

# Certes TrustNet Manager™

Group Encryption Management for Policies, Keys and Devices

## Product Overview

Certes TrustNet Manager™ 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 for distributing keys for group encryption deployments. TrustNet Manager offers simplified encryption management without requiring costly changes to your existing network infrastructure.

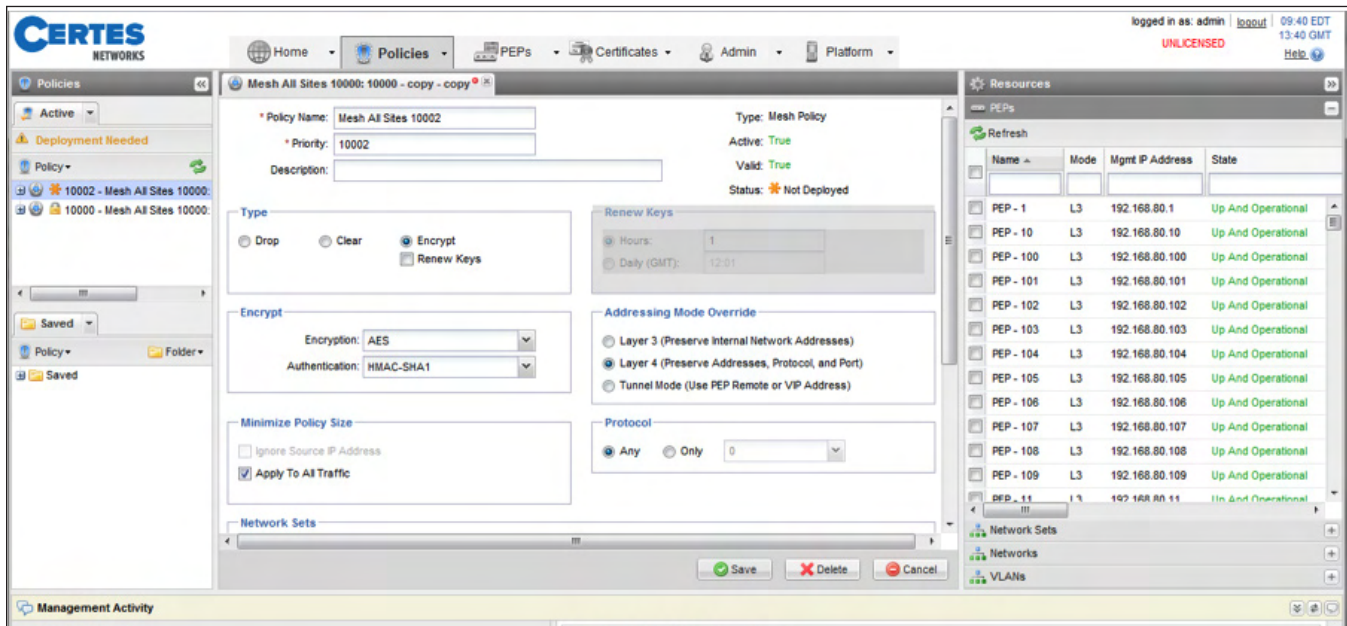


With Certes TrustNet Manager, users can:

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

## Policy Management

Certes TrustNet Manager acts as the central point of control for security personnel to define policies for what traffic to protect and how to protect it. Policies identify which network traffic to encrypt (based on any combination of VLAN ID, IP address, port information, or protocol ID) and specify what to do with it (encrypt, send in the clear or drop).



Encryption policies can be deployed and centrally managed from Certes TrustNet Manager.

## Encryption Key Management

Certes TrustNet Manager 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 TrustNet Manager'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.

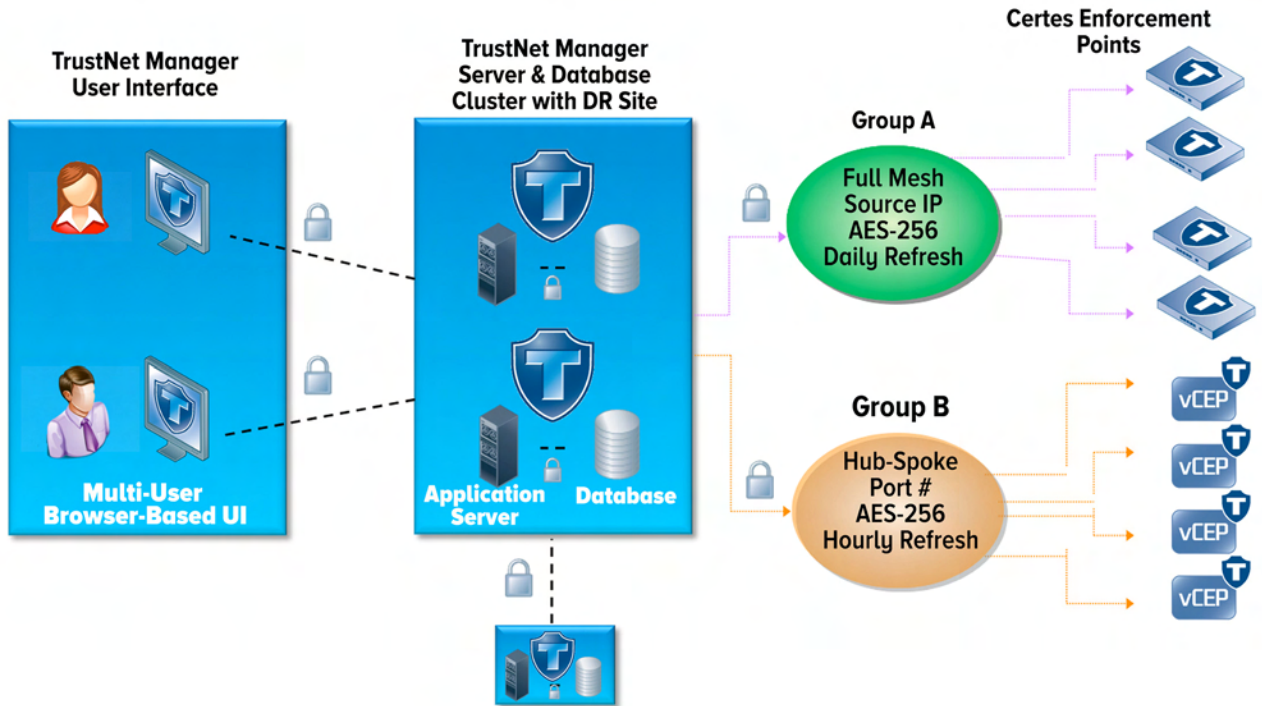
Certes TrustNet Manager helps you avoid costly misconfigurations and network outages by checking policies for mistakes and misconfigurations before new policies are deployed. It also deploys policy changes only to enforcement points that require changes.

**Security Management**

Using role-based access control, Certes TrustNet Manager 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. TrustNet Manager provides powerful logging and auditing capabilities to establish, maintain and prove regulatory compliance. TrustNet Manager also provides user-specific customizable dashboards and a dashboard to show device status as shown below.

**TrustNet Manager Architecture**

TrustNet Manager is built on a web-based three-tier architecture with clustering, disaster recovery and multi-tenancy included in the design from the beginning. The user interface provides multiple users with the ability to configure vCEP and CEP appliances and to define group encryption policies. TrustNet Manager handles policy and key generation and distribution to the vCEP and CEP enforcement points. Clustering provides redundancy and allows the system to scale linearly while the DR site capability provides additional redundancy. Service providers can offer encryption services to multiple end customers using a single instance of TrustNet Manager through the use of its built-in multi-tenancy capability.



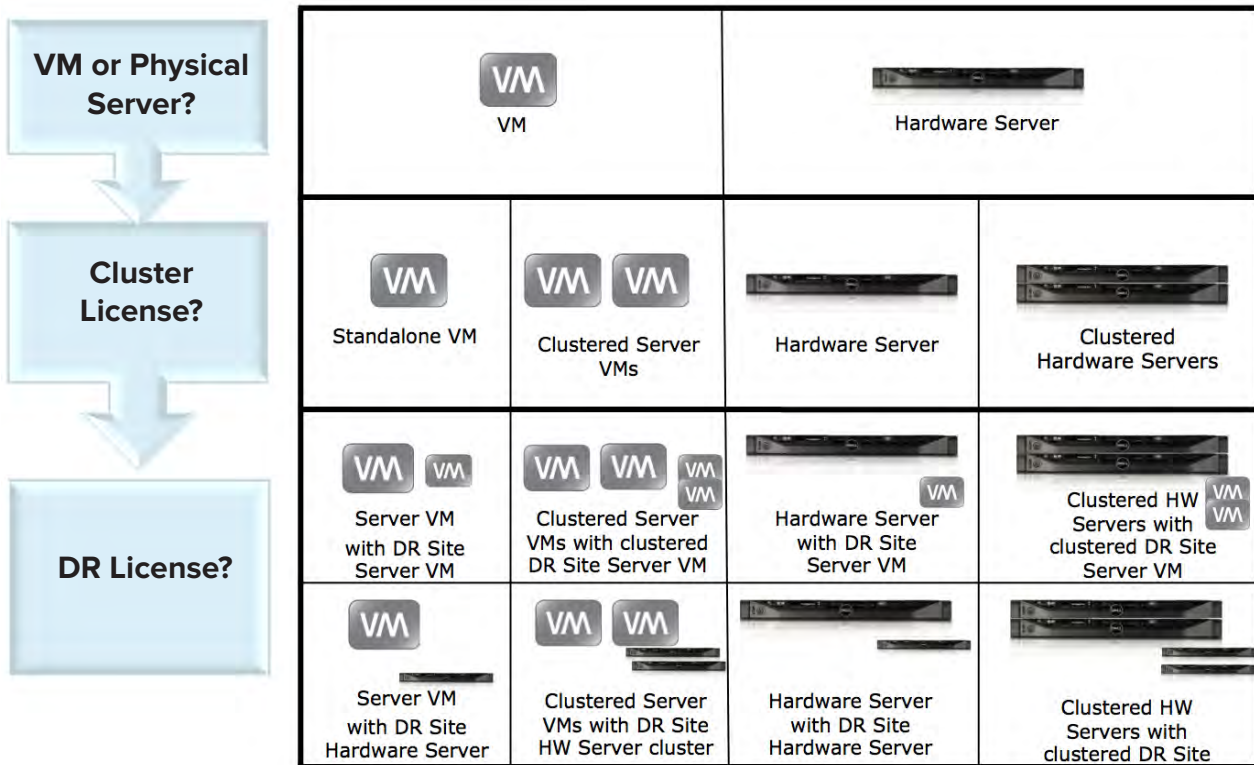
**Licensing**

A single license for Certes TrustNet Manager Software is included with TrustNet VSE and FSE Software licenses. The TrustNet Manager Software license can be applied to one server, and it includes a license for one active user. Additional clustered servers and disaster recovery servers can be added in order to provide additional scalability and redundancy. Each additional clustered server requires an additional cluster license, and each additional disaster recovery server requires an additional disaster recovery license. Each active TrustNet Manager user requires the purchase of an additional user license or mobile user license. User licenses are based on active users rather than named user accounts, so only the total number of simultaneous active users and mobile users need to be licensed.

For each server license purchased, customers can choose to deploy one of two available virtual server editions or a physical server. Please refer to the Configuration and Deployment section of this brochure for guidelines in choosing the correct edition for your deployment. Deployments of clustered and disaster recovery servers can be mixed among virtual and physical servers as shown in the table below.

**Deployment Options**

Certes TrustNet Manager reduces the cost of deploying a clustered server infrastructure by offering customers a choice of physical or virtual servers. Virtual servers can be used to cost-effectively deploy TrustNet Manager to an existing VMWare server or even to a laptop running VMWare Player.



### Configuration and Deployment

The detailed specification of the laptop, virtual machines and physical server configurations are shown below.

|  |  |  |
|--|--|--|
| <p><b>Standalone Edition</b> (laptop or desktop-based virtual machine)</p> | <p>Certes TrustNet Manager pre-installed on a virtual machine for standalone deployments. Additional servers for clustering or disaster recovery are not supported for this configuration.</p> <p>Recommended for smaller deployments on a laptop or desktop computer with few available resources or machines that have 32-bit processors.</p> <p>DHCP-assigned IP address by default (can be configured for static IP address)</p> | <p>Desktop or laptop machine running the latest major release of VMWare Player or VMWare Workstation.</p> <p>Host Operating Systems:<br/>           Microsoft Windows: 7, Vista, Server 2008, Server 2003, or XP<br/>           Linux: RedHat, SUSE, CentOS, Ubuntu and others (please refer to the latest VMWare specifications for the full list of supported operating systems).<br/>           CPU: Intel x86 Pentium-class 2 GHz or equivalent<br/>           Memory: 1 GB of RAM</p> <p>Disk: 20 GB of disk space available DVD includes:</p> <ul style="list-style-type: none"> <li>32 bit VMWare Virtual Machine (1 GB RAM, 20GB HDD) (for VMWare Player or VMWare Workstation) with TrustNet Manager and database pre-installed with a DHCP-assigned IP address</li> <li>Documentation</li> </ul> |
| <p><b>Server Edition</b> (server-based Virtual Machine)</p>                | <p>Certes TrustNet Manager pre-installed on a virtual machine (VM) for deployments of any size that require clustered or disaster-recovery servers.</p> <p>This virtual machine can be used as a standalone, cluster or disaster recovery server by configuring the server at installation time.</p>   | <p>Server-class machine running the latest version of VMWare ESX, ESXi, or vSphere.<br/>           Host Operating System: VMWare ESX, ESXi, or vSphere</p> <p>CPU: Intel x64 Xeon 2 GHz or equivalent<br/>           Memory: 2 GB memory available<br/>           Disk: 40 GB of disk space available</p> <p>DVD includes:</p> <ul style="list-style-type: none"> <li>A 64 bit VMWare Virtual Machine (2 GB RAM, 40GB HDD) (.OVA file that is deployed as an OVF template for VMWare ESX) with TrustNet Manager and database pre-installed with a statically-assigned IP address</li> <li>Documentation</li> </ul>   |
| <p><b>Hardware Server</b></p>  | <p>Certes TrustNet Manager pre-installed on a physical server*.</p> <p>Designed for any size deployment that requires a physical server, or deployments that require a hardware security module (HSM).</p> <p>* Physical server (part number TRUSTNET-MGR-HW) must be ordered in addition to TNM-SW software license(s)</p>  | <p>Server includes:</p> <ul style="list-style-type: none"> <li>Pre-installed TrustNet Manager and database with a statically assigned IP address</li> <li>Redundant installation of TrustNet Manager on a second drive (for recovery purposes).</li> </ul> <p>DVD includes:</p> <ul style="list-style-type: none"> <li>Documentation</li> </ul>  |

### Certes TrustNet Manager Technical Specifications

#### 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
- Communications authenticated using X.509 certificates

#### Certificate Management

- GUI interface for complete certificate management
- Generate signing requests
- Send requests (CSR) from the CEP/vCEP to the TrustNet Server
- Install certificates onto the CEP/vCEP

#### 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, vCEP

#### Device Management

- Import and export CEP/vCEP configurations
- Device templates for fast repeat configurations
- Shift-click and select multiple CEPs/vCEPs for bulk operations
- Compare saved configuration with running configuration
- Secure CEP/vCEP software upgrades
- Control user roles and passwords
- Monitor CEP/vCEP 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.

### Optional Hardened Physical Server Technical Specifications

#### Processor

- Quad Core Intel Xeon or equivalent with 8MB Cache Memory
- 8GB (4x2GB) 1333MHz Dual Ranked UDIMM

#### Internal Storage

- Two 160GB 7200RPM SATA Hard Drives
- Internal slim-line optical drive

#### Physical

- Form Factor: 1U Rack
- Dimensions: 1.67" x 17.10" x 24" (4.24 x 43.40 x 61.00 cm)

- Weight: ~ 30 lbs. (13.61kg)

#### Environmental

- Operating Temperature: 10° to 35°C (50° to 95°F) with a maximum humidity gradation of 10° per hour
- Operating Relative Humidity: 8% to 85% (non-condensing) with a maximum humidity gradation of 10% per hour
- Operating Maximum Vibration: 0.25 G at 3-200 Hz for 15 minutes
- Operating Maximum Shock: 31 G for 2.6ms

- Operating Altitude: -16 to 3048 m (-50 to 10,000 ft)

#### Power

- Redundant power supply (400W)

#### Regulatory

- FCC Part 15 Class A

#### Ports

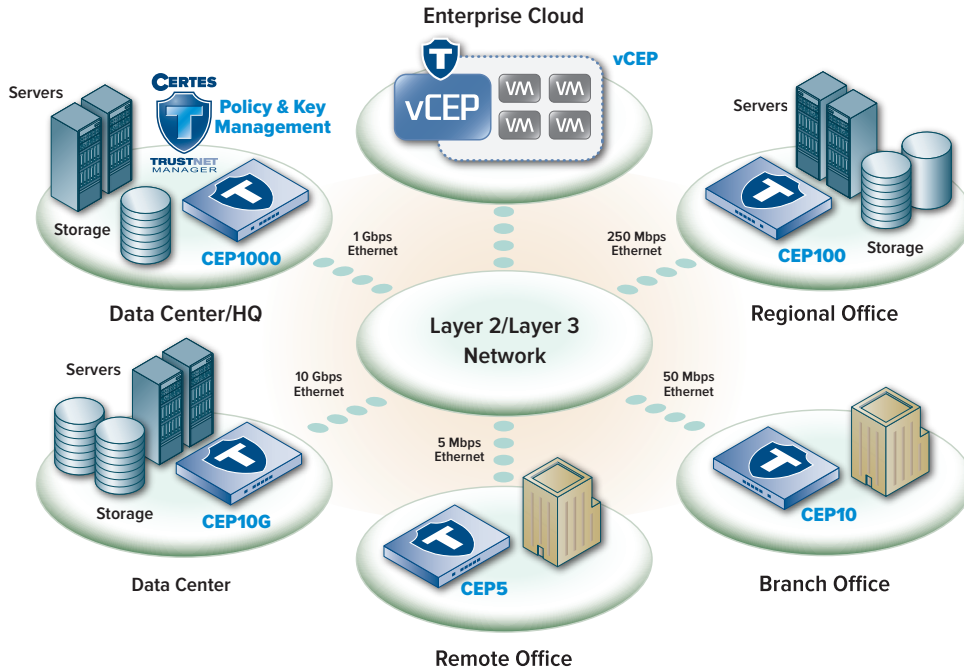
- On-Board Dual Gigabit NIC

### Ordering Information

| Part Number              | Description   |
|--------------------------|---|
| TRUSTNET-MGR-SW          | Certes TrustNet Manager Software License - Key, policy and device management software for Certes Networks encryption appliances. Includes one TrustNet Manager software license for use on one server, one management user license (one simultaneous active user with an unlimited number of named user accounts), documentation and software media (DVD). Additional management user licenses must be ordered separately to increase the number of simultaneous active users (see TRUSTNET-MGR-SW-USER). Customer should specify a delivery option - VMware virtual machine (VM) or pre-loaded on a hardened physical server. If the physical server option is specified, one or more physical server(s) (TRUSTNET-MGR-HW) must be ordered separately. |
| TRUSTNET-MGR-SW-CLSTR    | Software license for TrustNet Manager operated as a clustered application on one server.  |
| TRUSTNET-MGR-SW-DR       | Software license for TrustNet Manager operated as a Disaster Recovery server.   |
| TRUSTNET-MGR-SW-USER     | Software license for one additional simultaneous active management user of TrustNet Manager. One license must be purchased for each additional simultaneous GUI user of the multi-platform browser-based interface.   |
| TRUSTNET-MGR-SW-USER-MBL | Certes TrustNet Manager Server Software License for one additional simultaneous active GUI user with an optimized read-only mobile device interface (for iPhone and Android devices).   |
| TRUSTNET-MGR-HW          | Optimized and hardened physical server. Includes pre-installed TrustNet Manager software. A software license for TRUSTNET-MGR-SW, TRUSTNET-MGR-SW-CLSTR or TRUSTNET-MGR-SW-DR must be ordered separately.   |
| TRUSTNET-MGR-HW-HSM      | Hardware Security Module (HSM) add-on for the physical server (TRUSTNET-MGR-HW). The HSM module provides secure generation of keys, true random number generation, and other advanced security features. One HSM can be installed per physical server. The physical server (TRUSTNET-MGR-HW) must be ordered separately.  |

**Certes TrustNet Solution**

TrustNet Manager is an integral part of the Certes TrustNet Solution for network encryption and authentication that spans from the edge of the network to the IaaS cloud.



**TrustNet Features and Benefits**

| Feature   | Benefit  | Value   |
|---|--|---|
| Simple yet powerful drag and drop security policy builder             | Easy to create and deploy multi-layer encryption and authentication policies                                   | Reduce the time and cost of network security and compliance                     |
| Automatic key updates and rapid key revocation                        | Minimize risk of a data breach and react quickly in the event of an attack to minimize losses                  | Protect sensitive information and save money by insuring against data breaches  |
| Clustered architecture  | High Availability with linear scalability and Disaster Recovery  | Reduce network downtime. Support large and critical networks                    |
| Partial policy push and configuration validation                      | Fewer device and policy changes. All changes are validated   | Avoid mistakes and minimize network outages                                     |
| Role-based access control   | Provides separate roles for security control and network management  | Allows cost-effective and secure outsourcing without losing control of security |
| Powerful and usable logging and auditing capabilities                 | Easy to establish, maintain and prove compliance   | Simplify compliance and reduce initial and ongoing compliance costs             |
| Browser-based multi-user interface; server can be physical or virtual | Secure group encryption management in a browser by multiple authorized users from anywhere and on any platform | Usability and flexibility reduce OPEX compared to traditional site-to-site VPNs |
| Three-tier web-based architecture                                     | Ready for future growth into the cloud   | Cost-effective investment that will be able to meet future needs                |
| Fail-safe hitless key updates   | Group keys are updated only when all group members are ready; rekeys do not cause any traffic to be dropped    | Reduce network downtime   |
| Hardware Security Module (HSM) used for key generation                | Truly random keys provide stronger security  | Protect sensitive information and save money by insuring against data breaches  |

**Global Headquarters**  
 300 Corporate Center Dr., Suite 140  
 Pittsburgh, PA 15108  
 Tel: +1 (888) 833-1142  
 Fax: +1 (412) 262-2574  
 www.CertesNetworks.com

**North America Sales**  
 sales@certesnetworks.com

**Government Sales**  
 fedsales@certesnetworks.com

**Asia-Pacific Sales**  
 apac@certesnetworks.com

**Central & Latin America Sales**  
 cala@certesnetworks.com

**Europe, Middle East and Africa Sales**  
 emea@certesnetworks.com