

EnGenius®

The Neutron Series

User Manual



EWS1025CAM
version 1.0

2-Megapixel Wireless Cloud Managed Mesh Camera

Table of Contents

Chapter 1 Product Overview	6
Key Features	7
Introduction.....	8
System Requirements.....	9
Package Contents	9
Applications	10
Technical Specifications	11
Physical Interface.....	12
Chapter 2 Before You Begin	14
Considerations for Wireless Installation	15
Computer Settings.....	16
Hardware Installation.....	20
Mounting the Access Point	21
Chapter 3 Configuring Your Access Point.....	24
Default Settings.....	25
Web Configuration	26
Chapter 4 User Interface.....	30
Navigation Panel.....	31
Live View Management.....	33
Chapter 5 Access Point Settings.....	36
Device Status.....	37
Connections.....	40
Realtime	41
Chapter 6 Network.....	43
IPv4 Settings	44

Spanning Tree Settings.....	45
Chapter 7 Wireless	46
System Properties.....	47
Operation mode.....	48
2.4GHz/5GHz SSID Profile.....	51
Wireless Security	53
Wireless MAC Filter	56
Traffic Shaping.....	57
Fast Roaming	58
WDS Link Settings	59
Guest Network	61
RSSI Threshold	63
Management VLAN Settings.....	64
Chapter 8 DDNS	65
Chapter 9 UPnP	68
Chapter 10 Service Port	70
Chapter 11 Mesh	72
Status.....	73
Settings.....	74
Tools.....	75
Node List.....	75
Link Status	77
Ping	77
Trace Route	78
Throughput.....	78
Chapter 12 Management.....	79
Controller Settings	80

SNMP Settings.....	80
CLI/SSH Settings.....	83
HTTPS Settings.....	84
Email Alert	85
Date and Time Settings	86
WiFi Scheduler.....	87
Tools.....	89
LED Control.....	93
Device Discovery.....	94
Chapter 13 System Manager	95
Account Setting.....	96
Firmware Upgrade	98
Backup/Restore	99
Reset/Reboot	101
System Log	101
Chapter 14 Camera OverView	103
Camera Status	104
PC Storage Path	105
Chapter 15 Media	106
Video	107
Camera	108
Advance	115
Privacy Mask.....	117
Audio.....	118
Chapter 16 Event Management	119
Event Control	120
Motion Detection	123

Audio Detection	126
Tampering Detection.....	127
Event Action.....	128
Chapter 17 Event Server.....	130
Network Storage	131
FTP(File Transfer Protocol).....	134
E-Mail	135
Chapter 17 Storage Info.....	136
Storage Info.....	137
Appendix	139
Appendix A - FCC Interference Statement	140
Appendix B - CE Interference Statement.....	142

Chapter 1 **Product Overview**



Introduction

Key Features



- Deploy and manage with ease using EWS Series Wireless Management Switches.
- Advance Access Point mode with mesh network support.
- Dual Concurrent 2.4GHz and 5GHz architecture with max transfer rates of up to 300+867 Mbps.
- Internal 5dBi Omni-Directional MIMO antennas optimized for maximum RF performance.
- Backward compatible with IEEE802.11a/b/g/n wireless devices.
- Integrated Power over Ethernet (IEEE802.3af) for lowering deploying costs. Can be powered using either the included power adapter or via PoE with PoE 802.3af capable Switches or Injectors.
- Band Steering to load balance clients between 2.4GHz and 5 GHz for better throughput performance.
- Secure Guest Network option available.
- Stylish low profile design with easy ceiling mounting kit.
- Full HD Sony CMOS image sensor delivers 30fps in 1080P resolution.
- Provide true day/night functionality with 20 meter IR LEDs illuminator and IR cut filter.
- H.264 high compression video with VLAN and prioritizing QoS for delivering easily.
- EnGenius DDNS, P2P and Push Notification.
- Free iOS & Android APP for view / record.
- Free bundle Video Management Software.
- ONVIF compatible (Profile S).

Introduction

EnGenius Indoor Mesh Access Point Camera is a new concept of dual band concurrent, high power, high sensitivity and strong reliability for enterprise solutions. Easy setup and installation for combination of two products – Access point and IP camera, one PoE or DC power solve the power input, and single UI interface for all configurations. To integrate the hotspot service and surveillance, EWS1025CAM not only wireless mesh access point extends wireless access over large, metro scale areas, eliminates costly Ethernet cabling to every Wi-Fi access point, but also provides high resolution video streaming for security. It can be easily deployed and maintained with no configuration deployment and recovery capacity. Extended signal range from high-gain antenna arrays reduce the number of mesh nodes typically required. The EWS1025CAM is a component of the EWS Neutron Series Switches, delivering a robust wireless network with maximum capacity and uptime, the wireless mesh can be seamlessly deployed as an extension of wired and wireless networks, with central management through controllers. No IT experts required for installation, system automatically determines the optimal network topology and maintains the best connections between mesh nodes. The centralize functions of the wireless LAN to provide scalable management, advanced security, seamless mobility, and proven reliability.

This device is an enhanced-powered, long-range wireless access point. It is designed to operate in numerous environments; from large homes, small and medium-sized businesses, multiple-floor offices, hotels, and other venues, to larger enterprise deployments. Its enhanced-powered, long-range characteristics make it a cost-effective alternative to ordinary Access Points that don't have the range and reach to connect to a growing number of wireless users who wish to connect to a large hotspot or business network.

To protect sensitive data during wireless transmissions, the device offers different encryption settings for wireless transmissions, including industry standard WPA and WPA2 encryption. The device also includes MAC address filtering to allow network administrators to offer network access only to known computers and other devices based on their MAC addresses.

Maximum data rates are based on IEEE 802.11 standards. Actual throughput and range may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment, and mix of devices in the network. Features and specifications are subjected to change without prior notice. Trademarks and registered trademarks are the property of their respective owners. For United States of America: Copyright © 2016 EnGenius Technologies, Inc. All rights reserved.

System Requirements

The following are the Minimum System Requirements in order to configure the device:

- Computer with an Ethernet interface or wireless network capability
- Windows OS (XP, Vista, 7, 10), Mac OS, or Linux-based operating systems
- Web-Browsing Application (i.e. : Internet Explorer, Firefox, Safari, or another similar browser application)

Package Contents

The package contains the following items (all items must be in package to issue a refund):

- EWS1025CAM Managed Indoor Mesh Camera
- Power Adapter
- RJ-45 Ethernet Cable
- Quick Installation Guide
- Mounting Bracket
- Mount Screw kit

Applications

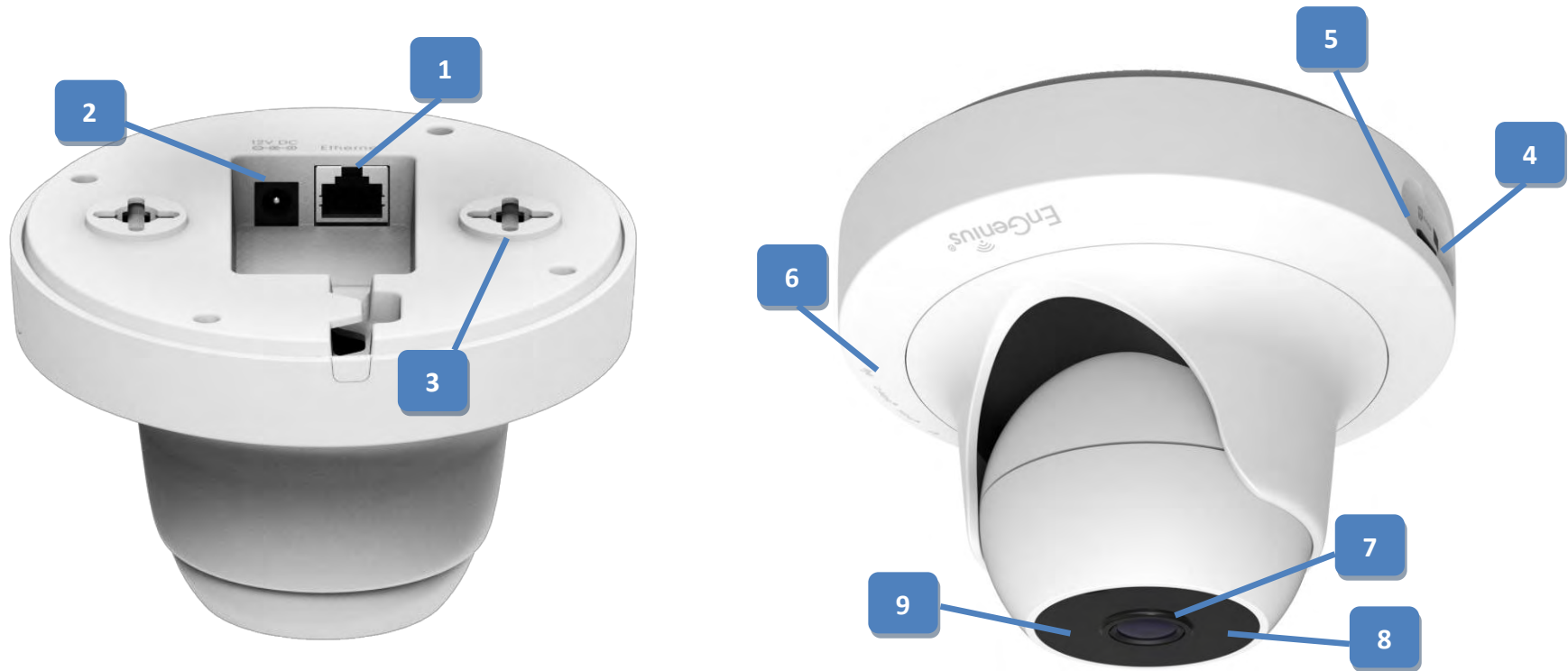
Wireless LAN (WLAN) products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of WLANs:

- **Difficult-to-Wire Environments:** There are many situations where wires cannot be installed, deployed easily, or cannot be hidden from view. Older buildings, sites with multiple buildings, and/or areas that make the installation of a Ethernet-based LAN impossible, impractical or expensive are sites where WLAN can be a network solution.
- **Temporary Workgroups:** Create temporary workgroups/networks in more open areas within a building; auditoriums, amphitheaters classrooms, ballrooms, arenas, exhibition centers, or temporary offices where one wants either a permanent or temporary Wireless LAN established.
- **The Ability to Access Real-Time Information:** Doctors/Nurses, Point-of-Sale Employees, and/or Warehouse Workers can access real-time information while dealing with patients, serving customers, and/or processing information.
- **Frequently Changing Environments:** Set up networks in environments that change frequently (i.e.: Show Rooms, Exhibits, etc.).
- **Small Office and Home Office (SOHO) Networks:** SOHO users require a cost-effective, easy, and quick installation of a small network.
- **Training/Educational Facilities:** Training sites at corporations or students at universities use wireless connectivity to exchange information between peers and easily access information for learning purposes.

Technical Specifications

		EWS1025CAM
Standard	2.4GHz	IEEE802.11b/g/n
	5GHz	IEEE802.11a/n/ac
Antennas		4 x Internal 5dBi Omni-Directional
Image Sensor		Sony 2Megapixel 1920 x1080 Progressive Scan COMS sensor
Lens		Fixed Board Lens, f =2.8mm/F2.0, F.O.V=120 Degree(Diagonal)
IR illuminator		20 Meter Range
Interface		1 x 10/100/1000 Gigabit Ethernet Port 1 x Reset Button 1 x Power Connector 1 x Micro SDXC card slot
LED Indicator		5GHz, 2.4GHz, Power, LAN, Mesh
PoE Support		IEEE802.3af
Power Requirement		External Power Adapter DC IN, 12V/1.5A
Environment		Operating: Temperature: 32°F to 122°F (0°C to 40°C) Humidity (Non-condensing): 90% or less Storage: Temperature: -4°F to 140°F (-20°C to 60°C) Humidity (Non-condensing): 90% or less
Dimensions		5.24 x 3.82 in./134 x 97mm
Weight		1.05lbs/478g

Physical Interface



1. LAN Port (802.3af PoE): Ethernet port for RJ-45 cable.
2. Power Connector: 12V DC IN for Power Adapter.
3. Ceiling Mount Hole: Using the provided mounting kit, the Access Point can be attached to a ceiling or wall.
4. Micro SD card slot: Supported SDXC card for local storage.
5. Reset Button: Press and hold for over 10 seconds to reset to factory default settings.
6. LED Indicators: LED lights for Mesh, WLAN 5GHz, WLAN 2.4GHz, LAN, and Power.
7. Lens: 2 Megapixel wind angle fixed board lens.
8. Built-in Microphone: One way audio for recording.

9. IR illuminator: 20 meter infrared for low lux environment.

RISK GROUP 1

WARNING IR emitted from this product. Do not stare at operating lamp.

Chapter 2 **Before You Begin**



Before You Begin

This section will guide you through the installation process. Placement of the EnGenius Access Point is essential to maximize the Access Point's performance. Avoid placing the Access Point in an enclosed space such as a closet, cabinet, or stairwell.

Considerations for Wireless Installation

The operating distance of all wireless devices can often not be pre-determined due to a number of unknown obstacles in the environment in which the device is deployed. Obstacles such as the number, thickness, and location of walls, ceilings, or other objects that the Access Point's wireless signals must pass through can weaken the signal. Here are some key guidelines for allowing the Access Point to have an optimal wireless range during setup.

- Keep the number of walls and/or ceilings between the Access Point and other network devices to a minimum. Each wall and/or ceiling can reduce the signal strength, resulting in a lower overall signal strength.
- Building materials make a difference. A solid metal door and/or aluminum studs may have a significant negative effect on the signal strength of the Access Point. Locate your wireless devices carefully so the signal can pass through drywall and/or open doorways. Materials such as glass, steel, metal, concrete, water (example: fish tanks), mirrors, file cabinets, and/or brick can also diminish wireless signal strength.
- Interference from your other electrical devices and/or appliances that generate RF noise can also diminish the Access Point's signal strength. The most common types of devices are microwaves or cordless phones.

Computer Settings

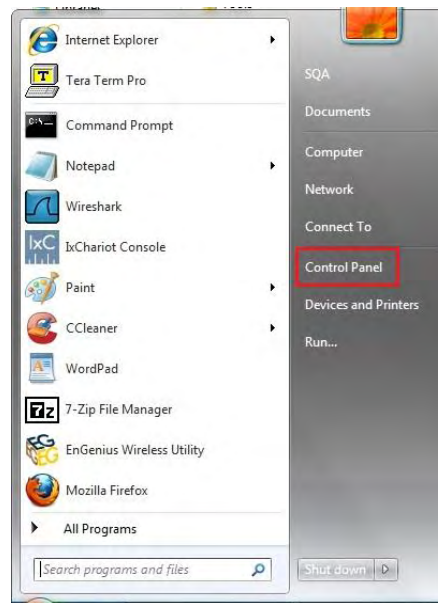
Windows XP/Windows 7

In order to use the Access Point, you must first configure the TCP/IPv4 connection of your Windows OS computer system.

1. Click the **Start** button and open the **Control Panel**.



Windows XP

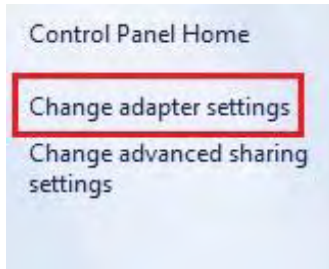


Windows 7

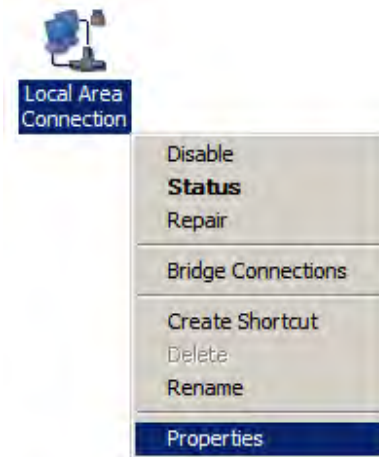
2a. In **Windows XP**, click on Network Connections.



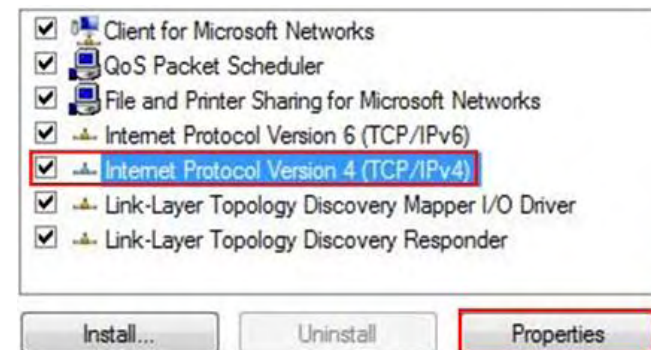
2b. In **Windows 7**, click **View network status and tasks** in the **Network and Internet** section, then select **Change adapter settings**.



3. Right click on **Local Area Connection** and select **Properties**.



4. Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



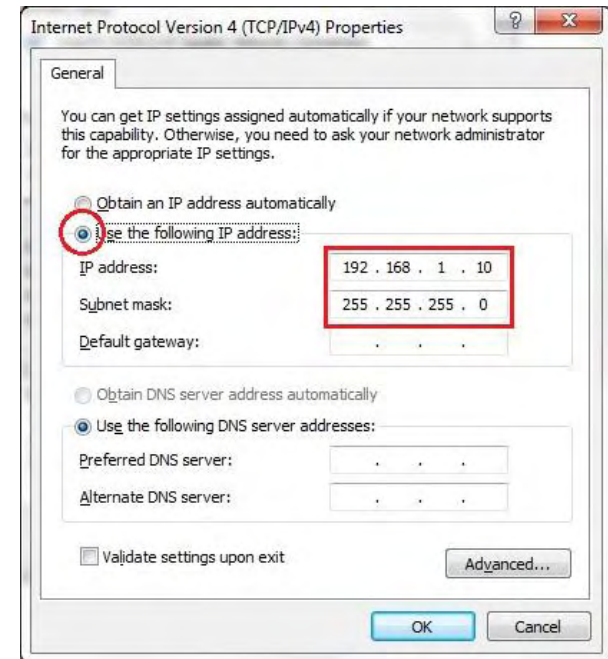
5. Select **Use the following IP address** and enter an IP address that is different from the Access Point and Subnet mask, then click **OK**.

Note: Ensure that the IP address and Subnet mask are on the same subnet as the device.

For example: EWS1025CAM IP address: 192.168.1.1

PC IP address: 192.168.1.2 - 192.168.1.255

PC Subnet mask: 255.255.255.0

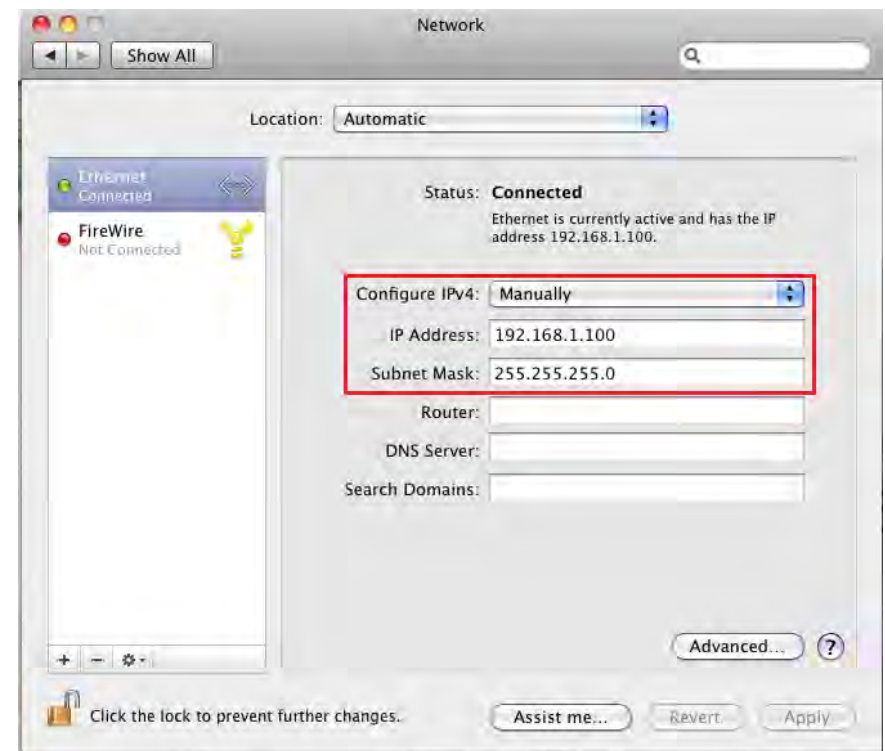


Apple Mac OS X

1. Go to **System Preferences** (it can be opened in the **Applications** folder or by selecting it in the Apple Menu).
2. Select **Network** in the **Internet & Network** section.

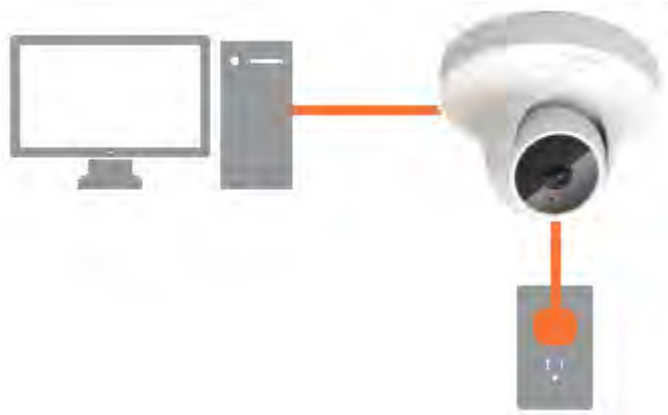


3. Highlight **Ethernet**.
4. In **Configure IPv4**, select **Manually**.
5. Enter an IP address that is different from the Access Point and Subnet mask, then click **OK**.
Note: Ensure that the IP address and Subnet mask are on the same subnet as the device.
For example: EWS1025CAM IP address: 192.168.1.1
PC IP address: 192.168.1.2 - 192.168.1.255
PC Subnet mask: 255.255.255.0
6. Click **Apply** when finished.



Hardware Installation

1. Ensure that the computer in use has an Ethernet Controller port (RJ-45 Ethernet Port). For more information, verify with your computer's user manual.
2. Connect one end of the Category 5e Ethernet cable into the RJ-45 port of the Access Point and the other end to the RJ-45 port of the computer. Ensure that the cable is securely connected to both the Access Point and the computer.
3. Connect the Power Adapter DC connector to the DC-IN port of the Access Point and the Power Adapter to an available electrical outlet. Once both connections are secure, verify the following:
 - a) Ensure that the **POWER** light is on (it will be **orange**).
 - b) Ensure that the 2.4 GHz/5 GHz WLAN light is on (it will be **blue** for 2.4G, and **green** for 5G).
 - c) Ensure that the LAN (Computer/ Access Point Connection) light is on (it will be **blue**).
 - d) Once all three lights are on, proceed to set up the Access Point using the computer.



Mounting the Access Point

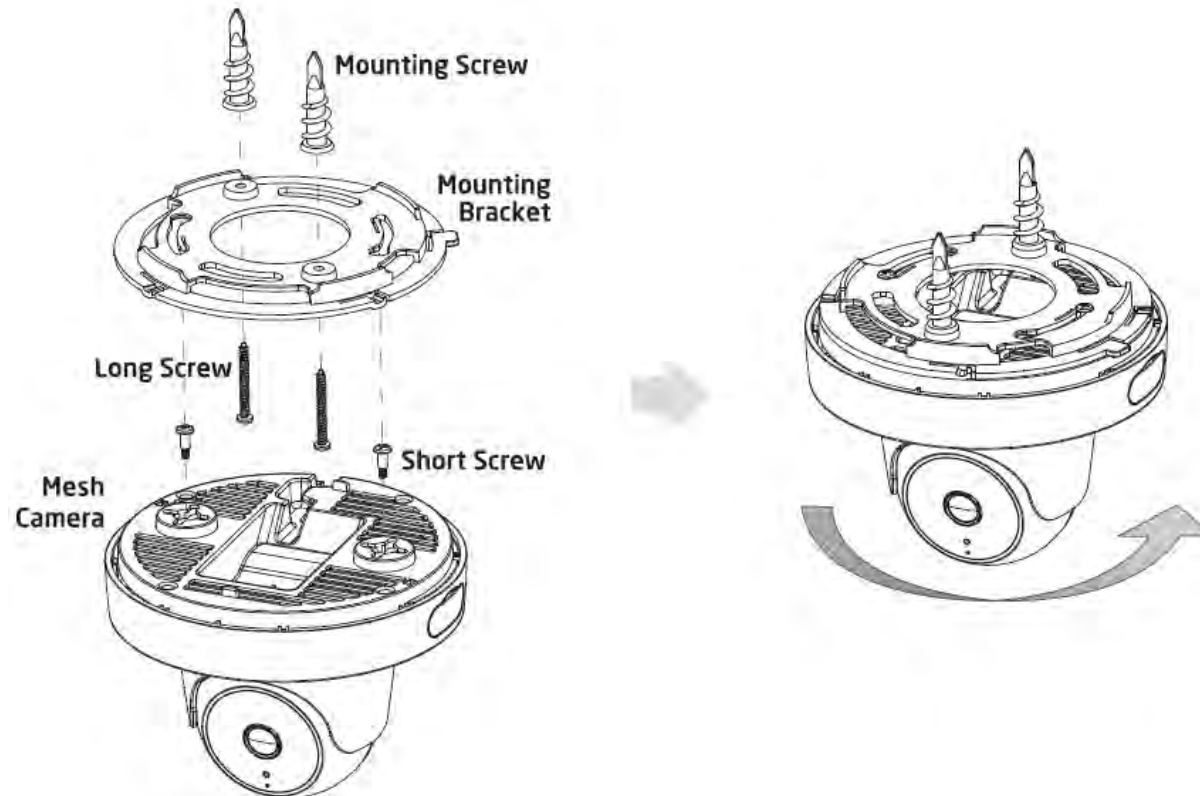
Using the provided hardware, the Access Point can be attached to a ceiling or wall.

To attach the Access Point to a ceiling or wall using the mounting bracket:

1. Attach the mounting bracket to the wall or ceiling using the provided wall/ceiling mounting hardware kit.
2. Insert the provided short screws into the bottom cover of the Access Point.

Leave enough of the screws exposed to ensure that the unit can be attached to the mounting bracket.

If extra space is required, use the provided spacers and long screws from the T-Rail mounting hardware kit to increase the space between the unit and the mounting bracket.

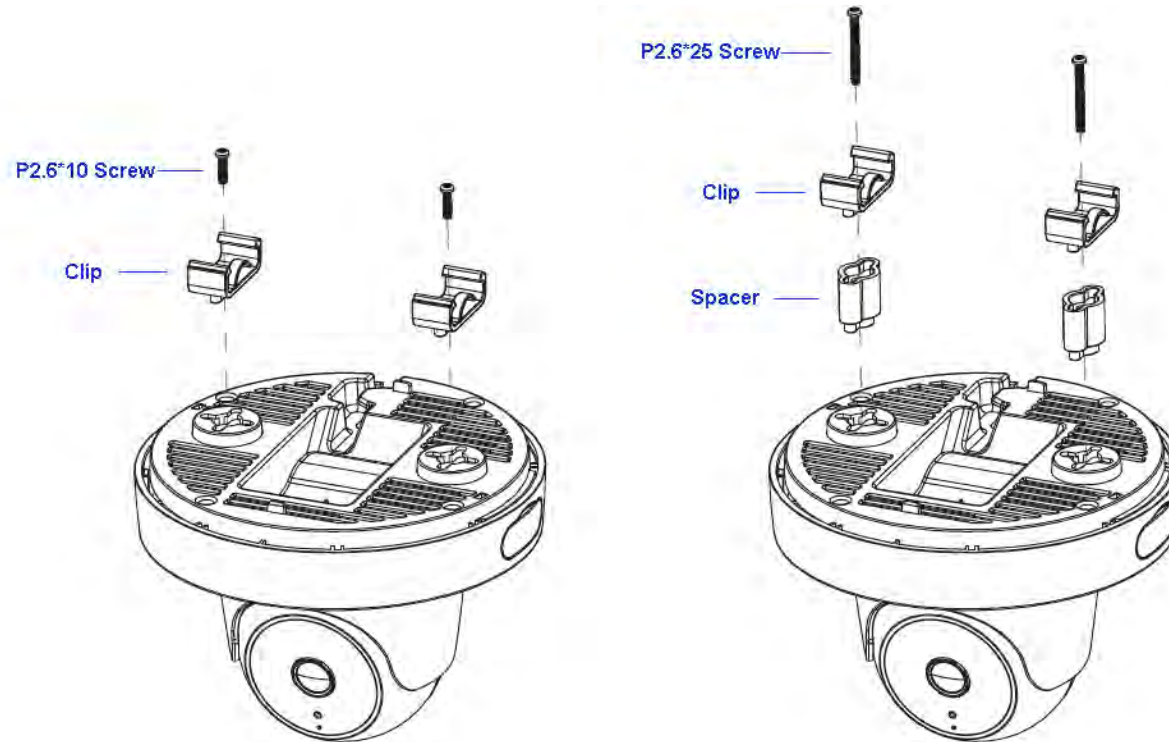


3. Mount the Access Point on the mounting bracket by rotating the unit clockwise about 90 degrees to secure it in place.

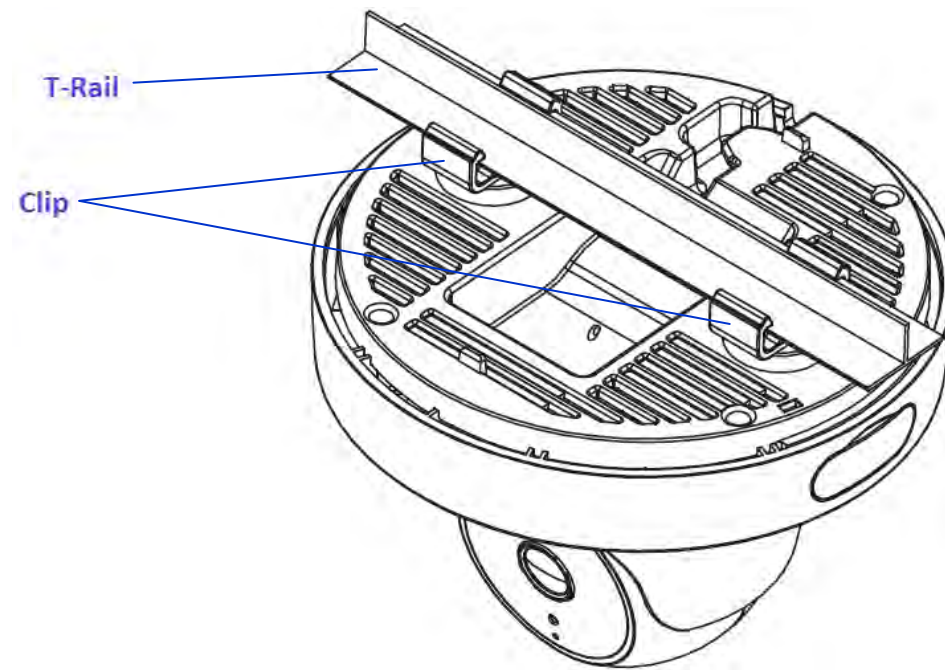
Attaching the Access Point to a ceiling using the provided T-Rail connectors:

1. Attach the T-Rail connectors to the bottom cover of the Access Point using the provided short screws.

Note: Two sizes of T-Rail connectors are included in the mounting hardware kit: 15/16in (2.38cm) and 9/16in (1.43cm). If extra space is required to accommodate drop ceiling tiles, use the provided spacers and long screws.



2. Line up the connected T-Rail connectors with an appropriately sized rail and press the unit onto the rail until it snaps into place.



Chapter 3 **Configuring Your Access Point**



Configuring Your Access Point

This section will show you how to configure the device using the web-based configuration interface.

Default Settings

Please use your Ethernet port or wireless network adapter to connect the Access Point.

IP Address	192.168.1.1/192.168.1.1200
Username/Password	admin/admin

Web Configuration

1. Open a web browser (Internet Explorer/Firefox/Safari) and enter the IP Address <http://192.168.1.1>.



Note: If you have changed the default LAN IP Address of the Access Point, ensure you enter the correct IP Address.

2. The default username and password are: **admin**. Once you have entered the correct username and password, click the **Login** button to open the web-based configuration page.



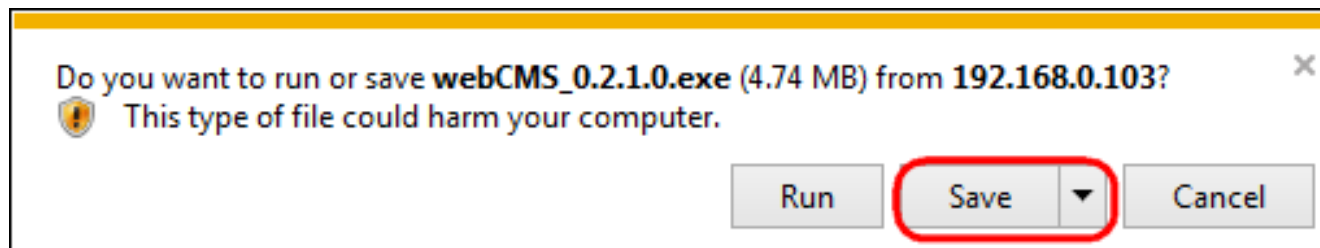
3. For the first time of login, you will be informed to download and install "WebCMS". Please click on "Download WebCMS" to start download (you will be required to have Internet connection on your router). WebCMS enables browsers to support camera feature. Don't worry if you are prompted with a different version number because the software upgrades from time to time.

WebCMS 0.2.3.0

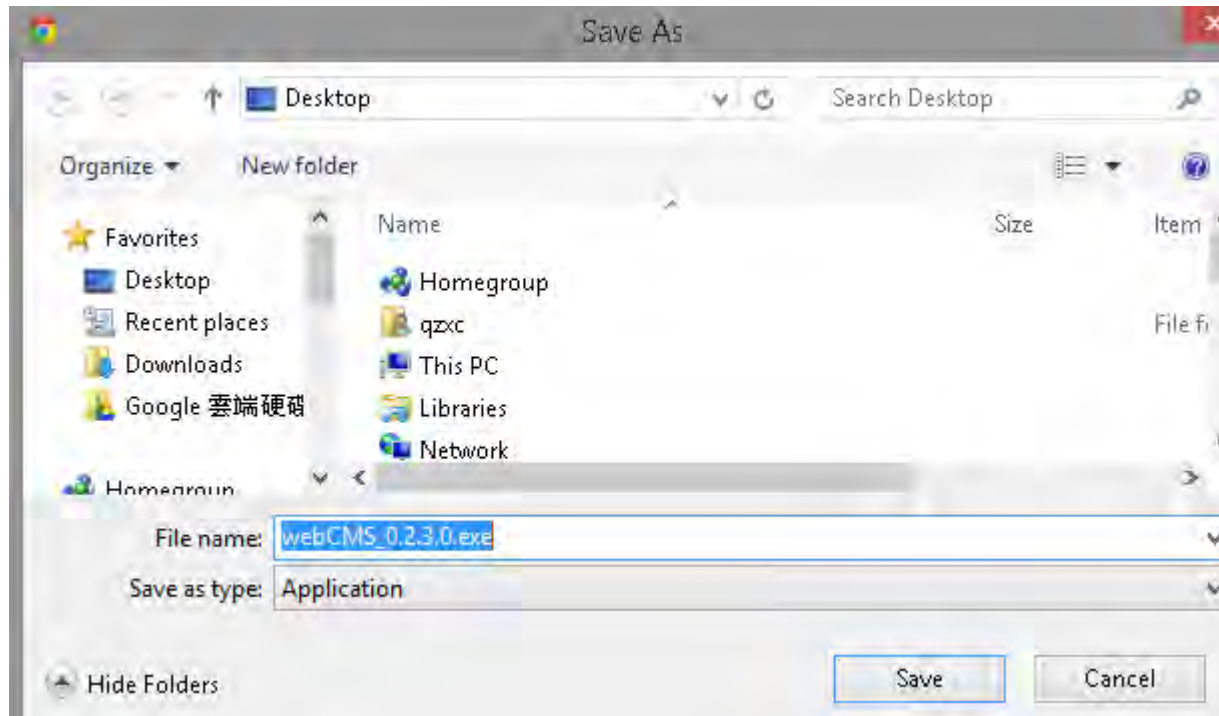
Installation of IP Camera "WebCMS" plug-in control requires your attention.
You need to download the latest "WebCMS" plug-in and install to continue view
camera web user interface.

Download WebCMS

If prompted with the following question, click on Save (**Internet Explorer**).



Save the downloaded file.



Once download is completed, you **MUST close all the browsers** before install WebCMS.

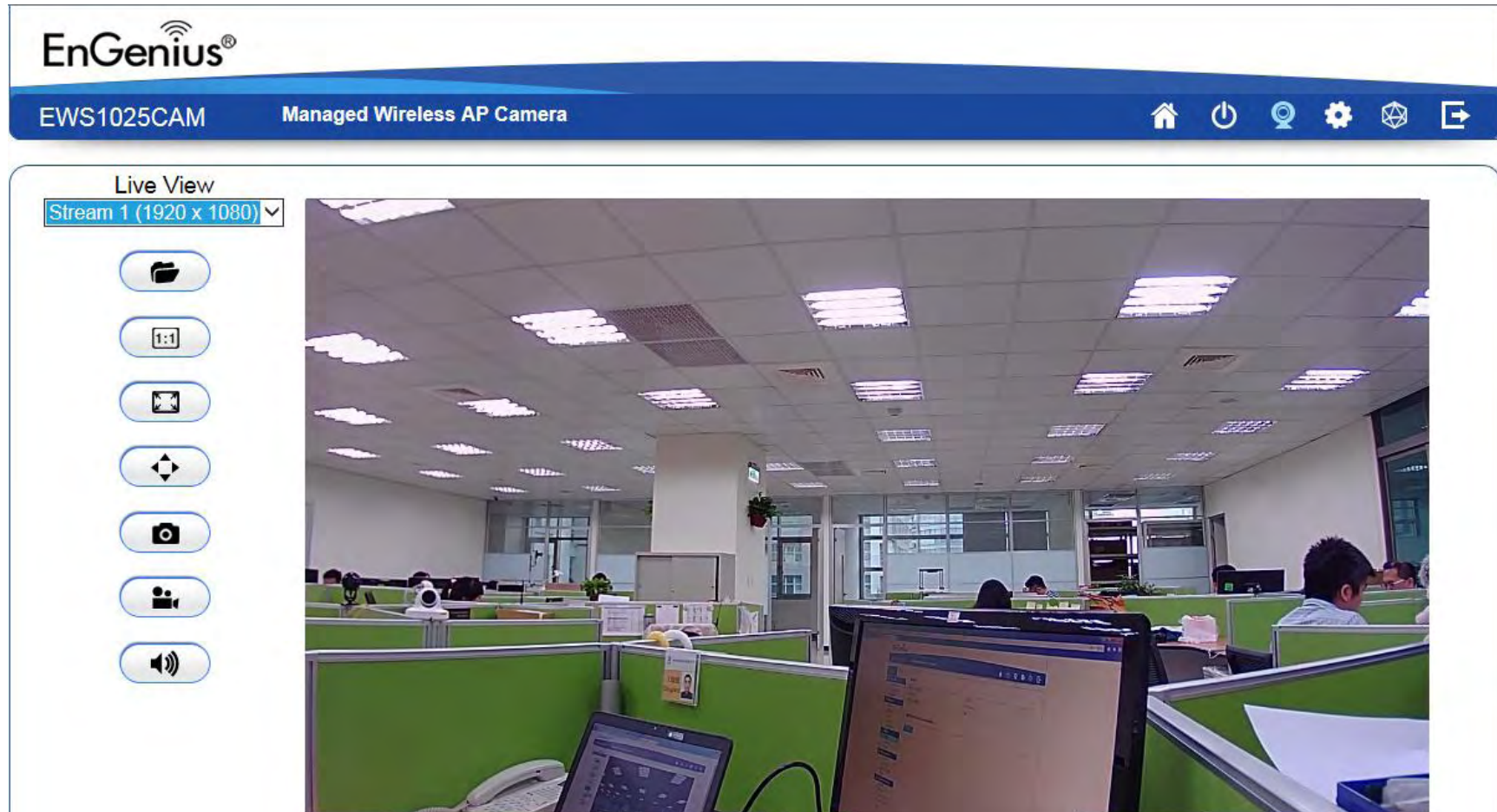


Double click on **WebCMS** to install the program. You may not have noticed, the installation is very fast, it only takes a few seconds for **WebCMS** to be installed.

When installation is completed, open the browser and login into the camera again. You should be able to see the camera viewer in live as shown below. If you do not see the viewer that means you did not install **WebCMS** properly or try login using other browsers.

NOTE: If you are seeing grey color in the viewer, it is because the camera has detected insufficient of light in the room and enabled night vision mode automatically. If you point your camera to a brighter area, you should be able to see it switched to normal color mode. Try a few places to get a feeling on how it works. If listening closely, you may hear the click sound from the camera when night vision is switched on and off.

4. If successful, you will be logged in and see the Access Point User Interface.



Chapter 4 **User Interface**



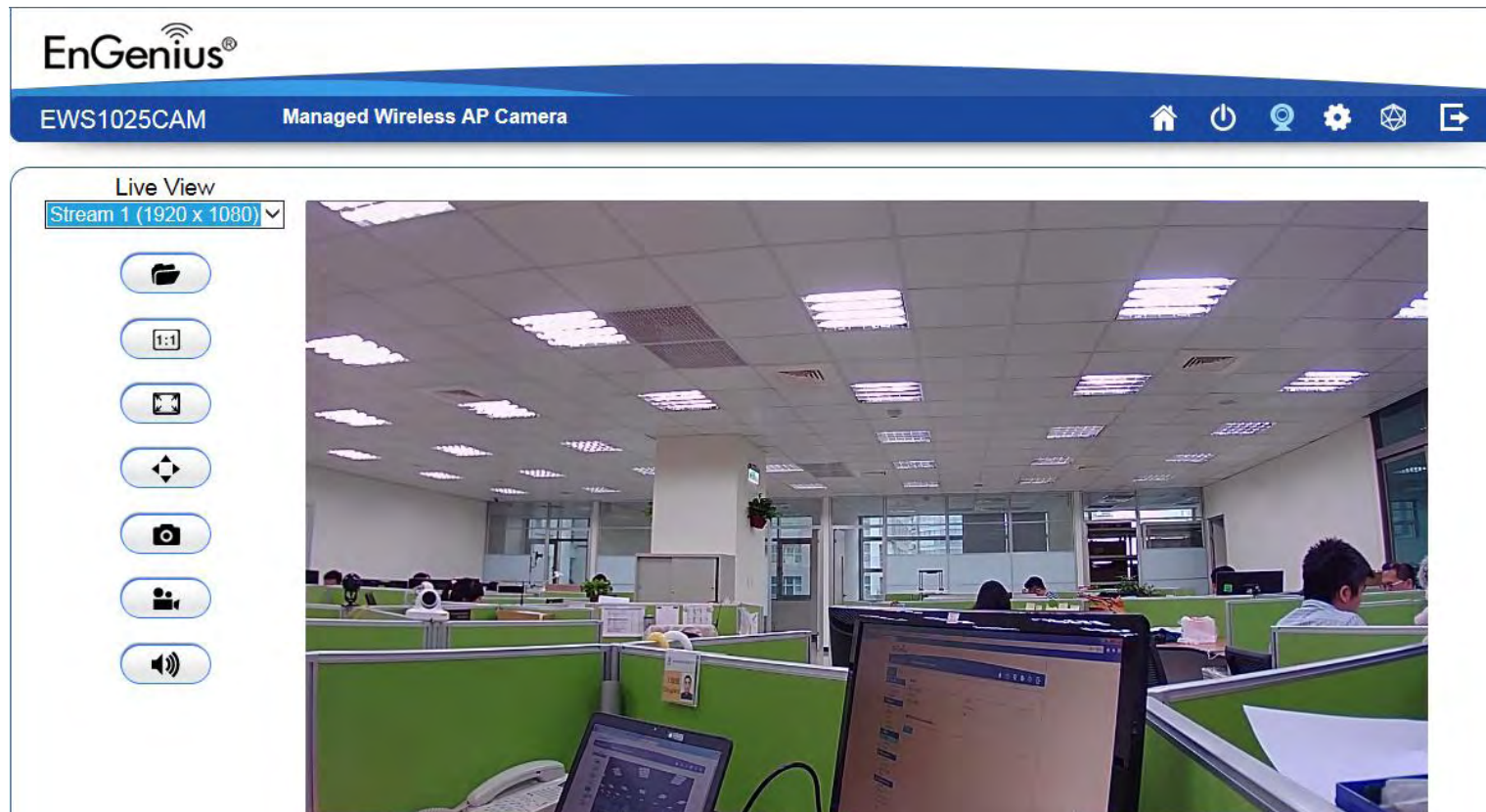
User Interface

The **User Interface** section contains the following options:

- Navigation Panel
- Live View Management

The following sections describe these options.

Navigation Panel



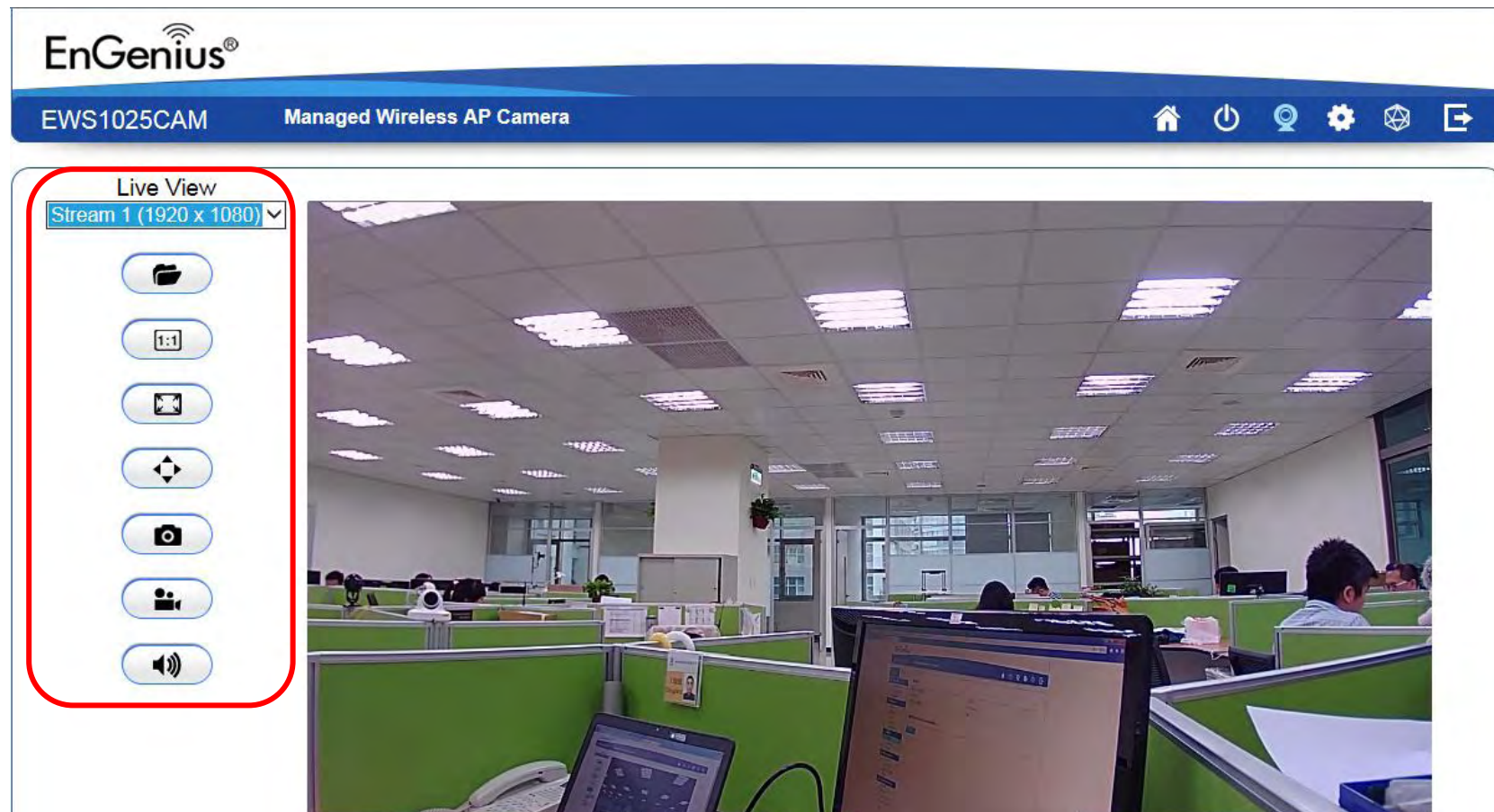
The **Navigation Panel** is located at the top-right corner of the page.



The descriptions are as follows:

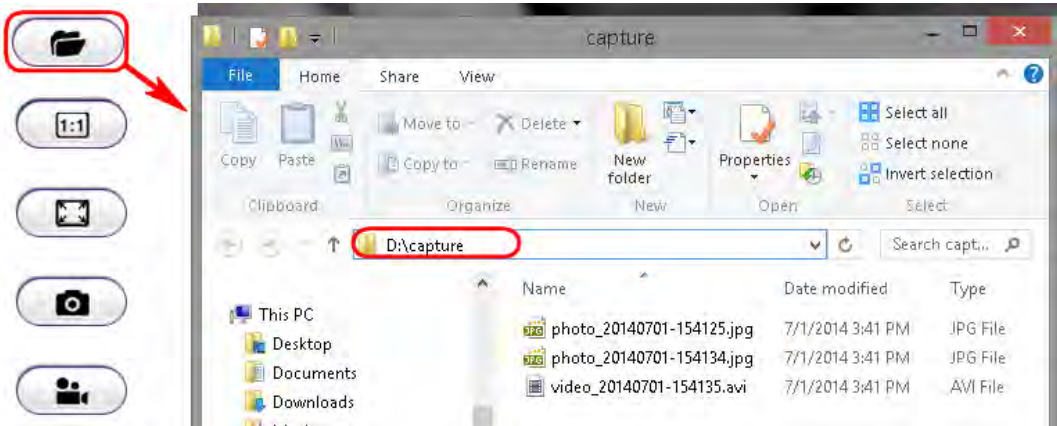
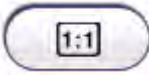
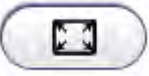
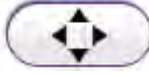
	Navigate to home page for device information and connection status
	Navigate to Reboot/Reset device page
	Navigate to camera live view page
	Navigate to the main setting page
	Navigate to the Mesh tools page
	Logout

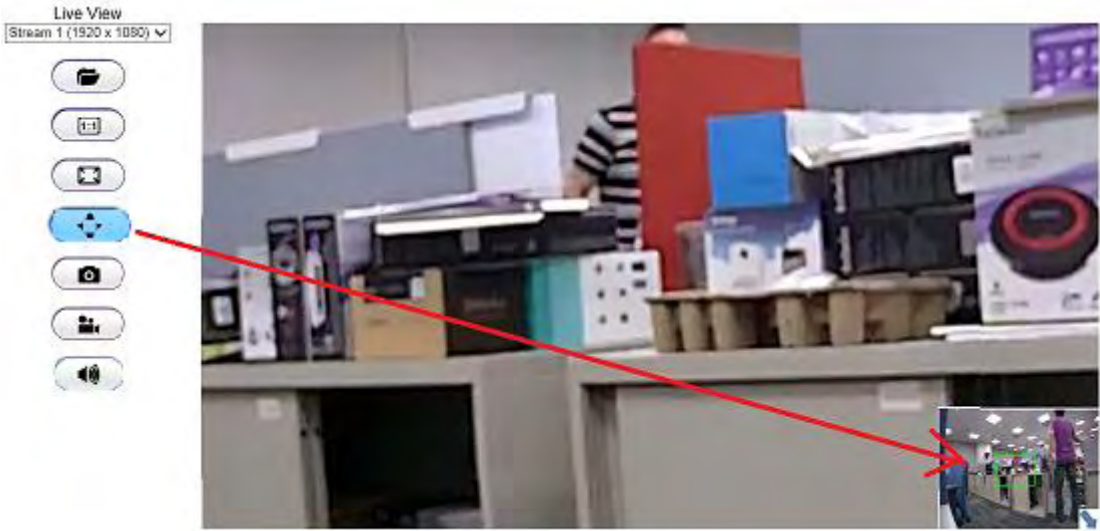
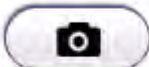
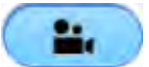
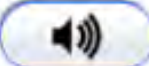
Live View Management



The **Live View Management** menu is located at the right side of the page.

Live View Stream 1 (1920 x 1080) Stream 2 (640 x 360)	There are two streams running concurrently: Stream1 (1920x1080) and Stream2 (640x360). Stream1 has the higher resolution than stream2. Stream2 serves lower resolution for mobile devices which has smaller screens. You can preview each stream at real time by selecting it from the list.
	This opens the local folder where the real time captured images and clips are stored. You may change the folder path at Main Menu → System → PC Storage Path

	
	This switch only applies to resolution 640 x 360. When enabled, the preview image will switched to 1:1 mode. By default the image will expand and fill the view screen if the actual image is smaller than the view. 
	This switch will hide the browser and expand the view to full screen. You can press ESC button to cancel the full screen mode.
	ePTZ display the digital zoom in for the region of interest, use your mouse to move the green window at the left bottom to the area you intend to monitor.

	 The screenshot shows a 'Live View' window with a toolbar on the left. The toolbar includes icons for: a folder (save), a 1:1 aspect ratio, a camera (snapshot), a video camera (recording), a speaker (audio), and a four-way arrow (pan/zoom). The pan/zoom icon is highlighted in blue. A red arrow points from this icon to a small inset video in the bottom right corner of the main video frame, which shows a wider view of the scene.
	This button takes a snap-shot on the real time view and store the image in the local folder.
	Toggle this button to start recording movie clip at real time. Click on the button to start recording. Please note that when icon changed to blue  icon the camera is recording. To stop recording, simply click the button again.
	Toggle this button to turn PC audio from the camera ON and OFF. The default is ON, click the button to turn it ON; the icon should change to  to signify OFF state.

Chapter 5 **Access Point Settings**



Overview

The **Overview** section contains the following options:

- Device Status
- Connections
- Real Time

The following sections describe these options.

Device Status

Clicking the **Device Status** link under the **Overview** menu shows the status information about the current operating mode.

- The **Device Information** section shows general system information such as Device Name, MAC address, Current Time, Firmware Version, and Management VLAN ID

Device Information

Device Name	EWS1025CAM-desk
MAC Address	
- LAN	88:DC:96:26:13:88
- Wireless LAN - 2.4GHz	88:DC:96:26:13:8A
- Wireless LAN - 5GHz	88:DC:96:26:13:8B
Country	USA
Current Local Time	Mon Jul 25 09:18:40 2016
Uptime	6h 50m 53s
Firmware Version	0.9.28 + 1.8.5
Management VLAN ID	Untagged
Registration Check Code	640187f6

- The **Memory Information** section shows system memory information such as used and Total available, Free, Cached and Buffered

Memory Information

Total Available	74088 kB / 126484 kB (58%)
Free	43440 kB / 126484 kB (34%)
Cached	22240 kB / 126484 kB (17%)
Buffered	8408 kB / 126484 kB (6%)

- The **LAN Information** section shows the Local Area Network settings such as the LAN IP Address, Subnet mask, Gateway, DNS Address, DHCP Client, and STP status.

LAN Information - IPv4

IP Address	10.0.93.25
Subnet Mask	255.255.255.0
Gateway	10.0.93.254
Primary DNS	10.0.93.240
Secondary DNS	10.0.92.240
DHCP Client	Enable
Spanning Tree Protocol(STP) 	Disable

- The **Wireless LAN Information 2.4 GHz/5GHz** section shows wireless information such as Operating Mode, Frequency, and Channel. Since the Access Point supports multiple-SSIDs, information about each SSID and security settings are displayed.

Wireless LAN Information - 2.4GHz

Operation Mode	Access Point			
Wireless Mode	802.11 B/G/N			
Channel Bandwidth	20 MHz			
Channel	2.412 GHz(Channel 1)			
Profile	SSID	Security	VID	802.1Q
#1	EnGenius26138A_1-2.4GHz_desk	None	1	Disable
#2	EnGenius26138A_2-2.4GHz	None	2	Disable
#3	EnGenius26138A_3-2.4GHz	None	3	Disable
#4	EnGenius26138A_4-2.4GHz	None	4	Disable
#5	EnGenius26138A_5-2.4GHz	None	5	Disable
#6	EnGenius26138A_6-2.4GHz	None	6	Disable
#7	EnGenius26138A_7-2.4GHz	None	7	Disable
#8	EnGenius26138A_8-2.4GHz	None	8	Disable
#9	EnGenius-2.4GHz_GuestNetwork	None		Disable

Wireless LAN Information - 5GHz

Operation Mode	Access Point			
Wireless Mode	802.11 N/AC			
Channel Bandwidth	40 MHz			
Channel	5.180 GHz(Channel 36)			
Profile	SSID	Security	VID	802.1Q
#1	EnGenius26138B_1-5GHz_desk	None	51	Disable
#2	EnGenius26138B_2-5GHz	None	52	Disable
#3	EnGenius26138B_3-5GHz	None	53	Disable
#4	EnGenius26138B_4-5GHz	None	54	Disable
#5	EnGenius26138B_5-5GHz	None	55	Disable
#6	EnGenius26138B_6-5GHz	None	56	Disable
#7	EnGenius26138B_7-5GHz	None	57	Disable
#8	EnGenius26138B_8-5GHz	None	58	Disable
#9	EnGenius-5GHz_GuestNetwork	None		Disable

- The **UID/DDNS** section shows each device is distributed with an exclusive unique identification (UID)/DDNS. You can find the default UID/DDNS shown here.

UID / DDNS	
Default UID	1dd3614
Default DDNS Name	1dd3614.engeniusddns.com

Connections

Clicking the **Connections** link under the **Overview** menu displays the list of clients associated to the Access Point's 2.4GHz/5GHz, along with the MAC address, TX, RX and signal strength for each client. Clicking **Kick** in the Block column removes this client.

Connection List - 2.4GHz

SSID	MAC Address	TX	RX	RSSI	Block
------	-------------	----	----	------	-------

Connection List - 5GHz

SSID	MAC Address	TX	RX	RSSI	Block
EnGenius05B06A_1-5GHz	00:02:6F:93:47:5C	162Kb	30Kb	-42dBm	<button>Kick</button>

Refresh

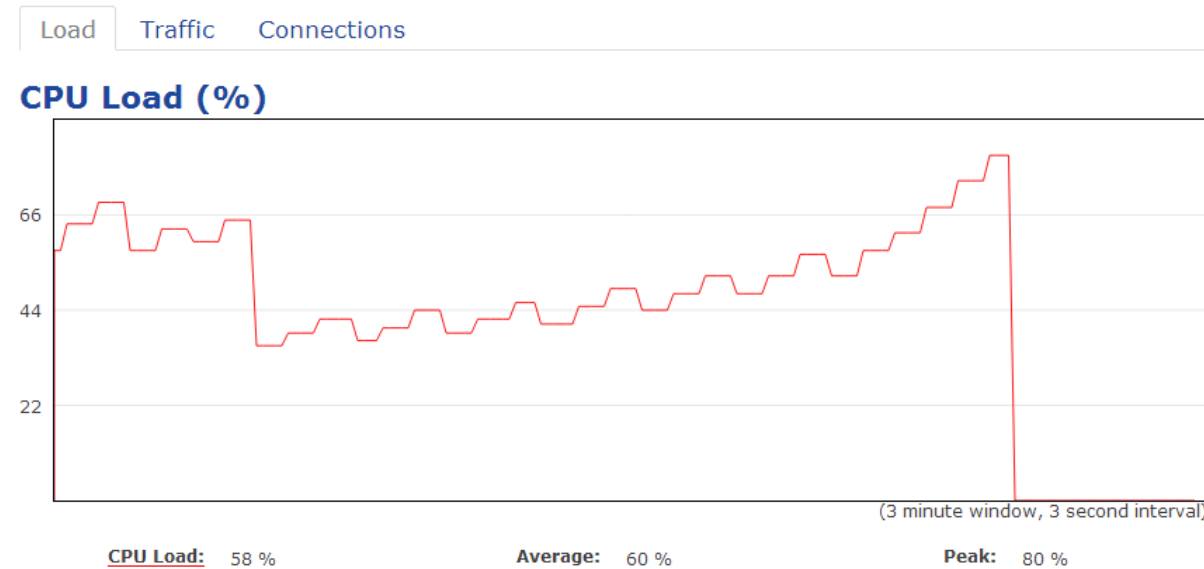
Click **Refresh** to refresh the Connection List page.

Realtime

Clicking the **Realtime** link under the **Overview** menu displays CPU load, Traffic and Connections

CPU Load:

3 minutes CPU loading percentage information, it displays current loading, average loading and peak loading status. Left bar is loading percentage; button is time tracing. Interval is every 3 seconds.



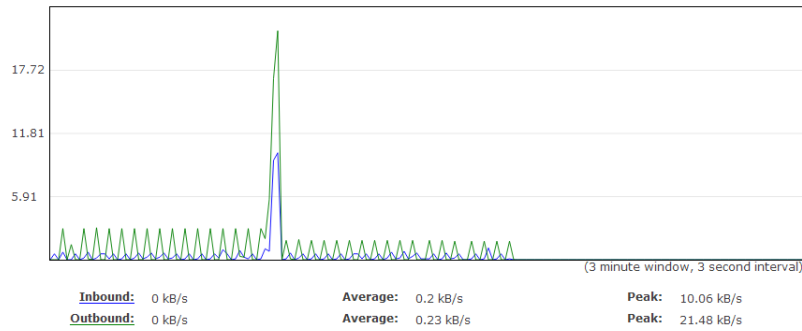
Realtime Traffic (kb/s):

2.4GHz and 5GHz and Ethernet port inbound and outbound traffic by current, average and peak time.

Load Traffic Connections

Realtime Traffic (kB/s)

EnGeniusCCDD10_1-2.4GHz EnGeniusCCDD11_1-5GHz LAN



Realtime Connection (Pkts):

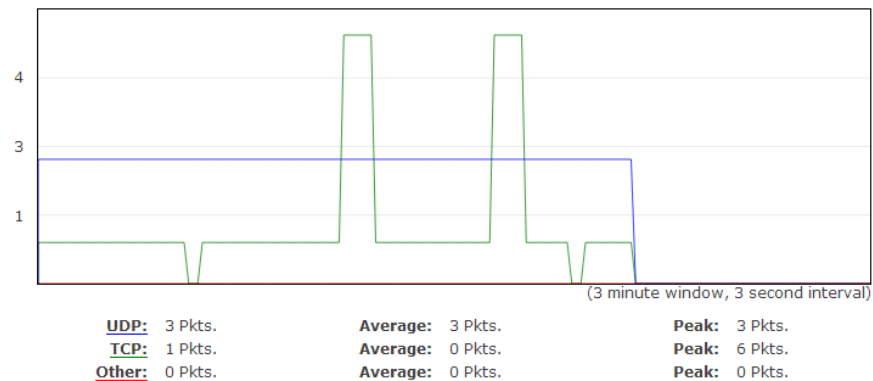
Overview on current active network connections. It displays UDP and TCP packets information and other connection status. UDP connections curve is in blue; TCP connection curve is in green; others curve is in red. Below of chart shows connections source and destination.

Load Traffic Connections

Realtime Connections (Pkts)

This page gives an overview over currently active network connections.

Active Connections



Network	Protocol	Source	Destination	Transfer
IPV4	UDP	192.168.1.22:137	192.168.1.255:137	19.32 KB (250 Pkts.)
IPV4	TCP	192.168.1.22:51427	ECB1750.lan:80	9.53 KB (76 Pkts.)

Chapter 6 **Network**



Basic

This page allows you to modify the device's IP settings and the Spanning Tree settings. Enabling Spanning Tree protocol will prevent network loops in your LAN network.

IPv4 Settings

IPv4 Settings

IP Network Setting	☐ DHCP ☒ Static IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

IP Network Setting: Select whether the device IP address will use the static IP address specified in the IP Address field or be obtained automatically when the device connects to a DHCP server.

IP Address: The IP Address of this device.

IP Subnet Mask: The IP Subnet mask of this device.

Gateway: The Default Gateway of this device. Leave it blank if you are unsure of this setting.

Primary/Secondary DNS: The primary/secondary DNS address for this device.

Spanning Tree Settings

Spanning Tree Protocol (STP) Settings

Status	☐ Enable ☒ Disable	
Hello Time	2	seconds (1-10)
Max Age	20	seconds (6-40)
Forward Delay	15	seconds (4-30)
Priority	32768	(0-65535)

Apply

Apply saved settings to take effect

Status: Enables or disables the Spanning Tree function.

Hello Time: Specify Bridge Hello Time, in seconds. This value determines how often the device sends handshake packets to communicate information about the topology throughout the entire Bridged Local Area Network.

Max Age: Specify Bridge Max Age, in seconds. If another bridge in the spanning tree does not send a hello packet for a long period of time, it is assumed to be inactive.

Forward Delay: Specifies Bridge Forward Delay, in seconds. Forwarding Delay Time is the time spent in each of the Listening and Learning states before the Forwarding state is entered. This delay is provided so that when a new bridge comes onto a busy network, it analyzes data traffic before participating.

Priority: Specify the Priority Number. A smaller number has greater priority.

Apply: Click Apply to save the changes.

Chapter 7 **Wireless**



System Properties

Device Name: Enter a name for the device. The name you type appears in SNMP management. This name is not the SSID and is not broadcast to other devices.

Region: Select Region to conform to local regulations.

Band Steering: Send 802.11n client to the 5GHz band, where 802.11b/g clients cannot go and leave 802.11b/g clients in 2.4GHz to operate their slower rate. Band Steering works within the Access Point by directing 5GHz-capable clients to the band.

Note: When enable band steering function, both 2.4GHz and 5GHz SSID and security setting must be the same.

EnGenius Band Steering supports following advanced settings,

***Prefer 5GHz:** When band steering is configured to Prefer 5GHz mode, the AP will steer dual band capable client devices to 5GHz radio when the RSSI value of these client devices on 5GHz radio is more than set one. The allowed RSSI value for default setting is -75dBm.

***Force 5GHz:** When band steering is configured to Force 5GHz mode, the AP will not dual band capable client devices to network to the 2.4GHz band only if the client devices are not currently associated on 2.4GHz radio in this AP.

***Band Balance:** When band steering is configured to Band Balance mode, the AP will steer dual band capable client devices to 5GHz when the RSSI value of these client devices on 5GHz radio is more than set one. To evenly allocate RF resource on the both 2.4GHz and 5GHz radios, users also can set the portion of client devices on 5GHz radio to assure smoothly connection. The default value of the 5GHz radio is 75%.

Save: Click **Save** to confirm the changes.

Operation mode

The EWS1025CAM supports five operating modes: Access Point, Client Bridge, WDS AP, WDS Bridge, and WDS Station.

2.4GHz 5GHz	Access Point	Client Bridge	WDS AP	WDS Bridge	WDS Station
Access Point	•	•	•	•	•
Client Bridge	•	X	•	X	X
WDS AP	•	•	•	•	•
WDS Bridge	•	X	•	X	X
WDS Station	•	X	•	X	X

This page displays the current status of the Wireless settings of the EWS1025CAM.

	2.4GHz	5GHz
Operation Mode	Access Point ☐ Green ?	Access Point ☐ Green ?
Wireless Mode	802.11 B/G/N ☐	802.11 AC/N ☐
Channel HT Mode	20MHz ☐	40MHz ☐
Extension Channel	Upper Channel ☐	Upper Channel ☐
Channel	Auto ☐	Ch 36 : 5.180 GHz ☐
Transmit Power	Auto ☐	Auto ☐
Data Rate	Auto ☐	Auto ☐
RTS/CTS Threshold ? (1 - 2346)	2346	2346
Client Limits	127 ☐ Enable ☒ Disable	127 ☐ Enable ☒ Disable
Aggregation ?	☒ Enable ☐ Disable 32 Frames 50000 Bytes(Max)	
Multicast to Unicast Stream Conversion	☒ Enable ? ☐ Disable ?	
AP Detection	Scan	Scan

2.4G/5G Wireless Network (Access Point / WDS AP mode)	
Wireless Mode	Wireless mode supports 802.11 b/g/n mixed mode in 2.4G and 802.11 ac/a/n mixed mode in 5G.
Channel HT Mode	Scroll down this list to select bandwidth for operating under a frequency band. The default channel bandwidth is 20 MHz on 2.4GHz frequency radio and 40 MHz on 5GHz frequency radio. Considering the different applications, users can decide to implement a channel bandwidth to fulfill real applications. The larger the channel, the greater the transmission quality and speed.

Channel / Frequency	Select the channel and frequency appropriate.
Auto	Check this option to enable auto-channel selection.
RTS/CTS Threshold	Threshold packet size for RTC/CTS. A small number causes RTS/CTS packet to be sent more often and consumes more bandwidth.
Client Limit	Limits the total number of clients on this radio. Once setting the ceiling of client numbers, the maximum associated client devices will be restricted at this number.
Aggregation	Merges data packets into one packet. This option reduces the number of packets, but also increases packet size.
AP Detection	AP Detection can select the best channel to use by scanning nearby areas for Access Points.
Current Profile	Configure up to eight different SSIDs (four in WDS AP mode). If many client devices will be accessing the network, you can arrange the devices into SSID groups. Click Edit to configure the profile and check whether you want to enable extra SSID.
Save	Click Save to confirm the changes.

Note: Only support four SSID in WDS AP mode.

2.4GHz/5GHz SSID Profile

Under **Wireless Settings**, you can edit the SSID profile to fit your needs. Click **Edit** under the SSID you would like to make changes to.

Wireless Settings - 2.4GHz

Enabled	SSID	Edit	Security	Hidden SSID	Client Isolation 	VLAN Isolation 	L2 Isolation	VLAN ID
☒	EnGenius506012_1-2.4GH.	Edit	None	☐	☐	☐	☐	1
☐	EnGenius506012_2-2.4GH.	Edit	None	☐	☐	☐	☐	2
☐	EnGenius506012_3-2.4GH.	Edit	None	☐	☐	☐	☐	3
☐	EnGenius506012_4-2.4GH.	Edit	None	☐	☐	☐	☐	4
☐	EnGenius506012_5-2.4GH.	Edit	None	☐	☐	☐	☐	5
☐	EnGenius506012_6-2.4GH.	Edit	None	☐	☐	☐	☐	6
☐	EnGenius506012_7-2.4GH.	Edit	None	☐	☐	☐	☐	7
☐	EnGenius506012_8-2.4GH.	Edit	None	☐	☐	☐	☐	8

Wireless Settings - 5GHz

Enabled	SSID	Edit	Security	Hidden SSID	Client Isolation 	VLAN Isolation 	L2 Isolation	VLAN ID
☒	EnGenius506013_1-5GHz	Edit	None	☐	☐	☐	☐	51
☐	EnGenius506013_2-5GHz	Edit	None	☐	☐	☐	☐	52
☐	EnGenius506013_3-5GHz	Edit	None	☐	☐	☐	☐	53
☐	EnGenius506013_4-5GHz	Edit	None	☐	☐	☐	☐	54
☐	EnGenius506013_5-5GHz	Edit	None	☐	☐	☐	☐	55
☐	EnGenius506013_6-5GHz	Edit	None	☐	☐	☐	☐	56
☐	EnGenius506013_7-5GHz	Edit	None	☐	☐	☐	☐	57
☐	EnGenius506013_8-5GHz	Edit	None	☐	☐	☐	☐	58

Enable: Check this option to enable this profile.

SSID: Specifies the SSID for the current profile.

Security: Displays the Security Mode the SSID uses. You can click **Edit** to change the security mode. For more details, see the next section.

Hidden SSID: Check this option to hide the SSID from clients. If checked, the SSID will not appear in the site survey.

Client Isolation: Check this option to prevent communication between client devices.

VLAN Isolation: Check this option to enable VLAN Isolation feature.

L2 Isolation: Check this option to enable L2 Isolation feature.

VLAN ID: Specifies the VLAN ID for the SSID profile.

Wireless Security

The Wireless Security section lets you configure the Access Point's security modes: WEP, WPA-PSK, WPA2-PSK, WPA-PSK Mixed, WPA-Enterprise, WPA2-Enterprise and WPA Mixed Enterprise.

It is strongly recommended that you use **WPA2-PSK**. Click on the **Edit** button under Wireless Settings next to the SSID to change the security settings.

WEP

Security Mode	WEP
Auth Type	Open System
Input Type	Hex
Key Length	40/64-bit (10 hex digits or 5 ASCII char)
Default Key	1
Key1	
Key2	
Key3	
Key4	

Auth Type: Select Open System or Shared Key.

Input Type: ASCII: Regular Text (Recommended) or HEX: Hexadecimal Numbers (For advanced users).

Key Length: Select the desired option and ensure the wireless clients use the same setting. Your choices are: 64, 128, and 152-bit password lengths.

Default Key: Select the key you wish to be default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only. You must enter a Key Value for the Default Key.

Encryption Key: Enter the Key Value or values you wish to use. The default is none.

WPA-PSK/WPA2-PSK (Pre-Shared Key)

Security Mode	WPA-PSK Mixed ▼
Encryption	Both(TKIP+AES) ▼
Passphrase	
Group Key Update Interval	3600

Encryption: Select the WPA/WPA2 encryption type you would like to use. Available options are Both, TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard). Please ensure that your wireless clients use the same settings.

Passphrase: Wireless clients must use the same Key to associate the device. If using ASCII format, the Key must be from 8 to 63 characters in length. If using HEX format, the Key must be 64 HEX characters in length.

Group Key Update Interval: Specify how often, in seconds, the Group Key changes.

WPA/WPA2-Enterprise

Security Mode	WPA Mixed-Enterprise ▼
Encryption	Both(TKIP+AES) ▼
Group Key Update Interval	3600
Radius Server	
Radius Port	1812
Radius Secret	
Radius Accounting	Disable ▼
Radius Accounting Server	
Radius Accounting Port	1813
Radius Accounting Secret	
Interim Accounting Interval	600

Encryption: Select the WPA/WPA2 encryption type you would like to use. Available options are Both, TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard). Please ensure that your wireless clients use the same settings.

Group Key Update Interval: Specify how often, in seconds, the group key changes.

Radius Server: Enter the IP address of the Radius server.

Radius Port: Enter the port number used for connections to the Radius server.

Radius Secret: Enter the secret required to connect to the Radius server.

Radius Accounting: Enables or disables the accounting feature.

Radius Accounting Server: Enter the IP address of the Radius accounting server.

Radius Accounting Port: Enter the port number used for connections to the Radius accounting server.

Radius Accounting Secret: Enter the secret required to connect to the Radius accounting server.

Interim Accounting Interval: Specify how often, in seconds, the accounting data sends.

Note: 802.11n does not allow WEP/WPA-PSK TKIP/WPA2-PSK TKIP security mode. The connection mode will automatically change from 802.11n to 802.11g.

Wireless MAC Filter

Wireless MAC Filter is used to allow or deny network access to wireless clients (computers, tablet PCs, NAS, smart phones, etc.) according to their MAC addresses. You can manually add a MAC address to restrict permission to access the Access Point. The default setting is: Disable Wireless MAC Filter.

Wireless MAC Filter

ACL Mode	Disabled						▼					
		:		:		:		:		:		Add
No.	MAC Address											

ACL (Access Control List) Mode: Determines whether network access is granted or denied to clients whose MAC addresses appear in the MAC address table on this page. Choices given are: Disabled, Deny MAC in the list, or Allow MAC in the list.

MAC Address: Enter the MAC address of the wireless client.

Add: Click **Add** to add the MAC address to the MAC Address table.

Delete: Deletes the selected entries.

Traffic Shaping

Traffic Shaping regulates the flow of packets leaving an interface to deliver improved Quality of Service.

Wireless Traffic Shaping

Enable Traffic Shaping

☐ Enable ☒ Disable

Download Limit

100

Mbps (1-999)

☐ Per User

Upload Limit

100

Mbps (1-999)

☐ Per User

Save

Save current setting(s)

Enable Traffic Shaping: Select to Enable or Disable Wireless Traffic Shaping.

Download Limit: Specifies the wireless transmission speed used for downloading.

Upload Limit: Specifies the wireless transmission speed used for uploading.

Per User: Check this option to enable wireless traffic shaping per user function. This function allow users to limit the maximum download / upload bandwidth for each client devices on this SSID.

Save: Click **Save** to apply the changes.

Fast Roaming

Enable the function to serve mobile client devices that roam from Access Point to Access Point. Some applications running on Client devices require fast re-association when they roam to a different Access Point

Please enter the settings of the SSID and initialize the Security mode to WPA enterprise, as well as to set the Radius Server firstly. Users can enable the Fast Roaming and implement the advanced search.

Please also set the same enterprise Encryption under the same SSID on other Access Points and enable the Fast Roaming. When the configuration is realized on different Access Point, the mobile client devices can run the voice service and require seamless roaming to prevent delay in conversation from Access Point to Access Point.

Fast Roaming

Enable Fast Roaming ☐ Enable ☒ Disable

Enable Fast Roaming: Enable or disable fast roaming feature.

Enable Advanced Search: Enable or disable advanced search feature.

WDS Link Settings

Using the WDS (Wireless Distribution System) feature will allow a network administrator or installer to connect to Access Points wirelessly. Doing so will extend the wired infrastructure to locations where cabling is not possible or inefficient to implement.

Note: Compatibility between different brands and models of Access Points is not guaranteed. It is recommended that the WDS network be created using the same models for maximum compatibility.

Also note: All Access Points in the WDS network need to use the same Channel and Security settings.

To create a WDS network, please enter the MAC addresses of the Access Points that you want included in the WDS.

There can be a maximum of four Access Points.

Note: Only applicable in WDS AP and WDS Bridge modes.

2.4 GHz/5 GHz WDS Link Settings

WDS Link Settings - 2.4GHz

Security None ▾

AES Passphrase
(8-63 ASCII characters or 64 hexadecimal digits)

ID	MAC Address	Mode
1		Disable ▾
2		Disable ▾
3		Disable ▾
4		Disable ▾

WDS Link Settings - 5GHz

Security	None ▾	
AES Passphrase	 (8-63 ASCII characters or 64 hexadecimal digits)	
ID	MAC Address	Mode
1		Disable ▾
2		Disable ▾
3		Disable ▾
4		Disable ▾

Security: Select None or AES from the drop-down list.

AES Passphrase: Enter the Key Values you wish to use.

Other Access Points must use the same Key to establish a WDS link.

MAC Address: Enter the Access Point's MAC address to where you want to extend the wireless area.

Mode: Select to disable or enable from the drop-down list.

Save: Click Save to confirm the changes.

Guest Network

The Guest Network function allows administrators to grant Internet connectivity to visitors or guests while keeping other networked devices (computers and hard drives) and sensitive personal or company information private and secure.

Guest Network Settings

Enable	SSID	Edit	Security	Hidden SSID	Client Isolation
☐	EnGenius-2.4GHz_GuestNetw	Edit	None	☐	☒
☐	EnGenius-5GHz_GuestNetwo	Edit	None	☐	☒

Enable SSID: Select to Enable or Disable SSID broadcasting.

SSID: Specify the SSID for the current profile. This is the name visible on the network to wireless clients.

Security: You can use None or WPA-PSK / WPA2-PSK security for this guest network.

Hidden SSID: Check this option to hide the SSID from broadcasting to discourage wireless users from connecting to a particular SSID.

Client Isolation: Check this option to prevent wireless clients associated with your access point to communicate with other wireless devices connected to the AP.

After enabling Guest Network in the SSID Config page, assign an IP Address, Subnet Mask and DHCP server IP address range for this Guest Network.

Manual IP Settings	
- IP Address	192.168.200.1
- Subnet Mask	255.255.255.0
Automatic DHCP Server Settings	
- Starting IP Address	192.168.200.100
- Ending IP Address	192.168.200.200
- WINS Server IP	0.0.0.0

Manual IP Settings

IP Address: Specify an IP Address for the Guest Network

Subnet Mask: Specify the the Subnet Mask IP Address for the Guest Network

Automatic DHCP Server Settings

Starting IP Address: Specify the starting IP Address range for the Guest Network.

Ending IP Address: Specify the ending IP Address range for the Guest Network.

WINS Server IP: Specify the WINS Server IP Address for the Guest Network. WINS means Windows Internet Name Service. It is Microsoft's implementation of NetBIOS Name Service (NBNS), a name server and service for NetBIOS computer names.

RSSI Threshold

The RSSI value can be adjusted to allow more clients to stay associated to this AP. Note that setting the RSSI value too low may cause wireless clients to reconnect frequently.

RSSI Threshold ⓘ	2.4GHz	5GHz
Status	☐ Enable ☒ Disable	☐ Enable ☒ Disable
RSSI	-90 dBm (Range: -100dBm ~ -60dBm)	-85 dBm (Range: -100dBm ~ -60dBm)

Caution: Enabling RSSI Threshold disassociates wireless clients that fall below the configured RSSI threshold and may cause wireless clients to reconnect frequently. It is recommended to disable this feature unless you deem it absolutely necessary.

RSSI Threshold: Enable the RSSI Threshold feature by ensuring that each client is served by at least one Access Point at any time. Access Points continuously monitor the connectivity quality of any client in their range and efficiently share this information with other Access Points in the vicinity of that client to coordinate which of them should serve the client best.

RSSI: Enter the RSSI (Received Signal Strength Index) in order to determine the handover procedure which the current wireless link will terminate. RSSI is an indication of the power level being received by the antenna. Therefore, the higher the RSSI number, the stronger the signal.

Management VLAN Settings

This section allows you to assign a VLAN tag to the packets. A VLAN is a group of computers on a network whose software has been configured so that they behave as if they were on a separate Local Area Network (LAN). Computers on VLAN do not have to be physically located next to one another on the LAN.

Management VLAN Settings

Status

☐ Enable ☒ Disable

4096

Caution: If you encounter disconnection issue during the configuration process, verify that the switch and the DHCP server can support the new VLAN ID and then connect to the new IP address.

Save

Save current setting(s)

Status: If your network includes VLANs and if tagged packets need to pass through the Access Point, select **Enable** and enter the VLAN ID. Otherwise, click **Disable**.

Save: Click **Save** to apply the changes.

Note: If you reconfigure the Management VLAN ID, you may lose your connection to the Access Point. Verify that the DHCP server supports the reconfigured VLAN ID and then reconnect to the Access Point using the new IP address.

Chapter 8 DDNS



You must Enable EnGenius Cloud first and then choose the Type.

UID/Dynamic DNS		☒ Enable ☐ Disable
☒ Using Default UID/EnGenius DDNS Services		
- Default UID		
- UID Status	Disconnected	
- Default DDNS Name		
- Alias DDNS Name		
Availability Check		
- Refresh Time	24HR	v
- DDNS Status	Disconnected	
☐ Use Other DDNS services		
- Service	dyndns.org v	
- Hostname		
- Username		
- Password		
Apply Apply saved settings to take effect		

A key part about EnGenius Cloud Service is DDNS. Dynamic DNS (DDNS) is a type of DNS that works with dynamic IP address. DDNS keeps update its mapping regularly and ensures a consistent matching so that your device can be accessed over the Internet using a fixed DDNS name. You can either use the default EnGenius DDNS Service or other 3rd party Service you prefer.

Users are recommended to use the free DDNS address printed on the label enclosed in the package. This is because ISP often leases dynamic WAN IP address that changes from time to time. DDNS domain name will always be the same even if the WAN IP address changes.

Default UID: default UID

UID Status: when working properly, it should show "Connected".

Default DDNS: shows the default DDNS

Alias DDNS Name: You may find that your DDNS is too difficult to remember. EnGenius provides free DDNS name registration as long as the alias is not yet been taken other EnGenius product users. You can check the availability by clicking on the button **Availability Check** for verification. In this example, "superman.engeniusddns.com" is available. That is, when the setting is activated, both DDNS name "**superman**.engeniusddns.com" and "**0e95c28**.engeniusddns.com" can be used to access this camera.

Refresh Time: options are 3HR, 6HR, 9HR, 12HR and 24HR. DDNS server needs to synchronize with your IP address often so that you can access your device over the Internet with DDNS name. Depends on your Internet Service provider, your WAN IP address lease time will be different. You can check with your local Internet Service provider for WAN IP address refresh time. The default setting is **24HR** (which means DDNS server will check the synchronization **every 24 hours**). Normally, the default setting 24HR is okay for most cases.

DDNS Status: when working properly, it should show "Connected".

Note: DDNS will only work only if your router is connected to the Internet. If router is not connected to the Internet, your DDNS status will show "Disconnected".

If you prefer to use third-party DDNS server, you can choose this option.

The current supported third-party DDNS services are 3322(qdns), DHS, DynDNS, ZoneEdit and CyberGate. Choose the one that best suits your purpose. You should provide your account information so that the camera can communicate with the selected DDNS vendor.

Your third-party DDNS service account credential should include the following information.

Host Name: please enter your registered Host Name

Username: please enter your registered Username

Password: please enter the password for this

Click **Apply** when configuration is done to activate new settings.

Chapter 9 UPnP



Universal Plug and Play (UPnP) allows the other device to detect the presence of the camera so that communication becomes possible. You should enable UPnP if you wish your camera to be recognized by your router. UPnP Traversal makes camera remote access over the Internet possible using camera DDNS name. You won't be able to access the camera if you disable UPnP feature. Please keep it **Enable** if you are not sure.

Hostname: You may rename your camera to other meaningful names such as storage room, lobby, or any other descriptions you find suitable to describe the space being monitored.

UPnP: Enable or Disable

UPnP Traversal: Enable or Disable

Upnp Settings

- UPnP ☒ Enable ☐ Disable

- UPnP Traversal ☒ Enable ☐ Disable

Apply

Apply saved settings to take effect

Click **Apply** when configuration is done to activate new settings.

Chapter 10 Service Port



The default setting is as follows. This is only reserved for advanced users who want to keep certain ports for other particular services. Changing the ports will result in unexpected result. Unless necessary, please keep the default setting.

Port Settings

Note: We recommend that you keep the default settings to ensure that the service to function properly.

- HTTP Port	80
- HTTP External Port	50000
- RTSP Port	554
- RTSP External Port	59367

Chapter 11 Mesh



Simple to deploy and create a mesh network by the EWS controller or EzMaster in minutes, but for standalone mode without these two applications, user needs to configure the same settings of Mesh network in each device, once EWS1025CAM plugged into any power source, the EnGenius mesh devices automatically optimizes routes between wireless mesh devices and creates a truly adaptive mesh infrastructure with all system. As the wireless environment changes, such as the addition of a new node or link broken, data paths are re-evaluated, and the mesh network self-tunes automatically to maintain its performance. All self-tuning processes are dynamic, occurring in the background and in real time.

Status

It shows the current status of mesh network, such as Enable/Disable, Interface, ID, Channel, and Type.

Status

Mesh Status	Enabled
Mesh Interface	5GHz
Mesh ID	11111111
Mesh Channel	36
Mesh Type	Root Node

For this mesh device list, system will display the information as device name, MAC address and IP address which connect to the mesh network. You can click the "Refresh" button to get the new status again.

Mesh Device List

Node	MAC Address	IP Address
EWS1025CAM-back	8A:DC:96:22:33:22	10.0.92.11
EWS1025CAM-room1	8A:DC:96:22:33:10	10.0.92.19
EWS1025CAM-room2	8A:DC:96:22:33:25	10.0.92.27
EWS1025CAM-desk	8A:DC:96:22:33:19	10.0.92.24
EWS1025CAM-room3	8A:DC:96:22:33:13	10.0.92.43

Settings

Each device must have the same settings in this setting page.

Note: If you have changed the settings in Network Wireless page, please make sure all the settings must be the same in each device.

Mesh Settings

Mesh	☒ Enable ☐ Disable
Operation Mode	☒ Mesh AP ☐ Mesh Point
Mesh Device Name	EWS1025CAM-desk
Mesh Band	☐ 2.4GHz ☒ 5GHz
Mesh ID	11111111
Password	11111111
Mesh RSSI	-80 (dBm)

Apply

Cancel

Mesh: Enable or Disable the mesh function, system will save the settings even mesh function is disable.

Operation Mode: The **Mesh AP** mode is mesh point with wireless AP function. And system will auto disable the wireless AP function when user selected the **Mesh Point** mode.

Mesh Device Name: You can click the hyper link to modify the Mesh device name from wireless setting page of device name.

Mesh Band: Select the 2.4GHz or 5GHz for the mesh backbone connection.

Mesh ID: The mesh ID should be maximum up to 8 characters in numbers 0 ~ 9.

Password: The mesh password should be maximum up to 12 characters.

Mesh RSSI: Enter the Mesh RSSI in order to determine the connection procedure which the current wireless link will terminate.
The higher the RSSI number, the stronger the signal.

Tools

This diagnostic tools page provides easy ways to check the current status of the mesh network. This section contains the following options:

Node List

Mesh ID 123 

123456789

5 Node(s)

2 Root Node(s)

Node	Type	Hops Count 	Neighbor Nodes 	(RSSI)	Signal Strength 
Linko_RD_blk1 88:dc:96:02:a0:11	Root Node 	— 	Linko_701 88:dc:96:25:99:50	-50	
			Linko_705 88:dc:96:00:20:31	-70	
			Linko_sales 88:dc:96:00:23:44	-65	
			Linko_8F 88:dc:96:03:12:a3	-78	
Linko_8F 88:dc:96:03:12:a3	Mesh Node 	4	Linko_701 00:1a:1e:25:99:50	-50	
			Linko_705 88:dc:96:00:20:31	-70	
			Linko_sales 88:dc:96:00:23:44	-65	
			Linko_RD_blk1 88:dc:96:02:a0:11	-78	

All the connected Mesh nodes will be displayed in this page.

Node: It shows the device name and MAC address.

Type: There are two types of the node. The **Root node** uplink to the gateway by wire, and connect with other mesh node by wireless simultaneously.

Hops Count: The hops count refers to the number of intermediate devices through which data must pass between the Mesh node itself and Root node. If the Hops Count number is more than 3, we recommend that you have to optimize your deployment of the device location. System shows “—” when the node is Root or alone node

Neighbor Nodes: Display all the neighbor nodes which discovered by individually mesh node, no matter with its signal strength allowed to link or not.

RSSI: The current signal strength of the node.

Signal Strength: There are four levels signal bar to display the RSSI, if the RSSI is below -76db, then it will display a red bar.

Link Status

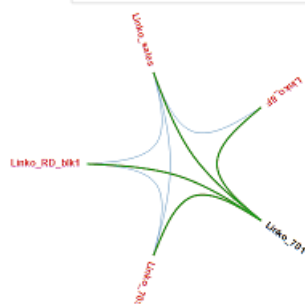
Node List

Link Status

Ping

Traceroute

Throughput



Unreachable Mesh Node(s)	RSSI	Detector Nodes
Linko_701 00:1a:1e:25:99:50	-90	Linko_702 Linko_RD_aa
Linko_705 88:dc:96:00:20:31	-80	Linko_sales Linko_RD_blk1 Linko_4F
Linko_sales 88:dc:96:00:23:44	-85	Linko_701
Linko_RD_blk1 88:dc:96:02:a0:11	-78	Linko_702 Linko_4F

The Mesh network view is an overview for all mesh nodes.

Mesh View: Mouse over on any Mesh node (black) for the linking status which is linking to other Mesh nodes (blue) with green line.

Unreachable Mesh Node(s): The nodes which can't be connected to the mesh network, due to the weak signal detected by neighbor nodes.

RSSI: The node is not allowed to link with mesh if its current signal strength is continuously lower than the Mesh RSSI which is in the mesh settings page.

Detector Nodes: The neighbor node(s) which detected the unreachable mesh node.

Ping

Ping Test Parameters

From	EWS1025CAM-desk (8A:D0:00:00:00:00) ▼	To	EWS1025CAM-back (8A:D0:00:00:00:00) ▼
Number of Pings	4		
Start	<pre>PING 8a:dc:96:22:33:93 (8a:dc:96:22:33:93) 20(48) bytes of data 20 bytes from 8a:dc:96:22:33:93 icmp_seq=1 ttl=50 time=0.49 ms 20 bytes from 8a:dc:96:22:33:93 icmp_seq=2 ttl=50 time=0.48 ms 20 bytes from 8a:dc:96:22:33:93 icmp_seq=3 ttl=50 time=0.52 ms 20 bytes from 8a:dc:96:22:33:93 icmp_seq=4 ttl=50 time=0.51 ms --- 8a:dc:96:22:33:93 ping statistics --- 4 packets transmitted, 4 received, 0% packet loss rtt min/avg/max/mdev = 0.482/0.501/0.518/0.015 ms</pre>		

This page allows you to analyze the connection quality of a mesh node to other mesh node in the mesh network.

Trace Route

Traceroute Test Parameters

From	EWS1025CAM-back (8A:D0:00:00:00:00) ▼	To	EWS1025CAM-desk (8A:D0:00:00:00:00) ▼
Start	<pre>traceroute to 8a:dc:96:50:60:13 (8a:dc:96:50:60:13), 50 hops max, 20 byte packets 1: 8a:dc:96:50:60:13 0.501 ms 0.422 ms 0.457 ms</pre>		

This page allows you to analyze the routing table to a target from a mesh node to other mesh node in the mesh network.

Throughput

Throughput Test

EWS1025CAM-desk (8A:D0:00:00:00:00) ▼	And	EWS1025CAM-back (8A:D0:00:00:00:00) ▼	Start
84.7 Mbits/sec	↔	84.3 Mbits/sec	

This page allows you to analyze the throughput from a mesh node to other mesh node in the mesh network.

Chapter 12 **Management**



Controller Settings

Adding EWS1025CAM to ezMaster Device Inventory, you must first bind the AP to ezMaster's Device Inventory by 'registering' the device. You can manually redirecting each AP to ezMaster, or skip this section if you are managing only local devices. You can test the ezMaster Device Inventory by IP address, and get the connection status between EWS1025CAM and ezMaster Device Inventory.

Controller Settings

Controller Address(Auto detection if leave empty)		Test
Connection Status	Disconnect	
Check Code	485de142	

SNMP Settings

This page allows you to assign the Contact Details, Location, Community Name, and Trap Settings for Simple Network Management Protocol (SNMP). This is a networking management protocol used to monitor network attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of the network. Upon receiving these messages, SNMP compatible devices (called agents) returns the data stored in their Management Information Bases. To configure SNMP Settings, click under the **Advanced** tab on the side bar under **Management**.

SNMP Settings

Status	☒ Enable ☐ Disable	
Contact		
Location		
Community Name (Read Only)	public	
Community Name (Read Write)	private	
Trap Destination		
- Port	162	
- IP Address		
- Community Name	public	
SNMPv3 Settings		
- Status	☒ Enable ☐ Disable	
- Username	admin	(1-31 Characters)
- Authorized Protocol	MD5	v
- Authorized Key	12345678	(8-32 Characters)
- Private Protocol	DES	v
- Private Key	12345678	(8-32 Characters)
- Engine ID		

Status: Enables or Disables the SNMP feature.

Contact: Specifies the contact details of the device.

Location: Specifies the location of the device.

Community Name (Read Only): Specifies the password for the SNMP community for read only access.

Community Name (Read/Write): Specifies the password for the SNMP community with read/write access.

Trap Destination Address: Specifies the port and IP address of the computer that will receive the SNMP traps.

Port: Displays the port number.

Trap Destination Community Name: Specifies the password for the SNMP trap community.

SNMPv3 Status: Enables or Disables the SNMPv3 feature.

User Name: Specifies the username for the SNMPv3.feature

Auth Protocol: Select the Authentication Protocol type: MDS or SHA.

Auth Key: Specify the Authentication Key for authentication.

Priv Protocol: Select the Privacy Protocol type: DES.

Priv Key: Specifies the privacy key for privacy.

Engine ID: Specifies the Engine ID for SNMPv3.

CLI/SSH Settings

Most users will configure the device through the graphical user interface (GUI). However, for those who prefer an alternative method there is the command line interface (CLI). The CLI can be accessed through a command console, modem or Telnet connection. For security's concern, you can enable SSH (Secure Shell) to establish a secure data communication.

CLI Setting

Status	☒ Enable ☐ Disable
--------	---

SSH Setting

Status	☐ Enable ☒ Disable
--------	---

CLI Status: Select **Enable** or **Disable** to enable or disable the ability to modify the Access Point via a command line interface (CLI).

SSH Status: Select **Enable** or **Disable** to enable or disable the ability to modify the Access Point via a command line interface (CLI) with a secure channel.

HTTPS Settings

Hypertext Transfer Protocol Secure (HTTPS) is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.

HTTPS Settings

Status	☐ Enable ☒ Disable
HTTPS Forward	☐ Enable ☒ Disable

Status: Select **Enable** or **Disable** to enable or disable the ability to modify the Access Point via a HTTPS.

HTTPS forward: Enable this option; it will be forwarded to HTTPS if user uses HTTP to access the Access Point.

Email Alert

The Access Point will send email alerts when configurations have been changed.

Email Alert

Status	☐ Enable
- From	
- To	
- Subject	
Email Account	
- Username	
- Password	
- SMTP Server	Port: 25
- Security Mode	None 
Send Test Mail	
Apply Apply saved settings to take effect	

Status: Check **Enable** to enable Email Alert feature.

From: Enter the address to show as the sender of the email.

To: Enter the address to show as the receiver of the email.

Subject: Enter the subject to show as the subject of the email.

Email Account

Username/Password: Enter the username and password required to connect to the SMTP server.

SMTP Server/Port: Enter the IP address/domain name and port of the SMTP server. The default port of SMTP Server is port 25.

Security Mode: Select the mode of security for the Email alert. The options are None, SSL/TLS and STARTTLS.

Send Test Mail: Click **Send Test Mail** button to test the Email Alert setup.

Apply: Click **Apply** to save the changes.

Date and Time Settings

This page allows you to set the internal clock of the Access Point. To access the Date and Time settings, click **Time Zone** under the **Management** tab on the side bar.

Date and Time Settings

☐ Manually Set Date and Time

Date: 2016 / 09 / 12

Time: 09 : 31 (24-Hour)

Synchronize with PC

☒ Automatically Get Date and Time

NTP Server: pool.ntp.org

Time Zone

Time Zone: UTC+00:00 Gambia, Liberia, Morocco

☐ Enable Daylight Saving

Start: January 1s Sun 00:00

End: January 1s Mon 00:00

Apply Apply saved settings to take effect

Manually Set Date and Time: Manually specify the date and time.

Synchronize with PC: Click to synchronize the Access Point's internal clock with the computer's time.

Automatically Get Date and Time: Enter the IP address of an NTP server or use the default NTP server to have the internal clock set automatically.

Time Zone: Choose the time zone you would like to use from the drop-down list.

Enable Daylight Savings: Check the box to enable or disable daylight savings time for the Access Point. Next, enter the dates that correspond to the present year's daylight savings time.

Click **Apply** to save the changes.

WiFi Scheduler

Use the schedule function to reboot the Access Point or control the wireless availability on a routine basis. The Schedule function relies on the GMT time setting acquired from a network time protocol (NTP) server. For details on how to connect the Access Point to an NTP server, see Date and Time Settings.

Auto Reboot Settings

You can specify how often you would like to reboot the Access Point.

Auto Reboot Setting

Status	☐ Enable ☒ Disable
Timer	☐ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday
	0 : 0

Status: Enables or disables the Auto Reboot function.

Timer: Specifies the time and frequency in rebooting the Access Point by Min, Hour and Day.

WiFi Scheduler

Wi-Fi Scheduler

Status	☐ Enable ☒ Disable NOTE: Please assure that the Time Zone Settings is synced with your local time when enabling the Wi-Fi Scheduler																								
Wireless Radio	2.4GHz v																								
SSID Selection	EnGenius506012_1-2.4GHz v																								
Schedule Templates	Choose a template v																								
Schedule Table	<table><thead><tr><th>Day</th><th>Available</th><th>Duration</th></tr></thead><tbody><tr><td>Sunday</td><td>available v </td><td>00 : 00 ~ 24 : 00</td></tr><tr><td>Monday</td><td>available v </td><td>00 : 00 ~ 24 : 00</td></tr><tr><td>Tuesday</td><td>available v </td><td>00 : 00 ~ 24 : 00</td></tr><tr><td>Wednesday</td><td>available v </td><td>00 : 00 ~ 24 : 00</td></tr><tr><td>Thursday</td><td>available v </td><td>00 : 00 ~ 24 : 00</td></tr><tr><td>Friday</td><td>available v </td><td>00 : 00 ~ 24 : 00</td></tr><tr><td>Saturday</td><td>available v </td><td>00 : 00 ~ 24 : 00</td></tr></tbody></table>	Day	Available	Duration	Sunday	available v	00 : 00 ~ 24 : 00	Monday	available v	00 : 00 ~ 24 : 00	Tuesday	available v	00 : 00 ~ 24 : 00	Wednesday	available v	00 : 00 ~ 24 : 00	Thursday	available v	00 : 00 ~ 24 : 00	Friday	available v	00 : 00 ~ 24 : 00	Saturday	available v	00 : 00 ~ 24 : 00
Day	Available	Duration																							
Sunday	available v	00 : 00 ~ 24 : 00																							
Monday	available v	00 : 00 ~ 24 : 00																							
Tuesday	available v	00 : 00 ~ 24 : 00																							
Wednesday	available v	00 : 00 ~ 24 : 00																							
Thursday	available v	00 : 00 ~ 24 : 00																							
Friday	available v	00 : 00 ~ 24 : 00																							
Saturday	available v	00 : 00 ~ 24 : 00																							
Apply Apply saved settings to take effect																									

Status: Enables or disables the WiFi Scheduler function.

Wireless Radio: Select 2.4GHz or 5GHz* to use WiFi Schedule.

SSID Selection: Select a SSID to use WiFi Schedule.

Schedule Templates: There are 3 templates available: Always available, Available 8-5 daily and Available 8-5 daily except weekends. Select Custom schedule if you want to set the schedule manually.

Schedule Table: Set the schedule manually.

*5GHz radio settings only available for dual radio models.

Tools

This section allows you to analyze the connection quality of the Access Point and trace the routing table to a target in the network.

Ping Test Parameters

Ping Test Parameters

Target IP / Domain Name	
Ping Packet Size	64 Bytes
Number of Pings	4

Target IP/Domain Name: Enter the IP address or Domain name you would like to search.

Ping Packet Size: Enter the packet size of each ping.

Number of Pings: Enter the number of times you wish to ping.

Start: Click **Start** to begin pinging target device (via IP).

Traceroute Parameters

Traceroute Test Parameters

Target IP / Domain Name	
Start	

Target IP/Domain Name: Enter an IP address or domain name you wish to trace.

Start: Click **Start** to begin the trace route operation.

Stop: Halts the traceroute test.

Nslookup Parameters

Nslookup Test Parameters

Target IP / Domain Name	
Start	

Target IP/Domain Name: Enter an IP address or domain name you wish to trace.

Start: Click **Start** to begin the Nslookup operation.

Speed Test Parameters

Speed Test Parameters

Target IP / Domain Name	
Time Period	20 Sec
Check Interval	5 Sec
Port	5001
Start	

Target IP/Domain Name: Enter an IP address or domain name you wish to run a Speed Test for.

Time Period: Enter the time in seconds that you would like the test to run for and in how many intervals.

Start: Starts the Speed Test.

IPv4: The Access Point uses IPv4 port 5001 for the speed test.

LED Control

This section allows you to control the LED control functions: Power status, LAN interface and 2.4GHz/5GHz/Mesh WLAN interface.

LED Control

Power	☒ Enable ☐ Disable
LAN	☒ Enable ☐ Disable
WLAN-2.4GHz	☒ Enable ☐ Disable
WLAN-5GHz	☒ Enable ☐ Disable
Mesh	☒ Enable ☐ Disable

Click **Apply** to save the settings after selecting your choices from the boxes.

Device Discovery

Under Device Discovery, you can choose for the Access Point to automatically scan for local devices to connect to. Click **Scan** to begin the process.

Device Discovery

Device Name	Operation Mode	IP Address	System MAC Address	Firmware Version
Scan				

Chapter 13 **System Manager**



Account Setting

This page allows you to change the username and password of the device. There are three types of the account settings:

1. Web Account By default, the username is **admin** and the password is **admin**. The password can contain from 0 to 12 alphanumeric characters and is case sensitive.
2. Onvif Account By default, the username is **onvif** and the password is **admin**. The password can contain from 0 to 12 alphanumeric characters and is case sensitive.
3. Viewer Account By default, the username is **guest** and the password is **guest**. The password can contain from 0 to 12 alphanumeric characters and is case sensitive. You can add four different accounts for viewer account.

Web Account List

Username	Action
admin	<button>Edit</button>

Onvif Account List

Username	Action
onvif	<button>Edit</button>

Viewer Account List

Username	Action
guest	<button>Edit</button>

Add

Administrator Username: Enter a new username for logging in to the Administrator Username entry box.

Current Password: Enter the old password for logging in to the Current Password entry box.

New Password: Enter the new password for logging in to the New Password entry box.

Verify Password: Re-enter the new password in the Verify Password entry box for confirmation.

Apply: Click **Apply** to save the changes.

Note: it is highly recommended that you change your password to something more unique for greater security.

Push Message Mobile List

Here will list the devices which enable the feature of push message on this camera. When an event triggered, camera will send the message to all the devices in this list. You can click "Delete" to disable the feature of the mobile device.

Mobile List

Description	Platform	Device Token	Action
John	iOS	7ef97c571d...	Delete
Mary	Android	APA91bGz0f...	Delete

Firmware Upgrade

This page allows you to upgrade the Firmware of the Access Point.

Firmware Upgrade

Current Firmware Version: 2.0.0

Select the new firmware from your hard disk.

	Browse...
Upload	

To Perform the Firmware Upgrade:

1. Click the **Browse...** button and navigate the OS File System to the location of the Firmware upgrade file.
2. Select the upgrade file. The name of the file will appear in the Upgrade File field.
3. Click the **Upload** button to commence the Firmware upgrade.

Note: The device is unavailable during the upgrade process and must restart when the upgrade is completed. Any connections to or through the device will be lost.

Backup/Restore

This page allows you to save the current device configurations. When you save the configurations, you can also reload the saved configurations into the device through the **Restore New Settings** from a file folder. If extreme problems occur, or if you have set the device incorrectly, you can use the **Reset** button in the **Reset to Default** section to restore all the configurations of the device to the original default settings. To Configure the Backup/Restore Settings, click **Backup/Restore** under the **Systems Manager** tab. All the settings can be separated to "Camera only" or "Access Point only".

Backup/Restore Settings

Backup Setting		
- Backup Setting 	☐ Camera ☐ Access Point ☒ All	<button>Export</button>
- Restore New Setting	<button>Browse ..</button>	<button>Import</button>
User Setting		
- Back Up Setting as Default	☐ Camera ☐ Access Point ☒ All	<button>Backup</button>
- Restore to User Default 	☐ Camera ☐ Access Point ☒ All	<button>Restore</button>
- Caution: Please write down your account number and password before saving. The user settings will now become the new default settings at the next successful login.		

Factory Setting

Backup Setting: Click **Export** to save the current device configurations to a file.

Restore New Setting: Choose the file you wish restore for settings and click **Import**.

Reset to Default: Click the **Reset** button to restore the Access Point to its factory default settings.

User Setting

Back Up Setting as Default: Click **Backup** to backup the user settings you would like to use as the default settings.

Restore to User Default: Click **Restore** to restore the Access Point to user's default settings.

All the settings can be separated to "Camera only" or "Access Point only"

Reset/Reboot

In some circumstances, you may be required to force the device to reboot. Click on **Reboot the Device** to reboot the device.

Reset the device

- Reset the device 

☐ Camera ☐ Access Point ☒ All

Reset

Reboot the device

Caution: Pressing this button will cause the device to reboot.

Reboot

System Log

This page allows you to setup the System Log and local log functions of the Access Point. Click **Log** under the **Systems Manager** tab to open up the System Log page.

System Log

Status ☒ Enable ☐ Disable

Log type All 





```
Jan 7 11:20:01 EWS320AP user.notice root: starting ntpd
Jan 7 11:20:01 EWS320AP cron.info crond[2159]: crond: USER root pid 3505 cmd sch
Jan 7 11:20:01 EWS320AP cron.info crond[2159]: crond: USER root pid 3501 cmd . /
Jan 7 11:18:01 EWS320AP cron.info crond[2159]: crond: USER root pid 969 cmd sche
Jan 7 11:16:01 EWS320AP cron.info crond[2159]: crond: USER root pid 2252 cmd sch
Jan 7 11:15:01 EWS320AP user.notice root: starting ntpd
Jan 7 11:15:01 EWS320AP cron.info crond[2159]: crond: USER root pid 1011 cmd . /
Jan 7 11:14:01 EWS320AP cron.info crond[2159]: crond: USER root pid 3582 cmd sch
Jan 7 11:12:01 EWS320AP cron.info crond[2159]: crond: USER root pid 954 cmd sche
Jan 7 11:10:01 EWS320AP user.notice root: starting ntpd
```

Remote Log ☐ Enable ☒ Disable

Log Server IP Address 0.0.0.0

 Apply

Apply saved settings to take effect

Status: Enables or disables the System Log function.

Log Type: Select the Log Type mode you would like to use.

Remote Log: Enables or disables the Remote Log feature. If enabled, enter the IP address of the Log you would like to remote to.

Log Server IP Address: Enter the IP address of the log server.

Apply: Click **Apply** to save the changes.

Chapter 14 **Camera OverView**



Camera Status

Status page displays the detail video streaming information on the page including Resolution, Video Codec, Frame Rate, Ethernet Bit Rate, WiFi Bit Rate and Audio Codec.

Video

Stream 1

Resolution	1920 x 1080
Video Codec	H.264
Frame Rate	30 fps
Bit Rate (Ethernet)	4 Mbps
Bit Rate (Wi-Fi)	1 Mbps
Audio Codec	AAC

Stream 2

Resolution	640 x 360
Video Codec	H.264
Frame Rate	15 fps
Bit Rate (Ethernet)	256 Kbps
Bit Rate (Wi-Fi)	256 Kbps
Audio Codec	AAC

PC Storage Path

Folder Path: click "Browse" to change the path

Snapshot File Type: support image format JPG, PNG & BMP

Recording File Type: support format AVI & MP4

Compression rate comparison (High to Low):

JPG > PNG > BMP

MP4 > AVI

You should consider keeping the default setting because it reduces image or clip file size.

Recording / Snapshot Path

Folder Path	C:\Users\102106\AppData\LocalLow	Browse
Snapshot File Type	JPG	
Recording File Type	AVI	

Note: The video recording and snapshot will be stored in the target folder.

Apply	Cancel
--------------------------------------	---------------------------------------

Chapter 15 **Media**



Video

☐ Display overlay

Timestamp and Video Title (A-Z, 0-9, :, /, -)

Stream 1

Compression Format	H.264
Resolution	1920 x 1080
Max. Frame per Second	30 fps
Bit Rate Encoding	Constant Bit Rate
Bit Rate Value	4 Mbps

Stream 2

Compression Format	H.264
Resolution	640 x 360
Max. Frame per Second	15 fps
Bit Rate Encoding	Constant Bit Rate
Bit Rate Value	256 Kbps

Note: You may adjust Bit Rate Value according to your connectivity mode or bandwidth conditions.

Higher bit rates delivers excellence resolution when video is viewed in full-screen on PC. Lower bit rates may be better choices in limited-bandwidth environments or via remote Wi-Fi network.

Default Settings

Apply

Cancel

Enable: it is recommended that you enable **Time Stamp and Video Title**; the timestamp will show on the top-left corner of your video as shown below.



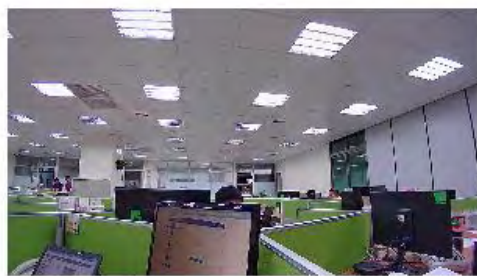
Camera

You can get better quality by tuning the lighting condition of the camera. For example, in a dark room you may want to set the Brightness higher to generate clearer result. When directly facing an outdoor window (too much light) you may want to lower the Brightness a bit. There may be different settings under different circumstance; therefore, you should tune the setting if the image quality has become too low to serve its purpose. Please refer to the following examples for comparison between low and high for each of the light settings.

Image Settings

Brightness 50
Contrast 50
Saturation 50
Sharpness 50

Flicker Control
Mirror/Flip
Day/Night Mode



Default Settings

Apply

Cancel

Light setting

Brightness



Contrast



Sturation



Sharpness



De-noise



Please note that some of the effects will be more obvious in higher resolution at real time.

Flicker Control

The supported options are: 60Hz & 50Hz

Flicker Control is an anti-flicker feature setting.

AC lamp can cause a flicker effect, which is a consequence of the AC power frequency (50 or 60 Hz). As the light can change from picture to picture, causing light flicker. This will lead to inconsistent light source between each snapshot. To eliminate flicker, configure your camera to PAL (60Hz) or NTSC (50Hz) modes to compensate the effects. Check the power supply of your region for proper setting.

Mirror

Support Mirrors: **None**, **Mirror**, **Flip** and **Both**

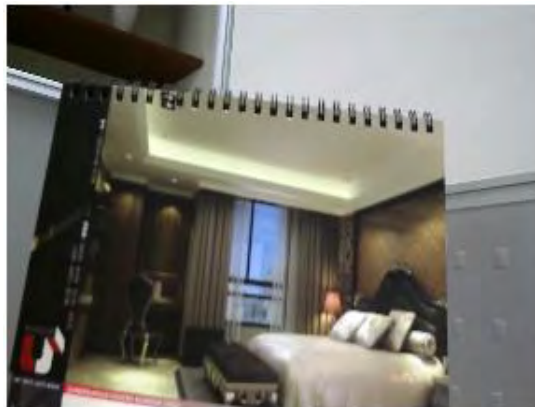
There are times that the camera will have to be mounted upside down for sideways. That is, the view become difficult to monitor when it is upside down. The **Mirror** setting does not reflect on the preview at real time (unlike lighting condition settings). Therefore, you have to click on **Apply** to see the result.

The following examples compare **none** with **a chosen mirror effect**.

Mirror (Horizontal)



None

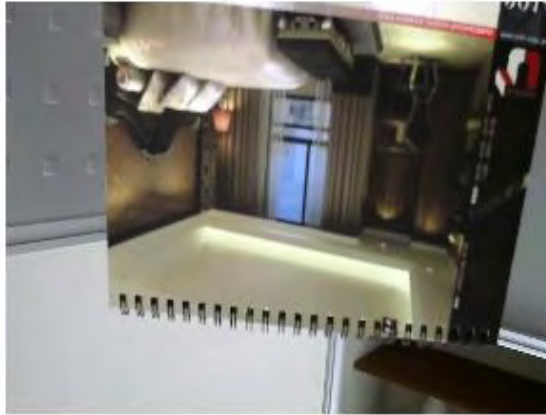


Mirror

Flip (Vertical)



None



Flip

Both (Horizontal and Vertical)



None



Both

Day/Night Mode

This controls **Night Vision** ON and OFF.

Auto: auto detect light sufficiency and switch between Day and Night automatically.

Day: force the camera to turn **OFF** Night Vision.

Night: force the camera to turn Night Vision **ON**.



Day



Night

Advance

Exposure Settings

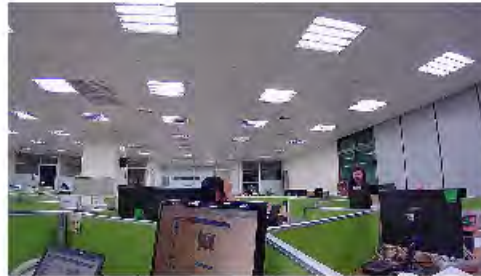
Mode Outdoor ▼
Gain Control 64X ▼

Shutter Time

Max (sec) 1/30 ▼
Min (sec) 1/10000 ▼

Others

EV Compensation 0 ▼
WDR Status ☒ Enable ☐ Disable
WDR Level 2 ▼
Low Light Compensation ☒ Enable ☐ Disable



Note: Click on Apply for checking the updated view.

Default Settings

Apply

Cancel

Exposure Settings

Mode: Manual, Indoor, Outdoor

For regular users, please choose indoor or outdoor, if you are not sure about the terms and behavior, the default values will be the preconfigured. The areas are grey out for preconfigured settings when you choose **Indoor** or **Outdoor**.

Manual

Choose **Manual** if you would like to fine tune some of the settings that suits your application. Please be noted that these settings may have impacts on the image quality and performance.

Exposure Settings

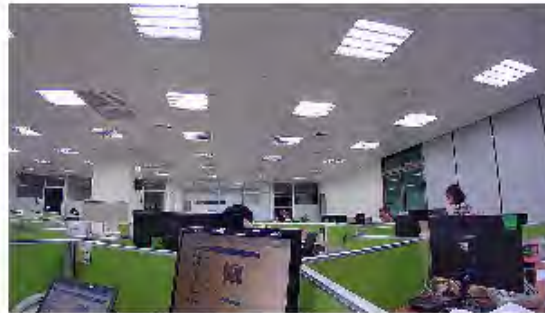
Mode	Manual ▼
Gain Control	64X ▼

Shutter Time

Max (sec)	1/30 ▼
Min (sec)	1/10000 ▼

Others

EV Compensation	0 ▼
WDR Status	☒ Enable ☐ Disable
WDR Level	2 ▼
Low Light Compensation	☒ Enable ☐ Disable



Note: Click on Apply for checking the updated view.

Default Settings

Apply

Cancel

Privacy Mask

Choose **Enable** if you would like to put certain areas in private. Please use selected window to hide certain area for privacy purpose.

Privacy Mask Settings

Privacy Mask Settings

Status ☒ Enable ☐ Disable Set up Privacy Mask window

☒

Window 1

☐

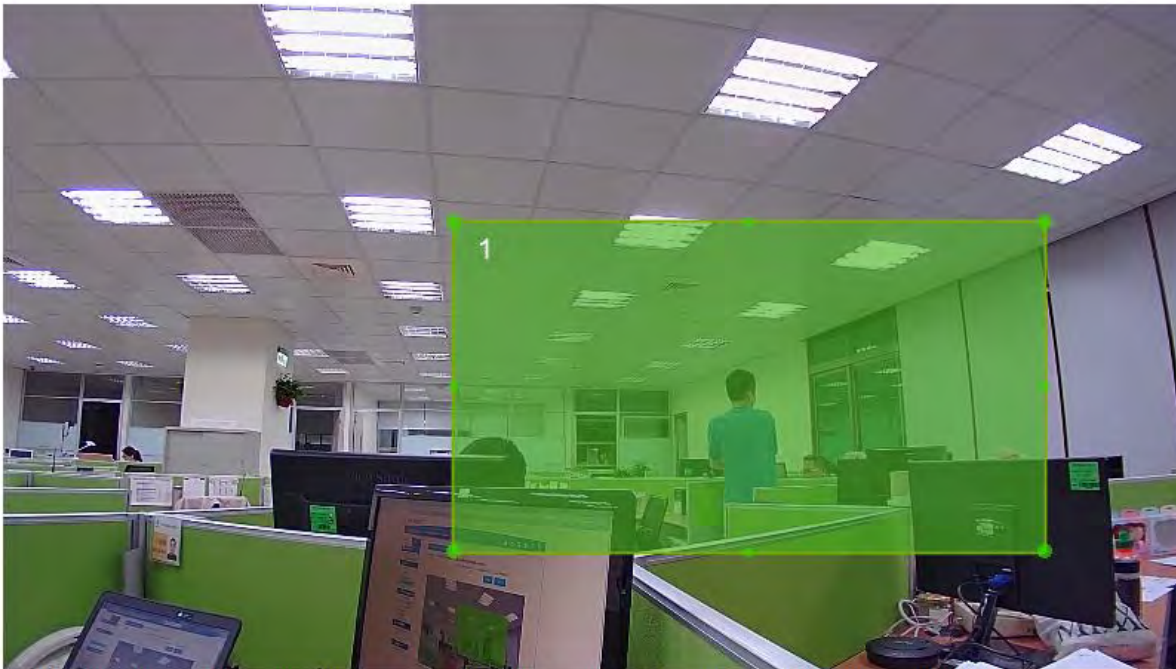
Window 2

☐

Window 3

Apply

Cancel



Note: You can adjust the motion detecting area by dragging the four corners to resize the window.

Audio

Status

If you audio is important to what you are monitoring, you need to set the audio status to Enable. So that the microphone can pick up sounds in the environment. On the other hand, if audio is not necessary (for instance an open space with a lot of noises), you are advised to disable the audio to reduce the clips file size. The default sample rate is 8k, and the bit rate is 16 bit.

Audio Settings

Status ☒ Enable ☐ Disable

Microphone (Input) Gain 50

Encoding

Input Gain: setting the sensitivity of the microphone. High gain will result in higher volume and but picks up more noise.

Encoding: supports G711A, AAC and G711U.

Chapter 16 **Event Management**



Event Control

This camera supports many smart features that allow you to utilize the camera in many application scenarios. This section will introduce each of them in detail.

Event Control

Enable	Name	Schedule	Trigger Type	Action Type	Storage Destination	Action
☐	Schedule Record	Always	Time	Record	SD Card	Edit
☐	Motion Detection	Always	Motion Detection	Disable	---	Edit
☐	Audio Detection	Always	Audio Detection	Disable	---	Edit

When camera detects an event that matches the predefined condition an **event** will be triggered and proceed with the defined actions; for instance, taking snapshots or recording videos for the specified length of time and interval. There are two profiles for default setting, you can click "Edit" for detail settings or create a new profile by "Add".

Event Control

Enable	☐ Enable ☒ Disable
Name	
Schedule	☐ Every Day ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun ☐ All Day
Time of day	From : To :
Trigger Type	☐ Time ☒ Detectors ☒ Motion Detection ☐ Audio Detection ☐ Tampering Detection

Event Notification

Push Message	☐ Enable ☒ Disable
E-Mail	☐ Enable ☒ Disable

Event Action

Action Type	Disable ▼
-------------	--

Enable/Disable the event control

Schedule to set the camera to record video regularly based on a predefined schedule.

Time of day can specify the time range for each schedule.

Trigger Type by Time or Detectors, if you select the detectors, it can be trigger by Motion detection, Audio detection or Tampering detection.

Event Notification can send the message to user when event triggered, you can select Push message, E-mail and VMS at the same time.

Event Action includes two types of the action when event triggered.

Event Action

Action Type

Disable
Record
Snapshot

Record to SD Card, Network Storage or FTP, please remember to setup and enable the correlate settings of Network Storage and FTP.

Event Action

Action Type

Record	▼
--------	---

Storage Destination

☒ SD Card ☐ Network Storage ☐ FTP

Snapshot to SD Card, Network Storage, FTP or E-Mail, please remember to setup and enable the correlate settings of Network Storage, FTP, E-mail.

Event Action

Action Type

Snapshot	▼
----------	---

Storage Destination

☒ SD Card ☐ Network Storage ☐ FTP ☐ E-Mail

Motion Detection

Enable: it is recommended that you enable **Time Stamp and Video**

Video OSD Prompt

☒ Enable ☐ Disable

Set up motion detecting window

- | | | | |
|-------------------------------------|----------|--------------------|---|
| ☒ | Window 1 | Sensitivity : 60 % |  |
| ☐ | Window 2 | Sensitivity : 60 % |  |
| ☐ | Window 3 | Sensitivity : 60 % |  |

Apply

Cancel



Note: You can adjust the motion detecting area by dragging the four corners to resize the window.

Motion Detection Window is a hot zone that the camera analyzes for motion (image changes). When a motion is detected within the zone an event will be triggered.

When the window is selected, use your mouse to move the window to the area you intend to monitor. There can be 3 windows at the most. The Windows are differentiated by color; Window 1 is Green, Window 2 is Red and Window 3 is Blue.

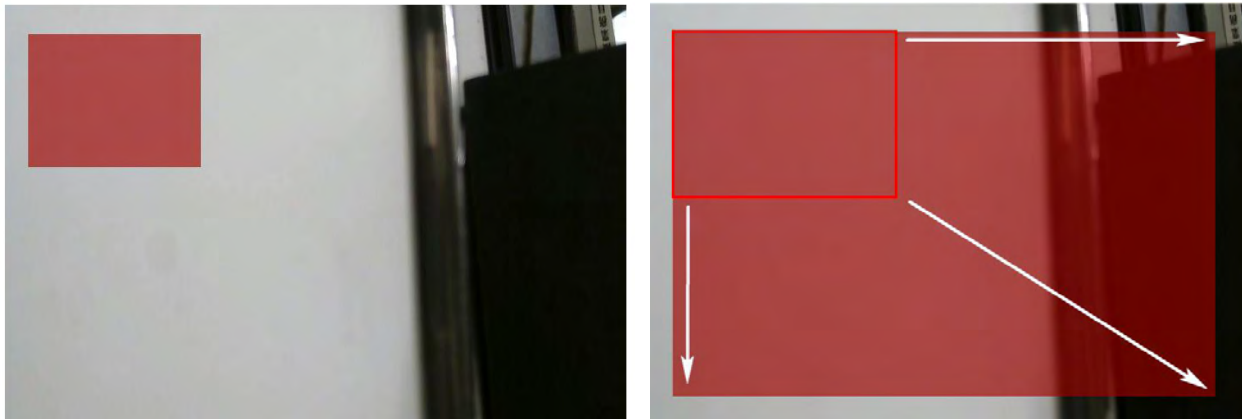
Video OSD Prompt displays the warning on the top left of the live view page when motion triggered.

Uncheck the window to remove the window from the view.

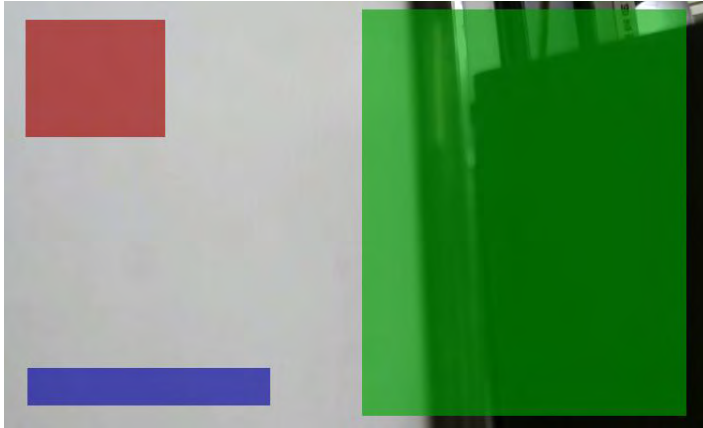
Sensitivity: Level 0% to Level 100% (with Level 100% being the most sensitive)

Depends on your application, high sensitivity will trigger event more often than low sensitivity and produce more snapshots or videos. However, overly sensitive events will fill up the storage very quickly. Even if you have unlimited storage space, large amount of files can become a problem when you need search through each of the files to find what you are really looking for. It may take some time for you to fine tune the optimal sensitivity for your application.

You can adjust the motion detecting area by dragging the four corners to resize the window.



Therefore, you can have a combination of three different detection window sizes.



Audio Detection

Sensitivity Level: 0% to 100% (with 100% being the most sensitive)

Similar to motion detection, high sensitivity will trigger events more often than low sensitivity and produce more snapshots or videos. However, over-sensitive events will fill up the storage very quickly. Even if you have unlimited storage space, large amount of files can become a problem when you need to search through each of the files to find what you are really looking for. It may take some time for you to fine tune the optimal sensitivity for your application.

Audio Detection Settings

Sensitivity Level  60 %

Tampering Detection

Tamper detection is a setting within your IP camera that will send you an alert when the camera is tampered with. Once an action has been detected, whether it's someone trying to knock the camera down or blocking its view, the alert lets you know to log into the actions to see what happened.

Video OSD Prompt displays the warning on the top left of the live view page when motion triggered.

Sensitivity Level: Level 0% to Level 100% (with Level 100% being the most sensitive)

Depends on your application, high sensitivity will trigger event more often than low sensitivity and produce more snapshots or videos. However, overly sensitive events will fill up the storage very quickly. Even if you have unlimited storage space, large amount of files can become a problem when you need search through each of the files to find what you are really looking for. It may take some time for you to fine tune the optimal sensitivity for your application

Tampering Detection Settings

Video OSD Prompt ☒ Enable ☐ Disable
Sensitivity Level  60 %

Event Action

This page provides **Event**-related settings.

Event Action/Buffer Duration until Next Event: can set 20sec(s), 30sec(s), 1min(s), 5min(s), 10min(s), if you set 20sec(s) for this item, system will ignore any trigger during this 20sec(s).

Event Snapshot/Snapshot Duration: can set 10sec(s), 20sec(s), if you set 10sec(s) for this item, system will send a snapshot in every 10sec(s).

Event Recording Stream Type: H.264 (1920x1080) or H.264 (640x360)

Video Length: the maximum video length of time per file

Detectors Pre-event Buffer: the length of pre-event time (0~5 seconds)

Record Duration: the length of recording time when alarm is triggered.

Event Action

Buffer Duration Until Next Event

Event Snapshot

Snapshot Duration

Event Recording

Video Format

Stream Type

Time

Video Length

Detectors

Pre-event Buffer

Record Duration

Apply

Cancel

Note:

If setting **Buffer Duration Until Next Event** to 30 seconds, the camera will keep recording for 30 seconds when event is triggered. In this case, if the **Video Length** is 10 seconds, then 3 files will be generated for single instance of event. If **Video Length** is 30 seconds, then only 1 file will be generated. Please note that pre-event buffer will extend the length of the video clip for the chosen extra length of time.

Chapter 17 **Event Server**



Network Storage

It is required for users to configure **Event Server** settings before setting camera **Event** or **Schedule Recording**. You will have to tell **where** the captured images or clips are going to be stored. The following concept diagram depicts the flow of the image file when and when captured. The file is stored at one of the predefined storage locations.

Network Storage and FTP are required to have existing servers ready for upload. **SMTP** is good for small image capture since it sends the file through email. You should choose what is best for your application.

This camera supports two types of Network Storage: **NFS** and **SAMBA**.

Before going further, you need to **Enable** to configure the network storage first.

Network Storage Settings

Status

☐ Enable ☒ Disable

Please refer to the following sections for **NFS** and **SMABA**.

NFS (Network File System)

Network Storage Settings

Status	☒ Enable ☐ Disable
Protocol	Network File System (NF)
Server	
Path	 (insert / if the path contains the subfolder, i.e. folder/subfolder)
Storage Size	---
Folder Size	GB (Integer only. 0 is no limit.)
☒ Overwrite	

Server: IP address of the NFS server

Path: enter the initial path if applicable

Folder Size: storage allocated for the camera; the default value 0 signifies infinity.

Overwrite: when the defined folder is full, the oldest files will be overwritten to accommodate the new one.

Click **Apply** when done.

SAMBA

Network Storage Settings

Status	☒ Enable ☐ Disable
Protocol	SAMBA
Server	
Path	/ (insert / if the path contains the subfolder, i.e. folder/subfolder)
Username	
Password	
Storage Size	---
Folder Size	0 GB (Integer only. 0 is no limit.)
☒ Overwrite	

Server: IP address of the SAMBA server

Path: enter the initial path if applicable

User Name: username for accessing SAMBA server

Password: password for accessing SAMBA server

Folder Size: storage allocated for the camera; the default value 0 signifies infinity.

Overwrite: when the defined folder is full, the oldest files will be overwritten to accommodate the new one.

Click **Test** to verify the connection with the server using the username and password. Click **Apply** when done.

FTP(File Transfer Protocol)

FTP Settings

Server IP address		e.g. 192.168.0.100
Port	21	
Username		
Password		
FTP Path	/	(insert / if the path contains the subfolder, i.e. folder/subfolder)

Server: IP address of the FTP server

Port: the FTP server port; default 21

User Name: username for accessing FTP server

Password: password for accessing FTP server

FTP Path: enter the initial path if applicable

Click **Test** to verify the connection with the server using the username and password.

Click **Apply** when done

E-Mail

E-mail SMTP Settings

Please refer to the settings from your email service provider to configure correctly.

Email Service Provider	Manual	
SSL/TLS	None	
SMTP Server		
Port	25	
Account		e.g. user@domain.com
Password		
From		e.g. user@domain.com
To		e.g. user1@domain.com,user2@domain.com
		Note: If you'd like to add multiple recipients, simply separate each email with a comma.
Subject	EWS1025 IPCam Alert	

EWS1025CAM allows camera to send captured images to the predefined email box to notify about an event or alarm.

SMTP is an email sender's server. You need to check whether your email service provider supports SMTP and obtain the required information for this setting.

Email Server Provider: supported Gmail, Yahoo and Hotmail.

SSL/TSL: select the type of the authentication as Transport Layer Security (TLS) protocol or Secure Sockets Layer (SSL) protocol

SMTP Server: enter the SMTP server address (e.g. smtp.gmail.com).

Port: enter SMTP server port (normally 587 or 465)

Account: the email account name; if your email is myemail@gmail.com, **myemail** is the account name.

Password: the password you use to login into your email box.

From: you can type in your email address or other address if you would like the receiver to reply the email to.

To: enter the receiver email here (usually your or the administrator's email).

Subject: enter the email subject here.

Chapter 17 **Storage Info**



Storage Info

System will display the storage information on this page; it includes the network storage status, total size and available size. User can click the "Refresh" button to get the latest information of these information.

Storage Info

	Status	Total Size	Available Size		
SD Card	Ready	15.30 GB	15.28 GB	Dismount	Format
Network Storage	Ready	100.00 GB	11.22 GB		

Refresh

Name	Size	Last Modified	Action
			
 tmp	---	2015/09/25 15:08:06	Delete
 timelapse-20150925-1343.avi	10123K	2015/09/25 14:49:16	Delete
 timelapse-20150925-1402.avi	8999K	2015/09/25 15:08:28	Delete

It depends on different browsers, user can double click the mouse on the records of .avi or .jpg file to save and view the video or snapshot.

This camera supports **MicroSD** card slot. Please be careful when choosing the SD card type. You need to insert a blank SD card into the slot as shown below. It may take a few seconds for the camera to recognize the inserted SD card.

You will be seeing the file list after inserted the SD card. If not, refresh the page by clicking on **Refresh** button and double check if the Micro SD card has been properly inserted into the slot.

Dismount: you should dismount the SD card before physically removing it from the slot to avoid file damage.

Format: You can clean a SD card by formatting it (all data will be erased).

You can browse through the folder like any other file manager by clicking on the folder name.
Click on the files to view it directly as shown below.

Name	Size	Last Modified	Action
 ..			
 tmp	---	2015/09/25 15:08:06	Delete
 <u>timelapse-20150925-1343.avi</u>	10123K	2015/09/25 14:49:16	Delete
 <u>timelapse-20150925-1402.avi</u>	8999K	2015/09/25 15:08:28	Delete

Appendix



Appendix A - FCC Interference Statement

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.



FCC Caution:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. Operations in the 5.15-5.25 GHz band are restricted to indoor usage only.

IMPORTANT NOTE:

Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed

and operated with a minimum distance of 21 cm between the radiator & your body.

Appendix B - CE Interference Statement

Europe – EU Declaration of Conformity

- **EN60950-1**
Safety of Information Technology Equipment
- **EN50385**
Generic standard to demonstrate the compliance of electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (0 Hz - 300 GHz)
- **EN 300 328**
Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- **EN 301 893**
Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive
- **EN 301 489-1**
Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- **EN 301 489-17**
Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 5GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

C€0560!

 Český [Czech]	<i>[Jméno výrobce]</i> tímto prohlašuje, že tento <i>[typ zařízení]</i> je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
 Dansk [Danish]	Undertegnede <i>[fabrikantens navn]</i> erklærer herved, at følgende udstyr <i>[udstyrets typebetegnelse]</i> overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
 Deutsch [German]	Hiermit erkläre <i>[Name des Herstellers]</i> , dass sich das Gerät <i>[Gerätetyp]</i> in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
 Eesti [Estonian]	Käesolevaga kinnitab <i>[tootja nimi = name of manufacturer]</i> seadme <i>[seadme tüüp = type of equipment]</i> vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
 English	Hereby, <i>[name of manufacturer]</i> , declares that this <i>[type of equipment]</i> is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
 Español [Spanish]	Por medio de la presente <i>[nombre del fabricante]</i> declara que el <i>[clase de equipo]</i> cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ <i>[name of manufacturer]</i> ΔΗΛΩΝΕΙ ΟΤΙ <i>[type of equipment]</i> ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EK.
 Français [French]	Par la présente <i>[nom du fabricant]</i> déclare que l'appareil <i>[type d'appareil]</i> est conforme aux

	exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
 Italiano [Italian]	Con la presente <i>[nome del costruttore]</i> dichiara che questo <i>[tipo di apparecchio]</i> è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo <i>[name of manufacturer / izgatavotāja nosaukums]</i> deklarē, ka <i>[type of equipment / iekārtas tips]</i> atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo <i>[manufacturer name]</i> deklaruoją, kad šis <i>[equipment type]</i> atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
 Nederlands [Dutch]	Hierbij verklaart <i>[naam van de fabrikant]</i> dat het toestel <i>[type van toestel]</i> in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
 Malti [Maltese]	Hawnhekk, <i>[isem tal-manifattur]</i> , jiddikjara li dan <i>[il-mudel tal-prodott]</i> jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Direttiva 1999/5/EC.
 Magyar [Hungarian]	Alulírott, <i>[gyártó neve]</i> nyilatkozom, hogy a <i>[... típus]</i> megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
 Polski [Polish]	Niniejszym <i>[nazwa producenta]</i> oświadczam, że <i>[nazwa wyrobu]</i> jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
 Português [Portuguese]	<i>[Nome do fabricante]</i> declara que este <i>[tipo de equipamento]</i> está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
 Slovensko [Slovenian]	<i>[Ime proizvajalca]</i> izjavlja, da je ta <i>[tip opreme]</i> v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	<i>[Meno výrobcu]</i> týmto vyhlasuje, že <i>[typ zariadenia]</i> spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
 Suomi [Finnish]	<i>[Valmistaja = manufacturer]</i> vakuuttaa täten että <i>[type of equipment = laitteen tyyppimerkintä]</i> tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
 Svenska [Swedish]	Härmed intygar <i>[företag]</i> att denna <i>[utrustningstyp]</i> står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.