OBJECT FIRST

White Paper

Fleet Manager: Unified Fleet Operations for Object First Deployments

A Zero Trust Approach to Distributed Backup Storage Operations

Executive Summary

Operating, securing, and monitoring distributed backup storage environments is becoming increasingly difficult. Modern backup needs often span multiple sites, storage clusters, and client environments, all of which add increasing complexity to this critical component of any risk management strategy. As organizations rapidly scale up infrastructure and service providers expand client footprints to accommodate accelerating AI and data needs, they need backup storage that can keep pace more easily and, more than that, simplify operations wherever possible to reduce risk.

The backup, IT, and infrastructure teams (along with service providers) responsible for ensuring data recovery and security face mounting practical challenges with authentication, VPNs, monitoring, data visibility, and maintaining ransomware-resilient backup storage. These challenges are amplified in environments where visibility is fragmented, remote access is inconsistent, and operational tasks must be repeated across multiple locations.

Fleet Manager is a secure, cloud-based service engineered to monitor distributed Object First deployments so CIOs and service providers can reduce complexity and focus on what matters. Built on Zero Trust and Secure by Design principles (as defined by CISA), Fleet Manager ensures Object First appliances keep data absolutely immutable while enabling secure remote access, centralized fleet visibility, and powerful monitoring operations.

This white paper outlines the challenges of distributed storage management, the capabilities of Fleet Manager, and how organizations and service providers can use it to reduce management complexity.

The Challenge: Distributed Backup Storage at Scale

Storage Management Complexity

Organizations responsible for backup storage are being asked to do more with less. They must protect all data within shrinking backup windows, keep systems online, and scale quickly to support new business needs. At the same time, teams are expected to take on new projects without adding overhead, avoid burnout, and consistently meet recovery objectives. They also need to keep client data secure and available while managing complexity and maintaining steady performance across multiple locations.

These demands become harder to meet when visibility is scattered across different tools and processes. Multiple identity systems make it difficult to enforce uniform security policies, while insecure unenrollment procedures in many tools can be manipulated during an attack.

Administrators often rely on manually extracting and combining data from several sites to gain end-to-end visibility, which slows down troubleshooting and increases the chance of missing important alerts. Limited insight into consumption, billing, and support contracts makes planning and budgeting more difficult.

There are also risks to the backup storage itself. Administrative access often allows destructive actions, undermining the very purpose of immutable storage. Lack of granular, role-based access controls and isolation for multi-tenant environments limits flexibility to secure storage systems. Remote access tools that are intended to simplify management, but rely on inbound connectivity, can inadvertently expand the attack surface. These insecurities create opportunities for attackers while compromising the work of IT teams trying to maintain secure, reliable operations.

Service Provider Challenges

Service providers face additional challenges as they manage distributed client environments, each with its own authentication systems, operational requirements, and compliance expectations. As environments grow, these inconsistencies create operational strain and increase the risk of misconfigurations or delays.

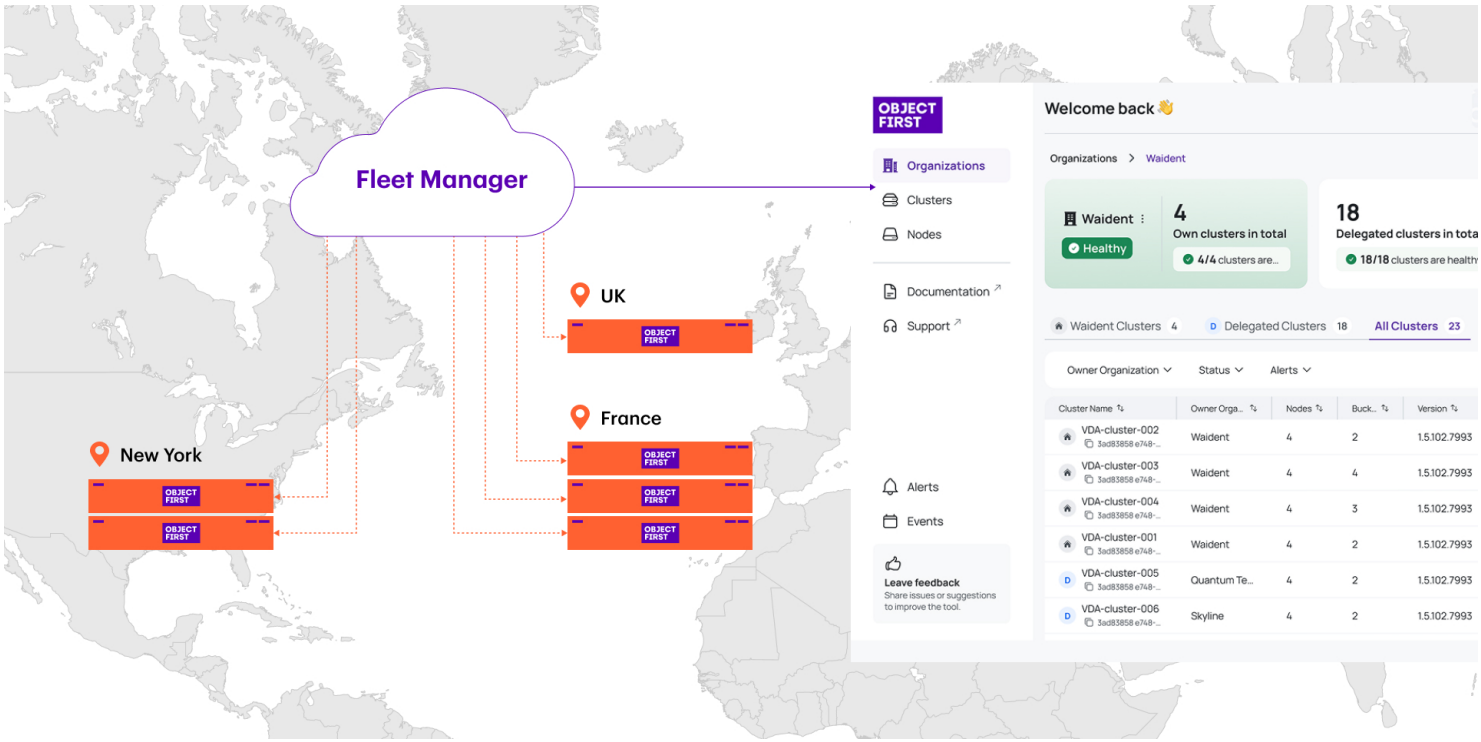
Without a unified dashboard that consolidates client data into a single location, providers must navigate separate interfaces and workflows for each client. Understanding billing, consumption, and support contracts becomes a manual and error-prone process, and delivering secure, scalable remote access across tenants requires significant effort.

Providers must also monitor offsite or client-owned hardware, adding logistical overhead that reduces efficiency and profitability. As client expectations rise, service providers are under pressure to deliver reliable, high-quality managed services without increasing costs.

The Cost of Inaction

Failing to address these operational and security challenges introduces significant risks and costs. It takes longer to restore data and business operations following ransomware incidents, especially when visibility gaps delay troubleshooting. Operational efficiency suffers as teams spend more time managing administrative tools and less time on higher-impact projects. Inconsistent access controls and fragmented security practices create unseen risks, while service providers struggle to scale their offerings without adding staff or sacrificing quality. Ultimately, these challenges erode confidence in the organization's ability to maintain ransomware-resilient backup storage—the last line of defense against company data loss.

Introducing Object First Fleet Manager



Product Overview

Object First Ootbi backup storage appliances solve these fundamental challenges by delivering absolutely immutable, Zero-Trust backup storage, which means attackers cannot modify or delete backup data, even with admin privileges. Object First Fleet Manager extends this with a secure cloud-hosted platform that oversees distributed Object First environments, enabling admins, CIOs, and service providers to streamline operations and concentrate on their highest-value priorities. Fleet Manager delivers:

- Reduced operational overhead with a cloud-based service that simplifies access management with integration of Entra ID.
- Centralized fleet dashboard to monitor utilization and health of distributed deployments.
- Multi-tenant access and visibility, with cluster, systems, and usage information and alerts.

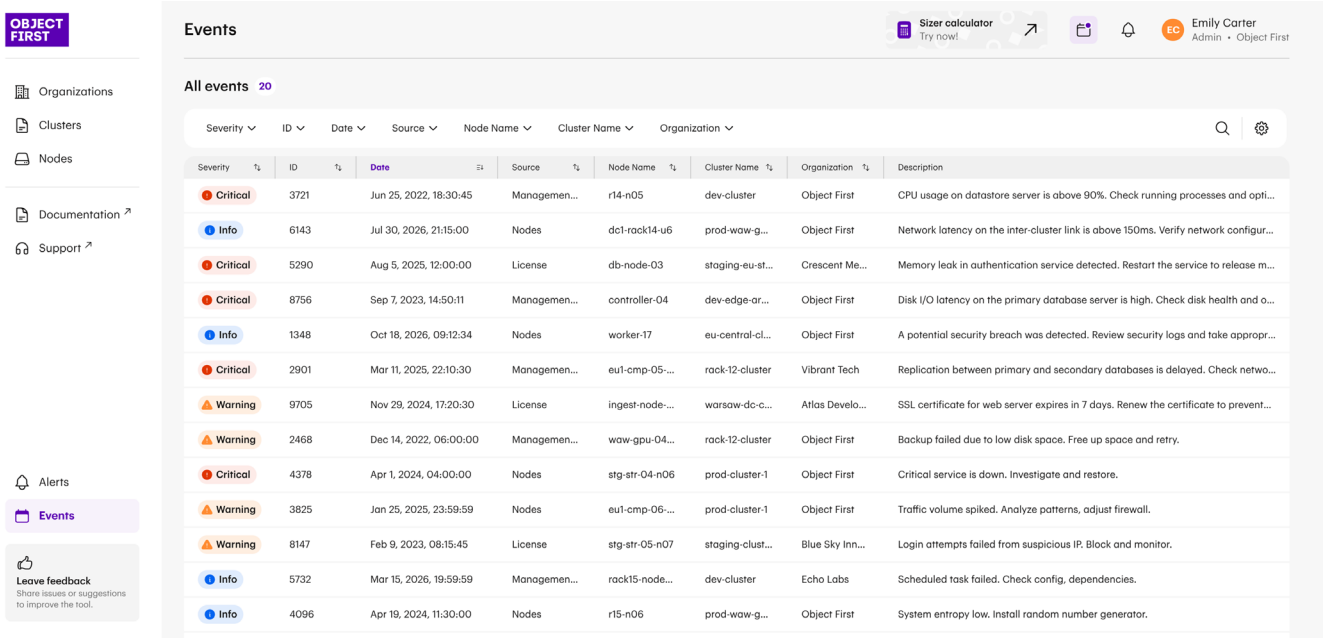
Fleet Manager is available to all Object First customers with active support agreements at no additional cost.

Secure Remote Access	• Zero Access cloud-based SaaS • No VPN required • Integrated authentication via Entra ID • Outbound-only connectivity • No destructive actions possible
Centralized Fleet View	• Multi-cluster monitoring • Storage utilization and hardware health • Centralized view of data usage and capacity trends • Single dashboard for all deployments
Cluster Operations Visibility	• Alerts for outages, overages, threats • RBAC and isolation for multi-tenant environment • Consumption and support contract dashboard • Usage information and operational insights

Key Features

Fleet Manager supports Object First's mission to deliver secure, simple, and powerful backup storage.

Secure Remote Access

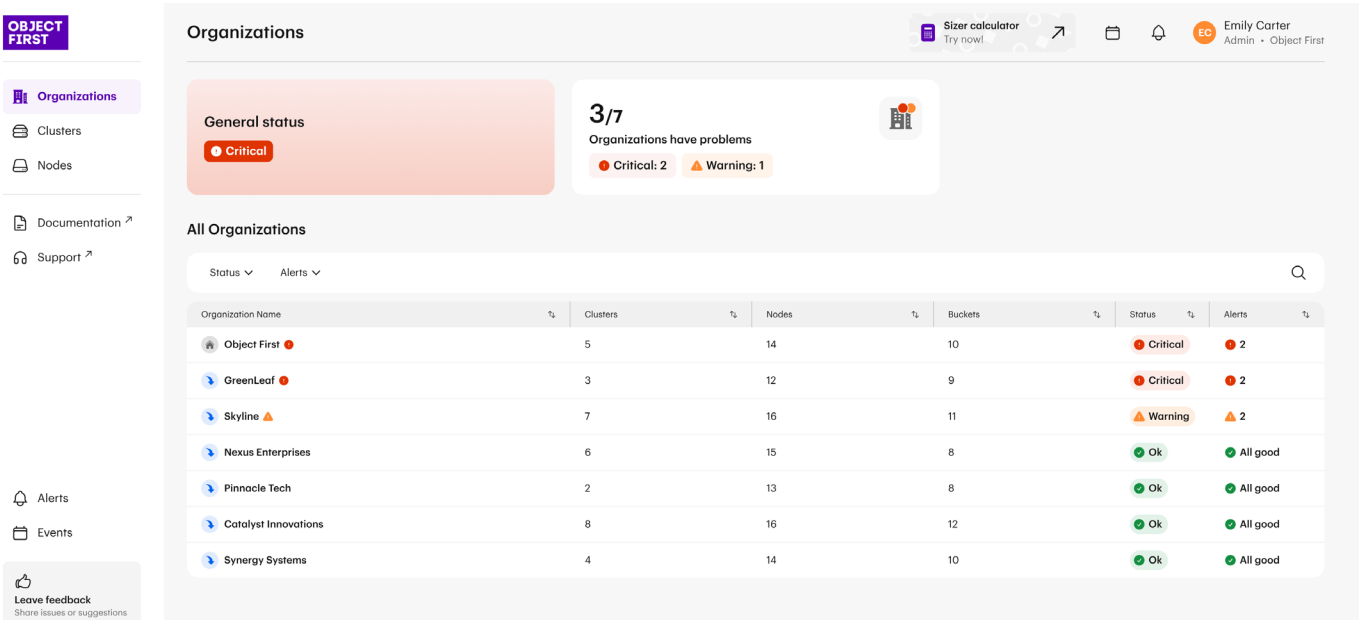


Fleet Manager is engineered exclusively for telemetry-based visibility and does not permit inbound access or remote control. No Ootbi backup data is ever received or visible to Fleet Manager. Its architecture follows a unidirectional, outbound-only monitoring model that removes the need for VPNs and reduces the attack surface through firewalled, one-way communication.

Authentication integrates with Entra ID, while role-based access controls are managed at the application layer to separate administrative responsibilities between onboarding users and non-administrative operators. Secure-by-Default and Secure by Design principles (as defined by CISA) guide every interaction, supported by least-privilege access, and alerts and events. Together, these capabilities ensure that remote operations never compromise the Absolute Immutability of backup data.

Fleet Manager uses the customer's own authentication system—including their identity provider, MFA requirements, and user-management rules—so organizations retain full control over who can access their environments. When customers choose to delegate cluster access to a service provider or another organization, Fleet Manager applies a dual-control process: Object First moderates the request, and the receiving organization must accept it before access is granted. This approach strengthens governance across multi-organization deployments while keeping day-to-day user management in the customer's hands.

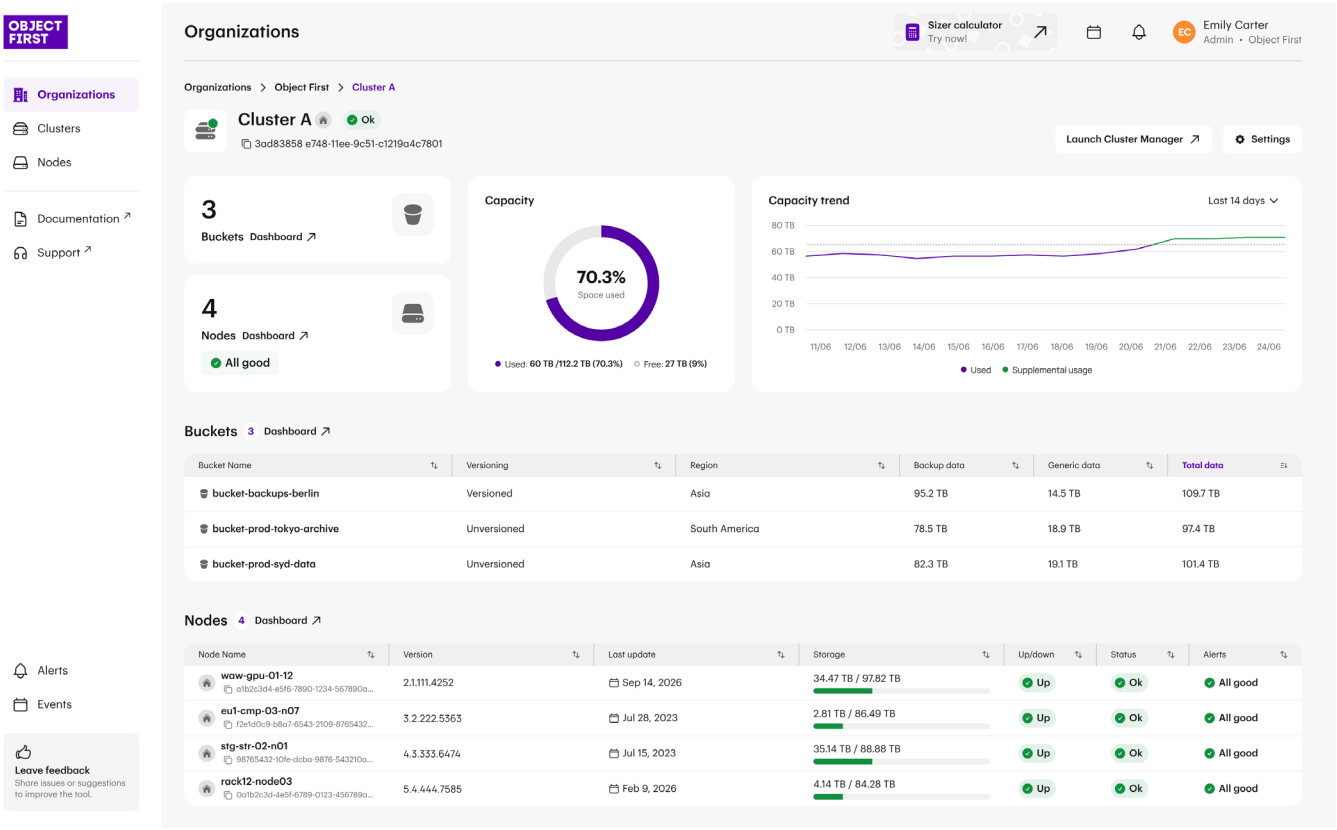
Simple, Centralized Fleet View



Fleet Manager simplifies distributed storage management by removing the operational overhead traditionally associated with multi-site environments. Enrollment is initiated directly from the Ootbi Cluster Manager UI and requires no additional hardware or software to configure, manage, or maintain. Once connected, enrolled clusters appear in a unified dashboard that consolidates monitoring, utilization, and alerting into a single-screen view.

Teams gain visual insights and clear visibility into consumption agreements and support contracts, enabling faster decision-making without manual data gathering. By consolidating visibility and reducing friction, Fleet Manager moves teams away from juggling scattered applications, subscriptions, and tools—and toward streamlined, centralized management in a single, intuitive location.

Powerful Cluster Operations



Fleet Manager delivers the operational capability required to monitor distributed environments at scale. Multi-tenant visibility enables service providers to oversee client environments from a single interface, while alerts and system events provide rapid visibility into outages, overages, and threats, ensuring high-priority activity is easy to identify and act on.

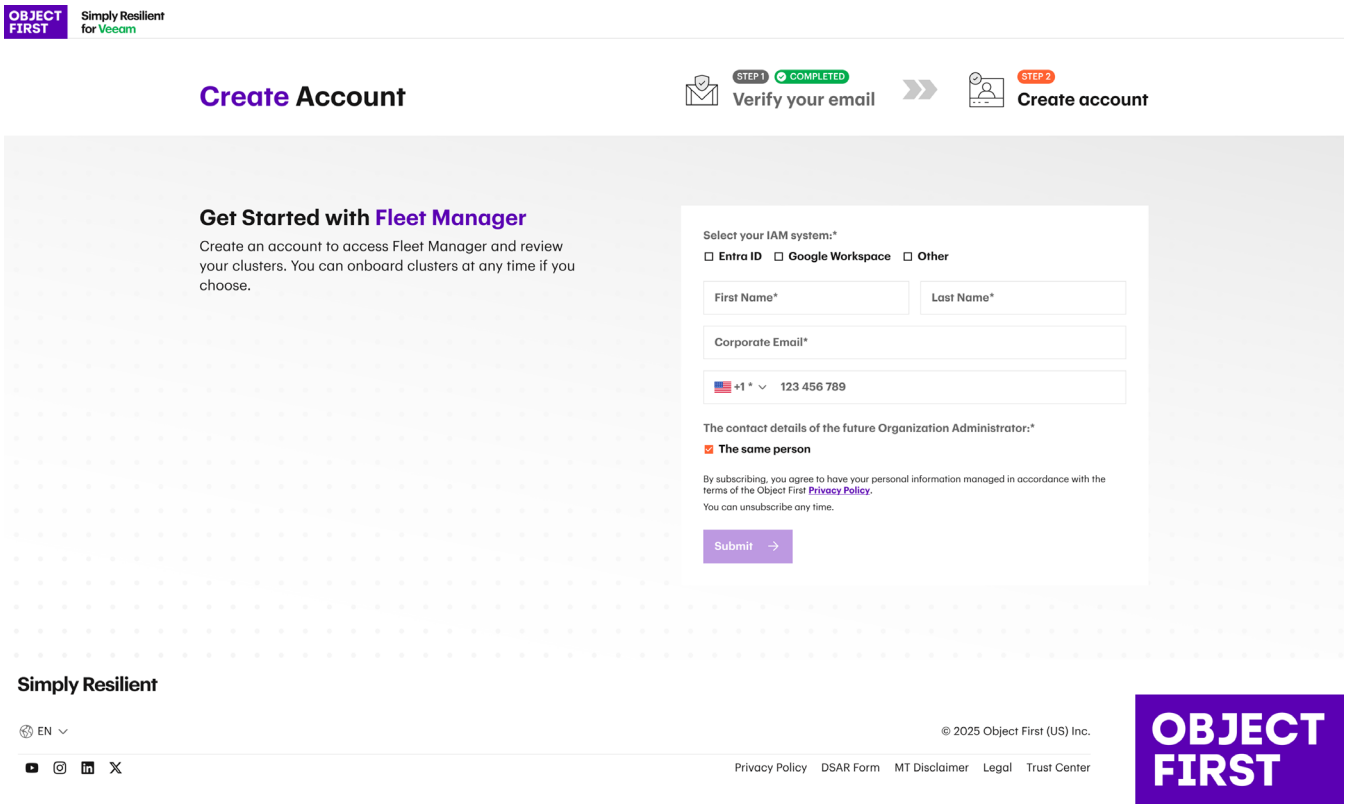
Additional capabilities, such as hardware health reporting and Honeypot alerts, expand visibility into operational and security-relevant activity. When Honeypot is enabled on the array, its alerts are viewable in the Fleet Manager UI, giving teams early awareness of suspicious behavior by detecting reconnaissance attempts against a built-in decoy that mimics a Veeam Backup & Replication server. These alerts help teams quickly identify high-priority activity without adding complexity or compromising Absolute Immutability.

With telemetry-based cloud connectivity and support for diverse client footprints, Fleet Manager empowers clients to better understand their distributed clusters at all times and act, whereas traditional solutions only present clients with information in fragmented pieces.

How Fleet Manager Works

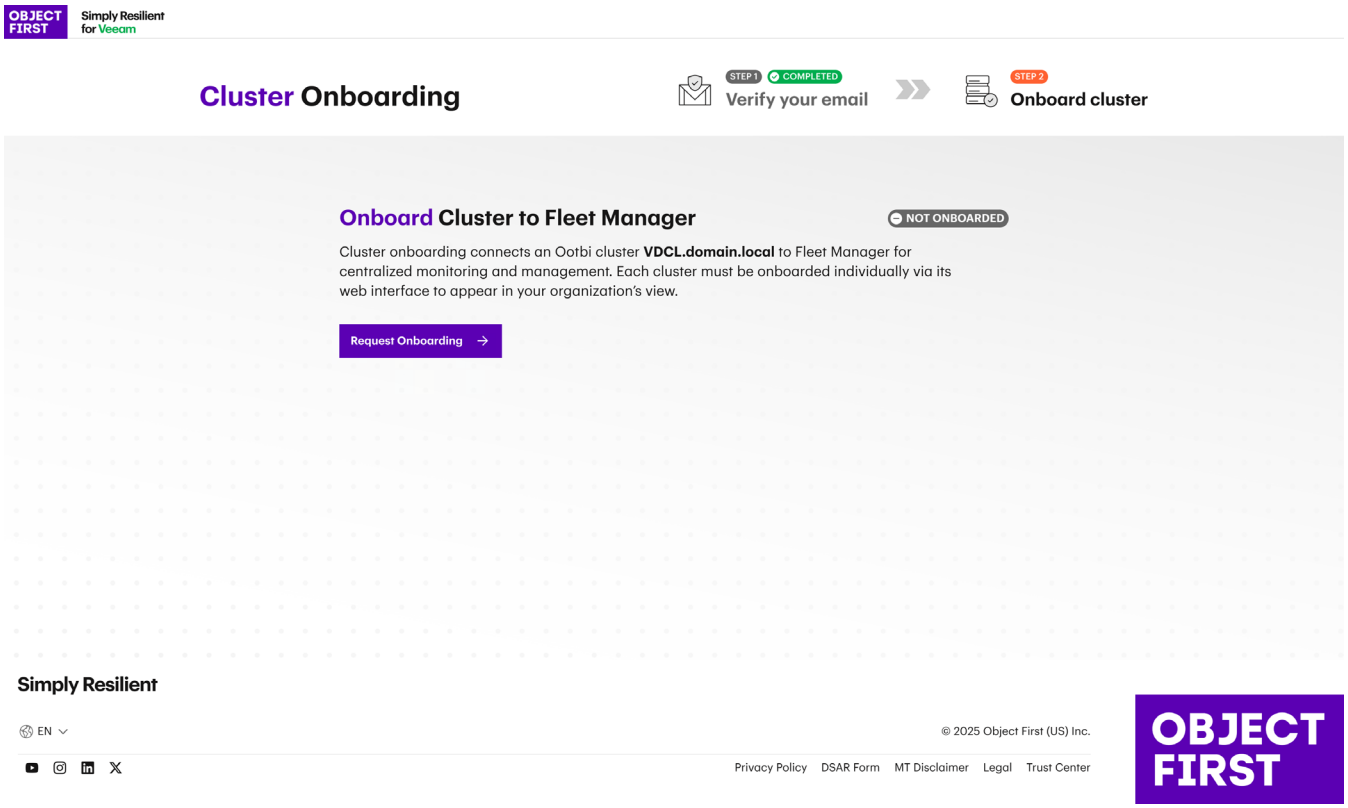
Organization Onboarding

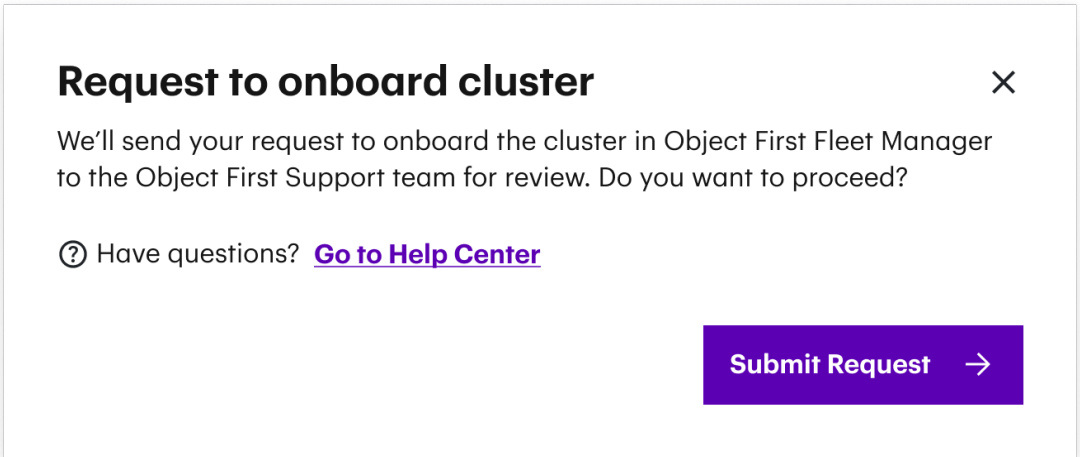
Organization onboarding is a one-time registration that establishes a secure organizational scope. This process creates authentication boundaries and RBAC isolation for multi-tenant environments. It must be completed before clusters can be added.

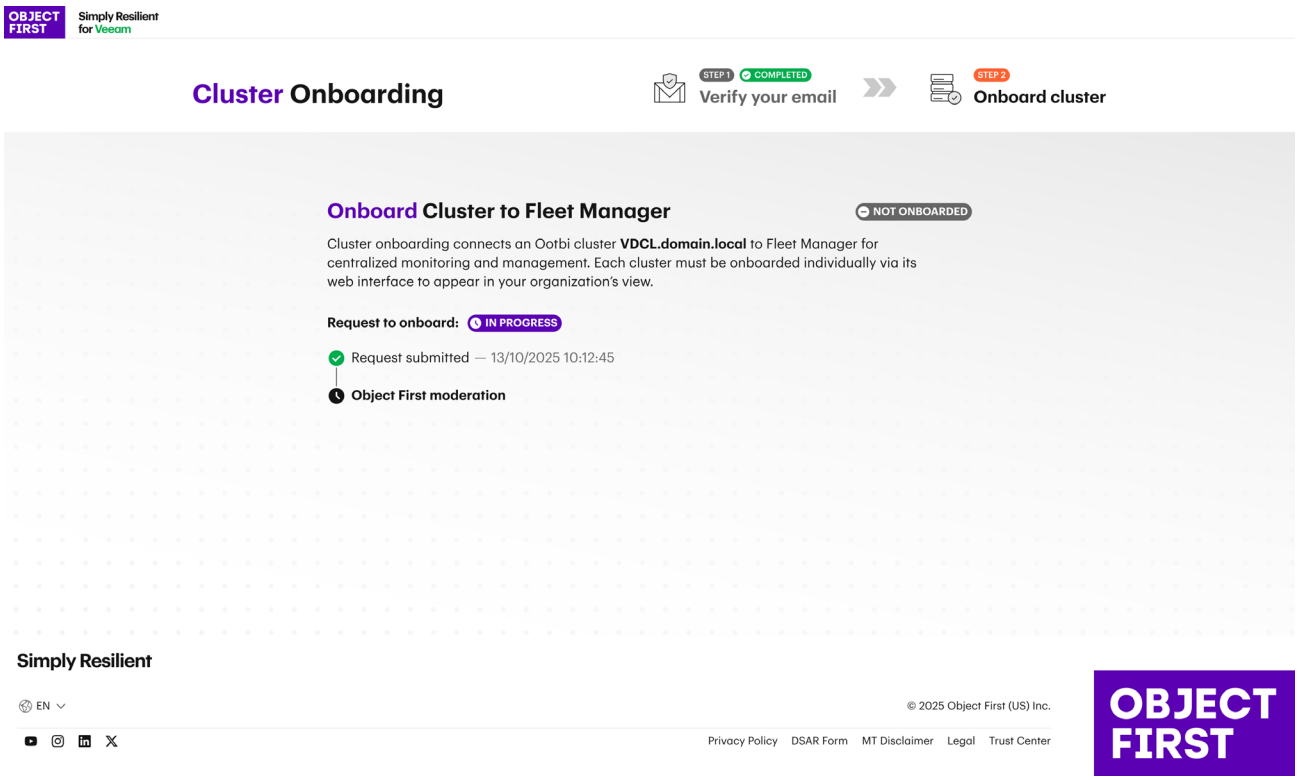


Cluster Onboarding

Cluster onboarding connects individual appliances or clusters to Fleet Manager. Cluster onboarding is required before delegation and is initiated from the cluster's web interface.

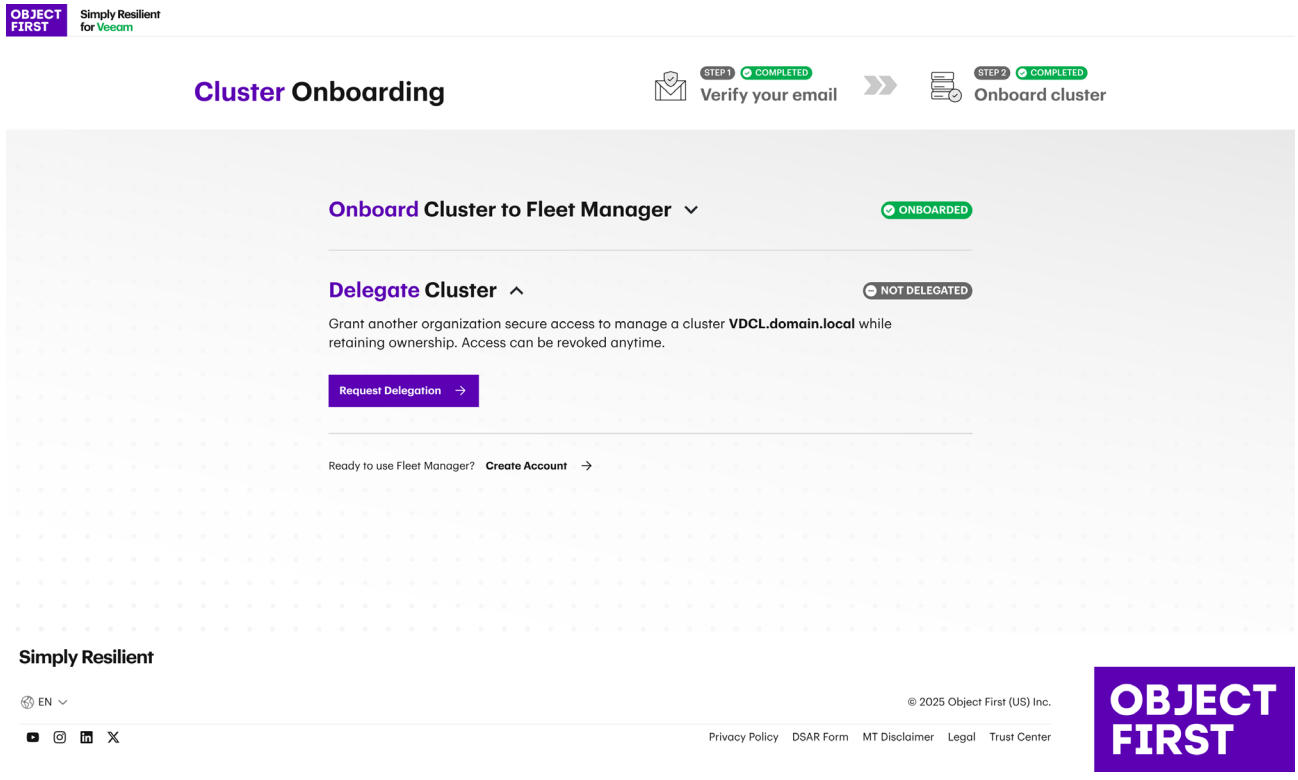


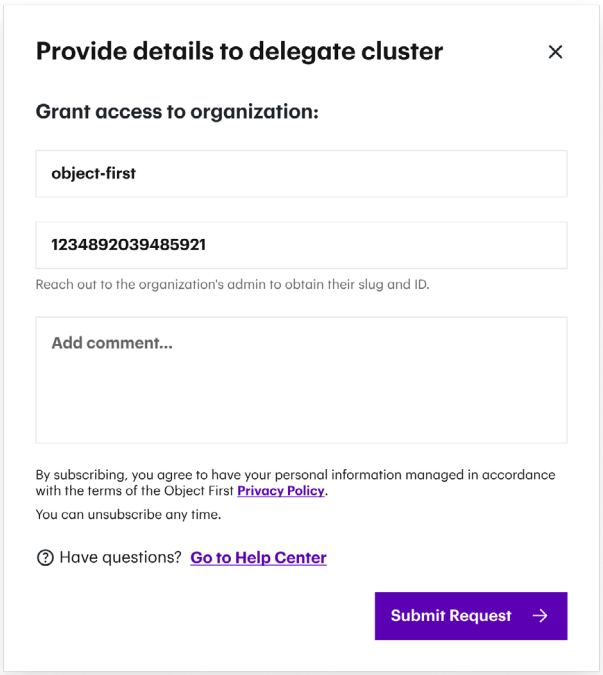


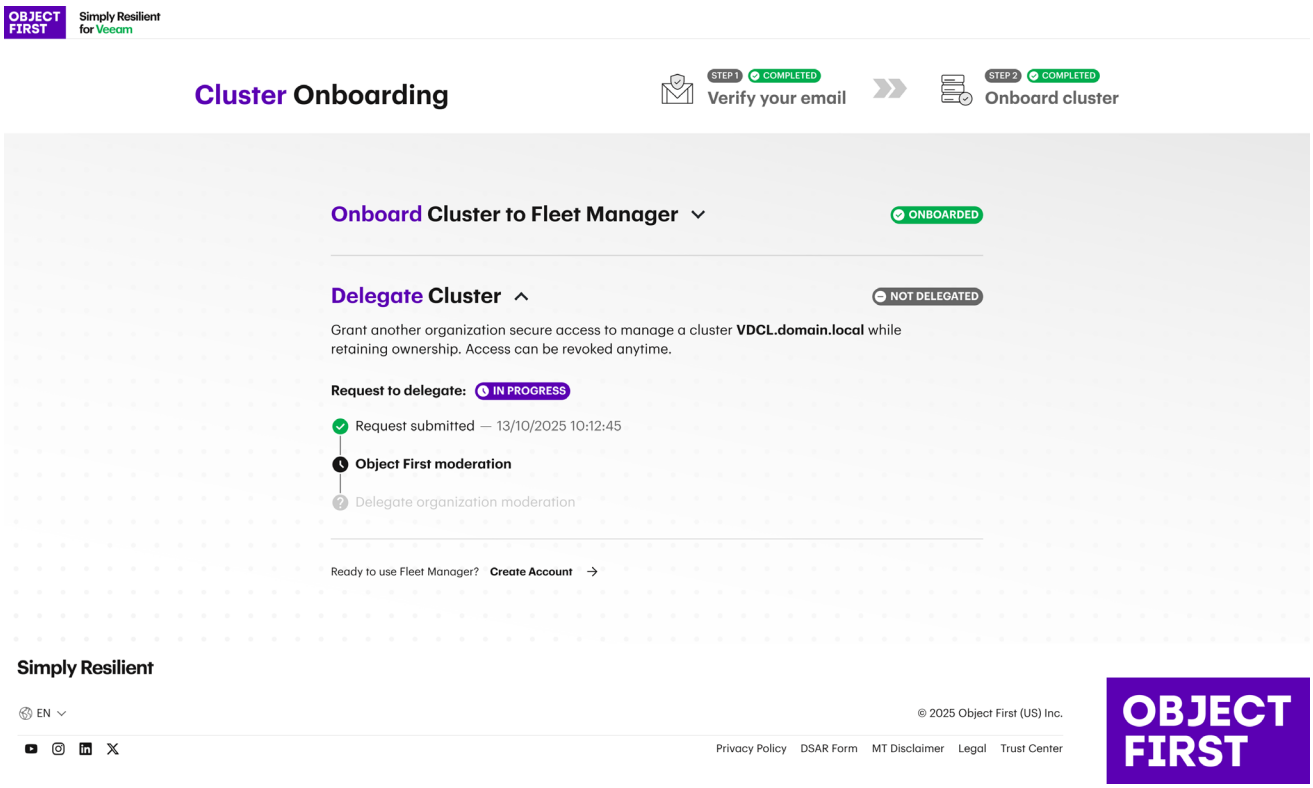


Cluster Delegation

Cluster delegation allows an owning organization to grant access to another organization, such as a service provider. Delegation maintains ownership while enabling operational visibility. It follows a one-to-one model, is revocable at any time, and supports co-managed IT, MSP/VCSP operations, and distributed IT teams.







Why Object First Fleet Manager?

Fleet Manager is a continuously evolving SaaS platform that strengthens resilience, reduces complexity, and scales fleet operations alongside your backup footprint—helping organizations and service providers stay focused on what matters most: meeting recovery objectives, maintaining ransomware-resilient backup storage, and supporting expanding environments without increasing overhead. With centralized monitoring, secure remote access, and a unified view of every Object First deployment, teams can spend less time managing tools and more time ensuring data is protected and ready when it's needed most.

Appendix

Understanding the difference between Fleet Manager and Ootbi Cluster Manager

Fleet Manager elevates your ability to manage distributed Object First appliances, but it's important to understand the differences between its capabilities and those of the local Cluster Manager.

	Fleet Manager	Cluster Manager
Cluster Management	Remotely monitor all enrolled clusters	Single cluster management
Monitoring	Complete fleet usage and health information from a single dashboard	Local cluster usage and health
Access Control	Delegate access to remotely view devices to various tenants	Manage roles for single cluster access
Alerts	Receive instant alerts on all clusters and individual devices	Receive alerts on devices within cluster
Backup Data Management	No backup data is ever transmitted or visible to Fleet Manager	Create S3 keys and buckets

Supported Use Cases

Fleet Manager has three use cases: client-only, client + service provider, and service provider only.

Client-Only Monitoring

Enterprise clients own and manage all clusters. Fleet Manager provides unified visibility, monitoring, and alerts.

Client + Service Provider Collaboration

Client owns clusters; service provider is granted delegated access. Both parties maintain visibility and operational alignment. Ideal for co-managed IT.

Service Provider–Only Access to Client Clusters

Client owns clusters; service provider handles day-to-day operations. Supports MSP/VCSP managed services models.

Use Case Summary Table

Use case	Organizational Onboarding	Cluster Onboarding	Delegation
Client monitoring their own clusters	Yes	Yes	No
Client + service provider	Yes	Yes	Yes
Service provider managing client cluster	SP only	Yes	Yes

OBJECT FIRST

Simply Resilient for Veeam

Contact Us →