THALES

Building a future we can all trust

CipherTrust Manager

Overview

CipherTrust Manager enables organizations to centrally manage encryption keys for Thales CipherTrust Data Security 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 central 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 integrate 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

Key Management   Access Policies   Auditing Reporting   Flexible APIs

THALES

CipherTrust Manager

Key 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.
- **Unified Management Console:** 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.
- **Centralized Administration and Access Controls:** Unifies key management operations with role-based access controls. Authenticates and authorizes administrators and key users using existing AD and LDAP credentials. Prevents unauthorized password change and alerts on simultaneous logins by same user.
- **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 secrets and opaque objects for usage on the platform.
- **Multi-tenancy Support:** Supports separation of duties with delegated user management within multiple domains.
- **Developer Friendly REST APIs:** Offers new REST interfaces, in addition to Key Management Interoperability Protocol (KMIP) and NAE-XML APIs, allows customers to remotely generate and manage keys.
- **Flexible HA Clustering and Intelligent Key Sharing:** Provides 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.
- **Broad Partner Ecosystem:** CipherTrust Manager provides centralized key management for wide variety of storage partners via KMIP and database partners via Transparent Database Encryption (TDE).

CipherTrust Manager Features

Features	Virtual Appliances		Physical Appliances	
	k170v	**k470v**	**k470**	**k570**
Administrative Interfaces	Management Console, REST API, kscfg (system configuration), (ksctl (Command Line Interface)			
Network Management	SNMP v1, v2c, v3, NTP, Syslog-TCP			
API Support	REST, NAE-XML, KMIP, PKCS#11, JCE, .NET, MCCAPI, MS CNG			
Secure Authentication	Local User , AD/LDAP, LDAPS, Certificate based authentication, Supports Open ID Connect (OIDC)			
System Formats	RFC-5424, CEF, LEEF			
Supported HSMs for Root of Trust	Luna Network HSM, Luna T-Series Network HSM, Luna Cloud HSM, AWS Cloud HSM, Azure Dedicated HSM, IBM Cloud HSM, IBM Cloud Hyper Protect Crypto Services Cloud HSM	Luna Network HSM, Luna T-Series Network HSM, Luna Cloud HSM, AWS Cloud HSM, Azure Dedicated HSM, IBM Cloud HSM, IBM Cloud Hyper Protect Crypto Services Cloud HSM	Luna Network HSM, Luna T-Series Network HSM, Luna Cloud HSM, AWS Cloud HSM, Azure Dedicated HSM, IBM Cloud HSM, IBM Cloud Hyper Protect Crypto Services Cloud HSM	N/A (has built in HSM)
Automated Deployment Support	Yes (via Cloud-Init)	Yes (via Cloud-Init)	No	Yes (via Secure Transport Mode)
Maximum Number of Keys	Tested up to 1M Keys (more possible with appropriately sized virtual environments)	Tested up to 1M Keys (more possible with appropriately sized virtual environments)	1 Million Keys	1 Million Keys
Maximum Domains (multi-tenancy)	100	1000	1000	1000

Appliance Specifications

Physical Appliances	k470	k570
Dimensions	19" x 21" x 1.725" (482.6mm x 533.4mm x 43.815mm)	
Hard Drive	1x 2TB SATA SE (Spinning Disk)	
CPU	Xeon E3-1275v6 Processor	
RAM	16GB	
NIC Support	4x1GB or 2x10Gb/2x1Gb (NIC Bonding capable)	
Rack Mount	Standard 1U rack mountable Sliding rails can be optionally purchased	
Reliability	Dual hot swappable power supplies	
Safety and Compliance	CSA C-US, FCC, CE, VCCI, C-TICK, KC Mark, BIS	
Mean Time Between Failure	165,279 hours	153,583 hours
FIPS Support	Integrates with an external FIPS Certified Physical or Cloud HSM as Secure Root of Trust	Embedded PCI-HSM FIPS 140-2 Level 3 certified – password and multi-factor (PED) (Certificate #3205)

Virtual Appliances	k170v	K470v
System Requirements	- RAM (GB): 16 - Hard Disk (GB): 100 - NICs: 1 or more - CPUs: up to 4 CPU max	- RAM (GB): 16 or more - Hard Disk (GB): 200 or more - NICS: 2 or more - CPUs:5 or more
Clouds/Hypervisors Supported	- Public Clouds: AWS Cloud, Microsoft Azure, Google Cloud Enterprise (GCE), Oracle Cloud Infrastructure (OCI), Alibaba Cloud - Private Clouds/Hypervisors: VMware vSphere (6.5, 6.7 and 7.0), Microsoft Hyper-V, Nutanix AHV, OpenStack (QCOW2) * AWS GovCloud, Azure Government Cloud also supported	

PlanetComm

Planet Communications Asia PLC.

157 Soi Ramindra 34, Ramindra Rd., Tarang, Bangkhen, Bangkok 10230
Tel: +66 2 792 2400 | Fax: +66 2 792 2499, +66 2 943 5771 | E-mail: marketing@planetcomm.com

PlanetComm:

> cpl.thalesgroup.com <

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us