

Security

Secrets Manager



Securely Manage Sensitive Information with Encryption

Secrets Manager is a service that securely stores and manages customer sensitive information by encrypting it in Secret form. Important information within the application's source code is removed by hard coding and can be inquired by calling the Secret stored in key-value form. Secrets are encrypted with user management keys and stored securely in conjunction with the Key Management Service.



Secure Sensitive Information

In conjunction with the Key Management Service(KMS), the customer's sensitive information is encrypted and stored in key-value form. Users can use encryption keys generated by KMS to protect their information more securely.



Segmented Access Management Policies

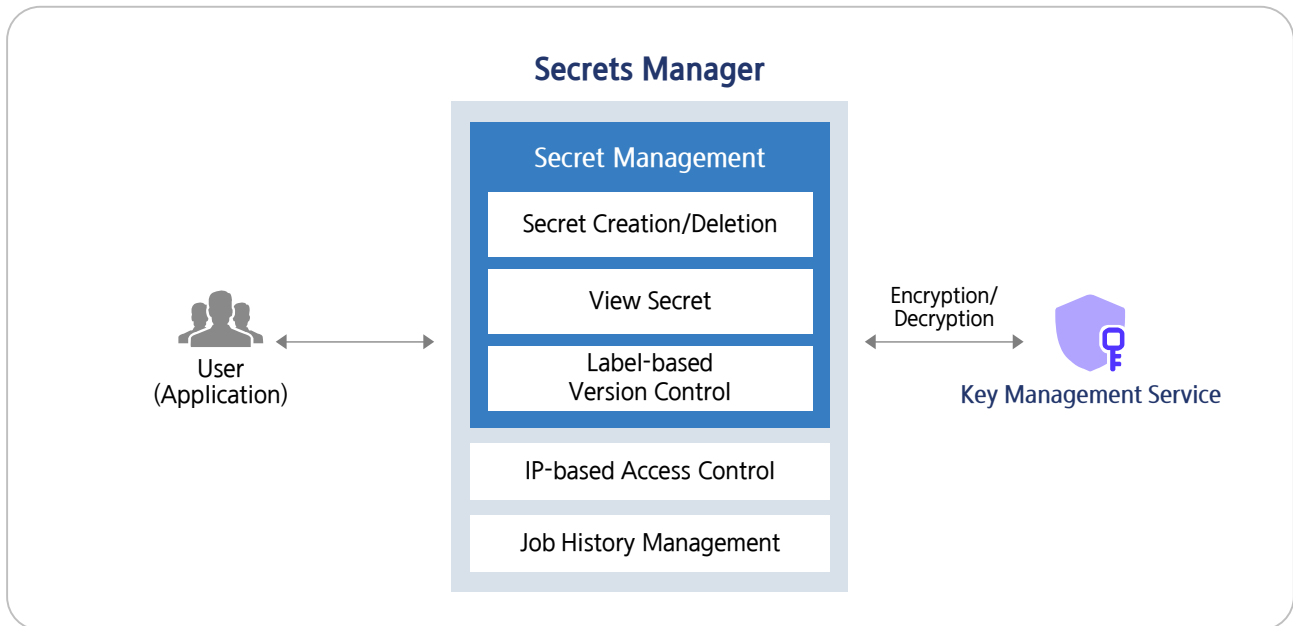
Access control through Identity and Access Management(IAM) and IP-based access control allow for more granular security policies for Secret.



Tracking Security Information History

Monitoring records Secret changes, and labels allow you to track the history of past versions of Secret.

Service Architecture



Key Features

- **Encrypt and store data**
 - Store sensitive information encrypted through KMS's encryption keys
 - Save encrypted with key-value pair, and key-value pairs in Secret can be stored up to 10 pairs
- **Label settings and rollback**
 - Set up to 20 labels in Secret
 - Configure up to 100 Secret versions, and roll-back is available in the requested version
- **Secret's access control**
 - IP-based access control(single IP)
 - Variable Classless Inter-Domain Routing(CIDR) access control of container environments

SAMSUNG SDS

 www.samsungsds.com / cloud.samsungsds.com
 contact.sds@samsung.com / scp_sales@samsung.com
 youtube.com/samsungsds

