RelativityOne alerting and monitoring: A comprehensive administrator's guide

RelativityOne provides robust built-in monitoring through its Security Center, Queue Management, and Instance Details dashboards, but **native email alerting is limited primarily to security events and imaging jobs**. For comprehensive job failure notifications across processing, production, and other agents, administrators must leverage the REST API ecosystem to build custom alerting solutions or integrate with external monitoring platforms. The platform does not offer native integrations with tools like Splunk or Azure Monitor, requiring middleware development for enterprise monitoring setups.

Native alerting capabilities center on security events

RelativityOne's **Security Center** serves as the primary built-in alerting system, delivering automated notifications for security-related events to members of the Security Notifications group. relativity Alert types include multiple failed logins, brute force attempts (**50+ failures within one hour**), login method changes, new login locations, and lockbox setting modifications. Alerts are categorized by severity—Critical, High, Medium, and Low—and support three states: Unresolved, Dismissed, and Resolved. relativity Relativity

The platform provides **automated remediation workflows** for certain security alerts. When administrators mark specific alerts as "Resolved," the system automatically reverts configuration changes, disables compromised accounts, or removes unauthorized group memberships. Relativity For example, resolving a "Brute Force Login" alert automatically disables the affected user account. relativity

Beyond security, native email notifications exist for **Imaging Sets only**. The Email Notification Recipients field on imaging sets accepts semicolon-delimited addresses and triggers emails upon completion—whether successful or with errors. relativity Processing jobs, production jobs, and other agent-driven tasks lack native email notification capabilities, representing a significant gap for operations teams.

Monitoring agent health requires multiple dashboard touchpoints

Agent monitoring in RelativityOne spans several administrative interfaces rather than a single unified dashboard:

Instance Details Tab displays real-time alerts for disabled agents and unresponsive servers, with direct navigation links to the Agents tab for troubleshooting. Relativity The Alerts section surfaces anything requiring immediate attention, while the Queues section shows status for Production, Branding, OCR, and Imaging queues.

Queue Management Tab provides instance-level visibility across all job queues with varying degrees of administrative control: relativity

Queue Type	Monitoring	Mass Operations Available
Processing and Imaging	Full status, documents remaining, priority	Cancel, Resume, Change priority
Production	Status, priority, workspace	Retry, Cancel, Change priority
OCR	Job status	Change priority
dtSearch	Indexing status	View only
Branding	Job progress	Change priority, Export list
PDF	Conversion status	Cancel jobs

Worker Monitoring Tab tracks processing and imaging worker health with metrics including threads in use, memory consumption (MB), CPU activity, tasks per minute, and last activity timestamp. Relativity Worker status displays as Idle, Running, or "Service not responding." Relativity Relativity

For agent failure detection, **RelativityOne's internal SRE team monitors stuck jobs** automatically. When processing jobs become stuck, the system creates internal priority incidents for engineering resolution— relativity but this monitoring is not customer-facing, and administrators receive no direct notification.

Agent-specific monitoring considerations vary by type

Different agent categories have distinct monitoring requirements and configurations:

Single-instance agents (one per environment):

- Telemetry Metrics Transmission Agent
- Billing Agent
- Workspace Delete Manager
- Workspace Upgrade Manager Relativity

Resource pool agents (one per pool or server):

- Branding Manager (up to 4 per pool)
- Analytics Cluster Manager (1 per Analytics server)
- Content Analyst Index Manager (1 per Analytics server)
- Analytics Categorization Manager (2 per Analytics server) Relativity

Processing Agents require the Server Manager agent to be running for status visibility. Relativity Relativity Jobs showing "Paused" status typically indicate agent issues. Relativity Processing History provides comprehensive tracking with auto-refresh options at 30-second, 1-minute, or 5-minute intervals. Relativity Relativity

dtSearch Index Agents automatically retry network-related errors up to three times at 30-second intervals. Relativity Worker status appears in Current Index Details, and fragmentation levels display in red when exceeding thresholds. Relativity

Integration Points Agents auto-deploy during application installation Relativity and track jobs through statuses: Pending → Validation → Processing → Completed/Failed. Relativity After maximum consecutive failed attempts, scheduled jobs stop automatically, and the "Next Scheduled Runtime (UTC)" field becomes blank. Relativity Relativity

Imaging Manager runs at a default interval of 3600 seconds (do not modify) and handles cleanup of stuck imaging jobs. One instance per environment is required. Relativity

Scheduled job monitoring lacks proactive notification

Monitoring scheduled jobs and scripts requires manual dashboard review or API polling:

Integration Points scheduled jobs track failures through the Job History tab. Relativity The Job History Errors tab captures item-level and job-level errors with system-generated descriptions explaining why jobs stopped. Relativity When consecutive failures exceed the maximum threshold, automation halts entirely. Relativity

Automated Workflows support scheduled triggers with configurable patterns and can send email notifications via the Send Email Checkpoint action. This provides one avenue for job-completion notifications, though setup requires workflow configuration per use case.

Script monitoring uses the Audit application—filter for RelativityScriptExecution action to view frequency, execution times, and performance impact. Relativity The Execution Time (ms) field helps identify long-running scripts causing performance degradation. Relativity relativity

For comprehensive scheduled job alerting, administrators must build custom solutions using the Processing Job Manager API, which returns job status, progress metrics, and error information that can be polled and forwarded to notification systems.

Third-party integration requires custom development

RelativityOne provides no native integrations with external monitoring platforms. Splunk, Azure Monitor, Datadog, and PagerDuty connections require building custom middleware:

Integration Type	Native Support	Implementation Path
Splunk	❌	Audit API → custom export → Splunk ingestion
Azure Monitor	❌	API polling → Azure Functions → Log Analytics
Datadog	❌	External Logging from custom apps
PagerDuty	❌	Event Handler webhooks → PagerDuty API
SIEM platforms	❌	Audit API data extraction

Key APIs for custom monitoring solutions:

- **Agent Manager API**: Add workers, delete unresponsive agents, develop monitoring for agent messages Relativity
- **Processing Job Manager**: Run/cancel jobs, retrieve processing set summaries including errors and status
- **Production Queue Manager**: Cancel, retry, set priority, retrieve job status
- **Audit APIs**: Query comprehensive audit records including user actions, timestamps, execution times
- **Notifications API**: Programmatically send emails requiring "Send Email Notification" admin permission Relativity

Outbound webhooks are not natively supported, but Post-Save Event Handlers can call external URLs via HTTP requests when objects are created or modified. Relativity This pattern enables event-driven alerting to external systems.

For custom application logging, Relativity recommends **External Logging** to services like New Relic, Datadog, or Seq—providing near real-time telemetry with finer control than internal logging mechanisms.

Best practices for comprehensive alerting implementation

Security alert thresholds follow Relativity's recommended configuration: resolve Critical and High alerts within 15 days, Relativity maintain at least two administrators in the Security Notifications group, Relativity enable Two-Factor Authentication, and monitor users inactive for 30+ days. Relativity

Agent interval configuration should follow these guidelines:

- Alert Manager agent: 30 seconds (recommended) Relativity
- Most agents: 5-second check-in interval (default) Relativity
- Structured Analytics Workers: minimum 4 workers, each with 1 GB RAM relativity Relativity

Infrastructure performance thresholds for monitoring:

- SQL disk read latency: <8ms (best), <20ms (acceptable)
- SQL write latency: 3-5ms for transaction logs relativity
- Page Life Expectancy: calculate as (DataCacheSizeGB / 4GB) × 300 seconds Relativity

Escalation procedure best practices:

1. **Critical alerts**: Investigate immediately, contact support@relativity.com Relativity
2. **High severity**: Investigate promptly, resolve within 15 days
3. **Medium severity**: Investigate each instance, determine business impact Relativity

4. **Low severity**: Review for unusual patterns, batch processing acceptable [Relativity] [Relativity]

Proactive monitoring approach includes notifying Relativity via the "Incoming Project Details: RelativityOne" form before large projects to ensure adequate capacity [Relativity] for Imaging, OCR, Branding, and Productions. [Relativity] [relativity] The MaxAnalyticsIndexIdleDays setting automatically disables unused analytics indexes. [Relativity]

Community and documentation resources for deeper learning

Official documentation at help.relativity.com covers Security Alerts configuration, Processing Administration, Audit application use cases, and Agent Management guides. The Infrastructure Planning Considerations PDF provides capacity planning guidance.

Relativity Community (community.relativity.com) offers peer support forums, technical guides, and access to the RelativityOne Service Status page for maintenance and issue notifications.

Training paths include Relativity Certified Administrator (RCA) certification requiring 3+ months experience and 40 hours of study. [Relativity] Relevant specialist certifications cover Analytics, Infrastructure, and Processing.

Partner resources from major implementers—Epiq, Lighthouse, Consilio, HaystackID, and FTI Technology—[Relativity]offer managed services with enhanced dashboard reporting and proactive monitoring capabilities beyond native RelativityOne features. [HaystackID]

Conclusion

RelativityOne's monitoring architecture provides strong visibility into system health through multiple dashboards but lacks unified alerting for non-security events. The Security Center delivers comprehensive security alerting with email notifications, [Relativity] while job and agent monitoring requires manual dashboard review or custom API integration. Organizations requiring proactive alerts for processing failures, agent issues, or scheduled job problems must invest in custom development using Relativity's REST APIs and Event Handler framework. The **recommended approach** combines Security Center for security events, Queue Management dashboards for operational monitoring, Audit application for forensic analysis, and custom API-based solutions for automated alerting to external platforms. For enterprises with existing monitoring stacks, building a middleware polling service that queries RelativityOne APIs and forwards events to Splunk, Datadog, or PagerDuty represents the most practical path to comprehensive alerting coverage.