backupta

[FedRAMP] Security Configuration Guide

Data classification

☒**External** ☐Internal ☐Confidential ☐Restricted

1. Revision History

Version	Date	Editor	Approver	Description of changes
1.0	February 13th 2026	Nicolas Motte	Paul Martin	Initial version

Table of Contents

2. Objective

This Secure Configuration Guide fulfills FedRAMP's REQUIRED (MUST) documentation for Recommended Secure Configuration. This document explains security-related settings that can be operated only by top-level administrative accounts and their security implications.

3. General Provider Responsibilities

3.1. Recommended Secure Configuration

Providers MUST create, maintain, and make available recommendations for securely configuring their cloud services (the Secure Configuration Guide) that includes at least the following information:

1. Required: Instructions on how to securely access, configure, operate, and decommission top-level administrative accounts that control enterprise access to the entire cloud service offering.
2. Required: Explanations of security-related settings that can be operated only by top-level administrative accounts and their security implications.

Notes:

- These requirements and recommendations refer to this guidance as a Secure Configuration Guide but cloud service providers may make this guidance available in various appropriate forms that provide the best customer experience.
- This guidance should explain how top-level administrative accounts are named and referred to in the cloud service offering.

3.1.1 Backupta’s connection to Okta

Backupta integrates with Okta using API Service Applications.

Customers MUST implement the integration using the following security model:

- Customers MUST configure two separate Okta API Service applications: Read & Write.
- Customers MUST enable Demonstrating Proof of Possession on both client Applications
- Customers MUST configure the clients to use JWKS authentication with the provided URL.
- Customers MUST limit the scopes assigned to the client Applications to the list provided in Backupta’s documentation, shared with the customer.

3.1.1.1 Read Application (Always Active)

The Read application MUST:

- Be permanently enabled.
- Be used for:
    - Backup data

  - Monitoring events
  - Viewing backup status
- NOT allow restore, revert, or deployment actions. This is attained by restricting the assigned scopes to **.read*

This application provides operational visibility without modification capability.

Security Objective:

Ensure daily monitoring activities do not expose write or restore privileges.

3.1.1.1 Write Application (Active on demand)

A separate Write application MUST be used for restore or revert operations.

This application:

- MUST be disabled by default.
- MUST be enabled only during authorized restore/revert activities.
- SHOULD be deactivated immediately after use.

Backupta’s recommended procedure to efficiently enable/disable the Application’s permissions is described in the documentation shared with the customer.

Security Objective:

Minimize standing write privileges and reduce the risk of unauthorized rollback or configuration modification.

3.1.2 Storage Configuration

Backupta supports customer-managed storage in:

- Amazon S3 (and S3 Compatible storages)
- Azure Blob Storage
- Google Cloud Storage

Customers are responsible for securely configuring their storage environment in accordance with their internal security policies and the provider’s best practices.

Customers MUST:

- Use a dedicated bucket or container per Okta tenant.
- Block public access.

- Enforce encryption at rest (provider-managed or customer-managed keys).
- Enforce encryption in transit (TLS 1.2 or higher).
- Configure appropriate retention policies aligned with compliance requirements.
- Enable immutability (Object Lock / Immutable Blob / Retention Lock) where regulatory requirements apply.
- Restrict access to Backupta using least-privilege IAM policies or federated identity.
- Avoid reusing buckets or containers containing unrelated data.

Improper storage configuration may result in:

- Unauthorized data access
- Inability to restore backups
- Accidental deletion of backup data
- Non-compliance with regulatory retention requirements

Detailed configuration instructions and security hardening steps are available in the dedicated storage prerequisite documents, shared with the customer:

- AWS S3 Storage Prerequisites
- Azure Blob Storage Prerequisites
- Google Cloud Storage Prerequisites

3.1.3 Single Sign-On (SSO) and Provisioning

3.1.3.1. Mandatory Use of Single Sign-On (SSO)

Customers MUST integrate Backupta with their enterprise Identity Provider (IdP) using Single Sign-On (SSO).

Backupta supports SAML or OIDC federation with enterprise IdPs (e.g., Microsoft Entra ID, Okta).

Security Requirements:

- Customers MUST have at least one breakglass account.
- All interactive user access MUST be authenticated through the customer’s IdP.
- Except for dedicated breakglass accounts, local password-based authentication MUST be deactivated (guaranteed by design by Backupta)
- MFA MUST be enforced at the IdP level.
- Conditional Access policies (device compliance, network restrictions, risk-based access) SHOULD be enforced by the IdP.
- Access to administrative roles MUST require phishing-resistant MFA where available.

Security Implication:

Using SSO centralizes authentication control, enables enforcement of enterprise security policies, and ensures that access can be immediately revoked through the customer's identity platform. Failure to use SSO increases the risk of orphaned accounts and inconsistent MFA enforcement.

3.1.3.2. Identity Lifecycle Management and Provisioning

Customers MUST use automated provisioning to manage user accounts and role assignments.

Security Requirements:

- User accounts MUST NOT be created manually except for the designated break-glass account.
- Role assignments MUST be managed through IdP group-based provisioning.
- When a user is disabled or removed in the IdP, access to Backupta MUST be automatically revoked.
- Privileged roles (Admin, Write) MUST be assigned via dedicated security groups.
- Role reviews SHOULD be conducted periodically (at least quarterly).

Security Implication:

Automated provisioning ensures timely access revocation and reduces the risk of privilege accumulation. Manual account management increases the likelihood of stale accounts and excessive permissions.

3.1.4 Administrative Roles

3.1.4.1. Top-Level Administrative Access (Super Administrator)

Backupta defines the highest-privilege account as the Super Administrator.

Security Requirements:

- Super Administrator access MUST be limited to a single technical "break-glass" account.
- The break-glass account MUST NOT be used for daily operations.
- The account MUST be used only for:
    - Organization-level configuration changes
    - Emergency recovery scenarios

    - Privileged role recovery
- Credentials MUST be stored in a secure password vault.
- All actions performed by this account MUST be logged and monitored. This can be achieved by integrating Backupta's audit log to a SIEM or regularly exporting them.
- Real-time alerting MUST be configured for any use of this account.

Security Implication:

Improper or frequent use of Super Administrator privileges increases the risk of privilege escalation, tenant-wide misconfiguration, or backup retention modification that could impact data recoverability.

3.1.4.2. Tenant Owner Role (Admin)

Each Backupta tenant MUST have exactly one designated Tenant Owner.

Responsibilities:
- Manages tenant-level configuration.
- Assigns roles to other users.
- Configures backup retention and storage settings.
- Approves restore or deployment operations (where approval workflows are enabled).

Security Requirements:
- MFA MUST be enabled.
- The Tenant Owner role MUST be assigned to a named individual account (no shared accounts).
- The Tenant Owner MUST NOT share credentials.
- Changes to retention, storage, or encryption settings MUST be logged.

Security Implication:

Improper configuration by a Tenant Owner could result in shortened retention periods, disabled immutability controls, or unauthorized access assignment.

3.1.4.3. Write (Operational Administrator) Role

Operational team members SHOULD be granted Write access.

Capabilities:
- Perform restore or revert operations.

- Execute approved deployment actions.
- Manage backup comparisons.

Restrictions:

- Cannot modify organization-level settings.
- Cannot change retention policies.
- Cannot assign privileged roles.
- Cannot delete tenant configuration.

This role supports operational continuity while limiting configuration risk.

Security Implication:

Write access allows operational recovery actions but does not permit structural changes to backup or security controls.

3.1.4.4. Read-Only Role

Personnel without deep expertise in Okta or tenant configuration SHOULD be granted Read-Only access.

Capabilities:

- View backups and event logs
- Review object history and comparisons.
- Monitor restore activity.
- Review Compliance controls

Restrictions:

- No modification capability.
- No restore execution.
- No configuration changes.

Security Implication:

Read-only access enables transparency and oversight without introducing operational or configuration risk.

3.2. Use Instructions

This Secure Configuration Guide can be requested by authorized federal agency personnel and authorized third-party assessors by contacting:

Email: compliance@backupta.com

Subject Line: Request for Secure Configuration Guide

Required Information in Request:

- Agency name and point of contact
- Purpose of request (e.g., security assessment, authorization review, operational use)
- Requester's role

Upon verification of the request, the guide will be provided within 2 business days.