EnGenius

Datasheet

EnGenius Fit Switches

EnGenius Fit Managed Switch Series

Optimal Performance, Enterprise Features & Robust Management Options

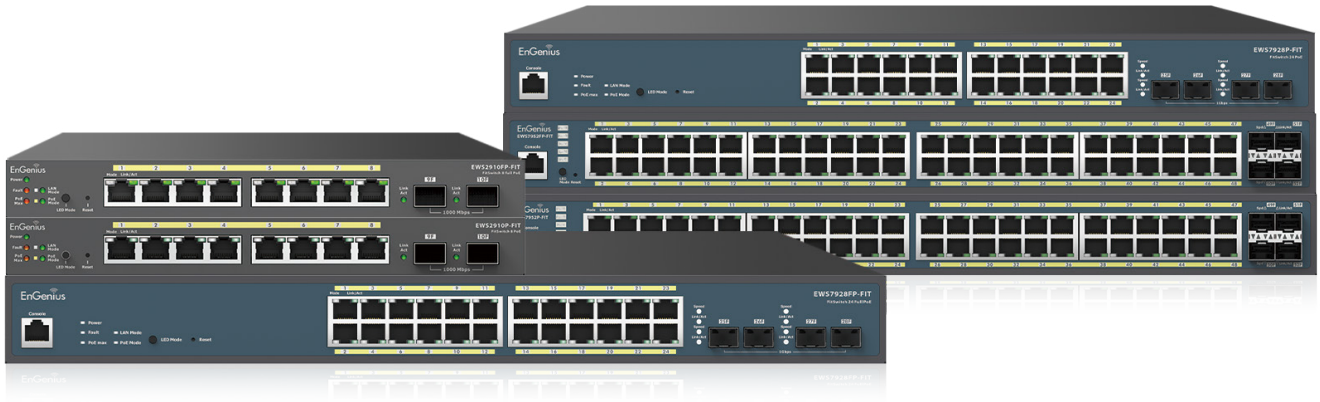
EnGenius Fit Switch Series offers enterprise-level features, simplified network configuration, monitoring, and diversified management options with optimal performance for different scales of organizations.

For ease of deployment, this can be addressed by selecting 8, 24, or 48 Gigabit Power-over-Ethernet ready layer-2+ switches with SFP Slots ports where the EnGenius Fit Managed Switch models also include desktop or rack mountable options with fanless or smart fan designs.

EnGenius Fit Managed Gigabit Switches can be managed remotely with FitXpress or on-premises management with FitController. All the switches support easy deployment and easy setup to create a reliable, efficiently managed network from scratch.

Features & Benefits

- Manage devices of multiple sites with FitXpress and manage up to 100 EnGenius APs or Switches with FitController
- A wide range of PoE/PoE+ switches that support 802.3af/at on all ports, supporting PoE budgets from 55W to 740W
- Up to Four SFP fiber ports with 1-Gigabit speed to extend connectivity via fiber uplinks, redundancy, and failover
- Security: Access Control List/Port Security; 802.1X & RADIUS Authentication
- Advanced QoS with IPv4/IPv6 ingress traffic filtering (ACLs) & prioritization
- IGMP and MLD snooping provides advanced multicast filtering
- 802.3ad Link Aggregation (LACP) supports traffic load balancing
- Dual firmware images improves reliability & network uptime
- FitXpress app or web enable users to configure devices quickly and monitor the installed or deployed devices on their smartphones or tablets.
- FitController, the plug-and-play hardware for on-premises, empowering you to monitor, manage, and troubleshoot locally.



Benefits to Help Grow Your Business

SFP Slots for Flexible Deployments

The switch's SFP Slots options connect wired network segments throughout buildings extending beyond the limitations of Ethernet cabling. By reducing delays, businesses experience more consistent and uninterrupted communications.

Maximum Power Supply Capabilities with 802.3at

By providing a wide range of PoE/PoE+ models that support 802.3af/at on all ports, companies can regulate power budgets according to device requirements and remotely power cycle individual ports, the 802.3at standard of EnGenius switches delivers up to 30W of power to optimize the power management.

Increased Access Control and Security

Protect the network with 802.1X port-based client authentication with dynamic VLAN and security through a RADIUS server. Utilizing administrators can use Access Control Lists (ACLs) to see who has access to network segments while screening traffic from unauthorized MAC or IP addresses. By establishing a guest VLAN to grant and limit Internet resources for visitors, guests can use the network while also keeping the network secure.

Improved VLAN/Voice and Quality of Service

Segment the network by departments or traffic types for increased performance and security with 802.1Q VLAN statically or dynamically. While 802.1p class of service prioritizes compliant VoIP and video traffic ensuring bandwidth intensive, time-sensitive data is forwarded immediately for clear, smooth voice and video delivery.

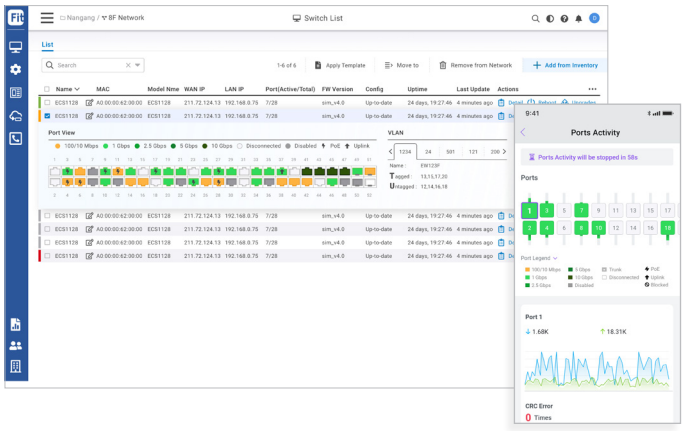
Network Traffic Management

EnGenius Fit Switches offer performance-enhancing features that reduce multicasting traffic, speed up port blocking and port forwarding, and increase bandwidth via load balancing. Control each port's available bandwidth speeds for connected devices like APs in areas where more or less speed is needed, such as in lobbies or conference rooms.

Easy Network Management

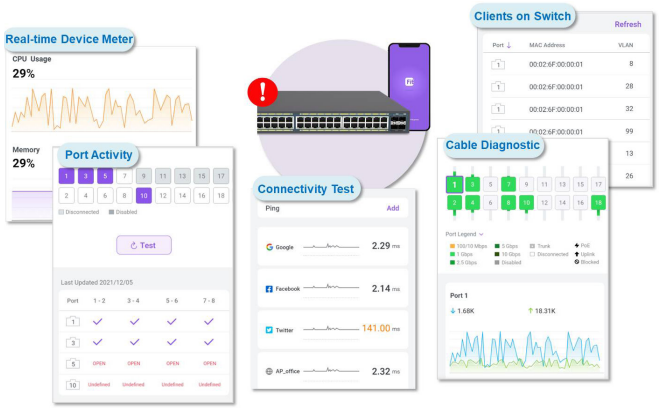
In-Depth Network Visibility

The EnGenius Fit Switches achieve network management and visibility, network topology view automatically maps the network deployment to display device relationships across the infrastructure. It can monitor The network's performance by viewing port statistics, system logs, and RMON data and viewing wired and wireless traffic via a comprehensive at-a-glance dashboard and get rich analytics and reporting.



Easy Monitoring & Troubleshooting

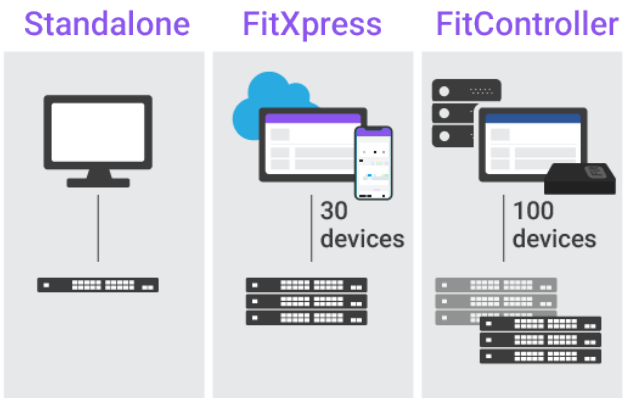
The EnGenius Fiton-premises management establishes the event based email alerts for notification of predetermined activities. It can and perform port diagnostics through ping tests and diagnose cable failure and trace the route data takes through the network to troubleshoot slowdowns or connection issues, that enabling troubleshoot issues without manual tracking, and access the management interface of other EnGenius Fit Switches directly from topology view with quick link.



Easy Network Management

Flexible Deployment with Multiple Management Modes

By using multiple methods to manage switches, EnGenius decreases administration time through remote management, visibility, and troubleshooting. Select the most effective management approach based on network architecture, administrative permissions, technical aptitude, or even budget.



Standalone Management

Each EnGenius EnGenius Fit Switch can be managed in a standalone setup from its intuitive user interface that provides full access into all the Layer 2+ switching features.

Smart and Remote Management with FitXpress

FitXpress offers an easy-to-use and secure Wi-Fi solution with the mobile app or web portal interface for businesses with fewer IT resources or multiple locations to manage. In addition, FitXpress contains easy Wi-Fi setups, comprehensive and intuitive interface, and handy Troubleshooting tools.

On-Premises Management with FitController

EnGenius Fit solution can manage up to 100 EnGenius switches with FitController, a plug-and-play and feature-rich hardware to empower you to monitor, manage, and troubleshoot locally, providing on-premises and subscription-free remote access capability.

Software Lists of Layer 2-Plus Managed Switches

Layer 2 Features

DHCP Snooping
DHCP snooping is a layer 2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. The fundamental use case for DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients.

DHCP Relay
A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet.

DHCP Option 82
DHCP option 82 provides additional security when DHCP is used to allocate network addresses. It enables the switch to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources.

PoE (Power over Ethernet)
Power over Ethernet (POE) is a technology that lets network cables carry electrical power. POE switch is a network switch that has Power over Ethernet injection built-in. Simply connect other network devices to the switch as normal, and the switch will detect whether they are POE-compatible and enable power automatically.

EEE (Energy Efficient Ethernet)
Energy Efficient Ethernet (EEE) reduces the power consumption of physical layer devices during periods of low link utilization. EEE saves energy by allowing PHY non-essential circuits shut down when there is no traffic.

Link Aggregation
A Link Aggregation Group (LAG) optimizes port usage by linking a group of ports together to form a single, logical, higher-bandwidth link. Aggregating ports multiplies the bandwidth and increases port flexibility for the Switch.

STP (Spanning Tree Protocol)
The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between Switches.

LBD (Loopback Detection)
Loopback Detection (LBD) is a feature on the switch that provides protection against loops by transmitting loop protocol packets out of ports where loop protection has been enabled. When the switch sends out a loop protocol packet and then receives the same packet, it shuts down the port that received the packet.

Jumbo Frame
Jumbo frames are network-layer PDUs that have 10000 bytes larger enough to carry an 8 KB application datagram plus packet header overhead. It needs to be configured to work on the ingress and egress port of each device along the end-to-end transmission path.

MAC Address Table
The MAC address table contains address information that the Switch uses to forward traffic between the inbound and outbound ports. All MAC addresses in the address table are associated with one or more ports.

LLDP (Link Layer Discovery Protocol)
Link Layer Discovery Protocol (LLDP) is essentially a neighbor discovery protocol that uses Ethernet connectivity to advertise information to devices on the same LAN and store information about the network. This information allows the device to quickly identify a variety of other devices, resulting in a LAN that interoperates smoothly and efficiently.

IGMP Snooping
Internet Group Management Protocol (IGMP) Snooping allows a Switch to forward multicast traffic intelligently. A Switch supporting IGMP Snooping can passively snoop on IGMP Query, Report, and Leave packets transferred between IP Multicast switches and IP Multicast hosts to determine the IP Multicast group membership.

MLD Snooping
Multicast Listener Discovery (MLD) Snooping operates on the IPv6 traffic level for discovering multicast listeners on a directly attached port and performs a similar function to IGMP Snooping for IPv4. MLD Snooping limits IPv6 multicast traffic by dynamically configuring the Switch port so that multicast traffic is forwarded only to those ports that wish to receive it. This reduces the flooding of IPv6 multicast packets in the specified VLANs.

Multicast Filtering
Multicast is a form of communication that allows multiple transmissions of multimedia and streaming data to specific recipients at the same time. Multicast Filtering feature lets you sort out selective multiple transmissions for

VLAN Features

802.1Q VLAN
A Virtual LAN (VLAN) is a group of ports that form a logical Ethernet segment on a Layer 2 Switch which provides better administration, security, and management of multicast traffic. A VLAN is a network topology configured according to a logical scheme rather than a physical layout. When you use a VLAN, users can be grouped by logical function instead of physical location.

PVID (Port VLAN ID)
When an untagged packet enters a Switch port, the PVID (Port VLAN ID) will be attached to the untagged packet and forward frames to a VLAN specified VID part of the PVID. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port that corresponded to the packet's destination address.

Voice VLAN
Enhance your Voice over IP (VoIP) service by configuring ports to carry IP voice traffic from IP phones on a specific VLAN. Voice VLAN provides QoS to VoIP, ensuring that the quality of the call does not deteriorate if the IP traffic is received erratically or unevenly.

Software Lists of Layer 2-Plus Managed Switches

VLAN Features

MAC based VLAN*
The MAC-based VLAN feature allows incoming untagged packets to be assigned to a VLAN and thus classify traffic based on the source MAC address of the packet. You define a MAC to VLAN mapping by configuring an entry in the MAC to VLAN table. An entry is specified using a source MAC address and the appropriate VLAN ID. The MAC to VLAN configurations are shared across all ports of the device.

Protocol VLAN*
A protocol-based VLAN processes traffic based on protocol. You can use a protocol-based VLAN to define filtering criteria for untagged packets. The smart switch always processes tagged packets according to the 802.1q standard and does not forward them to protocol-based VLANs.

VTP advertisement
VLAN Trunk Protocol (VTP) reduces administration in a switched network. Once the VLAN Trunking Protocol (VTP) is configured on the switches, the switches start advertising VLAN Trunking Protocol (VTP) information between them on their trunk ports. This reduces the need to configure the same VLAN everywhere.

Dynamic VLAN assignment
Dynamic VLAN assignment are used by network admins/engineers to place a wireless user into a specific VLAN based on the credentials supplied by the user. This task of assigning users to a specific VLAN is handled by a RADIUS authentication server. Users in an organization are then segmented into these dynamic VLANs based on the resources they can access.

* Available through future firmware upgrade.

Quality of Service

Quality of Service
Quality of Service (QoS) provides the ability to implement priority queuing within a network. In a Switch, multiple queues per port are often provided to give preference to certain packets over others based on user-defined criteria. When a packet is queued for transmission within a port, the rate at which it is processed depends on how the queue is configured and the amount of traffic present within other queues on the port. If a delay is necessary, packets are held in the queue until they are authorized for transmission.

Class of Service (CoS)
Class of service is a parameter used in data and voice protocols to differentiate the types of payloads contained in the packet being transmitted. The objective of such differentiation is generally associated with assigning priorities to the data payload or access levels to the telephone call.

CoS Mapping
Use the Class of Service (CoS) Mapping feature to specify which internal traffic class to map to the corresponding CoS value. CoS allows you to specify which data packets have greater precedence when traffic is buffered due to congestion.

Differentiated Services Code Point (DSCP)
Differentiated services or DiffServ is a computer networking architecture that specifies a simple and scalable mechanism for classifying and managing network traffic and providing quality of service (QoS) on modern IP networks. Use Differentiated Services Code Point (DSCP) Mapping feature to specify which internal traffic class to map to the corresponding DSCP values. DSCP Mapping increases the number of definable priority levels by reallocating bits of an IP packet for prioritization purposes.

Weighted Round-Robin (WRR)
Weighted round robin (WRR) is a network scheduling discipline. Each packet flow or connection has its own packet queue in a network interface controller. In WRR mode the number of packets sent from the queue is proportional to the weight of the queue (the higher the weight the more frames are sent).

Bandwidth Management
Bandwidth management is the process of measuring and controlling the communications (traffic, packets) on a network link, to avoid filling the link to capacity or overfilling the link, which would result in network congestion and poor performance of the network. Bandwidth is measured in bits per second (bit/s) or bytes per second (B/s).

Security

Radius Server
RADIUS proxy servers are used for centralized administration. Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service for greater convenience.

802.1X Authentication Protocol
IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

802.1x Port-based Access Control
The IEEE 802.1X port-based authentication provides a security standard for network access control with RADIUS servers and holds a network port disconnected until authentication is completed. With 802.1X port-based authentication, the supplicant provides the required credentials, such as user name, password, or digital certificate to the authenticator, and the authenticator forwards the credentials to the authentication server for verification to the guest VLAN.

MAC-Based Port Security (MAC-based Access Control)
Network security can be increased by limiting access on a specific port to users with specific MAC addresses. Port Security prevents unauthorized device to the Switch prior to stopping auto-learning processing.

Authenticated Host
The Authenticated Host displays the Authenticated User Name, Port, Session Time, Authenticated Method, and Mac Address.

Guest VLAN
A Guest VLAN is a VLAN that allows guests to get in the network. For example, employees and guests can access the wireless network of a company at the same time and be administratively separate.

VLAN Tag
Independent VLAN setting can be enable or disable. Any packet that enters the Device without a VLAN tag will have a VLAN tag inserted with a PVID (Ethernet Port VID).

Radius VLAN Assignment
VLAN assignments build on the use of RADIUS to control access to the network. Via RADIUS integration, a WiFi access point (WAP) requires not only an SSID and passphrase, but a user's unique set of credentials to access the network. Once a user has passed credentials through to the WAP and they are subsequently passed to the RADIUS server and directory service, the RADIUS server will reply to the WAP that the user has been authenticated and inform what VLAN they are assigned to.

Management VLAN
Feature is enabled with specified VLAN ID, the device will only allow management access with the same specified VLAN ID from remotely location by using protocols such as telnet, SSH, snmp, syslog etc.

Storm Control
Storm Control limits the amount of Broadcast, Unknown Multicast, and Unknown Unicast frames accepted and forwarded by the Switch. Storm Control can be enabled per port by defining the packet type and the rate that the packets are transmitted at.

Port Isolation
Port Isolation feature provides L2 isolation between ports within the same broadcast domain. When enabled, Isolated ports can forward traffic to Not Isolated ports, but not to other Isolated ports. Not Isolated ports can send traffic to any port; whether Isolated or Not Isolated.

DoS Attack Prevention
Denial of Service attack is an attack on the computer or network that restricts, reduce or prevents system restore accessibility to its legitimate users. It is a kind of attack in which an attacker or intruder tries to deprive system users or authorized users of accessing their computers, networks or sites. Enable DoS Attach prevention feature to classifying and blocking specific types of DoS attacks.

Software Lists of Layer 2-Plus Managed Switches

Security

Access Control List
An Access Control List (ACL) allows you to define classification rules or establish criteria to provide security to your network by blocking unauthorized users and allowing authorized users to access specific areas or resources. ACLs can provide basic security for access to the network by controlling whether packets are forwarded or blocked at the Switch ports.

Login Authentication Control
Support SSH/Telnet command or HTTP/HTTPS login methods

Management

Account Multi-Privileges Management
Enable this function to control management access to the Switch based on manually configured user names and passwords. A User account can only view settings without the right to configure the Switch, and an Admin account can configure all the functions of the Switch.

HTTPS
A secure communication protocol can be enabled to allow secure management web access over a computer network.

SSH Tunnel
A secure communication protocol can be enabled to allow secure remote shell access or command execution.

Command Line Interface (CLI)
CLI protocol provides the basic rules for making it possible to link a client to a command interpreter. The Telnet service for the Switch is enabled by default. For secure communication, it is better to use SSH over Telnet.

SNMP & MIB
v1/v2c/v3 support
MIB I/II, Private MIB
CLI supported

Remote Network Monitoring (RMON)
Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more freedom in selecting network-monitoring probes and consoles with features that meet their particular networking needs.

PoE Management
The PoE Management function support Power on/off per port, Power class configuration, Power feeding priority adjustment feature to monitoring the current power usage and assigns the total amount of power the Switch can provide to all of its PoE ports.

PD LifeGuard
The switch can detect and monitor connected PoE IP cameras or PoE PD (Powered Device) status in real time. Once the PoE PD stops working and responding, switch will recover failed PoE PD device automatically. The PoE lifeguard function with customizable parameters enhance the reliability and suitable for any types of application scenarios.

Port Mirroring
Use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, detecting intrusions, monitoring and predicting traffic patterns, and other correlating events.

Syslog
The Syslog protocol allows devices to send event notification messages in response to events, faults, or errors occurring on the platform as well as changes in configuration or other occurrences across an IP network to syslog servers.

Ping
The Packet Internet Groper (Ping) test allows you to verify connectivity to remote hosts. The Ping test operates by sending Internet Control Message Protocol (ICMP) request packets to the tested host and waits for an ICMP response.

Trace Route
The trace route feature is used to discover the routes that packets take when traveling to their destination. It will list all the routers it passes through until it reaches its destination, or fails to reach the destination and is discarded.

Cable Diagnostics
Cable Diagnostics helps you to detect whether your cable has connectivity problems provides information about where errors have occurred in the cable.

Dual Image
The Switch maintains two versions of the Switch image in its permanent storage. One image is the active image, and the second image is the backup image. The Dual Image screen enables the user to select which partition will be set as active after the next reset. The Switch boots and runs from the active image. If the active image is corrupt, the system automatically boots from the non-active image.

Firmware Update
Update switch throughout manually update
Update switch throughout one-click-update function

Configuration Backup/Restore
Backup overall setting of the switch. Users can restore this settings/configuration to one switch easily.

Reboot/Reset
Select to reboot or reset your switch under your application platform.

Switches Comparison Table

EnGenius Fit Switches			
			
Model Name	**FitSwitch 8 PoE**	**FitSwitch 8 Full PoE**	**FitSwitch 24 PoE**
Model Number	**EWS2910P-FIT**	**EWS2910FP-FIT**	**EWS7928P-FIT**
Switching Class	Layer 2+	Layer 2 +	Layer 2+
OS version	SNOS 2.0	SNOS 2.0	SNOS 2.0
Gigabit Ethernet Ports	8	8	24
SFP Ports	2	2	4
RJ45 Console Ports	-	-	1
Form Factor	Desktop	Desktop	19”1U
Power-over-Ethernet	802.3af	802.3af/at	802.3af/at
PoE Capable Ports	Ports 1-8	Ports 1-8	Ports 1-24
Total PoE Budget	55W	110W	240W
Switching Capacity (Gbps)	20Gbps	20Gbps	56Gbps
Full load Power consumption	63.72 Watts	119.45 Watts	283.88 Watts
Packet Buffer memory	512KB	512KB	512KB
Max. Packet Forwarding Rate (Mpps)	14.88Mpps	14.88Mpps	41.664Mpps
MAC Address Table Size	8K	8K	8K
Jumbo frame size	9K	9K	9K
Weight	0.6 kg	0.6 kg	3.6 kg
Dimensions	240mm x 105mm x 27mm	240mm x 105mm x 27mm	440mm x 260mm x 44mm
Operating Temp.	0 to 40°C	0 to 40°C	0 to 50°C
Storage Temp.	-20 to 70°C	-20 to 70°C	-20 to 70°C
Humidity	5% ~ 95%	5% ~ 95%	5% ~ 95%
Cloud-managed (FitXpress)	●	●	●
On-premises (FitController)	●	●	●
Standalone Mode	●	●	●

*Models vary depending on the region.

Switches Comparison Table

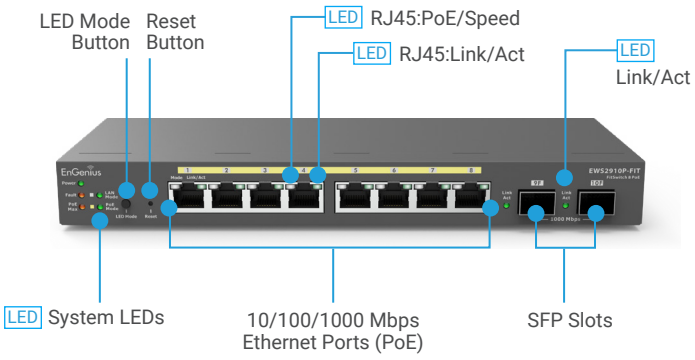
EnGenius Fit Switches			
			
Model Name	**FitSwitch 24 Full PoE**	**FitSwitch 48 PoE**	**FitSwitch 48 Full PoE**
Model Number	**EWS7928FP-FIT**	**EWS7952P-FIT**	**EWS7952FP-FIT**
Switching Class	Layer 2+	Layer 2+	Layer 2+
OS version	SNOS 2.0	SNOS 2.0	SNOS 2.0
Gigabit Ethernet Ports	24	48	48
SFP Ports	4	4	4
RJ45 Console Ports	1	1	1
Form Factor	19”1U	19”1U	19”1U
Power-over-Ethernet	802.3af/at	802.3af/at	802.3af/at
PoE Capable Ports	Ports 1-24	Ports 1-48	Ports 1-48
Total PoE Budget	410W	410W	740W
Switching Capacity (Gbps)	56Gbps	104Gbps	104Gbps
Full load Power consumption	470.5 Watts	430.2Watts	840.8 Watts
Packet Buffer memory	512KB	1.5MB	1.5MB
Max. Packet Forwarding Rate (Mpps)	41.664Mpps	77.376Mpps	77.376Mpps
MAC Address Table Size	8K	16K	16K
Jumbo frame size	9K	9K	9K
Weight	3.8 kg	6.4 kg	6.4 kg
Dimensions	440mm x 260mm x 44mm	440mm x 310mm x 44mm	440mm x 310mm x 44mm
Operating Temp.	0 to 50°C	0 to 50°C	0 to 50°C
Storage Temp.	-20 to 70°C	-20 to 70°C	-20 to 70°C
Humidity	5% ~ 95%	5% ~ 95%	5% ~ 95%
Cloud-managed (FitXpress)	●	●	●
On-premises (FitController)	●	●	●
Standalone Mode	●	●	●

*Models vary depending on the region.

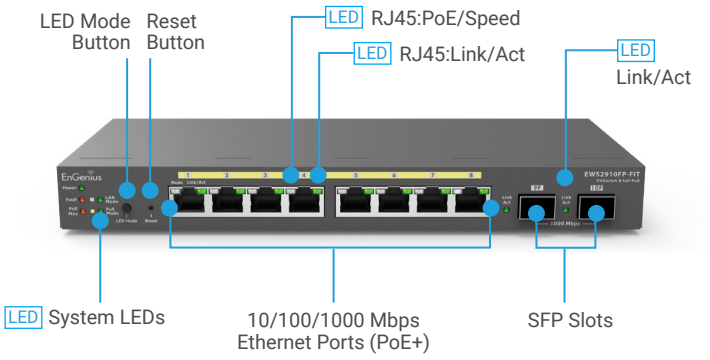
Product Views

EnGenius Fit Switches

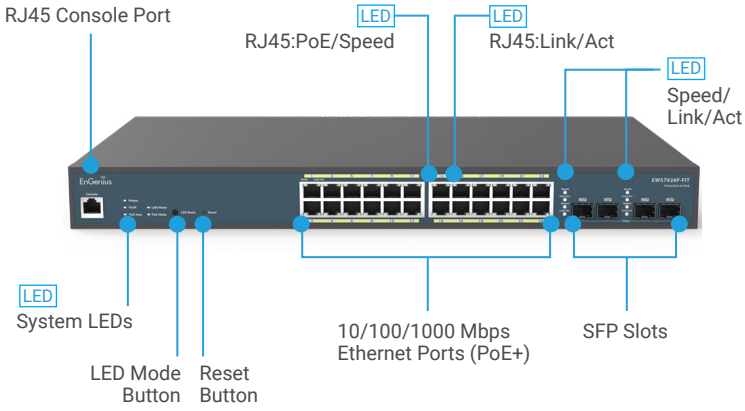
FitSwitch 8 PoE (EWS2910-FIT)



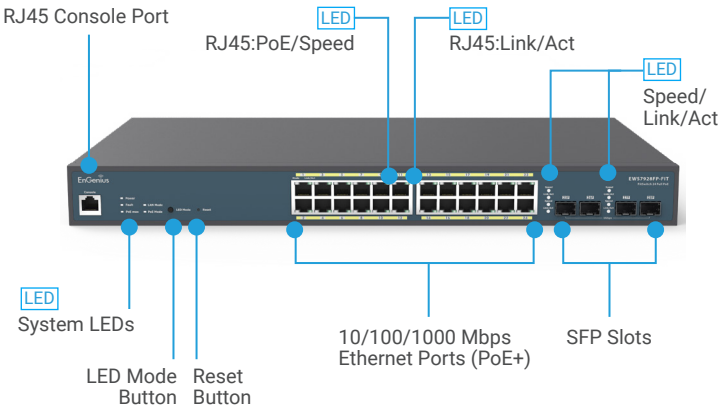
FitSwitch 8 Full PoE (EWS2910FP-FIT)



FitSwitch 24 PoE (EWS7928P-FIT)



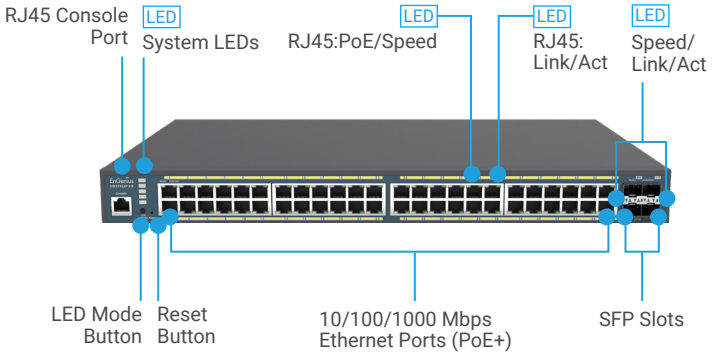
FitSwitch 24 Full PoE (EWS7928FP-FIT)



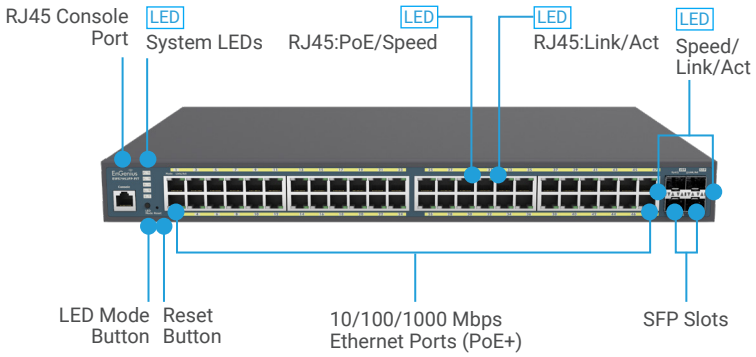
Product Views

EnGenius Fit Switches

FitSwitch 48 PoE (EWS7952P-FIT)



FitSwitch 48 Full PoE (EWS7952FP-FIT)



EnGenius Technologies | Costa Mesa, California, USA
Emaill: support@engeniustech.com
Website: www.engeniustech.com
Local contact: (+1) 714 432 8668

EnGenius Technologies Canada | Ontario, Canada
Email: support@engeniustech.com
Website: www.engeniustech.com
Local contact: (+1) 905 940 8181

EnGenius Networks Europe B.V. | Eindhoven, Netherlands
Email: support@engeniusnetworks.eu
Website: www.engeniusnetworks.eu
Local contact: (+31) 40 8200 887

EnGenius Networks Singapore Pte Ltd. | Singapore
Emaill: techsupport@engeniustech.com.sg
Website: www.engeniustech.com.sg
Local contact: (+65) 6227 1088

EnGenius Networks Dubai | Dubai, UAE
Emaill: support@engenius-me.com
Website: www.engenius-me.com
Local contact: (+971) 4 339 1227

恩碩科技股份有限公司 | Taiwan, R.O.C.
Email: support@engeniustech.com.tw
Website: www.engeniustech.com.tw
Local contact: (+886) 2 2652 1808