Secure Management Agent (SMA)
Model RSP-1890

Overview

The Secure Management Agent (SMA) provides secure access to network management tools over an IP network. It is capable of securing several network management protocols including converting unsecured SNMPv1 to SNMPv3 and providing SSL encryption of Human Machine Interfaces (HMI) (e.g., Telnet sessions, web configuration tools, etc.). The SMA can access multiple management tools simultaneously allowing an administrator to customize SNMP signaling with additional alarms from HMI ports.

The SMA hardware unit includes an embedded firewall with physical network separation to protect unsecured element managers. The unit's cloud based design allows viewing of management tools over any web browser (e.g., Internet Explorer, Firefox, Chrome).

Features

- Converts SNMPv1 or v2 into secure SNMPv3 protocol

- Secures Human Machine Interfaces for remote monitoring and control

- Allows customization of SNMP signaling with inclusion of alarms from other network management tools (e.g., Telnet sessions, web configuration tools, etc.)

- Management tool can be viewed with any web browser

- Embedded firewall with physical network separation

- Multi-level user access and SSL certification

- Includes automatic hardware failover and alerts

SMA Concept of Operations

Operational/ Technical Specifications

Protocol Conversion
Converts SNMPv1 or v2 into SNMPv3

Converts Telnet or HTTP into HTTPS

Hardware-based Design
Dual motherboards for physical separation between external network and managed device

Dual AC power supplies for uninterrupted use

Hardware-based design isolates SMA processing from other site functions

Dual Ethernet 10/100 Base-T ports for LAN and local access

Console Port (DB-9) for Hyper Terminal access

Web-based configuration tool for SMA management

1/2 of 1U rackmount space with optional double unit 19 inch tray

Powered by 85-264, 50-60Hz VAC

Power fail safe to warn administrator of site power failure

Security
Automatic login to SMA with access to RADIUS authentication

User authentication with lockout after user-defined number of failed attempts

Multi-level user access, i.e., Administrator, Maintenance, Monitor

Embedded Firewall

SSL encryption for data transfer

Upload of SSL certificates

Customization
Create custom SNMP signals from Telnet sessions or web configuration tools

SMA design allows for easy configuration for other hardware