IBM Guardium Key Lifecycle Manager

Centralize, simplify and automate encryption key management

Highlights
Manage encryption keys centrally

Get strong access management and security while simplifying key configuration and management

Monitor health and status of managed endpoint certificates

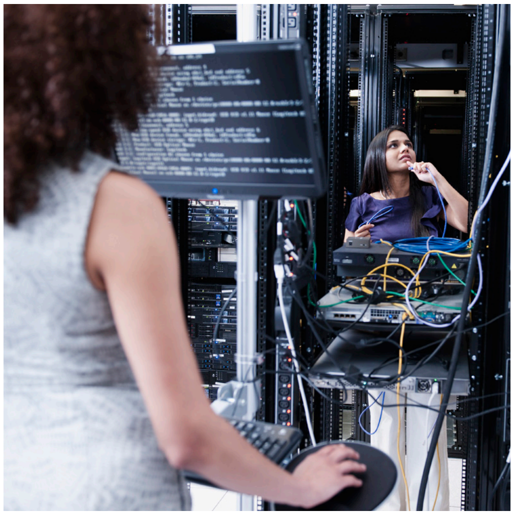
Expedite deployment with wizard-based assistance

Business data is growing at tremendous rates, driving the demand to protect data on premises and in the cloud. Enterprises respond by implementing encryption at various layers—in hardware, on files and in applications—which can result in encryption silos with inconsistent approaches to managing encryption keys. In some cases, there's no formal key management process in place.

Whether key management strategy is fragmented or nonexistent, organizations can be at risk of losing control of their data. These situations call for a solution that can integrate with other key managers and self-encrypting devices using standard protocols to centralize encryption key lifecycle management.

IBM® Guardium® Key Lifecycle Manager delivers streamlined encryption key management and support for your diverse key lifecycle needs by providing a simple solution to the complex problem of encryption key management. Encryption keys have their own lifecycles that are separate from the data that they protect. Guardium Key Lifecycle Manager helps you control key lifecycle processes from initialization and activation through rotation and deletion. The solution helps you simplify and automate manual tasks which can reduce operational costs.

As more data is stored across diverse or hybrid storage environments, there's a growing risk of data loss or compromise. To reduce these risks, data should be encrypted with the organization controlling the keys. Guardium Key Lifecycle Manager helps ensure sensitive information is protected in the event that encrypted data stores are misplaced, misused or stolen.



Centrally manage encryption keys

Guardium Key Lifecycle Manager serves keys at the time of use from a protected, centralized location that stores the key materials. This capability is made possible by its support of proprietary and internationally standardized protocols for serving symmetric and asymmetric keys. Supported protocols include Key Management Interoperability Protocol (KMIP v3.0), IBM Proprietary Protocol (IPP) and Representational State Transfer (REST) which allow Guardium Key Lifecycle Manager to manage encryption keys for IBM and non-IBM solutions. For organizations that want centralized control and policy-driven key management, Guardium Key Lifecycle Manager offers consolidated management of keys across domains and integrates well into most existing security-team methodologies.

Guardium Key Lifecycle Manager provides support for the encryption keys of a wide range of solutions. See this page for more information.

Get strong access management and security while simplifying key configuration and management

Guardium Key Lifecycle Manager allows organizations to define which administrators can perform custodial actions on keys. It can also limit permissions to only the functions that users need to perform their jobs. These role-based access control features let you separate duties by mapping permissions for actions performed against objects and enforcing data isolation and security. Authorized users can also group devices into separate domains. By default, the groups of devices have access only to the encryption keys defined within their group.

Prior to managing its encryption keys, each device is registered with the solution. Each time an encryption device reconnects to request a key, Guardium Key Lifecycle Manager verifies its identity and cryptographically authenticates it using the device’s identifying certificate. Any unknown device is either rejected or placed into a queue to be approved by the administrator. With this strategy, a rogue device is much less likely to be deployed on the network and used to intercept keys.

In addition to strong authentication, there is also enhanced security between the data encryption device and Guardium Key Lifecycle Manager. Temporary session keys are used to encrypt the encryption key and all traffic to the device. This approach to encryption helps improve data security while simplifying key management. The impact on performance is minimal because each encryption solution performs cryptographic tasks instead of reaching across the network.

IBM Guardium Key Lifecycle Manager provides an easy-to-use, web-based GUI that helps simplify key configuration and management tasks.

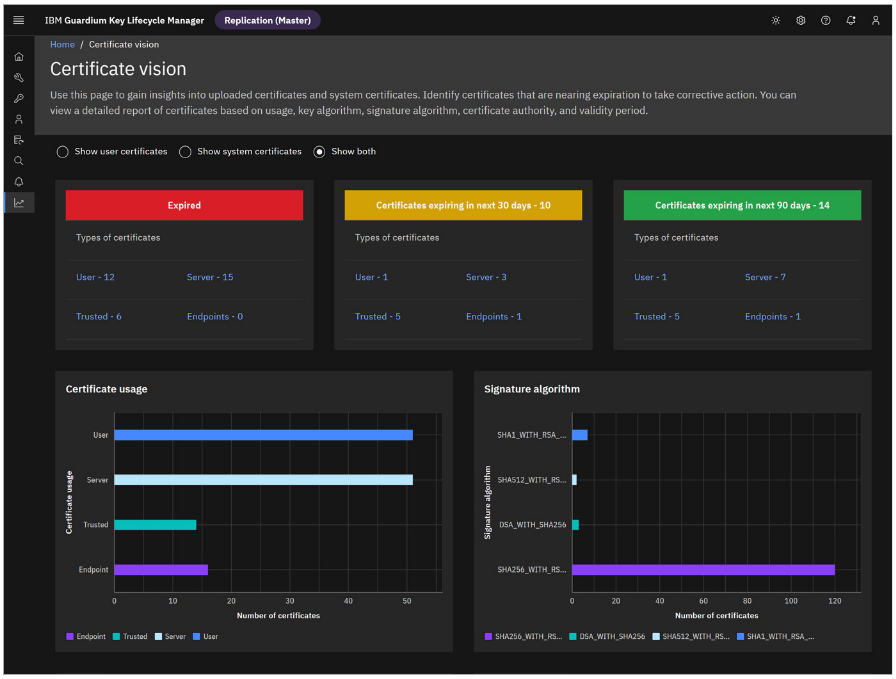
To help ensure that authorized access to protected data is not interrupted, Guardium Key Lifecycle Manager offers two methods for redundancy and high availability. The solution’s master-clone configuration allows users to deploy up to 20 backup copies of the key manager which can serve keys to any connected endpoint. The multimaster configuration provides near real-time synchronization of up to 21 instances across data centers and environments.

While the cryptography inside Guardium Key Lifecycle Manager is validated to FIPS 140-3 Level 1, users also have the option to use FIPS 140-3 Level 2 or Level 3 validated hardware to enhance key security. Guardium Key Lifecycle Manager can be deployed with an optional hardware security module (HSM) to store the master key in order to protect all keys stored in Guardium Key Lifecycle Manager. This capability can be enabled both for installs with existing data or for new installations of Guardium Key Lifecycle Manager.

Guardium Key Lifecycle Manager features a modern, intuitive user interface based on the IBM Carbon Design System. This design focuses on improving navigation, enhancing data visualization and streamlining key management tasks.

Once installed, the GUI allows administrators to perform basic local key lifecycle management and offers not only configuration and setup tools but also audit and compliance support. The software provides three ways to add encryption-enabled devices: Auto-acceptance of incoming devices; approval of devices that require administrators to select and accept from a pending device list; or manual addition of devices for extra security.

Guardium Key Lifecycle Manager also provides numerous methods for key backup and recovery in case of catastrophic failure. Administrators can configure rules for automated rollover of groups of keys so that new encryption keys are used automatically based on a configurable schedule. In this way, administrators can limit the amount of data encrypted with particular keys, minimize exposure when a key is compromised and perform cryptographic erasure of data by deleting relevant keys when data is set to expire. This automated key assignment frees an operations team from having to frequently interact with key management.



IBM Guardium Key Lifecycle Manager Replication (Master)

Home / Certificate vision

Certificate vision

Use this page to gain insights into uploaded certificates and system certificates. Identify certificates that are nearing expiration to take corrective action. You can view a detailed report of certificates based on usage, key algorithm, signature algorithm, certificate authority, and validity period.

○ Show user certificates ○ Show system certificates ● Show both

Expired	Certificates expiring in next 30 days - 10	Certificates expiring in next 90 days - 14
Types of certificates	Types of certificates	Types of certificates
User - 12 Server - 15	User - 1 Server - 3	User - 1 Server - 7
Trusted - 6 Endpoints - 0	Trusted - 5 Endpoints - 1	Trusted - 5 Endpoints - 1

Monitor health and status of managed endpoint certificates

Expired digital certificates can wreak havoc on a network's stability, and poor certificate maintenance can open an organization to security risks such as a man-in-the-middle attack. To help guard against these scenarios, the Guardium Key Lifecycle Manager certificate vision dashboard provides users with a snapshot of the health and expiration status of their endpoint certificates. This dashboard helps reduce security vulnerabilities and avoid potential network disruption. Users can easily identify which certificates require updating and remediation. Then these activities can be executed using an external certificate lifecycle management tool.

Expedite deployment with wizard-based assistance

Guardium Key Lifecycle Manager uses a wizard-based guide to help administrators navigate a series of simple, task-based screens that demonstrate key and device creation and the handling of new device requests. Administrators can also configure different devices to use specific communication protocols such as KMIP.

Once registered, encryption devices appear in the Guardium Key Lifecycle Manager key administration section and are ready for use as a highly secure endpoint. The keys associated with the devices can then be managed through the GUI, including updating, expiring or destroying the keys. Guardium Key Lifecycle Manager key administration welcome page provides critical notices to administrators including information about last backups and available protocols.

Conclusion

IBM Guardium Key Lifecycle Manager is an application that can be deployed on a variety of operating systems including Windows, Unix, Linux, container platforms and IBM mainframes. The application's design and architecture do not require extensive RAM or processing resources. In fact, the solution can typically be deployed requiring only 8 GB of RAM and a dual-core processor.

Thanks to the application's small footprint, it can be deployed as a virtual machine, ready to run in a container such as Red Hat® OpenShift®, Kubernetes or zCX, or on bare metal. This versatility allows organizations to easily manage multiple instances of the solution for redundancy and high availability or for alignment with the organizational structure. See this page for more on technical requirements.

For more information

Discover how IBM Guardium solutions can help you take a smarter integrated approach to safeguarding critical data across your hybrid multicloud environments. Visit ibm.com/guardium.

To learn more about IBM Guardium Key Lifecycle Manager,
please contact your IBM representative or IBM Business Partner,
or visit ibm.com/products/guardium-key-lifecycle-manager.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
December 2024

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

The client is responsible for ensuring compliance with all applicable laws and regulations. IBM does not provide legal advice nor represent or warrant that its services or products will ensure that the client is compliant with any law or regulation.