cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Manager

Overview

CipherTrust Manager enables organizations to centrally manage encryption keys for Thales CipherTrust Data Securiy Platform and third party products. It simplifies key lifecycle management tasks, including secure key generation, backup/restore, clustering, deactivation, and deletion.

It provides role-based access control to keys and policies, multi-tenancy support, and robust auditing and reporting of all key management and encryption operations.

CipherTrust Manager is the management point for the CipherTrust Data Security Platform. It provides a unified management console that makes it easy to discover and classify data, and to protect sensitive data wherever it resides using a comprehensive set of CipherTrust data protection connectors from Thales.

CipherTrust Manager is available in both virtual and physical form-factors that integrates with FIPS 140-2 validated Thales Luna Network or Cloud HSM, and third-party Hardware Security Modules (HSMs) for securely storing master keys with highest root of trust. These appliances can be deployed on-premises as well as in private or public cloud infrastructures. This allows customers to address compliance requirements, regulatory mandates and industry best practices for data security.

Benefits

- Centralized key and policy management for on-premises data stores and cloud infrastructures
- Reduced business risk with unified data discovery, classification and sensitive data protection
- Simplified management with self-service licensing portal and visibility into licenses in use
- Cloud friendly deployment options with support for AWS, Azure, Google Cloud, VMware, Oracle Cloud Infrastructure and more
- Expanded Hardware Security Module (HSM) support for superior key control
- Unparalleled partner ecosystem of integrations with leading enterprise storage, server, database, application and SaaS vendors

Essential Capabilities

- **Full Key Lifecycle Management and Automated Operations:** CipherTrust Manager simplifies management of encryption keys across their entire lifecycle, including secure key generation, backup/restore, clustering, deactivation, and deletion. It makes automated, policy-driven operations easy to perform, and generates alarms for events of interest.
- **Centralized Administration and Access Controls:** Unifies key management operations with role-based access controls and provides full audit log review. Authenticates and authorizes administrators and key users using existing AD and LDAP credentials.
- **Data Discovery and Classification:** Provides a unified console for discovering and classifying sensitive data integrated with a comprehensive set of CipherTrust data protection connectors to encrypt or tokenize data to reduce business risk and satisfy compliance regulations.
- **Self-service Licensing:** Streamlines provisioning of connector licenses through a new customer facing licensing portal. The new management console offers better visibility and control of licenses in use.
- **Secrets Management:** Provides the ability to create and manage secret and opaque objects for usage on the platform.
- **Multi-tenancy Support:** Provides capabilities required to create multiple domains with separation of duties to support large organizations with distributed locations.
- **Developer Friendly REST APIs:** Offers new REST interfaces, in addition to KMIP and NAE-XML APIs, allows customers to remotely generate and manage keys.
- **Flexible HA Clustering and Intelligent Key Sharing:** Provide the option of clustering physical and / or virtual appliances together to assure high availability as well as increased encryption transaction throughput.
- **Robust Auditing and Reporting:** Includes tracking of all key state changes, administrator access, and policy changes in multiple log formats (RFC-5424, CEF, LEEF) for easy integration with SIEM tools. In addition, customers can generate pre-configured/customizable email alerts. Audit trails are securely stored and signed for non-repudiation.
- **High-speed Interfaces with NIC Bonding:** The new k470 and k570 appliances provide optional 2x1GB/2x10GB network interface cards (NIC) as well as NIC bonding to increase available bandwidth.
- **Broad Use Cases Supported:** CipherTrust Manager supports a comprehensive set of encryption and Tokenization use cases through CipherTrust Data Security Platform and an ecosystem of partners.

Appliance Specifications

CipherTrust Manager Physical Appliances

Feature	k470	k570
Max Keys	1,000,000	1,000,000
Max Concurrent Sessions	1000	1000
FIPS 140-2 Certification	Integrates with external Level 3 certified Thales Luna or Cloud HSM, and third-party HSMs	Includes Level 3 certified HSM embedded in the appliance
Network Interface Card (NIC) Options	• 4x1GB • 2x1GB / 2x10GB • NIC bonding support included	
APIs Supported	• REST • JCE • MS CNG • NAE-XML	• KMIP • MSCAPI • .NET • PKCS#11

CipherTrust Manager Virtual Appliances

Feature	k170v	k470v
Max Keys	25,000	1,000,000
Max Concurrent Sessions	100	1000
System Requirements	• RAM (GB): 16 • Hard Disk (GB): 100 • NICs: 1 max • CPUs: 2 - 4 max	• RAM (GB): 16 or more • Hard Disk (GB): 200 or more • NICS: 2 or more • CPUs:5 or more No enforced limits on vm system
FIPS 140-2 Certification	• Integrates with external Thales Luna Network or Cloud HSMs	
API's Supported	• REST • JCE • MS CNG • NAE-XML	• KMIP • MSCAPI • .NET • PKCS#11

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.