

# CipherTrust Manager



## Overview

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.

## Deployment Options

CipherTrust Manager is available in both virtual and physical form-factors that integrate with FIPS 140-2 validated Thales Luna Network or Cloud HSM Hardware Security Modules (HSMs) to securely store master keys with the 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 public, private and hybrid clouds. Public: AWS, Azure, Google Cloud, Oracle Cloud and Alibaba 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



**Key  
Management**



**Access  
Policies**



**Auditing &  
Reporting**



**Flexible  
APIs**



**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.
- **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.
- **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 a 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
<b>Administrative Interfaces</b>	Management Console, REST API, kscfg (system configuration), (ksctl (Command Line Interface)			
<b>Network Management</b>	SNMP v1, v2c, v3, NTP, Syslog-TCP			
<b>Monitoring</b>	Prometheus, Splunk			
<b>API Support</b>	REST, NAE-XML, KMIP, PKCS#11, JCE, .NET, MCCAPI, MS CNG			
<b>Secure Authentication</b>	Local User , AD/LDAP, LDAPS, Certificate based authentication, Supports Open ID Connect (OIDC)			
<b>System Formats</b>	RFC-5424, CEF, LEEF			
<b>Supported HSMs for Root of Trust</b>	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, nShield Network 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, nShield Network 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, nShield Network HSM	<b>Built-in HSM</b> , 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, nShield Network HSM
<b>Automated Deployment Support</b>	Yes (via Terraform, Cloud-Init)	Yes (via Terraform, Cloud-Init)	No	Yes (via Secure Transport Mode)
<b>Maximum Number of Keys</b>	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
<b>Maximum Domains (multi-tenancy)</b>	100	1000	1000	1000
<b>FIPS Support</b>	FIPS 140-2 L1 ( <a href="#">Certificate #4430</a> )			
	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 #4090)

# 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	Cores: 4, Threads: 8, Processor Base Frequency: 3.8 GHz	
RAM	16 GB*	
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

Virtual Appliances	k170v	K470v
System Requirements	<ul style="list-style-type: none"> <li>RAM (GB): 16</li> <li>Hard Disk (GB): 100</li> <li>NICs: 1 or more</li> <li>CPUs: up to 4 CPU max</li> </ul>	<ul style="list-style-type: none"> <li>RAM (GB): 16 or more</li> <li>Hard Disk (GB): 200 or more</li> <li>NICS: 2 or more</li> <li>CPUs: 5 or more</li> </ul>
Clouds/Hypervisors Supported	<ul style="list-style-type: none"> <li>Public Clouds: AWS Cloud, Microsoft Azure, Google Cloud Enterprise (GCE), Oracle Cloud Infrastructure (OCI), Alibaba Cloud</li> <li>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</li> <li>Hybrid Clouds/Hypervisors: Azure Stack HCI, Azure Stack Hub</li> </ul>	

Safety Certifications	Applicable Administrative Unit
CB Scheme	50 countries
CSA-UL	Canada/US
<b>Emissions Certifications</b>	
FCC Part 15, Subpart B, Class B	US
EN55032:2010, EN55035:2017, EN61000-3-2:2006 +A1:2009 +A2:2009 EN61000-3-3:2008	EU
ICES-003 Issue 7 - October 2020	Canada
AS/NZ CISPR 32:2015	Australia/NZ
VCCI V-3/2009.04	Japan
KN22, KN24, KC Mark	South Korea
NOM	Mexico
BIS	India