D-Link®
Building Networks for People

Version 1.3

Smart WLAN Manager

Configuration Guide

Business Class Networking

Table of Contents

Introduction

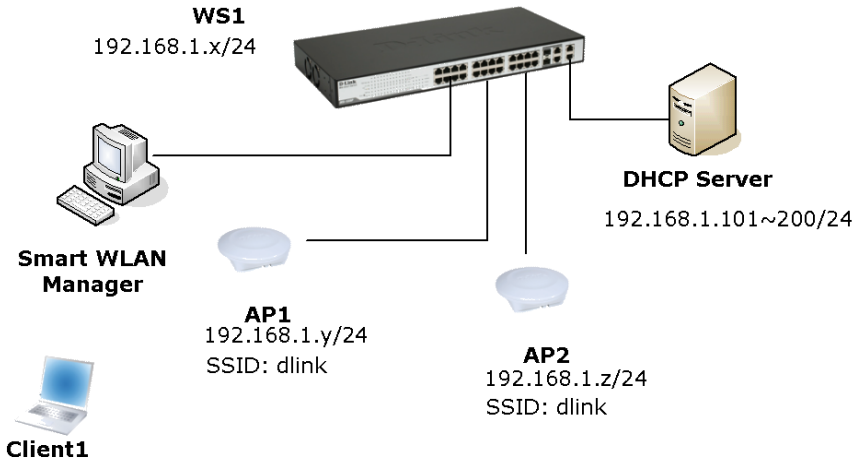
This document provides users with a quick guide that explains the essential operation of the Smart Wireless System (DES-1228P, DWL-3140AP, and Smart Wireless Manager). For detailed functions, please refer to the User Manual for each device.

Scenario 1 - Basic Setup

The diagram below shows a very basic L2 edge network configuration with one DES-1228P smart switch and two DWL-3140AP access points. All devices and the DHCP server are all in the same L2 domain.

The objectives in this setup are as follows:

- Understand the minimum configuration for operation.
- Discover the switch and APs.
- Understand the essential D-Link Web Smart Thin Access Point features.



The overview of the configuration steps for the Smart Wireless System is as follows:

1. Enable the wireless awareness function on the DES-1228P.
2. Discover the switch and APs.
3. Save the configuration.
4. Perform tests.

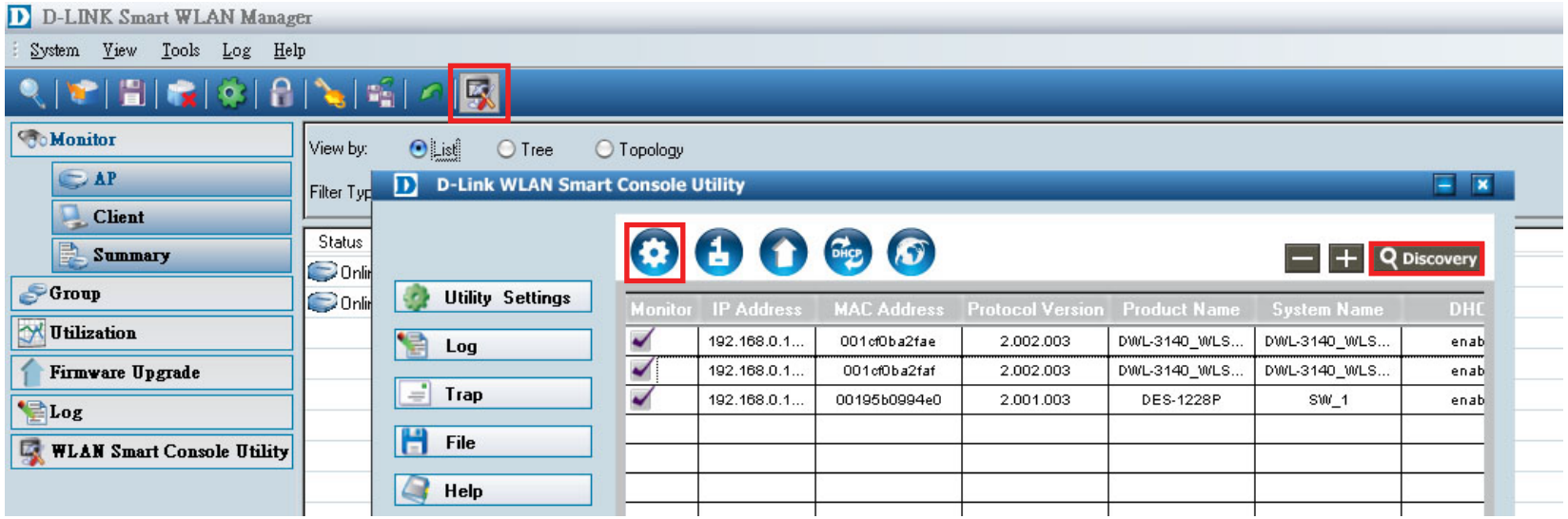
The table below shows the IP addresses used in this scenario. The following steps will guide you through the configuration of the Wireless Switch and the Access Point.

Device	Subnet
Wireless Switch	192.168.1.x/24
AP1	192.168.1.y/24
AP2	192.168.1.z/24
DHCP Pool	192.168.1.100~199/24

To begin the Wireless Switch configuration, connect APs to ports 9 and 17 (or any other unused ports). Continue to connect from a PC that is installed with the Smart Wireless Manager and on the same subnet (192.168.1.0/24) to port 1 (or any other unused port).

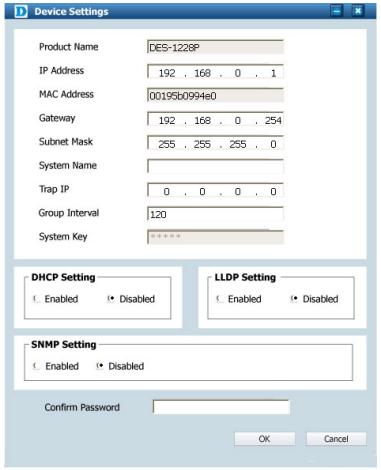
Enable the Wireless Awareness Function

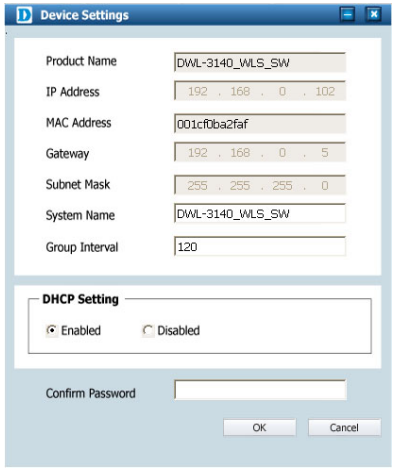
1. Launch the Smart WLAN Manager (no default password). Choose **Tools** > **Switch Discover Utility** or directly press the icon. The Discovery List window will appear. Click the **Discovery** button on the top right portion of the utility, and the Smart WLAN devices will be listed as shown below:



Note: DWL-3140AP with firmware version 1.00 cannot be discovered by the WLAN Smart Console. Please refer to the Firmware Upgrade section in the User Manual to upgrade the access points.

2. Select DES-1228P, and then click the device setting icon, the device setting window will appear. Enable DHCP Setting, LLDP Setting and SNMP Setting then click **OK**. (Note: The default password is admin). If the DHCP server is not in your environment, insert the manual IP address directly into the device setting window.

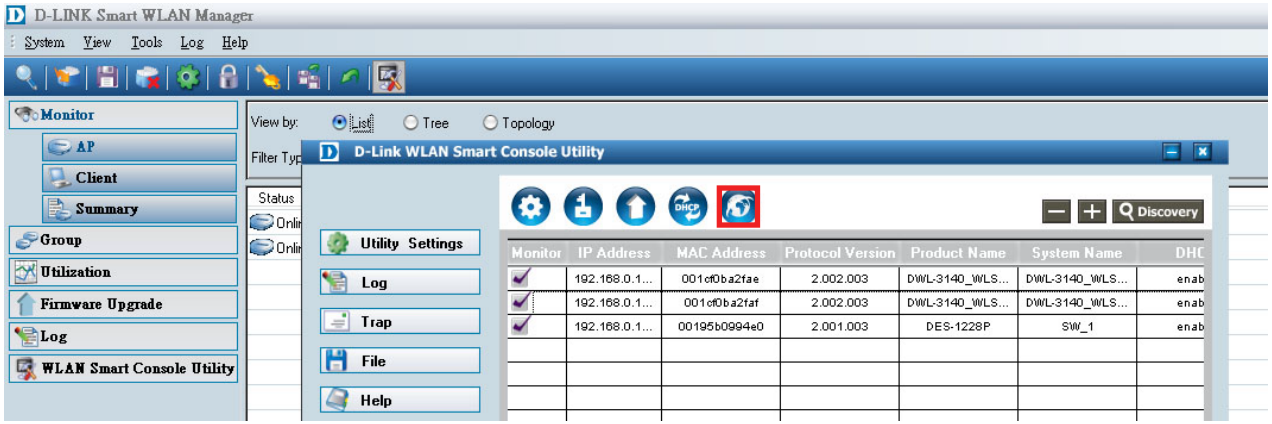




Note: The password for the DWL-3140AP in the Smart WLAN console is the SNMP community name, and the default value is “private”.

DES-1228P with firmware version 1.20 or earlier cannot configure LLDP and SNMP setting on the WLAN Smart Console Utility directly. Please refer to the following step to enable these two functions or find local technical support to upgrade the DES-1228P.

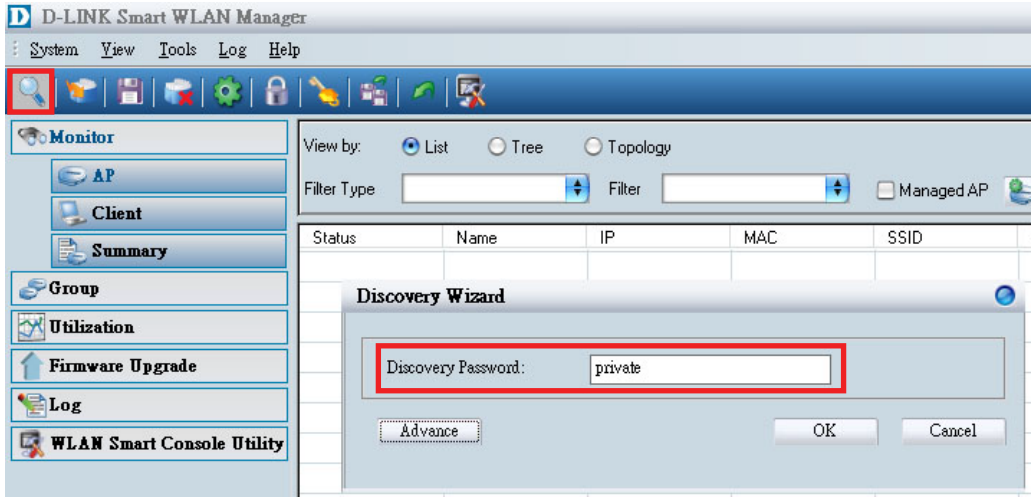
3. If you cannot find the LLDP/SNMP setting in the device setting window, click the web access icon to launch the Web-based Management Utility for the DES-1228P. (Note: The default password is admin).



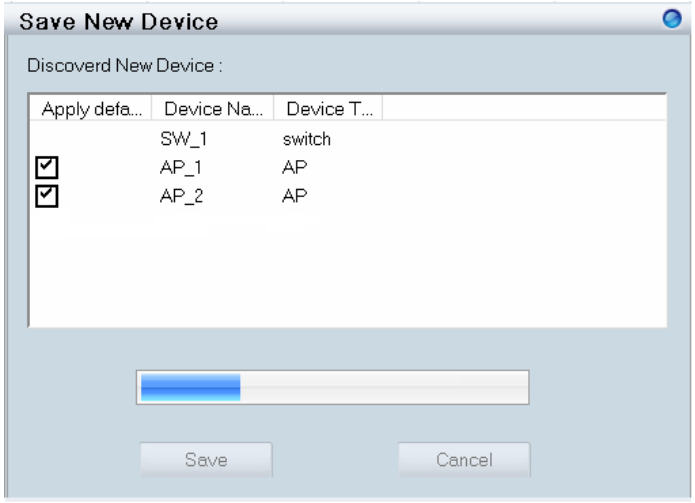
4. Enable the SNMP in **System** > **SNMP Settings** and enable the LLDP function in **Configuration** > **LLDP Setting**.

Discover the switch and APs

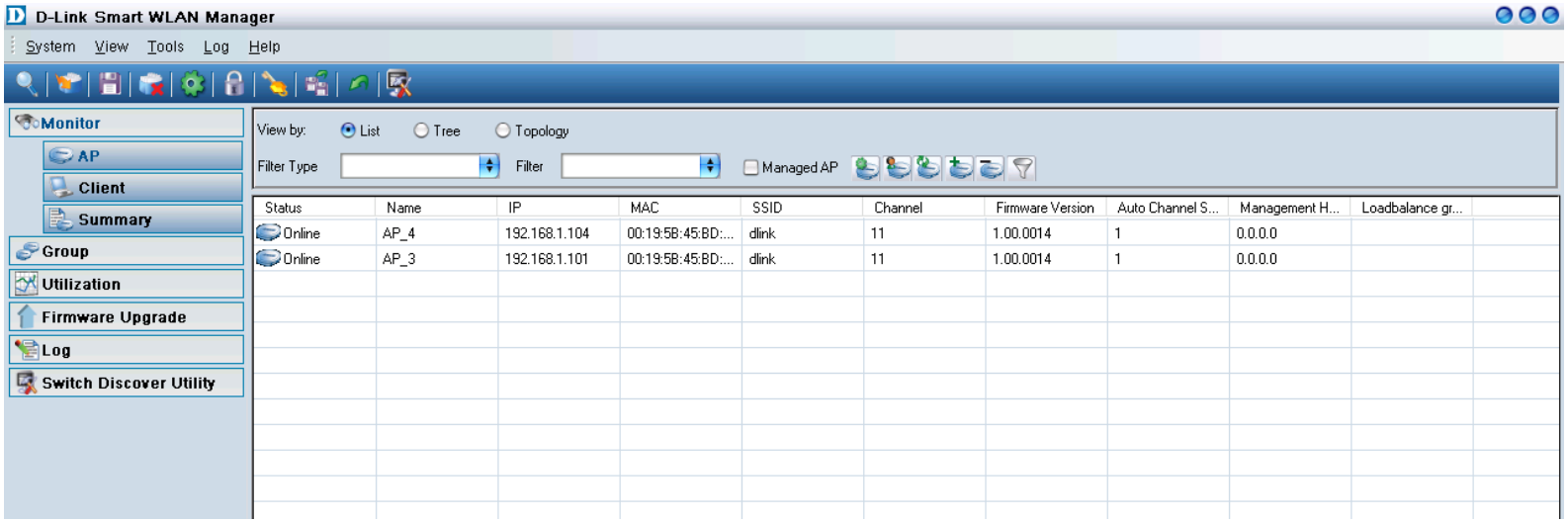
1. On the Smart WLAN Manager, choose **Tools** > **Discovery Wizard**. Fill in the Discovery password with the SNMP Read_Write Community Name “private” to discover the switch and APs.



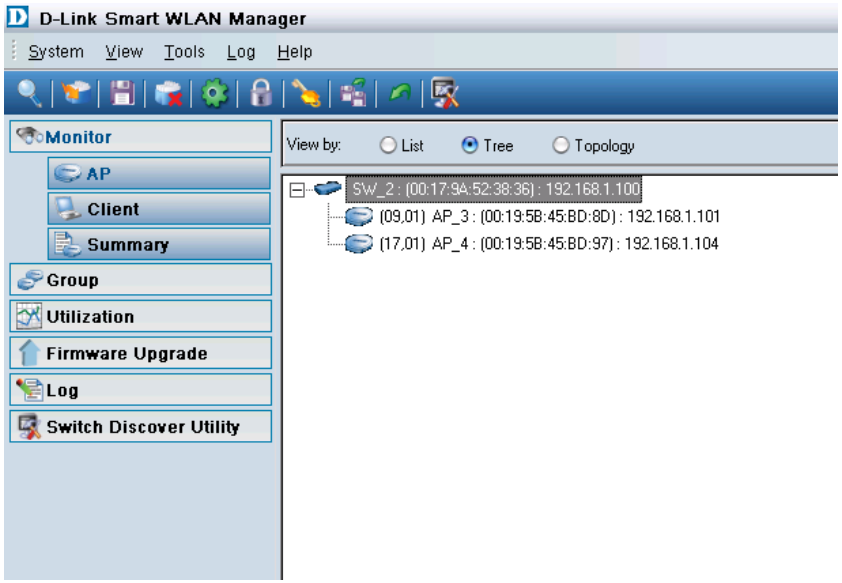
2. Click **OK** to scan the network by using the discovery password. The scanned results will appear as shown below.



3. Click **Save** to add the devices found into the database. The basic information of managed APs including *IP address*, *MAC address*, *SSID*, and *Channel* are listed as below:

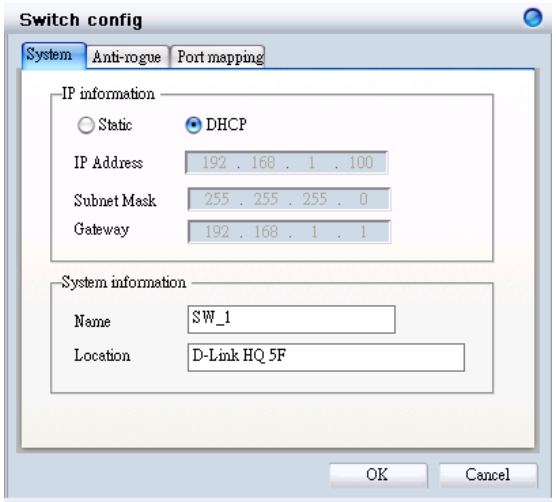


4. Change the view to tree view. The wireless switch and APs will be listed as shown below. This also shows which physical port the AP connects to the wireless switch.

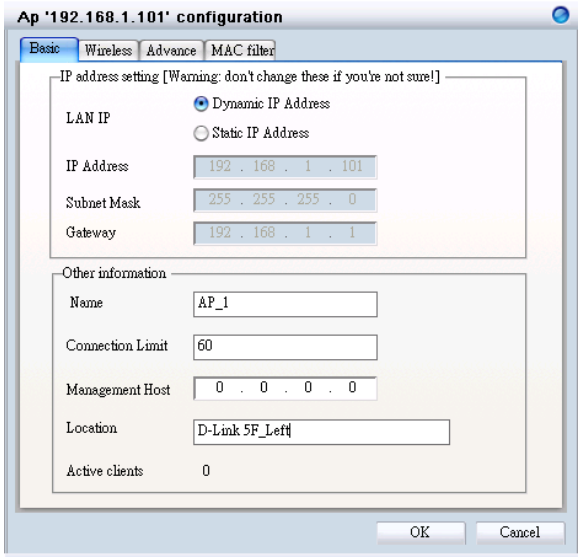


Basic Configuration

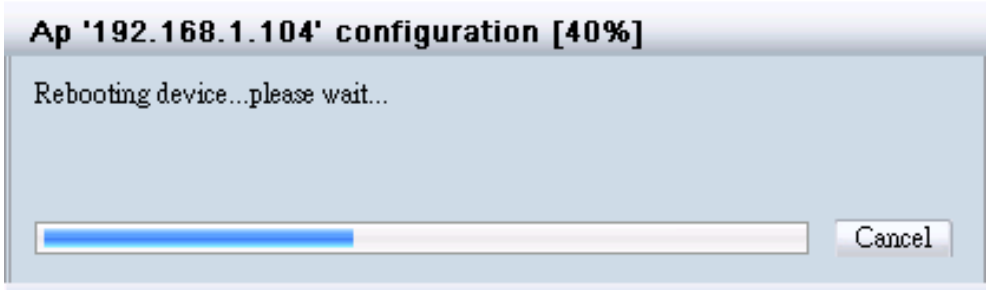
1. Double-click the switch entry, and the configuration window will appear. Click **OK** if any change is made.



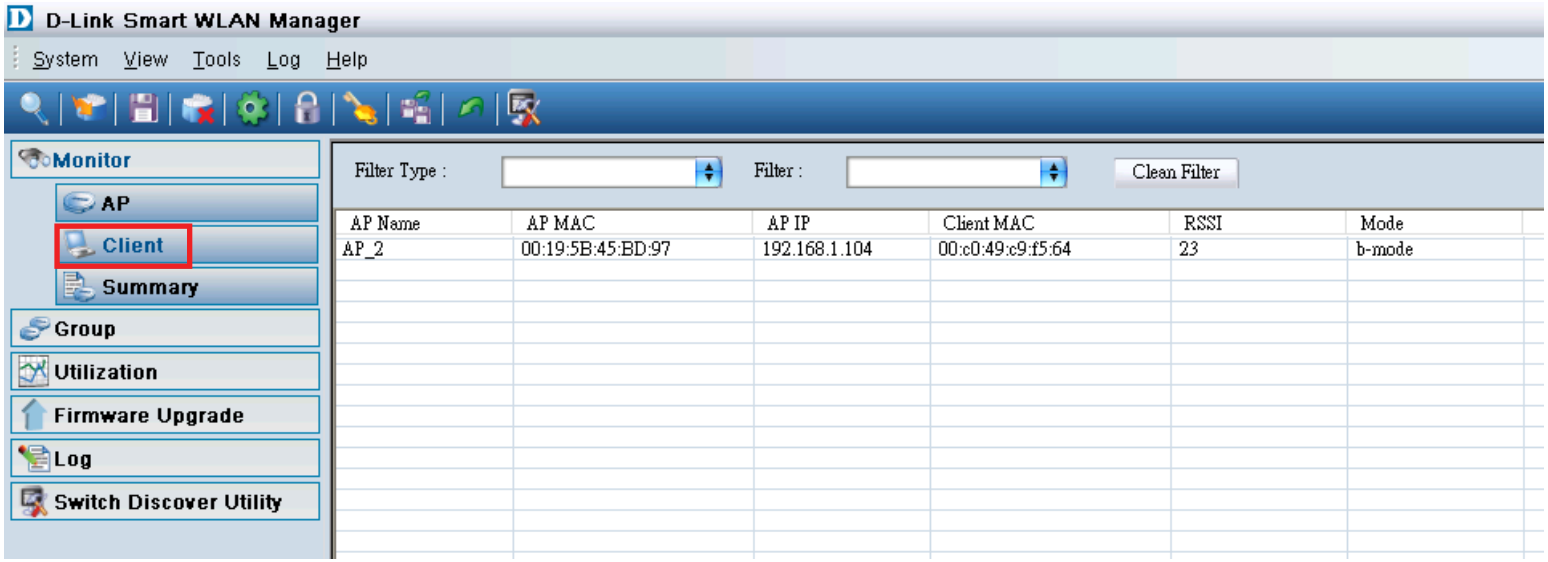
2. Similarly, double-click the AP entries, and the configuration window will appear. Click **OK** if any change is made.



3. The AP will reboot after the modification is made.



4. Use a wireless terminal (eg. Laptop or PDA) to connect to the SSID “dlink”; change to **Monitor** > **Client** and the client information will appear as shown below:



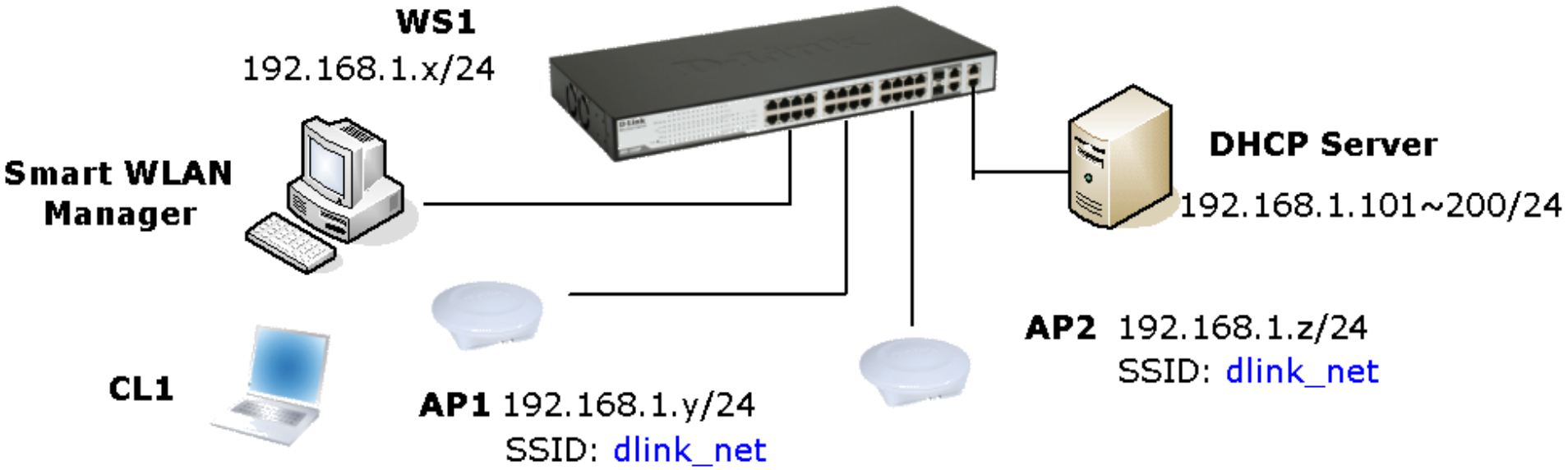
Performance Test

Ping AP, WS, and the default gateway from the client to test the connectivity.

Scenario 2 - Advanced Setup

Continued from the previous scenario, this session has the following objectives:

- Understand how to perform the central management for APs by group.
- Understand how to use the topology view.
- Understand how to enable the anti-rogue AP function.

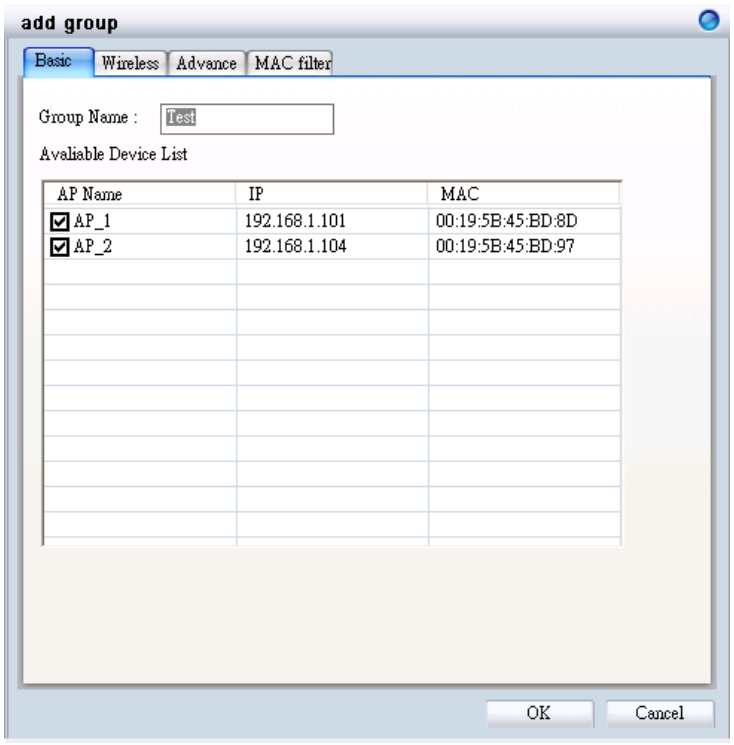


Enable the Wireless Awareness Function

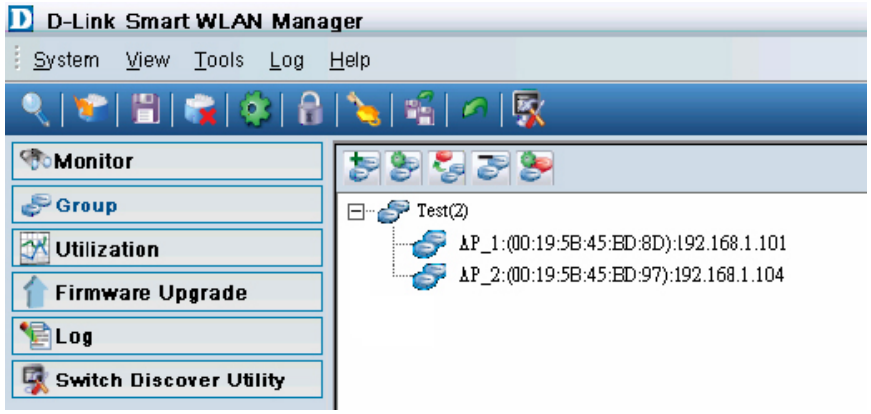
Smart WLAN Manager allows users to configure multiple access points at the same time by grouping them together. It makes the AP management more efficient, especially in large networks. Please see the following steps for more information on group configurations.

1. Change to the “Group” menu, and click the **Add Group** icon  . A window will appear. Fill in the group name “Test” and select both APs in the “Basic” tab.

2. Click **OK** and a confirmation message will appear. Click **OK** to confirm the change, and the group view will appear as shown below.

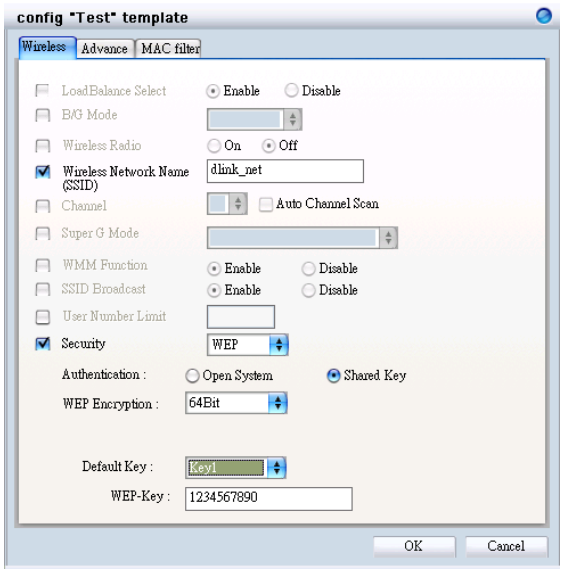


3. Select the “Test” group and click the **Config Group Template** icon . The Config template window will appear.

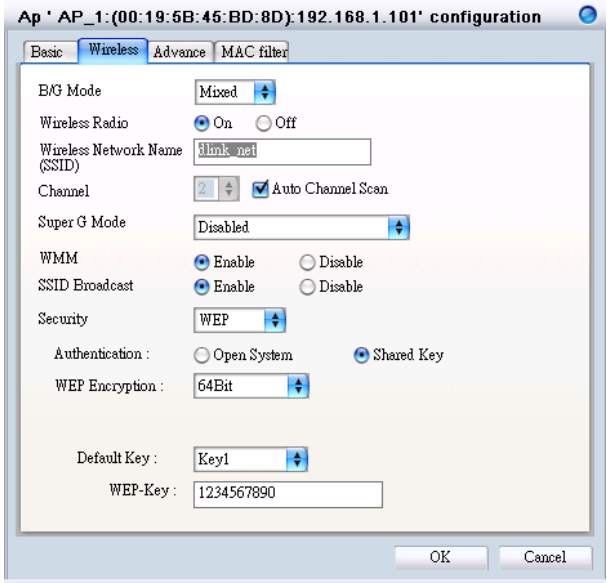


4. Check the Wireless Network Name and fill in new SSID “***dlink_net***”. Change the following settings:
   - Security: *WEP*
   - Authentication: *Shared Key*
   - WEP Encryption: *64Bit*
   - Default Key: *Key1*
   - WEP-Key: 1234567890

   Click **OK** to confirm the change and both APs will be rebooted.



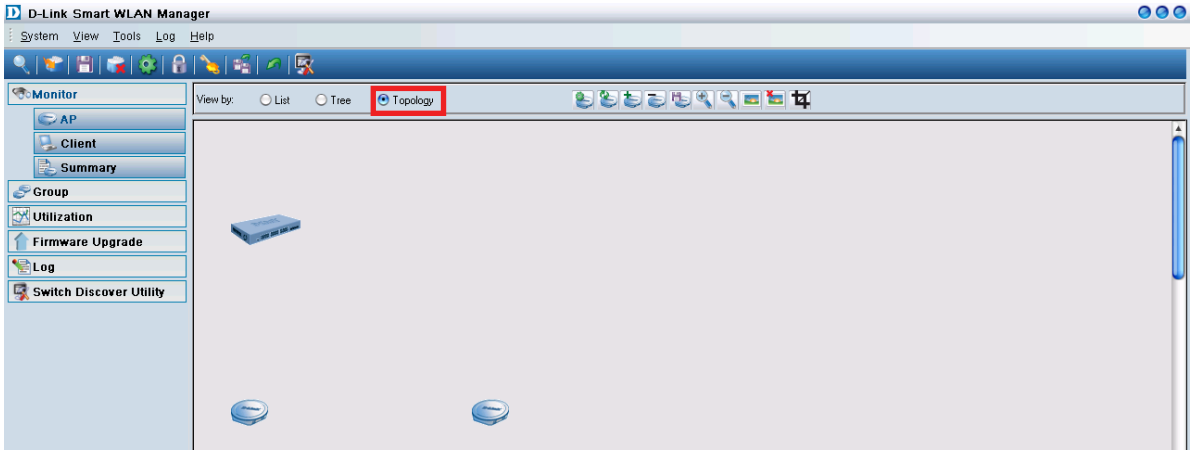
5. Right-click on an AP and select “Configuration”. Select the “Wireless” tab and note that all changes from the template will have been applied to the AP.



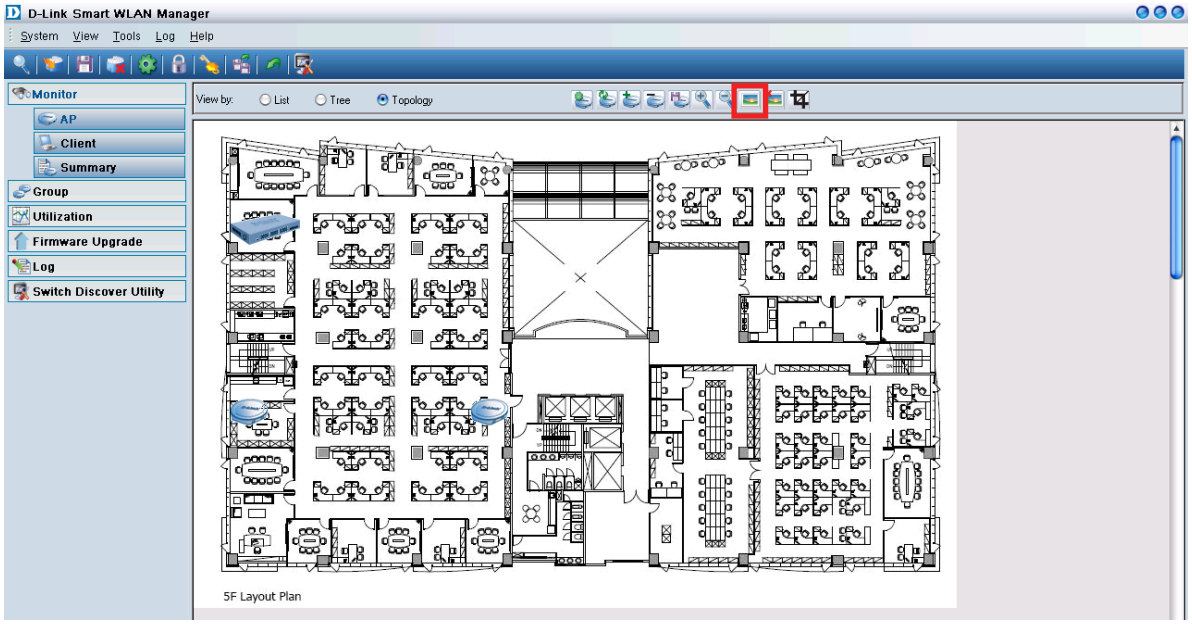
Topology View

Topology View offers users to visualize the status of the AP and wireless switch on the floor plan. With the topology view, users can locate the troubled AP very quickly once the failure occurs. Please see the following steps to configure topology view.

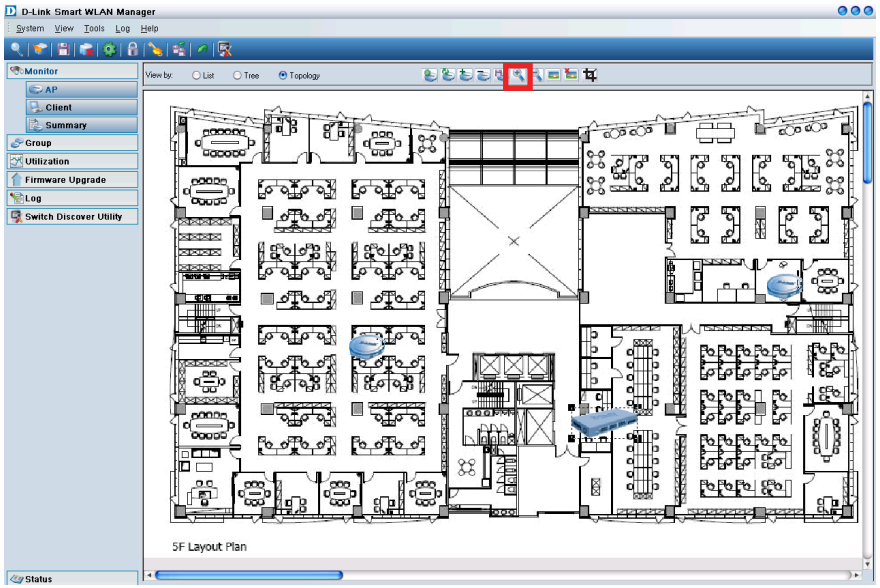
1. Select **Monitor** > **AP**, and view by topology.



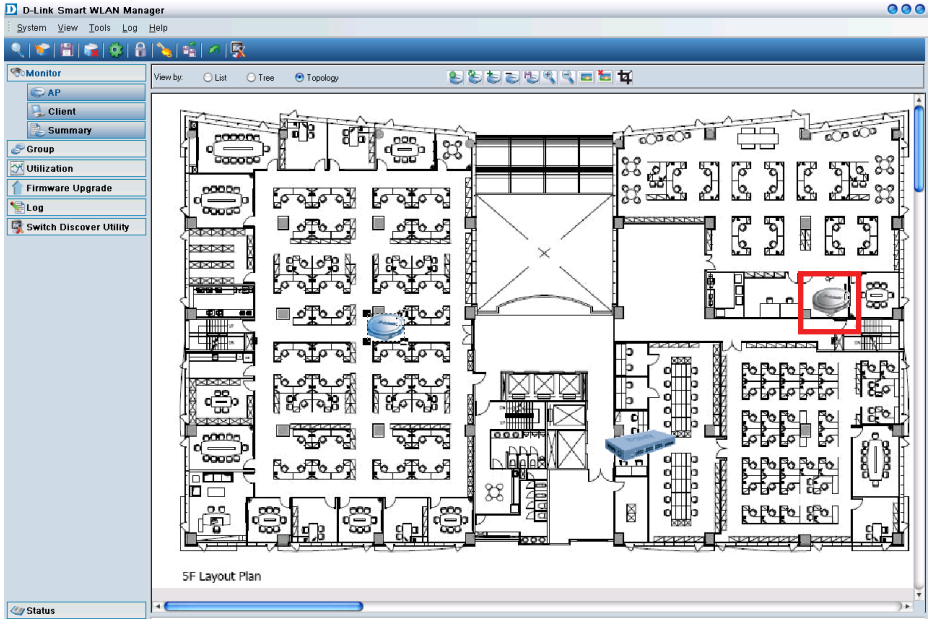
2. Click the **Load Map** icon to upload the floor plan file.



3. Zoom-in on the floor plan and drag the icons to their proper position, then click the “Save Topology Position” icon.



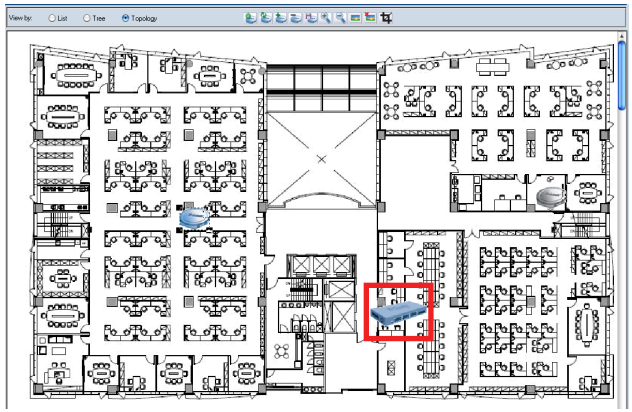
4. Disconnect an AP and observe the changes in the topology view.

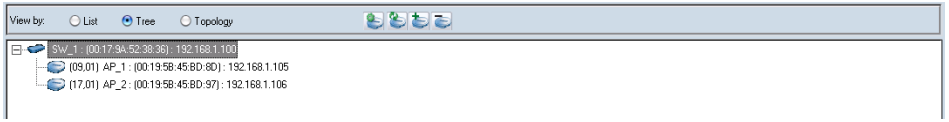


Configuring the Anti-Rogue AP

The Anti-Rogue AP function allows users to block illegal access points and keep network access security. Please continue with the following steps to configure the Anti-Rogue AP function.

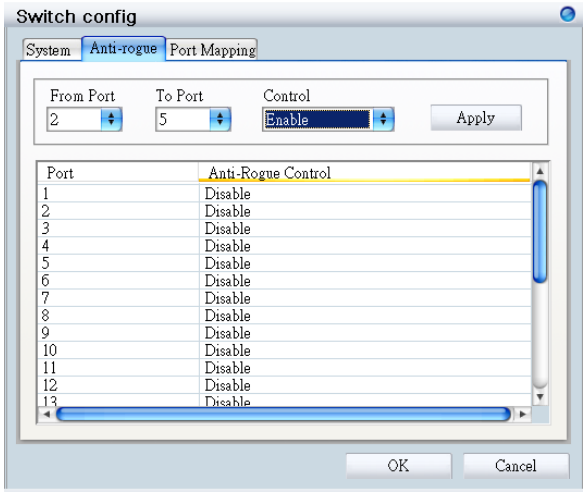
1. Double-click the switch you would like to enable the anti-rogue AP function from tree or topology view. The switch configuration window will appear.



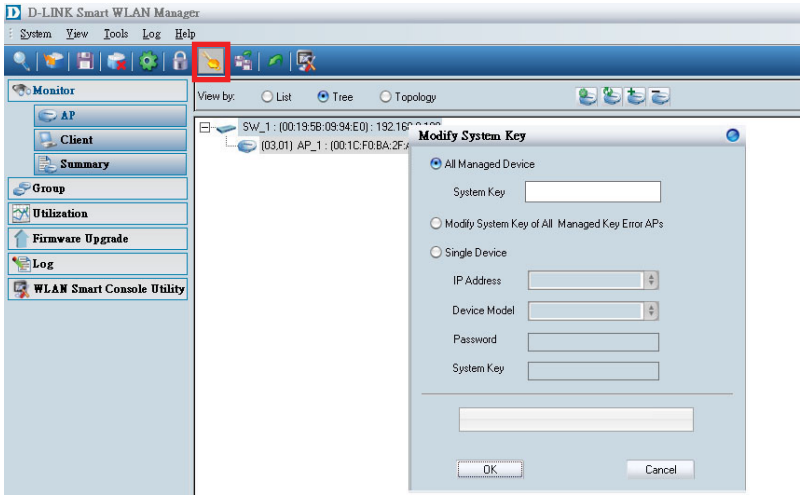


2. Decide which switch and ports will be the wireless port before configuring the Anti-Rogue AP function.

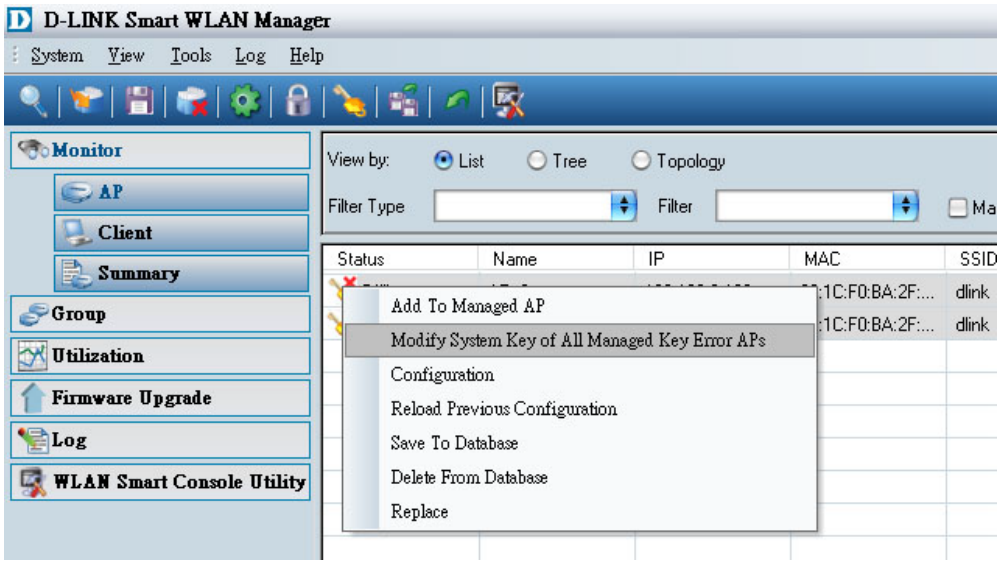
3. Configure the Anti-Rogue function in the “Anti-Rogue” tab. Make the appropriate selections from the “From Port” and the “To Port”. After selecting “Enable” from the Control selection, click the **Apply** button.

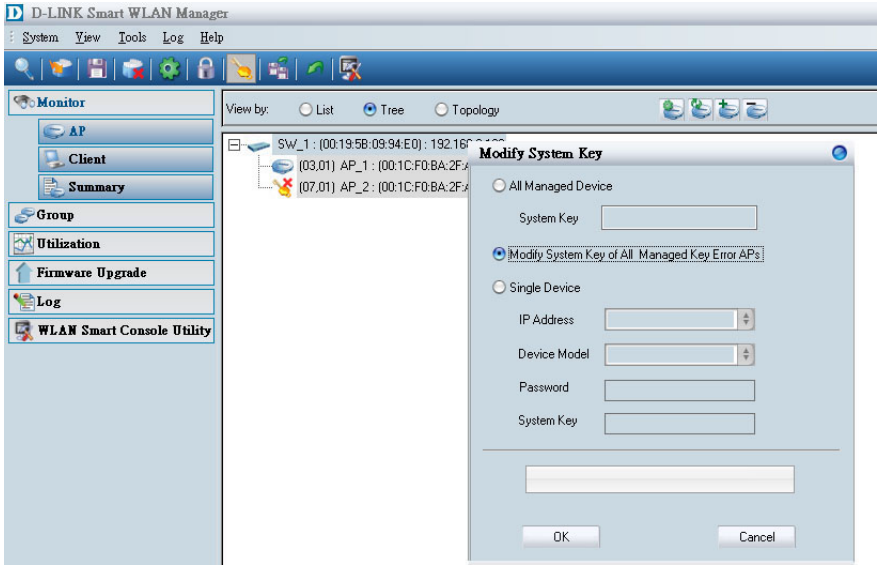


4. Click the “Modify All Device System Key” icon in the standard bar and key to set up the new configuration key. Select “All Managed Device” and input the new system key. Click **OK** to continue.



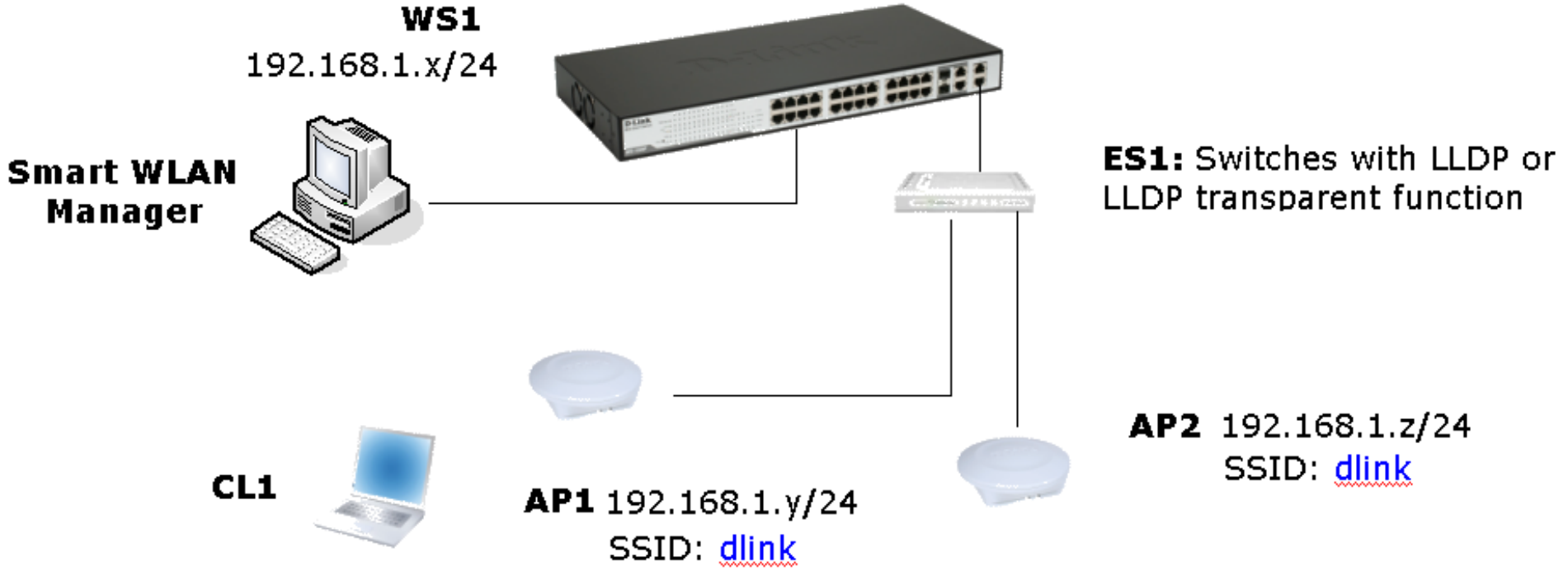
5. If a key error happens on access points, the devices status icon will change in the monitor list. Right-click the device icon and select **Modify System Key of All Managed Key Error APs** or go to the System Key configuration page and select **Modify System Key of All Managed Key Error APs** to change the system key of access points.





Scenario 3 – Connecting AP indirectly to Switch

In some large environments, the DES-1228P does not connect to the DWL-3140AP directly because of the limitation of the environment (Distance, number of AP…). Administrators have to make sure the devices between the switch and APs support the LLDP function or is transparent to the LLDP packet because the Smart WLAN Manager system is communicating to each other by the LLDP and SNMP protocol.



In this kind of topology, Smart WLAN Manager will behave a little differently with normal topology:

1. If either one of the APs under ES1 passed the anti-rogue authentication of the DES-1228P port, the switch port will not authenticate the other APs even if the system key is error.
2. If connecting more than two APs to ES1, the discovered APs will be shown as a replaced AP, not as a new AP.