



Wireless Controller User Manual

DWC-2000

Version 1.10



BUSINESS WIRELESS SOLUTION

Preface

D-Link reserves the right to revise this publication and to make changes in the content hereof without obligation to notify any person or organization of such revisions or changes. Information in this document may become obsolete as our services and websites develop and change.

Manual Revisions

| Revision | Date | Description |
|----------|--------------|--|
| 1.10 | May 27, 2016 | • DWC-2000 revision A1 initial release |

Trademarks

D-Link and the D-Link logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States or other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

© 2016 D-Link Corporation.

All rights reserved. This publication may not be reproduced, in whole or in part, without prior expressed written permission from D-Link Corporation.

Safety Instructions

Use the following safety guidelines to ensure your own personal safety and to help protect your system from potential damage.

Safety Cautions

To reduce the risk of bodily injury, electrical shock, fire, and damage to the equipment, observe the following precautions:

- Observe and follow service markings.
 - Do not service any product except as explained in your system documentation.
 - Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to electrical shock.
 - Only a trained service technician should service components inside these compartments.
- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:
 - The power cable, extension cable, or plug is damaged.
 - An object has fallen into the product.
 - The product has been exposed to water.
 - The product has been dropped or damaged.
 - The product does not operate correctly when you follow the operating instructions.
- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide or contact your trained service provider.
- Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- Allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.
- Also, be sure that attached devices are electrically rated to operate with the power available in your location.
- Use only approved power cable(s). If you have not been provided with a power cable for your system or for any AC powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.
- To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets.

-
- These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.
 - Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
 - To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
 - Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
 - Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications.
 - Always follow your local/national wiring rules.
 - When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:
 - Install the power supply before connecting the power cable to the power supply.
 - Unplug the power cable before removing the power supply.
 - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
 - Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.
 - This equipment is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

Protecting Against Electrostatic Discharge

Static electricity can harm delicate components inside your system. To prevent static damage, discharge static electricity from your body before you touch any of the electronic components, such as the microprocessor. You can do so by periodically touching an unpainted metal surface on the chassis.

You can also take the following steps to prevent damage from electrostatic discharge (ESD):

1. When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your system. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
2. When transporting a sensitive component, first place it in an antistatic container or package.
3. Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads, workbench pads and an antistatic grounding strap.

Table of Contents

| | |
|--|-----------|
| Preface | 2 |
| Manual Revisions | 2 |
| Trademarks | 2 |
| Safety Instructions | 3 |
| Safety Cautions | 3 |
| Protecting Against Electrostatic Discharge | 5 |
| Product Overview | 12 |
| Introduction | 12 |
| Features and Benefits | 13 |
| Package Contents | 14 |
| Required Tools and Information | 14 |
| Front Panel | 15 |
| Rear Panel | 15 |
| Installation | 16 |
| Unpacking | 16 |
| Selecting a Location | 16 |
| Rack Mount | 17 |
| Connecting the Wireless Controller | 18 |
| Basic Configuration | 19 |
| Log in to the Web Management Interface | 20 |
| Web Management Interface Layout | 22 |
| Standard Web Management Interface Features | 23 |
| Basic Configuration Procedures | 24 |
| Step #1: Enable DHCP Server (Optional) | 25 |
| Step #2: Configure Country Code | 26 |
| Step #3: Select APs to be Managed | 27 |
| Step #4: Change the SSID and Set Up Security | 29 |
| Step #5: Select MAC Authentication Mode | 34 |
| Step #6: Confirm Access Point Profile is Associated | 36 |
| Step #7: Configure Captive Portal Settings | 37 |
| Step #8: Use SSID with RADIUS Sever as Authenticator | 45 |
| Step #9: Configure Guest Management | 46 |
| Step #10: Configure a BYOD Environment | 53 |
| Where to Go from Here | 59 |
| Advanced WLAN Configuration | 60 |
| WLAN General Settings | 61 |
| Channel Plan and Power Settings | 64 |

| | |
|---|------------|
| Configure Channel Plan | 64 |
| Configure Power Settings | 66 |
| WIDS..... | 67 |
| Configure AP WIDS Settings..... | 67 |
| Configure Client WIDS Settings | 70 |
| Distributed Tunnel | 72 |
| Configure Distributed Tunnel | 72 |
| WLAN Visualization..... | 73 |
| Upload Images | 73 |
| Deleting Images | 73 |
| Launch | 74 |
| AP Discovery Methods | 75 |
| L2/ VLAN Discovery | 75 |
| Configure L2/ VLAN Discovery..... | 76 |
| L3/ IP Discovery | 77 |
| Configure L3/ IP Discovery | 77 |
| Managed APs | 78 |
| Add a Valid AP | 78 |
| Add a AP from Discovered AP List | 80 |
| Manual Change Channel and Power of Managed AP | 81 |
| Configure AP Debug Mode | 82 |
| Configure AP Provisioning..... | 83 |
| AP Profiles | 85 |
| Configure AP Profile | 85 |
| Configure AP Profile Radio | 87 |
| Configure AP Profile SSID..... | 93 |
| Configure AP Profile QoS..... | 94 |
| SSID Profiles..... | 98 |
| Configure SSID Profiles | 98 |
| Wireless Distribution System (WDS)..... | 102 |
| Configure WDS Managed AP Group | 104 |
| Configure WDS Managed AP | 105 |
| Configure WDS AP Link..... | 107 |
| Peer Group..... | 108 |
| Configure Peer Group..... | 108 |
| Synchronize Peer Group..... | 109 |
| AP Firmware Download | 110 |
| Advanced Network Configuration | 114 |
| IP Mode | 115 |
| LAN Configuration | 116 |
| IPv4 LAN Settings..... | 116 |
| IPv6 LAN Settings..... | 118 |

| | |
|---|------------|
| IPv6 Address Pools..... | 120 |
| IPv6 Router Advertisement | 122 |
| IPv6 Advertisement Prefixes | 124 |
| LAN DHCP Reserved IPs | 126 |
| Configure IGMP Setup..... | 127 |
| Configure Jumbo Frames..... | 128 |
| Link Aggregation..... | 129 |
| VLANs | 130 |
| Creating VLANs | 130 |
| Editing VLANs..... | 132 |
| Deleting VLANs..... | 132 |
| MultiVLAN Subnets..... | 133 |
| Port VLANs..... | 135 |
| MAC Based VLANs | 136 |
| Voice VLANs..... | 138 |
| Protocol Based VLANs..... | 139 |
| Double VLANs..... | 140 |
| GVRP | 141 |
| Routing | 142 |
| Configure IPv4 Static Routing..... | 142 |
| Configure IPv6 Static Routing..... | 144 |
| Editing/Deleting Static Routes | 146 |
| QoS Configuration | 147 |
| QoS Priority | 147 |
| Enabling QoS Mode..... | 148 |
| Defining DSCP and CoS on each port | 150 |
| Configuring 802.1p Priority | 151 |
| Configuring DSCP Priority | 152 |
| Port Shaping Rate..... | 153 |
| QoS Policy | 154 |
| Configure Policy Based QoS | 154 |
| Configure Flow-based Control..... | 156 |
| Configure Auto VoIP QoS..... | 157 |
| Configure Queue Scheduler..... | 158 |
| Queue Management | 159 |
| Setup CoS and DSCP Marking..... | 160 |
| Securing Your Network | 161 |
| Client Management..... | 162 |
| Viewing/Adding Wireless Known Clients | 162 |
| Editing/Deleting Clients | 164 |
| Group Management..... | 165 |
| Adding User Groups..... | 165 |
| Editing User Groups..... | 167 |

| | |
|--|------------|
| Deleting User Groups..... | 168 |
| Configuring Login Policies..... | 169 |
| Configuring Browser Policies..... | 170 |
| Configuring IP Policies | 171 |
| User Management | 172 |
| Adding Users Manually | 172 |
| Importing Users | 173 |
| Editing Users | 174 |
| Deleting Users | 175 |
| Password Rules..... | 176 |
| Guest Account Usage Management | 177 |
| Payment Gateway..... | 181 |
| Login Profiles | 182 |
| Customize the Captive Portal Login Page | 182 |
| Customize the SLA of the Captive Portal..... | 185 |
| External Authentication..... | 186 |
| Configure RADIUS Server | 186 |
| Configure POP3 Server..... | 188 |
| Configure POP3 Trusted CA..... | 189 |
| Configure LDAP Server..... | 190 |
| Blocked Clients..... | 192 |
| Status and Statistics | 193 |
| Viewing Statistic and Utilization | 195 |
| Manage Dashboard | 196 |
| Viewing System Status | 198 |
| Viewing USB Status..... | 199 |
| Viewing DHCP Clients | 200 |
| Viewing Captive Portal Sessions | 201 |
| Viewing Traffic on Interfaces | 202 |
| Viewing Link Aggregation | 204 |
| Viewing Controller Status and Statistics | 205 |
| Controller Associated Clients | 206 |
| Distributed Tunnel | 207 |
| Peer Controller Receive Status..... | 208 |
| Peer Controller Sent Status | 210 |
| Viewing Access Point Information | 211 |
| Global Status | 211 |
| All APs | 213 |
| Managed..... | 214 |
| Peer Managed..... | 216 |
| Authentication Failed..... | 217 |
| RF Scan | 218 |
| De-Authentication Attacks | 219 |

| | |
|---|------------|
| Hardware Capability | 221 |
| Associated Clients Global Status | 223 |
| Associated Clients | 224 |
| Ad Hoc Clients | 228 |
| Detected Clients | 229 |
| Viewing Cluster Information | 231 |
| Viewing WDS Group Status..... | 232 |
| WDS Group AP Status | 233 |
| Viewing WDS AP Status..... | 235 |
| Viewing WDS Link Status | 236 |
| Viewing WDS Link Statistics..... | 237 |
| Maintenance | 238 |
| System Settings | 239 |
| Set System Name | 239 |
| Set System Date and Time | 239 |
| Set Login Session Timeout..... | 240 |
| Set USB Share Ports..... | 240 |
| Activating Licenses..... | 241 |
| Remote Management..... | 242 |
| Using SNMP..... | 243 |
| Configure SNMP v3 User List..... | 243 |
| Configure SNMP Trap List..... | 244 |
| Configure SNMP Access Control List..... | 245 |
| Configure SNMP System Info..... | 246 |
| Configure Wireless SNMP Info | 246 |
| Backup Configuration Settings | 249 |
| Restoring Configuration Settings..... | 250 |
| Restoring Factory Default Settings | 251 |
| Rebooting the Wireless Controller | 252 |
| Upgrading Firmware..... | 253 |
| Wireless Controller Firmware Upgrade | 253 |
| Using the Command Line Interface..... | 255 |
| Troubleshooting | 256 |
| LED Troubleshooting | 257 |
| Power LED is OFF..... | 257 |
| LAN Port LEDs Not ON..... | 257 |
| Web Management Interface | 257 |
| Using the Reset Button to Restore Default Settings..... | 258 |
| Problems with Date and Time | 258 |
| Discovery Problems with Access Points..... | 258 |
| Connection Problems..... | 259 |

| | |
|---|------------|
| Network Performance and Rogue Access Point Detection..... | 259 |
| Using Diagnostic Tools on the Wireless Controller | 260 |
| Ping an IP Address | 260 |
| Using Traceroute | 261 |
| Performing DNS Lookups..... | 262 |
| Capturing Log Packets | 263 |
| Conducting a System Check | 264 |
| Log Settings | 265 |
| Defining What to Log..... | 265 |
| Tracking Traffic/Routing Logs..... | 267 |
| System Logging | 268 |
| Remote Logging | 269 |
| Syslog Server Configuration..... | 271 |
| Event Log | 272 |
| Current Logs | 273 |
| WLAN Logs..... | 274 |
| LAN Logs..... | 275 |
| Appendix A - Basic Planning Worksheet..... | 276 |
| Appendix B - Factory Default Settings..... | 279 |
| Appendix C - Glossary | 280 |
| Appendix D - Technical Specifications | 282 |

Product Overview

Introduction

The DWC-2000 Wireless Controller is intended to provide medium-to-large-sized businesses with a solution for configuring, managing, and monitoring up to 256 D-Link DWL-2600AP, DWL-3600AP, DWL-6600AP, DWL-8600AP, and/or DWL-8610AP access points from a central location.

Using the wireless controller and the access points with which it is associated lets you:

- Discover and configure D-Link access points on the WLAN
- Optimize wireless access point performance with centralized RF management, security, Quality of Service (QoS), and other configuration features
- Streamline security configuration tasks and set up guest access
- Monitor network status and statistics
- Perform maintenance tasks and firmware updates for the wireless management system and for D-Link access points on your wireless network
- Conduct troubleshooting procedures

Configuration is performed using configuration profiles. A configuration profile allows a wireless controller to distribute a set of radio, Service Set Identifier (SSID), and QoS parameters to the access points associated with that profile.

The wireless controller comes with one profile predefined. You can use this profile as is, edit it to suit your requirements, or create new configuration profiles as necessary. For example:

- An office building may have one configuration profile for access points located in one area of a facility (such as a general work area) and a different profile for access points in another area of the facility (for example, in the Human Resources department).
- A shopping mall may need several configuration profiles if several businesses share a WLAN, but each business has its own network.
- Large networks that need different policies per building or department could have access points configured for security policies for each building and department (for example, one for guests, one for management, one for sales, and so on).

Features and Benefits

The DWC-2000 Wireless Controller is intended for campuses, hospitality, and medium-to-large businesses. In a stacked configuration with the appropriate licenses, a wireless controller can support up to 256 access points. The wireless controller allows you to manage your wireless network from a central point, implement security and QoS features centrally, configure a guest access captive portal, and support Voice over Wi-Fi.

Scalable Architecture with Stacking and Redundancy

- Supports for 64 access points on a single wireless controller with no additional license.
- Purchased license packs (DWC-2000-AP32 / DWC-2000-AP32-LIC / DWC-2000-AP64 / DWC-2000-AP64-LIC / DWC-2000-AP128/ DWC-2000-AP128-LIC) in increments of 32/64/128 access points which allows for support of up to 256 access points on a single wireless controller.
- Up to 1,024 access point in a clustering group network.
- Maximum of 8 wireless controllers and support auto-failover redundancy while access points in full capacity.
- Supports IEEE 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac protocols.

Centralized Management and Configuration

- Auto-discovery of access points in L2 and L3 domains.
- Single point of management for the entire wireless network.
- Simplified profile-based configuration.
- DHCP server for dynamic IP address provisioning.
- Configurable management VLAN.
- Real-time monitoring of access points and associated client stations.
- System alarms and statistics reports on managed access points for managing, controlling, and optimizing network performance.

Security

- Identity-based security authentication with an external RADIUS server or an internal authentication server.
- Rogue access point detection, classification, and mitigation.
- Captive Portal for user authentication.
- Guest Management and ticket generation.

After the site survey is complete, use the collected data to set up an RF plan using the Basic Planning Worksheet in Appendix A.

After you complete the Basic Planning Worksheet, select a location for the wireless controller. The ideal location should:

- Be flat and clean, with no dust, water, moisture, or exposure to direct sunlight or vibrations.
- Be fairly cool and dry, and does not exceed 104° F (40° C).
- Not be prone to variations in temperature and humidity, or close to strong magnetic fields or a device that generates electric noise.
- Not place the wireless controller next to, on top of, or below any device that generates heat or will block the free flow of air through the wireless controller's ventilation slots. Leave at least 3 feet (91.4 cm) clear on both sides and rear of the controller.
- Allow you to reach the wireless controller and all cables attached to it.
- Have a working AC power outlet that is not controlled by a wall switch that can accidentally remove power to the outlet.

Package Contents

Each wireless controller package contains the following items:

- One D-Link DWC-2000 Wireless Controller
- One power cord
- One RJ-45 to DB-9 console cable
- One 3-foot Ethernet Category 5 UTP/straight-through cable
- One Reference CD-ROM containing product documentation in PDF format
- Two rack-mounting brackets
- Quick Installation Guide

Required Tools and Information

You will need the following additional items to install your wireless controller:

- D-Link DWL-2600AP, DWL-3600AP, DWL-6600AP, DWL-8600AP, and/or DWL-8610AP access points.
- A computer with a supported web browser for configuration (refer to page 20).

Front Panel



| | | |
|---|-------------------|---|
| 1 | Power LED | A solid green light indicates a good connect to a power source. This LED will be orange during bootup. |
| 2 | Reset Button | Press and hold for 10 seconds to reset the wireless controller back to the factory default settings. |
| 3 | Fan LED | Indicates the fan status on the wireless controller. |
| 4 | USB Ports | Two Universal Serial Bus (USB) 2.0 ports are provided for connecting USB flash drives, hard drives, and printers. A solid LED indicates the USB device is attached. This LED will blink during data transmission. |
| 5 | Module Bay | Slot for the hard disk drive module. |
| 6 | Fiber Ports (1-4) | Four 100/1000 SFP combo ports labeled 1 through 4 |
| 7 | LAN Ports (1-4) | Four Gigabit Ethernet ports labeled 1 through 4 let you connect Ethernet devices such as computers, switches, and network storage (NAS) devices. Each port has an Activity LED (left) and Link LED (right). |
| 8 | Console Port | The RJ-45 console cable lets you connect a PC to access the wireless controller's command-line interface. |

Rear Panel



| | | |
|---|---------------|---|
| 1 | On/Off Switch | Press to turn the wireless controller on and off. |
| 2 | Power Port | Connect the supplied power cord to a power outlet or surge protector. |

Installation

A DWC-2000 wireless controller system consists of one or more wireless controllers and a collection of DWL-2600AP, DWL-3600AP, DWL-6600AP, DWL-8600AP, and/or DWL-8610AP access points that are organized into groups based on location or network access. This section describes how to unpack and install the wireless controller system.

Unpacking

Follow these steps to unpack the wireless controller and prepare it for operation:

1. Open the shipping container and carefully remove the contents.
2. Return all packing materials to the shipping container and save it.
3. Confirm that all items listed on page 14 are included in the shipment. Check each item for damage. If any item is damaged or missing, notify your authorized D-Link representative.

Selecting a Location

Selecting the proper location for the wireless controller is essential for its successful operation. To ensure optimum performance, D-Link recommends that you perform a site survey. A site survey should enable you to:

- Identify how Wi-Fi coverage should be provided.
- Determine access point placement locations, and identify areas with weak signal or dead spots that require additional access points.
- Determine areas of heavier usage that might require dense access point coverage.
- Determine the indoor propagation of RF signals.
- Identify potential RF obstructions and interference sources.
- Run a spectrum analysis of channels of the site to ascertain current RF behavior, and detect both 802.11 and non-802.11 noise.
- Run an access point-to-client connectivity test to determine maximum throughput achievable on the client.

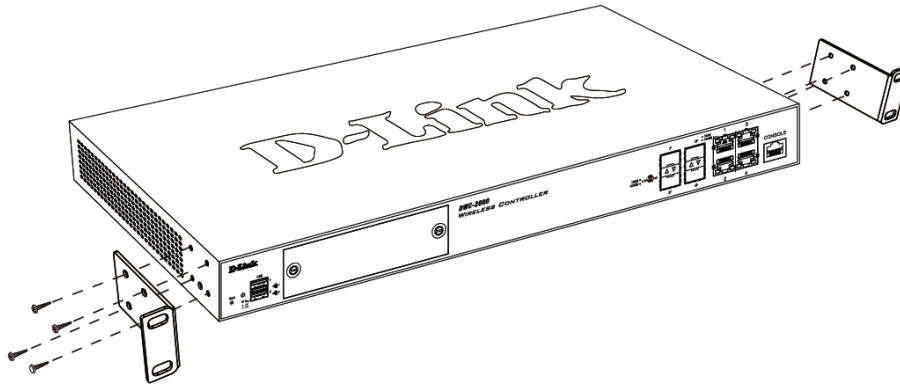
After the site survey is complete, use the collected data to set up an RF plan using the Basic Planning Worksheet in Appendix A. After you complete the Basic Planning Worksheet, select a location for the wireless controller. The ideal location should:

- Be flat and clean, with no dust, water, moisture, or exposure to direct sunlight or vibrations.
- Be fairly cool and dry, and does not exceed 104° F (40° C).
- Not be prone to variations in temperature and humidity, or close to strong magnetic fields or a device that generates electric noise.
- Not place the wireless controller next to, on top of, or below any device that generates heat or will block the free flow of air through the wireless controller's ventilation slots. Leave at least 3 feet (91.4 cm) clear on both sides and rear of the controller.
- Allow you to reach the wireless controller and all cables attached to it.
- Have a working AC power outlet that is not controlled by a wall switch that can accidentally remove power to the outlet.

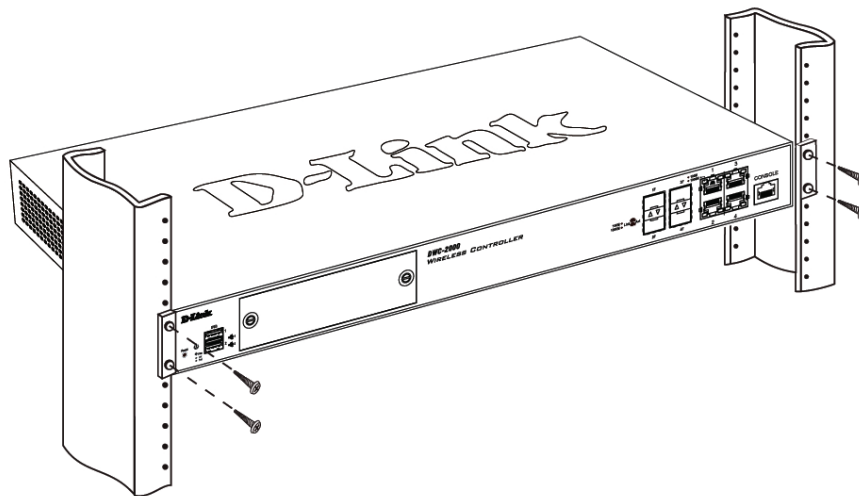
Rack Mount

The wireless controller can be mounted in a standard 19-inch equipment rack.

1. Attach the mounting brackets to each side of the chassis and secure them with the supplied screws.



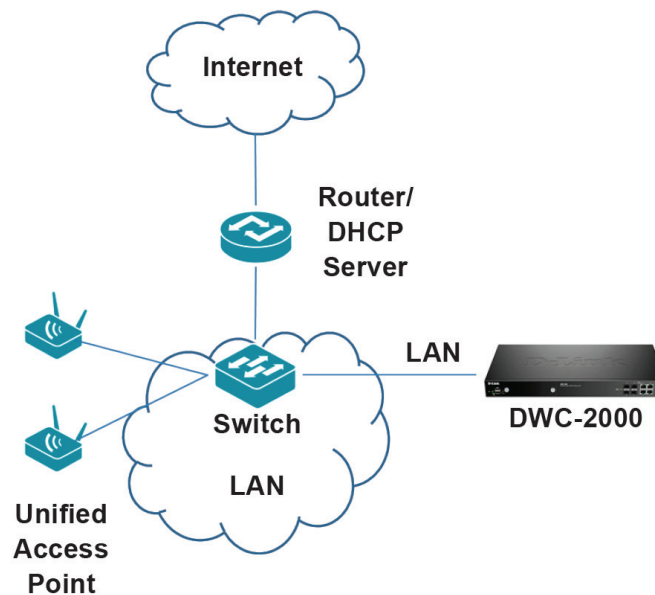
2. Use the screws provided with the equipment rack to mount the wireless controller into the rack.



Connecting the Wireless Controller

To install the wireless controller, perform the following procedure:

1. Install the switch and access points according to the instructions in their documentation.
2. Connect one end of an Ethernet LAN cable to one of the ports labeled LAN (1-4) on the front of the wireless controller. Connect the other end of the cable to an available RJ-45 port on a switch in the LAN network segment.
3. Connect one of the wireless controller ports labeled LAN (1-4) to the network or directly to a PC.



4. Using the supplied power cord, connect the wireless controller to a working AC outlet.
5. The Power LED will illuminate orange during boot up. The LED will turn green once the wireless controller has booted.

Basic Configuration

After you install the wireless controller, perform the basic configuration instructions described in this section which includes:

- “Log in to the Web Management Interface” on page 20
- “Web Management Interface Layout” on page 22
- “Standard Web Management Interface Features” on page 23
- “Basic Configuration Procedures” on page 24

Using the information in this chapter, you can perform the basic information and get your wireless controller up and running in a short period of time.

Log in to the Web Management Interface

Configuration procedures using the wireless controller's web management interface are performed using one of the following supported web browsers:

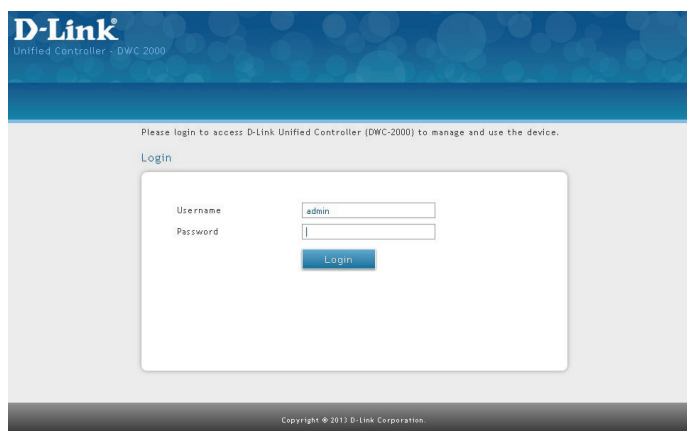
- Microsoft Internet Explorer 9.0 or higher
- Mozilla Firefox 23 or higher
- Apple Safari 5.1.7 or higher (Windows)
- Apple Safari 6.1.3 or higher (iOS)
- Google Chrome 26 or higher

Before you perform the following procedure:

- Configure your PC running the web browser to use an IP address on the 192.168.10.x network, with a subnet mask of 255.255.255.0.
- Configure your web browser to accept cookies, prompt for pop-ups, and allow sites to run JavaScript.
- Upgrade the firmware for your wireless controller (see "Upgrading Firmware" on page 20).
- Upgrade the firmware for your access points after you upgrade the wireless controller firmware (refer to the documentation for your access points).

To log in to the web management interface:

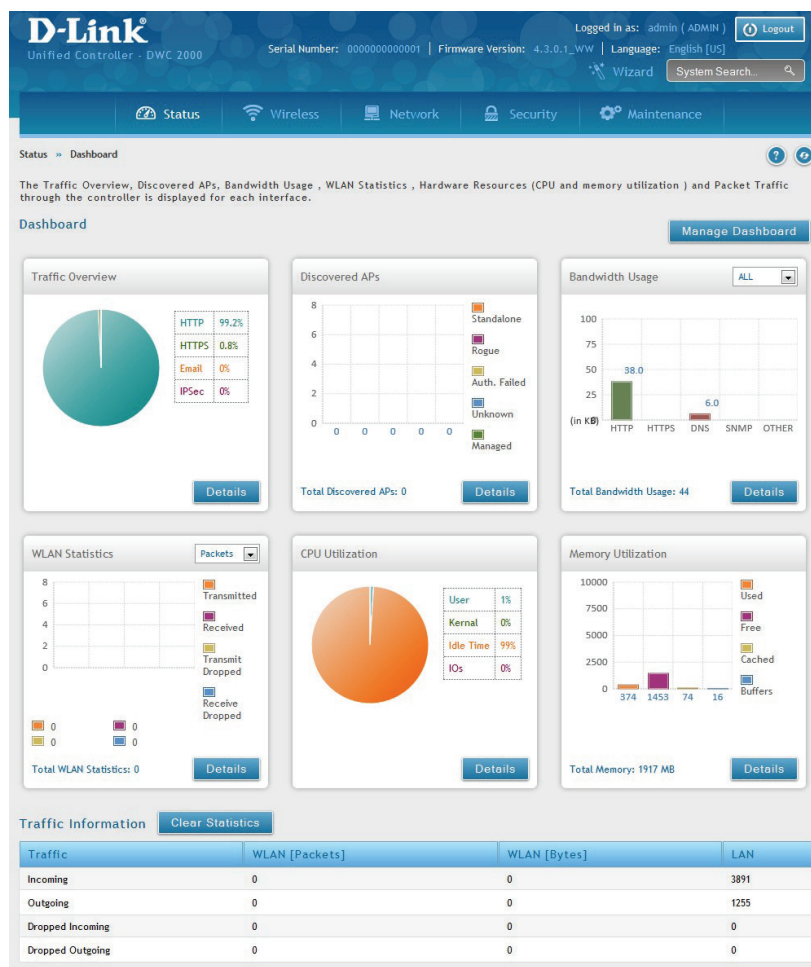
1. Launch a web browser on the PC.
2. In the address field of your web browser, type the IP address for the wireless controller web management interface. The default IP address is **http://192.168.10.1**. A login prompt will appear. If the login prompt does not appear, see "Web Management Interface" on page 257.



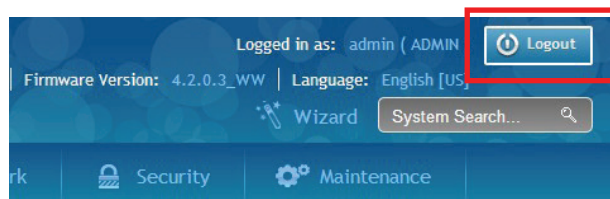
3. If you are logging in for the first time, the default user name is **admin** and the default password is **admin**. Both the user name and password are case-sensitive.

Note: We recommend that you change the password to a new, more secure password (see "Editing Users" on page 174) and record it in Appendix A.

- Click **Login**. The web management interface opens with the System Status page. This page displays general, LAN, and WLAN status information. You can return to this page at any time by clicking **Status > Dashboard**.



- To log out of the web management interface, click the **Logout** icon, which is in the top-right corner of the page in the System Menu area.



Web Management Interface Layout

A web management interface screen can include the following components:

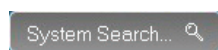
- **1st level:** Main navigation menu tab. The main navigation menu tabs appear across the top of the web management interface. These tabs provide access to all configuration menus and remain constant.
- **2nd level:** Main navigation submenu tab. The main navigation submenu tabs appear on drop-down menus when you move your mouse over the main navigation menu tabs.
- **3rd level:** Middle menu tabs. Some pages have menu tabs below the main navigation menu tab which lead to other pages when you click on them.
- **4th level:** Workspace. The workspace shows the parameters associated with the selected menu and submenu.
- **Action buttons:** Action buttons change the configuration or allow you to make changes to the configuration. Common action buttons are:
 - **Save:** Saves all configuration changes made on the current screen. Saved settings are retained when the wireless controller is powered off or rebooted, while unsaved configuration changes are lost.
 - **Cancel:** Resets options on the current screen to the last-applied or last-saved settings.
 - **Add:** Adds a new item to the current screen.
 - **Right-click:** Right-clicking list table items allow you to do more action for the existing items.
 - **Edit:** Modify the configuration of this item.
 - **Delete:** Delete this item.
 - **Move:** Move this item to specific position.
 - **Enable:** Enable this item.
 - **Disable:** Disable this item.
 - **Apply:** Apply this change to existing configuration.
 - **Copy:** Copy the configuration value of this item and create a new item.
 - **Manage:** Manage the discovered access point.
 - **View Information:** The information would be various depending on the items.

Standard Web Management Interface Features

There are several standard features in the web management interface.



The Help feature has explanations for the various functions and settings on the interface. Click on the question mark icon to bring up the Help menu. It is always located near the top right corner of the screen.



System Search allows you to search for a function or feature by typing in a word into the search box. The search box is always located near the top-right corner of the screen.



The Wizard feature provides a number of helpful guides to common configuration task such as setting up the device, connecting to the internet, configuring wired and wireless networking, setting security options, and creating new users. Click on the Wizard wand icon to bring up the wizard. It is always located near the top-right corner of the screen, on the left of the System Search box.



Refresh allows you to refresh the interface in order for changes to take effect immediately. Click on the refresh icon near the top-right corner of the screen, to the right of the Help icon.



Logout allows you to log out of the interface securely after you have finished. Click on the Logout icon at the top-right corner of the screen.



Menu Navigation Route - Displays the menu route for the current page.



Displays the number of items on the table in one page. The system can list 10, 25, 50, 100 entries in one page.



First/ Previous/ Next/ Last (on table)

Information would be shown in multiple pages. Use First/ Previous/ Next/ Last to switch pages. The page change function is always located near the bottom right corner of the table



Search bar (on table)

Table content search allows you to search information in the table by typing in a word into the search box. The search box is always located near the top right corner of the table.



Ranking/sort (on table)

Rank/sort the relative order of value and information on the table by clicking table header.

Basic Configuration Procedures

To perform common basic configuration procedures, follow the steps below:

- "Step #1: Enable DHCP Server (Optional)" on page 25
- "Step #2: Configure Country Code" on page 26
- "Step #3: Select APs to be Managed" on page 27
- "Step #4: Change the SSID and Set Up Security" on page 29
- "Step #5: Select MAC Authentication Mode" on page 34
- "Step #6: Confirm Access Point Profile is Associated" on page 36
- "Step #7: Configure Captive Portal Settings" on page 37
- "Step #8: Use SSID with RADIUS Sever as Authenticator" on page 45
- "Step #9: Configure Guest Management" on page 46
- "Step #10: Configure a BYOD Environment" on page 53

Step #1: Enable DHCP Server (Optional)

By default, Dynamic Host Configuration Protocol (DHCP) is disabled on the wireless controller. If you are not configuring your access points with static IP addresses, set up a DHCP server, or DHCP server relay on the network. If desired, perform the following procedure to configure your wireless controller to act as a DHCP server.

1. Click **Network > LAN > LAN Settings > IPv4 LAN Settings**. The LAN Settings page will appear.

2. Under *IP Address Setup*, change the IP Address and Subnet Mask to values used within your network. Record the settings; you will refer to them later in this procedure.
3. Click **Save**.
4. Wait 60 seconds and then relaunch your web browser.
5. In the web browser's address field, enter the new IP address you recorded in step 2.
6. Click **Network > LAN > LAN Settings > IPv4 LAN Settings**.
7. In the LAN Settings page, change *DHCP Mode* to **DHCP Server**. This will bring up several new fields below DHCP Mode.
8. Complete the fields below and click **Save**.

| Field | Description |
|-----------------------------|--|
| Starting IP Address | Enter the starting IP address in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address within the starting and ending IP address range. Starting and ending IP addresses should be in the same IP address subnet as the wireless controller's LAN IP address. |
| Ending IP Address | Enter the ending IP address in the IP address pool. |
| Default Gateway | Enter the IP address of the gateway for your LAN. |
| Domain Name | Enter the domain name. |
| Lease Time | Enter the lease time of the assigned IP addresses. |
| Configure DNS/ WINS | Turn this on to enter the IP address of the DNS or WINS server. |
| Primary DNS Server | If configured Domain Name System (DNS) servers are available on the LAN, enter the IP address of the primary DNS server. |
| Secondary DNS Server | If configured domain name system (DNS) servers are available on the LAN, enter the IP address of the secondary DNS server. |
| WINS Server | If Windows Internet Name Service (DNS) servers are available on the LAN, enter the IP address of the WINS server. |

Step #2: Configure Country Code

Each country has its regulation for the radio usage. Use the following procedure to select the country where the wireless networks are.

1. Click **Wireless > General > General**. The General Setting page will appear.
2. At the bottom, select the *Country Code* from the drop-down menu and click **Save**.

D-Link
Unified Controller - DWC 2000

Logged in as: admin (ADMIN) Logout

Serial Number: 0000000000001 | Firmware Version: 4.2.0.3_WW | Language: English [US]

Wizard System Search...

Status Wireless Network Security Maintenance

Wireless > General

This page will guide you through common and easy steps to configure your DWC-2000 controller WLAN global settings. Make sure that WLAN controller is being enabled for working of wireless functionality.

General Setting

WLAN Global Setup

IP Address: 192.168.10.1

Peer Group ID: 1 [Default: 1, Range: 1 - 255]

Client Roam Timeout: 30 [Range: 1 - 120] Seconds

Ad Hoc Client Status Timeout: 24 [Range: 0 - 168] Hours

AP Failure Status Timeout: 24 [Range: 0 - 168] Hours

Client MAC Authentication Mode: ☒ White-list ☐ Black-list

RF Scan Status Timeout: 24 [Range: 0 - 168] Hours

Detected Clients Status Timeout: [Range: 0 - 168] Hours

Tunnel IP MTU Size: [Range: 0 - 168] Hours

Cluster Priority: [Range: 0 - 168] Hours

AP Client QoS: [Range: 0 - 168] Hours

AP Validation

AP MAC Validation: [Range: 0 - 168] Hours

Require Authentication Passphrase: [Range: 0 - 168] Hours

Manage AP with Previous Release Code: [Range: 0 - 168] Hours

Country Configuration

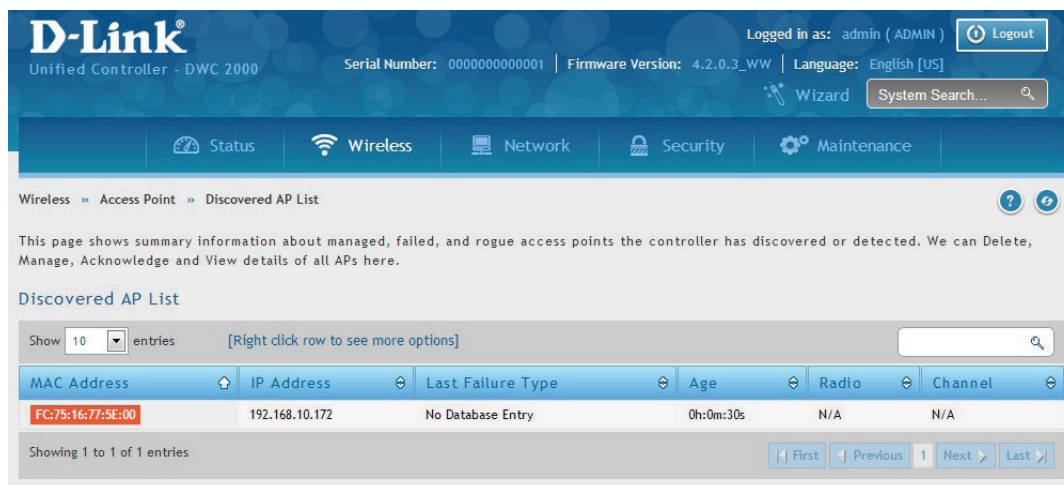
Country Code: US - United States

Save Cancel

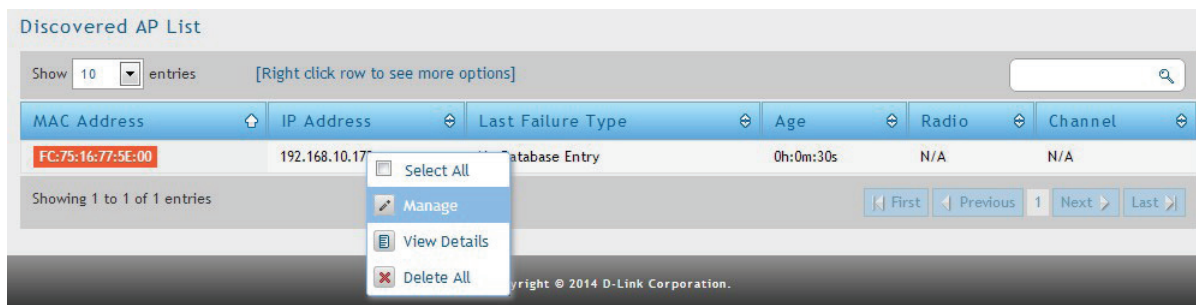
Step #3: Select APs to be Managed

The wireless controller automatically discovers managed and unmanaged access points on the WLAN that are in the same IP subnet. Use the following procedure to select the access points that the wireless controller will manage.

1. Click **Wireless > Access Point > Discovered AP List**. The Discovered AP List page will appear with a list of access points that the wireless controller has discovered.



2. Under *Discovered AP List*, right-click on the access point you want the wireless controller to manage and select **Manage**.



3. Complete the fields in the *Manage AP* page (refer to the next page) and click **Save**. When the confirmation appears, click **OK**.

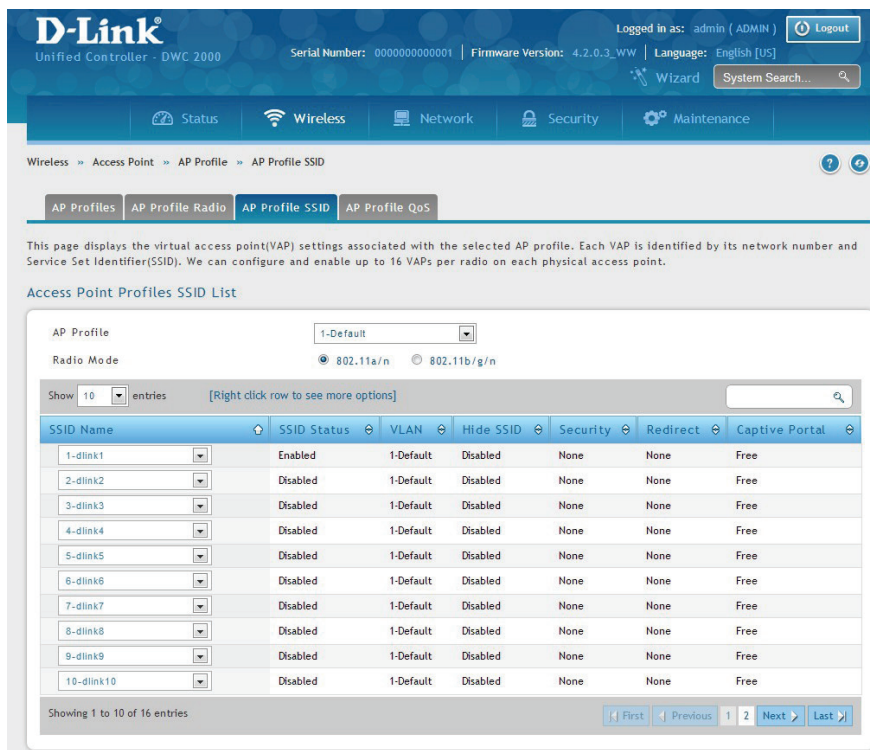
| Field | Description |
|------------------------------------|---|
| MAC Address | MAC address of the access point. |
| AP Mode | Select standalone, managed, or rogue. Selecting standalone will require you to fill out the fields below from Location to Expected Wired Network Mode. <ul style="list-style-type: none"> • Standalone • Managed = Access point profile configuration has been applied to the access point and the access point operating in managed mode. • Rogue = Access point has not tried to contact the wireless controller and the access point's MAC address is not in the Valid AP database. |
| Location | Optional field to identify location of the access point being managed. |
| Expected SSID | If AP Mode = Standalone, the SSID that the access point should be set to is displayed. This is for reference only. |
| Expected Channel | If AP Mode = Standalone, the channel to be used for wireless communication is displayed. This is for reference only. |
| Expected WDS Mode | If AP Mode = Standalone, the WDS (Wireless Distributed System) mode to be used if you intend to use WDS. This is for reference only. |
| Expected Security Mode | If AP Mode = Standalone, the security mode to be used is displayed. This is for reference only. |
| Expected Wired Network Mode | If AP Mode = Standalone, select whether wired networking is going to be allowed. This is for reference only. |
| Authentication | If AP Mode = Managed, turn on to require a password for authentication. |
| Profile | If AP Mode = Managed, select a profile to apply for AP configuration. |
| Radio | If AP Mode = Managed, this is Wireless radio mode that the access point is using is displayed. The fields below appear after you have selected Managed AP Mode. |
| Channel | If AP Mode = Managed, this is operating channel for the radio. |
| Power | If AP Mode = Managed, this is percentage of power to use for the radio. |

4. Repeat steps 2 and 3 for each additional access point you want the wireless controller to manage.

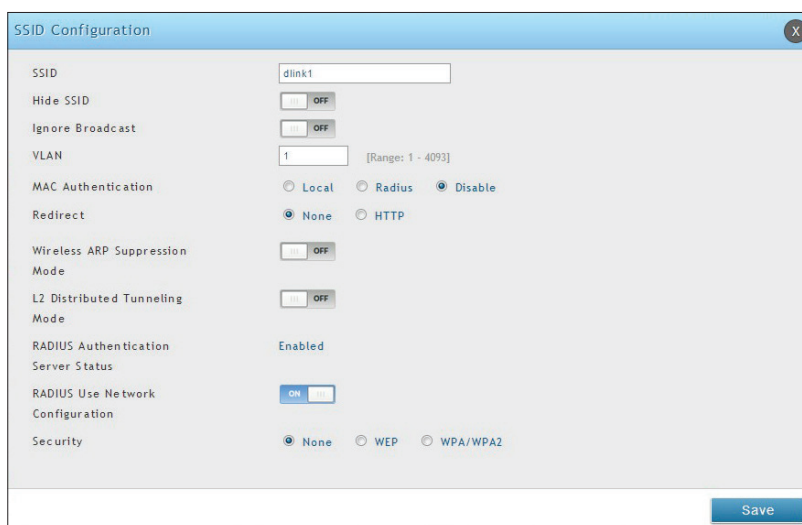
Step #4: Change the SSID and Set Up Security

You can configure up to 50 separate networks on the wireless controller and apply them across multiple radio and virtual access point interfaces. By default, 16 networks are pre-configured and applied in order to the access points on each radio. In this procedure, you will edit one of the pre-configured networks and change its SSID and security settings to suit your requirements.

1. Click **Wireless > Access Point > AP Profile > AP Profile SSID**. The following page will appear with a list of the wireless networks configured on the wireless controller.



2. Under the **SSID Status** column, select an SSID by right-clicking on it and clicking **Edit**. The following page will appear.



3. Complete the Security fields on the SSID Profile Configuration page.

| Field | Description |
|----------|---|
| SSID | Enter the case-sensitive name of the wireless network. Be sure the SSID is the same for all device in your wireless network. |
| VLAN | Enter a VLAN ID. Be sure this VLAN ID had been created on VLAN Setting (Network > VLAN > VLAN Setting). |
| Security | <p>The default access point profile does not use any security mechanism. To protect your network, we recommend you select a security mechanism to prevent unauthorized wireless clients from gaining access to your network. Choices are:</p> <ul style="list-style-type: none"> • None = no security mechanism is used. • WEP = enable WEP security. Complete the options in Table 3-1. • WPA/WPA2 = enable WPA/WPA2 security. Complete the options in Table 3-2. |

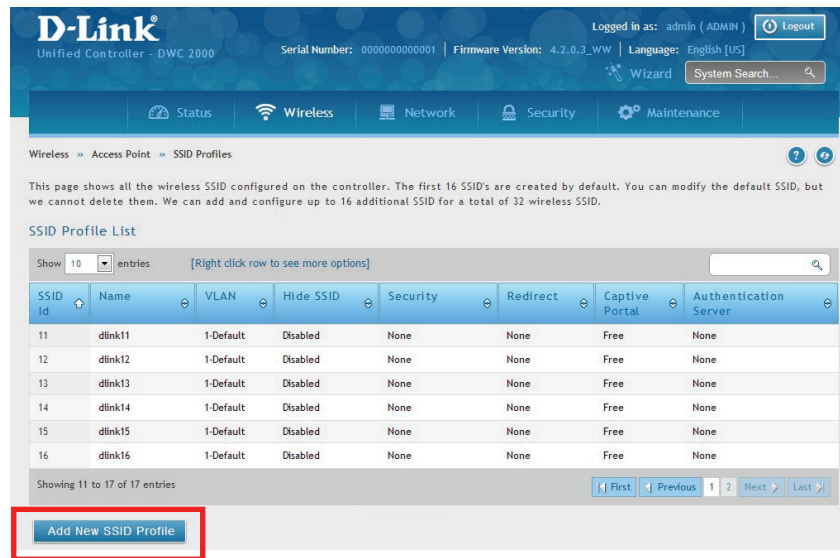
Table 3-1 WEP Page Settings

| Field | Description |
|-----------------------|---|
| Security | <ul style="list-style-type: none"> • Static WEP = uses static key management. You manually configure the same keys to encrypt data on both the wireless client and the access point. Dynamic WEP (WEP IEEE 802.1x) uses dynamically generated keys to encrypt client-to- access point traffic. • WEP IEEE 802.1X = screen refreshes, and there are no more fields to configure. The access point uses the global RADIUS server or the RADIUS server you specified for the wireless network. |
| Authentication | <p>Select the authentication type. Choices are:</p> <ul style="list-style-type: none"> • Open System = any wireless station can request authentication. The station that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station returns a frame that indicates whether it recognizes the sending station. • Shared Key = each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel. |
| WEP Key | <p>Select the key type. Choices are:</p> <ul style="list-style-type: none"> • ASCII = upper- and lower-case alphabetic letters, numeric digits, and special symbols such as @ and #. • HEX = digits 0 to 9 and letters A to F. |
| WEP Key Length (bits) | <p>Select the length of the WEP key. Choices are:</p> <ul style="list-style-type: none"> • 64 = 64 bits • 128 = 128 bits |
| Tx | Transfer Key Index. Indicates which WEP key the access point uses to encrypt the data it transmits. To select a transfer key, click the button in front of the key number and the field where you enter the key. |
| WEP Keys | <p>You can specify four WEP keys. In each text box, enter a string of characters for each of the RC4 WEP keys shared with the stations using the access point. Use the same number of characters for each key. The number of keys you enter depends on the WEP Key Type and WEP Key Length selections. The following list shows the number of keys to enter in the field:</p> <ul style="list-style-type: none"> • 64 bit = ASCII: 5 characters; Hex: 10 characters • 128 bit = ASCII: 13 characters; Hex: 26 characters <p>Each client station must be configured to use one of these WEP keys in the same slot as specified here.</p> |

Table 3-2 WPA/WPA2 Page Settings

| Field | Description |
|---|---|
| Security | <p>If you select WPA for Security, the following two additional security options are displayed.</p> <ul style="list-style-type: none"> WPA Personal = uses static key management. You manually configure the same keys to encrypt data on both the wireless client and the access point. WPA Enterprise uses a RADIUS server and dynamically generated keys to encrypt client-to- access point traffic. WPA Enterprise is more secure than WPA Personal, but you need a RADIUS server to manage the keys. WPA Enterprise = more secure than WPA Personal, but you need a RADIUS server to manage the keys. If you click this option, the screen refreshes and the WPA Key Type and WPA Key fields are hidden. The access point uses the global RADIUS server or the RADIUS server you specified for the wireless network. |
| WPA Versions | <p>Select the types of client stations you want to support. Choices are:</p> <p>WPA = if all client stations on the network support the original WPA but none supports WPA2, select WPA.</p> <p>WPA2 = if all client stations on the network support WPA2, use WPA2, which provides the best security per the IEEE 802.11i standard.</p> <p>WPA and WPA2 = if you have a mix of clients that support WPA2 or WPA, select both boxes. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security.</p> |
| WPA Ciphers | <p>Select the cipher suite you want to use. Choices are:</p> <ul style="list-style-type: none"> TKIP CCMP (AES) TKIP and CCMP (AES) <p>Both TKIP and AES clients can associate with the access point. WPA clients must have a valid TKIP key or AES-CCMP key to associate with the access point.</p> <p>802.11n clients cannot use the TKIP cipher. If you enable TKIP only, 802.11 clients cannot authenticate with the network.</p> |
| WPA Key Type | <p>Enter a WPA key type.</p> <p>Range: ASCII, including upper- and lower-case alphabetic letters, numeric digits, and special symbols such as @ and #</p> |
| WPA Key | <p>Enter the shared secret key for WPA Personal.</p> <p>Range: 8 – 62 characters, including upper- and lower-case alphabetic letters, numeric digits, and special symbols such as @ and #</p> |
| Bcast Key Refresh Rate (seconds) | <p>Enter a value to set the interval at which the broadcast (group) key is refreshed for clients associated to this VAP.</p> <p>Range: 0 - 86400 seconds (0 = broadcast key is not refreshed)</p> |
| Pre-Authentication | If Security= WPA Enterprise, turn on to enable pre-authentication. |
| Pre-Authentication Limit | If Security= WPA Enterprise, the Pre-Authentication Limit field will appear below for you to enter a value between 0 and 192. |
| Key Caching Hold Time | <p>If Security= WPA Enterprise, enter the amount of minutes a PMK will be held by the AP. This applies to Pairwise Master Keys (PMKs) generated by RADIUS, those that come from pre-authentication, and those that are forwarded to the AP. Note that this time limit can be overridden by RADIUS if the RADIUS server returns a longer time in the Session-Timeout attribute for a particular user. The valid values of this are from 1 – 1440 minutes. If you do not enter a value, APs will not forward the PMK for the wireless client to other APs in case the client roams to another AP.</p> |
| Session Key Refresh Rate | <p>If Security= WPA Enterprise, enter a value to set the interval at which the AP will refresh session (unicast) keys for each client associated to the VAP.</p> <p>The valid range is 0-86400 seconds. A value of 0 indicates that the broadcast key is not refresh.</p> |

- To add a new SSID, go to **Wireless > Access Point > SSID Profile** and click the **Add New SSID Profile** button.



- Fill out the fields below and click **Save**.

SSID Profile Configuration

SSID

Captive Portal Type

Hide SSID

Ignore Broadcast

VLAN

MAC Authentication

Redirect

Wireless ARP Suppression Mode

L2 Distributed Tunneling Mode

Free

OFF

OFF

1 [Range: 1 - 4093]

Local Radius Disable

None HTTP

OFF

OFF

Save

6. Click **Wireless > Access Point > AP Profile**. Click on the **AP Profile SSID** tab on the middle menu. The Access Point Profiles SSID List will appear.

AP Profile: 1-Default

Radio Mode: ☒ 802.11a/n ☐ 802.11b/g/n

Show 10 entries [Right click row to see more options]

| SSID Name | SSID Status | VLAN | Hide SSID | Security | Redirect | Captive Portal |
|------------|-------------|-----------|-----------|----------|----------|----------------|
| 1-dlink1 | Enabled | 1-Default | Disabled | None | None | Free |
| 2-dlink2 | Disabled | 1-Default | Disabled | None | None | Free |
| 3-dlink3 | Disabled | 1-Default | Disabled | None | None | Free |
| 4-dlink4 | Disabled | 1-Default | Disabled | None | None | Free |
| 5-dlink5 | Disabled | 1-Default | Disabled | None | None | Free |
| 6-dlink6 | Disabled | 1-Default | Disabled | None | None | Free |
| 7-dlink7 | Disabled | 1-Default | Disabled | None | None | Free |
| 8-dlink8 | Disabled | 1-Default | Disabled | None | None | Free |
| 9-dlink9 | Disabled | 1-Default | Disabled | None | None | Free |
| 10-dlink10 | Disabled | 1-Default | Disabled | None | None | Free |

Showing 1 to 10 of 16 entries

First Previous 1 2 Next Last

7. Select the SSID you wish to edit from the AP Profile drop-down menu.
8. Click the radio button next to the Radio Mode you prefer.
9. Select the SSID you wish to configure on the radio from SSID Name drop-down menu or right-click the SSID network you want to enable and click **Enable** on the AP Profile SSID List.

Note: SSID ID 1 is always enabled. If you do not want to have the first SSID enabled, you must create a new SSID to be able to swap another SSID in the first slot.

Step #5: Select MAC Authentication Mode

MAC authentication is useful in networks that operate in Open mode to grant and deny access to clients with specific MAC addresses. MAC Authentication can also be used in conjunction with 802.1X security methods, in which case MAC Authentication is done prior to 802.1X authentication. To enable MAC authentication, wireless clients must first be authenticated by the Unified Access Point (UAP) in order to connect to the network.

The wireless controller provides two MAC Authentication Mode, the white-list or the black-list.

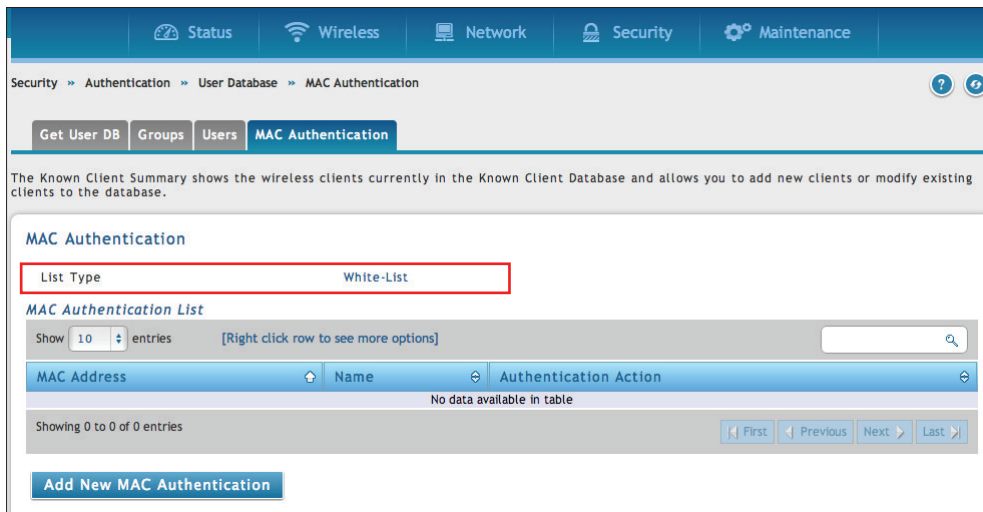
White-list: Select this option to grant access to any wireless clients with MAC addresses that are specified in the MAC Authentication database or RADIUS server, and are not explicitly denied access. If the MAC address is not in the database, then access will be denied to the client.

Black-list: Select this option to deny access to any wireless clients with MAC addresses that are specified in the MAC Authentication database or RADIUS server, and are not explicitly granted access. If the MAC address is not in the database, then access will be granted to the client.

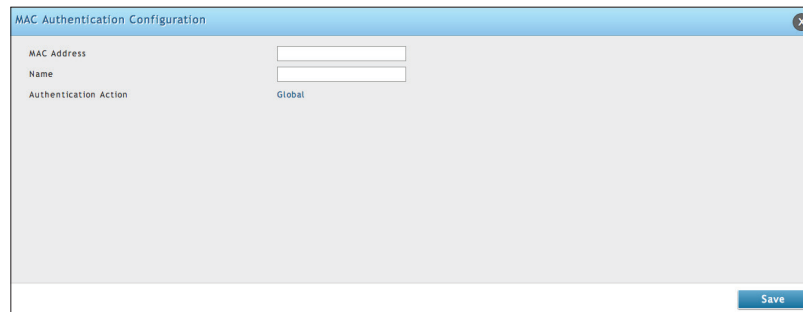
1. Click **Wireless > General > General**.
2. Next to *Client MAC Authentication Mode*, select **Black-list** or **White-list**. Click **Save**.

The screenshot shows the D-Link Unified Controller - DWC 2000 web interface. The top navigation bar includes links for Status, Wireless, Network, Security, and Maintenance. The 'Wireless' section is expanded, showing 'General' settings. The 'Client MAC Authentication Mode' is highlighted with a red box, showing two radio button options: 'White-list' (selected) and 'Black-list'. Below this, there are sections for 'WLAN Global Setup' (including IP Address, Peer Group ID, Client Roam Timeout, Ad Hoc Client Status Timeout, AP Failure Status Timeout, RF Scan Status Timeout, Detected Clients Status Timeout, Tunnel IP MTU Size, Cluster Priority, and AP Client QoS), 'AP Validation' (including AP MAC Validation, Require Authentication Passphrase, and Manage AP with Previous Release Code), and 'Country Configuration' (Country Code). The 'Save' and 'Cancel' buttons are at the bottom.

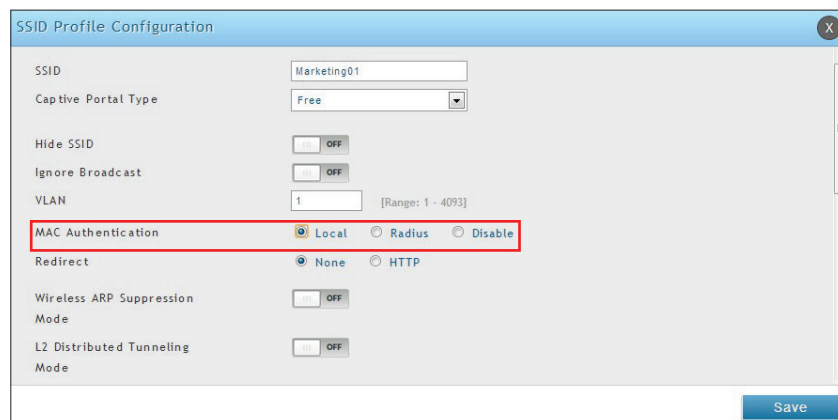
- Click **Security > Authentication > User Database > MAC Authentication**. The MAC Authentication setting page will appear. The *List Type* will display what your selection was in Step 2.



- Click **Add New MAC Authentication**. Fill in the client's MAC address and name, and then click **Save**.



- Click **Wireless > Access Point > SSID Profiles**.
- Select an SSID by right-clicking on it and clicking **Edit**. The following pop-up page will appear. Select **Local** and click **Save**.

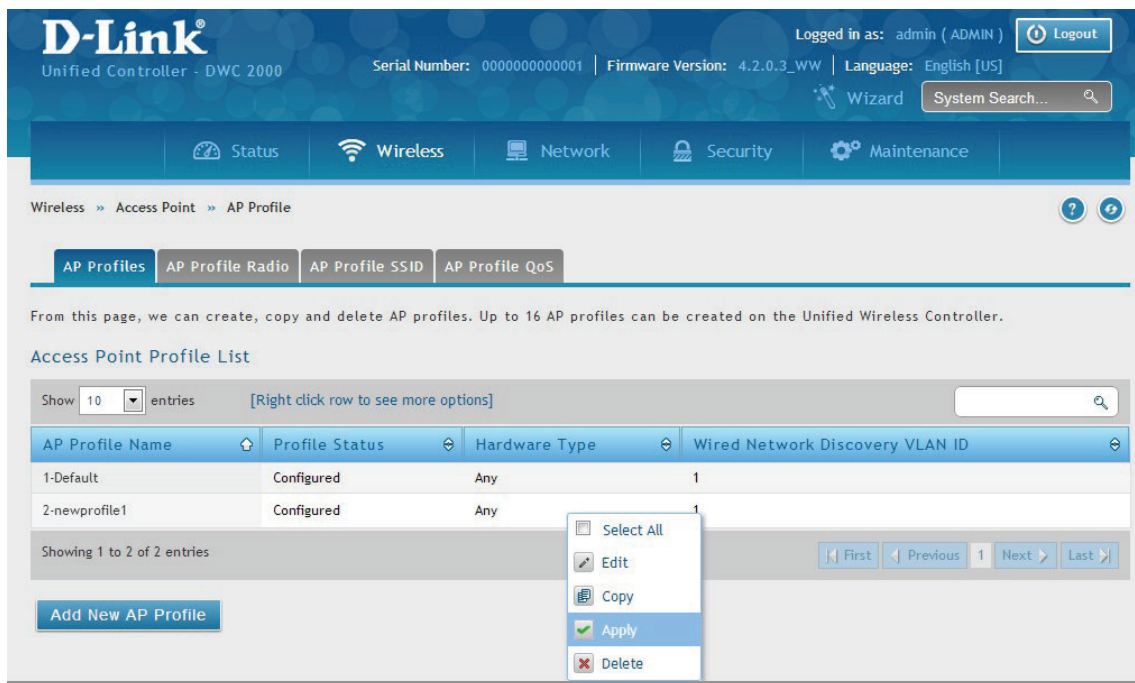



Step #6: Confirm Access Point Profile is Associated

Use the following procedure to confirm that the access point profile is associated with the wireless controller.

Note: Each time you change configuration settings, perform this procedure to apply the changes to the access point.

1. Go to **Wireless > Access Point > AP Profile**.

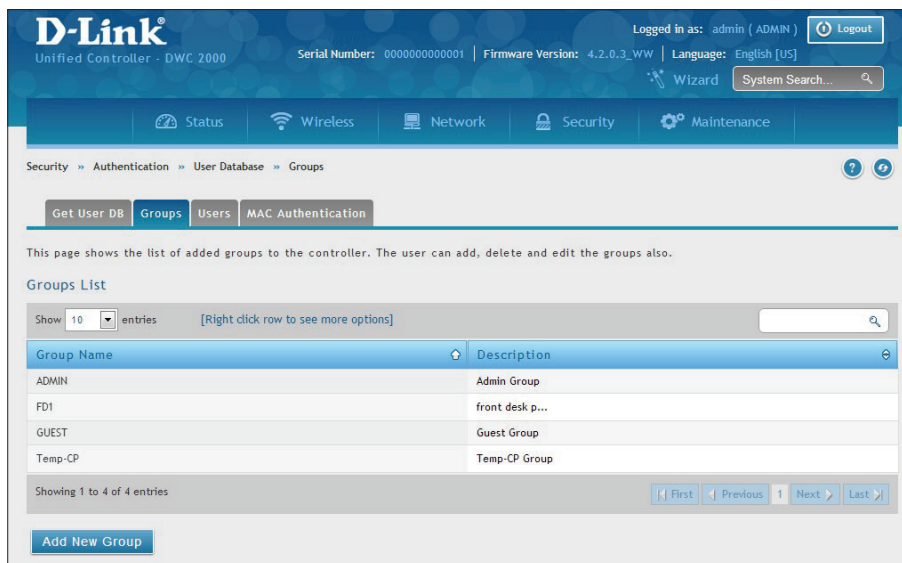


2. Under *Access Point Profile List*, right-click on the AP profile you want to update and click **Apply**.
3. Wait 30 seconds and then click the refresh icon  to verify that the profile is associated. Your associated access point is configured and ready to authenticate wireless users.

Step #7: Configure Captive Portal Settings

Configuring the wireless controller's captive portal settings with local database is a 4-step process:

1. Create a captive portal group
 - a. Go to **Security > Authentication > User Database > Groups**. The Groups List page will appear.



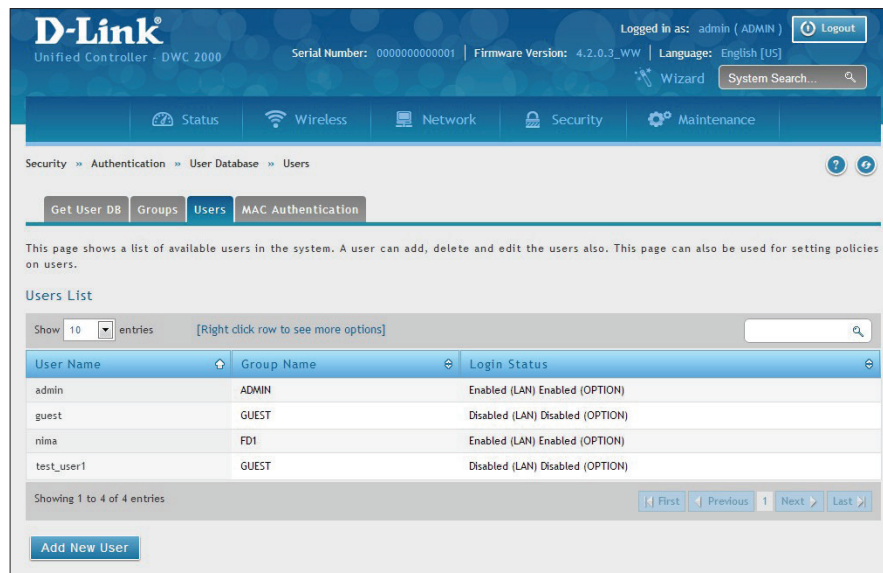
- b. Click **Add New Group**. The Group Configuration page will appear.

- c. Complete the fields in the table below and click **Save**.

| Field | Description |
|---------------------|---|
| Group Name | Enter a name for the group. |
| Description | Enter a description of the group. |
| Captive Portal User | Enable this option under <i>User Type</i> . |

2. Add captive portal users

- a. Go to **Security > Authentication > User Database > Users**. The Users List will appear.



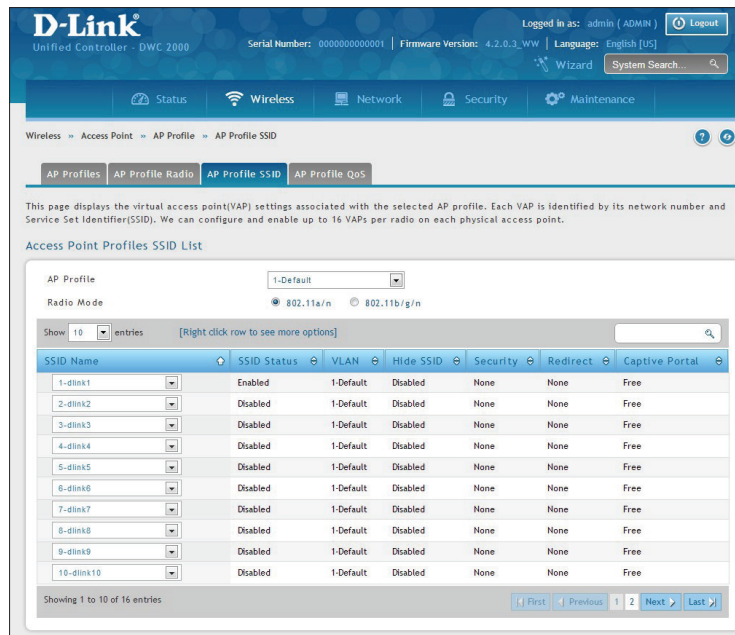
- b. Click **Add New User**. The User Configuration page will appear.

The screenshot shows the User Configuration form. It contains the following fields: User Name, First Name, Last Name, Select Group (a dropdown menu currently showing ADMIN), Password, and Confirm Password. A "Save" button is located at the bottom right of the form.

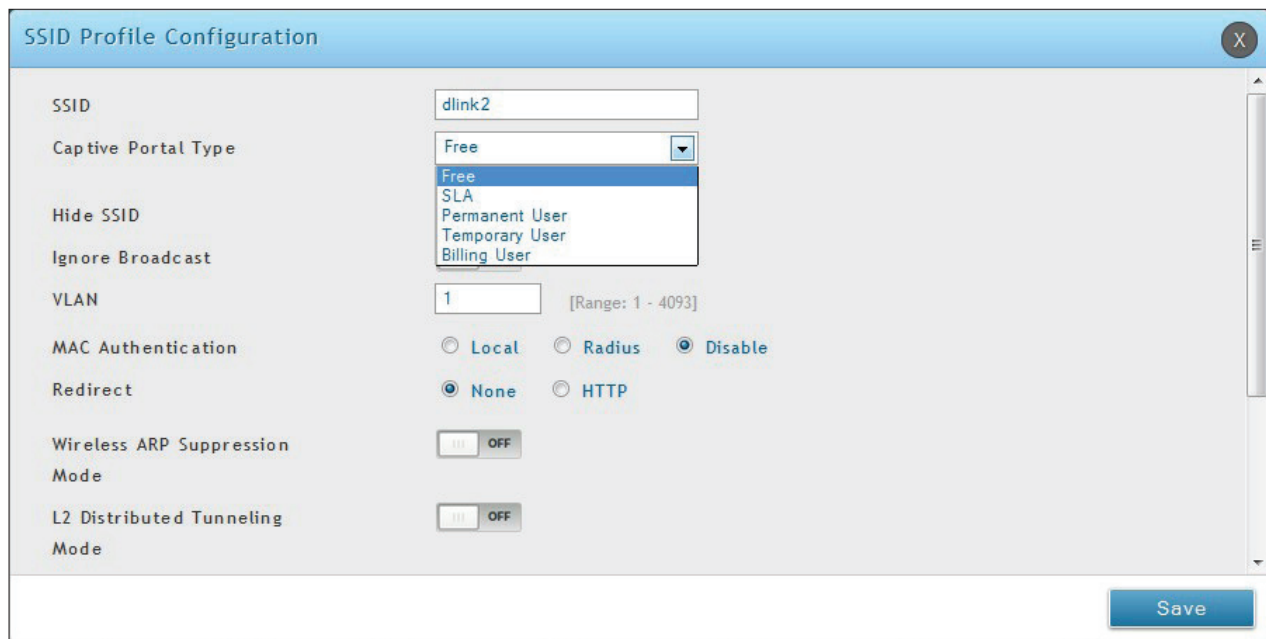
- c. Complete the fields in the table below and click **Save**.

| Field | Description |
|------------------------|---|
| User Name | Enter a unique name for this user. The name should allow you to easily identify this user from others you may add. |
| First Name | Enter the first name of the user. This is useful when the authentication domain is an external server, such as RADIUS. |
| Last Name | Enter the last name of the user. This is useful when the authentication domain is an external server, such as RADIUS. |
| Select Group | Select the captive portal group to which this user will belong. |
| Enable Password Change | This is the option for administrator to enable/ disable "change Password" link in Captive Portal page. |
| MultiLogin | More than one device can login with the same username/ password. |
| Password | Enter a case-sensitive password that the user must specify before gaining access to the Internet. For security, each typed password character is masked with a dot (•). |
| Confirm Password | Enter the same case-sensitive password entered in the Password field. For security, each typed password character is masked with a dot (•). |

3. Associate the captive portal group to a SSID Profile
 - a. Click **Wireless > Access Point > AP Profile > AP Profile SSID**.



- b. Under the SSID column, select an SSID that will use the Captive Portal function by right-clicking on it and clicking **Edit**. The following pop-up page will appear.



- c. Select a user type from the drop-down menu next to *Captive Portal Type*. Choosing **Free** will allow immediate access through the Captive Portal; choosing **SLA** will require the end user to agree to a service level agreement before being allowed access. Choosing **Permanent User** will allow for selecting an authentication method such as local user database, RADIUS, LDAP, or POP3. Choosing **Temporary User** or **Billing User** the authentication method is local user database.

In this case, the user account in the local database is a permanent user account. Select **Permanent User** on *Captive Portal Type* and select **Local User Database** on *Authentication Server*.

- d. Select the customized login page from the *Login Profile Name* drop-down menu.
- e. Click **Save**.

The captive portal is now associated to the selected SSID. To test your configuration from a client, connect to the captive portal SSID to log in to the captive portal. Enter an IP address on the captive portal network to see the controller redirect request to the captive portal page.

If the authentication database is using the RADIUS server, on step c above choose **Permanent User** on *Captive Portal Type* and select **RADIUS Server** on *Authentication Server*.

4. Customize the captive portal login page.

- a. Go to **Security > Authentication > Login Profiles**. The Login Profiles page will appear.

The screenshot shows the D-Link Unified Controller (DWC 2000) web interface. The top navigation bar includes tabs for Status, Wireless, Network, Security, and Maintenance. The Security tab is active, and the Login Profiles sub-tab is selected. The page displays a table with two login profiles: 'default' and 'default2', both with a status of 'Not In Use'. The interface includes a search bar and a 'System Search...' button at the top right. The bottom of the page shows a pagination bar indicating 'Showing 1 to 2 of 2 entries' and a 'First' button.

| Profile Name | Browser Title | Status |
|--------------|----------------------------|------------|
| default | D-link Wireless Controller | Not In Use |
| default2 | D-link Wireless Controller | Not In Use |

- 42

Save

- c. Complete the fields in the table below and click **Save**. The message *Operation Succeeded* will appear.

| Field | Description |
|--------------------------------|--|
| General Details | |
| Profile Name | Enter a name for this captive portal profile. The name should allow you to differentiate this captive profile from others you may set up. |
| Browser Title | Enter the text that will appear in the title of the browser during the captive portal session. |
| Background | Select whether the login page displayed during the captive portal session will show an image or color. Choices are: <ul style="list-style-type: none"> Image = displays an image as the background on the page. Use the Page Background Image field to select a background image. Color = sets the background color on the page. Select the color from the drop-down menu |
| Page Background Image | If you set <i>Background</i> to Image , upload the image file by clicking Add > Browse . Select an image, click Open and then click the Upload button. The maximum size of the image is 100 kb. |
| Page Background Color | If you set <i>Background</i> to Color , select the background color of the page that will appear during the captive portal session from the drop-down menu. |
| Custom Color | If you choose Custom on Page Background Color, enter the HTML color code. |
| Header Details | |
| Background | Select whether the login page displayed during the captive portal session will show an image or color. Choices are: <ul style="list-style-type: none"> Image = show image on the page. Use the Header Background Color field to select a background color. The maximum size of the image is 100 kb. Color = show background color on the page. Use the radio buttons to select an image. |
| Header Background Image | If you set <i>Background</i> to Image , upload the image file by clicking Add > Browse . Select an image, click Open and then click the Upload button. The maximum size of the image is 100 kb. |
| Header Background Color | If you set <i>Background</i> to Color , select the header color from the drop-down menu. |
| Custom Color | If you choose Custom on Page Background Color, you can choose particular color by filling in the HTML color code. |
| Header Caption | Enter the text that appears in the header of the login page during the captive portal session. |
| Caption Font | Select the font for the header text. |
| Font Size | Select the font size for the header text. |
| Font Color | Select the font color for the header text. |

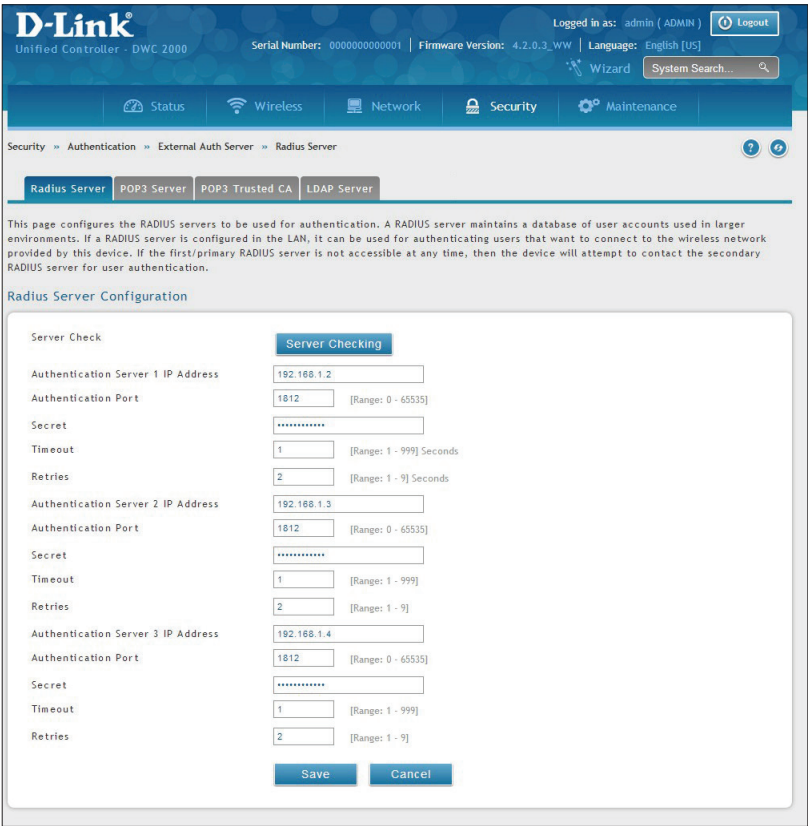
| Field | Description |
|------------------------------|--|
| Login Details | |
| Login Section Title | Enter the text that appears in the title of the login box when the user logs in to the captive portal session. This field is optional. |
| Welcome Message | Enter the welcome message that appears when users log in to the captive session successfully. This field is optional. |
| Error Message | Enter the error message that appears when users fail to log in to the captive session successfully. This field is optional. |
| Footer Details | |
| Change Footer Content | Enables or disables changes to the footer content on the login page. |
| Footer Content | If Change Footer Content is checked, enter the text that appears in the footer. |
| Footer Font Color | If Change Footer Content is checked, select the color of the text that appears in the footer. |

- d. Under *Login Profiles List*, right-click the profile and click **Show Preview** to view the profile you just configured. Confirm that the appearance of the login page suits your requirements. If not, repeat steps 4b and 4c as necessary.

Step #8: Use SSID with RADIUS Sever as Authenticator

To use SSID with RADIUS authentication, perform the following procedure.

- 1. Go to **Security > External Auth Server > RADIUS Server**.



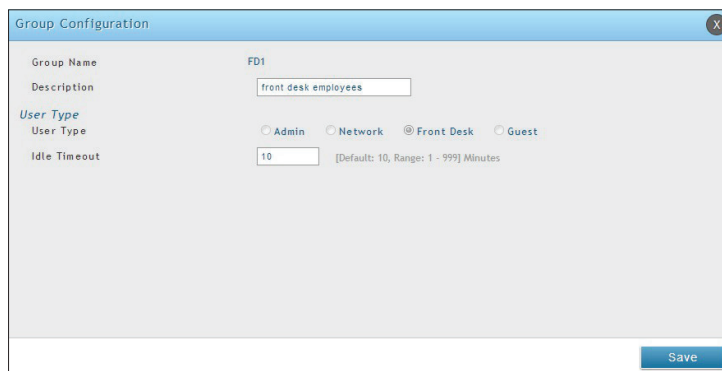
- 2. Complete the fields below and click **Save**. Your access point will be configured to use RADIUS authentication server.
- 3. Click **Server Checking** to test the connection between the DWC-2000 and your RADIUS server.

| Field | Description |
|----------------------------------|--|
| Server Checking | Click to test the connection between the controller and your RADIUS server. |
| Authentication Server IP Address | IP address of your RADIUS authentication server. |
| Authentication Port | RADIUS authentication port number to send RADIUS messages. |
| Secret | Enter the secret key that allows the device to log into the configured RADIUS server. It must match the secret on RADIUS server. |
| Timeout | Set the timeout in seconds. The controller should wait for a response from the RADIUS server. |
| Retries | The number of tries the controller will make to the RADIUS server before giving up. |

Step #9: Configure Guest Management

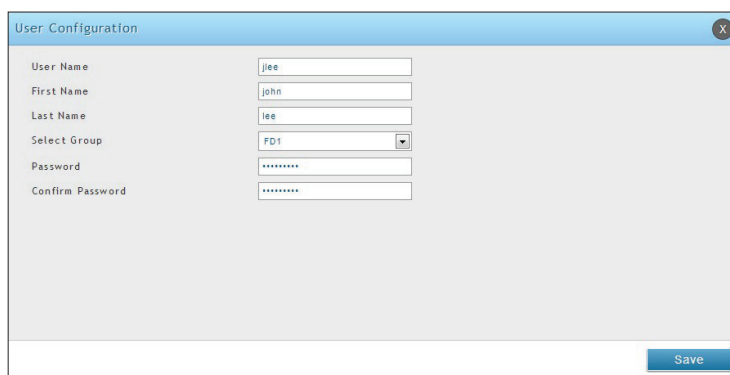
The wireless controller can generate temporary guest accounts from front desk manage accounts. To configure guest management, perform the following procedure.

1. Create a front desk group.
 - a. Go to **Security > Authentication > User Database > Groups**. The Groups List page will appear.
 - b. Click **Add New Group**. The Group Configuration page will appear.
 - c. Fill in group name and description, and select **Front Desk** on User Type.



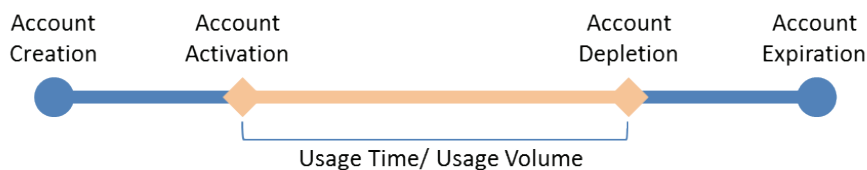
The Group Configuration dialog box is shown. It has a title bar with a close button (X). The fields are: Group Name (FD1), Description (front desk employees), User Type (radio buttons for Admin, Network, Front Desk (selected), Guest), and Idle Timeout (10). A note below the Idle Timeout field says "[Default: 10, Range: 1 - 999] Minutes". A Save button is at the bottom right.

2. Add front desk users.
 - a. Go to **Security > Authentication > User Database > Users**. The Users List will appear.
 - b. Click **Add New User**. The User Configuration page will appear.
 - c. Complete the fields and select the front desk group you created in the previous step on Selected Group.



The User Configuration dialog box is shown. It has a title bar with a close button (X). The fields are: User Name (jee), First Name (john), Last Name (lee), Select Group (FD1), Password (masked with asterisks), and Confirm Password (masked with asterisks). A Save button is at the bottom right.

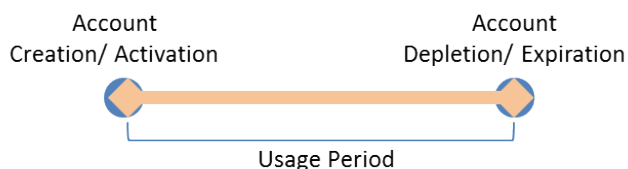
3. Create a billing profile.
 - a. Go to **Security > Authentication > Billing Profile**. Click **Add New Billing Profile**.
 - b. The billing profile settings include four milestones by timeline:



- Account Creation: the temporary account is generated by front desk account in the local database.
- Account Activation: the temporary account is activated and it is valid for use.
- Account Depletion: the temporary account is run out usage time or usage volume.
- Account Expiration: the temporary account is expired no matter usage time/ volume running out or not, and it is removed from the local database.

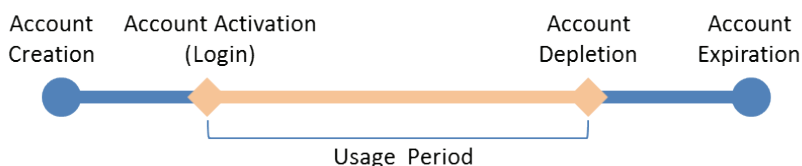
Below are five most common types of billing profiles:

- I. The temporary account usage time is limited by duration. The account has the expiration time. The account is valid while the account is created.



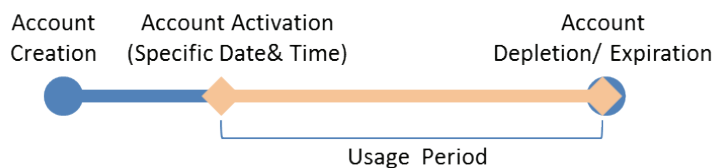
This billing profile is suitable for the scenario in Hotel. The temporary account is created and valid while customers check-in.

- II. The temporary account usage time is limited by duration. The account has the expiration time. The account is valid while the account first logs in.



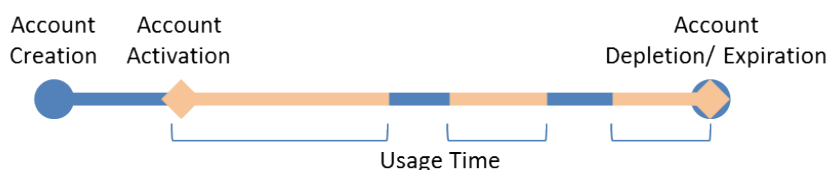
This billing profile is suitable for the scenario in Coffee Shop, Airport, etc. The customer can use wireless internet service for a period of time counting from first time logs in.

III. The temporary account is valid with specific date and time. The account has the expiration time.



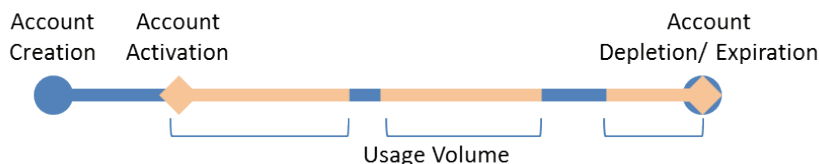
This billing profile is suitable for the scenario in Press Conference. The organizer generates accounts before the event and delivery account information to participator in advanced if necessary. The temporary account would be only valid from specific date and time.

IV. The temporary account has limited time usage. The account doesn't have the expiration time until the usage is run out.



This billing profile is suitable for the scenario in Hotspot. The service provider charge the wireless service based on usage time. This account allows multiple devices log in at the same time.

V. The temporary account has limited usage traffic. The account doesn't have the expiration time until the usage is run out.



This billing profile is suitable for a Hotspot scenario. The service provider charge the wireless service based on usage volume.

c. Complete the fields below:

The screenshot shows a web-based configuration window titled 'Captive Portal Billing Profile Configuration'. It contains several sections with input fields and checkboxes:

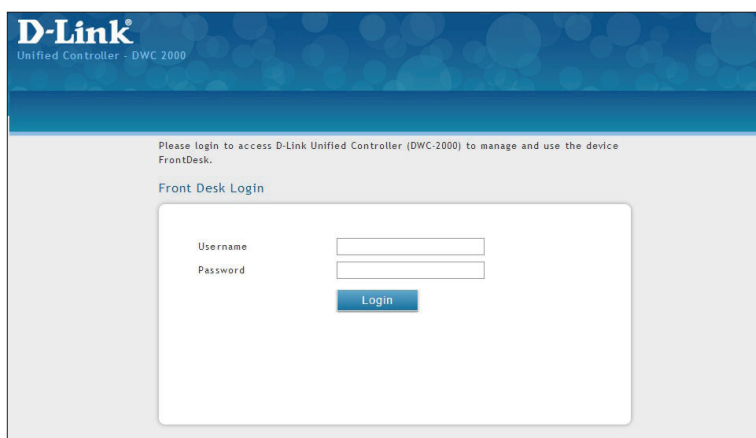
- Profile Details:**
 - Profile Name: [Text input field]
 - Profile Description: [Text input field]
 - Allow Multiple Login: ☐ OFF
 - Allow Customized account on Front Desk: ☐ OFF
 - Allow batch generation on Front Desk: ☐ OFF
 - Session Idle Timeout: [Text input field] [Default: 10, Range: 1 - 60] Minutes
 - Show alert message on login page while rest of usage time/traffic under: [Text input field] Hour
- Basic Limit by Duration:** Valid with Begin and End time. ☐ OFF
- Basic limit by usage:**
 - Maximum Usage Time: ☐ OFF
 - Maximum Usage Traffic: ☐ OFF
- Unit Price:** Set Price: ☐ OFF

A 'Save' button is located at the bottom right of the window.

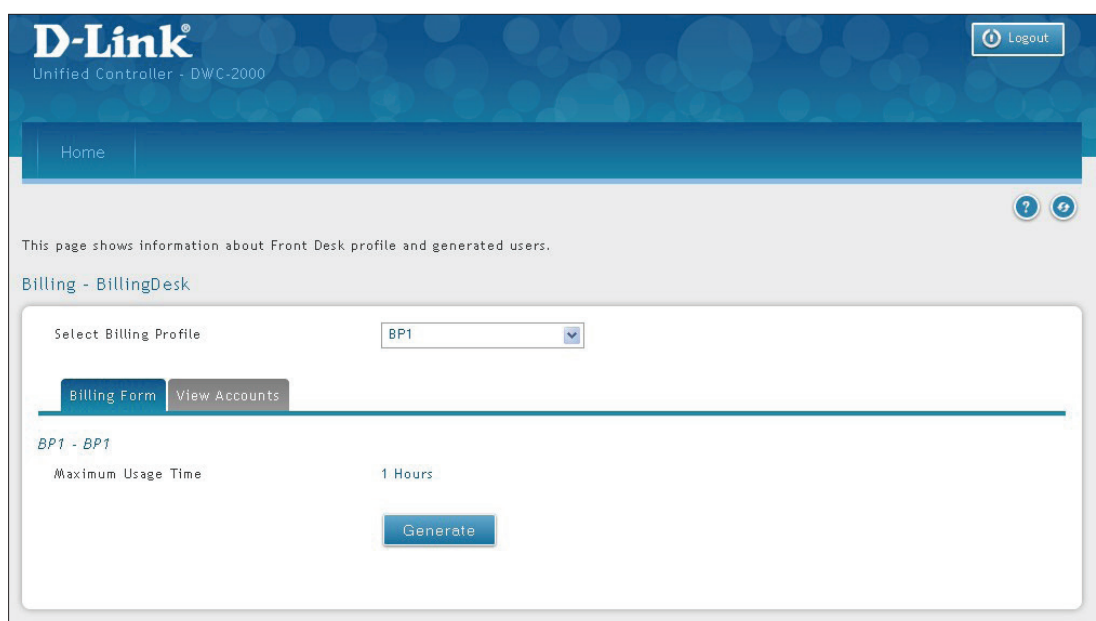
| Field | Description |
|--|--|
| Profile Details | |
| Profile Name | Each profile will be having a profile Name to identify itself. |
| Profile Description | This is the description of the profile |
| Allow Multiple Login | Checking this option will allow multiple users to use same captive portal login credentials created for this profile to login simultaneously. |
| Allow Customized Account on Front Desk | Checking this option enables front desk user to give customized account name to the captive portal users being created on this profile. |
| Allow Batch Generation on Front Desk | Checking this option enables front desk user to generate a batch of temporary captive portal users at one click. |
| Session Idle Timeout | Idle timeout for CP users generated for this profile. |
| Show Alert Message on Login Page while Rest of Usage Time/Traffic Under | Enter a value here in Hours/Days/MB/GB to get an alert message when usage time/traffic left reaches the desired limit. By default if 0 is entered it implies no alert message is required. |
| Basic Limit by Duration | |
| Valid with Begin and End Time | Limitations on Duration basis |
| Valid Begin | <p>If you enable <i>Valid with Begin and End Time</i>, There are 3 types of limiting user access by duration:</p> <ol style="list-style-type: none"> 1. Start While Account Created: Activate account when user is created 2. Start While Account Login: Activate account when user first login using his credentials. 3. Begin From: Activate account from this date |
| Start While Account Created | If you select <i>Start While Account Created</i> , enter a value in Hours/Days to set duration of usage time. |
| Start While Account Login | If you select <i>Start While Account Login</i> , enter a value in Hours/Days to set duration of usage time. |
| Begin From | If you choose <i>Begin From</i> , select a specific time and date for the account valid begin. |
| Allow Front Desk to Modify Duration | If you enable <i>Valid with Begin and End Time</i> , checking this option enables the front desk user to modify duration limits. |
| Basic Limit by Usage | |
| Maximum Usage Time | Maximum time user can stay login before his account expires. |
| Maximum Usage Traffic | Maximum traffic user can use before his account expires. Only inbound traffic shall be considered towards bandwidth usage. |
| Allow Front Desk to Modify Usage | If you enable <i>Maximum Usage Time</i> or <i>Maximum Usage Traffic</i> , checking this option enables the front desk user to modify usage limits. |

4. Select an Interface for the guest captive portal.
 - a. Click **Wireless > Access Point > SSID Profiles**. The SSID Profile List page will appear.
 - b. Under the SSID column, select an SSID that will use the Captive Portal function by right-clicking on it and clicking **Edit**.
 - c. Select a Captive Portal Type from the drop-down menu.
 - d. Click **Save**.

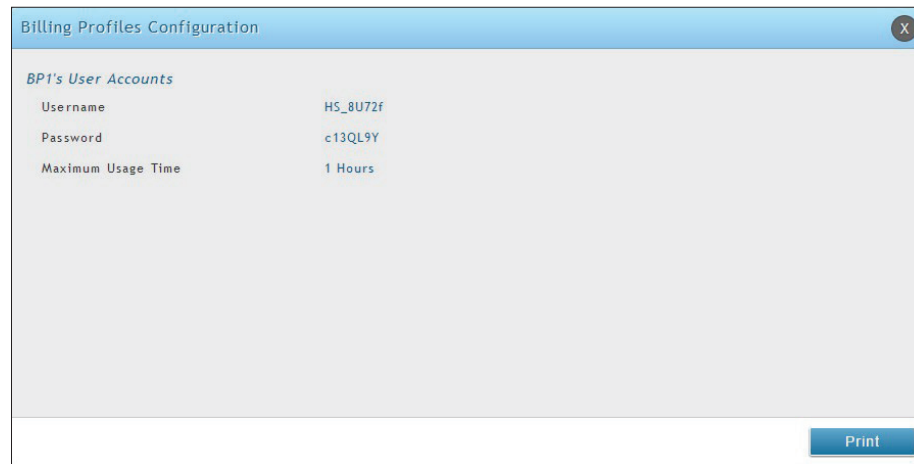
Note: Apply AP Profile from Wireless > Access Point > AP Profiles if the SSID have been associated with a used AP Profile to change the configuration.
5. Generate guest accounts.
 - a. Log in to the Front Desk page by entering the Front Desk page URL. This can be: **http://<ip_address>/frontdesk** (e.g.: **http://192.168.10.1/frontdesk**), or **http://<ip_address>/platform.cgi?page=billingDeskLogin.html**. Enter the username and password of a user in the "Front Desk" group.



- b. Select a billing profile. Modify the usage if you want. Click **Generate**.

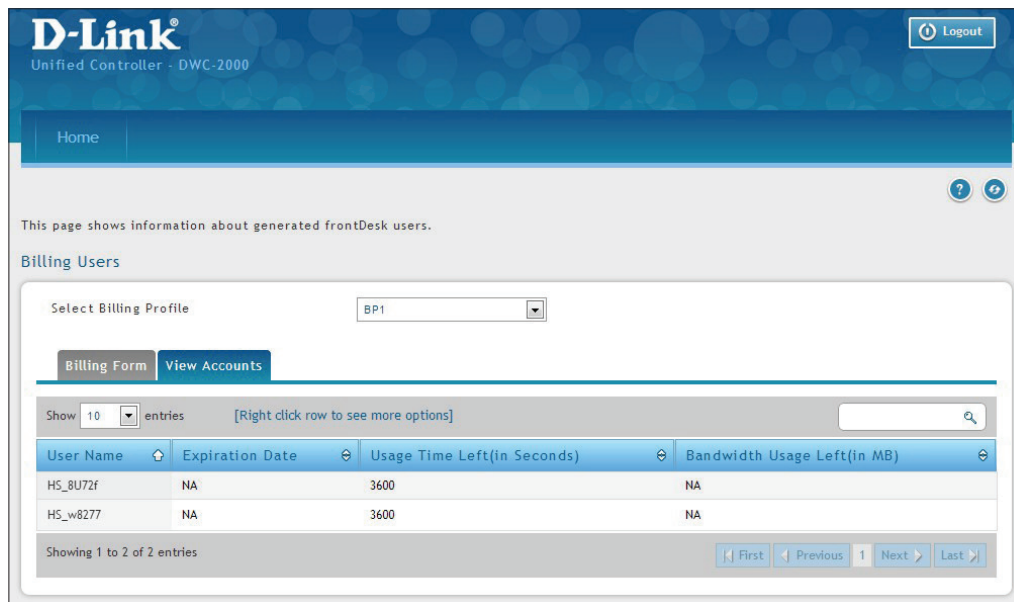


- c. Print out the account information by clicking **Print**. The information would send to the internet printer. Only one user account can be created at a time.

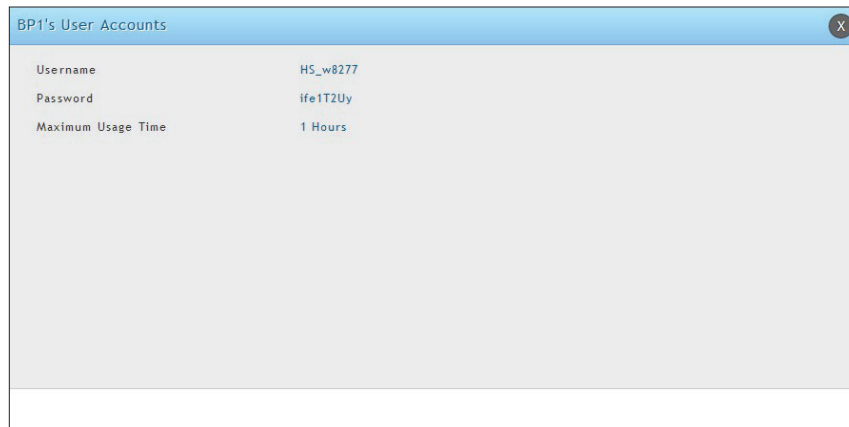


6. Monitor user account status.

- a. Monitor temporary account status and extend account usage duration or volume. Click **View Account** for reviewing generated temporary status.



- b. Select an account and right-click **View Details** to view more information.



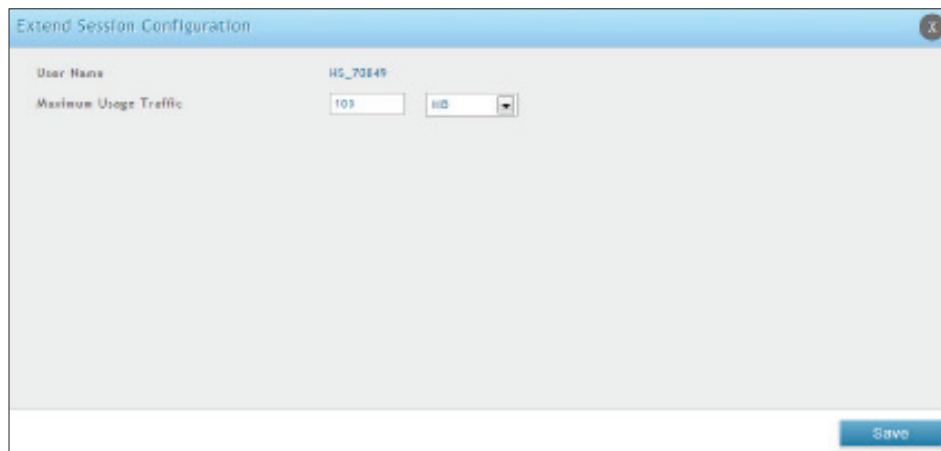
The screenshot shows a window titled "BP1's User Accounts" with a close button (X) in the top right corner. The window displays the following details for a user account:

| | |
|--------------------|----------|
| Username | HS_w8277 |
| Password | ife1T2Uy |
| Maximum Usage Time | 1 Hours |

7. Extend user account usage.
 - a. Select an account and right-click **Extend Session**. Manually change the usage time/traffic.

Note: Make sure that **Allow Front Desk to Modify Usage** is turned on in the "Captive Portal Billing Profile Configuration" page.

- b. Click **Save**.



The screenshot shows a window titled "Extend Session Configuration" with a close button (X) in the top right corner. The window displays the following configuration options:

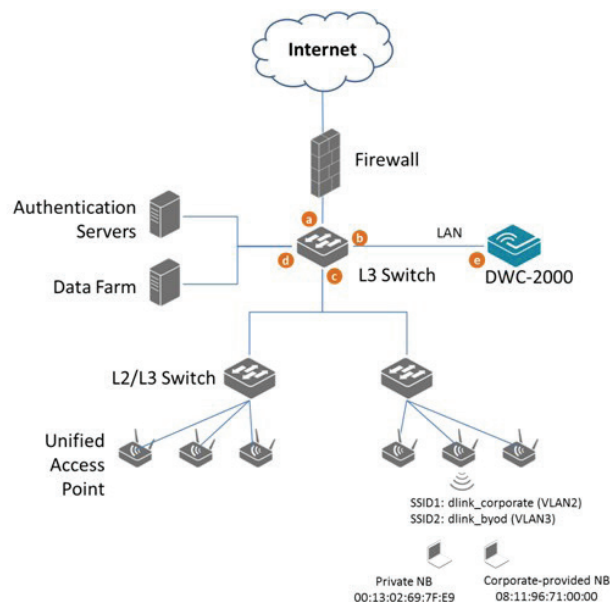
| | | |
|-----------------------|----------|----|
| User Name | HS_73849 | |
| Maximum Usage Traffic | 100 | MB |

A "Save" button is located at the bottom right of the window.

Step #10: Configure a BYOD Environment

The trend of Bring Your Own Device (BYOD) in the work place is a new challenge on network security and management. Many corporations that allow employees to use their own devices at work expect to have better performance and productivity; however, on the downside, corporations also are concerned with network security and information leakage by using private devices. How to distinguish between corporate-provided devices and private devices (BYOD device) is a major task for IT teams.

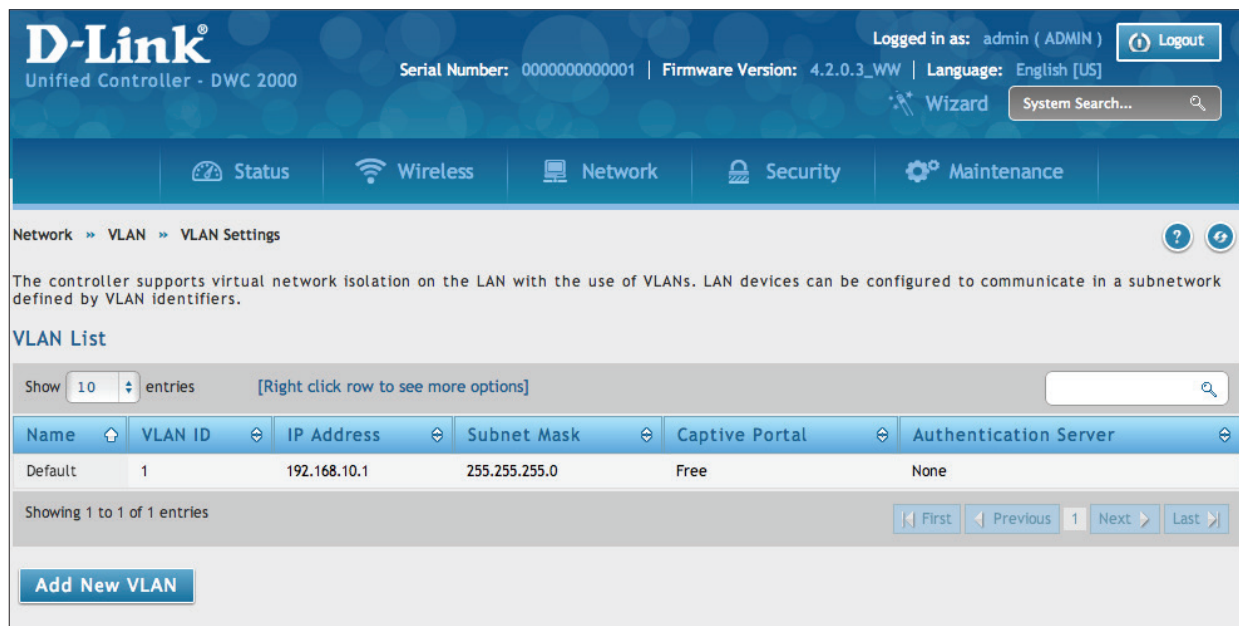
Use device MAC authentication to enforce client associating specific SSIDs based on the device which is corporate-provided or private. All connectivity from SSIDs required performing authentication before granted authority. To configure a BYOD environment, perform the following procedures:



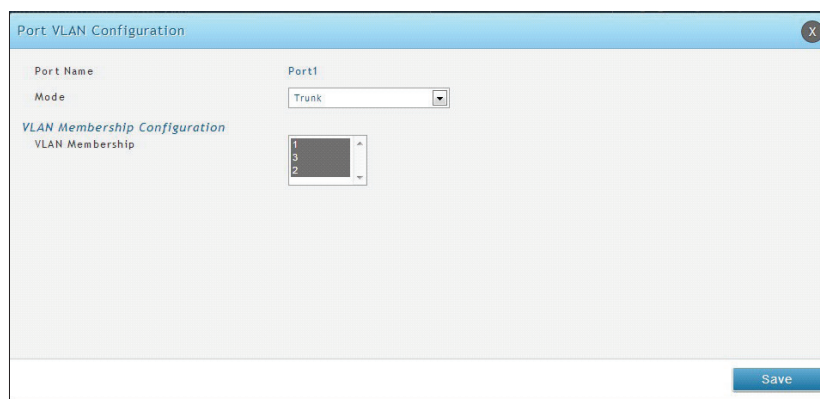
The authentication methods on each SSID are difference:

- **dlink_corporate SSID:** This SSID is for D-Link employees who works with cooperate-provided drives. It requires device MAC authentication and Captive Portal to complete the authentication process.
- **dlink_byod SSID:** This SSID is for D-Link employees who work with his/her private drive (BYOD device). It requires Captive Portal to complete the authentication process.

1. Set up VLANs based on the network architecture. Create three VLANs. VLAN1 is the default VLAN for AP management, VLAN2 is for the traffic associated from SSID dlink_corporate, and VLAN3 is for the traffic associated from SSID dlink_byod. Associate VLAN 1 to 3 memberships on Port1.
 - a. Go to **Network > VLAN > VLAN Settings**. The VLAN List will appear.
 - b. Click **Add New VLAN**. The VLAN Configuration page will appear.
 - c. Enter a VLAN ID and name.
 - d. Enter the IP range for your VLAN.



2. Associate VLAN 1 to three memberships in Trunk mode on Port1.
 - a. Go to **Network > VLAN > Port VLAN**.
 - b. Right-click port 1 and click **Edit**. Select **Trunk** from the *Mode* drop-down menu and then select VLAN1 to VLAN3 (hold CTRL and click 1, 2, and 3) next to *VLAN Membership*.
 - c. Click **Save**.



3. Create two SSIDs: **dlink_corporate** and **dlink_byod**, and assign VLAN 2 and 3 on these two SSIDs respectively. Enable MAC authentication on SSID dlink_corporate.
 - a. Go to **Wireless > Access Point > SSID Profiles**. The SSID Profile List will appear.
 - b. Click **Add New SSID Profile**. Create "SSID dlink_corporate" and "dlink byod".
 - c. Enable Captive Portal on both SSIDs and select the *Captive Portal Type* as **Permanent User**.
 - d. Select the Authentication Server. The authentication server can be either local database or external authentication sever (i.e., RADIUS).
 - e. Assign VLAN2 and VLAN3 to "dlink_corporate" and "dlink_byod" respectively.
 - f. Enable MAC authentication on "dlink_corporate".
 - g. Click **Save**.

The screenshot shows the 'SSID Profile Configuration' window for the SSID 'dlink_corporate'. The 'Captive Portal Type' is set to 'Permanent User'. Under 'Captive Portal Authentication Configuration', the 'Authentication Server' is 'Local User Database' and the 'Login Profile Name' is 'default'. The 'VLAN' is set to '2'. 'MAC Authentication' is set to 'Local'. 'Redirect' is set to 'None'. 'Wireless ARP Suppression' is 'OFF'. A 'Save' button is at the bottom right.

| | |
|--|---|
| SSID | dlink_corporate |
| Captive Portal Type | Permanent User |
| Captive Portal Authentication Configuration | |
| Authentication Server | Local User Database |
| Login Profile Name | default |
| Hide SSID | OFF |
| Ignore Broadcast | OFF |
| VLAN | 2 [Range: 1 - 4093] |
| MAC Authentication | <input checked="" type="radio"/> Local <input type="radio"/> Radius <input type="radio"/> Disable |
| Redirect | <input checked="" type="radio"/> None <input type="radio"/> HTTP |
| Wireless ARP Suppression | OFF |

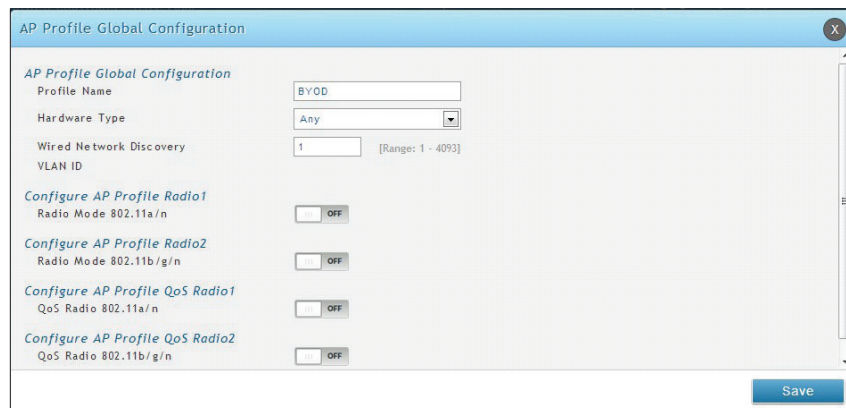
Save

The screenshot shows the 'SSID Profile Configuration' window for the SSID 'dlink_byod'. The 'Captive Portal Type' is set to 'Permanent User'. Under 'Captive Portal Authentication Configuration', the 'Authentication Server' is 'Local User Database' and the 'Login Profile Name' is 'default'. The 'VLAN' is set to '3'. 'MAC Authentication' is set to 'Disable'. 'Redirect' is set to 'None'. 'Wireless ARP Suppression' is 'OFF'. A 'Save' button is at the bottom right.

| | |
|--|---|
| SSID | dlink_byod |
| Captive Portal Type | Permanent User |
| Captive Portal Authentication Configuration | |
| Authentication Server | Local User Database |
| Login Profile Name | default |
| Hide SSID | OFF |
| Ignore Broadcast | OFF |
| VLAN | 3 [Range: 1 - 4093] |
| MAC Authentication | <input type="radio"/> Local <input type="radio"/> Radius <input checked="" type="radio"/> Disable |
| Redirect | <input checked="" type="radio"/> None <input type="radio"/> HTTP |
| Wireless ARP Suppression | OFF |

Save

4. Create an AP Profile "BYOD". Associate SSIDs on this profile.
 - a. Go to **Wireless > Access Point > AP Profile**.
 - b. Click **Add New AP Profile**. Create a profile called **BYOD**.
 - c. Click **Save**.



AP Profile Global Configuration

AP Profile Global Configuration

Profile Name: BYOD

Hardware Type: Any

Wired Network Discovery: 1 [Range: 1 - 4093]

VLAN ID: 1

Configure AP Profile Radio1
Radio Mode 802.11a/n: OFF

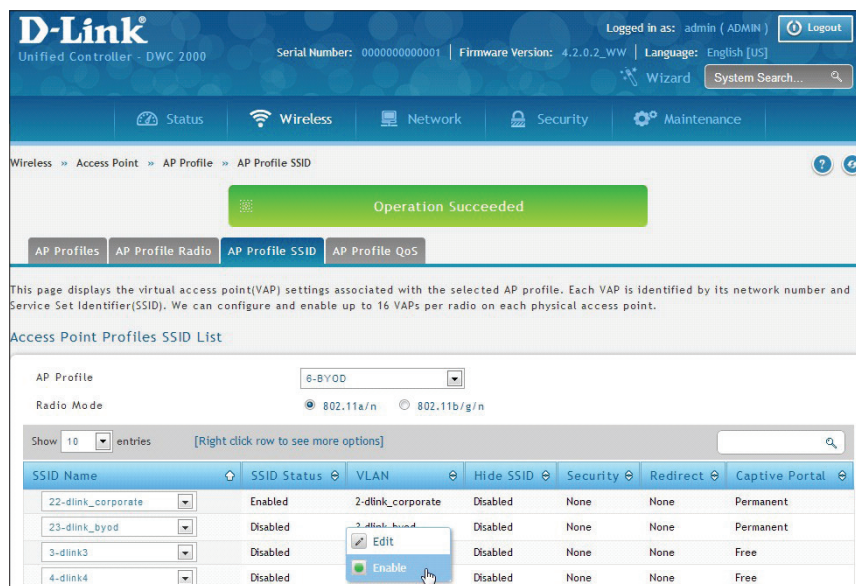
Configure AP Profile Radio2
Radio Mode 802.11b/g/n: OFF

Configure AP Profile QoS Radio1
QoS Radio 802.11a/n: OFF

Configure AP Profile QoS Radio2
QoS Radio 802.11b/g/n: OFF

Save

- d. Click the **AP Profile SSID** tab. Next to *AP Profile*, make sure **BYOD** is selected.
- e. In the SSID list, right-click the **dlink_corporate** row and select **Enable**.
- f. Right-click the **dlink_byod** row and select **Enable**.
- g. Both SSIDs are now associated with the BYOD SSID profile.



D-Link Unified Controller - DWC 2000

Serial Number: 00000000000001 | Firmware Version: 4.2.0.2_WW | Language: English [US]

Logged in as: admin (ADMIN) | Logout

Wizard | System Search...

Status | Wireless | Network | Security | Maintenance

Wireless > Access Point > AP Profile > AP Profile SSID

Operation Succeeded

AP Profiles | AP Profile Radio | AP Profile SSID | AP Profile QoS

This page displays the virtual access point(VAP) settings associated with the selected AP profile. Each VAP is identified by its network number and Service Set Identifier(SSID). We can configure and enable up to 16 VAPs per radio on each physical access point.

Access Point Profiles SSID List

AP Profile: 8-BYOD

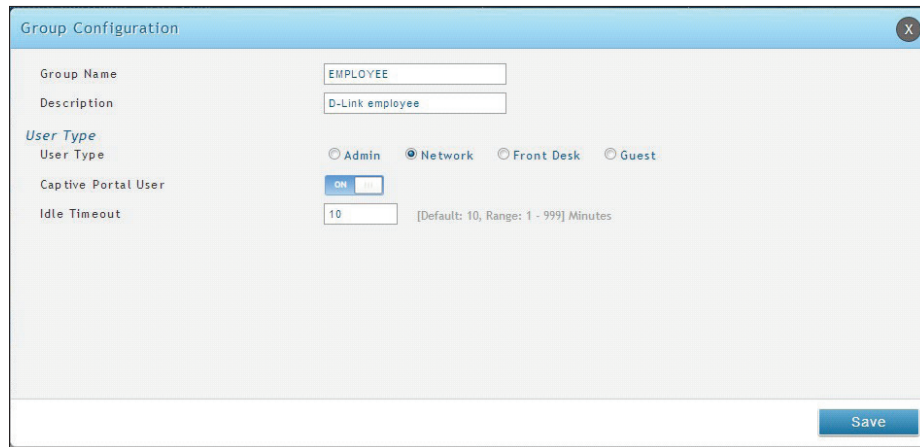
Radio Mode: 802.11a/n (selected) 802.11b/g/n

Show 10 entries [Right click row to see more options]

| SSID Name | SSID Status | VLAN | Hide SSID | Security | Redirect | Captive Portal |
|--------------------|-------------|-------------------|-----------|----------|----------|----------------|
| 22-dlink_corporate | Enabled | 2-dlink_corporate | Disabled | None | None | Permanent |
| 23-dlink_byod | Disabled | 3-dlink_byod | Disabled | None | None | Permanent |
| 3-dlink3 | Disabled | | Disabled | None | None | Free |
| 4-dlink4 | Disabled | | Disabled | None | None | Free |

Right-click context menu options: Edit, Enable

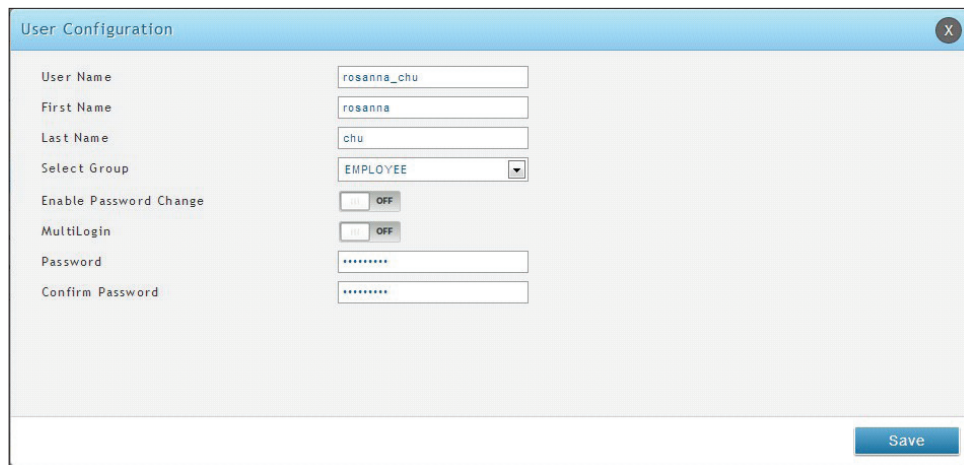
5. Create *Captive Portal* accounts on the local database.
 - a. To create a user group, go to **Security > Authentication > User Database > Group** tab.
 - b. Click **Add New Group**. Create a group called "EMPLOYEE". Next to *User Type* select **Network**, and toggle *Captive Portal User* to **On**. Enter an Idle Timeout value (in minutes).
 - c. Click **Save**.



The 'Group Configuration' dialog box is shown. It has a title bar with a close button (X). The form contains the following fields and controls:

- Group Name:** Text input field containing 'EMPLOYEE'.
- Description:** Text input field containing 'D-Link employee'.
- User Type:** Section with four radio buttons: ☐ Admin, ☒ Network, ☐ Front Desk, ☐ Guest.
- Captive Portal User:** Toggle switch set to 'ON'.
- Idle Timeout:** Text input field containing '10'. To its right is the text '[Default: 10, Range: 1 - 999] Minutes'.
- Save:** A blue button at the bottom right.

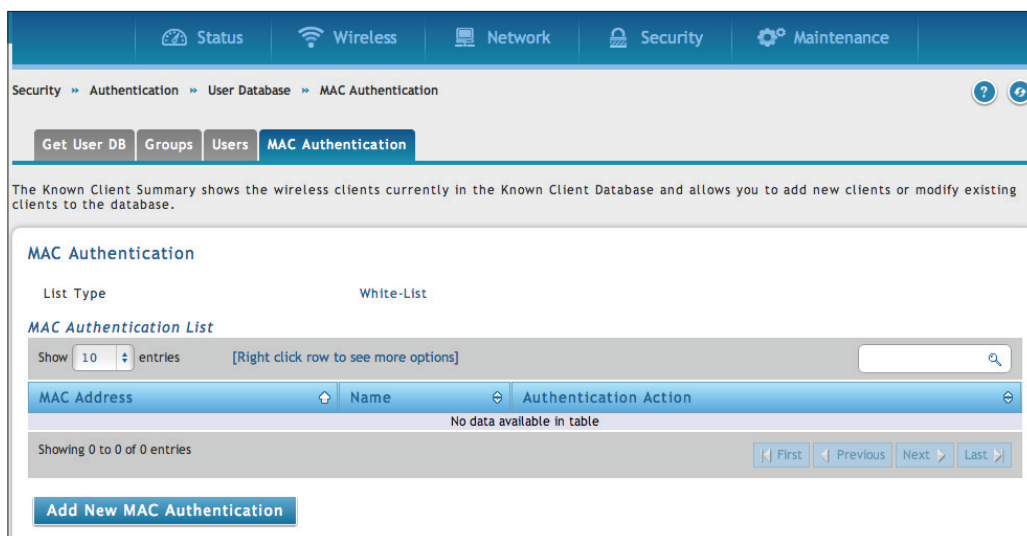
- d. Create user accounts. Go to **Security > Authentication > User Database > Users** tab.
 - e. Click **Add New User** to create user accounts. Fill in the fields and select EMPLOYEE next to *Select Group*.
 - f. Click **Save**.



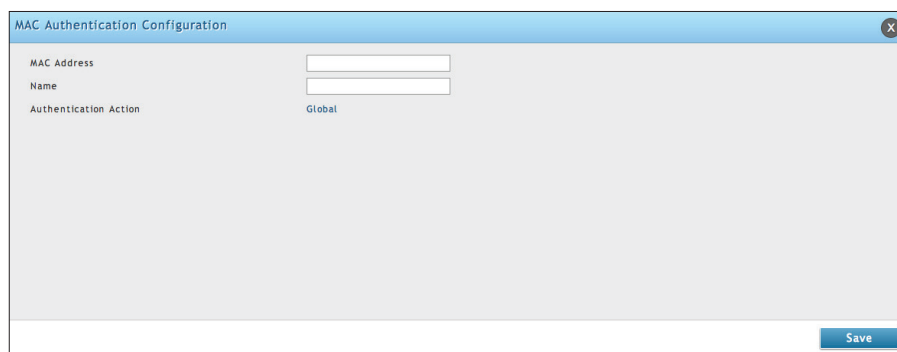
The 'User Configuration' dialog box is shown. It has a title bar with a close button (X). The form contains the following fields and controls:

- User Name:** Text input field containing 'rosanna_chu'.
- First Name:** Text input field containing 'rosanna'.
- Last Name:** Text input field containing 'chu'.
- Select Group:** Dropdown menu showing 'EMPLOYEE'.
- Enable Password Change:** Toggle switch set to 'OFF'.
- MultiLogin:** Toggle switch set to 'OFF'.
- Password:** Password input field (masked with asterisks).
- Confirm Password:** Password input field (masked with asterisks).
- Save:** A blue button at the bottom right.

6. Create device MAC authentication database on local database.
 - a. Go to **Security > Authentication > User Database > MAC Authentication** tab.
 - b. Next to *List Type*, the current type is displayed. To change the setting, refer to “Step #5: Select MAC Authentication Mode” on page 34.



- c. Click **Add New MAC Authentication**. Enter the MAC address of the device and a name.
 - d. Click **Save**.



Note: If the user authentication and MAC authentication database is external authentication server (i.e., RADIUS), please refer to “Step #8: Use SSID with RADIUS Sever as Authenticator” on page 45.

7. Discover and manage an access point from the network. Please refer to “Step #3: Select APs to be Managed” on page 27.

Where to Go from Here

After installing the basic configuration procedures, the wireless controller is ready for operation using the factory default settings in Appendix B. These settings should be suitable for most users and most situations.

The wireless controller also provides advanced configuration settings for users who want to take advantage of the more advanced features of the wireless controller. The following sections list the wireless controller's advanced settings. Users who do not understand these features should not attempt to reconfigure their wireless controller, unless advised to do so by the technical support staff.

Advanced WLAN Configuration

While the basic configuration described in the previous chapter is satisfactory for most users, large wireless networks or a complex setup may require the wireless controller's advanced configuration settings to be configured.

This chapter covers the following commonly used advanced wireless configuration settings.

- "WLAN General Settings" on page 61
- "Channel Plan and Power Settings" on page 64
- "WIDS" on page 67
- "Distributed Tunnel" on page 72
- "WLAN Visualization" on page 73
- "AP Discovery Methods" on page 75
- "Managed APs" on page 78
- "AP Profiles" on page 85
- "SSID Profiles" on page 98
- "Wireless Distribution System (WDS)" on page 102
- "Peer Group" on page 108
- "AP Firmware Download" on page 110

Note: *The procedures in this chapter should only be performed by expert users who understand networking concepts and terminology.*

WLAN General Settings

The WLAN General Configuration page contains the global configuration settings for all managed APs and the wireless controller including WLAN Global Setup, AP Validation, and Country Configuration.

Path: Wireless > General > General

To configure the WLAN general settings:

1. Click **Wireless > General > General**. The WLAN General Settings page will appear.

Unified Controller - DWC 2000

Serial Number: 0000000000001

Firmware Version: 4.2.0.3_WW

Language: English [US]

Logged in as: admin (ADMIN)

Logout

Wizard

System Search...

Status

Wireless

Network

Security

Maintenance

Wireless » General

This page will guide you through common and easy steps to configure your DWC-2000 controller WLAN global settings. Make sure that WLAN controller is being enabled for working of wireless functionality.

General Setting

WLAN Global Setup

IP Address

192.168.10.1

Peer Group ID

1

[Default: 1, Range: 1 - 255]

Client Roam Timeout

30

[Range: 1 - 120] Seconds

Ad Hoc Client Status Timeout

24

[Range: 0 - 168] Hours

AP Failure Status Timeout

24

[Range: 0 - 168] Hours

Client MAC Authentication Mode

☒ White-list
 ☐ Black-list

RF Scan Status Timeout

24

[Range: 0 - 168] Hours

Detected Clients Status Timeout

24

[Range: 0 - 168] Hours

Tunnel IP MTU Size

☒ 1500
 ☐ 1520

Cluster Priority

1

[Range: 0 - 255]

AP Client QoS

☐ ON
 ☒ OFF

AP Validation

AP MAC Validation

☒ Local
 ☐ Radius

Require Authentication Passphrase

☐ ON
 ☒ OFF

Manage AP with Previous Release Code

☐ ON
 ☒ OFF

Country Configuration

Country Code

US - United States

Save

Cancel

2. Complete the fields in the table on the next page.
3. Click **Save**.

| Field | Description |
|---------------------------------|--|
| WLAN Global Setup | |
| IP Address | Displays the current IP address of the wireless controller. |
| Peer Group ID | In order to support larger networks, you can configure wireless controllers as peers, with up to eight controllers in a cluster (peer group). Peer controllers share some information about APs and allow L3 roaming among them. Peers are grouped according to the group ID. |
| Client Roam Timeout | This value determines how long to keep an entry in the Associated Client Status list after a client has disassociated. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted. |
| Ad Hoc Client Status Timeout | This value determines how long to keep an entry in the Ad Hoc Client Status list. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted. |
| AP Failure Status Timeout | This value determines how long to keep an entry in the Ad Failure Client Status list. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted. |
| Client MAC Authentication | Select either White-list or Black-list . |
| RF Scan Status Timeout | This value determines how long to keep an entry in the RF Scan Status list. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted. |
| Detected Clients Status Timeout | This value determines how long to keep an entry in the Detected Client Status list. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted. |
| Tunnel IP MTU Size | <p>Select the maximum size of an IP packet handled by the network. The MTU is enforced only on tunneled VAPs. When IP packets are tunneled between the APs and the wireless controller, the packet size is increased by 20 bytes during transit. This means that clients configured for 1500 byte IP MTU size may exceed the maximum MTU size of existing network infrastructure which is set up to switch and route 1518 (1522-tagged) byte frames. If you increase the tunnel IP MTU size, you must also increase the physical MTU of the ports on which the traffic flows.</p> <p>Note: if any of the following conditions are true, you do not need to increase the tunnel IP MTU size:</p> <ul style="list-style-type: none"> • The wireless network does not use L3 tunneling. • The tunneling mode is used only for voice traffic, which typically has small packets. • The tunneling mode is used only for TCP based protocols, such as HTTP. This is because the AP automatically reduces the maximum segment size for all TCP connections to fit within the tunnel. |
| Cluster Priority | Specify the priority of this controller for the Cluster Controller election. The wireless controller with highest priority in a cluster becomes the Cluster Controller. If the priority is the same for all wireless controllers, then the wireless controller with lowest IP address becomes the Cluster Controller. A priority of 0 means that the wireless controller cannot become the Cluster Controller. The highest possible priority is 255. |
| AP Client QoS | <p>Enable or disable the client QoS feature. If AP Client QoS is disabled, the Client QoS configuration remains in place, but any ACLs or DiffServ policies applied to wireless traffic are not enforced.</p> <p>The Client QoS feature extends the primary QoS capabilities of the wireless controller to the wireless domain. More specifically, access control lists (ACLs) and differentiated service (DiffServ) policies are applied to wireless clients associated to the AP</p> |

| Field | Description |
|---|--|
| AP Validation | |
| AP MAC Validation | <p>For a wireless controller to manage an AP, you must add the MAC address of the AP to the Valid AP database, which can be kept locally on the controller or in an external RADIUS server. When the controller discovers an AP that is not managed by another wireless controller, it looks up the MAC address of the AP in the Valid AP database. If it finds the MAC address in the database, the controller validates the AP and assumes management.</p> <p>Select the database to use for AP validation. Choices are:</p> <ul style="list-style-type: none"> Local: Add the MAC address of each AP to the local Valid AP database. RADIUS: Configure the MAC address of each AP in an external RADIUS server. |
| Require Authentication Passphrase | <p>Select this option to require APs to be authenticated before they can associate with the controller. If you select this option, you must configure the passphrase on the AP while it is in standalone mode as well as in the Valid AP database. To configure the pass phrase on a standalone AP, log onto the AP Administration Web UI and go to the Managed Access Point page, or log onto the AP CLI and use the set managed-ap pass-phrase command.</p> <p>To configure the passphrase for an AP in the local Valid AP database, click the Valid AP page from the Basic Setup page. Then, click the MAC address of the AP and enter the passphrase in the Authentication Password field. If you enable authentication, it takes place immediately after the controller validates the AP.</p> |
| Manage AP with Previous Release Code | Discover and manage APs with older firmware. |
| Country Configuration | |
| Country Code | <p>Select the country code that represents the country where your controller and APs operate. When you click Submit, a pop-up message asks you to confirm the change. Wireless regulations vary from country to country. Make sure you select the correct country code so that your WLAN system complies with the regulations in your country.</p> |

Channel Plan and Power Settings

The wireless controller software contains a channel plan algorithm that automatically determines which RF channels each AP should use to minimize RF interference. When you enable the channel plan algorithm, the wireless controller periodically evaluates the operational channel on every AP it manages and changes the channel if the current channel is noisy.

Configure Channel Plan

Path: Wireless > General > Channel Algorithm

To configure Channel Algorithm setting:

1. Click **Wireless > General > Channel Algorithm > Channel Setting** tab. The Channel Setting page will appear.

The screenshot shows the D-Link Unified Controller - DWC 2000 web interface. The top navigation bar includes links for Status, Wireless, Network, Security, and Maintenance. The main content area is titled "Wireless >> General >> Channel Algorithm >> Channel Algorithm 5 GHz". Below this, there are three tabs: "Channel Setting" (selected), "Manual Channel Plan", and "Channel Plan History". A message states: "Through this page we can configure AP frequency related parameters for 5 GHz radio channel." Below this message are two tabs: "5 GHz" (selected) and "2.4 GHz". The "RF Channel 5 GHz Settings" section contains the following configuration options:

- Radio: 5 GHz (802.11 a/n/ac)
- Channel Plan Mode: ☒ Manual ☐ Interval ☐ Fixed Time
- Ignore Unmanaged Aps: ☒ ON ☐ OFF
- Channel Change Threshold: [Default: -82, Range: -99 to -1]
- Managed AP CH Conflict Threshold: [Default: -56, Range: -99 to -1]

At the bottom of the settings section are "Save" and "Cancel" buttons.

2. Each AP is dual-band capable of operating in the 2.4GHz and 5GHz frequencies. The 802.11a/n and 802.11b/g/n modes use different channel plans. Before you configure channel plan settings, select the mode to configure. Click either the **5GHz** or **2.4GHz** tab.

3. Select **Channel Plan Mode**. There are three type of modes:
 - **Manual** - With the manual channel plan mode, you control and initiate the calculation and assignment of the channel plan. You must manually run the channel plan algorithm and apply the channel plan to the APs.
 - **Interval** - In the interval channel plan mode, the controller periodically calculates and applies the channel plan. You can configure the interval to be from every 6 to every 24 hours. The interval period begins when you click **Submit**.
 - **Fixed Time** - If you select the fixed time channel plan mode, you specify the time for the channel plan and channel assignment. In this mode the plan is applied once every 24 hours at the specified time.
4. **Channel Plan Interval**: If you select the Interval channel plan mode, you can specify the frequency at which the channel plan calculation and assignment occurs. The interval time is in hours, and you can specify an interval that ranges between every 6 hours to every 24 hours.
5. **Channel Plan Fixed Time**: If you select the Fixed Time channel plan mode, you can specify the time at which the channel plan calculation and assignment occurs. The channel plan calculation will occur once every 24 hours at the time you specify.
6. **Ignore Unmanaged APs**: This function indicates whether the controller should pay attention only to APs managed by the cluster or all detected APs when deciding what channel select for the radio. The setting is enabled by default.
7. **Channel Change Threshold**: Configure the detected neighbor signal strength that triggers the channel plan to re-evaluate the current operation channel. If the operating channel detects neighbor APs operating on the same channel with signal below this threshold then the AP does not try to select a new channel for the radio. The default value for this threshold is -82dBm. The range is -99dBm to -1dBm.
8. **Managed AP CH Conflict Threshold**: Once the controller channel interference calculation has done, AP will prepare to change the radio to the less interference channel. To avoid two or more nearing APs change to the same channel at the same time. AP will cancel the channel changing if there have any nearing AP which the signal strength is above the "Managed AP CH conflict Threshold" are also attempt change to the same channel.
9. **Manual Channel Plan**: If you select Manual, click on the Manual Channel Plan tab. Here you can apply and start the channel algorithm on selected access points.
10. **Channel Plan History**: This field shows whether the controller is using the automatic channel adjustment algorithm on the AP 2.4GHz and 5GHz radio.

Configure Power Settings

Path: Wireless > General > Power Algorithm

You can set the power of the AP radio frequency transmission in the AP profile, the local database or in the RADIUS server. The power level in the AP profile is the default level for the AP, and the power will not be adjusted below the value in the AP profile. The settings in the local database and RADIUS server always override power set in the profile setting. If you manually set the power, the level is fixed and the AP will not use the automatic power adjustment algorithm.

To configure Channel Algorithm setting:

1. Click **Wireless > General > Power Algorithm > Power Setting** tab.

The screenshot shows the D-Link Unified Controller - DWC 2000 web interface. The top navigation bar includes Status, Wireless, Network, Security, and Maintenance. The breadcrumb trail is Wireless > General > Power Algorithm. The 'Power Setting' tab is selected. The page contains a 'Power Adjustment Mode' section with 'Manual' selected and 'Auto' as an option. Below it is a 'Power Threshold (dBm)' field set to -85, with a default of -85 and a range of -99 to -1 dBm. 'Save' and 'Cancel' buttons are at the bottom.

2. You can configure the power as a percentage of maximum power, where the maximum power is the minimum of power level allowed for the channel by the regulatory domain or the hardware capability. Select **Manual** or **Auto** Mode.
3. Enter the power change threshold. The default value is -85dBm. The power changes are initiated only if the neighbor radio hears the transmitting radio with the signal strength equal or above the threshold. The signal detected below the threshold is ignored.
4. If you select **Manual**, click on the **Manual Power Adjustments** tab. Here you can apply and start the power algorithm on selected access points.

The screenshot shows the 'Manual Power Adjustments' tab selected. It displays a 'Manual Power Adjustments List' table with columns for AP MAC Address, Location, Radio, Current Power, and New Power. The table is currently empty, showing 'No data available in table'. Below the table are 'Apply', 'Clear', and 'Start' buttons. The interface also shows the current status as 'None' and a 'Show 10 entries' dropdown.

WIDS

The Wireless Intrusion Detection System (WIDS) can help detect intrusion attempts into the wireless network and take automatic actions to protect the network.

Configure AP WIDS Settings

Path: Wireless > General > WIDS > AP WIDS Security

The WIDS AP Configuration page allows you to activate or deactivate various threat detection tests and set threat detection thresholds in order to help detect rogue APs on the wireless network. These changes can be done without disrupting network connectivity. Since some of the work is done by access points, the controller needs to send messages to the APs to modify its WIDS operational properties.

Note: The classification settings on the WIDS AP Configuration page are part of the global configuration on the controller and must be manually pushed to other controllers in order to synchronize that configuration.

Many of the tests are focused on identifying APs that are advertising managed SSIDs, but are not in fact managed APs. Detecting such an AP means that a network is either miss-configured or that a hacker set up a honeypot AP in the attempt to collect passwords or other secure information.

Although operational mode radios can detect most threats, the sentry radios detect the threats faster, especially when a potential rogue is operating on a different channel from any of the managed AP radios. The number of deployed sentry radios should be sufficient to provide coverage by one sentry radio in every geographical location within the network. A denser sentry deployment may be desirable in order to improve rogue or interferer signal triangulation.

To configure WIDS AP:

1. Go to **Wireless > General > WIDS > AP WIDS Security** tab.

D-Link
Unified Controller - DWC 2000

Serial Number: 00000000000001 | Firmware Version: 4.2.0.3_WW | Language: English (US)

Logged in as: admin (ADMIN) | Logout

Wizard | System Search...

Status | Wireless | Network | Security | Maintenance

Wireless > General > WIDS > AP WIDS Security

AP WIDS Security | AP WIDS Client Security

Through this page we can activate or deactivate various threat detection tests and set threat detection thresholds in order to help detect rogue APs on the wireless network. These changes can be done without disrupting network connectivity. Since some of the work is done by access points, the controller needs to send messages to the APs to modify its WIDS operational properties.

AP WIDS Security

| | |
|---|---|
| Administrator Configured Rogue AP | Enabled |
| Managed SSID from an Unknown AP | ON |
| Managed SSID from a Fake Managed AP | ON |
| AP without a SSID | ON |
| Fake Managed AP on an Invalid Channel | ON |
| Managed SSID Detected with Incorrect Security | ON |
| Invalid SSID from a Managed AP | ON |
| AP is Operating on an Illegal Channel | ON |
| Standalone AP with Unexpected Configuration | ON |
| Unexpected WDS Device Detected on Network | ON |
| Unmanaged AP Detected on Wired Network | ON |
| Rogue Detected Trap Interval | 300 [Range: 60 - 3600, 0 - Disable] Seconds |
| Wired Network Detection Interval | 60 [Range: 1 - 3600, 0 - Disable] Seconds |
| AP De-Authentication Attack | OFF |

Save Cancel

2. Enable or disable the security options as desired (refer to the table below) and click **Save**.

| Field | Description |
|--|---|
| Administrator Configured Rogue AP | If the source MAC address is in the valid-AP database on the controller or on the RADIUS server, and the AP type is marked as Rogue, then the AP state is Rogue. |
| Managed SSID from an Unknown AP | <p>This test checks whether an unknown AP is using the managed network SSID. A hacker may set up an AP with managed SSID to fool users into associating with the AP and revealing password and other secure information.</p> <p>Administrators with large networks who are using multiple clusters should either use different network names in each cluster or disable this test. Otherwise, if an AP in the first cluster detects APs in the second cluster transmitting the same SSID as APs in the first cluster then these APs are reported as rogues.</p> |
| Managed SSID from a Fake Managed AP | A hacker may set up an AP with the same MAC address as one of the managed APs and configure it to send one of the managed SSIDs. This test checks for a vendor field in the beacons which is always transmitted by managed APs. If the vendor field is not present, then the AP is identified as a fake AP. |
| AP without a SSID | <p>SSID is an optional field in beacon frames. To avoid detection a hacker may set up an AP with the managed network SSID, but disable SSID transmission in the beacon frames. The AP would still send probe responses to clients that send probe requests for the managed SSID fooling the clients into associating with the hacker's AP.</p> <p>This test detects and flags APs that transmit beacons without the SSID field. The test is automatically disabled if any of the radios in the profiles are configured not to send SSID field, which is not recommended because it does not provide any real security and disables this test.</p> |
| Fake Managed AP on an Invalid Channel | This test detects rogue APs that transmit beacons from the source MAC address of one of the managed APs, but on different channel from which the AP is supposed to be operating. |
| Managed SSID Detection with Incorrect Security | <p>During RF Scan the AP examines beacon frames received from other APs and determines whether the detected AP is advertising an open network, WEP, or WPA.</p> <p>If the SSID reported in the RF Scan is one of the managed networks and its configured security not match the detected security then this test marks the AP as rogue.</p> |
| Invalid SSID from a Managed AP | This test checks whether a known managed AP is sending an unexpected SSID. The SSID reported in the RF Scan is compared to the list of all configured SSIDs that are used by the profile assigned to the managed AP. If the detected SSID doesn't match any configured SSID then the AP is marked as rogue. |
| AP is Operating on an Illegal Channel | <p>The purpose of this test is to detect hackers or incorrectly configured devices that are operating on channels that are not legal in the country where the wireless system is set up.</p> <p>Note: In order for the wireless system to detect this threat, the wireless network must contain one or more radios that operate in sentry mode.</p> |
| Standalone AP with Unexpected Configuration | <p>If the AP is classified as a known standalone AP, then the controller checks whether the AP is operating with the expected configuration parameters. You configure the expected parameters for the standalone AP in the local or RADIUS Valid AP database. This test may detect network misconfiguration as well as potential intrusion attempts. The following parameters are checked:</p> <ul style="list-style-type: none"> • Channel Number • SSID • Security Mode • WDS Mode • Presence on a wired network |

| Field | Description |
|---|--|
| Unexpected WDS Device Detection on Network | If the AP is classified as a Managed or Unknown AP and wireless distribution system (WDS) traffic is detected on the AP, then the AP is considered to be Rogue. Only stand-alone APs that are explicitly allowed to operate in WDS mode are not reported as rogues by this test. |
| Unmanaged AP Detection on Wired Network | This test checks whether the AP is detected on the wired network. If the AP state is Unknown, then the test changes the AP state to Rogue. The flag indicating whether AP is detected on the wired network is reported as part of the RF Scan report. If AP is managed and is detected on the network then the controller simply reports this fact and doesn't change the AP state to Rogue. In order for the wireless system to detect this threat, the wireless network must contain one or more radios that operate in sentry mode. |
| Rogue Detected Trap Interval | Specify the interval, in seconds, between transmissions of the SNMP trap telling the administrator that rogue APs are present in the RF Scan database. If you set the value to 0, the trap is never sent. |
| Wired Network Detection Interval | Specify the number of seconds that the AP waits before starting a new wired network detection cycle. If you set the value to 0, wired network detection is disabled. |
| AP De-Authentication Attack | Enable or disable the AP de-authentication attack. The wireless controller can protect against rogue APs by sending de-authentication messages to the rogue AP. The de-authentication attack feature must be globally enabled in order for the wireless system to do this function. Make sure that no legitimate APs are classified as rogues before enabling the attack feature. This feature is disabled by default. |

Configure Client WIDS Settings

Path: Wireless > General > WIDS > AP WIDS Client Security

The Wireless Intrusion Detection System (WIDS) can help detect intrusion attempts into the wireless network and take automatic actions to protect the network. The settings you configure on the WIDS Client Configuration page help determine whether a detected client is classified as a rogue. Clients classified as rogues are considered to be a threat to network security.

Note: The classification settings on the WIDS Client Configuration page are part of the global configuration on the controller and must be manually pushed to other controllers in order to synchronize that configuration.

As part of the general association and authentication process, wireless clients send 802.11 management messages to APs. The WIDS feature tracks the following types of management messages that each detected client sends:

- Probe Requests
- 802.11 Authentication Requests.
- 802.11 De-Authentication Requests.

In order to help determine whether a client is posing a threat to the network by flooding the network with management traffic, the system keeps track of the number of times the AP received each message type and the highest message rate detected in a single RF Scan report. On the WIDS Client Configuration page, you can set thresholds for each type of message sent, and the APs monitor whether any clients exceed those thresholds or tests.

To configure WIDS Client:

1. Go to **Wireless > General > WIDS > AP WIDS Client Security** tab.

D-Link
Unified Controller - DWC 2000

Serial Number: 00000000000001 | Firmware Version: 4.2.0.3_VW | Language: English [US]

Logged in as: admin (ADMIN) | Logout

Wizard | System Search...

Wireless > General > WIDS > AP WIDS Client Security

AP WIDS Security | **AP WIDS Client Security**

The settings we configure on the WIDS Client Configuration page help determine whether a detected client is classified as a rogue. Clients classified as rogues are considered to be a threat to network security.

AP WIDS Client Security

| | |
|---|---|
| Not Present in OUI Database Test | <input type="checkbox"/> OFF |
| Not Present in Known Client Database Test | <input type="checkbox"/> OFF |
| Configured Authentication Rate Test | <input checked="" type="checkbox"/> ON |
| Configured Probe Requests Rate Test | <input checked="" type="checkbox"/> ON |
| Configured De-Authentication Requests Rate Test | <input checked="" type="checkbox"/> ON |
| Maximum Authentication Failures Test | <input checked="" type="checkbox"/> ON |
| Authentication with Unknown AP Test | <input type="checkbox"/> OFF |
| Client Threat Mitigation | <input type="checkbox"/> OFF |
| Known Client Database Lookup Method | <input checked="" type="checkbox"/> ON |
| Known Client Database Radius Server Name | Default-RADIUS-Server |
| Rogue Detected Trap Interval | 300 [Range: 60 - 3600, 0 - Disable] Seconds |
| De-Authentication Requests Threshold Interval | 60 [Range: 1 - 3600] Seconds |
| De-Authentication Requests Threshold Value | 10 [Range: 1 - 99999] |
| Authentication Requests Threshold Interval | 60 [Range: 1 - 3600] Seconds |
| Authentication Requests Threshold Value | 10 [Range: 1 - 99999] |
| Probe Requests Threshold Interval | 60 [Range: 1 - 3600] Seconds |
| Probe Requests Threshold Value | 120 [Range: 1 - 99999] |
| Authentication Failure Threshold Value | 10 [Range: 1 - 99999] |

2. Enable or disable the security options as desired (refer to the table below) and click **Save**.

| Field | Description |
|--|--|
| Not Present in OUI Database Test | This test checks whether the MAC address of the client is from a registered manufacturer identified in the OUI database. |
| Not Present in Known Client Database Test | This test checks whether the client, which is identified by its MAC address, is listed in the Known Client Database and is allowed access to the AP either through the Authentication Action of Grant or through the White List global action. If the client is in the Known Client Database and has an action of Deny, or if the action is Global Action and it is globally set to Black List, the client fails this test. |
| Configured Authentication Rate Test | This test checks whether the client has exceeded the configured rate for transmitting 802.11 authentication requests. |
| Configured Probe Requests Rate Test | This test checks whether the client has exceeded the configured rate for transmitting probe requests. |
| Configured De-Authentication Requests Rate Test | This test checks whether the client has exceeded the configured rate for transmitting de-authentication requests. |
| Maximum Authentication Failures Test | This test checks whether the client has exceeded the maximum number of failed authentications. |
| Authentication with Unknown AP Test | This test checks whether a client in the Known Client database is authenticated with an unknown AP. |
| Client Threat Mitigation | Select enable to send de-authentication messages to clients that are in the Known Clients database but are associated with unknown APs. The Authentication with Unknown AP Test must also be enabled in order for the mitigation to take place. Select disable to allow clients in the Known Clients database to remain authenticated with an unknown AP. |
| Known Client Database Lookup Method | When the controller detects a client on the network it performs a lookup in the Known Client database. Specify whether the controller should use the local or RADIUS database for these lookups. |
| Known Client Database Radius Server Name | If the known client database lookup method is RADIUS then this field specifies the RADIUS server name. |
| Rogue Detected Trap Interval | Specify the interval, in seconds, between transmissions of the SNMP trap telling the administrator that rogue APs are present in the RF Scan database. If you set the value to 0, the trap is never sent. |
| De-Authentication Requests Threshold Interval | Specify the number of seconds an AP should spend counting the de-authentication messages sent by wireless clients. |
| De-Authentication Requests Threshold Value | If the controller receives more than specified messages during the threshold interval the test triggers. |
| Authentication Requests Threshold Interval | Specify the number of seconds an AP should spend counting the authentication messages sent by wireless clients. |
| Authentication Requests Threshold Value | If the controller receives more than specified messages during the threshold interval the test triggers. |
| Probe Requests Threshold Interval | Specify the number of seconds an AP should spend counting the probe messages sent by wireless clients. |
| Probe Requests Threshold Value | Specify the number of probe requests a wireless client is allowed to send during the threshold interval before the event is reported as a threat. |
| Authentication Failure Threshold Value | Specify the number of 802.1X authentication failures a client is allowed to have before the event is reported as a threat. |

Distributed Tunnel

The Distributed Tunneling mode, also known as AP-AP tunneling mode, is used to support L3 roaming for wireless clients without forwarding any data traffic to the wireless controller.

In the AP-AP tunneling mode, when a client first associates with an AP in the wireless system, the AP forwards its data using the VLAN forwarding mode. The AP to which the client initially associates is the Home AP. The AP to which the client roams is the Association AP.

When a client roams to another AP in a different subnet the Association AP tunnels all traffic from the client to the Home AP using a CAPWAP L2 tunnel. The Home AP injects the traffic received over the tunnel into the wired network. If a client roams to another AP in the same subnet then the tunnel is not created, and the new AP becomes the Home AP for the client.

Configure Distributed Tunnel

Path: Wireless > General > Distributed Tunnel

1. Click **Wireless > General > Distributed Tunnel**.

The screenshot shows the D-Link Unified Controller (DWC 2000) web interface. The top navigation bar includes 'Status', 'Wireless', 'Network', 'Security', and 'Maintenance'. The 'Wireless' tab is selected, and the 'Distributed Tunnels' sub-tab is active. The page displays the following configuration settings:

| Setting | Value | Default / Range |
|---|-------|------------------------------------|
| Distributed Tunnel Clients | 128 | [Default: 128, Range: 1 - 8000] |
| Distributed Tunnel Idle Timeout | 120 | [Default: 120, Range: 30 - 3600] |
| Distributed Tunnel Timeout | 7200 | [Default: 7200, Range: 30 - 86400] |
| Distributed Tunnel Max Multicast Replications Allowed | 128 | [Default: 128, Range: 1 - 1024] |

Buttons: Save, Cancel

2. Configure the following settings:
 - **Distributed Tunnel Clients** - Specify the maximum number of distributed tunneling clients that can roam away from the Home AP at the same time.
 - **Distributed Tunnel Idle Timeout** - Specify the number of seconds of no activity by the client before the tunnel to that client is terminated and the client is forced to change its IP address.
 - **Distributed Tunnel Timeout** - Specify the number of seconds before the tunnel to the roamed client is terminated and the client is forced to change its IP address.
 - **Distributed Tunnel Max Multicast Replications Allowed** - Specify the maximum number of tunnels to which a multicast frame is copied on the Home AP.

3. Click **Save**.

WLAN Visualization

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

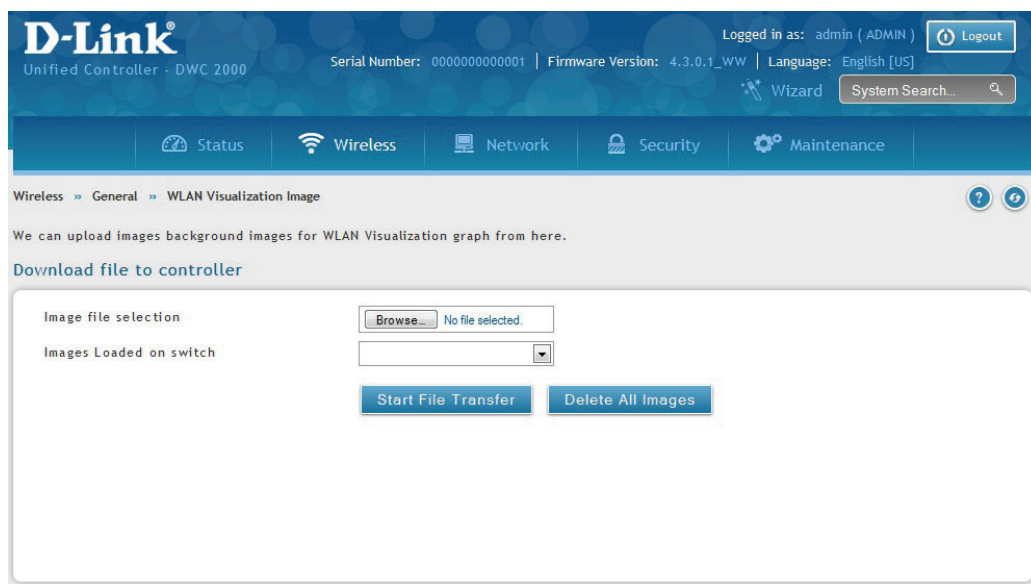
Upload Images

General > WLAN Visualization Image

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

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

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



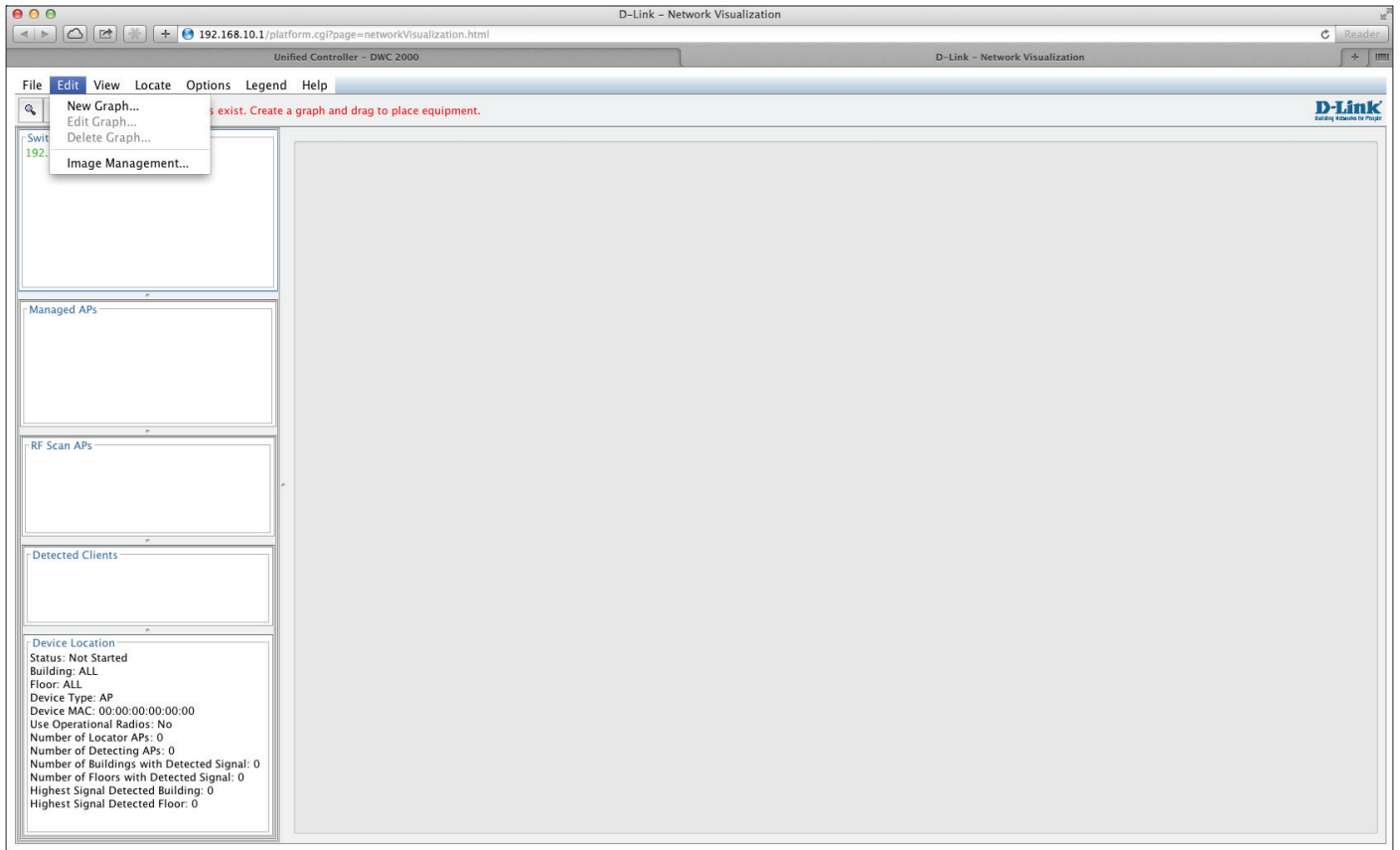
Deleting Images

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

Launch

Path: Wireless > General > WLAN Visualization

To launch the WLAN Visualization tool, click Wireless > General > WLAN Visualization. This will open a new browser window and starts the Java applet that allows the AP and WLAN controller network to be presented as a topology diagram (with or without a custom background image).



AP Discovery Methods

The wireless controller and AP can use the following methods to discover each other:

- L2 Discovery
- IP Address of AP Configured in the wireless controller
- IP Address of the wireless controller Configured in the AP

L2/ VLAN Discovery

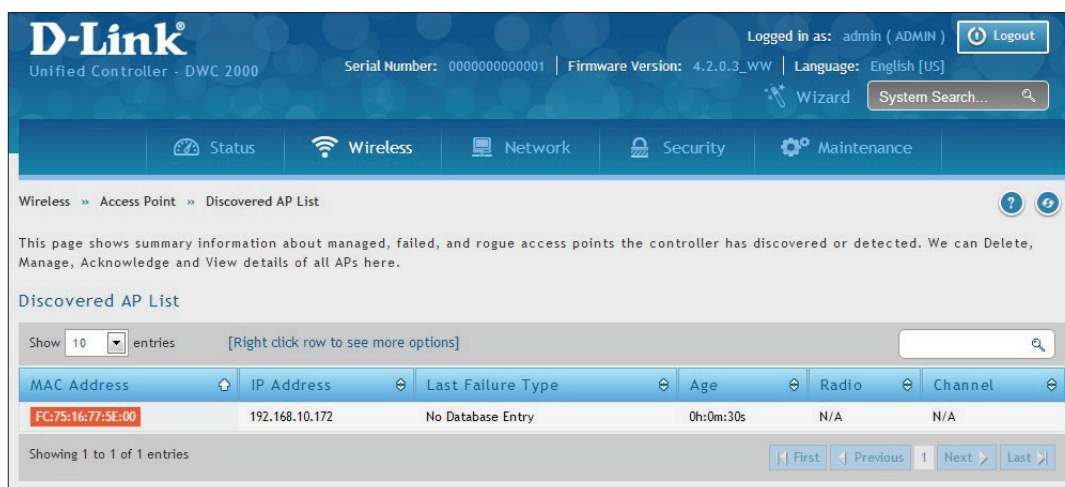
When the AP and the wireless controller are directly connected or in the same layer 2 broadcast domain and use the default VLAN settings, the wireless controller automatically discovers the AP through its broadcast of a L2 discovery message. The L2 discovery works automatically when the devices are directly connected or connected by using a layer 2 bridge. You can enable the discovery protocol on up to 16 VLANs.

By default, VLAN 1 is enabled on the AP, and VLAN 1 is enabled for discovery on the wireless controller. If the wireless controller and AP are in the same Layer 2 multicast domain, you might not need to take any action to enable AP discovery. The wireless controller also uses L2/VLAN discovery to find peer controllers within the L2 multicast domain.

The APs process the discovery message only when it comes in on the management VLAN. The APs do not forward the L2 discovery messages onto the wireless media.

From the wireless controller, you can check the discovery status of APs and peer controllers. To view information about whether the controller discovered any APs, navigate to the Wireless > Access Point > Discovered AP List page. The color of MAC address of the Discovered AP List indicating the AP is:

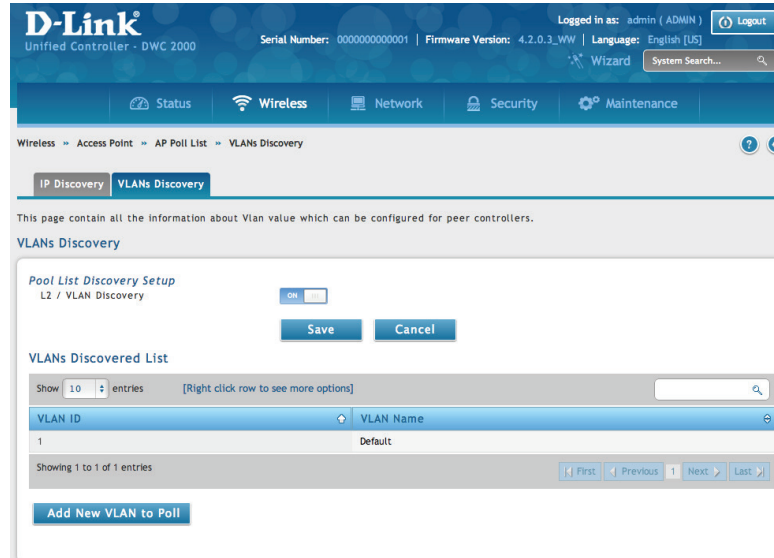
- Green = Managed AP
- Red = Connected Fail AP or AP (D-Link UAP) which is not in local or RADIUS Valid AP Database
- Gray = Unknown AP or Rogue AP
- Orange = Managed AP by peer controller



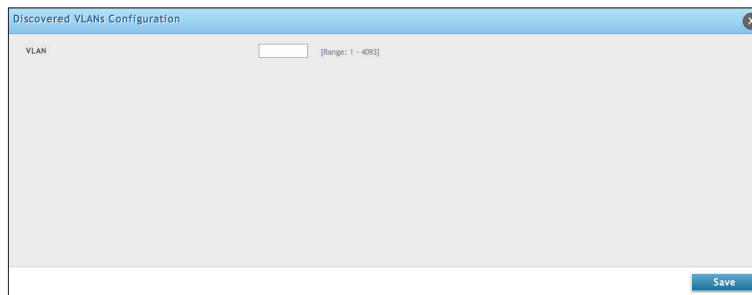
Configure L2/ VLAN Discovery

Path: Wireless > Access Point > AP Poll List

1. Click **Wireless > Access Point > AP Poll List > VLAN Discovery** tab.



2. Switch *L2/VLAN Discovery* to **ON** and click **Save**.
3. Click **Add New VLAN to Poll**. Enter a VLAN number.



4. Click **Save**.

L3/ IP Discovery

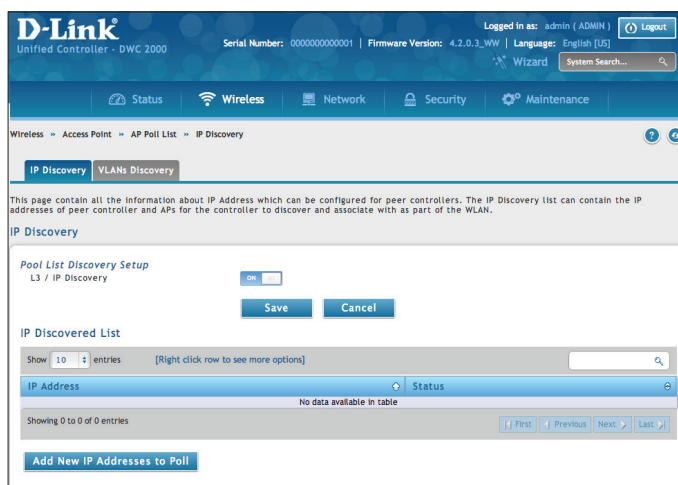
You can configure up to 256 IP addresses in the wireless controller for potential peer controllers and APs. The wireless controller sends association invitations to all IP addresses in this list. If the device accepts the invitation and is successfully validated by the controller, the controller and the AP or peer wireless controller are associated.

This discovery method mechanism is useful for peer wireless controller discovery and AP discovery when the devices are in different IP subnets. In fact, for a wireless controller to recognize a peer that is not on the same subnet, you must configure the IP addresses of each controller in the peer's L3 discovery list.

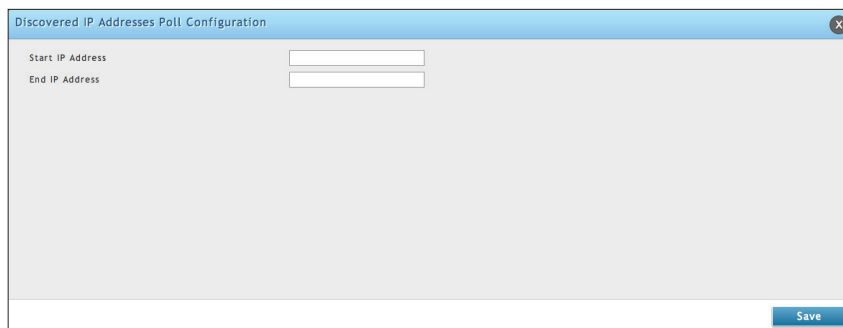
Configure L3/ IP Discovery

Path: Wireless > Access Point > AP Poll List

1. Click **Wireless > Access Point > AP Poll List > IP Discovery** tab.



2. Switch *L3/IP Discovery* to **On** and click **Save**.
3. Click **Add New IP Addresses to Poll**. Enter the IP range.



4. Click **Save**.
5. Navigate to **Wireless > Access Point > Discovered AP List**. Check the discovered AP via L3/ IP discovery.

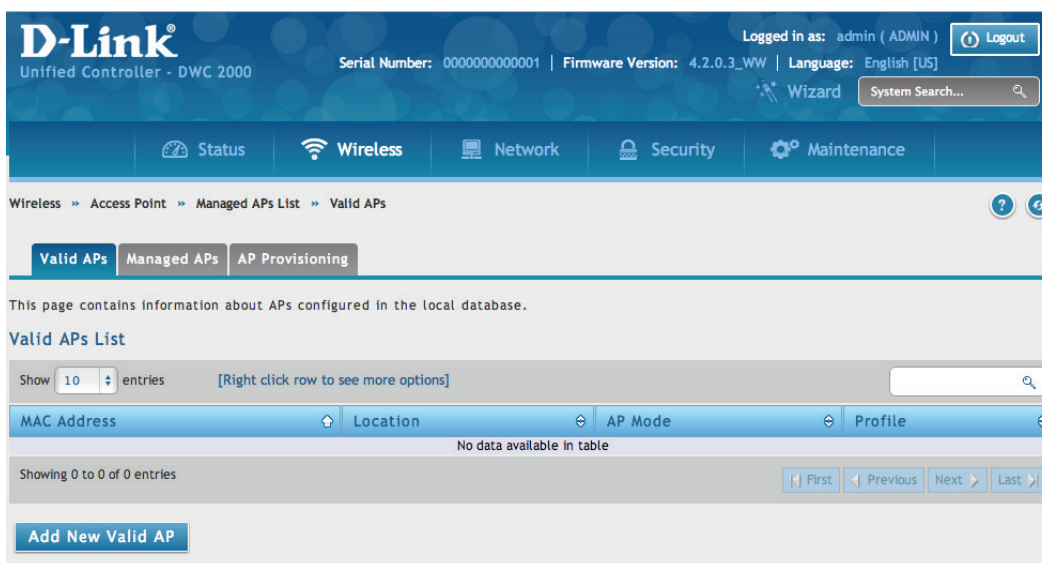
Managed APs

The managed AP information stores in controller local database. You can add/delete, change power/channel, or change the AP profile individually.

The Wireless Global Configuration page contains a field to select whether to use a local or RADIUS database for AP Validation. The Valid Access Point List page contains information about APs configured in the local database. If the AP Validation is set to RADIUS, information about the APs to be managed by the controller must be added to the external RADIUS database.

Add a Valid AP

1. Click **Wireless > Access Point > Managed APs List > Valid AP** tab.



2. Click **Add New Valid AP**.
3. Complete the fields on the next page and click **Save**.

Note: To add or delete an AP from the valid AP list, right-click the access point and select **Edit** or **Delete**.

Managed Mode

Valid APs Configuration

MAC address

AP Mode: ☒ Managed ☐ Standalone ☐ Rogue

Location

Authentication: ☒ ON

Profile: 1-Default

Radio 802.11a/n Channel: Auto

Power: Profile

Radio 802.11b/g/n Channel: Auto

Power: Profile

Save

Standalone Mode

Valid APs Configuration

MAC address

AP Mode: ☐ Managed ☒ Standalone ☐ Rogue

Location

Expected SSID

Expected Channel: Any

Expected WDS Mode: ☒ Any ☐ Normal ☐ bridge

Expected Security Mode: Any

Expected Wired Network Mode: ☒ Allowed ☐ Not Allowed

Save

Rogue Mode

Valid APs Configuration

MAC address

AP Mode: ☐ Managed ☐ Standalone ☒ Rogue

Location

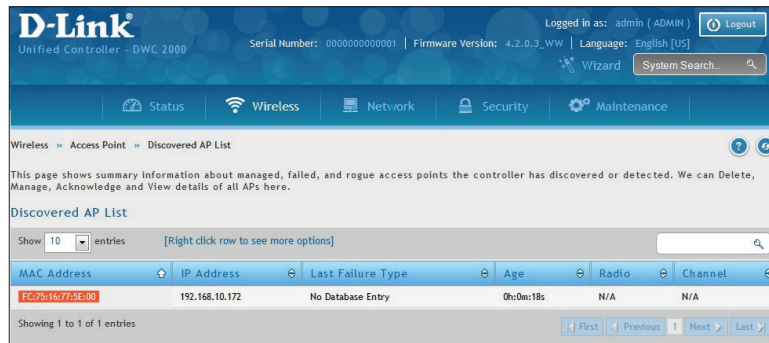
Save

| Field | Description |
|-----------------------------|--|
| MAC Address | MAC address of the access point. |
| AP Mode | Select standalone, managed, or rogue. Selecting standalone or managed will require you to fill out the fields (refer to the next page). <ul style="list-style-type: none"> Standalone Managed = access point profile configuration has been applied to the access point and the access point operating in managed mode. Rogue = access point has not tried to contact the wireless controller and the access point's MAC address is not in the Valid AP database. |
| Location | Optional field to identify location of the access point being managed. |
| Expected SSID | If AP Mode= Standalone, the SSID that the access point should be set to. This is for reference only. |
| Expected Channel | If AP Mode= Standalone, the channel to be used for wireless communication. This is for reference only. |
| Expected WDS Mode | If AP Mode= Standalone, the WDS (Wireless Distributed System) mode to be used if you intend to use WDS. This is for reference only. |
| Expected Security Mode | If AP Mode= Standalone, the security mode to be used. This is for reference only. |
| Expected Wired Network Mode | If AP Mode= Standalone, select whether wired networking is going to be allowed. This is for reference only. |
| Authentication Password | If AP Mode= Managed, turn on to require a password for authentication. |
| Profile | If AP Mode= Managed, select a profile to apply for AP configuration. |
| Radio | If AP Mode= Managed, this is Wireless radio mode that the access point is using. The fields below appear after you have selected Managed AP Mode. |
| Channel | If AP Mode= Managed, this is operating channel for the radio. |
| Power | If AP Mode= Managed, this is percentage of power to use for the radio. |

Add a AP from Discovered AP List

Path: Wireless > Access Point > Discovered AP List

1. Click **Wireless > Access Point > Discovered AP List**.



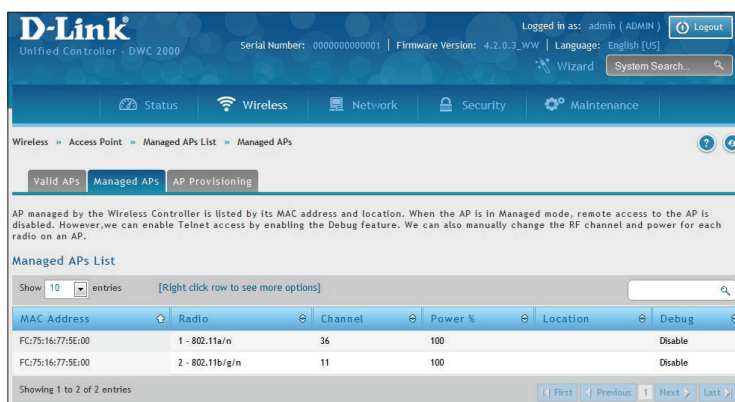
2. Right-click an AP and select **Manage**.
3. Select an AP Mode and Profile (refer to the previous page) and then click **Save**.

Manual Change Channel and Power of Managed AP

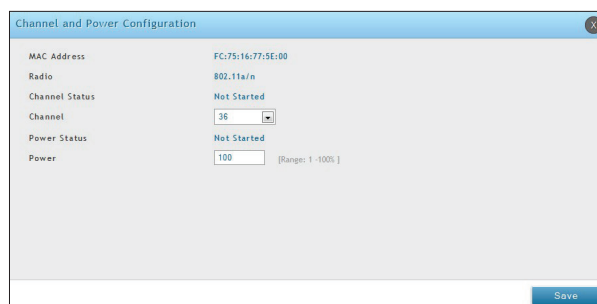
Path: Wireless > Access Point > Managed APs List > Managed APs

From the Managed AP page, you can also manually change the RF channel and power for each radio on an AP. The manual power and channel changes override the settings configured in the AP profile (including automatic channel selection) and take effect immediately. The manual channel and power assignments are not retained when the AP is reset or if the profile is reapplied to the AP, such as when the AP disassociates and re-associates with the controller.

1. Click **Wireless > Access Point > Managed APs List > Managed APs** tab.



2. Right-click on one of the entries and select **Channel and Power**.



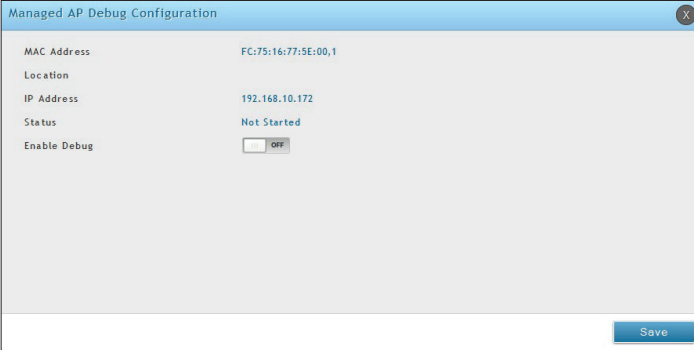
3. Select the channel as your desired. The available channels depend on the radio mode and country in which the APs operate. The manual channel change overrides the channel configured in the AP profile and is not retained when the AP reboots or when the AP profile is reapplied.
4. Change the power as your desired. You can set a new power level for the AP. The manual power change overrides the power setting configured in the AP profile and is not retained when the AP reboots or when the AP profile is reapplied.
5. Click **Save**.

Configure AP Debug Mode

Path: Wireless > Access Point > Managed APs List > Managed APs

When the AP is in Managed mode, remote access to the AP is disabled. However, you can enable Telnet access by enabling the Debug feature on the Managed APs page.

1. Click **Wireless** > **Access Point** > **Managed APs List** > **Managed APs** tab
2. Right-click on one of the entries and select **Debug**.



The image shows a 'Managed AP Debug Configuration' window. It contains the following fields and values:

| Field | Value |
|--------------|------------------------------|
| MAC Address | FC:75:16:77:5E:00,1 |
| Location | |
| IP Address | 192.168.10.172 |
| Status | Not Started |
| Enable Debug | <input type="checkbox"/> OFF |

A 'Save' button is located at the bottom right of the window.

3. Toggle *Enable Debug* to **On**.
4. Click **Save**.

Configure AP Provisioning

Path: Wireless > Access Point > Managed AP List > AP Provisioning

The AP Provisioning feature helps you add new APs to an existing switch cluster. With AP Provisioning, you can configure the access points with parameters that are needed to connect to the wireless network.

Use AP Provisioning to connect devices to a network enabled for mutual authentication (Wireless > Peer Group > Peer Configuration). If a network is not enabled for mutual authentication then APs can be attached to the network by properly configuring the local Valid AP database or RADIUS AP database and discovery options. The provisioning feature can optionally be used on networks not enabled for mutual authentication to simplify AP attachment to the cluster.

Use the AP Provisioning page to view detailed provisioning information about an AP and use Edit by right-click to specify the IP address of the primary or backup switch that provides provisioning information for the AP.

1. Click **Wireless > Access Point > Managed AP List > AP Provisioning** tab.

AP Provisioning Status List

| MAC Address | IP Address | Primary IP | Backup IP | New IP | New Backup IP | Status |
|--------------------|---------------|--------------|-----------|---------|---------------|-------------|
| *78:54:2e:2e:e4:80 | 192.168.10.87 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | Not Started |
| *78:54:2e:32:57:00 | 192.168.10.72 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | Not Started |
| *fc:75:16:77:0e:c0 | 192.168.10.65 | 192.168.10.1 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | Not Started |

Showing 1 to 3 of 3 entries

2. Right-click a managed AP and select **Edit**.

AP Provisioning Status

| | |
|-------------------------------------|-------------------|
| MAC Address | 78:54:2e:2e:e4:80 |
| IP Address | 192.168.10.87 |
| Time Since last update | 0d:00:00:01 |
| Primary IP Address | 0.0.0.0 |
| Backup IP Address | 0.0.0.0 |
| Mutual Authentication Mode | Disabled |
| Unmanaged AP Reprovisioning Mode | Disabled |
| AP provisioning Status | Not Started |
| AP Certificate and profile transmit | Not Started |
| New Primary IP Address | 0.0.0.0 |

Save

3. Enter the new primary address, new backup address and AP Profile.
4. Click **Save**.

| Field | Description |
|--|--|
| MAC Address | MAC address of the access point. |
| IP Address | IP address of the access point. |
| Time Since Last Update | Time since any information has been received from this access point. |
| Primary IP Address | The IP address of the primary provisioned switch as reported by the AP. |
| Backup IP Address | The IP address of the backup provisioned switch as reported by the AP. |
| Mutual Authentication Mode | Shows whether the Mutual Authentication mode is currently enabled. |
| Unmanaged AP Reprovisioning Mode | The configured re-provisioning mode in the AP, which is one of the following: <ul style="list-style-type: none"> • Enable - The AP can be reprovisioned when it is not managed. • Disable - The AP cannot be reprovisioned when it is not managed. |
| AP Provisioning Status | Status of the most recently issued AP provisioning command, which is one of the following: <ul style="list-style-type: none"> • Not Started - Provisioning has not been done for this AP. • Success - Provisioning finished successfully for this wireless controller. The AP Provisioning Status Table should reflect the latest provisioning configuration. • In Progress - Provisioning is executing for this AP. • Invalid Switch IP Address - Either primary or backup wireless controller IP address is not in the cluster or the mutual authentication mode is enabled and the primary wireless controller IP address is not specified. • Provisioning Rejected - AP is not managed and is configured not to accept provisioning data in unmanaged mode. • Timed Out - The last provisioning request timed out. |
| AP Certificate and Profile Transmit Status | Status of the last AP profile and X.509 Certificate distribution to the Primary and Backup switches. This status is changed as a result of the AP provisioning command. The X.509 certificate is sent to the primary and backup switches only if mutual authentication is enabled. The status is one of the following: <ul style="list-style-type: none"> • Not Started - No information for this AP has been sent to the primary and backup switch. • Success - AP Profile and X.509 Certificate is sent to Primary and Backup Switches. • Failed - The primary or backup switch wasn't in the cluster when this switch attempted to send the information. |
| New Primary IP Address | Enter the IP address of the wireless controller that should manage the AP. |
| New Backup IP Address | Enter the IP address of switch to which the AP should try to connect if it is unable to connect to the primary wireless controller. |
| Profile | Select an AP profile you want to use. |

AP Profiles

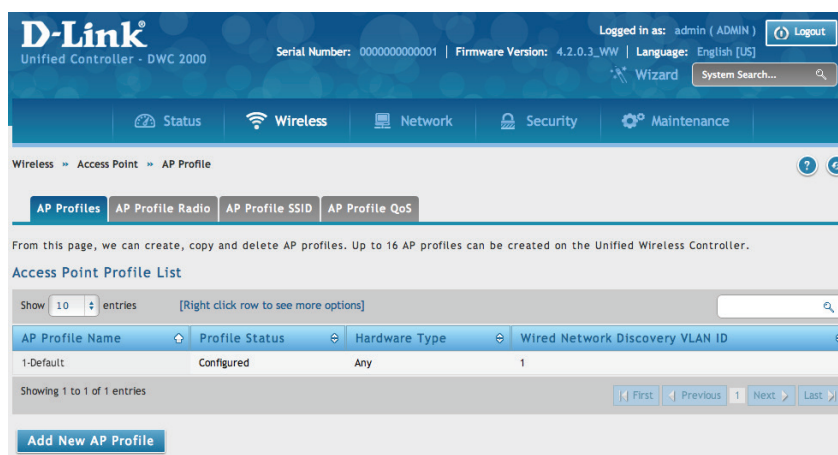
Access point configuration profiles are a useful feature for large wireless networks with APs that serve a variety of different users. You can create multiple AP profiles on the wireless controller to customize APs based on location, function, or other criteria. Profiles are like templates, and once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

- Profile Settings (Name, Hardware Type ID, Wired Network Discovery VLAN ID)
- Radio Settings
- SSID Settings
- QoS Configuration

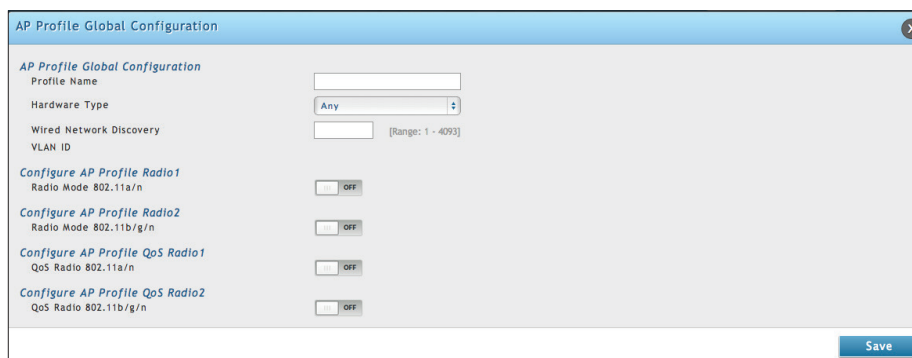
Configure AP Profile

Path: Wireless > Access Point > AP Profile > AP Profiles

1. Click **Wireless > Access Point > AP Profiles > AP Profiles** tab.



2. Click **Add New AP Profile**.



3. Complete the fields in the table below and click **Save**.

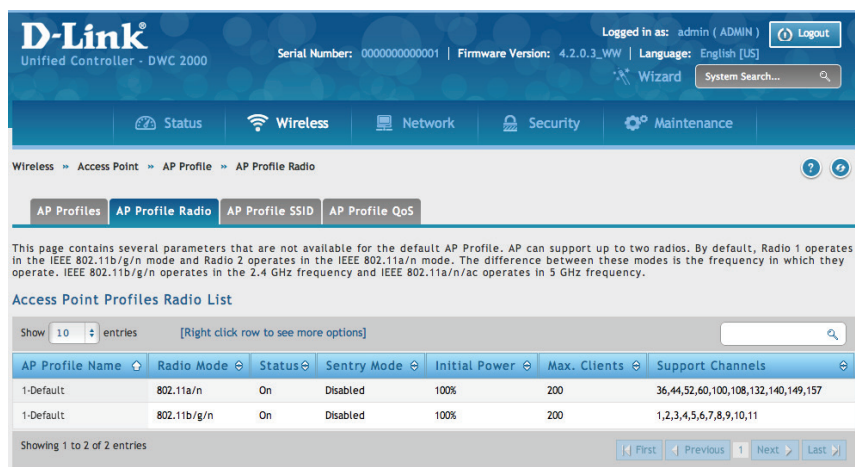
| Field | Description |
|---|---|
| AP Profile Global Configuration | |
| Profile Name | Identifies the name of the configured profile. |
| Hardware Type | Hardware type for the APs that use this profile. The hardware type is determined, in part, by the number of radios the AP supports (single or dual) and the IEEE 802.11 modes that the radio supports (a/b/g or a/b/g/n). The available options are: <ul style="list-style-type: none"> • Any. • DWL-8600AP Dual Radio a/b/g/n. • DWL-6600AP Dual Radio a/b/g/n. • DWL-3600AP Single Radio b/g/n. • DWL-2600AP Single Radio b/g/n. • DWL-8610AP Dual Radio a/b/g/n/ac |
| Wired network Discovery VLAN ID | LAN ID that the controller uses to send tracer packets in order to detect APs connected to the wired network. |
| Configure AP Profile Radio 1 | |
| Radio Mode 802.11a/n | In a new AP Profile, you can edit the radio 802.11a/n from here. You can also edit it from AP Profile Radio. |
| Configure AP Profile Radio 2 | |
| Radio Mode 802.11b/g/n | In a new AP Profile, you can edit the radio 802.11b/g/n from here. You can also edit it from AP Profile Radio. |
| Configure AP Profile QoS Radio 1 | |
| QoS Radio Mode 802.11a/n | In a new AP Profile, you can edit the QoS on radio 802.11a/n from here. You can also edit it from AP Profile Radio. |
| Configure AP Profile QoS Radio 2 | |
| QoS Radio Mode 802.11b/g/n | In a new AP Profile, you can edit the QoS on radio 802.11b/g/n from here. You can also edit it from AP Profile Radio. |

Configure AP Profile Radio

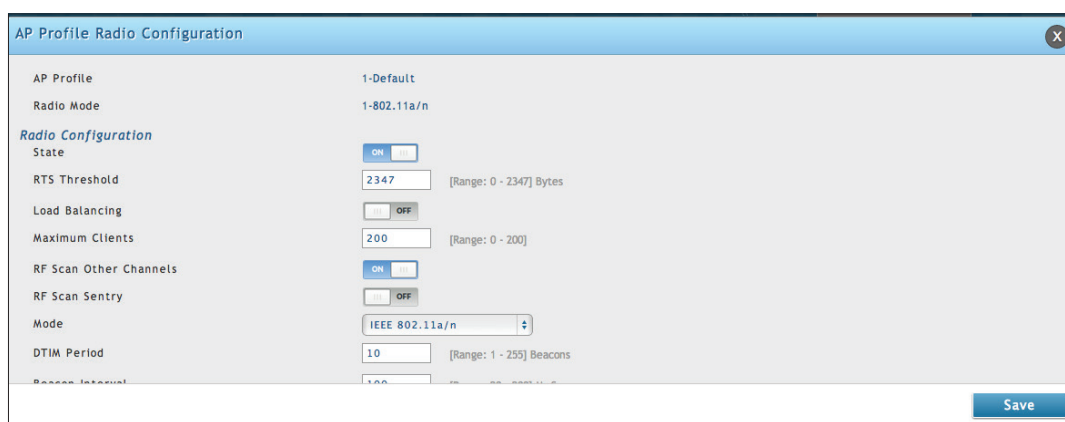
Path: Wireless > Access Point > AP Profile > AP Profile Radio

To accommodate a broad range of wireless clients and wireless network requirements, the AP can support up to two radios. By default, Radio 1 operates in the IEEE 802.11a/n mode, and Radio 2 operates in the IEEE 802.11b/g/n mode. The difference between these modes is the frequency in which they operate. IEEE 802.11b/g/n operates in the 2.4 GHz frequency, and IEEE 802.11a/n operates in the 5 GHz frequency of the radio spectrum.

1. Click **Wireless > Access Point > AP Profiles > AP Profiles Radio** tab.



2. Select the radio you want to change and right-click the row to edit.



3. Complete the fields in the table below and click **Save**.

| Field | Description |
|---------------------|---|
| AP Profile | The name of AP Profile |
| Radio Mode | The radio mode. 802.11a/n or 802.b/g/n |
| Radio Configuration | |
| State | <p>Specify whether you want the radio on or off by clicking On or Off.</p> <p>If you turn off a radio, the AP sends disassociation frames to all the wireless clients it is currently supporting so that the radio can be gracefully shutdown and the clients can start the association process with other available APs.</p> <p>ON= Radio ON OFF= Radio OFF</p> |
| Mode | <p>The Mode defines the Physical Layer (PHY) standard the radio uses.</p> <p>Select one of the following modes for each radio interface:</p> <ul style="list-style-type: none"> • IEEE 802.11a is a PHY standard that specifies operating in the 5 GHz U-NII band using orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 6 to 54 Mbps. • IEEE 802.11b/g operates in the 2.4 GHz ISM band. IEEE 802.11b is an enhancement of the initial 802.11 PHY to include 5.5 Mbps and 11 Mbps data rates. It uses direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) as well as complementary code keying (CCK) to provide the higher data rates. It supports data rates ranging from 1 to 11 Mbps. IEEE 802.11g is a higher speed extension (up to 54 Mbps) to the 802.11b PHY. It uses orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 1 to 54 Mbps. • IEEE 802.11a/n operates in the 5 GHz ISM band and includes support for both 802.11a and 802.11n devices. IEEE 802.11n is an extension of the 802.11 standard that includes multiple-input multiple-output (MIMO) technology. IEEE 802.11n supports data ranges of up to 248 Mbps and nearly twice the indoor range of 802.11 b, 802.11g, and 802.11a. • IEEE 802.11b/g/n operates in the 2.4 GHz ISM band and includes support for 802.11b, 802.11g, and 802.11n devices. • 5 GHz IEEE 802.11n is the recommended mode for networks with 802.11n devices that operate in the 5 GHz frequency that do not need to support 802.11a or 802.11b/g devices. IEEE 802.11n can achieve a higher throughput when it does not need to be compatible with legacy devices (802.11b/g or 802.11a). • 2.4 GHz IEEE 802.11n is the recommended mode for networks with 802.11n devices that operate in the 2.4 GHz frequency that do not need to support 802.11a or 802.11b/g devices. IEEE 802.11n can achieve a higher throughput when it does not need to be compatible with legacy devices (802.11b/g or 802.11a). • IEEE 802.11n/ac operates in 5GHz ISM band and includes support both 11n and 11ac devices. |
| RTS Threshold | <p>Specify a Request to Send (RTS) Threshold value between 0 and 2347.</p> <p>The RTS threshold indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed.</p> <p>Changing the RTS threshold can help control traffic flow through the AP, especially one with a lot of clients. If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the packet. On the other hand, sending more RTS packets can help the network recover from interference or collisions which might occur on a busy network, or on a network experiencing electromagnetic interference.</p> |

| Field | Description |
|--------------------------------|--|
| Load Balancing | If you enable load balancing, you can control the amount of traffic that is allowed on the AP. |
| Load Utilization | If Load Balancing is set to ON, this field allows you to set a threshold for the percentage of network bandwidth utilization allowed on the radio. Once the level you specify is reached, the AP stops accepting new client associations. Enter a percentage of utilization from 1 to 100. |
| Maximum Clients | Specify the maximum number of stations allowed to associate with this access point at any one time. You can enter a value between 0 and 200. |
| RF Scan Other Channels | The access point can perform RF scans to collect information about other wireless devices within range and then report this information to the wireless controller. If Scan Other Channels is set to ON, the radio periodically moves away from the operational channel to scan other channels. Enabling this mode causes the radio to interrupt user traffic, which may be noticeable with voice connections. When the Scan Other Channels= OFF is cleared, the AP scans only the operating channel. |
| RF Scan Sentry | Select this option to allow the radio to operate in sentry mode. When the RF Scan Sentry option= ON, the radio primarily performs dedicated RF scanning. The radio passively listens for beacons and traffic exchange between clients and other access points but does not accept connections from wireless clients. In sentry mode, all VAPs are disabled. Networks that deploy sentry APs or radios can detect devices on the network quicker and perform more thorough security analysis. In this mode, the radio switches from one channel to the next. The length of time spent on each channel is controlled by the scan duration. The default scan duration is 10 milliseconds. |
| RF Scan Interval | This field controls the length of time between channel changes during the RF Scan. |
| RF Scan Sentry Channels | The radio can scan channels in the radio frequency used by the 802.11b/g band (2.4 GHz), the 802.11a band (5 GHz), or both bands. Select the channel band for the radio to scan. Note: The band selection applies only to radios in sentry mode and is dependent upon the capabilities of the radio. |
| RF Scan Duration | This field controls the amount of time the radio spends scanning the other channel (in milliseconds) during an RF scan. |
| Rate Limiting | Enabling multicast and broadcast rate limiting can improve overall network performance by limiting the number of packets transmitted across the network. This feature is disabled by default. Note: The available rate limit values are very low for most environments, so enabling this feature is not recommended. <ul style="list-style-type: none"> To enable Multicast and Broadcast Rate Limiting, switch ON. To disable Multicast and Broadcast Rate Disabled, switch OFF. |
| Rate Limit | Enter the rate limit you want to set for multicast and broadcast traffic. The limit should be greater than 1, but less than 50 packets per second. Any traffic that falls below this rate limit will always conform to and be transmitted to the appropriate destination. The default and maximum rate limit setting is 50 packets per second. This field is disabled if Rate Limiting is disabled. |
| Rate Limit Burst | Setting a rate limit burst determines how much traffic bursts can be before all traffic exceeds the rate limit. This burst limit allows intermittent bursts of traffic on a network above the set rate limit. The default and maximum rate limit burst setting is 75 packets per second. This field is disabled if Rate Limiting is disabled. |

| Field | Description |
|------------------------------|--|
| Load Balancing | If you enable load balancing, you can control the amount of traffic that is allowed on the AP. |
| Channel Bandwidth | The 802.11n specification allows the use of a 40-MHz-wide channel in addition to the legacy 20-MHz channel available with other modes. The 40-MHz channel enables higher data rates but leaves fewer channels available for use by other 2.4 GHz and 5 GHz devices. The 40-MHz option is enabled by default for 802.11a/n modes and 20 MHz for 802.11b/g/n modes. You can use this setting to restrict the use of the channel bandwidth to a 20-MHz channel. |
| Protection | The protection feature contains rules to guarantee that 802.11 transmissions do not cause interference with legacy stations or applications. By default, these protection mechanisms are enabled (Auto). With protection enabled, protection mechanisms will be invoked if legacy devices are within range of the AP. You can disable (Off) these protection mechanisms; however, when 802.11n protection is off, legacy clients or APs within range can be affected by 802.11n transmissions. 802.11 protection is also available when the mode is 802.11b/g. When protection is enabled in this mode, it protects 802.11b clients and APs from 802.11g transmissions. |
| Space Time Block Code | Space Time Block Coding (STBC) is an 802.11n technique intended to improve the reliability of data transmissions. The data stream is transmitted on multiple antennas so the receiving system has a better chance of detecting at least one of the data streams. Select one of the following options: <ul style="list-style-type: none"> • ON=The AP transmits the same data stream on multiple antennas at the same time. • OFF=The AP does not transmits the same data on multiple antennas. |
| No Ack | Select Enable to specify that the AP should not acknowledge frames with QoSNoAck as the service class value. |
| DTIM Period | The Delivery Traffic Information Map (DTIM) message is an element included in some Beacon frames. It indicates which client stations, currently sleeping in low-power mode, have data buffered on the access point awaiting pick-up. The DTIM period you specify indicates how often the clients served by this access point should check for buffered data still on the AP awaiting pickup. Specify a DTIM period within the given range (1–255). The measurement is in beacons. For example, if you set this field to 1, clients will check for buffered data on the AP at every beacon. If you set this field to 10, clients will check on every 10th beacon. |
| Beacon Interval | Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second). The Beacon Interval value is set in milliseconds. Enter a value from 20 to 2000. |
| Automatic Channel | The channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The range of channels and the default channel are determined by the Mode of the radio interface. When the AP boots, the AP scans the RF area for occupied channels and selects a channel from the available non-interfering or clear channels. However, channel conditions can change during operation. Enabling the Automatic Channel makes APs assigned to this profile eligible for auto-channel selection. You can automatically or manually run the auto-channel selection algorithm to allow the controller to adjust the channel on APs as WLAN conditions change. By default, the global auto-channel mode is set to manual. To enable the automatic channel selection mode, go to the AP Management > RF Management page and select Fixed or Interval for the Channel Plan mode. You can also run the automatic channel selection algorithm manually from the Manual Channel Plan page. Note: If you assign a static channel to an AP in the Valid AP database or on the Advanced AP Management page, the AP will not participate in the auto-channel selection. |

| Field | Description |
|----------------------------------|---|
| Automatic Power | The power level affects how far an AP broadcasts its RF signal. If the power level is too low, wireless clients will not detect the signal or experience poor WLAN performance. If the power level is too high, the RF signal might interfere with other APs within range. Automatic power uses a proprietary algorithm to automatically adjust the RF signal to broadcast far enough to reach wireless clients, but not so far that it interferes with RF signals broadcast by other APs. The power level algorithm increases or decreases the power level in 10% increments based on presence or absence of packet retransmission errors. |
| Default Power | The automatic power algorithm will not reduce the power below the number you set in the default power field. By default, the power level is 100%. Therefore, even if you enable the automatic power, the power of the RF signal will not decrease. The power level is a percentage of the maximum transmission power for the RF signal. |
| APSD Mode | Select Enable to enable Automatic Power Save Delivery (APSD), which is a power management method. APSD is recommended if VoIP phones access the network through the AP. |
| Frag Threshold | The fragmentation threshold limits the size of packets transmitted over the network. Acceptable values are even numbers from 256-2345. Packets that are under the configured size are not fragmented. A value of 2346 means that packets are not fragmented. |
| Short Retries | The value in this field indicates the maximum number of transmission attempts on frame sizes less than or equal to the RTS Threshold. The range is 1-255. |
| Long Retries | The value in this field indicates the maximum number of transmission attempts on frame sizes greater than the RTS Threshold. The range is 1-255. |
| Transmit Lifetime | Shows the number of milliseconds to wait before terminating attempts to transmit the MSDU after the initial transmission. |
| Receive Lifetime | Shows the number of milliseconds to wait before terminating attempts to reassemble the MMPDU or MSDU after the initial reception of a fragmented MMPDU or MSDU. |
| Station Isolation | When this option is selected, the AP blocks communication between wireless clients. It still allows data traffic between its wireless clients and wired devices on the network, but not among wireless clients. This feature is disabled by default. <ul style="list-style-type: none"> To enable Multicast and Broadcast Rate Limiting, click ON. To disable Multicast and Broadcast Rate Disabled, click OFF. |
| Primary Channel | This setting is editable only when a channel is selected and the channel bandwidth is set to 40 MHz. A 40-MHz channel can be considered to consist of two 20-MHz channels that are contiguous in the frequency domain. These two 20-MHz channels are often referred to as the Primary and Secondary channels. The Primary Channel is used for 802.11n clients that support only a 20-MHz channel bandwidth and for legacy clients. Use this setting to set the Primary Channel as the upper or lower 20-MHz channel in the 40-MHz band. |
| Short Guard Interval | The guard interval is the dead time, in nanoseconds, between OFDM symbols. The guard interval prevents Inter-Symbol and Inter-Carrier Interference (ISI, ICI). The 802.11n mode allows for a reduction in this guard interval from the a and g definition of 800 nanoseconds to 400 nanoseconds. Reducing the guard interval can yield a 10% improvement in data throughput. Select one of the following options: <ul style="list-style-type: none"> ON= The AP transmits data using a 400 ns guard Interval when communicating with clients that also support the 400 ns guard interval. OFF= The AP transmits data using an 800 ns guard interval. |
| Radio Resource Management | Radio Resource Measurement (RRM) mode requires the Wireless System to send additional information in beacons, probe responses, and association responses. Enable or disable the support for radio resource measurement feature in the AP profile. The feature is set independently for each radio and is enabled by default. |

| Field | Description |
|----------------------------------|---|
| Multicast Tx Rate (Mbps) | Select the 802.11 rate at which the radio transmits multicast frames. The rate is in Mbps. The lowest rate in the 5 GHz band is 6 Mbps. |
| Channel | |
| Auto Eligible Channels | This field displays the channels that are supported for the radio mode currently selected on the page and for the country configured on the General Settings page. Press Ctrl to select multiple channels. |
| Basic Rate Set (Mbps) | These numbers indicate the data rates that all stations associating with the AP must support. |
| Supported Rate Set (Mbps) | These numbers indicate rates that the access point supports. You can select multiple rates. The AP automatically chooses the most efficient rate based on factors like error rates and distance of client stations from the AP. |

Configure AP Profile SSID

Path: Wireless > Access Point > AP Profile > AP Profile SSID

The AP Profile SSID List page displays the virtual access point (VAP) settings associated with the selected AP profile. Each VAP is identified by its network number and Service Set Identifier (SSID). You can configure and enable up to 16 VAPs per radio on each physical access point.

1. Click **Wireless > Access Point > AP Profiles > AP Profiles SSID** tab.

Wireless > Access Point > AP Profile > AP Profile SSID

AP Profiles | AP Profile Radio | **AP Profile SSID** | AP Profile QoS

This page displays the virtual access point(VAP) settings associated with the selected AP profile. Each VAP is identified by its network number and Service Set Identifier(SSID). We can configure and enable up to 16 VAPs per radio on each physical access point.

Access Point Profiles SSID List

AP Profile: 1-Default

Radio Mode: ☒ 802.11a/n ☐ 802.11b/g/n

Show 10 entries [Right click row to see more options]

| SSID Name | SSID Status | VLAN | Hide SSID | Security | Redirect | Captive Portal |
|------------|-------------|-----------|-----------|----------|----------|----------------|
| 1-dlink1 | Enabled | 1-Default | Disabled | None | None | Free |
| 2-dlink2 | Disabled | 1-Default | Disabled | None | None | Free |
| 3-dlink3 | Disabled | 1-Default | Disabled | None | None | Free |
| 4-dlink4 | Disabled | 1-Default | Disabled | None | None | Free |
| 5-dlink5 | Disabled | 1-Default | Disabled | None | None | Free |
| 6-dlink6 | Disabled | 1-Default | Disabled | None | None | Free |
| 7-dlink7 | Disabled | 1-Default | Disabled | None | None | Free |
| 8-dlink8 | Disabled | 1-Default | Disabled | None | None | Free |
| 9-dlink9 | Disabled | 1-Default | Disabled | None | None | Free |
| 10-dlink10 | Disabled | 1-Default | Disabled | None | None | Free |

Showing 1 to 10 of 16 entries

First Previous 1 2 Next Last

2. Select the AP Profile from the drop-down menu.
3. Select the Radio Mode (either **802.11a/n** or **802.11b/g/n**).
4. Select the SSID name from the drop-down menu.
5. Enable/disable the SSID by right-clicking **Enable** or **Disable**.

Note: SSID ID 1 is always enabled. If you do not want to have the first SSID enabled, you must create a new SSID to be able to swap another SSID in the first slot.

Configure AP Profile QoS

Path: Wireless > Access Point > AP Profile > AP Profile QoS

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

Configuring Quality of Service (QoS) on the wireless controller consists of setting parameters on existing queues for different types of wireless traffic, and effectively specifying minimum and maximum wait times (through Contention Windows) for transmission. The settings described here apply to data transmission behavior on the access point only, not to that of the client stations.

AP Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the access point to the client station. Station Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the client station to the access point.

You can specify custom QoS settings, or you can select a template that configures the AP profile with pre-defined settings that are optimized for data traffic or voice traffic.

1. Click **Wireless > Access Point > AP Profiles > AP Profiles QoS** tab.

The screenshot shows the D-Link Unified Controller - DWC 2000 web interface. The top navigation bar includes links for Status, Wireless, Network, Security, and Maintenance. The 'Wireless' tab is selected, and the breadcrumb trail indicates the path: Wireless > Access Point > AP Profile > AP Profile QoS. Below the breadcrumb, there are tabs for AP Profiles, AP Profile Radio, AP Profile SSID, and AP Profile QoS, with the latter being the active tab. A descriptive text block explains that QoS provides the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic. Below this, the 'Access Point Profiles QoS List' is displayed, showing a table with 2 entries. The table has columns for AP Profile Name, Radio Mode, and Template. The first entry is '1-Default' with Radio Mode '1-802.11a/n' and Template 'Custom'. The second entry is '1-Default' with Radio Mode '2-802.11b/g/n' and Template 'Custom'. The interface also includes a search bar, a 'Show 10 entries' dropdown, and pagination controls at the bottom.

| AP Profile Name | Radio Mode | Template |
|-----------------|---------------|----------|
| 1-Default | 1-802.11a/n | Custom |
| 1-Default | 2-802.11b/g/n | Custom |

2. Right-click the AP Profile and select **Edit**.

The screenshot shows the 'AP Profile QoS Configuration' window. It has a title bar with a close button. The main area is divided into sections: 'AP Profile' (1-Default), 'Radio Mode' (1-802.11a/n), and 'Template' (Custom selected, Factory Default and Voice unselected). Below is the 'AP EDCA Parameters' section. It contains two data queues: 'Data 0 (Voice)' and 'Data 1 (Video)'. For 'Data 0 (Voice)', the AIFS is 1, cwMin is 3, cwMax is 7, and Max. Burst is 1500. For 'Data 1 (Video)', the AIFS is 1. A 'Save' button is at the bottom right.

3. Complete the fields below and click **Save**.

| Field | Description |
|--|---|
| AP Profile | The name of AP Profile |
| Radio Mode | The radio mode. 802.11a/n or 802.b/g/n |
| Template | Select the QoS template to apply to the AP profile. If you select Custom, you can change the AP and station parameters. If you select Voice or Factory Defaults, the wireless controller will use the pre-defined settings for the template you select. |
| AP EDCA Parameters | |
| Queue | <p>Queues are defined for different types of data transmitted from AP-to-station:</p> <ul style="list-style-type: none"> • Data 0 (Voice)—High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. • Data 1 (Video)—High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. • Data 2 (best effort)—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. • Data 3 (Background)—Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). |
| AIFS (Inter-Frame Space) | The Arbitration Inter-Frame Spacing (AIFS) specifies a wait time for data frames. The wait time is measured in slots. Valid values for AIFS are 1 through 255. |
| cwMin (Minimum Contention Window) | <p>This parameter is input to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.</p> <p>The first random number generated will be a number between 0 and the number specified here.</p> <p>If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window.</p> <p>Valid values for the cwmin are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for cwmin must be lower than the value for cwmax.</p> |

| Field | Description |
|--|--|
| cwMan (Maximum Contention Window) | The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the cwmax are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for cwmax must be higher than the value for cwmin. |
| Max. Burst Length | AP EDCA Parameter Only (The Max. Burst Length applies only to traffic flowing from the access point to the client station.) This value specifies (in milliseconds) the Maximum Burst Length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance. Valid values for maximum burst length are 0.0 through 999. |
| General Parameters | |
| WMM Mode | Wi-Fi MultiMedia (WMM) is enabled by default. With WMM enabled, QoS prioritization and coordination of wireless medium access is on. With WMM enabled, QoS settings on the D-Link controller control downstream traffic flowing from the access point to client station (AP EDCA parameters) and the upstream traffic flowing from the station to the access point (station EDCA parameters). Disabling WMM deactivates QoS control of station EDCA parameters on upstream traffic flowing from the station to the access point. With WMM disabled, you can still set some parameters on the downstream traffic flowing from the access point to the client station (AP EDCA parameters). To disable WMM extensions, switch OFF. To enable WMM extensions, switch ON. |
| Station EDCA Parameters | |
| Queue | Queues are defined for different types of data transmitted from station-to-AP: <ul style="list-style-type: none"> • Data 0 (Voice)—Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. • Data 1 (Video)—Highest priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. • Data 2 (best effort)—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. • Data 3 (Background)—Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). |
| AIFS (Inter-Frame Space) | The Arbitration Inter-Frame Spacing (AIFS) specifies a wait time for data frames. The wait time is measured in slots. Valid values for AIFS are 1 through 255. |
| cwMin (Minimum Contention Window) | This parameter is used by the algorithm that determines the initial random backoff wait time (window) for data transmission during a period of contention. The value specified in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. The first random number generated will be a number between 0 and the number specified here. If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window. |

| Field | Description |
|--|---|
| cwMan (Maximum Contention Window) | The value specified in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. |
| TXOP Limit | Station EDCA Parameter Only (The TXOP Limit applies only to traffic flowing from the client station to the access point.) The Transmission Opportunity (TXOP) is an interval of time when a WME client station has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for client stations; that is, the interval of time when a WMM client station has the right to initiate transmissions on the wireless network. |

SSID Profiles

The SSID Profile list shows all the wireless networks configured on the controller. The first 16 networks are created by default. You can modify the default networks, but you cannot delete them. You can add and configure up to 16 additional networks for a total of 50 wireless networks. Multiple networks can have the same SSID.

Configure SSID Profiles

Path: Wireless > Access Point > SSID Profiles

1. Click Wireless > Access Point > SSID Profiles. The SSID Profile List page will appear.

D-Link®
Unified Controller - DWC 2000

Logged in as: admin (ADMIN) [Logout]
Serial Number: 0000000000001 | Firmware Version: 4.2.0.3_WW | Language: English [US]
Wizard System Search...

Status Wireless Network Security Maintenance

Wireless > Access Point > SSID Profiles

This page shows all the wireless SSID configured on the controller. The first 16 SSID's are created by default. You can modify the default SSID, but we cannot delete them. We can add and configure up to 16 additional SSID for a total of 32 wireless SSID.

SSID Profile List

Show 10 entries [Right click row to see more options]

| SSID Id | Name | VLAN | Hide SSID | Security | Redirect | Captive Portal | Authentication Server |
|---------|---------|-----------|-----------|----------|----------|----------------|-----------------------|
| 1 | dlink1 | 1-Default | Disabled | None | None | Free | None |
| 2 | dlink2 | 1-Default | Disabled | None | None | Free | None |
| 3 | dlink3 | 1-Default | Disabled | None | None | Free | None |
| 4 | dlink4 | 1-Default | Disabled | None | None | Free | None |
| 5 | dlink5 | 1-Default | Disabled | None | None | Free | None |
| 6 | dlink6 | 1-Default | Disabled | None | None | Free | None |
| 7 | dlink7 | 1-Default | Disabled | None | None | Free | None |
| 8 | dlink8 | 1-Default | Disabled | None | None | Free | None |
| 9 | dlink9 | 1-Default | Disabled | None | None | Free | None |
| 10 | dlink10 | 1-Default | Disabled | None | None | Free | None |

Showing 1 to 10 of 16 entries

First Previous 1 2 Next Last

Add New SSID Profile

2. To edit an existing SSID, right-click it and select **Edit**. To create a new SSID Profile, click the **Add New SSID Profile** button.

Note: SSID ID 1 is always enabled. If you do not want to have the first SSID enabled, you must create a new SSID to be able to swap another SSID in the first slot.

3. Complete the fields in the table below and click **Save**.

| Field | Description |
|-----------------------|---|
| SSID | Enter a name of your wireless network. Be sure SSID is the same for all device in your wireless network and is case-sensitive. |
| Captive Portal Type | <p>Captive Portal type is selected per SSID basis. There are four types of access on a SSID:</p> <ul style="list-style-type: none"> Free: No authentication is required for users connected to this SSID if this option is selected. SLA (Service Level Agreement): If this is selected, users connected to this SSID needs to accept Service Level Agreement before accessing anything outside this SSID. Permanent User: When this option is selected users need to get authenticated before accessing data outside this SSID. Only permanent Captive Portal users can login from this SSID. Temporary User: When this option is selected users need to get authenticated before accessing data outside this SSID. Only temporary Captive Portal users created by frontend user can login from this SSID. Billing User: When this option is selected users need to get authenticated before accessing data outside this SSID. The temporary Captive Portal billing users created via online wireless service purchasing. The wireless service packages are defined in Login Profile. |
| Authentication Server | <p>If Captive Portal Type = Permanent User, select the authentication server.</p> <p>All users that log in to the captive portal for this SSID are authenticated through the selected server. The available authentication servers are Local User Databass, Radius Server, LDAP Server, or POP3.</p> |
| Authentication Type | If Captive Portal Type = Permanent User and Authentication Server = RADIUS server, select the authentication type: PAP, CHAP, MSCHAP, or MSCHAPV2. |
| Login Profile Name | <p>If Captive Portal Type = Permanent User or Temporary User, select the Login Profile.</p> <p>Any of the available profiles can be used for this SSID.</p> |
| Hide SSID | <p>You can hide the SSID broadcast to discourage stations from automatically discovering your access point(s). When the broadcast SSID of the AP is hidden, the SSID name is not displayed in the list of available SSID on a client station. Instead, the client must have the exact SSID name configured in the supplicant before it is able to connect.</p> <p>Disabling the broadcast SSID is sufficient to prevent clients from accidentally connecting to your network, but it will not prevent even the simplest of attempts by a hacker to connect or monitor unencrypted traffic.</p> <p>ON = SSID is hidden OFF = SSID is broadcast</p> |

| Field | Description |
|-------------------------------|---|
| Ignore Broadcast | If a wireless client broadcasts probe requests to all available SSIDs, this option controls whether the AP will respond to the probe request. ON = Prohibits the AP from responding to client probe requests. OFF = Allow the AP to respond to client probe requests. |
| VLAN | Enter a VLAN ID. Be sure this VLAN ID has been created (Network > VLAN > VLAN Setting) |
| MAC Authentication | If enabled, wireless clients must be authenticated by the AP in order to connect to the network. To use MAC authentication, configure the client MAC addresses in one of the databases: Local or RADIUS. In the database, set a default action to either accept or deny that client or use the global action configured. MAC authentication is useful in networks that operate in Open mode to grant or deny access to clients with specific MAC addresses. MAC Authentication can also be used in conjunction with 802.1X security methods, in which the MAC Authentication is done prior to the 802.1X authentication. |
| Authentication Type | If Captive Portal Type = Permanent User and Authentication Server = RADIUS server, select the authentication type: PAP, CHAP, MSCHAP, or MSCHAPV2. |
| Redirect | Select the HTTP option in the <i>Redirect</i> field to redirect wireless clients to a custom Web page. When redirect mode is enabled, the user will be redirected to the URL you specify after the wireless client associates with an AP and the user opens a web browser to access the Internet. The custom Web page must be located on an external web server and might contain information such as the company logo and network usage policy. Note: The wireless client is redirected to the external Web server only once while it associated with the AP. Redirect functionality allows you to implement captive portal functionality; a captive portal is often used at Wi-Fi hotspots to provide branding for the hotspot provider and/or display a legal disclaimer, which the user can click-through to access the Internet. HTTP=HTTP Redirect is enabled None=HTTP Redirect is disabled |
| Redirect URL | If Redirect = HTTP, enter the URL where all initial HTTP accesses should be redirected to. This field is accessible only when HTTP is selected as the redirect type. |
| Wireless ARP Suppression Mode | Enable the mode to allow APs to reduce the number of broadcasted ARP requests on the wireless interfaces. Reducing broadcasts helps conserve power on the wireless clients. The wireless clients that use power-save mode must wake up and use more power when they detect broadcast frames. Note: Enabling this feature slightly degrades AP packet forwarding performance due to extra packet filtering to find DHCP packets and extra processing for ARP request and reply packets. Networks that do not use IPv4 should not enable this feature. |
| L2 Distributed Tunneling Mode | The distributed L2 tunneling mode supports L3 roaming for wireless clients without forwarding any data traffic to the Unified Wireless controller. Use the menu to enable or disable the mode. L2 tunneling is recommended when the Unified Wireless controller does not support hardware forwarding acceleration or hardware-based L2 tunnels. Note: 1 - When there is only one controller managing all APs and that controller goes down, all APs shut down their radios and the tunnel is terminated. After the controller recovers and the AP becomes managed again, the client that was previously tunneling traffic will re-associate and obtain an IP address on the network where its currently located. This IP address will be different from the IP address it was using when it was tunneling, and the traffic will not be tunneled. 2 - If the network has peer controllers and the tunnel is established between the APs managed by the peer controller then, when a controller managing the home AP fails, the controller managing the association AP detects the failure and terminates the tunnel. At this point the client is disassociated. When the client re-associates it obtains a new IP address. 3 - If the controller managing the association AP fails, then the scenario is the same as in item 1 above. The AP takes down all radios and the clients disassociate. |

| Field | Description |
|--|---|
| RADIUS Authentication Server Status | Indicates whether the RADIUS authentication server is configured for the VAP. |
| Security | <p>The default access point profile does not use any security mechanism. To protect your network, we recommend you select a security mechanism to prevent unauthorized wireless clients from gaining access to your network. Choices are:</p> <ul style="list-style-type: none"> • None = No security mechanism is used. • WEP = Enable WEP security. Complete the options in Table 3 4. • WPA/WPA2 = Enable WPA/WPA2 security. Complete the options in Table 3 5. |

Wireless Distribution System (WDS)

The Wireless Distribution System (WDS) - Managed AP feature allows you to add managed APs to the cluster using over-the-air WDS links through other managed APs. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required. With WDS, APs may be located outdoors where wired connection to the data network is unavailable, or in remote buildings that are not connected to the main campus with a wired network.

The WDS AP group consists of two types of APs: root APs and satellite APs. A root AP acts as a bridge or repeater on the wireless medium and communicates with the controller via the wired link. A satellite AP communicates with the controller via a WDS link to the root AP. The WDS links are secured using WPA2 Personal authentication and AES encryption. When the AP is in Managed mode, remote access to the AP is disabled. However, you can enable Telnet access by enabling the Debug feature on the Managed AP List Settings page.

Support for the WDS-managed AP feature within the Unified Wired and Wireless Access System includes the following:

- The wireless system can contain up to 12 WDS-managed AP groups.
- Each WDS-managed AP group can contain up to four APs.
- An AP can be a member of only one WDS AP group.
- Each satellite AP can have only one WDS link on the satellite APs. This means that a satellite AP must be connected to a root AP. A satellite AP cannot be connected to another satellite AP.

By default, an AP is configured as a root AP. For an AP to be attached to the Wireless System as a satellite AP, configure the following settings on the AP while it is in stand-alone mode:

- Satellite AP mode. This setting enables the satellite AP to discover and establish WDS link with the root AP. By default, the WDS Managed Mode is Root AP.
- Password for WPA2 Personal authentication used to establish the WDS links. Only the satellite APs need this configuration. The root APs get the password from the controller when they become managed.
- Static Channel. The APs on each end of a WDS link must use the same radio and channel to communicate. Configure the satellite AP to use a static channel. For a root AP, set the static channel when you add the AP to the Valid AP database on the controller.
- Optionally, to allow the Ethernet port on a satellite AP to provide wired access to the LAN, you must set the WDS Managed Ethernet Port to Enabled. It is disabled by default.

To configure a WDS managed group and its links, use the following general steps:

1. Configure the satellite APs by connecting to the AP management interface while the AP is in stand-alone mode. Set the WDS Managed Mode to Satellite AP and configure the WDS Group Password.
2. From the controller CLI or web-based interface, create a WDS group.
3. Configure the WDS group password. The password you configure on the controller should be the same as the password you configure on each satellite AP.
4. Add the MAC address of each AP to the WDS group.
5. Configure the WDS links by specifying the MAC address and radio of the AP on each end of the link.

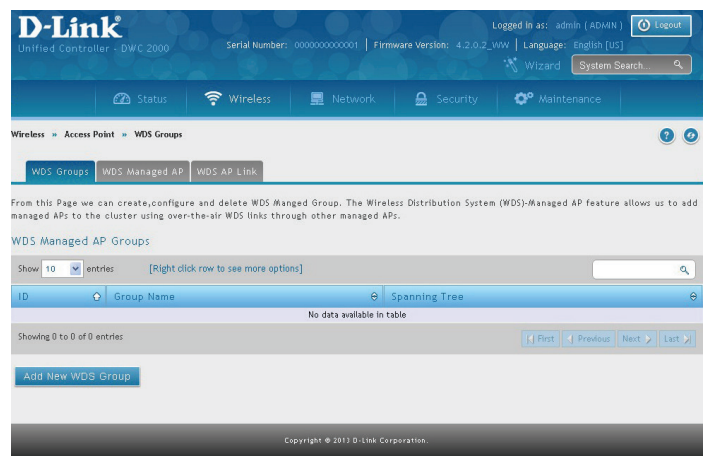
Keep the following considerations in mind when you configure and manage a WDS group:

- Make sure the radios that participate in the WDS link use the same channel. Use one of the following methods to control the channel:
 - When you configure the satellite AP in stand-alone mode, use the Radio page to set a static channel.
 - When you configure the AP in the Valid AP database, specify the channel that the radio must use. By default, the channel is set to Auto.
 - On the Radio page for the AP profile, select only one channel in the list of Auto Eligible channels. By default, multiple channels are enabled.
- D-Link recommends that satellite APs do not have wired connectivity to the wireless controller.
- A configuration push to WDS APs may take up to three minutes to complete.

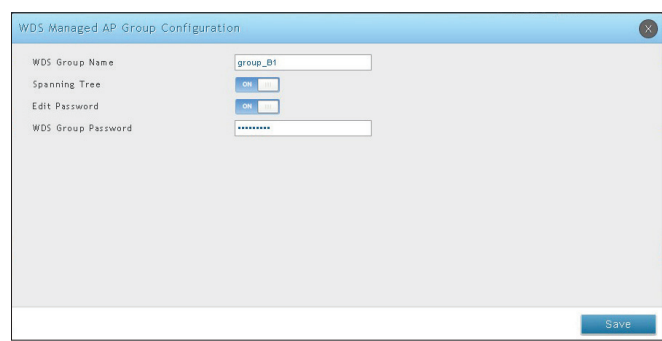
Configure WDS Managed AP

Path: Wireless > Access Point > WDS Groups > WDS Groups

- 1. Click **Wireless > Access Point > WDS Groups**.



- 2. Click **Add New WDS Group**.



- 3. Complete the fields in the table on the next page and click **Save**.

| Field | Description |
|----------------|--|
| WDS Group Name | A descriptive name of the WDS AP group, which can contain up to 32 characters. |
| Spanning Tree | Specifies whether to enable spanning tree on all APs in this WDS AP group. Spanning tree must be enabled if there are any potential loops in the network. For example if a satellite AP has links to two root APs then spanning tree must be enabled. Note: The spanning tree protocol running on the APs interacts with the spanning tree protocol running on the edge switches to which the APs are connected. |
| Edit Password | Password used for securing WPA2-Personal security on the WDS Link. Range: 8 – 63 ASCII characters. To create or change the password, select the Edit checkbox and type a password in the available field. This password must match the passwords set on the satellite APs in this group. By default, the password is AP-Group-n, where n is the AP group ID. |

Configure WDS Managed AP

Path: Wireless > Access Point > WDS Groups > WDS Managed AP

After you create a WDS-Managed AP group, use the WDS Managed AP Configuration page to view the APs that are members of the group, add new members, and change STP Priority values for existing members

1. Click **Wireless > Access Point > WDS Groups > WDS Managed AP** tab.

The screenshot shows the D-Link Unified Controller - DWC 2000 web interface. The top navigation bar includes tabs for Status, Wireless, Network, Security, and Maintenance. The 'Wireless' tab is selected, and the breadcrumb path 'Wireless > Access Point > WDS Groups > WDS Managed AP' is displayed. Below the breadcrumb, there are three sub-tabs: 'WDS Groups', 'WDS Managed AP' (which is active), and 'WDS AP Link'. A descriptive text block explains the page's function: 'This Page allows you to view the APs that are members of the group, add new members, and change STP Priority values for existing members. After you create a WDS-Managed AP group, use the WDS Managed AP Configuration page to view the APs that are members of the group, add new members, and change STP Priority values for existing members.' Below this is the 'WDS Managed AP List' section, which includes a search bar and a table. The table has columns for ID, AP MAC, AP Hardware Type, and STP Priority. A message 'No data available in table' is displayed in the table area. At the bottom of the list section, there is a button labeled 'Add New WDS Managed AP'.

D-Link® Unified Controller - DWC 2000

Serial Number: 0000000000001 | Firmware Version: 4.2.0.3_WW | Language: English [US]

Logged in as: admin (ADMIN) Logout

Wizard System Search...

Status Wireless Network Security Maintenance

Wireless > Access Point > WDS Groups > WDS Managed AP

WDS Groups WDS Managed AP WDS AP Link

This Page allows you to view the APs that are members of the group, add new members, and change STP Priority values for existing members. After you create a WDS-Managed AP group, use the WDS Managed AP Configuration page to view the APs that are members of the group, add new members, and change STP Priority values for existing members.

WDS Managed AP List

Show 10 entries [Right click row to see more options]

| ID | AP MAC | AP Hardware Type | STP Priority |
|----------------------------|--------|------------------|--------------|
| No data available in table | | | |

Showing 0 to 0 of 0 entries

First Previous Next Last

Add New WDS Managed AP

2. Click **Add New WDS Manage AP**.

WDS Managed AP Configuration

WDS Managed Group Id

Valid AP MAC Address

Hardware Type String

DWL-8600AP Dual Radio

WDS AP MAC Address

STP Priority

[Length: 0 - 64]

Save

3. Complete the fields in the table below and click **Save**.

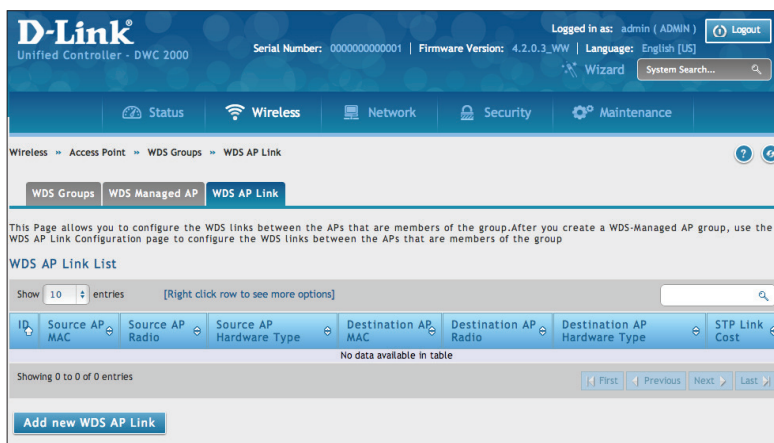
| Field | Description |
|----------------------|--|
| WDS Managed Group ID | Select the ID associated with the group to configure. |
| Valid AP MAC Address | MAC Address of the AP. |
| Hardware Type String | Select the AP from the drop-down menu. |
| WDS AP MAC Address | Enter the WDS AP MAC address. |
| STP Priority | <p>Spanning Tree Priority for this AP. The STP priority is used only when spanning tree mode is enabled.</p> <p>The STP priority determines which AP is selected as the root of the spanning tree and which AP has preference over another AP when multiple equal cost paths exist in the topology. The lower value for the spanning tree priority means that the AP is more likely to be used for bridging data into the campus network. You should assign a lower priority to the APs connected to the wired network than to the satellite APs.</p> <p>The STP priority value is rounded down to a multiple of 4096. The range is 0 – 61440, and the default value is 36864.</p> |

Configure WDS AP Link

Path: Wireless > Access Point > WDS Groups > WDS AP Link

After you create a WDS-Managed AP group, use the WDS AP Link Configuration page to configure the WDS links between the APs that are members of the group.

1. Click **Wireless > Access Point > WDS Groups > WDS AP Link** tab.



2. Click **Add New WDS AP Link**.

3. Complete the fields in the table below and click **Save**.

| Field | Description |
|-----------------------------------|---|
| WDS Managed Group ID | Select the ID associated with the group to configure. |
| Source AP MAC Address | MAC Address of the source AP. Note: The WDS links are bidirectional. The terms Source and Destination simply help to differentiate between the WDS link endpoints. |
| Source AP Radio | The radio number of the WDS link endpoint on the source AP. |
| Destination AP MAC Address | The MAC address of the destination AP in the group. |
| Destination Radio | The radio number of the WDS link endpoint on the destination AP. |
| Link Cost | Spanning Tree Path cost for the WDS link. The range is 0–255. When multiple alternate paths are defined in the WDS group, the link cost is used to indicate which links are the primary links and which links are the secondary links. The spanning tree selects the path with the lowest link cost. |

Peer Group

The Peer Group Configuration feature allows you to send a variety of configuration information from one wireless controller to all other wireless controllers. In addition to keeping the wireless controller synchronized, this function allows you to manage all wireless controllers in the cluster from one controller.

Configure Peer Group

Path: Wireless > Peer Group > Peer Configuration

You can copy portions of the wireless controller configuration from one controller to another controller in the cluster. The Peer Group Configuration Enable/Disable page allows you to select which parts of the configuration to copy to one or more peer wireless controllers in the group.

You can make changes to a configuration that has been sent to one or more peer controllers, and you can make changes to a configuration received from a peer controller. No changes automatically propagate from one controller to the cluster; you must manually initiate a request on one controller in order to copy any configuration to its peers.

1. Click **Wireless > Peer Group > Peer Configuration**.

The screenshot shows the D-Link Unified Controller - DWC 2000 interface. The top navigation bar includes Status, Wireless, Network, Security, and Maintenance. The 'Wireless' tab is selected, and the 'Peer Configuration' page is displayed. The page contains a list of configuration options with toggle switches:

- General: On
- Discovery: Off
- Channel / Power: On
- AP Database: On
- AP Profiles: On
- MAC Authentication Database: On
- Captive Portal: Off
- Radius Client: On
- Controller Provisioning Mode: On
- Mutual Authentication Mode: Off
- Unmanaged AP Reprovisioning Mode: On

At the bottom of the configuration list are 'Save' and 'Cancel' buttons.

2. Toggle each option to **On** or **Off**, and then click **Save**. Refer to the table on the next page.

| Field | Description |
|------------------------|--|
| General | Enable this field to include the basic and advanced global settings in the configuration that the controller pushes to its peers. The configuration does not include the controller IP address since that is a unique setting. |
| Discovery | Enable this field to include the L2 and L3 discovery information, including the VLAN list and IP list, in the configuration that the controller pushes to its peers. |
| Channel / Power | Enable this field to include the RF management information in the configuration that the controller pushes to its peers. |
| AP Database | Enable this field to include the AP Database (Valid AP) in the configuration that the controller pushes to its peers. |

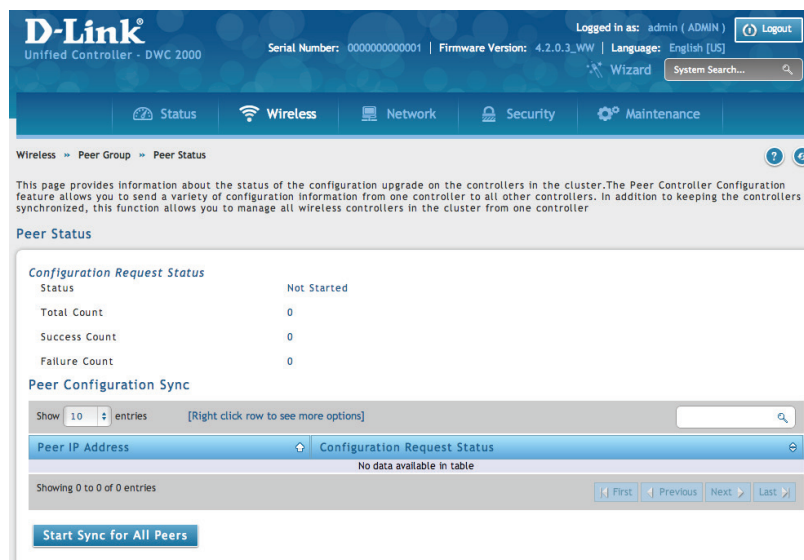
| | |
|---|---|
| AP Profiles | Enable this field to include all AP profiles in the configuration that the controller pushes to its peers. The AP profile includes the general AP settings, such as the hardware type, Radio settings, SSID Profiles, and QoS settings. |
| MAC Authentication DB | Enable this field to include the MAC Authentication Database in the configuration that the controller pushes to its peers. |
| Captive Portal | Enable this field to include the Captive Portal information in the configuration that the controller pushes to its peers. |
| RADIUS Client | Enable this field to include the Client RADIUS information in the configuration that the controller pushes to its peers. |
| Controller Provisioning Mode | Enable this field to send and receive provisioning messages. As a security feature, you can disable this option. |
| Mutual Authentication Mode | <p>Select Enable to require mutual authentication on the wireless network. When Disable is selected, mutual authentication is not required.</p> <p>Changing this parameter on one controller automatically updates the configuration on all other controllers in the cluster and all managed APs in the cluster.</p> <p>When this field is enabled, switch provisioning must be enabled in order for new controllers to be added to the cluster. If controller provisioning is disabled, the cluster will not accept certificates from a new controller.</p> |
| Unmanaged AP Reprovisioning Mode | Enable to allow access points to accept provisioning information when not managed by a controller. |

Synchronize Peer Group

Path: Wireless > Peer Group > Peer Status

Synchronize the settings among the peer group.

1. Click **Wireless > Peer Group > Peer Status**. Peer Status List will appear



2. Click **Start Sync for All Peers** to synchronize the settings to all controllers, or synchronize one of the peer group by right-clicking **Start Sync**.

AP Firmware Download

The Wireless Controller can upgrade software on the APs that it manages. The Cluster Controller can update code on APs managed by peer wireless controllers.

Path: Maintenance > Firmware > AP Firmware Download

1. Click **Maintenance > Firmware > AP Firmware Download > AP Firmware Download** tab.

D-Link®
Unified Controller - DWC 2000

Serial Number: 0000000000001 | Firmware Version: 4.2.0.3_VW | Language: English [US] | Logout

Wizard | System Search...

Status | Wireless | Network | Security | Maintenance

Maintenance > Firmware > AP Firmware Download

It may take about 12 minutes for the upgrade process to complete for an AP.

AP Firmware Download | AP Firmware Status

The Unified Wireless Controller can upgrade software on the APs that it manages. The Cluster Controller can update code on APs managed by peer wireless controllers.

AP Firmware Download

Server Address:

img_dw18600: D-Link 8600 AP Radios

File Path:

File Name:

img_dw13600/6600: D-Link 3600/6600 AP Radios

File Path:

File Name:

img_dw12600: D-Link 2600 AP Radios

File Path:

File Name:

img_dw18610: D-Link 8610 AP Radios

File Path:

File Name:

Group Size: [Default: 6, Range: 1 - 6]

Image Download Type:

Managed AP:

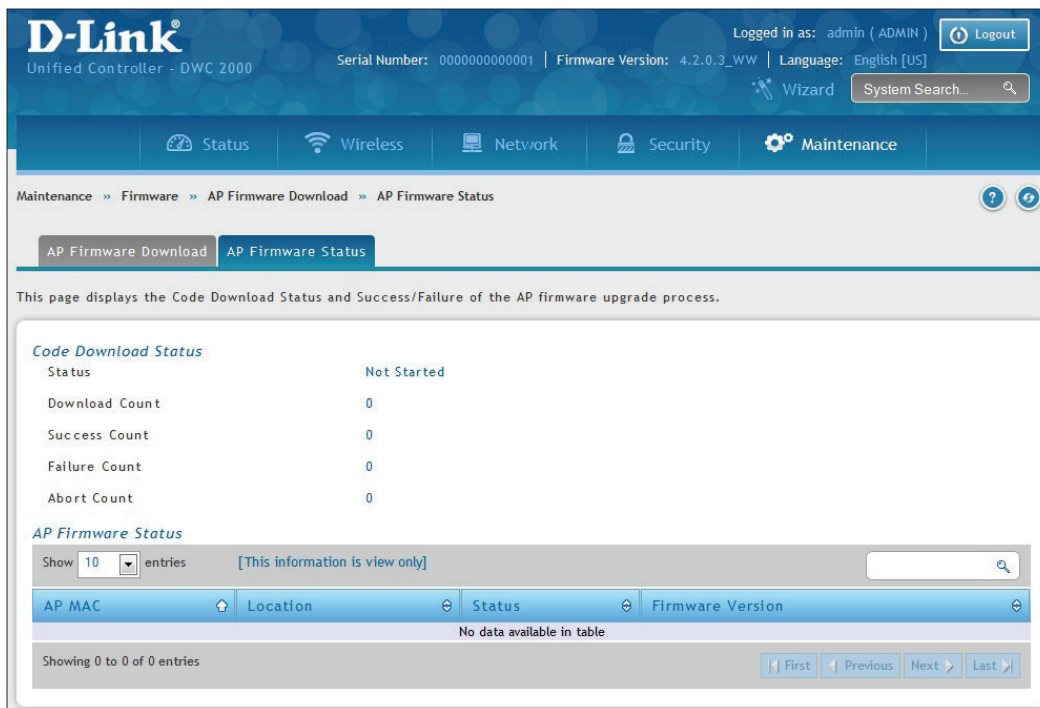
Save | Refresh

2. Complete the fields (refer to the table on the next page) and then select the AP(s) you want to upgrade. Use CTRL + click to select multiple APs.
3. Click **Save** to begin the upgrade process.

| Field | Description |
|---------------------|---|
| Server Address | Enter the IP address of the host where the upgrade file is located. The host must have a TFTP server installed and running. |
| File Path | Enter the file path on the TFTP server where the software is located. You may enter up to 96 characters. |
| File Name | Enter the name of the upgrade file. You may enter up to 32 characters, and the file extension .tar must be included. |
| Group Size | <p>When you upgrade multiple APs, each AP contacts the TFTP server to download the upgrade file. To prevent the TFTP server from being overloaded, you can limit the number of APs to be upgraded at a time.</p> <p>In the Group Size field, enter the number of APs that can be upgraded at the same time. When one group completes the upgrade, the next group begins the process.</p> |
| Image Download Type | <p>Type of the image to be downloaded, which can be one of the following:</p> <ul style="list-style-type: none">• All Images• DWL-8600AP• DWL-3600AP/ DWL-6600AP• DWL-2600AP• DWL-8610AP <p>Note: To download all images, make sure you specify the file path and file name for both images in the appropriate File Path and File Name fields.</p> |
| Managed AP | <p>The list shows all the APs that the controller manages. If the controller is the Cluster Controller, then the list shows the APs managed by all controllers in the cluster.</p> <p>Each AP is identified by its MAC address, IP address, and Location in the <MAC - IP - Location> format. To upgrade a single AP, select the AP MAC address from the drop down list. To upgrade all APs, select All from the top of the list. If All is selected, the Group Size field will limit the number of simultaneous AP upgrades in order not to overwhelm the TFTP server. To select multiple APs to upgrade, CTRL + click the APs to upgrade.</p> <p>Note: D-Link recommends that you upgrade all managed APs at the same time.</p> |

Path: Maintenance > Firmware > AP Firmware Download > AP Firmware Status

After the download begins, the AP Firmware Status tab will display information about the upgrade. Refer to the table below:



| Field | Description |
|------------------------|---|
| Code Download Status | |
| Status (Global) | <p>The status of the upgrade process for all APs:</p> <ul style="list-style-type: none"> • Not Started: The wireless controller has not started the download process. • Requested: A request to download AP software has been made, but the controller has not done any downloads. • Code Transfer in Progress: A download is in progress. • Failure: Download failed on all APs. • Aborted: Download was aborted before the AP loaded code from the TFTP server. • NVRAM-Update-in-Progress: Download completed successfully. The reset command has been sent to the AP. • Success: All APs are connected to the wireless controller. |
| Download Count | The number of managed APs to download software in the current download request. If you selected All for the managed APs to upgrade, the download count shows the number of managed APs at the time the download request was started. The value is 1 if only one AP is being updated. |
| Success Count | The number of APs that have successfully downloaded the new code. This value starts with 0 at the beginning of the download and increases by one for every AP that successfully downloaded the code. |
| Failure Count | The number of APs that failed to download the new code starting at 0 and incremental with each failure. |
| Abort Count | The number of APs for which the download was aborted, starting at 0 and incremental each aborted download. |

| AP Firmware Status | |
|--------------------|---|
| Status (per-AP) | <p>A table also appears and lists each AP, its download status, and the software version it is downloading. The status for an individual AP can have one of the following values:</p> <ul style="list-style-type: none">• Requested: A download is planned for this AP, but the AP is not in the current download group, so it hasn't been told to start the download yet.• Code-Transfer-In-Progress: The AP has been told to download the code.• Failure: The AP reported a failing code download.• Aborted: The download was aborted before the AP loaded code from the TFTP server.• Waiting-For-APs-To-Download: A download finished on this AP, and it is waiting for other APs to finish download. Reset command is not sent to the AP in this state.• NVRAM-Update-In-Progress: Download completed successfully. The reset command sent to the AP.• Timed-Out: The AP did not reconnect to the controller in the fixed time interval. |
| AP MAC | The managed AP MAC address. |
| Location | The location of the managed AP. |
| Status | Refer to Status (per-AP) above. |
| Firmware Version | The current firmware version of the managed AP. |

Advanced Network Configuration

While the basic configuration described in the previous chapter is satisfactory for most users, large wireless networks or a complex setup may require the wireless controller's advanced configuration settings to be configured.

This chapter covers the following commonly used advanced configuration settings.

- "IP Mode" on page 115
- "IPv4 LAN Settings" on page 116
- "IPv6 LAN Settings" on page 118
- "VLANs" on page 130
- "Configure IPv4 Static Routing" on page 142
- "Configure IPv6 Static Routing" on page 144
- "QoS Configuration" on page 147

Note: *The procedures in this chapter should only be performed by expert users who understand networking concepts and terminology.*

IP Mode

Path: Network > LAN > IP Mode

This page allows user to configure the IP protocol version to be used on the controller. In order to support IPv6 on the LAN, you must set the controller to be in IPv4 / IPv6 mode. This mode will allow IPv4 nodes to communicate with IPv6 devices through this controller.

1. Go to **Network > IPv6 > IP Mode**.



2. Next to *IP Mode*, select either **IPv4 only** or **IPv4 & IPv6**.
3. Click **Save**.

LAN Configuration

IPv4 LAN Settings

Path: Network > LAN > LAN Settings > IPv4 LAN Settings

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

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

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

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

1. Click **Network > LAN > LAN Settings > IPv4 LAN Settings**.

D-Link
Unified Controller - DWC 2000

Serial Number: 0000000000001 | Firmware Version: 4.2.0.3_WW | Language: English [US]

Logged in as: admin (ADMIN) | Logout

Wizard | System Search...

Status | Wireless | Network | Security | Maintenance

Network > LAN > LAN Settings > IPv4 LAN Settings

IPv4 LAN Settings | IPv6 LAN Settings | IPv6 Address Pools | IPv6 Prefix Length | Router Advertisement | Advertisement Prefixes

The LAN Configuration page allows you to configure the LAN interface of the controller including the DHCP Server which runs on it and Changes here affect all devices connected to the controller's LAN switch and also wireless LAN clients. Note that a change to the LAN IP address will require all LAN hosts to be in the same subnet and use the new address to access this GUI.

LAN Settings

IP Address Setup

IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0

DHCP Setup

DHCP Mode: None

Domain Name: DLink

Default Route

Enable Default Route: OFF

SNAT: OFF

DNS Host Name Mapping

| Host Name | IP Address |
|-----------|------------|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

2. Complete the fields in the table below and click **Save**.

| Field | Description |
|------------------------------|--|
| IP Address Setup | |
| IP Address | LAN interface IP address of the wireless controller. |
| Subnet Mask | The factory default: 255.255.255.0. |
| DHCP Setup | |
| DHCP Mode | <p>There are three DHCP modes to choose from:</p> <ul style="list-style-type: none"> • None: the controller's DHCP server is disabled for the LAN • DHCP Server. With this option the controller assigns an IP address within the specified range plus additional specified information to any LAN device that requests DHCP served addresses. • DHCP Relay: With this option enabled, DHCP clients on the LAN can receive IP address leases and corresponding information from a DHCP server on a different subnet. Specify the Relay Gateway, and when LAN clients make a DHCP request it will be passed along to the server accessible via the Relay Gateway IP address. |
| Domain Name | Enter a domain name. |
| Starting IP Address | If DHCP mode = DHCP Server: Enter the first IP address in the range. Any new DHCP client joining the LAN will be assigned an IP address between this address and the Ending IP Address. |
| Ending IP Address | If DHCP mode = DHCP Server: Enter the last IP address in the range of addresses to lease to LAN hosts. Any new DHCP client joining the LAN will be assigned an IP address between the Starting IP Address and this IP address. |
| Default Gateway | If DHCP mode = DHCP Server: Enter the default gateway. |
| Gateway | If DHCP mode= DHCP Relay. Enter the relay gateway address. |
| Default Route | |
| Enable Default Route | Enable or disable (ON=enabled) the default route function. |
| Gateway | If Enable Default Route=ON, enter the Gateway IP address. |
| DNS Server | If Enable Default Route= ON, enter the DNS Server IP address. |
| SNAT | Enable or disable SNAT (Source Network Address Translation). Enable SNAT if you have set up VLANs on your LAN network and it needs NAT to translate the source and origin address. |
| DNS Host Name Mapping | |
| Host Name | Enter a DNS host name. |
| IP Address | Enter the IP address of the DNS host name. |
| LAN Proxy | |
| Active DNS Proxy | <p>Enable or disable DNS proxy on this LAN.</p> <p>When this feature is enabled, the controller will act as a proxy for all DNS requests and communicate with the ISP's DNS servers (as configured in the Option settings page). All DHCP clients will receive the Primary/Secondary DNS IP along with the IP where the DNS Proxy is running, i.e. the box's LAN IP. All DHCP clients will receive the DNS IP addresses of the ISP excluding the DNS Proxy IP address when it is disabled. The feature is particularly useful in Auto Rollover mode. For example, if the DNS servers for each connection are different, then a link failure may render the DNS servers inaccessible. However, when the DNS proxy is enabled, then clients can make requests to the controller and in turn, sends those requests to the DNS servers of the active connection.</p> |

IPv6 LAN Settings

Path: Network > IPv6 > LAN Setting > IPv6 LAN Settings

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

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

1. Go to **Network > IPv6 > LAN Settings > IPv6 LAN Settings** tab.

D-Link
Unified Controller - DWC 2000

Serial Number: 0000000000001 | Firmware Version: 4.2.0.3_WW | Language: English [US]

Logged in as: admin (ADMIN) | Logout

Wizard | System Search...

Status | Wireless | Network | Security | Maintenance

Network > LAN > LAN Settings > IPv6 LAN Settings

IPv4 LAN Settings | **IPv6 LAN Settings** | IPv6 Address Pools | IPv6 Prefix Length | Router Advertisement | Advertisement Prefixes

This page allows user to IPv6 related LAN configurations. The IPv6 address is 128 bits, with a default 64 bit prefix that defines the network and is common among all LAN hosts. Changes here affect all devices connected to the controller's LAN switch. Note that a change to the default LAN IP address will require all LAN hosts to be in the same network prefix and use the new address to access this GUI.

IPv6 LAN Settings

LAN TCP/IP Setup

IPv6 Address:

IPv6 Prefix Length: [Range: 0 - 128]

DHCPv6

Status: ☒ ON ☐ OFF

Mode: ☒ Stateless ☐ Stateful

Domain Name:

Server Preference: [Range: 0 - 255]

DNS Servers:

Lease / Rebind Time: [Range: 0 - 604800] Seconds

Prefix Delegation: ☐ OFF

2. Complete the fields in the table below and on the next page.
3. Click **Save**.

| Field | Description |
|--------------------|---|
| LAN TCP/IP Setup | |
| IPv6 Address | The Wireless Controller's LAN IPv6 address. |
| IPv6 Prefix Length | The IPv6 network (subnet) is identified by the initial bits of the address called the prefix. All hosts in the network have the identical initial bits for their IPv6 address; the number of common initial bits in the networks addresses is set by the prefix length field. |

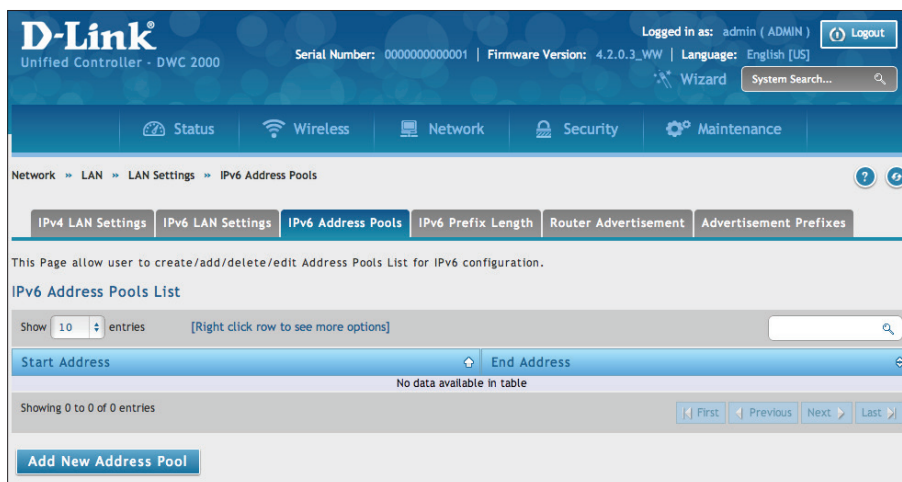
| Field | Description |
|----------------------------------|--|
| DHCPv6 | |
| Status | Toggle On to enable DHCPv6. It is disabled in default. |
| If DHCPv6 is Enabled (ON) | |
| Mode | <p>There are two ways to obtain an appropriate address for the gateway. You must select one of the following:</p> <ul style="list-style-type: none"> • Stateless Address Auto Configuration: This option will use router advertisement for address assignment. The IPv6 RADVD protocol will be enabled to advertise this controller as a DHCPv6 client. • Stateful Address Auto Configuration: Select this option to request an IPv6 address from any available DHCPv6 servers available on the ISP. |
| Domain Name | Name of the domain (Optional) for this DHCPv6 server. |
| Server Preference | This is used by the stateless DHCP to indicate the preference level of this DHCP server. DHCPv6 clients will pick up the DHCPv6 server which has highest preference value. The preference value must be a decimal integer and be between 0 and 255 (inclusive). |
| DNS Servers | <p>Select one of the following options for DNS servers for the DHCPv6 clients</p> <ul style="list-style-type: none"> • Use DNS Proxy: On button to enable DNS proxy on this LAN, or Off this button to disable this proxy. When this feature is enabled, the controller will act as a proxy for all DNS requests and communicate with the ISP's DNS servers (as configured in the Option settings page) • Use DNS from ISP: This option allows the ISP to define the DNS servers (primary/secondary) for the LAN DHCP client • Use below: if selected, the below configured Primary and Secondary DNS servers are used for DHCPv6 clients. |
| Primary DNS Server | Enter the primary DNS server address. |
| Secondary DNS Server | Enter the secondary DNS server address. |
| Lease/Rebind Time | Duration (in seconds) for which IP addresses will be leased to clients. |
| Prefix Delegation | On/Off button for Enable/Disable Prefix Delegation. |

IPv6 Address Pools

Path: Network > IPv6 > LAN Setting > IPv6 Address Pools/ Prefix Delegation

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

1. Go to **Network > LAN > LAN Settings > IPv6 Address Pools** tab.



2. Click **Add New Address Pool**.

The screenshot shows a dialog box titled 'IPv6 Address Pools Configuration'. It contains three input fields: 'Start IPv6 Address', 'End IPv6 Address', and 'Prefix Length'. The 'Prefix Length' field has a range indicator '[Range: 0 - 128]'. A 'Save' button is located at the bottom right of the dialog box.

3. Enter a starting IPv6 address, end IPv6 address, and the prefix length.
4. Click **Save**.

- Go to **Network > LAN > LAN Settings > IPv6 Prefix Length** tab.

The screenshot shows the D-Link Unified Controller - DWC 2000 web interface. The top navigation bar includes links for Status, Wireless, Network, Security, and Maintenance. The main content area is titled "IPv6 Prefix Length" and contains a table for managing the IPv6 Prefix Length List. The table is currently empty, showing "No data available in table". A button labeled "Add New Prefix Length" is visible at the bottom of the table area.

- Click **Add New Prefix Length**.

The screenshot shows the "IPv6 Prefix Length Configuration" dialog box. It contains two input fields: "Prefix" and "Prefix Length". The "Prefix Length" field has a range indicator "[Range: 0 - 128]". A "Save" button is located at the bottom right of the dialog box.

- Enter the IPv6 Prefix and Prefix Length. Click **Save**.

IPv6 Router Advertisement

Path: Network > LAN > LAN Settings > Router Advertisement

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

1. Go to **Network > LAN > LAN Settings > Router Advertisement** tab.

The screenshot displays the D-Link Unified Controller - DWC 2000 web interface. The top navigation bar includes links for Status, Wireless, Network, Security, and Maintenance. The main content area is titled 'Router Advertisement' and contains a sub-section 'Router Advertisement Daemon Setup'. This section includes the following configuration options:

- Status:** A toggle switch set to 'ON'.
- Advertise Mode:** Radio buttons for 'Unsolicited Multicast' (selected) and 'Unicast Only'.
- Advertise Interval:** A text input field set to '30', with a range of '10 - 1800'.
- RA Flags:**
 - Managed:** A toggle switch set to 'OFF'.
 - Other:** A toggle switch set to 'ON'.
 - Router Preference:** Radio buttons for 'Low', 'Medium', and 'High' (selected).
 - MTU:** A text input field set to '1500', with a range of '1280 - 1500'.
 - Router Lifetime:** A text input field set to '3600', with the unit 'Seconds'.

At the bottom of the configuration section are 'Save' and 'Cancel' buttons.

2. Complete the fields from the table on the next page.
3. Click **Save**.

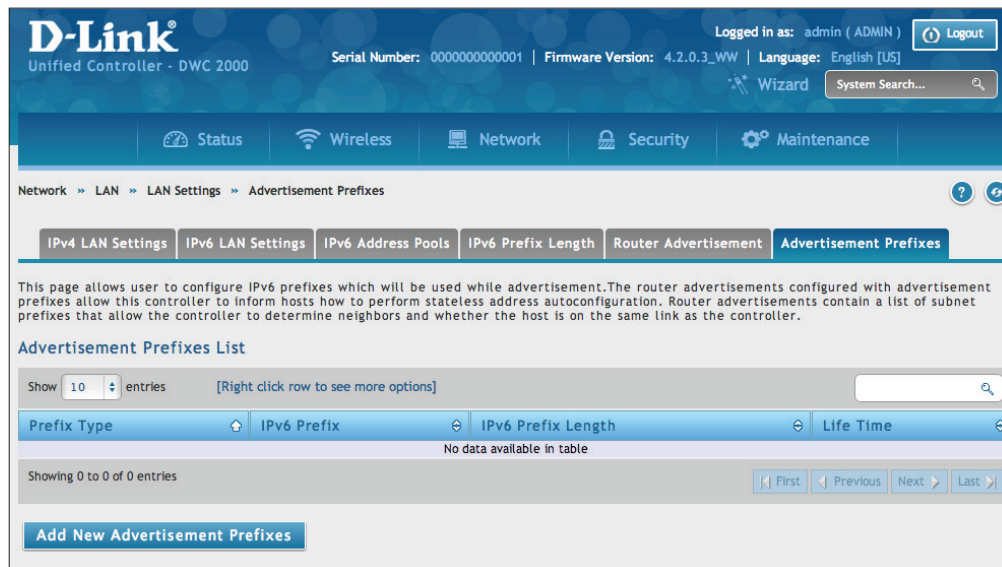
| Field | Description |
|--------------------|--|
| Status | Enable or disable the RADVD process here to allow stateless auto configuration of the IPv6 LAN network. |
| Advertise Mode | Two Advertise Modes: <ul style="list-style-type: none">• Unsolicited Multicast: select to send router advertisements (RA's) to all interfaces belonging to the multicast group.• Unicast Only: This option restricts advertisements to well known IPv6 addresses only (RA's are sent to the interface belonging to the known address only). |
| Advertise Interval | If Advertise Mode = Unsolicited Multicast, this sets the maximum advertise interval. The advertise interval used when RADVD is enabled is a random value between Minimum Router Advertisement Interval and Maximum Router Advertisement Interval. The minimum router advertisement interval is 1/3 of this configured value, and the default is 30 seconds. |
| RA Flags | The router advertisements (RA's) can be sent with one or both of these flags: Managed and Other.. Chose Managed to use the administered /stateful protocol for address auto configuration. If the Other flag is selected the host uses administered/stateful protocol for non-address auto configuration. |
| Router Preference | Choose between Low/Medium/High for the preference associated with the RADVD process of the controller. This feature is useful if there are other RADVD enabled devices on the LAN. The default is high. |
| MTU | This is used in RA's to ensure all nodes on the network use the same MTU value in the cases where the LAN MTU is not well known. The default is 1500 |
| Router Lifetime | The lifetime in seconds of the route. The default is 3600 seconds. |

IPv6 Advertisement Prefixes

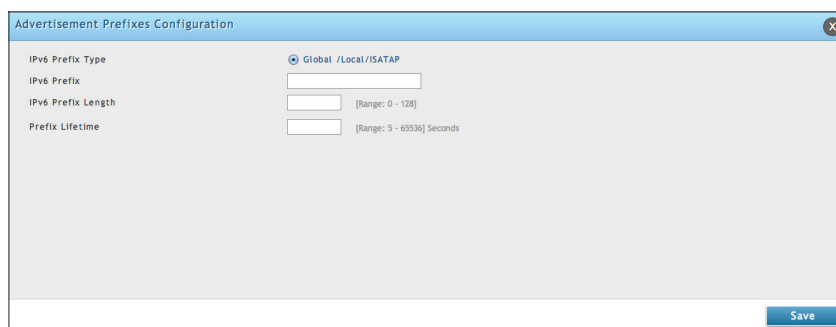
Path: Network > LAN Setting > Advertisement Prefixes

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

1. Go to **Network > LAN Settings > Advertisement Prefix** tab.



2. Click **Add New Advertisement Prefixes**.



3. Complete the fields from the table below.
4. Click **Save**.

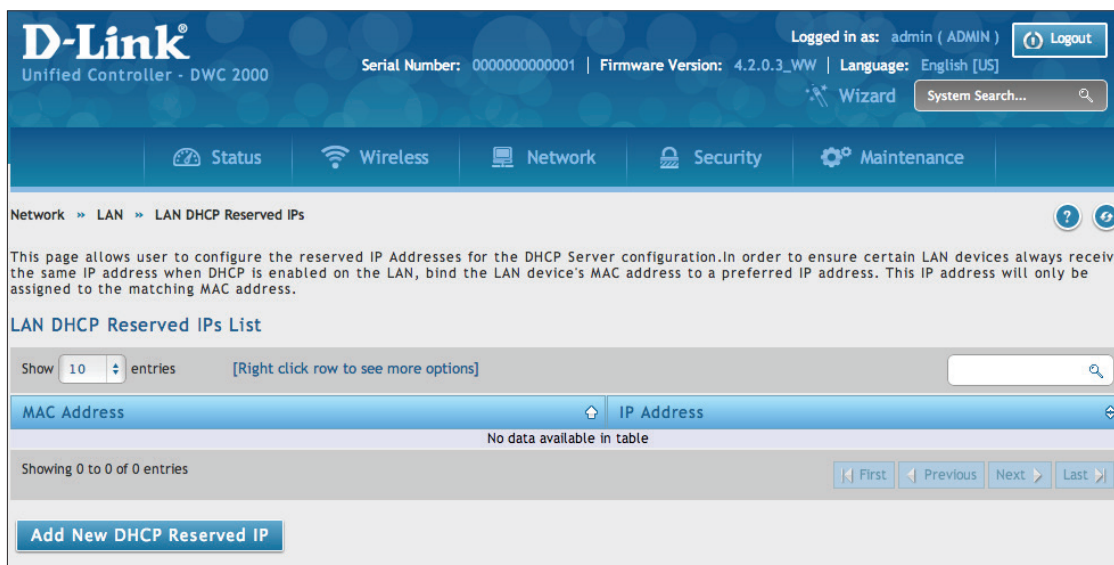
| Field | Description |
|--------------------|---|
| IPv6 Prefix Type | Select the prefix type as 6to4 or Global/Local/ISATAP. |
| SLA ID | If Ipv6 Prefix Type= 6to4, the SLA ID (Site-Level Aggregation Identifier) in the 6to4 address prefix is set to the interface ID of the interface on which the advertisements are sent. |
| IPv6 Prefix | If IPv6 Prefix Type= Global / Local / SATAP, then defines the IPv6 network address. |
| IPv6 Prefix Length | If Ipv6 Prefix Type= Global/ Local/ SATAP, and this is a numeric value that indicates the number of contiguous, higher order bits of the address that make up the network portion of the address. |
| Prefix Lifetime | The length of time over which the requesting controller is allowed to use the prefix. |

LAN DHCP Reserved IPs

Path: Network > LAN > LAN DHCP Reserved IPs

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

1. Click **Network > LAN > LAN DHCP Reserved IPs**.



2. Click **Add New DHCP Reserved IP**.

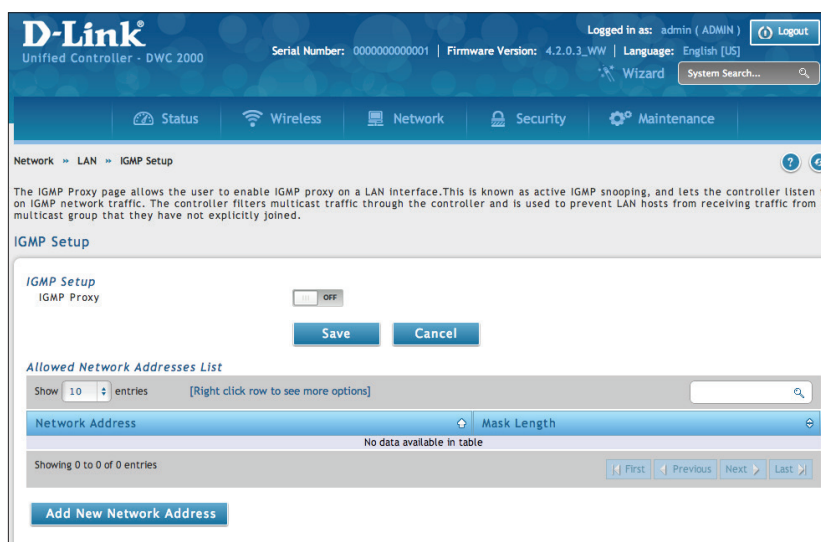
3. Enter the IP address you want to reserve and the MAC Address of the client you want to assign the IP address to.
4. Click **Save**

Configure IGMP Setup

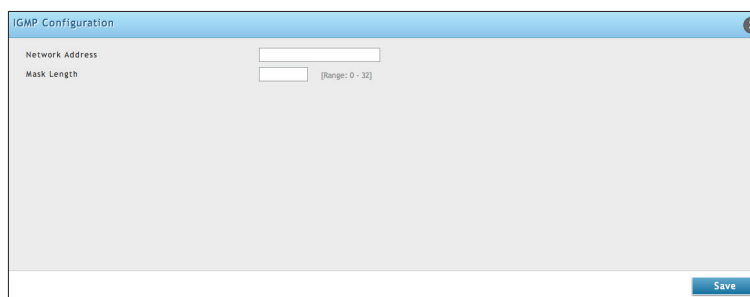
Path: Network > LAN > IGMP Setup

IGMP snooping allows the controller to 'listen' in on IGMP network traffic through the controller. This then allows the controller to filter multicast traffic and direct this only to hosts that need this stream. This is helpful when there is a lot of multicast traffic on the network (say from an IPTV application) where all LAN hosts do not need to receive this multicast traffic. Enabling IGMP snooping allows the controller to regulate the amount of multicast traffic on the network, to prevent flooding all LAN hosts. Active IGMP snooping is referred to IGMP Proxy, and this is available on your controller.

1. Click **Network > LAN > IGMP Setup**.



2. Next to IGMP Proxy, toggle to **ON**.
3. Click **Save**.
4. Click **Add New Network Address** to specify the IP network and host addresses of the multicast sources.



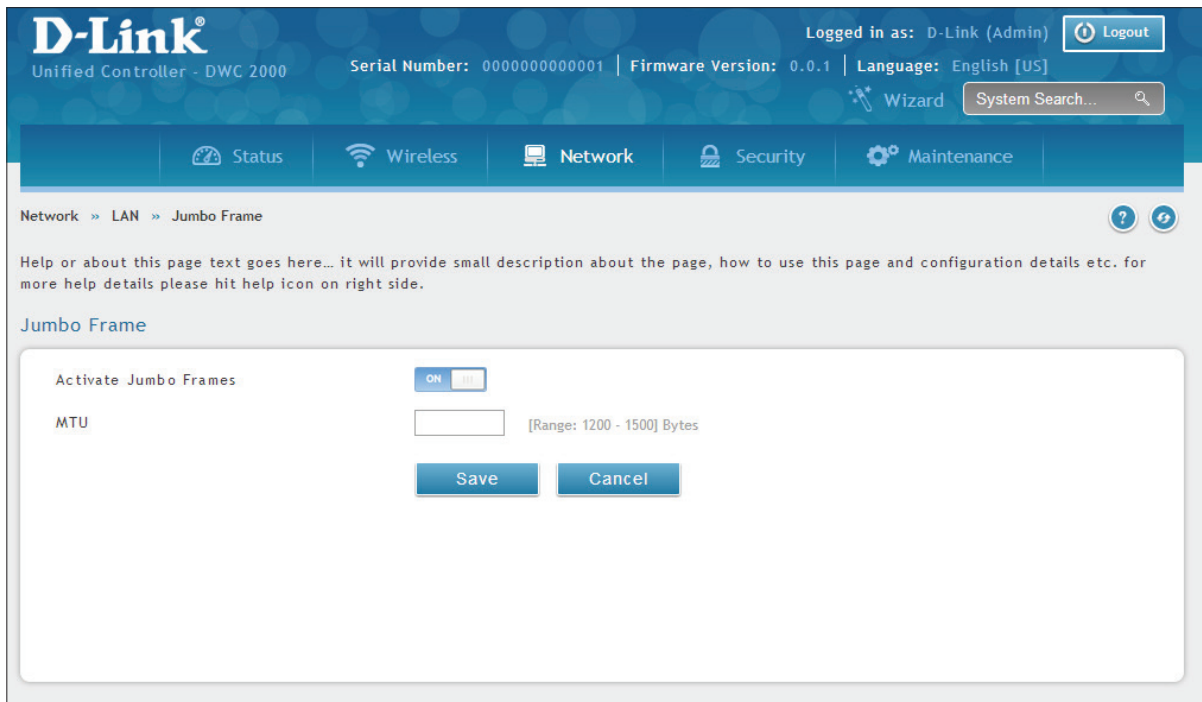
5. Enter the network address and mask length. Click **Save**.

Configure Jumbo Frames

Path: Network > LAN > Jumbo Frame

Jumbo frames are Ethernet frames with more than 1500 bytes of payload. When this option is enabled, the LAN devices can exchange information at Jumbo frames rate.

1. Click **Network > LAN > Jumbo Frame**.



The screenshot shows the D-Link Unified Controller web interface. The top header includes the D-Link logo, 'Unified Controller - DWC 2000', and system information: 'Serial Number: 0000000000001', 'Firmware Version: 0.0.1', and 'Language: English [US]'. A 'Logout' button is in the top right. Below the header is a navigation bar with tabs for Status, Wireless, Network, Security, and Maintenance. The 'Network' tab is selected, and the breadcrumb path 'Network > LAN > Jumbo Frame' is shown. A help icon is visible. Below the breadcrumb is a placeholder text: 'Help or about this page text goes here... it will provide small description about the page, how to use this page and configuration details etc. for more help details please hit help icon on right side.' The main content area is titled 'Jumbo Frame' and contains a configuration form. The form has a toggle switch for 'Activate Jumbo Frames' set to 'ON'. Below it is an input field for 'MTU' with a range of '[Range: 1200 - 1500] Bytes'. At the bottom of the form are 'Save' and 'Cancel' buttons.

2. Toggle Activate Jumbo Frames to **On** and enter a MTU value.
3. Click **Save**.

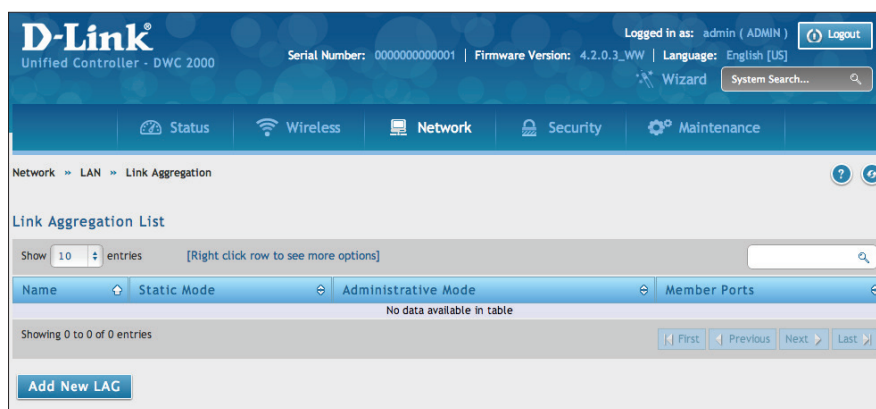
Link Aggregation

Path: Network > LAN > Link Aggregation

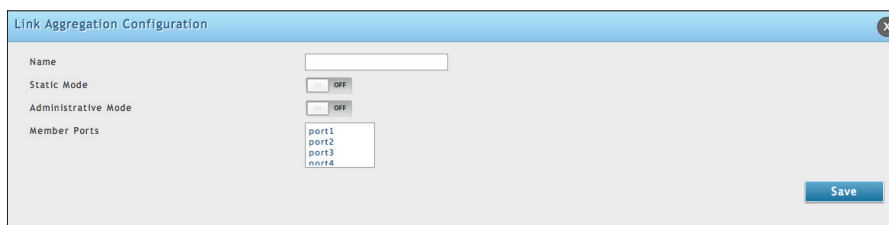
Link aggregation is used to combine a number of ports together to make a single high-bandwidth data pipeline. The controller treats all ports in a trunk group as a single port.

Link Aggregation Control Protocol (LACP) is used to negotiate a dynamic aggregated link between the controller and another network device that supports 802.3ad. For this to work, the controllers must comply with LACP to allow negotiation of the aggregated link.

1. Click **Network > LAN > Link Aggregation**.



2. Click **Add New LAC**. The following window will appear.



3. Complete the fields in the table below and click **Save**.

| Field | Description |
|----------------------------|--|
| Name | Enter a name for this configuration. |
| Static Mode | Activates or deactivates the Static Mode. Choices are: <ul style="list-style-type: none"> • ON = Use static mode. • OFF = Use dynamic mode (LACP). |
| Administrative Mode | Enables or disables this configuration. <ul style="list-style-type: none"> • ON = Enabled • OFF = Disabled |
| Member Ports | Select the ports to add to the configuration (ports 1-4). Hold CTRL and click for multiple ports. |

* Maximum four interfaces aggregate into one logical interface.

VLANs

A virtual Local Area Network (VLAN) is a logical segment in a switched network. It allows independent logical networks to be created within a single physical network. VLANs separate devices into different broadcast domains and Layer 3 subnets. Devices within a VLAN can communicate without routing. The primary use of VLANs is to split large switched networks, which are large broadcast domains.

The wireless controller provides VLAN functionality for assigning unique VLAN IDs to LAN ports so that traffic to and from that physical port can be isolated from the general LAN. VLAN filtering is particularly useful to limit broadcast packets of a device in a large network.

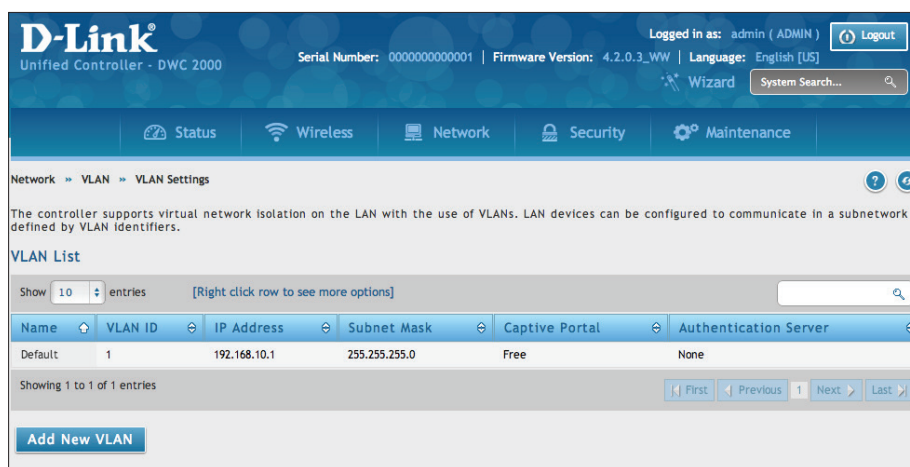
Creating VLANs

Path: Network > VLAN > VLAN Settings

You can create VLANs on the VLAN Settings page. After you create VLANs, you can use the same page to view, edit, and delete VLANs.

To create a VLAN:

1. Go to **Network > VLAN > VLAN Settings**.



2. Click **Add New VLAN**. The following pop-up box will appear.

The screenshot shows the 'VLAN Configuration' pop-up box. It contains the following fields and options:

- VLAN ID**: A text input field with a hint '[Default: 1, Range: 2 - 4093]'.
- Name**: A text input field.
- Activate InterVLAN Routing**: A checkbox set to 'OFF'.
- Captive Portal Type**: A dropdown menu set to 'Free'.
- Multi VLAN Subnet**: A section with two text input fields for **IP Address** and **Subnet Mask**.
- DHCP**: A section with a **DHCP Mode** dropdown menu set to 'None', and radio buttons for 'None', 'DHCP Server', and 'DHCP Relay'.
- LAN Proxy**: A section with an **Enable DNS Proxy** checkbox set to 'OFF'.
- Save**: A button at the bottom right.

3. Complete the fields in the table below and click **Save**.

| Field | Description |
|----------------------------|---|
| VLAN ID | Enter a unique ID to this VLAN (2 - 4093). |
| Name | Enter a unique name for this VLAN. The name should allow you to easily identify this VLAN from others you may add. |
| Activate InterVLAN Routing | Allows or denies communication between VLAN networks. Choices are: <ul style="list-style-type: none">• Checked = allow communications between different VLANs.• Unchecked = deny communications between different VLANs. |
| Captive Portal Type | Select the type of captive portal from free, SLA, Permanent User, Temporary User, or Billing User. |
| Authentication Server | Select the type of authentication server to authenticate captive portal for permanent, temporary, or billing users. |
| Login Profile Name | Select a captive portal from the drop-down menu. Click Create a Profile to create a new profile. |
| IP Address | Enter an IP address for the Multi-VLAN subnet. |
| Subnet Mask | Enter the subnet mask for the Multi-VLAN subnet. |
| DHCP Mode | Select whether to enable DHCP Server or DHCP Relay. |
| LAN Proxy | Click to enable DNS proxy. |

Editing VLANs

Path: Network > VLAN > VLAN Settings

To edit a VLAN:

1. Go to **Network > VLAN > VLAN Settings**.
2. Under VLAN List, right-click the VLAN you want to edit and click **Edit**. The following page will appear.
3. Edit the fields in the table on the previous page and click **Save**.

Deleting VLANs

Path: Network > VLAN > VLAN Settings

If you no longer need a VLAN, you can delete it.

Note: A precautionary message does not appear before you delete a VLAN. Therefore, be sure you do not need a VLAN before you delete it.

To delete a VLAN:

1. Go to **Network > VLAN > VLAN Settings**.
2. In the VLAN List, right-click the VLAN you want to delete and click **Delete**. (Or right-click on a VLAN and click **Select All**, then **Delete** to delete all VLANs.) The selected VLAN(s) will be deleted.

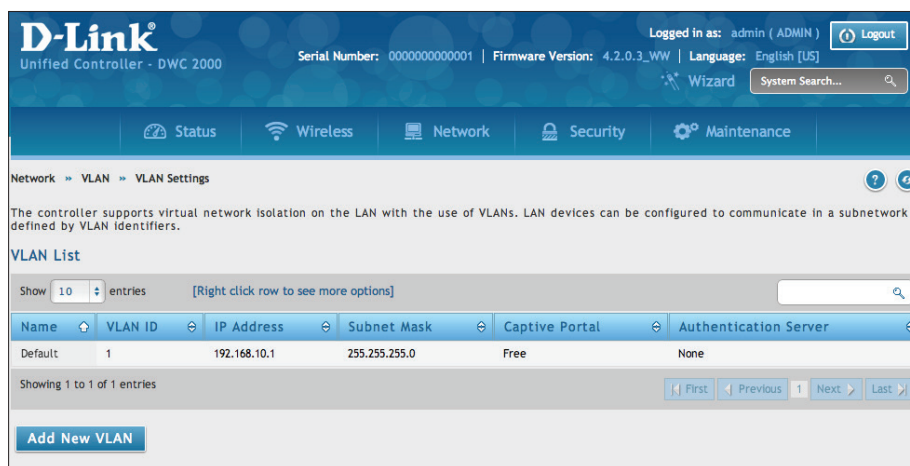
MultiVLAN Subnets

Path: Network > VLAN > VLAN Settings

Each VLAN can be assigned a unique IP address and subnet mask for the virtually isolated network. Unless you enabled inter-VLAN routing for the VLAN, the VLAN subnet determines the network address on the LAN that can communicate with the devices that correspond to the VLAN.

To view and edit the available multi-VLAN subnets:

1. Go to **Network > VLAN > VLAN Settings**.



2. To edit a multi-subnet VLAN, right-click the VLAN and click **Edit**.

The screenshot shows the 'VLAN Configuration' dialog box. It contains the following fields and options:

- Multi VLAN Subnet**
 - IP Address: [Text Field]
 - Subnet Mask: [Text Field]
- DHCP**
 - DHCP Mode: ☐ None ☒ DHCP Server ☐ DHCP Relay
 - Domain Name: [Text Field]
 - Starting IP Address: [Text Field]
 - Ending IP Address: [Text Field]
 - Default Gateway: [Text Field]
 - Primary DNS Server: [Text Field]
 - Secondary DNS Server: [Text Field]
 - Lease Time: [Text Field] [Range: 0 - 262800] Hours
- LAN Proxy**: [Text Field]
- Save** button at the bottom right.

2. Edit the settings as desired (refer to the table below) and click **Save**.

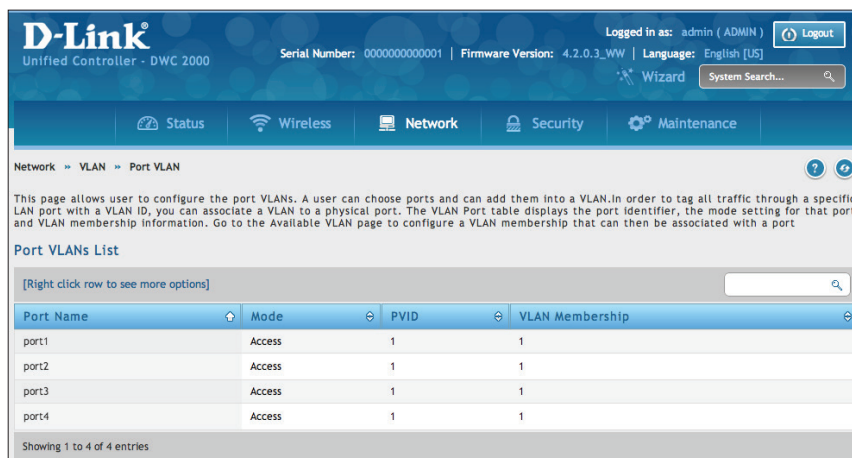
| Field | Description |
|-----------------------------|--|
| MultiVLAN Subnet | |
| IP Address | Edit the IP address for the Multi-VLAN subnet. |
| Subnet Mask | Edit the subnet mask for the Multi-VLAN subnet. |
| DHCP | |
| DHCP Mode | <p>Select a DHCP mode for the VLAN. Choices are:</p> <ul style="list-style-type: none"> • None: Select this setting if the computers on the LAN are configured with static IP addresses or are configured to use another DHCP server. The remaining fields become unavailable. • DHCP Server: Select this setting to use the wireless controller as a DHCP server. Complete the remaining settings on the page. • DHCP Relay: If you select this setting, you need only enter the relay gateway information. |
| Domain Name | Enter the domain name for the VLAN. |
| Starting IP Address | Enter the starting IP address in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address within the starting and ending IP address range. Starting and ending IP addresses should be in the same IP address subnet as the wireless controller's LAN IP address. |
| Ending IP Address | Enter the ending IP address in the IP address pool. |
| Default Gateway | (Optional) Enter the IP address of the gateway for your LAN. |
| Primary DNS Server | (Optional) If configured domain name system (DNS) servers are available on the VLAN, enter the IP address of the primary DNS server. |
| Secondary DNS Server | (Optional) If configured domain name system (DNS) servers are available on the VLAN, enter the IP address of the secondary DNS server. |
| Lease Time | Enter a time interval, in hours that a DHCP client can use the IP address that it receives from the DHCP server. When the lease time is about to expire, the client sends a request to the DHCP server to get a new lease. |
| Relay Gateway | Enter the gateway address. This is the only configuration parameter required in this section when DHCP Mode = DHCP Relay. |
| LAN Proxy | |
| Enable DNS Proxy | <p>Enables or disables DNS proxy on this LAN. The feature is particularly useful in Auto Rollover mode. For example, if the DNS servers for each connection are different, a link failure can render the DNS servers inaccessible. However, when the DNS proxy is enabled, clients can make requests to the wireless controller and the controller, in turn, sends those requests to the DNS servers of the active connection. Choices are:</p> <ul style="list-style-type: none"> • Checked - The wireless controller acts as a proxy for all DNS requests and communicates with the ISP's DNS servers (as configured in the Option settings page). All DHCP clients receive the primary and secondary DNS IP addresses, along with the IP address where the DNS proxy is running (i.e., the wireless controller's LAN IP). • Unchecked - All DHCP clients receive the DNS IP addresses of the ISP, excluding the DNS proxy IP address. |

Port VLANs

Path: Network > VLAN > Port VLAN

After you enable the wireless controller's VLAN function, use the Port VLAN page to configure the ports participating in the VLAN.

1. Go to **Network > VLAN > Port VLAN**.



2. Select the port and right-click **Edit**.



3. Change Mode and PVID. There are four modes:

- **Access:** Select to isolate this port from other VLANs. All data going into and out of the port is untagged. Traffic through a port in access mode looks like any other Ethernet frame.
- **General:** Select to allow the port to become a member of a user selectable set of VLANs. The port sends and receives data that is tagged or untagged with a VLAN ID. If the data into the port is untagged, it is assigned the defined PVID. All tagged data sent out of the port with the same PVID will be untagged.
- **Trunk:** Select to multiplex traffic for multiple VLANs over the same physical link. All data going into and out of the port is tagged. Untagged coming into the port is not forwarded, except for the default VLAN with PVID=1, which is untagged.
- **Interface:** Select to make it as a standalone interface. Manually define the interface IP address, subnet mask, and gateway.

4. Click **Save**.

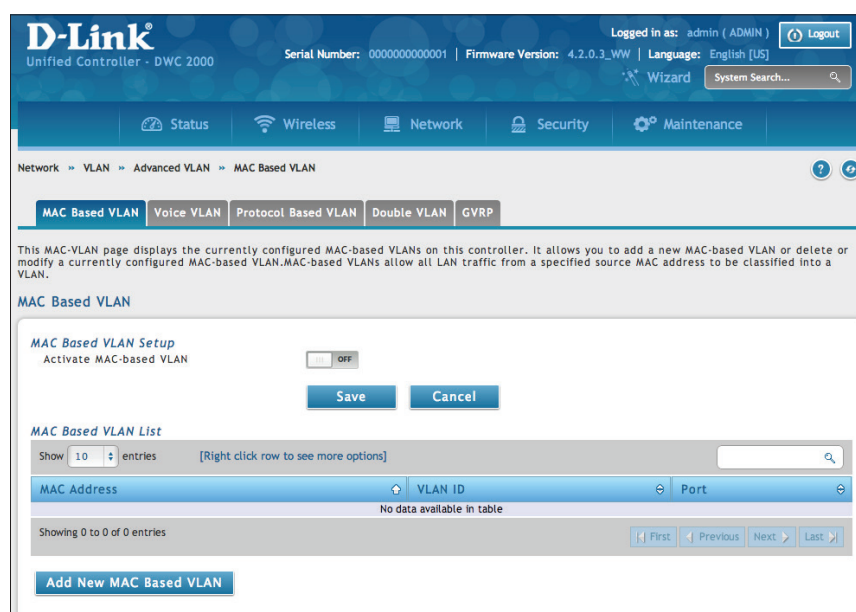
MAC Based VLANs

Path: Network > VLAN > Advanced VLAN > MAC Based VLAN

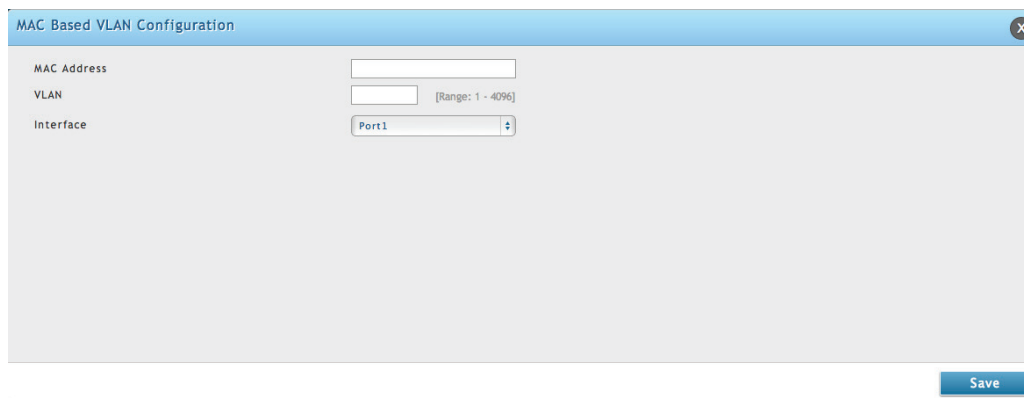
If a packet is untagged or priority tagged, the device shall associate it with the VLAN which corresponds to the source MAC address in its MAC-based VLAN tables. If there is no matching entry in the table, then the packet is subject to normal VLAN classification rules of the device.

Use the MAC-based VLAN Configuration page to map a MAC entry to the VLAN table. After the source MAC address and the VLAN ID are specified, the MAC-to-VLAN configurations are shared across all ports of the controller.

1. Go to **Network > VLAN > Advanced VLAN > MAC Based VLAN** tab.



2. Toggle *Activate MAC-based VLAN* to **ON** and click **Save**.
3. Click **Add New MAC Based VLAN**.



4. Complete the fields in the table below and click **Save**.

| Field | Description |
|-------------|--|
| MAC Address | Enter the MAC address of the client you want to add to a VLAN. |
| VLAN | Enter the VLAN ID number. |
| Interface | Select a port from the drop-down menu. |

Voice VLANs

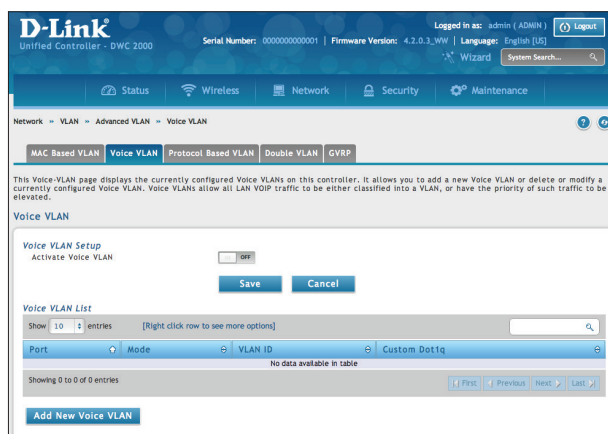
Path: Network > VLAN > Advanced VLAN > Voice VLAN

The voice VLAN feature enables controller ports to carry voice traffic with defined settings so that voice and data traffic are separated when coming onto the port. A voice VLAN ensures that the sound quality of an IP phone is safeguarded from deterioration when data traffic on the port is high.

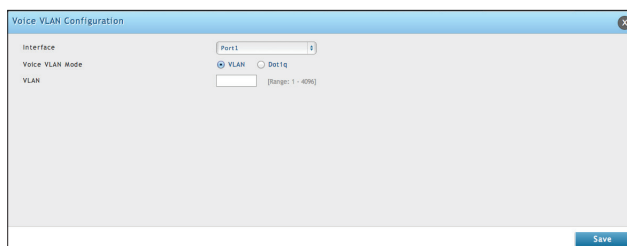
The inherent isolation provided by VLANs ensures that inter-VLAN traffic is under management control and that network-attached clients cannot initiate a direct attack on voice components. A QoS protocol based on the IEEE 802.1P class-of-service (CoS) protocol uses classification and scheduling to send network traffic from the controller in a predictable manner. The system uses the source MAC of the traffic traveling through the port to identify the IP phone data flow.

Voice VLAN is enabled per-port basis. A port can participate only in one voice VLAN at a time. The Voice VLAN feature is disabled by default.

1. Go to **Network > VLAN > Advanced VLAN > Voice VLAN** tab.



2. Toggle *Activate Voice VLAN* to **ON** and click **Save**.
3. Click **Add New Voice VLAN**.



4. Select the interface and Voice VLAN mode.
 - **VLAN:** The voice VLAN packets are uniquely identified by a number you assign. All voice traffic carries this VLAN ID to distinguish it from other data traffic which is assigned the port's default VLAN ID. However, voice traffic is not prioritized differently than other traffic.
 - **Dot1q:** This parameter is set by the VoIP device for all voice traffic to distinguish voice data from other traffic. All other traffic is assigned the port's default priority.
5. Click **Save**.

Protocol Based VLANs

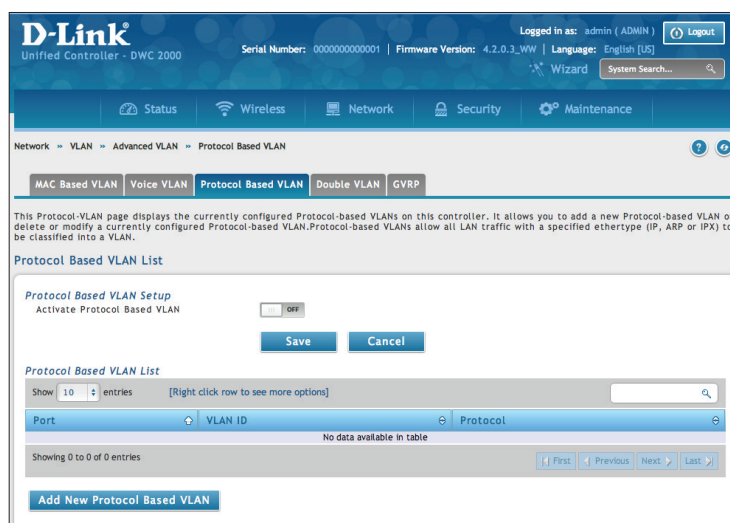
Path: Network > VLAN > Advanced VLAN > Protocol Based VLAN

In a protocol-based VLAN, traffic is bridged through specified ports based on the protocol associated with the VLAN. User-defined packet filters determine whether a particular packet belongs to a particular VLAN. Protocol-based VLANs are most often used in situations where network segments contain hosts running multiple protocols. You can use a protocol-based VLAN to define filtering criteria for untagged packets. By default, if you do not configure any port-based (IEEE 802.1Q) or protocol-based VLANs, untagged packets are assigned to VLAN 1. You can override this behavior by defining either port-based VLANs, protocol-based VLANs, or both. Tagged packets are always handled according to the IEEE 802.1Q standard and are not included in protocol-based VLANs.

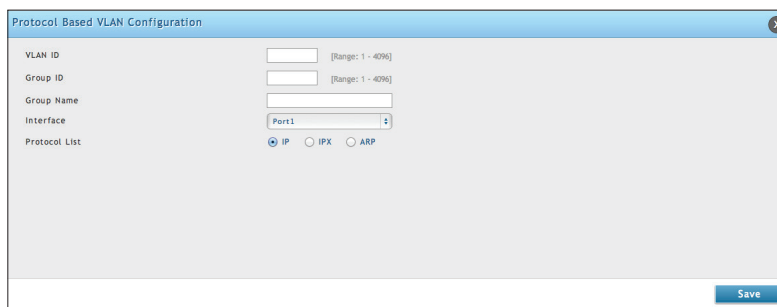
If you assign a port to a protocol-based VLAN for a specific protocol, untagged frames received on that port for that protocol will be assigned the protocol-based VLAN ID. Untagged frames received on the port for other protocols will be assigned the Port VLAN ID (PVID), which is either the default PVID (1) or a PVID you have specifically assigned to the port using the Port VLAN Configuration screen. Use the Protocol-based VLAN Configuration page to configure which protocols go to which VLANs, and then enable certain ports to use these settings.

You define a protocol-based VLAN by creating a group. Each group has a one-to-one relationship with a VLAN ID, can include one or more protocol definitions, and can include multiple ports.

1. Go to **Network > VLAN > Advanced VLAN > Protocol Based VLAN** tab.



2. Toggle *Activate Protocol Based VLAN* to **ON** and click **Save**.
3. Click **Add New Protocol Based VLAN**.



- Complete the fields in the table below and click **Save**.

| Field | Description |
|----------------------|---|
| VLAN ID | Specify the VLAN ID to associate with this group. The range is 1-3965. |
| Group ID | Identifies the group to configure. |
| Group Name | (Optional) Enter or modify a name to associate with protocol group ID. The name can be up to 16 characters. |
| Interface | Selects the interface(s) to add or remove from this group. |
| Protocol List | Specify one or more protocols to associate with this group. |

Double VLANs

Path: Network > VLAN > Advanced VLAN > Double VLAN

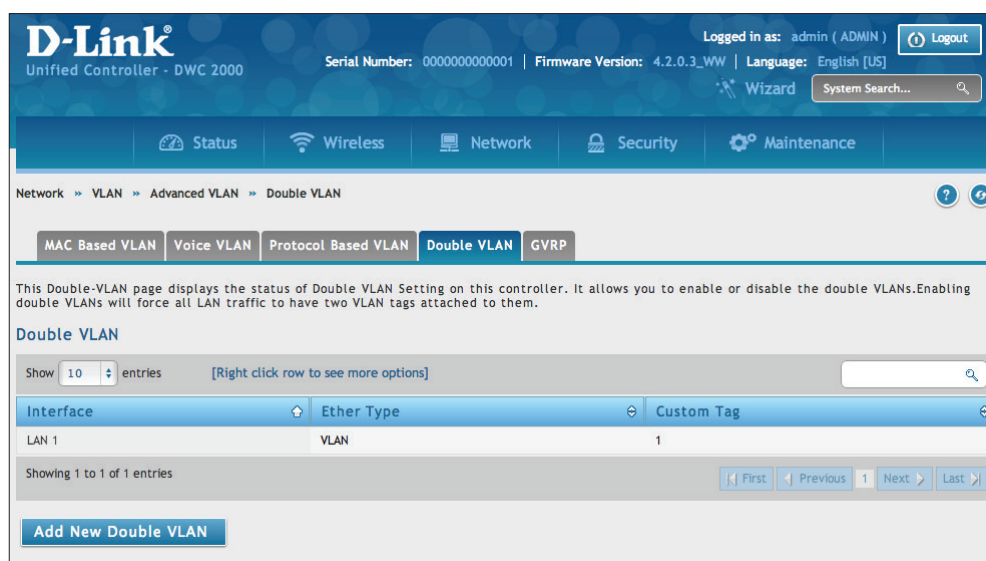
Double VLAN Tunneling allows the use of a second tag on network traffic. The additional tag helps differentiate between customers in the Metropolitan Area Networks (MAN) while preserving individual customer's VLAN identification when they enter their own 802.1Q domain.

With the introduction of this second tag, you do not need to divide the 4k VLAN ID space to send traffic on an Ethernet-based MAN.

With Double VLAN Tunneling enabled, every frame that is transmitted from an interface has a DVlan Tag attached while every packet that is received from an interface has a tag removed (if one or more tags are present).

Use the Double VLAN Tunneling page to configure Double VLAN frame tagging on one or more ports.

- Go to **Network > VLAN > Advanced VLAN > Double VLAN** tab.



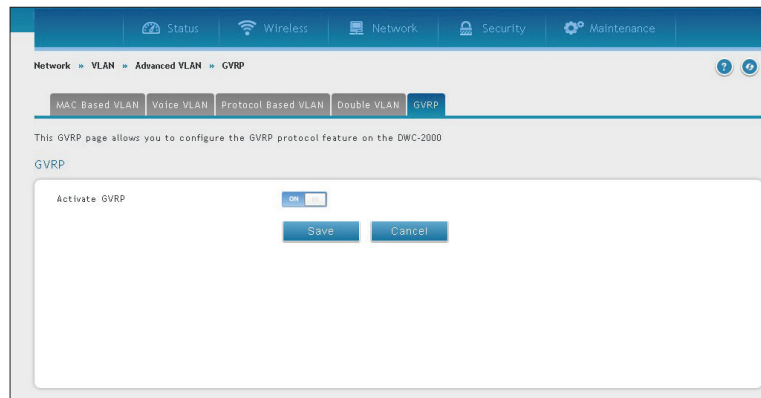
- Click **Add New Double VLAN**.
- Select the Ether Type: **Dot1q**, **VLAN**, or **Custom Tag**.
- Click **Save**.

GVRP

Path: Network > VLAN > Advanced VLAN > GVRP

The GARP VLAN Registration Protocol (GVRP) provides a mechanism that allows network controllers to dynamically register (and de-register) VLAN membership information with the networking devices attached the same segment, and for that information to be disseminated across all networking controllers in the bridged LAN that support GMRP.

1. Go to **Network > VLAN > Advanced VLAN > GVRP** tab.



2. Toggle *Activate GVRP* to **ON** and click **Save**.

Routing

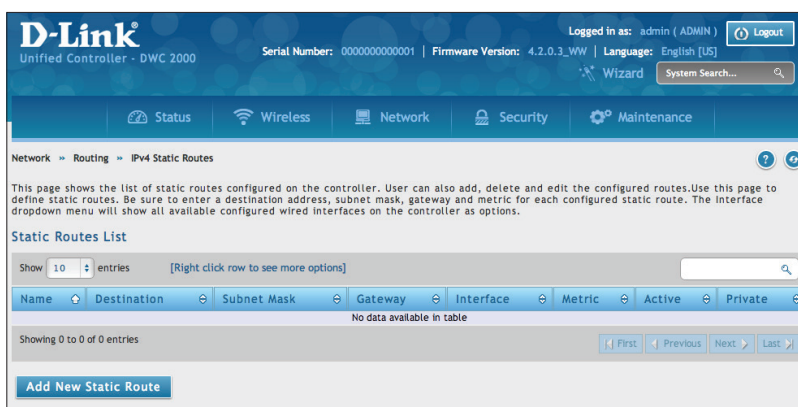
A static route tells network devices about an exact, fixed (hard-coded) destination. Static routes can work well with small networks. There are two kinds of static routing: Static Route and Protocol-Binding. The Static Route uses IP address to determine where is the next hop, whereas Protocol-Binding uses protocol. Configuring your wireless controller for static routing allows data transfers between it and a routing device without needing to use dynamic routing protocols.

Configure IPv4 Static Routing

Path: Network > Routing > IPv4 Static Routes

To add a static route:

1. Click **Network > Routing > IPv4 Static Routes**.



2. Click **Add New Static Route**. The Static Route Configuration page will appear.

3. Complete the fields in the table on the next page and click **Save**.

| Field | Description |
|------------------------|--|
| Route Name | Enter a unique name for this static route. The name should allow you to easily identify this static route from others you may add. |
| Active | Activates or deactivates the static route. Choices are: <ul style="list-style-type: none">• ON = activate static route.• OFF = deactivate static route. |
| Private | Designates the static route as private. Choices are: <ul style="list-style-type: none">• ON = static route is private.• OFF = static route is not private. |
| Destination IP Address | Enter the IP address of the static route's destination. |
| IP Subnet Mask | Enter the subnet mask of the static route. |
| Interface | Select the wireless controller interface that will interface to the static route. Choices are: <ul style="list-style-type: none">• LAN > VLAN: The wireless controller's LAN or VLAN port will interface to the static route. |
| Gateway IP Address | Enter the IP address of the gateway router, which is the next hop address for the wireless controller. |
| Metric | Enter the administrative distance of the route. |

Configure IPv6 Static Routing

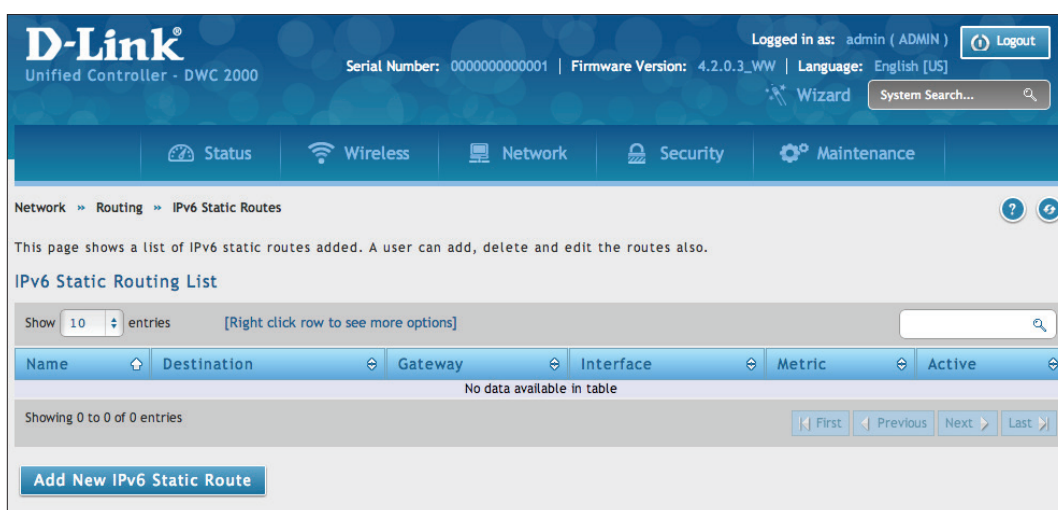
Path: Network > Routing > IPv6 Static Routing

Manually adding static routes to this device allows you to define the path selection of traffic from one interface to another. There is no communication between this controller and other devices to account for changes in the path; once configured the static route will be active and effective until the network changes.

The List of Static Routes displays all routes that have been added manually by an administrator and allows several operations on the static routes. The List of IPv4 Static Routes and List of IPv6 Static Routes share the same fields (with one exception):

To configure IPv6 Static Routing:

1. Go to **Network > Routing > IPv6 Static Routing**.



2. Click **Add New IPv6 Static Route**.

The screenshot shows the 'IPv6 Static Routing Configuration' dialog box. It has the following fields: 'Route Name' (text input), 'Active' (toggle switch, currently 'OFF'), 'IPv6 Destination' (text input), 'IPv6 Prefix Length' (text input with a range of 0 - 128), 'Interface' (radio button selected for 'LAN'), 'IPv6 Gateway' (text input), and 'Metric' (text input with a range of 2 - 15). A 'Save' button is located at the bottom right of the dialog box.

3. Complete the fields in the table below and click **Save**.

| Field | Description |
|--------------------|---|
| Route Name | Enter a unique name for this static route. The name should allow you to easily identify this static route from others you may add. |
| Active | Activates or deactivates the status route. Choices are: <ul style="list-style-type: none">• ON = activate static route.• OFF = deactivate static route. |
| IPv6 Destination | The wireless controller will lead to this destination host or IP address. |
| IPv6 Prefix Length | The number of prefix bits in the IPv6 address that define the subnet. |
| Interface | Select the wireless controller interface that will interface to the static route. Choices are: <ul style="list-style-type: none">• LAN = the wireless controller's LAN or VLAN port will interface to the static route. |
| IPv6 Gateway | IP Address of the gateway through which the destination host or network can be reached. |
| Metric | Determines the priority of the route. If multiple routes to the same destination exist, the route with the lowest metric is chosen. |

Editing/Deleting Static Routes

Path: Network > Routing > IPv4 Static Routes or IPv6 Static Routes

After you add static routes, you can edit it if you need to change settings. To edit a static route, right-click the static route you want to edit and click **Edit**.

To delete a static route, right-click the static route you want to remove and click **Delete**.

QoS Configuration

In a typical controller, each physical port consists of one or more queues for transmitting packets on the attached network. Multiple queues per port are often provided to give preference to certain packets over others based on user-defined criteria. When a packet is queued for transmission in a port, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in the other queues of the port. If a delay is necessary, packets get held in the queue until the scheduler authorizes the queue for transmission. As queues become full, packets have no place to be held for transmission and get dropped by the controller.

QoS is a means of providing consistent, predictable data delivery by distinguishing between packets that have strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given "special treatment" in a QoS capable network. With this in mind, all elements of the network must be QoS-capable. The presence of at least one node which is not QoS-capable creates a deficiency in the network path and the performance of the entire packet flow is compromised.

QoS Priority

Configuring QoS Priority settings is a 3-step process:

1. Enable QoS mode (next page), and
2. Define the Trust Mode on each port (refer to "Defining DSCP and CoS on each port" on page 150)
3. Define the DHCP or COS settings (refer to "Configuring DSCP Priority" on page 152 or "Configuring 802.1p Priority" on page 151).

Enabling QoS Mode

Path: Network > QoS > LAN QoS Priority

Using the QoS page, you can enable Quality of Service (QoS) on the wireless controller.

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

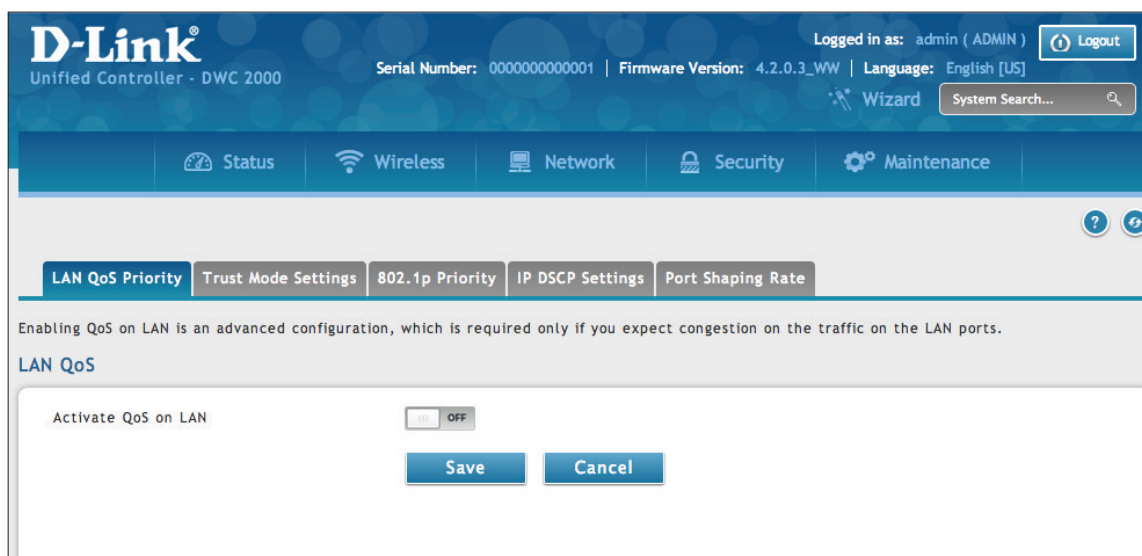
When you configure the QoS feature, you can select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective. It is especially useful if you expect traffic congestion on the wireless controller LAN ports.

QoS classification can be applied in Layer 2 or Layer 3 frames. For this reason, you can configure the wireless controller to use Layer 2 CoS settings or Layer 3 DSCP settings.

Note: The wireless controller also provides a CoS-to-DSCP map to map CoS values in incoming packets to a DSCP value that QoS uses internally to represent the priority of the traffic. To access this feature, click Network > QoS > QoS Priority.

To configure QoS mode:

1. Click **Network > QoS > LAN QoS Priority**.



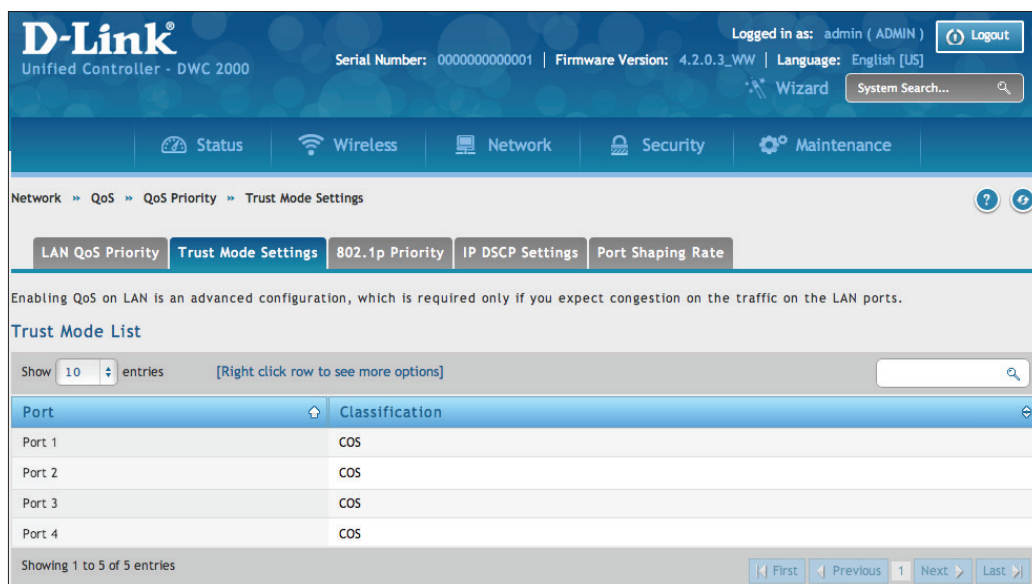
2. Toggle *Activate QoS on LAN* to **ON**.
3. On the middle menu on the LAN QoS Priority page, click the **Trust Mode Settings** tab. In the *Trust Mode List*, select a port by right-clicking it and clicking **Edit**. This brings up a pop-up box called Trust Mode Configuration.
4. Type in the port number for LAN Port and select either **CoS** or **DSCP** next to *Classify Using*.
5. Click **Save**.
6. Proceed to "Configuring DSCP Priority" on page 152 or "Configuring 802.1p Priority" on page 151 to configure values for DSCP and CoS and their priority.

Defining DSCP and CoS on each port

Path: Network > QoS > QoS Priority > Trust Mode Setting

Choose between CoS or DSCP for that port. When there is congestion on the port, the LAN port will check the value of one these fields in the packet and make a decision on the priority for that packet. Individual values for DSCP and CoS and the priority that they should be given are set by the Port Cos Mapping & Port DSCP Mapping pages under QoS.

1. Go to **Network > QoS > QoS Priority**. On the middle menu on the LAN QoS Priority page, click the *Trust Mode Settings* tab. In the Trust Mode List, select the mode by right-clicking it and clicking **Edit**. This brings up a popup box called Trust Mode Configuration.



2. Select **CoS** or **DSCP** mode.
3. Click **Save**.

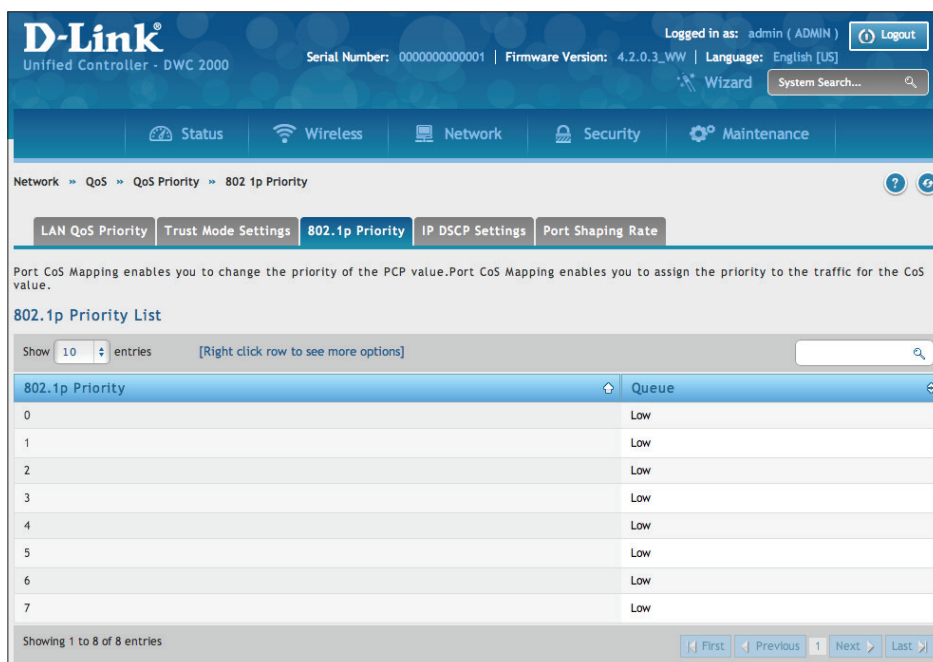
After you enable QoS mode, use the procedures in the following sections to configure the values and priorities used by DSCP and CoS.

Configuring 802.1p Priority

Path: Network > QoS > QoS Priority > 802.1P Priority

If you selected CoS for your QoS configuration, use the following procedure to configure and assign priority to the CoS fields in the IP packets.

1. Go to **Network > QoS > QoS Priority**. On the middle menu on the QoS Priority page, click the 802.1P Priority tab. In the 802.1p Priority List, each row corresponds to a CoS field in an IP packet. Select a CoS field by right-clicking on it and clicking **Edit**. This brings up a popup box called 802.1P Priority Configuration.



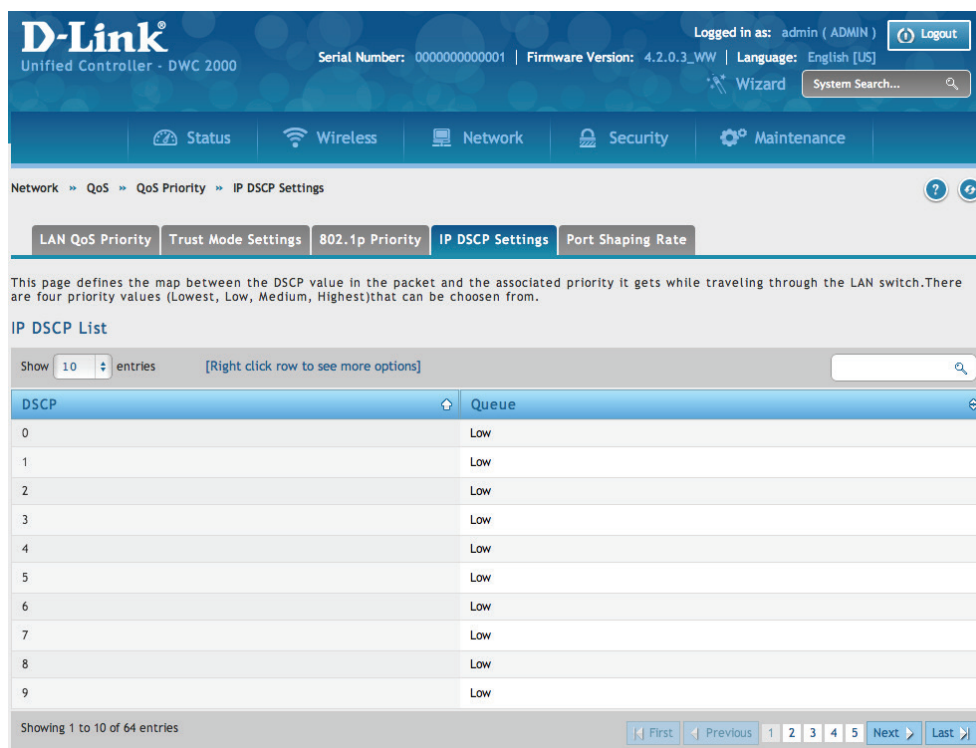
2. On the Queue drop-down list, select one of the following priorities:
 - Highest
 - Medium
 - Low
 - Lowest
3. Repeat step 2 for each additional CoS field you want to prioritize.
4. When you finish, click **Save**.

Configuring DSCP Priority

Path: Network > QoS > QoS Priority > IP DSCP Settings

If you selected DSCP for your QoS configuration, use the following procedure to configure and assign priority to the DSCP fields in IP packets.

- 1 Go to **Network > QoS > QoS Priority**. On the middle menu on the QoS Priority page, click the IP DSCP Settings tab. In the IP DSCP List, select a DSCP by right-clicking it and clicking **Edit**. This brings up a popup box called IP DSCP Configuration.



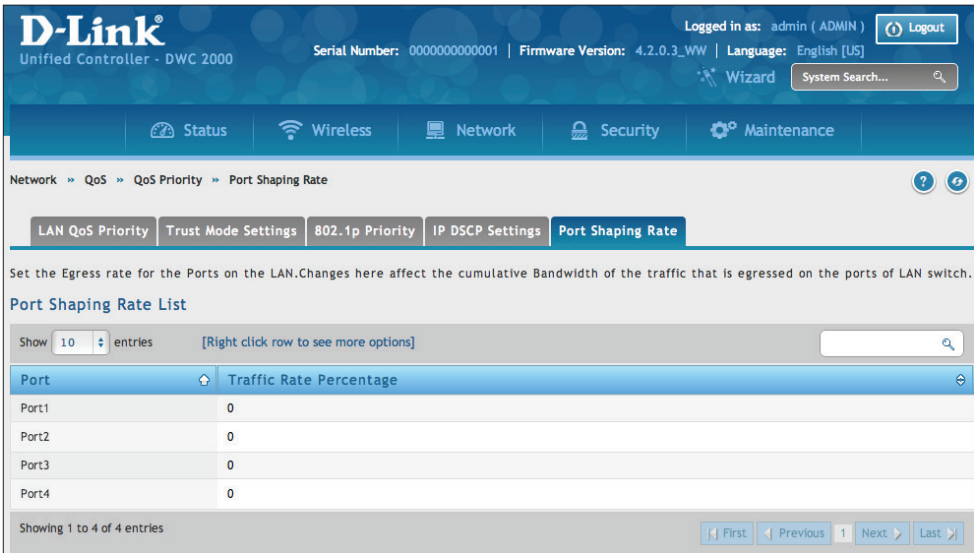
2. From the Queue drop-down list, select one of the following priorities:
 - Highest
 - Medium
 - Low
 - Lowest
3. Repeat step 2 for each additional DSCP field you want to prioritize.
4. When you finish, click **Save**.

Port Shaping Rate

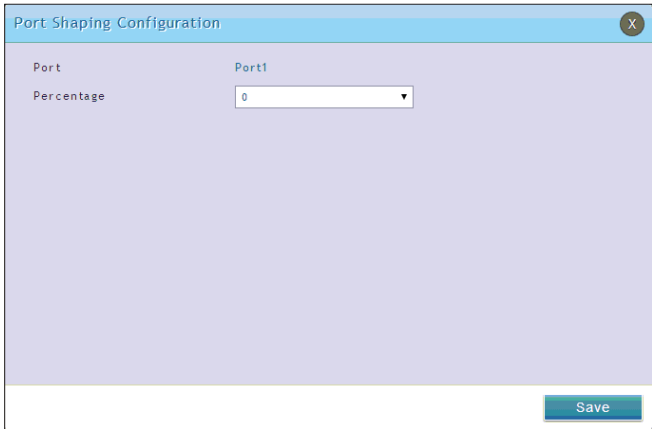
Path: Network > QoS > QoS Priority > Port Shaping Rate

This page allows configuring an interface shaping rate to all ports or to a specific port. Right-click and edit the percentage.

- 1. Go to **Network > QoS > QoS Priority > Port Shaping Rate** tab.



- 2. Right-click the port and select **Edit**.
- 3. Select the percentage you want to assign to the port from the drop-down menu and click **Save**.



| Field | Description |
|------------|--|
| Port | Port to be affected by the Port Shaping Rate |
| Percentage | Sets the limit on how much traffic can leave a port. The limit on maximum transmission bandwidth has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded. |

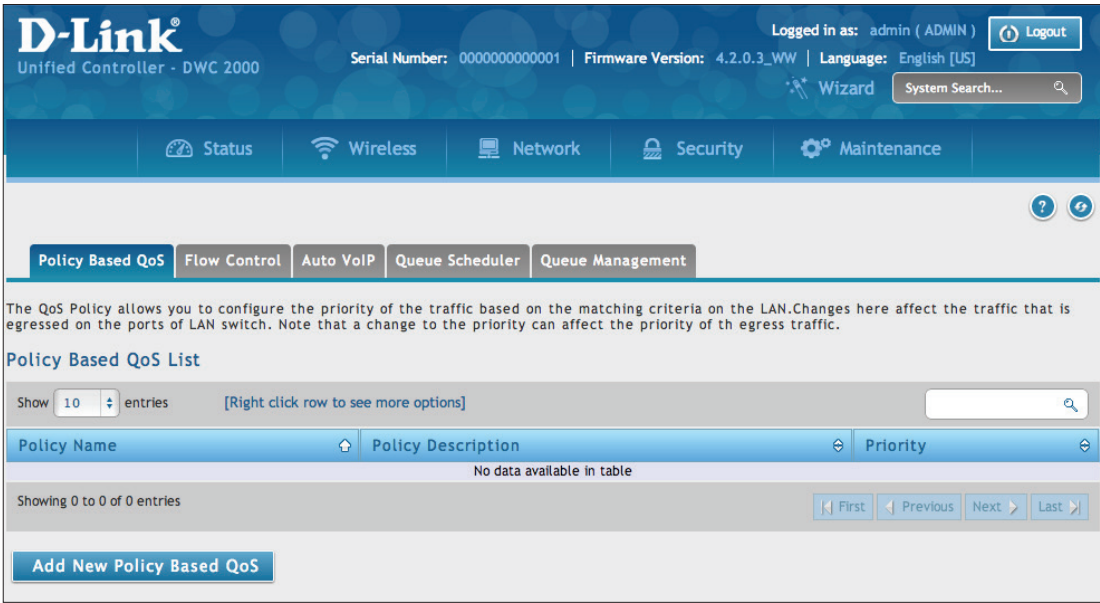
QoS Policy

The QoS Policy allows you to configure the priority of the traffic based on the matching criteria on the LAN. Changes here affect the traffic that is egressed on the ports. Note that a change to the priority can affect the priority of the egress traffic.

Configure Policy Based QoS

Path: Network > QoS > Policy Based QoS

- 1. Go to **Network > QoS > QoS Policy > Policy Based QoS** tab.



- 2. Click **Add New Policy Based QoS**.
- 3. Complete the fields in the table on the next page and click **Save**.

Policy Based QoS Configuration

Profile Name

Port

Port1

Port2

Port3

Port4

Profile Type

VLAN

VLAN

1

Priority

Highest

Save

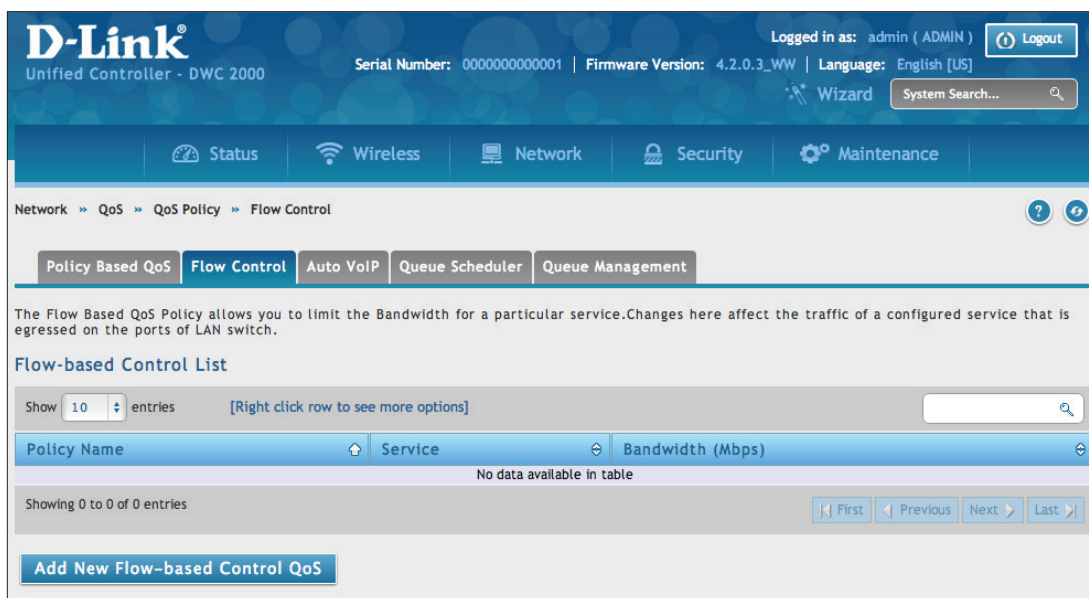
| Field | Description |
|--------------|---|
| Profile Name | The name of the profile. |
| Port | Select a port or ports. Hold CTRL to select multiple ports. |
| Profile Type | Matching criteria of this profile. The criteria are: <ul style="list-style-type: none">• VLAN• Destination MAC Address• Source MAC Address• Destination IP Address• Source IP Address• Source TCP Port• Destination TCP Port• Source UDP Address• Destination UDP Address |
| VLAN | If Profile Type = VLAN, enter a defined VLAN number. |
| MAC Address | If Profile Type = Destination MAC Address or Source MAC Address, enter a defined MAC Address. |
| IP Address | If Profile Type = Destination IP Address or Source IP Address, enter a defined IP Address. |
| L4 Port | If Profile Type= Source TCP Port, Destination TCP Port, Source UDP Port or Destination UDP Address, enter a defined port number. |
| Priority | Priority of the QoS rule. The priority choices are: <ul style="list-style-type: none">• Highest• High• Low• Lowest |

Configure Flow-based Control

Path: Network > QoS > QoS Policy > Flow Control

The Flow-Based QoS Policy allows you to limit the Bandwidth for a particular service. Changes here affect the traffic of a configured service that is egressed on the ports.

1. Go to **Network > QoS > QoS Policy > Flow Control** tab.



2. Click **Add New Flow-based Control QoS**.
3. Complete the fields in the table below and click **Save**.

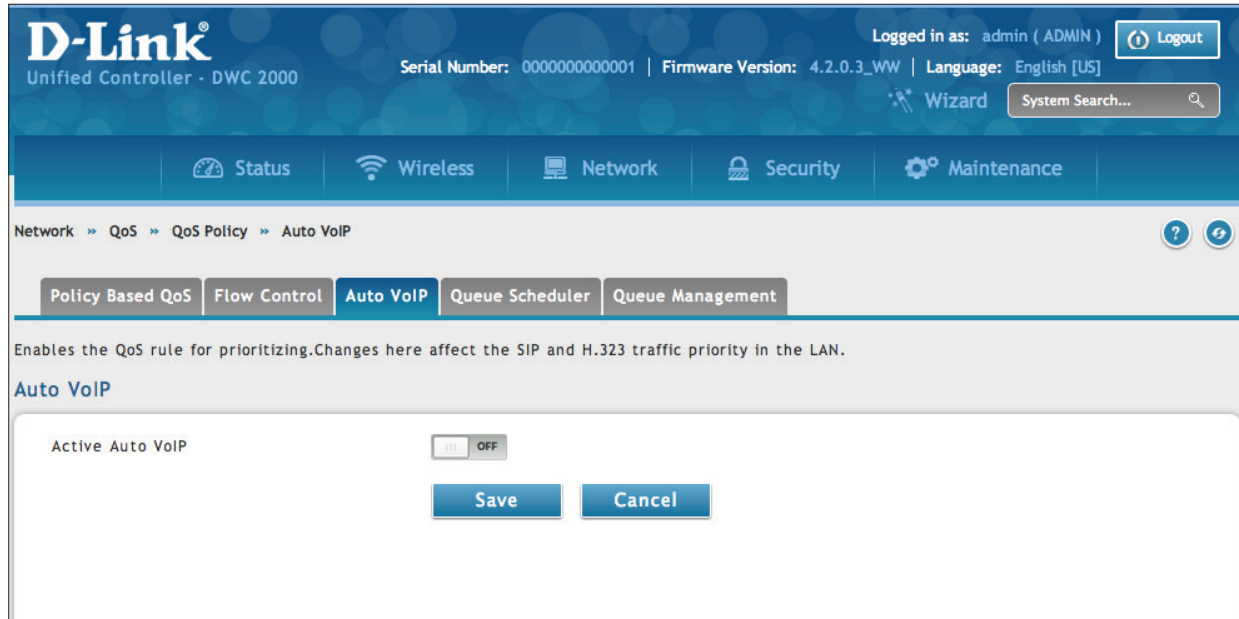
| Field | Description |
|------------------------|---|
| Profile Name | The name of the profile. |
| Service | Select the type of service you want to use. The choices are: Any, aim, bgp, bootp_client, bootp_server, cu-seeme udp, cu-seeme tcp, dns udp, dns tcp, finger, ftp, http, https, icmp, icq, imap2, imap3, irc, news, nfs, nntp, ping, pop3, pptp, rcmd, rea-audio, rexec, rlogin, rtelnet, rtsp tcp, rtsp udp, sftp, smtp, snmp tcp, snmp udp, snmp-traps tcp, snmp-traps udp, sql-net, ssh tcp, ssh udp, strmworks, tacacs, telnet, tftp, rip, kie, shhttpd, ipsec-udp-encap, ident, vddolive, ssh, sip-tcp, sip-udp, or icmpv6. |
| Source IP Address | The source IP address |
| Destination IP Address | The destination IP address |
| Bandwidth | Limit the Bandwidth for a particular service. |

Configure Auto VoIP QoS

Path: Network > QoS > QoS Policy > Auto VoIP

Enables the QoS rule for prioritizing. Changes here affect the SIP and H.323 traffic priority in the LAN.

1. Go to **Network** > **QoS** > **QoS Policy**. > **Auto VoIP** tab.
2. Enable *Active Auto VoIP* and click **Save**.

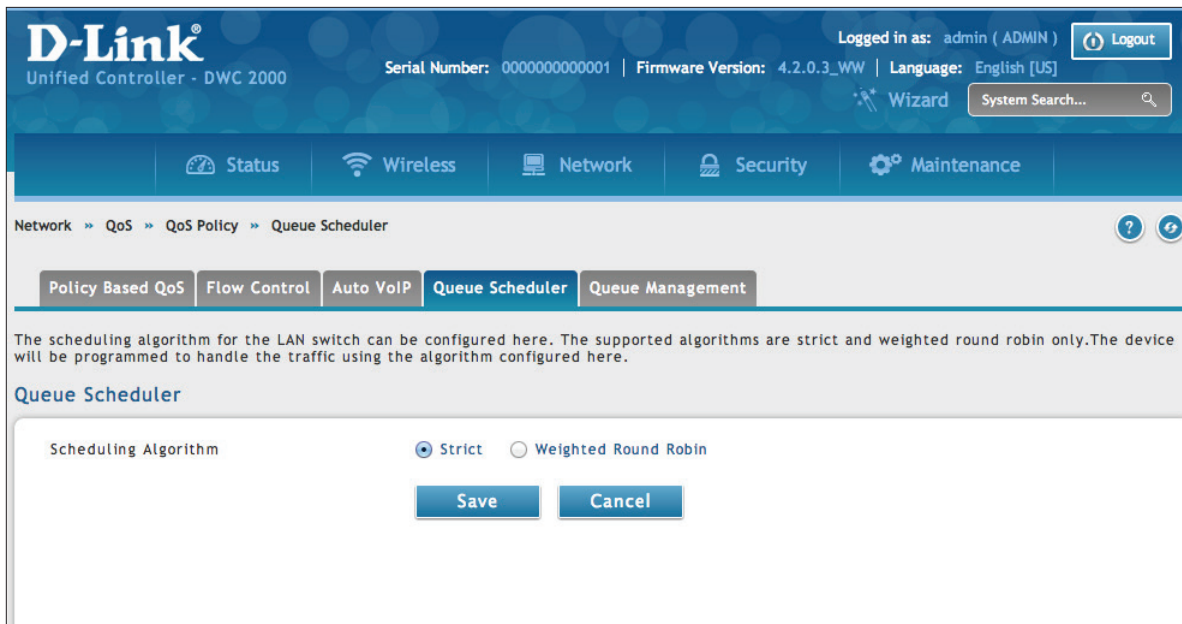


Configure Queue Scheduler

Path: Network > QoS > QoS Policy > Queue Scheduler

The supported algorithms are strict and weighted round robin only. The device will be programmed to handle the traffic using the algorithm configured here.

1. Go to **Network > QoS > QoS Policy > Queue Scheduler** tab.



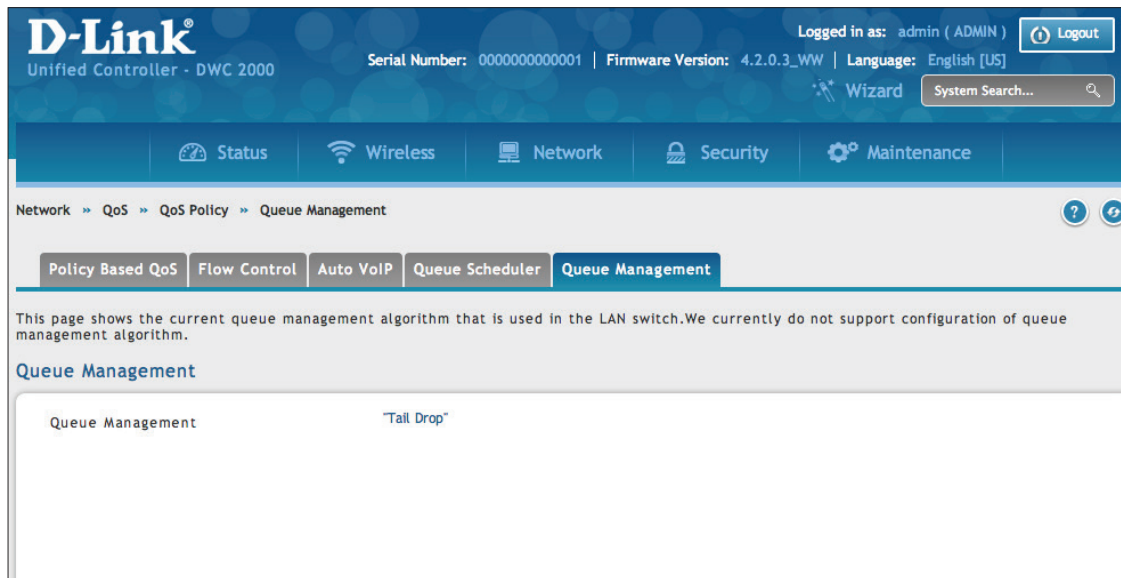
2. Select Scheduling Algorithm: Strict or Weighted Round Robin.
3. Click **Save**.

Queue Management

Path: Network > QoS > QoS Policy > Queue Management

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

1. Go to **Network > QoS > Option QoS > Queue Management** tab.



This page displays the current queue management algorithm that is used. We currently do not support configuration of queue management algorithm.

Setup CoS and DSCP Marking

Path: Network > QoS > CoS DSCP Marking

Remarking CoS to DSCP is an advanced QoS configuration, where the Layer 2 quality of service field is translated to a Layer 3 QoS field in the packet, so that upstream routers can make a QoS decision based on the DSCP field set in the packet. Once you enable CoS to DSCP marking by choosing the check box, you can choose the appropriate value of the DSCP for a given CoS value.

1. Go to **Network > QoS > CoS DSCP Marking**.

D-Link
Unified Controller - DWC 2000

Logged in as: admin (ADMIN) [Logout]

Serial Number: 0000000000001 | Firmware Version: 4.2.0.3_WW | Language: English [US]

Wizard System Search...

Status Wireless Network Security Maintenance

Network > QoS > CoS DSCP Marking

Remarking CoS to DSCP is an advanced QoS configuration, where the Layer 2 quality of service field is translated to a Layer 3 QoS field in the packet, so that upstream controllers can make a QoS decision based on the DSCP field set in the packet. Once you enable CoS to DSCP marking by choosing the check box, you can choose the appropriate value of the DSCP for a given CoS value.

CoS DSCP Marking List

CoS to DSCP Setup
Enable CoS to DSCP Marking ☒ ON

Save Cancel

CoS DSCP Marking List

Show 10 entries [Right click row to see more options]

| CoS | DSCP Value |
|-----|------------|
| 0 | 0 |
| 1 | 8 |
| 2 | 16 |
| 3 | 24 |
| 4 | 32 |
| 5 | 40 |
| 6 | 48 |
| 7 | 56 |

Showing 1 to 8 of 8 entries

First Previous 1 Next Last

2. Enable CoS and DSCP Marking and click **Save**.
3. Right-click on the CoS and select **Edit**. Change the mapping value between CoS and DSCP.
4. Click **Save**.

Securing Your Network

The wireless controller supports a number of features for securing your network. This chapter describes the following commonly used security features:

- "Client Management" on page 162
- "Group Management" on page 165
- "User Management" on page 172
- "Guest Account Usage Management" on page 177
- "External Authentication" on page 186
- "Blocked Clients" on page 192
- "WIDS" on page 67

Note: *The procedures in this chapter should only be performed by expert users who understand networking concepts and terminology.*

Client Management

Using the MAC Authentication page, you can view wireless clients in the MAC Authentication database. The database contains wireless client MAC addresses and names. The database is used to retrieve descriptive client names from the RADIUS server and implement MAC authentication.

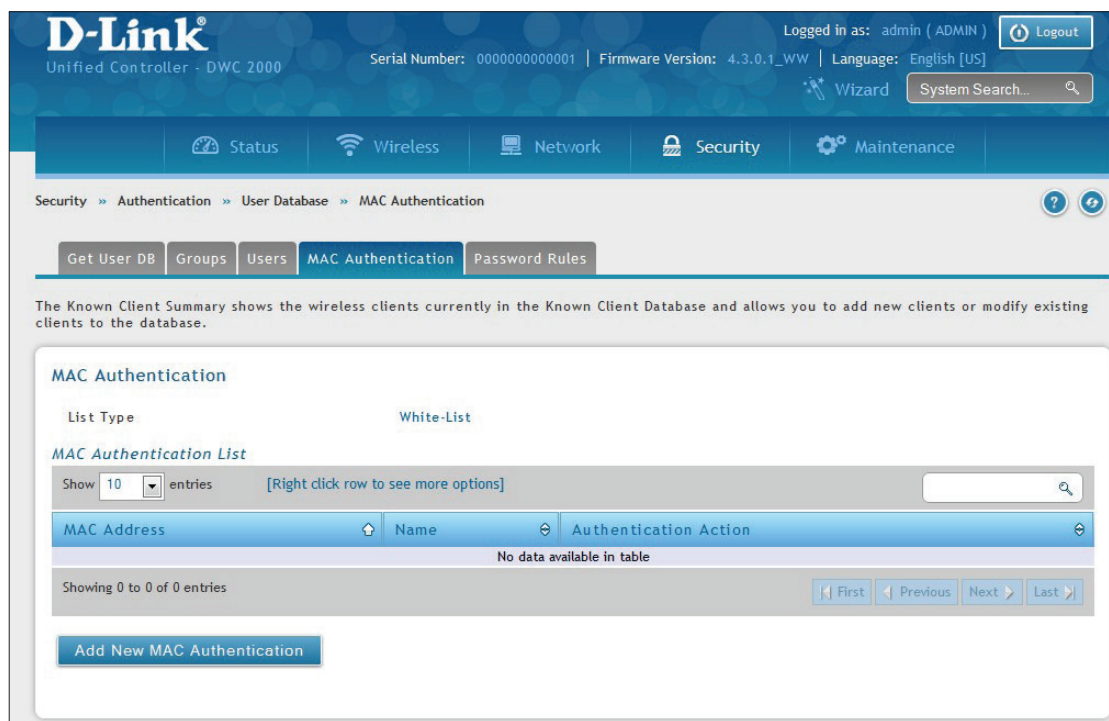
The page also lets you add, edit, and delete clients.

Viewing/Adding Wireless Known Clients

Path: Security > Authentication > User Database > MAC Authentication

To view wireless known clients:

1. Go to **Security > Authentication > User Database**.
2. Click on the **MAC Authentication** tab in the middle menu. The MAC Authentication page will appear displaying a list of the wireless clients in the MAC Authentication database.



3. Next to *List Type* the current global setting is displayed.

MAC authentication is a feature that grants or denies a client access to the network if the client's MAC address in the white-list or black-list. MAC Authentication is enable at the network level. The network configuration also defines whether MAC addresses are looked up on the local database or on the RADIUS server.

4. Click on Add New MAC Authentication. The MAC Authentication Configuration page will appear.

MAC Authentication Configuration

MAC Address

Name

Authentication Action

Global

Save

5. Complete the fields in the table below and click **Save**.

| Field | Description |
|-------------|---|
| MAC Address | Enter the MAC address for the known client. |
| Name | Enter the name of the known client. The name should allow you to differentiate this known client from others you may add. |

Editing/Deleting Clients

Path: Security > Authentication > User Database > MAC Authentication

After you add clients, you can edit or delete it if you need to change settings.

To edit or delete a client:

1. Go to **Security > Authentication > User Database > MAC Authentication**.
2. Under *MAC Authentication List*, right-click the client and select either **Edit** or **Delete**.
3. Change the desired settings (refer to the table on the previous page).
4. Click **Save**.

Group Management

A user group is a collection of users who share the same privileges. The following section describes how to add user groups. After you add a user group, you can configure its login policies, policies for browsers, and policies by IP. You can also edit user groups when changes are required and delete user groups you no longer need.

Adding User Groups

Path: Security > Authentication > User Database > Groups

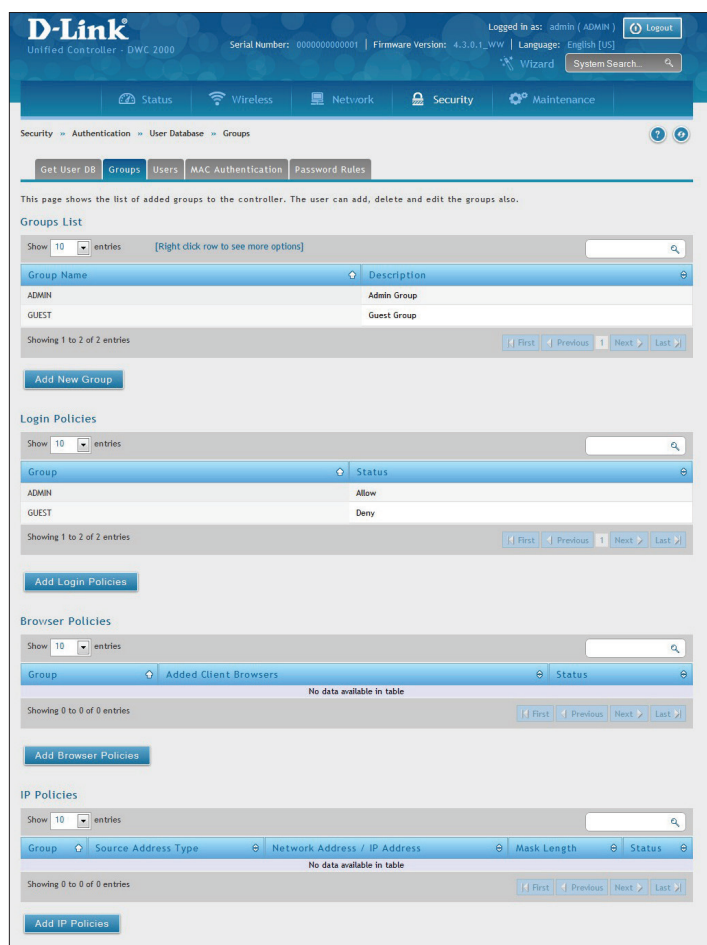
When you add a user group, you assign:

- A name that identifies the user group
- An optional user group description
- At least one privilege (or “user type”)
- An idle timeout value

After you define user groups, you can use the procedure under “User Management” on page 172 to populate the groups with users.

To add a user group:

1. Go to **Security > Authentication > User Database > Groups**.



2. Click **Add New Group**. The Group Configuration pop-up page will appear.

3. Complete the fields in the table below and click **Save**.

| Field | Description |
|----------------------------|--|
| Group Configuration | |
| Group Name | Enter a unique name for this group. The name should allow you to easily identify this group from others you may add. |
| Description | Enter a description for this user group. |
| User Type | |
| Admin | Click this to grant all users in this group super-user privileges. By default, there is one admin user. The group types for Admin users are: <ul style="list-style-type: none"> Captive Portal User - The users of the group having Captive Portal privilege will have permissions to access the Internet/Networks through Captive Portal authentication. |
| Network | Selecting Network enables an extra option, by default the group types for Network users are: <ul style="list-style-type: none"> Captive Portal User - The users of the group having Captive Portal privilege will have permissions to access the Internet/Networks through Captive Portal authentication. |
| Field | |
| Front Desk | The users of the group having Front Desk User privilege will have permissions to create temporary users who can access Internet/Network by using Hotspot. |
| Guest | The users of the group having Guest User privilege will only have view only permissions. Such users cannot configure the device. |
| Idle Timeout | Enter the number of minutes of inactivity that must occur before the users in this user group are logged out of their web management session automatically. Entering an Idle Timeout value of 0 (zero) means never log out. |

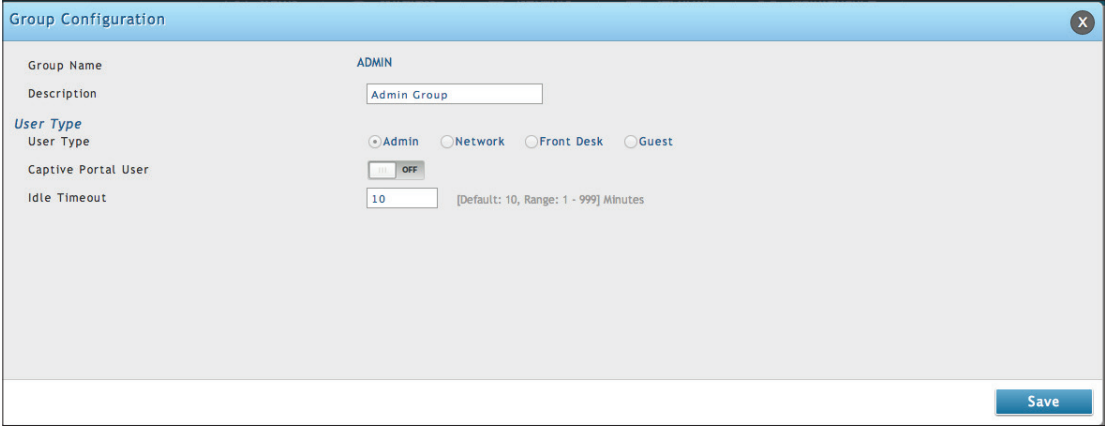
Editing User Groups

Path: Security > Authentication > User Database > Groups

There may be times when you need to edit a user group. For example, you might want to change the privileges for the user group or idle timeout.

To edit a user group:

1. Go to **Security > Authentication > User Database > Groups**. The Groups List page will appear.
2. Right-click the user group you want to edit and click **Edit**. The Group Configuration pop-up page will appear.

A screenshot of the 'Group Configuration' pop-up window. The window has a blue title bar with the text 'Group Configuration' and a close button (X) in the top right corner. The main area is light gray and contains the following fields: 'Group Name' with the value 'ADMIN'; 'Description' with a text box containing 'Admin Group'; 'User Type' with a section header and four radio buttons: 'Admin' (selected), 'Network', 'Front Desk', and 'Guest'; 'Captive Portal User' with a toggle switch set to 'OFF'; and 'Idle Timeout' with a text box containing '10' and a note '(Default: 10, Range: 1 - 999) Minutes'. A blue 'Save' button is located in the bottom right corner of the window.

3. Complete the fields in the previous page and click **Save**.

Deleting User Groups

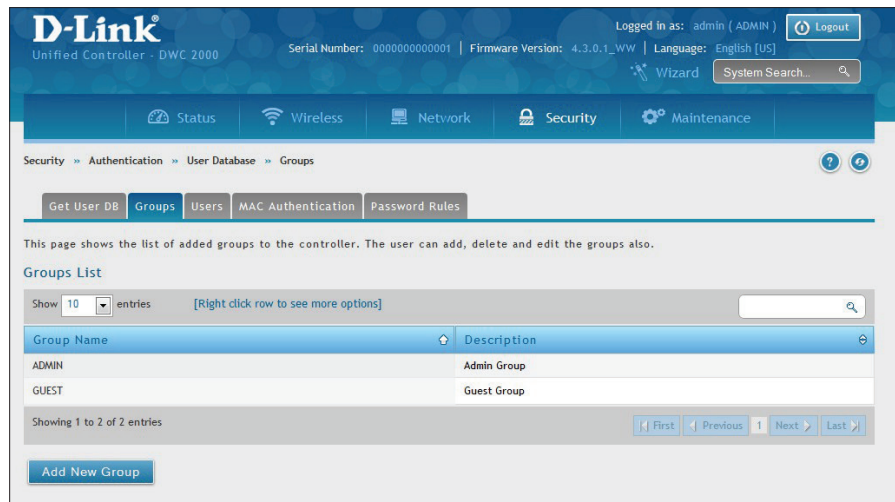
Path: Security > Authentication > User Database > Groups

If you no longer need a user group, you can delete it. Before you delete a user group, you must delete all users in it (see “Editing/Deleting Clients” on page 164).

Note: A precautionary message does not appear before you delete a user group. Therefore, be sure you do not need a user group before you delete it.

To delete a user group:

1. Go to **Security > Authentication > User Database > Groups**. The Groups page will appear.
2. Right-click on the user group you want to delete and click **Delete**. To delete all groups, click **Select All** and then **Delete**.



Configuring Login Policies

Path: Security > Authentication > User Database > Groups

Using the following procedure, you can grant or deny a user group login access to the web management interface.

- 1. Click **Security > Authentication > User Database > Groups**. The Groups page will appear.
- 2. Check the box next to a user group.
- 3. Click the **Add Login Policies button**. The Login Policies Configuration page will appear.

Login Policies Configuration

Group Name

ADMIN

Disable Login

☐ OFF

Save

- 4. Complete the fields from the table below and click **Save Settings**.

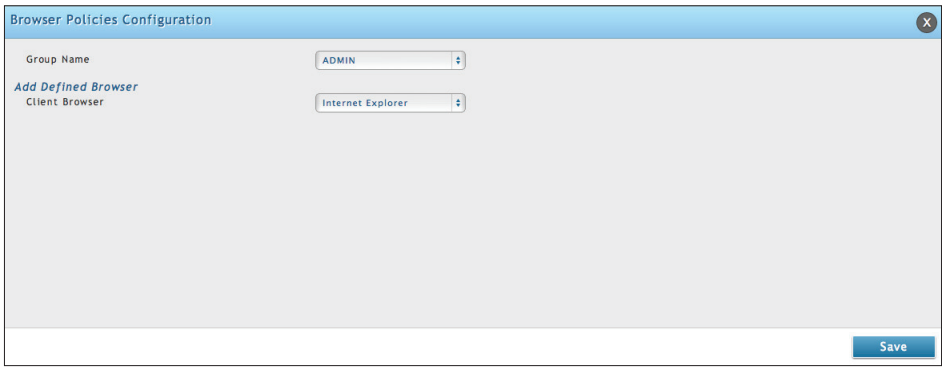
| Field | Description |
|---------------|--|
| Group Name | Name of the group. |
| Disable Login | Grants or denies login access to the web management interface for all users in this user group. Choices are: <ul style="list-style-type: none">• On: Disable login access.• Off: Enable login access. |

Configuring Browser Policies

Path: Security > Authentication > User Database > Groups

The following procedure describes how to configure browser-specific policies for user groups. Using this procedure, you can allow or deny the users in a user group from using particular web browsers to log in to the wireless controllers' web management interface.

- 1. Click **Security > Authentication > User Database > Groups**.
- 2. Click the **Add Browser Policies** button.



- 3. Under *Add Defined Browser*, click a browser from the *Client Browser* drop-down list and click **Add**. The selected browser will appear in the Defined Browsers area.

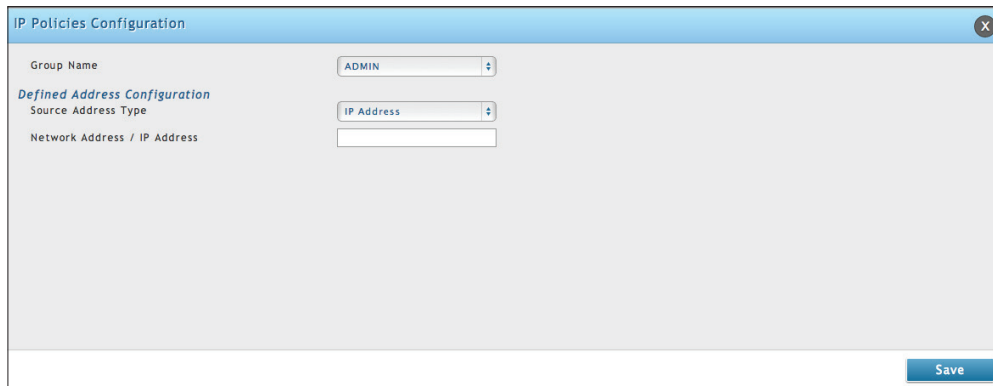
| Field | Description |
|----------------|--|
| Group Name | Select the group name from the drop-down menu. |
| Client Browser | Select a web browser from the drop-down menu. |

Configuring IP Policies

Path: Security > Authentication > User Database > Groups

The following procedure describes how to configure IP-specific policies for user groups. Using this procedure, you can allow or deny the users in a user group to log in to the wireless controllers' web management interface from a particular network or IP address.

1. Click **Security > Authentication > User Database > Groups**.
2. Click the **Add IP Policies** button. The IP Policies Configuration page will appear.



3. Complete the fields in the table below and click **Save**. The address you defined will appear in the Defined Addresses area.

| Field | Description |
|----------------------------|---|
| Group Name | Select a group name from the drop-down menu. |
| Source Address Type | Choices are: <ul style="list-style-type: none">• IP Address = specifies a particular IP address.• IP Network = specifies an entire IP network. |
| Network Address/IP Address | Enter the network or IP address. |
| Mask Length | Enter a subnet mask. |

User Management

After you add user groups, you can add users to the user groups. Users can be added individually, or they can be imported from a comma-separated-value (CSV) formatted file.

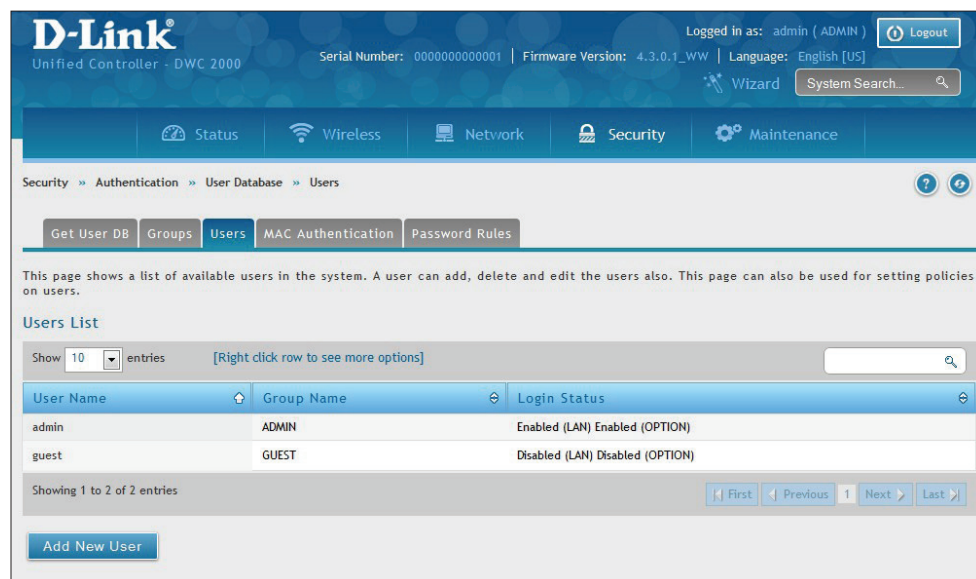
After you add users, you can edit them when changes are required and delete users when you no longer need them.

Adding Users Manually

Path: Security > Authentication > User Database > Users

One way of adding users is to add users individually.

1. Go to **Security > Authentication > User Database > Users**.



2. Click **Add New User**. The User Configuration pop-up page will appear.

The screenshot shows the "User Configuration" pop-up page. It contains the following fields:

- User Name:
- First Name:
- Last Name:
- Select Group:
- Password:
- Confirm Password:

A "Save" button is located at the bottom right of the form.

3. Complete the fields in the table below and click **Save**.

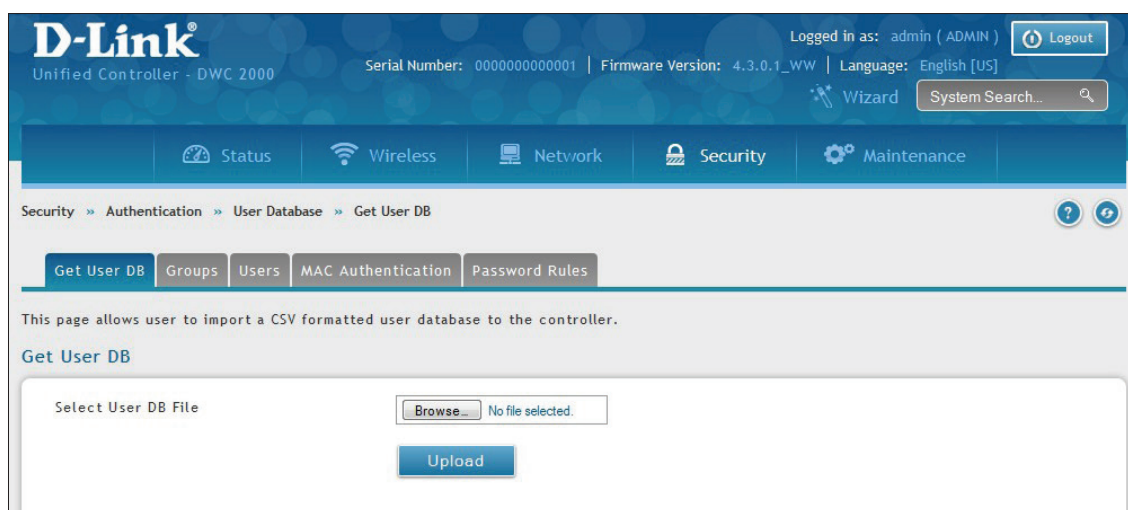
| Field | Description |
|------------------------|--|
| User Name | Enter a unique name for this user. The name should allow you to easily identify this user from others you may add. |
| First Name | Enter the first name of the user. |
| Last Name | Enter the last name of the user. |
| Select Group | Select the captive portal group to which this user will belong. |
| Password | Enter a case-sensitive login password that the user must specify at the login prompt to access the web management interface. For security, each typed password character is masked with a dot (•). |
| Confirm Password | Enter the same case-sensitive password entered in the Password field. For security, each typed password character is masked with a dot (•). |
| Enable Password Change | If the group user type is Captive Portal, enable password changes by user if needed. |
| MultiLogin | If the group user type is Captive Portal, enable MultiLogin allowing user using the same username/ password login via multiple devices at the same time. |

Importing Users

Path: Security > Authentication > User Database > Get User DB

A faster alternative to adding individual users is to import users from a CSV-formatted file.

1. Click **Security > Authentication > User Database > Get User DB**.



2. Click the **Browse** button.

3. In the *Choose File* dialog box, navigate to the location of the CSV file, and then click the file.

4. Click **Open** and then click **Upload**.

Editing Users

Path: Security > Authentication > User Database > Users

There may be times when you need to edit a user. For example, you might want to change the user's login password or idle timeout.

To edit a user:

1. Click **Security > Authentication > User Database > Users**. The Users List page will appear.
2. Right-click on the user you want to edit and click **Edit**.

The screenshot shows a 'User Configuration' window. The fields are as follows:

- User Name: admin
- First Name: admin
- Last Name: ssl
- Select Group: ADMIN
- Edit Password: ON
- Current Logged In Administrator Password: (empty)
- New Password: (masked with dots)
- Confirm New Password: (masked with dots)

A 'Save' button is located at the bottom right of the window.

3. Complete the fields in the table below and click **Save**.

| Field | Description |
|---|---|
| User Name | Enter a unique name for this user. The name should allow you to easily identify this user from others you may add. |
| First Name | Enter the first name of the user. |
| Last Name | Enter the last name of the user. |
| Select Group | Select the group to which this user will belong. |
| Edit Password | Toggle this option to enter the password to be used by this user to log in to the web management interface. |
| Enter Current Logged in Administrator Password | Enter the current case-sensitive login password. For security, each typed password character is masked with a dot (•). |
| New Password | Enter the new case-sensitive login password. For security, each typed password character is masked with a dot (•). Record the new password in Appendix A. |
| Confirm Password | Enter the new password again. |

Deleting Users

Path: Security > Authentication > User Database > Users

If you no longer a user, you can delete the user.

Note: A precautionary message does not appear before you delete a user. Therefore, be sure you do not need a user before you delete it.

To delete a user:

1. Click **Security > Authentication > User Database > Users**. The Users List page will appear.
2. Right-click on the user you want to delete and click **Delete**. To delete all users, click **Select All** and then **Delete**.

Password Rules

Path: Security > Authentication > User Database > Password Rules.

Rule the password length and characters to increase the security of Captive Portal user authentication.

1. Go to **Security > Authentication > User Database > Password Rules**.

The screenshot shows the D-Link Unified Controller web interface. The top header includes the D-Link logo, 'Unified Controller - DWC 2000', and system information like 'Serial Number: 0000000000001', 'Firmware Version: 4.3.0.1_WW', and 'Language: English [US]'. The user is logged in as 'admin (ADMIN)' with a 'Logout' button. The main navigation bar has tabs for Status, Wireless, Network, Security, and Maintenance. The breadcrumb trail is 'Security > Authentication > User Database > Password Rules'. Below the breadcrumb, there are tabs for 'Get User DB', 'Groups', 'Users', 'MAC Authentication', and 'Password Rules'. The 'Password Rules' tab is active. The page content area has a title 'Password Rules' and a description 'The table lists all the available Password Rules in the system.' Below this, there is a form with the following fields: 'Password Enforcement' (toggle OFF), 'Minimal Password Length' (input 8, default 8, range 4-64), 'Minimal Numeric Characters' (input 2, default 2, range 0-4), and 'New Password must be Different' (toggle OFF). At the bottom of the form are 'Save' and 'Cancel' buttons.

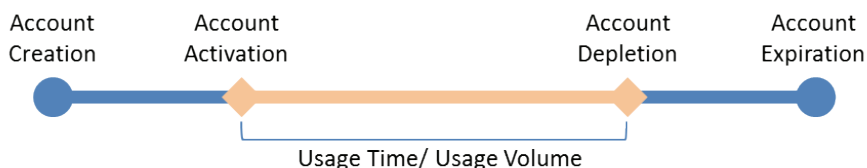
2. Complete the fields in the table below and click **Save**.

| Field | Description |
|---------------------------------------|--|
| Password Enforcement | Toggle on to turn on the following password rules. |
| Minimal Password Length | Enter the minimum number of characters required. |
| Minimal Numeric Characters | Enter the minimum number of numbers that users must use in their password. |
| New Password must be Different | Your new password configured must be different than old password. |

Guest Account Usage Management

Guest account is generated by the wireless controller. Set the relative billing profiles to control guest internet usage.

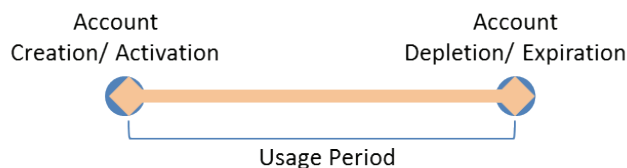
The billing profile settings include 4 milestones by timeline:



- Account Creation: the temporary account is generated by front desk account in the local database.
- Account Activation: the temporary account is activated and it is valid for use.
- Account Depletion: the temporary account is run out usage time or usage volume.
- Account Expiration: the temporary account is expired no matter usage time/ volume running out or not, and it is removed from the local database.

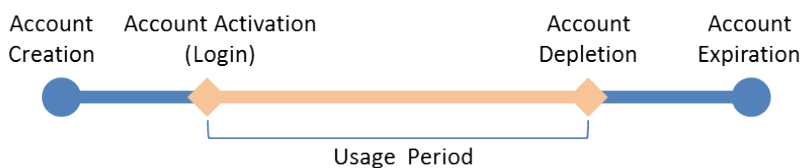
The billing profile can be various depending on how to put the value in the settings. Below are five most comment types of billing profiles:

1. The temporary account usage time is limited by duration. The account has the expiration time. The account is valid while the account is created.



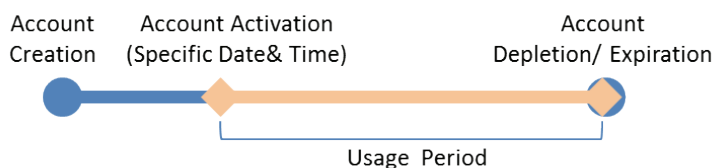
This billing profile is suitable for the scenario in Hotel. The temporary account is created and valid while customers check-in.

- The temporary account usage time is limited by duration. The account has the expiration time. The account is valid while the account first logs in.



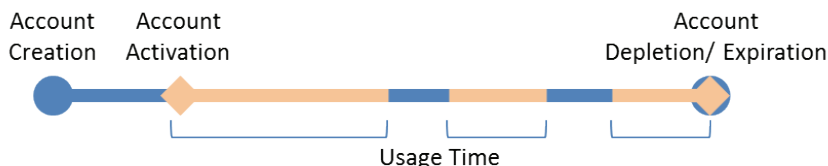
This billing profile is suitable for the scenario in Coffee Shop, Airport, etc. The customer can use wireless internet service for a period of time counting from first time logs in.

- The temporary account is valid with specific date and time. The account has the expiration time.



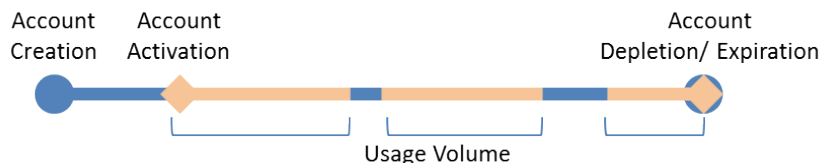
This billing profile is suitable for the scenario in Press Conference. The organizer generates accounts before the event and delivery account information to participator in advanced if necessary. The temporary account would be only valid from specific date and time.

- The temporary account has limited time usage. The account doesn't have the expiration time until the usage is run out.



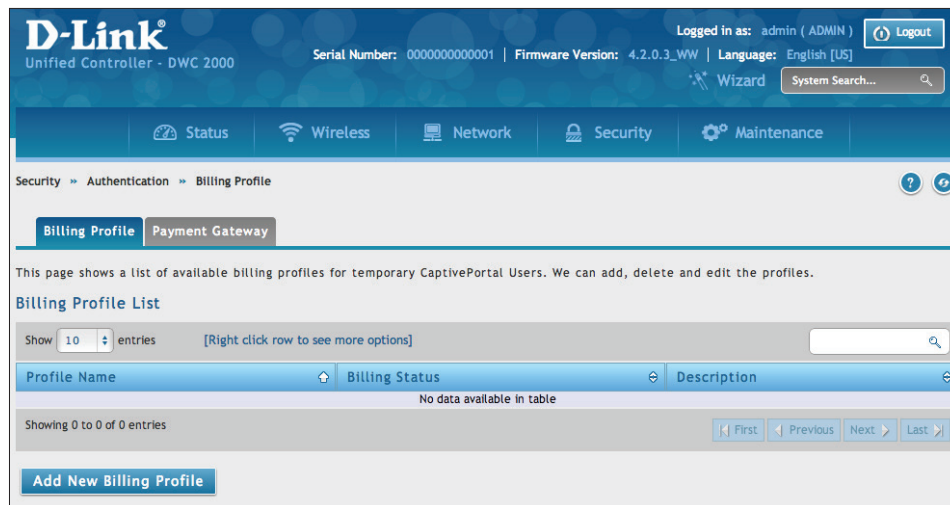
This billing profile is suitable for the scenario in Hotspot. The service provider charge the wireless service based on usage time. This account allows multiple devices log in at the same time.

- The temporary account has limited usage traffic. The account doesn't have the expiration time until the usage is run out.



This billing profile is suitable for a Hotspot scenario. The service provider charge the wireless service based on usage volume.

1. Click **Security > Authentication > Billing Profile**. The Billing Profile List page will be appear.



2. Click **Add New Billing Profile**.

3. Complete the fields in the table below and click **Save**.

| Field | Description |
|---|--|
| Profile Details | |
| Profile Name | Enter a name for this profile. |
| Profile Description | Enter a description for this profile. |
| Allow Multiple Login | Checking this option will allow multiple users to use the same captive portal login credentials created for this profile to login simultaneously. |
| Allow Customized Account on Front Desk | Checking this option enables front desk user to give customized account name to the captive portal users being created on this profile. |
| Allow Batch Generation on Front Desk | Checking this option enables front desk user to generate a batch of temporary captive portal users at one click. |
| Session Idle Timeout | Idle timeout for CP users generated for this profile. |
| Show Alert Message on Login Page while Rest of Usage Time/ Traffic Under | Enter a value here in Hours/Days/MB/GB to get an alert message when usage time/traffic left reaches the desired limit. By default if 0 is entered it implies no alert message is required. |

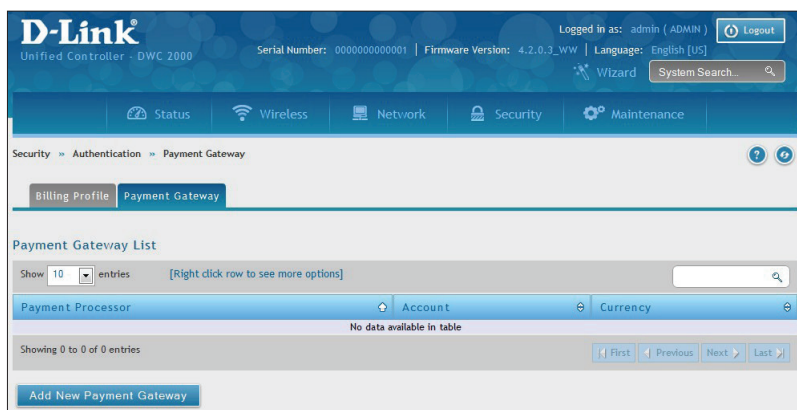
| Field | Description |
|---|---|
| Basic Limit by Duration | |
| Valid with Begin and End Time | Limitations on Duration basis |
| Basic Limit by Usage | |
| Maximum Usage Time | <p>When Basic Limit by Usage is toggled On, there will be three types of limiting users access by duration:</p> <ul style="list-style-type: none"> • Start While Account Created: Activate account when user is created • Start While Account Login: Activate account when user first login using his credentials. • Begin From: Activate account from this date |
| Maximum Usage Traffic | Maximum traffic user can use before his account expires. Only inbound traffic shall be considered towards bandwidth usage. |
| Allow Front Desk to Modify Usage | Checking this option enables front desk user to modify usage limits. |
| Unit Price | |
| Set Price | Enable the option to set the price for this billing profile. The price will be shown on the Captive Portal which is set the Captive Portal Type as Billing User |
| Price | Enter a price. |
| Monetary Unit | Select the Monetary Unit from drop down menu. The available options are from the Currency setting on Payment Gateway. |

Payment Gateway

Path: Security > Authentication > Billing Profile > Payment Gateway

A payment gateway is an e-commerce application service provider service that authorizes payment and money transfers to be made through the Internet. Configure payment gateway settings to allow user online purchasing wireless service from Captive Portal.

1. Click **Security > Authentication > Billing Profile > Payment Gateway** tab.



2. Click **Add New Payment Gateway**.

3. Complete the fields in the table below and click **Save**.

| Field | Description |
|---------------------------|---|
| Payment Processor | Select the payment agent. |
| Paypal | |
| Payment Receiver Email ID | The Paypal email account used for receiving payment. |
| API Username | The API username of the Paypal Premier/Business/Website Payment Pro account. |
| API Password | The API password of the Paypal account. |
| API Signature | The API signature of the Paypal Premier/Business/Website Payment Pro account. |
| APP ID | The APP ID which Paypal provided to you. |
| Currency | The payment unit type. |

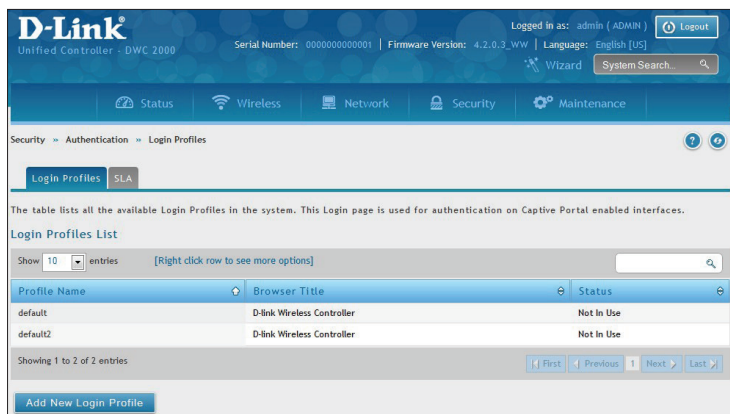
Login Profiles

When a wireless client connects to the SSIDs of access point or VLANs, the user sees a login page. The Login Profile and SLA page allows you to customize the appearance of that page with specific text and images. The wireless controller supports multiple login and SLA pages. Associate login page or SLAs on SSIDs or VLANs separately.

Customize the Captive Portal Login Page

Path: Security> Authentication> Login Profiles> Login Profiles

1. Go to **Security > Authentication > Login Profiles > Login Profiles** tab.



2. Click **Add New Login Profile**.

Login Profile Configuration

General Details

Profile Name:

Browser Title:

Background: ☒ Image ☐ Color

Page Background Image: Default:

Header Details

Background: ☒ Image ☐ Color

Header Background Image: Default:

Header Caption:

Caption Font:

Font Size:

Font Color:

Login Details

Login Section Title:

Welcome Message:

Error Message:

Footer Details

Change Footer Content:

Footer Content:

Footer Font Color:

External Payment Gateway

Enable External Payment Gateway: ☐

Session Title 1:

Message:

Session Title 2:

Success Message:

Session Title 3:

Failure Message:

Enable Billing Profiles

| Profile Name | Billing Status | Description | Status |
|----------------------------|----------------|-------------|--------|
| No data available in table | | | |

Service Disclaimer Text:

Payment Server:

3. Complete the fields in the table on the next page and click **Save**.

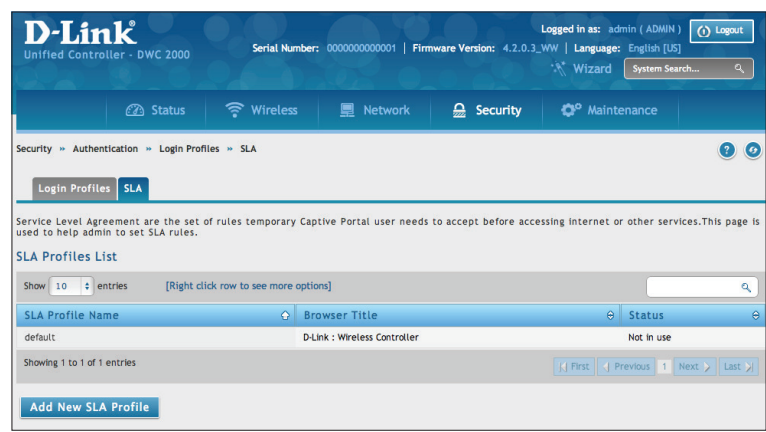
| Field | Description |
|---------------------------------|--|
| General Details | |
| Profile Name | Enter a name for this captive portal profile. The name should allow you to differentiate this captive profile from others you may set up. |
| Browser Title | Enter the text that will appear in the title of the browser during the captive portal session. |
| Background | <p>Select whether the login page displayed during the captive portal session will show an image or color. Choices are:</p> <ul style="list-style-type: none"> Image = displays an image as the background on the page. Use the Page Background Image field to select a background image. Color = sets the background color on the page. Select the color from the drop-down menu |
| Page Background Image | If you set <i>Background</i> to Image , upload the image file by clicking Add > Browse . Select an image, click Open and then click the Upload button. The maximum size of the image is 50 kb. |
| Page Background Upload | Choose the file you want to upload. |
| Page Background Color | If you set <i>Background</i> to Color , select the background color of the page that will appear during the captive portal session from the drop-down menu. |
| Custom Color | If you choose Custom on Page Background Color, enter the HTML color code. |
| Header Details | |
| Background | <p>Select whether the login page displayed during the captive portal session will show an image or color. Choices are:</p> <ul style="list-style-type: none"> Image = show image on the page. Use the Header Background Color field to select a background color. The maximum size of the image is 50 kb. Color = show background color on the page. Use the radio buttons to select an image. |
| Header Background Image | If you set <i>Background</i> to Image , upload the image file by clicking Add > Browse . Select an image, click Open and then click the Upload button. The maximum size of the image is 50 kb. |
| Header Background Upload | Choose the file you want to upload. |
| Header Background Color | If you set <i>Background</i> to Color , select the header color from the drop-down menu. |
| Custom Color | If you choose Custom on Page Background Color, you can choose particular color by filling in the HTML color code. |
| Header Caption | Enter the text that appears in the header of the login page during the captive portal session. |
| Caption Font | Select the font for the header text. |
| Font Size | Select the font size for the header text. |
| Font Color | Select the font color for the header text. |

| Field | Description |
|--|---|
| Login Details | |
| Login Section Title | Enter the text that appears in the title of the login box when the user logs in to the captive portal session. This field is optional. |
| Welcome Message | Enter the welcome message that appears when users log in to the captive session successfully. This field is optional. |
| Error Message | Enter the error message that appears when users fail to log in to the captive session successfully. This field is optional. |
| Footer Details | |
| Change Footer Content | Enables or disables changes to the footer content on the login page. |
| Footer Content | If Change Footer Content is checked, enter the text that appears in the footer. |
| Footer Font Color | If Change Footer Content is checked, select the color of the text that appears in the footer. |
| External Payment Gateway | |
| Enable External Payment Gateway | Enables or disables external payment gateway and online wireless service purchasing from on the login page. |
| Session Title 1 | Enter the text that appears in the title of the online purchasing login box when the user logs in to the captive portal session. |
| Message | Enter the text appears in the online purchasing login box when the user logs in to the captive portal session. |
| Session Title 2 | Enter the text that appears in the title of the message box while online purchasing is complete. |
| Success Message | Enter the text that appears in the message box while online purchasing is complete. |
| Session Title 3 | Enter the text that appears in the title of the message box while online purchasing is fail. |
| Failure Message | Enter the text that appears in the message box while online purchasing is fail. |
| Enable Billing Profile | Select the billing profile which will be shown on the login page. The table only listed the billing profiles which are set Unit Price. Enable the billing profile by switch ON on STATUS. |
| Service Disclaimer Text | Enter the service disclaimer text which is shown before user select and purchase wireless service. |
| Payment Server | Select the payment received account and its payment agent. |

Customize the SLA of the Captive Portal

Path: Security > Authentication > Login Profiles > SLA

- 1. Go to **Security > Authentication > Login Profiles > SLA** tab.



- 2. Click **Add New SLA Profile**.



- 3. Complete the fields in the table below and click **Save**

| Field | Description |
|----------------------|---|
| SLA Profile Name | Enter a name for this SLA profile. The name should allow you to differentiate this SLA from others you may set up. |
| Browser Title | Enter the text that will appear in the title of the browser during the captive portal session. |
| Term of Service Rule | Shows the set of rules on Captive Portal which is set for temporary and SLA type users. The user needs to accept before accessing internet. |

External Authentication

The local user database present in the controller itself is typically used for granting management access for the GUI or CLI. External authentication servers are typically more secure, and can be used for allowing wireless AP connections, authenticating IPsec endpoints, and even allowing access via a Captive Portal on the VLAN. This section describes the available authentication servers on the controller, and also the configuration requirements. In all cases, the “Server Checking” button is used to verify connectivity to the configured server(s).

Configure RADIUS Server

Path: Security > Authentication > External Auth Server > RADIUS Server

Enterprise Mode for wireless security uses a RADIUS Server for WPA and/or WPA2 security. A RADIUS server must be configured and accessible by the controller to authenticate wireless client connections to an AP enabled with a profile that uses RADIUS authentication.

- The Authentication IP Address is required to identify the server. A secondary RADIUS server provides redundancy in the event that the primary server cannot be reached by the controller when needed.
- Authentication Port - The port for the RADIUS server connection
- Secret - Enter the shared secret that allows this controller to log into the specified RADIUS server(s). This key must match the shared secret on the RADIUS Server.
- The Timeout and Retries fields are used to either move to a secondary server if the primary cannot be reached, or to give up the RADIUS authentication attempt if communication with the server is not possible.

To configure RADIUS Server:

1. Go to **Security > Authentication > External Auth Server > RADIUS Server** tab.

D-Link
Unified Controller - DWC 2000

Serial Number: 000000000001 | Firmware Version: 4.2.0.3_WW | Language: English [US]

Logged in as: admin (ADMIN) [Logout]

Wizard System Search...

Security > Authentication > External Auth Server > RADIUS Server

Radius Server POP3 Server POP3 Trusted CA LDAP Server

This page configures the RADIUS servers to be used for authentication. A RADIUS server maintains a database of user accounts used in larger environments. If a RADIUS server is configured in the LAN, it can be used for authenticating users that want to connect to the wireless network provided by this device. If the first/primary RADIUS server is not accessible at any time, then the device will attempt to contact the secondary RADIUS server for user authentication.

Radius Server Configuration

Server Check **Server Checking**

Authentication Server 1 IP Address: 192.168.1.2
 Authentication Port: 1812 [Range: 0 - 65535]
 Secret: *****
 Timeout: 1 [Range: 1 - 999] Seconds
 Retries: 2 [Range: 1 - 9] Seconds

Authentication Server 2 IP Address: 192.168.1.3
 Authentication Port: 1812 [Range: 0 - 65535]
 Secret: *****
 Timeout: 1 [Range: 1 - 999]
 Retries: 2 [Range: 1 - 9]

Authentication Server 3 IP Address: 192.168.1.4
 Authentication Port: 1812 [Range: 0 - 65535]
 Secret: *****
 Timeout: 1 [Range: 1 - 999]
 Retries: 2 [Range: 1 - 9]

Save Cancel

2. Complete the RADIUS server information from the table below and click **Save**.

| Field | Description |
|-----------------------|--|
| Authentication Server | IP address of the RADIUS authentication server. |
| Authentication Port | RADIUS authentication server port to send RADIUS messages. |
| Secret | Secret key that allows the device to log into the configured RADIUS server. It must match the secret on RADIUS server. |
| Timeout | Set the amount of time in seconds, the controller should wait for a response from the RADIUS server. |
| Retries | This determines the number of tries the controller will make to the RADIUS server before giving up. |

Configure POP3 Server

Path: Security > Authentication > External Auth Server > POP3 Server

POP3 is an application layer protocol most commonly used for e-mail over a TCP/IP connection. The authentication server can be used with SSL encryption over port 995 to send encrypted traffic to the POP3 server. The POP3 server's certificate is verified by a user-uploaded CA certificate. If SSL encryption is not used, port 110 will be used for the POP3 authentication traffic.

The wireless controller acts only as a POP3 client to authenticate a user by contacting an external POP3 server. This authentication option is available for IPsec, PPTP/L2TP Server and Captive Portal users. Note that POP3 for PPTP / L2TP servers is supported only with PAP and not with CHAP / MSCHAP / MSCHAPv2 encryption.

To configure POP3 Server:

1. Go to **Security > Authentication > External Auth Server > POP3 Server** tab.

The screenshot shows the D-Link Unified Controller web interface. The top navigation bar includes Status, Wireless, Network, Security, and Maintenance. The breadcrumb trail is Security > Authentication > External Auth Server > POP3 Server. The POP3 Server Configuration page is displayed, showing three authentication servers (Primary, Secondary, and Tertiary) and their respective ports, SSL settings, and CA files. The Timeout is set to 10 seconds and Retries to 5.

2. Complete the fields in the table below and click **Save**.

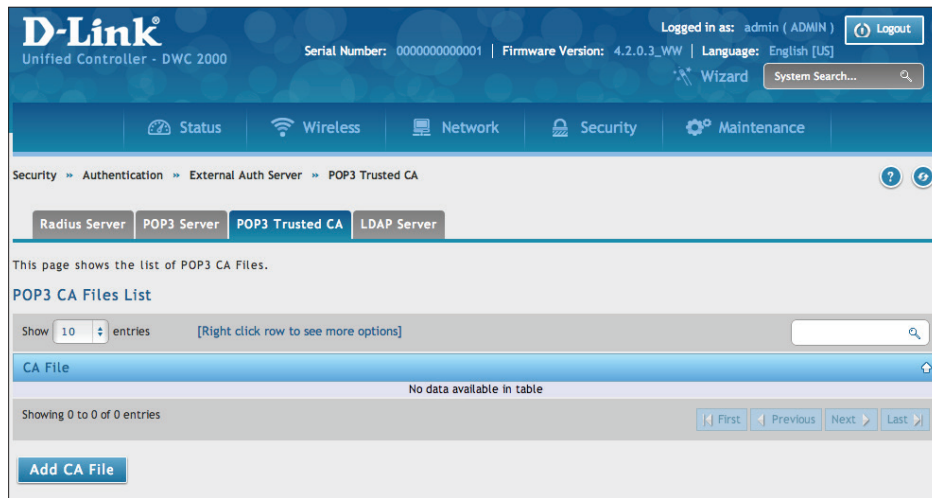
| Field | Description |
|------------------------------|---|
| Authentication Server | IP address of the POP3 authentication server. |
| Authentication Port | RADIUS authentication server port to send POP3 messages. |
| SSL Enable | Enable SSL support for POP3. If this option is enabled, it is mandatory to select a certificate authority for it. |
| CA File | Certificate Authority to verify POP3 server's certificate. |
| Timeout | Set the amount of time in seconds, the controller should wait for a response from the POP3 server. |
| Retries | This determines the number of tries the controller will make to the POP3 server before giving up. |

Configure POP3 Trusted CA

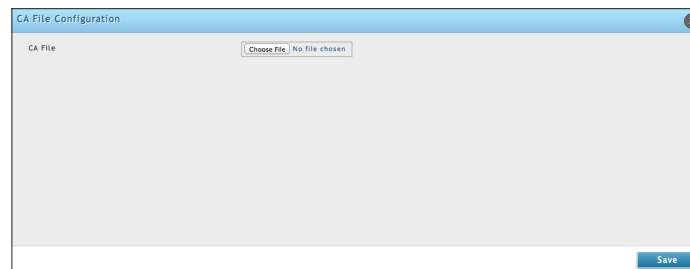
Path: Security > Authentication > External Auth Server > POP3 Trusted CA

A CA file is used as part of the POP3 negotiation to verify the configured authentication server identity. Each of the three configured servers can have a unique CA used for authentication.

1. Go to **Security > Authentication > External Auth Server > POP3 Trusted CA** tab.



2. Add the CA file by click **Add CA File**.



3. Click **Choose File** and browse to the CA file. Once selected, click **Save**.

Configure LDAP Server

Path: Security > Authentication > External Auth Server > LDAP Server

The LDAP authentication method uses LDAP to exchange authentication credentials between the controller and external server. The LDAP server maintains a large database of users in a directory structure, so users with the same username but belonging to different groups can be authenticated since the user information is stored in a hierarchal manner. Also of note is that configuring a LDAP server on Windows or Linux servers is considerably less complex than setting up NT Domain or Active Directory servers for user authentication.

The details configured on the controller will be passed for authenticating the controller and its hosts. The LDAP attributes, domain name (DN), and in some cases the administrator account & password are key fields in allowing the LDAP server to authenticate the controller.

To configure LDAP Server:

1. Go to **Security > Authentication > External Auth Server > LDAP Server** tab.

D-Link
Unified Controller - DWC 2000

Serial Number: 0000000000001 | Firmware Version: 4.2.0.3_WW | Language: English [US]

Logged in as: admin (ADMIN) [Logout]

Wizard System Search...

Status Wireless Network **Security** Maintenance

Security » Authentication » External Auth Server » LDAP Server

Radius Server POP3 Server POP3 Trusted CA **LDAP Server**

This page allows a user to configure authentication servers for LDAP authentication.

LDAP Server Configuration

| | | |
|------------------------------|---|----------|
| Authentication Server 1 | <input type="text"/> | |
| Authentication Server 2 | <input type="text"/> | Optional |
| Authentication Server 3 | <input type="text"/> | Optional |
| LDAP attribute 1 | <input type="text"/> | Optional |
| LDAP attribute 2 | <input type="text"/> | Optional |
| LDAP attribute 3 | <input type="text"/> | Optional |
| LDAP attribute 4 | <input type="text"/> | Optional |
| LDAP Base DN | <input type="text"/> | |
| Second LDAP Base DN | <input type="text"/> | Optional |
| Third LDAP Base DN | <input type="text"/> | Optional |
| Timeout | <input type="text"/> [Range: 1 - 999] Seconds | |
| Retries | <input type="text"/> 2 [Range: 1 - 9] | |
| First Administrator Account | <input type="text"/> admin | Optional |
| Password | <input type="password"/> | Optional |
| Second Administrator Account | <input type="text"/> | Optional |
| Password | <input type="password"/> | Optional |
| Third Administrator Account | <input type="text"/> | Optional |
| Password | <input type="password"/> | Optional |

Save **Cancel**

2. Complete the fields in the table on the next page and click **Save**.

| Field | Description |
|-----------------------------|---|
| Authentication Server (1-3) | IP address of the LDAP authentication server. |
| LDAP Attribute | These are attributes related to LDAP users configured in LDAP server. These may include attributes like SAM account name, Associated domain name etc. These can be used to distinguish between different users having same user name. |
| LDAP Base DN | LDAP authentication requires the base domain name; contact your administrator for the Base DN to use LDAP authentication for this domain. |
| Timeout | Set the amount of time in seconds, the controller should wait for a response from the LDAP server. |
| Retries | This determines the number of tries the controller will make to the LDAP server before giving up. |
| Administrator Account | Admin account in LDAP server that will be used when LDAP authentication is required for PPTP/L2TP connection. |
| Password | Enter the admin password. |

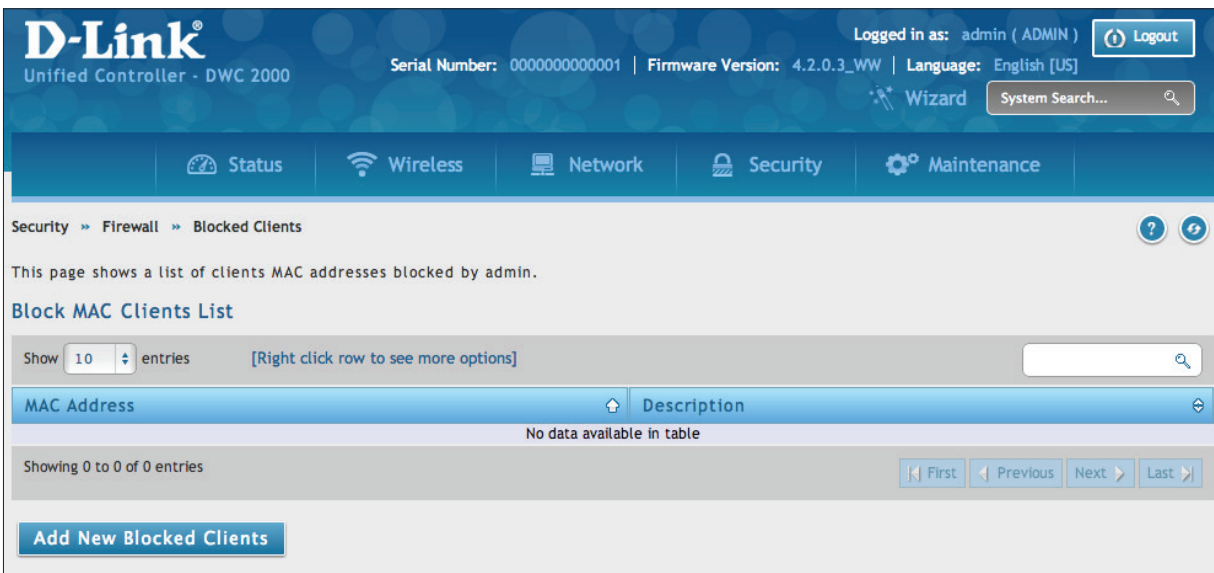
Blocked Clients

Path: Security > Firewall > Blocked Clients

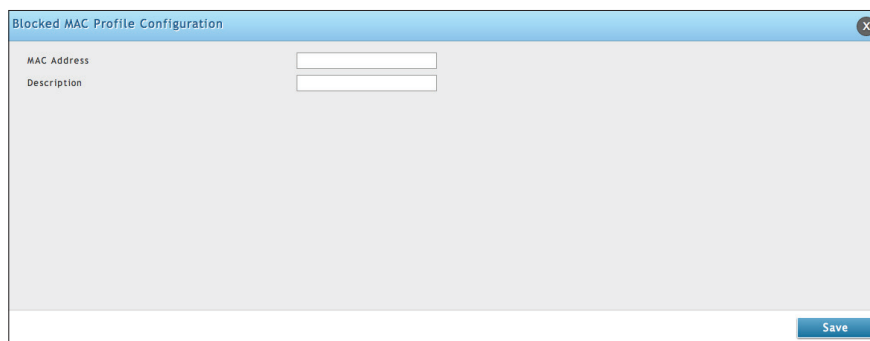
If traffic passes through the DCS-2000 directly, the controller will block the traffic from blocked clients (MAC address).

To add clients to block:

1. Go to **Security > Firewall > Blocked Clients**.



2. Click **Add New Blocked Clients**. Enter the client's MAC address and a description.
3. Click **Save**.



Status and Statistics

This chapter describes the following pages, which display wireless controller and access point status information and statistics.

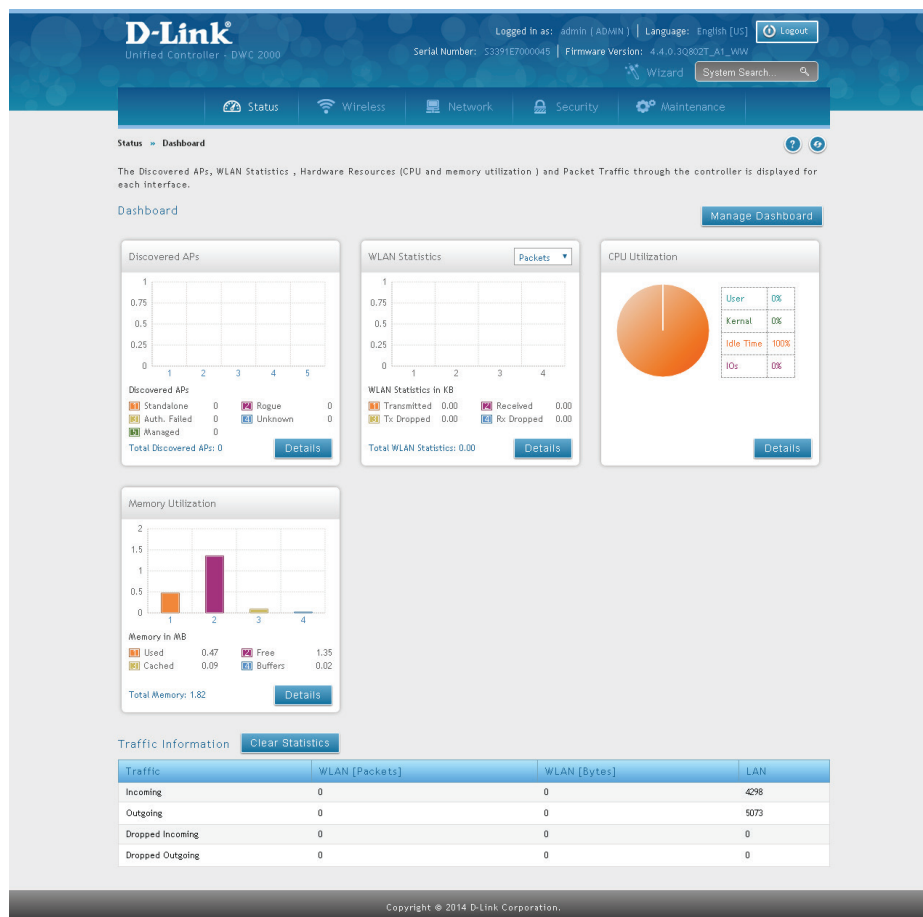
| Path | Description | Page |
|--|---|------|
| Status > Dashboard | Shows device status, wireless/ wired traffic statistic, tunnels, associated client, and utilization. | 195 |
| Status > Dashboard > Traffic Overview | Shows information about network services traffic on the access point's wired and wireless interfaces. | 197 |
| Status > System Information > Device | Summarizes the wireless controller configuration settings. | 198 |
| Status > System Information > All Logs | Shows log messages of controller activities (Current, WLAN, and LAN) | 274 |
| Status > System Information > USB Status | Shows information about the USB devices connected to the USB port(s) | 199 |
| Status > Network Information > DHCP Clients > LAN Leased Clients | Shows the list of DHCP clients connected to the LAN DHCP Server and to whom DHCP Server has given leases. | 200 |
| Status > Network Information > DHCP Clients > IPv6 Leased Clients | Shows the list of DHCPv6 clients connected to the LAN DHCPv6 Server and to whom DHCPv6 Server has given leases. | 200 |
| Status > Network Information > Captive Portal Session | Shows the runtime authentication sessions that are active on the controller. | 201 |
| Status > Network Information > Interfaces | Shows detailed transmit and receive statistics for each physical port. | 202 |
| Status > Network Information > Link Aggregation | Shows the link aggregation status. | 204 |
| Status > Wireless Information > Controller Status | Shows status and priority about the Controller. | 205 |
| Status > Wireless Information > Controller Status > Controller Associated Clients | Shows information about the controller that manages the access point to which the client is associated. | 206 |
| Status > Wireless Information > Controller Status > Distributed Tunnel | Shows information about all the distributed tunnel clients. | 207 |
| Status > Wireless Information > Controller Status > Peer Controller Receive Status | Shows information about the configuration a controller receives from a peer. | 208 |
| Status > Wireless Information > Controller Status > Peer Controller Sent Status | Shows information about the configuration a controller sends to a peer. | 210 |
| Status > Wireless Information > Access Point > Global Status | This page shows status and statistics about the Controller and all of the objects associated with it. | 211 |

| Path | Description | Page |
|--|---|------|
| Status> Wireless Information> Access Point > > All APs | Shows summary information about managed, failed, and rogue access points the wireless controller has discovered or detected. | 213 |
| Status > Wireless Information > Access Point > Managed | Shows details about the managed access points. | 214 |
| Status > Wireless Information > Access Point > Peer Managed | Shows information about the access points that each peer controller in the cluster manages. | 216 |
| Status > Wireless Information > Access Point > Authentication Failed | Shows information about access points that failed to establish communication with the wireless controller. | 217 |
| Status > Wireless Information > Access Point > RF Scan | Shows information about other access points and wireless clients that the managed AP has detected. | 218 |
| Status > Wireless Information > Access Point > De-Authentication Attacks | Shows information about rogue APs that the Cluster Controller has attacked by using the de-authentication attack feature. | 219 |
| Status > Wireless Information > Access Point > Hardware Capability | Shows information about radio hardware and IEEE mode supported by access points, along with software images available for downloading to access points. | 221 |
| Status > Wireless Information > Associated Clients > Global Status | Shows statistics about all the clients' traffic while the clients are associated with managed access points as well as throughout the roaming session. | 223 |
| Status > Wireless Information > Associated Clients > Associated Clients | Shows information about all the clients connected through managed access points. | 224 |
| Status > Wireless Information > Associated Clients > Ad Hoc Clients | Shows information about all ad-hoc clients. | 228 |
| Status > Wireless Information > Associated Clients > Detected Clients | Shows information about clients that have authenticated with an access point, and clients that disassociate and are no longer connected to the system. | 229 |
| Status > Wireless Information > Clustering | Shows information about other wireless controllers in the network. | 231 |
| Status > Wireless Information> WDS Groups Status | Shows the summary information about configured WDS links | 232 |
| Status> Wireless Information> WDS Group Status > WDS Group AP Status | Shows WDS group AP status configured APs and links in the WDS Group. | 233 |
| Status > Wireless Information> WDS Group Status> WDS AP Status | Shows the status of configured APs and links in the WDS Group. | 235 |
| Status > Wireless Information> WDS Group Status> WDS Link Status | Shows WDS links in the WDS Group. | 236 |
| Status > Wireless Information> WDS Group Status> WDS Link Statistics | Shows the statistic WDS links in the WDS Group. | 237 |

Viewing Statistic and Utilization

Path: Status > Dashboard

The wireless controller provides a dashboard that displays about the resources the system is using . The dashboard page is organized into the following sections:

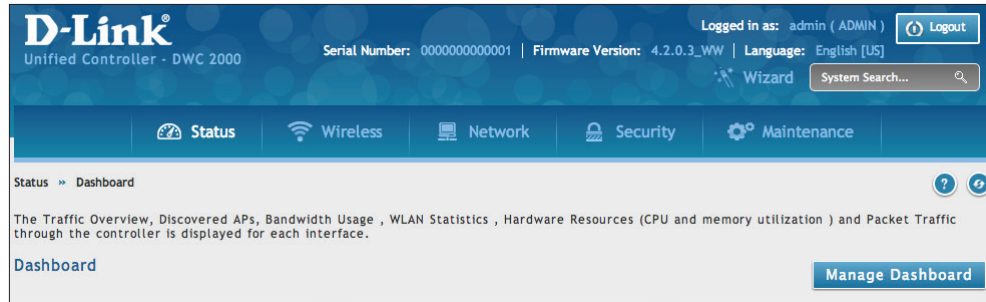


| Section | Description |
|---------------------|--|
| Discovered APs | Displays a chart of discovered Apps by their current status as detected by the DWC-2000. |
| WLAN Statistics | Displays a chart of traffic overview by bandwidth and packet information for WLAN traffic captured by all of the managed APs currently associated. |
| CPU Utilization | Percent of the CPU utilization currently consumed by the device. The CPU utilization is broken down into specifics such as all user space processes, such as management operations, kernel space processes, and CPU idle time or IO. |
| Memory Utilization | Displays a breakdown of memory usage by the amount used, free, cached, and currently in the system buffer. |
| Traffic Information | Displays a grid of traffic statistics for each interface. |

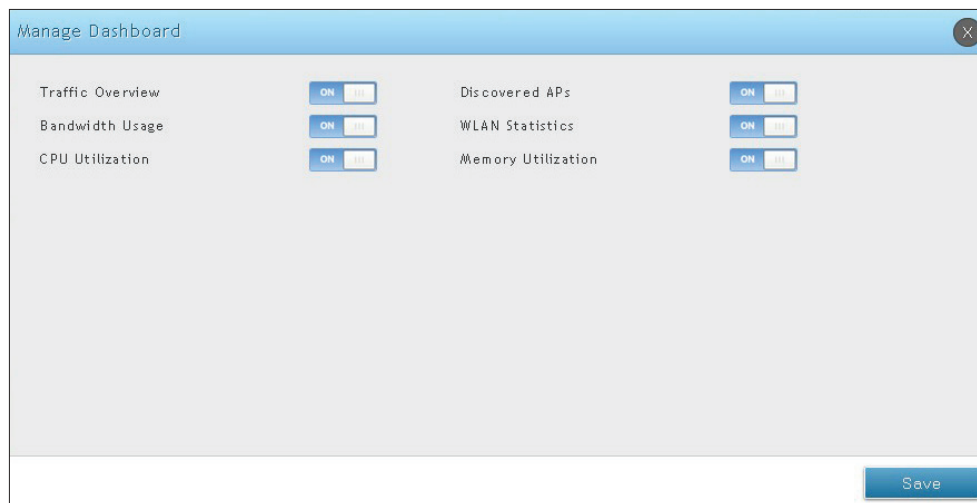
Manage Dashboard

To manage the dashboard:

1. Click on the **Manage Dashboard** button.

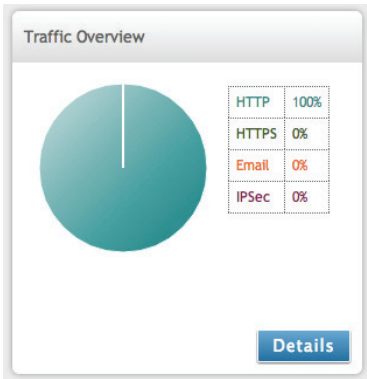


2. The following window will pop out and allow you to enable or disable the overview panels shown on the dashboard. Toggle the panel to **On** or **Off** and click **Save**.



Detail Information

You can review detail information or statistic by click Detail on each widget.



| Traffic Overview Details | |
|--------------------------|--------------|
| LAN | |
| HTTP | 70.407227 KB |
| HTTPs | 0.312500 KB |
| DNS | 6.211914 KB |
| IMAP2 | 0.000000 KB |
| IMAP3 | 0.000000 KB |
| NFS | 0.000000 KB |
| POP3 | 0.000000 KB |
| SMTP | 0.000000 KB |
| SNMP | 0.000000 KB |
| SSH | 0.000000 KB |
| TELNET | 0.000000 KB |

The Traffic Information table shows detailed transmit and receive statistics for each physical port. This includes:

- Port-specific packet-level information for each interface (LAN and VLANs)
- Transmitted and received packets
- Cumulating bytes/sec for transmit/receive directions for each interface

If you suspect issues with any of the wired ports, use this table to identify uptime or transmit level issues with the port. The statistics table has an auto-refresh control for displaying the most current port level data at each page refresh. The default auto-refresh for this page is 10 seconds. Click **Clear Statistics** to reset the traffic information.

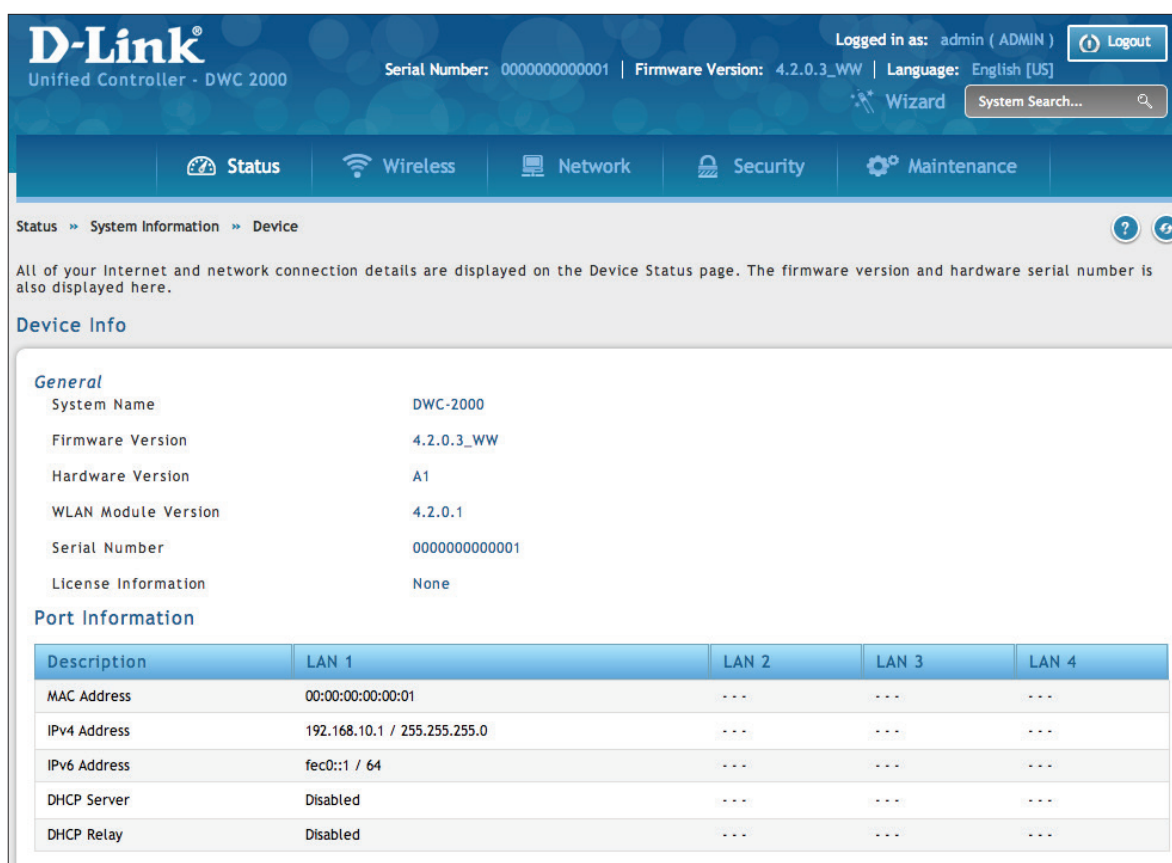
| Traffic Information | | Clear Statistics | |
|---------------------|----------------|------------------|------|
| Traffic | WLAN [Packets] | WLAN [Bytes] | LAN |
| Incoming | 0 | 0 | 3891 |
| Outgoing | 0 | 0 | 1255 |
| Dropped Incoming | 0 | 0 | 0 |
| Dropped Outgoing | 0 | 0 | 0 |

Viewing System Status

Path: Status > System Information > Device

The Device Info page summarizes the wireless controller configuration settings configured in the Setup and Advanced menus. This page is organized into the following sections:

- General - Shows system name, firmware version, WLAN module version, and serial number.
- Port Information – Shows information based on the administrator configuration parameters. Note that LAN1 will display the local interface of the controller. If you set any of the LAN ports to Standalone, information will be displayed under the corresponding LAN heading.



D-Link®
Unified Controller - DWC 2000

Logged in as: admin (ADMIN) [Logout]

Serial Number: 0000000000001 | Firmware Version: 4.2.0.3_WW | Language: English [US]

Wizard System Search...

Status Wireless Network Security Maintenance

Status » System Information » Device

All of your Internet and network connection details are displayed on the Device Status page. The firmware version and hardware serial number is also displayed here.

Device Info

General

| | |
|---------------------|---------------|
| System Name | DWC-2000 |
| Firmware Version | 4.2.0.3_WW |
| Hardware Version | A1 |
| WLAN Module Version | 4.2.0.1 |
| Serial Number | 0000000000001 |
| License Information | None |

Port Information

| Description | LAN 1 | LAN 2 | LAN 3 | LAN 4 |
|--------------|------------------------------|-------|-------|-------|
| MAC Address | 00:00:00:00:00:01 | --- | --- | --- |
| IPv4 Address | 192.168.10.1 / 255.255.255.0 | --- | --- | --- |
| IPv6 Address | fec0::1 / 64 | --- | --- | --- |
| DHCP Server | Disabled | --- | --- | --- |
| DHCP Relay | Disabled | --- | --- | --- |

Viewing USB Status

Path: Status > System Information > USB Status

The USB Status page summarizes the USB devices connected to the wireless controller . The wireless controller allows to connect USB printer and USB disk (for firmware upgrade only) directly. There are two USB ports.

StatusWirelessNetworkSecurityMaintenance

Status » System Information » USB Status

This page displays information about the USB devices connected to the USB port(s).this page will update dynamically to show the status of the USB devices connected to the controller.

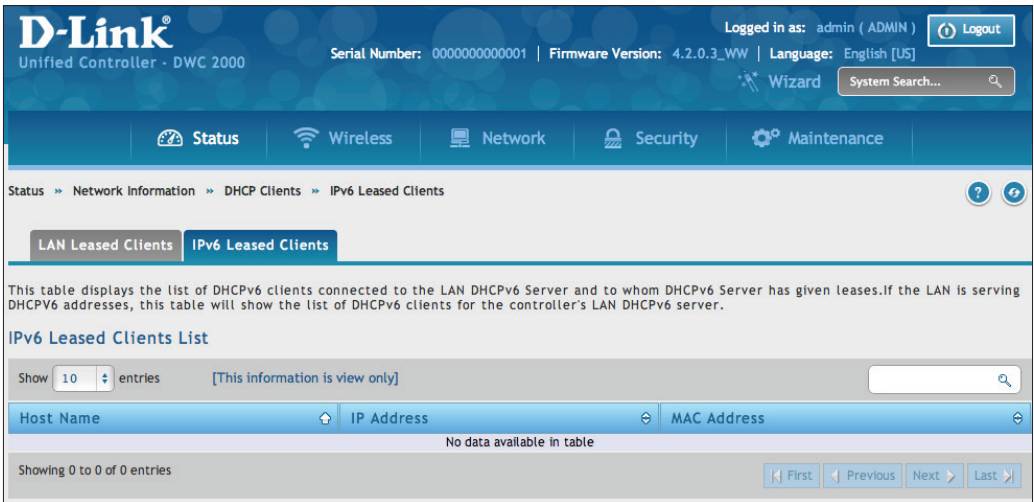
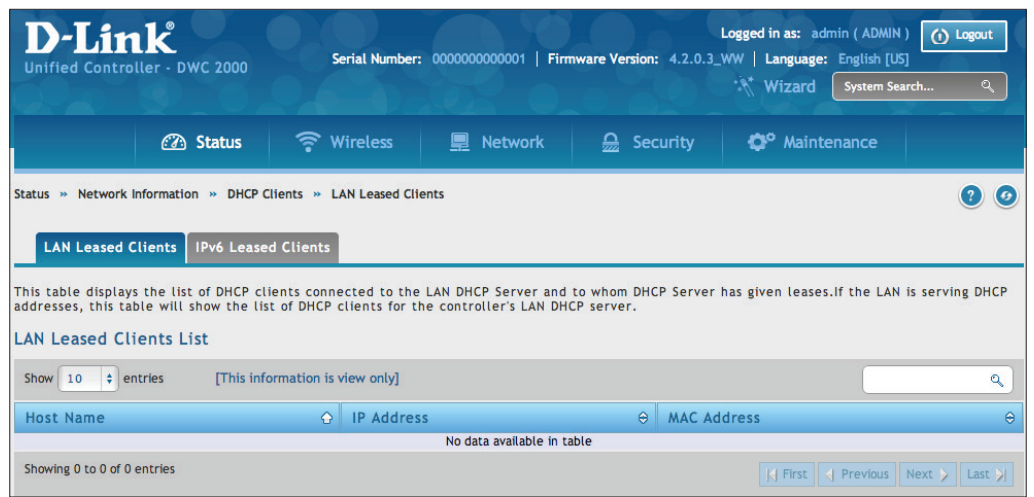
USB(s) Status

| Description | USB Port 1 | USB Port 2 |
|--------------|------------------|--------------|
| Status | connected | disconnected |
| Vendor | Kingston | NA |
| Model | DataTraveler_2.0 | NA |
| Type | storage | NA |
| Mount Status | 1 | NA |

Viewing DHCP Clients

Path: Status > Network Information > DHCP Clients

Two separated tabs shows a list of clients whom get IP leased from the wireless controller: LAN leased clients and LAN IPv6 leased clients.



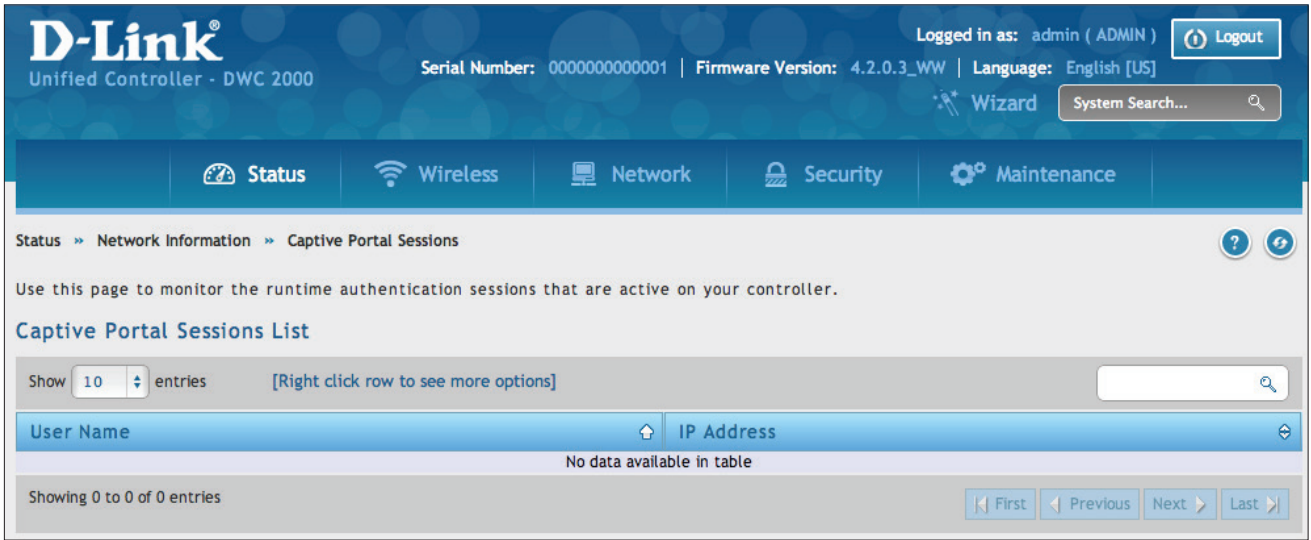
Viewing Captive Portal Sessions

Path: Status > Network Information > Captive Portal Sessions

The active run time internet sessions through the controller’s managed AP’s is listed in the below table. These users are present in the local or external user database and have had their login credentials approved for internet access.

If Internet session passthrough is enabled, select the session and right-click **Disconnect** allowing the admin to selectively drop an authenticated user.

Select the session and right-click **Block device**. The “Block Device” button will result in the selected client being added to the blocked list (Security > Firewall > Blocked Clients), and the current and future sessions from this client will be prevented.



Viewing Traffic on Interfaces

Path: Status > Network Information > Interfaces

This page shows the incoming/outgoing packets on each interface. Table fields are shown on the next page.

The screenshot shows the D-Link Unified Controller - DWC 2000 web interface. The top navigation bar includes 'Status', 'Wireless', 'Network', 'Security', and 'Maintenance'. The 'Status' tab is selected, and the breadcrumb path is 'Status > Network Information > Interfaces'. The page title is 'Interfaces'. Below the title, a message states: 'The profiled and packet traffic through the controller is displayed for each interface..'. The main content area is divided into three sections: 'LAN info', 'VLAN info', and 'WLAN info'.

LAN info

| Description | LAN 1 | LAN 2 | LAN 3 | LAN 4 |
|-----------------------------|--------------|-------|-------|-------|
| Incoming Packets / Bytes | 13893 / 1MB | --- | --- | --- |
| Outgoing Packets / Bytes | 13708 / 18MB | --- | --- | --- |
| Dropped In Packets / Bytes | 0 / 0B | --- | --- | --- |
| Dropped Out Packets / Bytes | 0 / 0B | --- | --- | --- |

VLAN info

Show 10 entries [This information is view only]

| VLAN | Incoming [Packets / Bytes] | Outgoing [Packets / Bytes] | Dropped In [Packets / Bytes] | Dropped Out [Packets / Bytes] |
|----------------------------|----------------------------|----------------------------|------------------------------|-------------------------------|
| No data available in table | | | | |

Showing 0 to 0 of 0 entries

WLAN info

| Data Information | Packets / Bytes |
|------------------|-----------------|
| Transmitted | 0 / 6B |
| Received | 0 / 5B |
| Transmit Dropped | 0 / 8B |
| Receive Dropped | 0 / 7B |

Active Info

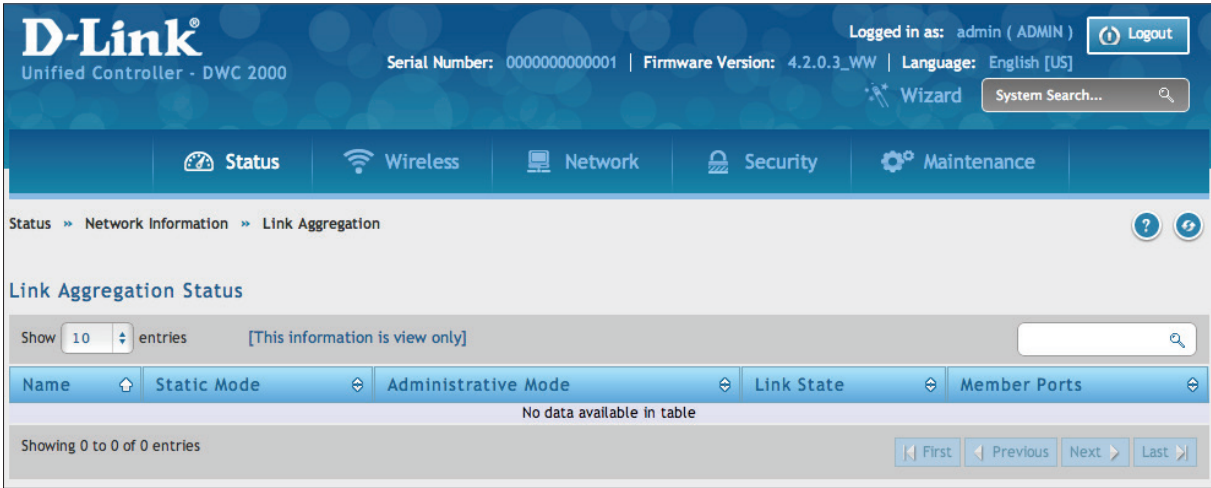
| Description | Count |
|-------------------|-------|
| ICMP Received | 10 |
| Available VLANs | 1 |
| Active Interfaces | 1 |

| Section | Description |
|---------------------------|---|
| LAN Info (LAN 1-4) | |
| Incoming Packets | The number of IP packets entering the port. |
| Outgoing Packets | The number of packets leaving the port. |
| Dropped In Packets | Packets dropped on the inbound path of the interface. |
| Dropped Out Packets | Packets dropped on the outbound path of the interface. |
| VLAN Info | |
| Port | The port that the VLAN is associated with. |
| Incoming Packets | The number of IP packets entering the port. |
| Outgoing Packets | The number of packets leaving the port. |
| Dropped In Packets | Packets dropped on the inbound path of the interface. |
| Dropped Out Packets | Packets dropped on the outbound path of the interface. |
| WLAN Info | |
| Transmitted | Total packets transmitted across all APs managed by the controller. |
| Received | Total packets received across all APs managed by the controller. |
| Transmit Dropped | Total packets transmitted across all APs managed by the controller that were dropped. |
| Receive Dropped | Packets dropped on the inbound path of the interface. |
| Dropped Out Packets | Total packets received across all APs managed by the controller that were dropped. |

Viewing Link Aggregation

Path: Status > Wireless Information > Controller Status > Link Aggregation

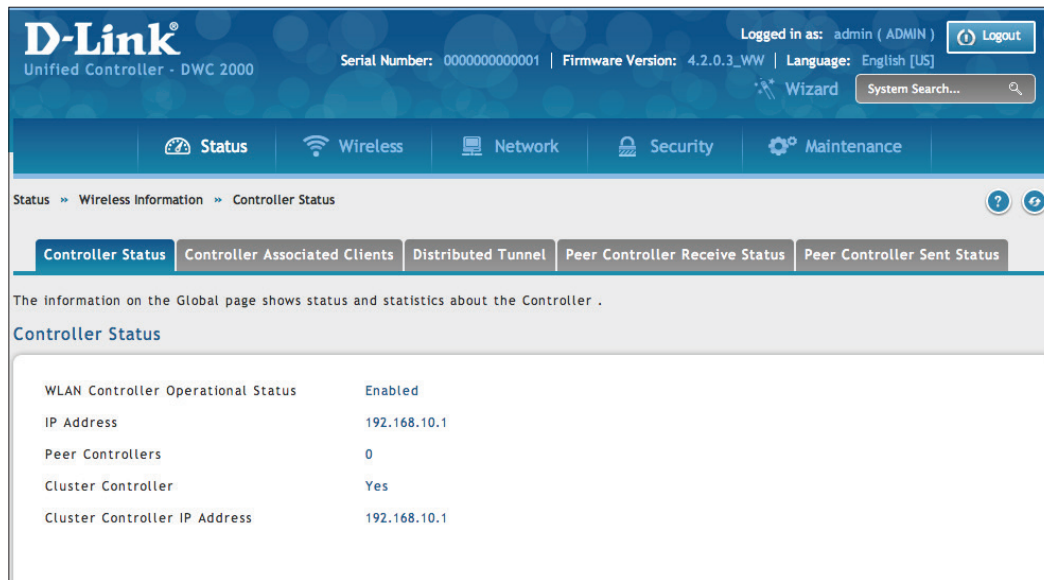
This page shows the link aggregation status.



Viewing Controller Status and Statistics

Path: Status > Wireless Information > Controller Status > Controller Status

This page shows the controller status and information.

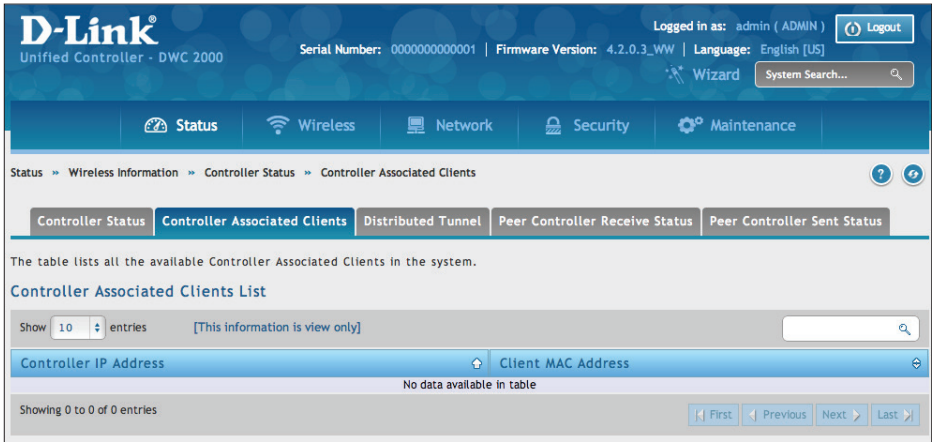


| Field | Description |
|------------------------------------|---|
| WLAN Controller Operational Status | This status field displays the operational status of the WLAN controller. |
| IP Address | The IP address of the wireless controller. |
| Peer Controllers | The number of peer WLAN controllers detected on the network. |
| Cluster Controller | Indicates whether this controller is the Cluster Controller for the cluster. Among a group of peer Controllers, one of the Controllers is automatically elected or configured to be the Cluster Controller. The Cluster Controller gathers status and statistics about all APs and clients in the peer group. Note: Only the Cluster Controller controller can display managed APs, clients, statistics, and RF Scan databases for the whole cluster. The Controllers that are not Cluster Controllers can display information only about locally attached devices. |
| Cluster Controller IP Address | The IP address of the peer controller that is the Cluster Controller. |

Controller Associated Clients

Path: Status > Wireless Information > Controller Status > Controller Associated Clients

This page shows the controller and its associated clients. If this controller is the Cluster Controller, it will also show the associated clients whom is managed with other peer controllers.



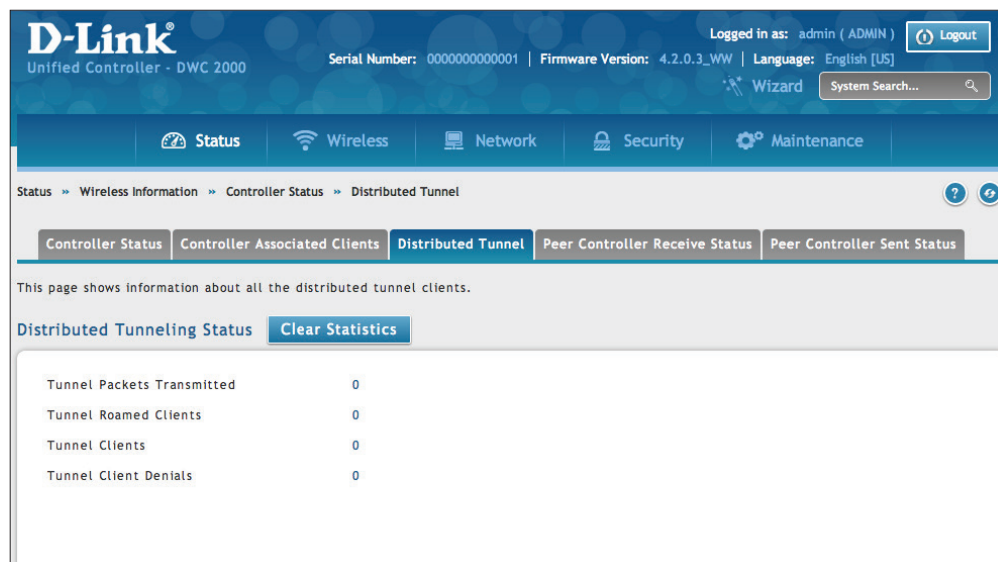
| Field | Description |
|-----------------------|---|
| Controller IP Address | Shows the IP address of the Controller that manages the AP to which the client is associated. |
| Client MAC Address | Shows the MAC address of the associated client. |

Distributed Tunnel

Path: Status > Wireless Information > Controller Status > Distributed Tunnel

The AP-AP tunneling mode is used to support L3 roaming for wireless clients without forwarding any data traffic to the wireless controller.

In the AP-AP tunneling mode, when a client first associates with an AP in the wireless system, the AP forwards the wireless client's data using VLAN forwarding mode. The AP the client initially associates with is called the Home AP. The AP the client roams to is called the Association AP.

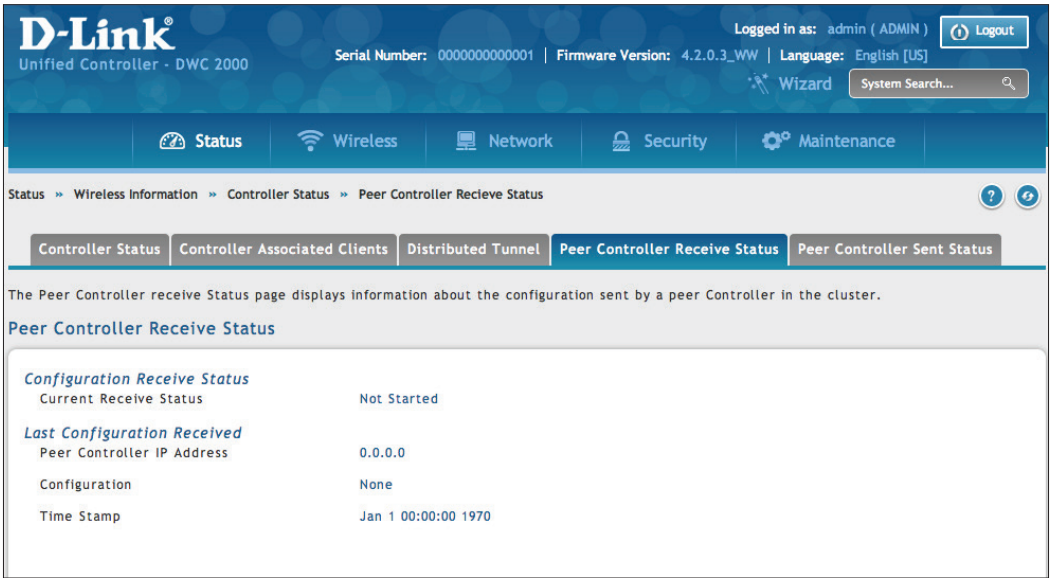


| Field | Description |
|---|---|
| Distributed Tunnel Packets Transmitted | Total number of packets sent by all APs via distributed tunnels. |
| Distributed Tunnel Roamed Clients | Total number of client that successfully roamed away from Home AP using distributed tunneling. |
| Tunnel Clients | Total number of clients that are associated with an AP that are using distributed tunneling. |
| Tunnel Client Denials | Total number of clients for which the system was unable to setup a distributed tunnel when client roamed. |

Peer Controller Receive Status

Path: Status > Wireless Information > Controller Status > Peer Controller Receive Status

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



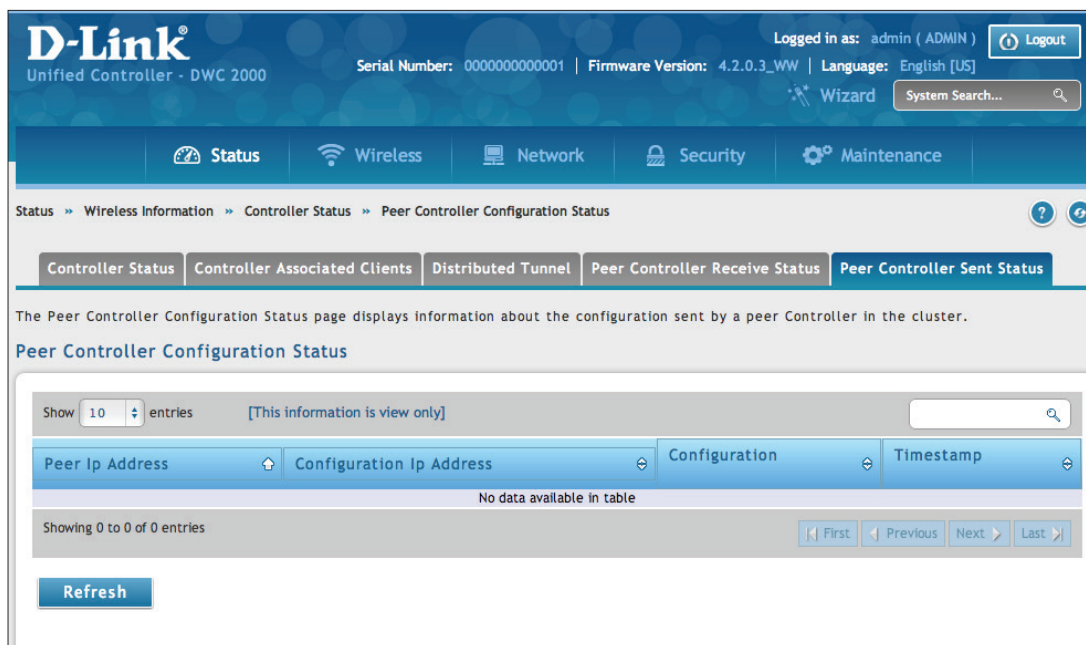
| Field | Description |
|------------------------|--|
| Current Receive Status | |
| Current Receive Status | Global status when wireless configuration is received from a peer controller. Possible status values are: <ul style="list-style-type: none">• Not Started• Receiving Configuration• Saving Configuration• Applying AP Profile Configuration• Success• Failure - Invalid Code Version• Failure - Invalid Hardware Version• Failure - Invalid Configuration |

| Last Configuration Received | |
|-----------------------------|---|
| Peer Controller IP Address | Peer controller IP address of the last wireless controller from which this controller received any wireless configuration data. |
| Configuration | <p>Shows which portions of configuration were last received from a peer controller. Possible values are:</p> <ul style="list-style-type: none">• Global• Discovery• Channel/Power• AP Database• AP Profiles• Known Client• Captive Portal• RADIUS Client• QoS ACL• QoS DiffServ• None = wireless controller has not received any configuration for another controller |
| Timestamp | <p>Shows the last time this wireless controller received any configuration data from a peer controller. The Peer Controller Managed AP Status page shows information about the access points that each peer controller in the cluster manages. Use the drop-down list at the top of this page to select a peer controller whose access point information you want to view. Each peer controller is identified by its IP address.</p> |

Peer Controller Sent Status

Path: Status > Wireless Information > Controller Status > Peer Controller Sent Status

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



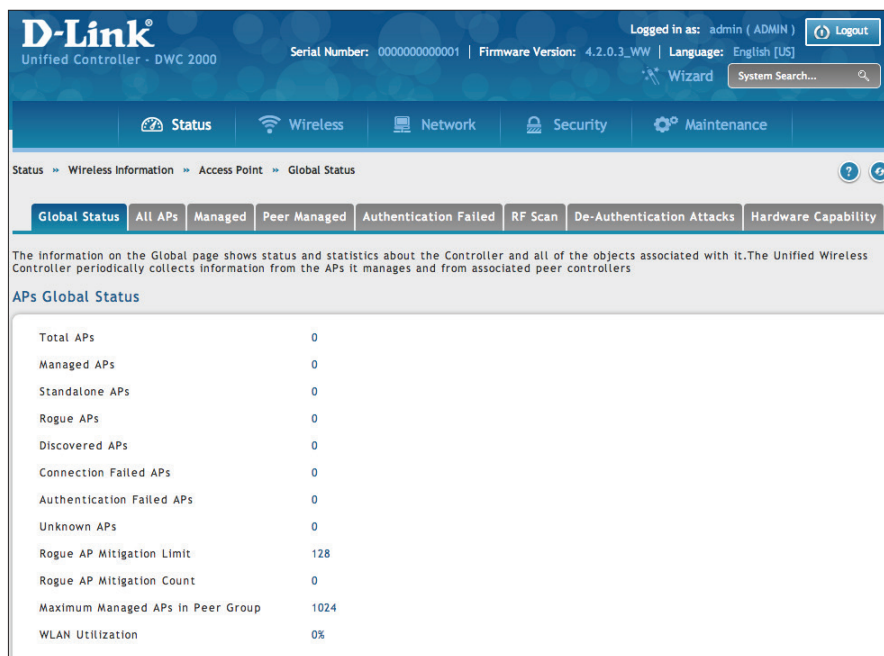
| Field | Description |
|-------------------------------------|--|
| Peer Controller IP Address | Shows the IP address of each peer wireless controller in the cluster that received configuration information. |
| Configuration Controller IP Address | Shows the IP Address of the controller that sent the configuration information. |
| Configuration | Identifies which parts of the configuration the controller received from the peer controller. |
| Timestamp | Shows when the configuration was applied to the controller. The time is displayed as UTC time and therefore only useful if the administrator has configured each peer controller to use NTP. |

Viewing Access Point Information

Global Status

Path: Status > Wireless Information > Access Point > Global Status

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



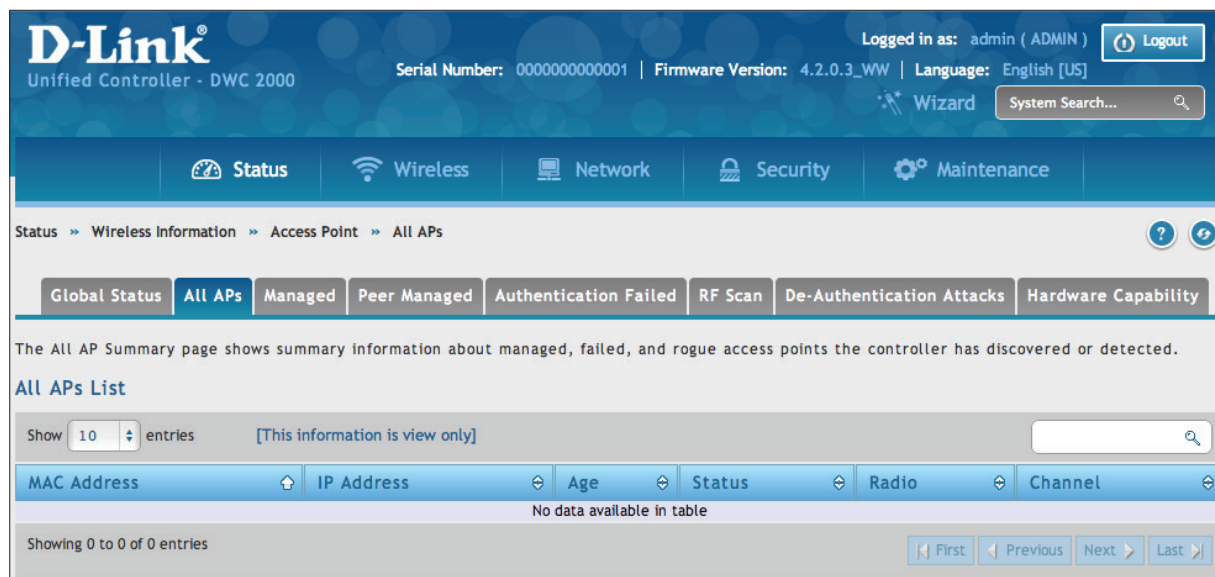
| Field | Description |
|----------------------------------|---|
| Total APs | Total number of Managed APs in the database. This value is always equal to the sum of Managed Access Points, Connection Failed Access Points, and Discovered Access Points. |
| Managed APs | Number of APs in the managed AP database that are authenticated, configured, and have an active connection with the Wireless controller. |
| Standalone APs | Number of trusted APs in Standalone mode. APs in Standalone mode are not managed by a controller. |
| Rogue APs | Number of Rogue APs currently detected on the WLAN. When an AP performs an RF scan, it might detect access points that have not been validated. It reports these APs as rogues. |
| Discovered APs | APs that have a connection with the controller, but haven't been completely configured. This value includes all managed APs with a Discovered or Authenticated status. |
| Connection Failed APs | Number of APs that were previously authenticated and managed, but currently don't have connection with the Wireless controller. |
| Authentication Failed APs | Number of APs that failed to establish communication with the FASTPATH Unified Wireless controller. |

| | |
|--|--|
| Unknown APs | Number of Unknown APs currently detected on the WLAN. If an AP configured to be managed by the Wireless controller is detected through an RF scan at any time that it is not actively managed it is classified as an Unknown AP. |
| Rogue AP Mitigation Limit | Maximum number of APs for which the system can send de-authentication frames. |
| Rogue AP Mitigation Count | Number of APs to which the wireless system is currently sending de-authentication messages to mitigate against rogue APs. A value of 0 indicates that mitigation is not in progress. |
| Maximum Managed APs in Peer Group | Maximum number of access points that can be managed by the cluster. |
| WLAN Utilization | Total network utilization across all APs managed by this controller. This is based on global statistics. |

All APs

Path: Status > Wireless Information > Access Point > All APs

The All APs List page shows summary information about managed, failed, and rogue access points the wireless controller has discovered or detected. Status entries can be deleted manually.

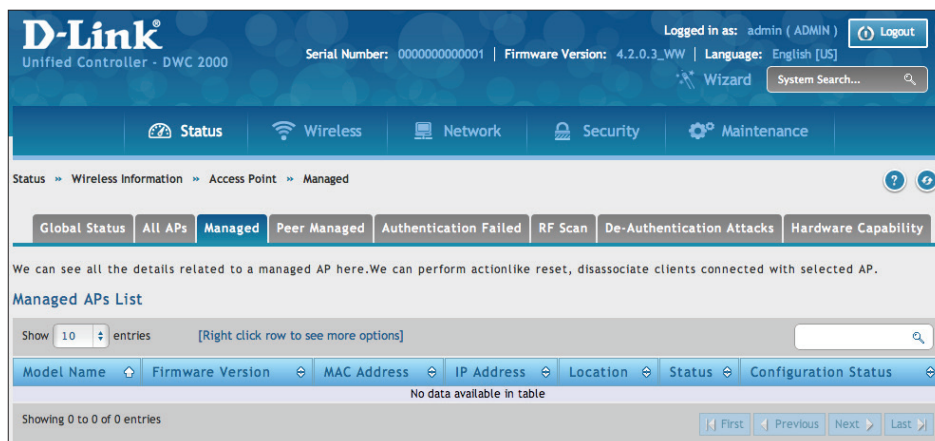


| Field | Description |
|-------------|---|
| MAC Address | MAC address of the access point. |
| IP Address | IP address of the access point. |
| Age | Amount of time that has passed since the access point was last detected and the information was last updated. |
| Status | Access point status. Possible values are: <ul style="list-style-type: none"> Managed = access point profile configuration has been applied to the access point and the access point is operating in managed mode. No Database Entry = access point's MAC address does not appear in the local or RADIUS Valid AP database. Authentication (Failed AP) = access point failed to be authenticated by the wireless controller or RADIUS server. Failed = wireless controller lost contact with the access point. A failed entry will remain in the Managed AP database unless you remove it. Note: a managed access point shows a failed status temporarily during a reset. Rogue = access point has not tried to contact the wireless controller and the access point's MAC address is not in the Valid AP database. |
| Radio | Wireless radio mode the access point is using. |
| Channel | Operating channel for the radio. |

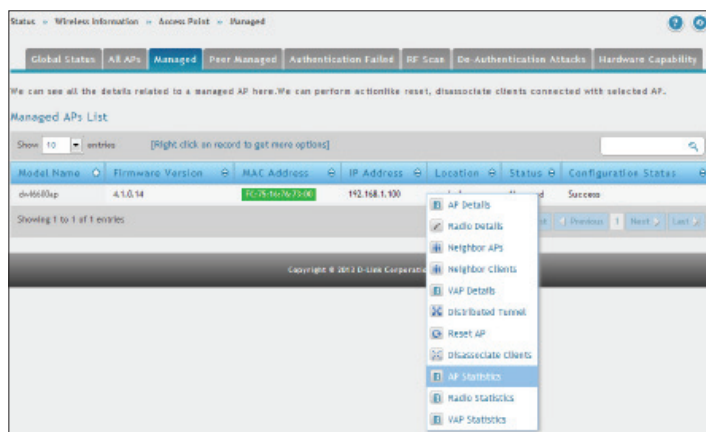
Managed

Path: Status > Wireless Information > Access Point > Managed

The Managed AP List page shows details about the managed access point. right clicking a managed access point enables more options.



| Field | Description |
|-------------------------------------|--|
| Model Name | The model of the managed AP. |
| Firmware Version | The firmware version of the managed AP. |
| MAC Address (*) Peer Managed | Ethernet address of the managed access point. If an asterisk (*) follows the MAC address, the access point is managed by a peer controller. |
| IP Address | Network IP address of the managed access point. |
| Location | An optional description of where the AP is physically located. Configured through the AP management section. |
| Status | <p>Current managed state of the access point. Possible values are:</p> <ul style="list-style-type: none"> Discovered = access point is discovered by the wireless controller, but not authenticated. Authenticated = access point has been validated and authenticated (if authentication is enabled), but it is not configured. Managed = profile configuration has been applied to the access point and the access point is operating in managed mode. Failed = wireless controller lost contact with the access point. A failed entry remains in the Managed AP database, unless you remove it. Note that a managed access point shows a failed status temporarily during a reset. <p>If management connectivity is lost for a managed access point, both of its radios are turned down and all clients associated with the access point are disassociated. The radios resume operation when that access point is managed again by a wireless controller.</p> |
| Configuration Status | Shows whether the configuration profile applied to the managed access point is successful or not. |



| Button | Description |
|----------------------|---|
| AP Details | Shows detailed status information collected from the access point. |
| Radio Details | Shows detailed status for a radio interface. |
| Neighbor APs | Shows the neighbor APs that the specified AP has discovered through periodic RF scans on the selected radio interface. |
| Neighbor Clients | Shows information about wireless clients associated with an access point or detected by the access point radio. |
| VAP Details | Shows summary information about the virtual access points (VAPs) for the selected access point and the access point radio interface that the wireless controller manages. |
| Distributed Tunnel | Shows information about the L2 tunnels currently in use on the access point. |
| Reset AP | Reset the managed AP back to the factory default settings. |
| Disassociate Clients | View disassociate clients with the selected AP. |

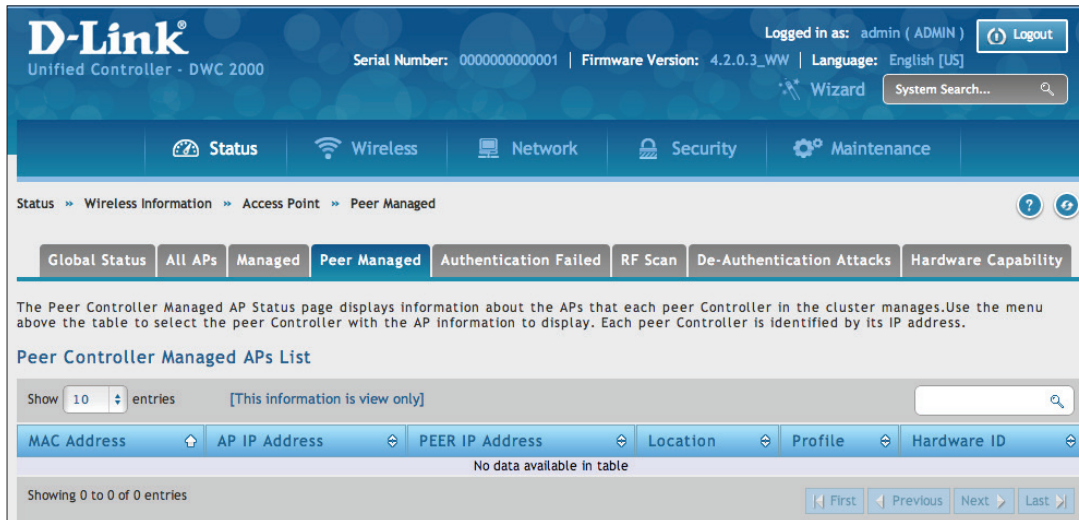
The Managed AP Statistics page shows information about traffic on the access point's wired and wireless interfaces. This information can help diagnose network issues, such as throughput problems. To view the statistics for a managed access point, right-click on its entry in the Managed AP List and select **AP Statistics**, **Radio Statistics**, and **VAP Statistics**.

| Button | Description |
|------------------|--|
| AP Statistics | Shows the number and type of packets transmitted and received on a specific access point. |
| Radio Statistics | Shows per-radio information about the number and type of packets transmitted and received for a specific access point. |
| VAP Statistics | Shows per-VAP information about the number of packets transmitted and received and the number of wireless client failures for a specific access point. |

Peer Managed

Path: Status > Wireless Information > Access Point > Peer Managed

The Peer Controller Managed APs List page provides information about the access points that each peer controller in the cluster manages. Each peer controller is identified by its IP address.

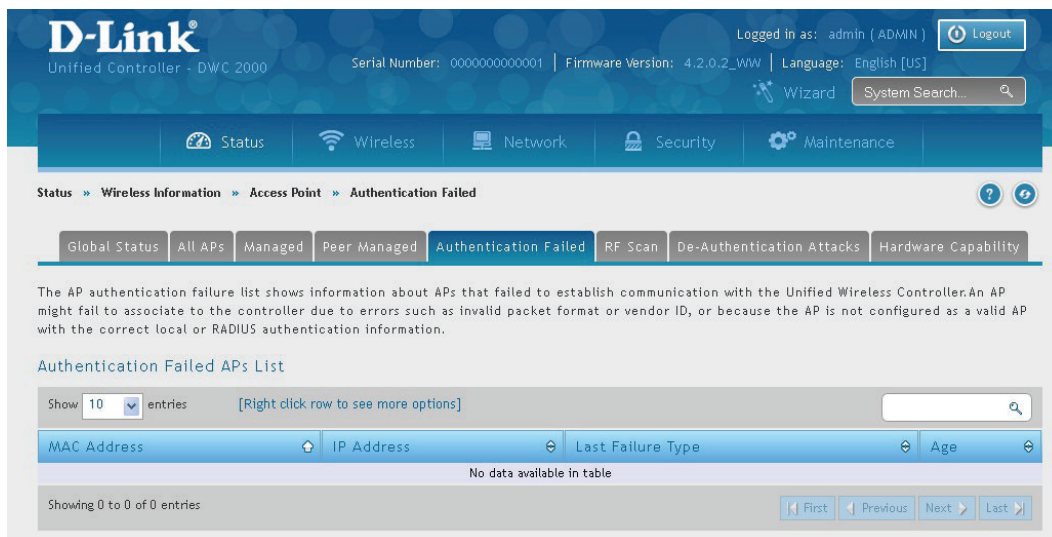


| Field | Description |
|-----------------|---|
| MAC Address | MAC address of each access point managed by the peer controller. |
| AP IP Address | IP address of the access point. |
| Peer IP Address | IP address of the peer controller that manages the access point. This field appears when All is selected from the drop-down menu. |
| Location | Descriptive location configured for the managed access point. |
| Profile | Access point profile that the wireless controller applies to the access point. |
| Hardware ID | Hardware ID associated with the access point hardware platform. |

Authentication Failed

Path: Status > Wireless Information > Access Point > Authentication Failed

An access point might fail to associate to the wireless controller due to errors such as invalid packet format or vendor ID, or because the access point is not configured as a valid access point with the correct local or RADIUS authentication information. The Authentication Failed APs List page shows information about access points that failed to establish communication with the wireless controller. Right-click on an AP to bring up options to manage, or to view details.



An access point can fail due to any of the reasons:

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

Fields on the AP Authentication Failure Status Page:

| Field | Description |
|-------------------|--|
| MAC Address | Ethernet address of the AP. If the MAC address of the access point is followed by an asterisk (*), it was reported by a peer controller. |
| IP Address | IP address of the access point. |
| Last Failure Type | Last type of failure that occurred. Possible values are: <ul style="list-style-type: none"> Local Authentication No Database Entry Not Managed RADIUS Authentication RADIUS Challenged RADIUS Unreachable Invalid RADIUS Response Invalid Profile ID Profile Mismatch-Hardware Type |
| Age | Time since failure occurred. |

RF Scan

Path: Status > Wireless Information > Access Point > RF Scan

The radio(s) on each access point can scan the radio frequency periodically to collect information about other access points and wireless clients that are within range. In normal operating mode, the access point always scans on the operational channel for the radio. The RF Scan page shows information about other access points and wireless clients that the wireless controller has detected. Right-click on an AP or client to bring up options to view details.

Status > Wireless Information > Access Point > RF Scan

Global Status All APs Managed Peer Managed Authentication Failed **RF Scan** De-Authentication Attacks Hardware Capability

Through AP RF Scan Status page, you can view information about all APs detected via RF scan, including those reported as Rogues. The radios on each AP can periodically scan the radio frequency to collect information about other APs and wireless clients that are within range. In normal operating mode the AP always scans on the operational channel for the radio.

RF Scan APs List

Show 10 entries [Right click on record to get more options]

| MAC Address | SSID | Physical Mode | Channel | Age | Status |
|-------------------|----------------|---------------|---------|-------------|---------|
| 08:05:50:55:87:00 | DAP-1658 | 802.11b/g | 2 | 0d:01:32:54 | Unknown |
| 08:00:43:76:17:06 | GO-RTW4000 | 802.11b/g | 6 | 0d:00:53:24 | Unknown |
| 08:17:9A:00:30:28 | D-Link | 802.11b/g | 1 | 0d:00:31:54 | Unknown |
| 08:17:9A:00:30:29 | D-Link_Guest | 802.11b/g | 1 | 0d:00:31:54 | Unknown |
| 08:17:9A:00:30:2A | D-Link | 802.11a | 56 | 0d:01:35:18 | Rogue |
| 08:17:9A:00:30:2B | D-Link | 802.11b/g | 11 | 0d:01:43:08 | Unknown |
| 08:17:9A:00:30:2C | D-Link_Guest | 802.11b/g | 11 | 0d:01:12:12 | Unknown |
| 08:18:87:70:68:06 | 07997-5 | 802.11a | 48 | 0d:00:10:20 | Unknown |
| 08:18:87:70:76:02 | DAP-1320-Hans | 802.11b/g | 11 | 0d:17:10:38 | Unknown |
| 08:18:87:70:77:03 | DAP-1320-Clare | 802.11b/g | 1 | 0d:02:14:16 | Unknown |

Showing 1 to 10 of 40 entries

First Previous 1 2 3 4 Next Last

| Field | Description |
|---------------|--|
| MAC Address | Ethernet MAC address of the detected access point. This could be a physical radio interface or VAP MAC. |
| SSID | The wireless name (Service Set Identifier) of the network, which is broadcast in the detected beacon frame. |
| Physical Mode | The 802.11 mode used on the access point. |
| Channel | Transmit channel of the access point. |
| Age | Time since this access point was last detected in an RF scan. Status entries for this page are collected at a point in time and eventually age out. The age value for each entry shows how long ago the wireless controller recorded the entry. |
| Status | Managed status of the access point. The valid values are: <ul style="list-style-type: none">• Managed = Neighbor access point is managed by the wireless system.• Standalone = Access point is managed in standalone mode and configured as a valid AP entry (local or RADIUS).• Rogue = Access point is classified as a threat by one of the threat detection algorithms.• Unknown = Access point is detected in the network but is not classified as a threat by the threat detection algorithms. |

De-Authentication Attacks

Path: Status > Wireless Information > Access Point > De-Authentication Attacks

The AP De-Authentication Attack page contains information about rogue APs that the Cluster Controller has attacked by using the de-authentication attack feature. The wireless controller can protect against rogue APs by sending de-authentication messages to the rogue AP. The de-authentication attack feature must be globally enabled in order for the wireless system to do this function. Make sure that no legitimate APs are classified as rogues before enabling the attack feature. This feature is disabled by default.

The wireless system can conduct the de-authentication attack against 16 APs at the same time. The intent of this attack is to serve as a temporary measure until the rogue AP is located and disabled.

The de-authentication attack is not effective for all rogue types, and therefore is not used on every detected rogue. The following rogues are not subjected to the attack:

- If the detected rogue is spoofing the BSSID of the valid managed AP then the wireless system does not attempt to use the attack because that attack may deny service to a legitimate AP and provide another avenue for a hacker to attack the system.
- The de-authentication attack is not effective against Ad hoc networks because these networks do not use authentication.
- The APs operating on channels outside of the country domain are not attacked because sending any traffic on illegal channels is against the law.

The wireless controller maintains a list of BSSIDs against which it is conducting a de-authentication attack. The controller sends the list of BSSIDs and channels on which the rogue APs are operating to every managed AP.

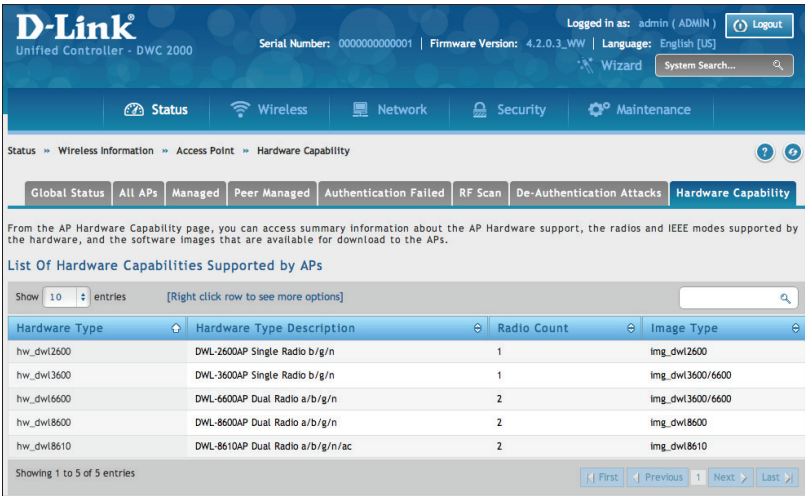


| Field | Description |
|---------------------------|---|
| BSSID | Shows the BSSID of the AP against which the attack is launched. The BSSID is a MAC address. |
| Channel | Identifies the channel on which the rogue AP is operating. |
| Time Since Attack Started | Shows the amount of time that has passed since the attack started on the AP. |
| RF Scan Report Age | Shows the amount of time that has passed since the RF Scan reported this AP. |

Hardware Capability

Path: Status > Wireless Information > Access Point > Hardware Capability

The wireless controller supports access points that have different hardware capabilities, such as number of radios, supported IEEE 802.11 modes, and software images. Using the AP Hardware Capability page, you view information about the radio hardware and IEEE modes supported by access points, as well as software images that are available for download to the access point.



| Field | Description |
|---------------------------|---|
| Hardware Type | Shows the ID number assigned to each access point hardware type. The wireless controller supports six different types of access point hardware. |
| Hardware Type Description | Describes the platform and the supported IEEE 802.11 modes. |
| Radio Count | Shows whether the hardware supports one radio or two radios. |
| Image Type | Shows the type of software the hardware requires. |

The right-click option will display the radio Information for the selected hardware type.

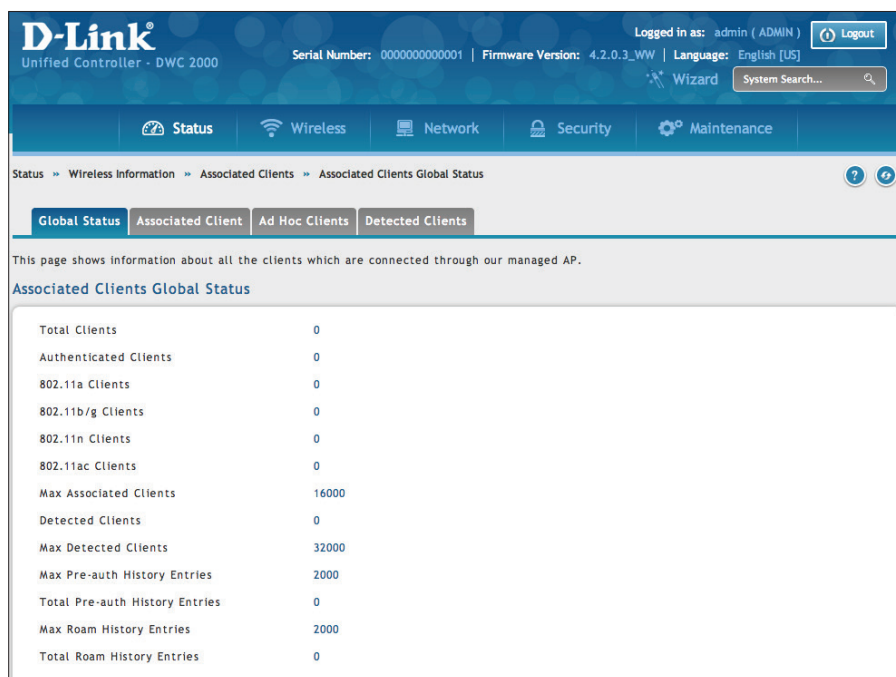


| Field | Description |
|---------------------------|---|
| Hardware Type Description | Shows the ID number assigned to each access point hardware type. The wireless controller supports six different types of access point hardware. |
| Radio Mode | Describes the platform and the supported IEEE 802.11 modes. |
| Radio Count | Shows whether the hardware supports one radio or two radios. |
| 802.11a Support | Shows whether support for IEEE 802.11a mode is enabled. |
| Radio Type Description | Displays the type of radio, which might contain information such as the manufacturer name and supported IEEE 802.11 modes. |
| 802.11bg Support | Shows whether support for IEEE 802.11bg mode is enabled. |
| VAP Count | Displays the number of VAPs the radio supports. |
| 802.11n Support | Shows whether support for IEEE 802.11n mode is enabled. |
| 802.11ac Support | Shows whether support for IEEE 802.11ac mode is enabled. |

Associated Clients Global Status

Path: Status > Wireless Information > Associated Clients > Global Status

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

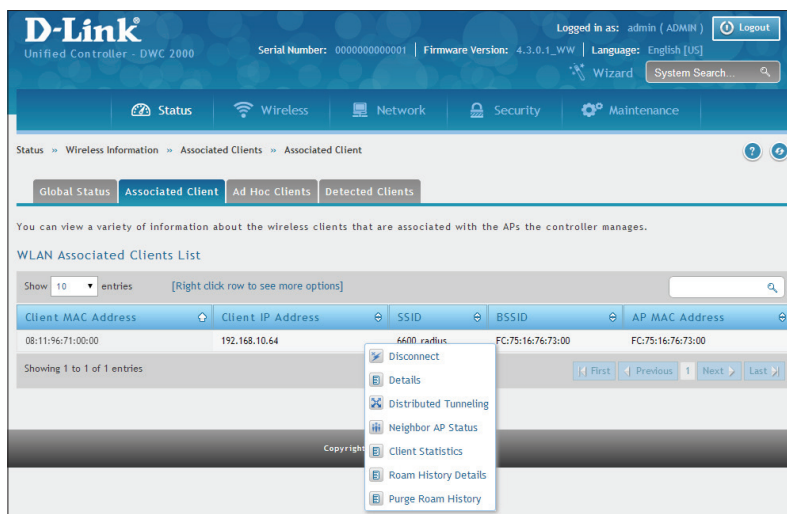


| Field | Description |
|---------------------------------------|---|
| Total Clients | Total number of clients in the database. This total includes clients with an Associated, Authenticated, or Disassociated status. |
| Authenticated Clients | Total number of clients in the associated client database with an Authenticated status. |
| 802.11a Clients | Total number of IEEE 802.11a-only clients that are authenticated. |
| 802.11b/g Clients | Total number of IEEE 802.11b/g-only clients that are authenticated. |
| 802.11n Clients | Total number of clients that are IEEE 802.11n capable and are authenticated. These include IEEE 802.11a/n, IEEE 802.11b/g/n, 5 GHz IEEE 802.11n, 2.4GHz IEEE 802.11n. |
| 802.11ac Clients | Total number of IEEE 802.11ac-only clients that are authenticated. |
| Max Associated Clients | Maximum number of clients that can associate with the wireless system. This is the maximum number of entries allowed in the Associated Client database. |
| Detected Clients | Number of wireless clients detected in the WLAN. |
| Max Detected Clients | Maximum number of clients that can be detected by the controller. The number is limited by the size of the Detected Client Database. |
| Max Pre-auth History Entries | Maximum number of Client Pre-Authentication events that can be recorded by the system. |
| Total Pre-auth History Entries | Current number of pre-authentication history entries in use by the system. |
| Maximum Roam History Entries | Maximum number of entries that can be recorded in the roam history for all detected clients. |
| Total Roam History Entries | Current number of pre-authentication history entries in use by the system. |

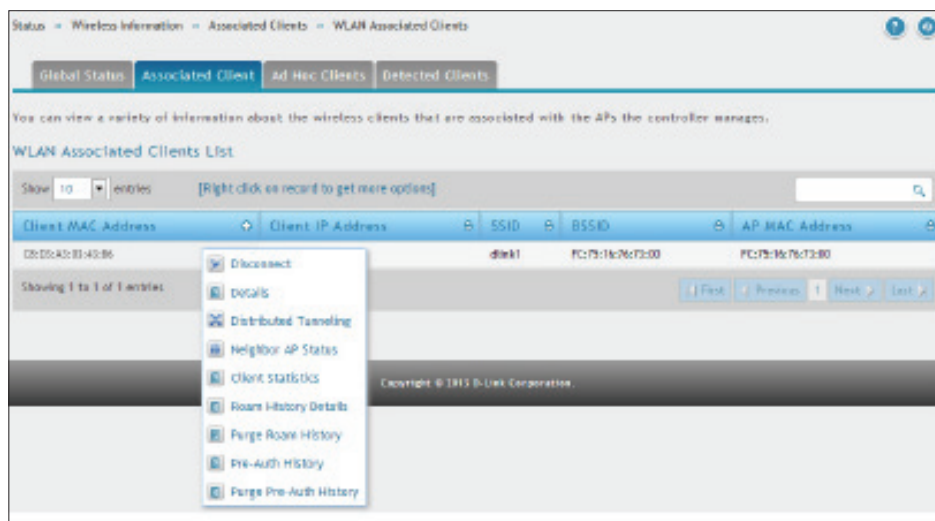
Associated Clients

Path: Status > Wireless Information > Associated Clients > Associated Clients

The WLAN Associated Clients page tracks the traffic associated with the client connected to the wireless controller. Right-clicking on a client and clicking the **View Details** button displays detailed information about the selected client.



| Field | Description |
|--------------------|--|
| Client MAC Address | Ethernet MAC address of the client station. |
| Client IP Address | The IP address of the client station. |
| SSID | Name of the wireless network on which the client is connected. |
| BSSID | MAC address for the managed access point/virtual access point where this client is associated. |
| AP MAC Address | Ethernet MAC address of the access point. |



| Field | Description |
|------------------------------|---|
| Disconnect | Disconnects the associated client. |
| Details | Shows detailed information about the associated client and the AP it is connected to. |
| Distributed Tunneling | Shows information about distributed tunneling status. |
| Neighbor AP Status | Shows information about the neighbor AP status. |
| Client Statistics | Shows detailed statistic information about the associated client and its bandwidth usage. |
| Roam History Details | Shows a history of the different APs the client has been connected to that are managed by the DWC-2000. |
| Purge Roam History | Will purge the roam history for the selected client. |

After right-clicking next to the MAC address, the Client Statistic page shows the fields in the table on the next page. This page shows information about the traffic a wireless client receives and transmits while it is associated with a single access point. Use the table to view details about an associated client. Each client is identified by its MAC address.



| | |
|--------------------------|-------------------|
| MAC Address | 08:11:96:71:00:00 |
| Packets Received | 134191 |
| Bytes Received | 12203681 |
| Packets Transmitted | 154447 |
| Bytes Transmitted | 245410278 |
| Packets Receive Dropped | 0 |
| Bytes Receive Dropped | 0 |
| Packets Transmit Dropped | 0 |
| Bytes Transmit Dropped | 0 |
| Fragments Received | 0 |
| Fragments Transmitted | 0 |
| Transmit Retries | 192 |
| Transmit Retries Failed | 26 |

| Field | Description |
|---------------------------------------|---|
| Packets Received | Total number of packets received from the client station. |
| Bytes Received | Total number of bytes received from the client station. |
| Packets Transmitted | Total number of packets transmitted to the client station. |
| Bytes Transmitted | Total number of bytes transmitted to the client station. |
| Packets Receive Dropped | Number of packets received from the client stations that were dropped. |
| Bytes Receive Dropped | Number of bytes received from the client stations that were dropped. |
| Packets Transmit Dropped | Number of packets transmitted to the client stations that were dropped. |
| Bytes Transmit Dropped | Number of bytes transmitted to the client stations that were dropped. |
| Fragments Received | Total number of fragmented packets received from the client station. |
| Fragments Transmitted | Total number of fragmented packets transmitted to the client station. |
| Transmit Retries | Number of times transmits to client station succeeded after one or more retries. |
| Transmit Retries Failed | Number of times transmits to client station failed after one or more retries. |
| TS Violate Packets Received | Count of packets received by an access point from a wireless client for the specified access category. |
| TS Violate Packets Transmitted | Count of packets transmitted by an access point to a wireless client for the specified access category. |
| Duplicates Received | Total number of duplicate packets received from the client station. |

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

The WLAN Associated Detected Clients Pre-Authentication History List page shows detected clients that have made pre-authentication requests and identifies the access points that received the requests.

Right-clicking next to the MAC address, the Pre-Auth History page shows the fields in the table on the next page.

| Pre-Authentication History | |
|----------------------------|-------------------|
| Client MAC Address | C8:E0:41:00:43:16 |
| AP MAC Address | Not Available |
| Radio Interface Number | Not Available |
| VAP BSSID address | Not Available |
| SSID | Not Available |
| Ext. Name | Not Available |
| Pre-auth Status | Unknown |
| Age | Not Available |

| Field | Description |
|--------------------------|--|
| MAC Address | MAC address of the client. |
| AP MAC Address | MAC address of the managed access point to which the client has pre-authenticated. |
| Radio Interface Number | Radio number to which the client is authenticated (Radio 1 or Radio 2). |
| VAP MAC Address | VAP MAC address to which the client roamed. |
| SSID | SSID name used by the VAP. |
| User Name | User name of client that authenticated via 802.1X. |
| Pre-Authorization Status | Indicates whether the client successfully authenticated. Shows a status of Success or Failure. |
| Age | Time since the history entry was added. |

The wireless system keeps a record of clients as they roam from one managed access point to another, and displays this information on the WLAN Associated Detected Clients Roam History List.

Right-clicking next to the MAC address, the Roam History page shows the fields in the table below.

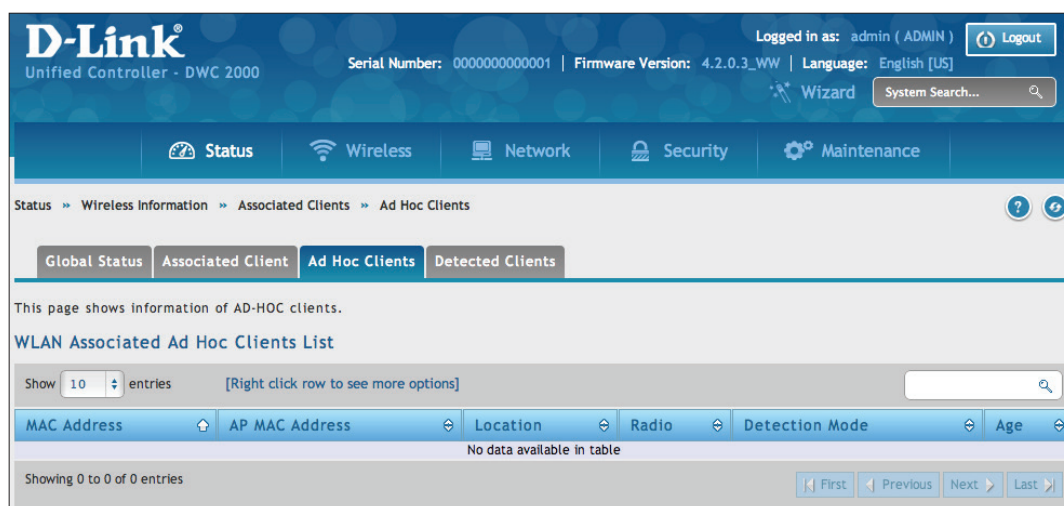
| List of Associated Clients Roam History | | | | | |
|---|-------|-------------------|-------------|--------|------------------|
| MAC Address | | 4C:21:00:4E:0E:EC | | | |
| AP MAC Address | Radio | VAP MAC Address | SSID | Status | Time Since Event |
| FC:75:16:77:0E:C0 | 1 | FC:75:16:77:0E:C0 | dwc2k_local | Roam | 0d:00:05:17 |

| Field | Description |
|------------------|--|
| AP MAC Address | MAC address of the managed access point to which the client has pre-authenticated. |
| Radio | Radio number to which the client is authenticated. |
| VAP MAC Address | VAP MAC address to which the client roamed. |
| SSID | SSID name used by the VAP. |
| Status | A flag indicating whether the history entry represents a new authentication or a roam event. |
| Time Since Event | Time since the history entry was added. |

Ad Hoc Clients

Path: Status > Wireless Information > Associated Clients > Ad Hoc Clients

An ad hoc client is a wireless client that gains access to the WLAN through a wireless client that is associated with an access point. The ad hoc client does not communicate directly with the AP. Ad hoc networks are a particular concern because they consume RF bandwidth and can present a security risk.



| Field | Description |
|----------------|---|
| MAC Address | The Ethernet address of the client. If the Detection Mode is Beacon then the client is represented as an AP in the RF Scan database and the Neighbor AP List. If the Detection Mode is Data Frame then the client information is in the Neighbor Client List. |
| AP MAC Address | The base Ethernet MAC Address of the managed AP which detected the client. |
| Location | The configured descriptive location for the managed AP. |
| Radio | The radio interface and its configured mode that detected the ad hoc device. |
| Detection Mode | The mechanism of detecting this Ad Hoc device. The possible values are Beacon Frame or Data Frame. |
| Age | Time since last detection of the ad hoc network. |

Right-click Commands on the WLAN Associated Ad Hoc Clients List

| Field | Description |
|------------|--|
| Delete All | Deletes all ad hoc client entries from the list. Clearing the list does not disassociate any of the ad hoc clients, and the clients might still be involved in the ad hoc network. |
| Deny | Blocks an ad hoc client from WLAN access. The MAC address is added to the Known Client database where the default action is Deny. |
| Allow | Allows an ad hoc client access to the WLAN. The MAC address is added to the Known Client database where the default action is Allow. |

Detected Clients

Path: Status > Wireless Information > Associated Clients > Detected Clients

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

| MAC Address | Client Name | Client Status | Age | Create Time |
|-------------------|-------------|---------------|-------------|-------------|
| 00:03:7F:00:01:C3 | | Detected | 0d 00:00:05 | 1d 05:10:39 |
| 00:05:5D:15:87:80 | | Detected | 0d 00:16:04 | 1d 03:25:13 |
| 00:05:5D:15:87:82 | | Detected | 0d 00:16:04 | 1d 03:25:13 |
| 00:06:66:20:45:89 | | Detected | 0d 15:28:17 | 1d 15:28:17 |
| 00:0C:E7:60:83:84 | | Detected | 0d 19:00:24 | 2d 00:35:35 |
| 00:12:2A:18:62:87 | | Detected | 0d 00:00:35 | 2d 00:21:02 |
| 00:12:40:E0:E3:51 | | Detected | 0d 19:25:58 | 1d 19:25:59 |
| 00:15:00:60:54:5C | | Detected | 0d 00:01:04 | 2d 00:25:36 |
| 00:15:00:60:58:54 | | Detected | 0d 00:01:05 | 2d 00:36:36 |
| 00:16:EA:C3:93:BA | | Detected | 0d 21:14:22 | 1d 21:14:22 |

Fields on the Detected Client Status Page are shown in the table below:

| Field | Description |
|---------------|---|
| MAC Address | Ethernet MAC address of the client. |
| Client Name | Name of the client, if available, from the Known Client Database. If the client is not in the database, the field is blank. |
| Client Status | Client status, which can be one of the following values: <ul style="list-style-type: none"> Authenticated = wireless client is authenticated with the wireless system. Detected = wireless client is detected by the wireless system, but is not a security threat. Black-Listed = client with this MAC address is specifically denied access via MAC authentication. Rogue = client is classified as a threat by one of the threat-detection algorithms. |
| Age | Time since any event has been received for this client that updated the detected client database entry. |
| Create Time | Time since this entry was first added to the detected client database. |

Right-click commands on the WLAN Detected Clients List are listed below:

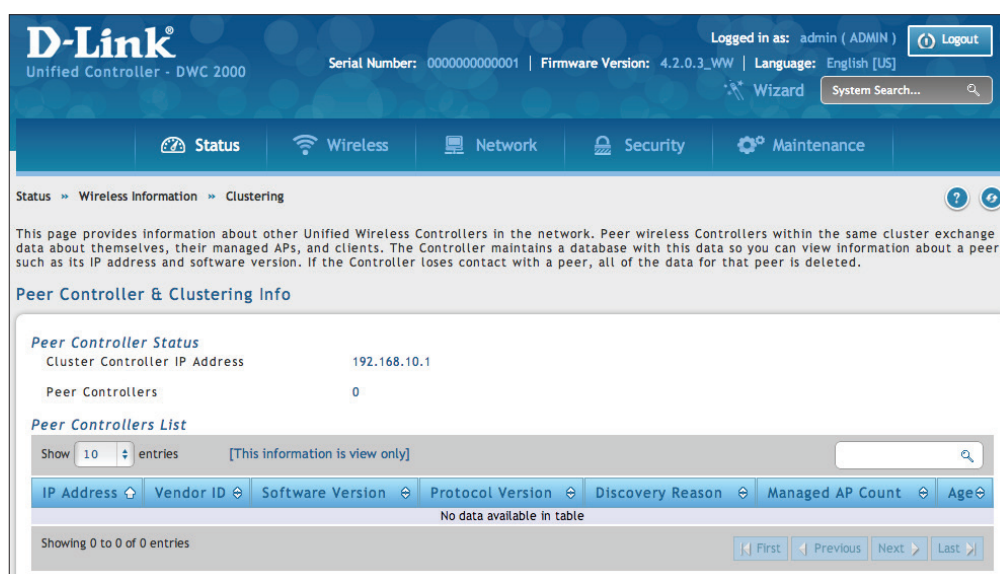
| Field | Description |
|------------------------|---|
| Details | Show detail information about the selected client. |
| Pre-Auth History | The Detected Client Pre-Authentication History page shows information about the pre-authentication requests that the detected client has made. |
| Roam History Details | A record of clients as they roam from one managed AP to another managed AP. A history of up to 10 APs is kept for each client. |
| Purge Roam History | Clears current roam history data from Roam History section. |
| Triangulation Detail | The Detected Client Triangulation page lists up to three non-sentry and three sentry managed APs that have detected the client. |
| Rogue Classification | The Wireless Intrusion Detection System (WIDS) can help detect intrusion attempts into the wireless network and take automatic actions to protect the network. The Unified Wireless controller allows you to activate or deactivate various threat detection tests and set threat detection thresholds. The WIDS Client Rogue Classification page provides information about the results of these tests. If a client has been classified as a rogue, this page provides information about which tests the client might have failed to trigger the classification. |
| Purge Pre-auth History | Clears pre auth data from Pre-Auth History section. |

Viewing Cluster Information

Path: Status > Wireless Information > Clustering

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

One wireless controller in a cluster is elected as a Cluster Controller. The Cluster Controller collects status and statistics from the other controllers in the cluster, including information about the access point's peer controller and the clients associated to those access points.



| Field | Description |
|--------------------------------------|---|
| Cluster Information | |
| Cluster Controller IP Address | IP address of the controller that controls the cluster. |
| Peer Controllers | Number of peer controllers. |
| Connected Peer Controllers | |
| IP Address | IP address of the peer wireless controller in the cluster. |
| Vendor ID | Vendor ID of the peer controller software. |
| Software Version | Software version for the given peer controllers. |
| Protocol Version | Protocol version supported by the software on the peer wireless controllers. |
| Discovery Reason | Discovery method of the given peer wireless controller, either through an L2 Poll or IP Poll. |
| Managed AP Count | Number of access points that the wireless controller manages currently. |
| Age | Time since last communication with the wireless controller, in hours, minutes, and seconds. |

Viewing WDS Group Status

Path: Status > Wireless Information > WDS Groups Status > WDS Groups Status

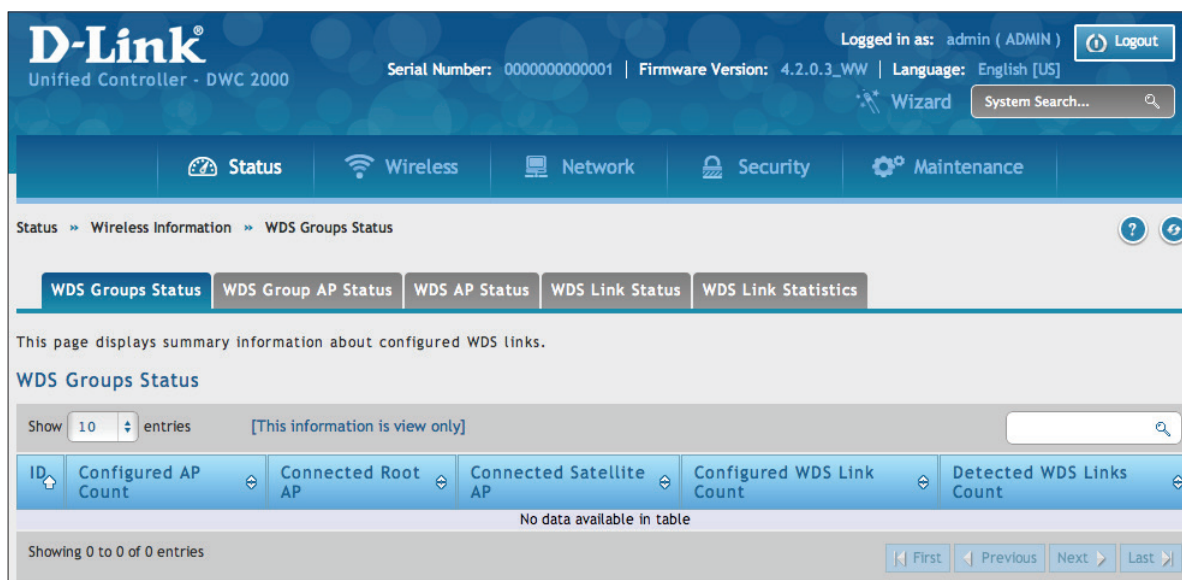
The Wireless Distribution System (WDS)-Managed AP feature allows you to add managed APs to the cluster using over-the-air WDS links through other managed APs. With WDS, APs may be located outdoors where wired connection to the data network is unavailable, or in remote buildings that are not connected to the main campus with a wired network.

The WDS AP group consists of the following managed APs:

- **Root AP:** Acts as a bridge or repeater on the wireless medium and communicates with the controller via the wired link
- **Satellite AP:** Communicates with the controller via a WDS link to the Root AP

The WDS links are secured using WPA2 Personal authentication and AES encryption.

This page displays summary information about configured WDS links. At least one group must be configured for the fields to display. To configure a WDS AP group, use the pages from Wireless > Access Point > WDS Groups.



| Field | Description |
|---------------------------|---|
| ID | Unique number that identifies the WDS AP group. |
| Configured AP Count | Number of APs configured in this WDS AP group. |
| Connected Root AP | Number of Root APs currently being managed by the controller that are members of this WDS AP Group. |
| Connected Satellite AP | Number of Satellite APs currently being managed by the controller that are members of this WDS AP Group. |
| Configured WDS Link Count | Number of configured bidirectional links in the WDS AP Group. |
| Detected WDS Links Count | Number of WDS links detected in the system. APs on both sides of the link must detect each other in order for the link to be counted. |

WDS Group AP Status

Path: Status > Wireless Information > WDS Groups Status > WDS Group AP Status

The WDS AP Group Status page displays detailed information about the configured APs and links in the WDS Group. From this page, you can also send a new password to group members.

D-Link
Unified Controller - DWC 2000

Serial Number: 0000000000001 | Firmware Version: 4.3.0.1_WW | Language: English [US]

Logged in as: admin (ADMIN) | Logout

Wizard | System Search

Status | Wireless | Network | Security | Maintenance

Status > Wireless Information > WDS Groups Status > WDS Group AP Status

WDS Groups Status | **WDS Group AP Status** | WDS AP Status | WDS Link Status | WDS Link Statistics

This page displays detailed information about the configured APs and links in the WDS Group.

WDS AP Status

| | |
|----------------------------------|------------------------------|
| ID | 1 |
| Configured AP Count | 0 |
| Connected AP Count | 0 |
| Source AP Count | 0 |
| Destination AP Count | 0 |
| Source Bridge AP MAC | 00:00:00:00:00:00 |
| Source Device Type | None |
| Config WDS Link Count | 0 |
| Detect WDS Link Count | 0 |
| Blocked WDS Link Count | 0 |
| WDS Group Password Change Status | Not Started |
| Edit Password | <input type="checkbox"/> OFF |

Save Cancel

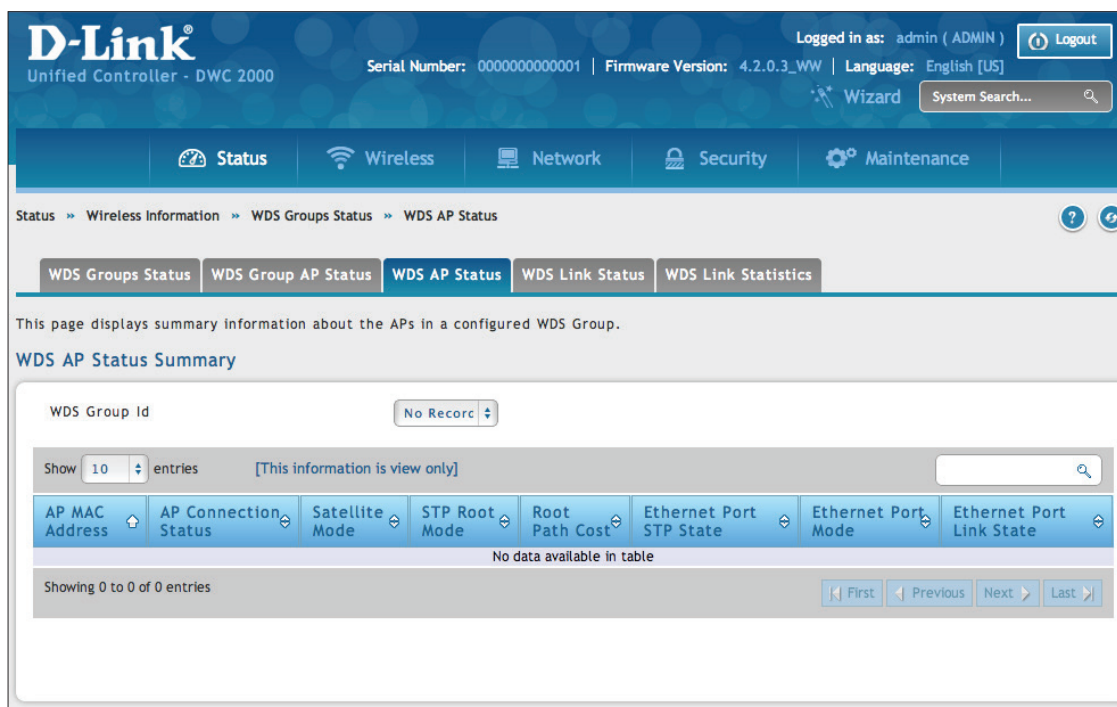
| Field | Description |
|-------------------------------|--|
| ID | Unique number that identifies the WDS AP group. |
| Configured AP Count | Number of APs configured in this WDS AP group. |
| Connected AP Count | Number of APs managed by the controller that are members of this WDS AP Group. This number is the sum of the Connected Root APs and Connected Satellite APs. |
| Source AP Count | Number of Root APs currently being managed by the controller that are members of this WDS AP Group. |
| Destination AP Count | Number of Satellite APs currently being managed by the controller that are members of this WDS AP Group. |
| Source Bridge AP MAC | MAC Address of the device elected as the Spanning Tree Root Bridge. If spanning tree is disabled this value is 00:00:00:00:00:00. |
| Source Device Type | The type of device elected as the Spanning Tree Root bridge: <ul style="list-style-type: none"> • None (STP is disabled) • Root AP • Satellite AP • External Device (STP Root is not one of the APs) |
| Config WDS Link Count | Number of configured bidirectional links in the WDS AP Group. |
| Detect WDS Links Count | Number of WDS links detected in the system. APs on both sides of the link must detect each other in order for the link to be counted. |

| | |
|---|--|
| Blocked WDS Link Count | Number of WDS links blocked by the spanning tree protocol. If the AP on one side of the link reports the link as blocking then the link is counted by this status parameter. |
| WDS Group Password Change Status | Status of the last attempt to configure the password for the WDS Group: <ul style="list-style-type: none"> • Not Started • Success • Invalid Password • Requested • Timed Out |
| Edit Password | To change the password for all controllers and APs in this WDS Group, select the Edit checkbox, type the new password, and then click Apply Password. Password must be minimum of 8 characters and can be up to 63 characters in length. |

Viewing WDS AP Status

Path: Status > Wireless Information > WDS Groups Status > WDS AP Status

The WDS AP Group Status page displays summary information about the APs in a configured WDS group.

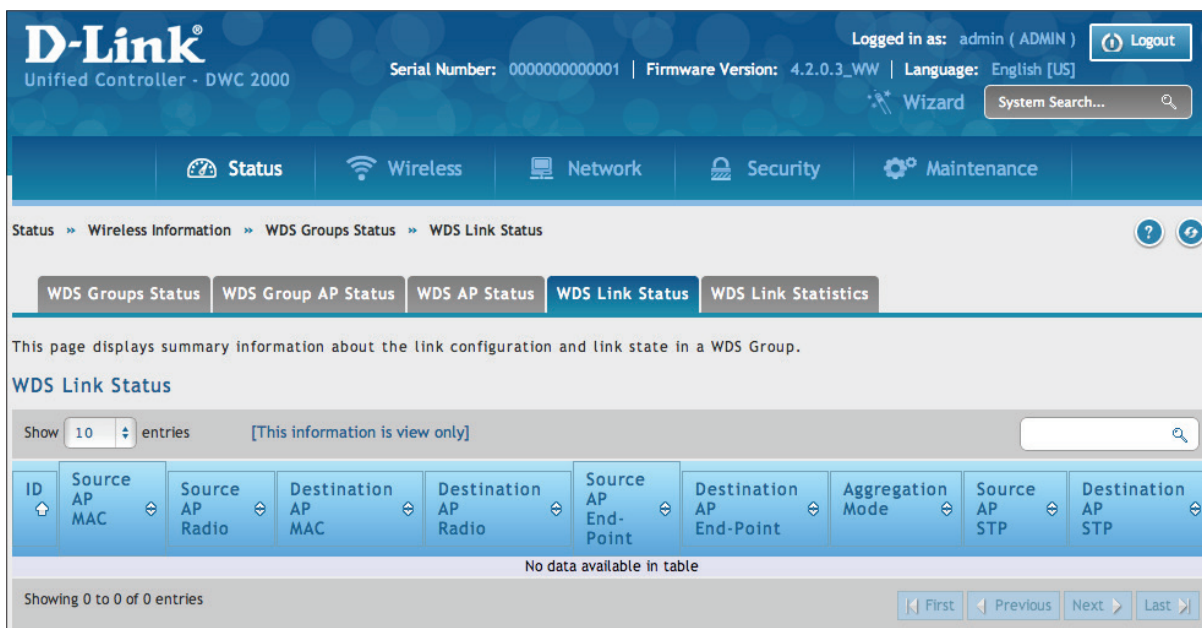


| Field | Description |
|--------------------------|--|
| Group ID | Use the drop-down menu above the fields to select the group number that identifies the configured WDS AP group. |
| AP MAC Address | Identifies the AP in the group by its MAC address. |
| AP Connection Status | Indicates whether the AP is currently being managed by one of the controllers in the cluster. |
| Satellite Mode | Indicates whether the AP is a Satellite AP connected to the network via a WDS link or a Root AP connected to the network via a wired link. |
| STP Root Mode | Indicates whether this AP is the root of the spanning tree. If spanning tree is disabled then the AP is always reported as Not STP Root. |
| Root Path Cost | Spanning Tree Path Cost to the root. The root AP always reports this value as 0. If spanning tree is disabled the value is also 0. |
| Ethernet Port STP State | When spanning tree is enabled on the APs in the WDS group this status parameter reports the spanning tree status of the Ethernet port. |
| Ethernet Port Mode | On Satellite APs the Ethernet port can be manually disabled. On root APs the port is always enabled. |
| Ethernet Port Link State | When the Ethernet port is enabled, this status reports the link state of the port. |

Viewing WDS Link Status

Path: Status > Wireless Information > WDS Groups Status> WDS Link Status

The WDS AP Link Status page displays summary information about the link configuration and link state in a WDS group.

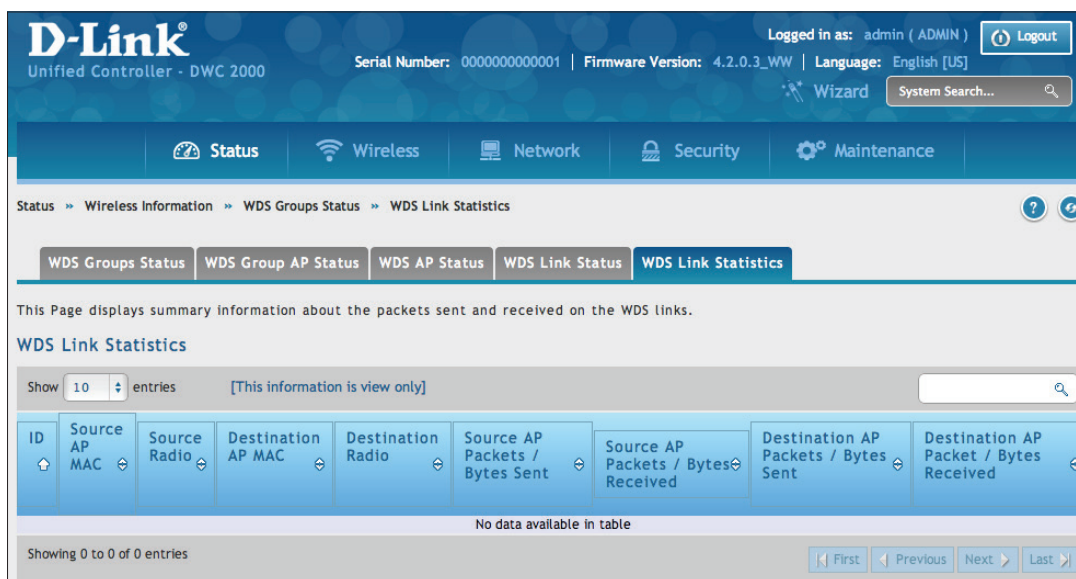


| Field | Description |
|---------------------------------|--|
| ID | The group number that identifies the configured WDS AP group. |
| Source AP MAC | The MAC address of one end-point of the WDS link. |
| Source AP Radio | The radio number of the WDS link endpoint on the source AP. |
| Destination AP MAC | The MAC address of the Source AP in the group. |
| Destination AP Radio | The radio number of the WDS link endpoint on the destination AP. |
| Source AP End-Point | Indicates whether the AP specified by the destination MAC detected the AP specified by the source MAC. |
| Destination AP End-Point | Indicates whether the AP specified by the source MAC detected the AP specified by the destination MAC. |
| Aggregation Mode | When parallel links are defined between two APs, this field indicates whether this link is part of the aggregation link pair. |
| Source AP STP | Spanning Tree State of the link on the source AP, which is one of the following: <ul style="list-style-type: none"> • Disabled (STP is disable or Link is down) • Forwarding • Learning • Listening • Blocking |
| Destination AP STP | Spanning Tree State of the link on the destination AP, which is one of the following: <ul style="list-style-type: none"> • Disabled (STP is disable or Link is down) • Forwarding • Learning • Listening • Blocking |

Viewing WDS Link Statistics

Path: Status > Wireless Information > WDS Groups Status > WDS Link Statistics

The WDS Group Link Statistics page displays summary information about the packets sent and received on the WDS links.



| Field | Description |
|---------------------------------------|--|
| ID | The group number that identifies the configured WDS AP group. |
| Source AP MAC | The MAC address of one end-point of the WDS link. |
| Source AP Radio | The radio number of the WDS link endpoint on the source AP. |
| Destination AP MAC | The MAC address of the Source AP in the group. |
| Destination AP Radio | The radio number of the WDS link endpoint on the destination AP. |
| Source AP End-Point | Indicates whether the AP specified by the destination MAC detected the AP specified by the source MAC. |
| Destination AP End-Point | Indicates whether the AP specified by the source MAC detected the AP specified by the destination MAC. |
| Source AP Packets/ Bytes Sent | Number of packets/bytes sent by the source AP. |
| Source AP Packets/Bytes Received | Number of packets/bytes received by the source AP. |
| Destination AP Packets/Bytes Sent | Number of packets/bytes sent by the destination AP. |
| Destination AP Packets/Bytes Received | Number of packets/bytes received by the destination AP. |

Maintenance

This chapter describes the following maintenance activities:

- "System Settings" on page 239
- "Activating Licenses" on page 241
- "Remote Management" on page 242
- "Using SNMP" on page 243
- "Backup Configuration Settings" on page 249
- "Restoring Configuration Settings" on page 250
- "Restoring Factory Default Settings" on page 251
- "Rebooting the Wireless Controller" on page 252
- "Wireless Controller Firmware Upgrade" on page 253
- "Using the Command Line Interface" on page 255
- "Log Settings" on page 265

System Settings

Set System Name

Path: Maintenance > Administration > System Setting

Enter a name for the system and click **Save**.

The screenshot shows the D-Link Unified Controller - DWC 2000 web interface. The top navigation bar includes 'Status', 'Wireless', 'Network', 'Security', and 'Maintenance'. The 'Maintenance' menu is expanded, showing 'Administration' > 'System Setting'. The page title is 'System Setting'. Below the title, it says 'This page allows user to set the controller identification name.' The 'System Setting' section contains a form with a label 'New Name for System' and a text input field containing 'DWC-2000'. There are 'Save' and 'Cancel' buttons below the input field.

Set System Date and Time

Path: Maintenance > Administration > Date and Time

You can configure your time zone, whether or not to adjust for Daylight Savings Time, and with which Network Time Protocol (NTP) server to synchronize the date and time. You can choose to set Date and Time manually, which will store the information on the controller's real time clock (RTC). If the controller has access to the internet, the most accurate mechanism to set the controller time is to enable NTP server communication.

To configure the date and time, following below steps:

1. Select the controller's time zone, relative to Greenwich Mean Time (GMT).
2. If supported for your region, click to Enable Daylight Savings.
3. Determine whether to use default or custom Network Time Protocol (NTP) servers. If custom, enter the server addresses or FQDN.

The screenshot shows the D-Link Unified Controller - DWC 2000 web interface. The top navigation bar includes 'Status', 'Wireless', 'Network', 'Security', and 'Maintenance'. The 'Maintenance' menu is expanded, showing 'Administration' > 'Date and Time'. The page title is 'Date and Time'. Below the title, it says 'This page allows us to set the date, time and NTP servers. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock time in a network of computers. Accurate time across a network is important for many reasons.' The 'Date and Time' section contains a form with the following fields: 'Current Device Time' (Sat Jan 01 02:44:20 AM GMT 2000), 'Time Zone' (GMT Greenwich Mean Time), 'Daylight Saving' (OFF), 'NTP Servers' (ON), 'NTP Server Type' (Default selected, Custom unselected), and 'Time to re-synchronize' (120 minutes). There are 'Save' and 'Cancel' buttons at the bottom.

Set Login Session Timeout

Path: Maintenance > Administration > Session Settings

Enter the session timeout value for administrator and guest users and then click **Save**.

D-Link® Unified Controller - DWC 2000

Serial Number: 00000000000001 | Firmware Version: 4.2.0.3_WW | Language: English [US]

Logged in as: admin (ADMIN) Logout

Wizard System Search...

Status Wireless Network Security Maintenance

Maintenance » Administration » Session Settings

The table lists all the available session Settings in the system.

Session Settings

| | | |
|---------------|----|---------------------------------------|
| Administrator | 10 | [Default: 10, Range: 0 - 999] Minutes |
| Guest | 10 | [Default: 10, Range: 0 - 999] Minutes |

Save Cancel

Set USB Share Ports

Path: Maintenance > Administration > USB Share Ports

Enable USB port sharing on USB port 1, 2, or both and click **Save**.

D-Link® Unified Controller - DWC 2000

Serial Number: 00000000000001 | Firmware Version: 4.2.0.3_WW | Language: English [US]

Logged in as: admin (ADMIN) Logout

Wizard System Search...

Status Wireless Network Security Maintenance

Maintenance » Administration » USB Share Ports

Connect Atleast one Printer to Configure USB Share Ports

This page allows the user to configure the SharePort feature available in the device.

USB Share Ports

USB Share Port Setup

| | |
|--------------------|-----|
| USB Port 1 Printer | OFF |
| USB Port 2 Printer | OFF |

Shared Enabled Interfaces List

| Interface Name | Enable Printer |
|----------------|----------------|
| default | OFF |

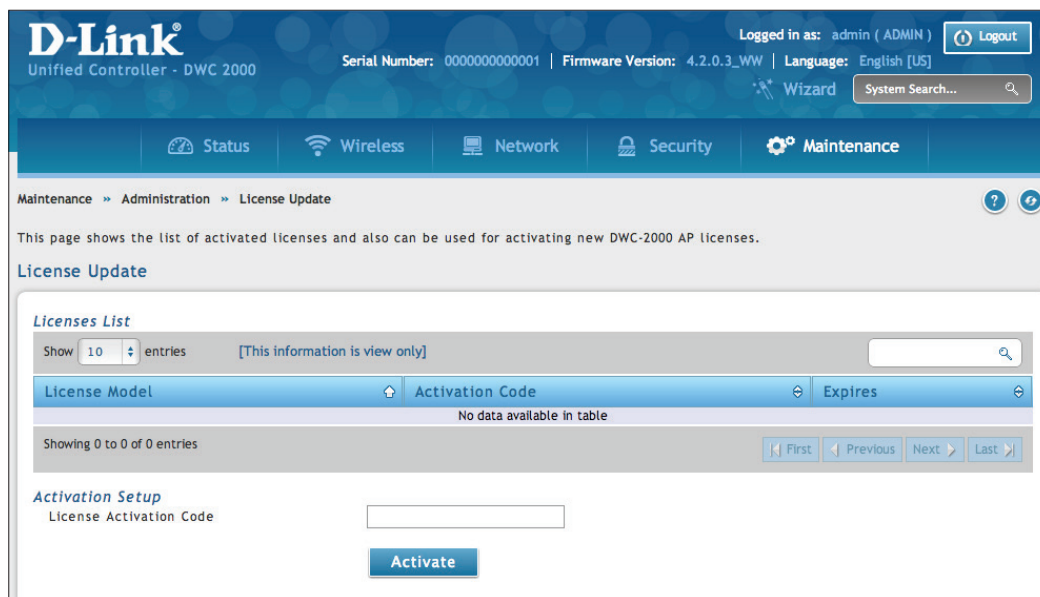
Save Cancel

Activating Licenses

Path: Maintenance > Administration > License Update

The License Update page lets you activate licenses for additional access points on the wireless controller.

1. Obtain an Activation Key from D-Link:
 - a. Find the wireless controller serial number on the bottom of the device.
 - b. Obtain a license key from D-Link after purchasing the license.
 - c. Open a web browser and go to <https://register.dlink.com> to register with D-Link.
 - d. If you do not have an account, register for a new account.
 - e. Log in with your username and password.
 - f. Click **License Key Activation** on the D-Link Global Registration Portal website.
 - g. Follow the directions to receive an activation code.
2. After obtaining the Activation Key, go to **Maintenance > Administration > License Update**. The License Update page will appear.



3. Under *Activation Setup*, enter the D-Link-supplied code for the license you want to activate in the Activation Code field.
4. Click **Activate**. The activation code will appear under List of Available Licenses.
5. Reboot the wireless controller to have the license take effect (refer to "Rebooting the Wireless Controller" on page 252).

Remote Management

Path: Maintenance > Administration > Remote Management

The Remote Access page allows you to enable remote management from outside your local network to configure your wireless controller. Select HTTP and/or HTTPS.

Note: When remote management is enabled, the controller is accessible to anyone who knows its IP address. It is HIGHLY RECOMMENDED that you change the default administrator and guest passwords before continuing.

1. Go to **Maintenance > Management > Remote Management**.

The screenshot shows the D-Link Unified Controller - DWC 2000 web interface. The top navigation bar includes 'Status', 'Wireless', 'Network', 'Security', and 'Maintenance'. The 'Maintenance' menu is expanded, showing 'Remote Management'. The 'Remote Management Setup' section has the following fields:

| Field | Value |
|---------------|-------------------------|
| HTTP | ON |
| HTTPS | ON |
| HTTPS Port No | 4443 [Range: 1 - 65535] |

Buttons: Save, Cancel

2. Set HTTP and/or HTTPS to **On**. If you select HTTPS, you may enter a port (4443 is the default setting).
3. Click **Save**.

Using SNMP

Path: Maintenance > Management > SNMP

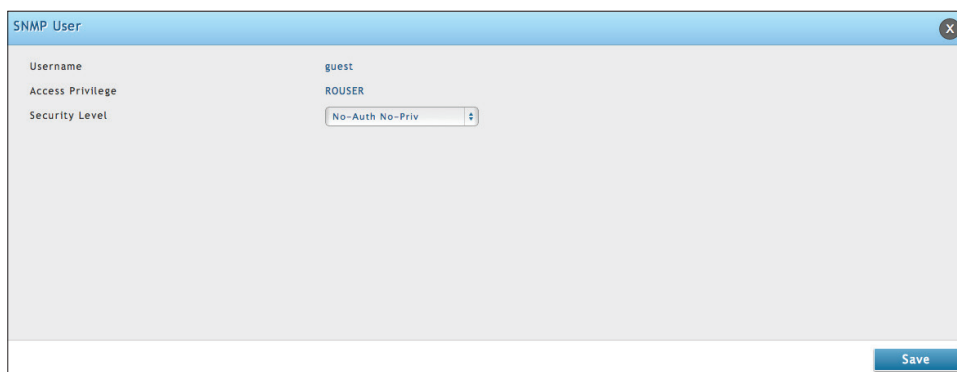
SNMP is an additional management tool that is useful when multiple routers in a network are being managed by a central Master system. When an external SNMP manager is provided with this controller's Management Information Base (MIB) file, the manager can update the controller's hierarchical variables to view or update configuration parameters. The controller as a managed device has an SNMP agent that allows the MIB configuration variables to be accessed by the Master (the SNMP manager). The Access Control List on the controller identifies managers in the network that have read-only or read-write SNMP credentials. The Traps List outlines the port over which notifications from this controller are provided to the SNMP community (managers) and also the SNMP version (v1, v2c, v3) for the trap.

Configure SNMP v3 User List

Go to **Maintenance > Management > SNMP > SNMP** tab.



1. Right-click either admin or guest and select **Edit**.

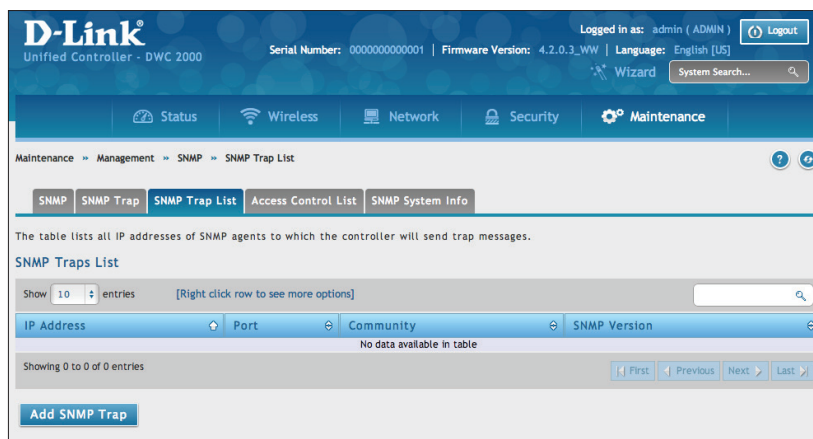


2. Set the security level.

- noAuthnoPriv: only requires a username match for authentication
- authNoPriv: Provides authentication based on the MD5 or SHA algorithms.
- authPriv: Provides authentication based on the MD5 or SHA algorithms as well as encryption privacy with the DES 256-bit standard.

3. Click **Save**.

Configure SNMP Trap List

1. Go to **Maintenance > Management > SNMP > SNMP Trap List** tab.2. Click **Add SNMP Trap**.

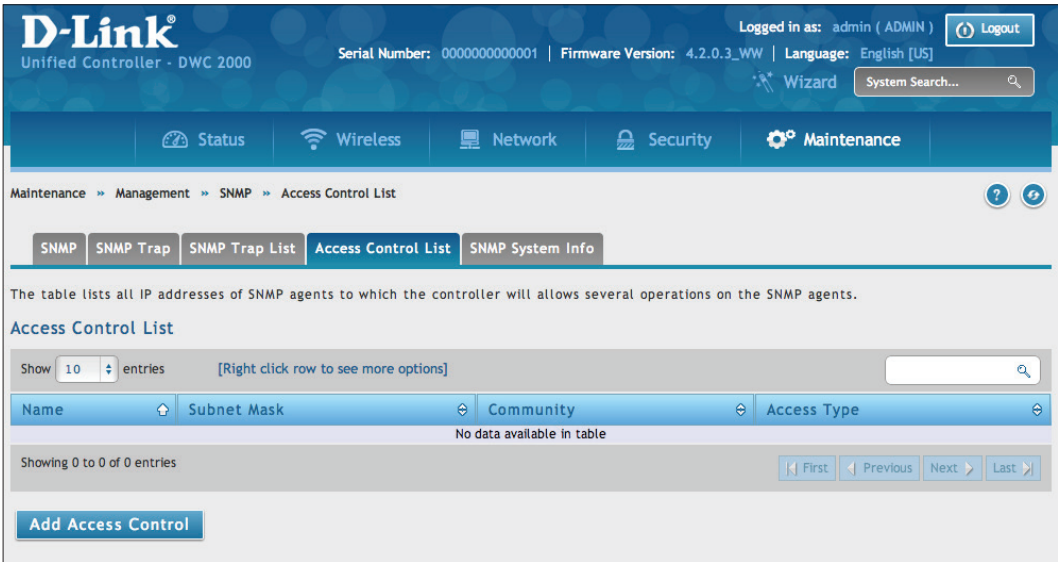
3. Complete the information on fields (refer to the table below).

4. Click **Save**.

| Field | Description |
|---------------------|--|
| IP Address | The IP Address of the SNMP trap agent. |
| Port | The SNMP trap port of the IP address to which the trap messages will be sent. |
| Community | The community string to which the agent belongs. Most agents are configured to listen for traps in the Public community. |
| Authentication Type | The SNMP version used by the trap agent. The choices are v1, v2c, or v3. |

Configure SNMP Access Control List

1. Go to **Maintenance > Management > SNMP > Access Control List** tab.



2. Click **Add Access Control**.

The screenshot shows a modal dialog box titled 'Access Control List'. It contains four input fields: 'IP Address', 'Subnet Mask', and 'Community'. Below these is the 'Access Type' section with two radio buttons: 'rocommunity' (which is selected) and 'rwcommunity'. A 'Save' button is located at the bottom right of the dialog box.

3. Complete the information on fields (refer to the table below).
4. Click **Save**.

| Field | Description |
|-------------|--|
| IP Address | The IP Address of the SNMP trap agent. |
| Subnet Mask | The network mask used to determine the list of allowed SNMP managers. |
| Community | The community string to which the agent belongs. |
| Access Type | Access will be either read only (ROcommunity) or read-write (RWcommunity). |

Configure SNMP System Info

1. Go to **Maintenance > Management > SNMP > SNMP System Info** tab.

The screenshot shows the D-Link Unified Controller - DWC 2000 web interface. The top navigation bar includes links for Status, Wireless, Network, Security, and Maintenance. The Maintenance tab is selected, and the breadcrumb trail is Maintenance > Management > SNMP > SNMP System Info. The page title is "SNMP System Info". Below the title, there is a description: "This page displays the current SNMP configuration of the controller. The following MIB (Management Information Base) fields are displayed and can be modified here." The configuration fields are: SysContact (empty), SysLocation (empty), and SysName (DWC-2000). There are Save and Cancel buttons at the bottom.

2. Enter the information as desired.
 - SysContact: The name of the contact person for this controller. Examples: admin, John Doe.
 - SysLocation: The physical location of the controller: Example: Rack #2, 4th Floor.
 - SysName: A name given for easy identification of the controller.
3. Click **Save**.

Configure Wireless SNMP Info

If you use Simple Network Management Protocol (SNMP) to manage the controller, you can configure the SNMP agent on the controller to send traps to the SNMP manager on your network from this page.

When an AP is managed by a controller, it does not send out any traps. The controller generates all SNMP traps based on its own events and the events it learns about through updates from the APs it manages.

All Wireless SNMP traps are disabled by default.

1. Go to **Maintenance > Management > SNMP > SNMP Trap** tab.

D-Link
Unified Controller - DWC 2000

Serial Number: 0000000000001 | Firmware Version: 4.2.0.3_WW | Language: English [US]

Logged in as: admin (ADMIN) | Logout

Wizard | System Search...

Status | Wireless | Network | Security | Maintenance

Maintenance » Management » SNMP » SNMP Trap

SNMP | **SNMP Trap** | SNMP Trap List | Access Control List | SNMP System Info

If you use Simple Network Management Protocol (SNMP) to manage the Unified Wireless Controller, you can configure the SNMP agent on the Controller to send traps to the SNMP manager on your network.

SNMP Trap

| | |
|---------------------------|------------------------------|
| AP Failure Traps | <input type="checkbox"/> OFF |
| AP State Change Traps | <input type="checkbox"/> OFF |
| Client Failure Traps | <input type="checkbox"/> OFF |
| Client State Change Traps | <input type="checkbox"/> OFF |
| Peer Controller Traps | <input type="checkbox"/> OFF |
| RF Scan Traps | <input type="checkbox"/> OFF |
| Rogue AP Traps | <input type="checkbox"/> OFF |
| WIDS Status Traps | <input type="checkbox"/> OFF |
| Wireless Status Traps | <input type="checkbox"/> OFF |

Save Cancel

2. Enable the trap as desired (refer to the table below).
3. Click **Save**.

| Field | Description |
|----------------------------------|--|
| AP Failure Traps | If you enable this field, the SNMP agent sends a trap if an AP fails to associate or authenticate with the controller |
| AP State Change Traps | If you enable this field, the SNMP agent sends a trap for one of the following reasons: <ul style="list-style-type: none"> Managed AP Discovered Managed AP Failed Managed AP Unknown Protocol Discovered Managed AP Load Balancing Utilization Exceeded |
| Client Failure Traps | If you enable this field, the SNMP agent sends a trap if a wireless client fails to associate or authenticate with an AP that is managed by the controller. |
| Client State Change Traps | If you enable this field, the SNMP agent sends a trap for one of the following reasons associated with the wireless client: <ul style="list-style-type: none"> Client Association Detected Client Disassociation Detected Client Roam Detected |
| Peer Controller Traps | If you enable this field, the SNMP agent sends a trap for one of the following reasons associated with a peer controller <ul style="list-style-type: none"> Peer Controller Discovered Peer Controller Failed Peer Controller Unknown Protocol Discovered Configuration command received from peer controller. (The controller does not need to be Cluster Controller for generating this trap.) |
| RF Scan Traps | If you enable this field, the SNMP agent sends a trap when the RF scan detects a new AP, wireless client, or ad-hoc client. |
| Rogue AP Traps | If you enable this field, the SNMP agent sends a trap when the controller discovers a rogue AP. The agent also sends a trap every Rogue Detected Trap Interval seconds if any rogue AP continues to be present in the network. |

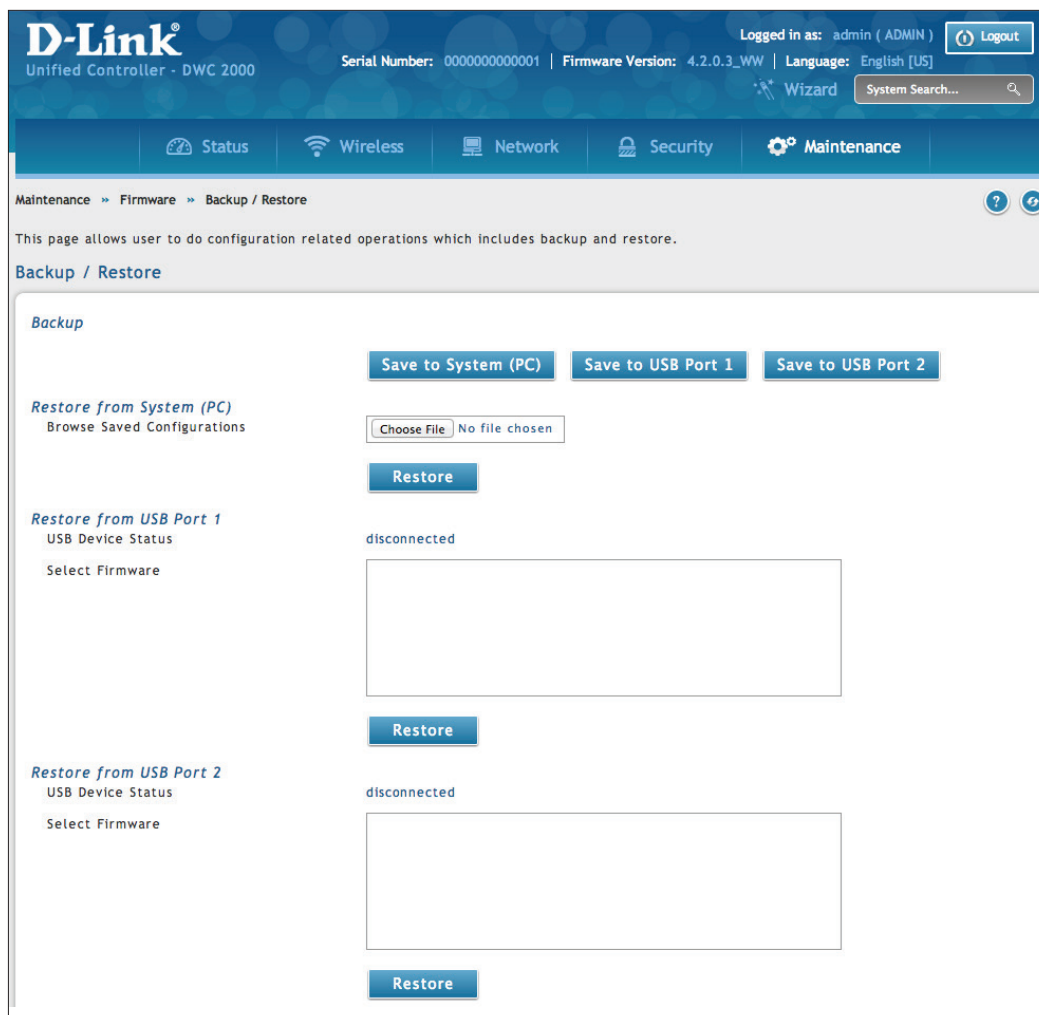
| Field | Description |
|------------------------------|--|
| TSPEC Traps | <p>If you enable this field, the SNMP agent sends a trap when the following TSPEC-related events occur:</p> <ul style="list-style-type: none">• An authorized WMM client is repeatedly using more bandwidth than was allocated for its traffic stream.• A WMM-enabled client is sending prioritized traffic without authorization to use admission controlled resources. |
| WIDS Status Traps | <p>If you enable this field, the SNMP agent sends a trap for one of the following reasons:</p> <ul style="list-style-type: none">• This controller has become Cluster Controller• Rogue Client detected• Rogue Client(s) continue to exist, after every Rogue Detected Trap Interval seconds• Maximum number of Managed APs in the peer group exceeded. |
| Wireless Status Traps | <p>If you enable this field, the SNMP agent sends a trap if the operational status of the controller (it need not be Cluster Controller for this trap) changes. It sends a trap if the Channel Algorithm is complete or the Power Algorithm is complete. It also sends a trap if any of the following databases or lists has reached the maximum number of entries:</p> <ul style="list-style-type: none">• Managed AP database• AP Neighbor List• Client Neighbor List• AP Authentication Failure List• RF Scan AP List• Client Association Database• Ad Hoc Clients List• Detected Clients List |

Backup Configuration Settings

Path: Maintenance > Firmware > Backup/Restore

After you configure the wireless controller as desired, back up the configuration settings. When you back up the settings, they are saved as a file. You can then use the file to restore the settings on the same wireless controller if something goes wrong or on a different wireless controller that will replace or work with other wireless controllers.

1. Click **Maintenance > Firmware > Backup/Restore**.



2. Click **Save from System (PC)**, **Save from USB Port 1**, or **Save from USB Port 2**, depending on the location the backup should be saved to.
 - A. If Save from System (PC) is chosen, a dialog box message will appear. Afterwards the browser will automatically begin the download to the default download location.
 - B. If Save from USB Port 1, or Save from USB Port 2 is chosen, the file will immediately be backed up to the corresponding USB flash drive without further prompts. If no USB flash medium is present, these options will do nothing.

Restoring Configuration Settings

Path: Maintenance > Firmware > Backup/Restore

After you use the procedure on the previous page to back up a wireless controller's configuration settings, you can restore the settings using the following procedure.

1. Click **Maintenance > Firmware > Backup/Restore**.

The screenshot shows the D-Link Unified Controller - DWC 2000 web interface. The top navigation bar includes links for Status, Wireless, Network, Security, and Maintenance. The Maintenance section is expanded, showing Firmware > Backup / Restore. The page title is 'Backup / Restore'. The main content area is divided into three sections: 'Backup', 'Restore from System (PC)', and 'Restore from USB Port 1' and 'Restore from USB Port 2'. The 'Backup' section has three buttons: 'Save to System (PC)', 'Save to USB Port 1', and 'Save to USB Port 2'. The 'Restore from System (PC)' section has a 'Choose File' button and a 'Restore' button. The 'Restore from USB Port 1' section shows a 'disconnected' status and a 'Restore' button. The 'Restore from USB Port 2' section also shows a 'disconnected' status and a 'Restore' button.

2. In the Restore to System (PC) section, click the **Choose File** button. Use the *Choose file* dialog box to find the backup file, then click the file and click **Open**.
3. Click **Restore**. A message will appear.
4. Click **OK** to close the message and restore the configuration settings from the selected file.

Restoring Factory Default Settings

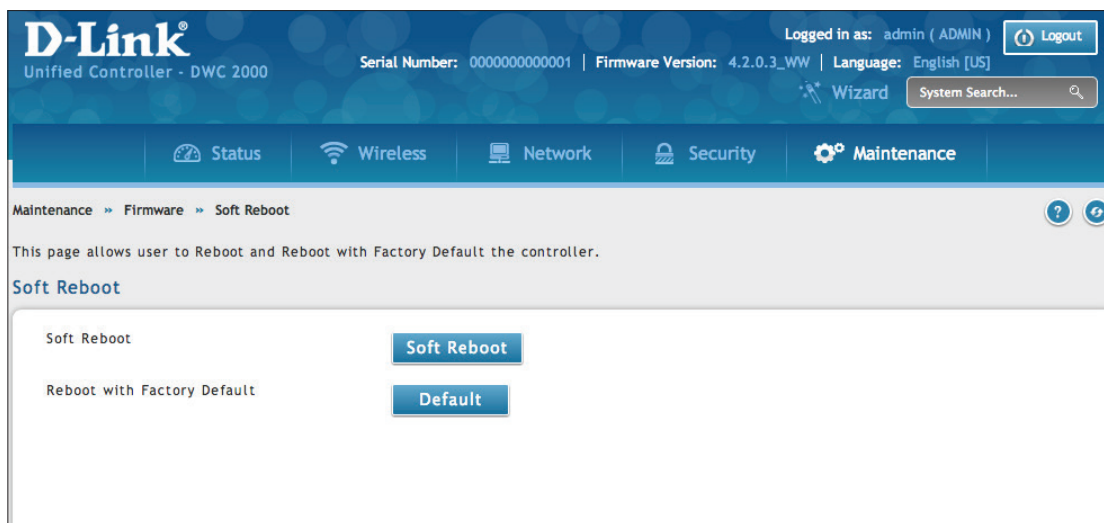
Path: Maintenance > Firmware > Soft Reboot

If you reset a wireless controller to its factory default settings, it returns to the state when it was new — all changes you made to the default configuration are lost. Examples of settings that get restored include critical things you need to get online, such as login password, SSID, IP addresses, and wireless security keys.

There are two ways to restore a wireless controller to its original factory default settings:

- Use the reset button on the back of the wireless controller (see “Using the Reset Button to Restore Default Settings” on page 258).
- Use the web management interface instructions below.

1. Click **Maintenance > Firmware > Soft Reboot**.



2. Next to Factory Default settings, click the **Default** button.
3. At the confirmation message, click **OK** to restore factory default settings; or click **Cancel** to retain your current settings.

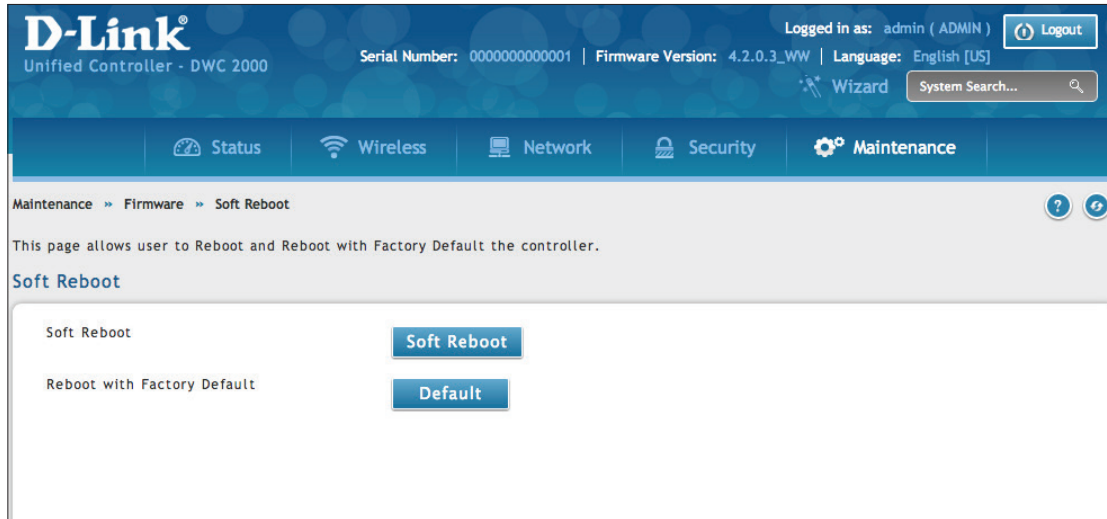
Note: After restoring the factory default configuration, the wireless controller's default LAN IP address is 192.168.10.1, the default login user name is **admin**, and the default login password is **admin**.

Rebooting the Wireless Controller

Path: Maintenance > Firmware > Soft Reboot

You can reboot the wireless controller. Rebooting performs a power cycle and keeps any customized overrides you made to the default settings.

1. Go to **Maintenance > Firmware > Soft Reboot**.



2. Next to Soft Reboot, click **Soft Reboot**. To reboot to the original factory default, click **Default**.
3. At the confirmation message, click **OK** to reboot the wireless controller or click **Cancel** to not reboot.

Upgrading Firmware

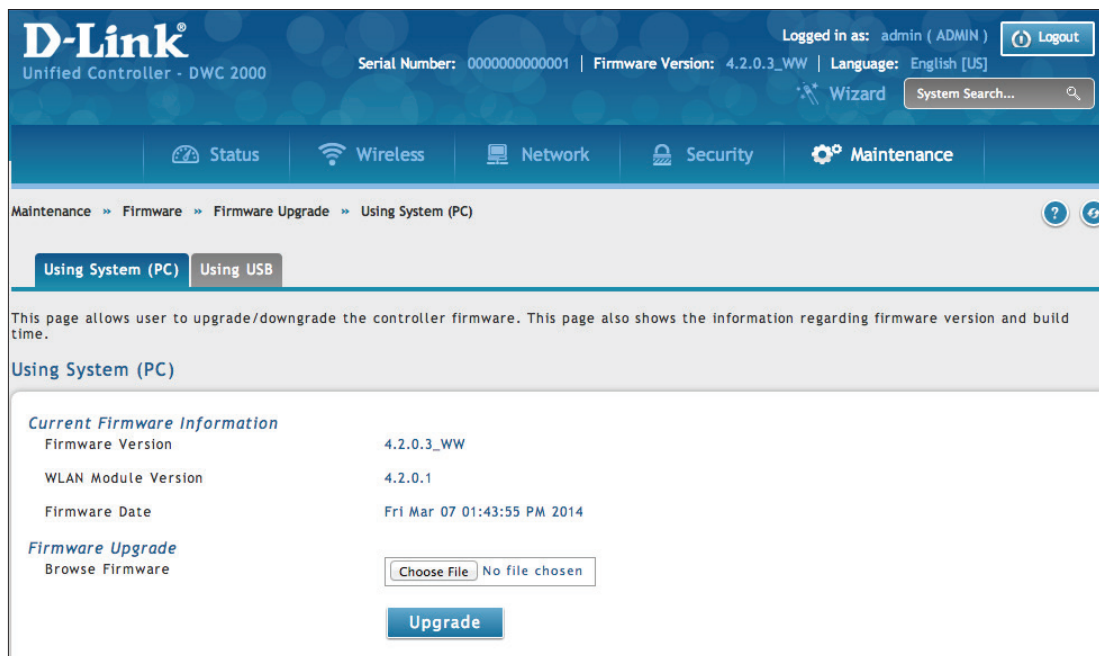
Wireless Controller Firmware Upgrade

Path: Maintenance > Firmware > Firmware Upgrade > Using System (PC)

D-Link is constantly improving the operation and performance of the wireless controller. When improvements are available, they are offered to customers as firmware upgrade releases.

After you install the wireless controller, check that it has the latest firmware. Thereafter, check for firmware releases and install them as they become available.

1. In the wireless controller web management interface, click **Maintenance > Firmware > Firmware Upgrade**. The Using System (PC) page will appear.



To use a USB drive to update the firmware, click the **Using USB** tab.

Maintenance » Firmware » Firmware Upgrade » Using USB

Please Connect a USB Storage Device!

Using System (PC)

Using USB

This page allows user to upgrade/downgrade the router firmware via USB Device.

Using USB

USB Port 1

USB Device Status

disconnected

Select Firmware

Upgrade

USB Port 2

USB Device Status

disconnected

Select Firmware

Upgrade

D-Link DWC-2000 User Manual

254

2. If the firmware version on the D-Link support website has a higher number than the firmware version shown under Firmware Information, continue with this procedure.
3. Download the new firmware from the D-Link website.
4. Under *Firmware Upgrade*, click the **Choose File** button.
5. In the Choose File dialog box, navigate to the firmware file, and then click the file and click **Open**. If you want to upgrade using a file from a USB drive, click the Using USB tab near the top of this page.
6. Click **Upgrade**.
7. At the confirmation message, click **OK** to start the firmware upgrade. A progress bar shows the progress of the upgrade.
***Note:** The upgrade process takes a few minutes. Do not interrupt the upgrade or turn off the system; otherwise, you can damage the firmware. Wait for the upgrade to complete before browsing any sites from your browser.*
8. When the upgrade completes, log in to the wireless controller web management interface, click **Maintenance > Firmware > Firmware Upgrade**, and confirm that the new firmware appears next to Firmware on the Using System (PC) page.
9. Record the firmware level in Appendix A.

Using the Command Line Interface

The wireless controller supports a command-line interface (CLI). The CLI lets you use a VT-100 terminal-emulation program to locally or remotely configure, monitor, and control the wireless controller and its managed access points via a simple text-based, tree-structured interface. The wireless controller supports SSH and Telnet management for command-line interaction.

The following procedure describes how to access the CLI:

Note: A separately purchased USB-to-DB9Fserial adapter will be helpful when connecting a PC or Linux workstation to the console. An RJ-45-to-DB9M cable is included with the wireless controller.

1. Connect a PC with a VT-100 terminal-emulation program to the Console port on the front panel of the wireless controller.
2. CLI login credentials are shared with the GUI for administrator users. When prompted, type cli in the SSH or console prompt and login with administrator user credentials.

For more information, refer to the Wireless Controller CLI Reference Guide: DWC-2000.

Troubleshooting

In the unlikely event you encounter a problem using the wireless controller, refer to the troubleshooting suggestions in this chapter to identify and resolve the problem.

The topics covered in this chapter are:

- "LED Troubleshooting" on page 257
- "Web Management Interface" on page 257
- "Using the Reset Button to Restore Default Settings" on page 258
- "Problems with Date and Time" on page 258
- "Discovery Problems with Access Points" on page 258
- "Connection Problems" on page 259
- "Network Performance and Rogue Access Point Detection" on page 259
- "Using Diagnostic Tools on the Wireless Controller" on page 260

LED Troubleshooting

After you apply power and turn on the wireless controller, the following sequence of events should occur:

1. When power is first applied, verify that the front panel (green) Power LED to the left of the USB ports is ON.
2. After approximately 2 minutes, verify that the right LAN port LED is ON for any local ports that are connected. This indicates that a link has been established to the connected device.
3. If a RJ-45 port is connected to a 1000Mbps device, verify that the port's left LED is orange. If a port is connected to a 100Mbps device, verify that the port's left LED is green. If a port is connected to a 10Mbps device, verify that the port's right LED is OFF.
4. If a SFP port is connected a 1000Mbps device, verify that the port's LED is orange. If a port is connected to a 100Mbps device, verify that the port's LED is green.

If any of these conditions do not occur, see the appropriate section below.

Power LED is OFF

If the Power and other LEDs are off when your wireless controller is turned on, confirm that the power cord is connected properly to the wireless controller and that the power cord is connected to a functioning power outlet that is not controlled by a wall switch.

If the error persists, please contact D-Link technical support.

LAN Port LEDs Not ON

If the LAN LEDs do not go ON when the Ethernet connection is made:

1. Check that the Ethernet cable connections are secure at the wireless controller and at the switch.
2. Be sure power is applied to the connected switch and that the switch is turned on.
3. Be sure you are using the correct cables (straight-through or crossover).

Web Management Interface

If you cannot access the wireless controller's web management interface from a PC on your local network:

- Check the Ethernet connection between the PC and the wireless controller.
- Be sure your PC's IP address is on the same subnet as the wireless controller. If you are using the recommended addressing scheme, be sure your PC is configured to use a static IPv4 address of 192.168.10.nnn (where nnn is the number 0 or a number from 2 to 255) and a subnet of 255.255.255.0.
- If the wireless controller's IP address has been changed and you do not know the current IP address, reset the wireless controller's configuration to factory default settings. This sets the wireless controller's IP address to 192.168.10.1 (refer to "Restoring Factory Default Settings" on page 251), but it also loses any changes you made to the factory default settings.
- If you do not want to revert to the factory default settings and lose your configuration settings, you can reboot the wireless controller and use a sniffer to capture packets sent during the reboot. Look at the ARP packets to find the wireless controller's LAN interface address.

Using the Reset Button to Restore Default Settings

If you cannot access the wireless controller's management interface for some reason, press the reset button on the front panel to restore the factory default settings.

To clear all settings and restore the factory default values:

1. Press and hold the reset button for at least 15 seconds.
2. Release the reset button. The reboot process is complete after several minutes.

Note: After restoring the factory default configuration, the wireless controller's default LAN IP address is 192.168.10.1, the default login user name is admin, and the default login password is admin.

Problems with Date and Time

The Date and Time page shows the current date and time of day. The wireless controller uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day.

If you find that the date and time stamps are not accurate, confirm that the wireless controller can reach the Internet.

Discovery Problems with Access Points

If the wireless controller does not discover any or all access points:

- Be sure the wireless controller is connected to the LAN (see "LAN Port LEDs Not ON" on page 257).
- Be sure you entered the appropriate IP address range if the access points operate in different VLANs, reside behind an IP subnet, or operate in standalone mode (see "Step #1: Enable DHCP Server (Optional)" on page 25).
- If you are using a firewall, unblock the UDP port number for each access port in the firewall.
- Be sure each access point is using a unique IP address (see "AP Discovery Methods" on page 75). If more than one access point has the same IP address, only one of them is discovered. In this case, add the access point to the managed list, change its IP address, and then run discovery again to discover the next access point with that IP address (see "Step #3: Select APs to be Managed" on page 27).

Connection Problems

When an access point is converted from standalone mode to managed mode, its static IP address changes to an IP address that is issued by the DHCP server, either one in the network or one that is configured on the wireless controller. This occurs to ensure that each managed access point has a unique IP address.

If there is no DHCP server or if the access point cannot reach the DHCP server, the access point remains in the Connecting state as it tries to obtain an IP address. If there is no DHCP server in the network, configure one on the wireless controller (see “Step #1: Enable DHCP Server (Optional)” on page 25). When a DHCP server becomes available, the access point can transition from the Connecting state to the Connected state.

If you added a new SSID, but the SSID does not appear under Wi-Fi Networks within 5 minutes, use the following procedure to reboot the Wireless Controller.

1. Click **Maintenance** > **Firmware** > **Soft Reboot**.
2. Click **Soft Reboot**.

Network Performance and Rogue Access Point Detection

When rogue access point detection is enabled, access points intermittently go off channel for short periods, which can affect network performance. If security concerns are more important than network performance, you can enable rogue access point detection. If network performance is more important than security concerns, you can temporarily disable rogue access point detection.

Using Diagnostic Tools on the Wireless Controller

Ping an IP Address

Path: Maintenance > Management > Diagnostics > Network Tools

As part of the diagnostics functions on the wireless controller, you can ping an IP address. You can use this function to test connectivity between the wireless controller and another device on the network connected to the wireless controller.

1. Go to **Maintenance > Management > Diagnostics > Network Tools**.

The screenshot displays the D-Link Unified Controller - DWC 2000 web interface. The top navigation bar includes links for Status, Wireless, Network, Security, and Maintenance. The Maintenance section is expanded, showing sub-menus for Network Tools, Capture Packets, and System Check. The Network Tools section is active, displaying a form for Command Output for Ping and Traceroute. The form includes a text input field for IP Address / Domain Name (containing 'www.dlink.com'), buttons for Ping and Traceroute, and a large text area for Command Output. Below this, there is a section for DNS Lookup with a text input field for Domain Name and a button for Lookup, followed by another Command Output text area.

2. Under *Command Output for Ping and Traceroute*, in the IP Address / Domain Name field, enter an IP address or domain name.
3. Click **Ping**. The results will appear in the Command Output display below.

Using Traceroute

Path: Maintenance > Management > Diagnostics > Network Tools

The wireless controller provides a Traceroute function that lets you map the network path to a public host. Up to 30 intermediate controllers (or “hops”) between this wireless controller and the destination will be displayed.

1. Go to **Maintenance > Management > Diagnostics > Network Tools**.

The screenshot shows the D-Link Unified Controller - DWC 2000 web interface. The top navigation bar includes links for Status, Wireless, Network, Security, and Maintenance. The Maintenance section is expanded, showing sub-links for Network Tools, Capture Packets, and System Check. The Network Tools section is active, displaying a form for Command Output for Ping and Traceroute. The form includes a text input field for IP Address / Domain Name (containing 'www.dlink.com'), buttons for Ping and Traceroute, and a large text area for Command Output. Below this, there is a section for DNS Lookup with a text input field for Domain Name and a button for Lookup.

2. Under *Command Output for Ping and Traceroute*, in the IP Address / Domain Name field, enter an IP address or domain name.
3. Click **Traceroute**. The results will appear in the Command Output display below.

Performing DNS Lookups

Path: Maintenance > Management > Diagnostics > Network Tools

The wireless controller provides a DNS lookup function that lets you retrieve the IP address of a Web, FTP, Mail, or any other server on the Internet.

1. Go to **Maintenance > Management > Diagnostics > Network Tools**.

The screenshot shows the D-Link Unified Controller web interface. The top navigation bar includes links for Status, Wireless, Network, Security, and Maintenance. The Maintenance section is expanded, showing Management > Diagnostics > Network Tools. The Network Tools section has tabs for Network Tools, Capture Packets, and System Check. The main content area displays the 'Command Output for Ping and Traceroute' section with a text input field containing 'www.dlink.com' and buttons for 'Ping' and 'Traceroute'. Below this is a 'DNS Lookup' section with a 'Domain Name' input field and a 'Lookup' button. Both sections have a 'Command Output' display area.

2. Under *DNS Lookup*, in the Domain Name field, enter an Internet name.
3. Click **Lookup**. The results will appear in the Command Output display below. If the host or domain entry exists, a response will appear with the IP address. If the message *Host Unknown* appears, the Internet name does not exist.

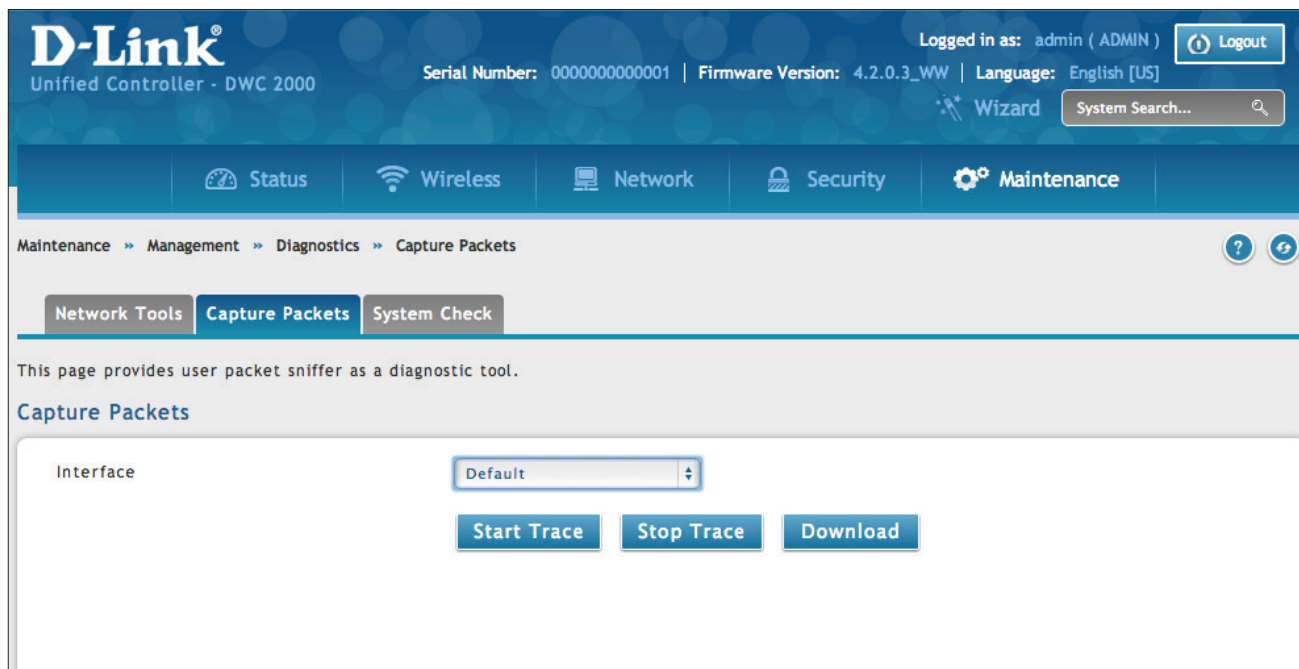
Capturing Log Packets

Path: Maintenance > Management > Management > Diagnostics > Capture Packets

The wireless controller lets you capture all packets that pass through the LAN or Option interface. The packet trace is limited to 1 MB of data per capture session. If the capture file size exceeds 1MB, it is deleted automatically and a new capture file is created.

To capture packets:

1. Go to **Maintenance > Management > Diagnostics > Capture Packets**.



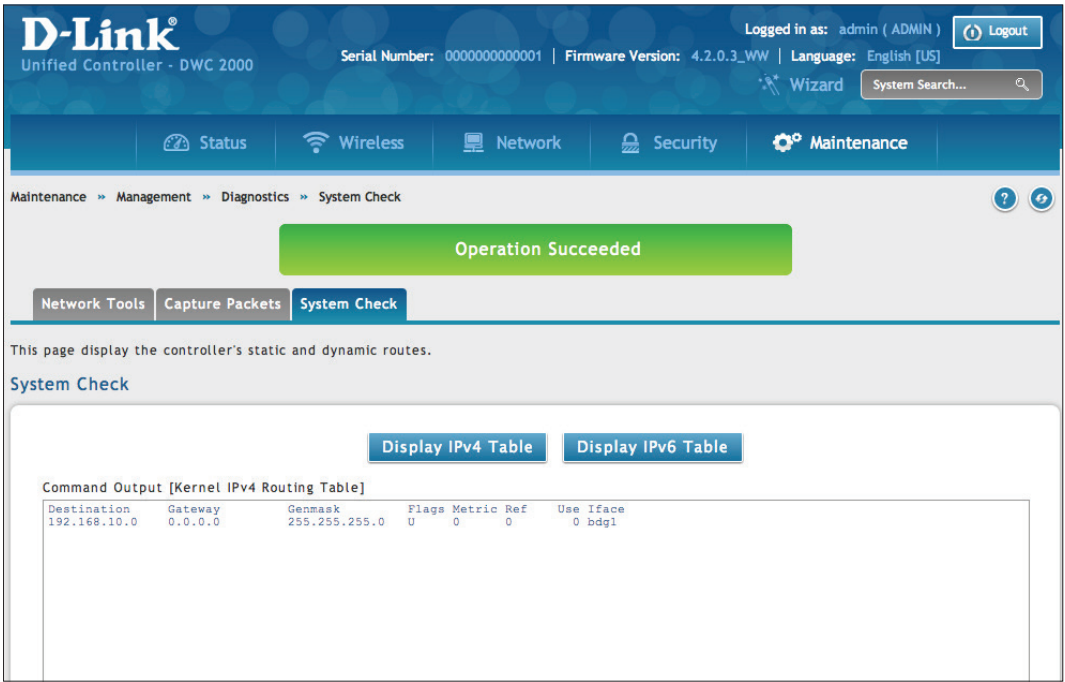
2. Select an interface from the drop-down menu.
3. Click **Start Trace**. The results are shown in the Command Output page. The trace can be downloaded by clicking the **Download** button, which will immediately begin the download to the browsers default download location.

Conducting a System Check

Path: Maintenance > Management > Diagnostics > System Check

As part of the diagnostics functions on the wireless controller, you can ping an IP address. You can use this function to test connectivity between the wireless controller and another device on the network connected to the wireless controller.

- 1. Go to **Maintenance > Management > Diagnostics > System Check**.



- 2. Click **Display IPv4 Table** or **Display IPv6 Table**. The results will appear in the Command Output display below.

Log Settings

The wireless controller lets you capture log messages. You can monitor the type of traffic that goes through the wireless controller and be notified of potential attacks or errors when they are detected by the controller. The following sections describe the log configuration settings and the ways you can access these logs.

Defining What to Log

Path: Maintenance > Logs Settings > Facility Logs

The Facility Logs page lets you determine the granularity of logs to receive from the wireless controller. Select one of the following facilities:

- Kernel = the Linux kernel. Log messages that correspond to this facility would correspond to traffic through the firewall or network stack.
- System = application and management-level features available on this wireless controller for managing the unit.

D-Link®
Unified Controller - DWC 2000

Logged in as: admin (ADMIN) [Logout](#)

Serial Number: 0000000000001 | Firmware Version: 4.2.0.3_WW | Language: English [US]

Wizard

Status Wireless Network Security **Maintenance**

Maintenance » Logs Settings » Facility Logs

This page allows user to configure logging severity levels for different logging facilities.

Facility Logs

Facility
Select Facility ☐ Kernel ☒ System

For Event Log

| | Event Log | Syslog |
|--------------|--|--|
| Emergency | <input type="button" value="ON"/> <input type="button" value="OFF"/> | <input type="button" value="ON"/> <input type="button" value="OFF"/> |
| Alert | <input type="button" value="ON"/> <input type="button" value="OFF"/> | <input type="button" value="ON"/> <input type="button" value="OFF"/> |
| Critical | <input type="button" value="ON"/> <input type="button" value="OFF"/> | <input type="button" value="ON"/> <input type="button" value="OFF"/> |
| Error | <input type="button" value="ON"/> <input type="button" value="OFF"/> | <input type="button" value="ON"/> <input type="button" value="OFF"/> |
| Warning | <input type="button" value="ON"/> <input type="button" value="OFF"/> | <input type="button" value="ON"/> <input type="button" value="OFF"/> |
| Notification | <input type="button" value="ON"/> <input type="button" value="OFF"/> | <input type="button" value="ON"/> <input type="button" value="OFF"/> |
| Information | <input type="button" value="ON"/> <input type="button" value="OFF"/> | <input type="button" value="ON"/> <input type="button" value="OFF"/> |
| Debugging | <input type="button" value="ON"/> <input type="button" value="OFF"/> | <input type="button" value="ON"/> <input type="button" value="OFF"/> |

For each facility, the following events (in order of severity) can be logged:

| Severity | Description |
|--------------|----------------------------------|
| Emergency | System is unusable |
| Alert | Action must be taken immediately |
| Critical | Critical conditions |
| Error | Error conditions |
| Warning | Warning conditions |
| Notification | Normal but significant condition |
| Information | Informational |
| Debugging | Debug-level messages |

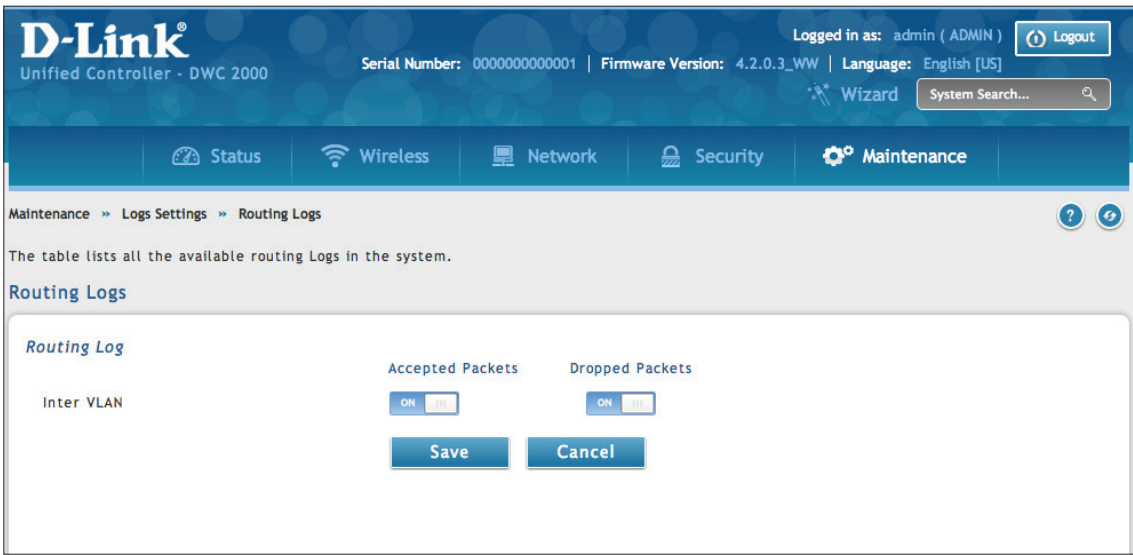
The display for logging can be customized based on whether the logs are sent to the Event Log viewer in the web management interface (the Event Log viewer is in the Status > System Information > All Logs > Current Logs) or a remote Syslog server for later review. E-mail logs, discussed in a subsequent section, follow the same configuration as logs configured for a Syslog server.

Tracking Traffic/Routing Logs

Maintenance > Logs Settings > Routing Logs

Traffic can be tracked based on whether the packet was accepted or dropped by the firewall. Denial of service attacks, general attack information, login attempts, dropped packets, and similar events can be captured for review by the IT administrator.

Note: Enabling logging options may generate a significant volume of log messages and is recommended for debugging purposes only.



| Option | Description |
|------------------|--|
| Accepted Packets | If enabled, tracks packets that were transferred through the segment successfully. |
| Dropped Packets | If enabled, tracks packets that were blocked from being transferred through the segment. |
| Routing Logs | |
| Inter VLAN: | If enable, tracks traffic from inter VLAN routing logs. |

After making your selections on this page, click **Save** to save your changes or click **Cancel** to revert to the previous settings.

System Logging

Path: Maintenance > Logs Settings > System Logs

The System Logs page lets you select the type of traffic passing through the wireless controller that you want to log for display in Syslog, E-mailed logs, or the Event Viewer. This page helps you capture suspicious activity such as denial-of-service attacks, general attack information, login attempts, dropped packets, and similar events. Traffic can be tracked based on whether the packet was accepted or dropped by the firewall.

D-Link®
Unified Controller - DWC 2000

Logged in as: admin (ADMIN) [Logout](#)

Serial Number: 00000000000001 | Firmware Version: 4.2.0.3_WW | Language: English [US]

Wizard

Status Wireless Network Security **Maintenance**

Maintenance » Logs Settings » System Logs

This page allows user to configure system wide log settings.

System Logs

| | |
|-----------------------------------|------------------------------|
| All Unicast Traffic | <input type="checkbox"/> OFF |
| All Broadcast / Multicast Traffic | <input type="checkbox"/> OFF |
| FTP Log | <input type="checkbox"/> OFF |
| Redirected ICMP Packets | <input type="checkbox"/> OFF |
| Invalid Packets | <input type="checkbox"/> OFF |

[Save](#) [Cancel](#)

| Routing Logs | |
|--|---|
| All Unicast Traffic | If enabled, tracks packets directed to the wireless controller. |
| All Broadcast / Multicast Traffic | If enabled, tracks all broadcast or multicast packets directed to the wireless controller. |
| FTP Logs | If checked, logged information is sent to FTP logs. |
| Redirected ICMP Packets | If checked, tracks the number of redirected Internet Control Message Protocol (ICMP) packets. |
| Invalid Packets | If checked, tracks the number of invalid packets received. |

Remote Logging

Path: Maintenance > Logs Settings > Remote Logs

The wireless controller can be configured to send logs to an email address. Email logs can be sent out based on a defined schedule by first choosing the frequency: hourly, daily, or weekly. The wireless controller lets you send configuration logs to three email recipients.

The screenshot shows the 'Remote Logging' configuration page in the D-Link Unified Controller interface. The page is titled 'Remote Logging' and includes a description: 'This page allows user to configure the remote logging options for the controller.' The configuration fields are as follows:

- Remote Log Identifier:** A text field containing 'DWC-2000'.
- E-Mail Log:** A dropdown menu set to 'ON'.
- E-Mail Server Address:** A text field.
- SMTP Port:** A text field with a range indicator '(Range: 1 - 65535)'.
- Return E-Mail Address:** A text field.
- Send to E-Mail Address (1):** A text field.
- Send to E-Mail Address (2):** A text field.
- Send to E-Mail Address (3):** A text field.
- Authentication with SMTP:** Radio buttons for 'None', 'Plain Login' (selected), and 'CRAM-MD5'.
- User Name:** A text field.
- Password:** A text field.
- Respond to Identd from SMTP:** A checkbox set to 'OFF'.
- E-Mail log by schedule:** A section with a 'Unit:' label and radio buttons for 'Never' (selected), 'Hourly', 'Daily', and 'Weekly'.

At the bottom of the form are 'Save' and 'Cancel' buttons.

| Option | Description |
|--|---|
| Log Options | |
| Remote Log Identifier | Enter a prefix used to identify the source of the message. This identifier is prefixed to both e-mail and Syslog messages. |
| Routing Logs | |
| Enable E-Mail Logs | Enables or disables email logs. Choices are: <ul style="list-style-type: none"> • ON = enable email logs. Complete the remaining fields on this page. • OFF = disable email logs. The remaining fields on this page are unavailable. |
| E-Mail Server Address | If Enable E-Mail Logs is enabled, enter the IP address or Internet Name of a Simple Mail Transfer Protocol (SMTP) server. The wireless controller will connect to this server to send e-mail logs when required. The SMTP server must be operational for email notifications to be received. |
| SMTP Port | If Enable E-Mail Logs is enabled, enter the SMTP port of the e-mail server. |
| Return E-Mail Address | If Enable E-Mail Logs is enabled, enter the e-mail address where replies from the SMTP server are to be sent (required for failure messages). |
| Send to E-mail Address(1-3) | If Enable E-Mail Logs is enabled, enter up to three email addresses where logs and alerts are to be sent. |
| Authentication with SMTP Server | If Enable E-Mail Logs is enabled, select an authentication if the SMTP server requires authentication before accepting connections. Choices are: <ul style="list-style-type: none"> • None = no authentication is used. The User Name and Password fields are not available. • Login Plain = authentication used to log in using Base64-encoded passwords over non-encrypted communication session. Base64-encoded passwords offer no cryptographic protection, making them vulnerable. • CRAM-MD5 = a challenge-response authentication mechanism defined in RFC 2195 based on the HMAC-MD5 MAC algorithm. CRAM-MD5 offers a higher level of authentication than Login Plain. |

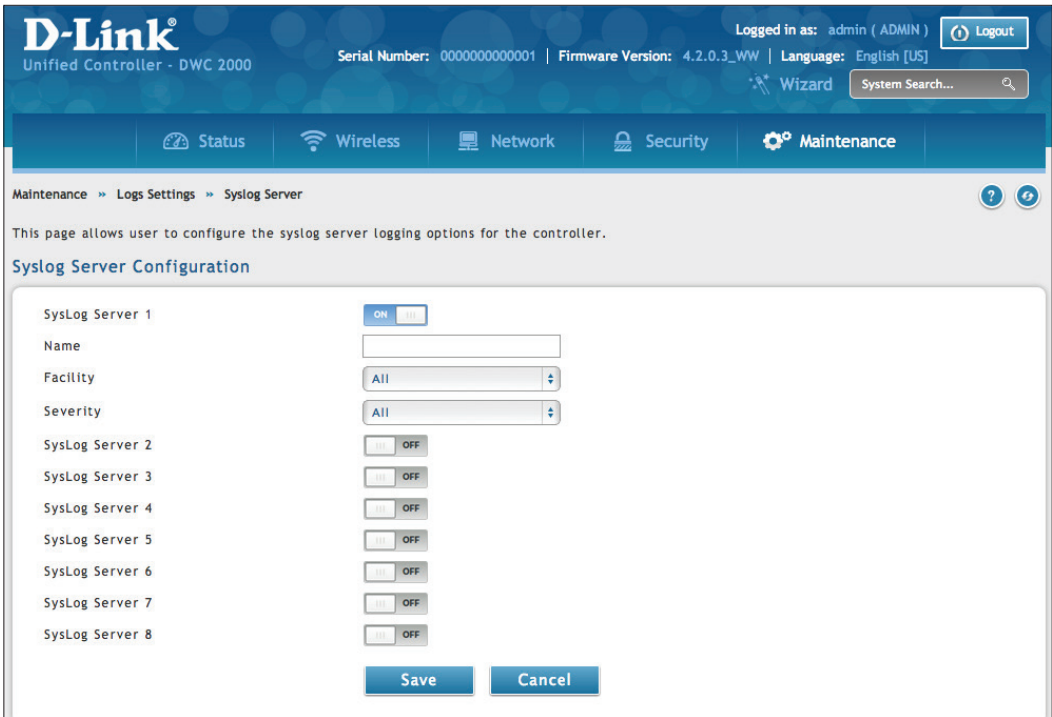
| Option | Description |
|--|--|
| User Name | If Authentication with SMTP Server is set to Login Plain or CRAM-MD5, enter the user name to be used for authentication. |
| Password | If Authentication with SMTP Server is set to Login Plain or CRAM-MD5, enter the case-sensitive password to be used for authentication. |
| Respond to Identd from SMTP Server | If Enable E-Mail Logs is checked, this option determines whether the wireless controller responds to IDENT requests from the SMTP server. Choices are: <ul style="list-style-type: none"> • ON = wireless controller responds to an IDENT request from the SMTP server. • OFF = wireless controller ignores IDENT requests from the SMTP server. |
| Send E-Mail Logs by Schedule | |
| To receive e-mail logs according to a schedule, configure the appropriate schedule settings. Scheduling options are enabled when the Enable E-Mail Logs option is checked. | |
| Unit | Select the period of time that you need to send the log. This option is useful when you do not want to receive logs by e-mail, but want to keep e-mail options configured, so you can use the Send Log function Event Log viewer pages. Choices are: <ul style="list-style-type: none"> • Never = disable sending of logs. • Hourly = send logs every hour. • Daily = send logs every day at the Time specified. • Weekly = send logs weekly, at the Day and Time specified. |
| Day | If Unit is set to Weekly, select the day when logs will be sent. |
| Time | If Unit is set to Daily or Weekly, select the time when logs will be sent. |

Syslog Server Configuration

Path: Maintenance > Logs Settings > Syslog Server

An external Syslog server is often used by network administrator to collect and store logs from the wireless controller. This remote device typically has less memory constraints than the local Event Viewer on the wireless controller’s web management interface. Therefore, a number of logs can be collected over a sustained period. This is useful for debugging network issues or to monitor controller traffic over a long duration.

The wireless controller supports 8 concurrent Syslog servers. Each server can be configured to receive different log facility messages of varying severity using the Remote Logging page. This page also lets you send configuration logs to three email recipients.

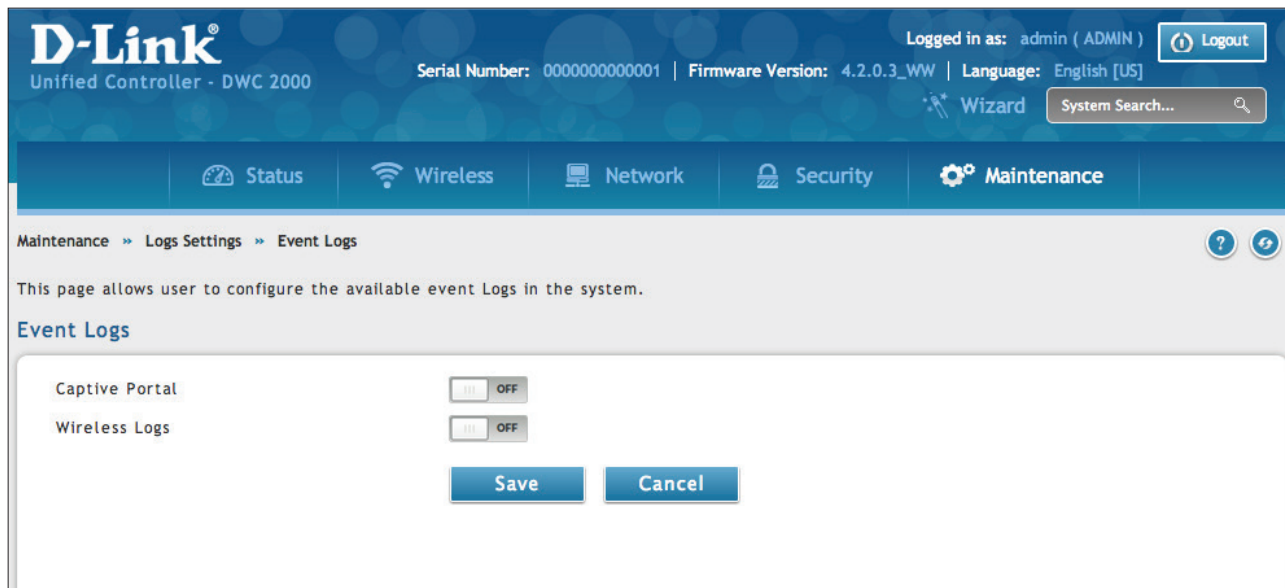


| Syslog Server Configuration | |
|---|---|
| To enable a Syslog server, click the ON/OFF switch next to an empty Syslog server field and enter an IP address or FQDN in the Name field. The selected facility and severity level messages are sent to the configured (and enabled) Syslog server after you save the settings on this page. | |
| Switch | To have the wireless controller send logs to a Syslog server, check one or more boxes. You can check up to 8 Syslog servers and use them concurrently. |
| FQDN/IP Address | Enter the IP address or Internet Name of the Syslog server. |
| Facility | For each syslog server, select a unique facility for logging. Facility values are defined in RFC 3164. Choices are: <ul style="list-style-type: none">AllKernelSystem |
| Syslog Severity | Select the appropriate Syslog severity. When a severity is selected, all Syslogs with severity equal to or greater than the chosen severity are logged on the configured Syslog Server. |

Event Log

Path: Maintenance > Logs Settings > Event Log

The wireless controller's web management interface displays configured log messages from the Status menu. When traffic through or to the wireless controller matches the settings in the Maintenance > Log Settings > FacilityLogs page (see "Log Settings" on page 265) or Maintenance > Log Settings > Routing Logs page (see "Tracking Traffic/Routing Logs" on page 267), the corresponding log message will appear in this window with a timestamp:



| Option | Description |
|----------------|--|
| Captive Portal | If enabled, the controller will log information related to wireless client logs in and log out via Captive Portal. |
| Wireless Logs | If enabled, the controller will log information relative to wireless activities. |

Note: To understand log messages, it is very important to have accurate system time that has been set manually or from a NTP server.

Current Logs

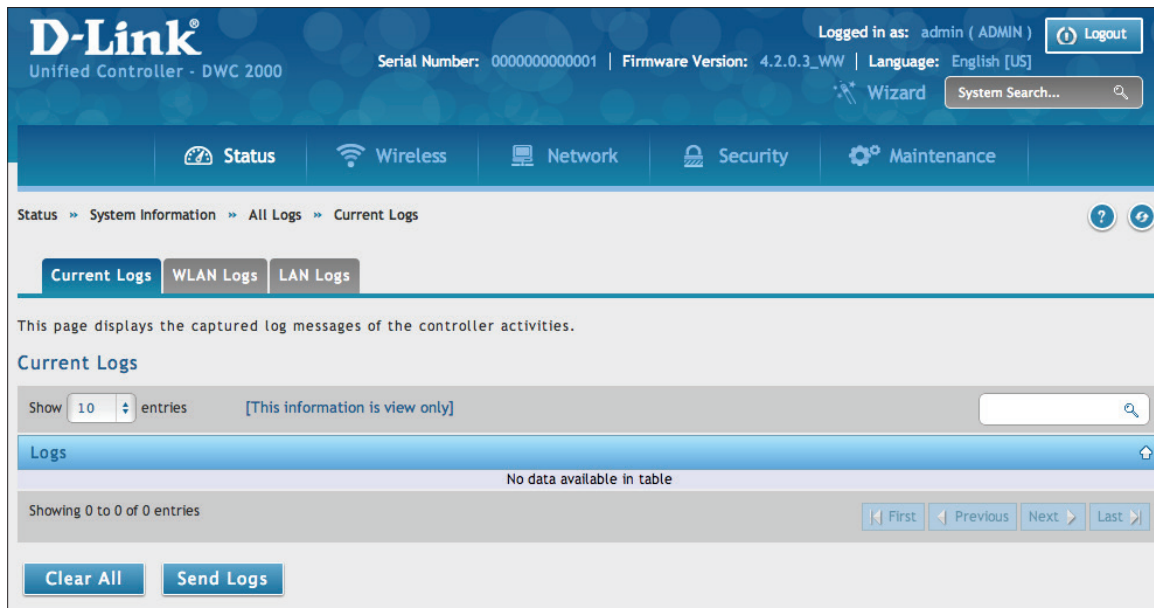
Path: Status > System Information > All Logs > Current Logs

The Display Logs window allows you to view configured log messages from the controller as they appear. Each log will appear with a timestamp as determined by the controller's configured time. If remote logging such as a Syslog server or e-mail logging is configured, the same logs are sent to the remote interface while being displayed here.

Click **Refresh** (Right side on the page) for refresh logs or reload page again.

Click **Clear All** to remove all entries in the Display Logs screen.

Click **Send Logs** to send all logs in the Display Logs screen to preconfigured e-mail recipients.



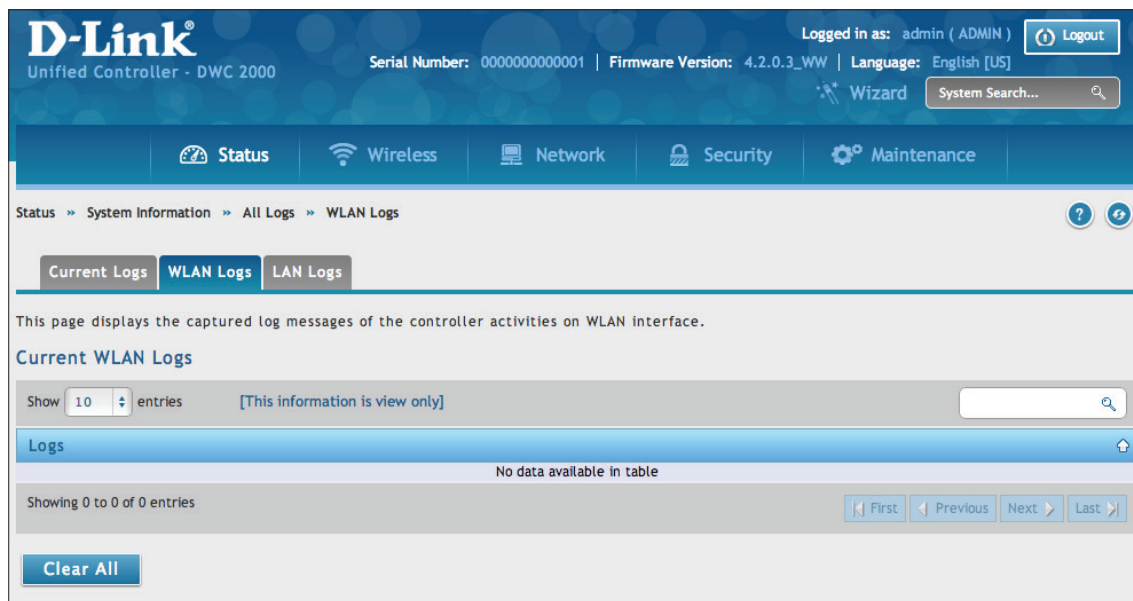
WLAN Logs

Path: Status > System Information > All Logs > WLAN Logs

The Display Logs window allows you to view configured log messages from the controller on WLAN interface as they appear. Each log will appear with a timestamp as determined by the controller's configured time. The same logs are sent to the WLAN interface while being displayed here.

Click **Refresh** (Right side on the page) for refresh logs or reload page again.

Click **Clear All** to remove all entries in the Display Logs screen.



LAN Logs

Path: Status > System Information > All Logs > LAN Logs

The Display Logs window allows you to view configured log messages from the controller on LAN interface as they appear. Each log will appear with a timestamp as determined by the controller's configured time. The same logs are sent to the WLAN interface while being displayed here.

Click **Refresh** (Right side on the page) for refresh logs or reload page again.

Click **Clear All** to remove all entries in the Display Logs screen.

The screenshot displays the D-Link Unified Controller - DWC 2000 web interface. At the top, the user is logged in as 'admin (ADMIN)' with a 'Logout' button. The interface includes a navigation bar with tabs for Status, Wireless, Network, Security, and Maintenance. The 'Status' tab is active, and the breadcrumb path is 'Status > System Information > All Logs > LAN Logs'. Below the breadcrumb, there are tabs for 'Current Logs', 'WLAN Logs', and 'LAN Logs', with 'LAN Logs' selected. A help icon is visible on the right. The main content area shows a list of log entries under the heading 'Current LAN Logs'. The list includes timestamps, source identifiers, and log messages. For example, the first entry is '<10> Feb 22 23:47:14 0.0.0.0-1 General[183543196]: bootos.c(289) 3 %% Event(0xaaaaaaaa)'. At the bottom, there is a pagination control showing 'Showing 1 to 10 of 34 entries' and navigation buttons for 'First', 'Previous', '1', '2', '3', '4', 'Next', and 'Last'.

Appendix A - Basic Planning Worksheet

RF planning enables you to specify how Wi-Fi coverage will be provided. It provides coverage maps and locations prone to weak signals or dead spots that might require additional access points to provide adequate Wi-Fi coverage.

A Basic Planning Worksheet similar to the one in this appendix allows you to collect the following critical information to expedite your planning efforts.

- Building dimensions
- Walls and possible obstructions to wireless coverage
- Number of floors
- Distance between floors
- Total number of users and number of users per access point
- Radio type(s)
- Desired access point data rates
- Areas where you want to deploy access points
- Areas where you cannot deploy an access point
- Areas where you do not want coverage

| Step | Task | Completed? |
|-------------------------------------|---|------------|
| Site Planning | | |
| 1 | Height of building | |
| 2 | Width of building | |
| 3 | Number of floors | |
| 4 | Floor dimensions | |
| 5 | Distance between floors | |
| 6 | Visual obstructions | |
| 7 | Possible causes of interference | |
| Access Point Planning | | |
| 1 | Frequency band | |
| 2 | Expected signal quality | |
| 3 | Number of clients per access point | |
| 4 | Total number of clients per floor | |
| 5 | Desired access point data rate | |
| Wireless Controller Planning | | |
| 1 | Change the wireless controller default password and record it here: | |
| 2 | Configure your time zone and record it here _____ | |
| 3 | Use default radio configuration? Profile Name: _____ Clients _____ Modes Available: 802.11 b/g: 802.11 n: 802.11 b/g/n: 802.11 a – 5 GHz Only: 802.11 a/n – 5 GHz Only: 802.11 a/n/ac - 5 GHz Only: | |
| 4 | SSID information Service Set Identifier (SSID) name: _____ Security (none, WEP, WPA, or WPA2): _____ | |
| 5 | Use wireless controller as a DHCP server? Yes = host name and IP address should be assigned dynamically. No = use DHCP relay or configure static IP addresses and record them below. IP address: IP subnet mask: Gateway IP address: Primary DNS server: Secondary DNS server: | |

| | | |
|----|---|--|
| 6 | LAN IP address: | |
| 7 | Subnet Mask: | |
| 8 | IP address range: Starting IP address range: Ending IP address range: | |
| 9 | Default gateway (optional): | |
| 10 | DNS server: Primary DNS server: Secondary DNS server: | |
| 11 | Domain: | |
| 12 | WINS server: | |
| 13 | Are you connected to the Internet? Yes No | |
| 14 | Confirm and record firmware levels for the wireless controller and all access points: DWC-2000 wireless controller: DWL-2600AP access point: DWL-3600AP access point: DWL-6600AP access point: DWL-8600AP access point: DWL-8610AP access point: | |
| 15 | Record MAC addresses for the wireless controller and all access points: DWC-2000 wireless controller: DWL-2600AP access point(s): DWL-3600AP access point(s): DWL-6600AP access point(s): DWL-8600AP access point(s): DWL-8610AP access point(s): | |

Appendix B - Factory Default Settings

| Feature | Description | Default Setting |
|--------------------------|--|---------------------|
| Device Login | User login URL | http://192.168.10.1 |
| | User name (case sensitive) | admin |
| | Login password (case sensitive) | admin |
| Local area network (LAN) | IP address | 192.168.10.1 |
| | IPv4 subnet mask | 255.255.255.0 |
| | DHCP server | Disabled |
| | DHCP starting IP address | 192.168.10.100 |
| | DHCP ending IP address | 192.168.10.254 |
| | Time zone | GMT |
| | Time zone adjusted for Daylight Savings Time | Disabled |
| | SNMP | Disabled |
| | Remote management | Disabled |

Appendix C - Glossary

Access Point - A device that provides network access to wireless devices.

ARP - Address Resolution Protocol. Broadcast protocol for mapping IP addresses to MAC addresses.

CHAP - Challenge-Handshake Authentication Protocol. Protocol for authenticating users to an ISP.

DDNS - Dynamic DNS. System for updating domain names in real time. Allows a domain name to be assigned to a device with a dynamic IP address.

DHCP - Dynamic Host Configuration Protocol. Protocol for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

DNS - Domain Name System. A hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network.

FQDN - Fully qualified domain name. Complete domain name, including the host portion. Example: serverA.companyA.com.

FTP - File Transfer Protocol. Protocol for transferring files between network nodes.

HTTP - Hypertext Transfer Protocol. Protocol used by web browsers and web servers to transfer files.

IKE - Internet Key Exchange. Mode for securely exchanging encryption keys in ISAKMP as part of building a VPN tunnel.

IP - Internet Protocol. The principal communications protocol used for relaying datagrams known as network packets across an internetwork using the Internet Protocol Suite. IP is responsible for routing packets across network boundaries. It is the primary protocol that establishes the Internet.

IPsec - IP security. Suite of protocols for securing VPN tunnels by authenticating or encrypting IP packets in a data stream. IPsec operates in either transport mode (encrypts payload but not packet headers) or tunnel mode (encrypts both payload and packet headers).

ISAKMP - Internet Key Exchange Security Protocol. Protocol for establishing security associations and cryptographic keys on the Internet.

ISP - Internet service provider.

MAC Address - Media-access-control address. Unique physical-address identifier attached to a network adapter.

MTU - Maximum transmission unit. Size, in bytes, of the largest packet that can be passed on. The MTU for Ethernet is a 1500-byte packet.

NAT - Network Address Translation. Process of rewriting IP addresses as a packet passes through a controller or firewall. NAT enables multiple hosts on a LAN to access the Internet using the single public IP address of the LAN's gateway controller.

NetBIOS - Microsoft Windows protocol for file sharing, printer sharing, messaging, authentication, and name resolution.

NTP - Network Time Protocol. Protocol for synchronizing a controller to a single clock on the network, known as the clock master.

PAP - Password Authentication Protocol. Protocol for authenticating users to a remote access server or ISP.

PPPoE - Point-to-Point Protocol over Ethernet. Protocol for connecting a network of hosts to an ISP without the ISP having to manage the allocation of IP addresses.

PPTP - Point-to-Point Tunneling Protocol. Protocol for creation of VPNs for the secure transfer of data from remote clients to private servers over the Internet.

RADIUS - Remote Authentication Dial-In User Service. Protocol for remote user authentication and accounting. Provides centralized management of usernames and passwords.

RSA - Rivest-Shamir-Adleman. Public key encryption algorithm.

SSID - Service Set Identifier. A case-sensitive, 32-alphanumeric character unique identifier used for naming wireless networks. The SSID differentiates one wireless network from another. All access points and devices trying to connect to a specific wireless network must use the same SSID to enable effective roaming.

Subnet - A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 100.100.100 belong to the same subnet.

TCP - Transmission Control Protocol. Protocol for transmitting data over the Internet with guaranteed reliability and in-order delivery.

UDP - User Data Protocol. Protocol for transmitting data over the Internet quickly but with no guarantee of reliability or in-order delivery.

VPN - Virtual private network. Network that enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. Uses tunneling to encrypt all information at the IP level.

WINS - Windows Internet Name Service. Service for name resolution. Allows clients on different IP subnets to dynamically resolve addresses, register themselves, and browse the network without sending broadcasts.

Wireless Controller - D-Link device that centralizes and simplifies network management of a wireless LAN by consolidating individually managed access points into a single, unified solution.

Appendix D - Technical Specifications

| Capacity | |
|-------------------------------|--|
| Max. APs per device | Default: 64 Upgradable to 256 |
| Max. APs per clustering group | 1024 |
| Max. clustering controllers | 8 |
| Compatibility | |
| Unified Access Point Model | <ul style="list-style-type: none"> • DWL-2600AP • DWL-3600AP • DWL-6600AP • DWL-8600AP • DWL-8610AP |
| SFP Transceiver Model | <ul style="list-style-type: none"> • DEM-210 (B1/C1/D1/E1) • DEM-211 (B1/C1/D1/E1) • DEM-220T (B1/C1/D1/E1) • DEM-302S-BXD (A1) • DEM-302S-BXU (A1) • DEM-302S-LX (A1) • DEM-310GT (F1/G1/H1/I1) • DEM-311GT (F1/G1/H1/I1) • DEM-312GT2 (D1/E1) • DEM-314GT (E1/F1/G1/H1) • DEM-315GT (E1/F1/G1/H1) • DEM-330T (B1/B2/C1/D1) • DEM-330R (B1/B2/C1/D1) • DEM-331T (B1/B2/C1/D1) • DEM-331R (B1/B2/C1/D1) • DGS-712 (C1) |
| Upgrade License | <ul style="list-style-type: none"> • DWC-2000-AP32 / DWC-2000-AP32-LIC: additional 32 managed AP Licenses • DWC-2000-AP64 / DWC-2000-AP64-LIC: additional 64 managed AP licenses • DWC-2000-AP128 / DWC-2000-AP128-LIC: additional 128 managed AP licenses |