors with clientless remote access anywhere and anytime using SSL VPN tunnels.

There are three types of licenses available to activate increased functionality for the DWC. These licenses are not activated by default.

1. **VPN license** upgrade enables the following features: ISP Connection types (PPPoE, PPTP, L2TP, NAT/Transparent mode), Option2/DMZ port, IP Aliasing, Dynamic Routing (RIP), VPN (PPTP client/server, L2TP client /server , SSLVPN, OpenVPN) , Intel AMT, Dynamic DNS, Website Filter, Application Rules, Firewall Rules, UPNP, IGMP proxy, and ALG/SMTP-ALG
2. **AP license** upgrades the number of APs controller can manage. You can upgrade up to 3 AP licenses. By default DWC-1000 can manage up to 6 AP's. You increase the number by 6 upon each AP license.
3. **WCF License** is a powerful dynamic web filtering function that can be used in many places. It is ideal for companies that want to ensure that employees aren't wasting time online, schools that want to prevent their students from viewing questionable online material, or libraries and small businesses like coffee stores that want to limit customers from accessing certain sites on their network. You can filter up to 32 categories of websites in total, such as pornography, gambling, online shopping, and many others. You can easily block or unblock these categories in just a few clicks. The dynamic WCF also has a logging feature. Whenever a user tries to access a website that is

blocked, or the time stamp of login/logout, the corresponding event will be logged.

1.1 About this User Manual

This document is a high level manual to allow new D-Link Wireless Controller users to configure connectivity, WLAN configuration, setup VPN tunnels, establish firewall rules and AP management and perform general administrative tasks. Typical deployment and use case scenarios are described in each section. For more detailed setup instructions and explanations of each configuration parameter, refer to the online help that can be accessed from each page in the controller GUI.

> ✍ For this user manual all screenshots are taken with an activated VPN license which enables VPN / Firewall features.

1.2 Typographical Conventions

The following is a list of the various terms, followed by an example of how that term is represented in this document:

- Product Name: D-Link Wireless Controller
    - Model number: DWC-1000
- GUI Menu Path/GUI Navigation – ***Monitoring > Controller Status***
- Important note – ✍

Chapter 2. Configuring Your Network

To enable management access for the browser based web GUI access or SNMP manager, you must connect the controller to the network. The default IP address/subnet mask of the controller management interface is **192.168.10.1** / **255.255.255.0** and DHCP server on the LAN is disabled by default on the controller. You must connect the controller to a **192.168.10.0** network.

After you configure network information, such as the IP address and subnet mask, and the controller is physically and logically connected to the network, you can manage and monitor the controller remotely through Web browser, or an SNMP-based network management system. Once the initial setup is complete, the DWC-1000 can be managed through wired interface connected to controller.

> ✍ Access the controller’s GUI for management by using any web browser, such as Microsoft Internet Explorer or Mozilla Firefox.

Go to **http://192.168.10.1** (default IP address) to display the controller’s management login screen.

Default login credentials for the management GUI:

- Username: **admin**
- Password: **admin**

> ✍ If the controller’s LAN IP address was changed, use that IP address in the navigation bar of the browser to access the controller’s management UI.

2.1 LAN Configuration

Setup > Network Settings > LAN Setup Configuration

By default, in the controller the Dynamic Host Configuration Protocol (DHCP) mode is set to “None”. The DHCP mode can be set as a DHCP server or DHCP relay. When DHCP mode is DHCP server, the controller functions as a DHCP server to assign IP address leases to hosts on the WLAN or LAN. With DHCP, PCs and other LAN devices can be assigned IP addresses, the default gateway, as well as addresses for DNS servers, Windows Internet Name Service (WINS) servers. The PCs in the LAN are assigned IP addresses from a pool of addresses specified in this procedure. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications the default DHCP and TCP/IP settings are satisfactory. If you want another PC on your network to be the DHCP server or if you are manually configuring the network settings of all of your PCs, set the DHCP mode to 'none'. DHCP relay can be used to forward DHCP lease information from another LAN device that is the network's DHCP server; this is particularly useful for wireless clients.

Instead of using a DNS server, you can use a Windows Internet Naming Service (WINS) server. A WINS server is the equivalent of a DNS server but uses the NetBIOS protocol to resolve hostnames. The controller includes the WINS server IP address in the DHCP configuration when acknowledging a DHCP request from a DHCP client.

You can also enable DNS proxy for the LAN. When this is enabled the controller then as a proxy for all DNS requests and communicates with the ISP's DNS servers. When disabled all DHCP clients receive the DNS IP addresses of the ISP.

To configure LAN Connectivity, please follow the steps below:

1. In the LAN Setup page, enter the following information for your controller:

IP address: (factory default: 192.168.10.1).

> ✍ If you change the IP address and click Save Settings, the GUI will not respond. Open a new connection to the new IP address and log in again. Be sure the LAN host (the machine used to manage the controller) has obtained IP address from newly assigned pool (or has a static IP address in the controller's LAN subnet) before accessing the controller via changed IP address.

Subnet mask: (factory default: 255.255.255.0).

2. In the DHCP section, select the DHCP mode:

None: the controller's DHCP server is disabled for the LAN

DHCP Server. With this option the controller assigns an IP address within the specified range plus additional specified information to any LAN device that requests DHCP served addresses.

If DHCP is being enabled, enter the following DHCP server parameters:

DHCP Relay: With this option enabled, DHCP clients on the LAN can receive IP address leases and corresponding information from a DHCP server on a different subnet. Specify the Relay Gateway, and when LAN clients make a DHCP request it will be passed along to the server accessible via the Relay Gateway IP address.

Starting and Ending IP Addresses: Enter the first and last continuous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address in this range. The default starting address is 192.168.10.100. The default ending address is 192.168.10.254. These addresses should be in the same IP address subnet as the controller’s LAN IP address. You may wish to save part of the subnet range for devices with statically assigned IP addresses in the LAN.

Default Gateway (Optional): Enter the IP address of the controller which you want to make it as a default other than DWC-1000

Primary and Secondary DNS servers: If configured domain name system (DNS) servers are available on the LAN enter their IP addresses here.

Domain Name: Enter domain name

WINS Server (optional): Enter the IP address for the WINS server or, if present in your network, the Windows NetBios server.

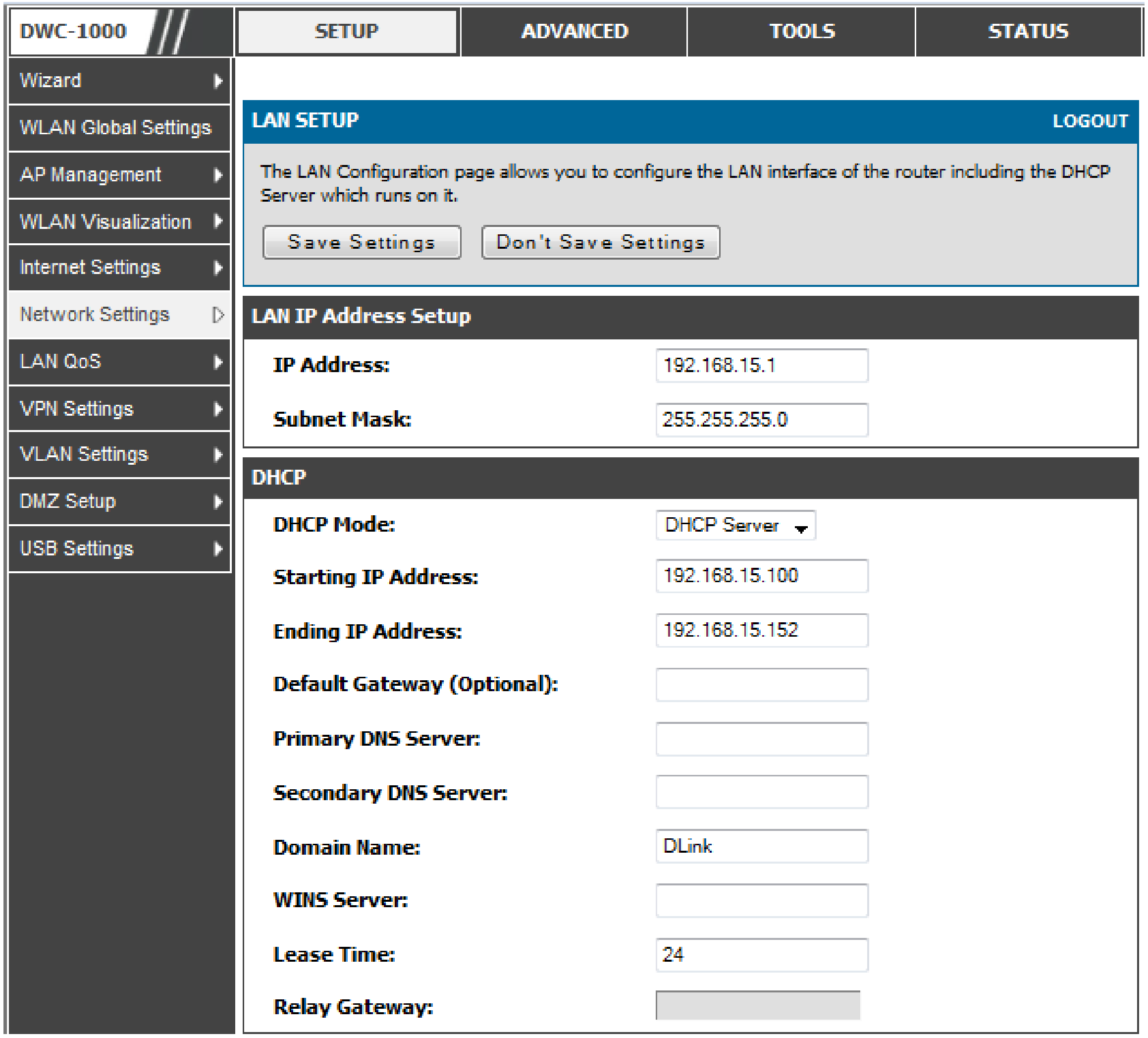
Lease Time: Enter the time, in hours, for which IP addresses are leased to clients.

Enable DNS Proxy: To enable the controller to act as a proxy for all DNS requests and communicate with the ISP’s DNS servers, click the checkbox.

Relay Gateway: Enter the gateway address. This is the only configuration parameter required in this section when DHCP Relay is selected as its DHCP mode

3. Click Save Settings to apply all changes.

Figure 1: Setup page for LAN TCP/IP settings (DHCP server)



LAN SETUP

The LAN Configuration page allows you to configure the LAN interface of the router including the DHCP Server which runs on it.

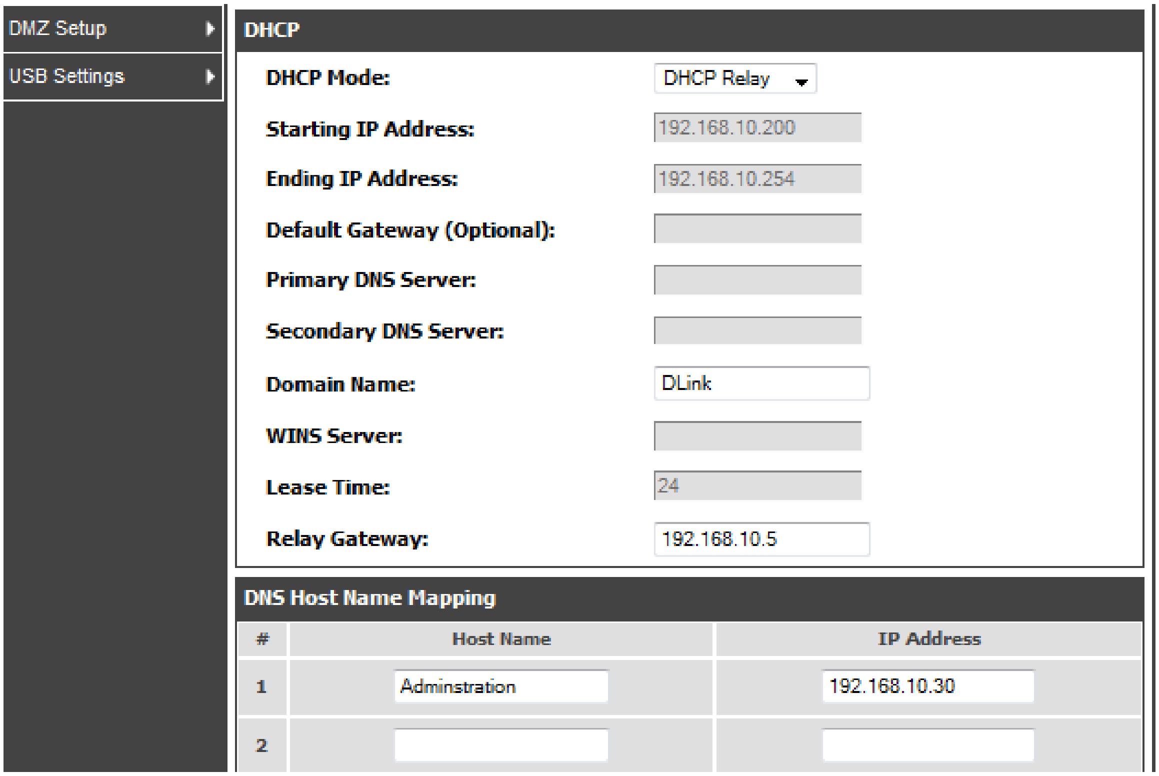
LAN IP Address Setup

IP Address:	192.168.15.1
Subnet Mask:	255.255.255.0

DHCP

DHCP Mode:	DHCP Server
Starting IP Address:	192.168.15.100
Ending IP Address:	192.168.15.152
Default Gateway (Optional):	
Primary DNS Server:	
Secondary DNS Server:	
Domain Name:	DLink
WINS Server:	
Lease Time:	24
Relay Gateway:	

Figure 2: Setup page for LAN TCP/IP settings (DHCP Relay)



DHCP

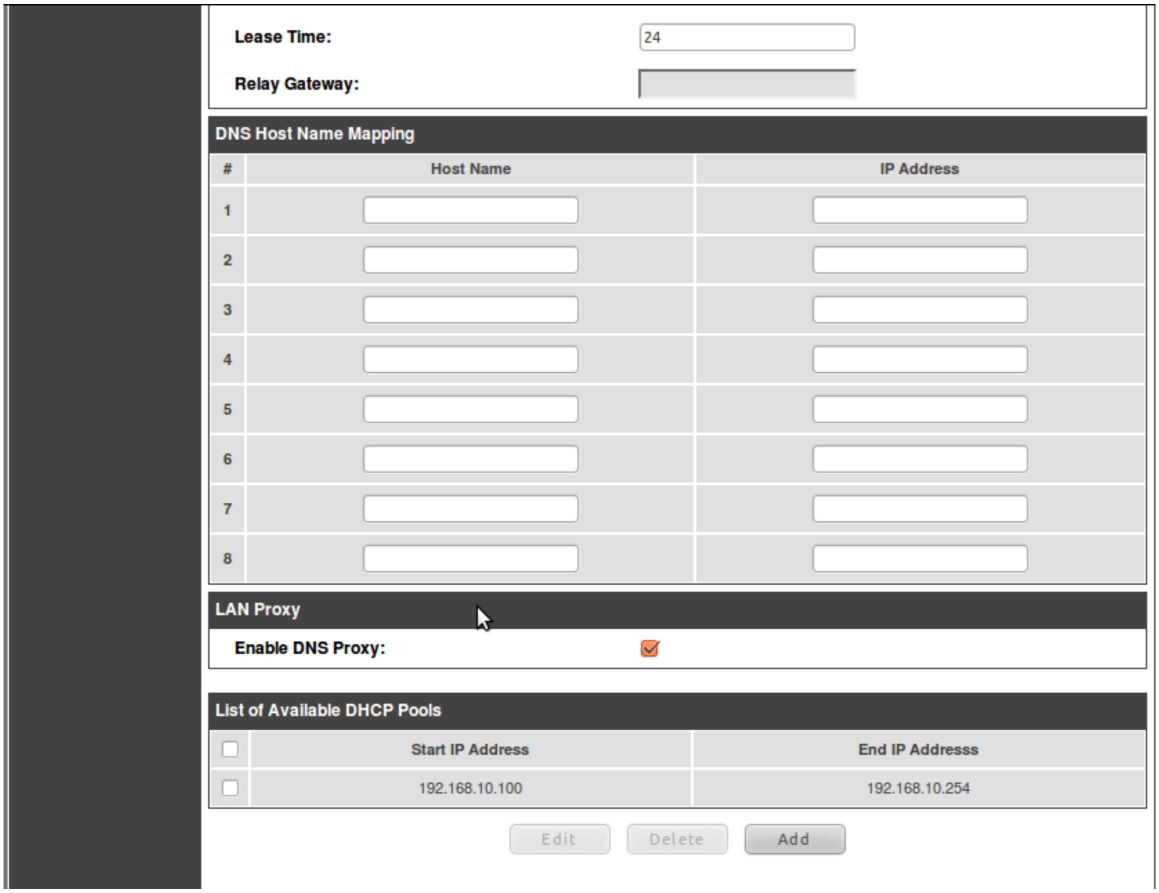
DHCP Mode:	DHCP Relay
Starting IP Address:	192.168.10.200
Ending IP Address:	192.168.10.254
Default Gateway (Optional):	
Primary DNS Server:	
Secondary DNS Server:	
Domain Name:	DLink
WINS Server:	
Lease Time:	24
Relay Gateway:	192.168.10.5

DNS Host Name Mapping

#	Host Name	IP Address
1	Adminstration	192.168.10.30
2		

When DHCP relay is enabled, DHCP clients on the LAN can receive IP address leases and corresponding information from a DHCP server on a different subnet. Specify the Relay Gateway, and when LAN clients make a DHCP request it will be passed along to the server accessible via the Relay Gateway IP address.

Figure 3: Setup page for LAN TCP/IP settings (continued)



Lease Time: 24

Relay Gateway:

DNS Host Name Mapping

#	Host Name	IP Address
1		
2		
3		
4		
5		
6		
7		
8		

LAN Proxy

Enable DNS Proxy: ☑

List of Available DHCP Pools

□	Start IP Address	End IP Addresss
□	192.168.10.100	192.168.10.254

2.1.1 LAN DHCP Reserved IPs

Setup > Network Settings > LAN DHCP Reserved IPs

The controller DHCP server can assign TCP/IP configurations to computers in the LAN explicitly by adding client's network interface hardware address and the IP address to be assigned to that client in DHCP server's database. Whenever DHCP server receives a request from client, hardware address of that client is compared with the hardware address list present in the database, if an IP address is already assigned to that computer or device in the database , the customized IP address is configured otherwise an IP address is assigned to the client automatically from the DHCP pool.

IP Addresses: The LAN IP address of a host that is reserved by the DHCP server.

MAC Addresses: The MAC address that will be assigned the reserved IP address when it is on the LAN.

The actions that can be taken on list of reserved IP addresses are:

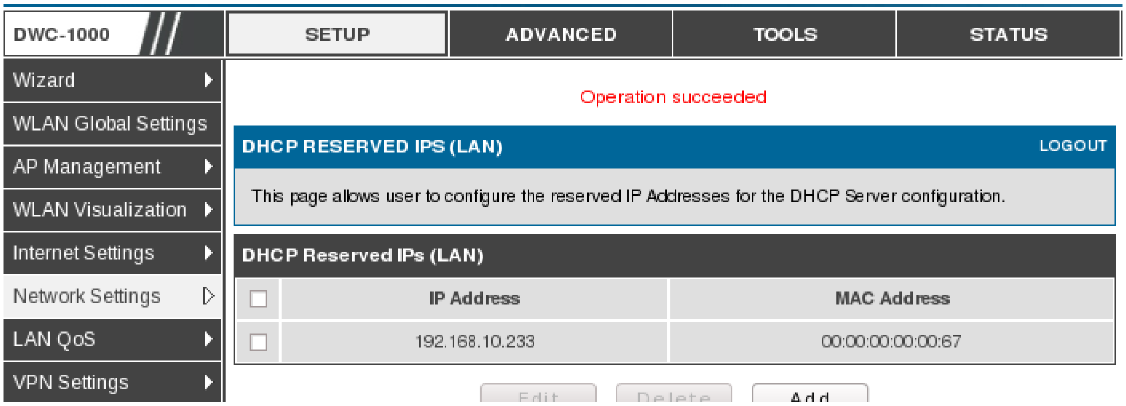
Select: Selects all the reserved IP addresses in the list.

Edit: Opens the LAN DHCP Reserved IP Configuration page to edit the selected binding rule.

Delete: Deletes the selected IP address reservation(s)

Add: Opens the LAN DHCP Reserved IP Configuration page to add a new binding rule.

Figure 4: LAN DHCP Reserved IPs



Operation succeeded

DHCP RESERVED IPS (LAN)

This page allows user to configure the reserved IP Addresses for the DHCP Server configuration.

DHCP Reserved IPs (LAN)

□	IP Address	MAC Address
□	192.168.10.233	00:00:00:00:00:67

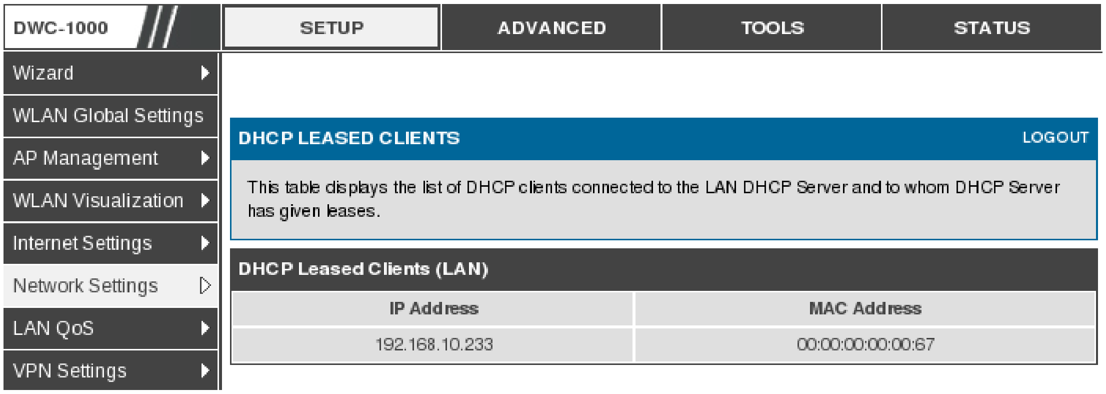
.

2.1.2 LAN DHCP Leased Clients

Setup > Network Settings > LAN DHCP Leased Clients

This page provides the list of clients connect to LAN DHCP server.

Figure 5: LAN DHCP Leased Clients



This table displays the list of DHCP clients connected to the LAN DHCP Server and to whom DHCP Server has given leases.

DHCP Leased Clients (LAN)

IP Address	MAC Address
192.168.10.233	00:00:00:00:00:67

IP Addresses: The LAN IP address of a host that matches the reserved IP list. **MAC Addresses**: The MAC address of a LAN host that has a configured IP address reservation.

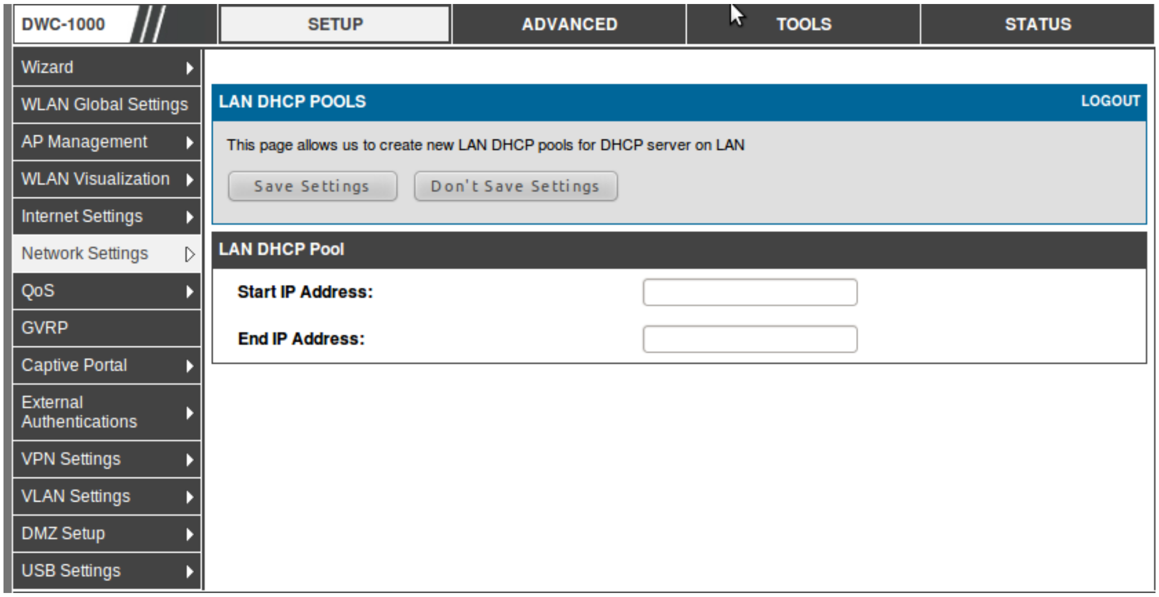
2.1.3 LAN DHCP Pools

Setup > Network Settings > LAN DHCP Pools

Upon enabling DHCP, you can define a set of IP ranges (referred to as “pools”) from which to assign LAN clients IP addresses. Each LAN on the router can sub-divded into 8 pools. The subnet and network of each pool must be within that of the LAN, configured on the LAN Settings page. Most importantly, pool IP addresss must not overlap on another.

New LAN DHCP clients will be assigned IP addresses starting with the “Start” IP address in the first pool in the list of pools. Clients will continue to receive sequential IP addresses until the “End” IP address of the first pool. Then, if further pools are configured, the next LAN client to join the domain of this router will receive the “Start” IP address of the second configured pool, and so on.

Figure 6: LAN DHCP Pool configuration



LAN DHCP POOLS

This page allows us to create new LAN DHCP pools for DHCP server on LAN

LAN DHCP Pool

Start IP Address:

End IP Address:

Once confirgured, the list of DHCP Pools at the bottom of the LAN Setup Configuration page (Figure 3) is updated with the new pool range.

2.1.4 LAN Configuration in an IPv6 Network

Advanced > IPv6 > IPv6 LAN > IPv6 LAN Config

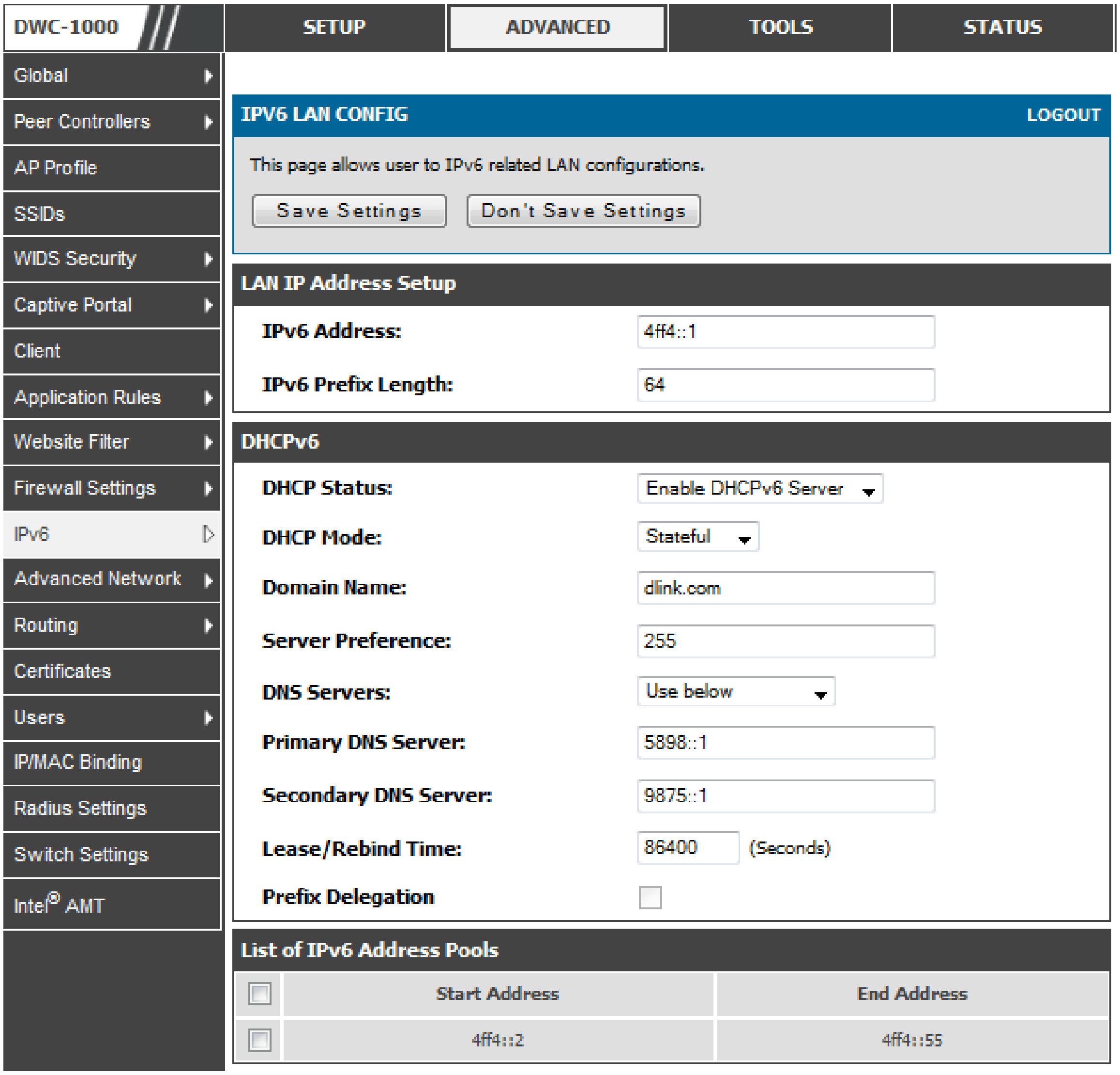
In IPv6 mode, the LAN DHCP server is enabled by default (similar to IPv4 mode). The DHCPv6 server will serve IPv6 addresses from configured address pools with the IPv6 Prefix Length assigned to the LAN.

> ✍ IPv4 / IPv6 mode must be enabled in the ***Advanced > IPv6 > Routing mode*** to enable IPv6 configuration options.

LAN IP Address Setup

The default IPv6 LAN address for the router is **fec0::1**. You can change this 128 bit IPv6 address based on your network requirements. The other field that defines the LAN settings for the router is the prefix length. The IPv6 network (subnet) is identified by the initial bits of the address called the prefix. By default this is **64** bits long. All hosts in the network have common initial bits for their IPv6 address; the number of common initial bits in the network's addresses is set by the prefix length field.

Figure 7: IPv6 LAN and DHCPv6 configuration



IPV6 LAN CONFIG

This page allows user to IPv6 related LAN configurations.

LAN IP Address Setup

- IPv6 Address: 4ff4::1
- IPv6 Prefix Length: 64

DHCPv6

- DHCP Status: Enable DHCPv6 Server
- DHCP Mode: Stateful
- Domain Name: dlink.com
- Server Preference: 255
- DNS Servers: Use below
- Primary DNS Server: 5898::1
- Secondary DNS Server: 9875::1
- Lease/Rebind Time: 86400 (Seconds)
- Prefix Delegation ☐

List of IPv6 Address Pools

☐	Start Address	End Address
☐	4ff4::2	4ff4::55

If you change the IP address and click Save Settings, the GUI will not respond. Open a new connection to the new IP address and log in again. Be sure the LAN host (the machine used to manage the router) has obtained IP address from newly assigned pool (or has a static IP address in the router's LAN subnet) before accessing the router via changed IP address.

DHCP v6

As with an IPv4 LAN network, the router has a DHCPv6 server. If enabled, the router assigns an IP address within the specified range plus additional specified information to any LAN PC that requests DHCP served addresses.

The following settings are used to configure the DHCPv6 server:

DHCP Status: This allow to Enable/Disable DHCPv6 server.

DHCP Mode: The IPv6 DHCP server is either stateless or stateful. If stateless is selected an external IPv6 DHCP server is not required as the IPv6 LAN hosts are auto-configured by this controller. In this case the controller advertisement daemon (RADVD) must be configured on this device and ICMPv6 controller discovery messages are used by the host for auto-configuration. There are no managed addresses to serve the LAN nodes. If stateful is selected the IPv6 LAN host will rely on an external DHCPv6 server to provide required configuration settings

The **Domain Name** of the DHCPv6 server is an optional setting

Server Preference: To indicate the preference level of this DHCP server. DHCP advertise messages with the highest server preference value to a LAN host are preferred over other DHCP server advertise messages. The default is 255.

DNS servers: The details can be manually entered here (primary/secondary options). An alternative is to allow the LAN DHCP client to receive the DNS server details from the ISP directly. By selecting Use DNS Proxy, this router acts as a proxy for all DNS requests and communicates with the ISP’s DNS servers (an optional configuration parameter).

Primary and Secondary DNS servers: If there are configured domain name system (DNS) servers available on the LAN enter the IP addresses here.

Lease/Rebind time: It sets the duration of the DHCPv6 lease from this router to the LAN client.

IPv6 Address Pools

This feature allows you to define the IPv6 delegation prefix for a range of IP addresses to be served by the gateway’s DHCPv6 server. Using a delegation prefix you can automate the process of informing other networking equipment on the LAN of DHCP information specific for the assigned prefix.

Prefix Delegation

The following settings are used to configure the Prefix Delegation:

Prefix Delegation: Select this option to enable prefix delegation in DHCPv6 server. This option can be selected only in Stateless Address Auto Configuration mode of DHCPv6 server.

Prefix Address: IPv6 prefix address in the DHCPv6 server prefix pool

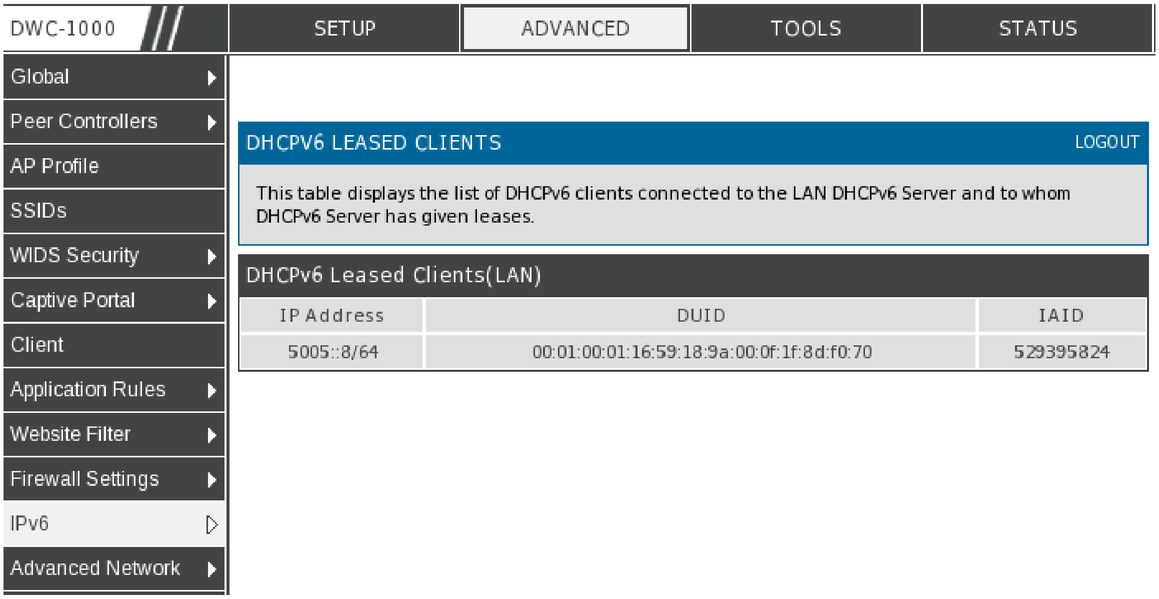
Prefix Length: Length prefix address

2.1.5 DHCPv6 Leased Clients

Advanced > IPv6 > IPv6 LAN > DHCPv6 Leased Clients

This page provides the list of DHCPv6 clients connected to the LAN DHCPv6 Server and to whom DHCPv6 Server has given leases.

Figure 8: DHCPv6 Leased Clients



DHCPV6 LEASED CLIENTS

This table displays the list of DHCPv6 clients connected to the LAN DHCPv6 Server and to whom DHCPv6 Server has given leases.

DHCPv6 Leased Clients(LAN)

IP Address	DUID	IAID
5005::8/64	00:01:00:01:16:59:18:9a:00:0f:1f:8d:f0:70	529395824

IP Addresses: This is the DHCP server IP address.

DUID: Each DHCP client and server has a DUID. DHCP servers use DUIDs to identify clients for the selection of configuration parameters and in the association of

IAs with clients. DHCP clients use DUIDs to identify a server in messages where a server needs to be identified.

IAID: An identifier for an IA, chosen by the client. Each IA has an IAID, which is chosen to be unique among all IAIDs for IAs belonging to that client.: This is the DHCP server IP address.

2.1.6 Configuring IPv6 Router Advertisements

Router Advertisements are analogous to IPv4 DHCP assignments for LAN clients, in that the router will assign an IP address and supporting network information to devices that are configured to accept such details. Router Advertisement is required in an IPv6 network is required for stateless auto configuration of the IPv6 LAN. By configuring the Router Advertisement Daemon on this router, the DWC-1000 will listen on the LAN for router solicitations and respond to these LAN hosts with router advisements.

RADVD

Advanced > IPv6 > IPv6 LAN > Router Advertisement

To support stateless IPv6 auto configuration on the LAN, set the RADVD status to Enable. The following settings are used to configure RADVD:

RADVD Status: You can enable the RADVD process here to allow stateless auto configuration of the IPv6 LAN network.

Advertise Mode: Select Unsolicited Multicast to send router advertisements (RA’s) to all interfaces in the multicast group. To restrict RA’s to well-known IPv6 addresses on the LAN, and thereby reduce overall network traffic, select Unicast only.

Advertise Interval: When advertisements are unsolicited multicast packets, this interval sets the maximum time between advertisements from the interface. The actual duration between advertisements is a random value between one third of this field and this field. The default is 30 seconds.

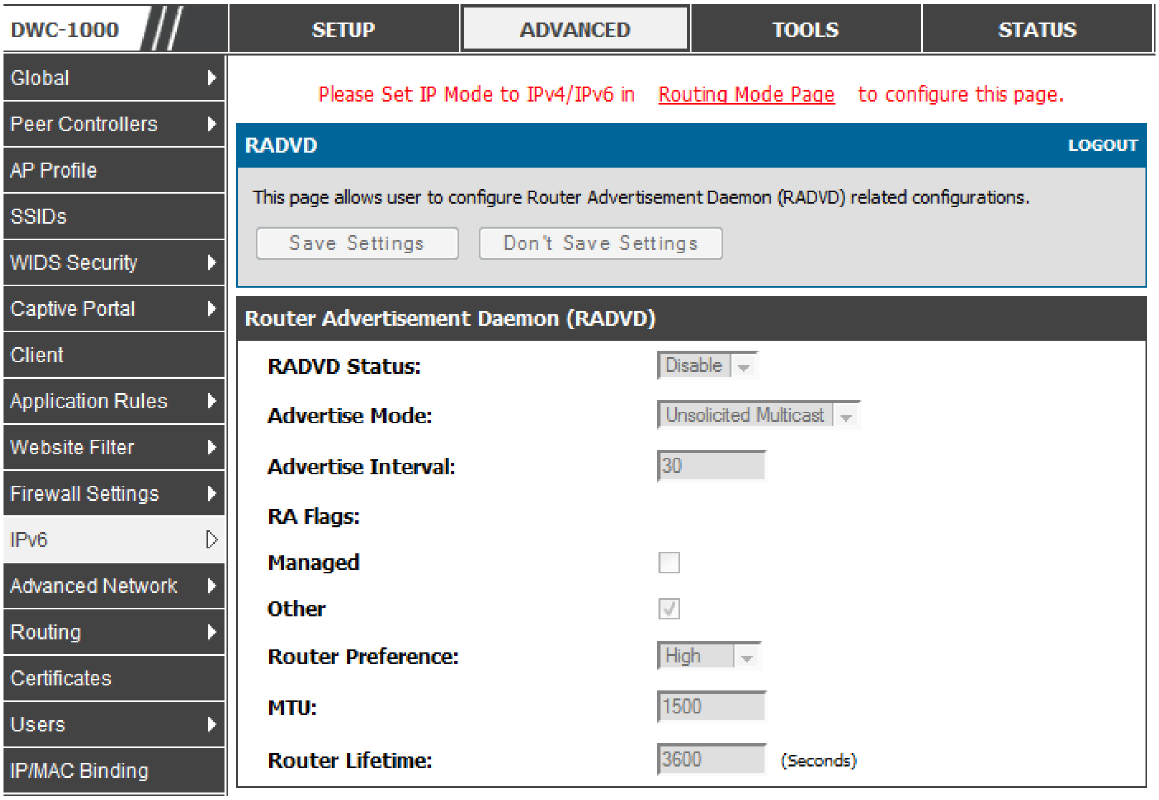
RA Flags: The router advertisements (RA’s) can be sent with one or both of these flags. Chose Managed to use the administered /stateful protocol for address auto configuration. If the Other flag is selected the host uses administered/stateful protocol for non-address auto configuration.

Router Preference: this low/medium/high parameter determines the preference associated with the RADVD process of the router. This is useful if there are other RADVD enabled devices on the LAN as it helps avoid conflicts for IPv6 clients.

MTU: The router advertisement will set this maximum transmission unit (MTU) value for all nodes in the LAN that are auto configured by the router. The default is 1500.

Router Lifetime: This value is present in RA's and indicates the usefulness of this router as a default router for the interface. The default is 3600 seconds. Upon expiration of this value, a new RADVD exchange must take place between the host and this router.

Figure 9: Configuring the Router Advertisement Daemon



Please Set IP Mode to IPv4/IPv6 in Routing Mode Page to configure this page.

RADVD

This page allows user to configure Router Advertisement Daemon (RADVD) related configurations.

Router Advertisement Daemon (RADVD)

RADVD Status:	Disable
Advertise Mode:	Unsolicited Multicast
Advertise Interval:	30
RA Flags:	
Managed	□
Other	☑
Router Preference:	High
MTU:	1500
Router Lifetime:	3600 (Seconds)

Advertisement Prefixes

Advanced > IPv6 > IPv6 LAN > Advertisement Prefixes

The router advertisements configured with advertisement prefixes allow this router to inform hosts how to perform stateless address auto configuration. Router advertisements contain a list of subnet prefixes that allow the router to determine neighbors and whether the host is on the same link as the router.

The following prefix options are available for the router advertisements:

IPv6 Prefix Type: To ensure hosts support IPv6 to IPv4 tunnel select the 6to4 prefix type. Selecting Global/Local/ISATAP will allow the nodes to support all other IPv6 routing options

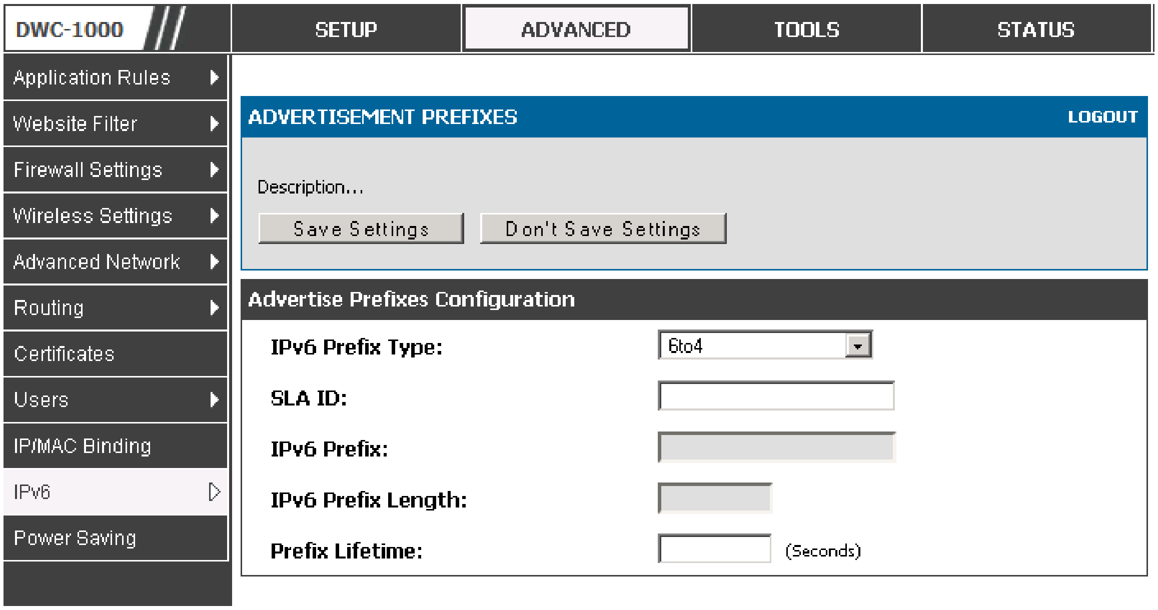
SLA ID: The SLA ID (Site-Level Aggregation Identifier) is available when 6to4 Prefixes are selected. This should be the interface ID of the router's LAN interface used for router advertisements.

IPv6 Prefix: When using Global/Local/ISATAP prefixes, this field is used to define the IPv6 network advertised by this router.

IPv6 Prefix Length: This value indicates the number contiguous, higher order bits of the IPv6 address that define up the network portion of the address. Typically this is 64.

Prefix Lifetime: This defines the duration (in seconds) that the requesting node is allowed to use the advertised prefix. It is analogous to DHCP lease time in an IPv4 network.

Figure 10: IPv6 Advertisement Prefix settings



ADVERTISEMENT PREFIXES

Description...

Advertise Prefixes Configuration

IPv6 Prefix Type:	6to4
SLA ID:	
IPv6 Prefix:	
IPv6 Prefix Length:	
Prefix Lifetime:	(Seconds)

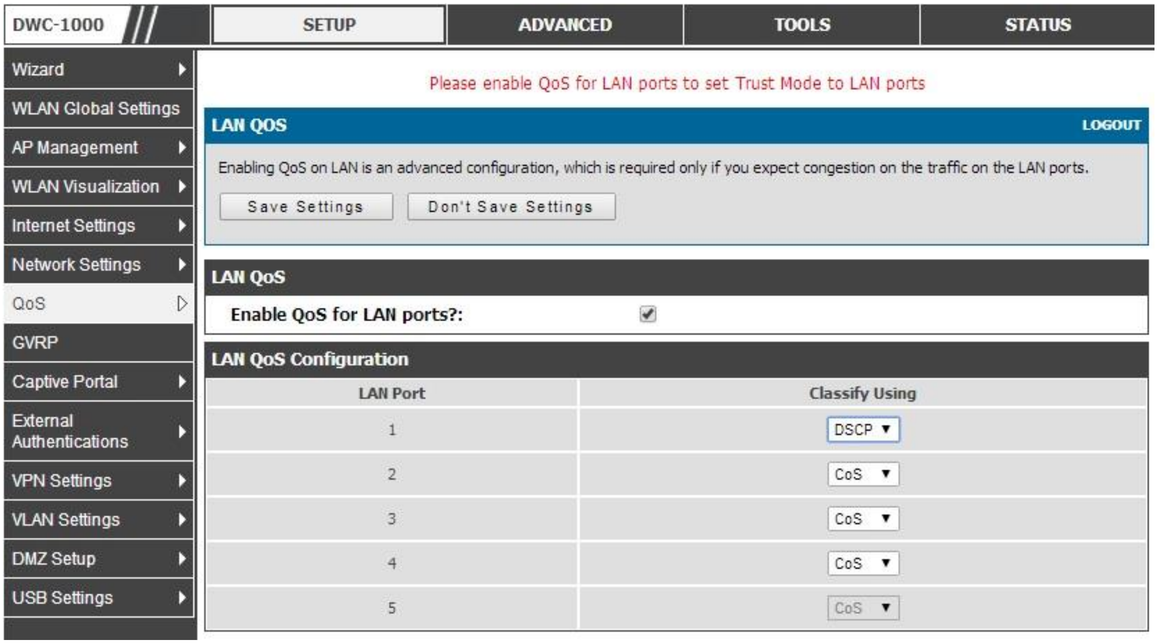
2.2 QoS

2.2.1 LAN QoS Configuration

Setup > QoS > LAN QoS > Trust Mode Configuration

Enabling QoS on LAN is an advanced configuration, which is required only if you expect congestion on the traffic on the LAN ports. This page allows you to enable QoS and configure each port to trust a CoS or DSCP values in the packet.

Figure 11: LAN QoS Configuration



Please enable QoS for LAN ports to set Trust Mode to LAN ports

LAN QOS

Enabling QoS on LAN is an advanced configuration, which is required only if you expect congestion on the traffic on the LAN ports.

LAN QoS

Enable QoS for LAN ports?: ☑

LAN QoS Configuration

LAN Port	Classify Using
1	DSCP ▼
2	CoS ▼
3	CoS ▼
4	CoS ▼
5	CoS ▼

LAN Port: This list out the available LAN ports

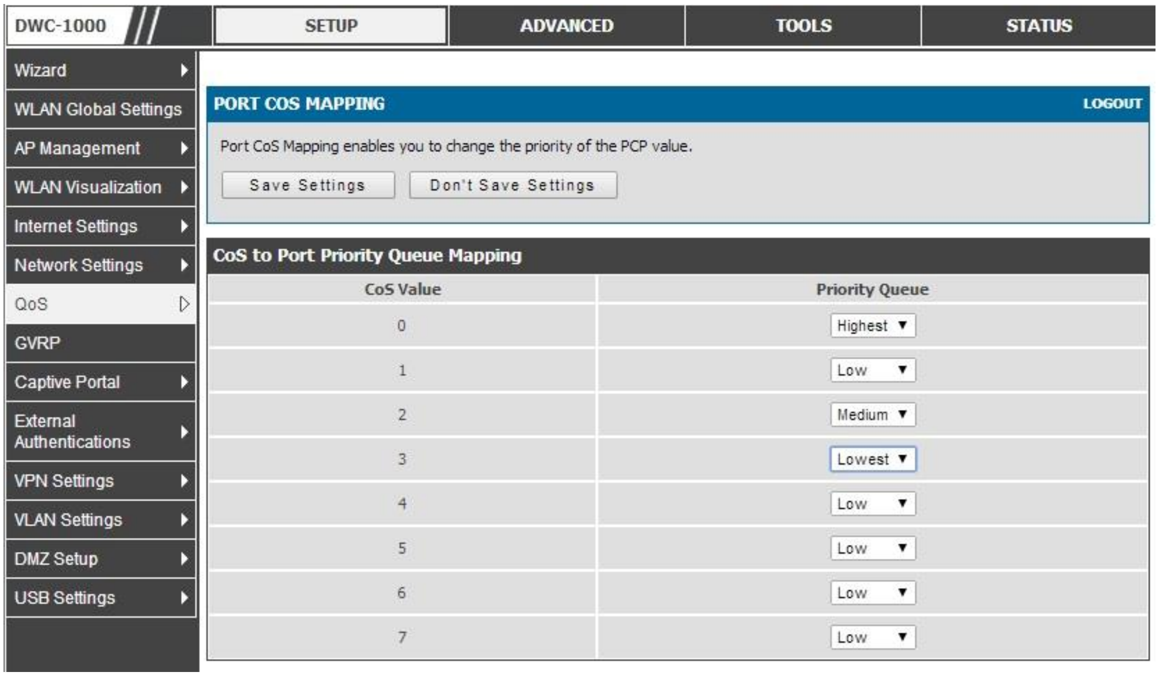
Classify Using: This provide the list of QoS services available on the port

2.2.2 801.P Priority (CoS to Port Mapping)

Setup > QoS > 801.P Priority

Port CoS Mapping enables you to change the priority of the PCP value.

Figure 12: 801.P Configuration



PORT COS MAPPING

Port CoS Mapping enables you to change the priority of the PCP value.

CoS to Port Priority Queue Mapping

CoS Value	Priority Queue
0	Highest
1	Low
2	Medium
3	Lowest
4	Low
5	Low
6	Low
7	Low

CoS Value: value of the CoS in the PCP part of the LAN traffic.

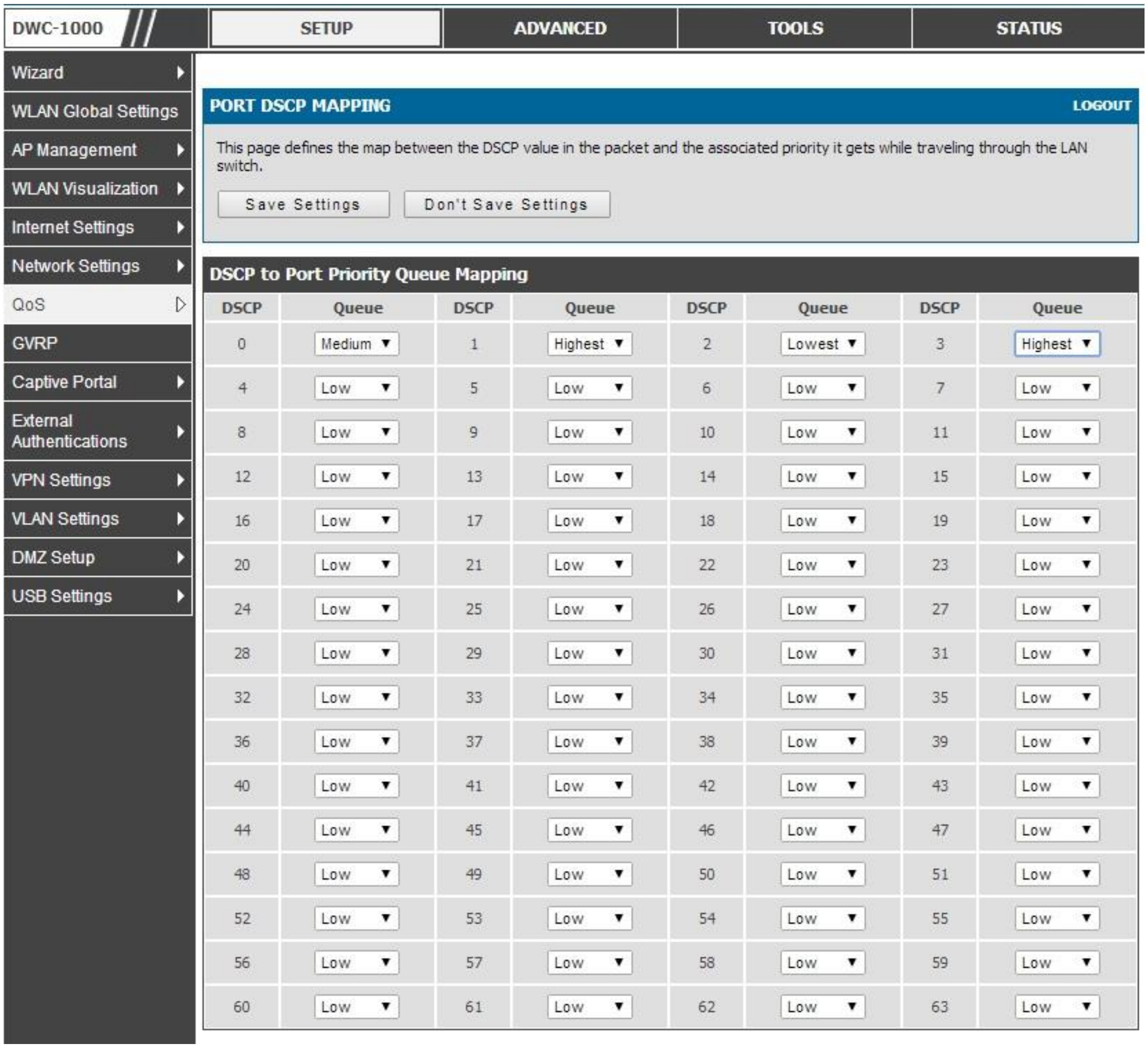
Priority Queue: Priority for the particular CoS value

2.2.3 DSCP Configuration

Setup > QoS > IP DSCP Configuration

This page allows configuring IP DSCP values to which you can map an internal traffic class.

Figure 13: Port DSCP Mapping



PORT DSCP MAPPING

This page defines the map between the DSCP value in the packet and the associated priority it gets while traveling through the LAN switch.

DSCP to Port Priority Queue Mapping

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0	Medium	1	Highest	2	Lowest	3	Highest
4	Low	5	Low	6	Low	7	Low
8	Low	9	Low	10	Low	11	Low
12	Low	13	Low	14	Low	15	Low
16	Low	17	Low	18	Low	19	Low
20	Low	21	Low	22	Low	23	Low
24	Low	25	Low	26	Low	27	Low
28	Low	29	Low	30	Low	31	Low
32	Low	33	Low	34	Low	35	Low
36	Low	37	Low	38	Low	39	Low
40	Low	41	Low	42	Low	43	Low
44	Low	45	Low	46	Low	47	Low
48	Low	49	Low	50	Low	51	Low
52	Low	53	Low	54	Low	55	Low
56	Low	57	Low	58	Low	59	Low
60	Low	61	Low	62	Low	63	Low

DSCP: Lists the IP DSCP values to which you can map an internal traffic class. The values range from 0-63.

Queue: This provides the priority of the queue

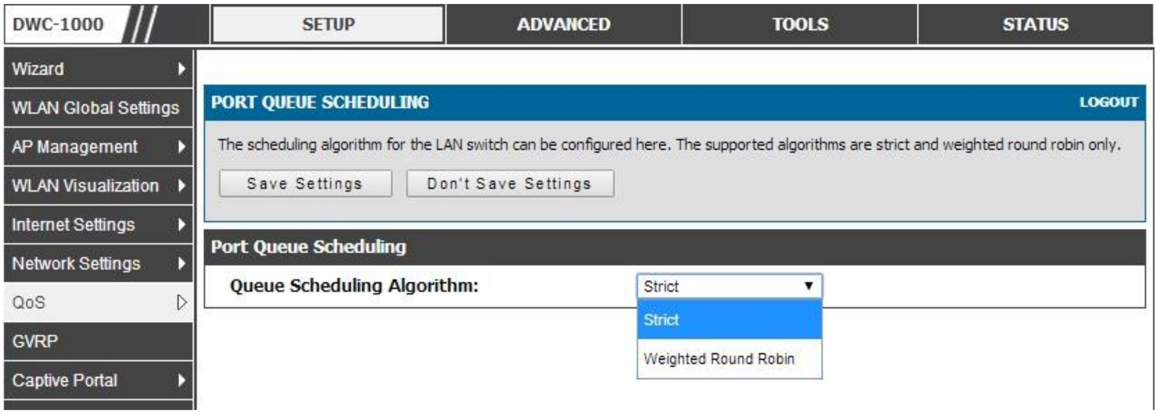
2.2.4 Port Queue Scheduling

Setup > QoS > Queue Scheduler

This page allows the admin to determine the queuing scheduling algorithm.

Queuing scheduling algorithm: The scheduling algorithm for the LAN controller can be configured here. The supported algorithms are strict and weighted round robin only. The device will be programmed to handle the traffic using the algorithm configured here

Figure 14: Port Queue Scheduler



The scheduling algorithm for the LAN switch can be configured here. The supported algorithms are strict and weighted round robin only.

Queue Scheduling Algorithm: Strict

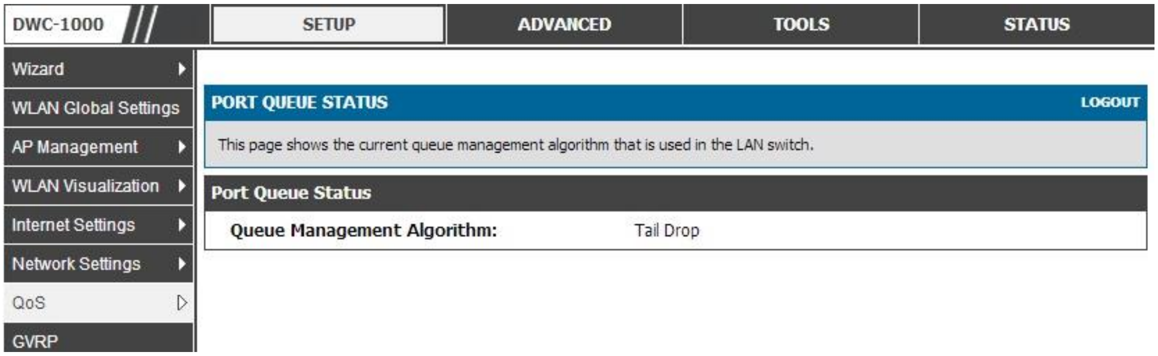
2.2.5 Port Queue Status

Setup > QoS > Queue Management

This page shows the current queue management algorithm that is used in the LAN controller

Queuing Management algorithm: Display the current queue management algorithm that is used in the LAN controller

Figure 15: Port Queue Status



PORT QUEUE STATUS

This page shows the current queue management algorithm that is used in the LAN switch.

Port Queue Status

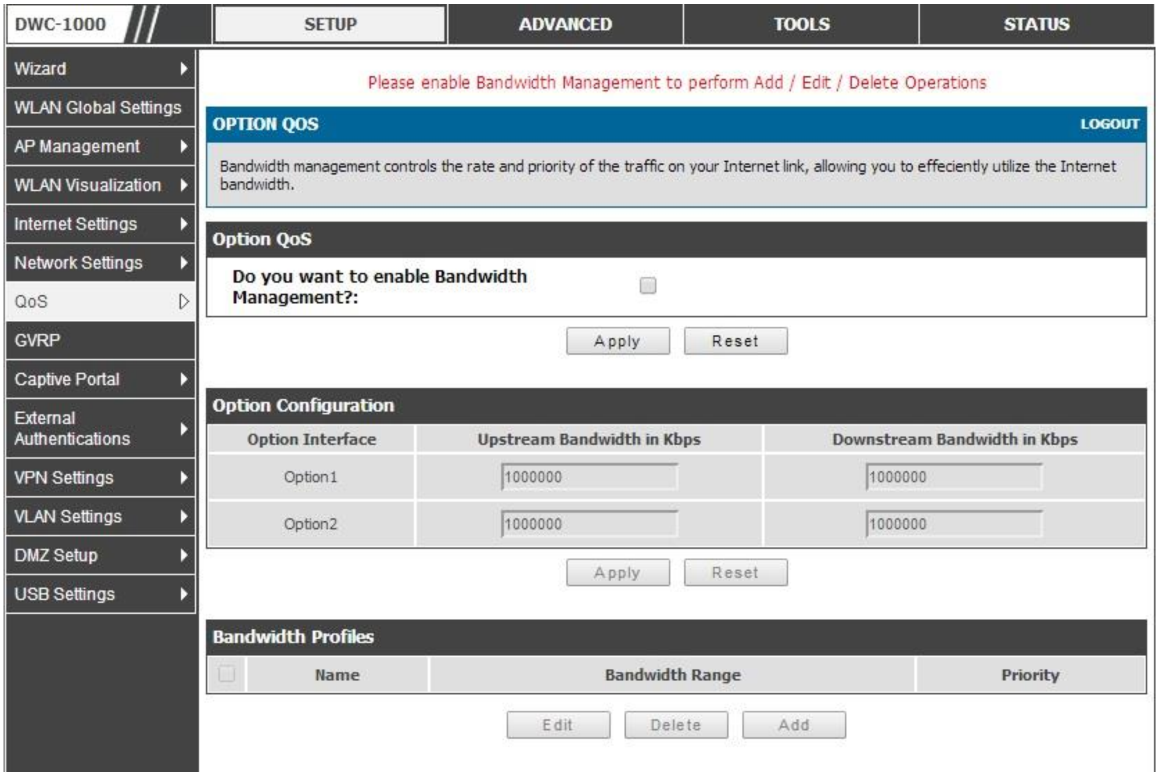
Queue Management Algorithm:	Tail Drop

2.2.6 Option QoS Configuration

Setup > QoS > Option QoS Configuration

This page allows configuring the Option QoS and defining the bandwidth for Option interfaces.

Figure 16: Option QoS Configuration



Please enable Bandwidth Management to perform Add / Edit / Delete Operations

OPTION QOS

Bandwidth management controls the rate and priority of the traffic on your Internet link, allowing you to effeciently utilize the Internet bandwidth.

Option QoS

Do you want to enable Bandwidth Management?: ☐

Option Configuration

Option Interface	Upstream Bandwidth in Kbps	Downstream Bandwidth in Kbps
Option1	1000000	1000000
Option2	1000000	1000000

Bandwidth Profiles

☐	Name	Bandwidth Range	Priority

Option QoS: To enable Bandwidth management select the check box and click Apply.

Option Configuration: Define the upstream and downstream for bandwidth for Option1 and Option 2 interfaces.

Bandwidth Profile: Click Add to define bandwidth profile

Bandwidth Management

Profile Name: Allows defining a profile name.

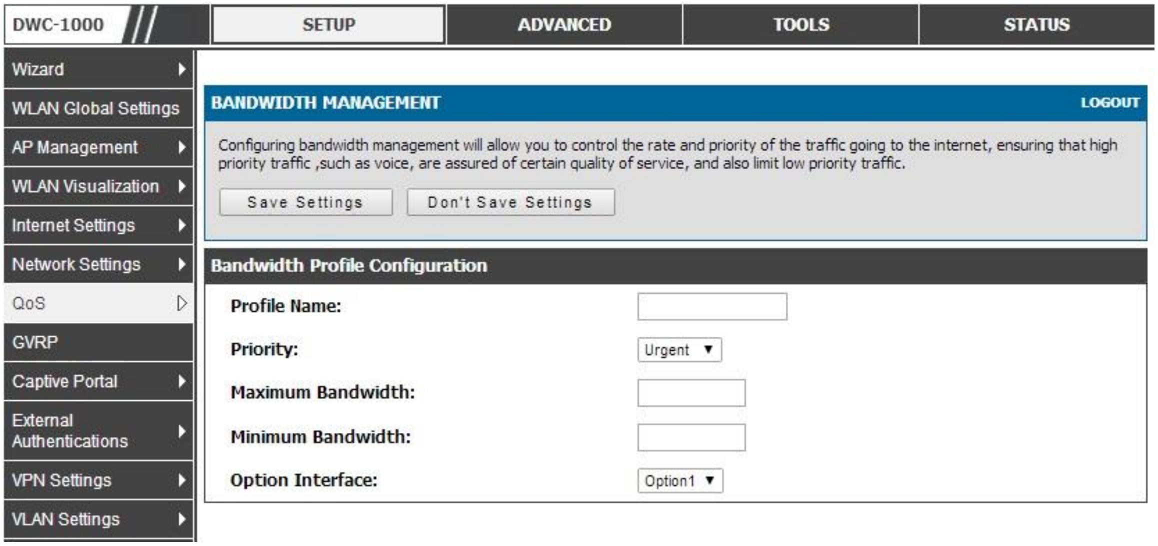
Priority: Select the priority of profile.

Maximum Bandwidth: Provide the maximum allowed bandwidth of the profile

Minimum Bandwidth: Provide the minimum allowed bandwidth of the profile

Option Interface: Select the interface Option1/Option2

Figure 17: Bandwidth Profile Configuration



Configuring bandwidth management will allow you to control the rate and priority of the traffic going to the internet, ensuring that high priority traffic ,such as voice, are assured of certain quality of service, and also limit low priority traffic.

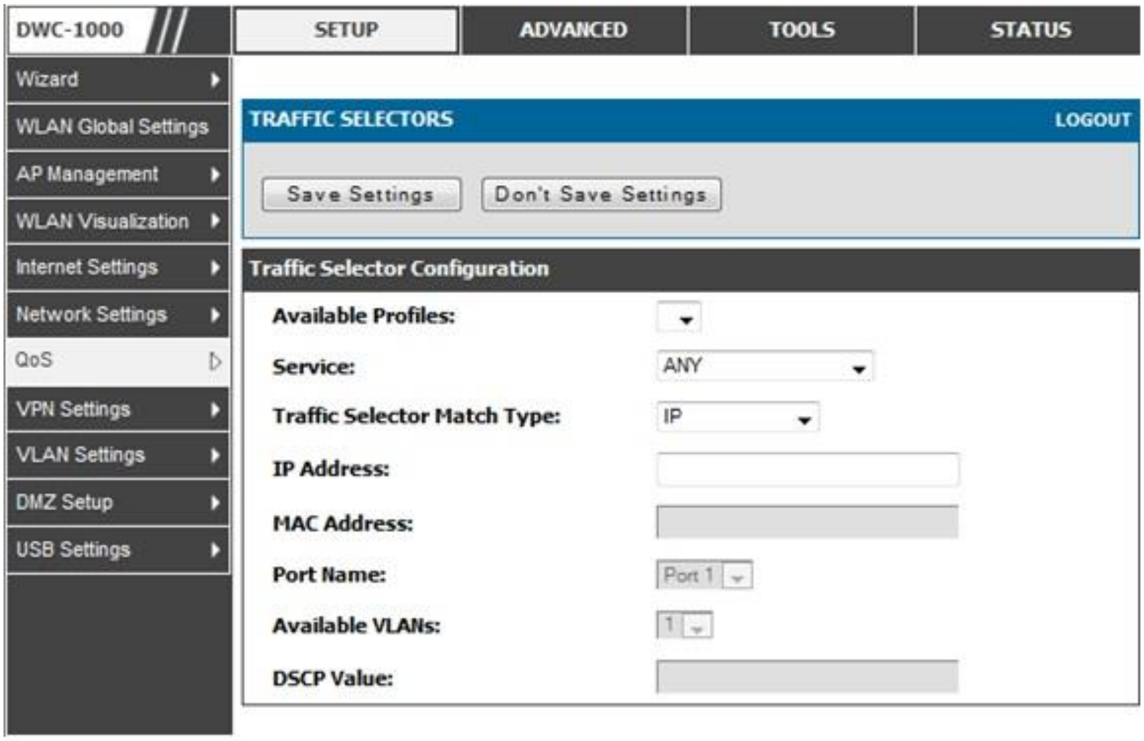
Profile Name:	
Priority:	Urgent ▼
Maximum Bandwidth:	
Minimum Bandwidth:	
Option Interface:	Option1 ▼

2.2.7 Traffic Selector Configuration

Setup > QoS > Traffic Selector Configuration

After you create a bandwidth profile, you can associate it with a traffic flow.

Figure 18: Traffic Selector Configuration



Traffic Selector Configuration

Available Profiles:	
Service:	ANY
Traffic Selector Match Type:	IP
IP Address:	
MAC Address:	
Port Name:	Port 1
Available VLANs:	1
DSCP Value:	

Available Profiles: Select one of the previously configured bandwidth profiles to associate this traffic selector.

Service: Select one of the services from the available services.

Traffic Selector Match Type: Choose the method for identifying the host that is controlled by this traffic Selector: IP Address, MAC Address, Port Name, VLAN Name, DSCP value or BSSID.

IP Address: Enter IP Address of LAN host, if you chose IP as the Match Type.

MAC Address: Enter a valid MAC Address, if you chose MAC Address as the Match Type.

Port Name: Select the LAN port number, if you chose Port Name as the Match Type.

Available VLANs: Select a VLAN, if you chose VLAN Name as the Match Type.

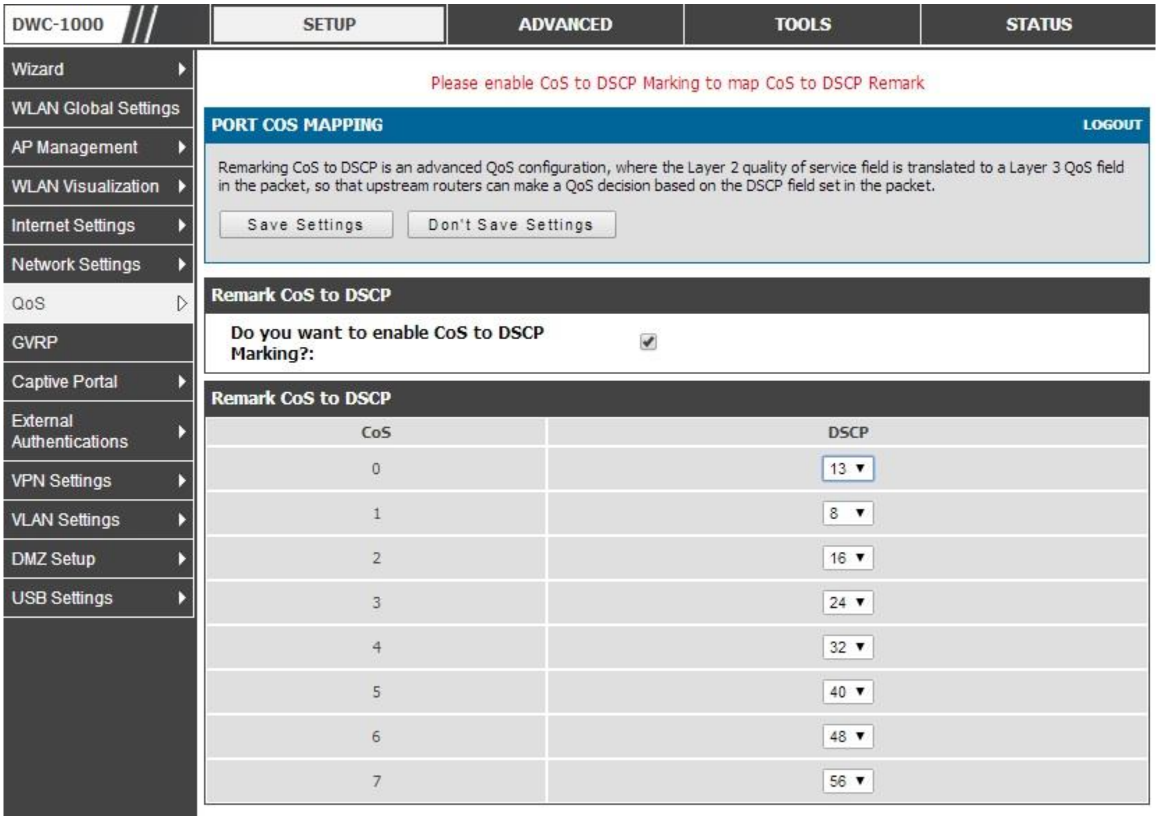
DSCP value: Enter a valid DSCP value between 0 and 63, if choose DSCP as the Match Type.

2.2.8 Remark CoS to DSCP

Setup > QoS > Remark CoS to DSCP

Remarking CoS to DSCP is an advanced QoS configuration, where the Layer 2 quality of service field is translated to a Layer 3 QoS field in the packet, so that upstream routers can make a QoS decision based on the DSCP field set in the packet.

Figure 19: Remark CoS to DSCP



Please enable CoS to DSCP Marking to map CoS to DSCP Remark

PORT COS MAPPING

Remarking CoS to DSCP is an advanced QoS configuration, where the Layer 2 quality of service field is translated to a Layer 3 QoS field in the packet, so that upstream routers can make a QoS decision based on the DSCP field set in the packet.

Remark CoS to DSCP

Do you want to enable CoS to DSCP Marking?: ☑

Remark CoS to DSCP

CoS	DSCP
0	13 ▼
1	8 ▼
2	16 ▼
3	24 ▼
4	32 ▼
5	40 ▼
6	48 ▼
7	56 ▼

Once you enable CoS to DSCP marking by choosing the check box, you can choose the appropriate value of the DSCP for a given CoS value.

2.3 VLAN Configuration

The controller supports virtual network isolation on the LAN with the use of VLANs. LAN devices can be configured to communicate in a subnet defined by VLAN identifiers. LAN ports can be assigned unique VLAN IDs so that traffic to and from that physical port can be isolated from the general LAN. VLAN filtering is particularly useful to limit broadcast packets of a device in a large network

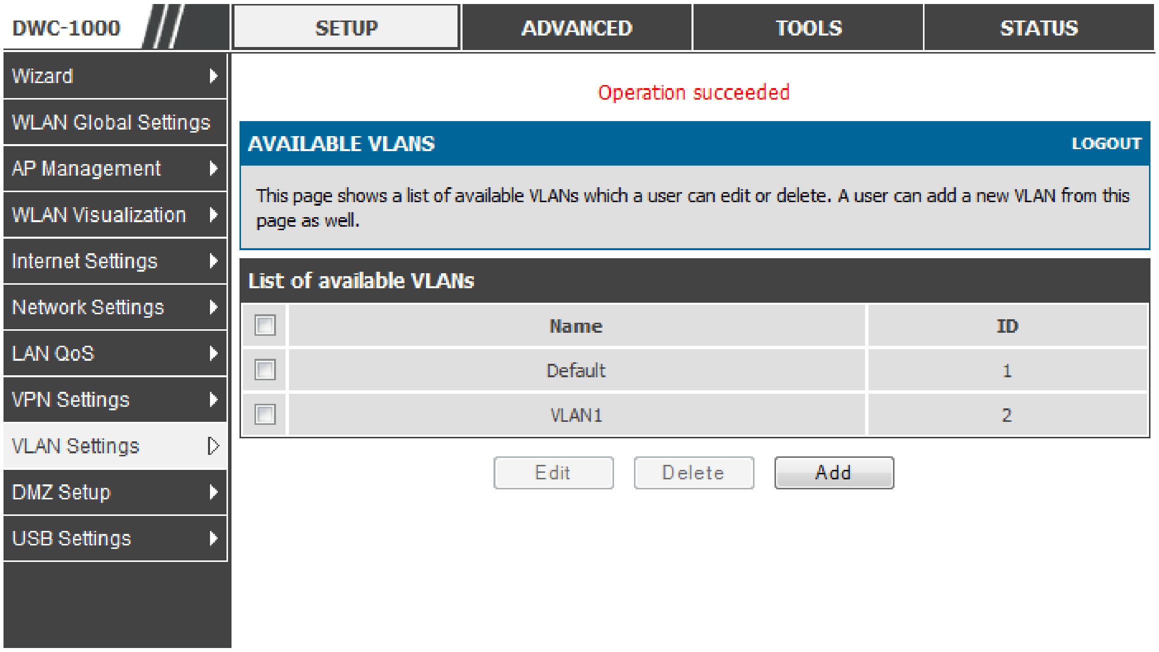
VLAN support is disabled by default in the controller. In the VLAN Configuration page, enable VLAN support on the controller and then proceed to the next section to define the virtual network.

Setup > VLAN Settings > Available VLAN

The Available VLAN page shows a list of configured VLANs by name and VLAN ID. A VLAN membership can be created by clicking the Add button below the List of Available VLANs.

A VLAN membership entry consists of a VLAN identifier and the numerical VLAN ID which is assigned to the VLAN membership. The VLAN ID value can be any number from 2 to 255. VLAN ID 1 is reserved for the default VLAN, which is used for untagged frames received on the interface. By enabling Inter VLAN Routing, you will allow traffic from LAN hosts belonging to this VLAN ID to pass through to other configured VLAN IDs that have Inter VLAN Routing enabled.

Figure 20: Adding VLAN memberships to the LAN



Operation succeeded

AVAILABLE VLANS

This page shows a list of available VLANs which a user can edit or delete. A user can add a new VLAN from this page as well.

List of available VLANs

□	Name	ID
□	Default	1
□	VLAN1	2

2.3.1 VLAN Configuration Options

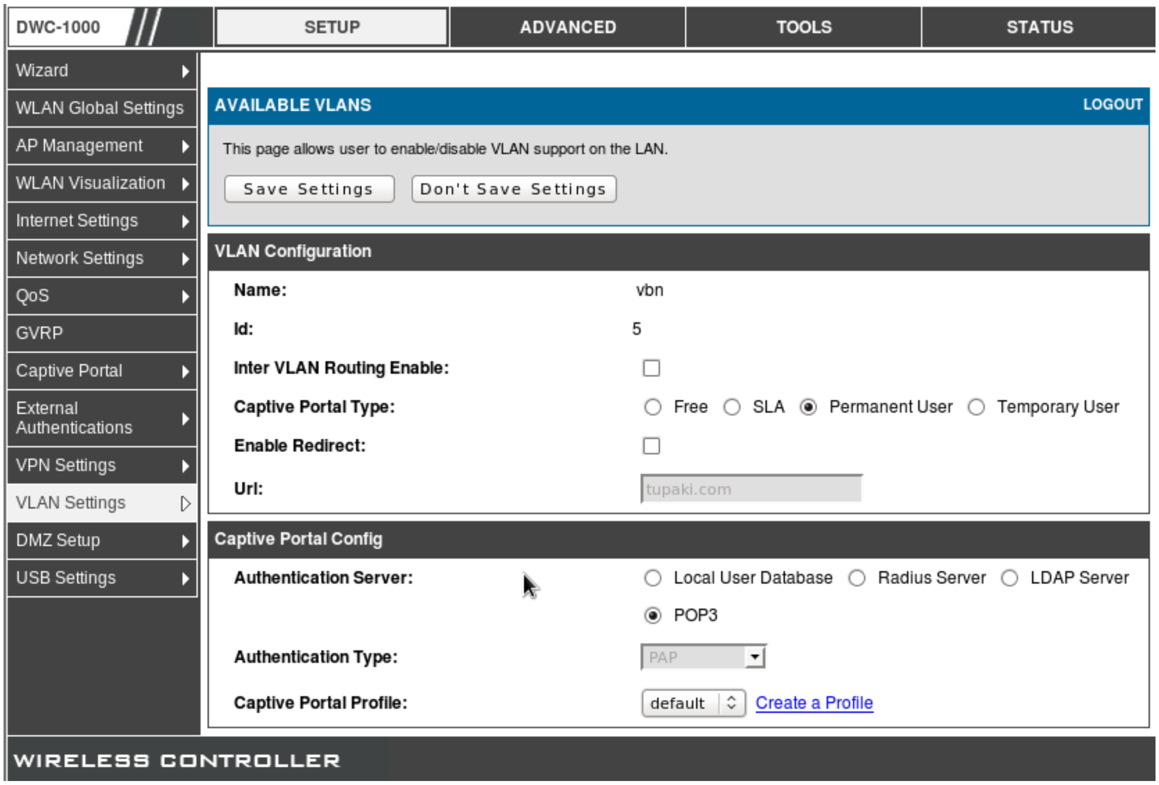
Setup>VLAN Settings> VLAN Configuration

As part of VLAN configuration, the user can enable specific features for clients within that network.

Inter VLAN routing allows clients with that VLAN ID to communicate to other clients in different VLANs, as long as the other VLAN also has inter-VLAN routing enabled. Without this option, VLAN clients are isolated and cannot communicate between each other.

Another feature that can be enabled and configured on a per-VLAN basis is the captive portal. While the captive portal profiles and display are defined in the ***Setup > Captive Portal*** section, this configuration page allows the admin to add Captive Portal support for that VLAN by choosing a Captive Portal type.

Figure 21: VLAN Configuration Options



AVAILABLE VLANS

This page allows user to enable/disable VLAN support on the LAN.

VLAN Configuration

Name: vbn

Id: 5

Inter VLAN Routing Enable: □

Captive Portal Type: ○ Free ○ SLA ● Permanent User ○ Temporary User

Enable Redirect: □

Url: tupaki.com

Captive Portal Config

Authentication Server: ○ Local User Database ○ Radius Server ○ LDAP Server ● POP3

Authentication Type: PAP

Captive Portal Profile: default Create a Profile

Captive Portal Type: Select any of the 4 types of access types Free, SLA, Permanent User, and Temporary User.

- **Free**: No authentication is required for users connected to this VLAN . This option means that the VLAN does not have Captive Portal in use for joining this network.

- **SLA**: SLA stands for Service Level Agreement. If this is selected as Captive Portal type, then users connected to this VLAN needs to accept Service Level Agreement before accessing anything outside this VLAN.

- **Permanent User**: When this option is selected users need to get authenticated before accessing data outside this VLAN. Only permanent Captive Portal users can login from this VLAN. Administrator can create Permanent Captive portal users, only those users can login from captive portal to access data outside VLAN

- **Temporary User**: When this option is selected, users will get authenticated before accessing data outside this VLAN. Only temporary Captive Portal users created by front desk user can login from this VLAN. Administrator can create front desk user and front desk user will login to front desk page and he will generate Temporary users. Only Temporary users created by front desk user are allowed to access data outside VLAN

Enable Redirect: Selecting this option will enable redirection for captive portal user after login to the captive portal page successfully. This is available for SLA, Permanent User, and Temporary User types. For the SLA type, the user will be redirected to the SLA page or the logout page based on the user agreement on the re-directed page.

URL: This field accepts the redirection URL if ‘Enable Redirect’ is selected. This is the site that the user will be taken to after success portal login.

Authentication Server: This lists the available authentication servers among which one can be selected for this VLAN. All users login into the captive portal for this VLAN are authenticated through the selected server. This option appears only if Captive Portal type is selected as Permanent user. The list of available authentication servers is Local User Database, RADIUS Server, LDAP Server and POP3. Whenever a Permanent user tries to login to the captive portal the user will be authenticated based on the Authentication server type selected by the admin while configuring VLAN.

Authentication Type: This option is available for RADIUS authentication servers. The available authentication types are PAP/CHAP/MSCHAP/MSCHAPV2. Based on Authentication type configured by the admin in VLAN, the portal user will be authenticated.

Captive Portal Profile: The configured and available captive portal login profiles are shown here. Any of the available profiles can be used for the configuring VLAN.

Create a profile: This is a link to create a new captive Portal Login profile. Upon clicking the link the admin will be taken to the configuration page to create new login profile and configure the VLAN with that profile.

2.3.2 Associating VLANs to ports

In order to tag all traffic through a specific LAN port with a VLAN ID, you can associate a VLAN to a physical port.

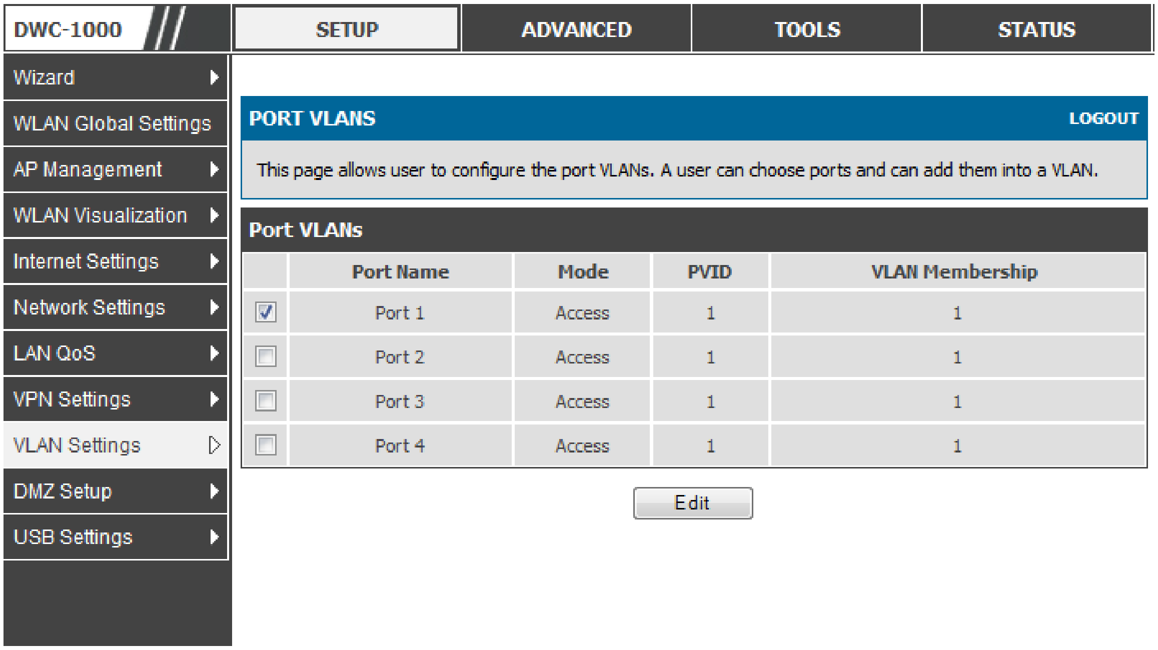
Setup > VLAN Settings > Port VLAN

VLAN membership properties for the LAN and wireless LAN are listed on this page. The VLAN Port table displays the port identifier, the mode setting for that port and VLAN membership information. The configuration page is accessed by selecting one of the four physical ports or a configured access point and clicking Edit.

The edit page offers the following configuration options:

- Mode: The mode of this VLAN can be **General**, **Access**, or **Trunk**. The default is access.
- In **General** mode the port is a member of a user selectable set of VLANs. The port sends and receives data that is tagged or untagged with a VLAN ID. If the data into the port is untagged, it is assigned the defined PVID. In the configuration from Figure 6, Port 3 is a General port with PVID 3, so untagged data into Port 3 will be assigned PVID 3. All tagged data sent out of the port with the same PVID will be untagged. This is mode is typically used with IP Phones that have dual Ethernet ports. Data coming from phone to the controller port on the controller will be tagged. Data passing through the phone from a connected device will be untagged.

Figure 22: Port VLAN list



PORT VLANS

This page allows user to configure the port VLANs. A user can choose ports and can add them into a VLAN.

Port VLANs

	Port Name	Mode	PVID	VLAN Membership
☑	Port 1	Access	1	1
□	Port 2	Access	1	1
□	Port 3	Access	1	1
□	Port 4	Access	1	1

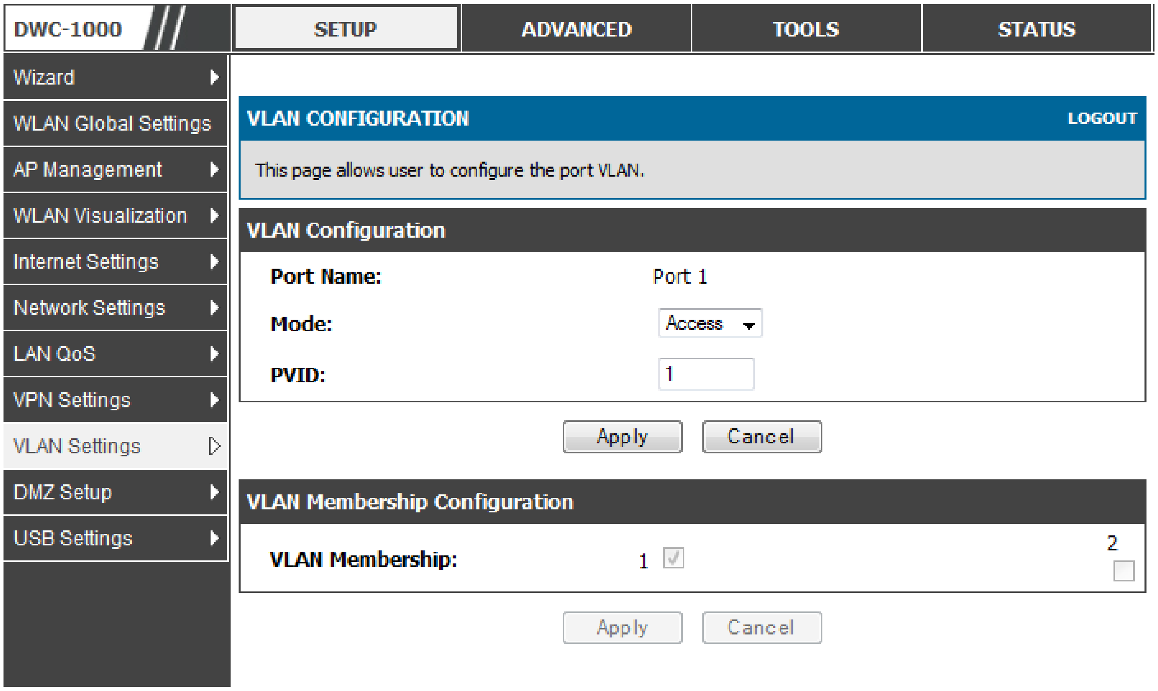
- In **Access** mode the port is a member of a single VLAN (and only one). All data going into and out of the port is untagged. Traffic through a port in access mode looks like any other Ethernet frame.

- In **Trunk** mode the port is a member of a user selectable set of VLANs. All data going into and out of the port is tagged. Untagged coming into the port is not forwarded, except for the default VLAN with PVID=1, which is untagged. Trunk ports multiplex traffic for multiple VLANs over the same physical link.

- Select PVID for the port when the General mode is selected.

- Configured VLAN memberships will be displayed on the VLAN Membership Configuration for the port. By selecting one more VLAN membership options for a General or Trunk port, traffic can be routed between the selected VLAN membership IDs

Figure 23: Configuring VLAN membership for a port



VLAN CONFIGURATION

This page allows user to configure the port VLAN.

VLAN Configuration

Port Name: Port 1

Mode: Access

PVID: 1

VLAN Membership Configuration

VLAN Membership: 1 ☑ 2 □

2.3.3 Multiple VLAN Subnets

Setup > VLAN Settings > Multiple VLAN Subnets

Each configured VLAN ID can map directly to a subnet within the LAN. Each LAN port can be assigned a unique IP address and a VLAN specific DHCP server can be configured to assign IP address leases to devices on this VLAN.

VLAN ID: The PVID of the VLAN that will have all member devices be part of the same subnet range.

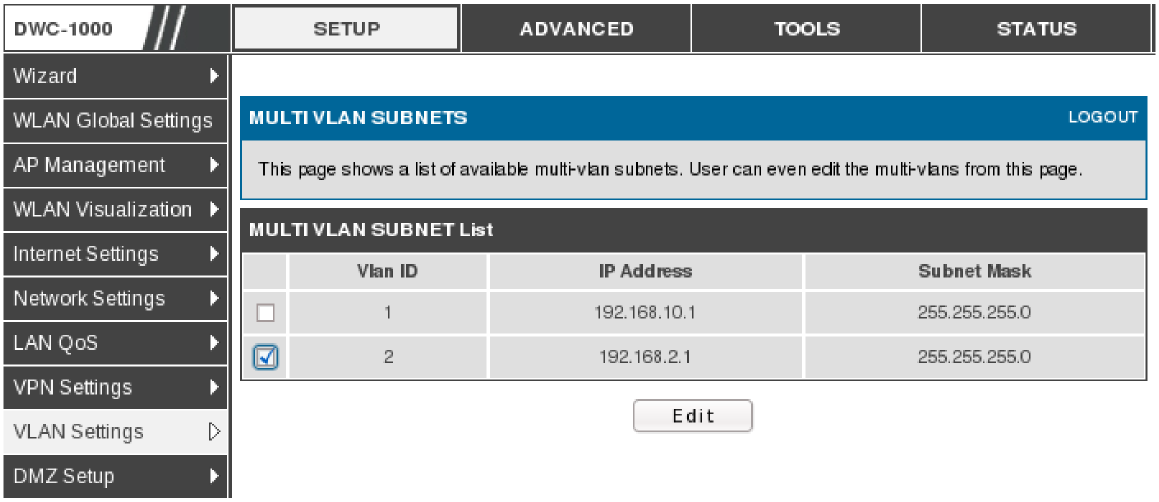
IP Address: The IP address associated with a port assigned this VLAN ID.

Subnet Mask: Subnet Mask for the above IP Address.

The following actions are supported from this page**:**

Edit: The Edit button will link to the Port VLAN Configuration page, allowing you to make changes to the selected port VLAN attributes.

Figure 24: Multiple VLAN Subnets



MULTI VLAN SUBNETS

This page shows a list of available multi-vlan subnets. User can even edit the multi-vlans from this page.

MULTI VLAN SUBNET List

	Vlan ID	IP Address	Subnet Mask
□	1	192.168.10.1	255.255.255.0
☑	2	192.168.2.1	255.255.255.0

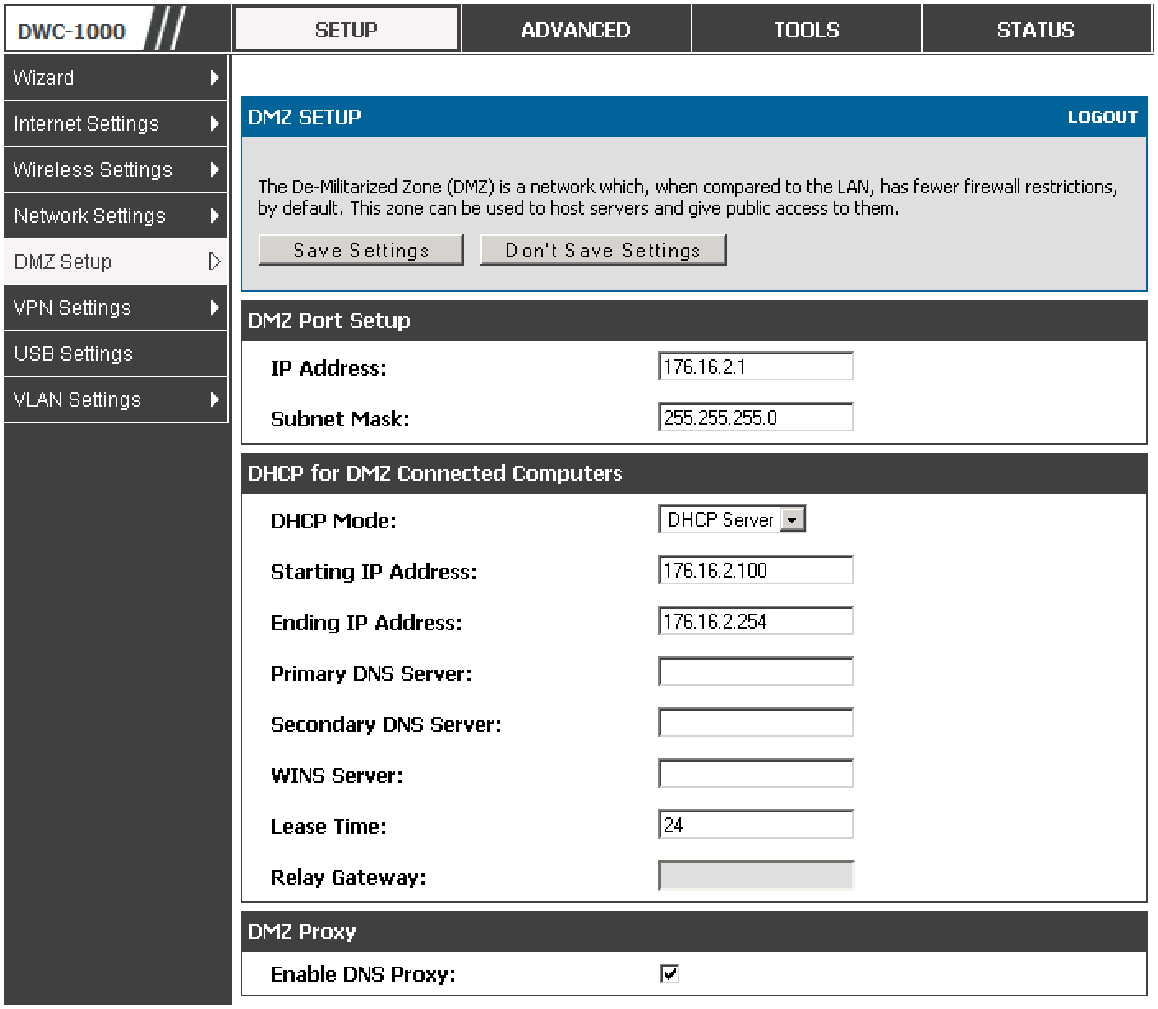
2.4 Configurable Port: DMZ Setup

This controller supports one of the physical ports (Option Ports) to be configured as a secondary Ethernet port or a dedicated DMZ port. A DMZ is a sub network that is open to the public but behind the firewall. The DMZ adds an additional layer of security to the LAN, as specific services/ports that are exposed to the internet on the DMZ do not have to be exposed on the LAN. It is recommended that hosts that must be exposed to the internet (such as web or email servers) be placed in the DMZ network. Firewall rules can be allowed to permit access specific services/ports to the DMZ from both the LAN or Option. In the event of an attack to any of the DMZ nodes, the LAN is not necessarily vulnerable as well.

Setup > DMZ Setup > DMZ Setup Configuration

DMZ configuration is identical to the LAN configuration. There are no restrictions on the IP address or subnet assigned to the DMZ port, other than the fact that it cannot be identical to the IP address given to the LAN interface of this gateway.

Figure 25: DMZ configuration



DMZ SETUP

The De-Militarized Zone (DMZ) is a network which, when compared to the LAN, has fewer firewall restrictions, by default. This zone can be used to host servers and give public access to them.

DMZ Port Setup

IP Address: 176.16.2.1

Subnet Mask: 255.255.255.0

DHCP for DMZ Connected Computers

DHCP Mode: DHCP Server

Starting IP Address: 176.16.2.100

Ending IP Address: 176.16.2.254

Primary DNS Server:

Secondary DNS Server:

WINS Server:

Lease Time: 24

Relay Gateway:

DMZ Proxy

Enable DNS Proxy: ☑

In order to configure a DMZ port, the controller configurable port must be set to DMZ in the ***Setup > Internet Settings > Configurable Port*** page.

2.5 Universal Plug and Play (UPnP)

The following feature is available upon licensed activation of VPN / Firewall features for the system.

Advanced > Advanced Network > UPnP

Universal Plug and Play (UPnP) is a feature that allows the controller to discovery devices on the network that can communicate with the controller and allow for auto configuration. If a network device is detected by UPnP, the controller can open internal or external ports for the traffic protocol required by that network device.

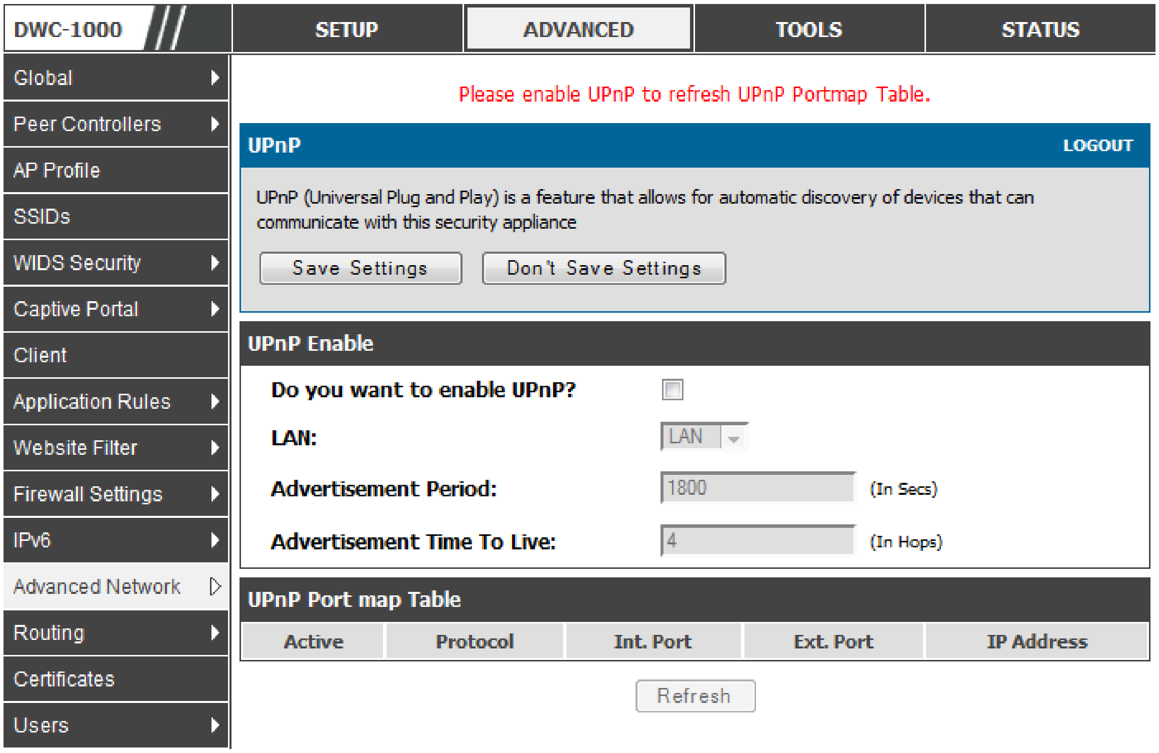
Once UPnP is enabled, you can configure the controller to detect UPnP-supporting devices on the LAN (or a configured VLAN). If disabled, the controller will not allow for automatic device configuration.

Configure the following settings to use UPnP:

Advertisement Period: This is the frequency that the controller broadcasts UPnP information over the network. A large value will minimize network traffic but cause delays in identifying new UPnP devices to the network.

Advertisement Time to Live: This is expressed in hops for each UPnP packet. This is the number of steps a packet is allowed to propagate before being discarded. Small values will limit the UPnP broadcast range. A default of 4 is typical for networks with few controllers.

Figure 26: UPnP Configuration



Please enable UPnP to refresh UPnP Portmap Table.

UPnP

UPnP (Universal Plug and Play) is a feature that allows for automatic discovery of devices that can communicate with this security appliance

UPnP Enable

Do you want to enable UPnP?	□
LAN:	LAN
Advertisement Period:	1800 (In Secs)
Advertisement Time To Live:	4 (In Hops)

UPnP Port map Table

Active	Protocol	Int. Port	Ext. Port	IP Address

UPnP Port map Table

The UPnP Port map Table has the details of UPnP devices that respond to the controller advertisements. The following information is displayed for each detected device:

Active: A yes/no indicating whether the port of the UPnP device that established a connection is currently active

Protocol: The network protocol (i.e. HTTP, FTP, etc.) used by the DWC

Int. Port (Internal Port): The internal ports opened by UPnP (if any)

Ext. Port (External Port): The external ports opened by UPnP (if any)

IP Address: The IP address of the UPnP device detected by this controller

Click Refresh to refresh the port map table and search for any new UPnP devices

2.6 Captive Portal

The captive portal technique forces an HTTP client on a network to see a special web page (usually for authentication purposes) before using the Internet normally. A captive portal turns a web browser into an authentication device.

LAN users can gain internet access via web portal authentication with the appliance. Also referred to as Run-Time Authentication, a Captive Portal is ideal for a web café scenario where users initiate HTTP connection requests for web access but are not interested in accessing any LAN services. Firewall policies set by the administrator will define which users require authentication for HTTP access, and when a matching user request is made the appliance will intercept the request and prompt for a username / password. The login credentials are compared against the Runtime Authentication users in user database prior to granting HTTP access.

A user can use captive portal for guest and registered users at the same time. A captive portal presents a web page which requires action on the part of the user before network access is granted. The required action can be simply viewing and agreeing to an acceptable use policy, or entering a user ID and password which must be validated against a database of authorized users.

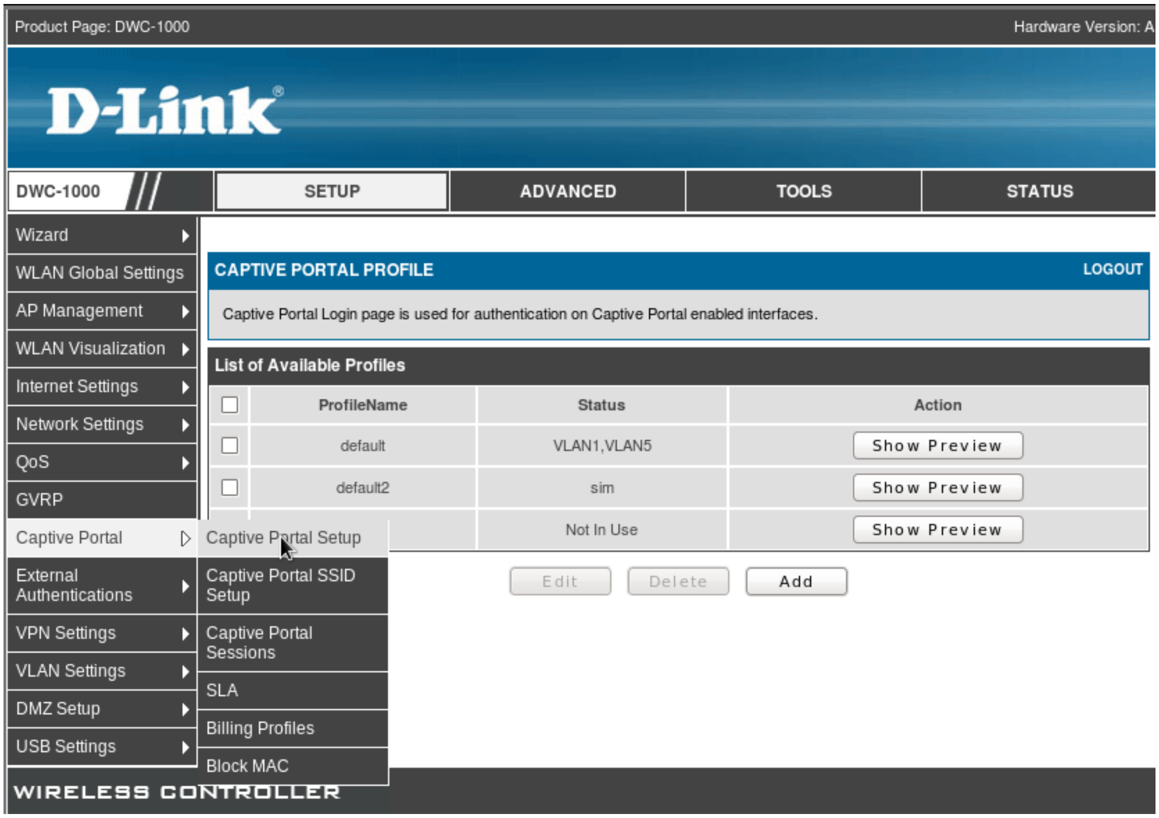
> ✍ Captive Portal is available for LAN and WLAN users only and not for DMZ hosts.

2.6.1 Captive Portal Setup

Setup > Captive Portal > Setup

Captive Portal profiles are the grouping of display settings that are pushed to the WLAN client that hits a particular portal. The Captive Portal Setup page allows for management of these profiles, and this setup page displays configured custom Captive Portal profiles and indicates which are in use.

Figure 27: Captive Portal Setup



CAPTIVE PORTAL PROFILE

Captive Portal Login page is used for authentication on Captive Portal enabled interfaces.

List of Available Profiles

□	ProfileName	Status	Action
□	default	VLAN1,VLAN5	Show Preview
□	default2	sim	Show Preview
		Not In Use	Show Preview

List of Available Profiles

Any one of these profiles can be used for Captive Portal Login page while enabling Captive Portal.

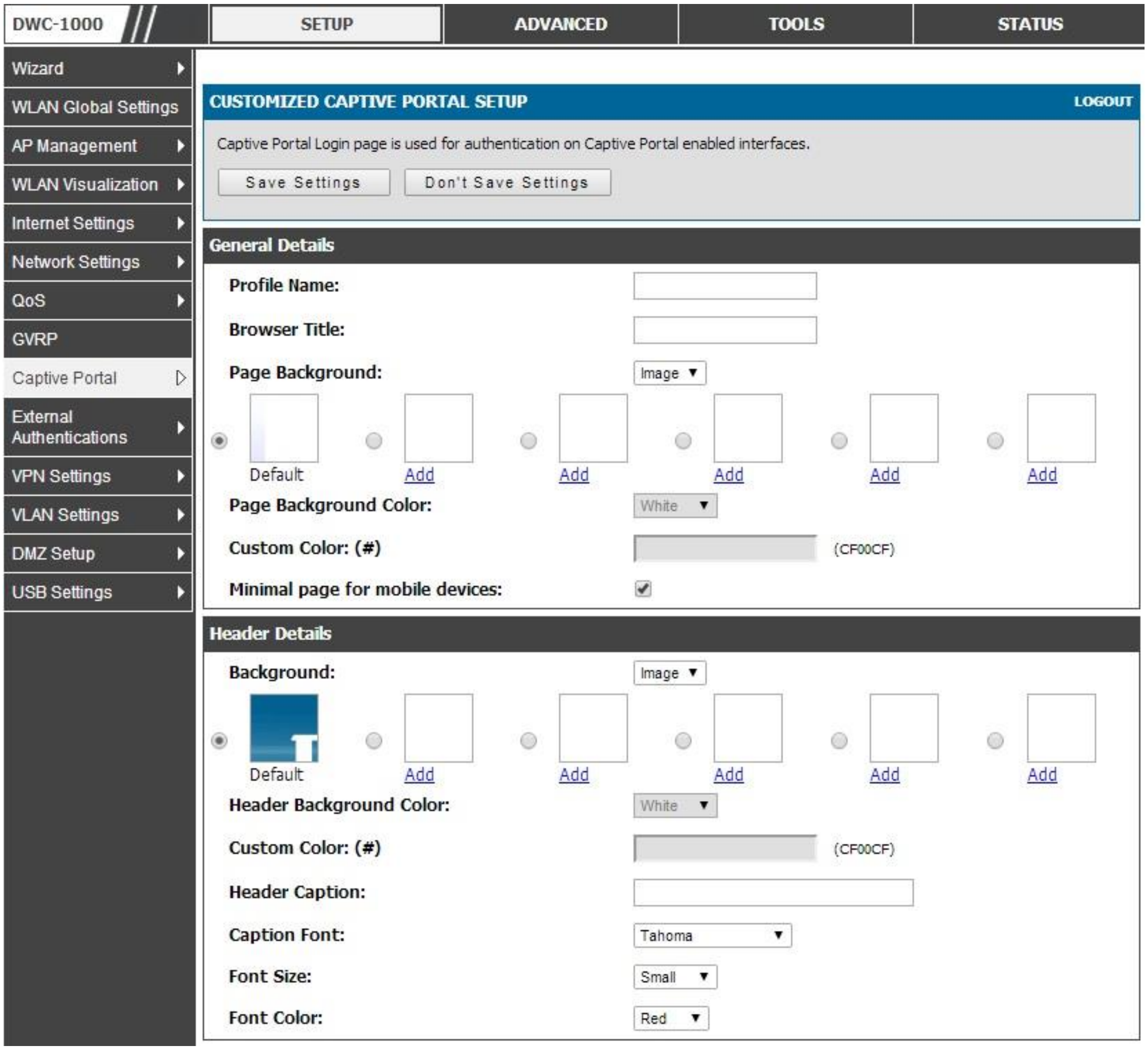
Edit: Can edit the added profiles. The default Profile cannot be edited.

Delete: Will delete the profile selected. You cannot delete the default profile and the current profile being used.

Add: Will let you add a new profile. Maximum allowed number of profiles are 5 excluding default.

Show Preview: Will show preview of the page, if a profile is selected.

Figure 28: Adding or Editing a Custom Captive Portal



CUSTOMIZED CAPTIVE PORTAL SETUP

Captive Portal Login page is used for authentication on Captive Portal enabled interfaces.

General Details

Profile Name:

Browser Title:

Page Background: Image

Page Background Color: White

Custom Color: (#) (CF00CF)

Minimal page for mobile devices: ☑

Header Details

Background: Image

Header Background Color: White

Custom Color: (#) (CF00CF)

Header Caption:

Caption Font: Tahoma

Font Size: Small

Font Color: Red

Managing an existing or creating a new captive portal profile will direct the admin to the Customized Captive Portal Setup page. This page defines what the wireless client will see (messages, color, background, page titles, web page headers etc.) as part of hitting the Captive Portal page.

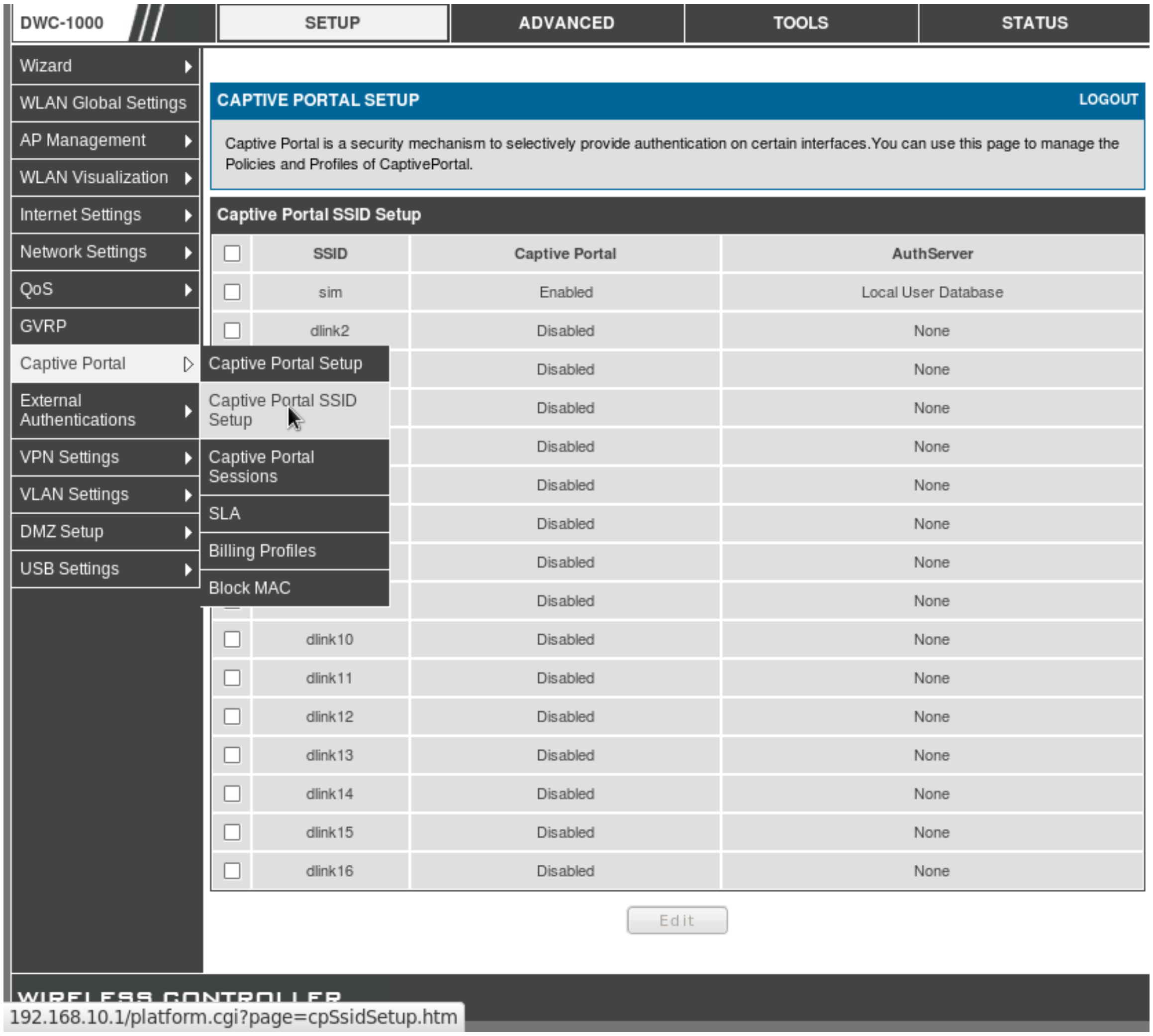
After customizing the profile, the admin has access to this profile to configuring captive portal on VLAN or for a particular SSID. This customized profile will be shown in captive portal login page.

2.6.2 Captive Portal SSID Setup

Setup > Captive Portal > Captive Portal SSID Setup

This feature allows the administrator to configure existing SSIDs with Captive Portal authentication. These SSID's can be those hosted by this system or by AP's managed by this WLAN controller. By default this page contains 16 SSIDs to configure. If needed, the appliance supports another 48 SSIDs to enable for Captive Portal vial the SSIDs page in the advanced settings.

Figure 29: List of SSID's associated with Captive Portals



CAPTIVE PORTAL SETUP

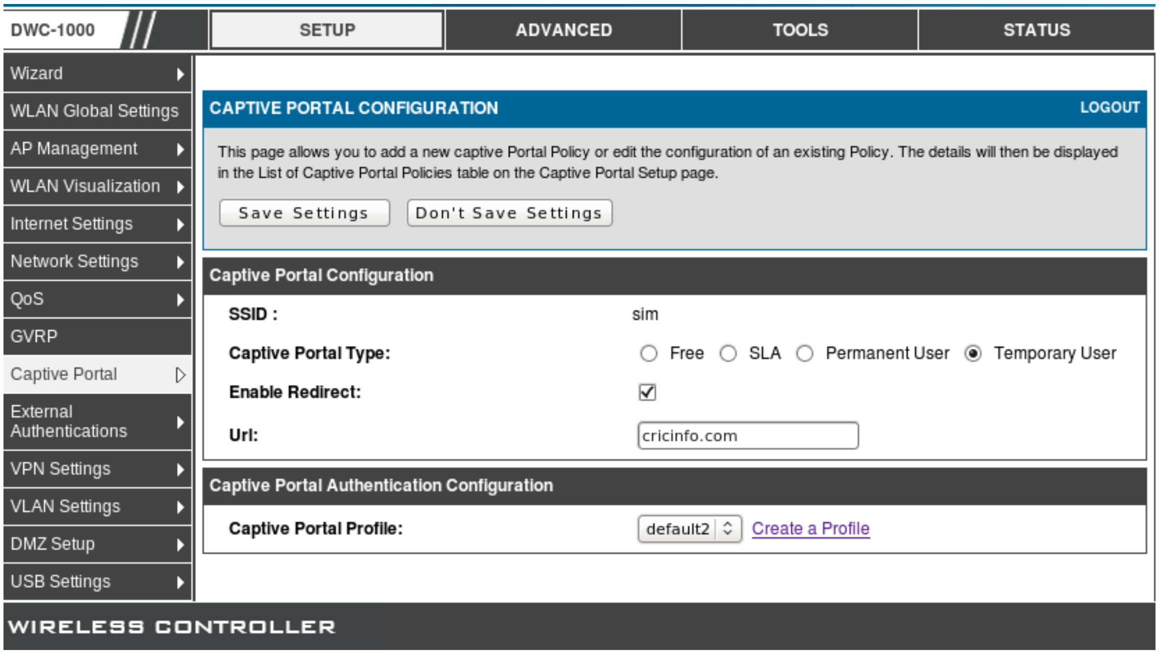
Captive Portal is a security mechanism to selectively provide authentication on certain interfaces.You can use this page to manage the Policies and Profiles of CaptivePortal.

Captive Portal SSID Setup

□	SSID	Captive Portal	AuthServer
□	sim	Enabled	Local User Database
□	dlink2	Disabled	None
		Disabled	None
		Disabled	None
		Disabled	None
		Disabled	None
		Disabled	None
		Disabled	None
		Disabled	None
□	dlink10	Disabled	None
□	dlink11	Disabled	None
□	dlink12	Disabled	None
□	dlink13	Disabled	None
□	dlink14	Disabled	None
□	dlink15	Disabled	None
□	dlink16	Disabled	None

Selecting an SSID and clicking Edit will allow that SSID to be associated with a Captive Portal profile. The Captive Portal Configuration page will be available for that SSID.

Figure 30: Associating a Captive Portal to a specific SSID



CAPTIVE PORTAL CONFIGURATION

This page allows you to add a new captive Portal Policy or edit the configuration of an existing Policy. The details will then be displayed in the List of Captive Portal Policies table on the Captive Portal Setup page.

Captive Portal Configuration

SSID : sim

Captive Portal Type: ○ Free ○ SLA ○ Permanent User ● Temporary User

Enable Redirect: ☑

Url: cricinfo.com

Captive Portal Authentication Configuration

Captive Portal Profile: default2

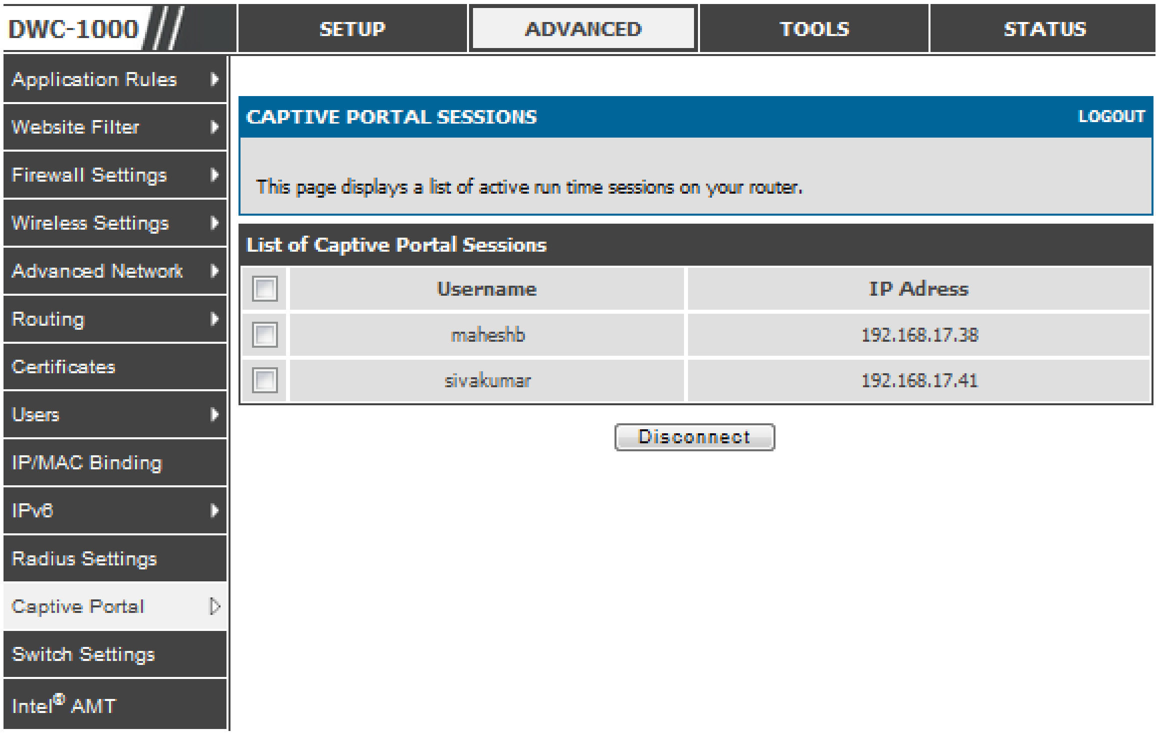
The fields of this configuration page match that of the VLAN Configuration page.

2.6.3 Captive Portal Session

Setup > Captive Portal > Captive Portal Sessions

The Active Runtime internet sessions through the controller firewall are listed in the below table. These users are present in the local or external user database and have had their login credentials approved for internet access. A ‘Disconnect’ button allows the DWC-1000 admin to selectively drop an authenticated user.

Figure 31: Active Runtime sessions



CAPTIVE PORTAL SESSIONS

This page displays a list of active run time sessions on your router.

List of Captive Portal Sessions

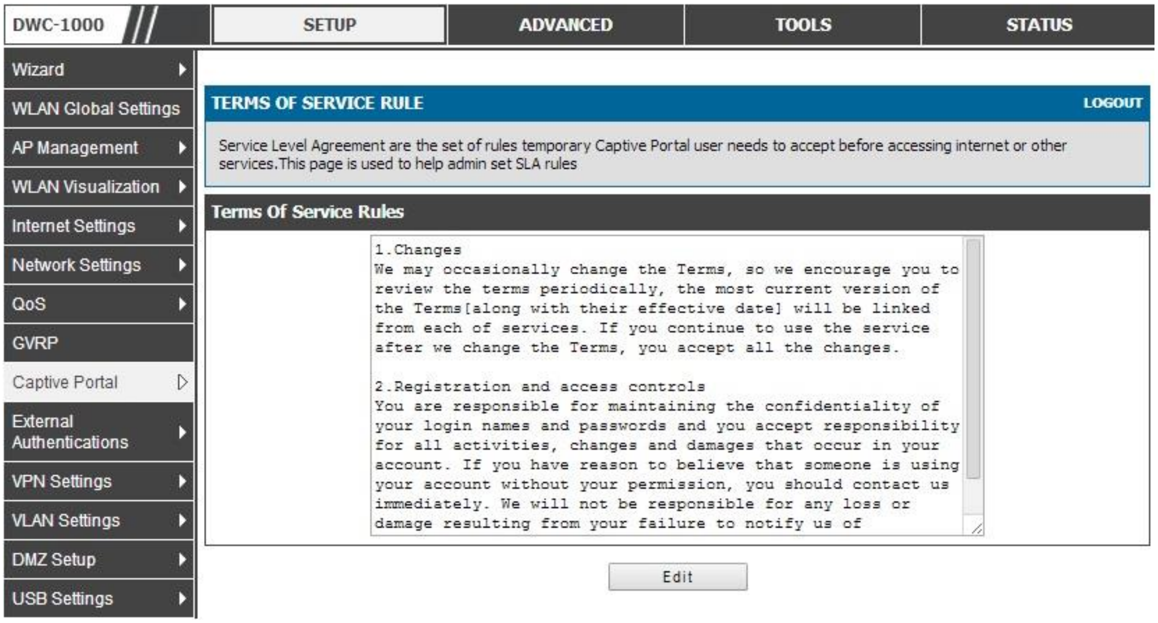
□	Username	IP Adress
□	maheshb	192.168.17.38
□	sivakumar	192.168.17.41

2.6.4 Service Level Agreement (SLA)

Setup>Captive Portal>SLA

This section allows the administrator to modify the Service Level Agreement, which is the set of rules to be accepted before the appliance grants internet access in case of temporary and SLA type captive portal users.

Figure 32: Defining the Terms of Service for a Portal



TERMS OF SERVICE RULE

Service Level Agreement are the set of rules temporary Captive Portal user needs to accept before accessing internet or other services.This page is used to help admin set SLA rules

Terms Of Service Rules

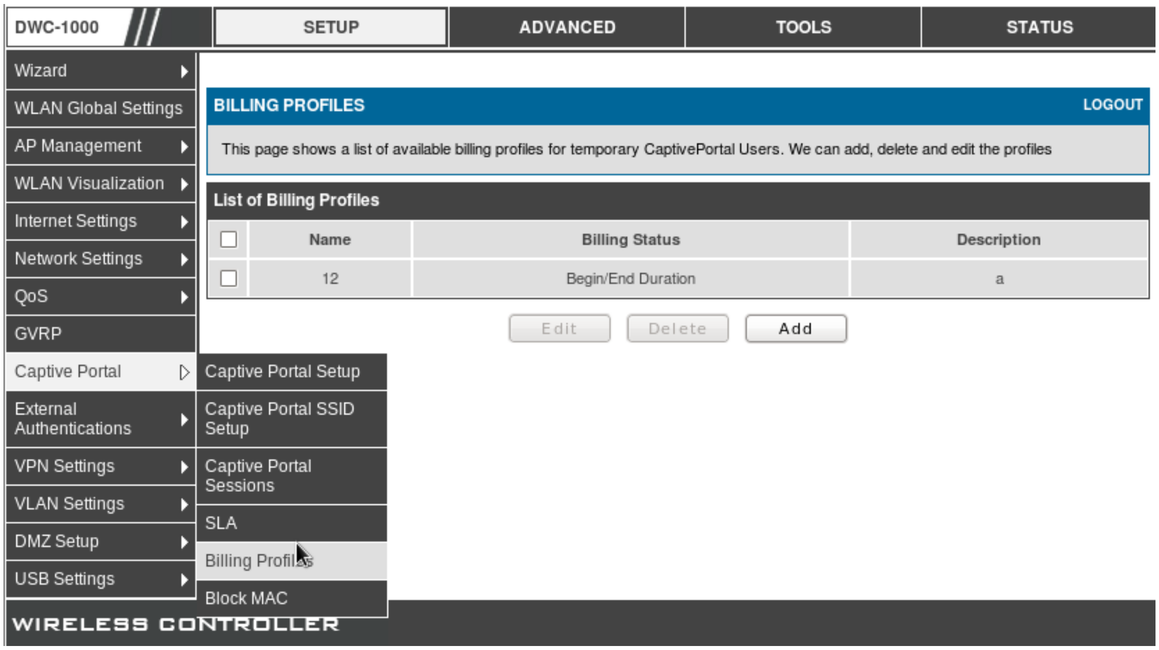
```
1.Changes
We may occasionally change the Terms, so we encourage you to
review the terms periodically, the most current version of
the Terms[along with their effective date] will be linked
from each of services. If you continue to use the service
after we change the Terms, you accept all the changes.

2.Registration and access controls
You are responsible for maintaining the confidentiality of
your login names and passwords and you accept responsibility
for all activities, changes and damages that occur in your
account. If you have reason to believe that someone is using
your account without your permission, you should contact us
immediately. We will not be responsible for any loss or
damage resulting from your failure to notify us of
```

2.6.5 Billing Profiles

Setup>Captive Portal>Billing Profiles

This feature allows the administrator to create customized accounting and billing types using billing profiles. All profiles created here are displayed to front desk user on their homepage. The front desk user has administrative privileges to generate temporary captive portal users for a profile and those users will be having these accounting and billing properties applied.

Figure 33: List of Configured Billing Profiles



BILLING PROFILES

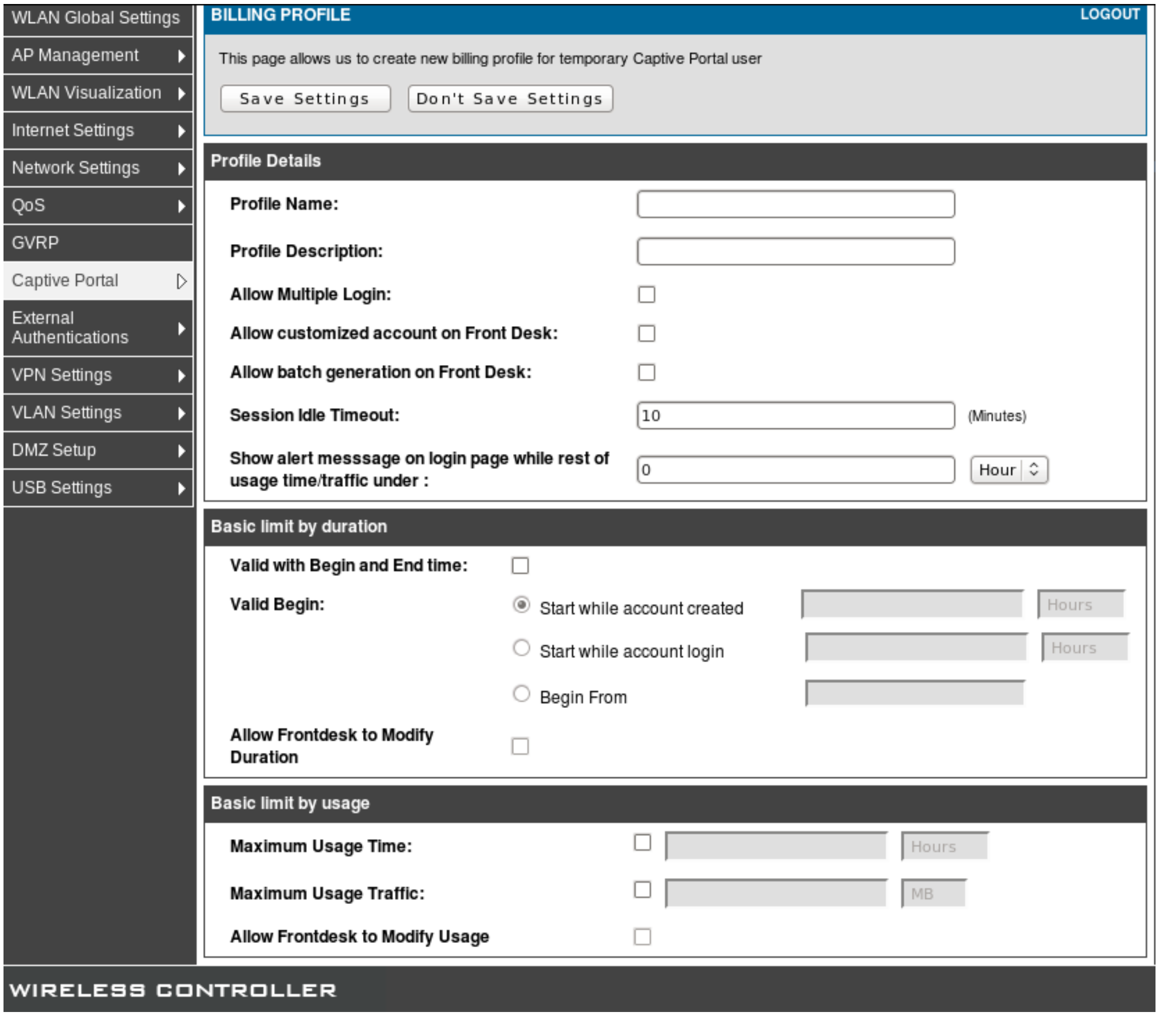
This page shows a list of available billing profiles for temporary CaptivePortal Users. We can add, delete and edit the profiles

List of Billing Profiles

□	Name	Billing Status	Description
□	12	Begin/End Duration	a

Adding or modifying a billing profile will open the selected Profile's setup page.

Figure 34: Billing Profiles Configuration Settings



This page allows us to create new billing profile for temporary Captive Portal user

Profile Details

Profile Name:	
Profile Description:	
Allow Multiple Login:	□
Allow customized account on Front Desk:	□
Allow batch generation on Front Desk:	□
Session Idle Timeout:	10 (Minutes)
Show alert messsage on login page while rest of usage time/traffic under :	0 Hour

Basic limit by duration

Valid with Begin and End time:	□		
Valid Begin:	● Start while account created		Hours
	○ Start while account login		Hours
	○ Begin From		
Allow Frontdesk to Modify Duration	□		

Basic limit by usage

Maximum Usage Time:	□		Hours
Maximum Usage Traffic:	□		MB
Allow Frontdesk to Modify Usage	□		

Profile Name: Each profile uses a unique Name to identify itself. This profile name will be displayed whenever the front desk user login to the front desk page to create temporary users.

Profile Description: A helpful description of the purpose / intent of this profile can be noted here for future administrator reference.

Allow Multiple Login: Selecting this option will allow multiple wireless users to employ the same captive portal login credentials created for this profile to login simultaneously.

Allow customized account on Front Desk: This option will let the front desk user (who can administer captive portal credentials) to give customized account name to the captive portal users being created on this profile.

Allow batch generation on Front Desk: Selecting this option enables the front desk user to generate a batch of temporary CP users at one click.

Session Idle Timeout: This defines the Idle timeout for CP users generated for this profile.

Show alert message on login page while rest of usage time/traffic under: Enter a value here in Hours/Days/MB/GB to get an alert message when usage time/traffic left reaches the desired limit. By default if 0 is entered it implies no alert message is required.

Basic Limit by Duration

This is section is used to configure the parameters required in limiting the user access on duration basis.

Valid Begin: There are 3 types of limiting user access by duration.

Start While Account Created: This option is to activate account when user is created

Start While Account Login: This option is to activate account when user first login using his credentials.

Begin From: This option is to activate account from this date

Allow Frontdesk to modify duration: Checking this option enables the Frontdesk user to modify duration limits.

Basic Limit by Usage

This section is for limiting user on Usage basis.

Maximum Usage Time: used to set maximum time user can stay login before his account expires

Maximum Usage Traffic: used to set maximum traffic user can use before his account expires. Only inbound traffic shall be considered towards bandwidth usage.

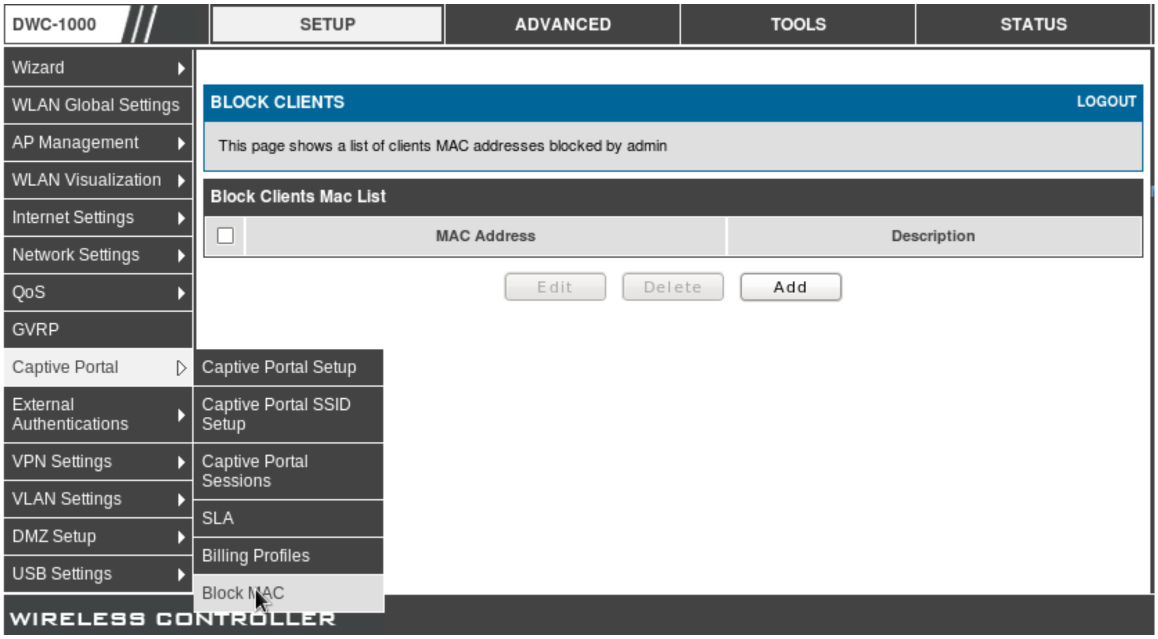
Allow Frontdesk to modify usage: Checking this option enables the Frontdesk user to modify usage limits.

2.6.6 Block MAC

Setup>Captive Portal>Block MAC

This feature allows the administrator to add a MAC address and description of the corresponding device to a "black list" for the Captive Portal. Adding a MAC address to the list will result in denying access to the clients having these MAC address.

Figure 35: List of MAC addresses not allowed to authenticate via the Captive Portal



This page shows a list of clients MAC addresses blocked by admin

Block Clients Mac List

□	MAC Address	Description

2.6.7 Hotspot

Hotspot support is a feature that offers Internet access over a wireless local area network (WLAN) through the use of a router connected to a link to an Internet service provider. Hotspots typically use Wi-Fi to offer clients internet service via approval through the captive portal.

The typical Hotspot application is an administrator at a front desk or reception granting temporary user accounts for internet access through a captive portal. This portal will have an SLA and associated billing profile. Whenever the front desk admin creates new temporary user accounts, the admin will have to push these temporary accounts to the peer controller manually via the DWC GUI.

However in a clustering setup, temporary users created in one controller will be pushed automatically to the peer controller. The billing profiles associated with that user will have to be pushed manually to peer controllers in advance. This will allow the auto-synchronization of temporary users to take place between peer controllers.

Example:

- In a hotel, the controller administrator creates a set of billing and captive portal profiles and pushes them from the DWC controller to all peer controllers
- The front desk administrator creates temporary accounts for a new guest
- The temporary accounts will be pushed automatically to all peer controllers so that guests can have access to the portal and be authenticated for internet access from any floor, any peer controller.

The front desk administrator has the ability to create 256 temporary users. Each peer controller can manage 1024 total temporary users. For the auto-synchronization to work it is a requirement that each controller in the cluster have synchronized time settings, to enable time-based billing or accounting for the user.

> ✍ Note: accounting is on a per-controller basis. This means that a temporary user authenticated on one controller will not have its usage statistics shared among controllers in the event that the same user credentials are used to authenticate via another peer or cluster controller.

2.6.8 Captive Portal Front Desk

The Front Desk user has the ability to create temporary user accounts for internet access thorugh the Captive Portal. This user does not have full administrative priviledges, but instead will be able to create a user based on pre-defined billing profiles.

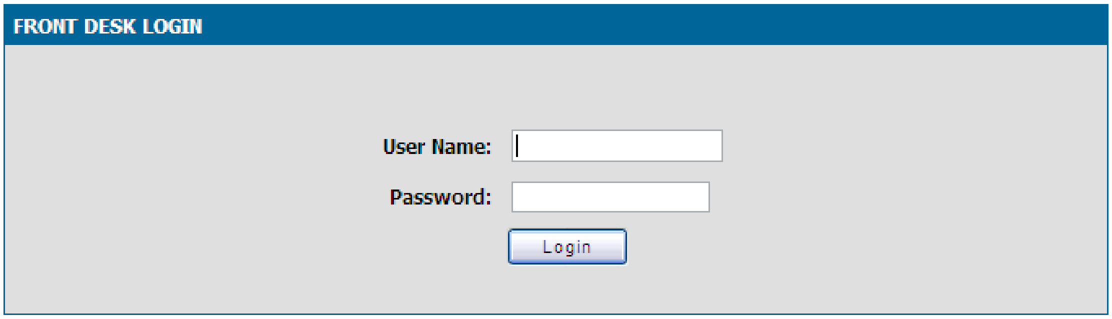
All created Billing Profiles (described in Section 2.6.5) are available for display on the Front Desk user's admin page. From this page, create a new temporary user ID and associate a pre-defined Billing Profile to this user. The Front Desk user will b able to leverage the features like batch user generation, customized account names, or modifying usage limits for these temporary CP users if the admin has enabled the Billing Profile with this support.

Section 2.6.2 outlines how to associate an SSID for Captive Portal authentication. For users given access by the Front Desk, the Captive Portal Type needs to be a temporary user. This will allow for the usage limits to have control on the amount or duration of internet access.

The last step to leverage this feature is to create a Front Desk group and assign a user to this group (i.e. username = HotelAdmin). The Front Desk user (HotelAdmin) will be allowed to access the appliance's management interface via the following URL: <Controller_LAN_IP>/frontdesk. With the defined login credentials the Front Desk user can now create and customize temporary accounts for internet access through the selected Billing Profile.

- ✍ The entered URL of <Controller_LAN_IP>/frontdesk will redirect to <Controller_LAN_IP>/platform.cgi?page=billingDeskLogin.htm. I.e. if the LAN IP address is the default 192.168.10.1, then the Front Desk user's entry of 192.168.10.1/frontdesk" in their browser's URL will redirect to http://192.168.10.1/platform.cgi?page=billingDeskLogin.htm.
- ✍ Opening the Front Desk page from the same browser as the current admin session will not auto-redirect to the correct page.

Figure 36: Login prompt for Front Desk users



FRONT DESK LOGIN

User Name:

Password:

In the Front Desk configuration page, attributes enabled in the Billing Profile are available for management, such as batch user generation, customized account names, or modifying usage limits. The Generate button is required to create the Temporary User accounts, and the View Accounts section has a summary of all users generated by this Front Desk User.

2.7 WLAN global configuration

Setup > WLAN Global Settings

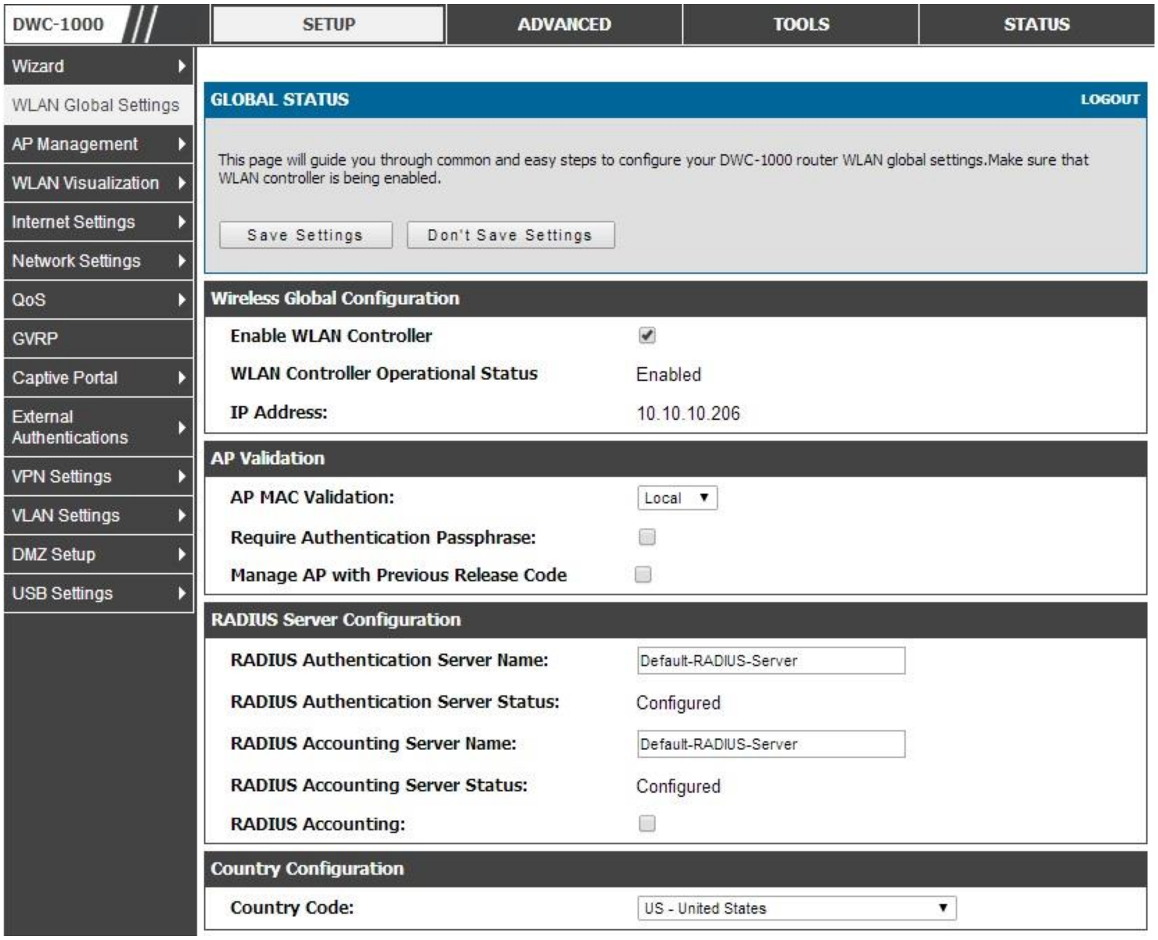
Following are the options available to enable the WLAN function on DWC-1000

Enable WLAN Controller: Select this option to enable WLAN controller functionality on the system. Clear the option to administratively disable the WLAN controller. If you clear the option, all peer controller and APs that are associated with this controller are disassociated. Disabling the WLAN controller does not affect non-WLAN features on the controller, such as VLAN or STP functionality.

WLAN Controller Operational Status: Shows the operational status of the controller. The status can be one of the following values:

- Enabled
- Enable-Pending
- Disabled
- Disable-Pending

Figure 37: WLAN global configuration



GLOBAL STATUS

This page will guide you through common and easy steps to configure your DWC-1000 router WLAN global settings.Make sure that WLAN controller is being enabled.

Wireless Global Configuration

Enable WLAN Controller	☑
WLAN Controller Operational Status	Enabled
IP Address:	10.10.10.206

AP Validation

AP MAC Validation:	Local ▼
Require Authentication Passphrase:	□
Manage AP with Previous Release Code	□

RADIUS Server Configuration

RADIUS Authentication Server Name:	Default-RADIUS-Server
RADIUS Authentication Server Status:	Configured
RADIUS Accounting Server Name:	Default-RADIUS-Server
RADIUS Accounting Server Status:	Configured
RADIUS Accounting:	□

Country Configuration

Country Code:	US - United States ▼

IP Address: This field shows the IP address of the WLAN interface on the controller. If the controller does not have the Routing Package installed, or if routing is disabled, the IP address is the network interface. If the routing package is installed and enabled, this is the IP address of the routing or loopback interface you configure for the controller features.

AP MAC Validation Method: Add the MAC address of the AP to the Valid AP database, which can be kept locally on the controller or in an external RADIUS server. When the controller discovers an AP that is not managed by another ccontroller, it looks up the MAC address of the AP in the Valid AP database. If it finds the MAC address in the database, the controller validates the AP and assumes management. Select the database to use for AP validation and, optionally, for authentication if the Require Authentication Passphrase option is selected.

- **Local**: If you select this option, you must add the MAC address of each AP to the local Valid AP database.
- **RADIUS**: If you select this option, you must configure the MAC address of each AP in an external RADIUS server.

Require Authentication Passphrase: Select this option to require APs to be authenticated before they can associate with the controller. If you select this option, you must configure the passphrase on the AP while it is in standalone mode as well as in the Valid AP database.

RADIUS Authentication Server Name: Enter the name of the RADIUS server used for AP and client authentications. The name can contain up to 32 alphanumeric characters. Spaces, underscores, and dashes are also permitted. The controller acts as the RADIUS client and performs all RADIUS transactions on behalf of the APs and wireless clients.

RADIUS Authentication Server Configured: Indicates whether the RADIUS authentication server is configured.

RADIUS Accounting Server Name: Enter the name of the RADIUS server used for reporting wireless client associations and disassociations. The name can contain up to 32 alphanumeric characters. Spaces, underscores, and dashes are also permitted.

RADIUS Accounting Server Configured: Indicates whether the RADIUS accounting server is configured.

RADIUS Accounting: Select to enable RADIUS accounting for wireless clients.

Country Code: Select the country code that represents the country where your controller and APs operate. When you click Submit, a pop-up message asks you to confirm the change. Wireless regulations vary from country to country. Make sure you select the correct country code so that your WLAN system complies with the regulations in your country.

2.8 Wireless Discovery configuration

The wireless controller can discover, validate, authenticate, or monitor the following system devices:

- Peer wireless controllers
- APs
- Wireless clients
- Rogue APs
- Rogue wireless clients

Setup > AP Management > Poll List

The wireless controller can discover peer wireless controller and APs regardless of whether these devices are connected to each other, located in the same Layer 2 broadcast domain, or attached to different IP subnets. In order for the controller to discover other WLAN devices and establish communication with them, the devices must have their own IP address, must be able to find other WLAN devices, and must be compatible. When the controller discovers and validates APs, the controller takes over the management of the AP. If you configure the AP in Standalone mode, the existing AP configuration is replaced by the default AP Profile configuration on the controller.

L3/IP Discovery: Select or clear this option to enable or disable IP-based discovery of access points and peer wireless controller. When the L3/IP Discovery option is selected, IP polling is enabled and the controller will periodically poll each address in the configured IP List. By default, L3/IP Discovery is enabled.

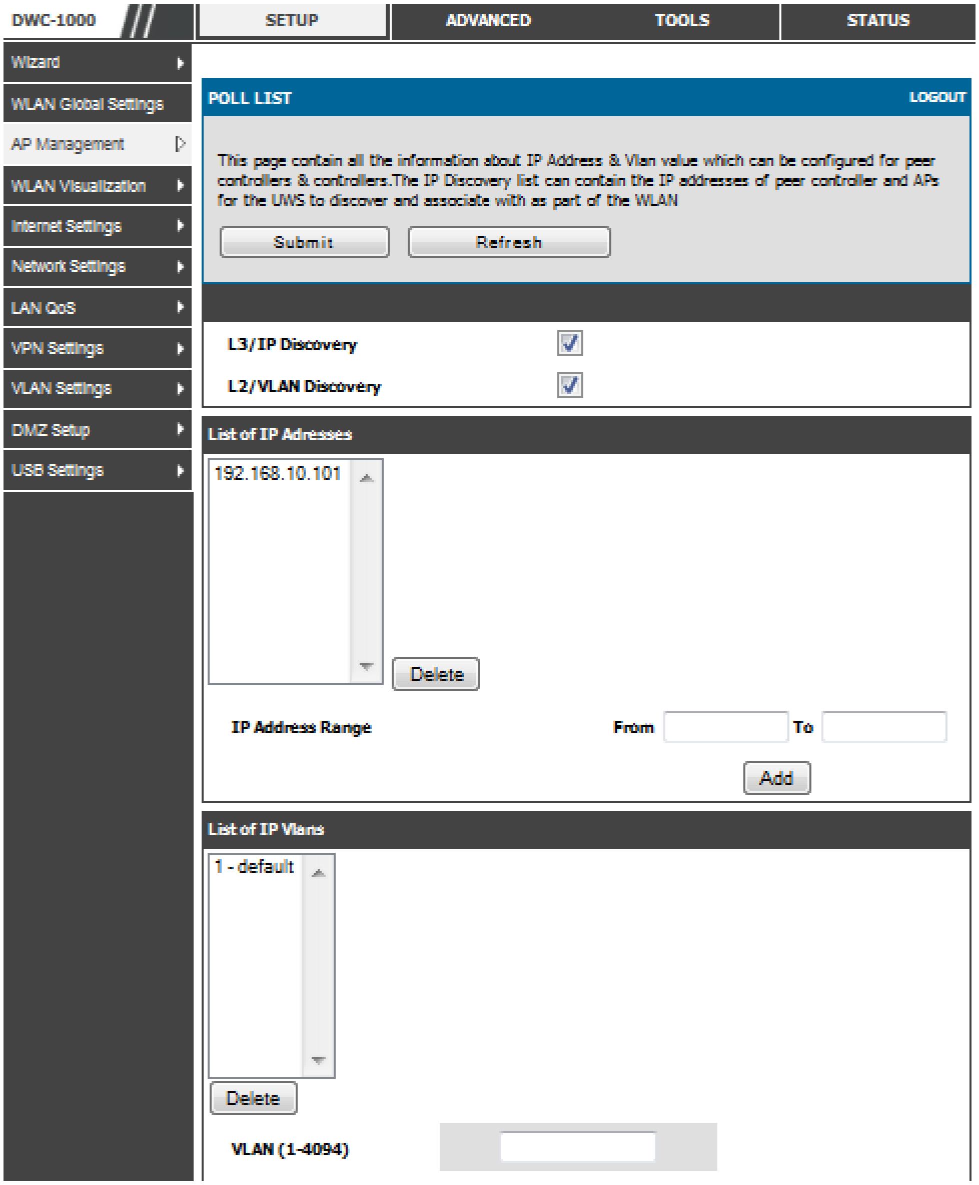
List of IP Address: Shows the list of IP addresses configured for discovery.

To remove entries from the list, select one or more entries and click Delete. Hold the "shift" key or “control” key to select specific entry.

IP Address Range: This text field is used to add a range of IP address entries to the IP List. Enter the IP address at the start of the address range in the From field, and enter the IP address at the end of the range in the To field, then click

Add. All IP addresses in the range are added to the IP List. Only the last octet is allowed to differ between the From address and the To address.

Figure 38: Configuring the Wireless Discovery



POLL LIST

This page contain all the information about IP Address & Vlan value which can be configured for peer controllers & controllers.The IP Discovery list can contain the IP addresses of peer controller and APs for the UWS to discover and associate with as part of the WLAN

L3/IP Discovery ☑

L2/VLAN Discovery ☑

List of IP Adresses

192.168.10.101

IP Address Range From To

List of IP Vlans

1 - default

VLAN (1-4094)

L2/VLAN Discovery: The D-Link Wireless Device Discovery Protocol is a good discovery method to use if the controller and APs are located in the same Layer 2 multicast domain. The wireless controller periodically sends a multicast packet containing the discovery message on each VLAN enabled for discovery

The following actions are supported from this page:

Add: Adds the data in the IP Address or VLAN field to the appropriate list.

Delete: Deletes the selected entry from the IP or VLAN list.

2.8.1 Wireless Discovery Status

Status > Global Info > IP Discovery

The IP Discovery list can contain the IP addresses of peer controller and APs for the DWC-1000 to discover and associate with as part of the WLAN

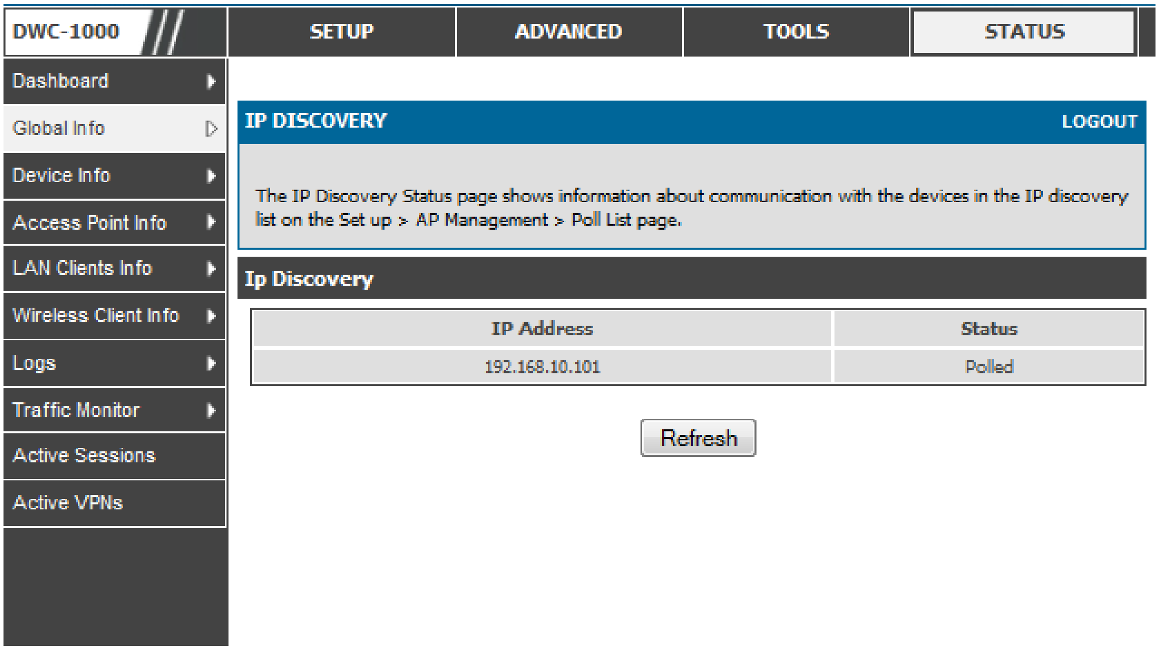
IP Address: Shows the IP address of the device configured in the IP Discovery list

Status: The wireless discovery status is in one of the following states:

- **Not Polled**: The controller has not attempted to contact the IP address in the L3/IP Discovery list.
- **Polled**: The controller has attempted to contact the IP address.
- **Discovered**: The controller contacted the peer controller or the AP in the L3/IP Discovery list and has authenticated or validated the device.
- **Discovered - Failed**: The controller contacted the peer controller or the AP with IP address in the L3/IP Discovery list and was unable to authenticate or validate the device.

If the device is an access point, an entry appears in the AP failure list with a failure reason.

Figure 39: Wireless Discovery status



IP DISCOVERY

The IP Discovery Status page shows information about communication with the devices in the IP discovery list on the Set up > AP Management > Poll List page.

Ip Discovery

IP Address	Status
192.168.10.101	Polled

The following actions are supported from this page:

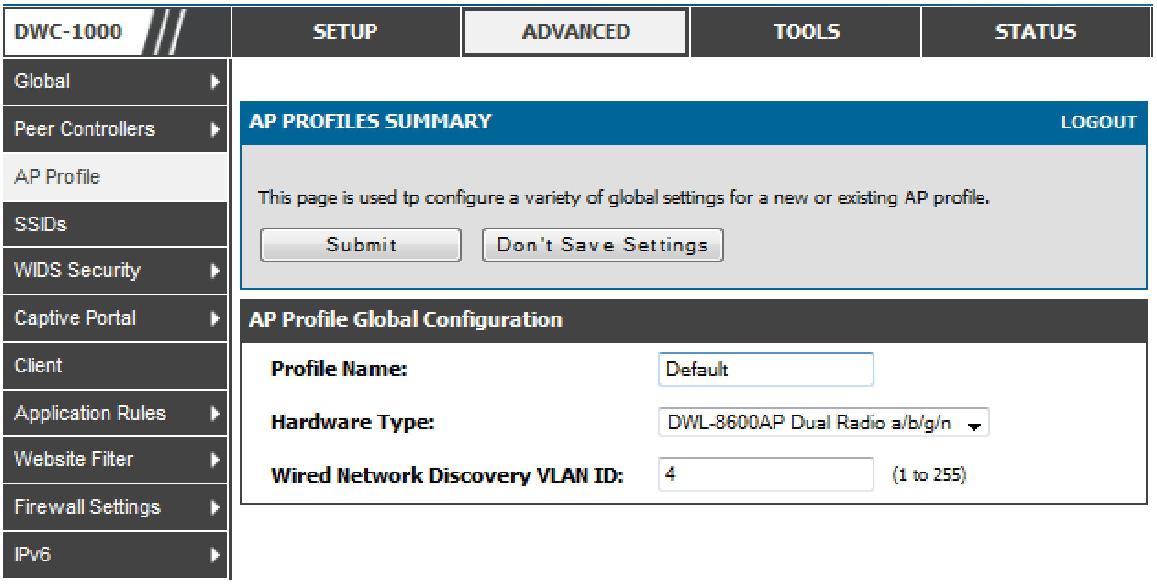
Refresh: Updates the page with the latest information

2.8.2 AP Profile Global Configuration

Advanced > AP Profile

Access Point Profile Summary page, you can Add, Copy, Edit, Delete AP profiles. To add a new profile, click Add in AP Profile Summary page. In the AP Profile Global Configuration page, enter the name of the profile in the Profile Name field, select Hardware type and enter the valid VLAN ID and then click Submit.

Figure 40: AP Profile Global Configuration



This page is used tp configure a variety of global settings for a new or existing AP profile.

Profile Name:	Default	
Hardware Type:	DWL-8600AP Dual Radio a/b/g/n	
Wired Network Discovery VLAN ID:	4	(1 to 255)

Profile Name: The Access Point profile name you added. Use 0 to 32 characters. Only alphanumeric characters are allowed. No special characters are allowed.

Hardware Type: Select the hardware type for the APs that use this profile. The hardware type is determined, in part, by the number of radios the AP supports (single or dual) and the IEEE 802.11 modes that the radio supports (a/b/g or a/b/g/n). The option available in the Hardware Type ID is:

- DWL-8600AP & DWL-6600AP Dual Radio a/b/g/n
- DWL-3600AP & DWL-2600AP Single Radio b/g/n
- DWL-8610AP Dual Radio a/b/g/n/ac.

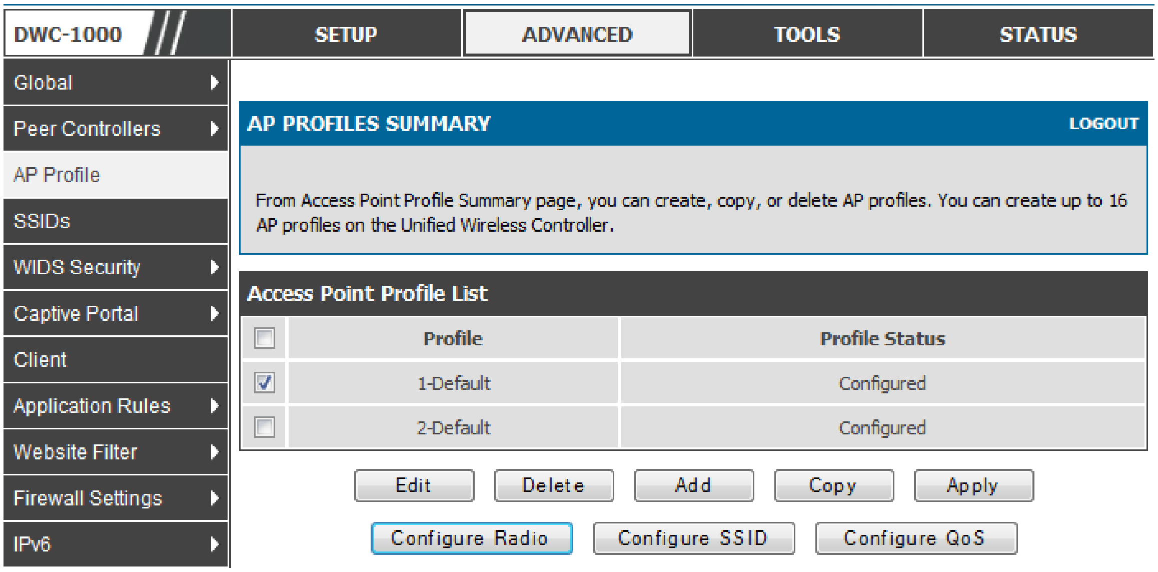
Wired Network Discovery VLAN ID: Enter the VLAN ID that the controller uses to send tracer packets in order to detect APs connected to the wired network.

AP Profile

Advanced > AP Profile

Access point configuration profiles are a useful feature for large wireless networks with APs that serve a variety of different users. You can create multiple AP profiles on the Controller to customize APs based on location, function, or other criteria. Profiles are like templates, and once you create an AP profile, you can apply that profile to any AP.

Figure 41: AP Profile List



AP PROFILES SUMMARY

From Access Point Profile Summary page, you can create, copy, or delete AP profiles. You can create up to 16 AP profiles on the Unified Wireless Controller.

Access Point Profile List

□	Profile	Profile Status
☑	1-Default	Configured
□	2-Default	Configured

For each AP profile, you can configure the following features:

- Profile settings

(Name, Hardware Type ID, Wired Network Discovery VLAN ID)

- Radio settings
- SSID settings
- QoS settings

Profile: The Access Point profile name you added. Use 0 to 32

characters.

Profile Status: can have one of the following values:

- **Associated**: The profile is configured, and one or more APs managed by the controller are associated with this profile.
- **Associated-Modified**: The profile has been modified since it was applied to one or more associated APs; the profile must be re-applied for the changes to take effect.
- **Apply Requested**: After you select a profile and click Apply, the screen refreshes and shows that an apply has been requested.
- **Apply In Progress**: The profile is being applied to all APs that use this profile. During this process the APs reset, and all wireless clients are disassociated from the AP.
- **Configured**: The profile is configured, but no APs managed by the controller currently use this profile.

✍ Associate a profile with an AP. Entry of the AP is valid and available in database of the controller.

The following actions are supported from this page**:**

Edit: To edit the existing AP profile.

Delete: To delete the existing AP profile.

Add: Add a new AP profile

Copy: Copy the existing AP profile.

Apply: Update the AP profile configuration details entered.

Configure Radio: Allows configuration of the AP profile Radio configuration.

Configure SSID: Allows configuration of the AP profile VAP configuration.

Configure QoS: Allows configuration of the AP profile QoS configuration.

Radio Configuration

Radio Mode: From this field, you can select the radio that you want to configure. By default, Radio 1 operates in IEEE 802.11a/n mode, and Radio 2 operates in IEEE 802.11b/g/n mode. If you change the mode, the labels for the radios change accordingly. Changes to the settings apply only to the selected radio. The DWL-3600AP is a single-radio AP. Any settings you configure for Radio 1 (802.11a/n) are not applied to the DWL-3600AP. If the selected Hardware Type ID for the AP profile is DWL-3600AP, the radio selectors are not available.

State: Specify whether you want the radio on or off by clicking On or Off. If you turn off a radio, the AP sends disassociation frames to all the wireless clients it is currently supporting so that the radio can be gracefully shutdown and the clients can start the association process with other available APs

Radio Scheduler: If you have configured a time of day active schedule in the Tools > Schedules menu, it will be available for selection in this drop down menu. You can associate a pre-defined schedule with this radio to turn on / off radio functionality during desired times of the day / week.

✍ Ensure that firmware v4.2.0.6_B101 or above for DWC-1000, 4.2.0.1_B009 or above for DWL-2600AP, 4.1.0.11_B015 or above for DWL-3600AP, 4.2.0.9_B009 or above for DWL-6600AP, and 4.1.0.14_RFsc or above for DWL-8600AP are being used to leverage the above feature.

RTS: Threshold Specify a Request to Send (RTS) Threshold value between 0 and 2347. The RTS threshold indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed. Changing the RTS threshold can help control traffic flow through the AP, especially one with a lot of clients. If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the packet. On the other hand, sending more RTS packets can help the network recover from interference or collisions which might occur on a busy network, or on a network experiencing electromagnetic interference.

Load Balancing: If you enable load balancing, you can control the amount of traffic that is allowed on each of the active AP's.

Load Utilization: This field allows you to set a threshold for the percentage of network bandwidth utilization allowed on the radio. Once the level you specify is reached, the AP stops accepting new client associations. Enter a percentage of utilization from 1 to 100.

Maximum Clients: Specify the maximum number of stations allowed to associate with this access point at any one time. You can enter a value between 0 and 200.

RF Scan Other Channels: The access point can perform RF scans to collect information about other wireless devices within range and then report this information to the DWC-1000 wireless controller. If you select the Scan Other Channels option, the radio periodically moves away from

the operational channel to scan other channels. Enabling this mode causes the radio to interrupt user traffic, which may be noticeable with voice connections. When the Scan Other Channels option is cleared, the AP scans only the operating channel.

RF Scan Sentry: Select this option to allow the radio to operate in sentry mode. When the RF Scan Sentry option is selected, the radio primarily performs dedicated RF scanning. The radio passively listens for beacons and traffic exchange between clients and other access points but does not accept connections from wireless clients. In sentry mode, all VAPs are disabled. Networks that deploy sentry APs or radios can detect devices on the network quicker and perform more through security analysis. In this mode, the radio controllers from one channel to the next. The length of time spent on each channel is controlled by the scan duration. The default scan duration is 10 milliseconds.

Mode: The Mode defines the Physical Layer (PHY) standard the radio uses. Select one of the following modes for each radio interface.

- IEEE 802.11a is a PHY standard that specifies operating in the 5 GHz U-NII band using orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 6 to 54 Mbps.
- IEEE 802.11a/n operates in the 5 GHz ISM band and includes support for both 802.11a and 802.11n devices. IEEE 802.11n is an extension of the 802.11 standard that includes multiple-input multiple-output (MIMO)

technology. IEEE 802.11n supports data ranges of up to 248 Mbps and nearly twice the indoor range of 802.11 b, 802.11g, and 802.11a.

- 5 GHz IEEE 802.11n is the recommended mode for networks with 802.11n devices that operate in the 5 GHz frequency that do not need to support 802.11a or 802.11b/g devices. IEEE 802.11n can achieve a higher throughput when it does not need to be compatible with legacy devices (802.11b/g or 802.11a).
- IEEE 802.11b/g operates in the 2.4 GHz ISM band. IEEE 802.11b is an enhancement of the initial 802.11 PHY to include 5.5 Mbps and 11 Mbps data rates. It uses direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) as well as complementary code keying (CCK) to provide the higher data rates. It supports data rates ranging from 1 to 11 Mbps. IEEE 802.11g is a higher speed extension (up to 54 Mbps) to the 802.11b PHY. It uses orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 1 to 54 Mbps.
- IEEE 802.11b/g/n operates in the 2.4 GHz ISM band and includes support for 802.11b, 802.11g, and 802.11n devices.
- 2.4 GHz IEEE 802.11n is the recommended mode for networks with 802.11n devices that operate in the 2.4 GHz frequency that do not need to support 802.11a or 802.11b/g devices. IEEE 802.11n can achieve a higher throughput when it does not need to be compatible with legacy devices (802.11b/g or 802.11a).
- IEEE 802.11a/n/ac operates in the 5 GHz ISM band and includes support for 802.11a , 802.11n and 802.11ac devices.
- IEEE 802.11n/ac operates in the 5 GHz ISM band and includes support for 802.11n and 802.11ac devices.

DTIM Period: The Delivery Traffic Information Map (DTIM) message is an element included in some

Beacon frames. It indicates which client stations, currently sleeping in low-power mode, have data buffered on the access point awaiting pick-up. The DTIM period you specify indicates how often the clients served by this access point should check for buffered data still on the AP awaiting pickup.

Specify a DTIM period within the given range (1–255). The measurement is in beacons. For example, if you set this field to 1, clients will check for buffered data on the AP at every beacon. If you set this field to 10, clients will check on every 10th beacon.

Beacon Interval: Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second). The Beacon Interval value is set in milliseconds. Enter a value from 20 to 2000.

Automatic Channel: The channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The range of channels and the default channel are determined by the Mode of the radio interface. When the AP boots, each AP radio scans the RF area for occupied channels and selects a channel from the available non-interfering or clear channels. However, channel conditions can change during operation. Enabling the Automatic Channel makes the radio of APs assigned to this profile eligible for auto-channel selection. You can automatically or manually run the autochannel selection algorithm to allow the DWC-1000 controller to adjust the channel on APs as WLAN conditions change.

Automatic Power: The power level affects how far an AP broadcasts its RF signal. If the power level is too low, wireless clients will not detect the signal or experience poor WLAN performance. If the power level is too high, the RF signal might interfere with other APs within range. Automatic power uses a proprietary algorithm to automatically adjust the RF signal to broadcast far enough to reach wireless clients, but not so far that it interferes with RF signals broadcast by other APs. The power level algorithm increases or decreases the power level in 10% increments based on presence or absence of packet retransmission errors.

Initial Power: The automatic power algorithm will not reduce the power below the number you set in the initial power field. By default, the power level is 100%. Therefore, even if you enable the automatic power, the power of the RF signal will not decrease. The power level is a percentage of the maximum transmission power for the RF signal.

APSD Mode: Select Enable to enable Automatic Power Save Delivery (APSD), which is a power management method. APSD is recommended if VoIP phones access the network through the AP.

RF Scan Interval: This field controls the length of time between channel changes during the RF Scan.

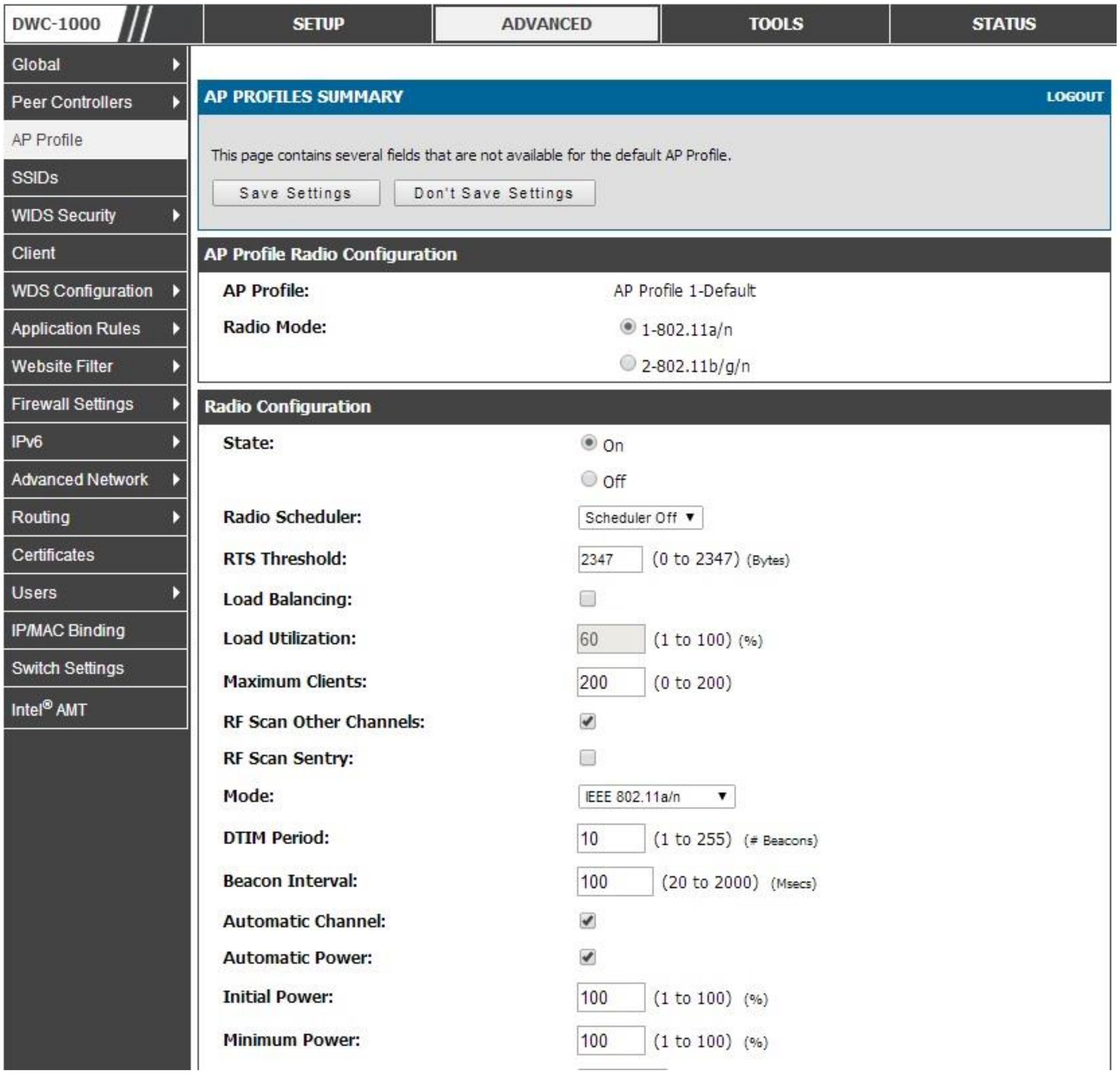
Long Retries The value in this field indicates the maximum number of transmission attempts on frame sizes greater than the RTS Threshold. The range is 1-255.

Rate Limiting: Enabling multicast and broadcast rate limiting can improve overall network performance by limiting the number of packets transmitted across the network. This feature is disabled by default.

✍ Note: The available rate limit values are very low for most environments, so enabling this feature is not recommended except for advanced users.

- To enable Multicast and Broadcast Rate Limiting, click **Enabled**.
- To disable Multicast and Broadcast Rate Disabled, click **Disabled**.

Figure 42: AP Profile - Radio configuration (Part-1)



AP PROFILES SUMMARY

This page contains several fields that are not available for the default AP Profile.

AP Profile Radio Configuration

AP Profile: AP Profile 1-Default

Radio Mode: ● 1-802.11a/n ○ 2-802.11b/g/n

Radio Configuration

State: ● On ○ Off

Radio Scheduler: Scheduler Off ▼

RTS Threshold: 2347 (0 to 2347) (Bytes)

Load Balancing: □

Load Utilization: 60 (1 to 100) (%)

Maximum Clients: 200 (0 to 200)

RF Scan Other Channels: ☑

RF Scan Sentry: □

Mode: IEEE 802.11a/n ▼

DTIM Period: 10 (1 to 255) (# Beacons)

Beacon Interval: 100 (20 to 2000) (Msecs)

Automatic Channel: ☑

Automatic Power: ☑

Initial Power: 100 (1 to 100) (%)

Minimum Power: 100 (1 to 100) (%)

Transmit Lifetime: Shows the number of milliseconds to wait before terminating attempts to transmit the MSDU after the initial transmission.

Rate Limit: Enter the rate limit you want to set for multicast and broadcast traffic. The limit should be greater than 1, but less than 50 packets per second. Any traffic that falls below this rate limit will always conform to and be transmitted to the appropriate destination. The default and maximum rate limit setting is 50 packets per second. This field is disabled if Rate Limiting is disabled.

Receive Lifetime: Shows the number of milliseconds to wait before terminating attempts to reassemble the MMPDU or MSDU after the initial reception of a fragmented MMPDU or MSDU.

Rate Limit Burst: Setting a rate limit burst determines how much traffic bursts can be before all traffic exceeds the rate limit. This burst limit allows intermittent bursts of traffic on a network above the set rate limit. The default and maximum rate limit burst setting is 75 packets per second. This field is disabled if Rate Limiting is disabled.

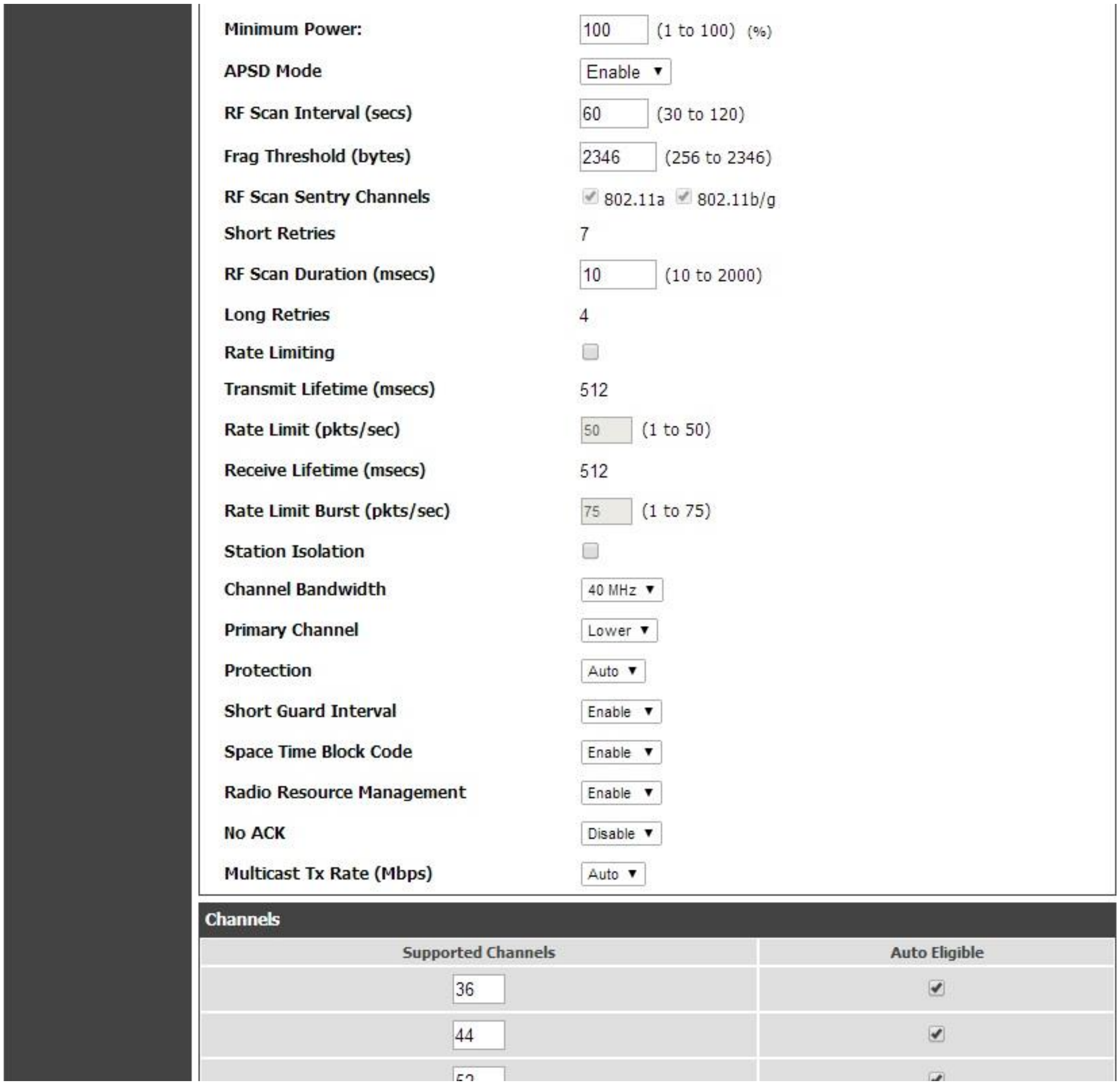
Station Isolation: When this option is selected, the AP blocks communication between wireless clients. It still allows data traffic between its wireless clients and wired devices on the network, but not among wireless clients. This feature is disabled by default.

- To enable Multicast and Broadcast Rate Limiting, click **Enabled**.
- To disable Multicast and Broadcast Rate Disabled, click **Disabled**.

Channel Bandwidth: The 802.11n specification allows the use of a 40-MHz-wide channel in addition to the legacy 20-MHz channel available with other modes. The 40-MHz channel enables higher data rates but leaves fewer channels available for use by other 2.4 GHz and 5 GHz devices. The 40-MHz option is enabled by default for 802.11a/n modes and 20 MHz for 802.11b/g/n modes. You can use this setting to restrict the use of the channel bandwidth to a 20-MHz channel. If the selected mode is 11a/n/ac or 11n/ac then the 80MHz bandwidth option is available.

Primary Channel: This setting is editable only when a channel is selected and the channel bandwidth is set to 40 MHz. A 40-MHz channel can be considered to consist of two 20-MHz channels that are contiguous in the frequency domain. These two 20-MHz channels are often referred to as the Primary and Secondary channels. The Primary Channel is used for 802.11n clients that support only a 20-MHz channel bandwidth and for legacy clients. Use this setting to set the Primary Channel as the upper or lower 20-MHz channel in the 40-MHz band.

Figure 43: AP Profile - Radio configuration (Part-2)



Minimum Power:	100 (1 to 100) (%)
APSD Mode	Enable ▼
RF Scan Interval (secs)	60 (30 to 120)
Frag Threshold (bytes)	2346 (256 to 2346)
RF Scan Sentry Channels	☑ 802.11a ☑ 802.11b/g
Short Retries	7
RF Scan Duration (msecs)	10 (10 to 2000)
Long Retries	4
Rate Limiting	☐
Transmit Lifetime (msecs)	512
Rate Limit (pkts/sec)	50 (1 to 50)
Receive Lifetime (msecs)	512
Rate Limit Burst (pkts/sec)	75 (1 to 75)
Station Isolation	☐
Channel Bandwidth	40 MHz ▼
Primary Channel	Lower ▼
Protection	Auto ▼
Short Guard Interval	Enable ▼
Space Time Block Code	Enable ▼
Radio Resource Management	Enable ▼
No ACK	Disable ▼
Multicast Tx Rate (Mbps)	Auto ▼

Channels

Supported Channels	Auto Eligible
36	☑
44	☑
52	☑

Protection: The protection feature contains rules to guarantee that 802.11 transmissions do not cause interference with legacy stations or applications. By default, these protection mechanisms are enabled (Auto). With protection enabled, protection mechanisms will be invoked if legacy devices are within range of the AP. You can disable (Off) these protection mechanisms; however, when 802.11n protection is off, legacy clients or APs within range can be affected by 802.11n transmissions. 802.11 protection is also available when the mode is 802.11b/g. When protection is enabled in this mode, it protects 802.11b clients and APs from 802.11g transmissions.

Short Guard Interval: The guard interval is the dead time, in nanoseconds, between OFDM symbols. The guard interval prevents Inter-Symbol and Inter-Carrier Interference (ISI, ICI). The 802.11n mode allows for a reduction in this guard interval from the a and g definition of 800 nanoseconds to 400 nanoseconds. Reducing the guard interval can yield a 10% improvement in data throughput. Select one of the following options:

- **Enable**: The AP transmits data using a 400 ns guard Interval when communicating with clients that also support the 400 ns guard interval.
- **Disable**: The AP transmits data using an 800 ns guard interval.

Space Time Block Code: Space Time Block Coding (STBC) is an 802.11n technique intended to improve the reliability of data transmissions. The data stream is transmitted on multiple antennas so the receiving system has a better chance of detecting at least one of the data streams. Select one of the following options:

- **Enable**: The AP transmits the same data stream on multiple antennas at the same time.
- **Disable**: The AP does not transmits the same data on multiple antennas.

Radio Resource Management: Radio Resource Measurement (RRM) mode requires the Wireless System to send additional information in beacons, probe responses, and association responses. Enable or disable the support for radio resource measurement feature in the AP profile. The feature is set independently for each radio and is enabled by default.

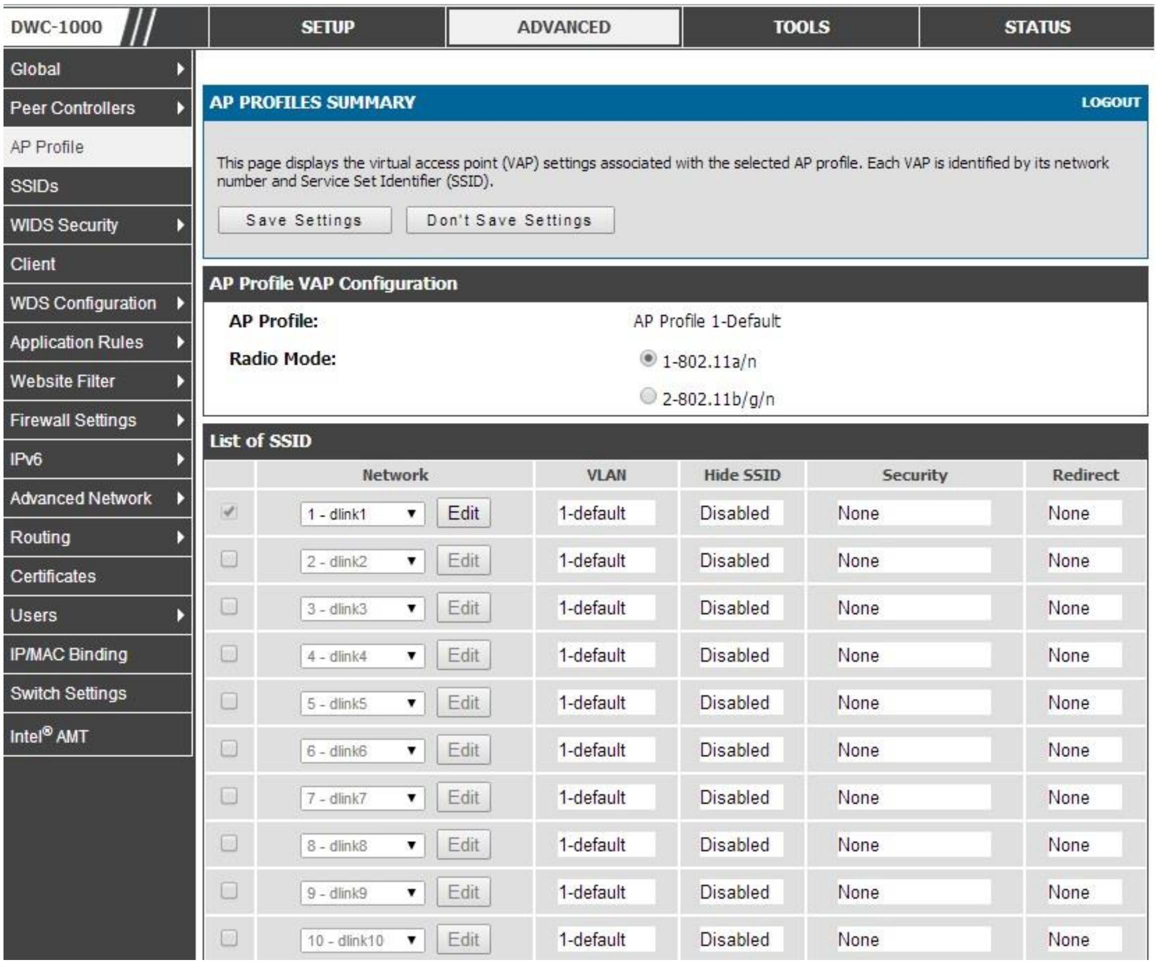
No ACK: Select Enable to specify that the AP should not acknowledge frames with QoS-NoAck as the service class value.

Multicast Tx Rate (Mbps): Select the 802.11 rate at which the radio transmits multicast frames. The rate is in Mbps. The lowest rate in the 5 GHz band is 6 Mbps.

SSID Configuration

The SSID Configuration page displays the virtual access point (VAP) settings associated with the selected AP profile. Each VAP is identified by its network number and Service Set Identifier (SSID).

Figure 44: AP Profile - SSID configuration



AP PROFILES SUMMARY

This page displays the virtual access point (VAP) settings associated with the selected AP profile. Each VAP is identified by its network number and Service Set Identifier (SSID).

AP Profile VAP Configuration

AP Profile: AP Profile 1-Default

Radio Mode: ● 1-802.11a/n ○ 2-802.11b/g/n

List of SSID

	Network		VLAN	Hide SSID	Security	Redirect
☑	1 - dlink1 ▼	Edit	1-default	Disabled	None	None
☐	2 - dlink2 ▼	Edit	1-default	Disabled	None	None
☐	3 - dlink3 ▼	Edit	1-default	Disabled	None	None
☐	4 - dlink4 ▼	Edit	1-default	Disabled	None	None
☐	5 - dlink5 ▼	Edit	1-default	Disabled	None	None
☐	6 - dlink6 ▼	Edit	1-default	Disabled	None	None
☐	7 - dlink7 ▼	Edit	1-default	Disabled	None	None
☐	8 - dlink8 ▼	Edit	1-default	Disabled	None	None
☐	9 - dlink9 ▼	Edit	1-default	Disabled	None	None
☐	10 - dlink10 ▼	Edit	1-default	Disabled	None	None

Radio Mode: From this field, you can select the radio that you want to configure. By default, Radio 1 operates in IEEE 802.11a/n mode, and Radio 2 operates in IEEE 802.11b/g/n mode. If you change the mode, the labels for the radios change accordingly. Changes to the settings apply only to the selected radio. The DWL-3600AP is a single-radio AP. Any settings you configure for Radio 1 (802.11a/n) are not applied to the DWL-3600AP. If the selected Hardware Type ID for the AP profile is DWL-3600AP, the radio selectors are not available.

Network: Use the option to the left of the network to enable or disable the corresponding VAP on the selected radio. When enabled, use the menu to select a networks to assign to the VAP. You can configure up to 64 separate networks on the controller and apply them across multiple radio and VAP interfaces. By default, 16 networks are pre-configured and applied in

order to the VAPs on each radio. Enabling a VAP on one radio does not automatically enable it on the other radio.

VLAN: Shows the VLAN ID of the VAP. To change this setting, click Edit.

L3 Tunnel: Shows whether L3 Tunneling is enabled on the network.

Note: When L3 tunneling is enabled, the VLAN ID configured above is not used. In fact, the controller puts the management VLAN ID, if any, on the tunneled packets destined to the AP.

Hide SSID: Shows whether the VAP broadcasts the SSID. If enabled, the SSID for this network is not included in AP beacons. To change this setting, click Edit.

Security: Shows the current security settings for the VAP. To change this setting, click Edit. Redirect Shows whether HTTP redirect is enabled. The possible values for the field are as follows:

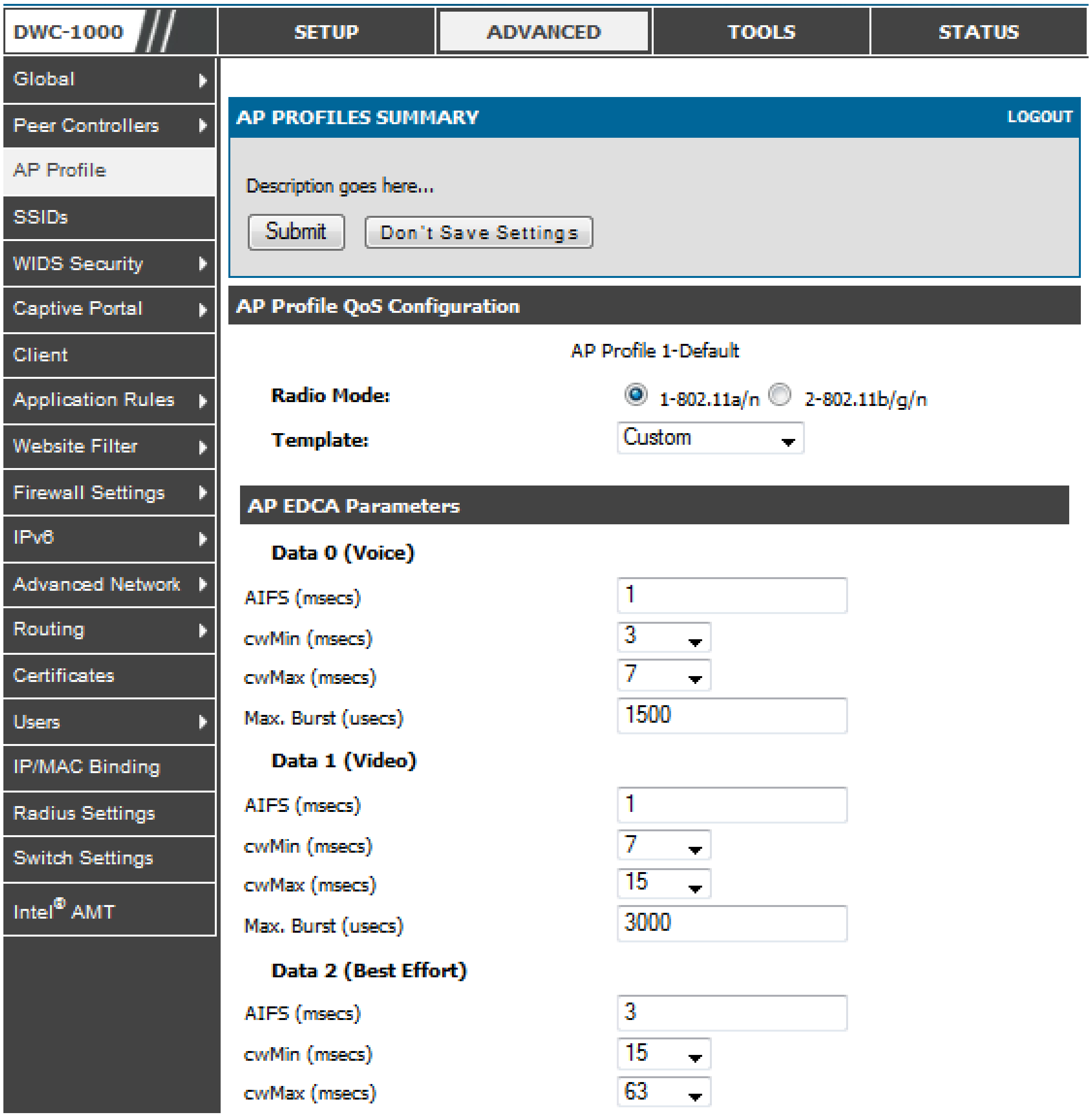
- **HTTP**: HTTP Redirect is enabled
- **None**: HTTP Redirect is disabled

Edit: Click Edit to modify settings for the corresponding network. When you click Edit, the Wireless Network Configuration page appears.

QoS Configuration

Quality of Service (QoS) provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic, different types of audio, video, and streaming media as well as traditional IP data over the DWC-1000.

Figure 45: AP Profile - QoS configuration (Part-1)



Description goes here...

AP Profile QoS Configuration

AP Profile 1-Default

Radio Mode: ● 1-802.11a/n ○ 2-802.11b/g/n

Template: Custom

AP EDCA Parameters

Data 0 (Voice)

AIFS (msecs)	1
cwMin (msecs)	3
cwMax (msecs)	7
Max. Burst (usecs)	1500

Data 1 (Video)

AIFS (msecs)	1
cwMin (msecs)	7
cwMax (msecs)	15
Max. Burst (usecs)	3000

Data 2 (Best Effort)

AIFS (msecs)	3
cwMin (msecs)	15
cwMax (msecs)	63

Configuring Quality of Service (QoS) on the DWC-1000 consists of setting parameters on existing queues for different types of wireless traffic, and effectively specifying minimum and maximum wait times (through Contention Windows) for transmission. The settings described here apply to data transmission behavior on the access point only, not to that of the client stations. **AP Enhanced Distributed Channel Access** (EDCA) Parameters affect traffic flowing from the access point to the client station. **Station Enhanced Distributed Channel Access** (EDCA) Parameters affect traffic flowing from the client station to the access point. You can specify custom QoS settings, or you can select a template that configures the AP profile with pre-defined settings that are optimized for data traffic or voice traffic.

Radio Mode: From this field, you can select the radio for which you want to configure QoS settings. Settings for each radio are configured separately. By default, Radio 1 operates in IEEE 802.11a/n mode, and Radio 2 operates in IEEE 802.11b/g/n mode. If you change the mode, the labels for the radios change accordingly. Changes to the settings apply only to the selected radio. The DWL--3600AP is a single- radio AP. Any settings you configure for Radio 1 (802.11a/n) are not applied to the DWL--3600AP. If the selected Hardware Type ID for the AP profile is DWL--3600AP, the radio selectors are not available.

Template: Select the QoS template to apply to the AP profile. If you select Custom, you can change the AP and station parameters. If you select Voice or Factory Defaults, the controller will use the pre-defined settings for the template you select.

AP EDCA Parameters:

Queue: Queues are defined for different types of data transmitted from AP-to-station:

- **Data 0 (Voice):** High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
- **Data 1 (Video):** High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.
- **Data 2 (best effort):** Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.

- **Data 3 (Background):** Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).

AIFS (Inter-Frame Space): The Arbitration Inter-Frame Spacing (AIFS) specifies a wait time for dataframes. The wait time is measured in slots. Valid values for AIFS are 1 through 255.

cwMin (Minimum Contention Window): This parameter is input to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. The first random number generated will be a number between 0 and the number specified here. If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window. Valid values for the cwmin are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for cwmin must be lower than the value for cwmax.

cwMax (Maximum Contention Window): The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the cwmax are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The

value for cwmax must be higher than the value for cwmin.

Max. Burst Length: AP EDCA Parameter Only (The Max. Burst Length applies only to traffic flowing from the access point to the client station.) This value specifies (in milliseconds) the Maximum Burst Length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance. Valid values for maximum burst length are 0.0 through 999

WMM Mode: Wi-Fi MultiMedia (WMM) is enabled by default. With WMM enabled, QoS prioritization and coordination of wireless medium access is on. With WMM enabled, QoS settings on the DWC-1000 wireless controller control downstream traffic flowing from the access point to client station (AP EDCA parameters) and the upstream traffic flowing from the station to the access point (station EDCA parameters). Disabling WMM deactivates QoS control of station EDCA parameters on upstream traffic flowing from the station to the access point With WMM disabled, you can still set some parameters on the downstream traffic flowing from the access point to the client station (AP EDCA parameters).

- To disable WMM extensions, click **Disabled**.
- To enable WMM extensions, click **Enabled**

Station EDCA Parameters

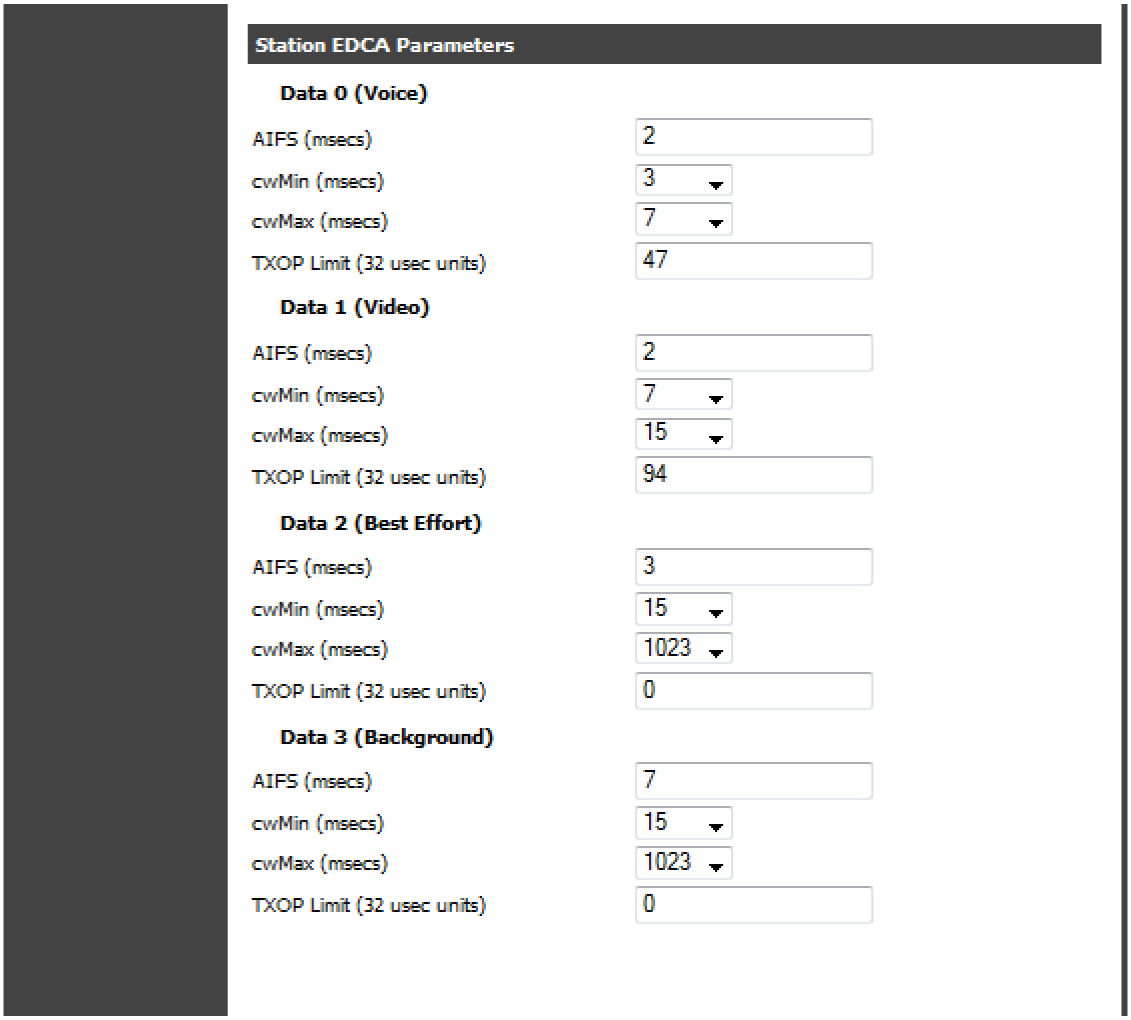
Queue: Queues are defined for different types of data transmitted from station-to-AP:

- **Data 0 (Voice):** High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
- **Data 1 (Video):** High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.
- **Data 2 (best effort):** Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
- **Data 3 (Background):** Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).

AIFS (Inter-Frame Space): The Arbitration Inter-Frame Spacing (AIFS) specifies a wait time for data frames. The wait time is measured in slots. Valid values for AIFS are 1 through 255.

cwMin (Minimum Contention Window): This parameter is used by the algorithm that determines the initial random backoff wait time (window) for data transmission during a period of contention for The value specified in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. The first random number generated will be a number between 0 and the number specified here. If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window. **cwMax (Maximum Contention Window)**: The value specified in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. **TXOP Limit:** Station EDCA Parameter Only (The TXOP Limit applies only to traffic flowing from the client station to the access point.) The Transmission Opportunity (TXOP) is an interval of time when a WME client station has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for client stations; that is, the interval of time when a WMM client station has the right to initiate transmissions on the wireless network.

Figure 46: AP Profile - QoS configuration (Part-2)



Station EDCA Parameters

Data 0 (Voice)

AIFS (msecs)	2
cwMin (msecs)	3
cwMax (msecs)	7
TXOP Limit (32 usec units)	47

Data 1 (Video)

AIFS (msecs)	2
cwMin (msecs)	7
cwMax (msecs)	15
TXOP Limit (32 usec units)	94

Data 2 (Best Effort)

AIFS (msecs)	3
cwMin (msecs)	15
cwMax (msecs)	1023
TXOP Limit (32 usec units)	0

Data 3 (Background)

AIFS (msecs)	7
cwMin (msecs)	15
cwMax (msecs)	1023
TXOP Limit (32 usec units)	0

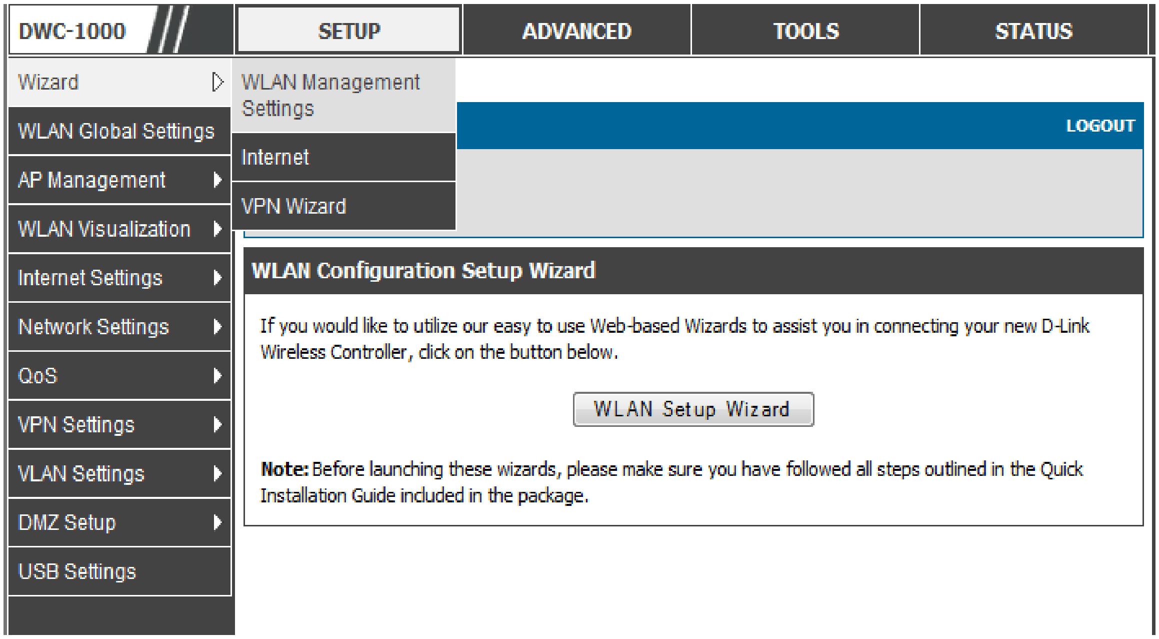
Chapter 3. Configuring Wireless LAN

3.1 WLAN Setup Wizard

Setup>Wizard>WLAN Settings

The WLAN controller can manage external AP’s and also act as an AP for wireless LAN clients. The Wireless Wizard is a user friendly approach to configure a wireless LAN connection using the controller’s built in 802.11 radio. It allows user to aim your wireless adapter, measure network performance and quickly identify and fix wireless broadband problems. The Wizard includes a Wi-Fi analyzer to easily identify the best channel and resolve interference issues. One can even compare the performance of his/her broadband network to networks around the world.

Figure 47: The Wireless LAN setup Wizard launch



If you would like to utilize our easy to use Web-based Wizards to assist you in connecting your new D-Link Wireless Controller, click on the button below.

Note: Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

Wireless Network Setup Wizard helps user to get wireless network up and running via easy steps:

Step 1: Wireless Global Configuration

Step 2: Wireless Default Profile Configuration

Step 3: Wireless Default Radio Configuration

Step 4: Wireless Default VAP Configuration

Step 5: Valid Access Point Summary

Step 6: Save Settings and Connect

Wireless Global Configuration

Country Code: Select the country code that represents the country where your controller and APs operate. Make sure you select the correct country code so that your WLAN system complies with the regulations in your country.

> ✍ Changing the country code disables and re-enables the controller. Any channel and radio mode settings that are invalid for the regulatory domain are reset to the default values. The country code (IEEE 802.11d) is transmitted in beacons and probe responses from the access points.

Wireless Default Radio Configuration

AP Profile Name: AP Profile Name can be alphanumeric identifier that can contain a maximum of 32 characters. This profile name is associated to default profile 1.

State: Here the admin indicates whether to enable or disable the radio. If user turns off a radio, the AP sends disassociation frames to all the wireless clients it is currently supporting so that the radio can be gracefully shutdown and the clients can start the association process with other available APs.

Mode (802.11a/n): The Mode defines the Physical Layer (PHY) standard the radio uses. Select one of the following modes for radio interface.

- IEEE 802.11a is a PHY standard that specifies operating in the 5 GHz U-NII band using orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 6 to 54 Mbps.
- IEEE 802.11a/n operates in the 5 GHz ISM band and includes support for both 802.11a and 802.11n devices. IEEE 802.11n is an extension of the 802.11 standard that includes multiple-input multiple-output (MIMO) technology. IEEE 802.11n supports data ranges of up to 248 Mbps and nearly twice the indoor range of 802.11 b, 802.11g, and 802.11a

- 5 GHz IEEE 802.11n is the recommended mode for networks with 802.11n devices that operate in the 5 GHz frequency that do not need to support 802.11a or 802.11b/g devices. IEEE 802.11n can achieve a higher throughput when it does not need to be compatible with legacy devices (802.11b/g or 802.11a).

Mode (802.11b/g/n): The Mode defines the Physical Layer (PHY) standard the radio uses. Select one of the following modes for radio interface.

- IEEE 802.11b/g operates in the 2.4 GHz ISM band. IEEE 802.11b is an enhancement of the initial 802.11 PHY to include 5.5 Mbps and 11 Mbps data rates. It uses direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) as well as complementary code keying (CCK) to provide the higher data rates. It supports data rates ranging from 1 to 11 Mbps. IEEE 802.11g is a higher speed extension (up to 54 Mbps) to the 802.11b PHY. It uses orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 1 to 54 Mbps.
- IEEE 802.11b/g/n operates in the 2.4 GHz ISM band and includes support for 802.11b, 802.11g, and 802.11n devices.
- 2.4 GHz IEEE 802.11n is the recommended mode for networks with 802.11n devices that operate in the 2.4 GHz frequency that do not need to support 802.11a or 802.11b/g devices. IEEE 802.11n can achieve a higher throughput when it does not need to be compatible with legacy devices (802.11b/g or 802.11a).

Wireless **Default VAP Configuration**

SSID: Wireless clients identify a wireless network by the SSID, which is an alphanumeric key that uniquely identifies a wireless local area network. The SSID can be up to thirty-two characters in length, and there are no restrictions on the characters that may be used in an SSID.

Security: The default AP profile does not use any security mechanism by default. In order to protect your network, D-Link strongly recommends that you select a security mechanism so that unauthorized wireless clients cannot gain access to your network. The following WLAN network security options are available in WLAN wizard.

- None: No security

- Static WEP: security require is Static-WEP. Authentication as "shared-key", type "ascii" and length "128"(bits) are used for setting Static WEP key through the WLAN wizard
- WPA Personal : This type of security supports version WPA and WPA2, with ciphers ccmp and tkip , bcast-key-refresh-rate 300 are used for setting WPA Personal Key through the WLAN wizard.

Valid Access Point Summary

MAC address: This field shows the MAC address of the AP broadcast by this controller

> ✍ Note: Experienced WLAN administrators can input all the settings in one page via the Manual Wireless Network Setup.

3.2 WLAN Visualization support

Setup>WLAN Visualization

WLAN Visualization is a tool that provides a graphical representation of the wireless network through a Web browser. The WLAN Visualization graph does not have a background image of its own, and so the administrator can upload a static graphic image that provides the wireless topology of the APs and controllers in the wireless network.

3.2.1 Download Image

User can upload one or more images, such as your office floor plan, to provide customized information for the WLAN Visualization feature. Images file formats that are recommended to upload should be in one of the following formats:

- GIF (Graphics Interchange Format)
- JPG (Joint Photographic Experts Group)

It is also recommended that you do not use color images since the WLAN components might not show up well. Once user uploads an image file and save the running configuration, the image remains on the switch and you can assign it to an existing graph using the WLAN Visualization application.

Figure 48: WLAN Visualization Image import

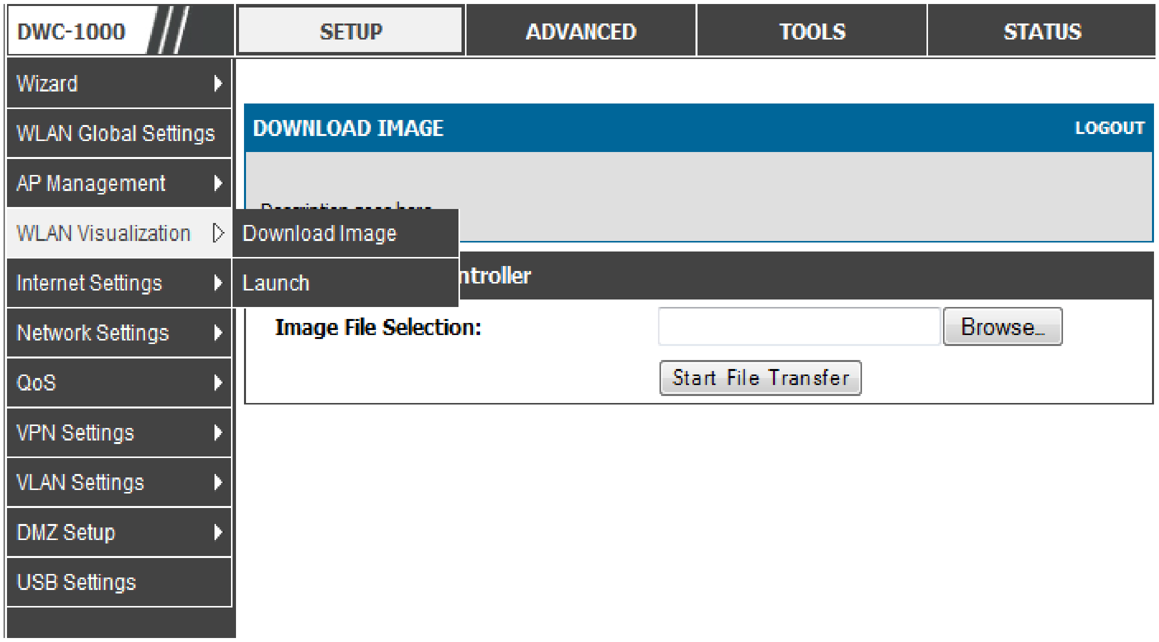


Image File Selection:

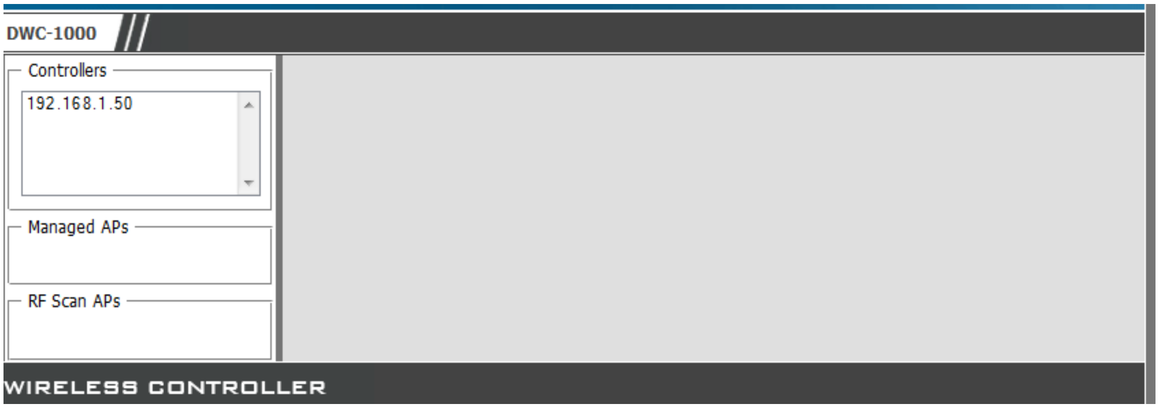
Deleting Images

This option is available only if images are already loaded onto the controller. To delete all images loaded onto the switch, click Delete All Images. Deleting background images is not recommended. However, if user uses has to delete the images user will need to refresh the WLAN Visualization tool after deleting images.

3.2.2 Visualization Launch

To start the WLAN Visualization tool, the Launch Menu under WLAN Visualization has to be used This opens a new browser window and starts the Java applet that allows the AP and WLAN controller network to be presented as a topology diagram (with or without a custom background image).

Figure 49: The launched visualization page



192.168.1.50

Chapter 4. Monitoring Status and Statistics

4.1 System Overview

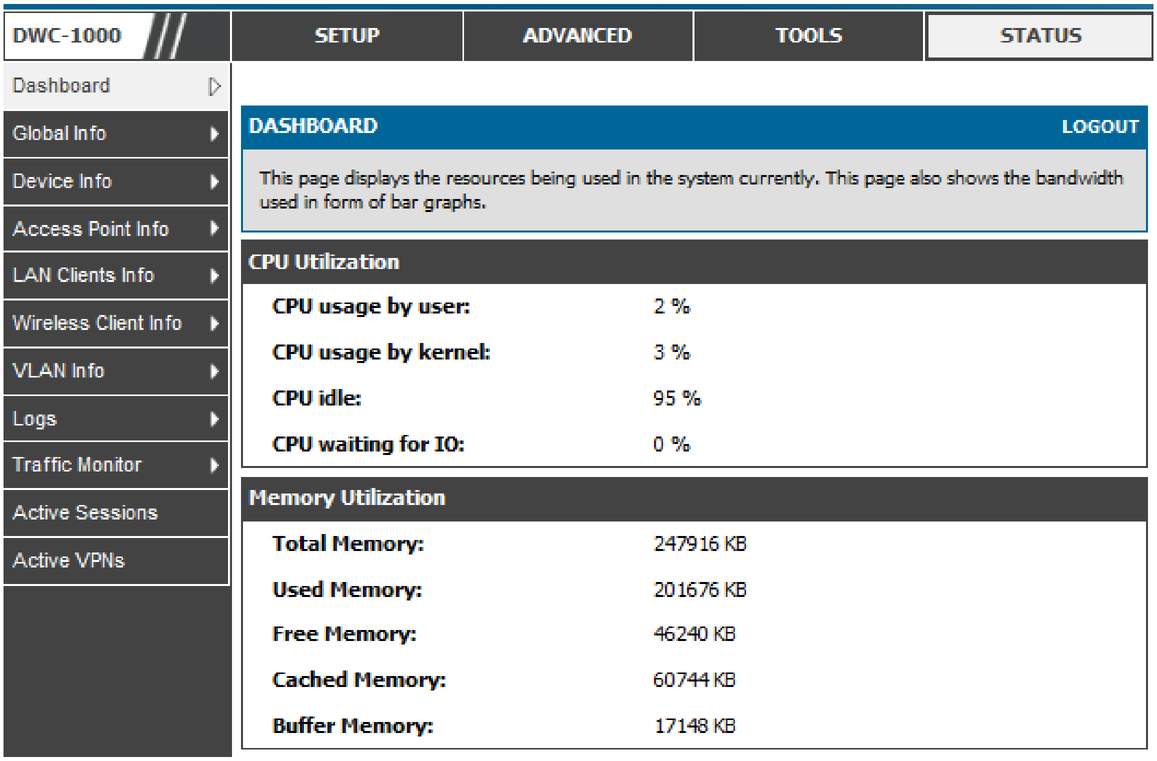
The Status page allows you to get a detailed overview of the system configuration. The settings for the wired and wireless interfaces are displayed in the DWC-1000 Status page, and then the resulting hardware resource and controller usage details are summarized on the controller Dashboard.

4.1.1 Dashboard

Status > Dashboard > General

The DWC-1000 dashboard page gives a summary of the CPU and Memory utilization.

Figure 50: Dashboard



This page displays the resources being used in the system currently. This page also shows the bandwidth used in form of bar graphs.

CPU Utilization

CPU usage by user:	2 %
CPU usage by kernel:	3 %
CPU idle:	95 %
CPU waiting for IO:	0 %

Memory Utilization

Total Memory:	247916 KB
Used Memory:	201676 KB
Free Memory:	46240 KB
Cached Memory:	60744 KB
Buffer Memory:	17148 KB

CPU Utilization

This section displays the router's processor statistics.

CPU usage by user: Percent of the CPU utilization being consumed currently by all user space processes, such as SSL VPN or management operations.

CPU usage by kernel: percent of the CPU utilization being consumed currently by kernel space processes, such as firewall operations.

CPU idle: percent of CPU cycles that are currently not in use.

CPU waiting for IO: percent of CPU cycles that are allocated to input/output devices.

Memory Utilization

This section displays memory status of system.

Total Memory: Indicates total available volatile physical memory.

Used Memory: Indicates memory used by all processes in system.

Free Memory: Indicates available free memory in system.

Cached Memory: Indicates cached memory in system.

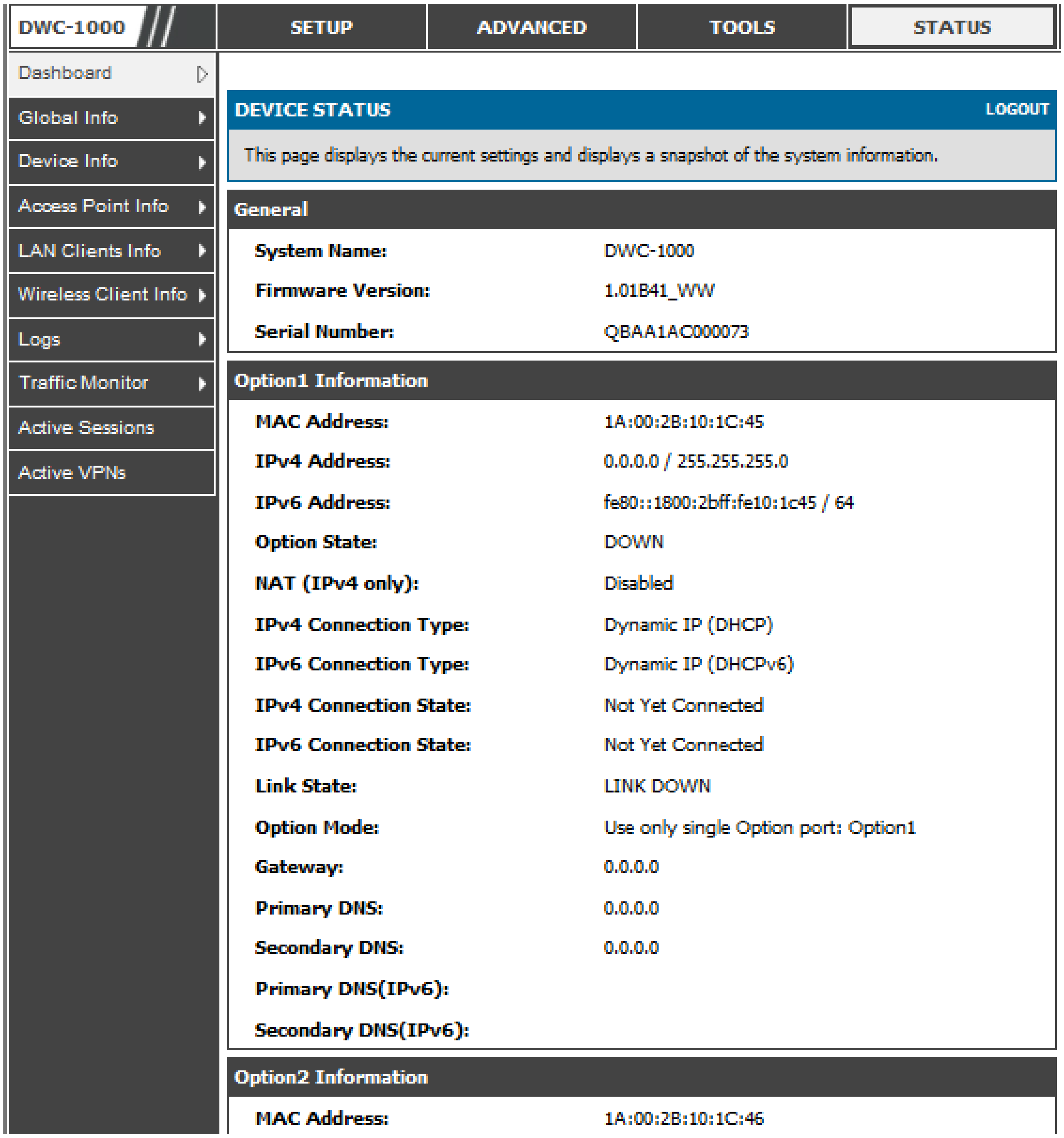
Buffer Memory: Indicates buffered memory in system

4.1.2 Device Status

Status > Device Info > Device Status

The DWC-1000 Status page gives a summary of the controller configuration settings configured in the Setup and Advanced menus. The static hardware serial number and current firmware version are presented in the General section. The Option and LAN interface information shown on this page are based on the administrator configuration parameters. The radio band and channel settings are presented below along with all configured and active APs that are enabled on this controller.

Figure 51: Device Status display



DEVICE STATUS

This page displays the current settings and displays a snapshot of the system information.

General

System Name:	DWC-1000
Firmware Version:	1.01B41_WW
Serial Number:	QBAA1AC000073

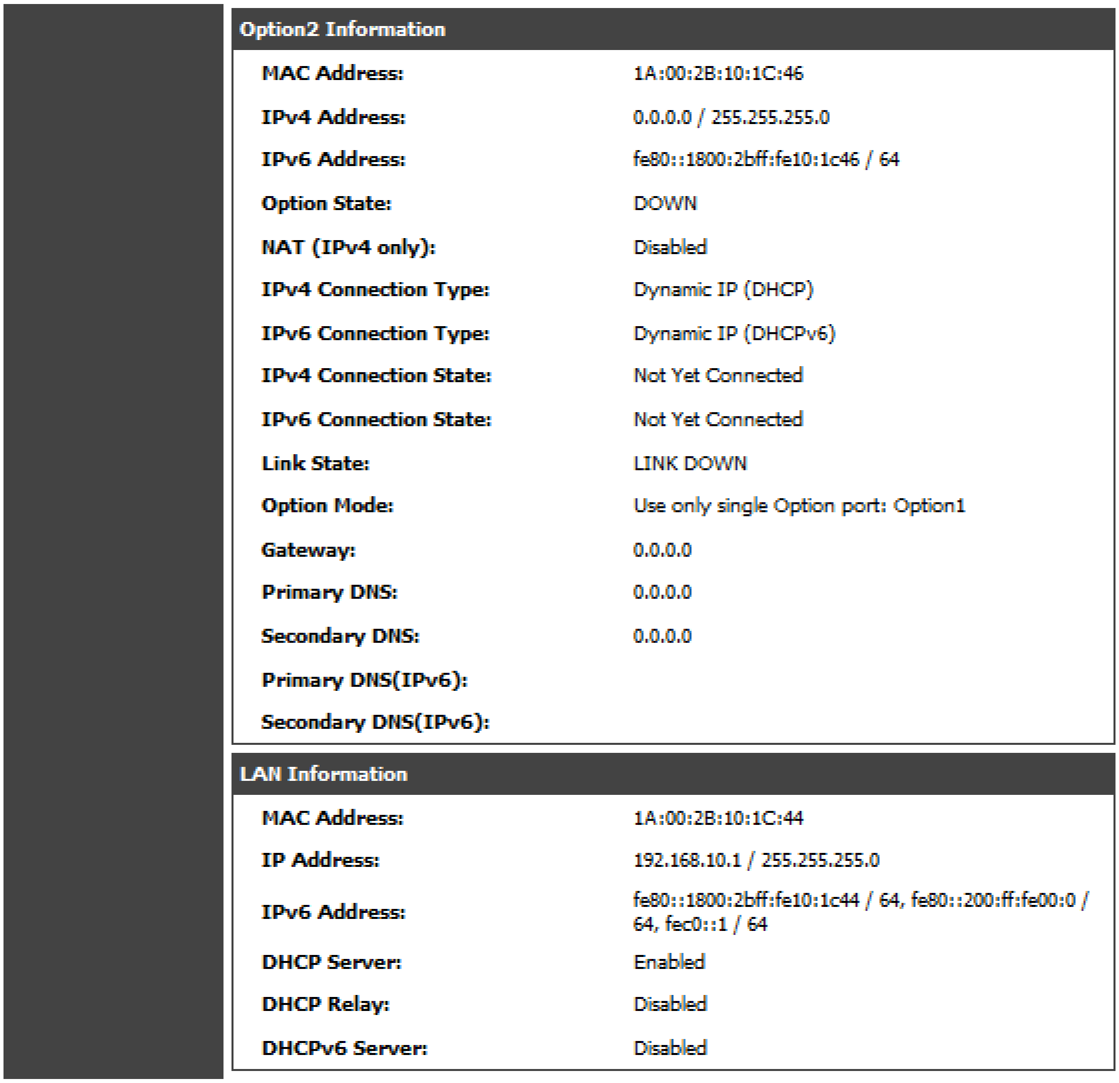
Option1 Information

MAC Address:	1A:00:2B:10:1C:45
IPv4 Address:	0.0.0.0 / 255.255.255.0
IPv6 Address:	fe80::1800:2bff:fe10:1c45 / 64
Option State:	DOWN
NAT (IPv4 only):	Disabled
IPv4 Connection Type:	Dynamic IP (DHCP)
IPv6 Connection Type:	Dynamic IP (DHCPv6)
IPv4 Connection State:	Not Yet Connected
IPv6 Connection State:	Not Yet Connected
Link State:	LINK DOWN
Option Mode:	Use only single Option port: Option1
Gateway:	0.0.0.0
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0
Primary DNS(IPv6):	
Secondary DNS(IPv6):	

Option2 Information

MAC Address:	1A:00:2B:10:1C:46

Figure 52: Device Status display (continued)



Option2 Information	
MAC Address:	1A:00:2B:10:1C:46
IPv4 Address:	0.0.0.0 / 255.255.255.0
IPv6 Address:	fe80::1800:2bff:fe10:1c46 / 64
Option State:	DOWN
NAT (IPv4 only):	Disabled
IPv4 Connection Type:	Dynamic IP (DHCP)
IPv6 Connection Type:	Dynamic IP (DHCPv6)
IPv4 Connection State:	Not Yet Connected
IPv6 Connection State:	Not Yet Connected
Link State:	LINK DOWN
Option Mode:	Use only single Option port: Option1
Gateway:	0.0.0.0
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0
Primary DNS(IPv6):	
Secondary DNS(IPv6):	

LAN Information	
MAC Address:	1A:00:2B:10:1C:44
IP Address:	192.168.10.1 / 255.255.255.0
IPv6 Address:	fe80::1800:2bff:fe10:1c44 / 64, fe80::200:ff:fe00:0 / 64, fec0::1 / 64
DHCP Server:	Enabled
DHCP Relay:	Disabled
DHCPv6 Server:	Disabled

4.1.3 Wireless LAN AP information

Status > Device Info > Wireless LAN AP Information

The Managed AP status pages allows to access configuration and association information about managed APs and their neighbors.

View AP Details: Shows detailed status information collected from the AP.

View Radio Details: Shows detailed status for a radio interface. Use the radio button to navigate between the two radio interfaces.

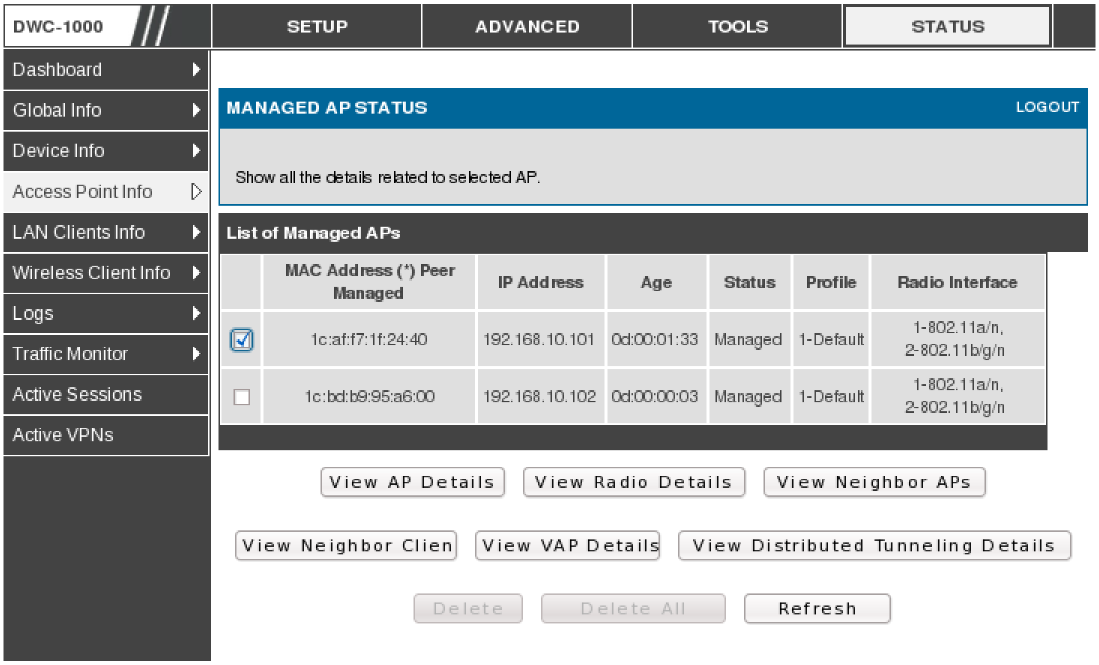
View Neighbour APs: Shows the neighbour APs that the specified AP has discovered through periodic RF scans on the selected radio interface.

View Neighbour Clients: Shows information about wireless clients associated with an AP or detected by the AP radio.

View VAP Details: Shows summary information about the virtual access points (VAPs) for the selected AP and radio interface on the APs that the controller manages.

View Distributed Tunneling Details: Shows information about the L2 tunnels currently in use on the AP.

Figure 53: Wireless LAN AP information



Show all the details related to selected AP.

List of Managed APs

	MAC Address (*) Peer Managed	IP Address	Age	Status	Profile	Radio Interface
☑	1c:af:f7:1f:24:40	192.168.10.101	0d:00:01:33	Managed	1-Default	1-802.11a/n, 2-802.11b/g/n
□	1c:bd:b9:95:a6:00	192.168.10.102	0d:00:00:03	Managed	1-Default	1-802.11a/n, 2-802.11b/g/n

MAC Address: The Ethernet address of the controller managed AP. If the MAC address of the AP is followed by an asterisk (*), it is managed by a peer controller.

IP Address: The network IP address of the managed AP

Age: Time since last communication between the controller and the AP.

Status: The current managed state of the AP. The possible values are:

- **Discovered**: The AP is discovered and by the controller, but is not yet authenticated.
- **Authenticated**: The AP has been validated and authenticated (if authentication is enabled), but it is not configured.
- **Managed**: The AP profile configuration has been applied to the AP and it's operating in managed mode.
- **Failed**: The controller lost contact with the AP, a failed entry will remain in the managed AP database unless you remove it. Note that a managed AP will temporarily show a failed status during a reset.

> ✍ Note: When management connectivity is lost for a managed AP, then both radios of the AP are turned down. All the clients associated with the AP get disassociated. The radios become operational if and when that AP is managed again by a controller.

Profile: The AP profile configuration currently applied to the managed AP. The profile is assigned to the AP in the valid AP database.

Radio Interface: Shows the wireless radio mode that each radio on the AP is using.

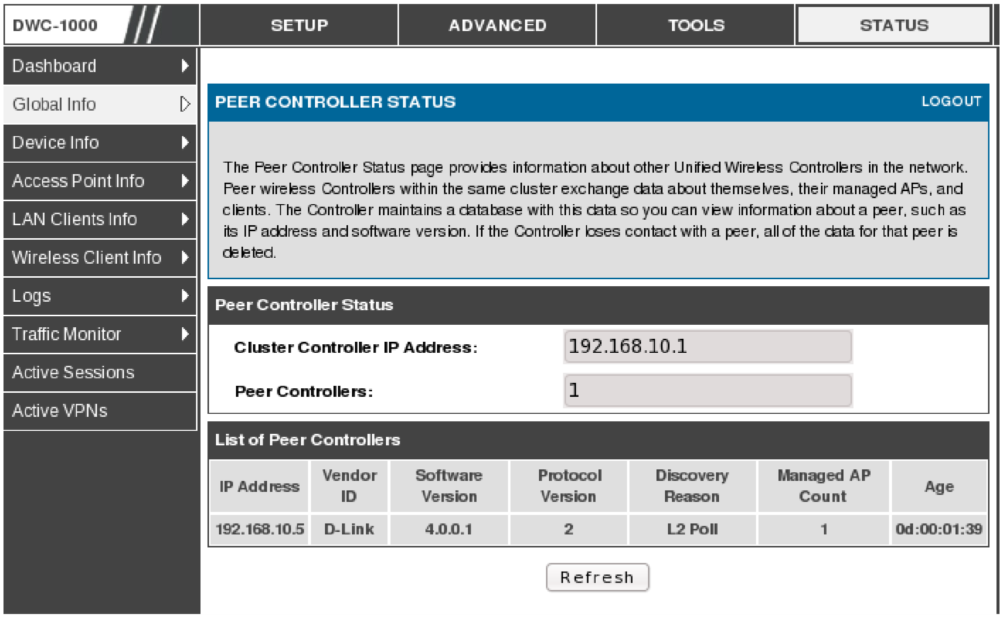
4.1.4 Cluster information

Status > Device Info > Cluster Information

The Peer Controller Status page provides information about other wireless controller in the network. Peer wireless controller within the same cluster exchange data about themselves, their managed APs, and clients. The controller maintains a database with this data so you can view information about a peer, such as its IP address and software version. If the controller loses contact with a peer, all of the data for that peer is deleted.

One of the controller in a cluster is elected as a Cluster Controller. The Cluster Controller collects status and statistics from all the other controllers in the cluster, including information about the APs peer controller manage and the clients associated to those APs.

Figure 54: Cluster information



PEER CONTROLLER STATUS

The Peer Controller Status page provides information about other Unified Wireless Controllers in the network. Peer wireless Controllers within the same cluster exchange data about themselves, their managed APs, and clients. The Controller maintains a database with this data so you can view information about a peer, such as its IP address and software version. If the Controller loses contact with a peer, all of the data for that peer is deleted.

Peer Controller Status

Cluster Controller IP Address:	192.168.10.1
Peer Controllers:	1

List of Peer Controllers

IP Address	Vendor ID	Software Version	Protocol Version	Discovery Reason	Managed AP Count	Age
192.168.10.5	D-Link	4.0.0.1	2	L2 Poll	1	0d:00:01:39

Cluster Controller IP Address: IP address of the controller that controls the cluster.

Peer Controllers: Displays the number of peer controllers in the cluster.

IP Address: IP address of the peer wireless controller in the cluster.

Vendor ID: Vendor ID of the peer controller software.

Software Version: The software version for the given peer controllers

Protocol Version: Indicates the protocol version supported by the software on the peer controllers

Discovery Reason: The discovery method of the given peer controller, which can be through an L2 Poll or IP Poll

Managed AP Count: Shows the number of APs that the controller currently manages.

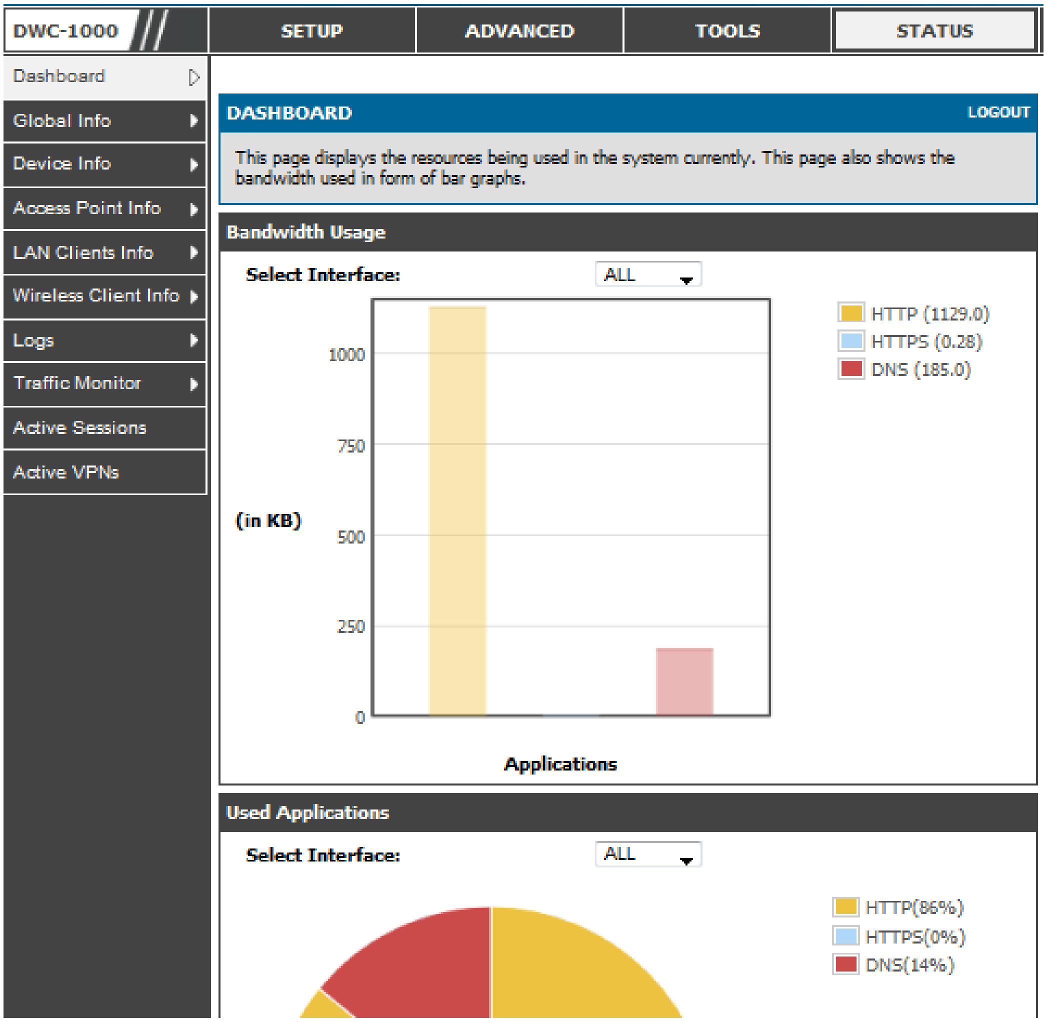
Age: Time since last communication with the controller in Hours, Minutes, and Seconds.

4.1.5 Resource Utilization

Status > Dashboard > Interface

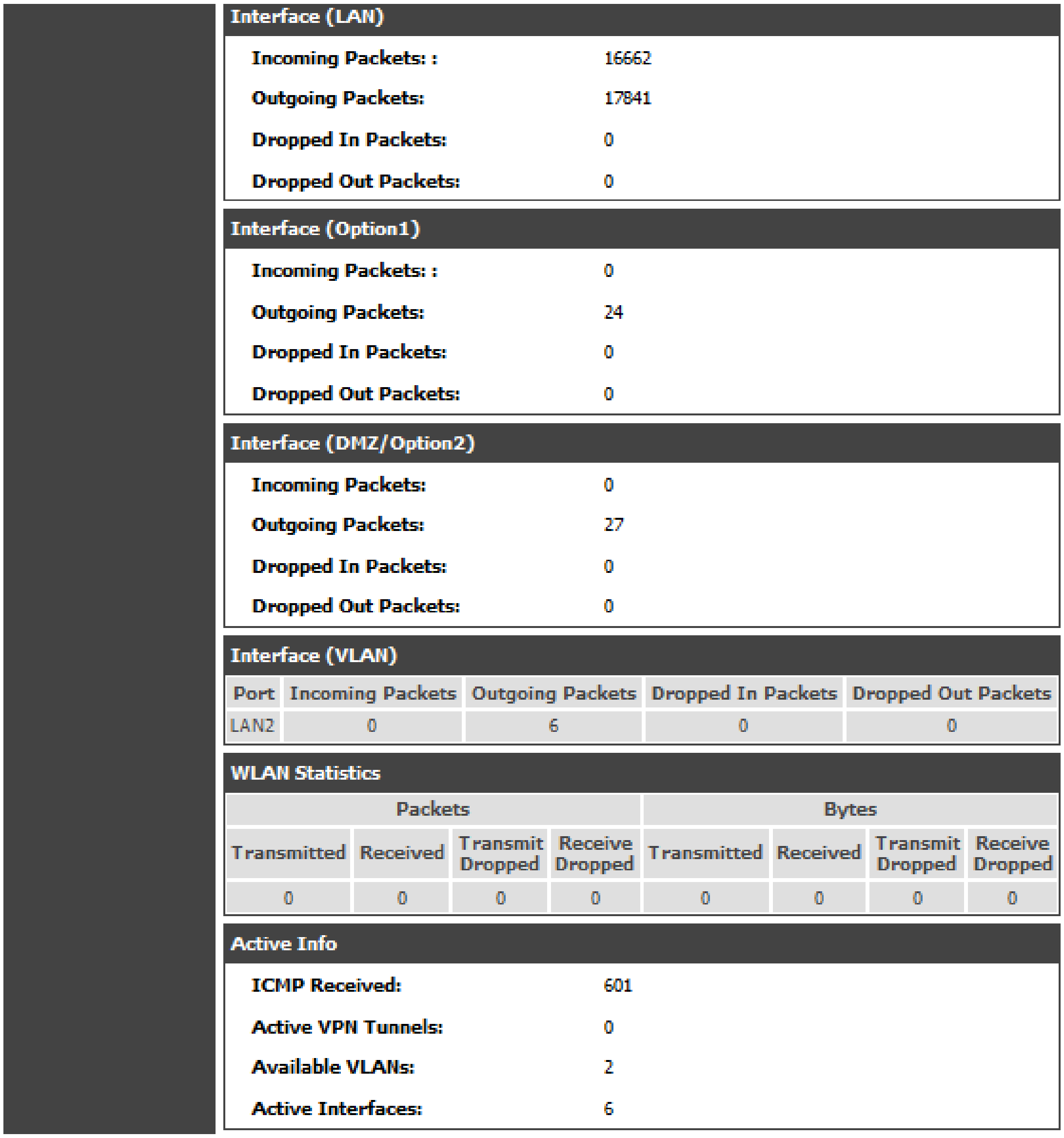
The Dashboard page presents hardware and usage statistics. The CPU and Memory utilization is a function of the available hardware and current configuration and traffic through the controller. Interface statistics for the wired connections (LAN, Option1, Option 2/DMZ, VLANs) provide indication of packets through and packets dropped by the interface. Click refresh to have this page retrieve the most current statistics.

Figure 55: Resource Utilization statistics



This page displays the resources being used in the system currently. This page also shows the bandwidth used in form of bar graphs.

Figure 56: Resource Utilization data (continued)



Interface (LAN)

Incoming Packets: :	16662
Outgoing Packets:	17841
Dropped In Packets:	0
Dropped Out Packets:	0

Interface (Option1)

Incoming Packets: :	0
Outgoing Packets:	24
Dropped In Packets:	0
Dropped Out Packets:	0

Interface (DMZ/Option2)

Incoming Packets:	0
Outgoing Packets:	27
Dropped In Packets:	0
Dropped Out Packets:	0

Interface (VLAN)

Port	Incoming Packets	Outgoing Packets	Dropped In Packets	Dropped Out Packets
LAN2	0	6	0	0

WLAN Statistics

Packets				Bytes			
Transmitted	Received	Transmit Dropped	Receive Dropped	Transmitted	Received	Transmit Dropped	Receive Dropped
0	0	0	0	0	0	0	0

Active Info

ICMP Received:	601
Active VPN Tunnels:	0
Available VLANs:	2
Active Interfaces:	6

4.2 Traffic Statistics

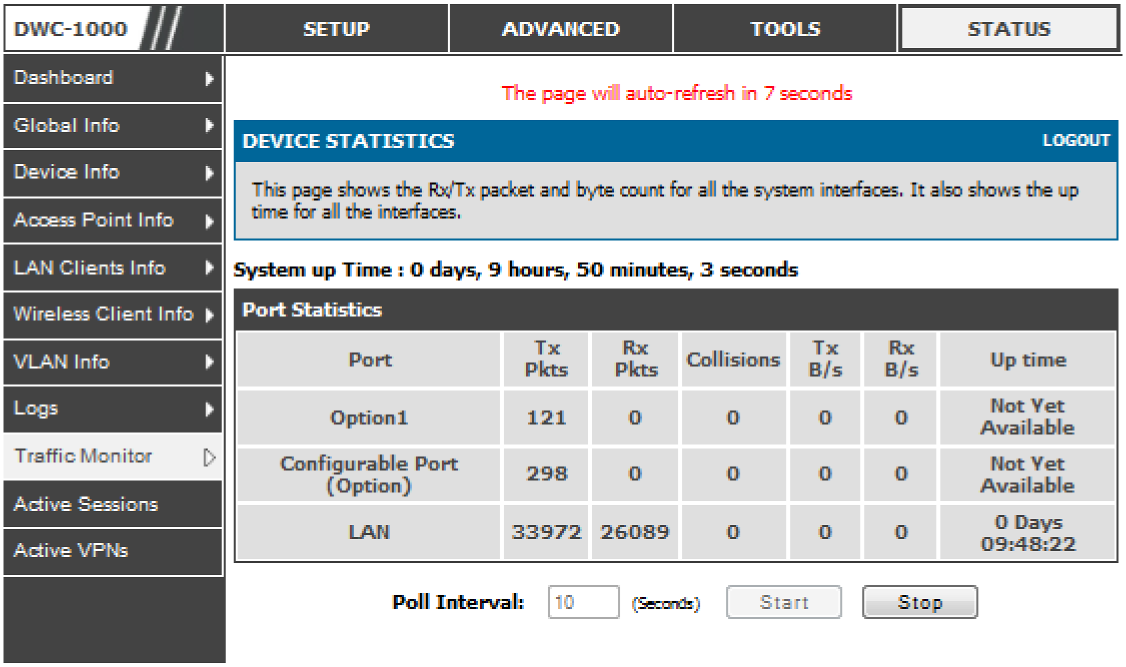
4.2.1 Wired Port Statistics

Status > Traffic Monitor > Device Statistics

Detailed transmit and receive statistics for each physical port are presented here. Each interface (Option1, Option 2/DMZ, LAN, and VLANs) have port specific packet level information provided for review. Transmitted/received packets, port collisions, and the cumulating bytes/sec for transmit/receive directions are provided for each interface along with the port up time. If you suspect issues with any of the wired ports, this table will help diagnose uptime or transmit level issues with the port.

The statistics table has auto-refresh control which allows display of the most current port level data at each page refresh. The default auto-refresh for this page is 10 seconds.

Figure 57: Physical port statistics



The page will auto-refresh in 7 seconds

DEVICE STATISTICS

This page shows the Rx/Tx packet and byte count for all the system interfaces. It also shows the up time for all the interfaces.

System up Time : 0 days, 9 hours, 50 minutes, 3 seconds

Port Statistics

Port	Tx Pkts	Rx Pkts	Collisions	Tx B/s	Rx B/s	Up time
Option1	121	0	0	0	0	Not Yet Available
Configurable Port (Option)	298	0	0	0	0	Not Yet Available
LAN	33972	26089	0	0	0	0 Days 09:48:22

Poll Interval: 10 (Seconds)

4.3 Associated Client Status/Statistics

4.3.1 Managed AP Statistics

Status > Traffic Monitor > Managed AP Statistics

The managed AP statistics page shows information about traffic on the wired and wireless interfaces of the access point. This information can help diagnose network issues, such as throughput problems. The following figure shows the Managed Access Point Statistics page with a managed AP.

MAC Address: This field shows the MAC address of the client station

Interface: This field shows the interface type WLAN or Ethernet.

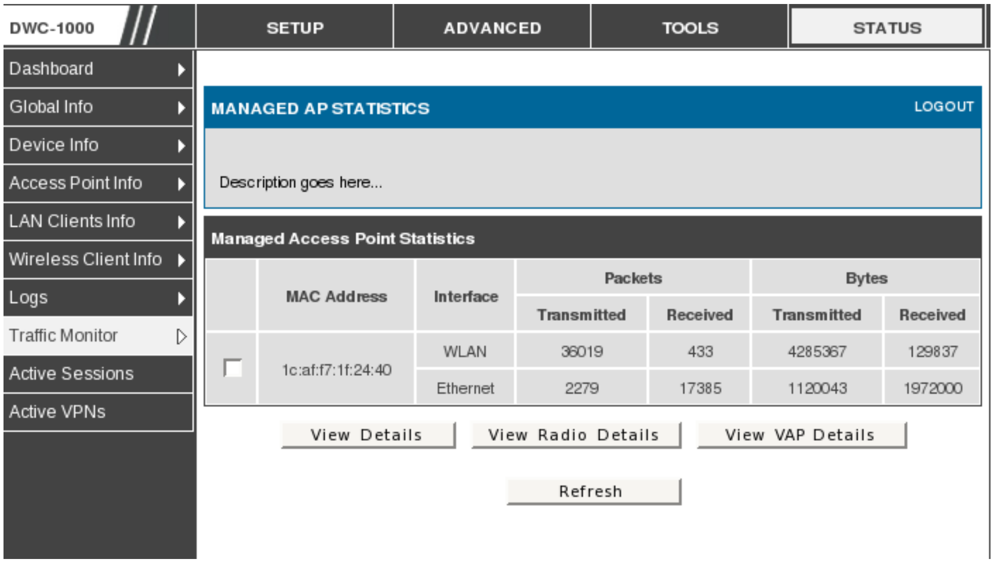
Packet Transmitted: This field shows the packet transmitted to the client station

Packet Received: This field shows the packet received to the client station

Bytes Transmitted: This field shows the bytes transmitted to the client station

Bytes Received: This field shows the bytes received to the client station

Figure 58: Managed AP Statistics



MANAGED AP STATISTICS

Description goes here...

Managed Access Point Statistics

	MAC Address	Interface	Packets		Bytes	
			Transmitted	Received	Transmitted	Received
□	1c:af:f7:1f:24:40	WLAN	36019	433	4285367	129837
		Ethernet	2279	17385	1120043	1972000

The following actions are supported from this page:

View Details: Shows detailed status information collected from the AP.

View Radio Details: Shows detailed status for a radio interface

View VAP Details: Shows summary information about the virtual access points (VAPs) for the selected AP and radio interface on the APs that the controller manages

Refresh: Updates the page with the latest information

4.3.2 LAN Associated Clients

Status > Traffic Monitor > Associated Clients Statistics > LAN Associated Clients

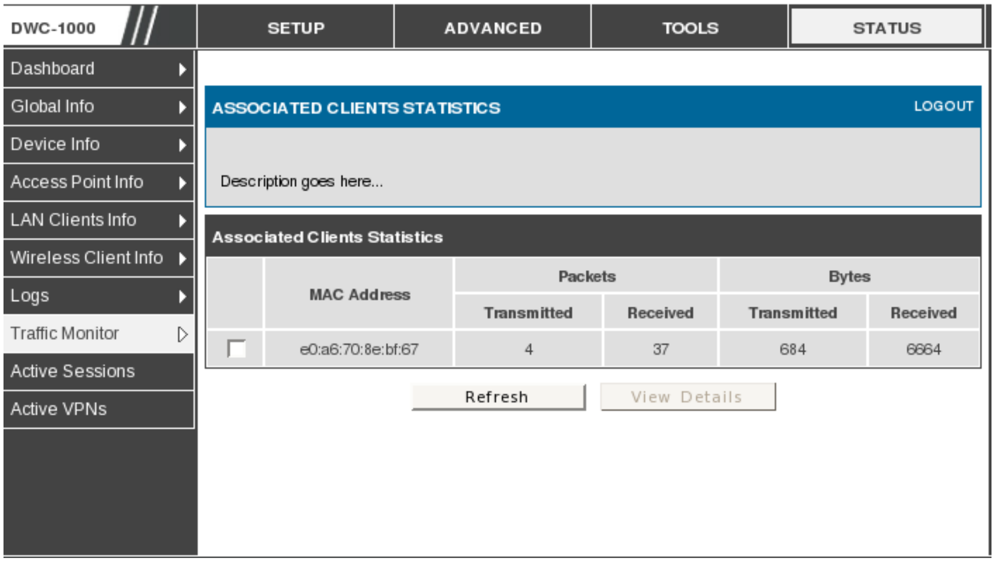
The controller tracks the traffic the client connected wireless controller.

Name: The LAN host name if available through NetBIOS.

IP Address: The LAN device's IP address.

MAC Address: The MAC address of the connected LAN client.

Figure 59: LAN Associated Clients



ASSOCIATED CLIENTS STATISTICS

Description goes here...

Associated Clients Statistics

	MAC Address	Packets		Bytes	
		Transmitted	Received	Transmitted	Received
□	e0:a6:70:8e:bf:67	4	37	684	6664

The following actions are supported from this page:

Refresh: Updates the page with the latest information

View Details: Shows detailed status associated client.

4.3.3 WLAN Associated Clients

Status > Traffic Monitor > Associated Clients Statistics > WLAN Associated Clients

The wireless client can roam among APs without interruption in WLAN service. The controller tracks the traffic the client sends and receives during the entire wireless session while the client roams among APs that the controller manages. The controller stores statistics about client traffic while it is associated with a single AP as well as throughout the roaming session.

MAC Address: This field shows the MAC address of the client station

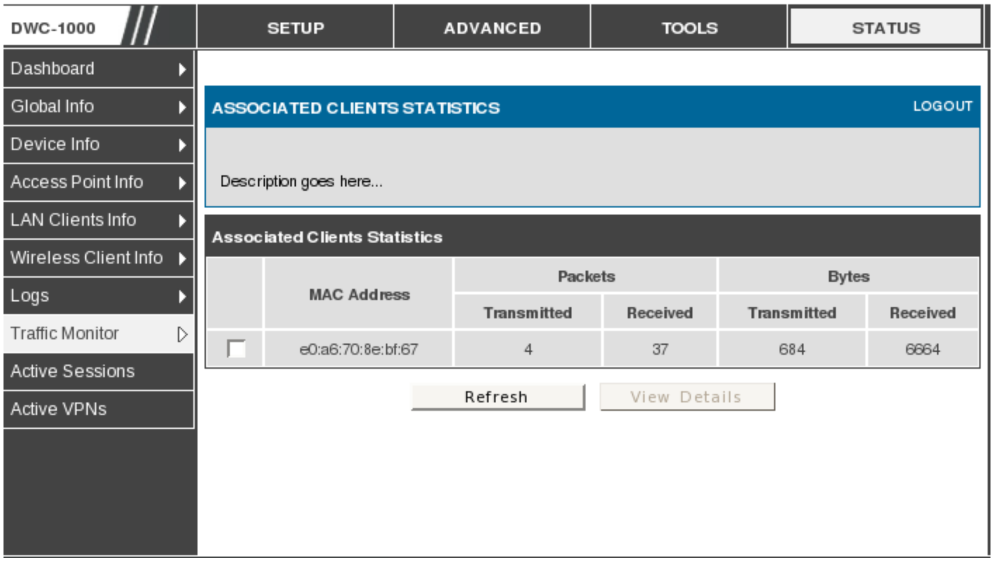
Packet Transmitted: This field shows the packet transmitted to the client station

Packet Received: This field shows the packet received to the client station

Bytes Transmitted: This field shows the bytes transmitted to the client station

Bytes Received: This field shows the bytes received to the client station

Figure 60: WLAN Associated Clients



ASSOCIATED CLIENTS STATISTICS

Description goes here...

Associated Clients Statistics

	MAC Address	Packets		Bytes	
		Transmitted	Received	Transmitted	Received
☐	e0:a6:70:8e:bf:67	4	37	684	6664

The following actions are supported from this page:

Refresh: Updates the page with the latest information

View Details: Shows detailed status associated client.

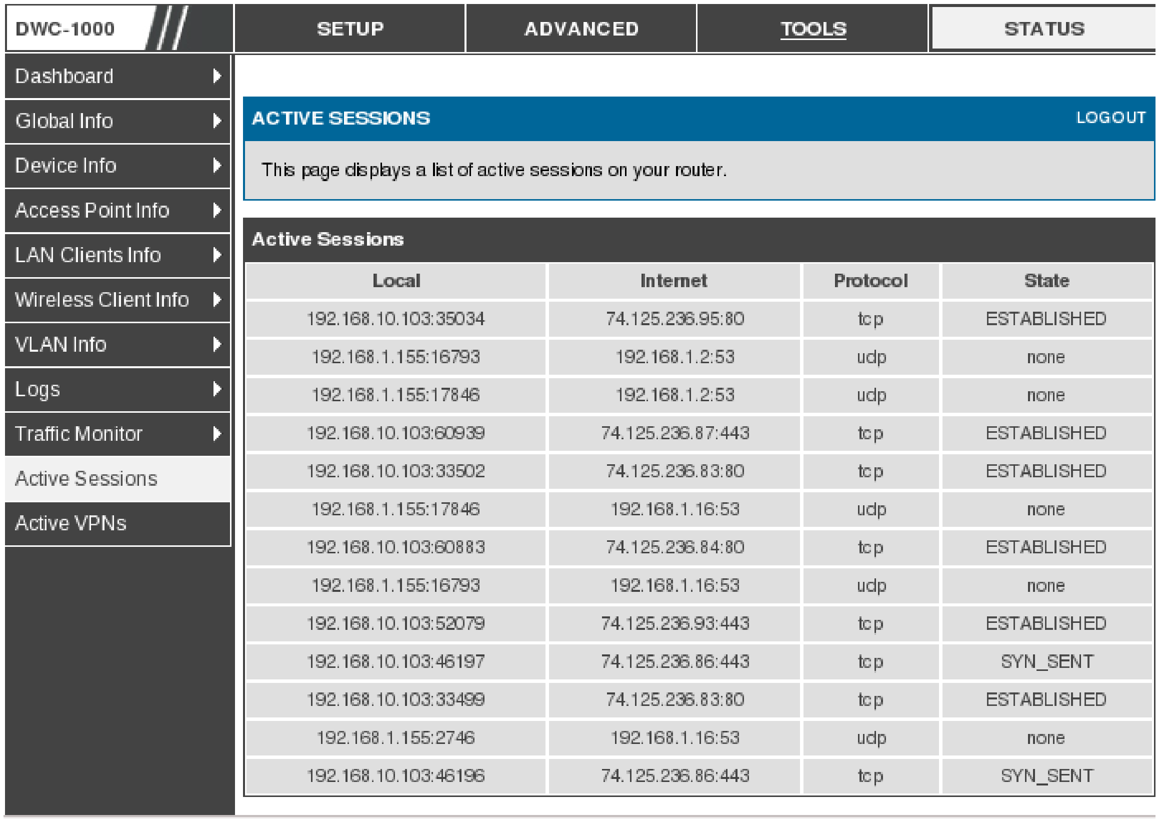
4.4 Active Connections

4.4.1 Sessions through the Controller

Status > Active Sessions

This table lists the active internet sessions through the controllers firewall. The session's protocol, state, local and remote IP addresses are shown.

Figure 61: List of current Active Firewall Sessions



ACTIVE SESSIONS

This page displays a list of active sessions on your router.

Active Sessions

Local	Internet	Protocol	State
192.168.10.103:35034	74.125.236.95:80	tcp	ESTABLISHED
192.168.1.155:16793	192.168.1.2:53	udp	none
192.168.1.155:17846	192.168.1.2:53	udp	none
192.168.10.103:60939	74.125.236.87:443	tcp	ESTABLISHED
192.168.10.103:33502	74.125.236.83:80	tcp	ESTABLISHED
192.168.1.155:17846	192.168.1.16:53	udp	none
192.168.10.103:60883	74.125.236.84:80	tcp	ESTABLISHED
192.168.1.155:16793	192.168.1.16:53	udp	none
192.168.10.103:52079	74.125.236.93:443	tcp	ESTABLISHED
192.168.10.103:46197	74.125.236.86:443	tcp	SYN_SENT
192.168.10.103:33499	74.125.236.83:80	tcp	ESTABLISHED
192.168.1.155:2746	192.168.1.16:53	udp	none
192.168.10.103:46196	74.125.236.86:443	tcp	SYN_SENT

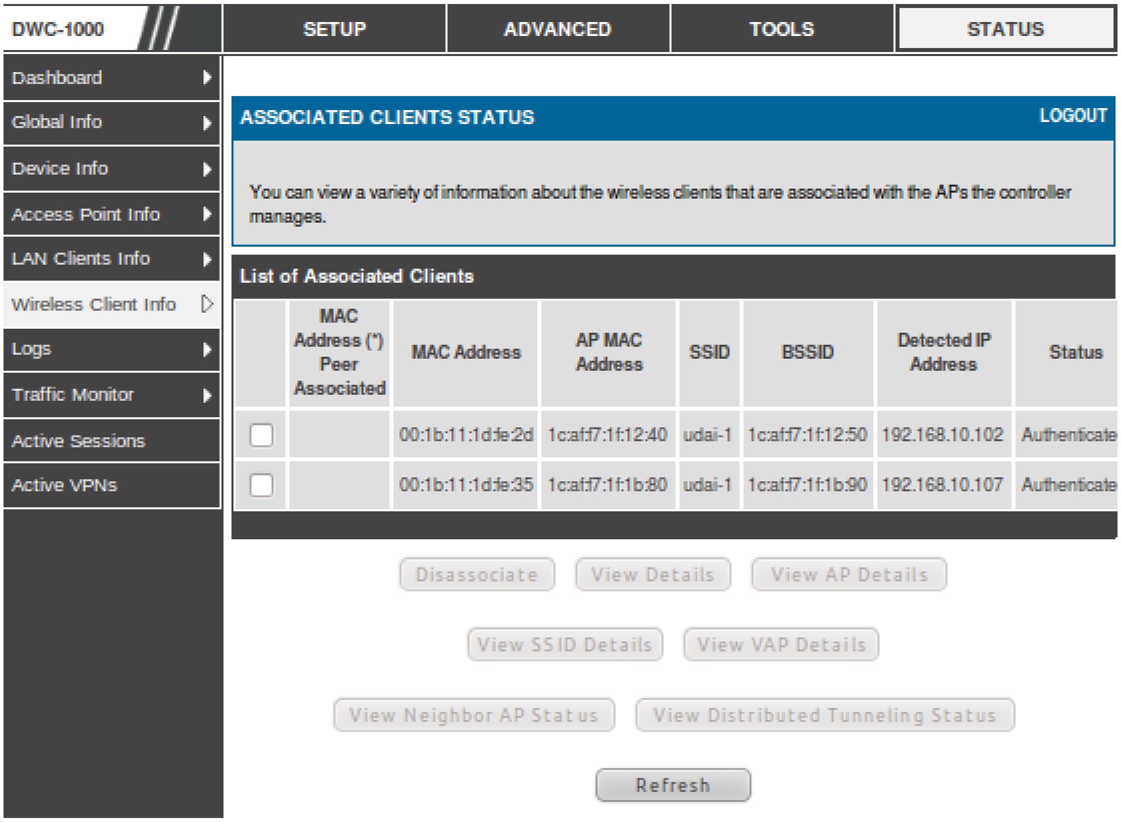
4.5 LAN Client Info

4.5.1 Associated Clients

Status > LAN Client Info > Associated Clients

The clients that are associated with the APs the controller manages as displayed.

Figure 62: Associated Clients



ASSOCIATED CLIENTS STATUS

You can view a variety of information about the wireless clients that are associated with the APs the controller manages.

List of Associated Clients

	MAC Address (*) Peer Associated	MAC Address	AP MAC Address	SSID	BSSID	Detected IP Address	Status
□		00:1b:11:1d:fe:2d	1c:af:f7:1f:12:40	udai-1	1c:af:f7:1f:12:50	192.168.10.102	Authenticate
□		00:1b:11:1d:fe:35	1c:af:f7:1f:1b:80	udai-1	1c:af:f7:1f:1b:90	192.168.10.107	Authenticate

MAC Address: The Ethernet address of the client station. If the MAC address is followed by an asterisk (*), the client is associated with an AP managed by a peer controller.

AP MAC Address: The Ethernet address of the AP.

SSID: The network on which the client is connected.

BSSID: The Ethernet MAC address for the managed AP VAP where this client is associated.

Detected IP Address: Identifies the IPv4 address of the client, if available.

Status: Indicates whether or not the client has associated and/or authenticated. The valid values are:

- **Associated**: The client is currently associated to the managed AP.
- **Authenticated**: The client is currently associated and authenticated to the managed AP.

- **Disassociated**: The client has disassociated from the managed AP. If the client does not roam to another managed AP within the client roam timeout, it will be deleted.

Disassociate: Disassociates the client from the managed AP.

View Details: For each client associated with an AP that the controller manages, you can view detailed status information about the client and its association with the access point.

View Neighbour Status: The associated client status shows information about access points that the client detects. The information on this page can help you determine the managed AP an associated client might use for roaming.

View Distributed Tunneling Status: The associated client status shows information about access points that the client detects. The AP-AP tunnelling mode is used to support L3 roaming for wireless clients without forwarding any data traffic to the wireless controller

View SSID Details: Each managed AP can be from different networks that each have a unique SSID. Although several wireless clients might be connected to the same physical AP, they might not connect by using the same SSID. The WLAN > Monitoring > Client > Associated Clients > SSID Status page lists the SSIDs of the networks that each wireless client associated with a managed AP has used for WLAN access.

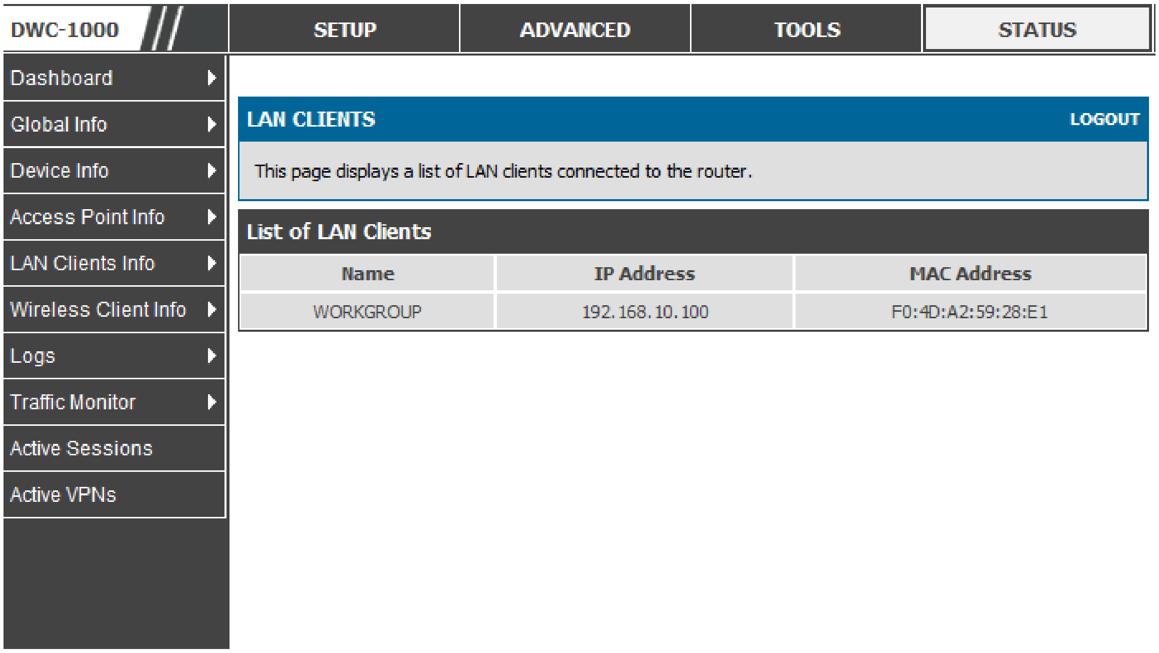
View VAP Details: Each AP has set of Virtual Access Points (VAPs) per radio, and every VAP has a unique MAC address (BSSID). This displays the VAP Associated Client Status page which shows information about the VAPs on the managed AP that have associated wireless clients.

4.5.2 LAN Clients

Status > LAN Client Info >LAN Clients

The LAN clients to the controller are identified by an ARP scan through the LAN controller. The NetBios name (if available), IP address and MAC address of discovered LAN hosts are displayed.

Figure 63: List of LAN hosts



LAN CLIENTS

This page displays a list of LAN clients connected to the router.

List of LAN Clients

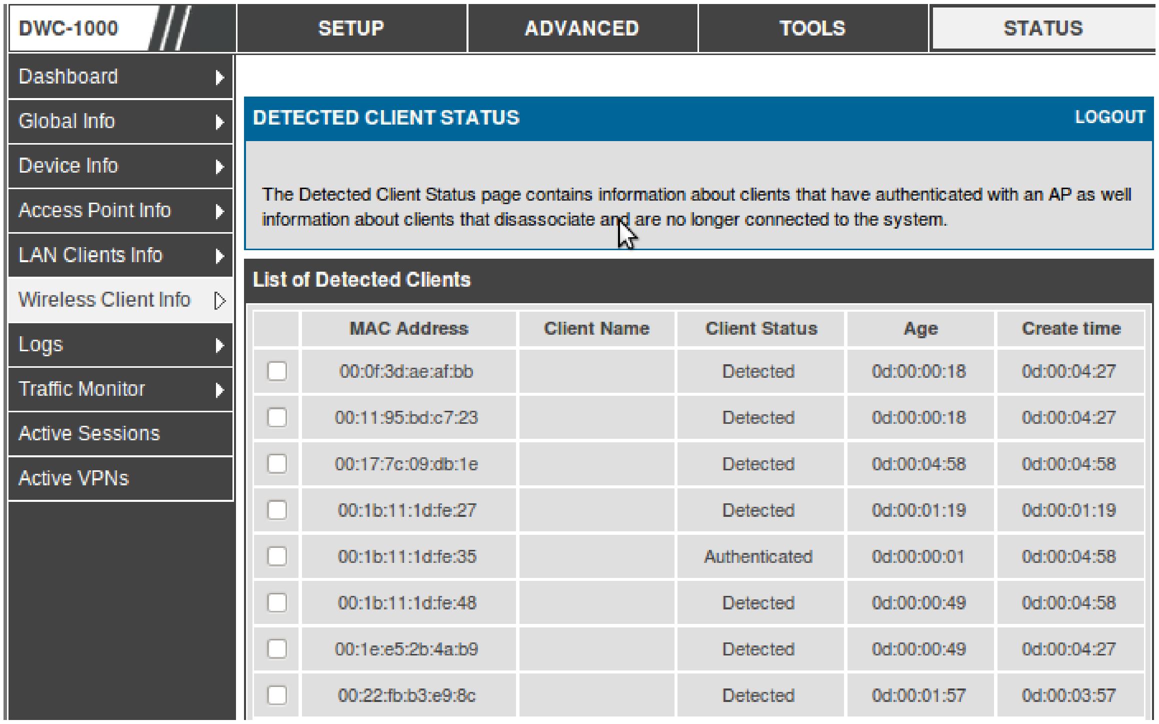
Name	IP Address	MAC Address
WORKGROUP	192.168.10.100	F0:4D:A2:59:28:E1

4.5.3 Detected Clients

Status > LAN Client Info > Detected Clients

Wireless clients are detected by the wireless system when the clients either attempt to interact with the system or when the system detects traffic from the clients. The Detected Client Status page contains information about clients that have authenticated with an AP as well information about clients that disassociate and are no longer connected to the system.

Figure 64: Detected Clients



DETECTED CLIENT STATUS

The Detected Client Status page contains information about clients that have authenticated with an AP as well information about clients that disassociate and are no longer connected to the system.

List of Detected Clients

	MAC Address	Client Name	Client Status	Age	Create time
□	00:0f:3d:ae:af:bb		Detected	0d:00:00:18	0d:00:04:27
□	00:11:95:bd:c7:23		Detected	0d:00:00:18	0d:00:04:27
□	00:17:7c:09:db:1e		Detected	0d:00:04:58	0d:00:04:58
□	00:1b:11:1d:fe:27		Detected	0d:00:01:19	0d:00:01:19
□	00:1b:11:1d:fe:35		Authenticated	0d:00:00:01	0d:00:04:58
□	00:1b:11:1d:fe:48		Detected	0d:00:00:49	0d:00:04:58
□	00:1e:e5:2b:4a:b9		Detected	0d:00:00:49	0d:00:04:27
□	00:22:fb:b3:e9:8c		Detected	0d:00:01:57	0d:00:03:57

MAC Address: The Ethernet MAC address of the client.

Client Name: Shows the name of the client, if available, from the Known Client Database. If client is not in the database then the field is blank.

Client Status: Shows the client status, which can be one of the following:

- Authenticated. The wireless client is authenticated with the wireless system.
- Detected. The wireless client is detected by the wireless system but is not a security threat.
- Black-Listed. The client with this MAC address is specifically denied access via
- MAC Authentication.
- Rogue. The client is classified as a threat by one of the threat detection algorithms.

Age: Time since any event has been received for this client that updated the detected client database entry.

Create Time: Time since this entry was first added to the detected clients database.

4.5.4 Active VPN Tunnels

> ✍ The following feature is available upon licensed activation of VPN / Firewall features for the system.

Status > Active VPNs

You can view and change the status (connect or drop) of the controllers IPsec security associations. Here, the active IPsec SAs (security associations) are listed along with the traffic details and tunnel state. The traffic is a cumulative measure of transmitted/received packets since the tunnel was established.

If a VPN policy state is “IPsec SA Not Established”, it can be enabled by clicking the Connect button of the corresponding policy. The Active IPsec SAs table displays a list of active IPsec SAs. Table fields are as follows.

Policy Name: IKE or VPN policy associated with this SA.

Endpoint: IP address of the remote VPN gateway or client.

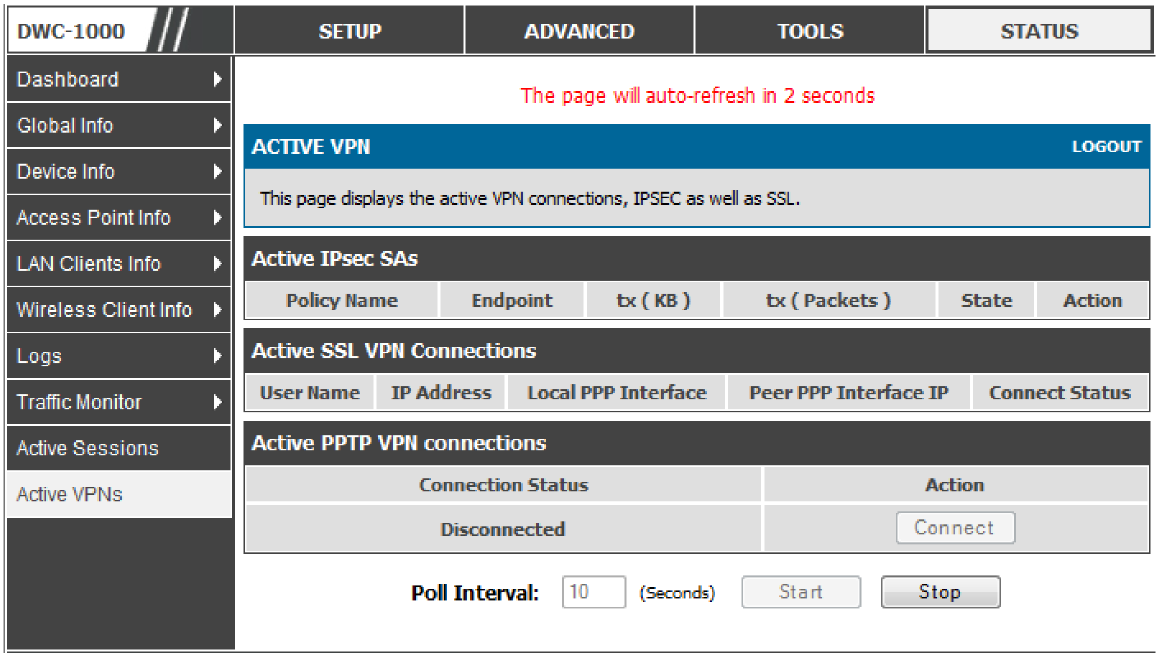
Tx (KB): Kilobytes of data transmitted over this SA.

Tx (Packets): Number of IP packets transmitted over this SA.

State: Status of the SA for IKE policies: Not Connected or IPsec SA Established.

Action: Click Connect to establish an inactive SA (connection) or Disconnect to terminate an active SA (connection).

Figure 65: List of current Active VPN Sessions



The page will auto-refresh in 2 seconds

ACTIVE VPN

This page displays the active VPN connections, IPSEC as well as SSL.

Active IPsec SAs

Policy Name	Endpoint	tx (KB)	tx (Packets)	State	Action

Active SSL VPN Connections

User Name	IP Address	Local PPP Interface	Peer PPP Interface IP	Connect Status

Active PPTP VPN connections

Connection Status	Action
Disconnected	Connect

Poll Interval: 10 (Seconds)

All active SSL VPN connections, both for VPN tunnel and VPN Port forwarding, are displayed on this page as well. Table fields are as follows.

User Name: The SSL VPN user that has an active tunnel or port forwarding session to this controller.

IP Address: IP address of the remote VPN client.

Local PPP Interface: The interface (Option 1or Option2) through which the session is active.

Peer PPP Interface IP: The assigned IP address of the virtual network adapter.

Connect Status: Status of the SSL connection between this controller and the remote VPN client: Not Connected or Connected.

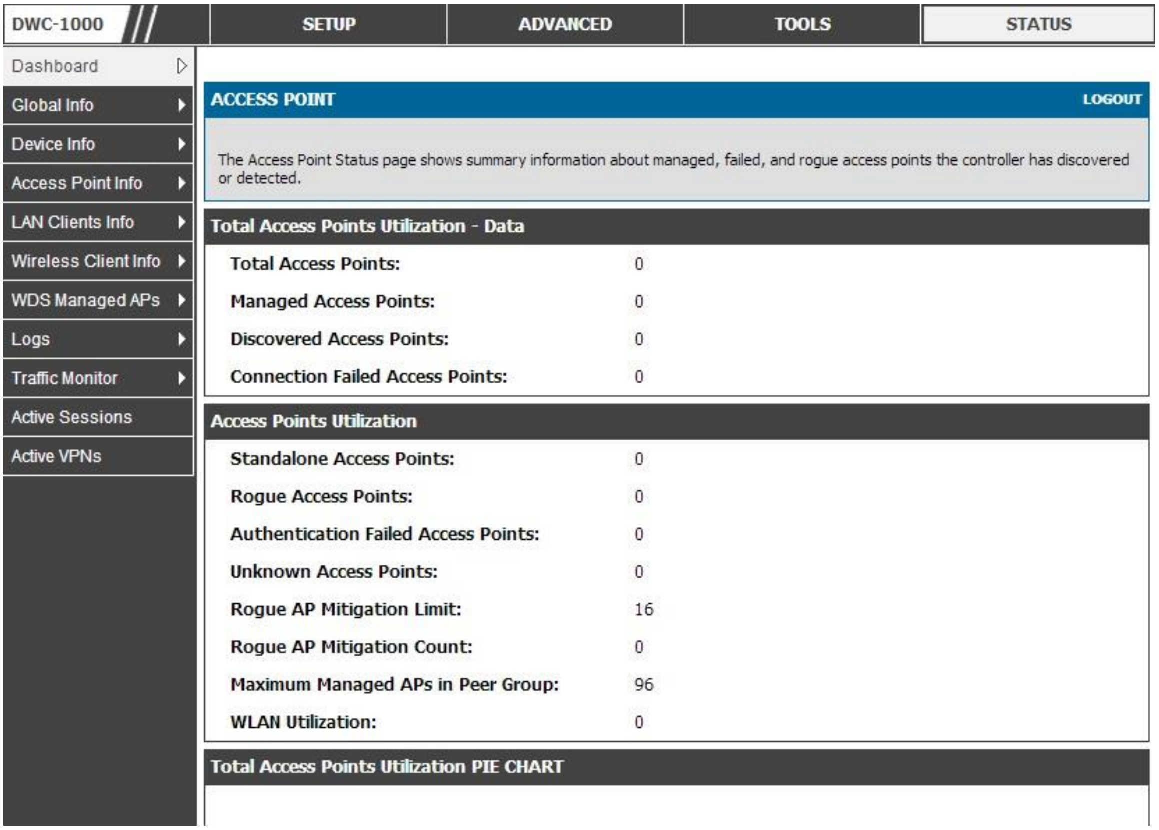
4.6 Access Point

4.6.1 Access Point Status

Status > General > Access Point

The Access Point Status page shows summary information about managed, failed, and rogue access points the controller has discovered or detected.

Figure 66: AP Statistics



ACCESS POINT

The Access Point Status page shows summary information about managed, failed, and rogue access points the controller has discovered or detected.

Total Access Points Utilization - Data

Total Access Points:	0
Managed Access Points:	0
Discovered Access Points:	0
Connection Failed Access Points:	0

Access Points Utilization

Standalone Access Points:	0
Rogue Access Points:	0
Authentication Failed Access Points:	0
Unknown Access Points:	0
Rogue AP Mitigation Limit:	16
Rogue AP Mitigation Count:	0
Maximum Managed APs in Peer Group:	96
WLAN Utilization:	0

Total Access Points Utilization PIE CHART

Total Access Points Utilization

Total Access Points: Total number of Managed APs in the database. This value is always equal to the sum of Managed Access Points, Connection Failed Access Points, and Discovered Access Points.

Managed Access Points: Number of APs in the managed AP database that are authenticated, configured, and have an active connection with the controller.

Discovered Access Points: APs that have a connection with the controller, but haven't been completely configured. This value includes all managed APs with a Discovered or Authenticated status.

Connection Failed Access Points: Number of APs that were previously authenticated and managed, but currently don't have connection with the controller.

Access Points Utilization

Standalone Access Points: Number of trusted APs in Standalone mode. APs in Standalone mode are not managed by a controller.

Rogue Access Points: Number of Rogue APs currently detected on the WLAN. When an AP performs an RF scan, it might detect access points that have not been validated. It reports these APs as rogues.

Authentication Failed Access Points:

Number of APs that failed to establish communication with the controller.

Unknown Access Points: Number of Unknown APs currently detected on the WLAN. If an AP configured to be managed by the controller is detected through an RF scan at any time that it is not actively managed it is classified as an Unknown AP.

Rogue AP Mitigation Limit: Maximum number of APs for which the system can send de-authentication frames.

Rogue AP Mitigation Count: Number of APs to which the wireless system is currently sending de-authentication messages to mitigate against rogue APs. A value of 0 indicates that mitigation is not in progress.

Maximum Managed APs in Peer Group: Maximum number of access points that can be managed by the cluster.

WLAN Utilization: Total network utilization across all APs managed by this controller. This is based on global statistics.

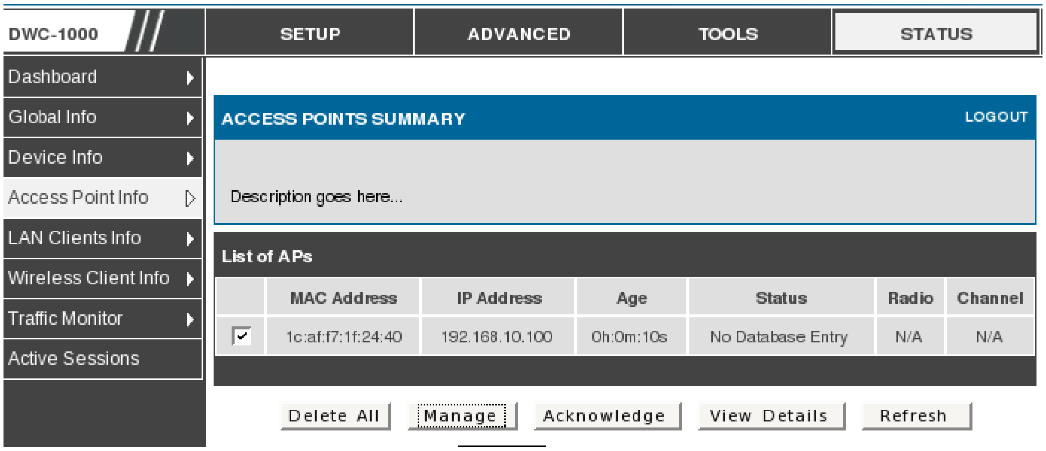
4.6.2 AP Summary

Status > Access Point Info> APs Summary

The List of AP page shows summary information about managed, failed, and rogue access points the controller has discovered or detected. The status entries can be deleted manually. To clear all APs from the All Access Points status page except Managed Access Points, click **Delete All**.

To configure an Authentication Failed AP to be managed by the controller the next time it is discovered, select the check box next to the MAC address of the AP and\click Manage. You will be presented with the Valid Access Point Configuration page.

Figure 67: AP status



Description goes here...

List of APs

	MAC Address	IP Address	Age	Status	Radio	Channel
☑	1c:af:f7:1f:24:40	192.168.10.100	0h:0m:10s	No Database Entry	N/A	N/A

MAC Address: Shows the MAC address of the access point.

IP Address: The network address of the access point.

Age: Shows how much time has passed since the AP was last detected and the information was last updated.

Status : Shows the access point status

- **Managed**: The AP profile configuration has been applied to the AP and it's operating in managed mode.
- **No Database Entry**: MAC address of the AP does not appear in the local or RADIUS Valid AP database.
- **Authentication (Failed AP)**: The AP failed to be authenticated by the controller or RADIUS server. Since AP is not configured as a valid AP which the correct local or RADIUS authentication information.
- **Failed**: The controller lost contact with the AP; a failed entry will remain in the managed AP database unless you remove it. Note that a managed AP will temporarily show a failed status during a reset.
- **Rogue**: The AP has not attempted to contact the controller and the MAC address of the AP is not in the Valid AP database.

Radio: Shows the wireless radio mode the AP is using.

Channel: Shows the operating channel for the radio.

The following actions are supported from this page

Delete All: Manually clear all APs from the All Access Points status page except Managed Access Points.

Manage: Configure an Authentication Failed AP to be managed by the controller the next time it is discovered. Select the check box next to the MAC address of the AP before you click Manage You will be presented with the Valid Access Point Configuration page. You can then configure the AP and click Submit to save the AP in the local Valid AP database. If you use a RADIUS server for AP validation, you must add the MAC address of the AP to the AP database on the RADIUS server.

Acknowledge: Identify an AP as an Acknowledged Rogue. Select the check box next to the MAC address of the AP before you click Acknowledge. The controller adds the AP to the Valid AP database as an Acknowledged Rogue.

View Details: To view the details configured APs. Select the check box next to the MAC address of the AP before you click View Details.

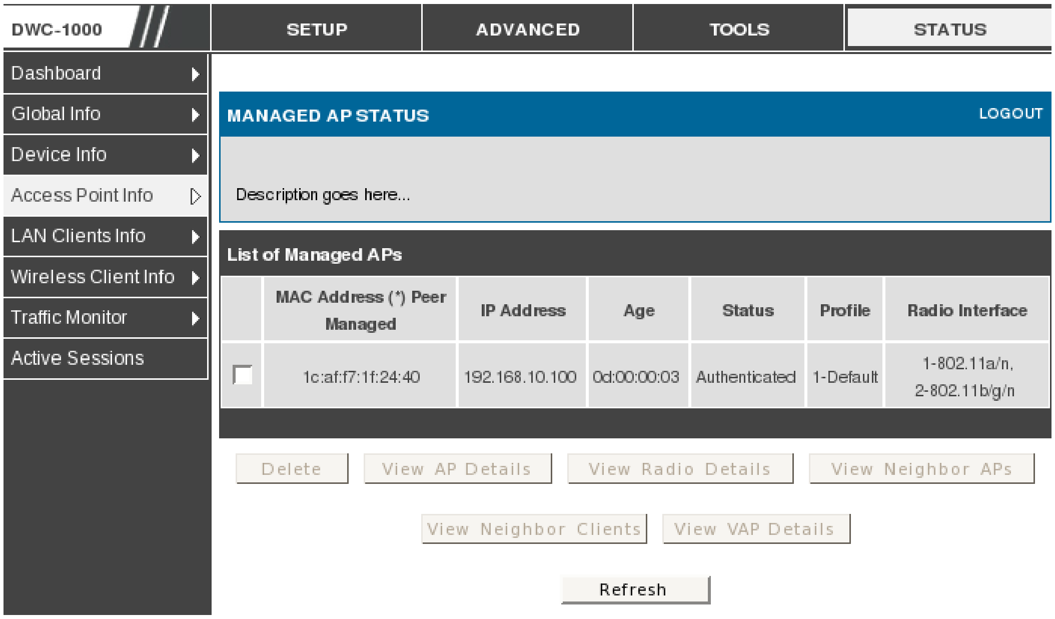
Refresh: Updates the page with the latest information

4.6.3 Managed AP Status

Status > Access Point Info> Managed AP Status

In the Managed AP Status page, you can access a variety of information about each AP that the controller manages.

Figure 68: Managed AP status



MANAGED AP STATUS

Description goes here...

List of Managed APs

	MAC Address (*) Peer Managed	IP Address	Age	Status	Profile	Radio Interface
□	1c:af:f7:1f:24:40	192.168.10.100	0d:00:00:03	Authenticated	1-Default	1-802.11a/n, 2-802.11b/g/n

MAC Address: The Ethernet address of the controller-managed AP.

IP Address: The network IP address of the managed AP.

Age: Time since last communication between the Controller and the AP.

Status: The current managed state of the AP. The possible values are

- **Discovered**: The AP is discovered and by the controller, but is not yet authenticated.
- **Authenticated**: The AP has been validated and authenticated (if authentication is enabled), but it is not configured.

- **Managed**: The AP profile configuration has been applied to the AP and it's operating in managed mode.
- **Failed**: The Controller lost contact with the AP, a failed entry will remain in the managed AP database unless you remove it. Note that a managed AP will temporarily show a failed status during a reset.

Profile: The AP profile configuration currently applied to the managed AP. The profile is assigned to the AP in the valid AP database.

Radio Interface: Shows the wireless radio mode that each radio on the AP is using.

The following actions are supported from this page**:**

Delete: Manually clear existing APs

View AP Details: Shows detailed status information collected from the AP.

View Radio Details: Shows detailed status for a radio interface

View Neighbor Details: Shows the neighbour APs that the specified AP has discovered through periodic RF scans on the selected radio interface

View Neighbor Clients: Shows information about wireless clients associated with an AP or detected by the AP radio

View VAP Details: Shows summary information about the virtual access points (VAPs) for the selected AP and radio interface on the APs that the controller manages

4.6.4 Authentication Failure Status

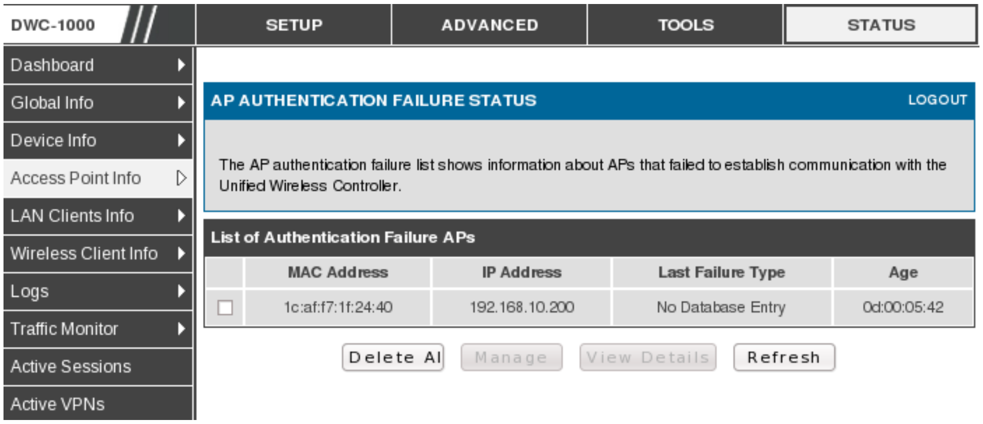
Status > Access Point Info> Authentication Failure Status

An AP might fail to associate to the controller due to errors such as invalid packet format or vendor ID, or because the AP is not configured as a valid AP with the correct local or RADIUS authentication information The AP authentication failure list shows information about APs that failed to establish communication with the DWC-1000 wireless controller

The AP can fail due to one of the following reasons:

- **No Database Entry**: The MAC address of the AP is not in the local Valid AP database or the external RADIUS server database, so the AP has not been validated.
- **Local Authentication**: The authentication password configured in the AP did not match the password configured in the local database.
- **Not Managed**: The AP is in the Valid AP database, but the AP Mode in the local database is not set to Managed.
- **RADIUS Authentication**: The password configured in the RADIUS client for the RADIUS server was rejected by the server.
- **RADIUS Challenged**: The RADIUS server is configured to use the Challenge-Response authentication mode, which is incompatible with the AP.
- **RADIUS Unreachable**: The RADIUS server that the AP is configured to use is unreachable.
- **Invalid RADIUS Response**: The AP received a response packet from the RADIUS server that was not recognized or invalid.
- **Invalid Profile ID**: The profile ID specified in the RADIUS database may not exist on the controller. This can also happen with the local database when the configuration has been received from a peer controller.
- **Profile Mismatch** • -Hardware Type: The AP hardware type specified in the AP Profile is not compatible with the actual AP hardware.

Figure 69: Authentication Failure Status



AP AUTHENTICATION FAILURE STATUS

The AP authentication failure list shows information about APs that failed to establish communication with the Unified Wireless Controller.

List of Authentication Failure APs

	MAC Address	IP Address	Last Failure Type	Age
□	1c:af:f7:1f:24:40	192.168.10.200	No Database Entry	0d:00:05:42

MAC Address: The Ethernet address of the AP. If the MAC address of the AP is followed by an asterisk (*), it was reported by a peer controller.

IP Address: The IP address of the AP.

Last Failure Type: Indicates the last type of failure that occurred, which can be one of the following:

- Local Authentication
- No Database Entry
- Not Managed
- RADIUS Authentication
- RADIUS Challenged
- RADIUS Unreachable
- Invalid RADIUS Response
- Invalid Profile ID
- Profile Mismatch-Hardware Type

Age: Time since failure occurred.

4.6.5 AP RF Scan Status

Status > Access Point Info> AP RF Scan Status

The radios on each AP can periodically scan the radio frequency to collect information about other APs and wireless clients that are within range. In normal operating mode the AP always scans on the operational channel for the radio.

MAC Address: The Ethernet MAC address of the detected AP. This could be a physical radio interface or VAP MAC.

SSID: Service Set ID of the network, which is broadcast in the detected beacon frame.

Physical Mode: Indicates the 802.11 mode being used on the AP.

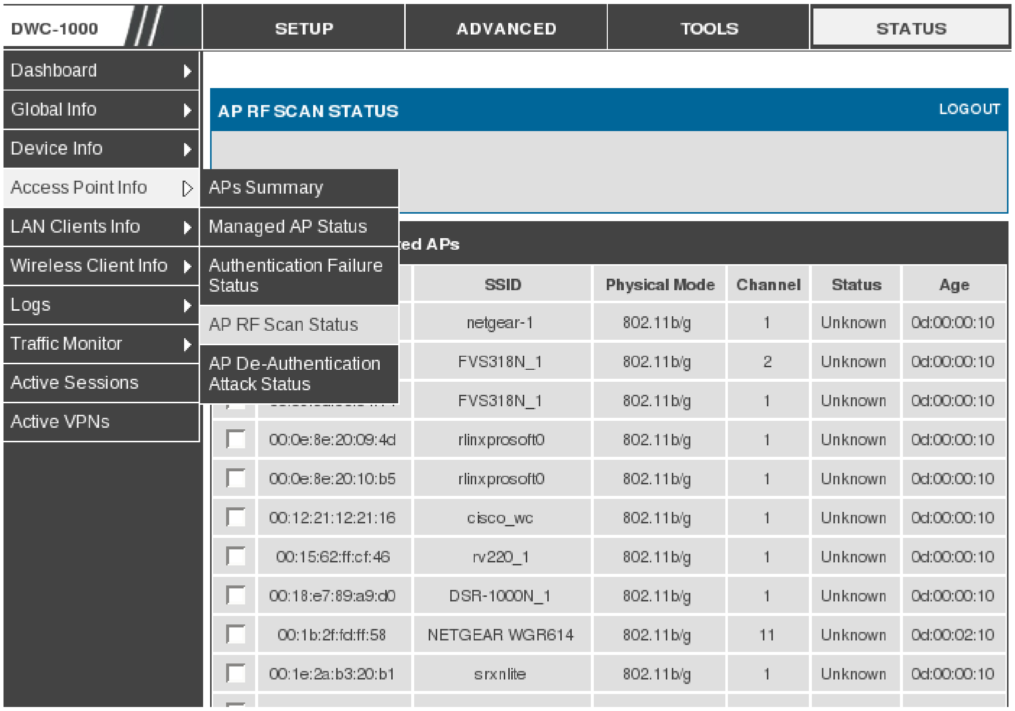
Channel: Transmit channel of the AP.

Status: Indicates the managed status of the AP, whether this is a valid AP known to the controller or a Rogue on the network. The valid values are:

- **Managed**: The neighbor AP is managed by the wireless system.
- **Standalone**: The AP is managed in standalone mode and configured as a valid AP entry (local or RADIUS).
- **Rogue**: The AP is classified as a threat by one of the threat detection algorithms.
- **Unknown**: The AP is detected in the network but is not classified as a threat by the threat detection algorithms.

Age: Time since this AP was last detected in an RF scan. Status entries for the RF Scan Status page are collected at a point in time and eventually age out. The age value for each entry shows how long ago the controller recorded the entry.

Figure 70: AP RF Scan Status



AP RF SCAN STATUS

ed APs

		SSID	Physical Mode	Channel	Status	Age
		netgear-1	802.11b/g	1	Unknown	0d:00:00:10
		FVS318N_1	802.11b/g	2	Unknown	0d:00:00:10
		FVS318N_1	802.11b/g	1	Unknown	0d:00:00:10
□	00:0e:8e:20:09:4d	rlinxprosoft0	802.11b/g	1	Unknown	0d:00:00:10
□	00:0e:8e:20:10:b5	rlinxprosoft0	802.11b/g	1	Unknown	0d:00:00:10
□	00:12:21:12:21:16	cisco_wc	802.11b/g	1	Unknown	0d:00:00:10
□	00:15:62:ff:cf:46	rv220_1	802.11b/g	1	Unknown	0d:00:00:10
□	00:18:e7:89:a9:d0	DSR-1000N_1	802.11b/g	1	Unknown	0d:00:00:10
□	00:1b:2f:fd:ff:58	NETGEAR WGR614	802.11b/g	11	Unknown	0d:00:02:10
□	00:1e:2a:b3:20:b1	srxnlite	802.11b/g	1	Unknown	0d:00:00:10

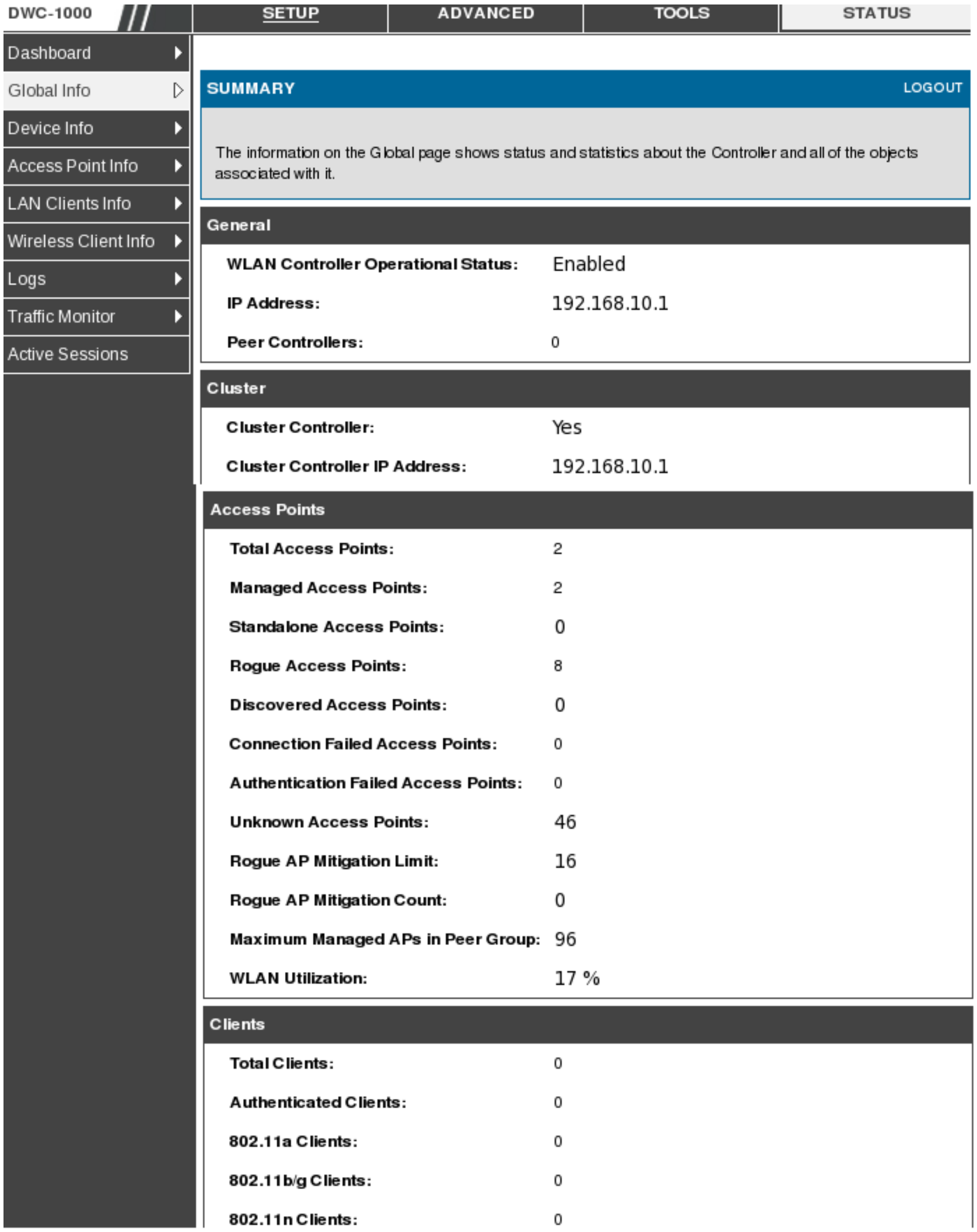
4.7 Global Info

4.7.1 Global status

Status > Global Info > Global Status

The DWC-1000 controller periodically collects information from the APs it manages and from associated peer controller. The information on the Global page shows status and statistics about the controller and all of the objects associated with it.

Figure 71: Global Status (Part 1)



SUMMARY

The information on the Global page shows status and statistics about the Controller and all of the objects associated with it.

General

WLAN Controller Operational Status:	Enabled
IP Address:	192.168.10.1
Peer Controllers:	0

Cluster

Cluster Controller:	Yes
Cluster Controller IP Address:	192.168.10.1

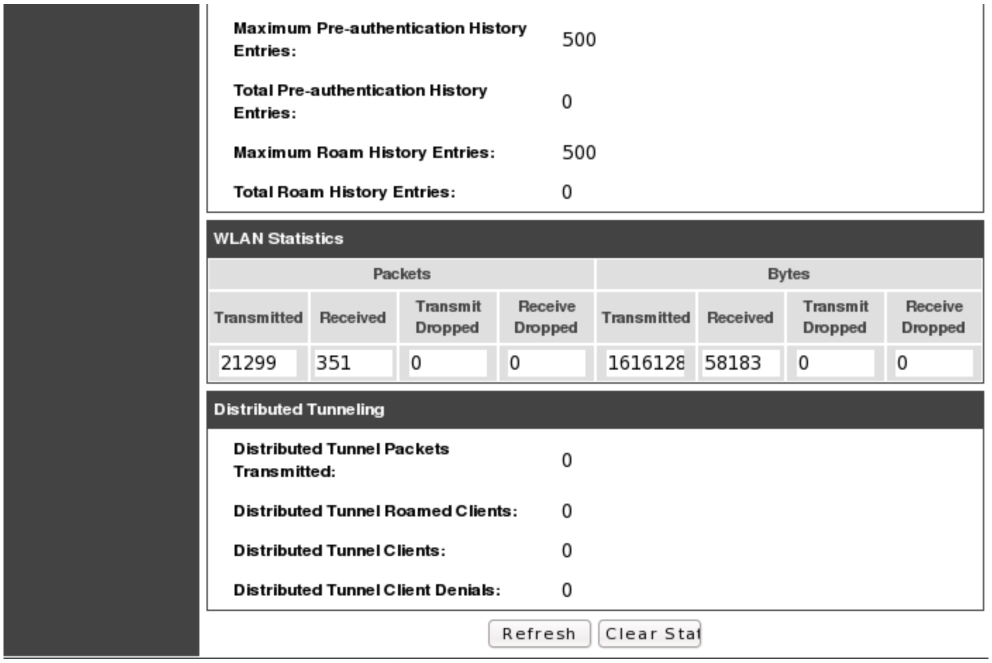
Access Points

Total Access Points:	2
Managed Access Points:	2
Standalone Access Points:	0
Rogue Access Points:	8
Discovered Access Points:	0
Connection Failed Access Points:	0
Authentication Failed Access Points:	0
Unknown Access Points:	46
Rogue AP Mitigation Limit:	16
Rogue AP Mitigation Count:	0
Maximum Managed APs in Peer Group:	96
WLAN Utilization:	17 %

Clients

Total Clients:	0
Authenticated Clients:	0
802.11a Clients:	0
802.11b/g Clients:	0
802.11n Clients:	0

Figure 72: Global Status (Part 2)



Maximum Pre-authentication History Entries:	500
Total Pre-authentication History Entries:	0
Maximum Roam History Entries:	500
Total Roam History Entries:	0

WLAN Statistics

Packets				Bytes			
Transmitted	Received	Transmit Dropped	Receive Dropped	Transmitted	Received	Transmit Dropped	Receive Dropped
21299	351	0	0	1616128	58183	0	0

Distributed Tunneling

Distributed Tunnel Packets Transmitted:	0
Distributed Tunnel Roamed Clients:	0
Distributed Tunnel Clients:	0
Distributed Tunnel Client Denials:	0

WLAN Controller Operational Status: This status field displays the operational status of this controller (a WLAN controller). The WLAN Controller may be configured as enabled, but is operationally disabled due to configuration dependencies. If the operational status is disabled, the reason will be displayed in the following status field.

IP Address: IP address of the controller.

Peer Controller: Number of peer WLAN controllers detected on the network.

Cluster Controller: Indicates whether this controller is the Cluster Controller for the cluster.

Cluster Controller IP Address: The IP address of the peer controller that is the Cluster Controller.

Total Access Points: Total number of Managed APs in the database. This value is always equal to the sum of Managed Access Points, Connection Failed Access Points, and Discovered Access Points.

Managed Access Points: Number of APs in the managed AP database that are authenticated, configured, and have an active connection with the controller.

Standalone Access Points: Number of trusted APs in Standalone mode. APs in Standalone mode are not managed by a controller.

Rogue Access Points: Number of Rogue APs currently detected on the WLAN. When an AP performs an RFscan, it might detect access points that have not been validated. It reports these APs as rogues.

Discovered Access Points: APs that have a connection with the controller, but haven't been completely configured. This value includes all managed APs with a Discovered or Authenticated status.

Connection Failed Access Points: Number of APs that were previously authenticated and managed, but currently don't have connection with the Unified Controller.

Authentication Failed Access Points: Number of APs that failed to establish communication with the Unified Controller.

Unknown Access Points: Number of Unknown APs currently detected on the WLAN. If an AP configured to be managed by the Unified Controller is detected through an RF scan at any time that it is not actively managed it is classified as an Unknown AP.

Rogue AP Mitigation Limit: Maximum number of APs for which the system can send de-authentication frames.

Rogue AP Mitigation Count: Number of APs to which the wireless system is currently sending the authentication messages to mitigate against rogue APs. A value of 0 indicates that mitigation is not in progress.

Maximum Managed APs in Peer Group: Maximum number of access points that can be managed by the cluster.

WLAN Utilization: Total network utilization across all APs managed by this controller. This is based on global statistics.

Total Clients: Total number of clients in the database. This total includes clients with an Associated, Authenticated, or Disassociated status.

Authenticated Clients: Total number of clients in the associated client database with an Authenticated status.

802.11a Clients: Total number of IEEE 802.11a only clients that are authenticated.

802.11b/g Clients: Total number of IEEE 802.11b/g only clients that are authenticated.

802.11n Clients: Total number of clients that are IEEE 802.11n capable and are authenticated. These include IEEE 802.11a/n, IEEE 802.11b/g/n, 5 GHz IEEE 802.11n, 2.4GHz IEEE 802.11n.

Maximum Associated Clients: Maximum number of clients that can associate with the wireless system. This is the maximum number of entries allowed in the Associated Client database.

Detected Clients: Number of wireless clients detected in the wireless network environment.

Maximum Detected Clients: Maximum number of clients that can be detected by the controller. The number is limited by the size of the Detected Client Database.

Maximum Pre-authentication History Entries: Maximum number of Client Pre-authentication events that can be recorded by the system.

Total Pre-authentication History: Entries Current number of pre-authentication history entries in use by the system.

Maximum Roam History Entries: Maximum number of entries that can be recorded in the roam history for all detected clients.

Total Roam History Entries: Current number of roam history entries in use by the system.

AP Provisioning Count: Current number of AP provisioning entries configured on the system.

WLAN Bytes Transmitted: Total bytes transmitted across all APs managed by the controller.

WLAN Packets Transmitted: Total packets transmitted across all APs managed by the controller.

WLAN Bytes Received Total bytes received across all APs managed by the controller.

WLAN Packets Received: Total packets received across all APs managed by the controller.

WLAN Bytes Transmit Dropped: Total bytes transmitted across all APs managed by the controller that were dropped.

WLAN Packets Transmit Dropped: Total packets transmitted across all APs managed by the controller that were dropped.

WLAN Bytes Receive Dropped: Total bytes received across all APs managed by the controller that were dropped.

WLAN Packets Receive Dropped: Total packets received across all APs managed by the controller that were dropped.

Distributed Tunnel Packets Transmitted: Total number of packets sent by all APs via distributed tunnels.

Distributed Tunnel Roamed Clients: Total number of clients that successfully roamed away from Home AP using distributed tunneling.

Distributed Tunnel Clients: Total number of clients that are associated with an AP that are using distributed tunneling.

Distributed Tunnel Client Denials: Total number of clients for which the system was unable to set up a distributed tunnel when client roamed

The following actions are supported from this page:

Refresh: Updates the page with the latest information.

Clear Statistics: Reset all counters on the page to zero

4.7.2 Peer Controller Status

Status > Global Info > Peer Controller > Status

The Peer Controller Status page provides information about other Wireless Controllers in the network. Peer wireless controllers within the same cluster exchange data about themselves, their managed APs, and clients. The controller maintains a database with this data so you can view information about a peer, such as its IP address and software version. If the controller loses contact with a peer, all of the data for that peer is deleted. One controller in a cluster is elected as a Cluster Controller. The Cluster Controller collects status and statistics from all the other controllers in the cluster, including information about the APs peer controllers manage and the clients associated to those APs.

Cluster Controller IP Address: IP address of the controller that controls the cluster.

Peer Controllers: Displays the number of peer controller in the cluster.

List of Peer Controllers

IP Address: IP address of the peer wireless controller in the cluster.

Vendor ID: Vendor ID of the peer controller software.

Software Version: The software version for the given peer controller.

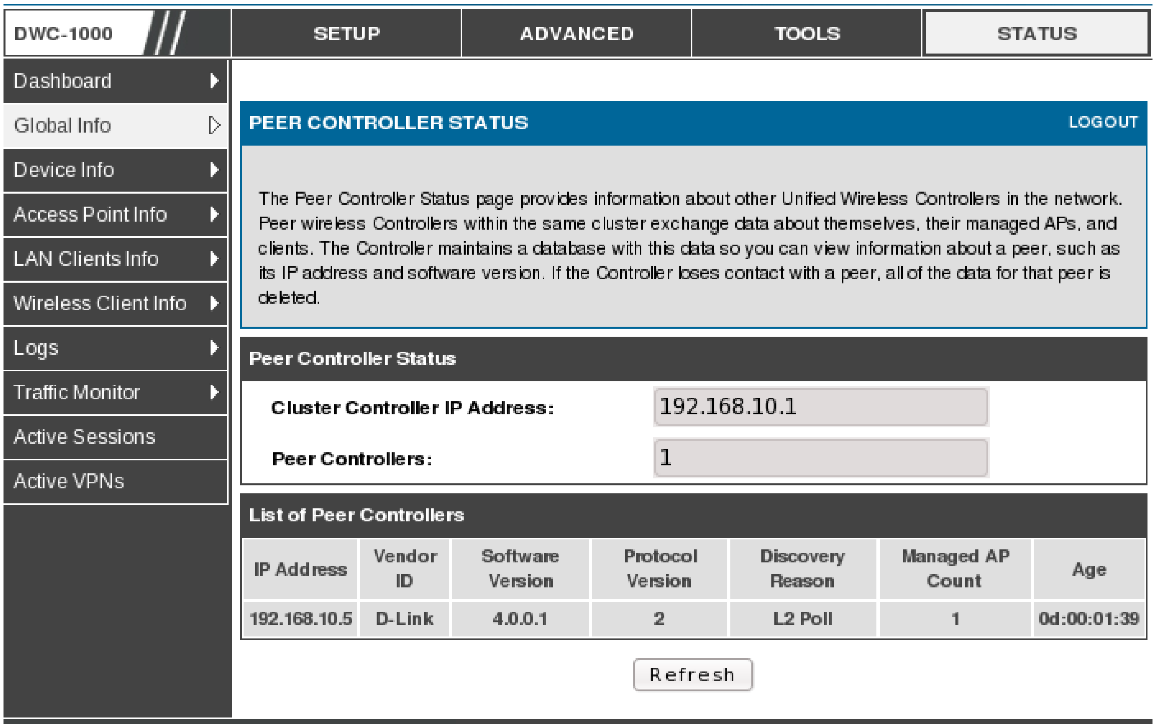
Protocol Version: Indicates the protocol version supported by the software on the peer controller.

Discovery Reason: The discovery method of the given peer controller, which can be through an L2 Poll or IP Poll

Managed AP Count: Shows the number of APs that the controller currently manages.

Age: Time since last communication with the controller in Hours, Minutes, and Seconds.

Figure 73: Peer Controller Status



PEER CONTROLLER STATUS

The Peer Controller Status page provides information about other Unified Wireless Controllers in the network. Peer wireless Controllers within the same cluster exchange data about themselves, their managed APs, and clients. The Controller maintains a database with this data so you can view information about a peer, such as its IP address and software version. If the Controller loses contact with a peer, all of the data for that peer is deleted.

Peer Controller Status

Cluster Controller IP Address:	192.168.10.1
Peer Controllers:	1

List of Peer Controllers

IP Address	Vendor ID	Software Version	Protocol Version	Discovery Reason	Managed AP Count	Age
192.168.10.5	D-Link	4.0.0.1	2	L2 Poll	1	0d:00:01:39

The following actions are supported from this page

Refresh: Updates the page with the latest information

4.7.3 Peer Controller Configuration Status

Status > Global Info > Peer Controller > Configuration

You can push portions of the controller configuration from one controller to another controller in the cluster. The Peer Controller Configuration Status page displays information about the configuration sent by a peer controller in the cluster. It also identifies the IP address of each peer controller that received the configuration information

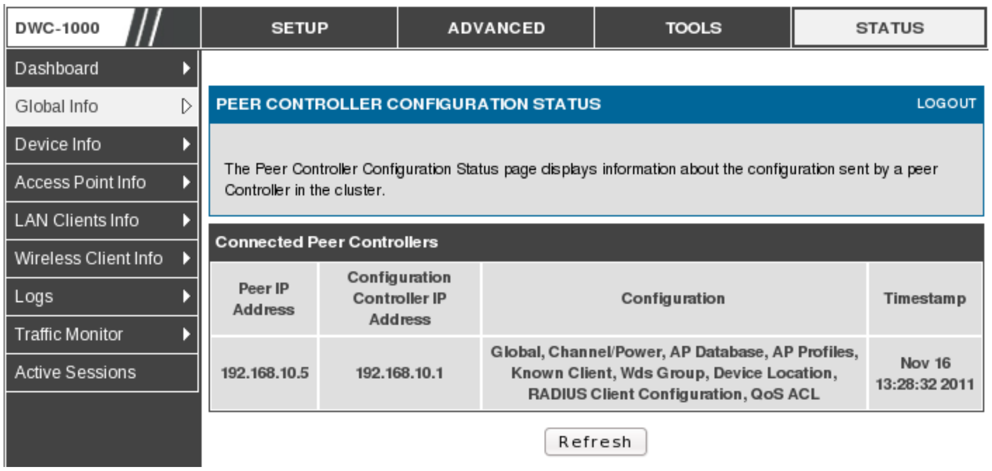
Peer IP Address: Shows the IP address of each peer wireless controller in the cluster that received configuration information.

Configuration Controller IP Address: Shows the IP Address of the controller that sent the configuration information.

Configuration: Identifies which parts of the configuration the controller received from the peer controller.

Timestamp: Shows when the configuration was applied to the controller. The time is displayed as UTC time and therefore only useful if the administrator has configured each peer controller to use NTP.

Figure 74: Peer Controller Configuration Status



PEER CONTROLLER CONFIGURATION STATUS

The Peer Controller Configuration Status page displays information about the configuration sent by a peer Controller in the cluster.

Connected Peer Controllers

Peer IP Address	Configuration Controller IP Address	Configuration	Timestamp
192.168.10.5	192.168.10.1	Global, Channel/Power, AP Database, AP Profiles, Known Client, Wds Group, Device Location, RADIUS Client Configuration, QoS ACL	Nov 16 13:28:32 2011

The following actions are supported from this page

Refresh: Updates the page with the latest information

4.7.4 Peer Controller Managed AP Status

Status > Global Info > Peer Controller > Managed AP

The Peer Controller Managed AP Status page displays information about the APs that each peer controller in the cluster manages. Use the menu above the table to select the peer controller with the AP information to display. Each peer controller is identified by its IP address

MAC Address: Shows the MAC address of each AP managed by the peer controller.

Peer Controller IP: Shows the IP address of the peer controller that manages the AP. This field displays when “All” is selected from the drop-down menu.

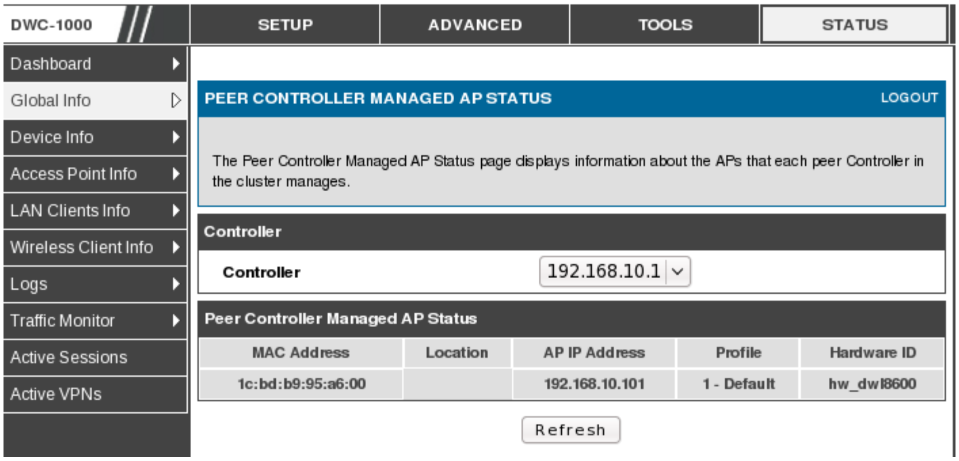
Location: The descriptive location configured for the managed AP.

AP IP Address: The IP address of the AP.

Profile: The AP profile applied to the AP by the controller.

Hardware ID: The Hardware ID associated with the AP hardware platform

Figure 75: Peer Controller Managed AP Status



PEER CONTROLLER MANAGED AP STATUS

The Peer Controller Managed AP Status page displays information about the APs that each peer Controller in the cluster manages.

Controller

Controller: 192.168.10.1

Peer Controller Managed AP Status

MAC Address	Location	AP IP Address	Profile	Hardware ID
1c:bd:b9:95:a6:00		192.168.10.101	1 - Default	hw_dwl8600

4.7.5 IP Discovery

Status > Global Info > IP Discovery

The IP Discovery list can contain the IP addresses of peer controllers and APs for the wireless controller to discover and associate with as part of the WLAN

IP Address: Shows the IP address of the device configured in the IP Discovery list.

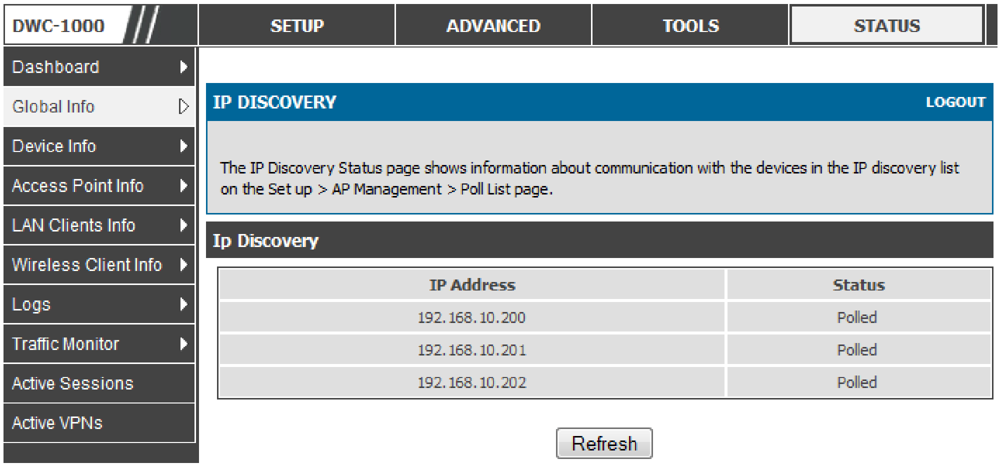
Status: The status is in one of the following states:

- **Not Polled**: The controller has not attempted to contact the IP address in the L3/IP Discovery list.
- Polled: The controller has attempted to contact the IP address.

- Discovered: The controller contacted the peer controller or the AP in the L3/IP Discovery list and has authenticated or validated the device.
- Discovered - Failed: The controller contacted the peer controller or the AP with IP address in the L3/IP Discovery list and was unable to authenticate or validate the device.

> ✍ Note: If the device is an access point, an entry appears in the AP failure list with a failure reason.

Figure 76: IP Discovery



The IP Discovery Status page shows information about communication with the devices in the IP discovery list on the Set up > AP Management > Poll List page.

IP Address	Status
192.168.10.200	Polled
192.168.10.201	Polled
192.168.10.202	Polled

4.7.6 Configuration Receive Status

Status > Global Info > Config Receive Status

The Peer Controller Configuration feature allows you to send the critical wireless configuration from one controller to all other controllers. In addition to keeping the controllers synchronized, this function enables the administrator to manage all wireless controllers in the cluster from one controller. The Peer Controller Configuration Received Status page provides information about the configuration a controller has received from one of its peers

Current Receive Status: Indicates the global status when wireless configuration is received from a peer controller. The possible status values are as follows:

- Not Started
- Receiving Configuration
- Saving Configuration,
- Applying AP Profile Configuration
- Success
- Failure - Invalid Code Version
- Failure - Invalid Hardware Version
- Failure - Invalid Configuration

Last Configuration Received: Peer controller IP Address indicates the last controller from which this controller received any wireless configuration data.

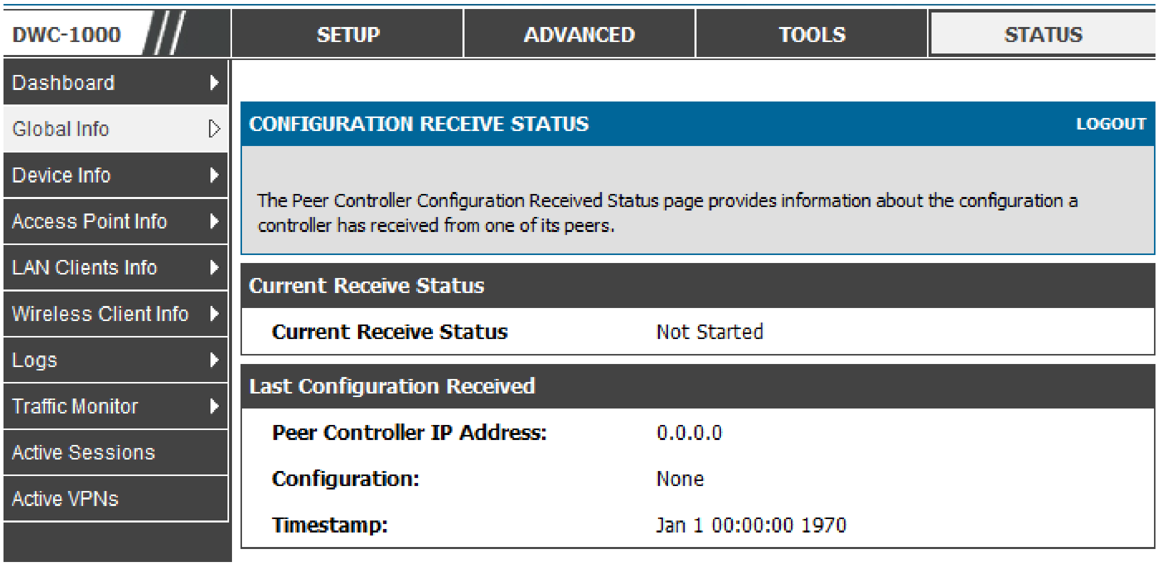
Configuration: Indicates which portions of configuration were last received from a peer controller, which can be one or more of the following:

- Global
- Discovery
- Channel/Power
- AP Database
- AP Profiles
- Known Client
- Captive Portal
- RADIUS Client
- QoS ACL
- QoS DiffServ

If the controller has not received any configuration for another controller, the value is **None**.

Timestamp: Indicates the last time this controller received any configuration data from a peer controller. The Peer Controller Managed AP Status page displays information about the APs that each peer controller in the cluster manages. Use the menu above the table to select the peer controller with the AP information to display. Each peer controller is identified by its IP address

Figure 77: Configuration Receive Status



CONFIGURATION RECEIVE STATUS

The Peer Controller Configuration Received Status page provides information about the configuration a controller has received from one of its peers.

Current Receive Status

Current Receive Status	Not Started

Last Configuration Received

Peer Controller IP Address:	0.0.0.0
Configuration:	None
Timestamp:	Jan 1 00:00:00 1970

4.7.7 AP Hardware Capability

Status > Global Info > AP H/W Capability

The controller can support APs that have different hardware capabilities, such as the supported number of radios, the supported IEEE 802.11 modes, and the software image required by the AP. From the AP Hardware Capability tab, you can access summary information about the AP Hardware support, the radios and IEEE modes supported by the hardware, and the software images that are available for download to the APs

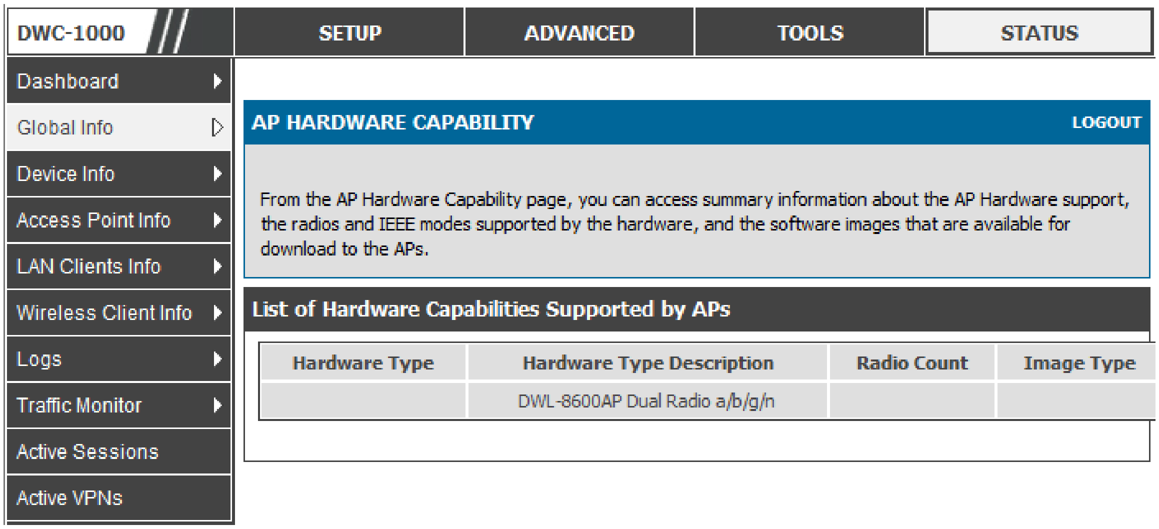
Hardware Type: Identifies the ID number assigned to each AP hardware type. The controller supports up to six different AP hardware types.

Hardware Type Description: Includes a description of the platform and the supported IEEE 802.11 modes.

Radio Count: Specifies whether the hardware supports one radio or two radios.

Image Type: Specifies the type of software the hardware requires.

Figure 78: AP Hardware Capability



AP HARDWARE CAPABILITY

From the AP Hardware Capability page, you can access summary information about the AP Hardware support, the radios and IEEE modes supported by the hardware, and the software images that are available for download to the APs.

List of Hardware Capabilities Supported by APs

Hardware Type	Hardware Type Description	Radio Count	Image Type
	DWL-8600AP Dual Radio a/b/g/n		

Each Radio will allow you to find out more information in the “View Radio Details” button. The following information is captured for each radio:

802.11a Support: Shows whether support for IEEE 802.11a mode is enabled.

Radio Type Description: Displays the type of radio, which might contain information such as the manufacturer name and supported IEEE 802.11 modes.

802.11bg Support: Shows whether support for IEEE 802.11bg mode is enabled.

VAP Count: Displays the number of VAPs the radio supports.

802.11n Support: Shows whether support for IEEE 802.11n mode is enabled.

802.11ac Support: Shows whether support for IEEE 802.11ac mode is enabled.

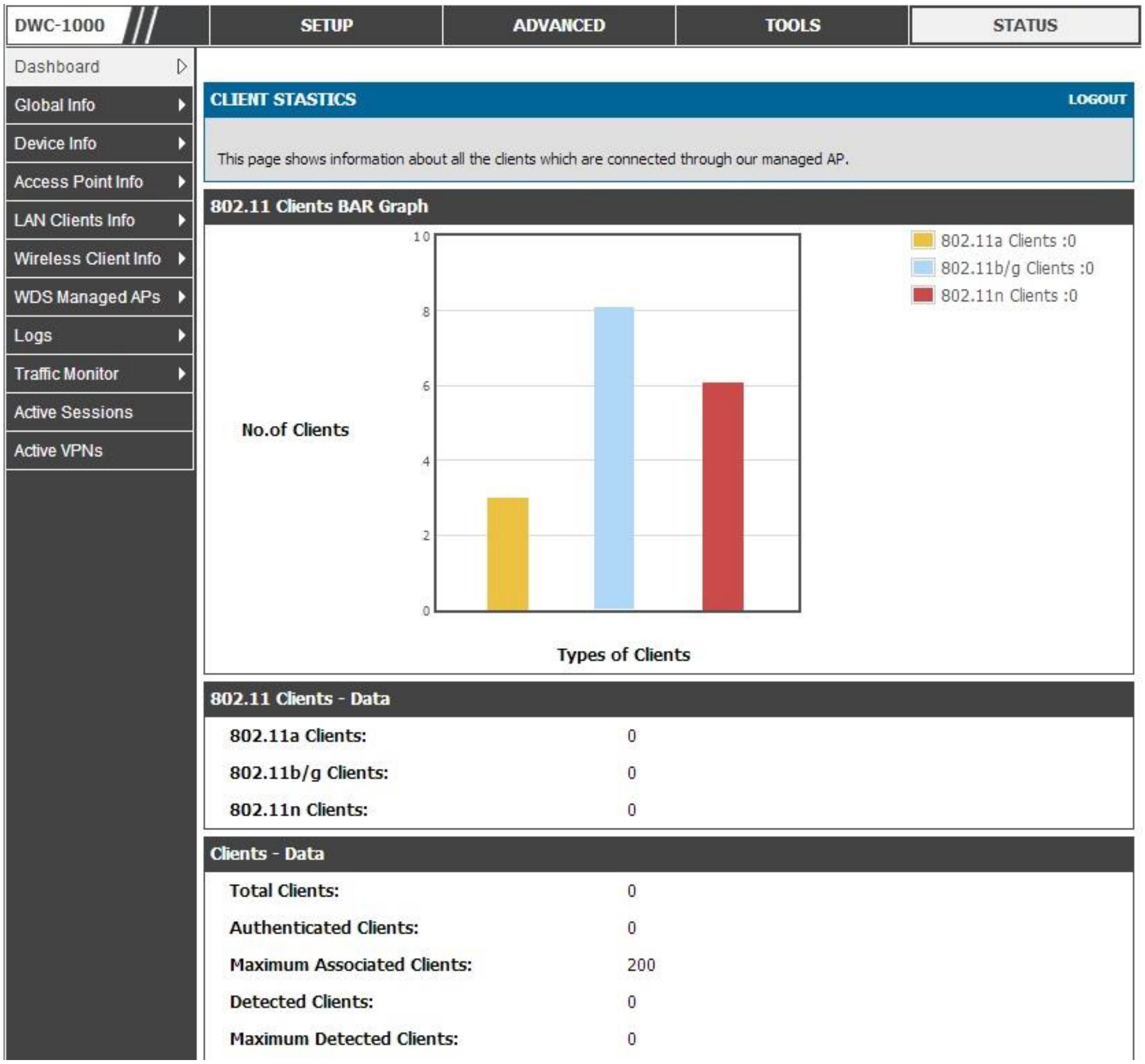
4.8 Wireless Client Status

4.8.1 Client Status

Status > General > Clients

This page shows information about all the clients which are connected through our managed AP.

Figure 79: Client Statistics



CLIENT STASTICS

This page shows information about all the clients which are connected through our managed AP.

802.11 Clients BAR Graph

802.11 Clients - Data

802.11a Clients:	0
802.11b/g Clients:	0
802.11n Clients:	0

Clients - Data

Total Clients:	0
Authenticated Clients:	0
Maximum Associated Clients:	200
Detected Clients:	0
Maximum Detected Clients:	0

802.11 Clients – Data

802.11a Clients: Total number of IEEE 802.11a only clients that are authenticated.

802.11b/g Clients: Total number of IEEE 802.11b/g only clients that are authenticated.
802.11n Clients: Total number of clients that are IEEE 802.11n capable and are authenticated. These include IEEE 802.11a/n, IEEE 802.11b/g/n, 5 GHz IEEE 802.11n, 2.4GHz IEEE 802.11n.

Clients – Data

Total Clients: Total number of clients in the database. This total includes clients with an Associated, Authenticated, or Disassociated status.

Authenticated Clients: Total number of clients in the associated client database with an Authenticated status.

Maximum Associated Clients: Maximum number of clients that can associate with the wireless system. This is the maximum number of entries allowed in the Associated Client database.

Detected Clients: Number of wireless clients detected in the WLAN.

Maximum Detected Clients: Maximum number of clients that can be detected by the controller. The number is limited by the size of the Detected Client Database.

Maximum Pre-authentication History Entries: Maximum number of Client Pre-Authentication events that can be recorded by the system.

Total Pre-authentication History Entries: Current number of pre-authentication history entries in use by the system.

Maximum Roam History Entries: Maximum number of entries that can be recorded in the roam history for all detected clients.

Total Roam History Entries: Current number of pre-authentication history entries in use by the system.

4.8.2 Associated Client Status

Status > Wireless Client Info> Associated Clients > Status

You can view a variety of information about the wireless clients that are associated with the APs the controller manages.

MAC Address: The Ethernet address of the client station. If the MAC address is followed by an asterisk (*), the client is associated with an AP managed by a peer controller.

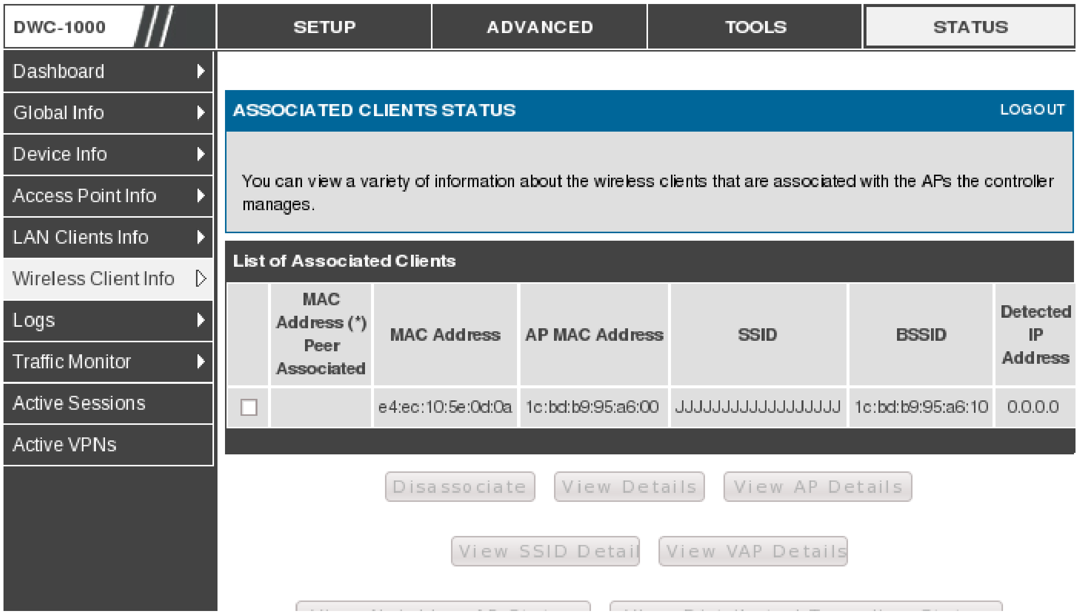
AP MAC Address: The Ethernet address of the AP.

SSID: The network on which the client is connected.

BSSID: The Ethernet MAC address for the managed AP VAP where this client is associated.

Detected IP Address: Identifies the IPv4 address of the client, if available.

Figure 80: Associated Client Status



ASSOCIATED CLIENTS STATUS

You can view a variety of information about the wireless clients that are associated with the APs the controller manages.

List of Associated Clients

	MAC Address (*) Peer Associated	MAC Address	AP MAC Address	SSID	BSSID	Detected IP Address
□		e4:ec:10:5e:0d:0a	1c:bd:b9:95:a6:00	JJJJJJJJJJJJJJJJJJ	1c:bd:b9:95:a6:10	0.0.0.0

The following actions are supported from this page:

Disassociate: Disassociates the selected client from the managed AP.

View Details: Display associated client details.

View AP Details: Display associated AP details.

View SSID Details: Lists the SSIDs of the networks that each wireless client associated with a managed AP has used for WLAN access

View VAP Details: Shows information about the VAPs on the managed AP that have associated wireless clients

View Neighborr AP Status: Shows information about access points that the client detects.

4.8.3 Associated Client SSID Status

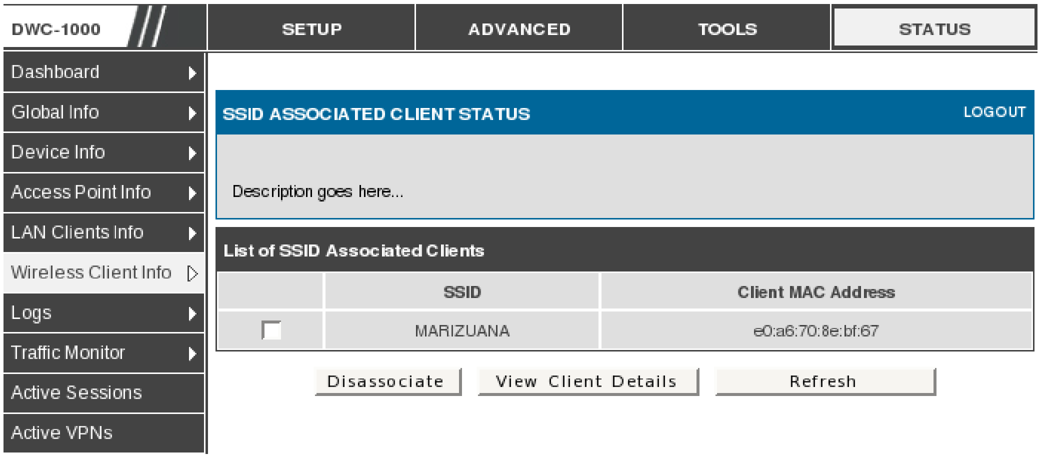
Status > Wireless Client Info> Associated Clients > SSID Status

Each managed AP can have up to 16 different networks that each has a unique SSID. Although several wireless clients might be connected to the same physical AP, they might not connect by using the same SSID

SSID: Indicates the network on which the client is connected.

Client MAC Address: The Ethernet address of the client station.

Figure 81: Associated Client SSID Status



SSID ASSOCIATED CLIENT STATUS

Description goes here...

List of SSID Associated Clients

	SSID	Client MAC Address
□	MARIZUANA	e0:a6:70:8e:bf:67

The following actions are supported from this page:

Disassociate: Disassociates the client from the managed AP.

View Client Details: Display associated client details.

Refresh: Updates the page with the latest information

4.8.4 Associated Client VAP Status

Status > Wireless Client Info> Associated Clients > VAP Status

Each AP has 16 Virtual Access Points (VAPs) per radio, and every VAP has a unique MAC address (BSSID).The VAP Associated Client Status page which shows information about the VAPs on the managed AP that have associated wireless clients. To disconnect a client from an AP, select the box next to the BSSID, and then click Disassociate

BSSID: Indicates the Ethernet MAC address for the managed AP VAP where this client is associated.

SSID: Indicates the SSID for the managed AP VAP where this client is associated.

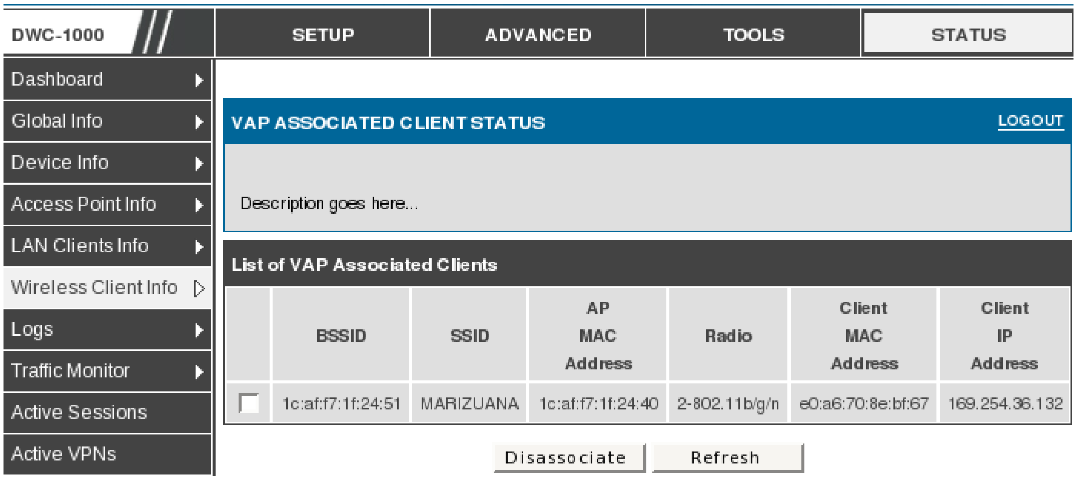
AP MAC Address: This field indicates the base AP Ethernet MAC address for the managed AP.

Radio: Displays the managed AP radio interface the client is associated to and its configured mode.

Client MAC Address: The Ethernet address of the client station.

Client IP Address: The IP address of the client station.

Figure 82: Associated Client VAP Status



VAP ASSOCIATED CLIENT STATUS

Description goes here...

List of VAP Associated Clients

	BSSID	SSID	AP MAC Address	Radio	Client MAC Address	Client IP Address
□	1c:af:f7:1f:24:51	MARIZUANA	1c:af:f7:1f:24:40	2-802.11b/g/n	e0:a6:70:8e:bf:67	169.254.36.132

The following actions are supported from this page:

Disassociate: Disassociates the client from the managed AP.

Refresh: Updates the page with the latest information

4.8.5 Controller Associated Client Status

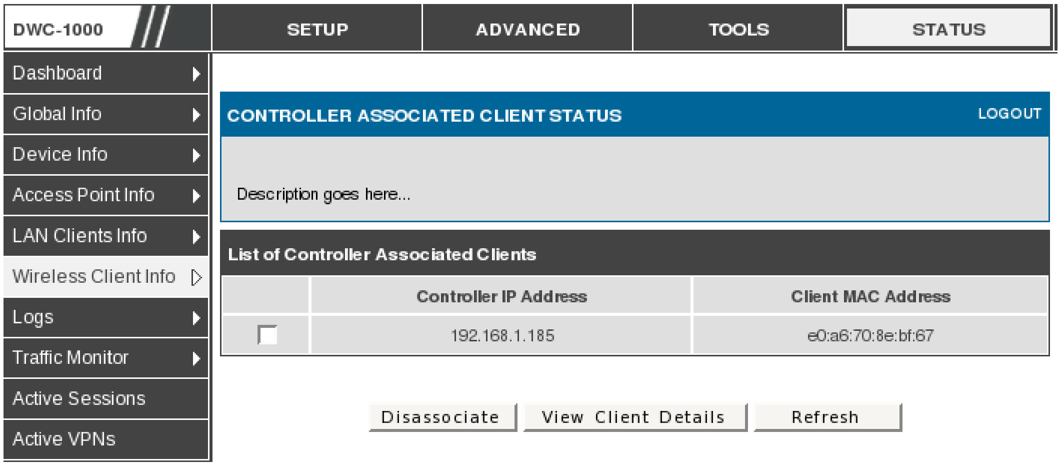
Status > Wireless Client Info> Associated Clients > Controller Status

This shows information about the controller that manages the AP to which the client is associated

Controller IP Address: Shows the IP address of the controller that manages the AP to which the client is associated.

Client MAC Address: Shows the MAC address of the associated client.

Figure 83: Controller Associated Client Status



CONTROLLER ASSOCIATED CLIENT STATUS

Description goes here...

List of Controller Associated Clients

	Controller IP Address	Client MAC Address
□	192.168.1.185	e0:a6:70:8e:bf:67

The following actions are supported from this page:

Disassociate: Disassociates the client from the managed AP.

View Client Details: Display associated client details.

Refresh: Updates the page with the latest information

4.8.6 Detected Client Status

Status > Wireless Client Info> Detected Clients

Wireless clients are detected by the wireless system when the clients either attempt to interact with the system or when the system detects traffic from the clients. The Detected Client Status page contains information about clients that have authenticated with an AP as well information about clients that disassociate and are no longer connected to the system.

MAC Address: The Ethernet address of the client.

Client Name: Shows the name of the client, if available, from the Known Client Database. If client is not in the database then the field is blank.

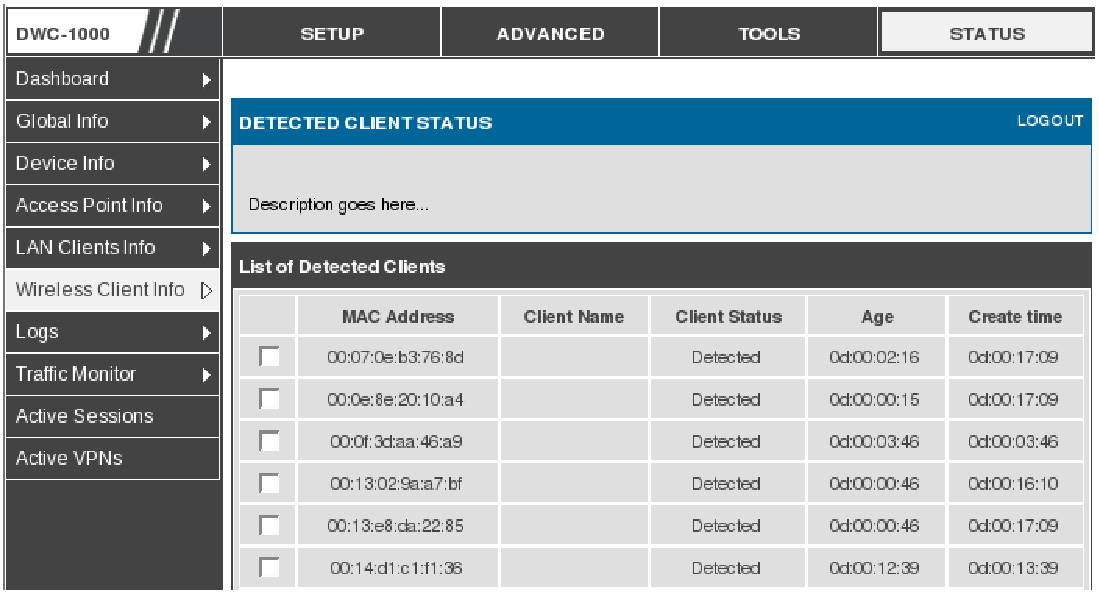
Client Status: Shows the client status, which can be one of the following:

- **Authenticated**: The wireless client is authenticated with the wireless system.
- **Detected**: The wireless client is detected by the wireless system but is not a security threat.
- **Black-Listed**: The client with this MAC address is specifically denied access via MAC Authentication.
- **Rogue**: The client is classified as a threat by one of the threat detection algorithms.

Age: Time since any event has been received for this client that updated the detected client database entry.

Create Time: Time since this entry was first added to the detected client's database.

Figure 84: Detected Client Status



DETECTED CLIENT STATUS

Description goes here...

List of Detected Clients

	MAC Address	Client Name	Client Status	Age	Create time
□	00:07:0e:b3:76:8d		Detected	0d:00:02:16	0d:00:17:09
□	00:0e:8e:20:10:a4		Detected	0d:00:00:15	0d:00:17:09
□	00:0f:3d:aa:46:a9		Detected	0d:00:03:46	0d:00:03:46
□	00:13:02:9a:a7:bf		Detected	0d:00:00:46	0d:00:16:10
□	00:13:e8:da:22:85		Detected	0d:00:00:46	0d:00:17:09
□	00:14:d1:c1:f1:36		Detected	0d:00:12:39	0d:00:13:39

The following actions are supported from this page:

Delete: Delete the selected client from the list. If the client is detected again, it will be added to the list.

Delete All: Deletes all non-authenticated clients from the Detected Client database. As clients are detected, they are added to the database and appear in the list.

Acknowledge All Rogues: Clear the rogue status of all clients listed as rogues in the Detected Client database, The status of an acknowledge client is returned to the status it had when it was first detected. If the detected client fails any of the tests that classify it as a threat, it will be listed as a Rogue again

Refresh: Updates the page with the latest information.

4.8.7 Pre-Authorization History

Status > Wireless Client Info> Pre-Auth History

To help authenticated clients roam without losing sessions and needing to re-authenticate, wireless clients can attempt to authenticate to other APs within range that the client could possibly associate with. For successful pre-authentication, the target AP must have a VAP with an SSID and security configuration that matches that of the client, including MAC authentication, encryption method, and pre-shared key or RADIUS parameters. The AP that the client is associated with captures all pre-authentication requests and sends them to the controller.

MAC Address: MAC address of the client.

AP MAC Address: MAC Address of the managed AP to which the client has pre-authenticated.

Radio Interface Number: Radio number to which the client is authenticated, which is either Radio 1 or Radio 2.

VAP MAC Address: VAP MAC address to which the client roamed.

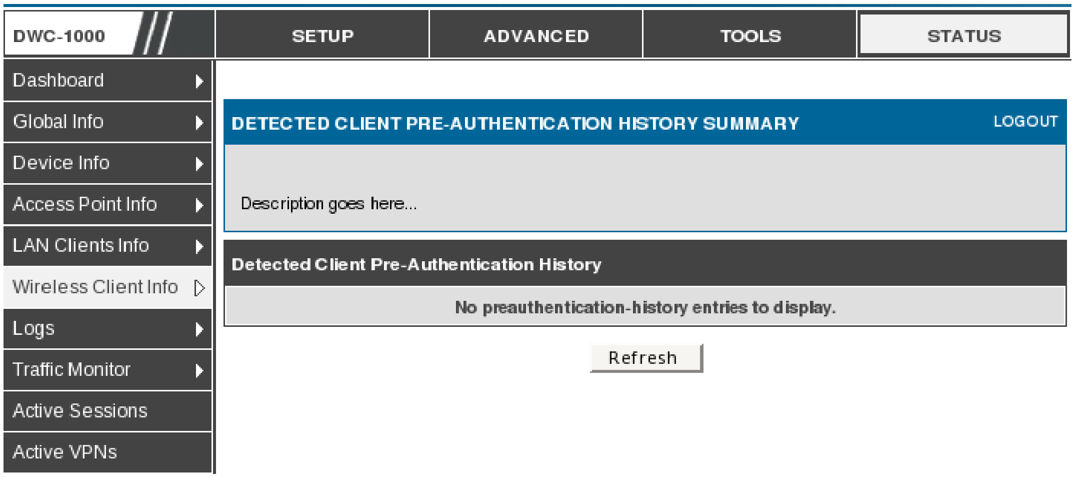
SSID: SSID Name used by the VAP.

Age: Time since the history entry was added.

User Name: Indicates the user name of client that authenticated via 802.1X.

Pre-Authentication Status: Indicates whether the client successfully authenticated and shows a status of Success or Failure.

Figure 85: Pre-Auth History



DETECTED CLIENT PRE-AUTHENTICATION HISTORY SUMMARY

Description goes here...

Detected Client Pre-Authentication History

No preauthentication-history entries to display.

This page includes the following button:

Refresh: Updates the page with the latest information.

4.8.8 Detected Client Roam History

Status > Wireless Client Info> Roam History

The wireless system keeps a record of clients as they roam from one managed AP to another managed AP.

MAC Address: MAC address of the detected client.

AP MAC Address: MAC Address of the managed AP to which the client authenticated.

Radio Interface Number: Radio Number to which the client is authenticated.

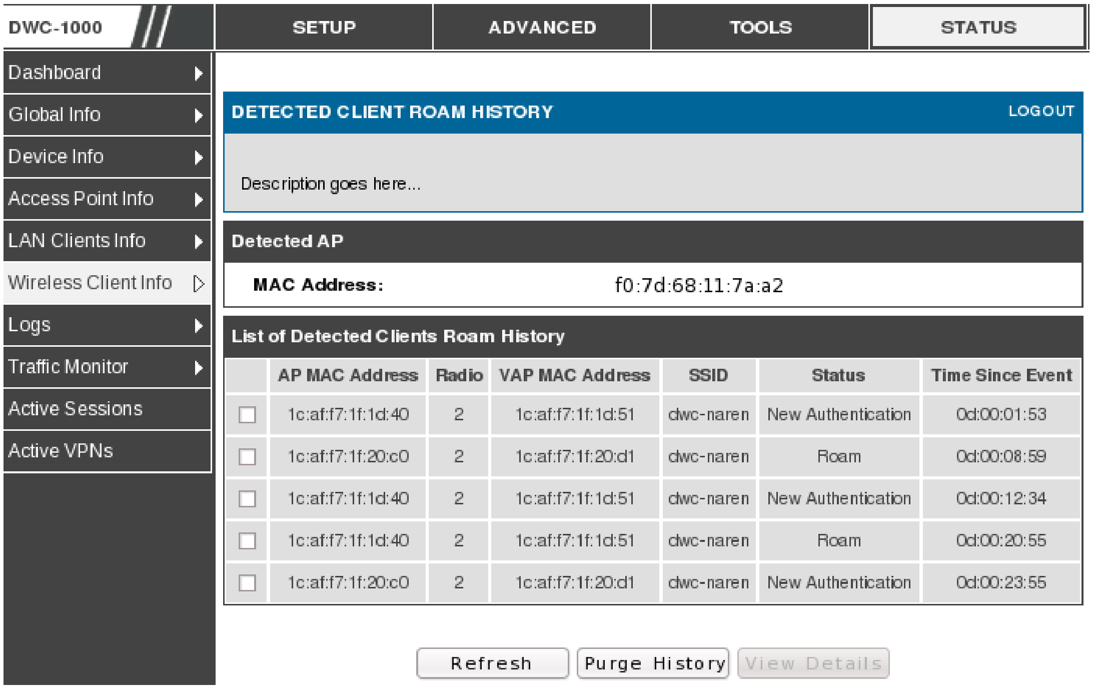
VAP MAC Address: VAP MAC address to which the client roamed.

SSID: Name used by the VAP.

New Authentication: A flag indicating whether the history entry represents a new authentication or a roam event.

Age: Time since the history entry was added.

Figure 86: Detected Client Roam History



DETECTED CLIENT ROAM HISTORY

Description goes here...

Detected AP

MAC Address: f0:7d:68:11:7a:a2

List of Detected Clients Roam History

	AP MAC Address	Radio	VAP MAC Address	SSID	Status	Time Since Event
□	1c:af:f7:1f:1d:40	2	1c:af:f7:1f:1d:51	dwc-naren	New Authentication	0d:00:01:53
□	1c:af:f7:1f:20:c0	2	1c:af:f7:1f:20:d1	dwc-naren	Roam	0d:00:08:59
□	1c:af:f7:1f:1d:40	2	1c:af:f7:1f:1d:51	dwc-naren	New Authentication	0d:00:12:34
□	1c:af:f7:1f:1d:40	2	1c:af:f7:1f:1d:51	dwc-naren	Roam	0d:00:20:55
□	1c:af:f7:1f:20:c0	2	1c:af:f7:1f:20:d1	dwc-naren	New Authentication	0d:00:23:55

This page includes the following button:

Refresh: Updates the page with the latest information.

Purge History: To purge the history when the list of entries is full.

View Details: Shows the details of the detected clients.

Chapter 5. AP Management

The AP Management contains links to the following pages that help you manage and maintain the APs on your DWC-1000 wireless controller network:

- Valid Access Point Configuration
- RF Management
- Access Point Software Download
- Local OUI Database
- AP Provisioning
- Manual Management

5.1 Valid Access Point Configuration

Setup > AP Management > Valid AP

MAC Address This field shows the MAC address of the AP. To change this field, you must delete the entire Valid AP configuration and then enter the correct MAC address from the page that lists all Valid AP's

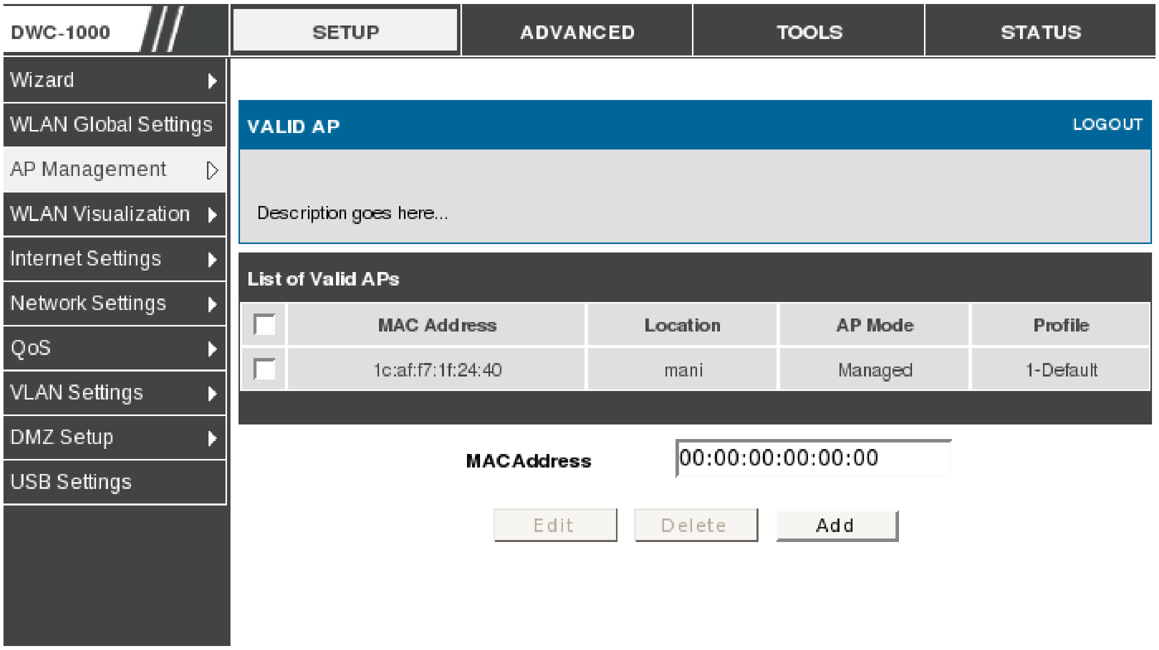
Location: To help you identify the AP, you can enter a location. This field accepts up to 32 alphanumeric characters

AP Mode You can configure the AP to be in one of three modes:

- **Standalone**: The AP acts as an individual access point in the network.
- **Managed**: If an AP is in Managed Mode, the Administrator Web UI and SNMP services on the AP are disabled.
- **Rogue**: Select Rogue as the AP mode if you wish to be notified (through an SNMP trap, if enabled) when this AP is detected in the network.

Profile: If you configure multiple AP Profiles, you can select the profile to assign to this AP

Figure 87: Valid Access Point Configuration



VALID AP

Description goes here...

List of Valid APs

□	MAC Address	Location	AP Mode	Profile
□	1c:af:f7:1f:24:40	mani	Managed	1-Default

MACAddress 00:00:00:00:00:00

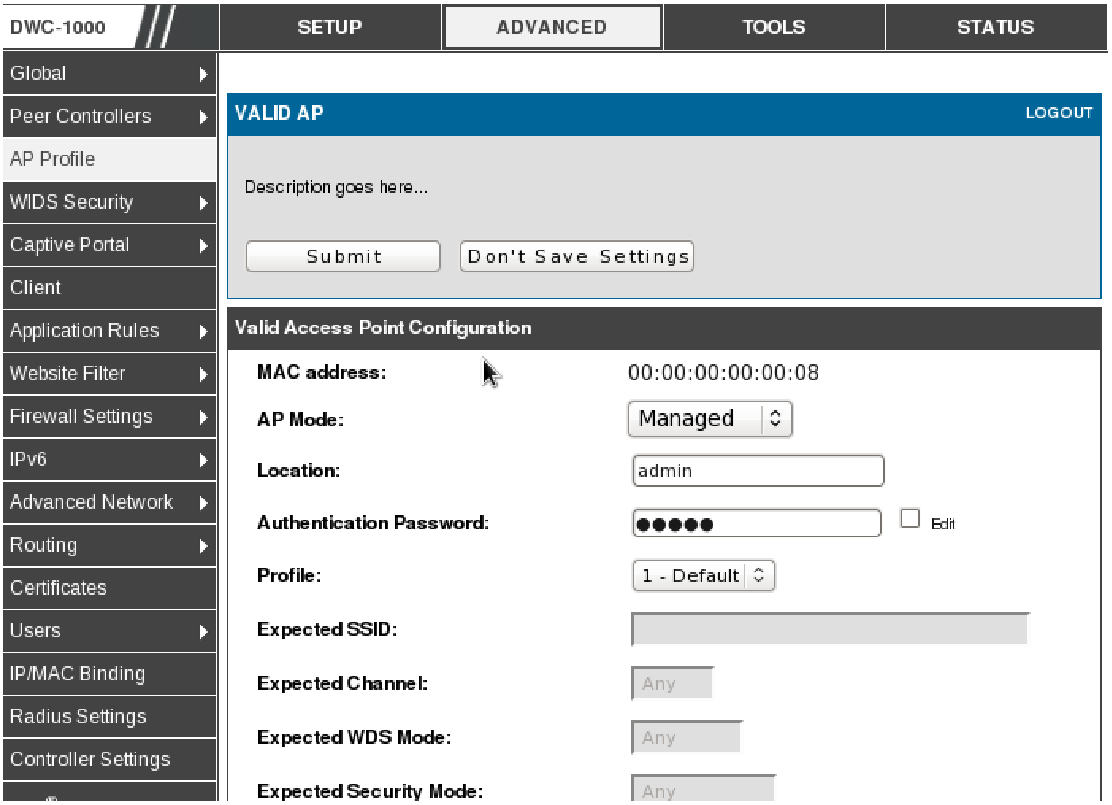
The following actions are supported from this page:

Edit: To edit AP details in Valid AP page.

Delete: To delete a valid AP provide valid MAC address in Valid AP page.

Add: To add an AP in Valid AP page.

Figure 88: Add a Valid Access Point



Description goes here...

Valid Access Point Configuration

MAC address:	00:00:00:00:00:08
AP Mode:	Managed
Location:	admin
Authentication Password:	●●●●● □ Edit
Profile:	1 - Default
Expected SSID:	
Expected Channel:	Any
Expected WDS Mode:	Any
Expected Security Mode:	Any

MAC Address: This field shows the MAC address of the AP. To change this field, you must delete the entire Valid AP configuration and then enter the correct MAC address from the page that lists all Valid APs.

AP Mode: You can configure the AP to be in one of three modes:

- **Standalone**: The AP acts as an individual access point in the network. You do not manage the AP by using the controller. Instead, you log on to the AP itself and manage it by using the Administrator Web User Interface (UI), CLI, or

SNMP. If you select the Standalone mode, the screen refreshes and different fields appear. For Standalone mode the following fields are enabled Expected SSID, Expected Channel, Expected WDS Mode, Expected Security Mode and Expected Wired Network Mode.

- **Managed**: The AP is part of the D-Link Wireless Controller, and you manage it by using the Wireless Controller. If an AP is in Managed Mode, the Administrator Web UI and SNMP services on the AP are disabled.
- **Rogue**: Select Rogue as the AP mode if you wish to be notified (through an SNMP trap, if enabled) when this AP is detected in the network. Additionally, the when this AP is detected through an RF scan, the status is listed as Rogue. If you select the Rogue mode, the screen refreshes, and fields that do not apply to this mode are hidden.

Location: To help you identify the AP, you can enter a location. This field accepts up to 32 alphanumeric characters.

Authentication Password: You can require that the AP authenticate itself with the controller upon discovery. Edit option and enter the password in this field. The valid password range is between 8 and 63 alphanumeric characters. The password in this field must match the password configured on the AP.

Profile: If you configure multiple AP Profiles, you can select the profile to assign to this AP

Expected SSID: Enter the SSID that identifies the wireless network on the standalone AP.

Expected Channel: Select the channel that the standalone AP uses. If the AP is configured to automatically select a channel, or if you do not want to specify a channel, select Any

Expected WDS Mode: Standalone APs can use a Wireless Distribution System (WDS) link to communicate with each other without wires. The menu contains the following options:

- **Bridge**: Select this option if the standalone AP you add to the Valid AP database is configured to use one or more WDS links.
- **Normal**: Select this option if the standalone AP is not configured to use any WDS links.

- **Any**: Select this option if the standalone AP might use a WDS link.

Expected Security Mode: Select the option to specify the type of security the AP uses:

- **Any**: Any security mode
- **Open**: No security
- **WEP**: Static WEP or WEP 802.1X
- **WPA/WPA2**: WPA and/or WPA2 (Personal or Enterprise)

Expected Wired Network Mode: If the standalone AP is allowed on the wired network, select Allowed. If the AP is not permitted on the wired network, select Not Allowed

Channel: The Channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The range of channels and the default channel are determined by the Mode of the radio interface and the country in which the APs operate.

Power: The power level affects how far an AP broadcasts its RF signal. If the po wer level is too low, wireless clients will not detect the signal or experience poor WLAN performance. If the power level is too high, the RF signal might interfere with other APs within range.

5.2 RF Management

5.2.1 RF Configuration

Setup > AP Management > RF Management > RF Configuration

The radio frequency (RF) broadcast channel defines the portion of the radio spectrum that the radio on the access point uses for transmitting and receiving. The range of available channels for an access point is determined by the IEEE 802.11 mode (also referred to as band) of the access point.

The controller contains a channel plan algorithm that automatically determines which RF channels each AP should use to minimize RF interference. When you enable the channel plan algorithm, the controller periodically evaluates the operational channel on every AP it manages and changes the channel if the current channel is noisy

Channel Plan: Each AP is dual-band capable of operating in the 2.4 GHz and 5 GHz frequencies. The 802.11a/n and 802.11b/g/n modes use different channel plans. Before you configure channel plan settings, select the mode to configure.

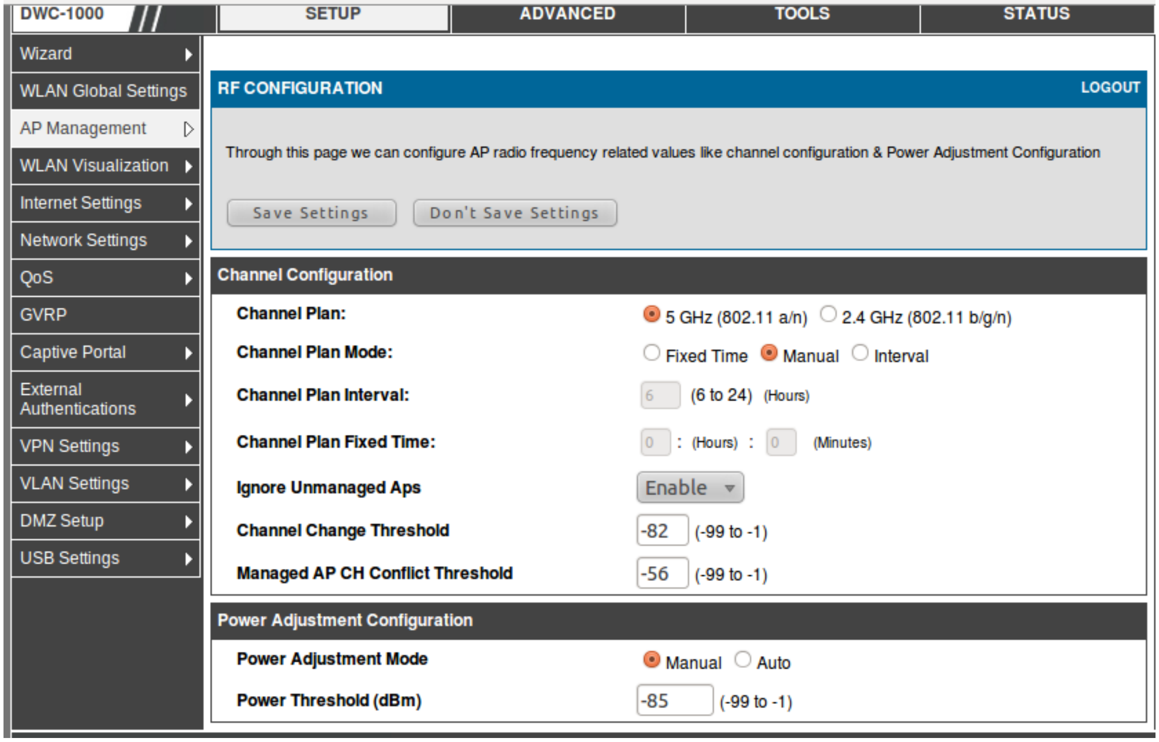
Channel Plan Mode: This field indicates the channel assignment mode. The mode of channel plan assignment can be one of the following:

- **Fixed Time**: If you select the fixed time channel plan mode, you specify the time for the channel plan and channel assignment. In this mode the plan is applied once every 24 hours at the specified time.
- **Manual**: With the manual channel plan mode, you control and initiate the calculation and assignment of the channel plan. You must manually run the channel plan algorithm and apply the channel plan to the APs.
- **Interval**: In the interval channel plan mode, the controller periodically calculates and applies the channel plan. You can configure the interval to be from every 6 to every 24 hours. The interval period begins when you click Submit.

Channel Plan Interval: If you select the Interval channel plan mode, you can specify the frequency at which the channel plan calculation and assignment occurs. The interval time is in hours, and you can specify an interval that ranges between every 6 hours to every 24 hours.

Channel Plan Fixed Time: If you select the Fixed Time channel plan mode, you can specify the time at which the channel plan calculation and assignment occurs. The channel plan calculation will occur once every 24 hours at the time you specify.

Figure 89: RF configuration



RF CONFIGURATION

Through this page we can configure AP radio frequency related values like channel configuration & Power Adjustment Configuration

Channel Configuration

Channel Plan: ● 5 GHz (802.11 a/n) ○ 2.4 GHz (802.11 b/g/n)

Channel Plan Mode: ○ Fixed Time ● Manual ○ Interval

Channel Plan Interval: 6 (6 to 24) (Hours)

Channel Plan Fixed Time: 0 : (Hours) : 0 (Minutes)

Ignore Unmanaged Aps: Enable

Channel Change Threshold: -82 (-99 to -1)

Managed AP CH Conflict Threshold: -56 (-99 to -1)

Power Adjustment Configuration

Power Adjustment Mode: ● Manual ○ Auto

Power Threshold (dBm): -85 (-99 to -1)

Ignore Unmanaged APs: Enable this option to exclude unmanaged APs from the channel plan configuration settings from this section.

Channel Change Threshold: This is the threshold strength, in dBm, for neighbor to be considered "noisy". If this threshold is exceeded the Channel Plan will be run.

Managed AP CH Conflict Threshold: This is the threshold, in dBm, below which managed APs that have a conflicting channel compared to the Channel Plan will have their channel updated.

Power Adjustment Mode: You can set the power of the AP radio frequency transmission in the AP profile, the local database or in the RADIUS server. The power level in the AP profile is the default level for the AP, and the power will not be adjusted below the value in the AP profile. The settings in the local database and RADIUS server always override power set in the profile setting. If you manually set the power, the level is fixed and the AP will not use the automatic power adjustment algorithm. You can configure the power as a percentage of maximum power, where the maximum power is the minimum of power level allowed for the channel by the regulatory domain or the hardware capability.

- **Manual**: In this mode, you run the proposed power adjustments manually from the Manual Power Adjustments page.
- **Auto:** In this mode, the controller periodically calculates the power adjustments and applies the power for all APs automatically

Power Threshold (dBm): The threshold, in dBm, below which Power Adjustment Mode takes effect.

✍ This setting gets applied to both radios of the AP.

The following actions are supported from this page:

Submit: Updates the controller with the values you enter.

5.2.2 Channel Plan History

Setup > AP Management > RF Management > Channel Plan History

The wireless controller stores channel assignment information for the APs it manages. The Cluster Controller that controls the cluster maintains the channel history information for all controllers in the cluster. On the Cluster Controller, the page shows information about the radios on all APs managed by controllers in the cluster that are eligible for channel assignment and were successfully assigned a new channel.

Channel Plan: The 5 GHz and 2.4 GHz radios use different channel plans, so the controller tracks the channel history separately for each radio. The channel information that displays on the page is only for the radio you select.

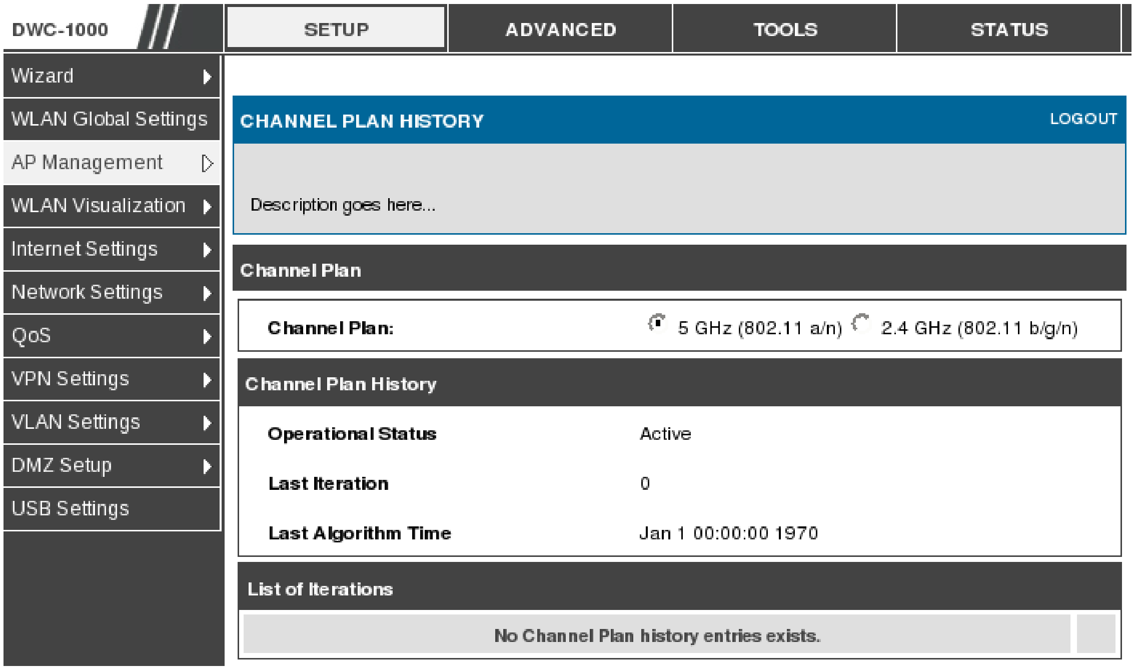
Operational Status: This field shows whether the controller is using the automatic channel adjustment algorithm on the AP radios.

Last Iteration: The number in this field indicates the most recent iteration of channel plan adjustments. The APs that received a channel adjustment in previous iterations cannot be assigned new channels in the next iteration to prevent the same APs from being changed time after time.

Last Algorithm Time: Shows the date and time when the channel plan algorithm last ran.

AP MAC Address: This table displays the channel assigned to an AP in an iteration of the channel plan (Location, Radio,Iteration, Channel)

Figure 90: Channel Plan History



CHANNEL PLAN HISTORY

Description goes here...

Channel Plan

Channel Plan: ● 5 GHz (802.11 a/n) ○ 2.4 GHz (802.11 b/g/n)

Channel Plan History

Operational Status	Active
Last Iteration	0
Last Algorithm Time	Jan 1 00:00:00 1970

List of Iterations

No Channel Plan history entries exists.

5.2.3 Manual Channel Plan

Setup > AP Management > RF Management > Manual Channel Plan

If you specify Manual as the Channel Plan Mode on the Configuration tab, the Manual Channel Plan page allows you to initiate the channel plan algorithm. To manually run the channel plan adjustment feature, select the radio to update the channels on (5 GHz or 2.4 GHz) and click Start.

Channel Plan: The 5 GHz and 2.4 GHz radios use different channel plans, so the controller tracks the channel history separately for each radio. The channel information that displays on the page is only for the radio you select.

Channel plan algorithm (Current Status): Shows the Current Status of the plan, which is one of the following states:

- **None**: The channel plan algorithm has not been manually run since the last controller reboot.
- **Algorithm in Progress**: The channel plan algorithm is running.
- **Algorithm Complete**: The channel plan algorithm has finished running.

A table displays to indicate proposed channel assignments. Each entry shows the AP along with the current and new channel. To accept the proposed channel change, click Apply. You must manually apply the channel plan for the proposed assignments to be applied.

- **Apply In Progress**: The controller is applying the proposed channel plan and adjusting the channel on the APs listed in the table.
- **Apply Complete**: The algorithm and channel adjustment are complete

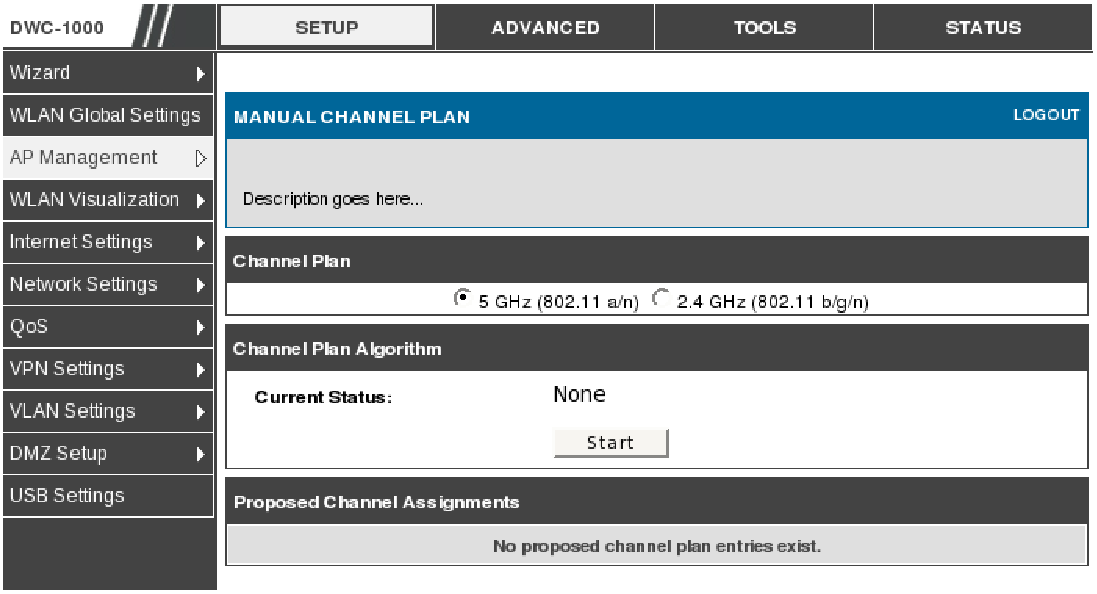
Proposed Channel Assignments: If no APs appear in the table after the algorithm is complete, the algorithm does not recommend any channel changes.

- **Current Channel**: Shows the current operating channel for the AP that the algorithm recommends for new channel assignments.
- **New Channel**: Shows the proposed operating channel for the AP.

The following actions are supported from this page:

Start: To initiate the channel plan algorithm

Figure 91: Manual Channel Plan



MANUAL CHANNEL PLAN

Description goes here...

Channel Plan

● 5 GHz (802.11 a/n) ○ 2.4 GHz (802.11 b/g/n)

Channel Plan Algorithm

Current Status: None

Proposed Channel Assignments

No proposed channel plan entries exist.

5.2.4 Manual Power Adjustment Plan

Setup > AP Management > RF Management > Manual Power Adjustment Plan

If you select Manual as the Power Adjustment Mode on the Configuration tab, you can manually initiate the power adjustment algorithm on the Manual Power Adjustments page.

Current Status: Shows the Current Status of the plan, which is one of the

following states:

- **None**: The power adjustment algorithm has not been manually run since the last controller reboot.
- **Algorithm In Progress**: The power adjustment algorithm is running.
- **Algorithm Complete**: The power adjustment algorithm has finished running.
- A table displays to indicate proposed power adjustments. Each entry shows the AP along with the current and new power levels.
- **Apply In Progress**: The controller is adjusting the power levels that the APs use.
- **Apply Complete**: The algorithm and power adjustment are complete. AP MAC Address Identifies the

AP MAC address: Identifies the AP MAC address.

Location: Identifies the location of the AP, which is set in the Valid AP database.

Radio Interface: Identifies the radio.

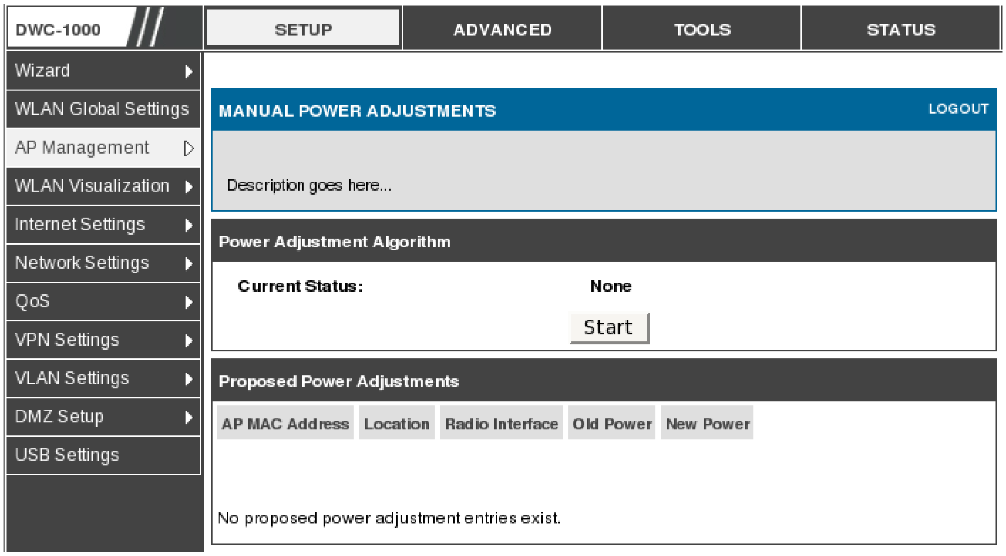
Old Power: Shows the earlier power level for the AP.

New Power: Shows the proposed power level for the AP.

The following actions are supported from this page:

Start: To initiate the power adjustment algorithm.

Figure 92: Manual Power Adjustment Plan



Description goes here...

Power Adjustment Algorithm

Current Status: None

Proposed Power Adjustments

AP MAC Address	Location	Radio Interface	Old Power	New Power

No proposed power adjustment entries exist.

5.3 Access Point Software Download

Setup > AP Management > Software Download

The wireless controller can upgrade software on the APs that it manages.

✍ The AP firmware version must as same as DWC-1000 WLAN module version

Server Address: Enter the IP address of the host where the upgrade file is located. The host must have a TFTP server installed and running.

File Path: Enter the file path on the TFTP server where the software is located. You may enter up to 96 characters.

File Name: Enter the name of the upgrade file. You may enter up to 32 characters, and the file extension .tar must be included.

Group Size: When you upgrade multiple APs, each AP contacts the TFTP server to download the upgrade file. To prevent the TFTP server from being overloaded, you can limit the number of APs to be upgraded at a time. In the Group Size field, enter the number of APs that can be upgraded at the same time. When one group completes the upgrade, the next group begins the process

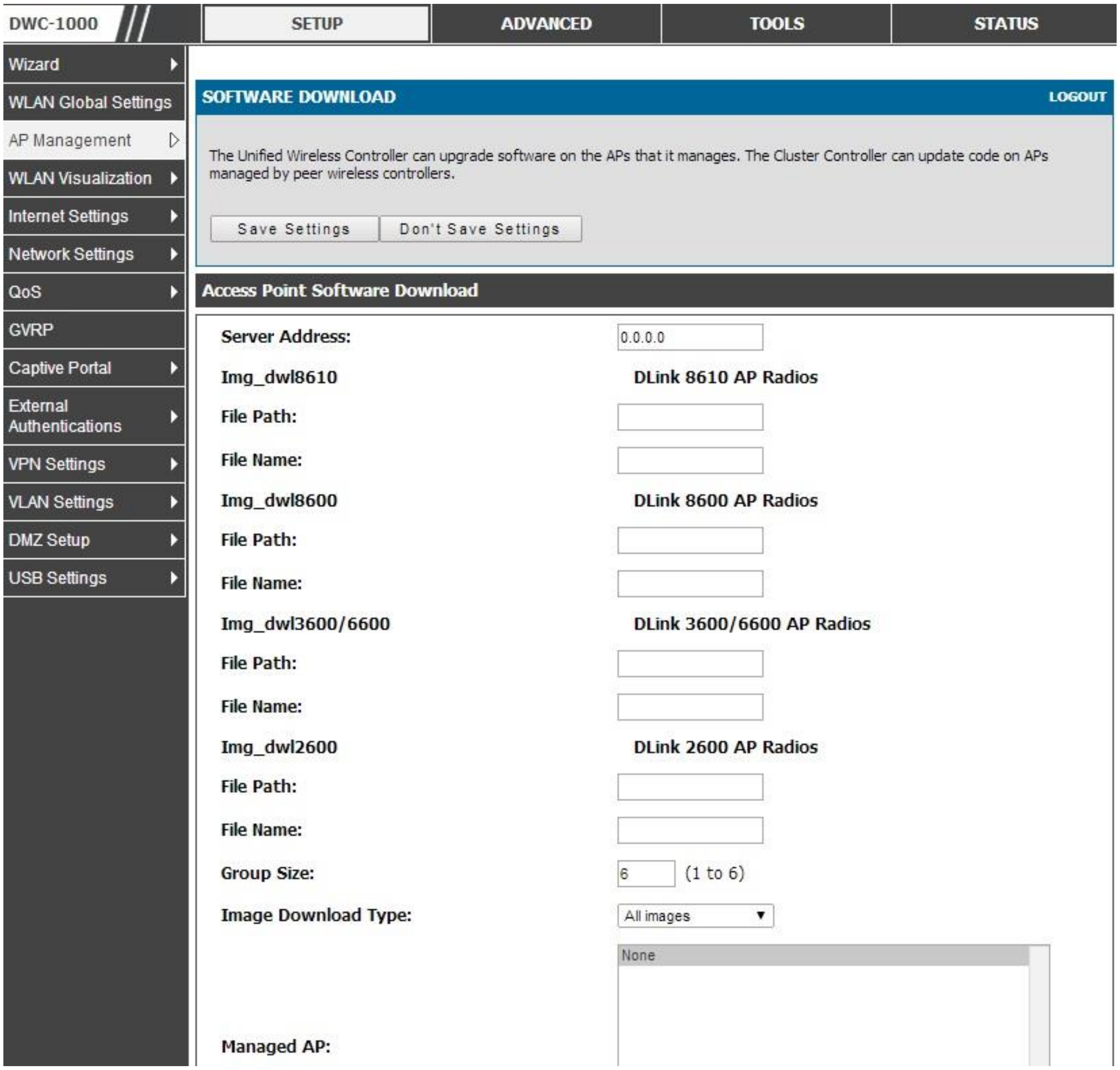
Image Download Type: Type of the image to be downloaded, which can be one of the following:

- All images (img_dwl8600, img_dwl3600/6600 and img_dwl8610)
- img_dwl8600
- img_dwl3600/6600
- img_dwl2600
- img_dwl8610

✍ To download all images, make sure you specify the file path and file name for both images in the appropriate File Path and File Name fields.

Managed AP: The list shows all the APs that the controller manages. If the controller is the Cluster Controller, then the list shows the APs managed by all controllers in the cluster. Each AP is identified by its MAC address, IP address, and Location in the <MAC - IP - Location> format. To upgrade a single AP, select the AP MAC address from the drop down list. To upgrade all APs, select All from the top of the list. If All is selected, the Group Size field will limit the number of simultaneous AP upgrades in order not to overwhelm the TFTP server

Figure 93: Access Point Software Download



SOFTWARE DOWNLOAD

The Unified Wireless Controller can upgrade software on the APs that it manages. The Cluster Controller can update code on APs managed by peer wireless controllers.

Access Point Software Download

Server Address:	0.0.0.0
Img_dwl8610	DLink 8610 AP Radios
File Path:	
File Name:	
Img_dwl8600	DLink 8600 AP Radios
File Path:	
File Name:	
Img_dwl3600/6600	DLink 3600/6600 AP Radios
File Path:	
File Name:	
Img_dwl2600	DLink 2600 AP Radios
File Path:	
File Name:	
Group Size:	6 (1 to 6)
Image Download Type:	All images
Managed AP:	None

5.4 Local OUI Database Summary

Setup > AP Management > Local OUI Database

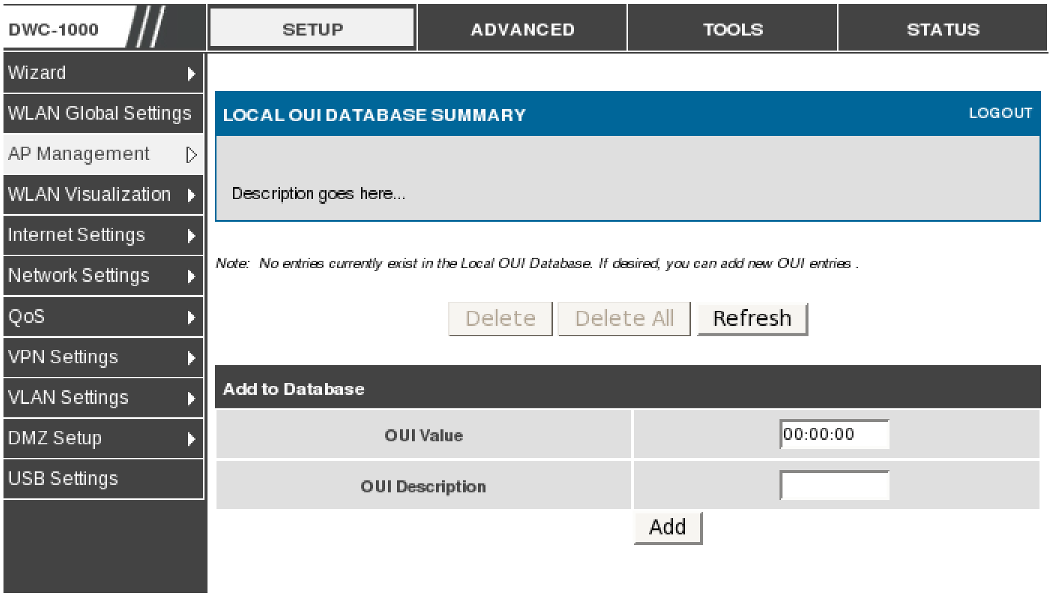
To help identify AP and Wireless Client adapter manufacturers detected in the wireless network, the wireless controller contains a database of registered Organizationally Unique Identifiers (OUIs). This is a read-only list with over 10,000 registrations. From the Local OUI Database Summary page, you can enter up to 64 user-defined OUIs. The local list is searched first, so the same OUI can be located in the local list as well as the read-only list.

OUI Value: Enter the OUI that represents the company ID in the format XX:XX:XX where XX is a hexadecimal number between 00 and FF. The first three bytes of the MAC address represents the company ID assignment.

> ✍ The first byte of the OUI must have the least significant bit set to 0. For example 02:FF:FF is a valid OUI, but 03:FF:FF is not.

OUI Description: Enter the organization name associated with the OUI. The name can be up to 32alphanumeric characters..

Figure 94: Local OUI Database



Description goes here...

Note: No entries currently exist in the Local OUI Database. If desired, you can add new OUI entries .

OUI Value	00:00:00
OUI Description	

5.5 AP Provisioning Summary

Setup > AP Management > AP Provisioning Summary Status

The AP Provisioning feature helps you add new APs to an existing controller cluster. With AP Provisioning, you can configure the access points with parameters that are needed to connect to the wireless network. Use AP Provisioning to connect devices to a network enabled for mutual authentication. If a network is not enabled for mutual authentication then APs can be attached to the network by properly configuring the local Valid AP database or RADIUS AP database and discovery options. The provisioning feature can optionally be used on networks not enabled for mutual authentication to simplify AP attachment to the cluster.

MAC Address: MAC address of the AP

IP Address: IP Address of the AP.

Primary IP Address: The IP address of the primary provisioned controller as reported by the AP.

Backup IP Address: The IP address of the backup provisioned controller as reported by the AP.

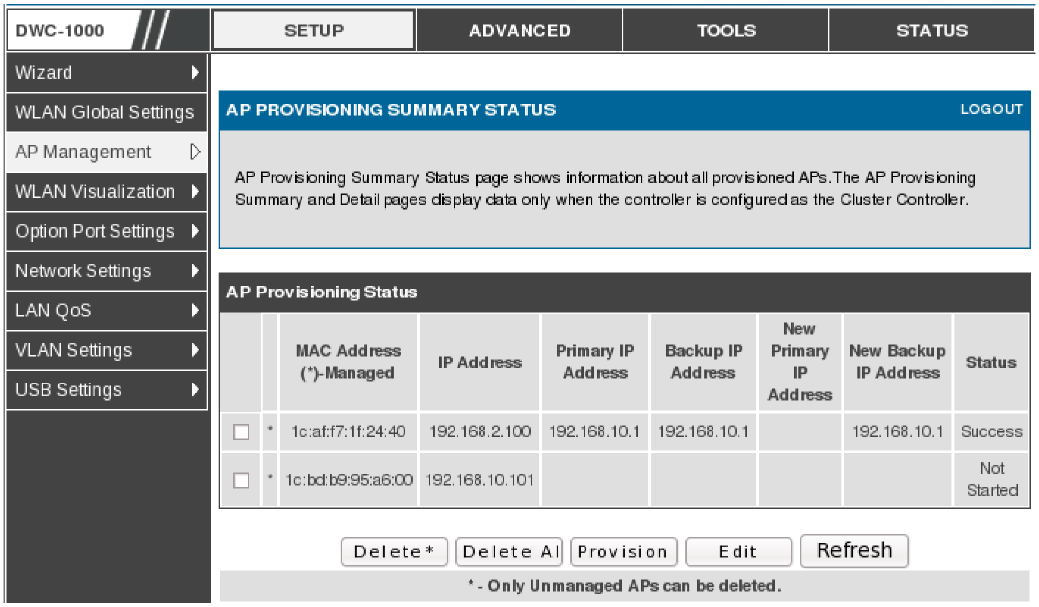
New Primary IP Address: Enter the IP address of primary controller to which the AP should try to connect.

New Backup IP Address: Enter the IP address of controller to which the AP should try to connect if it is unable to connect to the primary controller.

Status: Status of the most recently issued AP provisioning command, which has one of the following values:

- **Not Started**: Provisioning has not been started for this AP.
- **Success**: Provisioning finished successfully for this controller. The AP Provisioning Status table should reflect the latest provisioning configuration.
- **In Progress**: Provisioning is in progress for this AP.
- **Invalid Controller IP Address**: Either primary or backup controller IP address is not in the cluster or the mutual authentication mode is enabled and the primary controller IP address is not specified.
- **Provisioning Rejected**: AP is not managed and is configured not to accept provisioning data in unmanaged mode.
- **Timed Out**: The last provisioning request timed out.

Figure 95: AP Provisioning Summary Status



AP PROVISIONING SUMMARY STATUS

AP Provisioning Summary Status page shows information about all provisioned APs.The AP Provisioning Summary and Detail pages display data only when the controller is configured as the Cluster Controller.

AP Provisioning Status

		MAC Address (*)-Managed	IP Address	Primary IP Address	Backup IP Address	New Primary IP Address	New Backup IP Address	Status
□	*	1c:af:f7:1f:24:40	192.168.2.100	192.168.10.1	192.168.10.1		192.168.10.1	Success
□	*	1c:bd:b9:95:a6:00	192.168.10.101					Not Started

* - Only Unmanaged APs can be deleted.

The following actions are supported from this page:

Delete: Remove the selected AP from the AP provisioning list.

Delete All: Remove all APs from the AP provisioning list.

Provision: Initiate provisioning for the selected AP. You can provision an AP only from the cluster controller. After the AP is provisioned, it should become managed by the controller with the configured Primary IP Address and appear in the AP provisioning database as a managed AP.

Edit: Edit the parameters of selected AP from the AP provisioning list

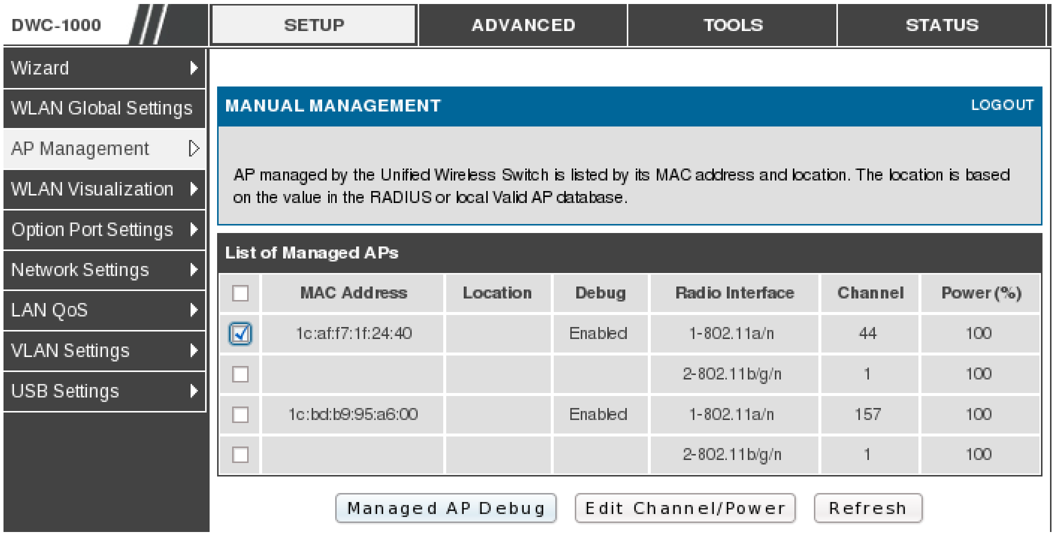
Refresh: Updates the page with the latest information

5.6 Manual Management

Setup > AP Management > Manual Management

When the AP is in Managed mode, remote access to the AP is disabled. From the Manual Management page, you can also manually change the RF channel and power for each radio on an AP. The manual power and channel changes override the settings configured in the AP profile (including automatic channel selection) and take effect immediately. The manual channel and power assignments are not retained when the AP is reset or if the profile is reapplied to the AP, such as when the AP disassociates and re-associates with the controller.

Figure 96: Manual Management



MANUAL MANAGEMENT

AP managed by the Unified Wireless Switch is listed by its MAC address and location. The location is based on the value in the RADIUS or local Valid AP database.

List of Managed APs

□	MAC Address	Location	Debug	Radio Interface	Channel	Power (%)
☑	1c:af:f7:1f:24:40		Enabled	1-802.11a/n	44	100
□				2-802.11b/g/n	1	100
□	1c:bd:b9:95:a6:00		Enabled	1-802.11a/n	157	100
□				2-802.11b/g/n	1	100

MAC Address: Shows the MAC address of the AP.

Location: Shows the AP location, which is based on the value configured in the RADIUS or local Valid AP database.

Debug: To help you troubleshoot, you can enable Telnet access to the AP so that you can debug the device from the CLI. The Debug field shows the debug status and can be one of the following:

- Disabled
- Set Requested
- Set in Progress
- Enabled

To change the status, select the AP and click the Managed AP Debug button.

Radio Interface: Identifies the radio to which the channel and power settings apply.

Channel: Select the AP and click the Edit Channel/Power button to access the Managed AP Channel/Power Adjust page. From that page, you can set a new channel for Radio 1 or Radio 2. The available channels depend on the radio mode and country in which the APs operate. The manual channel change overrides the channel configured in the AP profile and is not retained when the AP reboots or when the AP profile is reapplied.

Power: Select the AP and click the Edit Channel/Power button to access the Managed AP Channel/Power Adjust page. From that page, you can set a new power level for the AP. The manual power change overrides the power setting configured in the AP profile and is not retained when the AP reboots or when the AP profile is reapplied

Chapter 6. Connecting to the Internet: Option Setup

This controller has two Option ports that can be used to establish a connection to the internet. The following ISP connection types are supported: DHCP, Static, PPPoE, PPTP, L2TP.

It is assumed that you have arranged for internet service with your Internet Service Provider (ISP). Please contact your ISP or network administrator for the configuration information that will be required to setup the controller.

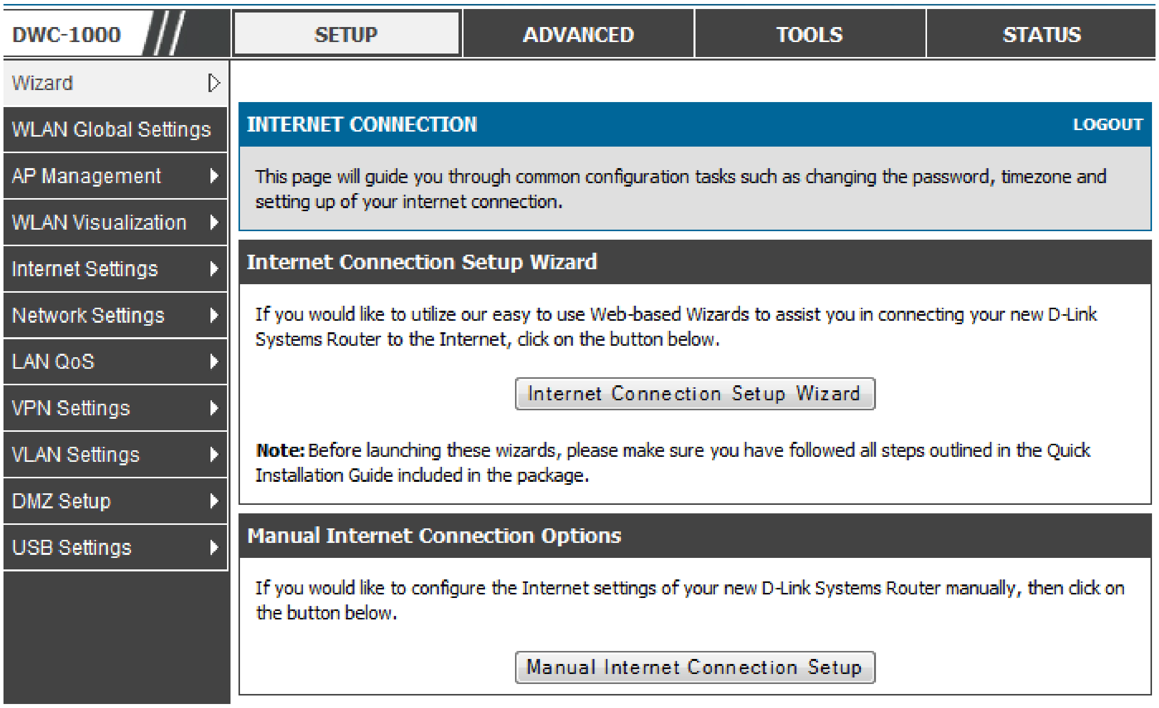
> ✍ The ISP Connection types: PPPoE, PPTP, L2TP, NAT/Transparent mode feature are available upon licensed activation of VPN / Firewall features for the system.

6.1 Internet Connection Setup Wizard

Setup > Wizard > Internet

The Internet Connection Setup Wizard is available for users new to networking. By going through a few straightforward configuration pages you can take the information provided by your ISP to get your Option connection up and enable internet access for your network.

Figure 97: Internet Connection Setup Wizard



This page will guide you through common configuration tasks such as changing the password, timezone and setting up of your internet connection.

If you would like to utilize our easy to use Web-based Wizards to assist you in connecting your new D-Link Systems Router to the Internet, click on the button below.

Note: Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

If you would like to configure the Internet settings of your new D-Link Systems Router manually, then click on the button below.

You can start using the Wizard by logging in with the administrator password for the controller. Once authenticated set the time zone that you are located in, and then choose the type of internet connection type: DHCP, Static, PPPoE, PPTP, L2TP. Depending on the connection type a username/password may be required to register this controller with the ISP. In most cases the default settings can be used if the ISP did not specify that parameter. The last step in the Wizard is to click the Connect button, which confirms the settings by establishing a link with the ISP. Once connected, you can move on and configure other features in this controller.

6.2 Option Configuration

Setup > Internet Settings > Option1 Settings > Option1 Setup

You must either allow the controller to detect Option connection type automatically or configure manually the following basic settings to enable Internet connectivity:

Connection type: Based on the ISP you have selected for the primary Option link for this controller, choose Static IP address, DHCP client, Point-to-Point Tunneling Protocol (PPTP), Point-to-Point Protocol over Ethernet (PPPoE), Layer 2 Tunneling Protocol

(L2TP). Required fields for the selected ISP type become highlighted. Enter the following information as needed and as provided by your ISP:

PPPoE Profile Name. This menu lists configured PPPoE profiles, particularly useful when configuring multiple PPPoE connections (i.e. for Japan ISPs that have multiple PPPoE support).

ISP login information. This is required for PPTP and L2TP ISPs.

- User Name
- Password
- Secret (required for L2TP only)

MPPE Encryption: For PPTP links, your ISP may require you to enable Microsoft Point-to-Point Encryption (MPPE).

Split Tunnel (supported for PPTP and L2TP connection). This setting allows your LAN hosts to access internet sites over this Option link while still permitting VPN traffic to be directed to a VPN configured on this Option port.

> ✍ If split tunnel is enabled, DWC won’t expect a default route from the ISP server. In such case, user has to take care of routing manually by configuring the routing from Static Routing page.

To keep the connection always on, click **Keep Connected**. To log out after the connection is idle for a period of time (useful if your ISP costs are based on logon times), click Idle Timeout and enter the time, in minutes, to wait before disconnecting in the Idle Time field.

6.2.1 Option Port IP address

Your ISP assigns you an IP address that is either dynamic (newly generated each time you log in) or static (permanent). The IP Address Source option allows you to define whether the address is statically provided by the ISP or should be received dynamically at each login. If static, enter your IP address, IPv4 subnet mask, and the ISP gateway’s IP address. PPTP and L2TP ISPs also can provide a static IP address and subnet to configure, however the default is to receive that information dynamically from the ISP.

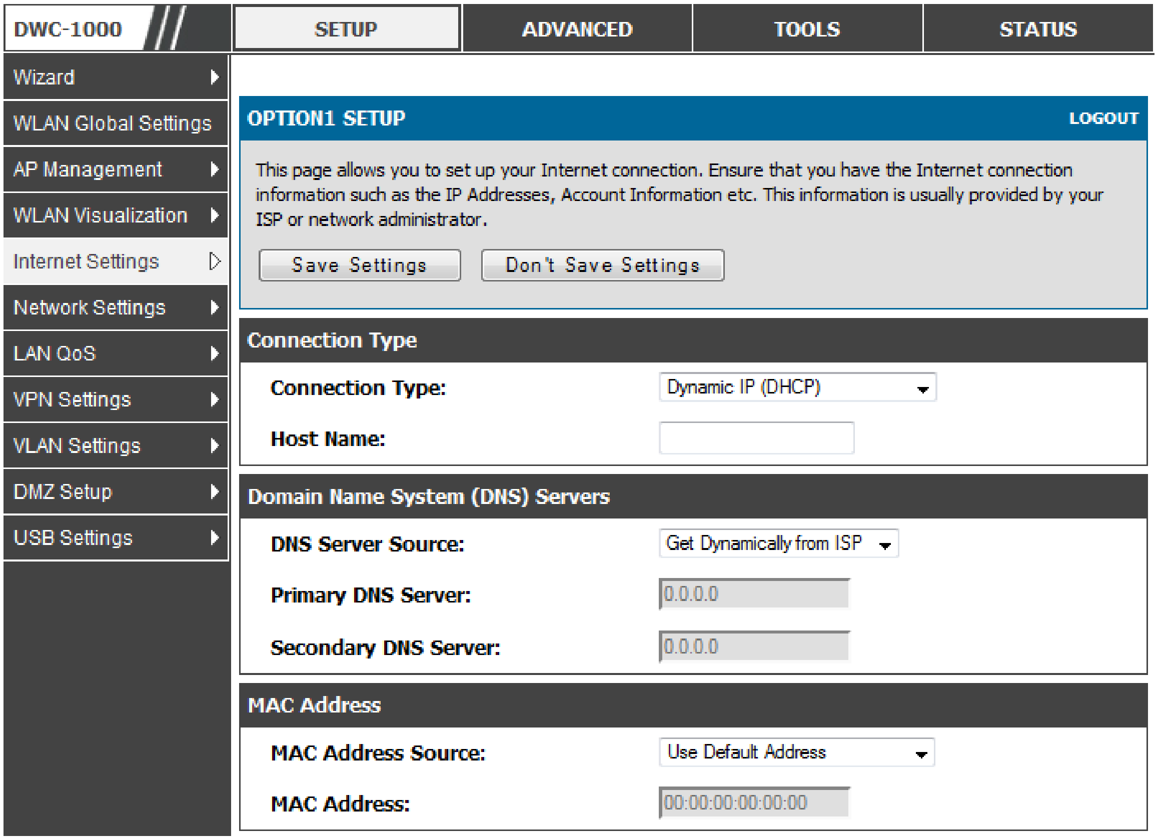
6.2.2 Option DNS Servers

The IP Addresses of Option Domain Name Servers (DNS) are typically provided dynamically from the ISP but in some cases you can define the static IP addresses of the DNS servers. DNS servers map Internet domain names (example: www.google.com) to IP addresses. Click to indicate whether to get DNS server addresses automatically from your ISP or to use ISP-specified addresses. If its latter, enter addresses for the primary and secondary DNS servers. To avoid connectivity problems, ensure that you enter the addresses correctly.

6.2.3 DHCP Option

For DHCP client connections, you can choose the MAC address of the controller to register with the ISP. In some cases you may need to clone the LAN host’s MAC address if the ISP is registered with that LAN host.

Figure 98: Manual Option1 configuration



This page allows you to set up your Internet connection. Ensure that you have the Internet connection information such as the IP Addresses, Account Information etc. This information is usually provided by your ISP or network administrator.

Connection Type

Connection Type: Dynamic IP (DHCP)

Host Name:

Domain Name System (DNS) Servers

DNS Server Source: Get Dynamically from ISP

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

MAC Address

MAC Address Source: Use Default Address

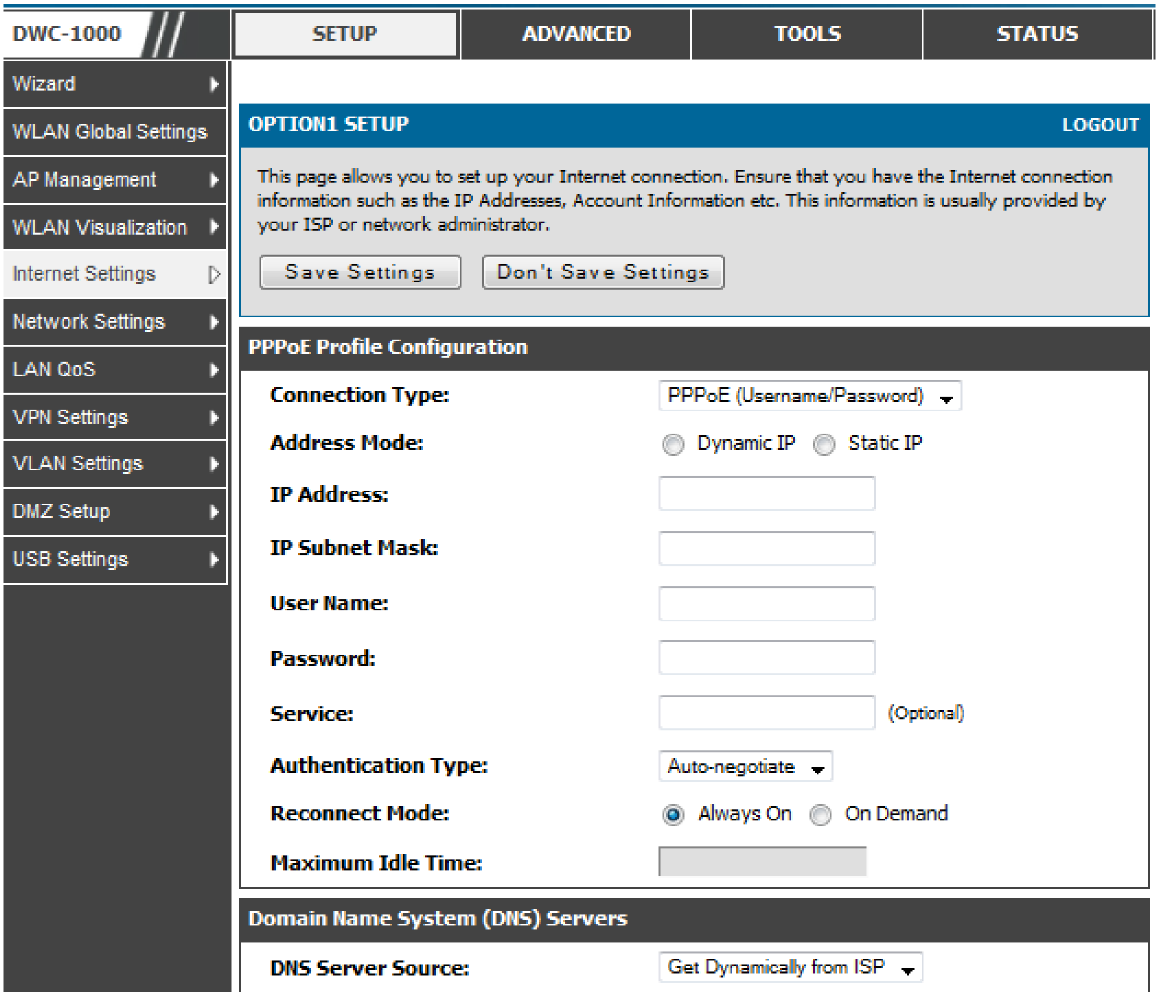
MAC Address: 00:00:00:00:00:00

6.2.4 PPPoE

Setup > Internet Settings > Option1 Settings > Option1 Setup

The PPPoE ISP settings are defined on the Option Configuration page. There are two types of PPPoE ISP's supported by the DWC-1000: the standard username/password PPPoE and Japan Multiple PPPoE.

Figure 99: PPPoE configuration for standard ISPs



This page allows you to set up your Internet connection. Ensure that you have the Internet connection information such as the IP Addresses, Account Information etc. This information is usually provided by your ISP or network administrator.

PPPoE Profile Configuration

Connection Type:	PPPoE (Username/Password)
Address Mode:	○ Dynamic IP ○ Static IP
IP Address:	
IP Subnet Mask:	
User Name:	
Password:	
Service:	(Optional)
Authentication Type:	Auto-negotiate
Reconnect Mode:	● Always On ○ On Demand
Maximum Idle Time:	

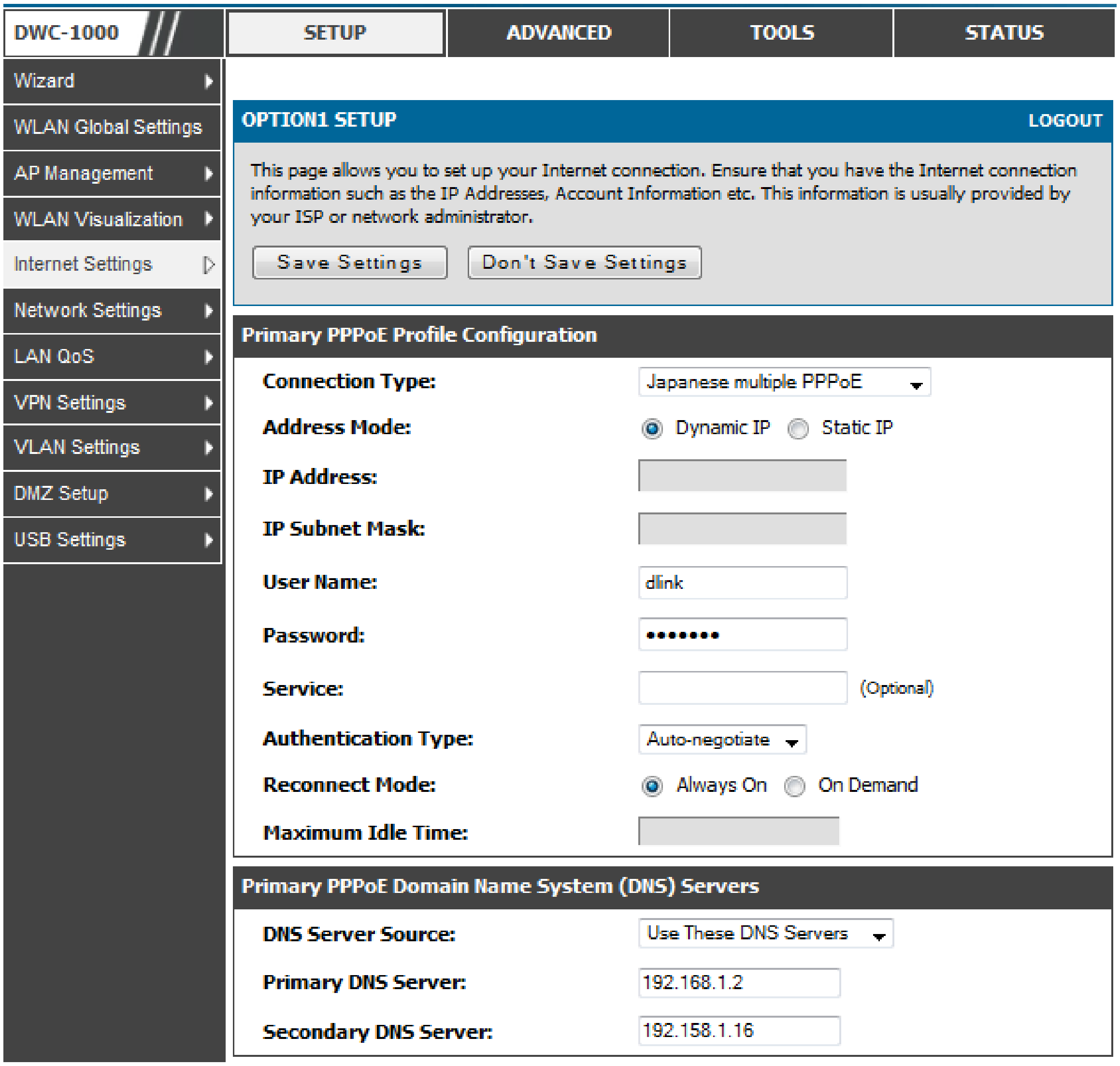
Domain Name System (DNS) Servers

DNS Server Source:	Get Dynamically from ISP

Most PPPoE ISP's use a single control and data connection, and require username / password credentials to login and authenticate the DWC-1000 with the ISP. The ISP connection type for this case is "PPPoE (Username/Password)". The GUI will prompt you for authentication, service, and connection settings in order to establish the PPPoE link.

For some ISP's, most popular in Japan, the use of "Japanese Multiple PPPoE" is required in order to establish concurrent primary and secondary PPPoE connections between the DWC-1000 and the ISP. The Primary connection is used for the bulk of data and internet traffic and the Secondary PPPoE connection carries ISP specific (i.e. control) traffic between the DWC-1000 and the ISP.

Figure 100: Option1 configuration for Japanese Multiple PPPoE (part 1)



OPTION1 SETUP

This page allows you to set up your Internet connection. Ensure that you have the Internet connection information such as the IP Addresses, Account Information etc. This information is usually provided by your ISP or network administrator.

Primary PPPoE Profile Configuration

Connection Type:	Japanese multiple PPPoE
Address Mode:	● Dynamic IP ○ Static IP
IP Address:	
IP Subnet Mask:	
User Name:	dlink
Password:	•••••••
Service:	(Optional)
Authentication Type:	Auto-negotiate
Reconnect Mode:	● Always On ○ On Demand
Maximum Idle Time:	

Primary PPPoE Domain Name System (DNS) Servers

DNS Server Source:	Use These DNS Servers
Primary DNS Server:	192.168.1.2
Secondary DNS Server:	192.158.1.16

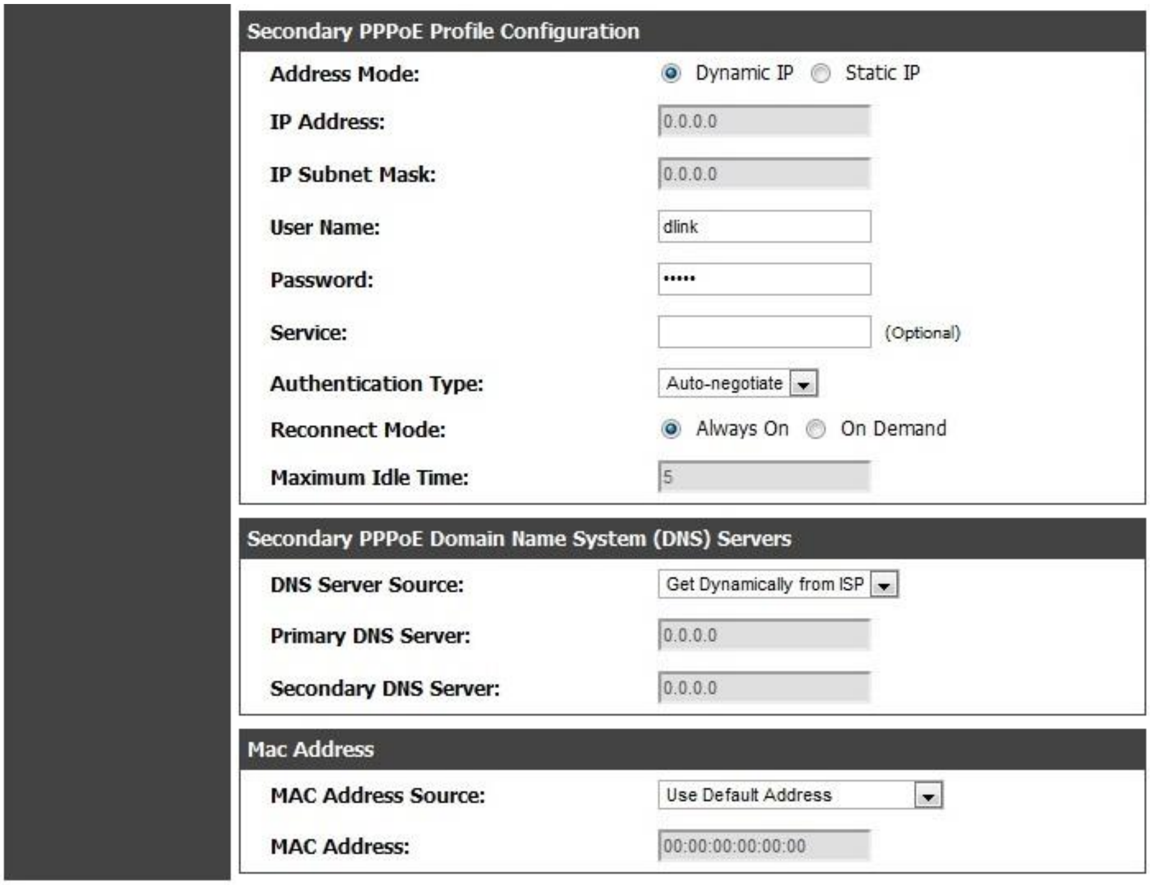
There are a few key elements of a multiple PPPoE connection:

- Primary and secondary connections are concurrent
- Each session has a DNS server source for domain name lookup, this can be assigned by the ISP or configured through the GUI
- The DWC-1000 acts as a DNS proxy for LAN users

- Only HTTP requests that specifically identify the secondary connection's domain name (for example *.flets) will use the secondary profile to access the content available through this secondary PPPoE terminal. All other HTTP / HTTPS requests go through the primary PPPoE connection.

When Japanese multiple PPPoE is configured and secondary connection is up, some predefined routes are added on that interface. These routes are needed to access the internal domain of the ISP where he hosts various services. These routes can even be configured through the static routing page as well.

Figure 101: Option1 configuration for Multiple PPPoE (part 2)



Secondary PPPoE Profile Configuration

Address Mode:	● Dynamic IP ○ Static IP
IP Address:	0.0.0.0
IP Subnet Mask:	0.0.0.0
User Name:	dlink
Password:	•••••
Service:	(Optional)
Authentication Type:	Auto-negotiate
Reconnect Mode:	● Always On ○ On Demand
Maximum Idle Time:	5

Secondary PPPoE Domain Name System (DNS) Servers

DNS Server Source:	Get Dynamically from ISP
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0

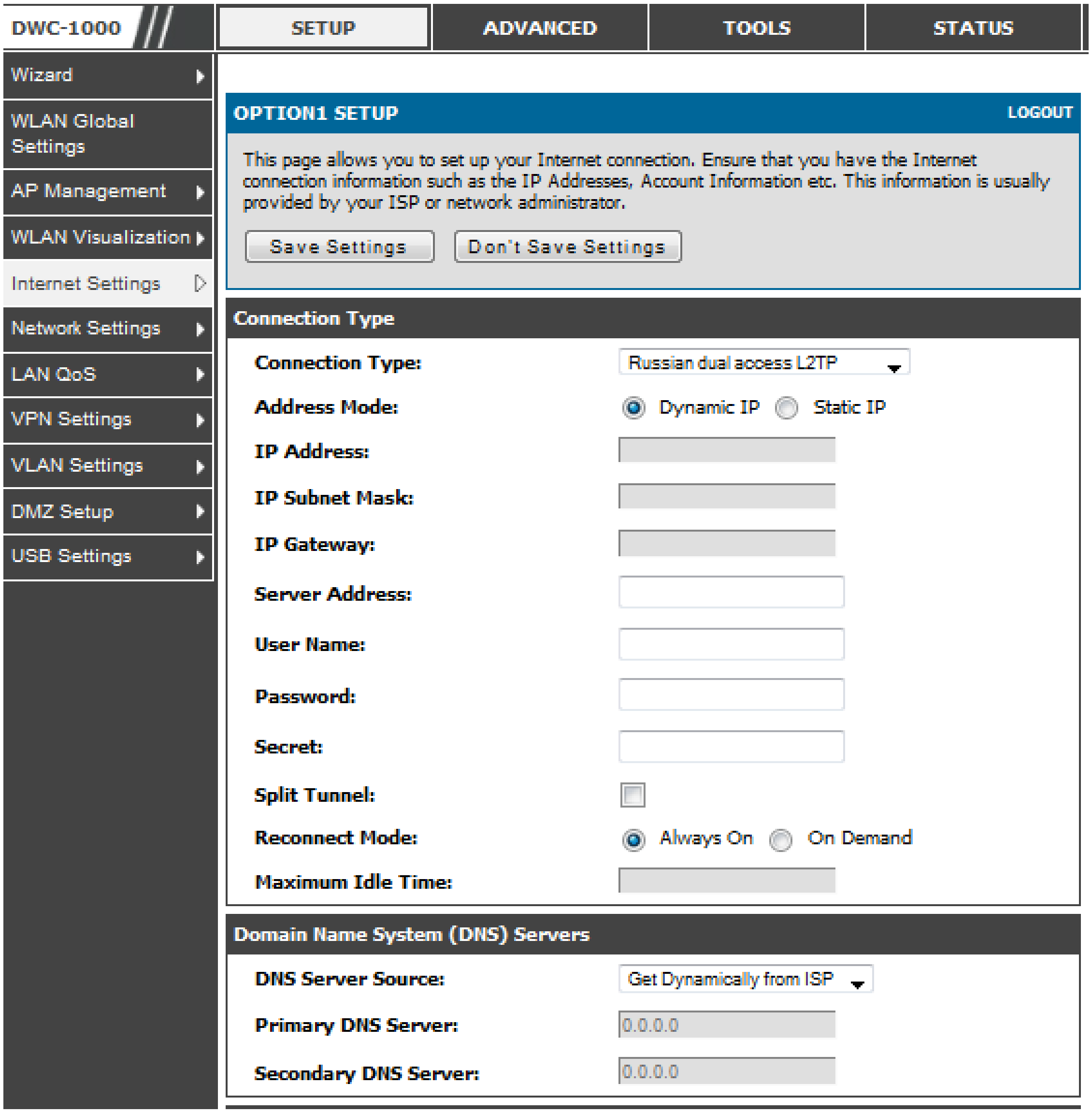
Mac Address

MAC Address Source:	Use Default Address
MAC Address:	00:00:00:00:00:00

6.2.5 Russia L2TP and PPTP Option

For Russia L2TP Option connections, you can choose the address mode of the connection to get an IP address from the ISP or configure a static IP address provided by the ISP. For DHCP client connections, you can choose the MAC address of the controller to register with the ISP. In some cases you may need to clone the LAN host’s MAC address if the ISP is registered with that LAN host.

Figure 102: Russia L2TP ISP configuration



OPTION1 SETUP

This page allows you to set up your Internet connection. Ensure that you have the Internet connection information such as the IP Addresses, Account Information etc. This information is usually provided by your ISP or network administrator.

Connection Type

Connection Type:	Russian dual access L2TP
Address Mode:	● Dynamic IP ○ Static IP
IP Address:	
IP Subnet Mask:	
IP Gateway:	
Server Address:	
User Name:	
Password:	
Secret:	
Split Tunnel:	□
Reconnect Mode:	● Always On ○ On Demand
Maximum Idle Time:	

Domain Name System (DNS) Servers

DNS Server Source:	Get Dynamically from ISP
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0

6.2.6 Option Configuration in an IPv6 Network

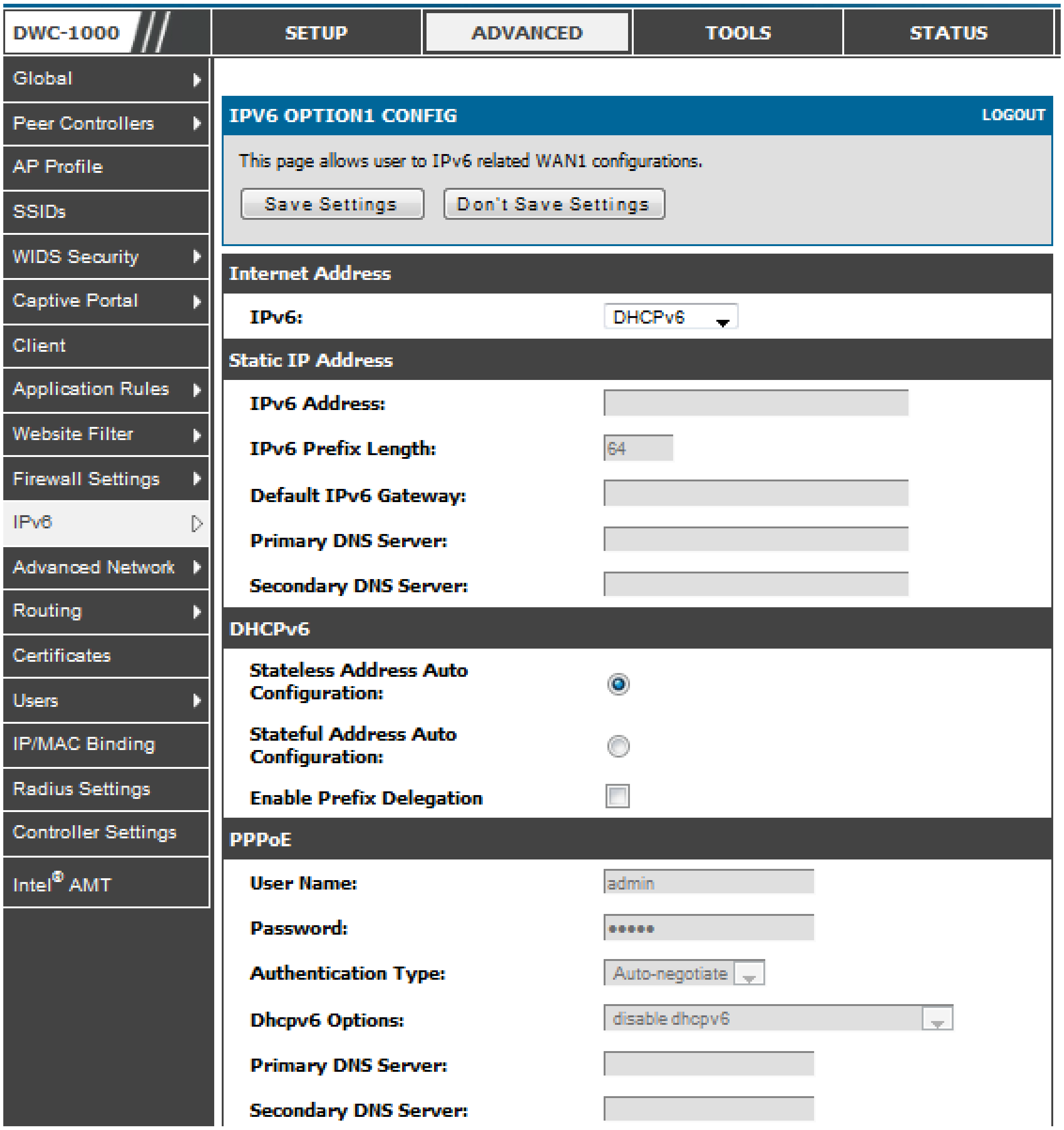
Advanced > IPv6 > IPv6 Option1 Config

For IPv6 Option connections, this controller can have a static IPv6 address or receive connection information when configured as a DHCPv6 client. In the case where the ISP assigns you a fixed address to access the internet, the static configuration settings must be completed. In addition to the IPv6 address assigned to your controller, the

IPv6 prefix length defined by the ISP is needed. The default IPv6 Gateway address is the server at the ISP that this controller will connect to for accessing the internet. The primary and secondary DNS servers on the ISP's IPv6 network are used for resolving internet addresses, and these are provided along with the static IP address and prefix length from the ISP.

When the ISP allows you to obtain the Option IP settings via DHCP, you need to provide details for the DHCPv6 client configuration. The DHCPv6 client on the gateway can be either stateless or stateful. If a stateful client is selected the gateway will connect to the ISP's DHCPv6 server for a leased address. For stateless DHCP there need not be a DHCPv6 server available at the ISP, rather ICMPv6 discover messages will originate from this gateway and will be used for auto configuration. A third option to specify the IP address and prefix length of a preferred DHCPv6 server is available as well.

Figure 103: IPv6 Option1 Setup page



IPV6 OPTION1 CONFIG

This page allows user to IPv6 related WAN1 configurations.

Internet Address

IPv6: DHCPv6

Static IP Address

IPv6 Address:

IPv6 Prefix Length: 64

Default IPv6 Gateway:

Primary DNS Server:

Secondary DNS Server:

DHCPv6

Stateless Address Auto Configuration: ●

Stateful Address Auto Configuration: ○

Enable Prefix Delegation ☐

PPPoE

User Name: admin

Password: •••••

Authentication Type: Auto-negotiate

Dhcpv6 Options: disable dhcpv6

Primary DNS Server:

Secondary DNS Server:

Prefix Delegation: Select this option to request controller advertisement prefix from any available DHCPv6 servers available on the ISP, the obtained prefix is updated to the advertised prefixes on the LAN side. This option can be selected only in Stateless Address Auto Configuration mode of DHCPv6 Client.

When IPv6 is PPPoE type, the following PPPoE fields are enabled.

Username: Enter the username required to log in to the ISP.

Password: Enter the password required to login to the ISP.

Authentication Type: The type of Authentication in use by the profile: Auto-Negotiate/PAP/CHAP/MS-CHAP/MS-CHAPv2.

Dhcpv6 Options: The mode of Dhcpv6 client that will start in this mode: disable dhcpv6/stateless dhcpv6/stateful dhcpv6/stateless dhcpv6 with prefix delegation.

Primary DNS Server: Enter a valid primary DNS Server IP Address.

Secondary DNS Server: Enter a valid secondary DNS Server IP Address.

Click **Save Settings** to save your changes.

6.2.7 Checking Option Status

Setup > Internet Settings > Option1 Settings > Option 1 Status

The status and summary of configured settings for both Option 1and Option 2 are available on the Option Status page. You can view the following key connection status information for each Option port:

MAC Address: MAC Address of the Option port.

IPv4 Address: IP address of the Option port followed by the Option subnet.

Option State: Indicates the state of the Option port (UP or DOWN)

NAT (**IPv4 only):** Indicates if the security appliance is in NAT mode (enabled) or routing mode (disabled).

IPv4 Connection Type: Indicates if the Option IPv4 address is obtained dynamically through a DHCP server or assigned statically by the user or obtained through a PPPoE (Username/Password)/PPTP (Username/Password)/L2TP (Username/Password)/Japanese multiple PPPoE/Russian dual access PPPoE/Russian dual access PPTP/ Russian dual access L2TP ISP connection.

IPv4 Connection State: Indicates if the Option is connected to the Internet Service Provider.
Link State: Detects if a link is present on the Option Interface

Option Mode: Indicates if Option1 or Option2 is in use

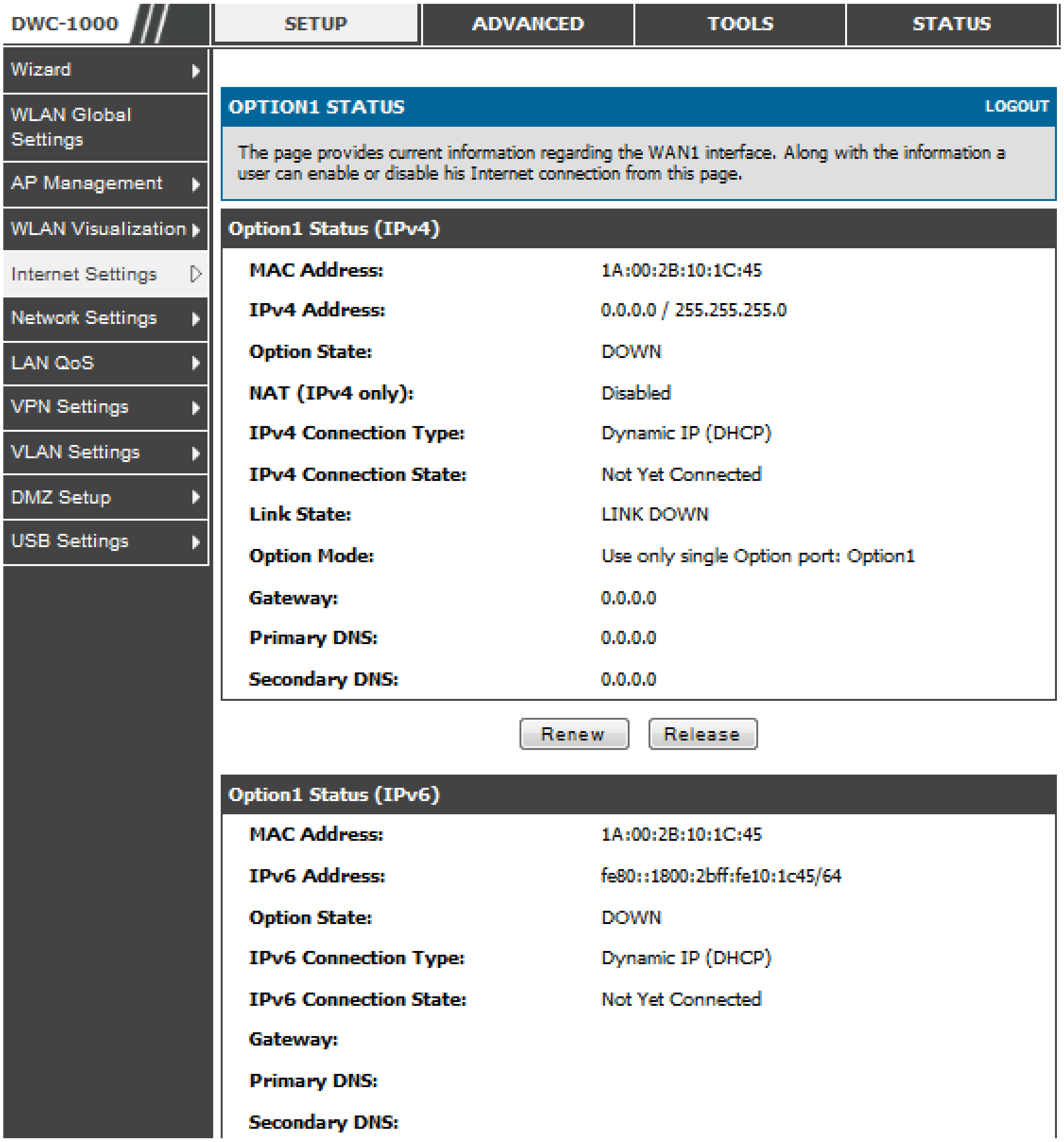
Gateway: Gateway IP address of the Option port.

Primary DNS: Primary DNS server IP address of the Option port.

Secondary DNS: Secondary DNS server IP address of the Option port. If the Connection Status indicated that the association with the ISP is active, then the Option can be disconnected by clicking the Disable button.

If the Connection Status indicated that the association with the ISP is active, then the Option can be disconnected by clicking the **Disable** button.

Figure 104: Connection Status information of Option1



OPTION1 STATUS

The page provides current information regarding the WAN1 interface. Along with the information a user can enable or disable his Internet connection from this page.

Option1 Status (IPv4)

MAC Address:	1A:00:2B:10:1C:45
IPv4 Address:	0.0.0.0 / 255.255.255.0
Option State:	DOWN
NAT (IPv4 only):	Disabled
IPv4 Connection Type:	Dynamic IP (DHCP)
IPv4 Connection State:	Not Yet Connected
Link State:	LINK DOWN
Option Mode:	Use only single Option port: Option1
Gateway:	0.0.0.0
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0

Option1 Status (IPv6)

MAC Address:	1A:00:2B:10:1C:45
IPv6 Address:	fe80::1800:2bff:fe10:1c45/64
Option State:	DOWN
IPv6 Connection Type:	Dynamic IP (DHCP)
IPv6 Connection State:	Not Yet Connected
Gateway:	
Primary DNS:	
Secondary DNS:	

The Option status page allows you to Enable or Disable static Option links. For Option settings that are dynamically received from the ISP, you can Renew or Release the link parameters if required.

6.3 Features with Multiple Option Links

This controller supports multiple Option links. This allows you to take advantage of failover and load balancing features to ensure certain internet dependent services are prioritized in the event of unstable Option connectivity on one of the ports.

Setup > Internet Settings > Option Mode

To use Auto Failover or Load Balancing, Option link failure detection must be configured. This involves accessing DNS servers on the internet or ping to an internet address (user defined). If required, you can configure the number of retry attempts when the link seems to be disconnected or the threshold of failures that determines if the Option port is down.

6.3.1 Auto Failover

In this case one of your Option ports is assigned as the primary internet link for all internet traffic. The secondary Option port is used for redundancy in case the primary link goes down for any reason. Both Option ports (primary and secondary) must be configured to connect to the respective ISP’s before enabling this feature. The secondary Option port will remain unconnected until a failure is detected on the primary link (either port can be assigned as the primary). In the event of a failure on the primary port, all internet traffic will be rolled over to the backup port. When configured in Auto Failover mode, the link status of the primary Option port is checked at regular intervals as defined by the failure detection settings.

Note that both Option1 and Option2 can be configured as the primary internet link.

- **Auto-Rollover** using Option port
- **Primary Option**: Selected Option is the primary link (Option1/ Option2)
- **Secondary Option**: Selected Option is the secondary link.

Failover Detection Settings: To check connectivity of the primary internet link, one of the following failure detection methods can be selected:

- **DNS lookup using Option DNS Servers**: DNS Lookup of the DNS Servers of the primary link are used to detect primary Option connectivity.

- **DNS lookup using Option Servers**: DNS Lookup of the custom DNS Servers can be specified to check the connectivity of the primary link.
- **Ping these IP addresses**: These IP's will be pinged at regular intervals to check the connectivity of the primary link.
- **Retry Interval is**: The number tells the controller how often it should run the above configured failure detection method.
- **Failover after**: This sets the number of retries after which failover is initiated.

6.3.2 Load Balancing

This feature allows you to use multiple Option links (and presumably multiple ISP's) simultaneously. After configuring more than one Option port, the load balancing option is available to carry traffic over more than one link. Protocol bindings are used to segregate and assign services over one Option port in order to manage internet flow. The configured failure detection method is used at regular intervals on all configured Option ports when in Load Balancing mode.

DWC-1000 currently supports three algorithms for Load Balancing:

Round Robin: This algorithm is particularly useful when the connection speed of one Option port greatly differs from another. In this case you can define protocol bindings to route low-latency services (such as VOIP) over the higher-speed link and let low-volume background traffic (such as SMTP) go over the lower speed link. Protocol binding is explained in next section.

Spill Over: If Spill Over method is selected, Option 1 acts as a dedicated link till a threshold is reached. After this, Option 2 will be used for new connections. You can configure spill-over mode by using following options:

- **Load Tolerance**: It is the percentage of bandwidth after which the controller controllers to secondary Option.
- **Max Bandwidth**: This sets the maximum bandwidth tolerable by the primary Option.

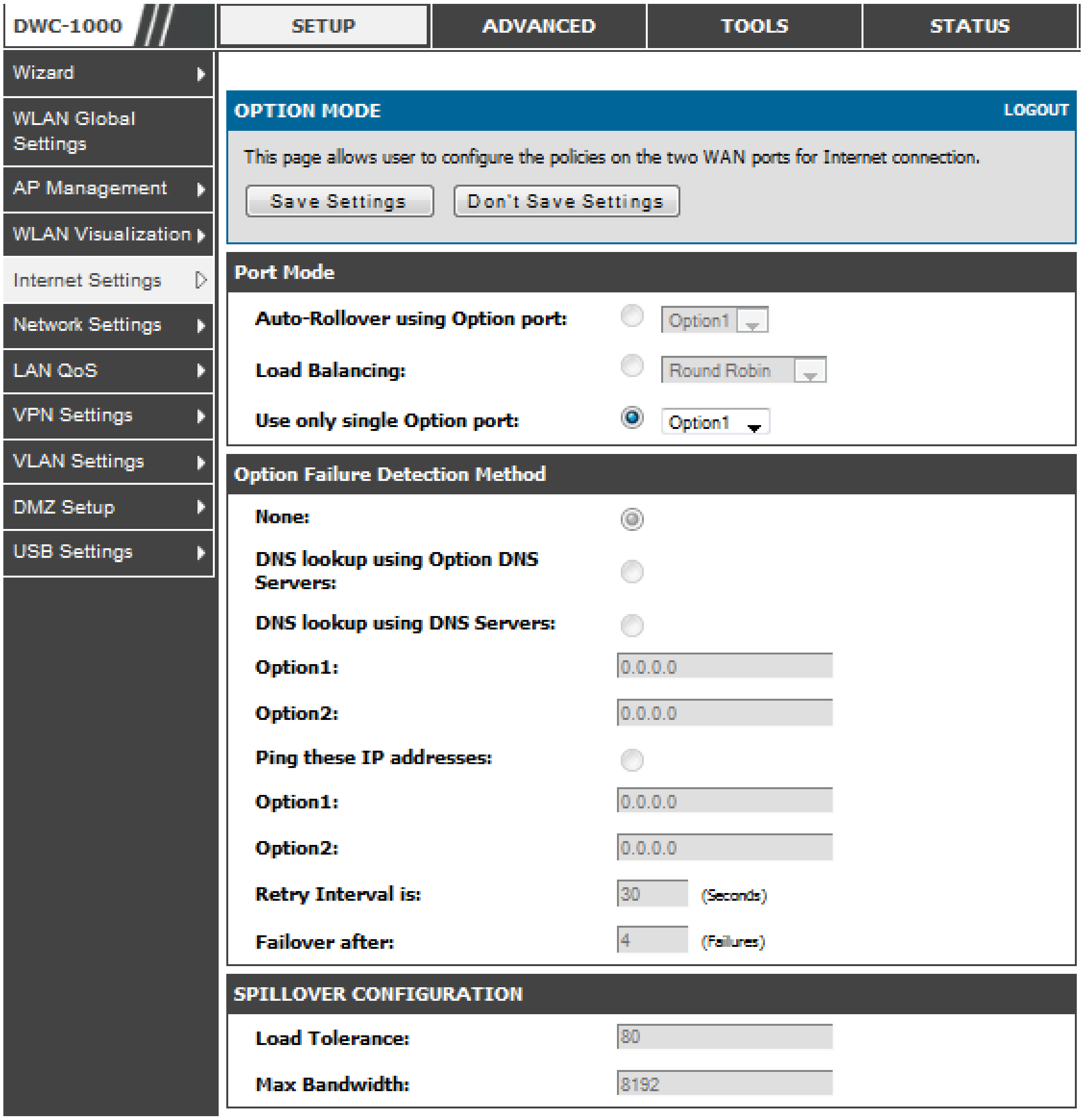
If the link bandwidth goes above the load tolerance value of max bandwidth, the controller will spill-over the next connections to secondary Option.

For example, if the maximum bandwidth of primary Option is 1 Kbps and the load tolerance is set to 70. Now every time a new connection is established the bandwidth increases. After a certain number of connections say bandwidth reached 70% of 1Kbps, the new connections will be spilled-over to secondary Option. The maximum value of load tolerance is 80 and the least is 20.

Protocol Bindings: Refer Section 6.3.3 for details

Load balancing is particularly useful when the connection speed of one Option port greatly differs from another. In this case you can define protocol bindings to route low-latency services (such as VOIP) over the higher-speed link and let low-volume background traffic (such as SMTP) go over the lower speed link.

Figure 105: Load Balancing is available when multiple Option ports are configured and Protocol Bindings have been defined



OPTION MODE

This page allows user to configure the policies on the two WAN ports for Internet connection.

Port Mode

Auto-Rollover using Option port: ○ Option1

Load Balancing: ○ Round Robin

Use only single Option port: ● Option1

Option Failure Detection Method

None: ●

DNS lookup using Option DNS Servers: ○

DNS lookup using DNS Servers: ○

Option1: 0.0.0.0

Option2: 0.0.0.0

Ping these IP addresses: ○

Option1: 0.0.0.0

Option2: 0.0.0.0

Retry Interval is: 30 (Seconds)

Failover after: 4 (Failures)

SPILLOVER CONFIGURATION

Load Tolerance: 80

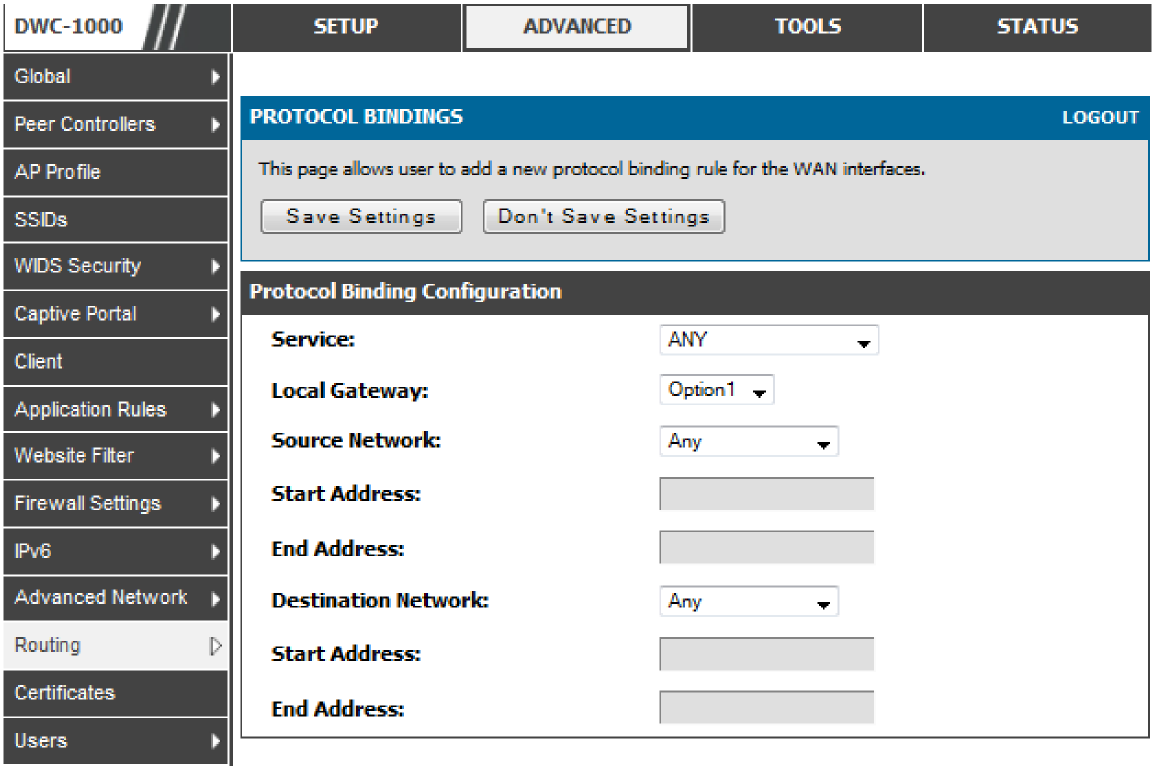
Max Bandwidth: 8192

6.3.3 Protocol Bindings

Advanced > Routing > Protocol Bindings

Protocol bindings are required when the Load Balancing feature is in use. Choosing from a list of configured services or any of the user-defined services, the type of traffic can be assigned to go over only one of the available Option ports. For increased flexibility the source network or machines can be specified as well as the destination network or machines. For example the VOIP traffic for a set of LAN IP addresses can be assigned to one Option and any VOIP traffic from the remaining IP addresses can be assigned to the other Option link. Protocol bindings are only applicable when load balancing mode is enabled and more than one Option is configured.

Figure 106: Protocol binding setup to associate a service and/or LAN source to an Option and/or destination network



PROTOCOL BINDINGS

This page allows user to add a new protocol binding rule for the WAN interfaces.

Protocol Binding Configuration

Service:	ANY
Local Gateway:	Option1
Source Network:	Any
Start Address:	
End Address:	
Destination Network:	Any
Start Address:	
End Address:	

Service: Select one of the various services available for protocol binding

Local Gateway: select the port that sets the local gateway for this protocol binding (either option1 or option2)

Source Network: Select one of the following:

Any: No specific network needs to be given.

Single Address: Limit to one computer. Requires the IP address of the computer that will be part of the source network for this protocol binding

Address Range: Select if you want to allow computers within an IP address range to be a part of the source network. Requires Start address and End address

Start Address: IP address from where the range needs to begin, or the single address if that is the source network selected.

End Address: IP address where the range needs to end

Destination Network: Select one of the following:

Any: No specific network needs to be given.

Single Address: Limit to one computer. Requires the IP address of the computer that will be part of the destination network for this protocol binding

Address Range: Select if you want to allow computers within an IP address range to be a part of the destination network. Requires Start address and End address

Start Address: IP address from where the range needs to begin, or the single address if that is the destination network selected.

End Address: IP address where the range needs to end

6.4 Routing Configuration

Routing between the LAN and Option will impact the way this controller handles traffic that is received on any of its physical interfaces. The routing mode of the gateway is core to the behavior of the traffic flow between the secure LAN and the internet.

6.4.1 Routing Mode

Setup > Internet Settings > Routing Mode

This device supports classical routing, network address translation (NAT), and transport mode routing.

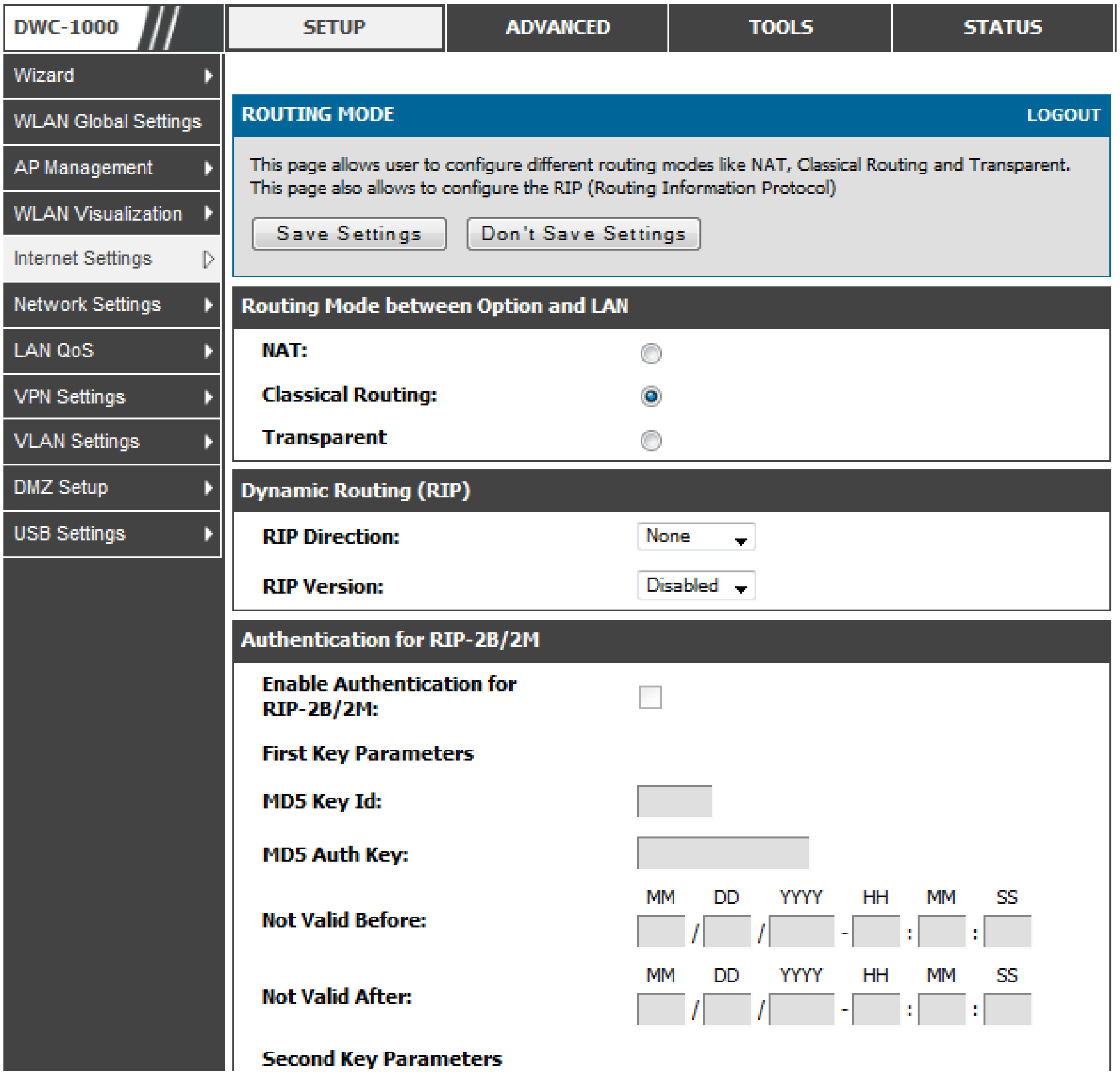
- With ***classical routing***, devices on the LAN can be directly accessed from the internet by their public IP addresses (assuming appropriate firewall settings). If your ISP has assigned an IP address for each of the computers that you use, select Classic Routing.

- ***NAT*** is a technique which allows several computers on a LAN to share an Internet connection. The computers on the LAN use a "private" IP address range while the Option port on the controller is configured with a single "public" IP address. Along with connection sharing, NAT also hides internal IP addresses from the computers on the Internet. NAT is required if your ISP has assigned only one IP address to you. The computers that connect through the controller will need to be assigned IP addresses from a private subnet.

- ***Transparent routing*** between the LAN and Option does not perform NAT. Broadcast and multicast packets that arrive on the LAN interface are switched to the Option and vice versa, if they do not get filtered by firewall or VPN policies. To maintain the LAN and Option in the same broadcast domain select Transparent mode, which allows bridging of traffic from LAN to Option and vice versa, except for controller -terminated traffic and other management traffic. All DWC features are supported in transparent mode assuming the LAN and Option are configured to be in the same broadcast domain.

> ✍ NAT routing has a feature called “NAT Hair-pinning” that allows internal network users on the LAN and DMZ to access internal servers (e.g. an internal FTP server) using their externally-known domain name. This is also referred to as “NAT loopback” since LAN generated traffic is redirected through the firewall to reach LAN servers by their external name.

Figure 107: Routing Mode is used to configure traffic routing between Option and LAN, as well as Dynamic routing (RIP)



ROUTING MODE

This page allows user to configure different routing modes like NAT, Classical Routing and Transparent. This page also allows to configure the RIP (Routing Information Protocol)

Routing Mode between Option and LAN

NAT: ○

Classical Routing: ●

Transparent ○

Dynamic Routing (RIP)

RIP Direction: None

RIP Version: Disabled

Authentication for RIP-2B/2M

Enable Authentication for RIP-2B/2M: □

First Key Parameters

MD5 Key Id:

MD5 Auth Key:

Not Valid Before: MM / DD / YYYY - HH : MM : SS

Not Valid After: MM / DD / YYYY - HH : MM : SS

Second Key Parameters

6.4.2 Dynamic Routing (RIP)

> ✍ The following feature is available upon licensed activation of VPN / Firewall features for the system.

Setup > Internet Settings > Routing Mode

Dynamic routing using the Routing Information Protocol (RIP) is an Interior Gateway Protocol (IGP) that is common in LANs. With RIP this controller can exchange routing information with other supported controllers in the LAN and allow for dynamic adjustment of routing tables in order to adapt to modifications in the LAN without interrupting traffic flow.

The RIP direction will define how this controller sends and receives RIP packets. Choose between:

- **Both**: The controller both broadcasts its routing table and also processes RIP information received from other controllers. This is the recommended setting in order to fully utilize RIP capabilities.
- **Out Only**: The controller broadcasts its routing table periodically but does not accept RIP information from other controllers.
- **In Only**: The controller accepts RIP information from other controller, but does not broadcast its routing table.
- **None**: The controller neither broadcasts its route table nor does it accept any RIP packets from other controllers. This effectively disables RIP.
  - The RIP version is dependent on the RIP support of other routing devices in the LAN.
- **Disabled**: This is the setting when RIP is disabled.

RIP-1 is a class-based routing version that does not include subnet information. This is the most commonly supported version.

RIP-2 includes all the functionality of RIPv1 plus it supports subnet information. Though the data is sent in RIP-2 format for both RIP-2B and RIP-2M, the mode in which packets are sent is different. RIP-2B broadcasts data in the entire subnet while RIP-2M sends data to multicast addresses.

If RIP-2B or RIP-2M is the selected version, authentication between this controller and other controllers (configured with the same RIP version) is required. MD5 authentication is used in a first/second key exchange process. The authentication key validity lifetimes are configurable to ensure that the routing information exchange is with current and supported controllers detected on the LAN.

6.4.3 Static Routing

Advanced > Routing > Static Routing

Advanced > IPv6 > IPv6 Static Routing

Manually adding static routes to this device allows you to define the path selection of traffic from one interface to another. There is no communication between this controller and other devices to account for changes in the path; once configured the static route will be active and effective until the network changes.

The List of Static Routes displays all routes that have been added manually by an administrator and allows several operations on the static routes. The List of IPv4 Static Routes and List of IPv6 Static Routes share the same fields (with one exception):

Name: Name of the route, for identification and management.

Active: Determines whether the route is active or inactive. A route can be added to the table and made inactive, if not needed. This allows routes to be used as needed without deleting and re-adding the entry. An inactive route is not broadcast if RIP is enabled.

Private: Determines whether the route can be shared with other controllers when RIP is enabled. If the route is made private, then the route will not be shared in a RIP broadcast or multicast. This is only applicable for IPv4 static routes.

Destination: the route will lead to this destination host or IP address.

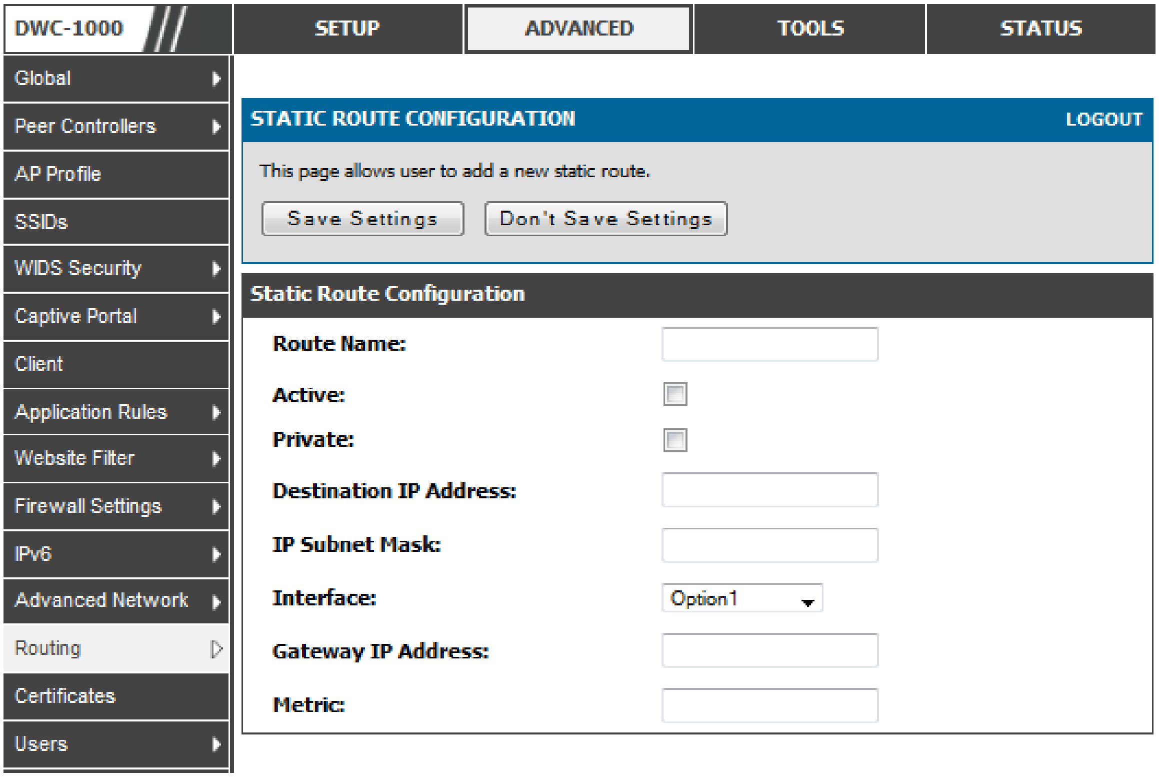
IP Subnet Mask: This is valid for IPv4 networks only, and identifies the subnet that is affected by this static route

Interface: The physical network interface (Option1, Option2, DMZ or LAN), through which this route is accessible.

Gateway: IP address of the gateway through which the destination host or network can be reached.

Metric: Determines the priority of the route. If multiple routes to the same destination exist, the route with the lowest metric is chosen.

Figure 108: Static route configuration fields



STATIC ROUTE CONFIGURATION

This page allows user to add a new static route.

Static Route Configuration

Route Name:	
Active:	□
Private:	□
Destination IP Address:	
IP Subnet Mask:	
Interface:	Option1
Gateway IP Address:	
Metric:	

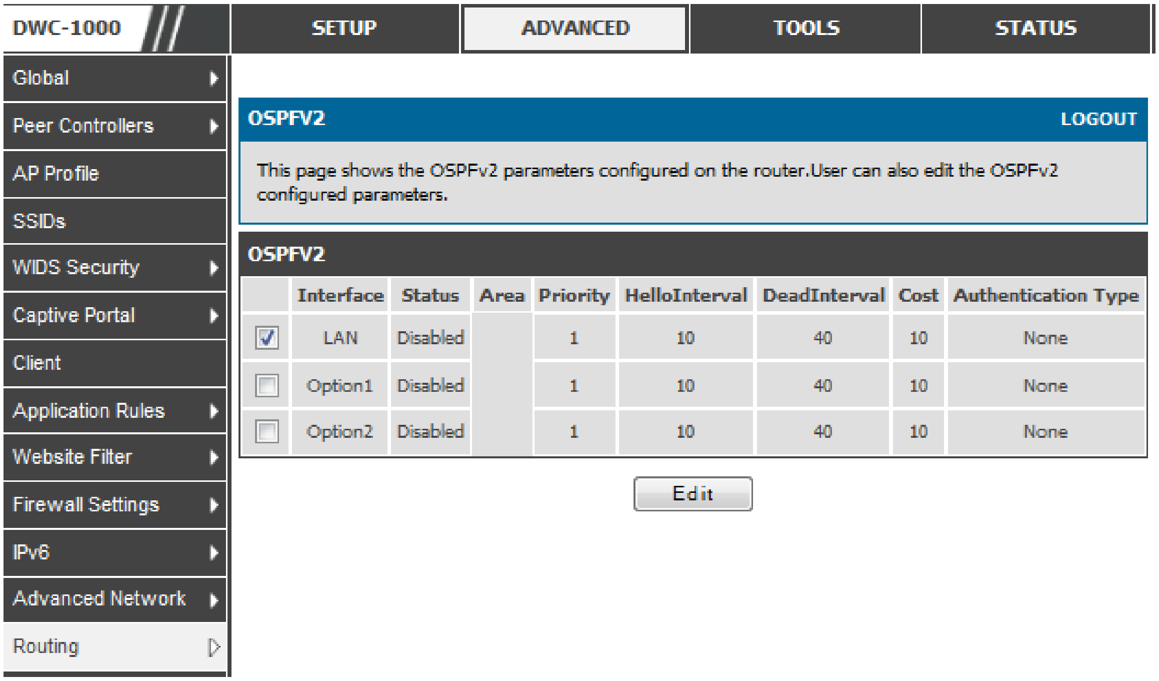
6.5 OSPF

Advanced > Routing > OSPF

Advanced > IPv6 > OSPF

This page shows the OSPFv2 and OSPFv3 parameters configured on the controller. You can also edit the configured parameters from the OSPF configuration page.

Figure 109: OSPFv2 status – IPv4



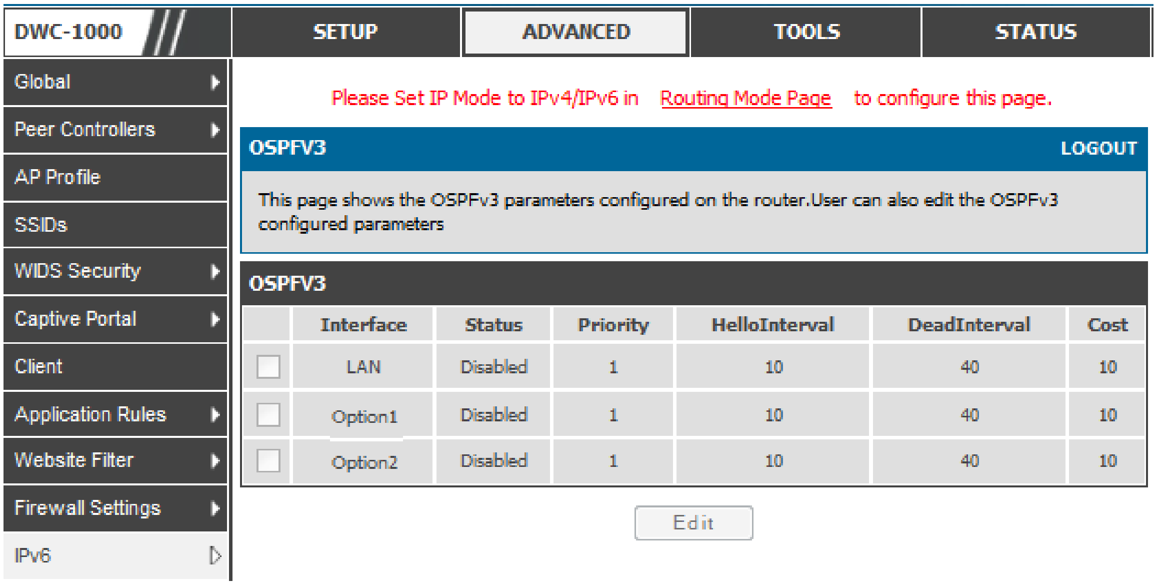
OSPFV2

This page shows the OSPFv2 parameters configured on the router.User can also edit the OSPFv2 configured parameters.

OSPFV2

	Interface	Status	Area	Priority	HelloInterval	DeadInterval	Cost	Authentication Type
☑	LAN	Disabled		1	10	40	10	None
□	Option1	Disabled		1	10	40	10	None
□	Option2	Disabled		1	10	40	10	None

Figure 110: OSPFv3 status – IPv6



Please Set IP Mode to IPv4/IPv6 in Routing Mode Page to configure this page.

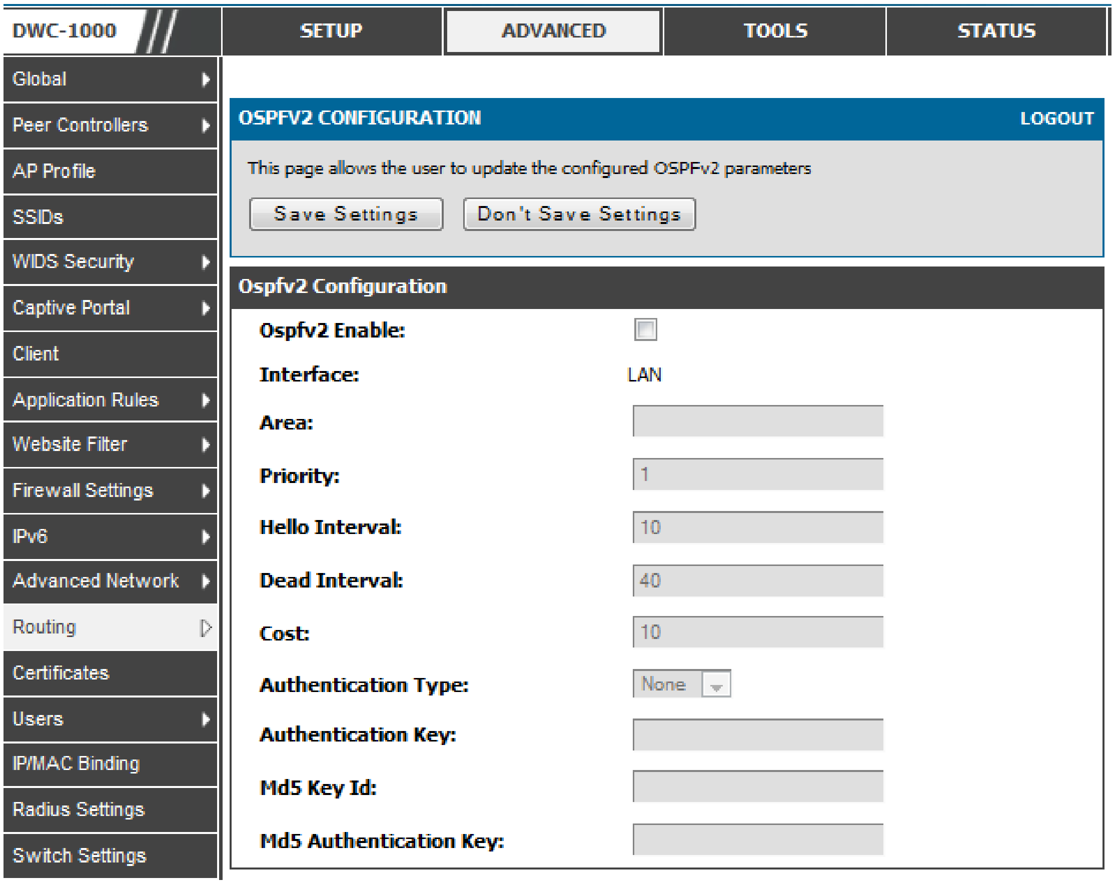
OSPFV3

This page shows the OSPFv3 parameters configured on the router.User can also edit the OSPFv3 configured parameters

OSPFV3

	Interface	Status	Priority	HelloInterval	DeadInterval	Cost
□	LAN	Disabled	1	10	40	10
□	Option1	Disabled	1	10	40	10
□	Option2	Disabled	1	10	40	10

Figure 111: OSPFv2 Configuration



This page allows the user to update the configured OSPFv2 parameters

Ospfv2 Enable:	□
Interface:	LAN
Area:	
Priority:	1
Hello Interval:	10
Dead Interval:	40
Cost:	10
Authentication Type:	None
Authentication Key:	
Md5 Key Id:	
Md5 Authentication Key:	

OSPFv2 Enable: A check box to enable/disable OSPFv2.

Interface: The physical network interface on which OSPFv2 is Enabled/Disabled.

Area: The area to which the interface belongs. Enter values from 1 to 255.Two routers having a common segment; their interfaces have to belong to the same area on that segment. The interfaces should belong to the same subnet and have similar mask.

Priority: Helps to determine the OSPFv2 designated router for a network. The router with the highest priority will be more eligible to become Designated Router. Setting the value to 0, makes the router ineligible to become Designated Router. The default value is 1.Lower value means higher priority.

HelloInterval: The number of seconds for HelloInterval timer value. Setting this value, Hello packet will be sent every timer value seconds on the specified interface. This value must be the same for all routers attached to a common network. The default value is 10 seconds.

DeadInterval: The number of seconds that a device’s hello packets must not have been seen before its neighbors declare the OSPF router down. This value must be the same for all routers attached to a common network. The default value is 40 seconds. OSPF requires these intervals to be exactly the same between two neighbors. If any of these intervals are different, these routers will not become neighbors on a particular segment

Cost: The cost of sending a packet on an OSPFv2 interface.

Authentication Type: This column displays the type of authentication to be used for OSPFv2.If Authentication type is none the interface does not authenticate OSPF packets. If Authentication Type is Simple then OSPF packets are authenticated using simple text key.If Authentication Type is MD5 then the interface authenticates OSPF packets with MD5 authentication.

Authentication Key: Assign a specific password to be used by neighboring OSPF routers on a network segment that is using Authentication. Routers in the same area that want to participate in the routing domain will have to be configured with the same key.
Md5 Key Id: Input the unique MD-5 key ID to be used by neighboring OSPF routers on a network segment that is using Authentication. Type as MD5

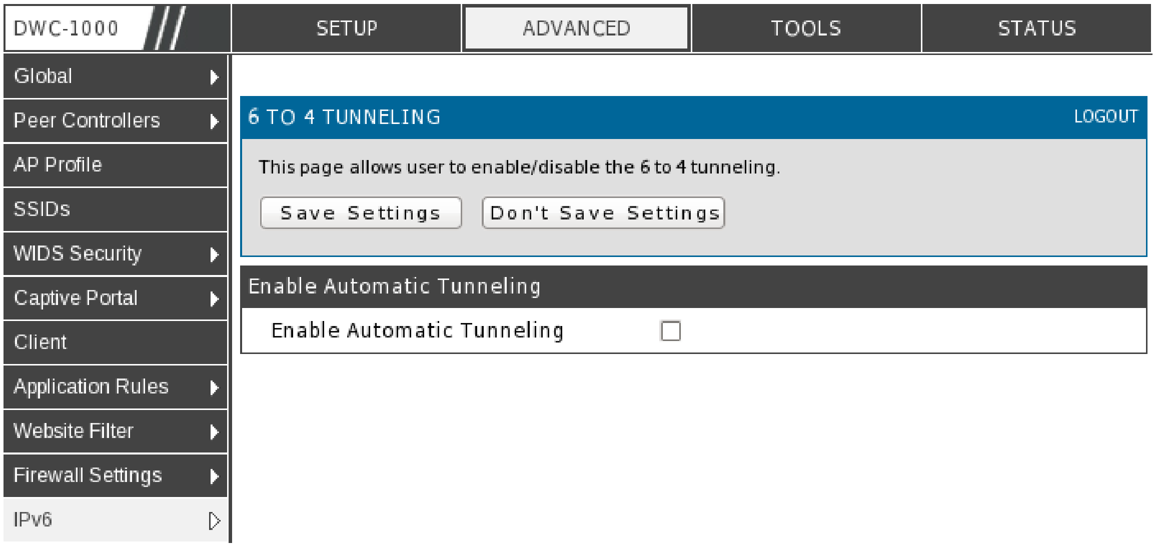
Md5 Authentication Key: Input the authentication key for this MD5 key to be used by neighboring OSPF routers on a network segment that is using Authentication Type as MD5

6.6 6to4 Tunneling

Advanced > IPv6 > 6to4 Tunneling

6to4 is an Internet transition mechanism for migrating from IPv4 to IPv6, a system that allows IPv6 packets to be transmitted over an IPv4 network. Select the check box to **Enable Automatic Tunneling** and allow traffic from an IPv6 LAN to be sent over a IPv4 Option to reach a remote IPv6 network.

Figure 112: 6to4 Tunneling



6 TO 4 TUNNELING

This page allows user to enable/disable the 6 to 4 tunneling.

Enable Automatic Tunneling

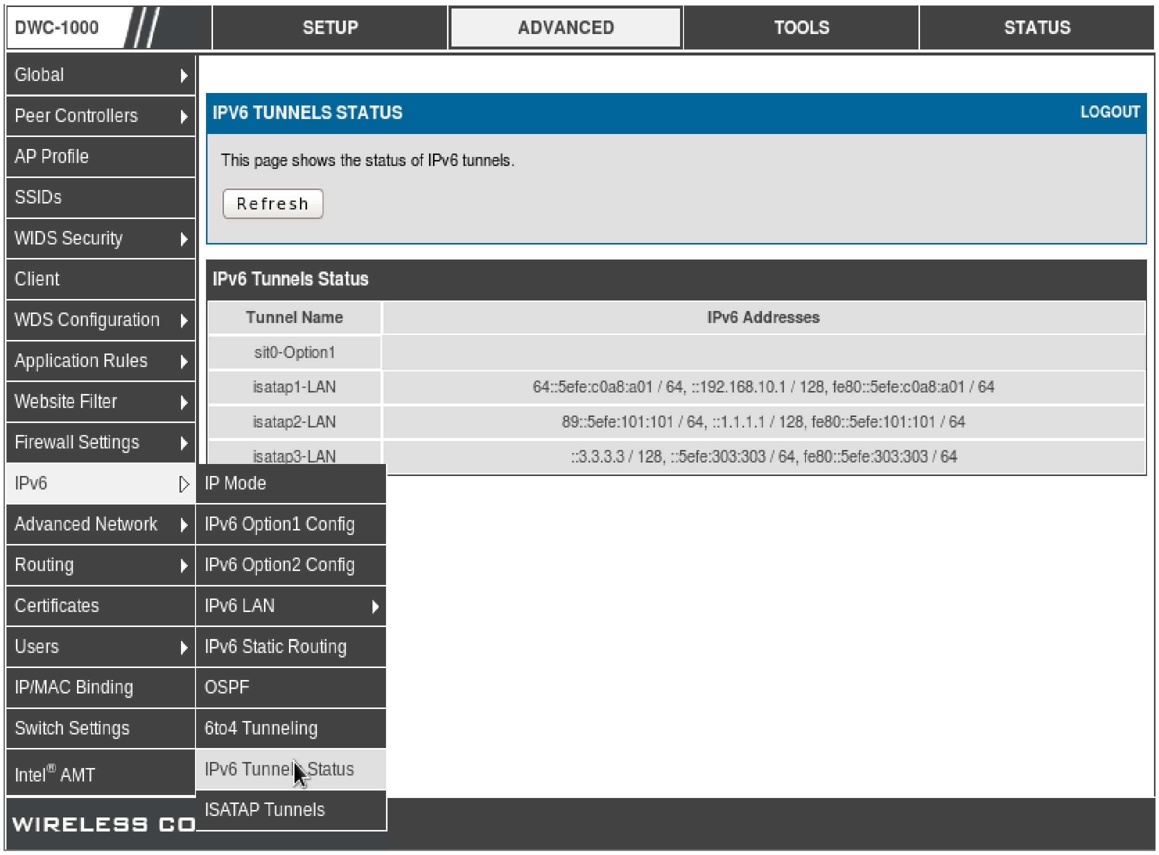
Enable Automatic Tunneling □

6.7 IPv6 Tunnels Status

Advanced>IPv6>IPv6 Tunnels Status

This status page displays the IPv6 tunnels (6to4 and ISATAP) status in the GUI.

Figure 113: IPv6 Tunnel Status display



IPV6 TUNNELS STATUS

This page shows the status of IPv6 tunnels.

IPv6 Tunnels Status

Tunnel Name	IPv6 Addresses
sit0-Option1	
isatap1-LAN	64::5efe:c0a8:a01 / 64, ::192.168.10.1 / 128, fe80::5efe:c0a8:a01 / 64
isatap2-LAN	89::5efe:101:101 / 64, ::1.1.1.1 / 128, fe80::5efe:101:101 / 64
isatap3-LAN	::3.3.3.3 / 128, ::5efe:303:303 / 64, fe80::5efe:303:303 / 64

Tunnel Name: The active IPv6 to IPv4 tunnel identifier.

IPv6 Addresses: the source IPv6 address(es) in your LAN that have data being sent over this tunnel.

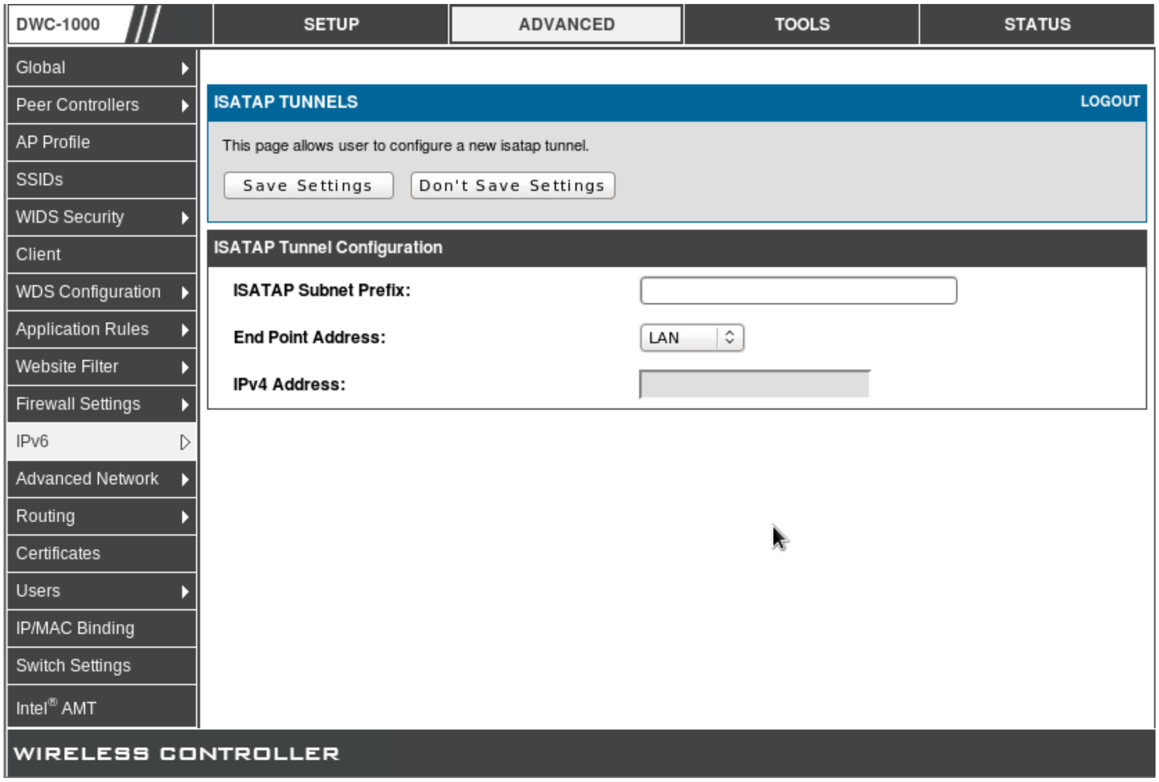
6.8 ISATAP Tunnels

Advanced>IPv6>ISATAP Tunnels

This feature allows the administrator to configure ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) is an IPv6 transmission mechanism meant to transmit IPv6 packets between dual-stack nodes over an IPv4 network. Unlike 6to4, ISATAP uses IPv4 as a virtual non broadcast multiple-access network data link layer, so that it doesn't require the underlying IPv4 network infrastructure to support multicast. To configure ISATAP tunnel administrator needs to configure the following fields:

ISATAP Subnet Prefix: This is the 64-bit subnet prefix that is assigned to the logical ISATAP subnet for this intranet. This can be obtained from your ISP or internet registry, or derived from RFC 4193.

Figure 114: ISATAP Tunnel Configuration



ISATAP TUNNELS

This page allows user to configure a new isatap tunnel.

ISATAP Tunnel Configuration

ISATAP Subnet Prefix:

End Point Address: LAN

IPv4 Address:

End Point Address: This is the endpoint address for the tunnel that starts with this router. The endpoint can be the LAN interface (assuming the LAN is an IPv4 network), or a specific LAN IPv4 address.

IPv4 Address: The end point address if not the entire LAN.

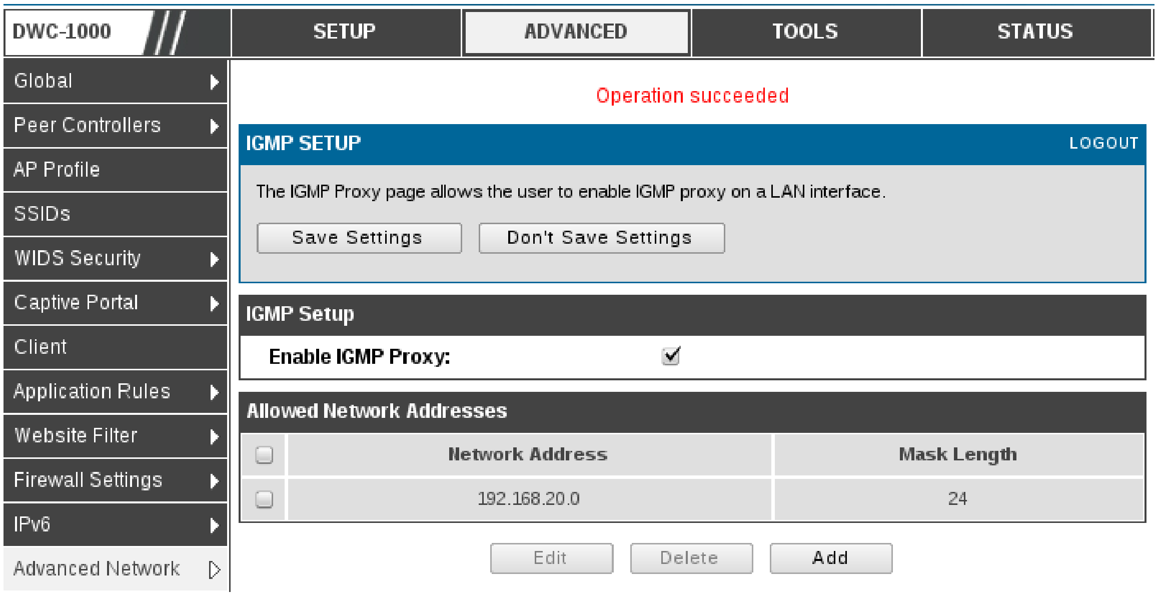
6.9 IGMP Setup

> ✍ The following feature is available upon licensed activation of VPN / Firewall features for the system.

Advanced > Advanced Network > IGMP Setup

Active IGMP snooping is referred to as IGMP proxy. When in use IGMP packets through the LAN are filtered in order to reduce the amount of multicast traffic in the network..

Figure 115: IGMP Setup



Operation succeeded

IGMP SETUP

The IGMP Proxy page allows the user to enable IGMP proxy on a LAN interface.

IGMP Setup

Enable IGMP Proxy: ☑

Allowed Network Addresses

□	Network Address	Mask Length
□	192.168.20.0	24

Enable IGMP Proxy: Check this to enable IGMP proxy on this LAN

Allowed Network Addresses: All the IP network addresses/host addresses of the multicast sources are listed here.

Network Address: The IP network or the host address of the multicast source.

Mask Length: The length of the subnet mask.

The following actions are supported from this page**:**

Add: To add a network/host address along with mask length.

Edit: To edit a network/host address along with mask length.

Delete: To delete a network/host address along with mask length..

6.10 Option Port Settings

Advanced > Advanced Network > Option Port Setup

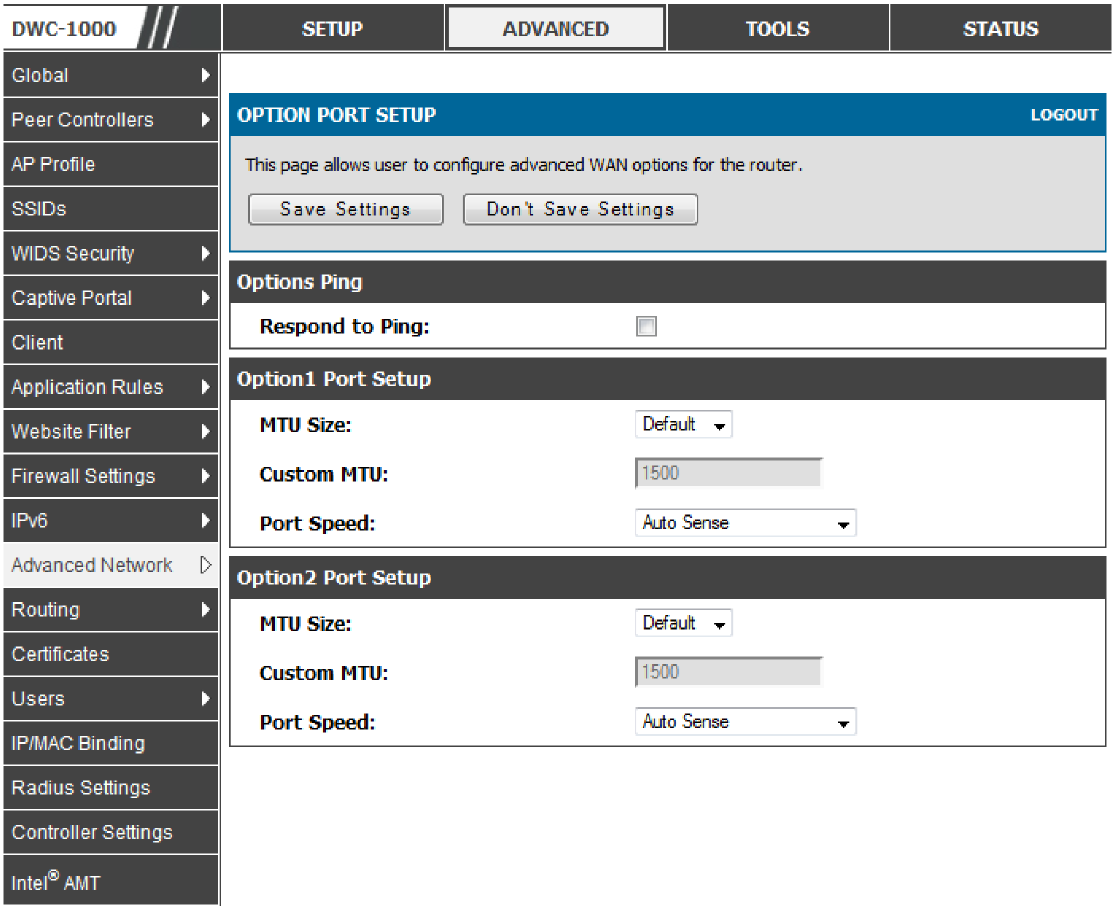
The physical port settings for each Option link can be defined here. If your ISP account defines the Option port speed or is associated with a MAC address, this information is required by the controller to ensure a smooth connection with the network.

The default MTU size supported by all ports is 1500. This is the largest packet size that can pass through the interface without fragmentation. This size can be increased, however large packets can introduce network lag and bring down the interface speed. Note that a 1500 byte size packet is the largest allowed by the Ethernet protocol at the network layer.

The port speed can be sensed by the controller when Auto is selected. With this option the optimal port settings are determined by the controller and network. The duplex (half or full) can be defined based on the port support, as well as one of three port speeds: 10 Mbps, 100 Mbps and 1000 Mbps (i.e. 1 Gbps). The default setting is 100 Mbps for all ports.

The default MAC address is defined during the manufacturing process for the interfaces, and can uniquely identify this controller. You can customize each Option port’s MAC address as needed, either by letting the Option port assume the current LAN host’s MAC address or by entering a MAC address manually.

Figure 116: Physical Option port settings



OPTION PORT SETUP

This page allows user to configure advanced WAN options for the router.

Options Ping

Respond to Ping: □

Option1 Port Setup

MTU Size: Default

Custom MTU: 1500

Port Speed: Auto Sense

Option2 Port Setup

MTU Size: Default

Custom MTU: 1500

Port Speed: Auto Sense

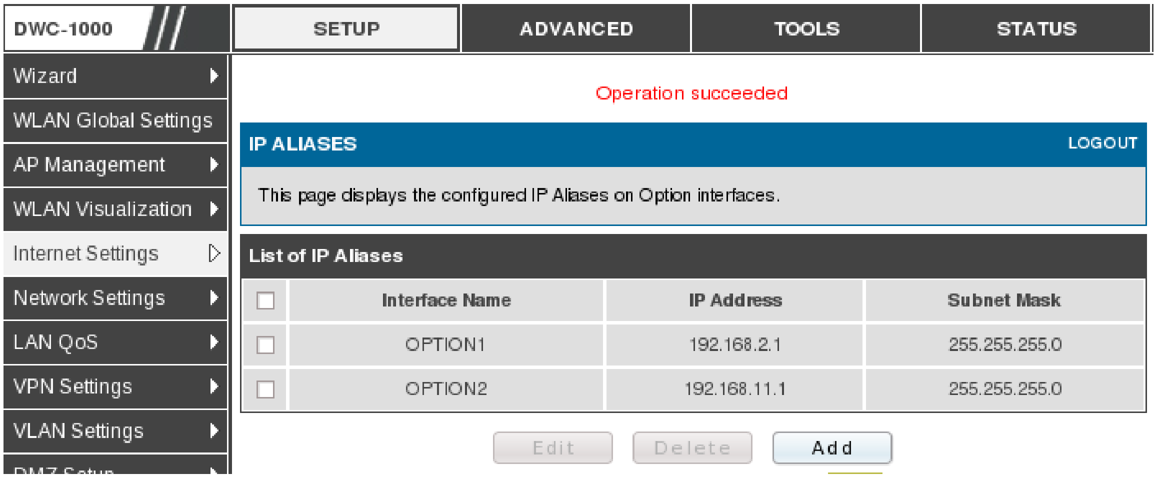
6.11 IP Aliases

> ✍ The following feature is available upon licensed activation of VPN / Firewall features for the system.

Setup > Internet Settings >IP Aliases

The List of IP Aliases displays the configured IP Aliases on the controller.

Figure 117: IP Aliases



Operation succeeded

This page displays the configured IP Aliases on Option interfaces.

□	Interface Name	IP Address	Subnet Mask
□	OPTION1	192.168.2.1	255.255.255.0
□	OPTION2	192.168.11.1	255.255.255.0

Interface Name: The interface on which the Alias was configured.

IP Address: The IP Address of the configured IP Alias.

Subnet Mask: The Subnet Mask of the configured IP Alias.

The following actions are supported from this page**:**

Edit: Opens the IP Alias configuration page to edit the selected IP Alias

Add: Opens the IP Alias configuration page to add a new IP Alias.

Delete: Deletes the selected IP Aliases.

Chapter 7. Securing the Private Network

> ✍ The following feature is available upon licensed activation of VPN / Firewall features for the system.

You can secure your network by creating and applying rules that your controller uses to selectively block and allow inbound and outbound Internet traffic. You then specify how and to whom the rules apply. To do so, you must define the following:

- Services or traffic types (examples: web browsing, VoIP, other standard services and also custom services that you define)
- Direction for the traffic by specifying the source and destination of traffic; this is done by specifying the “From Zone” (LAN/ Option /DMZ) and “To Zone” (LAN/ Option /DMZ)
- Schedules as to when the controller should apply rules
- Any Keywords (in a domain name or on a URL of a web page) that the controller should allow or block
- Rules for allowing or blocking inbound and outbound Internet traffic for specified services on specified schedules
- MAC addresses of devices that should not access the internet
- Port triggers that signal the controller to allow or block access to specified services as defined by port number
- Reports and alerts that you want the controller to send to you

You can, for example, establish restricted-access policies based on time-of-day, web addresses, and web address keywords. You can block Internet access by applications and services on the LAN, such as chat rooms or games. You can block just certain groups of PCs on your network from being accessed by the Option or public DMZ network.

7.1 Firewall Rules

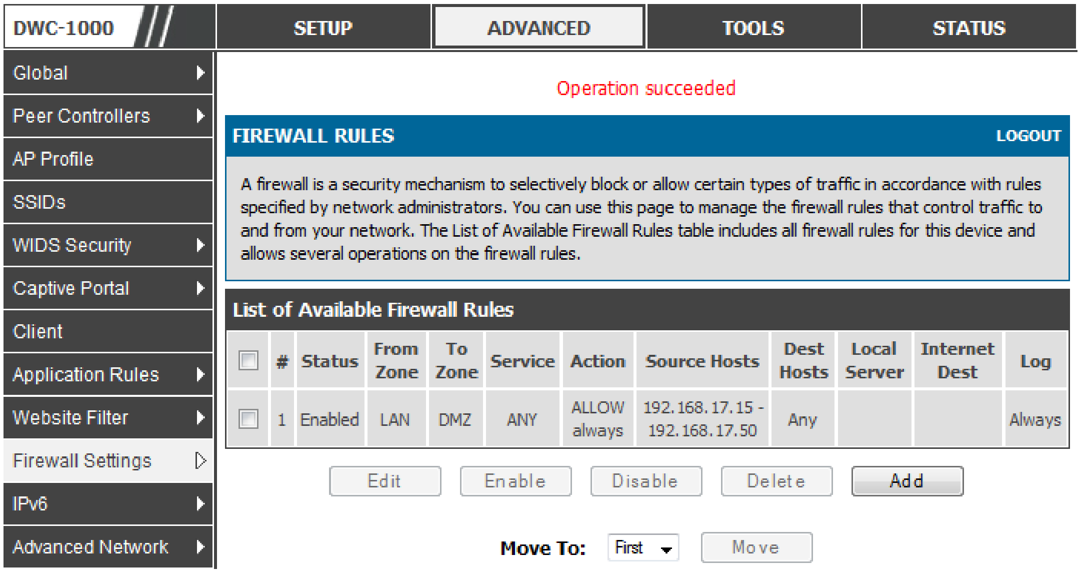
Advanced > Firewall Settings > Firewall Rules

Inbound (Option to LAN/DMZ) rules restrict access to traffic entering your network, selectively allowing only specific outside users to access specific local resources. By default all access from the insecure Option side are blocked from accessing the secure LAN, except in response to requests from the Option or DMZ. To allow outside devices to access services on the secure LAN, you must create an inbound firewall rule for each service.

If you want to allow incoming traffic, you must make the controllers Option port IP address known to the public. This is called "exposing your host." How you make your address known depends on how the Option ports are configured; for this controller you may use the IP address if a static address is assigned to the Option port, or if your Option address is dynamic a DDNS (Dynamic DNS) name can be used.

Outbound (LAN/DMZ to Option) rules restrict access to traffic leaving your network, selectively allowing only specific local users to access specific outside resources. The default outbound rule is to allow access from the secure zone (LAN) to either the public DMZ or insecure Option. On other hand the default outbound rule is to deny access from DMZ to insecure Option. You can change this default behavior in the ***Firewall Settings > Default Outbound Policy*** page. When the default outbound policy is allow always, you can to block hosts on the LAN from accessing internet services by creating an outbound firewall rule for each service.

Figure 118: List of Available Firewall Rules



Operation succeeded

FIREWALL RULES

A firewall is a security mechanism to selectively block or allow certain types of traffic in accordance with rules specified by network administrators. You can use this page to manage the firewall rules that control traffic to and from your network. The List of Available Firewall Rules table includes all firewall rules for this device and allows several operations on the firewall rules.

List of Available Firewall Rules

□	#	Status	From Zone	To Zone	Service	Action	Source Hosts	Dest Hosts	Local Server	Internet Dest	Log
□	1	Enabled	LAN	DMZ	ANY	ALLOW always	192.168.17.15 - 192.168.17.50	Any			Always

Move To: First

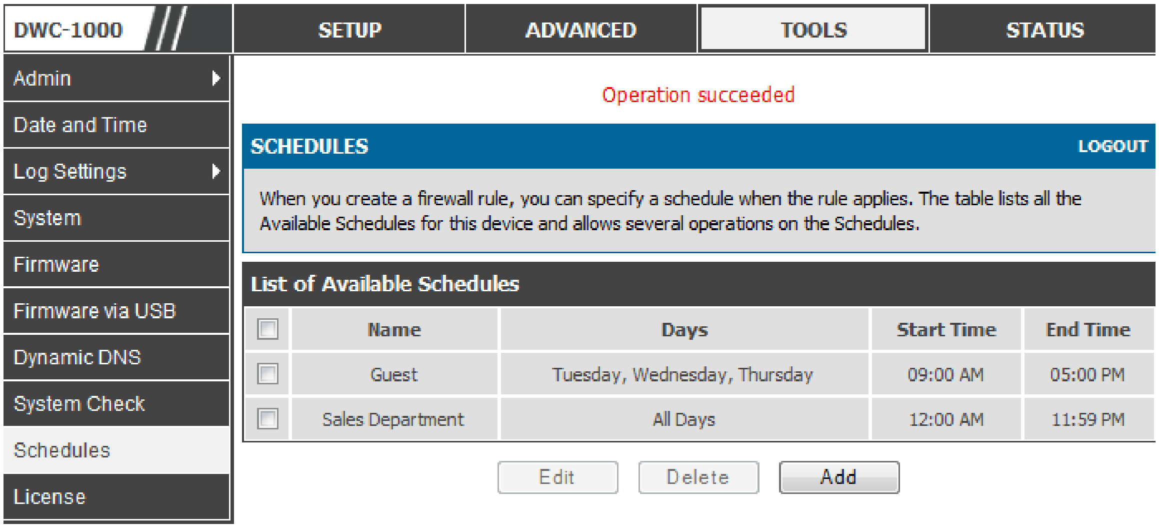
7.2 Defining Rule Schedules

Tools > Schedules

Firewall rules can be enabled or disabled automatically if they are associated with a configured schedule. The schedule configuration page allows you to define days of the week and the time of day for a new schedule, and then this schedule can be selected in the firewall rule configuration page.

> All schedules will follow the time in the controller's configured time zone. Refer to the section on choosing your Time Zone and configuring NTP servers for more information.

Figure 119: List of Available Schedules to bind to a firewall rule



Operation succeeded

SCHEDULES

When you create a firewall rule, you can specify a schedule when the rule applies. The table lists all the Available Schedules for this device and allows several operations on the Schedules.

List of Available Schedules

□	Name	Days	Start Time	End Time
□	Guest	Tuesday, Wednesday, Thursday	09:00 AM	05:00 PM
□	Sales Department	All Days	12:00 AM	11:59 PM

7.3 Configuring Firewall Rules

> ✎ The following feature is available upon licensed activation of VPN / Firewall features for the system.

Advanced > Firewall Settings > Firewall Rules

All configured firewall rules on the controller are displayed in the Firewall Rules list. This list also indicates whether the rule is enabled (active) or not, and gives a summary of the From/To zone as well as the services or users that the rule affects.

To create a new firewall rules, follow the steps below:

1. View the existing rules in the List of Available Firewall Rules table.
2. To edit or add an outbound or inbound services rule, do the following:
   - To edit a rule, click the checkbox next to the rule and click Edit to reach that rule's configuration page.
   - To add a new rule, click Add to be taken to a new rule's configuration page. Once created, the new rule is automatically added to the original table.

3. Chose the From Zone to be the source of originating traffic: either the secure LAN, public DMZ, or insecure Option. For an inbound rule Option should be selected as the From Zone.

4. Choose the To Zone to be the destination of traffic covered by this rule. If the From Zone is the Option, the To Zone can be the public DMZ or secure LAN. Similarly if the From Zone is the LAN, then the To Zone can be the public DMZ or insecure Option.

5. Parameters that define the firewall rule include the following:

   - Service: ANY means all traffic is affected by this rule. For a specific service the drop down list has common services, or you can select a custom defined service.

   - Action & Schedule: Select one of the 4 actions that this rule defines: BLOCK always, ALLOW always, BLOCK by schedule otherwise ALLOW, or ALLOW by schedule otherwise BLOCK. A schedule must be preconfigured in order for it to be available in the dropdown list to assign to this rule.

   - Source & Destination users: For each relevant category, select the users to which the rule applies:

     - Any (all users)
     - Single Address (enter an IP address)
     - Address Range (enter the appropriate IP address range)

   - Log: traffic that is filtered by this rule can be logged; this requires configuring the controller’s logging feature separately.

   - QoS Priority: Outbound rules (where To Zone = insecure Option only) can have the traffic marked with a QoS priority tag. Select a priority level:

     - Normal-Service: ToS=0 (lowest QoS)
     - Minimize-Cost: ToS=1
     - Maximize-Reliability: ToS=2
     - Maximize-Throughput: ToS=4

   - Minimize-Delay: ToS=8 (highest QoS)

6. Inbound rules can use Destination NAT (DNAT) for managing traffic from the Option. Destination NAT is available when the To Zone = DMZ or secure LAN.

   - With an inbound allow rule you can enter the internal server address that is hosting the selected service.
   - You can enable port forwarding for an incoming service specific rule (From Zone = Option) by selecting the appropriate checkbox. This will allow the selected service traffic from the internet to reach the appropriate LAN port via a port forwarding rule.
   - Translate Port Number: With port forwarding, the incoming traffic to be forwarded to the port number entered here.
   - External IP address: The rule can be bound to a specific Option interface by selecting either the primary Option or configurable port Option as the source IP address for incoming traffic.

> ✍ This controller supports multi-NAT and so the External IP address does not necessarily have to be the Option address. On a single Option interface, multiple public IP addresses are supported. If your ISP assigns you more than one public IP address, one of these can be used as your primary IP address on the Option port, and the others can be assigned to servers on the LAN or DMZ. In this way the LAN/DMZ server can be accessed from the internet by its aliased public IP address.

7. Outbound rules can use Source NAT (SNAT) in order to map (bind) all LAN/DMZ traffic matching the rule parameters to a specific Option interface or external IP address (usually provided by your ISP).

Once the new or modified rule parameters are saved, it appears in the master list of firewall rules. To enable or disable a rule, click the checkbox next to the rule in the list of firewall rules and choose Enable or Disable.

> ✍ The controller applies firewall rules in the order listed. As a general rule, you should move the strictest rules (those with the most specific services or addresses) to the top of the list. To reorder rules, click the checkbox next to a rule and click up or down.

Figure 120: Example where an outbound SNAT rule is used to map an external IP address (209.156.200.225) to a private DMZ IP address (10.30.30.30)

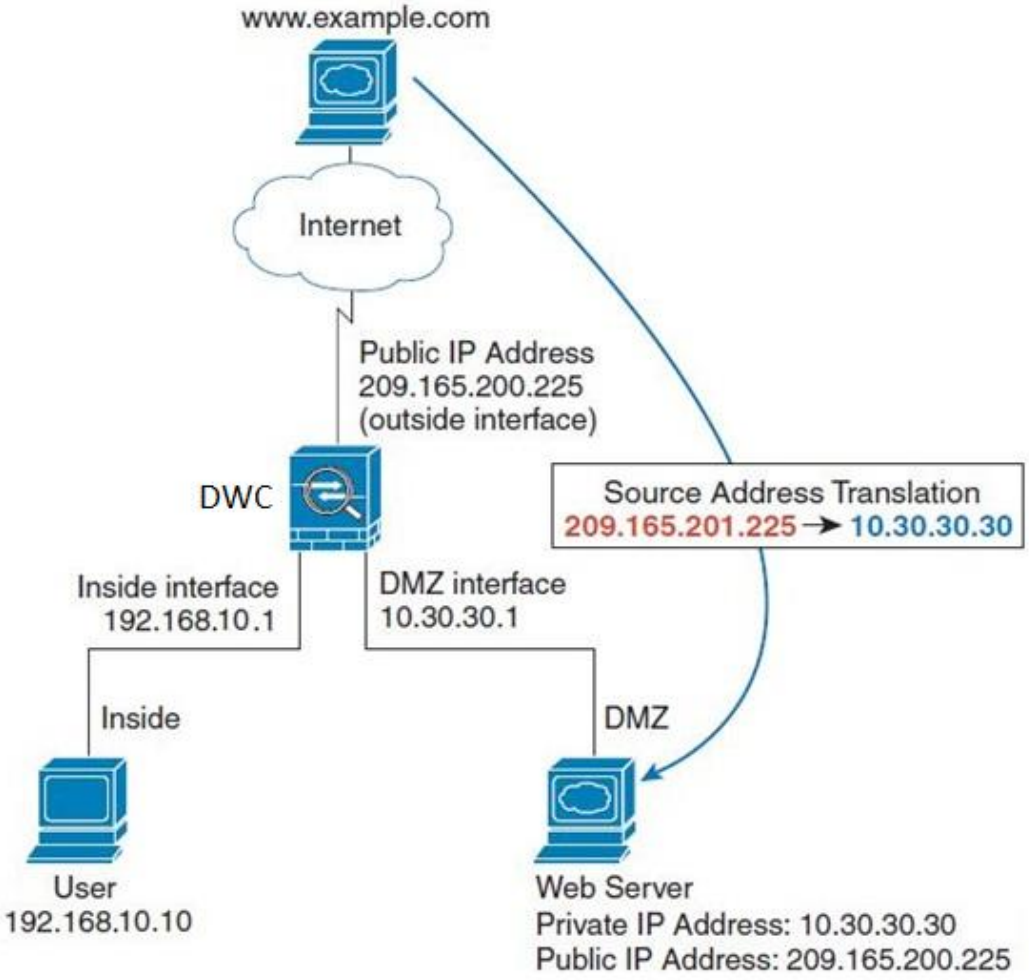
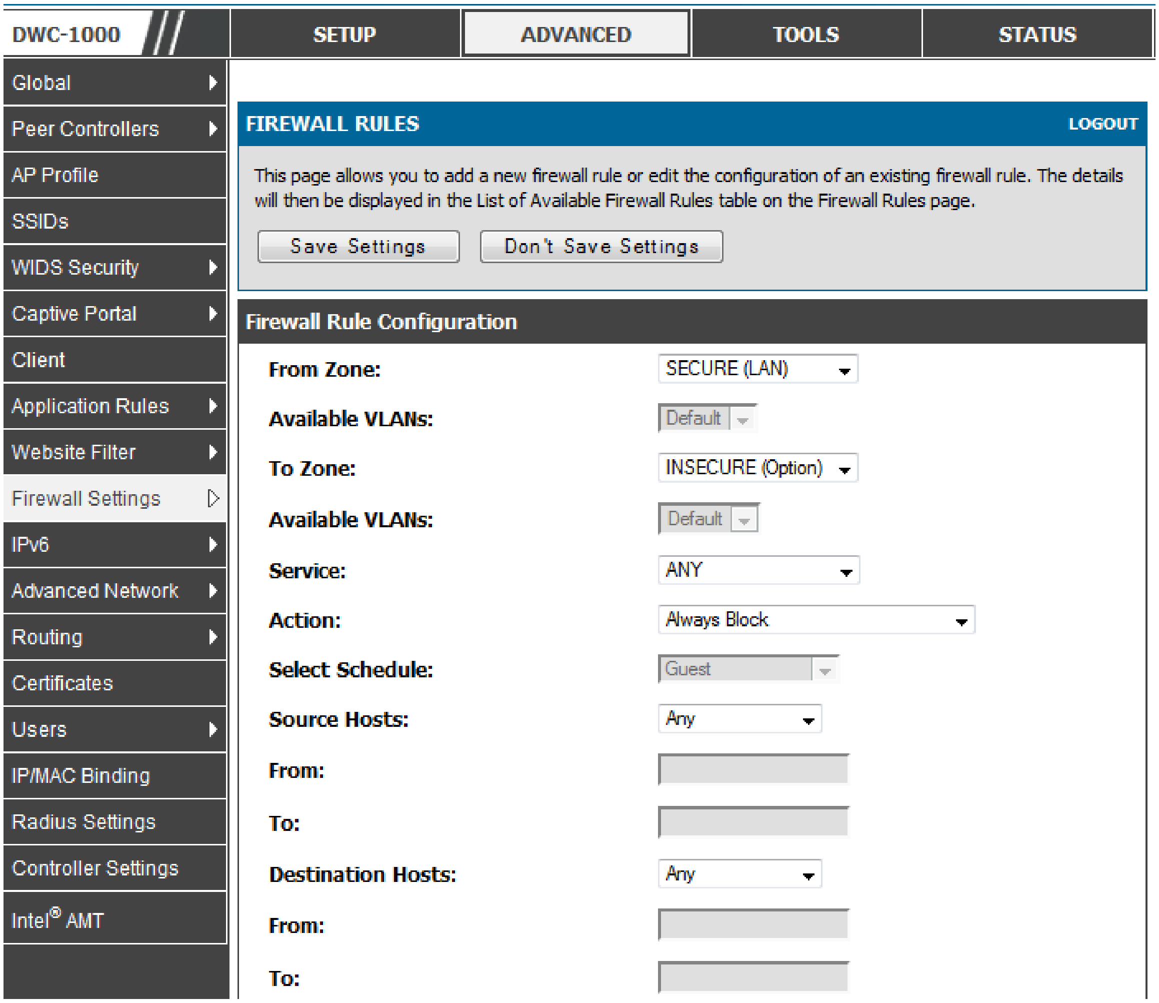


Figure 121: The firewall rule configuration page allows you to define the To/From zone, service, action, schedules, and specify source/destination IP addresses as needed.



This page allows you to add a new firewall rule or edit the configuration of an existing firewall rule. The details will then be displayed in the List of Available Firewall Rules table on the Firewall Rules page.

Firewall Rule Configuration

From Zone:	SECURE (LAN)
Available VLANs:	Default
To Zone:	INSECURE (Option)
Available VLANs:	Default
Service:	ANY
Action:	Always Block
Select Schedule:	Guest
Source Hosts:	Any
From:	
To:	
Destination Hosts:	Any
From:	
To:	

7.3.1 Firewall Rule Configuration Examples

Example 1: Allow inbound HTTP traffic to the DMZ

Situation: You host a public web server on your local DMZ network. You want to allow inbound HTTP requests from any outside IP address to the IP address of your web server at any time of day.

Solution: Create an inbound rule as follows.

Parameter	**Value**
From Zone	Insecure (Option 1/ Option2)
To Zone	Public (DMZ)
Service	HTTP
Action	ALLOW always
Send to Local Server (DNAT IP)	192.168.5.2 (web server IP address)
Destination Users	Any
Log	Never

Example 2: Allow videoconferencing from range of outside IP addresses

Situation: You want to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses (132.177.88.2 - 132.177.88.254), from a branch office.

Solution: Create an inbound rule as follows. In the example, CUSeeMe (the video conference service used) connections are allowed only from a specified range of external IP addresses.

Parameter	**Value**
From Zone	Insecure (Option 1/ Option2)
To Zone	Secure (LAN)
Service	CU-SEEME:UDP
Action	ALLOW always
Send to Local Server (DNAT IP)	192.168.10.11
Destination Users	Address Range
From	132.177.88.2
To	134.177.88.254
Enable Port Forwarding	Yes (enabled)

Example 3: Multi-NAT configuration

Situation: You want to configure multi-NAT to support multiple public IP addresses on one Option port interface.

Solution: Create an inbound rule that configures the firewall to host an additional public IP address. Associate this address with a web server on the DMZ. If you arrange with your ISP to have more than one public IP address for your use, you can use the additional public IP addresses to map to servers on your LAN. One of these public IP addresses is used as the primary IP address of the controller. This address is used to provide Internet access to your LAN PCs through NAT. The other addresses are available to map to your DMZ servers.

The following addressing scheme is used to illustrate this procedure:

- Option IP address: 10.1.0.118

- LAN IP address: 192.168.10.1; subnet 255.255.255.0
- Web server host in the DMZ, IP address: 192.168.12.222
- Access to Web server: (simulated) public IP address 10.1.0.52

Parameter	**Value**
From Zone	Insecure (Option 1/ Option 2)
To Zone	Public (DMZ)
Service	HTTP
Action	ALLOW always
Send to Local Server (DNAT IP)	192.168.12.222 (web server local IP address)
Destination Users	Single Address
From	10.1.0.52
Option Users	Any
Log	Never

Example 4: Bloc

Example 4: Block traffic by schedule if generated from specific range of machines

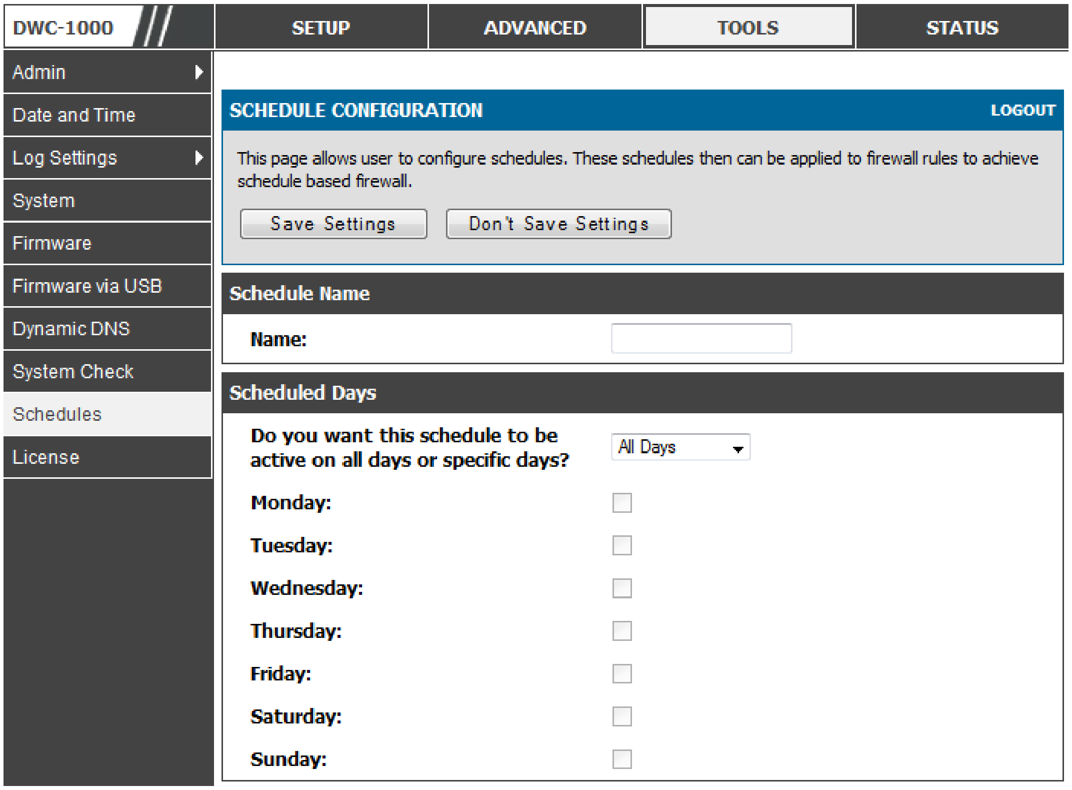
Use Case: Block all HTTP traffic on the weekends if the request originates from a specific group of machines in the LAN having a known range of IP addresses, and anyone coming in through the Network from the Option (i.e. all remote users).

Configuration:

1. Setup a schedule:

- To setup a schedule that affects traffic on weekends only, navigate to Security: Schedule, and name the schedule "Weekend"
- Define "weekend" to mean 12 am Saturday morning to 12 am Monday morning – all day Saturday & Sunday
- In the Scheduled days box, check that you want the schedule to be active for "specific days". Select "Saturday" and "Sunday"
- In the scheduled time of day, select "all day" – this will apply the schedule between 12 am to 11:59 pm of the selected day.
- Click apply – now schedule "Weekend" isolates all day Saturday and Sunday from the rest of the week.

Figure 122: Schedule configuration for the above example.



SCHEDULE CONFIGURATION

This page allows user to configure schedules. These schedules then can be applied to firewall rules to achieve schedule based firewall.

Schedule Name

Name:

Scheduled Days

Do you want this schedule to be active on all days or specific days? All Days

Monday: □

Tuesday: □

Wednesday: □

Thursday: □

Friday: □

Saturday: □

Sunday: □

2. Since we are trying to block HTTP requests, it is a service with To Zone: Insecure (Option 1/ Option2) that is to be blocked according to schedule "Weekend".

3. Select the Action to “Block by Schedule, otherwise allow”. This will take a predefined schedule and make sure the rule is a blocking rule during the defined dates/times. All other times outside the schedule will not be affected by this firewall blocking rule

4. As we defined our schedule in schedule “Weekend”, this is available in the dropdown menu

5. We want to block the IP range assigned to the marketing group. Let’s say they have IP 192.168.10.20 to 192.168.10.30. On the Source Users dropdown, select Address Range and add this IP range as the from and To IP addresses.

6. We want to block all HTTP traffic to any services going to the insecure zone. The Destination Users dropdown should be “any”.

7. We don’t need to change default QoS priority or Logging (unless desired) – clicking apply will add this firewall rule to the list of firewall rules.

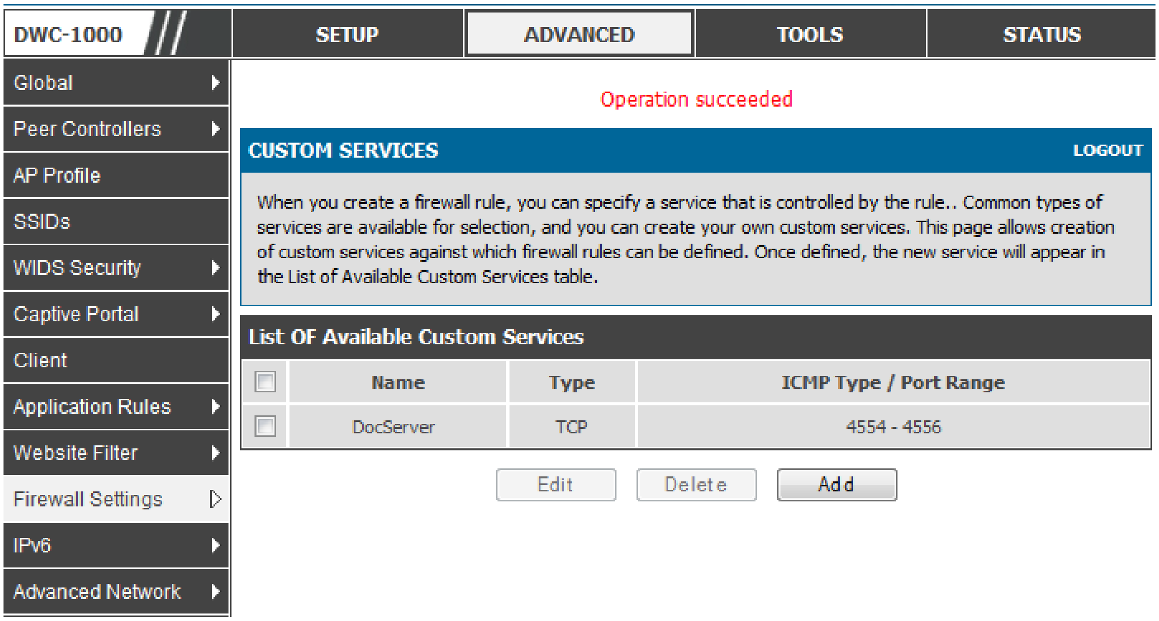
8. The last step is to enable this firewall rule. Select the rule, and click “enable” below the list to make sure the firewall rule is active

7.4 Security on Custom Services

Advanced > Firewall Settings > Custom Services

Custom services can be defined to add to the list of services available during firewall rule configuration. While common services have known TCP/UDP/ICMP ports for traffic, many custom or uncommon applications exist in the LAN or Option. In the custom service configuration menu you can define a range of ports and identify the traffic type (TCP/UDP/ICMP) for this service. Once defined, the new service will appear in the services list of the firewall rules configuration menu.

Figure 123: List of user defined services.



Operation succeeded

CUSTOM SERVICES

When you create a firewall rule, you can specify a service that is controlled by the rule.. Common types of services are available for selection, and you can create your own custom services. This page allows creation of custom services against which firewall rules can be defined. Once defined, the new service will appear in the List of Available Custom Services table.

List OF Available Custom Services

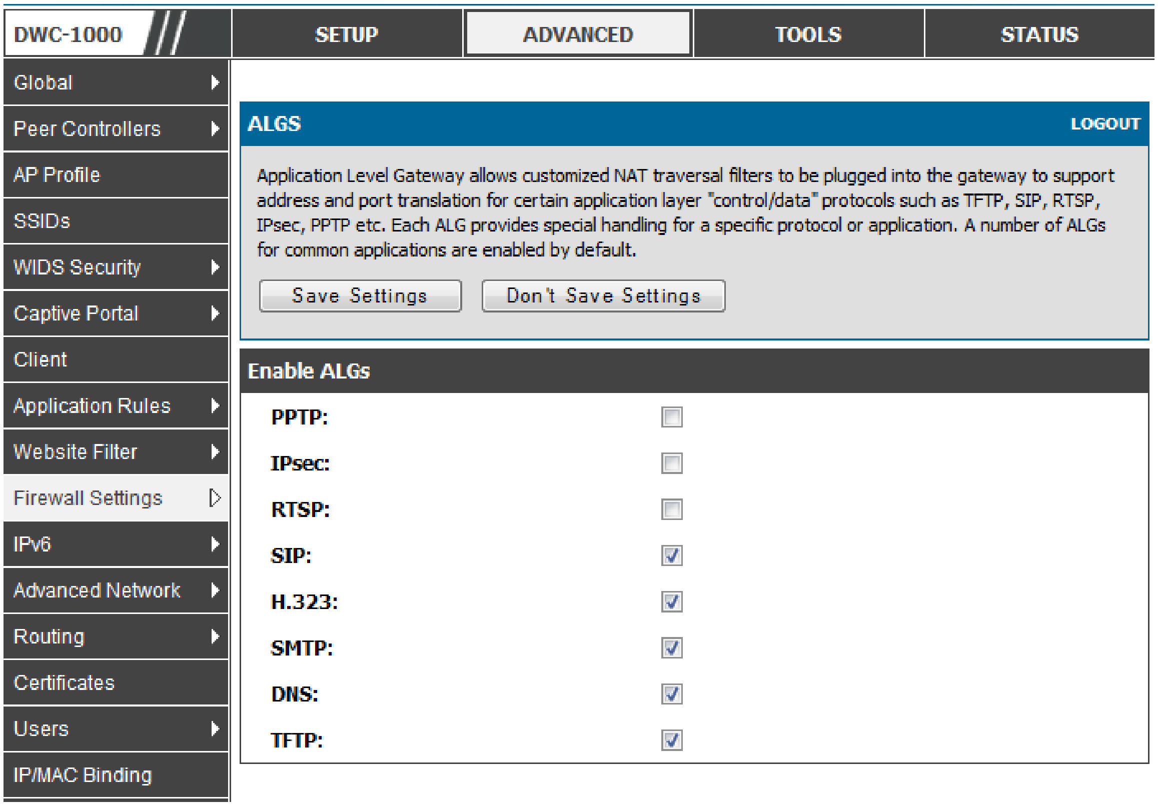
□	Name	Type	ICMP Type / Port Range
□	DocServer	TCP	4554 - 4556

7.5 ALG support

Advanced > Firewall Settings > ALGs

Application Level Gateways (ALGs) are security component that enhance the firewall and NAT support of this controller to seamlessly support application layer protocols. In some cases enabling the ALG will allow the firewall to use dynamic ephemeral TCP/ UDP ports to communicate with the known ports a particular client application (such as H.323 or RTSP) requires, without which the admin would have to open large number of ports to accomplish the same support. Because the ALG understands the protocol used by the specific application that it supports, it is a very secure and efficient way of introducing support for client applications through the controller’s firewall.

Figure 124: Available ALG support on the controller.



Application Level Gateway allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as TFTP, SIP, RTSP, IPsec, PPTP etc. Each ALG provides special handling for a specific protocol or application. A number of ALGs for common applications are enabled by default.

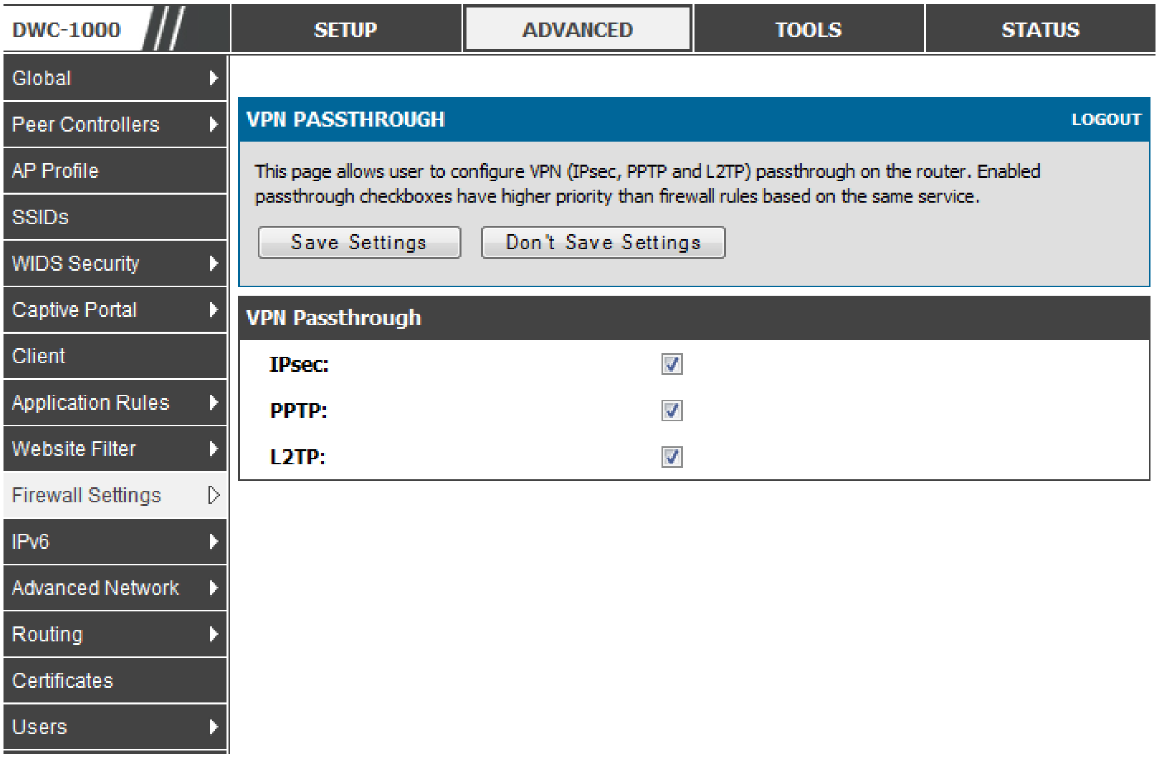
PPTP:	□
IPsec:	□
RTSP:	□
SIP:	☑
H.323:	☑
SMTP:	☑
DNS:	☑
TFTP:	☑

7.6 VPN Passthrough for Firewall

Advanced > Firewall Settings > VPN Passthrough

This controller’s firewall settings can be configured to allow encrypted VPN traffic for IPsec, PPTP, and L2TP VPN tunnel connections between the LAN and internet. A specific firewall rule or service is not appropriate to introduce this passthrough support; instead the appropriate check boxes in the VPN Passthrough page must be enabled.

Figure 125: Passthrough options for VPN tunnels



This page allows user to configure VPN (IPsec, PPTP and L2TP) passthrough on the router. Enabled passthrough checkboxes have higher priority than firewall rules based on the same service.

IPsec: ☑

PPTP: ☑

L2TP: ☑

7.7 Client

Advanced > Client

The Known Client Summary shows the wireless clients currently in the Known Client Database and allows you to add new clients or modify existing clients to the database.

MAC Address: Shows the MAC address of the known client.

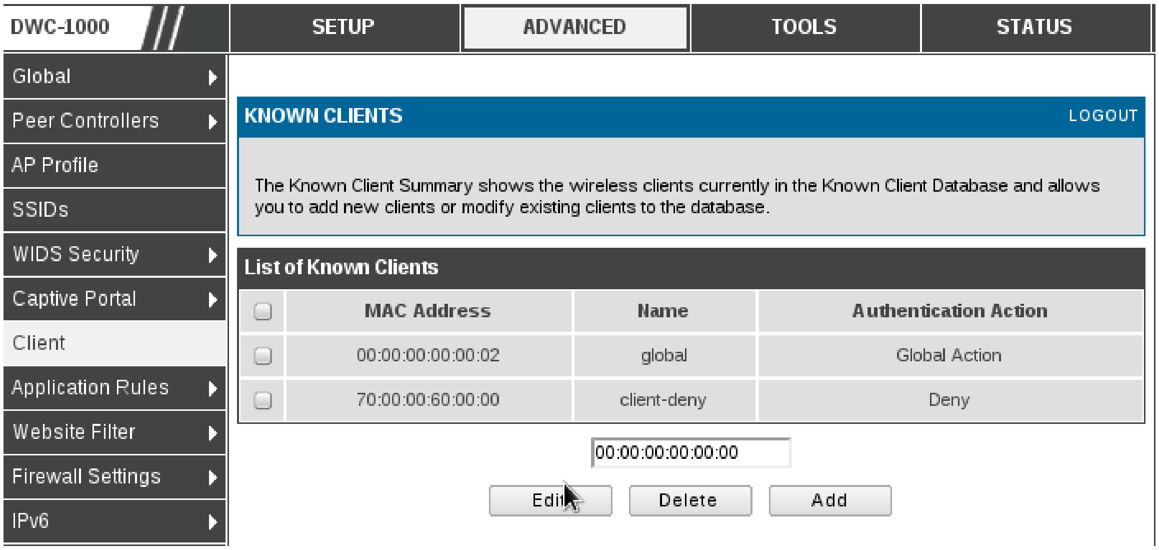
Name: Shows the descriptive name configured for the client when it was added to the Known Client database.

Authentication Action: When MAC authentication is enabled on the network, this field shows the action to take on a wireless client. The following options are available.

Grant: Allow the client with the specified MAC address to access the network. **Deny**: Prohibit the client with the specified MAC address from accessing the network.

Global Action: Use the global white-list or black-list action configured on the Advanced Global Configuration page to determine how to handle the client.

Figure 126: List of Known Clients



The Known Client Summary shows the wireless clients currently in the Known Client Database and allows you to add new clients or modify existing clients to the database.

List of Known Clients

□	MAC Address	Name	Authentication Action
□	00:00:00:00:00:02	global	Global Action
□	70:00:00:60:00:00	client-deny	Deny

00:00:00:00:00:00

The following actions are supported from this page:

Add: Add a client with the MAC address you enter in the field to the Known Client database.

Delete: Removes the selected client from the Known Client database.

Edit: changes the setting of particular MAC address

7.8 Application Rules

> The following feature is available upon licensed activation of VPN / Firewall features for the system.

Advanced > Application Rules > Application Rules

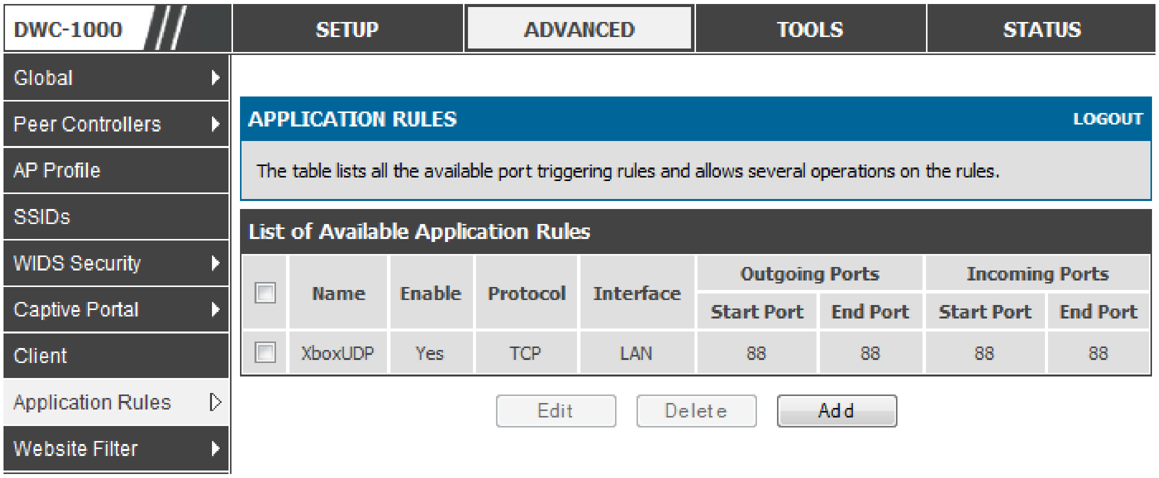
Application rules are also referred to as port triggering. This feature allows devices on the LAN or DMZ to request one or more ports to be forwarded to them. Port triggering waits for an outbound request from the LAN/DMZ on one of the defined outgoing ports, and then opens an incoming port for that specified type of traffic. This can be thought of as a form of dynamic port forwarding while an application is transmitting data over the opened outgoing or incoming port(s).

Port triggering application rules are more flexible than static port forwarding that is an available option when configuring firewall rules. This is because a port triggering rule does not have to reference a specific LAN IP or IP range. As well ports are not left open when not in use, thereby providing a level of security that port forwarding does not offer.

> ✍ Port triggering is not appropriate for servers on the LAN, since there is a dependency on the LAN device making an outgoing connection before incoming ports are opened.

Some applications require that when external devices connect to them, they receive data on a specific port or range of ports in order to function properly. The controller must send all incoming data for that application only on the required port or range of ports. The controller has a list of common applications and games with corresponding outbound and inbound ports to open. You can also specify a port triggering rule by defining the type of traffic (TCP or UDP) and the range of incoming and outgoing ports to open when enabled.

Figure 127: List of Available Application Rules showing 4 unique rules



APPLICATION RULES

The table lists all the available port triggering rules and allows several operations on the rules.

List of Available Application Rules

	Name	Enable	Protocol	Interface	Outgoing Ports		Incoming Ports	
					Start Port	End Port	Start Port	End Port
□	XboxUDP	Yes	TCP	LAN	88	88	88	88

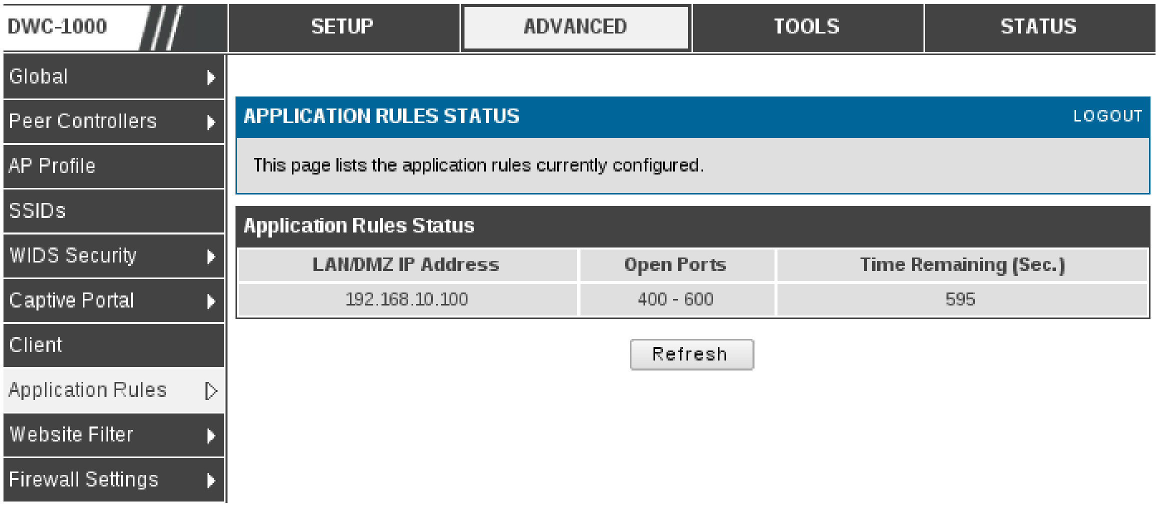
The application rule status page will list any active rules, i.e. incoming ports that are being triggered based on outbound requests from a defined outgoing port.

7.9 Application Rules Status

Advanced > Application Rules > Application Rules Status

This page allows displaying the list of available application rules and corresponding status

Figure 128: List of Available Application Rules and corresponding status



This page lists the application rules currently configured.

Application Rules Status

LAN/DMZ IP Address	Open Ports	Time Remaining (Sec.)
192.168.10.100	400 - 600	595

.

7.10 Web Content Filtering

The gateway offers some standard web filtering options to allow the admin to easily create internet access policies between the secure LAN and insecure Option. Instead of creating policies based on the type of traffic (as is the case when using firewall rules), web based content itself can be used to determine if traffic is allowed or dropped.

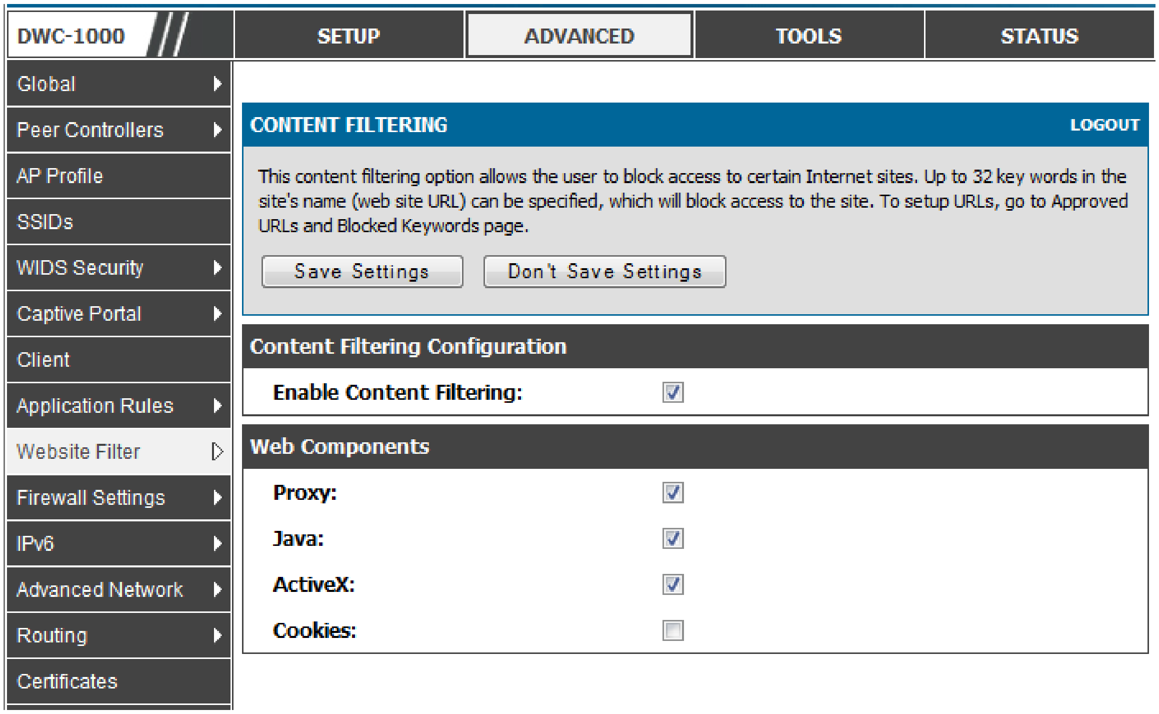
7.10.1 Content Filtering

> ✍ The following feature is available upon licensed activation of VPN / Firewall features for the system.

Advanced > Website Filter > Content Filtering

Content filtering must be enabled to configure and use the subsequent features (list of Trusted Domains, filtering on Blocked Keywords, etc.). Proxy servers, which can be used to circumvent certain firewall rules and thus a potential security gap, can be blocked for all LAN devices. Java applets can be prevented from being downloaded from internet sites, and similarly the gateway can prevent ActiveX controls from being downloaded via Internet Explorer. For added security cookies, which typically contain session information, can be blocked as well for all devices on the private network.

Figure 129: Content Filtering used to block access to proxy servers and prevent ActiveX controls from being downloaded



This content filtering option allows the user to block access to certain Internet sites. Up to 32 key words in the site's name (web site URL) can be specified, which will block access to the site. To setup URLs, go to Approved URLs and Blocked Keywords page.

Content Filtering Configuration

Enable Content Filtering: ☑

Web Components

Proxy: ☑

Java: ☑

ActiveX: ☑

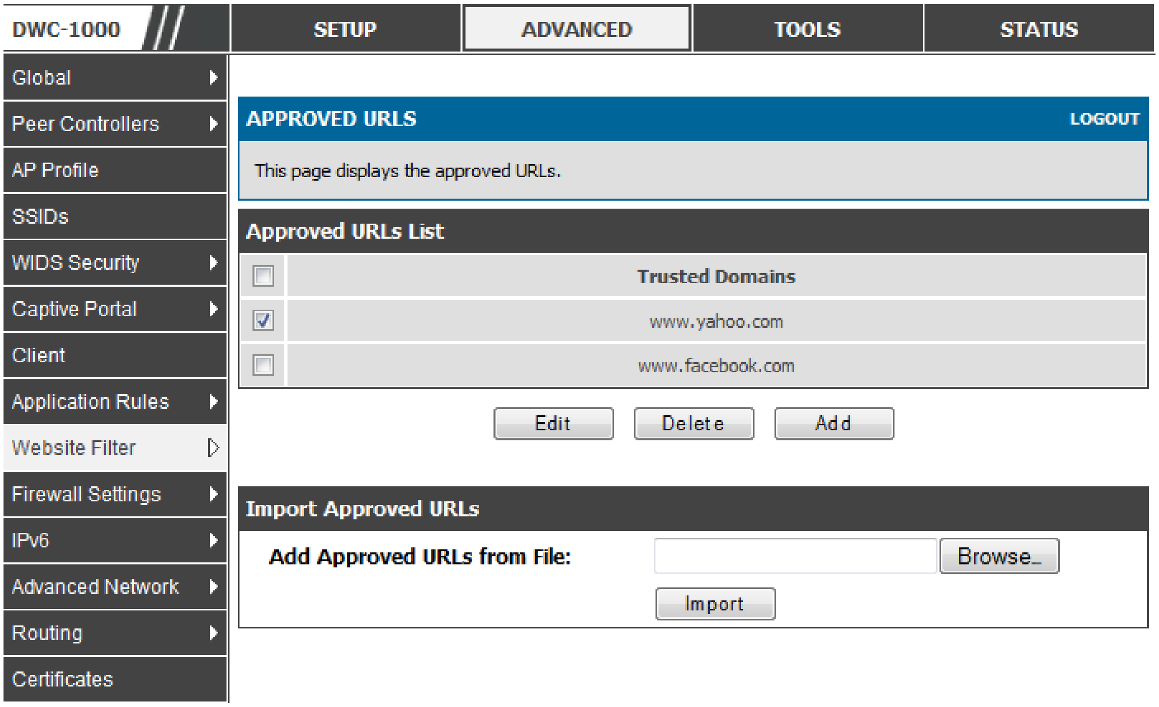
Cookies: □

7.10.2 Approved URLs

Advanced > Website Filter > Approved URLs

The Approved URLs is an acceptance list for all URL domain names. Domains added to this list are allowed in any form. For example, if the domain "yahoo" is added to this list then all of the following URL's are permitted access from the LAN: www.yahoo.com, yahoo.co.uk, etc. Import/export from a text or CSV file for Approved URLs is also supported

Figure 130: Two trusted domains added to the Approved URLs List



APPROVED URLS

This page displays the approved URLs.

Approved URLs List

□	Trusted Domains
☑	www.yahoo.com
□	www.facebook.com

Import Approved URLs

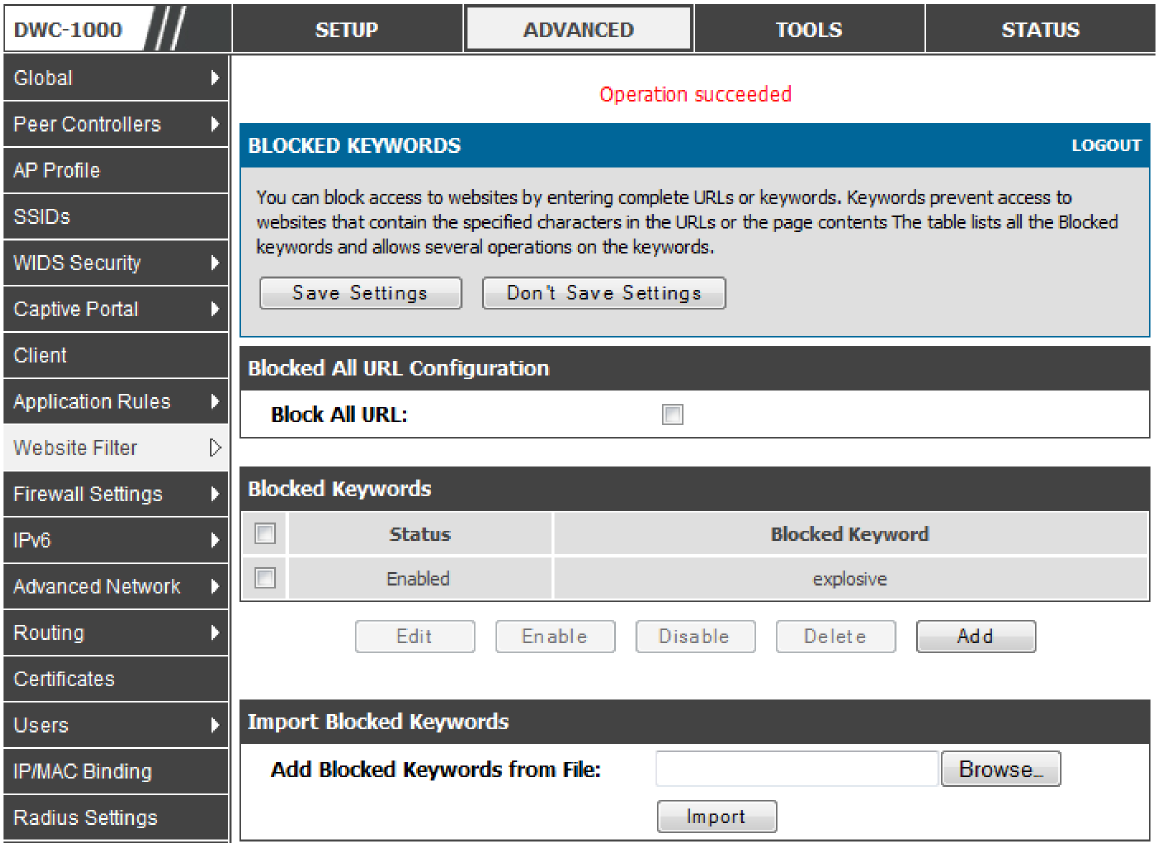
Add Approved URLs from File:

7.10.3 Blocked Keywords

Advanced > Website Filter > Blocked Keywords

Keyword blocking allows you to block all website URL's or site content that contains the keywords in the configured list. This is lower priority than the Approved URL List; i.e. if the blocked keyword is present in a site allowed by a Trusted Domain in the Approved URL List, then access to that site will be allowed. Import/export from a text or CSV file for keyword blocking is also supported.

Figure 131: One keyword added to the block list



Operation succeeded

BLOCKED KEYWORDS

You can block access to websites by entering complete URLs or keywords. Keywords prevent access to websites that contain the specified characters in the URLs or the page contents The table lists all the Blocked keywords and allows several operations on the keywords.

Blocked All URL Configuration

Block All URL: □

Blocked Keywords

□	Status	Blocked Keyword
□	Enabled	explosive

Import Blocked Keywords

Add Blocked Keywords from File:

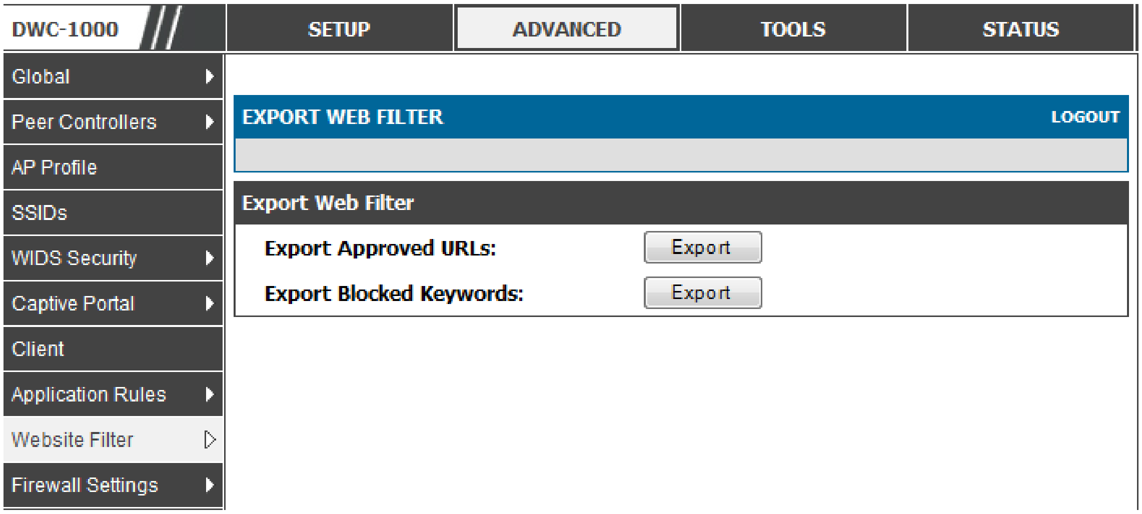
7.10.4 Export Web Filter

Advanced > Website Filter > Export

Export Approved URLs: Feature enables the user to export the URLs to be allowed to a csv file which can then be downloaded to the local host. The user has to click the export button to get the csv file.

Export Blocked Keywords: This feature enables the user to export the keywords to be blocked to a csv file which can then be downloaded to the local host. The user has to click the export button to get the csv file.

Figure 132: Export Approved URL list



Export Approved URLs: Export

Export Blocked Keywords: Export

7.11 Content Keeper Support (Web Content Filtering)

Web Content Filtering (WCF) is branded as Content Keeper. It monitors, manages and controls all web traffic and fully examines new and/or unknown sites in real time as the data passes through the appliance. It manages and controls downloads and desktop access to web content. Content Keeper has support for content list blocking and category filtering (considered Dynamic WCF).

Syslog support for Content Keeper permits the appliance to continuously off-load log files as the data is accumulated, rather than tying up the users network with one huge daily log file off-load.

7.12 Dynamic WCF

Advanced>Website Filter>Category Filtering

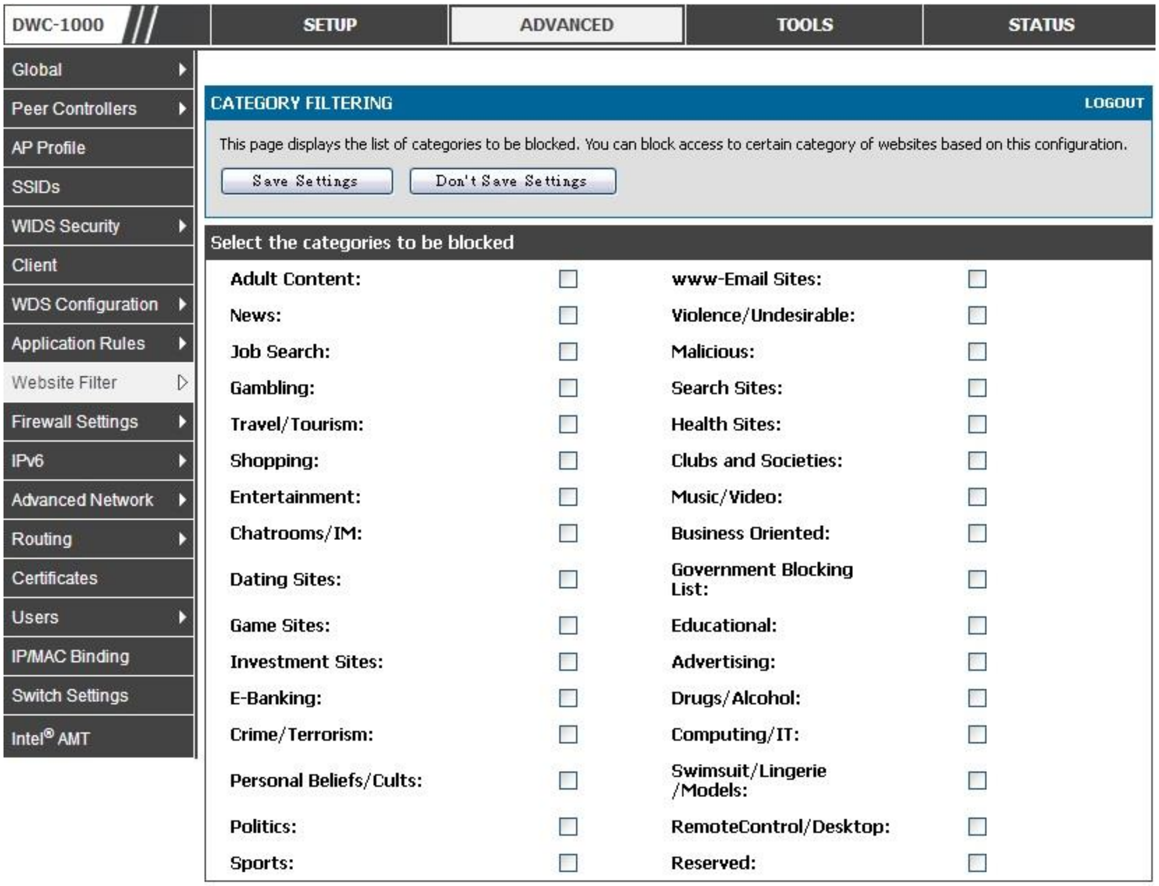
This feature allows the administrator to block access from a range of web content categories. The system needs the WCF licensee and then Content Filtering option, which allows the user to filter out internet sites, needs to be enabled.

The Dynamic Content Filtering configuration page will let the administrator choose from a range of pre-defined categories to be blocked. When enabled, access to a website belonging to one of these configured categories will be blocked with an error page.

- Adult Content: Sites that host explicit sex content, nudity and sites that use profanity.
- News: Sites that offer news and information on current events, including newspapers, broadcasters and other publishers.
- Job Search: Sites that offer job listings, interview coaching and other employment-related services.
- Gambling: Sites that offer online gambling or information about gambling.
- Travel/Tourism: Sites with travel and tourism information like city maps and services including planning trips, reservations for bus/train/airlines, hotel booking etc.
- Shopping: Online shops, catalogs, auction sites and classified ads etc.
- Entertainment: Websites for TV, movies, entertainment news etc. and sites hosting video content of movies, TV streaming etc.
- Chatrooms/IM: Social networking sites, chartrooms and instant messaging sites.
- Dating Sites: Online dating, matchmaking, relationship advice, personal ads and web pages related to marriage.
- Game Sites: Sites that offer online games, MORPG and information about computer games, cheat codes etc.
- Investment Sites: Sites for brokerages, trusts, insurance and other investments related organizations.
- E-banking: Sites providing online banking services offered by financial institutions
- Crime/Terrorism: Sites providing information on anti-social activities like murder, sabotage, bombing etc.
- Personal Beliefs/Cults: Sites about religion, places of worship, religious groups, and occultism.
- Politics: Sites about politics, elections and legislation and sites that promote a politician or political party.
- Sports: Sites about sports teams, fan clubs, and generally about all kinds of sports.

- www Email Sites: Websites that allow users to send and/or receive email through a web accessible email account.

Figure 133: Category Filtering options



CATEGORY FILTERING

This page displays the list of categories to be blocked. You can block access to certain category of websites based on this configuration.

Select the categories to be blocked

Adult Content:	□	www-Email Sites:	□
News:	□	Violence/Undesirable:	□
Job Search:	□	Malicious:	□
Gambling:	□	Search Sites:	□
Travel/Tourism:	□	Health Sites:	□
Shopping:	□	Clubs and Societies:	□
Entertainment:	□	Music/Video:	□
Chatrooms/IM:	□	Business Oriented:	□
Dating Sites:	□	Government Blocking List:	□
Game Sites:	□	Educational:	□
Investment Sites:	□	Advertising:	□
E-Banking:	□	Drugs/Alcohol:	□
Crime/Terrorism:	□	Computing/IT:	□
Personal Beliefs/Cults:	□	Swimsuit/Lingerie /Models:	□
Politics:	□	RemoteControl/Desktop:	□
Sports:	□	Reserved:	□

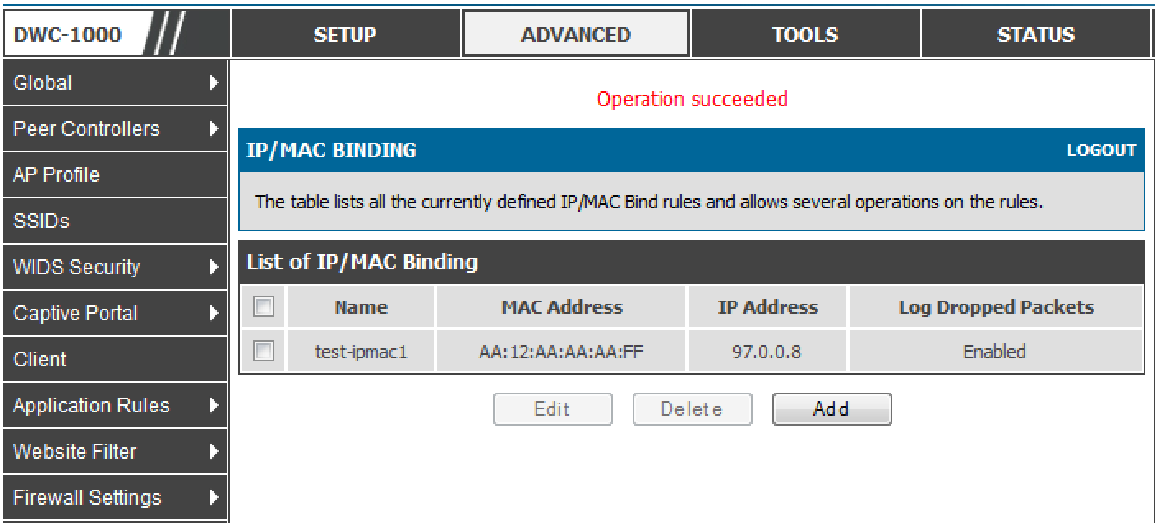
7.13 IP/MAC Binding

Advanced > IP/MAC Binding

Another available security measure is to only allow outbound traffic (from the LAN to Option) when the LAN node has an IP address matching the MAC address bound to it. This is IP/MAC Binding, and by enforcing the gateway to validate the source traffic’s IP address with the unique MAC Address of the configured LAN node, the administrator can ensure traffic from that IP address is not spoofed. In the event of a violation (i.e.

the traffic's source IP address doesn't match up with the expected MAC address having the same IP address) the packets will be dropped and can be logged for diagnosis.

Figure 134: Example binding a LAN host's MAC Address to a served IP address



Operation succeeded

IP/MAC BINDING

The table lists all the currently defined IP/MAC Bind rules and allows several operations on the rules.

List of IP/MAC Binding

□	Name	MAC Address	IP Address	Log Dropped Packets
□	test-ipmac1	AA:12:AA:AA:AA:FF	97.0.0.8	Enabled

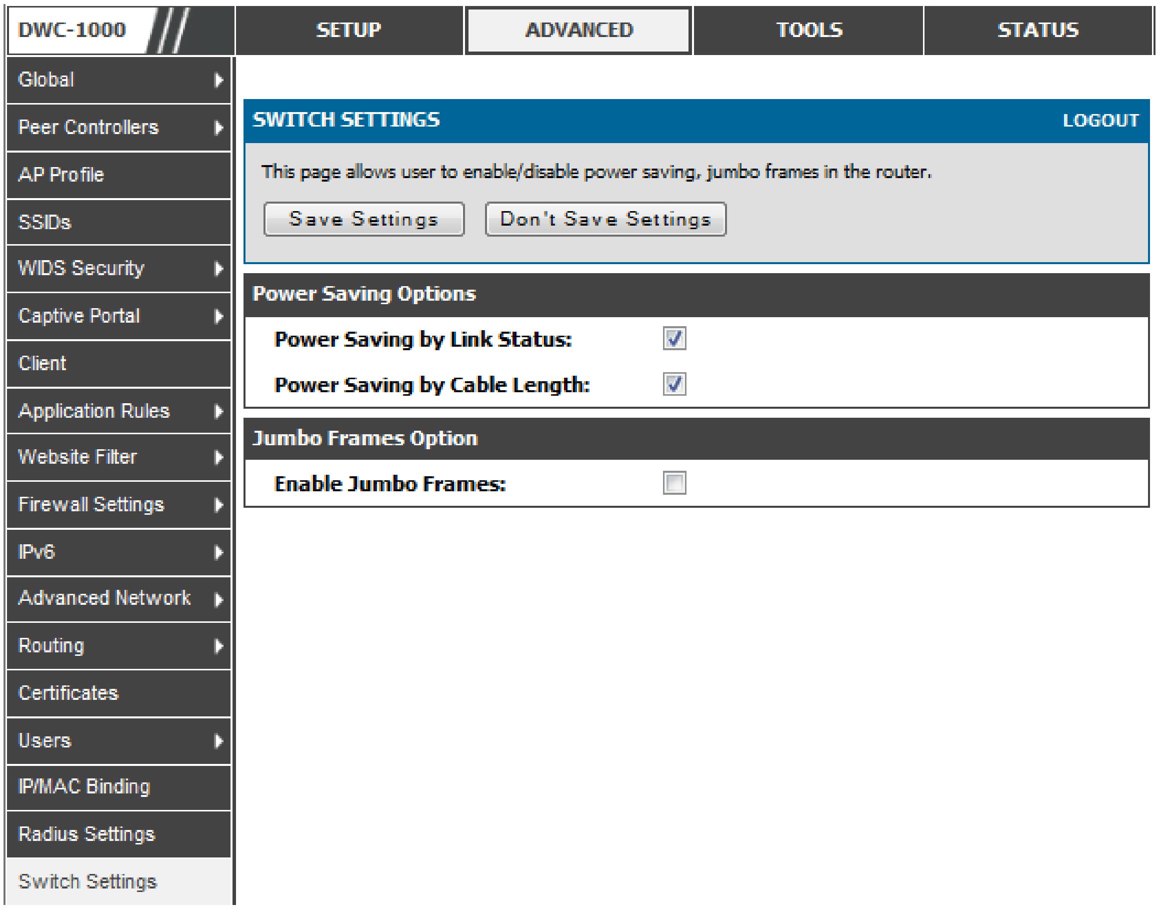
In the above example, if there is an IP/MAC Binding violation, the violating packet will be dropped and logs will be captured.

7.14 Switch Settings

Advanced > Switch Settings

This page allows user to enable/disable power saving, jumbo frames in the router.

Figure 135: Switch settings



SWITCH SETTINGS

This page allows user to enable/disable power saving, jumbo frames in the router.

Power Saving Options

Power Saving by Link Status: ☑

Power Saving by Cable Length: ☑

Jumbo Frames Option

Enable Jumbo Frames: □

Power Saving State: When enabled, the total power to the LAN controller is dependent on the number of connected ports. The overall current draw when a single port is connected is less than when all of the available LAN ports have an active Ethernet connection.

Length Detection State: When enabled the LAN controller will reduce the overall current supplied to the LAN port when a small cable length is connected to that port. Longer cables have higher resistance than shorter cables and require more power to transmit packets over that distance. This option will reduce the power to a LAN port if an Ethernet cable of less than 10 ft. is detected as being connected to that port.

Jumbo Frames Option: When enabled, LAN side devices can exchange traffic containing jumbo frames.

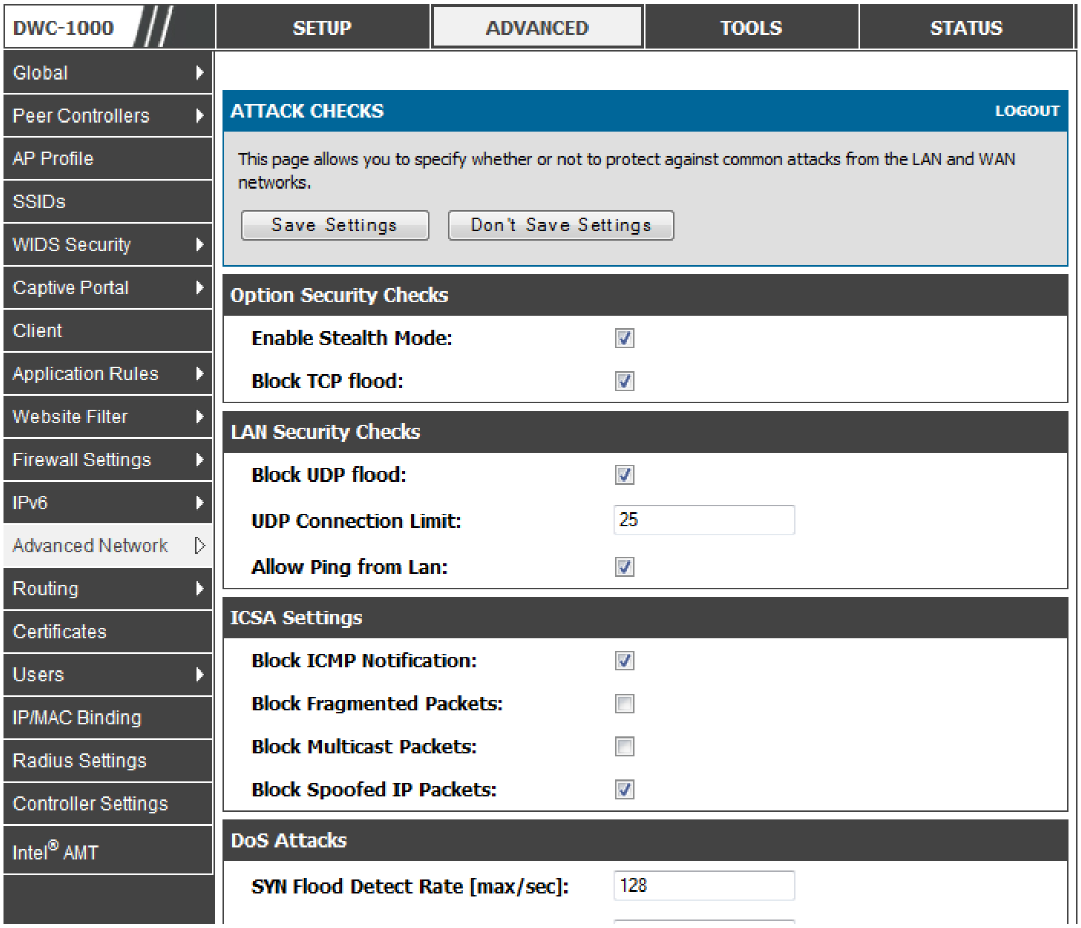
7.15 Protecting from Internet Attacks

Advanced > Advanced Network > Attack Checks

Attacks can be malicious security breaches or unintentional network issues that render the controller unusable. Attack checks allow you to manage Option security threats such as continual ping requests and discovery via ARP scans. TCP and UDP flood attack checks can be enabled to manage extreme usage of Option resources.

Additionally certain Denial-of-Service (DoS) attacks can be blocked. These attacks, if uninhibited, can use up processing power and bandwidth and prevent regular network services from running normally. ICMP packet flooding, SYN traffic flooding, and Echo storm thresholds can be configured to temporarily suspect traffic from the offending source.

Figure 136: Protecting the controller and LAN from internet attacks



ATTACK CHECKS

This page allows you to specify whether or not to protect against common attacks from the LAN and WAN networks.

Option Security Checks

Enable Stealth Mode: ☑

Block TCP flood: ☑

LAN Security Checks

Block UDP flood: ☑

UDP Connection Limit: 25

Allow Ping from Lan: ☑

ICSA Settings

Block ICMP Notification: ☑

Block Fragmented Packets: □

Block Multicast Packets: □

Block Spoofed IP Packets: ☑

DoS Attacks

SYN Flood Detect Rate [max/sec]: 128

Chapter 8. IPsec / PPTP / L2TP VPN

> ✍ The following feature is available upon licensed activation of VPN / Firewall features for the system.

A VPN provides a secure communication channel ("tunnel") between two gateway controller or a remote PC client. The following types of tunnels can be created:

- **Gateway-to-gateway VPN**: to connect two or more controller to secure traffic between remote sites.
- **Remote Client** (client-to-gateway VPN tunnel): A remote client initiates a VPN tunnel as the IP address of the remote PC client is not known in advance. The gateway in this case acts as a responder.

Remote client behind a NAT controller: The client has a dynamic IP address and is behind a NAT controller. The remote PC client at the NAT controller initiates a VPN tunnel as the IP address of the remote NAT controller is not known in advance. The gateway Option port acts as responder.

Figure 137: Example of Gateway-to-Gateway IPsec VPN tunnel using two DWC controllers connected to the Internet

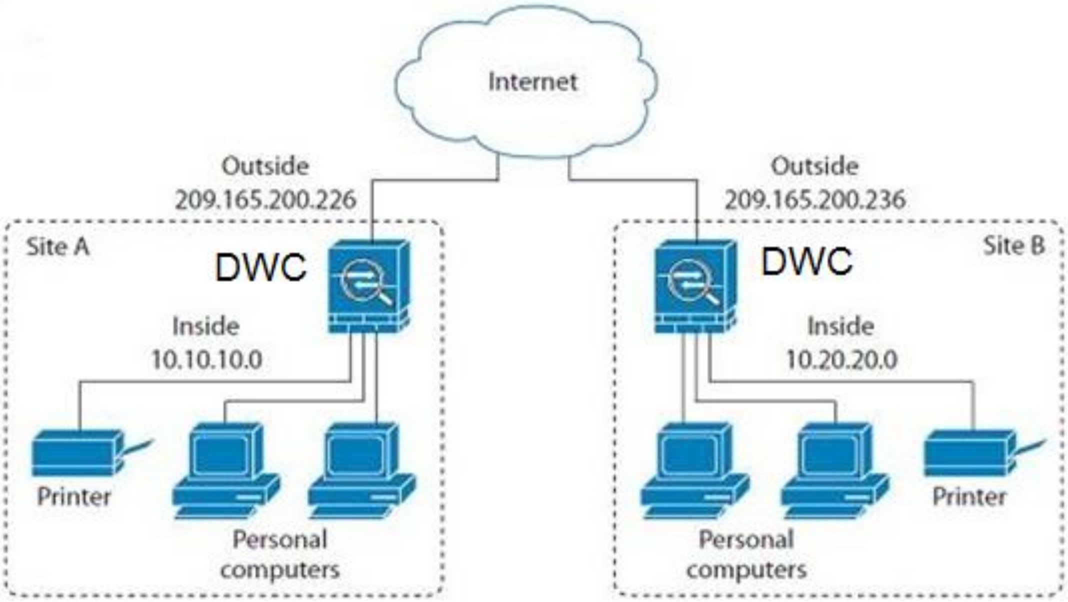
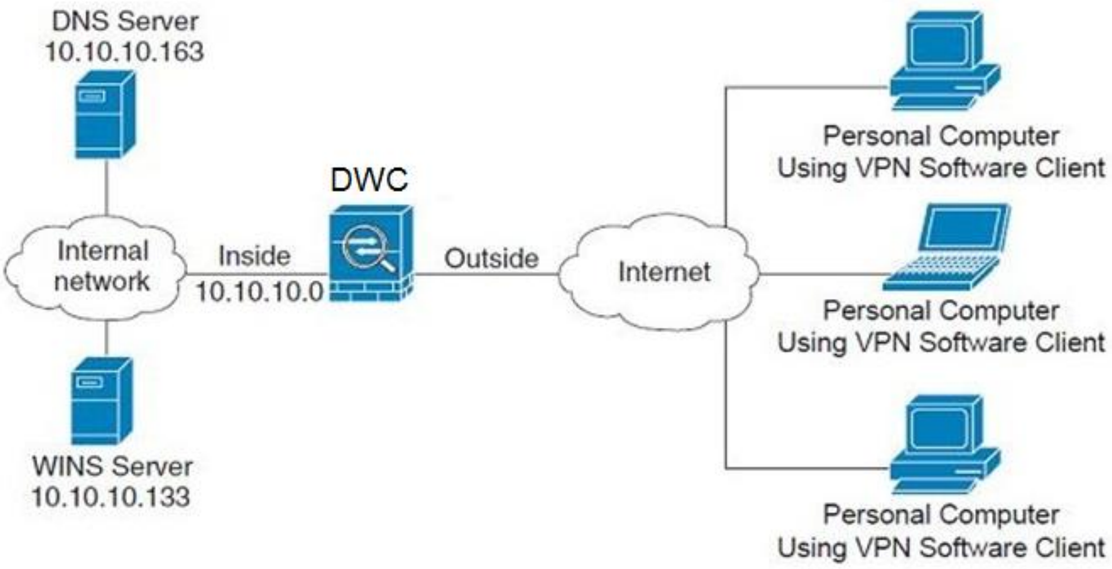


Figure 138: Example of three IPsec client connections to the internal network through the DWC IPsec gateway

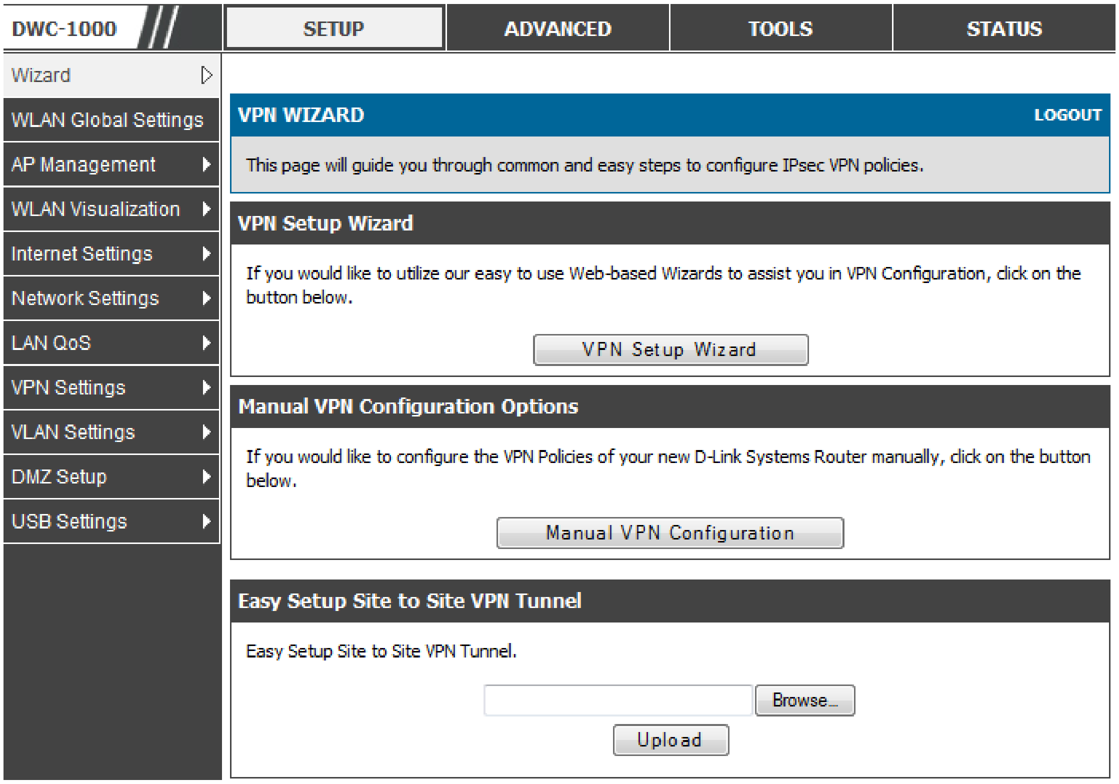


8.1 VPN Wizard

Setup > Wizard > VPN Wizard

You can use the VPN wizard to quickly create both IKE and VPN policies. Once the IKE or VPN policy is created, you can modify it as required.

Figure 139: VPN Wizard launch screen



VPN WIZARD

This page will guide you through common and easy steps to configure IPsec VPN policies.

VPN Setup Wizard

If you would like to utilize our easy to use Web-based Wizards to assist you in VPN Configuration, click on the button below.

Manual VPN Configuration Options

If you would like to configure the VPN Policies of your new D-Link Systems Router manually, click on the button below.

Easy Setup Site to Site VPN Tunnel

Easy Setup Site to Site VPN Tunnel.

To easily establish a VPN tunnel using VPN Wizard, follow the steps below:

1. Select the VPN tunnel type to create

The tunnel can either be a gateway to gateway connection (site-to-site) or a tunnel to a host on the internet (remote access).

Set the Connection Name and pre-shared key: the connection name is used for management, and the pre-shared key will be required on the VPN client or gateway to establish the tunnel

Determine the local gateway for this tunnel; if there is more than 1 Option configured the tunnel can be configured for either of the gateways.

2. Configure Remote and Local Option address for the tunnel endpoints

Remote Gateway Type: identify the remote endpoint of the tunnel by FQDN or static IP address

Remote Option IP address / FQDN: This field is enabled only if the peer you are trying to connect to is a Gateway. For VPN Clients, this IP address or Internet Name is determined when a connection request is received from a client.

Local Gateway Type: identify this controller's endpoint of the tunnel by FQDN or static IP address

Local Option IP address / FQDN: This field can be left blank if you are not using a different FQDN or IP address than the one specified in the Option port's configuration.

3. Configure the Secure Connection Remote Accessibility fields to identify the remote network:

Remote LAN IP address: address of the LAN behind the peer gateway

Remote LAN Subnet Mask: the subnet mask of the LAN behind the peer

> ✍ **Note:** The IP address range used on the remote LAN must be different from the IP address range used on the local LAN.

4. Review the settings and click Connect to establish the tunnel.

The Wizard will create an Auto IPsec policy with the following default values for a VPN Client or Gateway policy (these can be accessed from a link on the Wizard page):

Parameter	**Default value from Wizard**
Exchange Mode	Aggressive (Client policy) or Main (Gateway policy)
ID Type	FQDN
Local Option ID	wan_local.com (only applies to Client policies)
Remote Option ID	wan_remote.com (only applies to Client policies)
Encryption Algorithm	3DES
Authentication Algorithm	SHA-1
Authentication Method	Pre-shared Key
PFS Key-Group	DH-Group 2(1024 bit)
Life Time (Phase 1)	24 hours
Life Time (Phase 2)	8 hours
NETBIOS	Enabled (only applies to Gateway policies)

✍ The VPN Wizard is the recommended method to set up an Auto IPsec policy. Once the Wizard creates the matching IKE and VPN policies required by the Auto policy, one can modify the required fields through the edit link. Refer to the online help for details.

Easy Setup Site to Site VPN Tunnel

If you find it difficult to configure VPN policies through VPN wizard use easy setup site to site VPN tunnel. This will add VPN policies by importing a file containing pre-configured VPN policies.

8.2 Configuring IPsec Policies

Setup > VPN Settings > IPsec > IPsec Policies

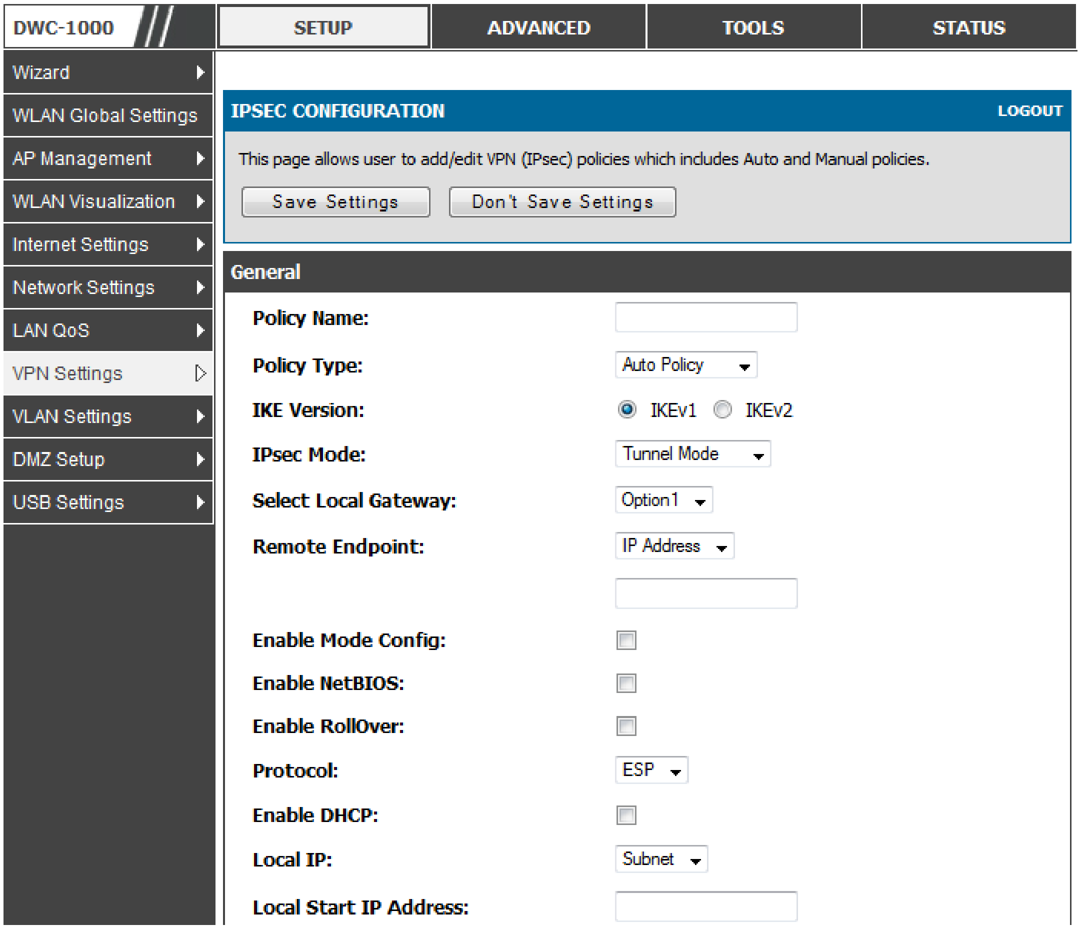
An IPsec policy is between this controller and another gateway or this controller and a IPsec client on a remote host. The IPsec mode can be either tunnel or transport depending on the network being traversed between the two policy endpoints.

Transport: This is used for end-to-end communication between this controller and the tunnel endpoint, either another IPsec gateway or an IPsec VPN client on a host. Only the data payload is encrypted and the IP header is not modified or encrypted.

Tunnel: This mode is used for network-to-network IPsec tunnels where this gateway is one endpoint of the tunnel. In this mode the entire IP packet including the header is encrypted and/or authenticated.

When tunnel mode is selected, you can enable NetBIOS and DHCP over IPsec. DHCP over IPsec allows this controller to serve IP leases to hosts on the remote LAN. As well in this mode you can define the single IP address, range of IPs, or subnet on both the local and remote private networks that can communicate over the tunnel.

Figure 140: IPsec policy configuration



IPSEC CONFIGURATION

This page allows user to add/edit VPN (IPsec) policies which includes Auto and Manual policies.

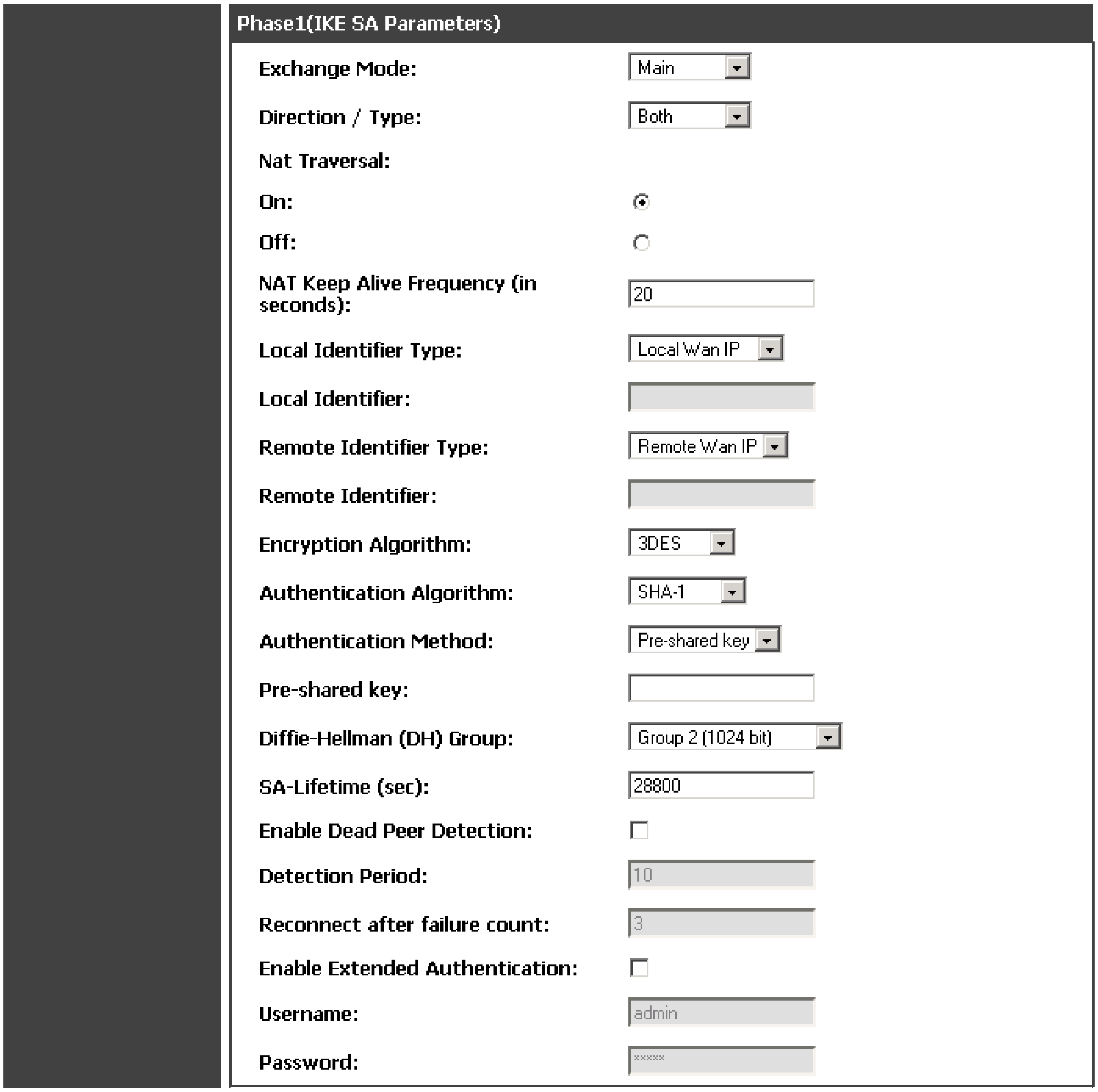
General

Policy Name:	
Policy Type:	Auto Policy
IKE Version:	● IKEv1 ○ IKEv2
IPsec Mode:	Tunnel Mode
Select Local Gateway:	Option1
Remote Endpoint:	IP Address
Enable Mode Config:	□
Enable NetBIOS:	□
Enable RollOver:	□
Protocol:	ESP
Enable DHCP:	□
Local IP:	Subnet
Local Start IP Address:	

Once the tunnel type and endpoints of the tunnel are defined you can determine the Phase 1 / Phase 2 negotiation to use for the tunnel. This is covered in the IPsec mode setting, as the policy can be Manual or Auto. For Auto policies, the Internet Key Exchange (IKE) protocol dynamically exchanges keys between two IPsec hosts. The Phase 1 IKE parameters are used to define the tunnel's security association details. The Phase 2 Auto policy parameters cover the security association lifetime and encryption/authentication details of the phase 2 key negotiation.

The VPN policy is one half of the IKE/VPN policy pair required to establish an Auto IPsec VPN tunnel. The IP addresses of the machine or machines on the two VPN endpoints are configured here, along with the policy parameters required to secure the tunnel

Figure 141: IPsec policy configuration continued (Auto policy via IKE)



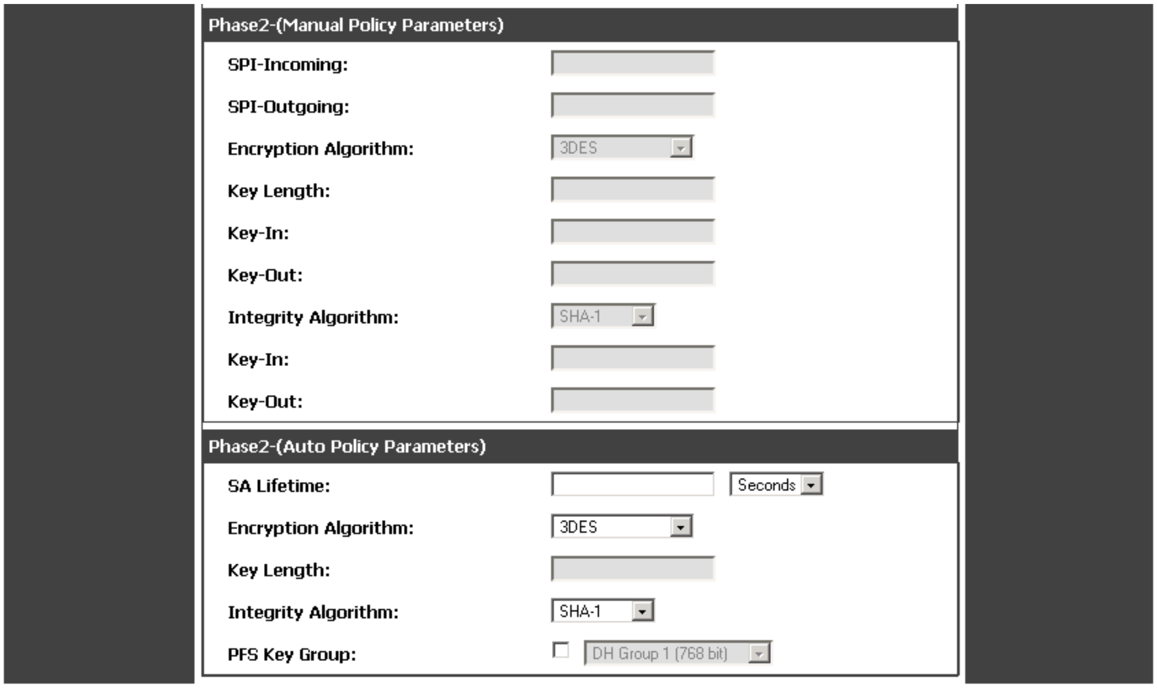
Phase1(IKE SA Parameters)

Exchange Mode:	Main
Direction / Type:	Both
Nat Traversal:	
On:	●
Off:	○
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP
Local Identifier:	
Remote Identifier Type:	Remote Wan IP
Remote Identifier:	
Encryption Algorithm:	3DES
Authentication Algorithm:	SHA-1
Authentication Method:	Pre-shared key
Pre-shared key:	
Diffie-Hellman (DH) Group:	Group 2 (1024 bit)
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	□
Detection Period:	10
Reconnect after failure count:	3
Enable Extended Authentication:	□
Username:	admin
Password:	*****

A Manual policy does not use IKE and instead relies on manual keying to exchange authentication parameters between the two IPsec hosts. The incoming and outgoing security parameter index (SPI) values must be mirrored on the remote tunnel endpoint. As well the encryption and integrity algorithms and keys must match on the remote IPsec host exactly in order for the tunnel to establish successfully. Note that using Auto policies with IKE are preferred as in some IPsec implementations the SPI (security parameter index) values require conversion at each endpoint.

DWC-1000 supports VPN roll-over feature. This means that policies configured on primary Option will rollover to the secondary Option in case of a link failure on a primary Option. This feature can be used only if your Option is configured in Auto-Rollover mode.

Figure 142: IPsec policy configuration continued (Auto/Manual Phase 2)



Phase2-(Manual Policy Parameters)

SPI-Incoming:	
SPI-Outgoing:	
Encryption Algorithm:	3DES
Key Length:	
Key-In:	
Key-Out:	
Integrity Algorithm:	SHA-1
Key-In:	
Key-Out:	

Phase2-(Auto Policy Parameters)

SA Lifetime:	Seconds
Encryption Algorithm:	3DES
Key Length:	
Integrity Algorithm:	SHA-1
PFS Key Group:	□ DH Group 1 (768 bit)

8.2.1 Extended Authentication (XAUTH)

You can also configure extended authentication (XAUTH). Rather than configure a unique VPN policy for each user, you can configure the VPN gateway controller to authenticate users from a stored list of user accounts or with an external authentication server such as a RADIUS server. With a user database, user accounts created in the controller are used to authenticate users.

With a configured RADIUS server, the controller connects to a RADIUS server and passes to it the credentials that it receives from the VPN client. You can secure the connection between the controller and the RADIUS server with the authentication protocol supported by the server (PAP or CHAP). For RADIUS – PAP, the controller first checks in the user database to see if the user credentials are available; if they are not, the controller connects to the RADIUS server.

8.2.2 Internet over IPSec tunnel

In this feature all the traffic will pass through the VPN Tunnel and from the Remote Gateway the packet will be routed to Internet. On the remote gateway side, the outgoing packet will be SNAT'ed.

8.3 Configuring VPN clients

Remote VPN clients must be configured with the same VPN policy parameters used in the VPN tunnel that the client wishes to use: encryption, authentication, life time, and PFS key-group. Upon establishing these authentication parameters, the VPN Client user database must also be populated with an account to give a user access to the tunnel.

> ✍ VPN client software is required to establish a VPN tunnel between the controller and remote endpoint. Open source software (such as OpenVPN or Openswan) as well as Microsoft IPsec VPN software can be configured with the required IKE policy parameters to establish an IPsec VPN tunnel. Refer to the client software guide for detailed instructions on setup as well as the controller’s online help.

The user database contains the list of VPN user accounts that are authorized to use a given VPN tunnel. Alternatively VPN tunnel users can be authenticated using a configured Radius database. Refer to the online help to determine how to populate the user database and/or configure RADIUS authentication.

8.4 PPTP / L2TP Tunnels

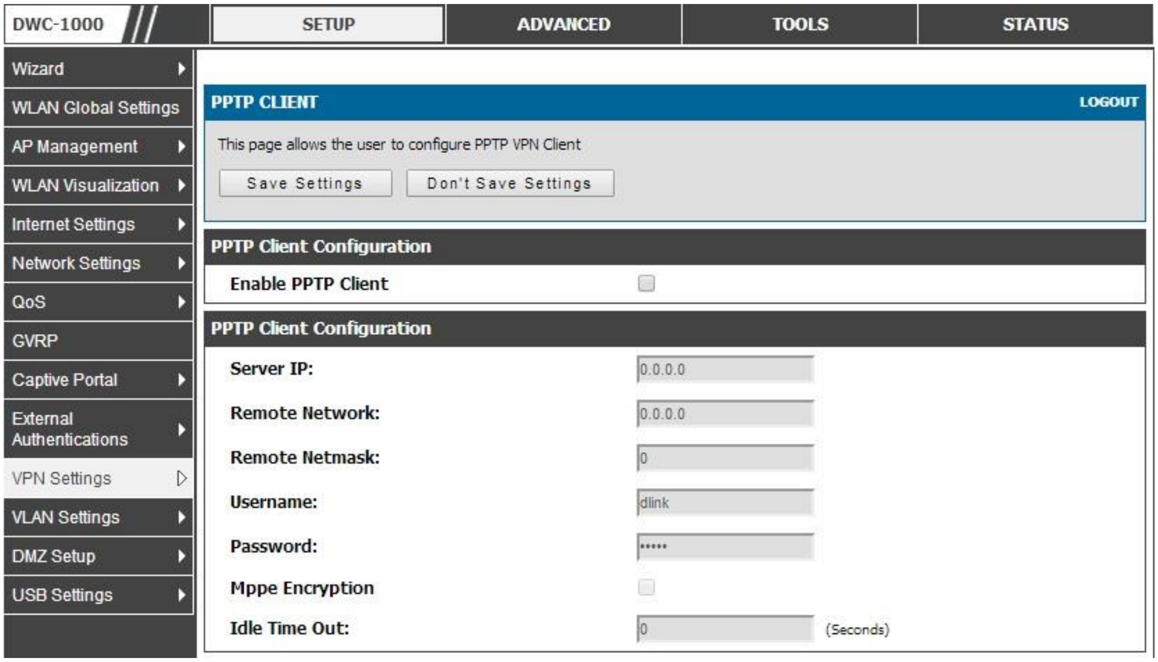
This controller supports VPN tunnels from either PPTP or L2TP ISP servers. The controller acts as a broker device to allow the ISP's server to create a TCP control connection between the LAN VPN client and the VPN server.

8.4.1 PPTP Tunnel Support

Setup > VPN Settings > PPTP > PPTP Client

PPTP VPN Client can be configured on this controller. Using this client we can access remote network which is local to PPTP server. Once client is enabled, the user can access ***Status > Active VPNs*** page and establish PPTP VPN tunnel clicking Connect. To disconnect the tunnel, click Drop.

Figure 143: PPTP tunnel configuration – PPTP Client



PPTP CLIENT

This page allows the user to configure PPTP VPN Client

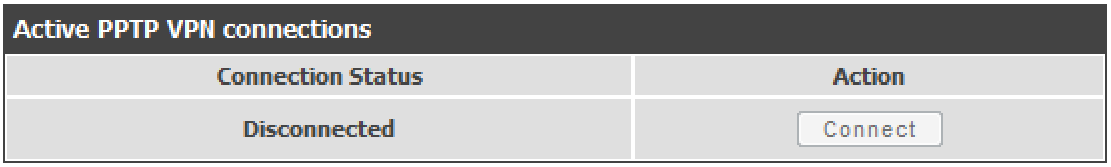
PPTP Client Configuration

Enable PPTP Client	□

PPTP Client Configuration

Server IP:	0.0.0.0
Remote Network:	0.0.0.0
Remote Netmask:	0
Username:	dlink
Password:	•••••
Mppe Encryption	□
Idle Time Out:	0 (Seconds)

Figure 144: PPTP VPN connection status



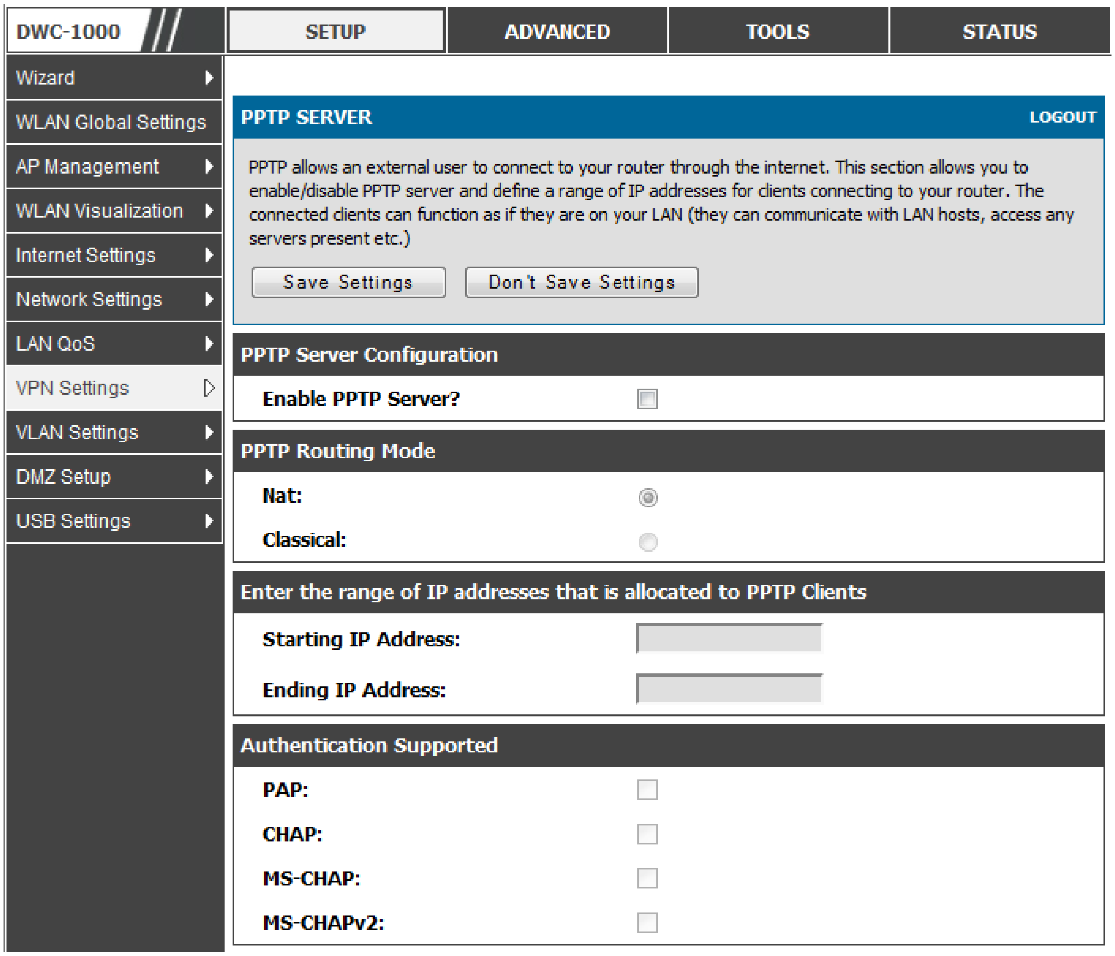
Active PPTP VPN connections

Connection Status	Action
Disconnected	Connect

Setup > VPN Settings > PPTP > PPTP Server

A PPTP VPN can be established through this controller. Once enabled a PPTP server is available on the controller for LAN and Option PPTP client users to access. Once the PPTP server is enabled, PPTP clients that are within the range of configured IP addresses of allowed clients can reach the controller’s PPTP server. Once authenticated by the PPTP server (the tunnel endpoint), PPTP clients have access to the network managed by the controller.

Figure 145: PPTP tunnel configuration – PPTP Server



PPTP SERVER

PPTP allows an external user to connect to your router through the internet. This section allows you to enable/disable PPTP server and define a range of IP addresses for clients connecting to your router. The connected clients can function as if they are on your LAN (they can communicate with LAN hosts, access any servers present etc.)

PPTP Server Configuration

Enable PPTP Server? □

PPTP Routing Mode

Nat: ●

Classical: ○

Enter the range of IP addresses that is allocated to PPTP Clients

Starting IP Address:

Ending IP Address:

Authentication Supported

PAP: □

CHAP: □

MS-CHAP: □

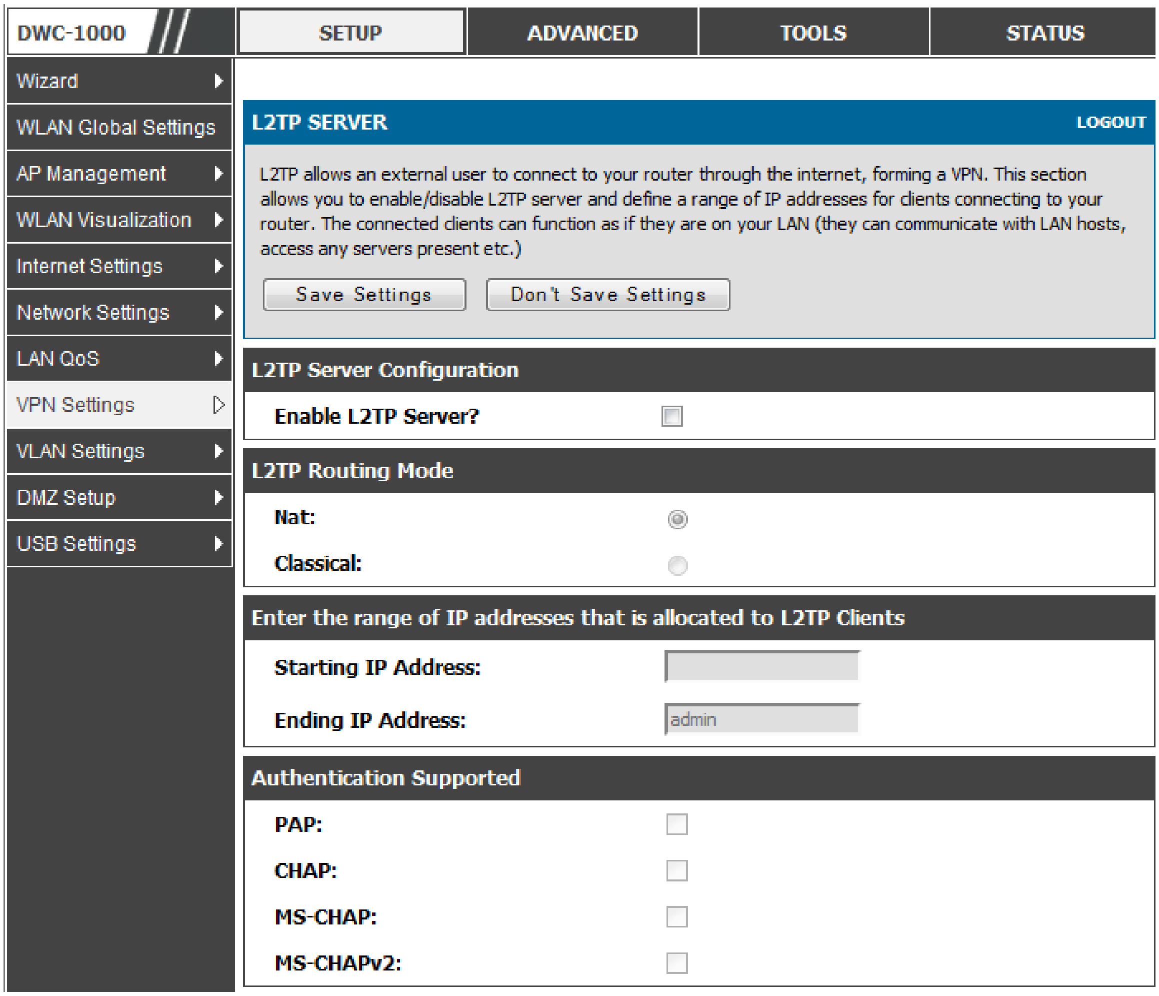
MS-CHAPv2: □

8.4.2 L2TP Tunnel Support

Setup > VPN Settings > L2TP > L2TP Server

A L2TP VPN can be established through this controller. Once enabled a L2TP server is available on the controller for LAN and Option L2TP client users to access. Once the L2TP server is enabled, L2TP clients that are within the range of configured IP addresses of allowed clients can reach the controller's L2TP server. Once authenticated by the L2TP server (the tunnel endpoint), L2TP clients have access to the network managed by the controller.

Figure 146: L2TP tunnel configuration – L2TP Server



L2TP allows an external user to connect to your router through the internet, forming a VPN. This section allows you to enable/disable L2TP server and define a range of IP addresses for clients connecting to your router. The connected clients can function as if they are on your LAN (they can communicate with LAN hosts, access any servers present etc.)

L2TP Server Configuration

Enable L2TP Server? □

L2TP Routing Mode

Nat: ●

Classical: ○

Enter the range of IP addresses that is allocated to L2TP Clients

Starting IP Address:

Ending IP Address: admin

Authentication Supported

PAP: □

CHAP: □

MS-CHAP: □

MS-CHAPv2: □

8.4.3 OpenVPN Support

Setup > VPN Settings > OpenVPN > OpenVPN Configuration

OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. When used in a multiclient-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority. An Open VPN can be established through this controller. Check/Uncheck this and click save settings to start/stop the OpenVPN server.

Mode: OpenVPN daemon mode. It can run in server mode, client mode or access server client mode. In access server client mode, the user has to download the auto login profile from the OpenVPN Access Server and upload the same to connect.

Server IP: OpenVPN server IP address to which the client connects(Applicable in client mode).

VPN Network: Address of the Virtual Network.

VPN Netmask: Netmask of the Virtual Network.

Port: The port number on which OpenVPN server (or Access Server) runs.

Tunnel Protocol: The protocol used to communicate with the remote host. Ex: TCP, UDP. UDP is the default.

Encryption Algorithm: The cipher with which the packets are encrypted. Ex: BF-CBC, AES-128,AES-192 and AES-256. BF-CBC is the default

Hash algorithm: Message digest algorithm used to authenticate packets. Ex: SHA1, SHA256 and SHA512. SHA1 is the default.

Tunnel Type: Select Full Tunnel to redirect all the traffic through the tunnel. Select Split Tunnel to redirect traffic to only specified resources (added from OpenVpnClient Routes) through the tunnel. Full Tunnel is the default.

Enable Client to Client communication: Enable this to allow OpenVPN clients to communicate with each other in split tunnel case. Disabled by default.

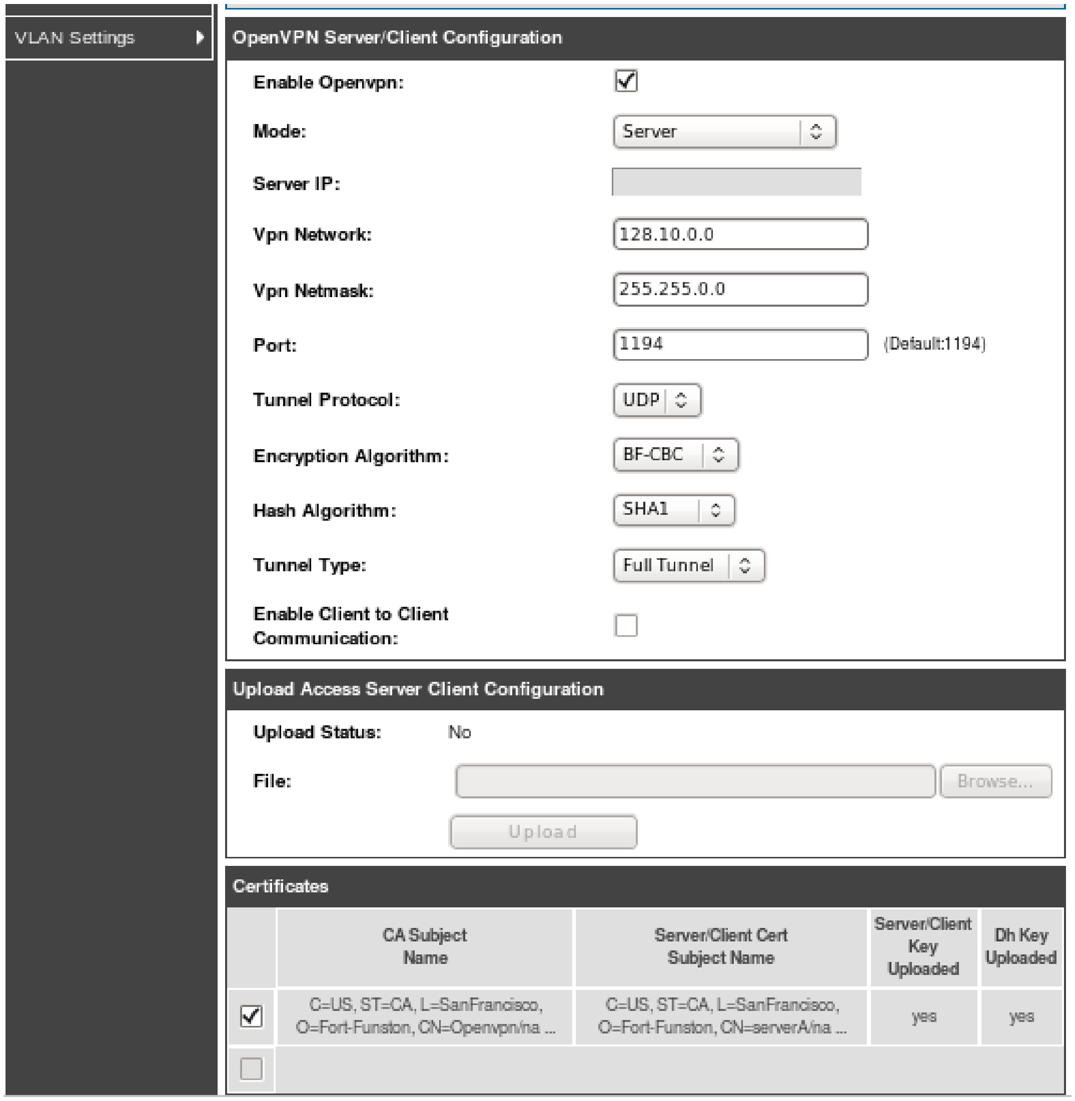
Upload Access Server Client Configuration: The user has to download the auto login profile and upload here to connect this controller to the OpenVPN Access Server.

Certificates: Select the set of certificates OpenVPN server uses. First Row: Set of certificates and keys the server uses. Second Row: Set of certificates and keys newly uploaded.

Enable TLS Authentication Key: Enabling this adds TLS authentication which adds an additional layer of authentication. Can be checked only when the TLS key is uploaded. Disabled by default.

Click **Save Settings** to save the configuration entered.

Figure 147: OpenVPN configuration



OpenVPN Server/Client Configuration

Enable Openvpn:	☑
Mode:	Server
Server IP:	
Vpn Network:	128.10.0.0
Vpn Netmask:	255.255.0.0
Port:	1194 (Default:1194)
Tunnel Protocol:	UDP
Encryption Algorithm:	BF-CBC
Hash Algorithm:	SHA1
Tunnel Type:	Full Tunnel
Enable Client to Client Communication:	□

Upload Access Server Client Configuration

Upload Status: No

File:

Certificates

	CA Subject Name	Server/Client Cert Subject Name	Server/Client Key Uploaded	Dh Key Uploaded
☑	C=US, ST=CA, L=SanFrancisco, O=Fort-Funston, CN=Openvpn/na ...	C=US, ST=CA, L=SanFrancisco, O=Fort-Funston, CN=serverA/na ...	yes	yes
□				

Chapter 9. SSL VPN

> ✍ The following feature is available upon licensed activation of VPN / Firewall features for the system.

The controller provides an intrinsic SSL VPN feature as an alternate to the standard IPsec VPN. SSL VPN differs from IPsec VPN mainly by removing the requirement of a pre-installed VPN client on the remote host. Instead, users can securely login through the SSL User Portal using a standard web browser and receive access to configured network resources within the corporate LAN. The controller supports multiple concurrent sessions to allow remote users to access the LAN over an encrypted link through a customizable user portal interface, and each SSL VPN user can be assigned unique privileges and network resource access levels.

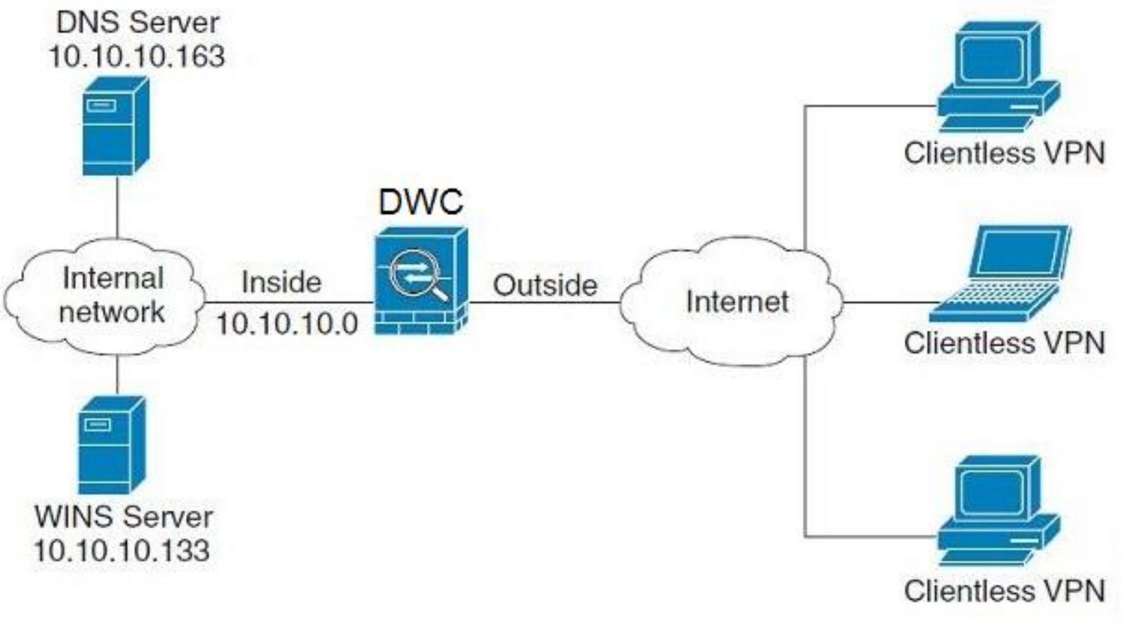
The remote user can be provided different options for SSL service through this controller:

VPN Tunnel: The remote user's SSL enabled browser is used in place of a VPN client on the remote host to establish a secure VPN tunnel. A SSL VPN client (Active-X or Java based) is installed in the remote host to allow the client to join the corporate LAN with pre-configured access/policy privileges. At this point a virtual network interface is created on the user's host and this will be assigned an IP address and DNS server address from the controller. Once established, the host machine can access allocated network resources.

Port Forwarding: A web-based (ActiveX or Java) client is installed on the client machine again. Note that Port Forwarding service only supports TCP connections between the remote user and the controller. The controller administrator can define specific services or applications that are available to remote port forwarding users instead of access to the full LAN like the VPN tunnel.

> ✍ ActiveX clients are used when the remote user accesses the portal using the Internet Explorer browser. The Java client is used for other browsers like Mozilla Firefox, Netscape Navigator, Google Chrome, and Apple Safari.

Figure 148: Example of clientless SSL VPN connections to the DWC-1000



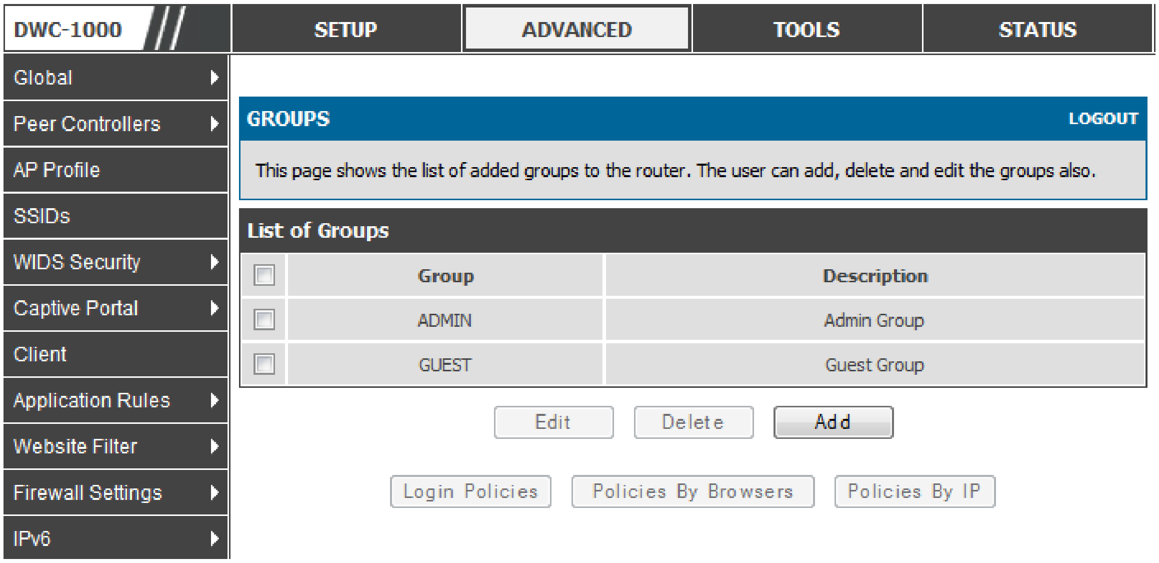
9.1 Groups and Users

Advanced > Users > Groups

The group page allows creating, editing and deleting groups. The groups are associated to set of user types. The lists of available groups are displayed in the "List of Group" page with Group name and description of group.

- Click **Add** to create a group.
- Click **Edit** to update an existing group.
- Click **Delete** to clear an existing group.

Figure 149: List of Groups



This page shows the list of added groups to the router. The user can add, delete and edit the groups also.

List of Groups

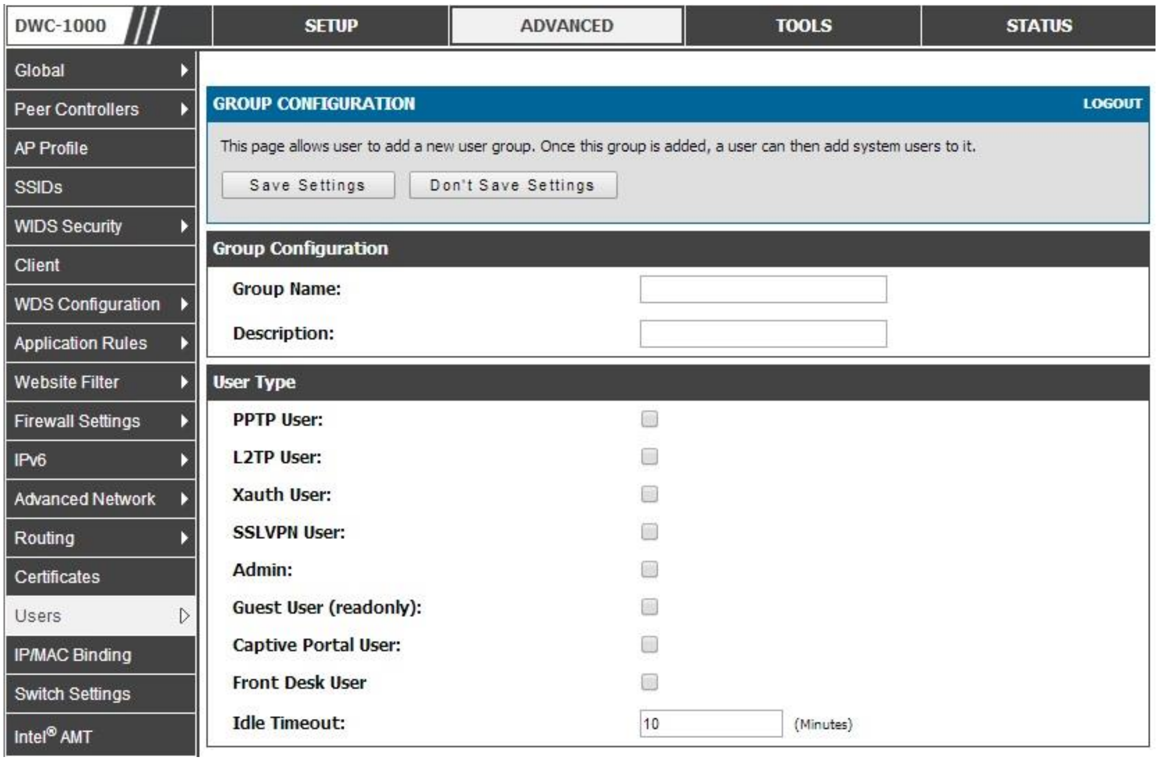
□	Group	Description
□	ADMIN	Admin Group
□	GUEST	Guest Group

Group configuration page allows to create a group with a different type of users. The user types are as follows:

- **PPTP User**: These are PPTP VPN tunnel LAN users that can establish a tunnel with the PPTP server on the Option.
- **L2TP User**: These are L2TP VPN tunnel LAN users that can establish a tunnel with the L2TP server on the Option.

- **Xauth User**: This user’s authentication is performed by an externally configured RADIUS or other Enterprise server. It is not part of the local user database.
- **SSLVPN User**: This user has access to the SSL VPN services as determined by the group policies and authentication domain of which it is a member. The domain-determined SSL VPN portal will be displayed when logging in with this user type.
- **Admin**: This is the controller’s super-user, and can manage the controller, use SSL VPN to access network resources, and login to L2TP/PPTP servers on the Option. There will always be one default administrator user for the GUI
- **Guest User (read-only)**: The guest user gains read only access to the GUI to observe and review configuration settings. The guest does not have SSL VPN access.
- **Captive Portal User**: These captive portal users has access through the controller. The access is determined based on captive portal policies.
- **Front Desk User:** The front desk user has the ability to create temporary HotSpot users that can access the internet or other networks via Captive Portal authentication.
- **Idle Timeout**: This the log in timeout period for users of this group.

Figure 150: User Group Configuration



GROUP CONFIGURATION

This page allows user to add a new user group. Once this group is added, a user can then add system users to it.

Group Configuration

Group Name:	
Description:	

User Type

PPTP User:	□
L2TP User:	□
Xauth User:	□
SSLVPN User:	□
Admin:	□
Guest User (readonly):	□
Captive Portal User:	□
Front Desk User	□
Idle Timeout:	10 (Minutes)

When SSLVPN users are selected, the SSLVPN settings are displayed with the following parameters as captured in SSLVPN Settings. As per the Authentication Type SSL VPN details are configured.

- **Authentication Type**: The authentication Type can be one of the following: Local User Database (default), Radius-PAP, Radius-CHAP, Radius-MSCHAP, Radius-MSCHAPv2, NT Domain, Active Directory and LDAP.

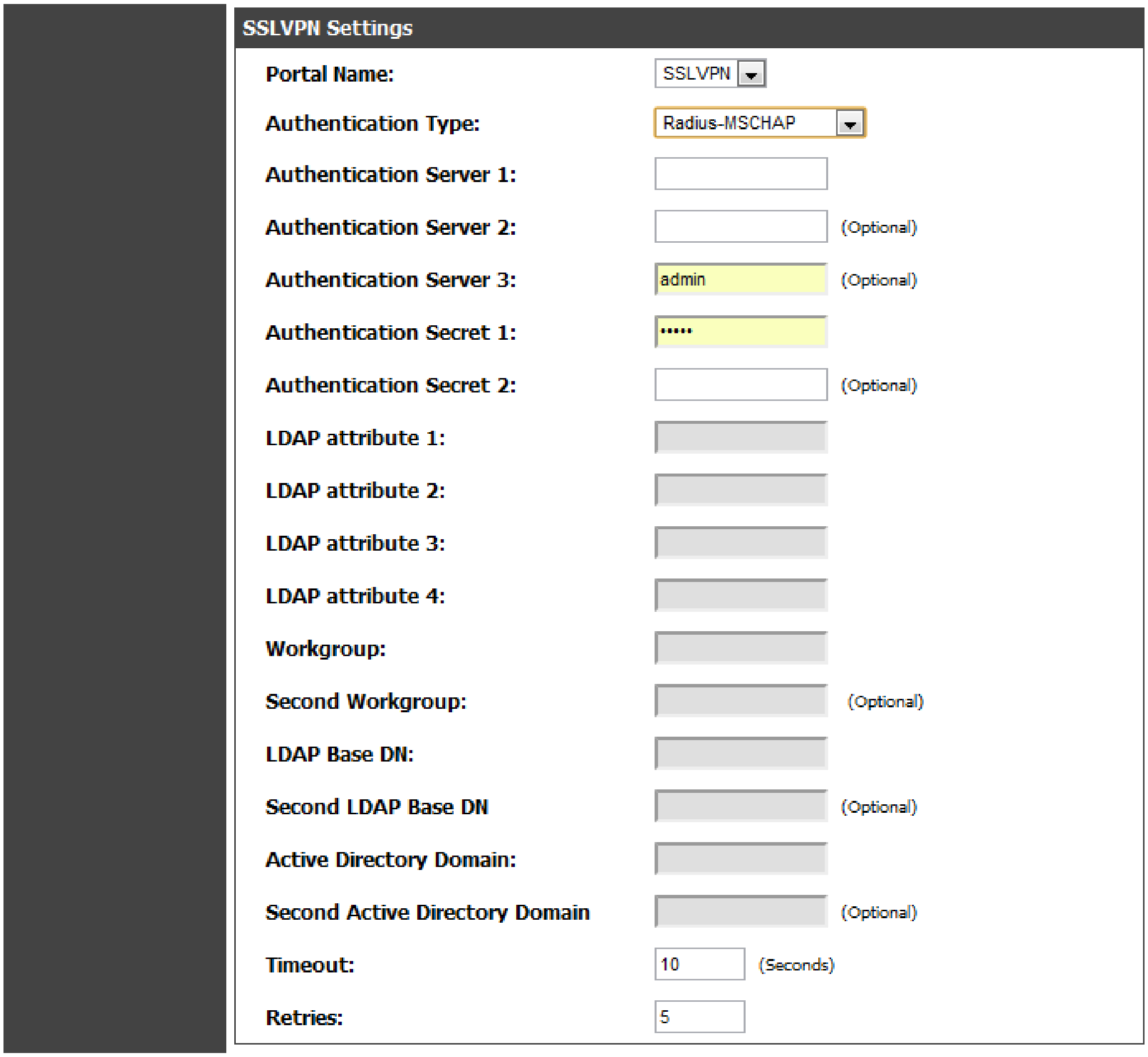
- **Authentication Secret**: If the domain uses RADIUS authentication then the authentication secret is required (and this has to match the secret configured on the RADIUS server).

- **Workgroup**: This is required is for NT domain authentication. If there are multiple workgroups, user can enter the details for up to two workgroups.

- **LDAP Base DN**: This is the base domain name for the LDAP authentication server. If there are multiple LDAP authentication servers, user can enter the details for up to two LDAP Base DN.

- **Active Directory Domain**: If the domain uses the Active Directory authentication, the Active Directory domain name is required. Users configured in the Active Directory database are given access to the SSL VPN portal with their Active Directory username and password. If there are multiple Active Directory domains, user can enter the details for up to two authentication domains.
- **Timeout**: The timeout period for reaching the authentication server.
- **Retries**: The number of retries to authenticate with the authentication server after which the DWC-1000 stops trying to reach the server.

Figure 151: SSLVPN Settings



SSLVPN Settings

Portal Name:	SSLVPN	
Authentication Type:	Radius-MSCHAP	
Authentication Server 1:		
Authentication Server 2:		(Optional)
Authentication Server 3:	admin	(Optional)
Authentication Secret 1:	•••••	
Authentication Secret 2:		(Optional)
LDAP attribute 1:		
LDAP attribute 2:		
LDAP attribute 3:		
LDAP attribute 4:		
Workgroup:		
Second Workgroup:		(Optional)
LDAP Base DN:		
Second LDAP Base DN		(Optional)
Active Directory Domain:		
Second Active Directory Domain		(Optional)
Timeout:	10	(Seconds)
Retries:	5	

Login Policies

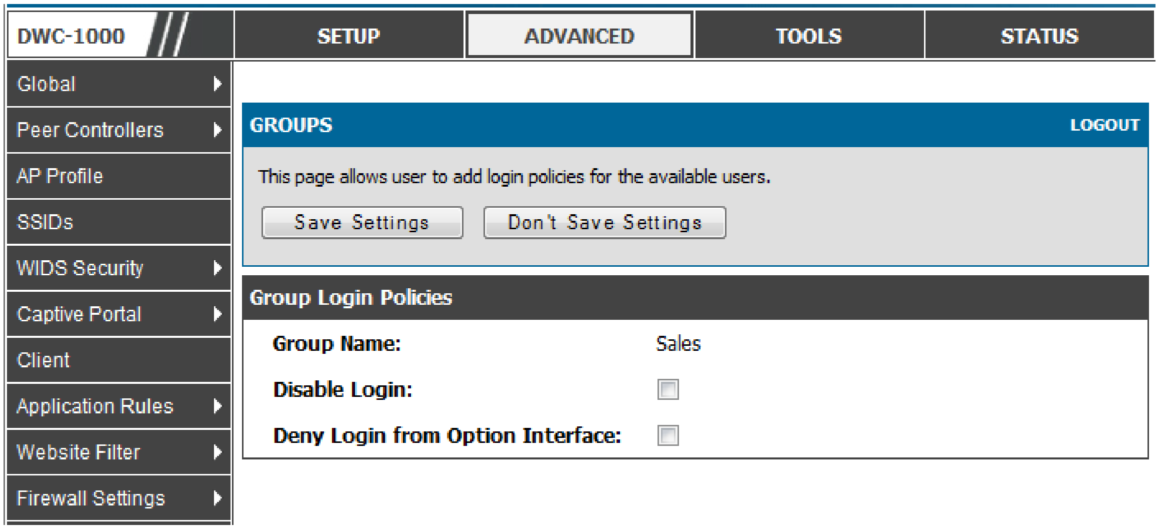
To set login policies for the group, select the corresponding group click "Login policies". The following parameters are configured:

Group Name: This is the name of the group that can have its login policy edited

Disable Login: Enable to prevent the users of this group from logging into the devices management interface(s)

Deny Login from Option interface: Enable to prevent the users of this group from logging in from an Option (wide area network) interface. In this case only login through LAN is allowed.

Figure 152: Group login policies options



This page allows user to add login policies for the available users.

Group Login Policies

Group Name:	Sales
Disable Login:	□
Deny Login from Option Interface:	□

Policy by Browsers

To set browser policies for the group, select the corresponding group click "Policy by Browsers". The following parameters are configured:

Group Name: This is the name of the group that can have its login policy edited

Deny Login from Defined Browsers: The list of defined browsers below will be used to prevent the users of this group from logging in to the controller’s GUI. All non-defined browsers will be allowed for login for this group.

Allow Login from Defined Browsers: The list of defined browsers below will be used to allow the users of this group from logging in to the controllers GUI. All non-defined browsers will be denied for login for this group.

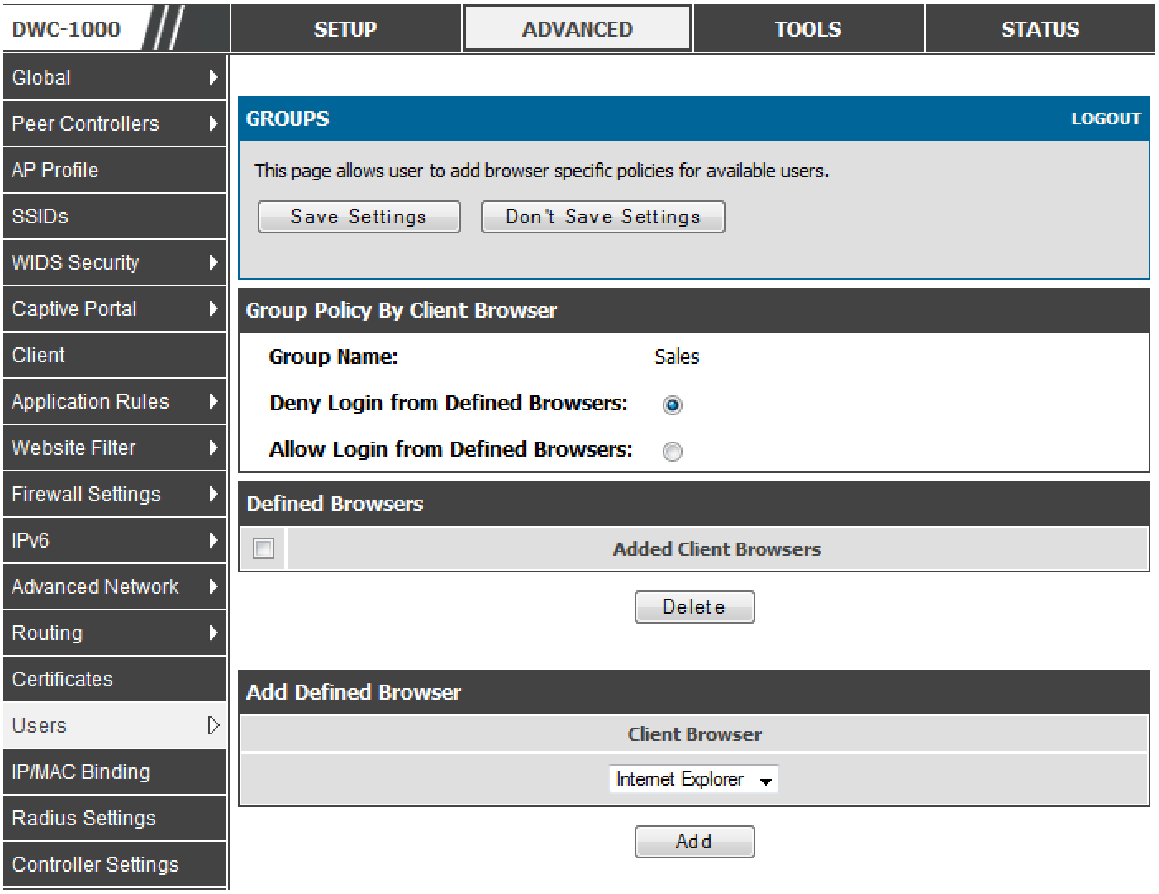
Defined Browsers: This list displays the web browsers that have been added to the Defined Browsers list, upon which group login policies can be defined. (Check Box At First Column Header): Selects all the defined browsers in the table.

Delete: Deletes the selected browser(s).

You can add to the list of Defined Browsers by selecting a client browser from the drop down menu and clicking Add. This browser will then appear in the above list of Defined Browsers.

Click **Save Settings** to save your changes.

Figure 153: Browser policies options



This page allows user to add browser specific policies for available users.

Group Policy By Client Browser

Group Name: Sales

Deny Login from Defined Browsers: ●

Allow Login from Defined Browsers: ○

Defined Browsers

□	Added Client Browsers

Add Defined Browser

Client Browser
Internet Explorer

Policy by IP

To set policies bye IP for the group, select the corresponding group click "Policy by IP". The following parameters are configured:

Group Name: This is the name of the group that can have its login policy edited

Deny Login from Defined Browsers: The list of defined browsers below will be used to prevent the users of this group from logging in to the controller GUI. All non-defined browsers will be allowed for login for this group.

Allow Login from Defined Browsers: The list of defined browsers below will be used to allow the users of this group from logging in to the controller GUI. All non-defined browsers will be denied for login for this group.

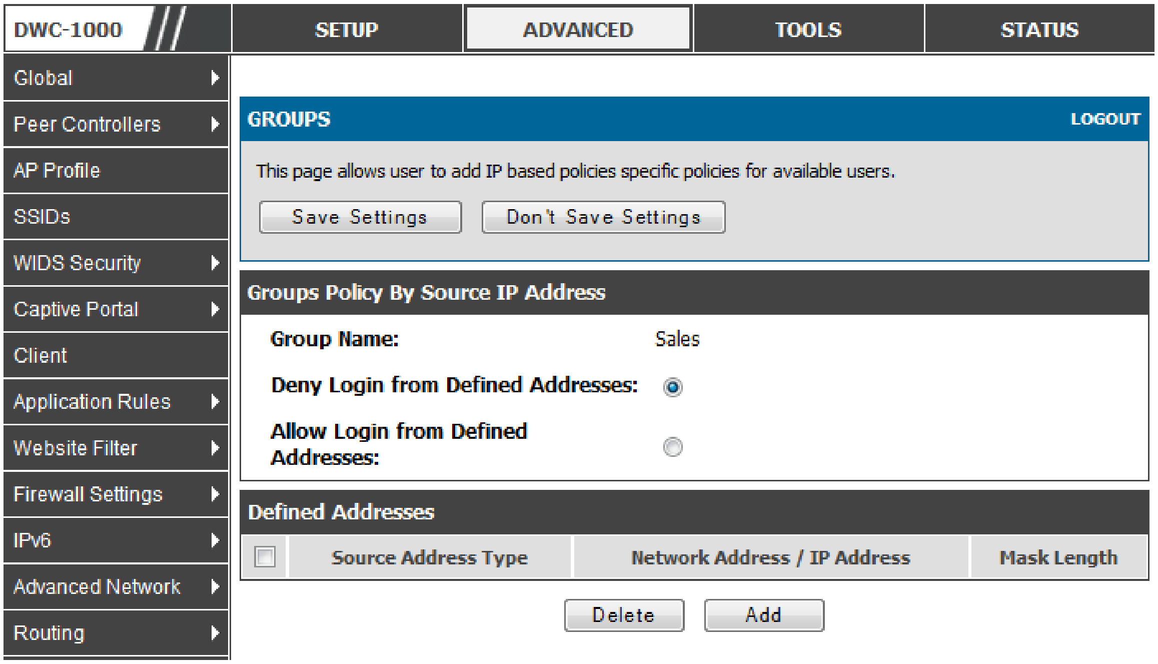
Defined Browsers: This list displays the web browsers that have been added to the Defined Browsers list, upon which group login policies can be defined. (Check Box At First Column Header): Selects all the defined browsers in the table.

Delete: Deletes the selected browser(s).

You can add to the list of Defined Browsers by selecting a client browser from the drop down menu and clicking Add. This browser will then appear in the above list of Defined Browsers.

Click **Save Settings** to save your changes.

Figure 154: IP policies options



This page allows user to add IP based policies specific policies for available users.

Groups Policy By Source IP Address

Group Name: Sales

Deny Login from Defined Addresses: ●

Allow Login from Defined Addresses: ○

Defined Addresses

□	Source Address Type	Network Address / IP Address	Mask Length

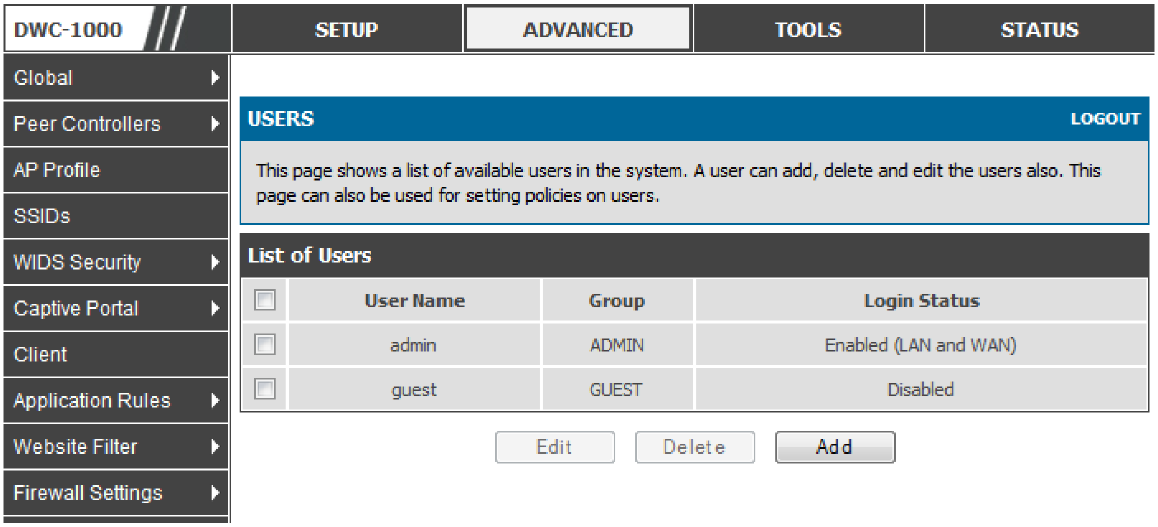
Login Policies, Policy by Browsers, Policy by IP are applicable SSL VPN user only.

Advanced > Users > Users

The users page allows adding, editing and deleting existing groups. The user are associated to configured groups. The lists of available users are displayed in the "List of Users" page with User name, associated group and Login status.

- Click **Add** to create a user.
- Click **Edit** to update an existing user.
- Click **Delete** to clear an existing user

Figure 155: Available Users with login status and associated Group



USERS

This page shows a list of available users in the system. A user can add, delete and edit the users also. This page can also be used for setting policies on users.

List of Users

□	User Name	Group	Login Status
□	admin	ADMIN	Enabled (LAN and WAN)
□	guest	GUEST	Disabled

9.1.1 Users and Passwords

Advanced > Users > Users

The user configurations allow creating users associated to group. The user settings contain the following key components:

User Name: This is unique identifier of the user.

First Name: This is the user’s first name

Last Name: This is the user’s last name

Select Group: A group is chosen from a list of configured groups.

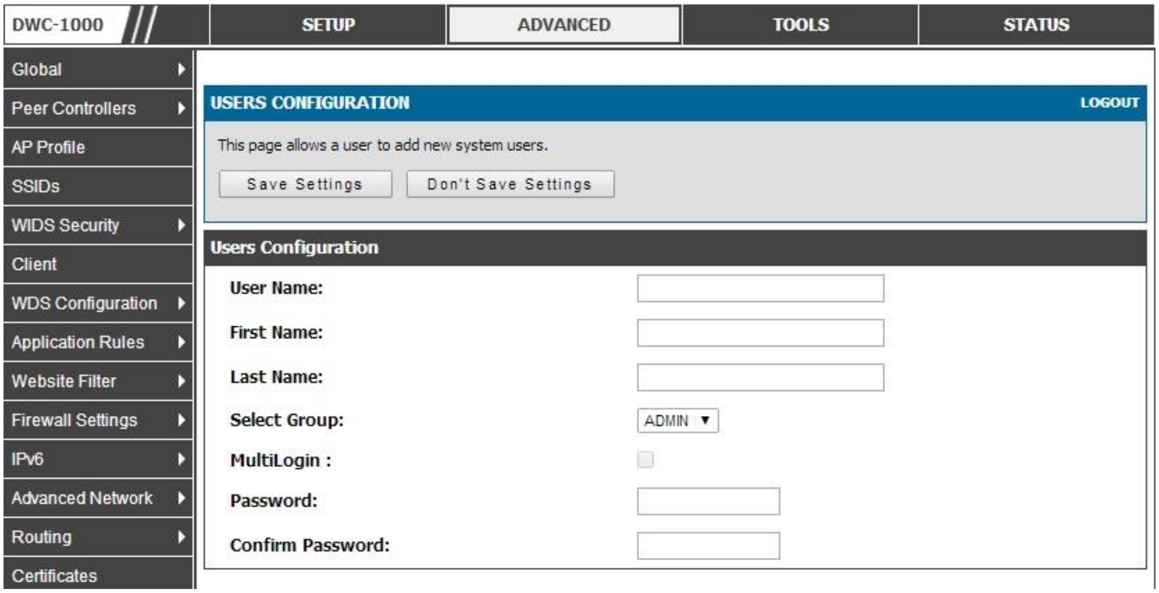
MultiLogin: Allow multiple users to login with the same credentials assigned to this user. It is particularly useful for Captive Portal users.

Password: The password associated with the user name.

Confirm Password: The same password as above is required to mitigate against typing errors.

It is recommended that passwords contains no dictionary words from any language, and is a mixture of letters (both uppercase and lowercase), numbers, and symbols. The password can be up to 30 characters.

Figure 156: User Configuration options



This page allows a user to add new system users.

User Name:

First Name:

Last Name:

Select Group: ADMIN

MultiLogin : □

Password:

Confirm Password:

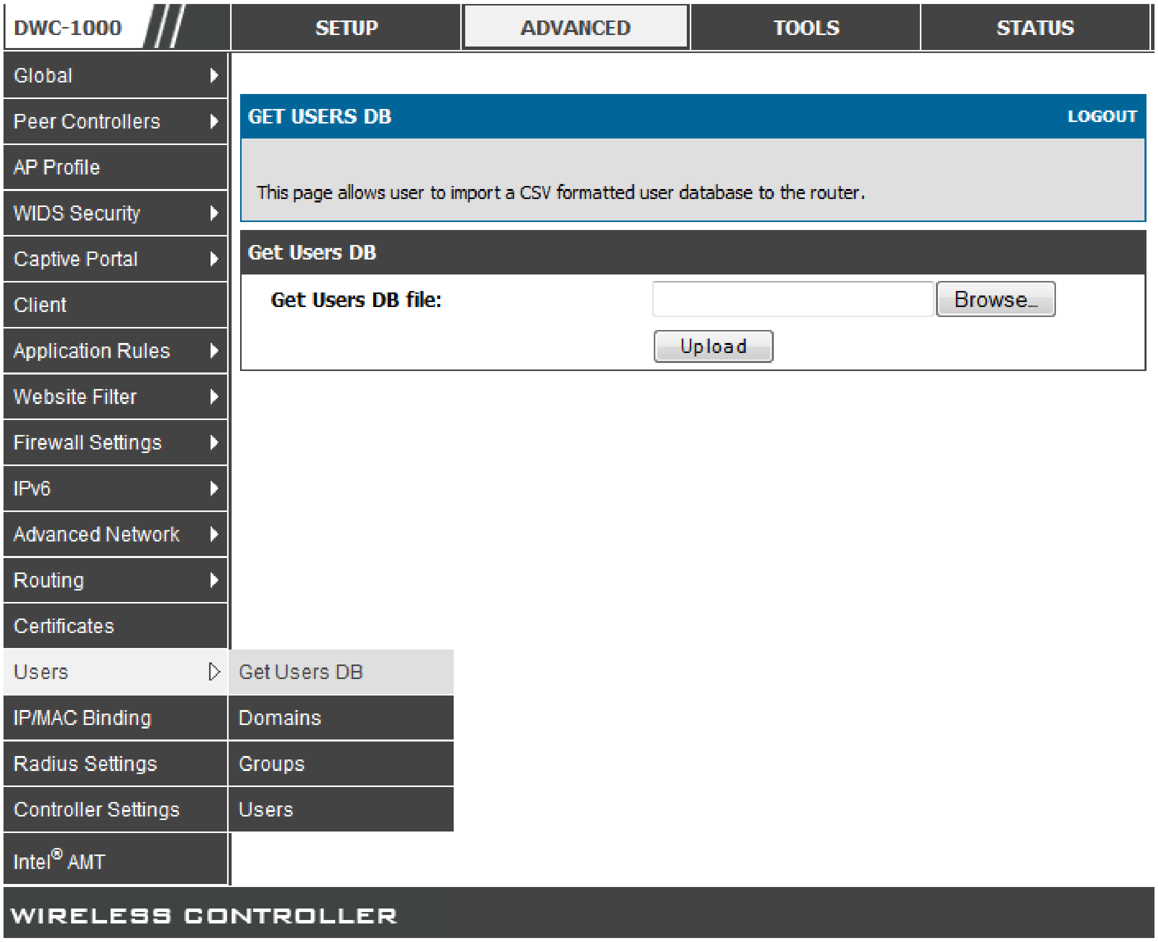
9.1.2 User Database

Advanced>Users>Get User DB

This feature allows the administrator to import a CSV formatted user database to the router. The local user database stored in this router's memory can be extracted for review with the help of this feature

Get Users DB file: Here the selected Comma-Separated-Value (CSV) format file on the local host containing, the users database can be uploaded to apply the configuration.

Figure 157: User Database export



GET USERS DB

This page allows user to import a CSV formatted user database to the router.

Get Users DB

Get Users DB file:

The user may only add system users using the CSV file upload mechanism. Before adding users to different groups, the groups must be created using GUI. Also edit and delete operations on users can be more conveniently handled through GUI as it is much easier to select a particular user for edit/delete. This mechanism of .csv file upload is more convenient than GUI only for adding a large number of users where users could be added at one go rather than one at a time through the GUI.

Creating a CSV file to Upload to the User Database

There are some core assumptions and requirements for creating a compatible CSV file of users to upload to the DWC:

1. Each line corresponds to a single entry.
2. All the fields must be enclosed within double quotes. Consecutive fields must beseperated by commas. There cannot be any leading or trailing spaces in aline.
3. There should be no spaces between fields.
4. The Group must already be present in the device, configured via the GUI only.
5. Duplicate user names are not permitted

The following format must be used for adding a user via the CSV (file:

```
"UserName","FirstName","LastName","GroupName","MultiLogin","enable
password change","Password"
```

The fields can have the following values:

- UserName: Name of the user. Text field and cannot be NULL.
- FirstName: Text field and cannot be NULL
- LastName: Text field and cannot be NULL
- GroupName: pre-configured Group of which this user is a member. Text field and cannot be NULL
- MultiLogSup: If 1, then enable multiple users to login with this user's credentials. This is a Boolean value, cannot be NULL.
- Enable password change: If 1, then allow the captive portal user to modify their password. This is a Boolean value, cannot be NULL.
- Password: Text field and cannot be NULL

Example:

1. The following Groups have already been created in the GUI:

    a. "l2tp" with L2TP VPN capability.

b. "pptp" with PPTP VPN capability.

c. "cp" with Captive Portal capabality.

2. Here is a compatible CSV file:

```
"test","te","st","pptp","0","0","test"
"test1","tes","st1","l2tp","0","0","test1"
"test2","ee","ff","ADMIN","0","0","test2"
"test3","dd","gg","GUEST","1","0","test3"
"test4","qq","ss","cp","1","1","test4"
```

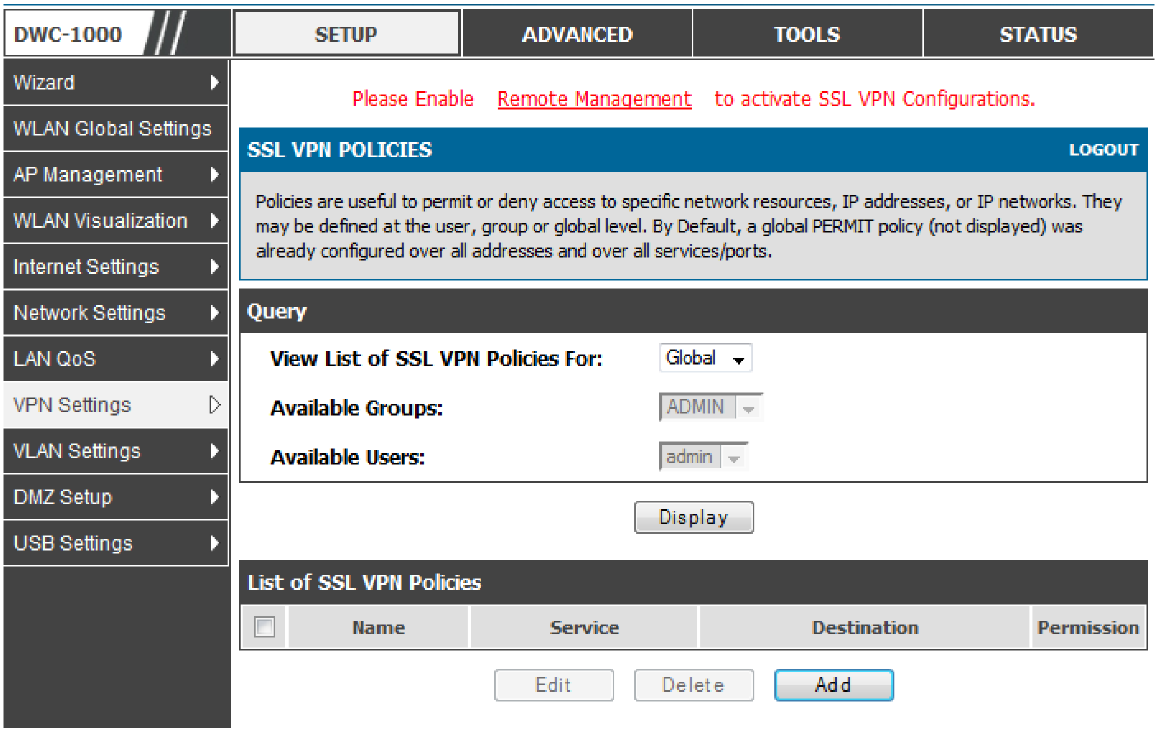
9.2 Using SSL VPN Policies

Setup > VPN Settings > SSL VPN Server > SSL VPN Policies

SSL VPN Policies can be created on a Global, Group, or User level. User level policies take precedence over Group level policies and Group level policies take precedence over Global policies. These policies can be applied to a specific network resource, IP address or ranges on the LAN, or to different SSL VPN services supported by the controller. The List of Available Policies can be filtered based on whether it applies to a user, group, or all users (global).

> ✍ A more specific policy takes precedence over a generic policy when both are applied to the same user/group/global domain. I.e. a policy for a specific IP address takes precedence over a policy for a range of addresses containing the IP address already referenced.

Figure 158: List of SSL VPN polices (Global filter)



Please Enable Remote Management to activate SSL VPN Configurations.

SSL VPN POLICIES

Policies are useful to permit or deny access to specific network resources, IP addresses, or IP networks. They may be defined at the user, group or global level. By Default, a global PERMIT policy (not displayed) was already configured over all addresses and over all services/ports.

Query

View List of SSL VPN Policies For:	Global
Available Groups:	ADMIN
Available Users:	admin

List of SSL VPN Policies

□	Name	Service	Destination	Permission

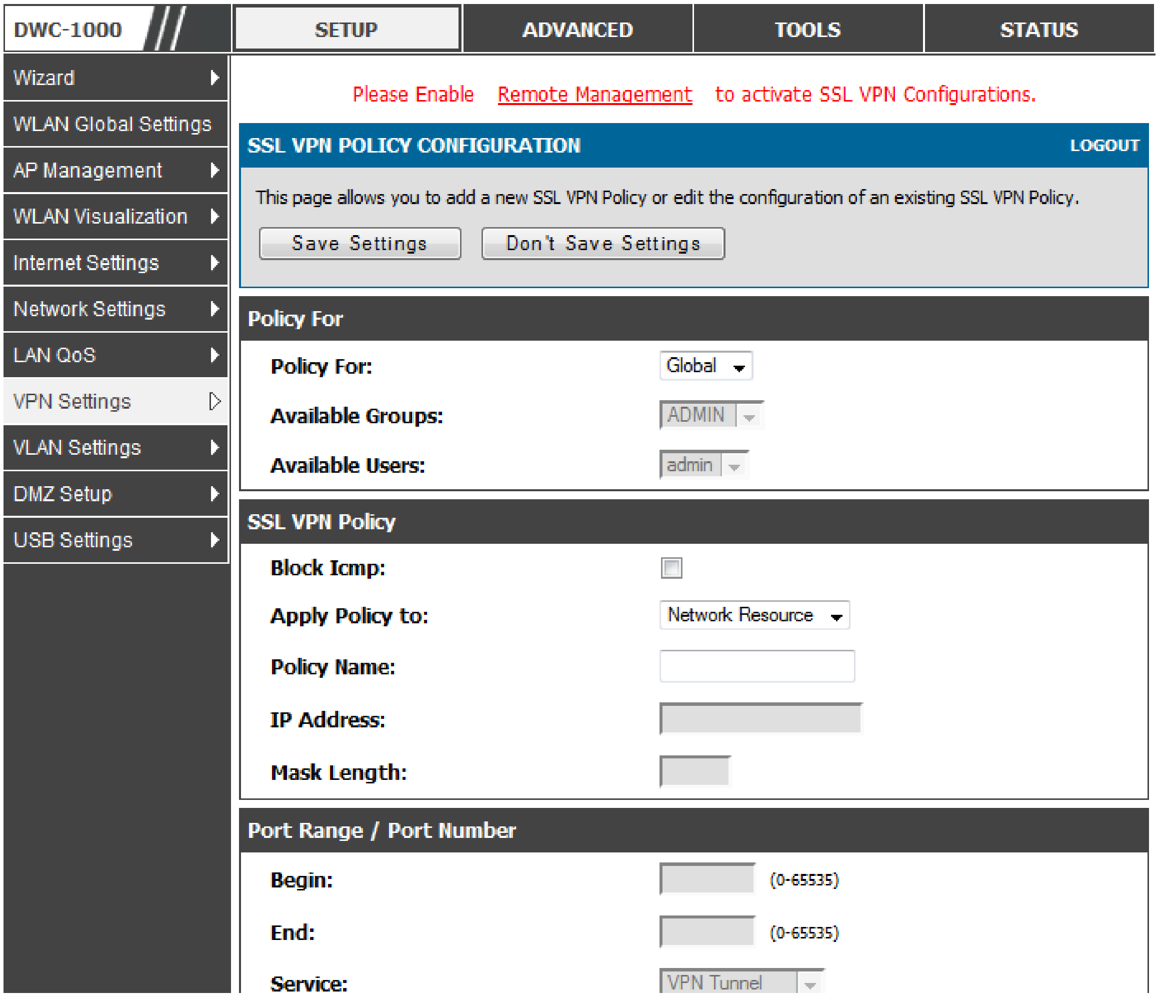
To add a SSL VPN policy, you must first assign it to a user, group, or make it global (i.e. applicable to all SSL VPN users). If the policy is for a group, the available configured groups are shown in a drop down menu and one must be selected. Similarly, for a user defined policy a SSL VPN user must be chosen from the available list of configured users.

The next step is to define the policy details. The policy name is a unique identifier for this rule. The policy can be assigned to a specific Network Resource (details follow in the subsequent section), IP address, IP network, or all devices on the LAN of the controller. Based on the selection of one of these four options, the appropriate configuration fields are required (i.e. choosing the network resources from a list of defined resources, or defining the IP addresses). For applying the policy to addresses the port range/port number can be defined.

The final steps require the policy permission to be set to either permit or deny access to the selected addresses or network resources. As well the policy can be specified for one or all of the supported SSL VPN services (i.e. VPN tunnel)

Once defined, the policy goes into effect immediately. The policy name, SSL service it applies to, destination (network resource or IP addresses) and permission (deny/permit) is outlined in a list of configured policies for the controller.

Figure 159: SSL VPN policy configuration



Please Enable Remote Management to activate SSL VPN Configurations.

SSL VPN POLICY CONFIGURATION

This page allows you to add a new SSL VPN Policy or edit the configuration of an existing SSL VPN Policy.

Policy For

Policy For: Global

Available Groups: ADMIN

Available Users: admin

SSL VPN Policy

Block Icmp: ☐

Apply Policy to: Network Resource

Policy Name:

IP Address:

Mask Length:

Port Range / Port Number

Begin: (0-65535)

End: (0-65535)

Service: VPN Tunnel

To configure a policy for a single user or group of users, enter the following information:

Policy For: The policy can be assigned to a group of users, a single user, or all users (making it a global policy). To customize the policy for specific users or groups, the user can select from the Available Groups and Available Users drop down.

Apply Policy To: This refers to the LAN resources managed by the DWC-1000, and the policy can provide (or prevent) access to network resources, IP address, IP network, etc.

Policy Name: This field is a unique name for identifying the policy. IP address: Required when the governed resource is identified by its IP address or range of addresses.

Mask Length: Required when the governed resource is identified by a range of addresses within a subnet.

Port Range: If the policy governs a type of traffic, this field is used for defining TCP or UDP port number(s) corresponding to the governed traffic. Leaving the starting and ending port range blank corresponds to all UDP and TCP traffic.

Service: This is the SSL VPN service made available by this policy. The services offered are VPN tunnel, port forwarding or both.

Defined Resources: This policy can provide access to specific network resources. Network resources must be configured in advance of creating the policy to make them available for selection as a defined resource. Network resources are created with the following information

Permission: The assigned resources defined by this policy can be explicitly permitted or denied.

9.2.1 Using Network Resources

Setup > VPN Settings > SSL VPN Server > Resources

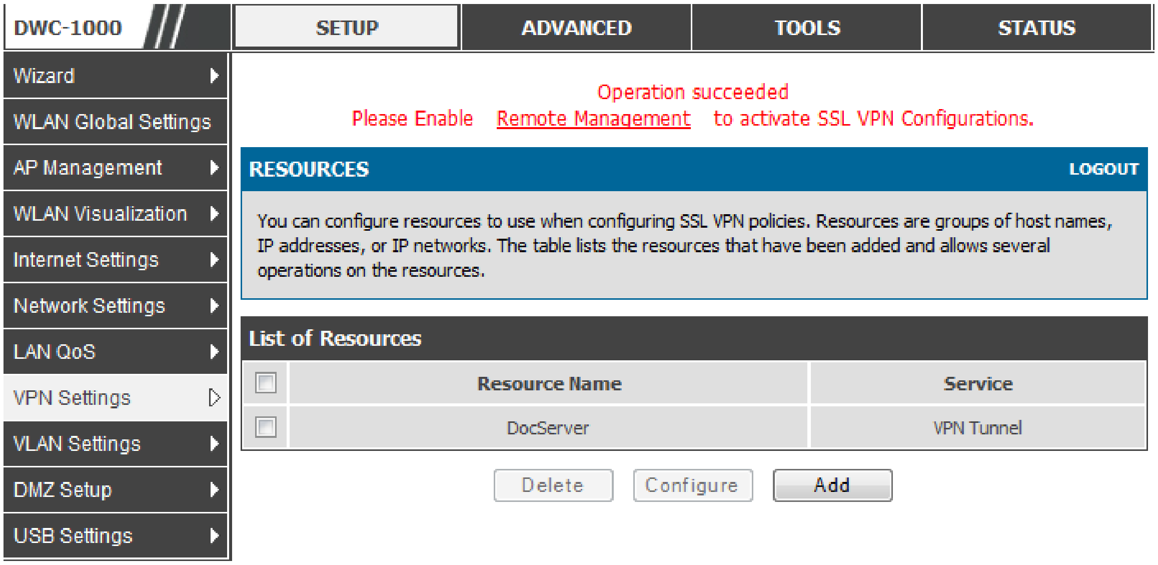
Network resources are services or groups of LAN IP addresses that are used to easily create and configure SSL VPN policies. This shortcut saves time when creating similar policies for multiple remote SSL VPN users.

Adding a Network Resource involves creating a unique name to identify the resource and assigning it to one or all of the supported SSL services. Once this is done, editing one of the created network resources allows you to configure the object type (either IP address or IP range) associated with the service. The Network Address, Mask Length, and Port Range/Port Number can all be defined for this resource as required. A network resource can be defined by configuring the following in the GUI:

Resource Name: A unique identifier name for the resource.

Service: The SSL VPN service corresponding to the resource (VPN tunnel, Port Forwarding or All).

Figure 160: List of configured resources, which are available to assign to SSL VPN policies



Operation succeeded
Please Enable Remote Management to activate SSL VPN Configurations.

RESOURCES

You can configure resources to use when configuring SSL VPN policies. Resources are groups of host names, IP addresses, or IP networks. The table lists the resources that have been added and allows several operations on the resources.

List of Resources

□	Resource Name	Service
□	DocServer	VPN Tunnel

9.3 Application Port Forwarding

Setup > VPN Settings > SSL VPN Server > Port Forwarding

Port forwarding allows remote SSL users to access specified network applications or services after they login to the User Portal and launch the Port Forwarding service. Traffic from the remote user to the controller is detected and re-routed based on configured port forwarding rules.

Internal host servers or TCP applications must be specified as being made accessible to remote users. Allowing access to a LAN server requires entering the local server IP address and TCP port number of the application to be tunneled. The table below lists some common applications and corresponding TCP port numbers:

TCP Application	**Port Number**
FTP Data (usually not needed)	20
FTP Control Protocol	21
SSH	22
Telnet	23
SMTP (send mail)	25
HTTP (web)	80
POP3 (receive mail)	110
NTP (network time protocol)	123
Citrix	1494
Terminal Services	3389
VNC (virtual network computing)	5900 or 5800

As a convenience for remote users, the hostname (FQDN) of the network server can be configured to allow for IP address resolution. This host name resolution provides users with easy-to-remember FQDN's to access TCP applications instead of error-prone IP addresses when using the Port Forwarding service through the SSL User Portal.

To configure port forwarding, following are required:

Local Server IP address: The IP address of the local server which is hosting the application.

TCP port: The TCP port of the application

Once the new application is defined it is displayed in a list of configured applications for port forwarding.

allow users to access the private network servers by using a hostname instead of an IP address, the FQDN corresponding to the IP address is defined in the port forwarding host configuration section.

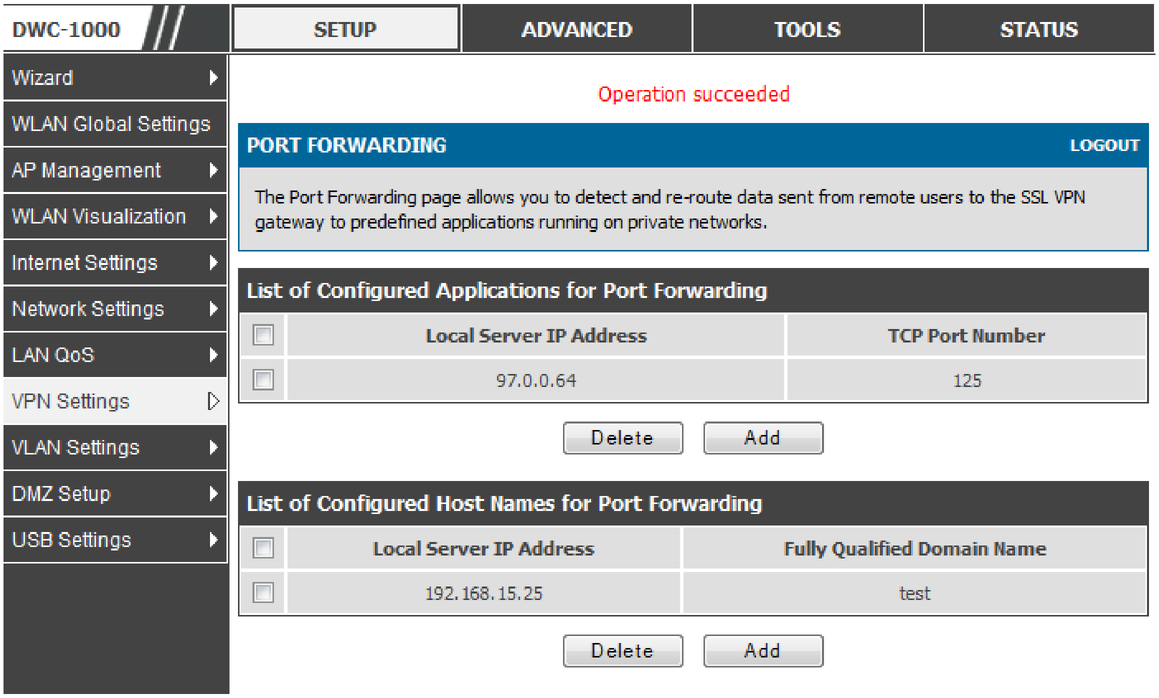
Local server IP address: The IP address of the local server hosting the application. The application should be configured in advance.

Fully qualified domain name: The domain name of the internal server is to be specified

Once the new FQDN is configured, it is displayed in a list of configured hosts for port forwarding.

> ✍ Defining the hostname is optional as minimum requirement for port forwarding is identifying the TCP application and local server IP address. The local server IP address of the configured hostname must match the IP address of the configured application for port forwarding.

Figure 161: List of Available Applications for SSL Port Forwarding



Operation succeeded

PORT FORWARDING

The Port Forwarding page allows you to detect and re-route data sent from remote users to the SSL VPN gateway to predefined applications running on private networks.

List of Configured Applications for Port Forwarding

□	Local Server IP Address	TCP Port Number
□	97.0.0.64	125

List of Configured Host Names for Port Forwarding

□	Local Server IP Address	Fully Qualified Domain Name
□	192.168.15.25	test

9.4 SSL VPN Client Configuration

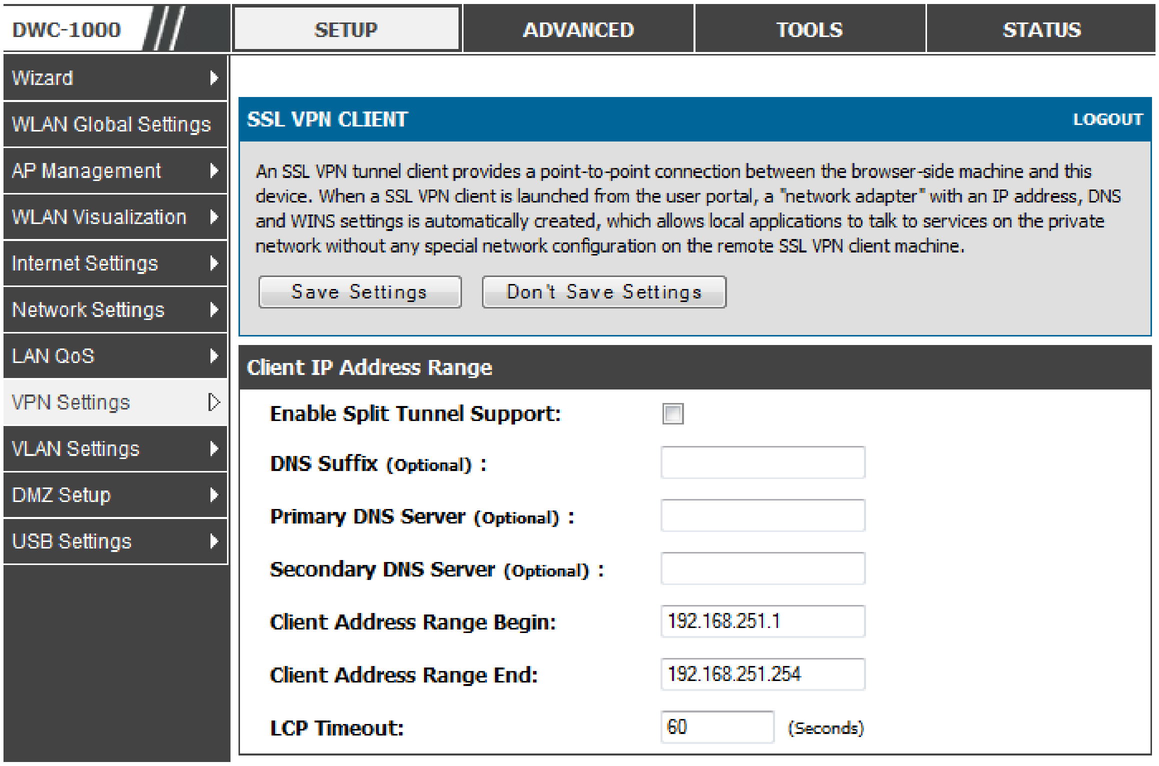
Setup > VPN Settings > SSL VPN Client > SSL VPN Client

An SSL VPN tunnel client provides a point-to-point connection between the browser-side machine and this controller. When a SSL VPN client is launched from the user portal, a "network adapter" with an IP address from the corporate subnet, DNS and WINS settings is automatically created. This allows local applications to access services on the private network without any special network configuration on the remote SSL VPN client machine.

It is important to ensure that the virtual (PPP) interface address of the VPN tunnel client does not conflict with physical devices on the LAN. The IP address range for the SSL VPN virtual network adapter should be either in a different subnet or non-overlapping range as the corporate LAN.

> ✍ The IP addresses of the client's network interfaces (Ethernet, Wireless, etc.) cannot be identical to the controller's IP address or a server on the corporate LAN that is being accessed through the SSL VPN tunnel.

Figure 162: SSL VPN client adapter and access configuration



An SSL VPN tunnel client provides a point-to-point connection between the browser-side machine and this device. When a SSL VPN client is launched from the user portal, a "network adapter" with an IP address, DNS and WINS settings is automatically created, which allows local applications to talk to services on the private network without any special network configuration on the remote SSL VPN client machine.

Client IP Address Range

Enable Split Tunnel Support:	☐
DNS Suffix (Optional) :	
Primary DNS Server (Optional) :	
Secondary DNS Server (Optional) :	
Client Address Range Begin:	192.168.251.1
Client Address Range End:	192.168.251.254
LCP Timeout:	60 (Seconds)

The controller allows full tunnel and split tunnel support. Full tunnel mode just sends all traffic from the client across the VPN tunnel to the controller. Split tunnel mode only sends traffic to the private LAN based on pre-specified client routes. These client routes give the SSL client access to specific private networks, thereby allowing access control over specific LAN services.

Client level configuration supports the following:

Enable Split Tunnel Support: With a split tunnel, only resources which are referenced by client routes can be accessed over the VPN tunnel. With full tunnel support (if the split tunnel option is disabled the DWC-1000 acts in full tunnel mode) all addresses on the private network are accessible over the VPN tunnel. Client routes are not required.

DNS Suffix: The DNS suffix name which will be given to the SSL VPN client. This configuration is optional.

Primary DNS Server: DNS server IP address to set on the network adaptor created on the client host. This configuration is optional.

Secondary DNS Server: Secondary DNS server IP address to set on the network adaptor created on the client host. This configuration is optional.

Client Address Range Begin: Clients who connect to the tunnel get a DHCP served IP address assigned to the network adaptor from the range of addresses beginning with this IP address

Client Address Range End: The ending IP address of the DHCP range of addresses served to the client network adaptor.

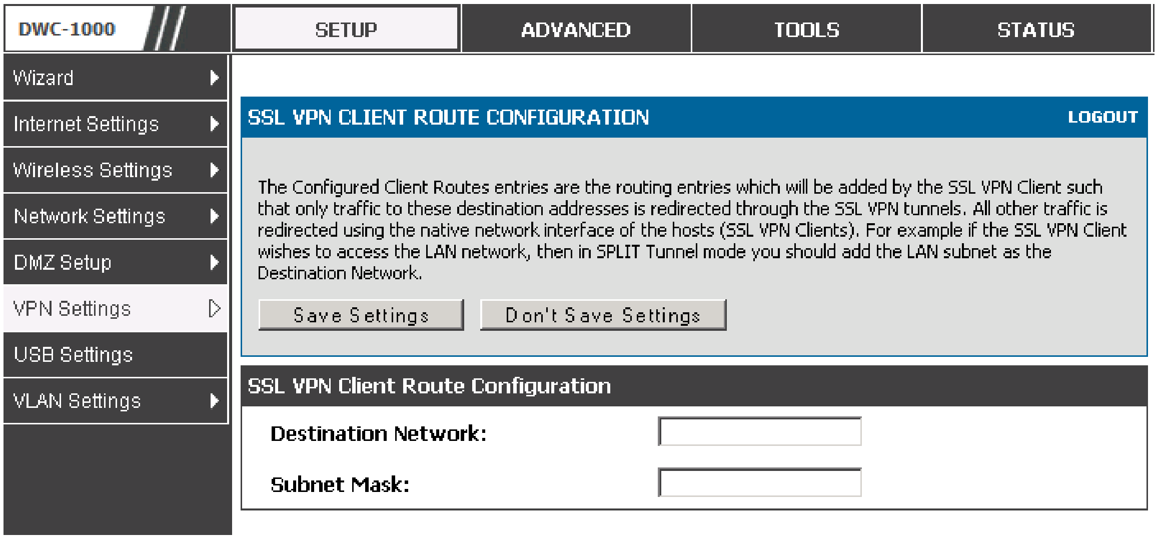
Setup > VPN Settings > SSL VPN Client > Configured Client Routes

If the SSL VPN client is assigned an IP address in a different subnet than the corporate network, a client route must be added to allow access to the private LAN through the VPN tunnel. As well a static route on the private LAN’s firewall (typically this controller) is needed to forward private traffic through the VPN Firewall to the remote SSL VPN client. When split tunnel mode is enabled, the user is required to configure routes for VPN tunnel clients:

Destination Network: The network address of the LAN or the subnet information of the destination network from the VPN tunnel clients’ perspective is set here.

Subnet Mask: The subnet information of the destination network is set here.

Figure 163: Configured client routes only apply in split tunnel mode



SSL VPN CLIENT ROUTE CONFIGURATION

The Configured Client Routes entries are the routing entries which will be added by the SSL VPN Client such that only traffic to these destination addresses is redirected through the SSL VPN tunnels. All other traffic is redirected using the native network interface of the hosts (SSL VPN Clients). For example if the SSL VPN Client wishes to access the LAN network, then in SPLIT Tunnel mode you should add the LAN subnet as the Destination Network.

SSL VPN Client Route Configuration

Destination Network:

Subnet Mask:

9.4.1 Creating Portal Layouts

Setup > VPN Settings > SSL VPN Server > Portal Layouts

The controller allows you to create a custom page for remote SSL VPN users that is presented upon authentication. There are various fields in the portal that are customizable for the domain, and this allows the controller administrator to communicate details such as login instructions, available services, and other usage details in the portal visible to remote users. During domain setup, configured portal layouts are available to select for all users authenticated by the domain.

> ✍ The default portal LAN IP address is https://192.168.10.1/scgi-bin/userPortal/portal. This is the same page that opens when the "User Portal" link is clicked on the SSL VPN menu of the controller GUI.

The controller administrator creates and edits portal layouts from the configuration pages in the SSL VPN menu. The portal name, title, banner name, and banner contents are all customizable to the intended users for this portal. The portal name is appended to the SSL VPN portal URL. As well, the users assigned to this portal (through their authentication domain) can be presented with one or more of the controller's supported SSL services such as the VPN Tunnel page or Port Forwarding page.

To configure a portal layout and theme, following information is needed:

Portal Layout Name: A descriptive name for the custom portal that is being configured. It is used as part of the SSL portal URL.

Portal Site Title: The portal web browser window title that appears when the client accesses this portal. This field is optional.

Banner Title: The banner title that is displayed to SSL VPN clients prior to login. This field is optional.

Banner Message: The banner message that is displayed to SSL VPN clients prior to login. This field is optional.

Display banner message on the login page: The user has the option to either display or hide the banner message in the login page.

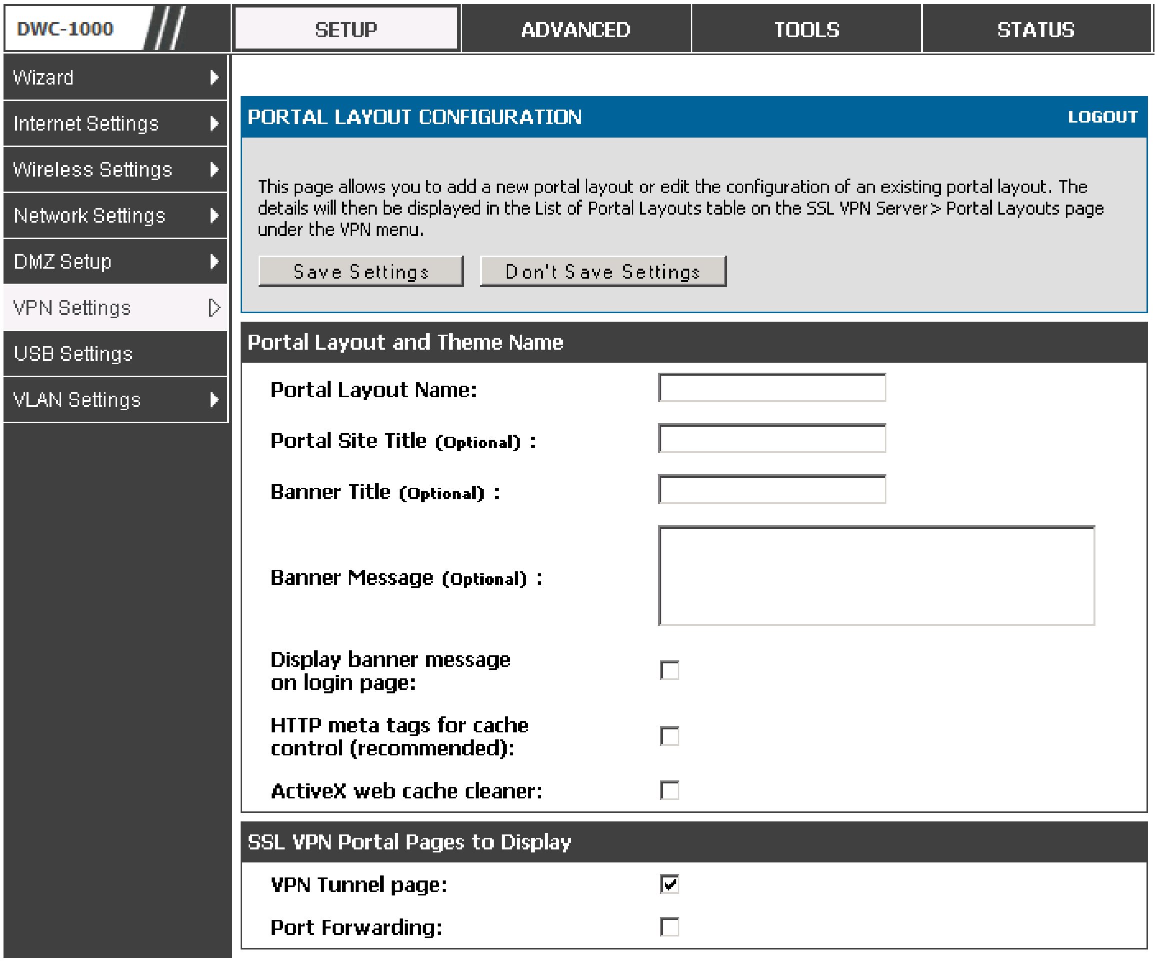
HTTP meta tags for cache control: This security feature prevents expired web pages and data from being stored in the client's web browser cache. It is recommended that the user selects this option.

ActiveX web cache cleaner: An ActiveX cache control web cleaner can be pushed from the gateway to the client browser whenever users login to this SSL VPN portal.

SSL VPN portal page to display: The User can either enable VPN tunnel page or Port Forwarding, or both depending on the SSL services to display on this portal.

Once the portal settings are configured, the newly configured portal is added to the list of portal layouts.

Figure 164: SSL VPN Portal configuration



PORTAL LAYOUT CONFIGURATION

This page allows you to add a new portal layout or edit the configuration of an existing portal layout. The details will then be displayed in the List of Portal Layouts table on the SSL VPN Server > Portal Layouts page under the VPN menu.

Portal Layout and Theme Name

Portal Layout Name:	
Portal Site Title (Optional) :	
Banner Title (Optional) :	
Banner Message (Optional) :	
Display banner message on login page:	□
HTTP meta tags for cache control (recommended):	□
ActiveX web cache cleaner:	□

SSL VPN Portal Pages to Display

VPN Tunnel page:	☑
Port Forwarding:	□

Chapter 10. Advanced System Functionalities

10.1 USB Device Setup

Setup > USB Settings > USB Status

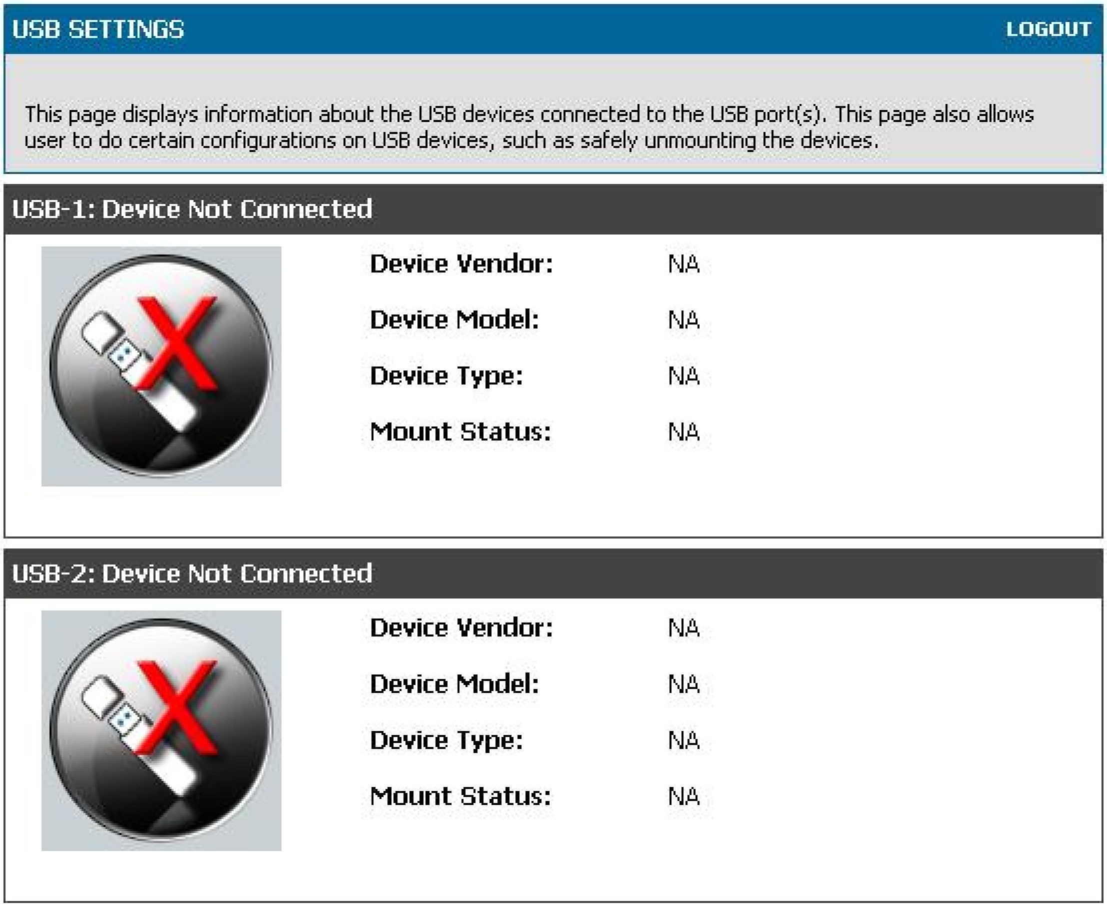
The DWC-1000 Wireless controller has a USB interface for printer access, file sharing.

- USB Mass Storage: also referred to as a “share port”, files on a USB disk connected to the DWC can be accessed by LAN users as a network drive.
- USB Printer: The DWC can provide the LAN with access to printers connected through the USB. The printer driver will have to be installed on the LAN host and traffic will be routed through the DWC between the LAN and printer.

To configure printer on a Windows machine, follow below given steps:

1. Click **'Start'** on the desktop.
2. Select ‘**Printers and faxes’** option.
3. Right click and select **'add printer'** or click on **'Add printer'** present at the left menu.
4. Select the '**Network Printer'** radio button and click next (select "device isn't listed in case of Windows7").
5. Select the **'Connect to printer using URL'** radio button ('Select a shared printer by name ‘in case of Windows 7) and give the following URL http://< controller’s LAN IP address>:631/printers/<Model Name> (Model Name can be found in the USB status page of controller’s GUI).
6. Click **'next'** and select the appropriate driver from the displayed list.
7. Click on **'next'** and 'finish' to complete adding the printer.

Figure 165: USB Device Detection



This page displays information about the USB devices connected to the USB port(s). This page also allows user to do certain configurations on USB devices, such as safely unmounting the devices.

USB-1: Device Not Connected

Device Vendor:	NA
Device Model:	NA
Device Type:	NA
Mount Status:	NA

USB-2: Device Not Connected

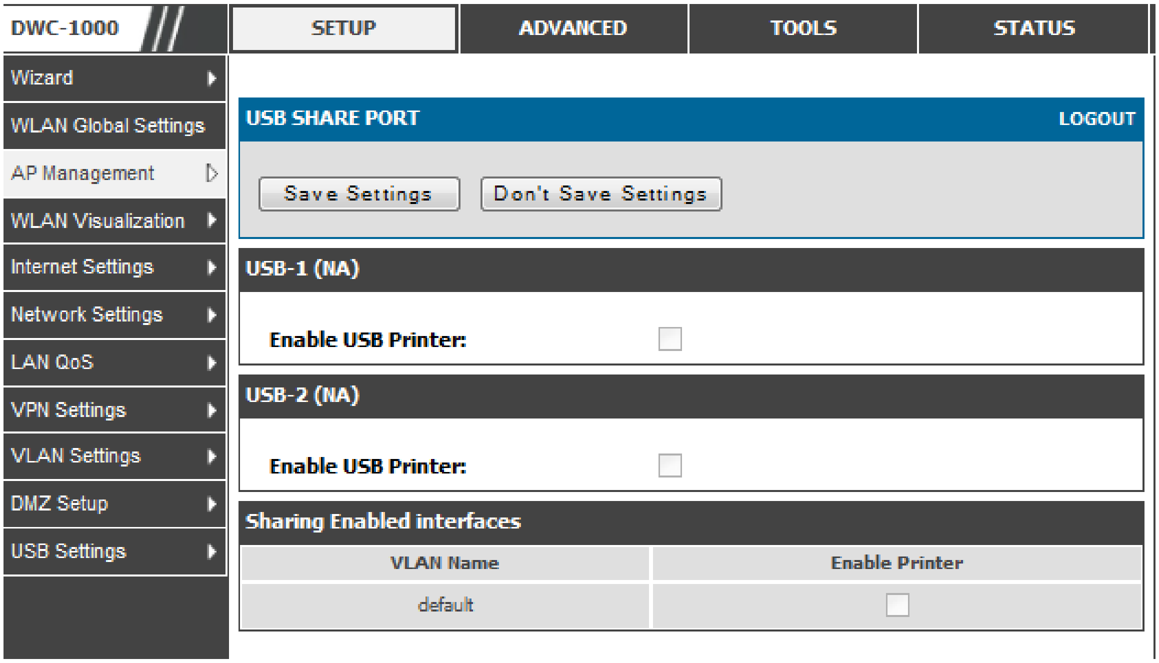
Device Vendor:	NA
Device Model:	NA
Device Type:	NA
Mount Status:	NA

10.2 USB Share Port

Setup > USB Settings > USB Status

The DWC-1000 Wireless controller has a USB interface for printer access this page allows you to enable USB device support for both interface USB1 and USB2. It also allows you to enable printer access from a particular VLAN.

Figure 166: USB Share Port



USB SHARE PORT

USB-1 (NA)

Enable USB Printer: □

USB-2 (NA)

Enable USB Printer: □

Sharing Enabled interfaces

VLAN Name	Enable Printer
default	□

10.3 Authentication Certificates

Advanced > Certificates

This gateway uses digital certificates for IPsec VPN authentication as well as SSL validation (for HTTPS and SSL VPN authentication). You can obtain a digital certificate from a well-known Certificate Authority (CA) such as VeriSign, or generate and sign your own certificate using functionality available on this gateway. The gateway comes with a self-signed certificate, and this can be replaced by one signed by a CA as per your networking requirements. A CA certificate provides strong assurance of the server’s identity and is a requirement for most corporate network VPN solutions.

The certificates menu allows you to view a list of certificates (both from a CA and self-signed) currently loaded on the gateway. The following certificate data is displayed in the list of Trusted (CA) certificates:

CA Identity (Subject Name): The certificate is issued to this person or organization

Issuer Name: This is the CA name that issued this certificate

Expiry Time: The date after which this Trusted certificate becomes invalid

A self certificate is a certificate issued by a CA identifying your device (or self-signed if you don't want the identity protection of a CA). The Active Self Certificate table lists the self certificates currently loaded on the gateway. The following information is displayed for each uploaded self certificate:

Name: The name you use to identify this certificate, it is not displayed to IPsec VPN peers or SSL users.

Subject Name: This is the name that will be displayed as the owner of this certificate. This should be your official registered or company name, as IPsec or SSL VPN peers are shown this field.

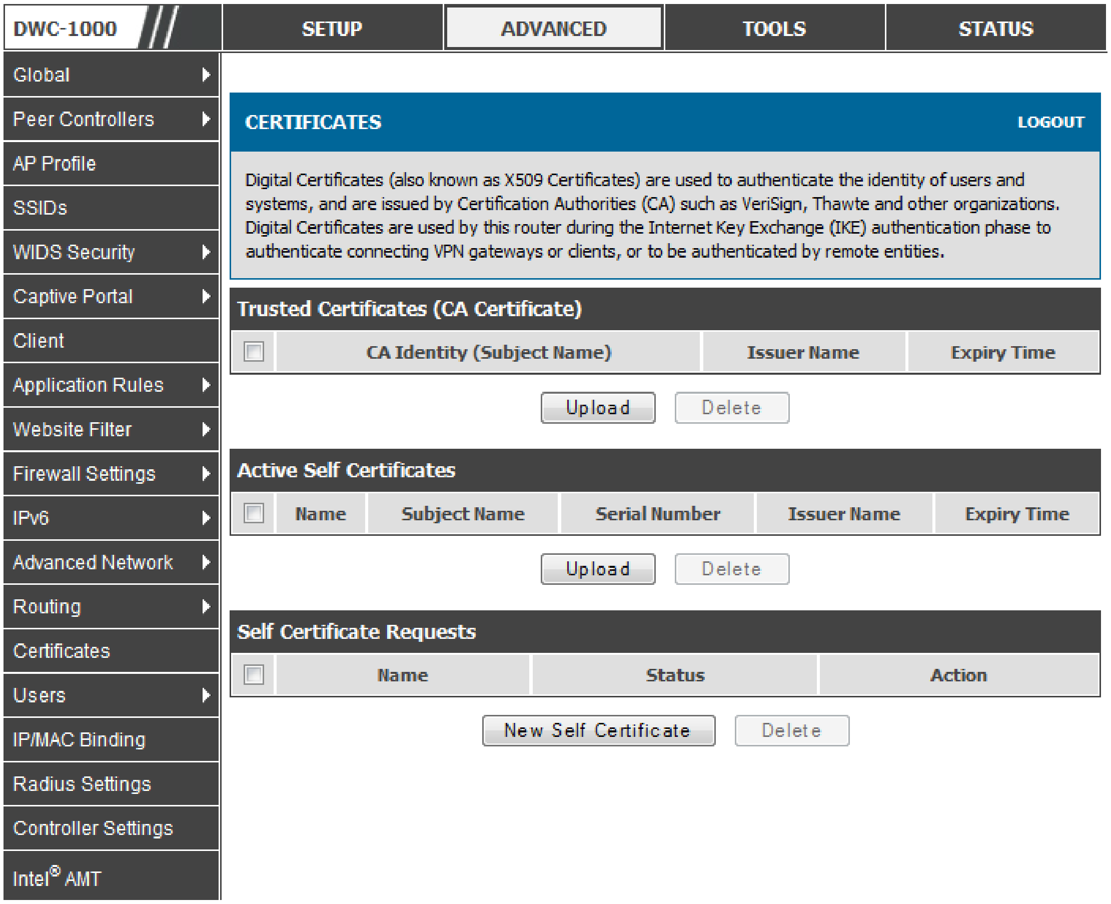
Serial Number: The serial number is maintained by the CA and used to identify this signed certificate.

Issuer Name: This is the CA name that issued (signed) this certificate

Expiry Time: The date after which this signed certificate becomes invalid – you should renew the certificate before it expires.

To request a self certificate to be signed by a CA, you can generate a Certificate Signing Request from the gateway by entering identification parameters and passing it along to the CA for signing. Once signed, the CA's Trusted Certificate and signed certificate from the CA are uploaded to activate the self-certificate validating the identity of this gateway. The self certificate is then used in IPsec and SSL connections with peers to validate the gateway's authenticity.

Figure 167: Certificate summary for IPsec and HTTPS management



CERTIFICATES

Digital Certificates (also known as X509 Certificates) are used to authenticate the identity of users and systems, and are issued by Certification Authorities (CA) such as VeriSign, Thawte and other organizations. Digital Certificates are used by this router during the Internet Key Exchange (IKE) authentication phase to authenticate connecting VPN gateways or clients, or to be authenticated by remote entities.

Trusted Certificates (CA Certificate)

□	CA Identity (Subject Name)	Issuer Name	Expiry Time

Active Self Certificates

□	Name	Subject Name	Serial Number	Issuer Name	Expiry Time

Self Certificate Requests

□	Name	Status	Action

10.4 Intel ®AMT

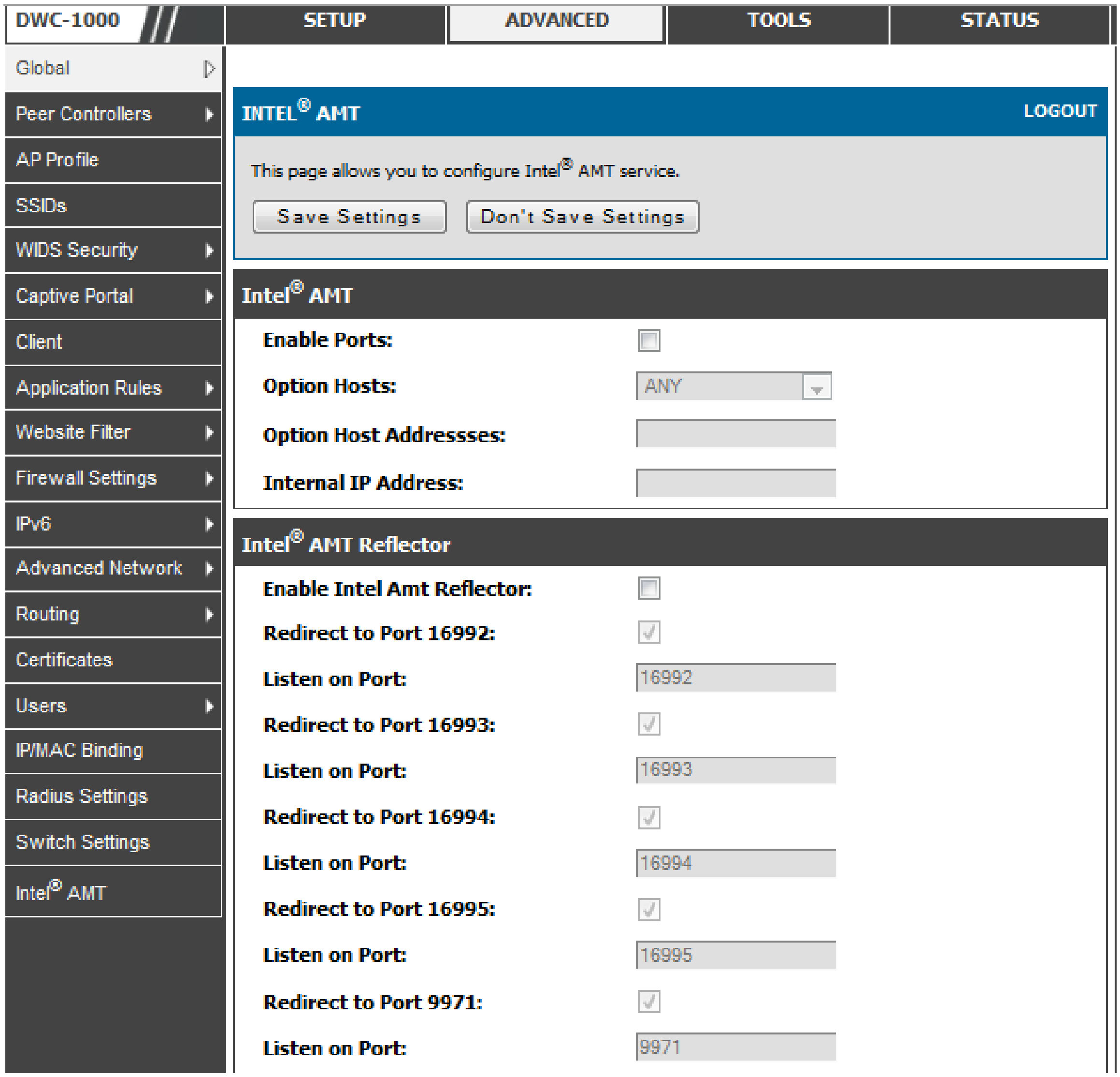
This feature is available upon licensed activation of VPN / Firewall features for the system.

Advanced > Intel ®AMT

Intel® Active Management Technology enables IT managers to remotely access and manage every networked computing system, even those that lack a working operating system or hard drive, or are turned off as long as the PC/Notebook is connected to line power and to the network even if PC/Notebook is off or OS is crashed. Intel® AMT uses a separate management processor that runs independently on the client machine and can be reached through the wired or wireless network. With D-Link DSR Routers, Intel®

AMT Technology could cross Internet seamlessly and it's an ideal solution to help IT managers for asset management over Internet..

Figure 168: Intel ®AMT



This page allows you to configure Intel® AMT service.

Enable Ports:	□
Option Hosts:	ANY
Option Host Addressses:	
Internal IP Address:	
Enable Intel Amt Reflector:	□
Redirect to Port 16992:	☑
Listen on Port:	16992
Redirect to Port 16993:	☑
Listen on Port:	16993
Redirect to Port 16994:	☑
Listen on Port:	16994
Redirect to Port 16995:	☑
Listen on Port:	16995
Redirect to Port 9971:	☑
Listen on Port:	9971

Enable Ports: When enabled, inbound/outbound firewall rules are added for certain ports to enable Intel® AMT service.

Option Hosts: If the user selects ANY, all Option side hosts are granted access to the local server. If the user selects "Specify Option IPs", he must provide a comma separated list of Option host addresses that are to be allowed access to the Local Server (LAN Host).

Option Host Addresses: The user must provide a comma separated list of Option IP addresses that must be allowed access to the Local Server in case he has selected "Specify Option IPs" in the Drop down menu. Only commas are allowed and there should be no spaces between the comma and the IP address

Internal IP Address: The user must provide a single IP address of the LAN host (Local Server).

Enable Intel® AMT Reflector: Check this box to reflect back the data on selected ports to the client initiating the connection.

Redirect to Port 16992: Check this box to redirect to port 16992 of the client initiating the connection.

Listen on Port: Enter the port on which server should listen for incoming connections.

Redirect to Port 16993: Check this box to redirect to port 16993 of the client initiating the connection.

Listen on Port: Enter the port on which server should listen for incoming connections.

Redirect to Port 16994: Check this box to redirect to port 16994 of the client initiating the connection.

Listen on Port: Enter the port on which server should listen for incoming connections.
Redirect to Port 16995: Check this box to redirect to port 16995 of the client initiating the connection.

Listen on Port: Enter the port on which server should listen for incoming connections.
Redirect to Port 9971: Check this box to redirect to port 9971 of the client initiating the connection.

Listen on Port: Enter the port on which server should listen for incoming connections.

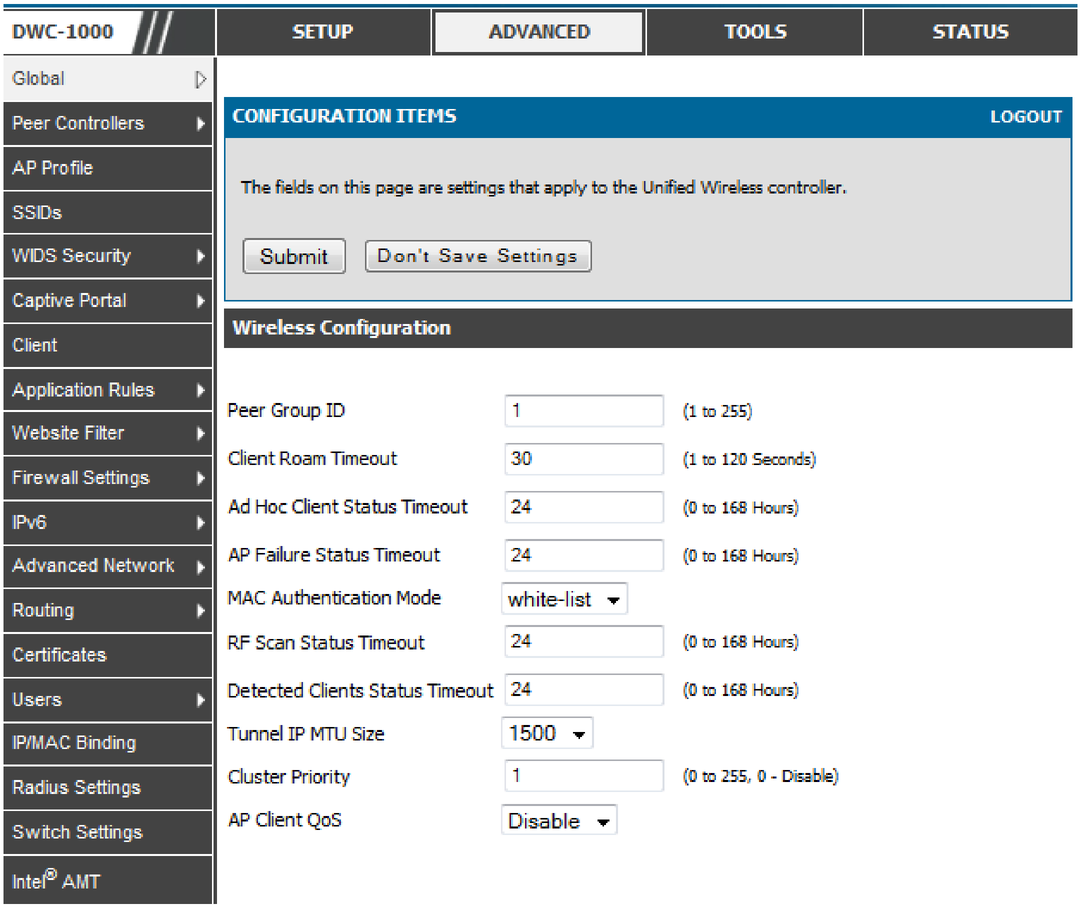
Chapter 11. Advanced Wireless Controller Features

11.1 General

Advanced > Global > General

The fields on the advanced Wireless Global Configuration page are settings that apply to the DWC-1000 Wireless Controller.

Figure 169: Wireless Configuration



The fields on this page are settings that apply to the Unified Wireless controller.

Peer Group ID	1	(1 to 255)
Client Roam Timeout	30	(1 to 120 Seconds)
Ad Hoc Client Status Timeout	24	(0 to 168 Hours)
AP Failure Status Timeout	24	(0 to 168 Hours)
MAC Authentication Mode	white-list	
RF Scan Status Timeout	24	(0 to 168 Hours)
Detected Clients Status Timeout	24	(0 to 168 Hours)
Tunnel IP MTU Size	1500	
Cluster Priority	1	(0 to 255, 0 - Disable)
AP Client QoS	Disable	

Peer Group ID: In order to support larger networks, you can configure wireless controllers as peers, with up to 8 controllers in a cluster (peer group). Peer controllers share some information about APs and allow L3 roaming among them. Peers are grouped according to the Group ID.

Client Roam Timeout: This value determines how long to keep an entry in the Associated Client Status list after a client has disassociated. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted.

Ad Hoc Client Status Timeout: This value determines how long to keep an entry in the Ad Hoc Client Status list. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted.
AP Failure Status Timeout: This value determines how long to keep an entry in the AP Authentication Failure Status list. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted.
MAC Authentication Mode: Select the global action to take on wireless clients in the white-list: Select this option to specify that any wireless clients with MAC addresses that are specified in the Known Client database, and are not explicitly denied access, are granted access. If the MAC address is not in the database then the access to the client is denied.

Detected Clients Status Timeout: This value determines how long to keep an entry in the Detected Client Status list. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted.
Tunnel IP MTU Size: Select the maximum size of an IP packet handled by the network. The MTU is enforced only on tunneled VAPs.
When IP packets are tunneled between the APs and the Unified Wireless controller, the packet size is increased by 20 bytes during transit. This means that clients configured for 1500 byte IP MTU size may exceed the maximum MTU size of existing network infrastructure which is set up to controller and route 1518 (1522-tagged) byte frames. If you increase the tunnel IP MTU size, you must also increase the physical MTU of the ports on which the traffic flows. Note: f any of the following conditions are true, you do not need to increase the tunnel IP MTU size:
The wireless network does not use L3 tunneling.
The tunneling mode is used only for voice traffic, which typically has small packets. The tunneling mode is used only for TCP based protocols, such as HTTP. This is because the

AP automatically reduces the maximum segment size for all TCP connections to fit within the tunnel.

Cluster Priority: Specify the priority of this controller for the Cluster Controller election. The controller with highest priority in a cluster becomes the Cluster Controller. If the priority is the same for all controllers, then the controller with lowest IP address becomes the Cluster Controller. A priority of 0 means that the controller cannot become the Cluster Controller. The highest possible priority is 255.
AP Client QoS: Enable or disable the client QoS feature. If AP Client QoS is disabled, the Client QoS configuration remains in place, but any ACLs or DiffServ policies applied to wireless traffic are not enforced.
The Client QoS feature extends the primary QoS capabilities of the Unified Wireless controller to the wireless domain. More specifically, access control lists (ACLs) and differentiated service (DiffServ) policies are applied to wireless clients associated to the Apothem maximum MTU size of existing network infrastructure which is set up to controller and route 1518 (1522-tagged) byte frames. If you increase the tunnel IP MTU size, you must also increase the physical MTU of the ports on which the traffic flows.

11.2 SNMP Trap

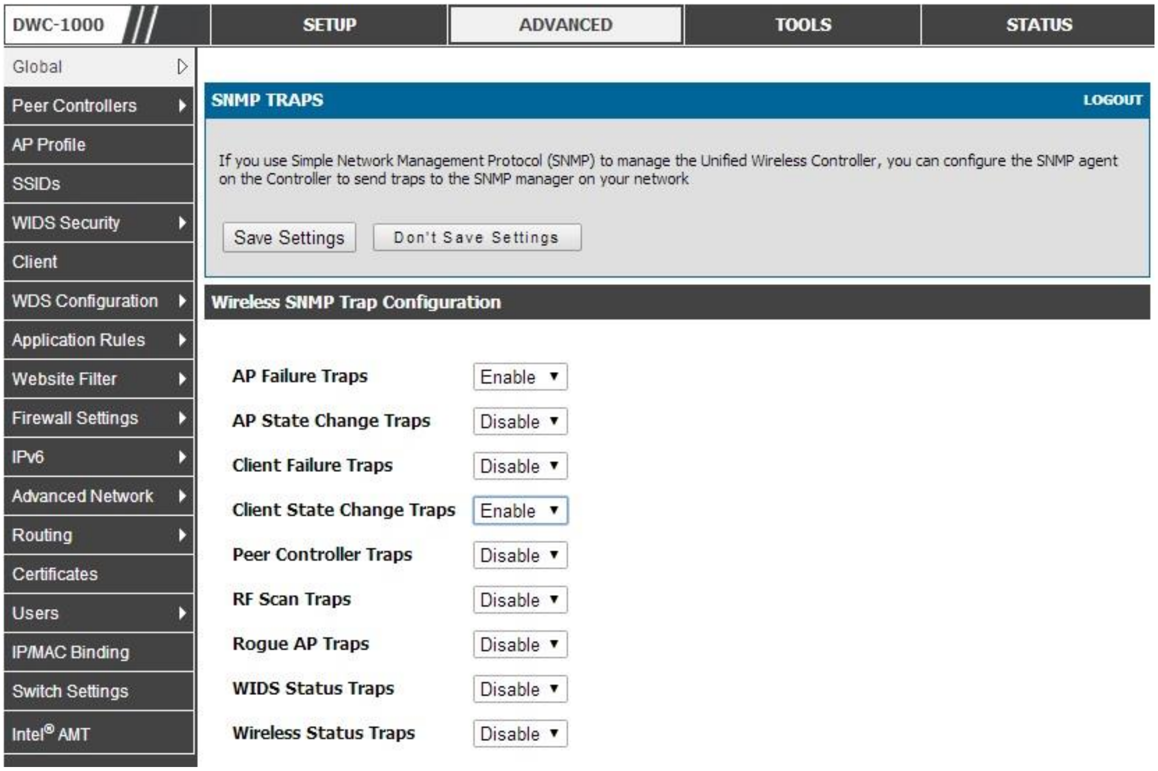
Advanced > Global > General

Traps are asynchronous notifications sent from the SNMP agent to a SNMP manager. Traps allow an agent to notify the management station of significant events by way of an unsolicited SNMP message. The device can act as an agent and can send asynchronous notification when certain events happen.

DWC-1000 supports both public and private traps:

- **Public** traps include traps specified in RFC-1215. Details are in the SNMPv2-MIB.txt MIB file available with the DWC-1000 firmware. Example: the coldStart trap comes under snmpTraps which is having value 1.
- **Private** traps mainly consist of wireless traps. Details are in the dlinkwlan.mib file. Example: the wsClientAssociationDetected trap comes under wsTraps which having value 20.

Figure 170: SNMP Trap settings



If you use Simple Network Management Protocol (SNMP) to manage the Unified Wireless Controller, you can configure the SNMP agent on the Controller to send traps to the SNMP manager on your network

Wireless SNMP Trap Configuration

AP Failure Traps	Enable
AP State Change Traps	Disable
Client Failure Traps	Disable
Client State Change Traps	Enable
Peer Controller Traps	Disable
RF Scan Traps	Disable
Rogue AP Traps	Disable
WIDS Status Traps	Disable
Wireless Status Traps	Disable

To user SNMP traps, associate the device to a trap manager. Add the trap manager IP address and port in the ***Maintenance > Management > SNMP > SNMP Trap List*** page:

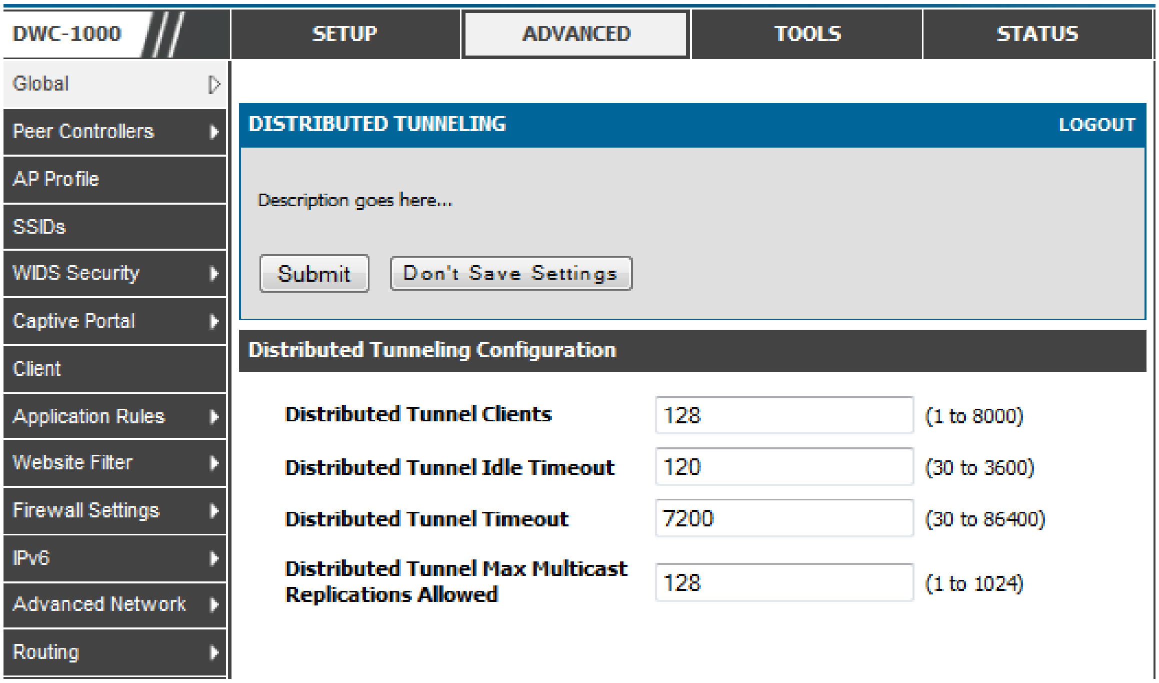
- IP Address: IP address of SNMP manager
- Port: Trap port number [Range: 0 - 65535]
- Community: community used for authentication
- Authentication Type - v1/v2c/v3

11.3 Distributed Tunneling

Advanced > Global > Distributed Tunneling

The Distributed Tunneling mode, also known as AP-AP tunneling mode, is used to support L3 roaming for wireless clients without forwarding any data traffic to the wireless controller. In the AP-AP tunneling mode, when a client first associates with an AP in the wireless system the AP forwards its data using the VLAN forwarding mode. The AP to which the client initially associates is the Home AP. The AP to which the client roams is the Association AP.

Figure 171: Distributed Tunneling



DISTRIBUTED TUNNELING

Description goes here...

Distributed Tunneling Configuration

Distributed Tunnel Clients	128	(1 to 8000)
Distributed Tunnel Idle Timeout	120	(30 to 3600)
Distributed Tunnel Timeout	7200	(30 to 86400)
Distributed Tunnel Max Multicast Replications Allowed	128	(1 to 1024)

Distributed Tunnel Clients: Specify the maximum number of distributed tunneling clients that can roam away from the Home AP at the same time.

Distributed Tunnel Idle Timeout: Specify the number of seconds of no activity by the client before the tunnel to that client is terminated and the client is forced to change its IP address.

Distributed Tunnel Timeout: Specify the number of seconds before the tunnel to the roamed client is terminated and the client is forced to change its IP address.

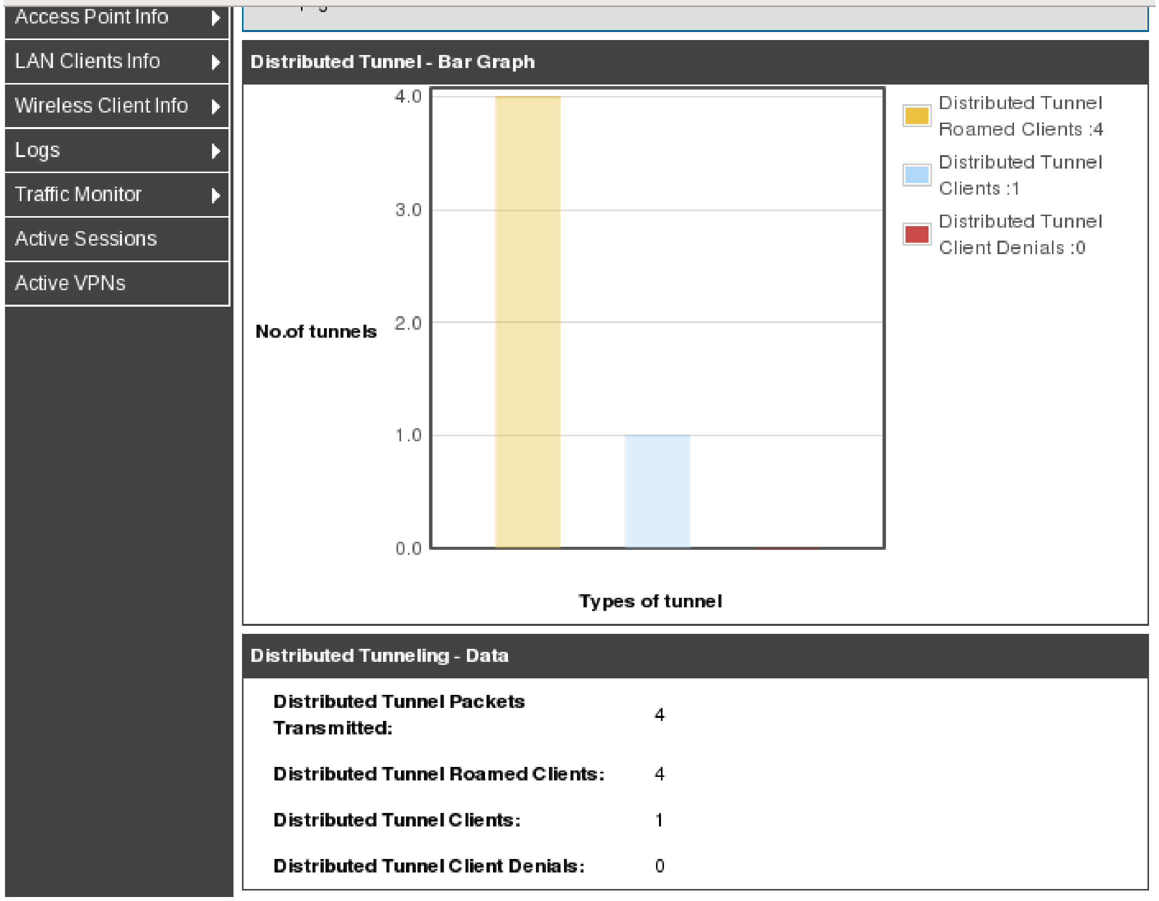
Distributed Tunnel Max Multicast Replications Allowed: Specify the maximum number of tunnels to which a multicast frame is copied on the Home AP.

11.3.1 Distributed Tunneling Status

Status > Dashboard > Distributed Tunneling

This page shows information about all the distributed tunnel clients.

Figure 172: Distributed Tunneling Clients


Access Point Info
LAN Clients Info
Wireless Client Info
Logs
Traffic Monitor
Active Sessions
Active VPNs
Distributed Tunnel - Bar Graph
4.0
3.0
2.0
1.0
0.0
No.of tunnels
Types of tunnel
Distributed Tunnel Roamed Clients :4
Distributed Tunnel Clients :1
Distributed Tunnel Client Denials :0
Distributed Tunneling - Data

Distributed Tunnel Packets Transmitted:	4
Distributed Tunnel Roamed Clients:	4
Distributed Tunnel Clients:	1
Distributed Tunnel Client Denials:	0

Distributed Tunnel Packets: Transmitted: Total number of packets sent by all APs via distributed tunnels.

Distributed Tunnel Roamed Clients: Total number of clients that successfully roamed away from Home AP using distributed tunneling.

Distributed Tunnel Clients: Total number of clients that are associated with an AP that are using distributed tunneling.

Distributed Tunnel Client Denials: Total number of clients for which the system was unable to set up a distributed tunnel when client roamed.

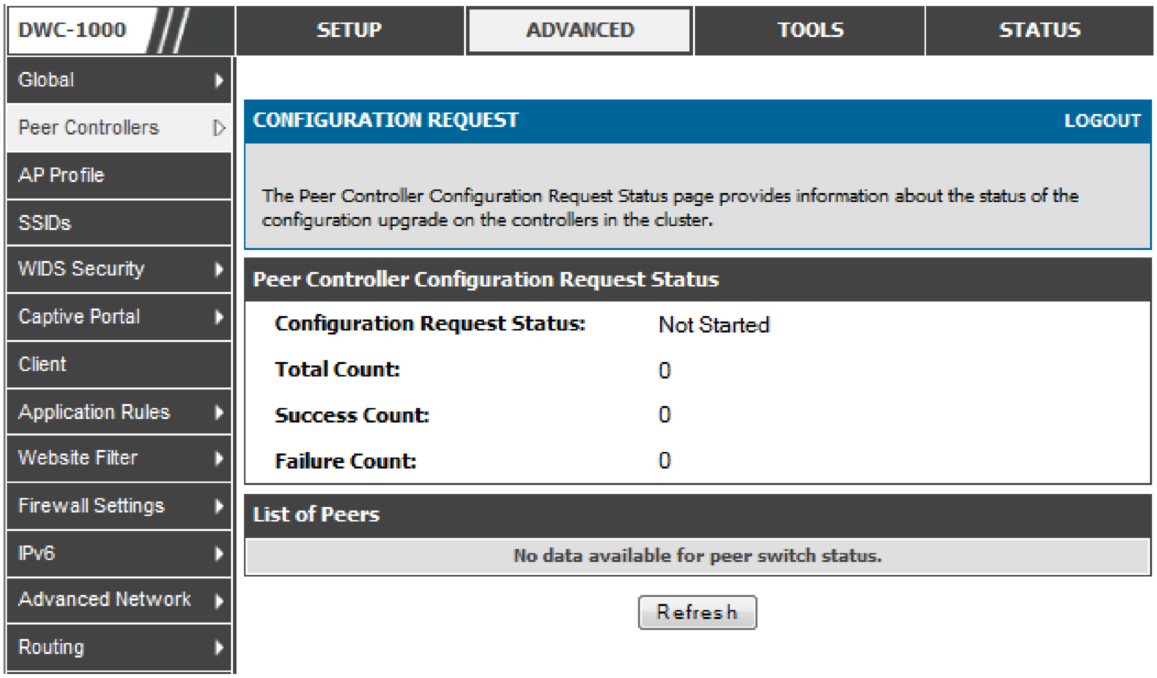
11.4 Peer Controller Configuration

11.4.1 Peer Controller Configuration Request Status

Advanced > Peer Controller > Configuration Request Status

The Peer Controller Configuration feature allows you to send a variety of configuration information from one controller to all other controllers. In addition to keeping the controllers synchronized, this function allows you to manage all wireless controllers in the cluster from one controller. The Peer Controller Configuration Request Status page provides information about the status of the configuration upgrade on the controllers in the cluster

Figure 173: Peer Controller Configuration Request Status



The Peer Controller Configuration Request Status page provides information about the status of the configuration upgrade on the controllers in the cluster.

Peer Controller Configuration Request Status

Configuration Request Status:	Not Started
Total Count:	0
Success Count:	0
Failure Count:	0

List of Peers

No data available for peer switch status.

Peer Controller Configuration Request Status:

Configuration Request Status: Indicates the global status for a configuration push operation to one or more peer controllers. The status can be one of the following:

- Not Started.
- Receiving Configuration.
- Saving Configuration.
- Success.
  Failure Invalid Code Version.
- Failure Invalid Hardware Version.
- Failure Invalid Configuration

Total Count: Indicates the number of peer controllers included at the time a configuration download request is started, the value is 1 if a download request is for a single controller.

Success Count: Indicates the total number of peer controllers that have successfully completed a configuration download.

Failure Count: Indicates the total number of peer controllers that have failed to complete a configuration download.

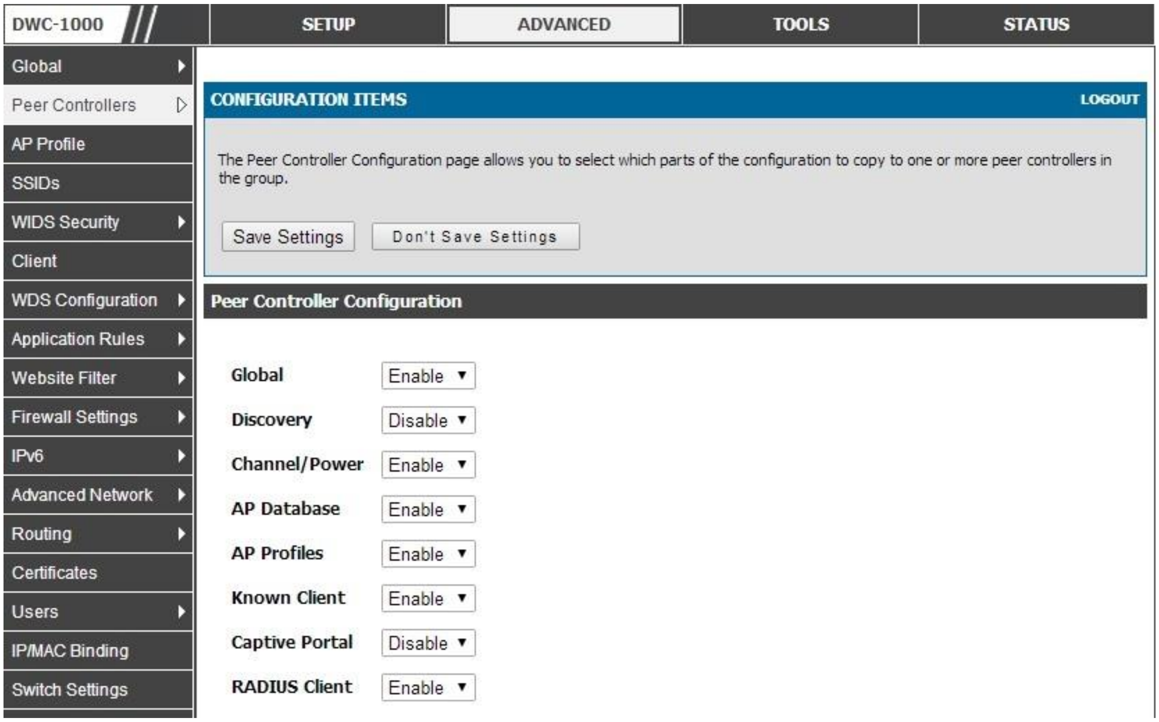
List of Peers Peer IP Address: Lists the IP address of each controller in the cluster and indicates the configuration request status of that controller.

11.4.2 Peer Controller Configuration

Advanced > Peer Controller > Configuration Items

The Peer Controller Configuration items pages allows to Enable/Disable allows you to select which parts of the configuration to copy to one

Figure 174: Peer Controller Configuration



CONFIGURATION ITEMS

The Peer Controller Configuration page allows you to select which parts of the configuration to copy to one or more peer controllers in the group.

Peer Controller Configuration

Global: Enable
Discovery: Disable
Channel/Power: Enable
AP Database: Enable
AP Profiles: Enable
Known Client: Enable
Captive Portal: Disable
RADIUS Client: Enable

Global: Enable this field to include the basic and advanced global settings in the configuration that the controller pushes to its peers. The configuration does not include the controller IP address since that is a unique setting.

Discovery: Enable this field to include the L2 and L3 discovery information, including the VLAN list and IP list, in the configuration that the controller pushes to its peers.

Channel/Power: Enable this field to include the RF management information in the configuration that the controller pushes to its peers.

AP Database: Enable this field to include the AP Database in the configuration that the controller pushes to its peers.

AP Profiles: Enable this field to include all AP profiles in the configuration that the controller pushes to its peers. The AP profile includes the global AP settings, such as the hardware type, Radio settings, VAP and Wireless Network settings, and QoS settings.

Known Client: Enable this field to include the Known Client Database in the configuration that the controller pushes to its peers.

Captive Portal: Enable this field to include Captive Portal information in the configuration that the controller pushes to its peers.

RADIUS Client: Enable this field to include the Client RADIUS information in the configuration that the controller pushes to its peers.

11.5 WIDS Configuration

The D-Link Wireless Controller Wireless Intrusion Detection System (WIDS) can help detect intrusion attempts into the wireless network and take automatic actions to protect the network.

11.5.1 WIDS AP configuration

Advanced > WIDS Security > AP

The WIDS AP Configuration page allows you to activate or deactivate various threat detection tests and set threat detection thresholds in order to help detect rogue APs on the wireless network. These changes can be done without disrupting network connectivity. Since some of the work is done by access points, the controller needs to send messages to the APs to modify its WIDS operational properties

Administrator configured rogue AP: If the source MAC address is in the valid-AP database on the controller or on the RADIUS server and the AP type is marked as Rogue, then the AP state is Rogue.

Managed SSID from an unknown AP: This test checks whether an unknown AP is using the managed network SSID. A hacker may set up an AP with managed SSID to fool users into associating with the AP and revealing password and other secure information. Administrators with large networks who are using multiple clusters

should either use different network names in each cluster or disable this test. Otherwise, if an AP in the first cluster detects APs in the second cluster transmitting the same SSID as APs in the first cluster then these APs are reported as rogues.

Managed SSID from a fake managed AP: A hacker may set up an AP with the same MAC address as one of the managed APs and configure it to send one of the managed SSIDs. This test checks for a vendor field in the beacons which is always transmitted by managed APs. If the vendor field is not present, then the AP is identified as a fake AP.

AP without an SSID: SSID is an optional field in beacon frames. To avoid detection a hacker may set up an AP with the managed network SSID, but disable SSID transmission in the beacon frames. The AP would still send probe responses to clients that send probe requests for the managed SSID fooling the clients into associating with the hacker's AP. This test detects and flags APs that transmit beacons without the SSID field. The test is automatically disabled if any of the radios in the profiles are configured not to send SSID field, which is not recommended because it does not provide any real security and disables this test.

Fake managed AP on an invalid channel: This test detects rogue APs that transmit beacons from the source MAC address of one of the managed APs, but on different channel from which the AP is supposed to be operating.

Managed SSID detected with incorrect security: During RF Scan the AP examines beacon frames received from other APs and determines whether the detected AP is advertising an open network, WEP, or WPA. If the SSID reported in the RF Scan is one of the managed networks and its configured security not match the detected security then this test marks the AP as rogue.

Invalid SSID from a managed AP: This test checks whether a known managed AP is sending an unexpected SSID. The SSID reported in the RF Scan is compared to the list of all configured SSIDs that are used by the profile assigned to the managed AP. If the detected SSID doesn't match any configured SSID then the AP is marked as rogue.

AP is operating on an illegal channel: The purpose of this test is to detect hackers or incorrectly configured devices that are operating on channels that are not legal in the country where the wireless system is set up. Note: In order for the wireless system to detect this threat, the wireless network must contain one or more radios that operate in sentry mode.

Standalone AP with unexpected configuration: If the AP is classified as a known standalone AP, then the controller checks whether the AP is operating with the expected configuration parameters. You configure the expected parameters for the standalone AP in the local or RADIUS Valid AP database. This test may detect network misconfiguration as well as potential intrusion attempts. The following parameters are checked:

- Channel Number
- SSID
- Security Mode
- WDS Mode.
- Presence on a wired network.

Unexpected WDS device detected on network: If the AP is classified as a Managed or Unknown AP and wireless distribution system (WDS) traffic is detected on the AP, then the AP is considered to be Rogue. Only stand-alone APs that are explicitly allowed to operate in WDS mode are not reported as rogues by this test.

Unmanaged AP detected on wired network: This test checks whether the AP is detected on the wired network. If the AP state is Unknown, then the test changes the AP state to Rogue. The flag indicating whether AP is detected on the wired network is reported as part of the RF Scan report. If AP is managed and is detected

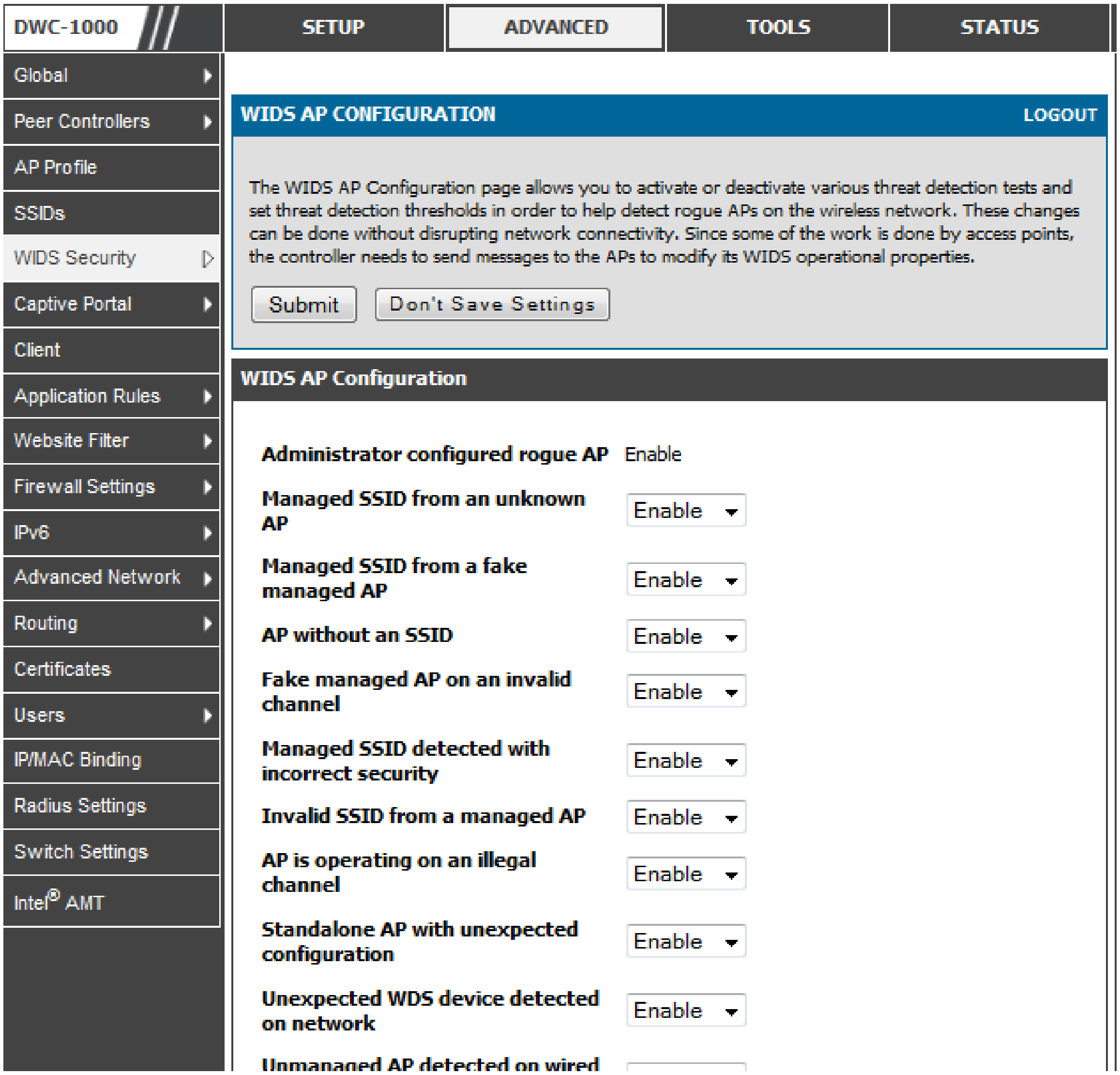
on the network then the controller simply reports this fact and doesn't change the AP state to Rogue. In order for the wireless system to detect this threat, the wireless network must contain one or more radios that operate in sentry mode

Rogue Detected Trap Interval: Specify the interval, in seconds, between transmissions of the SNMP trap telling the administrator that rogue APs are present in the RF Scan database. If you set the value to 0, the trap is never sent.

Wired Network Detection Interval: Specify the number of seconds that the AP waits before starting a new wired network detection cycle. If you set the value to 0, wired network detection is disabled

AP De-Authentication Attack: Enable or disable the AP de-authentication attack. The wireless controller can protect against rogue APs by sending DE authentication messages to the rogue AP. The de-authentication attack feature must be globally enabled in order for the wireless system to do this function. Make sure that no legitimate APs are classified as rogues before enabling the attack feature. This feature is disabled by default.

Figure 175: WIDS AP Configuration



WIDS AP CONFIGURATION

The WIDS AP Configuration page allows you to activate or deactivate various threat detection tests and set threat detection thresholds in order to help detect rogue APs on the wireless network. These changes can be done without disrupting network connectivity. Since some of the work is done by access points, the controller needs to send messages to the APs to modify its WIDS operational properties.

WIDS AP Configuration

Administrator configured rogue AP	Enable
Managed SSID from an unknown AP	Enable
Managed SSID from a fake managed AP	Enable
AP without an SSID	Enable
Fake managed AP on an invalid channel	Enable
Managed SSID detected with incorrect security	Enable
Invalid SSID from a managed AP	Enable
AP is operating on an illegal channel	Enable
Standalone AP with unexpected configuration	Enable
Unexpected WDS device detected on network	Enable
Unmanaged AP detected on wired	

11.5.2 WIDS Client Configuration

Advanced > WIDS Security > Client

The settings you configure on the WIDS Client Configuration page help determine whether a detected client is classified as a rogue. Clients classified as rogues are considered to be a threat to network security

The WIDS feature tracks the following types of management messages that each detected client sends:

- Probe Requests
- 802.11 Authentication Requests
- 802.11 De-Authentication Requests.

In order to help determine whether a client is posing a threat to the network by flooding the network with management traffic, the system keeps track of the number of times the AP received each message type and the highest message rate detected in a single RF Scan report. On the WIDS Client Configuration page, you can set thresholds for each type of message sent, and the APs monitor whether any clients exceed those thresholds or tests.

Not Present in OUI Database Test: This test checks whether the MAC address of the client is from a registered manufacturer identified in the OUI database.

Known Client Database Test: This test checks whether the client, which is identified by its MAC address, is listed in the Known Client Database and is allowed access to the AP either through the Authentication Action of Grant or through the White List global action. If the client is in the Known Client Database and has an action of Deny, or if the action is Global Action and it is globally set to Black List, the client fails this test.

Configured Authentication Rate Test: This test checks whether the client has exceeded the configured rate for transmitting 802.11 authentication requests.

Configured Probe Requests Rate Test: This test checks whether the client has exceeded the configured rate for transmitting probe requests.

Configured De-Authentication Requests Rate Test: This test checks whether the client has exceeded the configured rate for transmitting de-authentication requests.

Maximum Authentication Failures Test: This test checks whether the client has exceeded the maximum number of failed authentications.

Authentication with Unknown AP Test: This test checks whether a client in the Known Client database is authenticated with an unknown AP.

Client Threat Mitigation: Select enable to send de-authentication messages to clients that are in the Known Clients database but are associated with unknown APs. The Authentication with Unknown AP Test must also be enabled in order for the mitigation to take place. Select disable to allow clients in the Known Clients database to remain authenticated with an unknown AP.

Known Client Database Lookup Method: When the controller detects a client on the network it performs a lookup in the Known Client database. Specify whether the controller should use the local or RADIUS database for these lookups.

Known Client Database RADIUS Server Name: If the known client database lookup method is RADIUS then this field specifies the RADIUS server name.

Rogue Detected Trap Interval: Specify the interval, in seconds, between transmissions of the SNMP trap telling the administrator that rogue APs are present in the RF Scan database. If you set the value to 0, the trap is never sent.

De-Authentication Requests Threshold Interval: Specify the number of seconds an AP should spend counting the DE authentication messages sent by wireless clients.

De-Authentication Requests Threshold Value: If controller receives more than specified messages during the threshold interval the test triggers.

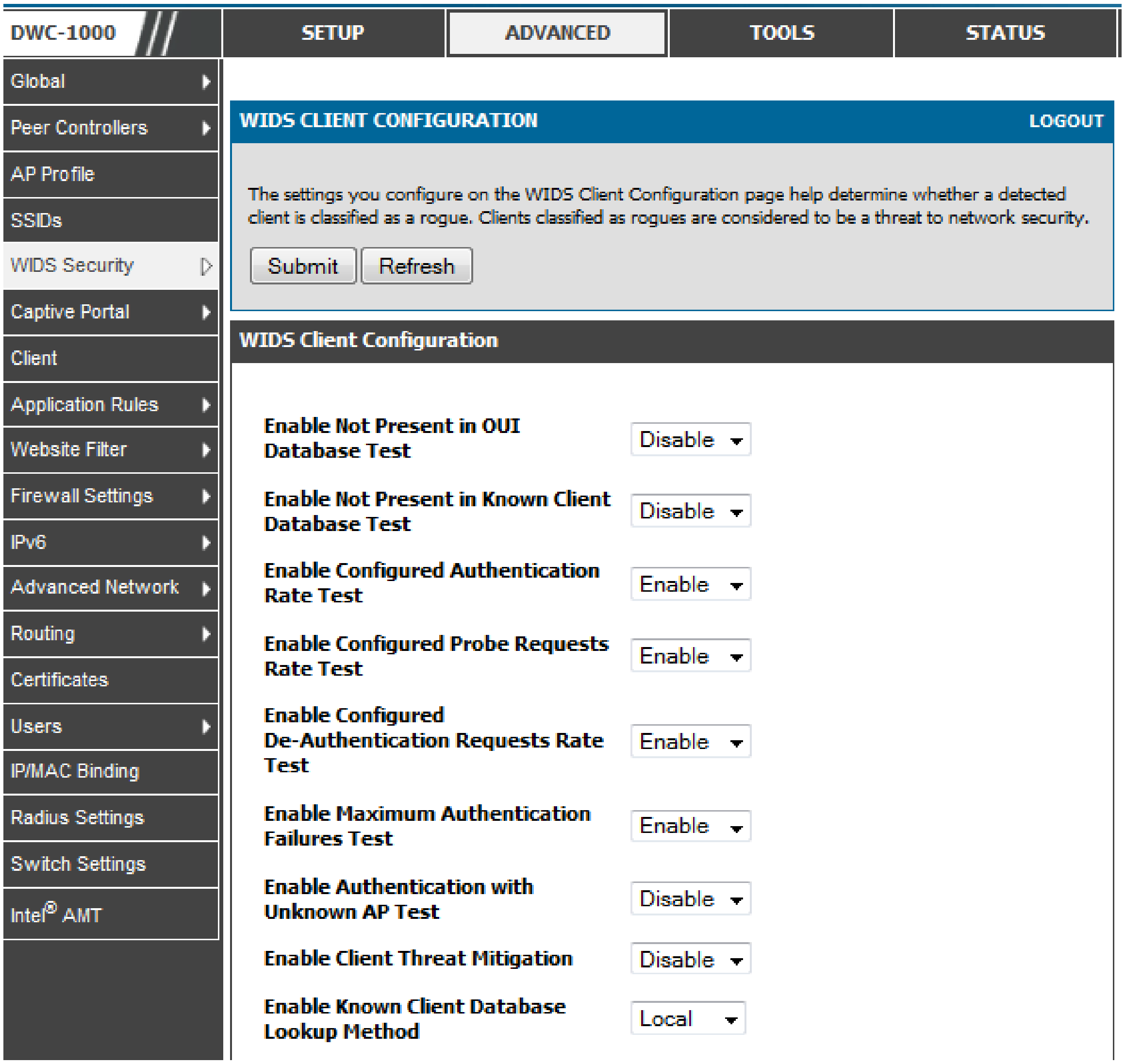
Authentication Requests Threshold Interval: Specify the number of seconds an AP should spend counting the authentication messages sent by wireless clients.

Authentication Requests Threshold Value: If controller receives more than specified messages during the threshold interval the test triggers. Probe Requests Threshold Interval Specify the number of seconds an AP should spend counting the probe messages sent by wireless clients.

Probe Requests Threshold Value: Specify the number of probe requests a wireless client is allowed to send during the threshold interval before the event is reported as a threat.

Authentication Failure Threshold Value: Specify the number of 802.1X authentication failures a client is allowed to have before the event is reported as a threat.

Figure 176: WIDS Client Configuration



WIDS CLIENT CONFIGURATION

The settings you configure on the WIDS Client Configuration page help determine whether a detected client is classified as a rogue. Clients classified as rogues are considered to be a threat to network security.

WIDS Client Configuration

Enable Not Present in OUI Database Test	Disable
Enable Not Present in Known Client Database Test	Disable
Enable Configured Authentication Rate Test	Enable
Enable Configured Probe Requests Rate Test	Enable
Enable Configured De-Authentication Requests Rate Test	Enable
Enable Maximum Authentication Failures Test	Enable
Enable Authentication with Unknown AP Test	Disable
Enable Client Threat Mitigation	Disable
Enable Known Client Database Lookup Method	Local

11.6 WDS Settings

Advanced>WDS Configuration

The Wireless Distribution System (WDS) Managed AP feature allows administrator to add managed APs to the cluster using over-the-air WDS links through other managed APs. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required. With WDS, APs may be located outdoors where wired connection to the data network is unavailable, or in remote buildings that are not connected to the main campus with a wired network.

The WDS AP group consists of two types of APs: root APs and satellite APs. A root AP acts as a bridge or repeater on the wireless medium and communicates with the controller via the wired link. A satellite AP communicates with the controller via a WDS link to the root AP. The WDS links are secured using WPA2 Personal authentication and AES encryption.

Support for the WDS-managed AP feature within the Unified Wired and Wireless Access System includes the following:

- The wireless system can contain up to two WDS-managed AP groups.
- Each WDS-managed AP group can contain up to four APs.
- An AP can be a member of only one WDS AP group.
- Each satellite AP can have only one WDS link on the satellite APs. This means that a satellite AP must be connected to a root AP. A satellite AP cannot be connected to another satellite AP.

By default, an AP is configured as a root AP. For an AP to be attached to the Wireless System as a satellite AP, configure the following settings on the AP while it is in stand-alone mode:

Satellite AP mode: This setting enables the satellite AP to discover and establish WDS link with the root AP. By default, the WDS Managed Mode is Root AP.

Password: This is for WPA2 Personal authentication used to establish the WDS links. Only the satellite APs need this setting. The root APs get the password from the controller when they become managed.

Static Channel: The APs on each end of a WDS link must use the same radio and channel to communicate. Configure the satellite AP to use a static channel. For a root AP, set the static channel when you add the AP to the Valid AP database on the controller.

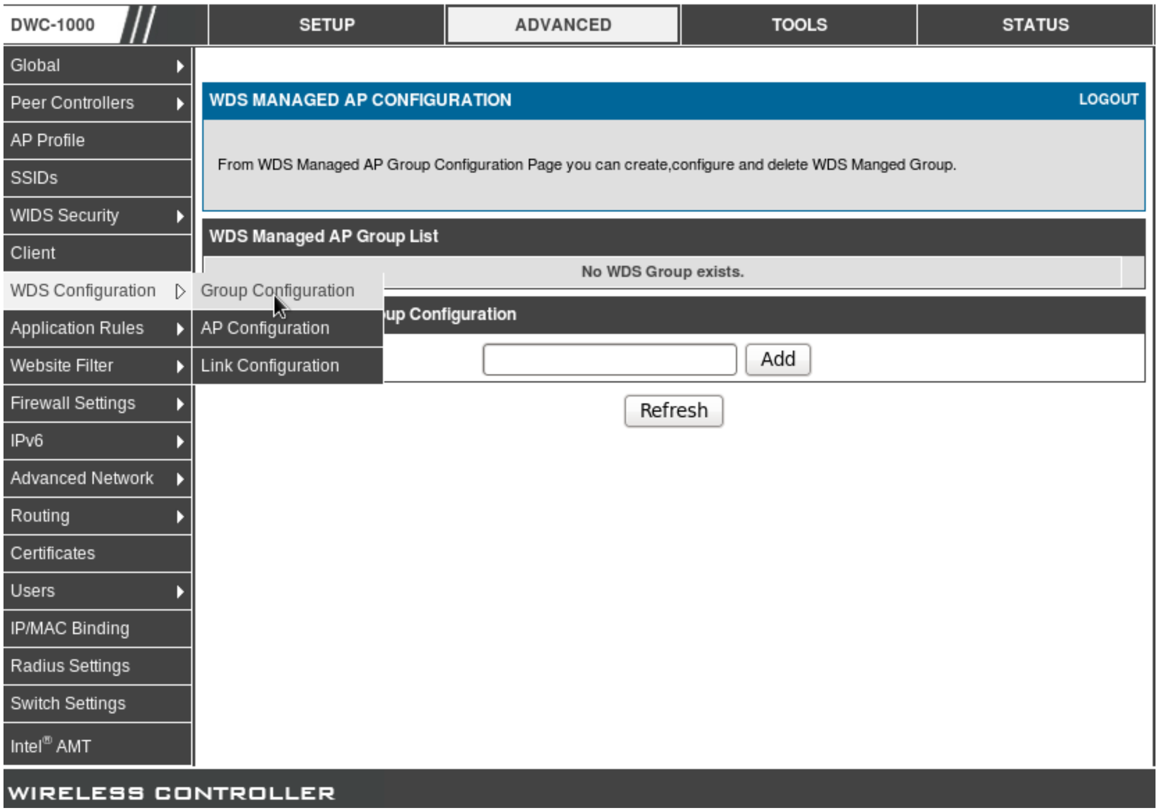
Optionally, to allow the Ethernet port on a satellite AP to provide wired access to the LAN, you must set the WDS Managed Ethernet Port to Enabled. It is disabled by default.

WDS configuration is divided into three sections: Group, AP, and Link configuration.

11.6.1 Group Configuration

WDS Group ID: Define the group’s ID, which will be used in AP and Link configuration pages to identify this group.

Figure 177: WDS Group Configuration



WDS MANAGED AP CONFIGURATION

From WDS Managed AP Group Configuration Page you can create,configure and delete WDS Manged Group.

WDS Managed AP Group List

No WDS Group exists.

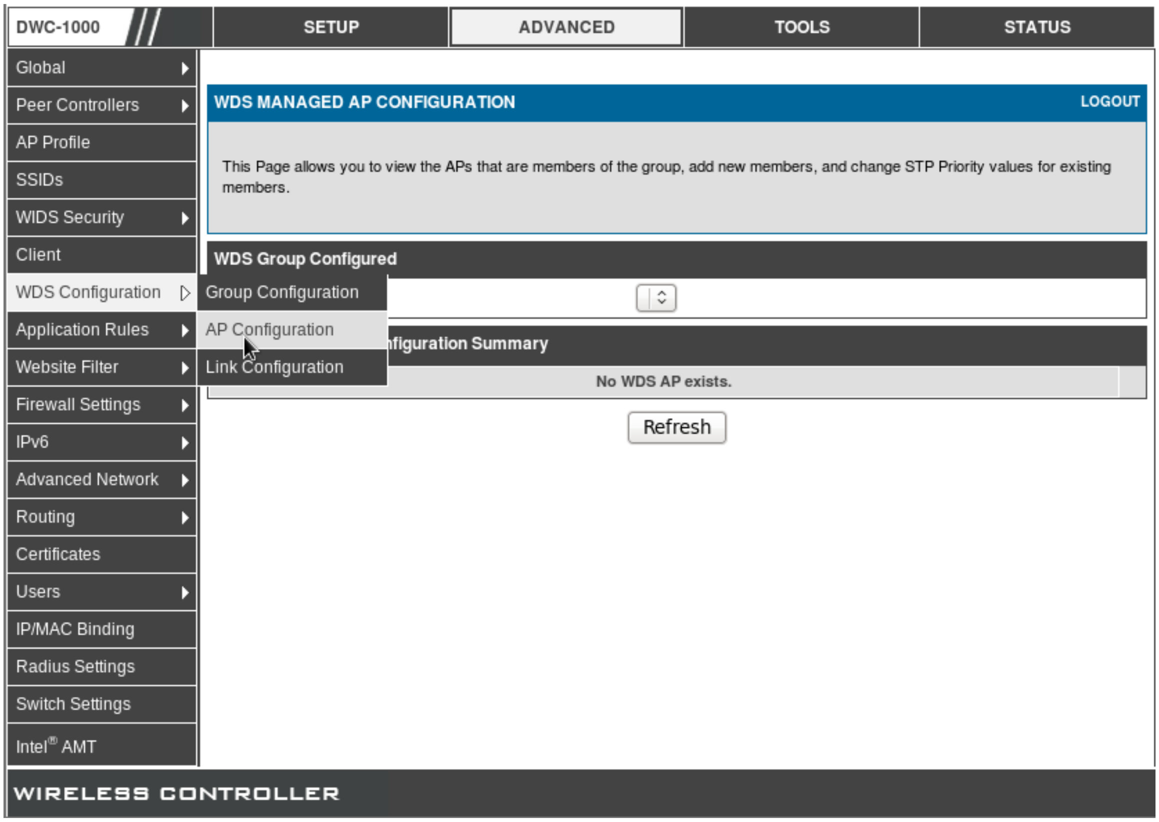
up Configuration

11.6.2 AP Configuration

After creating a WDS-Managed AP group, use the WDS Managed AP Configuration page to view the APs that are members of the group, add new members, and change STP Priority values for existing members.

> ✍ Note: After changing WDS-Managed AP group settings, make sure to push the configuration to other controllers in the cluster.

Figure 178: WIDS Managed AP Configuration



This Page allows you to view the APs that are members of the group, add new members, and change STP Priority values for existing members.

No WDS AP exists.

The following fields are available on the WDS Managed AP Summary page. **WDS Group ID**: Select the ID associated with the group to configure.

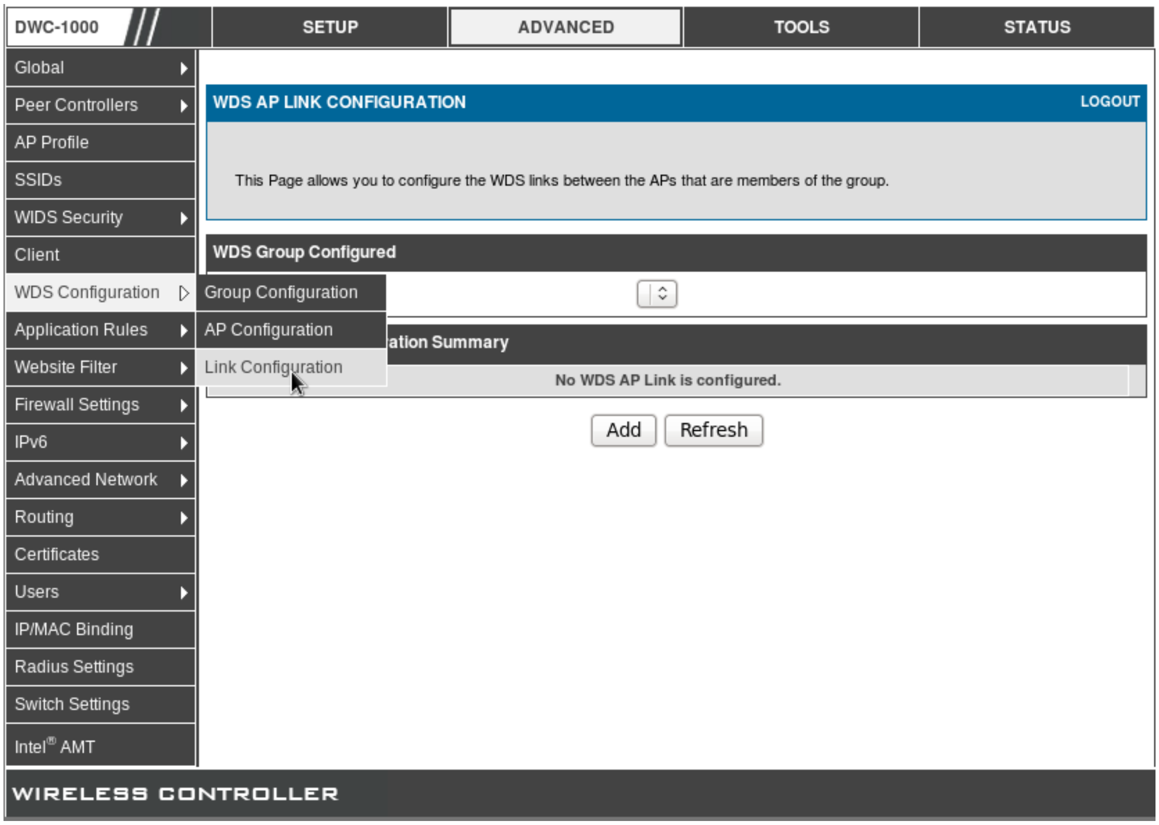
AP MAC Address: MAC Address of the AP.

STP Priority: Spanning Tree Priority for this AP. The STP priority is used only when spanning tree mode is enabled. The STP priority determines which AP is selected as the root of the spanning tree and which AP has preference over another AP when multiple equal cost paths exist in the topology. The lower value for the spanning tree priority means that the AP is more likely to be used for bridging data into the campus network. You should assign a lower priority to the APs connected to the wired network than to the Satellite Aps. The STP priority value is rounded down to a multiple of 4096. The range is 0-61440, and the default value is 36864.

11.6.3 Link Configuration

After creating a WDS-Managed AP group, we can use the WDS AP Link Configuration page to configure the WDS links between the APs that are members of the group.

Figure 179: WDS AP Link Configuration



This Page allows you to configure the WDS links between the APs that are members of the group.

No WDS AP Link is configured.

The following fields are available on the WDS AP Link Configuration page:

> ✍ Note: After changing WDS-Managed AP group settings, make sure to push the configuration to other controllers in the cluster.: Select the ID associated with the group to configure.

Source AP MAC Address: MAC Address of the source AP. The AP must be included in the selected WDS group. Note: The WDS links are bidirectional. The terms Source and Destination simply reflect the WDS link endpoints specified when the WDS link is created.

Source Radio: The radio number of the WDS link endpoint on the source AP. **Dest AP MAC Address**: The MAC address of the destination AP in the group.

Destination Radio: The radio number of the WDS link endpoint on the destination AP.

STP Link Cost: Spanning Tree Path cost for the WDS link. The range is 0â€“255. When multiple alternate paths are defined in the WDS group, the link cost is used to indicate which links are the primary links and which links are the secondary links. The spanning tree selects the path with the lowest link cost.

✍ Note: if no links have been configured for the selected WDS group, only the Add and Refresh buttons display.

✍ Note: After changing WDS-Managed AP group settings, make sure to push the configuration to other controllers in the cluster.

11.7 External Authentications

✍ This feature is available with the VPN / Firewall license.

The admin can configure external authentication (XAUTH). Rather than configure a unique VPN policy for each user, the admin can configure the VPN gateway router to authenticate users from a stored list of user accounts or with an external authentication server such as a RADIUS server. With a user database, user accounts created in the router are used to authenticate users.

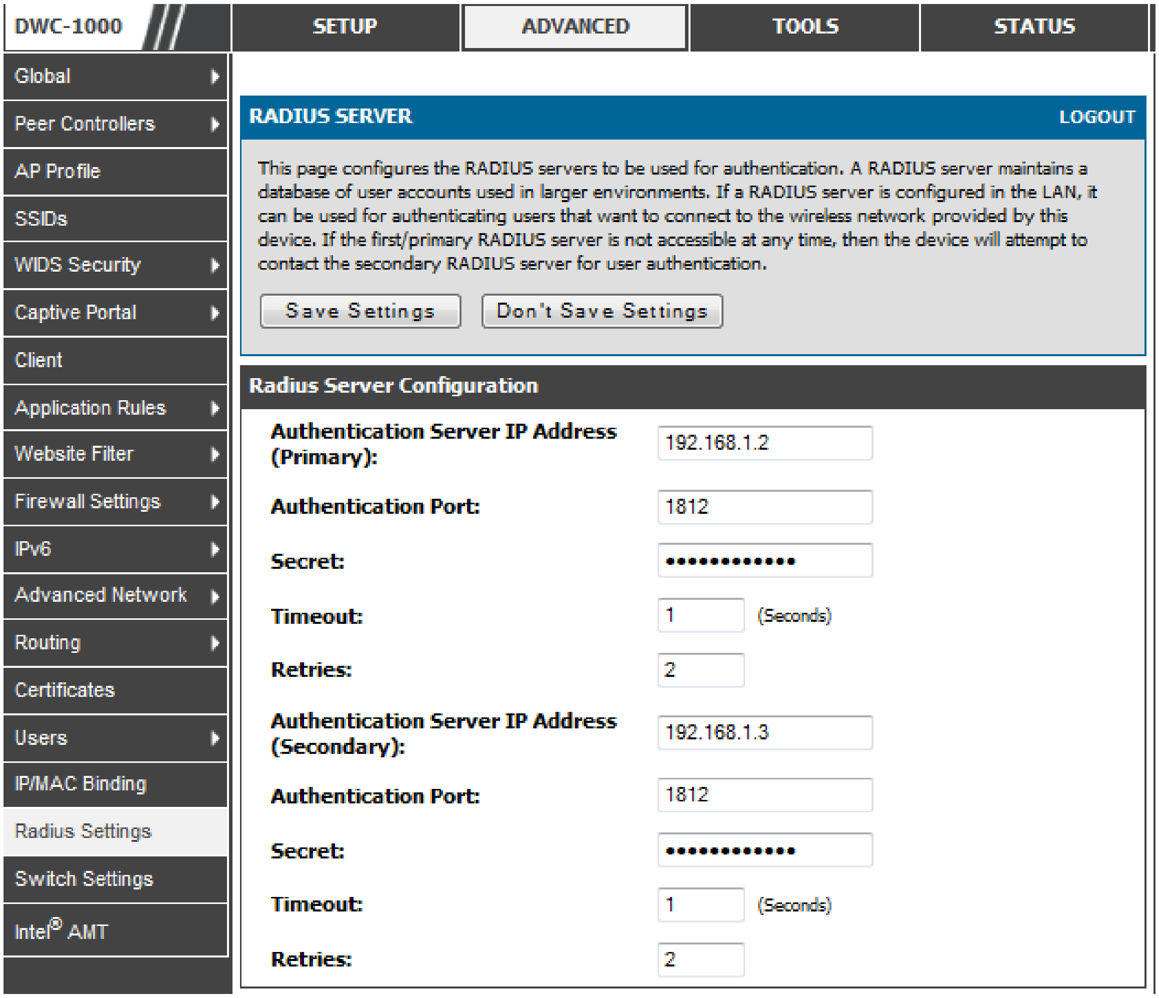
With a configured RADIUS server, the router connects to a RADIUS server and passes to it the credentials that it receives from the VPN client. You can secure the connection between the router and the RADIUS server with the authentication protocol supported by the server (PAP or CHAP). For RADIUS – PAP, the router first checks in the user database to see if the user credentials are available; if they are not, the router connects to the RADIUS server.

11.7.1 RADIUS Settings

Setup > External Authentications > RADUIS Settings

From the RADIUS Server Configuration page, you can add a new RADIUS server, configure settings for a new or existing RADIUS server, and view RADIUS server status information.

Figure 180: RADIUS Server Configuration



This page configures the RADIUS servers to be used for authentication. A RADIUS server maintains a database of user accounts used in larger environments. If a RADIUS server is configured in the LAN, it can be used for authenticating users that want to connect to the wireless network provided by this device. If the first/primary RADIUS server is not accessible at any time, then the device will attempt to contact the secondary RADIUS server for user authentication.

Radius Server Configuration

Authentication Server IP Address (Primary):	192.168.1.2
Authentication Port:	1812
Secret:	•••••••••••••
Timeout:	1 (Seconds)
Retries:	2
Authentication Server IP Address (Secondary):	192.168.1.3
Authentication Port:	1812
Secret:	•••••••••••••
Timeout:	1 (Seconds)
Retries:	2

Authentication Server IP Address (Primary): IP address of the primary RADIUS authentication server.

Authentication Server IP Address (Secondary): IP address of the secondary RADIUS authentication server.

Authentication Port: RADIUS authentication server port to send RADIUS messages.

Secret: Secret key that allows the device to log into the configured RADIUS server. It must match the secret on RADIUS server.

Timeout: Set the amount of time in seconds, the router should wait for a response from the RADIUS server.

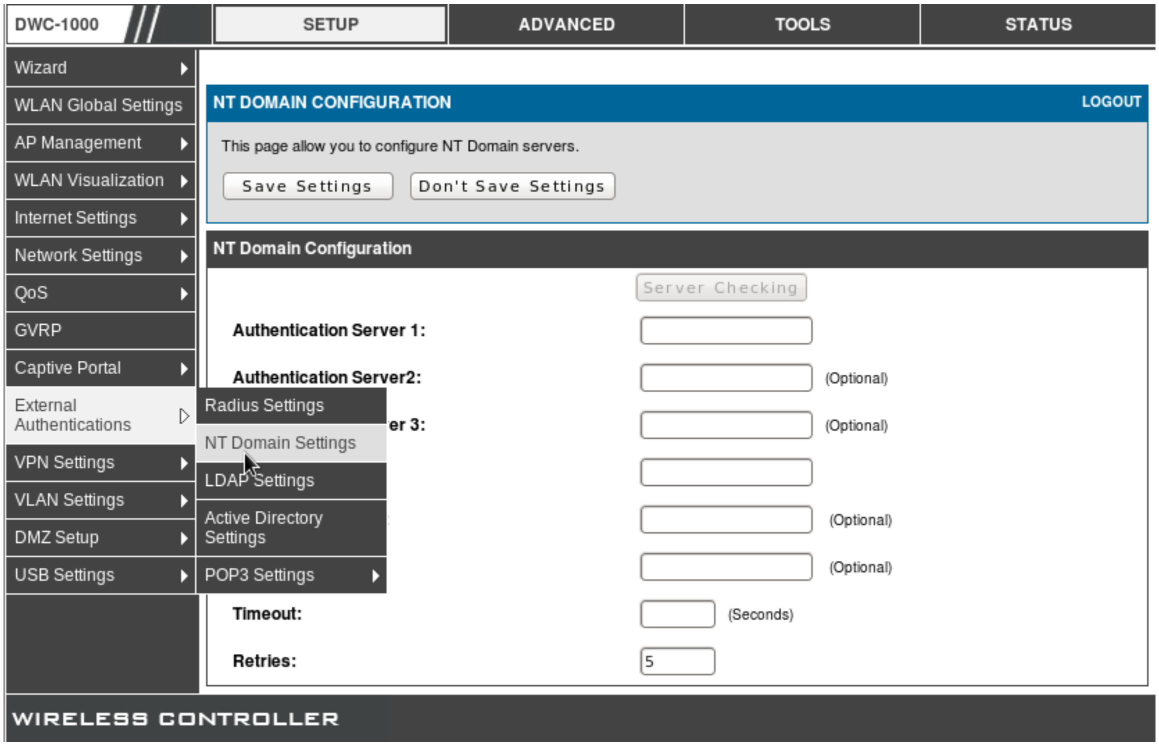
Retries: This determines the number of tries the router will make to the RADIUS server before giving up.

11.7.2 NT Domain Settings

Setup>External Authentications>NT Domain Settings

NT Domain offers centralized control over the network. The samba module is used to provide domain control. The authentication protocol used is NTLM (NT LAN MANAGER), which is a challenge-response authentication protocol. First the client will send a negotiate message with the values configured by the admin as part of the NT domain. Next the server will send the challenge message, and finally the client will send authenticate message to server. With success at all steps the authentication will take place.

Figure 181: NT Domain Configuration



This page allow you to configure NT Domain servers.

NT Domain Configuration

Authentication Server 1:

Authentication Server2: (Optional)

er 3: (Optional)

(Optional)

(Optional)

Timeout: (Seconds)

Retries: 5

After configuring NT Domain Settings, users in to the configured domain are able to authenticate. The following fields needs to be configured in NT Domain configuration.

Authentication Server 1: The IP Address of the primary authentication server.

Authentication Server 2: The IP Address of the secondary authentication server; it is an optional field.

Authentication Server 3: The IP Address of the tertiary authentication server; it is an optional field.

Workgroup: This is the Workgroup for Authentication Server 1.The NT domain type of authentication requires the workgroup field; contact your administrator for the workgroup needed to configure NT Domain authentication.

Second Workgroup: Workgroup for Authentication Server 2. Though it is optional, if Authentication Server2 is defined this field becomes necessary.

Third Workgroup: Workgroup for Authentication Server 3. Though it is optional, if Authentication Server2 is defined this field becomes necessary.

Timeout: Set the amount of time in seconds, the appliance should wait for a response from the authentication server.

Retries: The number of attempts the appliance will make to the authentication server before giving and considering the authentication attempt as failed.

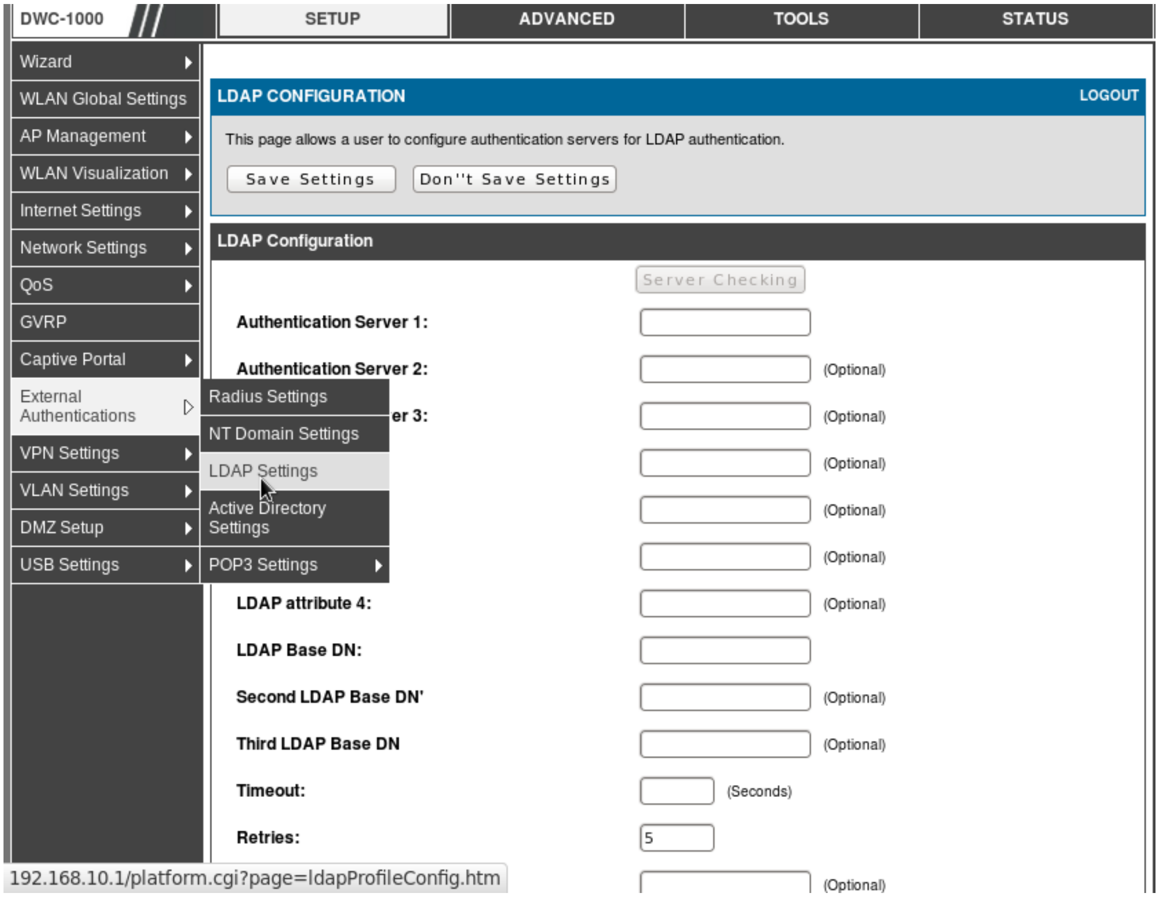
After configuring all fields in NT Domain settings, to check the server reachability the administrator can use Server Checking option. When the administrator clicks on server checking button the server reachability status for the configured servers is returned.

11.7.3 LDAP Settings

Setup>External Authentications>LDAP Settings

LDAP (Lightweight Directory Access Protocol) is often used by organizations as a central repository for user information and as an authentication service. It is an application protocol for accessing and maintaining distributed directory. This appliance uses port 389 for binding the LDAP authentication server.

Figure 182: LDAP Authentication Configuration



This page allows a user to configure authentication servers for LDAP authentication.

Authentication Server 1:	
Authentication Server 2:	(Optional)
er 3:	(Optional)
	(Optional)
	(Optional)
	(Optional)
LDAP attribute 4:	(Optional)
LDAP Base DN:	
Second LDAP Base DN'	(Optional)
Third LDAP Base DN	(Optional)
Timeout:	(Seconds)
Retries:	5
	(Optional)

192.168.10.1/platform.cgi?page=ldapProfileConfig.htm

The administrator can configure authentication servers for LDAP authentication. After configuring the servers with the below listed parameters, whenever user tries to authenticate the client will send an LDAP Request to server and server sends backs the LDAP Response determining authentication success.

Authentication Server 1: The IP Address of the primary authentication server.

Authentication Server 2: The IP Address of the secondary authentication server; it is an optional field.

Authentication Server 3: The IP Address of the tertiary authentication server; it is an optional field.

LDAP attribute 1-4: These are attributes related to LDAP users configured in LDAP server and defined by the LDAP server administrator. These may include attributes like

SAM account name, Associated Domain Name and so on. These can be used to distinguish between different users having same user name.

LDAP Base DN: LDAP authentication requires the base domain name; contact your administrator for the Base DN to use LDAP authentication for this domain. This Domain name is for Authentication Server1

Second LDAP Base DN (optional): Base domain name for Authentication Server2 (if in use).

Third LDAP Base DN (optional): Base domain name for Authentication Server3 (if in use).

Timeout: Set the amount of time in seconds, the appliance should wait for a response from the authentication server.

Retries: The number of attempts the appliance will make to the authentication server before giving and considering the authentication attempt as failed.

First Administrator Account: Primary admin account in LDAP server that will be used when LDAP authentication is required for PPTP/L2TP connection.

Password: Primary admin password.

Second Administrator Account: Second admin account in LDAP server that will be used when LDAP authentication is required for PPTP/L2TP connection.

Password: Second admin password.

Third Administrator Account: Third admin account in LDAP server that will be used when LDAP authentication is required for PPTP/L2TP connection.

Password: Third admin password.

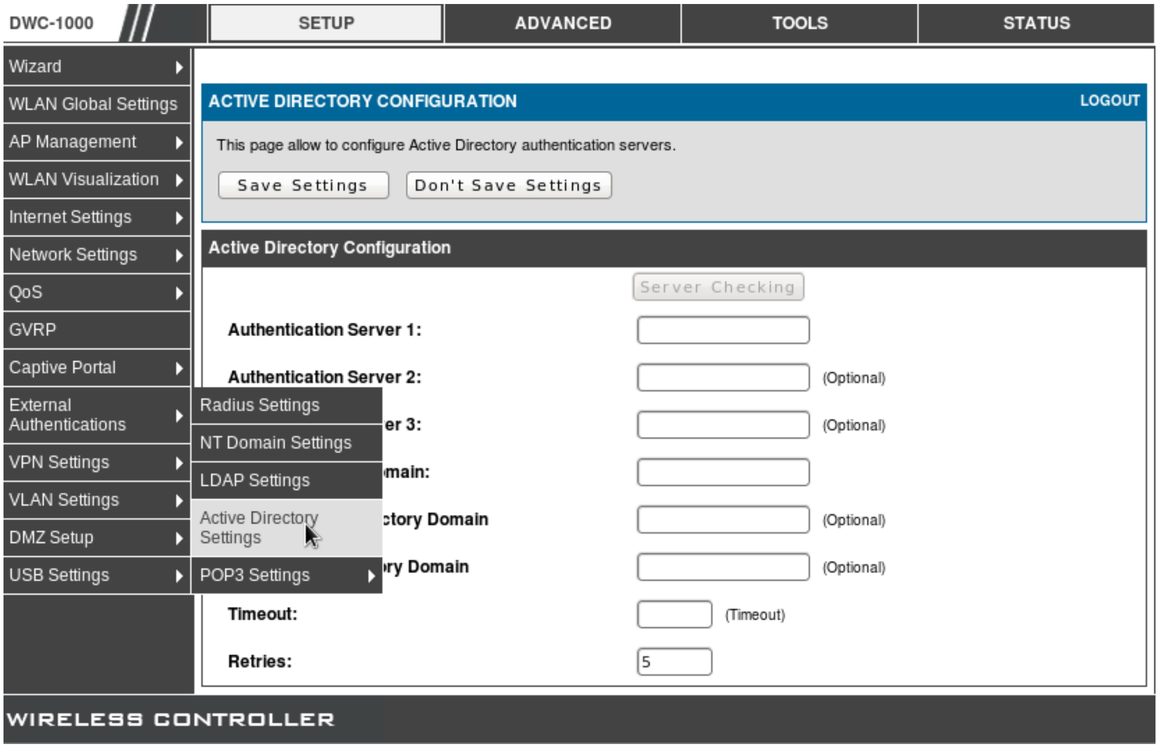
After configuring all fields in LDAP configuration, to check the server reachability the administrator can use Server Checking option. When the administrator clicks on server checking button the server reachability status for the configured servers is returned.

11.7.4 Active Directory Settings

Setup>External Authentications>Active Directory Settings

Active Directory (AD) structure is a hierarchical arrangement of Information about objects. The objects fall into two broad categories resources (e.g., printers) and security principals (user or computer accounts and groups). Security principals are assigned unique security identifiers. The AD client on the appliance will use Authentication port 88 to communicate with server.

Figure 183: Active Directory Configuration



ACTIVE DIRECTORY CONFIGURATION

This page allow to configure Active Directory authentication servers.

Active Directory Configuration

Authentication Server 1:		
Authentication Server 2:		(Optional)
er 3:		(Optional)
main:		
ctory Domain		(Optional)
ry Domain		(Optional)
Timeout:		(Timeout)
Retries:	5	

After configuring the AD server(s), whenever user tries to authenticate with credentials the client will send AS Request to server and server sends backs the AS Response.

Authentication Server 1: The IP Address of the primary authentication server.

Authentication Server 2: The IP Address of the secondary authentication server; it is an optional field.

Authentication Server 3: The IP Address of the tertiary authentication server; it is an optional field.

Active Directory Domain: Since Active Directory is the chose authentication type, admin must enter the Active Directory domain name in this field. Users that are registered in the Active Directory database can now access the SSL VPN portal by using their Active Directory user name and password.

Second Active Directory Domain (optional): Active Directory Domain for Authentication Server2 (if in use)

Third Active Directory Domain (optional): Active Directory Domain for Authentication Server3 (if in use)

Timeout: Set the amount of time in seconds, the appliance should wait for a response from the authentication server.

Retries: The number of attempts the appliance will make to the authentication server before giving and considering the authentication attempt as failed.

After configuring all fields in Active Directory settings, to check the server reachability the administrator can use Server Checking option. When the administrator clicks on server checking button the server reachability status for the configured servers is returned.

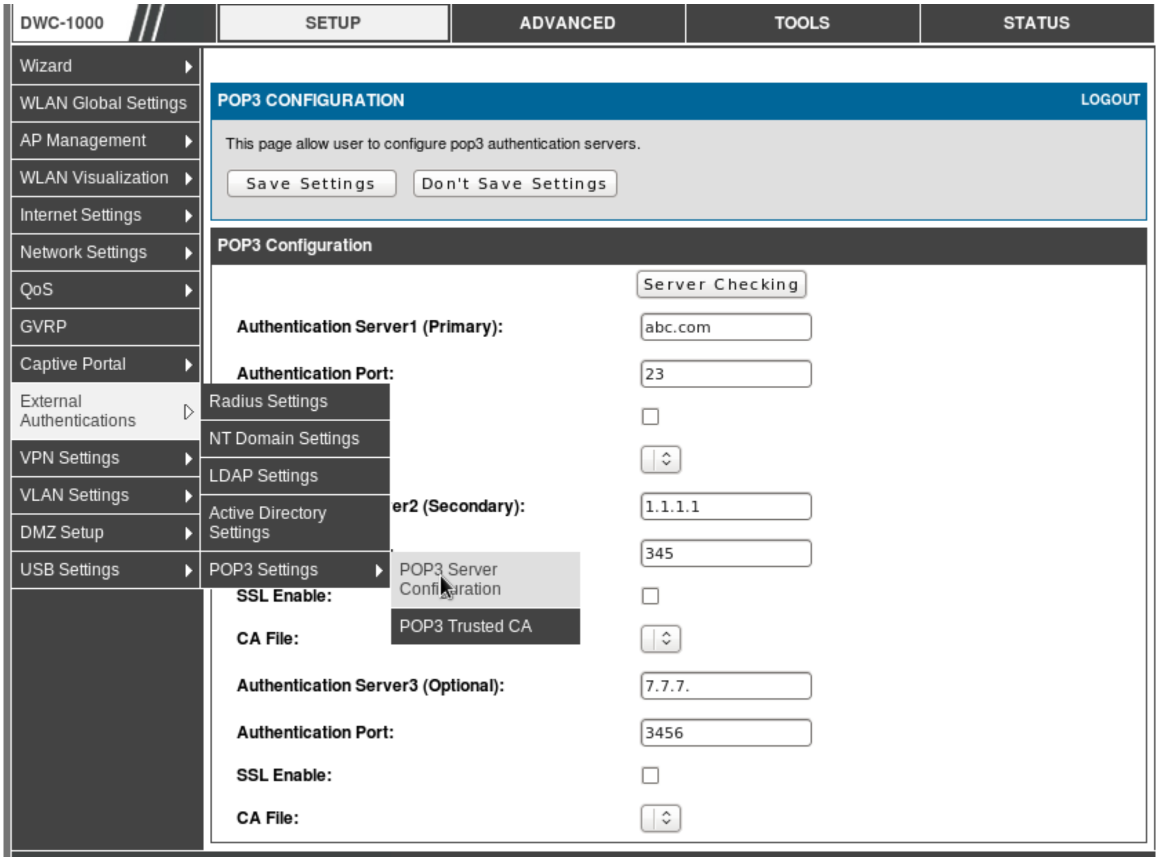
11.7.5 POP3 Settings

Setup>External Authentications>POP3 Settings

POP3 (Post Office Protocol) is commonly used by email clients to retrieve email. It supports both SSL as well as plain accounts. Enabling SSL support will have the client send a SSL socket to the POP server. The POP client on the appliance uses authentication 110 port for plain type and 995 for SSL type. Each step will return at greeting messages: if success it will receive +OK else -ERROR.

If SSL support is enabled, a certificate authority must be selected to use for the SSL authentication.

Figure 184: POP3 Server Configuration



POP3 CONFIGURATION

This page allow user to configure pop3 authentication servers.

POP3 Configuration

Authentication Server1 (Primary): abc.com

Authentication Port: 23

□

er2 (Secondary): 1.1.1.1

345

SSL Enable: □

CA File:

Authentication Server3 (Optional): 7.7.7.

Authentication Port: 3456

SSL Enable: □

CA File:

Authentication Server 1: The IP Address of the primary authentication server.

Authentication Server 2: The IP Address of the secondary authentication server; it is an optional field.

Authentication Server 3: The IP Address of the tertiary authentication server; it is an optional field.

Authentication Port: Authentication port for respective authentication server.

SSL Enable: Enable SSL support for POP3. If this option is enabled, it is mandatory to select a certificate authority for it.

CA File: Certificate Authority file to verify POP3 server's certificate.

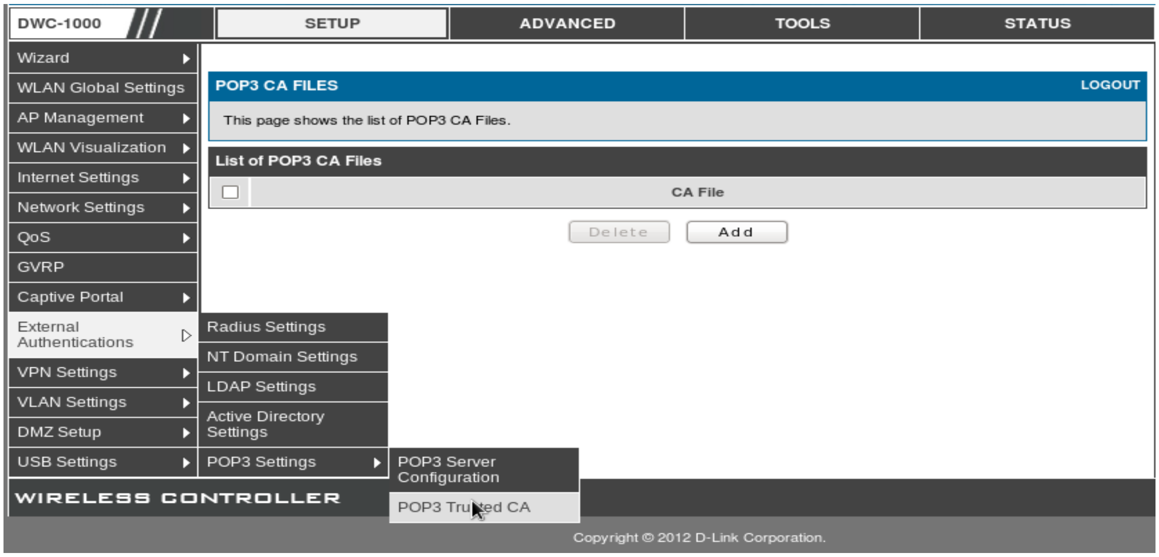
Timeout: Set the amount of time in seconds, the appliance should wait for a response from the authentication server.

Retries: The number of attempts the appliance will make to the authentication server before giving and considering the authentication attempt as failed.

After configuring all fields in Active Directory settings, to check the server reachability the administrator can use Server Checking option. When the administrator clicks on server checking button the server reachability status for the configured servers is returned.

To Add the CA certificate in case of SSL support, the admin needs to upload certificate in the POP3 CA file page.

Figure 185: POP3 CA File List



POP3 CA FILES

This page shows the list of POP3 CA Files.

List of POP3 CA Files

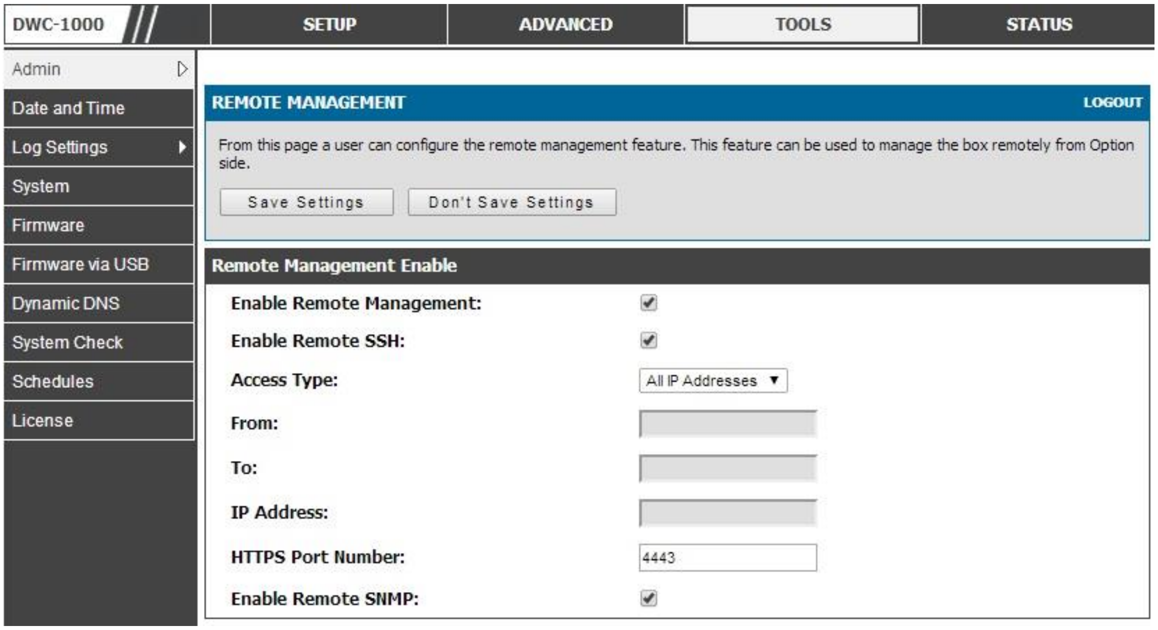
□	CA File

Chapter 12. Administration & Management

12.1 Remote Management

Both HTTPS and telnet access can be restricted to a subset of IP addresses. The controller administrator can define a known PC, single IP address or range of IP addresses that are allowed to access the GUI with HTTPS. The opened port for SSL traffic can be changed from the default of 4443 at the same time as defining the allowed remote management IP address range.

Figure 186: Remote Management



REMOTE MANAGEMENT

From this page a user can configure the remote management feature. This feature can be used to manage the box remotely from Option side.

Remote Management Enable

Enable Remote Management:	☑
Enable Remote SSH:	☑
Access Type:	All IP Addresses ▼
From:	
To:	
IP Address:	
HTTPS Port Number:	4443
Enable Remote SNMP:	☑

12.2 CLI Access

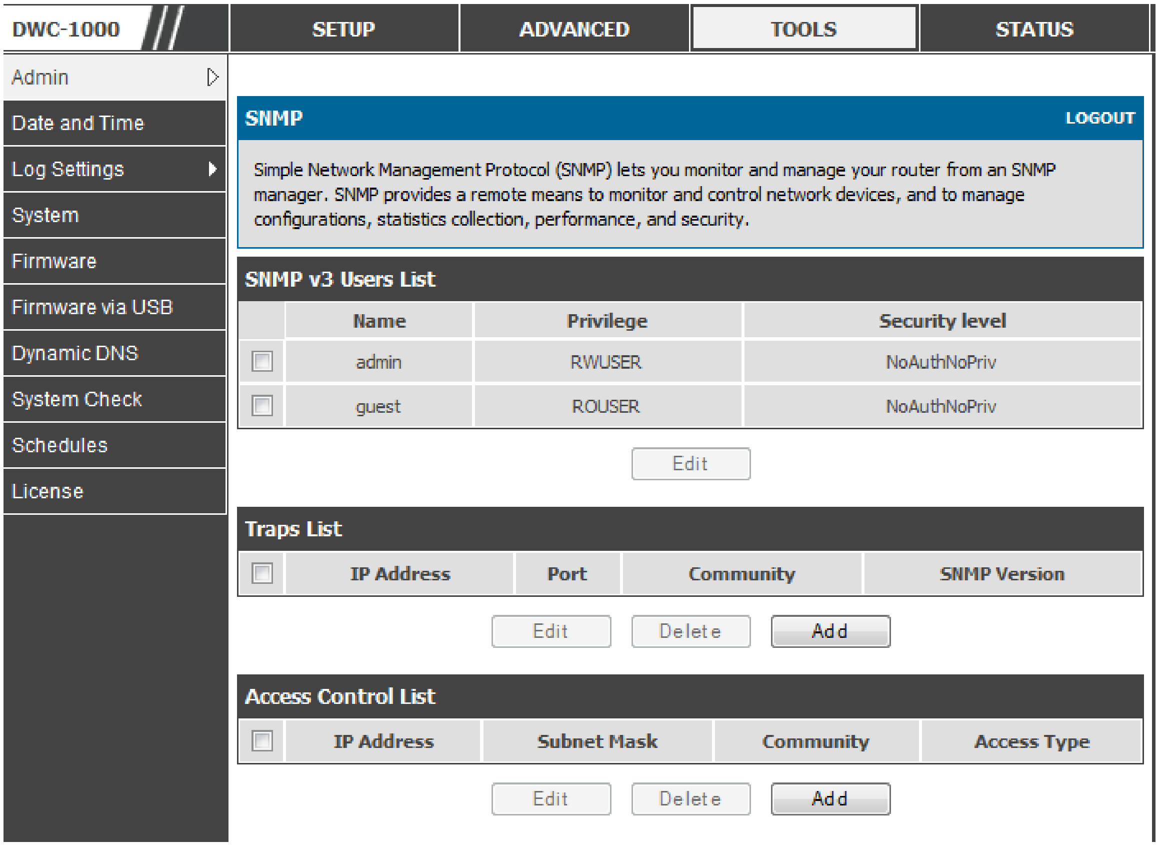
In addition to the web-based GUI, the gateway supports SSH and Telnet management for command-line interaction. The CLI login credentials are shared with the GUI for administrator users. To access the CLI, type “cli” in the SSH or console prompt and login with administrator user credentials.

12.3 SNMP Configuration

Tools > Admin > SNMP

SNMP is an additional management tool that is useful when multiple controller in a network are being managed by a central Master system. When an external SNMP manager is provided with this controller Management Information Base (MIB) file, the manager can update the controller hierarchal variables to view or update configuration parameters. The controller as a managed device has an SNMP agent that allows the MIB configuration variables to be accessed by the Master (the SNMP manager). The Access Control List on the controller identifies managers in the network that have read-only or read-write SNMP credentials. The Traps List outlines the port over which notifications from this controller are provided to the SNMP community (managers) and also the SNMP version (v1, v2c, v3) for the trap.

Figure 187: SNMP Users, Traps, and Access Control



SNMP

Simple Network Management Protocol (SNMP) lets you monitor and manage your router from an SNMP manager. SNMP provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SNMP v3 Users List

	Name	Privilege	Security level
□	admin	RWUSER	NoAuthNoPriv
□	guest	ROUSER	NoAuthNoPriv

Traps List

□	IP Address	Port	Community	SNMP Version

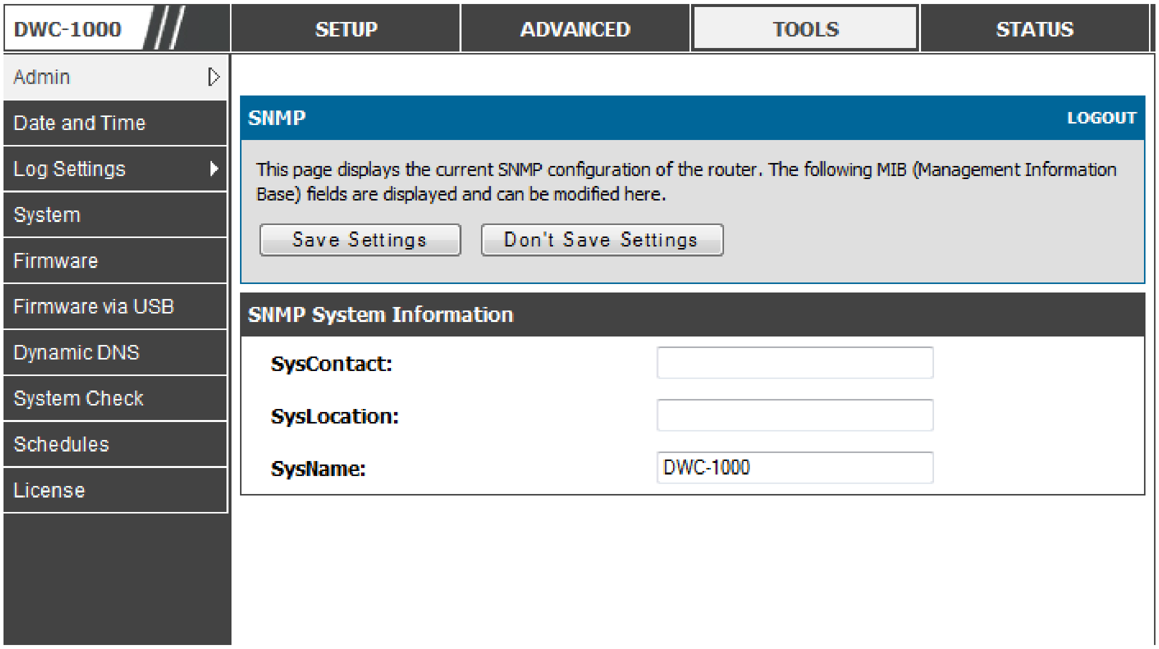
Access Control List

□	IP Address	Subnet Mask	Community	Access Type

Tools > Admin > SNMP System Info

The controller is identified by an SNMP manager via the System Information. The identifier settings The SysName set here is also used to identify the controller for SysLog logging.

Figure 188: SNMP system information for this controller



This page displays the current SNMP configuration of the router. The following MIB (Management Information Base) fields are displayed and can be modified here.

SysContact:

SysLocation:

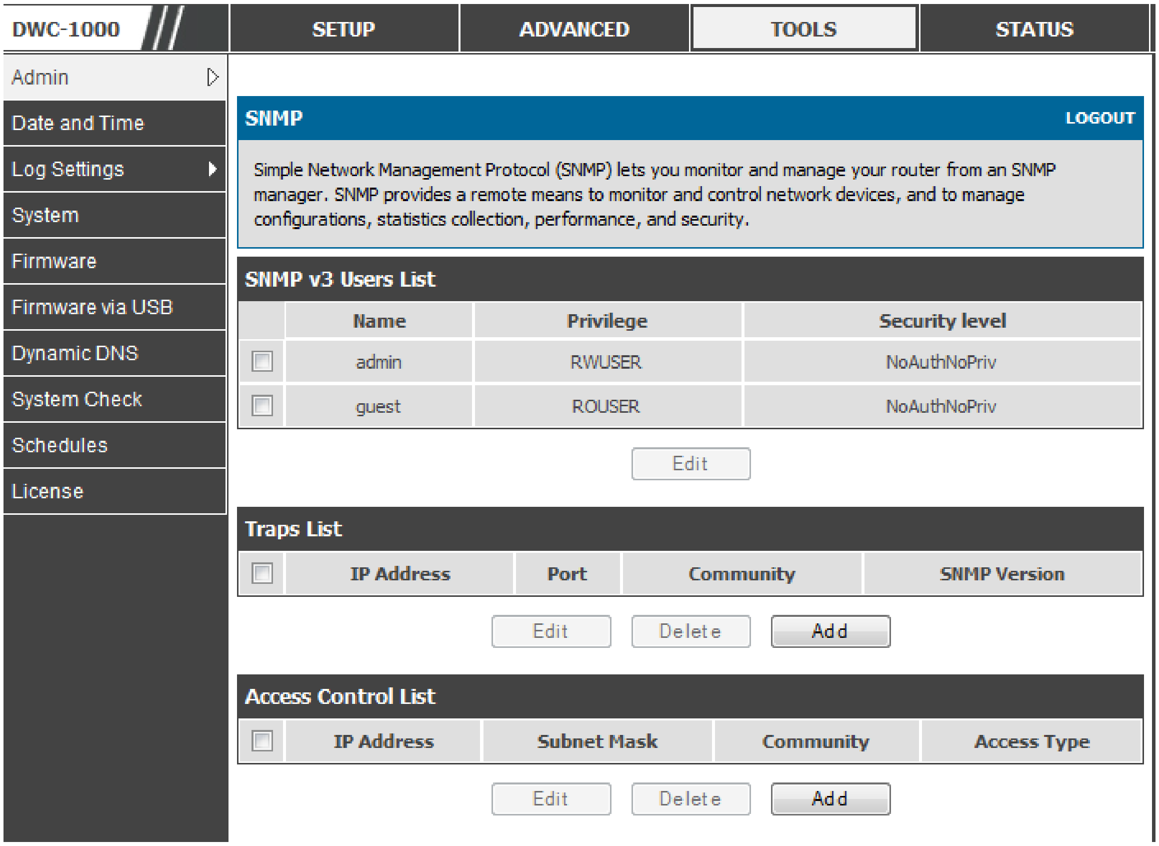
SysName: DWC-1000

12.4 SNMP Traps

Advanced > Global > SNMP Traps

If you use Simple Network Management Protocol (SNMP) to manage the DWC-1000 wireless controller, you can configure the SNMP agent on the controller to send traps to the SNMP manager on your network. When an AP is managed by a controller, it does not send out any traps. The controller generates all SNMP traps based on its own events and the events it learns about through updates from the APs it manages.

Figure 189: SNMP Traps



Simple Network Management Protocol (SNMP) lets you monitor and manage your router from an SNMP manager. SNMP provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SNMP v3 Users List

	Name	Privilege	Security level
□	admin	RWUSER	NoAuthNoPriv
□	guest	ROUSER	NoAuthNoPriv

Traps List

□	IP Address	Port	Community	SNMP Version

Access Control List

□	IP Address	Subnet Mask	Community	Access Type

AP Failure Traps: If you enable this field, the SNMP agent sends a trap if an AP fails to associate or authenticate with the controller.

AP State Change Traps: If you enable this field, the SNMP agent sends a trap for one of the following reasons, each containing location objects:

- Managed AP Discovered
- Managed AP Failed
- Managed AP Unknown Protocol Discovered.
- Managed AP Load Balancing Utilization Exceeded.

Client Failure Traps: If you enable this field, the SNMP agent sends a trap with failure info for clients authenticated by AP's managed by the controller, with each trap containing location objects:

- Client Association Failure
- Client Authentication Failure

Client State Change Traps: If you enable this field, the SNMP agent sends a trap for one of the following reasons associated with the wireless client, each containing location objects:

- Client Association Detected.
- Client Disassociation Detected.
- Client Roam Detected.

Peer Controller Traps: If you enable this field, the SNMP agent sends a trap for one of the following reasons associated with a peer controller.

- Peer Controller Discovered
- Peer Controller Failed
- Peer Controller Unknown Protocol Discovered.

Configuration command received from peer controller. (The controller need not be Cluster Controller for generating this trap.

RF Scan Traps: If you enable this field, the SNMP agent sends a trap when the RF scan detects a new AP, wireless client, or ad-hoc client.

Rogue AP Traps: If you enable this field, the SNMP agent sends a trap when the controller discovers a rogue AP. The agent also sends a trap every Rogue Detected Trap Interval seconds if any rogue AP continues to be present in the network.

Wireless Status Traps: If you enable this field, the SNMP agent sends a trap if the operational status of the Unified Wireless controller (it need not be Cluster Controller for this trap) changes. It sends a trap if the Channel Algorithm is complete or the Power Algorithm is complete. It also sends a trap if any of the following databases or lists has reached the maximum number of entries:

1- Managed AP database.

2- AP Neighbor List.

3- Client Neighbor List.

4- AP Authentication Failure List.

5- RF Scan AP List.

6- Client Association Database.

7- Ad Hoc Clients List.

8- Detected Clients List.

12.5 Configuring Time Zone and NTP

Tools > Date and Time

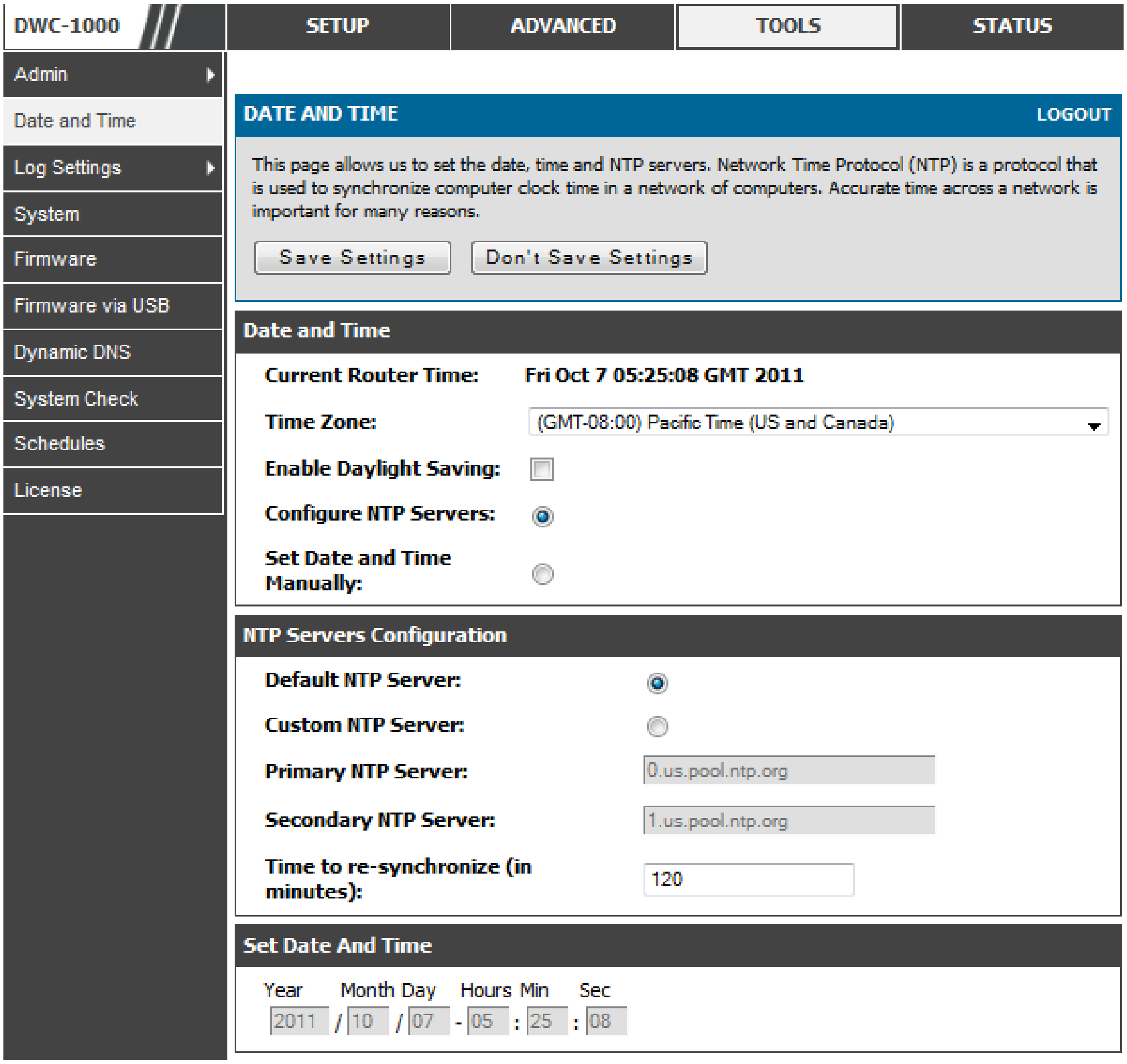
You can configure your time zone, whether or not to adjust for Daylight Savings Time, and with which Network Time Protocol (NTP) server to synchronize the date and time. You can choose to set Date and Time manually, which will store the information on the controller real time clock (RTC). If the controller has access to the internet, the most accurate mechanism to set the controller time is to enable NTP server communication.

> ✍ Accurate date and time on the controller is critical for firewall schedules, Wi-Fi power saving support to disable APs at certain times of the day, and accurate logging.

Please follow the steps below to configure the NTP server:

1. Select the controller time zone, relative to Greenwich Mean Time (GMT).
2. If supported for your region, click to Enable Daylight Savings.
3. Determine whether to use default or custom Network Time Protocol (NTP) servers. If custom, enter the server addresses or FQDN.

Figure 190: Date, Time, and NTP server setup



This page allows us to set the date, time and NTP servers. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock time in a network of computers. Accurate time across a network is important for many reasons.

Date and Time

Current Router Time:	Fri Oct 7 05:25:08 GMT 2011
Time Zone:	(GMT-08:00) Pacific Time (US and Canada)
Enable Daylight Saving:	□
Configure NTP Servers:	●
Set Date and Time Manually:	○

NTP Servers Configuration

Default NTP Server:	●
Custom NTP Server:	○
Primary NTP Server:	0.us.pool.ntp.org
Secondary NTP Server:	1.us.pool.ntp.org
Time to re-synchronize (in minutes):	120

Set Date And Time

Year	Month	Day	Hours	Min	Sec
2011	10	07	05	25	08

12.6 Log Configuration

This controller allows you to capture log messages for traffic through the firewall, VPN, and over the wireless AP. As an administrator you can monitor the type of traffic that goes through the controller and also be notified of potential attacks or errors when they are detected by the controller. The following sections describe the log configuration settings and the ways you can access these logs.

12.6.1 Defining What to Log

Tools > Log Settings > Logs Facility

The Logs Facility page allows you to determine the granularity of logs to receive from the controller. There are three core components of the controller, referred to as Facilities:

Kernel: This refers to the Linux kernel. Log messages that correspond to this facility would correspond to traffic through the firewall or network stack.

System: This refers to application and management level features available on this controller, including SSL VPN and administrator changes for managing the unit.

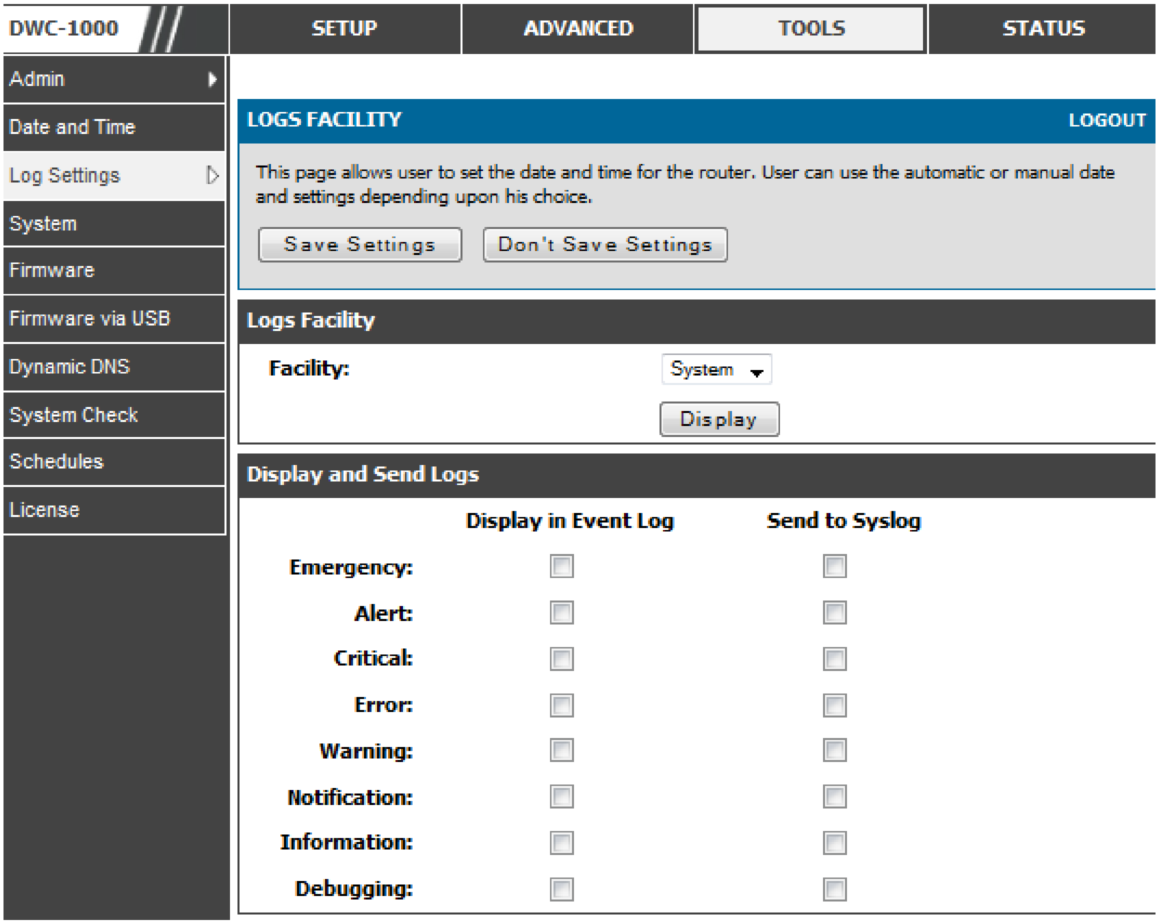
Wireless: This facility corresponds to the 802.11 driver used for providing AP functionality to your network.

Local1-UTM: This facility corresponds to IPS (Intrusion Prevention System) which helps in detecting malicious intrusion attempts from the Option.

For each facility, the following events (in order of severity) can be logged: Emergency, Alert, Critical, Error, Warning, Notification, Information, Debugging. When a particular severity level is selected, all events with severity equal to and greater than the chosen severity are captured. For example if you have configured CRITICAL level logging for the Wireless facility, then 802.11 logs with severities CRITICAL, ALERT, and EMERGENCY are logged. The severity levels available for logging are:

- EMERGENCY: system is unusable
- ALERT: action must be taken immediately
- CRITICAL: critical conditions
- ERROR: error conditions
- WARNING: warning conditions
- NOTIFICATION: normal but significant condition
- INFORMATION: informational
- DEBUGGING: debug-level messages

Figure 191: Facility settings for Logging



LOGS FACILITY

This page allows user to set the date and time for the router. User can use the automatic or manual date and settings depending upon his choice.

Logs Facility

Facility: System

Display and Send Logs

	Display in Event Log	Send to Syslog
Emergency:	□	□
Alert:	□	□
Critical:	□	□
Error:	□	□
Warning:	□	□
Notification:	□	□
Information:	□	□
Debugging:	□	□

The display for logging can be customized based on where the logs are sent, either the Event Log viewer in the GUI (the Event Log viewer is in the ***Status > Logs*** page) or a remote Syslog server for later review. E-mail logs, discussed in a subsequent section, follow the same configuration as logs configured for a Syslog server.

Tools > Log Settings > Logs Configuration

This page allows you to determine the type of traffic through the controller that is logged for display in Syslog, E-mailed logs, or the Event Viewer. Denial of service attacks, general attack information, login attempts, dropped packets, and similar events can be captured for review by the IT administrator.

Traffic through each network segment (LAN, Option, DMZ) can be tracked based on whether the packet was accepted or dropped by the firewall.

Accepted Packets are those that were successfully transferred through the corresponding network segment (i.e. LAN to Option). This option is particularly useful when the Default Outbound Policy is “Block Always” so the IT admin can monitor traffic that is passed through the firewall.

- **Example**: If Accept Packets from LAN to Option is enabled and there is a firewall rule to allow SSH traffic from LAN, then whenever a LAN machine tries to make an SSH connection, those packets will be accepted and a message will be logged. (Assuming the log option is set to Allow for the SSH firewall rule.)

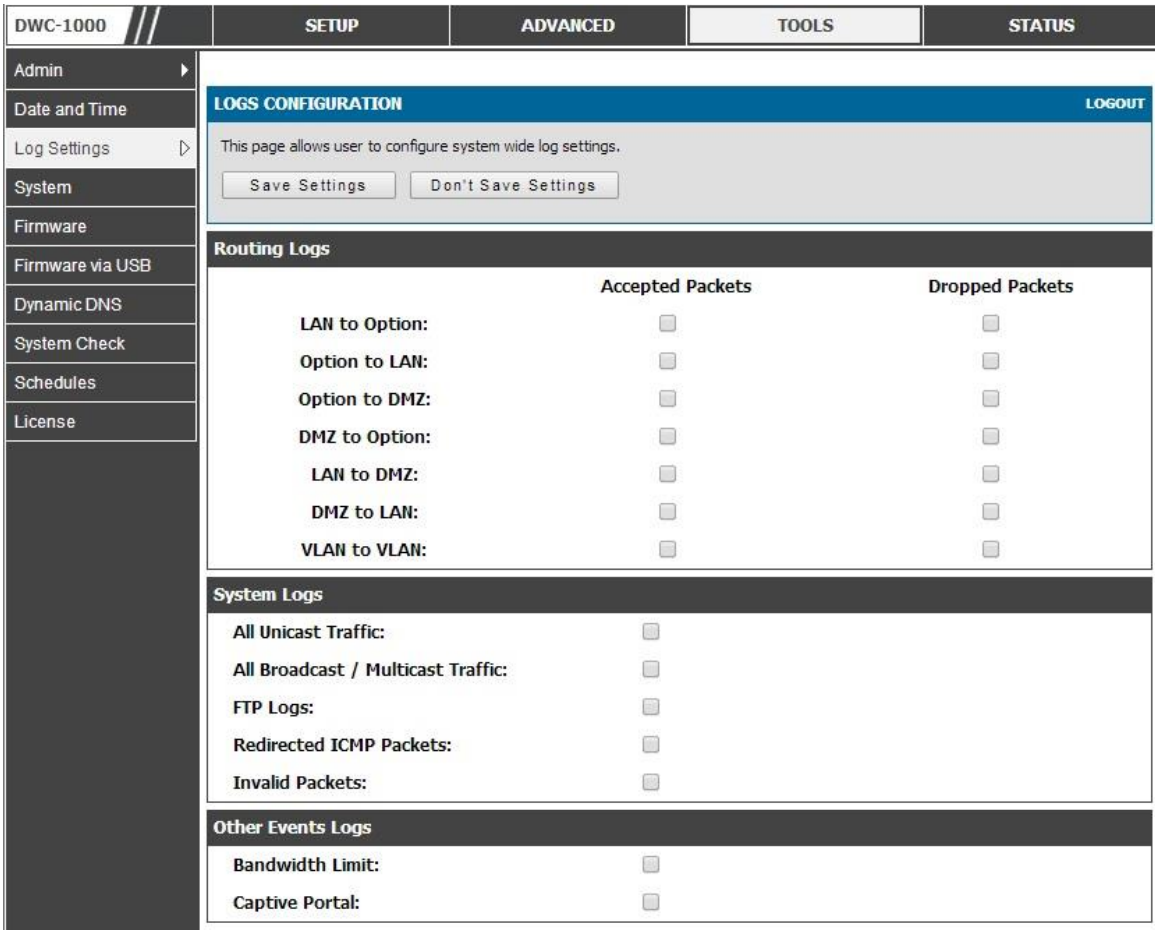
Dropped Packets are packets that were intentionally blocked from being transferred through the corresponding network segment. This option is useful when the Default Outbound Policy is “Allow Always”.

- **Example**: If Drop Packets from LAN to Option is enabled and there is a firewall rule to block SSH traffic from LAN, then whenever a LAN machine tries to make an SSH connection, those packets will be dropped and a message will be logged. (Make sure the log option is set to allow for this firewall rule.)

> ✍ Enabling accepted packet logging through the firewall may generate a significant volume of log messages depending on the typical network traffic. This is recommended for debugging purposes only.

In addition to network segment logging, unicast and multicast traffic can be logged. Unicast packets have a single destination on the network, whereas broadcast (or multicast) packets are sent to all possible destinations simultaneously. One other useful log control is to log packets that are dropped due to configured bandwidth profiles over a particular interface. This data will indicate to the admin whether the bandwidth profile has to be modified to account for the desired internet traffic of LAN users.

Figure 192: Log configuration options for traffic through controller



LOGS CONFIGURATION

This page allows user to configure system wide log settings.

Routing Logs

	Accepted Packets	Dropped Packets
LAN to Option:	□	□
Option to LAN:	□	□
Option to DMZ:	□	□
DMZ to Option:	□	□
LAN to DMZ:	□	□
DMZ to LAN:	□	□
VLAN to VLAN:	□	□

System Logs

All Unicast Traffic:	□
All Broadcast / Multicast Traffic:	□
FTP Logs:	□
Redirected ICMP Packets:	□
Invalid Packets:	□

Other Events Logs

Bandwidth Limit:	□
Captive Portal:	□

12.6.2 Sending Logs to E-mail or Syslog

Tools > Log Settings > Remote Logging

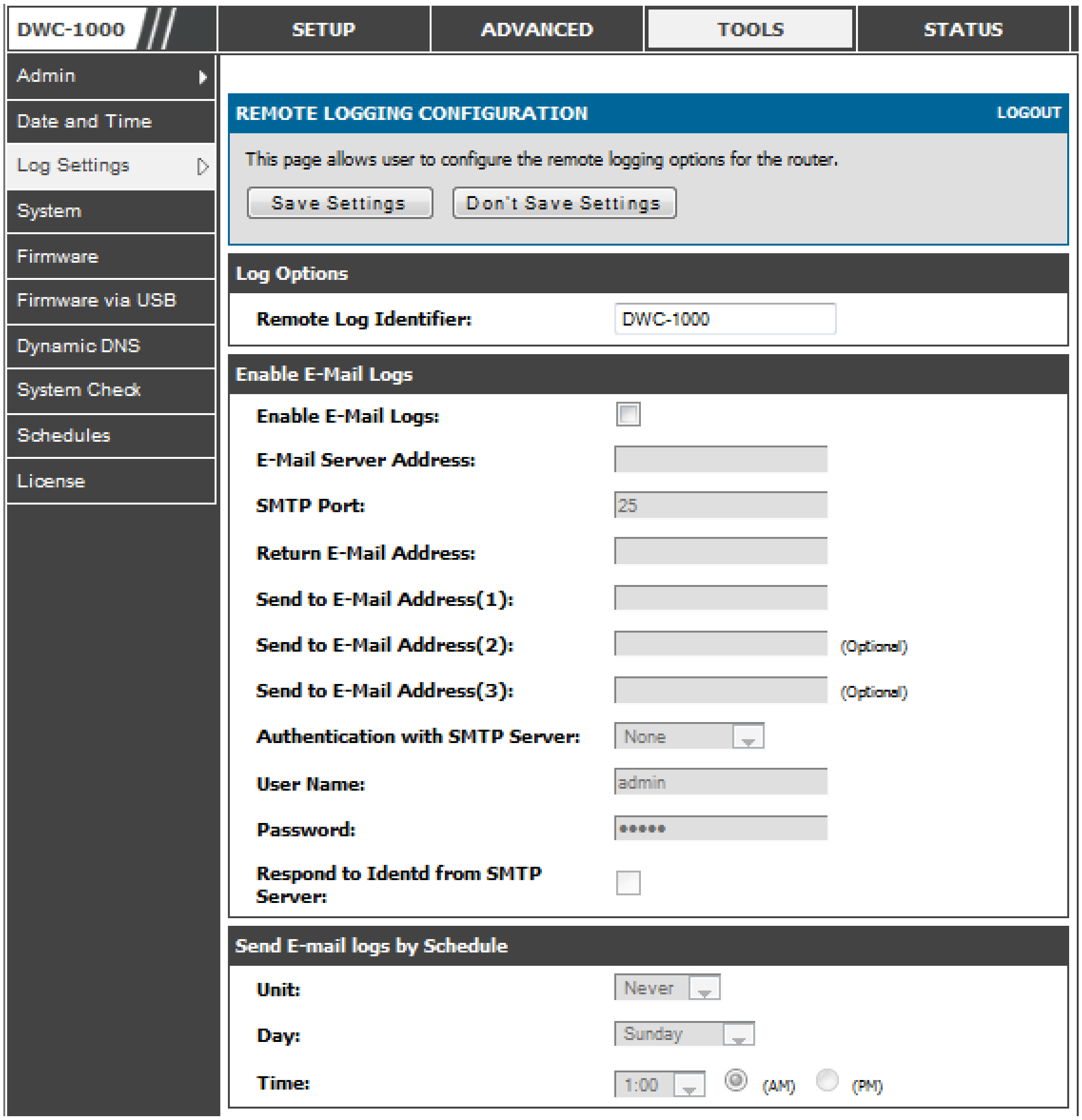
Once you have configured the type of logs that you want the controller to collect, they can be sent to either a Syslog server or an E-Mail address. For remote logging a key configuration field is the Remote Log Identifier. Every logged message will contain the configured prefix of the Remote Log Identifier, so that syslog servers or email addresses that receive logs from more than one controller can sort for the relevant device’s logs.

Once you enable the option to e-mail logs, enter the e-mail server’s address (IP address or FQDN) of the SMTP server. The controller will connect to this server when sending e-mails out to the configured addresses. The SMTP port and return e-mail addresses are required fields to allow the controller to package the logs and send a valid e-mail that is accepted by one of the configured “send-to” addresses. Up to three e-mail addresses can be configured as log recipients.

In order to establish a connection with the configured SMTP port and server, define the server’s authentication requirements. The controller supports Login Plain (no encryption) or CRAM-MD5 (encrypted) for the username and password data to be sent to the SMTP server. Authentication can be disabled if the server does not have this requirement. In some cases the SMTP server may send out IDENT requests, and this controller can have this response option enabled as needed.

Once the e-mail server and recipient details are defined you can determine when the controller should send out logs. E-mail logs can be sent out based on a defined schedule by first choosing the unit (i.e. the frequency) of sending logs: Hourly, Daily, or Weekly. Selecting Never will disable log e-mails but will preserve the e-mail server settings.

Figure 193: E-mail configuration as a Remote Logging option



REMOTE LOGGING CONFIGURATION

This page allows user to configure the remote logging options for the router.

Log Options

Remote Log Identifier: DWC-1000

Enable E-Mail Logs

Enable E-Mail Logs: □

E-Mail Server Address:

SMTP Port: 25

Return E-Mail Address:

Send to E-Mail Address(1):

Send to E-Mail Address(2): (Optional)

Send to E-Mail Address(3): (Optional)

Authentication with SMTP Server: None

User Name: admin

Password: •••••

Respond to Identd from SMTP Server: □

Send E-mail logs by Schedule

Unit: Never

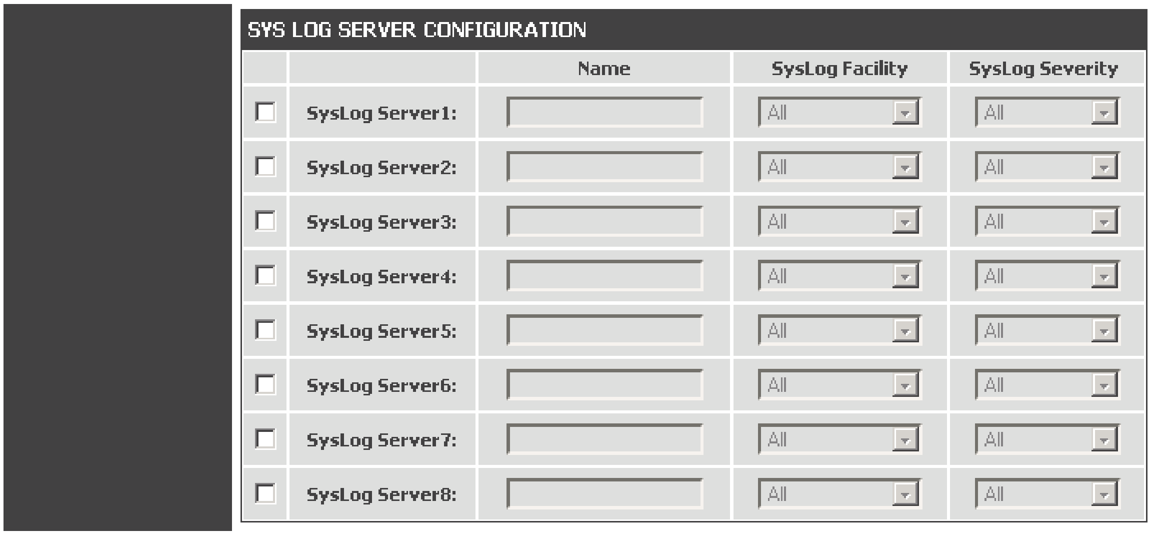
Day: Sunday

Time: 1:00 ● (AM) ○ (PM)

An external Syslog server is often used by network administrator to collect and store logs from the controller. This remote device typically has less memory constraints than the local Event Viewer on the controller GUI, and thus can collect a considerable number of logs over a sustained period. This is typically very useful for debugging network issues or to monitor controller traffic over a long duration.

This controller supports up to 8 concurrent Syslog servers. Each can be configured to receive different log facility messages of varying severity. To enable a Syslog server select the checkbox next to an empty Syslog server field and assign the IP address or FQDN to the Name field. The selected facility and severity level messages will be sent to the configured (and enabled) Syslog server once you save this configuration page's settings.

Figure 194: Syslog server configuration for Remote Logging (continued)



SYS LOG SERVER CONFIGURATION

		Name	SysLog Facility	SysLog Severity
□	SysLog Server1:		All	All
□	SysLog Server2:		All	All
□	SysLog Server3:		All	All
□	SysLog Server4:		All	All
□	SysLog Server5:		All	All
□	SysLog Server6:		All	All
□	SysLog Server7:		All	All
□	SysLog Server8:		All	All

12.6.3 Event Log Viewer in GUI

Status > Logs > View All Logs

The controller GUI lets you observe configured log messages from the Status menu. Whenever traffic through or to the controller matches the settings determined in the ***Tools > Log Settings > Logs Facility*** or ***Tools > Log Settings > Logs Configuration*** pages, the corresponding log message will be displayed in this window with a timestamp.

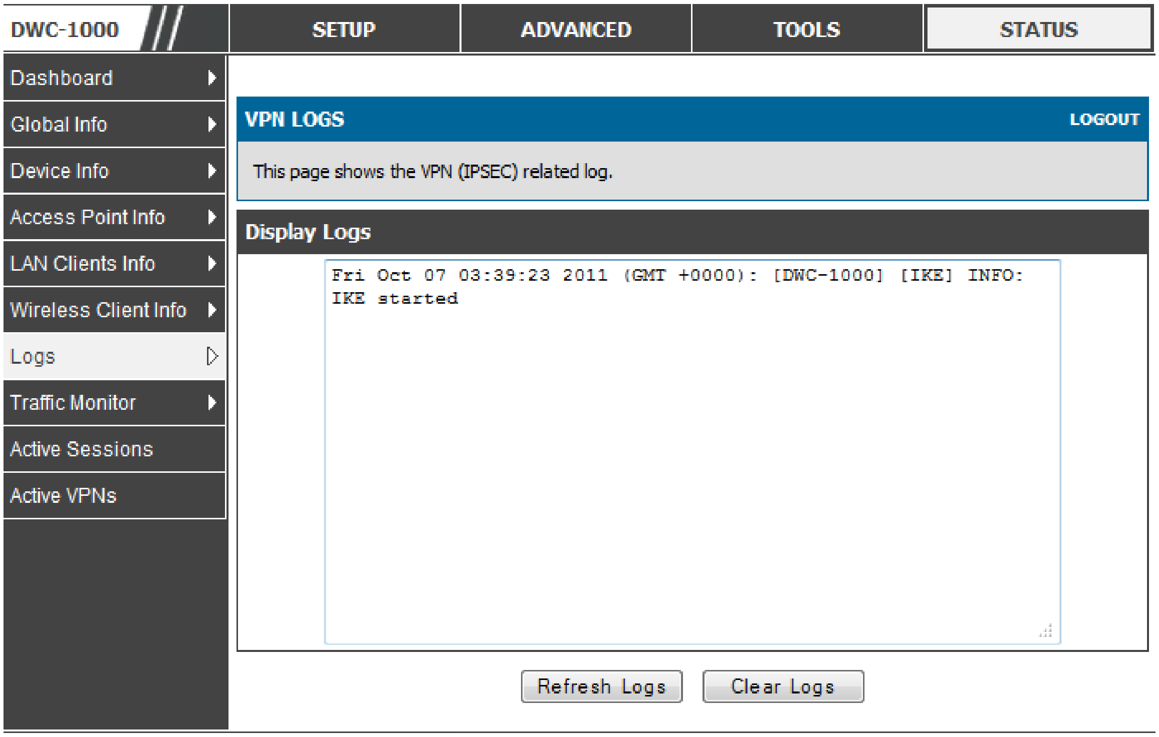
> ✍ It is very important to have accurate system time (manually set or from a NTP server) in order to understand log messages.

Status > Logs > VPN Logs

> ✍ The following feature is available upon licensed activation of VPN / Firewall features for the system.

This page displays IPsec VPN log messages as determined by the configuration settings for facility and severity. This data is useful when evaluating IPsec VPN traffic and tunnel health.

Figure 195: VPN logs displayed in GUI event viewer



This page shows the VPN (IPSEC) related log.

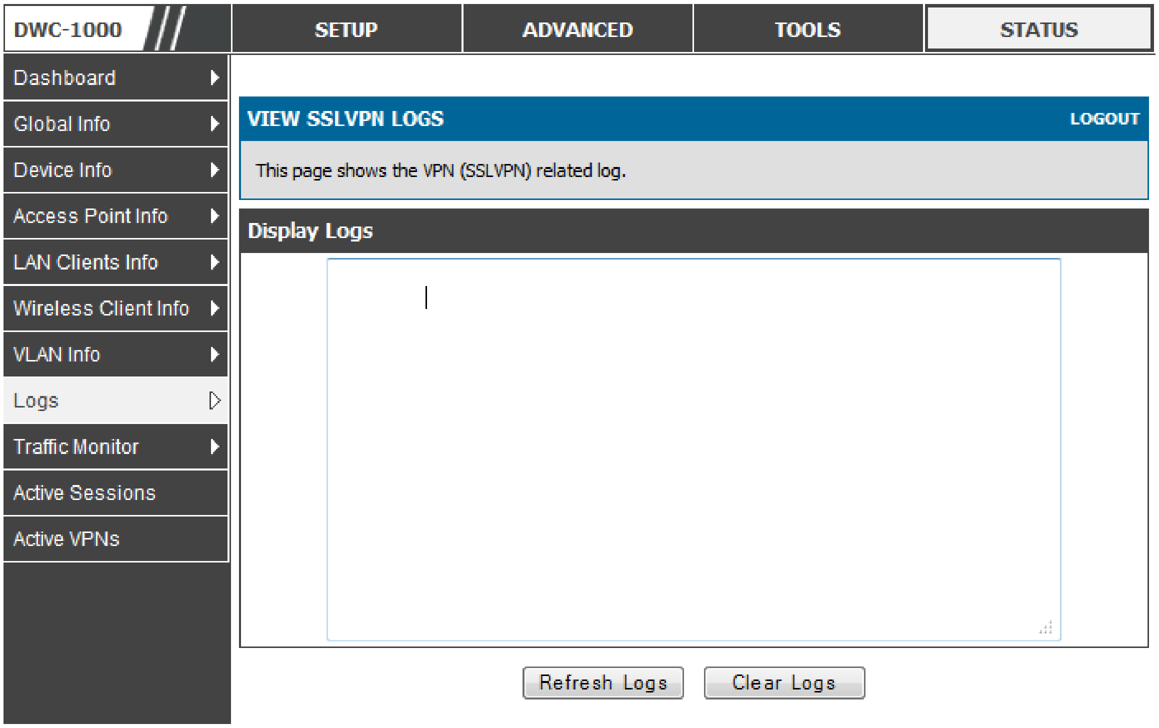
```
Fri Oct 07 03:39:23 2011 (GMT +0000): [DWC-1000] [IKE] INFO:
IKE started
```

Status > Logs > SSLVPN Logs

> ✍ The following feature is available upon licensed activation of VPN / Firewall features for the system.

This page displays SSLVPN log messages as determined by the configuration settings for facility and severity. This data is useful when evaluating SSL VPN traffic and tunnel health.

Figure 196: SSL VPN logs displayed in GUI event viewer



VIEW SSLVPN LOGS

This page shows the VPN (SSLVPN) related log.

Display Logs

12.7 Backing up and Restoring Configuration Settings

Tools > System

You can back up the controller custom configuration settings to restore them to a different device or the same controller after some other changes. During backup, your settings are saved as a file on your host. You can restore the controller saved settings from this file as well. This page will also allow you revert to factory default settings or execute a soft reboot of the controller.

> **IMPORTANT!** During a restore operation, do NOT try to go online, turn off the controller, shut down the PC, or do anything else to the controller until the operation is complete. This will take approximately 1 minute. Once the LEDs are turned off, wait a few more seconds before doing anything with the controller.

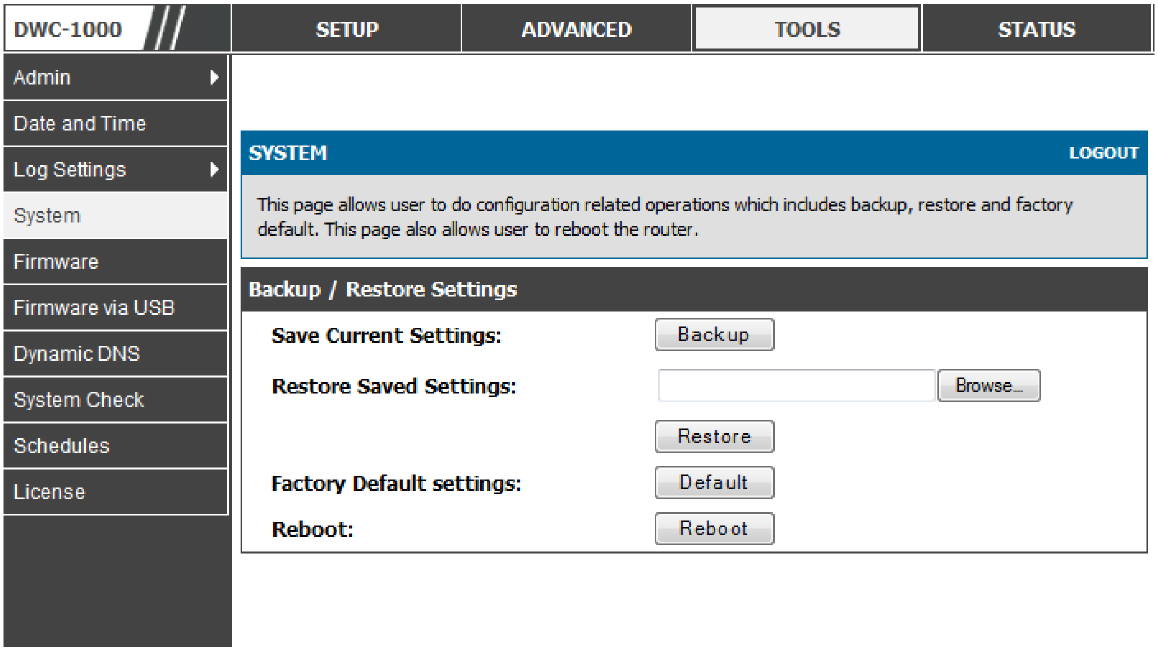
For backing up configuration or restoring a previously saved configuration, please follow the steps below:

1. To save a copy of your current settings, click the Backup button in the Save Current Settings option. The browser initiates an export of the configuration file and prompts to save the file on your host.

2. To restore your saved settings from a backup file, click Browse then locate the file on the host. After clicking Restore, the controller begins importing the file’s saved configuration settings. After the restore, the controller reboots automatically with the restored settings.

3. To erase your current settings and revert to factory default settings, click the Default button. The controller will then restore configuration settings to factory defaults and will reboot automatically. (See Appendix B for the factory default parameters for the controller).

Figure 197: Restoring configuration from a saved file will result in the current configuration being overwritten



This page allows user to do configuration related operations which includes backup, restore and factory default. This page also allows user to reboot the router.

Save Current Settings:

Restore Saved Settings:

Factory Default settings:

Reboot:

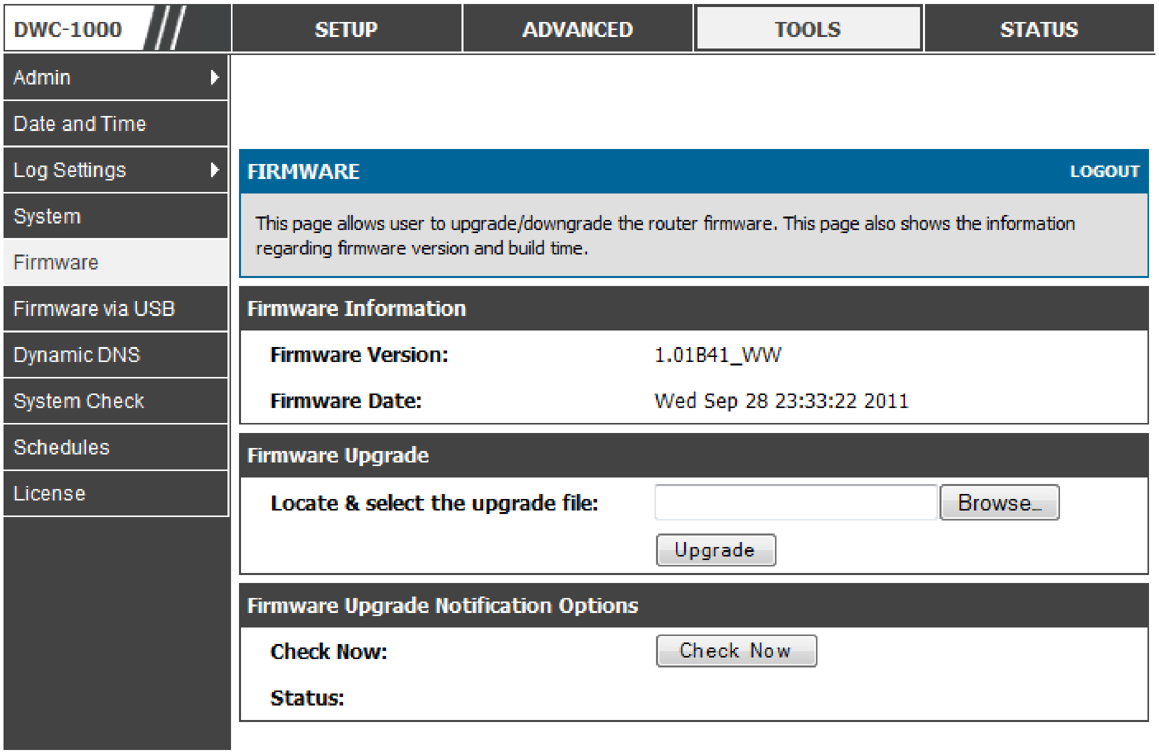
12.8 Upgrading Wirelesss Controller Firmware

Tools > Firmware

You can upgrade to a newer software version from the Administration web page. In the Firmware Upgrade section, to upgrade your firmware, click Browse, locate and select the firmware image on your host, and click Upgrade. After the new firmware image is validated, the new image is written to flash, and the controller is automatically rebooted with the new firmware. The Firmware Information and also the ***Status > Device Info > Device Status*** page will reflect the new firmware version.

> **IMPORTANT!** During firmware upgrade, do NOT try to go online, turn off the DWC-1000, shut down the PC, or interrupt the process in anyway until the operation is complete. This should take only a minute or so including the reboot process. Interrupting the upgrade process at specific points when the flash is being written to may corrupt the flash memory and render the controller unusable without a low-level process of restoring the flash firmware (not through the web GUI).

Figure 198: Firmware version information and upgrade option



FIRMWARE

This page allows user to upgrade/downgrade the router firmware. This page also shows the information regarding firmware version and build time.

Firmware Information

Firmware Version:	1.01B41_WW
Firmware Date:	Wed Sep 28 23:33:22 2011

Firmware Upgrade

Locate & select the upgrade file:

Firmware Upgrade Notification Options

Check Now:

Status:

This controller also supports an automated notification to determine if a newer firmware version is available for this controller. By clicking the Check Now button in the notification section, the controller will check a D-Link server to see if a newer firmware version for this controller is available for download and update the Status field below.

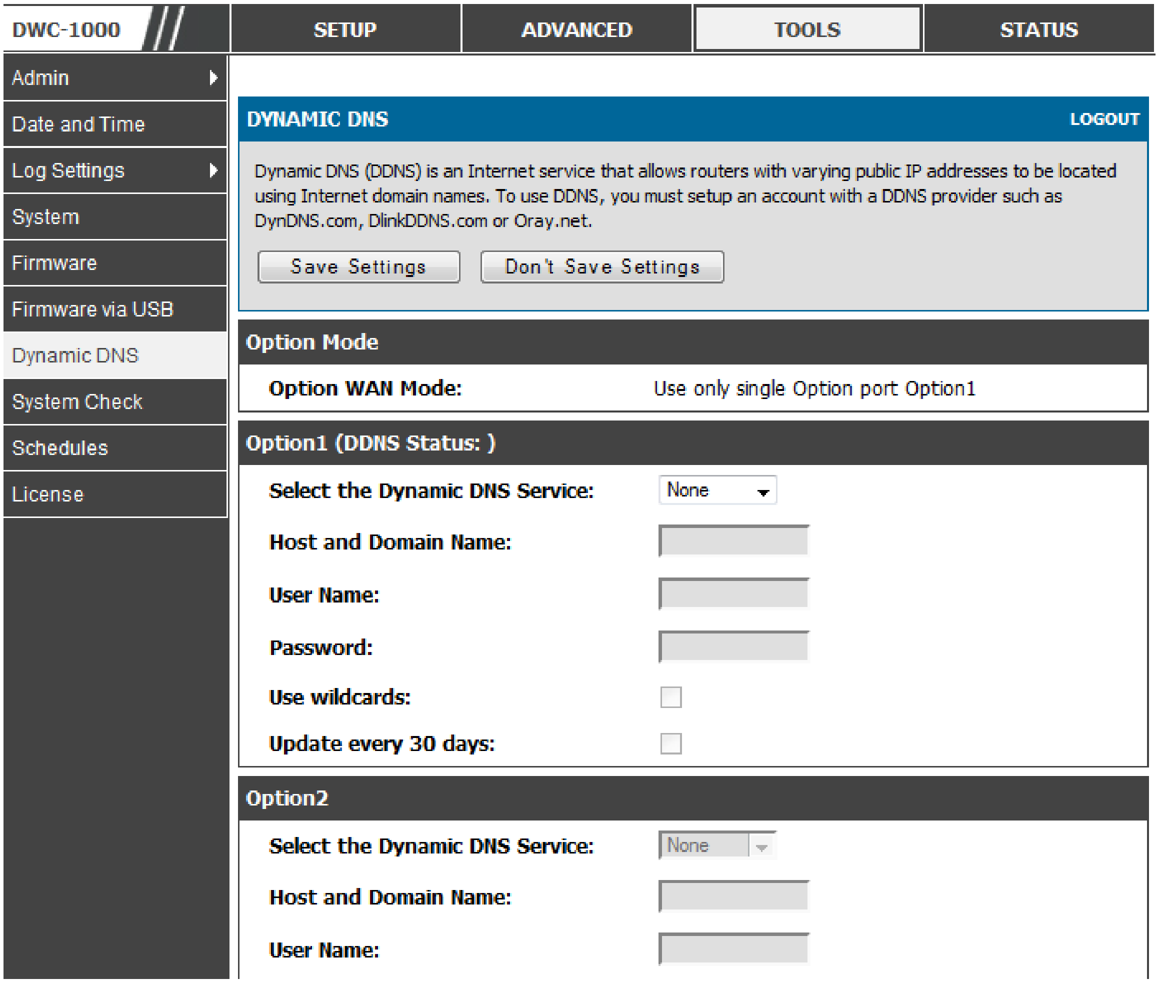
12.9 Dynamic DNS Setup

Tools > Dynamic DNS

Dynamic DNS (DDNS) is an Internet service that allows controller with varying public IP addresses to be located using Internet domain names. To use DDNS, you must setup an account with a DDNS provider such as DynDNS.org, D-Link DDNS, or Oray.net.

Each configured Option can have a different DDNS service if required. Once configured, the controller will update DDNS services changes in the Option IP address so that features that are dependent on accessing the controller Option via FQDN will be directed to the correct IP address. When you set up an account with a DDNS service, the host and domain name, username, password and wildcard support will be provided by the account provider.

Figure 199: Dynamic DNS configuration



Dynamic DNS (DDNS) is an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. To use DDNS, you must setup an account with a DDNS provider such as DynDNS.com, DlinkDDNS.com or Oray.net.

Option Mode

Option WAN Mode: Use only single Option port Option1

Option1 (DDNS Status:)

Select the Dynamic DNS Service: None

Host and Domain Name:

User Name:

Password:

Use wildcards: □

Update every 30 days: □

Option2

Select the Dynamic DNS Service: None

Host and Domain Name:

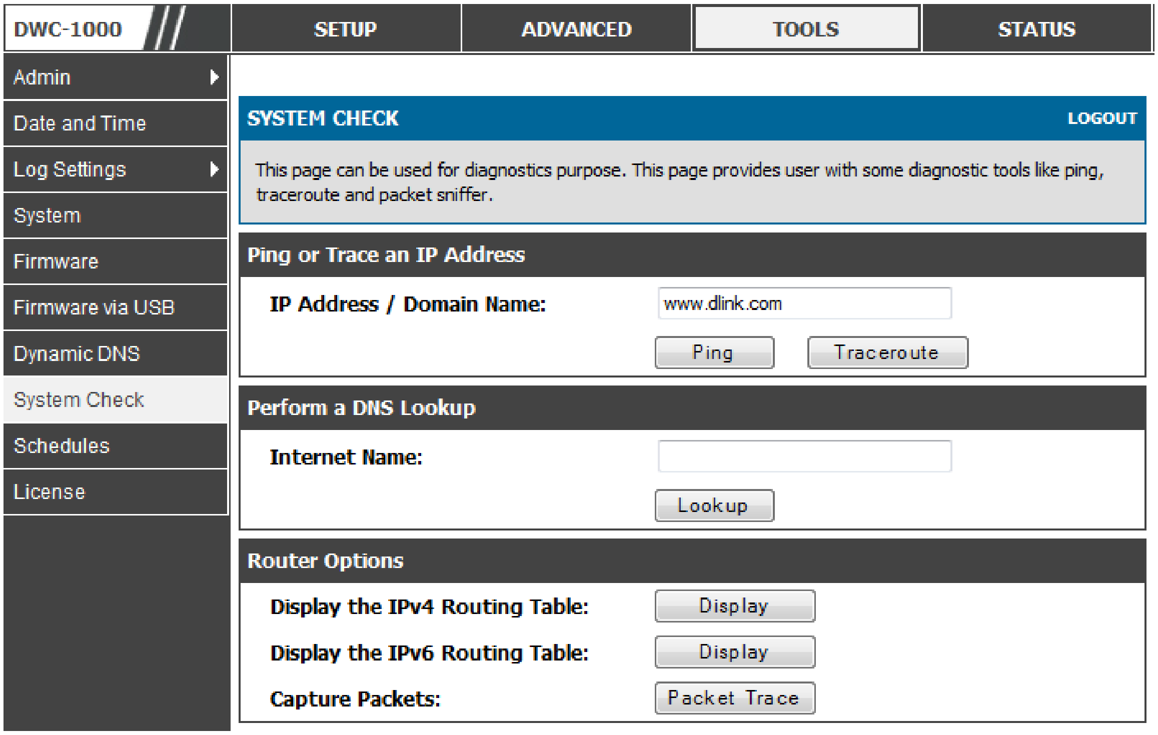
User Name:

12.9.1 Using Diagnostic Tools

Tools > System Check

The controller has built in tools to allow an administrator to evaluate the communication status and overall network health.

Figure 200: Controller diagnostics tools available in the GUI



SYSTEM CHECK

This page can be used for diagnostics purpose. This page provides user with some diagnostic tools like ping, traceroute and packet sniffer.

Ping or Trace an IP Address

IP Address / Domain Name: www.dlink.com

Perform a DNS Lookup

Internet Name:

Router Options

Display the IPv4 Routing Table:

Display the IPv6 Routing Table:

Capture Packets:

12.9.2 Ping

This utility can be used to test connectivity between this controller and another device on the network connected to this controller. Enter an IP address and click PING. The command output will appear indicating the ICMP echo request status.

12.9.3 Trace Route

This utility will display all the controller present between the destination IP address and this controller. Up to 30 “hops” (intermediate controller) between this controller and the destination will be displayed.

12.9.4 DNS Lookup

To retrieve the IP address of a Web, FTP, Mail or any other server on the Internet, type the Internet Name in the text box and click Lookup. If the host or domain entry exists, you will see a response with the IP address. A message stating “Unknown Host” indicates that the specified Internet Name does not exist.

> ✍ This feature assumes there is internet access available on the Option link(s).

12.9.5 Router Options

The static and dynamic routes configured on this controller can be shown by clicking Display for the corresponding routing table. Clicking the Packet Trace button will allow the controller to capture and display traffic through the DWC-1000 between the LAN and Option interface as well. This information is often very useful in debugging traffic and routing issues.

Chapter 13. License Activation

Tools > License

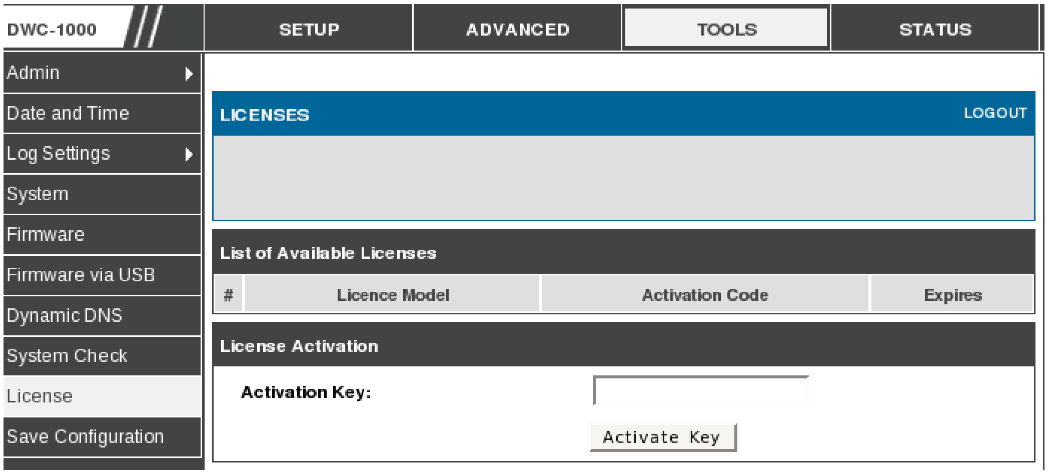
The DWC-1000 can be upgraded with three optional license packs:

1. The DWC-1000-AP6/DWC-1000-AP6-LIC License Packs enable the Wireless Controller to manage 6 extra access points. The DWC-1000 can be upgraded up to 3 times with this license pack, enabling it to support up to 24 access points in total.
2. The DWC-1000-VPN/DWC-1000-VPN-LIC License Packs enable the Wireless Controller to support VPN, Firewall, Website Filter (static WCF) and routing functions.
3. The DWC-1000-WCF-12/DWC-1000-WCF-12-LIC License Packs enable the dynamic WCF (Category filtering) feature for one year. It allows you to filter up to 32 categories of websites to restrict users from accessing them from your network, such as pornography, gambling, online shopping, and many others. Dynamic WCF also has a logging feature. Whenever a user tries to access a website that is blocked, the corresponding event will be logged.

✍ Ensure that firmware v4.2.0.6 or above for DWC-1000 is being used.

✍ Ensure that DWC-1000-VPN License is already activated before activating DWC-1000-WCF-12 License.

Figure 201: Installing a License



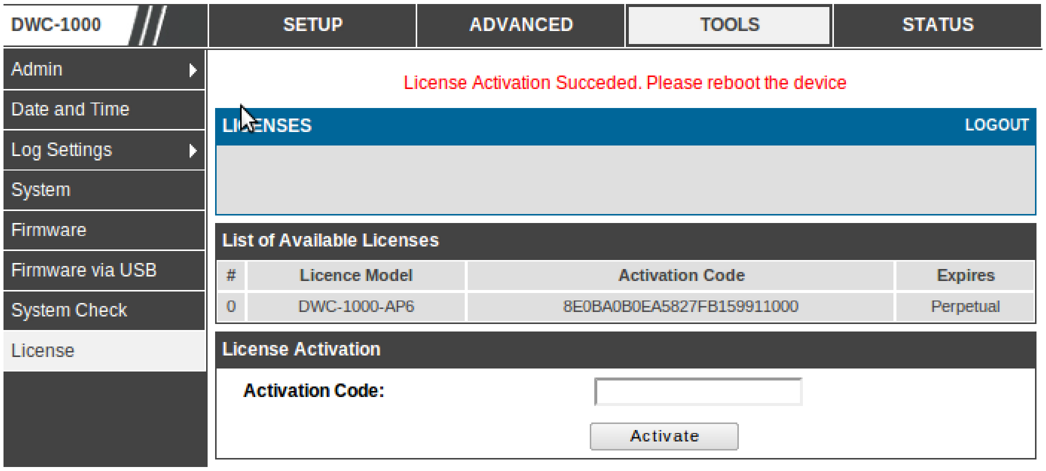
List of Available Licenses

#	Licence Model	Activation Code	Expires

License Activation

Activation Key:

Figure 202: Available Licenses Display after installing a License



License Activation Succeded. Please reboot the device

List of Available Licenses

#	Licence Model	Activation Code	Expires
0	DWC-1000-AP6	8E0BA0B0EA5827FB159911000	Perpetual

License Activation

Activation Code:

> The newly licensed features will be enabled after system reboot.

Appendix A. Glossary

ARP	Address Resolution Protocol. Broadcast protocol for mapping IP addresses to MAC addresses.
CHAP	Challenge-Handshake Authentication Protocol. Protocol for authenticating users to an ISP.
DDNS	Dynamic DNS. System for updating domain names in real time. Allows a domain name to be assigned to a device with a dynamic IP address.
DHCP	Dynamic Host Configuration Protocol. Protocol for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.
DNS	Domain Name System. Mechanism for translating H.323 IDs, URLs, or e-mail IDs into IP addresses. Also used to assist in locating remote gatekeepers and to map IP addresses to hostnames of administrative domains.
FQDN	Fully qualified domain name. Complete domain name, including the host portion. Example: serverA.companyA.com.
FTP	File Transfer Protocol. Protocol for transferring files between network nodes.
HTTP	Hypertext Transfer Protocol. Protocol used by web browsers and web servers to transfer files.
IKE	Internet Key Exchange. Mode for securely exchanging encryption keys in ISAKMP as part of building a VPN tunnel.
IPsec	IP security. Suite of protocols for securing VPN tunnels by authenticating or encrypting IP packets in a data stream. IPsec operates in either transport mode (encrypts payload but not packet headers) or tunnel mode (encrypts both payload and packet headers).

ISAKMP	Internet Key Exchange Security Protocol. Protocol for establishing security associations and cryptographic keys on the Internet.
ISP	Internet service provider.
MAC Address	Media-access-control address. Unique physical-address identifier attached to a network adapter.
MTU	Maximum transmission unit. Size, in bytes, of the largest packet that can be passed on. The MTU for Ethernet is a 1500-byte packet.
NAT	Network Address Translation. Process of rewriting IP addresses as a packet passes through a controller or firewall. NAT enables multiple hosts on a LAN to access the Internet using the single public IP address of the LAN's gateway controller.
NetBIOS	Microsoft Windows protocol for file sharing, printer sharing, messaging, authentication, and name resolution.
NTP	Network Time Protocol. Protocol for synchronizing a controller to a single clock on the network, known as the clock master.
PAP	Password Authentication Protocol. Protocol for authenticating users to a remote access server or ISP.
PPPoE	Point-to-Point Protocol over Ethernet. Protocol for connecting a network of hosts to an ISP without the ISP having to manage the allocation of IP addresses.
PPTP	Point-to-Point Tunneling Protocol. Protocol for creation of VPNs for the secure transfer of data from remote clients to private servers over the Internet.

RADIUS	Remote Authentication Dial-In User Service. Protocol for remote user authentication and accounting. Provides centralized management of usernames and passwords.
RSA	Rivest-Shamir-Adleman. Public key encryption algorithm.
TCP	Transmission Control Protocol. Protocol for transmitting data over the Internet with guaranteed reliability and in-order delivery.
UDP	User Data Protocol. Protocol for transmitting data over the Internet quickly but with no guarantee of reliability or in-order delivery.
VPN	Virtual private network. Network that enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. Uses tunneling to encrypt all information at the IP level.
WINS	Windows Internet Name Service. Service for name resolution. Allows clients on different IP subnets to dynamically resolve addresses, register themselves, and browse the network without sending broadcasts.

Appendix B. Factory Default Settings

Feature	Description	Default Setting
Device login	User login URL	http://192.168.10.1
	User name (case sensitive)	admin
	Login password (case sensitive)	admin
Internet Connection	Option MAC address	Use default address
	Option MTU size	1500
	Port speed	Autosense
Local area network (LAN)	IP address	192.168.10.1
	IPv4 subnet mask	255.255.255.0
	RIP direction	None
	RIP version	Disabled
	RIP authentication	Disabled
	DHCP server	Enabled

	DHCP starting IP address	192.168.10.2
	DHCP ending IP address	192.168.10.100
	Time zone	GMT
	Time zone adjusted for Daylight Saving Time	Disabled
	SNMP	Disabled
	Remote management	Disabled
Firewall	Inbound communications from the Internet	Disabled (except traffic on port 80, the HTTP port)
	Outbound communications to the Internet	Enabled (all)
	Source MAC filtering	Disabled
	Stealth mode	Enabled

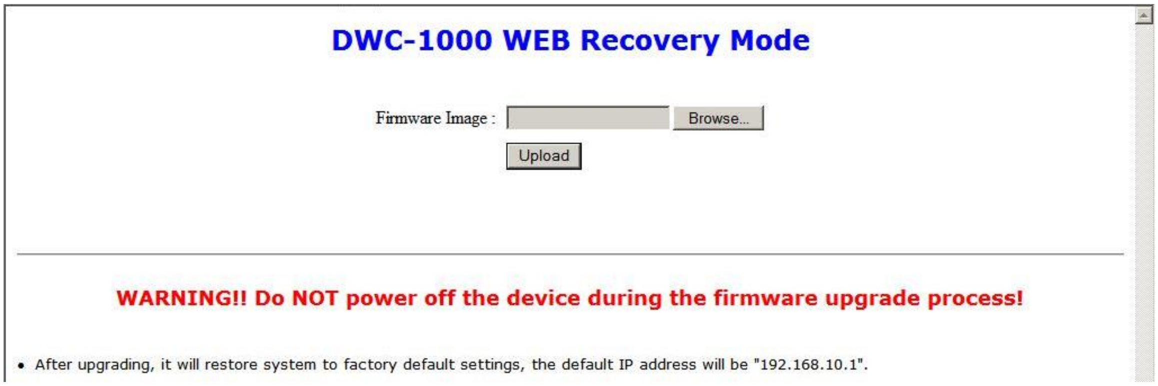
Appendix C. Recovery from Upgrade Failure

The DWC-1000 has a feature to allow for recovering from a corrupted firmware upgrade event. In rare occurrences the firmware upgrade operation can fail and render the web UI inaccessible. To recover, follow the following instructions.

1. Connect your LAN host that has a verified firmware image located on it to the LAN of the DWC-1000. The host's IP address should be in the 192.168.1.x subnet.
2. You can force the controller into "Recovery Mode"by:
   a. Turn on "Power" and push "Reset" button. The system LED will flash 5 times and the system will be in recovery mode.
   b. If during upgrade the firmware checksum integrity check fails, the system will reboot and the system LED will flash 5 times. This indicates that recovery mode has been entered.
3. The DWC-1000 LAN IP address is 192.168.1.1 and open this site with any browser.
4. Select the firmware image on your host – these screens will allow you to upload the full DWC-1000 firmware image to restore full system functionality prior to the upgrade issue.

The following screenshots demonstrate the expected display when the system is in recovery mode.

Recovery Mode launch:



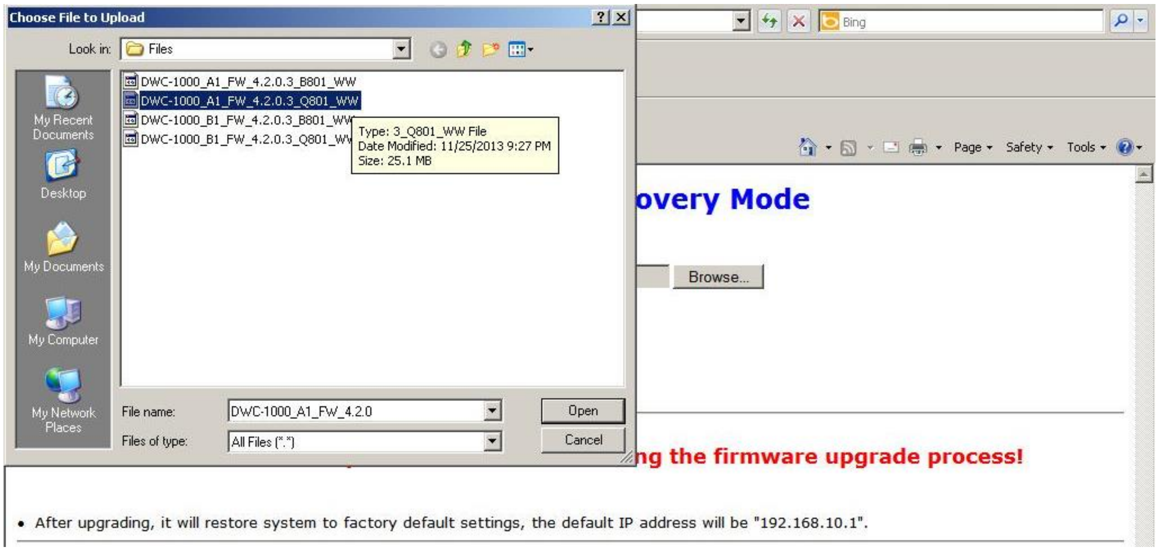
DWC-1000 WEB Recovery Mode

Firmware Image :

WARNING!! Do NOT power off the device during the firmware upgrade process!

- After upgrading, it will restore system to factory default settings, the default IP address will be "192.168.10.1".

Selecting DWC-1000 firmware on host:



Look in: Files

DWC-1000_A1_FW_4.2.0.3_B801_WW
DWC-1000_A1_FW_4.2.0.3_Q801_WW
DWC-1000_B1_FW_4.2.0.3_B801_WW
DWC-1000_B1_FW_4.2.0.3_Q801_WW

Type: 3_Q801_WW File
Date Modified: 11/25/2013 9:27 PM
Size: 25.1 MB

File name: DWC-1000_A1_FW_4.2.0

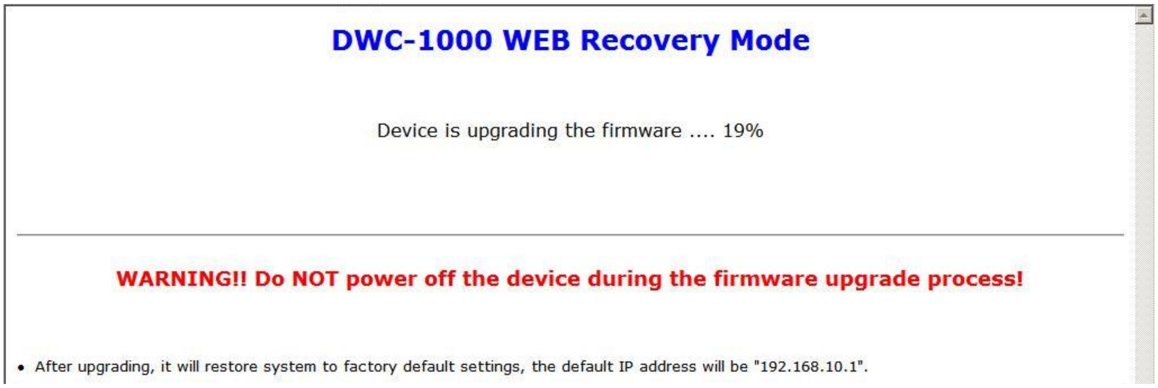
Files of type: All Files (*.*)

overy Mode

ng the firmware upgrade process!

- After upgrading, it will restore system to factory default settings, the default IP address will be "192.168.10.1".

Upgrade in Progress:



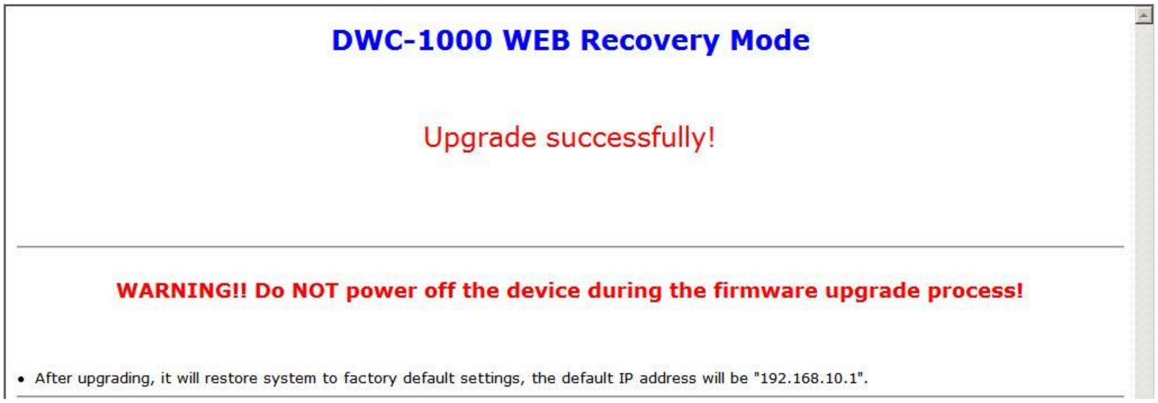
DWC-1000 WEB Recovery Mode

Device is upgrading the firmware 19%

WARNING!! Do NOT power off the device during the firmware upgrade process!

- After upgrading, it will restore system to factory default settings, the default IP address will be "192.168.10.1".

After a successful upgrade, the unit will reboot:



DWC-1000 WEB Recovery Mode

Upgrade successfully!

WARNING!! Do NOT power off the device during the firmware upgrade process!

- After upgrading, it will restore system to factory default settings, the default IP address will be "192.168.10.1".

Appendix D. Product Statement

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: 10.9 watts
Switched Off: 0 watts