MANAGE ALL YOUR WEB CONFIGURATION INTERFACES FROM A SINGLE SCREEN

The Secure Multi-web Remoting Tool (SMRT) automatically monitors the web-based configuration tools of a large number of devices and displays status changes and alarms on a single screen. The device status and alarms are also transmitted to a Network Management System (NMS) via SNMPv3 for centralized monitoring and control.

The SMRT display provides at-a-glance status indication of each individual device and allows operators to "drill down" to the web configuration screen of each individual device. Among the many benefits of the SMRT is its simplicity and ability to reduce the man-power needed to manage a large number of devices thus providing a highly reliable network at **significantly lower operating costs**.


SMRT Management Screen

- Automatically monitors web configuration tools for status changes and alarms.

- One SMRT unit can monitor up to 64 devices. Several SMRT units can be linked for a larger network.

- SMRT manager can be viewed with any web browser and requires no local install.

- SNMPv3 traps of status changes and alarms sent to a Network Management System (NMS).

- Hardware-based design simplifies installation and protects SMRT processing.

- Embedded firewall with multi-level user access and PKI authentication.

- Command Enable switch provides physical prevention of remote access to SMRT.

- Allows incorporation of any device with a web configuration screen.

- Only one external IP address required to host up to 64 local devices.

SMRT Unit Occupies 1/3 of 1U Rack-Mount Space

SMRT Concept of Operations
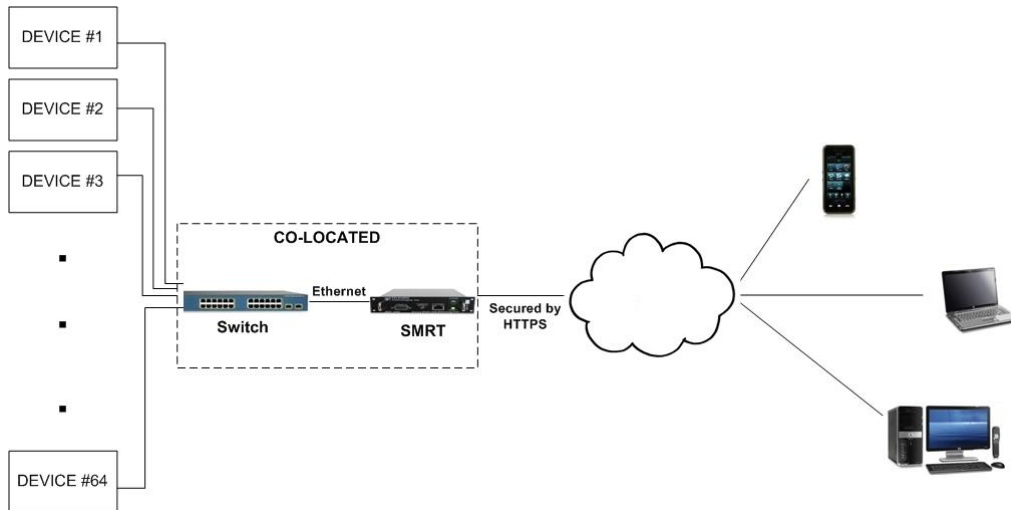
The SMRT has been deployed worldwide by the Defense Information Systems Agency (DISA)

Cryptography	
FIPS 140-2 Level 1 Compliance	Yes
Public / private key pair generation / certificate signing request	Yes
Symmetric Key Cryptography	Yes
Hashing	Yes
Random Number Generation	Yes
Protocols	
HTTPS	Yes
IPSec	Yes
TLS (version 1.1 minimum per NIST SP 800-52)	Yes
SSH (v2)	Yes
NTPv3 / v4 compliant	Yes
SNMPv3 / v2c / v1	Yes
Syslog	Yes
Public Key Infrastructure (PKI)	
Supports Multiple Public Key Infrastructures	Yes
Certificate revocation checking (OCSP and CRL)	Yes
Supports PKI-based Two Factor authentication (CAC)	Yes
Authentication, Authorization, Accounting (AAA)	
Supports Centralization Authentication and Authorization (RADIUS)	Yes
Multi-level user access (Administrator, Maintenance, Monitor)	Yes
802.1x Support	Yes
Auditing	
Audit log / trail	Yes