



**TRUSTNET
MANAGER**

Ascent DataGuard

Encryption as a Service (EaaS)

Ascent DataGuard, powered by TrustNet Manager from Certes Networks, is a web-based management platform that simplifies security management while preserving network performance and functionality. It provides a browser-based user interface for managing policies and devices and a back end server for distributing group encryption keys. Ascent DataGuard offers simplified encryption management without requiring costly changes to your existing network infrastructure.

Ascent DataGuard allows you to:

- Manage network encryption from anywhere using a web-based interface
- Define and distribute security policies with simple drag-and-drop simplicity
- Separate security management from network management
- Review and audit system events to simplify regulatory compliance
- Automatically validate changes before deployment

PRODUCT SNAPSHOT

- Simplify encryption management
- Protect the network without compromising performance or availability using group encryption
- Empower the security team to control network security
- Platform for future growth into the cloud

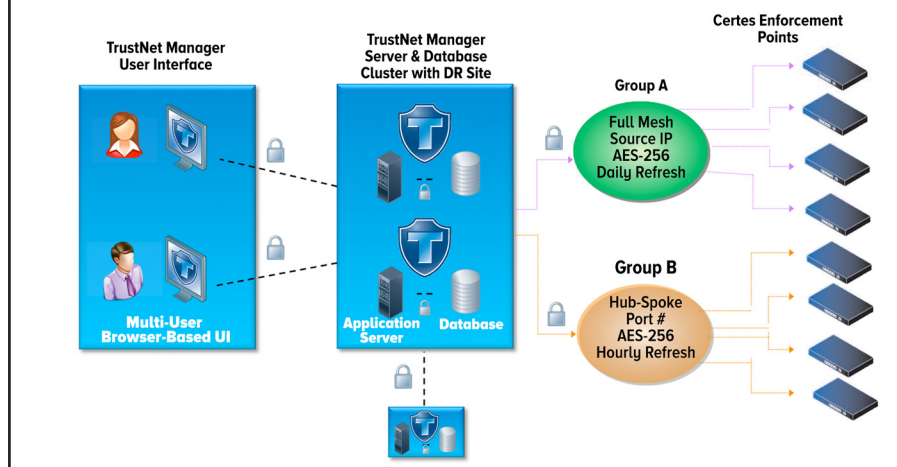
FEATURES AND BENEFITS

- Easy to configure policies for any network
- Separate roles for security control and network management
- Simple management for network encryption appliances
- Manage from anywhere with a browser-based multi-user interface
- Maintain compliance with logging and auditing
- Fail-safe group rekeys
- Clustered server architecture for high availability and scale
- Flexible physical or virtual server options reduce cost

COMPREHENSIVE PROTECTION

- IPsec site-to-site networks
- MPLS meshed networks
- Metro Ethernet and VPLS networks
- Voice over IP
- Video and Multicast applications
- Group encryption over public networks
- Multi-carrier networks

Solutions Architecture



Group Encryption Policy and Key Updates

Ascent DataGuard reliably distributes the group encryption policies and keys to Certes Enforcement Points (CEPs) throughout the network and it periodically sends key updates (rekeys). Key updates minimize the risk of a brute-force attack on the encrypted data by reducing the amount of information encrypted with the same key.

With Ascent DataGuard's fail-safe rekey feature, group keys are updated only when all of the group members are ready to receive the new key. This avoids network outages that occur when some group members receive a new key while other group members continue to use the old key.

CERTIFICATIONS



Headquarters

Ascent Data
90 Beta Drive
Pittsburgh, PA 15238
Phone: 412.968.4000
Fax: 412.967.9504

To learn more about how we can help your business, call Ascent Data today at 412.968.4000, email sales@ascentdata.com or visit www.ascentdata.com.

Role-Based Access Control

Using role-based access control, Ascent DataGuard provides separate roles for security control and network management. This allows the security team to outsource network management without losing control of the security policies and keys. Ascent DataGuard also provides powerful logging and auditing capabilities to establish, maintain and prove regulatory compliance.

Group Encryption Management for Policies, Keys and Devices

POLICY GENERATION

- Mesh topologies
- Hub and spoke topologies
- Multicast networks
- Point-to-point connections
- IPsec site-to-site connections

KEY GENERATION

- Generates encryption keys associated with policies
- Optional HSM card for hardware-based random number generation

KEY DISTRIBUTION

- Distributes encryption keys to enforcement points
- Scheduled key updates by period (hours) or daily at a pre-determined time
- Cluster-based server with disaster recovery for reliable re-keys
- All communications involving policies and keys are secured using TLS and transmitted through the management ports of the enforcement points
- Communications authenticated using X.509 certificates

CERTIFICATE MANAGEMENT

- GUI interface for complete certificate management
- Generate signing requests
- Send requests (CSR) from the CEP to the

TrustNet Server

- Install certificates onto the CEP

SYSTEM SYNCHRONIZATION

- Time synchronization via Network Time Protocol (NTP) version 3, RFC 1035 Supported Encryption Devices (software versions 1.5 or later)
- CEP10 VSE, CEP100 VSE, CEP1000 VSE, and CEP10G VSE
- CEP10, CEP10-R, CEP100, CEP100-XSA, CEP1000

DEVICE MANAGEMENT

- Import and export CEP configurations
- Device templates for fast repeat configurations
- Shift-click and select multiple CEPs for bulk operations
- Compare saved configuration with running configuration
- Secure CEP firmware upgrades
- Control user roles and passwords
- Monitor CEP status, counters and statistics

BROWSER REQUIREMENTS

For optimal security, stability and performance, the latest major release of the following browsers are fully supported and tested on a rolling basis*:

- Microsoft Internet Explorer®
- Mozilla Firefox®
- Google Chrome™

* Earlier versions and unlisted browsers may be fully or partially supported.

Industry Compliance Standards

Ascent DataGuard takes the pain, complexity and expense out of complying with industry and government data protection requirements. Whether you are subject to PCI DSS, HIPAA, HITECH, NERC CIP Standards, Sarbanes-Oxley or any data privacy/protection mandate, our network encryption solutions allow you to secure your network, achieve regulatory compliance, and reduce the cost of deploying, managing and maintaining the encrypted network.