

## Features

- GUI ease-of-use with web-based access convenience
- HTTPS web security via SSL and TLS protocols
- Support for industry-standard web browsers
- Uses standard MNS-6K CLI commands and features
- Included in MNS-6K for all 6K-Series Switches



The Magnum™ Secure Web Manager (SWM) offers users a safe and secure method for accessing mission-critical Magnum Switches from the convenience of a web browser. SWM is an embedded web site residing in Flash memory within a Magnum 6K-Series Switch that monitors switch activity and supports changing configuration settings from a web browser. SWM's graphical user interface (GUI) allows users to make requests and changes in HTML, which is then translated into Command Line Interface (CLI) commands that are recognized by the 6K Switches. The SWM defaults to HTTPS, a secure form of the HTTP web interface, that utilizes authentication and encryption to ensure that only authorized users have access to the switches.

Network managers have legitimate concerns regarding web access to critical LAN switches. Attempted attacks via the web have become common, and password protection is not robust enough for most applications. Nonetheless, technology for highly-secure web used does exist, and it is protecting millions of financial funds transfers and credit card transactions daily. The Magnum Secure Web Manager uses the same proven technologies, SSL (Secure Socket Layer) and TLS (Transport Layer Security), to provide secure web access for mission-critical applications for MNS-6K users.

SWM allows authorized users to browse pages that display current MNS-6K software settings, and provides access to graphical images of the 6K's port configurations, port statistics, and utilization figures. An Event Log provides operating history. Authorized users may specify configuration changes to be made using tools such as forms, lists that can be modified, and check-boxes. Changes become part of the current MNS-6K settings when the "Apply" button is clicked.

SSL and TLS provide communications privacy over the Internet, preventing eavesdropping, tampering, promiscuous snooping, and message forgery. They run above TCP/IP, but below application protocols, providing the encryption / decryption processes needed to transform HTTP web access into secure HTTPS web access. Using public-key encryption, an SSL-enabled client and an SSL-enabled server can confirm each other's identity and establish an encrypted connection, thus providing the convenience of web access without compromising security in mission critical applications.