



Enhance Digital
Security And Operational Efficiency With

CertSecure Manager

CertSecure Manager

Encryption Consulting's CertSecure Manager is an all-in-one vendor neutral certificate lifecycle management (CLM) solution for enterprises seeking an easy-to-use tool that seamlessly integrates with cloud-native environments. With CertSecure Manager, you can effortlessly manage and secure your digital certificates, ensuring that your organization's sensitive information remains protected while complying with regulatory standards.

Key Features at a Glance

Improved Compliance: Enhance compliance by ensuring adherence to industry standards such as HIPAA, PCI-DSS, and GDPR through certificate policy compliance and monitoring of certificate usage.

Enhanced Security: Improve your digital security by managing certificates, validating them, restricting access to sensitive data, safeguarding your digital environment, and protecting against security threats.

Cost Savings: Minimizes the time and resources required for manual certificate management processes and reduces the risk of certificate-related outages, resulting in cost savings.

Increased Efficiency: Automates certificate management processes, save time and effort on manual tasks and enable IT resources to focus on strategic initiatives.

Features related to CertSecure Manager

True Vendor Neutral Solution:

CertSecure connects all your public and private trust to create a single pane of glass for your certificate needs. It is a true vendor-neutral solution, allowing you to add both public and private trust Certificate Authorities of your choice from different networks to create a truly hybrid infrastructure.

API Integration:

The API feature seamlessly integrates certificate management operations with your existing applications, automating PKI processes and certificate issuance. This integration provides easy access to your certificate inventory, streamlines application workflows, reduces human errors and manual intervention.

Better Visibility: Provide a clear overview of the digital certificate inventory and facilitate tracking of the certificate lifecycle, which enables prompt detection and resolution of issues.

CertSecure Manager's offering for On-Prem, Cloud and SaaS deployments

Inventory: The inventory system acts as a centralized location for managing digital certificates from public trust CAs such as DigiCert, Sectigo, GlobalSign, Entrust and private trust CAs like Microsoft PKI, AWS, GCP, HashiCorp and EJBCA.

Reports: Intelligent data is generated based on the inventory, with reports such as an inventory report, an expiration report (listing certificates expiring soon), and a key length report (highlighting any certificates that use weaker cryptography keys).

Certificate Enrollment: The system provides a web interface and APIs to request new certificates from registered public and private CAs, creating a more controlled certificate enrollment environment with approval-based enrollment.

Automation: The system enables automated deployment of new certificates onto web servers such as IIS, Nginx, Apache, and Tomcat, as well as load balancers like F5, to minimize downtime and prevent outages.

Alerts: The system includes a built-in alert feature that sends notifications when a certificate is about to expire, as well as other important updates that require attention.

CertDiscovery: Enables organization to discover certificates being used in a network, identify vulnerabilities, and track certificate usage on servers. It also allows users to upload certificate discovery reports from tools like Tenable and Qualys.

Inventory Management:

CertSecure's inventory management centralizes digital certificates, automating renewal and revocation, hence ensuring secure, compliant management across sources.

Certificate Enrollment:

CertSecure provides self-service for digital certificate requests, reducing operational and management costs and enabling users to obtain certificates quickly. Policies and controls ensure only authorized users can request certificates, improving efficiency and security.

Strategic Departmental Segregation:

CertSecure facilitates meticulous organization division, enabling logical separation among your organization's various departments. Each department gains autonomy with its dedicated users and PKI Admins, ensuring streamlined control within the specific domain to align with regulatory and compliance requirements.

Certificate Discovery:

Certificate Discovery enables efficient management of your certificate landscape, improves security posture, and ensures compliance. Identifying and monitoring untracked certificates reducing the risk of missing critical certificates or letting them expire, improving your overall PKI posture.

See it in action

Encryption Consulting LLC is a customer-focused cyber security consulting firm providing an array of services in all aspects of data protection.

Contact Us

