



Data Retention and Deletion Policy

Customer workspace suspension, offboarding, and verified data destruction

Status	Effective
Owner	Atomation LLC
Effective date	July 11, 2026
Classification	Public policy

Atomation LLC minimizes retained customer information and separates reversible suspension from permanent deletion. This policy applies to customer workspaces in the Atomation Okta Assessment service.

Policy summary

Lifecycle stage	Default treatment
Active	Customer access and approved assessment collection are enabled.
Suspended	Access, active sessions, new scans, and scheduled collection are disabled. Configuration and assessment data remain intact for reactivation.
Offboarding	A cancelled workspace remains suspended for 30 days by default. No new customer data is collected.
Immediate purge	An authorized Atomation operator may bypass the offboarding window after reauthentication and explicit permanent-deletion confirmation.
Permanent purge	Atomation removes workspace data from its control plane, assessment engine, and object storage, then verifies that scoped records and objects are absent.
Backups	Daily and monthly encrypted recovery sets normally expire within 30 days and are not copied to a separate NAS archive.

Suspension and reactivation

- Suspension is reversible and reserves the customer slug.
- Client login and existing client sessions are disabled.
- Manual, operator-triggered, API-triggered, and scheduled assessment collection are disabled.
- Customer configuration, connected-org references, assessment history, findings, and reports remain available for reactivation.
- Reactivation requires a new login and does not silently restore a pre-suspension browser session.

Cancellation and offboarding

- The default offboarding period is 30 days in suspended status.
- Atomation may provide an approved export before permanent deletion.
- A customer-authorized immediate-deletion request or explicitly confirmed operator action may bypass the 30-day period.
- Deleting a partner account removes partner access but does not delete or suspend linked customer workspaces.

Permanent deletion

- Permanent deletion requires a suspended workspace, operator reauthentication, and explicit confirmation naming the affected workspace.
- Atomation deletes control-plane records, tenant credentials and keys, SSO and SCIM configuration, workspace users, invitations, assessment runs, snapshots, findings, report artifacts, branding, and other workspace-scoped objects.
- Atomation does not require or attempt deletion of the customer's Okta API Services application during local data destruction. The customer remains responsible for removing that application in Okta.
- The customer slug becomes reusable only after the purge verifies completion.
- A minimal deletion receipt may retain the purge time, non-content workspace reference, receipt digest, operation identifier, and verification outcome. It contains no customer assessment content, credentials, raw payloads, or findings.

Backups and recovery copies

- Atomation does not create a separate customer-data archive on a local NAS.
- Daily and monthly encrypted recovery sets normally expire within 30 days. If backup failure would otherwise leave no validated recovery point for active customers, the sole older encrypted set may be retained temporarily as a documented incident until a replacement validates. It remains inaccessible for ordinary use, and the deletion ledger must be reapplied on restore.
- Backup copies are not available for ordinary product access or customer restoration after permanent deletion.
- Disaster recovery during the backup-expiration window must reapply the deletion ledger before the restored environment becomes available.

Product improvement and schema observations

Atomation does not retain customer content for model or product training. Atomation may retain sanitized, de-identified technical schema observations needed to improve collectors and deterministic rules, including response shape, supported object types, field types, field presence, and compatibility failures.

Before retention, those observations must remove customer values, people, email addresses, Okta org URLs, tenant and application identifiers, secrets, tokens, findings, raw payloads, customer-defined labels that reveal business information, and other information that can identify the customer or its users. Identifiable customer content requires a separate explicit written opt-in and approved handling terms.

Exceptions and records

- A documented legal hold or binding legal obligation may delay deletion of specifically required records.
- Contracts, invoices, tax records, and security-incident records follow separately approved legal and accounting schedules and are not reusable assessment content.
- Reports already downloaded by a customer or partner are outside Atomation's storage control.

Contact

Questions and deletion requests may be sent to support@atomation.io.