GUARDIAN SERIES 3

Centralized Management Platform

Centralized Cryptographic Infrastructure Management

Enterprise Management Capabilities and Business Insights for your Data Security Ecosystem

Ensuring a secure and reliable cryptographic infrastructure requires constant attention and adaptation to ever-changing throughput rates, emerging compliance mandates, and expanding functional requirements that incorporate a wide range of hardware security modules, key management servers, and more. Typically, management of these devices requires multiple administrators and key officers to regularly visit each device, often spread between geographically dispersed data centers. The Guardian Series 3 brings centralized management, monitoring, load balancing, audit logging, and reporting to your environment, giving you the freedom to focus on other priorities while complex cryptographic device management tasks are greatly reduced or even eliminated altogether.

The Guardian's robust monitoring engine tracks vital information for managed devices and groups in real-time. Fully customizable notifications delivered via SMTP, SNMP, SMS, and syslog let administrators oversee infrastructure health and gain actionable insights. Administrators can even customize and view graphical reports and analyses.

Endless access, exactly when you need it

The Guardian allows authorized users to centralize management of Futurex devices through synchronous peering and remote configuration, making in-person physical management of your cryptographic infrastructure virtually obsolete.

- CENTRALIZED MANAGEMENT OF FUTUREX DEVICES
- CUSTOMIZED ALERTING AND NOTIFICATIONS
- KEY AND CERTIFICATE REPLICATING FOR HIGH AVAILABILITY
- AUDIT LOG REPOSITORY FOR ALL MANAGED DEVICES

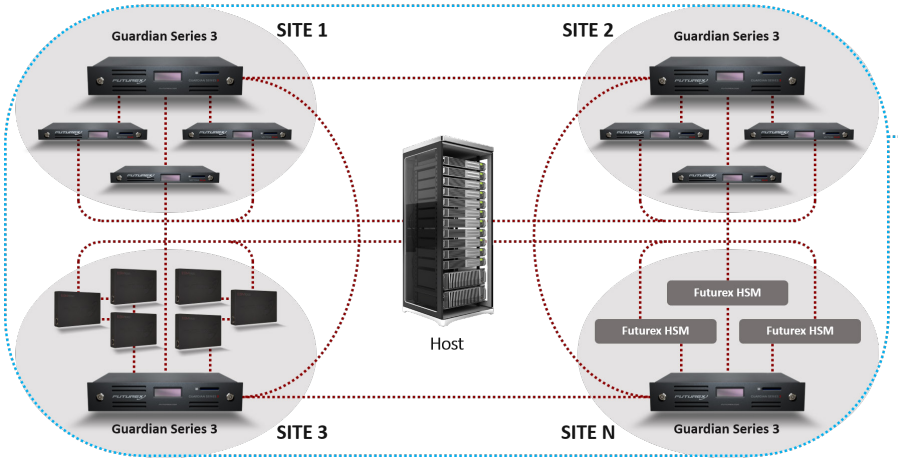
Ease of Use

- Powerful user interface for intuitive operation
- Seamless addition process for new Futurex client devices
- Remote web management enabling lights-out data centers
- Rapid modification of resource allocation

Intelligent Load Distribution and Automated Failover

- Active-active redundancy prevents loss of functionality in the event of a disaster, redistributing the processing load to backup Futurex devices
- Automatic synchronization of keys, certificates, and device information among client devices

Product Overview: Guardian Series 3



Enterprise Management for Your Core Cryptographic Infrastructure

- Centralized management, configuration, log auditing, & key loading
- User-defined device grouping system with drag-and-drop functionality, simplifying the process of managing multiple environments or regions collectively within the Guardian
- Remotely "push" updates for distributing and installing firmware on managed devices, reducing travel time and expenses

Web Analytics and Management Platform

- At-a-glance health assessment for the entire crypto infrastructure
- User-friendly dashboard
- Mobile-friendly support for all major web browsers
- Ability to create custom reports of various outputs (CSV, HTML, etc.)
- Customizable global cryptographic view featuring default or user-defined graphs

Regulatory Compliance Becomes an Easy Process

- Centralized firmware updating simplifies the process of keeping client devices up-to-date
- Consolidate data logs from all client devices
- Permission-based user authentication system enables group-specific function blocking and can restrict users to job-specific functionality

Customized Notification and Alerting

- User-definable alerting parameters and priority-based notifications
- Simple Mail Transport Protocol (SMTP) and Short Message Service (SMS) let administrators oversee infrastructure health, receive proactive alerts in critical situations, and gain actionable intelligence
- Simple Network Message Protocol (SNMP) and syslog functionality transmit log and error messages to a central network monitoring tool

FUTUREX.COM

ENGINEERING CAMPUS / 864 Old Boerne Road, Bulverde, Texas 78163 USA
TF/ (800) 251-5112 P/ +1 (830) 980-9782 info@futurex.com

Add Remote Management

Organizations with multiple backup or disaster recovery sites are able to use an Excrypt Touch remote configuration tablet from a single location to manage network-connected Futurex devices. Travel time is reduced, data center access is kept to an absolute minimum, and updates are able to be delivered quickly and effectively across an entire infrastructure.

Product Specifications

Dimensions and Weight

Weight: 40.5 pounds (18.4 kg)
Width: 19 inches (48.3 cm)
Height: 2U - 3.47 inches (8.81 cm)
Depth: 22.3 inches (56.7 cm)

Industry Compliance Standards

- FIPS 140-2 Level 3
- PCI HSM
- ANSI X9.24 Part 1 and Part 2—TR-39
- RoHS
- FCC Part 15 - Class B

Alerting and Notification Formats

SMTP, SNMP, SMS, Syslog

Operating Conditions

Power: 100 - 240 VAC 50/60 Hz. 225 Watts
Operating temp: -40° to 140°F (-40° to 60°C)
Storage temp: -40° to 140°F (-40° to 60°C)
Operating relative humidity: 20% to 80%
Storage relative humidity: 5% to 95%

External Hardware Requirements

Keyboard: Standard USB
Mouse: Standard USB
Video: SVGA 1024x768 at 75Hz refresh
Optional: Securus remote access tablet for hardware-secured configuration and management from remote locations

Centralized Management Capabilities

- Master File Key loading
- General settings and configuration
- User and permissions administration
- Log management and audit reporting
- Firmware distribution and installation
- Synchronization of keys, certificates, & settings across multiple client devices