



## **D-Link DGS-3630-28PC/SI/E network switch Managed L3 Gigabit Ethernet (10/100/1000) Power over Ethernet (PoE) Black, Grey**

Model: DGS-3630-28PC/SI/E

Manufacturer: D-LINK

EAN: 790069472299

Product Code: 1037433

---

## **R67,141**

---

## **Outperforming the competition**

The DGS-3630-28TC was benchmarked against a market leading competitor's device. It matched or exceeded the competitor's performance across all tests despite being significantly lower in price with

---

The product information provided is for reference purposes only. Technical specifications, photos, descriptions and prices may change without prior notice. The manufacturer and seller are not responsible for possible data discrepancies or typographical errors. We recommend checking the current information before purchasing.

shop.cssi.co.za | sales@cssi.co.za | +27 (11)541-9950

a much lower power consumption.

## **Versatile Management**

The DGS-3630 Series provides:

- Network Assistant Utility
- Industry-standard CLI
- Intuitive web-based management interface

Support for SNMP allows centralized management of a large number of devices and out-of-band management is available via a dedicated console port.

A mini-USB console port allows the DGS-3630 Series to be managed without any extra connectors, and a USB Type A port can be used to store logs, configuration, and firmware images.

## **High Availability and Flexibility**

Includes stacking technology, which allows multiple switches to be combined to form a single physical or virtual stack.

Scale your network using just a stacking cable and without the need for stacking modules.

Increased redundancy over multiple physical units, simplifies management and provides a single IP address to manage all members in the stack.

## **Security, Performance & Availability**

Robust set of QoS features helps ensure that critical network services such as Voice over IP and video conferencing are given high priority through the network.

The D-Link Safeguard Engine increases the switch's reliability, serviceability, and availability by preventing malicious flooding traffic caused by worms or virus attacks.