

Thales Crypto Command Center



Centralize your crypto management HSM resources and reduce IT security infrastructure costs with Thales Crypto Command Center.

Overview

IT security departments and service providers can now quickly and securely expand IT capabilities, gain visibility, and streamline their infrastructure in physical, cloud, hybrid cloud and virtual environments with Crypto Command Center. This is the market's first solution to fully exploit the benefits of virtualization including reduced costs and innovation, by provisioning Thales Luna Network Hardware Security Modules (HSMs) without compromising security or compliance.

Together, Crypto Command Center and Luna Network HSMs combine to form one complete, centralized solution for the management of your crypto HSM resources—a crypto hypervisor. Deliver on-demand provisioning of crypto resources for data protection in minutes instead of days, while allowing the application and data owners to maintain full control of encryption services and data.

Experience the benefits of centralized HSM management through the Premium license for full production environments, or a Freemium license that facilitates a rapid proof of concept in non-production environments.

Crypto Command Center benefits

- Centralized crypto resources
- Maintain a standardized, consistent level of security through crypto templates and automation
- Visibility across device pools through easy monitoring and reporting
- Export logs for monitoring and analysis systems including Splunk
- Easily view cryptographic materials per partition
- Support for Active Directory
- Increased security and sharing of hardware through multi-tenancy with role separation
- Shared resources across multiple tenants
- Offer easy to implement Crypto as a Service
- Provision single or groups of HSM partitions in minutes vs hours, and lower total cost of ownership

Highlighted capabilities

- **Crypto as a Service:** Enterprise and Service Providers can quickly and cost-effectively provision and manage single or groups of Luna Network HSMs from one central location.
- **Monitoring & Alerting:** help administrators make capacity planning decisions, troubleshoot issues, receive email alerts on service-impacting events, and quickly support application owners.
- **Route to Cloud:** administer Luna HSMs hosted in a hybrid cloud service platform without compromising security or compliance.
- **Comprehensive Crypto Resource Reporting:** benefit from centralized high availability and resource management, and improved client visibility.
- **Automation through Crypto Service Templates:** easily create and deploy your own custom, repeatable crypto templates to enforce security and consistency.
- **High Availability and Reliability:** deploy crypto resources in high availability to minimize downtime.
- **Remote Cloud HSM Management:** benefit from easy access and reduced total cost of ownership in a hybrid environment.
- **Provision** up to 100 partitions per device.
- **Dynamic Resource Management:** quickly spin up/spin down crypto resources.

Crypto Command Center

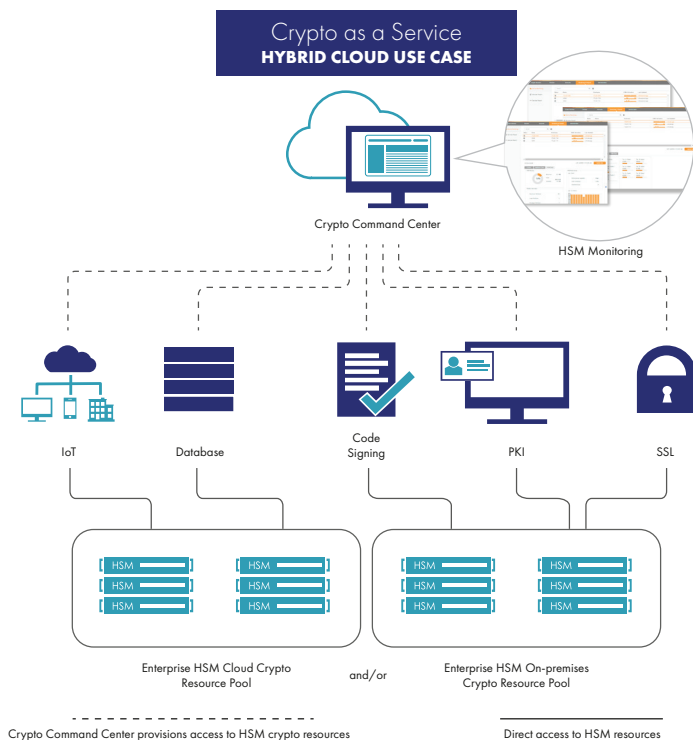
A complete crypto management solution offering the following advantages:

- Market's first true crypto hypervisor—a single, centralized platform for managing cryptographic resources.
- Monitor crypto resources, generate dynamic reports and always be up to date on the status of your HSM device pool.
- Tight integration with Luna Network HSMs through REST API.
- Provision, manage, and administer Luna Network HSMs on-premises, virtually, or in hybrid and cloud environments with this highly scalable solution.
- Deploy crypto resources quickly and efficiently to meet current and future encryption needs in minutes, not hours as was historically the case.
- Discovery of unmanaged crypto resources and partitions.
- Service Management—import unmanaged crypto resources, reassign device pool ownership, and dynamically reassign services.
- HSM Device Logs — easily download and export device logs to a third-party monitoring and analytics tool such as Splunk.

Crypto as a Service—typical challenges

Challenge	Effect	Solution
Lack of Security	Stakeholders implement inconsistent crypto deployments, increasing the risk of unauthorized data disclosure and fraud.	Standardization through crypto templates and automation eradicates the risk of non-compliance, and ensures security even in heavily regulated industries.
Inefficiency	Encryption islands are created by a variety of departments deploying point solutions. Additionally, as encryption needs grow, the demand to crypto enable applications increases, requiring additional resources and expertise.	Centralized management of crypto resources eliminates encryption islands. Automation, scalability and delegation of responsibilities to non-crypto experts reduces costs and shortens time-to-market when implementing encryption solutions. Monitoring enables administrators to quickly determine the status of their appliances and be proactive in making capacity and maintenance decisions.
Complexity	Deploying crypto resources requires skilled resources and time.	Crypto service templates* remove the complexity and empower more users to use crypto in the enterprise. Monitoring removes the need for traditionally CLI-intensive tasks and accelerates adoption.
Reduced Quality	Disruption of operations due to spikes in demand or security breaches, and lack of disaster recovery options.	High Availability (HA) ensures business continuity and consistent service levels. Monitoring enables administrators to quickly determine the status of their appliances and be proactive in making capacity and maintenance decisions.
Lack of Visibility	Administrators cannot readily see the status or health of HSM device pools.	Monitoring and reporting provide convenient centralized view across the device pool, while email alerting keeps administrators informed of service-impacting events.

*A Crypto Service is a Luna Network HSM partition or a HA Group that is used for cryptographic applications such as code signing, database encryption, and PKI.



Available solutions

Crypto Command Center:

1. Premium:

- Base Offering—Provisioning
- Enhanced Offering - Management and Monitoring License

2. Freemium:

- Management and Monitoring License

Supported Technologies:

Crypto Command Center can manage PED—and password-authenticated Luna Network HSM devices that meet the following minimum requirements:

Appliance Software:

- Luna HSM software 6.1, 6.2, 6.2.1, 7.0, 7.1, 7.2, and 7.4
- REST API required

Firmware:





- 6.10.9 or higher

Backup:

- Cloning or Key Export

Authentication:

- PED—or Password-authenticated
- PED—authenticated devices must support remote PED

> cpl.thalesgroup.com <    

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

Model Comparison

Feature	Freemium Version	Premium Version
Number of Crypto Services	Provision up to 20 crypto services	Provision an unlimited amount of crypto services
Database	PostgreSQL included	PostgreSQL included. Oracle integration also supported in Premium version.
Customer Support	No customer support or service plan	Optional customer support and service plan available
Deployment Environment	Test environments only	Test and production environments
High Availability	Not available	HA configurations available

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.