APPLIED AI FIELD NOTES — EXECUTIVE BRIEF

Mastering the Claude Compliance API

Tom M. Gomez

May 25, 2026

Luminity Digital

INTELLIGENCE, ENGINEERED. DELIVERED.

INTRODUCTION & ACCESS

INTRODUCTION TO COMPLIANCE API

Comprehensive Compliance Monitoring

- Centralized API for tracking user and organizational activities
- Supports **audit logs**, chat, file, and project data retrieval

Enterprise-Grade Security & Retention

- Data retained for up to **6 years** for activity records
- Granular access controls via scoped API keys

Key Use Cases

- Enables **audit pipelines** for compliance review
- Facilitates eDiscovery and DLP enforcement

ACCESS AND ENABLEMENT

Who Can Access the Compliance API?

- Available to **Claude Enterprise** and **Claude Platform** customers (excluding Public Sector).
- Console organizations receive Activity Feed access; Enterprise organizations unlock full API capabilities.

Enablement Steps for Organizations

- Primary Owners (Enterprise) or Admins (Platform) initiate enablement in Organization settings.
- Enablement cascades to all linked organizations under the parent.

Role Requirements for Access

- Only **Primary Owners** (Enterprise) or **Admins** (Platform) can create API keys.
- Role-based access ensures secure and controlled API usage.

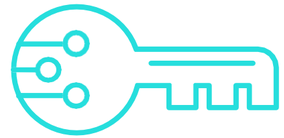
API KEYS AND SCOPES EXPLAINED

Understanding API Key Types

- Compliance Access Keys unlock full API capabilities for Enterprise organizations.
- Admin API Keys provide access to the Activity Feed only in Claude Console.

Scope Selection & Permissions

- Choose scopes like **read:compliance_activities** or **read:compliance_user_data** based on integration needs.
- Scopes are immutable after creation; create new keys for different permissions.



Key Management Best Practices

- Store keys securely in a secrets manager; never in source control.
- Rotate keys regularly and delete compromised keys immediately.

DATA HANDLING & ACTIVITY FEED

ACTIVITY FEED FUNDAMENTALS

Comprehensive Activity Tracking

- Captures organization-wide events including chats, files, projects, and administrative actions
- Supports audit, eDiscovery, and compliance monitoring

Long-Term Data Retention

- Activity Feed records are retained for **6 years**
- Activities are queryable within 1 minute of occurrence

Granular Access via API Scopes

- Endpoints require specific scopes: **read:compliance_activities** for Activity Feed, others for user and org data
- Compliance Access Keys unlock full API; Admin API keys access Activity Feed only

RETRIEVING CHATS, FILES, AND PROJECTS

Accessing Chat Content

- Retrieve chat metadata and full message content using the Compliance API with the **read:compliance_user_data** scope.
- Supports incremental review and export for compliance and audit needs.

Managing Files and Attachments

- Download original user uploads, tool-generated files, and assistant-created artifacts by their unique IDs.
- Project attachments include both binary files and plain-text documents, each accessible via dedicated endpoints.

Project Metadata and Attachments

- Bundle related chats, instructions, and knowledge base content for comprehensive project oversight.
- List and retrieve project attachments for eDiscovery and DLP workflows.

eDiscovery and DLP Workflows

- Enable electronic discovery exports and enforce data loss prevention by programmatically retrieving and deleting content.
- Hard-deleted content is **immediate and permanent**; ensure proper authorization before deletion.

DELETING CONTENT SECURELY

Permanent Deletion of Data

- Compliance API enables **immediate and irreversible** removal of chats, files, and projects.

Hard-Delete Endpoints

- Dedicated endpoints ensure secure deletion—no recovery window after action.

Pre-Deletion Requirements

- All chats must be detached from a project before the project can be deleted.

Compliance and Authorization

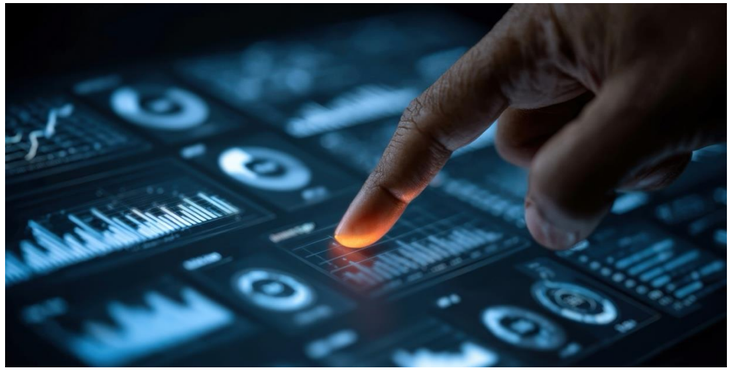
- Explicit authorization and correct API scopes are required for deletion operations.

INTEGRATION, RETENTION, & SECURITY

INTEGRATION PATTERNS & SIEM CORRELATION

Activity Feed Consumption Strategies

- Choose between **window polling** for scheduled, stateless ingestion or **cursor-driven incremental reads** for real-time, low-latency updates.
- Both methods ensure at-least-once delivery and require careful cursor management to avoid missing or duplicating events.



SIEM Integration and Event Correlation

- Compliance API activities can be joined with SIEM logs using actor fields like **user_id**, email_address, and ip_address.
- Correlate API access events with network and identity logs for comprehensive security monitoring.

Key Fields for Log Joining

- Leverage **actor.user_id** for stable identity mapping across systems.
- Use **created_at** timestamps for time-window correlation and audit trail completeness.

RETENTION & DATA MANAGEMENT

Long-Term Activity Feed Retention

- Compliance activities are stored for **6 years**, ensuring robust audit trails.

Organization-Controlled Content Policies

- Chat, file, and project data retention is managed by each organization's own policy.
- Content hard-deleted via Compliance API is **immediately and permanently** removed.

Export and Archival Strategies

- Export Activity Feed records for legal holds or extended audits beyond 6 years.
- Archive chat and file content before retention windows expire to ensure eDiscovery readiness.

ERROR HANDLING & TROUBLESHOOTING

Understanding Error Types

- Identify common errors: authentication, permission, rate limits, and resource conflicts.
- Error responses include clear type and message for troubleshooting.

Effective Troubleshooting Strategies

- Resolve authentication issues by verifying API keys and scopes.
- Address permission errors by creating new keys with required scopes.
- Handle rate limit errors by monitoring headers and implementing backoff strategies.

Integration Best Practices

- Persist pagination cursors for reliable data retrieval.
- Deduplicate activities using unique IDs to ensure data integrity.
- Log request IDs and error details for support escalation.

SECURITY & COMPLIANCE INTEGRATIONS

Feature	Details
Audit Log Events	Compliance API includes audit logs for full visibility across Claude deployments
Security Platform Integrations	Supports integration with SIEM tools (Splunk, Datadog, Sentinel, Cribl) for monitoring activity
Chain of Custody	Exported records should include provenance metadata: source endpoint, query parameters, timestamp, and content hash

MANAGING AND ROTATING API KEYS

Secure Key Rotation Process

- Create a new API key with identical scopes before retiring the old one.
- Update integrations to use the new key and verify successful access.
- Delete the old key immediately after migration to prevent unauthorized use.

Responding to Key Compromise

- Delete compromised keys without delay to halt further access.
- Audit the Activity Feed for **compliance_api_accessed** events linked to the compromised key.
- Rotate any downstream credentials that may have been exposed.

Ensuring Access Continuity

- Maintain valid pagination cursors during key rotation; cursors are scoped to the organization, not the key.
- Keys do not expire automatically; manage and rotate proactively for ongoing security.

WRAP-UP & REFERENCES

TAKEAWAYS & BEST PRACTICES

Strengthen Enterprise Governance

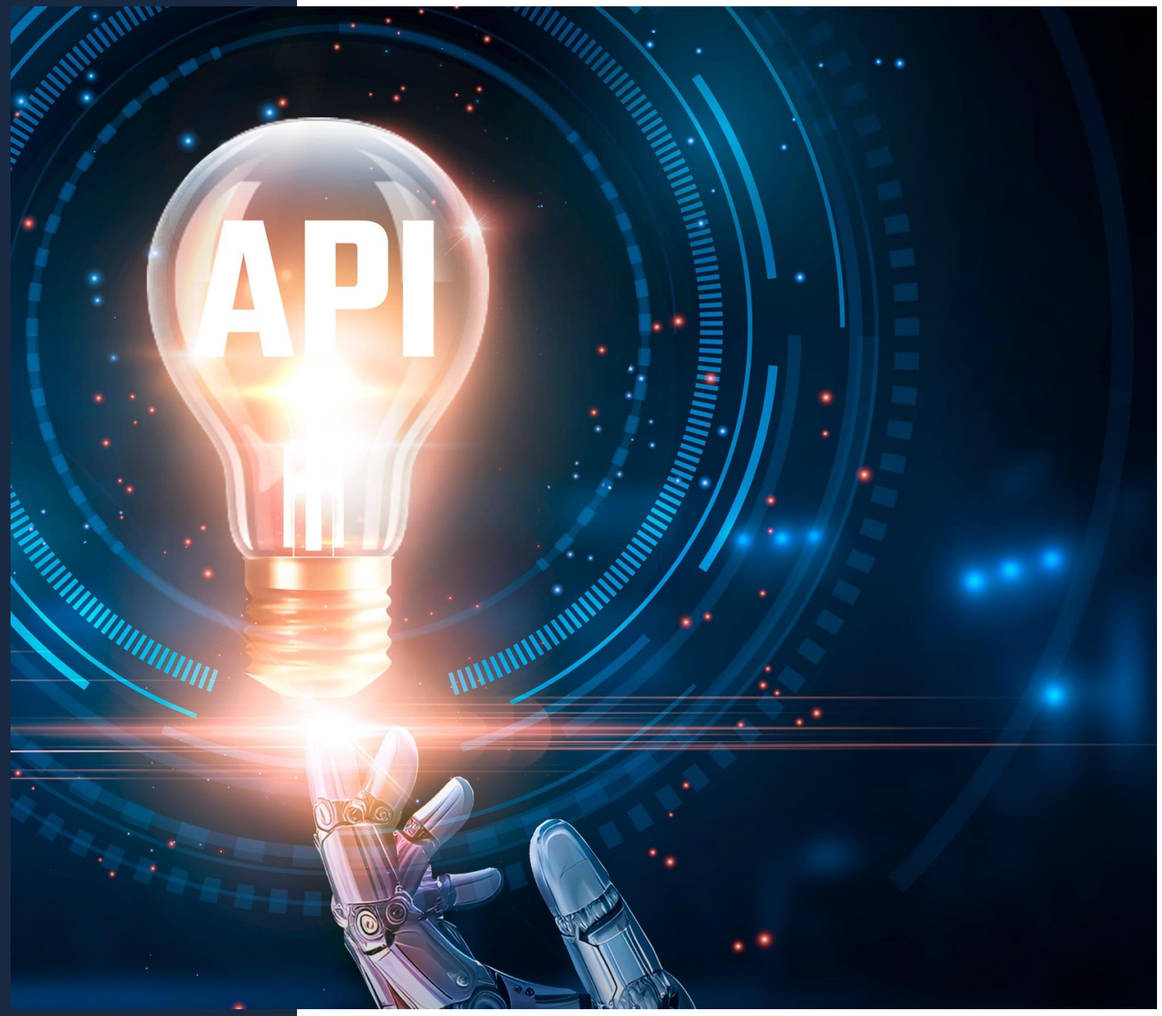
- Utilize the Compliance API to monitor and control organizational activities across all Claude deployments.
- Enable full visibility into chats, files, and projects for compliance and audit needs.

Key Management & Data Retention

- Create and manage API keys with **scoped permissions** for secure access.
- Rotate keys regularly and store secrets securely to prevent unauthorized access.
- Export activity feed and content before retention windows expire; hard-deleted data is **irrecoverable**.

SIEM Integration & Monitoring

- Correlate Compliance API events with your SIEM using user IDs, email addresses, and IP addresses.
- Track compliance_api_accessed activities to audit who accessed sensitive data.



4 QUESTIONS FOR THE CIO-CISO-CCO MEET

1) Who owns the SIEM integration – and which pattern?

- Window polling or cursor-driven reads – which one, and who owns it: security or platform?

2) What's our authorization gate before hard delete?

- Deletes are permanent and irrecoverable – is there a named approval workflow before this ships?

3) Does this feed cover Cowork – or is that a blind spot?

- The API doesn't audit Cowork. Do regulated workloads stay off it until coverage lands?

4) Are we exporting ahead of the retention cliff?

- Content ages out under our own policy. Are we archiving before the window closes?

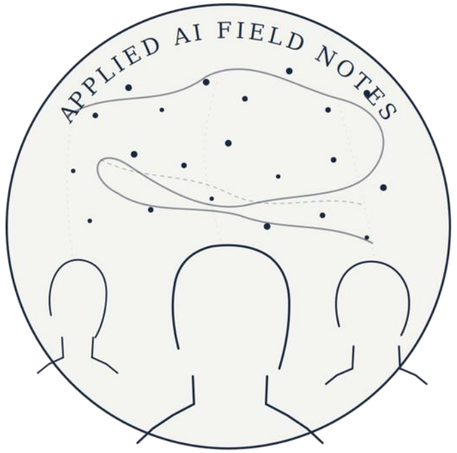
Connect with Us

Read our Insights

REFERENCES

Mapping the empirical evidence. Discovering the patterns that matter for Agentic AI in production.

Read the detailed insights on the Luminity Digital Blog https://www.luminitydigital.com/insights



Subscribe to our Weekly Newsletter | **Follow us on LinkedIn** - https://www.linkedin.com/company/luminity-digital

KEY REFERENCES:

- **Claude API Guide –** https://platform.claude.com/docs/en/manage-claude/compliance-api
- **Access the Compliance API -** https://support.claude.com/en/articles/13015708-access-the-compliance-api
- **Compliance API Reference** - https://platform.claude.com/docs/en/api/compliance
- **Claude Support – Claude Compliance API Integrations -** https://support.claude.com/en/articles/15167101-get-started-with-claude-compliance-api-integrations

RELATED REFERENCES:

Access Audit Logs - https://support.claude.com/en/articles/9970975-access-audit-logs#h_41cdad187a
Data Exports - https://support.claude.com/en/articles/9970975-access-audit-logs#h_41cdad187a

This brief is an independent educational work; its content has not been reviewed or endorsed by Anthropic. Claude and the Claude Compliance API are products of Anthropic, PBC; all referenced documentation and trademarks remain the property of Anthropic.