

# Audit Viewer

Section	Description
Feature Area	Troubleshooting / IT and Integrations
Navigation	Admin → Troubleshooting → Audit Viewer
Alt Navigation	Menu → IT and Integrations → Audit Viewer
Primary Function	Monitor, filter, and review all admin configuration change events across the Genesys Cloud organization
Typical Use Cases	Compliance auditing, change management, security review, troubleshooting unexpected configuration changes

The Audit Viewer enables administrators to filter and view events that Genesys Cloud generates based on service actions for administrative functions. It provides two modes: a full-page viewer with detailed filtering and a mini footer viewer accessible from any admin page.

## Study Notes

Topic	Explanation
Audit Viewer	Tool that logs and displays admin-level configuration events across the org
Full-Page Viewer	Main audit interface with complete filtering and event detail — opened from Admin or Menu
Mini Viewer (Footer)	Lightweight version available at the bottom of any admin page; less detail than full viewer
Event	A logged action triggered by a user or an upstream service/API
Entity	The object being acted upon (e.g., a queue, a flow, a user)
Property Changes	Detail view shows values before and after each change
Related Events	Upstream or downstream events linked to the selected event
RemoteIP	IP address of the user who triggered the event (visible in event details)
Real-time vs Async	The UI viewer shows <b>real-time query</b> results only; async queries require the API or Amazon EventBridge

Topic	Explanation
Amazon EventBridge	Integration that allows orgs to consume <b>all</b> audit events — useful for backup or ingestion into external log tooling

# Permissions

Action	Permission Required
View audit events	Audits > Audit > View
View interaction audit trail (separate)	Audits > Interaction Details > View

“ The **Admin role** is also listed as a prerequisite for full use of the Audit Viewer.

# Navigation

Task	Path
Open full-page viewer	Admin → Troubleshooting → Audit Viewer
Alt full-page path	Menu → IT and Integrations → Audit Viewer
Open mini footer viewer	Bottom of any admin page under <a href="#">Menu → IT and Integrations</a> → hover → click <b>Show audits footer</b>
Close mini footer viewer	Click <b>Hide audits footer</b>
Go from footer to full page	Click <b>Link to full page audit viewer</b> icon in the footer

# Viewer Modes

Mode	Description	Detail Level
Full-Page Viewer	Main audit log interface with date range, service filter, entity filter, user filter, and event detail panel	Full
Mini Viewer (Footer)	Lightweight footer panel visible from any admin page	Limited

# Filtering Options (Full-Page Viewer)

Filter	Description
Date Range	Select Start and End dates/times. Default: current day. <b>Maximum interval: last 14 days</b>
Filter by Service	Select Service Name → Entity Type → Action to narrow results
Filter by Entity	Enter an Entity ID to find all events affecting a specific object (e.g., a specific queue ID)
Filter by User	Enter a user name to see all events performed by that user
Refresh	Apply filters and reload results

“ **Important:** The UI viewer only supports queries for the **last 14 days**. For events older than 14 days, use the **Audit APIs** available in the Genesys Cloud Developer Center.

## Event Detail View

Clicking any event in the results opens the Details panel, which shows:

Detail Field	Description
Who performed the action	User name, or API / upstream service if system-generated
Causing event link	If an upstream service triggered the event, a related link is available
RemoteIP	IP address of the user who triggered the event
Property Changes	Before and after values for each changed property
Related Events	Linked upstream or downstream events — click <b>See related audits</b>

## Data Retention & API Access

Method	Scope	Notes
Audit Viewer UI	Last 14 days (real-time query)	Date interval cannot exceed 14 days
Audit APIs (Developer Center)	Beyond 14 days	Use asynchronous query endpoints
Amazon EventBridge	All available audit events	Useful for backup or ingestion into external SIEM/log tooling

# Interaction Audit Trail (Related but Separate Feature)

The Audit Viewer covers **org-wide admin changes**. There is a separate **Audit Trail** tab on individual interactions that tracks recording and evaluation-level access:

Attribute	Detail
Navigation	Performance → Workspace → Interactions → click interaction → <b>Audit Trail</b> tab → <b>Load All Audits</b>
Alt Navigation	Menu → Analytics → Analytics Workspace → Interactions tab
Permission Required	Audits > Interaction Details > View
Roles	Quality Administrator, Quality Evaluator
Objects tracked	Evaluations, Annotations, Recordings, Calibrations, Screen Recordings, Surveys

# Compliance Use Cases

Regulation	How Audit Viewer Helps
GDPR	Track who accessed or changed user/contact data configurations
HIPAA	Verify access controls and configuration change history
PCI-DSS	Audit routing, recording, and security configuration changes
Internal Change Management	Identify who changed a queue, flow, role, or schedule and when

# Best Practices

Practice	Reason
Review audit logs regularly	Required by many compliance frameworks
Use Filter by Service to scope searches	Reduces noise when investigating a specific area
Use Filter by Entity for targeted investigations	Quickly find all changes to a specific object by its ID
Export or stream to external tooling via EventBridge	Retain events beyond the 14-day UI window
Grant <code>Audits &gt; Audit &gt; View</code> only to appropriate roles	Audit logs contain sensitive config change history

# Key Takeaways

Topic	Summary
Navigation	<code>Admin → Troubleshooting → Audit Viewer</code> or <code>Menu → IT and Integrations → Audit Viewer</code>
Permission	<code>Audits &gt; Audit &gt; View</code>
Viewer modes	Full-page (detailed) and mini footer (lightweight)
Date limit	Last <b>14 days</b> in UI; older data via Audit API
Event details	Who, what, before/after values, RemoteIP, related events
Filtering	By date range, service, entity ID, or user
Real-time only	UI shows real-time query results; async data via API or EventBridge
Interaction Audit Trail	Separate feature on individual interactions — different permission and navigation

Revision #1

Created 13 March 2026 07:05:02 by Cesar Gzz

Updated 13 March 2026 07:05:10 by Cesar Gzz