LevelOne

WHG series

Secure WLAN Controller

Quick Installation Guide

English

Default Settings

IP (Mgmt Access*)	**172.30.0.1**
IP (LAN Access)	**192.168.1.254**
Username	**admin**
Password	**admin**

* Mgmt port is only available on certain models

V1.2

Introducing the LevelOne Secure WLAN Controller is the most advanced yet simple deployment and cost-effective wireless solution. The LevelOne WHG Secure WLAN Controller is an ideal security solution for small to larger-scale WLAN deployments, including airport terminals, campuses, enterprises, hotels and Telco hotspot application. The WHG Secure WLAN Controller integrates “secure access control”, “visitor account provisioning”, “flexible accounting and billing”, and “centralized WLAN management” into one box to provide simplified manageability and instant mobility.

Product Comparison Table

Capacity	WHG-311	WHG-315	WHG-401	WHG-505	WHG-515	WHG-707
Size	13"	19"(1U)	19"(1U)	19"(1U)	19"(1U)	19"(1U)
WAN	2 x GbE	2 x GbE	2 x GbE	2 x GbE	2 x GbE	2 x GbE, 2 x SFP
LAN	8 x GbE	8 x GbE	2 x GbE	2 x GbE	4 x GbE	4 x GbE, 2 x SFP
Management	n/a	n/a	Yes	Yes	Yes	n/a
Account	3000	4000	5000	6000	10000	15000
Managed AP	30	50	150	200	250	500
Monitored IP	100	100	200	200	250	500
Service Zones	9	9	9	9	9	9
User Groups	8	8	16	24	24	24
User Policies	Global + 12	Global +12	Global + 24	Global + 40	Global + 40	Global + 40
Local VPN	80	120	240	500	600	1000
Concurrent User	100	150	300	500	800	1500

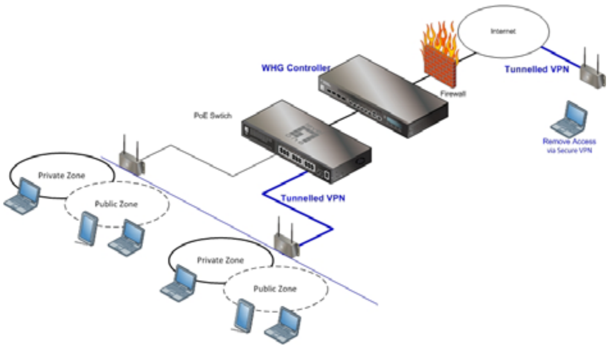
Hardware Installation

Please follow the following steps to install WHG

1. Connect the power to the power socket on the rear panel.
2. The Power LED should be on to indicate a proper connection.
3. Connect an Ethernet cable to the WAN1 Port on the front panel. Connect the other end of the Ethernet cable to a xDSL/cable modem, or a switch/hub of an internal network. The LED of this port should be on to indicate a proper connection.
4. Connect an Ethernet cable to any LAN Port on the front panel. Connect the other end of the Ethernet cable to an administrator PC to configure the WHG system, an AP for extending wireless coverage, a switch for connecting more wired clients, or a client PC. The LED of this LAN port should be on to indicate a proper connection.

Getting Started

The WHG Controller is capable of managing user authentication, authorization and accounting. The user account information is stored in the local database or a specified external database server (AAA Server).
It features an external payment gateway with integrated user authentication, allowing users to easily pay the fee and enjoy the Internet service by using credit cards through Authorize.net, PayPal, SecurePay, or WorldPay.
The WHG introduces the concept of Service Zones - multiple virtual networks, each with its own definable Access Control profiles. This is very useful for hotspot owners to provide different customers or staff with different levels of network services.

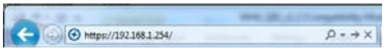


Web Management Interface

The WHG supports web-based configuration. Upon the completion of hardware installation, it can be configured via web browsers with JavaScript enabled such as Internet Explorer version 6.0 and above or Firefox.

1. To access the Web Management Interface, connect a PC to any LAN Port. Make sure you have set DHCP in TCP/IP of your PC to get an IP address automatically. Start your Browser to access the Web Management Interface

2. Enter the gateway IP address of the WHG in the address field of your Browser. The default gateway IP address is https://192.168.1.254 ("https" is used for a secured connection).

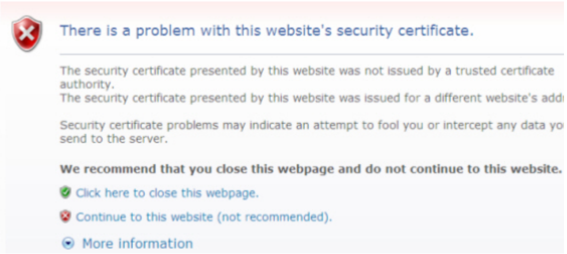


https://192.168.1.254/

3. The administrator login page will appear. Enter "admin" as the default username, and "admin" as the default password in the User Name and Password fields respectively. Click Enter to log in.

4. After a successful login, a System Home page will appear on the screen. From the Home Page, network administrator can navigate to "Setup Wizard", "Quick Links", "System Overview" and "Main Menu".

On first time use, if you connect to the WHG without a **trusted SSL certificate**, the Browser will treat the WHG as an **untrusted** website and throw a "**Certificate Error**". This can be safely ignored. Just press "**Continue to this website**" to continue. The default user login page will then appear in the browser.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's add

Security certificate problems may indicate an attempt to fool you or intercept any data yo send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Note:

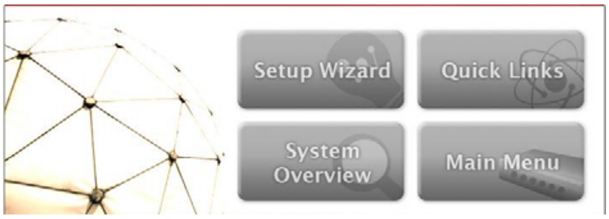
If you can't get to the login screen, the reasons may be:

1) The PC is configured incorrectly so that the PC can't obtain the IP address automatically from the LAN port
2) The IP address and the default gateway are not under the same network segment. In that case configure your PC to have a fixed IP address such as 192.168.1.xxx and try again.

For PC related configuration steps, please consult the WHG User Manual "**PC Network Configuration & User Login**".

Setting Up

WHG provides a **Setup Wizard** for quick configuration. Click on the **Setup Wizard** button to start the configuration process.

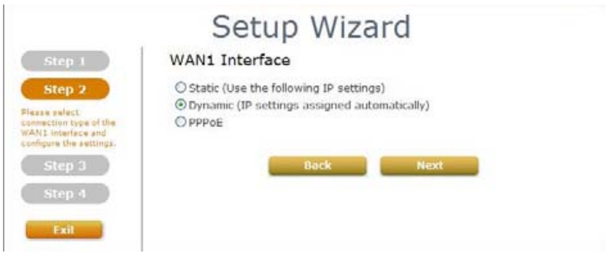


Step 1: General

- Enter a new password in the ***New Password*** field, and re-enter it again in the ***Verify Password*** field (a maximum of 20 characters and no spaces allowed in between).
- Select an appropriate time zone from the ***Time Zone*** drop-down list box to set up the system time.
- Click ***Next*** to continue.

Note

For security concern, it is strongly recommended to change the administrator password



Setup Wizard

Please select connection type of the WAN1 interface and configure the settings.

WAN1 Interface

○ Static (Use the following IP settings)
● Dynamic (IP settings assigned automatically)
○ PPPoE

Step 2: WAN1 Interface

For setting up both wired WAN and wireless LAN functions:

- Select a proper type of Internet connection for WAN1 interface from the following three available connections: **Static**, **Dynamic**, or **PPPoE**. Your ISP or network administrator can advise on the connection type available to you. Above depicts an example for **Dynamic**.
- Click ***Next*** to continue.

Step 3: Local User Account (Optional)

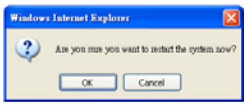
New local accounts can be created and added into the database via this optional function. If local user accounts are not required, click ***Skip*** to go directly to **Step 4**. However, it is recommended to create at least one local user account in order to verify the system's readiness upon completion of this **Setup Wizard**.

- Enter the *Username* (e.g. **"testuser**) and *Password* (e.g. **"testuser"**) to create a new local account.

- Click ***Next*** to continue.
- More local accounts can be added by clicking the ***Back*** button in **Step 4**.

Step 4: Confirm and Restart

- Click ***Finish*** to save current settings and restart the system.
- A confirmation dialog box will then appear. Click ***OK*** to continue.



Windows Internet Explorer

Are you sure you want to restart the system now?

- A **Confirm and Restart** message will appear on the screen during the restarting process. Please do not interrupt the system until the Administrator Login Page appears.

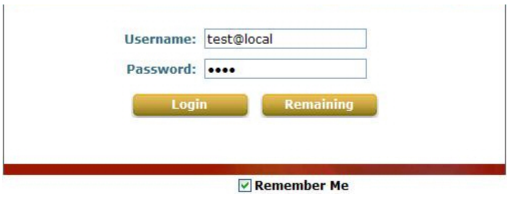
Note:
The system is trying to locate a DNS server at this stage. Therefore, a longer startup time is required if the configured DNS cannot be found.

- When the following Administrator Login Page appears, it means the restart process is now completed.

User Login

To verify whether the configuration of the new local user account(s) created via the Setup Wizard has been completed successfully:

1. Connect a client device (e.g. laptop, PC) to any LAN Port of WHG. The device will obtain an IP address automatically via DHCP.
2. Open a web browser on a client device, access any URL, and then the default User Login Page will appear.
3. Enter the Username and Password of a local user account previously generated via Setup Wizard (e.g. “testuser@local” as the Username and “testuser” as the Password); then Click Login.



Username: test@local

Password: ●●●●

☑ Remember Me

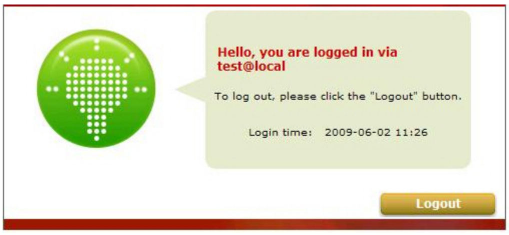
Note:

1. WHG supports multiple authentication options including built-in local user database and external authentication database (e.g. RADIUS). The system will automatically identify which authentication option is used from the full username entered.

2. The format of a full (valid) username is userid@postfix, where “userid” is the user ID and “postfix” is the name of the selected authentication option.
3. Exception: The postfix can be omitted only when the default authentication option is used. For example, “LOCAL” is the default authentication option at this system; therefore, you may enter either “testuser” or “testuser@local” in the Username field.

Congratulations!

The Login Success Page will appear after a client has successfully logged into WHG and has been authenticated by the system.
The appearance of Login Success Page means that WHG has been installed and configured properly.



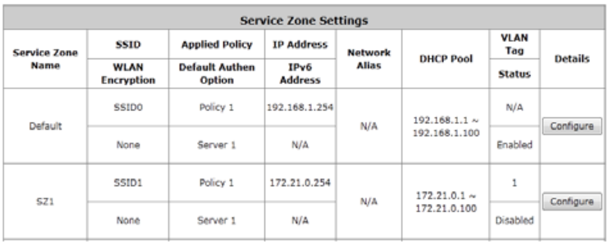
Hello, you are logged in via test@local

To log out, please click the "Logout" button.

Login time: 2009-06-02 11:26

Service Zone

LevelOne Service Zones are virtual machines that has its’ own network interface, DHCP server, authentication configuration, user pages as well as security and user policy settings. By associating a unique VLAN Tag and SSID with a Service Zone, administrators can separate wired network and wireless network into different logical networks isolated from one another. Users attempting to access the resources within the Service Zone will be controlled based on the access control profile of the Service Zone, such as authentication, security feature, wireless encryption method, traffic control, and etc. There are nine Service Zone profiles in total, Default Service Zone and Service Zones 1 ~ 8.

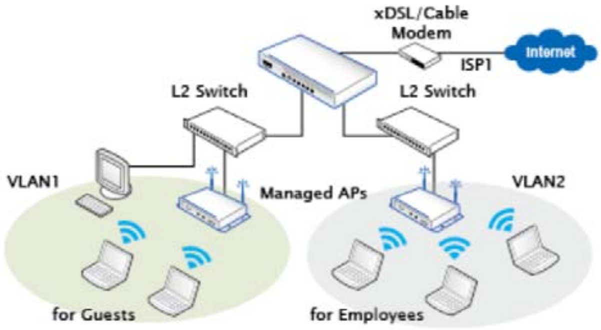


Service Zone Settings

Service Zone Name	SSID WLAN Encryption	Applied Policy Default Authen Option	IP Address IPv6 Address	Network Alias	DHCP Pool	VLAN Tag Status	Details
Default	SSID0	Policy 1	192.168.1.254	N/A	192.168.1.1 ~ 192.168.1.100	N/A	Configure
	None	Server 1	N/A			Enabled	
SZ1	SSID1	Policy 1	172.21.0.254	N/A	172.21.0.1 ~ 172.21.0.100	1	Configure
	None	Server 1	N/A			Disabled	

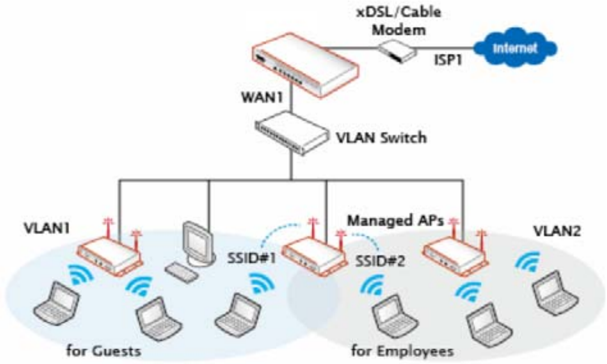
Simple network environment

For most simple internal network, there are just two subnets for example. Using Port-Based model is an easy and better way. In Port-Based mode (configurable in Port Location Mapping tab page), each LAN port can only serve traffic from one Service Zone. An example of network application diagram is shown as below: one Service Zone for Employees and one for Guests.

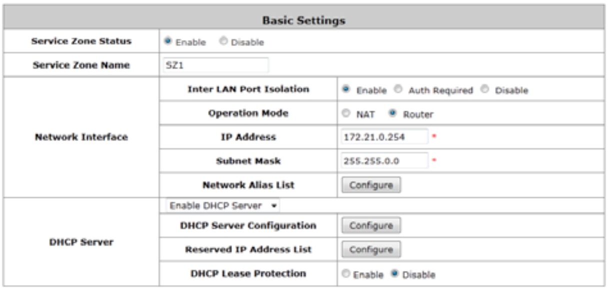


Multiple subnet network environment

On the other hand, if the internal network is a multiple subnets network environment, Tag-Based model will satisfy to your demands. In Tag-Based mode, each LAN port will serve traffics from different Service Zones; a VLAN switch or VLAN AP is required to take care of the VLAN tags carried within the message frames.
An example of network application diagram is shown as below: more than two Service Zones for different departments.



Go to ***System => Service Zones => Service Zone Configuration***



Basic Settings		
Service Zone Status	● Enable ○ Disable	
Service Zone Name	SZ1	
Network Interface	Inter LAN Port Isolation	● Enable ○ Auth Required ○ Disable
	Operation Mode	○ NAT ● Router
	IP Address	172.21.0.254 *
	Subnet Mask	255.255.0.0 *
	Network Alias List	Configure
DHCP Server	Enable DHCP Server ▾	
	DHCP Server Configuration	Configure
	Reserved IP Address List	Configure
	DHCP Lease Protection	○ Enable ● Disable

- Service Zone Status: Each service zone can be enabled or disabled except for the default service zone.
- Service Zone Name: The name of service zone could be input here.
- Network Interface:
  - VLAN Tag (Tag Base Only): The VLAN tag number that is mapped to the Service Zone.
  - Inter LAN Port Isolation (Port Base Only): Select Enable, Auth Required or Disable. When the
  - When the option is “Enabled”, clients under different LAN ports cannot ping each other. When the option is “Disabled”, clients under different LAN ports can ping each other. When the option is “Auth Required”, clients under different LAN ports cannot ping each other unless both of them has successfully authenticated.
  - Operation Mode: Contains NAT mode and Router mode. When NAT mode is chosen, service zone
  - When the NAT mode is chosen, Service Zone runs in NAT mode. When Router mode is chosen, Service Zone runs in Router mode.
  - IP Address: The IP Address of this service zone.
  - Subnet Mask: The subnet Mask of this service zone.
  - IPv6 Settings: The IPv6 Address and configuration of this service zone (when IPv6 is enabled).
  - Network Alias List: Administrator may optionally set many alias network segments for a service zone. This feature can allow a single service zone to be seen as many service zones.

Additional to hide the IP address of a Service Zone’s network interface and to some degree, provide protection from possible attacks from LAN clients.

- DHCP Server: From the drop down menu, DHCP server for this particular service zone may be Disabled, Enabled or Relayed.

Please note that when “Enable DHCP Relay” is enabled, fill in the IP address of the external DHCP Server, and the IP address of clients will be assigned by an external DHCP server. The system will only relay DHCP information from the external DHCP server to downstream clients of this service zone. Please note that Controller should be in the same subnet as the DHCP server.

Note:
For the set up of **AP Management**, please refer to the User Manual.