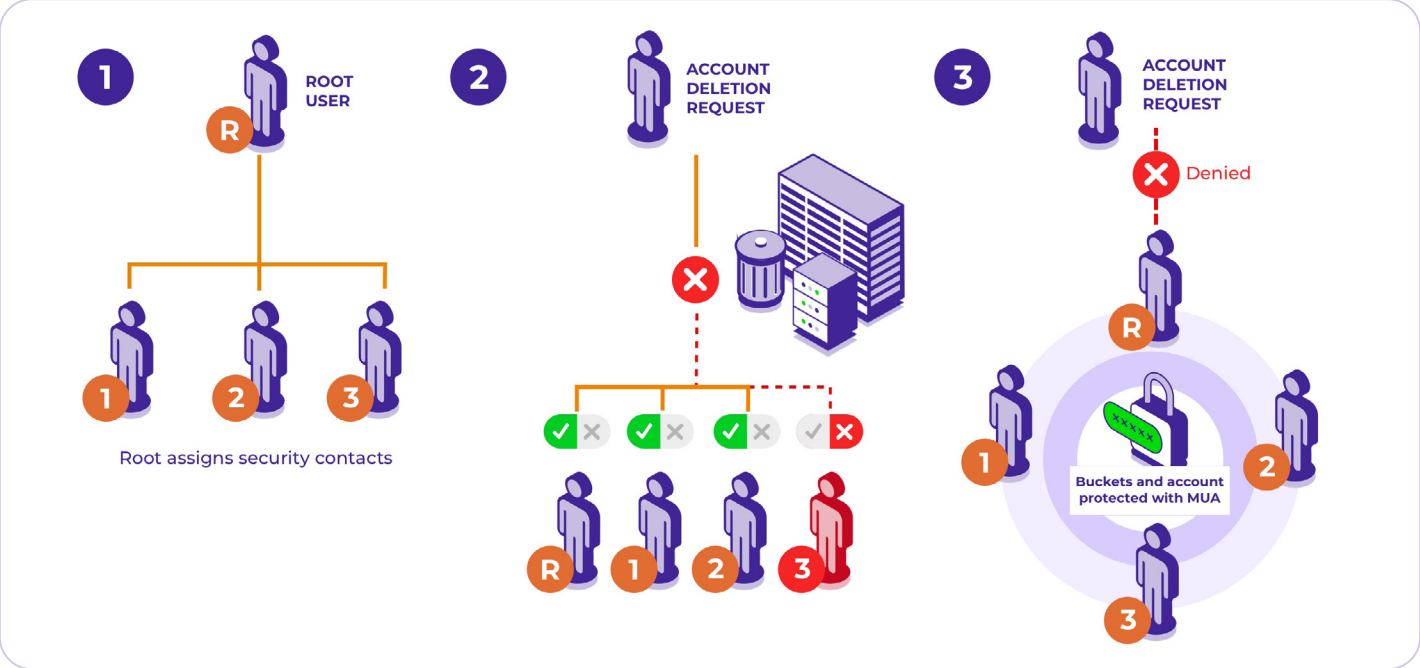
Wasabi Multi-User Authentication

Achieve Account Immutability for Cyber Resilient Cloud Storage

There are multiple ways in which a user can lose data today—from ransomware, cyberattacks, natural disasters, or hardware failure. But one attack vector promises to be the hardest to stop if not properly prepared against: internal user data deletion.

This can happen either by malicious actors who gain access and wipe an account clean, or by employees unintentionally taking irreversible actions. Whether from error or targeted intent, the result can be catastrophic: permanent and complete data or account loss.

Wasabi's Multi-User Authentication (MUA) is specifically designed to protect your organization from this worst-case scenario. It introduces an additional layer of control and verification, ensuring that no single person can take critical actions without oversight.



1. The root user designates up to three security contacts as approvers for account and bucket deletion requests.
2. If a rogue user or unintentional deletion request occurs, those approved contacts receive a message for the approval or denial of that bucket or account deletion, depending on their assigned responsibilities. Each can individually prevent irreversible damage by approving or denying the request. Only acceptance by all contacts produces a successful deletion. Once one contact denies the request, however, it is completely denied.
3. When a deletion request is denied, the requester and all designated security contacts are notified. With MUA, high-risk actions like account and bucket deletion require multi-user approval, preventing irreversible changes.

How does Multi-User Authentication work?

MUA enables an account safeguard for high-risk operations, such as account or bucket deletion. With MUA, up to three security contacts are allowed per account and are designated by the root account user within the Wasabi account. These are trusted individuals who are empowered to approve or deny critical account-level actions. When an account deletion request is made, each contact receives a notification and must explicitly confirm the request before it proceeds. If any one of the contacts denies it, or there is no response after 24 hours of the request, the request is null and void.

Importantly, MUA builds on top of Multi-Factor Authentication (MFA) and does not replace it. Only the Root User can add or remove security contacts, and any changes require MFA validation. Anytime a security contact is added or removed, Wasabi immediately notifies them for verification, ensuring transparency and reducing the risk of account or bucket tampering. This dual-authorization approach is central to a defense-in-depth security strategy, offering a human-in-the-loop barrier to destructive actions that might otherwise bypass technical controls.

Why it matters: the final layer of immutability

If an attacker gains access to the root credentials, or if a mistake is made internally, the account itself and, by extension, all stored data, can be deleted. Even with tools like Wasabi Object Lock enabled to protect objects from being deleted or overwritten, MUA adds additional account security against single points of failure by requiring consensus from your designated security leaders before any irreversible actions can take place.

Multi-User Authentication is more than a feature. It's a foundational pillar of cyber-resilient cloud storage, especially in a time when ransomware threats and internal missteps can destroy years of critical data in seconds. Turn on MUA today and move one step closer to a storage solution that's not only affordable and scalable but also secure by design.

Learn more about MUA and other recommended security features of Wasabi with the Wasabi Documentation Center.