Entrust KeyControl Compliance Manager

Unify your dashboard and create full visibility of keys and secrets across on-premises and cloud environments

Overview

The need for cryptography to establish identity, protect data from unauthorized alteration, and prevent denial of service has never been higher. Cryptographic techniques secure communications over networks, protecting information stored in databases and across many other critical applications.

These techniques involve the use of cryptographic keys that must be managed and protected throughout their lifecycle. Without proper key management, keys can be lost, stolen, or compromised, leading to security breaches and the loss of confidential information. Additionally, effective key management is essential for ensuring compliance with regulatory and industry standards.

As organizations manage an increasing number and diversity of keys and secrets, a consistent global strategy for managing keys across IT assets should include full visibility of all keys and secrets, as well as all related information such as the key owner, the key usage, the key history, how the key was generated, and for what purpose.

KEY FEATURES

- Key and secret inventory across on-premises and cloud key management systems
- Supports all types of keys and secrets including KMIP keys, TDE keys, SSH keys, cloud keys, application keys, passwords, tokens, etc.
- Supports AWS KMS, Azure Key Vault, and GCP KMS
- Key documentation workflows
- Key reporting and alerting
- Deployed as a virtual appliance on-premises or in the cloud
- High-availability (HA) support with active-active clustering
- Supports separation of duties, least privilege, dual control, and multitenancy
- Audit logs and forensic export
- Automated compliance engine for PCI DSS, NIST 800-130, NIST 800-57, and other standards

Learn more about KeyControl at entrust.com

Entrust KeyControl Compliance Manager

Manual processes for creating and managing cryptographic assets often leads to poor key hygiene, including lack of key documentation, compliance, and key rotation, which further increases the risk of data breaches.

With Entrust KeyControl Compliance Manager, businesses can easily establish and maintain a key inventory and achieve full visibility on all related information for all keys, across on-premises and cloud environments, including key history and usage.

In creating a single unified dashboard, the solution allows you to view and monitor your organization's cryptographic assets located in one or many vaults – whether configured locally or geographically distributed.

BENEFITS

Unifies visibility on keys and automated documentation process

KeyControl Compliance Manager provides a singular dashboard view of your key inventory across on-premises, public cloud, and hybrid cloud. It provides granular details on which keys are being used and can include information about ownership, environment, purpose, and critical system.

With KeyControl Compliance Manager, organizations can answer questions like:

- Who is the key owner?
- How is the key generated?
- How critical is a key?

The answers to those questions trigger documentation workflow when a lack of information is detected or upon an event related to the lifecycle of a key.

The dashboard also considers the human factors related to key management. By streamlining and automating processes, KeyControl Compliance Manager helps to reduce the likelihood of human error.

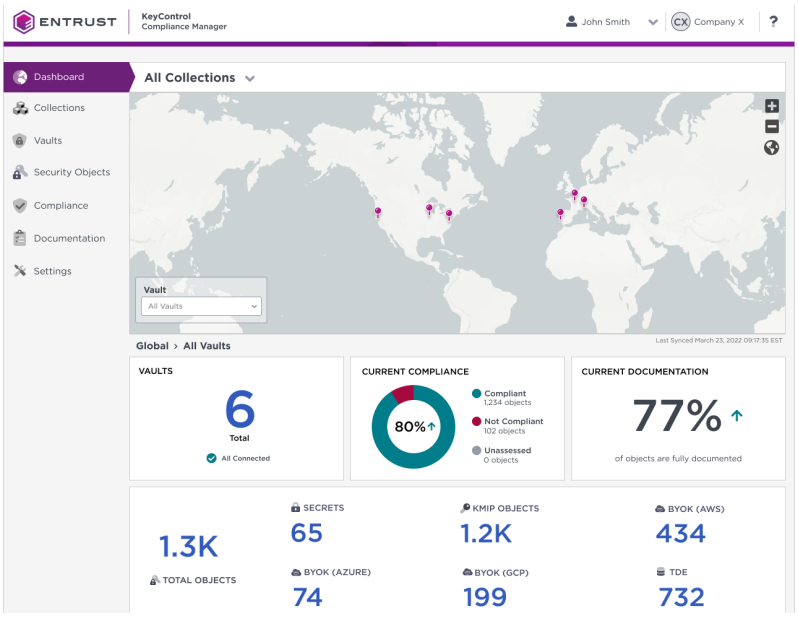


Figure 1: Illustrative view of the dashboard representing six decentralized vaults, cryptographic keys, and secrets.

Learn more about KeyControl at entrust.com

Entrust KeyControl Compliance Manager

BENEFITS

Facilitates compliance with regulatory requirements and standards

Beyond the cyber-threat risk, an increasingly complex regulatory environment brings its own risks to businesses. Ensuring compliance with legal requirements or standards is sometimes not possible when keys are not sufficiently documented or there is no centralized visibility into keys.

As your number of keys increases, meeting compliance requirements will consume more and more resources, so the real question is how to ensure compliance while managing costs.

KeyControl Compliance Manager provides an automatic approach to help support visibility, reporting, and complying with industry regulations such as Payment Card Industry Data Security Standard (PCI DSS), NIST SP 800-130, and NIST 800-53.

These capabilities provide a quick payback by reducing the need for staff and ensuring keys are always documented and managed in accordance with a particular security policy or an industry-specific standard.

KeyControl Compliance Manager makes it easier to demonstrate compliance to auditors. Wherever you operate and whatever the regulation, KeyControl Compliance Manager can help you achieve and maintain compliance, improving your security and managing your risks.

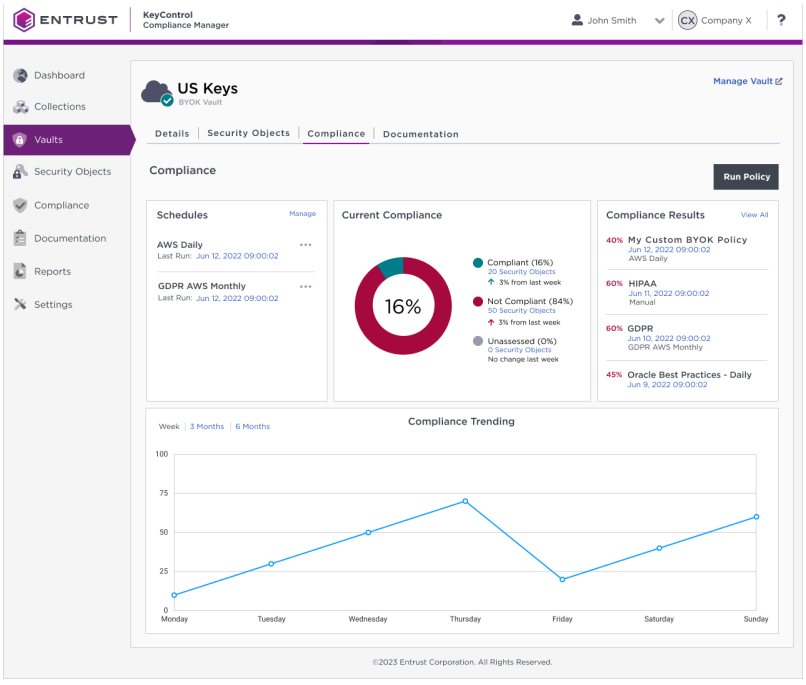


Figure 2: Compliance view of the dashboard detailing the inventory of keys and secrets in USA region and compliance results in relation to several regulatory templates

Learn more about KeyControl at entrust.com

Entrust KeyControl Compliance Manager

Technical Specifications

Key and secret support:

- KMIP keys, TDE Keys, SSH Keys, API keys, tokenization keys, passwords, container secrets, database secrets

Cloud support:

- AWS KMS, Azure Key Vault, GCP KMS

Authentication protocol:

- Active Directory, LDAP, OIDC, SAMLv2

Management and Monitoring:

- Centralized management with Web UI and Rest API
- Syslog and Splunk integration

Platform support:

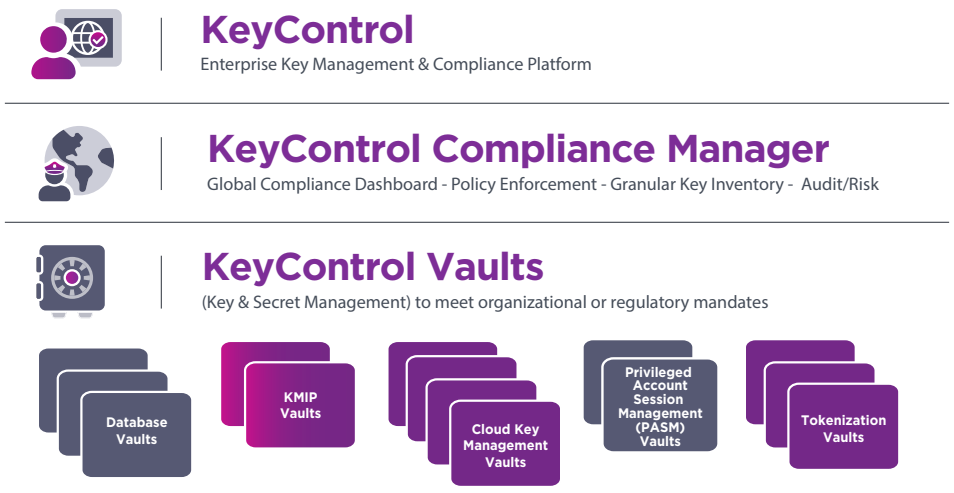
- Private cloud platforms: VMware Cloud Foundation (VCF), vSphere, VxRail, Nutanix
- Public cloud platforms: AWS, IBM Cloud, Microsoft Azure, VMware Cloud (VMC) on AWS, Google Cloud Platform (GCP)

Deployment media:

- ISO, OVA (Open Virtual Appliance), AMI (Amazon Web Services Marketplace), or VHD (Microsoft Azure Marketplace)

Entrust KeyControl Platform

Entrust KeyControl Compliance Manager is part of a suite of products designed to manage key lifecycles at scale for encrypted workloads in virtualized environments across on-premises, multi-cloud, and hybrid deployments.



For more details on the KeyControl platform, KeyControl Compliance Manager, and the range of vaults download the Entrust KeyControl Solution Brochure.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223