Key rotation

Archived: 2026-04-06 01:49:55 UTC

This page discusses key rotation in Cloud Key Management Service. Key rotation is the process of creating new encryption keys to replace existing keys. By rotating your encryption keys on a regular schedule or after specific events, you can reduce the potential consequences of your key being compromised. For specific instructions to rotate a key, see Rotating keys.

Why rotate keys?

For symmetric encryption, periodically and automatically rotating keys is a recommended security practice. Some industry standards, such as Payment Card Industry Data Security Standard (PCI DSS), require the regular rotation of keys.

Cloud Key Management Service **does not** support automatic rotation of asymmetric keys. See Considerations for asymmetric keys in this document.

Rotating keys provides several benefits:

- Limiting the number of messages encrypted with the same key version helps prevent attacks enabled by cryptanalysis. Key lifetime recommendations depend on the key's algorithm, as well as either the number of messages produced or the total number of bytes encrypted with the same key version. For example, the recommended key lifetime for symmetric encryption keys in Galois/Counter Mode (GCM) is based on the number of messages encrypted, as noted at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf.
- In the event that a key is compromised, regular rotation limits the number of actual messages vulnerable to compromise.

  If you suspect that a key version is compromised, disable it and revoke access to it as soon as possible.
- Regular key rotation ensures that your system is resilient to manual rotation, whether due to a security breach or the need to migrate your application to a stronger cryptographic algorithm. **Validate your key rotation procedures before a real-life security incident occurs.**

You can also manually rotate a key, either because it is compromised, or to modify your application to use a different algorithm.

How often to rotate keys

We recommend that you rotate keys automatically on a regular schedule. A rotation schedule defines the frequency of rotation, and optionally the date and time when the first rotation occurs. The rotation schedule can be

based on either the key's age or the number or volume of messages encrypted with a key version.

Some security regulations require periodic, automatic key rotation. Automatic key rotation at a defined period, such as every 90 days, increases security with minimal administrative complexity.

You should also manually rotate a key if you suspect that it has been compromised, or when security guidelines require you to migrate an application to a stronger key algorithm. You can schedule a manual rotation for a date and time in the future. Manually rotating a key does not pause, modify, or otherwise impact an existing automatic rotation schedule for the key.

Don't rely on irregular or manual rotation as a primary component of your application's security.

After you rotate keys

Rotating keys creates new active key versions, but doesn't re-encrypt your data and doesn't disable or delete previous key versions. Previous key versions remain active and incur costs until they are destroyed. Re-encrypting data removes your reliance on old key versions, allowing you to destroy them to avoid incurring additional costs. To learn how to re-encrypt your data, see Re-encrypting data.

You must make sure that a key version is no longer in use before destroying the key version.

Considerations for asymmetric keys

Cloud KMS does not support automatic rotation for asymmetric keys, because additional steps are required before you can use the new asymmetric key version.

- For asymmetric keys used for **signing**, you must distribute the public key portion of the new key version. Afterward, you can specify the new key version in calls to the `CryptoKeyVersions.asymmetricSign` method to create a signature, and update applications to use the new key version.
- For asymmetric keys used for **encryption**, you must distribute and incorporate the public portion of the new key version into applications that encrypt data, and grant access to the private portion of the new key version, for applications that decrypt data.

What's next

- Rotate a key.
- Enable or disable a key.
- Learn more about re-encrypting data.
