D-Link®

Version 3.0 | 05/09/2013

User Manual

AP Manager II v3.0 - Business Class Networking

Table of Contents

Product Overview 1
Before you Begin 2
System Requirements 2
Access Point Requirements 2

Installation 3
Setup Wizard 3
Using the AP Manager II v3.0 11
The AP Manager II v3.0 Control Panel 12
Discovering Devices 13
Advanced Discovery 15
Access Point Report 16
Station Report 18
Model Report 19
Band Report 20
Group View 21
Group - Configuration 23
Group - Configuration - Set IP 25
Group - Configuration Update 27
Configuration - Firmware Upgrade 29
Configuration - Web Management 32
Configuration - Telnet 34
Configuration - Change Access Password 35
Configuration - Enable SNMP 36
Configuration - Configuration Comparison 38
Sorting 39
View Mode 40
Properties 41
The Access Point Manager II v3.0 42
The Home Panel 43
Basic - Wireless 44
Basic - LAN 50
Basic - IPv6 51
Advanced - Performance 53
Advanced - Multi-SSID 55
Advanced - VLAN 57
Advanced - Add/Edit VLAN's 58
Advanced - Intrusion 60
Advanced - Schedule 61
Advanced - DHCP Server 62
Advanced - AP Array 66
Advanced - AP Array - Alternative Settings 68
Advanced - Web Redirection 71
Advanced - Internal RADIUS Server 73
Advanced - Filters 74
Advanced - Traffic Control 76
Advanced - ARP Spoofing Prevention Settings 82
Maintenance - Admin 83
Maintenance - Firmware and SSL 89
Maintenance - Configuration File 90
Maintenance - Date and Time 91
Status - Device Information 93

Status - Client Information 94
Status - WDS Information.....95
Status - Channel Analyze 96
Status - Stats - Ethernet Traffic Statistics.....97
Status - Stats - WLAN Traffic Statistics.....99
Status - Log - Log View..... 101
Status - Log - Log Settings..... 102
System 104
AP Manager II v3.0 - Multi Configuration..... 105
AP Manager II v3.0 - Multi Configuration - Create a new template..... 106
AP Manager II v3.0 - Edit a Template..... 113
AP Manager II v3.0 - Delete a Template 114
AP Manager II v3.0 - Save the Configuration 115
AP Manager II v3.0 - Import the Configuration 116
AP Manager II v3.0 - Events (Event) Manager ... 126
AP Manager II v3.0 - Unread Events 127
AP Manager II v3.0 - Deleting Events..... 129
AP Manager II v3.0 - Setting Events..... 130
AP Manager II v3.0 - Event Search 150
AP Manager II v3.0 - Exporting Events 152
AP Manager II v3.0 - Setting Notices..... 153
AP Manager II v3.0 - Create Watchlist..... 154
AP Manager II v3.0 - Tools - Topology..... 157
AP Manager II v3.0- Tools - Site Planning 167
AP Manager II v3.0 - Tools - Config Comparison..... 172
AP Manager II v3.0 - Report..... 175
AP Manager II v3.0 - Report - Association..... 176
AP Manager II v3.0 - Report - Security..... 179
AP Manager II v3.0 - Report - Utilization 180
AP Manager II v3.0 - Report - Channel 181
AP Manager II v3.0- Report -Rogue AP 182
AP Manager II v3.0 - Report -Syslog 183
AP Manager II v3.0 - Report -Custom 184
AP Manager II v3.0 - Report -Monitor..... 185
AP Manager II v3.0 - User Manager 188
AP Manager II v3.0 - Options 191

Product Overview

MANAGE THE NETWORK

AP Manager II v3.0 is a versatile and convenient software solution for IT staff to manage the network and their routers. The AP Manager is the ideal solution for network infrastructure management. Connect one or many routers to the main management system and contol and run IP management from one location.

STREAM DIGITAL MEDIA CONTENT THROUGHOUT THE NETWORK

Managing the backbone of your network couldn't be easier with the AP Manager II v.3.0. Control how data is routed and trafficed thoughout the network.

PROTECTION, PERFORMANCE, AND FLEXIBILITY

The AP Manager has fail-safe security built-in. Security is managed at the network layer so data is secure and safe. Manage the speed of a network by throttling the bandwidth. Give priority to users who demand mission critical access. Install new IP topologies from one location and manage its throughput using our great management tools.

Before you Begin

- Check box contents
- Check system requirements
- Ensure that you have the hardware you need for your router

System Requirements

For best results, the following minimum requirements are recommended on any system used to configure a router:

- Computer with: 1Ghz processor / 512MB RAM / 200MB available space / CD-ROM drive
- Windows® XP (with Service Pack 2), Windows Vista®, Windows® 7
- Mac OS® X 10.5.6 or greater
- Installed Ethernet Adapter
- Postgre SQL 8.3

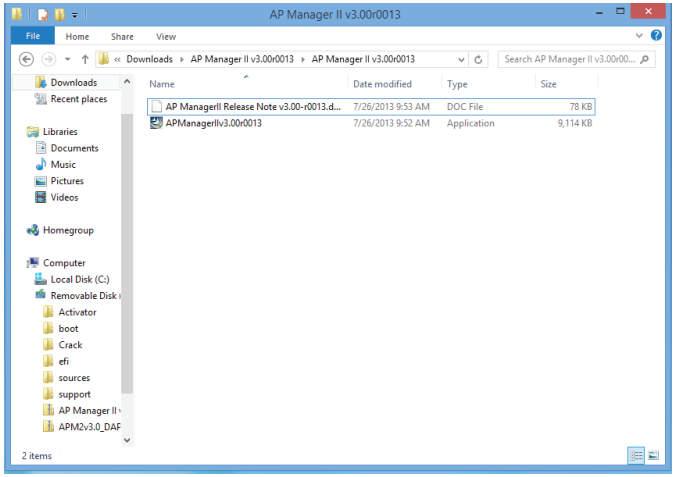
Access Point Requirements

- SNMP must be enabled on Access Points used with AP Manager v3.0

Installation
Setup Wizard

To run the Setup Wizard, insert the CD into your CD-ROM drive.

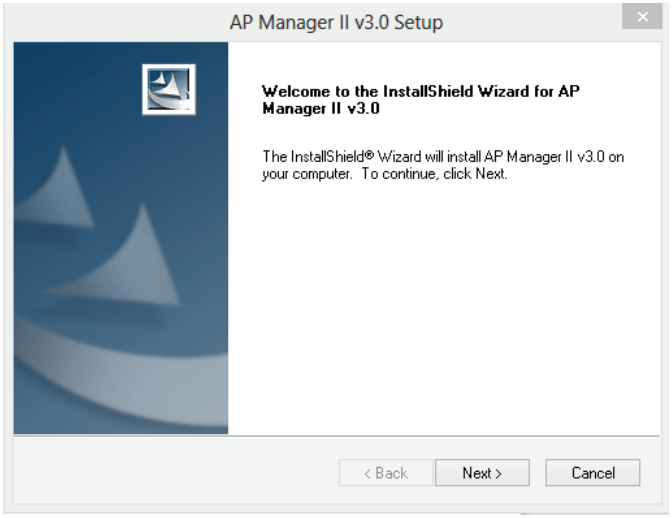
Step 1 - When the autorun screen appears, click **Install.** Otherwise, click the AP Manager v3.0 installation icon.



Note: *Windows Firewall presents you with a warning message to unblock the device. Click Unblock to give your computer access to the installation process.*

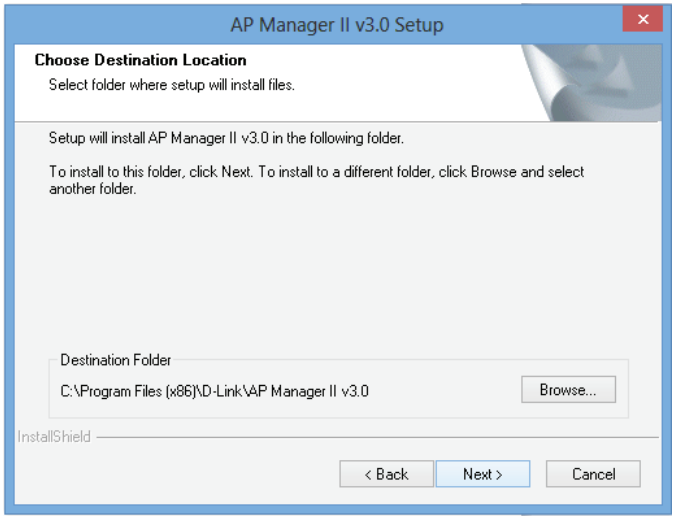
Step 2 - The AP Manager II v3.0 Installation window appears.

Click **Next** to continue.



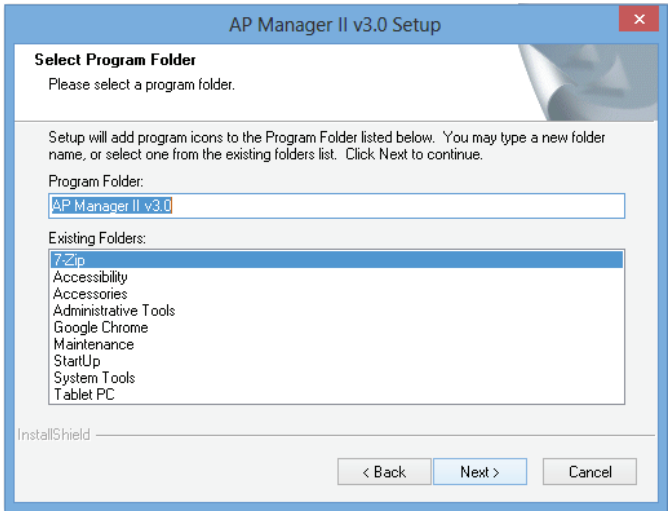
Step 3 - Select the installation location.

Click **Next** to continue.



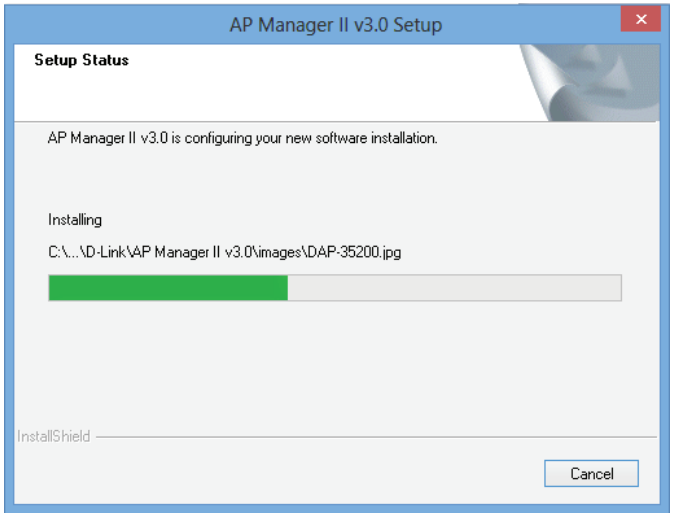
Step 4 - Select the Program Folder

Click **Next** to continue.

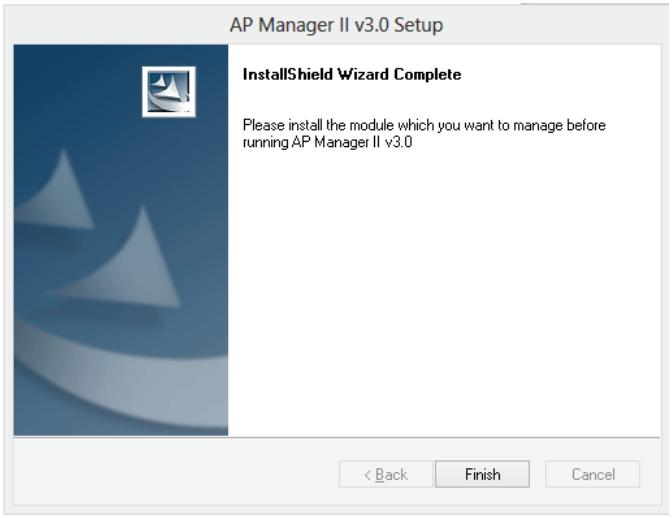


Step 5 - The installation begins.

Please be patient while the installation process takes place (a matter of seconds)

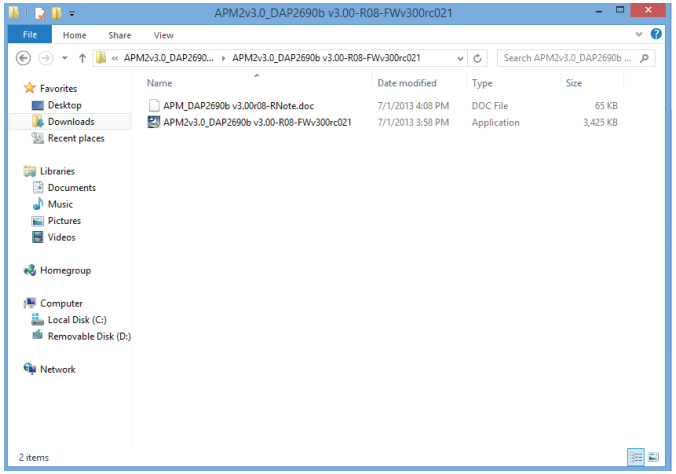


Step 6 - Click Finish to exit the Wizard.



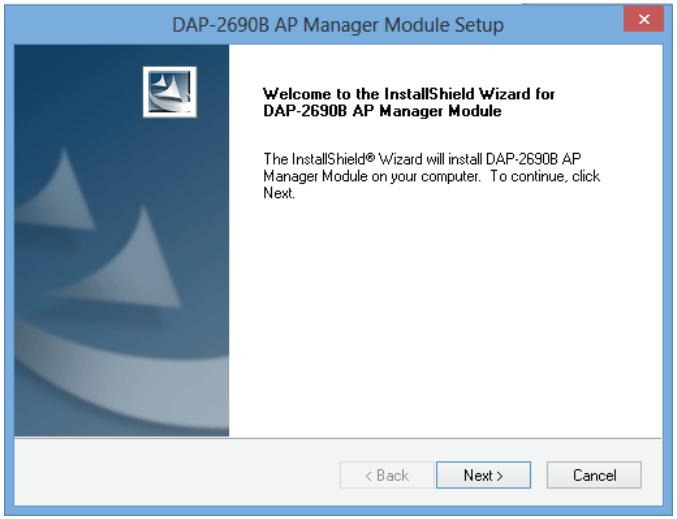
Step 7 - An AP Manager II v3.0 icon appears automatically on your desktop. Before you click the icon to start the program, install the module

Step 8 - Browse to the location where you have the module. Double-click the module to install.



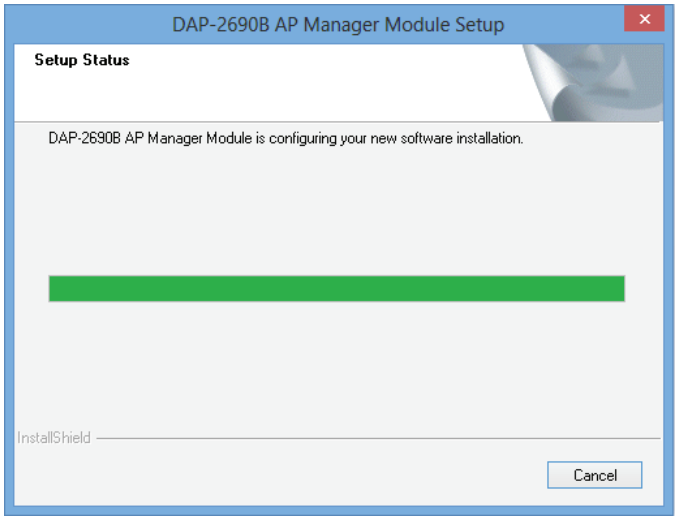
Step 9 - The module Wizard for the DAP-2690 AP Manager v3.0 begins.

Click **Next** to continue.

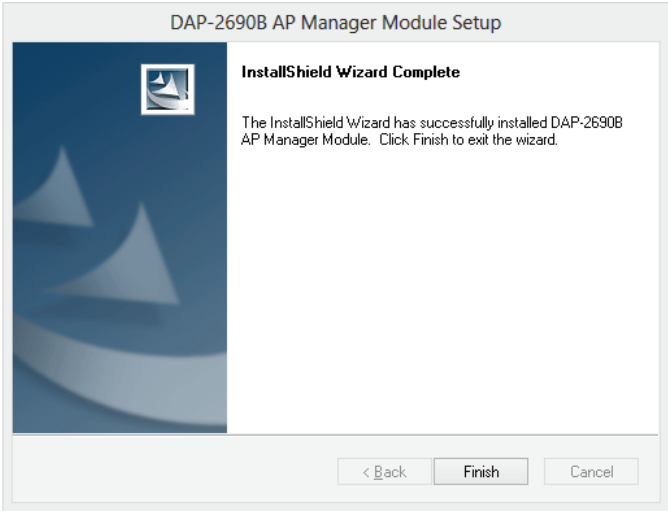


Step 10 - The wizard installs the module momentarily.

Click **Cancel** if you wish to exit otherwise wait for the installation process to complete.



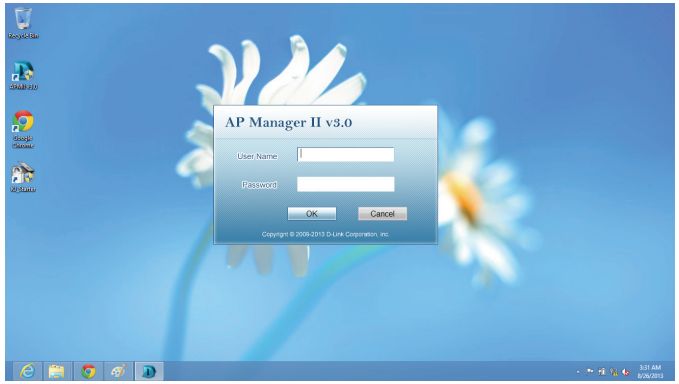
Step 11- Click **Finish** to close the wizard.



Step 12- **Right-click** the icon and click **Run as administrator**.

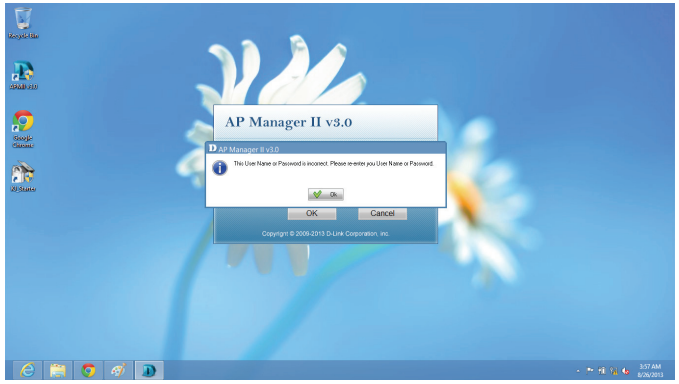
Step 13 - Enter the **Username** and **Password** at the log-in screen.

Click **OK** to continue.



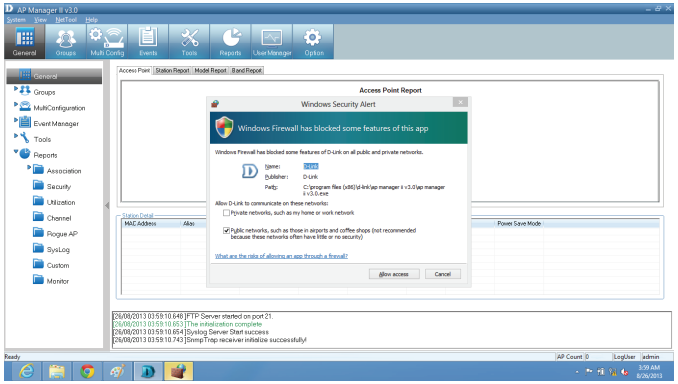
Step 14 - If you have entered the wrong details, the software will warn you and prompt you to enter the correct information.

Click **OK** to continue and enter the correct details once again.

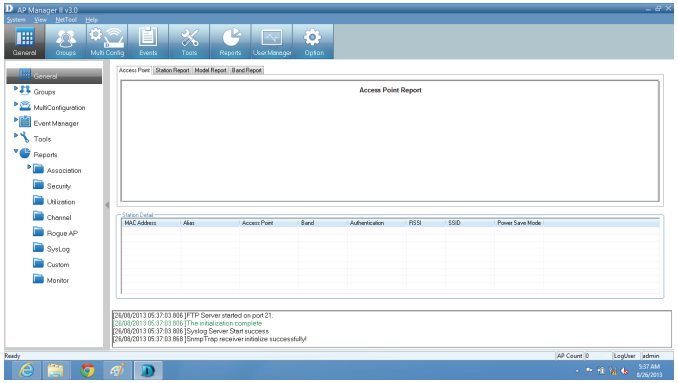


Step 15 - Windows Firewall blocks the program if you do not provide it access.

Click the **Allow access** button to continue.



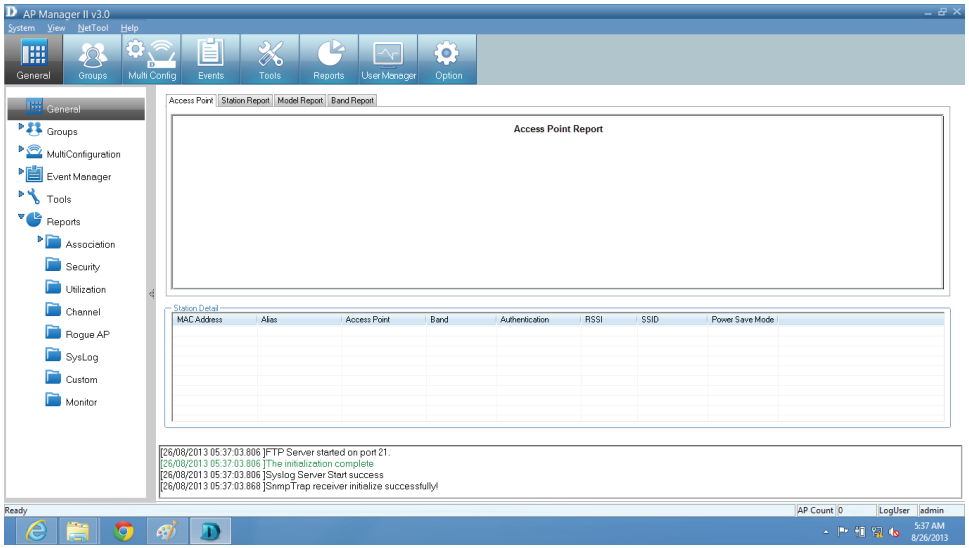
This completes the installation process for the main software. You are now presented with the **AP Manager II v3.0** main control panel.



Using the AP Manager II v3.0

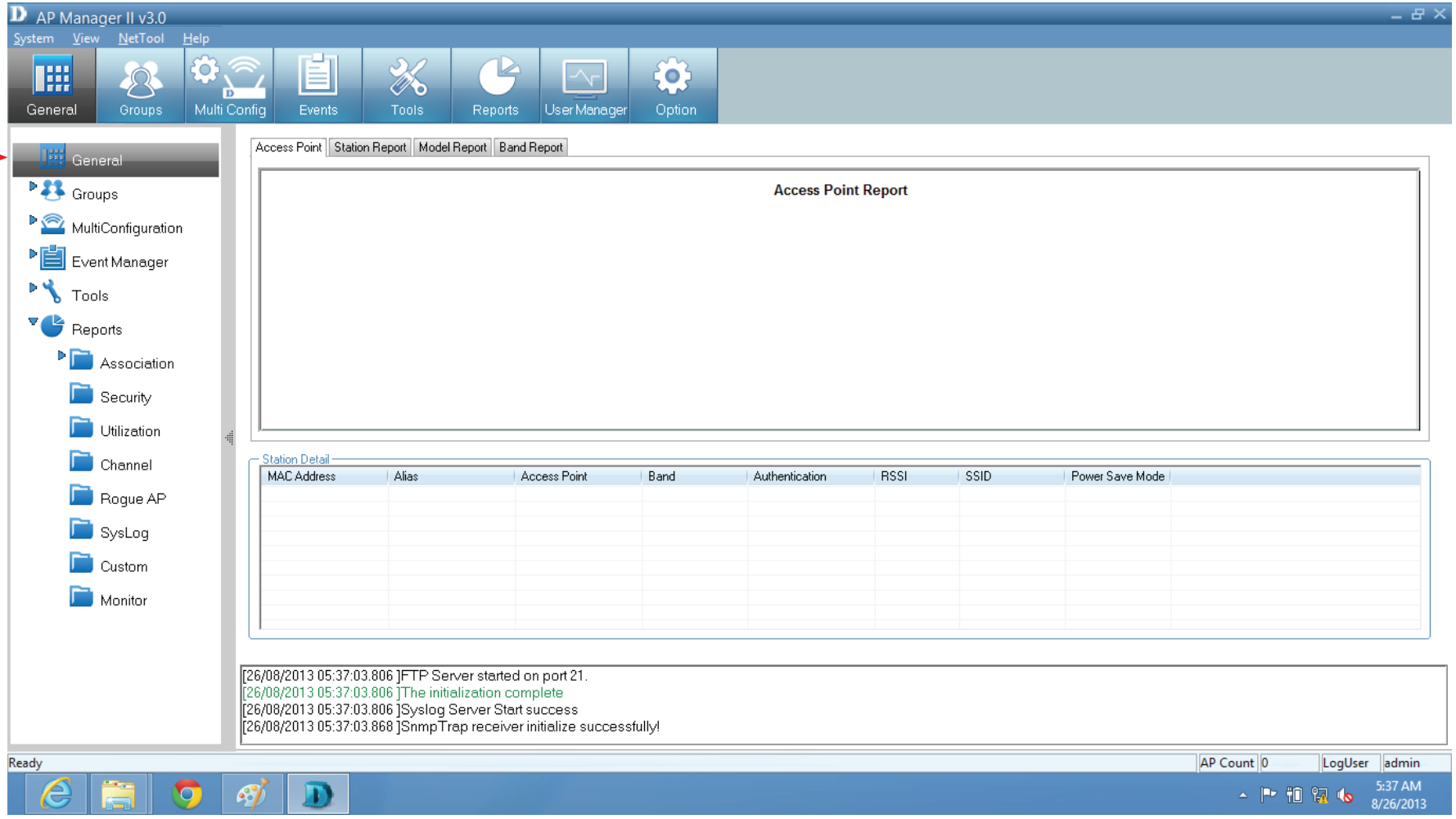
Launch the **AP Manager II v3.0** by clicking:

1. Start Menu
2. Select Programs
3. Select D-Link AP Manager II v3.0
4. Select AP Manager II v3.0



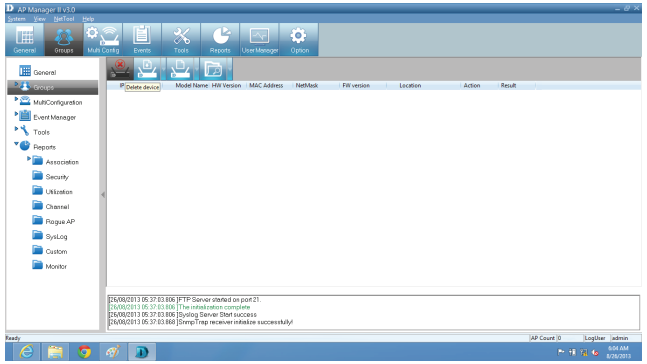
The AP Manager II v3.0 Control Panel

The **Main Control Panel** has eight key configuration Windows. **General**, **Groups**, **Multi Config**, **Events, Tools, Reports**, **User Manager**, and **Option**. The **General** window offers simple data information on the **Access Point, Station Report(s), Model Report(s), and a Band Report.**

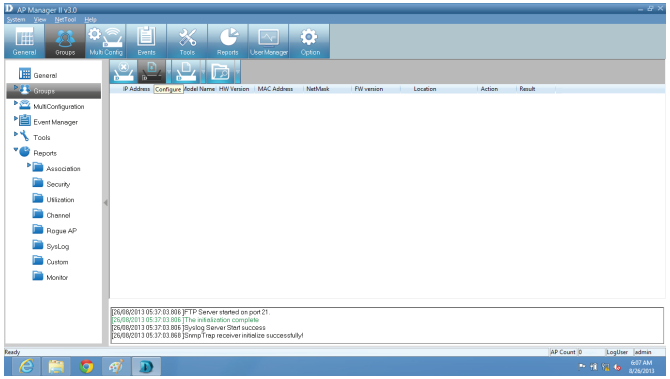


Discovering Devices

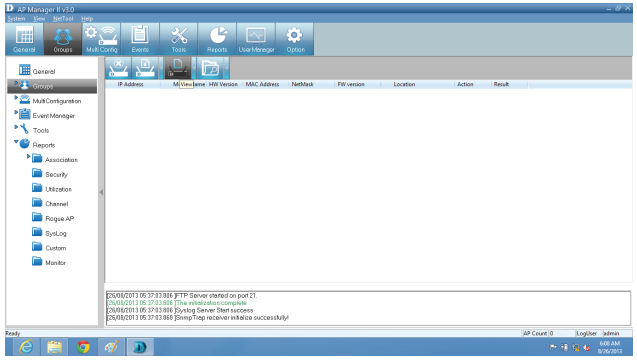
Before you can manage and monitor the **Access Point**, you must discover the device. Click **Groups** on the main menu bar. **Groups** has four main icons. **Delete**, **Configure**, ***View***, and **Discover**.



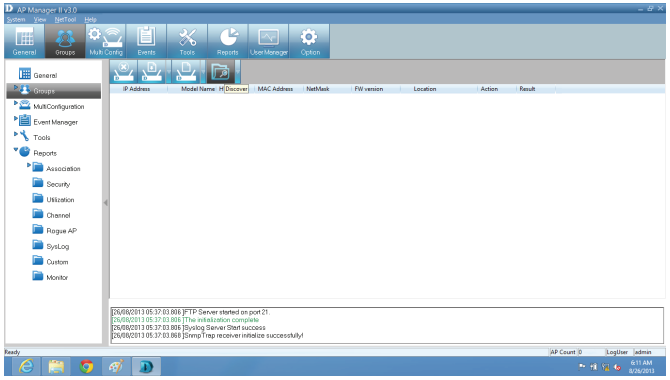
Delete



Configure

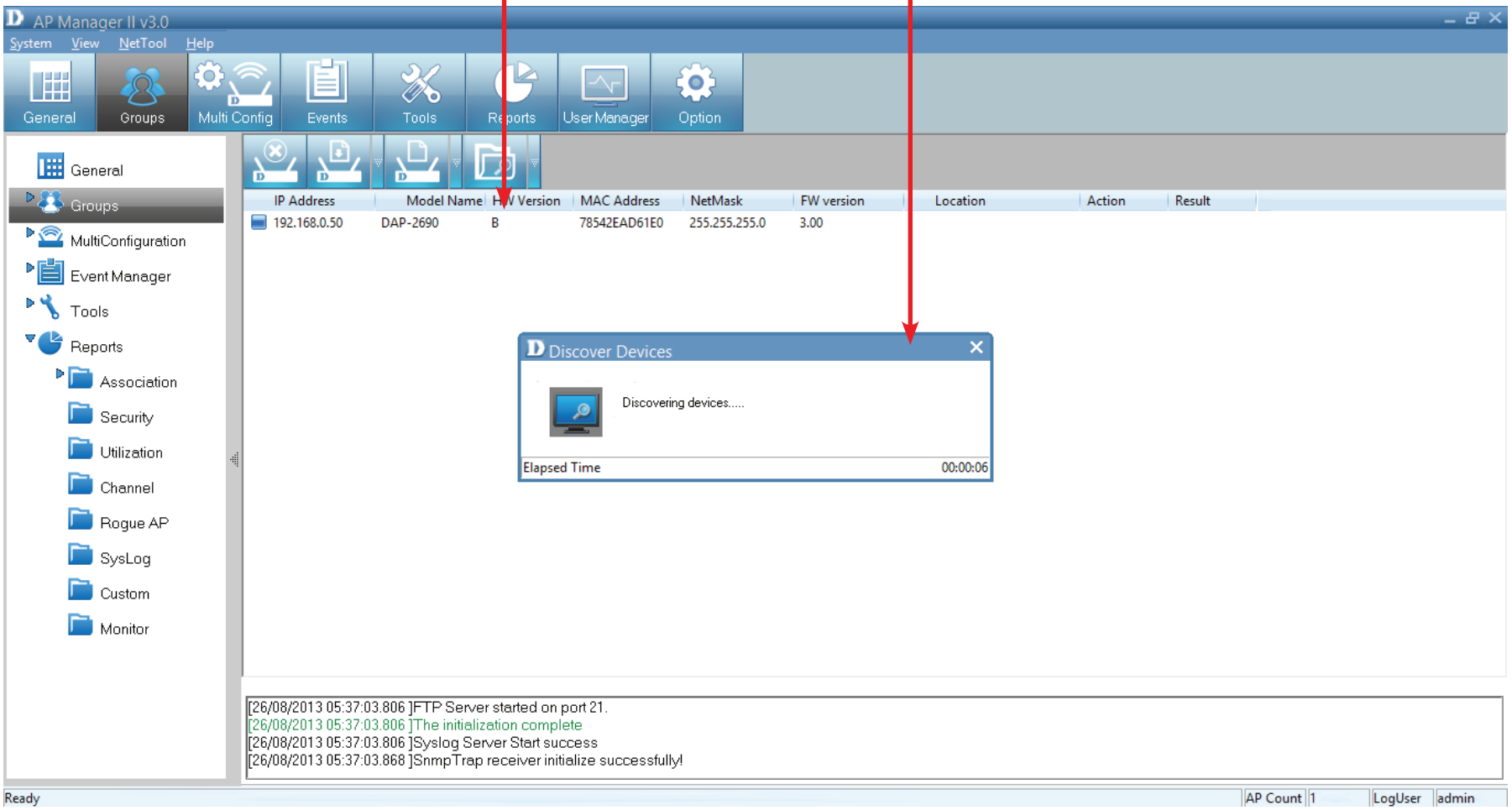


View



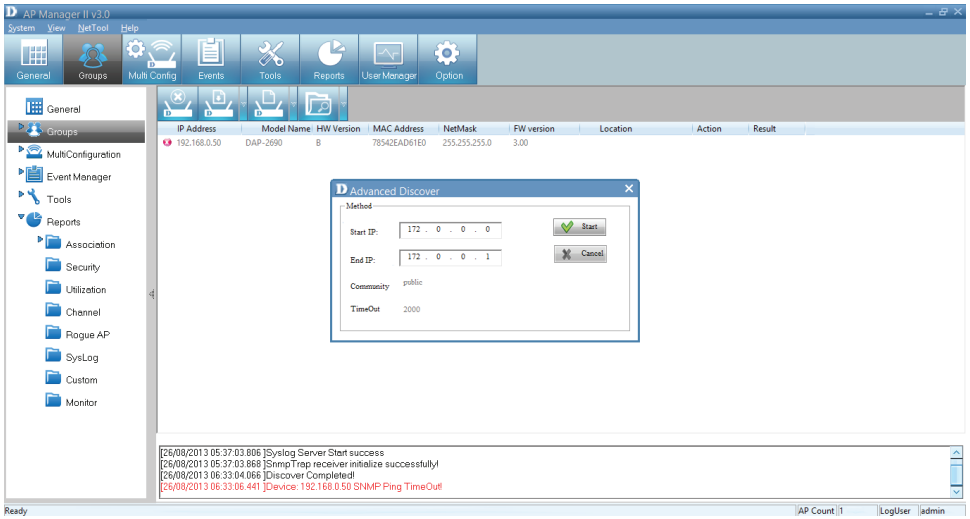
Discover

Click **Discover** to find the **Access Point**. The following dialogue window will appear during the **Discovery process.** If you AP is connected, it is detected and shown on the screen.



Advanced Discovery

The standard discovery can only discover the **Access Point's** in the same sub network. To discover the **Access Points** in the other network segments, click the arrow next to the **Discover** icon and from the drop-down list click **Advanced Discover**.



Under **Advanced Discover**, enter the **Start IP** and the **End IP** and click the **Start** button to search for **Access Points** within the specified **IP range**. Once other **Access Points** are discovered their status will be updated by the icons associated to it.

New Access Point

Managed Access Point

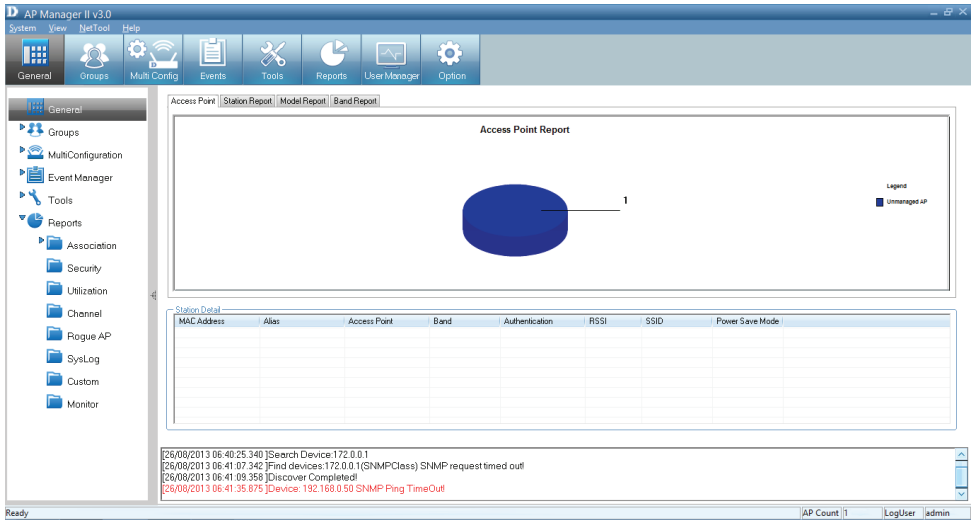
The Access Point cannot be pinged but can be modified.

The Access Point is offline and/or the SNMP engine is disabled.

The Access Point is specified as a Rogue AP

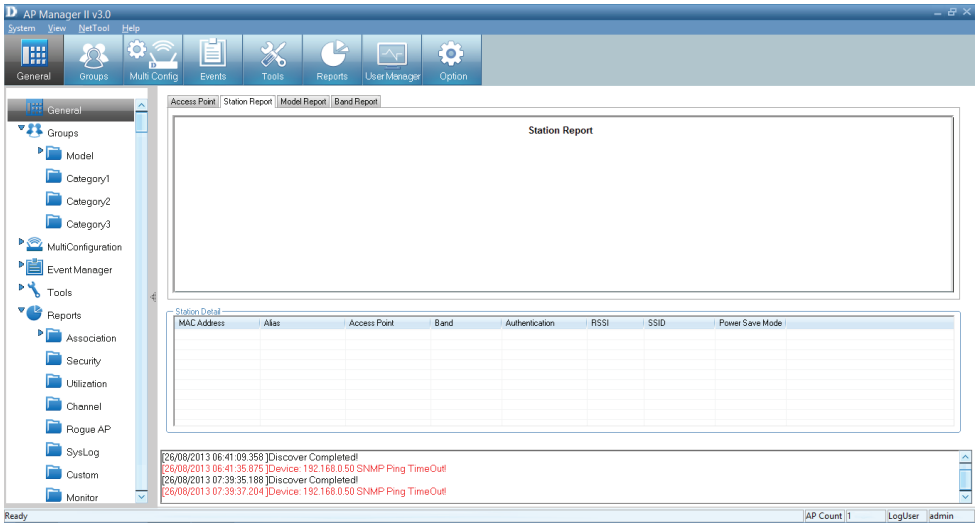
Access Point Report

The **Access Point Report** shows the discovered AP's. Access Points are divided into **Managed Access Points** and **Unmanaged Access Points**. The Managed APs are listed in the **Station Detail** table below the Access Point Report.

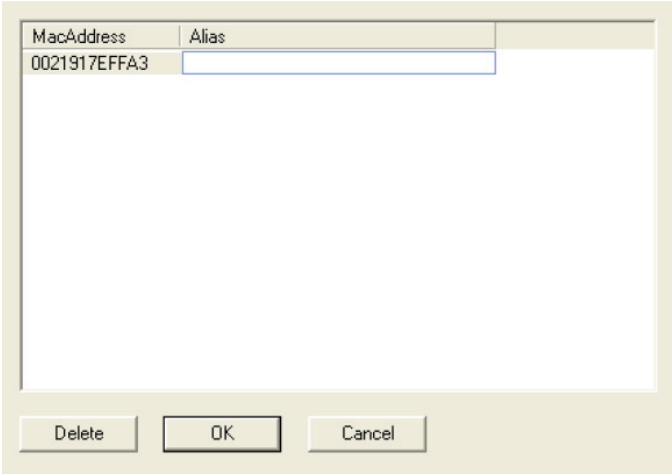


The **Station Report** table lists the **MAC Address, Alias, Access Point, Band, Authentication type, RSSI, SSID**, and **Power Save Mode** of all stations connected to the Managed APs.

Remove an **Access Point** from the list by right-clicking it and selecting **Kick Off.**

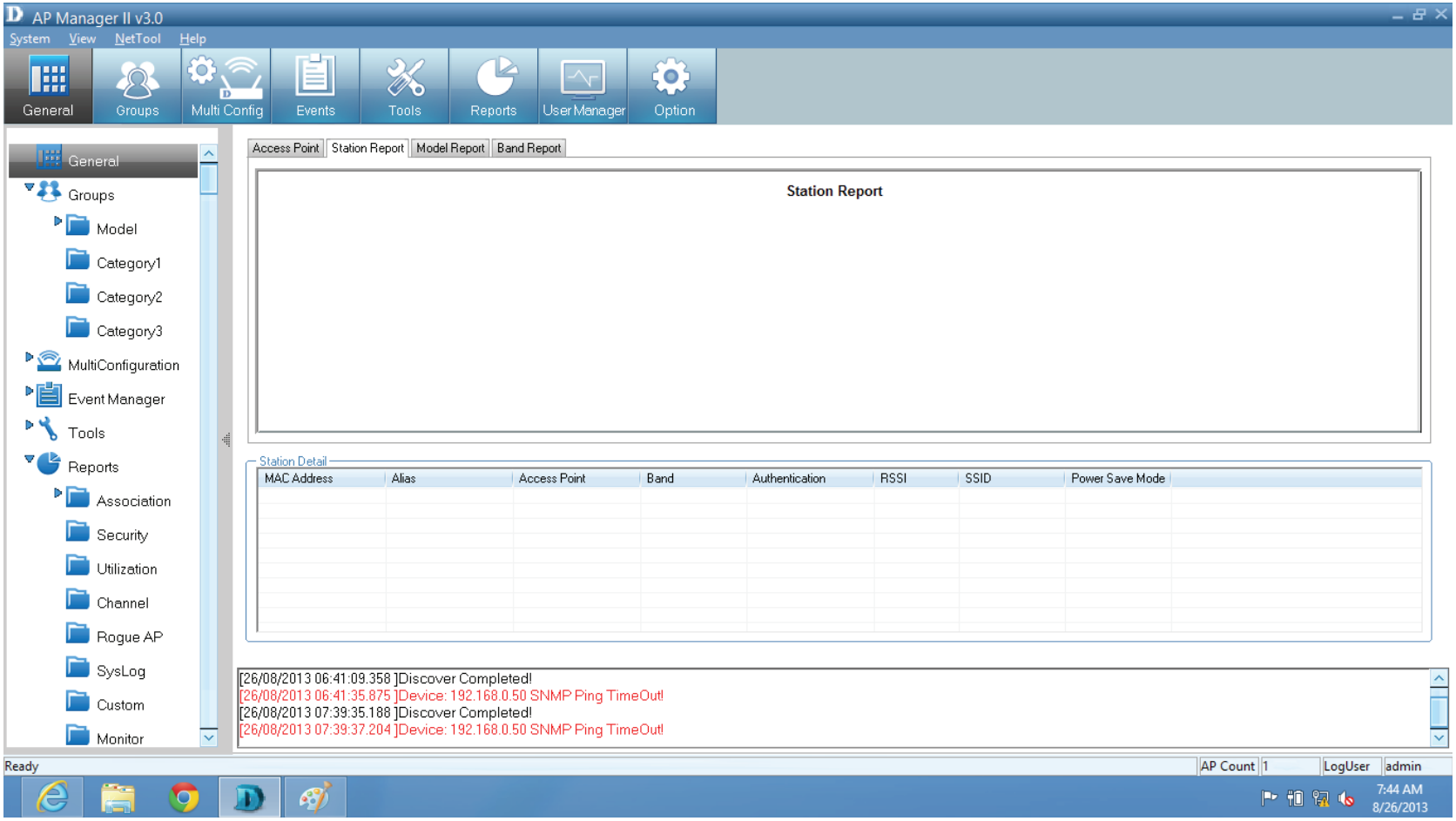


Create an **Alias** by right-clicking the **Access Point** and selecting **Alias**. In the Alias management window, type the new name. Click **OK** to continue.



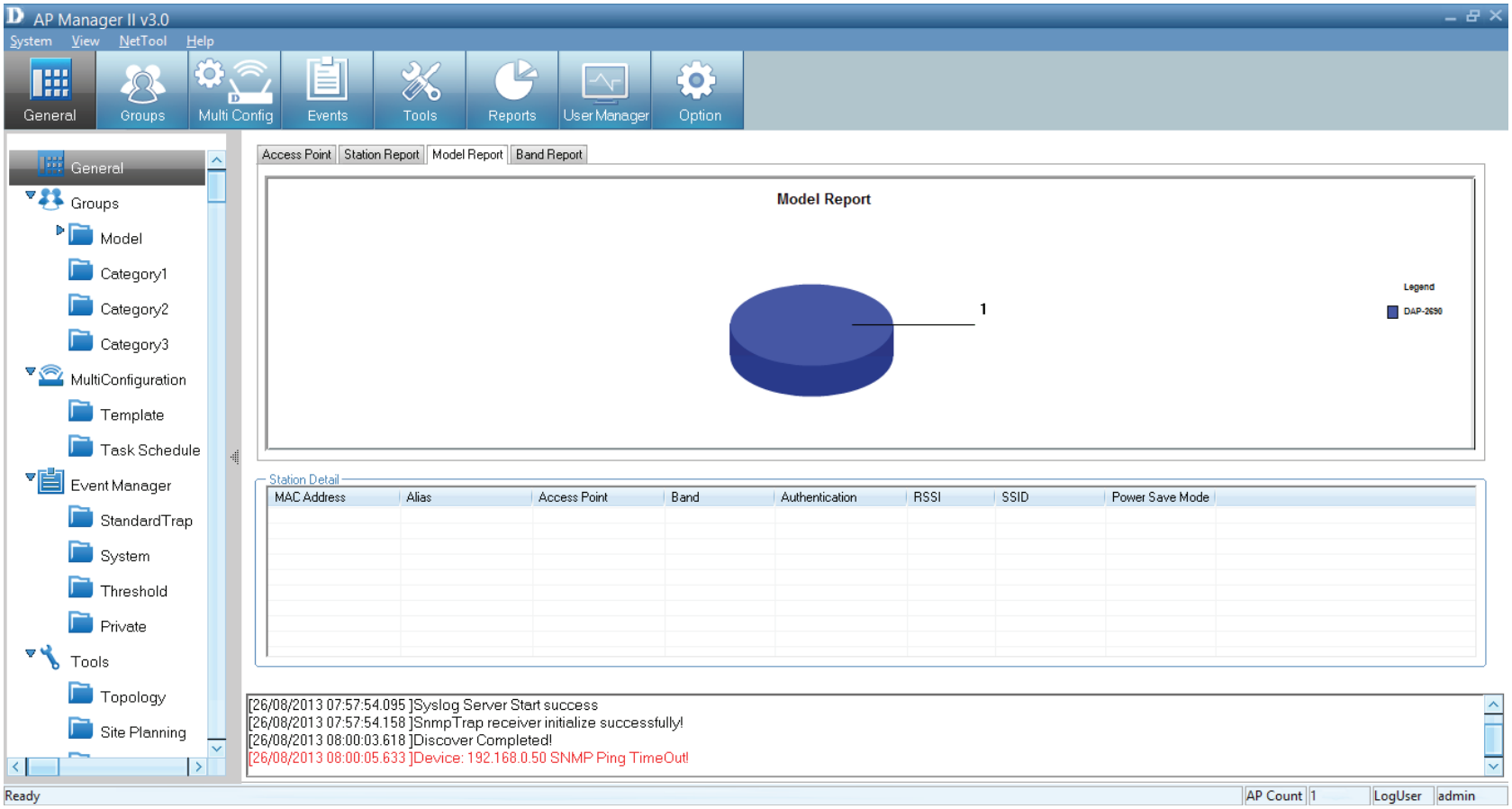
Station Report

The **Station Report** displays a graphical representation of the associated wireless stations. It classifies the stations by bands, and shows the station numbers of every band.



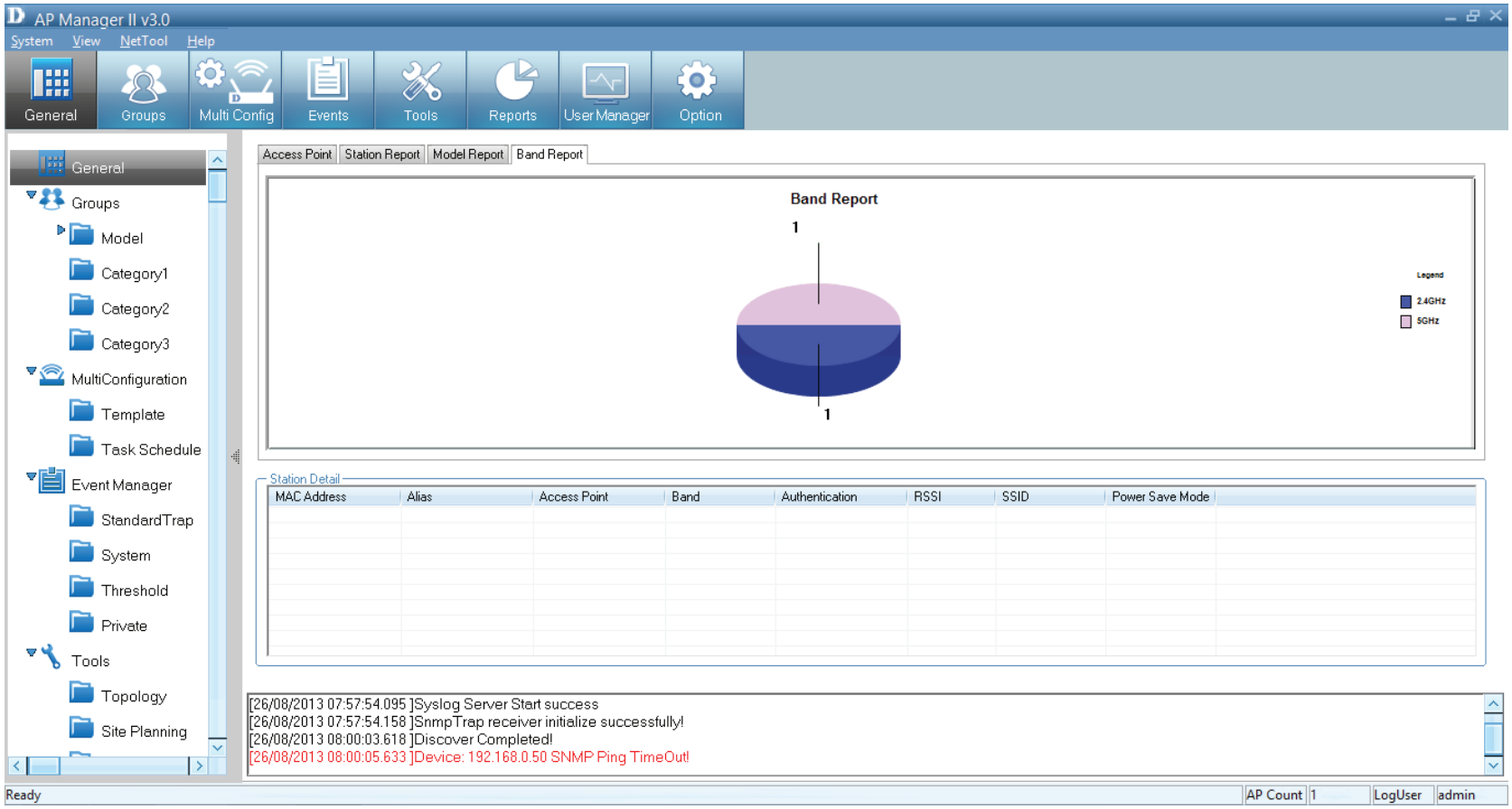
Model Report

The **Model Report** displays a graphical representation of the numerical distribution of models the AP Manager II has discovered and is currently managing.



Band Report

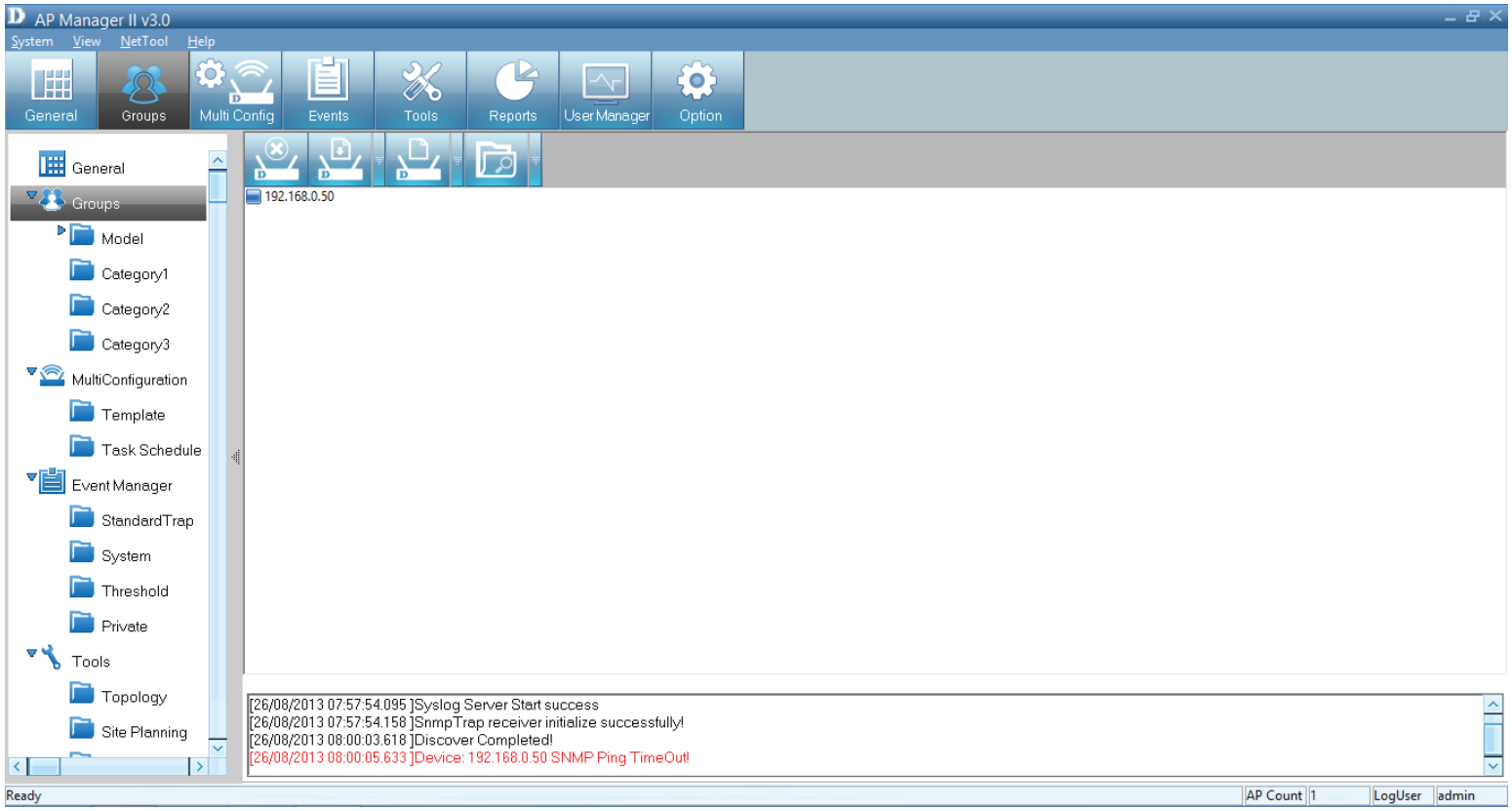
The **Band Report** displays a graphical representation of the 2.4GHz and 5GHz WLAN bands (802.11a, 802.11b/802.11g and 802.11b/g/n) currently being used by the Access Point. It shows the number Access Points on every band.



Group View

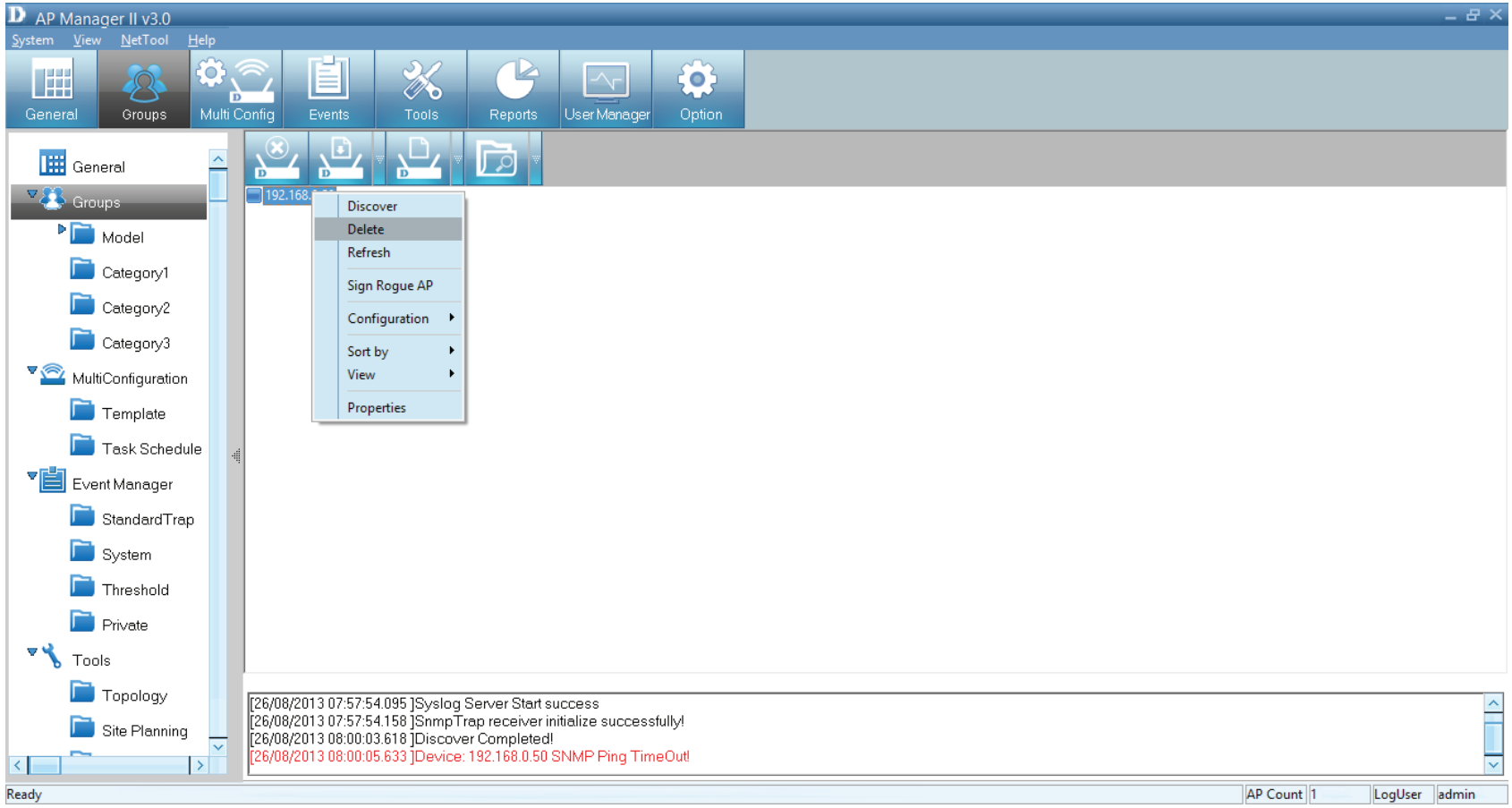
The **Group View Panel** displays the access points the AP Manager II v3.0 discovers and currently manages. You can group these access points by model or into categories that can make their distribution easier to visualize.

The AP Manager II v3.0 can actively monitor and manage several D-Link Access Points. They are installed as plug-ins under the installation directory. Add or remove supported model freely and once access points are detected during the discovery process, its listed in the main **Group View Panel**.



To **Delete** an access point.

Highlight it in **Group View** mode, right-click the access point, and select **Delete**.



Note: To view a list of supported access points, please go to the Frequently Asked Questions page at http://support.dlink.com/faq

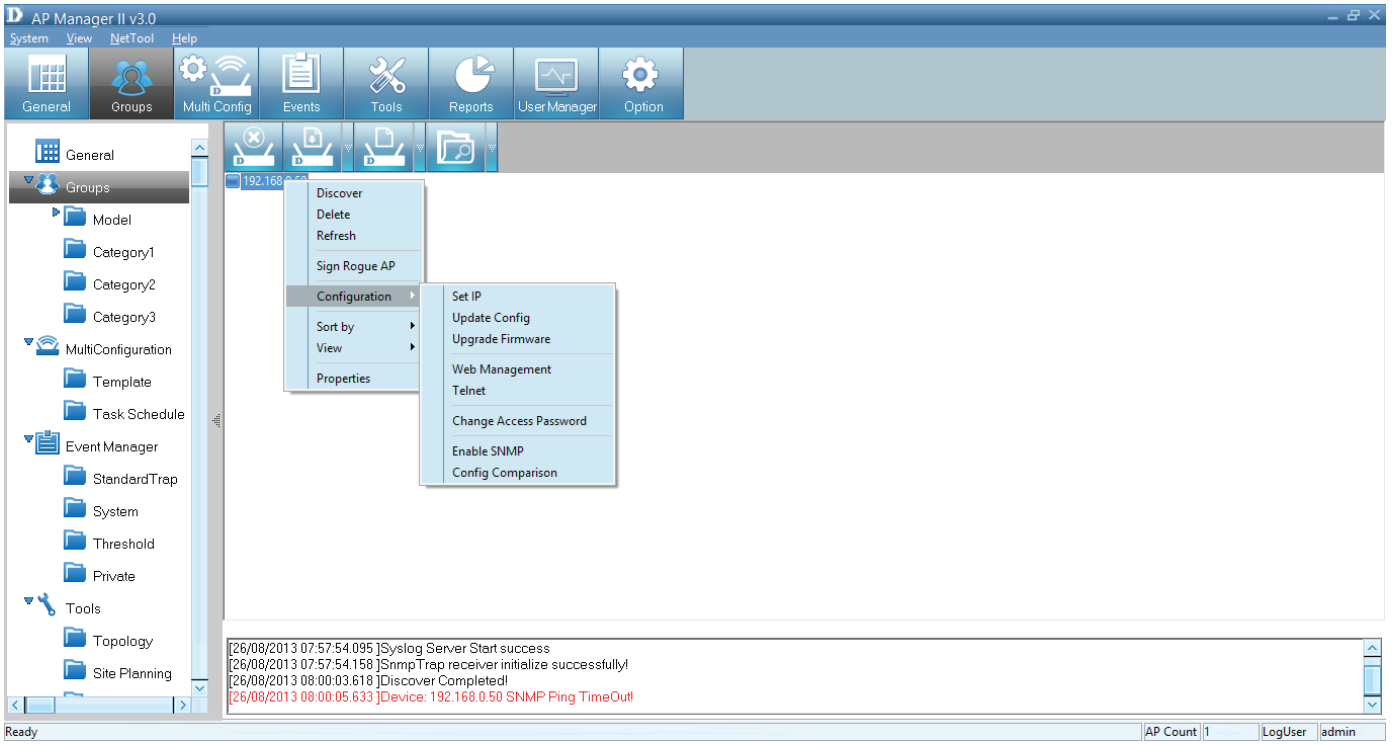
Group - Configuration

There are three main ways to configure an Access Point.

Right-click the **Access Point** and click **Configuration**. A new list of configurational options are available.

The options available from the drop-down menu are:

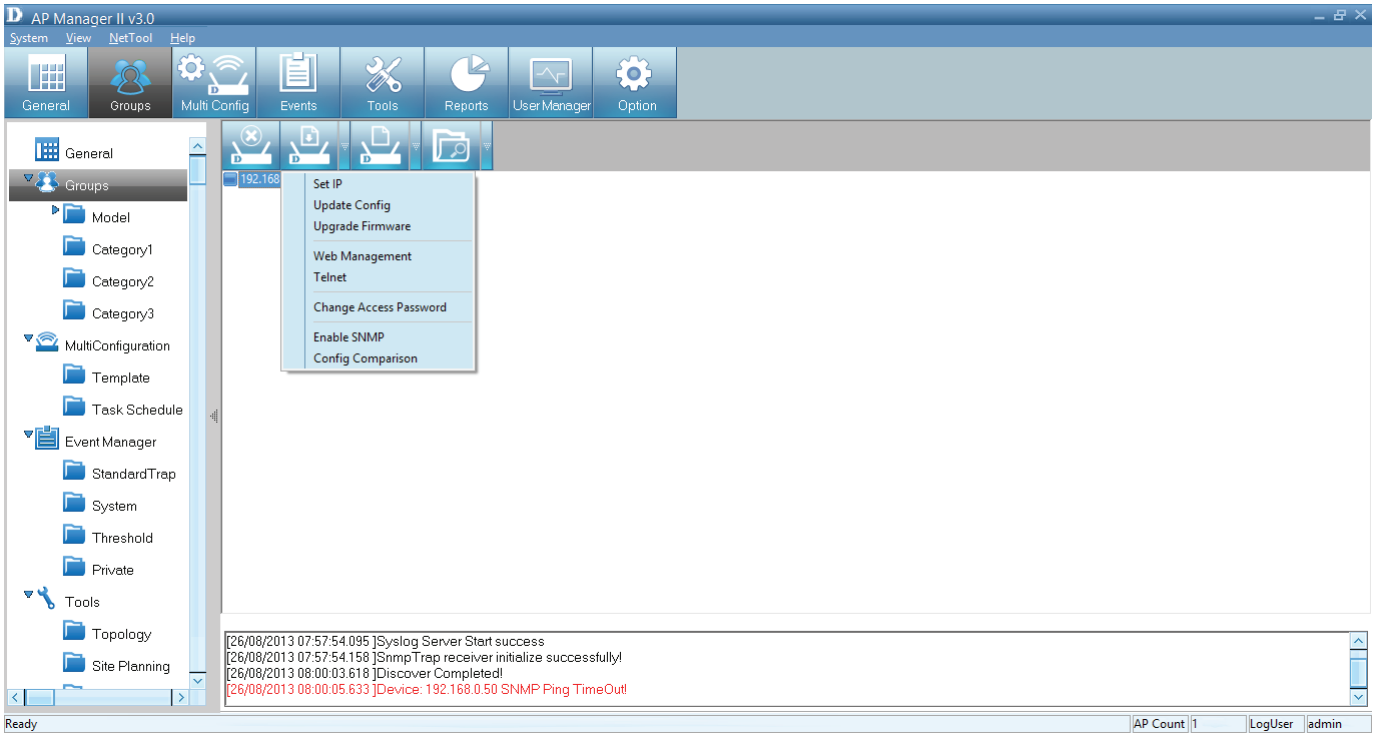
Set IP
Update Config
Upgrade Firmware
Web Management
Telnet
Change Access Password
Enable SNMP
Config Comparison



The second option is to click the arrow next to the **Configure** button.

Use this option to provide the same choices as done in the first selection.

Set IP
Update Config
Upgrade Firmware
Web Management
Telnet
Change Access Password
Enable SNMP
Config Comparison



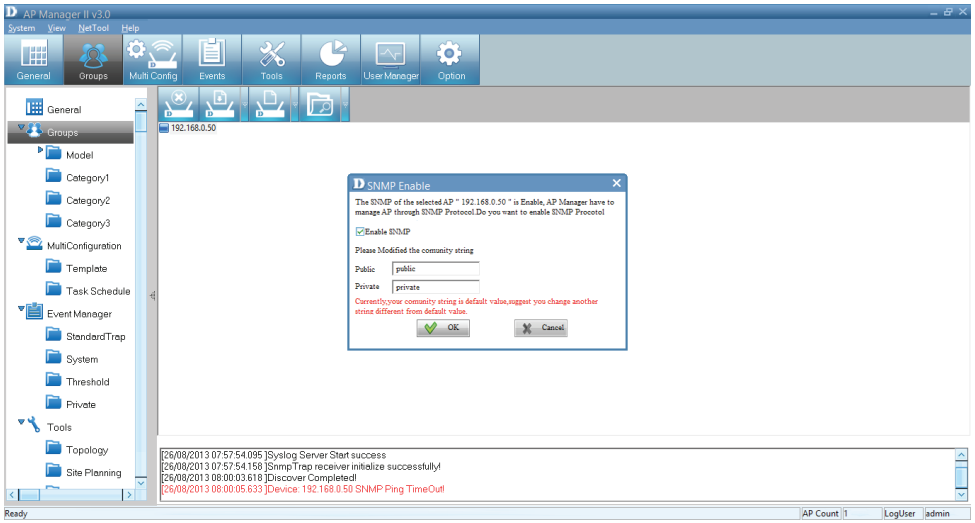
Group - Configuration - Set IP

You can manually set the IP Address of a selected Access Point.

To quickly access IP configuration tools, double-click the Access Point.

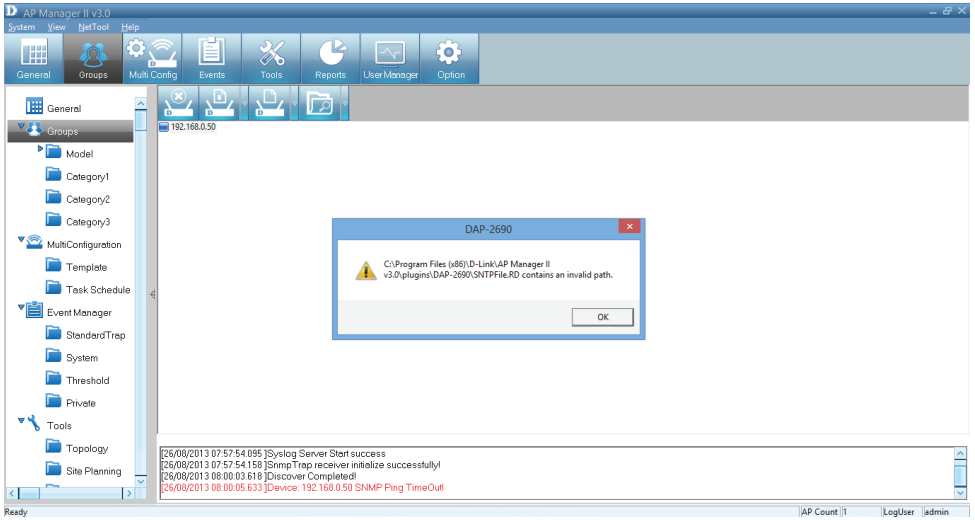
Set the **IP address**, **Subnet Mask**, and **Default Gateway**. Click **OK** to continue.

When a new Access Point is discovered, you can use this function to assign it a new IP address, Subnet Mask and Default Gateway to the device.



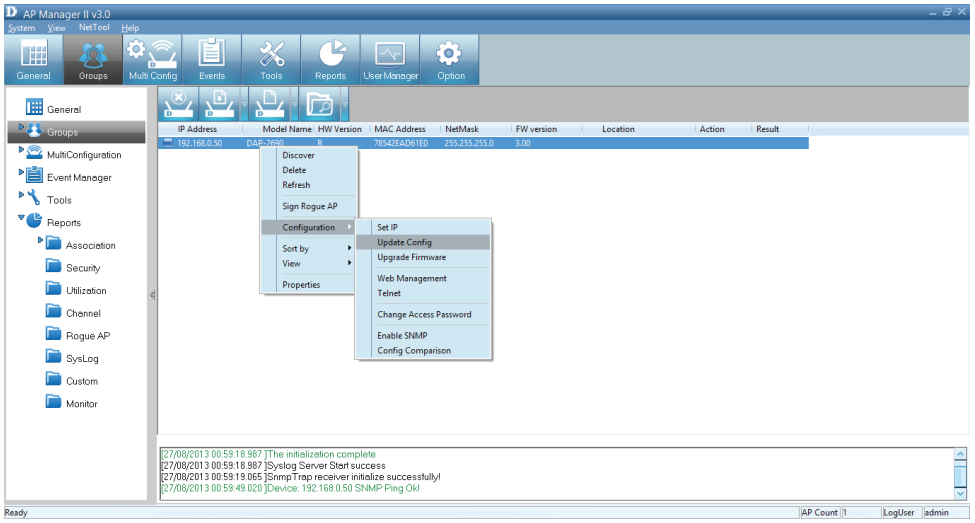
The Action column show the executing operation, while the Results column shows the progress by percentage. You can set the IP addresses of multiple devices this way. If the operation fails, please check the physical connections, and the username and password settings. (Refer to the Set Password section for details)

If you have entered the wrong IP information, you are prompted to re-enter new details. Click **OK** to try again.

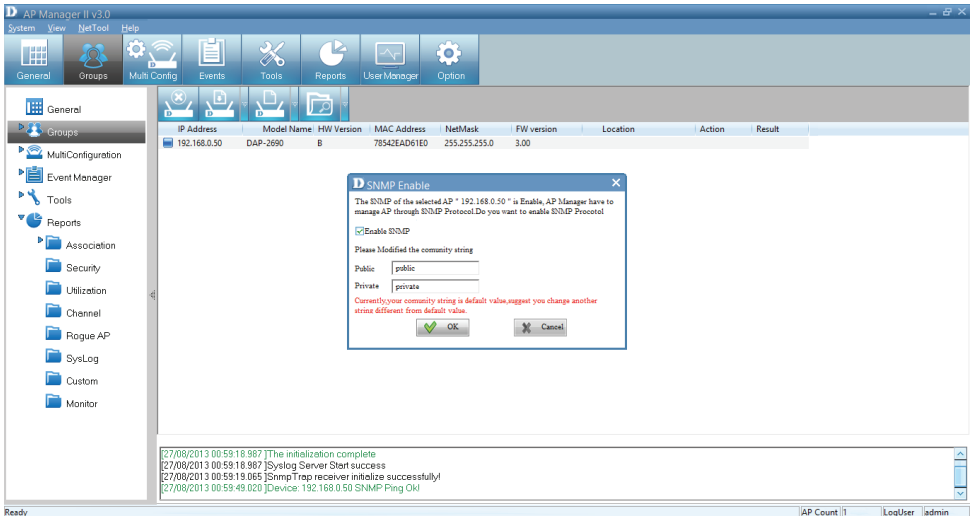


Group - Configuration Update

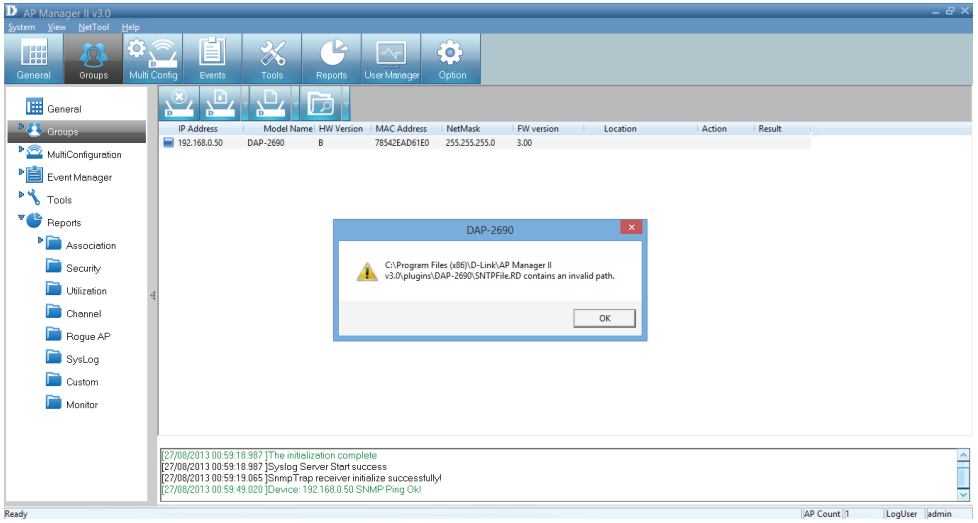
Right-click the device, go to **Configuration**, and click **Update Config**.



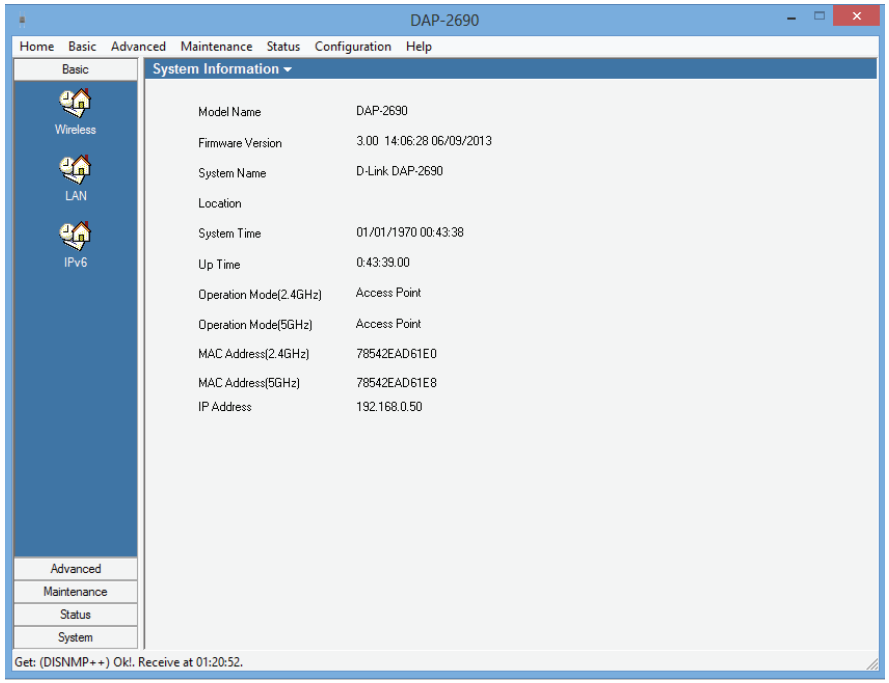
The **SNMP** preview window prompts you to **enable SNMP**. Click OK to continue.



If the original settings are not clear an invalid path notice will appear.

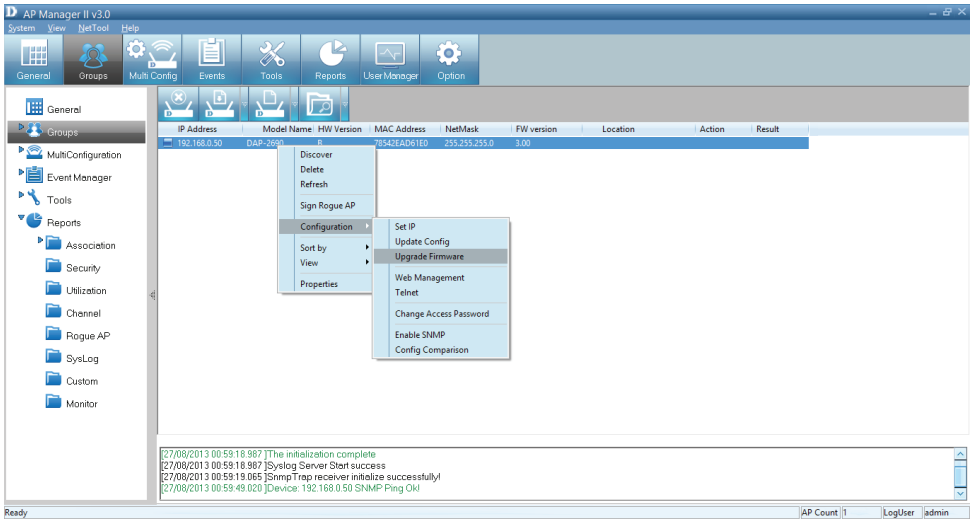


The program redirects you to the Access Point's configuration tools.

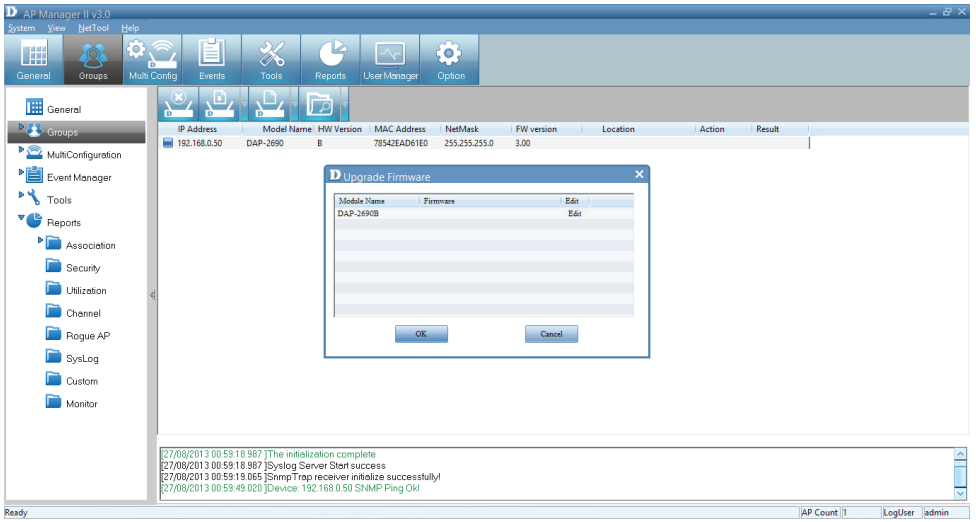


Configuration - Firmware Upgrade

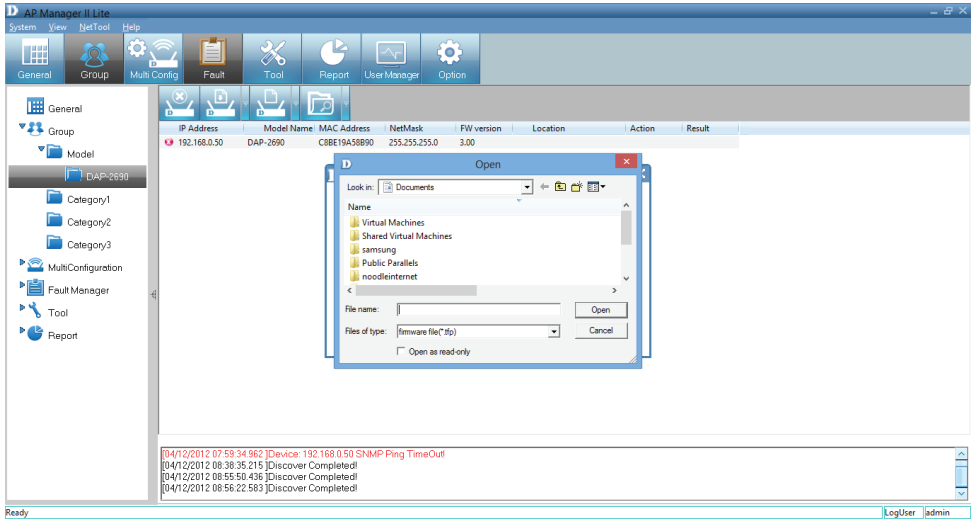
Right-click the device, go to **Configuration**, and click **Upgrade Firmware**.



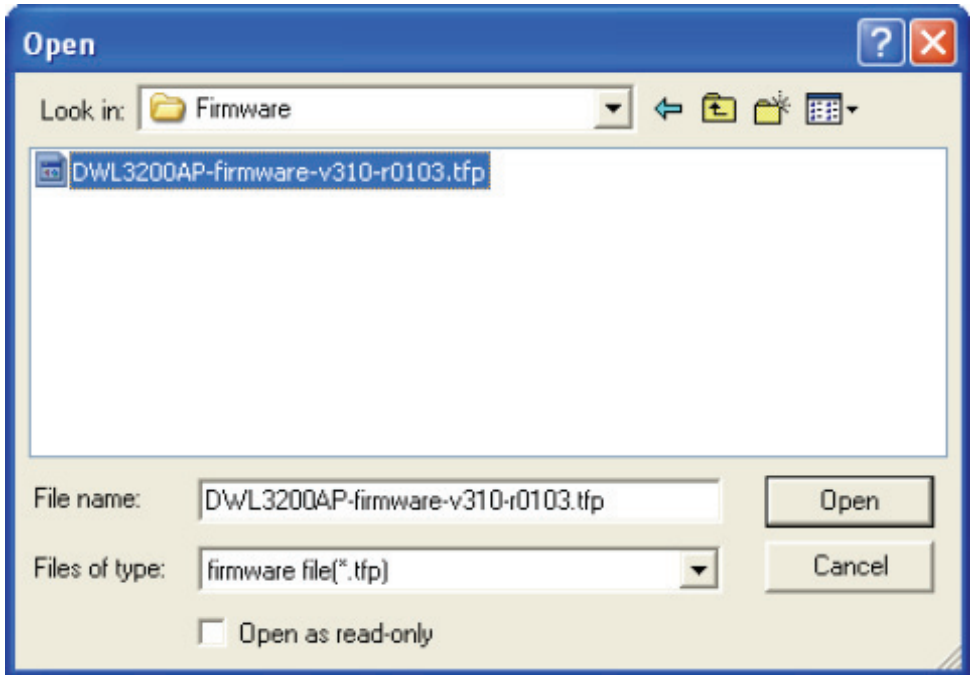
The **Upgrade Firmware** configuration window opens.



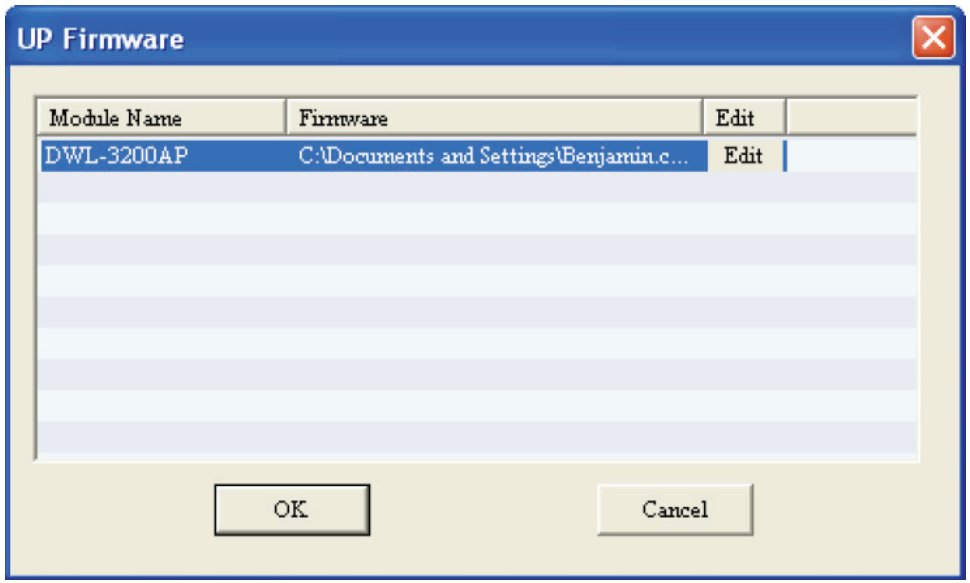
Select the Access Point's firmware you wish to upgrade. Click the **Edit** field. A new window opens prompting you to search for the new firmware on your PC.



Once you have located the firmware, select it and click **Open**.

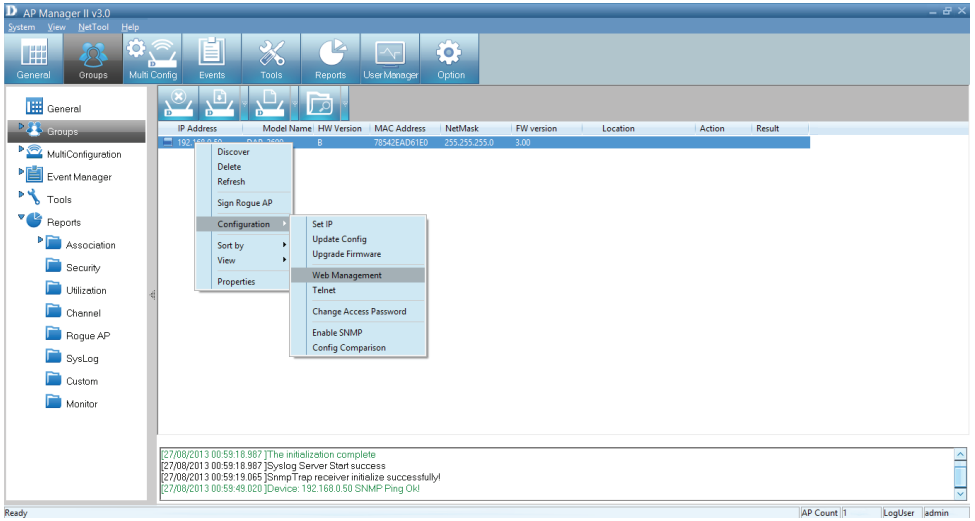


Upload the firmware to the Access Point. Click **OK** to continue.

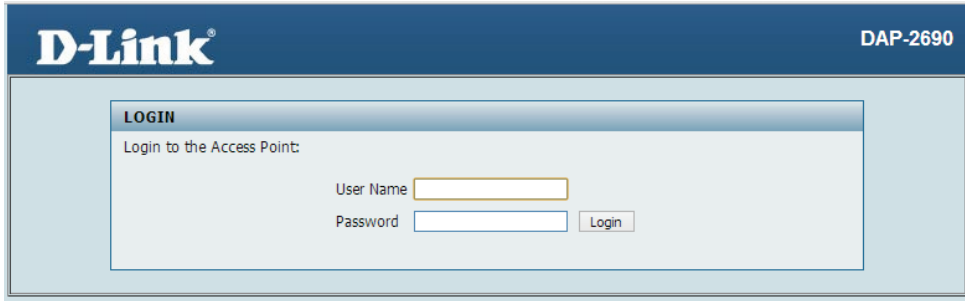


Configuration - Web Management

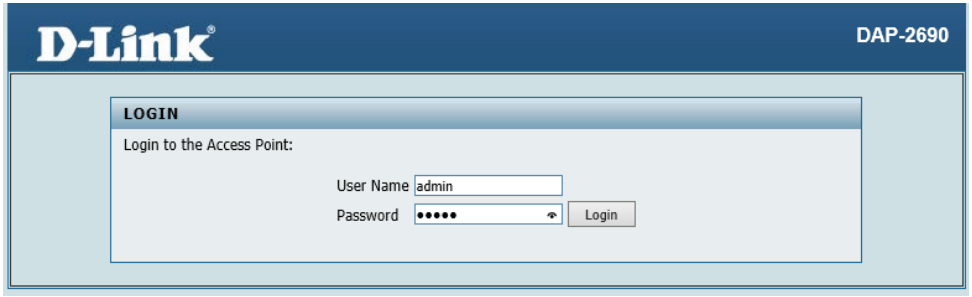
Right-click the device, go to **Configuration**, and click **Web Management**.



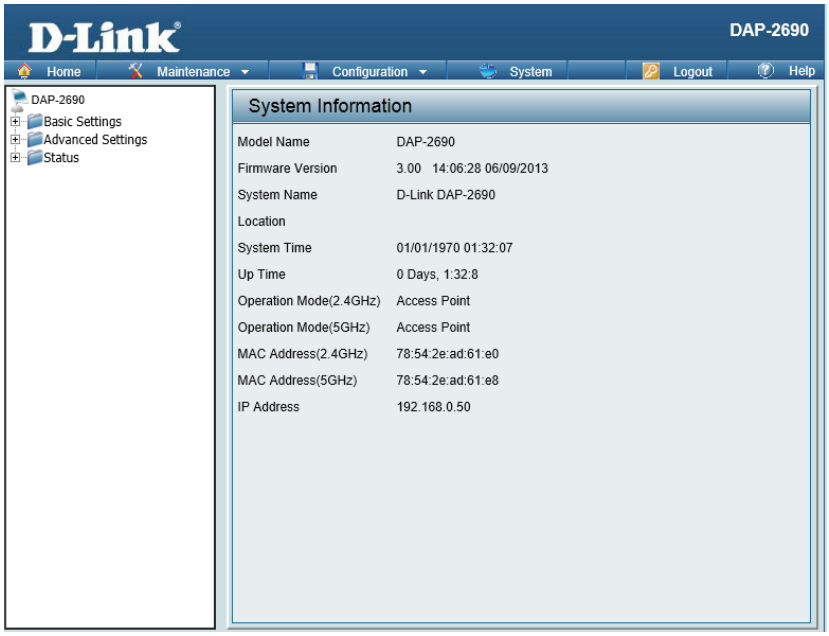
Enter a User name and Password into the fields provided and click OK. Your PC's web browser will open and the Access Point's IP address will be entered into the address field. You can configure the Access Point using its built-in web-based manager as you would normally.



Enter the Username and Password details.

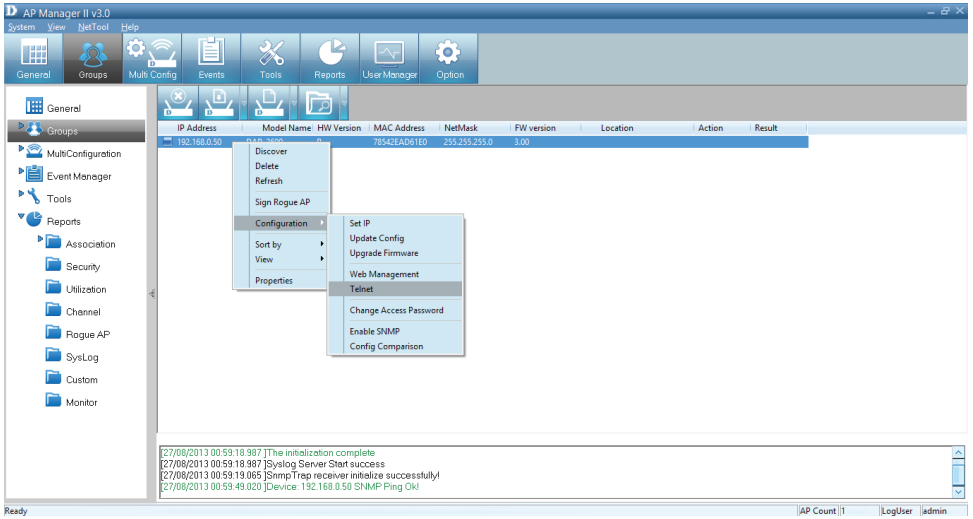


This launches the browser interface.

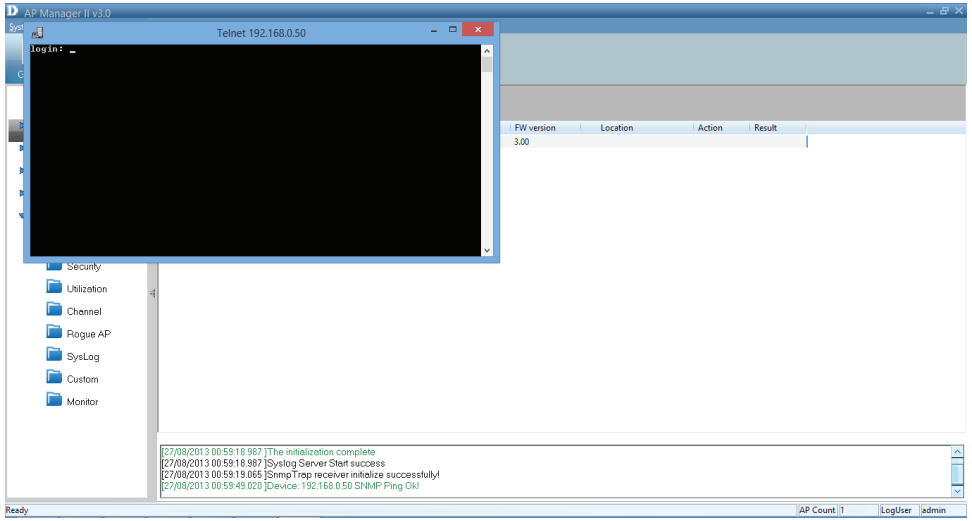


Configuration - Telnet

Right-click the device, go to **Configuration**, and click **Telnet**.

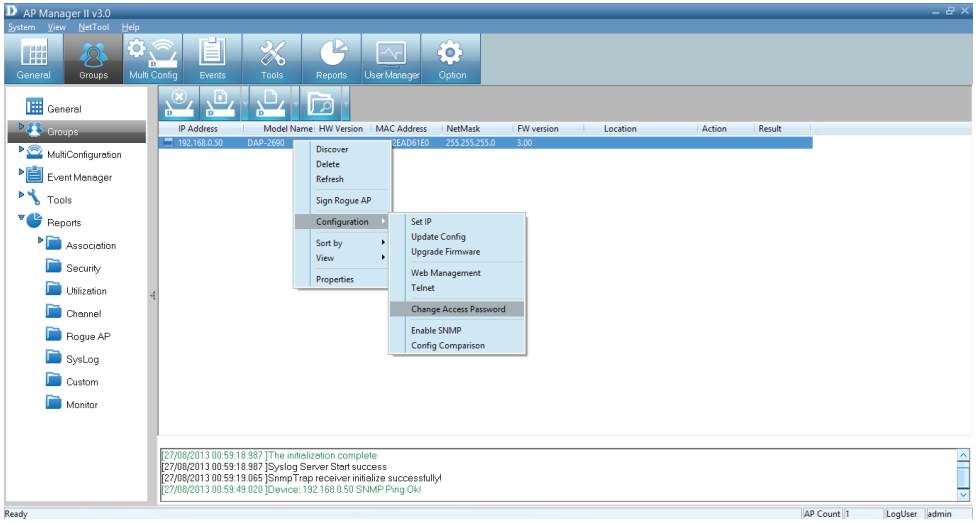


Once you have clicked Telnet, it opens the Command Prompt. This gives you access to the built-in Telnet CLI Manager. Type in the Username and Password in the console manager.

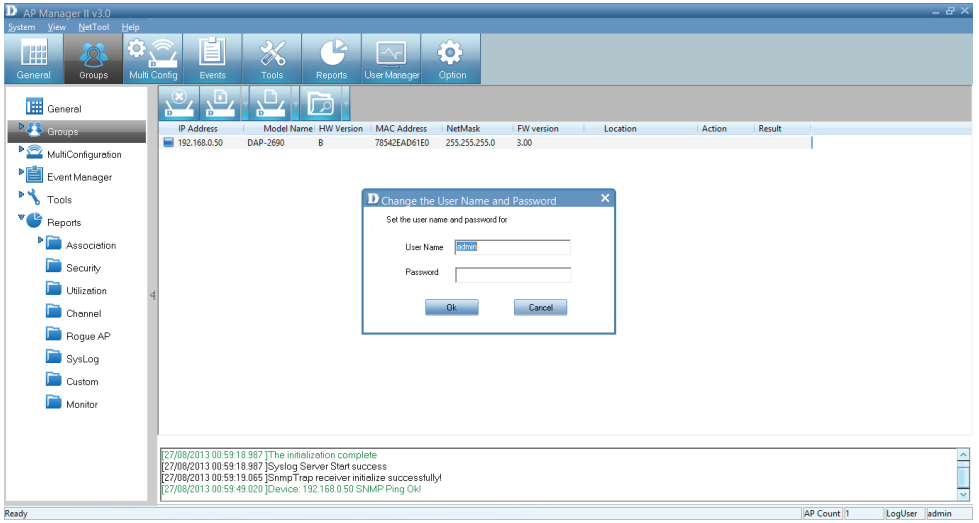


Configuration - Change Access Password

Right-click the device, go to **Configuration**, and click **Change Access Password**.

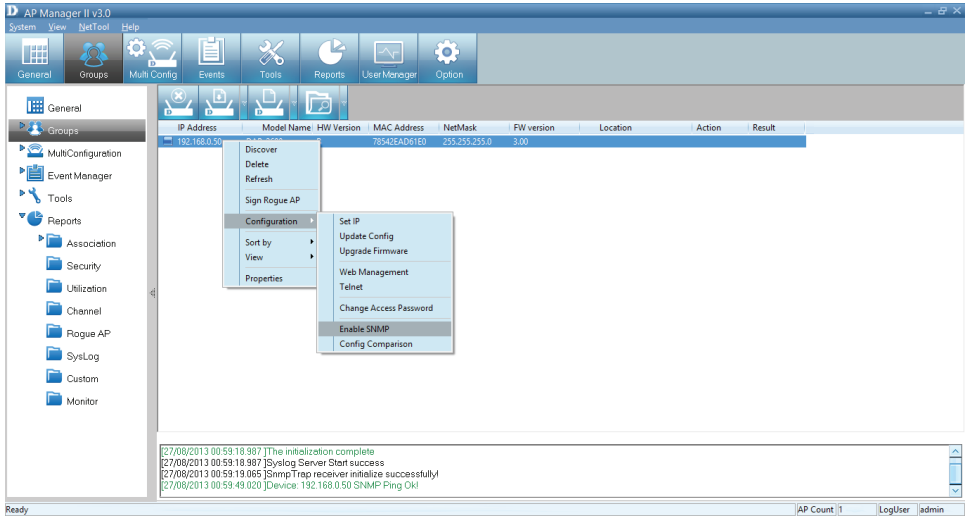


The **Change Username and Password** window asks you to enter the new **Username and Password** details. Click **OK** when complete to continue.

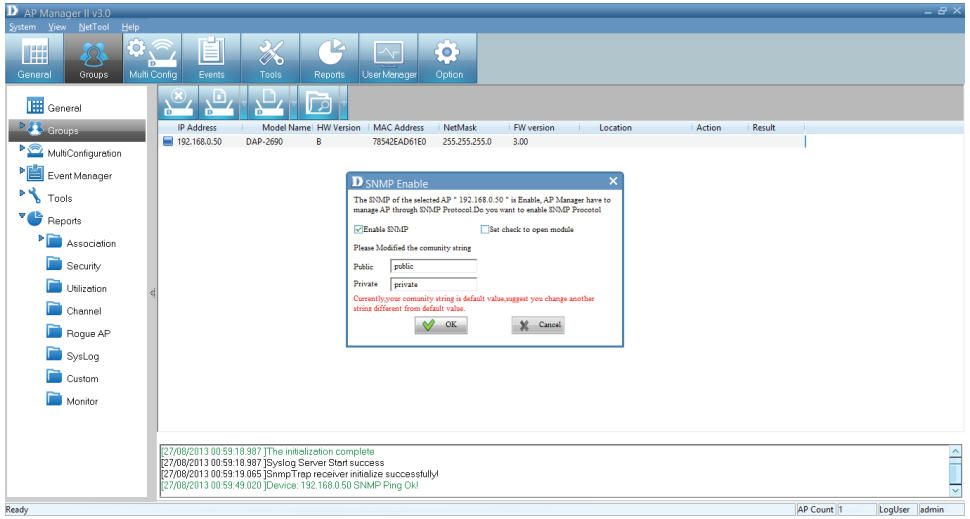


Configuration - Enable SNMP

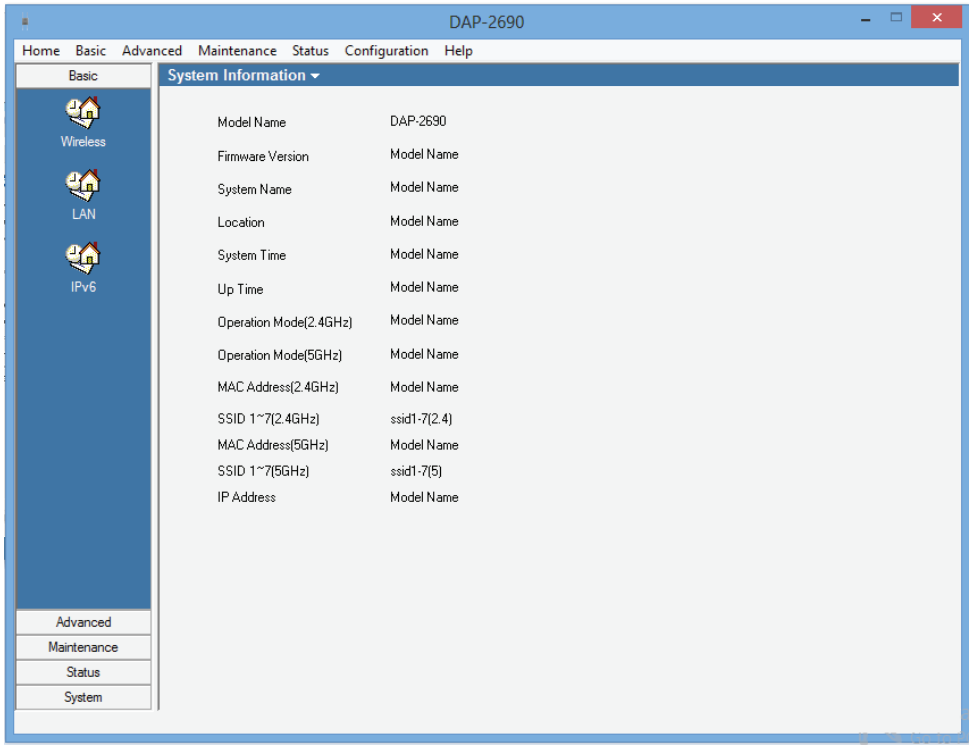
Right-click the device, go to **Configuration**, and click **Enable SNMP**.



Under the **SNMP Enable Manager**, click the checkbox to **Enable SNMP**. Click the **Set check to open module** checkbox if you need this application. Enter the **Public** and **Private** data in the fields provided and click **OK** to complete.



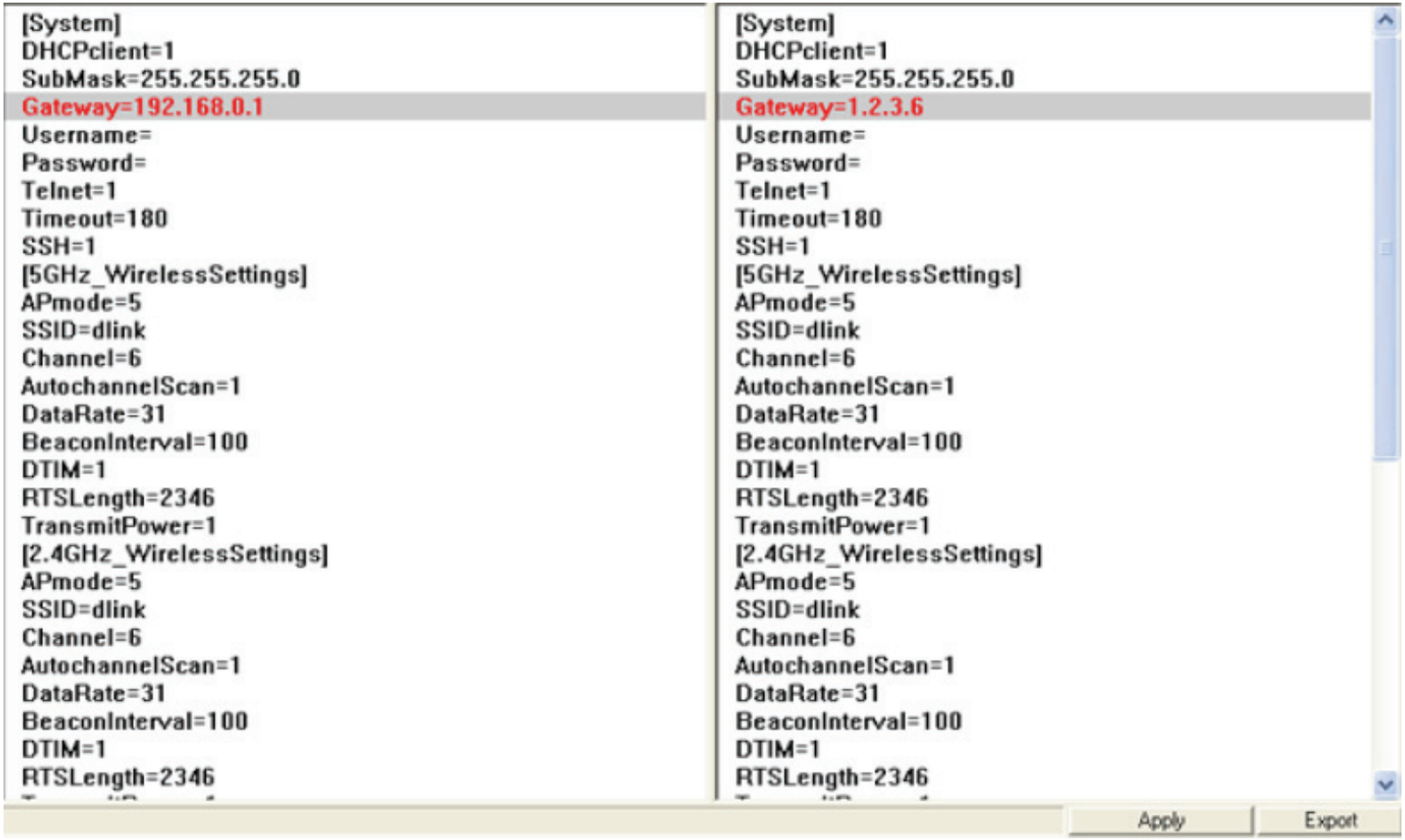
The D-Link Manager software opens and you can configure it using this tool.



Configuration - Configuration Comparison

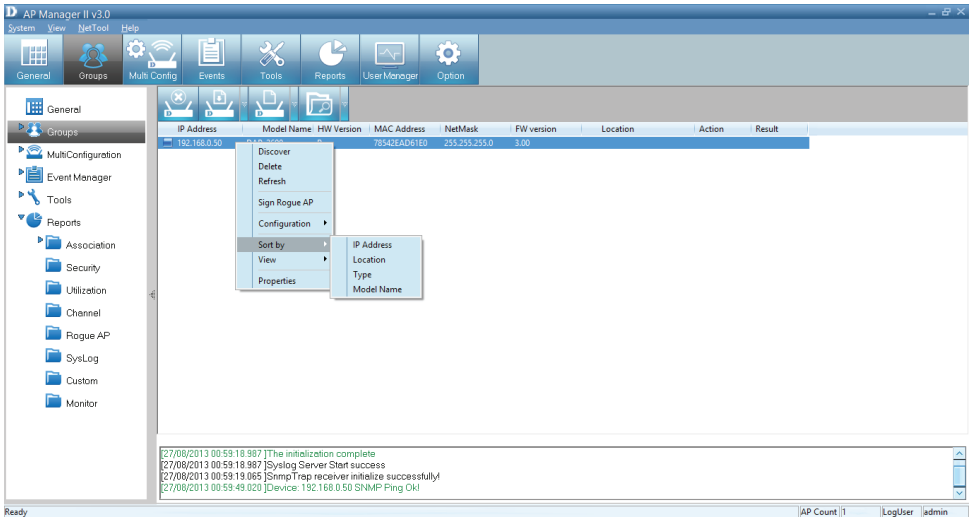
Right-click the device, go to **Configuration**, and click **Config Comparison**.

Config Comparison needs two Access Points to work. Compare each configuration option against the other Access Point. Click **Apply** to continue.



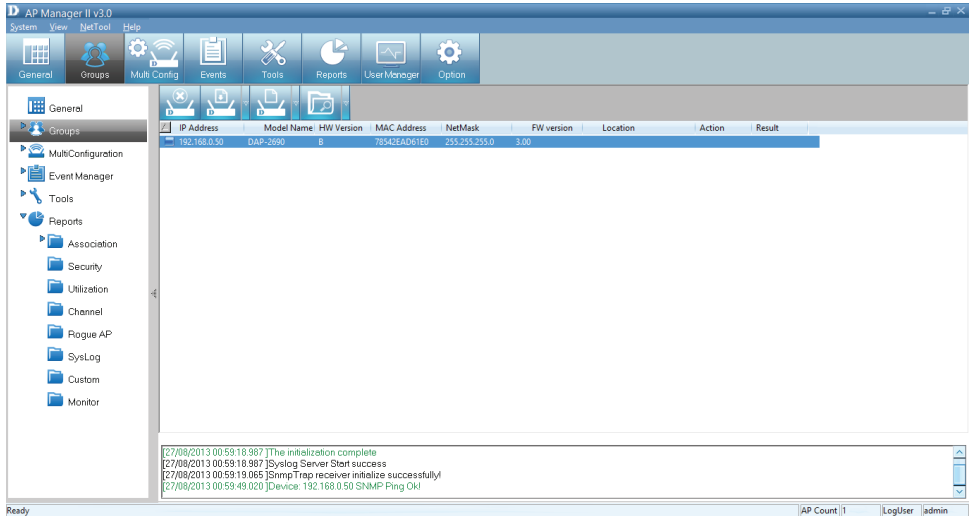
Sorting

Right-click the device, go to **Sort By**



You can change the order of the **Access Points** by **IP Address**, **Location**, **Type**, and **Model Name**.

Once you have selected the sorting option, a **grey arrow** is placed beside it to represent its designation.

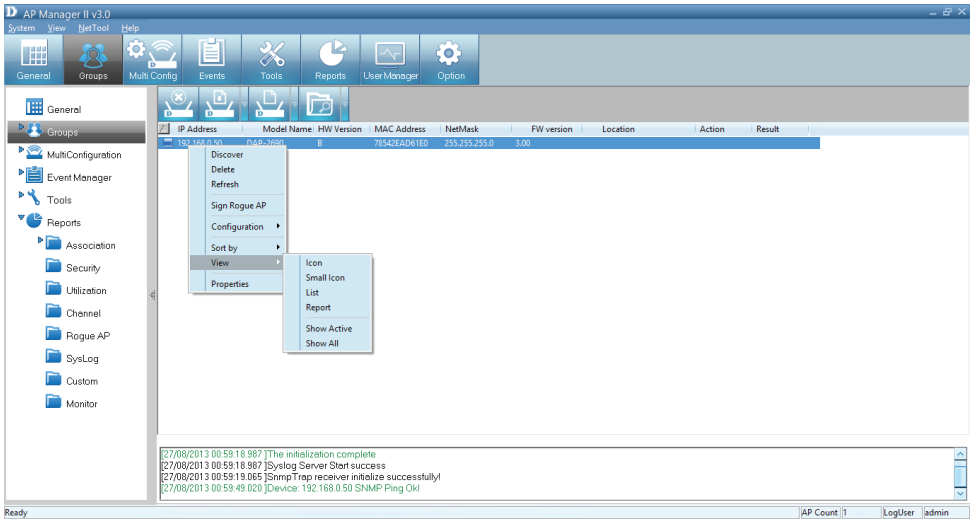


IP Address: Sorts by IP Address column
Location: Sorts by Location column
Type: Sorts by either Managed, Unmanaged or Rogue Access Point.
Model Name: Sorts by Access Point model name.

View Mode

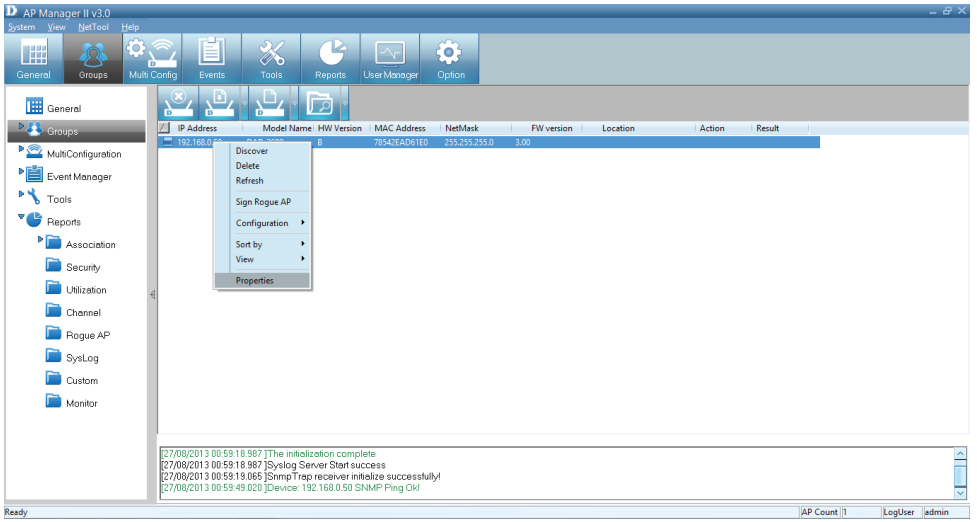
Right-click the device, go to **View**

You can **view** the Access Points based on different parameters. The options are: **Icon**, **Small Icon**, **List, Report**, **Show Active**, and **Show All**.

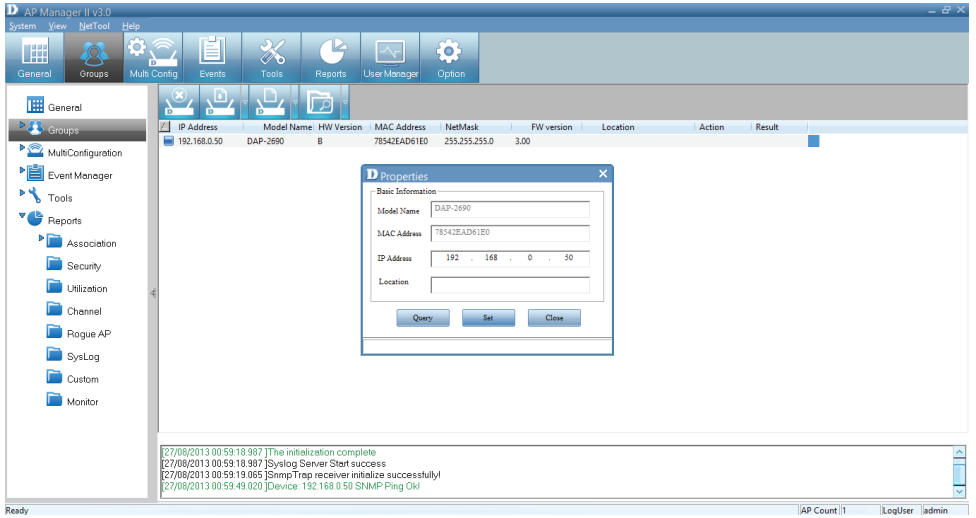


Properties

Right-click the device, go to **Properties**

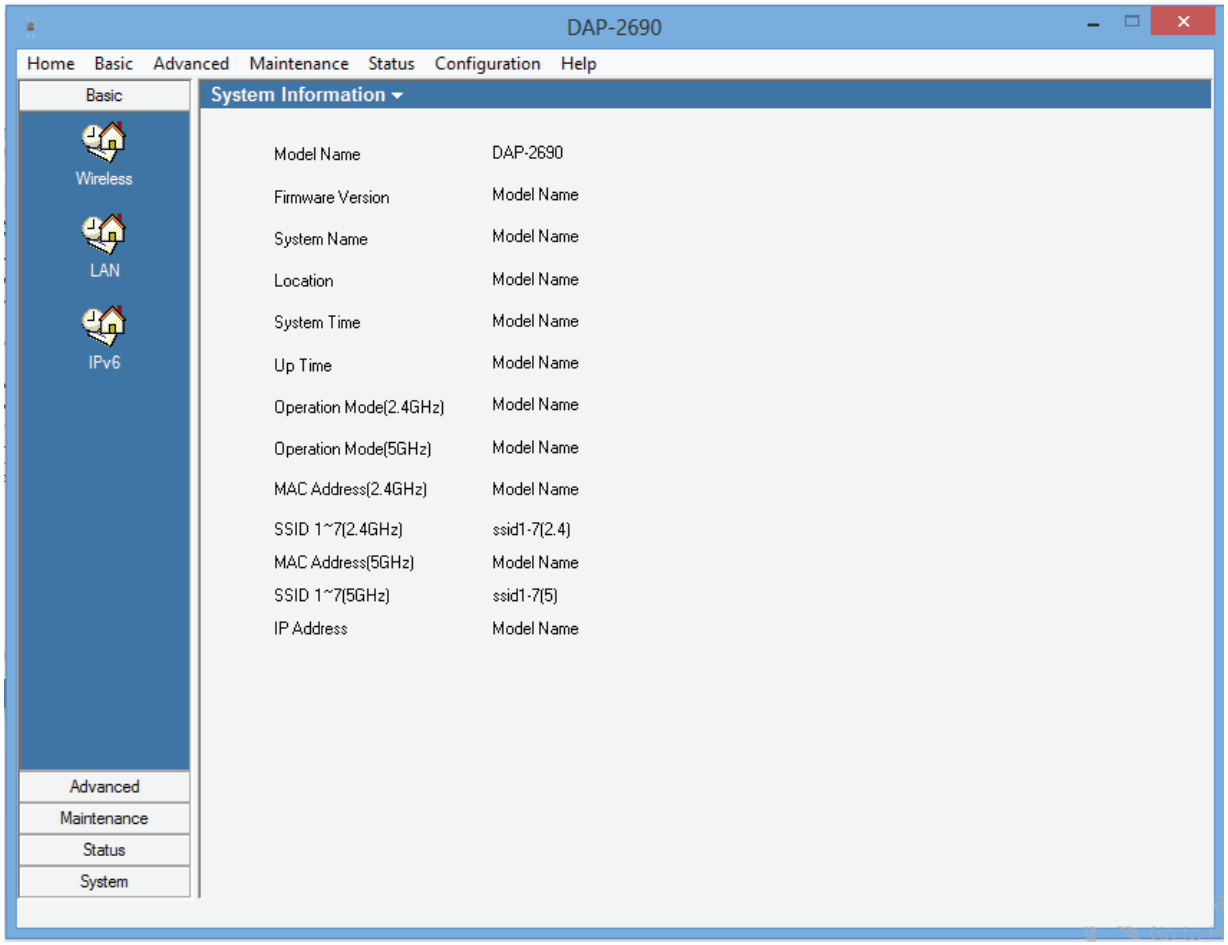


You can enter a description string in the **Location** textbox to describe the Access Point and then click the **Set** button to apply the changes.



The Access Point Manager II v3.0

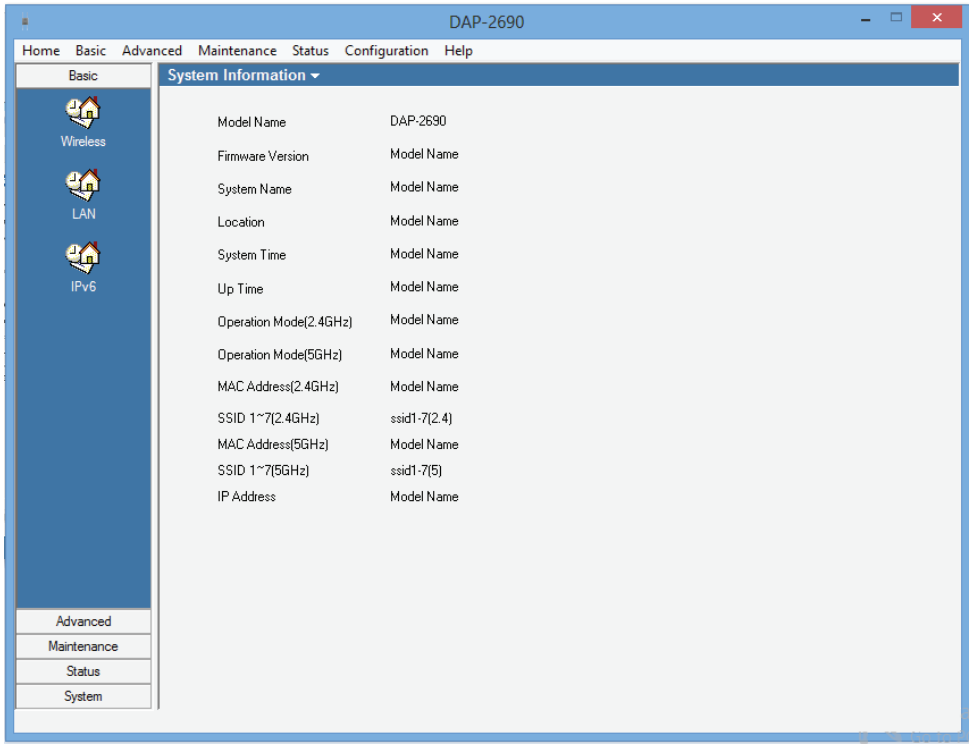
The Access Point Manager is the main tool used to configure each Access Point. Users can save and load configuration files. When the files are loaded, you must click Apply if you want the settings to be applied to the selected device(s).



Navigate any Access Point configuration using the menu on the left side of the window. This menu contains the following sections: **Basic**, **Advanced**, **Maintenance**, **Status**, and **System**. These sections and their menus will be discussed in detail in the following pages.

The Home Panel

The Home > System Information page contains basic configuration information about the Access Point being configured. The information available are:

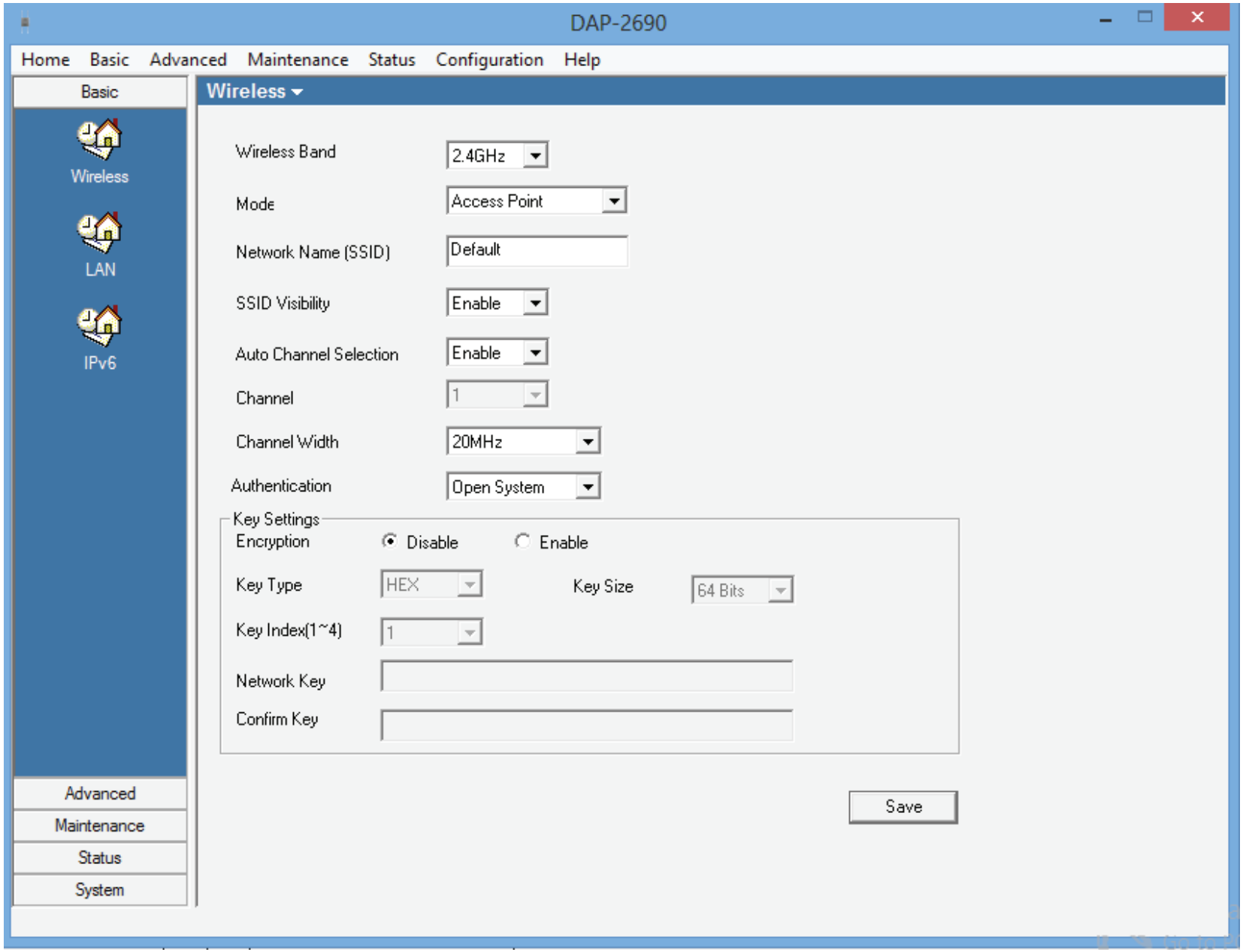


Model Name
Firmware Version
System Name
Location
System Time
Up Time
Operation Mode (2.4GHz)
Operation Mode (5GHz)
MAC Address (2.4GHz)
SSID 1~7 (2.4GHz)
MAC Address (5GHz)
SSID 1~7 (5GHz)
IP Address

There will be minor differences when using AP Manager II with a single band AP and a dual band AP.

This manual refernces both 802.11g and 802.11n configuration settings.

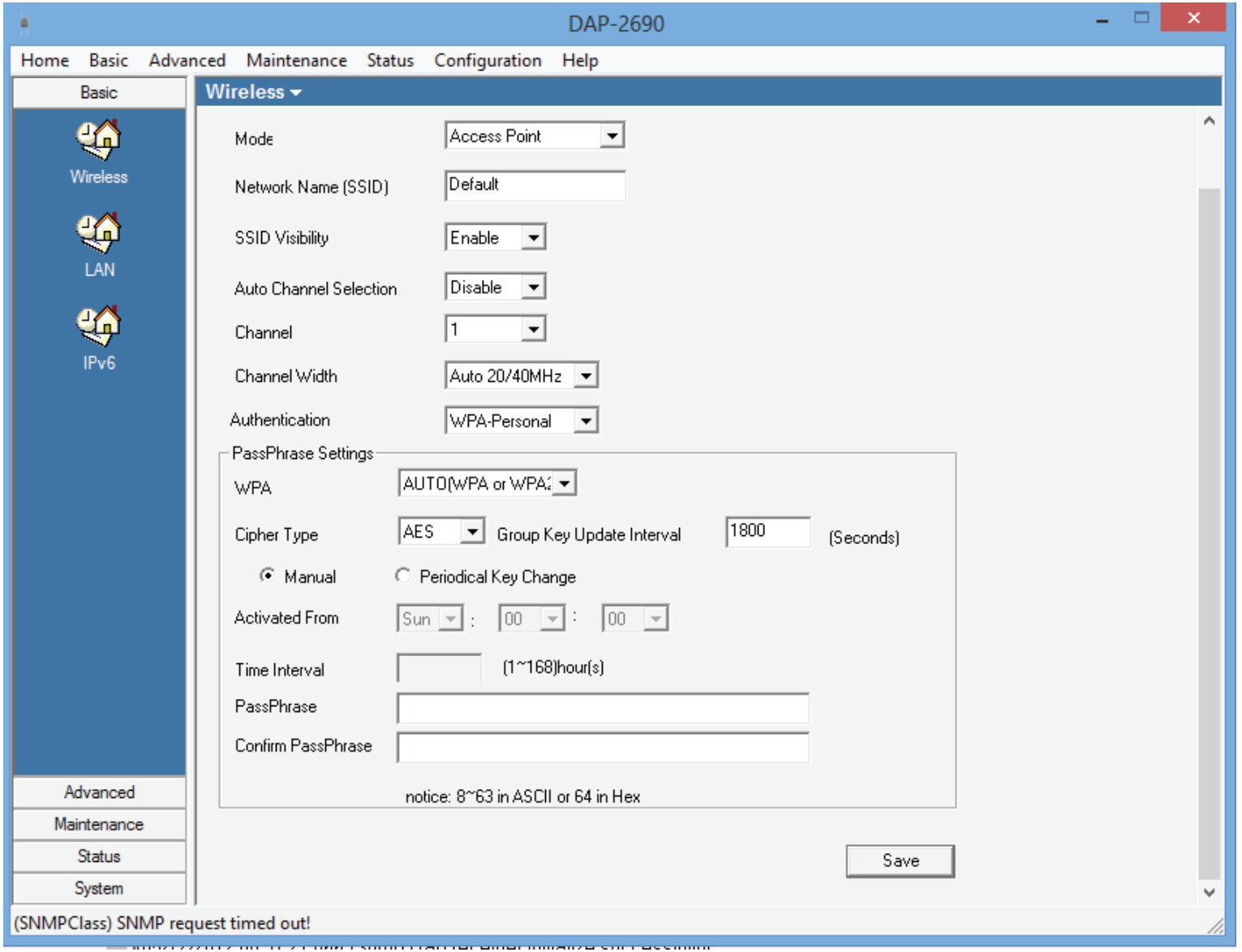
Basic - Wireless



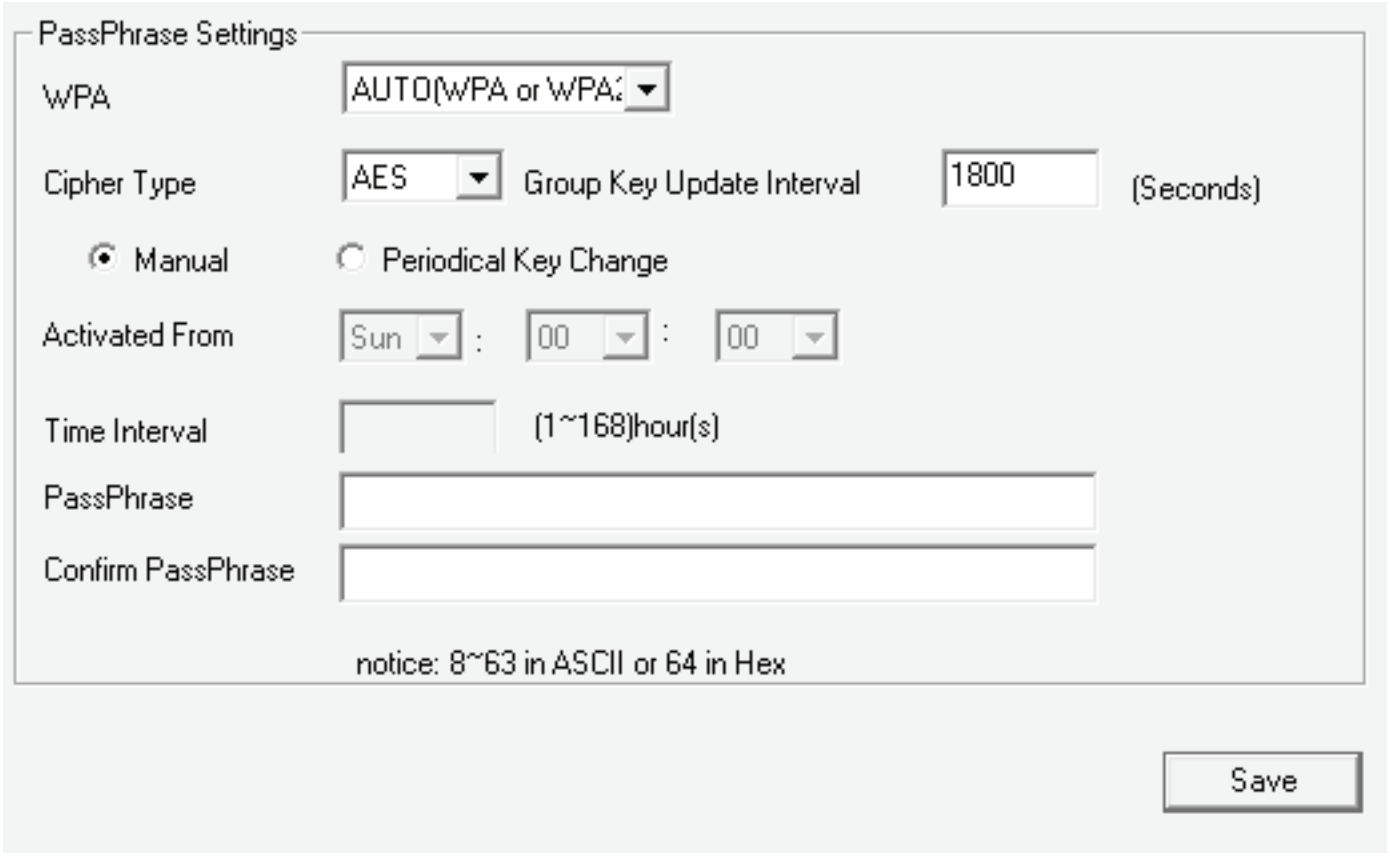
COMPONENT	DESCRIPTION
Wireless Band	Select between 2.4GHz or 5GHz frequency
Mode	Select the Wireless mode. Options include, Access Point, WDS with AP, WDS, and Wireless Client
Network Name (SSID)	The Service Set (network) Identifier of your wireless network
SSID Visibility	Enable to allow others to see it or select Disable to make it invisible to others
Auto Channel Selection	Select Enable for it to be auto select. Select Disable to manually select channels
Channel	Select between 1-3 Allows you to select a channel or set the Access Point to auto scan channels. 802.11g may not be set manually in certain regions (e.g. Europe and USA) in order to comply with DFS (Dynamic Frequency Selection) regulations.
Channel Width	Select the frequency range 20MHz or Auto 20/40MHz
Authentication	Select the security method: Open System, Shared Key, WPA-Personal, WPA-Enterprise, and 802.1x Select Open System/Shared Key to allow either form of data encryption. Select WPA-Enterprise to secure your network with the inclusion of a RADIUS server. Select WPA-Personal to secure your network using a password and dynamic key changes. (No RADIUS server required.) Select WPA2-Enterprise to secure your network with the inclusion of a RADIUS server and upgrade the encryption of data with the Advanced Encryption Standard (AES). Select WPA2-Personal to secure your network using a password and dynamic key. No RADIUS server is required and encryption of data is upgraded with the Advanced Encryption Standard (AES). Select WPA-Auto-Enterprise to allow the client to either use WPA-Enterprise or WPA2-Enterprise. Select WPA-Auto-Personal to allow the client to either use WPA-Personal or WPA2-Personal.
Key Settings Encryption	Select Disable or Enable
Key Type	When enabled, select between ASCII and HEX and the key size either 64bit or 128bit
Key Index (1-4)	Select between 1-4
Network Key	Ask your administrator about this or type in the details provided in the field
Confirm Key	Repeat the details as entered above
Save	Click this button to save your work

WIRELESS - AUTHENTICATION

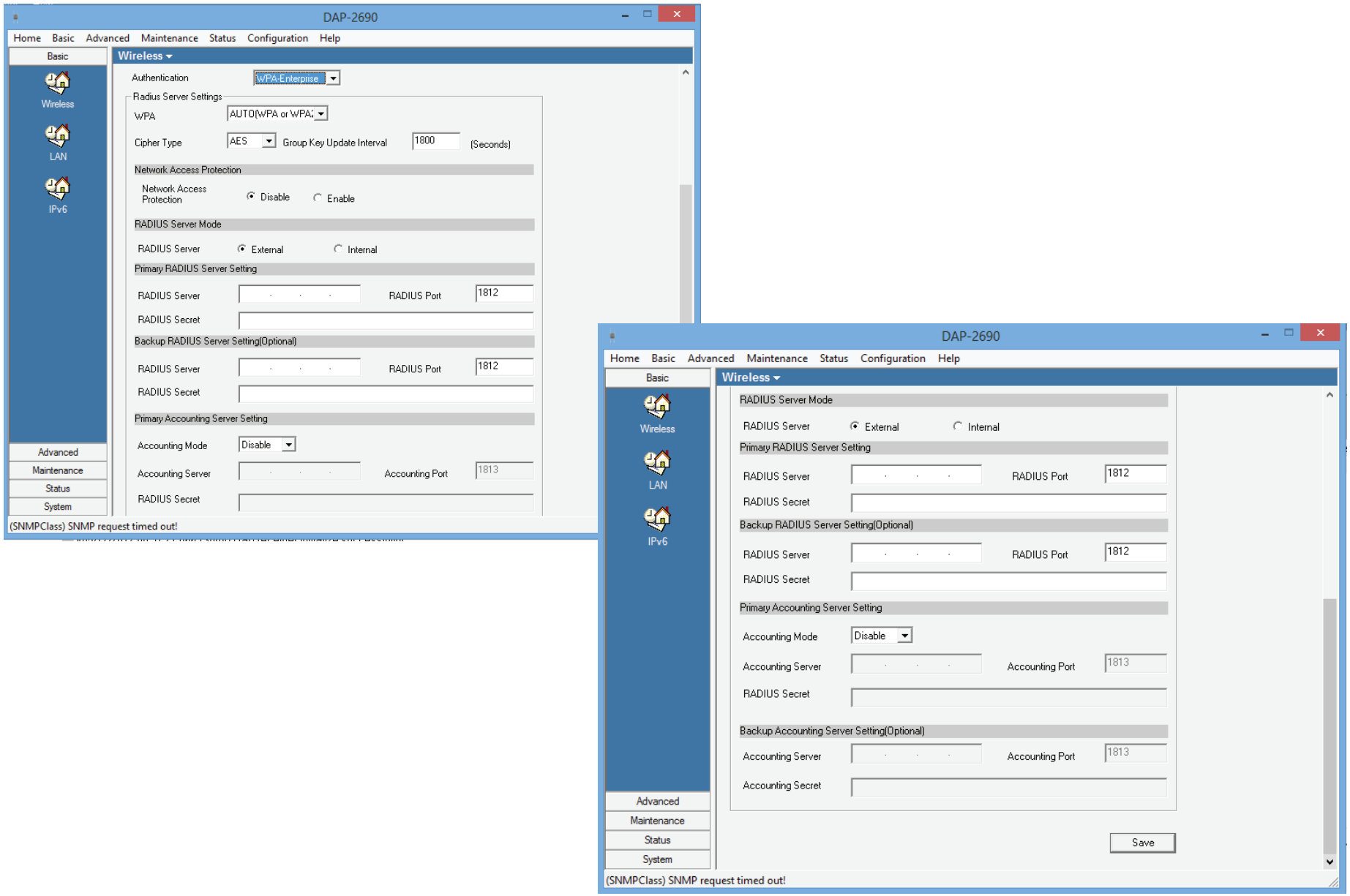
If one changes the Authentication method under Wireless, one would notice, that when you switch between methods the window below changes. Toggle between different network authentication methods to determine your settings. For WPA-Personal, the image below shows the options available.



COMPONENT	DESCRIPTION
PassPhrase Settings	Toggle between Auto (WPA or WPA2), WPA2 only and WPA only.
Cipher Type	Select Auto, TKIP, or AES from the drop-down menu
Group Key Update Interval	Select the interval validity. 1800 is the recommended setting. A lower interval may reduce transfer rates.
Passphrase	Enter a PassPhrase between 8-63 characters in length.



WPA-ENTERPRISE

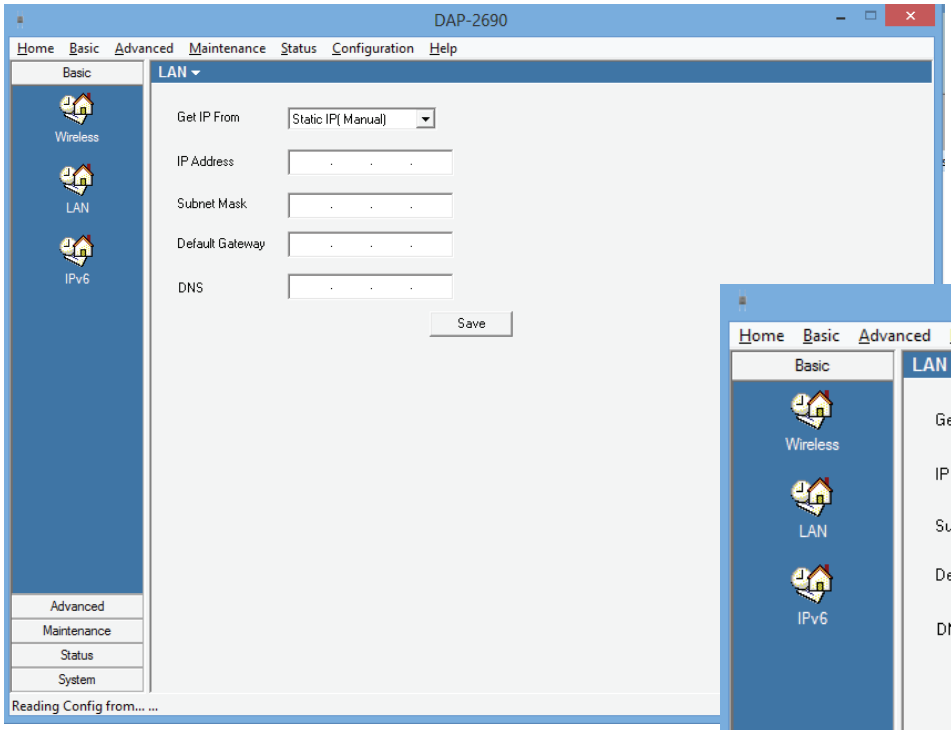


WPA-ENTERPRISE

COMPONENT	DESCRIPTION
WPA	Toggle between Auto (WPA or WPA2), WPA2 only and WPA only.
Cipher Type	AES
Group Key Update Interval	Select the interval validity. 1800 is the recommended setting. A lower interval may reduce transfer rates.
Network Access Protection	Select to Enable or Disable this function
Radius Server Mode	RADIUS Server - Select External or Internal
Primary RADIUS Server Settings	Enter the IP address of the RADIUS server
RADIUS Port	Enter the port used on the RADIUS server
RADIUS Secret:	Enter the RADIUS secret.
Accounting Mode	Click to Enable or Disable
Accounting Server:	Enter the IP address of the Accounting server.
Accounting Port:	Enter the port used on the Accounting server.
Backup Accounting Server Settings	Accounting Server, Accounting Port, and Accounting Secret

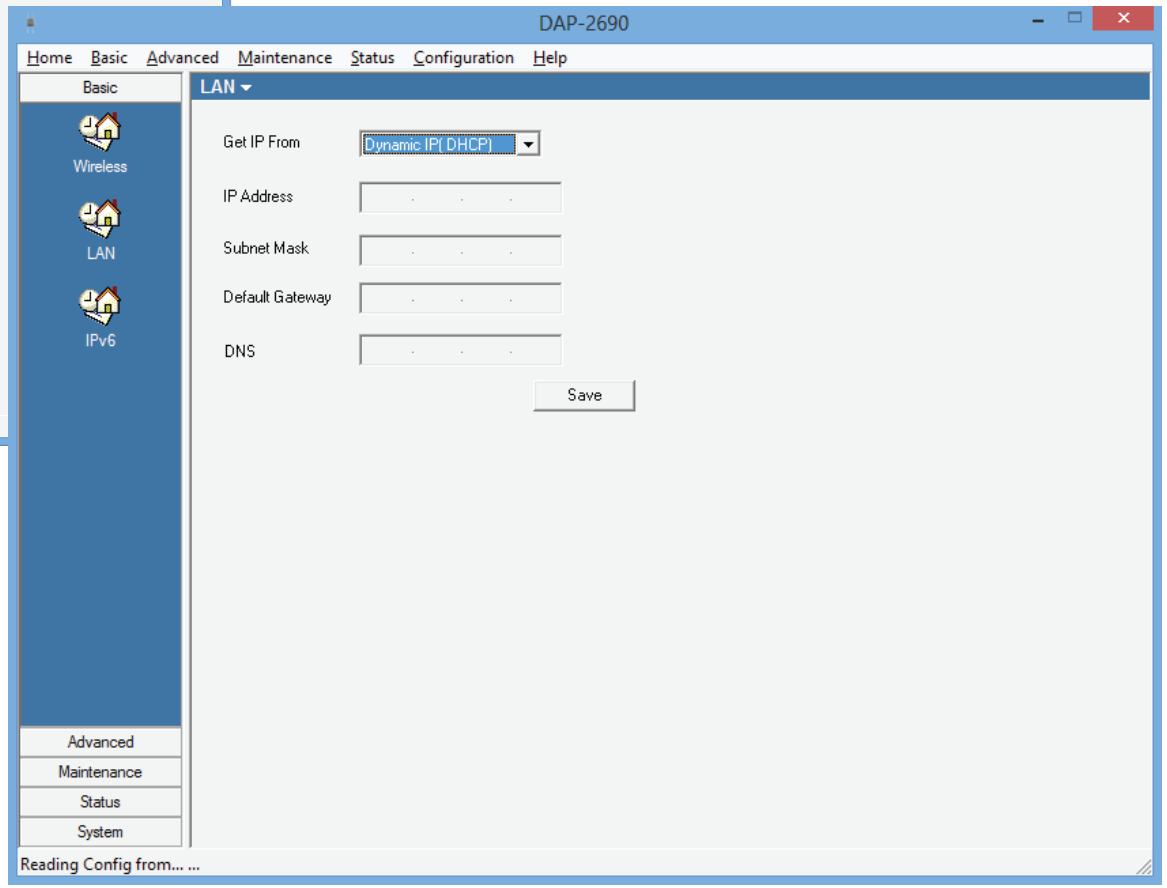
Basic - LAN

Connect your Access Point to a LAN connection with Static IP or Dynamic IP. With Static you will need to enter the details manually. Whereas with Dynamic, setting IP's are automatic, assigned by your default router.



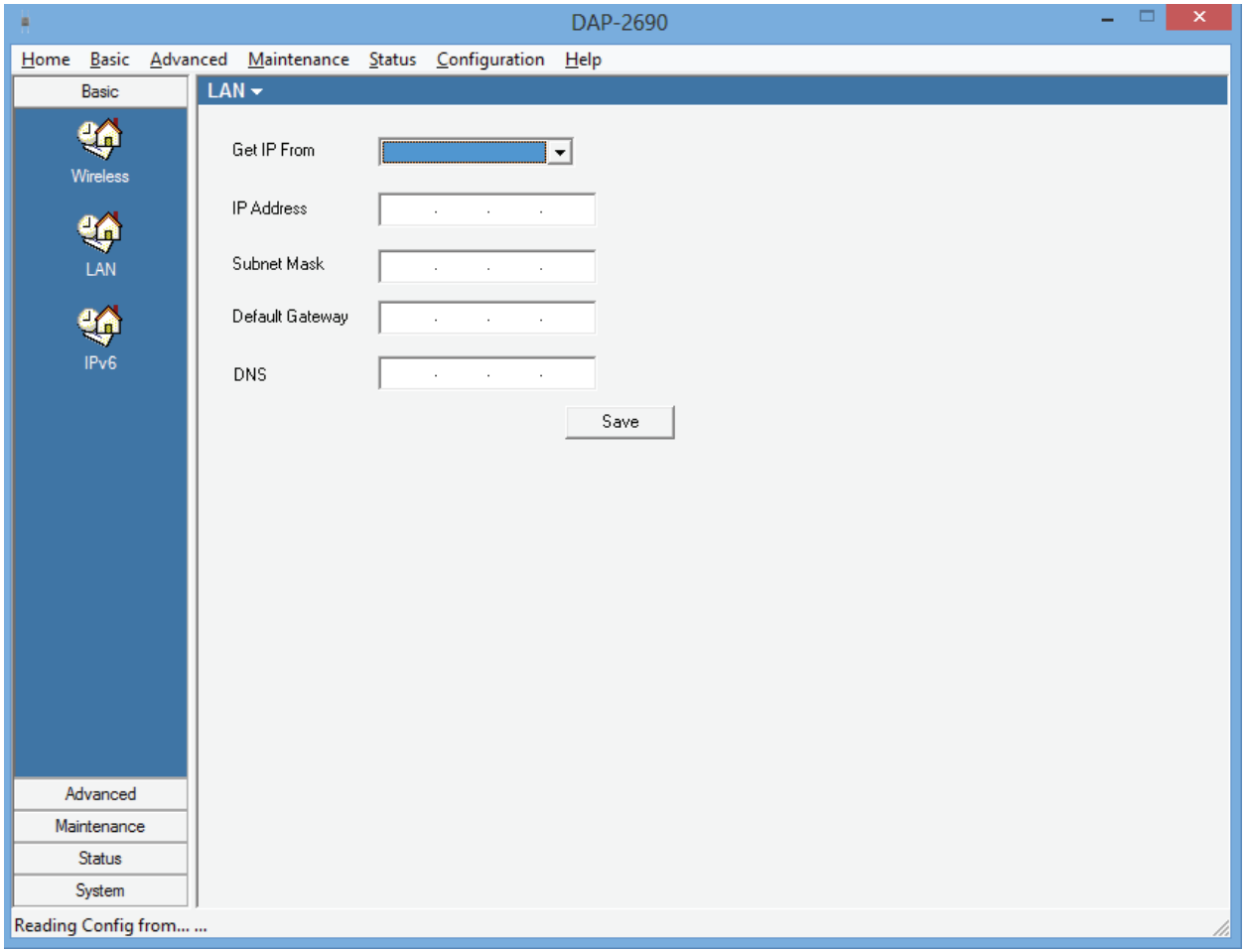
Note: Before beginning with Static configuration, know the following: **IP range**, **Subnet Mask**, **Default Gateway,** and **DNS settings**.

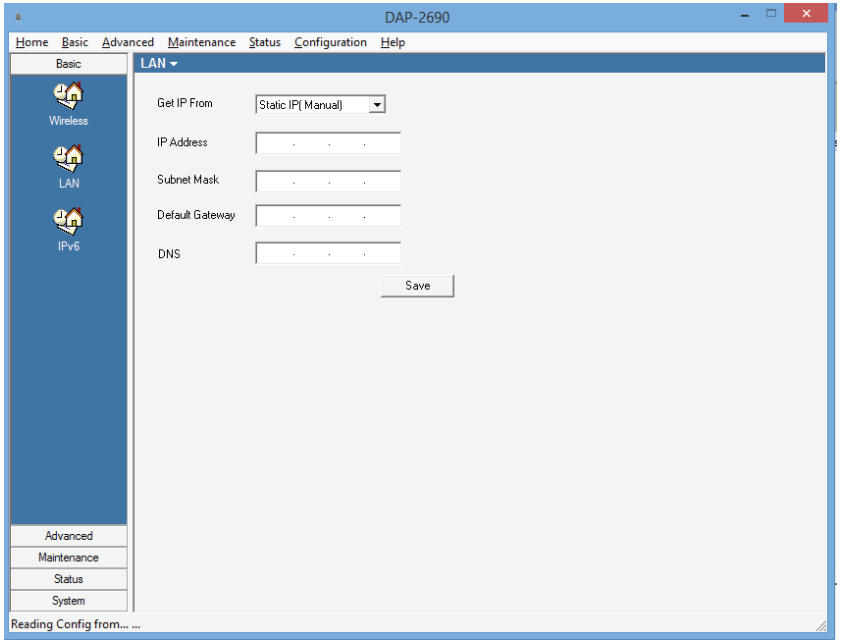
Note: The Access Point acts as a DHCP client , receiving its IP from the DHCP server.



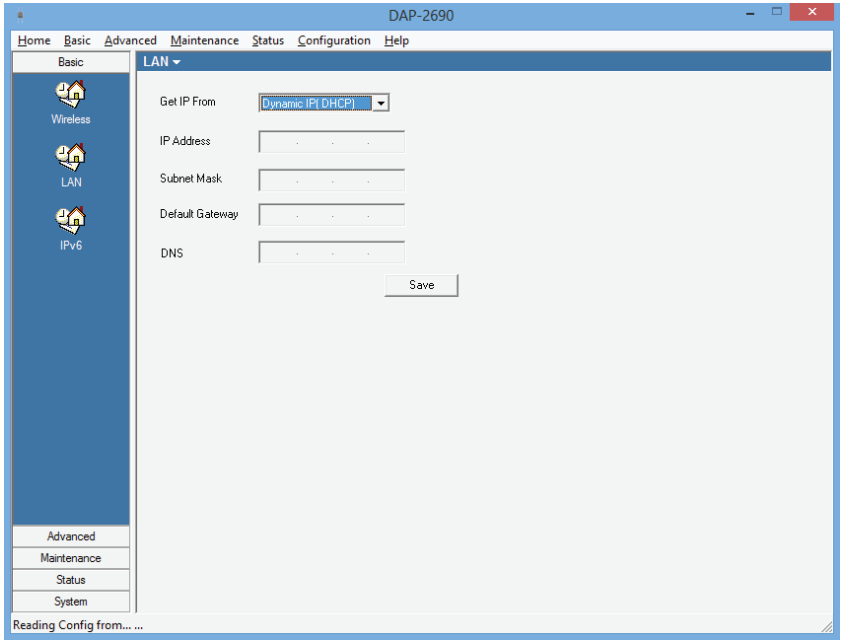
Basic - IPv6

What is IPv6? - The familiar IP addresses that are assigned to practically every device that can access the Internet— computers, smartphones, cameras—follow the IPv4 naming scheme which was developed in 1977. The 32-bit system, which follows the xxx.xxx.xxx.xxx pattern, with each set of numbers ranging from 0 to 254, is capable of generation up to 4.3 billion possible addresses. IPv4 systems and IPv6 systems can run in parallel, the newer standard is not backwards-compatible. A user on the IPv6 network with an IPv6 address is limited to accessing Websites and services that also have an IPv6 address.





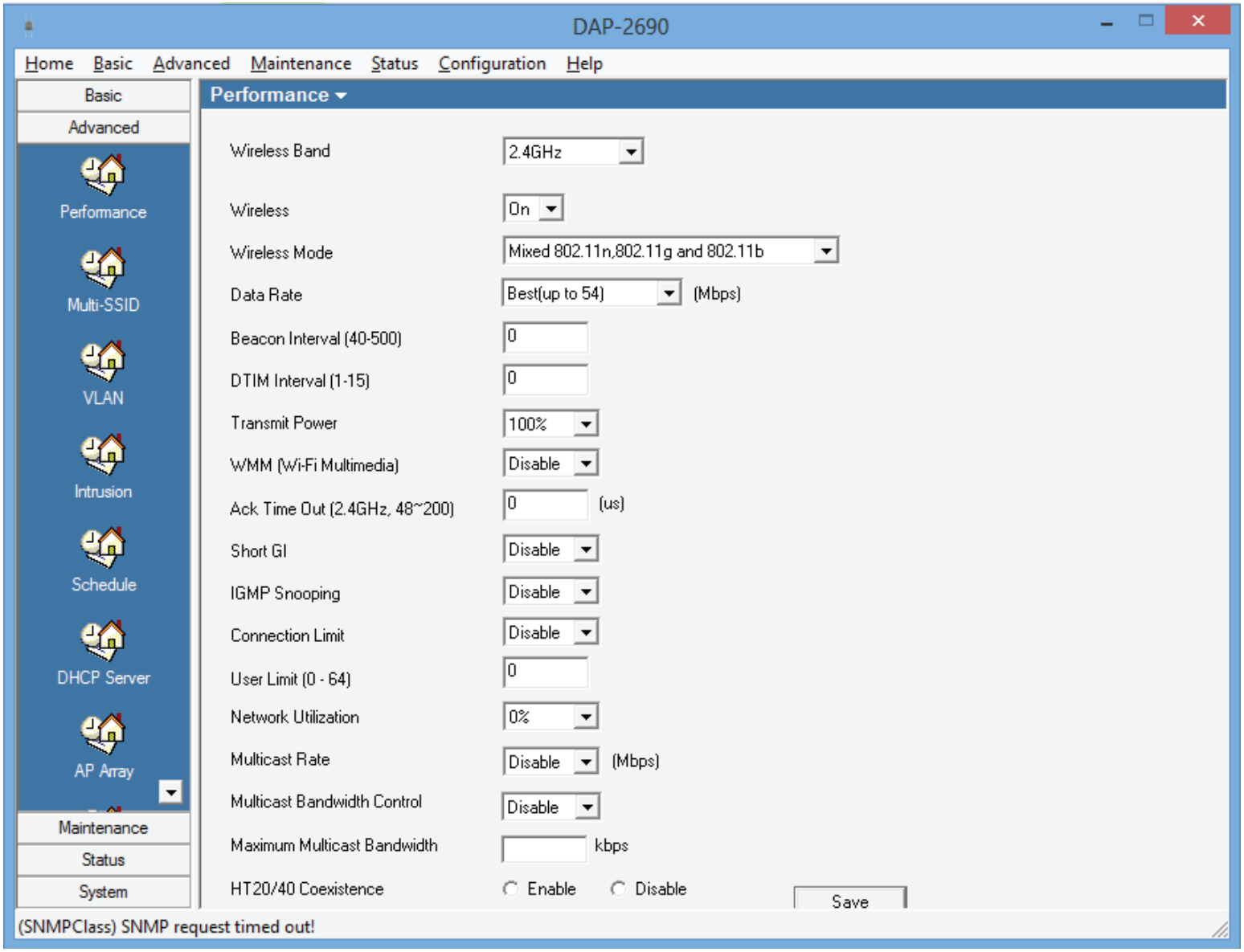
Static IP - Enter the details manually.



Dynamic IP - Have the DHCP server assign an IP to the Access Point

Advanced - Performance

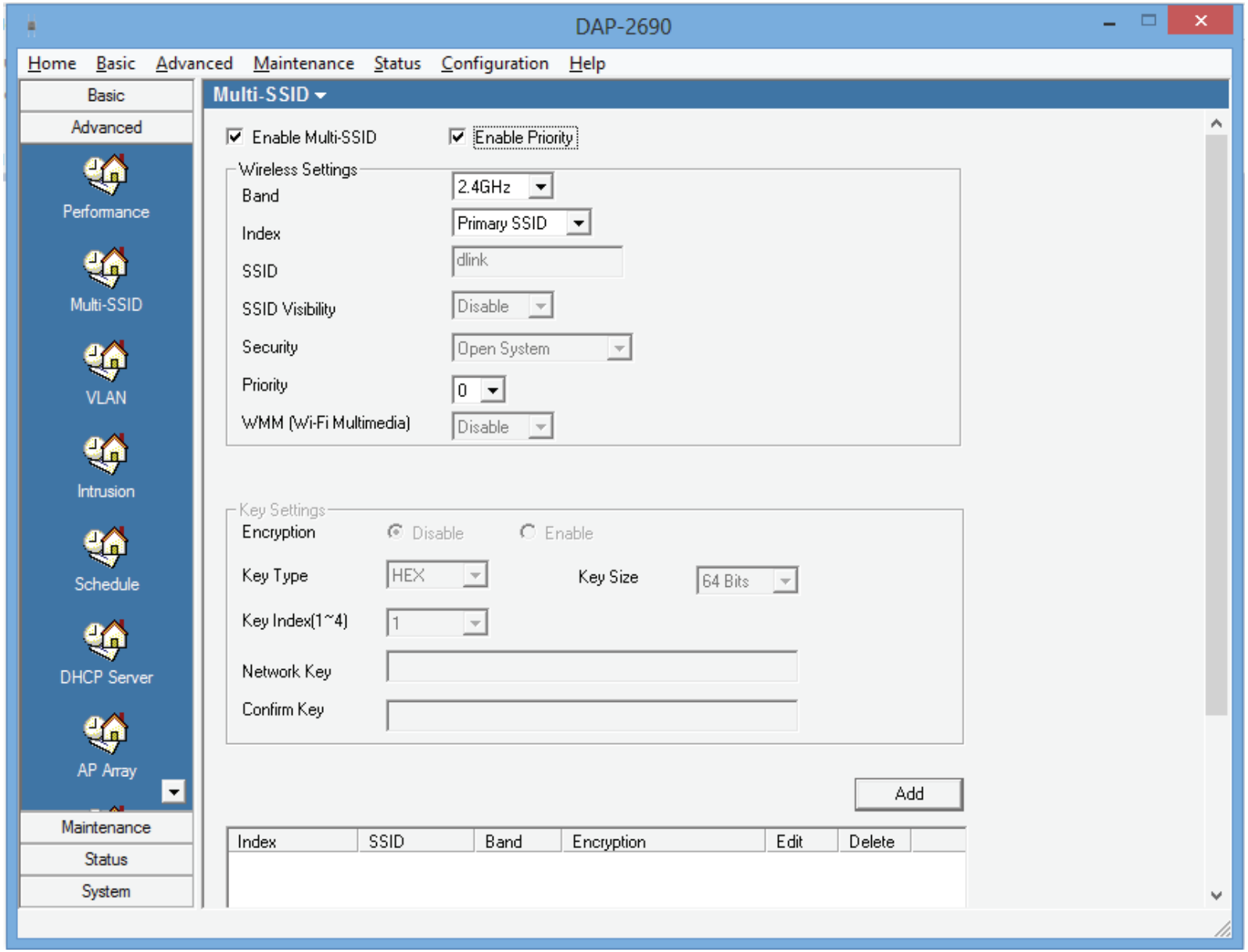
Handles the connection speed options.



COMPONENT	DESCRIPTION
Wireless Band	Select between 2.4GHz and 5GHz
Wireless	Select On/Off
Wireless Mode	Mixed 802.11n, 802.11g, and 802.11b/ 802.11g, and 802.11b/ 802.11n Only
Data Rate	up to 54Mbps
Beacon Interval	Beacons are packets sent by an access point to synchronize a network. Specify the beacon value for the selected device(s) here. The default value of 100 is recommended
DTIM Interval (1-15)	DTIM (Delivery Traffic Indication Message) is a countdown informing clients of the next listening window for broadcast and multicast messages.
Transmit Power	Range from 12.5% - 100%
WMM (Wi-Fi Multimedia)	Select Enable/Disable, (Wi-Fi Multimedia) Improves the user experience for audio, video, and voice applications over a Wi-Fi network. WMM is based on a subset of the IEEE 802.11e WLAN QoS standard.
Ack Time Out (2.4GHz, 48-200)	Select the time-out range
Short GI	Select Enable/Disable
IGMP Snooping	Selec Enable/Disable
Connection Limit	Select Enable/Disable
User Limit (0-64)	Limit the number of users that access this AP
Network Utilization	Limit how the network is used
Multicast Rate	Select between Disable/ 1/2Mbps
Multicast Bandwidth Control	Select between Enable/Disable
Maximum Multicast Bandwidth	Enter a rate in kbps
HT20/40 Coexistence	Select to Enable or Disable
Save	Click to save all configuration changes

Advanced - Multi-SSID

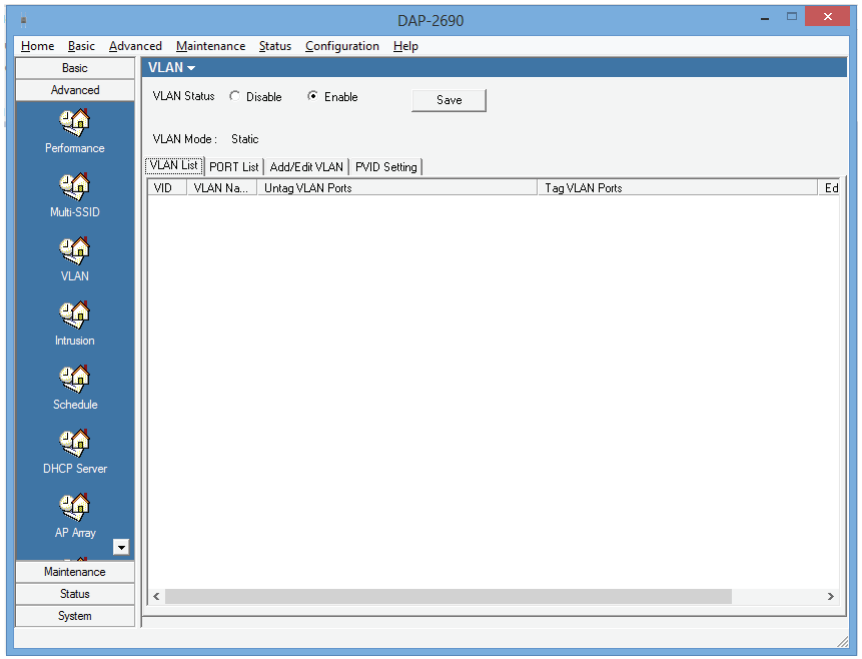
SSID Configuration - Click the checkbox to Enable Multi-SSID and Enable Priority



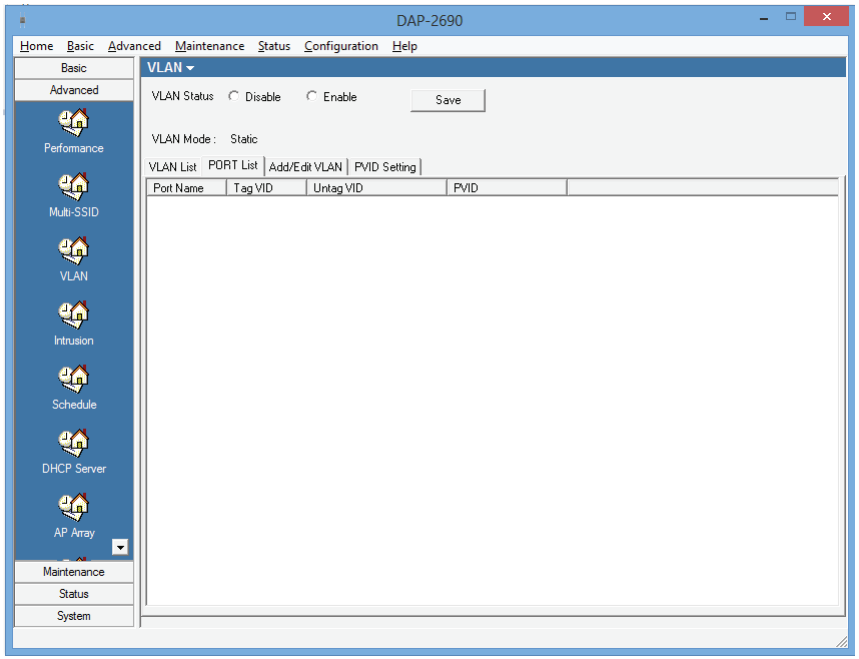
COMPONENT	DESCRIPTION
Wireless Settings - Band	Select between 2.4GHz and 5GHz
Index	Select between the Primary SSID, SSID 1/2/3/4/5/6/7
SSID	Enter a name in the field provided
SSID Visibility	Select to Enable/Disable
Security	Select between Open System/ WPA-Personal/ WPA-Enterprise/ 802.1x
Priority	Select between 1-7
WMM (Wi-Fi Multimedia)	Select Enable/Disable, (Wi-Fi Multimedia) Improves the user experience for audio, video, and voice applications over a Wi-Fi network. WMM is based on a subset of the IEEE 802.11e WLAN QoS standard.
Key Settings - Encryption	Select to Enable/Disable
Key Type	Select ASCII or HEX
Key Size	64 /128 Bits
Key Index (1-4)	Select between 1-4
Network Key	Enter a key value
Confirm Key	Repeat the key value entry
Add	Click Add to add it to the SSID table
Save	Click Save to activate your configuration options

Advanced - VLAN

VLAN Configuration - Select to Enable or Disable VLAN settings. VLAN allows for the partitioning of physical networks.

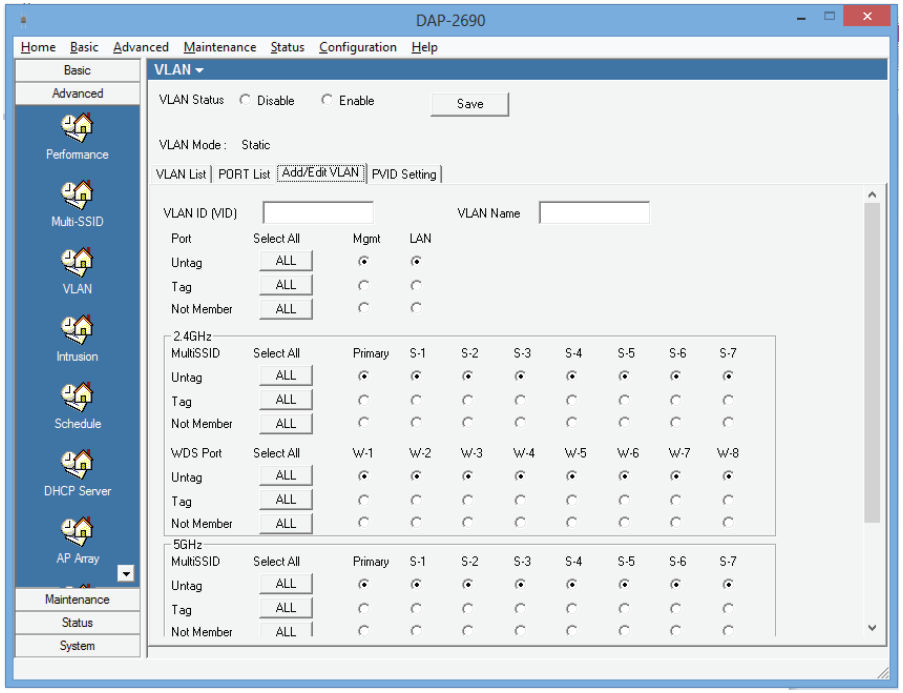


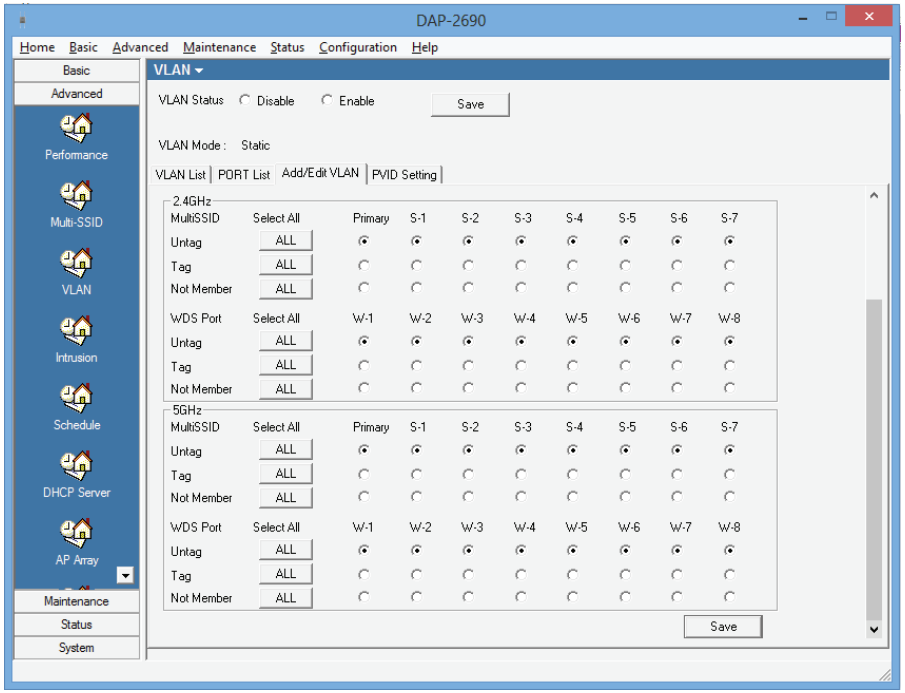
VLAN List - Adding VLAN's populates the VLAN List table.



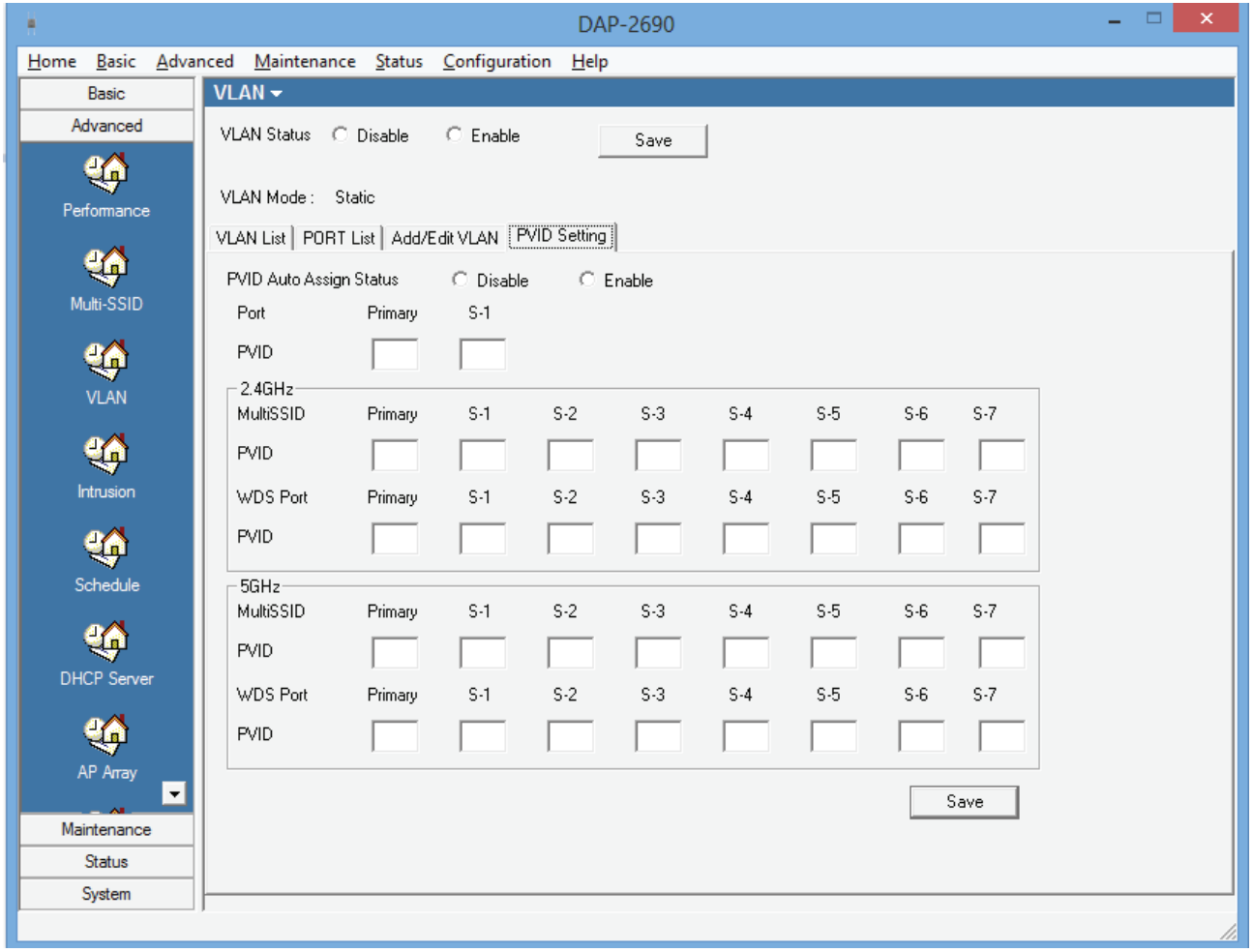
Port List - Adds ports to the list as it becomes populated.

Advanced - Add/Edit VLAN's





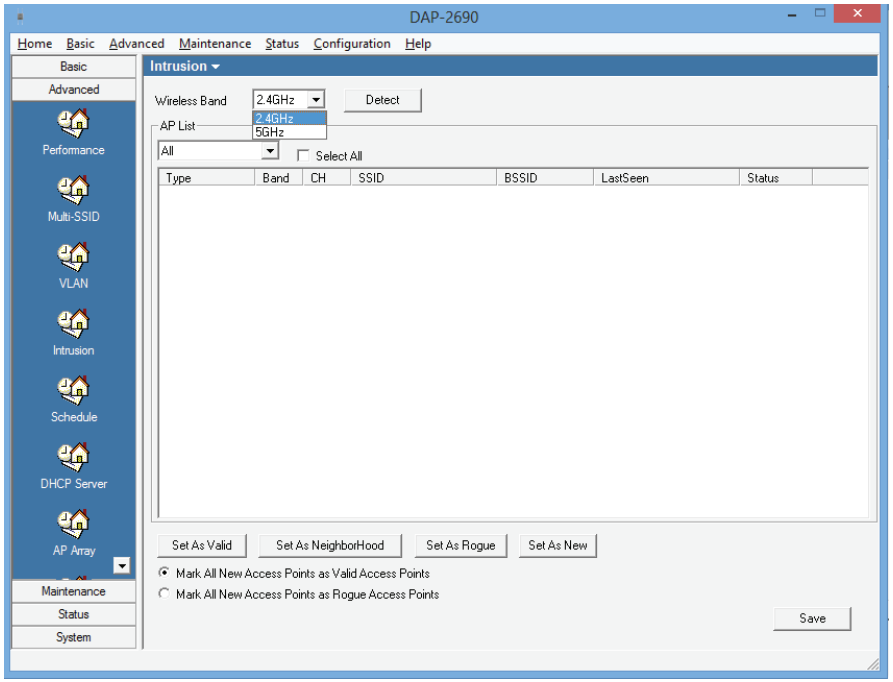
COMPONENT	DESCRIPTION
VLAN ID	Enter an ID for the VLAN
VLAN Name	Enter a name for the VLAN
Port	Select a Port number or select all
2.4GHz MultiSSID	Select an SSID to add to the VLAN
5GHz MultiSSID	Select an SSID to add to the VLAN

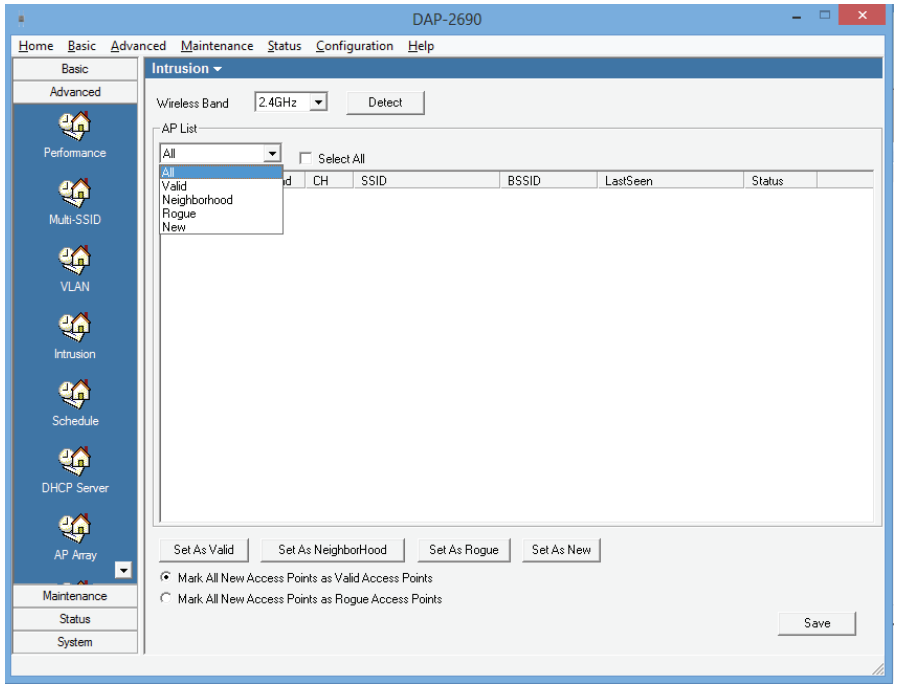


COMPONENT	DESCRIPTION
PVID Auto Assign Status	Select Enable/Disable to activate the feature
Port	Select Primary or S-1
PVID	Enter the specific updates
2.4GHz	Select between MultiSSID PVID settings and WDS Port settings
5GHz	Select between MultiSSID PVID settings and WDS Port settings

Advanced - Intrusion

Intrusion Configuration - Select tools to monitor the networks security



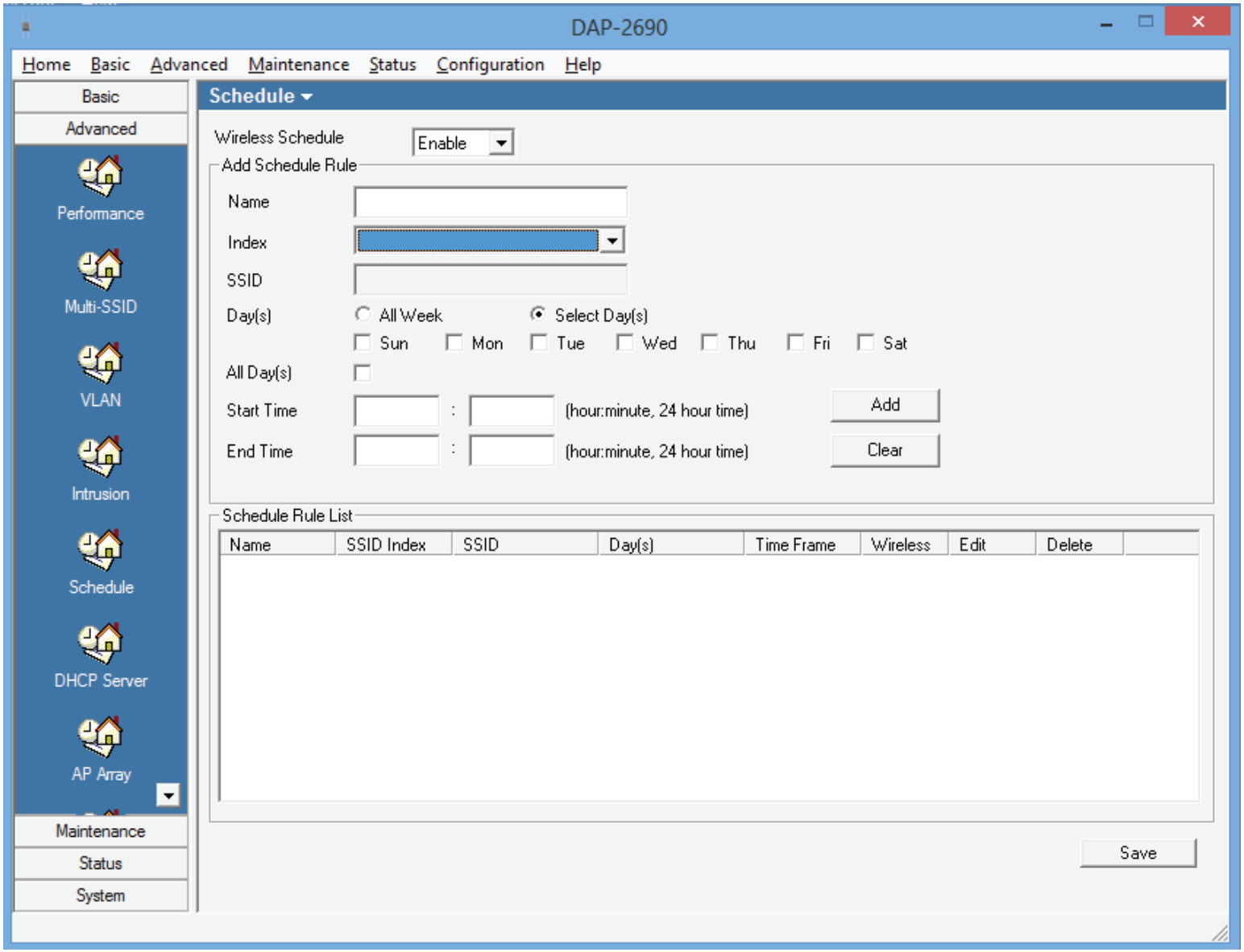


COMPONENT	DESCRIPTION
Wireless Band	Select between 2.4GHz and 5GHz then click Detect
AP List	From the drop-down list select All, Valid, Neighborhood, Rogue, and New / Alternatively, click the Select All checkbox

Once you have populated the Intrusion table, select your option by choosing either the **Set as Valid, Set as Neighborhood, Set as Rogue**, or **Set as New** button. The intrusion data is monitored by **Type, Band, Channel, SSID, BSSID, Last Seen, and Status.**

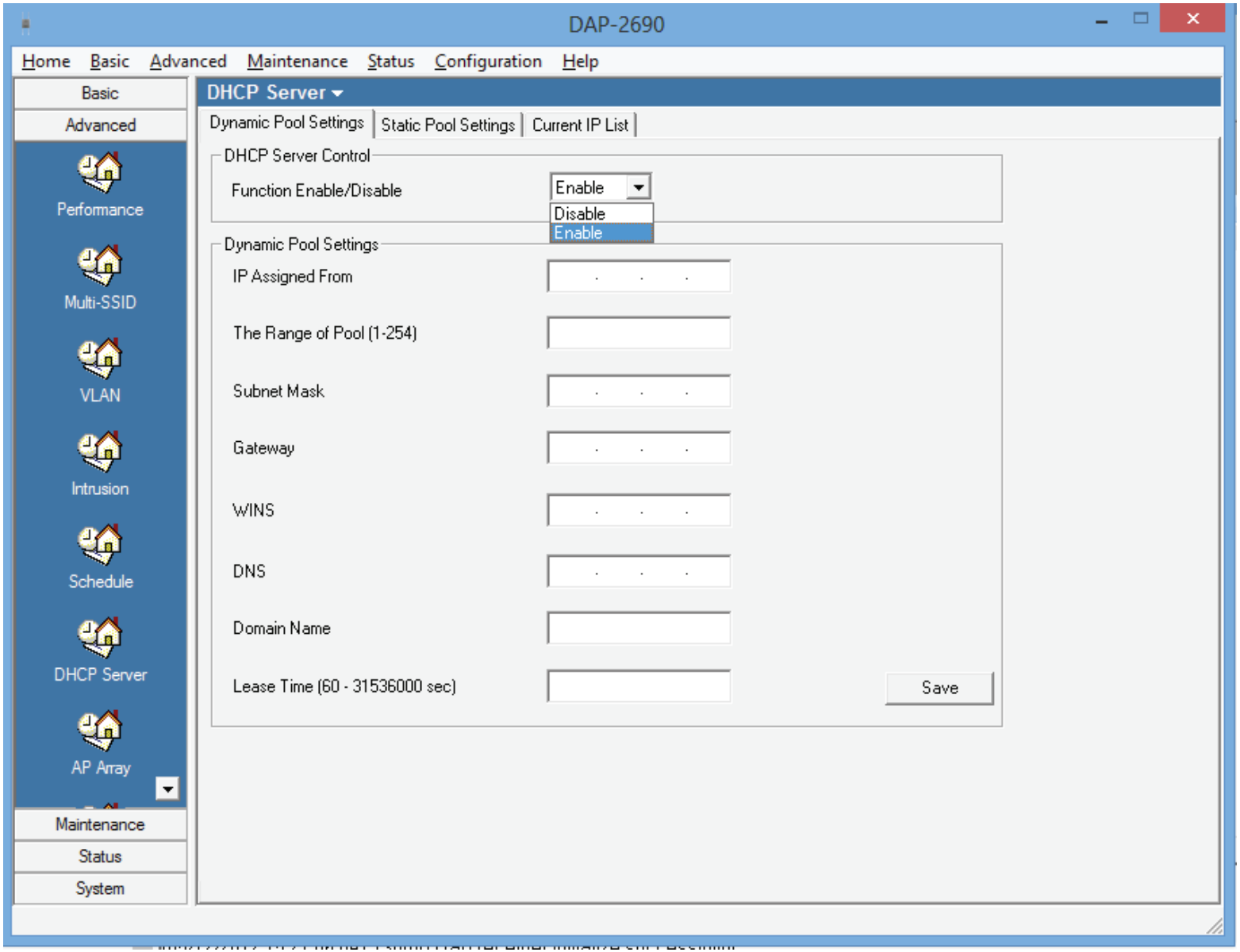
Advanced - Schedule

Scheduling - Select a schedule for each SSID



Advanced - DHCP Server

DHCP Server - Control and configure the DHCP server.

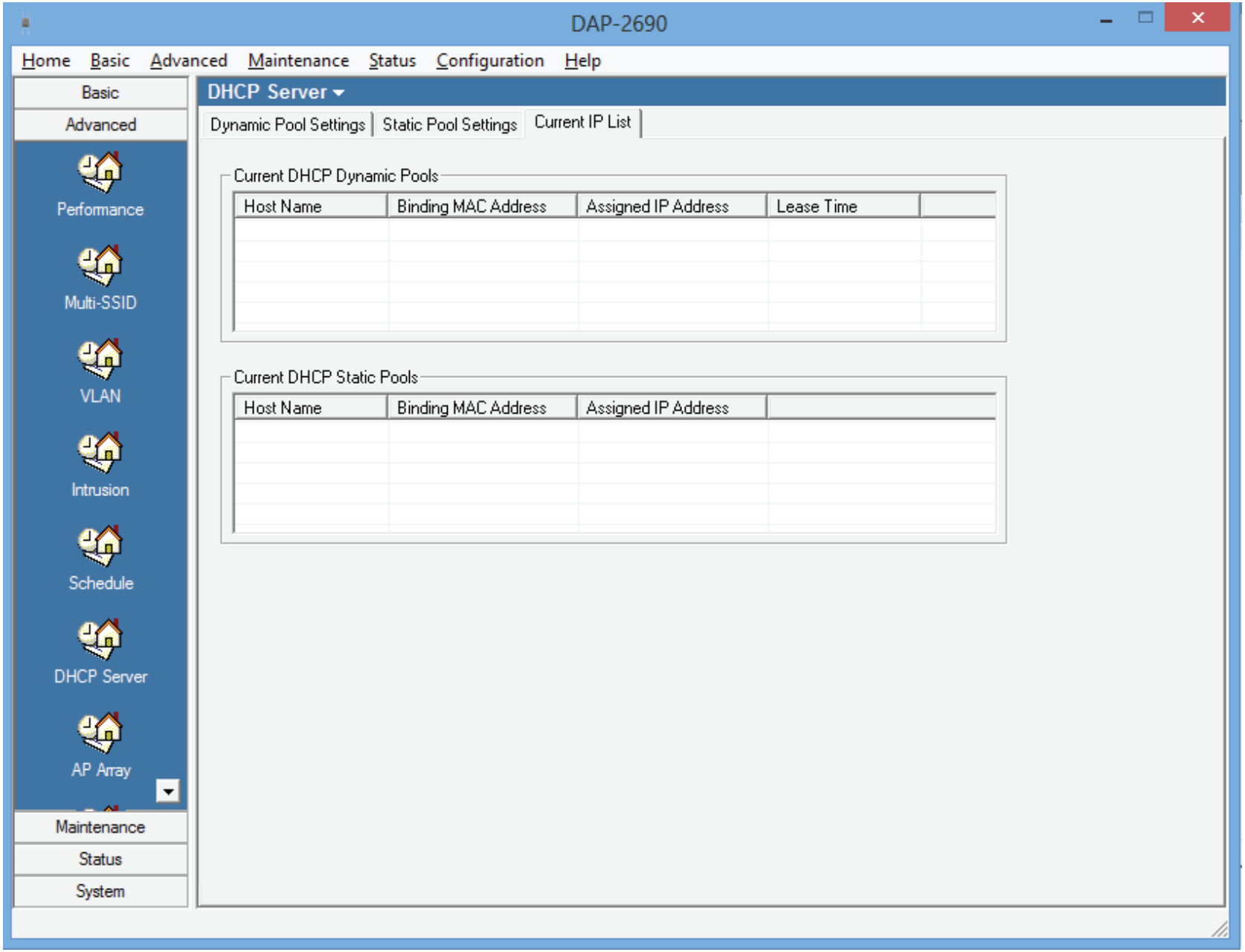


Dynamic Pool Settings

COMPONENT	DESCRIPTION
DHCP Server Control	Select to Enable/Disable
IP Assigned From	Enter an IP to start from
The Range of Pool	Enter the IP pool range
Subnet Mask	Enter an subnet mask
Gateway	Enter a Gateway IP
WINS	Enter a WINS address
DNS	Enter a DNS address
Domain Name	Enter a Domain Name
Lease Time	Enter the IP duration
Save	Click Save to saving your configuration settings

Static Pool Settings

COMPONENT	DESCRIPTION
DHCP Server Control	Select to Enable/Disable
IP Assigned From	Enter an IP to start from
The Range of Pool	Enter the IP pool range
Subnet Mask	Enter an subnet mask
Gateway	Enter a Gateway IP
WINS	Enter a WINS address
DNS	Enter a DNS address
Domain Name	Enter a Domain Name
Lease Time	Enter the IP duration
Save	Click Save to saving your configuration settings


DAP-2690
Home
Basic
Advanced
Maintenance
Status
Configuration
Help
Basic
Advanced
Performance
Multi-SSID
VLAN
Intrusion
Schedule
DHCP Server
AP Array
Maintenance
Status
System
DHCP Server
Dynamic Pool Settings
Static Pool Settings
Current IP List
Current DHCP Dynamic Pools
Host Name
Binding MAC Address
Assigned IP Address
Lease Time
Current DHCP Static Pools
Host Name
Binding MAC Address
Assigned IP Address

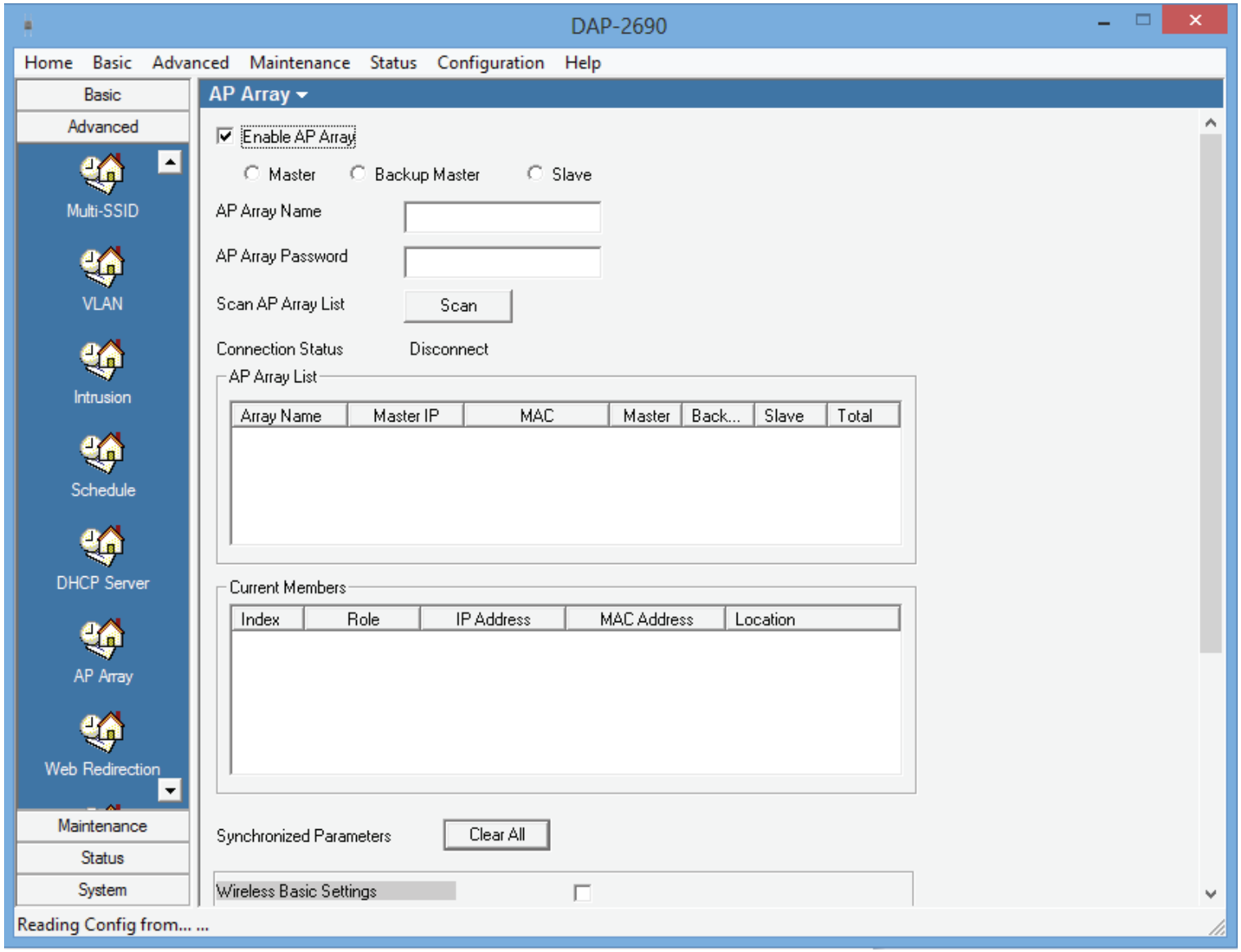
Current IP List

COMPONENT	DESCRIPTION
Current DHCP Dynamic Pools	
Host Name	The host name is the main DHCP host provider
Binding MAC Address	These are the MAC addresses of the connected AP's
Assigned IP Address	These are the IP addresses assigned by the DHCP server
Lease Time	The IP life span

COMPONENT	DESCRIPTION
Current DHCP Static Pools	
Host Name	The host name is the main DHCP Static host provider
Binding MAC Address	These are the MAC addresses of the connected AP's
Assigned IP Address	These are the IP addresses assigned by the DHCP server
Lease Time	The IP life span

Advanced - AP Array

AP Array is enabling one or more Access Points to form a team of network devices. These Access Points amount to an array. They can be used as backup devices for when one or more than one goes down.

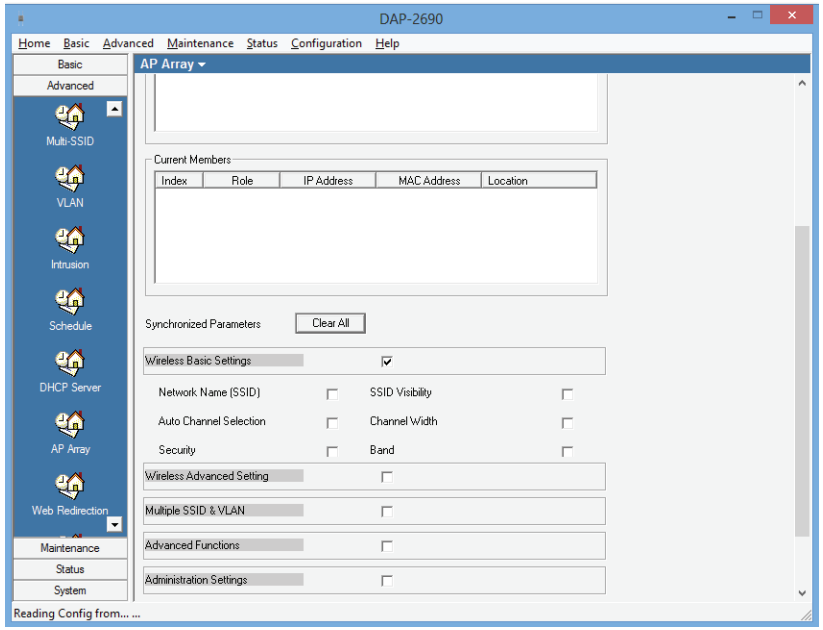


COMPONENT	DESCRIPTION
Enable AP Array	Click the checkbox to start the AP Array
Master	Select this to make the Access Point the main device
Backup Master	Select this option to make this Access Point the backup to the main device
Slave	Select this option to make this Access Point the slave to either the Master or the Backup Master
AP Array Name	Enter a name for the Access Point array
AP Array Password	Enter a password for the Access Point
Scan AP Array List	Click the Scan button to scan the network
Connection Status	This will mention if you are connected or disconnected
AP Array List	This list is populated once arrays are added
Current Members	This is a list of the Access Point Array members
Sychronize Parameters	Click Clear All to clear the list

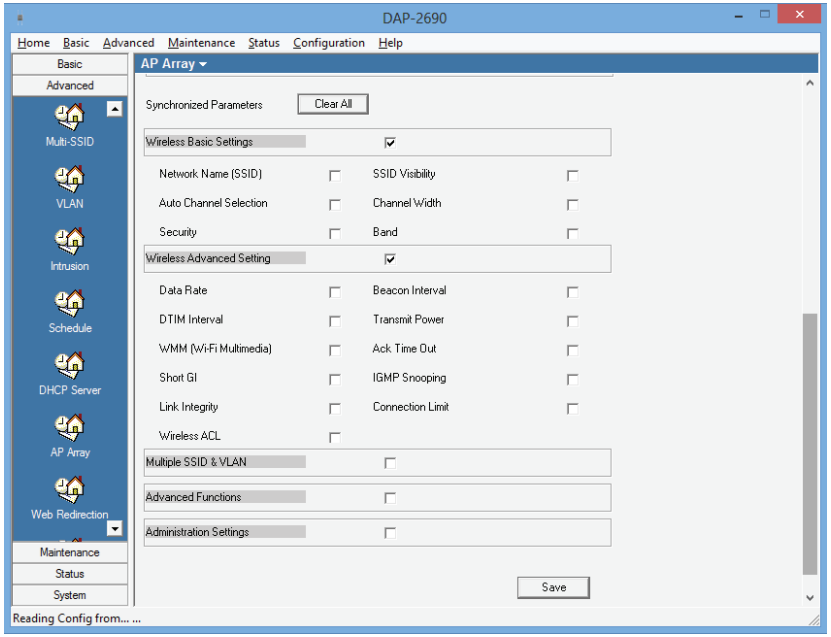
Advanced - AP Array - Alternative Settings

Under the main Array Settings there is also settings for Wireless Basic Settings, Wireless Advanced Settings, Multiple SSID & VLAN settings, Advanced Functions, and Administrative Settings. Let's take a closer look.

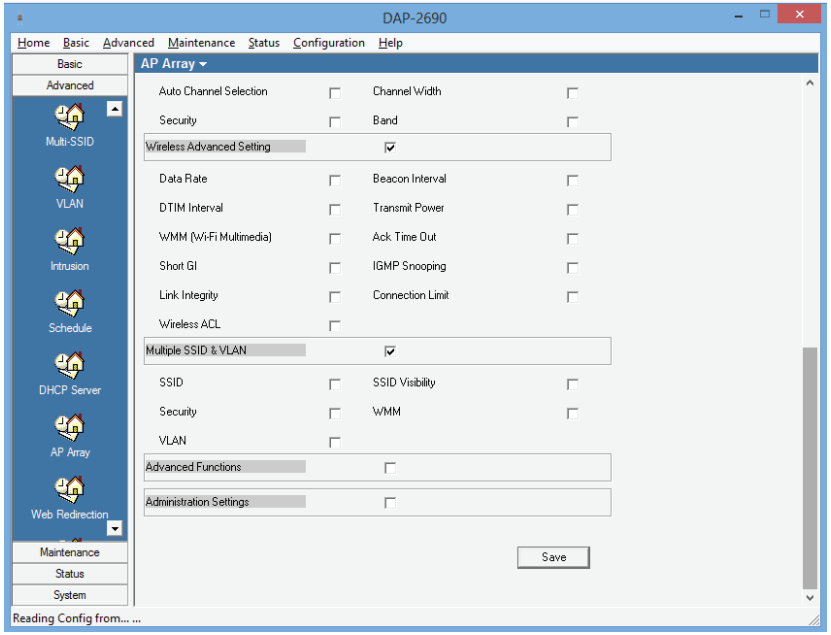
Click the checkbox next to Wireless Basic Settings. The options expand to include: Network Name (SSID), SSID Visibility, Auto Channel Selection, Channel Width, Security, and Band. Select the options you need in your configuration.



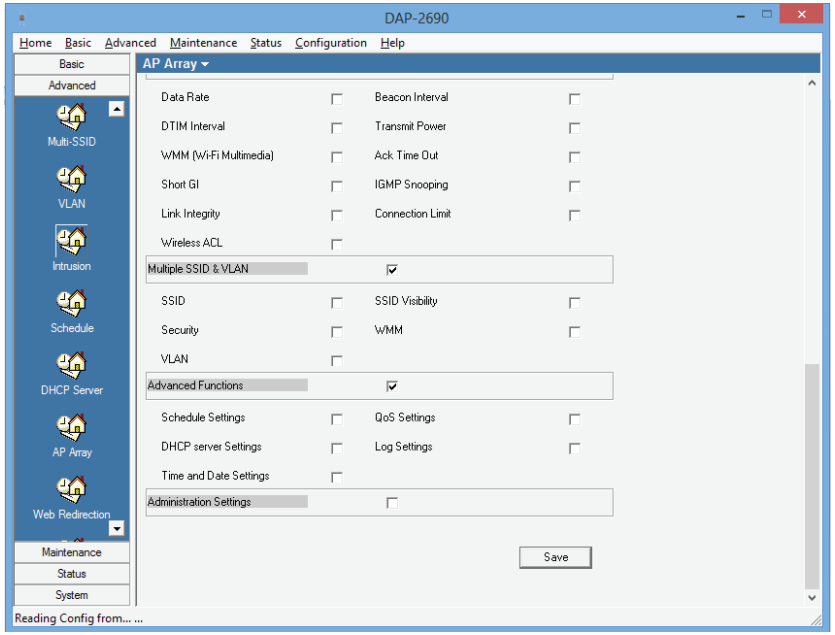
Click the checkbox next to Wireless Advanced Settings. The options expand to include: Date Rate, Beacon Interval, DTIM Interval, Transmit Power, WMM (Wi-Fi Multimedia), Ack Time Out, Short GI, IGMP Snooping, Link Integrity, Connection Limit, Wireless ACL. Select the options you need in your configuration.



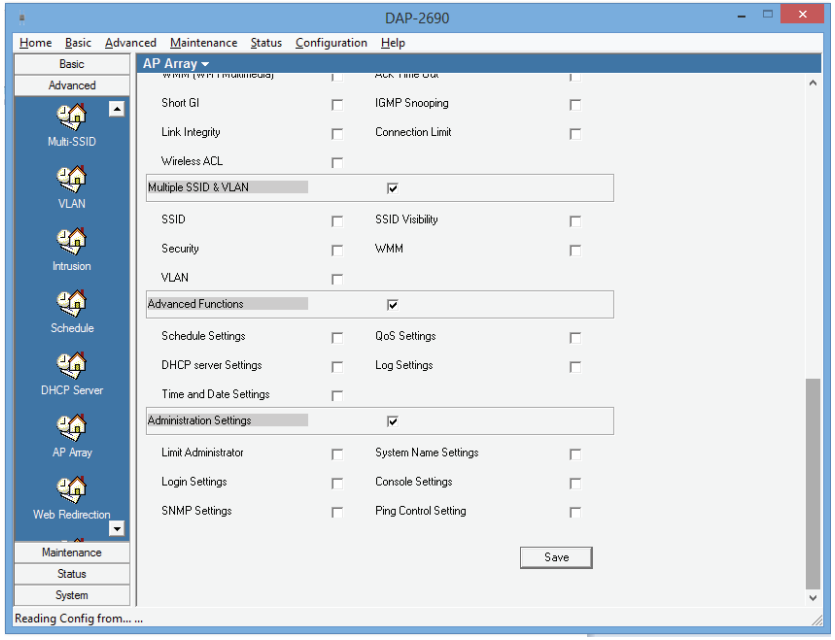
Click the checkbox next to Multiple SSID & VLAN. The options expand to include: SSID, SSID Visibility, Security, WMM, or VLAN. Select the options you need in your configuration.



Click the checkbox next to Advanced Functions. The options expand to include:Schedule Settings, QoS Settings, DHCP server Settings, Log Settings, Time and Date Settings. Select the options you need in your configuration.

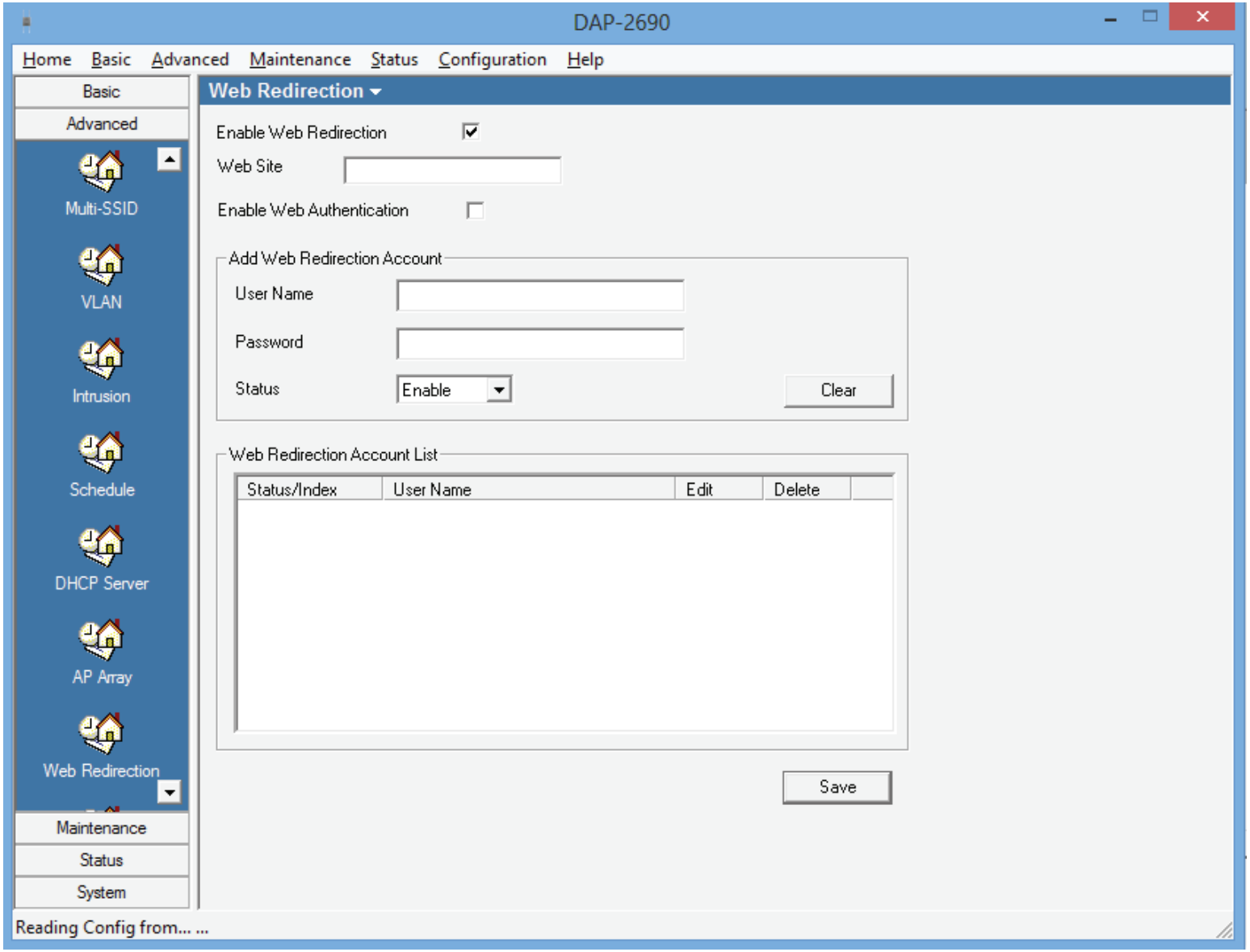


Click the checkbox next to Administrative Settings. The options expand to include:Limit Administrator, System Name Settings, Login Settings, Console Settings, SNMP Settings, and Ping Control Settings. Select the options you need in your configuration.



Advanced - Web Redirection

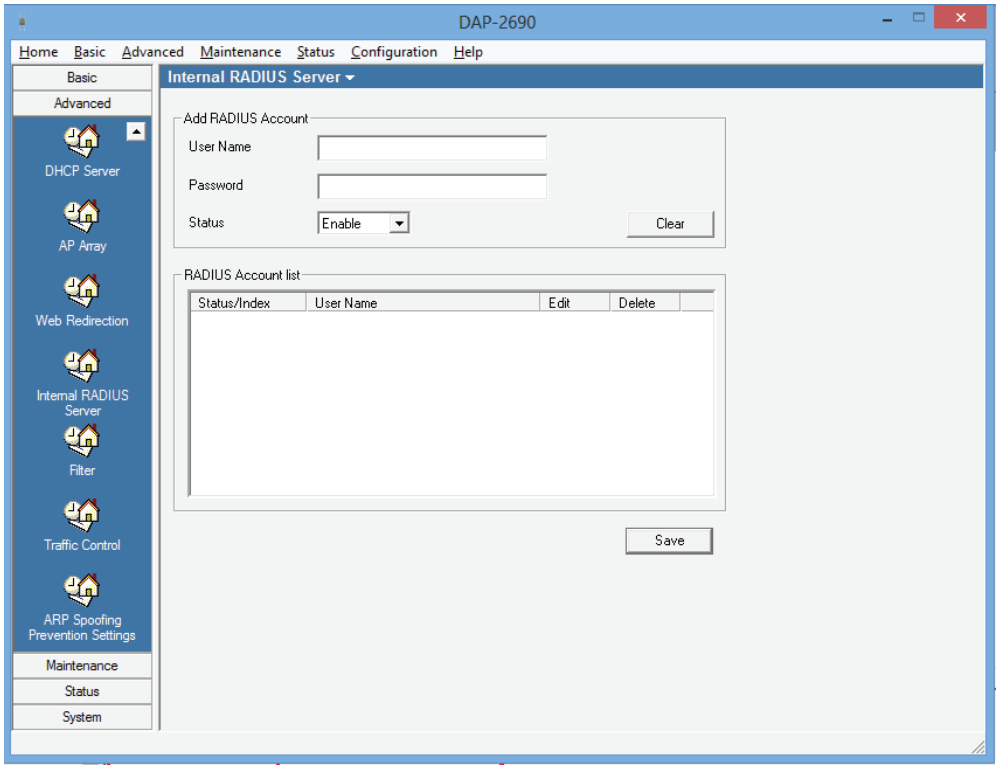
Web redirection is what the name implies. It will redirect data to a web address or web IP.



COMPONENT	DESCRIPTION
Enable Web Redirection	Click the checkbox to enable this function
Web Site	Enter the website details
Enable Web Authentication	Check this checkbox to enable authentication on the web server
Add Web Redirection Account	
Username	Enter a username for the account details
Password	Enter a password for the redirection
Status	Select between Enable or Disable
Clear	Click clear to erase data
Web Redirection Account List	Data entered into earlier will promulgate in this list
Save	Click Save to save settings

Advanced - Internal RADIUS Server

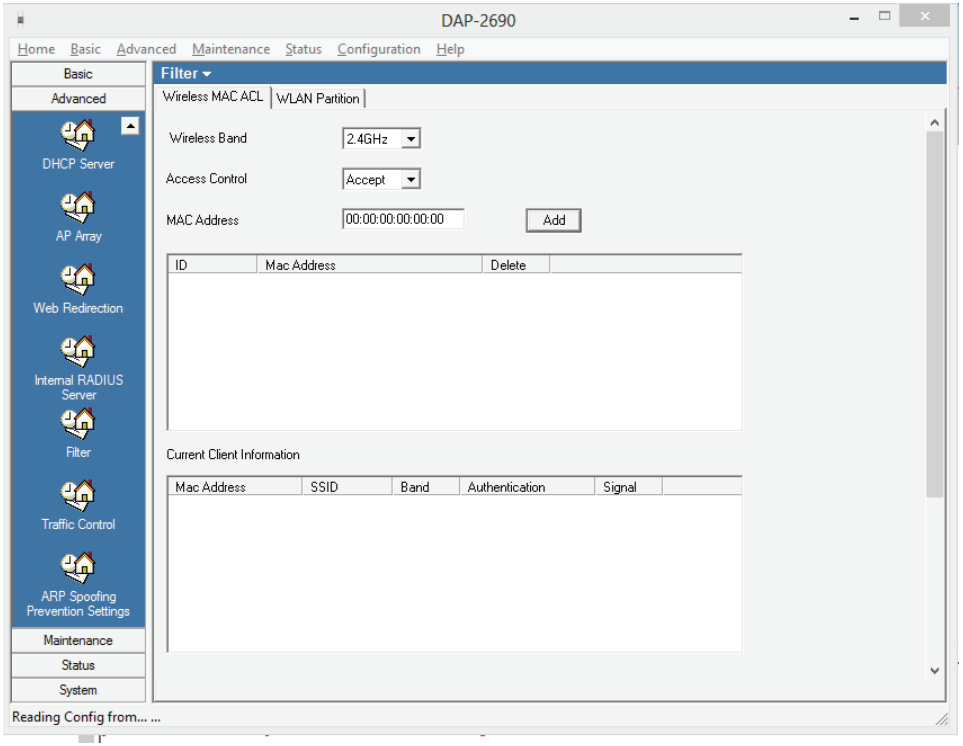
The Access Point allows you to set RADIUS Server



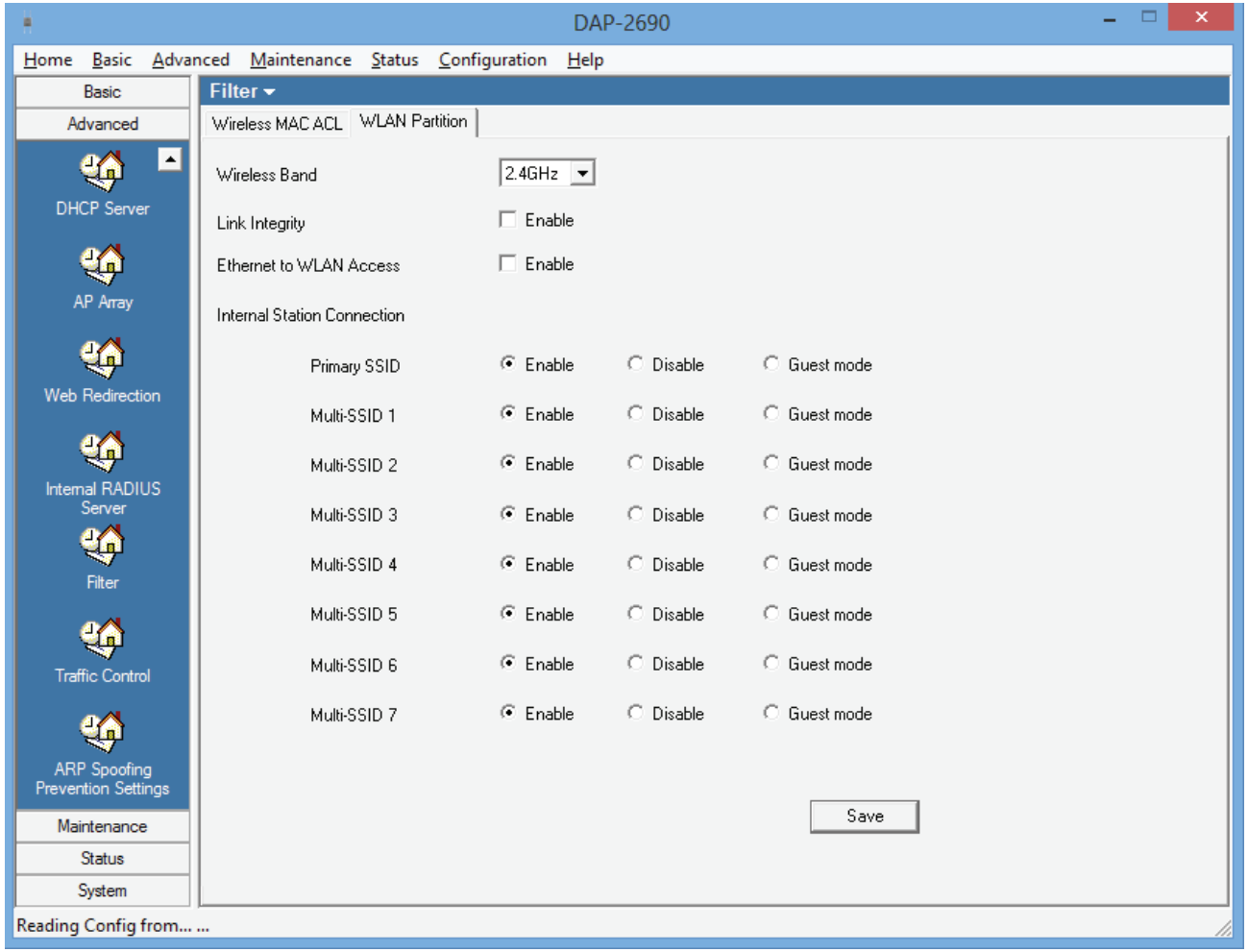
COMPONENT	DESCRIPTION
Add RADIUS Account	
User Name	Enter a username for the account
Password	Enter a password for the RADIUS Account
Status	Click to enable or disable
Clear	Click clear to erase data
RADIUS Account List	Data entered into earlier will promulgate in this list
Save	Click Save to save settings

Advanced - Filters

The Filter protects your Access Point on two fronts: MAC addressing and WLAN partitioning.



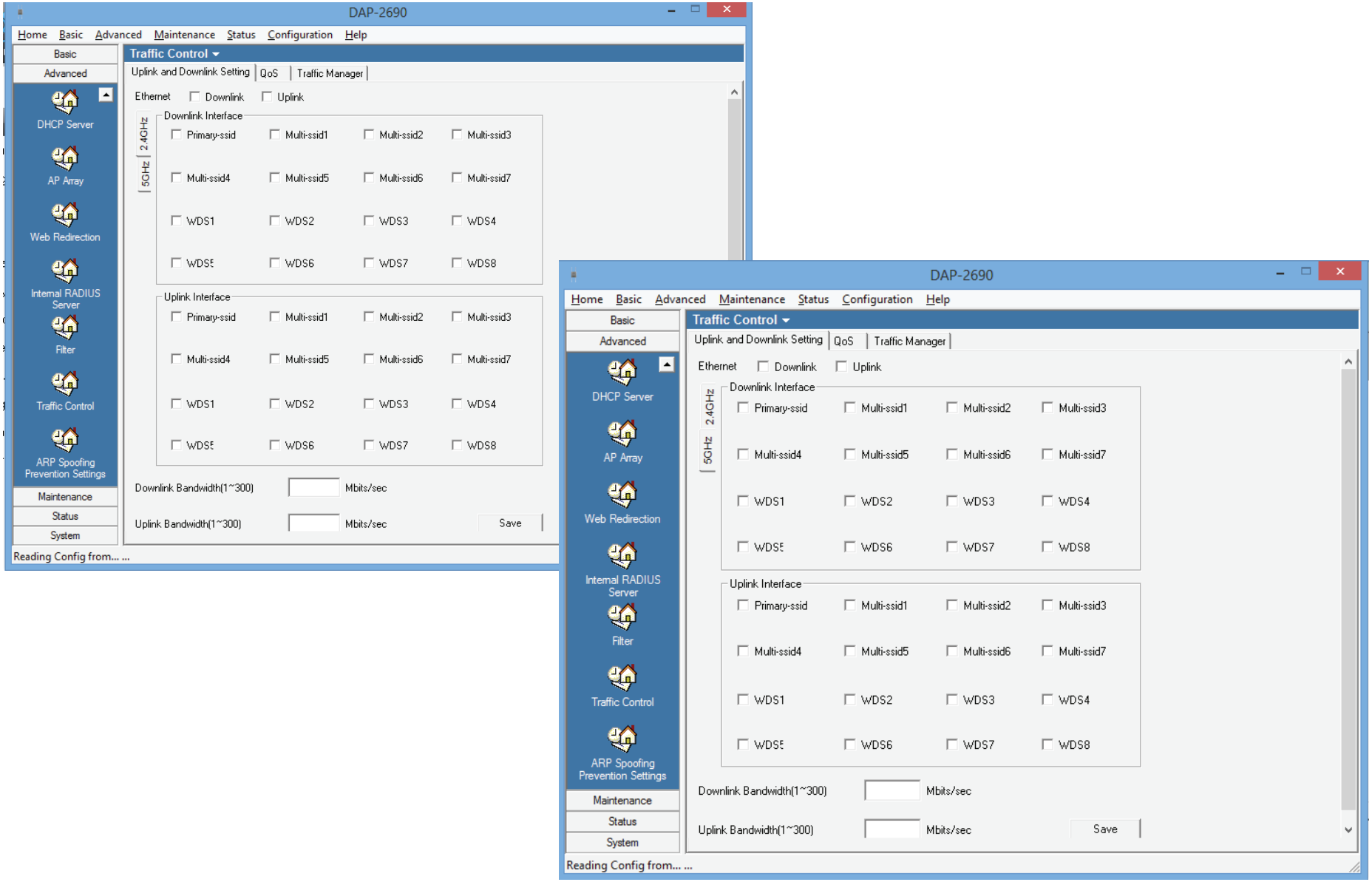
COMPONENT	DESCRIPTION
Wireless Band	Select between 2.4GHz or 5GHz
Access Control	Select between Accept, Reject, or Disable
MAC Address	Enter the MAC address details
Add	Click the Add button to add it to the list
Current Client Information	This list is populated as devices are added
Upload ACL File	Click Browse to add an ACL file to the list and click Upload when ready
Download ACL File	Click the Download button to dowload the file to your local hard drive
Save	Click Save to save settings



COMPONENT	DESCRIPTION
Wireless Band	Select between 2.4GHz or 5GHz
Link Integrity	Click the checkbox to enable
Ethernet to WLAN Access	Click the checkbox to enable
Internal Station Connection	For each SSID, either select to Enable/ Disable/ or set in Guest mode
Save	Click Save to save settings

Advanced - Traffic Control

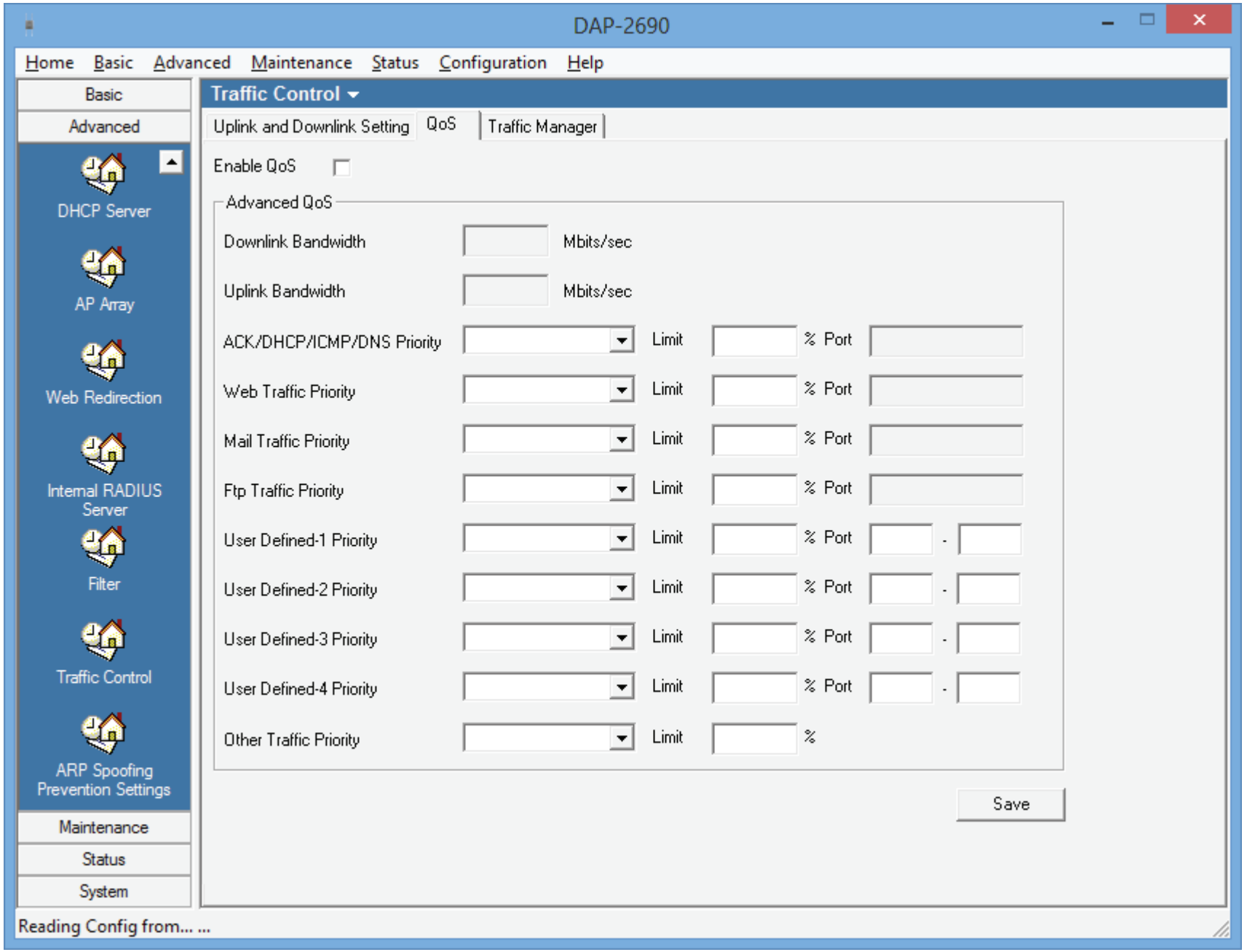
Control downloads and uploads to or from the Access Point. These network links can be controlled in 2.5GHz or 5GHz modes. Toggle between the two modes.



Uplink and Downlink Settings

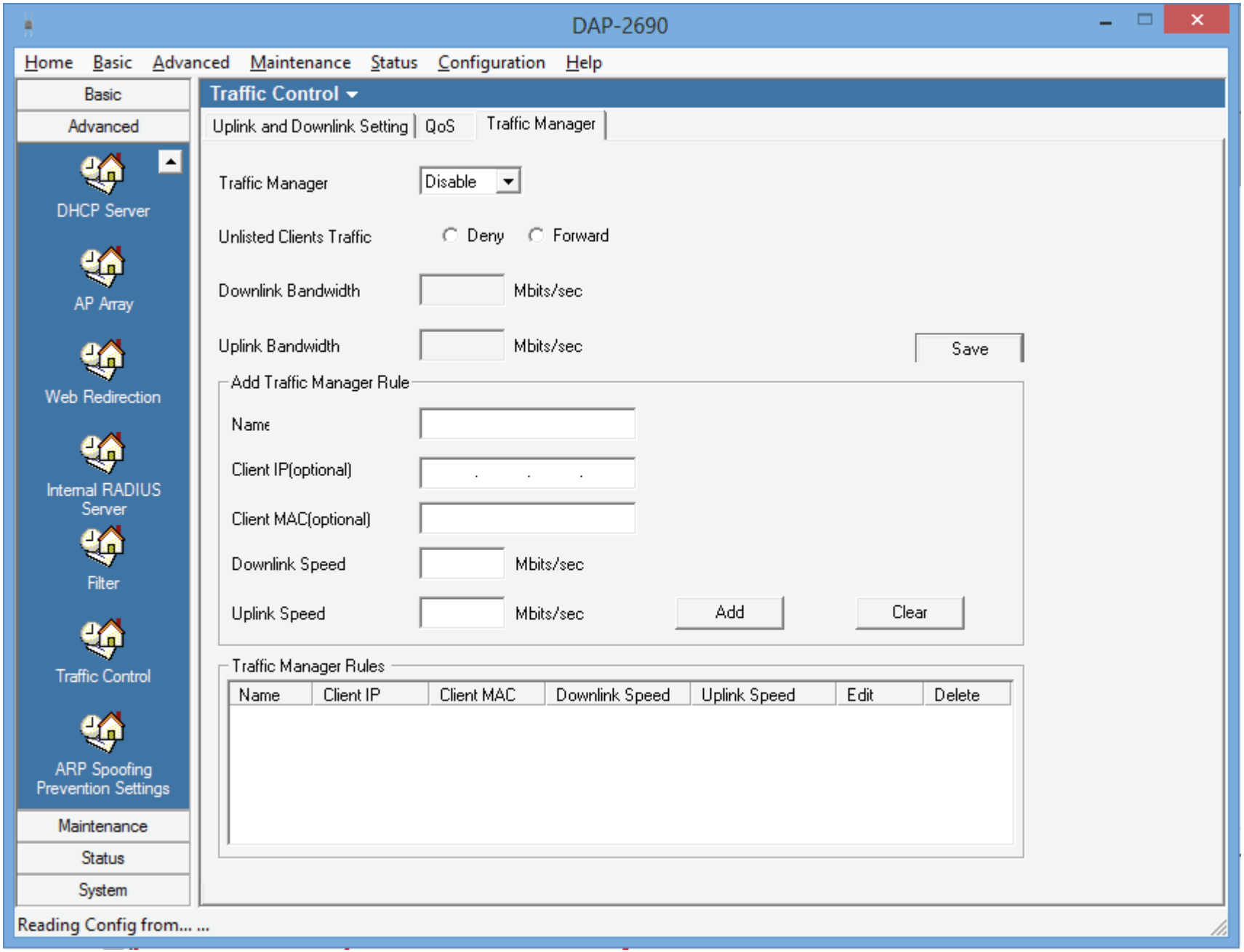
COMPONENT	DESCRIPTION
Ethernet	Click either the Downlink or Uplink checkboxes to configure the settings
For Downlink Interface	Click the checkbox to enable any of the SSID's
Select between	Primary-ssid, Multi-ssid1, Multi-ssid2, Multi-ssid3, Multi-ssid4, Multi-ssid5, Multi-ssid6, Multi-ssid7, WDS1, WDS2, WDS3, WDS4, WDS5,WDS6,WDS7, WDS8
For Downlink Interface	Click the checkbox to enable any of the SSID's
Select between	Primary-ssid, Multi-ssid1, Multi-ssid2, Multi-ssid3, Multi-ssid4, Multi-ssid5, Multi-ssid6, Multi-ssid7, WDS1, WDS2, WDS3, WDS4, WDS5,WDS6,WDS7, WDS8
Download Bandwidth (1~300)	Enter a value in Mbits/sec
Uplink Bandwidth (1~300)	Enter a value in Mbits/Sec
Save	Click Save to save your settings

QoS


DAP-2690
Home
Basic
Advanced
Maintenance
Status
Configuration
Help
Basic
Advanced
DHCP Server
AP Array
Web Redirection
Internal RADIUS Server
Filter
Traffic Control
ARP Spoofing Prevention Settings
Maintenance
Status
System
Traffic Control
Uplink and Downlink Setting
QoS
Traffic Manager
Enable QoS
Advanced QoS
Downlink Bandwidth
Mbits/sec
Uplink Bandwidth
Mbits/sec
ACK/DHCP/ICMP/DNS Priority
Limit
% Port
Web Traffic Priority
Mail Traffic Priority
Ftp Traffic Priority
User Defined-1 Priority
User Defined-2 Priority
User Defined-3 Priority
User Defined-4 Priority
Other Traffic Priority
Save
Reading Config from... ...

COMPONENT	DESCRIPTION
Enable QoS	Click the checkbox to enable this function (this function does not work unless you have set uplink and downlink parameters
Advanced QoS	
Downlink Bandwidth	Enter a value Mbits/sec
Uplink Bandwidth	Enter a value Mbits/sec
ACK/DHCP/ICMP/ DNS Priority	Select between Highest Priority, Second Priority, Third Priority, and Low Priority. Enter the amount traction and the Port number
Web Traffic Priority	Select between Highest Priority, Second Priority, Third Priority, and Low Priority. Enter the amount traction and the Port number
Mail Traffic Priority	Select between Highest Priority, Second Priority, Third Priority, and Low Priority. Enter the amount traction and the Port number
FTP Traffic Priority	Select between Highest Priority, Second Priority, Third Priority, and Low Priority. Enter the amount traction and the Port number
User Defined-1 Priority	Select between Highest Priority, Second Priority, Third Priority, and Low Priority. Enter the amount traction and the Port number
User Defined-2 Priority	Select between Highest Priority, Second Priority, Third Priority, and Low Priority. Enter the amount traction and the Port number
User Defined-3 Priority	Select between Highest Priority, Second Priority, Third Priority, and Low Priority. Enter the amount traction and the Port number
User Defined-4 Priority	Select between Highest Priority, Second Priority, Third Priority, and Low Priority. Enter the amount traction and the Port number
Other Traffic Priority	Select between Highest Priority, Second Priority, Third Priority, and Low Priority. Enter the amount traction
Save	Click the save button to save settings

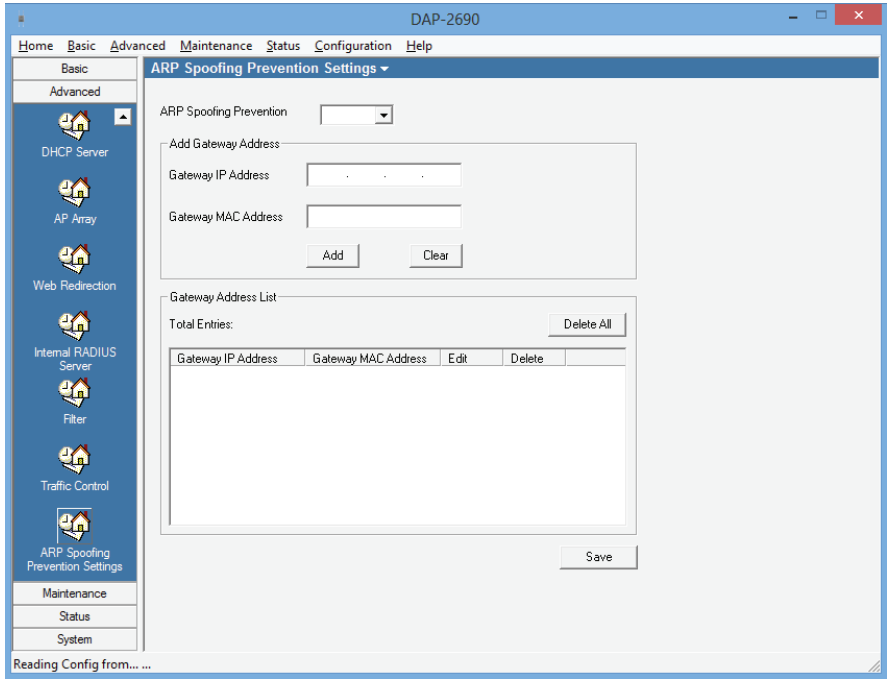
Traffic Manager



COMPONENT	DESCRIPTION
Traffic Manager	Click to Enable or Disable
Unlisted Client Traffic	Select Deny or Forward
Downlink Bandwidth	Enter a value Mbits/sec
Uplink Bandwidth	Enter a value Mbits/sec
Save	Click the save button to save settings
Add Traffic Manager Rule	
Name	Enter a name in the field provided
Client IP (optional)	Enter the IP specifics
Client MAC (optional)	Enter the MAC specifics
Downlink Speed	Enter a value in Mbits/sec
Uplink Speed	Enter a value in Mbits/sec
Add	Click Add to add it to the Traffic Manager Rules
Clear	Click Clear to discard the information

Advanced - ARP Spoofing Prevention Settings

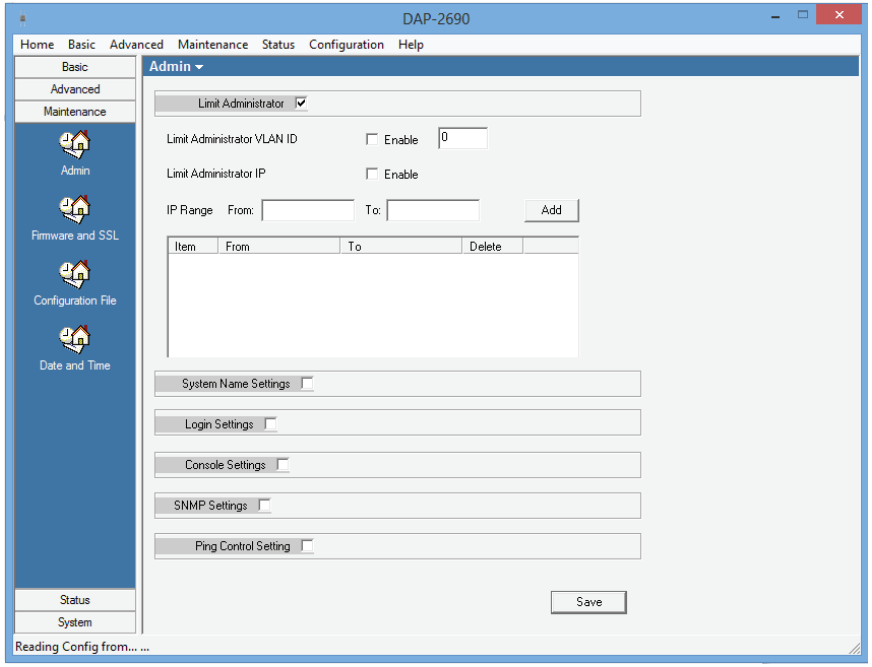
This provides ARP Spoofing prevention techniques to provide an added feature to the router.



COMPONENT	DESCRIPTION
ARP Spoofing Prevention	Click to Enable or Disable
Add Gateway Address	
Gateway IP Address	Enter the Gateway IP
Gateway MAC Address	Enter the MAC address
Add	Click Add to include it to the Gateway Address List
Clear	Click Clear to discard the information
Delete All	Select a device and delete one or all
Save	Click the Save button to save settings

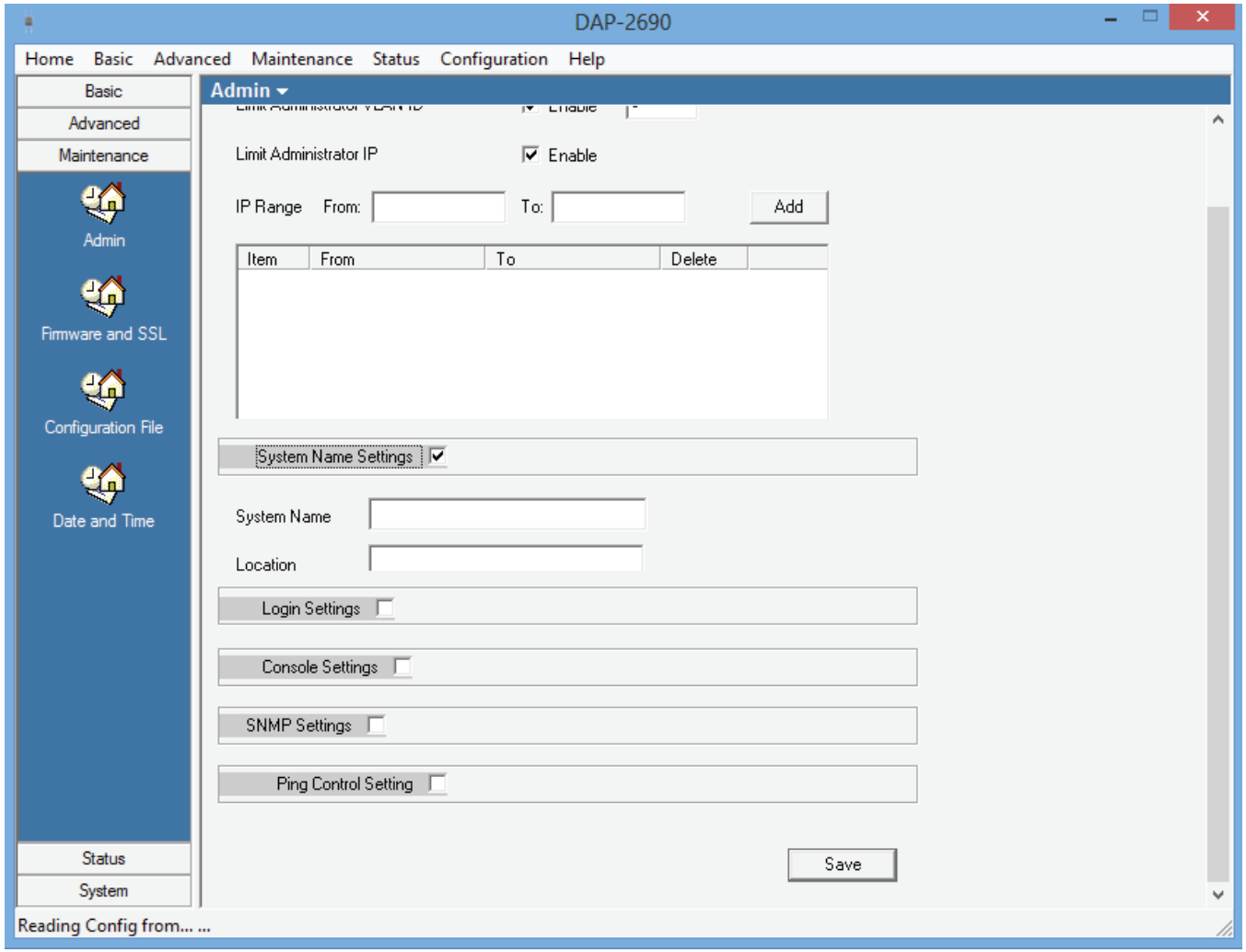
Maintenance - Admin

All devices need to be maintained and managed. Click on the link to proceed.



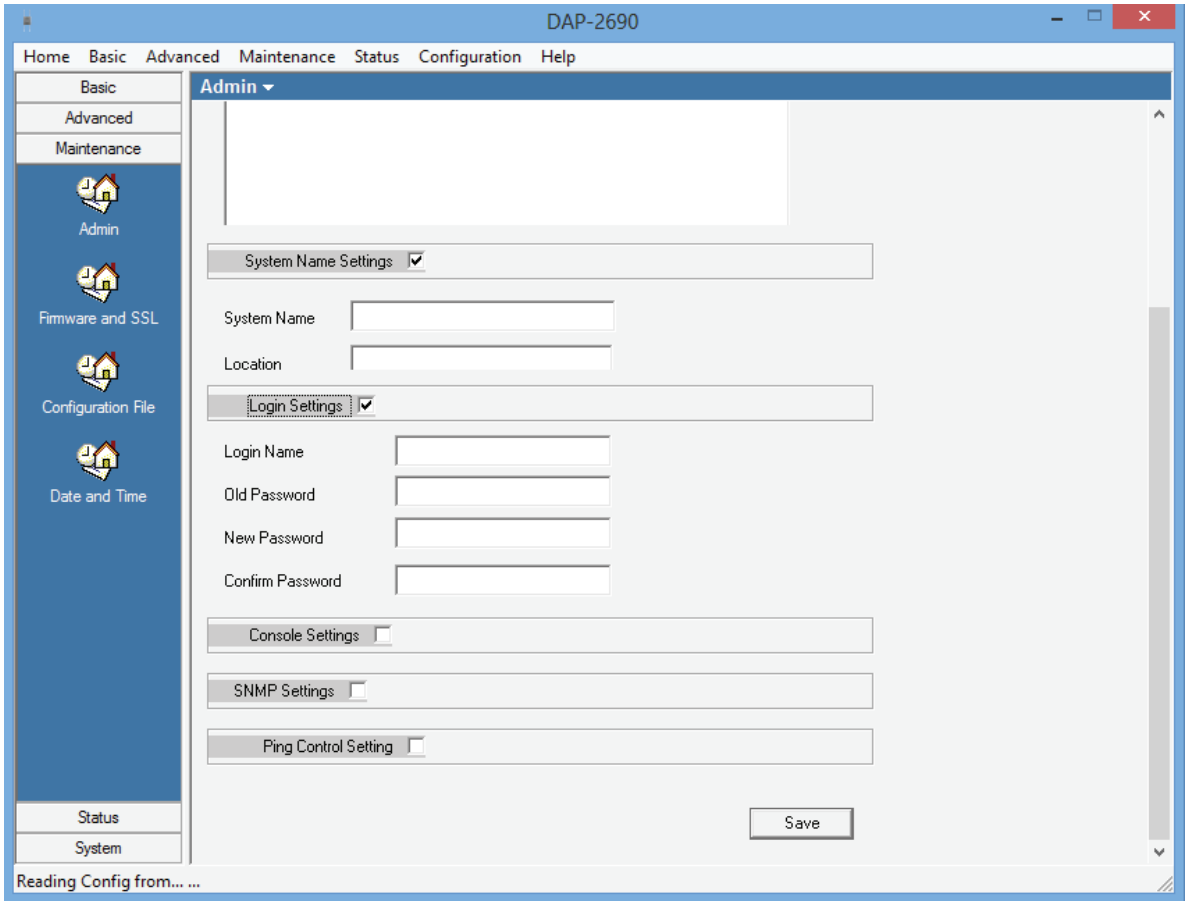
COMPONENT	DESCRIPTION
Limit Administrator	Click to Enable or Disable
Limit Administrator VLAN ID	Click the checkbox to enable this function and enter a value in the field provided
Limit Administrator IP	Click the checkbox to enable this function
IP Range	Enter a value in the From field, to the To field
Add	Click Add to include it to the Administration limitations
Save	Click the Save button to save settings

System Name Settings



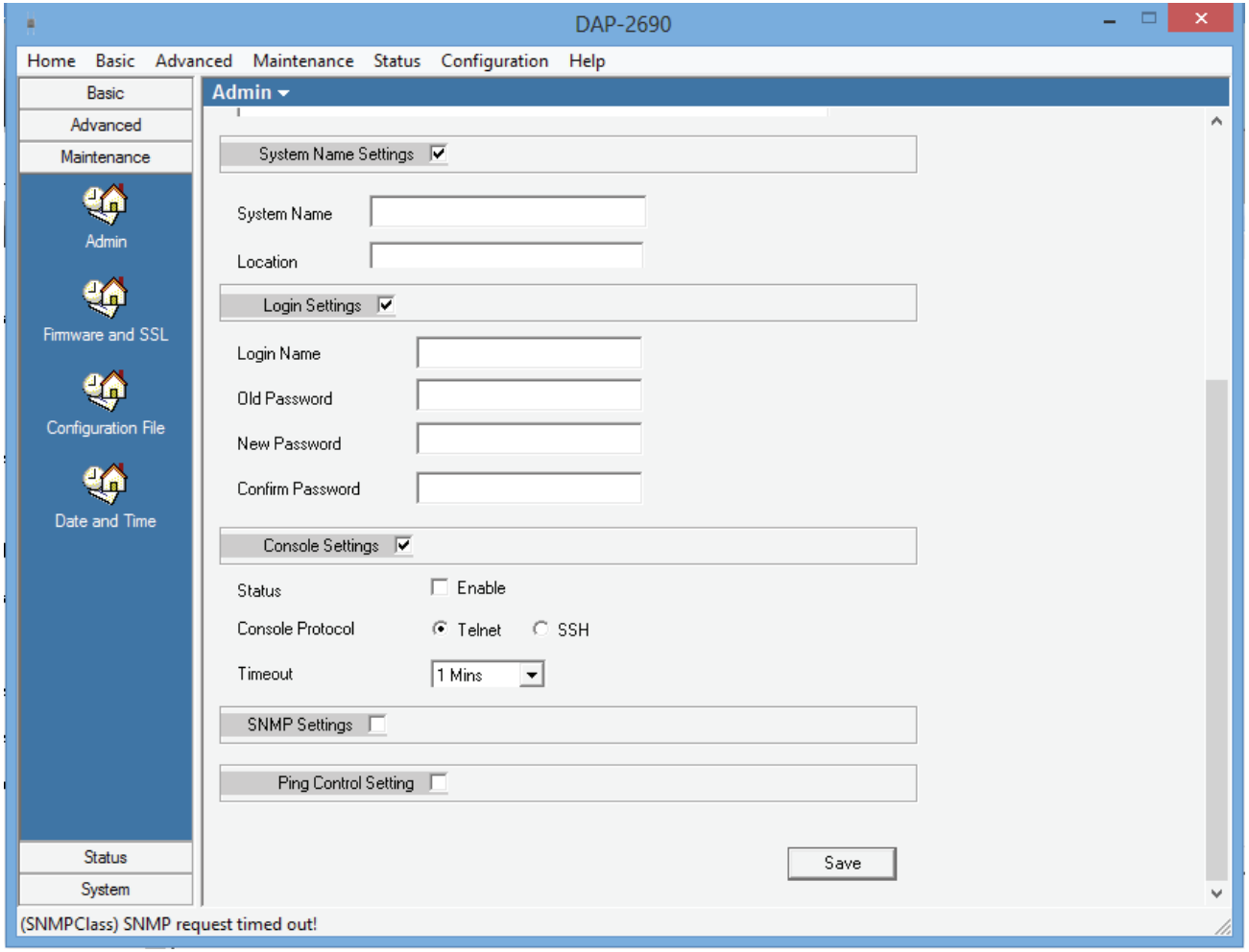
COMPONENT	DESCRIPTION
System Name Settings	Click to Enable or Disable
System Name	Enter a system name in the field provided
Location	Enter a location in the field provided
Save	Click the Save button to save settings

Login Settings



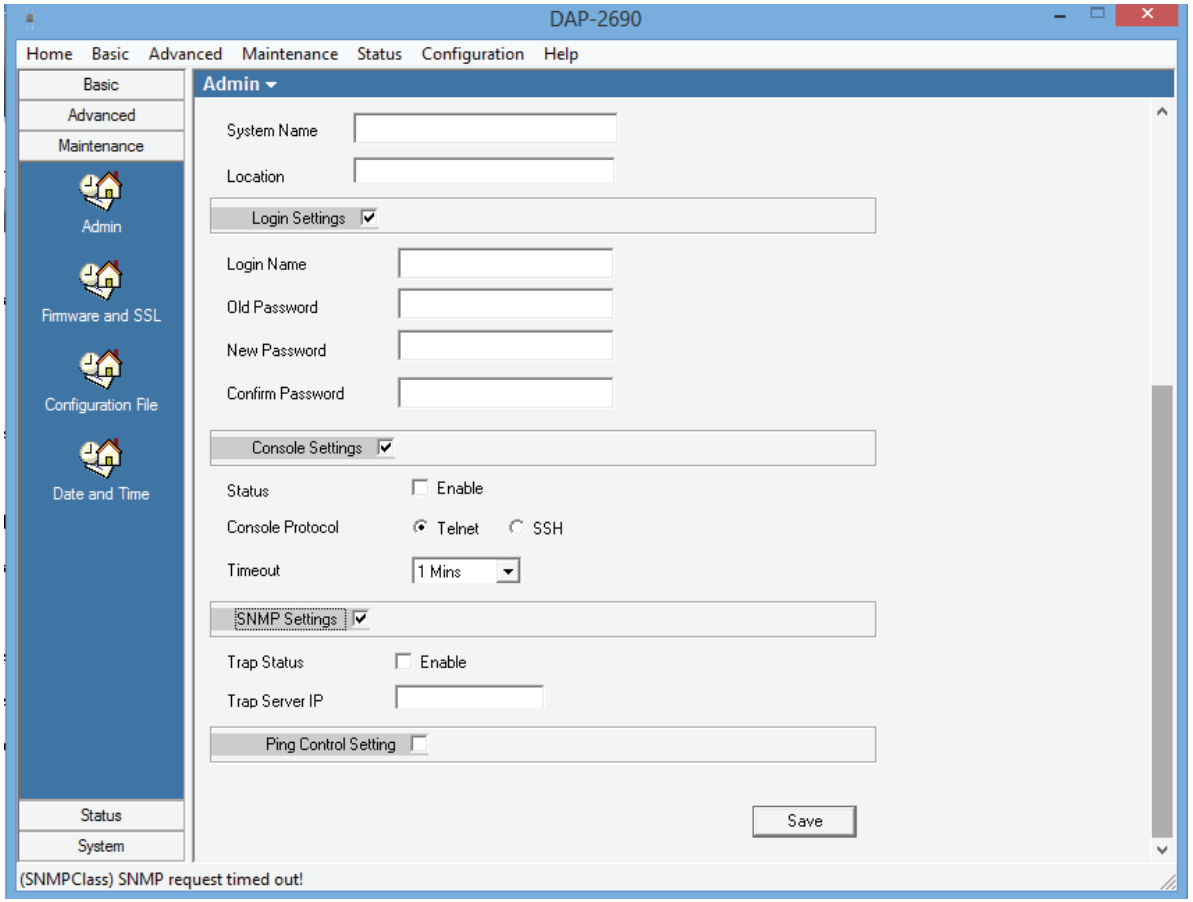
COMPONENT	DESCRIPTION
Login Settings	Click to Enable or Disable
Login Name	Enter a login name in the field provided
Old Password	Enter the old password details
New Password	Enter the new password details
Confirm Password	Enter the details to confirm your password details
Save	Click the Save button to save settings

Console Settings



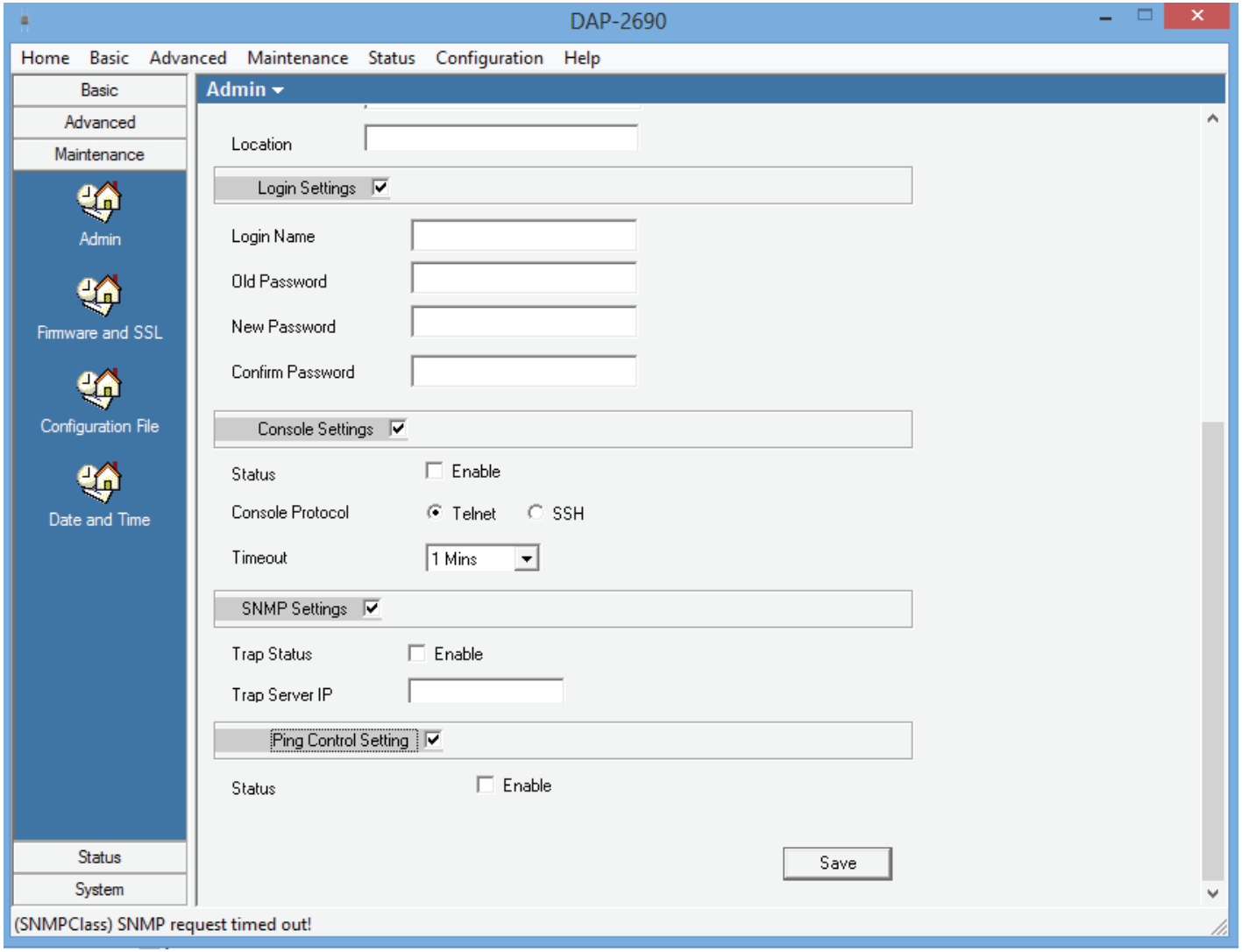
COMPONENT	DESCRIPTION
Console Settings	Click to Enable or Disable
Status	Click the checkbox to enable this feature
Console Protocol	Select between Telnet or SSH
Timeout	From the drop-down list, select from 1,3,5,10, 15 minutes or never
Save	Click the Save button to save settings

SNMP Settings



COMPONENT	DESCRIPTION
SNMP Settings	Click to Enable or Disable
Trap Status	Click the checkbox to enable this feature
Trap Server IP	Enter an IP address for trap messages
Save	Click the Save button to save settings

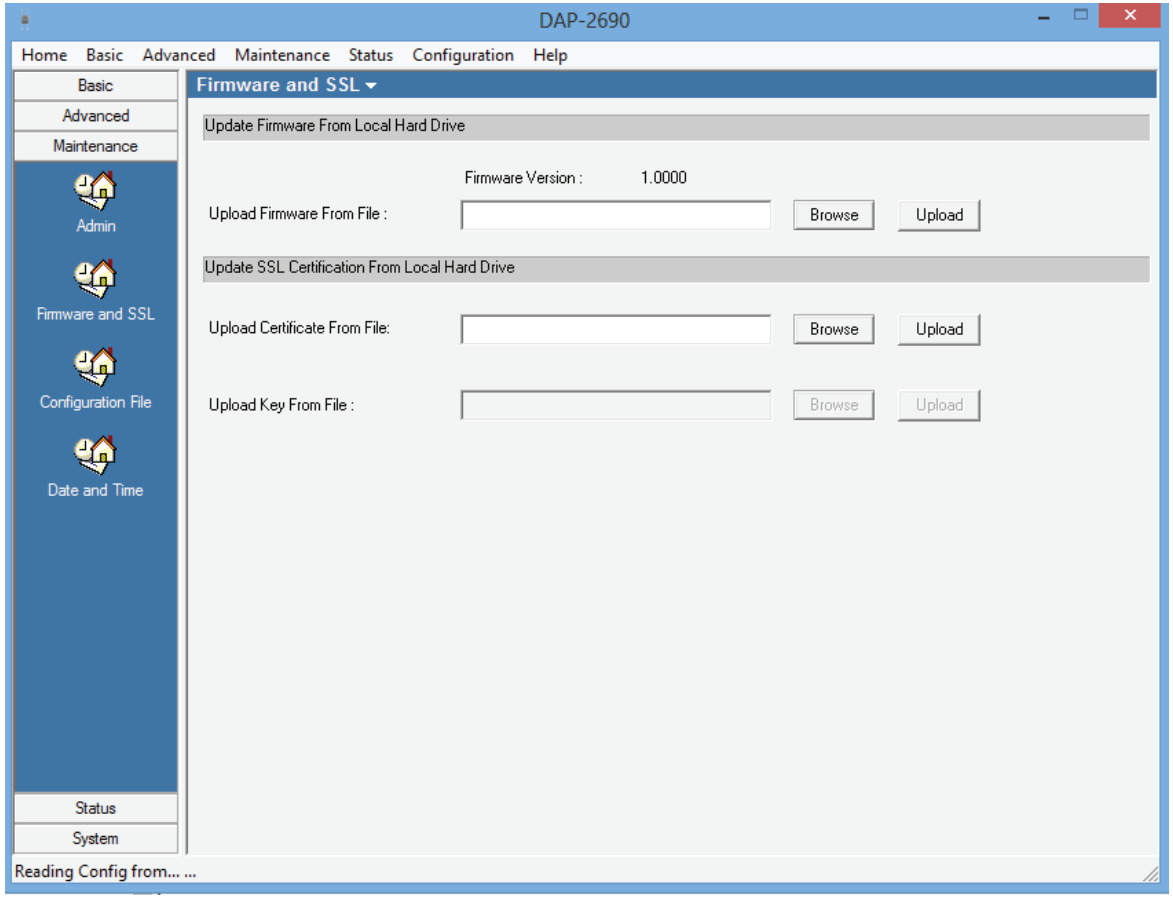
Ping Control Settings



COMPONENT	DESCRIPTION
Ping Control Settings	Click to Enable or Disable
Status	Click the checkbox to enable this feature
Save	Click the Save button to save settings

Maintenance - Firmware and SSL

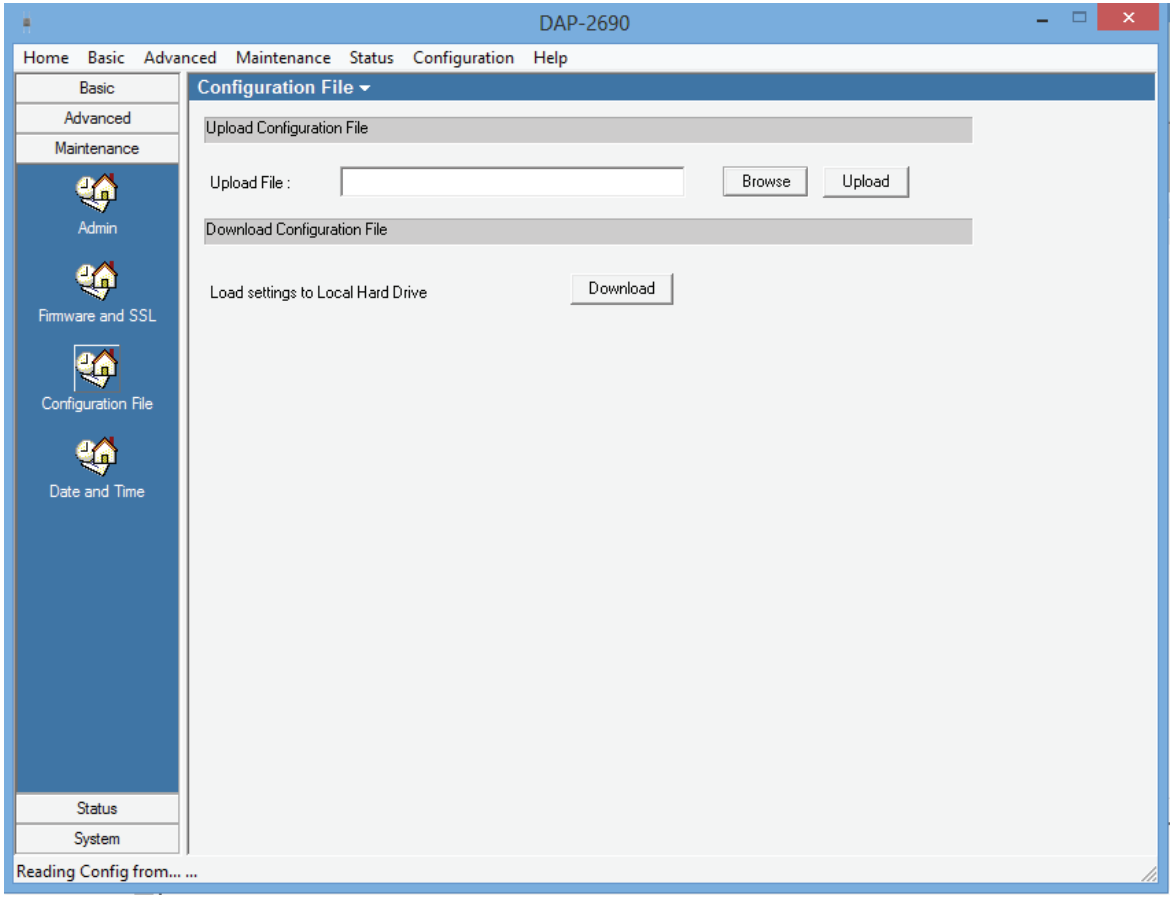
Use this function to update the firmware of the Access Point.



COMPONENT	DESCRIPTION
Update Firmware from Local Hard Drive	Click the Browse button to find the new firmware, select it, and upload the new firmware.
Upload Certificate from File	Click the Browse button to find the new SSL certificate, select it, and upload the new SSL certificate to the system
Upload Key From File	Click the Browse button to find the key, select it, and upload it to the Access Point

Maintenance - Configuration File

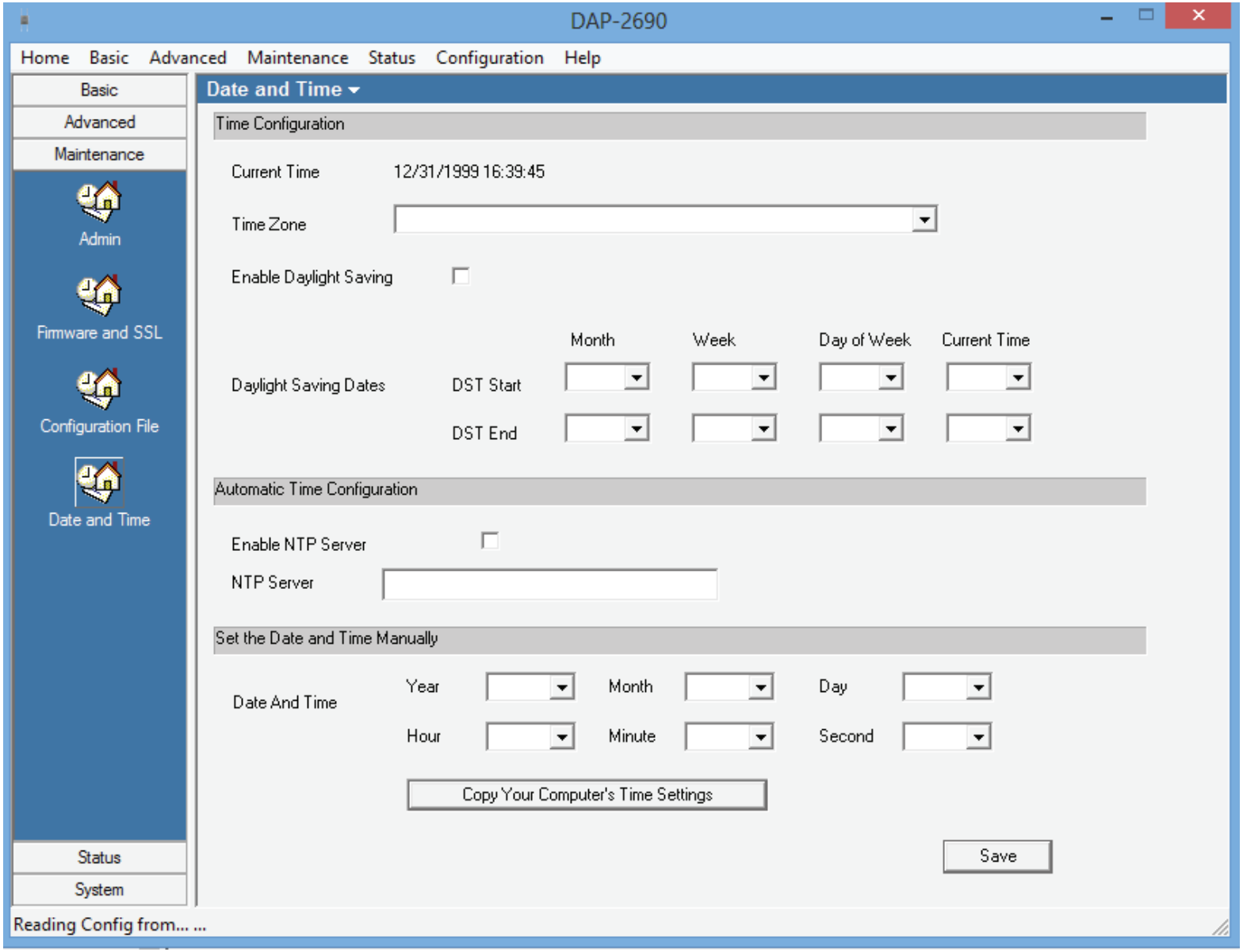
Use this function to configure one or many (in an array or separately) Access Points.



COMPONENT	DESCRIPTION
Upload Configuration File	Click the Browse button to find the Configuration file, select it, and upload the new firmware.
Download Configuration File	Click the Download button to download this file to your hard drive

Maintenance - Date and Time

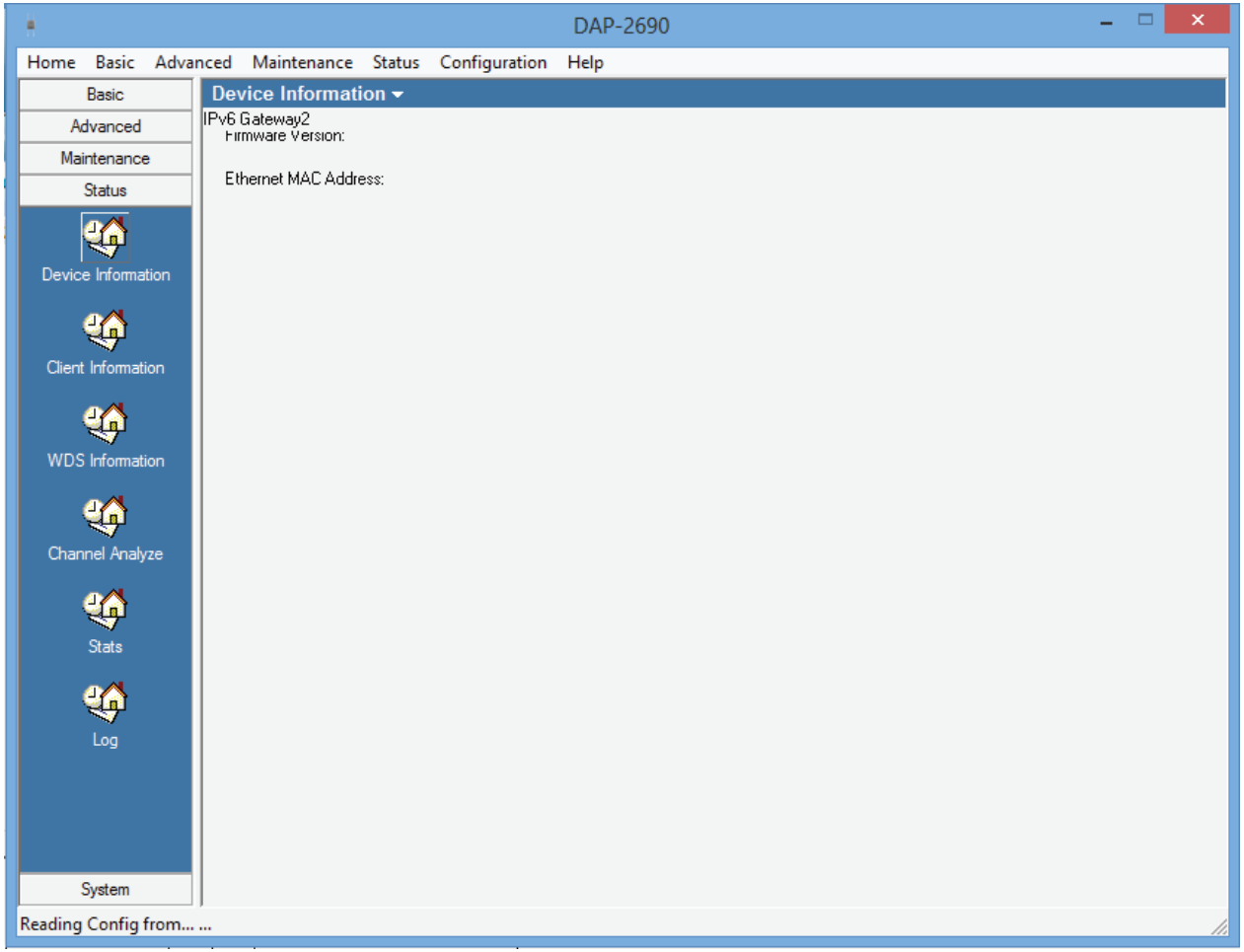
Use this function to configure the Date and Time sttings



COMPONENT	DESCRIPTION
Current Time	This is automatically set
Time Zone	Select a time zone from the drop-down list
Enable Daylight Saving	Click the checkbox to enable daylight savings time. Adjust the Daylight Saving Dates according to Month, Week, Day of the Week, and Current Time
Automatic Time Configuration	
Enable NTP Server	Click the checkbox to enable the NTP Server
NTP Server	Enter the NTP Server IP address
Set the Date and Time Manually	Enter the date and time settings according to the year/month/day, hour/ minute/second to manually confgiure the time
Copy Your Computer's Time Settings	Click this button to have the time synced with your computer
Save	Click the Save button to save settings

Status - Device Information

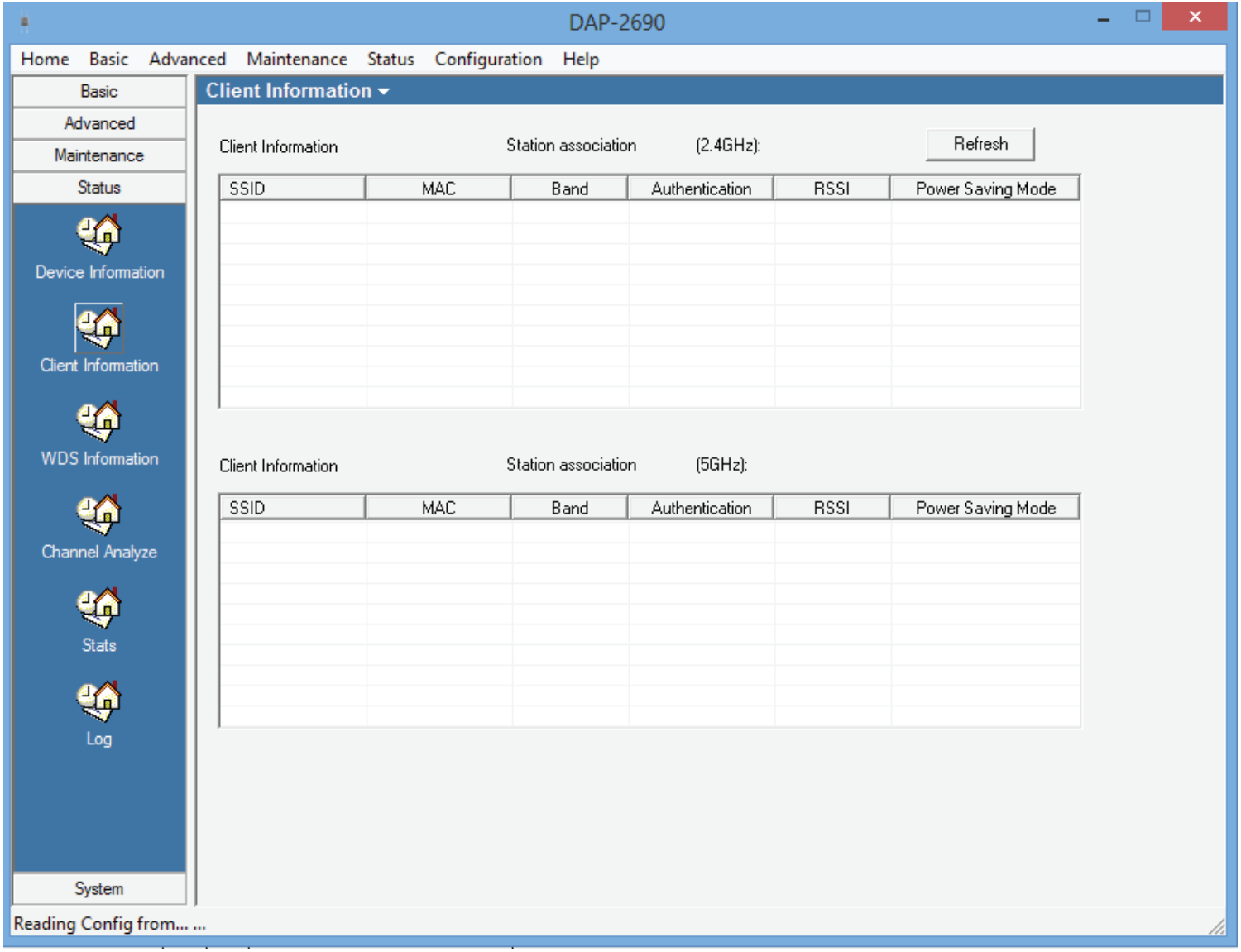
The Status section allows you to configure parameters pertaining to the current conditions of your Access Point. All statistics and functions can be analysed for clarity.



COMPONENT	DESCRIPTION
IPv6 Gateway2 Firmware Version	Describes the firmware version and number
Ethernet MAC Address	Describes the Access Points MAC details

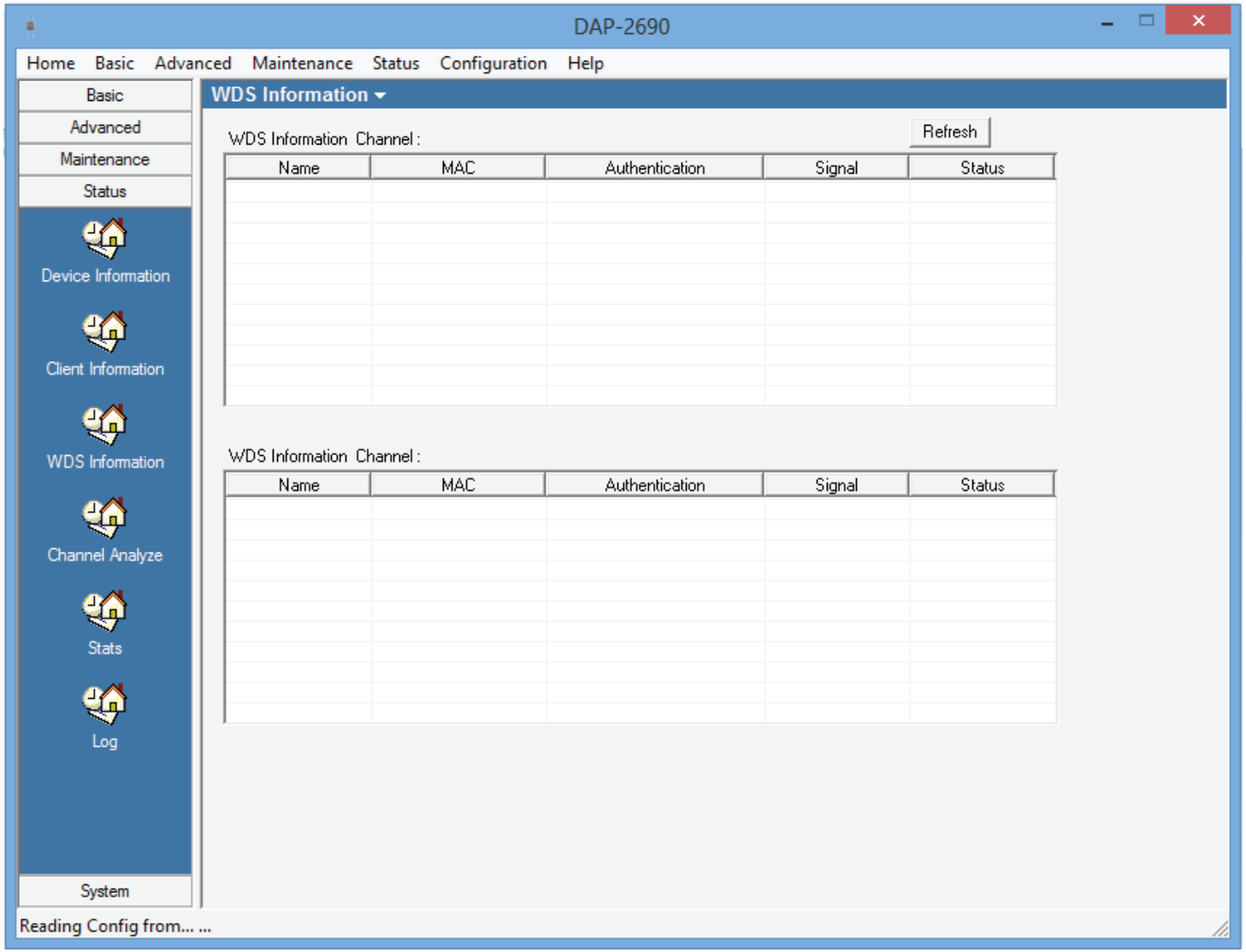
Status - Client Information

The Client Information section denotes all information about the clients attached to the main Access Point. The table below shows all client access points attached to it. It provides information on SSID, MAC address, Band, Authentication, RSSI, and Power Saving Mode. Click the Refresh button to keep monitoring the devices. You can view the 2.4GHz and 5GHz spectrum.



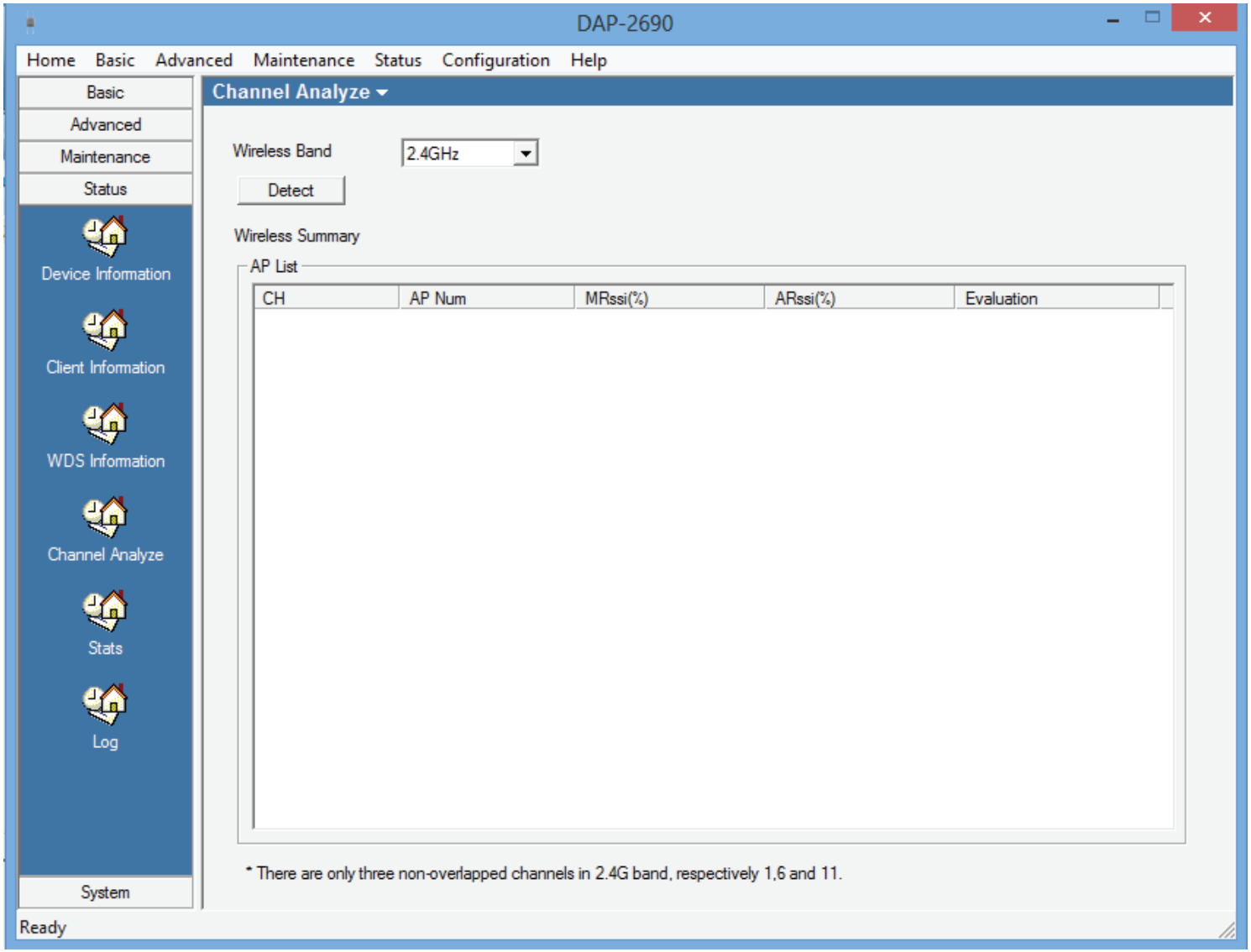
Status - WDS Information

Wireless Distribution System is a technology that reads the wireless interconnection of Access Points. It allows for the expansion of multiple access points. This section displays information on the Channel name, the MAC address details, the Authentication, the Signal strength, and the Status.



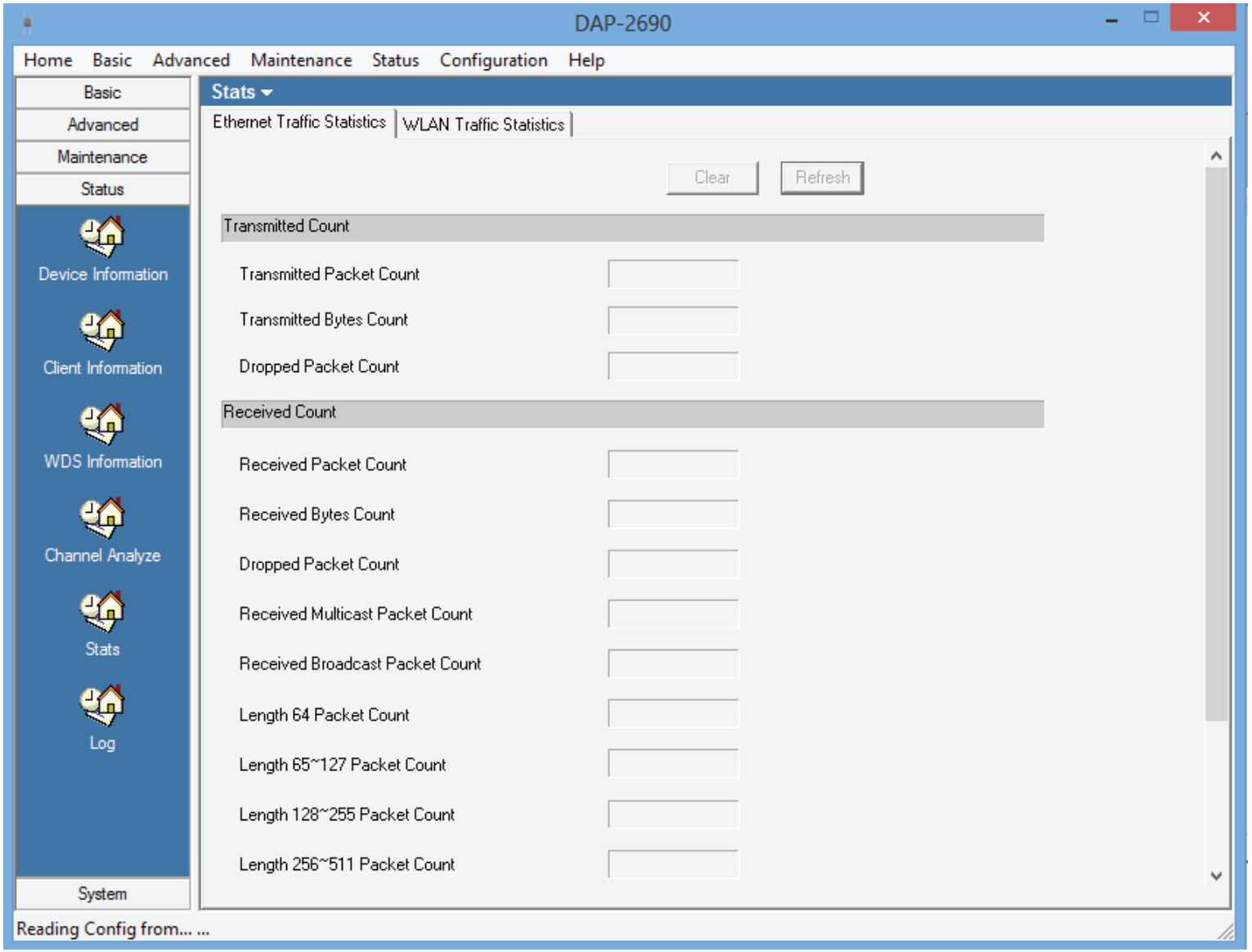
Status - Channel Analyze

Channel Analyze is a section where each wireless band is analyzed for quality and strength. Select either 2.4GHz or 5GHz. Click the Detect button. All summarized information will be displayed on the AP list. Information displayed are: Channel, Access Point number, MRssi percentage, and Evaluation.



Status - Stats - Ethernet Traffic Statistics

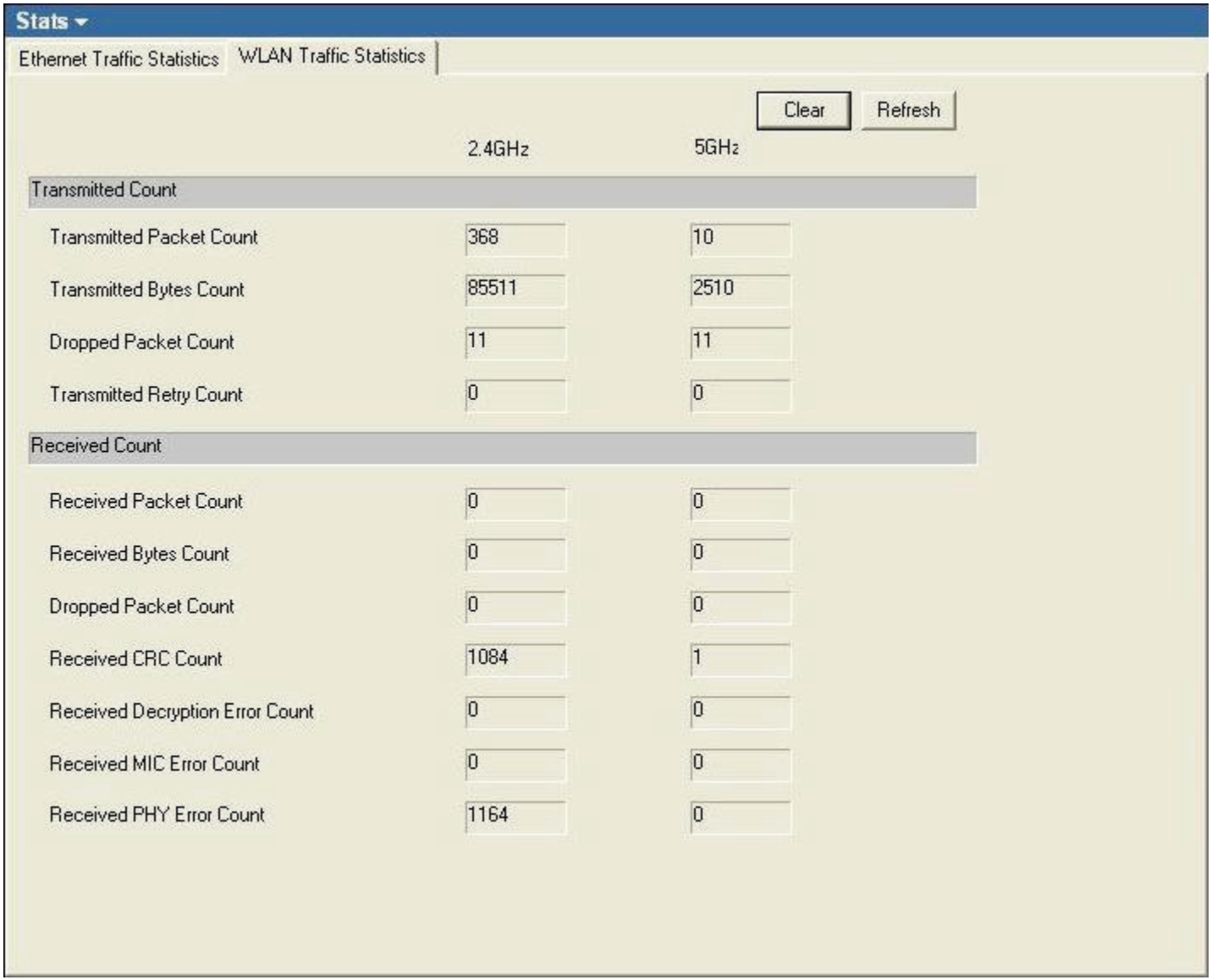
The Stats seciton provides information on Ethernet Traffic Statistics and WLAN Traffic Statistics.



COMPONENT	DESCRIPTION
Clear	Click the Clear button to delete all stats posted
Refresh	Click the Refresh button to display an up-to-date stat report
Transmitted Count	
Transmitted Packet Count	Displays the transmitted packets
Transmitted Byte Count	Displays the transmitted bytes
Dropped Packet Count	Displays the amount of packets dropped
Received Count	
Received Packet Count	Displays the packets received
Received Byte Count	Displays the bytes received
Dropped Packet Count	Displays the amount of packets dropped
Received Multicast Packet Count	Displays the multicast packets
Received Broadcast Packet Count	Displays the broadcasted packets
Length 64 Packet Count	Dsiplays 64 bit packet data
Length 65~127 Packet Count	Displays the packet in that data range
Length 128~255 Packet Count	Displays the packets in that data range
Length 256~511 Packet Count	Displays the packets in that data range
Length 512~1023 Packet Count	Displays the packets in that data range
Length 1024~1518 Packet Count	Displays the packets in that data range
Length 1519~max. Packet Count	Displays the packets in that data range

Status - Stats - WLAN Traffic Statistics

The Stats seciton provides information on Ethernet Traffic Statistics and WLAN Traffic Statistics.

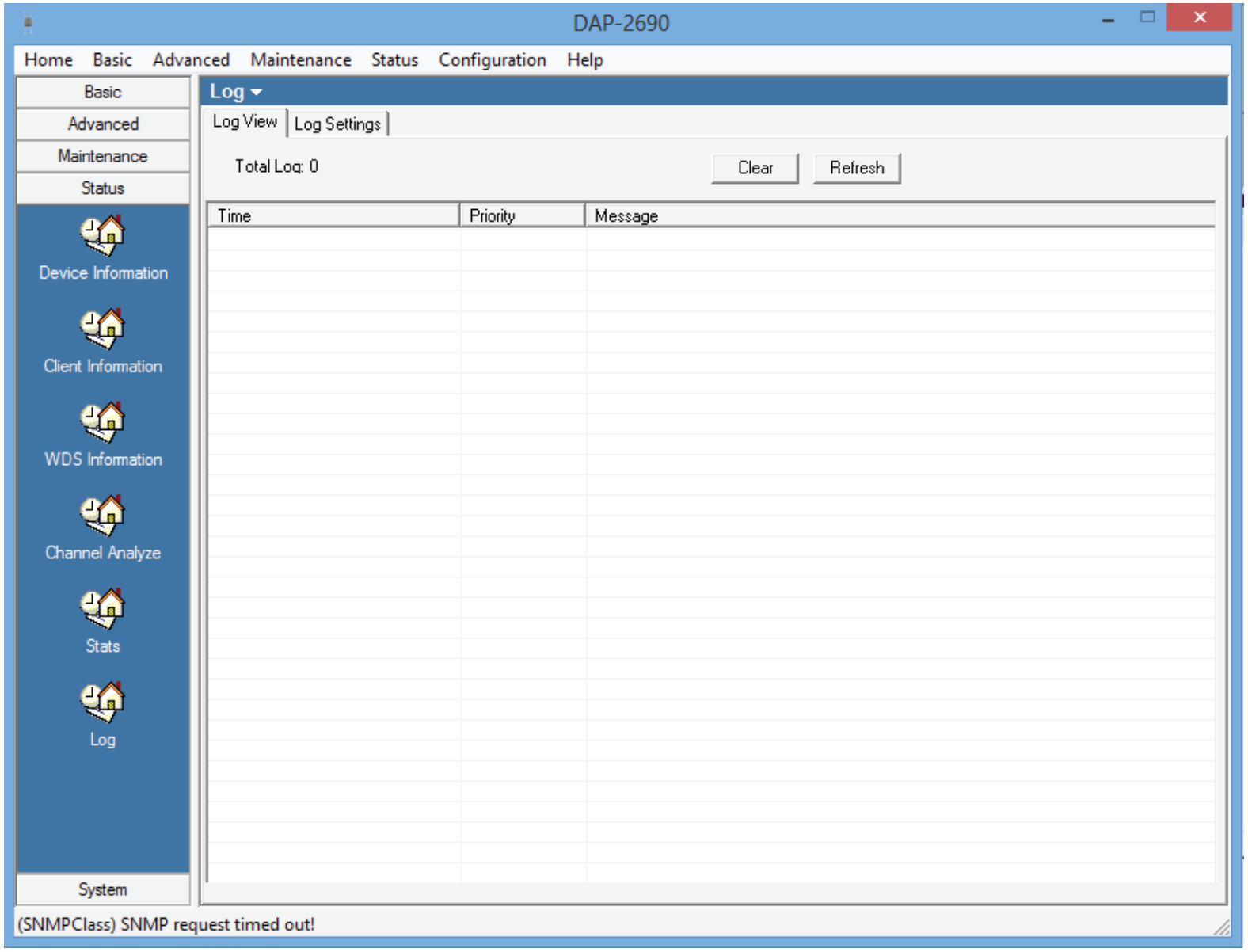


These statistical information are presented in 2.4GHz and 5GHz formats.

COMPONENT	DESCRIPTION
Clear	Click the Clear button to delete all stats posted
Refresh	Click the Refresh button to display an up-to-date stat report
Transmitted Count	
Transmitted Packet Count	Displays the transmitted packets
Transmitted Byte Count	Displays the transmitted bytes
Dropped Packet Count	Displays the amount of packets dropped
Received Count	
Received Packet Count	Displays the packets received
Received Byte Count	Displays the bytes received
Dropped Packet Count	Displays the amount of packets dropped
Received Multicast Packet Count	Displays the multicast packets
Received Broadcast Packet Count	Displays the broadcasted packets
Length 64 Packet Count	Dsiplays 64 bit packet data
Length 65~127 Packet Count	Displays the packet in that data range
Length 128~255 Packet Count	Displays the packets in that data range
Length 256~511 Packet Count	Displays the packets in that data range
Length 512~1023 Packet Count	Displays the packets in that data range
Length 1024~1518 Packet Count	Displays the packets in that data range
Length 1519~max. Packet Count	Displays the packets in that data range

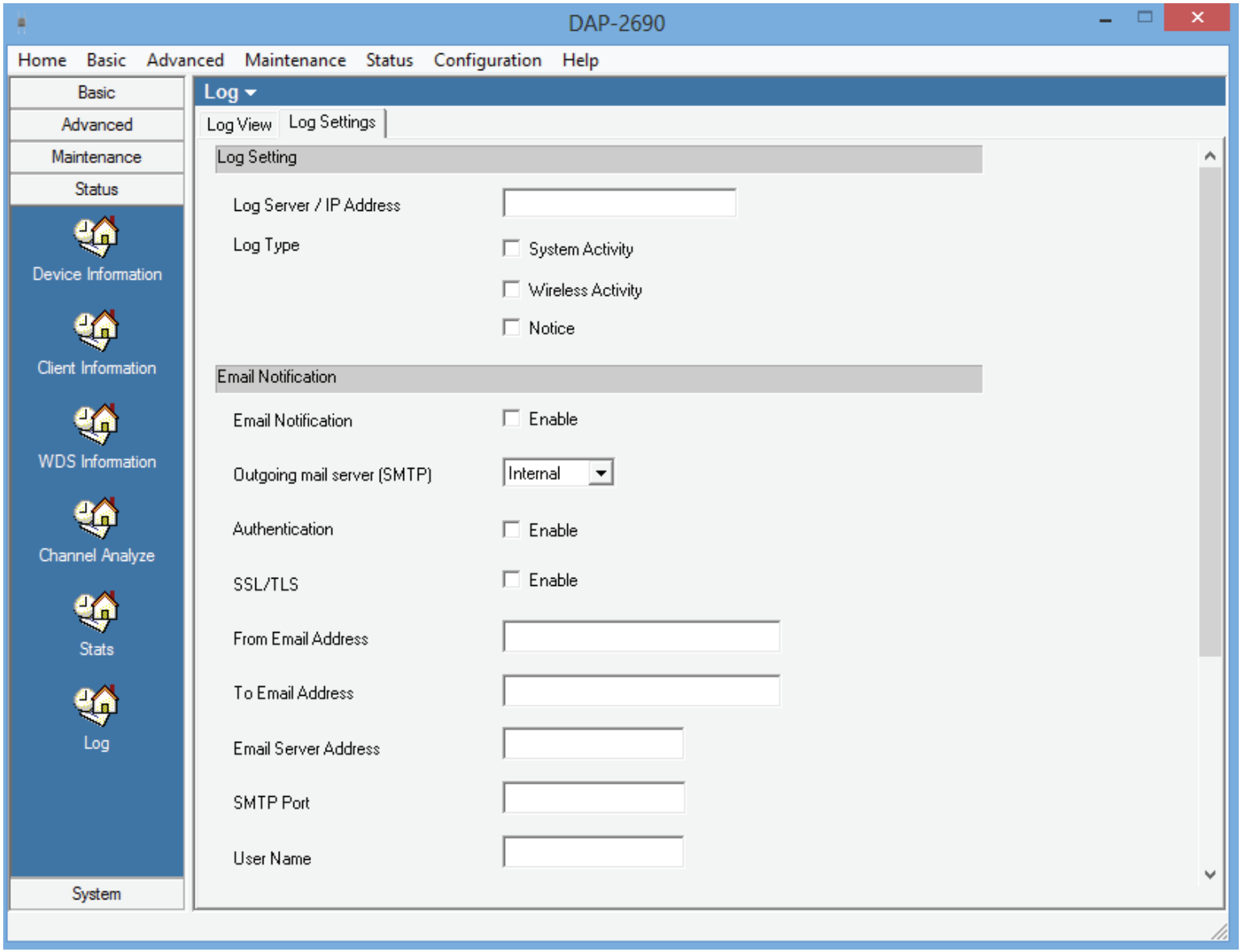
Status - Log - Log View

The Log section is divided into two parts, Log View and Log Settings. Under Log View click Clear to restart the log process and click Refresh to renew log information.



Status - Log - Log Settings

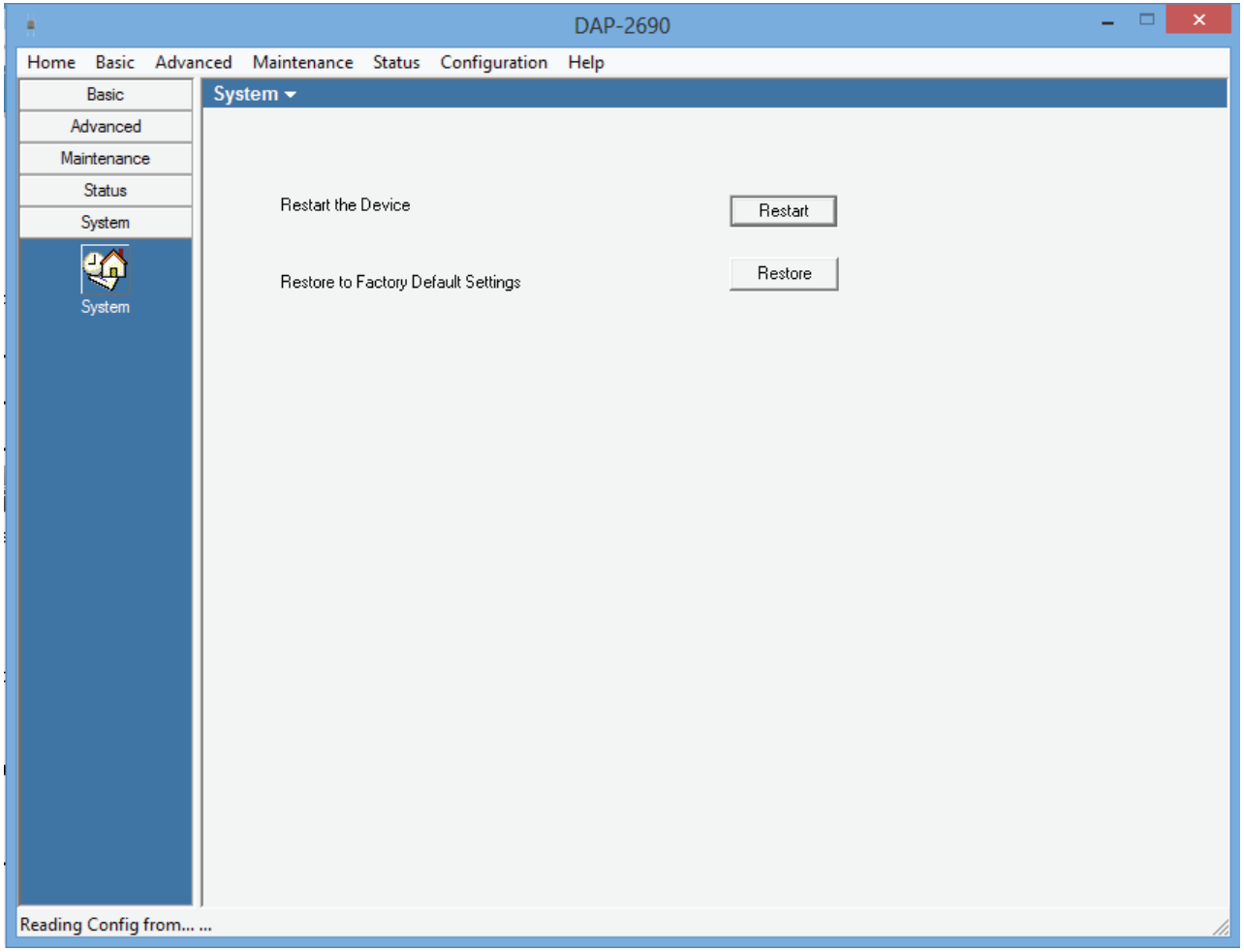
Change the Log Settings here based on the following criteria:



COMPONENT	DESCRIPTION
Log Server/IP Address	Enter the log server IP address information
Log Type	Click the checkbox to activate logging for System Activity Click the checkbox to activate logging for Wireless Activity Click the checkbox to activate logging for notifications
Email Notifications	
Email Notifications	Click the checkbox to Enable
Outgoing mail server	Select from internal mail server, Gmail server or Hotmail server
Authentication	Click the checkbox to enable
SSL/TLS	Click the checkbox to enable
From Email Address	Enter the email address details in this field
To Email Address	Enter the email address details in this field
Email Server Address	Enter the email server address details here
SMTP Port	Enter the port details here
User Name	Enter the username you wish to use
Password	Enter the password details here
Confirm Password	Enter the password a second time to reconfirm it
Email Log Schedule	
Schedule	Schedule within the time frame provided on the drop-down list
Save	Click the Save button to save your configuration

System

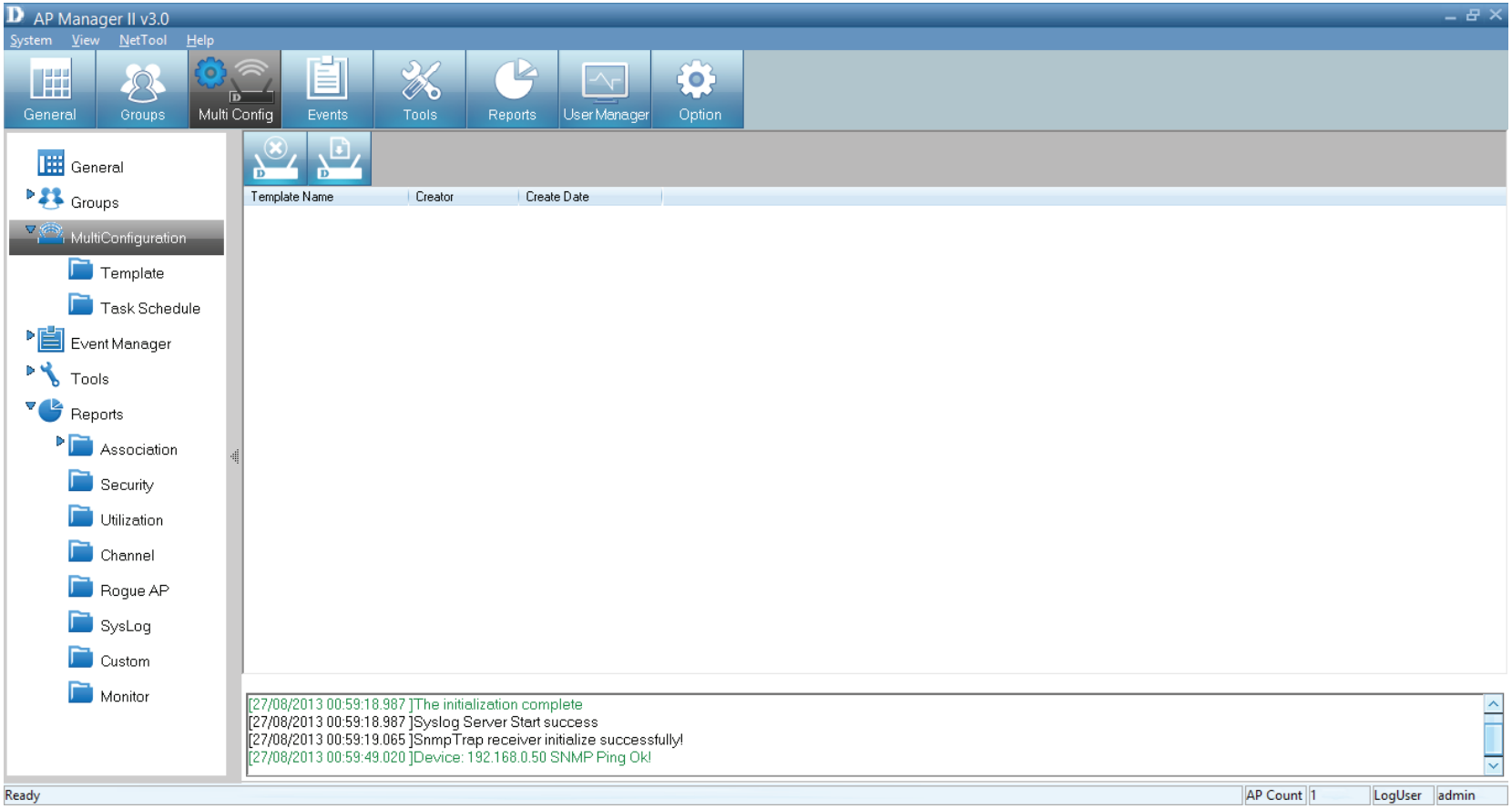
System, allows you to return to factory default and restart the device



COMPONENT	DESCRIPTION
Restart the Device	Click the Restart button to restart the device
Restore to Factory Default Settings	Click the Restore button to go back to factory settings

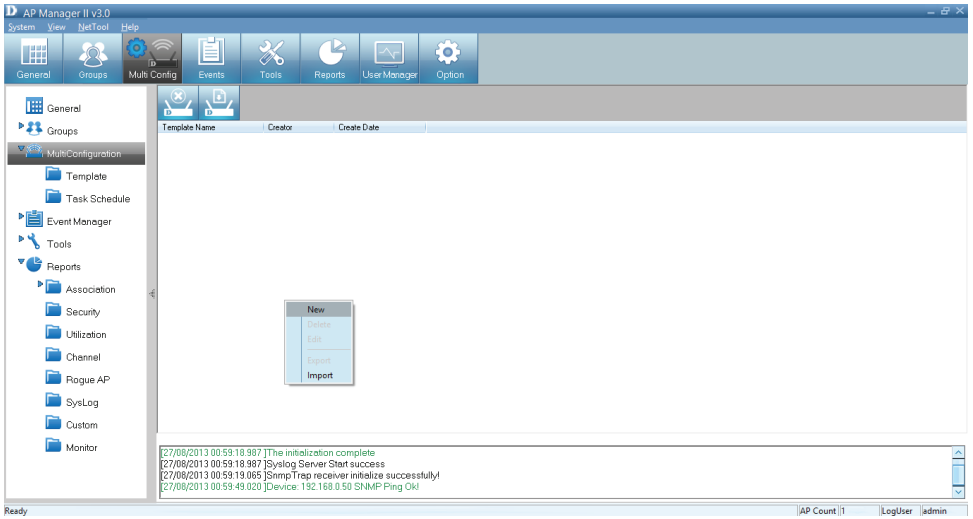
AP Manager II v3.0 - Multi Configuration

Administrators can manage the configuration of Access Points. AP Manager II v3.0 does this using a template. The same profile can be used for multiple Access Points. Each template profile has unique settings which include System, Wireless, Security and Filter settings.



AP Manager II v3.0 - Multi Configuration - Create a new template

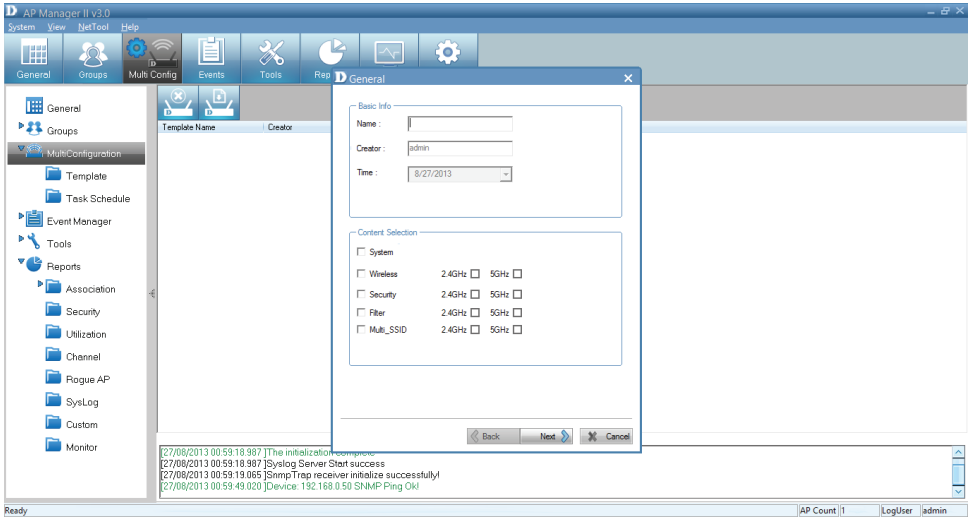
To create a new template, right-click anywhere on the template view window and select the New item.



Under **General**, **Basic Info** type in a name for the new configuration. A **creator** is already selected under **Admin**, the time is already set.

Under **Content Selection**, click the checkbox to configure. There are **System**, **Wireless** (2.4GHz/5GHz), **Security** (2.4GHz/5GHz), **Filter** (2.4GHz/5GHz), and **Multi_SSID** (2.4GHz/5GHz) options.

Click **Next** to continue.

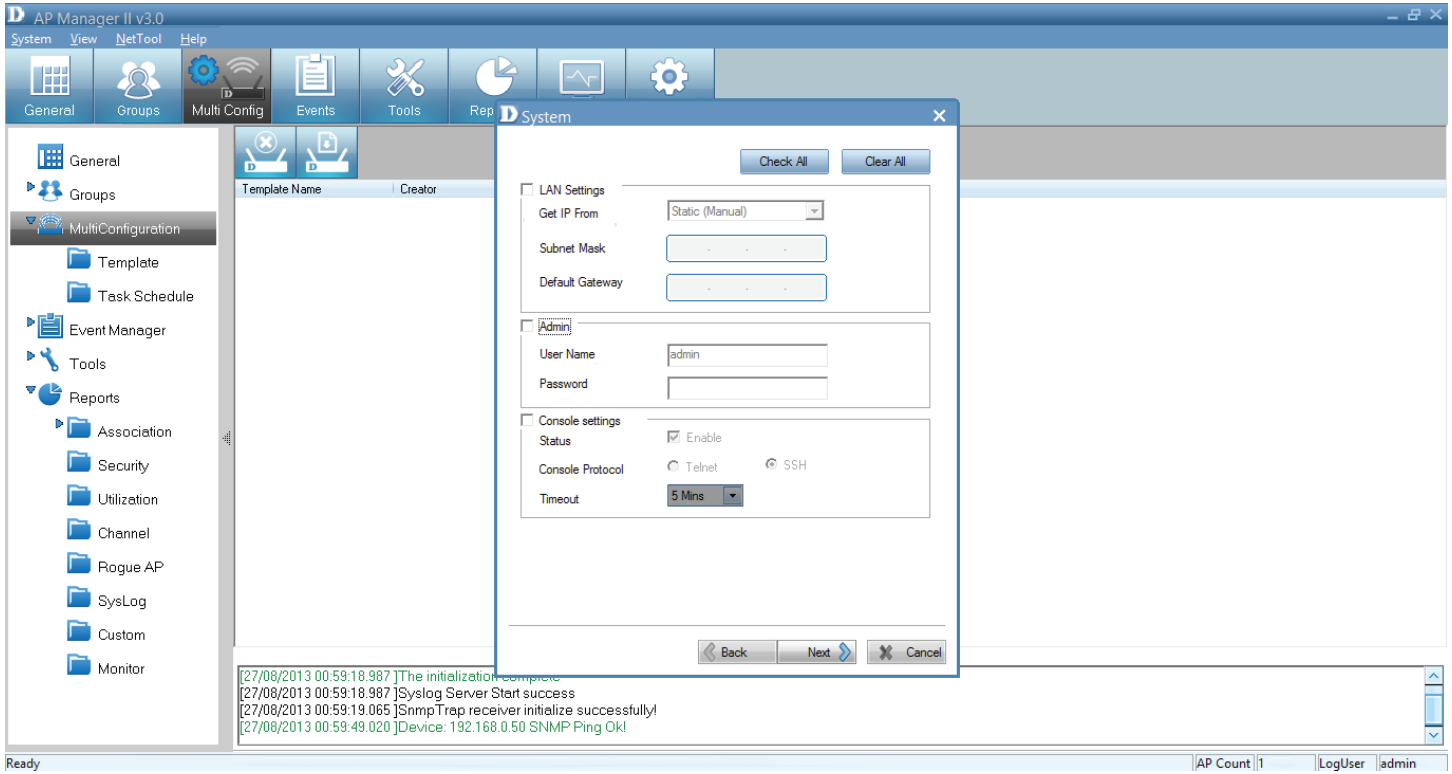


Under **System**, click the **LAN Settings** checkbox and configure the **IP (Static or Dynamic)**, enter **Subnet** details, and **Default Gateway** options.

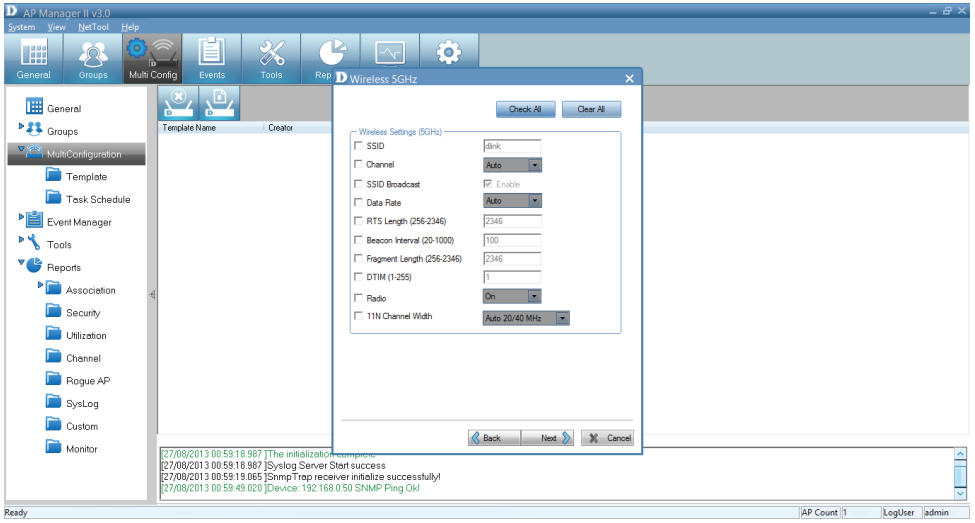
For **Admin**, enter a **username and password**

For **Console Settings**, select to enable it, select the **Console Protocol** and the **timeout** period.

Click **Next** to continue



Under **Wireless 5GHz**, you have the option to set the following:

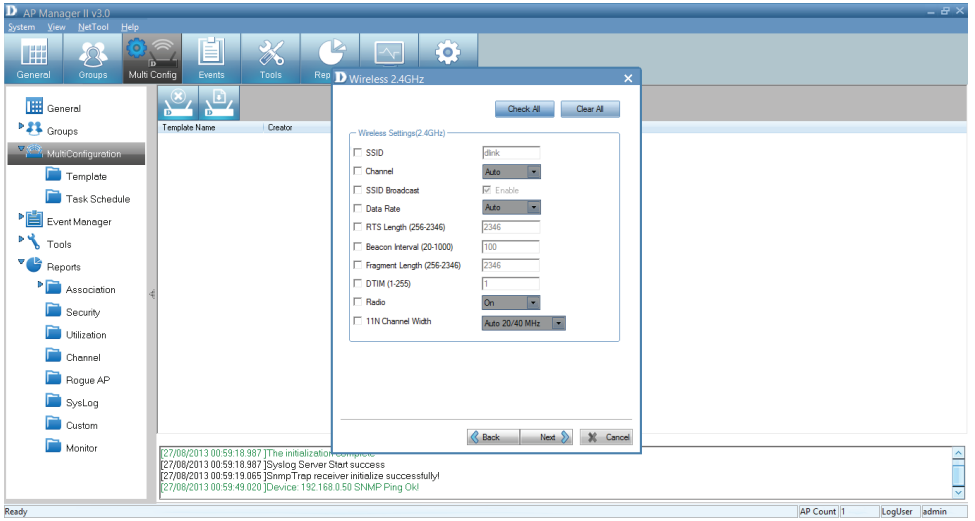


SSID - Enter a name for the SSID
Channel - Select between Auto or a configurable range
SSID Broadcast - Click to enable it
Data Rate - Select Auto or the speed option
RTS Length - Enter a range
Beacon Interval - Enter a range
Fragment Length - Enter a value
DTIM - Enter an appropriate value
Radio - Select to turn this feature on or off
11n Channel Width - Select the range

If you are unsure of all the settings, there is also the option to **Check All**.

Click **Next** to continue

Under **Wireless 2.4GHz**, you have the option to set the following:

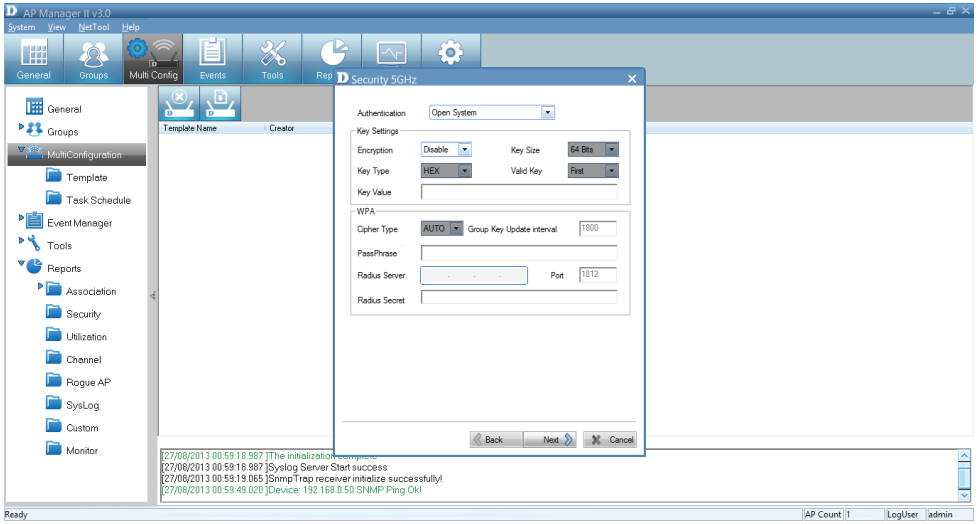


SSID - Enter a name for the SSID
Channel - Select between Auto or a configurable range
SSID Broadcast - Click to enable it
Data Rate - Select Auto or the speed option
RTS Length - Enter a range
Beacon Interval - Enter a range
Fragment Length - Enter a value
DTIM - Enter an appropriate value
Radio - Select to turn this feature on or off
11n Channel Width - Select the range

If you are unsure of all the settings, there is also the option to **Check All**.

Click **Next** to continue

Under **Security 5GHz**, you have the option to set the following:



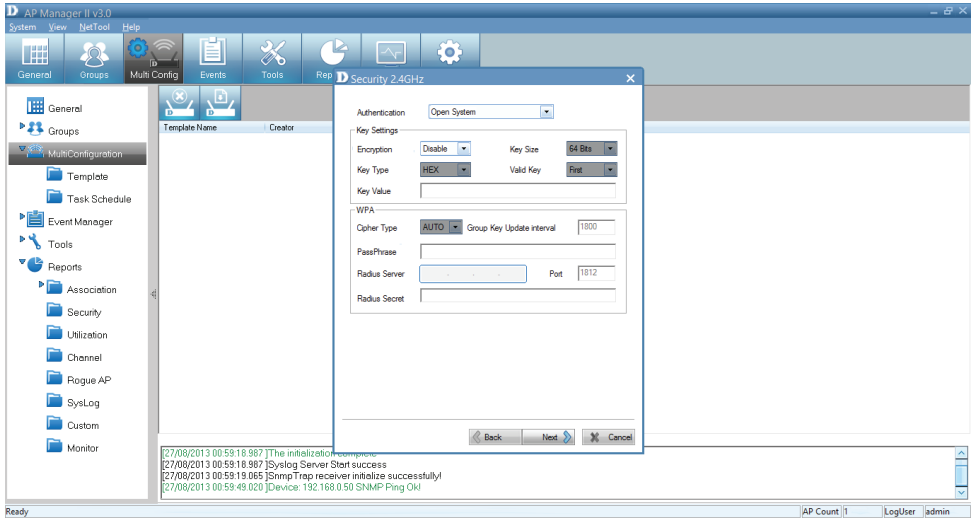
Authentication - Select between an Open System, Shared Key, Open System/Shared Key, WPA-Personal, WPA-Enterprise, WPA2-Personal, WPA2-Enterprise, WPA-Auto-Personal, and WPA-Auto-Enterprise

Key Settings - Select to enable the device then Key Type, Key Size, Valid Key, and Key Value

WPA - Set the following parameters: Cipher Type, Group Key Update Interval, Pass Phrase, RADIUS Server, Port, and RADIUS Secret.

Click **Next** to continue.

Under **Security 2.4GHz**, you have the option to set the following:



Authentication - Select between an Open System, Shared Key, Open System/Shared Key, WPA-Personal, WPA-Enterprise, WPA2-Personal, WPA2-Enterprise, WPA-Auto-Personal, and WPA-Auto-Enterprise

Key Settings - Select to enable the device then Key Type, Key Size, Valid Key, and Key Value

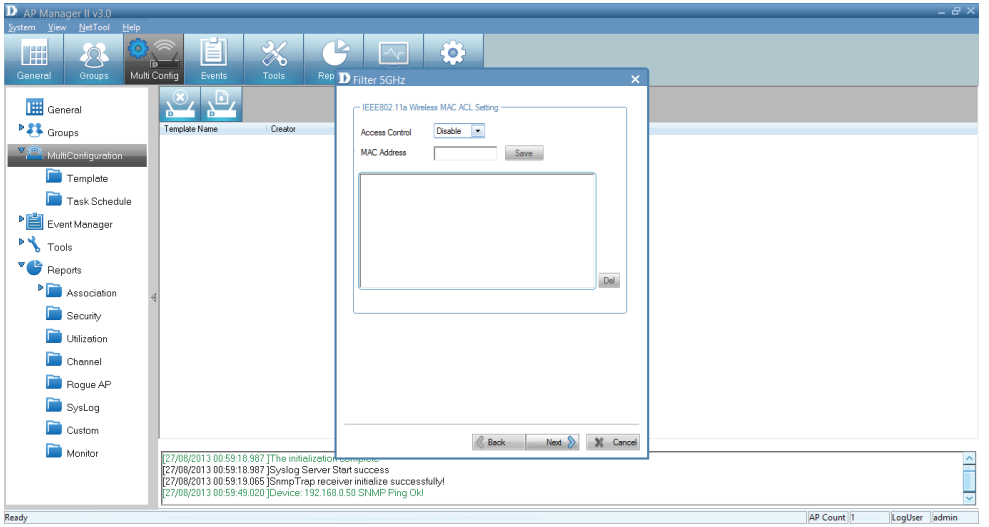
WPA - Set the following parameters: Cipher Type, Group Key Update Interval, Pass Phrase, RADIUS Server, Port, and RADIUS Secret.

Click **Next** to continue.

Under **Filter 5GHz,** the IEEE802. 11a Wireless MAC ACL Settings, select the Access Control method, enter a MAC Address, and click Save.

Use **Del** if you wish to delete an item.

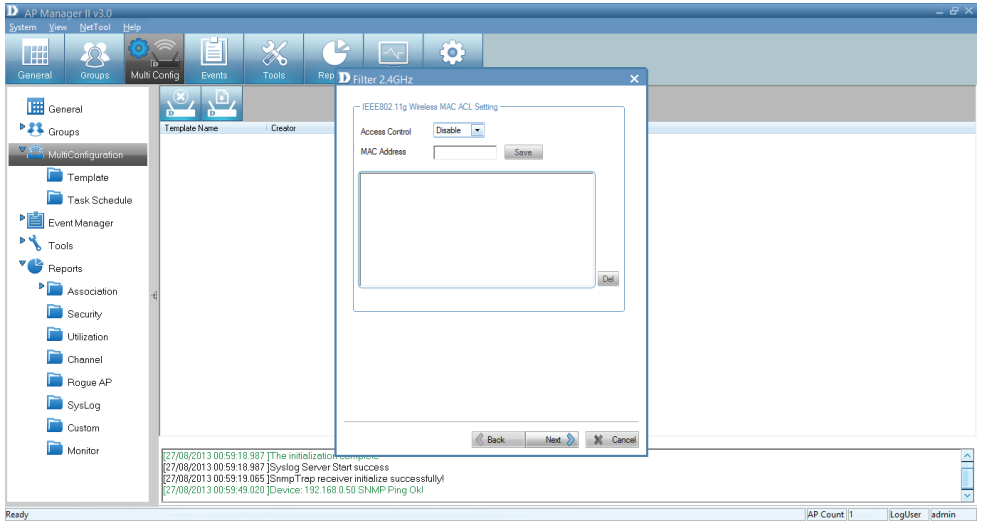
Click **Next** to continue.



Under **Filter 2.4GHz,** the IEEE802. 11a Wireless MAC ACL Settings, select the Access Control method, enter a MAC Address, and click Save.

Use **Del** if you wish to delete an item.

Click **Next** to continue.

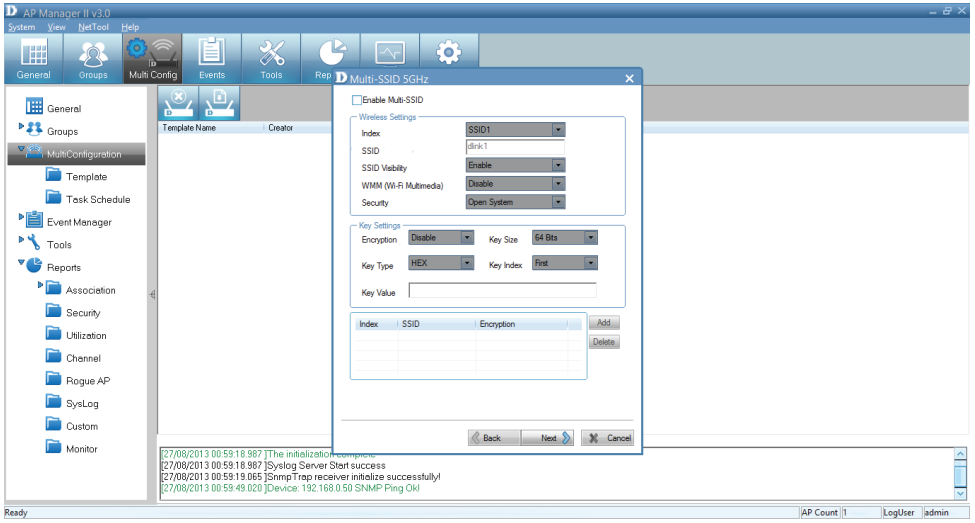


Under **Multi SSID 5GHz,** select to enable the feature. The Wireless Settings allow you to index it by SSID number or name. Enter an SSID name, select the SSID visibility, select to enable/disable WMM settings, and select a Security method.

Key Settings - Select to enable the device then Key Type, Key Size, Valid Key, and Key Value

The table below populates with data. Use the Add button to add info or the Delete button to delete parameters.

Click **Next** to continue.

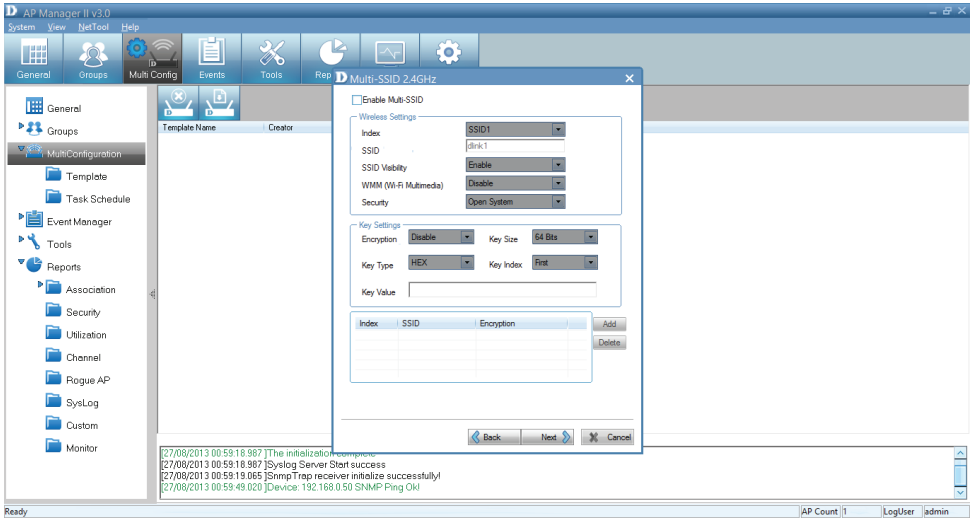


Under **Multi SSID 5GHz,** select to enable the feature. The Wireless Settings allow you to index it by SSID number or name. Enter an SSID name, select the SSID visibility, select to enable/disable WMM settings, and select a Security method.

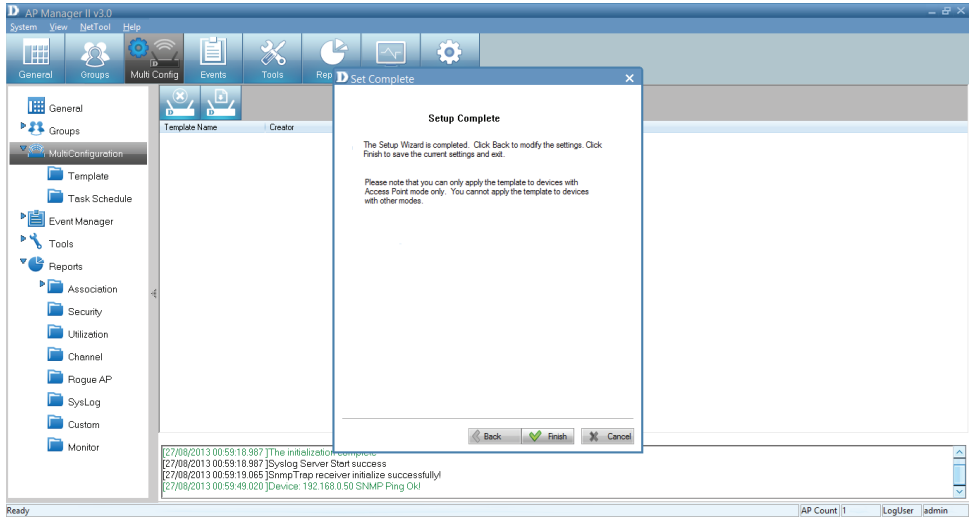
Key Settings - Select to enable the device then Key Type, Key Size, Valid Key, and Key Value

The table below populates with data. Use the Add button to add info or the Delete button to delete parameters.

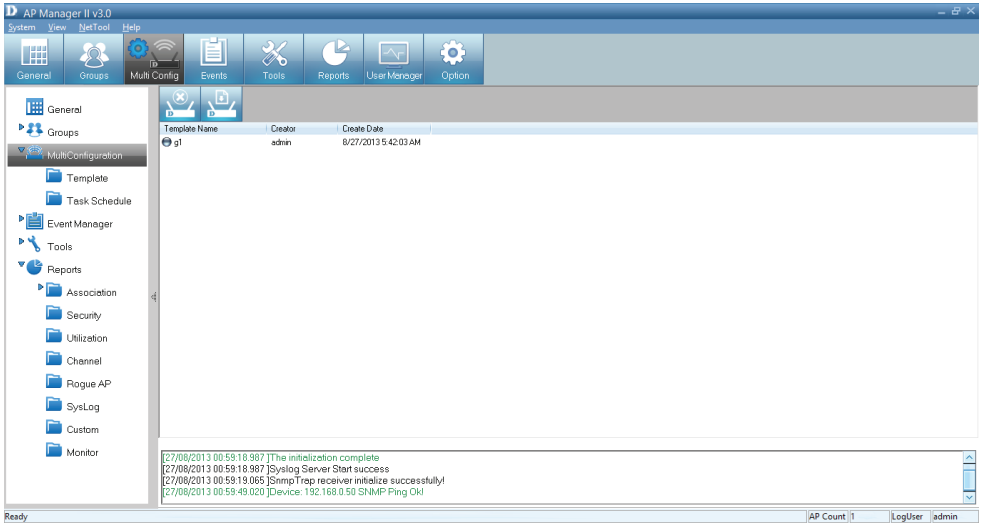
Click **Next** to continue.



The **Template setup** is complete. Read the instructions and click **Finish**.

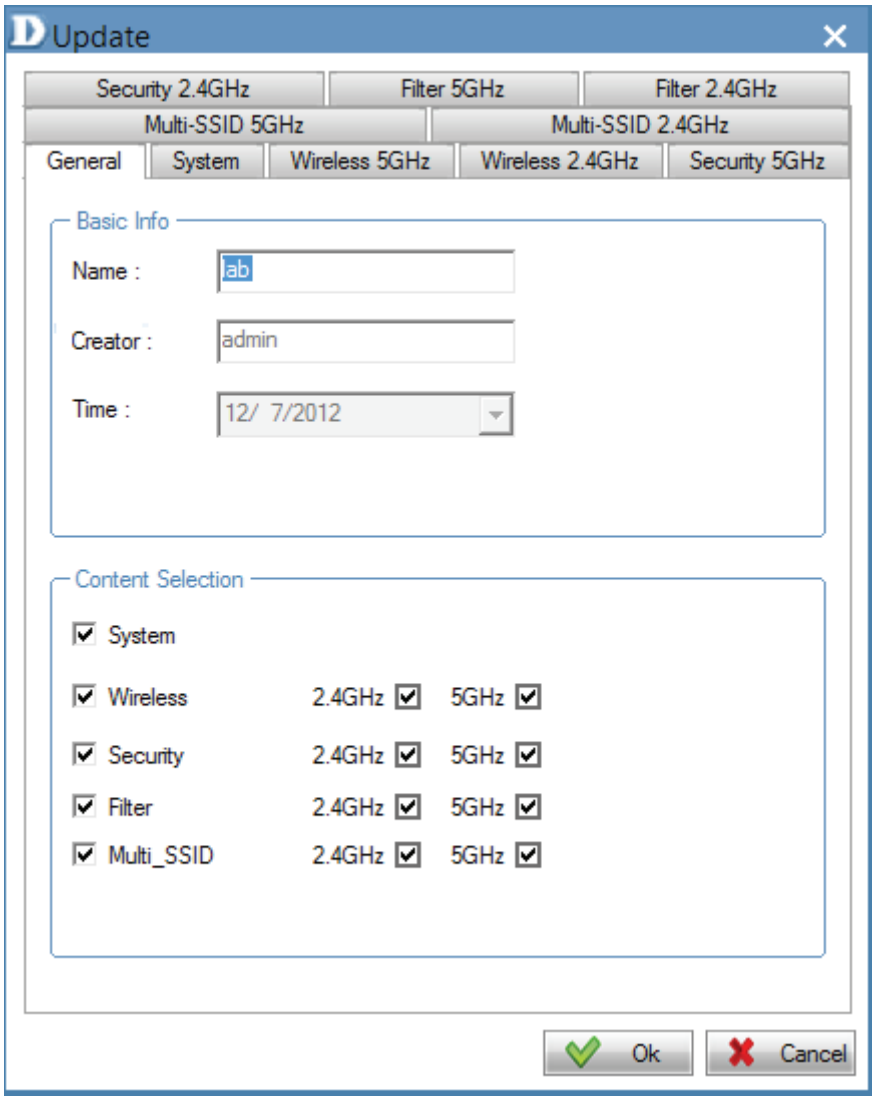


The new Template is now in the Multi Config window.



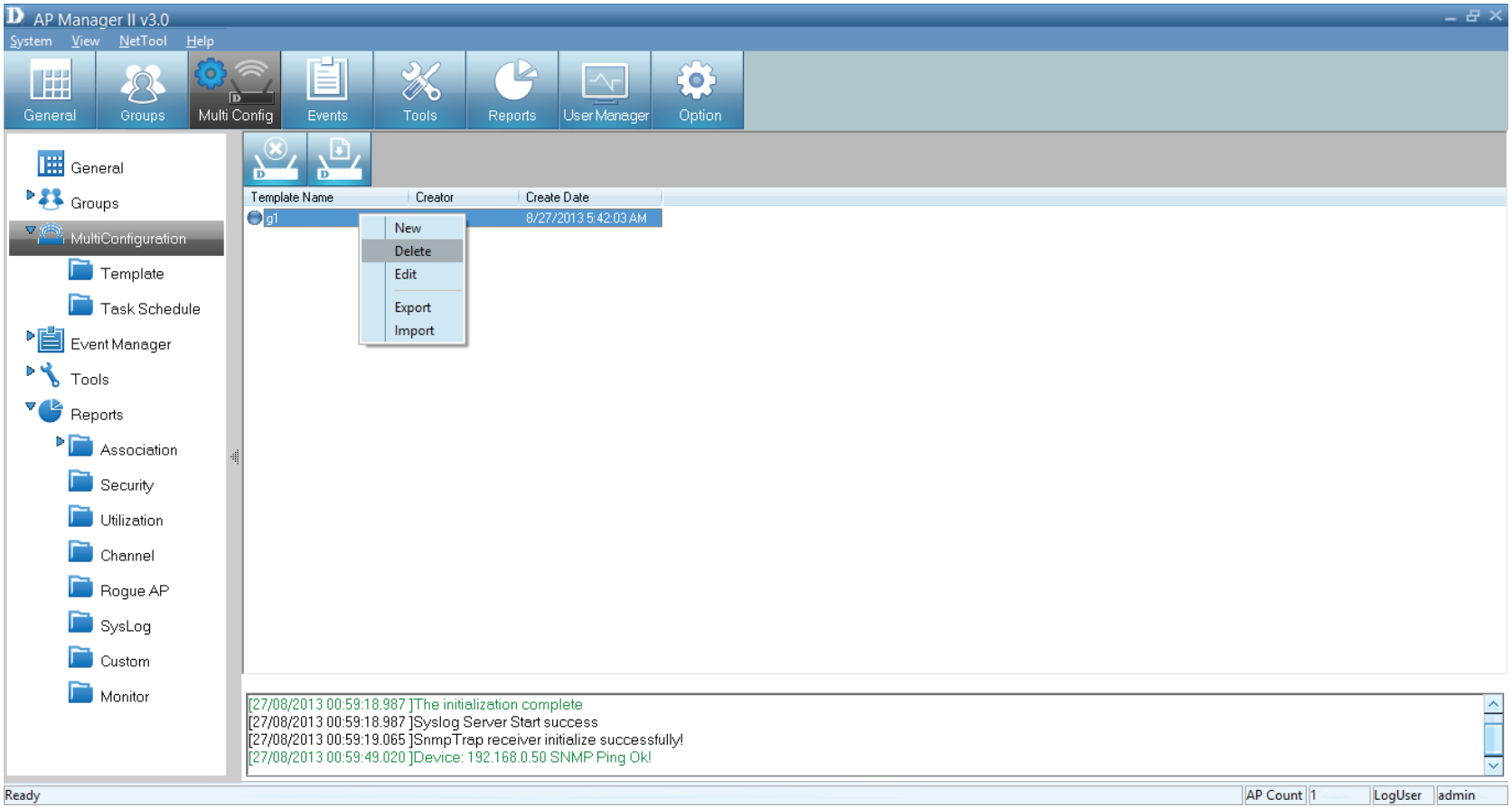
AP Manager II v3.0 - Edit a Template

To edit a template, double-click the template or right-click the template and select Edit item from the drop-down menu.



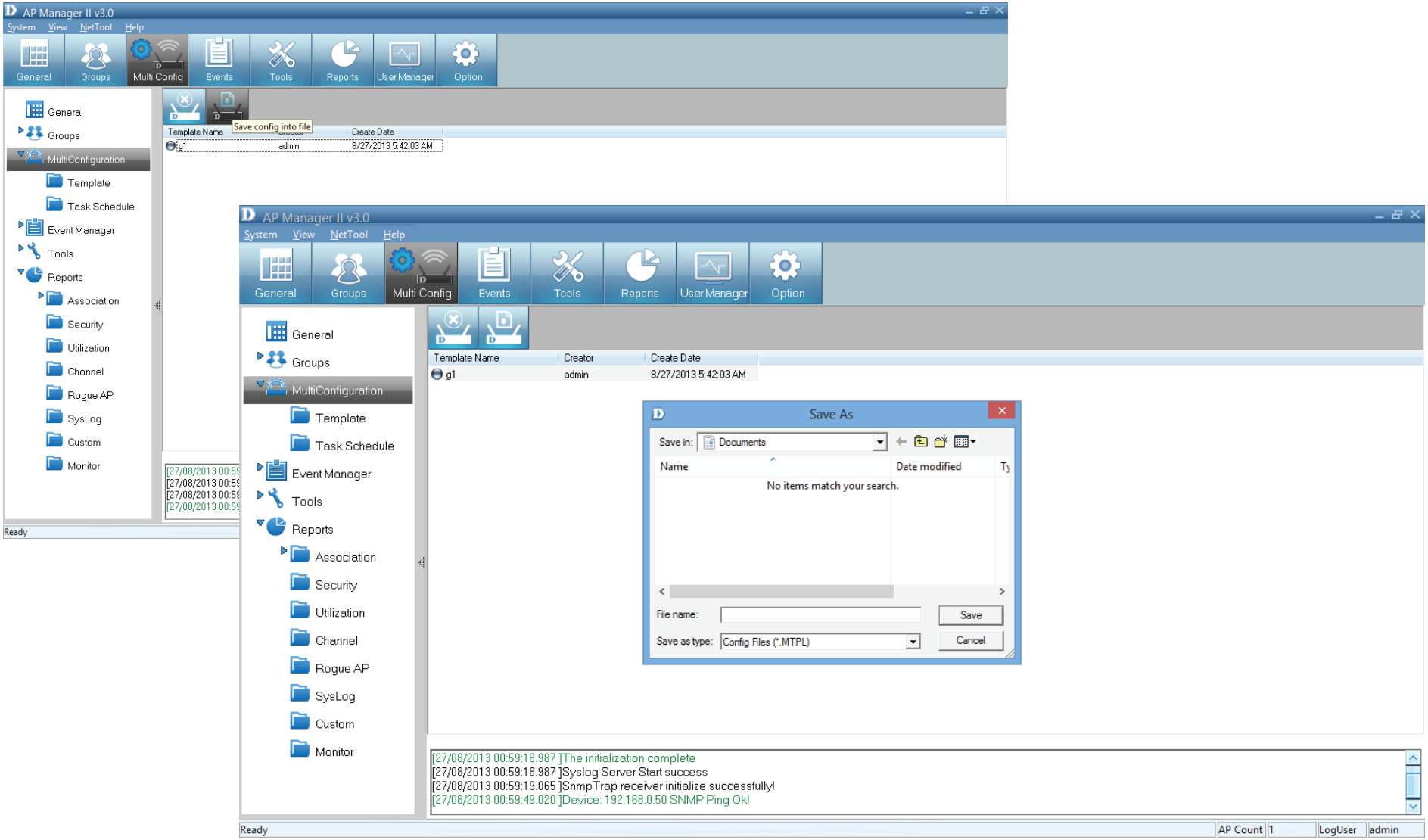
AP Manager II v3.0 - Delete a Template

To delete an existing template, right-click the template, and select the Delete item from the drop-down menu or click the Delete icon.



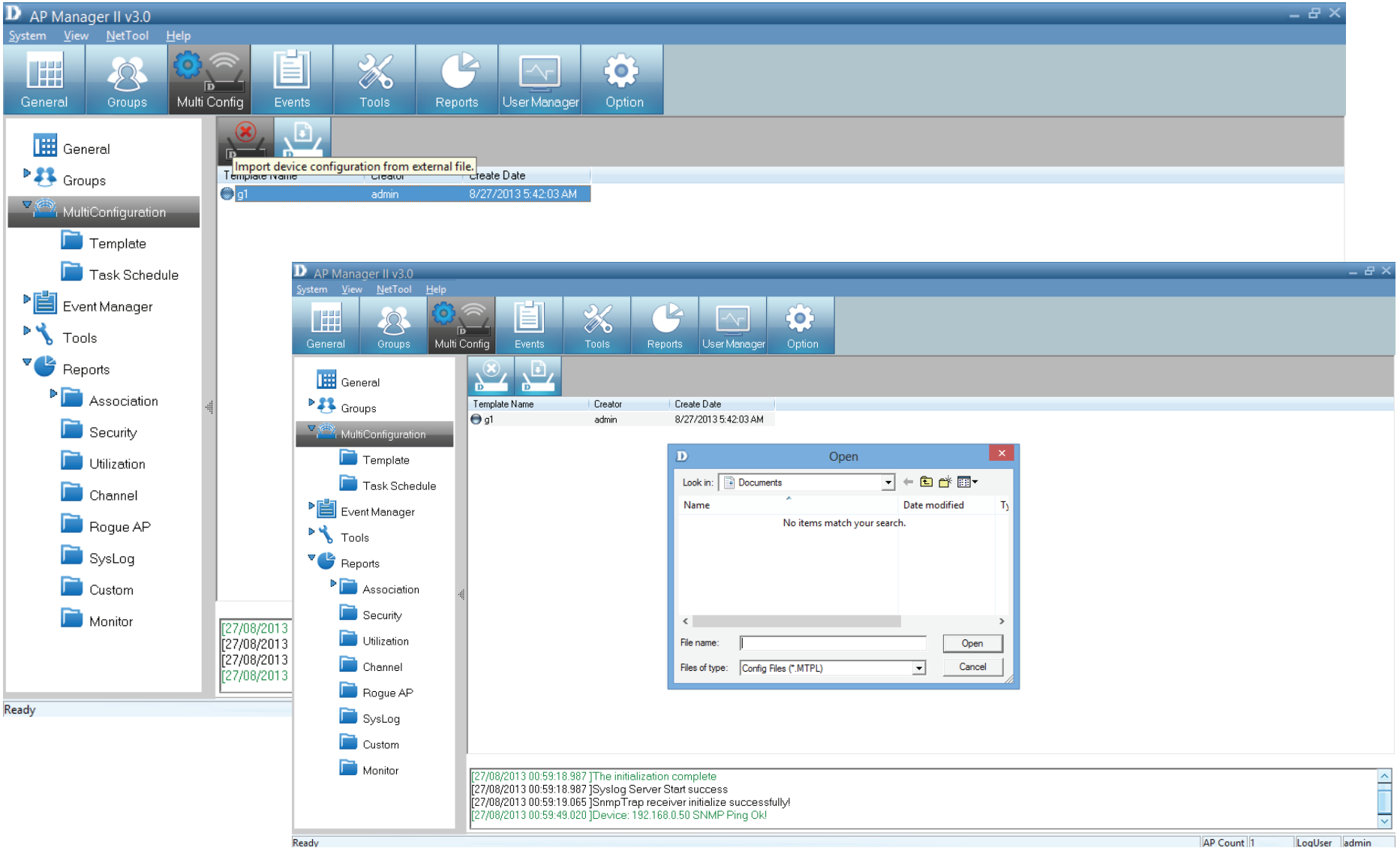
AP Manager II v3.0 - Save the Configuration

To save the configuration file, just click the right icon. A menu pops up for you to save it.



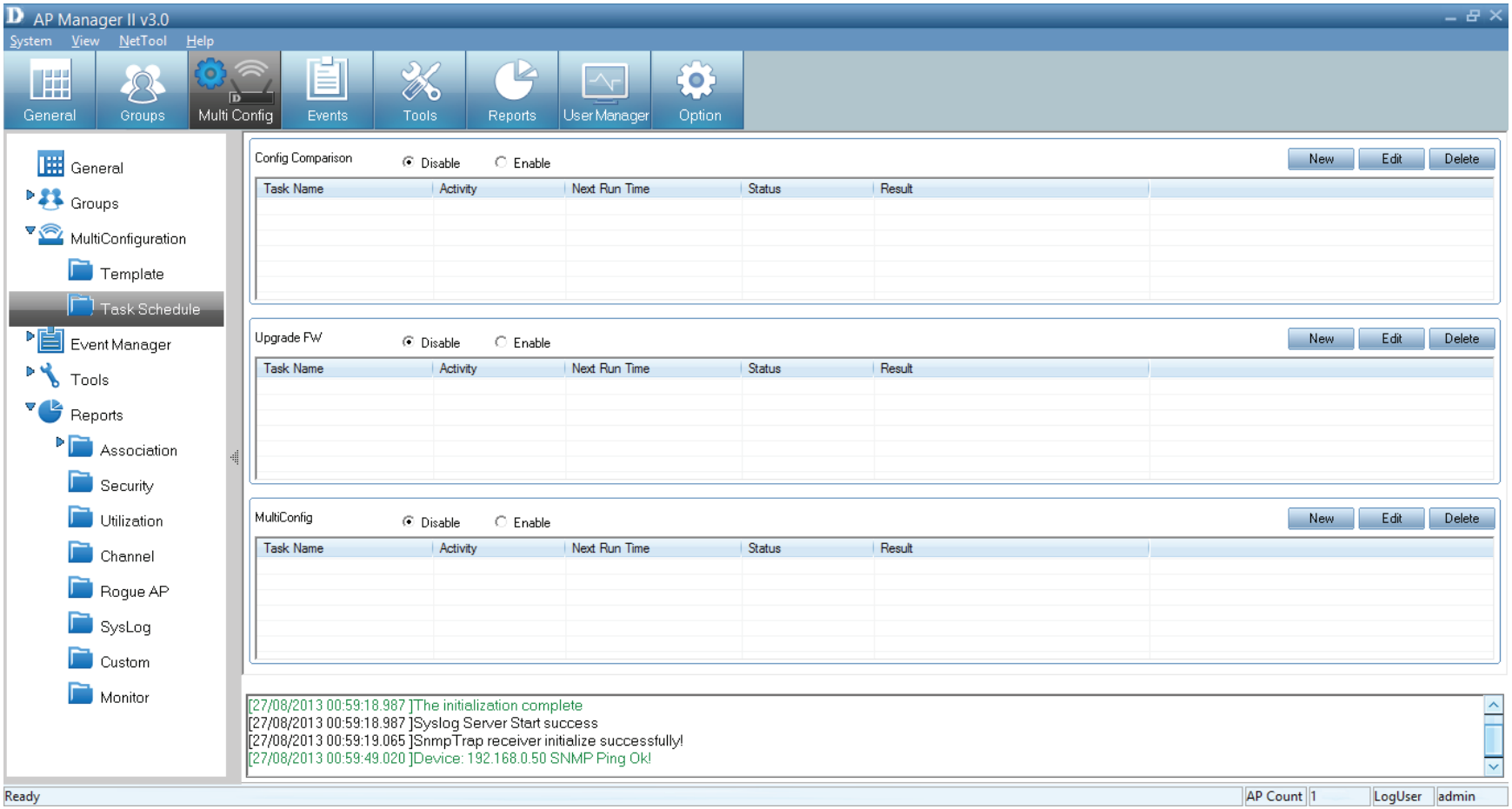
AP Manager II v3.0 - Import the Configuration

To Import a configuration file, click the import file above the template window.



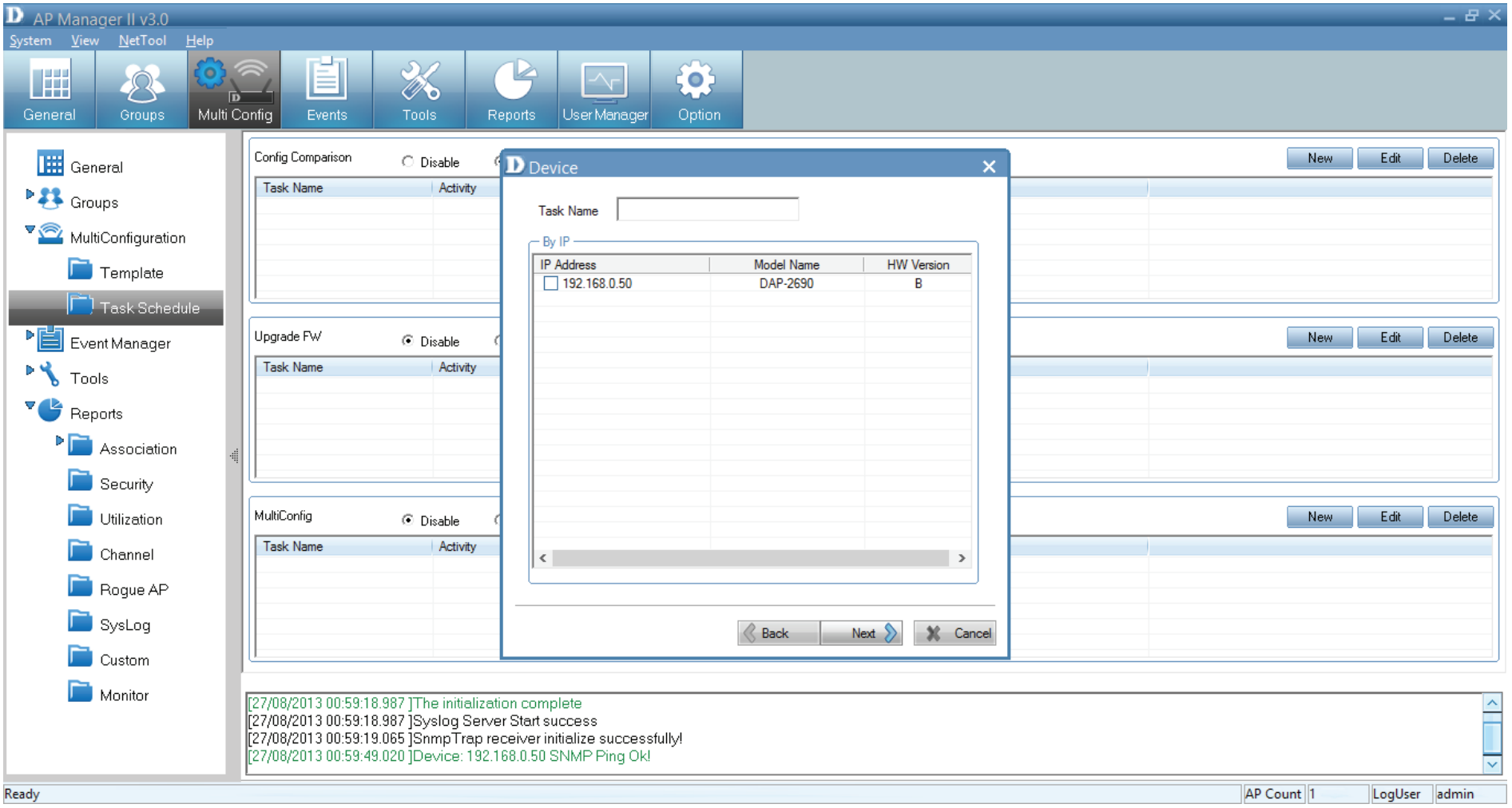
When you scroll through the MultiConfiguration options, you will notice that it has a Template folder. The Template folder is the folder you created in previous pages.

Click Task Scheduler to see the main configuration options - Config Comparison, Upgrade Firmware (FW), and MutiConfig. To enable each one, click the Enable radio button.



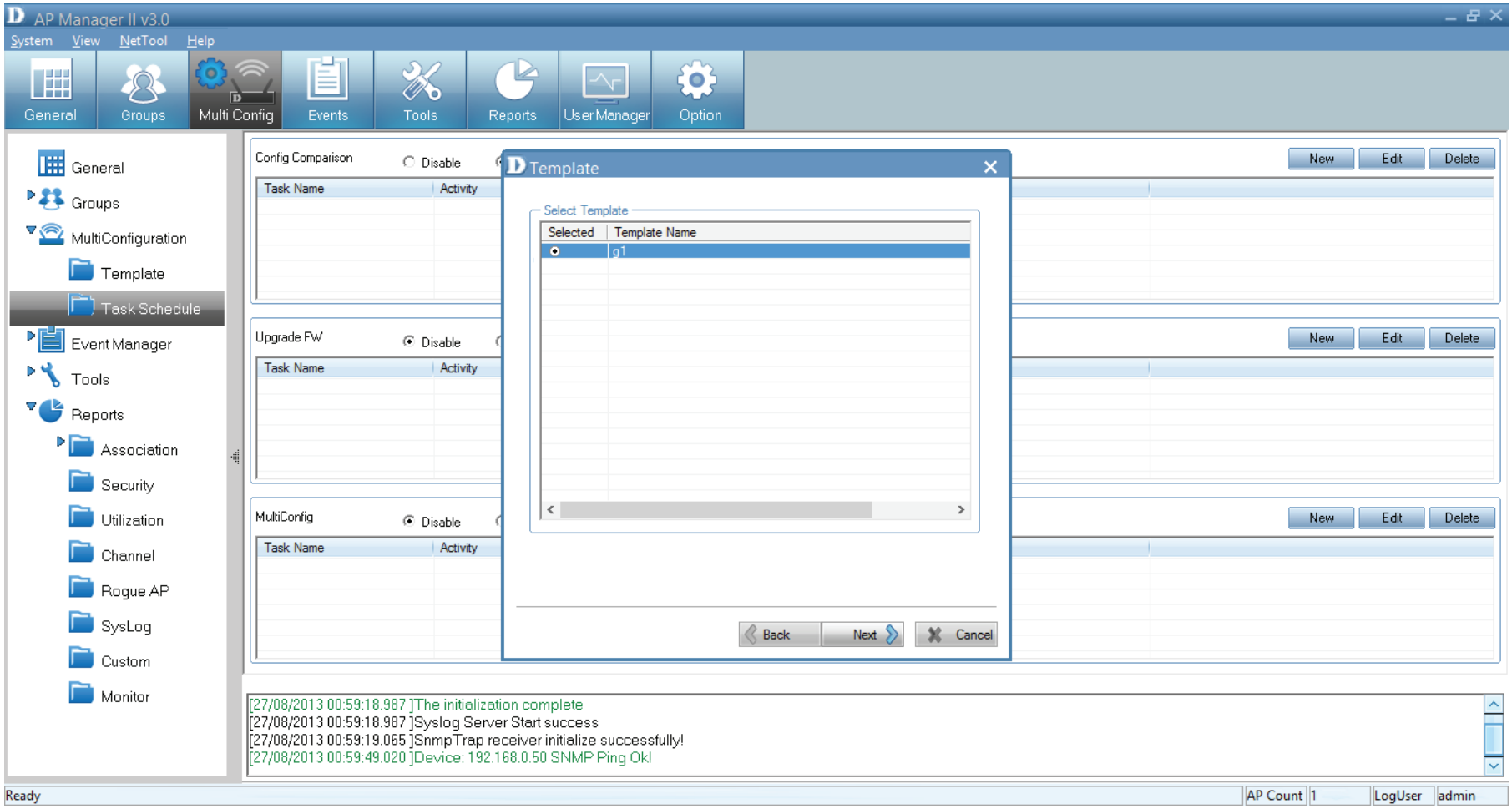
For the **Config Comparison**, click the **Enable** radio button, click **New** and view the options.

Give the **Task** a name, then select the devices and click **Next**.



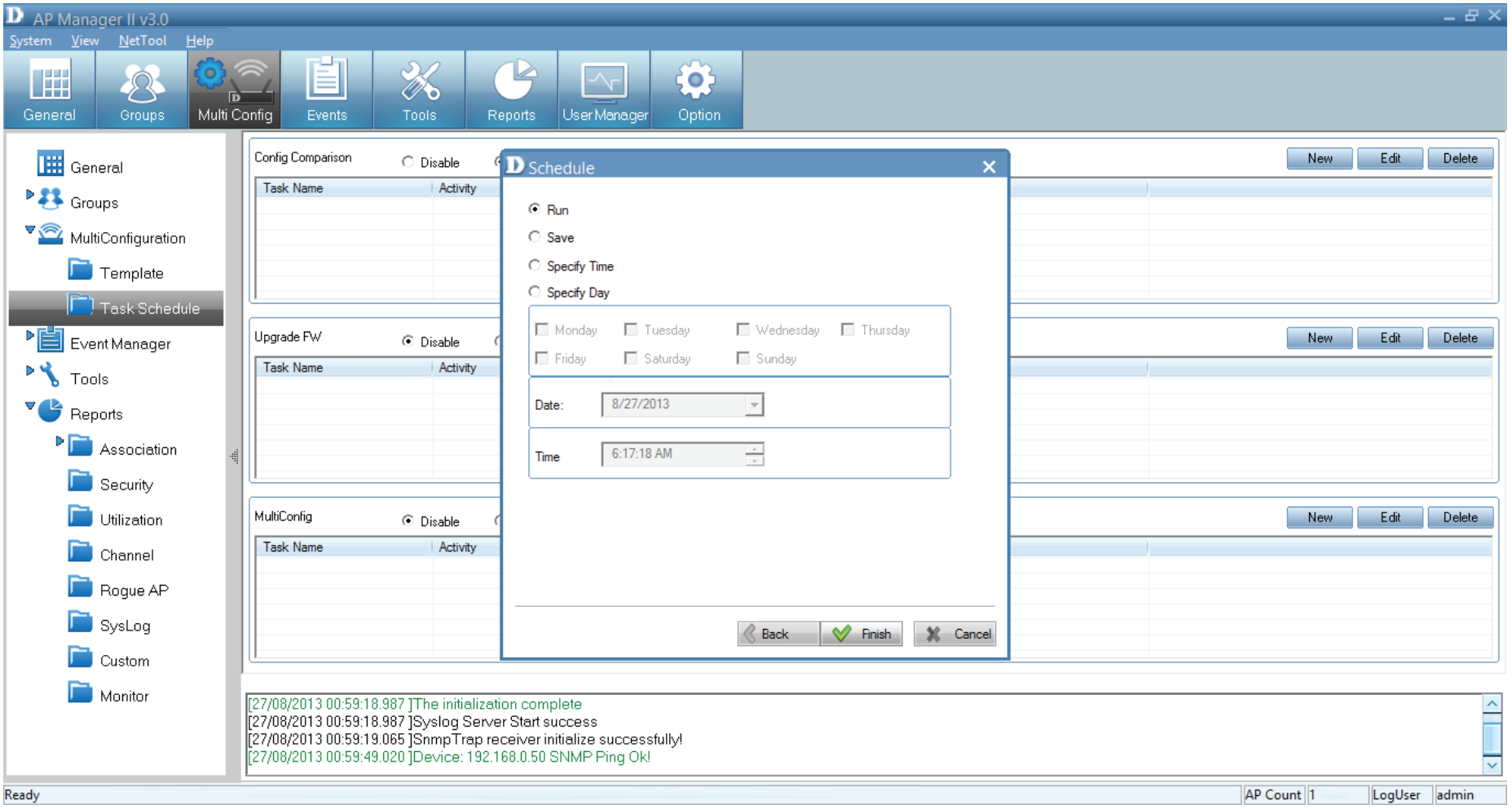
Select a **Template** from the list provided.

Click **Next** to continue.



Select a **Schedule** time frame - **Run, Save, Specify Time, Specify Day** and then enter the **Date** and **Times**.

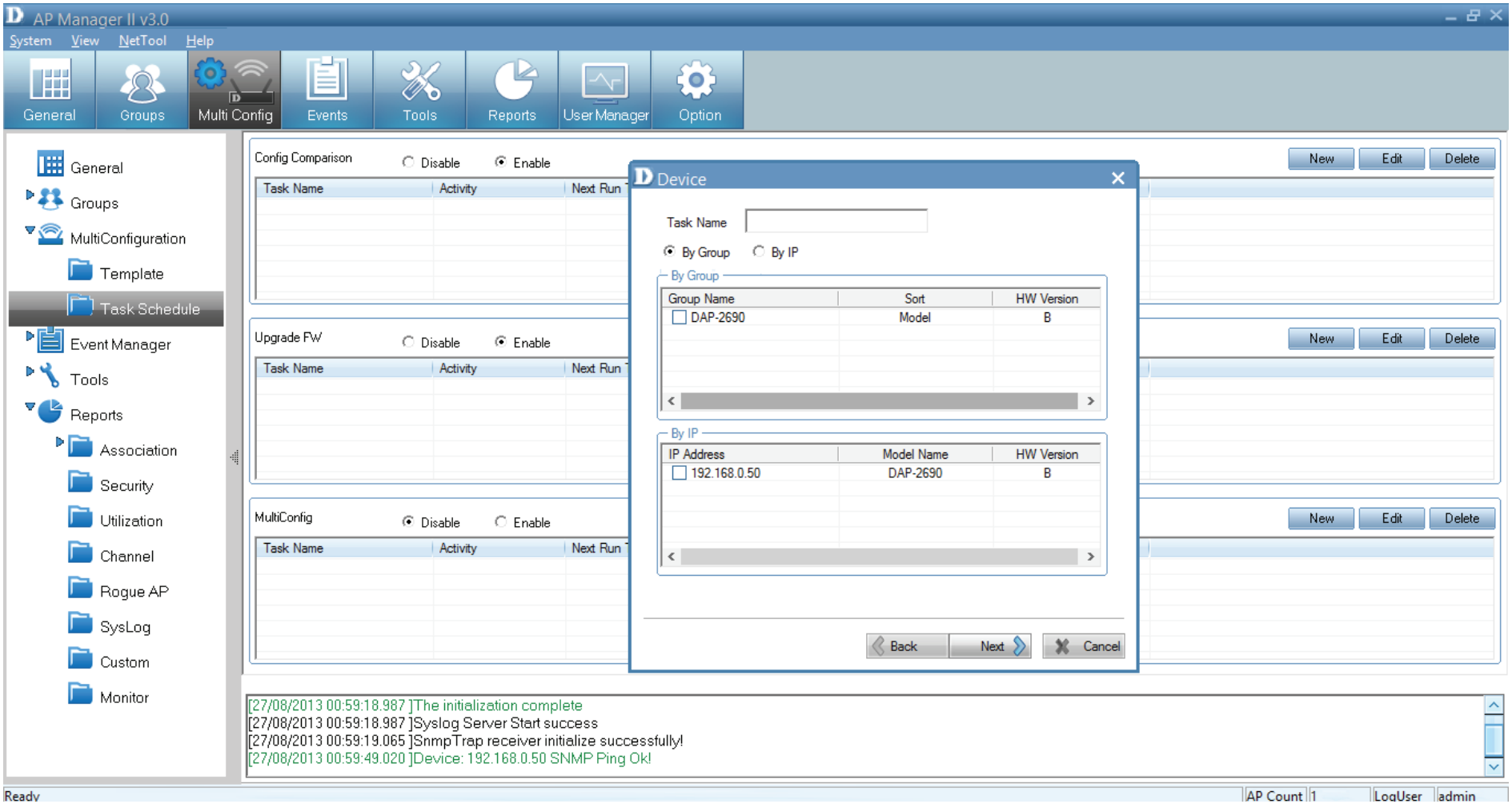
Click **Finish** when complete.



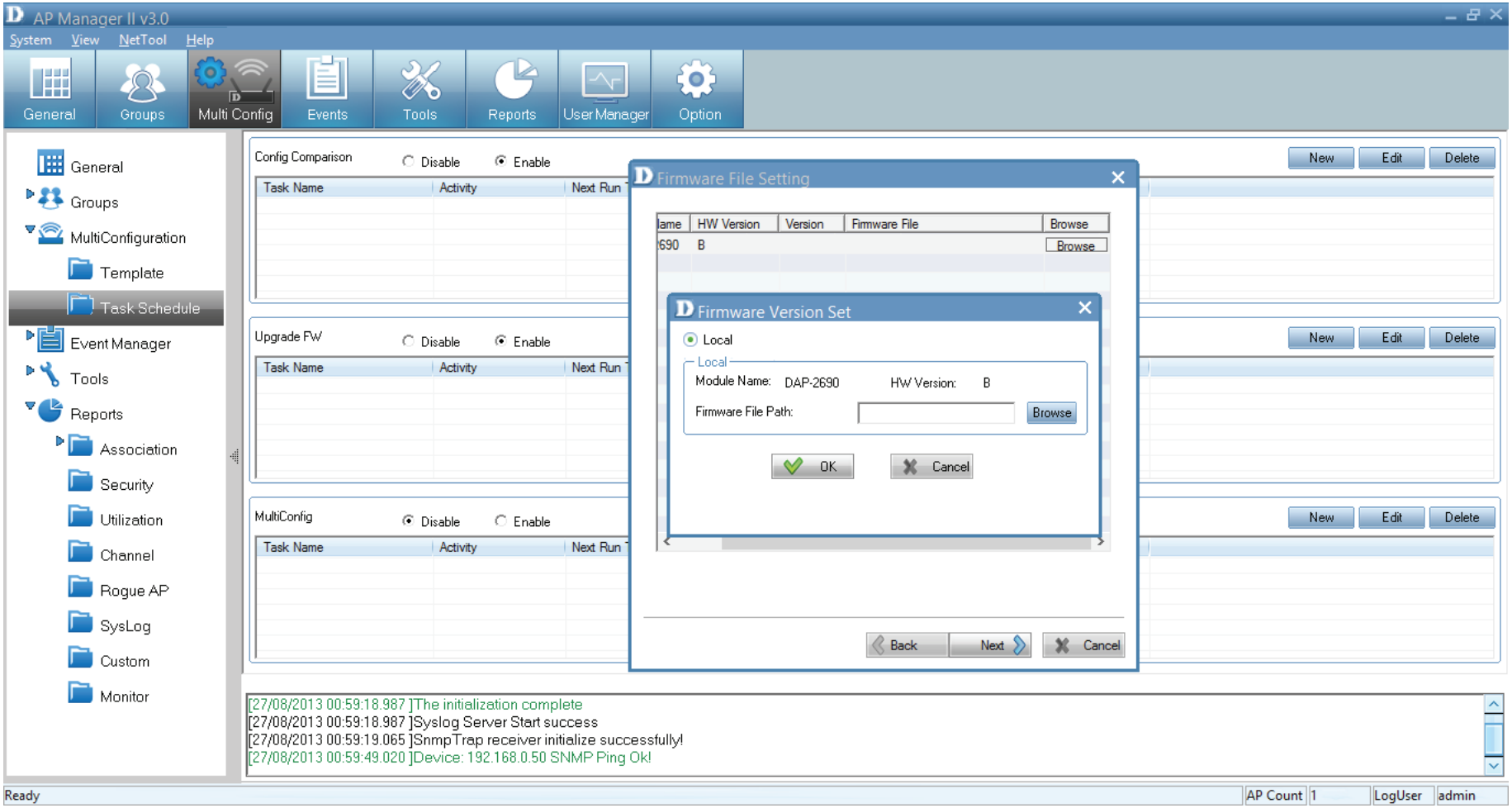
For **Upgrade Firmware**, click the **Enable** radio button, then view the devices available.

Give the **Task** a name, select to do it by **Group** or by **IP**

Click **Next** to continue.



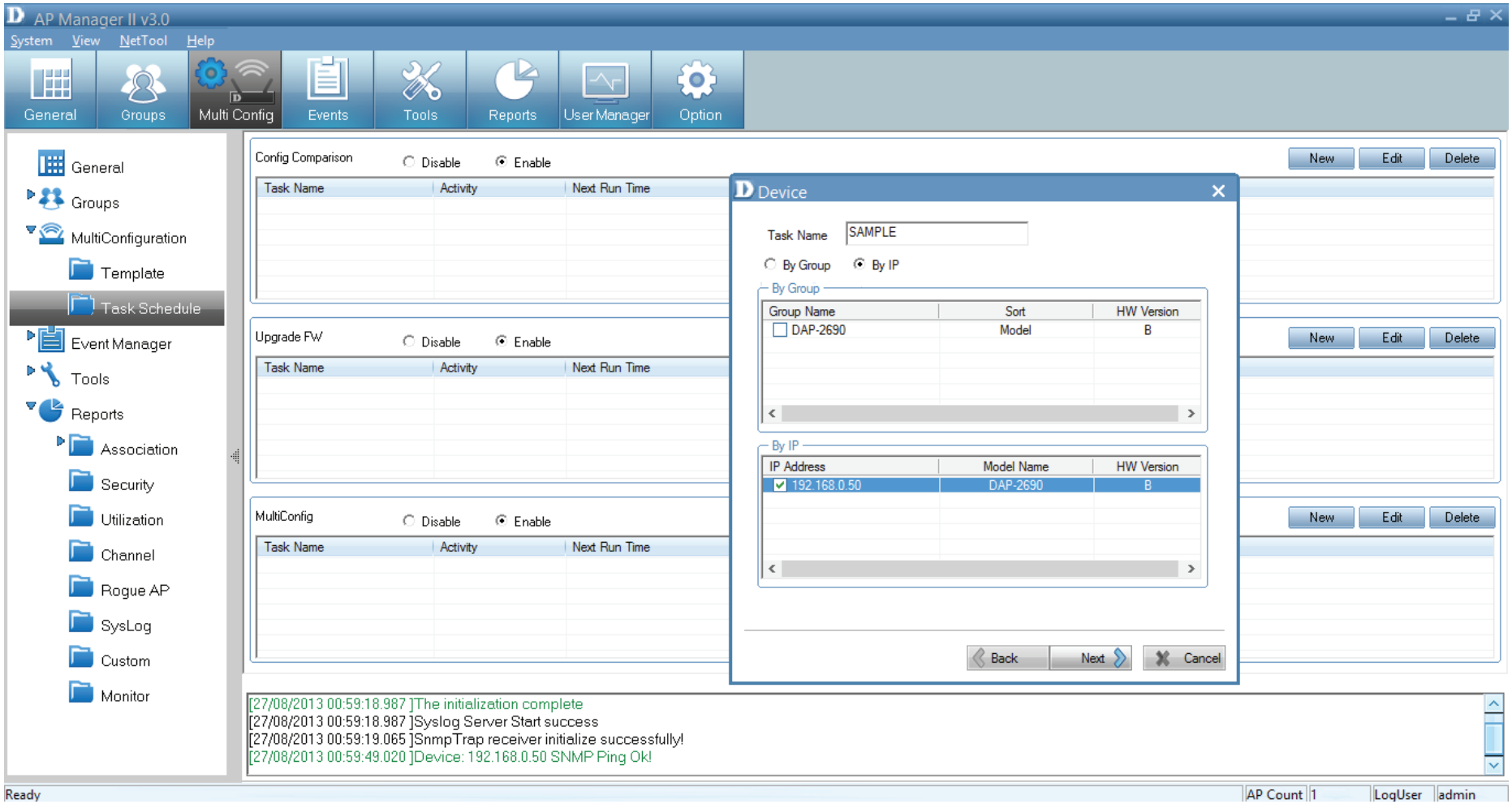
Under F**irmware File Settings**, click the **browse** button next to your device, fild the new firmware, and click **Next.**



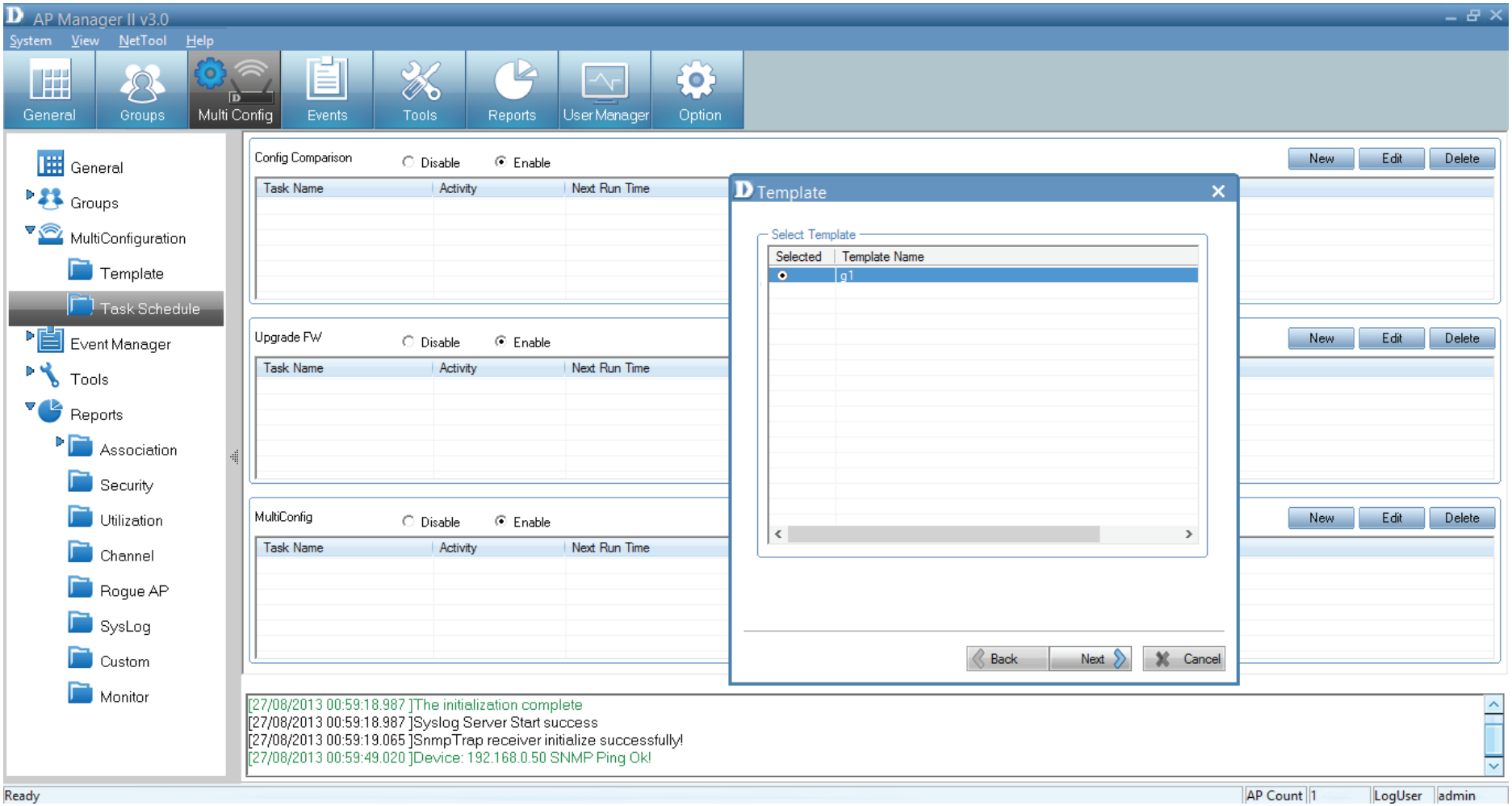
Under **MultiConfig**, click the **Enable** radio button, and New.

Under **Device** enter a **Task Name,** select by **Group** or **IP**

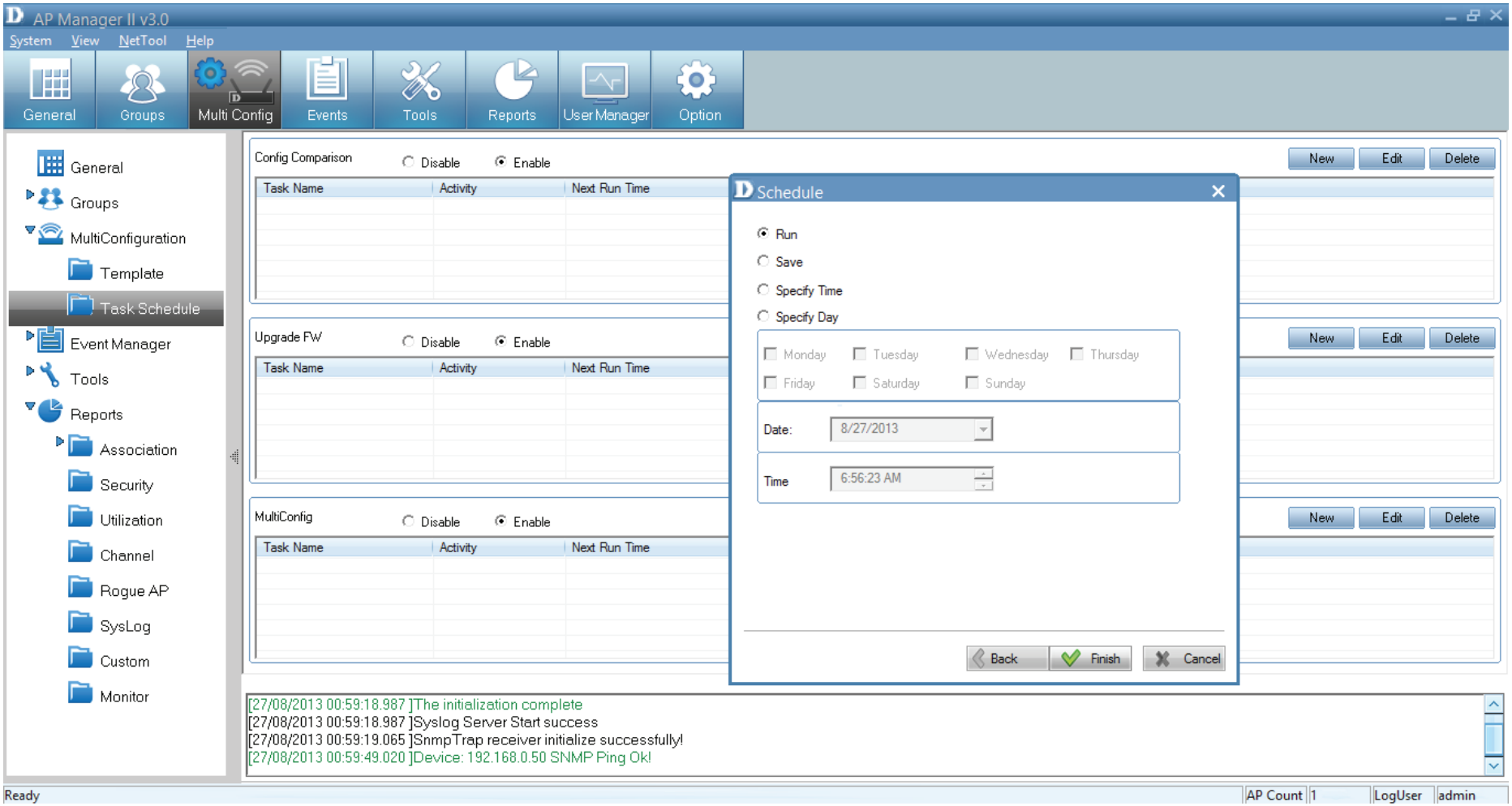
Click **Next** to continue.



Under **Template**, select a template for this configuration and click **Next**

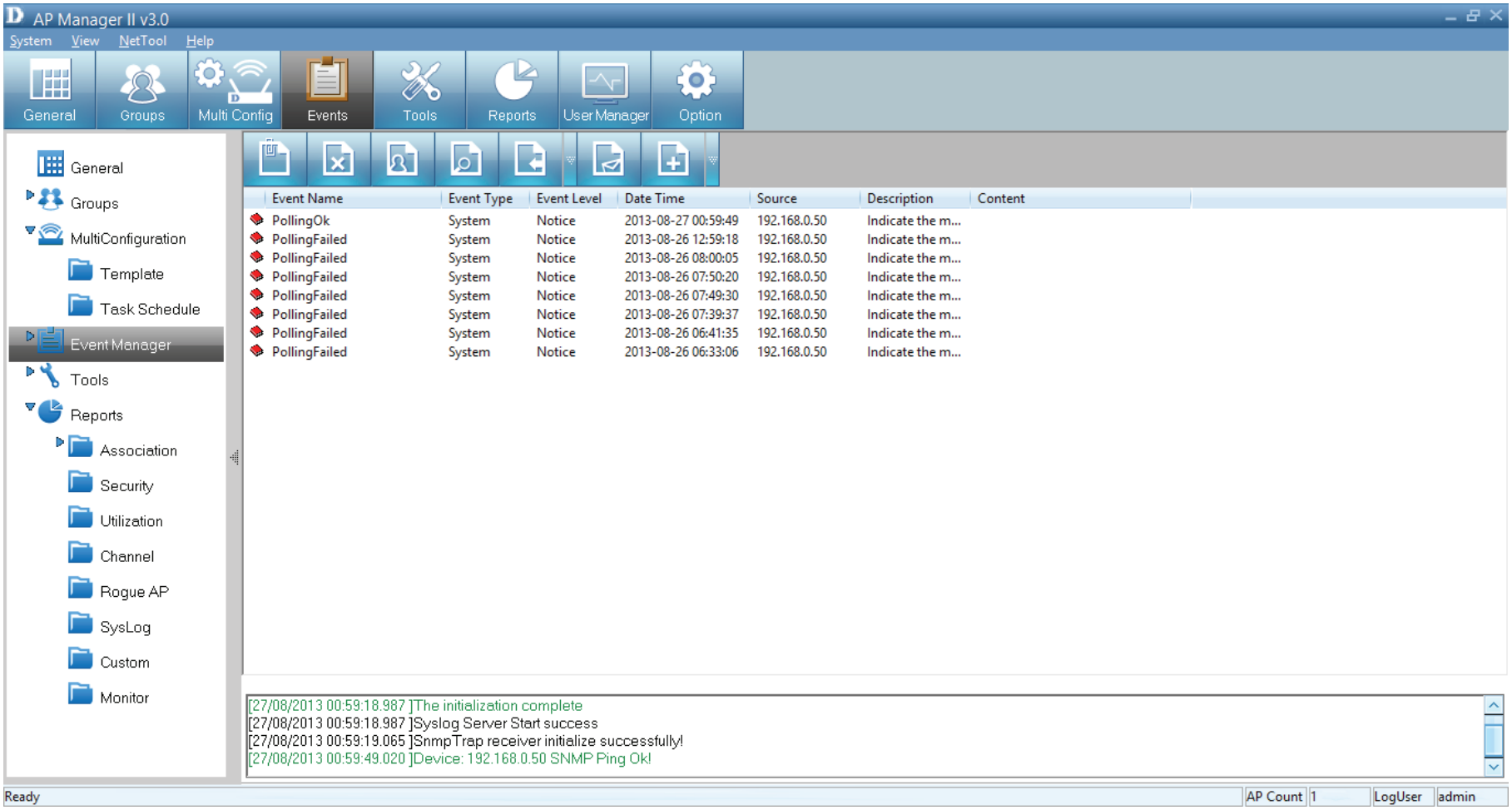


Under **Schedule**, select one of the options provided and click **Finish**.



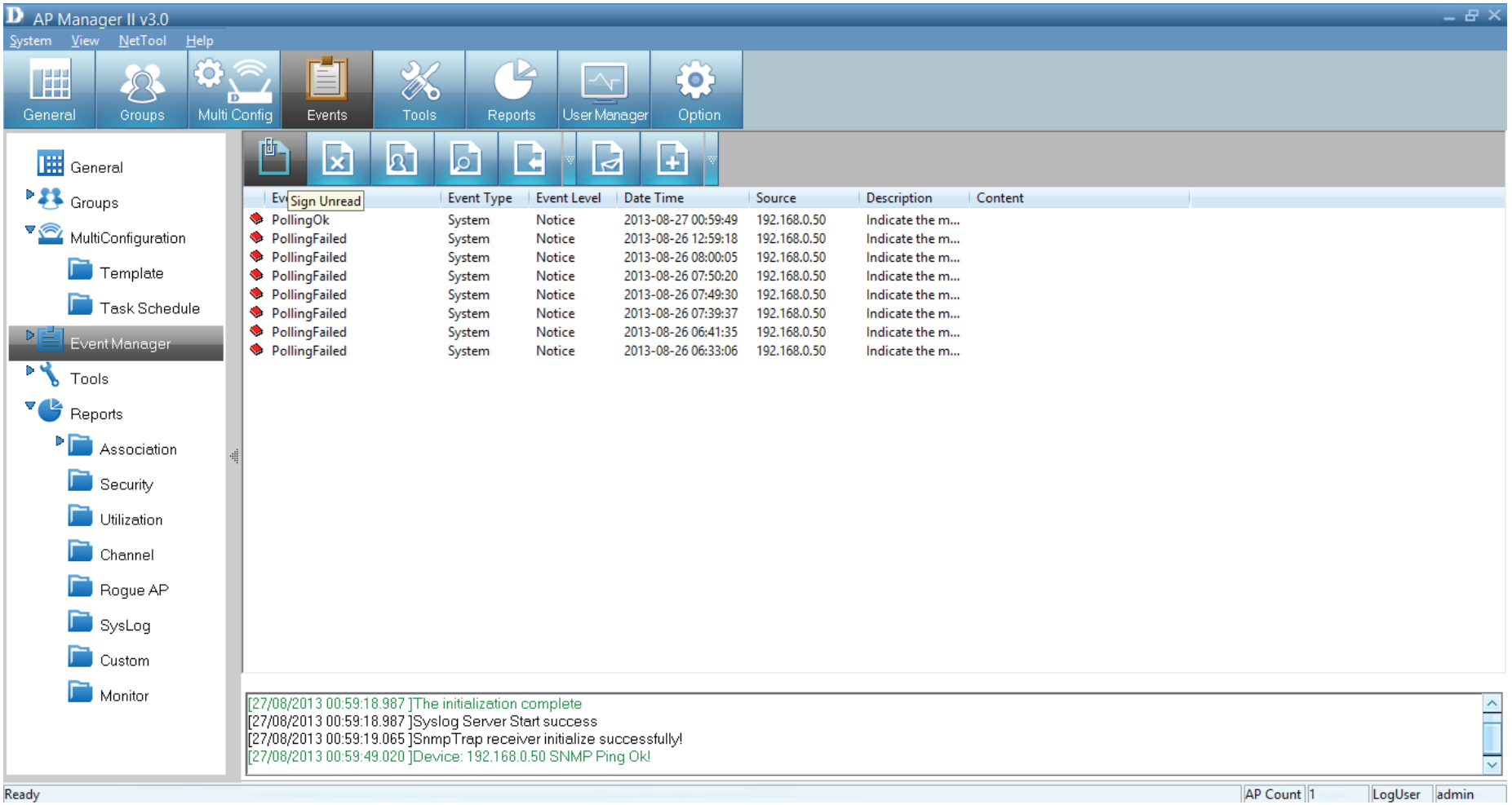
AP Manager II v3.0 - Events (Event) Manager

Events (Event) Manager can be accessed from both the side panel and the top panel. Click this icon to access details relation to faults experienced using the Access Point.

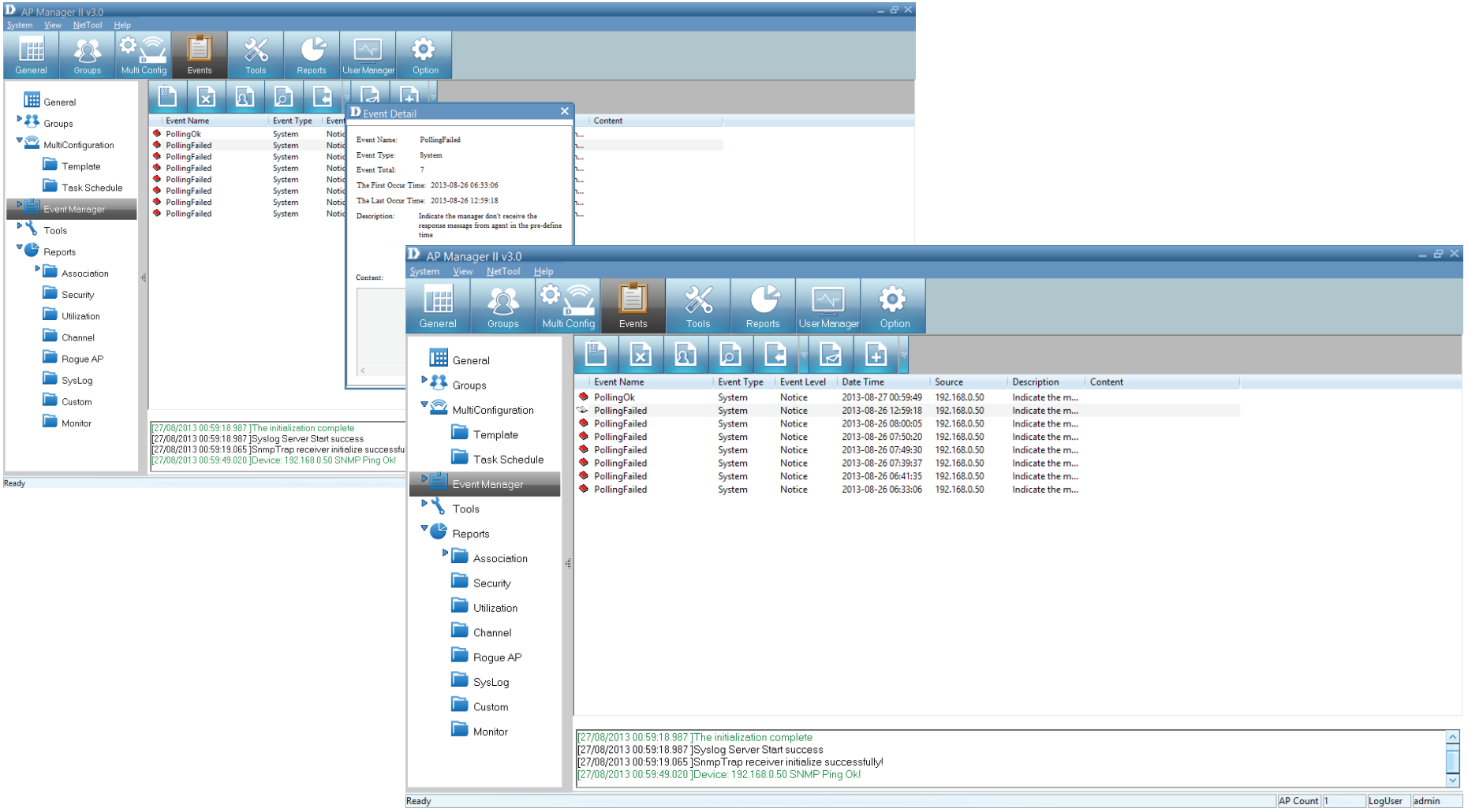


AP Manager II v3.0 - Unread Events

Click this icon to mark the message as **Unread**.

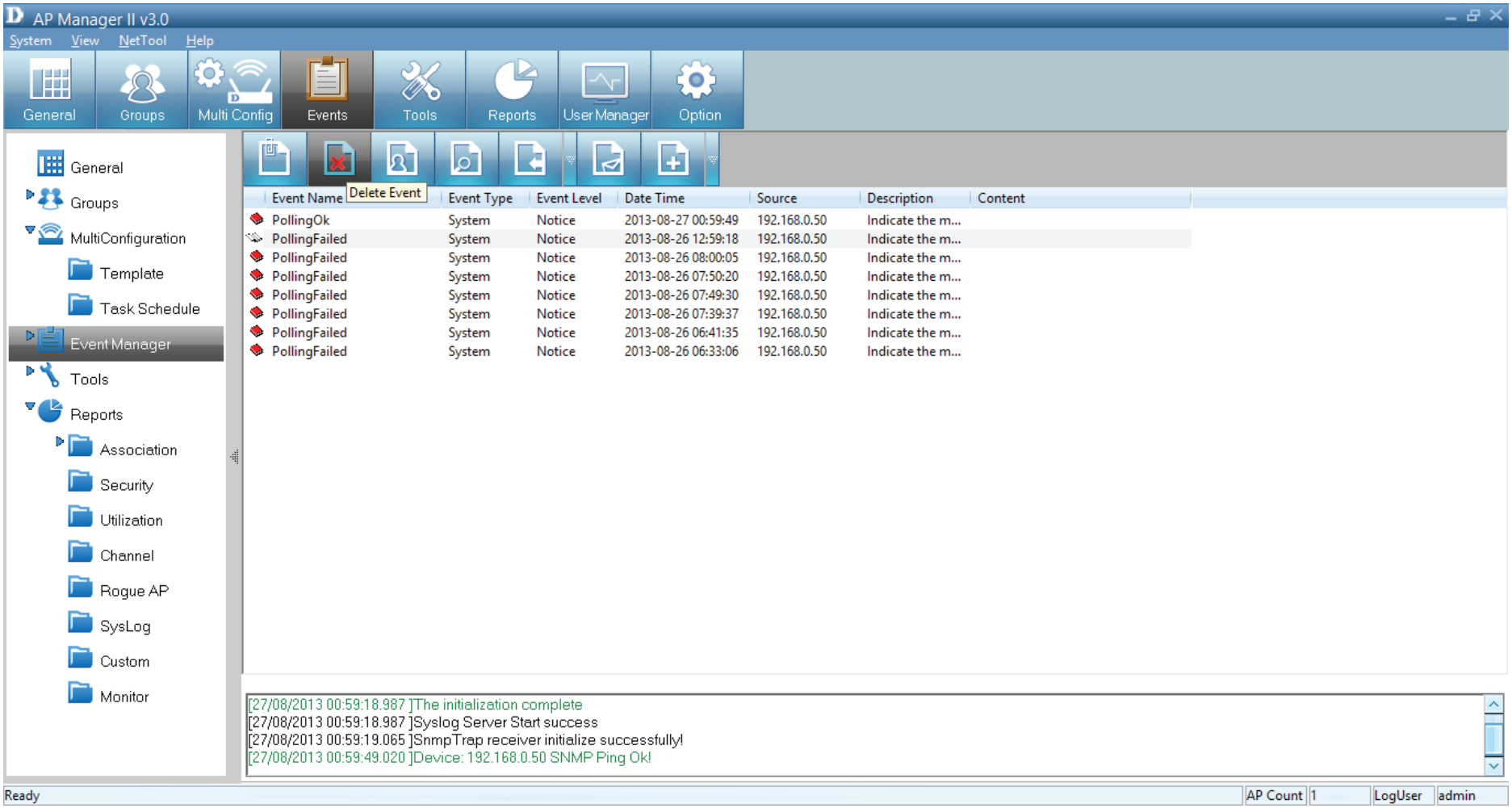


Double-click an event to view its details. The icon now changes to an open book.



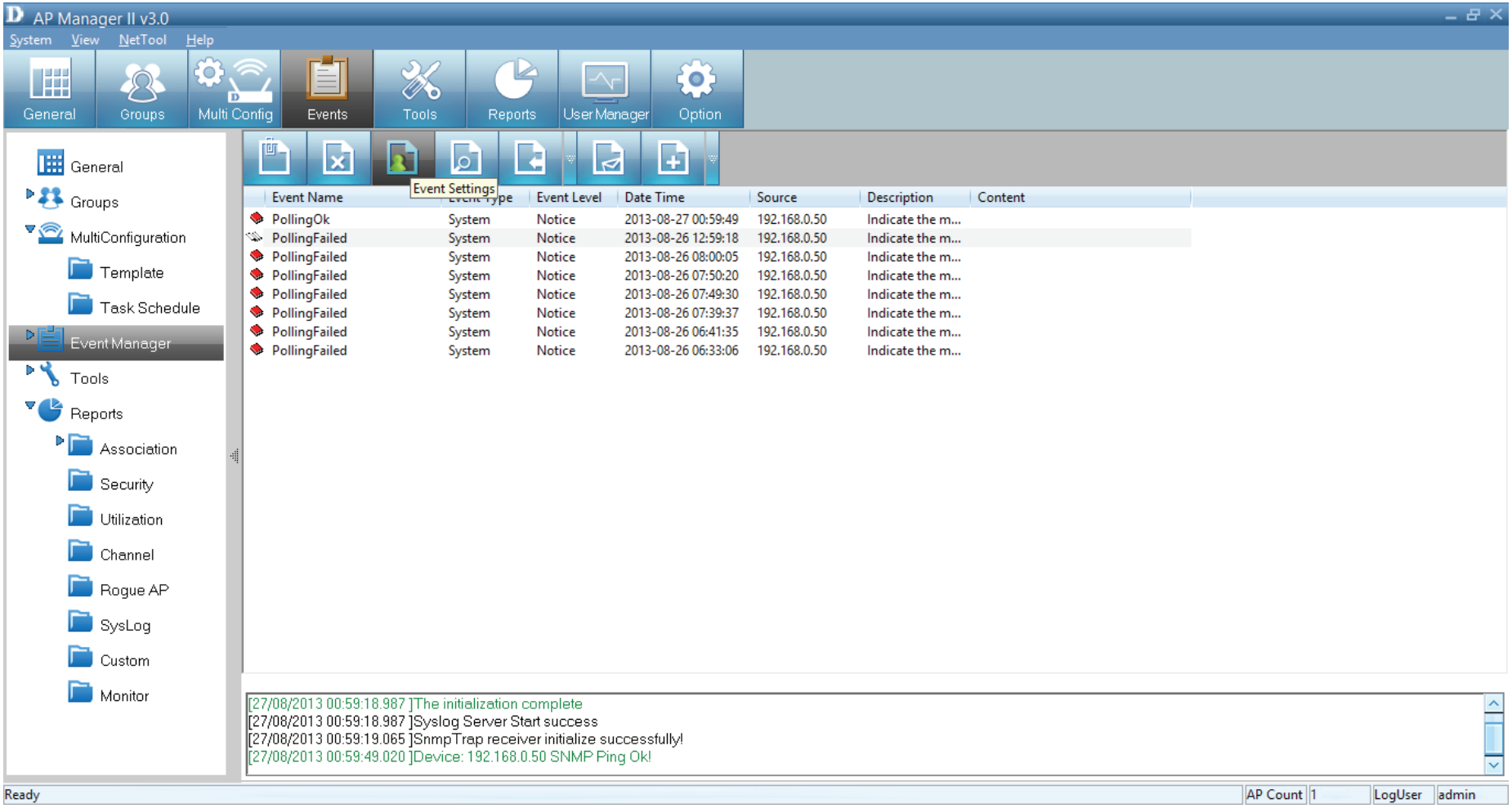
AP Manager II v3.0 - Deleting Events

Click this icon to **Delete** an event. **Confirm** delete by clicking **Yes**, or **No** to exit and do nothing.

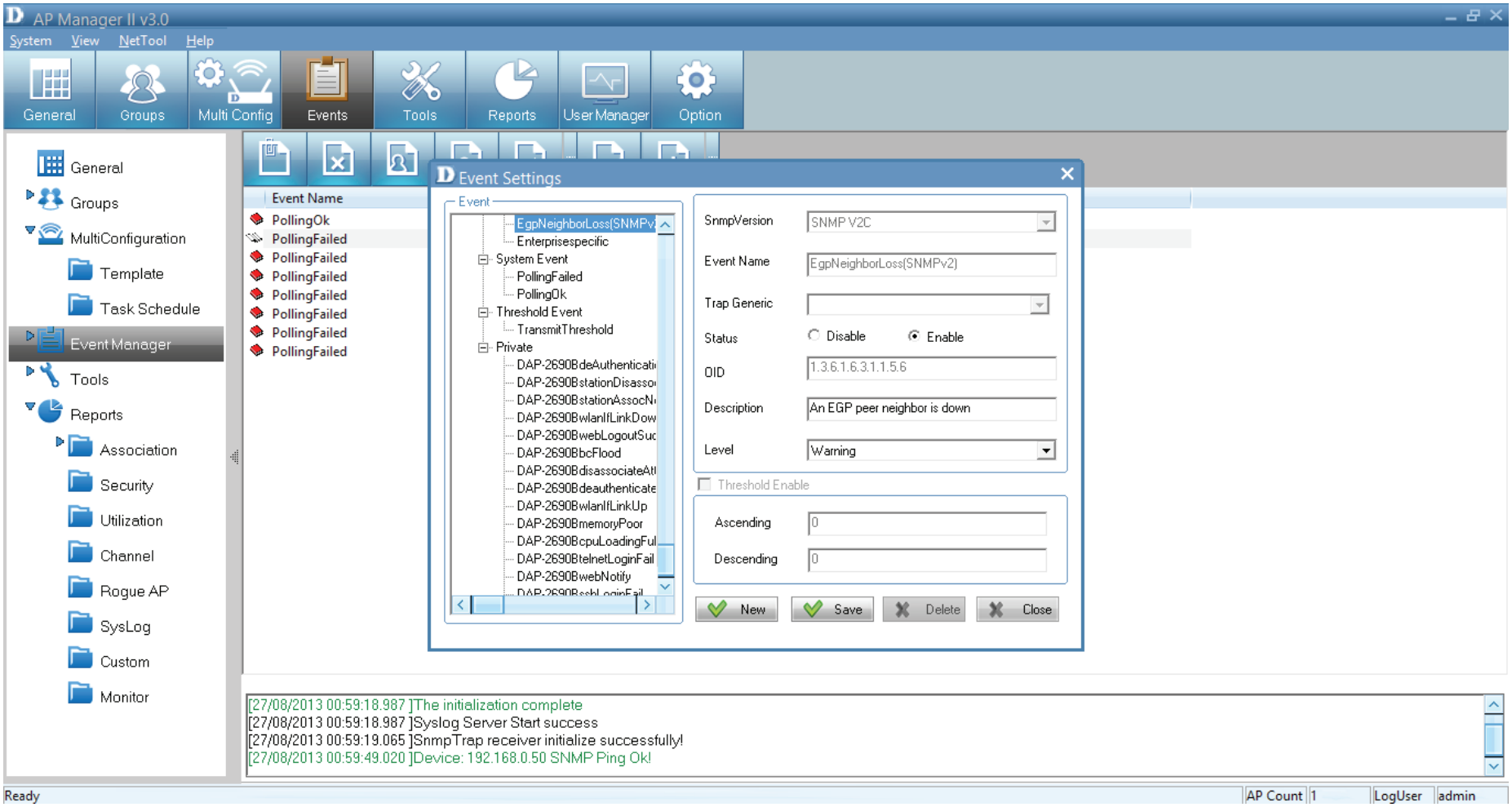


AP Manager II v3.0 - Setting Events

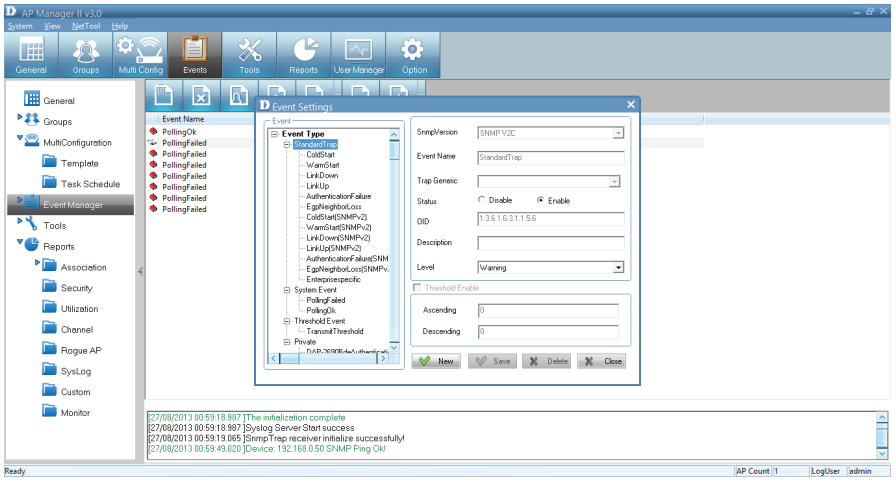
Click this icon to show **Event Settings**



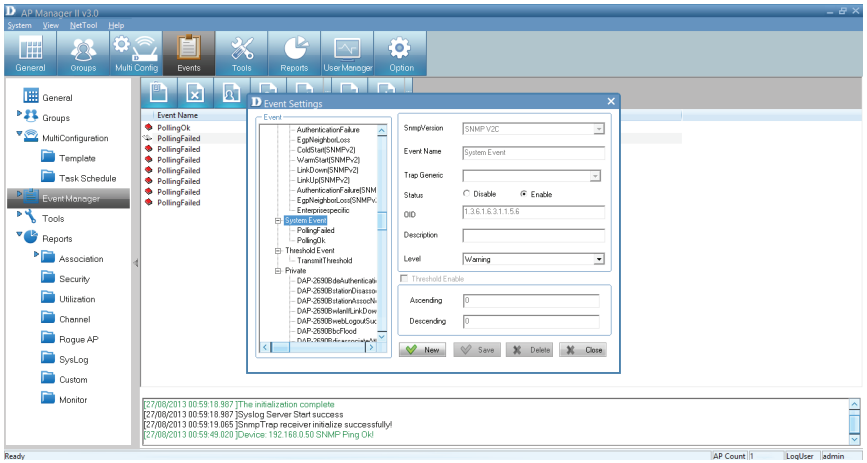
The main **Event Settings Panel** opens.



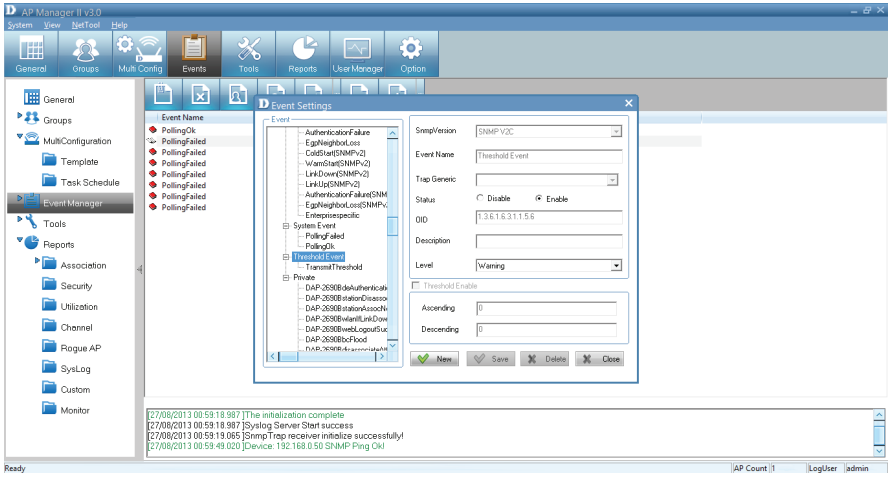
The **Events Panel** consists of four main **Event Types**.



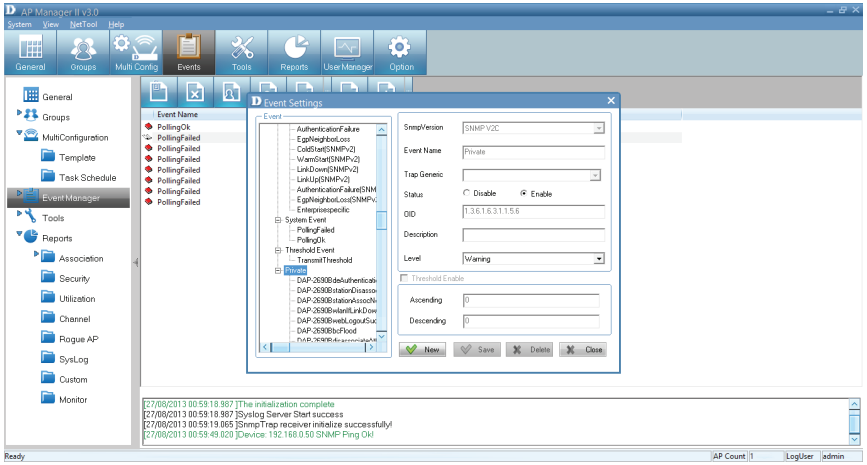
Standard Trap



System Event



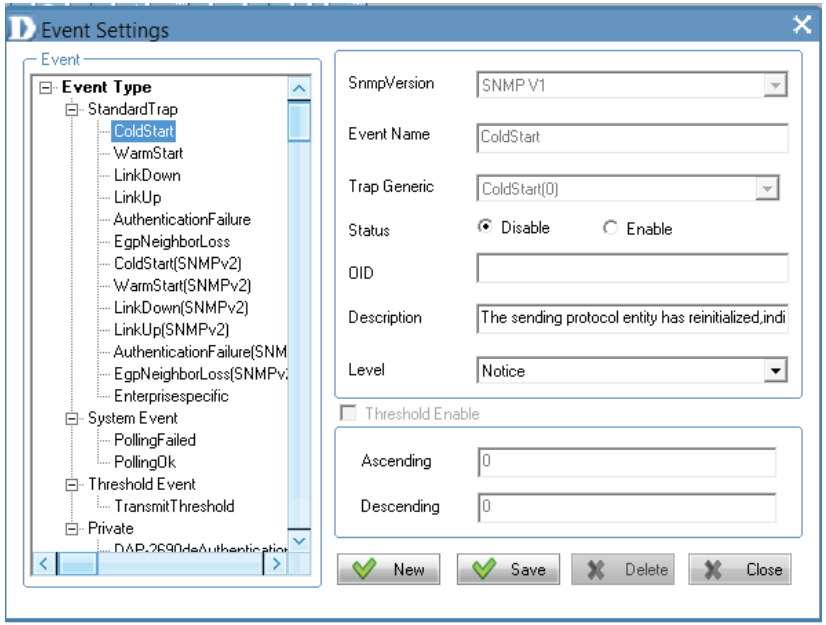
Threshold Event



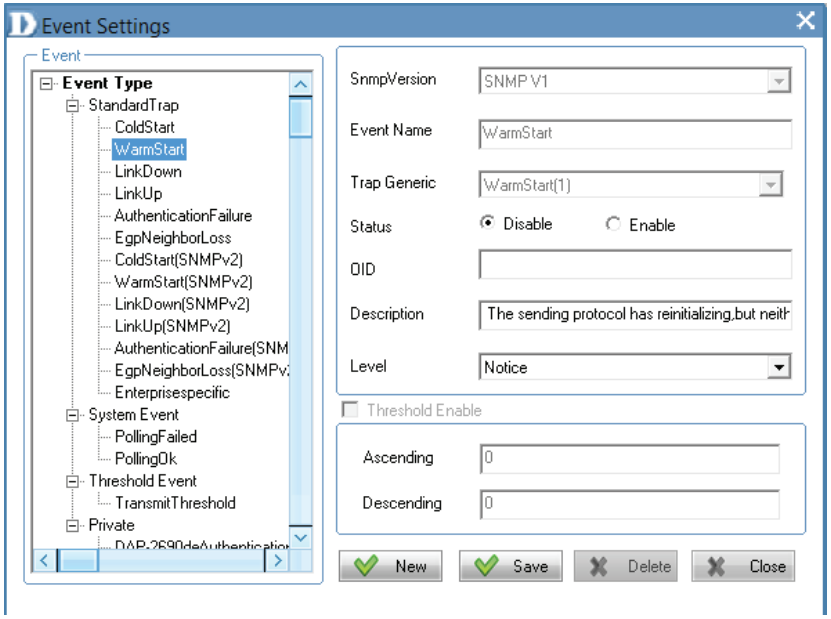
Private

Standard Trap - The standard trap view window displays the standard trap data received from Access Points and consists of the following options:

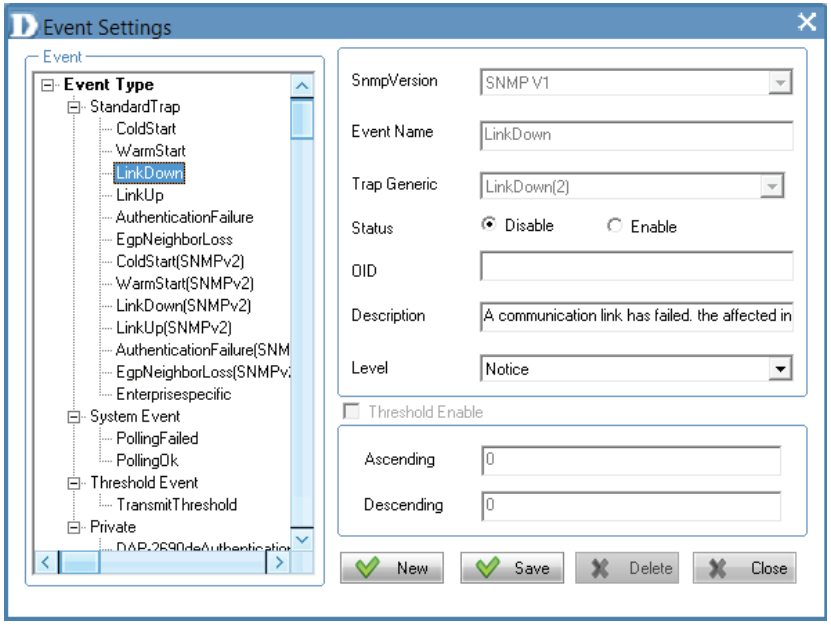
ColdStart



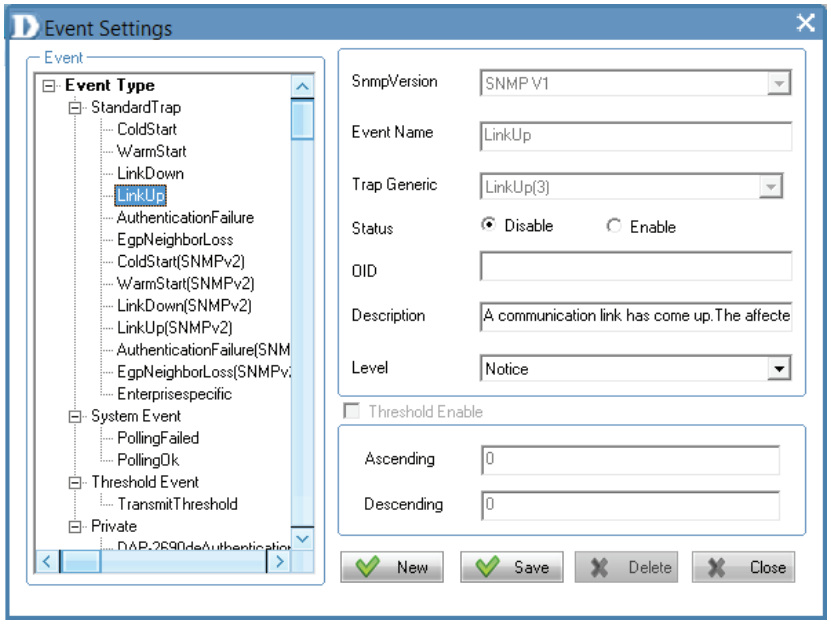
WarmStart



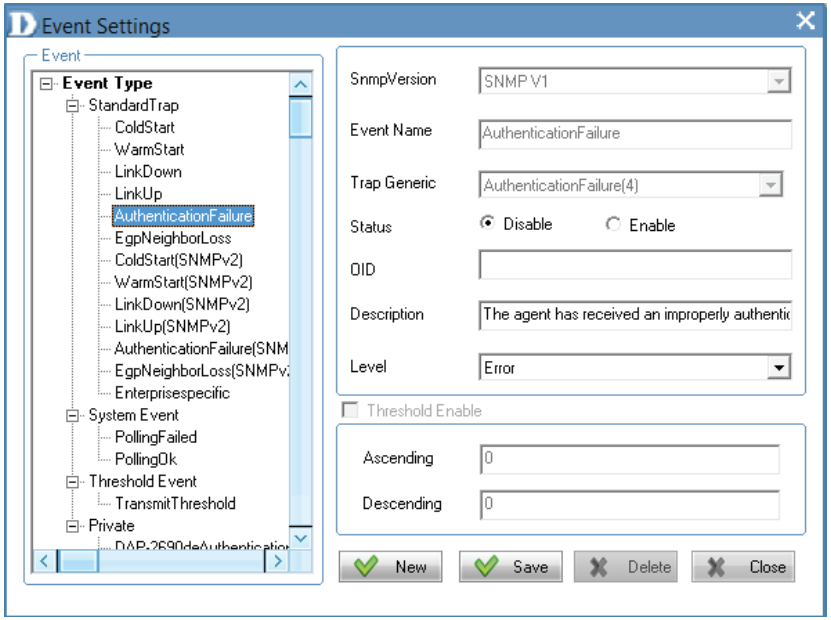
LinkDown



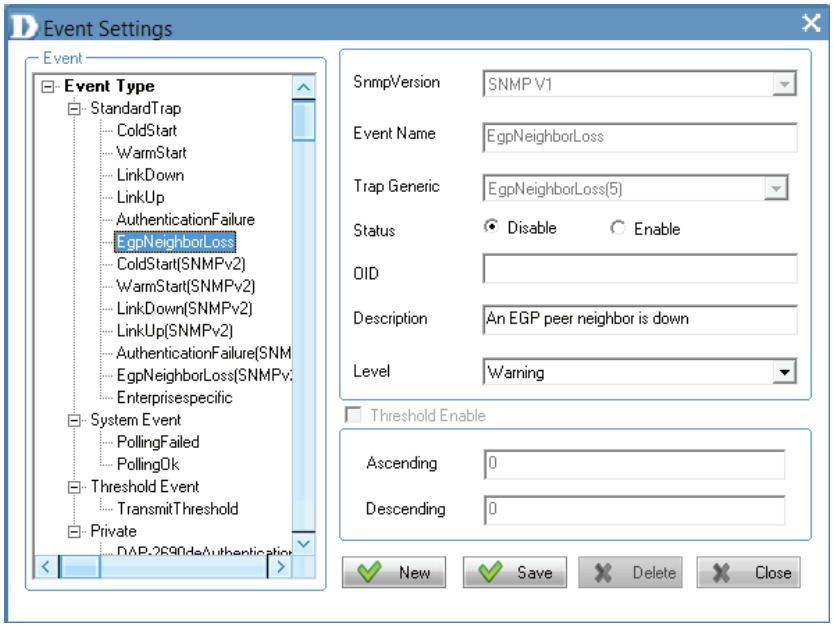
LinkUp



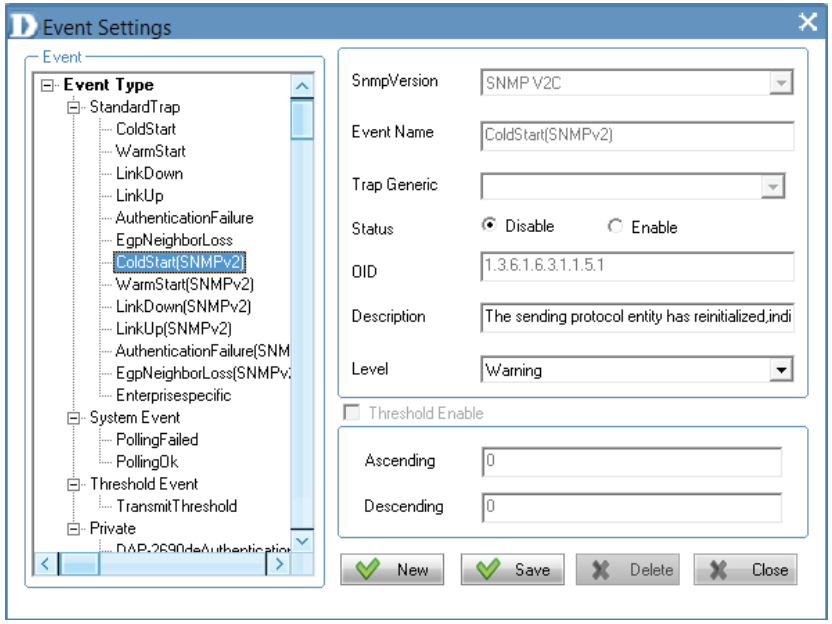
AuthenticationFailure



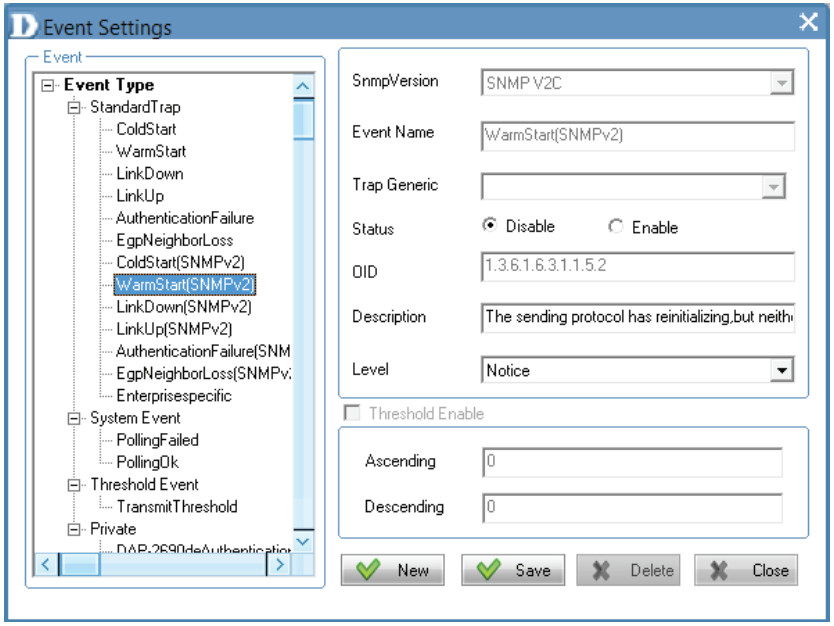
EgpNeighborLoss



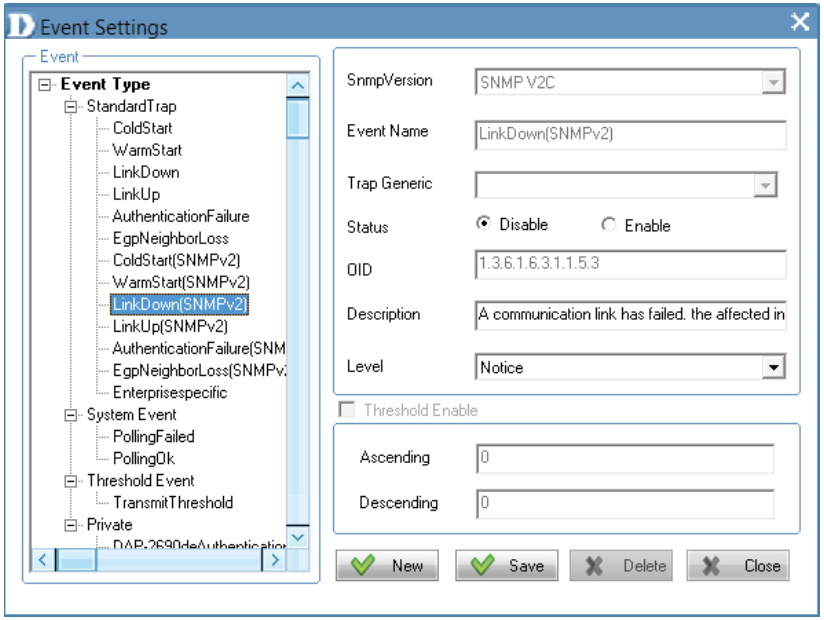
ColdStart (SNMPv2)



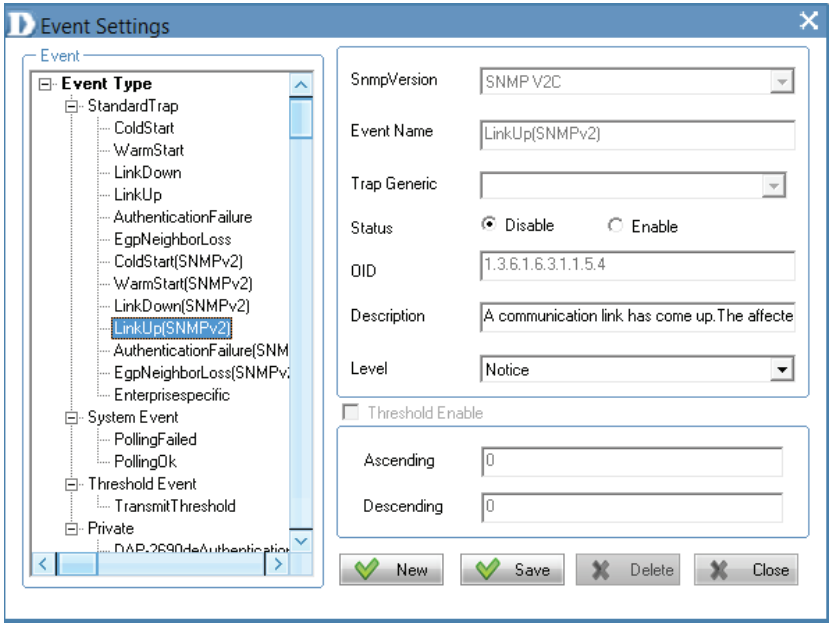
WarmStart (SNMPv2)



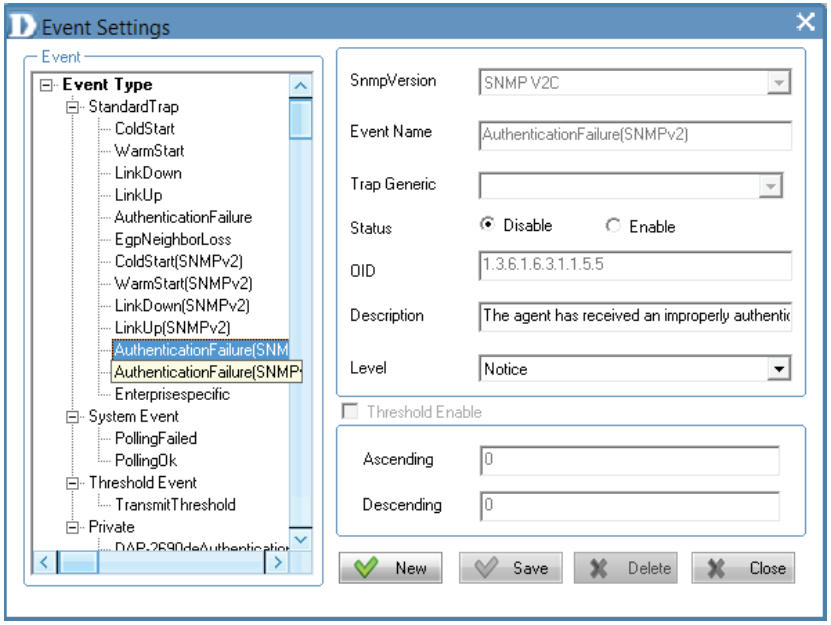
LinkDown (SNMPv2)



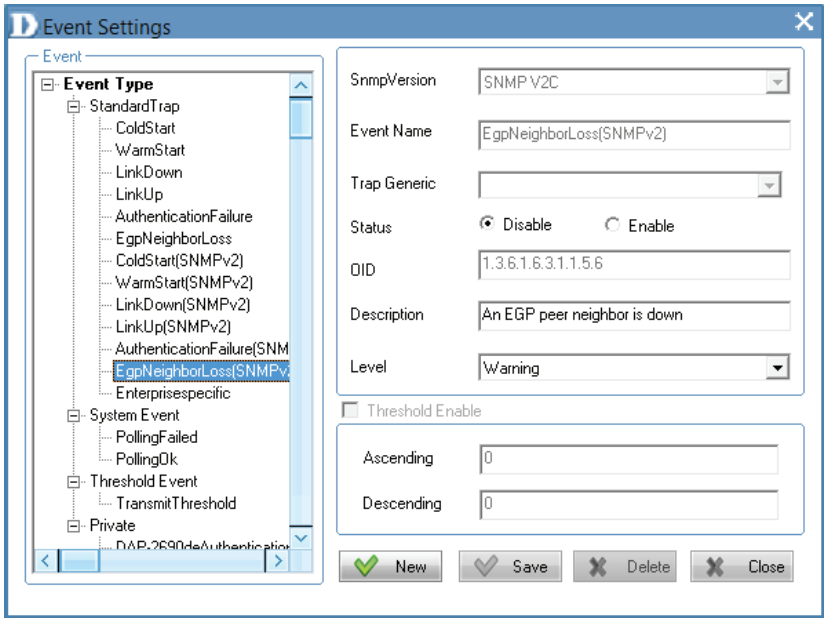
LinkUp (SNMPv2)



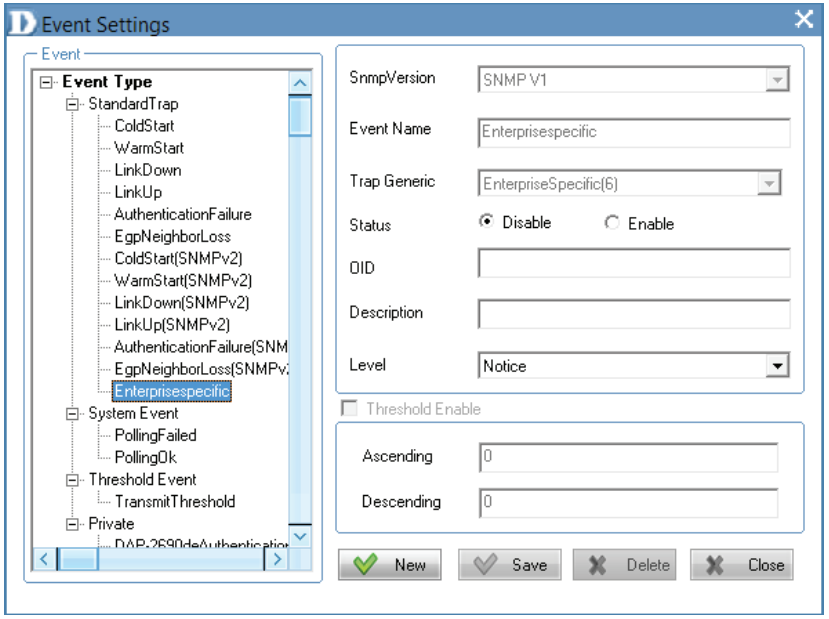
AuthenticationFailure(SNMPv2)



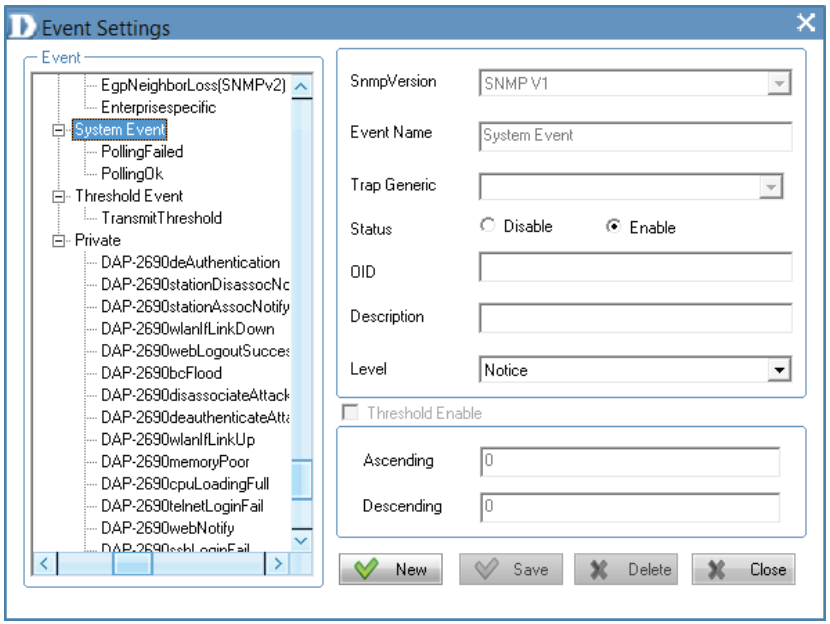
EgpNeighborLoss (SNMPv2)



Enterprisespecific



System Event - To configure the trap condition, click the System Event icon in the tool bar to set the event settings. It consists of the following options:

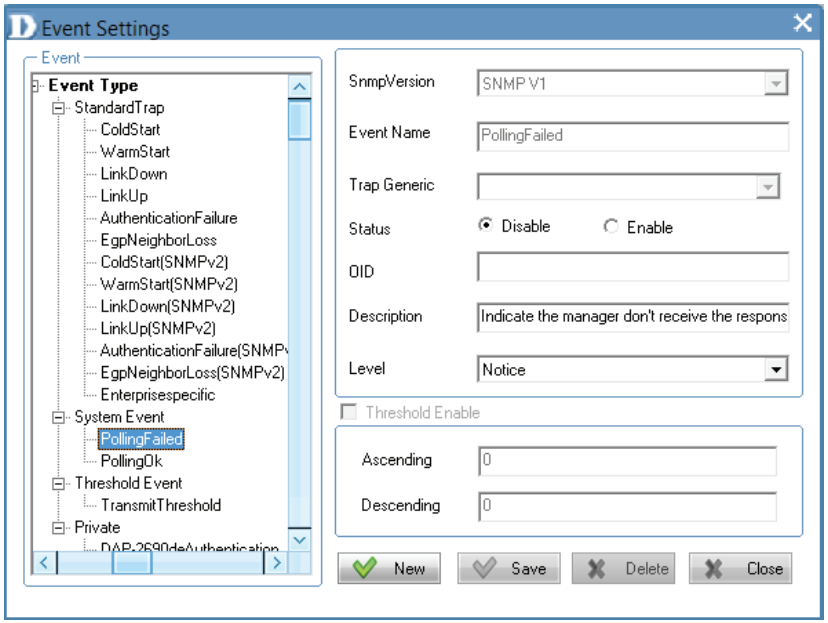


System Event

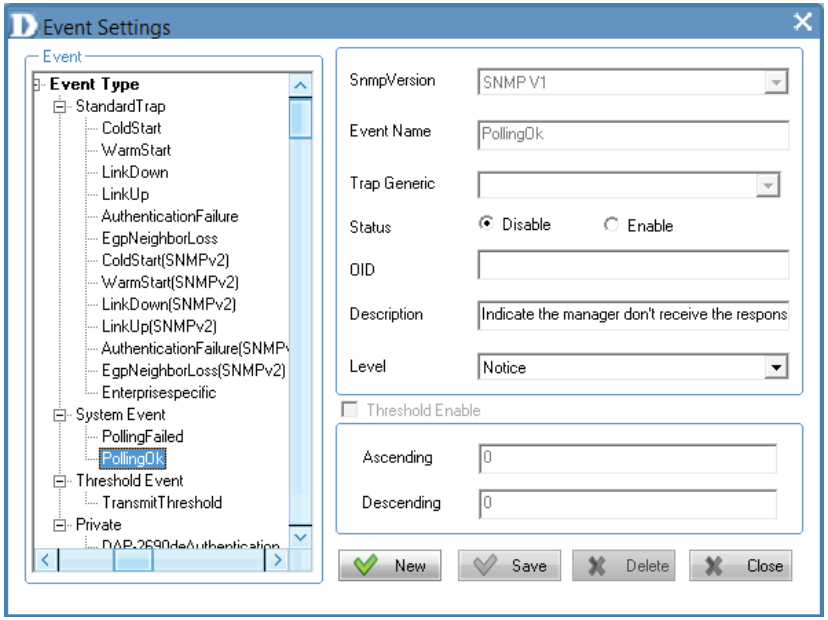
To modify an event setting, select the event from the Event Type list and then change the items. After the setting, click Save button to apply the changes.

To add a new event, click New button, and configure the settings in the event creation window.

PollingFailed

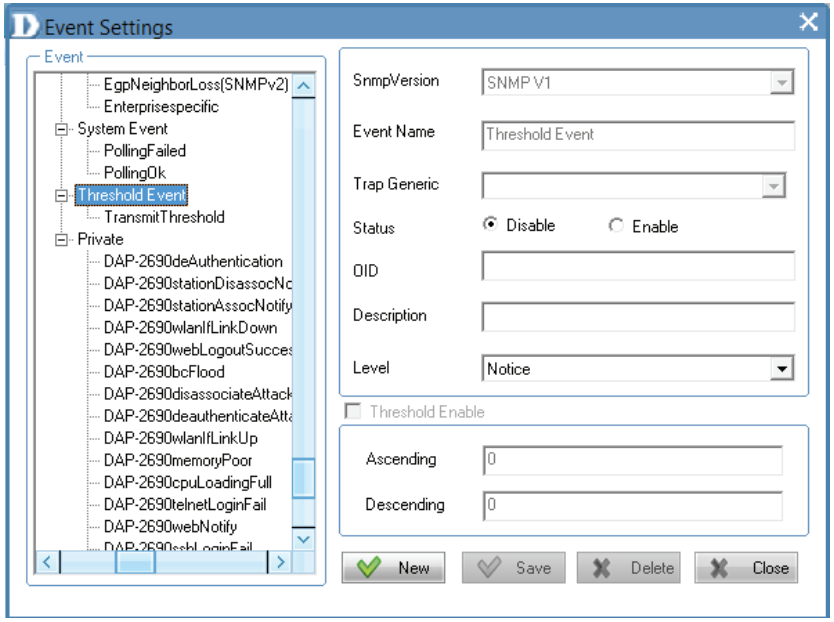


PollingOK

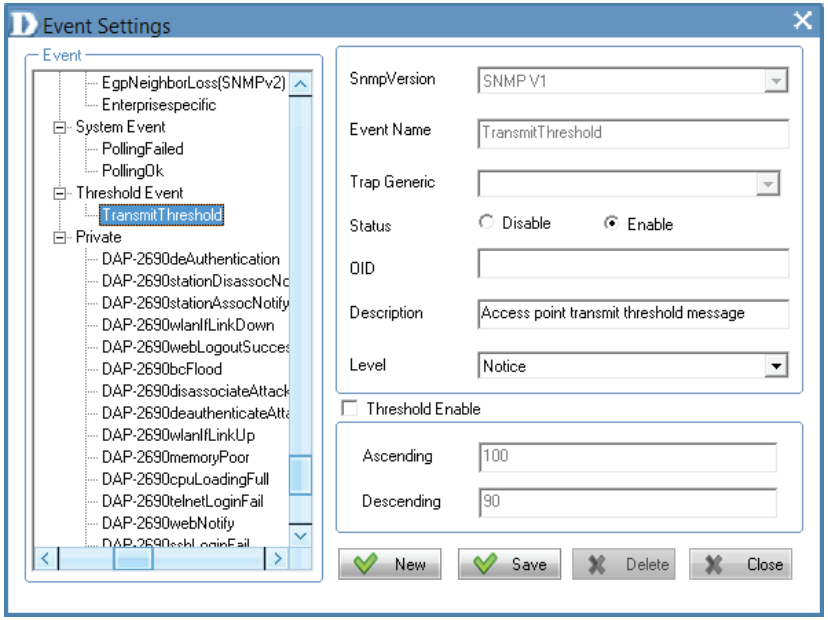


Threshold Event consists of the following options:

Threshold Event

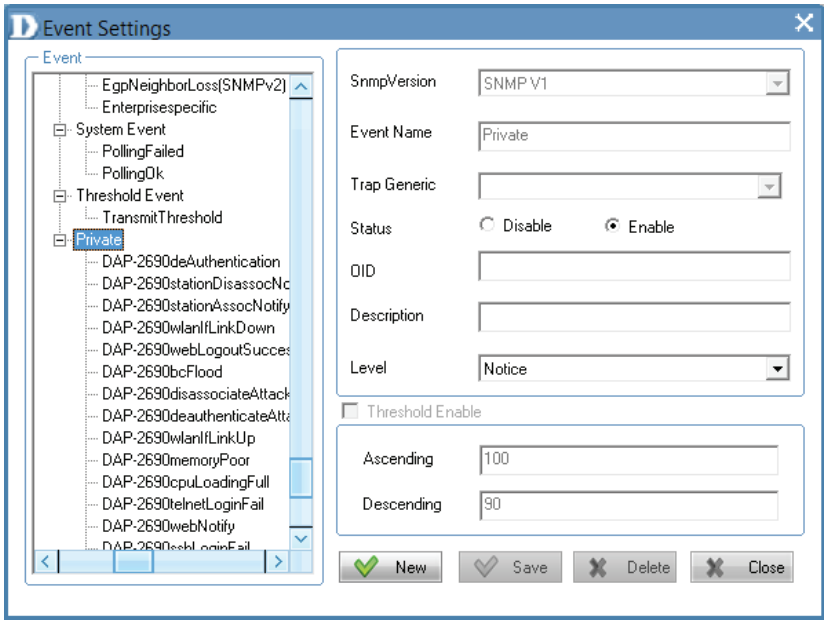


Transmit Threshold

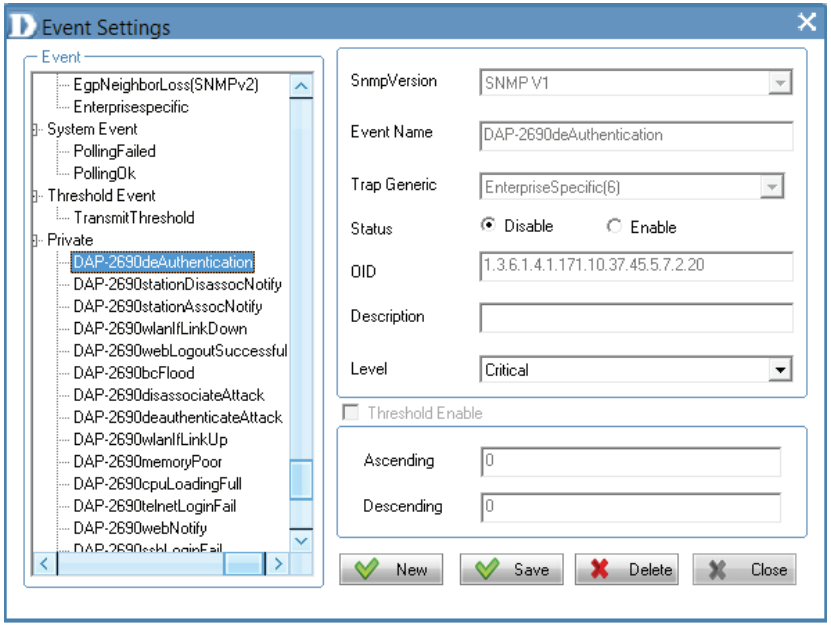


Private consists of the following options:

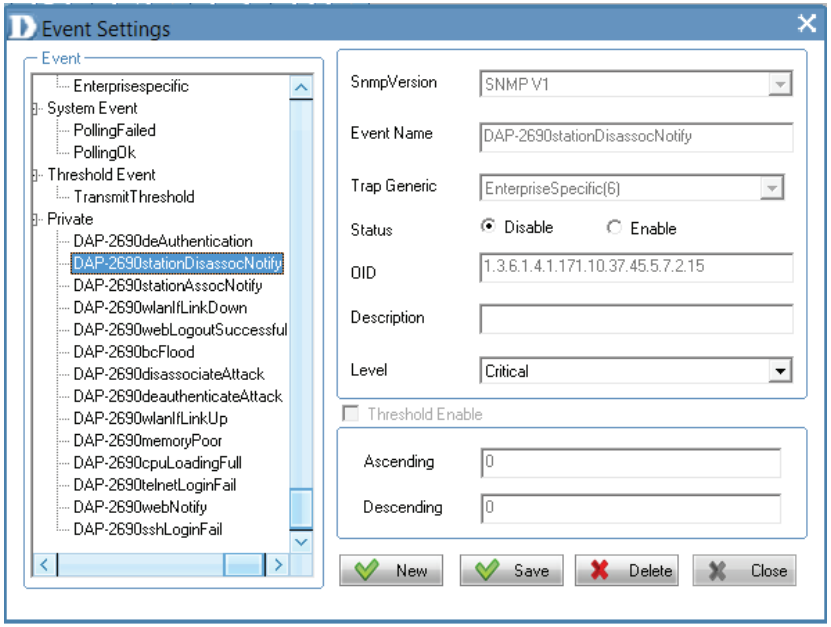
Private



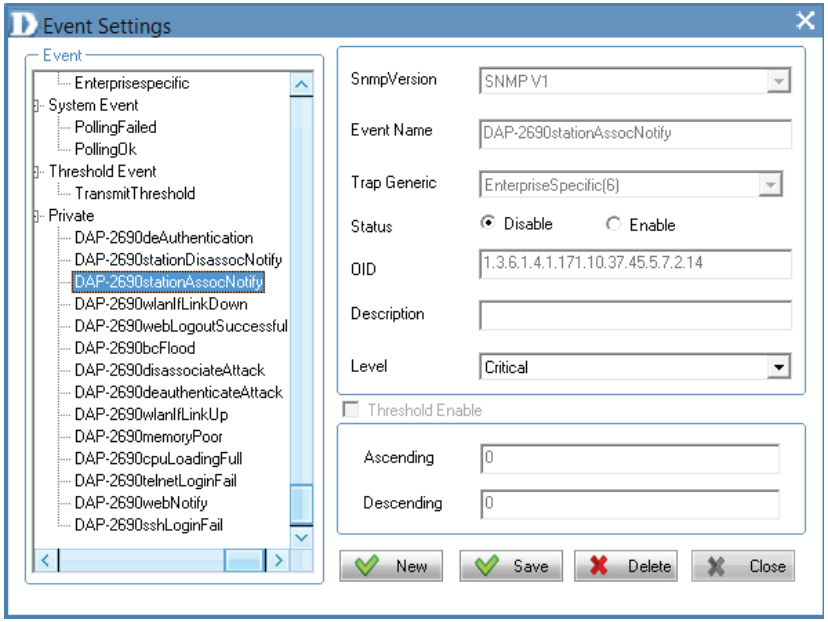
DAP-2690deAuthentication



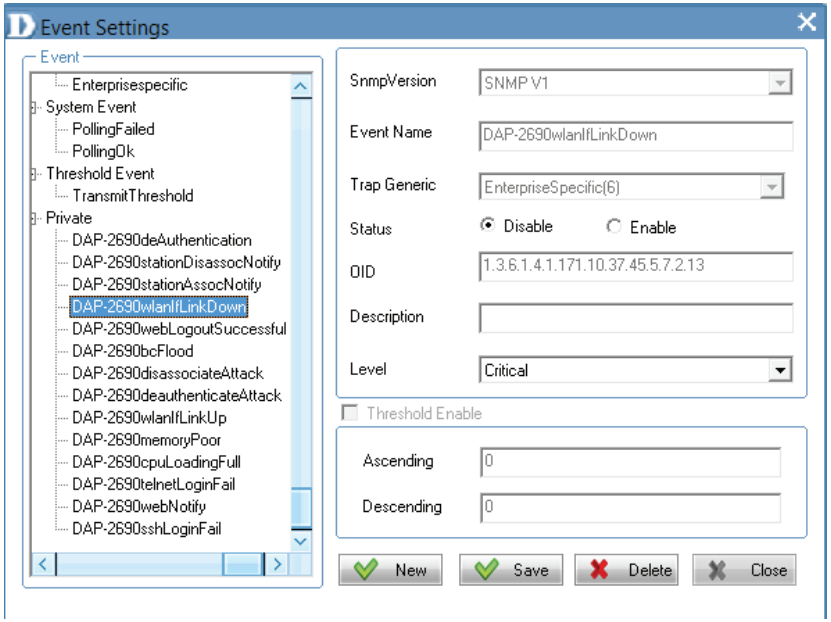
DAP-2690stationDisassocNotify



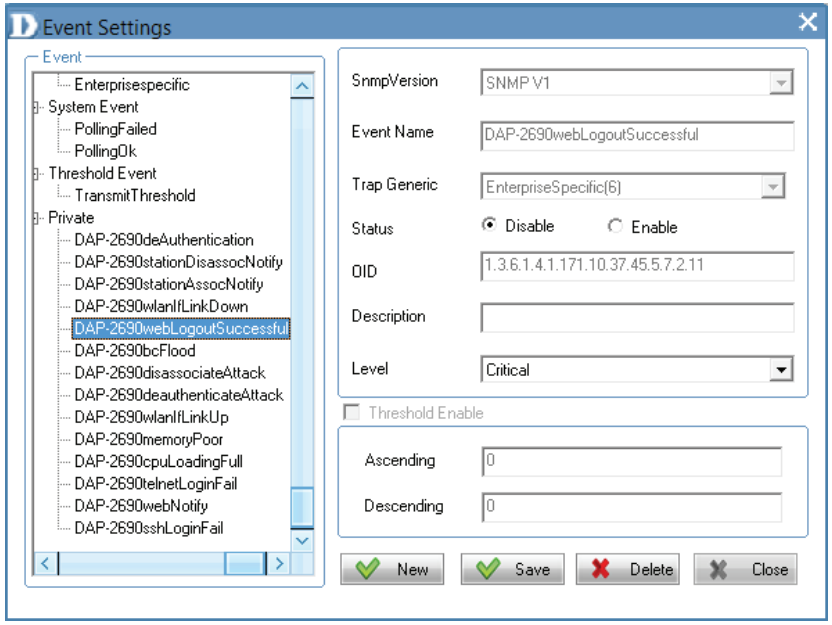
DAP-2690stationAssocNotify



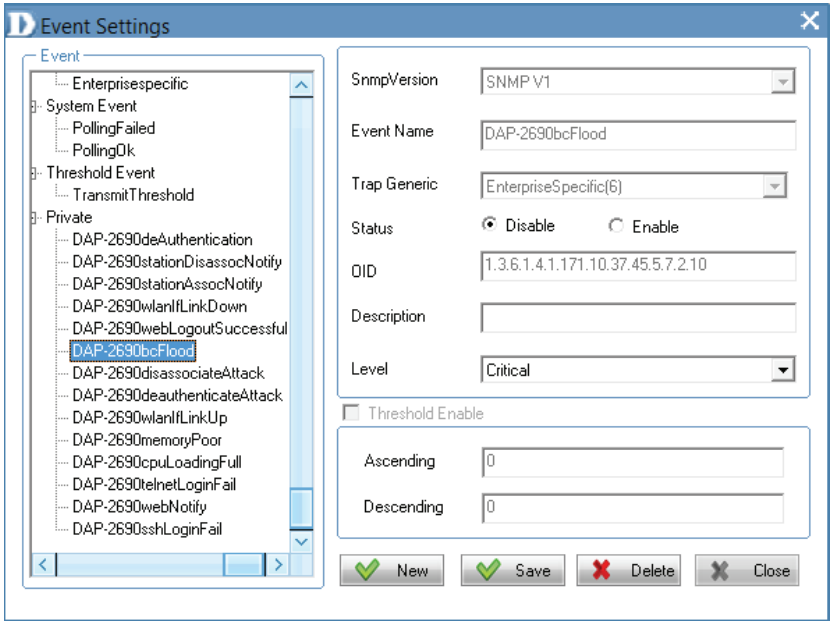
DAP-2690wlanIfLinkDown



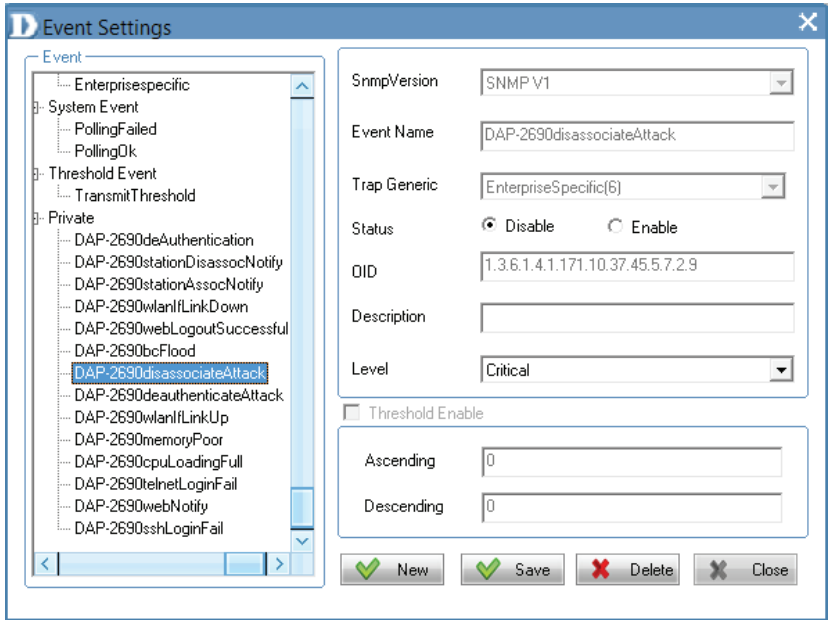
DAP-2690webLogoutSuccessful



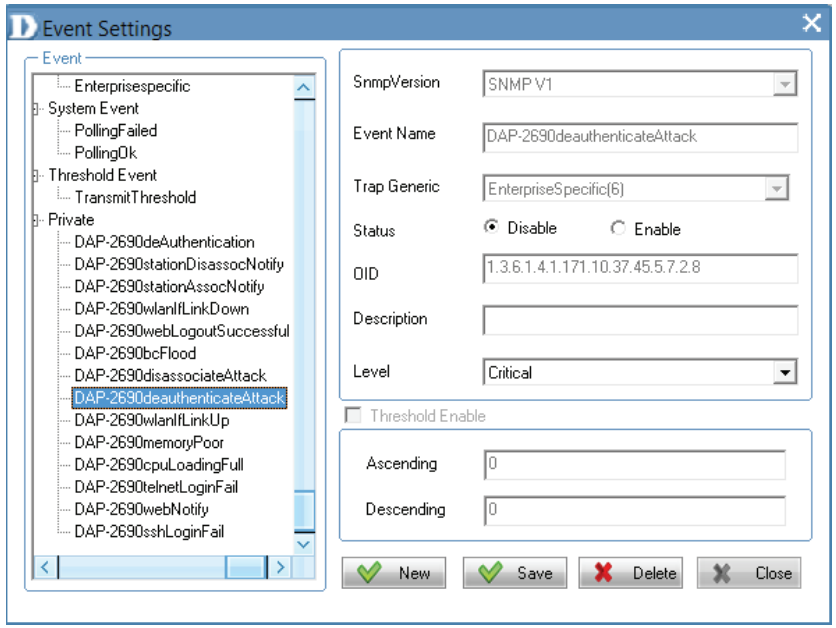
DAP-2690bcFlood



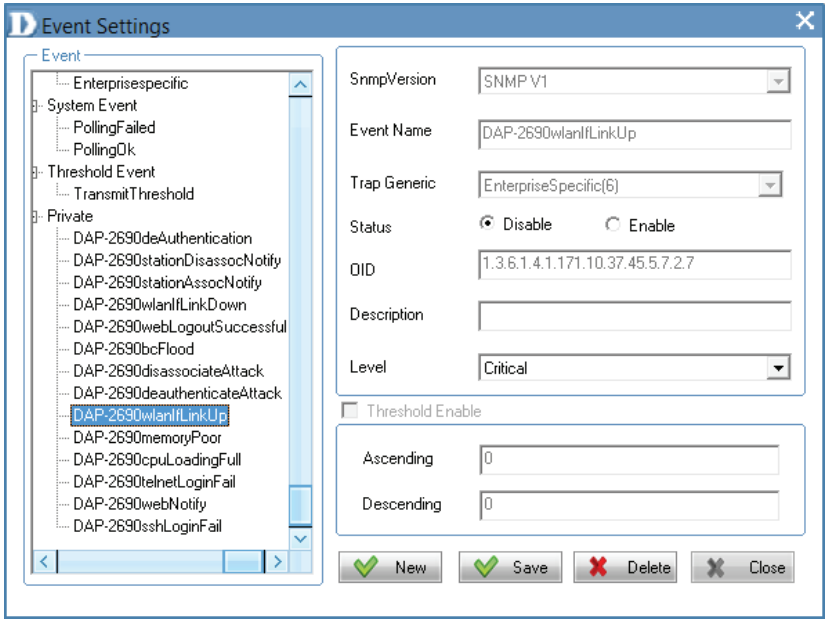
DAP-2690disassociateAttack



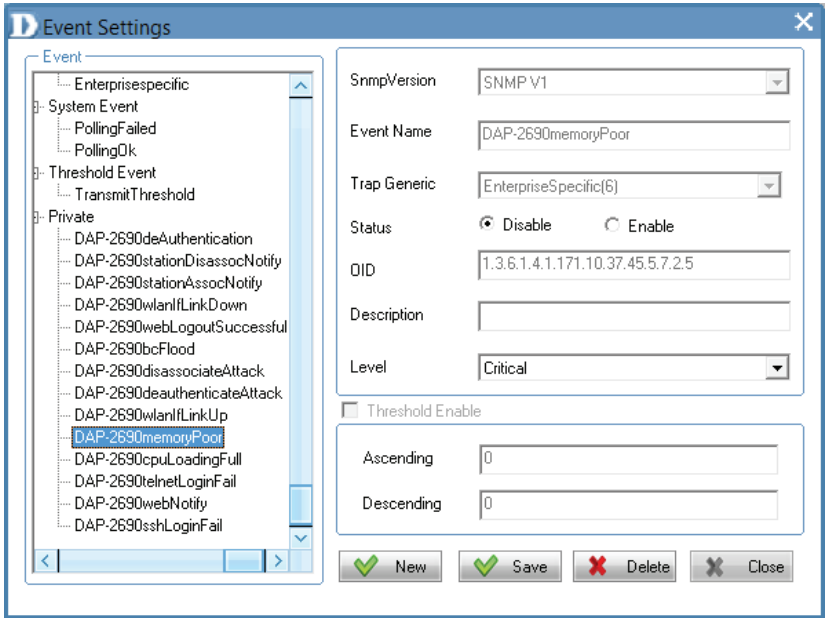
DAP-2690deauthenticateAttack



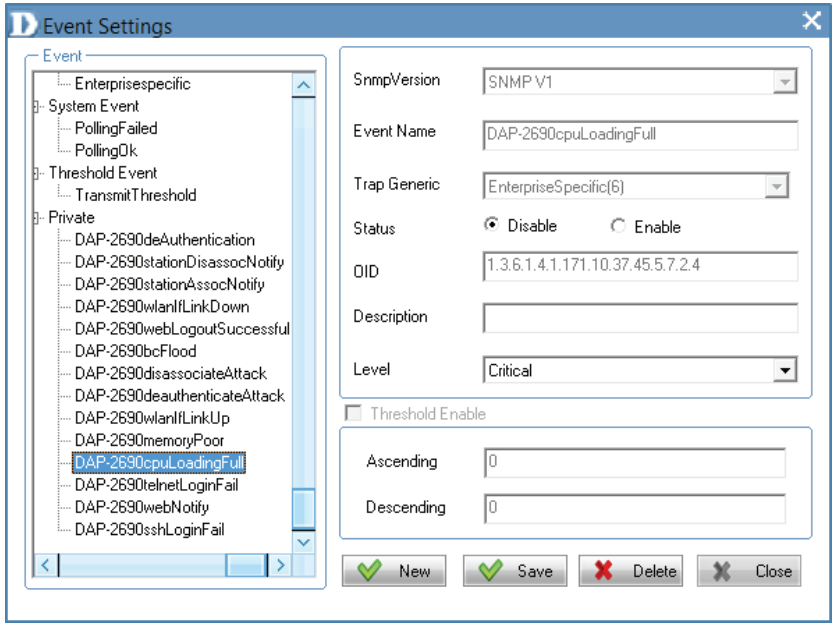
DAP-2690wlanIfLinkUp



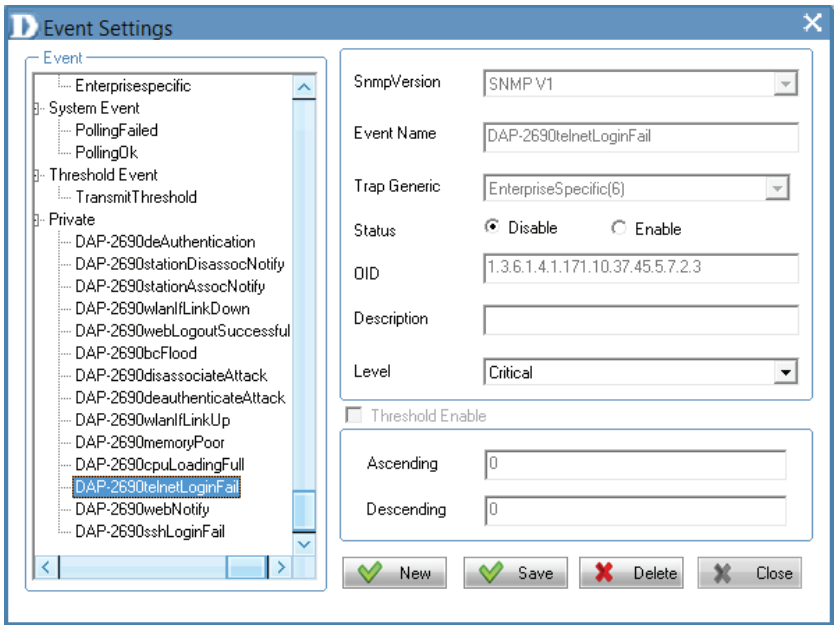
DAP-2690memoryPoor



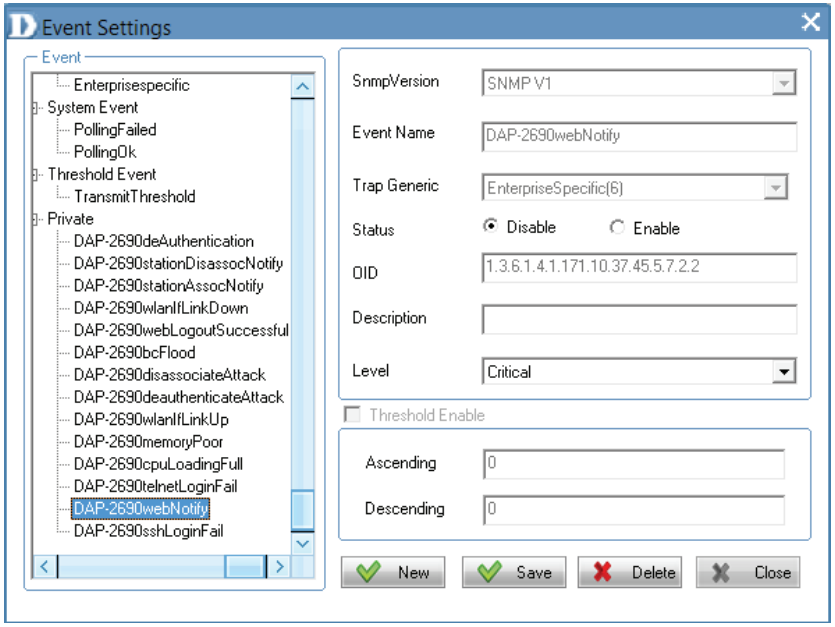
DAP-2690cpuLoadingFull



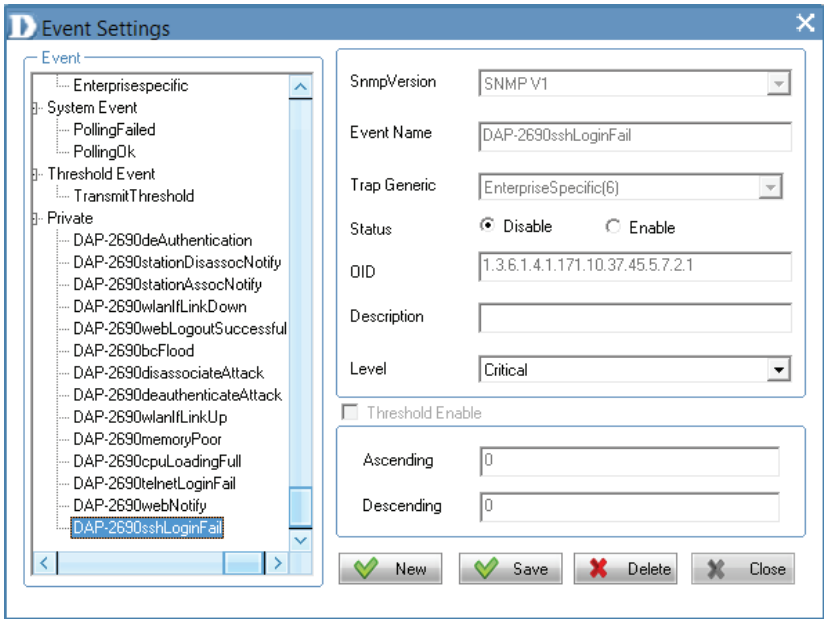
DAP-2690telnetLoginFail



DAP-2690webnotify

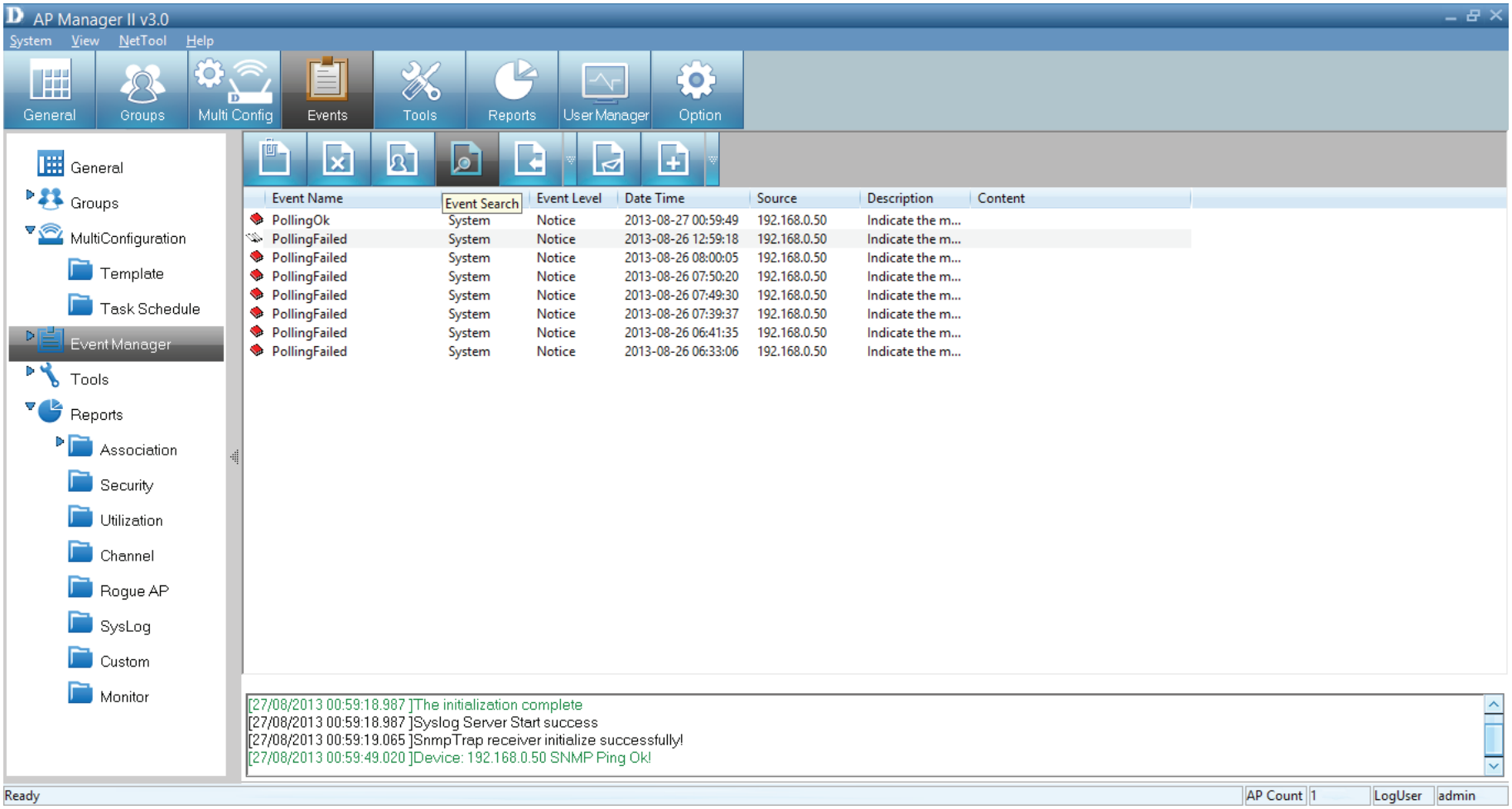


DAP-2690sshLoginFail

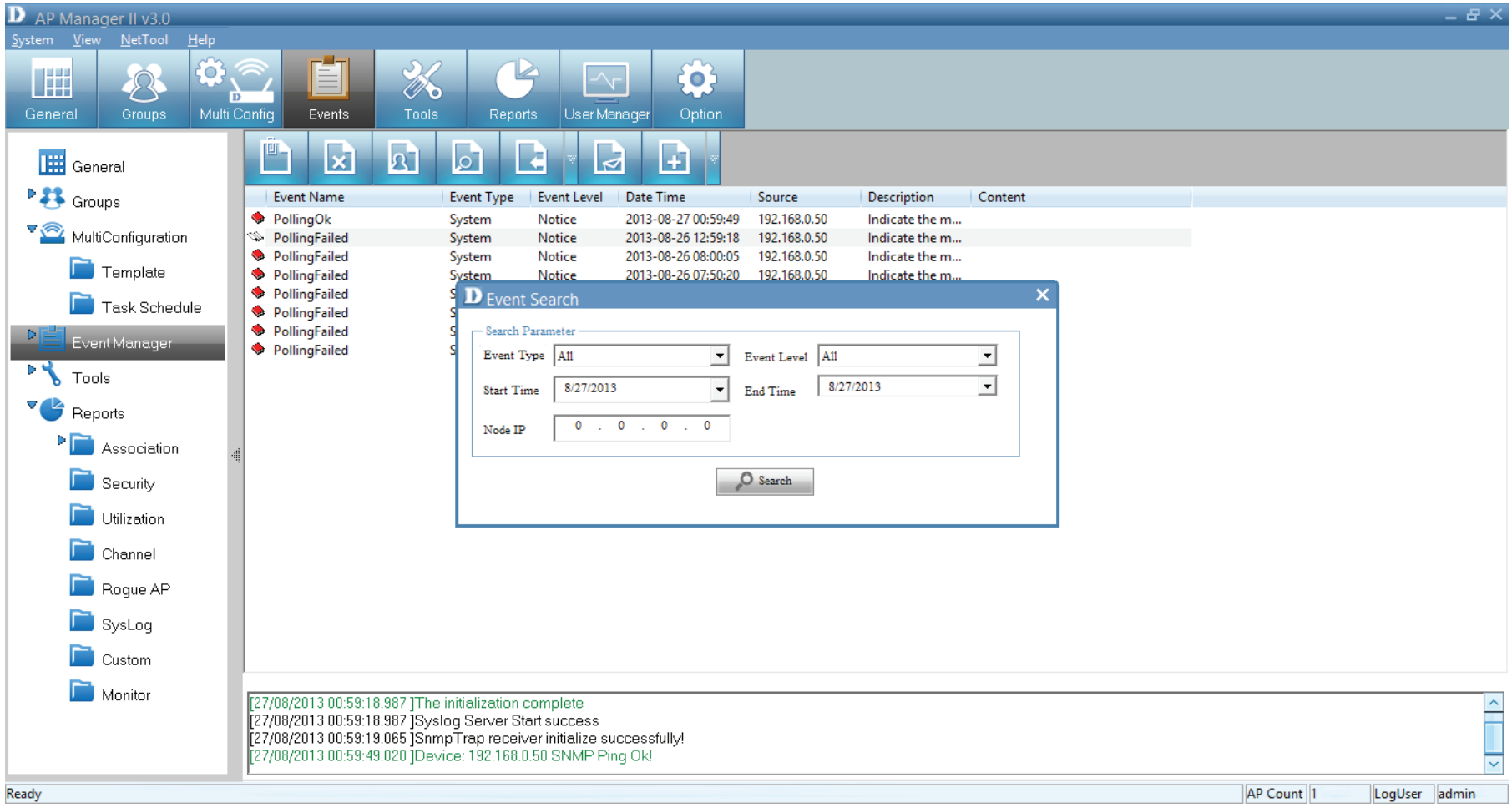


AP Manager II v3.0 - Event Search

Click this icon to showthe results of an **Event Search**

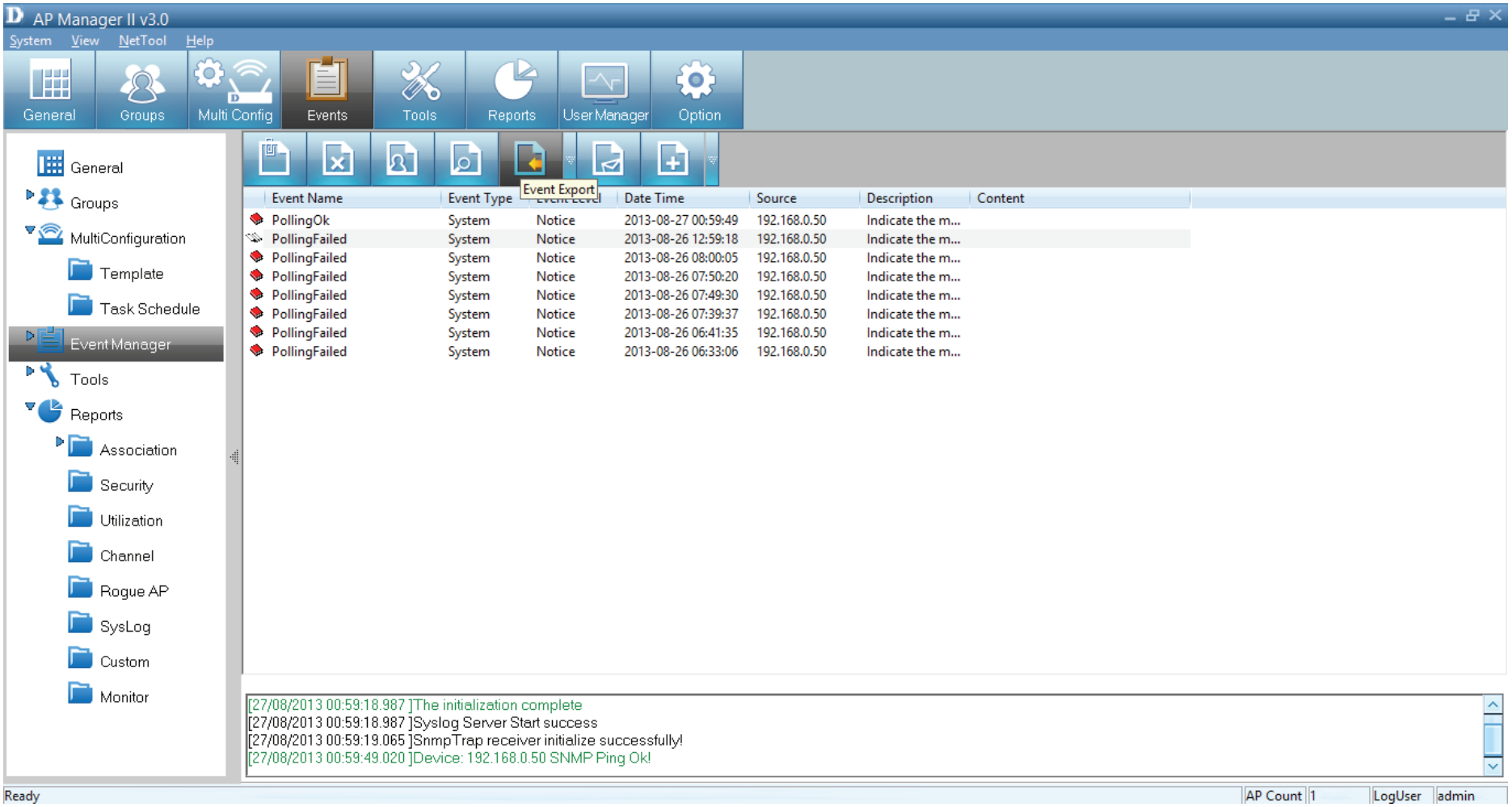


Once you have clicked the **Event Search** icon, a box opens for you to enter the **Event Type**, the **Event Level**, **Start Time**, **End Time**, **Node IP** and click **Search**



AP Manager II v3.0 - Exporting Events

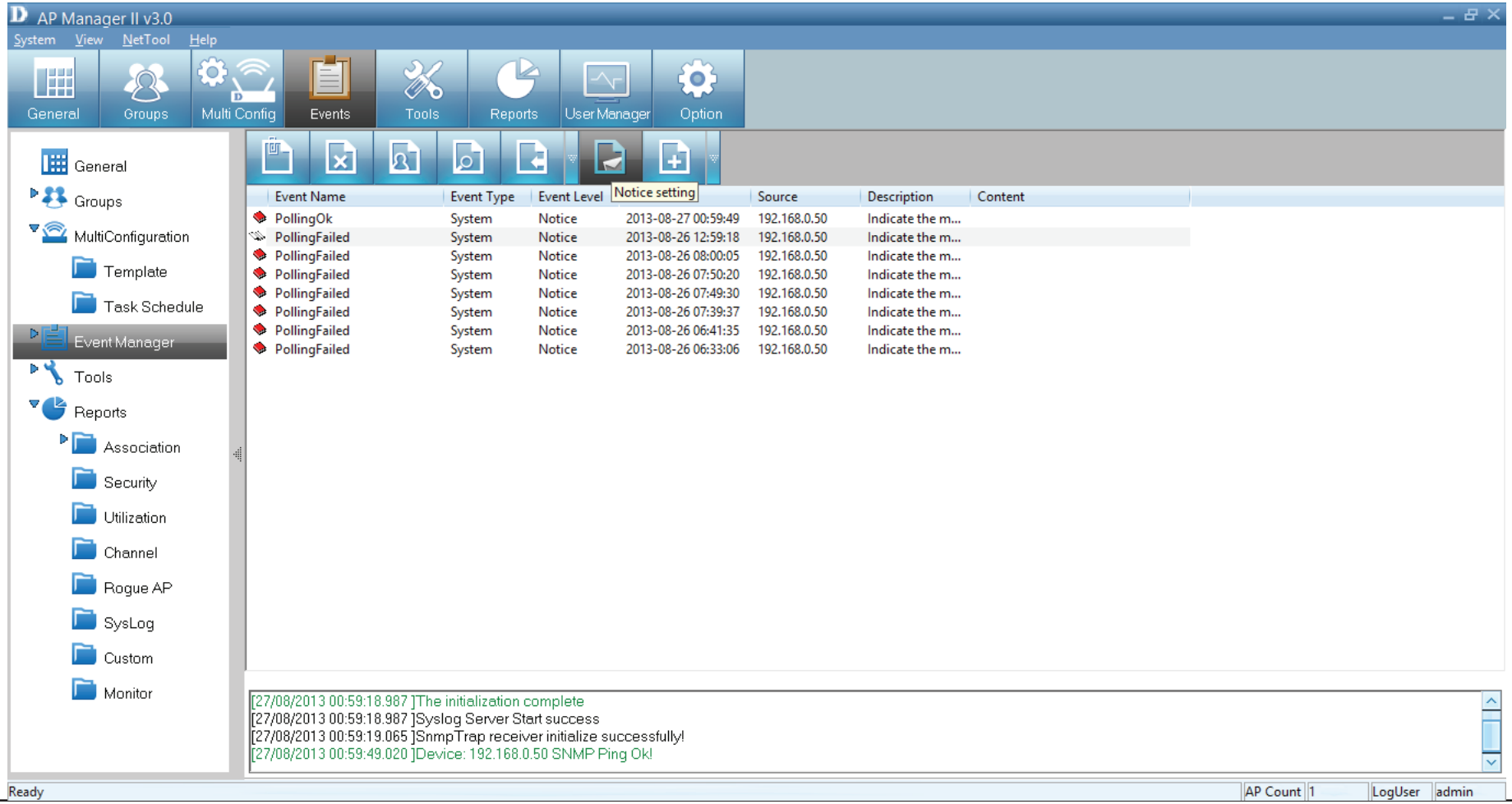
Click this icon to do an **Event Export.** AP Manager II v3.0 can export the event results to the files in the format of **Text/Excel/PDF**. To save event results, highlight the event record in the event window and click the Event Export icon in the tools bar, then select the file format you want to save, AP Manager II v3.0 will save all the records of that type to file.



AP Manager II v3.0 - Setting Notices

Click this icon to view the Notice Settings. AP Manager II v3.0 can set the corresponding actions when some level of events occurs. To configure the notice setting, click the Notice Settings icon in the tools bar, as shown below

Play sound: Click Browse to select the sound file. AP Manager II v3.0 will play the sound file when this level of event occurs
Show Pop Message: AP Manager II v3.0 will pop a message window when this level of event occurs
Send Email: Enter the Email information of To/From email address, SMTP server, UserName/Password [Optional], Subject and Message in the respective column. AP Manager II v3.0 will send this email when this level of event occurs.

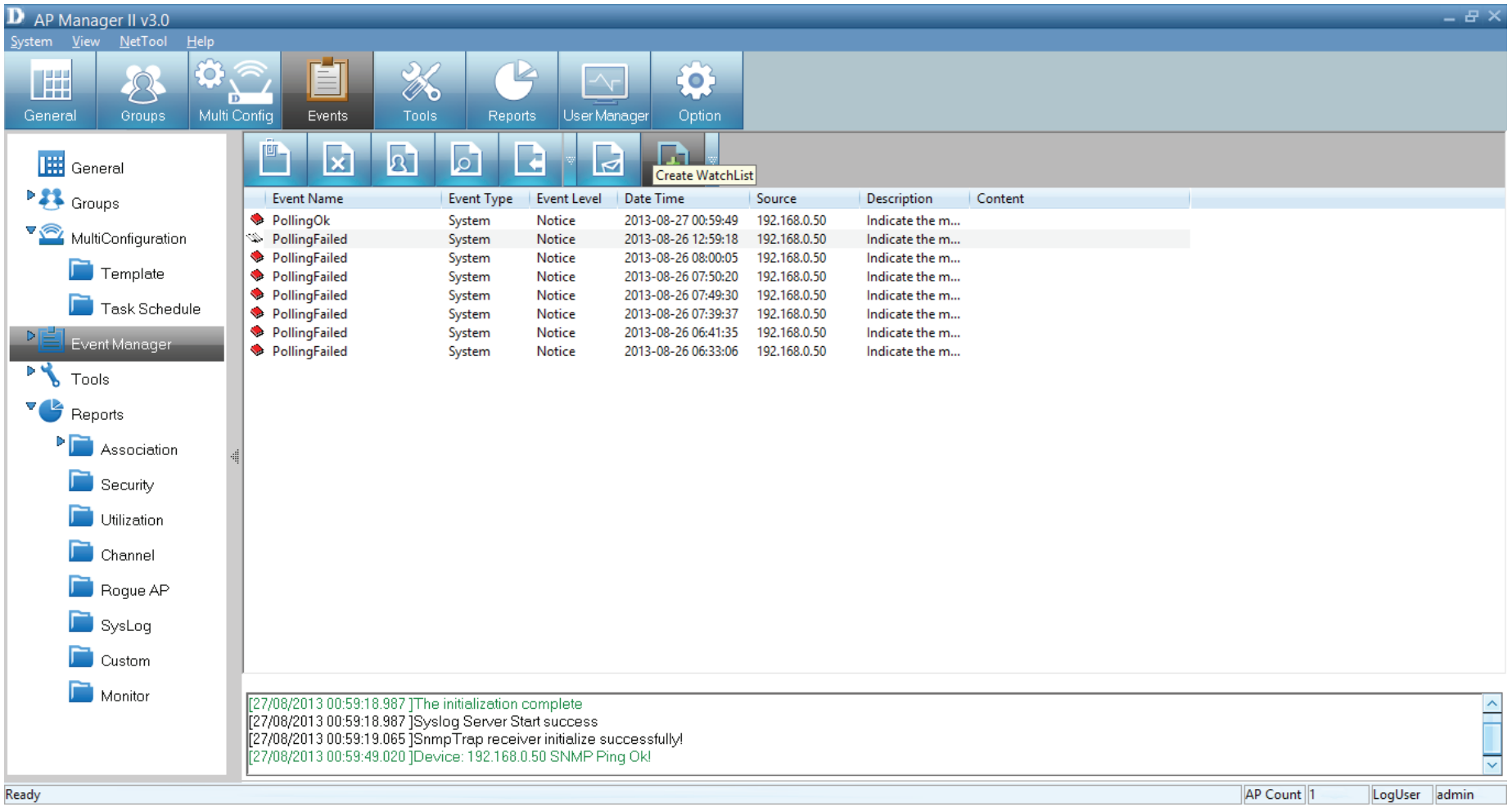


AP Manager II v3.0 - Create Watchlist

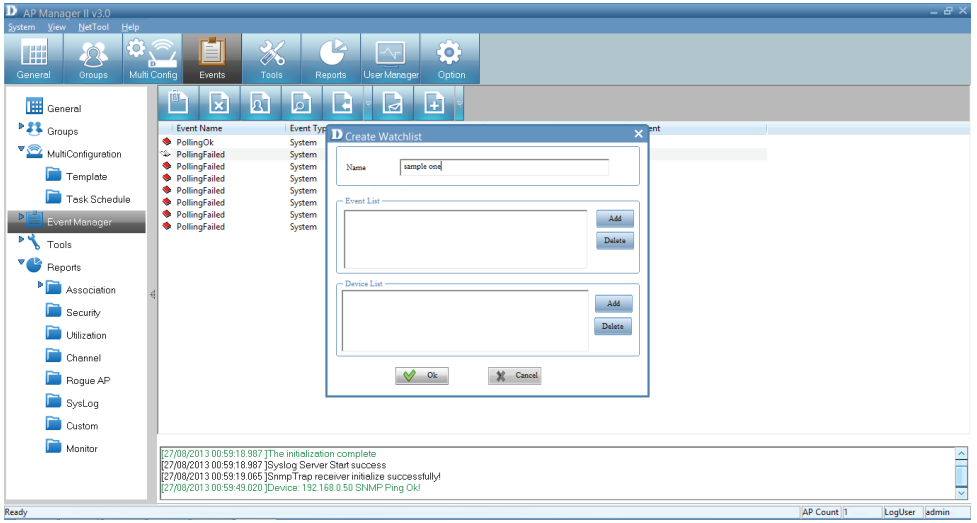
AP manager II v3.0 allows a user to add custom watch list(s) which only shows the specified devices and events.

To create a watchlist, please follow the steps below:

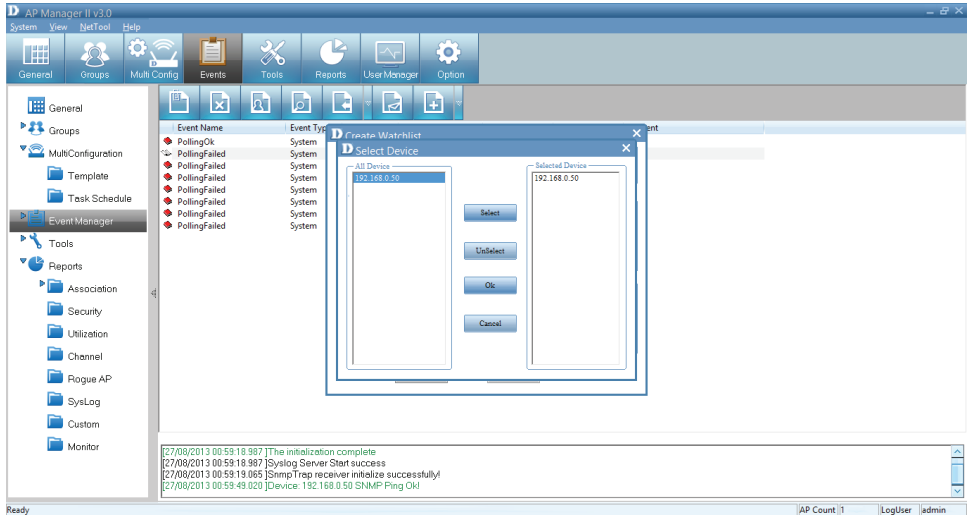
Click the **Create Watchlist** item under the icon of the tools bar, and enter the **Watch list Name** in Create list form.



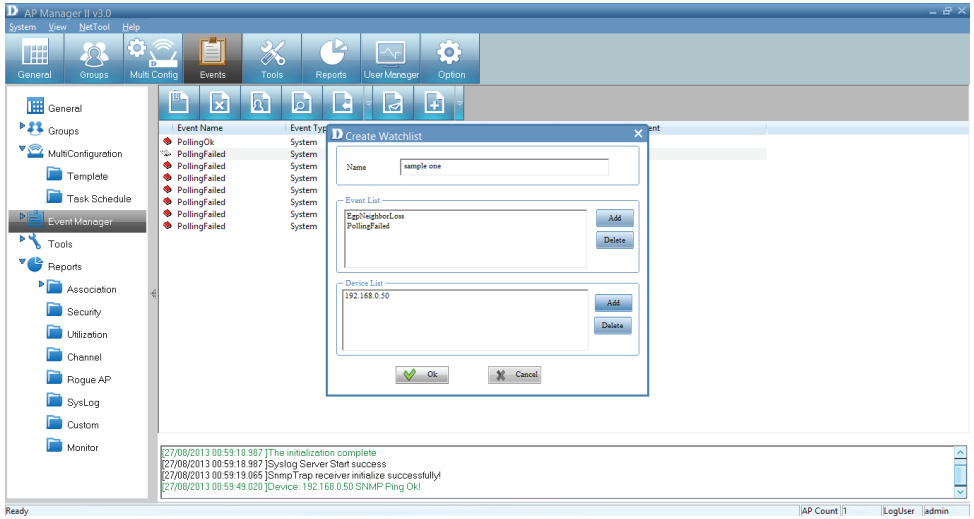
Enter the **Watch list Name** in Create list form.



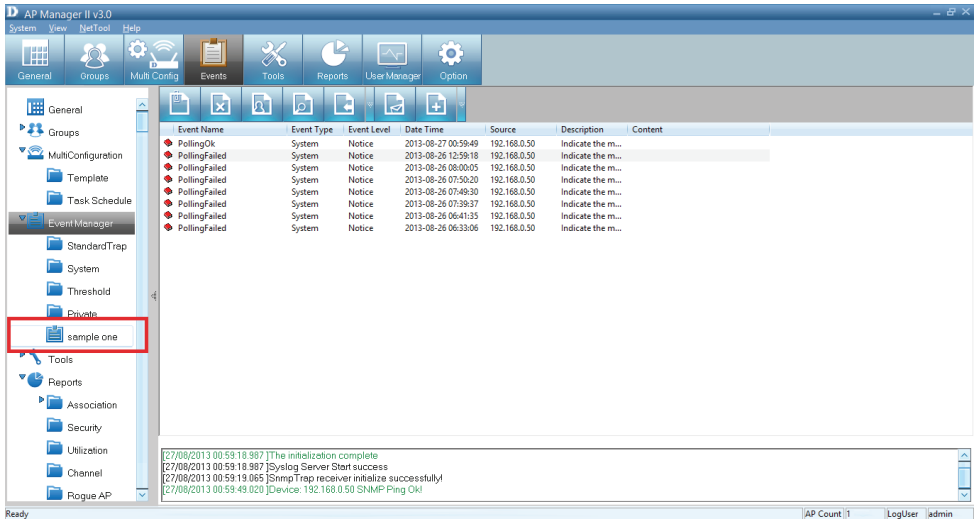
Click the **Add** button to insert the events into event list, and select the events that need to be added in Select Event form, click the Select button, then click the OK button



Click the **Add** button to insert the devices into device list, and select the devices that need to be added in Select Device form, click the Select button, then click the OK button.

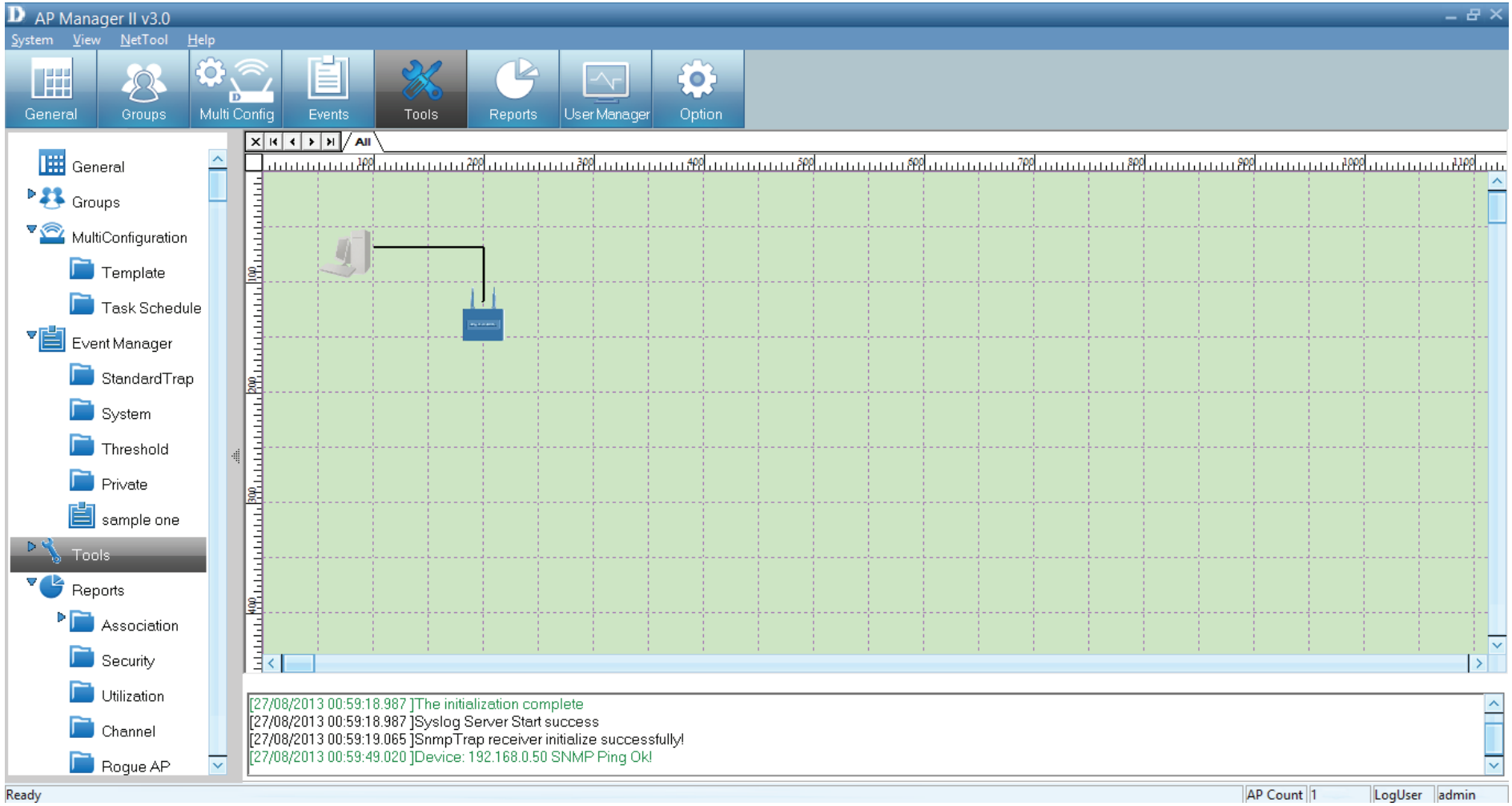


The new **Watchlist** now appears on the left-hand panel.

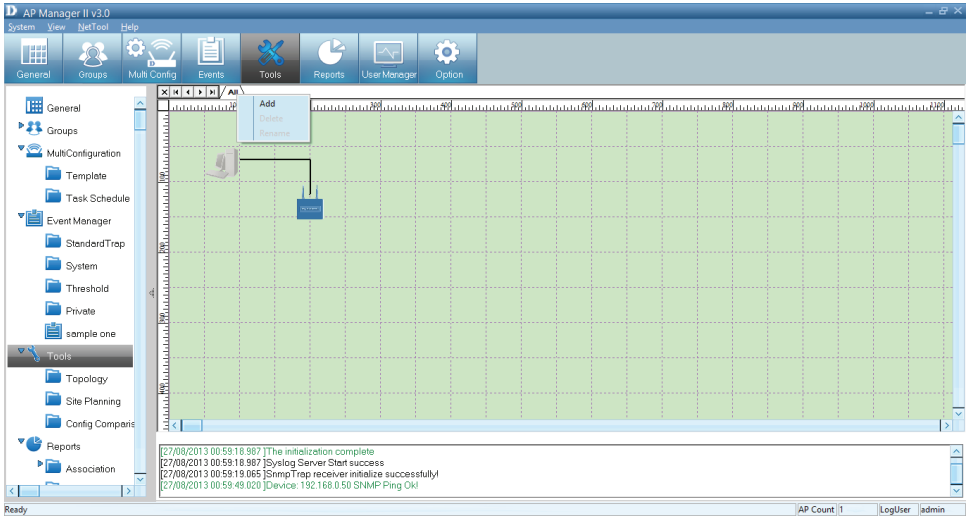


AP Manager II v3.0 - Tools - Topology

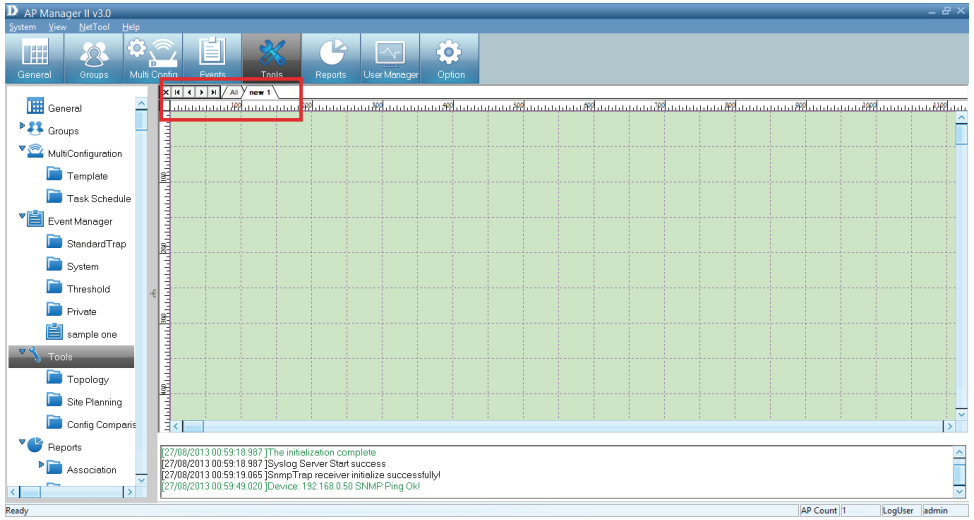
You can create a topology map to graphically represent planned or existing networks to aid network design, and also AP Manager II v3.0 will periodically poll network devices to monitor its status. You can further customize their diagrams with selected icons and bitmap files used for the background. When a topology map is opened, AP Manager II will discover the devices connected on the network and display their icons on the map.



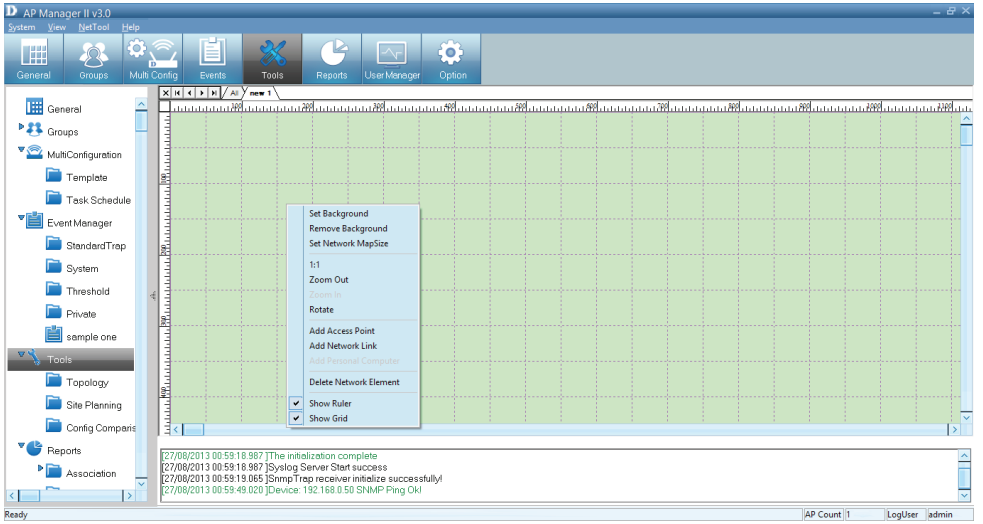
To create a new topology view, right-click on the tab, and click **Add.**



The new workspace is created.

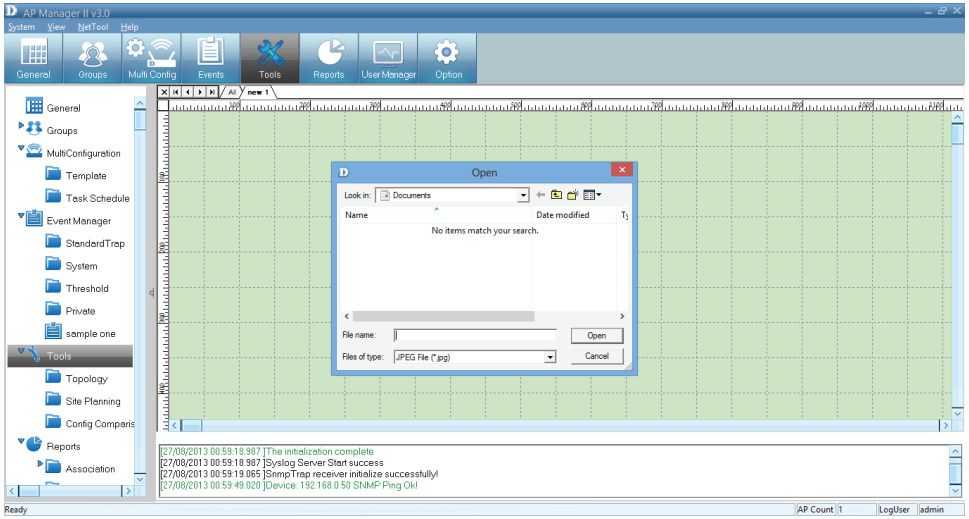


Right-click on the workspace.



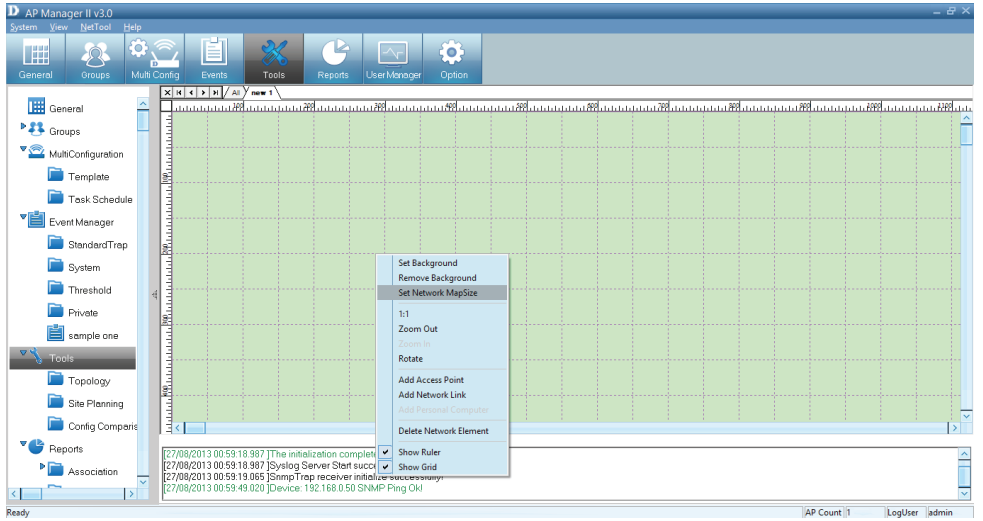
To change the background, click **Set Background**. The edit window opens for you to browse to the folder where you want to change the color. Click **Open** to load.

To remove the background, right-click the blank area and select Remove Background.

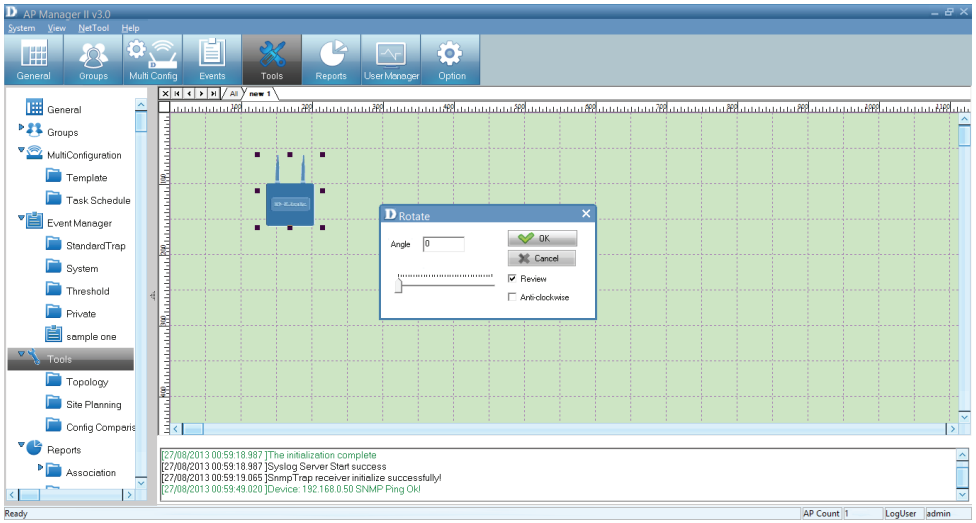


To **Set Network Map Size**, right click and click Set Network Map Size. The Map Size window appears.

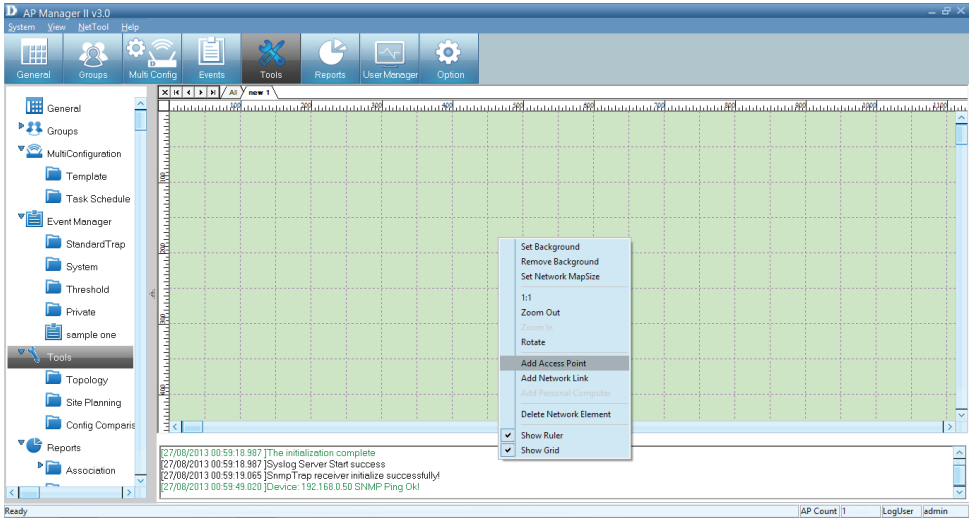
Change the **Width** and **Height** settings and click **OK**.



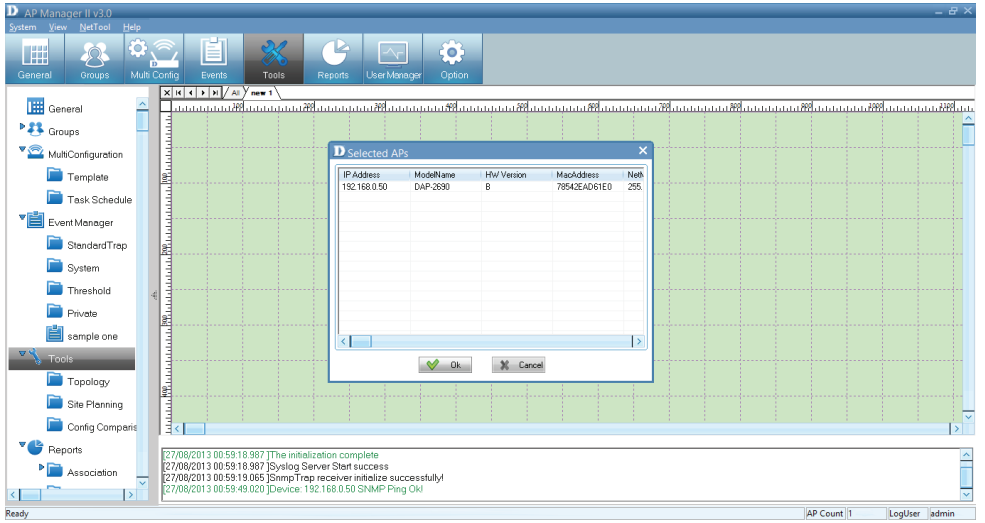
To **Rotate** the image, select the image first and click **Rotate**. Enter a figure in the field provided or use the slider to set the rotation. Click OK when complete.



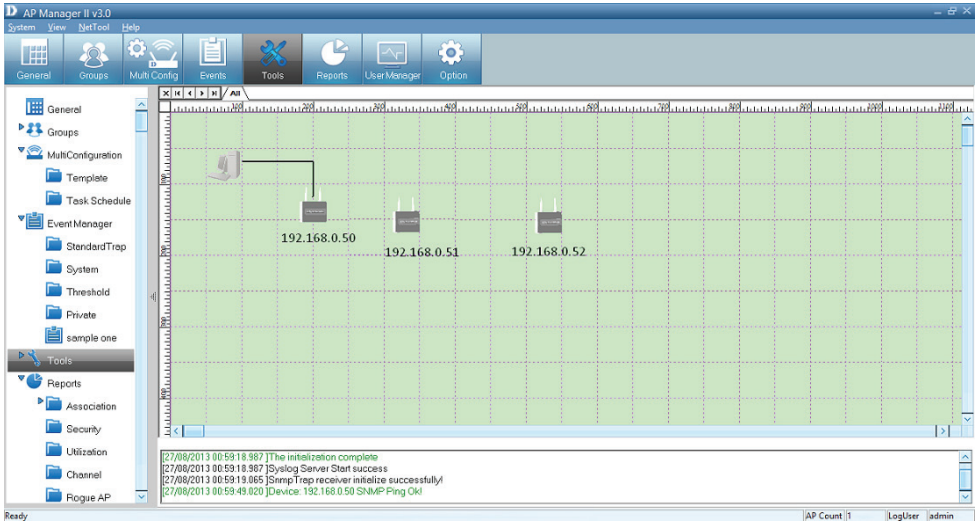
To add an access point, right-click in an open space and select **Add Access Point**.



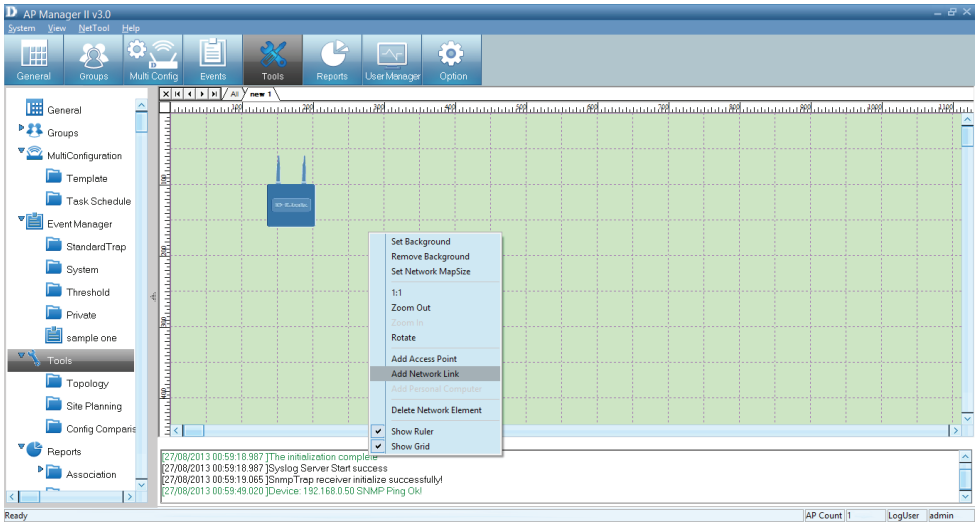
Under **Selected AP**s, select the new Access Point you wish to use and click OK. The new Access Point appears on the screen alongside the Access Point you previously had.



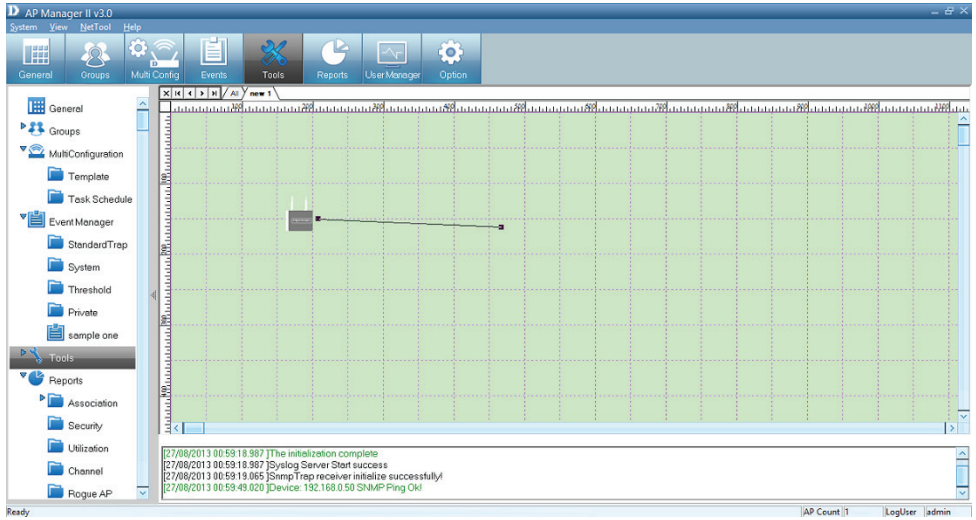
The new Access Points appear on the workspace.



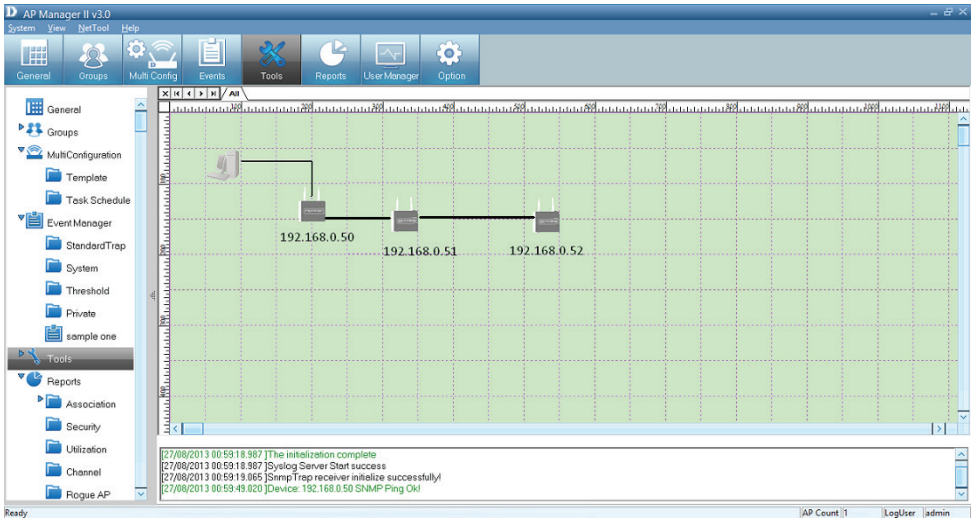
To add lines, and organize the APs more efficiently, right-click in the workspace and click **Add Network Link**.



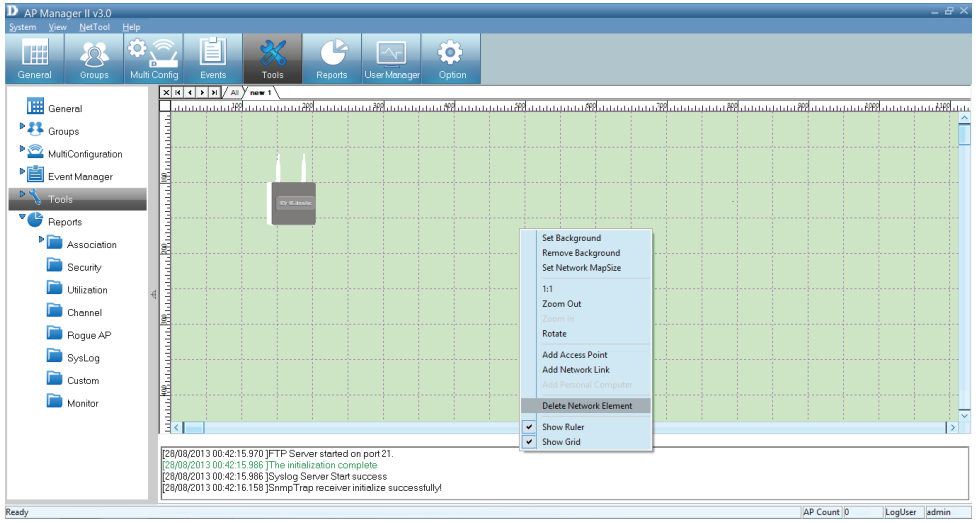
A drawing icon appears for you to create a line between devices.



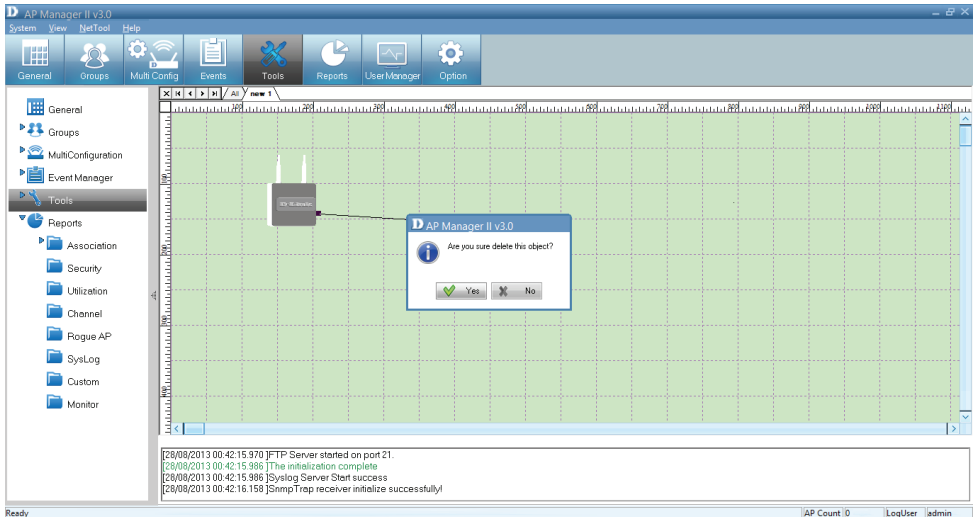
The topology now appears like normal network schematic.



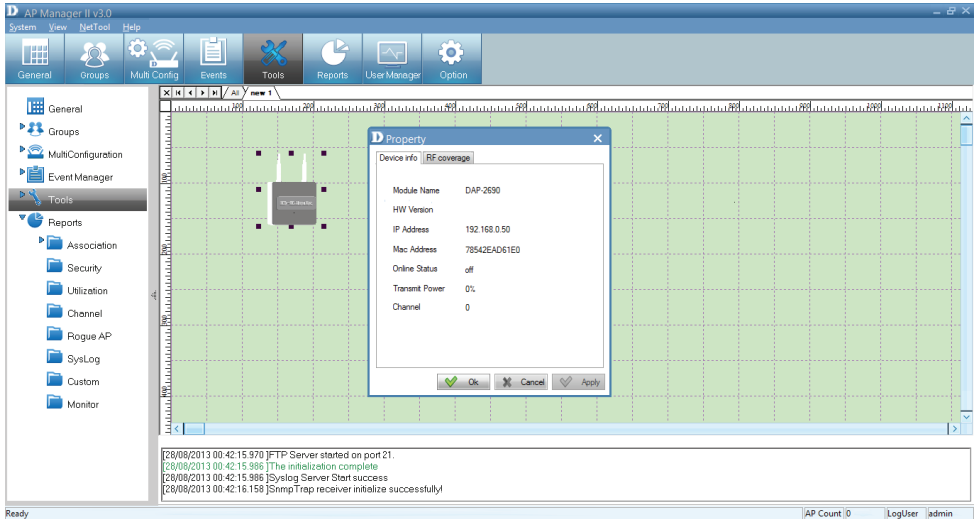
To delete a device, right-click the device and click **Delete Network Element**.



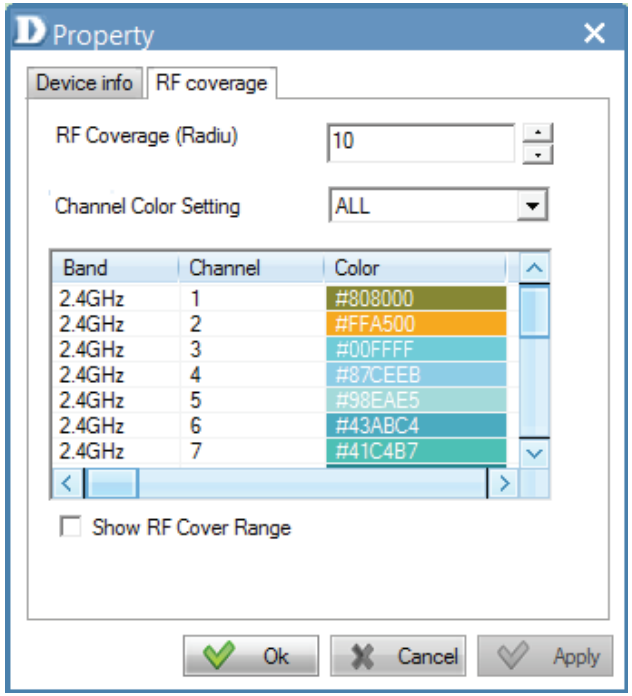
A warning message appears prompting you to verify your selection. Click **Yes** to continue with deleting the device or click **No**.



To find out the properties of each device, double-click the device. The Properties window appears.

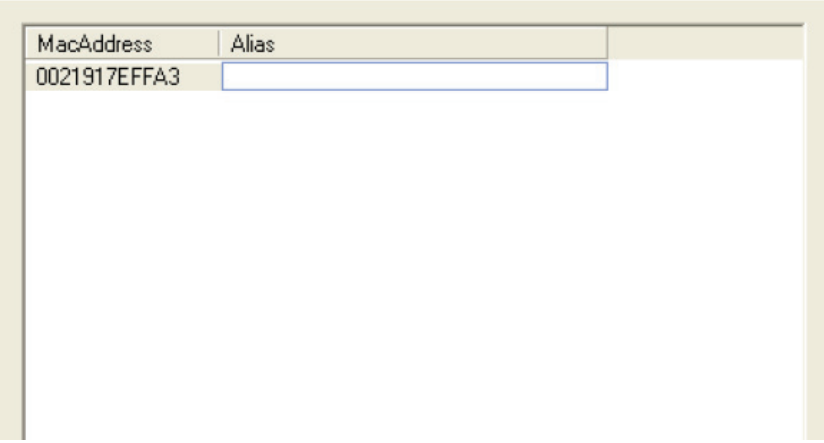


To define the **RF Coverage**, select the **RF Coverage tab**, click the up/down arrows to select the **RF Coverage**.



To define the channel color settings, click ALL or the device you want to configure. Double-click each channel or the color you want to change. A color pallette pops up for you to select a new color.

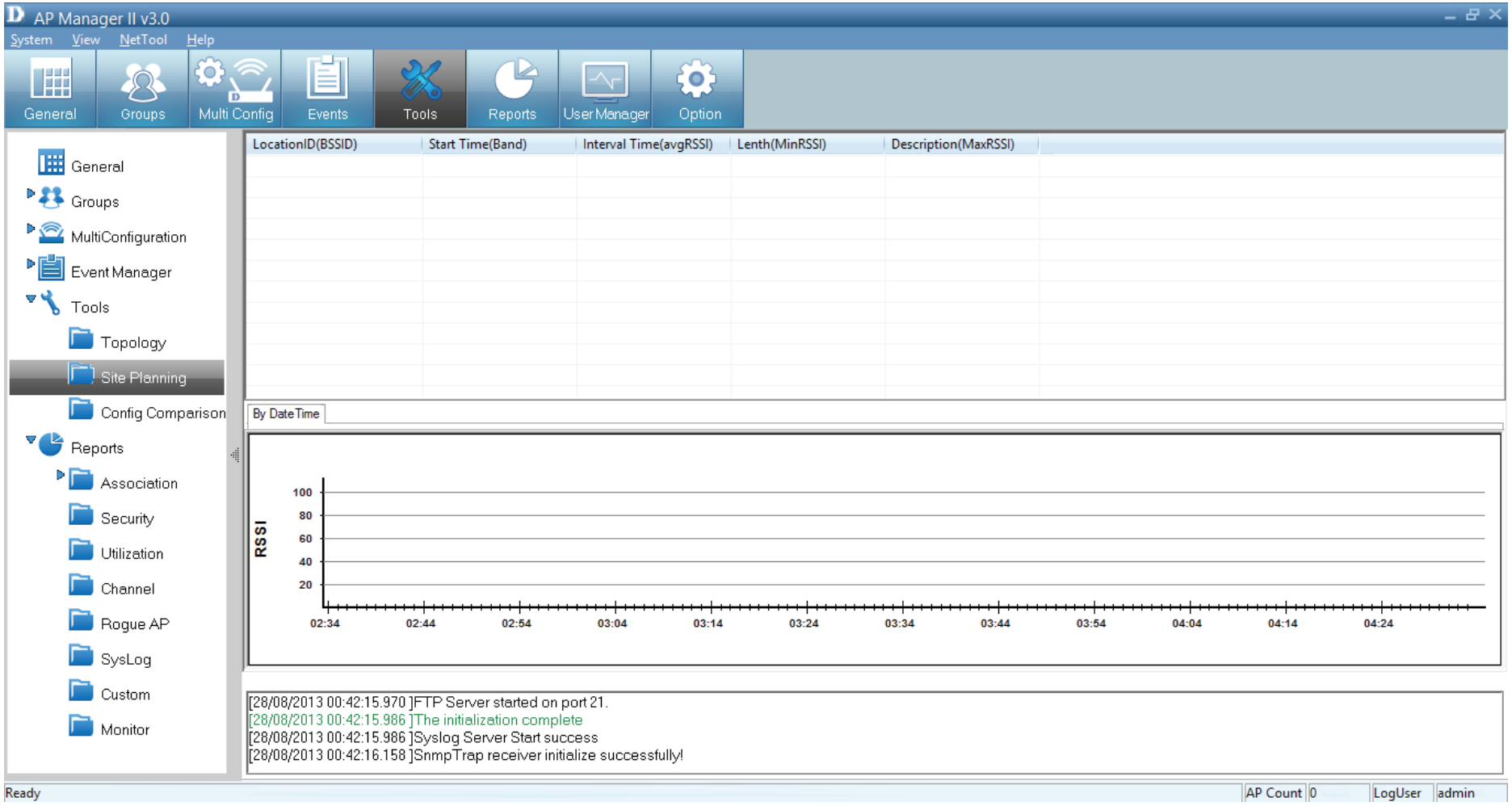
Click **Apply** and **OK** to finish.



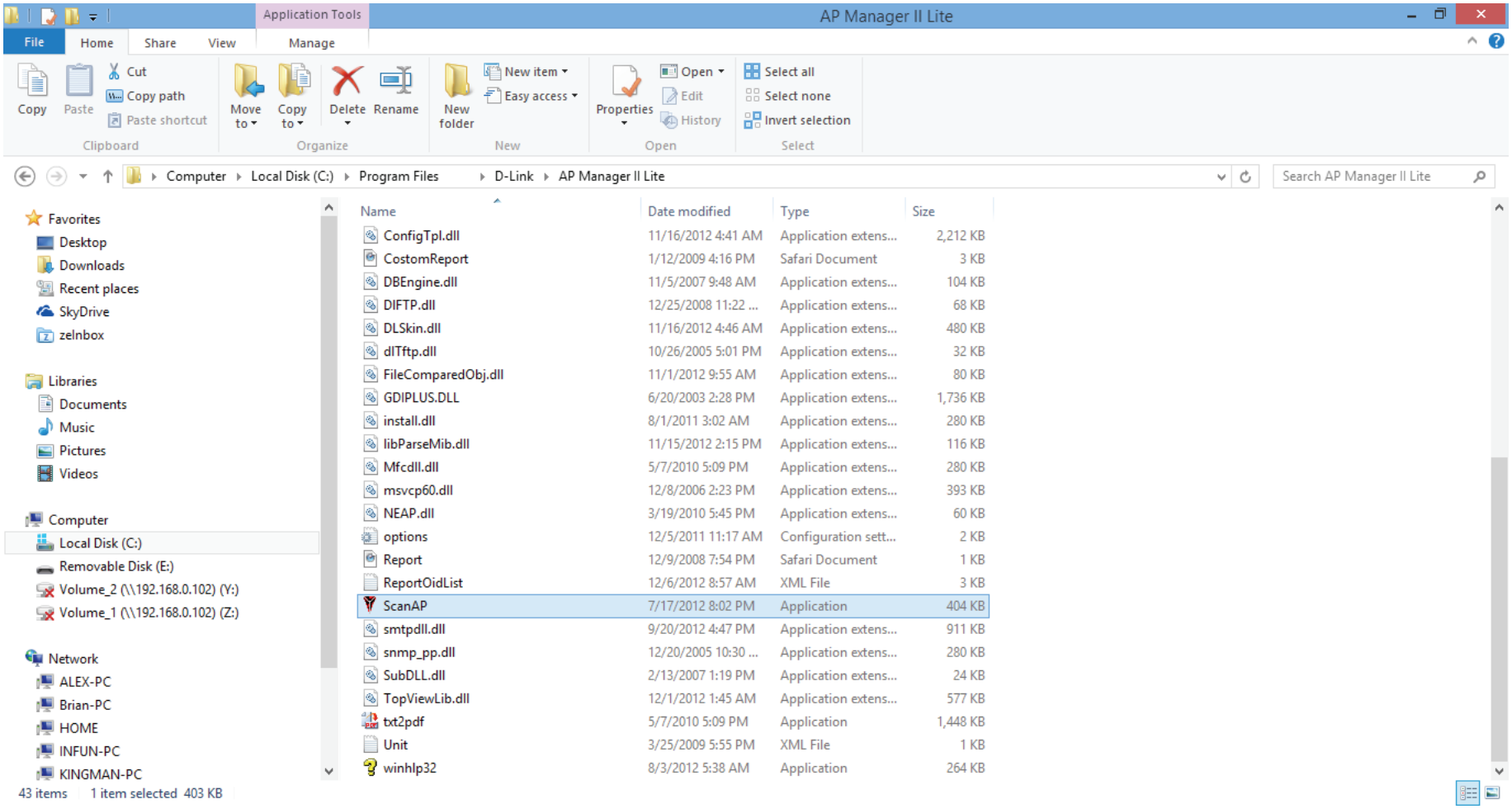
AP Manager II v3.0- Tools - Site Planning

Site Planning is designed to help a user layout the wireless network. Before establishing a wireless network, a user needs to plan and evaluate the wireless network . A user locates Access Points using his/her notebook to scan for Access Points. Once the Access Points are located, it can be imported into the AP Manager II for analysis.

The Site Planning Interface shows the Location ID (BSSID), the Start Time (Band), the Interval Time (average RSSI), the Length (Min RSSI), and a description (MaxRSSI).

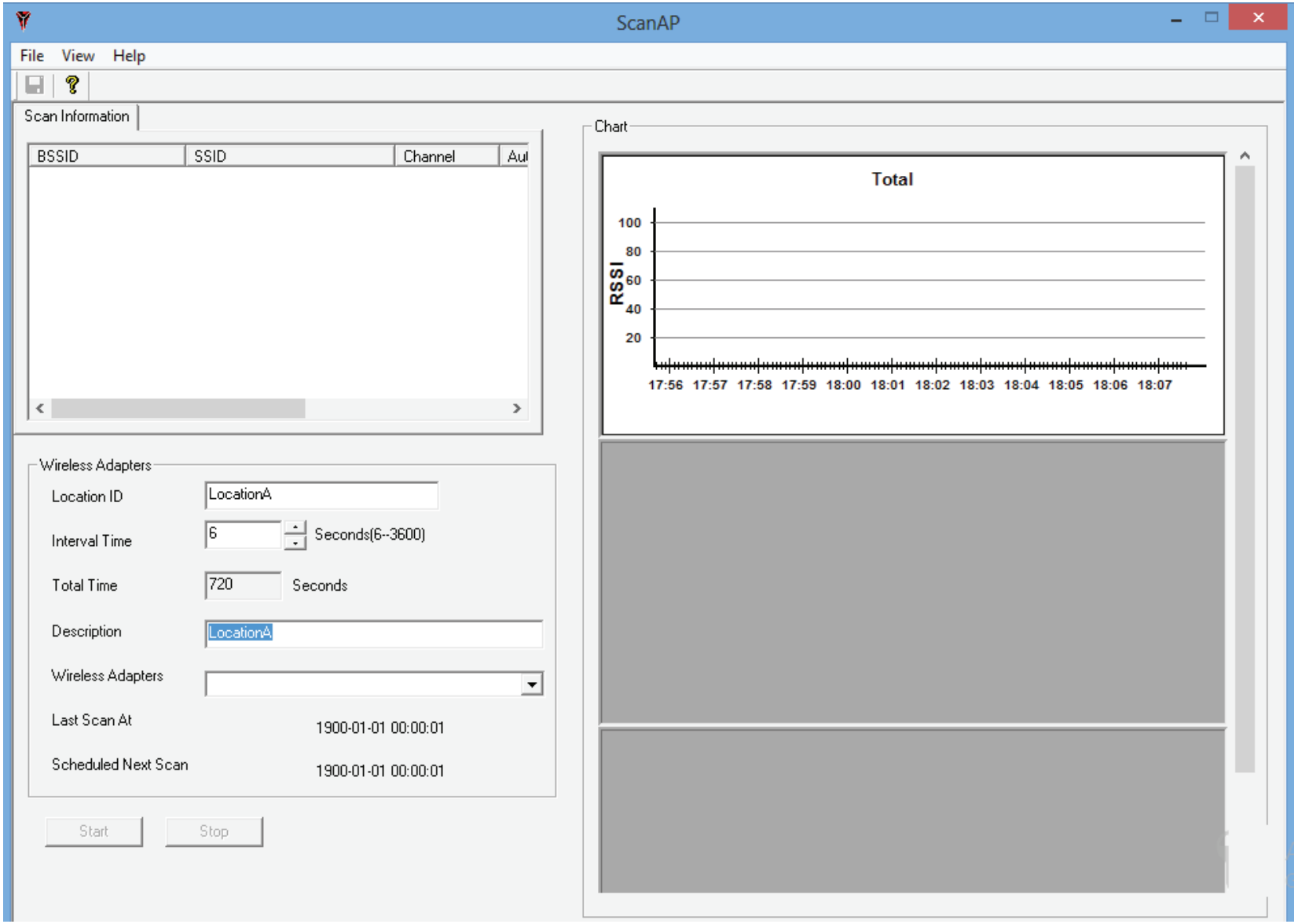


To run the scan, go to the directory where the AP Manager II is located. Double-click the **ScanAP.exe**. file.

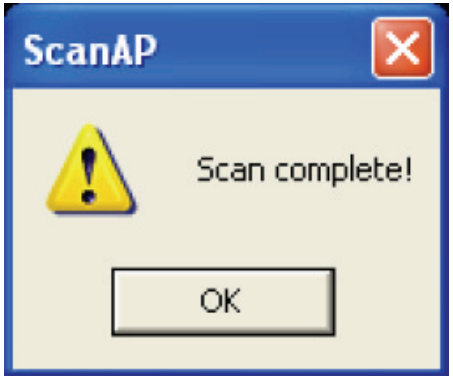


To collect the **Access Points RF information**, click **ScanAP**.

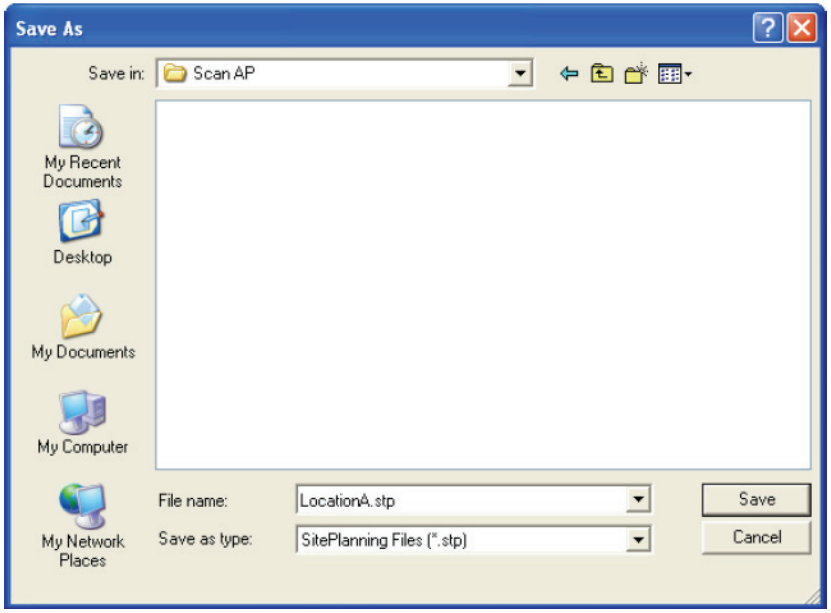
Select the target Access Point. Enter the Location ID, Description, and select the interval Time and wireless adapter, and then click the Start button.



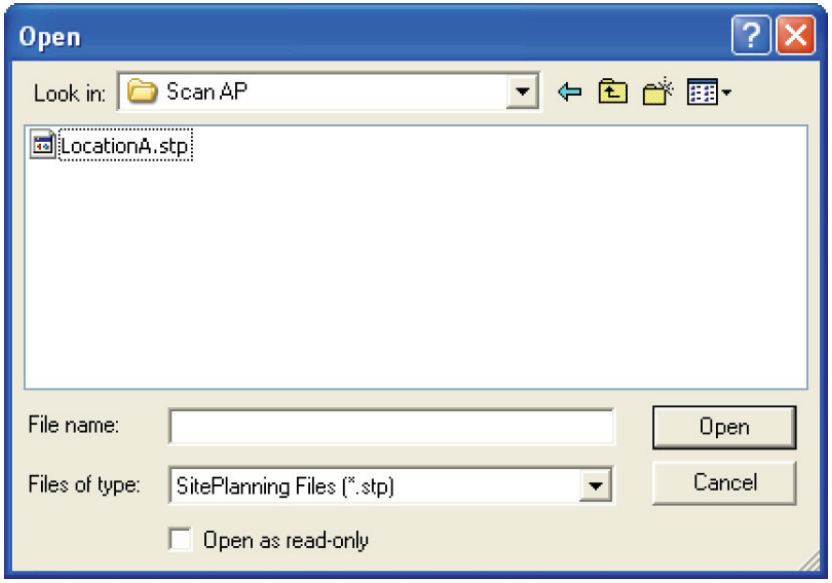
ScanAP starts to collect information on the Access Point. The Access Point is complete when a prompt message appears.



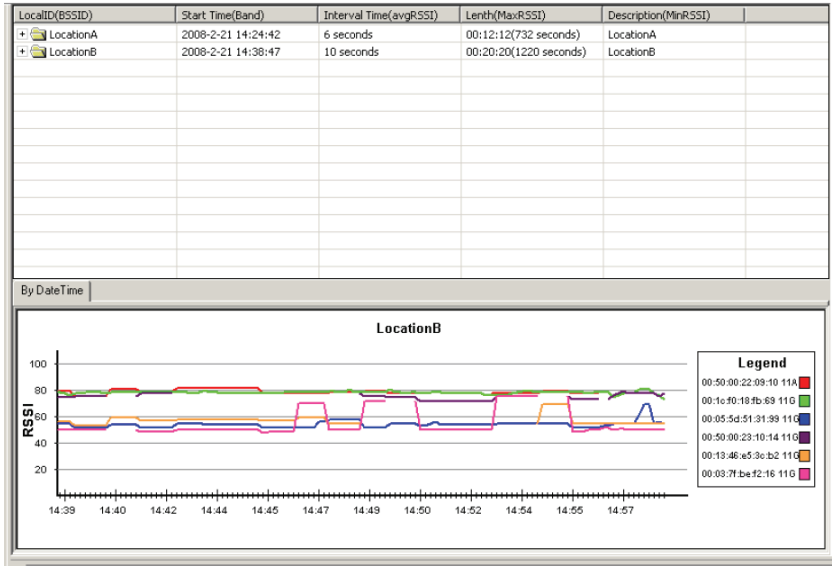
You can also save the location information. When you are prompted to click the Save button.



To load the Location Information, click the Load button from the Site Planning window and click Open.

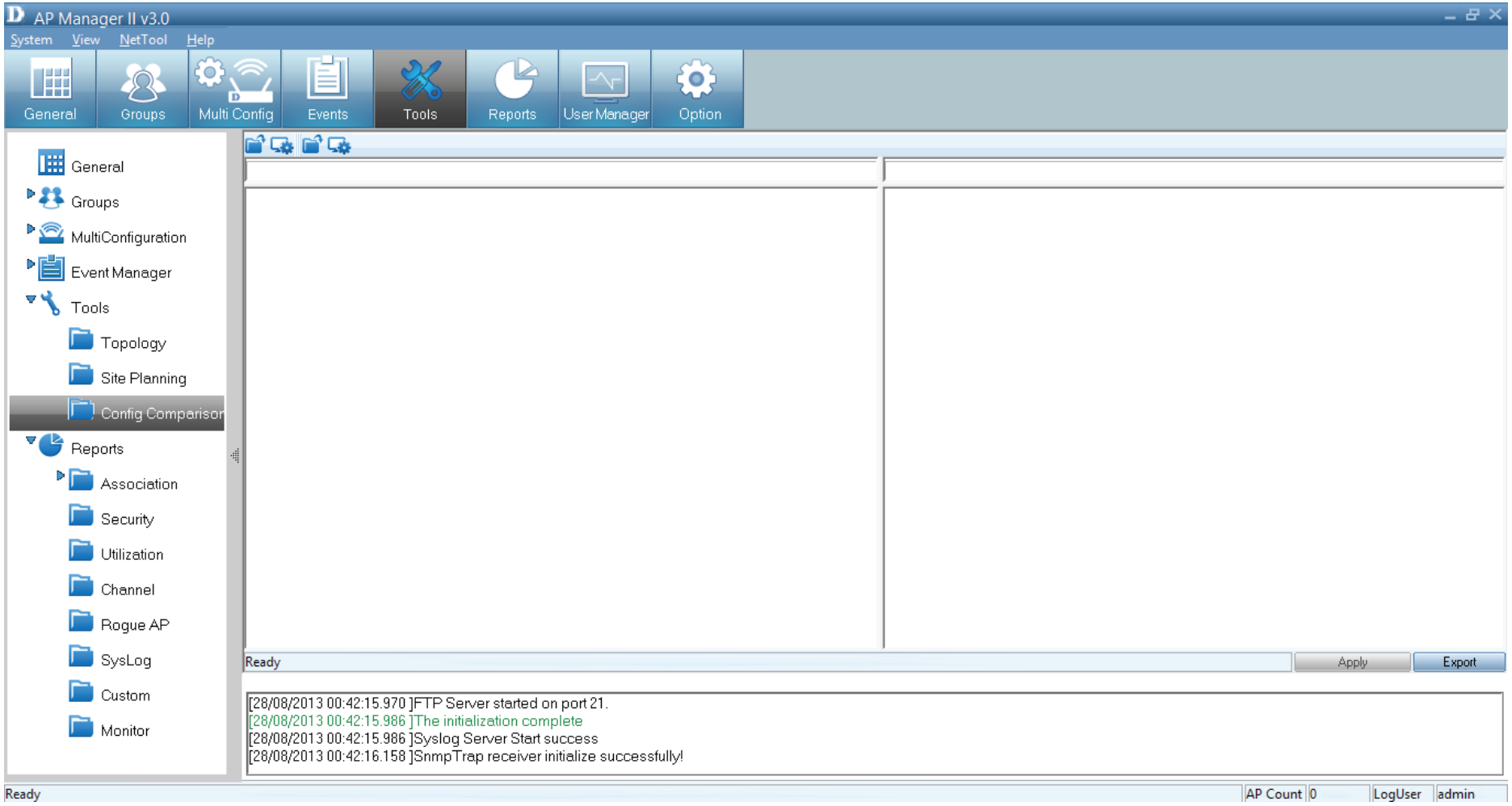


Select the file from the list or expand the file to see the details on each location.

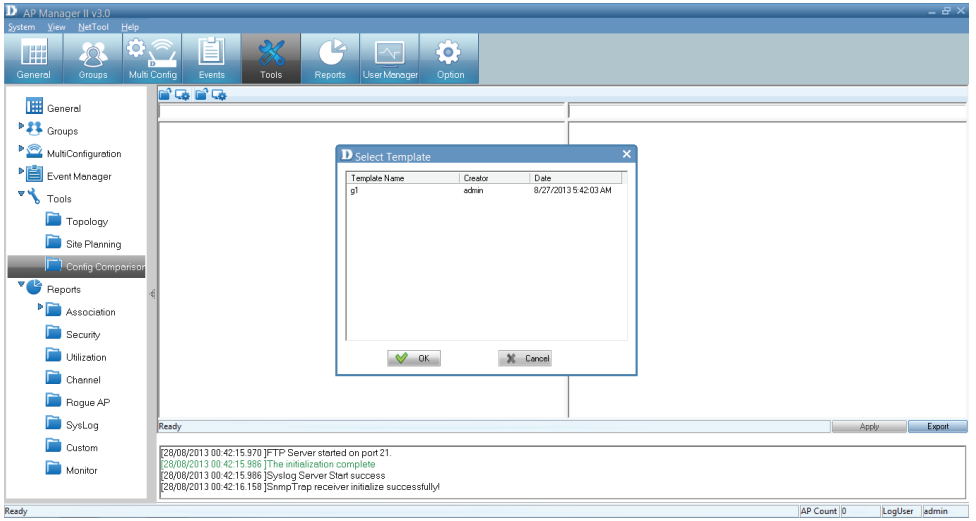


AP Manager II v3.0 - Tools - Config Comparison

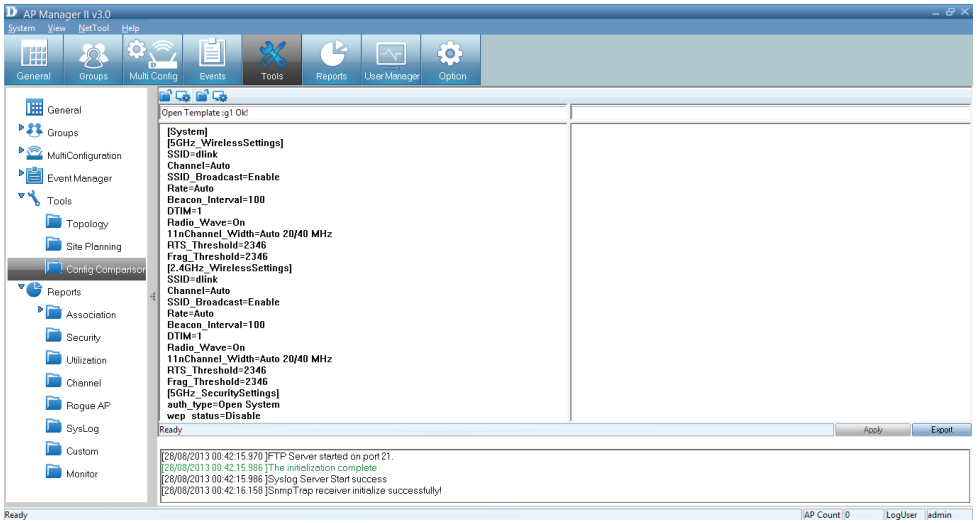
The Config Comparison tool dispays windows side-by-side. It provides all system data on the Access Point to view and collate.



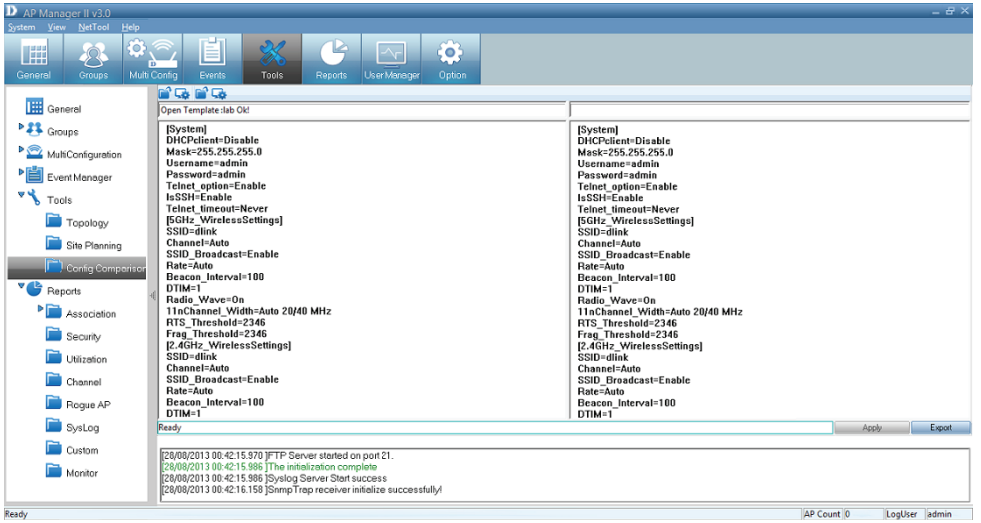
Select the File icon to open the Template. Click the Template you want to compare and click OK.



The Template is displayed in the left pane. The second option is to click this icon It downloads the file to the comparison table.

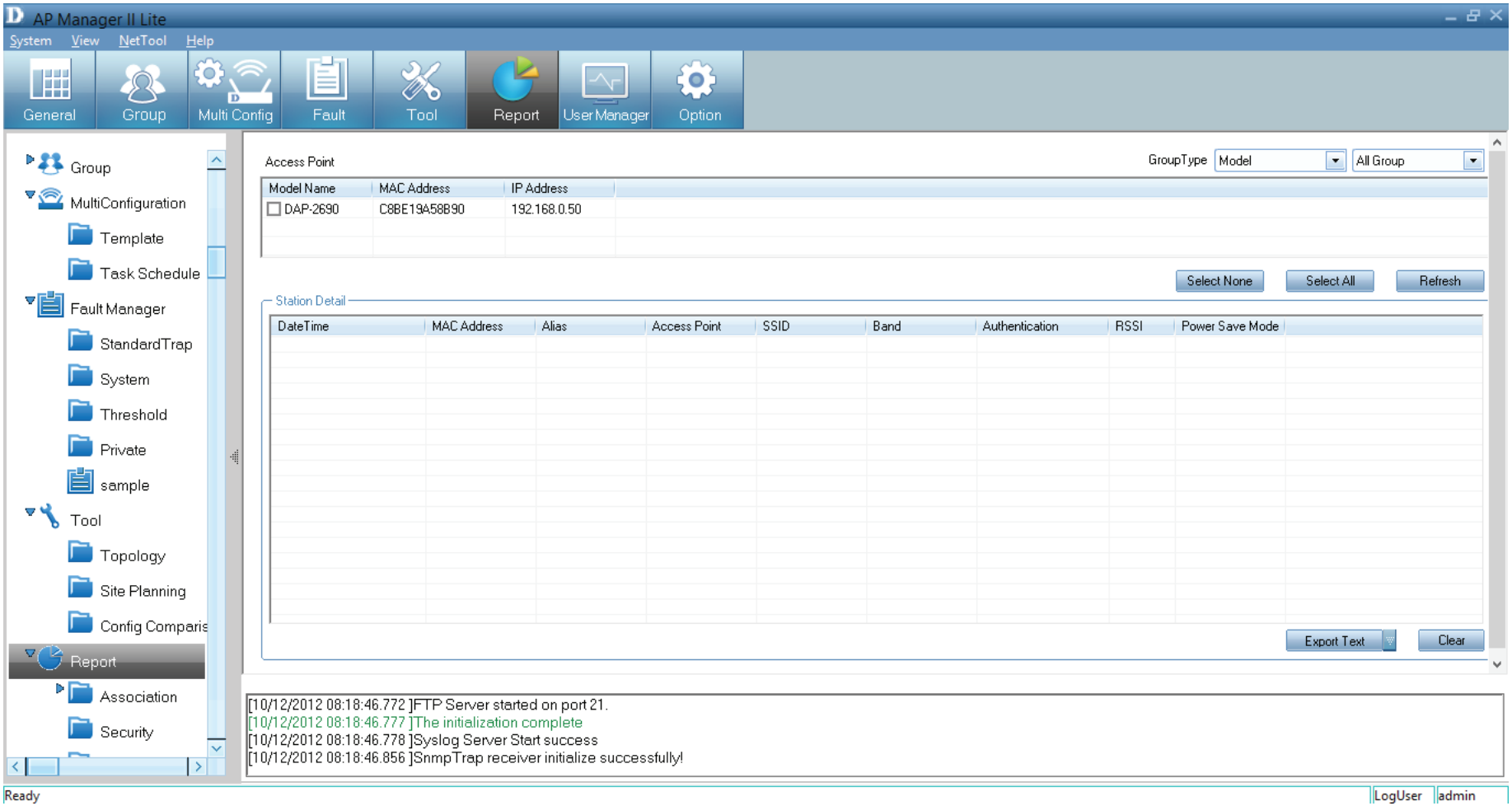


Once you have downloaded both profiles, they are displayed side-by-side for analysis.



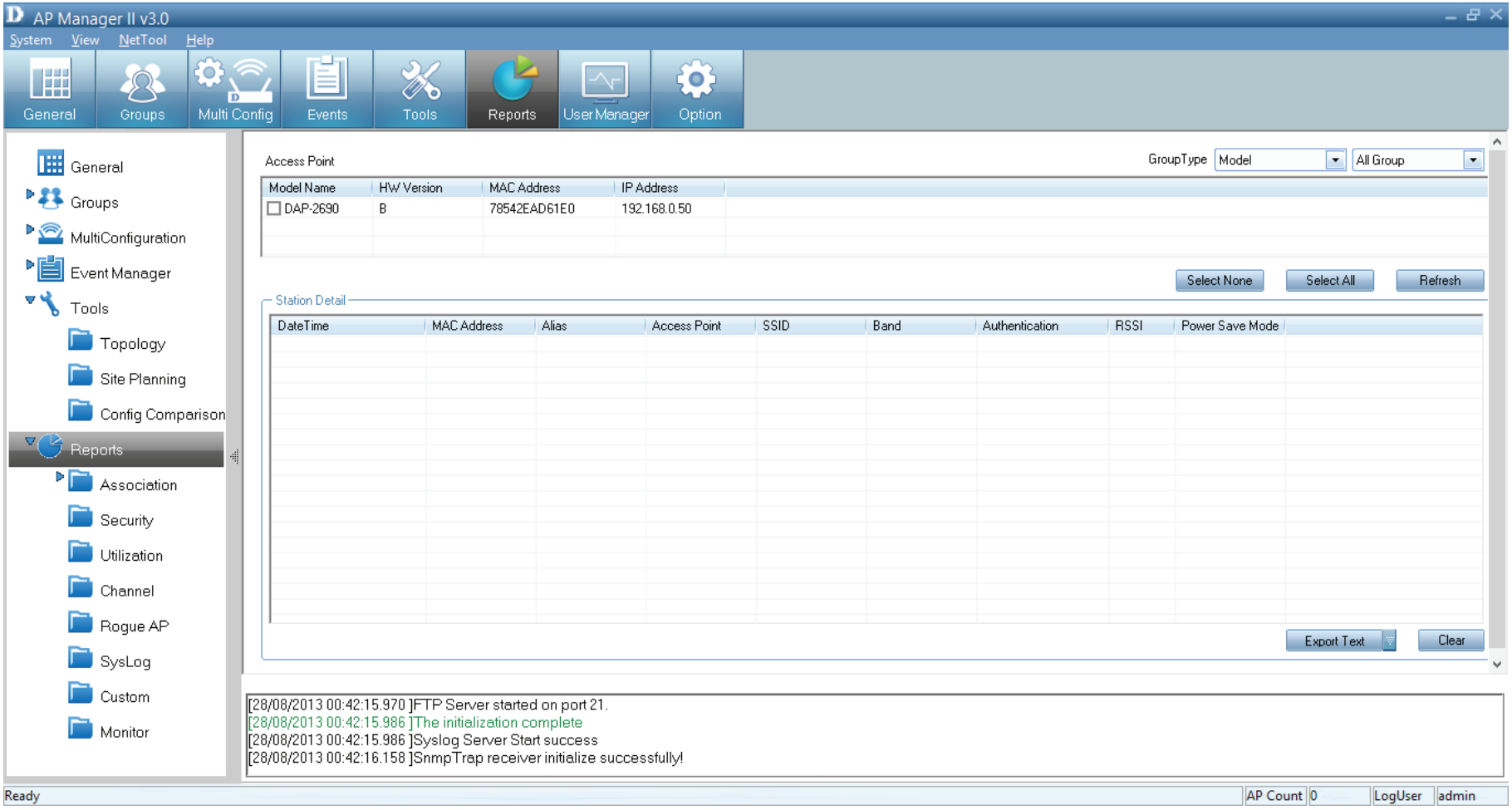
AP Manager II v3.0 - Report

Report is segmented into different categories. Each category is assigned a funtion to summarize details on its particular area. The Reports are: based on Association, Security, Utlization, Channel, Rogue AP, Syslog, Custom and Monitor.



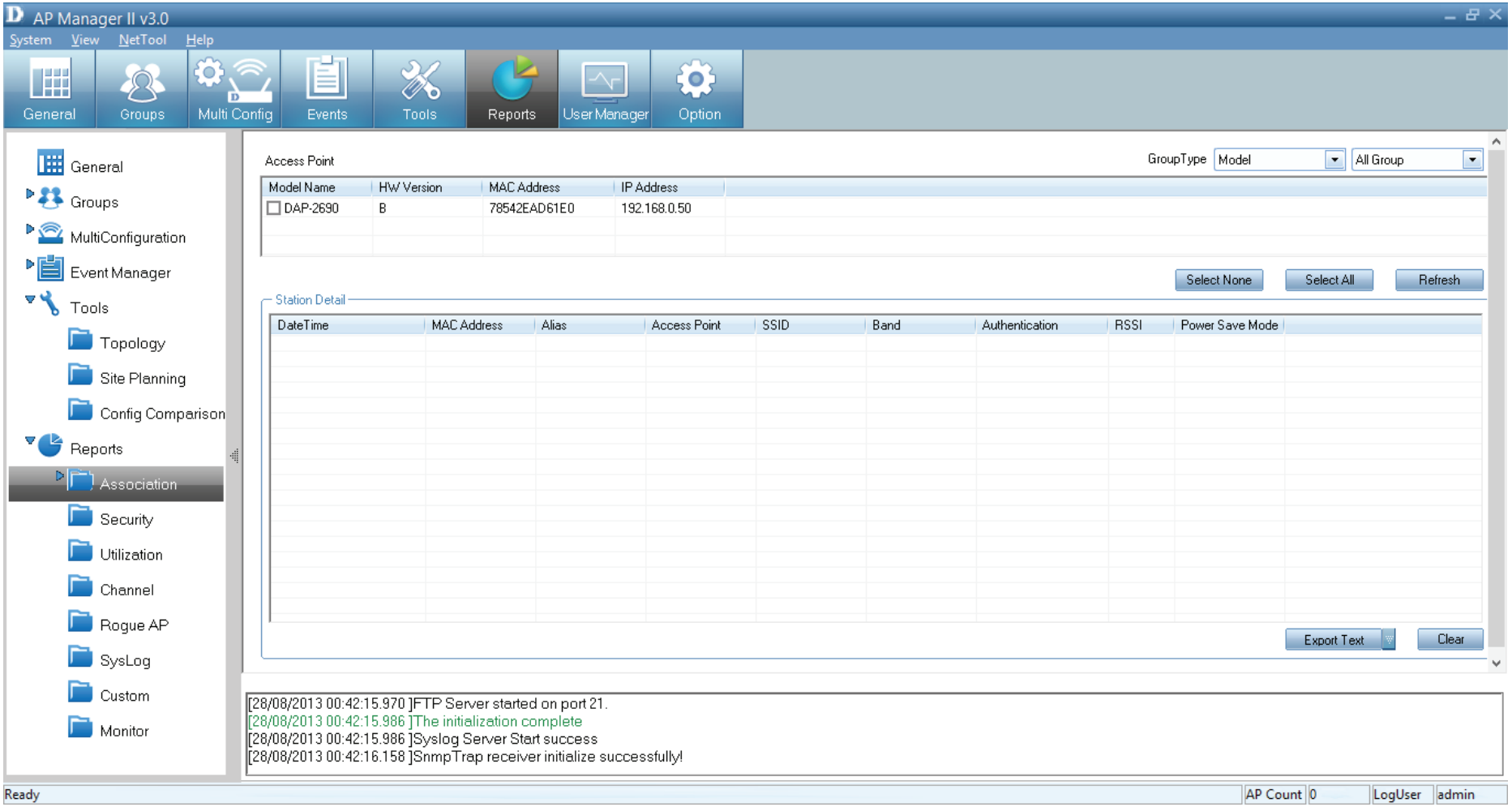
AP Manager II v3.0 - Report - Association

The association window shows managed Access Points and their associated client stations in two ways – By Access Point and By Wireless Station.



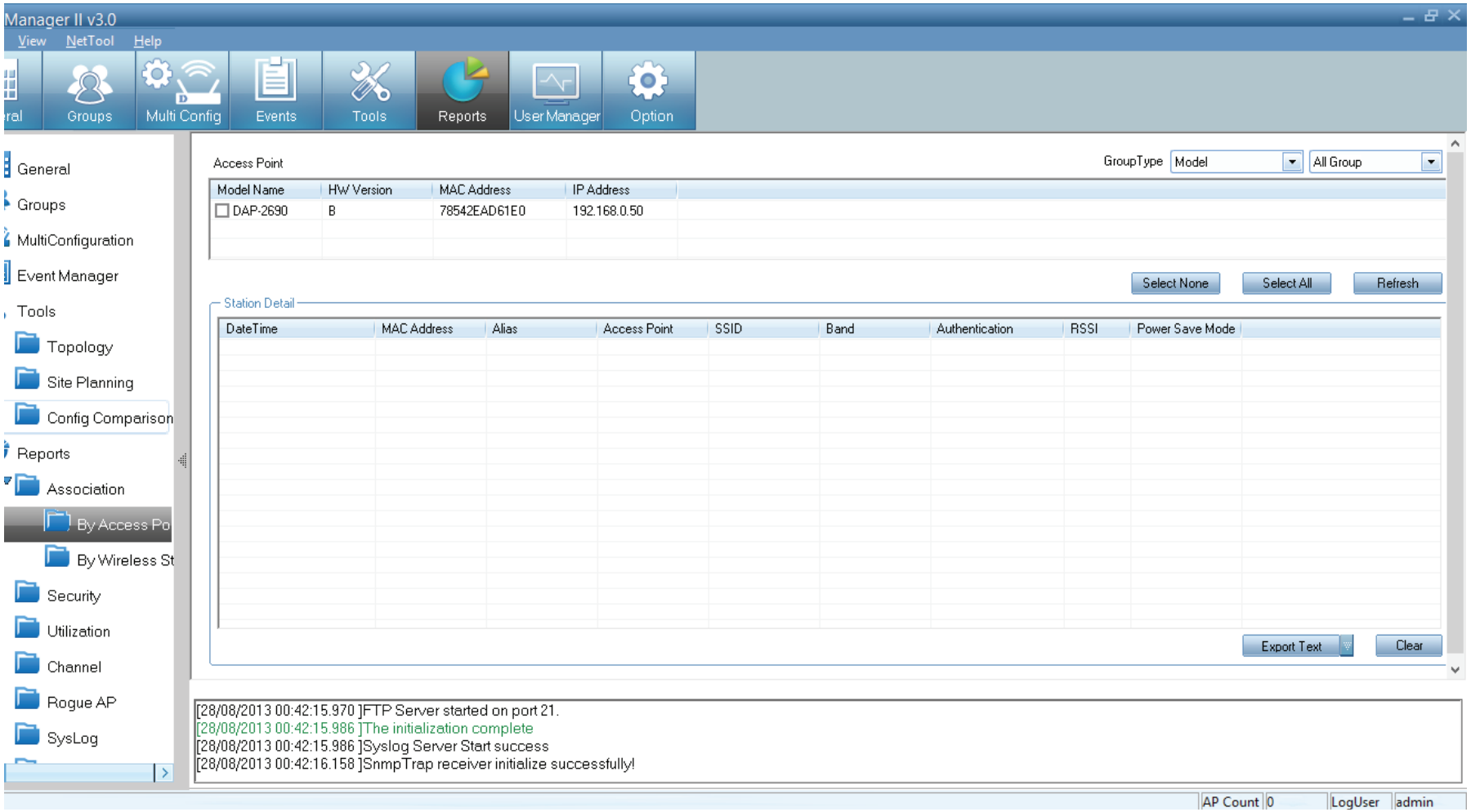
By Access Point - Highlight an Access Point and the details of client stations that associated with the AP list are shown. The detail information includes, Date/Time, MAC Address, Alias, Access Point, SSID, Band, Authentication, RSSI and Power save mode.

From the Group Type, you can specify the summary to show the data according to a specified model or group. To export the Access Point data to a file, click a file type from the Export Text drop-down menu or click the Export Text button, and then enter a file name in the Export window, click the Save button to save the Access Point data.



By Wireless Station - To list the Access Points according to the specified station and detected date, choose the date range from From/To drop-down menu, or type the Mac address of the device.

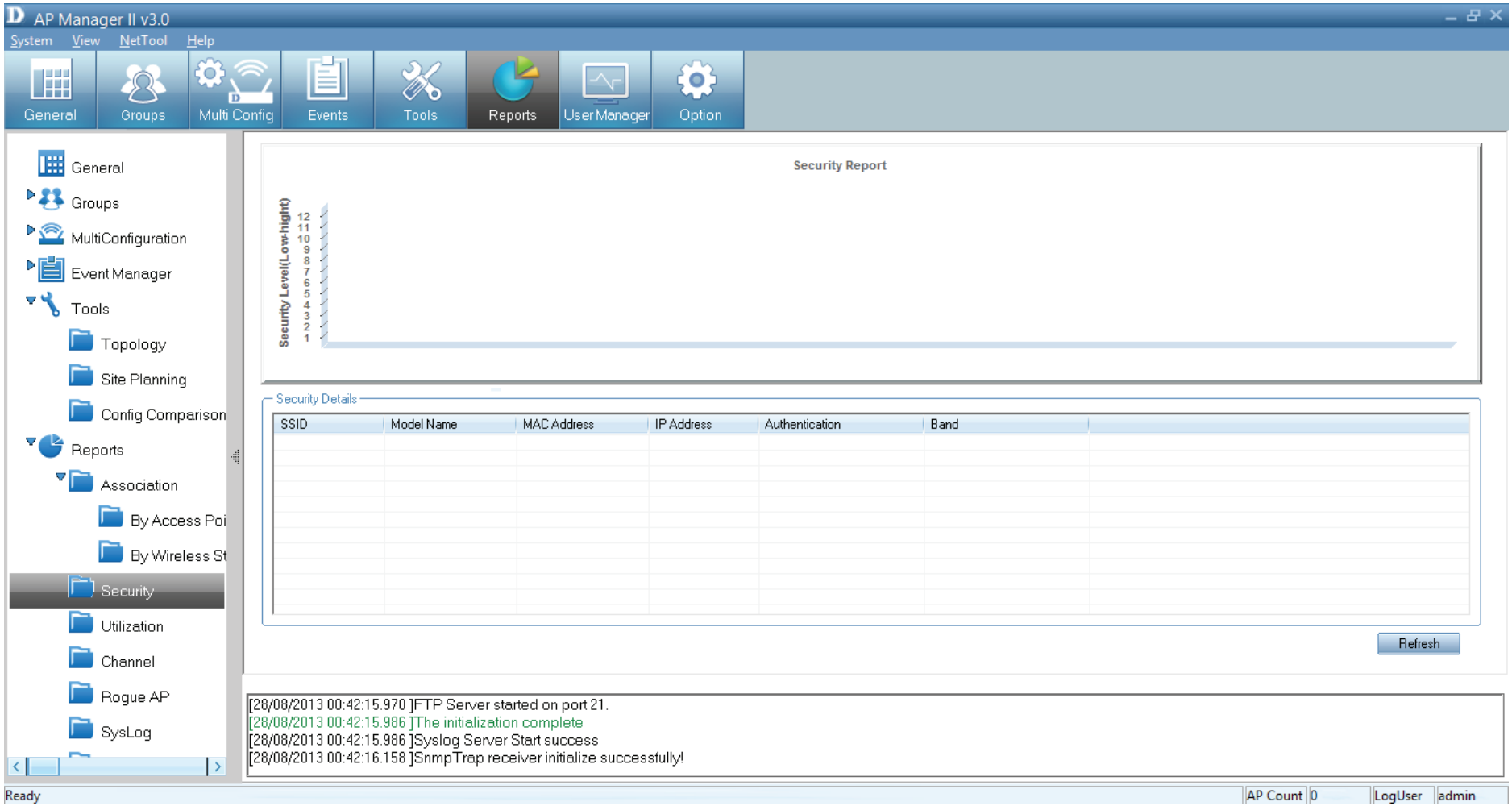
Export the Access Point data to a file, click a file type from the Export Text drop-down menu or click the Export Text button, and then enter a file name in the Export window, click the Save button to save the Access Point data.



AP Manager II v3.0 - Report - Security

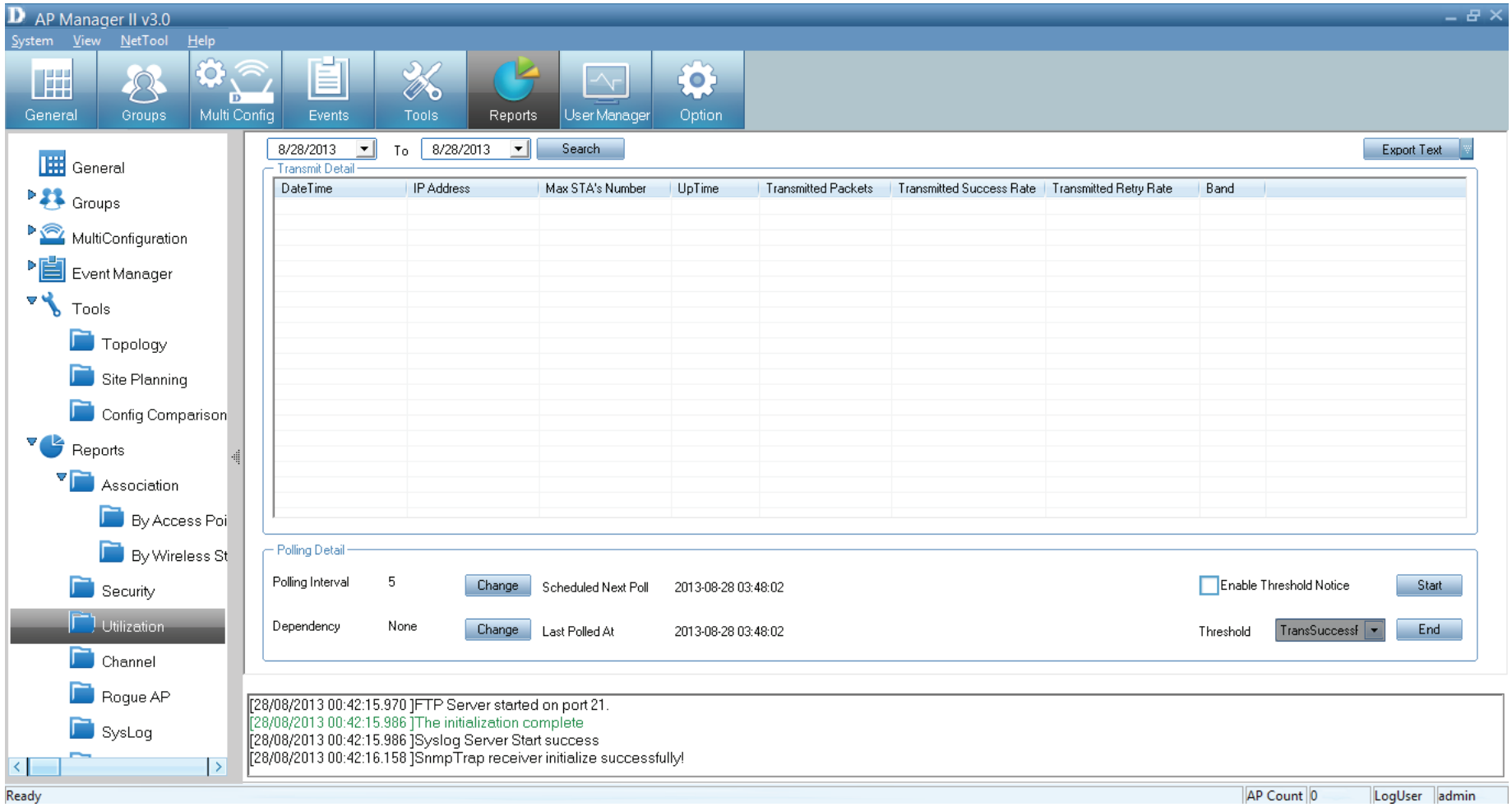
The Security pane graphically lists the security level of the managed Access Point(s) from lowest to highest - Open System, Shared Key, WPA-Personal, WPA-Enterprise, WPA2-Personal, and WPA2-Enterprise.

The Security Details pane shows the **SSID**, **Mode Name, MAC Address, IP Address, Authentication, and Band** information of the Access Points.



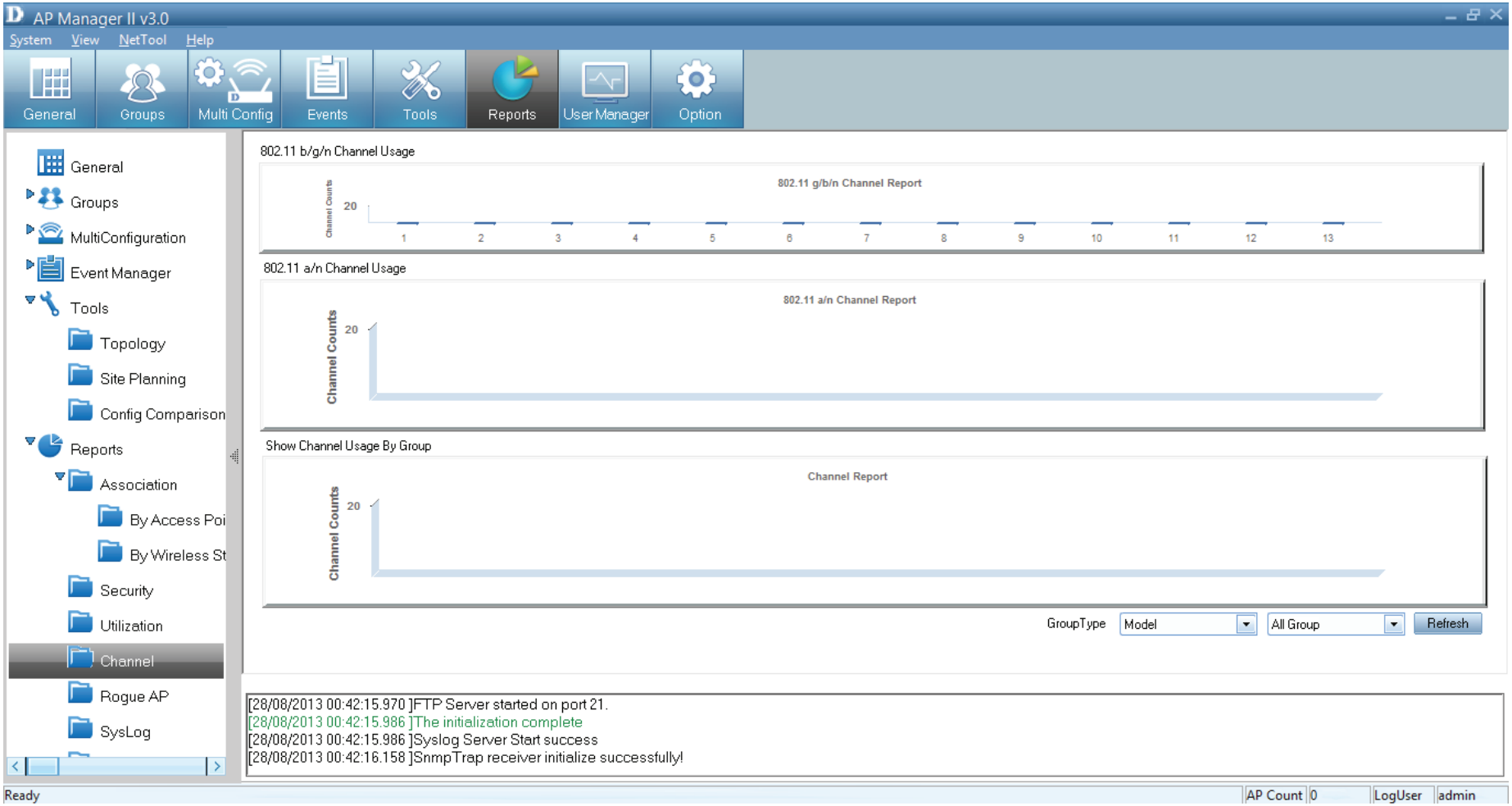
AP Manager II v3.0 - Report - Utilization

The **Utilization window** shows the band usage of a specific Access Point. To show the usage, the AP Manager II should poll the Access Points. To start the polling, select the Access Points that AP Manager II will poll from the Select window by clicking the Change button of Dependency and then click Start button. You can also enable the threshold notice by clicking the Enable Threshold Notice and select the type of Threshold Column.



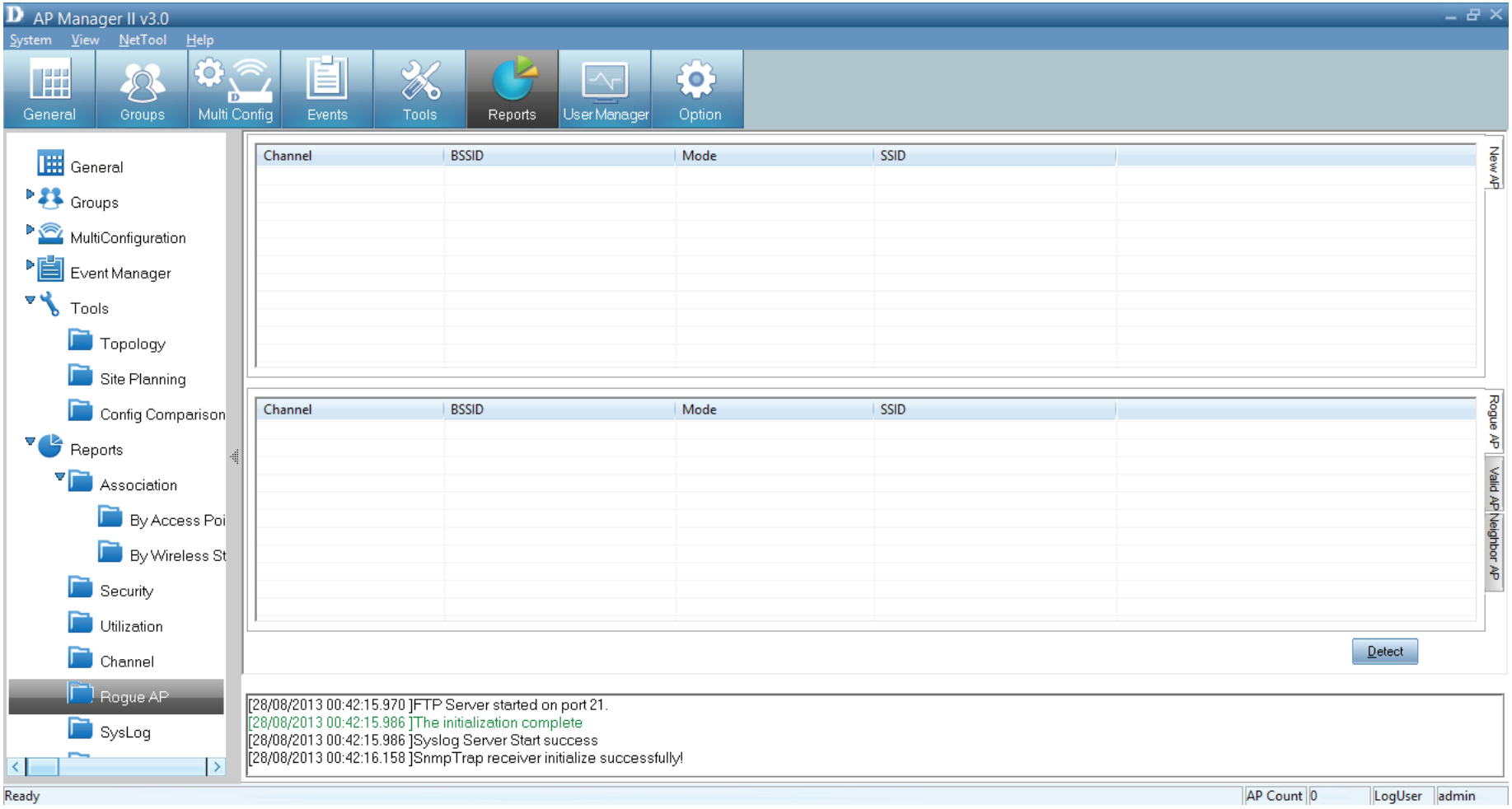
AP Manager II v3.0 - Report - Channel

The channel window graphically lists the channel usage of the managed Access Points. From the Group Type, specify the graph data according to a specific model or group.



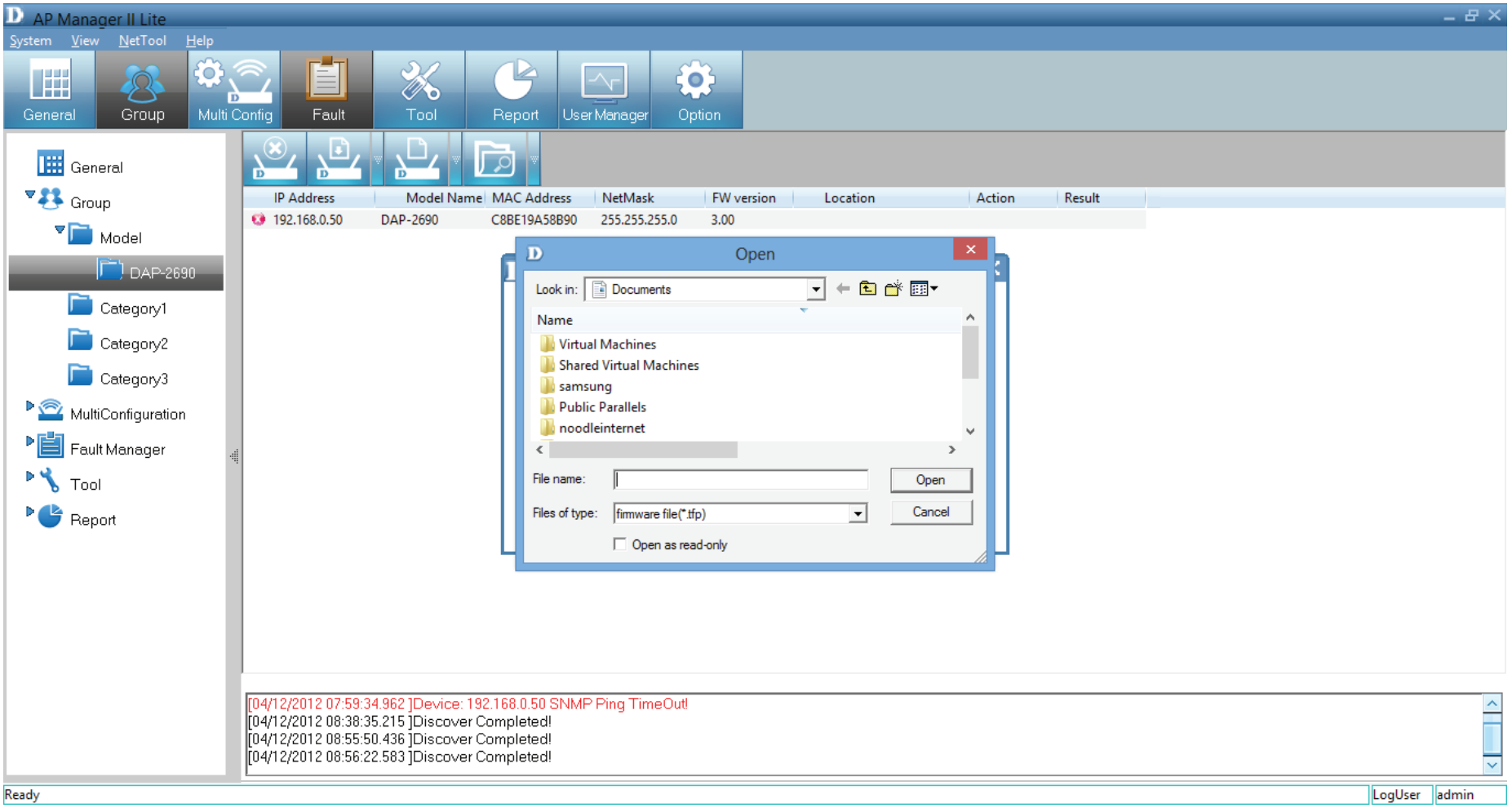
AP Manager II v3.0- Report -Rogue AP

The Rogue AP pane shows the Access Points that are not a part of same subnet. Rogue Access Points are showed by Channel, BSSID, Mode, and SSID. To categorize the APs, click the Detect button to scan the APs around, and click the category at the right side of window, then drag the AP from top window to bottom window



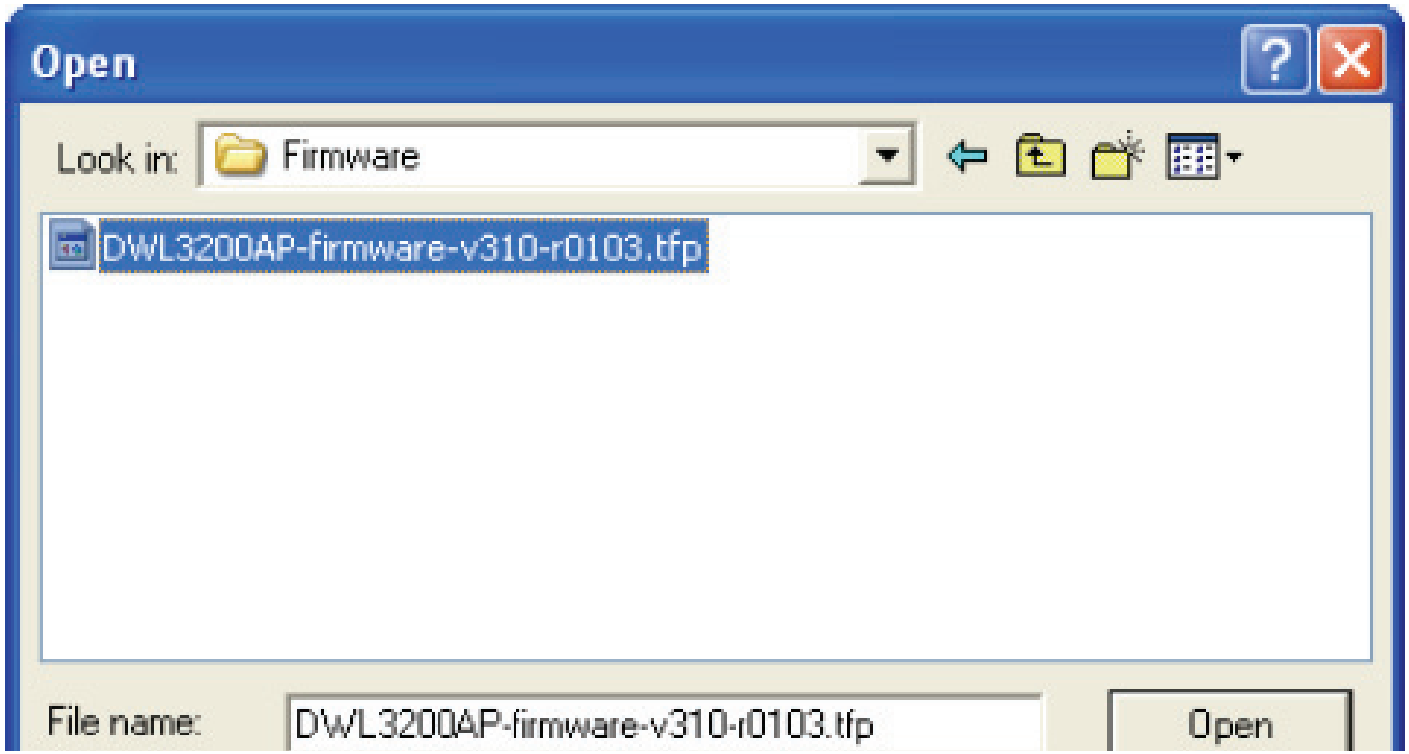
AP Manager II v3.0 - Report -Syslog

The Syslog window shows the System log information of the managed Access Point.



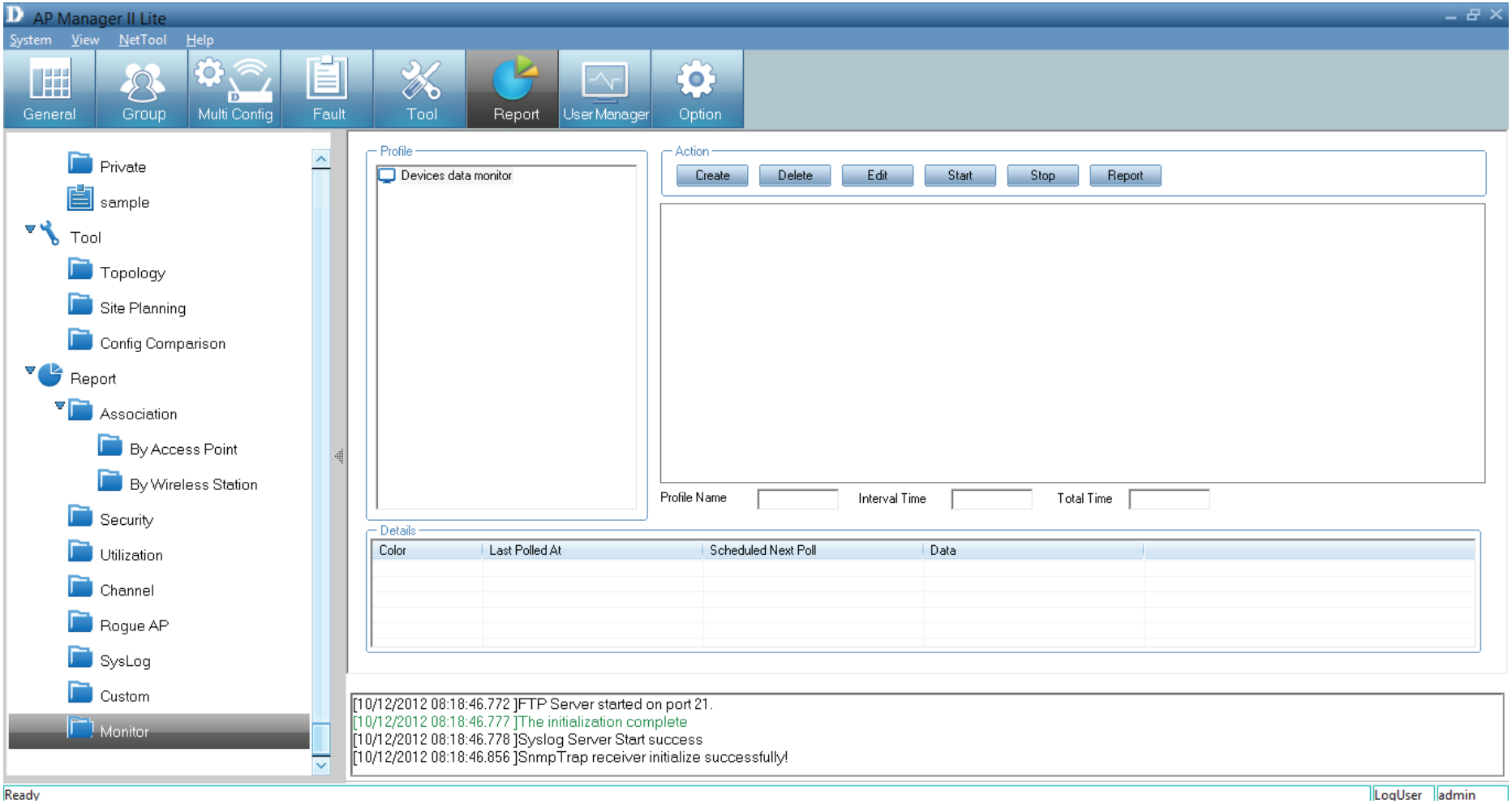
AP Manager II v3.0 - Report -Custom

The Custom log report allows you to configure the read-out from a specific date to a designated date. Click the Search button once you have finalized your time fram. Alternatively, create a custom configuration according to the Group Type (Model or Category) and Group.

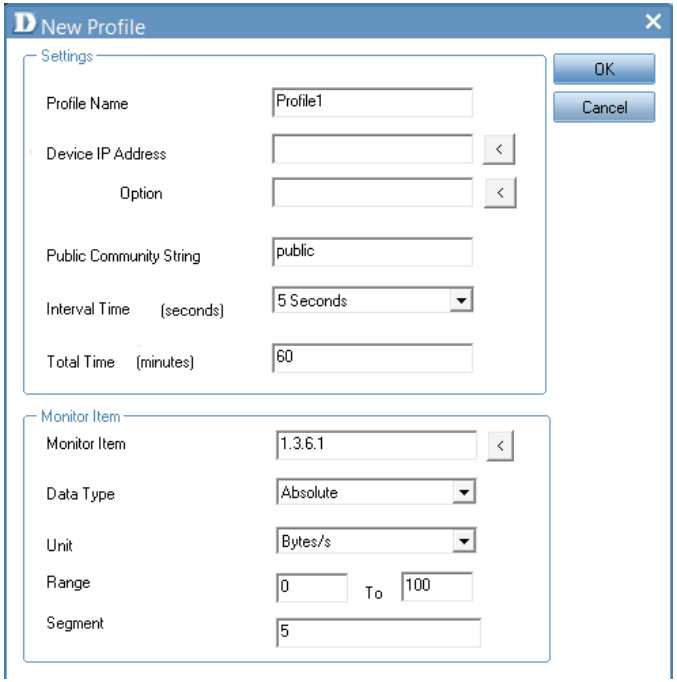


AP Manager II v3.0 - Report -Monitor

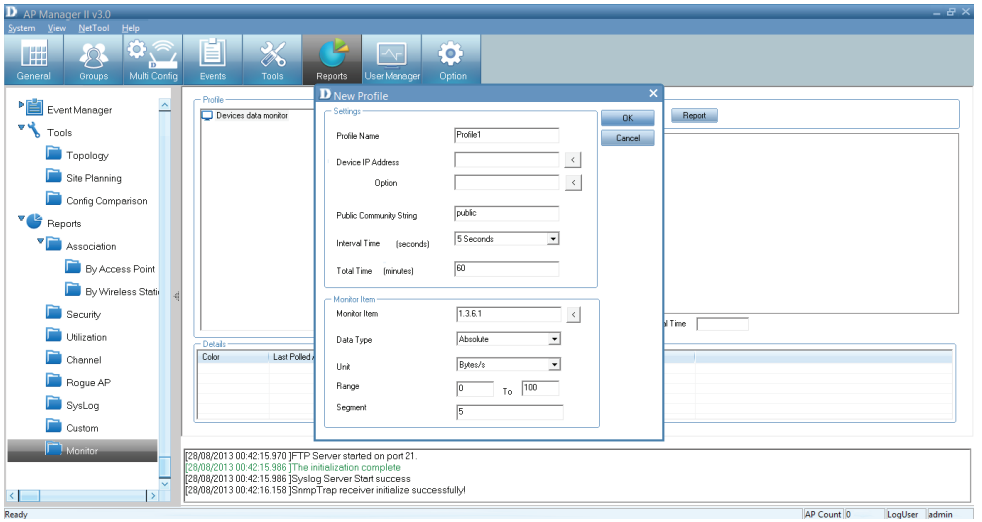
The Monitor window shows the performance of an Access Point you create from scratch.



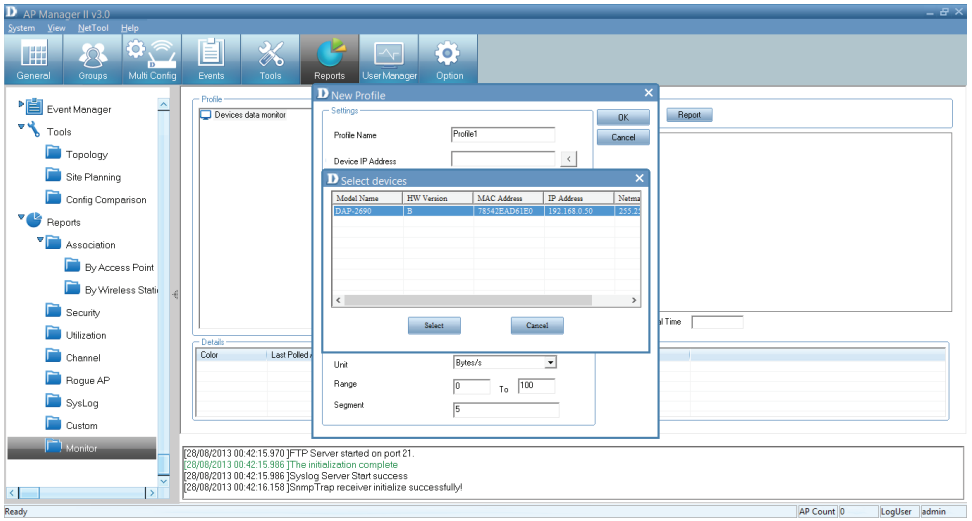
Create a new Surveillance profile by clicking the **Create** button under **Action**.



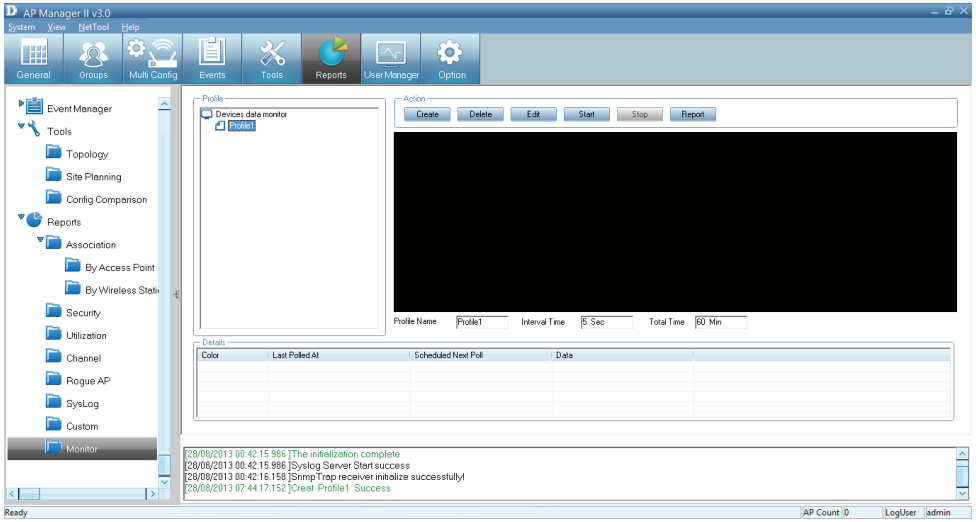
The Profile is automatically generated
The **Device IP Address** - click the arrow to access it
Option - click the arrow to access it.
Public Community String - automatically generated
Interval Time - select from the drop-down list
Total Time - enter a value in minutes



Once all the information is entered into the fields provided, click OK

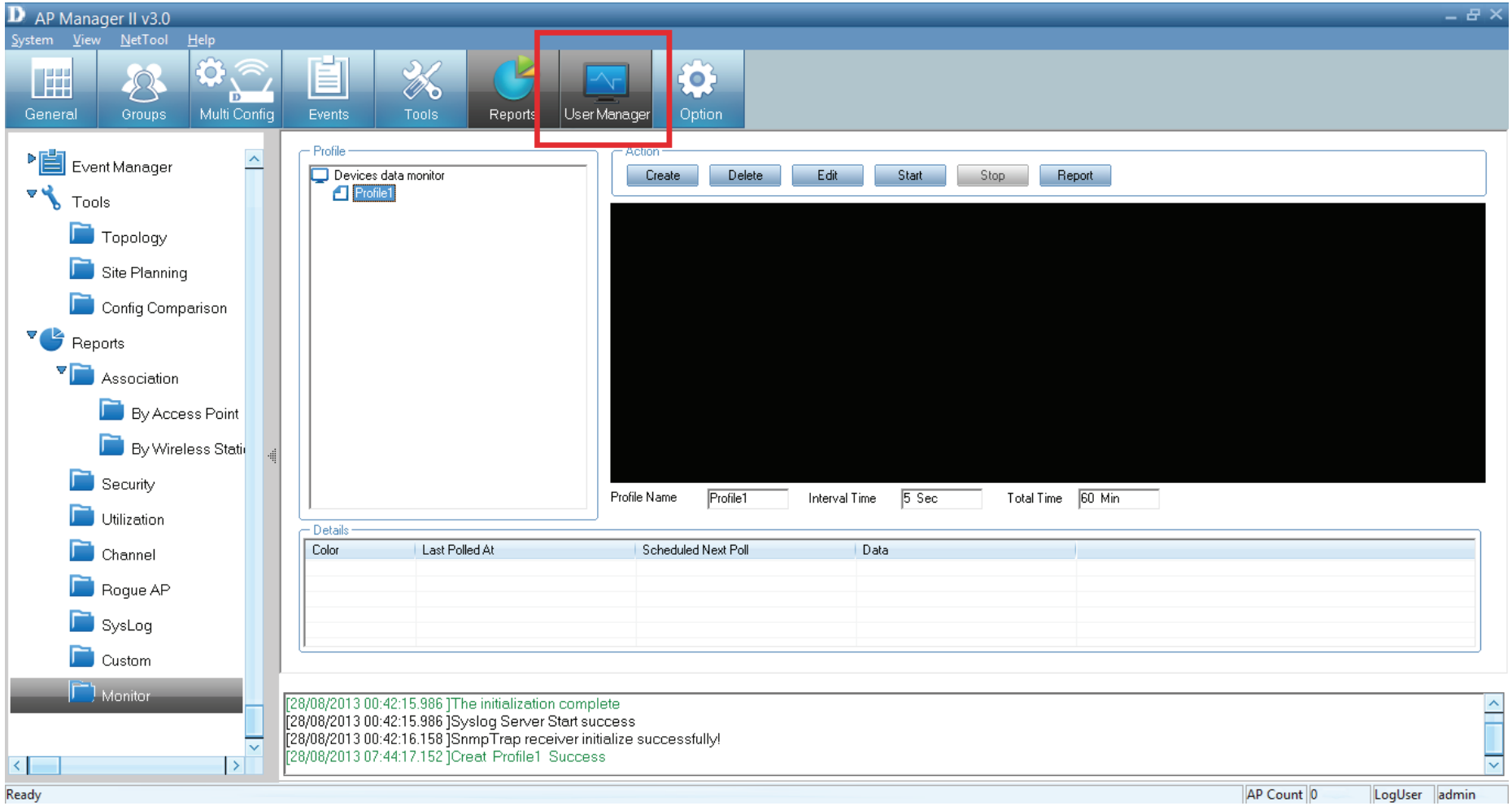


The Access Point monitors the profile you just created.

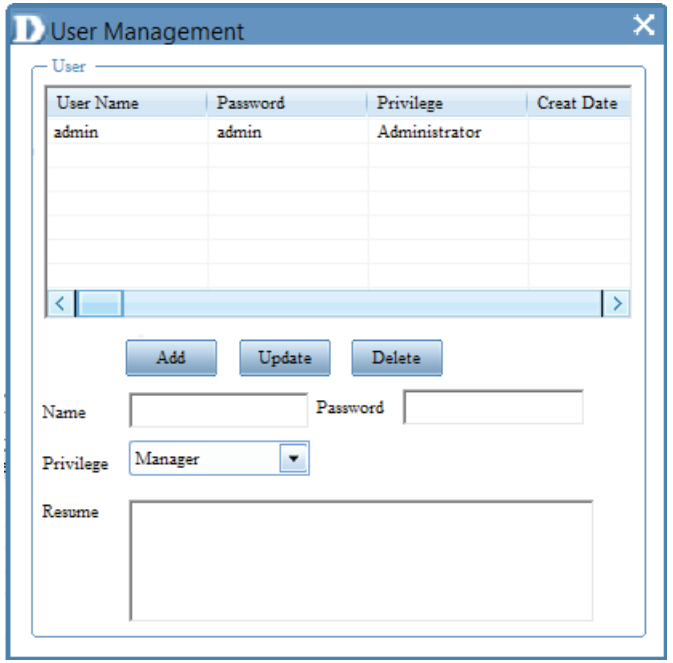


AP Manager II v3.0 - User Manager

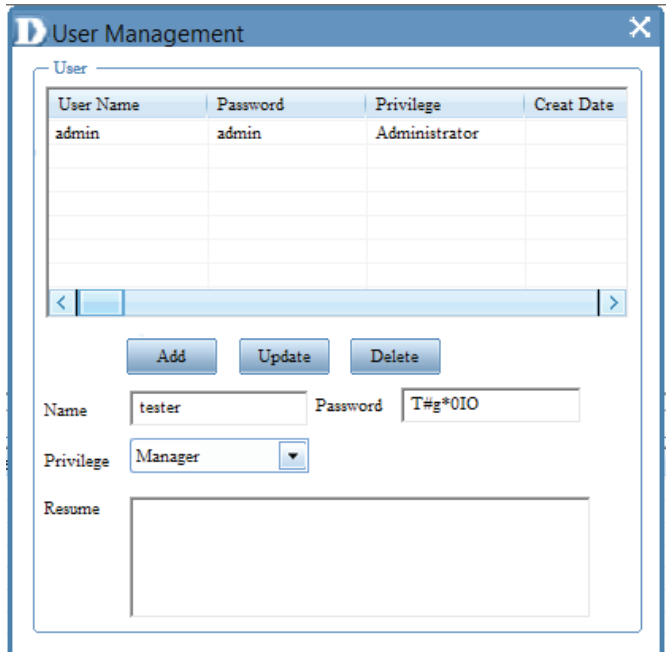
The AP Manager II allows you to manage user profiles. To manage users, click the User Manager icon at the top of the Toolbar.



This brings up the **User Management** pane. This shows the current user(s), **Privilege and Account Creation Date**.



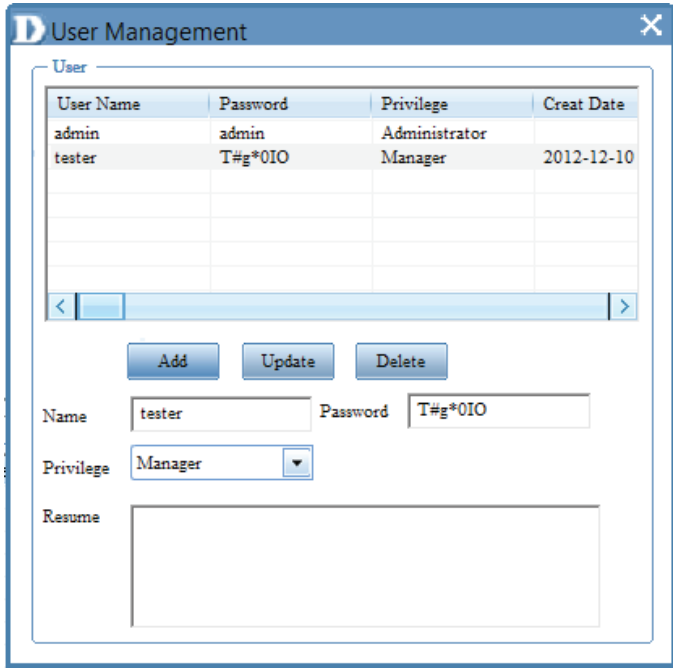
To create a new user, enter the details provided, **Name** and **Password,** and **Privilege** rights from the drop-down menu. Click the **Add** button.



Explanation of privilege levels:

- Administrator: Owns all the rights of the AP Manager II.
- Manager: Owns all the rights except user manager.
- Guest: Can only view the information.

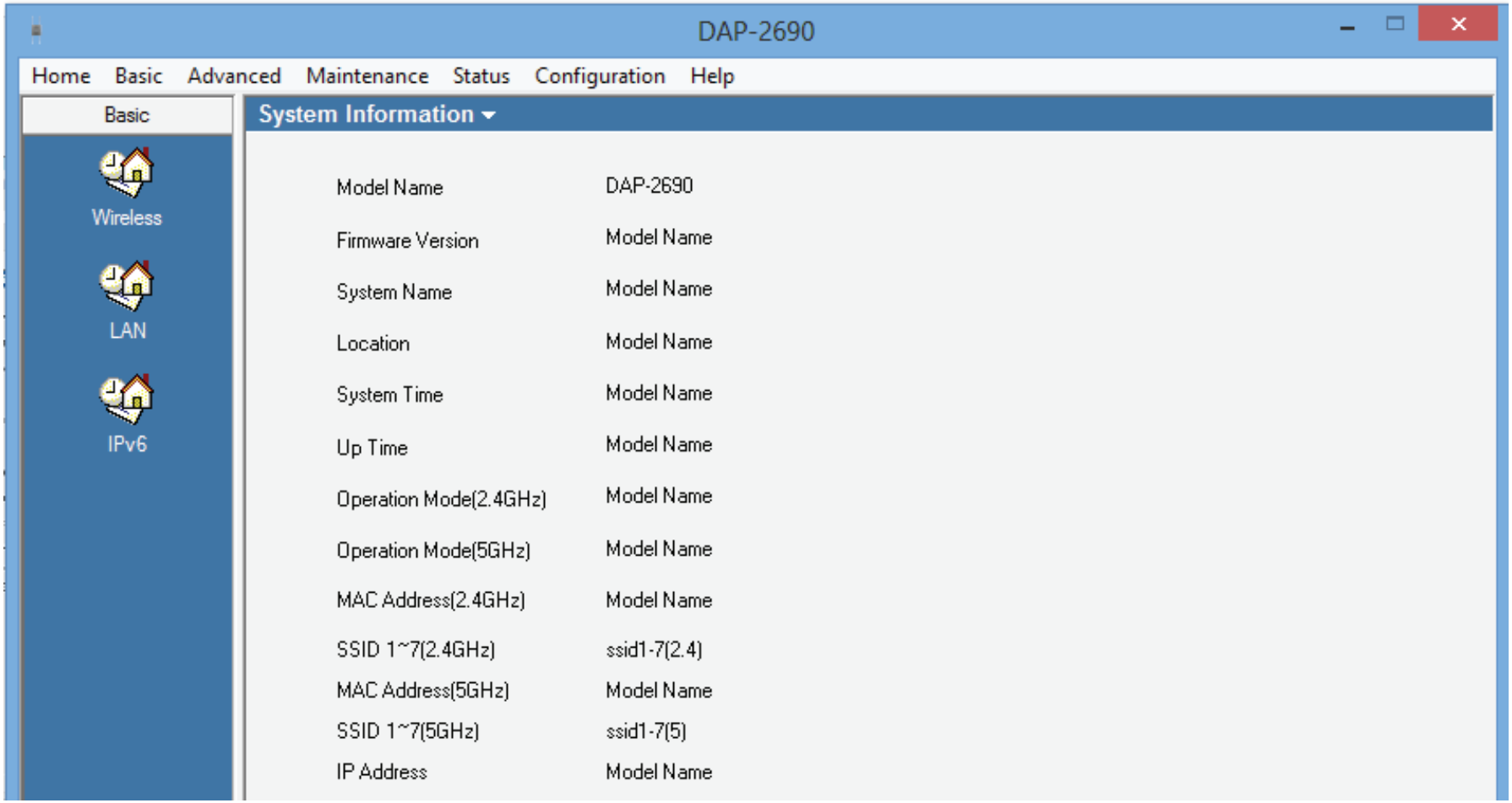
The new details now populates the **User Management** table.



To delete a user, click the **Delete** button.

AP Manager II v3.0 - Options

A user can change the software operation environment of the AP Manager II. To configure the system environment, click Options in the main Toolbar.



The **Options** configuration window has four tabs - **General, Module, Database Maintenance, and Advanced**. The **General** section consists of **Logon Settings, SNMP Settings, Polling Settings**, and **Discover**.

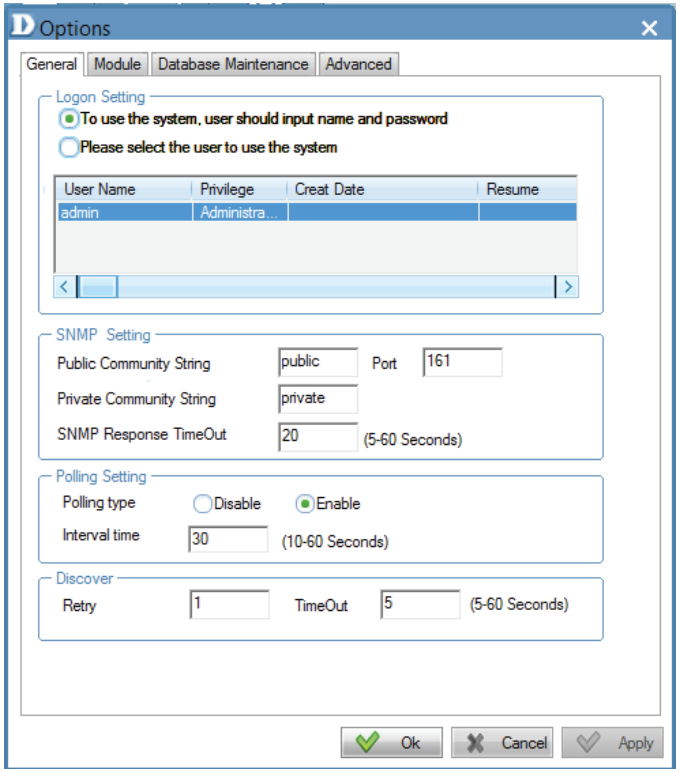
Logon Settings - Select whether a user enters a username and password or select a specific user to use the system.

SNMP Settings - Select the Public/Private Community String, the Port number, and the SNMP Response TimeOut

Polling Settings - Selec to enable or disable the Polling type and the interval period

Discover - Enter a value for the Discovery Retry and Timeout duration.

Click **Apply**, then **OK** when you are finished with the configuration. Click **Cancel** if you wish not to make any changes.



The Module is divided into two sections: **Select firmware file for model** and **Rogue AP**.

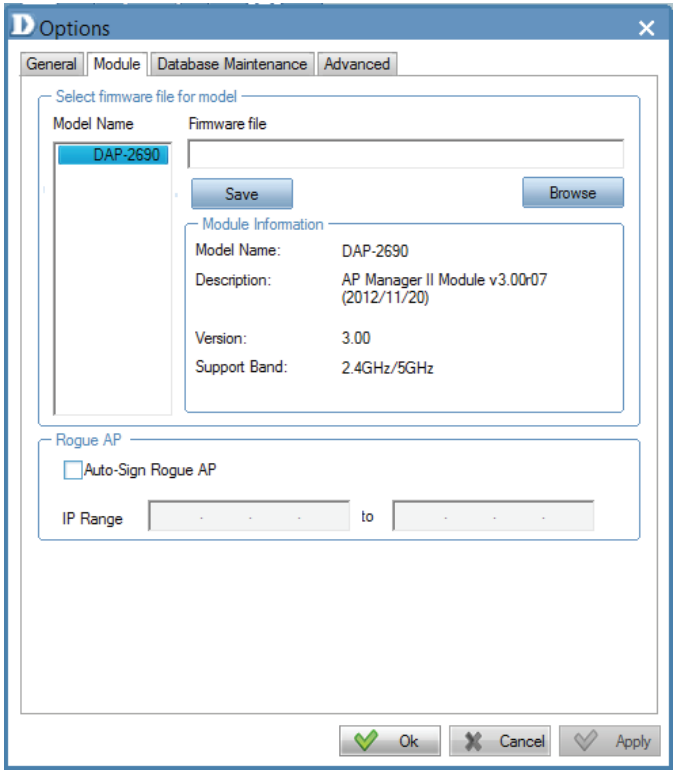
Model Name - Details automatically provided

Firmware File - Click the Browse button to find the new/ updated firmware. Click Save when complete.

Module Information - This displays the current information.

Rogue AP - This can be auto-signed. Click the checkbox next to Auto-Sign Rogue AP and enter an IP Range

Click **Apply**, then **OK** when you are finished with the configuration. Click **Cancel** if you wish not to make any changes.



The Database Maintenance allows users to configure the database according to their needs. Data is available for **Fault Data, Wireless Station Data, System Log Data, Utilization Data amd SysLog Data**

Data is further segmented into Notice by Records and **Clear Rule.**

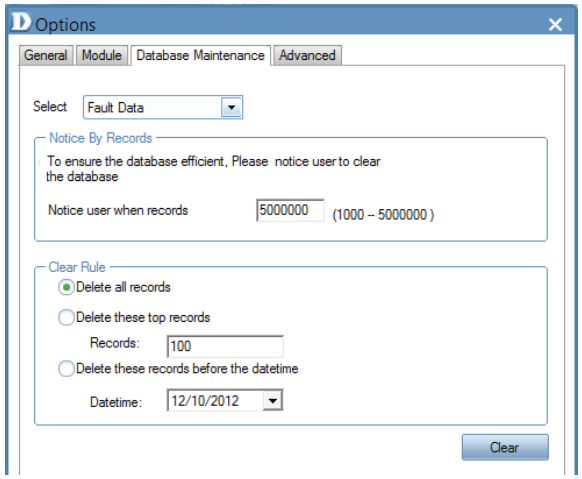
Under **Notice By Record,** enter a value in the field provided

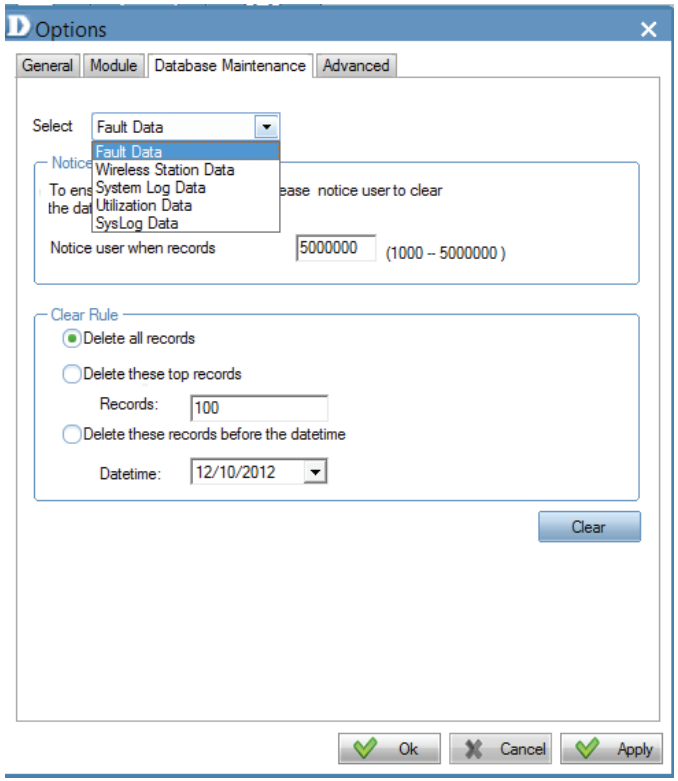
Under **Clear Rule**, there are three main options.:

Delete all records - self explanatory
Delete these top records - enter a value accordingly
Delete these records before the datetime - enter the calendar date

Click **Clear** if you wish to start over.

Click **Apply**, then **OK** when you are finished with the configuration. Click **Cancel** if you wish not to make any changes.





The Advanced tab is divided into two sections, TimeOut Settings and FTP Server settings

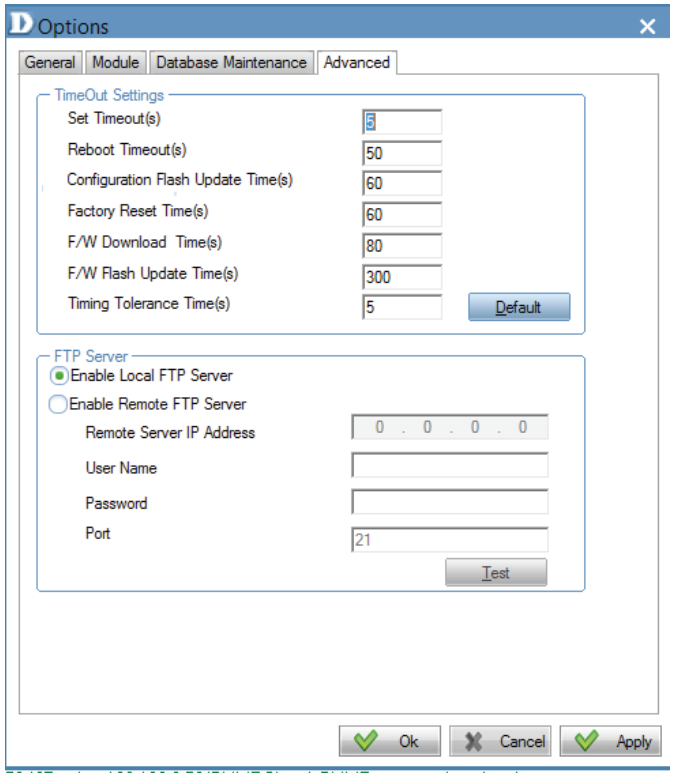
TimeOut Settings

Under **TimeOut Settings,** enter a value in the field provided for the folllowing settings:

Set Timeout
Reboot Timeout
Configuration Flash Update Time
F/W Download Time
F/W Flash Update Time
Time Tolerance Time

Under **FTP Server**, there are two main options.:

Enable Local FTP Server -
Enable Remote FTP Server - Enter Remote IP Address
Username
Password
Port

Click **Test** to see its functionality

Click **Apply**, then **OK** when you are finished with the configuration. Click **Cancel** if you wish not to make any changes.