Product Brief

THALES
Building a future we can all trust

CipherTrust Manager

thalestct.com

THALES

CipherTrust Manager simplifies key lifecycle management tasks, including secure key generation, backup/restore, clustering, deactivation, and deletion by enabling organizations to centrally manage encryption keys for Thales CipherTrust Data Security Platform and third-party products. Role-based access provides control to keys and policies, multi-tenancy support, and robust auditing and reporting of all key management and encryption operations.

As the central management point for the CipherTrust Data Security Platform (CDSP), CipherTrust Manager provides a unified management console that makes it easy to discover and classify data, and to protect sensitive data wherever it resides. CDSP makes available a comprehensive set of CipherTrust Data Protection Connectors from Thales, including Secrets Management and Ransomware Protection, and REST, KMIP, and NAE XML APIs for custom solutions.

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.
- Quorum Authorization: Allows an administrator to require multiple approvers for a sensitive operation.
- 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.
- 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 a wide variety of storage partners via KMIP and database partners via Transparent Database Encryption (TDE).
- Root of Trust: CipherTrust Manager can use Thales TCT's Luna T-Series HSMs as root of trust. Meeting government mandates for U.S. Supply Chain, the high-assurance, tamper-resistant Luna T-Series HSMs are designed, developed, manufactured, sold, and supported in the United States. CipherTrust k160 uses a removable FIPS 140 certified token or high assurance token as a root of trust.

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 public, private and hybrid clouds. Public: AWS, Azure, Google Cloud, Oracle Cloud. Government: AWS GovCloud, Azure Government Cloud. Private image files: VMware vSphere OVA, Microsoft Hyper-V VHDX, Nutanix AHV VMDK and OpenStack QCOW2. Hybrid cloud image files: Azure Stack HCI, Azure Stack Hub
- 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

THALES

CipherTrust Manager

THALES

Deployment Options

CipherTrust Manager is available in both virtual and physical form-factors that integrate with FIPS 140 validated Thales Luna T-Series Network or Cloud Hardware Security Modules (HSMs) to securely store master keys with the highest root of trust. These appliances can be deployed onpremises 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.

CipherTrust Manager Features

	Virtual Appliances		Physical Appliances	
Features	**k170v**	**k470v**	**k160**	**k570**
Administrative Interfaces	Management Console, REST API, kscfg (system configuration), (ksctl (Command Line Interface)			
Network Management	SNMP v1, v2c, v3, NTP, Syslog-TCP			
Monitoring	Prometheus, Splunk			
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 as a ServiceHSM , Luna Cloud HSM, AWS Cloud HSM, Azure Dedicated HSM, IBM Cloud HSM, IBM Cloud Hyper Protect Crypto Services Cloud HSM		Removable token HSM using either a FIPS 140 Certified Token or High Assurance Token	Embedded FIPS 140 level 3 & CNSS approved Luna T-series HSM or Luna as a Service HSM
Automated Deployment Support	Yes (via Terraform, Cloud-Init)		No	Yes (via Secure Transport Mode)
Maximum Number of Keys	Tested up to 1M Keys (more possible with appropriately sized virtual environments)		10,000 Keys	1M Keys
Maximum Domains (multi-tenancy)	100	1000	100	1000
FIPS Support	FIPS 140 L1			
	Integrates with an external FIPS Certified Physical or Cloud HSM as Secure Root of Trust		FIPS 140 Certified Token HSM	Embedded Luna T-Series PCIe FIPS 140 Level 3 certified – password and multi-factor (PED)

Appliance Specifications

Physical Appliances	k160	k570
Dimensions	7" x 4.3" x 1.65" (177.8mm x 109.2mm x 41.9mm)	19" x 21" x 1.75" (482.6mm x 533.4mm x 44.45mm)"
Hard Drive	1x 256GB mSATA SSD SE	1x 2TB SATA SE (Spinning Disk)
CPU	Atom x6425E Processor SoC	Cores: 4, Threads: 8, Processor Base Frequency: 3.8 GHz
RAM	32GB	16 GB*
NIC Support	2x 1Gb (NIC Bonding capable)	4x1GB or 2x10Gb/2x1Gb (NIC Bonding capable)
Rack Mount	Custom1U shelf mount can be optionally purchased (can house up to two k160s)	Standard 1U rack mountable Sliding rails can be optionally purchased
Power	12V external power supply; locking DC power connector	Dual hot swappable power supplies
Safety and Compliance	FCC, CE	CSA C-US, FCC, CE, VCCI, C-TICK, KC Mark, BIS
Mean Time Between Failure	489,989 hours	153,583 hours

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) • Government Clouds AWS GovCloud, Azure Government Cloud • Private Clouds/Hypervisors: VMware vSphere (6.5, 6.7 and 7.0), Microsoft Hyper-V, Nutanix AHV, OpenStack (QCOW2) • Hybrid Clouds/Hypervisors: Azure Stack HCI, Azure Stack Hub	

Saftey Certifications	Applicable Administrative Unit
CSA-UL	• Canada/US
Emissions Certifications	**Applicable Administrative Unit**
FCC Part 15, Subpart B, Class B	• US

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com