



# SAS<sup>®</sup> Viya<sup>®</sup> 3.5 Administration: Auditing

## 3.5

This document might apply to additional versions of the software. Open this document in [SAS Help Center](#) and click on the version in the banner to see all available versions.

<b>Auditing: Overview</b> .....	<b>1</b>
<b>Auditing: How To</b> .....	<b>3</b>
View Audit Record Reports and Tables .....	3
View a File of Audit Records .....	4
Reset Audit Record Extraction .....	5
Change Auditing Configuration .....	5
Change the Amount of Data Displayed in the User Activity Report .....	7
<b>Auditing: How To (CLI)</b> .....	<b>8</b>
Introduction .....	8
Examples .....	8

---

## Auditing: Overview

An audit record is generated whenever these types of events occur:

- an action is performed on a resource (such as a folder or a job). Actions include access to the resource and any changes made to the resource (such as updating, creation, or deletion).
- a security-related action occurred, such as logging on to an application or changing an authorization rule

## 2

By default, these actions generate audit records:

- resource read failure
- resource created, updated, or deleted
- security actions (logon attempts, logoff attempts, accessing authorization rules, updating authorization rules)

See [“Change Auditing Configuration” on page 5](#) for information about changing the actions that generate an audit entry.

The audit records are stored in the SAS Infrastructure Data Server and, by default, are retained for seven days. Records older than seven days can be archived to a local storage location. See [“Change Auditing Configuration” on page 5](#) for information about changing the archiving behavior.

The Audit service only creates records. It cannot update records.

Audit records are listed by SAS administrators using the SAS Viya Audit Plug-in Command Line Interface (CLI). By default, the CLI returns a list of audit records that includes the following columns:

### ID

generated identifier of the audit record

### Time Stamp

the date and time that the action occurred. The time stamp uses ISO8601 format (YYYY-MM-DDThh:mm:ss.Z). Z specifies that the time is in UTC.

### Action

the action that was performed (such as read, create, or update)

### State

the outcome of the action (success or failure)

### User ID

the user, application, or service that initiated the action

### Application

the application or service that performed the action

### Administrative Action

The value for a given action is `true` if the user who created the action was signed on as a SAS administrator at the time of the action. The sign-on process has two steps: enter credentials for an administrative account, and opt in to assumable groups. If the user has not opted in to assumable groups, then the values in the Administrative Action column are `false`.

### URI

the Uniform Resource Identifier of the service that created the action.

The columns that are returned in a particular list command vary depending on the options that are specified in the command.

The following image illustrates a command that returns audit records that contain the action `remove`.

```
C:\AdminCli\WIN>sas-viya audit list --action remove
ID                               Time Stamp                Action  State  User ID  Application  Administrative Action  URI
f57e2d3c-12ba-4943-9bd8-fb3897d13b2a  2023-01-18T04:31:48.892Z  remove success sasin    files          true                  /files/files/
d320e07e-a6ff-4bad-b94a-939b5a27a61e  2023-01-18T04:31:50.705Z  remove success sasin    files          true                  /files/files/
abff7c6a-ad81-4333-8fd4-f4d34fd9397  2023-01-18T04:31:49.751Z  remove success sasin    files          true                  /files/files/
da4c3087-35bf-42c5-a814-a1ec4b594b67  2023-01-18T04:38:33.34Z   remove success stpweb1  files          false                 /files/files/
42cb6239-01bb-4c8b-a0ea-244287ad3b19  2023-01-18T04:37:19.649Z  remove success sasin    files          true                  /files/files/
c2eb6715-7217-41b3-892c-48bc5e650048  2023-01-18T04:38:29.078Z  remove success sasin    files          true                  /files/files/
8e30ec66-0ce9-4abe-8666-2d2fac5956c0  2023-01-18T04:38:29.52Z   remove success sasin    files          true                  /files/files/
ba700913-4d15-41f5-888c-d0b125ad8034  2023-01-18T04:38:34.725Z  remove failure stpweb2  files          false                 /files/files/
62baa731-e047-4772-82d7-cc14e36e4c7a  2023-01-18T04:31:45.975Z  remove success sasin    files          true                  /files/files/
```

To learn more about the CLI, see [“Auditing: How To \(CLI\)” on page 8](#).

SAS Viya operations infrastructure also includes a predefined task to process the audit records, create a CSV file of the extracted records, and then create a CAS table with the records. Predefined reports enable you to view detailed information about access to reports, applications data, and data plans; about access by user and about access failures. See [“View Audit Record Reports and Tables” on page 3](#) for more information.

---

# Auditing: How To

---

## View Audit Record Reports and Tables

---

The User Activity report is available from the SAS Environment Manager Dashboard. You can use it to view graphs and tables of the collected audit record data.

The genAudit task, which runs every two hours (by default), collects information from the audit records that is then used to create the User Activity report. Because the task runs using the credentials of the SAS install user (sas), it collects only those records to which the SAS install user has access. The SAS install user is not a SAS administrator ID.

---

**Note:** This report is not available if you are a tenant administrator.

---

Follow these steps to view the reports.

- 1 On the SAS Environment Manager Dashboard, select **Show Reports**. A gallery of available reports is displayed at the bottom of the Dashboard.
- 2 Click in the **User Activity** report and select **Open**. Use the control to navigate through the report gallery to locate the **User Activity** report.
- 3 The **User Activity** report contains pages that display the audit information based on different criteria, such as user activity, report access, and data table access. Audit records are retained for seven days, so by default, the report displays information from all of the past seven days. Use the slider on each report page to view information only for a selected time range.

Select the page of the report that contains the type of information that you want to view. These pages are available:

### Main

contains thumbnail graphs for the charts **Most active users**, **Activity counts**, **Most active data**, and **User Actions over time**.

### Most Active Users

displays the **Most Active Users** and **Activity Over Time** charts, and a table of the audit records ordered by level of user activity. The table does not display audit records from SAS internal users. Select a bar in the **Most Active Users** chart to display the **Activity Over Time** chart for the selected user, and to list the audit records only for the selected user.

### Application Usage

displays the **Most used Applications** and **Application Activity** charts, and a table of the audit records orders by level of application activity. Select a bar in the **Most used Applications** chart to display the **Application Activity** chart for the selected application, and to list the audit records only for the selected application.

**Report Activity**

displays the **Top Report Usage** chart and a table of the audit records for report access. By default, the chart and table display report activity for all users. To view the report usage and audit records only for a specific user, select the user in the **Users** menu.

**Data Activity**

displays the **Frequently Accessed Tables** chart and a table of the audit records for data table access. By default, the chart and table display data table activity for all users. To view the data table usage and audit records only for a specific user, select the user in the **Users** menu.

**Data Plan Activity**

displays the **Top Report Usage** chart and a table of the audit records for data plan access. By default, the chart and table display data plan activity for all users. To view the data plan usage and audit records only for a specific user, select the user in the **Users** menu.

**Failures**

displays the **Failed Requests per Application** and **Failed Activities** charts, and a table of the audit records only for failed requests. By default, the **Failed Activities** chart and the audit records table display failures for all applications. To view the **Failed Activities** chart and audit records for a specific application, select the application's bar in the **Failed Requests per Application** chart.

**Details**

displays a table of audit records. By default, the table displays all audit records. To filter the table, use the menus at the top of the table to display only those records matching your selected criteria. You can filter by user, application, action, and state, and multiple criteria are allowed

---

**Note:** If the User Activity report is blank or displays the message `Cannot find the requested data source`, you must verify that the command-line interface (CLI) was deployed properly in your SAS Viya environment. See [“Edit the Inventory File” in SAS Viya for Linux: Deployment Guide](#) for more information.

---

---

## View a File of Audit Records

The genAudit task is included in the default task list for the SAS Viya operations infrastructure agent. The task runs automatically every two hours and performs these functions:

- extract the audit records for reports, data plans, CAS management, and CAS access management
- write the extracted audit records to a CSV file in a cache location
- remove audit records in the CSV file from the eighth day of collection
- use the CSV file to create a table in the SystemData caslib called AUDIT

You can use the extracted audit data in the AUDIT table to perform analysis or create reports.

---

## Reset Audit Record Extraction

If the data created by the audit record extraction process becomes corrupted or incorrect, you can reset the extraction process. This action does not alter or remove any of the original audit records. It deletes only the data in the CSV file that is extracted by the genAudit task.

This is an example of a scenario where you should reset the process. The CSV file is designed to hold seven days of audit records, so one step in the process is to remove records only from the eighth day of collection. It does not remove records that are older than the eighth day. If something prevents the genAudit task from running on a particular day, the eighth-day records are not removed, and they remain in the CSV file from that point forward.

You should reset the extraction process if the sas-ops-agentsrv process is down for more than 24 hours.

To reset the record extraction process, delete all of the files in the directory `/opt/sas/viya/config/var/cache/auditcli` on the Operations host (as specified in the Ansible inventory.ini file). The genAudit task creates new extracted audit data when the task runs again after two hours.



---

## Change Auditing Configuration

You can change configuration properties for the audit service to control how audit records are archived and to specify the services and actions that produce audit records.

See [“Configuration Properties: How to Configure Services”](#) in *SAS Viya Administration: Configuration Properties* for more information.

## Change How Audit Records Are Archived

- 1 In SAS Environment Manager, select  **Configuration**.
- 2 In the **View** field, select **Definitions**.
- 3 To change the configuration for how audit records are archived, select **sas.audit.archive** in the definition list.
- 4 Click  **Edit**. You can modify these properties:

**batchSize**

specifies the number of audit records archived at a time.

**enabled**

specifies whether to archive audit records. If enabled, records older than the specified retention period are removed from the archive table. If not enabled, the records are not archived and remain in the table.

**localRetention**

specifies the number of days that audit records are retained in the audit table in the SAS Infrastructure Data Server before they are archived.

**scanSchedule**

specifies the time at which the archive process starts (the default value is 000\*\*?, which specifies midnight each day).

**storage.local.destination**

specifies the location where archived records are stored if the **storageType** property is set to **local**.



**storageType**

specifies whether records that are removed from the table are archived to a file (specify a value of **local** and specify a location in the **storage.local.destination** property) or discarded (specify a value of **none**).

- 5 Select **Save** to save your changes.

## Change Actions and Services That Create an Audit Record

The `sas.audit.record` property enables you to specify whether audit entries from specified applications or services or audit entries of a certain type are recorded. The fields in the **application** area control audit recording for specified services. The fields in the **type** area control audit recording for all services.

- 1 In SAS Environment Manager, select  **Configuration**.
- 2 In the **View** field, select **Definitions**.
- 3 To specify the actions and services that generate an audit record, select **sas.audit.record** in the definition list.
- 4 Click  **Edit**.
- 5 To specify whether entries are recorded from a specified application or service, select **+ Add property** in the **application** area.

In the Add Property window, specify the application or service in the **Name** field using the format `application.status`

- Valid values for *application* are `serviceName` values in the SAS Configuration Server. To obtain a list of all possible values, issue one of these commands:

Unix:

```
./sas-bootstrap-config catalog services | grep serviceName
```

Windows:

```
sas-bootstrap-config.exe catalog services | findstr serviceName
```

These commands return a list of `serviceNames` that you can use as values for *application*.

...

```
"serviceName": "SASStudioV",
"serviceName": "SASThemeDesigner",
"serviceName": "SASVisualAnalytics",
"serviceName": "alert-track",
"serviceName": "analyticsComponents",
"serviceName": "analyticsDataSegmentation",
...
```

- Valid values for *status* are `enabled` or `state`. Specify `enabled` to control whether audit records are enabled for the service. Specify `state` to specify the state when audit records are created.

Specify the value for the property in the **Value** field.

These are examples:

- Specify `identities.enabled` in the **Name** field and `false` in the **Value** field to disable recording of entries from the Identities service.
  - Specify `SASLogon.state` in the **Name** field and `failure` in the **Value** field to disable recording of entries from the SASLogon service.
- 6 To specify the type of read action records that are recorded for all services, specify the record type in the **resource.action.read.state** field in the **type** area. For example, specify **failure** to record only failed read actions for all services. Specify **all** to record all read actions for all services.
  - 7 To specify whether resource records are recorded for all services, specify either **true** or **false** in the **resource.enabled** field in the **type** area.
  - 8 To specify the type of security records that are recorded for all services, specify the record type in the **security.action.read.state** field in the **type** area. For example, specify **failure** to record only failed security actions for all services. Specify **all** to record all read actions for all services.
  - 9 To specify whether security records are recorded for all services, specify either **true** or **false** in the **resource.enabled** field in the **type** area.
  - 10 To specify whether entries are recorded for a specified action or audit type, select **+ Add property** in the **type** area. In the Add Property window, specify the property in the **Name** field and the value of the property in the **Value** field.
    - For actions, use the format `resource.action.action_type.enabled`. Specify the value for the property in the **Value** field.  
For example, specify `resource.action.read.enabled` in the **Name** field and `false` in the **Value** field to disable recording of all read records.
    - For audit types, use the format `audit_type.enabled`. Specify the value for the property in the **Value** field.  
For example, specify `resource.enabled` in the **Name** field and `false` in the **Value** field to disable recording of all resource records.
  - 11 Select **Save** to save your changes.

---

## Change the Amount of Data Displayed in the User Activity Report

By default, the User Activity report displays seven days' worth of data. If you want to change the amount of data displayed in the report, you must change both of these values:

- the `-d` argument on the `genAudit` task, which specifies the number of days' worth of data that is collected from the audit table, copied to the `audit.csv` file, and made available in the AUDIT CAS system data `caslib`, where it is used in the User Activity report.
- the `localRetention` property, which specifies the number of days that audit records are retained in the audit table in the SAS Infrastructure Data Server before they are archived.

Follow these steps to change the number of days' worth of audit data that is displayed in the User Activity report.

- 1 From a Linux command line, issue this command:

```
/opt/sas/viya/home/bin/ops-config -base config/ops-agentsrv/sas.ops.task/genAudit
load -values "commandArgs=-a reports,dataPlans,casManagement,casAccessManagement"
```

```
-l 1000 -d days"
```

The value *days* specifies the number of days of data that genAudit extracts from the SAS Infrastructure Data Server SAS Audit service, which is then used in the User Activity report. Change this value to the number of days of data that you want to display (for example, -d 30 specifies 30 days).

- 2 Restart the sas-ops-agentsrv service. See “[Start and Stop a Specific Server or Service](#)” in *SAS Viya Administration: General Servers and Services* for information about restarting the service on Linux. See “[Start and Stop a Specific Server or Service](#)” in *SAS Viya Administration: General Servers and Services* for information about restarting the service on Windows.
- 3 Verify that the task was modified correctly. Use this command to list the genAudit tasks so that you can verify that the task was updated as expected:

```
/opt/sas/viya/home/bin/ops-config -base config/ops-agentsrv list | grep genAudit
```

- 4 Use the steps in “[Change Auditing Configuration](#)” on page 5 to change the localRetention property. The value of the localRetention property should be greater than or equal to the value that you specified in the genAudit task.

---

**Note:** Customized values for the genAudit task are not retained when you upgrade from SAS Viya 3.4 to SAS Viya 3.5.

---



---

## Auditing: How To (CLI)

---

### Introduction

The command-line interface for the Audit service enables you to return selected information from selected audit records. The records that are parsed are maintained in the Audit service and in the audit database.

The options for the command `sas-admin audit list` are listed by submitting the `--help` option.

The Audit CLI is one of many available plug-in CLIs that are available for the SAS Viya platform. To use the Audit CLI, you must first download, install, and configure the CLI, as described in “[Command-Line Interface: Overview](#)” in *SAS Viya Administration: Using the Command-Line Interfaces*.

---

### Examples

**Example:** List all unsuccessful attempts by user `jthsmythe` to create new jobs in SAS Studio after a specified date, using ISO8601 time format.

```
sas-admin audit list --user-id-contains "smythe" --application SASStudio --action
create --state failure --after 2024-01-15 2024-01-15T00:00.0Z
```

**Example:** List successful logins to SAS Viya, as recorded by the SAS Viya infrastructure.



```
sas-admin audit list --include-system-accounts --action login --state success
```

**Example:** List to the screen the details of a single audit record based on a previously returned ID.

```
sas-admin audit list --id c680aeed-479c-493d-921D-5hfd1c5921f3 --details
```

